Příloha č. 1 Smlouvy

Technické specifikace

Splnění technických požadavků zadavatele doloží účastník formou popisu, nebo informací o souladu nabízeného řešení s požadavky zadavatele, odkazem na technickou specifikaci výrobce, přiložením datasheetu, nebo jiným obdobným způsobem, ze kterého je splnění požadavků zřejmé.

Next Generation Firewall

Obecné požadavky NGFW

- Počet kusů: 2 v HA clusteru
- Kvalita nabízeného řešení:
  - Nabízené řešení, resp. jeho výrobce, musí být v mezinárodně platném benchmarkovém reportu pro rok 2021 či novější, a to na úrovni umístění v „leaders segmentu“, přičemž předmětem benchmarkového reportu musí být síťové firewally a benchmark musí obsahovat posouzení minimálně TOP10 celosvětových výrobců. (např. Gartner Magic Quadrant, Forrester Wave)
- Rozsah licenční podpory:

Typ podpory	Úroveň podpory	Datum platnosti
Záruka zařízení	-	5 let
Firmware upgrade	Online	5 let
Podpora	8x5	5 let
Antimalware / Antivirus	Online	5 let
NGFW	Online	5 let
Web Filtering	Online	5 let
AntiSpam	Online	5 let

Technické požadavky NGFW

Požadovaná funkcionalita/vlastnost
Typ zařízení NG firewall
Platforma postavená na HW akcelerované architektuře (tj. zařízení vybavené specializovanými obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí)
Maximální velikost 1U
Příslušenství pro montáž do 19" rozvaděče součástí dodávky přepínače
Minimální počet neblokovaných portů 10GE s volitelným fyzickým rozhraním typu SFP+ – 2ks
Minimální počet neblokovaných portů 1GE s volitelným fyzickým rozhraním typu SFP – 8ks
Minimální počet neblokovaných portů 1GE metalických RJ45 portů – 12ks
Dedikovaný management port – RJ 45
Dedikovaná konzolový port – typ RJ45 nebo USB/miniUSB
Lokální úložiště pro logy (SSD disk) o minimální kapacitě 400GB
Podpora nasazení v HA Clusteru (porty nutné pro zapojení do HA nesmí ovlivnit počet požadovaných portů výše)
Interní redundantní napájecí zdroj

Interní redundantní ventilátory
Stavové filtrování IPv4, IPv6 UDP paket 64 byte min. 10 Gbps
Stavové filtrování IPv4, IPv6 UDP paket 512 byte min. 25 Gbps
Stavové filtrování IPv4, IPv6 UDP paket 1518 byte min. 25 Gbps
Počet souběžných TCP spojení min. 3 000 000
Počet nových spojení za sekundu min. 250 000
Propustnost FW služby IPS min. 5 Gbps
Propustnost NGFW (IPS, Application control) min. 3 Gbps
Propustnost IPSEC VPN min. 12 Gbps
Propustnost SSL VPN min 2 Gbps
SSL inspekce (IPS, HTTPS) min. 3,5 Gbps
SSL inspekce souběžných spojení min. 300 000
Počet IPSec VPN tunelů Gateway-to-Gateway min. 1800
Počet IPSec VPN tunelů Client-to-Gateway min. 5 000
Počet uživatelů současně připojených pomocí SSL VPN – 500, součástí musí být licence na minimálně 500 uživatelů
Podpora virtuálních kontextů hardware appliance min. 10 kontextů – pokud jsou licencovány, musí být licence součástí nabídky
Součástí dodávky musí být i veškeré potřebné licence pro služby NGFW do všech kontextů
Každý z virtuálních kontextů může pracovat buď v L2 režimu (transparentní režim inspekce) nebo L3 režimu (NAT/router režim s inspekcí)
Virtuální kontexty musí být možné propojit pomocí virtuálních propojů (bez nutnosti propojovat pomocí fyzických síťových rozhraní) bez omezení výkonu
Podpora Active Active i Active Passive HA, full mesh HA, synchronizace stavové tabulky mezi nódy clusteru
Režim vysoké dostupnosti (L2 HA, tj. virtuální MAC adresy)
Správa všech zařízení pracujících v režimu vysoké dostupnosti musí probíhat jednotně přes společné grafické konfigurační rozhraní
Grafické konfigurační rozhraní pro správu celého clusteru, dostupné pomocí webového prohlížeče (HTTPS) bez omezení na počet administrátorů a bez nutnosti instalovat dodatečnou management platformu nebo aplikaci.
Podpora LACP (802.3ad), VRRP
Funkce dynamického routingu (min. BGP, OSPF, RIP), pokud jsou tyto funkce licencované, licence, a to časově i místně neomezená, musí být součástí dodávky, a to jak pro IPv4, tak i IPv6
Funkce BFD (Bidirectional Forwarding Detection) pro routovací protokoly BGP a OSPF s možností upravit Min TX Interval, Min RX Interval, Discriminator pro jednotlivé rozhraní zařízení, a to i virtuální (VLAN interface)
IPv4 a IPv6 podpora PPTP, L2TP, GRE
Podpora SSL offload
Podpora TLS 1.3 i pro aplikační inspekce
Podpora IPv6 pro všechny funkce (tj. L3 protokoly a všechny NGFW funkce)
Podpora NAT64/NAT46
Podpora multicastu včetně routování a firewall funkcí (tvorba multicast FW politiky)
Možnost nastavovat firewall politiku na základě geografických údajů – GeoIP
Podpora firewall pravidel na základě identity uživatele pro MS AD prostředí – nastavení bezpečnosti uživateli na základě členství v AD skupině na doménovém kontroléru
Podpora detekce klientského zařízení s možností nastavovat firewall politiku na základě typu klientského zařízení (telefon, tablet, PC) včetně operačního systému (Android, iPhone, …) bez nutnosti instalovat klienty na koncové stanice
Podpora VPN SSL - portálový režim i tunelovací režim

