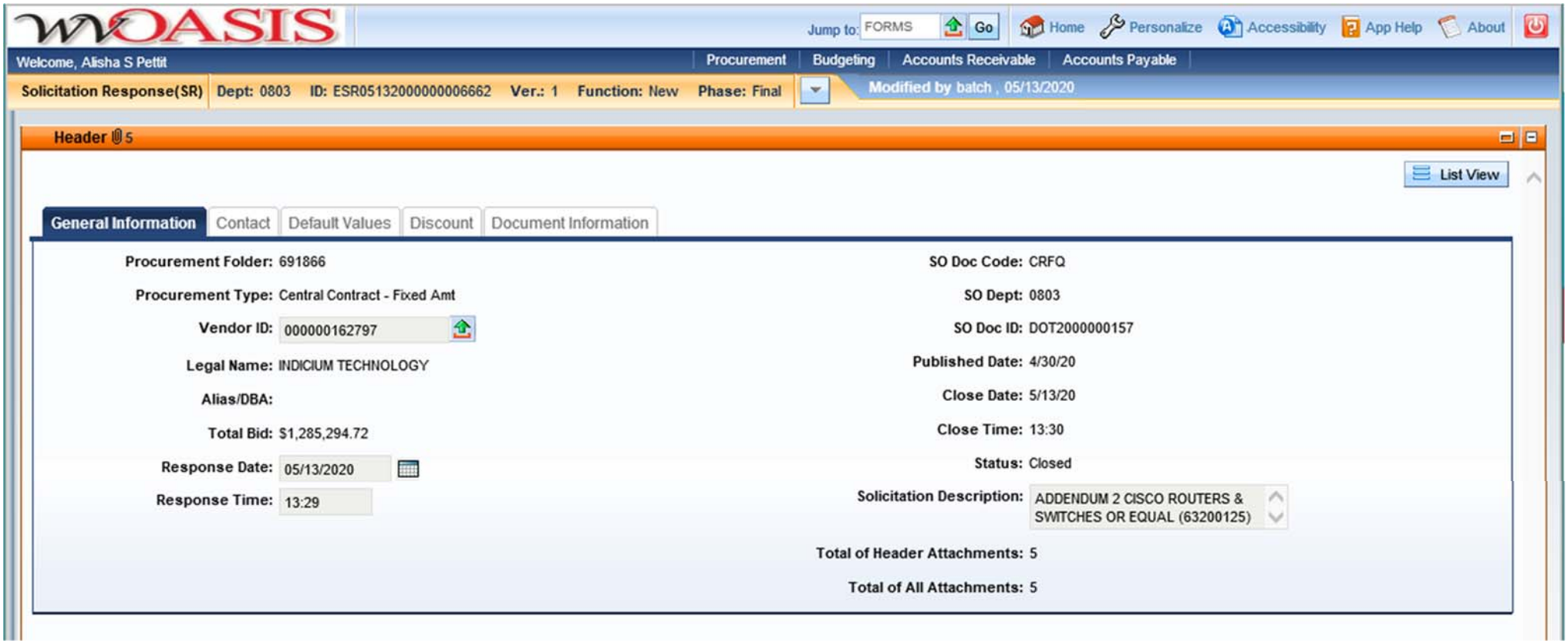
The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at ***WVPurchasing.gov*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.


WVOASIS
Jump to: FORMS Go
Home
Personalize
Accessibility
App Help
About
Welcome, Alisha S Pettit
Procurement
Budgeting
Accounts Receivable
Accounts Payable
Solicitation Response(SR) Dept: 0803 ID: ESR05132000000006662 Ver.: 1 Function: New Phase: Final
Modified by batch , 05/13/2020
Header 5
List View
General Information
Contact
Default Values
Discount
Document Information
Procurement Folder: 691866
Procurement Type: Central Contract - Fixed Amt
Vendor ID: 000000162797
Legal Name: INDICIUM TECHNOLOGY
Alias/DBA:
Total Bid: $1,285,294.72
Response Date: 05/13/2020
Response Time: 13:29
SO Doc Code: CRFQ
SO Dept: 0803
SO Doc ID: DOT2000000157
Published Date: 4/30/20
Close Date: 5/13/20
Close Time: 13:30
Status: Closed
Solicitation Description: ADDENDUM 2 CISCO ROUTERS & SWITCHES OR EQUAL (63200125)
Total of Header Attachments: 5
Total of All Attachments: 5

Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder : 691866

Solicitation Description : ADDENDUM 2 CISCO ROUTERS & SWITCHES OR EQUAL (63200125)

Proc Type : Central Contract - Fixed Amt

Date issued	Solicitation Closes	Solicitation Response	Version
	2020-05-13 13:30:00	SR 0803 ESR05132000000006662	1

VENDOR

000000162797

INDICIUM TECHNOLOGY

Solicitation Number: CRFQ 0803 DOT2000000157

Total Bid : $1,285,294.72 **Response Date:** 2020-05-13 **Response Time:** 13:29:46

Comments: This bid is my second bid showing an upgraded switch. Please consider both for evaluation purposes.

FOR INFORMATION CONTACT THE BUYER

Crystal G Hustead

(304) 558-2402
crystal.g.hustead@wv.gov

Signature on File **FEIN #** **DATE**

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	3.1.1 Cisco ISR 4321 Series Chassis Bundle or Equal-Year 1	10.00000	EA	$2,325.820000	$23,258.20

Comm Code	Manufacturer	Specification	Model #
43222612			

Extended Description : 3.1.1 CISCO ISR 4321 Series Chassis Bundle or equal with Year 1 Smart Net Coverage

Comments: Fortigate 100F

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	3.1.1 Cisco ISR 4321 Series Chassis Bundle or Equal-Year 2	10.00000	EA	$748.000000	$7,480.00

Comm Code	Manufacturer	Specification	Model #
43222612			

Extended Description : 3.1.1 CISCO ISR 4321 Series Chassis Bundle or equal with Year 2 Smart Net Coverage

Comments: FortiCare

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	3.1.1 Cisco ISR 4321 Series Chassis Bundle or Equal-Year 3	10.00000	EA	$748.000000	$7,480.00

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description : 3.1.1 CISCO ISR 4321 Series Chassis Bundle or equal with Year 3 Smart Net Coverage

Comments: FortiCare

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	3.1.1 Cisco ISR 4321 Series Chassis Bundle or Equal-Year 4	10.00000	EA	$748.000000	$7,480.00

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description : 3.1.1 CISCO ISR 4321 Series Chassis Bundle or equal with Year 4 Smart Net Coverage

Comments: FortiCare

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
5	3.1.2 Cisco ISR 4331 Series Chassis Bundle or Equal-Year 1	6.00000	EA	$2,325.820000	$13,954.92

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description : 3.1.2 CISCO ISR 4331 Series Chassis Bundle or Equal with Year 1 Smart Net Coverage.

Comments: Fortigate & FortiCare

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
6	3.1.2 Cisco ISR 4331 Series Chassis Bundle or Equal-Year 2	6.00000	EA	$748.000000	$4,488.00

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description : 3.1.2 CISCO ISR 4331 Series Chassis Bundle or Equal with Year 2 Smart Net Coverage.

Comments: FortiCare

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
7	3.1.2 Cisco ISR 4331 Series Chassis Bundle or Equal-Year 3	6.00000	EA	$748.000000	$4,488.00

Comm Code	Manufacturer	Specification	Model #
43222612			

Extended Description : 3.1.2 CISCO ISR 4331 Series Chassis Bundle or equal with Year 3 Smart Net coverage

Comments: FortiCare

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
8	3.1.2 Cisco ISR 4331 Series Chassis Bundle or Equal-Year 4	6.00000	EA	$748.000000	$4,488.00

Comm Code	Manufacturer	Specification	Model #
43222612			

Extended Description : 3.1.2 CISCO ISR 4331 Series Chassis Bundle or equal with Year 4 Smart Net coverage

Comments: FortiCare

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
9	3.1.3 Cisco ISR 1101 Series Port Router or Equal-Year 1	55.00000	EA	$2,325.820000	$127,920.10

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description : 3.1.3 Cisco ISR 1101 4 port router or equal with Year 1 Smart Net Coverage

Comments: FortiGate & FortiCare

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
10	3.1.3 Cisco ISR 1101 Series Port Router or Equal-Year 2	55.00000	EA	$748.000000	$41,140.00

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description : 3.1.3 Cisco ISR 1101 4 port router or equal with Year 2 Smart Net Coverage

Comments: FortiCare

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
11	3.1.3 Cisco ISR 1101 Series Port Router or Equal-Year 3	55.00000	EA	$748.000000	$41,140.00

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description : 3.1.3 Cisco ISR 1101 4 port router or equal with Year 3 Smart Net Coverage

Comments: FortiCare

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
12	3.1.3 Cisco ISR 1101 Series Port Router or Equal-Year 4	55.00000	EA	$748.000000	$41,140.00

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description : 3.1.3 Cisco ISR 1101 4 port router or equal with Year 4 Smart Net Coverage

Comments: FortiCare

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
13	3.1.4 Cisco Extreme Networks 12 Port Switch or Equal	90.00000	EA	$5,030.500000	$452,745.00

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description : 3.1.4 Cisco Extreme Networks 12 Port Switch or Equal

Comments: FortiSwitch 548D Series

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
17	3.1.5 Cisco Extreme Networks 48 Port Switch or Equal	70.00000	EA	$6,180.500000	$432,635.00

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description : 3.1.5 Cisco Extreme Networks 48 Port Switch or Equal

Comments: FortiSwitch 548D Series

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
21	3.1.6 Cisco Extreme Networks 24 Port Switch or Equal	15.00000	EA	$5,030.500000	$75,457.50

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description : 3.1.6 Cisco Extreme Networks 24 Port Switch or Equal

Comments: FortiSwitch 548D Series

ENGAGE
FORTINET ADVOCATE PARTNER

Innovative Solutions
TECHNOLOGY

CISCO ROUTERS & SWITCHES OR EQUAL

RFP – WEST VIRGINIA DIVISION OF HIGHWAYS

CRFQ DOT2000000157

RFP – Fortinet Introduction

TABLE OF CONTENTS

1. COMPANY INTRODUCTION

Indicium Technology dba Innovative Solutions Technology is an IT Solutions provider who leverages years of past performance supporting government agencies and businesses. We provide solutions to designed to secure the network and data on-premise or in the cloud. We provide certified personnel to design, implement and maintain the solutions we offer. In order to support WV Department of Highways we believe Fortinet was the best partner to put forth. The SD-WAN solution not only future proofs your network architecture, but with Fortinet you can implement a security driven networking strategy the provides cost savings as well as consolidated management and comprehensive visibility across your network. As you will see, the tightly integrated family of products is by design and intended to facilitate management of your network operation. By proposing Fortinet SD-WAN and Switches we have provided an opportunity to reduce the number of vendors and streamline your security solution stack. This is advantageous for the network operations team as well as from a support standpoint.

Fortinet

FORTINET

Founded: Nov. 2000

First Product Release: May 2002

Fortinet IPO: Nov. 2009
NASDAQ: FTNT

Headquarters: Sunnyvale, California

Employees: 4,900+

FY 2016 Revenue: $1.275B

Q3 2017 Revenue: $374M
Q3 2017 Billings: $432M
Q3 2017 EPS (GAAP): $0.15
Q3 2017 EPS (non-GAAP): $0.28
Market Cap (Oct. 26, 2017): $7B
$1.5B Cash and No Debt

Units Shipped to Date: 3.4M+

Customers: 330,000+

Global Patents Issued: 439
Global Patents Pending: 291

From the start, the Fortinet vision has been to deliver broad, truly integrated, high-performance security across the IT infrastructure.

We provide top-rated network and content security, as well as secure access products that share intelligence and work together to form a cooperative fabric. Our unique security fabric combines security processors, an intuitive operating system, and applied threat intelligence to give you proven security, exceptional performance, and better visibility and control—while providing easier administration.

Our flagship enterprise firewall platform, FortiGate, is available in a wide range of sizes and form factors to fit any environment and provide a broad array of next-generation security and networking functions. Complementary products can be deployed with a FortiGate to enable a simplified, end-to-end security infrastructure covering:

- Network security
- Data center security (physical and virtual)
- Cloud security (private, public, hybrid)
- Secure (wired and wireless) access
- Infrastructure (switching and routing) security
- Content security
- Endpoint security
- Application security

Fortinet is a true innovator and holds more than double the number of patents than any other dedicated network security vendor. Our market position and solution effectiveness have been widely validated by industry analysts, independent testing labs, business organizations, and media outlets worldwide. We are proud to count the majority of Fortune 500 companies among our satisfied customers.

Fortinet is headquartered in Sunnyvale, California, with 100+ offices around the world. Founded in 2000 by Ken Xie, the visionary founder and former president and CEO of NetScreen, Fortinet is led by a strong and seasoned management team with deep experience in networking and security.

2. FORTINET—YOUR SECURITY BUSINESS PARTNER

2.1 Why Fortinet?

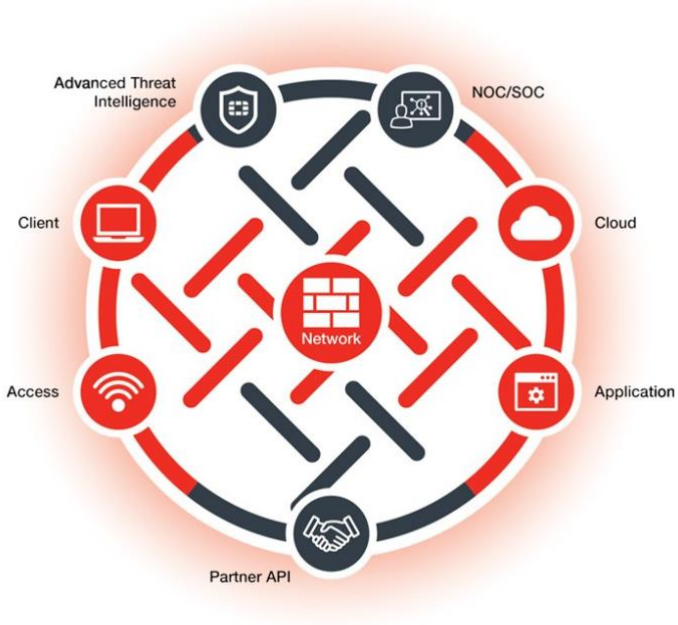
Fortinet Security Fabric

Organizations today require a fast and secure network to be successful. Whether or not you have the right protection immediately responding to threats throughout your network can determine if your business runs smoothly or is the victim of a security breach.

Fortinet is the only company with security solutions for network, endpoint, application, data center, cloud, and access designed to work together as an integrated and collaborative security fabric. This also means we are the only company that can truly provide you with a powerful, integrated end-to-end security solution across the entire attack surface.

To enable an effective defense, the data and security elements across all of your various environments must be well-integrated, able to share intelligence, and visible. The Fortinet Security Fabric gives you control, integration, and easy management of security across your entire organization, from IoT to the cloud.

The Fortinet Security Fabric is an intelligent framework designed for scalable, interconnected security combined with high awareness, actionable threat intelligence, and open API standards.



The Security Fabric is built on three key attributes:

- **Broad**: The Security Fabric covers the entire attack surface. Security can be applied to the network, endpoints, access, applications, and cloud.
- **Powerful**: The Security Fabric uses security processors to reduce the burden on infrastructure, delivering comprehensive security without affecting performance.

- **Automated**: The Security Fabric enables a fast and coordinated response to threats. All elements can rapidly exchange threat intelligence and coordinate actions.

Unparalleled Third-Party Certifications

Real-world testing is the best way to evaluate the effectiveness and speed of technology. The number of unverified claims from vendors about what their products can do is overwhelming. That's why we routinely submit our products and technologies for independent tests so that you can verify for yourself that our claims of top performance and effectiveness are valid.

We routinely receive top scores from organizations such as NSS Labs, ICSA Labs, and Virus Bulletin, and they also provide information on how we stack up against the competition.

More than 330,000 Customers and Growing

Our customers come in all sizes, represent a wide range of industries and organizations, and are located throughout the world. We are proud to count the majority of Fortune 500 companies among our satisfied customers.

2.2 Core Platform High-Level Overview

The backbone of the Fortinet Security Fabric is our flagship network security platform, FortiGate. It consists of physical and virtual appliances that provide a broad array of security and networking functions, including firewall, VPN, anti-malware, intrusion prevention, application control, web filtering, anti-spam, DLP, WAN acceleration, and WLAN control. FortiGate appliances, from the FortiGate 30D for small businesses all the way up to the FortiGate 7000 series for large enterprises, data centers, and service providers, deliver top-rated security and performance with efficient management through:

- FortiGuard – Our large global threat research team discovers new threats and delivers protective services 24x365 across a rich array of consolidated security technologies, including application control, intrusion prevention, web filtering, vulnerability management, anti-malware, anti-spam, and more. By developing and delivering all of our threat research and protection services in-house, we provide you with the fastest and most integrated response to threats. FortiGuard protection is independently validated as highly effective versus today's advanced threats.

- Fortinet Security Processing Units – Our custom-designed SPUs accelerate processing of security and networking functions to radically boost performance and scalability and provide you with the fastest network security appliance performance available. This allows you to stay ahead of rapidly growing bandwidth requirements and prevents your security solution from becoming a choke point in your network.

- FortiOS – Our proprietary operating system provides the foundation for and integration of all security and networking functions. This allows IT managers to deliver consistent and coordinated policies across all security devices, creating a faster and more robust

response to threats with a far lower administrative burden. Flexible licensing of FortiOS features gives you the flexibility to deploy what you need, where you need it--leading to a simpler, easier to maintain infrastructure as well.

- Single-pane-of-glass management - Our easy-to-use management platform—available in hardware appliance, virtual machine, and cloud form factors—provides centralized configuration, security policy management, aggregate logging, reporting, and forensic analysis for up to 10,000 Fortinet devices.

By integrating and accelerating multiple proprietary security and networking functions with purpose-built SPUs and FortiOS, delivering dynamic proprietary security service updates via FortiGuard, all managed through a simple comprehensive management console, Fortinet's network security platform delivers broad protection against dynamic security threats while reducing the operational burden, response time, and costs associated with managing multiple point products.

