



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.

Header 5

List View

General Information | Contact | Default Values | Discount | Document Information

Procurement Folder: 735927

SO Doc Code: CRFQ

Procurement Type: Central Purchase Order

SO Dept: 0603

Vendor ID:

SO Doc ID: ADJ2000000036

Legal Name: INDICIUM TECHNOLOGIES INC

Published Date: 6/5/20

Alias/DBA:

Close Date: 6/18/20

Total Bid: \$2,410.00

Close Time: 13:30

Response Date:

Status: Closed

Response Time:

Solicitation Description:

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 : 735927

Solicitation Description : Cisco Router, IP Base License, AC power supply & cable MCAS

Proc Type : Central Purchase Order

Date issued	Solicitation Closes	Solicitation Response	Version
	2020-06-18 13:30:00	SR 0603 ESR06172000000007707	1

VENDOR

000000162797
 INDICIUM TECHNOLOGIES INC

Solicitation Number: CRFQ 0603 ADJ2000000036

Total Bid : \$2,410.00 **Response Date:** 2020-06-17 **Response Time:** 21:00:20

Comments:

FOR INFORMATION CONTACT THE BUYER

John W Estep
 (304) 558-7839
 john.w.estep@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	Cisco Router, IP Base License, AC power supply & cable MCAS	1.00000	LS	\$2,410.000000	\$2,410.00

Comm Code	Manufacturer	Specification	Model #
43211501			

Extended Description :	Cisco Router, IP Base License, AC power supply & cable MCAS
-------------------------------	---

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 exceeds 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

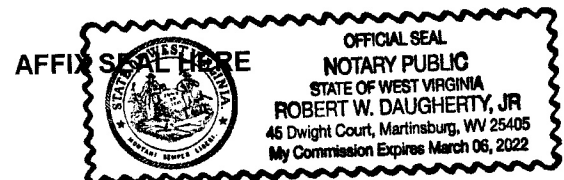
Authorized Signature: *Jamila Jones Fleet* Date: 12 May 2020

State of WV

County of Beekley, to-wit:

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

My Commission expires 03 - 06, 2022



NOTARY PUBLIC *Robert W Daugherty Jr*
Purchasing Affidavit (Revised 01/19/2018)

VENDOR PREFERENCE CERTIFICATE

Certification and application is hereby made for Preference in accordance with **West Virginia Code**, §5A-3-37. (Does not apply to construction contracts). **West Virginia Code**, §5A-3-37, provides an opportunity for qualifying vendors to request (at the time of bid) preference for their residency status. Such preference is an evaluation method only and will be applied only to the cost bid in accordance with the **West Virginia Code**. This certificate for application is to be used to request such preference. The Purchasing Division will make the determination of the Vendor Preference, if applicable.

1. **Application is made for 2.5% vendor preference for the reason checked:**
____ Bidder is an individual resident vendor and has resided continuously in West Virginia, or bidder is a partnership, association or corporation resident vendor and has maintained its headquarters or principal place of business continuously in West Virginia, for four (4) years immediately preceding the date of this certification; **or**,
____ Bidder is a resident vendor partnership, association, or corporation with at least eighty percent of ownership interest of bidder held by another entity that meets the applicable four year residency requirement; **or**,
____ Bidder is a nonresident vendor which has an affiliate or subsidiary which employs a minimum of one hundred state residents and which has maintained its headquarters or principal place of business within West Virginia continuously for the four (4) years immediately preceding the date of this certification; **or**,
2. **Application is made for 2.5% vendor preference for the reason checked:**
____ Bidder is a resident vendor who certifies that, during the life of the contract, on average at least 75% of the employees working on the project being bid are residents of West Virginia who have resided in the state continuously for the two years immediately preceding submission of this bid; **or**,
3. **Application is made for 2.5% vendor preference for the reason checked:**
____ Bidder is a nonresident vendor that employs a minimum of one hundred state residents, or a nonresident vendor which has an affiliate or subsidiary which maintains its headquarters or principal place of business within West Virginia and employs a minimum of one hundred state residents, and for purposes of producing or distributing the commodities or completing the project which is the subject of the bidder's bid and continuously over the entire term of the project, on average at least seventy-five percent of the bidder's employees or the bidder's affiliate's or subsidiary's employees are residents of West Virginia who have resided in the state continuously for the two immediately preceding years and the vendor's bid; **or**,
4. **Application is made for 5% vendor preference for the reason checked:**
____ Bidder meets either the requirement of both subdivisions (1) and (2) or subdivision (1) and (3) as stated above; **or**,
5. **Application is made for 3.5% vendor preference who is a veteran for the reason checked:**
____ Bidder is an individual resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard and has resided in West Virginia continuously for the four years immediately preceding the date on which the bid is submitted; **or**,
6. **Application is made for 3.5% vendor preference who is a veteran for the reason checked:**
____ Bidder is a resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard, if, for purposes of producing or distributing the commodities or completing the project which is the subject of the vendor's bid and continuously over the entire term of the project, on average at least seventy-five percent of the vendor's employees are residents of West Virginia who have resided in the state continuously for the two immediately preceding years.
7. **Application is made for preference as a non-resident small, women- and minority-owned business, in accordance with West Virginia Code §5A-3-59 and West Virginia Code of State Rules.**
____ Bidder has been or expects to be approved prior to contract award by the Purchasing Division as a certified small, women- and minority-owned business.
8. **Application is made for reciprocal preference.**
____ Bidder is a West Virginia resident and is requesting reciprocal preference to the extent that it applies.

Bidder understands if the Secretary of Revenue determines that a Bidder receiving preference has failed to continue to meet the requirements for such preference, the Secretary may order the Director of Purchasing to: (a) rescind the contract or purchase order; or (b) assess a penalty against such Bidder in an amount not to exceed 5% of the bid amount and that such penalty will be paid to the contracting agency or deducted from any unpaid balance on the contract or purchase order.

By submission of this certificate, Bidder agrees to disclose any reasonably requested information to the Purchasing Division and authorizes the Department of Revenue to disclose to the Director of Purchasing appropriate information verifying that Bidder has paid the required business taxes, provided that such information does not contain the amounts of taxes paid nor any other information deemed by the Tax Commissioner to be confidential.

Bidder hereby certifies that this certificate is true and accurate in all respects; and that if a contract is issued to Bidder and if anything contained within this certificate changes during the term of the contract, Bidder will notify the Purchasing Division in writing immediately.

Bidder: _____ Signed: Janita Jones-Fleet

Date: _____ Title: _____

*Check any combination of preference consideration(s) indicated above, which you are entitled to receive.



Where Innovation Works for You.

