



# Cybersecurity Products & Services

RFP#: COG-2127

Technical and Price Proposal

Submitted to:  
The Cooperative Council of Governors  
On Behalf of Equalis Group  
March 10, 2022

Electronic Submission via:  
[Equalis Group / Bonfire Hub](#)

By:  
Fortinet, Inc.  
899 Kifer Rd  
Sunnyvale, CA 94086-5205  
[www.fortinet.com](http://www.fortinet.com)

## Foreword

Fortinet, Inc. is pleased to respond to this Request for Proposal (RFP) for a national cooperative purchasing agreement through which Equalis Group Members will be able to purchase cybersecurity products and services.

In keeping with the instructions, our proposal consists of the electronic files containing the following information:

- A completed proposal checklist
- A technical proposal prepared on Proposal Form 1
- Other required proposal forms (Forms 3-23)
- Attachments referenced in Proposal Form 1:
  - Attachment A: Equalis Group Sample Administration Agreement
  - Attachment B: Price Proposal
- Supplemental information relevant to our proposal

We look forward to answering any questions you may have about our bid and, in the event we are awarded a contract, to the opportunity of providing high-quality products and services to Equalis Group Members.

For questions, please contact:

Cyd Stevenson  
Public Contracts Administrator  
Phone: 650-804-4690  
Email: [cstevenson@fortinet.com](mailto:cstevenson@fortinet.com)



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

## Table of Contents

Section	Title	Page
1.	<b>PROPOSAL FORM CHECKLIST .....</b>	<b>5</b>
2.	<b>PROPOSAL FORM 1 .....</b>	<b>(RFP PAGE 2)</b>
3.	<b>OTHER PROPOSAL FORMS .....</b>	<b>(RFP PAGE 31)</b>
	Proposal Form 2: Cost Proposal	
	Proposal Form 3: Diversity Vendor Certification Participation	
	Proposal Form 4: Certifications and Licenses	
	Proposal Form 5: Unresolved Findings for Recovery	
	Proposal Form 6: Mandatory Disclosures	
	Proposal Form 7: Dealer, Reseller, and Distributor Authorization	
	Proposal Form 8: Mandatory Supplier & Proposal Certifications	
	Proposal Form 9: Clean Air Act & Clean Water Act	
	Proposal Form 10: Debarment Notice	
	Proposal Form 11: Lobbying Certifications	
	Proposal Form 12: Contracto Certification Requirements	
	Proposal Form 13: Boycott Certification	
	Proposal Form 14: Federal Funds Certification Forms	
	Proposal Form 15: Arizona Contracto Requirements	
	Proposal Form 16: Ownership Disclosure Form (N.J.S. 52:25-24.2)	
	Proposal Form 17: Non-Collusion Affidavit	
	Proposal Form 18: Affirmative Action Affidavit (P.L. 1975, C.127)	
	Proposal Form 19: C.271 Political Contribution Disclosure Form	
	Proposal Form 20: Stockholder Disclosure Certification	
	Proposal Form 21: General Terms and Conditions Acceptance Form	
	Proposal Form 22: Equilis Group Administration Agreement Declaration	
	Proposal Form 23: Master Agreement Signature Form	

**ATTACHMENTS**

- A EQUALIS GROUP SAMPLE ADMINISTRATIVE AGREEMENT .....
- B PRICE PROPOSAL (PROPOSAL FORM 2 - SEE EXCEL DOCUMENT)

**APPENDICES (SUPPLEMENTAL INFORMATION)**

Products & Services  
Commercial Agreements  
NSE Certification Levels  
Case Studies



# PROPOSAL FORM CHECKLIST

## The following documents must be submitted with the Proposal

The below documents can be found in Section 2; Proposal Submission and Required Bid Forms and must be submitted with the proposal. Please note Proposal Form 2 is a separate attachment (attachment B).

### TECHNICAL PROPOSAL

- ☒ **Proposal Form 1: Technical Proposal**

**PROPOSAL PRICING:** Attachment B is provided separately in a Microsoft Excel file and is required to complete your cost proposal.

- ☒ **Proposal Form 2: Cost Proposal**

### OTHER REQUIRED PROPOSAL FORMS:

- ☒ **Proposal Form 3: Diversity Vendor Certification Participation**
- ☒ **Proposal Form 4: Certifications and Licenses**
- ☒ **Proposal Form 5: Unresolved Findings for Recovery**
- ☒ **Proposal Form 6: Mandatory Disclosures**
- ☒ **Proposal Form 7: Dealer, Reseller, and Distributor Authorization**
- ☒ **Proposal Form 8: Mandatory Supplier & Proposal Certifications**
- ☒ **Proposal Form 9: Clean Air Act & Clean Water Act**
- ☒ **Proposal Form 10: Debarment Notice**
- ☒ **Proposal Form 11: Lobbying Certification**
- ☒ **Proposal Form 12: Contractor Certification Requirements**
- ☒ **Proposal Form 13: Boycott Certification**
- ☒ **Proposal Form 14 Federal Funds Certification Forms**
- ☒ **Proposal Form 15: Arizona Contractor Requirements**
- ☒ **Proposal Form 16: Ownership Disclosure Form**
- ☒ **Proposal Form 17: Non-Collusion Affidavit**
- ☒ **Proposal Form 18: Affirmative Action Affidavit**
- ☒ **Proposal Form 19: C. 271 Political Contribution Disclosure Form**
- ☒ **Proposal Form 20: Stockholder Disclosure Certification**
- ☒ **Proposal Form 21: General Terms and Conditions Acceptance Form**
- ☒ **Proposal Form 22: Equalis Group Administration Agreement Declaration**
- ☒ **Proposal Form 23: Master Agreement Signature Form**

*(The rest of this page is intentionally left blank)*

# **Technical Proposal (Form 1)**

# PROPOSAL FORM 1: TECHNICAL PROPOSAL

1. <u>OVERVIEW &amp; QUALIFICATIONS</u>		
<b>1.1. Company Information</b>		
<b>1.1.1. Company Name:</b>	Fortinet, Inc.	
<b>1.1.2. Corporate Street Address:</b>	899 Kifer Rd.	
<b>1.1.3. Remittance Address:</b>	Sunnyvale, CA 94086	
<b>1.1.4. Main Telephone Number:</b>	408-235-7737	
<b>1.1.5. Website:</b>	<a href="http://www.fortinet.com">www.fortinet.com</a>	
<b>1.1.6. Formation.</b> In what year was the company formed? For how long has your company been operating under its present business name? If your company has changed its business name, include the most recent prior business name and the year of the name change.	Fortinet, Inc. was founded in 2000 and has been operating under the same name the entire time.	
<b>1.1.7. Legal Structure.</b> Check the box next to the option that best describes the company's legal structure. Include requested narrative in the space provided.	<input checked="" type="checkbox"/> Corporation – provide the State of incorporation and the company ownership structure. <input type="checkbox"/> <i>Partnership</i> – provide the State of registration and the names of all partners. <input type="checkbox"/> <i>Sole Proprietorship</i> – provide the State of registration and the name and title of the principal. <input type="checkbox"/> <i>Joint Venture</i> – provide the State of registration and the names and titles of all principals. <input type="checkbox"/> <i>Other</i> – provide detailed description of corporate structure and ownership.	
	Click here to provide additional information.	
<b>1.1.8. Federal Tax ID# or Social Security #:</b>	77-0560389	
<b>1.1.9. Primary Point of Contact.</b> Provide information about the Bidder representative/contact person authorized to answer questions regarding the proposal submitted by your company:	Contact Name:	Cyd Stevenson
	Title:	Public Contract Admin.
	Phone:	650-804-4690
	E-Mail Address	<a href="mailto:cstevenson@fortinet.com">cstevenson@fortinet.com</a>

<b>1.1.10. Authorized Representative.</b> Print or type the name of the Bidder representative authorized to address contractual issues, including the authority to execute a contract on behalf of Bidder, and to whom legal notices regarding contract termination or breach, should be sent (if not the same individual as in 1.1.9., provide the following information on each such representative and specify their function).	Contact Name:	John Whittle
	Title:	General Counsel
	Phone:	408-235-7737
	E-Mail Address	legal@fortinet.com
<b>1.2. Financial Strength &amp; Legal Considerations</b>		
<b>1.2.1. Financial Strength.</b> Demonstrate your financial strength and stability with meaningful data. This could include, but is not limited to, such items as financial statements, SEC filings, credit & bond ratings, letters of credit, and detailed reference letters. Note: you may mark this information as a “Trade Secret” per the terms outlined in the RFP.	<p>Fortinet is a 21-year-old, publicly-traded, US company (NASDAQ:FTNT). We have more than 565,000 customers worldwide. The financial highlights below, taken from the Form 10K we filed with the US Securities and Exchange Commission for 2021 (filed on <a href="#">February 25, 2022</a>) confirm that we are a profitable, financially stable company capable of fulfilling our obligations to Equalis Group Members under this contract</p> <p style="text-align: center;"><b>Financial Highlights for 2021</b></p> <ul style="list-style-type: none"> <li>• <b>Revenue:</b> Total revenue was \$3.34 billion for 2021, an increase of 28.8% compared to \$2.59 billion in 2020.</li> <li>• <b>Product Revenue:</b> Product revenue was \$1.26 billion for 2021, an increase of 36.9% compared to \$916.4 million in 2020.</li> <li>• <b>Service Revenue:</b> Service revenue was \$2.09 billion for 2021, an increase of 24.4% compared to \$1.68 billion in 2020.</li> <li>• <b>Billings<sup>1</sup>:</b> Total billings were \$4.18 billion for 2021, an increase of 35.3% compared to \$3.09 billion in 2020.</li> <li>• <b>Bookings<sup>2</sup>:</b> Total bookings were \$4.33 billion for 2021, an increase of 40.2% compared to \$3.09 billion in 2020.</li> <li>• <b>Deferred Revenue:</b> Total deferred revenue was \$3.45 billion as of December 31, 2021, an increase of 32.5% compared to \$2.61 billion as of December 31, 2020.</li> <li>• <b>GAAP Operating Income and Margin:</b> GAAP operating income was \$650.4 million for 2021, representing a GAAP operating margin of 19.5%. GAAP operating income was</li> </ul>	

	<p>\$531.8 million for 2020, representing a GAAP operating margin of 20.5%.</p> <ul style="list-style-type: none"> <li>• <b>Non-GAAP Operating Income and Margin<sup>1</sup>:</b> Non-GAAP operating income was \$875.5 million for 2021, representing a non-GAAP operating margin of 26.2%. Non-GAAP operating income was \$698.0 million for 2020, representing a non-GAAP operating margin of 26.9%.</li> <li>• <b>GAAP Net Income and Diluted Net Income Per Share Attributable to Fortinet, Inc.:</b> GAAP net income was \$606.8 million for 2021, compared to GAAP net income of \$488.5 million for 2020. GAAP diluted net income per share was \$3.63 for 2021, based on 167.1 million diluted weighted-average shares outstanding, compared to GAAP diluted net income per share of \$2.91 for 2020, based on 167.7 million diluted weighted-average shares outstanding.</li> <li>• <b>Non-GAAP Net Income and Diluted Net Income Per Share Attributable to Fortinet, Inc.<sup>1</sup>:</b> Non-GAAP net income was \$666.0 million for 2021, compared to non-GAAP net income of \$562.6 million for 2020. Non-GAAP diluted net income per share was \$3.99 for 2021, based on 167.1 million diluted weighted-average shares outstanding, compared to \$3.35 for 2020, based on 167.7 million diluted weighted-average shares outstanding.</li> <li>• <b>Cash Flow:</b> In 2021, cash flow from operations was \$1.50 billion compared to \$1.08 billion in 2020.</li> <li>• <b>Free Cash Flow<sup>1</sup>:</b> Free cash flow was \$1.20 billion during 2021, compared to \$907.8 million in 2020.</li> </ul> <p><b><u>Guidance</u></b></p> <p>For the first quarter of 2022, Fortinet currently expects:</p> <ul style="list-style-type: none"> <li>• Revenue in the range of \$865 million to \$895 million</li> <li>• Billings in the range of \$1.050 billion to \$1.090 billion</li> <li>• Non-GAAP gross margin in the range of 75.5% to 76.5%</li> <li>• Non-GAAP operating margin in the range of 19.5% to 20.5%</li> <li>• Diluted non-GAAP net income per share attributable to Fortinet, Inc. in the range of \$0.75 to \$0.80, assuming a non-GAAP effective tax rate of 18%. This assumes a diluted share count of 166 million to 168 million.</li> </ul> <p>For the fiscal year 2022, Fortinet currently expects:</p> <ul style="list-style-type: none"> <li>• Revenue in the range of \$4.275 billion to \$4.325 billion</li> <li>• Service revenue in the range of \$2.685 billion to \$2.715 billion</li> </ul>
--	---

	<ul style="list-style-type: none"> <li>• Billings in the range of \$5.400 billion to \$5.480 billion</li> <li>• Non-GAAP gross margin in the range of 74.0% to 76.0%</li> <li>• Non-GAAP operating margin in the range of 24.0% to 26.0%</li> <li>• Diluted non-GAAP net income per share attributable to Fortinet, Inc. in the range of \$4.85 to \$5.00, assuming a non-GAAP effective tax rate of 18%. This assumes a diluted share count of 169 million to 171 million.</li> </ul> <p>These statements are forward looking and actual results may differ materially. Refer to the Forward-Looking Statements section below for information on the factors that could cause our actual results to differ materially from these forward-looking statements.</p> <p>Our guidance with respect to non-GAAP financial measures excludes stock-based compensation, amortization of acquired intangible assets and gain on intellectual property matter. We have not reconciled our guidance with respect to non-GAAP financial measures to the corresponding GAAP measures because certain items that impact these measures are uncertain or out of our control, or cannot be reasonably predicted. Accordingly, a reconciliation of these non-GAAP financial measures to the corresponding GAAP measures is not available without unreasonable effort.</p> <p><sup>1</sup> A reconciliation of GAAP to non-GAAP measures has been provided in the financial statement tables included in this press release. An explanation of these measures is also included below under the heading "Non-GAAP Financial Measures".</p> <p><sup>2</sup> Bookings represents the total value of all orders received during the fiscal period. Backlog represents orders received but not fulfilled and excludes Alaxala. When an order is fulfilled, billings and revenue are recognized.</p>
<b>1.2.2. Bankruptcy &amp; Insolvency.</b> Describe any bankruptcy or insolvency for your organization (or its predecessors, if any) or any principal of the firm in the last three (3) years.	None
<b>1.2.3. Litigation.</b> Describe any litigation in which your company has been involved in the last three (3) years and the status of that litigation.	We are subject to various claims, complaints and legal actions that arise from time to time in the normal course of business. We accrue for contingencies when we believe that a loss is probable and that we can reasonably estimate the amount of any such loss. There can be no assurance existing for future legal proceedings arising in the ordinary course of business or otherwise will not have a material adverse effect on our business, consolidated financial position, results of operations or cash flows.
<b>1.3. Industry Qualifications</b>	

<p><b>1.3.1. Company Identification.</b> How is your organization best identified? Is it a manufacturer, distributor, dealer, reseller, or service provider?</p>	<p>Fortinet is a manufacturer and global leader in cybersecurity solutions provided to a wide variety of organizations, including enterprises, communication service providers, government organizations and small businesses. Our cybersecurity solutions are designed to provide broad visibility and segmentation of the digital attack surface through our integrated Fortinet Security Fabric platform, which features automated protection, detection and response.</p> <p>Please see more information regarding the <i>Fortinet Security Fabric</i> in <b>Appendix D</b>.</p>
<p><b>1.3.2. Manufacturer Authorization.</b> If your company is best described as a distributor/dealer/reseller (or similar entity), please provide your written authorization to act as a distributor, dealer, or reseller on behalf of the manufacturer of the product(s) proposed in this RFP.</p>	<p>Fortinet, Inc. will be authorizing channel partners / resellers to act on our behalf.</p>
<p><b>1.3.3. Network Relationship.</b> If your company is best described as a manufacturer or service provider, please describe how your dealer network operates to sell and deliver the Products &amp; Services proposed in this RFP. If applicable, is your network independent or company owned?</p>	<p>Fortinet uses a two-tier model with distributors and resellers. Our independent reseller network covers all 50 states and includes value-added and managed security service providers (MSSPs) serving national, regional, state, local markets. Many of our resellers are certified in state programs for small, minority-owned, women-owned, veteran-owned, and disabled veteran-owned businesses.</p> <p><b><i>Engage</i></b>, Fortinet’s partner program has a singular goal for our partners: Provide a valuable, flexible platform to build a profitable and highly-differentiated security practice that leverages the industry’s best solutions to drive customer success.</p> <p><b><u>Profitability Through Technology Differentiation</u></b> Fortinet’s breadth of products are tightly integrated into one highly-automated, high-performing platform that spans endpoint, network, and cloud, and includes tools to easily connect with adjacent technologies.</p> <p><b><u>Business Success with Proven Credibility</u></b> Fortinet’s innovation superiority with hundreds of patents and industry-leading threat intelligence, alongside our customer ratings and independent analyst reports leadership validates and differentiates your offerings.</p> <p><b><u>Long-Term, Sustained Growth</u></b></p>

	<p>We're in this with our partners! We have no direct sales team, and we offer sustained sales marketing, and executive support so our partners can grow productive, predictable, and profitable relationships.</p> <p><b><u>ENGAGE</u></b> Align our program to partner's level of experience and the benefits and billings requirements that fit their business.</p> <ul style="list-style-type: none"> <li>• Advocate: Interested in starting a relationship with Fortinet. Has limited requirements and benefits</li> <li>• Select: Committed to delivering superior security solutions that best fit small-to-medium business security concerns.</li> <li>• Advanced: Have proven success delivering the full spectrum of Fortinet's solutions with certified staff to handle various implementation requirements from customers.</li> <li>• Expert: Proven Fortinet solutions experts, and have demonstrated consistently high revenue and can deliver the full range of Fortinet solutions, with experts on staff to manage complex deployments.</li> </ul> <p><b><u>EXPAND</u></b> Offers flexibility into Fortinet's program.</p> <ul style="list-style-type: none"> <li>• Integrator: Primarily reselling to customers' on-premises, but offer some managed services.</li> <li>• MSSP: Most, if not all billings come from selling managed security services</li> <li>• Cloud: Born-in-the-cloud or cloud-certified partner</li> </ul> <p><b><u>SPECIALIZE</u></b> A way for a partner to quickly elevate themselves in a crowded field with training, enablement and targeted solutions to expand capabilities and offerings while driving growth and profitability.</p> <p><b>Specializations:</b></p> <ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• LAN Edge and SD-Branch</li> <li>• Data Center</li> <li>• Adaptive Cloud Security</li> <li>• Zero Truce Access</li> <li>• Operational Technology</li> <li>• Security Operations</li> </ul>
<p><b>1.3.4. Industry Experience.</b> How long has your company provided the</p>	<p>Fortinet has offered the products and services in this response since its inception, more than 20 year ago and</p>



<p>products and services outlined in your response to this RFP? What percentage of your company's revenue in each of the last three (3) full calendar years was generated from these products and services?</p>	<p>100% of our revenue is from the sale of the products and services proposed here.</p> <table border="1"> <thead> <tr> <th>Year</th><th>Total Revenue</th></tr> </thead> <tbody> <tr> <td>2021</td><td>\$3,340.0</td></tr> <tr> <td>2020</td><td>\$2,594.4</td></tr> <tr> <td>2019</td><td>\$2,163.0</td></tr> </tbody> </table>	Year	Total Revenue	2021	\$3,340.0	2020	\$2,594.4	2019	\$2,163.0
Year	Total Revenue								
2021	\$3,340.0								
2020	\$2,594.4								
2019	\$2,163.0								
<p><b>1.3.5. Geographic Reach.</b> Describe your company's service area in the United States and which areas you intend to offer services under a resulting contract if awarded.</p>	<p>Fortinet uses our reseller network to make this contract available to SLED customers throughout the United States. We want to make sure that OH public agencies receive the maximum benefit of this contract, so our installment of resellers will include OH, Regional and National resellers. If awarded, we will be selectively engaging with resellers in all regions of the US to greatly expand the utilization of this contract in all 50 states.</p>								
<p><b>1.3.6. Certifications and Licenses.</b> Provide a detailed explanation outlining the licenses and certifications that are i) required to be held, and ii) actually held by your organization (including third parties and subcontractors that you use). Has your company maintained these certifications on an ongoing basis? If not, when and why did your company lose any referenced certifications?</p> <p><b>NOTE:</b> Provide copies of any of the certificates or licenses included in your response in <b><u>Proposal Form 5 - Certifications and Licenses</u></b>.</p>	<p>Fortinet is committed to the independent testing and certification of its products and services. ICSA, AV-Comparatives, Virus Bulletin, and other independent testing organizations have consistently validated the effectiveness of Fortinet solutions. Fortinet earned ICSA's prestigious Excellence in Information Security Testing (EIST) award for 15 years of participation in 2017 and has been recognized by ICSA for outstanding achievement in information security certification testing 10 years in a row.</p> <p>The full list of product certifications are included in <b>Appendix D – Products &amp; Services</b></p> <p>Included in <b>Appendix D</b>, as well as referenced in Proposal Form 5, find our ISO 9001 certification.</p>								
<p><b>1.3.7. Awards.</b> Describe any relevant awards received by your company for its products, services, innovation, and/or operations. Include information about the issuing organization and the year(s) the award was issued to your company.</p>	<p>Recognized for the 12<sup>th</sup> time in Network Firewalls Gartner Magic Quadrant and also Ranked #1 in 3 of 5 use cases in the companion Critical Capabilities report.</p> <p>We believe this recognition is due to our powerful FortiGate NGFWs which enable organizations to build high-performance, ultra-scalable, and security-driven networks. You can security any edge while delivering optimal user experience, even in the most dynamic hybrid environments.</p>								
<p><b>1.4. Industry Qualifications</b></p>									

<p><b>1.4.1. Public Sector Cooperative Contracts.</b> What Public Sector Cooperative Contracts (e.g., state term contracts, public sector cooperatives, etc.) does your company have in place to provide products &amp; services defined in this RFP? For each contract, when was the contract established, what is the expiration date, and how much annual revenue does your company generate through the contract(s) in each of the last three (3) calendar years?</p>	<p>Fortinet's business model is to rely primarily on distributor- and reseller-held contracts and to pursue national cooperative purchasing contracts only when aligned with our core competency in cybersecurity.</p> <p>We currently hold the NCPA contract for IT Security and Data Protection Solutions. We work with 42 resellers, many of which will be invited to join us on this contract should we be awarded. Fortinet's entire catalog can be sold using this contract vehicle.</p> <p>The NCPA contract was established in April, 2018 and expires April 2023.</p> <p>We also hold the OETC-22B Networking contract. It was awarded in February, 2022, and is good for use in all 50 states.</p> <p>The OETC contract expires Feb, 2025 and we are listing 9 resellers initially.</p>
<p><b>1.4.2. Education Success.</b> What is the i) total dollar amount, and ii) percentage of your company's total annual revenue generated by sales to educational institutions (i.e., K-12 schools &amp; school districts and high education)?</p>	<div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 10%;"></div> <p>Trade Secret Information as defined in ORC 1333.61.</p>
<p><b>1.4.3. Government Success.</b> What is the i) total dollar amount, and ii) percentage of your company's total annual revenue generated by sales to local governments (i.e., municipalities, counties, special districts, and state agencies)?</p>	<p>See response for 1.4.2.</p>
<p><b>1.4.4. Public Sector Strategic Growth Plan.</b> Describe your company's three to five-year public sector sales objectives and the key elements of your strategic plan to achieve those objectives. What is the total annual dollar value of your company's total revenue generated by local governments and educational</p>	<div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div>

What percentage of your company's total annual revenue is generated by sales to local governments and educational institutions?

[illegible]

\_\_\_\_\_.

**1.4.5. *Customer References.*** Provide references of at least five (5) local government or educational institution customers for which your company has provided products and services similar in nature and scope to those defined in this RFP in the last three (3) years. Each reference should include:

- |            |            |
|------------|------------|
| [REDACTED] |            |
| [REDACTED] | [REDACTED] |
|            | [REDACTED] |
|            | [REDACTED] |
|            | [REDACTED] |
| [REDACTED] | [REDACTED] |
|            | [REDACTED] |
|            | [REDACTED] |
|            | [REDACTED] |
|            | [REDACTED] |
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |
|            | [REDACTED] |
|            | [REDACTED] |
|            | [REDACTED] |
|            | [REDACTED] |
| [REDACTED] |            |
| [REDACTED] | [REDACTED] |
|            | [REDACTED] |
|            | [REDACTED] |
|            | [REDACTED] |
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |
|            | [REDACTED] |

		[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
	[REDACTED]	
	■	[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
	■	[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
	■	[REDACTED]
	■	[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
	[REDACTED]	
	A	[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]
	■	[REDACTED]
		[REDACTED]
		[REDACTED]
	■	[REDACTED]
	■	[REDACTED]
		[REDACTED]
		[REDACTED]
		[REDACTED]

	<div> <div></div> <div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> </div> </div> <div></div> <div></div> <p>Customer References provided above are Trade Secret Information as defined in ORC 1333.61.</p>
--	---

## 2. Products & Services

### 2.1. PRODUCTS & SERVICES

<p><b>2.1.1. Product &amp; Services</b>  <b>Description(s).</b> Provide a detailed description of the products and services you are offering as a part of your proposal.</p> <p><b>IMPORTANT.</b> This description along with the products and services included in the <b>Attachment B – Cost Proposal</b> will be utilized to define the overall products and services available under a resulting contract.</p>	<p>See <b>Appendix D: Product &amp; Services:</b></p> <ul style="list-style-type: none"> <li>• Product Matrix</li> <li>• FortiCare Overview</li> <li>• Professional Services Overview</li> <li>• Service Fabric Portfolio</li> <li>• Fortinet Professional Services Engineer (PSE) Bio</li> <li>• Product Certifications</li> <li>• ISO 9001 Certification</li> </ul>
<p><b>2.1.2. Open Market Products.</b>  Provide a detailed description of your ability to accommodate requests for Open Market Products. Open Market Products is a category of products that cannot be found in your standard catalog offering or non-inventoried products.</p>	<p>Fortinet does not offer products that are not included in our pricelist.</p>
<p><b>2.1.3. Differentiators.</b> Describe what differentiates your company's products and services from your competitors.</p>	<p><b>THE FORTINET SECURITY FABRIC: A STRATEGIC DIFFERENTIATOR</b>  Fortinet delivers a unique approach to security for higher education institutions. This architecture, called the Fortinet Security Fabric, provides deep automated visibility, distributed network segmentation, and analytics for real-time response. The Fortinet Security Fabric allows universities and colleges of all sizes to leverage existing investments while moving towards a more resilient integrated security architecture.</p>

	<p>Network security must protect at the many edges of the network and also inside the network, with a layered approach. Vulnerabilities exist everywhere, from devices and data paths to applications and users. Because organizations encounter so many potential threats, there are also hundreds of network security management tools intended to address individual threats or exploits or assist with other mission-critical infrastructure needs, such as continuous compliance. Organizations should prioritize network security solutions that cover the multitude of threats, using a platform approach that prioritizes integration and automation.</p> <p>To address the challenges that make cybersecurity increasingly challenging, an <i>open ecosystem</i> to unify multivendor solutions is required. These solutions should be broad, integrated, and automated. Fortinet's Open Architecture provides the following essential elements.</p> <ul style="list-style-type: none"> <li>• Provides broad visibility – eliminate siloes in security elements – allowing them to communicate with each other</li> <li>• Integrated solutions – share threat intelligence, coordinate automated responses</li> <li>• Maximizing automation – eliminate routine manual steps and errors, fill the expertise gap, deliver synchronized, consistent security as a force multiplier</li> <li>• Simplify deployment – pre-integrated, pre-evaluated and unified solutions</li> </ul> <p><b>Fortinet's Security-Driven Networking</b> strategy tightly integrates an organization's network infrastructure and security architecture, enabling the network to scale and change without compromising security operations. This next-generation approach is essential for effectively defending today's highly dynamic environments – not only by providing consistent enforcement across today's highly flexible perimeters, but by also weaving security deep into the network itself.</p> <p><b>FortiTrust Access</b>, which simplifies Zero Trust Network Access (ZTNA), is a user-based subscription that provides all the elements necessary to add ZTNA to your FortiGate-based network. The offering includes the ZTNA agent in FortiClient and cloud-based orchestration from FortiClient Cloud.</p> <p>FortiTrust Access allows organizations to deploy a secure means of delivering application access control whether or not the user is connected to the network. Further, the application being accessed can be located anywhere: the data center, a private cloud, or a public cloud.</p> <p>As cloud adoption accelerates, organizations are increasingly reliant on secure cloud solutions and</p>
--	---

	<p>infrastructures. Yet, organizations often end up with a heterogeneous set of technologies in use, with disparate cloud security controls in various cloud environments. <i>Fortinet Adaptive Cloud Security Solutions</i> provide the necessary visibility and control across cloud cybersecurity infrastructures, enabling secure applications and connectivity from data center to cloud.</p> <p>The combination of accelerating threat evolution and expanded attack surfaces has brought enterprise security teams to a tipping point in the battle against cyber crime: they can no longer win by throwing more products and people at the problem. Facing budgetary and staffing constraints and a scarcity of white-hat security experts, security leaders often cannot fully execute on their security strategies. But even if they could, cyber criminals are leveraging artificial intelligence (AI) and agile development techniques to outpace human security analysts and outmaneuver even the newest network defenses. Still, security leaders must prevail. Their organization's digital transformation (DX) rests on the assumption of a secure network environment. To avoid the damaging impact of debilitating attacks and data breaches (the cost of cyber crime has increased by 72% over the past five years), executives must take security to a new level.</p> <p>To keep up with the volume, sophistication, and speed of today's cyber threats, organizations need security operations that can function at machine speed. By applying <i>artificial intelligence, machine learning, as well as integration and automation</i>, organizations can reduce risk and improve efficiency. Advanced threat detection and response capabilities along with centralized security monitoring and optimization can easily be added across the <u>entire Fortinet Security Fabric</u>.</p> <p>Combining behavior-based <i>endpoint protection, detection, and response</i> offers a modern approach to endpoint security. Fortinet uses multiple machine learning and deep learning technologies to power all three functions at each endpoint. Fortinet provides a range of behavior-based detection and response capabilities that include and go beyond the endpoint. <i>Sandbox, deception, user and entity behavior analytics</i> work as integrated extensions of inline security controls to thwart cyberattacks. Designed to meet the needs of organizations of varying size and security maturity, a range of security options provide <i>centralized visibility, analytics, and control</i> across the security infrastructure.</p> <p>An intrusion prevention system (IPS) is a critical component of network security to protect against new and existing</p>
--	--

	<p>vulnerabilities on devices and servers. To stop sophisticated threats and provide a superior user experience, IPS technologies must inspect all traffic, including encrypted traffic, with a minimal performance impact.</p> <p><b>FortiGuard AI/ML-powered IPS</b> provides near-real-time intelligence with thousands of intrusion prevention rules to detect and block known and zero-day threats before they reach your devices. Natively integrated across the Security Fabric, IPS delivers the industry's highest performance end-to-end protection. FortiGuard IPS security service is available for Next-Generation Firewalls (hardware, virtual machine, as-a-service) FortiClient, FortiProxy, FortiADC and our Cloud Sandbox. Add our OT and IoT services to get even more granular protection for operational technology and IoT devices.</p>
<p><b>2.1.4. Manufacturing.</b> If best identified as a manufacturer, describe your manufacturing process and any advantages it offers over your competitors. Your response may include, but is not limited to, facility locations, explanation of the materials used during various manufacturing processes, a description of the inspection &amp; quality control processes, and identification of manufacturing certifications (e.g., ISO).</p>	<p>Fortinet outsources the manufacturing of our security appliance products to a variety of contract manufacturers and original design manufacturers.</p> <p>Approximately 83% of our hardware is manufactured in Taiwan. We submit purchase orders to our contract manufacturers that describe the type and quantities of our products to be manufactured, the delivery date and other delivery terms. Once our products are manufactured, they are sent to either our warehouse in California or to our logistics partner in Taoyuan City, Taiwan, where accessory packaging and quality-control testing are performed.</p> <p>Outsourcing our manufacturing and a substantial portion of our logistics enables us to focus resources on our core competencies. Our proprietary SPUs, which are key to the performance of our appliances, are designed by Fortinet and built by contract manufacturers including Toshiba America Electronic Components, Inc. and Renesas Electronics America, Inc. These contract manufacturers use foundries in Taiwan and Japan operated by either Taiwan Semiconductor Manufacturing Company Limited or by the contract manufacturer itself.</p> <p>The components included in our products are sourced from various suppliers by us or, more frequently, by our contract manufacturers. Some of the components important to our business, including certain CPUs are available from limited or sole sources of supply.</p>
<p><b>2.1.5. Warranty.</b> Provide a copy of the manufacturer's warranty. If required, please attach the warranty as an attachment, as</p>	<p>See <b>Appendix E: Commercial Agreements</b>, which includes the following Supplemental Agreements (as defined in Section 2.2 of the Master Agreement) that applicable to our products and services:</p>



<p>instructed in this document. Describe notable features and/or characteristics of the warranty that a public sector customer would find interesting or appealing. Pricing related to the any extended warranty options must be included in <b><u>Attachment B – Cost Proposal.</u></b></p>	<ul style="list-style-type: none"> <li>• Fortinet Product License Agreement/EULA and Warranty Terms</li> <li>• Fortinet Services Terms and Conditions</li> <li>• Fortinet Professional Services Terms and Conditions</li> </ul> <p>Key warranty terms are:</p> <ul style="list-style-type: none"> <li>• Fortinet warrants that the hardware portion of any Fortinet product P ("Hardware") will be free from material defects in workmanship as compared to the functional specifications for the period of one year or five years (depending on the product line. Fortinet's sole obligation shall be to repair or offer replacement Hardware for the defective Hardware at no charge to the original owner. This obligation is exclusive of transport fees, labor, de- installation, installation, reconfiguration, or return shipment and handling fees and costs, and Fortinet shall have no obligation related thereto.</li> <li>• Fortinet warrants that Software as initially shipped by Fortinet will substantially conform to Fortinet's then-current functional specifications for the Software, as set forth in the applicable documentation for a period of ninety (90) days if the Software is properly installed on approved Hardware and operated as contemplated in its documentation.</li> </ul> <p>The support described above is provided by our FortiCare support team, which also provides the following services to our global customer base:</p> <ul style="list-style-type: none"> <li>• 24x7 support plans sold in one-, three-, and five-year increments.</li> <li>• Premium RMA plans providing next-day or (where available) four-hour delivery of replacement equipment.</li> </ul> <p>Advanced service programs for enterprise customers.</p>
<b>2.2. Additional Services</b>	
<p><b>2.2.1. Turnkey Capabilities.</b> Describe the capabilities available through your company and, if applicable, your authorized network of dealers, distributors, and resellers that support your ability to provide turnkey</p>	<p>FortiCare Professional Services is available for all Fortinet products and is customized to meet each customer’s needs from streamlined deployment, capability optimization, and ongoing operations. You can read more about the full range of offerings in <i>Appendix D / FortiCare Professional Services.</i></p>

solutions to Equalis Group Members. Your response may include, but is not limited to, site assessment, equipment consultations & recommendation, installation, inspection, and maintenance.	
<b>2.2.2. Installation or Set-up.</b> Is installation or set-up available to Members as a part of your proposal?	Fortinet does offer installation and set-up. Please refer to <b>Appendix D – Products &amp; Services</b> for full description of Fortinet implementation services.
<b>2.2.3. Installers.</b> If you responded Yes to the previous question, is the installation service performed by a company owned installation team or one of your dealers or resellers?	Installation services are performed by Fortinet and authorize resellers. Please refer to <b>Appendix D – Products &amp; Services</b> for more information.
<b>2.2.4. Qualifications.</b> Describe the qualification of your installation and set-up crews. Your response may include, but is not limited to, training and certification requirements.	Included in <b>Appendix D – Products &amp; Services</b> , you will find the basic <i>Fortinet Professional Services Engineer (PSE) Bio</i> .
<b>2.2.5. Training.</b> If yes, provide a description of the training services offered. <b>Note:</b> <i>Training services are not limited to those provided to the members but can also extend to the training you provide you dealers, distributors, and resellers.</i>	<p>The Fortinet Network Security Expert (NSE) program is an eight-level training and certification program that is designed to provide interested technical professionals with an independent validation of their network security skills and experience. The NSE program includes a wide range of self-paced and instructor-led courses, as well as practical, experiential exercises that demonstrate mastery of complex network security concepts.</p> <p>Please see <b>Appendix F – Fortinet Training</b>.</p>
<b>2.2.6. Maintenance Services.</b> If yes, provide a description of the maintenance services included in your proposal.	<p>FortiCare Services: Expertise at Your Service</p> <ul style="list-style-type: none"> <li>• 24x7 Global Support</li> <li>• 1,000+ NSE and industry Certified Global Resources</li> <li>• 3 Regional Centers of Expertise</li> <li>• 19 Support Centers</li> <li>• 40 Regional Depots</li> <li>• 200+ In-Country Depots</li> <li>• 4-hour Expedited Hardware Replacement Availability</li> </ul> <p>For detailed information, please see <b>Appendix D: Products and Services</b></p>
<b>2.3. Value Add</b>	

<p><b>2.3.1. Additional Offering.</b> Please include any additional products and services not included in the scope of the solicitation that you think will enhance and add value to this contract's participating agencies.</p>	<p>Fortinet's goal if awarded a contract under Equalis Group Cyber Security Products &amp; Services program is to establish a product, mutually beneficial partnership that benefits Equalis Group Members. To accomplish this, we have elected to include our entire commercial price list in this offer (with the exception of certain legacy products from our acquisition of Meru Networks in 2015). Given the nature of our business, most of the products and services that we offer fall squarely within the scope of this offer. However, our decision to include our full price list means that Equalis Group Members will also be able to acquire products from our other product lines, ie. FortiVoice (IP PBX phone systems for business), FortCamera/FortiRecorder (our network-based video security solution).</p> <p>Based on the evaluation criteria included in the RFP, it is clear that providing good value to Equalis Group Members also means demonstrating a commitment to effective support in these areas:</p> <ul style="list-style-type: none"> <li>• <b>Marketing.</b> To ensure we meet expectations for providing effective marketing support, we have included a senior-level marketing resource on our contract team for this contract to ensure Equalis Group Members are aware of our contract and know how to leverage it to obtain our best-of-breed cybersecurity products/solutions at competitive prices.</li> <li>• Increasing the presence of MWBEs and HUBs in the Equalis Group contracting program. Fortinet intends to allow authorized resellers to use our contract and has a strong program in place for recruiting and supporting our channel partners. This puts us in position to create opportunities for MWBEs and HUBs as authorized resellers.</li> <li>• <b>Customer Service.</b> See section 3.2.1 for our description of our comprehensive customer support program. This is the same customer support program that US Federal agencies and some of the world's largest financial institutions and telecommunications carriers rely on to provide support for their Fortinet Network Security and Security Fabric solutions.</li> </ul>
<p><b>3. <u>Business Operations</u></b></p>	
<p><b>3.1.1. Logistics</b></p>	

<p><b>3.1.2. Distribution Capabilities.</b> Describe how supplier proposes to distribute the products/services in Bidder's defined geographic reach.</p>	<p>Fortinet sells through a network of authorized distributors in the United States to support our commercial as well as our state and local business.</p> <ul style="list-style-type: none"> <li>• Exclusive Networks USA</li> <li>• Ingram Micro Inc.</li> <li>• TD Synnex</li> <li>• Carahsoft Technology Corporation</li> <li>• immixGroup</li> </ul> <p>All are well established, global distributors who have non-exclusive rights to distribute the full Fortinet line card here in the U. S.</p> <p>Resellers are free to choose which distributor(s) they work with, and are free to get quotes from multiple distributors to obtain the best possible pricing.</p>
<p><b>3.1.3. Distribution Centers.</b> Provide the number, size and location of Supplier's distribution facilities, warehouses, and retail network as applicable.</p>	<p>Fortinet's infrastructure for product distribution and support encompasses three global Centers of Excellence (COE) supplemented by 19 support centers, 40 regional depot, and 200+ in country depots.</p>
<p><b>3.1.4. Supply Chain.</b> Identify all other companies that will be involved in processing, handling, or shipping the products or services to the Equalis Group Member.</p>	<p>As noted previously, Fortinet uses a two-channel distribution model consisting of authorized resellers and authorized distributors. Companies at both the reseller level and the distributor level will be involved in receiving, handling and processing orders placed by Equalis Group Members.</p>
<p><b>3.1.5. Fill Rates.</b> Provide fill rates and average delivery timeframes met by specific distribution centers.</p>	<div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 90%;"></div> <div style="background-color: black; height: 15px; width: 10%;"></div> <p style="color: red;">Trade Secret Information as defined in ORC 1333.61.</p>
<p><b>3.1.6. On Time Delivery Rate.</b> Provide your average on-time delivery rate.</p>	<p>Fortinet's shipping term is EXW. When products are picked up from our dock, the actual delivery time varies depending on the customer's shipping method.</p>
<p><b>3.1.7. Expedited Orders.</b> Describe your approach to handling emergency orders and/or service. Your description may include, but is not limited to, response time, breadth of service coverage, and service level.</p>	<p>Every SLED sales team includes a Named Account Manager (NAM) and a Solutions Engineer (SE). Every Equalis Group Member will be able to call on either to have technical or order management issues escalated for resolution. This practice is baked into their job description. Any issue requiring emergency order of product or service is presented to Fortinet's Deal Desk to prioritize any and all approved escalations. The sales team is dedicated to ensuring the successful conclusion of any emergency order situation.</p>

3.2. Customer Service	
<p><b>3.2.1. Customer Service Department.</b> Describe your company's customer service department &amp; operations. Your description may include, but is not limited to, hours of operation, number and location of service centers, parts outlets, number of customer service representatives. Clarify if the service centers are owned by your company or if they are a network of subcontractors.</p>	<p>To provide effective support to a customer base that spans the globe, Fortinet has made it a priority to build a best-in-class global infrastructure for technical assistance and warranty/maintenance support. This infrastructure features three global Centers of Excellence (COE) supplemented by 19 support centers, 40 regional depot, and 200+ in country depots.</p> <p>This infrastructure provides the foundation for FortiCare Services, the program through which we will provide support for products covered by warranty, and thereafter, maintenance support for products covered by a FortiCare maintenance plan. The subsections below describe these services as they relate to the requirements for hardware and software maintenance.</p> <p><b><u>Hardware Maintenance</u></b> Our price list includes line items that will allow Equalis Group Members to purchase FortiCare Services for hardware appliance in one-, three-, and five-year increments. It also includes "bundles" that allow hardware, applicable FortiGuard security software subscriptions, and FortiCare services to be purchased together at a reduced price.</p> <p>Whether purchase separately or as part of a "bundle", an Equalis Group Member will be able to choose the hardware support plan that meets its needs from these options:</p> <ul style="list-style-type: none"> <li>• <b>FortCare 24x7 Service.</b> Provides access to technical support via the methods described above a 365x24x7 basis. This plan also includes an advanced replacement service for hardware failures.</li> <li>•</li> </ul> <p>For many products, Fortinet also provides the option to purchase Premium RMA Services. The available options with this service are:</p> <ul style="list-style-type: none"> <li>• <b>Next-day Delivery:</b> Parts delivered the day following RMA approval by Fortinet support</li> <li>• <b>4-Hour Courier:</b> Parts delivered on-site 24 hours a day, 7 days a week within 4 hours or RMA approval by Fortinet support (where available)</li> <li>• <b>4-Hour Courier with Onsite Engineer:</b> Engineer dispatched to perform the required RMA (Where available.)</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>Secure RMA Services:</b> This service allows for non-return of an appliance for those customers with strict rules and requirements for physical data protection.</li> </ul> <p><b><u>Software Maintenance</u></b></p> <p>Our price list includes perpetual licenses for a wide range of virtual appliances. We offer FortiCare Services packages (24x7) for these products in one-, three-, and five-year increments. These plans encompass technical support services for software products covered by an active warranty or maintenance plan. This support is available telephonically as well as through our web portal or by chat. Software error correction and software update services are also included.</p> <p><b><u>Premium Support Services</u></b></p> <p>In addition to the support services outlined above, Fortinet has included the following premium support services in our proposal as value-added services:</p> <ul style="list-style-type: none"> <li>• <b>Premium – Enterprise.</b> This is an annual service plan that provides fast-track access to an advanced services team. It also includes training and certification, a customized account plan, and pro-active after-hours support.</li> <li>• <b>Business – Enterprise.</b> This is an annual service plan that includes a designated engineer who will become familiar with the customer’s environment and assist in regular ticket reviews. It also includes bi-annual and root-cause analysis reporting.</li> <li>• <b>First-Enterprise.</b> This annual plan includes a designated lead engineer, aka technical account manager (TAM), who collaborates with the customer to build and maintain a long-term technical engagement, providing technical support, operational reviews and quarterly reporting. The service also includes best proactive guidance, upgrade assistance, extended software support to facilitate upgrade planning, and advanced notifications.</li> </ul>
<p><b>3.2.2. <i>Complaint Resolution.</i></b> Describe your customer complaint resolution process. Describe how unresolved complaints are handled.</p>	<p>As outlined in section 3.1.7, Equalis Group Members can start with their account team to resolve any product or service complaints.</p>
<p><b>3.3. Customer Set Up; Order &amp; Invoice Processing; Payment</b></p>	

<p><b>3.3.1. Authorized Distributors, Agents, Dealers, or Resellers.</b> Describe the different channels in which this contract will be made available to Equalis Group Members. Your response should include, but is not limited to, whether your organization will serve as the single point of sale or if the contract will be made available through a network of distributors, agents, dealers, or resellers.</p> <p><b>NOTE:</b> Bidders intending to authorize distributors, agents, dealers, or resellers must complete Proposal Form 6 - Dealer, Distributor and Reseller Authorization Form.</p>	<p>Fortinet sells through a two-tier channel system. Equalis Group Members, working with their chosen authorized Fortinet reseller, listed on Fortinet's website <a href="#">here</a>.</p>
<p><b>3.3.2. Customer Set Up.</b> Once an Equalis Group Member decides to accept your company's proposal for products and services as described in this RFP, what is the process for the Member to become a customer?</p>	<p>Before an authorized reseller listed on our Equalis contract submits a proposal to a customer that expresses interest in purchasing off our Equalis contract, the reseller will confirm that the customer is an Equalis Group Member. If not, the reseller will advise Fortinet so that Fortinet can provide them with any information they need to become an Equalis Group Member.</p> <p>Once it has been confirmed that the customer is an Equalis Group Member, a quote will be issued using the not-to-exceed prices on our Equalis contract price list. If the customer chooses to place an order, the reseller will instruct them to include Fortinet's Equalis contract number on their purchase order.</p> <p>Once the customer's products have been shipped, the customer should register as a customer (if not already registered) and register the products following instructions provided on the Fortinet website.</p>
<p><b>3.3.3. Order Process. Describe your company's proposal development and order submission process.</b></p>	<p>All quotes are provided by distributor to authorized reseller to Equalis Group Member who in turn place their order with their reseller, who, in turn places order with distributor. The distributor then places order with Fortinet. Any special pricing requires the Equalis Group Member, partner and distributor to reference a Fortinet approved special pricing (FTQ) number.</p>
<p><b>3.3.4. Invoice Process.</b> Describe your company's invoicing process.</p>	<p>Fortinet sells exclusively through authorized resellers who would invoice Equalis Group Members directly.</p>

<b>3.3.5. <i>Payment.</i></b> What are your standard payment terms? What methods of payment do your company accept?	Fortinet sells exclusively through authorized resellers who establish their own payment terms. If there are payment terms required by Equalis Group, Fortinet will recruit resellers who will be able to comply with those terms.
<b>3.3.6. <i>Financing.</i></b> Does your company offer any financing options or programs? If yes, describe the financing options available to Members.	Fortinet does not offer financing terms of any kind.
<b>3.4. Sustainability, Reclamation, and Recycling Initiatives</b>	
<b>3.4.1. <i>Sustainable Company Initiatives.</i></b> Describe the ways in which your company is addressing the issue of sustainability.	<p>Fortinet is committed to a sustainable environment. From such initiatives such as our commitment to carbon-neutrality for Scopes 1 and 2 in our owned facilities by 2030 and ensuring the use of 100% renewable energy in our owned facilities to ensuring that the environmental impact of our products is a priority issue from a social responsibility perspective - we are developing a robust sustainability program with engagement from our suppliers, customers, and employees. Fortinet is confident that we will progress towards a low-carbon future.</p> <p>For more detail on Fortinet’s Corporate Social Responsibility Policy, please visit <a href="https://www.fortinet.com/corporate/about-us/corporate-social-responsibility">https://www.fortinet.com/corporate/about-us/corporate-social-responsibility</a></p>
<b>4. <u>PRICING</u></b>	
<b>4.1. Cost Proposal</b>	
<b>4.1.1. <i>Pricing Model.</i></b> Provide a description of your pricing model or methodology identifying how the model works for the products and services included in your proposal.	Fortinet pricing methodology is <i>discount off MSRP</i> . Find details in pricing proposal.
<b>4.1.2. <i>Auditable.</i></b> Describe how the proposed pricing model is able to be audited by public sector agencies or CCOG to assure compliance with pricing in the Master Agreement.	All Equalis Group contract information will be published at <a href="https://www.fortinet.com/partners/EQUALIS_Group">https://www.fortinet.com/partners/EQUALIS_Group</a> . This will include the most current pricelist, authorized resellers and Fortinet account contacts.
<b>4.1.3. <i>Price Change Process.</i></b> Provide a description of your process for price changes.	Fortinet will publish updated pricelists quarterly on the website referenced in 4.1.2.



<p><b>4.1.4. Cost Proposal Value.</b> Which of the following statements best describes the pricing offered included in Bidder's cost proposal?</p>	<p>The prices offered in your Cost Proposal are:</p> <p><input type="checkbox"/> lower than what you offer other group purchasing organizations, cooperative purchasing organizations, or state purchasing departments.</p> <p><input checked="" type="checkbox"/> equal to what you offer other group purchasing organizations, cooperative purchasing organizations, or state purchasing departments.</p> <p><input type="checkbox"/> higher than what you offer other group purchasing organizations, cooperative purchasing organizations, or state purchasing departments.</p> <p><input type="checkbox"/> not applicable. Please explain below.</p> <p>It's important to note that Fortinet absorbs the 2% admin fee and is NOT passed through the partner to the Equalis Group Member.</p>
<p><b>4.1.5. Additional Savings.</b> Describe any quantity or volume discounts or rebate programs included in your Cost Proposal.</p>	<p>Additional discounts are available at the order level. Equalis Group Member should discuss with their reseller, who will negotiate with Fortinet.</p>
<p><b>4.1.6. Cost of Shipping.</b> Is the cost of shipping included in the pricing submitted with your response? If no, describe how cost associated with freight, shipping, and delivery are calculated.</p>	<p>Shipping costs are included in reseller invoice. Fortinet does not charge for shipping.</p>
<p><b>4.1.7. Pricing Open Market or Sourced Goods.</b> Propose a method for the pricing of Open Market Items. For example, you may supply such items "at cost" or "at cost plus a percentage" or you supply a quote for each such request.</p> <p><b>NOTE:</b> For a definition of Open Market Items, please refer to <b><u>Part One, Section 5 – Pricing</u></b>.</p>	<p>Fortinet does not offer products that are not included in our pricelist.</p>
<p><b>4.1.8. Total Cost of Acquisition.</b> Identify any total cost of acquisition costs that are NOT included in the pricing submitted with your response. This cost includes all additional charges that are not directly identified as freight or shipping</p>	<p>All Fortinet costs will be included in the cost proposal.</p>

<p>charges. For example, list costs for items like installation, set up, mandatory training, or initial inspection. Identify any parties that impose such costs and their relationship to the Bidder.</p>	
<b>5. <u>GO-TO-MARKET STRATEGY</u></b>	
<b>5.1. Bidder Organizational Structure &amp; Staffing of Relationship</b>	
<p><b>5.1.1. <i>Key Contacts.</i></b> Provide contact information and resumes for the person(s) who will be responsible for the following areas;</p> <ol style="list-style-type: none"> <li>1. Executive Contact</li> <li>2. Contract Manager</li> <li>3. Sales Leader</li> <li>4. Reporting Contact</li> <li>5. Marketing Contact.</li> </ol> <p>Indicate who the primary contact will be if it is not the Sales Leader</p>	<p><b><u>Executive Contact</u></b>  Kenny Holmes  Sr. Director, US SLED  618-830-3817  <a href="mailto:kholmes@fortinet.com">kholmes@fortinet.com</a>  <a href="#">LinkedIn Profile</a></p> <p><b><u>Contract Manager</u></b>  Cyd Stevenson  Public Sector Contractor Administrator  650-804-4690  <a href="mailto:cstevenson@fortinet.com">cstevenson@fortinet.com</a>  <a href="#">LinkedIn Profile</a></p> <p><b><u>Sales Leader</u></b>  Ryan Waters  VP US Commercial &amp; SLED  650-868-2618  <a href="mailto:rwaters@fortinet.com">rwaters@fortinet.com</a>  <a href="#">LinkedIn Profile</a></p> <p><b><u>Reporting Contact</u></b>  Cyd Stevenson  Public Sector Contractor Administrator  650-804-4690  <a href="mailto:cstevenson@fortinet.com">cstevenson@fortinet.com</a>  <a href="#">LinkedIn Profile</a></p> <p><b><u>Marketing Contact</u></b>  Michelle Coulombe  Director of North America SLED Field Marketing  617-686-5654  <a href="mailto:mcoulombe@fortinet.com">mcoulombe@fortinet.com</a>  <a href="#">LinkedIn Profile</a></p>
<p><b>5.1.2. <i>Sales Organization.</i></b> Provide a description of your sales</p>	<p>Fortinet SLED Sales organization is growing at a fantastic rate, more than doubling in the last two years.</p>

<p>organization, including key staff members, the size of the organization, in-house vs. third-party sales resources, geographic territories, vertical market segmentation, etc.</p>	<p>Leading the organization is a chief of staff that has the following groups reporting to him:</p> <p><b>Sales – East</b></p> <ul style="list-style-type: none"> <li>• 1 Vice President</li> <li>• 7 Regions, &gt; 55 AM/SE Teams</li> </ul> <p><b>Sales – West</b></p> <ul style="list-style-type: none"> <li>• 1 Vice President</li> <li>• 3 Regions, &gt; 32 AM/SE Teams</li> </ul> <p><b>Marketing</b></p> <ul style="list-style-type: none"> <li>• 1 Director</li> <li>• 14 Field &amp; Channel Marketing Teams</li> </ul> <p><b>Inside Sales</b></p> <ul style="list-style-type: none"> <li>• 4 Managers</li> <li>• &gt;30 Inside Sales</li> <li>• &gt;12 Business Development Reps</li> </ul> <p><b>Operations Programs</b></p> <p><b>SLED Program Development</b></p> <p><b>E-Rate Program Management</b></p> <p><b>Contract Management</b></p>
<p><b>5.2. Contract Implementation Strategy &amp; Expectations</b></p>	
<p><b>5.2.1. Contract Expectation.</b> What are your company's expectations in the event of a contract award?</p>	<p>The expectation it to use this contract in any and all opportunities that help us achieve our vision outlined in 5.2.2</p>
<p><b>5.2.2. Five (5) Year Sales Vision &amp; Strategy.</b> Describe your company's vision and strategy to leverage a resulting contract with Equalis over the next five (5) years. Your response may include but is not limited to; the geographic or public sector vertical markets being targeted; your strategy for acquiring new business and retaining existing business; how the contract will be deployed with your sales</p>	<p>Our core objective is to grow the Public Sector business outpacing the commercial segments while gaining market share in the US above the EU, EMEA, APAC business segments. Fortinet has over 600K customers with more than double the Next Generation Firewall deployments as our nearest competitor. We're recognized a leader in Gartner's Enterprise Firewall Magic Quadrant and participate in eight (8) total Magic Quadrants. Fortinet has over fifty (50) solutions that work in one Fabric platform with a single integrated user-interface (UI). To achieve our 40%+ growth targets were using a "land, expand,</p>

team; and the time frames in which this will be completed.	renew” strategy and model. That’s new logos, expansion of Firewall customers to full Fabric deployments to allow customers previously unachievable Cybersecurity efficacy for their organizations, and expanded renewal offering through Enterprise Agreements. Our business is run from a P&L and as an S&P 500 company were focused on multiple Key Performance Indicators (KPI’s) to obtain our aggressive targets. We are a 100% channel driven company using a distribution model. We have an aggressive hiring plan and new cybersecurity talent incubator starting with internships leading to entry-level cyber sales roles to career growth in sales, marketing, and business development. We have a mission of training another \$1Million+ people in Cybersecurity by 2025 through our world-class NSE Training Program.
<b>5.2.3. Sales Team Incentives.</b> Will your sales team be equally incentivized to leverage the Equalis Group Master Agreement when compared to their typical compensation structure?	We leverage quarterly incentives via our business partner model to drive required contract growth. We intend to continue using these incentives to drive sales via contracts. Over the next three to five years we will grow to over three hundred (300) dedicated sales teams for Government and Education (sales/engineering) and 25% of the US business segment.
<b>5.2.4. Sales Objectives.</b> What are your top line sales objectives in each of the five (5) years if awarded this contract?	See Response for 5.2.2
<b>6. ADMIN FEE &amp; REPORTING</b>	
<b>6.1. Bidder Organizational Structure &amp; Staffing of Relationship</b>	
<b>6.1.1. Administrative Fee.</b> Equalis Group only generates revenue when the Winning Supplier generates revenue based on contract utilization by current and future Members. The proposed Administrative Fee for this contract is <b>two percent (2%)</b> based on the terms disclosed in the <b><u>Attachment A – Model Administration Agreement</u></b> .	<input checked="" type="checkbox"/> <b>Agree</b> to proposed Administrative Fee <input type="checkbox"/> <b>Negotiate</b> Administrative Fee. Provide additional information below if you opt to negotiate.
	It’s important to note the Fortinet will absorb this fee. It will NOT be passed on to the reseller or Equalis Group Member.

<p><b>6.1.2. Sales &amp; Administrative Fee Reporting.</b> Equalis Group requires monthly reports detailing sales invoiced the prior month and associated Administrative Fees earned by the 15<sup>th</sup> of each month. Confirm that your company will meet this reporting requirement. If not, explain why and propose an alternative time schedule for providing these reports to Equalis Group.</p>	<p>Fortinet commits to meeting the reporting requirements for this contract.</p>
<p><b>6.1.3. Self-Audit.</b> Describe any self-audit process or program that you plan to employ to verify compliance with your proposed contract with Equalis Group. This process includes ensuring that Members obtain the correct pricing, reports reflect all sales made under the Contract, and Winning Supplier remit the proper admin fee to Equalis.</p>	<p>Fortinet Contract Manager will ensure that the website dedicated to this contract remains up to date and conduct onboarding calls with all authorized resellers to ensure they acknowledge the benefits and responsibilities of using this contract. Whenever possible, we would include an Equalis Group representative.</p> <p>As a matter of practice, monthly audits are currently conducted on all existing contract pricelists, partner lists, website updates; usually the last Friday of each month.</p>

## **APPENDIX D: PRODUCTS & SERVICES**

- Fortinet's Product Matrix
- FortiCare Services Brochure
- FortiCare Professional Services
- Fortinet Professional Services (PSE) Bio
- Fortinet Security Fabric
- Fortinet Product Certifications

## **APPENDIX E: COMMERCIAL AGREEMENTS**

- Product License Agreement / EULA and Warranty Terms
- Fortinet Service Terms & Conditions
- Fortinet Professional Service Terms & Conditions

## **APPENDIX F: NSE CERTIFICATION LEVELS**

## **APPENDIX G: CASE STUDIES**

## **IMPORTANT NOTE – DISCLAIMER BY FORTINET**

Thank you for considering Fortinet, the security leader!

To help ensure the process and understanding are clear, notwithstanding anything to the contrary:

- Responses and other information and statements provided are not binding on Fortinet in any way (whether by incorporation by reference or otherwise, such as representations and certifications in the response or other documentation or correspondence), are merely given to the knowledge of the respondent, and should not be relied upon as a binding commitment or promise, now or in the future
- Fortinet does not accept any master terms or other terms or agreement (including any attachments) related in any way to this Request for Proposal
- If Fortinet is selected as the vendor, subsequent thereto Fortinet is entitled to negotiate the terms of any agreement, and no document, contract or amendment is binding on Fortinet unless made in a formal, expressly-binding written agreement signed by Fortinet's General Counsel
- The responses and all information provided herein related to Fortinet or its products and services should be considered Fortinet confidential and proprietary information, and Fortinet provides confidential information hereunder in reliance on the recipient hereby agreeing to keep such information strictly confidential and to not use such information except to evaluate Fortinet in good faith as a vendor
- Performance criteria are measured under certain specific conditions and may vary, even materially, based on changes in the conditions such as in other environments
- Some information in this response is pre-release and forward looking and therefore is subject to change without notice. The purpose of this document is to provide a statement of the current direction of Fortinet's product strategy and product marketing efforts. Please note that this document includes Product Roadmap information and is neither intended to bind Fortinet to any particular course of product marketing and development nor to constitute a part of the license agreement or any contractual agreement with Fortinet or its subsidiaries or affiliates
- Fortinet reserves the right to make technical changes, and does not commit to any future deliverables
- Fortinet operates through a channel of independent distributors and resellers who are not agents of Fortinet and are not authorized to bind Fortinet in any way
- Any binding commitments to the end-customer must be obtained from the authorized reseller chosen by the customer, and any such commitment will not bind Fortinet in any way.

# **Other Required Forms**

## **Forms 3 through 23**



### PROPOSAL FORM 3: DIVERSITY VENDOR CERTIFICATION PARTICIPATION

**Diversity Vendor Certification Participation** - It is the policy of some Members participating in Equalis Group to involve minority and women business enterprises (M/WBE), small and/or disadvantaged business enterprises, disable veterans business enterprises, historically utilized businesses (HUB) and other diversity recognized businesses in the purchase of goods and services. Respondents shall indicate below whether or not they hold certification in any of the classified areas and include proof of such certification with their response.

a. **Minority Women Business Enterprise**

Respondent certifies that this firm is an MWBE

☐ Yes ☒ No

List certifying agency: Click or tap here to enter text.

b. **Small Business Enterprise (SBE) or Disadvantaged Business Enterprise (DBE)**

Respondent certifies that this firm is a SBE or DBE

☐ Yes ☒ No

List certifying agency: Click or tap here to enter text.

c. **Disabled Veterans Business Enterprise (DVBE)**

Respondent certifies that this firm is an DVBE

☐ Yes ☒ No

List certifying agency: Click or tap here to enter text.

d. **Historically Underutilized Businesses (HUB)**

Respondent certifies that this firm is an HUB

☐ Yes ☒ No

List certifying agency: Click or tap here to enter text.

e. **Historically Underutilized Business Zone Enterprise (HUBZone)**

Respondent certifies that this firm is an HUBZone

☐ Yes ☒ No

List certifying agency: Click or tap here to enter text.

f. **Other**

Respondent certifies that this firm is a recognized diversity certificate holder

☐ Yes ☒ No

List certifying agency: Click or tap here to enter text.

**PROPOSAL FORM 4: CERTIFICATIONS AND LICENSES**

Provide a copy of all current licenses, registrations and certifications issued by federal, state, and local agencies, and any other licenses, registrations, or certifications from any other governmental entity with jurisdiction, allowing Bidder to provide the products and services included in their proposal which can include, but not limited to licenses, registrations, or certifications. M/WBE, HUB, DVBE, small and disadvantaged business certifications and other diverse business certifications, as well as manufacturer certifications for sales and service must be included if applicable

Please also list and include copies of any certificates you hold that would show value for your response not already included above.

The table below contains federal certifications that are relevant to cybersecurity products/services as well as certifications from other organizations that certify cybersecurity products:

Category	Certification	Description	Latest Publication Date	
Product Certifications	<a href="#">ICSA Labs</a>	ICSA Labs is an independent division of Verizon. They provide third-party testing and certification of security and health-related IT products and network-connected devices to measure product compliance, reliability, and performance.	IPsec VPN	08/10/2021
			Firewall	08/25/2021
			WAF	09/27/2021
	<a href="#">AV-Comparatives</a>	AV-Comparatives is an independent lab offering systematic testing to determine whether security software—such as PC/Mac-based antivirus products and mobile security solutions—lives up to its claims. Using one of the largest sample collections in the world, they create a real-world environment for truly accurate testing. Certification by AV-Comparatives provides a globally recognized seal of approval for software performance.	Business Security Test: Mar-Jun 2021	
	<a href="#">SE Labs</a>	SE Labs tests a range of solutions, including endpoint software, network appliances, and cloud services, on their ability to detect attacks, protect against intrusions, or both.	Email Security Services Protection: Jan-Mar 2020	
	<a href="#">MEF 3.0</a>	MEF 3.0 is an SD-WAN Certification Program that uses Spirent as their SD-WAN Authorized Certification and Test Partner (ACTP). Certification involves rigorous tests of the service attributes and requirements defined in MEF 70 and described in detail in the upcoming MEF SD-WAN Certification Test Requirements (MEF W90) standard.	MEF 3.0 SD-WAN: Jun 2020	
Information Security	<a href="#">Virus Bulletin</a>	VB is a world leader in security software testing. Their publicly available test reports cover anti-malware protections of all types as well as enterprise-level email and web security solutions.	VBSpam	Sept 2021
			VB100	Sept 2021
	<a href="#">MITRE Engenuity</a>	MITRE Engenuity's ATT&CK™ evaluations assess the ability of a vendor's solutions to defend against specific adversary tactics and techniques. They openly publish these results to provide end-users with the information needed to make good purchasing decisions. These evaluations are not a competitive analysis. There are no scores, rankings, or ratings. Instead, they show how each vendor approaches threat detection in the context of the MITRE ATT&CK knowledge base to provide an unbiased assessment of detection and protection capabilities and highlight potential gaps to drive the industry forward.	Round 3: Fin7/Carbanak: Apr 2021	
	<a href="#">SOC2</a>	SOC2 is an auditing procedure that ensures that service providers securely manage their customers' data. It covers their security, availability, processing integrity, confidentiality, and/or privacy controls. Compliance is based on the AICPA's (American Institute of Certified Public Accountants) TSC (Trust Services Criteria).	SOC2 Type 2: Apr-Sept 2021	
Government Regulations	<a href="#">ISO</a>	ISO/IEC 27001 is an international standard for managing information security. It defines requirements and controls for establishing, implementing, maintaining, and continually improving an organization's Information Security Management System (ISMS).	ISO/IEC 27001: Jun 2021-Jun 2024	
	<a href="#">FIPS Validated</a>	The Federal Information Processing Standard 140-2 (FIPS 140-2) is an information technology security accreditation program for validating cryptographic modules developed by vendors that meet well-defined security standards.	FIPS 140-2 Level 1	Aug 2021
			FIPS 140-2 Level 2	Sept 2021
	<a href="#">Common Criteria</a>	Common Criteria is an international standard (ISO/IEC 15408) operated by 17 certificate-authorizing nations. 31 countries have accepted it for their respective government acquisition requirements for their IT/networking infrastructures.	CC EAL4+	Oct 2021
			FWcPP+IPS+VPN	Jan 2021

*(The rest of this page is intentionally left blank)*

## PROPOSAL FORM 5: UNRESOLVED FINDINGS FOR RECOVERY

**O.R.C. Chapter 9.24** prohibits CCOG from awarding a contract to any entity against whom the Auditor of State has issued a finding for recovery, if such finding for recovery is “unresolved” at the time of award. By submitting a proposal, a Bidder warrants that it is not now, and will not become, subject to an “unresolved” finding for recovery under **O.R.C. Chapter 9.24** prior to the award of any contract arising out of this RFP, without notifying CCOG of such finding. The Proposal Review Team will not evaluate a proposal from any Bidder whose name, or the name of any of the subcontractors proposed by the Bidder, appears on the website of the Auditor of the State of Ohio as having an “unresolved” finding for recovery.

