PŘÍLOHA Č. 1: NABÍDKA

PODROBNÁ SPECIFIKACE PŘEDMĚTU ZAKÁZKY
ČÁST I. SOFTWARE

KOMPONETA FIREWALL S IDS

4. NÁSTROJ PRO DETEKCI KYBERNETICKÝCH HROZEB (SW PRO FIREWALL S IDS)

V rámci zabezpečení ochrany sítě IS požaduje zadavatel pořízení nového SW firewallu s funkcionalitou detekce průniku IDS (Introduction Detection System). Toto řešení zvýší bezpečnost síťových prostředků nemocnice proti průniku z vnějšího prostředí sítě (WAN), prostřednictvím detekce a vyhodnocování pokusů o průnik s cílem zcizit, zneužít nebo poškodit data z informačních systémů nebo poškodit nebo zneužít prvky infrastruktury. Nastavení současných firewallů se opírá minimálně o informace o stavu samotného spojení, znalost kontrolovaných přenosů dat a monitoringu protokolů a prvky IDS.

Popis požadované funkcionality:

- systém IDS
- detekce neobvyklé aktivity
- vygenerování varování (alert)
- zápis do logu
- dle naimplementované logiky rozlišení externího nebo interního útoku

A. POUŽITÁ TERMINOLOGIE

pojem	význam
IDS/IPS	Systém prevence průniku
Blokování C&C komunikace	Nástroj pro blokování komunikace s ***command-and-control*** *servery* – řídicími počítače tzv. Botnet
Botnet	skupina počítačů pod kontrolou takzvaných **C&C serverů** (viz výše), které provádějí na pozadí nelegální úkoly bez vědomí uživatelů
VPN	Virtuální privátní síť – typ bezpečné komunikace
GUI	Grafické uživatelské rozhraní
DoS	**Denial of service (DoS)** (česky **odepření služby**) je typ útoku na internetové služby nebo stránky, jehož cílem je službu znefunkčnit a znepřístupnit ostatním uživatelům
TLS	**Transport Layer Security** (**TLS**) je kryptografický protokol poskytující možnost zabezpečené komunikace na intetu pro služby jako WWW, elektronická pošta atd.

B. ZÁKLADNÍ INFORMACE – NÁSTROJ PRO IDENTIFIKACI KYBERNETICKÝCH HROZEB - FIREWALL

Moderní systém firewall s funkcionalitou detekce průniku IDS – současný SW firewallu již není aktuální. Nový SW **zvýší bezpečnost síťových prostředků nemocnice proti průniku z vnějšího prostředí sítě**.

C. TABULKY MINIMÁLNÍCH POŽADAVKŮ

Níže jsou uvedeny minimální požadavky na nabízené řešení v jednotlivých strukturovaně členěných tabulkách. Uchazeč použije ve své nabídce tyto tabulky, ve kterých slovně uvede, zda požadavek je či není splněn (ANO / NE).

Požadavky na funkcionalitu

	Požadavek	ANO / NE
a. Paketový filtr a základní funkce	Stavové filtrování paketů	Ano
	Překlady komunikace (příchozí i odchozí)	Ano
	Možnost použití více internetů v režimu active-backup nebo balancing (dynamické routování)	Ano
	Montáž do standardních 19“ skříní (rack)	Ano
	100% administrace pouze přes webové rozhraní (bez nutnosti použít textové rozhraní typu TELNET/SSH konzole)	Ano
	Propojení a využívání Active Directory	Ano
	Podpora bezagentového přihlášení uživatelů (8. vrstva)	Ano
	DHCP server a DNS forwarded pro konkrétní sítě	Ano
	Možnost automatické zálohy UTM a v případě potřeby kompletní obnovy konfigurace nahráním ze zálohy	Ano
	Logování a rozšířený reporting (včetně statistik uživatelských aktivit)	Ano
	Vlastní API rozhraní pro propojení s dalšími interními nástroji	Ano
	Podpora routování BGP a OSPF	Ano

Požadavky na funkcionalitu – pokračování

	Požadavek	ANO / NE
b. Proaktivní ochrana perimetru	IDS/IPS	Ano
	Blokování C&C komunikace	Ano
	Možnost specifikace výjimek	Ano
	Identifikování kompromitovaného systému na základě C&C komunikace	Ano
	Aplikační kontrola (blokování konkrétních aplikací z pravidelně aktualizovaného seznamu výrobce)	Ano
	Logování	Ano