484 Williamsport Pike, Suite 135
Martinsburg, WV 25404



Quote

DATE: 6/17/20
QUOTE # 1270
QUOTE EXP: August 31 2020
Customer ID: WV Adjutant Gen.
 Period of Performance: TBA

CUSTOMER INFORMATION:

WV Adjutant General

Line Item	DESCRIPTION	QTY	Unit Cost	Extended Cost
0001	FG-100F 22 x GE RJ45 ports (including 2 x WAN ports, 1 x DMZ port, 1 x Mgmt port, 2 x HA ports, 16 x switch ports with 4 SFP port shared media), 4 SFP ports, 2x 10G SFP+ FortiLinks, dual power supplies redundancy.	1	\$ 1,600.00	\$ 1,600.00
0002	FC-10-F100F-284-02-12 FortiGate-100F 1 Year ASE FortiCare (24x7 plus Advanced Services Ticket Handling)	1	\$ 525.00	\$ 525.00
0003	FC-10-F100F-210-02-12 FortiGate-100F 1 Year Next Day Delivery Premium RMA Service (Requires 24x7 or ASE FortiCare)	1	\$ 285.00	\$ 285.00

Subtotal	\$2,410.00
Taxable	\$0.00
Tax rate	0.000%
Tax due	\$0.00
Other	\$0.00
TOTAL Due	\$2,410.00

OTHER COMMENTS

FORTINET

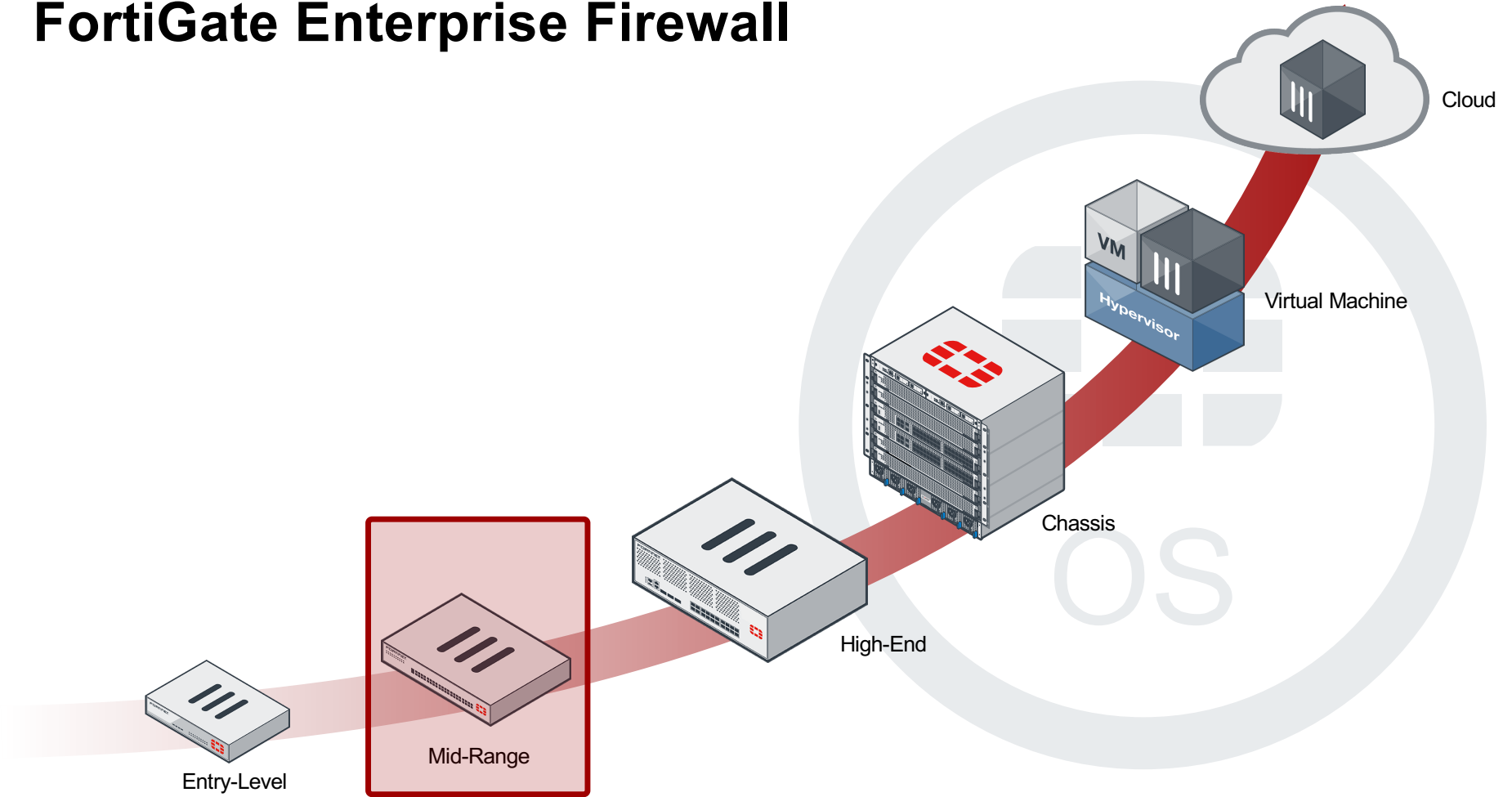
FortiGate Mid-Range Enterprise Firewall

FortiGate 100F

Presented by Jamila Jones-Fleet, Indicium Technology

Presented to : WV Adjutant General

FortiGate Enterprise Firewall



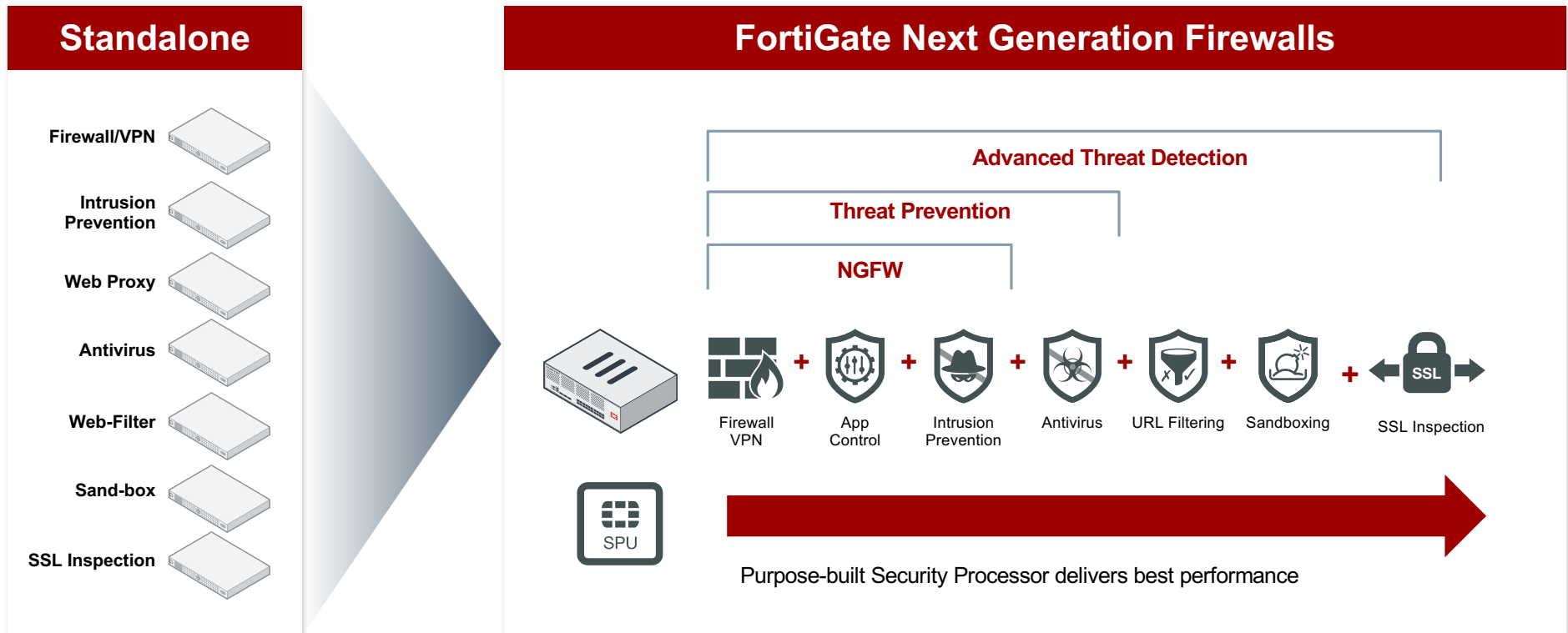
Securing Enterprise Network is Critical Priority