Is your company the subject of any unresolved findings for recoveries?

☐

Yes

☒

No

## PROPOSAL FORM 6: MANDATORY DISCLOSURES

### 1. *Mandatory Contract Performance Disclosure.*

Disclose whether your company's performance and/or the performance of any of the proposed subcontractor(s) under contracts for the provision of products and services that are the same or similar to those to be provided for the Program which is the subject of this RFP has resulted in any formal claims for breach of those contracts. For purposes of this disclosure, "**formal claims**" means any claims for breach that have been filed as a lawsuit in any court, submitted for arbitration (whether voluntary or involuntary, binding or not), or assigned to mediation. For any such claims disclosed, fully explain the details of those claims, including the allegations regarding all alleged breaches, any written or legal action resulting from those allegations, and the results of any litigation, arbitration, or mediation regarding those claims, including terms of any settlement. While disclosure of any formal claims will not automatically disqualify a Bidder from consideration, at the sole discretion of Equalis Group, such claims and a review of the background details may result in a rejection of a Bidder's proposal. Equalis Group will make this decision based on the Proposal Review Team's determination of the seriousness of the claims, the potential impact that the behavior that led to the claims could have on the Bidder's performance of the work, and the best interests of Members.

Provide statement here. [Company's Disclosure: We are subject to various claims, complaints and legal actions that arise from time to time in the normal course of business. We accrue for contingencies when we believe that a loss is probable and that we can reasonably estimate the amount of any such loss. There can be no assurance existing for future legal proceedings arising in the ordinary course of business or otherwise will not have a material adverse effect on our business, consolidated financial position, results of operations or cash flows.](#)

[Subcontractor Disclosure: Fortinet intends to list authorized resellers on our contract if awarded a contract for this program. As part of our request to add any company to our contract as an authorized reseller, we will provide a statement from that company addressing this mandatory contract disclosure. We understand that the information the company provides may affect Equalis's determination as to whether we will be allowed to add the company as an authorized reseller.](#)

### 2. *Mandatory Disclosure of Governmental Investigations.*

Indicate whether your company and/or any of the proposed subcontractor(s) has been the subject of any adverse regulatory or adverse administrative governmental action (federal, state, or local) with respect to your company's performance of services similar to those described in this RFP. If any such instances are disclosed, Bidders must fully explain, in detail, the nature of the governmental action, the allegations that led to the governmental action, and the results of the governmental action including any legal action that was taken against the Bidder by the governmental agency. While disclosure of any governmental action will not automatically disqualify a Bidder from consideration, such governmental action and a review of the background details may result in a rejection of the Bidder's proposal at Group's sole discretion. Equalis Group will make this decision based on the Proposal Review Team's determination of the seriousness of the claims, the potential impact that the behavior that led to the claims could have on the Bidder's performance of the work, and the best interests of Members.

Provide statement here. [Company's Disclosure: In April, 2019, Fortinet agreed to a settlement valued at \\$545,00 with the US Department of Justice to resolve allegations that it violated the False Claims Act by falsely representing that certain Fortinet products that were sold through a Federal contract were in compliance with the Trade Agreement Act. The Department of Justice statement on this settlement, which can be found here. Acknowledges that Fortinet cooperated with the government's investigation and made available information](#)

on its own internal investigation. Fortinet has also implemented quality controls to mitigate the risk of any future violations of regulations applicable to public contracts. We can provide information on those controls should Equalis require additional information.

**Subcontractor Disclosure:** If/when awarded a contract in this program, Fortinet intends to add authorized resellers to the contract. As part of our request to add any company to our contract as an authorized reseller, we will provide a statement from that company addressing this mandatory contract disclosure. We understand that the information the company provides may affect Equalis's determination as to whether we will be allowed to add the company as an authorized reseller.

## PROPOSAL FORM 7: DEALER, RESELLER, AND DISTRIBUTOR AUTHORIZATION

CCOG allows Suppliers to authorize dealers, distributors, and resellers to sell the products and services made available through, and consistent with the Terms and Conditions set forth in, the Master Agreement. If Supplier intends to authorize their dealers, distributors, or resellers access to the Master Agreement in the event of a contract award Supplier must provide a list, either in the form of a document or a weblink, to identify those organizations who are being authorized access to the Master Agreement.

Will the Supplier authorize dealers, distributors, resellers access to Master Agreement?

- ☒ **Yes**
- ☐ **No**

If yes, how will Supplier disclose which organization(s) will have access to the Master Agreement? This list can be updated from time to time upon CCOG's approval.

Bidder Response: Fortinet's standard practice upon contract award, is to invite selected authorized resellers to be listed on the contract. Those resellers are given an Addendum to their Partner agreement for review/approval which identifies terms and conditions in our contract that flow down to them and, if applicable, any information they need to provide to allow the Contracting Officer to confirm that they are qualified to perform on the contract. We then provide a list of the companies to be added to the contract to the Contracting Officer, along with any supporting information, for review/approval. If we add new resellers over the life of the contract, we follow a similar process.

## PROPOSAL FORM 8: MANDATORY SUPPLIER & PROPOSAL CERTIFICATIONS

CCOG may not enter into contracts with any suppliers who have been found to be ineligible for state contracts under specific federal or Ohio statutes or regulations. Bidders responding to any CCOG RFP MUST certify that they are NOT ineligible by signing each of the statements below. **Failure to provide proper affirming signature on any of these statements will result in a Bidder's proposal being deemed nonresponsive to this RFP.**

I, **Insert name here.**, hereby certify and affirm that [Fortinet, Inc.](#), has not been debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in transactions by the United States Department of Labor, the United States Department of Health and Human Services, or any other federal department or agency as set forth in 29 CFR Part 98, or 45 CFR Part 76, or other applicable statutes.

### AND

I, **Insert name here.**, hereby certify and affirm that [Fortinet, Inc.](#), is in compliance with all federal, state, and local laws, rules, and regulations, including but not limited to the Occupational Safety and Health Act and the Ohio Bureau of Employment Services and the following:

- Not penalized or debarred from any public contracts or falsified certified payroll records or any other violation of the Fair Labor Standards Act in the last three (3) years;
- Not found to have violated any worker's compensation law within the last three (3) years;
- Not violated any employee discrimination law within the last three (3) years;
- Not have been found to have committed more than one (1) willful or repeated OSHA violation of a safety standard *(as opposed to a record keeping or administrative standard)* in the last three (3) years;
- Not have an Experience Modification Rating of greater than 1.5 (a penalty-rated employer) with respect to the Bureau of Workers' Compensation risk assessment rating; and
- Not have failed to file any required tax returns or failed to pay any required taxes to any governmental entity within the past three (3) years.

### AND

I, **Insert name here.**, hereby certify and affirm that [Fortinet, Inc.](#), is not on the list established by the Ohio Secretary of State, pursuant to **ORC Section 121.23**, which identifies persons and businesses with more than one unfair labor practice contempt of court finding against them.

### AND

I, **Insert name here.**, hereby certify and affirm that [Fortinet, Inc.](#) either is not subject to a finding for recovery under **ORC Section 9.24**, or has taken appropriate remedial steps required under that statute to resolve any findings for recovery, or otherwise qualifies under that section to enter into contracts with CCOG.

I, **Insert name here.**, hereby affirm that this proposal accurately represents the capabilities and qualifications of [Fortinet, Inc.](#) and I hereby affirm that the cost(s) proposed to CCOG for the performance of services and/or provision of goods covered in this proposal in response to this CCOG RFP is a firm fixed price structure as described in the Cost Proposal, inclusive of all incidental as well as primary costs. *(Failure to provide the proper affirming signature on this item may result in the disqualification of your proposal.)*



**PROPOSAL FORM 9: CLEAN AIR ACT & CLEAN WATER ACT**

The Bidder is in compliance with all applicable standards, orders or regulations issued pursuant to the Clean Air Act of 1970, as Amended (42 U.S. C. 1857 (h), Section 508 of the Clean Water Act, as amended (33 U.S.C. 1368), Executive Order 117389 and Environmental Protection Agency Regulation, 40 CFR Part 15 as required under OMB Circular A-102, Attachment O, Paragraph 14 (1) regarding reporting violations to the grantor agency and to the United States Environment Protection Agency Assistant Administrator for the Enforcement.

Authorized  
signature:

DocuSigned by:

*John Whittle*

2EBD4ABC62DE44D...

Printed Name:

John Whittle

Company Name:

[Fortinet, Inc.](#)

Mailing Address:

[889 Kifer Rd. Sunnyvale, CA 94086-5205](#)

Email Address:

[legal@fortinet.com](mailto:legal@fortinet.com)

Job Title:

EVP, General Counsel

DocuSigned by:



3/10/2022

## PROPOSAL FORM 10: DEBARMENT NOTICE

I, the Bidder, certify that my company has not been debarred, suspended or otherwise ineligible for participation in Federal Assistance programs under Executive Order 12549, "Debarment and Suspension", as described in the Federal Register and Rules and Regulations.

Respondents Name: John Whittle

Mailing Address: 889 Kifer Rd. Sunnyvale, CA 94086-5205

Signature

Title of Signatory: EVP, General Counsel

DocuSigned by:

*John Whittle*

2EBD4ABC02DE44B...

DocuSigned by:



3/10/2022

## PROPOSAL FORM 11: LOBBYING CERTIFICATIONS

Submission of this certification is a prerequisite for making or entering into this transaction and is imposed by **Section 1352, Title 31, U.S. Code**. This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Any person who fails to file the required certification shall be subject to civil penalty of not less than ten thousand dollars (\$10,000) and not more than one hundred thousand dollars (\$100,000) for each such failure.


The undersigned certifies, to the best of his/her knowledge and belief, on behalf of Bidder that:

1. No Federal appropriated funds have been paid or will be paid on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of a Federal contract, the making of a Federal grant, the making of a Federal loan, the entering into a cooperative agreement, and the extension, continuation, renewal, amendment, or modification of a Federal contract, grant, loan, or cooperative agreement.
2. If any funds other than Federal appropriated funds have been or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract or cooperative agreement, the undersigned shall complete and submit Standard Form LLL, "Disclosure of Lobbying Activities," in accordance with its instructions.
3. The undersigned shall require that the language of this certification be included in the award documents for all covered sub-awards exceeding one hundred thousand dollars (\$100,000) in Federal funds at all appropriate tiers and that all sub-recipients shall certify and disclose accordingly.

Signature: DocuSigned by:  
John Whittle  
 2EBD4ABC62DE44D...

Date: 03/10/2022

DocuSigned by:



3/10/2022

## PROPOSAL FORM 12: CONTRACTOR CERTIFICATION REQUIREMENTS

### 1. *Contractor's Employment Eligibility*

By entering the contract, Contractor warrants compliance with the Federal Immigration and Nationality Act (FINA), and all other federal and state immigration laws and regulations. The Contractor further warrants that it is in compliance with the various state statutes of the states it will operate this contract in.

Participating Government Entities including School Districts may request verification of compliance from any Contractor or subcontractor performing work under this Contract. These Entities reserve the right to confirm compliance in accordance with applicable laws.

Should the Participating Entities suspect or find that the Contractor or any of its subcontractors are not in compliance, they may pursue any and all remedies allowed by law, including, but not limited to: suspension of work, termination of the Contract for default, and suspension and/or debarment of the Contractor. All costs necessary to verify compliance are the responsibility of the Contractor.

The Respondent complies and maintains compliance with the appropriate statutes which requires compliance with federal immigration laws by State employers, State contractors and State subcontractors in accordance with the E-Verify Employee Eligibility Verification Program.

Contractor shall comply with governing board policy of the CCOG Participating entities in which work is being performed.

### 2. *Fingerprint & Criminal Background Checks*


If required to provide services on school district property at least five (5) times during a month, contractor shall submit a full set of fingerprints to the school district if requested of each person or employee who may provide such service. Alternately, the school district may fingerprint those persons or employees. An exception to this requirement may be made as authorized in Governing Board policy. The district shall conduct a fingerprint check in accordance with the appropriate state and federal laws of all contractors, subcontractors or vendors and their employees for which fingerprints are submitted to the district. Contractor, subcontractors, vendors, and their employees shall not provide services on school district properties until authorized by the District.

The Respondent shall comply with fingerprinting requirements in accordance with appropriate statutes in the state in which the work is being performed unless otherwise exempted.

Contractor shall comply with governing board policy in the school district or Participating Entity in which work is being performed.

Signature: DocuSigned by:  
John Whittle  
 2EBD4ABC82DE44D...  
 Date: 03/10/2022

DocuSigned by:



3/10/2022

## PROPOSAL FORM 13: BOYCOTT CERTIFICATION

Bidder must certify that during the term of any Agreement, it does not boycott Israel and will not boycott Israel. "Boycott" means refusing to deal with, terminating business activities with, or otherwise taking any action that is intended to penalize, inflict economic harm on, or limit commercial relations specifically with Israel, or with a person or entity doing business in Israel or in an Israeli-controlled territory, but does not include an action made for ordinary business purposes.

Does Bidder agree? Agree, JL  
(Initials of Authorized Representative)

## PROPOSAL FORM 14: FEDERAL FUNDS CERTIFICATION FORMS

When a participating agency seeks to procure goods and services using funds under a federal grant or contract, specific federal laws, regulations, and requirements may apply in addition to those under state law. This includes, but is not limited to, the procurement standards of the Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards, 2 CFR 200 (sometimes referred to as the “Uniform Guidance” or “EDGAR” requirements). All bidders submitting proposals must complete this Federal Funds Certification Form regarding bidder’s willingness and ability to comply with certain requirements which may be applicable to specific participating agency purchases using federal grant funds. This completed form will be made available to Members for their use while considering their purchasing options when using federal grant funds. Members may also require Supplier Partners to enter into ancillary agreements, in addition to the contract’s general terms and conditions, to address the member’s specific contractual needs, including contract requirements for a procurement using federal grants or contracts.

**For each of the items below, respondent should certify bidder’s agreement and ability to comply, where applicable, by having respondents authorized representative complete and initial the applicable lines after each section and sign the acknowledgment at the end of this form.** If a Bidder fails to complete any item in this form, CCOG will consider the respondent’s response to be that they are unable or unwilling to comply. A negative response to any of the items may, if applicable, impact the ability of a participating agency to purchase from the Supplier Partner using federal funds.

### 1. *Supplier Partner Violation or Breach of Contract Terms*

Contracts for more than the simplified acquisition threshold currently set at one hundred fifty thousand dollars (\$150,000), which is the inflation adjusted amount determined by the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (Councils) as authorized by 41 USC 1908, must address administrative, contractual, or legal remedies in instances where Supplier Partners violate or breach contract terms, and provide for such sanctions and penalties as appropriate.

Any contract award will be subject to Terms and Conditions of the Master Agreement, as well as any additional terms and conditions in any purchase order, participating agency ancillary contract, or Member construction contract agreed upon by Supplier Partner and the participating agency which must be consistent with and protect the participating agency at least to the same extent as the CCOG Terms and Conditions.

The remedies under the contract are in addition to any other remedies that may be available under law or in equity. By submitting a proposal, you agree to these Supplier Partner violation and breach of contract terms.

Does Bidder agree? Agree, JL

(Initials of Authorized Representative)

## **2. Termination for Cause or Convenience**

When a participating agency expends federal funds, the participating agency reserves the right to immediately terminate any agreement in excess of ten thousand dollars (\$10,000) resulting from this procurement process in the event of a breach or default of the agreement by Offeror in the event Offeror fails to: (1) meet schedules, deadlines, and/or delivery dates within the time specified in the procurement solicitation, contract, and/or a purchase order; (2) make any payments owed; or (3) otherwise perform in accordance with the contract and/or the procurement solicitation. Participating agency also reserves the right to terminate the contract immediately, with written notice to offeror, for convenience, if participating agency believes, in its sole discretion that it is in the best interest of participating agency to do so. Bidder will be compensated for work performed and accepted and goods accepted by participating agency as of the termination date if the contract is terminated for convenience of participating agency. Any award under this procurement process is not exclusive and participating agency reserves the right to purchase goods and services from other offerors when it is in participating agency's best interest.

Does Bidder agree? Agree, JL  
(Initials of Authorized Representative)

## **3. Equal Employment Opportunity**

Except as otherwise provided under 41 CFR Part 60, all participating agency purchases or contracts that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 shall be deemed to include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR Part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

The equal opportunity clause provided under 41 CFR 60-1.4(b) is hereby incorporated by reference. Supplier Partner agrees that such provision applies to any participating agency purchase or contract that meets the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 and Supplier Partner agrees that it shall comply with such provision.

Does Bidder agree? Agree, JL  
(Initials of Authorized Representative)

## **4. Davis-Bacon Act**

When required by Federal program legislation, Supplier Partner agrees that, for all participating agency prime construction contracts/purchases in excess of two thousand dollars (\$2,000), Supplier Partner shall comply with the Davis-Bacon Act (40 USC 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, Supplier Partner is required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor. In addition, Supplier Partner shall pay wages not less than once a week.

Current prevailing wage determinations issued by the Department of Labor are available at [www.wdol.gov](http://www.wdol.gov). Supplier Partner agrees that, for any purchase to which this requirement applies, the award of the purchase to the Supplier Partner is conditioned upon Supplier Partner's acceptance of the wage determination.

Supplier Partner further agrees that it shall also comply with the Copeland "Anti-Kickback" Act (40 USC 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States". The Act provides that each Supplier Partner or subrecipient must be prohibited from inducing, by any means, any

person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled.

Does Bidder agree? Not Applicable. Fortinet, Inc. does not provide construction services. JL  
(Initials of Authorized Representative)

## **5. Contract Work Hours and Safety Standards Act**

Where applicable, for all participating agency contracts or purchases in excess of one hundred thousand dollars (\$100,000) that involve the employment of mechanics or laborers, Supplier Partner agrees to comply with 40 USC 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 USC 3702 of the Act, Supplier Partner is required to compute the wages of every mechanic and laborer on the basis of a standard work week of forty (40) hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of forty (40) hours in the work week. The requirements of 40 USC 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous, or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

Does Bidder agree? Not Applicable. Fortinet, Inc. does not provide services performed by mechanics and laborers. JL  
(Initials of Authorized Representative)

## **6. Right to Inventions Made Under a Contract or Agreement**

If the participating agency's Federal award meets the definition of "funding agreement" under 37 CFR 401.2(a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance or experimental, developmental, or research work under that "funding agreement," the recipient or subrecipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

Supplier Partner agrees to comply with the above requirements when applicable.

Does Bidder agree? Not Applicable. Fortinet, Inc. does not intend to accept orders for experimental, developmental, or research work under our contract. Fortinet will supply commercial products and services through the contract. JL  
(Initials of Authorized Representative)

## **7. Clean Air Act and Federal Water Pollution Control Act**

Clean Air Act (42 USC 7401-7671q.) and the Federal Water Pollution Control Act (33 USC 1251-1387), as amended – Contracts and subgrants of amounts in excess of one hundred fifty thousand dollars (\$150,000) must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act (42 USC 7401-7671q.) and the Federal Water Pollution Control Act, as amended (33 USC 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).

When required, Supplier Partner agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act and the Federal Water Pollution Control Act.



Does Bidder agree? Agree, JL  
(Initials of Authorized Representative)

## **8. Debarment and Suspension**

Debarment and Suspension (Executive Orders 12549 and 12689) – A contract award (see 2 CFR 180.220) must not be made to parties listed on the government-wide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR Part 1966 Comp. p. 189) and 12689 (3CFR Part 1989 Comp. p. 235), “Debarment and Suspension.” SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.

Supplier Partner certifies that Supplier Partner is not currently listed on the government-wide exclusions in SAM, is not debarred, suspended, or otherwise excluded by agencies or declared ineligible under statutory or regulatory authority other than Executive Order 12549. Supplier Partner further agrees to immediately notify the Cooperative and all Members with pending purchases or seeking to purchase from Supplier Partner if Supplier Partner is later listed on the government-wide exclusions in SAM, or is debarred, suspended, or otherwise excluded by agencies or declared ineligible under statutory or regulatory authority other than Executive Order 12549.

Does Bidder agree? Agree, JL  
(Initials of Authorized Representative)

## **9. Byrd Anti-Lobbying Amendment**

Byrd Anti-Lobbying Amendment (31 USC 1352) – Supplier Partners that apply or bid for an award exceeding one hundred thousand dollars (\$100,000) must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 USC 1352. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award. As applicable, Supplier Partner agrees to file all certifications and disclosures required by, and otherwise comply with, the Byrd Anti-Lobbying Amendment (31 USC 1352).

Does Bidder agree? Agree, JL  
(Initials of Authorized Representative)

## **10. Procurement of Recovered Materials**

For participating agency purchases utilizing Federal funds, Supplier Partner agrees to comply with Section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act where applicable and provide such information and certifications as a participating agency maybe required to confirm estimates and otherwise comply. The requirements of Section 6002 includes procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds ten thousand dollars (\$10,000) or the value of the quantity acquired during the preceding fiscal year exceeded ten thousand dollars (\$10,000); procuring solid

waste management services in a manner that maximizes energy and resource recovery, and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

Does Bidder agree? Agree, JL  
(Initials of Authorized Representative)

### **11. Profit as a Separate Element of Price**

For purchases using federal funds in excess of one hundred fifty thousand dollars (\$150,000), a participating agency may be required to negotiate profit as a separate element of the price. See, 2 CFR 200.324(b). When required by a participating agency, Supplier Partner agrees to provide information and negotiate with the participating agency regarding profit as a separate element of the price for a particular purchase. However, Supplier Partner agrees that the total price, including profit, charged by Supplier Partner to the participating agency shall not exceed the awarded pricing, including any applicable discount, under Supplier Partner's Group Purchasing Agreement.

Does Bidder agree? Agree, JL  
(Initials of Authorized Representative)

### **12. Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment**

Vendor agrees that recipients and subrecipients are prohibited from obligating or expending loan or grant funds to procure or obtain, extend or renew a contract to procure or obtain, or enter into a contract (or extend or renew a contract) to procure or obtain equipment, services, or systems that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system from companies described in Public Law 115-232, section 889. Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country are also prohibited.

Does Bidder agree? Agree, JL  
(Initials of Authorized Representative)

### **13. Domestic preferences for procurements**

For participating agency purchases utilizing Federal funds, Bidder agrees to provide proof, where applicable, that the materials, including but not limited to, iron, aluminum, steel, cement, and other manufactured products are produced in the United States.

"Produced in the United States" means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States.

"Manufactured products" means items and construction materials composed in whole or in part of non-ferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber.

Does Bidder agree? Agree, JL  
(Initials of Authorized Representative)

#### 14. General Compliance and Cooperation with Members

In addition to the foregoing specific requirements, Vendor agrees, in accepting any purchase order from a Member, it shall make a good faith effort to work with Members to provide such information and to satisfy such requirements as may apply to a particular participating agency purchase or purchases including, but not limited to, applicable recordkeeping and record retention requirements.

Does Bidder agree? Agree, JL  
(Initials of Authorized Representative)

#### 15. Applicability to Subcontractors

Offeror agrees that all contracts it awards pursuant to the Contract shall be bound by the foregoing terms and conditions.

Does Bidder agree? Agree, JL  
(Initials of Authorized Representative)

By signature below, I certify that the information in this form is true, complete, and accurate and that I am authorized by my company to make this certification and all consents and agreements contained herein.

Authorized  
signature:

DocuSigned by:  
  
2EBD4ABC62DE44D...

Printed Name: John Whittle  
Company Name: Fortinet, Inc.  
Mailing Address: 889 Kifer Rd. Sunnyvale, CA 94086-5205  
Job Title: EVP, General Counsel

DocuSigned by:  
  
3/10/2022

## **PROPOSAL FORM 15: ARIZONA CONTRACTOR REQUIREMENTS**

### **AZ Compliance with Federal and State Requirements**

Contractor agrees when working on any federally assisted projects with more than \$2,000.00 in labor costs, to comply with all federal and state requirements, as well as Equal Opportunity Employment requirements and all other federal and state laws, statutes, etc. Contractor agrees to post wage rates at the work site and submit a copy of their payroll to the member for their files. Contractor must retain records for three years to allow the federal grantor agency access to these records, upon demand. Contractor also agrees to comply with the Arizona Executive Order 75-5, as amended by Executive Order 99-4.

When working on contracts funded with Federal Grant monies, contractor additionally agrees to comply with the administrative requirements for grants, and cooperative agreements to state, local and federally recognized Indian Tribal Governments.

### **AZ compliance with workforce requirements**

Pursuant to ARS 41-4401, Contractor and subcontractor(s) warrant their compliance with all federal and state immigration laws and regulations that relate to their employees, and compliance with ARS 23-214 subsection A, which states, "... every employer, after hiring an employee, shall verify the employment eligibility of the employee through the E-Verify program"

CCOG reserves the right to cancel or suspend the use of any contract for violations of immigration laws and regulations. CCOG and its members reserve the right to inspect the papers of any contractor or subcontract employee who works under this contract to ensure compliance with the warranty above.

### **AZ Contractor Employee Work Eligibility**

By entering into this contract, contractor agrees and warrants compliance with A.R.S. 41-4401, A.R.S. 23-214, the Federal Immigration and Nationality Act (FINA), and all other Federal immigration laws and regulations. CCOG and/or CCOG members may request verification of compliance from any contractor or sub-contractor performing work under this contract. CCOG and CCOG members reserve the right to confirm compliance. In the event that CCOG or CCOG members suspect or find that any contractor or subcontractor is not in compliance, CCOG may pursue any and all remedies allowed by law, including but not limited to suspension of work, termination of contract, suspension and/or debarment of the contractor. All cost associated with any legal action will be the responsibility of the contractor.

### **AZ Non-Compliance**

All federally assisted contracts to members that exceed \$10,000.00 may be terminated by the federal grantee for noncompliance by contractor. In projects that are not federally funded, Respondent must agree to meet any federal, state, or local requirements as necessary. In addition, if compliance with the federal regulations increases the contract costs beyond the agreed upon costs in this solicitation, the additional costs may only apply to the portion of the work paid by the federal grantee.

### **Registered Sex Offender Restrictions (Arizona)**

For work to be performed at an Arizona school, contractor agrees that no employee or employee of a subcontractor who has been adjudicated to be a registered sex offender will perform work at any time when students are present, or reasonably expected to be present. Contractor agrees that a violation of this condition shall be considered a material breach and may result in the cancellation of the purchase order at the CCOG member's discretion. Contractor must identify any additional costs associated with compliance to this term. If no costs are specified, compliance with this term will be provided at no additional charge.

### **Offshore Performance of Work Prohibited**

Due to security and identity protection concerns, direct services under this contract shall be performed within the borders of the United States.

**Terrorism Country Divestments:** In accordance with A.R.S. 35-392, CCOG and CCOG members are prohibited from purchasing from a company that is in violation of the Export Administration Act. By entering into the contract, contractor warrants compliance with the Export Administration Act.

The undersigned hereby accepts and agrees to comply with all statutory compliance and notice requirements listed in this document.

Does Bidder agree? Fortinet cannot agree to all Arizona Contractor Requirements at this time but will make every effort to add AZ to the list of states served by our contract after contract award. JL

(Initials of Authorized Representative)

Date: 03/10/2022

**PROPOSAL FORM 16: OWNERSHIP DISCLOSURE FORM (N.J.S. 52:25-24.2)**

Pursuant to the requirements of P.L. 1999, Chapter 440 effective April 17, 2000 (Local Public Contracts Law), the Respondent shall complete the form attached to these specifications listing the persons owning 10 percent (10%) or more of the firm presenting the proposal.

**Company Name:** Fortinet, Inc.  
**Street:** 889 Kifer Rd  
**City, State, Zip Code:** Sunnyvale, CA 94086-5205

**Complete as appropriate:**

I, Click or tap here to enter text., certify that I am the sole owner of Click or tap here to enter text., that there are no partners, and the business is not incorporated, and the provisions of N.J.S. 52:25-24.2 do not apply.

**OR:**

I, Click or tap here to enter text., a partner in Click or tap here to enter text., do hereby certify that the following is a list of all individual partners who own a 10% or greater interest therein. I further certify that if one (1) or more of the partners is itself a corporation or partnership, there is also set forth the names and addresses of the stockholders holding 10% or more of that corporation's stock or the individual partners owning 10% or greater interest in that partnership.

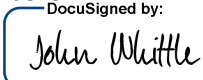
**OR:**

I, Click or tap here to enter text., an authorized representative of Fortinet, Inc., a corporation, do hereby certify that the following is a list of the names and addresses of all stockholders in the corporation who own 10% or more of its stock of any class. I further certify that if one (1) or more of such stockholders is itself a corporation or partnership, that there is also set forth the names and addresses of the stockholders holding 10% or more of the corporation's stock or the individual partners owning a 10% or greater interest in that partnership.

**(Note: If there are no partners or stockholders owning 10% or more interest, indicate none.)**

Name	Address	Interest
<u>none</u>		

I further certify that the statements and information contained herein, are complete and correct to the best of my knowledge and belief.

DocuSigned by:  
  
 Signature: 2EBD4ABC62DF44D  
 Date: 03/10/2022

DocuSigned by:



3/10/2022

## PROPOSAL FORM 17: NON-COLLUSION AFFIDAVIT

Bidder Name: Fortinet, Inc.

Street Address: 889 Kifer Rd.

City, State Zip: Sunnyvale, CA 94086-5205

State of New Jersey

County of Insert County name

I, Insert name here. of the Insert name of City in the County of Insert name of County, State of Insert name of State of full age, being duly sworn according to law on my oath depose and say that:

I am the Insert name of job title of the firm of Insert company name. the Bidder making the Proposal for the goods, services or public work specified under the Harrison Township Board of Education attached proposal, and that I executed the said proposal with full authority to do so; that said Respondent has not directly or indirectly entered into any agreement, participated in any collusion, or otherwise taken any action in restraint of free, competitive bidding in connection with the above proposal, and that all statements contained in said bid proposal and in this affidavit are true and correct, and made with full knowledge that the Harrison Township Board of Education relies upon the truth of the statements contained in said bid proposal and in the statements contained in this affidavit in awarding the contract for the said goods, services or public work.

I further warrant that no person or selling agency has been employed or retained to solicit or secure such contract upon an agreement or understanding for a commission, percentage, brokerage, or contingent fee, except bona fide employees or bona fide established commercial or selling agencies maintained by

Authorized  
signature:

Job Title: Insert job title here.

Subscribed and sworn before me

this \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_

\_\_\_\_\_  
Notary Public of New Jersey

My commission expires \_\_\_\_\_, 20\_\_\_\_

SEAL

**PROPOSAL FORM 18: AFFIRMATIVE ACTION AFFIDAVIT (P.L. 1975, C.127)**

Company Name: Fortinet, Inc.  
 Street Address: 889 Kifer Rd.  
 City, State, Zip Code: Sunnyvale, CA 94086-5205

**Bid Proposal Certification:**

Indicate below your compliance with New Jersey Affirmative Action regulations. Your proposal will be accepted even if you are not in compliance at this time. No contract and/or purchase order may be issued, however, until all Affirmative Action requirements are met.

**Required Affirmative Action Evidence:**

Procurement, Professional & Service Contracts (Exhibit A)

**Suppliers must submit with proposal:**

1. A photocopy of their Federal Letter of Affirmative Action Plan Approval  
OR
2. A photocopy of their Certificate of Employee Information Report  
OR
3. A complete Affirmative Action Employee Information Report (AA302)

**Public Work – Over \$50,000 Total Project Cost:**

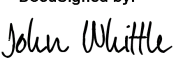
☐ No approved Federal or New Jersey Affirmative Action Plan. We will complete Report Form AA201-A upon receipt from the Harrison Township Board of Education

☐ Approved Federal or New Jersey Plan – certificate enclosed

*Unable to confirm status at time of proposal submission.*

I further certify that the statements and information contained herein, are complete and correct to the best of my knowledge and belief.

Authorized Signature:

DocuSigned by:  
  
 2EBD4ABC02DE44D...

Title of Signatory:

EVP, General Counsel

Date:

03/10/2022

**P.L. 1995, c. 127 (N.J.A.C. 17:27)**

**MANDATORY AFFIRMATIVE ACTION LANGUAGE**

**PROCUREMENT, PROFESSIONAL AND SERVICE CONTRACTS**

During the performance of this contract, the contractor agrees as follows:

DocuSigned by:



3/10/2022



The contractor or subcontractor, where applicable, will not discriminate against any employee or applicant for employment because of age, race, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation. The contractor will take affirmative action to ensure that such applicants are recruited and employed, and that employees are treated during employment, without regard to their age, race, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation. Such action shall include, but not be limited to the following: employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the Public Agency Compliance Officer setting forth provisions of this non-discrimination clause.

The contractor or subcontractor, where applicable will, in all solicitations or advertisement for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to age, race, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation.

The contractor or subcontractor, where applicable, will send to each labor union or representative of workers with which it has a collective bargaining agreement or other contract or understanding, a notice, to be provided by the agency contracting officer advising the labor union or workers' representative of the contractor's commitments under this act and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

The contractor or subcontractor, where applicable, agrees to comply with any regulations promulgated by the Treasurer pursuant to P.L. 1975, c. 127, as amended and supplemented from time to time and the Americans with Disabilities Act.

The contractor or subcontractor agrees to attempt in good faith to employ minority and female workers trade consistent with the applicable county employment goal prescribed by N.J.A.C. 17:27-5.2 promulgated by the Treasurer pursuant to P.L. 1975, C.127, as amended and supplemented from time to time or in accordance with a binding determination of the applicable county employment goals determined by the Affirmative

Action Office pursuant to N.J.A.C. 17:27-5.2 promulgated by the Treasurer pursuant to P.L. 1975, C.127, as amended and supplemented from time to time.

The contractor or subcontractor agrees to inform in writing appropriate recruitment agencies in the area, including employment agencies, placement bureaus, colleges, universities, labor unions, that it does not discriminate on the basis of age, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation, and that it will discontinue the use of any recruitment agency which engages in direct or indirect discriminatory practices.

The contractor or subcontractor agrees to revise any of its testing procedures, if necessary, to assure that all personnel testing conforms with the principles of job-related testing, as established by the statutes and court decisions of the state of New Jersey and as established by applicable Federal law and applicable Federal court decisions.

The contractor or subcontractor agrees to review all procedures relating to transfer, upgrading, downgrading and lay-off to ensure that all such actions are taken without regard to age, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation, and conform with the applicable employment goals, consistent with the statutes and court decisions of the State of New Jersey, and applicable Federal law and applicable Federal court decisions.

The contractor and its subcontractors shall furnish such reports or other documents to the Affirmative Action Office as may be requested by the office from time to time in order to carry out the purposes of these regulations, and public agencies shall furnish such information as may be requested by the Affirmative Action Office for conducting a compliance investigation pursuant to Subchapter 10 of the Administrative Code (NJAC 17:27).

---

Signature of Procurement Agent



## PROPOSAL FORM 19: C. 271 POLITICAL CONTRIBUTION DISCLOSURE FROM

### Public Agency Instructions

This page provides guidance to public agencies entering into contracts with business entities that are required to file Political Contribution Disclosure forms with the agency. **It is not intended to be provided to contractors.** What follows are instructions on the use of form local units can provide to contractors that are required to disclose political contributions pursuant to N.J.S.A. 19:44A-20.26 (P.L. 2005, c. 271, s.2). Additional information is available in Local Finance Notice 2006-1 ([https://www.nj.gov/dca/divisions/dlgs/resources/lfns\\_2006.html](https://www.nj.gov/dca/divisions/dlgs/resources/lfns_2006.html)).

1. The disclosure is required for all contracts in excess of \$17,500 that are **not awarded** pursuant to a “fair and open” process (N.J.S.A. 19:44A-20.7).
2. Due to the potential length of some contractor submissions, the public agency should consider allowing data to be submitted in electronic form (i.e., spreadsheet, pdf file, etc.). Submissions must be kept with the contract documents or in an appropriate computer file and be available for public access. **The form is worded to accept this alternate submission.** The text should be amended if electronic submission will not be allowed.
3. The submission must be **received from the contractor and** on file at least 10 days prior to award of the contract. Resolutions of award should reflect that the disclosure has been received and is on file.
4. The contractor must disclose contributions made to candidate and party committees covering a wide range of public agencies, including all public agencies that have elected officials in the county of the public agency, state legislative positions, and various state entities. The Division of Local Government Services recommends that contractors be provided a list of the affected agencies. This will assist contractors in determining the campaign and political committees of the officials and candidates affected by the disclosure.
  - a) The Division has prepared model disclosure forms for each county. They can be downloaded from the “County PCD Forms” link on the Pay-to-Play web site at [https://www.state.nj.us/dca/divisions/dlgs/programs/pay\\_2\\_play.html](https://www.state.nj.us/dca/divisions/dlgs/programs/pay_2_play.html). They will be updated from time-to-time as necessary.
  - b) A public agency using these forms **should edit them to properly reflect the correct legislative district(s)**. As the forms are county-based, **they list all legislative districts** in each county. **Districts that do not represent the public agency should be removed from the lists.**
  - c) Some contractors may find it easier to provide a single list that covers all contributions, regardless of the county. These submissions are appropriate and should be accepted.
  - d) The form may be used “as-is”, subject to edits as described herein.
  - e) The “Contractor Instructions” sheet is intended to be provided with the form. It is recommended that the Instructions and the form be printed on the same piece of paper. The form notes that the Instructions are printed on the back of the form; where that is not the case, the text should be edited accordingly.
  - f) The form is a Word document and can be edited to meet local needs, and posted for download on web sites, used as an e-mail attachment, or provided as a printed document.
5. It is recommended that the contractor also complete a “Stockholder Disclosure Certification.” This will assist the local unit in its obligation to ensure that contractor did not make any prohibited contributions to the committees listed on the Business Entity Disclosure Certification in the 12 months prior to the contract. (See Local Finance Notice 2006-7 for additional information on this obligation) A sample Certification form is part of this package and the instruction to complete it is included in the Contractor Instructions. **NOTE: This section is not applicable to Boards of Education.**

**C. 271 POLITICAL CONTRIBUTION DISCLOSURE FORM****Contractor Instructions**

Business entities (contractors) receiving contracts from a public agency that are NOT awarded pursuant to a “fair and open” process (defined at N.J.S.A. 19:44A-20.7) are subject to the provisions of P.L. 2005, c. 271, s.2 (N.J.S.A. 19:44A-20.26). This law provides that 10 days prior to the award of such a contract, the contractor shall disclose contributions to:

- any State, county, or municipal committee of a political party
- any legislative leadership committee\*
- any continuing political committee (a.k.a., political action committee)
- any candidate committee of a candidate for, or holder of, an elective office:
  - of the public entity awarding the contract
  - of that county in which that public entity is located
  - of another public entity within that county
  - or of a legislative district in which that public entity is located or, when the public entity is a county, of any legislative district which includes all or part of the county. The disclosure must list reportable contributions to any of the committees that exceed \$300 per election cycle that were made during the 12 months prior to award of the contract. See N.J.S.A. 19:44A-8 and 19:44A-16 for more details on reportable contributions.

N.J.S.A. 19:44A-20.26 itemizes the parties from whom contributions must be disclosed when a business entity is not a natural person. This includes the following:

- individuals with an “interest” ownership or control of more than 10% of the profits or assets of a business entity or 10% of the stock in the case of a business entity that is a corporation for profit
- all principals, partners, officers, or directors of the business entity or their spouses
- any subsidiaries directly or indirectly controlled by the business entity
- IRS Code Section 527 New Jersey based organizations, directly or indirectly controlled by the business entity, and filing as continuing political committees, (PACs). When the business entity is a natural person, “a contribution by that person’s spouse or child, residing therewith, shall be deemed to be a contribution by the business entity.” [N.J.S.A. 19:44A-20.26(b)] The contributor must be listed on the disclosure. Any business entity that fails to comply with the disclosure provisions shall be subject to a fine imposed by ELEC in an amount to be determined by the Commission which may be based upon the amount that the business entity failed to report. The enclosed list of agencies is provided to assist the contractor in identifying those public agencies whose elected official and/or candidate campaign committees are affected by the disclosure requirement. It is the contractor’s responsibility to identify the specific committees to which contributions may have been made and need to be disclosed. The disclosed information may exceed the minimum requirement. The enclosed form, a content-consistent facsimile, or an electronic data file containing the required details (along with a signed cover sheet) may be used as the contractor’s submission and is disclosable to the public under the Open Public Records Act. The contractor must also complete the attached Stockholder Disclosure Certification. This will assist the agency in meeting its obligations under the law.

**NOTE: This section does not apply to Board of Education contracts.**

\* N.J.S.A. 19:44A-3(s): “The term “legislative leadership committee” means a committee established, authorized to be established, or designated by the President of the Senate, the Minority Leader of the Senate, the Speaker of the General Assembly or the Minority Leader of the General Assembly pursuant to section 16 of P.L.1993, c.65 (C.19:44A-10.1) for the purpose of receiving contributions and making expenditures.”

**C. 271 POLITICAL CONTRIBUTION DISCLOSURE FORM**

Required Pursuant To N.J.S.A. 19:44A-20.26

This form or its permitted facsimile must be submitted to the local unit no later than 10 days prior to the award of the contract.

### Part I – Vendor Information

Vendor Name:	Fortinet, Inc.		
Address:	889 Kifer Rd.		
City:	Sunnyvale	State:CA	Zip:94086-5205

The undersigned being authorized to certify, hereby certifies that the submission provided herein represents compliance with the provisions of N.J.S.A. 19:44A-20.26 and as represented by the Instructions accompanying this form.

DocuSigned by:

*John Whittle*

2EBD4ABC62DF44D

John Whittle

EVP, General Counsel

Signature of Vendor

Printed Name

Title



3/10/2022

### Part II – Contribution Disclosure

Disclosure requirement: Pursuant to N.J.S.A. 19:44A-20.26 this disclosure must include all reportable political contributions (more than \$300 per election cycle) over the 12 months prior to submission to the committees of the government entities listed on the form provided by the local unit.

☐ Check here if disclosure is provided in electronic form.

Contributor Name	Recipient Name	Date	Dollar Amount
None			\$

☐ Check here if the information is continued on subsequent page(s)



**List of Agencies with Elected Officials Required for Political Contribution Disclosure**

**N.J.S.A. 19:44A-20.26**

**County Name:**

State: Governor, and Legislative Leadership Committees

Legislative District #s:

State Senator and two members of the General Assembly per district.

County:

Freeholders

County Clerk

Sheriff

{County Executive}

Surrogate

Municipalities (Mayor and members of governing body, regardless of title):

**USERS SHOULD CREATE THEIR OWN FORM, OR DOWNLOAD FROM [WWW.NJ.GOV/DCA/LGS/P2P](http://WWW.NJ.GOV/DCA/LGS/P2P) A COUNTY-BASED, CUSTOMIZABLE FORM.**

## PROPOSAL FORM 20: STOCKHOLDER DISCLOSURE CERTIFICATION

### Name of Business:

☐ I certify that the list below contains the names and home addresses of all stockholders holding 10% or more of the issued and outstanding stock of the undersigned.

OR

☒ I certify that no one stockholder owns 10% or more of the issued and outstanding stock of the undersigned.

### Check the box that represents the type of business organization:

- ☐ Partnership
- ☒ Corporation
- ☐ Sole Proprietorship
- ☐ Limited Partnership
- ☐ Limited Liability Corporation
- ☐ Limited Liability Partnership
- ☐ Subchapter S Corporation

Sign and notarize the form below, and, if necessary, complete the stockholder list below.

### Stockholders:

Name: Stockholder Name	Name: Stockholder Name
Home Address: Home Address	Home Address: Home Address
Name: Stockholder Name	Name: Stockholder Name
Home Address: Home Address	Home Address: Home Address
Name: Stockholder Name	Name: Stockholder Name
Home Address: Home Address	Home Address: Home Address
Subscribed and sworn before me this ____ day of _____, 2__.	<div> <div>DocuSigned by:</div> <div>John Whittle</div> <div>2EBD4ABC62DE44D...</div> </div> <div>(Affiant)</div> <div>John Whittle, EVP, General Counsel</div> <div>(Print name &amp; title of affiant)</div>
(Notary Public)	

DocuSigned



3/10/2022



My Commission expires:

(Corporate Seal)

## PROPOSAL FORM 21: GENERAL TERMS AND CONDITIONS ACCEPTANCE FORM

**Check one of the following responses to the General Terms and Conditions in this solicitation, including the Master Agreement:**

☐ We take no exceptions/deviations to the general terms and conditions  
(Note: If none are listed below, it is understood that no exceptions/deviations are taken.)

☒ We take the following exceptions/deviations to the general terms and conditions. All exceptions/deviations must be clearly explained. Reference the corresponding general terms and conditions that you are taking exceptions/deviations to. Clearly state if you are adding additions terms and conditions to the general terms and conditions. Provide details on your exceptions/deviations below:

Section	Original Language	Proposed Language
2.7 Indemnification	Winning Supplier shall protect, indemnify, and hold harmless both CCOG and Equalis Group and its Members, administrators, employees and agents against all claims, damages, losses and expenses arising out of or resulting from the actions of Winning Supplier, Winning Supplier employees or subcontractors in the preparation of the solicitation and the later execution of the contract, including any supplemental agreements with Members.	Either party shall protect, indemnify, and hold harmless the other party and its employees, agents, subcontractors, in case of CCOG, both CCOG and Equalis Group and its Members, administrators, employees and agents against all claims, damages, losses and expenses arising out of or resulting directly from the actual infringement of patent, trademark, trade secret, and copyright rights of any third party by the other party and its employees or subcontractors under this Agreement, as determined by final judgement.
2.10 Termination Rights	<p>The Parties shall have the termination rights set forth below.</p> <p><b>a. Insolvency.</b> If a petition in bankruptcy is filed by any Party, or if any Party is adjudicated as bankrupt, or if any Party makes a general assignment for the benefit of creditors, or if a receiver is appointed on account of the insolvency of any Party, then the other Parties, without prejudice to any other right or remedy, may terminate this Master Agreement upon giving at least five (5) business days prior written Notice of such termination.</p> <p><b>b. Mutual Consent.</b> This Master Agreement, or any Appendix, may be terminated at any time by the mutual written consent of the Parties.</p>	<p>The Parties shall have the termination rights set forth below.</p> <p><b>a. Insolvency.</b> If a petition in bankruptcy is filed by any Party, or if any Party is adjudicated as bankrupt, or if any Party makes a general assignment for the benefit of creditors, or if a receiver is appointed on account of the insolvency of any Party, then the other Parties, without prejudice to any other right or remedy, may terminate this Master Agreement upon giving at least five (5) business days prior written Notice of such termination.</p> <p><b>b. Mutual Consent.</b> This Master Agreement, or any Appendix, may be terminated at any time by the mutual written consent of the Parties.</p>

	<p><b>c. Breach.</b> In the event that any Party commits a material breach of its obligations under this Master Agreement, except for a payment obligation, the non-breaching Party(ies) may provide written Notice describing the material breach to the breaching Party. The breaching Party will have thirty (30) calendar days to cure such breach or provide acceptable reassurance to the non-breaching Party(ies), or, if the Parties agree that a cure or reassurance is not feasible within thirty calendar (30) days, such period of time for cure or satisfactory reassurance as the Parties may agree in writing. If the breach is not cured within such period or if satisfactory reassurance is not accepted by the non-breaching Party(ies) in such period, then the Party(ies) not in breach may terminate this Master Agreement upon ten (10) business days written Notice at the Addresses for Notices set forth in Appendix A.</p>	<p><b>c. Termination for Convenience.</b> Either partner may, without cause or for convenience, terminate this agreement upon written notice of 30 days to the other party.</p> <p><b>d. Breach.</b> In the event that any Party commits a material breach of its obligations under this Master Agreement, except for a payment obligation, the non-breaching Party(ies) may provide written Notice describing the material breach to the breaching Party. The breaching Party will have thirty (30) calendar days to cure such breach or provide acceptable reassurance to the non-breaching Party(ies), or, if the Parties agree that a cure or reassurance is not feasible within thirty calendar (30) days, such period of time for cure or satisfactory reassurance as the Parties may agree in writing. If the breach is not cured within such period or if satisfactory reassurance is not accepted by the non-breaching Party(ies) in such period, then the Party(ies) not in breach may terminate this Master Agreement upon ten (10) business days written Notice at the Addresses for Notices set forth in Appendix A.</p>
2.12 Audit of Winning Supplier	<p>CCOG and Equalis, whether directly or through an independent auditor or accounting firm, shall have the right to perform audits, including inspection of books, records, and computer data relevant to Winning Supplier's provision of Products &amp; Services to Program Participants pursuant to this Master Agreement, to ensure that pricing, inventory, quality, process, and business controls are maintained; provided, however, that such inspections and audits will be conducted upon reasonable notice to Winning Supplier and so as not to unreasonably interfere with Winning Supplier's business or operations.</p>	<p>CCOG and Equalis, whether directly or through an independent auditor or accounting firm, shall have the right to perform audits, including inspection of books, records, and computer data relevant to Winning Supplier's provision of Products &amp; Services to Program Participants pursuant to this Master Agreement are maintained; provided, however, that such inspections and audits will be conducted upon reasonable notice to Winning Supplier and so as not to unreasonably interfere with Winning Supplier's business or operations.</p>

<p>2.16 Governing Law; Invalidity</p>	<p>This Master Agreement shall be construed and enforced in accordance with, and governed by, the laws of the State of Ohio without regard to rules of conflict of laws. If any provision of this Master Agreement is declared unlawful or unenforceable by judicial determination or performance, then the remainder of this Master Agreement shall continue in force as if the invalidated provision did not exist. Any suits filed by any Party pursuant to this Master Agreement shall be brought in a court of competent jurisdiction located in Cuyahoga County, Ohio. In the event any Party initiates a suit and that suit is adjudicated by a court of competent jurisdiction, the prevailing Party shall be entitled to reasonable attorney's fees and costs from the non-prevailing Party in addition to any other relief to which the court determines the prevailing Party is entitled or awarded.</p>	<p>This Master Agreement shall be construed and enforced in accordance with, and governed by, the laws of the State of Ohio without regard to rules of conflict of laws. If any provision of this Master Agreement is declared unlawful or unenforceable by judicial determination or performance, then the remainder of this Master Agreement shall continue in force as if the invalidated provision did not exist. Any suits filed by any Party pursuant to this Master Agreement shall be brought in a court of competent jurisdiction located in Cuyahoga County, Ohio.</p>
---------------------------------------	---	--

*(Note: Unacceptable exceptions shall remove your proposal from consideration for award. CCOG shall be the sole judge on the acceptance of exceptions/deviations and the decision shall be final.)*

## PROPOSAL FORM 22: EQUALIS GROUP ADMINISTRATION AGREEMENT DECLARATION

**Attachment A - Sample Administration Agreement of this solicitation is for reference only. Contracting with Equalis Group and the Winning Supplier will occur after contract award.**

Execution of the Administration Agreement is required for the Master Agreement to be administered by Equalis Group. **Attachment A - Sample Administration Agreement** defines i) the roles and responsibilities of both parties relating to marketing and selling the Program to current and prospective Members, and ii) the financial terms between Equalis Group and Winning Supplier.

Redlined copies of this agreement should not be submitted with the response. Should a respondent be recommended for award, this agreement will be negotiated and executed between Equalis Group and the respondent. Respondents must select one of the following options for submitting their response.

- ☐ Bidder agrees to all terms and conditions outlined in the **Attachment A - Sample Administration Agreement.**
- ☒ Bidder wishes to negotiate directly with Equalis Group on terms and conditions outlined in the Sample Administration Agreement. Negotiations will commence after CCOG has completed contract award.

## PROPOSAL FORM 23: MASTER AGREEMENT SIGNATURE FORM

The undersigned hereby proposes and agrees to furnish goods and services in strict compliance with the terms, specifications, and conditions contained within this RFP and the Master Agreement at the prices proposed within the submitted proposal unless noted in writing. The undersigned further certifies that he/she is an officer of the company and has authority to negotiate and bind the company named below and has not prepared this proposal in collusion with any other Respondent and that the contents of this proposal as to prices, terms or conditions of said proposal have not been communicated by the undersigned nor by any employee or agent to any person engaged in this type of business prior to the official opening of this proposal.

### **BIDDERS MUST SUBMIT THIS FORM COMPLETED AND SIGNED WITH THEIR RESPONSE TO BE CONSIDERED FOR AWARD.**

**Company Name** Fortinet, Inc.  
**Address** 889 Kifer Rd  
**City/State/Zip** Sunnyvale, CA 94086-5205  
**Phone Number** Phone Number  
**Email Address** legal@fortinet.com  
**Printed Name** John Whittle  
**Job Title** EVP, General Counsel

**Authorized  
Signature**

DocuSigned by:

*John Whittle*

2EBD4ABC62DE44D...

DocuSigned by:



3/10/2022

### **Initial Term of the Master Agreement**

**Contract Effective Date:** May 1, 2022  
**Contract Expiration Date:** April 30, 2026  
**Contract Number:** [REDACTED]

*(Note: Contract Number will be applied prior to CCOG and Equalis Group countersigning.)*

### **THE COOPERATIVE COUNCIL OF GOVERNMENTS, INC.**

6001 Cochran Road, Suite 333  
Cleveland, Ohio 44139

**By:** \_\_\_\_\_  
**Name:** Scott A. Morgan  
**As:** CCOG Board President  
**Date:** \_\_\_\_\_

### **EQUALIS GROUP, LLC.**

5550 Granite Parkway, Suite 298  
Plano, Texas 75024

**By:** \_\_\_\_\_  
**Name:** Eric Merkle  
**As:** SVP, Procurement & Operations  
**Date:** \_\_\_\_\_

**Certificate Of Completion**

Envelope Id: CA6A827DA96E48CA822C69395DE34914

Status: Completed

Subject: Please DocuSign: Equalis RFP deadline March 10th

Source Envelope:

Document Pages: 38

Signatures: 10

Envelope Originator:

Certificate Pages: 5

Initials: 0

Beth Gao

AutoNav: Enabled

Stamps: 10

899 Kifer road

Envelopeld Stamping: Enabled

Sunnyvale, CA 94086

Time Zone: (UTC-08:00) Pacific Time (US &amp; Canada)

bgao@fortinet.com

IP Address: 98.234.36.247

**Record Tracking**

Status: Original

Holder: Beth Gao

Location: DocuSign

3/10/2022 7:35:39 AM

bgao@fortinet.com

**Signer Events****Signature****Timestamp**

Jing Li

**Signed**

Sent: 3/10/2022 7:42:13 AM

jili@fortinet.com

Resent: 3/10/2022 8:08:17 AM

Senior Legal Counsel

Resent: 3/10/2022 8:14:15 AM

Fortinet, Inc.

Viewed: 3/10/2022 8:15:45 AM

Security Level: Email, Account Authentication (None)

Signed: 3/10/2022 8:16:26 AM

Using IP Address: 98.47.167.227

**Electronic Record and Signature Disclosure:**

Accepted: 3/10/2022 7:57:06 AM

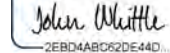
ID: f8e5906c-bbc5-4f69-92fd-a8ad5575c470

John Whittle

DocuSigned by:

Sent: 3/10/2022 8:16:41 AM

jwhittle@fortinet.com

2EBD4AB062DE44D...

Viewed: 3/10/2022 10:13:53 AM

EVP, General Counsel

Signed: 3/10/2022 10:14:16 AM

Fortinet, Inc.

Signature Adoption: Pre-selected Style

Security Level: Email, Account Authentication (None)

Using IP Address: 98.42.91.143

**Electronic Record and Signature Disclosure:**

Accepted: 3/10/2022 10:13:53 AM

ID: 6833548b-2eca-451b-b5b6-886682f78f69

**In Person Signer Events****Signature****Timestamp****Editor Delivery Events****Status****Timestamp****Agent Delivery Events****Status****Timestamp****Intermediary Delivery Events****Status****Timestamp****Certified Delivery Events****Status****Timestamp****Carbon Copy Events****Status****Timestamp****Witness Events****Signature****Timestamp****Notary Events****Signature****Timestamp****Envelope Summary Events****Status****Timestamps**

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	3/10/2022 7:42:13 AM
Certified Delivered	Security Checked	3/10/2022 10:13:53 AM
Signing Complete	Security Checked	3/10/2022 10:14:16 AM
Completed	Security Checked	3/10/2022 10:14:16 AM
Payment Events	Status	Timestamps
Electronic Record and Signature Disclosure		



## **CONSUMER DISCLOSURE**

From time to time, Fortinet, Inc (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign, Inc. (DocuSign) electronic signing system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to these terms and conditions, please confirm your agreement by clicking the 'I agree' button at the bottom of this document.

### **Getting paper copies**

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after signing session and, if you elect to create a DocuSign signer account, you may access them for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

### **Withdrawing your consent**

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

### **Consequences of changing your mind**

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. To indicate to us that you are changing your mind, you must withdraw your consent using the DocuSign 'Withdraw Consent' form on the signing page of a DocuSign envelope instead of signing it. This will indicate to us that you have withdrawn your consent to receive required notices and disclosures electronically from us and you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

### **All notices and disclosures will be sent to you electronically**

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

## **How to contact Fortinet, Inc:**

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: [rbrenner@fortinet.com](mailto:rbrenner@fortinet.com)

## **To advise Fortinet, Inc of your new e-mail address**

To let us know of a change in your e-mail address where we should send notices and disclosures electronically to you, you must send an email message to us at [rbrenner@fortinet.com](mailto:rbrenner@fortinet.com) and in the body of such request you must state: your previous e-mail address, your new e-mail address. We do not require any other information from you to change your email address..

In addition, you must notify DocuSign, Inc. to arrange for your new email address to be reflected in your DocuSign account by following the process for changing e-mail in the DocuSign system.

## **To request paper copies from Fortinet, Inc**

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an e-mail to [rbrenner@fortinet.com](mailto:rbrenner@fortinet.com) and in the body of such request you must state your e-mail address, full name, US Postal address, and telephone number. We will bill you for any fees at that time, if any.

## **To withdraw your consent with Fortinet, Inc**

To inform us that you no longer want to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your DocuSign session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an e-mail to [rbrenner@fortinet.com](mailto:rbrenner@fortinet.com) and in the body of such request you must state your e-mail, full name, US Postal Address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

## **Required hardware and software**

Operating Systems:	Windows® 2000, Windows® XP, Windows Vista®; Mac OS® X
Browsers:	Final release versions of Internet Explorer® 6.0 or above (Windows only); Mozilla Firefox 2.0 or above (Windows and Mac); Safari™ 3.0 or above (Mac only)
PDF Reader:	Acrobat® or similar software may be required to view and print PDF files
Screen Resolution:	800 x 600 minimum

Enabled Security Settings:	Allow per session cookies
----------------------------	---------------------------

\*\* These minimum requirements are subject to change. If these requirements change, you will be asked to re-accept the disclosure. Pre-release (e.g. beta) versions of operating systems and browsers are not supported.

**Acknowledging your access and consent to receive materials electronically**

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please verify that you were able to read this electronic disclosure and that you also were able to print on paper or electronically save this page for your future reference and access or that you were able to e-mail this disclosure and consent to an address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format on the terms and conditions described above, please let us know by clicking the 'I agree' button below.

By checking the 'I agree' box, I confirm that:

- I can access and read this Electronic CONSENT TO ELECTRONIC RECEIPT OF ELECTRONIC CONSUMER DISCLOSURES document; and
- I can print on paper the disclosure or save or send the disclosure to a place where I can print it, for future reference and access; and
- Until or unless I notify Fortinet, Inc as described above, I consent to receive from exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to me by Fortinet, Inc during the course of my relationship with you.

# **Attachments Referenced In Form 1**

**Attachment A**  
**Equalis Group Sample**  
**Administration Agreement**

## Attachment A – Equalis Group Sample Administration Agreement

THIS ADMINISTRATION AGREEMENT (this "**Agreement**"), effective as of **Month Day, Year** (the "**Effective Date**"), is entered into by and between **Winning Supplier**, a **State** corporation with its principal place of business at **street address, City, State Zip** ("**Winning Supplier**") and Equalis Group LLC, a Delaware limited liability company with its principal place of business at 5550 Granite Parkway, Suite 298, Plano, Texas 75024 ("**Equalis**"). Throughout this Agreement, Winning Supplier and Equalis are referred to interchangeably as in the singular "**Party**" or in the plural "**Parties**."

### SECTION 1. RECITALS

- A.** The Cooperative Council of Governments, Inc. ("**CCOG**") serves as a lead public agency (a "**Lead Public Agency**") for Equalis Group ("**Equalis Group**"), a national cooperative purchasing organization, by publicly procuring master cooperative purchasing agreements for products and services to be made available to Equalis Group members ("**Equalis Group Member**" or "**Member**").
- B.** CCOG issued request for proposal ("**RFP**") #**Number** dated **Month Day, Year** for contracting on behalf of Equalis Group Members for **definition of products and services solicited in the RFP** ("**Products & Services**") and awarded a contract to Winning Supplier.
- C.** CCOG, Equalis, and Winning Supplier entered into that certain master cooperative purchasing agreement (the "**Master Agreement**") #**contract number** effective as of **Month Day, Year** to provide Products & Services to Equalis Group Members.
- D.** Equalis serves as the Contract Administrator of the Master Agreement on behalf of CCOG.
- E.** Equalis actively promotes Master Agreements to current and prospective Equalis Group Members (collectively "**Prospective Participants**") through a range of marketing, prospecting, and sales strategies, including, but not limited to, marketing and sales collateral development, direct mail, web marketing, electronic communications, attendance at events, Winning Supplier sales representative training, and Winning Supplier field sales support (collectively, "**Equalis Services**") as more fully defined in **Appendix B**.
- F.** Any Prospective Participant who purchases Products & Services from Winning Supplier subject to the Master Agreement shall be considered a "**Program Participant**".
- G.** Winning Supplier desires to promote and expand its operations and increase the sales of its Products & Services to public sector, private sector, and non-profit organizations through Equalis Group.

NOW, THEREFORE, in consideration of the mutual promises contained herein, the Parties agree to the following terms and conditions:

## SECTION 2. BUSINESS TERMS

2.1. **Defined Terms.** Any capitalized terms contained herein not defined in this Agreement shall have the same meaning as defined in the Master Agreement.

2.2. **Appendices.** Winning Supplier agrees to provide Products & Services to Program Participants as may be agreed to by the Parties in accordance with the specific terms and conditions set forth in the Master Agreement, this Agreement, and the appendices attached hereto and made a part of this Agreement (if one, an “Appendix” or more, “Appendices”).

- (i) **Appendix A** defines Winning Supplier’s reporting requirements.
- (ii) **Appendix B** sets forth the roles and responsibilities of the Parties.
- (iii) **Appendix C** defines the financial terms between the Parties.

2.3. **Terms in Appendices.** In all cases where the terms of this Agreement and any Appendices disagree, the terms in the Appendix shall control.

2.4. **Publicity & Joint Marketing.**

(a) **Publicity.** A Party may only issue press releases or other public announcements with respect to this Agreement with the prior, written consent of the other Party.

(b) **Joint Marketing / Logo & Name Use.** Winning Supplier authorizes Equalis to use Winning Supplier’s trademarks, names, and logos as provided by Winning Supplier to Equalis. Equalis authorizes Winning Supplier to use Equalis’ trademarks, names, and logos as provided by Equalis to Winning Supplier. Each Party’s use of the other Party’s trademarks, names, and logos will be limited to standard communication, including correspondence, newsletters, and website material, and joint marketing efforts, including, but not limited to, utilizing the same on correspondence, collateral, agreements, websites, newsletters, or other marketing materials promoting the Products & Services pursuant to the Master Agreement and this Agreement. Notwithstanding the foregoing, the Parties understand and agree that except as provided herein, neither Party shall have any right, title, or interest in the other Party’s trademarks, names, and logos. Upon termination of this Agreement, each Party shall immediately cease use of the other Party’s trademarks, names, and logos.

## SECTION 3. TERMS & CONDITIONS

3.1. **Express Limitation of Equalis Liability.** With respect to any purchases of Products & Services by CCOG or any Program Participant pursuant to the Master Agreement, Equalis shall not be: (i) construed as a dealer, re-marketer, representative, partner, or agent of any type of the Winning Supplier, CCOG, or any Program Participant; (ii) obligated by, liable for, or in any way responsible for any order of Products & Services made by CCOG or any Program Participant or any employee thereof under the Master Agreement or for any payment required to be made with respect to such order for Products & Services; and (iii) obligated by, liable for, or in any way responsible for any failure by CCOG or any Program Participant to comply with procedures or requirements of applicable law or the Master Agreement or to obtain the due authorization and approval necessary to purchase Products & Services under the Master Agreement. Equalis makes no representation or guaranty with respect to any minimum purchases by CCOG or any Program Participant, whether individually

or collectively, or any employee thereof under this Agreement or the Master Agreement. The terms of this section shall survive the termination of this Agreement.

3.2. **Term & Termination.** The Term of this Agreement is the same as the Term of the Master Agreement. This Agreement shall only be terminated, and shall be terminated, if and when the Master Agreement is terminated. Upon termination of the Master Agreement for any reason, Winning Supplier shall continue making Administrative Fee and other payments, as set forth in **Appendix C**, to Equalis that are generated by individual Program Participant's purchase of Products & Services for a period of either i) one (1) year from the date of termination, or ii) through the then current expiration date of the Master Agreement, whichever is shorter, to the extent that Winning Supplier continues to generate revenue from each Program Participant's purchase of Products & Services following the termination of the Master Agreement.

3.3. **Audit of Winning Supplier.** Equalis, whether directly or through an independent auditor or accounting firm, shall have the right to perform audits, including inspection of books, records, and computer data relevant to Winning Supplier's provision of Products & Services to Program Participants and payment of Administrative Fees to Equalis pursuant to the Master Agreement and this Administration Agreement, to ensure that pricing, inventory, quality, process, and business controls are maintained; provided, however, that such inspections and audits will be conducted upon reasonable notice to Winning Supplier and so as not to unreasonably interfere with Winning Supplier's business or operations.

3.4. **Force Majeure.** This Agreement will be temporarily suspended during any period to the extent that either Party during that period is unable to carry out its obligations under this Agreement or the Appendices by reason of an Act of God or the public enemy, act of terrorism, pandemic or epidemic, fire, flood, labor disorder not caused by Winning Supplier, civil commotion, closing of the public highways not caused by Winning Supplier, government interference, government regulations, or any other event or occurrence beyond the reasonable control of the affected Party ("**Event of Force Majeure**"). Neither Party will have any liability to the other Party for a delay in performance nor failure to perform to the extent this Agreement or any Appendix is so temporarily suspended; provided that nothing contained herein shall apply to payment obligations with respect to obligations which have already been performed under this Agreement.

3.5. **Notices.** All notices, claims, certificates, requests, demands, and other communications required or permitted hereunder ("**Notice**") must be in writing and will be deemed given to the addresses set forth herein (a) when delivered personally to the recipient, (b) upon delivery by reputable overnight courier service (charges prepaid), or (c) upon delivery or refusal of delivery by certified or registered mail, return receipt requested, and addressed to the intended recipient. The Parties agree that day-to-day business communications, including notification of a change of address or revisions to any Appendix, may be made via electronic communication, including email.

3.6. **Addresses for Notices.** This section may be modified at any time by either Party providing the other Party with written Notice, including via email, of a change of address or addition or deletion to the individuals who will be copied on all Notices.



a. If to **Winning Supplier:**

and with copy to:

Winning Supplier  
Attn: Name, Title  
Street Address 1  
Street Address 2  
City, State Zip

Company Name  
Attn: Name, Title  
Street Address 1  
Street Address 2  
City, State Zip

b. If to **EQUALIS:**

Equalis Group LLC  
Attn: Eric Merkle, SVP  
5550 Granite Parkway, Suite 298  
Plano, Texas 75024

3.7. **Waiver.** Other than the rights and obligations with respect to payment provided by this Agreement, waiver by either Party of or the failure of either Party hereto to enforce at any time its rights with regard to any breach or failure to comply with any provision of this Agreement by the other Party may not be construed as, or constitute, a continuing waiver of such provision, or a waiver of any other future breach of or failure to comply with the same provision or any other provision of this Agreement.

