## 1. Oceněný výkaz výměr

| Výrobce | Obj. číslo | Popis | množ. | MJ | Kč/jedn. | Kč celkem |
|---|---|---|---|---|---|---|
| **NGFW typ 1** | | | | | | |
| Fortinet | | 7x 1Gbps intemí Ethernet port, 2x 1Gbps WAN porty, 1x 1Gbps DMZ port, datová propustnost bez aktivovaných bezpečnostních funkcí 2 Gbps, počet nových relací za sekundu 20000, počet současně aktivních relací1 mil., datová propustnost Ipsec VPN 1,5 Gbps | 2 | ks | 23 813 Kč | 47 626 Kč |
| Fortinet | | Servisní podpora na 1 rok 8x5, vč. updatů UTM funkcí (viz Technická specifikace díla - požadované funkcionality NGFW typ 1 / typ 2) | 2 | ks | 10 061 Kč | 20 122 Kč |
| **NGFW typ 2** | | | | | | |
| Fortinet | | 4x 1Gbps intemí Ethernet port, 1x 1Gbps WAN porty, datová propustnost bez aktivovaných bezpečnostních funkcí 800 Mbps, počet nových relací za sekundu 10000, počet současně aktivních relací 800000, datová propustnost Ipsec VPN 65 Mbps | 2 | ks | 10 240 Kč | 20 480 Kč |
| Fortinet | | Servisní podpora na 1 rok 8x5, vč. updatů UTM funkcí (viz Technická specifikace díla - požadované funkcionality NGFW typ 1 / typ 2) | 2 | ks | 6 656 Kč | 13 312 Kč |
| **Celkem NGFW typ 1 a 2** | | | | | | **101 540 Kč** |
| | | | | | | |
| **Instalace a konfigurace dle předaných podkladů v lokalitách** | | | | | | |
| | | Obchodní zóna Otvice | 1 | kpl | 21 000 Kč | 21 000 Kč |
| | | AN Chomutov | 1 | kpl | 21 000 Kč | 21 000 Kč |
| | | AN Jirkov | 1 | kpl | 42 000 Kč | 42 000 Kč |
| **Celkem instalace, konfigurace a zaškolení** | | | | | | **84 000 Kč** |
| | | | | | | |
| | | Celkem HW (firewally) | | | | 101540 |
| | | Celkem instalace a konfigurace | | | | 84000 |
| **Celkem dodávka firewallů** | | | | | | **185 540 Kč** |

## 4. Věcná část nabídky

**VĚCNÁ NABÍDKA (ZÁVAZNÝ VZOR)**

| NABÍZENÉ TECHNICKÉ ŘEŠENÍ MUSÍ SPLŇOVAT MINIMÁLNĚ NÍŽE UVEDENÉ POVINNÉ TECHNICKÉ PARAMETRY A FUNKCIONALITY | | SPLNĚNÍ POŽADOVANÝCH TECHNICKÝCH PARAMETRŮ | Kde je parametr uchazečem uveden |
|---|---|---|---|
| | | ANO / NE | Číslo str. nabídky |
| **NGFW typ 1** | | | |
| **Technické provedení bezpečnostního prvku** | | | |
| Parametr 1 | Provedení do racku 19“ včetně dodání montážních prvků, nebo dodání police pro montáž do racku 19“ | ANO | 90 |
| Parametr 2 | Maximální obsazená výška 1U (včetně případné police), maximální hloubka 600mm | ANO | 37 |
| Parametr 3 | Min 7x 1Gbps interní Ethernet port | ANO | 37 |
| Parametr 4 | 1x port management konzole | ANO | 37 |
| Parametr 5 | Min. 2x 1Gbps WAN Ethernet port | ANO | 37 |
| Parametr 6 | Min. 1x 1Gbps DMZ Ethernet port | ANO | 37 |
| **NGFW typ 2** | | | |
| Parametr 1 | Provedení do racku 19“ včetně dodání montážních prvků, nebo dodání police pro montáž do racku 19“ | ANO | 90 |
| Parametr 2 | Maximální obsazená výška 1U (včetně případné police), maximální hloubka 600mm | ANO | 43 |
| Parametr 3 | Min 4x 1Gbps interní Ethernet port | ANO | 43 |
| Parametr 4 | 1x port management konzole | ANO | 43 |
| Parametr 5 | Min. 1 x 1Gbps WAN Ethernet port | ANO | 43 |
| | | | |
| **Požadované funkcionality NGFW typ 1 / typ 2** | | | |
| Parametr 1 | Next Generation Firewall (NGFW) s hloubkovou analýzou paketů (DPI) | ANO | 37,43 |
| Parametr 2 | Antivirus (AV, včetně skenování archivních souborů) | ANO | 37,43 |
| Parametr 3 | Intrusion Prevention Systém (IPS) | ANO | 37,43 |
| Parametr 4 | Application Controll Systém (ACS, včetně kategorizace aplikací) | ANO | 36,42 |
| Parametr 5 | Antispam (AS, s možností přidávání vlastních pravidel, whitelist/blacklist) | ANO | 38,44 |

| | | | |
|---|---|---|---|
| Parametr 6 | Filtrování obsahu internetových stránek na základě jejich kategorizace | ANO | 38,44 |
| Parametr 7 | Kontrola obsahu zabezpečených protokolů | ANO | 37,43 |
| Parametr 8 | Automatická a bezobslužná aktualizace lokálních databází bezpečnostních komponent | ANO | 36, 42 |
| **Výkonové parametry NGFW typ 1** | | | |
| Váhově hodnocený parametr 1 | Datová propustnost bezpečnostního prvku bez aktivovaných bezpečnostních funkcí. | 3 Gbps | 33 |
| *Uchazeč uvede do sloupce „SPLNĚNÍ POŽADOVANÝCH TECHNICKÝCH PARAMETRŮ“ hodnotu datové propustnosti jím navrženého bezpečnostního prvku při velikosti paketů 1518, 512 a 64 byte UDP měřenou dle metodiky RFC 2544. Minimální přípustná hodnota je 2 Gbps.*<br><br>*Uchazeči obdrží počet bodů odpovídající poměru jimi nabízené hodnoty k hodnotě, kterou nabízí uchazeč s nejvyšší hodnotu tohoto parametru., To celé je násobeno maximálním možným počtem bodů pro tento parametr (20 bodů).*<br><br>*Počet bodů uchazeče = 20 * (Uchazečem nabízená hodnota / Nejvyšší nabízená hodnota)*<br><br>*Uchazeči, který ze všech uchazečů nabídne nejvyšší hodnotu tohoto parametru bude přidělen nejvyšší počet bodů.* | | | |
| Váhově hodnocený parametr 2 | Počet nových relací za sekundu | 30000 | 37 |
| *Uchazeč uvede do sloupce „SPLNĚNÍ POŽADOVANÝCH TECHNICKÝCH PARAMETRŮ“ hodnotu počtu nových relací za sekundu, které je bezpečnostní prvek schopen založit. Minimální přípustná hodnota tohoto parametru je 20000 rel/s.*<br><br>*Uchazeči obdrží počet bodů odpovídající poměru jimi nabízené hodnoty k hodnotě, kterou nabízí uchazeč s nejvyšší hodnotu tohoto parametru. To celé je násobeno maximálním možným počtem bodů pro tento parametr (10 bodů).*<br><br>*Počet bodů uchazeče = 10 * (Uchazečem nabízená hodnota / Nejvyšší nabízená hodnota)*<br><br>*Uchazeči, který ze všech uchazečů nabídne nejvyšší hodnotu tohoto parametru bude přidělen nejvyšší počet bodů.* | | | |
| Váhově hodnocený parametr 3 | Počet současně aktivních relací | 1,3 mil. | 37 |

| | | | |
|---|---|---|---|
| *Uchazeč uvede do sloupce „SPLNĚNÍ POŽADOVANÝCH TECHNICKÝCH PARAMETRŮ“ hodnotu počtu relací, které je bezpečnostní prvek schopen udržet. Minimální přípustná hodnota tohoto parametru je 1 mil. rel.*<br><br>*Uchazeči obdrží počet bodů odpovídající poměru jimi nabízené hodnoty k hodnotě, kterou nabízí uchazeč s nejvyšší hodnotu tohoto parametru. To celé je násobeno maximálním možným počtem bodů pro tento parametr (10 bodů).*<br><br>*Počet bodů uchazeče = 10 * (Uchazečem nabízená hodnota / Nejvyšší nabízená hodnota)*<br><br>*Uchazeči, který ze všech uchazečů nabídne nejvyšší hodnotu tohoto parametru bude přidělen nejvyšší počet bodů.* | | | |
| Váhově hodnocený parametr 4 | Datová propustnost IPSec VPN | 2 Gbps | 37 |
| *Uchazeč uvede do sloupce „SPLNĚNÍ POŽADOVANÝCH TECHNICKÝCH PARAMETRŮ“ hodnotu datové propustnosti IPSec VPN při velikosti paketů 512 byte. Minimální přípustná hodnota parametru je 1,5 Gbps.*<br><br>*Uchazeči obdrží počet bodů odpovídající poměru jimi nabízené hodnoty k hodnotě, kterou nabízí uchazeč s nejvyšší hodnotu tohoto parametru., To celé je násobeno maximálním možným počtem bodů pro tento parametr (20 bodů).*<br><br>*Počet bodů uchazeče = 20 * (Uchazečem nabízená hodnota / Nejvyšší nabízená hodnota)*<br><br>*Uchazeči, který ze všech uchazečů nabídne nejvyšší hodnotu tohoto parametru bude přidělen nejvyšší počet bodů.* | | | |
| **Výkonové parametry NGFW typ 2** | | | |
| Váhově hodnocený parametr 1 | Datová propustnost bezpečnostního prvku bez aktivovaných bezpečnostních funkcí. | 950 Mbps | 37 |
| *Uchazeč uvede do sloupce „SPLNĚNÍ POŽADOVANÝCH TECHNICKÝCH PARAMETRŮ“ hodnotu datové propustnosti jím navrženého bezpečnostního prvku při velikosti paketů 1518, 512 a 64 byte UDP měřenou dle metodiky RFC 2544. Minimální přípustná hodnota je 800Mbps.*<br><br>*Uchazeči obdrží počet bodů odpovídající poměru jimi nabízené hodnoty k hodnotě, kterou nabízí uchazeč s nejvyšší hodnotu tohoto parametru., To celé je násobeno maximálním možným počtem bodů pro tento parametr (15 bodů).*<br><br>*Počet bodů uchazeče = 15 * (Uchazečem nabízená hodnota / Nejvyšší nabízená hodnota)*<br><br>*Uchazeči, který ze všech uchazečů nabídne nejvyšší hodnotu tohoto parametru bude přidělen nejvyšší počet bodů.* | | | |
| Váhově hodnocený parametr 2 | Počet nových relací za sekundu | 15000 | 43 |

| | | | |
|---|---|---|---|
| *Uchazeč uvede do sloupce „SPLNĚNÍ POŽADOVANÝCH TECHNICKÝCH PARAMETRŮ“ hodnotu počtu nových relací za sekundu, které je bezpečnostní prvek schopen založit. Minimální přípustná hodnota tohoto parametru je 10000 rel/s.*<br><br>*Uchazeči obdrží počet bodů odpovídající poměru jimi nabízené hodnoty k hodnotě, kterou nabízí uchazeč s nejvyšší hodnotu tohoto parametru. To celé je násobeno maximálním možným počtem bodů pro tento parametr (5 bodů).*<br><br>*Počet bodů uchazeče = 5 * (Uchazečem nabízená hodnota / Nejvyšší nabízená hodnota)*<br><br>*Uchazeči, který ze všech uchazečů nabídne nejvyšší hodnotu tohoto parametru bude přidělen nejvyšší počet bodů.* | | | |
| Váhově hodnocený parametr 3 | Počet současně aktivních relací | 900000 | 43 |
| *Uchazeč uvede do sloupce „SPLNĚNÍ POŽADOVANÝCH TECHNICKÝCH PARAMETRŮ“ hodnotu počtu relací, které je bezpečnostní prvek schopen udržet. Minimální přípustná hodnota tohoto parametru je 800000 rel.*<br><br>*Uchazeči obdrží počet bodů odpovídající poměru jimi nabízené hodnoty k hodnotě, kterou nabízí uchazeč s nejvyšší hodnotu tohoto parametru. To celé je násobeno maximálním možným počtem bodů pro tento parametr (5 bodů).*<br><br>*Počet bodů uchazeče = 5 * (Uchazečem nabízená hodnota / Nejvyšší nabízená hodnota)*<br><br>*Uchazeči, který ze všech uchazečů nabídne nejvyšší hodnotu tohoto parametru bude přidělen nejvyšší počet bodů.* | | | |
| Váhově hodnocený parametr 4 | Datová propustnost IPSec VPN | 75 Mbps | 43 |
| *Uchazeč uvede do sloupce „SPLNĚNÍ POŽADOVANÝCH TECHNICKÝCH PARAMETRŮ“ hodnotu datové propustnosti IPSec VPN při velikosti paketů 512 byte. Minimální přípustná hodnota parametru je 65 Mbps.*<br><br>*Uchazeči obdrží počet bodů odpovídající poměru jimi nabízené hodnoty k hodnotě, kterou nabízí uchazeč s nejvyšší hodnotu tohoto parametru., To celé je násobeno maximálním možným počtem bodů pro tento parametr (15 bodů).*<br><br>*Počet bodů uchazeče = 15 * (Uchazečem nabízená hodnota / Nejvyšší nabízená hodnota)*<br><br>*Uchazeči, který ze všech uchazečů nabídne nejvyšší hodnotu tohoto parametru bude přidělen nejvyšší počet bodů.* | | | |
| **Sledování provozu a ukládání záznamů o provozu NGFW typ 1 / typ 2** | | | |

| | | | |
|---|---|---|---|
| Parametr 1 | Ukládání záznamů o stavu bezpečnostního prvku a datovém provozu procházejícím bezpečnostním prvkem bude prováděno lokálně, externím zařízením, nebo externí službou s tím, že musí existovat možnost, jak v budoucnu ukládat záznamy ze všech lokalit centrálně. Externí službou může být např. cloud výrobce. Systém pro centrální ukládání záznamů není předmětem této zakázky. | ANO | 45-60 |
| Parametr 2 | Systém pro sledování provozu bude mít možnost ukládat všechny události, nikoli pouze chyby, výstrahy, incidenty, porušení pravidel atd. | ANO | 61 |
| **Podrobně sledována budou** | | | |
| Parametr 1 | Veškerá rozhraní pevných i bezdrátových sítí | ANO | 46 |
| Parametr 2 | Veškeré funkce bezpečnostního prvku | ANO | 62-65 |
| Parametr 3 | Správa a stav zařízení | ANO | 66 |
| Parametr 4 | Přihlašování uživatelů do VPN a počítačové sítě (integrace s AD, SSO, …) | ANO | 76 |
| **Pro monitoring datového provozu a bezpečnostních funkcionalit budou ukládány minimálně tyto údaje** | | | |
| Parametr 1 | Datum a čas | ANO | 80-83 |
| Parametr 2 | Identifikátor zařízení | ANO | 80-83 |
| Parametr 3 | Zdrojové/cílové rozhraní | ANO | 80-83 |
| Parametr 4 | Zdrojová/cílová IP adresa | ANO | 80-83 |
| Parametr 5 | Zdrojový/cílový port | ANO | 80-83 |
| Parametr 6 | Služba (HTTP, FTP, SSH, …) | ANO | 80-83 |
| Parametr 7 | Uživatel (pokud je autentifikován) | ANO | 84 |
| Parametr 8 | Bezpečnostní akce (povoleno/zakázáno) | ANO | 80-83 |
| Parametr 9 | Identifikátor pravidla, na základě jehož vyhodnocení byla provedena bezpečnostní akce | ANO | 80-83 |
| Parametr 10 | Údaje specifické jednotlivým bezpečnostním funkcionalitám a zachyceným událostem | ANO | 80-83 |
| **Pro monitoring přihlašování uživatelů budou ukládány minimálně tyto údaje** | | | |
| Parametr 1 | Datum a čas | ANO | 84 |

| | | | |
|---|---|---|---|
| Parametr 2 | Identifikátor uživatele (např. login name, display name, …) | ANO | 84 |
| Parametr 3 | Identifikátor stanice, z níž proběhlo přihlášení (např. IP adresa, nebo hostname) | ANO | 84 |
| **Monitoring systému a stavu bezpečnostního prvku bude poskytovat lokálně minimálně tyto informace** | | | |
| Parametr 1 | Stav HW, doba provozu, kapacity, vytížení, překročení, atd. | ANO | 85 |
| Parametr 2 | Stav SW, aktualizace | ANO | 85 |
| Parametr 3 | Chyby a výstrahy | ANO | 85 |
| **Podpora IPv6** | | | |
| Parametr 1 | Plná podpora IPv6 pro všechny bezpečnostní funkce | ANO | 86 |
| Parametr 2 | Podpora IPv6 směrovacích a bezpečnostních politik | ANO | 86 |
| Parametr 3 | Dual stack routing | ANO | 86 |
| Parametr 4 | ICMPv6, DHCPv6 | ANO | 87 |
| Parametr 5 | IPv6 IPSec VPN | ANO | 78 |
| **Podpora VPN** | | | |
| Parametr 1 | Podpora „Site to Site“ IPSec VPN | ANO | 37,43 |
| Parametr 2 | Podpora „Client to Site“ IPSec VPN, nebo SSL VPN | ANO | 37,43 |
| Parametr 3 | Kontrola datového toku z VPN pomocí funkcí bezpečnostního prvku | ANO | 37,43 |
| **Další požadované vlastnosti bezpečnostního prvku** | | | |
| Parametr 1 | Podpora QoS | ANO | 75 |
| Parametr 2 | Podpora VLAN (802.1Q) | ANO | 78 |
| Parametr 3 | Podpora zabezpečení přístupu do počítačové sítě (802.1X) | ANO | 76 |
| Parametr 4 | Podpora autentizace založené na protokolu RADIUS | ANO | 76 |
| Parametr 5 | Podpora autentizace založené na integraci s Active Directory (SSO) | ANO | 76 |
| Parametr 6 | Podpora autentizace zařízení prostřednictvím RADIUS serveru pomocí MAC adresy | ANO | 77 |

| | | | |
|---|---|---|---|
| Parametr 7 | Podpora řízení průtoku dat (rate limiting, traffic shaping apod.) | ANO | 78 |
| Parametr 8 | Podpora SNMP | ANO | 76 |
| **Kvalita a záruka** | | | |
| Parametr 1 | Minimální záruční doba na aktivní prvky – 12 měsíců | ANO | 3, 32 |
| Parametr 4 | Školení administrátora (operátora) v místě sídla zadavatele | ANO | 32 |
| Parametr 5 | Školení administrátora (operátora) v českém jazyce | ANO | 32 |

## 5. Doplňující informace k nabídce

1. Nedílnou součástí této nabídky je příloha, která obsahuje technické listy k navrhovaným zařízením, a části technické dokumentace výrobce, společnosti Fortinet, v rozsahu 58 stran, ve, které jsou vzestupně očíslovány nepřerušenou řadou s čísly stran 33-90. Tato část nabídky je prokázáním všech parametrů, které jsou uvedeny a požadovány v příloze p05_vecna_nabidka.docx, která je součástí zadávací dokumentace.
2. Prokázání technické kvalifikace členů je uvedeno v prohlášení výrobce, společnosti Fortinet, které je nedílnou součástí této nabídky (strana 13) a nahrazuje certifikáty výrobce nabízené technologie.
3. Potvrzujeme, že záruční doba na aktivní prvky je 12 měsíců.
4. Potvrzujeme, že součástí nabídky je školení administrátora (operátora) v místě sídla zadavatele. Školení bude provedeno v českém jazyce.

V Chomutově, 12.7.2019

DataSOFT spol. s r.o.
Informační systémy
Kadaňská 2226, 430 03 Chomutov
tel.: +420-474-624223, tel./ fax: +420-474-629110
IČ: 47310405 DIČ: CZ47310405
2

……..

Ing. Zdeněk Honska, jednatel

DATA SHEET

# FortiGate/FortiWiFi® 60E Series

FortiGate 60E, 60E-POE, FortiWiFi 60E, FortiGate 61E and FortiWiFi 61E

**Secure SD-WAN**
**Unified Threat Management**


The FortiGate 60E series offers an excellent Security and SD-WAN solution in a compact fanless desktop form factor for enterprise branch offices and mid-sized businesses. Protect against cyber threats with industry-leading secure SD-WAN in a simple, affordable and easy to deploy solution.