Notes/Sources:

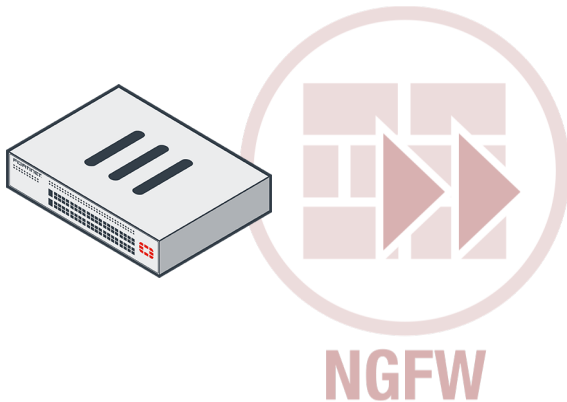
1. Gartner Magic Quadrant for Enterprise Firewall 2016; strategic planning assumptions.
2. Fortinet Threat Landscape Report Q1 2017
3. Gartner Magic Quadrant for Enterprise Firewall 2017; strategic planning assumptions.

Next Generation Firewall with Advanced Threat Detection



Top-rated NGFW with Deep Visibility

FortiGate Mid-Range Next Generation Firewall



Fortinet Key Differentiators

1. **Performance:** Security Processors (SPU) enable parallel path processing and delivers industry's best threat protection and SSL inspection performance
2. **Visibility:** FortiOS reduces complexity by supporting next generation security features and only vendor to provide end to end topology view in addition to applications, users and threats
3. **Security Effectiveness:** FortiGuard threat intelligence delivers best security effectiveness and received four time consecutive NSS Labs NGFW "Recommended" rating

Fortinet Security Fabric

BROAD

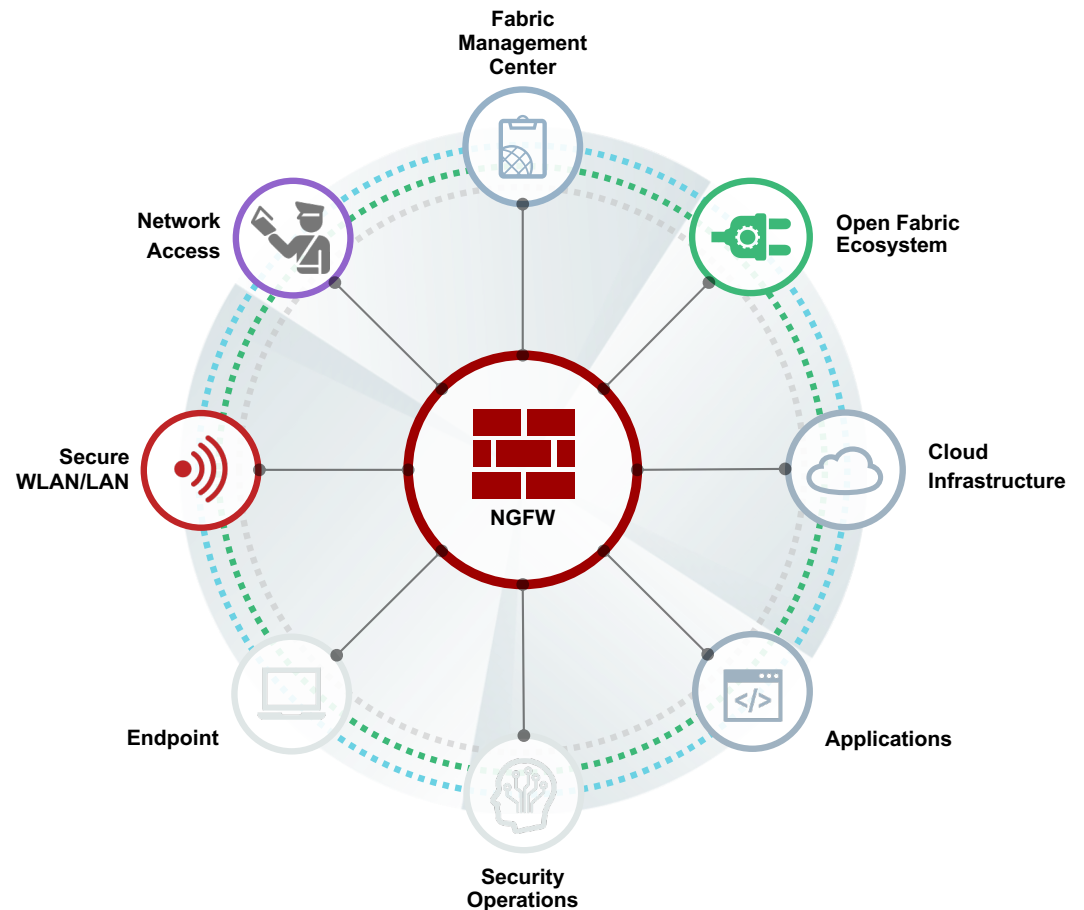
visibility of the entire digital attack surface to better manage risk