Fortinet offers a broad set of complementary solutions that integrate to form the Fortinet Security Fabric, allowing customers to further secure and simplify their networks, including:

- Sandboxes
- Web application firewalls
- Secure email gateways
- DDoS protection
- Application delivery controllers
- User identity management/authentication and tokens
- Endpoint security for desktops, laptops, and mobile devices
- Secure wireless LAN and WAN
- And more…

3. FORTINET LEADERSHIP

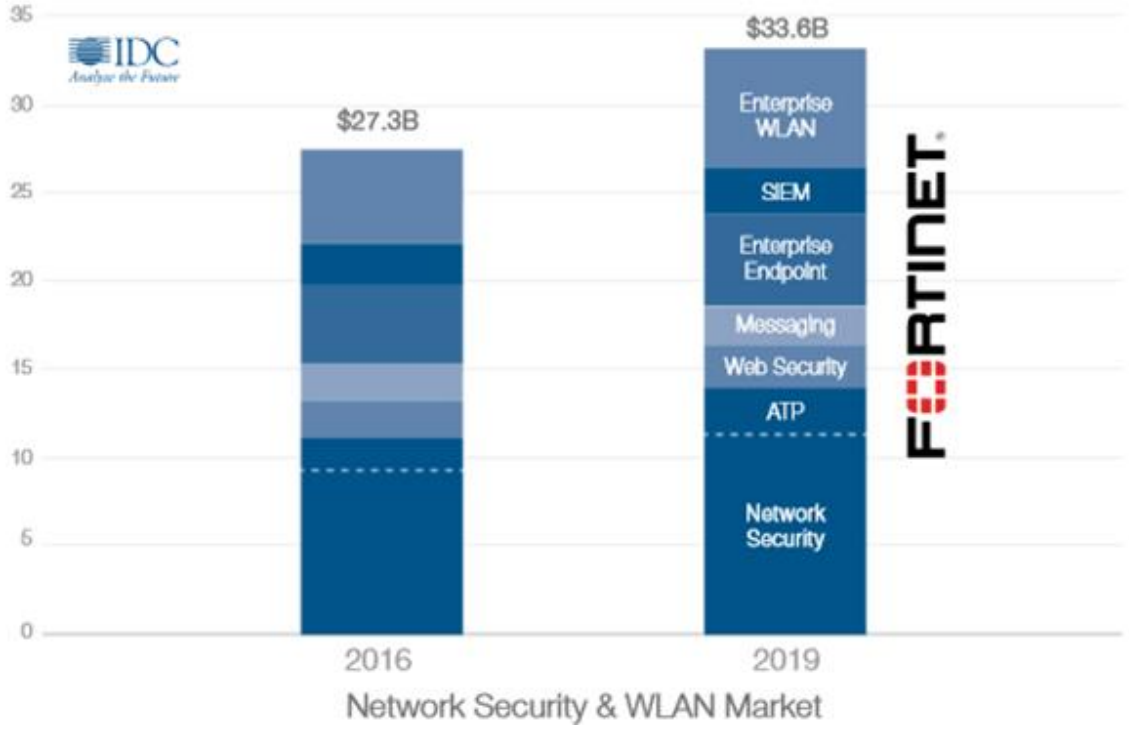
3.1 Industry Leadership

Fortinet's market leadership is recognized by the main industry research and analyst firms including IDC and Gartner:

IDC

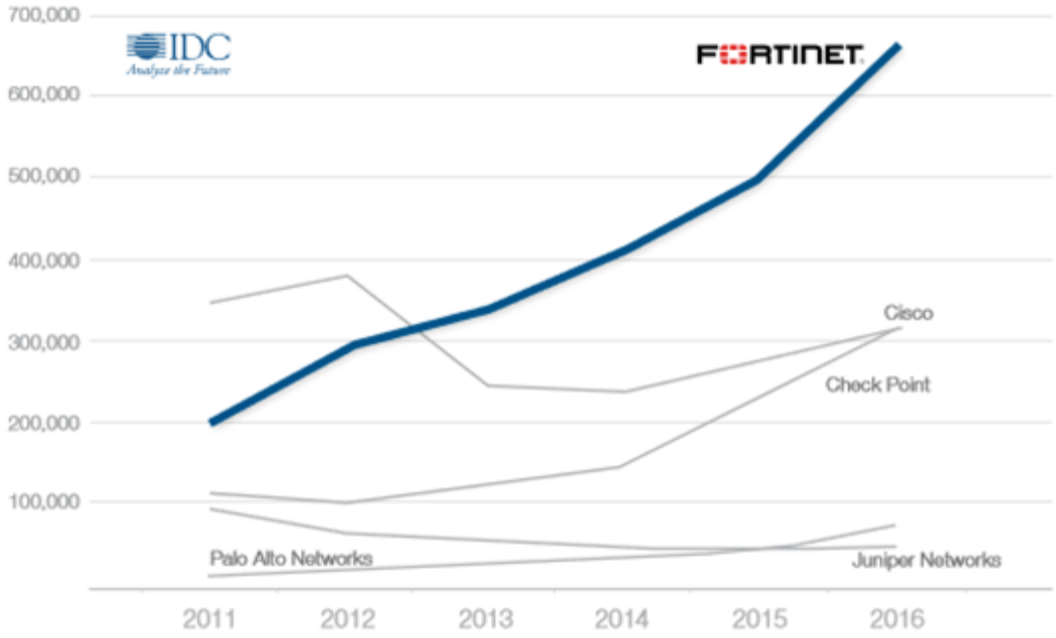
Fortinet is the world's largest network security appliance vendor (unit share) and top 4 network security vendor (revenue share) according to IDC.

Fortinet is a major player in many segments of the fast-growing Network Security and WLAN markets.



Sources:
IDC Worldwide Endpoint Security Forecast, 2016-2020
IDC Worldwide Security and Vulnerability Management Forecast, 2016-2020
IDC Worldwide Enterprise WLAN Forecast, 2016-2020
IDC Specialized Threat Analysis and Protection Forecast, 2016-2020
IDC Worldwide Web Security Forecast, 2016-2020
IDC Worldwide IT Security Products Forecast, 2015-2019

Fortinet is the largest network security appliance vendor (units) and growing quickly, according to IDC...



Source: IDC Worldwide Security Appliances Tracker, April 2017 (based on annual unit shipments)

Gartner

Fortinet is recognized by Gartner in six Magic Quadrants: Enterprise Firewall, UTM, Email Security, SIEM, WAF, and WLAN/LAN.

We are the leader and acknowledged pace-setter in the Gartner UTM Magic Quadrant, and Leader in the Enterprise Firewall Magic Quadrant

Gartner Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls)

*Source: https://www.gartner.com/doc/reprints?id=1-43QT4Y6&ct=170621&st=sb

3.2 Unparalleled Third-Party Certification and Validation

Fortinet believes that independent, third-party tests provide a critical and impartial measure of the quality of a product, and a mandatory reference for anyone making an IT security purchase decision. Fortinet participates in unbiased, credible testing so customers can see how we compare to alternative solutions and select the solution that is right for their needs.

Since its inception, Fortinet has received more certifications to validate our solutions than any other network security vendor. These test results are proof that in real world traffic and deployment scenarios, our products earn top ratings and perform as advertised or better. The quality of our security functionality is certified by ICSA Labs, NSS Labs, AV Comparatives, Virus Bulletin, and others. We also meet numerous government standards, such as FIPS 140-2, Common Criteria EAL4+, as well as other important certifications for IPv6 and ISO 9001.

Fortinet is NSS Labs “Recommended” in the following tests:

- NGFW
- DCIPS
- NGIPS
- Web Application Firewall
- Endpoint Protection
- Breach Detection (Sandbox)

Fortinet has participated in the following real-world group tests, open to the industry, and conducted by NSS Labs. In doing so, Fortinet stands out as the only vendor to provide an ATP Solution that is NSS Labs "Recommended" from the data center to the edge to the endpoint in the latest group tests.

The seven-year summary of Fortinet ratings in NSS Labs group tests shows a growing list of "Recommended" ratings.

Product	2011	2012	2013	2014	2015	2016	2017
Firewall	Neutral		Recommended				
NGFW		Neutral	Recommended	Recommended		Recommended	Recommended
Data Center IPS				Neutral		Recommended	
NGIPS					Recommended	Retested & Passed	
Breach Detection				Recommended	Recommended	Recommended	
Web Application Firewall				Recommended			Recommended
Adv. Endpoint Protection					Recommended		Recommended
DDoS						Neutral	

As of June 2017

Fortinet is the only vendor to receive NSS Labs "Recommended" from the edge to the endpoint.

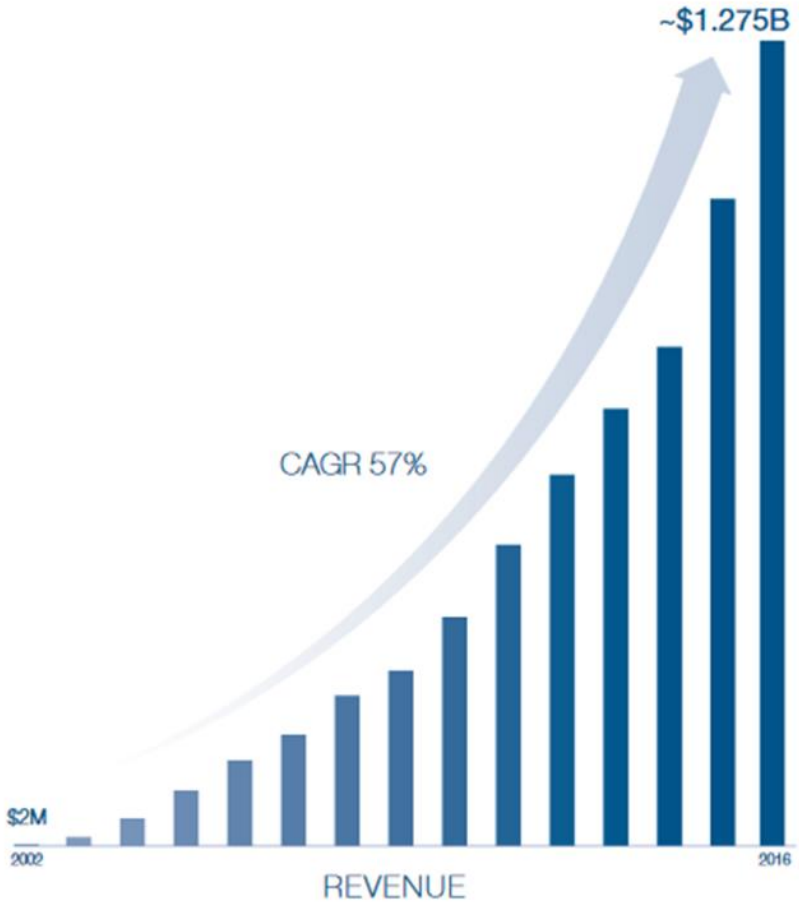
■ RECOMMENDED ☐ NEUTRAL ■ CAUTION ■ RETESTED & PASSED

Certification	Fortinet	Check Point	Cisco	Palo Alto	Juniper SRX	FireEye
NSS Labs Next-Gen Firewall	■	■	■	■	■	X
NSS Labs Data Center Firewall	■	X	X	X	X	X
NSS Labs Breach Detection System	■ ■	■	☐	■ ■	X	☐
NSS Labs WAF	■	X	X	X	X	X
NSS Labs NG IPS	■	X	■	☐	X	X
NSS Labs DC IPS	■	X	X	■	■	X
NSS Labs Advanced Endpoint	■	X	X	X	X	X
BreakingPoint Resiliency Score	■	X	X	☐	X	X
ICSA Firewall	■	■	X	■	■	X
ICSA IPS	■	X	X	X	X	X
ICSA Antivirus	■	X	X	X	X	X
ICSA WAF	■	X	X	X	X	X
ICSA ATD (Sandbox)	■	■	X	■	X	■
ICSA ATD (Email)	■	X	X	X	X	X
VB100 Virus	■	■	X	X	X	X
VBSpam	■	X	X	X	X	X
AV-Comparatives	■	X	X	X	X	X
Common Criteria	■	■	■	■	■	■
FIPS	■	■	■	■	■	■
UNH USGv6/IPv6	■	■	■	■	■	X

3.3 Financial Highlights

Fortinet enjoys a strong financial stability, making the company a long-term player in the IT security industry.

Fortinet generated over $1.275B in revenue and 26% year-over-year revenue growth in 2016, a growth rate far superior to the overall market.



Year	2012	2013	2014	2015	2016
Revenues	*$534m*	*$615m*	*$770m*	*$1B*	*$1.275B*
YoY Growth	*+23%*	*+15%*	*+25%*	*+31%*	*+26%*
Cash & Investments	*$740m*	*$843m*	*$991.7m*	*$1.16B*	*$1.31B*

The company is solidly profitable and has been cash-flow positive for more than eight years.

4. FORTINET ADVANTAGE

4.1 In-House Security Research and Services

Extensive knowledge of the threat landscape combined with the ability to respond quickly at multiple levels is the foundation for providing effective security. Hundreds of researchers at FortiGuard Labs scour the cyber landscape every day to discover emerging threats and develop effective countermeasures to protect more than 330,000 Fortinet customers around the world. Fortinet solutions, including the flagship FortiGate firewall platform, are powered by security services developed by FortiGuard Labs.

FortiGuard Services

FortiGuard security services are available as subscriptions for use in the FortiGate next-generation firewall and IPS platforms as well as with a number of other Fortinet products such as the FortiMail secure email gateway, FortiClient endpoint protection, FortiSandbox, FortiCache, and FortiWeb. You can choose individual services, or get access to all available services with the Enterprise Bundle.

Industry-validated Security Effectiveness

Fortinet solutions with FortiGuard services are consistently confirmed by NSS Labs, Virus Bulletin, AV Comparatives, and ICSA tests to deliver superior security effectiveness.

- 2016 VB Web test found that FortiGuard Web Filtering blocked 97.7% of direct malware downloads. It's the only web filtering service in the industry to receive VB Web certification.
- 2015 VB100 Reactive and Proactive Test ranked Fortinet one of the industry's most effective AV solutions at stopping both known and zero-day threats.
- 2016 VBSPAM test ranked Fortinet Antispam security effectiveness at 99.97 with a 99.998% spam catch rate (the second highest catch rate in the industry).
- 2015 AV Comparatives awarded its highest-level award, the Advanced+ rating to Fortinet for anti-phishing, file detection, and real-world protection.
- NSS Labs consistently awards Fortinet "Recommended" status for NGFW, NGIPS, and Breach Detection (Sandboxing).

FortiGate Solution Services

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with the FortiGuard Enterprise Bundle. This bundle contains the full set of FortiGuard security services plus FortiCare service and support offering the most flexibility and broadest range of protection in one package.

4.2 FortiCare Services

At Fortinet, we put a lot of care into making sure our customers are satisfied with our products and support. Our FortiCare support offerings are specifically designed to provide you with the support you need for all Fortinet products and services no matter where in the world you are.

Support and Advanced Services

With FortiCare Services, you can rest assured that your Fortinet security infrastructure is performing at its absolute best and protecting your critical assets and data. FortiCare Services includes both Support Services and Advanced Services.

FortiCare Support Services

FortiCare Support Services give you global support on a per-product basis. By subscribing to these services, you'll receive a timely response to any technical issue as well as complete visibility on ticket resolution progress.

All FortiCare Support Services include firmware upgrades, access to the support portal and associated technical resources, reporting on technical incidents (via the web, chat, and telephone), as well as a hardware return option.

- **FortiCare 8x5 Service**
  Get access to technical support via the web portal, online chat system, and telephone, including return and replace for hardware failures. You'll also have fast and easy written access to technical support requests.

- **FortiCare 24X7 Service**
  If you need 'round-the-clock access to mission-critical support services, the 24x7 Service will meet your requirements. You'll get access to technical support 24x365 as well as advanced replacement service for hardware failures.

- **FortiCare 360° Service**
  FortiCare 360° Service includes all the services of FortiCare 24x7 Service and provides recurring health checks with a personalized monthly audit report of FortiGate and FortiWiFi appliances. Fortinet engineers will perform device environmental and performance audits and make recommendations. You'll be aware of any potential issues and can take action to avoid service disruptions or performance slowdowns.

FortiCare Premium RMA Service is designed to minimize downtime. There are three options:

- Next-day delivery: Parts are delivered the day following RMA approval by Fortinet support.
- 4-hour courier: Parts are delivered on-site 24 hours a day, 7 days a week within 4 hours of RMA approval by Fortinet support.
- 4-hour on-site engineer: Parts are delivered on-site with an engineer, 24 hours a day, 7 days a week within 4 hours of RMA approval by Fortinet support.

FortiCare Secure RMA Service allows for non-return of an appliance for those customers with strict rules and requirements for physical data protection.

Advanced Services for Enterprise

FortiCare Advanced Services for Enterprise provides integrated support to sustain and optimize Fortinet appliances. The service is delivered by the Advanced Services team, experts in Fortinet and security technology that is deployed in a typical enterprise environment. This scalable service has different service levels ranging from focused

technical support to a comprehensive set of services to help with IT business continuity objectives. FortiCare Advanced Services for Enterprise includes the following options:

- **Premium** service provides technical support excellence through fast track access to the Advanced Services team. It also includes training and certification, a customized account plan, and proactive after-hours support.

- **Business** service includes a designated engineer who will become familiar with your environment and assist in regular ticket reviews. This level also includes bi-annual and root-cause analysis reporting, as well as Advanced Service Points which may be used to select the most appropriate service for your operational requirements.

- **First** service provides a technical account manager (TAM), who collaborates with you to build and maintain a long-term technical engagement, providing technical support, operational reviews, and quarterly reporting. The service also includes best practice guidance, upgrade assistance, extended software support to facilitate upgrade planning, and advanced notifications.

- **Global First** service provides larger geographical coverage by including a designated lead engineer per major region.

- The **Advanced Services Coordinator** acts as the single point of contact for Fortinet services, facilitating your overall service delivery and ensuring timely responses through a focused communication channel.

Advanced Services for Service Providers

FortiCare Advanced Services for Service Providers delivers integrated support to sustain and optimize Fortinet appliances for communications and managed security providers. Incident resolution is enhanced by engagement with the Advanced Services team, experts in security technologies deployed in typical service provider environments. This scalable service has two levels that provide a comprehensive set of services to help customers achieve their IT business continuity objectives:

- **Select** service delivers support excellence through fast-track access to technical experts. It also includes training and certification, a customized account plan, and a designated service delivery manager (SDM) who will build business-level relationships, driving the established objectives, as well as measuring and reporting on service quality.

- **Elite** service includes a designated lead engineer, who collaborates with you to build and maintain a long-term technical engagement using customer knowledge to enhance service delivery. The lead engineer will provide best practice guidance, upgrade assistance to facilitate upgrade planning, and advanced notifications of critical incidents. The SDM will assure service delivery and act as the voice of the customer within Fortinet support and service teams.

Professional Services

Fortinet's comprehensive product portfolio enables secure mission-critical environments. Our Professional Services organization has services to provide technical consulting on Fortinet solutions. The team has expertise with Fortinet and other vendor platforms, as well as industry network and security standards knowledge.

Professional Services for Security Products

Service Design & Transition Phase

- **Network Design & Integration:** Optimizes the integration of the Fortinet solution and advises on proposed design solutions.
- **Design & Configuration Review:** Provides a review of design documentation and accompanying configuration files.
- **Design & Configuration Validation:** Concentrates on the verification of the business-centric aspects of the customer environment and includes implementation of customer-specific test plans.
- **Firewall Migration & Replacement Campaign:** Provides "production-to-production" project support for customers migrating from a third-party vendor.
- **Software Upgrade & Platform Migration Campaign:** Assures a software upgrade or hardware migration.
- **Product Workshops:** Provide tailored training on a design solution created by Fortinet Professional Services.
- **Technical Design Authority & Implementation**: Provides a design lead throughout the project to ensure any issues that may arise are taken care of.

Service Operation Phase

Service Operation includes the following service offerings:

- **FortiGate Health Check**: Measures operational performance of the firewall in the customer's production environment and provides a firewall review to identify issues and provide configuration-tuning recommendations.
- **Security Hardening**: Provides up-to-date platform and version-specific hardening advice.
- **Compliance Audit Preparation**: Gives guidance on audit and compliance processes, including advice on the correct and optimal configuration of the deployed Fortinet solution.
- **Configuration Verification**: Recalibrates, restructures, or redesigns the customer's solution so that it is optimally deployed to meet current demands.
- **Lab Testing & Validation**: Gives assistance in performing functional testing as well as making planned network change (e.g., configuration change, upgrades, etc.) outcomes predictable and measurable.
- **Dedicated Resource Service**: Provides operational technical assistance by a Fortinet certified engineer. This service is available either remotely or on-site.

Security Analysis Services

With the increased frequency, volume, and impact of security attacks, such as Distributed Denial of Service (DDoS), more and more enterprises are deploying Fortinet products as essential elements of a complete security strategy.

The FortiCare Security Analysis Service, available for the **FortiDDoS** and **FortiWeb** product families, maximizes your investment by optimizing the configuration of your appliances for your specific security environment. Fortinet security experts analyze your infrastructure and security requirements to give your team a more in-depth understanding of the technology, resulting in the optimal configuration for your environment.

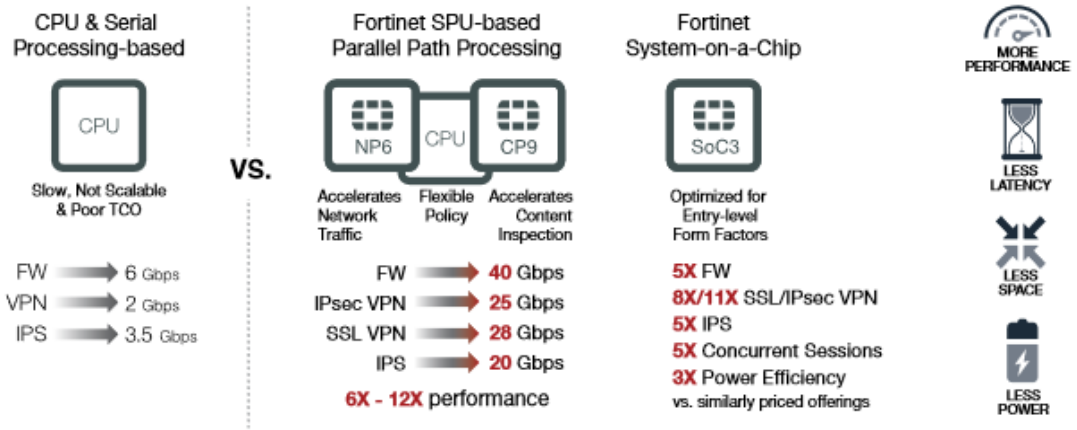
4.3 FortiOS Advantage

The Fortinet Security Fabric is an intelligent framework connecting your security devices together for effective, efficient, and comprehensive security. FortiOS enables the Security Fabric, letting you control the security and networking capabilities in all your Fortinet Security Fabric elements with one intuitive operating system.