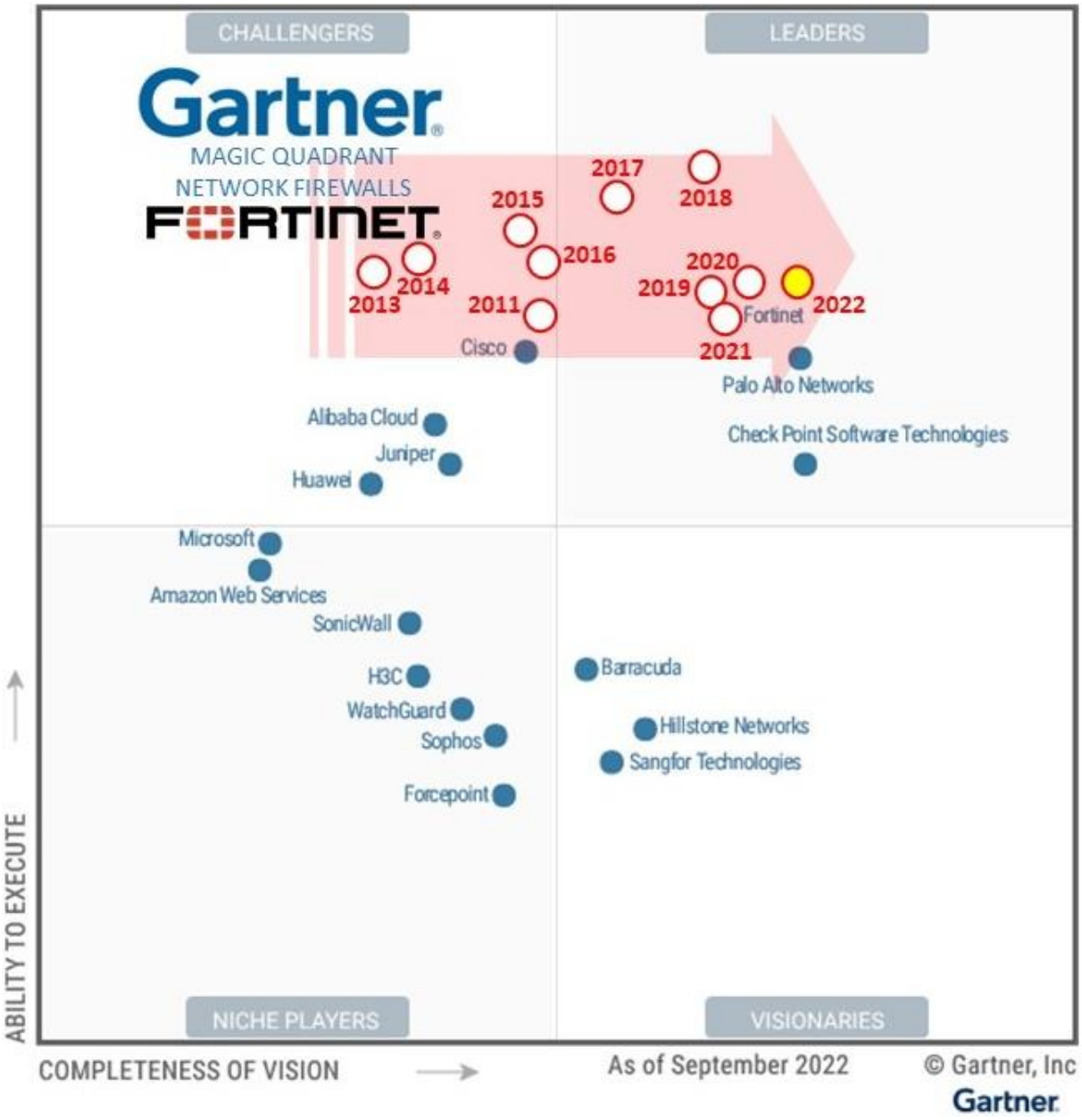
IPSEC gateway to gateway, hub and spoke, dial up konfigurace, podpora více tunelů (redundantní VPN)
Podpora Site-to-site IPSec VPN s podporou statického i dynamického routování
Antivir a antimalware kontrola pro vybrané protokoly, možnost volby různých databází
Antivir a antimalware požadujeme podporu archivace škodlivého obsahu, (ICAP pro offload)
Antivir, antimalware a antispam požadujeme automatické aktualizace signatur ze strany výrobce po dobu podpory zařízení
Pro antivir a antimalware výběr mezi proxy režimem (buffer) nebo flow režimem (inspekce on-the-fly)
Funkce kategorizace webových stránek (web filtering) s podporou kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze.
Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 3000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace.
Ověřování uživatelů proti LDAP, Active Directory, Single Sign On, Radius, TACACS+
Podpora dynamických profilů (možnost přiřadit konkrétní profil uživateli na základě ověření)
Podpora WAN optimalizace vybraných protokolů (Web Cache, Reverzní proxy, WCCP)
Traffic Shaping (QoS, prioritizace atd.)
Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu

Výše uvedené požadavky jsou splněny následujícím řešením

Product number	POPIS PRODUKTU	Množství
2x FortiGate 201F + 5 Years FortiCare & UTP		
FG-201F	FortiGate 201F 18 x GE RJ45 (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, 4 x 10GE SFP+ slots, NP6XLite and CP9 hardware accelerated, 480GB onboard SSD storage.	2
FC-10-F201F-950-02-60	5 Years Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and FortiCare Premium)	2

Mezinárodně platný benchmarkový report pro rok 2021 či novější, a to na úrovni umístění v „leaders segmentu“:

Gartner Magic Quadrant „NETWORK FIREWALLS“, září 2022



Datasheet Fortinet Fortigate 201F

Data Sheet

FortiGate 200F Series

FG-200F and FG-201F

Highlights

Gartner Magic Quadrant Leader for both Network Firewalls and WAN Edge Infrastructure.

