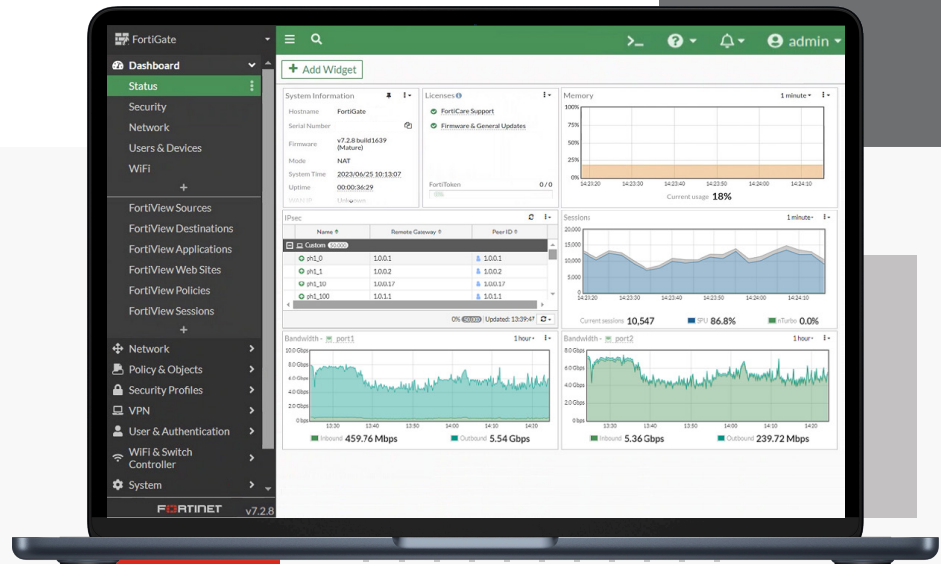# FortiGate Security Gateway Solutions

SecGW/SEG Solutions

Highlights

- Up to 3x more IPsec Tunnels
- Up to 8x IPsec Throughput
- Up to 5x Less Power Consumption
- Leverages Fortinet's NP7 SPU
- Integrated FortiGuard Labs AI security services

Proven, High Performance, and Flexible SecGW Platforms

Securing Radio Access Networks (RAN) connectivity to the core of the mobile network has never been as important as it is with the evolution of LTE, 5G, neutral hosts, small-cell and femto-cell deployments.

Fortinet Security Gateway (SecGW or SEG) solution offers a broad, scalable, and flexible set of tools, consumption models, and form factors, empowering service providers to protect their mobile core from RAN originating attacks, misbehavior, misconfiguration, and other types of threats that may impact the networks overall availability, confidentiality, and integrity. Our solution is natively secured with stateful L4 firewalling and continuous threat intelligence powered by FortiGuard Labs security services.

Overview

Fortinet's FortiGate, powered by FortiOS, have long provided iron-clad security services in many service providers and large enterprise networks.

Our Carrier-Grade IPsec/IPv4/IPv6/GTP/SCTP network services are based on the same familiar interface and proven carrier-grade reliability of the FortiOS.

Fortinet SecGW solutions deliver high predictability and service-level consistency to environments that generate massive amounts of connection set-ups and teardowns.

With Fortinet's powerful Security Processing Units (SPUs), a high level of performance is provided supporting up to 200,000 VPN tunnels from eNodeBs and gNodeBs, 40,000 VPN tunnels from other packet core sites and 800 Gbps of throughput in a single SecGW appliance with hardware acceleration, ensuring consistent high performance.

Highlights

- **Predictable high performance** for centralized and regional sites with security processing units (SPU and vSPU) for offload and acceleration, including packet encryption/decryption, hardware-generated NAT logs and IP fragment handling in the SPUs.

- **Security layer** between RAN and core domains and in the O-RAN domain: S1-MME, S1-U, N2, N3, X2, Xn, F1, E2, Operations and Maintenance (OAM).

- **Most energy efficient and smallest footprint** SecGW VNF for environments with limited resources, such as Private 5G, O-RAN or Multi-access Edge Computing (MEC).

- **Compact form factor** for space-constraint applications and lowers colocation cost for operators.

- **Native multi-tenancy support** with virtual domains (VDOMs) enables separate SecGW policies per network slice, eNodeB/gNodeB sets and traffic plane.