Networking	Security	Integration	Management
Firewall	Intrusion Prevention	Email	NOC/SOC/Policy
VPN	Application Control	WAF	Reporting & Compliance
Routing	Anti-malware	Endpoint	Topology Views
Switching	Anti-botnet	Sandboxing	Management
SD-WAN	Web Filtering	Vulnerability	Analytics
Wi-Fi Controller	Mobile Security	Partner APIs	VDOM/ADOM
More...	More...		More...

4.4 The Security Processor Advantage

Fortinet Security Processors radically increase the security performance, scalability, and throughput of Fortinet solutions while greatly shrinking space and power requirements compared to CPU-based solutions.



5. FORTINET SECURITY SOLUTION OVERVIEW

5.1 Security for Enterprises and Mid-Sized Organizations

Enterprise networks are evolving rapidly and adopting new technologies to meet business demands, but this also opens the door to cyber attacks. An integrated, collaborative security approach is required to close the security gaps and share intelligence for automatic, fast response to threats.

All Fortinet solutions work together in the Fortinet Security Fabric for easy management, full visibility, shared intelligence, and automatic remediation.

5.1.1 The Fortinet Enterprise Firewall Solution

Under constant attack, organizations cannot afford to choose between security and maintaining a high-performance business infrastructure. Your extended enterprise needs proven security that won't compromise performance: from deep within internal segments, to physical and virtual data centers, to dynamic cloud environments.

Deploying network security solutions from multiple vendors causes unnecessary complexity and introduces security gaps. Our Enterprise Firewall Solution delivers industry-leading security effectiveness with unmatched performance capabilities—through one operating system managed within a single pane of glass.

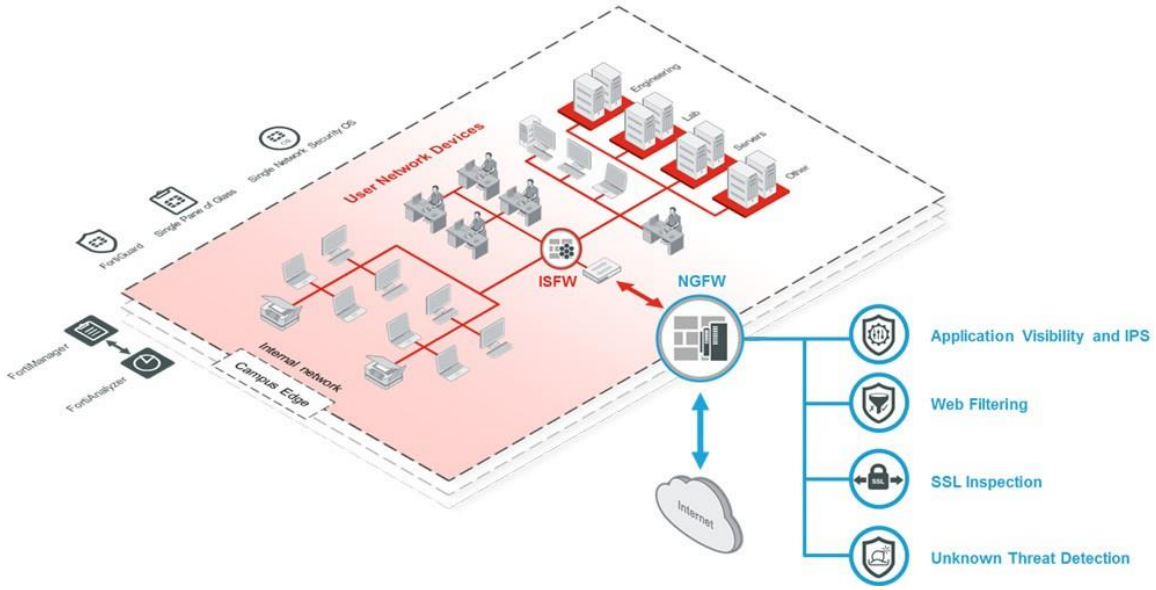
This consolidated architecture gives you an immediate responsive and intelligent defense against malware and emerging threats with an integrated security fabric that extends across your borderless network.

Fortinet Next-Generation Firewall (NGFW) Solution

Effective protection is an absolute necessity in today’s rapidly growing threat environment, as is having a fast, reliable network. You can't afford to choose between comprehensive security and network performance, and with Fortinet solutions, you don't have to.

The FortiGate next-generation firewall is a high-performance network security appliance that adds intrusion prevention, application and user visibility, SSL inspection, and unknown threat detection to the traditional firewall. Our NGFW appliance protects the edge of the campus and internal segments using the high performance of the FortiGate family with the security intelligence of FortiGuard Labs to:

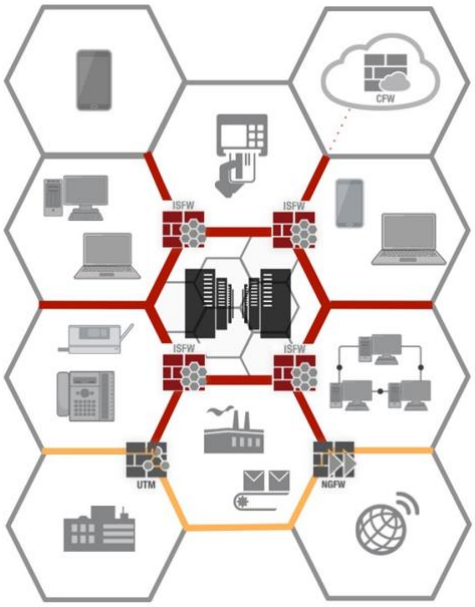
- Enforce security policies with granular control and visibility of users and devices for thousands of discrete applications
- Identify and stop threats with powerful intrusion prevention beyond port and protocol that examines the actual content of your network traffic
- Perform high-performance SSL inspection using industry-mandated ciphers
- Proactively detect malicious unknown code using our cloud-based sandbox service
- Provide you with real-time views into network activity with actionable application and risk dashboards and reports
- Deliver superior, multi-function performance by running on purpose-built appliances with custom security processors



Fortinet Internal Segmentation Firewall (ISFW) Solution

With advanced threats growing rapidly in number and sophistication, perimeter security is no longer enough to keep your sensitive information safe. Once a threat gains entry, it can spread and eventually extract the valuable assets it was sent to retrieve.

You can dramatically improve your security by adding FortiGate Internal Network Segmentation Firewalls to your network to prevent the proliferation of threats once they get inside. ISFWs provide network segmentation inside the perimeter. They may sit in front of specific servers that contain valuable intellectual property or a set of user devices or web applications sitting in the cloud.



Fortinet Data Center Firewall and IPS Solution

The enterprise data center is evolving rapidly, incorporating technologies such as virtualization, software-defined networking, and public cloud computing, along with advanced cyber security. Trying to apply traditional security solutions to these sorts of new technologies generally will not be effective. Enterprises need to evaluate their data center initiatives and how they will impact network security to ensure all areas of the data center remain protected.

In today's dynamic and complex data centers, security must be flexible, effective, and easy to manage. It needs to bring order to the chaos—not add to it. Fortinet can protect your physical, virtual, and cloud servers with one solution—whether it's for data center, private cloud, or public cloud deployments.

Fortinet SD-WAN Solution

Today's distributed enterprises typically spend a lot of time and resources on overly complicated security deployments that may not even be effective. As bandwidth requirements continue to increase at an alarming rate, many organizations are moving from MPLS to the Internet to increase bandwidth and reduce costs. In addition, groups within enterprises are directly accessing cloud applications. Both of these trends raise serious security concerns.

It doesn't have to be complicated to deploy and manage the right security in all the right places. The FortiGate Enterprise Firewall and Hybrid Virtual Appliance enable software-defined WAN (SD-WAN). It links network and security paths across the world through the Internet, 3G/4G, or private WAN links, making it a truly borderless infrastructure for the enterprise. It provides application visibility for encrypted traffic and smart load balancing which help to reduce WAN costs without impacting the SLA for business applications. With our new dynamic cloud application list, customers can easily migrate to SaaS applications and get the most optimized and secured path.

Multiple security features are commonly applied including: IPsec VPN, IPS, web filtering, and the industry's highest SSL inspection performance based on our purpose-built security processors. All of these features are managed via our orchestrator and centralized manager which enable zero-touch deployment and simplified administration.

5.1.2 Fortinet ATP (Includes Sandboxing)

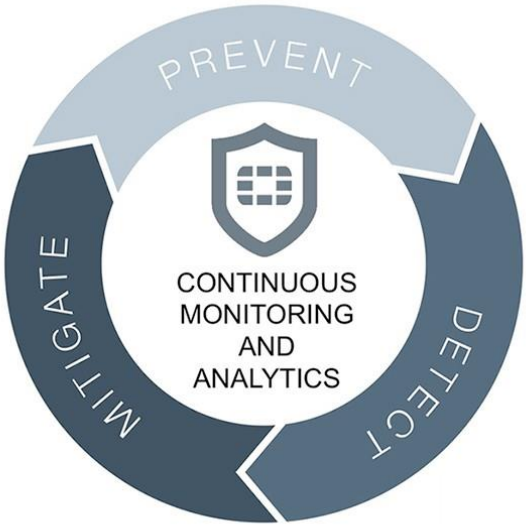
Today's threats are more sophisticated and successful than ever. According to our Fortinet Threat Landscape Report, on average, organizations were compromised by more than six active bots communicating back to their command and control infrastructures. Based on botnet activity, it was found 36% of organizations exhibited ransomware activity, so it should come as no surprise that an estimated $850M was paid in ransoms in 2016.

Of course, that implies that the other 64% of organizations that exhibited botnet activity were impacted by other malware—highlighting the importance of stronger measures to deal with the volume and sophistication of today's threat landscape.

With a dynamic attack surface due to the rise of IoT and cloud services, it's clear that no single technology will be able to stop every threat. To protect your enterprise against sophisticated threats, it is important to establish a comprehensive and cohesive security

infrastructure that is broad enough to cover all attack vectors, powerful enough to run the latest security technologies, and automated to keep pace with fast-moving attacks.

This is exactly what Fortinet Advanced Threat Protection delivers with its integrated, top-rated components spanning prevention, detection, and mitigation:



Prevent: Act on known threats and information

The most efficient way to protect your organization is to immediately block a variety of known threats without impacting network performance at the network, application layer, or endpoint. This is typically accomplished with next-generation firewalls, secure email gateways, web application firewalls, and endpoint security clients to stop malware, intrusions, botnets, etc.

Detect: Identify previously unknown threats

Zero-day attacks and sophisticated threats are often engineered to evade traditional security solutions. Advanced threat detection technologies must be added to automatically detect previously unknown threats and create actionable threat intelligence. Sandboxing in particular, tests unknown items in a secure, instrumented environment to see how they behave, in order to turn the unknown into the known. Extending prevention across all layers with this deeper inspection is critical to getting ahead of the more sophisticated threats.

Mitigate: Respond to potential incidents

Once a new threat is identified, it needs to be immediately mitigated. This can be handled automatically using direct intelligence sharing between detection and prevention products, or with assisted mitigation: a combination of people and technology working together.

Further, protections from previously unknown threats can be put into place across all the layers to complete the cycle and improve the organization’s security posture in advance of future attacks.

Not only are all Fortinet Advanced Threat Protection components powered by the leading security intelligence of FortiGuard Labs, they also leverage local intelligence dynamically generated by FortiSandbox and shared across the interconnected security infrastructure. This sharing automatically responds to the latest targeted attacks, continually improves an organization's security posture, closes natural gaps between multi-vendor point products, and reduces the time spent managing IT security.

5.1.3 Fortinet Data Center Security Solution

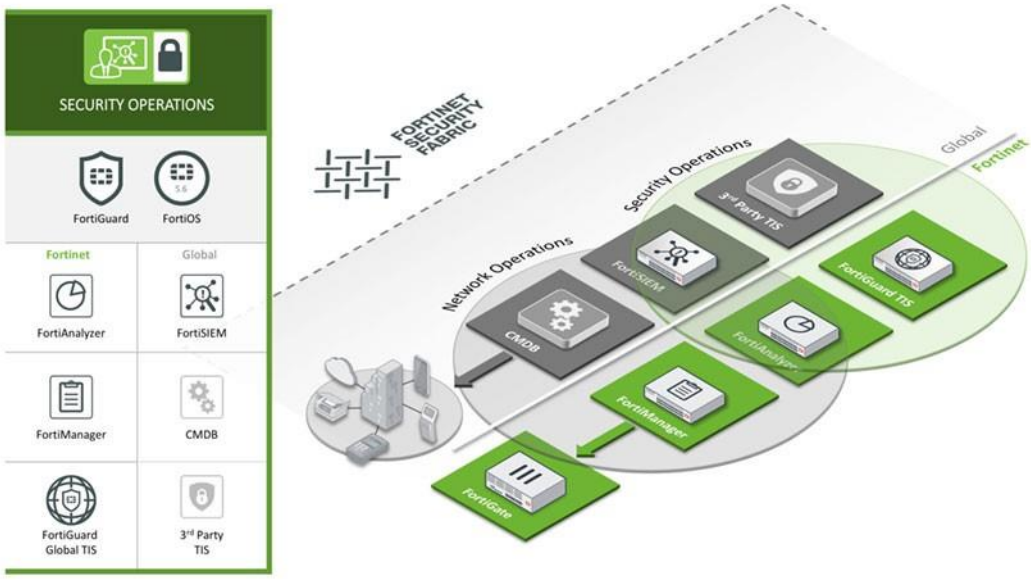
The enterprise data center is evolving rapidly with technologies such as virtualization, software-defined networking, and public cloud computing. Trying to apply traditional security to new technologies generally will not be effective. Enterprises need to evaluate their data center initiatives and how they will impact network security to ensure all areas of the data center remain protected.

Today's data centers are dynamic and complex. Security solutions need to be flexible, effective, and easy to manage so they bring order to the chaos instead of adding to it. Fortinet can protect your physical, virtual, and cloud servers with one solution—whether data center, private cloud, or public cloud deployments.

5.1.4 Fortinet Security Operations Solution

The increase in frequency and sophistication of cyber attacks has taken a toll on security, compliance, performance, and availability. The number of organizations that have suffered a breach is growing rapidly and will continue to increase if organizations are not able to discover threats and respond to them more quickly.

Enterprise networks are seeing an evolution of their network environments, going from centralized control to distributed networks with the advent of mobility, and now becoming borderless with the rapid adoption of virtual and cloud solutions. To monitor risks, enterprises have both a network operations center (NOC) and a security operations center (SOC), but they don't correlate or integrate the information they collect. But if a SOC and a NOC could share information, they'd be able to discover threats and initiate remediation much faster.



Our Security Operations solution covers both IT and security risk management across the entire enterprise, including pre-existing and future infrastructure. While Fortinet security products are already unified into a Security Fabric with a single OS and shared intelligence, the Security Operations solution includes information from network elements beyond the Fortinet devices. It breaks down the barrier between NOC and SOC, giving you a comprehensive view of your entire network so you can quickly find and respond to threats. It also helps manage and monitor compliance, increase application availability, and save IT resources.

Fortinet's Security Operations Solution delivers:

- Adaptive awareness of the threat landscape
- Rapid local and global threat detection for rapid response
- Reduced complexity in managing the onslaught of alerts and alarms
- A comprehensive and more holistic approach to managing risk
- Reporting and analytics that enable IT, line of business managers, C-level, and board members to better understand how the organization's risk profiles are being managed.

5.1.5 Fortinet Application Security Solution

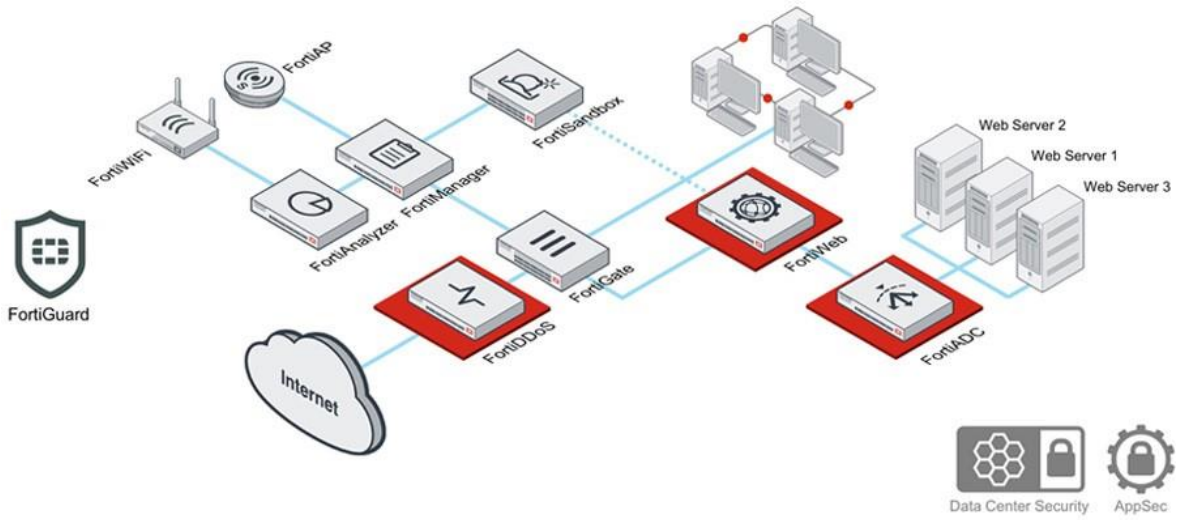
Web applications and email systems have long been favorite targets of hackers because they have access to valuable information and they are relatively easy to exploit. A successful attack can result in a variety of devastating consequences including financial loss, damage to brand reputation, and loss of customer trust. Most organizations do not recover from a major security breach, making it absolutely critical to protect your users and customers from threats that target applications and email systems.

Our Data Center Application Security solution consists of a robust and integrated set of products to protect against these attacks. We are the only company that delivers a complete

single-vendor solution with the proven performance and security effectiveness to meet the increasing demands of today's data centers. In addition, our application security solutions can be integrated with FortiGate next-generation firewalls and FortiSandbox sandbox for extra defenses against advanced persistent threats (APTs).

Fortinet's Data Center Application Security Solution includes:

- Web application protection
- Encryption/decryption
- DDoS attack mitigation



Web application protection

It's impossible to ensure all web applications on your system are free of vulnerabilities at any given time. Whether it's a previously undiscovered vulnerability, a vulnerability waiting to be patched, an out-of-support system, or some other issue, vulnerabilities are there, waiting to be exploited. Fortinet's FortiWeb Web Application Firewalls protect web-based applications from attacks that target vulnerabilities.

Encryption/decryption with ADC

When a secure web application begins to grow, new servers need to be added to handle the user capacity and encryption needs. When you reach this point, new problems arise: something needs to control the additional servers and servers can only handle limited amounts of secure traffic encryption and decryption.

FortiADC's SSL offloading provides class-leading secure traffic encryption and decryption, alleviating this task from the web application servers. FortiADC can provide up to a 20 times increase in secure application traffic capacity versus using only servers.

DDoS attack mitigation

Distributed Denial of Service (DDoS) attacks continue to be the top threat to IT security. DDoS attacks targeting the application layer tend to be small and hard to detect, but a successful attack will still shut down your vital services.

Fortinet's FortiDDoS DDoS Attack Mitigation appliances inspect all inbound and outbound traffic from a data center using 100% hardware and 100% behavior-based detection methods. FortiDDoS blocks all attacks including large bulk-volumetric and small application-layer attacks.