INTEGRATED

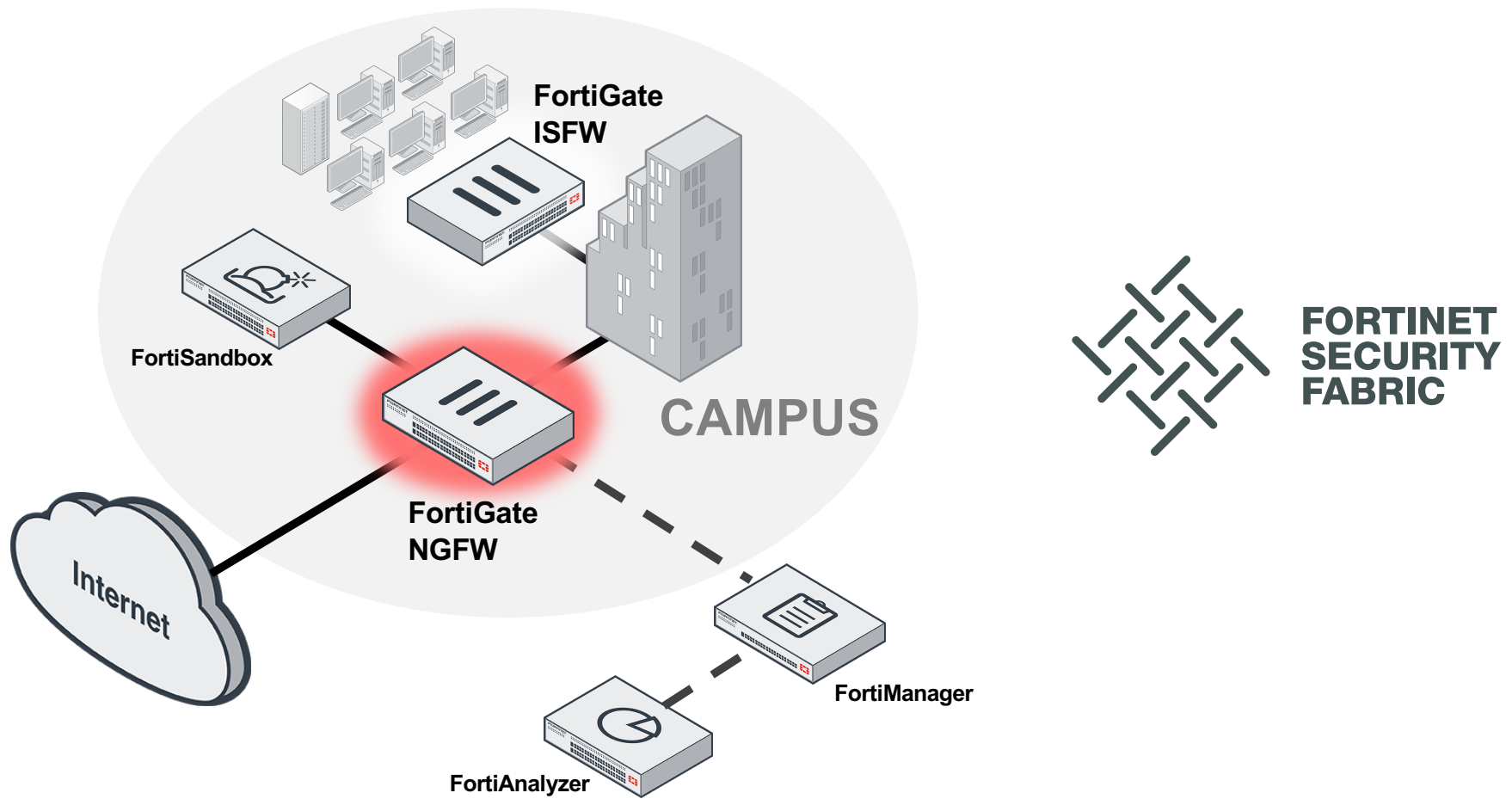
solution that reduces the complexity of supporting multiple point products

AUTOMATED

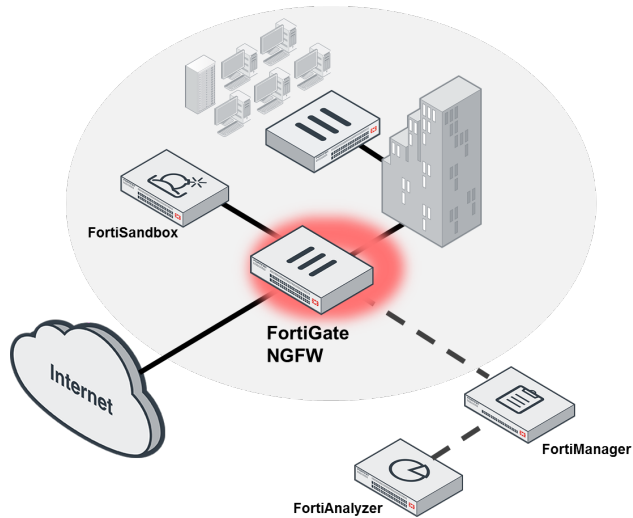
workflows to increase speed of operations and response



FortiGate Deployment at Edge and Internal Segments

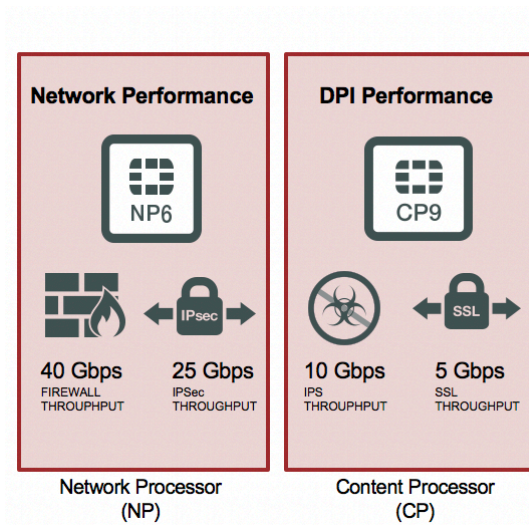






NGFW Use-case



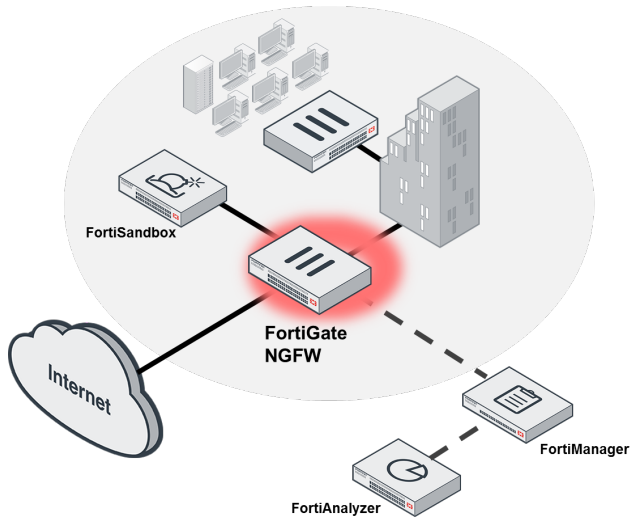
Fortinet Key Differentiator

- Performance:** Security Processors (SPU) enable parallel path processing and delivers industry's best threat protection and SSL inspection performance



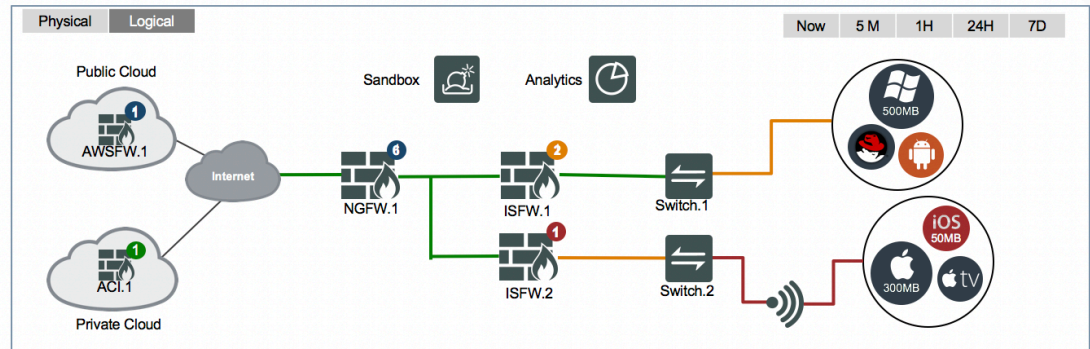
-  **More Performance**
-  **Less Latency**
-  **Less Space**
-  **Less Power**