3.8. **Governing Law; Invalidity.** This Agreement shall be construed and enforced in accordance with, and governed by, the laws of the State of Ohio without regard to rules of conflict of laws. If any provision of this Agreement is declared unlawful or unenforceable by judicial determination or performance, then the remainder of this Agreement shall continue in force as if the invalidated provision did not exist. Any suits filed by either Party pursuant to this Agreement shall be brought in a court of competent jurisdiction located in Cuyahoga County, Ohio. In the event either Party initiates a suit and that suit is adjudicated by a court of competent jurisdiction, the prevailing Party shall be entitled to reasonable attorney's fees and costs from the non-prevailing Party in addition to any other relief to which the court determines the prevailing Party is entitled or awarded.

3.9. **Modification.** No release, discharge, abandonment, waiver, alteration, or modification of any of the provisions of this Agreement, or any of the Appendices incorporated herein, shall be binding upon either Party unless set forth in a writing signed by authorized representatives of the Parties.

3.10. **Assignment.** This Agreement and the rights and obligations hereunder may not be assignable by either Party hereto without the prior written consent of the other Party, which consent shall not be unreasonably withheld, conditioned, or delayed, provided, however, that either Party may assign its respective rights and obligations under this Agreement without the consent of the other Party in the event either Party shall hereafter effect a corporate reorganization, consolidation, merger, merge into, sale to, or a transfer of all or substantially all of its properties or assets to another entity. Subject to the preceding sentence, this Agreement will be binding upon, inure to the benefit of, and be enforceable by the Parties and their respective successors and assigns. Any instrument purporting to make an assignment in violation of this section shall be null and void. This Agreement may be extended to additional entities affiliated with either Party upon the agreement of the other Party. No such extension will relieve the extending Party of its rights and obligations under this Agreement.

3.11. **No Third-Party Beneficiaries; Survival of Representations.** This Agreement is made solely for the benefit of the Parties to it, and no other persons will acquire or have any right under or by virtue of this Agreement. Except as otherwise provided herein, all representations, warranties, covenants, and agreements of the Parties shall remain in full force and effect regardless of any termination of this Agreement, in whole or in part.

3.12. **Entire Agreement.** The Master Agreement and this Agreement, together with all attachments, appendices, and exhibits hereto, constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior oral or written representations and agreements with regard to the same subject matter. The Parties acknowledge that this Agreement has been negotiated and incorporates their collective agreement as to the provisions to be contained herein. Therefore, no presumption will arise giving benefit of interpretation by virtue of authorship of any provision of this Agreement, and any ambiguity may not be construed for or against any Party.

3.13. **Execution in Counterparts.** This Agreement may be executed in one or more counterparts, each of which will be deemed an original. For purposes of this Agreement, a facsimile, scanned, or electronic signature will be deemed an original signature.

3.14. **Titles, Headings & Recitals.** The Preamble to this Agreement is hereby incorporated herein and made part of this Agreement. The Recitals stated within this Agreement are deemed to be a part of this Agreement. The titles and headings of the sections and paragraphs of this Agreement are inserted for convenience only and shall not constitute a part hereof or affect in any way the meaning or interpretation of this Agreement.

***[SIGNATURE PAGE TO FOLLOW]***

IN WITNESS WHEREOF, the Parties hereto have caused this Agreement to be executed by their duly authorized representatives as of the Effective Date.

**WINNING SUPPLIER**

By: \_\_\_\_\_  
Name: \_\_\_\_\_  
As: \_\_\_\_\_  
Date: \_\_\_\_\_

**EQUALIS GROUP LLC**

By: \_\_\_\_\_  
Name: Eric Merkle  
As: SVP, Sourcing & Operations  
Date: \_\_\_\_\_

SAMPLE

## APPENDIX A: WINNING SUPPLIER REPORTING REQUIREMENTS

This Appendix may be modified at any time with the mutual written consent of the Parties, including via email.

Winning Supplier shall electronically provide Equalis with a detailed line item monthly report showing the dollar volume of all member Products & Services sales under the contract for the previous month. Reports shall be sent via e-mail to Equalis offices at [Reporting@EqualisGroup.org](mailto:Reporting@EqualisGroup.org). Reports are due on the **fifteenth (15<sup>th</sup>)** day after the end of the previous month. It is the responsibility of Winning Supplier to collect and compile all sales under the Master Agreement from Program Participants and submit one (1) monthly report. Fields below marked as \*required indicate a required field. All other fields are preferred, but not required:

Member Data	Equalis Member ID
	Vendor Customer Number *required (or Equalis Member ID)
	Customer Name *required
	Customer Street Address *required
	Customer City *required
	Customer Zip Code *required
	Customer State *required
Distributor Data	Distributor Name
	Distributor ID
	Distributor Street Address
	Distributor City
	Distributor Zip Code
	Distributor State
Product Data	Product Category level 1
	Product Category level 2 (Where available or applicable)
	Product Category level 3 (Where available or applicable)
	Distributor Product Number
	Manufacturer Product Number
	Product Description
	Product Brand Name
	Product packaging Unit of Measure level 1
	Product packaging Unit of Measure level 2
	Product packaging Unit of Measure level 3
Spend Data	Purchase Unit of Measure
	Purchase Quantity
	Distributor Landed Cost Total \$ (without deviations)
	Distributor Landed Cost Total \$ (with mfr deviations)
	Customer Purchase Total \$ *required
	Admin Fee % *required
	Admin Fee \$ *required

SAMPLE

## APPENDIX B: ROLES & RESPONSIBILITIES

This Appendix defines the roles and responsibilities of Equalis and Winning Supplier under this Agreement. This Appendix may be modified at any time with the mutual written consent of the Parties, including via email.

### 1. Equalis Services.

- 1.1. **Winning Supplier Sales Representative Training.** Equalis will develop, as appropriate and subject to Winning Supplier approval, various sales training materials, sales tools, and marketing collateral to promote the Master Agreement and Winning Supplier's Products & Services. Equalis, as appropriate, will i) conduct periodic sales trainings with Winning Supplier sales representatives assigned to sell Products & Services, ii) provide sales representatives with marketing collateral and sales tools to utilize with sales prospects, with particular focus on the procurement process that led to the establishment of the Master Agreement, the legal ability for sales prospects in any state to purchase Products & Services through the Master Agreement without having to conduct their own bid or RFP process, and the key differentiators in the design of this program with Winning Supplier, and iii) attend at least one Winning Supplier company-wide sales and/or leadership meeting per year.
- 1.2. **Sales Support.** Equalis will engage in Winning Supplier sales efforts as agreed by the Parties through participating in i) individual sales calls, ii) joint sales calls, iii) communications and customer service, iv) discussions and communication with sales prospects during the sales process to address questions relating to the procurement process, legal authority to purchase through the Master Agreement, and program design, v) trainings for Equalis Members' teams, vi) regular business reviews to monitor Program success, and vii) general contract administration.
- 1.3. **Marketing.** Equalis will incorporate information about the Products & Services into Equalis Group's website and general collateral materials. Equalis and Winning Supplier will jointly develop and approve marketing materials to promote Products & Services, such as website content, brochures and collateral, talking points, press releases, and correspondence. Equalis will market the Products & Services to Prospective Participants as part of Equalis' ongoing marketing activities through Equalis Group; these marketing efforts may consist of a combination of i) general marketing of all of Equalis Group's Master Agreements, including the Master Agreement and Winning Supplier's Products & Services, ii) marketing of Winning Supplier's Products & Services specifically and/or as part of a package of selected Master Agreements to targeted Prospective Participants, and iii) attending trade shows, conferences, and meetings.

### 2. Winning Supplier Roles & Responsibilities.

As a condition to Winning Supplier entering into the Master Agreement, which is available to all Public Sector Entities, Winning Supplier must make certain representations, warranties, and covenants to Equalis designed to ensure the success of the Master Agreement for all Prospective Participants, sales prospects, and Winning Supplier.

- 2.1. **Equalis Group Membership Agreement.** Winning Supplier will make available the Equalis Group Master Intergovernmental Cooperative Purchasing Agreement (whether in hard copy, electronically, or via [www.EqualisGroup.org](http://www.EqualisGroup.org)) and request any Prospective Participants subject to the Master Agreement who have not already joined Equalis Group to join Equalis Group in conjunction with

executing Winning Supplier's Customer Agreements and/or beginning to purchase Products & Services from Winning Supplier to ensure that Winning Supplier and each Program Participant are in full compliance with applicable state procurement statutes.

2.2. **Corporate Commitment.** Winning Supplier commits that i) the Master Agreement has received all necessary corporate authorizations and support of Winning Supplier's executive management, ii) the Master Agreement will be promoted to Public Sector Entities, and iii) Winning Supplier will identify an executive corporate sponsor and a separate national account manager that will be responsible for the overall management of the Master Agreement and this Agreement.

2.3. **Sales Commitment.** Winning Supplier commits to market the Master Agreement as a market strategy in the public sector and that its sales force will be trained, engaged, and committed to offering the Master Agreement to Public Sector Entities through Equalis Group in the geographies defined in the Master Agreement. Winning Supplier commits that all sales under the Master Agreement will be accurately and timely reported to Equalis. Winning Supplier also commits that its sales force will be compensated, including sales incentives, for sales to Program Participants under the Master Agreement in a consistent or better manner compared to sales to Public Sector Entities if Winning Supplier were not awarded the Master Agreement. Winning Supplier will make available to interested Prospective Participants such price lists or quotes as may be necessary for such Prospective Participants to evaluate potential purchases of Products & Services under the Master Agreement.

2.4. **Marketing Commitment.** As mutually agreeable, Winning Supplier commits to work with Equalis to develop a sales and marketing plan ("Plan") within the first ninety (90) days of the Master Agreement Effective Date. The Plan may include, but is not limited to, the following:

2.4.1. Issuing co-branded press release

2.4.2. Publishing Master Agreement details and contact information on both Equalis Group and Winning Supplier's websites

2.4.3. Scheduling and holding training on the Master Agreement for the sales teams of both Equalis Group and Winning Supplier

2.4.4. Jointly participating in national and regional conferences

2.4.5. Jointly attending national and regional Equalis Group Member networking events

2.4.6. Designing, publishing, and distributing co-branded marketing materials

2.4.7. Engaging in ongoing marketing and promotion of the Master Agreement for the entire Term of the Master Agreement (e.g., developing and presenting case studies, collateral pieces, and presentations)

## APPENDIX C: FINANCIAL TERMS

This Appendix may be modified at any time with the mutual written consent of the Parties.

### 1. **Administrative Fee.**

On or before the fifteenth (15<sup>th</sup>) of each month, Winning Supplier shall remit to Equalis an administrative fee payment (the “**Administrative Fee**”) of **written number** percent (**number**%) of the total Winning Supplier revenue (the “**Equalis Group Spend**” or “**Spend**”) invoiced to Program Participants during the prior calendar month. “Spend” shall mean the cumulative purchases of Products & Services by Program Participants under the Master Agreement net of taxes, shipping costs, returns, and credits. All Administrative Fees not paid when due shall bear interest at a rate equal to the lesser of one- and one-half percent (1.5%) per month or the maximum rate permitted by law until paid in full.

See Finance/Revenue comments here.

### 2. **Case-by-Case Administrative Fee Adjustments.**

The Parties understand and acknowledge that Winning Supplier may have to provide aggressive deviated pricing on a case-by-case basis to win certain opportunities with Prospective Participants when those opportunities represent a sufficiently large Spend and/or are highly competitive. In such situations, Winning Supplier may request Equalis accept a reduced Administrative Fee. The Parties agree to evaluate each such situation as it arises and utilize best efforts to establish an adjusted Administrative Fee rate upon mutual written agreement (including via email) of the Parties.

### 3. **Rebates or Other Payments.**

Insert rebate or other payment language as agreed.



# **Appendices**

## **(Supplemental Information Relevant to Our Proposal**

# Products and Services

## FortiGate® Network Security Platform - \*Top Selling Models Matrix

	FG/FWF-40F	FG/FWF-60F	FG/FWF-80F	FG-100F
Firewall Throughput (1518/512/64 byte UDP)	5 / 5 / 5 Gbps	10/10/6 Gbps	10 / 10 / 7 Gbps	20 / 18 / 10 Gbps
IPsec VPN Throughput (512 byte) <sup>1</sup>	4.4 Gbps	6.5 Gbps	6.5 Gbps	11.5 Gbps
IPS Throughput (Enterprise Mix) <sup>2</sup>	1 Gbps	1.4 Gbps	1.4 Gbps	2.6 Gbps
NGFW Throughput (Enterprise Mix) <sup>2,4</sup>	800 Mbps	1 Gbps	1 Gbps	1.6 Gbps
Threat Protection Throughput (Ent. Mix) <sup>2,5</sup>	600 Mbps	700 Mbps	900 Mbps <sup>6</sup>	1 Gbps
Firewall Latency	2.97 µs	3.3 µs	3.23 µs	4.97µs
Concurrent Sessions	700,000	700,000	1.5 Million	1.5 Million
New Sessions/Sec	35,000	35,000	45,000	56,000
Firewall Policies	5,000	5,000	5,000	10,000
Max G/W to G/W IPSEC Tunnels	200	200	200	2,000
Max Client to G/W IPSEC Tunnels	250	500	2,500	16,000
SSL VPN Throughput	490 Mbps	900 Mbps	950 Mbps	1 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	200	200	200	500
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	310 Mbps	630 Mbps	715 Mbps	1 Gbps
Application Control Throughput (HTTP 64K) <sup>2</sup>	990 Mbps	1.8 Gbps	1.8 Gbps	2.2 Gbps
Max FortiAPs (Total / Tunnel)	16 / 8	64 / 32	96 / 48	128 / 64
Max FortiSwitches	8	16	16	32
Max FortiTokens	500	500	500	5,000
Virtual Domains ( Default/Max)	10 / 10	10 / 10	10 / 10	10 / 10
Interfaces	5x GE RJ45	10x GE RJ45	8x GE RJ45, 2x Shared Port Pairs	2x 10 GE SFP+, 18x GE RJ45, 4x Shared Port Pairs, 8x GE SFP
Local Storage	—	128 GB (61F)	128 GB (81F)	480 GB (101F)
Power Supplies	Single AC PS	Single AC PS	Single AC PS, dual inputs	Dual AC PS
Form Factor	Desktop	Desktop	Desktop	1 RU
Variants	WiFi, 3G4G	WiFi, Storage	WiFi, 3G4G, DSL, Bypass, Storage	—
	FG-200E	FG-200F	FG-400E	FG-600E
Firewall Throughput (1518/512/64 byte UDP)	20 / 20 / 9 Gbps	27 / 27 / 11 Gbps	32 / 32 / 24 Gbps	36 / 36 / 27 Gbps
IPsec VPN Throughput (512 byte) <sup>1</sup>	7.2 Gbps	13 Gbps	20 Gbps	20 Gbps
IPS Throughput (Enterprise Mix) <sup>2</sup>	2.2 Gbps	5 Gbps	7.8 Gbps	10 Gbps
NGFW Throughput (Enterprise Mix) <sup>2,4</sup>	1.8 Gbps	3.5 Gbps	6 Gbps	9.5 Gbps
Threat Protection Throughput (Ent. Mix) <sup>2,5</sup>	1.2 Gbps	3 Gbps	5 Gbps	7 Gbps
Firewall Latency	3 µs	4.78 µs	2.14 µs	1.54 µs
Concurrent Sessions	2 Million	3 Million	4 Million	8 Million
New Sessions/Sec	135,000	280,000	450,000	450,000
Firewall Policies	10,000	10,000	10,000	10,000
Max G/W to G/W IPSEC Tunnels	2,000	2,000	2,000	2,000
Max Client to G/W IPSEC Tunnels	10,000	16,000	50,000	50,000
SSL VPN Throughput	900 Mbps	2 Gbps	4.5 Gbps	7 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	500	500	5,000	10,000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	820 Mbps	4 Gbps	4.8 Gbps	8 Gbps
Application Control Throughput (HTTP 64K) <sup>2</sup>	3.5 Gbps	13 Gbps	12 Gbps	15 Gbps
Max FortiAPs (Total / Tunnel)	256 / 128	256 / 128	512 / 256	1,024 / 512
Max FortiSwitches	64	64	72	96
Max FortiTokens	5,000	5,000	5,000	5,000
Virtual Domains ( Default/Max)	10 / 10	10 / 10	10 / 10	10 / 10
Interfaces	18x GE RJ45, 4x GE SFP	4x 10 GE SFP+, 18x GE RJ45, 8x GE SFP	18x GE RJ45, 16x GE SFP	2x 10 GE SFP+, 10x GE RJ45, 8x GE SFP
Local Storage	480 GB (201E)	480 GB (201F)	480 GB (401E)	480 GB (601E)
Power Supplies	Single AC PS	Dual AC PS	Single AC PS, opt. Dual PS	Single AC PS, opt. Dual PS
Form Factor	1 RU	1 RU	1 RU	1 RU
Variants	—	—	—	—

# FortiGate® Network Security Platform - \*Top Selling Models Matrix

	FG-1100E	FG-1800F	FG-2200E	FG-2600F
Firewall Throughput (1518/512/64 byte UDP)	80 / 80 / 45 Gbps	198 / 197 / 140 Gbps	158 / 155 / 100 Gbps	198 / 196 / 120 Gbps
IPsec VPN Throughput (512 byte) <sup>1</sup>	48 Gbps	55 Gbps	98 Gbps	55 Gbps
IPS Throughput (Enterprise Mix) <sup>2</sup>	12.5 Gbps	17 Gbps	21 Gbps	24 Gbps
NGFW Throughput (Enterprise Mix) <sup>2,4</sup>	9.8 Gbps	11 Gbps	13.5 Gbps	19 Gbps
Threat Protection Throughput (Ent. Mix) <sup>2,5</sup>	7.1 Gbps	9.1 Gbps	11 Gbps	17 Gbps
Firewall Latency	2.76 µs	3.22 µs	3.09 µs	3.41 µs
Concurrent Sessions	8 Million	12 Million / 40 Million <sup>7</sup>	24 Million	24 Million / 40 Million <sup>7</sup>
New Sessions/Sec	500,000	750,000 / 2 Million <sup>7</sup>	500,000	1 Million / 2 Million <sup>7</sup>
Firewall Policies	100,000	100,000	100,000	100,000
Max G/W to G/W IPSEC Tunnels	20,000	20,000	20,000	20,000
Max Client to G/W IPSEC Tunnels	100,000	100,000	100,000	100,000
SSL VPN Throughput	8.4 Gbps	11 Gbps	10 Gbps	16 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	10,000	10,000	30,000	30,000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	10 Gbps	12 Gbps	17 Gbps	20 Gbps
Application Control Throughput (HTTP 64K) <sup>2</sup>	26 Gbps	34 Gbps	52 Gbps	64 Gbps
Max FortiAPs (Total, Tunnel)	4,096 / 2,048	4,096 / 2,048	4,096 / 2,048	4,096 / 2,048
Max FortiSwitches	196	196	196	196
Max FortiTokens	20,000	20,000	20,000	20,000
Virtual Domains ( Default/Max)	10 / 250	10 / 250	10 / 500	10 / 500
Interfaces	2× 40GE QSFP+, 4× 25GE SFP28, 4× 10GE SFP+, 8× GE SFP, 18× GE RJ45	4× 40 GE QSFP+, 12× 25 GE SFP28, 2×10 GE SFP+, 8× GE SFP, 18× GE RJ45	4× 40GE QSFP+, 20× 25GE SFP28, 14× GE RJ45	4× 100GE QSFP28/40GE QSFP+, 16× 25GE SFP28, 16× 10GE RJ45, 2× 10GE SFP+, 2× GE RJ45
Local Storage	960 GB (1101E)	2 TB (1801F)	2 TB (2201E)	2 TB (2601F)
Power Supplies	Dual PS	Dual PS	Dual PS	Dual PS
Form Factor	2 RU	2 RU	2 RU	2 RU
Variants	DC	DC	—	DC
	FG-3300E	FG-3400E	FG-3500F	FG-3600E
Firewall Throughput (1518/512/64 byte UDP)	160 / 158 / 100 Gbps	240 / 238 / 150 Gbps	595 / 590 / 420 Gbps	240 / 240 / 150 Gbps
IPsec VPN Throughput (512 byte) <sup>1</sup>	98 Gbps	140 Gbps	165 Gbps	140 Gbps
IPS Throughput (Enterprise Mix) <sup>2</sup>	27 Gbps	44 Gbps	72 Gbps	55 Gbps
NGFW Throughput (Enterprise Mix) <sup>2,4</sup>	23 Gbps	34 Gbps	65 Gbps	40 Gbps
Threat Protection Throughput (Ent. Mix) <sup>2,5</sup>	17 Gbps	25 Gbps	63 Gbps	30 Gbps
Firewall Latency	3.17 µs	3.33 µs	2.98 µs	3.27µs
Concurrent Sessions	50 Million	50 Million	140 Million / 348 Million <sup>7</sup>	50 Million
New Sessions/Sec	700,000	850,000	1 Million / 5 Million <sup>7</sup>	950,000
Firewall Policies	200,000	200,000	200,000	200,000
Max G/W to G/W IPSEC Tunnels	40,000	40,000	40,000	40,000
Max Client to G/W IPSEC Tunnels	200,000	200,000	200,000	200,000
SSL VPN Throughput	10 Gbps	11 Gbps	16 Gbps	12 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	30,000	30,000	30,000	30,000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	21 Gbps	30 Gbps	63 Gbps	34 Gbps
Application Control Throughput (HTTP 64K) <sup>2</sup>	70 Gbps	86 Gbps	135 Gbps	95 Gbps
Max FortiAPs (Total, Tunnel)	4,096 / 2,048	4,096 / 2,048	4,096 / 2,048	4,096 / 2,048
Max FortiSwitches	300	300	300	300
Max FortiTokens	20,000	20,000	20,000	20,000
Virtual Domains ( Default/Max)	10 / 500	10 / 500	10 / 500	10 / 500
Interfaces	4× 40GE QSFP+, 16× 25GE SFP28, 4× 10GE RJ45, 14× GE RJ45	4× 100GE QSFP28/40GE QSFP+, 24× 25GE SFP28, 2× GE RJ45	6× 100GE QSFP28/40GE QSFP+, 32× 25GE SFP28, 2× GE RJ45	6× 100GE QSFP28/40GE QSFP+, 32× 25GE SFP28, 2× GE RJ45
Local Storage	2 TB (3301E)	4 TB (3401E)	4 TB (3501F)	4 TB (3601E)
Power Supplies	Dual PS	Dual PS	Dual PS	Dual PS
Form Factor	2 RU	2 RU	2 RU	2 RU
Variants	—	DC	—	DC

\* Featured Top selling models, for complete FortiGate offerings please visit [www.fortinet.com](http://www.fortinet.com). FortiGate virtual appliances are also available. All performance values are “up to” and vary depending on system configuration.



# FortiGate® Network Security Platform - \*Top Selling Models Matrix

	FG-3960E	FG-3980E	FG-4200F	FG-4400F
Firewall Throughput (1518/512/64 byte UDP)	620 / 610 / 370 Gbps	1.05 Tbps / 1.05 Tbps / 680 Gbps	800 / 788 / 400 Gbps	1.15 / 1.14 / 0.50 Tbps
IPsec VPN Throughput (512 byte) <sup>1</sup>	280 Gbps	400 Gbps	210 Gbps	310 Gbps
IPS Throughput (Enterprise Mix) <sup>2</sup>	30 Gbps	32 Gbps	52 Gbps	94 Gbps
NGFW Throughput (Enterprise Mix) <sup>2,4</sup>	22 Gbps	28 Gbps	47 Gbps	82 Gbps
Threat Protection Throughput (Ent. Mix) <sup>2,5</sup>	13.5 Gbps	20 Gbps	45 Gbps <sup>6</sup>	75 Gbps <sup>6</sup>
Firewall Latency	3 µs	3 µs	3.02 µs	2.98 µs
Concurrent Sessions	160 Million	160 Million	210 Million / 450 Million <sup>7</sup>	210 Million / 700 Million <sup>7</sup>
New Sessions/Sec	720,000	800,000	1 Million / 7 Million <sup>7</sup>	1 Million / 10 Million <sup>7</sup>
Firewall Policies	200,000	200,000	200,000	200,000
Max G/W to G/W IPSEC Tunnels	40,000	40,000	40,000	40,000
Max Client to G/W IPSEC Tunnels	200,000	200,000	200,000	200,000
SSL VPN Throughput	9 Gbps	9.5 Gbps	16 Gbps	16 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	30,000	30,000	30,000	30,000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	23 Gbps	26 Gbps	50 Gbps	86 Gbps
Application Control Throughput (HTTP 64K) <sup>2</sup>	40 Gbps	55 Gbps	135 Gbps	140 Gbps
Max FortiAPs (Total, Tunnel)	8,192 / 4,096	8,192 / 4,096	8,192 / 4,096	8,192 / 4,096
Max FortiSwitches	300	300	300	300
Max FortiTokens	20,000	20,000	20,000	20,000
Virtual Domains ( Default/Max)	10 / 500	10 / 500	10 / 500	10 / 500
Interfaces	6× 100GE QSFP28/40GE QSFP+, 16× 10GE SFP+, 2x GE RJ45	10× 100GE QSFP28/40GE QSFP+, 16× 10GE SFP+, 2x GE RJ45	8× 100GE QSFP28/40GE QSFP+, 18× 25GE SFP28, 2x GE RJ45	12× 100GE QSFP28/40GE QSFP+, 20× 25GE SFP28, 2x GE RJ45
Local Storage	—	—	4 TB (4201F)	4 TB (4401F)
Power Supplies	3 PS	3 PS	Dual PS	4 PS
Form Factor	5 RU	5 RU	3 RU	4 RU
Variants	DC	DC	DC	DC
	FG-6300F	FG-6500F	FG-7060E	FG-7121F
Firewall Throughput (1518/512/64 byte UDP)	239 / 238 / 135 Gbps	239 / 238 / 135 Gbps	630 / 630 / 340 Gbps	1.89 / 1.88 / 1.129 Tbps
IPsec VPN Throughput (512 byte) <sup>1</sup>	96 Gbps	160 Gbps	100 Gbps	630 Gbps
IPS Throughput (Enterprise Mix) <sup>2</sup>	110 Gbps	170 Gbps	200 Gbps	675 Gbps
NGFW Throughput (Enterprise Mix) <sup>2,4</sup>	90 Gbps	150 Gbps	120 Gbps	550 Gbps
Threat Protection Throughput (Ent. Mix) <sup>2,5</sup>	60 Gbps	100 Gbps	96 Gbps	520 Gbps
Firewall Latency	5 µs	5 µs	7 µs	7.5 µs
Concurrent Sessions	120 Million	200 Million	320 Million	1 Billion
New Sessions/Sec	2 Million	3 Million	1.8 Million	9 Million
Firewall Policies	200,000	200,000	200,000	200,000
Max G/W to G/W IPSEC Tunnels	16,000	16,000	16,000	40,000
Max Client to G/W IPSEC Tunnels	90,000	90,000	64,000	260,000
SSL VPN Throughput	9 Gbps	9 Gbps	15 Gbps	13.7 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	30,000	30,000	48,000	30,000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	66 Gbps	110 Gbps	79.9 Gbps	540 Gbps
Application Control Throughput (HTTP 64K) <sup>2</sup>	150 Gbps	220 Gbps	160 Gbps	1.5 Tbps
Max FortiAPs (Total, Tunnel)	—	—	—	—
Max FortiSwitches	256	256	256	300
Max FortiTokens	20,000	20,000	20,000	20,000
Virtual Domains ( Default/Max)	10 / 500	10 / 500	10 / 500	10 / 500
Interfaces	4× 100GE QSFP28/40GE QSFP+, 24× 25GE SFP28, 3× 10GE SFP+, 2x GE RJ45	4× 100GE QSFP28/40GE QSFP+, 24× 25GE SFP28, 3× 10GE SFP+, 2x GE RJ45	Varied	Varied
Local Storage	2 TB NVMe (6301F)	2 TB NVMe (6501F)	—	4× 4 TB SSD
Power Supplies	3 PS	3 PS	4+2 PS	8 PS
Form Factor	3 RU	3 RU	8 RU	16 RU
Variants	DC	DC	DC	—

1. IPsec VPN performance test uses AES256-SHA256.

2. IPS, Application Control, NGFW and Threat Protection are measured with Logging enabled.

3. SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

4. NGFW performance is measured with Firewall, IPS and Application Control enabled, Enterprise Mix traffic.

5. Threat Protection performance is measured with Firewall, IPS, Application Control, (6.URL Filtering) and Malware Protection enabled, Enterprise Mix traffic.

7. Requires Hyperscale license



## FortiManager™ Centralized Management Platform

	FMG-200G	FMG-300F	FMG-400G	FMG-1000F	FMG-2000E	FMG-3000G	FMG-3700G	FMG-VM-BASE to FMG-VM-UL-UG
Devices/VDOMs (Maximum)	30	100	150	1,000	1,200	4,000+	10,000+	10 to Unlimited
Sustained Log Rates	50	50	50	50	50	150	150	Hardware dependent
GB/Day	2	2	2	2	2	10	10	1-50
Total Interfaces	4x GE RJ45	4x GE RJ45, 2x GE SFP	4x GE RJ45, 2x GE SFP	2x GE RJ45, 2x 10GE SFP+	4x GE RJ45, 2x 10GE SFP+	2x GE RJ45, 2x 25GE SFP28	2x 10GE RJ45, 2x 25GE SFP28	1 / 4 (vNIC Min / Max)
Storage Capacity	2x 4 TB	4x 4 TB	8x 4 TB	8x 4 TB	12x 3 TB	16x 4 TB	60x 4TB HDD + 6x 3.2TB NVMe SSD	80 GB / 16 TB (Min / Max)

## FortiAnalyzer™ Centralized Logging & Reporting Solution

	FAZ-150G	FAZ-300G	FAZ-800G	FAZ-1000F	FAZ-3000G	FAZ-3500G	FAZ-3700G	FAZ-VM-BASE to FAZ-VM-GB2000
GB Logs/Day	25	100	200	660	3,000	5,000	8,300	1 to +2,000
Analytic Sustained Rate (logs/sec)	500	2,000	4,000	20,000	42,000	60,000	100,000	—
Collector Sustained Rate (logs/sec)	750	3,000	6,000	30,000	60,000	90,000	150,000	—
Total Interfaces	2x GE RJ45	4x GE RJ45	4x GE RJ45, 2x GE SFP	2x GE RJ45, 2x 10GE SFP+	2x GE RJ45, 2x 25GE SFP28	2x GE RJ45, 2x 25GE SFP28	2x 10GE RJ45, 2x 25GE SFP28	1 / 4 (vNIC Min / Max)
Storage Capacity	2x 2 TB	2x 4 TB	4x 4 TB	8x 4 TB	16x 4 TB	24x 4 TB	60x 4TB HDD + 6x 3.2TB NVMe SSD	500 GB to +100 TB

## FortiSIEM™ Unified Event Correlation and Risk Management Solution

	FSM-500F "COLLECTOR"	FSM-2000F "SUPERVISOR"	FSM-3500G "SUPERVISOR"
All-in-One License Capacity	N/A	Up to 500	Up to 2,000
EPS Capacity (all features enabled)	5,000	Up to 15,000	Up to 40,000

## FortiAuthenticator™ User Identity Management Server

	FAC-300F	FAC-800F	FAC-3000F	FAC-VM BASE to FAC-VM-10000-UG
Max Local + Remote Users/ User Group	1,500 / 150	8,000 / 800	40,000 / 240,000	100 / 10 to +10,000 / 1,000
Max NAS Devices	500	2,666	80,000	33 to +33,333
Max FortiTokens	3,000	16,000	480,000	200 to +20,000
Interfaces	4x GE RJ45	4x GE RJ45, 2x SFP	4x GE RJ45, 2x SFP	1 - 4 vNICs
Storage Capacity	2	2x 2 TB	2x 2 TB	60 GB to 16 TB

## FortiAP™ Wireless Access Point

	FortiAP Series	FortiAP U-Series
Management	FortiGate-Managed, Cloud-Managed	FortiGate-Managed, Cloud-Managed, Controller-Managed
Security	Via FortiGate	Via FortiGate

\* Frequency selection and power may be restricted to abide by regional regulatory compliance laws.  
For Complete selection of FortiAPs, including remote and outdoor devices, please refer to Fortinet Wireless Solution Matrix

## FortiSwitch™ Secured Access Switch

	100 Series	200 Series	400 Series	500 Series	1000 Series	3000 Series
Main Port Speed	1 Gbps	1 Gbps	1 Gbps	1 Gbps	10/40 Gbps	40/100 Gbps
Main Port Count Options	8, 24, 48	24, 48	24, 48	24, 48	24, 48	32
Uplink Port Speed	1 or 10 Gbps	1 Gbps	10 Gbps	10 Gbps	40 or 100 Gbps	n/a
Redundant Power Supplies	—	Some Models	Some Models	Optional RSU	•	•
PoE Options	•	•	•	•	—	—

For Complete selection of FortiSwitches, please refer to <http://www.fortinet.com/products/fortiswitch>



## FortiNAC™ Network Access Control Solution

	FNC-CA-500C	FNC-CA-600C	FNC-CA-700C	FNC-M-550C
Type	Mid-range Control and Application Server	High Performance Control and Application Server	Ultra High Performance Control and Application Server	Centralized Management Appliance
Target Environment	Small Environments	Medium Environments	Large Environments with few Persistent Agents	Multi-site environments with multiple appliances
Capacity	Manages up to 1,000 ports in the network*	Manages up to 7,500 ports in the network*	Manages up to 15,000 ports in the network*	Unlimited

Virtual appliances are also available, please refer to [www.fortinet.com](http://www.fortinet.com) for more information

## FortiSandbox™ Advanced Threat Prevention System

	FSA-500F	FSA-1000F/-DC	FSA-2000E	FSA-3000F	FSA-VM
Sandbox Pre-Filter Throughput (Files/Hour) <sup>1</sup>	4,500	7,500	12,000	18,000	Hardware dependent
VM Sandboxing Throughput (Files/Hour) <sup>2</sup>	120	280	480	1,340	Hardware dependent
Real-world Effective Throughput (Files/Hour)	600 <sup>2</sup>	1,400 <sup>2</sup>	2,400 <sup>2</sup>	6,720 <sup>2</sup>	Hardware dependent
Number of VMs	2 +4 optional	2 +10 optional	4 +20 optional	8 + 64 optional	4, up to 54

<sup>1</sup> FortiSandbox pre-filtering is powered by FortiGuard Intelligence.  
<sup>2</sup> Measured based on real-world data when both prefilter and dynamic analysis are working consecutively.  
 \* Based on the assumption that 1 blade will be used as master in HA-cluster mode.

## FortiClient™ Advanced Endpoint Security

	Windows	MAC OS X	Linux	Android	iOS	Chromebook
Zero Trust Security (ZTNA) Options	✓	✓	✓	—	—	Partial
Next Generation Endpoint Security (EPP / APT) Options	✓	✓	✓	—	—	—
Cloud Based Endpoint Security (SASE) Options	✓	✓	✓	—	—	—
Security Fabric Components	✓	✓	Partial	Partial	Partial	Partial
VPN Client	✓	✓	SSL VPN only	✓	SSL VPN only	—

## FortiMail™ Messaging Security Server

	FML-200F	FML-400F	FML-900F	FML-2000F	FML-3000F	FML-3200E
Email Routing* (Msg/Hr)	50,000	250,000	800,000	1.6 Mil	3.5 Mil	3.4 Mil
Performance Enterprise ATP* (Msg/Hr)	30,000	150,000	400,000	800,000	2.1 Mil	2.0 Mil
Email Domains	20	100	800	1,000	2,000	2,000
Server Mode Mailboxes	150	400	1,500	2,000	3,000	3,000
Storage Capacity	1× 1 TB	2× 1 TB	2× 2 TB (8 TB Max)	2× 2 TB (12 TB Max)	2× 2 TB (20 TB Max)	2× 2 TB (20 TB Max)

\* Measured based on 100KB message size, no queuing.  
 Virtual appliances are also available, please refer to [www.fortinet.com](http://www.fortinet.com) for more information

## FortiWeb™ Web Application Firewall

	FWB-100E	FWB-400E	FWB-600E	FWB-1000E	FWB-2000F	FWB-3000F	FWB-4000F
Throughput (HTTP)	50 Mbps	250 Mbps	750 Mbps	1.3 Gbps	5 Gbps	10 Gbps	70 Gbps
Total Interfaces	4x GE RJ45	4x GE RJ45 4x GE SFP	2 (+2 bypass) x GE RJ45, 4x GE SFP	2 (+4 bypass) GE RJ45, 4x SFP GE, 2x 10GE SFP+	4x 10GE SFP+, 4x GE RJ45 Bypass, 4x GE SFP	10x 10GE SFP+ (incl. 2 Bypass), 8x GE RJ45 Bypass	2x 40GE QSFP Bypass, 10x 10GE SFP+ (incl. 2 Bypass), 8x GE RJ45 Bypass

Virtual appliances are also available, please refer to [www.fortinet.com](http://www.fortinet.com) for more information



# Virtual Appliance Support Matrix

	VMWare vSphere	Citrix Xen Server	Xen	KVM	Microsoft Hyper-V	Nutanix AHV	Amazon AWS	Microsoft Azure	Oracle OPC/OCI	Google GCP	Alibaba Aliyun
FortiGate-VM *	•	•	•	•	•	•	• / #	• / #	• /#	• /#	• / #
FortiManager-VM	•	•	•	•	•	•	• / #	•	•	•	•
FortiAnalyzer-VM	•	•	•	•	•	•	• / #	•	•	•	•
FortiWeb-VM	•	•	•	•	•	•	• / #	• / #	•	•	•
FortiWeb Manager- VM	•						•				
FortiMail-VM	•	•		•	•	•	• / #	• / #		•	
FortiAuthenticator- VM	•		•	•	•		•	•	•		
FortiADC-VM	•	•	•	•	•	•	• / #	• / #	• / #	• / #	
FortiVoice-VM	•	•		•	•		•	•			
FortiRecorder-VM	•	•		•	•		#				
FortiSandbox-VM	•			•	•	•	• / #	#			
FortiSIEM-VM	•			•	•	•	•	•			•
FortiProxy-VM	•			•							

\*Available as FortiGate-VMX solution for VMware NSX environment, AzureStack and RackSpace (PAYG)  
# on-demand

## List of Other Products

**FortiADC** Application Delivery Controller  
**FortiAI** Virtual Security Analyst™  
**FortiCASB** Cloud Access Security Broker  
**FortiCarrier** CGN Gateway  
**FortiCWP** Cloud Security Analytics  
**FortiDDoS** DDoS Mitigator  
**FortiDeceptor** Deception-based Solution  
**FortiEDR** EDR Solution

**FortiExtender** 3G/4G WAN Extender  
**FortiHypervisor** Hybrid Virtual Appliance  
**FortiInsight** UEBA Solution  
**FortiIsolator** Browser Isolation Platform  
**FortiMonitor** NPMD, DEM and IM Systems  
**FortiProxy** Secure Web Gateway  
**FortiRecorder** Network Video Security  
**FortiSIEM** SIEM with UEBA Solution

**FortiSOAR** SOAR Solution  
**FortiTester** Network Tester  
**FortiToken** 2 Factor Authentication Token  
**FortiVoice** Secure VoIP Solution  
**FortiWLC** Wireless Controller  
**FortiWLM** Wireless Manager  
**FortiXDR** Extended Detection and Response



www.fortinet.com

Copyright © 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.



# FortiCare Services

## Technical Support and Advanced Services



### Hit the ground running with your new capabilities

Fast-track return on investment with streamlined migration and deployment



### Get expert help when you need it

Accelerate incident resolution and maximize efficacy with 24×7 assistance from technical experts



### Enhance your security with tailored guidance

Increase productivity and avoid incidents with operational reviews, account planning, and upgrade assistance

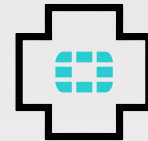
## Confidence in Your Investment

Businesses are making huge investments in security and Fortinet Fabric technologies to provide essential services critical to securing their most valuable assets. Organizations often lack the in-house expertise or resources for initial deployment, product support, and ongoing operations. At Fortinet, we understand these challenges and provide FortiCare Services to thousands of organizations every year to address them.

We want organizations to feel confident that they are maximizing the value of their investments quickly, and realizing efficiency and efficacy gains over time. Whether migrating to a Fortinet next-generation firewall (NGFW), implementing software-defined wide-area networking (SD-WAN) to protect your branch locations, or automating security operations functions, we will work with you to match the proper services with your unique business needs. We are dedicated to your success and provide the expertise you need, when you need it.

## FortiCare Services

FortiCare Services provides customers access to over 1,000 experts to ensure efficient and effective deployment, operations, and maintenance of their Fortinet capabilities. Accelerated implementation and configuration optimization are provided through Professional Services engagements and dedicated resources. Global technical support is offered 24×7 with flexible add-ons, including enhanced service level agreements (SLAs) and premium hardware replacement through 200+ in-country depots. For advanced needs of enterprises and service providers, Fortinet offers advanced services that provide high-touch account management and business guidance through designated resources. Additionally, Enterprise Support Agreements (ESAs) are available to simplify consumption of the services.



## Expertise at Your Service

- 24×7 Global Support
- 1,000+ NSE and Industry Certified Global Resources
- 3 Regional Centers of Expertise
- 19 Support Centers
- 40 Regional Depots
- 200+ In-country Depots
- 4-hour Expedited Hardware Replacement Availability

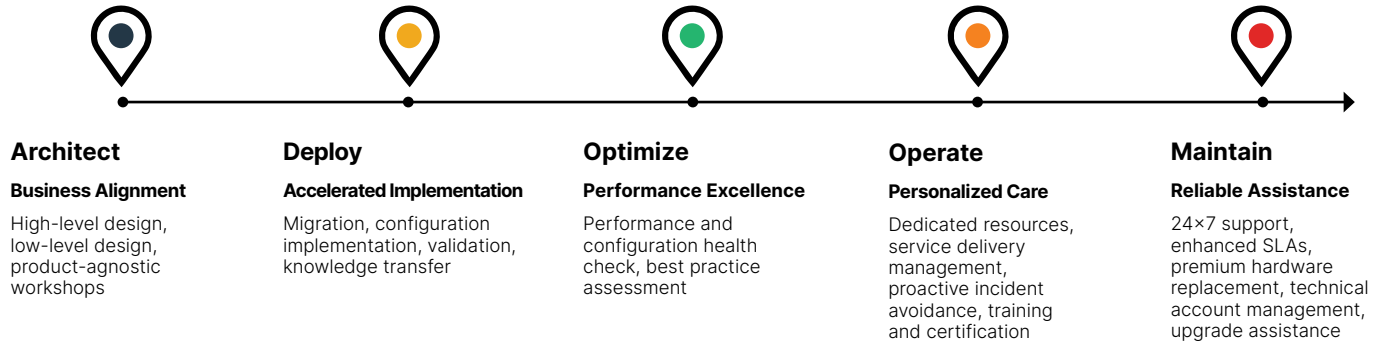
## FortiCare Worldwide

### 24×7 Support

[support.fortinet.com](https://support.fortinet.com)

## The Journey

Adopting new technologies is not a project with a start and a finish. Instead, it is a journey from design and implementation to optimization, operations, and ongoing management of the solution. Fortinet has you covered every step of the way, freeing up your resources to focus on your business.



## Feature Highlights: Technical Support

Organizations depend on Fortinet solutions to provide critical services. If any issues arise, they need to be addressed quickly to help ensure security and business continuity. Flexible support options help organizations maximize uptime, security, and performance according to the individual needs of each business.

### 24x7 FortiCare

Technical support is delivered through our global technical assistance and regional support centers.

- Global toll-free numbers are available 24x7
- Web chat for quick answers
- A support portal for ticket creation or to manage assets and life cycles
- Standard next-business-day RMA service

### ASE FortiCare

Fast-track access to technical experts for accelerated issue resolution.

- Direct access to dedicated enterprise support team
- Single-touch ticket handling by the ASE team
- Enhanced SLAs

*Available for FortiGate, FortiGate VM, and FortiWiFi appliances*

### Premium Hardware Replacement

Premium RMA options are available across the portfolio for expedited replacement of defective hardware.

- Next-day delivery
- 4-hour courier
- 4-hour courier with on-site engineer
- Secure RMA: non-return of defective hardware

### Best Practice Service

Connect with specialists who provide guidance on best-practice deployments, upgrades, and operations.

- Speed adoption of new capabilities with expert guidance, sample configurations, vetted playbooks, and example scripts
- Aid DevOps with practical advice on common feature usage, relevant tools, and sample code
- Access proven models for integration with third-party products

*Available for FortiManager, FortiMonitor, and FortiClient, FortiEDR, FortiSOAR*

## Self-service Resources

For expedited answers, Fortinet maintains ample self-service resources to get you the answers you need, fast. Resources include a knowledge base with tips, quick-start and video guides, and connections to the global Fortinet community.

Feature Highlights: Advanced Services

For enhanced security and tailored guidance, FortiCare Advanced Services gives you direct assistance from technical experts who know your business and can help accelerate issue resolution. With designated account management and service delivery, you can focus on your business while we focus on your success.



Entitlements vary by level but can include:

Designated advanced technical support	for focused resolution of incoming technical support issues.
Service delivery management	annual service and performance review. Quarterly operational review to cover technical ticket statistics, quality issues, overall ongoing ticket analysis, product life cycle, ongoing activity, and 90-day project planning.
Annual training package	including NSE 4 and NSE 5 training and certification vouchers.
Advanced service points	for remote after-hours assistance, product upgrade assistance, and software recommendations.
Root-cause analysis	of critical incidents (Priority-1 and Priority-2) related to Fortinet appliances.
Upgrade assistance	which may include software recommendation, upgrade testing, and planning assistance.

Advanced Service for Enterprise and Service Providers

Enterprise offerings come in three levels: PREMIUM, BUSINESS, and FIRST. Service Providers offerings come in two levels: SELECT and ELITE. Benefits vary by level.

Global FIRST and Global ELITE Advanced Services packages are also available to extend the geographical coverage of the service. This service level provides a designated lead engineer per region covering EMEA, Americas, and Asia Pacific. The service features, as described in the FIRST service, are provided within each region with global coordination.

## Feature Highlights: Professional Services

As networks and threats rapidly evolve, it's critical to make sure security capabilities can keep up. Given the global cybersecurity skills shortage, today's organizations often lack the in-house expertise or enough staff to deploy, operate, and maintain the new technologies required to close security gaps. FortiCare Professional Services delivers expert help to ensure Fortinet deployments are optimized for each customer's unique needs.

### Hit the Ground Running With New Capabilities

Fast-track return on investment (ROI) with streamlined expert deployment. Consultants with multivendor experience help swiftly migrate from legacy technologies and adopt new capabilities.

### Extend In-house Teams With Dedicated Resources

Offload redundant operational tasks including configuration, upgrades, and technical incident management to domain experts who know your business.

### Achieve Performance and Configuration Excellence

Adapt protections when there are changes in users, applications, and traffic patterns with regular reviews of configuration, performance, and policies, for reliability and sustained security.

## Product-agnostic Consulting Services

Cybersecurity Advisory and Consulting Services allow our experts to partner with business leaders, helping organizations be at their best through this ever-changing environment. Fortinet experts discover existing security posture elements through a vendor-agnostic approach; align findings to business goals, strategic objectives, and compliance requirements; and guide existing projects and future planning toward framework maturity.



### Discover

Business Goals  
Security Posture  
Systems/Objectives



### Align

Security Framework  
Compliance Requirements  
Strategic Objectives



### Guide

Architectural Design  
Operational Practices  
Maturity Roadmap

## FortiGuard Labs Consulting

Consulting services are designed to help your organization address your specific threat landscapes and improve your organization's ability to use threat intelligence to meet that challenge. These services leverage the expertise and experience of the FortiGuard Labs team and provide the answers to the questions organizations are asking most:



### Threats

What are the most important threats on which I should focus?



### Environment

Is my environment as secure as it needs to be?



### Operations

Are my people properly trained to defend us against the threats we face?

## Fortinet Technical Assistance Centers



Regional COE:	AMER Regional TAC:	EMEA Regional TAC:	APAC Regional TAC:
<ul style="list-style-type: none"> <li>Vancouver</li> <li>Sophia Antipolis</li> <li>Kuala Lumpur</li> </ul>	<ul style="list-style-type: none"> <li>Dallas</li> <li>Mexico City</li> <li>Miami</li> <li>Ottawa</li> <li>Sunnyvale</li> </ul>	<ul style="list-style-type: none"> <li>Bangalore</li> <li>Dubai</li> <li>Frankfurt</li> <li>Prague</li> </ul>	<ul style="list-style-type: none"> <li>Beijing</li> <li>Sydney</li> <li>Tokyo</li> </ul>

## FortiCare Services

	24x7 FortiCare	ASE FortiCare	Premium RMA	Best Practice Services	Advanced Services	Professional Services
Technical Support	✓	✓				
Enhanced SLAs		✓			✓	
Hardware Replacement	✓	✓	✓			
Technical Account Management					✓	
Architecture and Design						✓
Migration and Deployment						✓
Deployment and Upgrade Guidance				✓	✓	✓
Optimization and Integration						✓
Operations and Management						✓

Service	Description
<b>Technical Support</b>	
24x7 FortiCare	24x7 Technical Support per device—12 months.
ASE FortiCare	Advanced Support Experience Technical Support per device—12 months.
Best Practice Service	Best-practice guidance for deployments and upgrades per device—12 months.
<b>Advanced Services</b>	
Premium—Enterprise Technical Support Service	Premium—Enterprise Support Service—12 months.
Business—Enterprise Technical Support Service	Business—Enterprise Support Service provided by designated engineer—12 months.
First—Enterprise Technical Support Service	First—Enterprise Support Service provided by designated Technical Account Manager—12 months.
Global First—Enterprise Technical Support Service	Global First—Enterprise Support Service provided by designated TAM—12 months.
Select—Service Provider Technical Support Service	Select—Service Provider Support Service provided by advanced services team with Service Delivery Manager—12 months.
Elite—Service Provider Technical Support Service	Elite—Service Provider Support Service provided by advanced services team with designated Technical Account Manager and Service Delivery Manager—12 months.
Global Elite—Service Provider Technical Support Service	Global Elite—Service Provider Support Service provided by advanced services team with designated Technical Account Manager and Service Delivery Manager—12 months.
<b>Professional Services</b>	
Solution Architect Consultancy Service	Per-day solution architect consultancy engagement to document, design, and deliver security architecture improvements per agreed scope.
On-site or Remote Resource Service	Per-day charge for on-site or remote professional service engagement delivery.
On-site or Remote Dedicated Resource Service	12- or 6-month on-site or remote dedicated resource.
<b>FortiGuard Labs Consulting</b>	
FortiGuard Professional Services	FortiGuard Labs Consulting service—On-site or remote. Mitigation strategy, advanced offensive (red team) and defensive (blue team) techniques.
FortiGuard Penetration Testing Service	Remote penetration test of 1 web application or 1 mobile application.
FortiGuard Penetration Testing Service	Remote vulnerability assessment of up to 16 IPs, 32 IPs, 64 IPs, or 128 IPs.
Resource Service—Customer Readiness Testing (SOW)	Per-day charge for customer readiness testing (SOW).
Resource Service—Network Integration	Resource service—Network integration
Resource Service—Network Design and Optimization	Resource service—Network design and optimization
Resource Service—Security Assessment	Resource service—Security assessment
Incident Response Training	Incident response and forensics training
Digital Forensics and Incident Response Consulting Hourly	Digital forensics and incident response consulting services.



## SOLUTION BRIEF

# FortiCare Professional Services

## Introduction

As networks and threats rapidly evolve, it's critical to make sure security capabilities can keep up. Given the global cybersecurity skills shortage, today's organizations often lack the in-house expertise or enough staff to deploy, operate, and maintain the new technologies required to close security gaps. FortiCare Professional Services delivers expert help to ensure Fortinet deployments are optimized for each customer's unique needs. Our experts reduce risk with:

- Accelerated implementation
- Operational enablement for IT teams
- Capability optimization to provide the best security

Further, we can assist with ongoing operations of the Fortinet Security Fabric.

## Streamlined Deployment, Capability Optimization, and Ongoing Operations

### Hit the Ground Running With New Capabilities

Fast-track return on investment (ROI) with streamlined expert deployment. Consultants with multivendor experience help swiftly migrate from legacy technologies and adopt new capabilities. Driven by proven methodology, FortiCare Professional Services plans and executes implementations efficiently and effectively.

### Achieve Performance and Configuration Excellence

As a business evolves, it needs to adapt protections when there are changes in users, applications, and traffic patterns. Professional Services provides regular reviews of configuration, performance, and policies, for reliability and sustained security.

### Extend In-house Teams With Dedicated Resources

In-house IT teams can focus on more critical duties while Fortinet dedicated resources handle administration. Our engineers are domain experts who will get to know each business they are assigned to. Offload redundant operational tasks including configuration, upgrades, and technical incident management. Our experts work closely with in-house teams to maximize productivity by transferring technical and operational knowledge.



**FortiCare Professional Services is available for all Fortinet products and is customized to meet each customer's needs.**

## Professional Services Projects

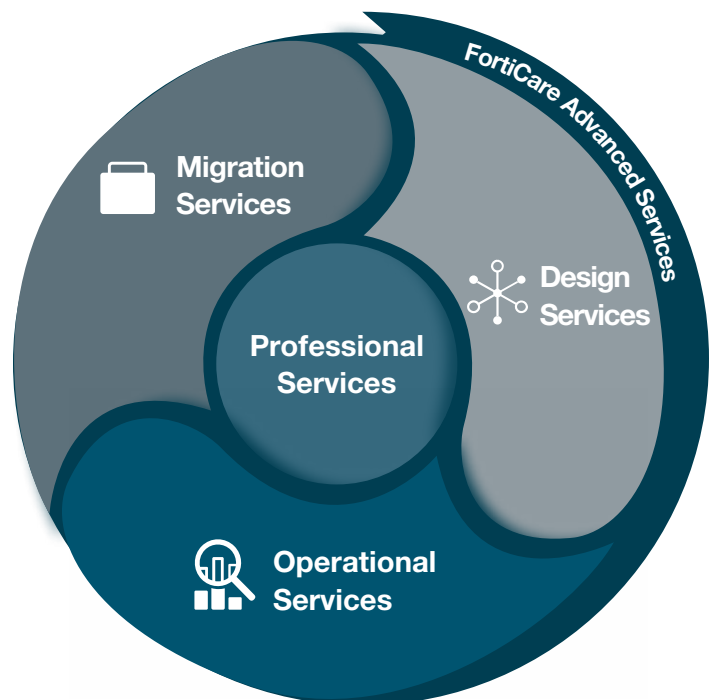
Examples of projects we have executed for our customers include:

<b>Migration from legacy vendor technologies to Fortinet</b>	Production-to-production planning, deployment, and policy migration for firewalls, UTMs, VPNs, and most WLAN/LAN security peripherals
<b>Design and configuration validation</b>	Fortinet solution optimization, integration, and proposed design solution validation
<b>Implementation and configuration</b>	Initial deployment, including installation, provisioning, integration, testing, and production rollout
<b>Integration of the Fortinet Security Fabric with other complementary technologies</b>	Integration with ServiceNow, Splunk, and other security technologies for enhanced visibility and reduced incident investigation timelines
<b>Compliance checks and audit preparation</b>	Guidance on audit and compliance processes, including advice on the correct and optimal configuration of the deployed Fortinet solution
<b>Performance and configuration health checks and policy optimization</b>	Operational performance measurement in a production environment, including a review to identify issues and provide configuration-tuning and policy-optimization recommendations
<b>Dedicated resources for ongoing assistance</b>	Experts available to help with operations after deployment

All service engagements include operational enablement and knowledge transfer to ensure in-house staff is able to operate and maintain the solutions after the service is complete. Although designed to be delivered remotely, on-site options are available.

## Ensure Security Deployments Are Effective and Efficient

Operational teams face challenges when deploying any new technology, and the complexities of today's enterprise networks make it increasingly important to architect and configure security solutions correctly. FortiCare Professional Services gives organizations expert resources to implement and integrate security deployments quickly, while ensuring they are optimized for each unique environment.





# Fortinet Professional Engineer (PSE) – BIO

---

**Summary PSE 1** - A seasoned consultant with over 18+ years of security and IT experience. Served as the Network Manager, Project Manager and Security lead on over ninety consulting engagements for both small medium and large organizations across different industries. Engagements involved performing a wide range of security services including but not restricted to security appliance configuration, deployment, information risk assessments, network security assessments and architecture, security policy development/review, penetration testing, and DRP/BCP development and testing.

### Technologies – PSE 1

- Firewalls, IDS/IPS, UTM, switching routing and routing protocols, Directory Services, Windows servers and desktops, Linux, Antivirus, IP video surveillance, Wi-Fi, security scanners, Security Event Management, VMware, Network topologies, VPN technology, cloud computing, ecommerce, Encryption, LDAP, Radius, Extrusion Prevention, Network Access Control, Security Gateways, Web Content Filtering, Identity Management, Application firewalls, Database monitoring.

**Summary PSE 2** - Over 12 years Technology Industry experience with a variety of roles from Training, Support, and Professional Services, with a primary focus on Network Security and Infrastructure Architecture.

### Technologies – PSE 2

- Security/Firewall
  - FortiGate, Linux IP Tables, Cisco PIX/ASA, IPSec/SSL VPNs, IPS/IDS, DoS, Certificates/PKI, Authentication, FW Virtualization
- Routing
  - Static, Policy Based Routing (PBR), RIP, OSPF, BGP, RPF, NAT, Load-Balancing
- Switching
  - Cisco CATOS/IOS, VTP/VLANS, STP, 802.3ad Link Aggregation
- WAN
  - Modem dialup, ISDN, xDSL, T1/T3, ATM, Fibre, GigE, WAN Optimization
- Services/Protocols
  - HTTP(S), SMTP, POP3, IMAP, DNS, FTP, TFTP, SYSLOG, DHCP, SIP, SNMP, ICMP, TCP, UDP, ESP, IKE, LDAP, RADIUS
- Network Monitoring and Management
  - HP Openview, FortiManager, FortiAnalyzer, Wireshark, SNMPc, Kiwi
- Server Applications
  - Windows Server: Active Directory, DNS, IIS
  - Linux: BIND, Apache, Syslog, Sendmail, Postfix, MySQL

### **Industry Experience (PSE 1 and PSE 2)**

Fortinet Professional Services engineers provide expert level consultation across all business sectors to include but not limited to the following.

- Health Care
- Financial
- Government
- Law
- Education

### **Specialties (PSE 1 and PSE 2)**

- Information Assurance, IT Security Governance, FISMA, HIPPA, Cobit
- Information/ Network Security Architecture, Vulnerability Assessment and Threat Management
- Integration of physical and logical security, Incident Response- Risk Management/ Crisis Management
- Continuity of Operation and Disaster Recovery, Defense-in-Depth (DiD),
- Risk Assessment and Compliance, Data Classification and Categorization
- Certification and Accreditation Program (CAP), Systems Security Plans Incident Response
- Security T&E – Security IAM/ IEM

### **Certifications (PSE 1 and PSE 2)**

All Fortinet Professional Services engineers are at a minimum NSE4 certified with the vast majority of engineers NSE7 certified. Fortinet PSEs also hold multiple industry certifications as well to include but not limited to the following.

- NSE 7, CISSP-ISSAP, FCSE, CISM, ITIL v3, NSA-IAM/IEM, CNSS-Network Protection - “Infosec Professional”
- CNSS-Security Management. NSTISSI-4011, CNSSI-4012, CNSSI-4013 (A), CNSSI-4014 (A), NSTISSI-4015, CNSSI 4016 (A), Security Management Certification – Network Security Certification
- CEH, GIAC, FCSP, CCSP, WCSP



# Fortinet Security Fabric

## Cybersecurity Platform to Enable Digital Innovation

**FortiOS**  
The Heart of the  
Fortinet Security Fabric



### Zero Trust Access



#### FortiNAC

Enforce dynamic network access control and network segmentation



#### FortiAuthenticator

Identify users wherever they are and enforce strong authentication



#### FortiClient

Endpoint integration, visibility, and protection across entire network



#### FortiToken Mobile

One-time password application with push notification

### Surveillance & Communications



#### FortiRecorder

Platform for management of cameras, systems, and storage



#### FortiCamera

Centrally-managed HDTV-quality security coverage reliability



#### FortiVoice

Centralized control and simplified management of phone systems



#### FortiFone

Robust IP Phones w/ HD Audio for versatile deployments

### Security-Driven Networking



#### FortiGate SD-WAN

Application-centric, scalable, and Secure SD-WAN with NGFW



#### FortiGate

NGFW w/ SOC acceleration and industry-leading secure SD-WAN



#### FortiSwitch

Deliver security, performance, and manageable access to data



#### FortiAP

Protect LAN Edge deployments with wireless connectivity



#### FortiExtender

Extend scalable and resilient LTE and LAN connectivity



#### FortiSASE

Secure access service edge to deliver security everywhere



#### FortiProxy

Enforce internet compliance and granular application control



#### FortiIsolator

Maintain an "air-gap" between browser and web content



#### FortiPresence

Real-time location trends, visitor analytics, and heat mapped flows

### Fabric Management Center | SOC



#### FortiXDR

Collect, normalize, and correlate data across security controls



#### FortiEDR

Automated protection and orchestrated incident response



#### FortiSIEM

Integrated security, performance, and availability monitoring



#### FortiSOAR

Automated security operations, analytics, and response



#### FortiAnalyzer

Correlation, reporting, and log management in Security Fabric



#### FortiSandbox

Secure virtual runtime environment to expose unknown threats



#### FortiDeceptor

Discover active attackers inside with decoy assets



#### FortiAI

Accelerate mitigation of evolving threats and threat investigation



#### FortiGuard MDR Service

Monitor and hunt for threats; analyze events; leverage alerts

### Adaptive Cloud Security



#### FortiGate VM

NGFW w/ SOC acceleration and industry-leading secure SD-WAN



#### FortiMail

Secure mail gateway to protect against SPAM and virus attacks



#### FortiWeb

Prevent web application attacks against critical web assets



#### FortiCASB

Prevent misconfigurations of SaaS applications and meet compliance



#### FortiADC

Application-aware intelligence for distribution of application traffic



#### FortiCWP

Manage risk and compliance through multi-cloud infrastructures



#### FortiGSLB

Ensure business continuity during unexpected network downtime



#### FortiDDoS

Machine-learning quickly inspects all Layer 3, 4, and 7 packets



#### FortiCloud Networking

Manage network access, assets, and services through single-pane



#### FortiPhish

Informative simulation to educate internal users of potential threats

### Fabric Management Center | NOC



#### FortiManager

Centralized management of your Fortinet security infrastructure



#### FortiCloud

Protect and deliver data and apps in the Cloud and on-premises



#### FortiMonitor

Analysis tool to provide NOC and SOC monitoring capabilities



#### FortiAIops

Network inspection to rapidly analyze, enable, and correlate

### Open Ecosystem



#### Extended Fabric Ecosystem

### FortiGuard Security Services



Content Security  
Web Security | Advanced SOC/NOC  
User Security | Device Security



SOC & NOC



User Security



Revised October 1, 2021

Icons on this document link to additional information

© Fortinet Inc. All Rights Reserved.

BROCHURE

# Fortinet Product Certifications





## Fortinet Product Certifications

Organizations looking to expand, upgrade, or replace their security solutions often find themselves struggling to compare solutions from different vendors. In addition to consistent information about features and functions, they also need information about the compliance and certification level of individual solutions and whether they will enable them to meet regulatory requirements.

To help companies navigate this process, third-party labs and auditors conduct independent testing to enable a fair comparison between products for things like performance, compliance, and functionality. Using industry standards and advanced benchmarking technologies, such as independent validation of products and services, is essential for businesses to evaluate whether a solution will meet their unique business requirements.

### Third-party Testing

Fortinet has actively participated in third-party testing since we first opened our doors. We are committed to the testing and certification process and believe that it provides three key benefits:

- It validates our design and development process. Third-party labs set standards for functionality, performance, and real-world use cases that help drive the development of key features.
- It helps improve our technology. Direct feedback from standardized benchmark testing helps us in our effort to continually improve our technologies.
- It allows our customers to easily compare our technologies against solutions from other vendors. Annual testing helps us set the bar higher every year, with the objective of achieving a leadership position in every test in which we participate.

### Certifications and Regulatory Compliance

Public and private sector organizations alike require solutions that meet regulatory and compliance requirements. Fortinet is committed to meeting a wide range of national, regional, and international requirements, and we subject our solutions and services to independent third-party audits and testing to guarantee compliance.

### The Fortinet Certifications Resource Center (CRC)

Fortinet's [CRC](#) is the repository for product compliance reports, certifications, and independent validation results from unbiased agencies. The scope of Fortinet's product certifications includes the following categories:

#### Product Certifications



Independent lab testing of Fortinet products using industry standards, best practices, and real-world testing environments

#### Information Security



Certifications and examinations of Fortinet's infrastructure security and networking solutions

#### Compliance



Certifications attesting to Fortinet products' compliance with public sector regulatory frameworks and standards



#### Certifications At-a-Glance

- Fortinet's commitment to innovation and excellence has earned the respect of independent test labs around the world
- 25+ years of consistent testing and compliance
- A wide range of global certifications across verticals

## Product Certifications Overview

Category	Certification	Description	Latest Publication Date	
Product Certifications	<a href="#">ICSA Labs</a>	ICSA Labs is an independent division of Verizon. They provide third-party testing and certification of security and health-related IT products and network-connected devices to measure product compliance, reliability, and performance.	IPsec VPN	08/10/2021
			Firewall	08/25/2021
			WAF	09/27/2021
	<a href="#">AV-Comparatives</a>	AV-Comparatives is an independent lab offering systematic testing to determine whether security software—such as PC/Mac-based antivirus products and mobile security solutions—lives up to its claims. Using one of the largest sample collections in the world, they create a real-world environment for truly accurate testing. Certification by AV-Comparatives provides a globally recognized seal of approval for software performance.	Business Security Test: Mar-Jun 2021	
	<a href="#">SE Labs</a>	SE Labs tests a range of solutions, including endpoint software, network appliances, and cloud services, on their ability to detect attacks, protect against intrusions, or both.	Email Security Services Protection: Jan-Mar 2020	
	<a href="#">MEF 3.0</a>	MEF 3.0 is an SD-WAN Certification Program that uses Spirent as their SD-WAN Authorized Certification and Test Partner (ACTP). Certification involves rigorous tests of the service attributes and requirements defined in MEF 70 and described in detail in the upcoming MEF SD-WAN Certification Test Requirements (MEF W90) standard.	MEF 3.0 SD-WAN: Jun 2020	
	<a href="#">Virus Bulletin</a>	VB is a world leader in security software testing. Their publicly available test reports cover anti-malware protections of all types as well as enterprise-level email and web security solutions.	VBSspam	Sept 2021
			VB100	Sept 2021
	<a href="#">MITRE Engenuity</a>	MITRE Engenuity's ATT&CK™ evaluations assess the ability of a vendor's solutions to defend against specific adversary tactics and techniques. They openly publish these results to provide end-users with the information needed to make good purchasing decisions. These evaluations are not a competitive analysis. There are no scores, rankings, or ratings. Instead, they show how each vendor approaches threat detection in the context of the MITRE ATT&CK knowledge base to provide an unbiased assessment of detection and protection capabilities and highlight potential gaps to drive the industry forward.	Round 3: Fin7/Carbanak: Apr 2021	
Information Security	<a href="#">SOC2</a>	SOC2 is an auditing procedure that ensures that service providers securely manage their customers' data. It covers their security, availability, processing integrity, confidentiality, and/or privacy controls. Compliance is based on the AICPA's (American Institute of Certified Public Accountants) TSC (Trust Services Criteria).	SOC2 Type 2: Apr-Sept 2021	
	<a href="#">ISO</a>	ISO/IEC 27001 is an international standard for managing information security. It defines requirements and controls for establishing, implementing, maintaining, and continually improving an organization's Information Security Management System (ISMS).	ISO/IEC 27001: Jun 2021-Jun 2024	
Government Regulations	<a href="#">FIPS Validated</a>	The Federal Information Processing Standard 140-2 (FIPS 140-2) is an information technology security accreditation program for validating cryptographic modules developed by vendors that meet well-defined security standards.	FIPS 140-2 Level 1	Aug 2021
			FIPS 140-2 Level 2	Sept 2021
	<a href="#">Common Criteria</a>	Common Criteria is an international standard (ISO/IEC 15408) operated by 17 certificate-authorizing nations. 31 countries have accepted it for their respective government acquisition requirements for their IT/networking infrastructures.	CC EAL4+	Oct 2021
			FWcPP+IPS +VPN	Jan 2021



## Summary

Fortinet is committed to the independent testing and certification of its products and services. ICSA, AV-Comparatives, Virus Bulletin, and other independent testing organizations have consistently validated the effectiveness of Fortinet solutions. Fortinet earned ICSA's prestigious Excellence in Information Security Testing (EIST) award for 15 years of participation in 2017 and has been recognized by ICSA for outstanding achievement in information security certification testing 10 years in a row.