5.1.6 Secure Access Solution

Organizations are changing the way they deploy access networks, connect devices, and enable business applications to address a number of challenges:

- The number and types of network-connected wireless devices and mobile applications continue to grow exponentially, presenting new vulnerabilities and increasing the attack surface.
- Users want fast Wi-Fi and a smooth experience across wired and wireless networks.
- IT needs reduced complexity of network management, application management, and device management.

Securing business communications, personal information, financial transactions, and mobile devices involves much more than network access control. It requires scanning for malware, preventing access to malicious websites, endpoint integrity checking, and controlling application usage. As a result, IT departments are faced with the difficult task of balancing the requirements of network security with the flexibility to onboard the growing number and diversity of clients.

Typical Wi-Fi solutions cannot satisfactorily address these requirements. Only Fortinet's Secure Access solution delivers three WLAN deployment options to meet the different WLAN requirements of today's enterprises. In addition to WLAN services, our secure access portfolio also provides the most flexible security platform with end-to-end enforcement.

Our three offerings: Integrated, Controller, and Cloud enable any organization to choose the topology and network management that best fits its needs, without having to compromise on security.

Integrated Wi-Fi

Our Integrated offering is a family of controller-managed access points that function in cooperation with a FortiGate next-generation firewall. In addition to consolidating all the functions of a network firewall, IPS, anti-malware, VPN, WAN optimization, web filtering, and application control in a single platform, FortiGate also includes an integrated Wi-Fi controller. Fortinet access points are either integrated into the FortiGate (FortiWiFi) or are connected directly to the FortiGate to provide comprehensive wireless coverage.

Controller Wi-Fi

Our Controller offering combines on-premises controller-based management, network applications, and a range of high-performance indoor and outdoor access points. This is the ideal solution when an organization needs a dedicated wireless network that can be separated from the underlying network's security infrastructure. The Controller solution offers flexible channel deployment options to drastically reduce site survey and channel planning work while securing traffic through wireless traffic segmentation. This solution scales for implementations ranging from medium to large enterprises.

Cloud Wi-Fi

Our Cloud solution is unlike any other Cloud Wi-Fi offering. Based on the FortiCloud Provisioning and Management Service and a new class of access points, the FortiAP-S series combines the elements of advanced firewall protection at the network edge with the simplicity and convenience of cloud management.

FortiSwitch

Our Ethernet LAN switches are available in a large range of models to fit any environment.

Ideal for small to medium businesses, distributed enterprises, and branch offices, FortiSwitch secure access switches deliver superior security, performance, and manageability. In addition, they help increase productivity for next-generation applications through faster network access speeds.

6. FORTISWITCH SECURE SWITCHING

FortiSwitch Ethernet Access and Data Center Switches are a feature-rich yet cost-effective range of devices, supporting the needs of enterprise campus and branch offices, as well as data center environments.

The FortiSwitch Secure Access Switch series integrates directly into the FortiGate Connected UTM, with switch administration and access port security managed from the familiar FortiGate interface. Regardless of how users and devices connect to the network, you have complete visibility and control over your network security and access through this single pane of glass, perfectly suited to threat-conscious organizations of any size.

Virtualization and cloud computing have created dense high-bandwidth Ethernet networking requirements in the data center, pushing the limits of existing data center switching. FortiSwitch Data Center switches meet these challenges by providing a high performance 10 or 40 GbE capable switching platform, with a low Total Cost of Ownership. Ideal for Top of Rack server or firewall aggregation applications, as well as enterprise network core or distribution deployments, these switches are purpose-built to meet needs of today's bandwidth intensive environments.

Integrated Security	Pervasive Security through Fortinet Security Fabric Integration addressing the broadest threat surface.
Simplified Management	FortiGate integration creates one interface to manage security and access.
Scalable	Able to scale from desktop to datacenter across platforms allowing flexibility to grow as devices and traffic increase.

Highlights

Wide Range of Models – With 1 GbE, 10 GbE and 40 GbE models, as well as Power over Ethernet options, there is a FortiSwitch to suit any deployment scenario.

Power over Ethernet (PoE) – Simplifies the installation of PoE equipment in the network, eliminating the need for the installation of additional power sockets to support APs and VOIP handsets.

Flexible management – Various management capabilities are available including CLI, Web or directly from a connected FortiGate GUI.

Network Segmentation Support – You can configure a single physical switch to support the convergence of voice, data and wireless traffic, while still meeting compliance requirements.

40GbE Capability – Future proofed 40 GbE will meet the bandwidth requirements of even the most intensive data center and network core applications.

Port Level Network Access Security Features – Secure Access Switch Series devices enable true port level network access security with 802.1X technology, managed centrally from any FortiGate.

Offering Limited Lifetime Warranty (hardware replacement) - Refer to policy at Fortinet Warranty Policy: http://www.fortinet.com/doc/legal/EULA.pdf

Security Fabric – FortiSwitch devices are essential part of Fortinet's Security Fabric, offering visibility, user access control, and threat mitigation at the switch port level.

6.1 Secure Access Switches – Simple, Secure, Scalable Unified Access Layer Ethernet Switches

Outstanding network security, performance, and manageability

Single-pane-of-glass management through tight integration with the industry leading FortiGate using FortiLink

FortiSwitch Secure Access switches deliver a Secure, Simple, Scalable Ethernet solution with outstanding security, performance and manageability for threat conscious small to mid-sized businesses, distributed enterprises and branch offices. Tightly integrated into the FortiGate® Network Security Platform, the FortiSwitch Secure Access switches can be managed directly from the familiar FortiGate interface. This single pane of glass management provides complete visibility and control of all users and devices on the network, regardless of how they connect.

When a device connects to a Secure Access Switch Ethernet port, it is first identified, and then the user is authenticated. Once authenticated, access to the network is granted based on pre-defined security policy from the FortiGate, ensuring secure network access across the enterprise, without impacting the user experience. If any attacks sent by the user is detected by FortiGate, the user can be quarantined on FortiSwitch to stop it from spreading malicious traffic to other hosts in the network.

Security Fabric Integration

Reduces complexity and decreases management cost with network security functions managed through a single console via FortiGate.

This integration allows all users to be authenticated against the same user database, regardless of whether they connect to the wired or wireless network, including temporary guest users.

In addition, same security policy can apply to a user or device regardless of how or where they connect to the network.

Models: FS-108D-POE, FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124D, FS-124D-POE, FS-224E, FS-224E-POE, FS-224D-FPOE, FS-248E, FS-248E-POE, FS-248E-FPOE, FS-424D, FS-424D-POE, FS-424D-FPOE, FS-448D, FS-448D-POE, FS-448D-FPOE, FS-524D, FS-524D-FPOE, FS-548D and FS-548D-FPOE.

Highlights

- Secure Access switches suitable for wire closet and desktop installations.
- Devices are identified and users authenticated prior to being granted access to the network.
- Security Fabric integration with actions taken on switch port level (user quarantine, Access VLAN, etc).
- Stackable up to 256 switches per FortiGate depending on model
- Centralized security management and reporting from FortiGate interface.
- Up to 48 ports in a compact 1 RU form factor.
- Power over Ethernet capable, including PoE+
- Ideal for converged network environments; enabling voice, data and wireless traffic to be delivered across a single network

Key Features & Benefits

Single Management Framework: Reduces complexity and decreases management cost with network security functions managed through a single console.

Single Policy Provisioning: The same security policy can apply to a user or device regardless of how or where they connect to the network. Enables access to certain network ports based on the role of a user within the organization, such as in shared conference rooms or engineering facilities.

Centralized Authentication: All users are authenticated against the same user database, regardless of whether they connect to the wired or wireless network, including temporary guest users.

Role-Based Ports: Enables access to certain network ports based on the role of a user within the organization, such as in shared conference rooms or engineering facilities.

6.1.1 FortiSwitch Rugged

FortiSwitch Rugged switches deliver all of the performance and security of the trusted FortiSwitch Secure, Simple, Scalable Ethernet solution, but with added reinforcement that makes them ideal for deployments in harsh outdoor environments.

Resilient, sturdy and capable of withstanding intense temperature uctuations, FortiSwitch Rugged ensures the integrity and performance of mission-critical networks in even the most challenging of deployments.

Add Ruggedized FortiGate for Tough and Powerful Protection

Engineered to survive in hostile environments with an extreme temperature range, the combination of FortiGate Rugged network security appliances with the FortiSwitch Rugged provides a connected network security solution.

Simple Network Deployment

The Power over Ethernet (PoE) capability enables simple installation of cameras, sensors and wireless access points in the network, with power and data delivered over the same network cable.

There is no need to contract electricians to install power for your PoE devices, reducing your overall network TCO.

Highlights

- Mean time between failure greater than 25 years
- Fanless passive cooling
- DIN-rail or wall-mountable
- Power over Ethernet capable including PoE+
- Redundant power input terminals
- Controlled by FortiGate

Kea Features and Benefits

Sturdy IP30 construction	Built to ingress protection 30 standards, the construction is designed to perform while enduring hostile conditions.
Passive cooling	With no fan and no moving parts, the mean time between failure is greater than 25 years.
Redundant power inputs	Maximizes network availability by eliminating the downtime associated with failure of a power input.
Power over Ethernet capability	Seamless integration of peripheral devices such as cameras, sensors and wireless access points into the network.

Models: FSR-112D-POE, FSR-124D

See datasheet environmental and compliance information.

6.2 Data Center Switches – High Performance Switching with Data Center Capabilities

Outstanding throughput, resiliency, and scalability

Single-pane-of-glass management through tight integration with FortiGate using FortiLink

FortiSwitch Data Center switches deliver a Secure, Simple, Scalable Ethernet solution with outstanding throughput, resiliency and scalability for organizations with high performance network requirements. They are ideal for Top of Rack server or firewall aggregation applications, as well as enterprise network core or edge deployments, where high performance 10 GE or 40 GE is required. Purpose-built to meet the needs of today's bandwidth intensive data centers and enterprise networks, FortiSwitch Data Center switches deliver high-performance with a low Total Cost of Ownership.

Security Fabric Integration

Reduces complexity and decreases management cost with network security functions managed through a single console via FortiGate.

This integration allows all users to be authenticated against the same user database, regardless of whether they connect to the wired or wireless network, including temporary guest users.

In addition, same security policy can apply to a user or device regardless of how or where they connect to the network.

High-performance and resilient managed data center switch

Designed in a compact 1 RU form factor, FortiSwitch Data Center switches are equipped with dual hot swappable power supplies to maximize network uptime. With 10 GE access ports and a high-throughput backplane, the FortiSwitch Data Center switches satisfy the Top of Rack server or firewall aggregation performance requirements of today's virtualization centric data centers. Advanced Link Aggregation with 802.3ad, Link Aggregation Control Protocol (LACP) and Multi-Chassis Link Aggregation Groups (MCLAG) provide increased uplink, server aggregation, or firewall aggregation throughput. Other advanced switch capabilities, such as large MAC address tables, jumbo frame support and port security, are standard features. The high-speed switching fabric is also well suited to enterprise network core or backbone network installations. FortiSwitch Data Center switches are a future-proof investment, providing the flexibility of deploying 1 GE, 10 GE or even 40 GE if required.

Models: FS-1024D, FS-1048D, FS-3032D

Highlights

- High capacity switch suitable for Top of Rack or enterprise network deployments.
- Stackable up to 256 switches per FortiGate depending on model
- Maximum availability through dual hot swappable power supplies.
- Simply management via web-based or command line interface.
- Switch security features protect vulnerable infrastructure without adding latency.
- 1 GE or 10 GE access ports, in a compact 1 RU form factor.
- 40 GE capability options.

Key Features and Benefits

10 GE Capability: Future-proofed 10 GE to satisfy the bandwidth requirements of intensive data center and network core applications.

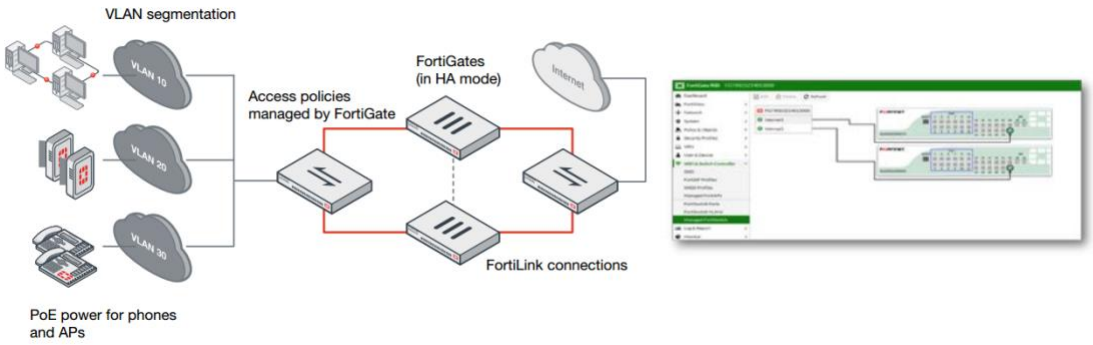
Dual Power Supply Units: Maximizes network availability by eliminating the downtime associated with single power supplies.

FortiLink, Web and CLI Management: Configuration and visibility into the network is made simple via FortiLink, web-based interface or CLI.

6.3 Deployment Options

6.3.1 FortiLink Mode

The FortiSwitch Secure Access Switch series integrates directly into the FortiGate* Connected UTM, with switch administration and access port security managed from the familiar FortiGate interface. Regardless of how users and devices connect to the network, you have complete visibility and control over your network security and access through this single pane of glass, perfectly suited to threat conscious organizations of any size. (* selected models only)



FortiLink Advantages

Feature	Fortilink Advantage
Auto Discovery	FortiGate discovers FortiSwitch without need of additional configuration
Segment Network Centrally	With FortiGate it becomes simple to attach policies to ports
Upgrade Image	FortiGate upgrades FortiSwitchOS
Zero-touch provisioning	FortiGate automatically authorizes and configures FortiSwitch

Security Fabric Integration	Security applied to the switch port – FortiSwitch is simple extension to FortiGate
Wired and Wireless Central Control	FortiGate as central Switch+Wireless controller
POE Management	Control power budget centrally
Centralized Authentication	All users are authenticated against the same user database
Centralized Management	Use FortiManager to centrally manage FGTs and corresponding managed FortiSwitch
Stack	Control up to 256 FortiSwitch from the same FGT GUI

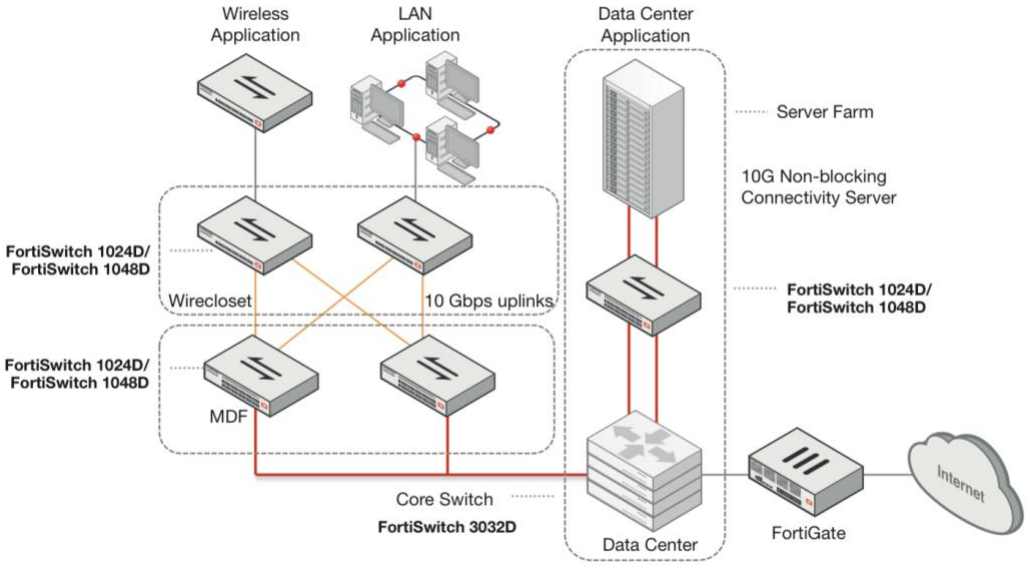
Capabilities: FortiLink Mode

	FORTISWITCH FORTILINK MODE (WITH FORTIGATE)
Management and Configuration	
Auto Discovery of Multiple Switches	Yes
Number of Managed Switches per FortiGate	8 to 256 Depending on FortiGate Model (Please refer to admin-guide)
FortiLink Stacking (Auto Inter-Switch Links)	Yes
Software Upgrade of Switches	Yes
Centralized VLAN Configuration	Yes
Switch POE Control	Yes
Link Aggregation Configuration	Yes
Spanning Tree	Yes
LLDP/MED	Yes
IGMP Snooping	Yes (not supported on 108D-POE, 224D-POE, 1xxE-Series)
L3 Routing and Services	Yes (FortiGate)
Policy-Based Routing	Yes (FortiGate)
Virtual Domain	Yes (FortiGate)
Security and Visibility	
802.1x Authentication (Port-based, MAC-based, MAB)	Yes
Syslog Collection	Yes
DHCP Snooping	Yes
Device Detection	Yes
MAC Black/While Listing	Yes (FortiGate)
Policy Control of Users and Devices	Yes (FortiGate)
UTM Features	
Firewall	Yes (FortiGate)
IPC, AV, Application Control, Botnet	Yes (FortiGate)
High Availability	
Support FortiLink FortiGate in HA Cluster	Yes
LAG support for FortiLink Connection	Yes
Active-Active Split LAG from FortiGate to FortiSwitches for Advanced Redundancy	Yes (with FS-2xx, 4xx, 5xx)

6.3.2 Standalone Mode

Virtualization and cloud computing have created dense high-bandwidth Ethernet networking requirements in the data center, pushing the limits of existing data center switching. FortiSwitch Data Center switches meet these challenges by providing a high performance 10 or 40 GE capable switching platform, with a low Total Cost of Ownership. Ideal for Top of

Rack server or firewall aggregation applications, as well as enterprise network core or distribution deployments, these switches are purpose-built to meet the needs of today's bandwidth intensive environments.

