ADVANCED FIREWALL
/ technical datasheet

a gigas group company

FORTIGATE ADVANCED FIREWALL

ONI uses Fortinet technology for its Cloud Datacenter. Fortinet is a leading manufacturer of solutions for advanced perimeter security and has proven experience in information protection, monitoring, inspection, and multi-layer traffic management, and strictly complies with the demands of important corporations.

With its FortiGate-VM platform, ONI' FortiGate Advanced Firewall offers its Cloud Datacenter users a comprehensive security solution which meets basic protection needs, information control, and access to Cloud resources.

In addition to ensuring a safe Cloud environment using the client's original platforms and their mobility needs, ONI' FortiGate Advanced Firewall allows the management of their private security policies to be simplified using centralized and comprehensive multi-platform management.

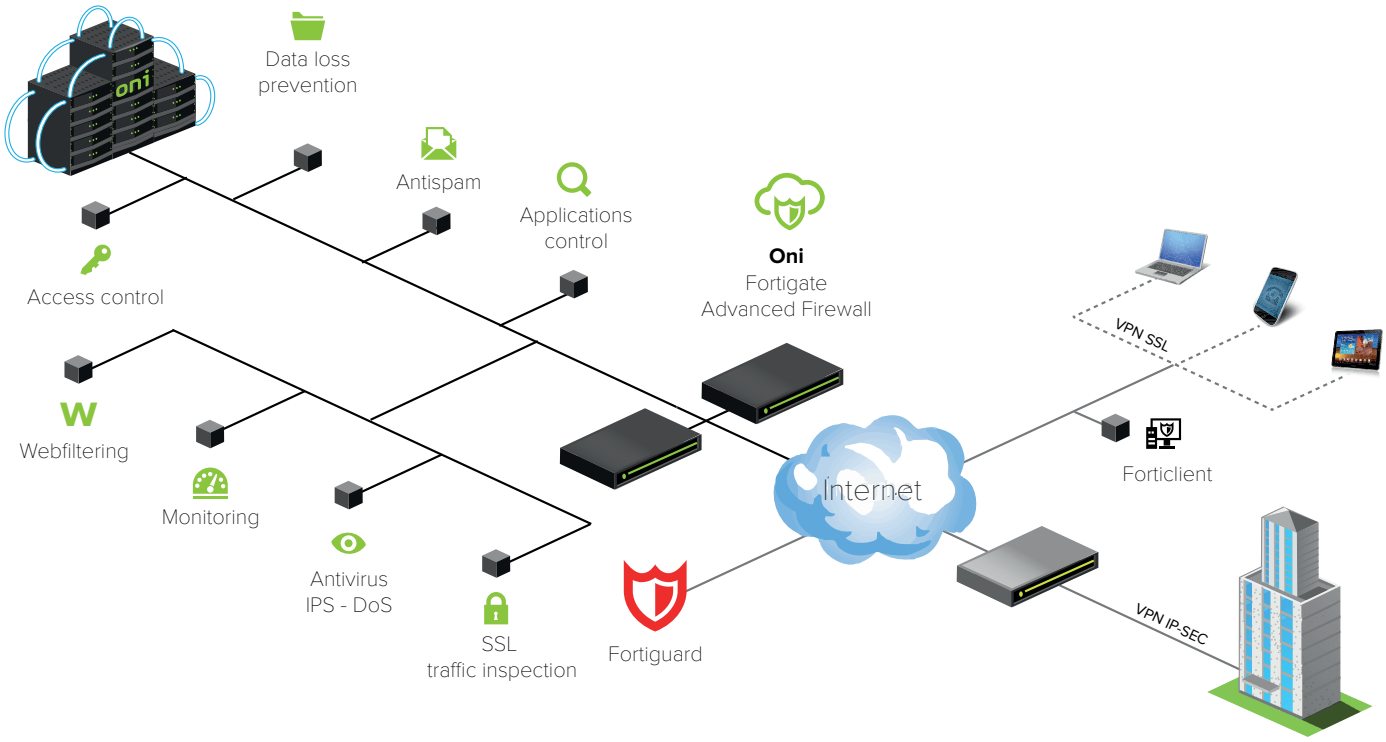
ONI' own team of engineers is available to clients 24 hours a day, 365 days a year. In addition to ensuring that the platform runs well and is free from threats and intrusions that can interfere with the quality of our services, our engineers can take on the management of the FortiGate Advanced Firewall as required our customers.