Požadavky na funkcionalitu – pokračování

	Požadavek	ANO / NE
c. VPN – vzdálené přístupy	IPSEC – Propojení vzdálených lokalit	Ano
	SSL VPN – Připojení vzdálených PC	Ano
	SSL VPN – Odlišný certifikát / uživatel	Ano
	SSL VPN – Uživatelský portál pro stažení VPN klienta	Ano
	SSL VPN – Dostupná instalace včetně konfigurace (bez nutnosti další konfigurace na koncových počítačích)	Ano
	Zobrazení aktuálně připojených uživatelů v GUI	Ano
	Licenčně neomezený počet VPN tunelů, připojených uživatelů a přenosu dat	Ano
	Neomezený počet SSL VPN klientů v ceně	Ano
	Logování	Ano

Požadavky na funkcionalitu – pokračování

	Požadavek	ANO / NE
d. Reverzní proxy pro ochranu interních web. serverů a aplikací	Ochrana skenováním antimalware motorem	Ano
	Filtrování http a https komunikace	Ano
	Ochrana proti Trojským koním	Ano
	Ochrana proti podvržení cookies (podepisování)	Ano
	Možnost monitorovat nebo blokovat (odmítnout) komunikaci	Ano
	Podpora reverzních formulářů přihlášení navázaných na Active Directory	Ano
	Blokování komunikace na základě reputační služby výrobce	Ano
	Možnost specifikace výjimek	Ano
	Logování	Ano

Požadavky na funkcionalitu – pokračování

	Požadavek	ANO / NE
e. Ochrana emailové komunikace (SMTP)	Ochrana skenováním antimalware motorem	Ano
	Ochrana proti spamům / phishing emailům	Ano
	Skenování příloh emailů včetně archivů	Ano
	Skenování odchozího i příchozího provozu	Ano
	Blokování komunikace na základě reputační služby výrobce	Ano
	Ochrana proti DoS útokům	Ano
	Nastavitelná a vynutitelná TLS komunikace pro konkrétní SMTP servery	Ano

	Šifrování odchozích e-mailů (nastavitelné a volitelné)	Ano
	Kontrola e-mailové fronty na UTM	Ano
	Karanténa uložená na UTM	Ano
	Logování a prohledávání logů minimálně na úrovni: Odesílatel, Příjemce, Předmět, Datum	Ano
	Stejné logování a prohledání i pro uživatele pomocí GUI „uživatelského portálu“ (jen pro e-maily konkrétního uživatele)	Ano
	Sandboxing	Ano
	Možnost specifikace výjimek	Ano
	Logování	Ano

Požadavky na funkcionalitu – pokračování

Požadavek		ANO / NE
f. Ochrana přístupů na internet	Ochrana skenováním antimalware motorem	Ano
	URL filtrování (minimálně 80+ kategorií)	Ano
	Filtrování http, HTTPS a FTP	Ano
	Možnost specifikovat povolené porty	Ano
	Možnost specifikace porty proxy	Ano
	Propojení s Active Directory	Ano
	Možnost definovat výjimky	Ano
	Pravidla platí pouze ve specifikovaný čas během dne	Ano
	Pravidla lze specifikovat na skupinu/uživatele z Active Directory	Ano
	Sandboxing	Ano
	Logování	Ano

Požadavky na funkcionalitu – pokračování

Požadavek			ANO / NE
g. Možnost rozšíření o správu WIFI	Řešení musí být rozšiřitelné o správu WIFI zařízení (vše od jednoho výrobce) a nesmí k tomu vyžadovat žádnou další licenci		Ano
	Výkon:	Firewall: 17 Gbps	Ano
		IPS propustnost: 4,5 Gbps	Ano
		VPN (AES) propustnost: 2,5 Gbps	Ano
		Propustnost Web proxy s aktivním AV: 1 Gbps	Ano
		Souběžná spojení: 5 milionů	Ano
		Nová spojení za sekundu: 80 tisíc	Ano

D. DETAILNÍ POPIS PLNĚNÍ

S ohledem na požadavek zadavatele na „Montáž do standardních 19“ skříní (rack)“ nabízíme řešení postavené na HW appliances od výrobce Fortinet (model FortiGate 600E) a softwarovém vybavení odpovídajícím Fortinet Unified Threat Protection (UTP) s aktualizacemi na 5 let. Uvedené řešení výkonově mnohonásobně převyšuje požadavky na propustnost síťového provozu a to i při maximální možné inspekci provozu. Sandboxing bude zajištěn využitím cloudové služby, která je kryta uvedenou softwarovou licencí UTP. S ohledem na bezvýpadkové řešení po celou předpokládanou dobu provozu (udržitelnosti provozu) nabízíme řešení ve forma HA clusteru dvou FG600E v režimu Active-Passive, čímž bude zajištěna i bezvýpadková implementace všech aktualizací systému.