### 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
- Prevent and detect against known and unknown attacks using continuous threat intelligence from AI powered FortiGuard Labs security services

### Performance

- Delivers industry's best threat protection performance and ultra-low latency using purpose-built security processor (SPU) technology
- Provides industry-leading performance and protection for SSL encrypted traffic

### Certification

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

### Networking

- Best of Breed SD-WAN capabilities to enable application steering using WAN path control for high quality of experience
- Delivers extensive routing, switching, wireless controller, high-performance, and scalable IPsec VPN capabilities

### Management

- Includes Management Console that's effective, simple to use, and provides comprehensive network automation & visibility.
- Provides Zero Touch Integration with Security Fabric's Single Pane of Glass Management
- Predefined compliance checklist analyzes the deployment and highlights best practices to improve 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 |
|---|---|---|---|---|
| **3 Gbps** | **400 Mbps** | **250 Mbps** | **200 Mbps** | Multiple GE RJ45 \| WiFi variants \| Variants with internal storage \| Variants with PoE/+ interfaces |

Refer to specification table for details

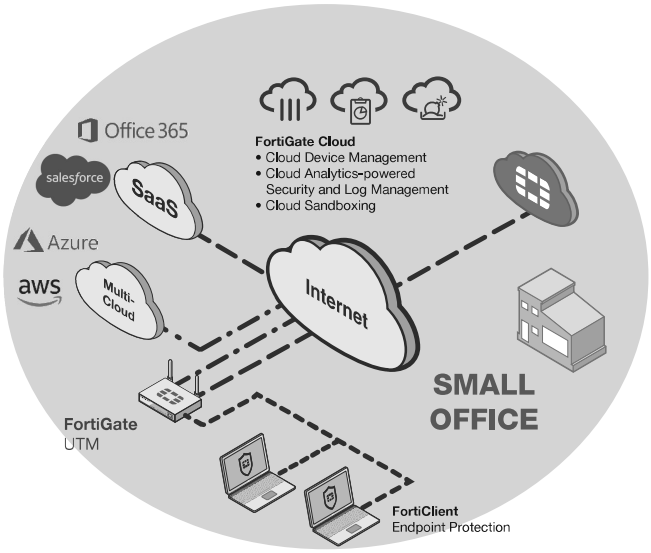
# Deployment

## Unified Threat Management (UTM)

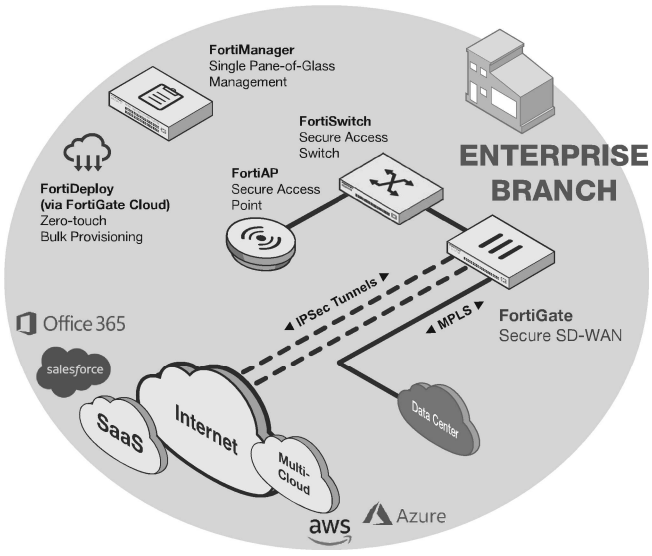
- Integrated wired and wireless networking to simplify IT
- Purpose-built hardware for industry best performance with easy administration through cloud management
- Provides consolidated security and networking for small businesses and consistently provides top-rated threat protection
- Proactively blocks newly discovered sophisticated attacks in real-time with advanced threat protection

## Secure SD-WAN

- Secure direct Internet access for Cloud Applications for improved latency and reduce WAN cost spending
- High-performance and cost-effective threat protection capabilities
- WAN Path Controller and Link Health Monitoring for better application performance and quality of experience
- Security Processer powered industry's best IPsec VPN and SSL Inspection performance
- Simplified Management and Zero Touch deployment



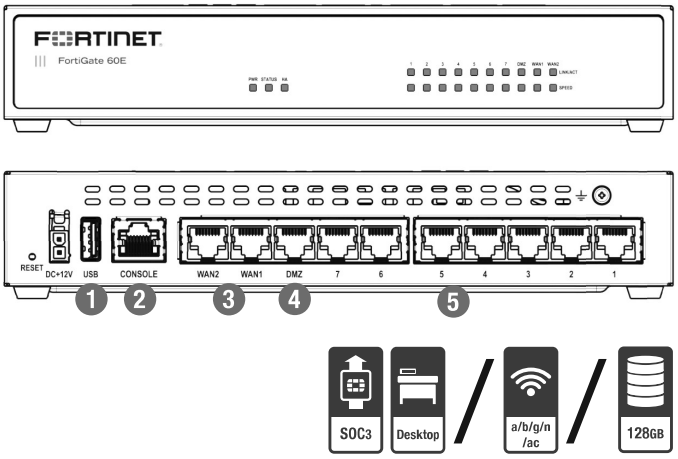

FortiWiFi 60E deployment in Small Office (UTM)




FortiGate 60E deployment in Enterprise Branch (Secure SD-WAN)

# Hardware

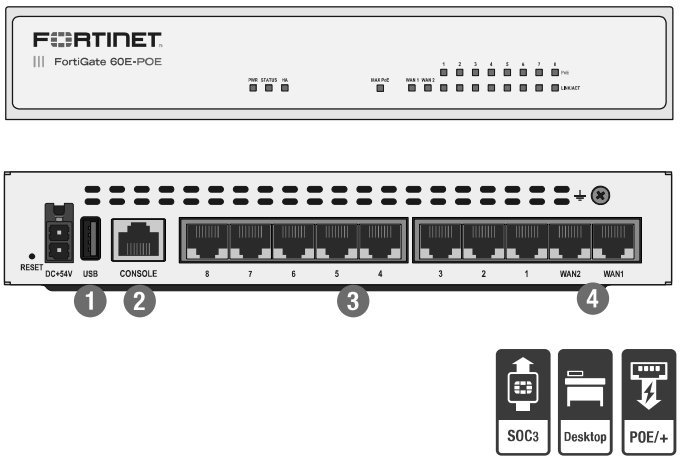
## FortiGate/FortiWiFi 60E/61E




### Interfaces

1. USB Port
2. Console Port
3. 2x GE RJ45 WAN Ports
4. 1x GE RJ45 DMZ Ports
5. 7x GE RJ45 Internal Ports

## FortiGate 60E-POE




### Interfaces

1. USB Port
2. Console Port
3. 8x GE RJ45 PoE/+ Ports
4. 2x GE RJ45 WAN Ports

### Powered by SPU SoC3


- Combines a RISC-based CPU with Fortinet's proprietary SPU content and network processors for unmatched performance
- Simplifies appliance design and enables breakthrough performance for smaller networks
- Supports firewall acceleration across all packet sizes for maximum throughput
- Delivers accelerated UTM content processing for superior performance and protection
- Accelerates VPN performance for high speed, secure remote access

### 3G/4G WAN Connectivity

The FortiGate/FortiWiFi 60E Series includes a USB port that allows you to plug in a compatible third-party 3G/4G USB modem, providing additional WAN connectivity or a redundant link for maximum reliability.

### Compact and Reliable Form Factor

Designed for small environments, you can place it on a desktop or wall-mount it. It is small, lightweight yet highly reliable with superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

### Superior Wireless Coverage

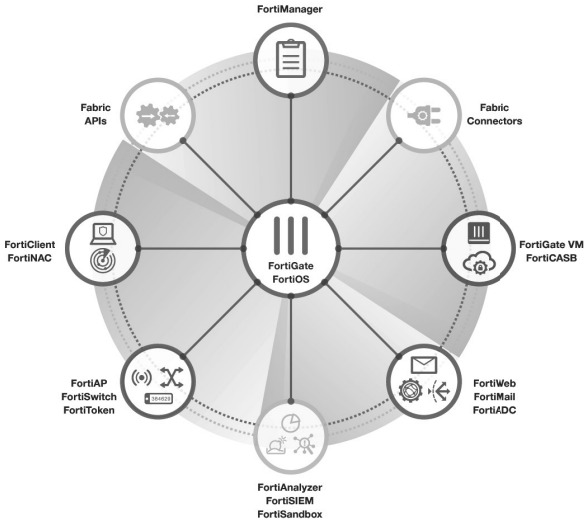
A built-in dual-band, dual-stream access point with internal antennas is integrated on the FortiWiFi 60E and provides speedy 802.11ac wireless access. The dual-band chipset addresses the PCI-DSS compliance requirement for rogue AP wireless scanning, providing maximum protection for regulated environments.

# Fortinet Security Fabric

## Security Fabric

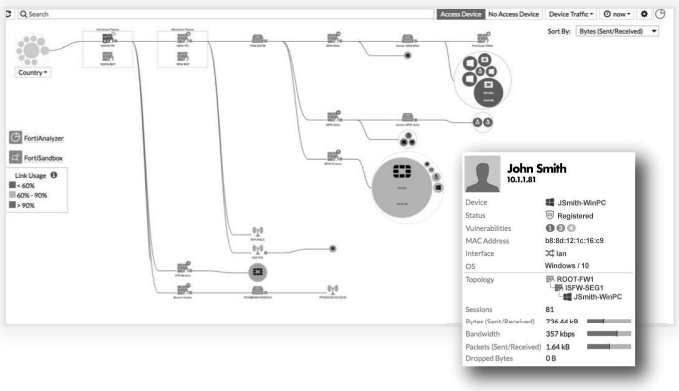
The Security Fabric delivers broad visibility, integrated AI-driven breach prevention, and automated operations, orchestration, and response across all Fortinet and its ecosystem deployments. It allows security to dynamically expand and adapt as more and more workloads and data are added. Security seamlessly follows and protects data, users, and applications as they move between IoT, devices, and cloud environments throughout the network. All this is ties together under a single pane of glass management for significantly thereby delivering leading security capabilities across your entire environment while also significantly reducing complexity.

FortiGates are the foundation of Security Fabric, expanding security via visibility and control by tightly integrating with other Fortinet security products and Fabric-Ready Partner solutions.




## FortiOS

Control all security and networking capabilities across the entire FortiGate platform with one intuitive operating system. Reduce complexity, costs, and response time with a truly consolidated next- generation security platform.




- A truly consolidated platform with a single OS and pane-of-glass for all security and networking services across all FortiGate platforms.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives, and ICSA validated security and performance. Ability to leverage latest technologies such as deception-based security.
- Control thousands of applications, block the latest exploits, and filter web traffic based on millions of real-time URL ratings in addition to true TLS 1.3 support.
- Prevent, detect, and mitigate advanced attacks automatically in minutes with integrated AI-driven breach prevention and advanced threat protection.
- Fulfil your networking needs with extensive routing, switching, and SD-WAN capabilities along with intent-based segmentation.
- Utilize SPU hardware acceleration to boost security capability performance.

# Services

## FortiGuard™ Security Services

FortiGuard Labs offers 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.

## FortiCare™ Support Services

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 60E | FORTIGATE 60E-POE | FORTIWIFI 60E | FORTIGATE 61E | FORTIWIFI 61E |
|---|---|---|---|---|---|
| **Hardware Specifications** | | | | | |
| GE RJ45 WAN / DMZ Ports | 2 / 1 | 2 | 2 / 1 | 2 / 1 | |
| GE RJ45 Internal Ports | 7 | – | 7 | 7 | |
| GE RJ45 PoE/+ Ports | – | 8 | – | – | |
| Wireless Interface | – | – | 802.11 a/b/g/n/ac | – | 802.11 a/b/g/n/ac |
| USB Ports | 1 | 1 | 1 | 1 | |
| Console (RJ45) | 1 | 1 | 1 | 1 | |
| Internal Storage | – | – | – | 1x 128 GB SSD | |
| **System Performance — Enterprise Traffic Mix** | | | | | |
| IPS Throughput [2] | 400 Mbps | | | | |
| NGFW Throughput [2, 4] | 250 Mbps | | | | |
| Threat Protection Throughput [2, 5] | 200 Mbps | | | | |
| **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) | 200 | | | | |
| 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 FortiSwitches Supported | 8 | | | | |
| Maximum Number of FortiAPs (Total / Tunnel Mode) | 30 / 10 | | | | |
| Maximum Number of FortiTokens | 500 | | | | |
| Maximum Number of Registered FortiClients | 200 | | | | |
| High Availability Configurations | Active / Active, Active / Passive, Clustering | | | | |
| **Dimensions** | | | | | |
| Height x Width x Length (inches) | 1.5 x 8.5 x 6.3 | | | | |
| Height x Width x Length (mm) | 38 x 216 x 160 | | | | |
| Weight | 1.9 lbs (0.9 kg) | 2.2 lbs (1.0 kg) | 1.9 lbs (0.9 kg) | 1.9 lbs (0.9 kg) | 1.9 lbs (0.9 kg) |
| Form Factor | Desktop | | | | |

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.

# Specifications

| | FORTIGATE 60E | FORTIGATE 60E-POE | FORTIWIFI 60E | FORTIGATE 61E | FORTIWIFI 61E |
|---|---|---|---|---|---|
| **Operating Environment and Certifications** | | | | | |
| Power Required | | | 100–240V AC, 50–60 Hz | | |
| Maximum Current | 110V AC / 1.5 A, 220V AC / 0.75 A | 0.8A | 115V AC / 0.9A, 230V AC / 0.6A | 115V AC / 0.9A, 230V AC / 0.6A | 115V AC / 0.9A, 230V AC / 0.6A |
| Total Available PoE Power Budget* | N/A | 75 W | N/A | N/A | N/A |
| Power Consumption (Average / Maximum) | 11.7 / 14 W | 20 / 95 W | 12.6 / 15.2 W | 11.9 / 14.3 W | 13 / 16 W |
| Heat Dissipation | 40 BTU/h | 324 BTU/h | 52 BTU/h | 49 BTU/h | 55 BTU/h |
| Operating Temperature | | | 32–104°F (0–40°C) | | |
| Storage Temperature | | | -31–158°F (-35–70°C) | | |
| Humidity | | | 10–90% non-condensing | | |
| Noise Level | | | Fanless 0 dBA | | |
| Operating Altitude | | | Up to 7,400 ft (2,250 m) | | |
| Compliance | | | FCC Part 15 Class B, C-Tick, VCCI, CE, UL/cUL, CB | | |
| Certifications | | | ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN | | |

* Maximum loading on each PoE/– port is 30 W (802.3at).

# Order Information

| Product | SKU | Description |
|---|---|---|
| FortiGate 60E | FG-60E | 10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port). Maximum managed FortiAPs (Total / Tunnel) 30 / 10. |
| FortiGate 60E-POE | FG-60E-POE | 10x GE RJ45 ports (including 8x PoE/PoE+ ports, 2x WAN ports) Maximum managed FortiAPs (Total / Tunnel) 30 / 10. |
| FortiWiFi 60E | FWF-60E | 10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port), Wireless (802.11a/b/g/n/ac). Maximum managed FortiAPs (Total / Tunnel) 30 / 10. |
| FortiGate 61E | FG-61E | 10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port), 128 GB SSD onboard storage. Maximum managed FortiAPs (Total / Tunnel) 30 / 10. |
| FortiWiFi 61E | FWF-61E | 10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port), Wireless (802.11a/b/g/n/ac), 128 GB SSD onboard storage. Maximum managed FortiAPs (Total / Tunnel) 30 / 10. |

# 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 | UTM | 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 | • | • | | |
| FortiCASB SaaS-only Service | • | • | | |
| FortiConverter Service | • | | | |
| SD-WAN Cloud Assisted Monitoring [2] | • | | | |
| SD-WAN Overlay Controller VPN Service [2] | • | | | |
| FortiAnalyzer Cloud [2] | • | | | |
| FortiManager Cloud [2] | • | | | |

1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 6.2

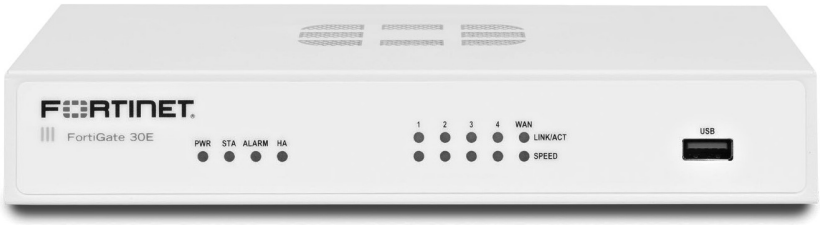
FORTINET®

www.fortinet.com

DATA SHEET

# FortiGate/FortiWiFi® 30E

**Secure SD-WAN**
**Unified Threat Management**




The FortiGate 30E series offers an excellent Security and SD-WAN solution in a compact fanless desktop form factor for enterprise branch offices and mid-sized businesses. Protect against cyber threats with industry-leading secure SD-WAN in a simple, affordable and easy to deploy solution.

### 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
- Prevent and detect against known and unknown attacks using continuous threat intelligence from AI powered FortiGuard Labs security services

### Performance
- Delivers industry's best threat protection performance and ultra-low latency using purpose-built security processor (SPU) technology
- Provides industry-leading performance and protection for SSL encrypted traffic

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

### Networking
- Best of Breed SD-WAN capabilities to enable application steering using WAN path control for high quality of experience
- Delivers extensive routing, switching, wireless controller, high-performance, and scalable IPsec VPN capabilities

### Management
- Includes Management Console that's effective, simple to use, and provides comprehensive network automation & visibility.
- Provides Zero Touch Integration with Security Fabric's Single Pane of Glass Management
- Predefined compliance checklist analyzes the deployment and highlights best practices to improve 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 |
|---|---|---|---|---|
| **950 Mbps** | **300 Mbps** | **200 Mbps** | **150 Mbps** | Multiple GE RJ45 \| WiFi variants |

Refer to specification table for details

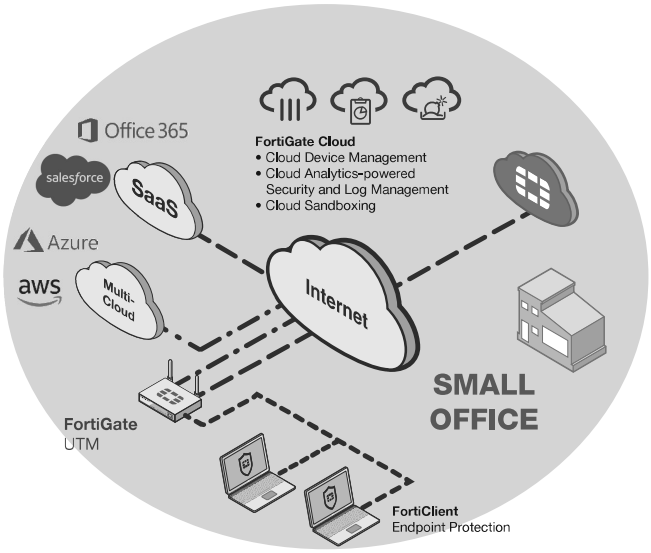
# Deployment

## Unified Threat Management (UTM)

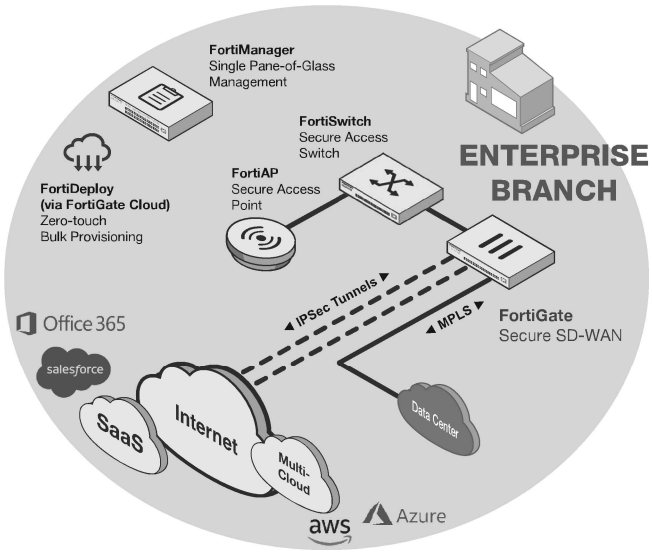
- Integrated wired and wireless networking to simplify IT
- Purpose-built hardware for industry best performance with easy administration through cloud management
- Provides consolidated security and networking for small businesses and consistently provides top-rated threat protection
- Proactively blocks newly discovered sophisticated attacks in real-time with advanced threat protection

## Secure SD-WAN

- Secure direct Internet access for Cloud Applications for improved latency and reduce WAN cost spending
- High-performance and cost-effective threat protection capabilities
- WAN Path Controller and Link Health Monitoring for better application performance and quality of experience
- Security Processer powered industry's best IPsec VPN and SSL Inspection performance
- Simplified Management and Zero Touch deployment



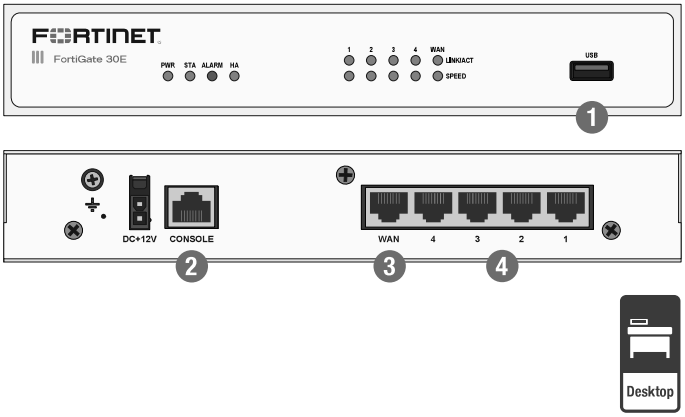

FortiWiFi 30E deployment in Small Office (UTM)



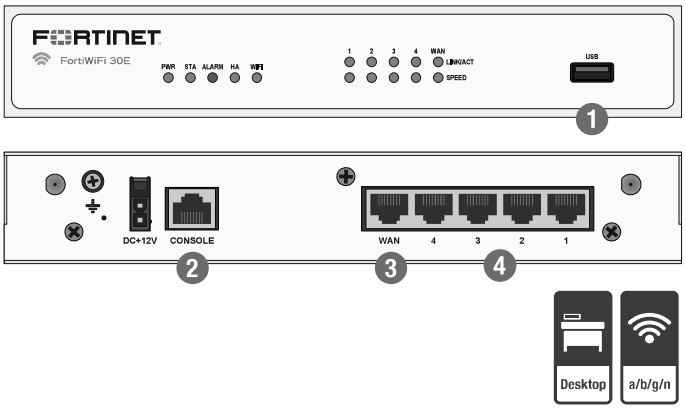

FortiGate 30E deployment in Enterprise Branch (Secure SD-WAN)

# Hardware

## FortiGate 30E




## FortiWiFi 30E




## Interfaces

1. USB Port
2. Console Port
3. 1x GE RJ45 WAN Port
4. 4x GE RJ45 Switch Ports

## Interfaces

1. USB Port
2. Console Port
3. 1x GE RJ45 WAN Port
4. 4x GE RJ45 Switch Ports

### Install in Minutes with FortiExplorer

The FortiExplorer wizard enables easy setup and configuration coupled with easy-to-follow instructions. FortiExplorer runs on popular iOS devices. Using FortiExplorer is as simple as starting the application and connecting to the appropriate USB port on the FortiGate. By using FortiExplorer, you can be up and running and protected in minutes.