Security-Driven Networking FortiOS delivers converged networking and security.

State-of-the-Art Unparalleled Performance with Fortinet's patented / SPU / vSPU processors.

Enterprise Security with consolidated AI / ML-powered FortiGuard Services.

Deep Visibility into applications, users, and devices beyond traditional firewall techniques.

AI/ML Security and Deep Visibility

The FortiGate 200F Series NGFW combines AI-powered security and machine learning to deliver Threat Protection at any scale. Get deeper visibility into your network and see applications, users, and devices before they become threats.

Powered by a rich set of AI/ML security capabilities that extend into an integrated security fabric platform, the FortiGate 200F Series delivers secure networking that is broad, deep, and automated. Secure your network end to end with advanced edge protection that includes web, content, and device security, while network segmentation and secure SD-WAN reduce complexity and risk in hybrid IT networks.

Universal ZTNA automatically controls, verifies, and facilitates user access to applications, reducing lateral threats by providing access only to validated users. Ultra-fast Threat Protection and SSL Inspection provides security at the edge you can see without impacting performance.

IPS	NGFW	Threat Protection	Interfaces
5 Gbps	3.5 Gbps	3 Gbps	Multiple GE RJ45, GE SFP, and 10 GE SFP+ slots

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

FortiOS, Fortinet's advanced operating system

FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into a simplified, single policy and management framework. Its organically built best-of-breed capabilities, unified operating system, and ultra-scalability allows organizations to protect all edges, simplify operations, and run their business without compromising performance or protection.

FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more, provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

FortiOS expands visibility and control, ensures the consistent deployment and enforcement of security policies, and enables centralized management across large-scale networks with the following key attributes:

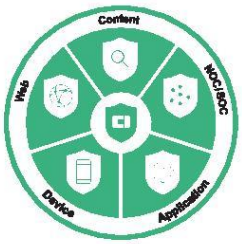
- Interactive drill-down and topology viewers that display real-time status
- On-click remediation that provides accurate and quick protection against threats and abuses
- Unique threat score system correlates weighted threats with users to prioritize investigations

Intuitive easy to use view into the network and endpoint vulnerabilities

Visibility with FOS Application Signatures

FortiConverter Migration Service

FortiConverter Service provides hassle-free migration to help organizations transition from a wide range of legacy firewalls to FortiGate Next-Generation Firewalls quickly and easily. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations can accelerate their network protection with the latest FortiOS technology.



FortiGuard Services

FortiGuard AI-Powered Security

FortiGuard's rich suite of security services counter threats in real time using AI-powered, coordinated protection designed by FortiGuard Labs security threat researchers, engineers, and forensic specialists.

Web Security

Advanced cloud-delivered URL, DNS (Domain Name System), and Video Filtering providing complete protection for phishing and other web born attacks while meeting compliance.

Additionally, its dynamic inline CASB (Cloud Access Security Broker) service is focused on securing business SaaS data, while inline ZTNA traffic inspection and ZTNA posture check provide per-sessions access control to applications. It also integrates with the FortiClient Fabric Agent to extend protection to remote and mobile users.

Content Security

Advanced content security technologies enable the detection and prevention of known and unknown threats and file-based attack tactics in real-time. With capabilities like CPRL (Compact Pattern Recognition Language), AV, inline Sandbox, and lateral movement protection make it a complete solution to address ransomware, malware, and credential-based attacks.

Device Security

Advanced security technologies are optimized to monitor and protect IT, IIoT, and OT (Operational Technology) devices against vulnerability and device-based attack tactics. Its validated near-real-time IPS intelligence detects, and blocks known and zero-day threats, provides deep visibility and control into ICS/OT/SCADA protocols, and provides automated discovery, segmentation, and pattern identification-based policies.

Advanced Tools for SOC/NOC

Advanced NOC and SOC management tools attached to your NGFW provide simplified and faster time-to-activation.

SOC-as-a-Service

Includes tier-one hunting and automation, log location, 24×7 SOC analyst experts, managed firewall and endpoint functions, and alert triage.

Fabric Rating Security Best Practices

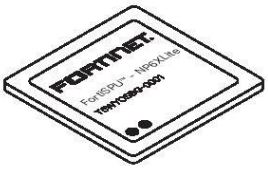
Includes supply chain virtual patching, up-to-date risk and vulnerability data to deliver quicker business decisions, and remediation for data breach situations.

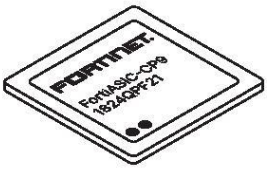
Secure Any Edge at Any Scale

Powered by Security Processing Unit (SPU)

Traditional firewalls cannot protect against today's content- and connection-based threats because they rely on off-the-shelf hardware and general-purpose CPUs, causing a dangerous performance gap. Fortinet's custom SPU processors deliver the power you need—up to 520Gbps—to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

ASIC Advantage





Network Processor 6XLite NP6XLite
Fortinet's new, breakthrough SPU NP6XLite network processor works inline with FortiOS functions delivering:

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

Content Processor 9 CP9
Content Processors act as co-processors to offload resource-intensive processing of security functions. The ninth generation of the Fortinet Content Processor, the CP9, accelerates resource-intensive SSL (including TLS 1.3) decryption and security functions while delivering:

- Pattern matching acceleration and fast inspection of real-time traffic for application identification
- IPS pre-scan/pre-match, signature correlation offload, and accelerated antivirus processing

FortiCare Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare Services help thousands of organizations get the most from our Fortinet Security Fabric solution. Our lifecycle portfolio offers Design, Deploy, Operate, Optimize, and Evolve services. Operate services offer device-level FortiCare Elite service with enhanced SLAs to meet our customer's operational and availability needs. In addition, our customized account-level services provide rapid incident resolution and offer proactive care to maximize the security and performance of Fortinet deployments.