**"Real-world third-party validation is an essential resource for enterprises considering security products, helping to cut through the confusion that can be caused by vendor marketing. Fortinet relies on a variety of third-party testing and compliance labs to provide reliable information to organizations making critical security purchasing decisions. They also demonstrate Fortinet's commitment to meeting high industry standards for security detection, performance, reliability, management, and value."**

*- Fortinet CEO Ken Xie*



[www.fortinet.com](http://www.fortinet.com)



# CERTIFICATE

The Certification Body of  
TÜV SÜD AMERICA INC.

hereby certifies that

**Fortinet Technologies (Canada) ULC**  
4190 Still Creek Drive Suite 400  
Burnaby, V5C 6C6 Canada  
(see page 2-4 for additional locations)

Has implemented a Quality Management System in accordance with:

**ISO 9001:2015**

The scope of this Quality Management System includes:

**The Design, Development and Manufacture of Network  
Security Products and the Delivery of Associated  
Security Services and Support Functions**

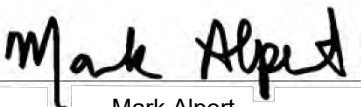
Certificate Expiry Date: June 30, 2023

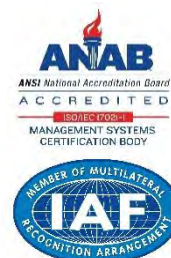
Certificate Registration No: 951 11 5647

Issue Date: July 8, 2020

Reissue Date: N/A



  
Mark Alpert  
Vice President, Business Assurance







# CERTIFICATE

## Fortinet Technologies (Canada) ULC

4190 Still Creek Drive Suite 400  
Burnaby, V5C 6C6 Canada

Scope - The Design, Development and Manufacture of Network Security Products and the Delivery of Associated Security Services and Support function

Processes – Order Entry, Scheduling, Planning for Product Realization, Product / Project Management, Software Development, Hardware Engineering, Production QC Management, Working Environment Control, Technical Documentation, Human Resources, Records Management & MIS Control

## Fortinet Technologies (Canada) ULC

326 Moodie Dr  
Nepean, ON, K2H 8G3 Canada

Scope - Development & Support for Fortinet mail and Preparation of Technical Documents

Processes – Software Development, Technical Support and Customer Service, Technical Documentation, Management & MIS Control, Human Resources

Certificate Expiry Date: June 30, 2023

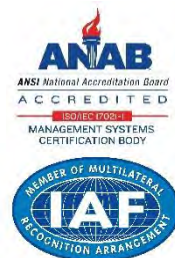
Certificate Registration No: 951 11 5647

Issue Date: July 8, 2020

Reissue Date: N/A



  
Mark Alpert  
Vice President, Business Assurance





# CERTIFICATE

**Fortinet Technologies (Canada) ULC**  
**4185 Still Creek**  
**Burnaby, V5C 6G9 Canada**

**Scope - Information Technology Support Location, Including  
 New Equipment Preparation and Troubleshooting for Headquarters**

**Processes – Record Management & MIS Control**

**Fortinet Inc.**  
**899 Kifer Road**  
**Sunnyvale, 94086 USA**

**Scope - The Design, Development and Manufacture of  
 Network Security Products and the Delivery of  
 Associated Security Services and Support Functions**

**Processes – Order Entry, Scheduling, Planning for Product Realization,  
 Product / Project Management, Software Development, Hardware  
 Engineering, Purchasing, Technical Support and Customer Service,  
 Records Management & MIS Control, Human Resources, Infrastructure  
 and Working Environment Control**

**Certificate Expiry Date: June 30, 2023**

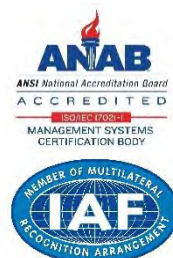
**Certificate Registration No: 951 11 5647**

**Issue Date: July 8, 2020**

**Reissue Date: N/A**



  
 Mark Alpert  
 Vice President, Business Assurance





America

# CERTIFICATE

**Fortinet Inc.**  
**1570 Atlantic St**  
**Union City, 94587 USA**

**Scope - The Manufacture, Quality Control and  
 Operation Function of Network Security Products**

**Processes – Production Control & Service Provision –  
 Product Integration, Shipping and Receiving IQC,  
 RMA Control and Management**

**Certificate Expiry Date: June 30, 2023**

**Certificate Registration No: 951 11 5647**

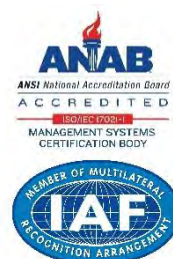
**Issue Date: July 8, 2020**

**Reissue Date: N/A**



*Mark Alpert*

Mark Alpert  
 Vice President, Business Assurance  
 Page 4 of 4



# **Commercial Agreements**

- **Fortinet Product License Agreement / EULA and Warranty Terms**
- **Fortinet Service Terms & Conditions  
For FortiCare, FortiGuard and other Fortinet Service Offerings**
- **Fortinet Professional Service Terms and Conditions**



## Product License Agreement / EULA and Warranty Terms

### Product License Agreement

The parties to this agreement are you (the end-customer) and Fortinet, Inc. ("Fortinet"). CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (THE OR THIS "AGREEMENT" OR "EULA"). USE OR INSTALLATION OF FORTINET PRODUCT(S) AND ANY UPDATES THERETO, INCLUDING HARDWARE APPLIANCE PRODUCTS, SOFTWARE AND FIRMWARE INCLUDED THEREIN BY FORTINET, AND STAND-ALONE SOFTWARE PRODUCTS SOLD BY FORTINET (TOGETHER, THE "PRODUCTS") CONSTITUTES ACCEPTANCE BY YOU OF THE TERMS IN THIS AGREEMENT, AS AMENDED OR UPDATED FROM TIME TO TIME IN FORTINET'S DISCRETION BY FORTINET PUBLISHING AN AMENDED OR UPDATED VERSION. FORTINET SHALL NOT BE BOUND BY ANY ADDITIONAL AND/OR CONFLICTING PROVISIONS IN ANY ORDER, RELEASE, ACCEPTANCE OR OTHER WRITTEN CORRESPONDENCE OR OTHER WRITTEN OR VERBAL COMMUNICATION UNLESS EXPRESSLY AGREED TO IN A WRITING SIGNED BY THE GENERAL COUNSEL OF FORTINET. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT START THE INSTALLATION PROCESS OR USE THE PRODUCTS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, YOU SHOULD IMMEDIATELY, AND IN NO EVENT LATER THAN FIVE (5) CALENDAR DAYS AFTER YOUR RECEIPT OF THE PRODUCT, IMMEDIATELY NOTIFY FORTINET LEGAL [LEGAL@FORTINET.COM](mailto:LEGAL@FORTINET.COM) OF REQUESTED EULA CHANGES.

#### 1. License Grant.

This is a license agreement between you and Fortinet, not a sales agreement. The term "Software", as used throughout this Agreement, includes all Fortinet and third party firmware and software provided to you with, or incorporated into, Fortinet appliances and any stand-alone software provided to you by Fortinet, with the exception of any open source software contained in Fortinet's Products which is discussed in detail in section 15 below, and the term "Software" includes any accompanying documentation, any updates and enhancements of the software or firmware provided to you by Fortinet, at its option. Fortinet grants to you a non-transferable (except as provided in section 5 ("Transfer") and section 15 ("Open Source Software") below), non-exclusive, revocable (in the event of your failure to comply with these terms, in the event of termination, or in the event Fortinet is not properly paid for the applicable Product) license to use the Software solely for your internal business purposes (provided, if (a) agreed by Fortinet in writing, (b) you are authorized by Fortinet in writing to provide managed service provider services ("MSSP") to your end-customers, and (c) you pay for an MSSP license, then you may use the Software and/or Software embedded in Fortinet Hardware to provide those services, subject to the other restrictions in this Agreement), in accordance with the terms set forth in this Agreement and subject to any further restrictions in Fortinet documentation (including license term restrictions), and solely on the Fortinet appliance, or, in the case of blades, CPUs, platform, devices or databases, on the single blade, CPU, platform, device or database on which Fortinet installed the Software, or, for stand-alone Software, solely on a single computer running a validly-licensed copy of the operating system for which the Software was designed unless and except set forth in the published documentation otherwise. For clarity, notwithstanding anything to the contrary, all licenses of Software to be installed on blades, CPUs, platforms, devices or databases are licensed per blade, solely for one blade and not for multiple blades that may be installed in a chassis, per CPU, per platform, per device, or per database basis, up to the blade, CPU, platform, device, database number defined in the license and as applicable and in accordance with the documentation. The Software is "in use" on any appliances, blades, CPUs, platforms, devices, or databases when it is loaded into temporary memory (i.e. RAM), accessed, downloaded, installed, or used on an appliance, blade, CPU, platform, device, or database. You agree that, except for the limited, specific license rights granted in this section 1, you receive no license rights to the Software.

#### 2. Limitation on Use.

You are prohibited from and may not attempt to, and, if you are a corporation, you are responsible to prevent your employees and contractors from attempting to: (a) modify, translate, reverse engineer, decompile, disassemble, create derivative works based on, sublicense, or distribute the Software; (b) rent or lease any rights in the Software in any form to any third party or make the Software available or accessible to third parties in any other manner (except as expressly permitted for MSSP partners); (c) transfer assignment or sublicense right to any other person or entity (except as provided in section 5); (d) remove any proprietary notice, labels, or marks on the Software, Products, and containers; (e) use the Software to determine, or disclose the results of, any benchmarking or performance measurements; (f) interfere with a platform for use of the Software; (g) use the Software on a device not owned and controlled by you; (h) use automated means to access online portions of the platform for the Software; (i) use the Software for third-party training, commercial time-sharing or service bureau use or (except as expressly set forth in this Agreement) use the Software to provide services to third parties; (j) share non-public features or content of the software with any third party; (k) access the software in order to build a competitive product or service, to build a product using similar ideas, features, functions or graphics of the software, or to copy any ideas, features, functions or graphics of the software; or, (l) engage in web scraping or data scraping on or related to the software, including without limitation, collection of information through any software that simulates human activity or any bot or web crawler.

#### 3. Proprietary Rights.

All rights (including copyrights, trade secret, patent and other intellectual property rights), title, interest in and to the Software and any Product, and any copy thereof remain with Fortinet. You acknowledge that no title or other intellectual property rights in the Software or other Products is transferred to you and you will not acquire any rights to the Software or other Products except for the specific limited license as expressly set forth in section 1 ("License Grant") above. You expressly agree and acknowledge that Fortinet owns, retains, and shall retain all intellectual property rights in and to, and you have no intellectual property rights in and to, the Products and the Software other than the License Grant. You agree to keep confidential all Fortinet confidential information and only to use such information for the purposes for which Fortinet disclosed it.

#### 4. Term and Termination.

The term of the license is the shorter of (a) the term as set forth in the ordering documents, other Fortinet documentation, or per Fortinet practices or policies (such as with evaluation or beta licenses or subscription or other term licenses) and (b) for the duration of Fortinet's copyright in the Software. Fortinet may terminate this Agreement, and the licenses and other rights herein, immediately without notice if you breach or fail to comply with any of the terms and conditions of this Agreement or for other reasons as stated in Fortinet's other documentation. You agree that, upon such termination, you will cease using the Software and any Product and either destroy all copies of the Fortinet documentation or return all materials to Fortinet.

#### 5. Transfer.

If you are a Fortinet contracted and authorized reseller or distributor of Products, you may transfer (not rent or lease unless specifically agreed to in writing by Fortinet) the Software to one end user on a permanent basis, provided that: (a) you ensure that your customer and the end user receives a copy of this Agreement, is bound by its terms and conditions, and, by selling the Product or Software, you hereby agree to enforce the terms in this Agreement against such end user, (ii) you at all times comply with all applicable United States export control laws and regulations, and (iii) you agree to refund any fees paid to you by an end user who purchased Product(s) from you but does not agree to the terms contained in this Agreement and therefore wishes to return the Product(s) as provided for in this Agreement. Further, if you are a non-authorized reseller of Products and Services, you are not authorized to sell Product(s), Software or Services, but, regardless, by selling Product(s), Software or Services, you hereby agree you are bound by the restrictions and obligations herein and are bound to: (i) ensure that your customer and the end user receives a copy of this Agreement and are bound in full by all restrictions and obligations herein (ii) enforce the restrictions and obligations in this Agreement against such customer and/or end user, (iii) comply with all applicable United States export control laws and regulations and all other applicable laws, and (iv) refund any fees paid to you by a customer and/or end user who purchased Product(s) from you but does not agree to the restrictions and obligations contained in this Agreement and therefore wishes to return the Product(s) as provided for in this Agreement. Notwithstanding anything to the contrary, distributors, resellers and other Fortinet partners (a) are not agents of Fortinet and (b) are not authorized to bind Fortinet in any way. Fortinet's license, warranty, and support is only available for Products that you purchased directly from an authorized Fortinet channel partner. Products not purchased from an authorized Fortinet channel partner are not eligible, will not be supported, and may be blocked from registration.

#### 6. Limited Warranty.

Fortinet provides this limited warranty for its product only to the single end-user person or entity that originally purchased the Product from Fortinet or its authorized reseller or distributor and paid for such Product. The warranty is only valid for Products which are properly registered on Fortinet's Support Website: <https://support.fortinet.com>, or such other website as provided by Fortinet, or for which the warranty otherwise starts according to Fortinet's policies, and any support is only valid for products properly purchased through authorized distributors and resellers. The warranty periods discussed below will start according to Fortinet's policies passed

at <http://www.fortinet.com/about-us/legal.html> or such other website as provided by Fortinet. It is the Fortinet distributor's and reseller's responsibility to make clear to the end user the date the product was originally shipped from Fortinet, and it is the end user's responsibility to understand the original ship date from the party from which the end user purchased the product. All warranty claims must be submitted in writing to Fortinet before the expiration of the warranty term or such claims are waived in full. Fortinet provides no warranty for any beta, donation or evaluation Products. Fortinet warrants that the hardware portion of the Products ("hardware") will be free from material defects in workmanship as compared to the functional specifications for the period set forth as follows and applicable to the Product type ("Hardware Warranty Period"): (a) a three hundred sixty-five (365) day limited warranty for the Hardware products; (b) for FortiAP, the warranty herein shall last from the start of the warranty period as discussed above until five (5) years following the product announced end-of-life date Hardware; (c) for FortiSwitch Hardware appliance products other than the FortiSwitch-5000 series, the warranty herein shall last from the start of the warranty period as discussed above until five (5) years following the product announced end-of-life date Hardware. Fortinet's sole obligation shall be to repair or offer replacement Hardware for the defective Hardware at no charge to the original owner. This obligation is exclusive of transport fees, labor, de-installation, installation, reconfiguration, or return shipment and handling fees and costs, and Fortinet shall have no obligation related thereto. Such repair or replacement will be rendered by Fortinet at an authorized Fortinet service facility as determined by Fortinet. The replacement Hardware need not be new or of an identical make, model, or part; Fortinet may, in its discretion, replace the defective Hardware (or any part thereof) with any reconditioned Product that Fortinet reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. The Hardware Warranty Period for the repaired or replacement Hardware shall be for the greater of the remaining Hardware Warranty Period or ninety days from the delivery of the repaired or replacement Hardware. If Fortinet determines in its reasonable discretion that a material defect is incapable of correction or that it is not practical to repair or replace defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by Fortinet upon return to Fortinet of the defective Hardware. All Hardware (or part thereof) that is replaced by Fortinet, or for which the purchase price is refunded, shall become the property of Fortinet upon replacement or refund. Fortinet warrants that Software as initially shipped by Fortinet will substantially conform to Fortinet's then-current functional specifications for the Software, as set forth in the applicable documentation for a period of ninety (90) days ("Software Warranty Period"), if the Software is properly installed on approved Hardware and operated as contemplated in its documentation. Fortinet's sole obligation shall be to repair or offer replacement Software for the non-conforming Software with software that substantially conforms to Fortinet's functional specifications. This obligation is exclusive of transport fees, labor, de-installation, installation, reconfiguration, or return shipment and handling fees and costs, and Fortinet shall have no obligation related thereto. Except as otherwise agreed by Fortinet in writing, the warranty replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by Fortinet for the Software. The Software Warranty Period shall extend for an additional ninety (90) days after any warranty replacement software is delivered. If Fortinet determines in its reasonable discretion that a material non-conformance is incapable of correction or that it is not practical to repair or replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by Fortinet; provided that the non-conforming Software (and all copies thereof) is first returned to Fortinet. The license granted respecting any Software for which a refund is given automatically terminates immediately upon refund. For purpose of the above hardware and software warranties, the term "functional specifications" means solely those specifications authorized and published by Fortinet that expressly state in such specifications that they are the functional specifications referred to in this section 6 of this Agreement, and, in the event no such specifications are provided to you with the Software or Hardware, there shall be no warranty on such Software.

#### 7. Disclaimer of Other Warranties and Restrictions.

EXCEPT FOR THE LIMITED WARRANTY SPECIFIED IN SECTION 6 ABOVE, THE PRODUCT AND SOFTWARE ARE PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY, IMPLIED OR EXPRESS WARRANTY OF MERCHANTABILITY, OR WARRANTY FOR FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS FROM THE DATE OF ORIGINAL SHIPMENT FROM FORTINET. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT. NOTWITHSTANDING ANYTHING TO THE CONTRARY, THE HARDWARE WARRANTY PERIOD DISCLOSED HEREIN DOES NOT APPLY TO CERTAIN FORTINET PRODUCTS, INCLUDING FORTINET FORTIAP, AND THE SOFTWARE WARRANTY DOES NOT APPLY TO CERTAIN FORTINET PRODUCTS. YOU HEREBY ACKNOWLEDGE AND AGREE THAT NO VENDOR CAN ASSURE COMPLETE SECURITY AND NOTHING HEREIN OR ELSEWHERE SHALL BE DEEMED TO IMPLY A SECURITY GUARANTEE OR ASSURANCE, AND FORTINET DISCLAIMS LIABILITY REGARDING YOUR WEB BROWSER'S REQUIREMENTS OR ANY THIRD PARTY DEVICE OR APPLIANCE USED TO OPERATE THE SOFTWARE.

The warranty in Section 6 above does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Fortinet or its authorized representative, (b) has not been installed, operated, repaired, updated to the latest version, or maintained in accordance with instructions supplied by Fortinet, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; (d) is licensed for beta, evaluation, donation, testing or demonstration purposes or for which Fortinet does not charge a purchase price or license fee; or (e) is procured from a non-authorized reseller or non-authorized distributor. In the case of beta, testing, evaluation, donation or free Software or Product, the end user acknowledges and agrees that such Software or Product may contain bugs or errors and could cause system failures, data loss and other issues, and the end user agrees that such Software or Product is provided "as-is" without any warranty whatsoever, and Fortinet disclaims any warranty or liability whatsoever. An end user's use of evaluation or beta Software or Product is limited to thirty (30) days from original shipment unless otherwise agreed in writing by Fortinet. For clarity, notwithstanding anything to the contrary, all sales are final and no provision in this EULA entitles you to return Products, other than as expressly set forth herein.

#### 8. Governing Law.

Any disputes arising out of this Agreement or Fortinet's limited warranty shall be governed by the laws of the state of California, without regard to the conflict of laws principles. In the event of any disputes arising out of this Agreement or Fortinet's limited warranty, the parties submit to the jurisdiction of the federal and state courts located in Santa Clara County, California, as applicable, and agree that any controversy or claim arising out of or relating to this Agreement shall be determined in the federal and state courts located in Santa Clara County, California, as applicable.

#### 9. Limitation of Liability.

TO THE MAXIMUM EXTENT PERMITTED BY LAW AND NOTWITHSTANDING ANYTHING TO THE CONTRARY, FORTINET IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY, INFRINGEMENT OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT OR SERVICE OR ANY DAMAGES OF ANY KIND WHATSOEVER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF PROFIT, LOSS OF OPPORTUNITY, LOSS OR DAMAGE RELATED TO USE OF THE PRODUCT OR SERVICE IN CONNECTION WITH HIGH RISK ACTIVITIES, DE-INSTALLATION AND INSTALLATION FEES AND COSTS, DAMAGE TO PERSONAL OR REAL PROPERTY, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, COMPUTER SECURITY BREACH, COMPUTER VIRUS INFECTION, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT INCLUDING ANY PRODUCT RETURNED TO FORTINET FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THE LIMITED WARRANTY IN SECTION 6 ABOVE, EVEN IF FORTINET HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE LIMITED WARRANTY IS, AT FORTINET'S SOLE AND ABSOLUTE DISCRETION: REPAIR, REPLACEMENT, OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT AS SPECIFICALLY STATED IN SECTION 6 ABOVE; PROVIDED, HOWEVER, IN NO EVENT SHALL ANY END-CUSTOMER REMEDIES UNDER THIS EULA AND ANY SUPPORT AGREEMENT EXCEED THE AMOUNT PAID TO FORTINET FOR THE SPECIFIC APPLICABLE DEFECTIVE OR NON-CONFORMING PRODUCT AT ISSUE.

#### 10. Compliance with Laws, including Import/Export Laws and FCPA.

You are advised that the Products may be subject to the United States Export Administration Regulations and other import and export laws and regulations known to United States law and regulation is prohibited. You agree to comply with all applicable international and national laws that apply to the Products as well as end user, end-use, and destination restrictions issued by U.S. and other governments. For additional information on U.S. export controls see <https://www.bis.doc.gov>. Fortinet assumes no responsibility or liability for your failure to obtain any necessary import and export approvals and licenses, and Fortinet reserves the right to terminate or suspend shipments, services and support in the event Fortinet has a reasonable basis to suspect any import or export violation. You represent that neither the United States Bureau of Industry and Security nor any other governmental agency has issued sanctions against you or otherwise suspended, revoked or denied your export privileges. You agree not to use or transfer the Products for any use relating to nuclear, chemical or biological weapons, or missile technology, unless authorized by the United States Government by

regulation or specific written license. Additionally, you agree not to directly or indirectly export, import or transmit the Products contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or use. Furthermore, you hereby agree that, for any orders that you place with Fortinet whereby any legal or regulatory requirements may apply to Fortinet such as requirements related to the International Traffic in Arms Regulations, or Buy American Act, or the Trade Agreements Act: you are responsible to ensure the Purchase Order submitted to Fortinet by you and/or any partners clearly states the specific requirement in writing, or otherwise Fortinet is not bound by any such requirements. You represent that you understand, and you hereby agree to comply with, all applicable laws including but not limited to the U.S. Foreign Corrupt Practices Act. You represent that you hereby agree that you and your employees have not accepted, and will not accept, anything of value, including money, meals, entertainment, paid-for travel, beta, testing, evaluation, donation or free Products and/or related services, or anything else of value, in exchange for Fortinet maintaining current business or for new business opportunities. You represent and warrant to Fortinet that you and your employees, consultants, agents and representatives will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving censorship, surveillance, detention, or excessive use of force. You agree you and your employees will be responsible to comply in full with all laws and policies applicable to any and all dealings with Fortinet in general and its distributors, resellers and partners.

#### 11. U.S. Government End Users.

The Software and accompanying documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement and its successors.

#### 12. Tax Liability.

You agree to be responsible for payment of any sales or use taxes imposed at any time on this transaction.

#### 13. General Provisions.

Except as specifically permitted and required in section 5 ("Transfer") above, you agree not to assign this Agreement or transfer any of the rights or obligations under this Agreement without the prior written consent of Fortinet. This Agreement shall be binding upon, and inure to the benefit of, the successors and permitted assigns of the parties. The United Nations Convention on Contracts for the International Sales of Goods is expressly excluded. This Agreement and other Fortinet Agreements may be amended or supplemented only by a writing that refers explicitly to the agreement signed on behalf of both parties, or, for this Agreement, as otherwise expressly provided in the lead-in above Section 1 above, provided, notwithstanding anything to the contrary and except for this Agreement which may be amended or updated as expressly provided in the lead-in above Section 1 above, for any amendment or other agreement to be binding on Fortinet, such amendment or other agreement must be signed by Fortinet's General Counsel. No waiver will be implied from conduct or failure to enforce rights nor effective unless in a writing signed on behalf of the party against whom the waiver is asserted. If any part of this Agreement is found unenforceable, that part will be enforced to the maximum extent permitted and the remainder shall continue in full force and effect. You acknowledge that you have read this Agreement, understand it, and agree to be bound by its terms and conditions. Notwithstanding anything to the contrary, this EULA constitutes the entire agreement between Fortinet and its end-customers and supersedes any and all prior representations or conflicting provisions, such as limitations of liability, warranties, or otherwise in any and all purported end customer agreements, whether entered into now or in the future. In the event of a conflict between this EULA and another agreement, this EULA shall prevail unless the conflicting agreement expressly states that it replaces this EULA, expressly referring to this EULA, and is agreed to in writing by authorized representatives of the parties (which, in the case of Fortinet, is Fortinet's General Counsel).

#### 14. Privacy.

You agree to Fortinet's collection, use, disclosure, protection and transfer of your information, as set forth in the Fortinet privacy policy on the Fortinet web site (<http://www.fortinet.com/about-us/privacy.html>), including (a) Fortinet's use of the Customer information to send information regarding Fortinet products and services; and (b) Fortinet's disclosure of your information to provide assistance to law enforcement, governmental agencies and other authorities or to allow Fortinet to protect its Customers' and/or end users' rights.

#### 15. Open Source Software.

Fortinet's products may include software modules that are licensed (or sublicensed) to the user under the GNU General Public License, Version 2, of June 1991 ("GPL") or GNU Lesser General Public License, Version 2.1, of February 1999 ("LGPL") or other open source software licenses which, among other rights, permit the user to use, copy, modify and redistribute modules, or portions thereof, and may also require attribution disclosures and access to the source code ("Open Source Software"). The GPL requires that for any Open Source Software covered under the GPL, which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any Open Source Software covered under the GPL, the source code is made available on this CD or download package. If any Open Source Software licenses require that Fortinet provide rights to use, copy or modify any Open Source Software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein. Fortinet will provide, for a charge reflecting our standard distribution costs, the complete machine-readable copy of the modified software modules. To obtain a complete machine-readable copy, please send your written request, along with a check in the amount of US \$25.00, to General Public License Source Code Request, Fortinet, Inc., 899 Kifer Rd, Sunnyvale, CA 94086 USA. To receive the modified software modules, you must also include the following information: (i) Name, (b) Address, (c) Telephone number, (d) E-mail Address, (e) Product purchased (if applicable), (f) Product Serial Number (if applicable). All open source software modules are licensed free of charge. There is no warranty for these modules, to the extent permitted by applicable law. The copyright holders provide these software modules "AS-IS" without warranty of any kind, either expressed or implied. In no event will the copyright holder for the open source software be liable to you for damages, including any special, incidental or consequential damages arising out of the use or inability to use the software modules, even if such holder has been advised of the possibility of such damages. A full copy of this license, including additional open source software license disclosures and third party license disclosures applicable to certain Fortinet products, may be obtained by contacting Fortinet's Legal Department at [legal@fortinet.com](mailto:legal@fortinet.com).



## GNU GENERAL PUBLIC LICENSE GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation,  
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law; that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this license; they are outside its scope. The act of running the Program (not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or, else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

Source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

### NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REPRODUCE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.  
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law; that is to say, a "work containing the Library" or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- The modified work must itself be a software library.
- You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

c) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2 instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not.

Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code may plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for your own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

15. The warranty disclaimer contained in Sections 11 and 12 of the preceding GPL License is incorporated herein.

**Fortinet Service Terms & Conditions**  
**For FortiCare, FortiGuard and other Fortinet Service Offerings**

---

THESE TERMS AND CONDITIONS APPLY TO THE PROVISION OF SERVICES BY FORTINET AND EXCLUSIVELY GOVERN THE LEGAL RELATIONSHIP BETWEEN YOU (THE "CUSTOMER") AND FORTINET. IT SETS FORTH THE LEGALLY BINDING RIGHTS AND OBLIGATIONS OF THE CUSTOMER IN RELATION TO FORTICARE SUPPORT OR FORTIGUARD SUBSCRIPTION SERVICES OR OTHER FORTINET SERVICE OFFERINGS. THE CUSTOMER CONSENTS TO BE BOUND BY THESE TERMS AND CONDITIONS (THE "AGREEMENT"). THE CUSTOMER REPRESENTS THAT IT IS A SOPHISTICATED ENTITY, THAT HAS READ AND UNDERSTANDS THIS AGREEMENT AND HAS HAD SUFFICIENT OPPORTUNITY TO CONSULT WITH COUNSEL BEFORE AGREEING TO THE TERMS HEREIN. IF THE CUSTOMER DOES NOT AGREE TO THE TERMS, THE CUSTOMER SHOULD NOT ACCEPT THE AGREEMENT AND SHOULD CONTACT [LEGAL@FORTINET.COM](mailto:LEGAL@FORTINET.COM) TO REQUEST CHANGES TO THE AGREEMENT. THE CUSTOMER AGREES THAT ANY OF THE FOLLOWING ACTIONS BY CUSTOMER REPRESENTATIVES REPRESENT THE CUSTOMER'S AUTHORIZED CONSENT TO BE BOUND BY THIS AGREEMENT: (I) RECEIVING, DOWNLOADING, DEPLOYING OR USING ANY SOFTWARE PROVIDED IN CONNECTION WITH FORTINET SERVICES, (II) RECEIVING, CONFIGURING, LOGGING IN, REGISTERING OR OTHERWISE USING OR BENEFITTING FROM THE SERVICES, OR (III) BY CLICKING ON THE "ACCEPT" BUTTON UPON REGISTRATION (ANY OF (I), (II), OR (III) SHALL CONSTITUTE "ACCEPTANCE" BY CUSTOMER). THE CUSTOMER HEREBY ACKNOWLEDGES AND AGREES THAT THE PERSON ENGAGING IN (I), (II), AND/OR (III) IS AUTHORIZED TO BIND THE CUSTOMER TO THE TERMS HEREIN. FOR CLARITY, NOTWITHSTANDING ANYTHING TO THE CONTRARY, IF CUSTOMER IS USING AN AUTOREGISTRATION TOOL OR HAS ENGAGED A FORTIPARTNER OR FORTINET TO REGISTER THE SERVICE CONTRACT ON ITS BEHALF, CUSTOMER ACKNOWLEDGES AND AGREES THAT ANY AND ALL UNITS REGISTERED USING SUCH TOOL SHALL BE SUBJECT TO THIS AGREEMENT.

Services are available independently or in connection with the purchase of Fortinet's commercial networking products and related equipment, including Hardware products with embedded Software, and stand-alone Software products sold and licensed to Customer pursuant to Fortinet's End User License Agreement ("EULA"), which EULA is available at <https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf>, and Customer hereby agrees to the terms of the EULA.

This Agreement constitutes a legal agreement between the parties with respect to FortiCare and FortiGuard Subscription services or other Services, and shall supersede all prior representations, discussions, negotiations and agreements, whether written or oral. Notwithstanding anything to the contrary, Fortinet is only bound by, and Customer is only entitled to, services pursuant to official service descriptions that are authorized by Fortinet pursuant to this Agreement and are contractually binding on Fortinet pursuant to the terms herein

**1. DEFINITIONS**

1.1. *"Active Service Coverage Level"* means the level of Technical Support as purchased by Customer pursuant to a Service Contract and defined in the applicable service description.

1.2. *"Customer"* means any entity or person that has purchased a Service Contract for use within their business and not for further sale.

1.3. *"Customer Service"* means a function and associated ticket type within TAC handling mainly non-technical queries and registration issues.

1.4. *"Documentation"* means any customer support manuals, technical manuals, and/or "Help" files within the Services that relate to the Services and that Fortinet makes available to Customer in connection with this Agreement and/or through the Services.

1.5. *"Enterprise Agreement Program"* means account based Service as described in applicable service description and, pursuant to this Agreement, that provides multiple Service Contracts through prior agreement and subsequent purchase.

1.6. *"FortiCare"* means a time-based subscription to Technical Support Services, as defined in the applicable service description, which may be purchased by Customer directly or from a third party, and which are delivered by Fortinet on behalf of that third party.

1.7. *"Fortinet"* means Fortinet, Inc.

1.8. *"FortiPartner"* means a Fortinet authorized distributor or reseller of Fortinet Products and Services.

1.9. *"Hardware"* means a Fortinet appliance or chassis, excluding all software incorporated or bundled with such devices.

1.10. *"Product Bundle"* means Product sold with defined Services.

1.11. *"Product"* means any Hardware with associated Software including Product Bundles, or stand-alone Software which is available for sale through a FortiPartner or directly from Fortinet and is covered by a Service Contract.

1.12. *"Registration Date"* means the date the Product or Service Contract or Renewal Service Contract is registered in the Support Portal. Service activation takes place on registration of the Service Contract subject to Fortinet's then-current Service start policy.

1.13. *"Renewal Service Contract"* means the continuation of a Service Contract pursuant to the terms of the Service Contract.

1.14. *"Serial Number"* means the unique identifier of a Product which may be registered in the Support Portal.

1.15. *"Service(s)"* when used individually means a subscription to one of Fortinet's service offerings (FortiCare,

FortiGuard, etc.) or in plural when generally referring to Fortinet's service offering, which may be purchased by the Customer directly or from a third party.

1.16. *"Service Contract"* means a time-limited subscription to Technical Support or other Services registered subject to this Agreement, provided pursuant to Fortinet's standard Service offering as defined in Fortinet's official applicable service description or pursuant to Fortinet's standard service practices.

1.17. *"Software"* means Fortinet computer software, Fortinet software subscription services and bug fixes, in each case provided by Fortinet either directly or from FortiPartner, whether purchased as embedded within the Hardware or as a standalone software product or operating software release or update service.

1.18. *"Support Portal"* means an on-line service portal designed to allow Customers to register and access their applicable purchased Services. For example, the Support Portal can be used to create Technical Tickets, access documentation, and obtain software releases. The Support Portal is available at <https://support.fortinet.com> or, for FortiPartners at <https://partnerportal.fortinet.com>.

1.19. *"TAC"* means Fortinet's technical assistance center which is comprised of a number of technical support centers.

1.20. *"Technical Support"* means the provision of technical support assistance to resolve issues related to Products and Services.

1.21. *"Technical Ticket"* means a Customer's request for Technical Support under a Service Contract, whereby Customer will provide a suitable description of the reason why Customer is seeking Technical Support and all technical details to allow Fortinet's support team to investigate Customer's request.

1.22. *"Upgrade Service Contract"* means a Service Contract which provides or amends an existing Service Contract with an additional service entitlement.

## 2. FORTICARE

2.1. Upon activation of a FortiCare Service Contract and pursuant to Active Service Coverage Level applicable to the Product, the Customer will obtain the following entitlements to the extent within the scope of its Service Contract: (a) access to the Support Portal; (b) access to the TAC for Customer Service assistance as well as resolution of Technical Tickets; (c) access to Software updates (maintenance and feature releases) exclusively for the Products covered by the FortiCare Service Contract; and (d) the replacement of Hardware determined by Fortinet to be defective exclusively for the Hardware covered by the FortiCare Service Contract. For more details refer to the FortiCare Technical Support Service and Fortinet's policies.

### *Technical Support*

2.2. Pursuant to Active Service Coverage Level, Fortinet shall provide Customer the following entitlements to the extent within the scope of Customer's Service Contract:

2.2.1. Assistance by telephone or via the Support Portal or via web-chat in relation to troubleshooting of Product technical issues, as well as usage and configuration.

2.2.2. 24x7 access to the TAC.

2.2.3. Access to the Support Portal for the Customer to create Technical Tickets, manage Product and Service assets, obtain Software updates exclusively for the Products covered by the FortiCare Service Contract, as well as providing access to Documentation including trouble-shooting information. Technical Tickets shall be processed by Fortinet in accordance with Sections 2.2.4 and 2.2.5.

2.2.4. Processing of Technical Tickets in accordance with the Technical Support procedures and support day/time limitations outlined in Fortinet's official applicable FortiCare service documents.

2.2.5. On a commercially-reasonable basis, provide acceptable workaround solutions, resolutions or Software maintenance releases to resolve Technical Tickets. The Customer acknowledges that Software and/or Hardware are never error-free and that, despite commercially-reasonable efforts, Fortinet may be unable to provide answers to, or be unable to resolve, some requests for Software or Hardware support.

2.2.6. Maintenance releases and feature updates for Software. Customer may access such updates via password-protected web access. This is subject to one copy per Software release or signature file as appropriate and is subject to the EULA and exclusively for the Products covered by the FortiCare Service Contract.

2.2.7. Where Hardware replacement is deemed necessary by Fortinet, and within scope of the Service Contract, Fortinet shall provide Hardware replacement services, using commercially-reasonable efforts, in accordance with the Active Service Coverage Level.

### *Hardware Replacement*

2.3. Hardware replacements are shipped to the Customer with incoterm DAP (Delivery At Place) using a Fortinet carrier, freight prepaid by Fortinet, excluding any import duties, taxes or other fees.

2.4. Hardware replacement Service is subject to geographical restrictions.

2.5. Fortinet is not responsible for transportation or custom delays. Customer compliance with export controls and destination customs processes may condition shipment times.

### *Product Life Cycle*

2.6. The type of Technical Support provided under FortiCare may vary depending on the Product's life cycle. An up-to-date version of the Product life cycle shall either be stored on the Support Portal or available by contacting Fortinet.



2.7. For any Software that is in the “End of Support” phase, as defined in Fortinet’s then-active Product life cycle policy, Fortinet may provide Technical Support for Software issues at its sole discretion. Such Support Services are limited to advisory support and do not include new Software releases to address Software defects unless otherwise stated in the Active Service Coverage Level.

#### *Exclusions*

2.8. Fortinet shall have no obligation to provide Technical Support under FortiCare in any of the following circumstances:

- FortiCare does not include any on-site activity, or any request for step-by-step installation and configuration of a Product or creation of custom SQL reports. Professional services may be available for purchase by Customer to provide such services.
- In the event the Customer alters, damages or modifies the Product or any portion thereof.
- For any problem caused by: accident; transportation; neglect, abuse, misapplication, or misuse; alteration, modification, or enhancement of the Product; failure to provide a suitable installation environment for the Product; use of supplies or materials not meeting Product specifications; use of the Product for other than the specific purposes for which the Product is designed.
- For the Product that is used on any systems other than the specified hardware platform for such Product as described in the Product’s then-current specifications. Fortinet shall have no liability for any changes in the Customer’s hardware, which may be necessary to use the Product due to a workaround or maintenance release.
- For any Hardware that is in the “End of Support” phase, as defined in Fortinet’s then active Product life cycle policy unless otherwise stated in the Active Service Coverage Level.
- For any Product that has not been publicly released.
- For third-party devices (including, without limitation, hardware, software, infrastructure such as cabling) or problems associated with such elements.
- Any usage of FortiGuard service updates that are not specifically authorized by Fortinet in writing including, without limitation, accessing signature packages for the purpose of duplication. For clarity, FortiGuard service updates are only provided for the Product that is covered by a FortiGuard Service Contract.
- For issues related to hardware consumables, which may be physically installed within a Fortinet appliance, such as SFPs, SDD cards and hard disks, if these are not Hardware and as a result of a technical analysis a fault or defect is traced to the use of non-Fortinet supplied hardware.
- For any other violation by Customer of this Agreement.

#### *Customer Obligations*

Customer is obligated and responsible for the following, and Fortinet’s responsibilities and obligations shall be subject in full to Customer meeting its following obligations:

2.9. Properly activate and register Service Contracts and proper inclusion in such activation and registration the correct and full Customer name and location who is the beneficiary of such Support Contract against a specified Product unit or Support Portal account. Customer acknowledges that the Agreement applies in full when the registration of the Products and Services is made by the Customer indirectly through a FortiPartner or Fortinet Customer Services. For all Service Contracts provided as part of the Enterprise Agreement Program, Fortinet will automatically register such Service Contracts and the effective date will be as communicated by Fortinet to the Customer.

2.10. Ensure that the Product covered by FortiCare Service Contract is used for its intended purpose and in line with the applicable Product specifications and is maintained in accordance with applicable Product documentation.

2.11. Maintain Software at the current Software release and upgrade to the latest release of Software if it is required to resolve a reported technical issue.

2.12. Comply with Fortinet’s Technical Support recommendations.

2.13. Provide access at Customer’s expense to the Product in order for Fortinet to troubleshoot a Technical Ticket, subject to the Customer and Fortinet agreeing on appropriate security measures to prevent unauthorized access to Customer’s network, provided, however, the ultimate responsibility for the security of the network lies with the Customer. Fortinet will not connect to the Customer’s network without prior authorization and such connection will be solely to provide Technical Support. Customer has the right to monitor such access by Fortinet. Where (a) the Customer causes delay in providing connectivity in accordance with this section or (b) Customer and Fortinet cannot agree on appropriate security measures to prevent unauthorized access to Customer’s network in the performance of Technical Support, Fortinet will be excused from any damages or other losses attributable to such delay or lack of agreement.

2.14. Cooperate in full with Fortinet, provide Fortinet all relevant information, and make available knowledgeable technical staff to aid in troubleshooting.

2.15. Return the Hardware unit within 30 days of the receipt of a replacement Hardware following Fortinet’s specifications for packaging and labeling of the returned Hardware unit, assume all costs associated with returning the Hardware unit and provide insurance for all returned Hardware equipment. For clarity, Hardware returns that are improperly packaged will not be accepted by Fortinet and returned at the Customer’s expense.

2.16. Ensure Service Contracts are transferred to any replacement Products. Customer acknowledges that this action is required to continue to receive FortiCare Services and accepts that there may be a delay of up to four hours to re-establish FortiGuard security services.

2.17. Maintaining reasonable internal security policies and processes, such as related to internal passwords, its facilities, its administrator access to information and systems, and use of wireless access points.

2.18. Ensure Customer does not share any Customer, Customer employee, or any third party sensitive, confidential, or private information with Fortinet, except as permitted and to the extent necessary for Fortinet to meet its obligations under this Agreement, and, in the event such is shared, with clear notice to Fortinet of proper handling requirements for, and sensitivity of, such information.

### 3. FORTIGUARD

3.1. FortiGuard is a Service that provides a threat research feed under which Fortinet undertakes commercially-reasonable efforts to provide solutions to identified network security threats. These are developed in response to evolving internet activity and delivered via security threat databases, produced by machine intelligence and experts.

3.2. Customer is responsible for configuring the frequency of FortiGuard security updates, which may be available on either an automatic or manual basis.

3.3. The creation of Technical Tickets for issues related to FortiGuard requires an active FortiCare Service Contract covering the FortiGuard service.

### 4. EVALUATIONS.

For registration of FortiGate-VM licenses for evaluation, and any other Software that Fortinet makes available for evaluation (together "Evaluation Software"), please be advised that the following terms apply:

4.1. All Evaluation Software is licensed pursuant to the EULA referenced above.

4.2. Fortinet makes available a limited, revocable license to Evaluation Software solely for the purpose of testing and evaluation, and not for commercial use or use in production environments. Fortinet disclaims liability and shall not be responsible for the Customer's use of Evaluation Software in production environments.

4.3. Unless otherwise noted on the Evaluation Software entitlement, the Evaluation Software license is limited to sixty (60) days from the start date provided by Fortinet ("Term"). The Customer must cease use of the Evaluation Software upon expiration of the Term. At Fortinet's discretion, a new Software license may be provided for additional Evaluation.

4.4. Fortinet retains all right, title, and interest in the Evaluation Software and all materials delivered in connection with such Evaluation Software, including without limitation, all changes and improvements made, requested, or suggested by Customer. All results of this evaluation and any feedback shall be deemed to be confidential information and trade secrets of Fortinet, and may not be disclosed by Customer to any third party without

Fortinet's written consent. At Fortinet's request, Customer shall provide to Fortinet any results of the Evaluation.

4.5. Customer also hereby affirms that Customer will comply fully with all relevant import and export laws and regulations of the United States and any other country ("Export Laws") with respect to any use of Confidential Information including but not limited to export, re-export, ship, transfer to an embargoed country or other sanction by the United States namely Cuba, Iran, N. Korea, Syria, Sudan and the Crimea Region of Ukraine are prohibited; that Customer is allowed to legally conduct business with Fortinet, and you are not on any United States government restricted lists (such as the Denied Persons List, Entity List, Unverified List, or Consolidated Screening List) or similar lists from any government that may restrict your ability to legally conduct business with Fortinet.

### 5. FEES, TERMS, AND TERMINATION

5.1. Ordering and use. Each Service is covered individually by this Agreement, and expires in accordance with the terms contained in this Agreement or according to Fortinet's policies and the term of the Service Contract. Accordingly, where this Agreement (including Service Contracts) terminates for a particular Service as related to a particular unit of Product or to a Support Portal account(s), the Agreement remains in full force and effect individually for any proper Service being provided related to any other Product unit or to other Support Portal account(s). Service Contracts may apply only to a single unit of Product or Support Portal account(s) as described in the relevant service description. An attempt to use a Service Contract with more than one unit of Product, (i.e. in addition to the unit of Product for which the Service Contract was originally purchased and registered) or with more than the designated Support Portal account(s), is considered a material breach of the Service Contract and will result in the termination of such Service Contract without refund of any fees paid by Customer and additional fees will be immediately due by Customer to Fortinet based on Fortinet's then-current list price for any incremental, additional Services beyond those authorized by the Service Contract.

5.2. Payment Terms. By purchasing Services directly or indirectly through a FortiPartner as the case may be, Customer agrees to pay the purchase price for the Services, and all sales, use, valued-added and other taxes and all customs duties and tariffs now or hereafter claimed or imposed by any governmental authority upon the sale of the Services. Where purchasing from Fortinet all payments shall be due upon purchase, in U.S. Dollars, and free of any currency control or other restrictions. All sales are final and the Services are not returnable.

5.3. Registration and renewal registration. Customer must register, directly or indirectly through a FortiPartner or Fortinet Customer Services, the standalone 'Service Contract Registration Number' which references the purchased standalone Service, within three hundred sixty-five (365) days from the date of the original shipment by

Fortinet of the Service Contract to its FortiPartner or Customer, whichever originally purchased directly from Fortinet. Customer is fully responsible to ensure complete and accurate information is included in the registration of the Service Contract. ANY STANDALONE SERVICE CONTRACTS WHICH ARE NOT REGISTERED WITHIN THREE HUNDRED SIXTY-FIVE (365) DAYS FROM THE DATE THE SERVICE CONTRACT WAS ORIGINALLY SHIPPED FROM FORTINET SHALL BE FORFEITED AND FORTINET SHALL HAVE NO OBLIGATION TO THE CUSTOMER REGARDING THIS AGREEMENT OR ANY RELATED SUPPORT SERVICES. It is the Customer's responsibility to register the Service Contract within the three hundred sixty-five (365) day period and to understand the original ship date from the party from which the Customer purchased the Product. In the case of Product Bundle, the Services begin in accordance with the Service activation policies set forth at: <https://www.fortinet.com/corporate/about-us/legal> under heading 7. For all Service Contracts provided as part of the Enterprise Agreement Program, Fortinet will automatically register such Service Contracts and the effective date will be as communicated by Fortinet and accepted by the Customer on receipt of purchase order therefore section 5.3 will not apply.

5.4. Notwithstanding anything to the contrary, Fortinet may register any Renewal Service Contract, or Upgrade Service Contract upon invoicing. Upon renewal of the Service Contract, Customer authorizes Fortinet to automatically register the Renewal Service Contract for subsequent renewal periods for which a purchase order has been placed. For clarity, registration is the responsibility of the Customer and Fortinet is not obliged to register the Renewal Service Contract or the Upgrade Service Contract.

5.5. In order to maintain a continuous service period, the effective date of any Renewal Service Contract shall begin the next calendar day following the expiration date of the previous Service Contract. In the event that registration of a Renewal Service Contract is beyond one hundred eighty (180) calendar days following the expiration date of the previous Service Contract, such Renewal Service Contract effective start date will be the date that is one hundred eighty (180) calendar days prior to the actual Registration Date of the Renewal Service Contract.

5.6. Term and Termination. Subject to the other provisions herein, this Agreement is valid for the length of time provided for in the Customer's purchased Service Contract which is viewable upon activation in the applicable Support Portal and which starts from (a) the Registration Date of the Service Contract or in the case of a Product Bundle the Registration Date of the Product; or (b) in the event of a Renewal Service Contract that has been registered prior to the expiration date of the previous Service Contract, starting from the calendar day following the expiration date of the previous Service Contract; or (c) in the event of a Renewal Service Contract that has not been registered prior to the expiration of the previous Service Contract, starting from the actual Registration Date of the Renewal Service Contract with the applicable term being amended based on the effective start date as described in section 5.5; or (d) the applicable start date as communicated by Fortinet in

respect of Services provided under the Enterprise Agreement Program. To the extent the Services experience any interruption due to Customer's failure to register a Renewal Service Contract, Fortinet shall not be responsible for providing Services during such interruption and will not be responsible for any losses or damages incurred by Customer or any third party attributable to this interruption in Services.

5.7. Fortinet reserves the right to terminate this Agreement and/or any and all Services being provided hereunder, in its discretion, in the event of (a) breach of any terms herein by Customer, (b) breach of any of the terms of the EULA; (c) transfer of the unit of Product to a third party, (d) use of the Support Contract for other Products than the entitled Product, or (e) non-payment to Fortinet or to its FortiPartner for any Services by the Customer or a third party, with such termination having immediate effect, if such breach has not been cured within fifteen (15) calendar days after written notice by Fortinet to Customer or immediately upon notice of termination in the event of a breach that by its nature cannot be remedied within fifteen (15) calendar days. Fortinet may also terminate this Agreement without notice if Customer becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors. Upon any termination, Fortinet shall have no obligation to provide the Services hereunder.

5.8. Third-party providers. Fortinet reserves the right to subcontract its obligations herein to third-party organizations. Fortinet also reserves the right to change service subcontractors without notice.

5.9. Non-Fortinet Support. To the extent Customer provides its own technical support or engages a non-approved third party to provide technical support, Fortinet is not responsible for such support, and Customer represents and warrants that all such technical support pursuant to Section 5.9 shall be performed in a satisfactory and commercially reasonable manner and will not infringe upon Fortinet's rights or the rights of any third party. Fortinet shall be relieved of its Technical Support obligations to the extent Customer's actions interfere with Fortinet's ability to meet its service obligations under the Active Service Coverage Level.

5.10. Service Description; Updates. A description of the various Services is available on the Fortinet website, and on the applicable services portal. In its sole discretion Fortinet may make updates to its Service offerings from time to time. If Fortinet makes a material change to the Services, those changes will be reflected in the on-line service descriptions stored on the applicable portal. Fortinet may also make changes to this Agreement, including any linked documents, from time to time. Unless otherwise noted by Fortinet, material changes to the Agreement will become effective thirty (30) days after they are posted, except if the changes apply to new Service functionality in which case they will be effective immediately. If Customer does not agree to the revised Agreement, Customer must stop using the Services and promptly notify Fortinet in writing. In no event shall Fortinet be obligated to refund Customer or FortiPartners, any amounts previously paid.

5.11. Service/support portal access and security. As part of the Services, Customer may receive administrative access ID's and passwords upon installation, registration. Customer shall be solely responsible for maintaining the security of its administration access information, and shall be fully responsible for, all activities which occur, relating to access to the Services under Customer's administrative access ID. Fortinet is not responsible for unexpected use of Services or data whether by ex-employees, compromised user passwords or any other misuse of Customer accounts. Upon termination of the Services, all data, including configuration data will be deleted, and Fortinet has no responsibility for such data.

5.12. Loss of data and accuracy of data. While Fortinet takes commercially reasonable and industry standard technical and organizational steps to ensure the security of the Services, it is not responsible for the accidental loss or destruction of any data any End User transmits using the applicable Service and Fortinet disclaims all liability of any kind in relation to the content or security of data that any End User sends or receives through the Service. Further, Fortinet does not guaranty the accuracy of the reports, which may be compromised by various network incidents that impact data collection and accuracy (e.g. network outages, hardware upgrades, and the like), and in no event does Fortinet guarantee security or privacy of the Customer's network or assets.

## 6. PRIVACY

6.1. Customer hereby consents to Fortinet's collection, use, protection and transfer of Customer's information as described in the Fortinet Privacy Policy on the Fortinet web site (<http://www.fortinet.com/aboutus/privacy.html>).

6.2. Customer consent and privacy. Fortinet recommends, and (where required by law) requires, the posting of legally sufficient notices to data subjects, consumers and other relevant individuals ("End Users") regarding the collection of End User data through the Services. IT IS CUSTOMER'S SOLE OBLIGATION TO COMPLY WITH ALL NATIONAL AND LOCAL LAWS REGARDING CONSUMER DATA PRIVACY AND PRIVACY DISCLOSURE LAWS.

6.3. Customer agrees and acknowledges, and warrants that it is responsible to ensure that all End Users agree and acknowledge, that Fortinet may be required by law to provide assistance to law enforcement, governmental agencies and other authorities. Accordingly, Customer agrees and shall procure that all End Users agree that:

6.3.1. Fortinet may implement and maintain an interception capability suitable to meet these regulatory requirements where Fortinet and/or FortiPartners are obliged by law to ensure or procure that such a capability is implemented and maintained;

6.3.2. Fortinet may implement and maintain a data retention capability for the Service to meet regulatory requirements where Fortinet and/or its FortiPartners are obliged by law to ensure or procure that data is retained; and

6.3.3. Fortinet may at times cooperate with law enforcement authorities and rights-holders in the investigation of any suspected or alleged illegal activity by Customer or End Users. If Fortinet is required to do so by law, this may include but is not limited to, disclosure of the Customer's or End Users' contact information to law enforcement authorities or rights-holders.

6.4. To the extent Customer receives administrative access IDs and passwords in connection with any accounts for the Services, Customer shall be solely responsible for maintaining its security, and shall be fully responsible for all activities which occur relating to access to the Services and use of any other features (including wireless access point(s), as applicable) under that administrative access ID and passwords. Customer agrees to notify Fortinet immediately of any actual or suspected unauthorized use of Customer's account or any other breach of security known by Customer.

6.5. Although some of our Services may provide certain notices or may seek certain consents from certain End Users, Fortinet does not provide legal advice, and Customer remains solely responsible and solely liable for independently (i) determining what notices and consents are legally required and (ii) providing such notices and obtaining such consents.

## 7. SOFTWARE RESTRICTIONS

7.1. Customer hereby agrees to the software restrictions in Fortinet's EULA and further agrees (i) not to or not to attempt to reverse engineer, disassemble, decompile or otherwise access, obtain or modify the source code, internal structure, Hardware design or organization of the Product or support updates or Software, or any part thereof, or to aid or to permit others to do so, except and only to the extent as expressly required by applicable law; (ii) not to remove any identification or notices of any proprietary or copyright restrictions from any Product or support updates or Software; (iii) not to copy the Product or support updates or Software, modify, translate or, unless otherwise agreed, develop any derivative works thereof or include any portion of the Software in any other software program; (iv) only to use the Product and support updates and Software for internal business purposes and in accordance with then active specification, and (v) to keep confidential any Software and support updates and not share them with third parties.

## 8. INDEMNIFICATION

8.1. Customer will defend Fortinet against any claim, demand, suit or proceeding made or brought against Fortinet by a third party arising out of Customer's breach of this Agreement, any infringement or misappropriation of intellectual property rights caused by Customer (whether or not Customer has concurrently violated this Agreement), or any illegality of Customer data (individually and collectively, a "Claim"), and will indemnify Fortinet from any damages, attorney fees and costs finally awarded against Fortinet as a result of, or for any amounts paid by Fortinet under a



settlement of, a Claim, provided Fortinet promptly gives Customer written notice of the Claim (provided that failure to so notify will not remove Customer's obligation except to the extent Customer is materially prejudiced thereby). For a Claim, Customer controls the defense and settlement of the Claim and Fortinet agrees to give Customer all reasonable assistance, at Customer's expense. Customer will not settle, compromise, or otherwise enter into any agreement regarding the disposition of any Claim without the prior written consent and approval of Fortinet unless such settlement (a) is solely for a cash payment, (b) requires no admission of liability or wrongdoing on the part of Fortinet, (c) imposes no obligation on Fortinet, (d) imposes no restriction on Fortinet's business, (e) provides that the parties to such settlement shall keep the terms of the settlement confidential, and (f) provides for a full and complete release of Fortinet. Customer shall reimburse Fortinet within 30 calendar days after demand for any losses incurred by Fortinet that is subject to an indemnification obligation as set forth in this Section.

## **9. WARRANTY**

9.1. Service Warranties. Fortinet provides its Services and Products on an "AS IS" basis. Neither Fortinet nor any of its officers, directors, employees, partners or agents, makes any representation, claim or warranty with respect to the Services or reports or data, whether express or implied, including without limitation, any warranty of quality, performance, non-infringement, merchantability, or fitness for a particular purpose, or any results generated from use of the Services or the reports. Fortinet makes no warranty that the Services will meet Customer's requirements, or that the Services will be uninterrupted, timely, or secure.

9.2. Fortinet will have no obligation to correct, and makes no warranty with respect to, errors caused by: (a) improper installation of the Software or Hardware; (b) changes that Customer has made to the Software or Hardware; (c) use of the Software or Hardware in a manner inconsistent with the documentation and instructions; (d) the combination of the Software or Hardware with hardware or software not approved by Fortinet; (e) malfunction, modification or relocation of Customer's Hardware or Software transferred to unapproved or unregistered devices; (f) Customer failure to use the Software and Services in accordance with local laws; or (g) business and/or service decisions based on reliance on the analysis or data aggregation results.

9.3. Product Warranties. The warranty limitations, restrictions on Customer and protections for Fortinet as contained in Fortinet's EULA are applicable. Except as expressly stated in its EULA, Fortinet does not provide any warranty whatsoever and nothing in this Agreement shall be construed as expanding or adding to the warranty set forth in the EULA. In the event of a conflict between this Agreement and the EULA, the EULA shall govern. Fortinet cannot guarantee that every question or problem raised in connection with the Services will be addressed or resolved, and in no event does Fortinet warrant or guaranty security and protection from all threats. EXCEPT FOR WARRANTIES CLEARLY AND EXPRESSLY STATED HEREIN,

NOTWITHSTANDING ANYTHING TO THE CONTRARY, FORTINET MAKES, AND CUSTOMER RECEIVES, NO OTHER WARRANTIES OF ANY KIND, EXPRESS, IMPLIED OR STATUTORY, ARISING IN ANY WAY OUT OF, RELATED TO, OR UNDER THIS AGREEMENT OR THE PROVISION OF MATERIALS OR SERVICES HEREUNDER, AND, TO THE EXTENT PERMISSIBLE BY LAW, FORTINET SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTY OF SATISFACTORY QUALITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY RIGHTS.

## **10. LIMITATION OF LIABILITY**

10.1. NOTWITHSTANDING ANYTHING TO THE CONTRARY, IN NO EVENT WILL FORTINET BE LIABLE TO THE CUSTOMER FOR ANY SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES OF ANY KIND, INCLUDING BUT NOT LIMITED TO ANY LOST PROFITS OR LOSS OF DATA HOWEVER CAUSED, WHETHER FOR BREACH OR REPUDIATION OF CONTRACT, TORT, BREACH OF WARRANTY, NEGLIGENCE, OR OTHERWISE, WHETHER OR NOT FORTINET WAS ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES. NOTWITHSTANDING ANYTHING TO THE CONTRARY, FORTINET'S TOTAL POSSIBLE LIABILITY TO THE CUSTOMER AND OTHERS ARISING FROM OR IN RELATION TO THIS AGREEMENT AND THE SERVICES, WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR STRICT LIABILITY, SHALL BE LIMITED TO THE TOTAL PAYMENTS MADE BY CUSTOMER TO FORTINET UNDER THIS AGREEMENT FOR THE PARTICULAR SERVICE CONTRACT AT ISSUE DURING THE THREE HUNDRED SIXTY-FIVE (365) CALENDAR DAYS PRIOR TO THE DATE OF THE EVENT GIVING RISE TO THE LIABILITY. THIS LIMITATION WILL APPLY TO ALL CAUSES OF ACTION IN THE AGGREGATE. IN NO EVENT WILL FORTINET BE LIABLE FOR THE COST OF PROCUREMENT OR REPLACEMENT OF SUBSTITUTE GOODS. IN THE EVENT FORTINET SUSPENDS OR TERMINATES SERVICES IN THE MIDDLE OF A SERVICE TERM FOR ANY REASON, NOTWITHSTANDING ANYTHING TO THE CONTRARY, FORTINET'S MAXIMUM LIABILITY SHALL BE THE PRO-RATED AMOUNT OF THE FEES ACTUALLY PAID TO FORTINET FOR SUCH SERVICES FOR THE PERIOD OF THE CURRENT TERM DURING WHICH NO SUCH SERVICES ARE PERFORMED (I.E. THE PRO-RATED AMOUNT PAID FOR THE PERIOD FROM SUSPENSION OR TERMINATION TO THE END OF THE CURRENT PAID-FOR TERM). FOR CLARITY, IF FORTINET IS ENTITLED TO TERMINATE THE SERVICE PURSUANT TO THIS AGREEMENT FORTINET SHALL OWE NO REFUND OR ANY OTHER AMOUNTS, AND, IN ADDITION, IN ALL EVENTS, CUSTOMER IS RESPONSIBLE TO WORK IN GOOD FAITH TO MITIGATE ANY DAMAGES CUSTOMER MAY REALIZE. THE FOREGOING LIMITATIONS OF LIABILITY SHALL NOT APPLY TO DAMAGES ARISING FROM DEATH OR PERSONAL INJURY IN ANY JURISDICTION WHERE SUCH LIMITATION IS PROHIBITED BY APPLICABLE LAW. FOR FURTHER CLARITY, NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT OR OTHERWISE, IN NO EVENT DOES FORTINET PROVIDE ANY GUARANTEE OR ASSURANCE REGARDING COMPREHENSIVE SECURITY OR ENSURING FULL SECURITY OF THE PRODUCTS, SERVICES, OR CUSTOMER'S ASSETS OR NETWORKS.

## 11. GENERAL PROVISIONS

**11.1. Compliance with laws.** Customer hereby agrees to comply with all applicable laws, such as data privacy and privacy disclosure laws. Fortinet's Products and Services may be subject to the United States Export Administration Regulations and other import and export laws. Diversion contrary to United States law and regulation is prohibited. Customer agrees to comply with, and ensure compliance with, all applicable laws that apply to the products as well as the Customer and destination restrictions issued by U.S. and other governments. As just one example, if Customer is a FortiPartner that provides Return Manufacture Authorization services ("RMA"), Services or other Services on behalf of another entity or otherwise provides Product or Services, Customer shall ensure proper, required export licenses are obtained for all Product, whether newly-purchased or RMA, prior to exporting those appliances and prior to providing any Services related to those appliances, if such export license is required. In addition, for RMA units or other units registered in a FortiPartner's name, the FortiPartner is responsible for all export compliance. In addition, if Customer or the end-user on whose behalf Customer is providing RMA, Services or other Services is designated a Denied Party, Specially Designated National, on the Entity List, or otherwise subject to an export license requirement after this agreement, then Fortinet may terminate or suspend, in its sole discretion, any and all Services related to Product or Services exported without full compliance with applicable export laws. For additional information on U.S. export controls see [www.bis.doc.gov](http://www.bis.doc.gov). Fortinet assumes no responsibility or liability for Customer's or partners' failure to obtain any necessary import and export approvals. Customer represents that neither the United States Bureau of Industry and Security nor any other governmental agency has issued sanctions against Customer or otherwise suspended, revoked or denied Customer's export privileges. Customer agrees not to use or transfer the Products or Services for any use relating to nuclear, chemical or biological weapons, or missile technology, unless authorized by the United States Government by regulation or specific written license. Additionally, Customer agrees not to directly or indirectly export, import or transmit the Products or Services contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or use. Customer represents that Customer understands, and Customer hereby agrees to comply with, all requirements of the U.S. Foreign Corrupt Practices Act and all other applicable laws. Fortinet is not responsible for Service delays or outages or loss of data resulting from activities related to Fortinet's and its service partners compliance with export regulations and cooperation with applicable domestic or foreign regulatory agencies (e.g., delays caused by requirement to obtain required licenses). Customer agrees, acknowledges and warrants that it will take reasonable steps to ensure it will meet all legal requirements to assist law enforcement agencies.

**11.2. Survival of terms.** The terms contained herein which by their nature are intended to survive the termination of this Agreement shall do so.

**11.3. Transferability.** Customer may not assign or otherwise transfer this Agreement without written consent from Fortinet. Any attempted assignment or attempted transfer without Fortinet's consent shall be null and void and may result on the termination of this Agreement and related Service Contracts. Fortinet may assign its rights and obligation under this Agreement to a third party without consent from Customer.

**11.4. Entire Agreement.** The provisions of this Agreement constitute the entire agreement between the parties with respect to the subject matter hereof, and this Agreement supersedes all prior agreements or representations, oral or written, regarding such subject matter. With the exception of the EULA, this Agreement takes precedence over any conflicting provisions in a document a Fortinet portal website such as a service description or support portal terms. This Agreement may be modified or amended only in accordance with Section 5.10 herein. All notices from Customer to Fortinet must be made by opening a new Support Ticket through the Support Portal.

**11.5. Confidential information.** Customer may be exposed to certain information concerning the Products and Services including, without limitation, maintenance releases (regularly scheduled and released updates and upgrades to software), feature releases (enhancements released through Fortinet's Product planning practices or through Customer requests) and other Product, Service or business information, which is Fortinet's confidential or proprietary information (herein "Confidential Information"). The Customer agrees that, during and after the term of this Agreement, the Customer will not use or disclose to any third party any Confidential Information without the prior written consent of Fortinet, and Customer will use reasonable efforts to protect the confidentiality of such Confidential Information. The Customer may disclose the Confidential Information only to its employees as is reasonably necessary for the purposes for which such information was disclosed to Customer; provided that each such employee is under a written obligation of nondisclosure which protects the Confidential Information under terms substantially similar to those herein. Fortinet may process and store Customer data in the United States or any other country in which Fortinet or its agents work or maintain facilities. Customer will take reasonable steps not to disclose to Fortinet any personally identifiable, confidential or sensitive data, and Customer hereby consents to Fortinet's processing and storage of Customer data, acknowledging and agreeing that Fortinet is merely a data processor.