### Wireless and 3G/4G WAN Extensions

The FortiGate supports external 3G/4G modems that allow additional or redundant WAN connectivity for maximum reliability. The FortiGate can also operate as a wireless access point controller to further extend wireless capabilities.

### Compact and Reliable Form Factor

Designed for small environments, you can simply place the FortiGate/FortiWiFi 30E on a desktop. It is small, lightweight yet highly reliable with superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

### Superior Wireless Coverage

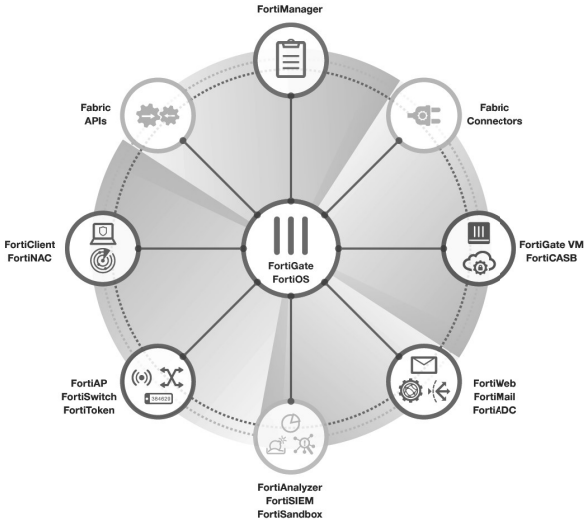
A built-in dual-band, dual-stream access point with internal antennas is integrated on the FortiWiFi 30E and provides speedy 802.11n coverage on 2.4 GHz or 5 GHz bands. The dual-band chipset addresses the PCI-DSS compliance requirement for rogue AP wireless scanning, providing maximum protection for regulated environments.

# Fortinet Security Fabric

## Security Fabric

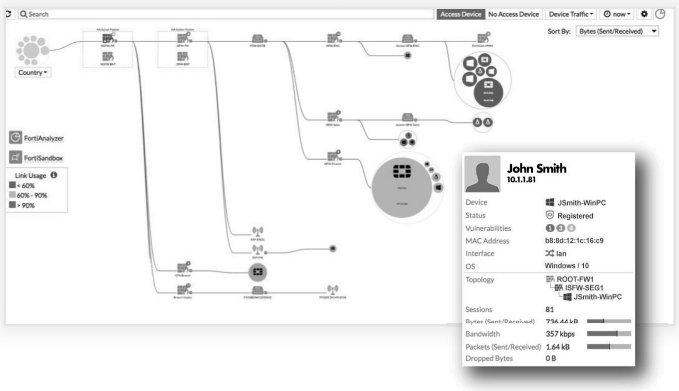
The Security Fabric delivers broad visibility, integrated AI-driven breach prevention, and automated operations, orchestration, and response across all Fortinet and its ecosystem deployments. It allows security to dynamically expand and adapt as more and more workloads and data are added. Security seamlessly follows and protects data, users, and applications as they move between IoT, devices, and cloud environments throughout the network. All this is ties together under a single pane of glass management for significantly thereby delivering leading security capabilities across your entire environment while also significantly reducing complexity.

FortiGates are the foundation of Security Fabric, expanding security via visibility and control by tightly integrating with other Fortinet security products and Fabric-Ready Partner solutions.




## FortiOS

Control all security and networking capabilities across the entire FortiGate platform with one intuitive operating system. Reduce complexity, costs, and response time with a truly consolidated next- generation security platform.




- A truly consolidated platform with a single OS and pane-of-glass for all security and networking services across all FortiGate platforms.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives, and ICSA validated security and performance. Ability to leverage latest technologies such as deception-based security.
- Control thousands of applications, block the latest exploits, and filter web traffic based on millions of real-time URL ratings in addition to true TLS 1.3 support.
- Prevent, detect, and mitigate advanced attacks automatically in minutes with integrated AI-driven breach prevention and advanced threat protection.
- Fulfil your networking needs with extensive routing, switching, and SD-WAN capabilities along with intent-based segmentation.
- Utilize SPU hardware acceleration to boost security capability performance.

# Services

## FortiGuard™ Security Services

FortiGuard Labs offers 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.

## FortiCare™ Support Services

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 30E | FORTIWIFI 30E |
|---|---|---|
| **Hardware Specifications** | | |
| GE RJ45 Switch Ports | 4 | |
| GE RJ45 WAN Port | 1 | |
| USB Port | 1 | |
| Console (RJ45) | 1 | |
| Wireless Interface | – | 802.11 a/b/g/n |
| **System Performance — Enterprise Traffic Mix** | | |
| IPS Throughput [2] | 300 Mbps | |
| NGFW Throughput [2, 4] | 200 Mbps | |
| Threat Protection Throughput [2, 5] | 150 Mbps | |
| **System Performance** | | |
| Firewall Throughput | 950 Mbps | |
| Firewall Latency (64 byte UDP packets) | 130 µs | |
| Firewall Throughput (Packets Per Second) | 180 Kpps | |
| Concurrent Sessions (TCP) | 900,000 | |
| New Sessions/Second (TCP) | 15,000 | |
| Firewall Policies | 5,000 | |
| IPsec VPN Throughput (512 byte) [1] | 75 Mbps | |
| Gateway-to-Gateway IPsec VPN Tunnels | 200 | |
| Client-to-Gateway IPsec VPN Tunnels | 250 | |
| SSL-VPN Throughput | 35 Mbps | |
| Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode) | 100 | |
| SSL Inspection Throughput (IPS, avg. HTTPS) [3] | 125 Mbps | |
| SSL Inspection CPS (IPS, avg. HTTPS) [3] | 120 | |
| SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3] | 45,000 | |
| Application Control Throughput (HTTP 64K) [2] | 400 Mbps | |
| CAPWAP Throughput (HTTP 64K) | 850 Mbps | |
| Virtual Domains (Default / Maximum) | 5 / 5 | |
| Maximum Number of FortiSwitches Supported | 8 | |
| Maximum Number of FortiAPs (Total / Tunnel Mode) | 2 / 2 | |
| Maximum Number of FortiTokens | 500 | |
| Maximum Number of Registered FortiClients | 200 | |
| High Availability Configurations | Active/Active, Active/Passive, Clustering | |

| | FORTIGATE 30E | FORTIWIFI 30E |
|---|---|---|
| **Dimensions** | | |
| Height x Width x Length (inches) | 1.61 x 8.27 x 5.24 | |
| Height x Width x Length (mm) | 41 x 210 x 133 | |
| Weight | 1.982 lbs (0.899 kg) | 2.008 lbs (0.911 kg) |
| Form Factor | Desktop | |
| **Environment** | | |
| Power Required | 100–240V AC, 60–50 Hz (External DC Power Adapter) | |
| Maximum Current | 100V / 0.6A, 240V / 0.4A | |
| Power Consumption (Average / Maximum) | 13 / 15 W | 16 / 19 W |
| Heat Dissipation | 52 BTU/h | 66 BTU/h |
| Operating Temperature | 32–104°F (0–40°C) | |
| Storage Temperature | -31–158°F (-35–70°C) | |
| Humidity | 10–90% non-condensing | |
| Noise Level | Fan-less 0 dBA | |
| Operating Altitude | Up to 7,400 ft (2,250 m) | |
| **Compliance** | | |
| Regulatory Compliance | FCC Part 15 Class B, C-Tick, VCCI, CE, UL/cUL, CB | |
| **Certifications** | | |
| | ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN | |

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 30E | FG-30E | 5x GE RJ45 ports (Including 1x WAN port, 4x Switch ports), Maximum managed FortiAPs (Total / Tunnel) 2 / 2. |
| FortiWiFi 30E | FWF-30E | 5x GE RJ45 ports (Including 1x WAN port, 4x Switch ports), Wireless (802.11a/b/g/n), Maximum managed FortiAPs (Total / Tunnel) 2 / 2. |
| **Optional Accessory** | | |
| Rack Mount Tray | SP-RACKTRAY-01 | Rack mount tray for supported products. |

# 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 | UTM | 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 | • | • | | |
| FortiCASB SaaS-only Service | • | • | | |
| FortiConverter Service | • | | | |
| SD-WAN Cloud Assisted Monitoring [2] | • | | | |
| SD-WAN Overlay Controller VPN Service [2] | • | | | |
| FortiAnalyzer Cloud [2] | • | | | |
| FortiManager Cloud [2] | • | | | |

1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 6.2

FORTINET®

www.fortinet.com

# Logging and reporting overview

Logging and reporting in FortiOS can help you in determining what is happening on your network, as well as informing you of certain network activity, such as detection of a virus or IPsec VPN tunnel errors. Logging and reporting go hand in hand, and can become a valuable tool for information as well as helping to show others the activity that is happening on the network.

This section explains logging and reporting features that are available in FortiOS, and how they can be used to help you manage or troubleshoot issues. This includes how the FortiGate unit records logs, what a log message is, and what the log database is.

## What is logging?

Logging records the traffic passing through the FortiGate unit to your network and what action the FortiGate unit took during its scanning process of the traffic. This recorded information is called a log message.

After a log message is recorded, it is stored within a log file which is then stored on a log device. A log device is a central storage location for log messages. The FortiGate unit supports several log devices, such as FortiAnalyzer units, the FortiCloud service, and Syslog servers. A FortiGate unit's system memory and local disk can also be configured to store logs, and because of this, are also considered log devices.

You must subscribe to FortiCloud before you will be able to configure the FortiGate unit to send logs to a FortiCloud server.

When the recorded activity needs to be read in a more human way, the FortiGate unit can generate a Report. A report gathers all the log information that is needed for the report, and presents it in a graphical format, with customizable design and automatically generated charts. Reports can be used to present a graphical representation of what is going on in the network. Reports can also be generated on a FortiAnalyzer unit; if you want to generate reports on a FortiAnalyzer, see the FortiAnalyzer Setup and Administration Guide to help you create and generate those reports.

### How the FortiGate unit records log messages

The FortiGate unit records log messages in a specific order, storing them on a log device. The order of how the FortiGate unit records log messages is as follows:

1. Incoming traffic is scanned.
2. During the scanning process, the FortiGate unit performs necessary actions, and simultaneously records the actions and results.
3. Log messages are sent to the log device.

### Example: How the FortiGate unit records a DLP event

1. The FortiGate unit receives incoming traffic and scans for any matches associated within its firewall policies containing a DLP sensor.

2. A match is found; the DLP sensor, dlp_sensor, had a rule within it called All-HTTP with the action Exempt applied to the rule. The sensor also has Enable Logging selected, which indicates to the FortiGate unit that the activity should be recorded and placed in the DLP log file.
3. The FortiGate unit exempts the match, and places the recorded activity (the log message) within the DLP log file.
4. According to the log settings that were configured, logs are stored on the FortiGate unit's local hard drive. The FortiGate unit places the DLP log file on the local hard drive.

## FortiOS features available for logging

Logs record FortiGate activity, providing detailed information about what is happening on your network. This recorded activity is found in log files, which are stored on a log device. However, logging FortiGate activity requires configuring certain settings so that the FortiGate unit can record the activity. These settings are often referred to as log settings, and are found in most security profiles, but also in **Log & Report > Log Settings**.

Log settings provide the information that the FortiGate unit needs so that it knows what activities to record. This topic explains what activity each log file records, as well as additional information about the log file, which will help you determine what FortiGate activity the FortiGate unit should record.

### Traffic

Traffic logs record the traffic that is flowing through your FortiGate unit. Since traffic needs firewall policies to properly flow through the unit, this type of logging is also referred to as firewall policy logging. Firewall policies control all traffic that attempts to pass through the FortiGate unit, between FortiGate interfaces, zones and VLAN sub-interfaces.

Logging traffic works in the following way:

- firewall policy has logging enabled on it (Log Allowed Traffic)
- packet comes into an inbound interface
- a possible log packet is sent regarding a match in the firewall policy, such as a URL filter
- traffic log packet is sent, per firewall policy
- packet passes and is sent out an interface

Traffic log messages are stored in the traffic log file. Traffic logs can be stored any log device, even system memory.

All security profile-related logs are now tracked within the Traffic logs, as of FortiOS 5.0, so all forward traffic can be searched in one place, such as if you are looking to see all activity from a particular address, security feature or traffic. Security profile logs are still tracked separately in the **Security Log** section, which only appears when logs exist.

If you have enabled and configured WAN Optimization, you can enable logging of this activity in the CLI using the `config wanopt setting` command. These logs contain information about WAN Optimization activity and are found in the traffic log file. When configuring logging of this activity, you must also enable logging within the security policy itself, so that the activity is properly recorded.

### Sniffer

The Sniffer log records all traffic that passes through a particular interface that has been configured to act as a One-Armed Sniffer, so it can be examined separately from the rest of the Traffic logs.

### Other Traffic

The traffic log also records interface traffic logging, which is referred to as Other Traffic. Other Traffic is enabled only in the CLI. When enabled, the FortiGate unit records traffic activity on interfaces as well as firewall policies. Logging Other Traffic puts a significant system load on the FortiGate unit and should be used only when necessary.

Logging other traffic works in the following way:

- firewall policy has logging enabled on it (Log Allowed Traffic) and other-traffic
- packet comes into an interface
- interface log packet is sent to the traffic log that is enabled on that particular interface
- possible log packet is sent regarding a match in the firewall policy, such as URL filter
- interface log packet is sent to the traffic log if enabled on that particular interface
- packet passes and is sent out an interface
- interface log packet is sent to traffic (if enabled) on that particular interface

### Event

The event log records administration management as well as FortiGate system activity, such as when a configuration has changed, admin login, or high availability (HA) events occur. Event logs are an important log file to record because they record FortiGate system activity, which provides valuable information about how your FortiGate unit is performing.

Event logs help you in the following ways:

- keeping track of configuration setting changes
- IPsec negotiation, SSL VPN and tunnel activity
- quarantine events, such as banned users
- system performance
- HA events and alerts
- firewall authentication events
- wireless events on models with WiFi capabilities
- activities concerning modem and internet protocols L2TP, PPP and PPPoE
- VIP activities
- AMC disk's bypass mode
- VoIP activities that include SIP and SCCP protocols.

As of 5.4, every 'execute' CLI command now generates an 'audit' event log, allowing you to track configuration changes. You can enable/disable this feature in the CLI:

```
config system global
   set cli-audit-log [enable|disable]
end
```

The FortiGate unit records event logs only when events are enabled.

### Traffic Shaping

Traffic shaping, per-IP traffic shaping and reverse direction traffic shaping settings can be applied to a firewall policy, appearing within the traffic log messages.

By enabling this feature, you can see what traffic shaping, per-IP traffic shaping and reverse direction traffic shaping settings are being used.

### Data Leak Prevention

Data Leak Prevention logs, or DLP logs, provide valuable information about the sensitive data trying to get through to your network as well as any unwanted data trying to get into your network. The DLP rules within a DLP sensor can log the following traffic types:

- email (SMTP, POP3 or IMAP; if SSL content SMTPS, POP3S, and IMAPS)
- HTTP
- HTTPS
- FTP
- NNTP
- IM

A DLP sensor must have log settings enabled for each DLP rule and compound rule, as well as applied to a firewall policy so that the FortiGate unit records this type of activity. A DLP sensor can also contain archiving options, which these logs are then archived to the log device.

### NAC Quarantine

Within the DLP sensor, there is an option for enabling NAC Quarantine. The NAC Quarantine option allows the FortiGate unit to record details of DLP operation that involve the ban and quarantine actions, and sends these to the event log file. The NAC Quarantine option must also be enabled within the Event Log settings. When enabling NAC quarantine within a DLP Sensor, you must enable this in the CLI because it is a CLI-only command.

### Media Access Control (MAC) Address

MAC address logs provide information about MAC addresses that the FortiGate unit sees on the network as well as those removed from the network. These log messages are stored in the event log (as subtype network; you can view these log messages in **Log & Report > System Events**) and are, by default, disabled in the CLI. You can enable logging MAC addresses using the following command syntax:

```
config log setting
   set neighbor-event enable
end
```

When enabled, a new log message is recorded every time a MAC address entry is added to the ARP table, and also when a MAC address is removed as well. A MAC address log message is also recorded when MAC addresses are connected to the local switch, or from a FortiAP or FortiSwitch unit.

### Application control

Application control logs provide detailed information about the traffic that internet applications such as Skype are generating. The application control feature controls the flow of traffic from a specific application, and the FortiGate unit examines this traffic for signatures that the application generates.

The log messages that are recorded provide information such as the type of application being used (such as P2P software), and what type of action the FortiGate unit took. These log messages can also help you to determine the top ten applications that are being used on your network. This feature is called application control monitoring and you can view the information from a widget on the Executive Summary page.

The application control list that is used must have logging enabled within the list, as well as logging enabled within each application entry. Each application entry can also have packet logging enabled. Packet logging for application control records the packet when an application type is identified, similar to IPS packet logging.

Logging of application control activity can only be recorded when an application control list is applied to a firewall policy, regardless of whether or not logging is enabled within the application control list.

### Antivirus

Antivirus logs are recorded when, during the antivirus scanning process, the FortiGate unit finds a match within the antivirus profile, which includes the presence of a virus or grayware signature. Antivirus logs provide a way to understand what viruses are trying to get in, as well as additional information about the virus itself, without having to go to the FortiGuard Center and do a search for the detected virus. The link is provided within the log message itself.

These logs provide valuable information such as:

- the name of the detected virus
- the name of the oversized file or infected file
- the action the FortiGate unit took, for example, a file was blocked
- URL link to the FortiGuard Center which gives detailed information about the virus itself

The antivirus profile must have log settings enabled within it so that the FortiGate unit can record this activity, as well as having the antivirus profile applied to a firewall policy.

### Web Filter

Web filter logs record HTTP traffic activity. These log messages provide valuable and detailed information about this particular traffic activity on your network. Web filtering activity is important to log because it can inform you about:

- what types of web sites employees are accessing
- users attempting to access banned web sites and how often this occurs
- network congestion due to employees accessing the Internet at the same time
- web-based threats resulting from users visiting non-business-related web sites

Web Filter logs are an effective tool to help you determine if you need to update your web filtering settings within a web filter profile due to unforeseen threats or network congestion. These logs also inform you about web filtering quotas that have been configured for filtering HTTP traffic.

You must configure logging settings within the web filter profile and apply the filter to a firewall policy so that the FortiGate unit can record the activity.

### IPS (attack)

IPS logs, also referred to as attack logs, record attacks that occurred against your network. Attack logs contain detailed information about whether the FortiGate unit protected the network using anomaly-based defense settings or signature-based defense settings, as well as what the attack was.

The IPS or attack log file is especially useful because the log messages that are recorded contain a link to the FortiGuard Center, where you can find more information about the attack. This is similar to antivirus logs, where a link to the FortiGuard Center is provided as well that informs you of the virus that was detected by the FortiGate unit.

An IPS sensor with log settings enabled must be applied to a firewall policy so that the FortiGate unit can record the activity.

### Packet logs

When you enable packet logging within an IPS signature override or filter, the FortiGate unit examines network packets, and if a match is found, saves them to the attack log. Packet logging is designed to be used as a diagnostic tool that can focus on a narrow scope of diagnostics, rather than a log that informs you of what is occurring on your network.

You should use caution when enabling packet logging, especially within IPS filters. Filter configuration that contains thousands of signatures could potentially cause a flood of saved packets, which would take up a lot of storage space on the log device. It would also take a great deal of time to sort through all the log messages, as well as consume considerable system resources to process.

You can archive packets, but you must enable this option on the Log Settings page. If your log configuration includes multiple FortiAnalyzer units, packet logs are only sent to the primary (first) FortiAnalyzer unit. Sending packet logs to the other FortiAnalyzer units is not supported.

### Email filter

Email filter logs, also referred to as spam filter logs, record information regarding the content within email messages. For example, within an email filter profile, a match is found that finds the email message to be considered spam.

Email filter logs are recorded when the FortiGate unit finds a match within the email filter profile and logging settings are enabled within the profile.

If you are using a Banned Words List for email filtering, note that the filter pattern number is only recorded when the source email address contains a banned word.

### Archives (DLP)

Recording DLP logs for network use is called DLP archiving. The DLP engine examines email, FTP, IM, NNTP, and web traffic. Archived logs are usually saved for historical use and can be accessed at any time. IPS packet logs can also be archived, within the Log Settings page.

You can start with the two default DLP sensors that have been configured specifically for archiving log data, Content_Archive and Content_Summary. They are available in **Security Profiles > Data Leak Prevention**. Content_Archive provides full content archiving, while Content_Summary provides summary archiving. For more information about how to configure DLP sensors, see the Security Features chapter of the FortiOS Handbook.

You must enable the archiving to record log archives. Logs are not archived unless enabled, regardless of whether or not the DLP sensor for archiving is applied to the firewall policy.

### Network scan

Network scan logs are recorded when a scheduled scan of the network occurs. These log messages provide detailed information about the network's vulnerabilities regarding software, as well as the discovery of any further vulnerabilities.

A scheduled scan must be configured and logging enabled within the Event Log settings, for the FortiGate unit to record these log messages.