Use Cases

Next Generation Firewall (NGFW)

- FortiGuard Labs' suite of AI-powered Security Services—natively integrated with your NGFW—secures web, content, and devices and protects networks from ransomware and sophisticated cyberattacks
- Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications across the attack surface
- Fortinet's patented SPU (Security Processing Unit) technology provides industry-leading high-performance protection

Secure SD-WAN

- FortiGate WAN Edge powered by one OS and unified security and management framework and systems transforms and secures WANs
- Delivers superior quality of experience and effective security posture for work-from-any where models, SD-Branch, and cloud-first WAN use cases
- Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing

Universal ZTNA

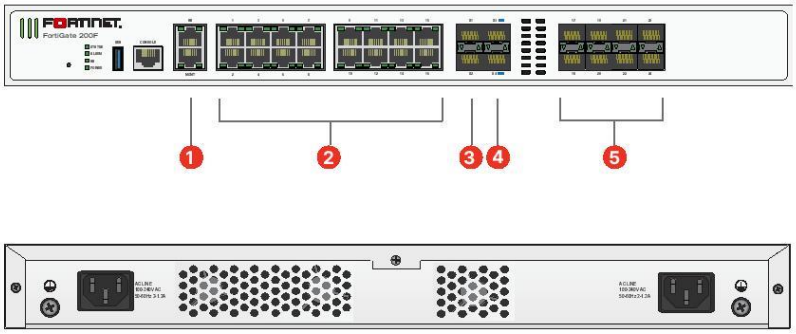
- Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies
- Provide extensive authentications, checks, and enforce policy prior to granting application access—every time
- Agent-based access with FortiClient or agentless access via proxy portal for guest or BYOD

Segmentation

- Dynamic segmentation adapts to any network topology to deliver true end-to-end security—from the branch to the datacenter and across multi-cloud environments
- Ultra-scalable, low latency, VXLAN segmentation bridges physical and virtual domains with Layer 4 firewall rules
- Prevents lateral movement across the network with advanced, coordinated protection from FortiGuard Security Services detects and prevents known, zero-day, and unknown attacks

Hardware

FortiGate 200F Series



Interfaces

1. 2 x GE RJ45 HA/ MGMT Ports
2. 16 x GE RJ45 Ports
3. 2 × 10 GE SFP+ Slots
4. 2 × 10 GE SFP+ FortiLink Slots
5. 8 x GE SFP Slots

Trusted Platform Module (TPM)

The FortiGate 200F Series features a dedicated module that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys. Hardware-based security mechanisms protect against malicious software and phishing attacks.

Dual Power Supplies

Power supply redundancy is essential in the operation of mission-critical networks. The FortiGate 200F Series offers dual built-in non-hot swappable power supplies.

Access Layer Security

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

Specifications

	FORTIGATE 200F	FORTIGATE 201F
Interfaces and Modules		
GE RJ45 Ports	16	
GE RJ45 Management / HA	1 / 1	
GE SFP Slots	8	
10 GE SFP+ FortiLink Slots (default)	2	
10 GE SFP+ Slots	2	
USB Port	1	
Console Port	1	
Onboard Storage	0	1× 480 GB SSD
Trusted Platform Module (TPM)	Yes	
Bluetooth Low Energy (BLE)	Yes	
Included Transceivers	0	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	5 Gbps	
NGFW Throughput [2,4]	3.5 Gbps	
Threat Protection Throughput [2,5]	3 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	27 / 27 / 11 Gbps	
Firewall Latency (64 byte, UDP)	4.78 µs	
Firewall Throughput (Packet per Second)	16.5 Mpps	
Concurrent Sessions (TCP)	3 Million	
New Sessions/Second (TCP)	280 000	
Firewall Policies	10 000	
IPsec VPN Throughput (512 byte) [1]	13 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2000	
Client-to-Gateway IPsec VPN Tunnels	16 000	
SSL-VPN Throughput	2 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	500	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	4 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	3500	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	300 000	
Application Control Throughput (HTTP 64K) [2]	13 Gbps	
CAPWAP Throughput (HTTP 64K)	20 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	64	
Maximum Number of FortiAPs (Total / Tunnel)	256 / 128	
Maximum Number of FortiTokens	5000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FORTIGATE 200F	FORTIGATE 201F
Dimensions and Power		
Height x Width x Length (inches)	1.73 × 17.01 × 13.47	
Height x Width x Length (mm)	44 × 432 × 342	
Weight	9.92 lbs (4.5 kg)	10.14 lbs (4.6 kg)
Form Factor (supports EIA/non-EIA standards)	Ear Mount, 1 RU	
AC Power Supply	100–240V AC, 50/60 Hz	
Power Consumption (Average / Maximum)	101.92 W / 118.90 W	104.52 W / 121.94 W
Current (Maximum)	100V / 2A, 240V / 1.2A	
Heat Dissipation	405.70 BTU/h	436.98 BTU/h
Redundant Power Supplies	Yes (Default dual non-swappable AC PSU for 1+1 Redundancy)	
Power Supply Efficiency Rating	80Plus Compliant	
Operating Environment and Certifications		
Operating Temperature	32°–104°F (0°–40°C)	
Storage Temperature	-31°–158°F (-35°–70°C)	
Humidity	20%–90% non-condensing	
Noise Level	49.9 dBA	
Forced Airflow	Side to Back	
Operating Altitude	Up to 7400 ft (2250 m)	
Compliance	FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL, CB, BSMI	
Certification	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.