- **A rich ecosystem of application programming interfaces** (APIs) and connectors for ease of onboarding and integration to the MNO's ecosystem, such as operation and management, orchestration, and business support system (BSS).

- **Resiliency and High Availability** with Active-Active and Active-Passive redundancy options including geo-redundancy supported by based on FortiGate Clustering Protocol (FGCP) and FortiGate Session Life Support Protocol (FGSP).

- **Certificate distribution** for CMPv2 in a distributed environment. Includes integration with FortiAuthenticator or other PKI devices.

- **Efficient Session Scaling** on GTP with **dynamic UDP ports** mandated by 3GPP in R16 or later.

Deployment Options

Showcasing flexibility, several deployment options are available such as centralized, distributed, and vRAN/O-RAN decomposition as shown below.

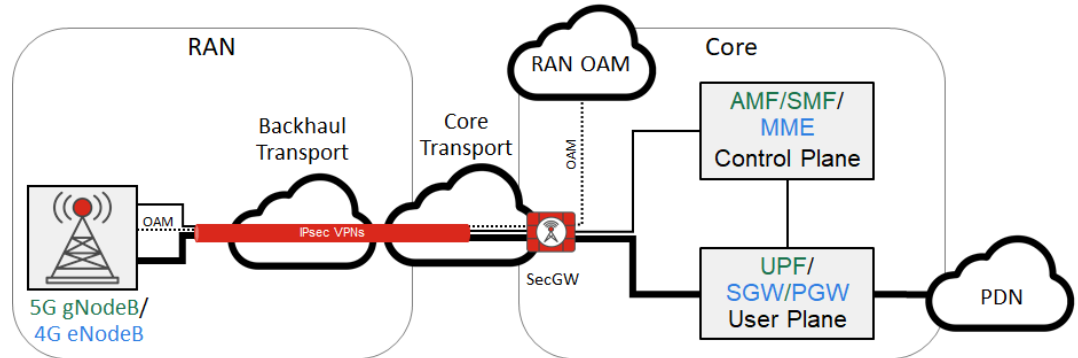**Available in**

Appliance

Virtual

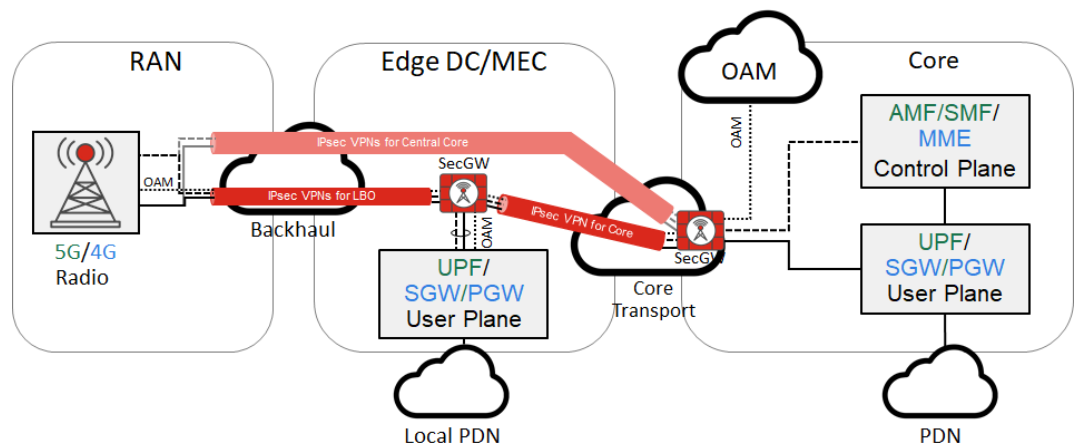Figure 1: Centralized SecGW/SEG Deployment