## Log messages

Log messages are recorded by the FortiGate unit, giving you detailed information about the network activity. Each log message has a unique number that helps identify it, as well as containing fields; these fields, often called log fields, organize the information so that it can be easily extracted for reports.

These log fields are organized in such a way that they form two groups: the first group, made up of the log fields that come first, is called the log header. The log header contains general information, such as the unique log identification and date and time that indicates when the activity was recorded. The log body is the second group, and contains all the other information about the activity. There are no two log message bodies that are alike, however, there may be fields common to most log bodies, such as the `srcintf` or `identidix` log fields.

The log header also contains information about the log priority level which is indicated in the `level` field. The priority level indicates the immediacy and the possible repercussions of the logged action. For example, if the field contains 'alert', you need to take immediate action with regards to what occurred. There are six log priority levels.

The log severity level is the level at and above which the FortiGate unit records logs. The log severity level is defined by you when configuring the logging location. The FortiGate unit will log all messages at and above the priority level you select. For example, if you select Error, the unit will log only Error, Critical, Alert, and Emergency level messages.

### Log priority levels

| Levels | Description |
|---|---|
| **0 - Emergency** | The system has become unstable. |
| **1 - Alert** | Immediate action is required. |
| **2 - Critical** | Functionality is affected. |
| **3 - Error** | An error condition exists and functionality could be affected. |
| **4 - Warning** | Functionality could be affected. |
| **5 - Notification** | Information about normal events. |
| **6 - Information** | General information about system operations. |

The Debug priority level, not shown above, is rarely used. It is the lowest log priority level and usually contains some firmware status information that is useful when the FortiGate unit is not functioning properly.

### Example log header fields

| Log header | |
|---|---|
| **date=(2010-08-03)** | The year, month and day of when the event occurred in yyyy-mm-dd format. |

| Log header | |
|---|---|
| **time=(12:55:06)** | The hour, minute and second of when the event occurred in the format hh:mm:ss. |
| **log_id=(2457752353)** | A five or ten-digit unique identification number. The number represents that log message and is unique to that log message. This ten-digit number helps to identify the log message. |
| **type=(dlp)** | The section of system where the event occurred. |
| **subtype=(dlp)** | The subtype category of the log message. |
| **level=(notice)** | The priority level of the event. See the table above. |
| **vd=(root)** | The name of the virtual domain where the action/event occurred in. If no virtual domains exist, this field always contains root. |

**Example log body fields**

| Log body | |
|---|---|
| **policyid=(1)** | The ID number of the firewall policy that applies to the session or packet. Any policy that is automatically added by the FortiGate will have an index number of zero. |
| **identidx=(0)** | The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy. |
| **sessionid=(311)** | The serial number of the firewall session of which the event happened. |
| **srcip=(10.10.10.1)** | The source IP address. |
| **srcport=(1190)** | The source port number. |
| **srcintf=(internal)** | The source interface name. |
| **dstip=(192.168.1.122)** | The destination IP address. |
| **dstport=(80)** | The destination port number. |
| **dstintf=(wan1)** | The destination interface name. |
| **service=(https)** | The IP network service that applies to the session or packet. The services displayed correspond to the services configured in the firewall policy. |
| **status=(detected)** | The action the FortiGate unit took. |

| Log body | |
|---|---|
| **hostname=(example.com)** | The home page of the web site. |
| **url=(/image/trees_pine_ forest/)** | The URL address of the web page that the user was viewing. |
| **msg=(data leak detected (Data Leak Prevention Rule matched)** | Explains the FortiGate activity that was recorded. In this example, the data leak that was detected matched the rule, All-HTTP, in the DLP sensor. |
| **rulename=(All-HTTP)** | The name of the DLP rule within the DLP sensor. |
| **action=(log-only)** | The action that was specified within the rule. In some rules within sensors, you can specify content archiving. If no action type is specified, this field display log-only. |
| **severity=(1)** | The level of severity for that specific rule. |

Logs from other devices, such as the FortiAnalyzer unit and Syslog server, contain a slightly different log header. For example, when viewing FortiGate log messages on the FortiAnalyzer unit, the log header contains the following log fields when viewed in the Raw format:

```
itime=1302788921 date=20110401 time=09:04:23 devname=FG50BH3G09601792 device_
    id=FG50BH3G09601792 log_id=0100022901 type=event subtype=system level=notice vd=root
```

The log body contains the rest of the information of the log message, and this information is unique to the log message itself.

For detailed information on all log messages, see the *FortiGate Log Message Reference*.

## Explanation of a debug log message

Debug log messages are only generated if the log severity level is set to Debug. The Debug severity level is the lowest log severity level and is rarely used. This severity level usually contains some firmware status information that is useful when the FortiGate unit is not functioning properly. Debug log messages are generated by all types of FortiGate features.

The following is an example of a debug log message:

```
date=2010-01-25 time=17:25:54 logid=9300000000 type=webfilter subtype=urlfilter
    level=debug msg="found in cache"
```

### Example of a Debug log message

| Debug log | |
|---|---|
| **date=(2010-01-25)** | The year, month and day of when the event occurred in the format yyyy-mm-dd. |
| **time=(17:25:54)** | The hour, minute and second of when the event occurred in the format hh:mm:ss. |

| Debug log | |
|---|---|
| **logid=(93000000000)** | A ten-digit unique identification number. The number represents that log message and is unique to that log message. This ten-digit number helps to identify the log message. |
| **type=(webfilter)** | The section of system where the event occurred. There are eleven log types in FortiOS 4.0. |
| **subtype=(urlfilter)** | The subtype of the log message. This represents a policy applied to the FortiGate feature in the firewall policy. |
| **level=(debug)** | The priority level of the event. There are six priority levels to specify. |
| **msg=("found in cache")** | Explains the activity or event that the FortiGate unit recorded. |

### Viewing log messages and archives

Depending on the log device, you may be able to view logs within the web-based manager or CLI on the FortiGate unit. If you have configured a FortiAnalyzer unit, local hard disk, or system memory, you can view log messages from within the web-based manager or CLI. If you have configured either a Syslog or WebTrends server, you will not be able to view log messages from the web-based manager or CLI. There is also no support for viewing log messages stored on a FortiCloud server, from the FortiGate unit's web-based manager or CLI.

You do not have to view log messages from only the web-based manager. You can view log messages from the CLI as well, using the `execute log display` command. This command allows you to see specific log messages that you already configured within the `execute log filter` command. The `execute log filter` command configures what log messages you will see, how many log messages you can view at one time (a maximum of 1000 lines of log messages), and the type of log messages you can view. For more information about viewing log messages in the CLI, see "Viewing logs from the CLI".

There are two log viewing options in FortiOS: Format and Raw. The Raw format displays logs as they appear within the log file. You can view log messages in the Raw format using the CLI or a text editor, such as Notepad. Format is in a more human-readable format, and you can easily filter information when viewing log messages this way. The Format view is what you see when viewing logs in the web-based manager.

When you download the log messages from within the log message page (for example, **Log & Report > Forward Traffic**), you are downloading log messages in the Raw format.

### Viewing log messages in detail

From any log page, you can view detailed information about the log message in the log viewer table, located (by default) at the bottom of the page. Each page contains this log viewer table. The Log Viewer Table can contain the Archive tab, which allows you to see the archived version of the log message. The Archive tab only displays the archived log's details if archiving is enabled and logs are being archived by the FortiGate unit, but archived logs will also be recorded when using a FortiAnalyzer unit or the FortiCloud service.

When you are viewing traffic log messages, some of the categories (such as 'Application Name') have entries that can be selected to open a dialog box containing FortiGuard information about the entry. From within the dialog box, you can select the Reference link and go directly to the corresponding FortiGuard page, which contains additional information.

Viewing logs in Raw format allows you to view all log fields at once, as well as have a log file available regardless of whether you are archiving logs or not. You download the log file by selecting **Download Log**. The log file is named in the following format: <log_type><log_location><log_date/time>.<log_number>.log. For example, SystemEventLog-disk-2012-09-19T12_13_46.933949.log, which is an event log. The time period is the day and month of when the log was downloaded, not the time period of the log messages within the file itself.

### Quarantine

Within the Log & Report menu, you can view detailed information about each quarantined file. The information can either be sorted or filtered, depending on what you want to view.

You must enable quarantine settings within an antivirus profile and the destination must be configured in the CLI using the `config antivirus quarantine` command. The destination can be either a FortiAnalyzer unit or local disk.

Sort the files by file name, date, service, status, duplicate count (DC), or time to live (TTL). Filter the list to view only quarantined files with a specific status or from a specific service.

The file quarantine list displays the following information about each quarantined file.

**Quarantine page**

Lists all files that are considered quarantined by the unit. On this page you can filter information so that only specific files are displayed on the page.

| GUI Item | Description |
|---|---|
| **Source** | Either **FortiAnalyzer** or **Local Disk**, depending where you configure to quarantined files to be stored. |
| **Sort by** | Sort the list. Choose from: **Status**, **Service**, **File Name**, **Date**, **TTL**, or **Duplicate Count**. Select **Apply** to complete the sort. |
| **Filter** | Filter the list. Choose either **Status** (infected, blocked, or heuristics) or **Service** (IMAP, POP3, SMTP, FTP, HTTP, MM1, MM3, MM4, MM7, IM, or NNTP). Select **Apply** to complete the filtering. Heuristics mode is configurable through the CLI only.<br><br>If your unit supports SSL content scanning and inspection Service can also be IMAPS, POP3S, SMTPS, or HTTPS. For more information, see the Security Features chapter of the FortiOS Handbook. |
| **Apply** | Select to apply the sorting and filtering selections to the list of quarantined files. |
| **Delete** | Select to delete the selected files. |
| **Page Controls** | Use the controls to page through the list. |

| GUI Item | Description |
|---|---|
| **Remove All Entries** | Removes all quarantined files from the local hard disk.<br><br>This icon only appears when the files are quarantined to the hard disk. |
| **File Name** | The file name of the quarantined file. When a file is quarantined, all spaces are removed from the file name, and a 32-bit checksum is performed on the file. The checksum appears in the replacement message but not in the quarantined file. The file is stored on the FortiGate hard disk with the following naming convention:<br><br><32bit_CRC>.<processed_filename><br><br>For example, a file named Over Size.exe is stored as 3fc155d2.oversize.exe. |
| **Date** | The date and time the file was quarantined, in the format dd/mm/yyyy hh:mm. This value indicates the time that the first file was quarantined if duplicates are quarantined. |
| **Service** | The service from which the file was quarantined (HTTP, FTP, IMAP, POP3, SMTP, MM1, MM3, MM4, MM7, IM, NNTP, IMAPS, POP3S, SMTPS, or HTTPS). |
| **Status** | The reason the file was quarantined: **infected**, **heuristics**, or **blocked**. |
| **Status Description** | Specific information related to the status, for example, “File is infected with “W32/Klez.h”” or “File was stopped by file block pattern.” |
| **DC** | Duplicate count. A count of how many duplicates of the same file were quarantined. A rapidly increasing number can indicate a virus outbreak. |
| **TTL** | Time to live in the format hh:mm. When the TTL elapses, the FortiGate unit labels the file as EXP under the TTL heading. In the case of duplicate files, each duplicate found refreshes the TTL.<br><br>The TTL information is not available if the files are quarantined on a FortiAnalyzer unit. |
| **Upload status** | **Y** indicates the file has been uploaded to Fortinet for analysis, **N** indicates the file has not been uploaded.<br><br>This option is available only if the FortiGate unit has a local hard disk. |
| **Download** | Select to download the corresponding file in its original format.<br><br>This option is available only if the FortiGate unit has a local hard disk. |
| **Submit** | Select to upload a suspicious file to Fortinet for analysis.<br><br>This option is available only if the FortiGate unit has a local hard disk. |

### Customizing the display of log messages on the web-based manager

Customizing log messages on the web-based manager allows you to remove or add columns from the page and filter the information that appears. For example, you can view only log messages that appeared on December 4, between the hours of 8:00 and 8:30 am.

1. Select the submenu in **Log & Report** in which you want to customize the display of log messages, such as **Log & Report > Forward Traffic**.
2. Right click on the title bar at the top of any column, and uncheck a column title such as **Date/Time** to remove it from the interface. Check other columns to add them to the interface. When you are finished, click outside the menu and the page will refresh with the new column settings in place.
3. Choose a column you'd like to filter, and select the funnel icon next to the title of the column. For example, select the funnel in the Src (Source) column. In the text field, enter the source IP address 1.1.1.1 and then select the check box beside **NOT**.
   This filters out the all log messages that have the 1.1.1.1 source IP address in the source IP log field, such as the ones generated when running log tests in the CLI.
4. Select **OK** to save the customize settings, and then view the log messages on the page.
   Log messages that originate from the 1.1.1.1 source address will no longer appear in the list.

### How to download log messages and view them from on a computer

After recording some activity, you can download log messages to view them from a computer. This is can be very useful when in a remote location, or if you want to view log messages at your convenience, or to view packet logs or traffic logs.

1. In Log & Report, select the submenu that you want to download log messages from.
   For example, **Log & Report > Forward Traffic**.
2. Select the **Download Log** option and save the log file to your computer.
   The log file will be downloaded like any other file. Log file names contain their log type and date in the name, so it is recommended to create a folder in which to archive your log messages, as they can be sorted easily.
3. Open a text editor such as Notepad, open the log file, and then scroll to view all the log messages.
   You can easily search or scroll through the logs to see the information that is available.

## Log files and types

As the log messages are being recorded, log messages are also being put into different log files. The log file contains the log messages that belong to that log type, for example, traffic log messages are put in the traffic log file.

When downloading the log file from within **Log & Report**, the file name indicates the log type and the device on which it is stored, as well as the date, time, and a unique id for that log.

This name is in the format <logtype> - <logdevice> - <date> T <time> . <id>.log.

For example, AntiVirusLog-disk-2012-09-13T11_07_57.922495.log.

Below, each of the different log files are explained. Traffic and Event logs come in multiple types, but all contain the base type such as 'Event' in the filename.

**Log Types based on network traffic**

| Log Type | Description |
|---|---|
| **Traffic** | The traffic logs records all traffic to and through the FortiGate interface. Different categories monitor different kinds of traffic, whether it be forward, local, or sniffer. |
| **Event** | The event logs record management and activity events within the device in particular areas: System, Router, VPN, User, Endpoint, HA, WAN Opt./Cache, and WiFi. For example, when an administrator logs in or logs out of the web-based manager, it is logged both in System and in User events. |
| **Antivirus** | The antivirus log records virus incidents in Web, FTP, and email traffic. |
| **Web Filter** | The web filter log records HTTP FortiGate log rating errors including web content blocking actions that the FortiGate unit performs. |
| **Application Control** | The application log records application usage, monitoring or blocking as configured in the security profiles. |
| **Intrusion** | The intrusion log records attacks that are detected and prevented by the FortiGate unit. |
| **Email Filter** | The email filter log records blocking of email address patterns and content in SMTP, IMAP, and POP3 traffic. |
| **Vulnerability Scan** | The Vulnerability Scan (Netscan) log records vulnerabilities found during the scanning of the network. |
| **Data Leak Prevention** | The Data Leak Prevention log records log data that is considered sensitive and that should not be made public. This log also records data that a company does not want entering their network. |
| **VoIP** | The VoIP log records VoIP traffic and messages. It only appears if VoIP is enabled on the Administrator Settings page. |

## Log database and datasets

The log database, also known as the SQL log database, is used to store logs on FortiGate units that have a built-in hard disk. The log database uses Structured Query Lanaguage (SQL), specifically it uses SQLite which is an embedded Relational Database Management System (RDBMS).

If you have disabled SQL logging and have factory defaults on the FortiGate unit, and then you upgrade the firmware, the upgrade will automatically disable SQL logging. When this occurs, you must re-enable SQL logging manually.

The FortiGate unit creates a database table for each log type, when log data is recorded. If the FortiGate unit is not recording log data, it does not create log tables for that device.

If you want to view the size of the database, as well as the log database table entries, use the `get report sql status` command. This command displays the amount of free space that is available as well as the first and last log database entry time and date.

The output of the `get report sql status` command contains information similar to the following:

```
Database size: 294912
Free size in database: 0
Database Page Size: 8192
Entry number:
Event: 49
Traffic: 370
Attack: 2
AntiVirus: 4
WebFilter: 254
AntiSpam: 2
Netscan: 18
Total: 699
First entry time: 2012-09-10 11:41:02
Last entry time: 2012-09-13 02:59:59
```

The log database is not only used to store logs, but also used to extract the information for reports. Reports are built from datasets, which are SQL statements that tell the FortiGate unit how to extract the information from the database. You can create your own datasets; however, SQL knowledge is required. Default datasets are available for reports.

### Notifications about network activity

Alert email messages provide notification about activities or events logged. These email messages also provide notification about log severities that are recorded, such as a critical or emergency.

You can send alert email messages to up to three email addresses. Alert messages are also logged and can be viewed from the Event Log menu, in the System Event log file.

You can use the alert email feature to monitor logs for log messages, and to send email notification about a specific activity or event logged. For example, if you require notification about administrators logging in and out, you can configure an alert email that is sent whenever an administrator logs in and out. You can also base alert email messages on the severity levels of the logs.

Before configuring alert email, you must configure at least one DNS server if you are configuring with an Fully Qualified Domain Server (FQDN). The FortiGate unit uses the SMTP server name to connect to the mail server, and must look up this name on your DNS server. You can also specify an IP address.

The default minimum log severity level is Alert. If the FortiGate unit collects more than one log message before an interval is reached, the FortiGate unit combines the messages and sends out one alert email.

### How to configure email notifications

The following explains how to configure an alert email notification for IPsec tunnel errors, firewall authentication failure, configuration changes and FortiGuard license expiry.

1. In **System > Advanced**, under **Email Service**, configure the SMTP server.
   The SMTP server settings allow the FortiGate unit to know exactly where the email will be sent from, as well as who to send it to. The SMTP server must be a server that does not support SSL/TLS connections; if the SMTP server does, the alert email configuration will not work. The FortiGate unit does not currently support SSL/TLS

connections for SMTP servers.

2. In **Log & Report > Alert E-mail**, enter the source email in the Email From field, and up to three target addresses in the Email To fields.
3. Below the email entry, you can configure the email responses. By default, the **Send alert email for the following** is enabled. Select the check boxes beside **IPsec tunnel errors**, **Configuration changes** and **Firewall authentication failure**.
   These alerts will be sent to the email address specified when the trigger occurs. For example, a user attempts to connect to the branch office of the company but cannot; the FortiGate unit detects an IPsec tunnel error, records the event, and then sends the notice to the email address specified in the SMTP server settings.
4. Select **FortiGuard license expiry time:** and then enter 10 so that the email notification will be sent ten days prior to the FortiGuard license expiration.
   You can choose up to 100 days prior to when the license will expire. The default time is 15 days. By using this alert email notification, you can easily know when to send an re-registration request long before the expiry.

## Log devices

The FortiGate unit supports a variety of log devices, including the FortiCloud service and FortiAnalyzer units. This provides greater flexibility not only when choosing a log device, but also when your logging requirements need updating.

When you have developed a plan that meets your logging needs and requirements, you need to select the log device that is appropriate for that plan. A log device must be able to store all the logs you need, and if you require archiving those logs, you must consider what log devices support this option.

During this process of deciding what log device meets your needs and requirements, you must also figure out how to provide a backup solution in the event the log device that the FortiGate unit is sending logs to has become unavailable. A backup solution should be an important part of your log setup because it helps you to maintain all logs and prevents lost logs, or logs that are not sent to the log device. For example, a daily backup of log files to the FortiAnalyzer unit occurs at 5 pm.

Log devices provide a central location for storing logs recorded by the FortiGate unit. The following are log devices that the FortiGate unit supports:

- FortiGate system memory
- Hard disk or AMC
- SQL database (for FortiGate units that have a hard disk)
- FortiAnalyzer unit
- FortiCloud service
- Syslog server

These log devices, except for the FortiGate system memory and local hard disk, can also be used as a backup solution. For example, you can configure logging to the FortiGate unit's local disk, but also configure logging to a FortiCloud server and archive logs to both the FortiCloud server and a FortiAnalyzer unit.

If you are formatting a disk that contains more than just logs, all information on the disk will be lost.

2. A match is found; the DLP sensor, dlp_sensor, had a rule within it called All-HTTP with the action Exempt applied to the rule. The sensor also has Enable Logging selected, which indicates to the FortiGate unit that the activity should be recorded and placed in the DLP log file.
3. The FortiGate unit exempts the match, and places the recorded activity (the log message) within the DLP log file.
4. According to the log settings that were configured, logs are stored on the FortiGate unit's local hard drive. The FortiGate unit places the DLP log file on the local hard drive.

## FortiOS features available for logging

Logs record FortiGate activity, providing detailed information about what is happening on your network. This recorded activity is found in log files, which are stored on a log device. However, logging FortiGate activity requires configuring certain settings so that the FortiGate unit can record the activity. These settings are often referred to as log settings, and are found in most security profiles, but also in **Log & Report > Log Settings**.

Log settings provide the information that the FortiGate unit needs so that it knows what activities to record. This topic explains what activity each log file records, as well as additional information about the log file, which will help you determine what FortiGate activity the FortiGate unit should record.

### Traffic

Traffic logs record the traffic that is flowing through your FortiGate unit. Since traffic needs firewall policies to properly flow through the unit, this type of logging is also referred to as firewall policy logging. Firewall policies control all traffic that attempts to pass through the FortiGate unit, between FortiGate interfaces, zones and VLAN sub-interfaces.

Logging traffic works in the following way:

- firewall policy has logging enabled on it (Log Allowed Traffic)
- packet comes into an inbound interface
- a possible log packet is sent regarding a match in the firewall policy, such as a URL filter
- traffic log packet is sent, per firewall policy
- packet passes and is sent out an interface

Traffic log messages are stored in the traffic log file. Traffic logs can be stored any log device, even system memory.