[6] Uses RSA-2048 certificate.

Ordering Information

Product	SKU	Description
FortiGate 200F	FG-200F	18 x GE RJ45 (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, 4 x 10GE SFP+ slots, NP6XLite and CP9 hardware accelerated.
FortiGate 201F	FG-201F	18 x GE RJ45 (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, 4 x 10GE SFP+ slots, NP6XLite and CP9 hardware accelerated, 480GB onboard SSD storage.
Optional Accessories	**SKU**	**Description**
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.
1 GE SFP LX transceiver module	FN-TRAN-LX	1 GE SFP LX transceiver module 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+ 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+ transceivers, extended range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for all systems with SFP+ and SFP/SFP+ slots.
10GE SFP+ Transceiver Module, 30km Long Range	FN-TRAN-SFP+BD27	10GE SFP+ transceiver module, 30km long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD33, ordered separately)
10GE SFP+ Transceiver Module, (connects to FN-TRAN-SFP+BD27, ordered separately)	FN-TRAN-SFP+BD33	10GE SFP+ transceiver module, 30km long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD27, ordered separately)
25 GE SFP28 passive direct attach Cable	FN-CABLE-SFP28-1	25 GE SFP28 passive direct attach cable 1m for systems with SFP28 slots.
25 GE SFP28 passive direct attach Cable	FN-CABLE-SFP28-3	25 GE SFP28 passive direct attach cable 3m for systems with SFP28 slots.
25 GE SFP28 passive direct attach Cable	FN-CABLE-SFP28-5	25 GE SFP28 passive direct attach cable 5m for systems with SFP28 slots.
100 GE QSFP28 breakout to 4× 25 GE SFP28 passive direct attach cable	FN-CABLE-QSFP28-4SFP28-1	100 GE QSFP28 breakout to 4× 25 GE SFP28 passive direct attach cable, 1m
100 GE QSFP28 breakout to 4× 25 GE SFP28 passive direct attach cable	FN-CABLE-QSFP28-4SFP28-3	100 GE QSFP28 breakout to 4× 25 GE SFP28 passive direct attach cable, 3m
100 GE QSFP28 breakout to 4× 25 GE SFP28 passive direct attach cable	FN-CABLE-QSFP28-4SFP28-5	100 GE QSFP28 breakout to 4× 25 GE SFP28 passive direct attach cable, 5m

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles		
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
Security Services	FortiGuard IPS Service	•	•	•	•
	FortiGuard Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
	FortiGuard Web Security — URL and web content, Video and Secure DNS Filtering	•	•	•	
	FortiGuard Anti-Spam		•	•	
	FortiGuard IoT Detection Service	•	•		
	FortiGuard Industrial Security Service	•	•		
	FortiCloud AI-based Inline Sandbox Service [1]	•			
NOC Services	FortiGate Cloud (SMB Logging + Cloud Management)	•			
	FortiGuard Security Fabric Rating & Compliance Monitoring Service	•	•		
	FortiConverter Service	•	•		
	FortiGuard SD-WAN Underlay Bandwidth and Quality Monitoring Service	•			
SOC Services	FortiAnalyzer Cloud	•			
	FortiAnalyzer Cloud with SOCaaS	•			
Hardware and Software Support	FortiCare Essentials	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	FortiGuard Application Control	included with FortiCare Subscription			
	FortiCloud ZTNA Inline CASB Service [1]				
	Internet Service (SaaS) DB Updates				
	GeoIP DB Updates				
	Device/OS Detection Signatures				
	Trusted Certificate DB Updates				
	DDNS (v4/v6) Service				

1. Available when running FortiOS 7.2

FortiGuard Bundles

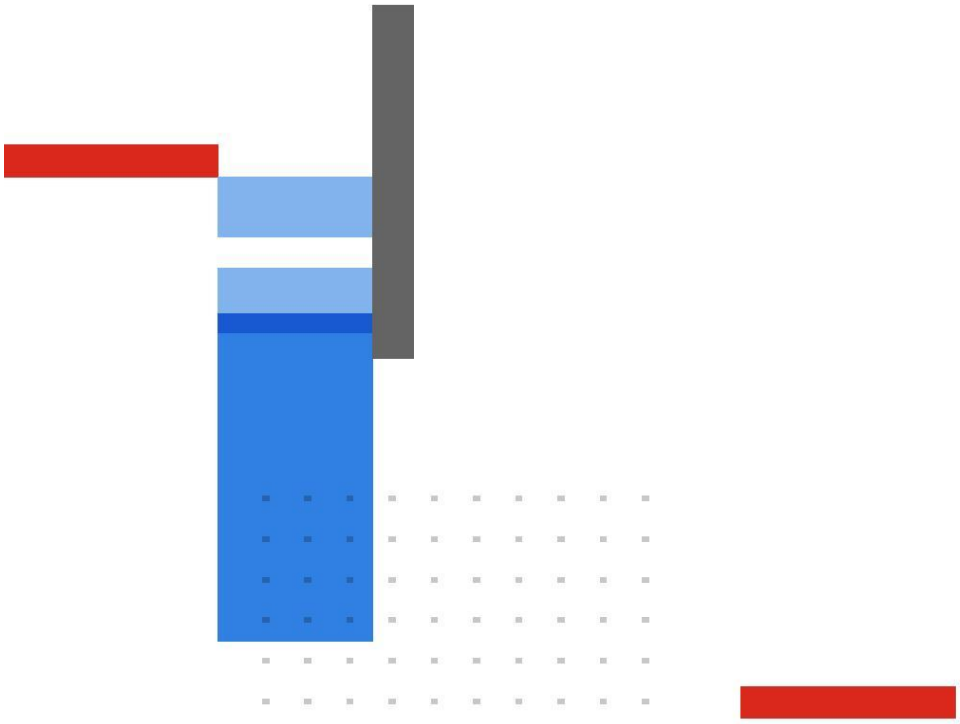
FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