Výhodou nabízeného řešení je možná integrace s bezpečnostními komponentami, které již ve své síti má zadavatel implementovány – firewally FG300E od roku 2019 slouží v WLAN guest síti a Forti Analyzer sloužící ke zpracování logů z firewallů.

Nabízené řešení je rovněž plně integrovatelné s nabízeným řešením pro LOG management a DDI/NAC. Do budoucna nabízené firewally disponují dostatečnou propustností a konektivitou na 10GE portech. Stejně tak nabízené modely FG600E obsahují výkonný wifi kontroler pro možnost v budoucnu využít bezdrátových wifi přístupových bodů od výrobce Fortinet.

KÓD PRODUKTU	POPIS PRODUKTU	POČET
2x FortiGate 600E + 5 Years 24x7 FortiCare & Unified Threat Protection (UTP)		
FG-600E	2 x 10GE SFP+ slots, 10 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 8 x switch ports), 8 x GE SFP slots, SPU NP6 and CP9 hardware accelerated	2
FC-10-F6H0E-950-02-60	5 Years Unified Threat Protection (UTP) (24x7 FortiCare plus Application Control, IPS, AV, Web Filtering and Antispam, FortiSandbox Cloud)	2

Součástí řešení je školení v rozsahu

- Základní seznámení s GUI FortiGate
- Vytváření bezpečnostních profilů a jejich použití
- Vytváření bezpečnostních pravidel a jejich správa
- Update Firmwaru
- Propojení Fortigate a LDAP
- FortiGate Explicit Proxy
- Práce s VDOMy

- Materiály pro školení:
  Fortinet Fortigate document Library https://docs.fortinet.com/product/fortigate/6.0

E. DATASHEET

DATA SHEET

FortiGate® 600E Series

FortiGate 600E and 601E

Next Generation Firewall
Secure SD-WAN
Secure Web Gateway
IPS

The FortiGate 600E series delivers next generation firewall (NGFW) capabilities for mid-sized to large enterprises deployed at the campus or enterprise branch level. Protects against cyber threats with high-powered security processors for optimized network performance, security efficacy, and deep visibility. Fortinet's Security-Driven Networking approach provides tight integration of the network to the new generation of security.

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

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

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

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

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

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

Firewall	IPS	NGFW	Threat Protection	Interfaces
36 Gbps	10 Gbps	9.5 Gbps	7 Gbps	Multiple GE RJ45, GE SFP and 10 GE SFP+ Slots

Refer to the specifications table for details

Deployment

Next Generation Firewall (NGFW)

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

Secure SD-WAN

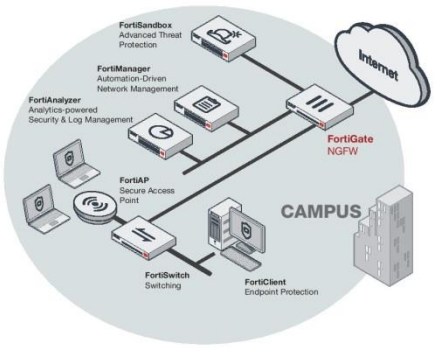
- Consistent business application performance with accurate detection, dynamic WAN path steering and optimization
- Multi-cloud access for faster SaaS adoption with end-to-end optimization
- Simplification with zero touch deployment and centralized management with auto-provisioning, analytics and reporting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

Secure Web Gateway (SWG)

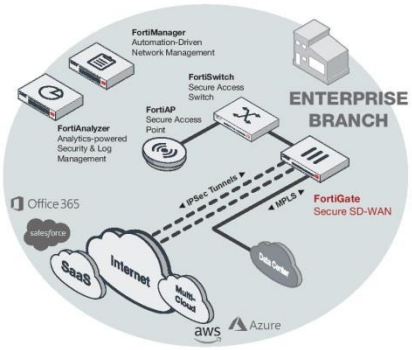
- Secure web access from both internal and external risks, even for encrypted traffic at high performance
- Enhanced user experience with dynamic web and video caching
- Block and control web access based on user or user groups across URL's and domains
- Prevent data loss and discover user activity to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