All security profile-related logs are now tracked within the Traffic logs, as of FortiOS 5.0, so all forward traffic can be searched in one place, such as if you are looking to see all activity from a particular address, security feature or traffic. Security profile logs are still tracked separately in the **Security Log** section, which only appears when logs exist.

If you have enabled and configured WAN Optimization, you can enable logging of this activity in the CLI using the `config wanopt setting` command. These logs contain information about WAN Optimization activity and are found in the traffic log file. When configuring logging of this activity, you must also enable logging within the security policy itself, so that the activity is properly recorded.

### Sniffer

The Sniffer log records all traffic that passes through a particular interface that has been configured to act as a One-Armed Sniffer, so it can be examined separately from the rest of the Traffic logs.

### Other Traffic

The traffic log also records interface traffic logging, which is referred to as Other Traffic. Other Traffic is enabled only in the CLI. When enabled, the FortiGate unit records traffic activity on interfaces as well as firewall policies. Logging Other Traffic puts a significant system load on the FortiGate unit and should be used only when necessary.

Logging other traffic works in the following way:

- firewall policy has logging enabled on it (Log Allowed Traffic) and other-traffic
- packet comes into an interface
- interface log packet is sent to the traffic log that is enabled on that particular interface
- possible log packet is sent regarding a match in the firewall policy, such as URL filter
- interface log packet is sent to the traffic log if enabled on that particular interface
- packet passes and is sent out an interface
- interface log packet is sent to traffic (if enabled) on that particular interface

### Event

The event log records administration management as well as FortiGate system activity, such as when a configuration has changed, admin login, or high availability (HA) events occur. Event logs are an important log file to record because they record FortiGate system activity, which provides valuable information about how your FortiGate unit is performing.

Event logs help you in the following ways:

- keeping track of configuration setting changes
- IPsec negotiation, SSL VPN and tunnel activity
- quarantine events, such as banned users
- system performance
- HA events and alerts
- firewall authentication events
- wireless events on models with WiFi capabilities
- activities concerning modem and internet protocols L2TP, PPP and PPPoE
- VIP activities
- AMC disk's bypass mode
- VoIP activities that include SIP and SCCP protocols.

As of 5.4, every 'execute' CLI command now generates an 'audit' event log, allowing you to track configuration changes. You can enable/disable this feature in the CLI:

```
config system global
   set cli-audit-log [enable|disable]
end
```

The FortiGate unit records event logs only when events are enabled.

### Traffic Shaping

Traffic shaping, per-IP traffic shaping and reverse direction traffic shaping settings can be applied to a firewall policy, appearing within the traffic log messages.

By enabling this feature, you can see what traffic shaping, per-IP traffic shaping and reverse direction traffic shaping settings are being used.

### Data Leak Prevention

Data Leak Prevention logs, or DLP logs, provide valuable information about the sensitive data trying to get through to your network as well as any unwanted data trying to get into your network. The DLP rules within a DLP sensor can log the following traffic types:

- email (SMTP, POP3 or IMAP; if SSL content SMTPS, POP3S, and IMAPS)
- HTTP
- HTTPS
- FTP
- NNTP
- IM

A DLP sensor must have log settings enabled for each DLP rule and compound rule, as well as applied to a firewall policy so that the FortiGate unit records this type of activity. A DLP sensor can also contain archiving options, which these logs are then archived to the log device.

### NAC Quarantine

Within the DLP sensor, there is an option for enabling NAC Quarantine. The NAC Quarantine option allows the FortiGate unit to record details of DLP operation that involve the ban and quarantine actions, and sends these to the event log file. The NAC Quarantine option must also be enabled within the Event Log settings. When enabling NAC quarantine within a DLP Sensor, you must enable this in the CLI because it is a CLI-only command.

### Media Access Control (MAC) Address

MAC address logs provide information about MAC addresses that the FortiGate unit sees on the network as well as those removed from the network. These log messages are stored in the event log (as subtype network; you can view these log messages in **Log & Report > System Events**) and are, by default, disabled in the CLI. You can enable logging MAC addresses using the following command syntax:

```
config log setting
   set neighbor-event enable
end
```

When enabled, a new log message is recorded every time a MAC address entry is added to the ARP table, and also when a MAC address is removed as well. A MAC address log message is also recorded when MAC addresses are connected to the local switch, or from a FortiAP or FortiSwitch unit.

### Application control

Application control logs provide detailed information about the traffic that internet applications such as Skype are generating. The application control feature controls the flow of traffic from a specific application, and the FortiGate unit examines this traffic for signatures that the application generates.

The log messages that are recorded provide information such as the type of application being used (such as P2P software), and what type of action the FortiGate unit took. These log messages can also help you to determine the top ten applications that are being used on your network. This feature is called application control monitoring and you can view the information from a widget on the Executive Summary page.

The application control list that is used must have logging enabled within the list, as well as logging enabled within each application entry. Each application entry can also have packet logging enabled. Packet logging for application control records the packet when an application type is identified, similar to IPS packet logging.

Logging of application control activity can only be recorded when an application control list is applied to a firewall policy, regardless of whether or not logging is enabled within the application control list.

### Antivirus

Antivirus logs are recorded when, during the antivirus scanning process, the FortiGate unit finds a match within the antivirus profile, which includes the presence of a virus or grayware signature. Antivirus logs provide a way to understand what viruses are trying to get in, as well as additional information about the virus itself, without having to go to the FortiGuard Center and do a search for the detected virus. The link is provided within the log message itself.

These logs provide valuable information such as:

- the name of the detected virus
- the name of the oversized file or infected file
- the action the FortiGate unit took, for example, a file was blocked
- URL link to the FortiGuard Center which gives detailed information about the virus itself

The antivirus profile must have log settings enabled within it so that the FortiGate unit can record this activity, as well as having the antivirus profile applied to a firewall policy.

### Web Filter

Web filter logs record HTTP traffic activity. These log messages provide valuable and detailed information about this particular traffic activity on your network. Web filtering activity is important to log because it can inform you about:

- what types of web sites employees are accessing
- users attempting to access banned web sites and how often this occurs
- network congestion due to employees accessing the Internet at the same time
- web-based threats resulting from users visiting non-business-related web sites

Web Filter logs are an effective tool to help you determine if you need to update your web filtering settings within a web filter profile due to unforeseen threats or network congestion. These logs also inform you about web filtering quotas that have been configured for filtering HTTP traffic.

You must configure logging settings within the web filter profile and apply the filter to a firewall policy so that the FortiGate unit can record the activity.

### IPS (attack)

IPS logs, also referred to as attack logs, record attacks that occurred against your network. Attack logs contain detailed information about whether the FortiGate unit protected the network using anomaly-based defense settings or signature-based defense settings, as well as what the attack was.

The IPS or attack log file is especially useful because the log messages that are recorded contain a link to the FortiGuard Center, where you can find more information about the attack. This is similar to antivirus logs, where a link to the FortiGuard Center is provided as well that informs you of the virus that was detected by the FortiGate unit.

An IPS sensor with log settings enabled must be applied to a firewall policy so that the FortiGate unit can record the activity.

### Packet logs

When you enable packet logging within an IPS signature override or filter, the FortiGate unit examines network packets, and if a match is found, saves them to the attack log. Packet logging is designed to be used as a diagnostic tool that can focus on a narrow scope of diagnostics, rather than a log that informs you of what is occurring on your network.

You should use caution when enabling packet logging, especially within IPS filters. Filter configuration that contains thousands of signatures could potentially cause a flood of saved packets, which would take up a lot of storage space on the log device. It would also take a great deal of time to sort through all the log messages, as well as consume considerable system resources to process.

You can archive packets, but you must enable this option on the Log Settings page. If your log configuration includes multiple FortiAnalyzer units, packet logs are only sent to the primary (first) FortiAnalyzer unit. Sending packet logs to the other FortiAnalyzer units is not supported.

### Email filter

Email filter logs, also referred to as spam filter logs, record information regarding the content within email messages. For example, within an email filter profile, a match is found that finds the email message to be considered spam.

Email filter logs are recorded when the FortiGate unit finds a match within the email filter profile and logging settings are enabled within the profile.

If you are using a Banned Words List for email filtering, note that the filter pattern number is only recorded when the source email address contains a banned word.

### Archives (DLP)

Recording DLP logs for network use is called DLP archiving. The DLP engine examines email, FTP, IM, NNTP, and web traffic. Archived logs are usually saved for historical use and can be accessed at any time. IPS packet logs can also be archived, within the Log Settings page.

You can start with the two default DLP sensors that have been configured specifically for archiving log data, Content_Archive and Content_Summary. They are available in **Security Profiles > Data Leak Prevention**. Content_Archive provides full content archiving, while Content_Summary provides summary archiving. For more information about how to configure DLP sensors, see the Security Features chapter of the FortiOS Handbook.

You must enable the archiving to record log archives. Logs are not archived unless enabled, regardless of whether or not the DLP sensor for archiving is applied to the firewall policy.

### Network scan

Network scan logs are recorded when a scheduled scan of the network occurs. These log messages provide detailed information about the network's vulnerabilities regarding software, as well as the discovery of any further vulnerabilities.

A scheduled scan must be configured and logging enabled within the Event Log settings, for the FortiGate unit to record these log messages.

### Other Traffic

The traffic log also records interface traffic logging, which is referred to as Other Traffic. Other Traffic is enabled only in the CLI. When enabled, the FortiGate unit records traffic activity on interfaces as well as firewall policies. Logging Other Traffic puts a significant system load on the FortiGate unit and should be used only when necessary.

Logging other traffic works in the following way:

- firewall policy has logging enabled on it (Log Allowed Traffic) and other-traffic
- packet comes into an interface
- interface log packet is sent to the traffic log that is enabled on that particular interface
- possible log packet is sent regarding a match in the firewall policy, such as URL filter
- interface log packet is sent to the traffic log if enabled on that particular interface
- packet passes and is sent out an interface
- interface log packet is sent to traffic (if enabled) on that particular interface

### Event

The event log records administration management as well as FortiGate system activity, such as when a configuration has changed, admin login, or high availability (HA) events occur. Event logs are an important log file to record because they record FortiGate system activity, which provides valuable information about how your FortiGate unit is performing.

Event logs help you in the following ways:

- keeping track of configuration setting changes
- IPsec negotiation, SSL VPN and tunnel activity
- quarantine events, such as banned users
- system performance
- HA events and alerts
- firewall authentication events
- wireless events on models with WiFi capabilities
- activities concerning modem and internet protocols L2TP, PPP and PPPoE
- VIP activities
- AMC disk's bypass mode
- VoIP activities that include SIP and SCCP protocols.

As of 5.4, every 'execute' CLI command now generates an 'audit' event log, allowing you to track configuration changes. You can enable/disable this feature in the CLI:

```
config system global
   set cli-audit-log [enable|disable]
end
```

The FortiGate unit records event logs only when events are enabled.

### Traffic Shaping

Traffic shaping, per-IP traffic shaping and reverse direction traffic shaping settings can be applied to a firewall policy, appearing within the traffic log messages.

# FortiOS™ 5.6

Fortinet's Network Operating System

Control all the security and networking capabilities in all your Fortinet Security Fabric elements with one intuitive operating system. Improve your protection and visibility while reducing operating expenses and saving time with a truly consolidated next-generation enterprise firewall solution. FortiOS enables the Fortinet Security Fabric vision for enhanced protection from IoT to Cloud.


## Security Fabric Integration

Deep visibility and control throughout the Security Fabric reduce the attack surface from IoT to Cloud.

## Accelerated Performance

Accelerated cloud-scale and security processor-based appliances enable maximum threat protection without affecting performance, even when logging is turned on.

## Efficient Operations

Security Fabric Audit with recommendations and automated actions, local and global threat intelligence sharing, and single pane of glass with NOC views help better manage your network.

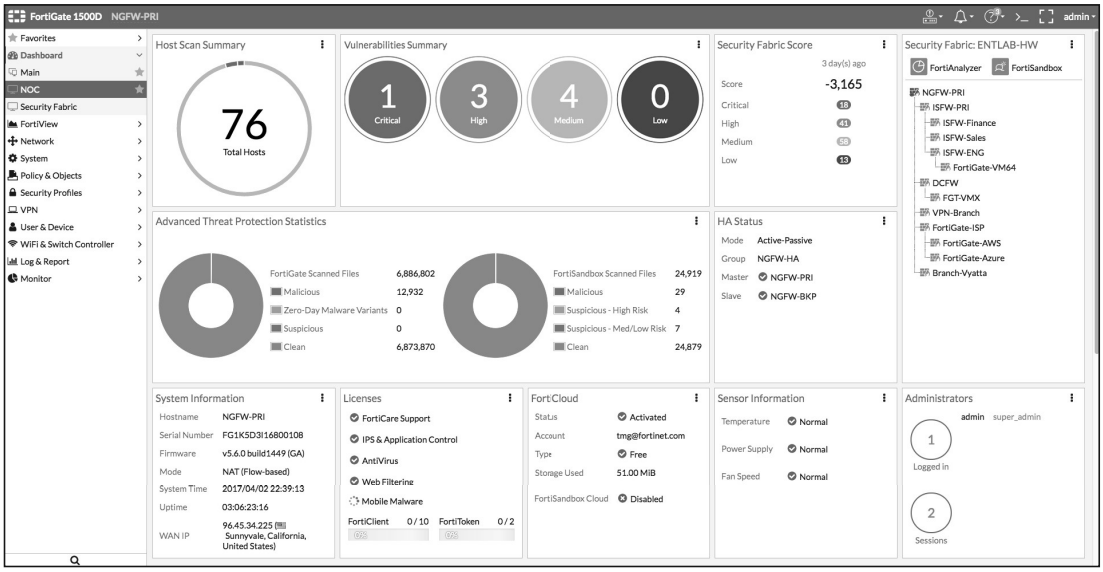
Seamlessly integrates with Fortinet centralized management solution and offers robust APIs.

## What's New — Highlights

- Security Fabric enhancements
- Security Fabric Audit
- Improved Dashboard
- Transparent web proxy
- NGFW policy mode
- Controlled failover between wireless controllers
- Multiple PSK for WPA Personal
- VXLAN support
- FortiView Endpoint Vulnerability chart
- FortiClient Profile updates
- CEF log support
- Adding Internet services to firewall policies
- Source and destination NAT in a single firewall policy
- NP6 Host Protection Engine

# OVERVIEW

## Introducing FortiOS 5.6




The transition to an evolving digital business model is one of the most challenging aspects of security today for an enterprise. As significant trends in computing and networking continue to drive changes across critical business infrastructures, architectures, and practices, organizations are looking for innovative network security solutions to help them embrace that evolution. The Fortinet Security Fabric, empowered by FortiOS 5.6, is an intelligent framework designed for scalable, interconnected security combined with high awareness, actionable threat intelligence, and open API standards for maximum flexibility and integration to protect even the most demanding enterprise environments. Fortinet's security technologies have earned the most independent certifications for security effectiveness and performance in the industry. The Fortinet Security Fabric closes gaps left by legacy point products and platforms by providing the broad, powerful, and automated protection that today's organizations require across their physical and virtual environments, from endpoint to the cloud.

## FortiOS 5.6 Anatomy

Control all the security and networking capabilities in all your FortiGates across your entire network with one intuitive operating system. FortiOS offers an extensive feature set that allows organizations of all sizes to deploy the security gateway setup that best suits their environments. As requirements evolve, you can modify them with minimal disruptions and cost.

<table>
<tr><td rowspan="2">Configuration</td><td rowspan="2">Log & Report</td><td rowspan="2">Diagnostics</td><td rowspan="2">Monitoring</td><td rowspan="2">Operation</td><td>Systems Integration</td><td>Central Mgmt. and Provisioning</td><td>Cloud & SDN Integration</td></tr>
<tr><td colspan="3">Visibility</td></tr>
<tr><td>Policy Objects</td><td>Device Identification</td><td>SSL inspection</td><td>Actions</td><td>Policy and Control</td><td colspan="2">AAA</td><td>Compliance</td></tr>
<tr><td>Anti-Malware</td><td>IPS & DoS</td><td>Application Control</td><td>Web Filtering</td><td rowspan="2">Security</td><td colspan="3" rowspan="2">Advanced Threat Protection (ATP)</td></tr>
<tr><td>Firewall</td><td>VPN</td><td>DLP</td><td>Email Filtering</td></tr>
<tr><td>SD WAN</td><td>Explicit Proxy</td><td>IPv6</td><td>High Availability</td><td rowspan="2">Networking</td><td rowspan="2">Wireless Controller</td><td rowspan="2">Switch Controller</td><td rowspan="2">WAN Interface Manager</td></tr>
<tr><td>Routing/NAT</td><td>L2/Switching</td><td>Offline Inspection</td><td>Essential Network Services</td></tr>
<tr><td>Physical Appliance (+SPU)</td><td>Virtual System</td><td>Hypervisor</td><td>Cloud</td><td>Platform Support</td><td colspan="3">Security Fabric</td></tr>
</table>

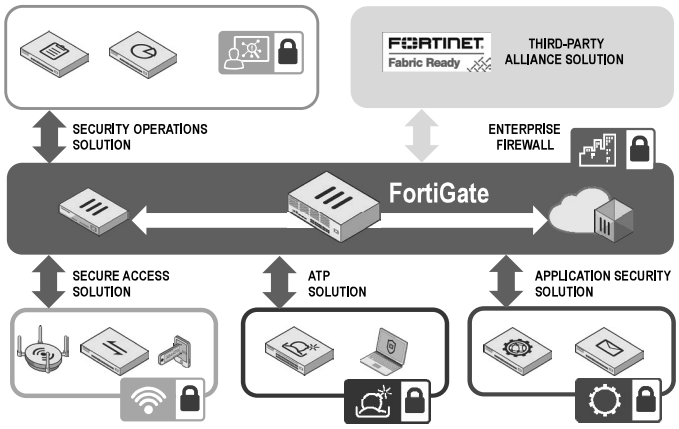
# HIGHLIGHTS

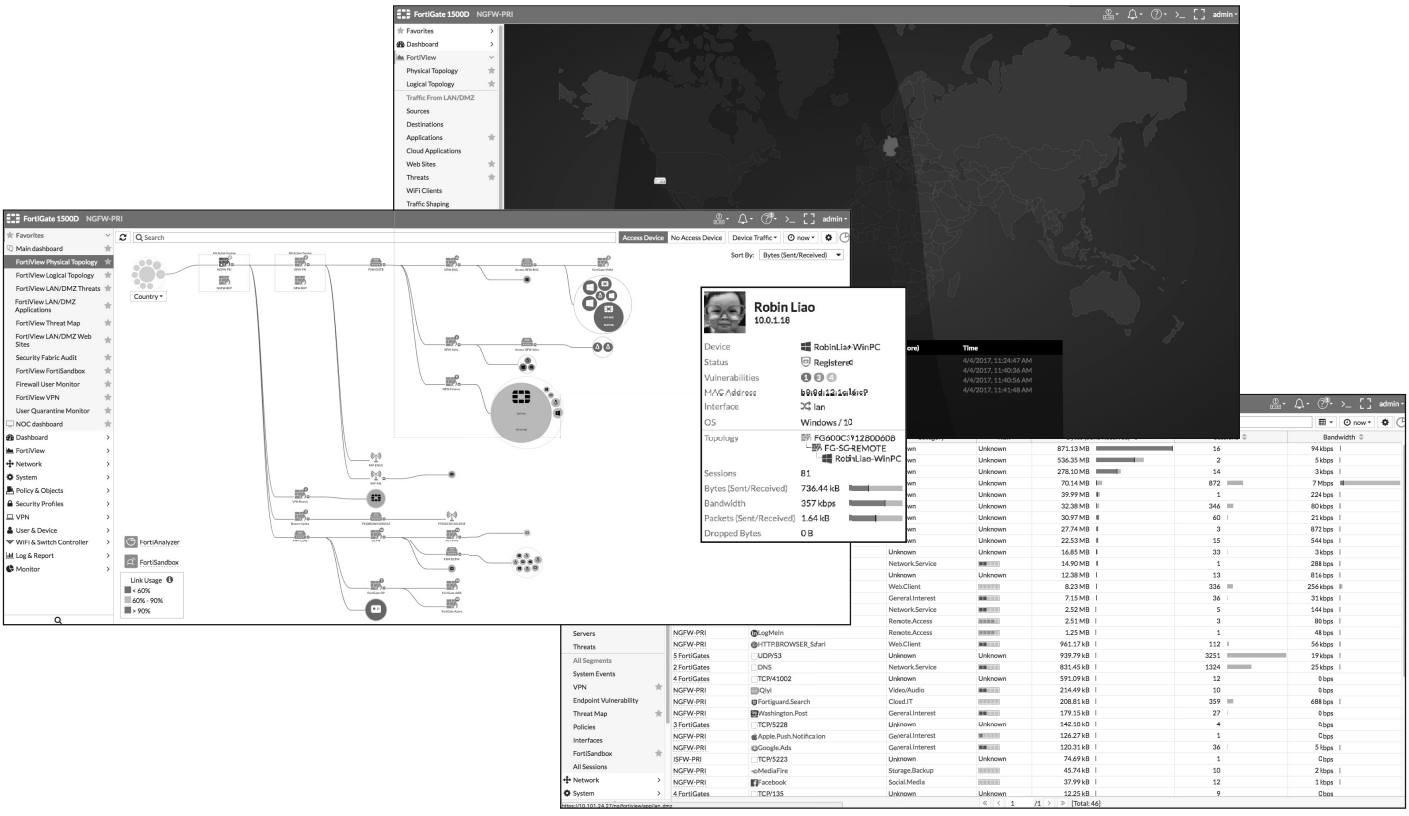
## Security Fabric

### FortiGate Integration

The Security Fabric allows security to dynamically expand and adapt as more and more workloads and data are added, and at the same time, seamlessly follow and protect data, users, and applications as they move back and forth between IoT, smart devices, and cloud environments throughout the network.

