Cybersecurity

ADVANCED FIREWALL

gigas

Gigas incorporates Fortinet technology, a leading provider of advanced perimeter security solutions, into its Cloud DataCenter to offer the Advanced Firewall service. This comprehensive solution, based on Gigas' IaaS and FortiGate virtual appliances (FortiGate-VM), designed to operate in virtualised and cloud environments, addresses the fundamental needs for protection, information control, and secure access to cloud resources.

The Gigas Advanced Firewall service enables secure integration of the cloud environment with clients' on-premises platforms and mobility needs, simplifying the management of security policies from a centralised console. With the new flexible licensing model, clients can align security features with their specific business requirements, choosing between two comprehensive protection packages: LITE and PRO.

Next-Generation Firewall (NGFW)

- Next-generation firewalls reduce complexity by combining threat protection security capabilities in a single high-performance system. •Provides multi-layer traffic inspection, including SSL-encrypted traffic, to identify and mitigate the most complex threats. • Ensures secure communications between multiple networks and remote users using SSL and IPsec VPN technologies to guarantee data confidentiality and integrity in transit. • Integrates SD-WAN functionalities to monitor and optimise network link quality and intelligently orchestrate traffic across the SD-WAN overlay.

Comprehensive Security

They provide comprehensive and unified protection. This includes:

- VPN (IPsec and SSL)
- Intrusion Prevention System (IPS)
- Application Control
- Anti-malware
- Web Filtering
- Secure DNS
- Secure SD-WAN functionalities
- And other advanced security features

Technical Features

- Unified Operating System (FortiOS)
- Flexible and agile deployment
- Native integration into the "Security Fabric"
- Dynamic scalability and high availability (HA)
- Reduced Capital Expenditure (CapEx)
- Flexible and predictable licensing models (OpEx
- Immediate deployment
- Business agility and fast "Time-to-Market"
- Complete network and information protection
- Efficient resource usage
- Enhanced intelligence: "Smart policies"
- Leading technology

Deployment Flexibility

As a virtual machine, it can be deployed in a wide variety of environments, including:

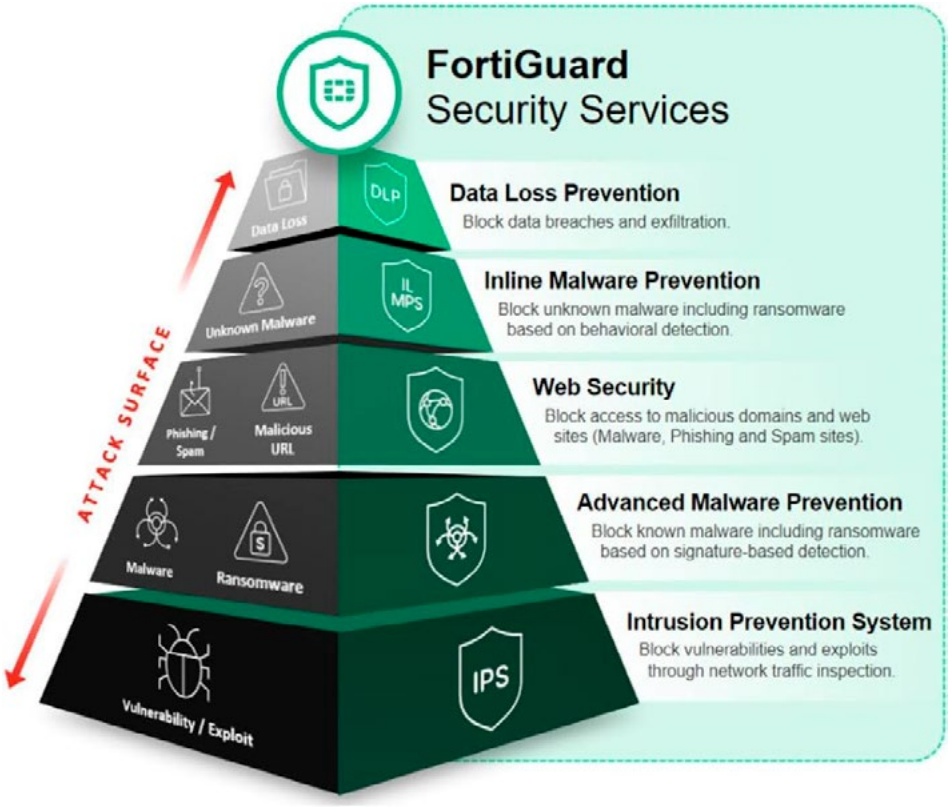
- **Public Clouds:** Available on major providers such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud, and others.
- **Private Clouds:** Seamlessly integrates with virtualization platforms such as VMware vSphere, Microsoft Hyper-V, KVM, and Citrix XenServer.
- **Hybrid Environments:** Allows consistent security policies to be extended from on-premises data centres to the cloud, enabling unified management across hybrid architectures.
- **Scalability:** Adapts to the organisation's performance requirements. Virtual machine resources (vCPU, vRAM) can be scaled, or high-availability (HA) clusters can be deployed to ensure business continuity and support higher traffic loads.
- **Centralised Management:** Like physical appliances, FortiGate-VM integrates into the Fortinet Security Fabric ecosystem, allowing centralised management and visibility through tools such as FortiManager and FortiAnalyzer. This simplifies the administration of security policies across the entire infrastructure.