ONI offers free trials for our Advaced Firewall. If you are interested, please write to business@oni.pt

ADVANTAGES

- **Complete network and information protection**
- **Immediate installation**
- **Efficient use of resources**
- **More Intelligence: "Smart policies"**
- **Free trial**
- **State of the art leader technology**

FORTINET



MODELS

Firewall model
Fortinet's Firewall technology offers multi-layer traffic inspections thanks to a comprehensive management solution with high levels of security. It combines engines for application control, antivirus, IPS, Web filtering, antispam, and VPN, along with advanced features such as an extreme threat database with automated updates, vulnerability management, and flow-based inspection to identify and mitigate the latest complex security threats. The FortiOS operating system was created to inspect and identify malware.

Features:
- NAT, PAT and Transparent (Bridge)
- Policy-Based NAT
- SIP/H.323/SCCP NAT Transversal
- VLAN Tagging (802.1Q)
- Vulnerability Management
- IPv6 Support

Control Model of Endpoint Accesses NAC
This model can enforce the use of security policies for users connecting to their corporate networks. This model verifies the installation, firewall operations and the update of antivirus signatures before allowing network access to new clients. It allows non-compliant servers who do not follow security policies to be quarantined.

Features:
- Monitoring and control of servers running FortiClient
- Vulnerability scanning of network nodes
- Quarantine portal
- Application detection and control
- Built-in application database

Antivirus / Antispyware model
Antivirus content inspection technology protects against viruses, spyware, worms, and other forms of malware which can infect network infrastructure and endpoint devices. By intercepting and inspecting traffic and level 7 content, antivirus protection ensures that malicious threats hidden within the application are identified and removed from data streams before they can cause any damage. A FortiGuard subscription service ensures that FortiGate devices are updated with the latest malware signatures for high levels of detection and mitigation.

Features:
- Automatic database updates
- Proxy-based antivirus
- Flow-based antivirus
- File quarantine
- IPv6 support

IPS Intrusion prevention model
IPS technology protects against current and emerging threats. In addition to signature-based threat detection, IPS carries out anomaly-based detection which alerts users to any traffic that matches attack behavior profiles. The Fortinet threat research team analyzes suspicious behavior, identifies and classifies emerging threats, and generates new signatures to include in FortiGuard's updates.

Features:
- Automatic database updates
- Protocol anomaly support
- IPS and DoS prevention sensor
- Custom signature support
- IPv6 support

WAN Optimization model
The goal of WAN optimization is to accelerate applications over geographically dispersed networks, while ensuring multi-threat inspection of all core network traffic. WAN optimization eliminates unnecessary and malicious traffic, optimizes legitimate traffic, and reduces the amount of bandwidth required to transmit data between applications and servers. Improved performance, reduced bandwidth and the consequent optimization of resources and infrastructure requirements allow for better control and therefore savings on associated expenses.

Features:
- Gateway-to-gateway optimization
- Bidirectional gateway-to-client optimization
- Web caching
- Secure tunnel
- Transparent mode

VPN Connection Management model
Fortinet VPN technology provides secure communications between multiple networks and hosts, using SSL and IPsec VPN technologies. FortiGate's VPN services are the ideal complement to complete content inspection, as well as protection and intrusion prevention in private areas of the network. This VPN connection management model allows QoS policies to be defined so that critical traffic profile communications traversing VPN tunnels can be prioritized.

Features:
- IPsec and VPN SSL
- DES, 3DES, AES and SHA-1/MD5 authentication
- PPTP, L2TP, VPN Pass Through
- SSL Single Sign-on
- Two-Factor Authentication

SSL-Encrypted Traffic Inspection model
SSL-encrypted traffic inspection protects endpoint clients and Web and application servers from hidden threats. SSL Inspection intercepts encrypted traffic and inspects it for threats before routing it to its final destination. It can be applied to client-oriented SSL traffic, such as users wishing to connect to a cloud-based CRM site, and to all inbound Web and application server traffic.
SSL inspection enables the enforcement of appropriate use policies on encrypted Web content and protects servers from threats which may be hidden inside encrypted traffic flows.

Features:
- Protocol support: HTTPS, SMTPS, POP3S, IMAPS
- Inspection support: Antivirus, Web Filtering, Antispam, Data loss prevention, SSL Offloaders

Data Loss Prevention model (DLP)
DLP uses a sophisticated pattern-matching engine to identify and prevent the transfer of sensitive information outside of the client's network perimeter, even when applications encrypt their communications. In addition to protecting your organization's critical data, Fortinet DLP provides audit trails to aid in policy compliance. Clients can select from a wide range of configurable actions to log, block, and archive data, and quarantine or ban users.