NGFW Use-case



Fortinet Key Differentiator

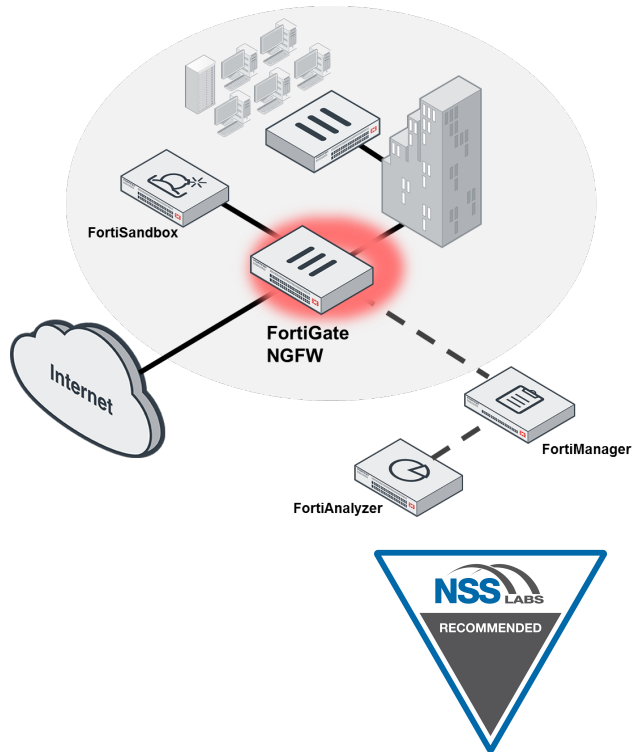
2. **Visibility:** FortiOS reduces complexity by supporting next generation security features and only vendor to provide end to end topology view in addition to applications, users and threats



Network Audit Risk Level	Critical	High	Medium	Low	Passed
Endpoint Vulnerability Score	Critical 100 Points	High 50 Points	Medium 5 Points	Low 2 Points	Info 1 Point



NGFW Use-case



Fortinet Key Differentiator

3. **Security Effectiveness:** FortiGuard threat intelligence delivers best security effectiveness and received four time consecutive NSS Labs NGFW “Recommended” rating

NGFW	2013	2014	2016	2017
Fortinet	Recommended	Recommended	Recommended	Recommended
Palo Alto Networks	Recommended	Caution	Neutral	Caution
Checkpoint	Recommended	Recommended	Recommended	Recommended
Cisco	Recommended	Recommended	Neutral/ Recommended	Recommended
Juniper	Neutral	Did not participate	Neutral	Caution



FortiGate Mid-Range (100 to 900 Series) Product Line



100 and 200 Series

- 7.4 to 20 Gbps Firewall
- 0.36 to 1.8 Gbps NGFW
- 0.25 to 1.2 Gbps TP
- Integrated 1GbE, RPS



300, 400 and 500 Series

- 8 to 16 Gbps Firewall
- 1.7 to 2.5 Gbps NGFW
- 1.5 to 2 Gbps TP
- Integrated 1GbE, RPS



600, 800 and 900 Series

- 36 to 52 Gbps Firewall
- 3.5 Gbps NGFW
- 2.4 Gbps TP
- Integrated 10GbE, 1GbE, RPS

[Refer Product Matrix for up-to date performance numbers and Specification definition](#)

FortiGate Reviews: Gartner and NSS Labs

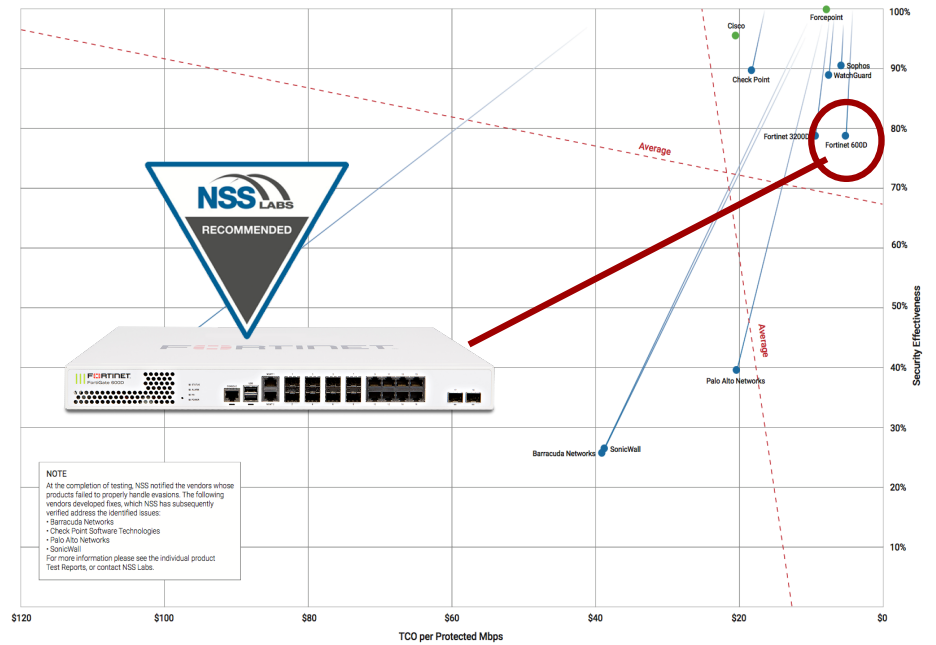
Gartner Enterprise FW MQ 2017: Leader

Figure 1. Magic Quadrant for Enterprise Network Firewalls



Source: Gartner (July 2017)

NSS Labs 2017 NGFW Testing: Recommended

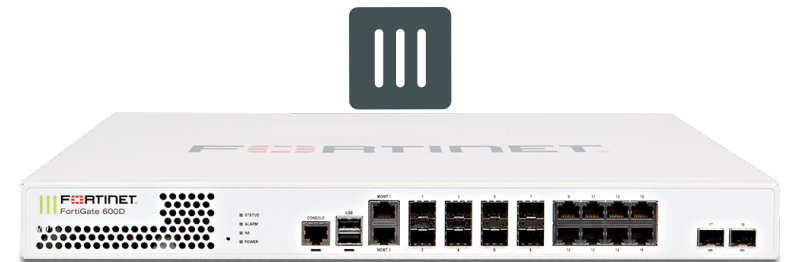


NOTE
 At the completion of testing, NSS notified the vendors whose products failed to properly handle evasions. The following vendors developed fixes, which NSS has subsequently verified address the identified issues:
 - Barracuda Networks
 - Check Point Software Technologies
 - Palo Alto Networks
 - SonicWall
 For more information please see the individual product Test Reports, or contact NSS Labs.