A FortiGate firewall may be deployed at the heart of the Security Fabric, expanding its security reach via visibility and control, by tightly integrating with other FortiGates and Fortinet products, plus Fabric-Ready solutions.




FortiView

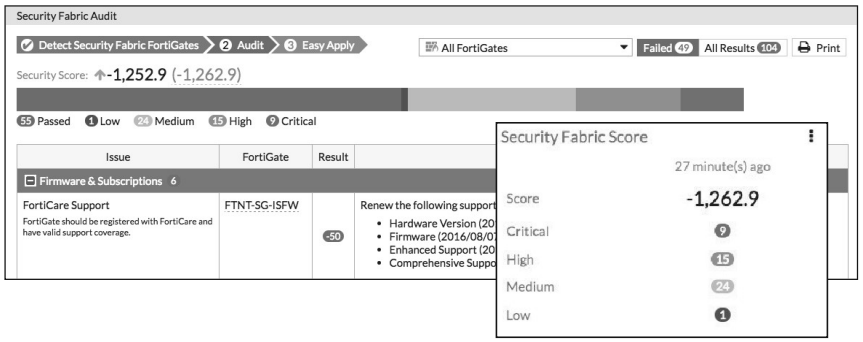
### Visibility

FortiView, in FortiOS 5.6, provides you with 360° visibility into your network traffic. With a single click you can view traffic by source, destination, application, threat, interface, device, policy, and country. Graphical visualizations, such as country and topology maps and volume-based bubble charts are available in addition to comprehensive table views. These allow you to identify issues quickly and intuitively.

# HIGHLIGHTS

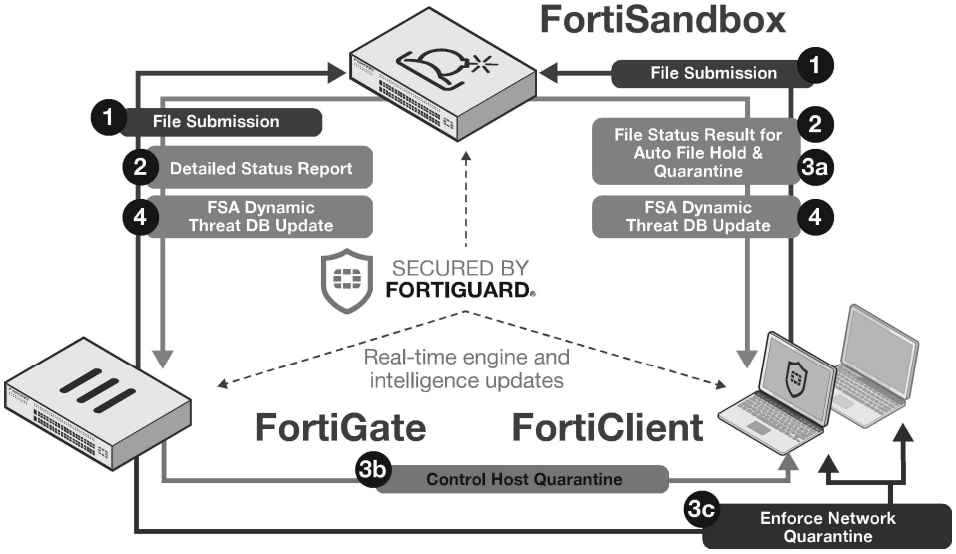
### Compliance

The Security Fabric Audit is a feature that allows you to analyze your Security Fabric deployment to identify potential vulnerabilities and highlight best practices that could be used to improve your network's overall security and performance. Also, by checking your Security Fabric Score, which is determined based on how many checks your network passes/fails during the Audit, you can be confident that your network is getting more secure over time.




### Advanced Threat Protection

Fortinet offers the most integrated and automated Advanced Threat Protection (ATP) solution available today through an ATP framework that includes FortiGate, FortiSandbox, FortiMail, FortiClient, and FortiWeb. These products easily work together to provide closed loop protection across all of the most common attack vectors. All products in the ATP framework are NSS Labs Recommended for both security effectiveness and performance value.




**Query**

1. File submission for analysis
2. Respective analysis results are returned

**Remediation**

3a. Auto File Quarantine on host with option to hold file until result

3b. Manual Host Quarantine by administrator

3c. Manual Source IP Quarantine using firewall

**Protection**

4. Proactive dynamic Threat DB update to gateway and host

| FEATURE | HIGHLIGHTS | THE FORTINET ADVANTAGE |
|---|---|---|
| System Integration | ▪ Standard-based monitoring output – SNMP Netflow/Sflow<br>▪ Syslog support to external (third-party) SIEM and logging system<br>▪ Technology alliance with specialized vendors in heterogeneous environment<br>▪ Native Integration with Fortinet Products — FortiMail, FortiCache, and FortiWeb | ▪ Detailed logs and SNMP output provide more insights so that organizations can accurately and quickly identify and resolve incidents or problems.<br>▪ Ability to reuse organization's existing systems lowers TCO and streamlines processes. |

# HIGHLIGHTS

| FEATURE | HIGHLIGHTS | THE FORTINET ADVANTAGE |
|---|---|---|
| Central Management and Provisioning | ▪ Fortinet/third-party automation and portal services support via APIs and CLI scripts<br>▪ Rapid deployment features including cloud-based provisioning solutions<br>▪ Developer community platform and professional service options for complex integrations | ▪ Comprehensive APIs and CLI commands offer feature-rich service enablement.<br>▪ Comprehensive rapid deployment options save time and costs.<br>▪ Fortinet Developer Network (FNDN) empowers large service providers and enterprises with shared implementation/customization/ integration knowledge. |
| Cloud and SDN Integration | ▪ Integration with Openstack, VMware NSX, and Cisco ACI infrastructure | ▪ Robust and comprehensive SDN integration capabilities allow organizations to implement cloud solutions securely without compromising agility. |
| Visibility | ▪ Drill-down and topology viewers that illustrate real-time and historical threat status and network usage with comprehensive contextual information<br>▪ **NEW:** Aggregated data views with remote control of downstream FortiGates<br>▪ **NEW:** Endpoint vulnerability views that present ranked vulnerable clients with details | ▪ One-click remediation against listed sources/destinations offers accurate and quick protection against threats and abuses.<br>▪ Unique threat score system correlates weighted threats with particular users to prioritize investigations.<br>▪ Fabric-wide views expand visibility beyond a single security entity, including endpoint vulnerabilities. |
| Authentication Authorization and Accounting (AAA) | ▪ Interface with FortiAuthenticator and a wide variety of external identity management systems to facilitate user authentication processes.<br>▪ Wide-ranging single sign-on identity acquisition methods, including Windows AD, terminal servers, access portals, and mail services<br>▪ Built-in token server that manages both physical and mobile tokens for use with various FortiOS authentication requirements such as VPN access and FortiGate administration. | ▪ FortiOS integrates with a wide variety of AAA services to facilitate user admission control from various entry points, giving users a simplified experience while implementing greater security.<br>▪ Easily implement two-factor authentication for user and administrator access at little cost. |
| Compliance | ▪ Periodic system configuration check using a pre-defined PCI-compliance checklist<br>▪ Endpoint enforcement: posture checking profile assignment based on device/user groups<br>▪ NEW: Fabric-wide FortiGate security configuration and client vulnerability status audits | ▪ Automates compliance auditing which frees up administration resources<br>▪ Simplified mobile user security enforcement by easily distributing and updating clients' security profiles that are consistent with gateway protection<br>▪ Quickly verify the status and health of your connected devices within the Fabric and identify any gaps that can potentially leave you at greater risk |
| Advance Threat Protection (ATP) | ▪ Flow- and proxy-based AV options for choice between protection and performance<br>▪ Local file quarantine (for models with storage)<br>▪ Anti-bot capability using IP reputation DB terminates botnet communication to C&C servers<br>▪ Receive dynamic remediation (malicious file checksum and URLs) DB updates and detail analysis reports from external Fortinet file analysis solution (FortiSandbox) | ▪ Supported by proven and industry-validated AV research services<br>▪ Ability to adopt robust ATP framework that reaches mobile users and branch offices, detecting and preventing advanced attacks that may bypass traditional defenses by examining files from various vectors, including encrypted files |
| Wireless Controller | ▪ Integrated wireless controller for Fortinet's wide range of AP form factors, including indoor, outdoor, and remote models, with no additional license or component fees<br>▪ Enterprise-class wireless management functionality, including rogue AP protection, wireless security, monitoring, and reporting<br>▪ **NEW:** 802.3az support on WAVE2 WiFi APs<br>▪ **NEW:** Manage distirbuted cloud-based FortiAPs | ▪ The wireless controller integrated into the FortiGate console provides true single-pane-of-glass management for ease-of-use and lower TCO. |
| Switch Controller | ▪ Integrated switch controller for Fortinet access switches with no additional license or component fees<br>▪ **NEW:** Improved GUI configuration support | ▪ Expands security to access level to stop threats and protect terminals from one another |
| WAN Interface Manager | ▪ Supports the use of 3G/4G modems via USB port or FortiExtender | ▪ Allows organizations to use or add 3G/4G connectivity for WAN connections while maintaining access control and defining usage for those links |

# HIGHLIGHTS

## Operation

FortiOS provides a broad set of operation tools that make identification and response to security and network issues effective. Security operations is further optimized with automations which contribute to faster and more accurate problem resolutions.

| FEATURE | HIGHLIGHTS | THE FORTINET ADVANTAGE |
|---|---|---|
| Configuration | ▪ Wide variety of configuration tools — Client software, Web UI, and CLI<br>▪ Ease of use with intuitive, state-of-the-art GUI and wizards<br>▪ One-click access and actions between log viewers, FortiView, policy tables, and more<br>▪ Intelligent object panel for policy setups and edits | ▪ Unique FortiExplorer configuration tool allows administrators to quickly access configurations, including via mobile phones and tablets.<br>▪ VPN wizards facilitate easy setup, including to popular mobile clients and other vendors' VPN gateways.<br>▪ Useful one-click access and actions bring administrators to next steps quickly and accurately to swiftly mitigate threats or resolve problems. |
| Log & Report | ▪ Detailed logs and out-of-the-box reports that are essential for compliance, audits, and diagnostic purposes<br>▪ **NEW:** Real-time logging to FortiAnalyzer and FortiCloud<br>▪ **NEW:** Common Event Format (CEF) support<br>▪ **NEW:** Logging consolidation within Security Fabric | ▪ Includes deep contextual information, including source device details and strong audit trail<br>▪ GUI Report Editor offering highly customizable reports<br>▪ Managing logs holistically simplifies configuration and guarantees that critical information from every FortiGate is centrally collected and available for analysis. This closes any gaps in intelligence. |
| Diagnostics | ▪ Diagnostic CLI commands, session tracer, and packet capture for troubleshooting hardware, system, and network issues<br>▪ Hardware testing suite on CLI<br>▪ Policy and routing GUI tracer | ▪ Comprehensive diagnostic tools help organizations quickly remediate problems and investigate abnormal situations. |
| Monitoring | ▪ Real-time monitors<br>▪ **NEW:** NOC Dashboard | ▪ Dashboard NOC view allows you to keep mission-critical information in view at all times. Interactive and drill-down widgets avoid dead-ends during your investigations, keeping analysis moving quickly and smoothly. |

## Policy and Control

FortiGate provides a valuable policy enforcement point in your network where you can control your network traffic and apply security technologies. With FortiOS, you can set consolidated policies that include granular security controls. Every security service is managed through a similar paradigm of control and can be easily plugged into a consolidated policy. Intuitive drag-and-drop controls allow you to easily create policies and one-click navigation shortcuts allow you to more quickly quarantine end points or make policy edits.

| FEATURE | HIGHLIGHTS | THE FORTINET ADVANTAGE |
|---|---|---|
| Policy Objects | ▪ GeoIP and FQDN defined address objects to intelligently track dynamic IP/IP ranges<br>▪ Internet Service DB: dynamically updated DB that provides a list of popular cloud applications with their vital information that can be used for policy setup, routing, and link load-balancing configurations. | ▪ Comprehensive range of object types that facilitate today's dynamic and granular network requirements |
| Device Identification | ▪ Identification and control of network access for different types of devices present on the network<br>▪ **NEW:** Improved device identification and management | ▪ Empowers organizations to add critical security to today's BYOD environment by identifying and controlling personal devices |
| SSL Inspection | ▪ Effectively examine SSL-encrypted traffic with various security controls, such as AV and DLP<br>▪ High-performance SSL inspection with content processors<br>▪ Reputable sites database for exemptions | ▪ Identify and block threats hidden within encrypted traffic without significantly impacting performance. |
| Actions | ▪ Implements security policies that use a combination of source objects, IPs, users, and/or devices.<br>▪ Highly customizable notifications are sent when user activities are not allowed.<br>▪ Automatically or manually quarantine users/attackers.<br>▪ Directs registered FortiClient to host quarantine. | ▪ Flexible policy setup using additional identified elements and active user notifications assist organizations in implementing effective network security, while robust quarantining features helps to mitigate threats. |

# HIGHLIGHTS

## Security

FortiGuard Labs provides the industry-leading security services and threat intelligence delivered through Fortinet solutions. FortiOS manages the broad range of FortiGuard services available for the FortiGate platform, including application control, intrusion prevention, web filtering, antivirus, advanced threat protection, SSL inspection, and mobile security. Services can be licensed a la carte or in a cost-effective bundle for maximum flexibility of deployment.

**Industry-leading security effectiveness**

Fortinet solutions are consistently validated for industry-leading security effectiveness in industry tests by NSS Labs for IPS and application control, by Virus Bulletin in the VB100 comparative anti-malware industry tests, and by AV Comparatives.

- Recommended Next Generation Firewall with near perfect, 99.6% security effectiveness rating. (2016 NSS Labs NGFW Test of FortiGate 3200D)
- Recommended Breach Detection Systems with 99%+ overall detection. (2016 NSS Breach Detection Systems Test of FortiGate 500D with FortiSandbox Cloud)
- Recommended Data Center Intrusion Prevention Systems with 99.9% exploit block rate, highest in test. (2016 NSS Data Center Intrusion Prevention Test with FortiGate 3000D)
- Highest antivirus security effectiveness of any vendor offering a next generation firewall and 2nd highest security effectiveness of all business antivirus solutions tested. (Oct 2014–April 2015 Virus Bulletin Reactive and Proactive Test average results)
- ICSA Certified network firewalls, network IPS, IPsec, SSL-TLS VPN, antivirus.

| FEATURE | HIGHLIGHTS | THE FORTINET ADVANTAGE |
|---|---|---|
| Anti-Malware | ▪ Flow- and proxy-based AV options for choice between protection and performance.<br>▪ Anti-bot capability using IP reputation DB terminates botnet communication to C&C servers.<br>▪ Receive dynamic remediation (malicious file checksum and URLs) DB updates and detail analysis reports from external Fortinet file analysis solution (FortiSandbox). | ▪ Supported by proven and industry-validated AV research services.<br>▪ Ability to adopt robust ATP framework that reaches mobile users and branch offices, detecting and preventing advanced attacks that may bypass traditional defenses by examining files from various vectors, including encrypted files. |
| IPS and DoS | ▪ Regular and rate-based signatures, supported by zero-day threat protection and research for effective. IPS implementation.<br>▪ Integrated DoS protection defends against abnormal traffic behaviors.<br>▪ CVE reference for IPS signatures. | ▪ Proven quality protection with "NSS Recommended" award for superior coverage and cost/performance.<br>▪ Adapts to enterprise needs with full IPS features and NGIPS capabilities, such as contextual visibility.<br>▪ Supports various network deployment requirements, such as sniffer mode, and compatible with active-bypass FortiBridge or built-in bypass ports for selected model. |
| Application Control | ▪ Detects and acts against traffic based on applications while providing visibility on network usage.<br>▪ Fine-grained control on popular cloud applications, such as SalesForce, Google Docs, and Dropbox. | ▪ Superior coverage, including both desktop and mobile applications, enabling better management of network access policies.<br>▪ Applies deeper application inspections for better control and visibility as more enterprises rely on public cloud services. |
| Web Filtering | ▪ Enterprise-class URL filtering solution that includes quotas, user overrides, transparent safe search, and search engine keyword logging.<br>▪ Superior coverage with URL ratings of over 70 languages and identifies redirected (cached and translated) sites. | ▪ Multi-layered anti-proxy avoidance capabilities with integrated application control and IPS allow organizations to implement air-tight web usage controls. |

# HIGHLIGHTS

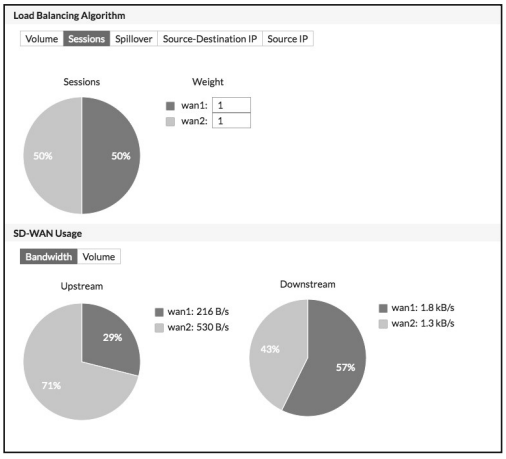
| FEATURE | HIGHLIGHTS | THE FORTINET ADVANTAGE |
|---|---|---|
| Firewall | ▪ High-performance firewall with SPU-powered appliance<br>▪ Easy-to-use policy management with unique Section or Global View options<br>▪ **NEW:** NGFW Policy-Based Mode | ▪ Industry's top firewall appliance with superior cost-performance ratio |
| VPN | ▪ Comprehensive enterprise-class features for various types of VPN setups<br>▪ SSL and IPsec VPN wizards | ▪ The FortiGate's unmatched performance for VPN allows organizations to establish secure communications and data privacy between multiple networks and hosts by leveraging custom security processors (SPUs) to accelerate encryption and decryption of network traffic. |
| DLP | ▪ Monitor network traffic and stop sensitive information from leaving the network by matching against file format and content definitions.<br>▪ The FortiExplorer Watermark Tool allows organizers to apply document marking for DLP. | ▪ Prevent sensitive information from leaving the network, easily and cost-effectively. |
| Email Filtering | ▪ Highly effective, multilayered spam filters with low false positives | ▪ Cost-efficient anti-spam solution for small organizations or branch<br>▪ offices without requiring investment in an additional system |

## Networking

With FortiOS you can manage your networking and security in one consistent native OS on the FortiGate. FortiOS delivers a wide range of networking capabilities, including extensive routing, NAT, switching, Wi-Fi, WAN, load balancing, and high availability, making the FortiGate a popular choice for organizations wanting to consolidate their networking and security functions.

### SD WAN

Fortinet's Distributed Enterprise Firewall enables software-defined WAN (SD-WAN). It essentially links network and security paths across the world through the Internet or private WAN links, making it a truly borderless infrastructure for the enterprise. In addition, it provides application visibility and intelligent load balancing. Consolidation and control of network security features in a centralized environment simplifies administration.




| FEATURE | HIGHLIGHTS | THE FORTINET ADVANTAGE |
|---|---|---|
| Routing / NAT | ▪ Comprehensive routing protocols and NAT support<br>▪ Traffic redirection with ICAP and WCCP support | ▪ Wide ranging routing features that meet carrier and enterprise resilience networking requirements |
| L2 / Switching | ▪ Ability to craft software switches or emulate VLAN switches from interfaces<br>▪ Support SPAN ports and port aggregation with multiple interfaces.<br>▪ Implement admission control modes on interfaces such as 802.1x or captive portal.<br>▪ Comprehensive WiFi and WAN interface configuration options<br>▪ **NEW:** VXLAN support | ▪ Flexible interface configurations offer various setup possibilities that best suit an organization's network requirements, while providing optional access security. |
| Offline Inspection | ▪ Sniffer mode allows threat and usage monitoring of network activities offline. | ▪ Offline mode provides flexibility when deploying into existing critical networks where in-line security solution is not yet appropriate. |

# HIGHLIGHTS

| FEATURE | HIGHLIGHTS | THE FORTINET ADVANTAGE |
|---|---|---|
| SD WAN | ▪ Comprehensive WAN Link LB algorithm, link status, plus quality checks, and policy routing support<br>▪ Direct traffic among WAN links based on applications and users/ user groups<br>▪ Manage the level of service and preference given to the various types and sources of traffic using traffic policing, traffic shaping, and queuing.<br>▪ Peer-to-peer and remote user WAN optimization for protocol optimization and byte caching technologies<br>▪ Web cached storage of remote files and web pages on local devices for easy local access to commonly accessed objects | ▪ Robust multi-link feature aids organizations in SD-WAN implementation.<br>▪ QoS capabilities adjust allocation of bandwidth to different traffic types, improving the performance and stability of latency-sensitive or bandwidth-intensive network applications.<br>▪ Built-in WAN optimization capabilities reduce network overhead, resulting in more efficient use of bandwidth and better application performance, without the need for costly WAN link upgrades. |
| High Availability | ▪ Support for industry standard VRRP and various proprietary solutions, with ability to combine more than one high availability solution into a single configuration | ▪ Flexible high availability offerings allow organizations to pick the most suitable solutions based on their network environments and SLA requirements. |
| IPv6 | ▪ Comprehensive IPv6 support for routing, NAT, security policies, and more | ▪ Operating mode options provide flexibility when deploying into existing or new networks, reducing network change requirements. |
| Explicit Proxy | ▪ Explicit HTTP and HTTPS, FTP over HTTP, or SOCKS proxying of IPv4 and IPV6 traffic on one or more interfaces<br>▪ **NEW:** Transparent web proxy | ▪ Integrated, enterprise-class explicit web proxy provides HTTP and HTTPS proxying with the added benefits of UTM security and user identity. |
| Essential Network Services | ▪ A wealth of networking services such as DHCP, DNS server, NTP server etc. | ▪ Built-in, out-of-the-box capabilities let organizations quickly provide necessary network services to internal terminals or to integrate with other network devices. |

## Platform Support


**Performance**

The FortiGate appliances deliver up to 5 times the next generation firewall performance and 10 times the firewall performance of equivalently priced platforms from other vendors. The high performance levels in the FortiGate are based on a Parallel Path Processing architecture in FortiOS that leverages performance, optimized security engines, and custom developed network and content processors. Thus, FortiGate achieved the best cost per Mbps performance value results.