**11.6. Governing Law, venue and settlement of controversies.** This Agreement shall be governed by the laws of the State of California, as applied to agreements entered into and to be performed entirely within California between California residents, without regard to the principles of conflict of laws or the United Nations Convention on Contracts for the International Sale of Goods. Any controversies or claims arising from or relating to this Agreement, or the breach hereof, which cannot be amicably settled by and between the parties, shall be referred to and finally settled by arbitration. The place of arbitration shall

be Santa Clara, California, pursuant to the Streamlined Arbitration Rules and Procedures of Judicial Arbitration and Mediation Services (JAMS), or its successor, before a sole, mutually agreed upon arbitrator and shall be conducted in English. Award for such dispute will be rendered by a single, neutral, mutually agreeable arbitrator. The parties specifically consent and agree that the Federal Courts located in the Northern District of California will have exclusive jurisdiction over enforcement of any arbitration decisions.

**11.7. Taxes and Duty.** Where purchasing directly from Fortinet, all prices payable under this Agreement are exclusive of all foreign, federal, state, municipal tax or duty now in force or enacted in the future. Customer shall comply with all applicable tax laws and regulations and the Customer will promptly pay or reimburse Fortinet for any costs and damages related to any liability incurred as a result of Customer's non-compliance or delay with its responsibilities herein. The Customer's obligations under this section shall survive termination or expiration of this Agreement.

**11.8. English language and interpretation.** This Agreement is in the English language only, which language shall be controlling in all respects. Any versions of this Agreement in any other language will be for accommodation only and will not be binding upon either party. In construing or interpreting this Agreement, the word "or" shall not be construed as exclusive, and the word "including" shall not be limiting. The parties agree that this Agreement shall be fairly interpreted in accordance with its terms without any strict construction in favor of or against either party and that ambiguities shall not be interpreted against the drafting party.

**11.9. No waiver and severability.** Failure by Fortinet to enforce any provision of this Agreement will not be deemed

a waiver of future enforcement of that or any other provision. The exercise by either party of any remedy under this Agreement will be without prejudice to its other remedies under this Agreement or otherwise. If for any reason a court of competent jurisdiction or an agreed-upon arbitrator finds any provision of this Agreement, or portion thereof, to be unenforceable, that provision of the Agreement shall be enforced to the maximum extent permissible so as to affect the intent of the parties, and the remainder of this Agreement shall continue in full force and effect.

**11.10. Force Majeure.** Fortinet shall be excused from performance to the extent performance is rendered impossible by strike, fire, flood, extreme weather, disaster, act of war or terrorism, military operations, riots, insurrection or civil disorder, national or local emergency, famine, disease, epidemic or pandemics, governmental acts or orders or restrictions, failure of suppliers or any other reason where failure to perform is beyond Fortinet's reasonable control.

**11.11. Future Functionality.** Customer agrees that its purchases of Products or Services are not contingent on the delivery of any future functionality or features, or dependent on any oral or written public comments made by Fortinet regarding future functionality or features.

**11.12. Relationship of the Parties.** The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties.

**11.13. No Third-Party Beneficiaries.** There are no third-party beneficiaries to this Agreement. For clarity, End Users are not third-party beneficiaries to this Agreement.

March 2021

-----End of Document-----

## Fortinet Professional Service Terms and Conditions

### Master Professional Services Agreement

---

CAREFULLY READ THE FOLLOWING TERMS OF FORTINET'S PROFESSIONAL SERVICES BETWEEN YOU AND FORTINET, INC., OR FORTINET, INC.'S SUBSIDIARIES OR AFFILIATES ("FORTINET"). YOU ARE AGREEING TO BE BOUND BY AND ACCEPT THESE TERMS AND CONDITIONS OF SALE. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, DO NOT SIGN THE STATEMENT OF WORK PROVIDED BY FORTINET.

FORTINET SHALL NOT BE BOUND BY ANY ADDITIONAL, INCONSISTENT, AND/OR CONFLICTING PROVISIONS IN ANY ORDER, RELEASE, ACCEPTANCE OR OTHER CORRESPONDENCE UNLESS EXPRESSLY AGREED TO IN A WRITING SIGNED BY FORTINET'S GENERAL COUNSEL, AND IN NO EVENT SHALL FORTINET BE DEEMED TO HAVE ACCEPTED ANY TERMS IN YOUR PURPORTED OFFER OR OFFER DOCUMENTS.

#### 1. SERVICES AND PROJECT MANAGERMENTS

- 1.1. **Statement of Work.** Fortinet agrees to provide certain security information technology, installation, or modification services (the "**Services**") to Company that are mutually agreed from time to time between the Parties. The specific Services will be set forth in one or more Statements of Work that the Parties may execute pursuant to these terms and conditions ("**Statement of Work**" or "**SOW**"), substantially in the form above. Each SOW shall be incorporated into and become part of these terms and conditions and be governed by the provisions of these terms and conditions. In the event of a conflict between the terms and conditions of these terms and conditions and a SOW, the provisions of these terms and conditions shall prevail unless the Parties have obtained the express written consent of authorized signatories of each Party to deviate from the terms and conditions of these terms and conditions for a particular SOW and the SOW expressly states that the conflicting terms in the SOW shall prevail over the terms of these terms and conditions. Fortinet shall not be required to commence work under these terms and conditions unless a Statement of Work is duly executed. To the extent applicable, "**Deliverables**" shall mean those items specifically described and itemized in the SOW as final work products to be delivered by Fortinet pursuant to such SOW. For clarity, unless expressly and specifically described in an SOW, Fortinet shall not have responsibility to perform Services.
- 1.2. **Points of Contact.** Fortinet and Company will each designate an individual in the Statement of Work to act as a primary point of contact between the Parties with respect to the Services ("**POCs**"). Such POCs will have the power to make technical and project-level decisions within the scope of these terms and conditions (including, for example, staffing decisions, Change Orders, and Acceptance of Deliverables) that are binding on their respective entities. Amendments to these terms and conditions, however, must be made in accordance with the clause hereto governing contract amendments.
- 1.3. **Changes to Services.** Either Party may request a change order ("**Change Order**") in the event of actual or anticipated change(s) to the agreed scope of Services, Deliverables, project schedule, price, or any other aspect of the Statement of Work. Fortinet will prepare a Change Order reflecting the proposed changes, including but not limited to the impact on the Deliverables, project schedule, and price. Absent a Change Order signed by the Parties, Fortinet shall not be bound to perform any additional or out-of-scope services beyond what is stated in the SOW. The Parties agree to negotiate all Change Order requests expeditiously and in good faith. The Parties further agree that: (a) Fortinet may at its discretion undertake and accomplish tasks of a de minimis nature necessary to perform its obligations under any SOW at no additional cost and without requiring the execution of a Change Order; and (b) Fortinet shall be compensated with or without a Change Order for unplanned idle time and project delays (to the extent such delays are not caused by Fortinet).
- 1.4. **Acceptance.** If applicable, following submission of any Deliverable(s) by Fortinet, Company will perform testing and review in accordance with previously agreed testing standards and procedures as agreed by the Parties in the SOW. By the expiration of such review period, Company will submit a written statement (a "**Deliverable Review Statement**") to the Fortinet Project Manager indicating acceptance of the Deliverable(s) ("**Acceptance**") or specifying in detail how the submitted Deliverable(s) fails to materially conform to the agreed specification, in which case Fortinet shall be afforded a commercially reasonable period of time not less than thirty (30) days to correct any nonconformities, whereupon the review cycle will recommence. Deliverables will be deemed to be fully and finally accepted by Company in the event Company has not submitted a Deliverable Review Statement to Fortinet before the expiration of the applicable review period, or when Company uses the Deliverable in its business, whichever occurs first ("**Deemed Acceptance**"). Fortinet may request that Company execute a Work Complete as confirmation of acceptance and Company shall execute such Work Complete and/or identify any issues with the Services that prevent confirmation of the Work Complete within five (5) business days of Fortinet's request. Unless specifically agreed in an SOW, Fortinet's invoicing will be on a periodic basis and not linked to Acceptance. Notwithstanding anything to the contrary, Company shall be obligated to pay for Services performed regardless of Acceptance.
- 1.5. **Company Input and Responsibilities.** Company will supply in a timely manner information, materials and actions necessary to the project including as applicable data, designs, programs, specifications, management decisions, approvals, acceptance criteria, and other information and material, plus any other assistance and materials as reasonably requested by Fortinet at Company's cost, for Fortinet's use in carrying out the Services ("**Inputs**"). Further Company responsibilities



may be set out in a Statement of Work or project planning document agreed between the Parties. Company may further provide equipment and software ("**Project Tools**") to Fortinet in order for Fortinet to provide the Services. Company shall bear all license, procurement and maintenance expenses related to the Project Tools.

- 1.6. **Performance Generally.** Fortinet's failure to perform its contractual responsibilities, to perform the services, or to meet agreed service levels shall be excused if and to the extent Fortinet's non-performance is caused by Company's omission to act, delay, wrongful action, failure to provide Inputs, or failure to perform its obligations under these terms and conditions

## **2. STAFFING**

- 2.1. **Team Composition.** Fortinet shall determine, after consultation with Company, the size, composition and distribution of the resource team, which Fortinet may change from time to time based upon the scope and complexity of the Services.
- 2.2. **Removal.** Company may require Fortinet to remove a team member if, after due consultation with Fortinet, it is reasonably determined that the individual is not suitable to perform the Services. Any such removal shall be effective after a minimum of fourteen (14) days written notice. Fortinet shall assign a replacement resource to the Services as soon as practicable. Company understands and acknowledges, however, that removal of a resource in fixed-price or fixed-schedule engagements may affect the pricing and project schedule for the affected Services and agrees to execute appropriate Change Orders to accommodate such removal.

## **3. PRICING, INVOICING & PAYMENT**

- 3.1. **Pricing & Payments.** Projects will be performed as stated on this SOW and be billed in accordance with Fortinet's then-current rates as of the date of execution of the SOW. Unless stated otherwise in the applicable SOW, if applicable, Customer must pay invoices within thirty (30) days from the date of Fortinet's invoice. Fortinet may charge interest at the lower of (a) a rate of 1.5% per month for delayed payments or (b) to the maximum extent allowed by law.
- 3.2. **Taxes.** The fees chargeable by Fortinet are stated exclusive of all taxes, duties and levies imposed by any government body. Company shall be liable and will pay for all applicable tax liabilities such as sales, services, use or value added taxes, but specifically excluding employment related taxes concerning Fortinet personnel and corporate taxes based on Fortinet's net income.

## **4. CONFIDENTIALITY**

- 4.1. The Parties agree that with respect to any business information of the disclosing Party which (a) is marked as "confidential," proprietary" or some similar indication; (b) is expressly advised by the disclosing Party to be confidential through some contemporaneous written means; or (c) which the receiving Party would reasonably construe to be confidential information under the circumstances (collectively referred to as "Confidential Information"): (i) to use such Confidential Information only in relation to the Services; (ii) not to disclose any such Confidential Information or any part thereof to a person outside the Party's business organization for any purposes unless expressly authorized by the owner of such Confidential Information; (iii) to limit dissemination of such Confidential Information to persons within the Party's business organization who are directly involved in the performance of Services under these terms and conditions and have a need to use such Confidential Information; (iv) to safeguard the Confidential Information to the same extent that it safeguards its own confidential materials or data.
- 4.2. Confidential Information shall not include information that: (a) is as of the time of its disclosure part of the public domain; (b) is subsequently learned from a third Party without a duty of confidentiality; (c) at the time of disclosure was already in the possession of the receiving Party; (d) was developed by employees or agents of the receiving Party independently of and without reference to any information communicated to the receiving Party; or (e) is required to be disclosed pursuant to a court order or government authority, whereupon the receiving Party shall, at its earliest opportunity, provide written notice to the disclosing Party prior to such disclosure and where feasible giving the disclosing Party a reasonable opportunity to secure a protective order or take other action as appropriate.
- 4.3. The Parties' obligations under this Section shall extend to the non-publicizing of any dispute arising out of these terms and conditions.
- 4.4. The terms of this clause shall continue in full force and effect for a period of three(3) years from the date of disclosure of such Confidential Information.
- 4.5. In the event of termination of these terms and conditions, upon written request of the disclosing Party, the receiving Party shall immediately return the disclosing Party's Confidential Information, or at the disclosing Party's option destroy any remaining Confidential Information and certify that such destruction has taken place, provided however that Fortinet may retain a minimum of one copy of all work product and relevant project documentation for archival and audit purposes.

## 5. PROPRIETARY RIGHTS

- 5.1. Retained Rights. Each Party owns, and will continue to own all right, title and interest in and to any inventions however embodied, know how, works in any media, software, information, trade secrets, materials, property or proprietary interest that it owned prior to these terms and conditions, or that it created or acquired independently of its obligations pursuant to these terms and conditions (collectively, "Retained Rights"). All Retained Rights not expressly transferred or licensed herein are reserved to the respective owner.
- 5.2. Deliverables and Fortinet Materials. All intellectual property rights in, or related to, any developments, Deliverables, enhancements, or other work product of Fortinet or related to the services to be performed hereunder or under any SOW shall be owned solely by Fortinet. Fortinet owns (or will own) any such material that is used in, enhanced, or developed in the course of providing services hereunder, and all intellectual property rights to such material, including: any and all rights throughout the word, arising out of, or associated with models, designs, patents, applications therefor, all trade secrets, proprietary information rights, know how, works of authorship, mask works, trade names, logos, trademarks, service marks, methodologies; delivery procedures; manuals; generic software tools, routines, frameworks, and components; generic content, research and background materials; templates; analytical models; project tools; development tools; and all other intellectual property and ownership rights (collectively, "Fortinet Materials"). To the extent any Fortinet Materials are necessarily required for the proper functioning of the Deliverables (such that the Deliverables will not function without the Fortinet Materials) or are embedded into the Deliverables, Fortinet grants to Company a perpetual, nonexclusive, non-transferable, royalty-free, worldwide license to use such Fortinet Materials solely in conjunction with its use of such Deliverables. Company acknowledges that the Fortinet Materials are Confidential Information of Fortinet, regardless of whether so designated. This section shall not prohibit fee-based licensing of certain intellectual property of Fortinet as may be agreed by the Parties.

## 6. REPRESENTATIONS, WARRANTIES AND COVENANTS

- 6.1. Authority to Contract. The Parties each represent and warrant that they have obtained all necessary corporate approvals to enter into these terms and conditions and that no consent, approval, or withholding of objection is required from any external authority with respect to the entering into of these terms and conditions. The Parties further represent and warrant that they are under no obligation or restriction, nor will they assume any such obligation or restriction, that would in any way interfere or conflict with any obligations under these terms and conditions.
- 6.2. Compliance with Laws. The Parties covenant that they will comply with all applicable laws and regulations in their conduct pursuant to these terms and conditions. The Parties further covenant that a change in laws that materially alters the assumptions upon which Fortinet entered these terms and conditions or a particular SOW shall warrant a Change Order.
- 6.3. Warranty on Services. Fortinet warrants that it will perform the Services in a professional and workmanlike manner and that its personnel have the requisite skills and experiences to perform the Services. Company agrees that in the event of a breach of the foregoing warranty, its only remedy shall be the re-performance of the Services by Fortinet.
- 6.4. Warranty Disclaimer. EXCEPT AS EXPRESSLY PROVIDED IN THIS SECTION 6, FORTINET EXCLUDES AND DISCLAIMS ALL OTHER WARRANTIES, CONDITIONS OR STATEMENTS, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR THAT DELIVERABLES WILL BE ERROR-FREE

## 7. INDEMNIFICATION

- 7.1. Subject to Section 8, Company shall indemnify, defend, and hold harmless from and against any damages, costs, attorneys' fees, penalties, fines, liabilities, or expenses that arise from third party actions or claims (collectively, "Losses") against Fortinet and its affiliates, officers and directors, employees, agents, and representatives relating to (a) death or injury to persons caused by the Company; (b) a violation of applicable laws by the Company; or (c) Company's infringement of a third Party's intellectual property rights where such third Party is located in either the country where the Services were provided or received.
- 7.2. Subject to Section 8, Fortinet shall indemnify, defend, and hold harmless from and against any damages, costs, attorneys' fees, penalties, fines, liabilities, or expenses that arise from third party actions or claims (collectively, "Losses") against Company relating to (a) death or injury to persons caused by the Fortinet; or (b) Fortinet's infringement of a third Party's intellectual property rights where such third Party is located in either the country where the Services were provided or received, provided however that Fortinet shall not have any liability to Company under this Section to the extent that any infringement or claim thereof is attributable to: (i) the combination, operation or use of a Deliverable with equipment or software supplied by Company where the Deliverable would not itself be infringing; (ii) compliance with designs, specifications or instructions provided by Company; (iii) use of a Deliverable in an application or environment for which it was not designed or contemplated under these terms and conditions; or (iv) modifications of a Deliverable by anyone other than Fortinet where the unmodified version of the Deliverable would not have been infringing. Fortinet will completely satisfy its obligations hereunder if, after receiving notice of a claim, Fortinet obtains for Company the right to

continue using such Deliverables as provided without infringement, or replace or modify such Deliverables so that they become non-infringing.

- 7.3. Promptly after an indemnitee receives notice of any claim for which it will seek indemnification pursuant to these terms and conditions, the indemnitee will notify the indemnitor of the claim in writing. No failure to so notify the indemnitor will abrogate or diminish the indemnitor's obligations under this Section if the indemnitor has or receives knowledge of the claim by other means or if the failure to notify does not materially prejudice its ability to defend the claim. Within fifteen (15) days after receiving an indemnitee's notice of a claim, but no later than ten (10) days before the date on which any formal response to the claim is due, the indemnitor will notify the Indemnitee in writing as to whether the indemnitor acknowledges its indemnification obligation and elects to assume control of the defense and settlement of the claim (a "**Notice of Election**"). In issuing a Notice of Election, the indemnitor waives any right of contribution against the indemnitee unless the Notice of Election expressly states that indemnitor believes in good faith that the Indemnitee may be liable for portions of the claim that are not subject to indemnification by the Indemnitor, in which case the indemnitee will have the right to participate in the defense and settlement of the claim at its own expense using counsel selected by it.
- 7.4. If the indemnitor timely delivers a Notice of Election, it will be entitled to have sole control over the defense and settlement of the claim except as provided in the immediately preceding paragraph. After delivering a timely Notice of Election, the indemnitor will not be liable to the Indemnitee for any attorneys' fees subsequently incurred by the indemnitee in defending or settling the claim. In addition, the indemnitor will not be required to reimburse the indemnitee for any amount paid or payable by the indemnitee in settlement of the claim if the settlement was agreed to without the written consent of the indemnitor.
- 7.5. If the indemnitor does not deliver a timely Notice of Election for a claim, the indemnitee may defend and/or settle the claim in such manner as it may deem appropriate, and the indemnitor will promptly reimburse the indemnitee upon demand for all Losses suffered or incurred by the Indemnitee with respect to the claim.
- 7.6. Exclusive Remedy. This Section 7 "Indemnification" constitutes the exclusive rights and remedies for the matters indemnified.

## 8. LIMITATION OF LIABILITY

- 8.1. Limitation of Liability. NOTWITHSTANDING ANYTHING TO THE CONTRARY ELSEWHERE CONTAINED IN THESE TERMS AND CONDITIONS, NEITHER PARTY SHALL, IN ANY EVENT, REGARDLESS OF THE FORM OF CLAIM, BE LIABLE FOR (1) ANY INDIRECT, SPECIAL, PUNITIVE, EXEMPLARY, SPECULATIVE OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, ANY LOSS OF USE, LOSS OF DATA, BUSINESS INTERRUPTION, AND LOSS OF INCOME OR PROFITS, IRRESPECTIVE OF WHETHER IT HAD AN ADVANCE NOTICE OF THE POSSIBILITY OF ANY SUCH DAMAGES; OR (2) DAMAGES RELATING TO ANY CLAIM THAT ACCRUED MORE THAN TWO (2) YEARS BEFORE THE INSTITUTION OF ADVERSARIAL PROCEEDINGS THEREON. TOTAL LIABILITY. SUBJECT TO THE ABOVE AND NOTWITHSTANDING ANYTHING TO THE CONTRARY ELSEWHERE CONTAINED HEREIN, THE MAXIMUM AGGREGATE LIABILITY OF FORTINET SHALL BE, REGARDLESS OF THE FORM OF CLAIM, THE CONSIDERATION RECEIVED BY FORTINET FOR THE STATEMENT OF WORK TO WHICH THE CLAIM RELATES DURING THE PRECEDING THREE (3) MONTHS. FOR CLAIMS THAT ARISE UNDER THESE TERMS AND CONDITIONS AND THAT DO NOT LOGICALLY RELATE TO A PARTICULAR STATEMENT OF WORK, THE MAXIMUM AGGREGATE LIABILITY OF FORTINET SHALL BE THE SUM OF THE CONSIDERATION RECEIVED UNDER ALL ACTIVE STATEMENTS OF WORK UNDER THESE TERMS AND CONDITIONS FOR THE PRECEDING THREE (3) MONTHS.

## 9. TERMINATION

- 9.1. Termination for Convenience. Fortinet may, without cause or for convenience, terminate any SOW and/or these terms and conditions upon written notice of two (2) months to the other party.
- 9.2. Termination for Cause. Either Party may terminate any SOW upon written notice to the other in the event that: (a) the other Party commits a material breach of these terms and conditions or Statement of Work and fails to cure such default to the non-defaulting Party's reasonable satisfaction within thirty (30) days after receipt of notice; or (b) the other Party becomes insolvent or bankrupt, assigns all or a substantial part of its business or assets for the benefit of creditors, permits the appointment of a receiver for its business or assets, becomes subject to any legal proceeding relating to insolvency or the protection of creditors' rights or otherwise ceases to conduct business in the normal course.
- 9.3. Effects of Termination. In the event of termination of an SOW hereunder, Company shall pay Fortinet: (1) all fees as specified in the SOW and expenses up to the effective date of the termination, including work in progress, plus fees for the applicable notice period irrespective of whether Company requires Fortinet's services during such period; and (2) any termination charges agreed by the Parties. If these terms and conditions is terminated before all SOWs executed hereunder are terminated or completed, the terms of these terms and conditions shall remain in full force until the termination or completion of such Statements of Work.

## 10. MISCELLANEOUS

- 10.1. Relationship of the Parties. It is understood and agreed that Fortinet will provide services under these terms and conditions as an independent contractor and that during the performance of Services under these terms and conditions, Fortinet's employees will not be considered employees of Company for any purpose whatsoever. Accordingly, Fortinet shall be solely responsible for the compensation of such employees and all employment-related taxes. Further, nothing herein shall be construed to entitle either Party to be a representative, agent, partner or joint venturer of the other.

## 11. FORCE MAJEURE

- 11.1. Force Majeure. Except for the obligation to make payments, nonperformance of either party shall be excused to the extent performance is rendered impossible by strike, fire, flood, governmental acts or orders or restrictions, failure of suppliers or any other reason where failure to perform is beyond the reasonable control of and is not caused by the negligence of the non-performing party. In the event such an event prevents performance thereunder for a period in excess of sixty (60) days, then the non-defaulting party may elect to terminate these terms and conditions and/or cancel or suspend any SOWs thereunder by a written notice to the defaulting party.

## 12. DISPUTE RESOLUTION

- 12.1. Dispute Resolution and Venue. Any controversies or claims arising from or relating to these terms and conditions, or the breach or validity thereof, which cannot be amicably settled by and between the parties, shall be referred to and finally settled by arbitration. The place of arbitration shall be Santa Clara, California, pursuant to the Streamlined Arbitration Rules and Procedures of Judicial Arbitration and Mediation Services (JAMS), or its successor, before a sole, mutually agreeable arbitrator, in accordance with the laws of the State of California for agreements made in and to be performed in that State.

## 13. GENERAL

- 13.1. Governing Law. These terms and conditions shall be interpreted and construed in accordance with the laws of the State of California, without regard to its conflicts of laws provisions.
- 13.2. Headings. The headings used in these terms and conditions are for the convenience of the Parties only and shall not be deemed a part of, or referenced in, construction of these terms and conditions.
- 13.3. Assignments. These terms and conditions will be binding on the Parties hereto and their respective successors and assigns. Neither Party may assign these terms and conditions or SOWs without the prior written consent of the other. Any assignment by operation of law, order of any court, or pursuant to any plan of merger, consolidation or liquidation, will be deemed an assignment for which prior consent is required and any assignment made without any such consent will be void and of no effect as between the Parties. Notwithstanding the forgoing Fortinet may assign these terms and conditions pursuant to a merger, acquisition, or sale of at least fifty percent (50%) its assets without consent.
- 13.4. Entire Agreement. The provisions of these terms and conditions, including any appendices, schedules, exhibits, or SOWs referred to herein and/or attached hereto, constitute the entire agreement between the parties with respect to the subject matter hereof, and these terms and conditions supersedes all prior agreements or representations, oral or written, regarding such subject matter. Except as provided for in these terms and conditions, these terms and conditions may not be modified or amended except in a writing signed by a duly authorized representative of each party, and, furthermore, Company acknowledges and agrees that Fortinet is not bound by any purported amendment or new agreement signed by a representative of Fortinet other than Fortinet's General Counsel. For clarity, only Fortinet's General Counsel is authorized to alter, amend, or modify these terms and conditions in any way or enter a new agreement on behalf of Fortinet or its affiliates, and any amendment or new agreement that is not signed by Fortinet's General Counsel, regardless of whether including a Fortinet, or Fortinet affiliate, company seal or chop, is null and void and of no force and effect.
- 13.5. Modifications. No amendment or change to these terms and conditions or any waiver or discharge or any rights or obligations under these terms and conditions will be valid unless in writing and signed by an authorized representative of the Party against which such amendment, change, waiver or discharge is sought to be enforced.
- 13.6. Severability. In the event that any provision of these terms and conditions conflicts with the law under which these terms and conditions is to be construed or if any such provision is held invalid by a competent authority, such provision will be deemed to be restated to reflect as nearly as possible the original intentions of the Parties in accordance with applicable law. The remainder of these terms and conditions will remain in full force and effect.
- 13.7. Survivability. Any provision of these terms and conditions that contemplates performance or observance subsequent to termination or expiration of these terms and conditions will survive termination or expiration of these terms and conditions and continue in full force and effect, including the following:

Pricing, Invoicing, and Payment (Section 3)  
Confidentiality (Section 4)  
Proprietary Rights (Section 5)  
Representations, Warranties, and Covenants (Section 6)  
Indemnification (Section 7)  
Limitation of Liability (Section 8)  
Dispute Resolution (Section 12)  
General (Section 13).

Notices. All notices, requests, demands and determinations under these terms and conditions other than routine operational communications will be in writing through (i) hand delivery, (ii) express overnight courier with a reliable system for tracking delivery, or (iii) confirmed facsimile or electronic mail with a copy sent by another means specified herein, to the following:

If to Fortinet: Fortinet, Inc.  
899 Kifer Rd  
Sunnyvale, CA 94086  
Attn: General Counsel  
  
with a copy to: Chief Financial Officer




If to Company: Address as set forth in the Statement of Work between  
Company and Fortinet.

June 2016




-----End of Document-----

# **NSE Certification Levels**

# Fortinet Training: NSE Certification Levels

Cybersecurity Awareness Certification		
	Information Security Awareness is the entry-level certification in the program. You will be introduced to today's cyberthreats and advised on how you can secure your information. You must successfully complete all lessons and pass all quizzes within the Information Security Awareness course to obtain the NSE 1 Certification.	Ideal for: Everyone Get started with <a href="#">NSE 1</a>
	After you develop a solid understanding of the threat landscape and the problems facing organizations and individuals, you will learn about the evolution of cybersecurity. In the second level, you will learn about the types of security products that have been created by security vendors to address security problems faced by networks and organizations.	Ideal for: Everyone Get started with <a href="#">NSE 2</a>
	NSE 3 introduces you to key Fortinet products and describes the cybersecurity problems they solve. The product lessons and use cases in this course are organized into the following Fortinet Security Fabric pillars: Security-Driven Networking, Zero Trust Access, Adaptive Cloud Security, and Security Operations.	Ideal for: Everyone Get started with <a href="#">NSE 3</a>

## Cybersecurity Technical Certification

	NSE 4 identifies your ability to configure, install, and manage the day-to-day configuration, monitoring, and operation of a FortiGate device to support specific corporate network security policies.	Ideal for: Network Security Administrators, Technical Support Engineers and System Engineers Get started with <a href="#">NSE 4</a>
	NSE 5 recognizes your ability to implement network security management and analytics using Fortinet security devices. The curriculum is recommended for those who require the expertise to centrally manage, analyze, and report on Fortinet security devices. This designation is recognized when you successfully pass a minimum of any two Fortinet NSE 5 certification exams.	Ideal for: Network Security Administrators, Technical Support Engineers and System Engineers Get started with <a href="#">NSE 5</a>
	NSE 6 recognizes comprehensive skills with fabric products beyond the firewall. This designation is recognized after you achieve at least four Fortinet Specialist certificates on Fortinet enhanced products, and is recommended for those who are involved in managing and supporting specific Fortinet security products.	Ideal for: Network Security Administrators, Technical Support Engineers and System Engineers Get started with <a href="#">NSE 6</a>



## Cybersecurity Advanced Certification



NSE 7 identifies your advanced skills in deploying, administering, and troubleshooting Fortinet security solutions. This curriculum offers courses for network and security professionals who are involved in advanced administration and support of security infrastructures using Fortinet solutions. You must successfully pass at least one of the NSE 7 exams to obtain this certification.

Ideal for:  
IT Security  
Architects,  
Network  
Security  
Administrators,  
Technical  
Support  
Engineers and  
System  
Engineers  
Get started  
with [NSE 7](#)

## Cybersecurity Expert Certification



The NSE 8 Fortinet Network Security Expert designation identifies your comprehensive and expert knowledge of network security design, configuration, and troubleshooting for complex networks. To attempt the exam, candidates must have related industry experience. We recommend that you complete the appropriate Professional, Analyst, Specialist, and Architect designation training and have extensive experience with Fortinet products in a production environment. The Fortinet Network Security Expert designation does not include training.

Ideal for:  
Network  
Security  
Cybersecurity  
Professionals  
Get started  
with [NSE 8](#)

# **Case Studies**



## CASE STUDY

# Creating the Perfect Environment To Learn: Safely, Securely, and Without Interruption



Trenton Public Schools is a comprehensive community public school district educating 11,500 students in prekindergarten through 12th grade from Trenton, in Mercer County, New Jersey. With 25 buildings serving 13 elementary schools, four middle schools, and three high schools, the district is dedicated to helping all students graduate with a vision for their future, motivated to learn continually and prepared to succeed in their choice of college or career.

Over a multiproject, multiyear timeline, the Trenton IT team has worked with Fortinet and its technology partner, Advanced Computer Solutions Group (ACSG), to meet the district's evolving network infrastructure needs. From standardized testing to internet use and the related risks of a cyber world, educating students in a secure and protected environment is of paramount importance for Trenton school district.

## Electronic Testing Requires Greater Speed

The Partnership for Assessment of Readiness for College and Careers (PARCC) is a consortium of six states that includes New Jersey, working to collaboratively develop a common set of examinations to measure student achievement of the Common Core State Standards and preparedness for college and careers.

Firewalls became pertinent when the PARCC electronic assessments replaced the existing statewide testing, and the Trenton legacy network was unable to handle the demands. Dennis Morgan, director of IT for Trenton Public Schools, recalls, "We needed to invest in our wide-area network (WAN) and internet feeds as our environment was no longer capable of supporting the speed and bandwidth that were required. On any given day, the infrastructure needs to be able to support almost 12,000 endpoints and we just weren't able to handle all the traffic."

## Network Security With Visibility

Led by Morgan, the Trenton technical team sought a robust firewall replacement. With a recommendation from its technology partner ACSG, the Fortinet FortiGate quickly became the top candidate because of its industry-leading threat protection and performance. Morgan recounts, "We did a lot of research and the FortiGate always has excellent reviews and an extremely competitive price point. Ease of use and low operational overhead are two additional factors of the FortiGate that seem to be consistently highlighted by reviewers and existing users."

*"Fortinet is the brand I know I can trust to deliver what we need."*

*– Dennis Morgan, Director of IT,  
Trenton Public Schools*

## Details

**Customer:** Trenton Public Schools

**Industry:** Education

**Location:** New Jersey

**Partner:** Advanced Computer Solutions Group

## Business Impact

- Enhanced, infrastructurewide protection and visibility
- Cost and resource savings
- Maximized uptime with high-availability firewalls and removing single points of failure
- State-of-the-art protection against distributed denial-of-service (DDoS) attacks ensures services are uninterrupted

An on-site proof of concept was conducted to verify the suitability of the FortiGates in the Trenton environment. Morgan and his colleagues had multiple conversations with the technical staff of other Fortinet deployments that were similar to the proposed Trenton implementation. At the successful conclusion of the evaluation phase, a decision was made to partner with Fortinet.

A pair of FortiGate next-generation firewalls (NGFWs) were deployed in a high-availability configuration to support the newly acquired 10 Gig bandwidth internet connection. The solution provided built-in redundancy and included comprehensive threat protection and web filtering. “We were able to consolidate multiple systems and functions onto the pair of FortiGates,” Morgan states. “Having no single points of failure and the refreshing ease of having one location to review logs and complete daily audits are huge benefits for us.”

The implementation went well thanks to a solid product and a trusted implementation team. Morgan comments, “Working with Fortinet and ACSG was excellent—with full support through the whole deployment process—the expertise and work ethic are amazing. During the initial setup, the FortiGate’s intuitive interface made it very easy to audit the network and decide which rules were valid and which could be easily omitted.”

## Solutions

- FortiGate
- FortiDDoS
- FortiVoice with over 500 handsets

## Adding DDoS Protection

DDoS attacks have become more prevalent with colleges and high schools seeing an escalating number of attempted breaches. While Trenton had not experienced any issues, several other school districts and colleges in New Jersey had been impacted.

To proactively address the increasing risk and based on the success of the FortiGate implementation, Morgan consulted with ACSG and the recommendation once again was Fortinet. He describes, “We tested and then bought a FortiDDoS appliance: We wanted to get ahead of the risk before Trenton became another statistic.”

The FortiDDoS provides 100% heuristic/behavior-based detection that is completely transparent to would-be attackers. The massively parallel architecture simultaneously monitors hundreds of thousands of parameters to alleviate the possibility of throughput interruptions caused by flawed analysis. The appliance is equipped with comprehensive reporting and analysis tools that are administered sharing the same console used for the district’s FortiGates.

## FortiVoice: Quality and Savings

As with many IT teams in the education sector, in addition to multiple other duties, Morgan and his colleagues also are responsible for managing and maintaining the district’s extensive phone system. When the Trenton team began looking for a replacement for the district’s aging legacy Voice-over-Internet-Protocol (VoIP) phone system, options ranged from the poorly made to the outrageously expensive.

After discussions with ACSG, a recommendation was made to evaluate Fortinet’s business phone system, FortiVoice. “We thoroughly tested all the components—the handsets are well made, and the service quality is excellent—and it was an easy sell to our School Board,” says Morgan. “Not only was this deployment the smoothest phone cutover that I have been a part of but with 500 extensions in place, we are able to lower our phone costs by close to 60%.”

## Value for Money

Education costs are rising, school budgets are tighter, and everyone is expected to do more with less. Sophisticated protection from Fortinet, and the ACSG/Fortinet partnership, have made it easier for Trenton Public Schools to offer a safe and adaptable infrastructure to its students and staff.

Morgan summarizes, “Today with Fortinet, our infrastructure is significantly more secure and has a greatly improved cost efficiency. We’ve been able to put advanced security measures in place to ensure that our students are not exposed to the massive number of negative elements that are out on the web. This is critically important to everyone in the district and Fortinet is the brand I know I can trust to deliver what we need.”



www.fortinet.com



# NEXT-GENERATION NETWORK SECURITY for 21<sup>st</sup>-Century Classrooms

**Forward-thinking schools are adopting personalized learning to transform the education landscape and increase student achievement.** Broward County Public Schools in Florida recently implemented its Digital 5: Pathways to Personalized Learning initiative, in which every fifth-grade student in approximately 100 of the district's elementary schools is provided with a mobile device, digital resources and online instructional material.

However, the district's dive into personalized learning — along with several other digital initiatives and an increased demand for bandwidth — required network expansion and new security measures. To meet these needs, the district implemented Fortinet's next-generation firewall solution — FortiGate.

Fortinet's consolidated approach to network security provided the district with the security, flexibility, scalability and manageability necessary to meet the district's growing bandwidth needs. On any given day there are approximately 125,000 devices connected to the district's network with plans to add more. "In the past we had a number of point products that we used for traffic shaping, content filtering and more. At the time they served us well, but it became time to grow, so we went with the Fortinet solution that embedded a number of those

into one platform," says Doug Pearce, director of technical support services at Broward County Public Schools.

The FortiGate platform protects the district's data center while providing a safe Internet experience for students and staff via the personalized learning initiative. "It's incumbent on school districts to provide a safe and secure environment for the kids. That is not just a fundamental moral obligation, but also a requirement of certain regulations and E-rate, in which we participate," says Pearce.

Fortinet, the global leader in high-performance cybersecurity solutions, positions schools, colleges and libraries to respond rapidly to a sophisticated cyber-threat landscape. "We are very proud to be protecting a number of schools and school districts across the country, enabling them to focus on the real objective at hand — providing students with a safe and uninterrupted learning environment," says Bryan Wood, Fortinet's vice president of education. Fortinet's consolidated approach to network security provides unparalleled performance and ease of management, coupled with significant savings. Strengthened by the industry's highest level of threat research, intelligence and analytics from FortiGuard Labs, Fortinet delivers best-in-class protection to provide the safest and most secure digital learning environments.

To learn more about Fortinet's cybersecurity solutions for education, please visit [www.fortinet.com/solutions/education.html](http://www.fortinet.com/solutions/education.html) or contact [education@fortinet.com](mailto:education@fortinet.com).

**FORTINET®**

**E-RATE**  
ELIGIBLE SOLUTIONS



# NAC PROVIDES SECURE BYOD AND AIDS HIPAA COMPLIANCE AT UC IRVINE MEDICAL CENTER



A world-class academic medical center with a full range of acute and general-care services, University of California's Irvine Medical Center is at the forefront of medical education and research and prides itself on delivering the highest quality patient care.

At UC Irvine Medical Center, mobile devices such as iPhones and iPads are a way of life for doctors, professors, medical students, and staff. When Allscripts, which supplies the medical center's electronic medical record (EMR) system, announced it was developing a mobile app, "We knew our doctors and medical personnel would be clamoring to use this application," explains Adam Gold, Director of Emerging Technologies at UC Irvine Medical Center. "The time had come when we needed a BYOD strategy that would enable our staff to securely use their own devices at the medical center."

Several challenges would need to be overcome along the way. The most pressing concern was protecting HIPAA-compliant data. Gold recognized that security had to start at the endpoint, so only approved, secure devices are allowed on the network.

## MANAGING SECURE EMR ACCESS AND HIPAA CONCERNS

Physicians, instructors, students, and hospital staff interact with the EMR system differently, and varied access levels had to be easy to define and applied automatically. The hospital also had to enforce its security policies without appearing heavy-handed, so users could get on the network easily with personal devices while EMR access continued to be protected.

Concerns about regulatory compliance were particularly daunting. Hospitals are subject to internal and external audits to verify that sensitive HIPAA information like patient records and research data is secure and protected from misuse. Demonstrating compliance is hard enough when all devices are under internal control, but a BYOD environment adds an even greater layer of uncertainty. With HIPAA fines that can reach millions of dollars, ensuring and documenting compliance is crucial. UC Irvine required complete endpoint visibility, and the ability to define access levels, for every device connecting to its network.

*"With 100% visibility and control over every device and user on our network, we can define and enforce granular policies to manage risk and ensure compliance."*

— Jeff Barnes  
Information Security Officer  
University of California, Irvine



## DETAILS

**CUSTOMER:** UC Irvine Medical Center

**INDUSTRY:** Medical

**LOCATION:** Irvine, California

## BUSINESS IMPACT

- Automatically identifies every device and user accessing the network, and blocks unsafe devices and unauthorized users
- Automatically provisions network access according to the user's specific profile
- Help desk calls were reduced by 30% because users can manage their own devices
- Ability to demonstrate regulatory compliance with a few clicks

## DEPLOYMENT

- Network Access Control

USING NAC FOR FULL VISIBILITY AND CONTROL TO DEMONSTRATE HIPAA COMPLIANCE

UC Irvine Medical Center chose the Fortinet Network Access Control (NAC) solution to solve the problem of visibility and access control, while providing traceability to demonstrate HIPAA compliance across the operation. To address the BYOD and mobile access security challenge, the NAC solution integrated with mobile device management (MDM) software. MDM software enables the medical center to have stronger control over BYOD and hospital-owned mobile devices. To access the network, mobile devices must download the MDM app. This app ensures that each device is provisioned for safe access, correlates devices with owners, and confirms that each device has the minimum required antivirus and system patches, before the device can access the network. MDM software can also help locate or wipe devices that are lost or stolen to prevent unauthorized network access. These controls are critical to ensure the integrity of the network and HIPAA compliance.

NAC also enables UC Irvine to identify every endpoint and device connected to its network in real time. It can identify any potential unauthorized device and quarantine it immediately. NAC keeps a history of activity for each individual device and endpoint, so it can identify any suspicious activity, as well as provide records of all data access.

In addition, NAC enables the medical center to easily control permission and access, ensuring that each device accesses only the necessary data for their particular function. NAC's ability to offer role-based access permissions is another key criterion for keeping HIPAA-compliant data secure.

UC Irvine is very pleased with the solution. The medical center even saw a 30% reduction in help desk calls, as NAC provides an automated help and remediation page. NAC offers the HIPAA-compliant security they require, along with an efficient, user-friendly experience that keeps productivity high in the fast-paced medical environment.



GLOBAL HEADQUARTERS  
Fortinet Inc.  
899 Kifer Road  
Sunnyvale, CA 94086  
United States  
Tel: +1.408.235.7700  
[www.fortinet.com/sales](http://www.fortinet.com/sales)

EMEA SALES OFFICE  
905 rue Albert Einstein  
06560 Valbonne  
France  
Tel: +33.4.8987.0500

APAC SALES OFFICE  
8 Temasek Boulevard #12-01  
Suntec Tower Three  
Singapore 038988  
Tel: +65-6395-7899  
Fax: +65-6295-0015

LATIN AMERICA HEADQUARTERS  
Sawgrass Lakes Center  
13450 W. Sunrise Blvd., Suite 430  
Sunrise, FL 33323  
Tel: +1.954.368.9990

## CASE STUDY

# Illinois State Treasurer's Office Sets an Example for State Agency Cybersecurity

Chief Information Officer (CIO) Joseph Daniels for the Illinois State Treasurer is responsible for protecting an extremely large financial institution against cyber threats. "The Treasurer is the Banker for the state, which has \$32 billion in assets," says Daniels. "That is a large amount of financial resources to manage and to secure for our constituents."

The agency's legacy security environment was challenging to maintain. To strengthen security and streamline management, the Illinois State Treasurer rolled out several integrated Fortinet solutions. The user interfaces and single-pane-of-glass visibility of the new infrastructure make life easier for the agency's security staff. They have also proven highly effective at threat detection, helping the agency pass, with flying colors, a required external security audit.

## The Pursuit of Security Best Practices

Cybersecurity is a major concern for Daniels. "Obviously, the cyber threat landscape changes every day," he says. "If you are not following best business practices and utilizing a layered approach to security, it is hard to combat advanced threats." However, as a relatively small state agency, the Illinois State Treasurer faces staffing constraints that complicate the pursuit of best practices. The IT team has 22 staff members, only 4 of whom have cybersecurity responsibilities.

Cybersecurity is a major concern for Daniels. "Obviously, the cyber threat landscape changes every day," he says. "If you are not following best business practices and utilizing a layered approach to security, it is hard to combat advanced threats." However, as a relatively small state agency, the Illinois State Treasurer faces staffing constraints that complicate the pursuit of best practices. The IT team has 22 staff members, only 4 of whom have cybersecurity responsibilities.

The agency had been standardized on another vendor's firewalls and other security solutions for decades, but those products were expensive and difficult to manage. Daniels needed to make a change. The Illinois State Treasurer was already using a FortiGate appliance for virtual private network (VPN) functionality. When Daniels learned that it was a fully functional next-generation firewall (NGFW), he looked into moving into a trial. Daniels had heard positive feedback about Fortinet from his peers at a large private-sector financial firm. His team embarked on a proof of concept with a FortiGate NGFW and immediately liked its ease of use. Within a few weeks of launching the NGFW proof of concept, Daniels had removed a significant portion of his existing cybersecurity architecture and replaced it with Fortinet solutions.

Daniels and his team also liked the Fortinet Security Fabric that provided the tight integration between FortiGate NGFWs and the FortiSandbox solution, which can execute questionable code in an isolated environment to determine whether the



*"Without the partnership with Fortinet, we would not have been able to shed light for our partner agencies, very similar to our own, on the importance of looking outside of the box for the way they do security."*

- Joseph Daniels, Chief Information Officer, Illinois State Treasurer

## Details

**Customer:** Illinois State Treasurer's Office

**Industry:** Government

**Location:** Springfield, Illinois

## Business Impact

- Simplifies training of limited security staff through single-pane-of-glass visibility
- Enabled rare perfect score on information-security audit, thanks to completeness of weekly threat assessments



code represents a true threat. When he joined the Illinois State Treasurer two years ago, the organization had a significant security backlog. Its infrastructure included over 2,500 different applications, many of which had not been assessed for potential threats in several years. An internal analysis of applications running on Treasury systems using FortiSandbox revealed several unwanted applications.

## Integrated Security Visibility, Improved Usability

In addition to FortiGate NGFWs and FortiSandbox, the Treasurer's Office rolled out FortiGate Cloud, a Software-as-a-Service (SaaS) solution that provides cloud-based management of FortiGate NGFWs. "FortiGate Cloud provides cyber threat assessment reports that I started having delivered every single week because they gave us a really good overview of our environment," Daniels says. The Treasurer's Office is also using FortiWeb, a web application firewall (WAF), to protect a cloud deployment in Microsoft Azure.

The FortiGate NGFWs enable the security team to achieve greater visibility into their network and isolate network traffic to a particular endpoint or application, something the legacy firewalls could not do. Any malware attempting to beacon out to a command-and-control server or perform data exfiltration will be rapidly identified and eradicated. Moreover, the Fortinet infrastructure consolidates information about threat detection and response networkwide, which is essential for securing sensitive data, such as account or routing numbers, and connections with external financial institutions. "Having that single-pane-of-glass visibility makes security management a lot easier," Daniels says.

The Fortinet solutions are also meeting expectations with regard to usability. The four-person security team needs to be able to easily onboard new employees and cross-train for different job roles. The FortiGate NGFWs make this possible. "They could come in, use the GUI, look at policies and procedures, follow all the training material out there, and really make the firewall the first secure point of entry for the agency."

Beyond training to achieve basic familiarity, Fortinet's extensive library of videos and guides have made it possible for the Treasurer's staff to solve many security problems without requiring external support. Daniels says, "You can walk step by step, from inception to completion, through all the training videos Fortinet provides. That documentation is critical for agencies without a huge staff because you can take anyone and walk them through it."

On the rare occasion that the team has experienced difficulties they cannot solve on their own—whether security issues or general IT challenges—the Fortinet support team has always been ready to help. According to Daniels, "If I could say anything, they are probably overly helpful. They keep our staff on track."

## Compliance Audit

With being not only a state government agency but also a financially regulated office, the Illinois State Treasurer undergoes frequent audits. Each year, the organization undergoes 12 months of internal audits and 9 months of review by an external auditor.

Daniels' team recently underwent their first information security audit, which occurs every two to five years, under his tenure. At that point, the organization had a partnership in place with Fortinet and had rewritten policies and procedures to follow the guidelines of the National Institute of Standards and Technology (NIST) and Microsoft's Security and Compliance Framework.

During the audit, Daniels says the weekly security reports provided by FortiGate Cloud were a critical resource. They provided him with the hard data necessary to answer auditors' questions and demonstrate compliance with required security controls. As a result, the audit passed without issue.

## Business Impact (contd.)

- Revealed suspicious applications lying dormant for 2-3 years through sandbox analysis
- Meets unclaimed property monitoring requirements and enables an unclaimed property "museum" with FortiCamera

## Solutions

- FortiGate NGFW with Enterprise
- FortiCare Support
- FortiSandbox
- FortiGate Cloud
- FortiCamera
- FortiAnalyzer
- FortiWeb

*"You can walk step by step, from inception to completion, through all the training videos Fortinet provides. That documentation is critical for agencies without a large staff because you can take anyone and walk them through it."*

- Joseph Daniels, Chief Information Officer, Illinois State Treasurer

However, Daniels believes in continuously working to improve his organization's security to meet evolving cyber threats. Since the audit, he has purchased FortiAnalyzer and is working to take advantage of its improved visibility and security analytics. "The FortiAnalyzer provides a much deeper dive into our network, so I am looking forward to the next audit that we have. We will be much better prepared."

## **An Integrated Platform Unlocks New Capabilities**

While network security is a significant priority for Daniels' team, it is not their only concern. The Illinois State Treasurer is also responsible for managing the lost and unclaimed property of Illinois residents. The agency's unclaimed-property division faces stringent security and auditing requirements, undergoing continuous external audits. Since the department is responsible for properly managing and securing property that belongs to Illinois citizens, every transaction and movement in the secure vaults requires constant video monitoring.

The unclaimed-property division had cameras deployed for surveillance of the vaults, but they were not meeting the organization's needs. The video feeds had poor picture quality and would occasionally fail. The team chose the FortiCamera surveillance solution to replace these impractical cameras. FortiCamera not only meets their requirements with impeccable picture quality and advanced monitoring capabilities but also seamlessly integrates into the Fortinet Security Fabric. This integration enables the security team to monitor the FortiCameras from the same dashboard as the rest of the agency's security architecture.

## **Providing an Example for Other Government Agencies**

Deploying Fortinet solutions has enabled the Illinois State Treasurer to act as an example for other state government agencies. Daniels participates in weekly calls with external agencies, where they share information about the security challenges that they are facing and how they are addressing them. According to Daniels, "Without the partnership with Fortinet, we would not have been able to shed light for our partner agencies, very similar to our own, on the importance of looking outside of the box for the way they do security."



[www.fortinet.com](http://www.fortinet.com)

## CASE STUDY

# County Government Agency Increases Visibility and Control of Entire Infrastructure

The Information Security (IS) team for Salt Lake County, Utah, supports up to 6,500 end-users across a variety of locations and business types. A team of only seven is responsible for maintaining security and managing user access for services and businesses across the entire county—including Salt Lake City.

## Replacing End-of-Life Legacy Hardware

About ten years ago, Salt Lake County first started working with Fortinet after existing security appliances from another vendor started having problems toward their end of life. They opened a request for proposals (RFP) to evaluate competing solutions. While price was a factor, they wanted physical next-generation firewalls (NGFWs) that could deliver ample performance and features for their needs at the time—which included protecting two internet feeds and two extranet partner feeds. Additionally, they knew they would need to scale their capabilities for growth in the near future.

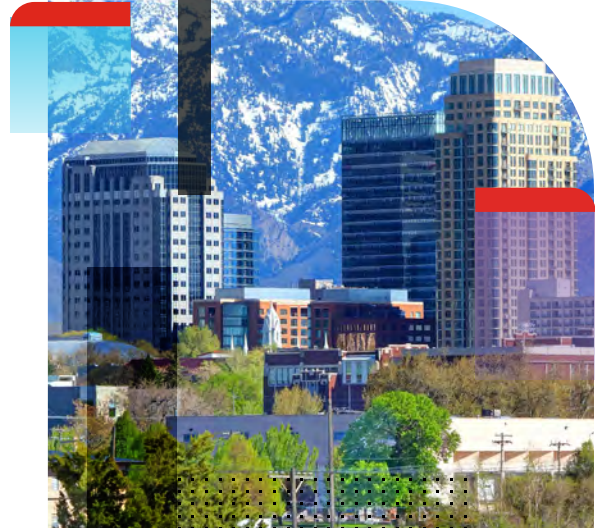
They initially chose FortiGate 600-series NGFWs for three different clusters to protect county networks. “Fortinet was miles ahead of everyone else in terms of ability and performance. That’s what impressed us. And I think Fortinet still outdoes everybody else when it comes to performance,” says Salt Lake County’s director of information security. This included the ability to perform deep packet inspections for encrypted traffic. Before working with Fortinet, the Salt Lake County IS team had spent several years unsuccessfully trying to implement inspection without bottlenecking network traffic.

## Changing Times and Growing Networks

Over the next decade, Salt Lake County would add more FortiGates to protect additional parts of the county’s infrastructure. Their current firewall deployments have scaled to 55 FortiGate NGFWs. One key reason for that expansion had to do with the growing number of county employees that needed a secure connection to the official network from home or in remote locations.

During the initial RFP, Salt Lake County was using another vendor’s solution for virtual private networking (VPN). When that vendor went out of business, they found themselves in need of a replacement. As Salt Lake County’s director of information security explains, “Rather than buy somebody else’s VPN, we just looked to our existing FortiGates. They were already licensed for VPN, we just hadn’t been using it. So really, it cost us nothing to change. And it saved us whatever the going rate would have been for a couple of VPN concentrators from someone else.”

Beyond perimeter protection and VPN access for employees, Salt Lake County also uses their FortiGates for WAN connections at remote sites, isolation of networks, and segmentation of PCI devices (e.g., point-of-sale [POS] terminals). They have also added other Fortinet security solutions to help complement specific security use-case needs.



*“Fortinet was miles ahead of everyone else in terms of ability and performance. That’s what impressed us. And I think Fortinet still outdoes everybody else when it comes to performance.”*

– Salt Lake County’s Director of Information Security

## Details

**Customer:** Salt Lake County

**Industry:** Government

**Location:** Utah

## Business Impact

- Enables network segmentation for PCI compliance via high-performance NGFW protection across distributed county-owned locations
- Provides secure remote login for county employees via robust virtual private network (VPN) and multi-factor authentication (MFA) capabilities

## Multi-factor authentication (MFA)

In addition to FortiGate's built-in VPN capabilities, the Salt Lake County IS team is also using FortiAuthenticator to add multi-factor authentication (MFA) capabilities to employee access for added security. One of the many things the county uses MFA for is timecard submissions across as many as 6,500 full- and part-time employees via their enterprise resource planning (ERP) system.

"Our biggest successes with Fortinet right now really includes two things. First, moving to Fortinet's VPN capabilities and being able to have multi-factor authentication has been awesome. And second, in the last couple of years, we wanted to add MFA to our applications. Previously, we were using a ridiculously expensive vendor for single-sign-on MFA. They had a whole year to prove themselves and they failed miserably," says Salt Lake County's director of information security.

As with their VPN problems, Salt Lake County looked to Fortinet to help serve their users without breaking their budget. They purchased an additional FortiAuthenticator appliance and FortiToken licenses to design their own solution—fulfilling their needs while dramatically reducing the total cost of ownership (TCO) for application MFA. "I'd say it's probably not even half of what we invested in that other solution. Our users like everything about using it and it has worked really well. We love it."

## Network Segmentation and PCI Compliance

At the majority of the county's branch locations, FortiGate NGFWs apply Layer 3 policies to segment certain things from the main county network that vendors need to access. Because the IS team does not want to connect vendors to any internal resources, they ensure vendor devices and users can only access what they need for their specific job functions—which minimizes risk to the broader organization.

The county's IS team also uses segmentation to ensure compliance with Payment Card Industry (PCI) regulations—ensuring that private credit card information of citizens who engage with county-owned businesses and services is kept safe from cyber criminals. This includes everything from people paying their taxes, donations to the aging center, visiting the local planetarium, or even making purchases at county golf courses and recreation centers.

## Endpoint Device Protection

After a frustratingly fruitless experience with another vendor's antivirus (AV) solution, Salt Lake County again looked to Fortinet for help. They needed to protect county-owned devices (e.g., laptops, desktops, servers) from malware and other endpoint-targeted attacks. They were already successfully using the Fortinet FortiClient solution to help manage IPsec VPN for county devices.

"We already had FortiClient. It works great on all our laptops. We thought, why don't we just use it everywhere? We already have the whole backend built. More licenses are all we have to buy. Fortinet has become kind of the Swiss Army knife when other people fail us," says Salt Lake County's director of information security.

They started using FortiClient for AV as well as off-network web filtering, which was a new capability added to the organization—helping to protect mobile devices from web-based attacks when using non-county network connections. "We keep coming back to Fortinet because the products work well and their price/performance beats the competition."

## Business Impact (contd.)

- Enabled cost-effective endpoint protection across all laptops, desktops, and servers—including antivirus (AV) and off-network filtering
- Simplified operations by centralizing network management and compliance reporting

## Solutions

- FortiGate
- FortiManager
- FortiAnalyzer
- FortiAuthenticator
- FortiToken
- FortiClient

*The biggest difference, really—things just work better. We have less frustration from the people."*

- Salt Lake County's Director of Information Security

## Centralized Management

As their infrastructure expanded, Salt Lake County security leaders also needed help managing the different Fortinet solutions they had deployed across the region. Scaling from three clusters of four firewalls each up to 55 individual FortiGate increases the need for greater visibility and centralized control. FortiManager was a perfect solution for their need to simplify network operations across all 55 firewalls.

Also, FortiAnalyzer provided real-time visibility into their FortiGate clusters while gaining insight into PCI compliance. As Salt Lake County's information security analyst explains, "It definitely is a huge advantage being able to centrally manage the devices—it saves time to where you have redundancies. You only have to manage it once instead of 55 times. If I had to go change a policy stack on ten firewalls, that's an hour and a half instead of five minutes."

## A Partnership Built on Solving Problems

The needs of any government organization are going to be unique to the place where network technologies are deployed. As demand for remote access grew over the last decade, Fortinet's proven NGFW capabilities helped pave the way for added support like VPN, MFA, and endpoint protection when other solutions could not achieve the same performance or cost benefits. Hopefully, Fortinet and Salt Lake County will continue to work together for another ten years—and beyond. "We've been a happy customer for a long time now," says Salt Lake County's director of information security.



[www.fortinet.com](http://www.fortinet.com)

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.





## CASE STUDY

# Propelling Research, Improving Efficiency, and Cutting Costs at University of South Carolina



Founded in 1801, the University of South Carolina system has eight campuses across the state, more than 50,000 students, and an annual budget in the billions of dollars today. The main campus in Columbia is recognized as one of the nation's top universities, with several of its undergraduate and graduate programs cited as number one in the country in various rankings. The university received \$258 million in research grants in FY 2018 and has an endowment of \$771 million.

Throughout 2017 and much of 2018, increased computing demand from campus researchers tested the capacity of the existing network and firewall infrastructure. The system suffered latency issues on a regular basis, frustrating students, faculty, and staff and impacting research projects. Worse yet, the network would occasionally become so overloaded that users were unable to access the network—once every three months or so during the worst stretch. “Each incident was different, but they all affected a large number of users,” recalls Jason Boryk, the lead architect and manager of the university's network architecture team.

After they devoted significant effort tweaking the existing system to prevent these problems, it became clear to the network architecture team that the existing infrastructure would need to be replaced. “What we had was not acceptable for a research university,” Boryk asserts. After meetings with internal stakeholders and university officials, the team began making plans to upgrade the university's Internet2 research network from 10 gigabits per second to 100 gigabits per second.

## Building a New Network

The team underwent a thorough planning process to build a state-of-the-art network backbone with robust security features built into the base architecture. “We did not want to just build the same network only 10 times bigger,” explains Jessie Hawkins, a systems architect for the university. “Rather, we strove to follow current best practices and build a robust, secure network that will serve us many years into the future.”

The infrastructure upgrade was concurrent with other technology changes that were in progress at the university. One pressing issue was that the on-premises data backup system was overloaded. “Our storage area network [SAN] was constantly at 97% of capacity, which is far more than recommended,” Hawkins says. “Rather than spend millions of dollars on more SAN capacity, we decided that we would move our backups to a cloud repository in Amazon Web Services.”

*“The ability to view the entire infrastructure on a single pane of glass is a huge benefit to our architecture, network, and security teams.”*

– Jessie Hawkins, Systems Architect,  
University of South Carolina

## Details

**Customer:** University of South Carolina

**Industry:** Education

**Location:** Columbia, South Carolina, USA

This change in the backup infrastructure was consistent with a university strategy that called for a gradual move to the cloud for most services. “In designing solutions for new applications and services, we are leveraging public and private cloud infrastructures to create a level of redundancy and stability that benefits an institution of our size,” notes Boryk. “Our goal is to gradually move legacy services to the cloud as well. Long term, we hope to use the cloud for high-availability and disaster-recovery purposes.”

## Incorporating a Robust Security

As they searched for a security solution to protect the new infrastructure, the university's team knew that it must support both on-premises and cloud-based resources, including backups to AWS. They also hoped to find a way to integrate all of the elements of the security infrastructure for centralized visibility and control.

“We have services with Azure, Amazon Web Services, and Google Cloud Platform,” Hawkins explains. “We were previously using the built-in security tools from each provider. The problem was that each tool worked a little differently. This meant that our small team had to specialize in three platforms, and the security team had to correlate security data from the three platforms manually.”

In the last half of 2018, the team underwent proofs of concept from three next-generation firewall (NGFW) vendors that included Fortinet. “We tested the ease of configuration, the general user-friendliness of the interface, the accuracy of the vendors' claims about throughput, processing power, and different firewall features,” Boryk says. “In short, we wanted a firewall solution that would scale to our current and future needs.”

## Selecting a Security Solution

FortiGate NGFWs quickly moved to the top of the list among the three major providers included in the proof of concept for several reasons. “Fortinet had, by far, the most scalable solution,” Boryk begins. “Its native 100-gigabit interface was a perfect fit for our new infrastructure, whereas no other vendor had comparable levels of throughput. Additionally, configuration was a much easier process than with the other firewalls, and in general, the FortiGate NGFWs were much easier to work with.”

Another major benefit of FortiGate NGFWs was the ability to integrate the entire security architecture—from the new data center infrastructure to the three cloud platforms—using the Fortinet Security Fabric. “The ability to view the entire infrastructure on a single pane of glass is a huge benefit to our architecture, network, and security teams,” Hawkins relates. The Fortinet Security Fabric provides an integrated security architecture to ensure that incident detection and response and remediation efforts are fully coordinated and optimally effective.

## Deploying the NGFWs

The university began by deploying six FortiGate 7060E NGFWs in the data center at its main campus, pushing them live in January 2019. “We opted for the top-of-the-line boxes because of our speed requirements and the relative ease of configuration at the scale where we are operating,” Hawkins explains. The team deployed FortiManager and FortiAnalyzer at the same time to provide centralized management, security automation, and robust reporting capabilities.

## Business Impact

- Reallocated 40 to 80 staff hours monthly for architecture team due to stability of new network infrastructure
- \$5 million cost avoidance for SSL/TLS inspection appliances required for competing solutions
- 27 staff hours in potential savings for each VPN setup
- 180 staff hours per year saved on a single, semiweekly report produced by the network team
- 15% reduction in storage cost
- Better coordination among the architecture, network, and security teams via centralized management and visibility

## Solutions

- FortiGate
- FortiManager
- FortiAnalyzer
- FortiSandbox Cloud
- Fortinet Professional Services
- Fortinet Network Security Academy
- FortiCare First program (Advanced Services technical support contract)

While the team currently routes all cloud traffic through the physical boxes using virtual domains (VDMs), they are conducting a trial of FortiGate VM virtual NGFWs to eventually protect virtual and cloud resources. “We expect the ease of configuration to be even greater with the virtual firewalls, which will be integrated seamlessly with the physical ones,” Boryk states.

The network team has activated, or is planning to activate, the secure sockets layer (SSL)/transport layer security (TLS) encryption, application control, intrusion prevention system (IPS), antivirus, and web filtering functionalities in the NGFW. “Having the SSL/TLS encryption built into the firewall was a requirement from our security team,” Boryk explains. “Other vendors we considered did not have the same level of capability and integration we needed without having to invest in separate SSL/TLS inspection appliances, integrate them into the network, and spend valuable time managing them.”

## Getting a Jump-start with Fortinet Services

The university received assistance with the initial deployment from a resident engineer from Fortinet Professional Services. “During our first engagement, our engineer got the firewalls up and functioning, explained configuration and troubleshooting to us, and deployed FortiManager and FortiAnalyzer,” Boryk remembers. “We also purchased an additional three-month engagement, during which we hope to create a more comprehensive firewall strategy and start working to thin our legacy rule set.” Streamlining the rule set is the second step of a process that began with migrating more than 10,000 rules—many of them obsolete—from their old infrastructure using tools from Fortinet.

The university also purchased a FortiCare First program (Advanced Services technical support contract), which assigns a dedicated technical account manager (TAM) who works alongside the university’s team to prioritize and coordinate support services. The team also invested heavily in training from the Fortinet Network Security Academy. “Everyone on the architecture, network, and security teams will receive full, classroom-based training on managing the solution,” Boryk comments.

## Achieving Impressive Results

In the short time since the initial deployment, the university is already seeing tangible results and can project further future gains based on preliminary results. The larger network upgrade project has stabilized the network and helped Boryk’s team reclaim a lot of time. “Just keeping the network stable required 10 to 20 hours per month for each of our four team members—or a total of 40 to 80 hours monthly,” he says. “On top of that, the events when our network required all hands on deck to return it to a stable state could sometimes require a full day of work for each of us. Getting that time back means that we can move on to strategic projects.”

Enabling cloud backup also promises significant savings for the university, with a significant number of backups slated to move to Azure by December 2019. “Backup administration time has already been sharply reduced, and the cost of backing up to the cloud is much lower than with our SAN,” Hawkins reports. “We expect a 15% annual saving in storage costs once we’re fully up and running with cloud backups.”

Leveraging built-in features such as the intrusion prevention system (IPS) in the FortiGate NGFW will also result in reduced licensing costs. “We currently have a separate point solution for IPS,” Boryk explains. “Once we turn on the FortiGate IPS, we will save significantly in licensing and management overhead per year in costs for that solution.”

Centralizing security operations on the FortiGate NGFWs is resulting in operational efficiencies as well. “We recently had to set up VPNs for private addressing from the university to one of our cloud providers,” Hawkins states. “That project required 28 staff hours but would have taken just a few minutes if our FortiGate NGFWs had been set up.” Another example of efficiency savings: one twice-a-week report produced by the network team now takes just a few minutes with FortiManager, compared with two hours previously. This saves 180 staff hours per year.



Better coordination among the architecture, network, and security teams is another benefit of the FortiGate NGFW and the Fortinet Security Fabric. “All our teams now use FortiManager and FortiAnalyzer to view status and run reports,” Hawkins relates. “It really contributes to a more coordinated and less siloed way of doing our jobs. And this benefit will grow as new elements are added to the Fortinet Security Fabric.”

## Completing the Transformation

The University of South Carolina team expects to have the new network backbone and the entire Fortinet Security Fabric fully deployed by summer of 2020. “It was a massive undertaking, but the benefits we are already seeing make the effort well worth it,” Boryk contends. “Our relationship with Fortinet has been more than positive. Everyone has been really supportive and has gone out of their way to ensure our success.”



[www.fortinet.com](http://www.fortinet.com)

## CASE STUDY

# Illinois Century Network Partners with Fortinet to Protect K-12 Broadband Connectivity

High-speed internet is absolutely vital to modern K-12 education. That may seem obvious, but a lack of broadband connectivity can have a severe impact on both student learning and school operations. To support equity in education statewide, the Illinois State Board of Education and Illinois Board of Higher Education teamed up in 2000. They developed the member-driven Illinois Century Network (ICN) to provide internet connectivity to every public K-12 school in the state, free of charge.