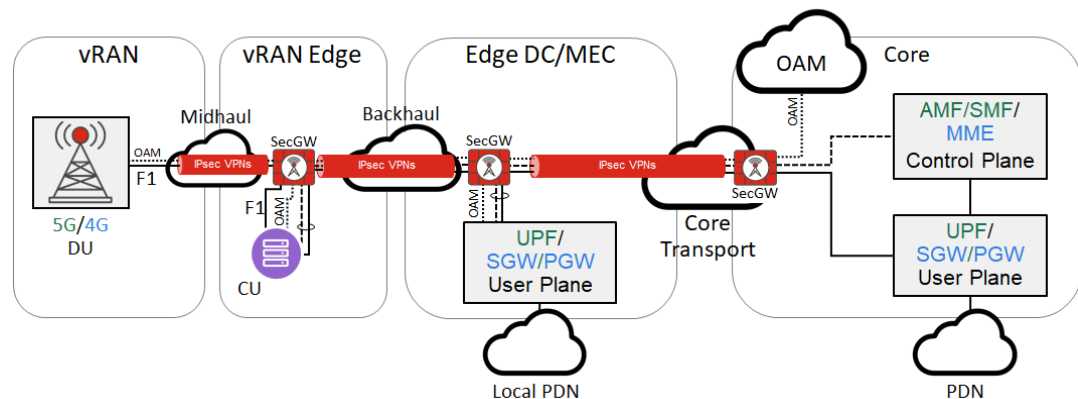Figure 2: Distributed SecGW/SEG Deployment

Figure 3: vRAN/O-RAN Decomposition SecGW/SEG Deployment

Features Summary

Confidentiality, Integrity, and Authentication

- Implements key SecGW function as defined by 3GPP specifications to protect 5G and 4G mobile packet core and RAN networks

- Add a security layer between the distinct RAN and Core domains, adding confidentiality and integrity to the traffic

- Protect user-, signaling- and management- traffic planes even when using a third-party transport network

- RAN sites and core are authenticated using certificates even if RAN sites belong to a competing MNO

- Prevent rogue radio sites from connecting to the packet core network

- Support for key distribution using Quantum Key Distribution (QKD) or Post-Quantum Cryptography (PQC) with carrier-grade scalability and ultra-high number of IPsec sessions and connection setup rates, and high throughput
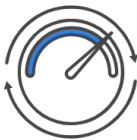
Performance

- Specialized hardware and virtual acceleration architecture

- High performance IPsec aggregation Gateway with IKEv2 support and high single-tunnel throughput

- Carrier grade connections per second (CPS) performance and delay for processing massive signaling surges due to RAN transport failures

- Low footprint form factors for very distributed deployments, such as O-RAN and MEC

- Detailed statistics per RAN site and IPsec session

- Consistent low latency for URLLC services

- Fortinet's NP7 purpose-built security processor units (SPU) deliver the industry's best performance and ultra-low latency

- Virtual SecGW appliances feature advanced virtual security processing units (vSPU) to high performance

Security

- Provides a powerful and stateful GTP and SCTP firewalling for the N3, S1-U, N2, S1-MME interfaces for blocking RAN/mobile-core attacks

- Detects and prevents of known attacks by using continuous threat intelligence from AI-powered FortiGuard Labs security services

Management

- Centralized management console that is effective and simple to use, which provides comprehensive network automation and visibility
- PKI integration using Certificate Management Protocol version 2 (CMPv2) for automatic enrollment and renewal
- Zero-Touch Provisioning with Single-Pane-of-Glass Management powered by the Fabric Management Center
- Application programming interfaces (APIs) and connectors for operations and management integration

Total Cost of Ownership (TCO) Reduction

- High performance, low footprint physical and virtual appliances, coupled with flexible licensing
- Lower TCO through efficient space and power consumption and efficient management and operations tools

Certification

- Independently tested and validated best security effectiveness and performance

Form Factors

- FortiGate physical appliances: 4800F, 4400F, 4200F, 3500F, 3000F, 2600F, 1800F
- FortiGate virtual appliances: VMUL, VM32, VM16, VM08, VM04
- FortiFirewall series: 4801F, 4400F, 4200F, 3501F, 3001F, 2601F, VMUL
- Public cloud support: AWS, MS Azure, Google Cloud, Oracle Cloud