IPS

- Purpose-built security processors delivering industry validated IPS performance with high throughput and low latency
- Deploy virtual patches at the network level to protect against network exploitable vulnerabilities and optimize network protection time
- Deep packet inspection at wire speeds offers unparalleled threat visibility into network traffic including traffic encrypted with the latest TLS 1.3
- Proactively block newly discovered sophisticated attacks in real-time with advanced threat protection provided by the intelligence services of the Fortinet Security Fabric



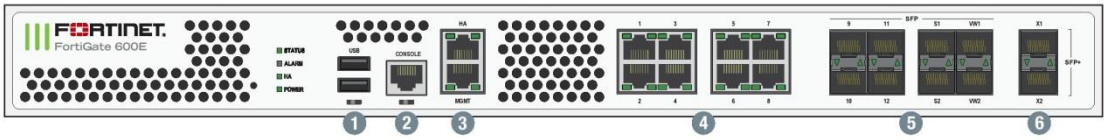
FortiGate 600E deployment in Campus (NGFW)

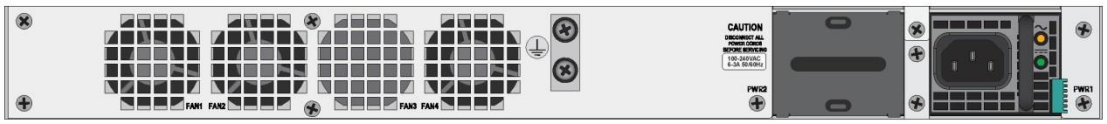


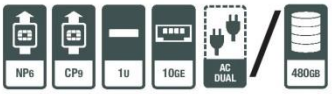
FortiGate 600E deployment in Enterprise Branch (Secure SD-WAN)

Hardware

FortiGate 600E/601E







Interfaces

1. USB Port
2. Console Port
3. 2x GE RJ45 MGMT/HA Ports
4. 8x GE RJ45 Ports
5. 8x GE SFP Slots
6. 2x 10 GE SFP+ Slots

Powered by SPU

- Custom SPU processors deliver the power you need to detect malicious content at multi-Gigabit speeds
- Other security technologies cannot protect against today's wide range of content- and connection-based threats because they rely on general-purpose CPUs, causing a dangerous performance gap
- SPU processors provide the performance needed to block emerging threats, meet rigorous third-party certifications, and ensure that your network security solution does not become a network bottleneck

Network Processor

Fortinet's new, breakthrough SPU NP6 network processor works inline with FortiOS functions delivering:

- Superior firewall performance for IPv4/IPv6, SCTP, and multicast traffic with ultra-low latency down to 2 microseconds
- VPN, CAPWAP, and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing

Content Processor

Fortinet's new, breakthrough SPU CP9 content processor works outside of the direct flow of traffic and accelerates the inspection of computationally intensive security features:

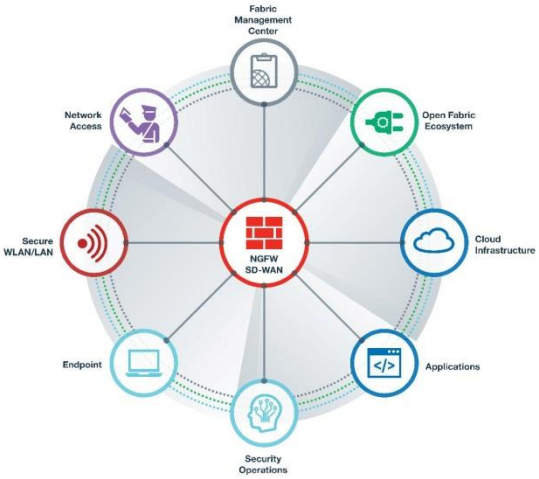
- Enhanced IPS performance with unique capability of full signature matching at ASIC
- SSL Inspection capabilities based on the latest industry mandated cipher suites
- Encryption and decryption offloading

Fortinet Security Fabric

Security Fabric

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

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



FortiOS

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

- A truly consolidated platform with a single OS and pane-of-glass for across the entire digital attack surface.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives, and ICSA validated security and performance.
- Leverage the latest technologies such as deception-based security.
- 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.
- Automatically prevent, detect, and mitigate advanced attacks within minutes with an integrated AI-driven security and advanced threat protection.
- Improve and unify the user experience with innovative SD-WAN capabilities with the ability to detect, contain, and isolate threats with automated segmentation.
- Utilize SPU hardware acceleration to boost network security performance.