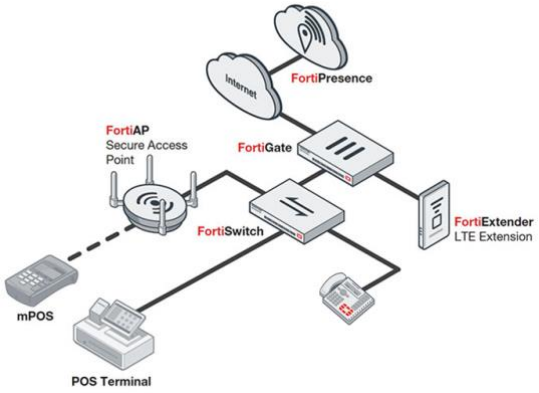


6.5 Solution Integration

Retail

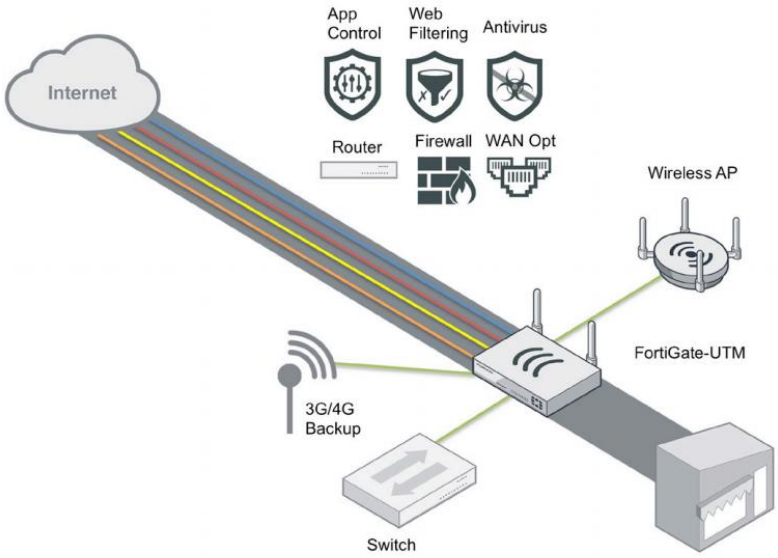
FortiSwitch integrates with Fortinet's complete solution for retail business. Benefits:

- Cost reduction
- Standardization
- Easy deployment in high scale
- Visibility
- Easily adapt to new retail tech



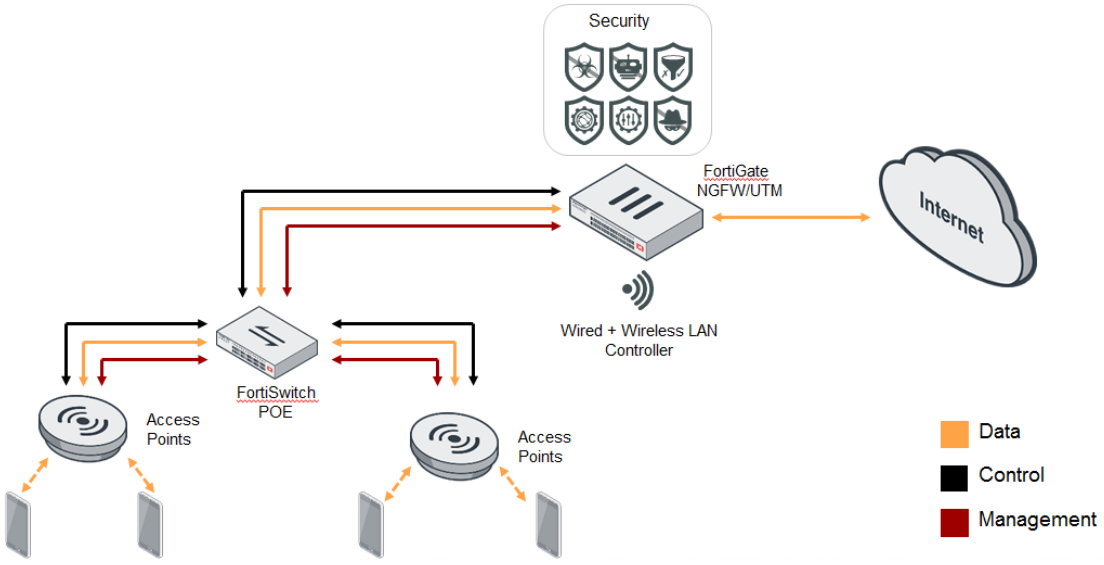
Connected UTM

FortiSwitch integrates with Connected UTM solution providing extended connectivity and POE for SMB deployments. With FortiLink, FortiSwitch becomes an extension to FortiGate and it's possible to easily enforce policies for all of the different wired and wireless devices, kiosks, systems, and terminals in the network from a "single pane of glass".



Secure Access Architecture

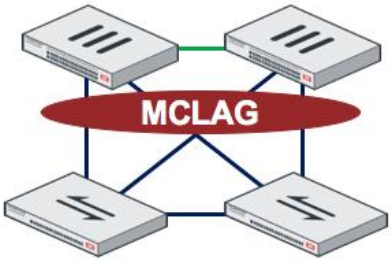
FortiSwitch integrates with Secure Access Architecture solution providing network infrastructure necessary to interconnect wired and wireless. It also provides POE to power wireless access points and other devices in the network. The complete network can be controlled via FortiGate in a “single pane of glass”.



FortiGate in HA

With the use of MCLAG, FortiGate HA pair can be connected in full mesh to FortiSwitch pair, providing complete link and switch level redundancy to the security solution.

Supported in FortiLink or Standalone mode.



7. FORTISWITCH COMMON REQUIREMENT SPECIFICATIONS AND ANSWERS

Use the following list to help answering RFP questions and, when possible, to tailor RFPs to Fortinet's favor. For supported models, check feature matrix in release notes. For physical/environmental specifications, refer to datasheets. For any unsupported feature, consult your regional SME/CSE.

7.1. General system requirements

Requirement	FortiLink	Standalone	Response
MUST support simple management access i.e. without the need for local management clients (HTTPS preferred)	**Yes**	**Yes**	**Fully Compliant:** FortiSwitch has a CLI however this is for initial setup and includes some debugging commands for convenience. All configuration and management of the platform is web based using standard browsers.
MUST support SNMP for polling of system statistics	**Yes**	**Yes**	**Fully Compliant:** FortiSwitch supports SNMP v1, v2c and v3. FortiSwitch MIBS are available for download from the Fortinet Technical Support web site.
MUST support SNMP Traps for key system thresholds (specify)	**Yes**	**Yes**	**Fully Compliant:** FortiSwitch supports configurable SNMP TRAPS for key system thresholds.
MUST support SNMP MIB download from system GUI	**Yes**	**Yes**	**Fully Compliant:** FortiSwitch MIBs are available in the GUI.
MUST display a visual representation of authentication in the GUI	**Yes**	**Yes**	**Fully Compliant:** FortiSwitch includes a "Logout" button showing that user is logged in the system and offering the option to logout.
MUST log all authentication events:			

Locally	**Yes**	**Yes**	**Fully Compliant:** All authentication attempts are logged to the local file system under Event logs with the sub-type "admin" with details of the authenticating system, username, disposition (success, failed) and details of any failure. Local logs can be stored up to maximum file size specified by the administrator, at which point the file overwritten or logging stops.
Via syslog	**Yes**	**Yes**	**Fully Compliant:** Logs can be automatically replicated out to multiple external SYSLOG in their entirety or selectively based on the SYSLOG level and facility. Logs are automatically exported to FortiGate in FortiLink mode.
MUST be simple to install, manage and upgrade	**Yes**	**Yes**	**Fully Compliant:** FortiSwitch is delivered in a fully self-contained appliance format consisting of a hardened OS and all preconfigured applications. FortiSwitch requires simple initial CLI configuration. Following installation, all configuration is performed via a simple web based GUI. All upgrades to the OS and application are performed via the upload of a firmware package available from the Fortinet Support Web Site. The file is simply downloaded to the desktop and uploaded to the appliance.
MUST support backup of the full system configuration via the GUI	**Yes,** as part of FortiGate config	**Yes**	**Fully Compliant:** Configuration can be backed up via the GUI.
MUST support a local user database	**Yes,** from FortiGate No need to login to the FSW	**Yes**	**Fully Compliant:** FortiSwitch allows configuration of multiple administrator accounts and corresponding access profiles to restrict permissions per configuration sub-system.
MUST support remote authentication users (LDAP, RADIUS and/or TACACS+)	**No**	**Yes**	**Fully Compliant:** FortiSwitch allows the configuration to remote authenticate users' logins. For full details on parameters please refer to the FortiSwitchOS admin guide.
MUST have built-in tcpdump-like tool and log collecting functionality	**Yes**	**Yes**	**Fully Compliant:** Packet Capture and diagnose features in CLI offer similar packet capture capabilities like tcpdump.

MUST support REST API for configuration and monitoring	**Yes**	**Yes**	**Fully Compliant:** Based on JSON API.
MUST support multiple configuration files with 2 bootable partitions for better availability and easy upgrade / fallback.	**Yes**	**Yes**	**Fully Compliant:** Configuration backup/restore and alternate boot partition
MUST support dual power supply	**Yes**	**Yes**	**Available on:** FS-424D, FS-448D, FS-448D-FPOE, FS-5xx, FS-10xxD, FS-3032D
MUST support external RPS	**Yes**	**Yes**	**Available on:** FS-124D-POE, FS-224D-FPOE, FS-248D-FPOE, FS-424D-POE, FS-424D-FPOE, FS-448D-POE, FS-224E-POE, FS-248E-POE, FS-248E-FPOE
MUST support breakout cables (40G to 4x10G)	**No**	**Yes**	**FS-5xx and FS-3xxx models**
MUST offer hardware lifetime warranty	**Yes**	**Yes**	
MUST support auto-ranging power supply with input voltages between 100 and 240V AC	**Yes**	**Yes**	
MUST support 802.3ah (100BASE-X single/multimode fiber only)	**Yes**	**Yes**	Supported on 108D-POE/112D-POE/224D-POE
MUST support 802.3az for energy efficient Ethernet	**No**	**No**	

7.2. Layer 2 Requirements

Requirement	FortiLink	Standalone	Response
MUST support jumbo frames	**Yes**	**Yes**	Max frame size = 9216
MUST support link auto-negotiation	**Yes**	**Yes**	**Fully Compliant:** 10G ports work also at 10/100/1000 speeds
MUST support manual link negotiation	**Yes, CLI**	**Yes**	**Fully Compliant**
MUST support Spanning Tree Protocol	**Yes**	**Yes**	**Fully Compliant:** MSTP (802.1s) native, and backwards compatible with RTSP (802.1w) and STP (802.1d)
MUST support Edge Port / Port Fast	**Yes**	**Yes**	
MUST support STP Root Guard	**Yes**	**Yes**	
MUST support BPDU Guard	**Yes**	**Yes**	
MUST support IEEE 802.1p Mapping to priority queue	**Yes**	**Yes**	

MUST support IEEE 802.1q VLAN tagging	**Yes**	**Yes**	
MUST support 4096 VLANs	**Yes**	**Yes**	
MUST support Private VLAN	**Yes**	**Yes**	Except on FS-108D-POE and FS-224D-POE In FortiLink mode, Access VLAN
MUST support IEEE 802.3ad Link Aggregation with LACP	**Yes**	**Yes**	**Fully Compliant:** maximum number of link members depends on model
MUST support load balancing algorithms with Link Aggregation	**Yes**	**Yes**	**Fully Compliant:** dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac
MUST support MCLAG (MultiChassis Link Aggregation)	**Yes**	**Yes**	**FOS 5.6.0** **FSWOS 3.6.0** Not supported on FS-1xx models
MUST support Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors	**Yes**	**No**	Supported if managed by FGT, all ISLs are automatically provisioned
MUST support MVR (Multicast VLAN Registration)	**No**	**No**	
MUST support load balancing algorithms with Link Aggregation	**Yes**	**Yes**	**Fully Compliant:** dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac
MUST support virtual wire	**Yes, CLI only**	**Yes**	
MUST support full line rate without traffic oversubscription	**Yes**	**Yes**	**Available on all models:** non-blocking, store-n-forward architecture
MUST support low latency mode (cut-through)	**No**	**Yes**	**Available on models:** FS-10xxD and FS-3032D
MUST support Ethernet protection mechanisms (IEEE 802.3ah or ITU-G.8031/8032)	**No**	**No**	**Check with CSE/PM for potential feasibility**
MUST support Shortest Path Bridging (SPB IEEE 802.1aq)	**No**	**No**	**Check with CSE/PM for potential feasibility**
MUST support Unidirectional Link Detection (UDLD)	**No**	**No**	**Cisco proprietary** **Use stp-loop-protection instead** **Or single member LAG with LACP** **Or Ethernet OAM (802.3ah) (roadmap)**
MUST support DCB (802.1Qbb and 802.1Qaz)	**No**	**No**	

7.3. Management requirements

Requirement	FortiLink	Standalone	Response
MUST support zero-touch provisioning	**Yes**	**No**	**Auto-discovery of switches**
MUST support stacking	**Yes**	**No**	FortiGate is the stack controller, with single pane of glass.
MUST support stacking topology auto-discovery	**Yes**	**No**	
MUST support firmware update from a central point	**Yes**	**No**	
MUST support end device identification	**Yes**	**No**	
MUST support integration with Fortinet Security Fabric	**Yes**	**No**	
MUST support complete view of all switching solution from a single pane of glass	**Yes**	**No**	
MUST support 802.1x MAC-based authentication	**Yes**	**Yes**	
MUST support MAC Authentication Bypass (MAB)	**Yes**	**Yes**	
MUST support Time-Domain Reflectometry (TDR) Support	**No**	**Yes**	Except FS-108D-POE, FS-224D-POE
MUST support telnet/SSH	**Yes**	**Yes**	
MUST support SNTP	**Yes**	**Yes**	
MUST support firmware download via TFTP/FTP/GUI	**Yes**	**Yes**	
MUST support RMON I and II standards	**No**	**No**	
MUST support Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically	**Yes**	**No**	
MUST support MAC address notification	**No**	**No**	
MUST support Bridge MIB (RFC-1493)	**Yes**	**Yes**	
MUST support POE MIB (RFC 3621)	**No**	**No**	

7.4. Authentication Requirements

Requirement	FortiLink	Standalone	Response
MUST support LLDP	**Yes**	**Yes**	

MUST support LLDP-MED	**Yes**	**Yes**	MED-TLVs: inventory and network policy
MUST support MAC based VLAN assignment (802.1v)	**Yes, CLI only**	**Yes**	
MUST support IP based VLAN assignment (802.1v)	**Yes, CLI only**	**Yes**	
MUST support protocol based VLAN assignment (802.1v)	**Yes, CLI only**	**Yes**	
MUST support 802.1x port-based authentication	**Yes**	**Yes**	
MUST support 802.1x authentication via certificate EAP-TLS and EAP-TTLS	**Yes**	**Yes**	
MUST support 802.1x guest VLAN assignment	**Yes**	**Yes**	
MUST support 802.1x authentication fail VLAN for unauthenticated users	**Yes**	**Yes**	
MUST support 802.1x MAC-based authentication	**Yes**	**Yes**	
MUST support MAC Authentication Bypass (MAB)	**Yes**	**Yes**	
MUST support captive portal	**Yes**	**No**	
MUST support LDAP	**No**	**Yes**	
MUST support RADIUS	**Yes**	**Yes**	
MUST support RADIUS Accounting	**Yes, CLI only**	**Yes**	
MUST support RADIUS Change of Authorization (CoA)	**No**	**Yes**	
MUST support TACACS+	**No**	**Yes**	

7.5. POE Requirements

Requirement	FortiLink	Standalone	Response
MUST display total POE power consumption	**Yes**	**Yes**	
MUST display per port POE power consumption	**Yes**	**Yes**	
MUST support POE port enable/disable	**Yes**	**Yes**	
MUST support POE port reset	**Yes**	**Yes**	
MUST support IEEE 802.3af	**Yes**	**Yes**	

MUST support IEEE 802.3at (POE+)	**Yes**	**Yes**	All “-POE” and “-FPOE” models except FS-108D-POE and FS-224D-POE

7.6. Layer 3 Requirements

Requirement	FortiLink	Standalone	Response
MUST support static routing	**Yes, via FortiGate**	**Yes**	
MUST support line rate L3 forwarding	**Yes, via FortiGate**	**Yes**	Refer to release notes for supported models
MUST support RIPv2	**Yes, via FortiGate**	**Yes**	Requires Advanced license. Not supported on FS-1xx models.
MUST support OSPFv2	**Yes, via FortiGate**	**Yes**	Requires Advanced license. Not supported on FS-1xx models.
MUST support BGP	**Yes, via FortiGate**	**Roadmap**	
MUST support VRRP	**Yes, via FortiGate**	**Yes**	Requires Advanced license. Not supported on FS-1xx models.
MUST support IGMP	**Yes, via FortiGate**	**Roadmap**	
MUST support PIM	**Yes, via FortiGate**	**Roadmap**	
MUST support ECMP	**Yes, via FortiGate**	**Yes**	
MUST support BFD	**No**	**Yes**	
MUST support GRE	**No**	**No**	
MUST support L2TP	**No**	**No**	
MUST support MPLS, MPLS-TP	**No**	**No**	
MUST support ISIS	**No**	**Roadmap**	

7.7. Security

Requirement	FortiLink	Standalone	Response
MUST support Storm Control	**Yes, CLI only**	**Yes**	
MUST support LoopGuard	**Yes**	**Yes**	
MUST support IGMP snooping	**Yes**	**Yes**	
MUST support IGMP querier	**Yes**	**Yes**	
MUST support DHCP snooping	**Yes**	**Yes***	
MUST support DHCP relay	**Yes, via FortiGate**	**Yes**	Includes option 82

MUST support DHCP server	**Yes, via FortiGate**	**No**	
MUST support Port mirroring	**Yes, CLI only**	**Yes**	
MUST support sFlow	**Yes, CLI only**	**Yes**	
MUST support ACL	**Yes, CLI only**	**Yes**	
MUST support ACL classifier	**Yes, CLI only**	**Yes**	**Fully Compliant:** src-mac, dst-mac, ether-type, src-prefix, dst-prefix, service-id, vlan-id
MUST support ACL drop action	**Yes, CLI only**	**Yes**	
MUST support ACL policer action	**Yes, CLI only**	**Yes**	
MUST support ACL counter action	**Yes, CLI only**	**Yes**	
MUST support ACL mirror action	**Yes, CLI only**	**Yes**	
MUST support ACL redirect action	**Yes, CLI only**	**Yes**	
MUST support security checks	**Yes, CLI only**	**Yes**	sip-eq-dip - TCP packet with Source IP equal to Destination IP. tcp_flag - DoS attack checking for TCP flags. tcp-port-eq TCP packet with Source and destination TCP port equal tcp-flag-FUP - TCP packet with FIN, URG and PSH flags set, and sequence number is zero. tcp-flag-SF - TCP packet with SYN and FIN flag set. v4-first-frag - DoS attack checking for IPv4 first fragment. udp-port-eq - IP packet with source and destination UDP port equal. tcp-hdr-partial - TCP packet with partial header. macsa-eq-macda - Packet with source MAC equal to Destination MAC.
MUST support port MAC limit	**Yes, CLI only**	**Yes**	
MUST support MAC-IP binding	**Yes**	**Yes**	Map a MAC address to an IP address to avoid untrusted hosts
MUST support static MAC	**Yes**	**Yes**	Map a MAC address to a port to avoid flooding
MUST support Dynamic ARP Inspection	**Yes, CLI only**	**Yes**	

MUST support Sticky Mac	**Yes, CLI only**	**Yes**	

7.8. QoS

Requirement	FortiLink	Standalone	Response
MUST support 8 queues per port	**Yes**	**Yes**	
MUST support packet classification	**Yes**	**Yes**	
MUST support packet marking	**Yes**	**Yes**	
MUST support packet queuing	**Yes**	**Yes**	
MUST support 802.1p	**Yes**	**Yes**	
MUST support TOS/DSCP	**Yes**	**Yes**	
MUST support strict scheduling mode	**Yes**	**Yes**	
MUST support Round Robin (RR)	**Yes**	**Yes**	
MUST support Weighted Round Robin (RR)	**Yes**	**Yes**	
MUST support policer	**Yes**	**Yes**	
MUST support QoS per VLAN	**Yes**	**Yes**	

7.9. IPv6 Support

FortiSwitch supports IPv6 for device management. L2 and L3 features are expected in the second half of 2018.

Requirement	FortiLink	Standalone	Response
MUST support IPv6 Ready logo	**No**	**No**	
MUST support IPv6 unicast static routing	**Yes**	**Yes**	Only for device management
MUST support MLDv1 and v2 snooping	**No**	**No**	
MUST support option processing	**Yes**	**Yes**	Only for device management
MUST support fragmentation	**Yes**	**Yes**	Only for device management
MUST support ICMPv6	**Yes**	**Yes**	Only for device management
MUST support TCP/UDP over IPv6	**Yes**	**Yes**	Only for device management
MUST support Ping	**Yes**	**Yes**	Only for device management
MUST support Traceroute	**Yes**	**Yes**	Only for device management

MUST support SSH	**Yes**	**Yes**	Only for device management
MUST support SNMP	**Yes**	**Yes**	Only for device management
MUST support HTTP/HTTPS	**Yes**	**Yes**	Only for device management
MUST support Syslog	**Yes**	**Yes**	Only for device management
MUST support RADIUS	**Yes**	**Yes**	Only for device management
MUST support TACACS+	**Yes**	**Yes**	Only for device management
MUST support NTPv4 over IPv6	**Yes**	**Yes**	Only for device management
MUST support IPv6 First Hop Security	**No**	**No**	
MUST support RA Guard	**No**	**No**	
MUST support DHCPv6 Guard	**No**	**No**	
MUST support Binding Integrity Guard	**No**	**No**	
MUST support ACL	**No**	**No**	

7.9. VxLAN Support

VxLAN support is expected in the second half of 2018.

7.10 FortiSwitch Rugged Environmental and Compliance

See datasheet environmental and compliance information for each model.