Features List

FEATURE	SUPPORTED MODES
Networking and Tunneling	
SecGW interfaces	S1-MME, S1-U, N2, N3, X2, Xn, F1, E2, OAM
Authentication of tunnel peers	PKI -based (CMPv2), IKEv2, IKEv1, EAP
Crypto schemes	Suite-B (AES-CBC and AES-GCM 128 and 256 bits), Diffie-Hellman Groups (15, 19, 21, 31, 32 and others), post-Quantum Crypto
Dynamic L3 routing	IPv4 and IPv6
SCTP Firewall with multi-homing	⊘
S1-AP/NGAP message flooding protection	⊘
DSCP copy down for IPsec	⊘ for prioritization of relevant traffic even if encrypted
IPsec tunnels	Dial-up, site-to-site
Tunnel profiles	⊘
Concurrent tunnel scale	Up to 200K
Elephant flows within VPN	⊘ HW accelerated
Extended sequence number (ESN)	⊘ HW accelerated
IP fragment handling	⊘ HW accelerated
Anti-replay and packet reordering	⊘ HW accelerated
Perfect forward secrecy	⊘
Dynamic routing	⊘
Reverse route injection	⊘
IKE configuration payload	⊘
High Availability and Redundancy	
Link aggregation groups (LAGs)	⊘
High availability	⊘ Supports Active/active, active/passive, clustering with Geo-redundancy
Security Threat Protection	
DoS mitigation for the core	⊘
Protocol inspection	⊘ Supports inspection of SCTP, GTP-U Payload

Hardware Specifications

METRIC	1800F	2600F	3000F	3500F	4200F	4400F	4800F
Performance and Capacity—SecGW							
IPsec VPN Throughput (512 byte) CBC[1]	55 Gbps	55 Gbps	105 Gbps	165 Gbps	210 Gbps	310 Gbps	800 Gbps
IPsec VPN Throughput (512 byte) GCM[2]	74 Gbps	74 Gbps	147 Gbps	185 Gbps	278 Gbps	365 Gbps	TBA
Max GW to GW IPsec Tunnels	20 000	20 000	40 000	40 000	40 000	40 000	40 000
Max Client to GW IPsec Tunnels	100 000	100 000	200 000	200 000	200 000	200 000	200 000
Interfaces and Modules							
10 GE/GE RJ45 Slots	16[5]	16	16				
10 GE/GE RJ45 Management Ports			2	2			2
25 GE SFP28/10 GE SFP+/GE SFP Slots	12	16	14	32	16	16	
25 GE SFP28/10 GE SFP+/GE SFP HA Slots	2[7]	2[7]	2		2	2	
25 GE SFP28/10 GE SFP+/GE SFP AUX Slots					2	2	
50 GE/25 GE/10 GE SFP56/28 Slots							12
100 GE QSFP28/40 GE QSFP+ Slots	4[6]	4	6	6	8	12	12[3]
400 GE/200 GE QSFP-DD Slots							8
GE SFP Slots	8[5]						
GE RJ45 Management Ports	2	2			2	2	
USB Ports	1	1	1	1	1	1	1
Console Port	1	1	1	1	1	1	1
Internal Storage	2 TB (1801F)	2 TB (2601F)	2 TB (3001F)	4 TB (3501F)	4 TB (4201F)	4 TB (4401F)	4 TB (4801F)
Included Transceivers	2x SFP+ (SR 10 GE)	2x SFP+ (SR 10 GE)	2x SFP+ (SR 10 GE)	2x SFP+ (SR 10 GE)	2x SFP+ (SR 10 GE)	2x SFP+ (SR 10 GE)	2x SFP+ (SR 10 GE)
Dimensions and Power							
Height x Width x Length (in)	3.5×17.25×21.1	3.5×17.25×21.1	3.5×17.4×21.9	3.5×17.4×21.9	5.22×17.20×26.17	6.97×17.20×26.17	6.89×17.13×26.10
Height x Width x Length (mm)	88.4×438×536	88.4×438×536	89×443×556	89×443×556	132.5×437×664.8	177×437×665	175×435×663
Weight[4]	30.2 lbs (13.7 kg)	30.6 lbs (13.9 kg)	37.3 lbs (16.9 kg)	43.8 lbs (19.9 kg)	59.75 lbs (27.1 kg)	81.8 lbs (37.1 kg)	90.83 lbs (41.2 kg)
Form Factor (Supports EIA/non-EIA standards)	Rack Mount, 2 RU	Rack Mount, 2 RU	Rack Mount, 2 RU	Rack Mount, 2 RU	Rack Mount, 3 RU	Rack Mount, 4 RU	Rack Mount, 4 RU
AC Power Supply	100–240V AC, 50/60 Hz	100–240V AC, 47/63 Hz	100–240V AC, 50/60 Hz	100–240V AC, 50/60 Hz	100–240V AC, 50/60 Hz	100–240V AC, 50/60 Hz	200-240V AC, 50/60 Hz
Power Consumption[4] (Average/Maximum)	388 W/544 W	416 W/510 W	425 W/680 W	760 W/1174 W	931 W/1291 W	1533 W/1875 W	1940 W/2372 W
AC Current (Maximum)	7A@100VAC, 3A@240VAC	6A	12A@120V, 9A@240V	12A@120V, 9A@240V	13.5A@120V, 5.5A@240V	20A@100V, 9A@240V	10.5A@200V, 12.5A@240V
Heat Dissipation[4]	1854.84 BTU/h	1740 BTU/h	2321 BTU/h	4006 BTU/h	4405 BTU/h	6397.77 BTU/h	8087.2 BTU/h
DC Power Input Range	-48V to -60V DC	-48V to -60V DC			-48V to -60V DC	-48V to -60V DC	-48V to -60V DC
DC Current (Maximum)	20A	15A			20A/100Apk	32A/100Apk	
Redundant Power Supplies	Yes, Hot Swappable	Yes, Hot Swappable	Yes, Hot Swappable	Yes, Hot Swappable	Yes, Hot Swappable	Yes, Hot Swappable, 2+2 (AC), 1+1 (DC)	Yes, Hot Swappable
Operating Environment and Certifications							
Operating Temperature	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)
Storage Temperature	-31°–158°F (-35°–70°C)	-31°–158°F (-35°–70°C)	-31°–158°F (-35°–70°C)	-31°–158°F (-35°–70°C)	-31°–158°F (-35°–70°C)	-31°–158°F (-35°–70°C)	-31°–158°F (-35°–70°C)
Humidity	10%–90% non-condensing	10%–90% non-condensing	5%–90% non-condensing	20%–90% non-condensing	20%–90% non-condensing	20%–90% non-condensing	20%–90% non-condensing
Noise Level	62.74 dBA	71.72 dBA	69 dBA	53.5 dBA	57 dBA	68.9 dBA	68.9 dBA
Operating Altitude	Up to 7400 ft (2250 m)	Up to 7400 ft (2250 m)	Up to 7400 ft (2250 m)	Up to 7400 ft (2250 m)	Up to 7400 ft (2250 m)	Up to 7400 ft (2250 m)	Up to 7400 ft (2250 m) [8]
Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB

1. IPsec VPN performance test uses AES256-CBC-SHA384
2. IPsec VPN performance test uses AES256-GCM-SHA384
3. 200GE/100GE/40GE QSFP56/28 Slots
4. Version without storage

5. GE only
6. 40GE QSFP+ only
7. 10GE SFP+ only
8. Operating at maximum temperature derates 1.5°C per 1000 ft (305 m)

Virtual Machine Specifications

METRIC	VM-04	VM-08	VM-16	VM-32	VM-UL
Performance and Capacity					
vCPU Support (minimum / Maximum)	1 / 04	1 / 08	1 / 16	1 / 32	1 / unlimited
Storage Support (Minimum / Maximum)	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB
IPsec VPN Throughput (1360 byte) GCM-vSPU off[10]	2.2 Gbps	5.5 Gbps	6.9 Gbps	11.1 Gbps	NA[9]
IPsec VPN Throughput (1360 byte) GCM-SPU on[11]	20 Gbps	32.5 Gbps	42.3 Gbps	47.3 Gbps	NA[9]
Max GW to GW IPsec Tunnels	40K	50K	50K	50K	NA[9]
Max Client to GW IPsec Tunnels	40K	50K	50K	50K	NA[9]

9 Will depend on the characteristics of the underlying platform

10 IPsec VPN performance test uses AES256-GCM-SHA384 with vSPU off (UDP, 1360 Byte/pkt)

11 IPsec VPN performance test uses AES256-GCM-SHA384 with vSPU on(UDP, 1360 Byte/pkt)

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

Datasheet numbers should only be used as a guidance for VM sizing, rather than a definitive information since performance measures vary quite significantly based up on the selected testbed (hardware + host OS), FortiOS version and configuration, as well as the tunning applied to achieve more performance. For numbers aligned with your own environment, make sure you engage with one of our pre-sales representatives for specific guidance before purchasing any licenses.

Actual performance may vary depending on the network and system configuration. Note that these metrics are updated periodically as the product performance keeps improving through internal testing. The discrepancy in the performance numbers may be noted in different versions of the document so ensure that you refer to the latest datasheets.