Features:
- Identification and control over data in motion
- Built-in pattern database
- RegEx based matching search engine
- Common file format inspection
- Various languages supported
- Flow-based DLP

Web filtering model
Web filtering protects servers, networks and sensitive information against Web-based threats by preventing users from accessing known phishing sites and sources of malware. In addition, administrators can enforce policies based on categories to easily prevent users from accessing inappropriate content and clogging networks with unwanted traffic.

Features:
- HTTP/HTTPS Filtering
- URL / Keyword / Phrase Block
- Blocks Java Applet, Cookies or Active X
- MIME content header filtering
- Flow-based Web filtering

High Availability model
ONI' and FortiGate's Advanced Firewall solution can be used in standalone mode or HA (High Availability) mode. High Availability (HA) configurations enhance reliability and increase performance by clustering multiple FortiGate appliances. FortiGate HA supports Active-Active and Active-Passive options to provide maximum flexibility. The HA feature is included as part of the FortiOS operating system.
- Active-Passive
- Stateful failover (FW and VPN)
- Links state monitor and failover
- Device failure detection and notification
- Server load balancing

Logging, reporting and monitoring
FortiGate's security devices provide extensive logging capabilities for traffic, systems, and network protection functions. They also allow details and graphical reports from detailed log information to be complied. These reports can provide historical and current analysis of network activity to help identify security issues and to prevent network misuse and abuse.

Features:
- Internal log storage and report generation
- Graphical real-time and historical monitoring
- Graphical report scheduling support
- Detailed graphical charts
- Optional FortiAnalyzer Logging (including per VDOM)
- Optional FortiGuard Analysis and Management Service

Application Control model
The application control model allows clients to enhance and optimize the management of security policies for thousands of applications running across networks, regardless of the port or protocol used for communication, thus optimizing the bandwidth use of each network.
The increase of Internet-based applications bombarding networks today make application control essential, as most application traffic looks like normal Web traffic to traditional firewalls.
Fortinet's application control provides granular control of applications along with traffic shaping capabilities and flow-based inspection options.

Features:
- Identifies and controls over 1,800 applications
- Traffic configuration (per application)
- Controls popular apps regardless of port or protocol
- Well-known applications include:
- AOL-IM
- ICQ
- WinNY
- Yahoo
- Gnutella
- Skype
- MSN
- BitTorrent
- eDonkey
- KaZaa
- MySpace
- Facebook
- Others

CONFIGURATION OPTIONS

FFortinet provides administrators with a variety of methods and wizards for configuring devices during installation. From an easy-to-use Web-based interface to the advanced capabilities of the command-line interface, the system offers the flexibility and simplicity that clients require.

Features:
- Web-based user interface
- Command line interface (CLI)

TECHNICAL FEATURES

FEATURES	ONI FG 200	ONI FG 400	ONI FG 600	ONI FG 700	ONI FG 800
Technical features					
vCPU (Min / Max)	1 / 1	1 / 1	1 / 2	1 / 4	1 / 8
RAM memory (Min / Max)	1GB / 2GB	1GB / 2GB	1GB / 4GB	1GB / 6GB	1GB / 12GB
Virtual Domains (vDOM)	1	10 / 10	10 / 25	10 / 50	10 / 250
Firewall policies (VDOM / System)	5.000	20.000 / 40.000	50.000 / 100.000	50.000 / 100.000	50.000 / 100.000
Unlimited user licenses	Yes	Yes	Yes	Yes	Yes
Performance					
Firewall Throughtput (VDP packets)	12Gbps	12 Gbps	15 Gbps	28 Gbps	33 Gbps
IPSec VPN Throughput (AES256+SHA1)	1 Gbps	1 Gbps	1.5 Gbps	3 Gbps	5.5 Gbps
IPS Throughput	3.5 Gbps / 1 Gbps	3.5 Gbps / 1 Gbps	5.5 Gbps / 1.5 Gbps	8 Gbps / 3 Gbps	15.5 Gbps / 6 Gbps
Antivirus Throughput	100 Mbps	200 Mbps	300 Mbps	350 Mbps	400 Mbps
Gateway-toGAteway IPSec VPN Tunnels (System / VDOM)	2.000	2.000	2.000	2.000	40.000
Client-to-Gateway IPSec VPN Tunnels	6.000	6.000	12.000	20.000	40.000
Concurrent sessions	1.0 Million	1.0 Million	2.6 Million	4.3 Million	8.5 Million
New sessions/Sec	85.000	85.000	100.000	125.000	150.000
VPN SSL concurrent users	1.000	1.000	2.000	4.500	10.000
VPN - SSL Throughput	800 Mbps	800 Mbps	830 Mbps	2 Gbps	4.5 Gbps