"It is pretty clear that students who do not have access to high-speed internet cannot participate in the modern world of rich-media, interactive content, and live interactive video sessions or streaming video," says Robin Woodsome, manager, ICN Field Operations. "For schools across the country, the new teaching models are driving a need for more bandwidth."

Administrative and other functions also suffer without high-speed connectivity. "Universities require K-12 schools to have high-speed bandwidth in order to participate in their research projects," adds Frank Walters, network architect for ICN. "Lack of broadband availability reduces students' opportunities and preparedness for university or college."

That is why, when Governor Pritzker launched Connect Illinois to expand the state's broadband capabilities in 2019, he dedicated substantial resources to upgrading the ICN network. "Governor Pritzker sees broadband connectivity as a utility, similar to electricity and water, streets and roads," explains Dale Walters, chief of network operations for the state of Illinois. "Through Connect Illinois, he provided \$20 million to the Illinois Century Network, to bring broadband internet to our public K-12 education institutions."

## Schools' WAN Service Must Be Secure

The ICN's infrastructure was dated, so the project focused on "upgrading to new optical networking hardware that could support speeds up to 100 Gbps," Dale Walters says. "Our goal was to build a broadband infrastructure to support the needs of K-12 public schools in every corner of the state—not only their current needs, but their needs for the next several years as well."

As the ICN team designed this new broadband network, security was a key concern. "Many school districts struggle with security," Frank Walters says. "Doing it properly is difficult and expensive, and experts are hard to find in some regions of the state. So, when we were strategizing how to get the schools the connectivity they need, we knew that we needed to provide a system that would be as secure as we could make it."



*"Our goal was to build a broadband infrastructure to support the needs of K-12 public schools in every corner of the state—not only their current needs, but their needs for the next several years as well."*

– Dale Walters, Chief of Network Operations, Illinois Century Network

## Details

**Customer:** Illinois Century Network

**Industry:** Government

**Location:** Springfield, Illinois

## Business Impact

- Secures broadband connectivity for schools statewide
- Adds no measurable latency to schools' internet traffic
- Minimizes total cost of ownership (TCO) for high-performance network security
- Minimizes staff time required for firewall management

They decided to design a wide-area network (WAN) that would be a safe place for schools to communicate with one another, he adds. “And then we would have a single presentation of those K-12 schools to the internet, through the firewalls that we provide. This became top-of-mind when the COVID-19 pandemic hit, because we saw a significant uptick in both ransomware and DDoS [distributed denial-of-service] attacks on our schools.”

Frank Walters emphasizes that the ICN's intention was not to provide all the security that a school or district would need. “We are not dipping into their local IT environments and trying to take over,” he says. “We want to assist schools with the needs that they identify, and whether they take advantage of our services is totally optional. Some schools opt to maintain the security solutions they already have in place. But we knew that since we would be providing those last-mile circuits for them, we also needed to provide an outer layer of security.”

### Protecting Schools at the WAN Edge

The Illinois Century Network sought a firewall solution for the WAN edge. They had previously been standardized with a different solution, but a cost-benefit analysis brought Fortinet to the forefront. “It is always risky to step away from what you know,” says Frank Walters. “But the state encouraged us to review the total cost of ownership [TCO] of each choice—not just the up-front purchase cost, but the cost of maintaining it, the cost of training, the whole ball of wax. When we started looking at the numbers, Fortinet stood out.”

The state imposed a tight deadline to complete the ICN broadband infrastructure. Initially, all participating schools’ internet traffic passed through the Chicago data center. The team rolled out a pair of FortiGate next-generation firewalls (NGFWs) to secure that traffic.

“We had to move quickly to meet the state deadline, so we implemented the firewalls in standalone mode,” says Andre Bouravnev, network supervisor for ICN. “That is changing. We have worked closely with Fortinet engineers to determine the best configuration of the firewalls. Since the deployment, we switched to a standby-active configuration for failover. The next step is to bring a second pair of FortiGate firewalls online in Springfield.”

The team is considering transitioning both NGFW pairs to active-active status, with load balancing between the two. Bouravnev reports that they will soon begin testing.

### Fortinet Generates Substantial TCO Savings

The NGFWs are already exceeding expectations. “We are now providing schools with an environment that is exactly what we said it would be,” says Frank Walters. “The security piece was crucial, and Fortinet was very helpful throughout the process in making sure everything was configured right for the schools.”

Currently, over 200 districts representing about 1,660 schools utilize the ICN, and more than 100 of those are taking advantage of the new broadband firewall services. Others have their own firewalls at the headend where their local-area network (LAN) connects to the ICN. Whether to take this layered security approach is up to district administrators.

“This is extremely beneficial to schools in underserved parts of the state, where broadband is not readily available,” Woodsome says. “Because we provide secure broadband service at no cost, we are helping those districts catch up so that they can deploy the same types of learning programs as schools in areas of the state where access is more readily available.”

### Solutions

- FortiGate
- FortiManager
- FortiAnalyzer

*“It is always risky to step away from what you know, but the state encouraged us to review the total cost of ownership [TCO] of each choice. When we started looking at the numbers, Fortinet stood out.”*

– Frank Walters, Network Architect,  
Illinois Century Network

The FortiGate NGFWs support those historically underserved schools by protecting traffic without introducing any latency. “We have done really thorough performance testing in the past few months, of different components of our network,” Bouravnev reports. “We have isolated the FortiGates and have not found any delay to customer traffic going through the firewall. Everything looks really good.”

For the ICN, the ability to minimize TCO while securing schools’ high-performance connectivity was key. Bouravnev estimates that with the Fortinet solution, ICN will save millions of dollars in capital and operating expenses over the next five years.

Network administrators use FortiManager to streamline and centralize configuration of the FortiGate NGFWs. They also use FortiAnalyzer for reporting and analysis of security events on the network. “We are very new to Fortinet, so we are still learning to get the most out of the tools,” Bouravnev says. “So far, though, we have been pleased, although the FortiGate is a fairly complex and sophisticated firewall, the GUI [graphical user interface] navigation of the firewall and the management tools is not complex. Unlike some security tools we have worked with previously, the Fortinet interface makes everything easy to find. The documentation and support are good as well.”




Ultimately, Bouravnev says, the ICN team is pleased with Fortinet. “We did not need a firewall that was overly complex, and we wanted it to be easy to manage and not require a lot of staff time. At the same time, we needed a network that could perform past 100 gigs. The Fortinet solutions match our needs well.”






[www.fortinet.com](http://www.fortinet.com)

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

# Fortinet Training: NSE Certification Levels

Cybersecurity Awareness Certification		
	Information Security Awareness is the entry-level certification in the program. You will be introduced to today's cyberthreats and advised on how you can secure your information. You must successfully complete all lessons and pass all quizzes within the Information Security Awareness course to obtain the NSE 1 Certification.	Ideal for: Everyone Get started with <a href="#">NSE 1</a>
	After you develop a solid understanding of the threat landscape and the problems facing organizations and individuals, you will learn about the evolution of cybersecurity. In the second level, you will learn about the types of security products that have been created by security vendors to address security problems faced by networks and organizations.	Ideal for: Everyone Get started with <a href="#">NSE 2</a>
	NSE 3 introduces you to key Fortinet products and describes the cybersecurity problems they solve. The product lessons and use cases in this course are organized into the following Fortinet Security Fabric pillars: Security-Driven Networking, Zero Trust Access, Adaptive Cloud Security, and Security Operations.	Ideal for: Everyone Get started with <a href="#">NSE 3</a>

## Cybersecurity Technical Certification

	NSE 4 identifies your ability to configure, install, and manage the day-to-day configuration, monitoring, and operation of a FortiGate device to support specific corporate network security policies.	Ideal for: Network Security Administrators, Technical Support Engineers and System Engineers Get started with <a href="#">NSE 4</a>
	NSE 5 recognizes your ability to implement network security management and analytics using Fortinet security devices. The curriculum is recommended for those who require the expertise to centrally manage, analyze, and report on Fortinet security devices. This designation is recognized when you successfully pass a minimum of any two Fortinet NSE 5 certification exams.	Ideal for: Network Security Administrators, Technical Support Engineers and System Engineers Get started with <a href="#">NSE 5</a>
	NSE 6 recognizes comprehensive skills with fabric products beyond the firewall. This designation is recognized after you achieve at least four Fortinet Specialist certificates on Fortinet enhanced products, and is recommended for those who are involved in managing and supporting specific Fortinet security products.	Ideal for: Network Security Administrators, Technical Support Engineers and System Engineers Get started with <a href="#">NSE 6</a>

## Cybersecurity Advanced Certification



NSE 7 identifies your advanced skills in deploying, administering, and troubleshooting Fortinet security solutions. This curriculum offers courses for network and security professionals who are involved in advanced administration and support of security infrastructures using Fortinet solutions. You must successfully pass at least one of the NSE 7 exams to obtain this certification.

Ideal for:  
IT Security  
Architects,  
Network  
Security  
Administrators,  
Technical  
Support  
Engineers and  
System  
Engineers  
Get started  
with [NSE 7](#)

## Cybersecurity Expert Certification



The NSE 8 Fortinet Network Security Expert designation identifies your comprehensive and expert knowledge of network security design, configuration, and troubleshooting for complex networks. To attempt the exam, candidates must have related industry experience. We recommend that you complete the appropriate Professional, Analyst, Specialist, and Architect designation training and have extensive experience with Fortinet products in a production environment. The Fortinet Network Security Expert designation does not include training.

Ideal for:  
Network  
Security  
Cybersecurity  
Professionals  
Get started  
with [NSE 8](#)





## Product License Agreement / EULA and Warranty Terms

### Product License Agreement

The parties to this agreement are you (the end-customer) and Fortinet, Inc. ("Fortinet"). CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (THE OR THIS "AGREEMENT" OR "EULA"). USE OR INSTALLATION OF FORTINET PRODUCT(S) AND ANY UPDATES THERETO, INCLUDING HARDWARE APPLIANCE PRODUCTS, SOFTWARE AND FIRMWARE INCLUDED THEREIN BY FORTINET, AND STAND-ALONE SOFTWARE PRODUCTS SOLD BY FORTINET (TOGETHER, THE "PRODUCTS") CONSTITUTES ACCEPTANCE BY YOU OF THE TERMS IN THIS AGREEMENT, AS AMENDED OR UPDATED FROM TIME TO TIME IN FORTINET'S DISCRETION BY FORTINET PUBLISHING AN AMENDED OR UPDATED VERSION. FORTINET SHALL NOT BE BOUND BY ANY ADDITIONAL AND/OR CONFLICTING PROVISIONS IN ANY ORDER, RELEASE, ACCEPTANCE OR OTHER WRITTEN CORRESPONDENCE OR OTHER WRITTEN OR VERBAL COMMUNICATION UNLESS EXPRESSLY AGREED TO IN A WRITING SIGNED BY THE GENERAL COUNSEL OF FORTINET. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT START THE INSTALLATION PROCESS OR USE THE PRODUCTS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, YOU SHOULD IMMEDIATELY, AND IN NO EVENT LATER THAN FIVE (5) CALENDAR DAYS AFTER YOUR RECEIPT OF THE PRODUCT, IMMEDIATELY NOTIFY FORTINET LEGAL [LEGAL@FORTINET.COM](mailto:LEGAL@FORTINET.COM) OF REQUESTED EULA CHANGES.

#### 1. License Grant.

This is a license agreement between you and Fortinet, not a sales agreement. The term "Software", as used throughout this Agreement, includes all Fortinet and third party firmware and software provided to you with, or incorporated into, Fortinet appliances and any stand-alone software provided to you by Fortinet, with the exception of any open source software contained in Fortinet's Products which is discussed in detail in section 15 below, and the term "Software" includes any accompanying documentation, any updates and enhancements of the software or firmware provided to you by Fortinet, at its option. Fortinet grants to you a non-transferable (except as provided in section 5 ("Transfer") and section 15 ("Open Source Software") below), non-exclusive, revocable (in the event of your failure to comply with these terms, in the event of termination, or in the event Fortinet is not properly paid for the applicable Product) license to use the Software solely for your internal business purposes (provided, if (a) agreed by Fortinet in writing, (b) you are authorized by Fortinet in writing to provide managed service provider services ("MSSP") to your end-customers, and (c) you pay for an MSSP license, then you may use the Software and/or Software embedded in Fortinet Hardware to provide those services, subject to the other restrictions in this Agreement), in accordance with the terms set forth in this Agreement and subject to any further restrictions in Fortinet documentation (including license term restrictions), and solely on the Fortinet appliance, or, in the case of blades, CPUs, platform, devices or databases, on the single blade, CPU, platform, device or database on which Fortinet installed the Software, or, for stand-alone Software, solely on a single computer running a validly-licensed copy of the operating system for which the Software was designed unless and except set forth in the published documentation otherwise. For clarity, notwithstanding anything to the contrary, all licenses of Software to be installed on blades, CPUs, platforms, devices or databases are licensed per blade, solely for one blade and not for multiple blades that may be installed in a chassis, per CPU, per platform, per device, or per database basis, up to the blade, CPU, platform, device, database number defined in the license and as applicable and in accordance with the documentation. The Software is "in use" on any appliances, blades, CPUs, platforms, devices, or databases when it is loaded into temporary memory (i.e. RAM), accessed, downloaded, installed, or used on an appliance, blade, CPU, platform, device, or database. You agree that, except for the limited, specific license rights granted in this section 1, you receive no license rights to the Software.

#### 2. Limitation on Use.

You are prohibited from and may not attempt to, and, if you are a corporation, you are responsible to prevent your employees and contractors from attempting to: (a) modify, translate, reverse engineer, decompile, disassemble, create derivative works based on, sublicense, or distribute the Software; (b) rent or lease any rights in the Software in any form to any third party or make the Software available or accessible to third parties in any other manner (except as expressly permitted for MSSP partners); (c) transfer assignment or sublicense right to any other person or entity (except as provided in section 5); (d) remove any proprietary notice, labels, or marks on the Software, Products, and containers; (e) use the Software to determine, or disclose the results of, any benchmarking or performance measurements; (f) interfere with a platform for use of the Software; (g) use the Software on a device not owned and controlled by you; (h) use automated means to access online portions of the platform for the Software; (i) use the Software for third-party training, commercial time-sharing or service bureau use or (except as expressly set forth in this Agreement) use the Software to provide services to third parties; (j) share non-public features or content of the software with any third party; (k) access the software in order to build a competitive product or service, to build a product using similar ideas, features, functions or graphics of the software, or to copy any ideas, features, functions or graphics of the software; or, (l) engage in web scraping or data scraping on or related to the software, including without limitation, collection of information through any software that simulates human activity or any bot or web crawler.

#### 3. Proprietary Rights.

All rights (including copyrights, trade secret, patent and other intellectual property rights), title, interest in and to the Software and any Product, and any copy thereof remain with Fortinet. You acknowledge that no title or other intellectual property rights in the Software or other Products is transferred to you and you will not acquire any rights to the Software or other Products except for the specific limited license as expressly set forth in section 1 ("License Grant") above. You expressly agree and acknowledge that Fortinet owns, retains, and shall retain all intellectual property rights in and to, and you have no intellectual property rights in and to, the Products and the Software other than the License Grant. You agree to keep confidential all Fortinet confidential information and only to use such information for the purposes for which Fortinet disclosed it.

#### 4. Term and Termination.

The term of the license is the shorter of (a) the term as set forth in the ordering documents, other Fortinet documentation, or per Fortinet practices or policies (such as with evaluation or beta licenses or subscription or other term licenses) and (b) for the duration of Fortinet's copyright in the Software. Fortinet may terminate this Agreement, and the licenses and other rights herein, immediately without notice if you breach or fail to comply with any of the terms and conditions of this Agreement or for other reasons as stated in Fortinet's other documentation. You agree that, upon such termination, you will cease using the Software and any Product and either destroy all copies of the Fortinet documentation or return all materials to Fortinet.

#### 5. Transfer.

If you are a Fortinet contracted and authorized reseller or distributor of Products, you may transfer (not rent or lease unless specifically agreed to in writing by Fortinet) the Software to one end user on a permanent basis, provided that: (a) you ensure that your customer and the end user receives a copy of this Agreement, is bound by its terms and conditions, and, by selling the Product or Software, you hereby agree to enforce the terms in this Agreement against such end user, (ii) you at all times comply with all applicable United States export control laws and regulations, and (iii) you agree to refund any fees paid to you by an end user who purchased Product(s) from you but does not agree to the terms contained in this Agreement and therefore wishes to return the Product(s) as provided for in this Agreement. Further, if you are a non-authorized reseller of Products and Services, you are not authorized to sell Product(s), Software or Services, but, regardless, by selling Product(s), Software or Services, you hereby agree you are bound by the restrictions and obligations herein and are bound to: (i) ensure that your customer and the end user receives a copy of this Agreement and are bound in full by all restrictions and obligations herein (ii) enforce the restrictions and obligations in this Agreement against such customer and/or end user, (iii) comply with all applicable United States export control laws and regulations and all other applicable laws, and (iv) refund any fees paid to you by a customer and/or end user who purchased Product(s) from you but does not agree to the restrictions and obligations contained in this Agreement and therefore wishes to return the Product(s) as provided for in this Agreement. Notwithstanding anything to the contrary, distributors, resellers and other Fortinet partners (a) are not agents of Fortinet and (b) are not authorized to bind Fortinet in any way. Fortinet's license, warranty, and support is only available for Products that you purchased directly from an authorized Fortinet channel partner. Products not purchased from an authorized Fortinet channel partner are not eligible, will not be supported, and may be blocked from registration.

#### 6. Limited Warranty.

Fortinet provides this limited warranty for its product only to the single end-user person or entity that originally purchased the Product from Fortinet or its authorized reseller or distributor and paid for such Product. The warranty is only valid for Products which are properly registered on Fortinet's Support Website: <https://support.fortinet.com>, or such other website as provided by Fortinet, or for which the warranty otherwise starts according to Fortinet's policies, and any support is only valid for products properly purchased through authorized distributors and resellers. The warranty periods discussed below will start according to Fortinet's policies passed

at <http://www.fortinet.com/about-us/legal.html> or such other website as provided by Fortinet. It is the Fortinet distributor's and reseller's responsibility to make clear to the end user the date the product was originally shipped from Fortinet, and it is the end user's responsibility to understand the original ship date from the party from which the end user purchased the product. All warranty claims must be submitted in writing to Fortinet before the expiration of the warranty term or such claims are waived in full. Fortinet provides no warranty for any beta, donation or evaluation Products. Fortinet warrants that the hardware portion of the Products ("hardware") will be free from material defects in workmanship as compared to the functional specifications for the period set forth as follows and applicable to the Product type ("Hardware Warranty Period"): (a) a three hundred sixty-five (365) day limited warranty for the Hardware products; (b) for FortiAP, the warranty herein shall last from the start of the warranty period as discussed above until five (5) years following the product announced end-of-life date Hardware; (c) for FortiSwitch Hardware appliance products other than the FortiSwitch-5000 series, the warranty herein shall last from the start of the warranty period as discussed above until five (5) years following the product announced end-of-life date Hardware. Fortinet's sole obligation shall be to repair or offer replacement Hardware for the defective Hardware at no charge to the original owner. This obligation is exclusive of transport fees, labor, de-installation, installation, reconfiguration, or return shipment and handling fees and costs, and Fortinet shall have no obligation related thereto. Such repair or replacement will be rendered by Fortinet at an authorized Fortinet service facility as determined by Fortinet. The replacement Hardware need not be new or of an identical make, model, or part; Fortinet may, in its discretion, replace the defective Hardware (or any part thereof) with any reconditioned Product that Fortinet reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. The Hardware Warranty Period for the repaired or replacement Hardware shall be for the greater of the remaining Hardware Warranty Period or ninety days from the delivery of the repaired or replacement Hardware. If Fortinet determines in its reasonable discretion that a material defect is incapable of correction or that it is not practical to repair or replace defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by Fortinet upon return to Fortinet of the defective Hardware. All Hardware (or part thereof) that is replaced by Fortinet, or for which the purchase price is refunded, shall become the property of Fortinet upon replacement or refund. Fortinet warrants that Software as initially shipped by Fortinet will substantially conform to Fortinet's then-current functional specifications for the Software, as set forth in the applicable documentation for a period of ninety (90) days ("Software Warranty Period"), if the Software is properly installed on approved Hardware and operated as contemplated in its documentation. Fortinet's sole obligation shall be to repair or offer replacement Software for the non-conforming Software with software that substantially conforms to Fortinet's functional specifications. This obligation is exclusive of transport fees, labor, de-installation, installation, reconfiguration, or return shipment and handling fees and costs, and Fortinet shall have no obligation related thereto. Except as otherwise agreed by Fortinet in writing, the warranty replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by Fortinet for the Software. The Software Warranty Period shall extend for an additional ninety (90) days after any warranty replacement software is delivered. If Fortinet determines in its reasonable discretion that a material non-conformance is incapable of correction or that it is not practical to repair or replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by Fortinet; provided that the non-conforming Software (and all copies thereof) is first returned to Fortinet. The license granted respecting any Software for which a refund is given automatically terminates immediately upon refund. For purpose of the above hardware and software warranties, the term "functional specifications" means solely those specifications authorized and published by Fortinet that expressly state in such specifications that they are the functional specifications referred to in this section 6 of this Agreement, and, in the event no such specifications are provided to you with the Software or Hardware, there shall be no warranty on such Software.

#### 7. Disclaimer of Other Warranties and Restrictions.

EXCEPT FOR THE LIMITED WARRANTY SPECIFIED IN SECTION 6 ABOVE, THE PRODUCT AND SOFTWARE ARE PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY, IMPLIED OR EXPRESS WARRANTY OF MERCHANTABILITY, OR WARRANTY FOR FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS FROM THE DATE OF ORIGINAL SHIPMENT FROM FORTINET. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT. NOTWITHSTANDING ANYTHING TO THE CONTRARY, THE HARDWARE WARRANTY PERIOD DISCLOSED HEREIN DOES NOT APPLY TO CERTAIN FORTINET PRODUCTS, INCLUDING FORTINET FORTIAP, AND THE SOFTWARE WARRANTY DOES NOT APPLY TO CERTAIN FORTINET PRODUCTS. YOU HEREBY ACKNOWLEDGE AND AGREE THAT NO VENDOR CAN ASSURE COMPLETE SECURITY AND NOTHING HEREIN OR ELSEWHERE SHALL BE DEEMED TO IMPLY A SECURITY GUARANTEE OR ASSURANCE, AND FORTINET DISCLAIMS LIABILITY REGARDING YOUR WEB BROWSER'S REQUIREMENTS OR ANY THIRD PARTY DEVICE OR APPLIANCE USED TO OPERATE THE SOFTWARE.

The warranty in Section 6 above does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Fortinet or its authorized representative, (b) has not been installed, operated, repaired, updated to the latest version, or maintained in accordance with instructions supplied by Fortinet, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; (d) is licensed for beta, evaluation, donation, testing or demonstration purposes or for which Fortinet does not charge a purchase price or license fee; or (e) is procured from a non-authorized reseller or non-authorized distributor. In the case of beta, testing, evaluation, donation or free Software or Product, the end user acknowledges and agrees that such Software or Product may contain bugs or errors and could cause system failures, data loss and other issues, and the end user agrees that such Software or Product is provided "as-is" without any warranty whatsoever, and Fortinet disclaims any warranty or liability whatsoever. An end user's use of evaluation or beta Software or Product is limited to thirty (30) days from original shipment unless otherwise agreed in writing by Fortinet. For clarity, notwithstanding anything to the contrary, all sales are final and no provision in this EULA entitles you to return Products, other than as expressly set forth herein.

#### 8. Governing Law.

Any disputes arising out of this Agreement or Fortinet's limited warranty shall be governed by the laws of the state of California, without regard to the conflict of laws principles. In the event of any disputes arising out of this Agreement or Fortinet's limited warranty, the parties submit to the jurisdiction of the federal and state courts located in Santa Clara County, California, as applicable, and agree that any controversy or claim arising out of or relating to this Agreement shall be determined in the federal and state courts located in Santa Clara County, California, as applicable.

#### 9. Limitation of Liability.

TO THE MAXIMUM EXTENT PERMITTED BY LAW AND NOTWITHSTANDING ANYTHING TO THE CONTRARY, FORTINET IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY, INFRINGEMENT OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT OR SERVICE OR ANY DAMAGES OF ANY KIND WHATSOEVER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF PROFIT, LOSS OF OPPORTUNITY, LOSS OR DAMAGE RELATED TO USE OF THE PRODUCT OR SERVICE IN CONNECTION WITH HIGH RISK ACTIVITIES, DE-INSTALLATION AND INSTALLATION FEES AND COSTS, DAMAGE TO PERSONAL OR REAL PROPERTY, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, COMPUTER SECURITY BREACH, COMPUTER VIRUS INFECTION, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT INCLUDING ANY PRODUCT RETURNED TO FORTINET FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THE LIMITED WARRANTY IN SECTION 6 ABOVE, EVEN IF FORTINET HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE LIMITED WARRANTY IS, AT FORTINET'S SOLE AND ABSOLUTE DISCRETION: REPAIR, REPLACEMENT, OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT AS SPECIFICALLY STATED IN SECTION 6 ABOVE; PROVIDED, HOWEVER, IN NO EVENT SHALL ANY END-CUSTOMER REMEDIES UNDER THIS EULA AND ANY SUPPORT AGREEMENT EXCEED THE AMOUNT PAID TO FORTINET FOR THE SPECIFIC APPLICABLE DEFECTIVE OR NON-CONFORMING PRODUCT AT ISSUE.

#### 10. Compliance with Laws, including Import/Export Laws and FCPA.

You are advised that the Products may be subject to the United States Export Administration Regulations and other import and export laws and regulations known to United States law and regulation is prohibited. You agree to comply with all applicable international and national laws that apply to the Products as well as end user, end-use, and destination restrictions issued by U.S. and other governments. For additional information on U.S. export controls see <https://www.bis.doc.gov>. Fortinet assumes no responsibility or liability for your failure to obtain any necessary import and export approvals and licenses, and Fortinet reserves the right to terminate or suspend shipments, services and support in the event Fortinet has a reasonable basis to suspect any import or export violation. You represent that neither the United States Bureau of Industry and Security nor any other governmental agency has issued sanctions against you or otherwise suspended, revoked or denied your export privileges. You agree not to use or transfer the Products for any use relating to nuclear, chemical or biological weapons, or missile technology, unless authorized by the United States Government by

regulation or specific written license. Additionally, you agree not to directly or indirectly export, import or transmit the Products contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or use. Furthermore, you hereby agree that, for any orders that you place with Fortinet whereby any legal or regulatory requirements may apply to Fortinet such as requirements related to the International Traffic in Arms Regulations, or Buy American Act, or the Trade Agreements Act: you are responsible to ensure the Purchase Order submitted to Fortinet by you and/or any partners clearly states the specific requirement in writing, or otherwise Fortinet is not bound by any such requirements. You represent that you understand, and you hereby agree to comply with, all applicable laws including but not limited to the U.S. Foreign Corrupt Practices Act. You represent that you hereby agree that you and your employees have not accepted, and will not accept, anything of value, including money, meals, entertainment, paid-for travel, beta, testing, evaluation, donation or free Products and/or related services, or anything else of value, in exchange for Fortinet maintaining current business or for new business opportunities. You represent and warrant to Fortinet that you and your employees, consultants, agents and representatives will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving censorship, surveillance, detention, or excessive use of force. You agree you and your employees will be responsible to comply in full with all laws and policies applicable to any and all dealings with Fortinet in general and its distributors, resellers and partners.

#### 11. U.S. Government End Users.

The Software and accompanying documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement and its successors.

#### 12. Tax Liability.

You agree to be responsible for payment of any sales or use taxes imposed at any time on this transaction.

#### 13. General Provisions.

Except as specifically permitted and required in section 5 ("Transfer") above, you agree not to assign this Agreement or transfer any of the rights or obligations under this Agreement without the prior written consent of Fortinet. This Agreement shall be binding upon, and inure to the benefit of, the successors and permitted assigns of the parties. The United Nations Convention on Contracts for the International Sales of Goods is expressly excluded. This Agreement and other Fortinet Agreements may be amended or supplemented only by a writing that refers explicitly to the agreement signed on behalf of both parties, or, for this Agreement, as otherwise expressly provided in the lead-in above Section 1 above, provided, notwithstanding anything to the contrary and except for this Agreement which may be amended or updated as expressly provided in the lead-in above Section 1 above, for any amendment or other agreement to be binding on Fortinet, such amendment or other agreement must be signed by Fortinet's General Counsel. No waiver will be implied from conduct or failure to enforce rights nor effective unless in a writing signed on behalf of the party against whom the waiver is asserted. If any part of this Agreement is found unenforceable, that part will be enforced to the maximum extent permitted and the remainder shall continue in full force and effect. You acknowledge that you have read this Agreement, understand it, and agree to be bound by its terms and conditions. Notwithstanding anything to the contrary, this EULA constitutes the entire agreement between Fortinet and its end-customers and supersedes any and all prior representations or conflicting provisions, such as limitations of liability, warranties, or otherwise in any and all purported end customer agreements, whether entered into now or in the future. In the event of a conflict between this EULA and another agreement, this EULA shall prevail unless the conflicting agreement expressly states that it replaces this EULA, expressly referring to this EULA, and is agreed to in writing by authorized representatives of the parties (which, in the case of Fortinet, is Fortinet's General Counsel).

#### 14. Privacy.

You agree to Fortinet's collection, use, disclosure, protection and transfer of your information, as set forth in the Fortinet privacy policy on the Fortinet web site (<http://www.fortinet.com/about-us/privacy.html>), including (a) Fortinet's use of the Customer information to send information regarding Fortinet products and services; and (b) Fortinet's disclosure of your information to provide assistance to law enforcement, governmental agencies and other authorities or to allow Fortinet to protect its Customers' and/or end users' rights.

#### 15. Open Source Software.

Fortinet's products may include software modules that are licensed (or sublicensed) to the user under the GNU General Public License, Version 2, of June 1991 ("GPL") or GNU Lesser General Public License, Version 2.1, of February 1999 ("LGPL") or other open source software licenses which, among other rights, permit the user to use, copy, modify and redistribute modules, or portions thereof, and may also require attribution disclosures and access to the source code ("Open Source Software"). The GPL requires that for any Open Source Software covered under the GPL, which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any Open Source Software covered under the GPL, the source code is made available on this CD or download package. If any Open Source Software licenses require that Fortinet provide rights to use, copy or modify any Open Source Software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein. Fortinet will provide, for a charge reflecting our standard distribution costs, the complete machine-readable copy of the modified software modules. To obtain a complete machine-readable copy, please send your written request, along with a check in the amount of US \$25.00, to General Public License Source Code Request, Fortinet, Inc., 899 Kifer Rd, Sunnyvale, CA 94086 USA. To receive the modified software modules, you must also include the following information: (i) Name, (b) Address, (c) Telephone number, (d) E-mail Address, (e) Product purchased (if applicable), (f) Product Serial Number (if applicable). All open source software modules are licensed free of charge. There is no warranty for these modules, to the extent permitted by applicable law. The copyright holders provide these software modules "AS-IS" without warranty of any kind, either expressed or implied. In no event will the copyright holder for the open source software be liable to you for damages, including any special, incidental or consequential damages arising out of the use or inability to use the software modules, even if such holder has been advised of the possibility of such damages. A full copy of this license, including additional open source software license disclosures and third party license disclosures applicable to certain Fortinet products, may be obtained by contacting Fortinet's Legal Department at [legal@fortinet.com](mailto:legal@fortinet.com).



## GNU GENERAL PUBLIC LICENSE GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation,  
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law; that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this license; they are outside its scope. The act of running the Program (not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or, else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

Source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

### NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REPRODUCE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.  
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law; that is to say, a "work containing the Library" or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- The modified work must itself be a software library.
- You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

c) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2 instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not.

Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code may plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for your own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

15. The warranty disclaimer contained in Sections 11 and 12 of the preceding GPL License is incorporated herein.

**Fortinet Service Terms & Conditions**  
**For FortiCare, FortiGuard and other Fortinet Service Offerings**

---

THESE TERMS AND CONDITIONS APPLY TO THE PROVISION OF SERVICES BY FORTINET AND EXCLUSIVELY GOVERN THE LEGAL RELATIONSHIP BETWEEN YOU (THE "CUSTOMER") AND FORTINET. IT SETS FORTH THE LEGALLY BINDING RIGHTS AND OBLIGATIONS OF THE CUSTOMER IN RELATION TO FORTICARE SUPPORT OR FORTIGUARD SUBSCRIPTION SERVICES OR OTHER FORTINET SERVICE OFFERINGS. THE CUSTOMER CONSENTS TO BE BOUND BY THESE TERMS AND CONDITIONS (THE "AGREEMENT"). THE CUSTOMER REPRESENTS THAT IT IS A SOPHISTICATED ENTITY, THAT HAS READ AND UNDERSTANDS THIS AGREEMENT AND HAS HAD SUFFICIENT OPPORTUNITY TO CONSULT WITH COUNSEL BEFORE AGREEING TO THE TERMS HEREIN. IF THE CUSTOMER DOES NOT AGREE TO THE TERMS, THE CUSTOMER SHOULD NOT ACCEPT THE AGREEMENT AND SHOULD CONTACT [LEGAL@FORTINET.COM](mailto:LEGAL@FORTINET.COM) TO REQUEST CHANGES TO THE AGREEMENT. THE CUSTOMER AGREES THAT ANY OF THE FOLLOWING ACTIONS BY CUSTOMER REPRESENTATIVES REPRESENT THE CUSTOMER'S AUTHORIZED CONSENT TO BE BOUND BY THIS AGREEMENT: (I) RECEIVING, DOWNLOADING, DEPLOYING OR USING ANY SOFTWARE PROVIDED IN CONNECTION WITH FORTINET SERVICES, (II) RECEIVING, CONFIGURING, LOGGING IN, REGISTERING OR OTHERWISE USING OR BENEFITTING FROM THE SERVICES, OR (III) BY CLICKING ON THE "ACCEPT" BUTTON UPON REGISTRATION (ANY OF (I), (II), OR (III) SHALL CONSTITUTE "ACCEPTANCE" BY CUSTOMER). THE CUSTOMER HEREBY ACKNOWLEDGES AND AGREES THAT THE PERSON ENGAGING IN (I), (II), AND/OR (III) IS AUTHORIZED TO BIND THE CUSTOMER TO THE TERMS HEREIN. FOR CLARITY, NOTWITHSTANDING ANYTHING TO THE CONTRARY, IF CUSTOMER IS USING AN AUTOREGISTRATION TOOL OR HAS ENGAGED A FORTIPARTNER OR FORTINET TO REGISTER THE SERVICE CONTRACT ON ITS BEHALF, CUSTOMER ACKNOWLEDGES AND AGREES THAT ANY AND ALL UNITS REGISTERED USING SUCH TOOL SHALL BE SUBJECT TO THIS AGREEMENT.

Services are available independently or in connection with the purchase of Fortinet's commercial networking products and related equipment, including Hardware products with embedded Software, and stand-alone Software products sold and licensed to Customer pursuant to Fortinet's End User License Agreement ("EULA"), which EULA is available at <https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf>, and Customer hereby agrees to the terms of the EULA.

This Agreement constitutes a legal agreement between the parties with respect to FortiCare and FortiGuard Subscription services or other Services, and shall supersede all prior representations, discussions, negotiations and agreements, whether written or oral. Notwithstanding anything to the contrary, Fortinet is only bound by, and Customer is only entitled to, services pursuant to official service descriptions that are authorized by Fortinet pursuant to this Agreement and are contractually binding on Fortinet pursuant to the terms herein

**1. DEFINITIONS**

1.1. *"Active Service Coverage Level"* means the level of Technical Support as purchased by Customer pursuant to a Service Contract and defined in the applicable service description.

1.2. *"Customer"* means any entity or person that has purchased a Service Contract for use within their business and not for further sale.

1.3. *"Customer Service"* means a function and associated ticket type within TAC handling mainly non-technical queries and registration issues.

1.4. *"Documentation"* means any customer support manuals, technical manuals, and/or "Help" files within the Services that relate to the Services and that Fortinet makes available to Customer in connection with this Agreement and/or through the Services.

1.5. *"Enterprise Agreement Program"* means account based Service as described in applicable service description and, pursuant to this Agreement, that provides multiple Service Contracts through prior agreement and subsequent purchase.

1.6. *"FortiCare"* means a time-based subscription to Technical Support Services, as defined in the applicable service description, which may be purchased by Customer directly or from a third party, and which are delivered by Fortinet on behalf of that third party.

1.7. *"Fortinet"* means Fortinet, Inc.

1.8. *"FortiPartner"* means a Fortinet authorized distributor or reseller of Fortinet Products and Services.

1.9. *"Hardware"* means a Fortinet appliance or chassis, excluding all software incorporated or bundled with such devices.

1.10. *"Product Bundle"* means Product sold with defined Services.

1.11. *"Product"* means any Hardware with associated Software including Product Bundles, or stand-alone Software which is available for sale through a FortiPartner or directly from Fortinet and is covered by a Service Contract.

1.12. *"Registration Date"* means the date the Product or Service Contract or Renewal Service Contract is registered in the Support Portal. Service activation takes place on registration of the Service Contract subject to Fortinet's then-current Service start policy.

1.13. *"Renewal Service Contract"* means the continuation of a Service Contract pursuant to the terms of the Service Contract.

1.14. *"Serial Number"* means the unique identifier of a Product which may be registered in the Support Portal.

1.15. *"Service(s)"* when used individually means a subscription to one of Fortinet's service offerings (FortiCare,

FortiGuard, etc.) or in plural when generally referring to Fortinet's service offering, which may be purchased by the Customer directly or from a third party.

1.16. *"Service Contract"* means a time-limited subscription to Technical Support or other Services registered subject to this Agreement, provided pursuant to Fortinet's standard Service offering as defined in Fortinet's official applicable service description or pursuant to Fortinet's standard service practices.

1.17. *"Software"* means Fortinet computer software, Fortinet software subscription services and bug fixes, in each case provided by Fortinet either directly or from FortiPartner, whether purchased as embedded within the Hardware or as a standalone software product or operating software release or update service.

1.18. *"Support Portal"* means an on-line service portal designed to allow Customers to register and access their applicable purchased Services. For example, the Support Portal can be used to create Technical Tickets, access documentation, and obtain software releases. The Support Portal is available at <https://support.fortinet.com> or, for FortiPartners at <https://partnerportal.fortinet.com>.

1.19. *"TAC"* means Fortinet's technical assistance center which is comprised of a number of technical support centers.

1.20. *"Technical Support"* means the provision of technical support assistance to resolve issues related to Products and Services.

1.21. *"Technical Ticket"* means a Customer's request for Technical Support under a Service Contract, whereby Customer will provide a suitable description of the reason why Customer is seeking Technical Support and all technical details to allow Fortinet's support team to investigate Customer's request.

1.22. *"Upgrade Service Contract"* means a Service Contract which provides or amends an existing Service Contract with an additional service entitlement.

## 2. FORTICARE

2.1. Upon activation of a FortiCare Service Contract and pursuant to Active Service Coverage Level applicable to the Product, the Customer will obtain the following entitlements to the extent within the scope of its Service Contract: (a) access to the Support Portal; (b) access to the TAC for Customer Service assistance as well as resolution of Technical Tickets; (c) access to Software updates (maintenance and feature releases) exclusively for the Products covered by the FortiCare Service Contract; and (d) the replacement of Hardware determined by Fortinet to be defective exclusively for the Hardware covered by the FortiCare Service Contract. For more details refer to the FortiCare Technical Support Service and Fortinet's policies.

### *Technical Support*

2.2. Pursuant to Active Service Coverage Level, Fortinet shall provide Customer the following entitlements to the extent within the scope of Customer's Service Contract:

2.2.1. Assistance by telephone or via the Support Portal or via web-chat in relation to troubleshooting of Product technical issues, as well as usage and configuration.

2.2.2. 24x7 access to the TAC.

2.2.3. Access to the Support Portal for the Customer to create Technical Tickets, manage Product and Service assets, obtain Software updates exclusively for the Products covered by the FortiCare Service Contract, as well as providing access to Documentation including trouble-shooting information. Technical Tickets shall be processed by Fortinet in accordance with Sections 2.2.4 and 2.2.5.

2.2.4. Processing of Technical Tickets in accordance with the Technical Support procedures and support day/time limitations outlined in Fortinet's official applicable FortiCare service documents.

2.2.5. On a commercially-reasonable basis, provide acceptable workaround solutions, resolutions or Software maintenance releases to resolve Technical Tickets. The Customer acknowledges that Software and/or Hardware are never error-free and that, despite commercially-reasonable efforts, Fortinet may be unable to provide answers to, or be unable to resolve, some requests for Software or Hardware support.

2.2.6. Maintenance releases and feature updates for Software. Customer may access such updates via password-protected web access. This is subject to one copy per Software release or signature file as appropriate and is subject to the EULA and exclusively for the Products covered by the FortiCare Service Contract.

2.2.7. Where Hardware replacement is deemed necessary by Fortinet, and within scope of the Service Contract, Fortinet shall provide Hardware replacement services, using commercially-reasonable efforts, in accordance with the Active Service Coverage Level.

### *Hardware Replacement*

2.3. Hardware replacements are shipped to the Customer with incoterm DAP (Delivery At Place) using a Fortinet carrier, freight prepaid by Fortinet, excluding any import duties, taxes or other fees.

2.4. Hardware replacement Service is subject to geographical restrictions.

2.5. Fortinet is not responsible for transportation or custom delays. Customer compliance with export controls and destination customs processes may condition shipment times.

### *Product Life Cycle*

2.6. The type of Technical Support provided under FortiCare may vary depending on the Product's life cycle. An up-to-date version of the Product life cycle shall either be stored on the Support Portal or available by contacting Fortinet.

2.7. For any Software that is in the “End of Support” phase, as defined in Fortinet’s then-active Product life cycle policy, Fortinet may provide Technical Support for Software issues at its sole discretion. Such Support Services are limited to advisory support and do not include new Software releases to address Software defects unless otherwise stated in the Active Service Coverage Level.

#### *Exclusions*

2.8. Fortinet shall have no obligation to provide Technical Support under FortiCare in any of the following circumstances:

- FortiCare does not include any on-site activity, or any request for step-by-step installation and configuration of a Product or creation of custom SQL reports. Professional services may be available for purchase by Customer to provide such services.
- In the event the Customer alters, damages or modifies the Product or any portion thereof.
- For any problem caused by: accident; transportation; neglect, abuse, misapplication, or misuse; alteration, modification, or enhancement of the Product; failure to provide a suitable installation environment for the Product; use of supplies or materials not meeting Product specifications; use of the Product for other than the specific purposes for which the Product is designed.
- For the Product that is used on any systems other than the specified hardware platform for such Product as described in the Product’s then-current specifications. Fortinet shall have no liability for any changes in the Customer’s hardware, which may be necessary to use the Product due to a workaround or maintenance release.
- For any Hardware that is in the “End of Support” phase, as defined in Fortinet’s then active Product life cycle policy unless otherwise stated in the Active Service Coverage Level.
- For any Product that has not been publicly released.
- For third-party devices (including, without limitation, hardware, software, infrastructure such as cabling) or problems associated with such elements.
- Any usage of FortiGuard service updates that are not specifically authorized by Fortinet in writing including, without limitation, accessing signature packages for the purpose of duplication. For clarity, FortiGuard service updates are only provided for the Product that is covered by a FortiGuard Service Contract.
- For issues related to hardware consumables, which may be physically installed within a Fortinet appliance, such as SFPs, SDD cards and hard disks, if these are not Hardware and as a result of a technical analysis a fault or defect is traced to the use of non-Fortinet supplied hardware.
- For any other violation by Customer of this Agreement.

#### *Customer Obligations*

Customer is obligated and responsible for the following, and Fortinet’s responsibilities and obligations shall be subject in full to Customer meeting its following obligations:

2.9. Properly activate and register Service Contracts and proper inclusion in such activation and registration the correct and full Customer name and location who is the beneficiary of such Support Contract against a specified Product unit or Support Portal account. Customer acknowledges that the Agreement applies in full when the registration of the Products and Services is made by the Customer indirectly through a FortiPartner or Fortinet Customer Services. For all Service Contracts provided as part of the Enterprise Agreement Program, Fortinet will automatically register such Service Contracts and the effective date will be as communicated by Fortinet to the Customer.

2.10. Ensure that the Product covered by FortiCare Service Contract is used for its intended purpose and in line with the applicable Product specifications and is maintained in accordance with applicable Product documentation.

2.11. Maintain Software at the current Software release and upgrade to the latest release of Software if it is required to resolve a reported technical issue.

2.12. Comply with Fortinet’s Technical Support recommendations.

2.13. Provide access at Customer’s expense to the Product in order for Fortinet to troubleshoot a Technical Ticket, subject to the Customer and Fortinet agreeing on appropriate security measures to prevent unauthorized access to Customer’s network, provided, however, the ultimate responsibility for the security of the network lies with the Customer. Fortinet will not connect to the Customer’s network without prior authorization and such connection will be solely to provide Technical Support. Customer has the right to monitor such access by Fortinet. Where (a) the Customer causes delay in providing connectivity in accordance with this section or (b) Customer and Fortinet cannot agree on appropriate security measures to prevent unauthorized access to Customer’s network in the performance of Technical Support, Fortinet will be excused from any damages or other losses attributable to such delay or lack of agreement.

2.14. Cooperate in full with Fortinet, provide Fortinet all relevant information, and make available knowledgeable technical staff to aid in troubleshooting.

2.15. Return the Hardware unit within 30 days of the receipt of a replacement Hardware following Fortinet’s specifications for packaging and labeling of the returned Hardware unit, assume all costs associated with returning the Hardware unit and provide insurance for all returned Hardware equipment. For clarity, Hardware returns that are improperly packaged will not be accepted by Fortinet and returned at the Customer’s expense.

2.16. Ensure Service Contracts are transferred to any replacement Products. Customer acknowledges that this action is required to continue to receive FortiCare Services and accepts that there may be a delay of up to four hours to re-establish FortiGuard security services.

2.17. Maintaining reasonable internal security policies and processes, such as related to internal passwords, its facilities, its administrator access to information and systems, and use of wireless access points.

2.18. Ensure Customer does not share any Customer, Customer employee, or any third party sensitive, confidential, or private information with Fortinet, except as permitted and to the extent necessary for Fortinet to meet its obligations under this Agreement, and, in the event such is shared, with clear notice to Fortinet of proper handling requirements for, and sensitivity of, such information.

### 3. FORTIGUARD

3.1. FortiGuard is a Service that provides a threat research feed under which Fortinet undertakes commercially-reasonable efforts to provide solutions to identified network security threats. These are developed in response to evolving internet activity and delivered via security threat databases, produced by machine intelligence and experts.

3.2. Customer is responsible for configuring the frequency of FortiGuard security updates, which may be available on either an automatic or manual basis.

3.3. The creation of Technical Tickets for issues related to FortiGuard requires an active FortiCare Service Contract covering the FortiGuard service.

### 4. EVALUATIONS.

For registration of FortiGate-VM licenses for evaluation, and any other Software that Fortinet makes available for evaluation (together "Evaluation Software"), please be advised that the following terms apply:

4.1. All Evaluation Software is licensed pursuant to the EULA referenced above.

4.2. Fortinet makes available a limited, revocable license to Evaluation Software solely for the purpose of testing and evaluation, and not for commercial use or use in production environments. Fortinet disclaims liability and shall not be responsible for the Customer's use of Evaluation Software in production environments.

4.3. Unless otherwise noted on the Evaluation Software entitlement, the Evaluation Software license is limited to sixty (60) days from the start date provided by Fortinet ("Term"). The Customer must cease use of the Evaluation Software upon expiration of the Term. At Fortinet's discretion, a new Software license may be provided for additional Evaluation.

4.4. Fortinet retains all right, title, and interest in the Evaluation Software and all materials delivered in connection with such Evaluation Software, including without limitation, all changes and improvements made, requested, or suggested by Customer. All results of this evaluation and any feedback shall be deemed to be confidential information and trade secrets of Fortinet, and may not be disclosed by Customer to any third party without

Fortinet's written consent. At Fortinet's request, Customer shall provide to Fortinet any results of the Evaluation.

4.5. Customer also hereby affirms that Customer will comply fully with all relevant import and export laws and regulations of the United States and any other country ("Export Laws") with respect to any use of Confidential Information including but not limited to export, re-export, ship, transfer to an embargoed country or other sanction by the United States namely Cuba, Iran, N. Korea, Syria, Sudan and the Crimea Region of Ukraine are prohibited; that Customer is allowed to legally conduct business with Fortinet, and you are not on any United States government restricted lists (such as the Denied Persons List, Entity List, Unverified List, or Consolidated Screening List) or similar lists from any government that may restrict your ability to legally conduct business with Fortinet.

### 5. FEES, TERMS, AND TERMINATION

5.1. Ordering and use. Each Service is covered individually by this Agreement, and expires in accordance with the terms contained in this Agreement or according to Fortinet's policies and the term of the Service Contract. Accordingly, where this Agreement (including Service Contracts) terminates for a particular Service as related to a particular unit of Product or to a Support Portal account(s), the Agreement remains in full force and effect individually for any proper Service being provided related to any other Product unit or to other Support Portal account(s). Service Contracts may apply only to a single unit of Product or Support Portal account(s) as described in the relevant service description. An attempt to use a Service Contract with more than one unit of Product, (i.e. in addition to the unit of Product for which the Service Contract was originally purchased and registered) or with more than the designated Support Portal account(s), is considered a material breach of the Service Contract and will result in the termination of such Service Contract without refund of any fees paid by Customer and additional fees will be immediately due by Customer to Fortinet based on Fortinet's then-current list price for any incremental, additional Services beyond those authorized by the Service Contract.

5.2. Payment Terms. By purchasing Services directly or indirectly through a FortiPartner as the case may be, Customer agrees to pay the purchase price for the Services, and all sales, use, valued-added and other taxes and all customs duties and tariffs now or hereafter claimed or imposed by any governmental authority upon the sale of the Services. Where purchasing from Fortinet all payments shall be due upon purchase, in U.S. Dollars, and free of any currency control or other restrictions. All sales are final and the Services are not returnable.

5.3. Registration and renewal registration. Customer must register, directly or indirectly through a FortiPartner or Fortinet Customer Services, the standalone 'Service Contract Registration Number' which references the purchased standalone Service, within three hundred sixty-five (365) days from the date of the original shipment by



Fortinet of the Service Contract to its FortiPartner or Customer, whichever originally purchased directly from Fortinet. Customer is fully responsible to ensure complete and accurate information is included in the registration of the Service Contract. ANY STANDALONE SERVICE CONTRACTS WHICH ARE NOT REGISTERED WITHIN THREE HUNDRED SIXTY-FIVE (365) DAYS FROM THE DATE THE SERVICE CONTRACT WAS ORIGINALLY SHIPPED FROM FORTINET SHALL BE FORFEITED AND FORTINET SHALL HAVE NO OBLIGATION TO THE CUSTOMER REGARDING THIS AGREEMENT OR ANY RELATED SUPPORT SERVICES. It is the Customer's responsibility to register the Service Contract within the three hundred sixty-five (365) day period and to understand the original ship date from the party from which the Customer purchased the Product. In the case of Product Bundle, the Services begin in accordance with the Service activation policies set forth at: <https://www.fortinet.com/corporate/about-us/legal> under heading 7. For all Service Contracts provided as part of the Enterprise Agreement Program, Fortinet will automatically register such Service Contracts and the effective date will be as communicated by Fortinet and accepted by the Customer on receipt of purchase order therefore section 5.3 will not apply.

5.4. Notwithstanding anything to the contrary, Fortinet may register any Renewal Service Contract, or Upgrade Service Contract upon invoicing. Upon renewal of the Service Contract, Customer authorizes Fortinet to automatically register the Renewal Service Contract for subsequent renewal periods for which a purchase order has been placed. For clarity, registration is the responsibility of the Customer and Fortinet is not obliged to register the Renewal Service Contract or the Upgrade Service Contract.

5.5. In order to maintain a continuous service period, the effective date of any Renewal Service Contract shall begin the next calendar day following the expiration date of the previous Service Contract. In the event that registration of a Renewal Service Contract is beyond one hundred eighty (180) calendar days following the expiration date of the previous Service Contract, such Renewal Service Contract effective start date will be the date that is one hundred eighty (180) calendar days prior to the actual Registration Date of the Renewal Service Contract.

5.6. Term and Termination. Subject to the other provisions herein, this Agreement is valid for the length of time provided for in the Customer's purchased Service Contract which is viewable upon activation in the applicable Support Portal and which starts from (a) the Registration Date of the Service Contract or in the case of a Product Bundle the Registration Date of the Product; or (b) in the event of a Renewal Service Contract that has been registered prior to the expiration date of the previous Service Contract, starting from the calendar day following the expiration date of the previous Service Contract; or (c) in the event of a Renewal Service Contract that has not been registered prior to the expiration of the previous Service Contract, starting from the actual Registration Date of the Renewal Service Contract with the applicable term being amended based on the effective start date as described in section 5.5; or (d) the applicable start date as communicated by Fortinet in

respect of Services provided under the Enterprise Agreement Program. To the extent the Services experience any interruption due to Customer's failure to register a Renewal Service Contract, Fortinet shall not be responsible for providing Services during such interruption and will not be responsible for any losses or damages incurred by Customer or any third party attributable to this interruption in Services.

5.7. Fortinet reserves the right to terminate this Agreement and/or any and all Services being provided hereunder, in its discretion, in the event of (a) breach of any terms herein by Customer, (b) breach of any of the terms of the EULA; (c) transfer of the unit of Product to a third party, (d) use of the Support Contract for other Products than the entitled Product, or (e) non-payment to Fortinet or to its FortiPartner for any Services by the Customer or a third party, with such termination having immediate effect, if such breach has not been cured within fifteen (15) calendar days after written notice by Fortinet to Customer or immediately upon notice of termination in the event of a breach that by its nature cannot be remedied within fifteen (15) calendar days. Fortinet may also terminate this Agreement without notice if Customer becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors. Upon any termination, Fortinet shall have no obligation to provide the Services hereunder.

5.8. Third-party providers. Fortinet reserves the right to subcontract its obligations herein to third-party organizations. Fortinet also reserves the right to change service subcontractors without notice.

5.9. Non-Fortinet Support. To the extent Customer provides its own technical support or engages a non-approved third party to provide technical support, Fortinet is not responsible for such support, and Customer represents and warrants that all such technical support pursuant to Section 5.9 shall be performed in a satisfactory and commercially reasonable manner and will not infringe upon Fortinet's rights or the rights of any third party. Fortinet shall be relieved of its Technical Support obligations to the extent Customer's actions interfere with Fortinet's ability to meet its service obligations under the Active Service Coverage Level.

5.10. Service Description; Updates. A description of the various Services is available on the Fortinet website, and on the applicable services portal. In its sole discretion Fortinet may make updates to its Service offerings from time to time. If Fortinet makes a material change to the Services, those changes will be reflected in the on-line service descriptions stored on the applicable portal. Fortinet may also make changes to this Agreement, including any linked documents, from time to time. Unless otherwise noted by Fortinet, material changes to the Agreement will become effective thirty (30) days after they are posted, except if the changes apply to new Service functionality in which case they will be effective immediately. If Customer does not agree to the revised Agreement, Customer must stop using the Services and promptly notify Fortinet in writing. In no event shall Fortinet be obligated to refund Customer or FortiPartners, any amounts previously paid.

5.11. Service/support portal access and security. As part of the Services, Customer may receive administrative access ID's and passwords upon installation, registration. Customer shall be solely responsible for maintaining the security of its administration access information, and shall be fully responsible for, all activities which occur, relating to access to the Services under Customer's administrative access ID. Fortinet is not responsible for unexpected use of Services or data whether by ex-employees, compromised user passwords or any other misuse of Customer accounts. Upon termination of the Services, all data, including configuration data will be deleted, and Fortinet has no responsibility for such data.

5.12. Loss of data and accuracy of data. While Fortinet takes commercially reasonable and industry standard technical and organizational steps to ensure the security of the Services, it is not responsible for the accidental loss or destruction of any data any End User transmits using the applicable Service and Fortinet disclaims all liability of any kind in relation to the content or security of data that any End User sends or receives through the Service. Further, Fortinet does not guaranty the accuracy of the reports, which may be compromised by various network incidents that impact data collection and accuracy (e.g. network outages, hardware upgrades, and the like), and in no event does Fortinet guarantee security or privacy of the Customer's network or assets.

## 6. PRIVACY

6.1. Customer hereby consents to Fortinet's collection, use, protection and transfer of Customer's information as described in the Fortinet Privacy Policy on the Fortinet web site (<http://www.fortinet.com/aboutus/privacy.html>).

6.2. Customer consent and privacy. Fortinet recommends, and (where required by law) requires, the posting of legally sufficient notices to data subjects, consumers and other relevant individuals ("End Users") regarding the collection of End User data through the Services. IT IS CUSTOMER'S SOLE OBLIGATION TO COMPLY WITH ALL NATIONAL AND LOCAL LAWS REGARDING CONSUMER DATA PRIVACY AND PRIVACY DISCLOSURE LAWS.

6.3. Customer agrees and acknowledges, and warrants that it is responsible to ensure that all End Users agree and acknowledge, that Fortinet may be required by law to provide assistance to law enforcement, governmental agencies and other authorities. Accordingly, Customer agrees and shall procure that all End Users agree that:

6.3.1. Fortinet may implement and maintain an interception capability suitable to meet these regulatory requirements where Fortinet and/or FortiPartners are obliged by law to ensure or procure that such a capability is implemented and maintained;

6.3.2. Fortinet may implement and maintain a data retention capability for the Service to meet regulatory requirements where Fortinet and/or its FortiPartners are obliged by law to ensure or procure that data is retained; and

6.3.3. Fortinet may at times cooperate with law enforcement authorities and rights-holders in the investigation of any suspected or alleged illegal activity by Customer or End Users. If Fortinet is required to do so by law, this may include but is not limited to, disclosure of the Customer's or End Users' contact information to law enforcement authorities or rights-holders.

6.4. To the extent Customer receives administrative access IDs and passwords in connection with any accounts for the Services, Customer shall be solely responsible for maintaining its security, and shall be fully responsible for all activities which occur relating to access to the Services and use of any other features (including wireless access point(s), as applicable) under that administrative access ID and passwords. Customer agrees to notify Fortinet immediately of any actual or suspected unauthorized use of Customer's account or any other breach of security known by Customer.

6.5. Although some of our Services may provide certain notices or may seek certain consents from certain End Users, Fortinet does not provide legal advice, and Customer remains solely responsible and solely liable for independently (i) determining what notices and consents are legally required and (ii) providing such notices and obtaining such consents.

## 7. SOFTWARE RESTRICTIONS

7.1. Customer hereby agrees to the software restrictions in Fortinet's EULA and further agrees (i) not to or not to attempt to reverse engineer, disassemble, decompile or otherwise access, obtain or modify the source code, internal structure, Hardware design or organization of the Product or support updates or Software, or any part thereof, or to aid or to permit others to do so, except and only to the extent as expressly required by applicable law; (ii) not to remove any identification or notices of any proprietary or copyright restrictions from any Product or support updates or Software; (iii) not to copy the Product or support updates or Software, modify, translate or, unless otherwise agreed, develop any derivative works thereof or include any portion of the Software in any other software program; (iv) only to use the Product and support updates and Software for internal business purposes and in accordance with then active specification, and (v) to keep confidential any Software and support updates and not share them with third parties.

## 8. INDEMNIFICATION

8.1. Customer will defend Fortinet against any claim, demand, suit or proceeding made or brought against Fortinet by a third party arising out of Customer's breach of this Agreement, any infringement or misappropriation of intellectual property rights caused by Customer (whether or not Customer has concurrently violated this Agreement), or any illegality of Customer data (individually and collectively, a "Claim"), and will indemnify Fortinet from any damages, attorney fees and costs finally awarded against Fortinet as a result of, or for any amounts paid by Fortinet under a

settlement of, a Claim, provided Fortinet promptly gives Customer written notice of the Claim (provided that failure to so notify will not remove Customer's obligation except to the extent Customer is materially prejudiced thereby). For a Claim, Customer controls the defense and settlement of the Claim and Fortinet agrees to give Customer all reasonable assistance, at Customer's expense. Customer will not settle, compromise, or otherwise enter into any agreement regarding the disposition of any Claim without the prior written consent and approval of Fortinet unless such settlement (a) is solely for a cash payment, (b) requires no admission of liability or wrongdoing on the part of Fortinet, (c) imposes no obligation on Fortinet, (d) imposes no restriction on Fortinet's business, (e) provides that the parties to such settlement shall keep the terms of the settlement confidential, and (f) provides for a full and complete release of Fortinet. Customer shall reimburse Fortinet within 30 calendar days after demand for any losses incurred by Fortinet that is subject to an indemnification obligation as set forth in this Section.

## **9. WARRANTY**

9.1. Service Warranties. Fortinet provides its Services and Products on an "AS IS" basis. Neither Fortinet nor any of its officers, directors, employees, partners or agents, makes any representation, claim or warranty with respect to the Services or reports or data, whether express or implied, including without limitation, any warranty of quality, performance, non-infringement, merchantability, or fitness for a particular purpose, or any results generated from use of the Services or the reports. Fortinet makes no warranty that the Services will meet Customer's requirements, or that the Services will be uninterrupted, timely, or secure.

9.2. Fortinet will have no obligation to correct, and makes no warranty with respect to, errors caused by: (a) improper installation of the Software or Hardware; (b) changes that Customer has made to the Software or Hardware; (c) use of the Software or Hardware in a manner inconsistent with the documentation and instructions; (d) the combination of the Software or Hardware with hardware or software not approved by Fortinet; (e) malfunction, modification or relocation of Customer's Hardware or Software transferred to unapproved or unregistered devices; (f) Customer failure to use the Software and Services in accordance with local laws; or (g) business and/or service decisions based on reliance on the analysis or data aggregation results.

9.3. Product Warranties. The warranty limitations, restrictions on Customer and protections for Fortinet as contained in Fortinet's EULA are applicable. Except as expressly stated in its EULA, Fortinet does not provide any warranty whatsoever and nothing in this Agreement shall be construed as expanding or adding to the warranty set forth in the EULA. In the event of a conflict between this Agreement and the EULA, the EULA shall govern. Fortinet cannot guarantee that every question or problem raised in connection with the Services will be addressed or resolved, and in no event does Fortinet warrant or guaranty security and protection from all threats. EXCEPT FOR WARRANTIES CLEARLY AND EXPRESSLY STATED HEREIN,

NOTWITHSTANDING ANYTHING TO THE CONTRARY, FORTINET MAKES, AND CUSTOMER RECEIVES, NO OTHER WARRANTIES OF ANY KIND, EXPRESS, IMPLIED OR STATUTORY, ARISING IN ANY WAY OUT OF, RELATED TO, OR UNDER THIS AGREEMENT OR THE PROVISION OF MATERIALS OR SERVICES HEREUNDER, AND, TO THE EXTENT PERMISSIBLE BY LAW, FORTINET SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTY OF SATISFACTORY QUALITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY RIGHTS.

## **10. LIMITATION OF LIABILITY**

10.1. NOTWITHSTANDING ANYTHING TO THE CONTRARY, IN NO EVENT WILL FORTINET BE LIABLE TO THE CUSTOMER FOR ANY SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES OF ANY KIND, INCLUDING BUT NOT LIMITED TO ANY LOST PROFITS OR LOSS OF DATA HOWEVER CAUSED, WHETHER FOR BREACH OR REPUDIATION OF CONTRACT, TORT, BREACH OF WARRANTY, NEGLIGENCE, OR OTHERWISE, WHETHER OR NOT FORTINET WAS ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES. NOTWITHSTANDING ANYTHING TO THE CONTRARY, FORTINET'S TOTAL POSSIBLE LIABILITY TO THE CUSTOMER AND OTHERS ARISING FROM OR IN RELATION TO THIS AGREEMENT AND THE SERVICES, WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR STRICT LIABILITY, SHALL BE LIMITED TO THE TOTAL PAYMENTS MADE BY CUSTOMER TO FORTINET UNDER THIS AGREEMENT FOR THE PARTICULAR SERVICE CONTRACT AT ISSUE DURING THE THREE HUNDRED SIXTY-FIVE (365) CALENDAR DAYS PRIOR TO THE DATE OF THE EVENT GIVING RISE TO THE LIABILITY. THIS LIMITATION WILL APPLY TO ALL CAUSES OF ACTION IN THE AGGREGATE. IN NO EVENT WILL FORTINET BE LIABLE FOR THE COST OF PROCUREMENT OR REPLACEMENT OF SUBSTITUTE GOODS. IN THE EVENT FORTINET SUSPENDS OR TERMINATES SERVICES IN THE MIDDLE OF A SERVICE TERM FOR ANY REASON, NOTWITHSTANDING ANYTHING TO THE CONTRARY, FORTINET'S MAXIMUM LIABILITY SHALL BE THE PRO-RATED AMOUNT OF THE FEES ACTUALLY PAID TO FORTINET FOR SUCH SERVICES FOR THE PERIOD OF THE CURRENT TERM DURING WHICH NO SUCH SERVICES ARE PERFORMED (I.E. THE PRO-RATED AMOUNT PAID FOR THE PERIOD FROM SUSPENSION OR TERMINATION TO THE END OF THE CURRENT PAID-FOR TERM). FOR CLARITY, IF FORTINET IS ENTITLED TO TERMINATE THE SERVICE PURSUANT TO THIS AGREEMENT FORTINET SHALL OWE NO REFUND OR ANY OTHER AMOUNTS, AND, IN ADDITION, IN ALL EVENTS, CUSTOMER IS RESPONSIBLE TO WORK IN GOOD FAITH TO MITIGATE ANY DAMAGES CUSTOMER MAY REALIZE. THE FOREGOING LIMITATIONS OF LIABILITY SHALL NOT APPLY TO DAMAGES ARISING FROM DEATH OR PERSONAL INJURY IN ANY JURISDICTION WHERE SUCH LIMITATION IS PROHIBITED BY APPLICABLE LAW. FOR FURTHER CLARITY, NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT OR OTHERWISE, IN NO EVENT DOES FORTINET PROVIDE ANY GUARANTEE OR ASSURANCE REGARDING COMPREHENSIVE SECURITY OR ENSURING FULL SECURITY OF THE PRODUCTS, SERVICES, OR CUSTOMER'S ASSETS OR NETWORKS.



## 11. GENERAL PROVISIONS

**11.1. Compliance with laws.** Customer hereby agrees to comply with all applicable laws, such as data privacy and privacy disclosure laws. Fortinet's Products and Services may be subject to the United States Export Administration Regulations and other import and export laws. Diversion contrary to United States law and regulation is prohibited. Customer agrees to comply with, and ensure compliance with, all applicable laws that apply to the products as well as the Customer and destination restrictions issued by U.S. and other governments. As just one example, if Customer is a FortiPartner that provides Return Manufacture Authorization services ("RMA"), Services or other Services on behalf of another entity or otherwise provides Product or Services, Customer shall ensure proper, required export licenses are obtained for all Product, whether newly-purchased or RMA, prior to exporting those appliances and prior to providing any Services related to those appliances, if such export license is required. In addition, for RMA units or other units registered in a FortiPartner's name, the FortiPartner is responsible for all export compliance. In addition, if Customer or the end-user on whose behalf Customer is providing RMA, Services or other Services is designated a Denied Party, Specially Designated National, on the Entity List, or otherwise subject to an export license requirement after this agreement, then Fortinet may terminate or suspend, in its sole discretion, any and all Services related to Product or Services exported without full compliance with applicable export laws. For additional information on U.S. export controls see [www.bis.doc.gov](http://www.bis.doc.gov). Fortinet assumes no responsibility or liability for Customer's or partners' failure to obtain any necessary import and export approvals. Customer represents that neither the United States Bureau of Industry and Security nor any other governmental agency has issued sanctions against Customer or otherwise suspended, revoked or denied Customer's export privileges. Customer agrees not to use or transfer the Products or Services for any use relating to nuclear, chemical or biological weapons, or missile technology, unless authorized by the United States Government by regulation or specific written license. Additionally, Customer agrees not to directly or indirectly export, import or transmit the Products or Services contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or use. Customer represents that Customer understands, and Customer hereby agrees to comply with, all requirements of the U.S. Foreign Corrupt Practices Act and all other applicable laws. Fortinet is not responsible for Service delays or outages or loss of data resulting from activities related to Fortinet's and its service partners compliance with export regulations and cooperation with applicable domestic or foreign regulatory agencies (e.g., delays caused by requirement to obtain required licenses). Customer agrees, acknowledges and warrants that it will take reasonable steps to ensure it will meet all legal requirements to assist law enforcement agencies.