Performance metrics were observed using DELL R740 (CPU Intel Xeon Platinum 8268 CPU, 192G memory), with SRIOV NIC Intel X710. Tested with FortiOS 7.0.6 running on KVM/ RedHat 8.4.

vSPU refers to the combination of FortiOS vNP and DPDK libraries in the FortiGate-VM. vNP is the software emulation of a subset of Fortinet's Network Processor (NP).

Applicable to 7.0.6+. The actual working number of consumable network interfaces varies depending on the Linux RedHat KVM instance types/sizes and may be less.

vSPU requires at least 2vCPUs.

Flexible Licensing

SecGW platforms and functionality can be delivered via two different pricing models:

CAPEX pricing model – FortiGate

In this pricing model, the complete platform, physical and/or virtual FortiGate, is paid up front covering the full capacity that the platform can deliver.

Bandwidth-based pricing model – FortiFirewall

This pricing model consists of two components:

- The barebone platform, physical and/or virtual FortiFirewall, is paid upfront
- Perpetual and stackable bandwidth licenses in steps of 10Gbps and 100Gbps are added to meet capacity needs. This is a network-wide bandwidth license that allows for short, rare burst of traffic exceeding the licensed capacity

Ordering Information

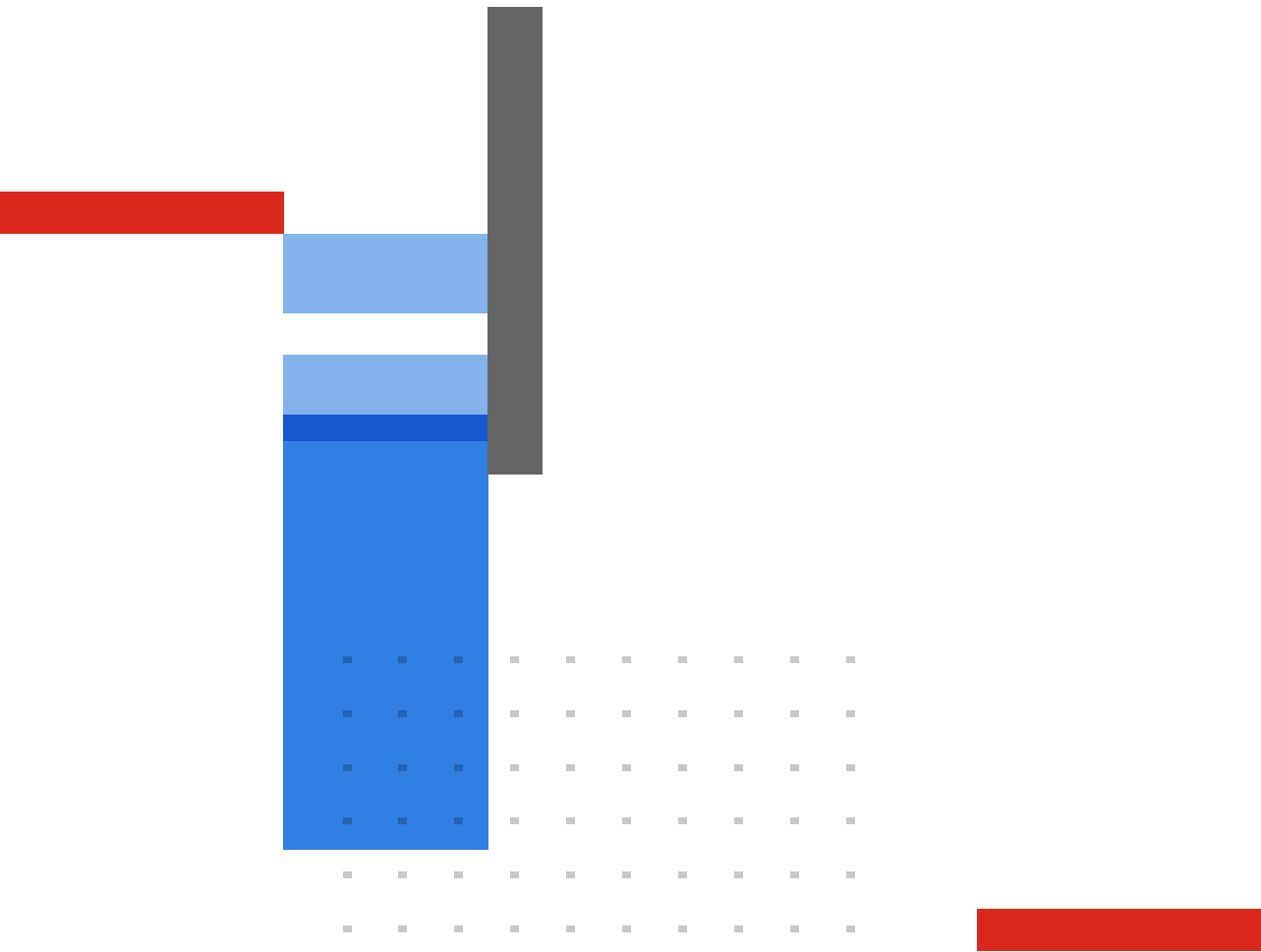| SECURITY GATEWAY PHYSICAL PLATFORMS		
Model	FortiGate SKU	FortiFirewall SKU
1800F	FG-1800F	FFW-1801F
FortiCare 24×7 Support for 1800F	FC-10-F18F1-247-02-DD	FC-10-F181F-247-02-DD
2600F	FG-2600F	FFW-2600F
FortiCare 24×7 Support for 2600F	FC-10-FD26F-247-02-DD	FC-10-F260F-247-02-DD
3000F	FG-3000F	FFW-3001F
FortiCare 24×7 Support for 3000F	FC-10-FF3K1-247-02-DD	FC-10-FF3K1-247-02-DD
3500F	FG-3500F	FFW-3501F
FortiCare 24×7 Support for 3500F	FC-10-F3K5F-247-02-DD	FC-10-FF35F-247-02-DD
4200F	FG-4200F	FFW-4200F
FortiCare 24×7 Support for 4200F	FC-10-F42HF-247-02-DD	FC-10-B420F-247-02-DD
4400F	FG-4400F	FFW-4400F