**Ultimate deployment flexibility**

Protect your entire network inside and out through a policy-driven network segmentation strategy using the Fortinet solution. It is easy to deploy segment optimized firewalls, leveraging the wide range of FortiGate platforms and the flexibility of FortiOS to protect internal network segments, the network perimeter, distributed locations, public and private clouds, and the data center — making sure you have the right mix of capabilities and performance for each deployment mode.

| FEATURE | HIGHLIGHTS | THE FORTINET ADVANTAGE |
|---|---|---|
| Physical Appliance (+SPU) | ▪ Integration with proprietary hardware architecture that includes acceleration components (SPU) and multicore processors. | ▪ Superior software and hardware integration ensures most optimal use of hardware components, yielding best cost/performance for customers. |
| Virtual Systems | ▪ Virtual Domains (VDOMs): Virtualized FOS components to multiple logical systems on a single virtual or physical appliance.<br>▪ Proxy and Flow-based VDOM options to simplify security profile settings | ▪ Offers MSSPs and large organizations the ability to run separate instances of FOS for multi-tenant environment or to consolidate various security gateways for lower TCO. |
| Hypervisor | ▪ Support for popular hypervisor platforms, including VMware vSphere, Citrix and open source Xen, KVM, and MS Hyper-V. | ▪ Consistent management and features between physical and virtual appliances reduces management cost and simplifies deployments. |
| Cloud | ▪ Support for public cloud services: Amazon Web Services (AWS) and Microsoft Azure. | ▪ Consistent management and features between on-premises and cloud platforms reduces management cost and simplifies deployments. |

# SPECIFICATIONS

## Security Fabric

### SYSTEM INTEGRATION

SNMP System Monitoring:
- SNMP v1and v2c support
- SNMP v3 implementation includes support for queries, traps, authentication, and privacy
- SNMP traps alerting to events such as a full log disk or a virus detected

Traffic Monitoring:
- sFlow version 5 and Netflow V9.0

External Logging:
- Syslog
- Reliable syslog (RAW Profile) based on RFC 3195
- WebTrends WELF compatible

Technology ecosystem encompasses leading partners in the Firewall and Network Risk Management, SDN and Virtualization, Security Information and Event Management (SIEM), Systems Integration, Testing and Training, and Wireless markets

Native integration with FortiMail, FortiCache, and FortiWeb

Security Fabric logging
- Synchronised logging to FortiAnalyzer configurations among FortiGates
- Data exchange (information such as topology and device asset tags) with FortiAnalyzer

### CENTRAL MANAGEMENT AND PROVISIONING

Central management support: FortiManager, FortiCloud hosted service, web service APIs

Rapid deployment: Install wizards, USB auto-install, local and remote script execution

### CLOUD AND SDN INTEGRATION

Integration with Openstack, VMWare NSX, and Cisco ACI infrastructure

### VISIBILITY

Interactive and graphical visualizer for user, device, network, and security activities (FortiView):
- A variety of GUI consoles that display current and historical status using different perspectives such as 'sources', 'destinations', 'interfaces', 'applications', 'threats' etc.
- Phyiscal and logical topology views
- Threat and VPN map
- Data views options: Table, bubble chart, or world map if applicable
- File analysis/sandbox result view (FortiSandbox integration required)
- Endpoint Vulnerbility view (FortiClient integration required)
- Accelerated session indication on 'All sessions' FortiView Console
- WHOIS Lookup for Public IP addresses within FortiView and log tables

Aggregated data views with downstream FortiGates within a Security Fabric
- presented on FortiView and monitors

### AUTHENTICATION AUTHORIZATION AND ACCOUNTING (AAA)

Local user database and remote user authentication service support: LDAP, Radius and TACACS+, two-factor authentication

Single-sign-on: Intergation with Windows AD, Microsoft Exchange Server, Novell eDirectory, FortiClient, Citrix and Terminal Server Agent, Radius (accounting message), POP3/POP3S, user access (802.1x, captive portal) authentication

PKI and certificates: X.509 certificates, SCEP support, Certificate Signing Request (CSR) creation, auto-renewal of certificates before expiry, OCSP support

Integrated token server that provisions and manages physical, SMS, and Soft One Time Password (OTP) tokens

### COMPLIANCE

Run a series of system configuration compliance check and log results periodically or on-demand

Security Fabric Audit: Audit FortiGate within the fabric, provide results and recommendation, then allow users to easily apply remediations for some items.

Manages network devices compliance via client software:
- Posture checking: Enforce client software installation and desired settings accordingly to device type/group and/or user/usergroup and/or locations (IPs)
- Quarantine clients if hit vulnerability level threshold

### ADVANCE THREAT PROTECTION (ATP)

External cloud-based or on-premise file analysis (OS sandbox) integration:
- File submission (with option to select types)
- Receive file analysis reports
- Receive dynamic signature updates from file analysis system (file checksum and malicious URL DB)

### WIRELESS CONTROLLER

Manages and provisions settings for local and remote Thin Access points or switches (selected models)

Set up access and authentication methods for SSIDs and VLANs, supports integrated or external captive portal, 802.1x, preshared keys

Multiple PSK for WPA Personal

WiFi Security: Rogue AP suppression, wireless IDS

Wireless topology support: Fast roaming, AP load balancing, Wireless Mesh and bridging

Controlled failover between wireless controllers

### SWITCH CONTROLLER

Extends access control and security to wired devices by managing Fortinet switches (FortiSwitch) via CAPWAP-like communication.

Ability to configure switch port features such as PoE, VLAN assignment

### WAN INTERFACE MANAGER

Support USB 3G/4G Wireless WAN modems

## Operation

### CONFIGURATION

Management Access: HTTPS via web browser, SSH, telnet, console

FortiExplorer:
- Management client for Windows and IOS platforms
- Ease-of-use by using USB connectivity

Feature Store: Toggle GUI component displays

GUI configuration:
- 'One-Click' access that transfer administrators to next step panels quickly
- Dynamic object selectors and predictive search queries

Web UI administration language support: English, Spanish, French, Portuguese, Japanese, Simplified Chinese, Traditional Chinese, Korean

### LOG & REPORT

Logging facilities support: Local memory & storage (if available), multiple syslog servers, multiple FortiAnalyzers, WebTrends servers, FortiCloud hosted service

Reliable logging using TCP option (RFC 3195)

Encrypted logging & log Integrity with FortiAnalyzer

Scheduled batch log uploading or real-time logging

Detailed traffic logs:fForwarded, violated sessions, local traffic, invalid packets

Comprehensive event logs: systems & administrators activity audits, routing & networking, VPN, user authentications, WiFi related events

Brief traffic log format option

Sending logs to syslog servers in Common Event Format (CEF)

IP and service port name resolution option

### DIAGNOSTICS

Diagnostic CLI commands, session tracer, and packet capture for troubleshooting hardware, system, and network issues.

Policy and routing GUI tracer

Packet flow CLI tracer

Hardware testing suite on CLI

### MONITORING

Graphical Monitors: Real-time system, network service, and users status viewers

Dashboard: customized widgets and layout

## Policy and Control

### POLICY OBJECTS

Policy objects: predefined, customs, object grouping, tagging, and coloring

Address objects: subnet, IP, IP range, GeoIP (Geography), FQDN

Internet Service DB: Dynamically updated DB that provides a list of popular cloud applications with their vital information that can be used for policy setup, routing and link load-balacing configurations.

# SPECIFICATIONS

## Security

### DEVICE IDENTIFICATION

Device Identification: Device and OS fingerprinting, automatic classification, inventory management

Support for MAC Authentication enforcement and bypass

### SSL INSPECTION

Inspect SSL encrypted traffic option for IPS, application control, antivirus, web filtering, and DLP

SSL MITM Mirroring

SSL Inspection Method options: SSL certificate inspection or full SSL inspection

SSL inspection exemption by site reputation DB, web categories, and/or policy addresses

### ACTIONS

User notifications: customizable replacement message for block sites and attachments

Web Browser top banner insert (Fortinet Bar): shows application control violations, Endpoint control enforcement, web browsing quota etc

User quarantine:
- Manually assigned with perpetual or customizable duration
- Automatically when triggered by violated IPS signature

### ANTI-MALWARE

Botnet server IP blocking with global IP reputation database

Antivirus database type selection (on selected models)

Flow-based or proxy-based AV option:
- Support for popular web, mail, and FTP protocols
- Scan encrypted traffic with SSL inspection

Option to treat Windows executables in email attachments as viruses

File quarantine (local storage required)

### IPS AND DOS

IPS engine: 7,000+ up-to-date signatures, protocol anomaly detection, rate-based detection, custom signatures, manual, automatic pull or push signature update, threat encyclopedia integration

IPS Actions: Default, monitor, block, reset, or quarantine (attackers IP, attackers IP and Victim IP, incoming interface) with expiry time

Filter-Based Selection: Severity, target, OS, application, and/or protocol

Packet logging option

IP(s) exemption from specified IPS signatures

IPv4 and IPv6 rate-based DOS protection (available on most models) with threshold settings against TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCTP/ICMP session flooding (source/destination)

IDS sniffer mode

Active bypass with bypass Interfaces (selected models) and FortiBridge

### APPLICATION CONTROL

Detects thousands of applications in 18 Categories: Business, Cloud IT, Collaboration, Email, Game, General Interest, Mobile, Network Service, P2P, Proxy, Remote Access, Social Media, Storage/Backup, Update, Video/Audio, VoIP, Web Chat and Industrial.

Custom application signature support

Supports detection for traffic using HTTP/2 protocol and able to block QUIC traffic so taht browser automatically falls back to HTTP/2 + TLS 1.2

Filter-based overrides: By behavior, category, popularity, technology, risk, vendor, and/or protocol

Actions: Allow, block, reset session (CLI only), monitor only

SSH Inspection

Deep application control over popular public cloud services, such as SalesForce, Google Docs, and Dropbox

### WEB FILTERING

Web filtering inspection mode support: Proxy-based, flow-based, and DNS

Manually defined web filtering based on URL, web content and MIME header

Dynamic web filtering with cloud-based real-time categorization database:
- Over 250 million URLs rated into 78 categories, in 70 languages

Safe Search enforcement: transparently inserts Safe Search parameter to queries. Supports Google, Yahoo!, Bing and Yandex, definable YouTube Education Filter

Proxy avoidance prevention: Proxy site category blocking, rate URLs by domain & IP address, block redirects from cache & translation sites, proxy avoidance application blocking (application control), proxy behavior blocking (IPS)

Web filtering local categories & category rating override

Web filtering profile override: Allows administrator to temporarily assign different profiles to user/user group/IP

Restrict access to Google Corporate Accounts only

Additional features offered by proxy-based web filtering:
- Filter Java Applet, ActiveX, and/or cookie
- Block HTTP Post
- Log search keywords
- Rate images by URL
- Block HTTP redirects by rating
- Exempt scanning encrypted connections on certain categories for privacy
- Web Browsing quota by categories

### FIREWALL

Operating modes: NAT/route and transparent (bridge)

Schedules: One-time, recurring

Session helpers and ALGs: DCE/RPC, DNS-TCP, DNS-UDP, FTP, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle)

VoIP traffic support: SIP/H.323 /SCCP NAT traversal, RTP pin holing

Protocol type support: SCTP, TCP, UDP, ICMP, IP

User and device-based policies

Policy Management: Section or global policy management view

NGFW policy mode: setup policies with applications and URLs as objects

### VPN

Customizable SSL VPN portal: Color themes, layout, bookmarks, connection tools, client download

SSL VPN realm support: Allows multiple custom SSL VPN logins associated with user groups (URL paths, design)

Single-sign-on bookmarks: reuse previous login or predefined credentials to access resources

Personal bookmarks management: allow administrators to view and maintain remote client bookmarks

Limit SSL portal concurrent users

One time login per user options: Prevents concurrent logins using same username

SSL VPN web mode: For thin remote clients equipped with a web browser only and support web application, such as HTTP/HTTPS Proxy, FTP, Telnet, SMB/CIFS, SSH, VNC, RDP, Citrix

SSL VPN tunnel mode: for remote computers that run a variety of client and server applications, SSL VPN client supports MAC OSX, Linux, Windows Vista and with 64-bit Windows operating systems

SSL VPN port forwarding mode: uses a Java Applet that listens on local ports on the user's computer. When it receives data from a client application, the port forward module encrypts and sends the data to the SSL VPN device, which then forwards the traffic to the application server.

Host integrity checking and OS check (for windows terminals only) prior to SSL tunnel mode connections

MAC host check per portal

Cache cleaning option just before the SSL VPN session ends

Virtual desktop option to isolates the SSL VPN session from the client computer's desktop environment

IPsec VPN:
- Remote peer support: IPsec-compliant dialup clients, peers with static IP/dynamic DNS
- Authentication method: Certificate, pre-shared key
- IPsec Phase 1 mode: Aggressive and main (ID protection) mode
- Peer acceptance options: Any ID, specific ID, ID in dialup user group
- Supports IKEv1, IKEv2 (RFC 4306)
- IKE mode configuration support (as server or client), DHCP over IPsec
- Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128, AES192, AES256
- Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512
- Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14
- XAuth support as client or server mode
- XAuth for dialup users: Server type option (PAP, CHAP, Auto), NAT Traversal option
- Configurable IKE encryption key expiry, NAT traversal keepalive frequency
- Dead peer detection
- Replay detection
- Autokey keep-alive for Phase 2 SA

IPsec Configuration Wizard for termination with popular third-party devices

IPsec VPN deployment modes: Gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel, VPN termination in transparent mode,

IPsec VPN Configuration options: Route-based or policy-based

VPN monitoring: View and manage current IPsec and SSL VPN connections in details

Other VPN support: L2TP client (on selected models) and server mode, L2TP over IPsec, PPTP, GRE over IPEC

# SPECIFICATIONS

### DLP

Web filtering inspection mode support: proxy-based, flow-based and DNS

DLP message filter:
- Protocol supported: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP
- Actions: Log only, block, quarantine user/IP/Interface
- Predefined filter: Credit card number, Social Security ID

DLP file filter:
- Protocols Supported: HTTP-POST, HTTP=-GET,SMTP, POP3, IMAP, MAPI, FTP, NNTP
- Filter options: size, file type, watermark, content, if encrypted

DLP watermarking: Allows filter files that pass through the FortiGate unit and contain a corporate identifier (a text string) and a sensitivity level (Critical, Private, and Warning) hidden in a watermark. Support Windows and Linux free watermarking tools.

DLP fingerprinting: Generates a checksum fingerprint from intercepted files and compare it to those in the fingerprint database.

DLP archiving: Records full content in email, FTP, IM, NNTP, and web traffic

### EMAIL FILTERING

Mail protocol support: IMAP(S), POP3(S), and SMTP(S)

Anti-Spam DB query: IP address check, URL check, and email checksum

Local Spam Filtering: HELO DNS Lookup, return email DNS check, and Black/White List

## Networking

### ROUTING / NAT

Static and policy routing

Dynamic routing protocols: RIPv1 and v2, OSPF v2 and v3, ISIS, BGP4

Content routing: WCCP and ICAP

NAT configuration: Per policy based and central NAT Table

NAT support: NAT64, NAT46, static NAT, dynamic NAT, PAT, Full Cone NAT, STUN

Multicast traffic: sparse and dense mode, PIM support

### L2 / SWITCHING

Layer-2 interface modes: Port aggregated, loopback, VLANs (802.1Q and Trunking), virtual hardware, software, and VLAN switches

VXLAN support:
- interVTEP (VXLAN Tunnel End Point)
- Support for multiple remote IPs, these remote IPs can be IPv4 unicast, IPv6 unicast, IPv4 multicast, or IPv6 multicast.

Virtual Wire Pair:
- Process traffic only between 2 assigned interfaces on the same network segment
- available on both transparent and NAT/route Mode
- Option to implement wildcard VLANs setup

### OFFLINE INSPECTION

Sniffer Mode: An interface can be dedicated to its exclusive use where all traffic entering the interface is processed by the sniffer.

Offline Security inspection: AV, Web Filtering, Application Control, IPS, and Anti-spam

### SD WAN

WAN Load balancing (weighted) algorithms: By volume, sessions, source-destination IP and Source IP

Usage-based WAN link assignment: Routes new sessions to interfaces that have not reached a configured bandwidth limit

WAN link checks:
- Ping or HTTP probes
- Monitoring Criterias including latency, jitter, and packet loss
- Configurable warning, alert, and failure thresholds

Route Overrides Rules which direct specific traffic based on source/user/usergroups and cloud applications/ policy address objects.

Traffic shaping and QoS per policy or applications: Shared policy shaping, per-IP shaping, maximum and guaranteed bandwidth, maximum concurrent connections per IP, traffic prioritization, Type of Service (TOS), and Differentiated Services (DiffServ) support

Traffic Shaping Policies: Assigns traffic shape profile according to matching policy based on source, destination, service, application, application category, and/or URL category.

Inline and out-of-path WAN optimization topology, peer to peer and remote client support

Transparent Mode option: Keeps the original source address of the packets, so servers appear to receive traffic directly from clients.

WAN optimization techniques: Protocol optimization and byte caching

WAN Optimization protocols supported: CIFS, FTP, HTTP(S), MAPI, TCP

Secure Tunneling option: Use AES-128bit-CBC SSL to encrypt the traffic in the WAN optimization tunnel

Tunnel sharing option: Multiple WAN optimization sessions share the same tunnel

Web caching: Object caching that accelerates web applications and web servers by reducing bandwidth usage, server load, and perceived latency. Supports caching of HTTP 1.0 and HTTP 1.1 web sites

SSL Offloading with Web caching:
- Full mode: Performs both decryption and encryption of the HTTPS traffic
- Half mode: Only performs one encryption or decryption action

Option to exempt certain web sites from web caching with URL patterns

Support advanced web caching configurations and options:
- Always revalidate, Max cache object zie, negative response duration, fresh factor, Max/Min/Default TTL, proxy FQDN, Max HTTP request/message length, ignore options, cache expired objects, revalidated prama-no-cache

WAN optimization and web cache monitor

### EXPLICIT PROXY

Explicit web & FTP proxy: FTP, HTTP, and HTTPS proxying on one or more interfaces

Proxy auto-config (PAC): Provide automatic proxy configurations for explicit web proxy users

Proxy chaining: Web proxy forwarding to redirect web proxy sessions to other proxy servers

Web proxy forwarding server monitoring and health checking

IP reflect capability

Load balancing for forward proxy and proxy chaining

Explicit web proxy authentication: IP-Based authentication and per session authentication

Transparent web proxy

### IPV6

IPv6 Support: Management over IPv6, IPv6 routing protocols, IPv6 tunnelling, firewall and UTM for IPv6 traffic, NAT46, NAT64, IPv6 IPsec VPN

### HIGH AVAILABILITY

High availability modes: Active-passive, active-active, virtual clusters, VRRP, FG-5000 series clustering

Redundant heartbeat interfaces

HA reserved management interface

Failover:
- Port, local and remote link monitoring
- Stateful failover
- Subsecond failover
- Failure detection notification

Deployment Options:
- HA with link aggregation
- Full mesh HA
- Geographically dispersed HA

Standalone session synchronization

### ESSENTIAL NETWORK SERVICES

Built-in DHCP, NTP, DNS Server, and DNS proxy

FortiGuard NTP, DDNS, and DNS service

## Platform Support

### PHYSICAL APPLIANCE (+SPU)

Integrates with SPU components for traffic processing acceleration.

### VIRTUAL SYSTEMS

Virtual Systems (FortiOS Virtual Domains) divide a single FortiGate unit into two or more virtual instances of FortiOS that function separately and can be managed independently.

Configurable virtual systems resource limiting and management such as maximum/guaranteed 'active sessions' and log disk quota

VDOM operating modes: NAT/Route or Transparent

VDOM security inspection modes: Proxy or Flow-based

# SPECIFICATIONS

| HYPERVISOR |
| --- |
| Support for popular hypervisor platform, including VMware vSphere, Citrix and open source Xen, KVM, and MS hyper-V |

| CLOUD |
| --- |
| Support for public cloud services: Amazon AWS and Microsoft Azure |

## Others

| OTHERS |
| --- |
| Web Application Firewall:<br>- Signature based, URL constraints and HTTP method policy |
| Server load balancing: traffic can be distributed across multiple backend servers:<br>- Based on multiple methods including static (failover), round robin, weighted or based on round trip time, number of connections.<br>- Supports HTTP, HTTPS, IMAPS, POP3S, SMTPS, SSL or generic TCP/UDP or IP protocols.<br>- Session persistence is supported based on the SSL session ID or based on an injected HTTP cookie. |

NOTE: Feature set based on FortiOS V5.4.GA, some features may not apply to all models. For availability, please refer to Software feature Matrix on docs.fortinet.com

# REFERENCES

| RESOURCE | URL |
| --- | --- |
| The FortiOS Handbook — The Complete Guide | http://docs.fortinet.com/fgt.html |
| Fortinet Knowledge Base | http://kb.fortinet.com/ |
| Product Data Sheets & Matrix | http://www.fortinet.com/resource_center/datasheets.html |

GLOBAL HEADQUARTERS
Fortinet Inc.
899 KIFER ROAD
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

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

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990

## Log messages

Log messages are recorded by the FortiGate unit, giving you detailed information about the network activity. Each log message has a unique number that helps identify it, as well as containing fields; these fields, often called log fields, organize the information so that it can be easily extracted for reports.