Services

FortiGuard™ Security Services

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

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 600E	FORTIGATE 601E
Interfaces and Modules		
10 GE SFP+ Slots	2	
GE RJ45 Interfaces	8	
GE SFP Slots	8	
GE RJ45 Management Ports	2	
USB Ports	2	
RJ45 Console Port	1	
Local Storage	–	2x 240 GB SSD
Included Transceivers	2x SFP (SX 1 GE)	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	10 Gbps	
NGFW Throughput [2, 4]	9.5 Gbps	
Threat Protection Throughput [2, 5]	7 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	36 / 36 / 27 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)	36 / 36 / 27 Gbps	
Firewall Latency (64 byte, UDP)	2 µs	
Firewall Throughput (Packet per Second)	40.5 Mpps	
Concurrent Sessions (TCP)	8 Million	
New Sessions/Second (TCP)	450,000	
Firewall Policies	10,000	
IPsec VPN Throughput (512 byte) [1]	20 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2,000	
Client-to-Gateway IPsec VPN Tunnels	50,000	
SSL-VPN Throughput	7 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	10,000	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	8 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	5,500	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	800,000	
Application Control Throughput (HTTP 64K) [2]	15 Gbps	
CAPWAP Throughput (HTTP 64K)	18 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	96	
Maximum Number of FortiAPs (Total / Tunnel)	1,024 / 512	
Maximum Number of FortiTokens	5,000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FORTIGATE 600E	FORTIGATE 601E
Dimensions and Power		
Height x Width x Length (inches)	1.75 x 17.0 x 15.0	
Height x Width x Length (mm)	44.45 x 432 x 380	
Weight	16.1 lbs (7.3 kg)	16.6 lbs (7.5 kg)
Form Factor (supports EIA / non-EIA standards)	Rack Mount, 1 RU	
Power Consumption (Average / Maximum)	129 W / 244 W	
Power Source	100–240V 50–60Hz	
Current (Maximum)	6A @ 100V	
Heat Dissipation	832 BTU/h	
Redundant Power Supplies (Hot Swappable)	optional	
Operating Environment and Certifications		
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Humidity	10–90% non-condensing	
Noise Level	59 dBA	
Operating Altitude	Up to 9,843 ft (3,000 m)	
Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6	

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 600E	FG-600E	2x 10 GE SFP+ slots, 10x GE RJ45 ports (including 1x MGMT port, 1x HA port, 8x switch ports), 8x GE SFP slots, SPU NP6 and CP9 hardware accelerated.
FortiGate 601E	FG-601E	2x 10 GE SFP+ slots, 10x GE RJ45 ports (including 1x MGMT port, 1x HA port, 8x switch ports), 8x GE SFP slots, SPU NP6 and CP9 hardware accelerated, 2x 240 GB onboard SSD storage.
Optional Accessories		
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Active Direct Attach Cable, 10m / 32.8 ft	SP-CABLE-ADASFP+	10 GE SFP+ active direct attach cable, 10m / 32.8 ft for all systems with SFP+ and SFP/SFP+ slots.
Optional Power Supply	SP-FG300E-PS	AC power supply for FG-300/301E, FG-400/401E, FG-500/501E, FG-600/601E, FAZ-200F/300F/800F and FMG-200F/300F.

Bundles

FortiGuard Bundle

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

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

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

FORTINET

www.fortinet.com

FST-PROD-DS-GT6H2

FG-600E-DAT-R11-202006

F. SEZNAM NÁROKŮ NA SOUČINNOST

Schválení implementačního plánu

Připravené napájení pro dva 1U firewall appliance s napájecími zdroji 230 V 50 Hz
Připravená síťová infrastruktura vč. adresování a připravených portů na páteřních přepínačích
Připravený prostor v datacentrovém rozvaděči, racku, o velikosti minimálně 2U

Zajištění přístupu – fyzického – při instalaci
Zajištění přístupu – vzdáleného – při konfiguraci