**11.2. Survival of terms.** The terms contained herein which by their nature are intended to survive the termination of this Agreement shall do so.

**11.3. Transferability.** Customer may not assign or otherwise transfer this Agreement without written consent from Fortinet. Any attempted assignment or attempted transfer without Fortinet's consent shall be null and void and may result on the termination of this Agreement and related Service Contracts. Fortinet may assign its rights and obligation under this Agreement to a third party without consent from Customer.

**11.4. Entire Agreement.** The provisions of this Agreement constitute the entire agreement between the parties with respect to the subject matter hereof, and this Agreement supersedes all prior agreements or representations, oral or written, regarding such subject matter. With the exception of the EULA, this Agreement takes precedence over any conflicting provisions in a document a Fortinet portal website such as a service description or support portal terms. This Agreement may be modified or amended only in accordance with Section 5.10 herein. All notices from Customer to Fortinet must be made by opening a new Support Ticket through the Support Portal.

**11.5. Confidential information.** Customer may be exposed to certain information concerning the Products and Services including, without limitation, maintenance releases (regularly scheduled and released updates and upgrades to software), feature releases (enhancements released through Fortinet's Product planning practices or through Customer requests) and other Product, Service or business information, which is Fortinet's confidential or proprietary information (herein "Confidential Information"). The Customer agrees that, during and after the term of this Agreement, the Customer will not use or disclose to any third party any Confidential Information without the prior written consent of Fortinet, and Customer will use reasonable efforts to protect the confidentiality of such Confidential Information. The Customer may disclose the Confidential Information only to its employees as is reasonably necessary for the purposes for which such information was disclosed to Customer; provided that each such employee is under a written obligation of nondisclosure which protects the Confidential Information under terms substantially similar to those herein. Fortinet may process and store Customer data in the United States or any other country in which Fortinet or its agents work or maintain facilities. Customer will take reasonable steps not to disclose to Fortinet any personally identifiable, confidential or sensitive data, and Customer hereby consents to Fortinet's processing and storage of Customer data, acknowledging and agreeing that Fortinet is merely a data processor.

**11.6. Governing Law, venue and settlement of controversies.** This Agreement shall be governed by the laws of the State of California, as applied to agreements entered into and to be performed entirely within California between California residents, without regard to the principles of conflict of laws or the United Nations Convention on Contracts for the International Sale of Goods. Any controversies or claims arising from or relating to this Agreement, or the breach hereof, which cannot be amicably settled by and between the parties, shall be referred to and finally settled by arbitration. The place of arbitration shall

be Santa Clara, California, pursuant to the Streamlined Arbitration Rules and Procedures of Judicial Arbitration and Mediation Services (JAMS), or its successor, before a sole, mutually agreed upon arbitrator and shall be conducted in English. Award for such dispute will be rendered by a single, neutral, mutually agreeable arbitrator. The parties specifically consent and agree that the Federal Courts located in the Northern District of California will have exclusive jurisdiction over enforcement of any arbitration decisions.

**11.7. Taxes and Duty.** Where purchasing directly from Fortinet, all prices payable under this Agreement are exclusive of all foreign, federal, state, municipal tax or duty now in force or enacted in the future. Customer shall comply with all applicable tax laws and regulations and the Customer will promptly pay or reimburse Fortinet for any costs and damages related to any liability incurred as a result of Customer's non-compliance or delay with its responsibilities herein. The Customer's obligations under this section shall survive termination or expiration of this Agreement.

**11.8. English language and interpretation.** This Agreement is in the English language only, which language shall be controlling in all respects. Any versions of this Agreement in any other language will be for accommodation only and will not be binding upon either party. In construing or interpreting this Agreement, the word "or" shall not be construed as exclusive, and the word "including" shall not be limiting. The parties agree that this Agreement shall be fairly interpreted in accordance with its terms without any strict construction in favor of or against either party and that ambiguities shall not be interpreted against the drafting party.

**11.9. No waiver and severability.** Failure by Fortinet to enforce any provision of this Agreement will not be deemed

a waiver of future enforcement of that or any other provision. The exercise by either party of any remedy under this Agreement will be without prejudice to its other remedies under this Agreement or otherwise. If for any reason a court of competent jurisdiction or an agreed-upon arbitrator finds any provision of this Agreement, or portion thereof, to be unenforceable, that provision of the Agreement shall be enforced to the maximum extent permissible so as to affect the intent of the parties, and the remainder of this Agreement shall continue in full force and effect.

**11.10. Force Majeure.** Fortinet shall be excused from performance to the extent performance is rendered impossible by strike, fire, flood, extreme weather, disaster, act of war or terrorism, military operations, riots, insurrection or civil disorder, national or local emergency, famine, disease, epidemic or pandemics, governmental acts or orders or restrictions, failure of suppliers or any other reason where failure to perform is beyond Fortinet's reasonable control.

**11.11. Future Functionality.** Customer agrees that its purchases of Products or Services are not contingent on the delivery of any future functionality or features, or dependent on any oral or written public comments made by Fortinet regarding future functionality or features.

**11.12. Relationship of the Parties.** The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties.

**11.13. No Third-Party Beneficiaries.** There are no third-party beneficiaries to this Agreement. For clarity, End Users are not third-party beneficiaries to this Agreement.

March 2021

-----End of Document-----

## Fortinet Professional Service Terms and Conditions

### Master Professional Services Agreement

---

CAREFULLY READ THE FOLLOWING TERMS OF FORTINET'S PROFESSIONAL SERVICES BETWEEN YOU AND FORTINET, INC., OR FORTINET, INC.'S SUBSIDIARIES OR AFFILIATES ("FORTINET"). YOU ARE AGREEING TO BE BOUND BY AND ACCEPT THESE TERMS AND CONDITIONS OF SALE. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, DO NOT SIGN THE STATEMENT OF WORK PROVIDED BY FORTINET.

FORTINET SHALL NOT BE BOUND BY ANY ADDITIONAL, INCONSISTENT, AND/OR CONFLICTING PROVISIONS IN ANY ORDER, RELEASE, ACCEPTANCE OR OTHER CORRESPONDENCE UNLESS EXPRESSLY AGREED TO IN A WRITING SIGNED BY FORTINET'S GENERAL COUNSEL, AND IN NO EVENT SHALL FORTINET BE DEEMED TO HAVE ACCEPTED ANY TERMS IN YOUR PURPORTED OFFER OR OFFER DOCUMENTS.

#### 1. SERVICES AND PROJECT MANAGERMENTS

- 1.1. **Statement of Work.** Fortinet agrees to provide certain security information technology, installation, or modification services (the "**Services**") to Company that are mutually agreed from time to time between the Parties. The specific Services will be set forth in one or more Statements of Work that the Parties may execute pursuant to these terms and conditions ("**Statement of Work**" or "**SOW**"), substantially in the form above. Each SOW shall be incorporated into and become part of these terms and conditions and be governed by the provisions of these terms and conditions. In the event of a conflict between the terms and conditions of these terms and conditions and a SOW, the provisions of these terms and conditions shall prevail unless the Parties have obtained the express written consent of authorized signatories of each Party to deviate from the terms and conditions of these terms and conditions for a particular SOW and the SOW expressly states that the conflicting terms in the SOW shall prevail over the terms of these terms and conditions. Fortinet shall not be required to commence work under these terms and conditions unless a Statement of Work is duly executed. To the extent applicable, "**Deliverables**" shall mean those items specifically described and itemized in the SOW as final work products to be delivered by Fortinet pursuant to such SOW. For clarity, unless expressly and specifically described in an SOW, Fortinet shall not have responsibility to perform Services.
- 1.2. **Points of Contact.** Fortinet and Company will each designate an individual in the Statement of Work to act as a primary point of contact between the Parties with respect to the Services ("**POCs**"). Such POCs will have the power to make technical and project-level decisions within the scope of these terms and conditions (including, for example, staffing decisions, Change Orders, and Acceptance of Deliverables) that are binding on their respective entities. Amendments to these terms and conditions, however, must be made in accordance with the clause hereto governing contract amendments.
- 1.3. **Changes to Services.** Either Party may request a change order ("**Change Order**") in the event of actual or anticipated change(s) to the agreed scope of Services, Deliverables, project schedule, price, or any other aspect of the Statement of Work. Fortinet will prepare a Change Order reflecting the proposed changes, including but not limited to the impact on the Deliverables, project schedule, and price. Absent a Change Order signed by the Parties, Fortinet shall not be bound to perform any additional or out-of-scope services beyond what is stated in the SOW. The Parties agree to negotiate all Change Order requests expeditiously and in good faith. The Parties further agree that: (a) Fortinet may at its discretion undertake and accomplish tasks of a de minimis nature necessary to perform its obligations under any SOW at no additional cost and without requiring the execution of a Change Order; and (b) Fortinet shall be compensated with or without a Change Order for unplanned idle time and project delays (to the extent such delays are not caused by Fortinet).
- 1.4. **Acceptance.** If applicable, following submission of any Deliverable(s) by Fortinet, Company will perform testing and review in accordance with previously agreed testing standards and procedures as agreed by the Parties in the SOW. By the expiration of such review period, Company will submit a written statement (a "**Deliverable Review Statement**") to the Fortinet Project Manager indicating acceptance of the Deliverable(s) ("**Acceptance**") or specifying in detail how the submitted Deliverable(s) fails to materially conform to the agreed specification, in which case Fortinet shall be afforded a commercially reasonable period of time not less than thirty (30) days to correct any nonconformities, whereupon the review cycle will recommence. Deliverables will be deemed to be fully and finally accepted by Company in the event Company has not submitted a Deliverable Review Statement to Fortinet before the expiration of the applicable review period, or when Company uses the Deliverable in its business, whichever occurs first ("**Deemed Acceptance**"). Fortinet may request that Company execute a Work Complete as confirmation of acceptance and Company shall execute such Work Complete and/or identify any issues with the Services that prevent confirmation of the Work Complete within five (5) business days of Fortinet's request. Unless specifically agreed in an SOW, Fortinet's invoicing will be on a periodic basis and not linked to Acceptance. Notwithstanding anything to the contrary, Company shall be obligated to pay for Services performed regardless of Acceptance.
- 1.5. **Company Input and Responsibilities.** Company will supply in a timely manner information, materials and actions necessary to the project including as applicable data, designs, programs, specifications, management decisions, approvals, acceptance criteria, and other information and material, plus any other assistance and materials as reasonably requested by Fortinet at Company's cost, for Fortinet's use in carrying out the Services ("**Inputs**"). Further Company responsibilities

may be set out in a Statement of Work or project planning document agreed between the Parties. Company may further provide equipment and software ("**Project Tools**") to Fortinet in order for Fortinet to provide the Services. Company shall bear all license, procurement and maintenance expenses related to the Project Tools.

- 1.6. **Performance Generally.** Fortinet's failure to perform its contractual responsibilities, to perform the services, or to meet agreed service levels shall be excused if and to the extent Fortinet's non-performance is caused by Company's omission to act, delay, wrongful action, failure to provide Inputs, or failure to perform its obligations under these terms and conditions

## **2. STAFFING**

- 2.1. **Team Composition.** Fortinet shall determine, after consultation with Company, the size, composition and distribution of the resource team, which Fortinet may change from time to time based upon the scope and complexity of the Services.
- 2.2. **Removal.** Company may require Fortinet to remove a team member if, after due consultation with Fortinet, it is reasonably determined that the individual is not suitable to perform the Services. Any such removal shall be effective after a minimum of fourteen (14) days written notice. Fortinet shall assign a replacement resource to the Services as soon as practicable. Company understands and acknowledges, however, that removal of a resource in fixed-price or fixed-schedule engagements may affect the pricing and project schedule for the affected Services and agrees to execute appropriate Change Orders to accommodate such removal.

## **3. PRICING, INVOICING & PAYMENT**

- 3.1. **Pricing & Payments.** Projects will be performed as stated on this SOW and be billed in accordance with Fortinet's then-current rates as of the date of execution of the SOW. Unless stated otherwise in the applicable SOW, if applicable, Customer must pay invoices within thirty (30) days from the date of Fortinet's invoice. Fortinet may charge interest at the lower of (a) a rate of 1.5% per month for delayed payments or (b) to the maximum extent allowed by law.
- 3.2. **Taxes.** The fees chargeable by Fortinet are stated exclusive of all taxes, duties and levies imposed by any government body. Company shall be liable and will pay for all applicable tax liabilities such as sales, services, use or value added taxes, but specifically excluding employment related taxes concerning Fortinet personnel and corporate taxes based on Fortinet's net income.

## **4. CONFIDENTIALITY**

- 4.1. The Parties agree that with respect to any business information of the disclosing Party which (a) is marked as "confidential," proprietary" or some similar indication; (b) is expressly advised by the disclosing Party to be confidential through some contemporaneous written means; or (c) which the receiving Party would reasonably construe to be confidential information under the circumstances (collectively referred to as "Confidential Information"): (i) to use such Confidential Information only in relation to the Services; (ii) not to disclose any such Confidential Information or any part thereof to a person outside the Party's business organization for any purposes unless expressly authorized by the owner of such Confidential Information; (iii) to limit dissemination of such Confidential Information to persons within the Party's business organization who are directly involved in the performance of Services under these terms and conditions and have a need to use such Confidential Information; (iv) to safeguard the Confidential Information to the same extent that it safeguards its own confidential materials or data.
- 4.2. Confidential Information shall not include information that: (a) is as of the time of its disclosure part of the public domain; (b) is subsequently learned from a third Party without a duty of confidentiality; (c) at the time of disclosure was already in the possession of the receiving Party; (d) was developed by employees or agents of the receiving Party independently of and without reference to any information communicated to the receiving Party; or (e) is required to be disclosed pursuant to a court order or government authority, whereupon the receiving Party shall, at its earliest opportunity, provide written notice to the disclosing Party prior to such disclosure and where feasible giving the disclosing Party a reasonable opportunity to secure a protective order or take other action as appropriate.
- 4.3. The Parties' obligations under this Section shall extend to the non-publicizing of any dispute arising out of these terms and conditions.
- 4.4. The terms of this clause shall continue in full force and effect for a period of three(3) years from the date of disclosure of such Confidential Information.
- 4.5. In the event of termination of these terms and conditions, upon written request of the disclosing Party, the receiving Party shall immediately return the disclosing Party's Confidential Information, or at the disclosing Party's option destroy any remaining Confidential Information and certify that such destruction has taken place, provided however that Fortinet may retain a minimum of one copy of all work product and relevant project documentation for archival and audit purposes.

## 5. PROPRIETARY RIGHTS

- 5.1. Retained Rights. Each Party owns, and will continue to own all right, title and interest in and to any inventions however embodied, know how, works in any media, software, information, trade secrets, materials, property or proprietary interest that it owned prior to these terms and conditions, or that it created or acquired independently of its obligations pursuant to these terms and conditions (collectively, "Retained Rights"). All Retained Rights not expressly transferred or licensed herein are reserved to the respective owner.
- 5.2. Deliverables and Fortinet Materials. All intellectual property rights in, or related to, any developments, Deliverables, enhancements, or other work product of Fortinet or related to the services to be performed hereunder or under any SOW shall be owned solely by Fortinet. Fortinet owns (or will own) any such material that is used in, enhanced, or developed in the course of providing services hereunder, and all intellectual property rights to such material, including: any and all rights throughout the word, arising out of, or associated with models, designs, patents, applications therefor, all trade secrets, proprietary information rights, know how, works of authorship, mask works, trade names, logos, trademarks, service marks, methodologies; delivery procedures; manuals; generic software tools, routines, frameworks, and components; generic content, research and background materials; templates; analytical models; project tools; development tools; and all other intellectual property and ownership rights (collectively, "Fortinet Materials"). To the extent any Fortinet Materials are necessarily required for the proper functioning of the Deliverables (such that the Deliverables will not function without the Fortinet Materials) or are embedded into the Deliverables, Fortinet grants to Company a perpetual, nonexclusive, non-transferable, royalty-free, worldwide license to use such Fortinet Materials solely in conjunction with its use of such Deliverables. Company acknowledges that the Fortinet Materials are Confidential Information of Fortinet, regardless of whether so designated. This section shall not prohibit fee-based licensing of certain intellectual property of Fortinet as may be agreed by the Parties.

## 6. REPRESENTATIONS, WARRANTIES AND COVENANTS

- 6.1. Authority to Contract. The Parties each represent and warrant that they have obtained all necessary corporate approvals to enter into these terms and conditions and that no consent, approval, or withholding of objection is required from any external authority with respect to the entering into of these terms and conditions. The Parties further represent and warrant that they are under no obligation or restriction, nor will they assume any such obligation or restriction, that would in any way interfere or conflict with any obligations under these terms and conditions.
- 6.2. Compliance with Laws. The Parties covenant that they will comply with all applicable laws and regulations in their conduct pursuant to these terms and conditions. The Parties further covenant that a change in laws that materially alters the assumptions upon which Fortinet entered these terms and conditions or a particular SOW shall warrant a Change Order.
- 6.3. Warranty on Services. Fortinet warrants that it will perform the Services in a professional and workmanlike manner and that its personnel have the requisite skills and experiences to perform the Services. Company agrees that in the event of a breach of the foregoing warranty, its only remedy shall be the re-performance of the Services by Fortinet.
- 6.4. Warranty Disclaimer. EXCEPT AS EXPRESSLY PROVIDED IN THIS SECTION 6, FORTINET EXCLUDES AND DISCLAIMS ALL OTHER WARRANTIES, CONDITIONS OR STATEMENTS, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR THAT DELIVERABLES WILL BE ERROR-FREE

## 7. INDEMNIFICATION

- 7.1. Subject to Section 8, Company shall indemnify, defend, and hold harmless from and against any damages, costs, attorneys' fees, penalties, fines, liabilities, or expenses that arise from third party actions or claims (collectively, "Losses") against Fortinet and its affiliates, officers and directors, employees, agents, and representatives relating to (a) death or injury to persons caused by the Company; (b) a violation of applicable laws by the Company; or (c) Company's infringement of a third Party's intellectual property rights where such third Party is located in either the country where the Services were provided or received.
- 7.2. Subject to Section 8, Fortinet shall indemnify, defend, and hold harmless from and against any damages, costs, attorneys' fees, penalties, fines, liabilities, or expenses that arise from third party actions or claims (collectively, "Losses") against Company relating to (a) death or injury to persons caused by the Fortinet; or (b) Fortinet's infringement of a third Party's intellectual property rights where such third Party is located in either the country where the Services were provided or received, provided however that Fortinet shall not have any liability to Company under this Section to the extent that any infringement or claim thereof is attributable to: (i) the combination, operation or use of a Deliverable with equipment or software supplied by Company where the Deliverable would not itself be infringing; (ii) compliance with designs, specifications or instructions provided by Company; (iii) use of a Deliverable in an application or environment for which it was not designed or contemplated under these terms and conditions; or (iv) modifications of a Deliverable by anyone other than Fortinet where the unmodified version of the Deliverable would not have been infringing. Fortinet will completely satisfy its obligations hereunder if, after receiving notice of a claim, Fortinet obtains for Company the right to

continue using such Deliverables as provided without infringement, or replace or modify such Deliverables so that they become non-infringing.

- 7.3. Promptly after an indemnitee receives notice of any claim for which it will seek indemnification pursuant to these terms and conditions, the indemnitee will notify the indemnitor of the claim in writing. No failure to so notify the indemnitor will abrogate or diminish the indemnitor's obligations under this Section if the indemnitor has or receives knowledge of the claim by other means or if the failure to notify does not materially prejudice its ability to defend the claim. Within fifteen (15) days after receiving an indemnitee's notice of a claim, but no later than ten (10) days before the date on which any formal response to the claim is due, the indemnitor will notify the Indemnitee in writing as to whether the indemnitor acknowledges its indemnification obligation and elects to assume control of the defense and settlement of the claim (a "**Notice of Election**"). In issuing a Notice of Election, the indemnitor waives any right of contribution against the indemnitee unless the Notice of Election expressly states that indemnitor believes in good faith that the Indemnitee may be liable for portions of the claim that are not subject to indemnification by the Indemnitor, in which case the indemnitee will have the right to participate in the defense and settlement of the claim at its own expense using counsel selected by it.
- 7.4. If the indemnitor timely delivers a Notice of Election, it will be entitled to have sole control over the defense and settlement of the claim except as provided in the immediately preceding paragraph. After delivering a timely Notice of Election, the indemnitor will not be liable to the Indemnitee for any attorneys' fees subsequently incurred by the indemnitee in defending or settling the claim. In addition, the indemnitor will not be required to reimburse the indemnitee for any amount paid or payable by the indemnitee in settlement of the claim if the settlement was agreed to without the written consent of the indemnitor.
- 7.5. If the indemnitor does not deliver a timely Notice of Election for a claim, the indemnitee may defend and/or settle the claim in such manner as it may deem appropriate, and the indemnitor will promptly reimburse the indemnitee upon demand for all Losses suffered or incurred by the Indemnitee with respect to the claim.
- 7.6. Exclusive Remedy. This Section 7 "Indemnification" constitutes the exclusive rights and remedies for the matters indemnified.

## 8. LIMITATION OF LIABILITY

- 8.1. Limitation of Liability. NOTWITHSTANDING ANYTHING TO THE CONTRARY ELSEWHERE CONTAINED IN THESE TERMS AND CONDITIONS, NEITHER PARTY SHALL, IN ANY EVENT, REGARDLESS OF THE FORM OF CLAIM, BE LIABLE FOR (1) ANY INDIRECT, SPECIAL, PUNITIVE, EXEMPLARY, SPECULATIVE OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, ANY LOSS OF USE, LOSS OF DATA, BUSINESS INTERRUPTION, AND LOSS OF INCOME OR PROFITS, IRRESPECTIVE OF WHETHER IT HAD AN ADVANCE NOTICE OF THE POSSIBILITY OF ANY SUCH DAMAGES; OR (2) DAMAGES RELATING TO ANY CLAIM THAT ACCRUED MORE THAN TWO (2) YEARS BEFORE THE INSTITUTION OF ADVERSARIAL PROCEEDINGS THEREON. TOTAL LIABILITY. SUBJECT TO THE ABOVE AND NOTWITHSTANDING ANYTHING TO THE CONTRARY ELSEWHERE CONTAINED HEREIN, THE MAXIMUM AGGREGATE LIABILITY OF FORTINET SHALL BE, REGARDLESS OF THE FORM OF CLAIM, THE CONSIDERATION RECEIVED BY FORTINET FOR THE STATEMENT OF WORK TO WHICH THE CLAIM RELATES DURING THE PRECEDING THREE (3) MONTHS. FOR CLAIMS THAT ARISE UNDER THESE TERMS AND CONDITIONS AND THAT DO NOT LOGICALLY RELATE TO A PARTICULAR STATEMENT OF WORK, THE MAXIMUM AGGREGATE LIABILITY OF FORTINET SHALL BE THE SUM OF THE CONSIDERATION RECEIVED UNDER ALL ACTIVE STATEMENTS OF WORK UNDER THESE TERMS AND CONDITIONS FOR THE PRECEDING THREE (3) MONTHS.

## 9. TERMINATION

- 9.1. Termination for Convenience. Fortinet may, without cause or for convenience, terminate any SOW and/or these terms and conditions upon written notice of two (2) months to the other party.
- 9.2. Termination for Cause. Either Party may terminate any SOW upon written notice to the other in the event that: (a) the other Party commits a material breach of these terms and conditions or Statement of Work and fails to cure such default to the non-defaulting Party's reasonable satisfaction within thirty (30) days after receipt of notice; or (b) the other Party becomes insolvent or bankrupt, assigns all or a substantial part of its business or assets for the benefit of creditors, permits the appointment of a receiver for its business or assets, becomes subject to any legal proceeding relating to insolvency or the protection of creditors' rights or otherwise ceases to conduct business in the normal course.
- 9.3. Effects of Termination. In the event of termination of an SOW hereunder, Company shall pay Fortinet: (1) all fees as specified in the SOW and expenses up to the effective date of the termination, including work in progress, plus fees for the applicable notice period irrespective of whether Company requires Fortinet's services during such period; and (2) any termination charges agreed by the Parties. If these terms and conditions is terminated before all SOWs executed hereunder are terminated or completed, the terms of these terms and conditions shall remain in full force until the termination or completion of such Statements of Work.



## 10. MISCELLANEOUS

- 10.1. Relationship of the Parties. It is understood and agreed that Fortinet will provide services under these terms and conditions as an independent contractor and that during the performance of Services under these terms and conditions, Fortinet's employees will not be considered employees of Company for any purpose whatsoever. Accordingly, Fortinet shall be solely responsible for the compensation of such employees and all employment-related taxes. Further, nothing herein shall be construed to entitle either Party to be a representative, agent, partner or joint venturer of the other.

## 11. FORCE MAJEURE

- 11.1. Force Majeure. Except for the obligation to make payments, nonperformance of either party shall be excused to the extent performance is rendered impossible by strike, fire, flood, governmental acts or orders or restrictions, failure of suppliers or any other reason where failure to perform is beyond the reasonable control of and is not caused by the negligence of the non-performing party. In the event such an event prevents performance thereunder for a period in excess of sixty (60) days, then the non-defaulting party may elect to terminate these terms and conditions and/or cancel or suspend any SOWs thereunder by a written notice to the defaulting party.

## 12. DISPUTE RESOLUTION

- 12.1. Dispute Resolution and Venue. Any controversies or claims arising from or relating to these terms and conditions, or the breach or validity thereof, which cannot be amicably settled by and between the parties, shall be referred to and finally settled by arbitration. The place of arbitration shall be Santa Clara, California, pursuant to the Streamlined Arbitration Rules and Procedures of Judicial Arbitration and Mediation Services (JAMS), or its successor, before a sole, mutually agreeable arbitrator, in accordance with the laws of the State of California for agreements made in and to be performed in that State.

## 13. GENERAL

- 13.1. Governing Law. These terms and conditions shall be interpreted and construed in accordance with the laws of the State of California, without regard to its conflicts of laws provisions.
- 13.2. Headings. The headings used in these terms and conditions are for the convenience of the Parties only and shall not be deemed a part of, or referenced in, construction of these terms and conditions.
- 13.3. Assignments. These terms and conditions will be binding on the Parties hereto and their respective successors and assigns. Neither Party may assign these terms and conditions or SOWs without the prior written consent of the other. Any assignment by operation of law, order of any court, or pursuant to any plan of merger, consolidation or liquidation, will be deemed an assignment for which prior consent is required and any assignment made without any such consent will be void and of no effect as between the Parties. Notwithstanding the forgoing Fortinet may assign these terms and conditions pursuant to a merger, acquisition, or sale of at least fifty percent (50%) its assets without consent.
- 13.4. Entire Agreement. The provisions of these terms and conditions, including any appendices, schedules, exhibits, or SOWs referred to herein and/or attached hereto, constitute the entire agreement between the parties with respect to the subject matter hereof, and these terms and conditions supersedes all prior agreements or representations, oral or written, regarding such subject matter. Except as provided for in these terms and conditions, these terms and conditions may not be modified or amended except in a writing signed by a duly authorized representative of each party, and, furthermore, Company acknowledges and agrees that Fortinet is not bound by any purported amendment or new agreement signed by a representative of Fortinet other than Fortinet's General Counsel. For clarity, only Fortinet's General Counsel is authorized to alter, amend, or modify these terms and conditions in any way or enter a new agreement on behalf of Fortinet or its affiliates, and any amendment or new agreement that is not signed by Fortinet's General Counsel, regardless of whether including a Fortinet, or Fortinet affiliate, company seal or chop, is null and void and of no force and effect.
- 13.5. Modifications. No amendment or change to these terms and conditions or any waiver or discharge or any rights or obligations under these terms and conditions will be valid unless in writing and signed by an authorized representative of the Party against which such amendment, change, waiver or discharge is sought to be enforced.
- 13.6. Severability. In the event that any provision of these terms and conditions conflicts with the law under which these terms and conditions is to be construed or if any such provision is held invalid by a competent authority, such provision will be deemed to be restated to reflect as nearly as possible the original intentions of the Parties in accordance with applicable law. The remainder of these terms and conditions will remain in full force and effect.
- 13.7. Survivability. Any provision of these terms and conditions that contemplates performance or observance subsequent to termination or expiration of these terms and conditions will survive termination or expiration of these terms and conditions and continue in full force and effect, including the following:

Pricing, Invoicing, and Payment (Section 3)  
Confidentiality (Section 4)  
Proprietary Rights (Section 5)  
Representations, Warranties, and Covenants (Section 6)  
Indemnification (Section 7)  
Limitation of Liability (Section 8)  
Dispute Resolution (Section 12)  
General (Section 13).

Notices. All notices, requests, demands and determinations under these terms and conditions other than routine operational communications will be in writing through (i) hand delivery, (ii) express overnight courier with a reliable system for tracking delivery, or (iii) confirmed facsimile or electronic mail with a copy sent by another means specified herein, to the following:

If to Fortinet: Fortinet, Inc.  
899 Kifer Rd  
Sunnyvale, CA 94086  
Attn: General Counsel  
  
with a copy to: Chief Financial Officer

If to Company: Address as set forth in the Statement of Work between  
Company and Fortinet.

June 2016

-----End of Document-----





## CASE STUDY

# Creating the Perfect Environment To Learn: Safely, Securely, and Without Interruption



Trenton Public Schools is a comprehensive community public school district educating 11,500 students in prekindergarten through 12th grade from Trenton, in Mercer County, New Jersey. With 25 buildings serving 13 elementary schools, four middle schools, and three high schools, the district is dedicated to helping all students graduate with a vision for their future, motivated to learn continually and prepared to succeed in their choice of college or career.

Over a multiproject, multiyear timeline, the Trenton IT team has worked with Fortinet and its technology partner, Advanced Computer Solutions Group (ACSG), to meet the district's evolving network infrastructure needs. From standardized testing to internet use and the related risks of a cyber world, educating students in a secure and protected environment is of paramount importance for Trenton school district.

## Electronic Testing Requires Greater Speed

The Partnership for Assessment of Readiness for College and Careers (PARCC) is a consortium of six states that includes New Jersey, working to collaboratively develop a common set of examinations to measure student achievement of the Common Core State Standards and preparedness for college and careers.

Firewalls became pertinent when the PARCC electronic assessments replaced the existing statewide testing, and the Trenton legacy network was unable to handle the demands. Dennis Morgan, director of IT for Trenton Public Schools, recalls, "We needed to invest in our wide-area network (WAN) and internet feeds as our environment was no longer capable of supporting the speed and bandwidth that were required. On any given day, the infrastructure needs to be able to support almost 12,000 endpoints and we just weren't able to handle all the traffic."

## Network Security With Visibility

Led by Morgan, the Trenton technical team sought a robust firewall replacement. With a recommendation from its technology partner ACSG, the Fortinet FortiGate quickly became the top candidate because of its industry-leading threat protection and performance. Morgan recounts, "We did a lot of research and the FortiGate always has excellent reviews and an extremely competitive price point. Ease of use and low operational overhead are two additional factors of the FortiGate that seem to be consistently highlighted by reviewers and existing users."

*"Fortinet is the brand I know I can trust to deliver what we need."*

*– Dennis Morgan, Director of IT,  
Trenton Public Schools*

## Details

**Customer:** Trenton Public Schools

**Industry:** Education

**Location:** New Jersey

**Partner:** Advanced Computer Solutions Group

## Business Impact

- Enhanced, infrastructurewide protection and visibility
- Cost and resource savings
- Maximized uptime with high-availability firewalls and removing single points of failure
- State-of-the-art protection against distributed denial-of-service (DDoS) attacks ensures services are uninterrupted

An on-site proof of concept was conducted to verify the suitability of the FortiGates in the Trenton environment. Morgan and his colleagues had multiple conversations with the technical staff of other Fortinet deployments that were similar to the proposed Trenton implementation. At the successful conclusion of the evaluation phase, a decision was made to partner with Fortinet.

A pair of FortiGate next-generation firewalls (NGFWs) were deployed in a high-availability configuration to support the newly acquired 10 Gig bandwidth internet connection. The solution provided built-in redundancy and included comprehensive threat protection and web filtering. “We were able to consolidate multiple systems and functions onto the pair of FortiGates,” Morgan states. “Having no single points of failure and the refreshing ease of having one location to review logs and complete daily audits are huge benefits for us.”

The implementation went well thanks to a solid product and a trusted implementation team. Morgan comments, “Working with Fortinet and ACSG was excellent—with full support through the whole deployment process—the expertise and work ethic are amazing. During the initial setup, the FortiGate’s intuitive interface made it very easy to audit the network and decide which rules were valid and which could be easily omitted.”

## Solutions

- FortiGate
- FortiDDoS
- FortiVoice with over 500 handsets

## Adding DDoS Protection

DDoS attacks have become more prevalent with colleges and high schools seeing an escalating number of attempted breaches. While Trenton had not experienced any issues, several other school districts and colleges in New Jersey had been impacted.

To proactively address the increasing risk and based on the success of the FortiGate implementation, Morgan consulted with ACSG and the recommendation once again was Fortinet. He describes, “We tested and then bought a FortiDDoS appliance: We wanted to get ahead of the risk before Trenton became another statistic.”

The FortiDDoS provides 100% heuristic/behavior-based detection that is completely transparent to would-be attackers. The massively parallel architecture simultaneously monitors hundreds of thousands of parameters to alleviate the possibility of throughput interruptions caused by flawed analysis. The appliance is equipped with comprehensive reporting and analysis tools that are administered sharing the same console used for the district’s FortiGates.

## FortiVoice: Quality and Savings

As with many IT teams in the education sector, in addition to multiple other duties, Morgan and his colleagues also are responsible for managing and maintaining the district’s extensive phone system. When the Trenton team began looking for a replacement for the district’s aging legacy Voice-over-Internet-Protocol (VoIP) phone system, options ranged from the poorly made to the outrageously expensive.

After discussions with ACSG, a recommendation was made to evaluate Fortinet’s business phone system, FortiVoice. “We thoroughly tested all the components—the handsets are well made, and the service quality is excellent—and it was an easy sell to our School Board,” says Morgan. “Not only was this deployment the smoothest phone cutover that I have been a part of but with 500 extensions in place, we are able to lower our phone costs by close to 60%.”

## Value for Money

Education costs are rising, school budgets are tighter, and everyone is expected to do more with less. Sophisticated protection from Fortinet, and the ACSG/Fortinet partnership, have made it easier for Trenton Public Schools to offer a safe and adaptable infrastructure to its students and staff.

Morgan summarizes, “Today with Fortinet, our infrastructure is significantly more secure and has a greatly improved cost efficiency. We’ve been able to put advanced security measures in place to ensure that our students are not exposed to the massive number of negative elements that are out on the web. This is critically important to everyone in the district and Fortinet is the brand I know I can trust to deliver what we need.”



www.fortinet.com



# NEXT-GENERATION NETWORK SECURITY for 21<sup>st</sup>-Century Classrooms

**Forward-thinking schools are adopting personalized learning to transform the education landscape and increase student achievement.** Broward County Public Schools in Florida recently implemented its Digital 5: Pathways to Personalized Learning initiative, in which every fifth-grade student in approximately 100 of the district's elementary schools is provided with a mobile device, digital resources and online instructional material.

However, the district's dive into personalized learning — along with several other digital initiatives and an increased demand for bandwidth — required network expansion and new security measures. To meet these needs, the district implemented Fortinet's next-generation firewall solution — FortiGate.

Fortinet's consolidated approach to network security provided the district with the security, flexibility, scalability and manageability necessary to meet the district's growing bandwidth needs. On any given day there are approximately 125,000 devices connected to the district's network with plans to add more. "In the past we had a number of point products that we used for traffic shaping, content filtering and more. At the time they served us well, but it became time to grow, so we went with the Fortinet solution that embedded a number of those

into one platform," says Doug Pearce, director of technical support services at Broward County Public Schools.

The FortiGate platform protects the district's data center while providing a safe Internet experience for students and staff via the personalized learning initiative. "It's incumbent on school districts to provide a safe and secure environment for the kids. That is not just a fundamental moral obligation, but also a requirement of certain regulations and E-rate, in which we participate," says Pearce.

Fortinet, the global leader in high-performance cybersecurity solutions, positions schools, colleges and libraries to respond rapidly to a sophisticated cyber-threat landscape. "We are very proud to be protecting a number of schools and school districts across the country, enabling them to focus on the real objective at hand — providing students with a safe and uninterrupted learning environment," says Bryan Wood, Fortinet's vice president of education. Fortinet's consolidated approach to network security provides unparalleled performance and ease of management, coupled with significant savings. Strengthened by the industry's highest level of threat research, intelligence and analytics from FortiGuard Labs, Fortinet delivers best-in-class protection to provide the safest and most secure digital learning environments.


To learn more about Fortinet's cybersecurity solutions for education, please visit [www.fortinet.com/solutions/education.html](http://www.fortinet.com/solutions/education.html) or contact [education@fortinet.com](mailto:education@fortinet.com).

**FORTINET®**

**E-RATE**  
ELIGIBLE SOLUTIONS



## NAC PROVIDES SECURE BYOD AND AIDS HIPAA COMPLIANCE AT UC IRVINE MEDICAL CENTER



*"With 100% visibility and control over every device and user on our network, we can define and enforce granular policies to manage risk and ensure compliance."*

— Jeff Barnes  
Information Security Officer  
University of California, Irvine



A world-class academic medical center with a full range of acute and general-care services, University of California's Irvine Medical Center is at the forefront of medical education and research and prides itself on delivering the highest quality patient care.

At UC Irvine Medical Center, mobile devices such as iPhones and iPads are a way of life for doctors, professors, medical students, and staff. When Allscripts, which supplies the medical center's electronic medical record (EMR) system, announced it was developing a mobile app, "We knew our doctors and medical personnel would be clamoring to use this application," explains Adam Gold, Director of Emerging Technologies at UC Irvine Medical Center. "The time had come when we needed a BYOD strategy that would enable our staff to securely use their own devices at the medical center."

Several challenges would need to be overcome along the way. The most pressing concern was protecting HIPAA-compliant data. Gold recognized that security had to start at the endpoint, so only approved, secure devices are allowed on the network.

### MANAGING SECURE EMR ACCESS AND HIPAA CONCERNS

Physicians, instructors, students, and hospital staff interact with the EMR system differently, and varied access levels had to be easy to define and applied automatically. The hospital also had to enforce its security policies without appearing heavy-handed, so users could get on the network easily with personal devices while EMR access continued to be protected.

Concerns about regulatory compliance were particularly daunting. Hospitals are subject to internal and external audits to verify that sensitive HIPAA information like patient records and research data is secure and protected from misuse. Demonstrating compliance is hard enough when all devices are under internal control, but a BYOD environment adds an even greater layer of uncertainty. With HIPAA fines that can reach millions of dollars, ensuring and documenting compliance is crucial. UC Irvine required complete endpoint visibility, and the ability to define access levels, for every device connecting to its network.

### DETAILS

**CUSTOMER:** UC Irvine Medical Center

**INDUSTRY:** Medical

**LOCATION:** Irvine, California

### BUSINESS IMPACT

- Automatically identifies every device and user accessing the network, and blocks unsafe devices and unauthorized users
- Automatically provisions network access according to the user's specific profile
- Help desk calls were reduced by 30% because users can manage their own devices
- Ability to demonstrate regulatory compliance with a few clicks

### DEPLOYMENT

- Network Access Control

USING NAC FOR FULL VISIBILITY AND CONTROL TO DEMONSTRATE HIPAA COMPLIANCE

UC Irvine Medical Center chose the Fortinet Network Access Control (NAC) solution to solve the problem of visibility and access control, while providing traceability to demonstrate HIPAA compliance across the operation. To address the BYOD and mobile access security challenge, the NAC solution integrated with mobile device management (MDM) software. MDM software enables the medical center to have stronger control over BYOD and hospital-owned mobile devices. To access the network, mobile devices must download the MDM app. This app ensures that each device is provisioned for safe access, correlates devices with owners, and confirms that each device has the minimum required antivirus and system patches, before the device can access the network. MDM software can also help locate or wipe devices that are lost or stolen to prevent unauthorized network access. These controls are critical to ensure the integrity of the network and HIPAA compliance.

NAC also enables UC Irvine to identify every endpoint and device connected to its network in real time. It can identify any potential unauthorized device and quarantine it immediately. NAC keeps a history of activity for each individual device and endpoint, so it can identify any suspicious activity, as well as provide records of all data access.

In addition, NAC enables the medical center to easily control permission and access, ensuring that each device accesses only the necessary data for their particular function. NAC's ability to offer role-based access permissions is another key criterion for keeping HIPAA-compliant data secure.

UC Irvine is very pleased with the solution. The medical center even saw a 30% reduction in help desk calls, as NAC provides an automated help and remediation page. NAC offers the HIPAA-compliant security they require, along with an efficient, user-friendly experience that keeps productivity high in the fast-paced medical environment.



GLOBAL HEADQUARTERS  
Fortinet Inc.  
899 Kifer Road  
Sunnyvale, CA 94086  
United States  
Tel: +1.408.235.7700  
[www.fortinet.com/sales](http://www.fortinet.com/sales)

EMEA SALES OFFICE  
905 rue Albert Einstein  
06560 Valbonne  
France  
Tel: +33.4.8987.0500

APAC SALES OFFICE  
8 Temasek Boulevard #12-01  
Suntec Tower Three  
Singapore 038988  
Tel: +65-6395-7899  
Fax: +65-6295-0015

LATIN AMERICA HEADQUARTERS  
Sawgrass Lakes Center  
13450 W. Sunrise Blvd., Suite 430  
Sunrise, FL 33323  
Tel: +1.954.368.9990

## CASE STUDY

# Illinois State Treasurer's Office Sets an Example for State Agency Cybersecurity

Chief Information Officer (CIO) Joseph Daniels for the Illinois State Treasurer is responsible for protecting an extremely large financial institution against cyber threats. "The Treasurer is the Banker for the state, which has \$32 billion in assets," says Daniels. "That is a large amount of financial resources to manage and to secure for our constituents."

The agency's legacy security environment was challenging to maintain. To strengthen security and streamline management, the Illinois State Treasurer rolled out several integrated Fortinet solutions. The user interfaces and single-pane-of-glass visibility of the new infrastructure make life easier for the agency's security staff. They have also proven highly effective at threat detection, helping the agency pass, with flying colors, a required external security audit.

## The Pursuit of Security Best Practices

Cybersecurity is a major concern for Daniels. "Obviously, the cyber threat landscape changes every day," he says. "If you are not following best business practices and utilizing a layered approach to security, it is hard to combat advanced threats." However, as a relatively small state agency, the Illinois State Treasurer faces staffing constraints that complicate the pursuit of best practices. The IT team has 22 staff members, only 4 of whom have cybersecurity responsibilities.

Cybersecurity is a major concern for Daniels. "Obviously, the cyber threat landscape changes every day," he says. "If you are not following best business practices and utilizing a layered approach to security, it is hard to combat advanced threats." However, as a relatively small state agency, the Illinois State Treasurer faces staffing constraints that complicate the pursuit of best practices. The IT team has 22 staff members, only 4 of whom have cybersecurity responsibilities.

The agency had been standardized on another vendor's firewalls and other security solutions for decades, but those products were expensive and difficult to manage. Daniels needed to make a change. The Illinois State Treasurer was already using a FortiGate appliance for virtual private network (VPN) functionality. When Daniels learned that it was a fully functional next-generation firewall (NGFW), he looked into moving into a trial. Daniels had heard positive feedback about Fortinet from his peers at a large private-sector financial firm. His team embarked on a proof of concept with a FortiGate NGFW and immediately liked its ease of use. Within a few weeks of launching the NGFW proof of concept, Daniels had removed a significant portion of his existing cybersecurity architecture and replaced it with Fortinet solutions.

Daniels and his team also liked the Fortinet Security Fabric that provided the tight integration between FortiGate NGFWs and the FortiSandbox solution, which can execute questionable code in an isolated environment to determine whether the



*"Without the partnership with Fortinet, we would not have been able to shed light for our partner agencies, very similar to our own, on the importance of looking outside of the box for the way they do security."*

- Joseph Daniels, Chief Information Officer, Illinois State Treasurer

## Details

**Customer:** Illinois State Treasurer's Office

**Industry:** Government

**Location:** Springfield, Illinois

## Business Impact

- Simplifies training of limited security staff through single-pane-of-glass visibility
- Enabled rare perfect score on information-security audit, thanks to completeness of weekly threat assessments

code represents a true threat. When he joined the Illinois State Treasurer two years ago, the organization had a significant security backlog. Its infrastructure included over 2,500 different applications, many of which had not been assessed for potential threats in several years. An internal analysis of applications running on Treasury systems using FortiSandbox revealed several unwanted applications.

## Integrated Security Visibility, Improved Usability

In addition to FortiGate NGFWs and FortiSandbox, the Treasurer's Office rolled out FortiGate Cloud, a Software-as-a-Service (SaaS) solution that provides cloud-based management of FortiGate NGFWs. "FortiGate Cloud provides cyber threat assessment reports that I started having delivered every single week because they gave us a really good overview of our environment," Daniels says. The Treasurer's Office is also using FortiWeb, a web application firewall (WAF), to protect a cloud deployment in Microsoft Azure.

The FortiGate NGFWs enable the security team to achieve greater visibility into their network and isolate network traffic to a particular endpoint or application, something the legacy firewalls could not do. Any malware attempting to beacon out to a command-and-control server or perform data exfiltration will be rapidly identified and eradicated. Moreover, the Fortinet infrastructure consolidates information about threat detection and response networkwide, which is essential for securing sensitive data, such as account or routing numbers, and connections with external financial institutions. "Having that single-pane-of-glass visibility makes security management a lot easier," Daniels says.

The Fortinet solutions are also meeting expectations with regard to usability. The four-person security team needs to be able to easily onboard new employees and cross-train for different job roles. The FortiGate NGFWs make this possible. "They could come in, use the GUI, look at policies and procedures, follow all the training material out there, and really make the firewall the first secure point of entry for the agency."

Beyond training to achieve basic familiarity, Fortinet's extensive library of videos and guides have made it possible for the Treasurer's staff to solve many security problems without requiring external support. Daniels says, "You can walk step by step, from inception to completion, through all the training videos Fortinet provides. That documentation is critical for agencies without a huge staff because you can take anyone and walk them through it."

On the rare occasion that the team has experienced difficulties they cannot solve on their own—whether security issues or general IT challenges—the Fortinet support team has always been ready to help. According to Daniels, "If I could say anything, they are probably overly helpful. They keep our staff on track."

## Compliance Audit

With being not only a state government agency but also a financially regulated office, the Illinois State Treasurer undergoes frequent audits. Each year, the organization undergoes 12 months of internal audits and 9 months of review by an external auditor.

Daniels' team recently underwent their first information security audit, which occurs every two to five years, under his tenure. At that point, the organization had a partnership in place with Fortinet and had rewritten policies and procedures to follow the guidelines of the National Institute of Standards and Technology (NIST) and Microsoft's Security and Compliance Framework.

During the audit, Daniels says the weekly security reports provided by FortiGate Cloud were a critical resource. They provided him with the hard data necessary to answer auditors' questions and demonstrate compliance with required security controls. As a result, the audit passed without issue.

## Business Impact (contd.)

- Revealed suspicious applications lying dormant for 2-3 years through sandbox analysis
- Meets unclaimed property monitoring requirements and enables an unclaimed property "museum" with FortiCamera

## Solutions

- FortiGate NGFW with Enterprise
- FortiCare Support
- FortiSandbox
- FortiGate Cloud
- FortiCamera
- FortiAnalyzer
- FortiWeb

*"You can walk step by step, from inception to completion, through all the training videos Fortinet provides. That documentation is critical for agencies without a large staff because you can take anyone and walk them through it."*

- Joseph Daniels, Chief Information Officer, Illinois State Treasurer

However, Daniels believes in continuously working to improve his organization's security to meet evolving cyber threats. Since the audit, he has purchased FortiAnalyzer and is working to take advantage of its improved visibility and security analytics. "The FortiAnalyzer provides a much deeper dive into our network, so I am looking forward to the next audit that we have. We will be much better prepared."

## **An Integrated Platform Unlocks New Capabilities**

While network security is a significant priority for Daniels' team, it is not their only concern. The Illinois State Treasurer is also responsible for managing the lost and unclaimed property of Illinois residents. The agency's unclaimed-property division faces stringent security and auditing requirements, undergoing continuous external audits. Since the department is responsible for properly managing and securing property that belongs to Illinois citizens, every transaction and movement in the secure vaults requires constant video monitoring.

The unclaimed-property division had cameras deployed for surveillance of the vaults, but they were not meeting the organization's needs. The video feeds had poor picture quality and would occasionally fail. The team chose the FortiCamera surveillance solution to replace these impractical cameras. FortiCamera not only meets their requirements with impeccable picture quality and advanced monitoring capabilities but also seamlessly integrates into the Fortinet Security Fabric. This integration enables the security team to monitor the FortiCameras from the same dashboard as the rest of the agency's security architecture.

## **Providing an Example for Other Government Agencies**

Deploying Fortinet solutions has enabled the Illinois State Treasurer to act as an example for other state government agencies. Daniels participates in weekly calls with external agencies, where they share information about the security challenges that they are facing and how they are addressing them. According to Daniels, "Without the partnership with Fortinet, we would not have been able to shed light for our partner agencies, very similar to our own, on the importance of looking outside of the box for the way they do security."



[www.fortinet.com](http://www.fortinet.com)



## CASE STUDY

# County Government Agency Increases Visibility and Control of Entire Infrastructure

The Information Security (IS) team for Salt Lake County, Utah, supports up to 6,500 end-users across a variety of locations and business types. A team of only seven is responsible for maintaining security and managing user access for services and businesses across the entire county—including Salt Lake City.

## Replacing End-of-Life Legacy Hardware

About ten years ago, Salt Lake County first started working with Fortinet after existing security appliances from another vendor started having problems toward their end of life. They opened a request for proposals (RFP) to evaluate competing solutions. While price was a factor, they wanted physical next-generation firewalls (NGFWs) that could deliver ample performance and features for their needs at the time—which included protecting two internet feeds and two extranet partner feeds. Additionally, they knew they would need to scale their capabilities for growth in the near future.

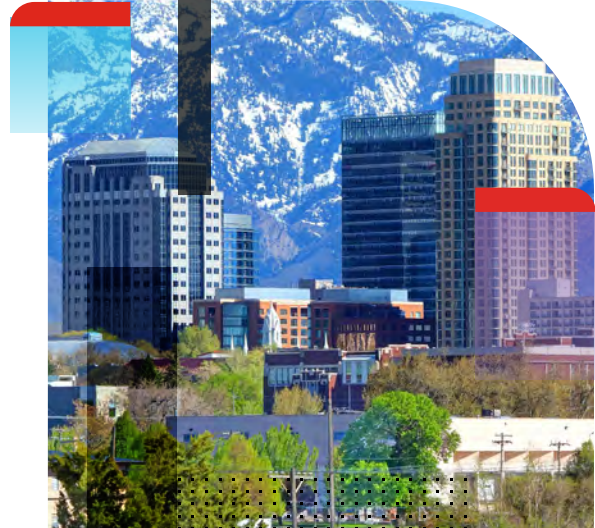
They initially chose FortiGate 600-series NGFWs for three different clusters to protect county networks. “Fortinet was miles ahead of everyone else in terms of ability and performance. That’s what impressed us. And I think Fortinet still outdoes everybody else when it comes to performance,” says Salt Lake County’s director of information security. This included the ability to perform deep packet inspections for encrypted traffic. Before working with Fortinet, the Salt Lake County IS team had spent several years unsuccessfully trying to implement inspection without bottlenecking network traffic.

## Changing Times and Growing Networks

Over the next decade, Salt Lake County would add more FortiGates to protect additional parts of the county’s infrastructure. Their current firewall deployments have scaled to 55 FortiGate NGFWs. One key reason for that expansion had to do with the growing number of county employees that needed a secure connection to the official network from home or in remote locations.

During the initial RFP, Salt Lake County was using another vendor’s solution for virtual private networking (VPN). When that vendor went out of business, they found themselves in need of a replacement. As Salt Lake County’s director of information security explains, “Rather than buy somebody else’s VPN, we just looked to our existing FortiGates. They were already licensed for VPN, we just hadn’t been using it. So really, it cost us nothing to change. And it saved us whatever the going rate would have been for a couple of VPN concentrators from someone else.”

Beyond perimeter protection and VPN access for employees, Salt Lake County also uses their FortiGates for WAN connections at remote sites, isolation of networks, and segmentation of PCI devices (e.g., point-of-sale [POS] terminals). They have also added other Fortinet security solutions to help complement specific security use-case needs.



*“Fortinet was miles ahead of everyone else in terms of ability and performance. That’s what impressed us. And I think Fortinet still outdoes everybody else when it comes to performance.”*

– Salt Lake County’s Director of Information Security

## Details

**Customer:** Salt Lake County

**Industry:** Government

**Location:** Utah

## Business Impact

- Enables network segmentation for PCI compliance via high-performance NGFW protection across distributed county-owned locations
- Provides secure remote login for county employees via robust virtual private network (VPN) and multi-factor authentication (MFA) capabilities

## Multi-factor authentication (MFA)

In addition to FortiGate's built-in VPN capabilities, the Salt Lake County IS team is also using FortiAuthenticator to add multi-factor authentication (MFA) capabilities to employee access for added security. One of the many things the county uses MFA for is timecard submissions across as many as 6,500 full- and part-time employees via their enterprise resource planning (ERP) system.

"Our biggest successes with Fortinet right now really includes two things. First, moving to Fortinet's VPN capabilities and being able to have multi-factor authentication has been awesome. And second, in the last couple of years, we wanted to add MFA to our applications. Previously, we were using a ridiculously expensive vendor for single-sign-on MFA. They had a whole year to prove themselves and they failed miserably," says Salt Lake County's director of information security.

As with their VPN problems, Salt Lake County looked to Fortinet to help serve their users without breaking their budget. They purchased an additional FortiAuthenticator appliance and FortiToken licenses to design their own solution—fulfilling their needs while dramatically reducing the total cost of ownership (TCO) for application MFA. "I'd say it's probably not even half of what we invested in that other solution. Our users like everything about using it and it has worked really well. We love it."

## Network Segmentation and PCI Compliance

At the majority of the county's branch locations, FortiGate NGFWs apply Layer 3 policies to segment certain things from the main county network that vendors need to access. Because the IS team does not want to connect vendors to any internal resources, they ensure vendor devices and users can only access what they need for their specific job functions—which minimizes risk to the broader organization.

The county's IS team also uses segmentation to ensure compliance with Payment Card Industry (PCI) regulations—ensuring that private credit card information of citizens who engage with county-owned businesses and services is kept safe from cyber criminals. This includes everything from people paying their taxes, donations to the aging center, visiting the local planetarium, or even making purchases at county golf courses and recreation centers.

## Endpoint Device Protection

After a frustratingly fruitless experience with another vendor's antivirus (AV) solution, Salt Lake County again looked to Fortinet for help. They needed to protect county-owned devices (e.g., laptops, desktops, servers) from malware and other endpoint-targeted attacks. They were already successfully using the Fortinet FortiClient solution to help manage IPsec VPN for county devices.

"We already had FortiClient. It works great on all our laptops. We thought, why don't we just use it everywhere? We already have the whole backend built. More licenses are all we have to buy. Fortinet has become kind of the Swiss Army knife when other people fail us," says Salt Lake County's director of information security.

They started using FortiClient for AV as well as off-network web filtering, which was a new capability added to the organization—helping to protect mobile devices from web-based attacks when using non-county network connections. "We keep coming back to Fortinet because the products work well and their price/performance beats the competition."

## Business Impact (contd.)

- Enabled cost-effective endpoint protection across all laptops, desktops, and servers—including antivirus (AV) and off-network filtering
- Simplified operations by centralizing network management and compliance reporting

## Solutions

- FortiGate
- FortiManager
- FortiAnalyzer
- FortiAuthenticator
- FortiToken
- FortiClient

*The biggest difference, really—things just work better. We have less frustration from the people."*

- Salt Lake County's Director of Information Security

## Centralized Management

As their infrastructure expanded, Salt Lake County security leaders also needed help managing the different Fortinet solutions they had deployed across the region. Scaling from three clusters of four firewalls each up to 55 individual FortiGates increases the need for greater visibility and centralized control. FortiManager was a perfect solution for their need to simplify network operations across all 55 firewalls.

Also, FortiAnalyzer provided real-time visibility into their FortiGate clusters while gaining insight into PCI compliance. As Salt Lake County's information security analyst explains, "It definitely is a huge advantage being able to centrally manage the devices—it saves time to where you have redundancies. You only have to manage it once instead of 55 times. If I had to go change a policy stack on ten firewalls, that's an hour and a half instead of five minutes."

## A Partnership Built on Solving Problems

The needs of any government organization are going to be unique to the place where network technologies are deployed. As demand for remote access grew over the last decade, Fortinet's proven NGFW capabilities helped pave the way for added support like VPN, MFA, and endpoint protection when other solutions could not achieve the same performance or cost benefits. Hopefully, Fortinet and Salt Lake County will continue to work together for another ten years—and beyond. "We've been a happy customer for a long time now," says Salt Lake County's director of information security.



[www.fortinet.com](http://www.fortinet.com)

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.



## CASE STUDY

# Propelling Research, Improving Efficiency, and Cutting Costs at University of South Carolina



Founded in 1801, the University of South Carolina system has eight campuses across the state, more than 50,000 students, and an annual budget in the billions of dollars today. The main campus in Columbia is recognized as one of the nation's top universities, with several of its undergraduate and graduate programs cited as number one in the country in various rankings. The university received \$258 million in research grants in FY 2018 and has an endowment of \$771 million.

Throughout 2017 and much of 2018, increased computing demand from campus researchers tested the capacity of the existing network and firewall infrastructure. The system suffered latency issues on a regular basis, frustrating students, faculty, and staff and impacting research projects. Worse yet, the network would occasionally become so overloaded that users were unable to access the network—once every three months or so during the worst stretch. “Each incident was different, but they all affected a large number of users,” recalls Jason Boryk, the lead architect and manager of the university's network architecture team.

After they devoted significant effort tweaking the existing system to prevent these problems, it became clear to the network architecture team that the existing infrastructure would need to be replaced. “What we had was not acceptable for a research university,” Boryk asserts. After meetings with internal stakeholders and university officials, the team began making plans to upgrade the university's Internet2 research network from 10 gigabits per second to 100 gigabits per second.

## Building a New Network

The team underwent a thorough planning process to build a state-of-the-art network backbone with robust security features built into the base architecture. “We did not want to just build the same network only 10 times bigger,” explains Jessie Hawkins, a systems architect for the university. “Rather, we strove to follow current best practices and build a robust, secure network that will serve us many years into the future.”

The infrastructure upgrade was concurrent with other technology changes that were in progress at the university. One pressing issue was that the on-premises data backup system was overloaded. “Our storage area network [SAN] was constantly at 97% of capacity, which is far more than recommended,” Hawkins says. “Rather than spend millions of dollars on more SAN capacity, we decided that we would move our backups to a cloud repository in Amazon Web Services.”

*“The ability to view the entire infrastructure on a single pane of glass is a huge benefit to our architecture, network, and security teams.”*

– Jessie Hawkins, Systems Architect,  
University of South Carolina

## Details

**Customer:** University of South Carolina

**Industry:** Education

**Location:** Columbia, South Carolina, USA



This change in the backup infrastructure was consistent with a university strategy that called for a gradual move to the cloud for most services. “In designing solutions for new applications and services, we are leveraging public and private cloud infrastructures to create a level of redundancy and stability that benefits an institution of our size,” notes Boryk. “Our goal is to gradually move legacy services to the cloud as well. Long term, we hope to use the cloud for high-availability and disaster-recovery purposes.”

## Incorporating a Robust Security

As they searched for a security solution to protect the new infrastructure, the university's team knew that it must support both on-premises and cloud-based resources, including backups to AWS. They also hoped to find a way to integrate all of the elements of the security infrastructure for centralized visibility and control.

“We have services with Azure, Amazon Web Services, and Google Cloud Platform,” Hawkins explains. “We were previously using the built-in security tools from each provider. The problem was that each tool worked a little differently. This meant that our small team had to specialize in three platforms, and the security team had to correlate security data from the three platforms manually.”

In the last half of 2018, the team underwent proofs of concept from three next-generation firewall (NGFW) vendors that included Fortinet. “We tested the ease of configuration, the general user-friendliness of the interface, the accuracy of the vendors' claims about throughput, processing power, and different firewall features,” Boryk says. “In short, we wanted a firewall solution that would scale to our current and future needs.”

## Selecting a Security Solution

FortiGate NGFWs quickly moved to the top of the list among the three major providers included in the proof of concept for several reasons. “Fortinet had, by far, the most scalable solution,” Boryk begins. “Its native 100-gigabit interface was a perfect fit for our new infrastructure, whereas no other vendor had comparable levels of throughput. Additionally, configuration was a much easier process than with the other firewalls, and in general, the FortiGate NGFWs were much easier to work with.”

Another major benefit of FortiGate NGFWs was the ability to integrate the entire security architecture—from the new data center infrastructure to the three cloud platforms—using the Fortinet Security Fabric. “The ability to view the entire infrastructure on a single pane of glass is a huge benefit to our architecture, network, and security teams,” Hawkins relates. The Fortinet Security Fabric provides an integrated security architecture to ensure that incident detection and response and remediation efforts are fully coordinated and optimally effective.

## Deploying the NGFWs

The university began by deploying six FortiGate 7060E NGFWs in the data center at its main campus, pushing them live in January 2019. “We opted for the top-of-the-line boxes because of our speed requirements and the relative ease of configuration at the scale where we are operating,” Hawkins explains. The team deployed FortiManager and FortiAnalyzer at the same time to provide centralized management, security automation, and robust reporting capabilities.

## Business Impact

- Reallocated 40 to 80 staff hours monthly for architecture team due to stability of new network infrastructure
- \$5 million cost avoidance for SSL/TLS inspection appliances required for competing solutions
- 27 staff hours in potential savings for each VPN setup
- 180 staff hours per year saved on a single, semiweekly report produced by the network team
- 15% reduction in storage cost
- Better coordination among the architecture, network, and security teams via centralized management and visibility

## Solutions

- FortiGate
- FortiManager
- FortiAnalyzer
- FortiSandbox Cloud
- Fortinet Professional Services
- Fortinet Network Security Academy
- FortiCare First program (Advanced Services technical support contract)

While the team currently routes all cloud traffic through the physical boxes using virtual domains (VDMs), they are conducting a trial of FortiGate VM virtual NGFWs to eventually protect virtual and cloud resources. “We expect the ease of configuration to be even greater with the virtual firewalls, which will be integrated seamlessly with the physical ones,” Boryk states.

The network team has activated, or is planning to activate, the secure sockets layer (SSL)/transport layer security (TLS) encryption, application control, intrusion prevention system (IPS), antivirus, and web filtering functionalities in the NGFW. “Having the SSL/TLS encryption built into the firewall was a requirement from our security team,” Boryk explains. “Other vendors we considered did not have the same level of capability and integration we needed without having to invest in separate SSL/TLS inspection appliances, integrate them into the network, and spend valuable time managing them.”

## Getting a Jump-start with Fortinet Services

The university received assistance with the initial deployment from a resident engineer from Fortinet Professional Services. “During our first engagement, our engineer got the firewalls up and functioning, explained configuration and troubleshooting to us, and deployed FortiManager and FortiAnalyzer,” Boryk remembers. “We also purchased an additional three-month engagement, during which we hope to create a more comprehensive firewall strategy and start working to thin our legacy rule set.” Streamlining the rule set is the second step of a process that began with migrating more than 10,000 rules—many of them obsolete—from their old infrastructure using tools from Fortinet.

The university also purchased a FortiCare First program (Advanced Services technical support contract), which assigns a dedicated technical account manager (TAM) who works alongside the university’s team to prioritize and coordinate support services. The team also invested heavily in training from the Fortinet Network Security Academy. “Everyone on the architecture, network, and security teams will receive full, classroom-based training on managing the solution,” Boryk comments.

## Achieving Impressive Results

In the short time since the initial deployment, the university is already seeing tangible results and can project further future gains based on preliminary results. The larger network upgrade project has stabilized the network and helped Boryk’s team reclaim a lot of time. “Just keeping the network stable required 10 to 20 hours per month for each of our four team members—or a total of 40 to 80 hours monthly,” he says. “On top of that, the events when our network required all hands on deck to return it to a stable state could sometimes require a full day of work for each of us. Getting that time back means that we can move on to strategic projects.”

Enabling cloud backup also promises significant savings for the university, with a significant number of backups slated to move to Azure by December 2019. “Backup administration time has already been sharply reduced, and the cost of backing up to the cloud is much lower than with our SAN,” Hawkins reports. “We expect a 15% annual saving in storage costs once we’re fully up and running with cloud backups.”

Leveraging built-in features such as the intrusion prevention system (IPS) in the FortiGate NGFW will also result in reduced licensing costs. “We currently have a separate point solution for IPS,” Boryk explains. “Once we turn on the FortiGate IPS, we will save significantly in licensing and management overhead per year in costs for that solution.”

Centralizing security operations on the FortiGate NGFWs is resulting in operational efficiencies as well. “We recently had to set up VPNs for private addressing from the university to one of our cloud providers,” Hawkins states. “That project required 28 staff hours but would have taken just a few minutes if our FortiGate NGFWs had been set up.” Another example of efficiency savings: one twice-a-week report produced by the network team now takes just a few minutes with FortiManager, compared with two hours previously. This saves 180 staff hours per year.

Better coordination among the architecture, network, and security teams is another benefit of the FortiGate NGFW and the Fortinet Security Fabric. “All our teams now use FortiManager and FortiAnalyzer to view status and run reports,” Hawkins relates. “It really contributes to a more coordinated and less siloed way of doing our jobs. And this benefit will grow as new elements are added to the Fortinet Security Fabric.”

## Completing the Transformation

The University of South Carolina team expects to have the new network backbone and the entire Fortinet Security Fabric fully deployed by summer of 2020. “It was a massive undertaking, but the benefits we are already seeing make the effort well worth it,” Boryk contends. “Our relationship with Fortinet has been more than positive. Everyone has been really supportive and has gone out of their way to ensure our success.”



[www.fortinet.com](http://www.fortinet.com)

## CASE STUDY

# Illinois Century Network Partners with Fortinet to Protect K-12 Broadband Connectivity

High-speed internet is absolutely vital to modern K-12 education. That may seem obvious, but a lack of broadband connectivity can have a severe impact on both student learning and school operations. To support equity in education statewide, the Illinois State Board of Education and Illinois Board of Higher Education teamed up in 2000. They developed the member-driven Illinois Century Network (ICN) to provide internet connectivity to every public K-12 school in the state, free of charge.

"It is pretty clear that students who do not have access to high-speed internet cannot participate in the modern world of rich-media, interactive content, and live interactive video sessions or streaming video," says Robin Woodsome, manager, ICN Field Operations. "For schools across the country, the new teaching models are driving a need for more bandwidth."