Requirement	FortiLink	Response
MUST support operating temperature range **-40 - +75 Celsius**	**Yes**	
MUST support storage temperature range **-40 - +85 Celsius**	**Yes**	
MUST support humidity (non-condensing) **5-95%**	**Yes**	
MUST support **EMI:** Radiated Emission: CISPR 22, EN55022 Class B Conducted Emission: EN55022 Class B	**Yes**	
MUST support **EMS**: ESD: IEC61000-4-2 Radiated RF (RS): IEC61000-4-3 EFT: IEC61000-4-4 Surge: IEC61000-4-5 Conducted RF (CS): IEC61000-4-6	**Yes**	
MUST support RoHS (Pb free) and WEEE	**Yes**	
MUST support MTBF >30 years	**Yes**	
MUST support fanless cooling	**Yes**	
MUST support Ingress Protection **IP30**	**Yes**	
MUST be **plenum-rated**	**No**	
MUST support **NEMA TS-2**	**No**	
MUST support **FCC Part 15, Class A**	**Yes**	
MUST support **CE**	**Yes**	
MUST support **UL**	**No**	
MUST support **CAN ICES-3 (A) / NMB-3 (A)**	**Yes**	
MUST support **KEMA, ODVA Industrial EtherNet/IP, PROFINETY2, ABB IT Certificate**	**No**	
MUST support **Shock IEC 60068-2-27** (Operational Shock, Non-Operational Shock)	**No**	
MUST support **Vibration IEC 60068-2-6, IEC 60068-2-64, EN61373** (Operational Vibration, Non-operational Vibration)	**No**	

West Virginia Ethics Commission

Disclosure of Interested Parties to Contracts

(Required by *W. Va. Code* § 6D-1-2)

Name of Contracting Business Entity: Indicium Technology **Address:** 484 Williamsport Pike Suite 135

Name of Authorized Agent: Jamila Jones-Fleet **Address:** Martinsburg, WV 25404

Contract Number: DOT2000000157 **Contract Description:** Cisco Routers or Equal

Governmental agency awarding contract: WEST VIRGINIA DIVISION OF HIGHWAYS

☐ **Check here if this is a Supplemental Disclosure**

List the Names of Interested Parties to the contract which are known or reasonably anticipated by the contracting business entity for each category below *(attach additional pages if necessary)*:

1. **Subcontractors or other entities performing work or service under the Contract**
   ☐ Check here if none, otherwise list entity/individual names below.

2. **Any person or entity who owns 25% or more of contracting entity (not applicable to publicly traded entities)**
   ☐ Check here if none, otherwise list entity/individual names below.
   Jamila Jones-Fleet

3. **Any person or entity that facilitated, or negotiated the terms of, the applicable contract (excluding legal services related to the negotiation or drafting of the applicable contract)**
   ☐ Check here if none, otherwise list entity/individual names below.

Signature: Jamila Jones-Fleet Date Signed: 12 May 2020

Notary Verification

State of WV, County of Berkeley:

I, Jamila Jones-Fleet, the authorized agent of the contracting business entity listed above, being duly sworn, acknowledge that the Disclosure herein is being made under oath and under the penalty of perjury.

Taken, sworn to and subscribed before me this 12 day of May, 20.

Robert W Daugherty JR
Notary Public's Signature

To be completed by State Agency:
Date Received by State Agency: _____
Date submitted to Ethics Commission: _____
Governmental agency submitting Disclosure: _____

OFFICIAL SEAL
NOTARY PUBLIC
STATE OF WEST VIRGINIA
ROBERT W. DAUGHERTY, JR
45 Dwight Court, Martinsburg, WV 25405
My Commission Expires March 06, 2022

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

CONSTRUCTION CONTRACTS: Under W. Va. Code § 5-22-1(i), the contracting public entity shall not award a construction contract to any bidder that is known to be in default on any monetary obligation owed to the state or a political subdivision of the state, including, but not limited to, obligations related to payroll taxes, property taxes, sales and use taxes, fire service fees, or other fines or fees.

ALL CONTRACTS: Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

EXCEPTION: The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

DEFINITIONS:

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Employer default" means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

"Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceed five percent of the total contract amount.

AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (*W. Va. Code* §61-5-3) that: (1) for construction contracts, the vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: Indicium Technology

Authorized Signature: Jamila Jones-Fleet Date: 12 May 2020

State of WV

County of Berkeley, to-wit:

Taken, subscribed, and sworn to before me this 12 day of MAY, 2020.

My Commission expires 03-06, 2022

AFFIX SEAL HERE

OFFICIAL SEAL
NOTARY PUBLIC
STATE OF WEST VIRGINIA
ROBERT W. DAUGHERTY, JR
45 Dwight Court, Martinsburg, WV 25405
My Commission Expires March 06, 2022

NOTARY PUBLIC Robert W Daugherty Jr

SOLICITATION NUMBER: CRFQ DOT2000000157
Addendum Number: 1

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[ ] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[✓] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[ ] Other

Description of Modification to Solicitation:

1. To provide answers to vendor questions

No other changes

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ATTACHMENT A

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: DOT2000000157

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[X]	Addendum No. 1	[ ]	Addendum No. 6
[ ]	Addendum No. 2	[ ]	Addendum No. 7
[ ]	Addendum No. 3	[ ]	Addendum No. 8
[ ]	Addendum No. 4	[ ]	Addendum No. 9
[ ]	Addendum No. 5	[ ]	Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Indicium Technology
Company

Jamila Jones-Fleet
Authorized Signature

13 May 2020
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.
Revised 6/8/2012

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Quotation
21 — Info Technology

Proc Folder: 691866
Doc Description: ADDENDUM 2 CISCO ROUTERS & SWITCHES OR EQUAL (63200125)
Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No	Version
2020-04-30	2020-05-13 13:30:00	CRFQ 0803 DOT2000000157	3

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Name, Address and Telephone Number:

Indicium Technology
484 Williamsport Pike, Suite 135
Martinsburg, WV 25404
703-945-8265

FOR INFORMATION CONTACT THE BUYER

Crystal G Hustead
(304) 558-2402
crystal.g.hustead@wv.gov

Signature X **FEIN #** **DATE**

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION:

THE STATE OF WEST VIRGINIA PURCHASING DIVISION FOR THE AGENCY, WEST VIRGINIA DIVISION OF HIGHWAYS, IS SOLICITING BIDS TO ESTABLISH A CONTRACT FOR THE PURCHASE OF CISCO ROUTERS AND SWITCHES OR EQUAL PER THE ATTACHED DOCUMENTS.

QUESTIONS REGARDING THE SOLICITATION MUST BE SUBMITTED IN WRITING TO CRYSTAL.G.HUSTEAD@WV.GOV PRIOR TO THE QUESTION PERIOD DEADLINE CONTAINED IN THE INSTRUCTIONS TO VENDORS SUBMITTING BIDS

INVOICE TO	SHIP TO
DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV25305-0430 US	DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV 25305-0430 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	3.1.1 Cisco ISR 4321 Series Chassis Bundle or Equal-Year 1	10.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43222612			

Extended Description :

3.1.1 CISCO ISR 4321 Series Chassis Bundle or equal with Year 1 Smart Net Coverage

INVOICE TO	SHIP TO
DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV25305-0430 US	DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV 25305-0430 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	3.1.1 Cisco ISR 4321 Series Chassis Bundle or Equal-Year 2	10.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43222612			

Extended Description :

3.1.1 CISCO ISR 4321 Series Chassis Bundle or equal with Year 2 Smart Net Coverage

INVOICE TO	SHIP TO
DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV25305-0430 US	DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV 25305-0430 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	3.1.1 Cisco ISR 4321 Series Chassis Bundle or Equal-Year 3	10.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description :

3.1.1 CISCO ISR 4321 Series Chassis Bundle or equal with Year 3 Smart Net Coverage

INVOICE TO	SHIP TO
DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV25305-0430 US	DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV 25305-0430 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	3.1.1 Cisco ISR 4321 Series Chassis Bundle or Equal-Year 4	10.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description :

3.1.1 CISCO ISR 4321 Series Chassis Bundle or equal with Year 4 Smart Net Coverage

INVOICE TO	SHIP TO
DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV25305-0430 US	DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV 25305-0430 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
5	3.1.2 Cisco ISR 4331 Series Chassis Bundle or Equal-Year 1	6.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description :

3.1.2 CISCO ISR 4331 Series Chassis Bundle or Equal with Year 1 Smart Net Coverage.

INVOICE TO	SHIP TO
DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV25305-0430 US	DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV 25305-0430 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
6	3.1.2 Cisco ISR 4331 Series Chassis Bundle or Equal-Year 2	6.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description :

3.1.2 CISCO ISR 4331 Series Chassis Bundle or Equal with Year 2 Smart Net Coverage.

INVOICE TO	SHIP TO
DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV25305-0430 US	DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV 25305-0430 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
7	3.1.2 Cisco ISR 4331 Series Chassis Bundle or Equal-Year 3	6.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43222612			

Extended Description :

3.1.2 CISCO ISR 4331 Series Chassis Bundle or equal with Year 3 Smart Net coverage

INVOICE TO	SHIP TO
DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV25305-0430 US	DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV 25305-0430 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
8	3.1.2 Cisco ISR 4331 Series Chassis Bundle or Equal-Year 4	6.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43222612			

Extended Description :

3.1.2 CISCO ISR 4331 Series Chassis Bundle or equal with Year 4 Smart Net coverage

INVOICE TO	SHIP TO
DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV25305-0430 US	DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV 25305-0430 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
9	3.1.3 Cisco ISR 1101 Series Port Router or Equal-Year 1	55.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description :

3.1.3 Cisco ISR 1101 4 port router or equal with Year 1 Smart Net Coverage

INVOICE TO	SHIP TO
DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV25305-0430 US	DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV 25305-0430 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
10	3.1.3 Cisco ISR 1101 Series Port Router or Equal-Year 2	55.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description :

3.1.3 Cisco ISR 1101 4 port router or equal with Year 2 Smart Net Coverage

INVOICE TO	SHIP TO
DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV25305-0430 US	DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV 25305-0430 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
11	3.1.3 Cisco ISR 1101 Series Port Router or Equal-Year 3	55.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description :

3.1.3 Cisco ISR 1101 4 port router or equal with Year 3 Smart Net Coverage

INVOICE TO	SHIP TO
DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV25305-0430 US	DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV 25305-0430 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
12	3.1.3 Cisco ISR 1101 Series Port Router or Equal-Year 4	55.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description :

3.1.3 Cisco ISR 1101 4 port router or equal with Year 4 Smart Net Coverage

INVOICE TO	SHIP TO
DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV25305-0430 US	DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV 25305-0430 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
13	3.1.4 Cisco Extreme Networks 12 Port Switch or Equal	90.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description :

3.1.4 Cisco Extreme Networks 12 Port Switch or Equal

INVOICE TO	SHIP TO
DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV25305-0430 US	DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV 25305-0430 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
17	3.1.5 Cisco Extreme Networks 48 Port Switch or Equal	70.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description :

3.1.5 Cisco Extreme Networks 48 Port Switch or Equal

INVOICE TO	SHIP TO
DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV25305-0430 US	DIVISION OF HIGHWAYS INFORMATION SERVICE DIVISION 1900 KANAWHA BLVD E, BLDG 5 RM 920 CHARLESTON WV 25305-0430 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
21	3.1.6 Cisco Extreme Networks 24 Port Switch or Equal	15.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43222609			

Extended Description :

3.1.6 Cisco Extreme Networks 24 Port Switch or Equal

SCHEDULE OF EVENTS

Line	Event	Event Date
1	VENDOR QUESTION DEADLINE	2020-04-24

SOLICITATION NUMBER: CRFQ DOT2000000157
Addendum Number: 2

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[ ] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[✓] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[ ] Other

Description of Modification to Solicitation:

1. To provide answers to additional vendor questions

No other changes

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ATTACHMENT A

CRFQ DOT2000000157
Cisco Routers & Switches or Equal (63200125)
Addendum #2

Question#1:
On this solicitation is a bidder allowed to bid on parts of the requirements? i.e. May be unable to bid on Extreme but certainly can on Cisco.

Answer #1:
Per 4.1 The Contract shall be awarded to the Vendor that provides the Contract Items meeting the required specifications for the lowest overall total cost as shown on the Pricing Pages.

Question #2:
Would you consider procuring from multiple bidders on this, meaning a Cisco provider and an Extreme provider?

Answer #2:

Per 4.1 The Contract shall be awarded to the Vendor that provides the Contract Items meeting the required specifications for the lowest overall total cost as shown on the Pricing Pages.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: DOT2000000157

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[X]	Addendum No. 1	[ ]	Addendum No. 6
[X]	Addendum No. 2	[ ]	Addendum No. 7
[ ]	Addendum No. 3	[ ]	Addendum No. 8
[ ]	Addendum No. 4	[ ]	Addendum No. 9
[ ]	Addendum No. 5	[ ]	Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Indicium Technology
Company

Jamila Jones-Fleet
Authorized Signature

13 May 2020
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.
Revised 6/8/2012

FORTINET

WHITE PAPER

Fortinet Secure SD-WAN Reference Architecture

Executive Summary

The onset of digital transformation (DX) has introduced new technologies and solutions alongside lower-cost connectivity options for business, resulting in many organizations modernizing their legacy wide-area networks (WANs). With more and more data becoming digitized, the emergence of the public cloud, including the adoption of Software-as-a-Service (SaaS) applications, necessitates a redesign of the WAN architecture, specifically the branch, edge network, and security architecture. Software-defined WAN (SD-WAN) solutions leverage corporate WAN and multi-cloud connectivity to protect application performance at the network edge of branch sites.

This reference architecture white paper explains the evolution of WAN to SD-WAN architecture and highlights the benefits of modernizing networking infrastructure. It also provides details and security requirements with tips on what to look for when implementing a Secure SD-WAN solution from data center to branch.

Legacy WAN Architecture

Legacy WAN connectivity models, such as the one represented in Figure 1, often consisted of a single hub site, such as a data center or headquarters, with a single spoke or branch.

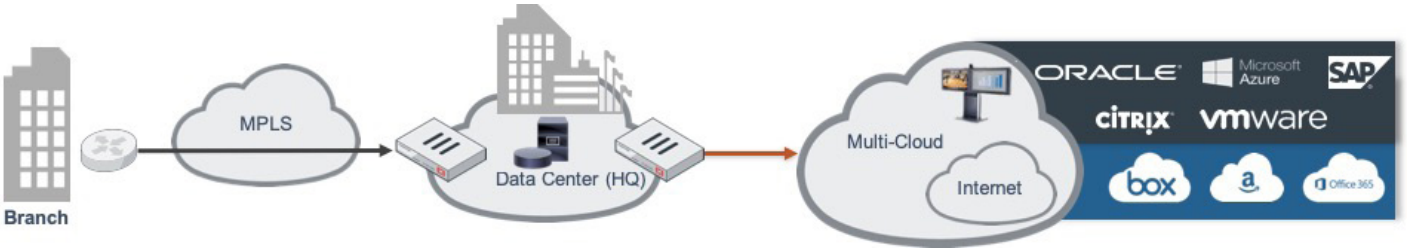


Figure 1: Legacy WAN hub-and-spoke architecture.

The routing aspect of traditional hub-and-spoke WAN architecture is simplistic in nature. Each spoke site must route all nonlocal traffic to the hub regardless of the final destination. Typically, this calls for a single static route, but adding redundant connectivity via multiple circuits can introduce higher levels of complexity. Traditional WAN architectures with legacy hardware and software solutions can still provide connectivity, performance, and security for organizations.

However, consider a branch user's legacy path to the public internet in Figure 1. To arrive at a website, packets would first need to traverse the WAN, navigate through a security stack, then proceed to the website. While this architecture traditionally minimizes branch infrastructure, it has for the most part fallen short when it comes to user experience. Users are often accustomed to broadband connectivity at their homes, something legacy WAN architecture fails to deliver for users.

Legacy security architectures deliver a centralized security stack across distributed enterprises. Figure 1a shows an example architecture where multiple functions exist within separate solutions. Branch sites might have a simple router for connectivity to an MPLS circuit, and because all traffic must first traverse the WAN, it makes sense to centralize advanced security capabilities at the data center instead of building distributed stacks at each branch. Due to the centralized stack architecture, WAN bandwidth has the propensity to become congested with traffic that ultimately will not be permitted to continue.

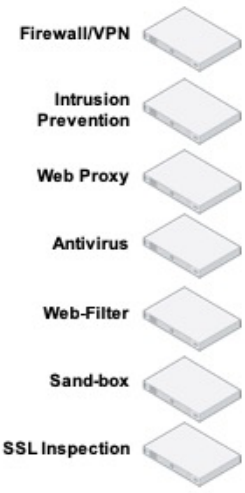


Figure 1a: Example security stack.

Fundamentals of SD-WAN

SD-WAN modernization is not just about replacing end-of-life hardware or software—it is a business solution. Organizations are adopting DX because the way business users consume technology has changed. Cloud adoption, device consolidation, and connectivity cost savings are significant drivers for infrastructure evolution. Delivering an improved user experience and increased productivity often motivate technology leaders to initiate WAN transformation projects.

SD-WAN Core Capabilities:

- Multi-path control
- Application awareness
- Dynamic application steering

Using control and data planes, SD-WAN solutions take advantage of branches with multiple points of connectivity to the internet or corporate WAN. It then decides which of these paths is most appropriate for a specific application. Data is transmitted over the optimal path to ensure performance and maximize availability.

SD-WAN protects application availability and performance across the corporate WAN or across the internet to multi-cloud environments by leveraging WAN path failover, link aggregation, link remediation, and active path performance metrics. Essentially, SD-WAN determines which path best meets performance expectations for a particular application and assigns packets or sessions to that WAN path.

Networking Improvements

A modernized WAN edge architecture with an SD-WAN solution implementation can demonstrate key improvements for an organization.

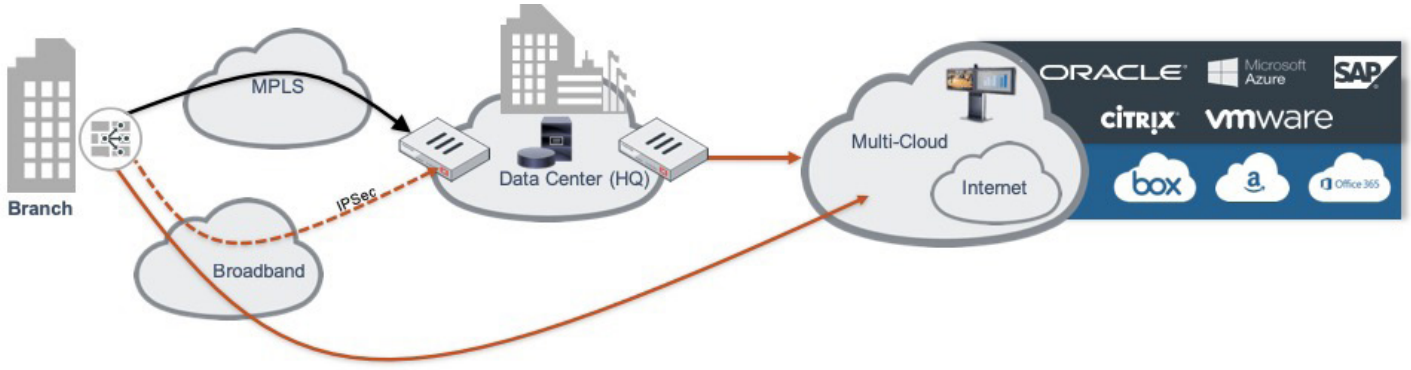


Figure 2: Modernized SD-WAN architecture.

As demonstrated by Figure 2, a branch with SD-WAN has multiple connections. In this example, the corporate WAN MPLS network remains, but the organization has introduced a single broadband connection to provide direct internet access from the branch. The organization has also established a secure IPsec tunnel to the data center over the broadband connection, creating a multi-path environment to both the data center and multi-cloud environment.

When compared to the legacy single-path architecture in Figure 3 with only one option to route traffic, it is clear why SD-WAN adoption is on the rise.

Figure 3: Legacy single path.

Secure SD-WAN

Introducing direct internet access at the branch also establishes direct connectivity to a volatile threat landscape. Branches with SD-WAN now require advanced security capabilities at the network edge. It is not enough to simply provide direct internet access with SD-WAN. Organizations need a Secure SD-WAN with built-in threat protection. Secure SD-WAN provides a security stack at the branch edge where it will provide direct services without traversing the corporate WAN.

Direct internet access applied to an MPLS-based WAN inherently provides for a redundant connectivity architecture. In terms of data-center connectivity, broadband delivers an alternative path for critical applications that will normally only traverse the MPLS network. In the same way, the MPLS network will continue to provide its path to the internet but is now superseded by the internet broadband connection.