SECURITY PACKS

Security Packs	LITE	PRO
Intrusion Prevention System (IPS)	✓	✓
Advanced Malware Protection (AMP)		
Antivirus	✓	✓
Botnet	✓	✓
Mobile Malware	✓	✓
Outbreak Prevention	✓	✓
Sandbox SaaS (Detection Only)	✓	✓
Inline SaaS Application Security (CASB)	✓	✓
AI-based Inline Malware Prevention		✓
Web Security		
Web and Content Filtering		✓
Secure DNS Filtering		✓
Video Filtering		✓
Attack Surface Security Rating		
IoT Security		✓
Security Self-check		✓
Data Loss Prevention		✓

AVAILABLE PRODUCTS

Model	vCores	GB RAM	Security Pack
FW Lite 1v	1	4	Lite
FW Pro 1v	1	4	Pro
FW Lite 2v	2	8	Lite
FW Pro 2v	2	8	Pro
FW Lite 4v	4	16	Lite
FW Pro 4v	4	16	Pro
FW Pro 6v	6	24	Pro
FW Pro 8v	8	32	Pro



LITE PACK

IPS: Intrusion Prevention

- ✓ Monitors network traffic for malicious content.
- ✓ Uses AI/ML models for real-time threat detection and applies virtual patches to protect against newly discovered vulnerabilities.

AMP: Protección Antimalware

- ✓ Provides real-time defence against all types of file-based threats, including viruses, spyware, and ransomware.

  Protection is enhanced with global threat intelligence and multi-layered security to block known malware.

CASB Seguridad de aplicaciones

- ✓ Aims to provide advanced control and security over SaaS (Software as a Service) applications when accessed from a network protected by the Advanced Firewall.

PRO PACK

The Pro Pack includes all the features of the Lite Pack plus the following:

Web Security

- ✓ Web Filtering: Blocks access to malicious, phishing, or inappropriate sites and analyses links in emails to detect potential threats
- ✓ DNS Filtering: Provides full visibility of DNS traffic, blocks high-risk domains, and protects against advanced attack techniques such as DNS tunnelling.
- ✓ IP Reputation and Anti-Botnet: Prevents communication with botnets, blocks DDoS attacks from known sources, and stops data exfiltration and communication with Command & Control (C&C) centres.

DLP: Data Loss Prevention

- ✓ Identifies and prevents the transfer of sensitive information outside the network perimeter. Ensures visibility and protection of data across networks, clouds, and users, simplifying compliance with privacy regulations.

Zero-Day Threat Prevention

- ✓ Incorporates an AI-based online malware prevention engine. Analyses and filters unknown files in real time, providing protection in under a second against zero-day threats and sophisticated attacks. The service includes sandboxing and aligns with the MITRE ATT&CK® framework to accelerate incident investigation.

Security Rating

- ✓ Security Rating: Provides security and compliance assessments, as well as risk ratings, to evaluate the organisation's security posture against industry best practices.
- ✓ IoT Security: Automatically discovers and classifies IoT devices on the network, allowing vulnerabilities to be remediated and virtual patches applied for protection.

CONFIGURATION OPTIONS

The Advanced Firewall offers administrators a variety of methods and wizards for configuring devices during deployment. From a simple web interface to a command-line interface with advanced features, the system provides the flexibility and simplicity the client needs.

Features:

- Web-based user interface
- Command-Line Interface (CLI)

TECHNICAL SPECIFICATIONS

SPECIFICATIONS	FW Lite/Pro 1v	FW Lite/Pro 2v	FW Lite/Pro 4v	FW Pro 6v	FW Pro 8v
Technical specifications					
vCPU	1	2	4	6	8
RAM	4GB	8GB	16GB	24GB	32GB
Firewall Policies (System)	20.000 / 40.000	50.000 / 100.000	50.000 / 100.000	50.000 / 100.000	50.000 / 100.000
Performance					
Firewall Throughtput (UDP packets)	12 Gbps	15 Gbps	28 Gbps	30 Gbps	33 Gbps
IPSec VPN Throughput (AES256+SHA1)	1 Gbps	1.5 Gbps	3 Gbps	4.5 Gbps	5.5 Gbps
IPS Throughput	3.5 Gbps / 1 Gbps	5.5 Gbps / 1.5 Gbps	8 Gbps / 3 Gbps	10 Gbps / 4.5 Gbps	15.5 Gbps / 6 Gbps
Antivirus Throughput	200 Mbps	300 Mbps	350 Mbps	375 Mbps	400 Mbps
Gateway to Gateway IPSec VPN Tunnels (System / VDOM)	2.000	2.000	2.000	2.000	4.000
Client-to-Gateway IPSec VPN Tunnels	6.000	12.000	20.000	30.000	40.000
Concurrent Sessions	1.0 Million	2.6 Million	4.3 Million	6 Million	8.5 Million
New Sessions/Second	85.000	100.000	125.000	130.000	150.000
Concurrent SSL VPN Users	1.000	2.000	4.500	6.500	10.000
VPN - SSL Throughput	800 Mbps	830 Mbps	2 Gbps	3 Gbps	4.5 Gbps