FortiCare Elite

FortiCare Elite services offers enhanced service-level agreements (SLAs) and accelerated issue resolution. This advanced support offering provides access to a dedicated support team. Single-touch ticket handling by the expert technical team streamlines resolution. This option also provides Extended End-of-Engineering-Support (EoE's) of 18 months for added flexibility and access to the new FortiCare Elite Portal. This intuitive portal provides a single unified view of device and security health.

Fortinet CSR Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



www.fortinet.com

January 25, 2023

FG-200F-DAT-R17-20230125

Řešení emailové bezpečnosti

Obecné požadavky na řešení emailové bezpečnosti

Obecné vlastnosti:

- Produkt: E-mailová gateway pro kontrolu příchozí i odchozí pošty, plně softwarové řešení
- Kvalita nabízeného řešení:
    - Nabízené řešení, resp. jeho výrobce, musí být v mezinárodně platném benchmarkovém reportu pro rok 2021 či novější, a to na úrovni umístění v „leaders segmentu“, přičemž předmětem benchmarkového reportu musí být síťové firewally a benchmark musí obsahovat posouzení minimálně TOP10 celosvětových výrobců. (např. Gartner Magic Quadrant, Forrester Wave)
- Rozsah licenční podpory: 5 let
- Podpora MTA: min. Microsoft Exchange, Microsoft Office 365, Postfix
- V případě cloud host řešení, nezbytné dodržet následující požadavky:
    - Umístění data centra na území EHP (EEA)
    - Segregace dat
    - Šifrování dat
    - Dodržování zákonných požadavků v souladu s GDPR
    - Certifikace dle ISO 27017

Technické požadavky na řešení emailové bezpečnosti

Požadovaná funkcionalita/vlastnost
Podpora šifrovaného spojení (TLS) mezi skenerem a e-mailovým serverem
Ochrana příchozí i odchozí komunikace
Ochrana proti Phishingu
Antispam
Marketing/Graymail filtr
Detekce exploitů u PDF a Office dokumentů
Antimalware na základě databáze signatur vendora
Kontrola URL na základě databáze vendora
Detekce neznámých vzorků malware pomocí technologie strojového učení (Machine Learning)
Kontrola podezřelých souborů a URL v Sandboxu (Sandbox as a Service)
Podpora blokace na základě RBL (Real-time Blackhole List) a DNSBL (DNS blacklist)
Podpora geoblokace nastavovat politiku na základě geografických údajů – GeoIP
Možnost omezení příjmu e-mailů z definované domény jen z určitách IP adres (filter odesilatele)
Podpora pro SPF, DKIM i DMARC
Detekce spoofingu a podvržených e-mailů
Automatická detekce hesla k zašifrované příloze z těla e-mailu
Podpora pro skenování zašifrovaných příloh pomocí definované databáze hesel
Napojení na XDR (Trend Micro Vision One) ve vlastnictví zadavatele
Podpora Syslog pro export záznamů
Korelace e-mailových logů s koncovými stanicemi v rámci XDR
Podpora DLP na základě: • Regulárních výrazů • Klíčových slov • Atributů souborů
Podpora přeposílání logů na syslog
Možnost přístupu k e-mailům pomocí cloudové webové konzole v případě, že je cílový e-mail server nedostupný

Retence logů 60 dní
Možnost generovat logy v PDF
Možnost nastavení akce pro definované emaily/detekce: • Karanténa • Notifikace odesilatele, příjemce, administrátora • Doručení/přesměrování na konkrétní e-mailový server • Změna příjemce
Podpora ukládání zpráv do karantény min. 60 dní
Podpora karantény pro koncové uživatele včetně nastavení oprávnění pro koncové uživatele
Filtrování e-mailů na základě: • Parametrů hlavičky • Velikost • Název souboru • Přípona souboru • Typ souboru (true file type) • Klíčová slova v předmětu, těle, příloze • Příloha je šifrovaná • Příloha obsahuje aktivní prvky (například makro) • Počtu příjemců
Auditování administrátorských změn (audit log)
Podpora integrace s Active Directory
Outlook plugin pro možnost hlášení false positive/false negative