Administrative and other functions also suffer without high-speed connectivity. "Universities require K-12 schools to have high-speed bandwidth in order to participate in their research projects," adds Frank Walters, network architect for ICN. "Lack of broadband availability reduces students' opportunities and preparedness for university or college."

That is why, when Governor Pritzker launched Connect Illinois to expand the state's broadband capabilities in 2019, he dedicated substantial resources to upgrading the ICN network. "Governor Pritzker sees broadband connectivity as a utility, similar to electricity and water, streets and roads," explains Dale Walters, chief of network operations for the state of Illinois. "Through Connect Illinois, he provided \$20 million to the Illinois Century Network, to bring broadband internet to our public K-12 education institutions."

## Schools' WAN Service Must Be Secure

The ICN's infrastructure was dated, so the project focused on "upgrading to new optical networking hardware that could support speeds up to 100 Gbps," Dale Walters says. "Our goal was to build a broadband infrastructure to support the needs of K-12 public schools in every corner of the state—not only their current needs, but their needs for the next several years as well."

As the ICN team designed this new broadband network, security was a key concern. "Many school districts struggle with security," Frank Walters says. "Doing it properly is difficult and expensive, and experts are hard to find in some regions of the state. So, when we were strategizing how to get the schools the connectivity they need, we knew that we needed to provide a system that would be as secure as we could make it."



*"Our goal was to build a broadband infrastructure to support the needs of K-12 public schools in every corner of the state—not only their current needs, but their needs for the next several years as well."*

– Dale Walters, Chief of Network Operations, Illinois Century Network

## Details

**Customer:** Illinois Century Network

**Industry:** Government

**Location:** Springfield, Illinois

## Business Impact

- Secures broadband connectivity for schools statewide
- Adds no measurable latency to schools' internet traffic
- Minimizes total cost of ownership (TCO) for high-performance network security
- Minimizes staff time required for firewall management



They decided to design a wide-area network (WAN) that would be a safe place for schools to communicate with one another, he adds. “And then we would have a single presentation of those K-12 schools to the internet, through the firewalls that we provide. This became top-of-mind when the COVID-19 pandemic hit, because we saw a significant uptick in both ransomware and DDoS [distributed denial-of-service] attacks on our schools.”

Frank Walters emphasizes that the ICN's intention was not to provide all the security that a school or district would need. “We are not dipping into their local IT environments and trying to take over,” he says. “We want to assist schools with the needs that they identify, and whether they take advantage of our services is totally optional. Some schools opt to maintain the security solutions they already have in place. But we knew that since we would be providing those last-mile circuits for them, we also needed to provide an outer layer of security.”

### Protecting Schools at the WAN Edge

The Illinois Century Network sought a firewall solution for the WAN edge. They had previously been standardized with a different solution, but a cost-benefit analysis brought Fortinet to the forefront. “It is always risky to step away from what you know,” says Frank Walters. “But the state encouraged us to review the total cost of ownership [TCO] of each choice—not just the up-front purchase cost, but the cost of maintaining it, the cost of training, the whole ball of wax. When we started looking at the numbers, Fortinet stood out.”

The state imposed a tight deadline to complete the ICN broadband infrastructure. Initially, all participating schools’ internet traffic passed through the Chicago data center. The team rolled out a pair of FortiGate next-generation firewalls (NGFWs) to secure that traffic.

“We had to move quickly to meet the state deadline, so we implemented the firewalls in standalone mode,” says Andre Bouravnev, network supervisor for ICN. “That is changing. We have worked closely with Fortinet engineers to determine the best configuration of the firewalls. Since the deployment, we switched to a standby-active configuration for failover. The next step is to bring a second pair of FortiGate firewalls online in Springfield.”

The team is considering transitioning both NGFW pairs to active-active status, with load balancing between the two. Bouravnev reports that they will soon begin testing.

### Fortinet Generates Substantial TCO Savings

The NGFWs are already exceeding expectations. “We are now providing schools with an environment that is exactly what we said it would be,” says Frank Walters. “The security piece was crucial, and Fortinet was very helpful throughout the process in making sure everything was configured right for the schools.”

Currently, over 200 districts representing about 1,660 schools utilize the ICN, and more than 100 of those are taking advantage of the new broadband firewall services. Others have their own firewalls at the headend where their local-area network (LAN) connects to the ICN. Whether to take this layered security approach is up to district administrators.

“This is extremely beneficial to schools in underserved parts of the state, where broadband is not readily available,” Woodsome says. “Because we provide secure broadband service at no cost, we are helping those districts catch up so that they can deploy the same types of learning programs as schools in areas of the state where access is more readily available.”

### Solutions

- FortiGate
- FortiManager
- FortiAnalyzer

*“It is always risky to step away from what you know, but the state encouraged us to review the total cost of ownership [TCO] of each choice. When we started looking at the numbers, Fortinet stood out.”*

– Frank Walters, Network Architect,  
Illinois Century Network

The FortiGate NGFWs support those historically underserved schools by protecting traffic without introducing any latency. “We have done really thorough performance testing in the past few months, of different components of our network,” Bouravnev reports. “We have isolated the FortiGates and have not found any delay to customer traffic going through the firewall. Everything looks really good.”

For the ICN, the ability to minimize TCO while securing schools’ high-performance connectivity was key. Bouravnev estimates that with the Fortinet solution, ICN will save millions of dollars in capital and operating expenses over the next five years.

Network administrators use FortiManager to streamline and centralize configuration of the FortiGate NGFWs. They also use FortiAnalyzer for reporting and analysis of security events on the network. “We are very new to Fortinet, so we are still learning to get the most out of the tools,” Bouravnev says. “So far, though, we have been pleased, although the FortiGate is a fairly complex and sophisticated firewall, the GUI [graphical user interface] navigation of the firewall and the management tools is not complex. Unlike some security tools we have worked with previously, the Fortinet interface makes everything easy to find. The documentation and support are good as well.”

Ultimately, Bouravnev says, the ICN team is pleased with Fortinet. “We did not need a firewall that was overly complex, and we wanted it to be easy to manage and not require a lot of staff time. At the same time, we needed a network that could perform past 100 gigs. The Fortinet solutions match our needs well.”



[www.fortinet.com](http://www.fortinet.com)

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

## FortiGate® Network Security Platform - \*Top Selling Models Matrix

	FG/FWF-40F	FG/FWF-60F	FG/FWF-80F	FG-100F
Firewall Throughput (1518/512/64 byte UDP)	5 / 5 / 5 Gbps	10/10/6 Gbps	10 / 10 / 7 Gbps	20 / 18 / 10 Gbps
IPsec VPN Throughput (512 byte) <sup>1</sup>	4.4 Gbps	6.5 Gbps	6.5 Gbps	11.5 Gbps
IPS Throughput (Enterprise Mix) <sup>2</sup>	1 Gbps	1.4 Gbps	1.4 Gbps	2.6 Gbps
NGFW Throughput (Enterprise Mix) <sup>2,4</sup>	800 Mbps	1 Gbps	1 Gbps	1.6 Gbps
Threat Protection Throughput (Ent. Mix) <sup>2,5</sup>	600 Mbps	700 Mbps	900 Mbps <sup>6</sup>	1 Gbps
Firewall Latency	2.97 µs	3.3 µs	3.23 µs	4.97µs
Concurrent Sessions	700,000	700,000	1.5 Million	1.5 Million
New Sessions/Sec	35,000	35,000	45,000	56,000
Firewall Policies	5,000	5,000	5,000	10,000
Max G/W to G/W IPSEC Tunnels	200	200	200	2,000
Max Client to G/W IPSEC Tunnels	250	500	2,500	16,000
SSL VPN Throughput	490 Mbps	900 Mbps	950 Mbps	1 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	200	200	200	500
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	310 Mbps	630 Mbps	715 Mbps	1 Gbps
Application Control Throughput (HTTP 64K) <sup>2</sup>	990 Mbps	1.8 Gbps	1.8 Gbps	2.2 Gbps
Max FortiAPs (Total / Tunnel)	16 / 8	64 / 32	96 / 48	128 / 64
Max FortiSwitches	8	16	16	32
Max FortiTokens	500	500	500	5,000
Virtual Domains ( Default/Max)	10 / 10	10 / 10	10 / 10	10 / 10
Interfaces	5x GE RJ45	10x GE RJ45	8x GE RJ45, 2x Shared Port Pairs	2x 10 GE SFP+, 18x GE RJ45, 4x Shared Port Pairs, 8x GE SFP
Local Storage	—	128 GB (61F)	128 GB (81F)	480 GB (101F)
Power Supplies	Single AC PS	Single AC PS	Single AC PS, dual inputs	Dual AC PS
Form Factor	Desktop	Desktop	Desktop	1 RU
Variants	WiFi, 3G4G	WiFi, Storage	WiFi, 3G4G, DSL, Bypass, Storage	—
	FG-200E	FG-200F	FG-400E	FG-600E
Firewall Throughput (1518/512/64 byte UDP)	20 / 20 / 9 Gbps	27 / 27 / 11 Gbps	32 / 32 / 24 Gbps	36 / 36 / 27 Gbps
IPsec VPN Throughput (512 byte) <sup>1</sup>	7.2 Gbps	13 Gbps	20 Gbps	20 Gbps
IPS Throughput (Enterprise Mix) <sup>2</sup>	2.2 Gbps	5 Gbps	7.8 Gbps	10 Gbps
NGFW Throughput (Enterprise Mix) <sup>2,4</sup>	1.8 Gbps	3.5 Gbps	6 Gbps	9.5 Gbps
Threat Protection Throughput (Ent. Mix) <sup>2,5</sup>	1.2 Gbps	3 Gbps	5 Gbps	7 Gbps
Firewall Latency	3 µs	4.78 µs	2.14 µs	1.54 µs
Concurrent Sessions	2 Million	3 Million	4 Million	8 Million
New Sessions/Sec	135,000	280,000	450,000	450,000
Firewall Policies	10,000	10,000	10,000	10,000
Max G/W to G/W IPSEC Tunnels	2,000	2,000	2,000	2,000
Max Client to G/W IPSEC Tunnels	10,000	16,000	50,000	50,000
SSL VPN Throughput	900 Mbps	2 Gbps	4.5 Gbps	7 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	500	500	5,000	10,000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	820 Mbps	4 Gbps	4.8 Gbps	8 Gbps
Application Control Throughput (HTTP 64K) <sup>2</sup>	3.5 Gbps	13 Gbps	12 Gbps	15 Gbps
Max FortiAPs (Total / Tunnel)	256 / 128	256 / 128	512 / 256	1,024 / 512
Max FortiSwitches	64	64	72	96
Max FortiTokens	5,000	5,000	5,000	5,000
Virtual Domains ( Default/Max)	10 / 10	10 / 10	10 / 10	10 / 10
Interfaces	18x GE RJ45, 4x GE SFP	4x 10 GE SFP+, 18x GE RJ45, 8x GE SFP	18x GE RJ45, 16x GE SFP	2x 10 GE SFP+, 10x GE RJ45, 8x GE SFP
Local Storage	480 GB (201E)	480 GB (201F)	480 GB (401E)	480 GB (601E)
Power Supplies	Single AC PS	Dual AC PS	Single AC PS, opt. Dual PS	Single AC PS, opt. Dual PS
Form Factor	1 RU	1 RU	1 RU	1 RU
Variants	—	—	—	—

# FortiGate® Network Security Platform - \*Top Selling Models Matrix

	FG-1100E	FG-1800F	FG-2200E	FG-2600F
Firewall Throughput (1518/512/64 byte UDP)	80 / 80 / 45 Gbps	198 / 197 / 140 Gbps	158 / 155 / 100 Gbps	198 / 196 / 120 Gbps
IPsec VPN Throughput (512 byte) <sup>1</sup>	48 Gbps	55 Gbps	98 Gbps	55 Gbps
IPS Throughput (Enterprise Mix) <sup>2</sup>	12.5 Gbps	17 Gbps	21 Gbps	24 Gbps
NGFW Throughput (Enterprise Mix) <sup>2,4</sup>	9.8 Gbps	11 Gbps	13.5 Gbps	19 Gbps
Threat Protection Throughput (Ent. Mix) <sup>2,5</sup>	7.1 Gbps	9.1 Gbps	11 Gbps	17 Gbps
Firewall Latency	2.76 µs	3.22 µs	3.09 µs	3.41 µs
Concurrent Sessions	8 Million	12 Million / 40 Million <sup>7</sup>	24 Million	24 Million / 40 Million <sup>7</sup>
New Sessions/Sec	500,000	750,000 / 2 Million <sup>7</sup>	500,000	1 Million / 2 Million <sup>7</sup>
Firewall Policies	100,000	100,000	100,000	100,000
Max G/W to G/W IPSEC Tunnels	20,000	20,000	20,000	20,000
Max Client to G/W IPSEC Tunnels	100,000	100,000	100,000	100,000
SSL VPN Throughput	8.4 Gbps	11 Gbps	10 Gbps	16 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	10,000	10,000	30,000	30,000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	10 Gbps	12 Gbps	17 Gbps	20 Gbps
Application Control Throughput (HTTP 64K) <sup>2</sup>	26 Gbps	34 Gbps	52 Gbps	64 Gbps
Max FortiAPs (Total, Tunnel)	4,096 / 2,048	4,096 / 2,048	4,096 / 2,048	4,096 / 2,048
Max FortiSwitches	196	196	196	196
Max FortiTokens	20,000	20,000	20,000	20,000
Virtual Domains ( Default/Max)	10 / 250	10 / 250	10 / 500	10 / 500
Interfaces	2× 40GE QSFP+, 4× 25GE SFP28, 4× 10GE SFP+, 8× GE SFP, 18× GE RJ45	4× 40 GE QSFP+, 12× 25 GE SFP28, 2×10 GE SFP+, 8× GE SFP, 18× GE RJ45	4× 40GE QSFP+, 20× 25GE SFP28, 14× GE RJ45	4× 100GE QSFP28/40GE QSFP+, 16× 25GE SFP28, 16× 10GE RJ45, 2× 10GE SFP+, 2× GE RJ45
Local Storage	960 GB (1101E)	2 TB (1801F)	2 TB (2201E)	2 TB (2601F)
Power Supplies	Dual PS	Dual PS	Dual PS	Dual PS
Form Factor	2 RU	2 RU	2 RU	2 RU
Variants	DC	DC	—	DC
	FG-3300E	FG-3400E	FG-3500F	FG-3600E
Firewall Throughput (1518/512/64 byte UDP)	160 / 158 / 100 Gbps	240 / 238 / 150 Gbps	595 / 590 / 420 Gbps	240 / 240 / 150 Gbps
IPsec VPN Throughput (512 byte) <sup>1</sup>	98 Gbps	140 Gbps	165 Gbps	140 Gbps
IPS Throughput (Enterprise Mix) <sup>2</sup>	27 Gbps	44 Gbps	72 Gbps	55 Gbps
NGFW Throughput (Enterprise Mix) <sup>2,4</sup>	23 Gbps	34 Gbps	65 Gbps	40 Gbps
Threat Protection Throughput (Ent. Mix) <sup>2,5</sup>	17 Gbps	25 Gbps	63 Gbps	30 Gbps
Firewall Latency	3.17 µs	3.33 µs	2.98 µs	3.27µs
Concurrent Sessions	50 Million	50 Million	140 Million / 348 Million <sup>7</sup>	50 Million
New Sessions/Sec	700,000	850,000	1 Million / 5 Million <sup>7</sup>	950,000
Firewall Policies	200,000	200,000	200,000	200,000
Max G/W to G/W IPSEC Tunnels	40,000	40,000	40,000	40,000
Max Client to G/W IPSEC Tunnels	200,000	200,000	200,000	200,000
SSL VPN Throughput	10 Gbps	11 Gbps	16 Gbps	12 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	30,000	30,000	30,000	30,000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	21 Gbps	30 Gbps	63 Gbps	34 Gbps
Application Control Throughput (HTTP 64K) <sup>2</sup>	70 Gbps	86 Gbps	135 Gbps	95 Gbps
Max FortiAPs (Total, Tunnel)	4,096 / 2,048	4,096 / 2,048	4,096 / 2,048	4,096 / 2,048
Max FortiSwitches	300	300	300	300
Max FortiTokens	20,000	20,000	20,000	20,000
Virtual Domains ( Default/Max)	10 / 500	10 / 500	10 / 500	10 / 500
Interfaces	4× 40GE QSFP+, 16× 25GE SFP28, 4× 10GE RJ45, 14× GE RJ45	4× 100GE QSFP28/40GE QSFP+, 24× 25GE SFP28, 2× GE RJ45	6× 100GE QSFP28/40GE QSFP+, 32× 25GE SFP28, 2× GE RJ45	6× 100GE QSFP28/40GE QSFP+, 32× 25GE SFP28, 2× GE RJ45
Local Storage	2 TB (3301E)	4 TB (3401E)	4 TB (3501F)	4 TB (3601E)
Power Supplies	Dual PS	Dual PS	Dual PS	Dual PS
Form Factor	2 RU	2 RU	2 RU	2 RU
Variants	—	DC	—	DC

\* Featured Top selling models, for complete FortiGate offerings please visit [www.fortinet.com](http://www.fortinet.com). FortiGate virtual appliances are also available. All performance values are “up to” and vary depending on system configuration.



# FortiGate® Network Security Platform - \*Top Selling Models Matrix

	FG-3960E	FG-3980E	FG-4200F	FG-4400F
Firewall Throughput (1518/512/64 byte UDP)	620 / 610 / 370 Gbps	1.05 Tbps / 1.05 Tbps / 680 Gbps	800 / 788 / 400 Gbps	1.15 / 1.14 / 0.50 Tbps
IPsec VPN Throughput (512 byte) <sup>1</sup>	280 Gbps	400 Gbps	210 Gbps	310 Gbps
IPS Throughput (Enterprise Mix) <sup>2</sup>	30 Gbps	32 Gbps	52 Gbps	94 Gbps
NGFW Throughput (Enterprise Mix) <sup>2,4</sup>	22 Gbps	28 Gbps	47 Gbps	82 Gbps
Threat Protection Throughput (Ent. Mix) <sup>2,5</sup>	13.5 Gbps	20 Gbps	45 Gbps <sup>6</sup>	75 Gbps <sup>6</sup>
Firewall Latency	3 µs	3 µs	3.02 µs	2.98 µs
Concurrent Sessions	160 Million	160 Million	210 Million / 450 Million <sup>7</sup>	210 Million / 700 Million <sup>7</sup>
New Sessions/Sec	720,000	800,000	1 Million / 7 Million <sup>7</sup>	1 Million / 10 Million <sup>7</sup>
Firewall Policies	200,000	200,000	200,000	200,000
Max G/W to G/W IPSEC Tunnels	40,000	40,000	40,000	40,000
Max Client to G/W IPSEC Tunnels	200,000	200,000	200,000	200,000
SSL VPN Throughput	9 Gbps	9.5 Gbps	16 Gbps	16 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	30,000	30,000	30,000	30,000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	23 Gbps	26 Gbps	50 Gbps	86 Gbps
Application Control Throughput (HTTP 64K) <sup>2</sup>	40 Gbps	55 Gbps	135 Gbps	140 Gbps
Max FortiAPs (Total, Tunnel)	8,192 / 4,096	8,192 / 4,096	8,192 / 4,096	8,192 / 4,096
Max FortiSwitches	300	300	300	300
Max FortiTokens	20,000	20,000	20,000	20,000
Virtual Domains ( Default/Max)	10 / 500	10 / 500	10 / 500	10 / 500
Interfaces	6× 100GE QSFP28/40GE QSFP+, 16× 10GE SFP+, 2x GE RJ45	10× 100GE QSFP28/40GE QSFP+, 16× 10GE SFP+, 2x GE RJ45	8× 100GE QSFP28/40GE QSFP+, 18× 25GE SFP28, 2x GE RJ45	12× 100GE QSFP28/40GE QSFP+, 20× 25GE SFP28, 2x GE RJ45
Local Storage	—	—	4 TB (4201F)	4 TB (4401F)
Power Supplies	3 PS	3 PS	Dual PS	4 PS
Form Factor	5 RU	5 RU	3 RU	4 RU
Variants	DC	DC	DC	DC
	FG-6300F	FG-6500F	FG-7060E	FG-7121F
Firewall Throughput (1518/512/64 byte UDP)	239 / 238 / 135 Gbps	239 / 238 / 135 Gbps	630 / 630 / 340 Gbps	1.89 / 1.88 / 1.129 Tbps
IPsec VPN Throughput (512 byte) <sup>1</sup>	96 Gbps	160 Gbps	100 Gbps	630 Gbps
IPS Throughput (Enterprise Mix) <sup>2</sup>	110 Gbps	170 Gbps	200 Gbps	675 Gbps
NGFW Throughput (Enterprise Mix) <sup>2,4</sup>	90 Gbps	150 Gbps	120 Gbps	550 Gbps
Threat Protection Throughput (Ent. Mix) <sup>2,5</sup>	60 Gbps	100 Gbps	96 Gbps	520 Gbps
Firewall Latency	5 µs	5 µs	7 µs	7.5 µs
Concurrent Sessions	120 Million	200 Million	320 Million	1 Billion
New Sessions/Sec	2 Million	3 Million	1.8 Million	9 Million
Firewall Policies	200,000	200,000	200,000	200,000
Max G/W to G/W IPSEC Tunnels	16,000	16,000	16,000	40,000
Max Client to G/W IPSEC Tunnels	90,000	90,000	64,000	260,000
SSL VPN Throughput	9 Gbps	9 Gbps	15 Gbps	13.7 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	30,000	30,000	48,000	30,000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	66 Gbps	110 Gbps	79.9 Gbps	540 Gbps
Application Control Throughput (HTTP 64K) <sup>2</sup>	150 Gbps	220 Gbps	160 Gbps	1.5 Tbps
Max FortiAPs (Total, Tunnel)	—	—	—	—
Max FortiSwitches	256	256	256	300
Max FortiTokens	20,000	20,000	20,000	20,000
Virtual Domains ( Default/Max)	10 / 500	10 / 500	10 / 500	10 / 500
Interfaces	4× 100GE QSFP28/40GE QSFP+, 24× 25GE SFP28, 3× 10GE SFP+, 2x GE RJ45	4× 100GE QSFP28/40GE QSFP+, 24× 25GE SFP28, 3× 10GE SFP+, 2x GE RJ45	Varied	Varied
Local Storage	2 TB NVMe (6301F)	2 TB NVMe (6501F)	—	4× 4 TB SSD
Power Supplies	3 PS	3 PS	4+2 PS	8 PS
Form Factor	3 RU	3 RU	8 RU	16 RU
Variants	DC	DC	DC	—

1. IPsec VPN performance test uses AES256-SHA256.

2. IPS, Application Control, NGFW and Threat Protection are measured with Logging enabled.

3. SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

4. NGFW performance is measured with Firewall, IPS and Application Control enabled, Enterprise Mix traffic.

5. Threat Protection performance is measured with Firewall, IPS, Application Control, (6.URL Filtering) and Malware Protection enabled, Enterprise Mix traffic.

7. Requires Hyperscale license



## FortiManager™ Centralized Management Platform

	FMG-200G	FMG-300F	FMG-400G	FMG-1000F	FMG-2000E	FMG-3000G	FMG-3700G	FMG-VM-BASE to FMG-VM-UL-UG
Devices/VDOMs (Maximum)	30	100	150	1,000	1,200	4,000+	10,000+	10 to Unlimited
Sustained Log Rates	50	50	50	50	50	150	150	Hardware dependent
GB/Day	2	2	2	2	2	10	10	1-50
Total Interfaces	4x GE RJ45	4x GE RJ45, 2x GE SFP	4x GE RJ45, 2x GE SFP	2x GE RJ45, 2x 10GE SFP+	4x GE RJ45, 2x 10GE SFP+	2x GE RJ45, 2x 25GE SFP28	2x 10GE RJ45, 2x 25GE SFP28	1 / 4 (vNIC Min / Max)
Storage Capacity	2x 4 TB	4x 4 TB	8x 4 TB	8x 4 TB	12x 3 TB	16x 4 TB	60x 4TB HDD + 6x 3.2TB NVMe SSD	80 GB / 16 TB (Min / Max)

## FortiAnalyzer™ Centralized Logging & Reporting Solution

	FAZ-150G	FAZ-300G	FAZ-800G	FAZ-1000F	FAZ-3000G	FAZ-3500G	FAZ-3700G	FAZ-VM-BASE to FAZ-VM-GB2000
GB Logs/Day	25	100	200	660	3,000	5,000	8,300	1 to +2,000
Analytic Sustained Rate (logs/sec)	500	2,000	4,000	20,000	42,000	60,000	100,000	—
Collector Sustained Rate (logs/sec)	750	3,000	6,000	30,000	60,000	90,000	150,000	—
Total Interfaces	2x GE RJ45	4x GE RJ45	4x GE RJ45, 2x GE SFP	2x GE RJ45, 2x 10GE SFP+	2x GE RJ45, 2x 25GE SFP28	2x GE RJ45, 2x 25GE SFP28	2x 10GE RJ45, 2x 25GE SFP28	1 / 4 (vNIC Min / Max)
Storage Capacity	2x 2 TB	2x 4 TB	4x 4 TB	8x 4 TB	16x 4 TB	24x 4 TB	60x 4TB HDD + 6x 3.2TB NVMe SSD	500 GB to +100 TB

## FortiSIEM™ Unified Event Correlation and Risk Management Solution

	FSM-500F "COLLECTOR"	FSM-2000F "SUPERVISOR"	FSM-3500G "SUPERVISOR"
All-in-One License Capacity	N/A	Up to 500	Up to 2,000
EPS Capacity (all features enabled)	5,000	Up to 15,000	Up to 40,000

## FortiAuthenticator™ User Identity Management Server

	FAC-300F	FAC-800F	FAC-3000F	FAC-VM BASE to FAC-VM-10000-UG
Max Local + Remote Users/ User Group	1,500 / 150	8,000 / 800	40,000 / 240,000	100 / 10 to +10,000 / 1,000
Max NAS Devices	500	2,666	80,000	33 to +33,333
Max FortiTokens	3,000	16,000	480,000	200 to +20,000
Interfaces	4x GE RJ45	4x GE RJ45, 2x SFP	4x GE RJ45, 2x SFP	1 - 4 vNICs
Storage Capacity	2	2x 2 TB	2x 2 TB	60 GB to 16 TB

## FortiAP™ Wireless Access Point

	FortiAP Series	FortiAP U-Series
Management	FortiGate-Managed, Cloud-Managed	FortiGate-Managed, Cloud-Managed, Controller-Managed
Security	Via FortiGate	Via FortiGate

\* Frequency selection and power may be restricted to abide by regional regulatory compliance laws.  
For Complete selection of FortiAPs, including remote and outdoor devices, please refer to Fortinet Wireless Solution Matrix

## FortiSwitch™ Secured Access Switch

	100 Series	200 Series	400 Series	500 Series	1000 Series	3000 Series
Main Port Speed	1 Gbps	1 Gbps	1 Gbps	1 Gbps	10/40 Gbps	40/100 Gbps
Main Port Count Options	8, 24, 48	24, 48	24, 48	24, 48	24, 48	32
Uplink Port Speed	1 or 10 Gbps	1 Gbps	10 Gbps	10 Gbps	40 or 100 Gbps	n/a
Redundant Power Supplies	—	Some Models	Some Models	Optional RSU	•	•
PoE Options	•	•	•	•	—	—

For Complete selection of FortiSwitches, please refer to <http://www.fortinet.com/products/fortiswitch>



## FortiNAC™ Network Access Control Solution

	FNC-CA-500C	FNC-CA-600C	FNC-CA-700C	FNC-M-550C
Type	Mid-range Control and Application Server	High Performance Control and Application Server	Ultra High Performance Control and Application Server	Centralized Management Appliance
Target Environment	Small Environments	Medium Environments	Large Environments with few Persistent Agents	Multi-site environments with multiple appliances
Capacity	Manages up to 1,000 ports in the network*	Manages up to 7,500 ports in the network*	Manages up to 15,000 ports in the network*	Unlimited

Virtual appliances are also available, please refer to [www.fortinet.com](http://www.fortinet.com) for more information

## FortiSandbox™ Advanced Threat Prevention System

	FSA-500F	FSA-1000F/-DC	FSA-2000E	FSA-3000F	FSA-VM
Sandbox Pre-Filter Throughput (Files/Hour) <sup>1</sup>	4,500	7,500	12,000	18,000	Hardware dependent
VM Sandboxing Throughput (Files/Hour) <sup>2</sup>	120	280	480	1,340	Hardware dependent
Real-world Effective Throughput (Files/Hour)	600 <sup>2</sup>	1,400 <sup>2</sup>	2,400 <sup>2</sup>	6,720 <sup>2</sup>	Hardware dependent
Number of VMs	2 +4 optional	2 +10 optional	4 +20 optional	8 + 64 optional	4, up to 54

<sup>1</sup> FortiSandbox pre-filtering is powered by FortiGuard Intelligence.  
<sup>2</sup> Measured based on real-world data when both prefilter and dynamic analysis are working consecutively.  
 \* Based on the assumption that 1 blade will be used as master in HA-cluster mode.

## FortiClient™ Advanced Endpoint Security

	Windows	MAC OS X	Linux	Android	iOS	Chromebook
Zero Trust Security (ZTNA) Options	✓	✓	✓	—	—	Partial
Next Generation Endpoint Security (EPP / APT) Options	✓	✓	✓	—	—	—
Cloud Based Endpoint Security (SASE) Options	✓	✓	✓	—	—	—
Security Fabric Components	✓	✓	Partial	Partial	Partial	Partial
VPN Client	✓	✓	SSL VPN only	✓	SSL VPN only	—

## FortiMail™ Messaging Security Server

	FML-200F	FML-400F	FML-900F	FML-2000F	FML-3000F	FML-3200E
Email Routing* (Msg/Hr)	50,000	250,000	800,000	1.6 Mil	3.5 Mil	3.4 Mil
Performance Enterprise ATP* (Msg/Hr)	30,000	150,000	400,000	800,000	2.1 Mil	2.0 Mil
Email Domains	20	100	800	1,000	2,000	2,000
Server Mode Mailboxes	150	400	1,500	2,000	3,000	3,000
Storage Capacity	1× 1 TB	2× 1 TB	2× 2 TB (8 TB Max)	2× 2 TB (12 TB Max)	2× 2 TB (20 TB Max)	2× 2 TB (20 TB Max)

\* Measured based on 100KB message size, no queuing.  
 Virtual appliances are also available, please refer to [www.fortinet.com](http://www.fortinet.com) for more information

## FortiWeb™ Web Application Firewall

	FWB-100E	FWB-400E	FWB-600E	FWB-1000E	FWB-2000F	FWB-3000F	FWB-4000F
Throughput (HTTP)	50 Mbps	250 Mbps	750 Mbps	1.3 Gbps	5 Gbps	10 Gbps	70 Gbps
Total Interfaces	4x GE RJ45	4x GE RJ45 4x GE SFP	2 (+2 bypass) x GE RJ45, 4x GE SFP	2 (+4 bypass) GE RJ45, 4x SFP GE, 2x 10GE SFP+	4x 10GE SFP+, 4x GE RJ45 Bypass, 4x GE SFP	10x 10GE SFP+ (incl. 2 Bypass), 8x GE RJ45 Bypass	2x 40GE QSFP Bypass, 10x 10GE SFP+ (incl. 2 Bypass), 8x GE RJ45 Bypass

Virtual appliances are also available, please refer to [www.fortinet.com](http://www.fortinet.com) for more information



# Virtual Appliance Support Matrix

	VMWare vSphere	Citrix Xen Server	Xen	KVM	Microsoft Hyper-V	Nutanix AHV	Amazon AWS	Microsoft Azure	Oracle OPC/OCI	Google GCP	Alibaba Aliyun
FortiGate-VM *	•	•	•	•	•	•	• / #	• / #	• /#	• /#	• / #
FortiManager-VM	•	•	•	•	•	•	• / #	•	•	•	•
FortiAnalyzer-VM	•	•	•	•	•	•	• / #	•	•	•	•
FortiWeb-VM	•	•	•	•	•	•	• / #	• / #	•	•	•
FortiWeb Manager- VM	•						•				
FortiMail-VM	•	•		•	•	•	• / #	• / #		•	
FortiAuthenticator- VM	•		•	•	•		•	•	•		
FortiADC-VM	•	•	•	•	•	•	• / #	• / #	• / #	• / #	
FortiVoice-VM	•	•		•	•		•	•			
FortiRecorder-VM	•	•		•	•		#				
FortiSandbox-VM	•			•	•	•	• / #	#			
FortiSIEM-VM	•			•	•	•	•	•			•
FortiProxy-VM	•			•							

\*Available as FortiGate-VMX solution for VMware NSX environment, AzureStack and RackSpace (PAYG)  
# on-demand

## List of Other Products

**FortiADC** Application Delivery Controller  
**FortiAI** Virtual Security Analyst™  
**FortiCASB** Cloud Access Security Broker  
**FortiCarrier** CGN Gateway  
**FortiCWP** Cloud Security Analytics  
**FortiDDoS** DDoS Mitigator  
**FortiDeceptor** Deception-based Solution  
**FortiEDR** EDR Solution

**FortiExtender** 3G/4G WAN Extender  
**FortiHypervisor** Hybrid Virtual Appliance  
**FortiInsight** UEBA Solution  
**FortiIsolator** Browser Isolation Platform  
**FortiMonitor** NPMD, DEM and IM Systems  
**FortiProxy** Secure Web Gateway  
**FortiRecorder** Network Video Security  
**FortiSIEM** SIEM with UEBA Solution

**FortiSOAR** SOAR Solution  
**FortiTester** Network Tester  
**FortiToken** 2 Factor Authentication Token  
**FortiVoice** Secure VoIP Solution  
**FortiWLC** Wireless Controller  
**FortiWLM** Wireless Manager  
**FortiXDR** Extended Detection and Response



www.fortinet.com

Copyright © 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.



# FortiCare Services

## Technical Support and Advanced Services



### Hit the ground running with your new capabilities

Fast-track return on investment with streamlined migration and deployment



### Get expert help when you need it

Accelerate incident resolution and maximize efficacy with 24×7 assistance from technical experts



### Enhance your security with tailored guidance

Increase productivity and avoid incidents with operational reviews, account planning, and upgrade assistance

## Confidence in Your Investment

Businesses are making huge investments in security and Fortinet Fabric technologies to provide essential services critical to securing their most valuable assets. Organizations often lack the in-house expertise or resources for initial deployment, product support, and ongoing operations. At Fortinet, we understand these challenges and provide FortiCare Services to thousands of organizations every year to address them.

We want organizations to feel confident that they are maximizing the value of their investments quickly, and realizing efficiency and efficacy gains over time. Whether migrating to a Fortinet next-generation firewall (NGFW), implementing software-defined wide-area networking (SD-WAN) to protect your branch locations, or automating security operations functions, we will work with you to match the proper services with your unique business needs. We are dedicated to your success and provide the expertise you need, when you need it.

## FortiCare Services

FortiCare Services provides customers access to over 1,000 experts to ensure efficient and effective deployment, operations, and maintenance of their Fortinet capabilities. Accelerated implementation and configuration optimization are provided through Professional Services engagements and dedicated resources. Global technical support is offered 24×7 with flexible add-ons, including enhanced service level agreements (SLAs) and premium hardware replacement through 200+ in-country depots. For advanced needs of enterprises and service providers, Fortinet offers advanced services that provide high-touch account management and business guidance through designated resources. Additionally, Enterprise Support Agreements (ESAs) are available to simplify consumption of the services.



## Expertise at Your Service

- 24×7 Global Support
- 1,000+ NSE and Industry Certified Global Resources
- 3 Regional Centers of Expertise
- 19 Support Centers
- 40 Regional Depots
- 200+ In-country Depots
- 4-hour Expedited Hardware Replacement Availability

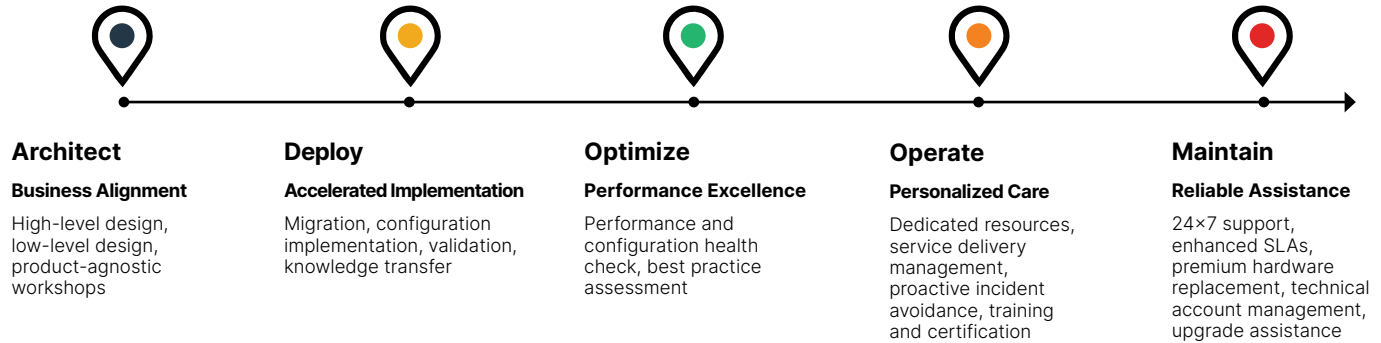
## FortiCare Worldwide

### 24×7 Support

[support.fortinet.com](https://support.fortinet.com)

## The Journey

Adopting new technologies is not a project with a start and a finish. Instead, it is a journey from design and implementation to optimization, operations, and ongoing management of the solution. Fortinet has you covered every step of the way, freeing up your resources to focus on your business.



## Feature Highlights: Technical Support

Organizations depend on Fortinet solutions to provide critical services. If any issues arise, they need to be addressed quickly to help ensure security and business continuity. Flexible support options help organizations maximize uptime, security, and performance according to the individual needs of each business.

### 24×7 FortiCare

Technical support is delivered through our global technical assistance and regional support centers.

- Global toll-free numbers are available 24×7
- Web chat for quick answers
- A support portal for ticket creation or to manage assets and life cycles
- Standard next-business-day RMA service

### ASE FortiCare

Fast-track access to technical experts for accelerated issue resolution.

- Direct access to dedicated enterprise support team
- Single-touch ticket handling by the ASE team
- Enhanced SLAs

*Available for FortiGate, FortiGate VM, and FortiWiFi appliances*

### Premium Hardware Replacement

Premium RMA options are available across the portfolio for expedited replacement of defective hardware.

- Next-day delivery
- 4-hour courier
- 4-hour courier with on-site engineer
- Secure RMA: non-return of defective hardware

### Best Practice Service

Connect with specialists who provide guidance on best-practice deployments, upgrades, and operations.

- Speed adoption of new capabilities with expert guidance, sample configurations, vetted playbooks, and example scripts
- Aid DevOps with practical advice on common feature usage, relevant tools, and sample code
- Access proven models for integration with third-party products

*Available for FortiManager, FortiMonitor, and FortiClient, FortiEDR, FortiSOAR*

## Self-service Resources

For expedited answers, Fortinet maintains ample self-service resources to get you the answers you need, fast. Resources include a knowledge base with tips, quick-start and video guides, and connections to the global Fortinet community.

Feature Highlights: Advanced Services

For enhanced security and tailored guidance, FortiCare Advanced Services gives you direct assistance from technical experts who know your business and can help accelerate issue resolution. With designated account management and service delivery, you can focus on your business while we focus on your success.



Entitlements vary by level but can include:

Designated advanced technical support	for focused resolution of incoming technical support issues.
Service delivery management	annual service and performance review. Quarterly operational review to cover technical ticket statistics, quality issues, overall ongoing ticket analysis, product life cycle, ongoing activity, and 90-day project planning.
Annual training package	including NSE 4 and NSE 5 training and certification vouchers.
Advanced service points	for remote after-hours assistance, product upgrade assistance, and software recommendations.
Root-cause analysis	of critical incidents (Priority-1 and Priority-2) related to Fortinet appliances.
Upgrade assistance	which may include software recommendation, upgrade testing, and planning assistance.

Advanced Service for Enterprise and Service Providers

Enterprise offerings come in three levels: PREMIUM, BUSINESS, and FIRST. Service Providers offerings come in two levels: SELECT and ELITE. Benefits vary by level.

Global FIRST and Global ELITE Advanced Services packages are also available to extend the geographical coverage of the service. This service level provides a designated lead engineer per region covering EMEA, Americas, and Asia Pacific. The service features, as described in the FIRST service, are provided within each region with global coordination.

## Feature Highlights: Professional Services

As networks and threats rapidly evolve, it's critical to make sure security capabilities can keep up. Given the global cybersecurity skills shortage, today's organizations often lack the in-house expertise or enough staff to deploy, operate, and maintain the new technologies required to close security gaps. FortiCare Professional Services delivers expert help to ensure Fortinet deployments are optimized for each customer's unique needs.

### Hit the Ground Running With New Capabilities

Fast-track return on investment (ROI) with streamlined expert deployment. Consultants with multivendor experience help swiftly migrate from legacy technologies and adopt new capabilities.

### Extend In-house Teams With Dedicated Resources

Offload redundant operational tasks including configuration, upgrades, and technical incident management to domain experts who know your business.

### Achieve Performance and Configuration Excellence

Adapt protections when there are changes in users, applications, and traffic patterns with regular reviews of configuration, performance, and policies, for reliability and sustained security.

## Product-agnostic Consulting Services

Cybersecurity Advisory and Consulting Services allow our experts to partner with business leaders, helping organizations be at their best through this ever-changing environment. Fortinet experts discover existing security posture elements through a vendor-agnostic approach; align findings to business goals, strategic objectives, and compliance requirements; and guide existing projects and future planning toward framework maturity.



### Discover

Business Goals  
Security Posture  
Systems/Objectives



### Align

Security Framework  
Compliance Requirements  
Strategic Objectives



### Guide

Architectural Design  
Operational Practices  
Maturity Roadmap

## FortiGuard Labs Consulting

Consulting services are designed to help your organization address your specific threat landscapes and improve your organization's ability to use threat intelligence to meet that challenge. These services leverage the expertise and experience of the FortiGuard Labs team and provide the answers to the questions organizations are asking most:



### Threats

What are the most important threats on which I should focus?



### Environment

Is my environment as secure as it needs to be?



### Operations

Are my people properly trained to defend us against the threats we face?

## Fortinet Technical Assistance Centers



### Regional COE:

- Vancouver
- Sophia Antipolis
- Kuala Lumpur

### AMER Regional TAC:

- Dallas
- Mexico City
- Miami
- Ottawa
- Sunnyvale

### EMEA Regional TAC:

- Bangalore
- Dubai
- Frankfurt
- Prague

### APAC Regional TAC:

- Beijing
- Sydney
- Tokyo

## FortiCare Services

	24x7 FortiCare	ASE FortiCare	Premium RMA	Best Practice Services	Advanced Services	Professional Services
Technical Support	✓	✓				
Enhanced SLAs		✓			✓	
Hardware Replacement	✓	✓	✓			
Technical Account Management					✓	
Architecture and Design						✓
Migration and Deployment						✓
Deployment and Upgrade Guidance				✓	✓	✓
Optimization and Integration						✓
Operations and Management						✓

Service	Description
<b>Technical Support</b>	
24x7 FortiCare	24x7 Technical Support per device—12 months.
ASE FortiCare	Advanced Support Experience Technical Support per device—12 months.
Best Practice Service	Best-practice guidance for deployments and upgrades per device—12 months.
<b>Advanced Services</b>	
Premium—Enterprise Technical Support Service	Premium—Enterprise Support Service—12 months.
Business—Enterprise Technical Support Service	Business—Enterprise Support Service provided by designated engineer—12 months.
First—Enterprise Technical Support Service	First—Enterprise Support Service provided by designated Technical Account Manager—12 months.
Global First—Enterprise Technical Support Service	Global First—Enterprise Support Service provided by designated TAM—12 months.
Select—Service Provider Technical Support Service	Select—Service Provider Support Service provided by advanced services team with Service Delivery Manager—12 months.
Elite—Service Provider Technical Support Service	Elite—Service Provider Support Service provided by advanced services team with designated Technical Account Manager and Service Delivery Manager—12 months.
Global Elite—Service Provider Technical Support Service	Global Elite—Service Provider Support Service provided by advanced services team with designated Technical Account Manager and Service Delivery Manager—12 months.
<b>Professional Services</b>	
Solution Architect Consultancy Service	Per-day solution architect consultancy engagement to document, design, and deliver security architecture improvements per agreed scope.
On-site or Remote Resource Service	Per-day charge for on-site or remote professional service engagement delivery.
On-site or Remote Dedicated Resource Service	12- or 6-month on-site or remote dedicated resource.
<b>FortiGuard Labs Consulting</b>	
FortiGuard Professional Services	FortiGuard Labs Consulting service—On-site or remote. Mitigation strategy, advanced offensive (red team) and defensive (blue team) techniques.
FortiGuard Penetration Testing Service	Remote penetration test of 1 web application or 1 mobile application.
FortiGuard Penetration Testing Service	Remote vulnerability assessment of up to 16 IPs, 32 IPs, 64 IPs, or 128 IPs.
Resource Service—Customer Readiness Testing (SOW)	Per-day charge for customer readiness testing (SOW).
Resource Service—Network Integration	Resource service—Network integration
Resource Service—Network Design and Optimization	Resource service—Network design and optimization
Resource Service—Security Assessment	Resource service—Security assessment
Incident Response Training	Incident response and forensics training
Digital Forensics and Incident Response Consulting Hourly	Digital forensics and incident response consulting services.



## SOLUTION BRIEF

# FortiCare Professional Services

## Introduction

As networks and threats rapidly evolve, it's critical to make sure security capabilities can keep up. Given the global cybersecurity skills shortage, today's organizations often lack the in-house expertise or enough staff to deploy, operate, and maintain the new technologies required to close security gaps. FortiCare Professional Services delivers expert help to ensure Fortinet deployments are optimized for each customer's unique needs. Our experts reduce risk with:

- Accelerated implementation
- Operational enablement for IT teams
- Capability optimization to provide the best security

Further, we can assist with ongoing operations of the Fortinet Security Fabric.

## Streamlined Deployment, Capability Optimization, and Ongoing Operations

### Hit the Ground Running With New Capabilities

Fast-track return on investment (ROI) with streamlined expert deployment. Consultants with multivendor experience help swiftly migrate from legacy technologies and adopt new capabilities. Driven by proven methodology, FortiCare Professional Services plans and executes implementations efficiently and effectively.

### Achieve Performance and Configuration Excellence

As a business evolves, it needs to adapt protections when there are changes in users, applications, and traffic patterns. Professional Services provides regular reviews of configuration, performance, and policies, for reliability and sustained security.

### Extend In-house Teams With Dedicated Resources

In-house IT teams can focus on more critical duties while Fortinet dedicated resources handle administration. Our engineers are domain experts who will get to know each business they are assigned to. Offload redundant operational tasks including configuration, upgrades, and technical incident management. Our experts work closely with in-house teams to maximize productivity by transferring technical and operational knowledge.



**FortiCare Professional Services is available for all Fortinet products and is customized to meet each customer's needs.**

## Professional Services Projects

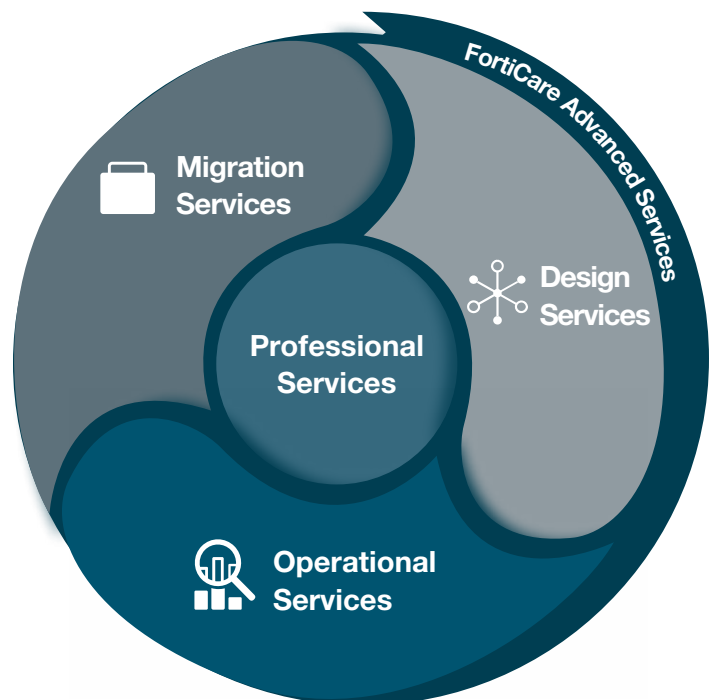
Examples of projects we have executed for our customers include:

<b>Migration from legacy vendor technologies to Fortinet</b>	Production-to-production planning, deployment, and policy migration for firewalls, UTMs, VPNs, and most WLAN/LAN security peripherals
<b>Design and configuration validation</b>	Fortinet solution optimization, integration, and proposed design solution validation
<b>Implementation and configuration</b>	Initial deployment, including installation, provisioning, integration, testing, and production rollout
<b>Integration of the Fortinet Security Fabric with other complementary technologies</b>	Integration with ServiceNow, Splunk, and other security technologies for enhanced visibility and reduced incident investigation timelines
<b>Compliance checks and audit preparation</b>	Guidance on audit and compliance processes, including advice on the correct and optimal configuration of the deployed Fortinet solution
<b>Performance and configuration health checks and policy optimization</b>	Operational performance measurement in a production environment, including a review to identify issues and provide configuration-tuning and policy-optimization recommendations
<b>Dedicated resources for ongoing assistance</b>	Experts available to help with operations after deployment

All service engagements include operational enablement and knowledge transfer to ensure in-house staff is able to operate and maintain the solutions after the service is complete. Although designed to be delivered remotely, on-site options are available.

## Ensure Security Deployments Are Effective and Efficient

Operational teams face challenges when deploying any new technology, and the complexities of today's enterprise networks make it increasingly important to architect and configure security solutions correctly. FortiCare Professional Services gives organizations expert resources to implement and integrate security deployments quickly, while ensuring they are optimized for each unique environment.



[www.fortinet.com](http://www.fortinet.com)



# Fortinet Professional Engineer (PSE) – BIO

---

**Summary PSE 1** - A seasoned consultant with over 18+ years of security and IT experience. Served as the Network Manager, Project Manager and Security lead on over ninety consulting engagements for both small medium and large organizations across different industries. Engagements involved performing a wide range of security services including but not restricted to security appliance configuration, deployment, information risk assessments, network security assessments and architecture, security policy development/review, penetration testing, and DRP/BCP development and testing.

### Technologies – PSE 1

- Firewalls, IDS/IPS,UTM, switching routing and routing protocols, Directory Services, Windows servers and desktops, Linux, Antivirus, IP video surveillance, Wi-Fi, security scanners, Security Event Management, VMware, Network topologies, VPN technology, cloud computing, ecommerce, Encryption, LDAP, Radius, Extrusion Prevention, Network Access Control, Security Gateways, Web Content Filtering, Identity Management, Application firewalls, Database monitoring.

**Summary PSE 2** - Over 12 years Technology Industry experience with a variety of roles from Training, Support, and Professional Services, with a primary focus on Network Security and Infrastructure Architecture.

### Technologies – PSE 2

- Security/Firewall
  - FortiGate, Linux IP Tables, Cisco PIX/ASA, IPSec/SSL VPNs, IPS/IDS, DoS, Certificates/PKI, Authentication, FW Virtualization
- Routing
  - Static, Policy Based Routing (PBR), RIP, OSPF, BGP, RPF, NAT, Load-Balancing
- Switching
  - Cisco CATOS/IOS, VTP/VLANS, STP, 802.3ad Link Aggregation
- WAN
  - Modem dialup, ISDN, xDSL, T1/T3, ATM, Fibre, GigE, WAN Optimization
- Services/Protocols
  - HTTP(S), SMTP, POP3, IMAP, DNS, FTP, TFTP, SYSLOG, DHCP, SIP, SNMP, ICMP, TCP, UDP, ESP, IKE, LDAP, RADIUS
- Network Monitoring and Management
  - HP Openview, FortiManager, FortiAnalyzer, Wireshark, SNMPc, Kiwi
- Server Applications
  - Windows Server: Active Directory, DNS, IIS
  - Linux: BIND, Apache, Syslog, Sendmail, Postfix, MySQL

### **Industry Experience (PSE 1 and PSE 2)**

Fortinet Professional Services engineers provide expert level consultation across all business sectors to include but not limited to the following.

- Health Care
- Financial
- Government
- Law
- Education

### **Specialties (PSE 1 and PSE 2)**

- Information Assurance, IT Security Governance, FISMA, HIPPA, Cobit
- Information/ Network Security Architecture, Vulnerability Assessment and Threat Management
- Integration of physical and logical security, Incident Response- Risk Management/ Crisis Management
- Continuity of Operation and Disaster Recovery, Defense-in-Depth (DiD),
- Risk Assessment and Compliance, Data Classification and Categorization
- Certification and Accreditation Program (CAP), Systems Security Plans Incident Response
- Security T&E – Security IAM/ IEM

### **Certifications (PSE 1 and PSE 2)**

All Fortinet Professional Services engineers are at a minimum NSE4 certified with the vast majority of engineers NSE7 certified. Fortinet PSEs also hold multiple industry certifications as well to include but not limited to the following.

- NSE 7, CISSP-ISSAP, FCSE, CISM, ITIL v3, NSA-IAM/IEM, CNSS-Network Protection - “Infosec Professional”
- CNSS-Security Management. NSTISSI-4011, CNSSI-4012, CNSSI-4013 (A), CNNSI-4014 (A), NSTISSI-4015, CNSSI 4016 (A), Security Management Certification – Network Security Certification
- CEH, GIAC, FCSP, CCSP, WCSP



# Fortinet Security Fabric

## Cybersecurity Platform to Enable Digital Innovation

**FortiOS**  
The Heart of the  
Fortinet Security Fabric



### Zero Trust Access



- FortiNAC**  
Enforce dynamic network access control and network segmentation
- FortiAuthenticator**  
Identify users wherever they are and enforce strong authentication
- FortiClient**  
Endpoint integration, visibility, and protection across entire network
- FortiToken Mobile**  
One-time password application with push notification

### Surveillance & Communications



- FortiRecorder**  
Platform for management of cameras, systems, and storage
- FortiCamera**  
Centrally-managed HDTV-quality security coverage reliability
- FortiVoice**  
Centralized control and simplified management of phone systems
- FortiFone**  
Robust IP Phones w/ HD Audio for versatile deployments

### Security-Driven Networking



- FortiGate SD-WAN**  
Application-centric, scalable, and Secure SD-WAN with NGFW
- FortiGate**  
NGFW w/ SOC acceleration and industry-leading secure SD-WAN
- FortiSwitch**  
Deliver security, performance, and manageable access to data
- FortiAP**  
Protect LAN Edge deployments with wireless connectivity
- FortiExtender**  
Extend scalable and resilient LTE and LAN connectivity
- FortiSASE**  
Secure access service edge to deliver security everywhere
- FortiProxy**  
Enforce internet compliance and granular application control
- FortiIsolator**  
Maintain an "air-gap" between browser and web content
- FortiPresence**  
Real-time location trends, visitor analytics, and heat mapped flows

### Fabric Management Center | SOC



- FortiXDR**  
Collect, normalize, and correlate data across security controls
- FortiEDR**  
Automated protection and orchestrated incident response
- FortiSIEM**  
Integrated security, performance, and availability monitoring
- FortiSOAR**  
Automated security operations, analytics, and response
- FortiAnalyzer**  
Correlation, reporting, and log management in Security Fabric
- FortiSandbox**  
Secure virtual runtime environment to expose unknown threats
- FortiDeceptor**  
Discover active attackers inside with decoy assets
- FortiAI**  
Accelerate mitigation of evolving threats and threat investigation
- FortiGuard MDR Service**  
Monitor and hunt for threats; analyze events; leverage alerts

### Adaptive Cloud Security



- FortiGate VM**  
NGFW w/ SOC acceleration and industry-leading secure SD-WAN
- FortiMail**  
Secure mail gateway to protect against SPAM and virus attacks
- FortiWeb**  
Prevent web application attacks against critical web assets
- FortiCASB**  
Prevent misconfigurations of SaaS applications and meet compliance
- FortiADC**  
Application-aware intelligence for distribution of application traffic
- FortiCWP**  
Manage risk and compliance through multi-cloud infrastructures
- FortiGSLB**  
Ensure business continuity during unexpected network downtime
- FortiDDoS**  
Machine-learning quickly inspects all Layer 3, 4, and 7 packets
- FortiCloud Networking**  
Manage network access, assets, and services through single-pane
- FortiPhish**  
Informative simulation to educate internal users of potential threats

### Fabric Management Center | NOC



- FortiManager**  
Centralized management of your Fortinet security infrastructure
- FortiCloud**  
Protect and deliver data and apps in the Cloud and on-premises
- FortiMonitor**  
Analysis tool to provide NOC and SOC monitoring capabilities
- FortiAIops**  
Network inspection to rapidly analyze, enable, and correlate

### Open Ecosystem



- Extended Fabric Ecosystem**

### FortiGuard Security Services



Content Security  
Web Security | Advanced SOC/NOC  
User Security | Device Security



Revised October 1, 2021

Icons on this document link to additional information

© Fortinet Inc. All Rights Reserved.

BROCHURE

# Fortinet Product Certifications





## Fortinet Product Certifications

Organizations looking to expand, upgrade, or replace their security solutions often find themselves struggling to compare solutions from different vendors. In addition to consistent information about features and functions, they also need information about the compliance and certification level of individual solutions and whether they will enable them to meet regulatory requirements.

To help companies navigate this process, third-party labs and auditors conduct independent testing to enable a fair comparison between products for things like performance, compliance, and functionality. Using industry standards and advanced benchmarking technologies, such as independent validation of products and services, is essential for businesses to evaluate whether a solution will meet their unique business requirements.

### Third-party Testing

Fortinet has actively participated in third-party testing since we first opened our doors. We are committed to the testing and certification process and believe that it provides three key benefits:

- It validates our design and development process. Third-party labs set standards for functionality, performance, and real-world use cases that help drive the development of key features.
- It helps improve our technology. Direct feedback from standardized benchmark testing helps us in our effort to continually improve our technologies.
- It allows our customers to easily compare our technologies against solutions from other vendors. Annual testing helps us set the bar higher every year, with the objective of achieving a leadership position in every test in which we participate.

### Certifications and Regulatory Compliance

Public and private sector organizations alike require solutions that meet regulatory and compliance requirements. Fortinet is committed to meeting a wide range of national, regional, and international requirements, and we subject our solutions and services to independent third-party audits and testing to guarantee compliance.

### The Fortinet Certifications Resource Center (CRC)

Fortinet's [CRC](#) is the repository for product compliance reports, certifications, and independent validation results from unbiased agencies. The scope of Fortinet's product certifications includes the following categories:

#### Product Certifications



Independent lab testing of Fortinet products using industry standards, best practices, and real-world testing environments

#### Information Security



Certifications and examinations of Fortinet's infrastructure security and networking solutions

#### Compliance



Certifications attesting to Fortinet products' compliance with public sector regulatory frameworks and standards



#### Certifications At-a-Glance

- Fortinet's commitment to innovation and excellence has earned the respect of independent test labs around the world
- 25+ years of consistent testing and compliance
- A wide range of global certifications across verticals

## Product Certifications Overview

Category	Certification	Description	Latest Publication Date	
Product Certifications	<a href="#">ICSA Labs</a>	ICSA Labs is an independent division of Verizon. They provide third-party testing and certification of security and health-related IT products and network-connected devices to measure product compliance, reliability, and performance.	IPsec VPN	08/10/2021
			Firewall	08/25/2021
			WAF	09/27/2021
	<a href="#">AV-Comparatives</a>	AV-Comparatives is an independent lab offering systematic testing to determine whether security software—such as PC/Mac-based antivirus products and mobile security solutions—lives up to its claims. Using one of the largest sample collections in the world, they create a real-world environment for truly accurate testing. Certification by AV-Comparatives provides a globally recognized seal of approval for software performance.	Business Security Test: Mar-Jun 2021	
	<a href="#">SE Labs</a>	SE Labs tests a range of solutions, including endpoint software, network appliances, and cloud services, on their ability to detect attacks, protect against intrusions, or both.	Email Security Services Protection: Jan-Mar 2020	
	<a href="#">MEF 3.0</a>	MEF 3.0 is an SD-WAN Certification Program that uses Spirent as their SD-WAN Authorized Certification and Test Partner (ACTP). Certification involves rigorous tests of the service attributes and requirements defined in MEF 70 and described in detail in the upcoming MEF SD-WAN Certification Test Requirements (MEF W90) standard.	MEF 3.0 SD-WAN: Jun 2020	
	<a href="#">Virus Bulletin</a>	VB is a world leader in security software testing. Their publicly available test reports cover anti-malware protections of all types as well as enterprise-level email and web security solutions.	VBSspam	Sept 2021
			VB100	Sept 2021
	<a href="#">MITRE Engenuity</a>	MITRE Engenuity's ATT&CK™ evaluations assess the ability of a vendor's solutions to defend against specific adversary tactics and techniques. They openly publish these results to provide end-users with the information needed to make good purchasing decisions. These evaluations are not a competitive analysis. There are no scores, rankings, or ratings. Instead, they show how each vendor approaches threat detection in the context of the MITRE ATT&CK knowledge base to provide an unbiased assessment of detection and protection capabilities and highlight potential gaps to drive the industry forward.	Round 3: Fin7/Carbanak: Apr 2021	
Information Security	<a href="#">SOC2</a>	SOC2 is an auditing procedure that ensures that service providers securely manage their customers' data. It covers their security, availability, processing integrity, confidentiality, and/or privacy controls. Compliance is based on the AICPA's (American Institute of Certified Public Accountants) TSC (Trust Services Criteria).	SOC2 Type 2: Apr-Sept 2021	
	<a href="#">ISO</a>	ISO/IEC 27001 is an international standard for managing information security. It defines requirements and controls for establishing, implementing, maintaining, and continually improving an organization's Information Security Management System (ISMS).	ISO/IEC 27001: Jun 2021-Jun 2024	
Government Regulations	<a href="#">FIPS Validated</a>	The Federal Information Processing Standard 140-2 (FIPS 140-2) is an information technology security accreditation program for validating cryptographic modules developed by vendors that meet well-defined security standards.	FIPS 140-2 Level 1	Aug 2021
			FIPS 140-2 Level 2	Sept 2021
	<a href="#">Common Criteria</a>	Common Criteria is an international standard (ISO/IEC 15408) operated by 17 certificate-authorizing nations. 31 countries have accepted it for their respective government acquisition requirements for their IT/networking infrastructures.	CC EAL4+	Oct 2021
			FWcPP+IPS +VPN	Jan 2021



## Summary

Fortinet is committed to the independent testing and certification of its products and services. ICSA, AV-Comparatives, Virus Bulletin, and other independent testing organizations have consistently validated the effectiveness of Fortinet solutions. Fortinet earned ICSA's prestigious Excellence in Information Security Testing (EIST) award for 15 years of participation in 2017 and has been recognized by ICSA for outstanding achievement in information security certification testing 10 years in a row.

**"Real-world third-party validation is an essential resource for enterprises considering security products, helping to cut through the confusion that can be caused by vendor marketing. Fortinet relies on a variety of third-party testing and compliance labs to provide reliable information to organizations making critical security purchasing decisions. They also demonstrate Fortinet's commitment to meeting high industry standards for security detection, performance, reliability, management, and value."**

*- Fortinet CEO Ken Xie*



[www.fortinet.com](http://www.fortinet.com)



# CERTIFICATE

The Certification Body of  
TÜV SÜD AMERICA INC.

hereby certifies that

**Fortinet Technologies (Canada) ULC**  
4190 Still Creek Drive Suite 400  
Burnaby, V5C 6C6 Canada  
(see page 2-4 for additional locations)

Has implemented a Quality Management System in accordance with:

**ISO 9001:2015**

The scope of this Quality Management System includes:

**The Design, Development and Manufacture of Network  
Security Products and the Delivery of Associated  
Security Services and Support Functions**

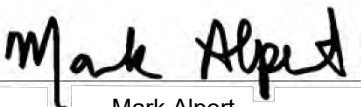
Certificate Expiry Date: June 30, 2023

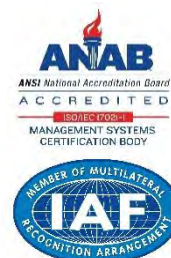
Certificate Registration No: 951 11 5647

Issue Date: July 8, 2020

Reissue Date: N/A



  
Mark Alpert  
Vice President, Business Assurance







America

# CERTIFICATE

## Fortinet Technologies (Canada) ULC

4190 Still Creek Drive Suite 400  
Burnaby, V5C 6C6 Canada

Scope - The Design, Development and Manufacture of Network  
Security Products and the Delivery of Associated Security  
Services and Support function

Processes – Order Entry, Scheduling, Planning for Product Realization,  
Product / Project Management, Software Development,  
Hardware Engineering, Production QC Management, Working  
Environment Control, Technical Documentation, Human Resources,  
Records Management & MIS Control

## Fortinet Technologies (Canada) ULC

326 Moodie Dr  
Nepean, ON, K2H 8G3 Canada

Scope - Development & Support for Fortinet mail and  
Preparation of Technical Documents

Processes – Software Development, Technical Support and  
Customer Service, Technical Documentation, Management &  
MIS Control, Human Resources

Certificate Expiry Date: June 30, 2023

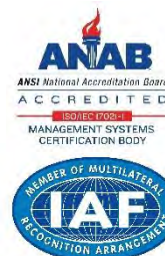
Certificate Registration No: 951 11 5647

Issue Date: July 8, 2020

Reissue Date: N/A



  
Mark Alpert  
Vice President, Business Assurance





# CERTIFICATE

**Fortinet Technologies (Canada) ULC**  
**4185 Still Creek**  
**Burnaby, V5C 6G9 Canada**

**Scope - Information Technology Support Location, Including  
 New Equipment Preparation and Troubleshooting for Headquarters**

**Processes – Record Management & MIS Control**

**Fortinet Inc.**  
**899 Kifer Road**  
**Sunnyvale, 94086 USA**

**Scope - The Design, Development and Manufacture of  
 Network Security Products and the Delivery of  
 Associated Security Services and Support Functions**

**Processes – Order Entry, Scheduling, Planning for Product Realization,  
 Product / Project Management, Software Development, Hardware  
 Engineering, Purchasing, Technical Support and Customer Service,  
 Records Management & MIS Control, Human Resources, Infrastructure  
 and Working Environment Control**

**Certificate Expiry Date: June 30, 2023**

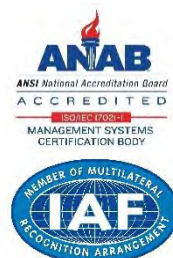
**Certificate Registration No: 951 11 5647**

**Issue Date: July 8, 2020**

**Reissue Date: N/A**



  
 Mark Alpert  
 Vice President, Business Assurance





# CERTIFICATE

**Fortinet Inc.**  
1570 Atlantic St  
Union City, 94587 USA

**Scope - The Manufacture, Quality Control and  
Operation Function of Network Security Products**

**Processes – Production Control & Service Provision –  
Product Integration, Shipping and Receiving IQC,  
RMA Control and Management**

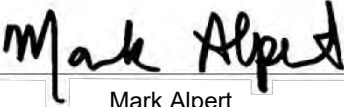
**Certificate Expiry Date: June 30, 2023**

**Certificate Registration No: 951 11 5647**

**Issue Date: July 8, 2020**

**Reissue Date: N/A**



  
Mark Alpert  
Vice President, Business Assurance  
Page 4 of 4