FortiGate Mid-Range (100 to 900 Series) Summary

Next Generation Firewall

- **Industry Leading Performance (SPU)**
 - » Purpose built security processor technology
 - » Enable security without compromising performance
 - » High SSL Inspection performance
- **Security Fabric Visibility and Automation (FortiOS)**
 - » Reduce point products with layered security
 - » Granular visibility of applications, users and devices
 - » Fabric topology view with automated audit recommendation
- **Best Security Effectiveness (FortiGuard)**
 - » 4th Consecutive NGFW NSS Labs “Recommended” rating
 - » Prevent Exploits, Malware and Malicious web-sites
 - » Detect unknown zero day attacks



FortiLink enables Secure Access

FortiLink protocols enable FortiGate to manage Fortinet's network access layer

Simplicity

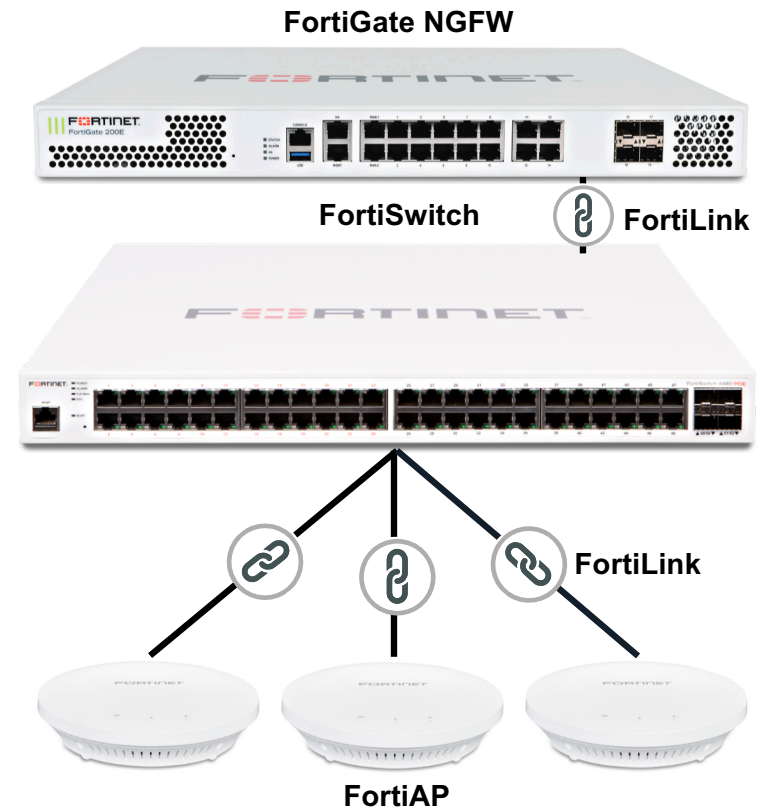
- Flexible architecture, scales as needs change
- Management visibility and analytics across wired, wireless, and security

Security

- » Firewall and switch ports equally secure, SSIDs tied directly to firewall policies
- » Global Security polices down to port and WLAN level

Lower Cost of Ownership

- Access Management included with SD-Branch. No licenses required



Network Access with FortiLink

Manage FortiSwitch Access in the FortiGate GUI

- Security and Access Management through one interface.

Global Security polices

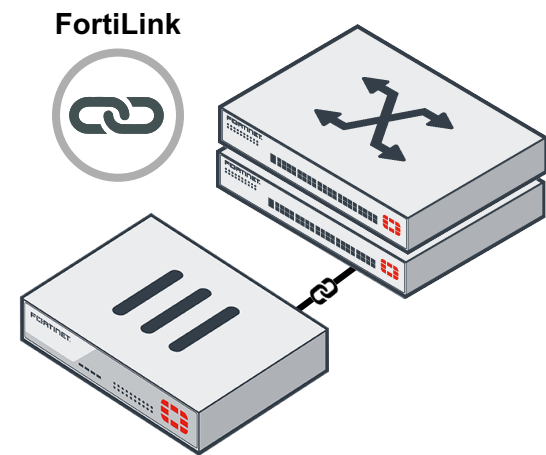
- Same Security Policies and Inspection
- Easy implementation of role base access and control

Simplify Deployment and Provisioning

- Auto discovery
- Device detection

Scalable

- Stack up to 300 switches per FortiGate



No license required. Free.

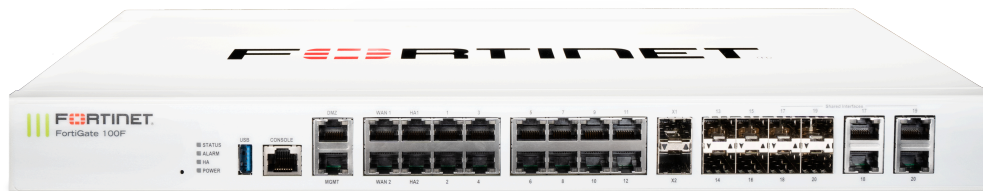


FERTINET®

FortiGate® 100F Series

FortiGate 100F and 101F

Next Generation Firewall
Secure SD-WAN
Secure Web Gateway



The FortiGate 100F series delivers next generation firewall (NGFW) capabilities for mid-sized to large enterprises deployed at the campus or enterprise branch level. Protects against cyber threats with high-powered security processors for optimized network performance, security efficacy and deep visibility. Fortinet’s Security-Driven Networking approach provides tight integration of the network to the new generation of security.

Security

- Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement
- Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic
- Prevents and detects against known attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services
- Proactively blocks unknown sophisticated attacks in real-time with the Fortinet Security Fabric integrated AI-powered FortiSandbox

Performance

- Engineered for Innovation using Fortinet’s purpose-built security processors (SPU) to deliver the industry’s best threat protection performance and ultra-low latency
- Provides industry-leading performance and protection for SSL encrypted traffic including the first firewall vendor to provide TLS 1.3 deep inspection

Certification

- Independently tested and validated best security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs, ICASA, Virus Bulletin, and AV Comparatives

Networking

- Application aware routing with in-built SD-WAN capabilities to achieve consistent application performance and the best user experience
- Built-in advanced routing capabilities to deliver high performance with encrypted IPSEC tunnels at scale

Management

- Includes a management console that is effective and simple to use, which provides a comprehensive network of automation & visibility
- Provides Zero Touch Provisioning leveraging Single Pane of Glass Management powered by the Fabric Management Center
- Predefined compliance checklists analyze the deployment and highlight best practices to improve the overall security posture

Security Fabric

- Enables Fortinet and Fabric-ready partners’ products to provide broader visibility, integrated end-to-end detection, threat intelligence sharing, and automated remediation
- Automatically builds Network Topology visualizations which discover IoT devices and provide complete visibility into Fortinet and Fabric-ready partner products

Firewall	IPS	NGFW	Threat Protection	Interfaces
20 Gbps	2.6 Gbps	1.6 Gbps	1 Gbps	Multiple GE RJ45, GE SFP and 10 GE SFP+ slots

Refer to the specifications table for details

Deployment

Next Generation Firewall (NGFW)

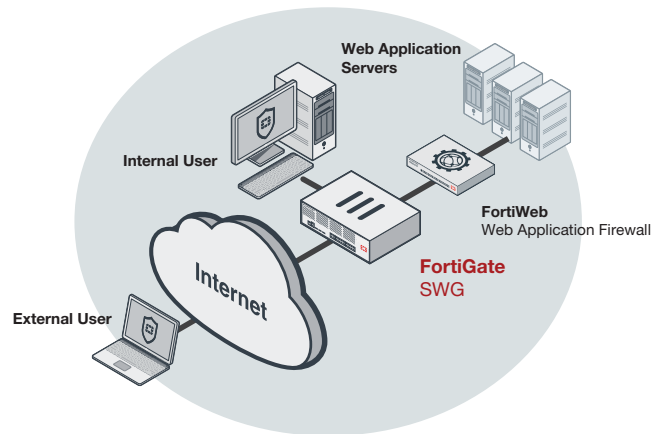
- Reduce the complexity and maximize your ROI by integrating threat protection security capabilities into a single high-performance network security appliance, powered by Fortinet's Security Processing Unit (SPU)
- Full visibility into users, devices, applications across the entire attack surface and consistent security policy enforcement irrespective of asset location
- Protect against network exploitable vulnerabilities with industry-validated IPS that offers low latency and optimized network performance
- Automatically block threats on decrypted traffic using the Industry's highest SSL inspection performance, including the latest TLS 1.3 standard with mandated ciphers
- Proactively block newly discovered sophisticated attacks in real-time with AI-powered FortiGuard Labs and advanced threat protection services included in the Fortinet Security Fabric