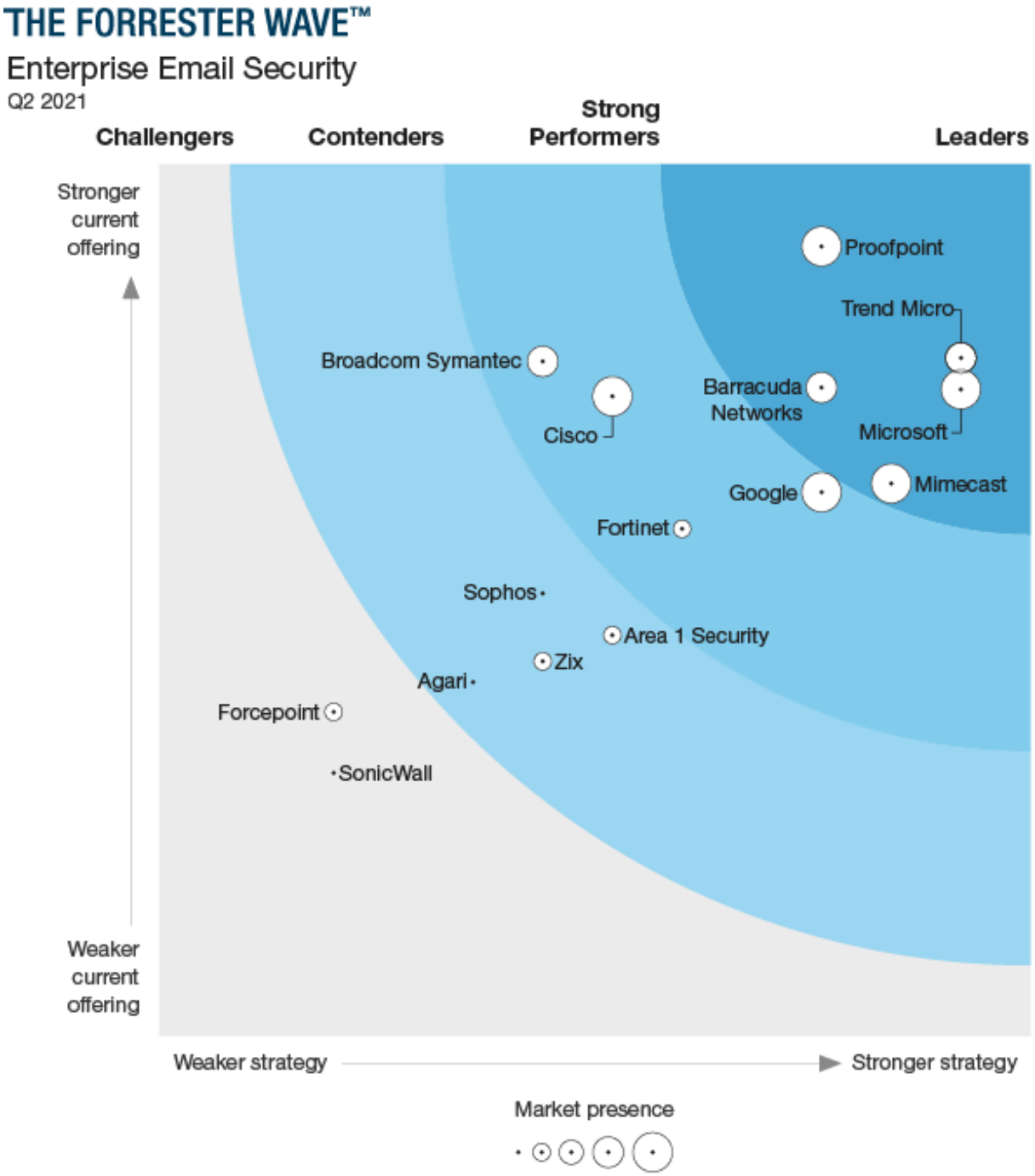
Výše uvedené požadavky jsou splněny následujícím řešením

Product number	POPIS PRODUKTU	Množství
DF01047912	Trend Micro Email Security Advanced: New, Government, 5-250 User License,12 months	150
DF01048200	Trend Micro Email Security Advanced: Renew, Government, 5-250 User License,24 months	150
DF01048200	Trend Micro Email Security Advanced: Renew, Government, 5-250 User License,24 months	150

Řešení pokrývá požadovaných 150 emailových schránek v souladu s přílohou č. 7 zadávací dokumentace. Licence pokrývají požadavek zadavatele na období 5 let (postupně budou aplikovány licence na 12 měsíců, následně na dalších 24 měsíců a nakonec poslední licence a zbývajících 24 měsíců).

Mezinárodně platný benchmarkový report pro rok 2021 či novější, a to na úrovni umístění v „leaders segmentu“:

The Forrester Wave™: „ENTERPRISE EMAIL SECURITY“, Q2 2021



Datasheet Trend Micro

Datasheet

TREND MICRO

Trend Micro™

Email Security

Stop more phishing, ransomware, and fraud attacks by using a cross-generational blend of threat techniques

Email is mission critical, but email-based threats, including ransomware and business email compromise (BEC), are growing exponentially–and it's difficult to keep up. Even your savviest employees can mistakenly click on a malicious link and expose your enterprise to a cyberattack.

Trend Micro™ Email Security stops more phishing, ransomware, and BEC attacks. Our solution uses an optimum blend of cross-generational threat techniques, like machine learning, sandbox analysis, data loss prevention (DLP), and other methods to stop all types of email threats. This solution minimizes management overhead and integrates with other Trend Micro security layers to share threat intelligence and provide central visibility of threats across your organization. Email Security protects Microsoft Exchange™, Microsoft Office 365, Gmail™, and other hosted and on-premises email solutions.