Multi-path Control

The aforementioned core SD-WAN functionality demonstrated in Figure 2 highlights the need for multi-path control. There are three members that comprise the SD-WAN virtual link: an MPLS connection (blue), a broadband connection (solid orange), and an IPsec tunnel (broken orange). The Secure SD-WAN solution must be able to distinguish between applications to leverage the full functionality of the solution. By distinguishing applications and controlling multi-path environments, Secure SD-WAN provides dynamic application steering via packets or sessions to traverse available paths to the corporate WAN or multi-cloud environments.

Figure 4: SD-WAN virtual link.

Fortinet presents two main strategies for organizations to steer applications: best quality and minimum quality service-level agreement (SLA). Best quality determines which path is outperforming based on chosen metrics, by at least 10%. If the difference between the identified members is within the defined threshold, Secure SD-WAN selects the higher-priority link.

Alternatively, an organization may opt for an SLA strategy. FortiGate evaluates metrics defined within a performance SLA with respect to each member in the SD-WAN policy. If the primary path does not meet the SLA for the defined threshold(s), FortiGate will move the traffic to an alternate path. If no path meets the threshold(s), FortiGate chooses the path with the highest priority. To aid application steering, the Secure SD-WAN solution provides active path metrics. In conjunction with customer-defined SLAs, the SD-WAN policy engine determines which paths are viable transports for each application.

While SD-WAN routing is more complex than the legacy architecture, this implementation can continue to leverage static routes. Yet, Secure SD-WAN functionality controls route or path selection based on the dynamic application steering policy.

WAN Architecture Requirements

This section defines key high-level requirements for a WAN architecture modernization project. Noted requirements may be familiar to the reader, but all should not come solely from an organization's IT leadership or team members.

Improving Branch User Experience

It is important to understand how the branch business operates to measure and improve end-user experience. Though there are numerous IT/security considerations, there are also key business drivers that define a Secure SD-WAN design. It is beneficial for IT/security project leaders to meet with business leaders and end-users to gain the full scope of impact for new technology efforts.

For Secure SD-WAN projects, it is key to identify the applications branches use and where application servers reside (e.g., data center, multi-cloud, etc.). Once an organization has developed a relational diagram or map, the next step is to measure and determine performance baseline metrics for each application, then have the business prioritize these applications. Voice and video applications often take priority due to real-time communications requirements, but others that serve specific business objectives may fall into the critical category. Supporting the case with metrics to demonstrate gain goes a long way toward validating modernized WAN architecture.

Reduce Operating Expenses (OpEx)

Updating organizational contracts, agreements, or simple acquisition of WAN connectivity should reduce monthly OpEx. Organizations are able to take advantage of lower-cost, higher-bandwidth broadband connectivity in place of MPLS circuits.

Another means of reducing OpEx and potentially capital expenses (CapEx) is through device consolidation. Organizations with existing direct internet access may still be undergoing modernization with SD-WAN adoption. Some organizations have a costly infrastructure approach with multiple network and security vendors and disparate solutions at the branch edge. A Secure SD-WAN device is able to consolidate vendors and solutions, which reduces OpEx.

10X

The amount of potential savings by migrating from MPLS to SD-WAN.[1]

WAN Architecture Requires Security

Anything short of a fully integrated next-generation firewall (NGFW) is not delivering a Secure SD-WAN branch solution. Security services handoffs to third parties fall short of OpEx reduction regardless of whether the solution is on-premises or in the cloud. Further, the security architecture at the edge is not the same as the security architecture at the core. While unified threat management (UTM) devices have been protecting small and medium businesses (SMBs) for decades, they are also capable of serving enterprises.

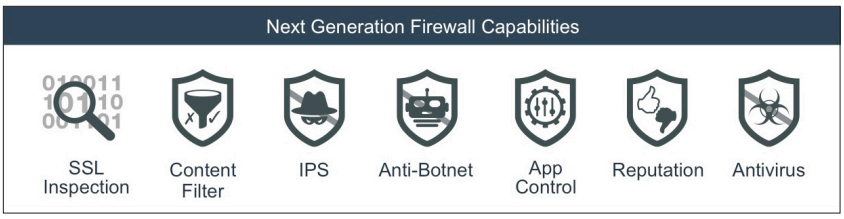


Figure 5: Security requirements.

UTMs can deliver sufficient security for distributed enterprise branch locations and provide services, including NGFWs, intrusion prevention systems (IPS), secure sockets layer (SSL) inspection, web content filtering, anti-malware gateways, and advanced routing compatibility. Device consolidation to a single, comprehensive Secure SD-WAN solution tackles the requirements listed in Figure 5.

Key Requirements Summary:

- Know the existing WAN architecture and how it serves business objectives
- List desired business outcomes of a WAN architecture refresh
- Understand security implications of the WAN architecture redesign
- Determine how much the organization spends on existing WAN architecture
- Establish a performance baseline to plan and achieve improvements

A Reflection of Existing WAN Architecture

While having accurate documentation and diagrams of an existing architecture may seem like an obvious step, it can be overlooked. Security architects can become burdened with remediation drills, resulting in a lack of detailed, accurate documentation of WAN architecture. An organization must understand its current WAN architecture to adequately propose a modernization project.

Fortinet Secure SD-WAN Solution Architecture

The Fortinet Secure SD-WAN solution is comprised of multiple components. Overall, the components that make up the Fortinet Secure SD-WAN solution are: FortiGate, FortiManager, FortiAnalyzer, and FortiDeploy.

FortiGate runs FortiOS, the core of the Secure SD-WAN solution. **FortiManager** drives orchestration and management. **FortiAnalyzer** and **FortiDeploy** help the whole solution come together, delivering a solution that is unmatched by other vendors.

Figure 5a: Secure SD-WAN architecture components.

Secure SD-WAN must satisfy business outcomes with regard to the architecture and how they serve different roles within an organization (e.g., CIO, CISO, et al). It is also important to understand how other Fortinet solutions such as FortiExtender and FortiAuthenticator extend beyond SD-WAN, providing complete coverage across the branch to further build out the Fortinet Security Fabric.

Management, Control, and Data Planes

In organizations with small deployments of one to three sites, each FortiGate may act as a management, control, and data plane. More commonly, distributed deployments will utilize the full spectrum of Secure SD-WAN components. Such a deployment will divide the same roles, as shown in Figure 6.

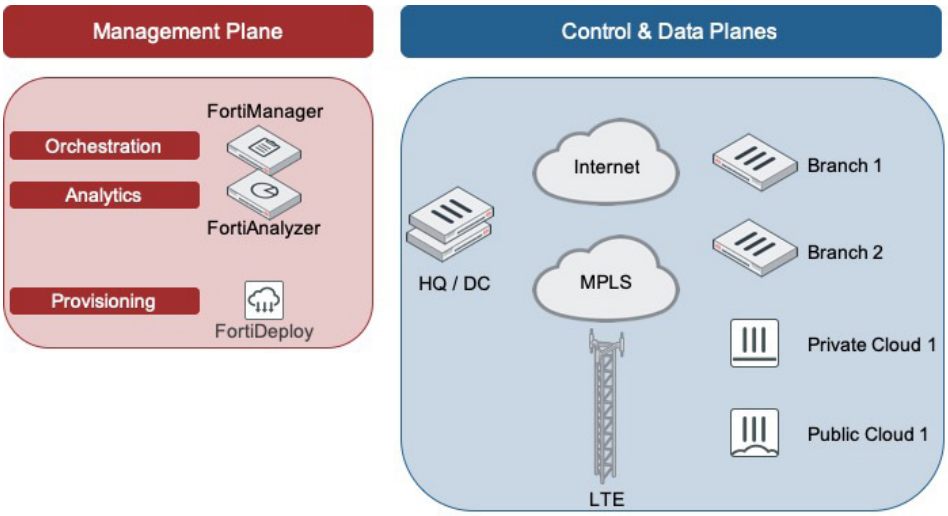


Figure 6: Secure SD-WAN architecture components.

The FortiGate, with its underlying operating system FortiOS, is the basic component of the Secure SD-WAN solution. It is able to stand alone and provide full functionality including NGFW, advanced security features, and SD-WAN capabilities. Acting in all roles, FortiGate easily consolidates WAN edge solutions into one comprehensive device. FortiGate also delivers routing protocol support (e.g., RIP, BGP, OSPF, etc.) and VPN pairing as a spoke or hub, enables WAN optimization via protocol optimization, byte, and object caching, and even acts as an access layer controller. In addition, the FortiGate supports packet priority to ensure those business-critical applications take precedence in times of congestion.

FortiGate Form Factors

With respect to distributed deployments and FortiGate models, typical edge devices range from the edge models 30E to 200E on the physical appliance implementation to VM01 to VM16 on the virtual machine implementation. Several small branch appliances come with Wi-Fi, 3G, 4G, and LTE options to further consolidate branch solutions.

The most popular FortiGate branch device is the 60E model. See an overview of the FortiGate 60E specifications in Figure 7.

Secure SD-WAN now supports IPv6.

It supports all load balance modes, health checking, and service rules for source address, source user and group, and destination address.

Newly released FortiOS 6.2 adds new capabilities and improves existing SD-WAN functionality.

New Features:

- Overlay controller VPN
- Bandwidth monitoring service
- Forward error correction
- BGP additional path support
- SLA logging
- Multiple IPsec tunnels as a single interface

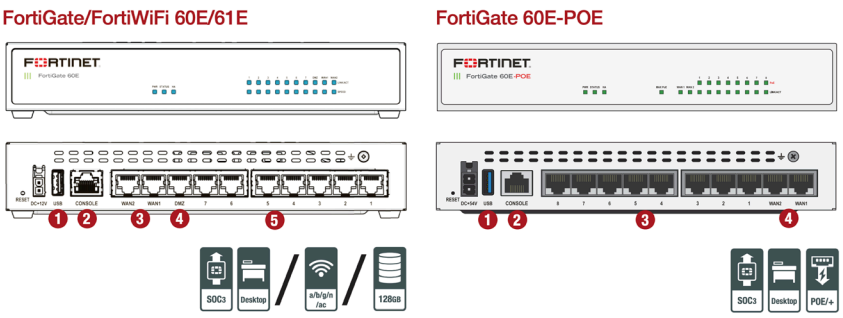


Figure 7: FortiGate 60E specifications.

Figure 8 details the performance data of the FortiGate 60E series appliances.

System Performance	
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	3 / 3 / 3 Gbps
Firewall Latency (64 byte UDP packets)	3 µs
Firewall Throughput (Packets Per Second)	4.5 Mpps
Concurrent Sessions (TCP)	1.3 Million
New Sessions/Second (TCP)	30,000
Firewall Policies	5,000
IPsec VPN Throughput (512 byte) [1]	2 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	200
Client-to-Gateway IPsec VPN Tunnels	500
SSL-VPN Throughput	150 Mbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	100
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	135 Mbps
SSL Inspection CPS (IPS, avg. HTTPS) [3]	135
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	75,000
Application Control Throughput (HTTP 64K) [2]	650 Mbps
CAPWAP Throughput (HTTP 64K)	890 Mbps
Virtual Domains (Default / Maximum)	10 / 10
Maximum Number of Switches Supported	8
Maximum Number of FortiAPs (Total / Tunnel Mode)	30 / 10
Maximum Number of FortiTokens	100
Maximum Number of Registered FortiClients	200
High Availability Configurations	Active / Active, Active / Passive, Clustering

Figure 8: FortiGate 60E series performance specifications.

Most Secure SD-WAN branch deployments are going to implement IPsec tunnels to securely transport packets between branch sites, to the data center, or to the cloud. Considering typical branch deployment requirements, 2 Gbps of VPN throughput offers more bandwidth than many branches require. Enabling application control, which examines the application layer of packets, decreases throughput only to 890 Mbps, still supporting branch bandwidth needs. Enabling full secure sockets layer (SSL)/transport layer security (TLS) inspection and enabling IPS provides for 135 Mbps.

The reason the FortiGate 60E series appliance boasts such performance is because of the Fortinet system-on-a-chip (SOC3) purpose-built processor and now SOC4, the only purpose-built processor designed to accelerate SD-WAN.

The Fortinet incumbent SOC3 accelerates the 60E series security appliances to further speed its best-in-class throughput with consolidated security and networking capabilities. The SOC3 more than doubles the secure networking performance over the enterprise-class CPUs found in competing security solutions and propels the FortiGate 60E series distributed enterprise firewalls to unprecedented levels of security and performance.[2]

SOC4 Release

Fortinet recently released the SOC4 processor leading with the FortiGate 100F series appliance. The SOC4 is the only purpose-built processor specifically designed to accelerate SD-WAN capabilities.

World's First SD-WAN ASIC:

- Fastest application steering
- Accelerated WAN overlay
- Best-of-breed security performance
- Security extension acceleration

Specification	FortiGate 60E (SOC3 ASIC)	Industry Average (Based on this price point)	Distributed Enterprise Advantage using FortiGate 60E
Firewall	3000 Mbps	630 Mbps	**5x** higher firewall throughput compare to industry average
IPSEC VPN (AES256 and 1400 bytes)	3000 Mbps	275 Mbps	**11x** higher VPN with AES256 encryption compare to industry average helps more users to securely access public cloud applications
IPS Throughput	1400 Mbps	300 Mbps	**5x** higher IPS throughput compare to industry average benefits higher threat prevention
SSL Inspection	340 Mbps	45 Mbps	**8x** better SSL inspection throughput compare to industry average provides complete protection against rising SSL traffic
Concurrent Sessions	1.3 Million	0.27 Million	**5x** higher sessions compare to industry average increases the productivity as more users are getting benefit of complete security
Power Consumption	5 W	15 W	**3x** lower power consumption enables high scalability

**Industry Averages Calculated By Price Point of Competing Solutions from CheckPoint, Dell, and Cisco Meraki*

Figure 9: FortiGate 60E industry comparison.

Fortinet has a multitude of options to choose from after an organization has determined its branch edge requirements.

FortiGate Routing

Before an organization can properly introduce Secure SD-WAN into its WAN architecture, it first must lay out how packets might get from one site to another. In legacy networks, organizations might use static routes or border gateway protocol (BGP) for dynamic routing between a multitude of sites. FortiGate fully supports BGP, even for Secure SD-WAN deployments.

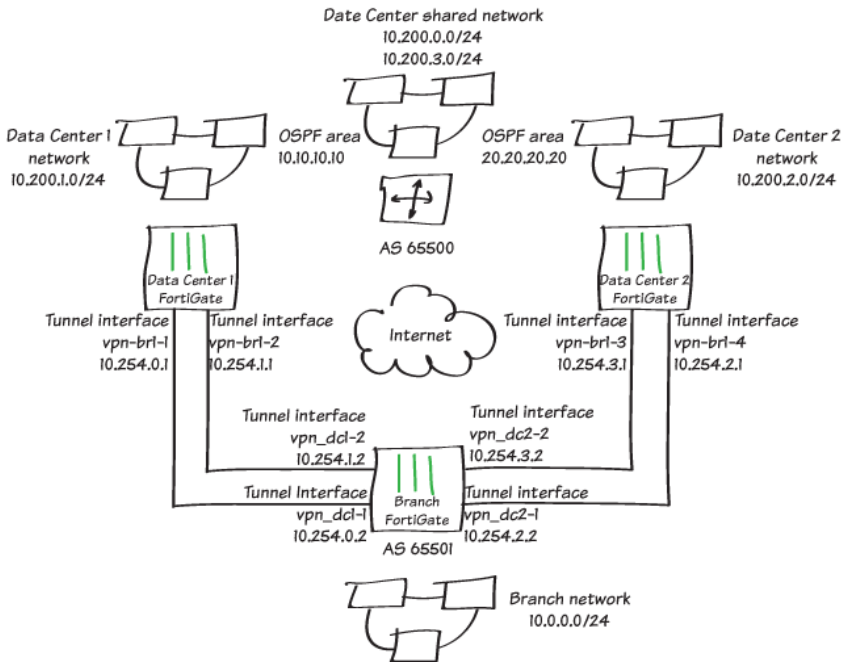


Figure 10: Client-side Secure SD-WAN with IPsec VPN.

Tech Tip

For all FortiGate models, the numeric differentiation denotes a larger amount of hard disk within the appliance. For instance, 61E comes with 128 GB SSD storage.

Figure 10 demonstrates the BGP routing environment within a private space. In this case, the customer is using IPsec tunnels over the internet to connect its WAN. AS 65500 is defined in the data center and AS 65501 is assigned at the branch. Data-center networks are advertised across the WAN to the branch by each of the FortiGate NGFWs at the data-center edge. For example, DCFW 1 (the upper left FortiGate in the diagram) will advertise routes to 10.200.1.0/24, 10.200.0.0/24, and 10.200.3.0/24. On the right FortiGate, it too will advertise the 10.200.0.0/24 and 10.200.3.0/24 networks. However, it will not advertise the 10.200.1.0/24, but instead advertise the 10.200.2.0/24 network. Each network will advertise its own back end without advertising the other. Advertising both is possible and will work in some scenarios.

There is one note of caution when it comes to BGP and dynamic routing. Sometimes, as is the case here, we introduce networks that are advertised from more than one hop (router). In these routing architectures, asynchronous routing, especially in a Secure SD-WAN environment where firewall functionality enforces sessions (return path forwarding, or anti-spoofing), is something to look out for and address.

From the client side, FortiGate will advertise the 10.0.0.0/24 network. In addition to advertising their own routes, the data center FortiGate NGFWs will also act as route reflectors, letting all other participating members (branches) know about route updates from branch participants. This functionality reduces the necessity for each branch to communicate its route updates to all other branches. This can cause unnecessary overhead traffic and potential delays with updating routes across the WAN. There are other cautions for large networks concerning convergence times and memory consumption; yet, most enterprises will not likely encounter these challenges.

While Open Shortest Path First (OSPF) is noted in the diagram, FortiGate does not participate in this back-end data-center-to-data-center routing scheme (though the FortiGate does support OSPF). Engage the internal network architecture team when spinning up a Secure SD-WAN project to ensure that the routing scheme is both supported and properly designed.

Even though administrators and engineers must configure routes using the SD-WAN virtual WAN link, FortiGate installs individual routes for member interfaces into the routing table. These routes are each active and share similar attributes (e.g., destination address and subnet, distance, and priority). This action allows the FortiGate NGFW to remove individual routes in the event of an interface outage and to redirect all traffic to the remaining member interfaces without affecting SD-WAN members.

WAN Paths (SD-WAN Interfaces)

The FortiGate Secure SD-WAN solution is largely comprised of autonomous underlay and overlay interfaces aggregated into a single virtual WAN link.

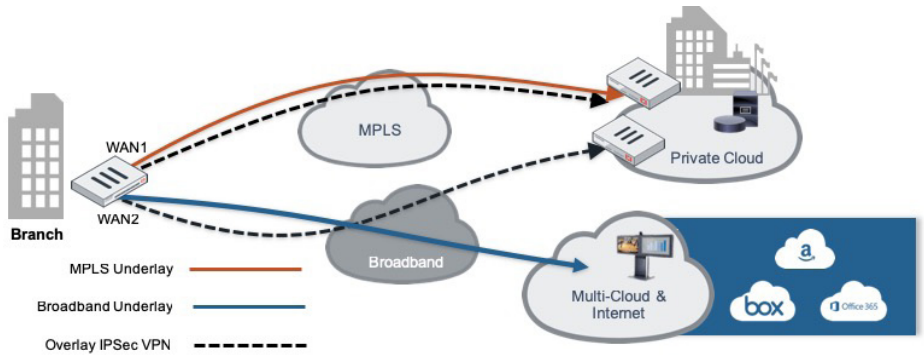


Figure 11: SD-WAN interface members (underlay and overlay).

Tech Tip

It is a best practice to create static black hole routes with destinations set to each branch network (or small enough to cover all branches). If the data center FortiGate NGFWs temporarily lose connectivity with a branch network, traffic destined to that network is sent to the black hole until connectivity has been restored and the routes converged through BGP.

Terms to Know

Underlay transport
The raw transport typically associated with the wire attached to the FortiGate device. There is a one-to-one relationship between underlay interfaces and FortiGate physical interfaces. Examples include MPLS, broadband, or 4G/LTE connections over Ethernet.