FortiCare Support for 4400F	FC-10-F44HF-247-02-DD	FC-10-B440F-247-02-DD
4800F	FG-4800F	FG-4801F
FortiCare Support for 4800F	FC-10-F48HF-247-02-DD	FC-10-B481F-247-02-DD
SECURITY GATEWAY VIRTUAL PLATFORMS		
Model	FortiGate SKU	FortiFirewall SKU
VM-04 virtual appliance	FG-VM04	
FortiCare 24×7 Support for FortiGate VM-04	FC-10-FVM04-248-02-DD	
VM-08	FG-VM08	
FortiCare 24×7 Support for FortiGate VM-08	FC-10-FVM08-248-02-DD	
VM-16	FG-VM16	
FortiCare 24×7 Support for FortiGate VM-16	FC-10-FVM16-248-02-DD	
VM-32	FG-VM32	
FortiCare 24×7 Support for FortiGate VM-32	FC-10-FVM32-248-02-DD	
VM-UL	FG-VMUL	FF-VMBB
FortiCare 24×7 Support for FortiGate VM-UL	FC-10-FVMUL-248-02-DD	FC-10-FVMBB-248-02-DD
SECURITY GATEWAY FORTIFIREWALL BANDWIDTH LICENSES[12]		
Product	FortiGate SKU	FortiFirewall SKU
10 Gbps SecGW Bandwidth License for FortiFirewall (stackable)	N/A (included in Platform)	FG-PBW-10G
FortiCare Support for 10 Gbps SecGW Bandwidth License for FortiFirewall	N/A (included in Platform)	FC1-10-FGPBW-248-01-DD
100 Gbps SecGW Bandwidth License for FortiFirewall (stackable)	N/A (included in Platform)	FG-PBW-100G
FortiCare Support for 100 Gbps SecGW Bandwidth License for FortiFirewall	N/A (included in Platform)	FC2-10-FGPBW-248-01-DD
1Tbps SecGW Bandwidth License for FortiFirewall (stackable)	N/A (included in Platform)	FG-PBW-1000G
FortiCare Support for 1Tbps SecGW Bandwidth License for FortiFirewall	N/A (included in Platform)	FC3-10-FGPBW-248-01-DD

12 Network-wide bandwidth licenses to be added on the top of a collection of FortiFirewall physical or virtual platforms

This pricing model allows operators to better align their costs with revenues from their customers, with flexibility of adding a network-wide peak bandwidth license based on traffic usage.

Fortinet Corporate Social Responsibility 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.

F🔴RTINET

www.fortinet.com

July 24, 2024

FSGW-DAT-R02-20240724