Secure SD-WAN

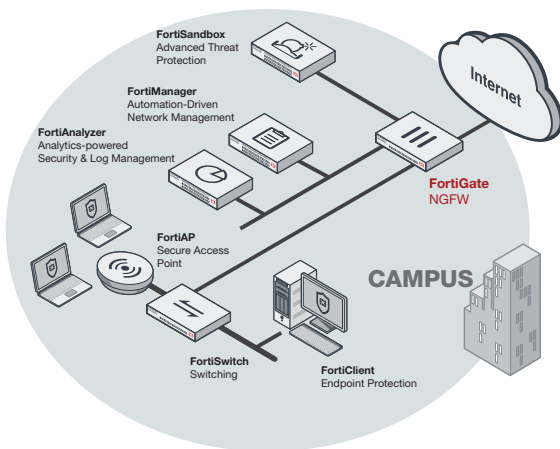
- Consistent business application performance with accurate detection, dynamic WAN path steering and optimization
- Multi-cloud access for faster SaaS adoption with end-to-end optimization
- Simplification with zero touch deployment and centralized management with auto-provisioning, analytics and reporting
- Strong security posture with next generation firewall and real-time threat protection

Secure Web Gateway (SWG)

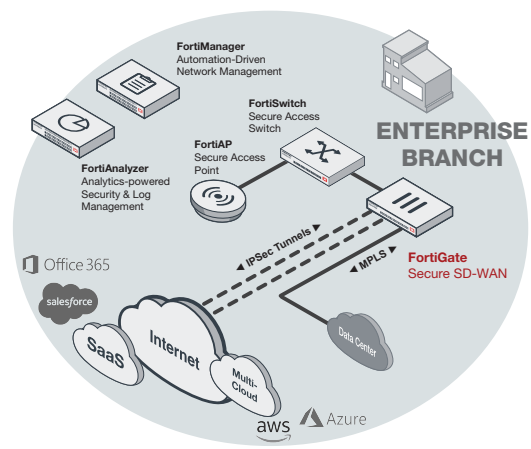
- Secure web access from both internal and external risks, even for encrypted traffic at high performance
- Enhanced user experience with dynamic web and video caching
- Block and control web access based on user or user groups across URL's and domains
- Prevent data loss and discover user activity to known and unknown cloud applications
- Block DNS requests against malicious domains
- Multi-layered advanced protection against zero-day malware threats delivered over the web



FortiGate 100F SWG deployment



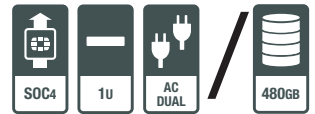
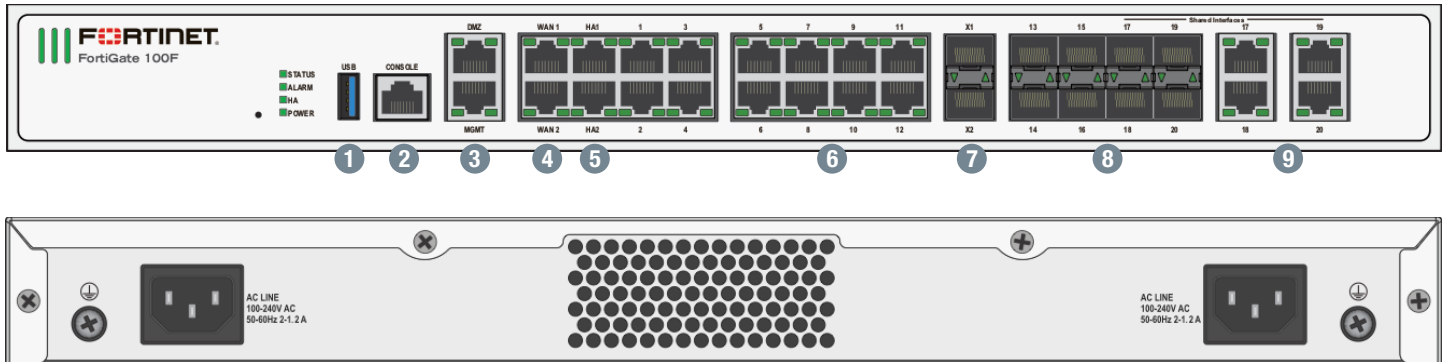
FortiGate 100F deployment in Campus (NGFW)



FortiGate 100F deployment in Enterprise Branch (Secure SD-WAN)

Hardware

FortiGate 100F/101F



Interfaces

- | | |
|---|--|
| <ol style="list-style-type: none"> 1. USB Port 2. Console Port 3. 2x GE RJ45 MGMT/DMZ Ports 4. 2x GE RJ45 WAN Ports 5. 2x GE RJ45 HA Ports | <ol style="list-style-type: none"> 6. 12x GE RJ45 Ports 7. 2x 10 GE SFP+ FortiLink Slots 8. 4x GE SFP Slots 9. 4x GE RJ45/SFP Shared Media Pairs |
|---|--|

Powered by Purpose-built Secure SD-WAN ASIC SOC4



- Combines a RISC-based CPU with Fortinet's proprietary Security Processing Unit (SPU) content and network processors for unmatched performance
- Delivers industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for best user-experience on direct internet access
- Enables best of breed NGFW Security and Deep SSL Inspection with high performance
- Extends security to access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity

Dual Power Supplies

Power supply redundancy is essential in the operation of mission-critical networks. The FortiGate 100F Series offers dual built-in non-hot swappable power supplies.

Extends Security to Access Layer with FortiLink Ports

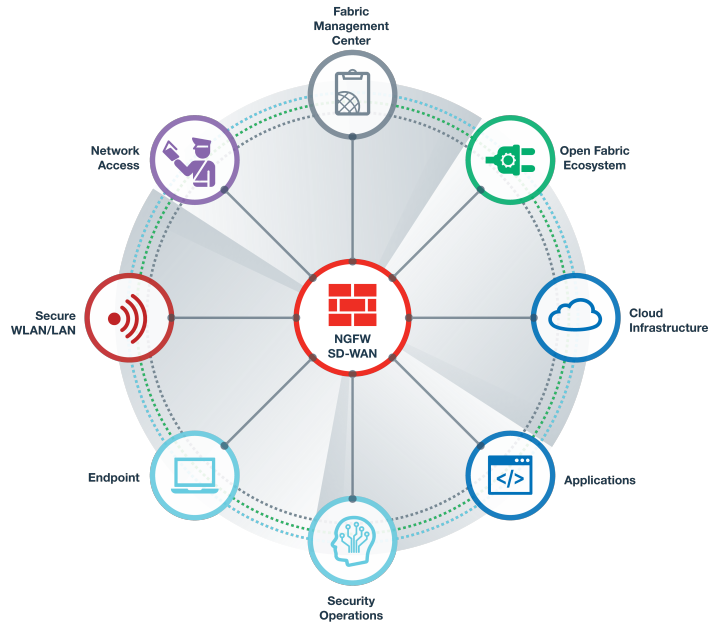
FortiLink protocol enables you to converge security and the network access by integrating the FortiSwitch into the FortiGate as a logical extension of the NGFW. These FortiLink enabled ports can be reconfigured as regular ports as needed.