Overlay transport
A virtual interface riding an underlay transport. There may be a one-to-many (physical interface to overlay interface) relationship for overlay transports. Examples include IPsec tunnel and VLAN interfaces.

In Figure 11, there are four unique interfaces defined on the branch FortiGate. From a physical perspective, there are two connections (WAN1 and WAN2)—one to the MPLS network and the other through the broadband provider. However, this organization has created two IPsec overlay interfaces—one tunneling over each physical underlay. In total, these four interfaces are all available to become members of the FortiGate virtual WAN link. This organization may choose to configure primary/secondary paths, or even aggregate multiple paths to increase bandwidth.

On the FortiGate NGFW, any defined interface, whether underlay or overlay, may be included as a member of the SD-WAN virtual WAN link. In FortiOS 6.x, each virtual domain (VDOM) may have one SD-WAN virtual WAN link or SD-WAN interface. If an organization is considering introducing VDOMs at one or more branch sites, the design team should consider inter-VDOM routing to ensure that the SD-WAN capabilities are leveraging more than one external WAN path.

Tech Tip

Not all interfaces within FortiGate must be added to the SD-WAN virtual WAN link. To exempt a nonparticipating interface, FortiGate supports the configuration of an implicit rule to address negation. This ensures SD-WAN policy-based routing rules do not match traffic unless the traffic is intended for SD-WAN interfaces.

Administrators must specify at least two virtual WAN link member interfaces. SD-WAN should be configured early during the initial setup of FortiGate because interfaces already referenced by a firewall policy or static route are not eligible to be added as a member interface.

Virtual Private Network Connections

VPN connections are instrumental in Secure SD-WAN deployments. As an overlay interface, VPN tunnels sometimes exist in some level of multiplier of the underlay interfaces.

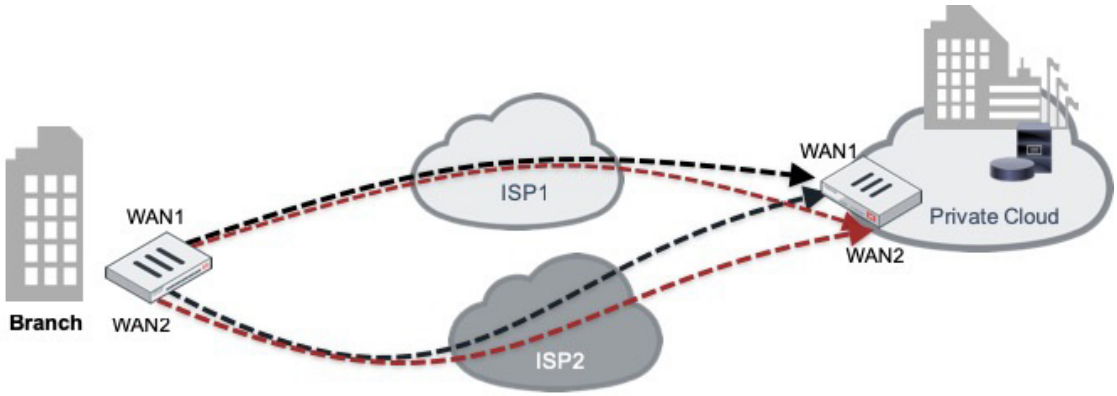


Figure 12: IPsec overlay interfaces.

There are two underlay interfaces in Figure 12 labeled WAN1 and WAN2. From these two interfaces, this organization has created four overlay interfaces on the branch FortiGate. Essentially, there is a full mesh of connectivity between the underlay interfaces using IPsec tunnels. In total, this particular organization may choose to add six interfaces to the SD-WAN virtual WAN link, consisting of the two underlay interfaces and four overlay interfaces.

FortiGate supports numerous connections for IPsec tunnels and architectures, from common hub and spoke and partial mesh, to full mesh VPN architectures. Figure 13 demonstrates a typical hub-and-spoke VPN architecture.

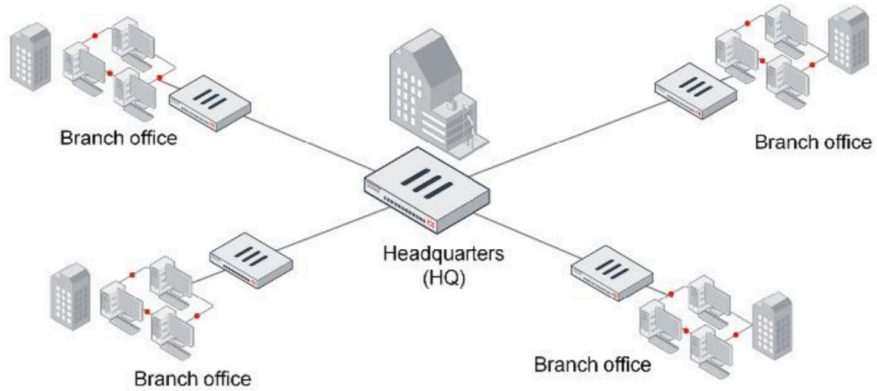


Figure 13: Hub-and-spoke WAN (VPN) architecture.

In this architecture, the path between sites passes through the hub. Further, in a legacy WAN environment, all traffic passes through the hub. However, with WAN edge modernization, each of these branch sites would receive direct internet access, allowing Secure SD-WAN to optimize path selection and protect application performance and availability, whether the application resides in the corporate data center or in a multi-cloud environment. Partial or full mesh provides branch sites with direct connectivity to one another. FortiGate includes auto-discovery VPN (ADVPN) to dynamically negotiate on-demand direct VPNs between spoke sites with the assistance of the hub site. While this capability typically requires the use of routing protocols so spokes are able to learn routes from one another, the FortiGate device serving in hub roles maintains a record of networks for each spoke and is able to communicate routes while facilitating a direct connection between two spokes.

Tech Tip

FortiOS 6.2 allows administrators to add forward error correction (FEC) to IPsec VPN members to lower packet loss ratio for critical business applications like voice and video.

Once an administrator configures the FortiGate IPsec tunnels, they can add the interface as members of the SD-WAN virtual WAN link. This allows FortiGate to leverage performance SLAs, SD-WAN policy, security policy, and prioritization as part of the SD-WAN virtual WAN link.

Integrated NGFW

The most beneficial aspect of Fortinet Secure SD-WAN are the integrated NGFW capabilities. Other solution architectures (e.g., offloading to third parties, tunneling to the cloud, etc.) are viable, but SD-WAN is primarily about WAN edge control and optimization. Therefore, it makes sense to perform as much control at the edge as possible without extending budgetary constraints. FortiGate meets and exceeds both of these requirements.

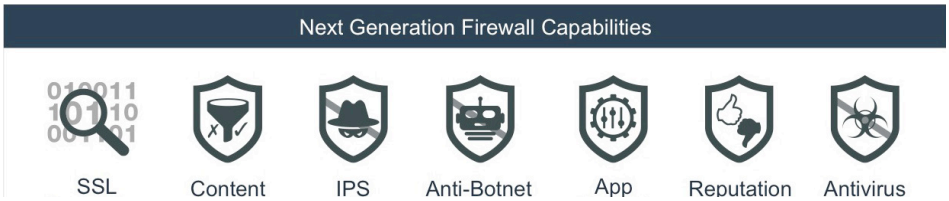


Figure 14: Security requirements.

Providing a full set of SD-WAN and security functions at the branch edge, prior to consuming costly bandwidth, FortiGate Secure SD-WAN is unrivaled in price, performance, and security effectiveness. Examine the architecture of FortiGate NGFW key features with respect to SD-WAN and WAN edge modernization.

The best value delivered in every FortiGate appliance is the SOC3. These purpose-built security processors radically boost performance and scalability to enable the fastest network security appliance available. This propels organizations to stay ahead of rapidly growing bandwidth requirements by preventing security from impacting network performance. Fortinet security processors accelerate specific parts of packet processing and content scanning functions. This customized technology enables organizations to run multiple security applications without degradation in performance. Without performance degradation, an organization is enabled to run both SD-WAN and advanced security features on the same appliance (consolidation) and at the same cost (OpEx savings).

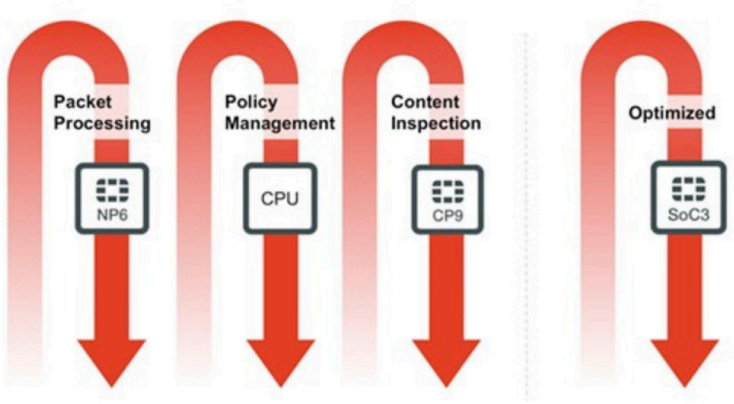


Figure 15: FortiGate parallel path processing (PPP).

The security processors in Figure 15 are used to scale from 1 Gbps to 1 Tbps of firewall throughput—independent of packet size. Fortinet parallel path processing architecture optimizes the high-performance hardware and software resources available in packet flow to deliver ultra-low latency and maximum throughput.

FortiGate is a stateful packet filter (firewall) at its core, ensuring secure session-based connectivity from the branch edge. FortiGate is a comprehensive Secure SD-WAN solution providing security and WAN path control at the branch edge.

Firewall policy is a well-established capability to provide identity-based granular security policy. For SD-WAN deployments, the FortiGate security policy is simplified. Instead of providing rules for individual virtual WAN link members, one only needs to identify the SD-WAN interface within the policy. The policy will apply to all member interfaces, making it easier for organizations to combine SD-WAN and security capabilities in one interface, whether that be the FortiGate itself or FortiManager. This provides granular authorization and access control, along with a mechanism to introduce advanced security features at the branch edge.

While application control is necessary for SD-WAN dynamic application steering, it also plays a role in security. For example, some organizations may permit downloading files from cloud repositories such as Dropbox. However, these same organizations may not permit users to upload files to these same repositories. In that case, organizations need a combination of SSL inspection, application control, and security policy features for the SD-WAN interface.

Without SSL inspection, any device would be incapable of determining the activity of the session. Without application control, the edge device would not be able to quickly determine the application, therefore allocating the session to subsequent rules. Even if organizations could identify application and user activity, they cannot introduce a granular identity-based security policy without a firewall rule base. These combined features allow for not only precise WAN path control but also the introduction of advanced security features, including IPS, anti-malware, and URL filtering.

In addition, FortiGate supports offloading file samples to a FortiSandbox for zero-day malware protection. FortiGate enables a single, full security stack.

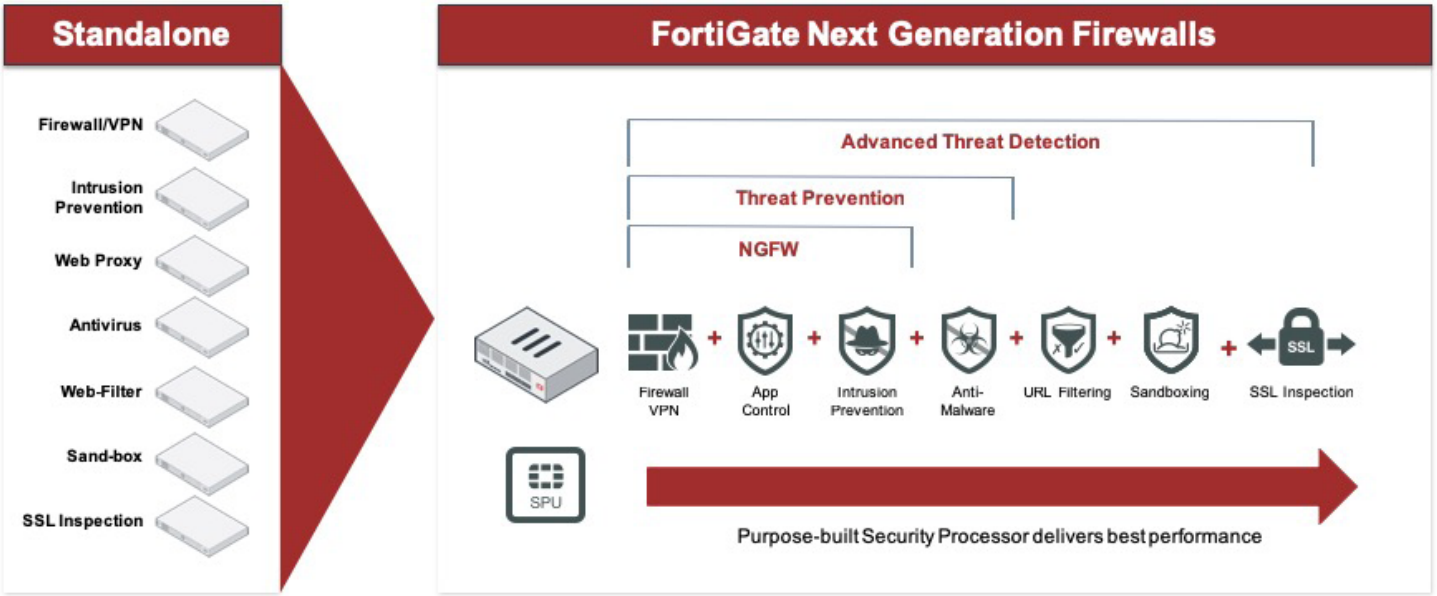


Figure 16: Standalone versus FortiGate security architecture.

A standalone branch edge strategy appears costly. Fortinet packs all seven of the featured capabilities into FortiGate form factors with unrivaled performance, with threat intelligence driven through Fortinet's own FortiGuard Labs global threat research and response team.

SD-WAN Packet Prioritization

Legacy WAN architecture typically includes quality of service (QoS). Where MPLS networks exist, so do low-bandwidth connections, leaving some branches with slow connectivity. While these may be more than sufficient for some branches, they also beg for QoS features to protect critical business applications. Typically including voice (VoIP) and video, these applications are marked at an edge device (router), so they receive priority transmission over the WAN. In addition, the FortiGate also provides packet-shaping capabilities, including default priority buckets and differentiated services marking. Priority allows critical business applications to receive preferential ordering across a specified virtual WAN link member interface if congestion begins to impact overall performance of that interface.

Management and Orchestration

FortiManager provides centralized management and orchestration of Secure SD-WAN branch edge devices. An organization's FortiManager may reside on-premises, in a private cloud, or in public cloud environments. Regardless of location, FortiManager maintains connectivity to each FortiGate device, monitors performance SLAs, and presents a single-pane-of-glass view into global connectivity. It also provides templates for security policy configuration, SD-WAN policy configuration, and performance SLA definition.

Secure SD-WAN administrators only need FortiManager to control their entire deployment. With flexibility to support APIs and Security Fabric Connectors, FortiManager seamlessly integrates into the greater workflow within any organization.

Tech Tip

Use IPsec VPN templates to configure site-to-site VPN tunnels (via FortiGate or FortiManager). Because there are many options to configure when setting up tunnel negotiation, templates reduce the chance for manual mistakes.

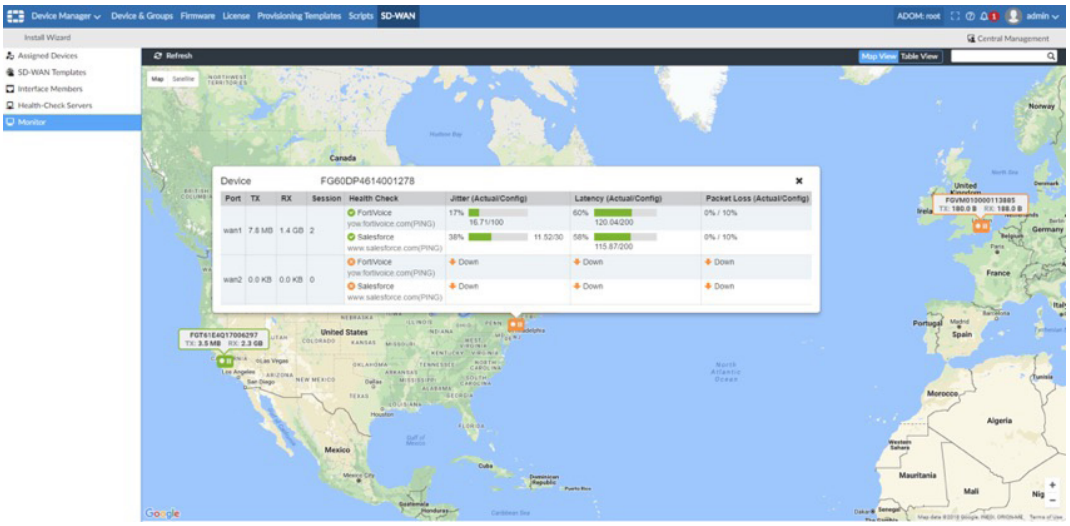


Figure 17: FortiManager geographical monitoring.

Zero-Touch Deployment

FortiManager is also a key part of enabling zero-touch deployment (ZTD). By adding a ZTD key to an order, organizations register devices in the FortiDeploy system as ZTD devices. Customers then identify a routable IP address for FortiManager in the FortiDeploy system. When a new device is simply plugged into power and connected to the internet via Ethernet, FortiGate automatically calls home, receives the FortiManager IP address, and immediately requests connectivity to FortiManager.

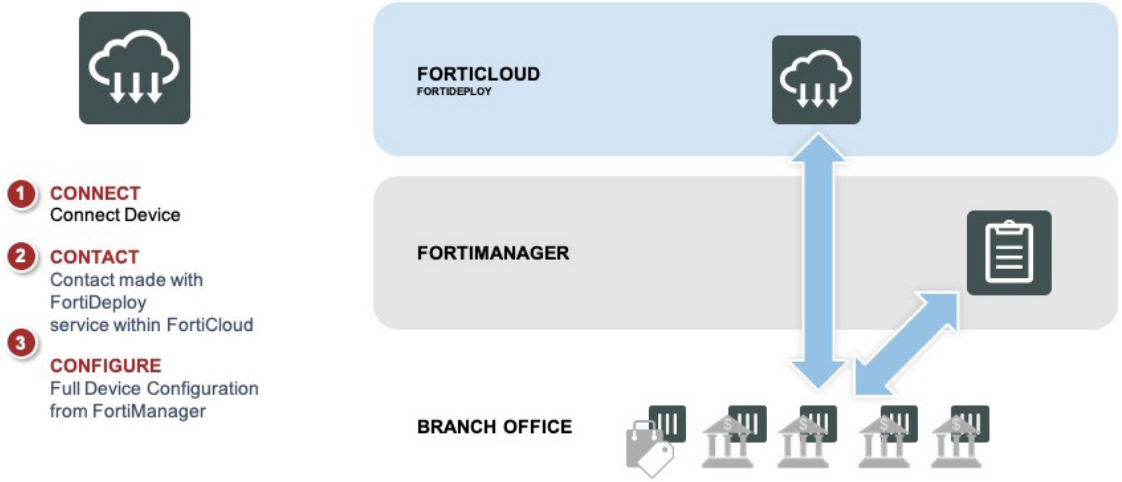


Figure 18: Fortinet zero-touch deployment process.

Once the devices are authorized, FortiManager pushes configuration templates to each device, fully configuring them for security and SD-WAN functionality at the branch.

Conclusion

Fortinet simplifies the necessary WAN edge architecture for organizations by providing a comprehensive Secure SD-WAN solution via FortiGate. Consolidating numerous devices at the branch edge, FortiGate with FortiOS provides routing capability for support of both static and dynamic protocols. Additionally, FortiGate offers replacement of multidevice security architectures, without sacrificing performance through the introduction of SPUs. Finally, FortiGate offers proven performance and manageability of SD-WAN core functionality. FortiGate is the only Secure SD-WAN solution delivering network and security architecture in one robust, easy-to-deploy, and easy-to-manage solution.

[1] Based on internal Fortinet research and testing.
[2] Ibid.

April 3, 2019 8:50 AM

379990-0-0-EN

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2019:WP-Fortinet-Secure-SD-WAN-Architecture:wp-fortinet-secure-sd-wan-architecture Folder:wp-fortinet-secure-sd-wan-architecture