FORRESTER®
WAVE LEADER 2021
Enterprise Email Security

KEY FEATURES

- **Layered protection:** Provides comprehensive protection for phishing, spam, and graymail with multiple techniques, including sender, content and image analysis, machine learning, and more.
- **Email fraud protection:** Protects against BEC scams with enhanced machine learning and expert rules to analyze both the header and content of the email. Includes Trend Micro™ Writing Style DNA as an additional layer to conduct authorship analysis for BEC protection. (Trend Micro™ Cloud App Security license required for Writing Style DNA.)
- **Document exploit protection:** Detects advanced malware and exploits in PDFs, Microsoft Office, and other documents using static and heuristic logic to detect and examine abnormalities.
- **Advanced threat protection:** Discovers unknown malware using multiple patternless techniques, including pre-execution machine learning and top-rated sandbox technology from Trend Micro™ Deep Discovery™ for dynamic analysis of potentially malicious attachments or embedded URLs in a secure virtual environment.
- **File password extraction:** Heuristically extracts or opens password-protected files by leveraging a combination of user-defined passwords and message content.
- **URL time-of-click:** Blocks emails with malicious URLs before delivery and re-checks URL safety when a user clicks on it.
- **Source verification and authentication:** Includes Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting, and Conformance (DMARC).
- **Threat intelligence:** Uses the Trend Micro™ Smart Protection Network™, one of the largest threat intelligence databases, to correlate web, email, file, domain registries, and many other threat sources to identify attacker infrastructures before they are launched.
- **Email encryption:** Policy-driven email encryption includes hosted key management service and enables recipients to read encrypted emails on any device using a web browser.
- **DLP:** Includes DLP templates to make it easier to track, document, and safeguard confidential and sensitive information.
- **Email continuity:** Provides a standby email system that gives uninterrupted use of email in the event of a mail server outage.
- **Flexible reporting:** Generates reports based on scheduled and customizable content.
- **Trend Micro™ Connected Threat Defense™:** Synchronizes with Trend Micro Apex Central™ to implement a file and URL suspicious objects list.

Datasheet

What Email Security can do for you:

Stops phishing and spam

- Examines the authenticity and reputation of the email sender to screen out malicious senders.
- Analyzes email content using a variety of techniques to filter out spam and phishing.
- Protects against malicious URLs at delivery and at time-of-click (rewrites and analyzes URLs at the time of click and blocks them if malicious).

Detects and blocks advanced threats

- Detects and blocks ransomware and other types of zero-day malware using pre-execution machine learning, macro analysis, exploit detection, and dynamic sandbox analysis for files and URLs.
- Pre-execution machine learning filters unknown malware before sandbox analysis, enhancing efficiency and efficacy of advanced threat protection.
- Shares threat information with other security layers to guard against persistent and targeted attacks.

Protects against BEC

- Examines email behavior (an unsecure email provider, forged domain, or a reply to a free email service), intention (financial implication, urgency, or a call to action), and authorship (writing style).
- Allows you to have the flexibility to define your organization's high-profile users list for BEC protection.

Gives you peace of mind

- 24/7 technical support.
- All emails for customers in Europe, the Middle East, and Africa (EMEA) are routed to data centers in Western Europe. Emails for Australia and New Zealand are routed to data centers in Australia. Emails for Japan are routed to data centers in Japan. Emails for South and Southeast Asian countries are routed to data centers in Singapore. Emails for the rest of the world are routed to data centers in the U.S.
- The service is hosted on Amazon Web Services (AWS). Data centers in different regions operate independently and are not interconnected due to data privacy and sovereignty considerations

COMPARISON TABLE: TREND MICRO EMAIL SECURITY

CAPABILITY	STANDARD	ADVANCED
Email sender analysis and authentication by SPF, DKIM, and DMARC	Yes	Yes
Protection: Known threats (spam, malware, malicious URLs, and graymail)	Yes	Yes
Protection: Unknown malware detection	Exploit detection, predictive machine learning	Exploit detection, predictive machine learning, sandbox analysis for files
Protection: Unknown URL protection	URL time-of-click	URL time-of-click, sandbox analysis for URLs
Protection: Artificial intelligence (AI)-based fraud/BEC detection, checking email header and content	Yes	Yes
Protection: AI-based fraud/BEC detection, checking email sender authorship	–	Yes*
File-password extraction	–	Yes
Compliance: DLP and email encryption	Yes	Yes
Reporting: Customizable and scheduled reports	Yes	Yes
Syslog for exporting logs	Yes	Yes
Connected Threat Defense: Implementing of file and URL suspicious object lists from Apex Central	Yes	Yes
End user quarantine	Yes	Yes
Email continuity: Provides uninterrupted use of email in the event of a mail server outage	–	Yes
Mail tracking search window	30 days	60 days

*Cloud App Security license required

Service requirements

https://docs.trendmicro.com/en-us/enterprise/trend-micro-email-security-online-help/about/service-requirements.aspx

Podpora provozu

Technické požadavky na podporu provozu

Zadavatel požaduje, aby účastník po poskytnutí licencí pro NGFW a Emailové bezpečnostní řešení zahájil poskytování konzultační a technická podpory provozu pro dodané a implementované řešení s následujícími parametry:

- Měsíční alokace zdrojů: 8 hodin
- Dostupnost podpory:
  - Web-based helpdesk pro zakládání tiketů či požadavků v režimu 24x7
  - Email-based helpdesk pro zakládání tiketů či požadavků v režimu 24x7
  - Telefonický helpdesk pro konzultace v režimu 8x5
  - Veškerá konzultační a technická podpora bude poskytována v režimu 8x5, tj. v pracovní dny v běžnou pracovní dobu

Výše uvedené požadavky jsou splněny následujícím řešením

Kontakty na dodavatele:

- Web based helpdesk: support.altepro.cz
- Telefonická podpora: +420 840 11 22 33
- E-mailová podpora: support@altepro.cz

Podpora implementace

Technické požadavky na podporu implementace

Zadavatel požaduje, aby dodavatel v implementační fázi zajistil:

- Fyzickou instalaci v prostředí zadavatele
  - Součástí fyzické instalace je rovněž i dodávka veškerých transceiverů a patchcordů (optických i metalických) pro zapojení řešení do funkčního celku minimálně v rozsahu požadavků zadávací dokumentace a dle požadavků zadavatele
  - Součástí fyzické instalace je rovněž i dodávka napájecích PDU kabelů pro připojení na připravené PDU lišty v rozvaděčích zadavatele
- Fyzickou implementaci v prostředí zadavatele dle požadavků zadavatele, a to certifikovanými specialisty na jednotlivé dodávané oblasti.

Rozsah implementace představuje v souhrnu 10 x 8 hodin (mandays) práce technického týmu.