Fortinet Security Fabric

Security Fabric

The Security Fabric is the cybersecurity platform that enables digital innovations. It delivers broad visibility of the entire attack surface to better manage risk. Its unified and integrated solution reduces the complexity of supporting multiple-point products, while automated workflows increase operational speeds and reduce response times across the Fortinet deployment ecosystem. The Fortinet Security Fabric covers the following key areas under a single management center:

- **Security-Driven Networking** that secures, accelerates, and unifies the network and user experience
- **Zero Trust Network Access** that identifies and secures users and devices in real-time, on and off of the network
- **Dynamic Cloud Security** that protects and controls cloud infrastructures and applications
- **AI-Driven Security Operations** that automatically prevents, detects, isolates, and responds to cyber threats



FortiOS

FortiGates are the foundation of the Fortinet Security Fabric—the core is FortiOS. All security and networking capabilities across the entire FortiGate platform are controlled with one intuitive operating system. FortiOS reduces complexity, costs, and response times by truly consolidating next-generation security products and services into one platform.

- A truly consolidated platform with a single OS and pane-of-glass for across the entire digital attack surface.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives, and ICSA validated security and performance.
- Leverage the latest technologies such as deception-based security.

Services



FortiGuard Labs offer real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet’s solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world’s leading threat monitoring organizations and other network and security vendors, as well as law enforcement agencies.



Our FortiCare customer support team provides global technical support for all Fortinet products. With support staff in the Americas, Europe, Middle East, and Asia, FortiCare offers services to meet the needs of enterprises of all sizes.



For more information, please refer to forti.net/fortiguard and forti.net/forticare

Specifications

	FORTIGATE 100F	FORTIGATE 101F
Hardware Specifications		
GE RJ45 Ports		12
GE RJ45 Management/HA/DMZ Ports		1 / 2 / 1
GE SFP Slots		4
10 GE SFP+ Slots		2
GE RJ45 WAN Ports		2
GE RJ45 or SFP Shared Ports *		4
USB Port		1
Console Port		1
Internal Storage	—	1x 480 GB SSD
Included Transceivers		0
System Performance — Enterprise Traffic Mix		
IPS Throughput ²		2.6 Gbps
NGFW Throughput ^{2,4}		1.6 Gbps
Threat Protection Throughput ^{2,5}		1 Gbps
System Performance		
Firewall Throughput (1518 / 512 / 64 byte UDP packets)		20 / 18 / 10 Gbps
Firewall Latency (64 byte UDP packets)		5 µs
Firewall Throughput (Packets Per Second)		15 Mpps
Concurrent Sessions (TCP)		1.5 Million
New Sessions/Second (TCP)		56,000
Firewall Policies		10,000
IPsec VPN Throughput (512 byte) ¹		11.5 Gbps
Gateway-to-Gateway IPsec VPN Tunnels		2,500
Client-to-Gateway IPsec VPN Tunnels		16,000
SSL-VPN Throughput		1 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)		500
SSL Inspection Throughput (IPS, avg. HTTPS) ³		1 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) ³		1,800
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³		135,000
Application Control Throughput (HTTP 64K) ²		2.2 Gbps
CAPWAP Throughput (HTTP 64K)		15 Gbps
Virtual Domains (Default / Maximum)		10 / 10
Maximum Number of FortiSwitches Supported		24
Maximum Number of FortiAPs (Total / Tunnel Mode)		128 / 64
Maximum Number of FortiTokens		5,000
High Availability Configurations		Active / Active, Active / Passive, Clustering

	FORTIGATE 100F	FORTIGATE 101F
Dimensions		
Height x Width x Length (inches)	1.73 x 17 x 10	
Height x Width x Length (mm)	44 x 432 x 254	
Form Factor (supports EIA / non-EIA standards)	Rack Mount, 1 RU	
Weight	7.25 lbs (3.29 kg)	7.56 lbs (3.43 kg)
Environment		
Power Required	100–240V AC, 50-60	
Maximum Current	100V / 1A, 240V / 0.5A	
Power Consumption (Average / Maximum)	35.1 W / 38.7 W	35.3 W / 39.1 W
Heat Dissipation	119.77 BTU/h	121.13 BTU/h
Redundant Power Supplies	Yes	
Environment		
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Operating Altitude	Up to 7,400 ft (2,250 m)	
Humidity	10–90% non-condensing	
Noise Level	40.4 dBA	
Compliance	FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL, CB, BSMI	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; IPv6	

* Copper SFP module is not supported.

Note: All performance values are "up to" and vary depending on system configuration.

1. IPsec VPN performance test uses AES256-SHA256.
2. IPS (Enterprise Mix), Application Control, NGFW, and Threat Protection are measured with Logging enabled.
3. SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

4. NGFW performance is measured with Firewall, IPS, and Application Control enabled.
5. Threat Protection performance is measured with Firewall, IPS, Application Control, and Malware Protection enabled.

Order Information

Product	SKU	Description
FortiGate 100F	FG-100F	22x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 1x Mgmt port, 2x HA ports, 16x switch ports with 4 SFP port shared media), 4 SFP ports, 2x 10 GE SFP+ FortiLinks, dual power supplies redundancy
FortiGate 101F	FG-101F	22x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 1x Mgmt port, 2x HA ports, 16x switch ports with 4 SFP port shared media), 4 SFP ports, 2x 10 GE SFP+ FortiLinks, 480GB onboard storage, dual power supplies redundancy
Optional Accessories		
1 GE SFP LX transceiver module	FG-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots
1 GE SFP RJ45 transceiver module	FG-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots
1 GE SFP SX transceiver module	FG-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots
10 GE SFP+ transceiver module, short range	FG-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots

Bundles



FortiGuard Bundle

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 one of these FortiGuard Bundles.

Bundles	360 Protection	Enterprise Protection	Unified Threat Protection	Threat Protection
FortiCare	ASE ¹	24x7	24x7	24x7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web Filtering Service	•	•	•	•
FortiGuard Antispam Service	•	•	•	•
FortiGuard Security Rating Service	•	•	•	•
FortiGuard Industrial Service	•	•	•	•
FortiGuard IoT Detection Service ²	•	•	•	•
FortiConverter Service	•	•	•	•
IPAM Cloud ²	•	•	•	•
SD-WAN Orchestrator Entitlement ²	•	•	•	•
SD-WAN Cloud Assisted Monitoring	•	•	•	•
SD-WAN Overlay Controller VPN Service	•	•	•	•
FortiAnalyzer Cloud	•	•	•	•
FortiManager Cloud	•	•	•	•

1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 6.4