These log fields are organized in such a way that they form two groups: the first group, made up of the log fields that come first, is called the log header. The log header contains general information, such as the unique log identification and date and time that indicates when the activity was recorded. The log body is the second group, and contains all the other information about the activity. There are no two log message bodies that are alike, however, there may be fields common to most log bodies, such as the `srcintf` or `identidix` log fields.

The log header also contains information about the log priority level which is indicated in the `level` field. The priority level indicates the immediacy and the possible repercussions of the logged action. For example, if the field contains 'alert', you need to take immediate action with regards to what occurred. There are six log priority levels.

The log severity level is the level at and above which the FortiGate unit records logs. The log severity level is defined by you when configuring the logging location. The FortiGate unit will log all messages at and above the priority level you select. For example, if you select Error, the unit will log only Error, Critical, Alert, and Emergency level messages.

### Log priority levels

| Levels | Description |
|---|---|
| **0 - Emergency** | The system has become unstable. |
| **1 - Alert** | Immediate action is required. |
| **2 - Critical** | Functionality is affected. |
| **3 - Error** | An error condition exists and functionality could be affected. |
| **4 - Warning** | Functionality could be affected. |
| **5 - Notification** | Information about normal events. |
| **6 - Information** | General information about system operations. |

The Debug priority level, not shown above, is rarely used. It is the lowest log priority level and usually contains some firmware status information that is useful when the FortiGate unit is not functioning properly.

### Example log header fields

| Log header | |
|---|---|
| **date=(2010-08-03)** | The year, month and day of when the event occurred in yyyy-mm-dd format. |

| Log header | |
|---|---|
| **time=(12:55:06)** | The hour, minute and second of when the event occurred in the format hh:mm:ss. |
| **log_id=(2457752353)** | A five or ten-digit unique identification number. The number represents that log message and is unique to that log message. This ten-digit number helps to identify the log message. |
| **type=(dlp)** | The section of system where the event occurred. |
| **subtype=(dlp)** | The subtype category of the log message. |
| **level=(notice)** | The priority level of the event. See the table above. |
| **vd=(root)** | The name of the virtual domain where the action/event occurred in. If no virtual domains exist, this field always contains root. |

**Example log body fields**

| Log body | |
|---|---|
| **policyid=(1)** | The ID number of the firewall policy that applies to the session or packet. Any policy that is automatically added by the FortiGate will have an index number of zero. |
| **identidx=(0)** | The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy. |
| **sessionid=(311)** | The serial number of the firewall session of which the event happened. |
| **srcip=(10.10.10.1)** | The source IP address. |
| **srcport=(1190)** | The source port number. |
| **srcintf=(internal)** | The source interface name. |
| **dstip=(192.168.1.122)** | The destination IP address. |
| **dstport=(80)** | The destination port number. |
| **dstintf=(wan1)** | The destination interface name. |
| **service=(https)** | The IP network service that applies to the session or packet. The services displayed correspond to the services configured in the firewall policy. |
| **status=(detected)** | The action the FortiGate unit took. |

| Log body | |
|---|---|
| **hostname=(example.com)** | The home page of the web site. |
| **url=(/image/trees_pine_ forest/)** | The URL address of the web page that the user was viewing. |
| **msg=(data leak detected (Data Leak Prevention Rule matched)** | Explains the FortiGate activity that was recorded. In this example, the data leak that was detected matched the rule, All-HTTP, in the DLP sensor. |
| **rulename=(All-HTTP)** | The name of the DLP rule within the DLP sensor. |
| **action=(log-only)** | The action that was specified within the rule. In some rules within sensors, you can specify content archiving. If no action type is specified, this field display log-only. |
| **severity=(1)** | The level of severity for that specific rule. |

Logs from other devices, such as the FortiAnalyzer unit and Syslog server, contain a slightly different log header. For example, when viewing FortiGate log messages on the FortiAnalyzer unit, the log header contains the following log fields when viewed in the Raw format:

```
itime=1302788921 date=20110401 time=09:04:23 devname=FG50BH3G09601792 device_
    id=FG50BH3G09601792 log_id=0100022901 type=event subtype=system level=notice vd=root
```

The log body contains the rest of the information of the log message, and this information is unique to the log message itself.

For detailed information on all log messages, see the *FortiGate Log Message Reference*.

## Explanation of a debug log message

Debug log messages are only generated if the log severity level is set to Debug. The Debug severity level is the lowest log severity level and is rarely used. This severity level usually contains some firmware status information that is useful when the FortiGate unit is not functioning properly. Debug log messages are generated by all types of FortiGate features.

The following is an example of a debug log message:

```
date=2010-01-25 time=17:25:54 logid=9300000000 type=webfilter subtype=urlfilter
    level=debug msg="found in cache"
```

### Example of a Debug log message

| Debug log | |
|---|---|
| **date=(2010-01-25)** | The year, month and day of when the event occurred in the format yyyy-mm-dd. |
| **time=(17:25:54)** | The hour, minute and second of when the event occurred in the format hh:mm:ss. |

| Debug log | |
|---|---|
| **logid=(93000000000)** | A ten-digit unique identification number. The number represents that log message and is unique to that log message. This ten-digit number helps to identify the log message. |
| **type=(webfilter)** | The section of system where the event occurred. There are eleven log types in FortiOS 4.0. |
| **subtype=(urlfilter)** | The subtype of the log message. This represents a policy applied to the FortiGate feature in the firewall policy. |
| **level=(debug)** | The priority level of the event. There are six priority levels to specify. |
| **msg=("found in cache")** | Explains the activity or event that the FortiGate unit recorded. |

### Viewing log messages and archives

Depending on the log device, you may be able to view logs within the web-based manager or CLI on the FortiGate unit. If you have configured a FortiAnalyzer unit, local hard disk, or system memory, you can view log messages from within the web-based manager or CLI. If you have configured either a Syslog or WebTrends server, you will not be able to view log messages from the web-based manager or CLI. There is also no support for viewing log messages stored on a FortiCloud server, from the FortiGate unit's web-based manager or CLI.

You do not have to view log messages from only the web-based manager. You can view log messages from the CLI as well, using the `execute log display` command. This command allows you to see specific log messages that you already configured within the `execute log filter` command. The `execute log filter` command configures what log messages you will see, how many log messages you can view at one time (a maximum of 1000 lines of log messages), and the type of log messages you can view. For more information about viewing log messages in the CLI, see "Viewing logs from the CLI".

There are two log viewing options in FortiOS: Format and Raw. The Raw format displays logs as they appear within the log file. You can view log messages in the Raw format using the CLI or a text editor, such as Notepad. Format is in a more human-readable format, and you can easily filter information when viewing log messages this way. The Format view is what you see when viewing logs in the web-based manager.

When you download the log messages from within the log message page (for example, **Log & Report > Forward Traffic**), you are downloading log messages in the Raw format.

### Viewing log messages in detail

From any log page, you can view detailed information about the log message in the log viewer table, located (by default) at the bottom of the page. Each page contains this log viewer table. The Log Viewer Table can contain the Archive tab, which allows you to see the archived version of the log message. The Archive tab only displays the archived log's details if archiving is enabled and logs are being archived by the FortiGate unit, but archived logs will also be recorded when using a FortiAnalyzer unit or the FortiCloud service.

When you are viewing traffic log messages, some of the categories (such as 'Application Name') have entries that can be selected to open a dialog box containing FortiGuard information about the entry. From within the dialog box, you can select the Reference link and go directly to the corresponding FortiGuard page, which contains additional information.

**To configure a remote user - web-based manager:**

1. Go to **User & Device > User Definition** and select **Create New**.
2. Follow the User Creation Wizard, entering the following information and then select **Create**:

| | |
|---|---|
| **User Type** | Remote RADIUS User |
| **User Name** | User2 |
| **RADIUS server** | OurRADIUSsrv |
| **Email Address**<br>**SMS** | (optional) |
| **Enable** | Select |

**To configure a remote user - CLI:**

```
config user local
   edit User2
      set name User2
      set type radius
      set radius-server OurRADIUSsrv
   end
```

### Creating user groups

There are two user groups: an FSSO user group for FSSO users and a firewall user group for other users. It is not possible to combine these two types of users in the same user group.

### Creating the FSSO user group

For this example, assume that FSSO has already been set up on the Windows network and that it uses Advanced mode, meaning that it uses LDAP to access user group information. You need to

- configure LDAP access to the Windows AD global catalog
- specify the collector agent that sends user logon information to the FortiGate unit
- select Windows user groups to monitor
- select and add the Engineering and Sales groups to an FSSO user group

**To configure LDAP for FSSO - web-based manager:**

1. Go to **User & Device > LDAP Servers** and select **Create New**.
2. Enter the following information:

| | |
|---|---|
| **Name** | ADserver |
| **Server Name / IP** | 10.11.101.160 |
| **Distinguished Name** | dc=office,dc=example,dc=com |
| **Bind Type** | Regular |

## Dashboard

The FortiOS dashboard provides a location to view real-time system information. By default, the dashboard displays the key statistics of the FortiGate unit itself, providing the memory and CPU status, as well as the health of the ports, whether they are up or down and their throughput.

The FortiOS 5.6 **Dashboard** has a new layout with a Network Operations Center (NOC) view with a focus on alerts. Widgets are interactive; by clicking or hovering over most widgets, the user can get additional information or follow links to other pages.

Enhancements to the GUI dashboard and its widgets are:

- Multiple dashboard support.
- VDOM and global dashboards.
- Updated resize control for widgets.
- Notifications moved to the top header bar (moved existing dashboard notifications to the header and added additional ones).
- Reorganization of **Add Widget** dialog.
- New **Host Scan Summary** widget.
- New **Vulnerabilities Summary** widget that displays endpoint vulnerability information much like the FortiClient Enterprise Management Server (EMS) summary.
- Multiple bug fixes.


Features that were only visible through old dashboard widgets have been placed elsewhere in the GUI:

- Restore configuration.
- Configuration revisions.
- Firmware management.
- Enabling / disabling VDOMs.

As with most advanced routing features on your FortiGate unit, IPv6 settings for dynamic routing protocols must be enabled before they will be visible in the GUI. To enable IPv6 configuration in the GUI, enable it in **System > Feature Visibility**. Alternatively, you can directly configure IPv6 for RIP, BGP, or OSPF protocols using CLI commands.

## Dual stack routing

Dual stack routing implements dual IP layers in hosts and routers, supporting both IPv6 and IPv4. A dual stack architecture supports both IPv4 and IPv6 traffic and routes the appropriate traffic as required to any device on the network. Administrators can update network components and applications to IPv6 on their own schedule, and even maintain some IPv4 support indefinitely if that is necessary. Devices that are on this type of network, and connect to the Internet, can query Internet DNS servers for both IPv4 and IPv6 addresses. If the Internet site supports IPv6, the device can easily connect using the IPv6 address. If the Internet site does not support IPv6, then the device can connect using the IPv4 addresses.

In FortiOS, dual stack architecture it is not comprised merely of basic addressing functions that operate in both versions of IP. The other features of the appliance, such as UTM and routing, can also use both IP stacks.

If an organization with a mixed network uses an Internet service provider that does not support IPv6, they can use an IPv6 tunnel broker to connect to IPv6 addresses that are on the Internet. FortiOS supports IPv6 tunnelling over IPv4 networks to tunnel brokers. The tunnel broker extracts the IPv6 packets from the tunnel and routes them to their destinations.

## IPv6 tunnelling

IPv6 Tunnelling is the act of tunnelling IPv6 packets from an IPv6 network through an IPv4 network to another IPv6 network. Unlike NAT, once the packet reaches its final destination, the true originating address of the sender will still be readable. The IPv6 packets are encapsulated within packets with IPv4 headers, which carry their IPv6 payload through the IPv4 network.

The key to IPv6 tunnelling is the ability of the two devices to be dual stack compatible in order to work with both IPv4 and IPv6 at the same time. In the process, the entry node of the tunnel portion of the path will create an encapsulating IPv4 header and transmit the encapsulated packet. The exit node at the end of the tunnel receives the encapsulated packet, removes the IPv4 header, updates the IPv6 header, and processes the packet.

There are two types of tunnels in IPv6:

**Automatic tunnels:** Automatic tunnels are configured by using IPv4 address information embedded in an IPv6 address – the IPv6 address of the destination host includes information about which IPv4 address the packet should be tunnelled to.

**Configured tunnels:** Configured tunnels must be configured manually. These tunnels are used when using IPv6 addresses that do not have any embedded IPv4 information. The IPv6 and IPv4 addresses of the endpoints of the tunnel must be specified.

### Tunnel configuration

There are a few ways in which the tunnelling can be performed depending on which segment of the path between the endpoints of the session the encapsulation takes place.

**Host to Host:** Dual Stack capable hosts that are interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans the entire path taken by the IPv6 packets.

```
edit <name>
   set dhcp-relay-agent-option [enable | disable]
next
```

For more information about the DHCP relay option, see RFC 3046 (DHCP Relay Agent Information Option).

### Configuring DHCP with IPv6

You can use DHCP with IPv6, using the CLI. To configure DHCP, ensure IPv6 is enabled by going to **System > Feature Visibility** and enable **IPv6** under **Basic Features**. Use the following CLI command:

```
config system dhcp6 server
```

For more information about the configuration options, see the FortiOS CLI Reference Guide.

### DHCPv6 prefix delegation

Prefix delegation is supported for DHCP for IPv6 addressing. It is not practical to manually provision networks on a large scale in IPv6 networking. The DHCPv6 prefix delegation feature is used to assign a network address prefix, and automate the configuration and provisioning of the public routable addresses for the network.

You can enable the prefix delegation, using the following CLI commands:

```
config system interface
   edit "wan1"
      config ipv6
         set ip6-mode dhcp
         set ip6-allowaccess ping
         set dhcp6-prefix-delegation enable
         end
      end
```

### DHCPv6 prefix hint

This feature is used to "hint" to upstream DCHPv6 servers a desired prefix length for their subnet to be assigned in response to its request.

There is a possibility of duplicate prefixes being sent by ISP when using a /64 bit subnet because the first 64 bits of the address are derived from the MAC address of the interface. This could cause an issue if the system administrator wishes to divide the host networks into 2 /64 bit subnets.

By receiving a /60 bit (for example) network address, the administrator can then divide the internal host works without the danger of creating duplicate subnets.

Also included in the new feature, are preferred times for the life and valid life of the DHCP lease.

DHCPv6 hint for the prefix length:

`set dhcp6-prefix-hint` <DHCPv6 prefix that will be used as a hint to the upstream DHCPv6 server>

DHCPv6 hint for the preferred life time:

`set dhcp6-prefix-hint-plt` <integer> 1 ~ 4294967295 seconds or "0" for unlimited lease time

DHCPv6 hint for the valid life time:

`set dhcp6-prefix-hint-vlt` <integer> 1 ~ 4294967295 seconds or "0" for unlimited lease time

1. Configure the RADIUS server to return the following attributes for each user:
   Tunnel-Type (value: VLAN)
   Tunnel-Medium-Type (value: IEEE-802)
   Tunnel_Private-Group-Id (value: the VLAN ID for the user's VLAN)
2. Configure the FortiGate to access the RADIUS server.
3. Configure the SSID with WPA2-Enterprise authentication. In the **Authentication** field, select **RADIUS Server** and choose the RADIUS server that you will use.
4. Create VLAN subinterfaces on the SSID interface, one for each VLAN. Set the VLAN ID of each as appropriate. You can do this on the **Network > Interfaces** page.
5. Enable Dynamic VLAN assignment for the SSID. For example, if the SSID interface is "office", enter:
   ```
   config wireless-controller vap
      edit office
         set dynamic-vlan enable
      end
   ```
6. Create security policies for each VLAN. These policies have a WiFI VLAN subinterface as **Incoming Interface** and allow traffic to flow to whichever **Outgoing Interface** these VLAN users will be allowed to access.

### MAC-based authentication

Wireless clients can also be supplementally authenticated by MAC address. A RADIUS server stores the allowed MAC address for each client and the wireless controller checks the MAC address independently of other authentication methods.

MAC-based authentication must be configured in the CLI. In the following example, MAC-based authentication is added to an existing access point “vap1” to use RADIUS server hq_radius (configured on the FortiGate):

```
config wireless-controller vap
   edit vap1
      set radius-mac-auth enable
      set radius-mac-auth-server hq_radius
   end
```

### Authenticating guest WiFi users

The FortiOS Guest Management feature enables you to easily add guest accounts to your FortiGate unit. These accounts are authenticate guest WiFi users for temporary access to a WiFi network managed by a FortiGate unit. To implement guest access, you need to

1. Go to **User & Device > User Groups** and create one or more guest user groups.
2. Go to **User & Device > Guest Management** to create guest accounts. You can print the guest account credentials or send them to the user as an email or SMS message.
3. Go to **WiFi & Switch Controller > SSID** and configure your WiFi SSID to use captive portal authentication. Select the guest user group(s) that you created.

Guest users can log into the WiFi captive portal with their guest account credentials until the account expires. For more detailed information about creating guest accounts, see “Managing Guest Access” in the Authentication chapter of the FortiOS Handbook.

## Configuring firewall policies for the SSID

For users on the WiFi LAN to communicate with other networks, firewall policies are required. This section describes creating a WiFi network to Internet policy.

Before you create firewall policies, you need to define any firewall addresses you will need.

```
config system dhcp server
   edit <server_entry_number>
      config exclude-range
         edit <sequence_number>
            set start-ip <address>
            set end-ip <address>
         end
      end
   end
```

### Viewing information about DHCP server connections

To view information about DHCP server connections, go to **Monitor > DHCP Monitor**. On this page, you can also add IP addresses to the reserved IP address list.

### Breaking an address lease

If you need to end an IP address lease, you can break the lease. This is useful if you have limited addresses and longer lease times, when some leases are no longer necessary, for example, with corporate visitors.

To break a lease, use the following CLI command:

```
execute dhcp lease-clear <ip_address>
```

## Interface MTU packet size

You can change the maximum transmission unit (MTU) of the packets that FortiGate transmits to improve network performance. Ideally, the MTU should be the same as the smallest MTU of all the networks between FortiGate and the destination of the packets. If the packets that the FortiGate unit sends are larger than the smallest MTU, they are broken up or fragmented, which slows down transmission. You can easily experiment by lowering the MTU to find an MTU size for optimum network performance.

- 68 to 1500 bytes for static mode
- 576 to 1500 bytes for DHCP mode
- 576 to 1492 bytes for PPPoE mode
- Larger frame sizes (if supported by the FortiGate model), up to 9216 bytes for NP2, NP4, and NP6-accelerated interfaces

This option is available only for physical interfaces. Virtual interfaces associated with a physical interface inherit the physical interface MTU size.

Interfaces on some FortiGate models support frames larger than the traditional 1500 bytes. Jumbo frames are supported on FortiGate models that have either a SOC2 or NP4lite (except for the FortiGate 30D), and on FortiGate 100D series models. For information about your FortiGate model's hardware, see the FortiOS Hardware Acceleration Guide. For other models, contact Fortinet Customer Support for the maximum frame size that is supported.

If you need to send larger frames over a route, all Ethernet devices on that route must support the larger frame size. Otherwise, the larger frames will not be recognized and will be dropped.

If you have standard size and larger size frame traffic on the same interface, routing alone cannot route them to different routes based only on frame size. However, you can use VLANs to make sure the larger frame traffic is routed over network devices that support the larger size. VLANs inherit the MTU size from the parent interface. You must configure the VLAN to include both ends of the route, as well as all switches and routers along the route.

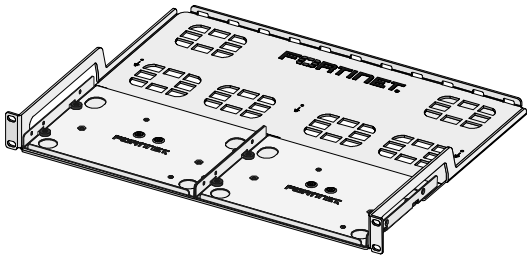
# Fortinet Rack Mount Tray

## Supported Devices

The Fortinet Rack Mount Tray (SP-RACKTRAY-02) supports the following devices:

| | |
|---|---|
| FortiGate 30D | Tray Mount (Plastic Casing) |
| FortiGate 30D-POE | Tray Mount (Plastic Casing) |
| FortiGate 30E | Adapter Bracket |
| FortiGate 50E | Adapter Bracket |
| FortiGate 51E | Adapter Bracket |
| FortiGate 60D | Adapter Bracket |
| FortiGate 60D-POE | Adapter Bracket |
| FortiGate 60E | Adapter Bracket |
| FortiGate 60E-POE | Adapter Bracket |
| FortiGate 61E | Adapter Bracket |
| FortiGate 70D | Tray Mount |
| FortiGate 70D-POE | Tray Mount |
| FortiGate 80D | Tray Mount |
| FortiGate 80E | Tray Mount |
| FortiGate 80E-POE | Tray Mount |
| FortiGate 81E | Tray Mount |
| FortiGate 81E-POE | Tray Mount |
| FortiGate 90D | Tray Mount |
| FortiGate 90D-POE | Tray Mount |
| FortiGate 90E | Tray Mount |
| FortiGate 90E-POE | Tray Mount |
| FortiGate 91E | Tray Mount |
| FortiGate 92D | Tray Mount |

Mounting instructions are available in the Fortinet Rack Mount Tray QuickStart Guide, available in the Fortinet Document Library (forti.net/tray).




Fortinet.com