

Overview

Overview Fortinet positions themselves as a leading firewall vendor in the Unified Threat Management (UTM) market – their entry in the door is the UTM “hook”. Their ASIC-based appliance offerings range from low end at 50 Mbps firewall to high-end at 40+ Gbps and include multiple security services such as antivirus, firewall, IPSec and SSL VPN, IPS, Web filtering, and anti-spam– all running off of a single ASIC with CPU assist. All of these technologies are developed and managed in-house. Their product portfolio includes FortiManager and FortiLog for centralized management and reporting.

SSG Strengths

- **Integrated security and routing.**
 - Integrates LAN/WAN interfaces, protocols and encapsulations to deliver powerful option of consolidating multiple devices
 - Security zones, virtual routers and virtual LANs deliver granular segmentation capabilities to facilitate internal security by dividing the network into secure domains, each with its own security policy.
 - Provides significant opportunity to consolidate routing and security thereby reducing capital and operational costs
- **Flexible I/O options and supporting protocols.**
 - SSG 350M is a purpose-built platform with improved performance, modular memory, and a wider range of I/O options.
 - Supports five I/O expansion cards and modularity providing a wide range of WAN connectivity options including T1, E1, Sync Serial, ADSL/ADSL2/ADSL2+, G.SHDSL, and 100/1000 Ethernet SFP.
- **A complete set of Unified Threat Management (UTM) security features.** UTM features include stateful firewall, IPSec VPN, IPS, antivirus (includes anti-spyware, anti-adware, anti-phishing), anti-spam, and Web filtering.
- **Best-in-class UTM partners delivering key technology and support.**
 - Kaspersky for antivirus, anti-phishing, anti-spyware - #1 in catch rate testing
 - SurfControl / Websense for Web filtering - Top vendor in the Web filtering market
 - Symantec for anti-spam – Top vendor in the anti-spam market
- **VPN Resiliency.** Route-based VPNs leverage dynamic routing and VPN monitoring to deliver secure communications that are resilient to network failures.
- **High Availability:** SSG family can offer WAN redundancy across 2 firewalls, using virtual routers, and bridge group eliminating the need of external WAN router and switch.
- **Centralized management.** Multiple SSGs and all security, routing and UTM features can be managed centrally via the Juniper Networks Netscreen-Security Manager.
- **Complementary offerings.** Best-in-class complementary solutions including: SSL VPN, stateful firewall/VPN appliances, application acceleration, WAN acceleration, and enterprise class routers.

Fortinet Strengths

- A leader in the new Unified Threat Management (UTM) category as tracked by IDC. UTM is defined as any solution running FW, AV, and IPS and is billed as the next generation security appliance category.
- Strong SMB presence where all-in-one appliances are appealing to those customers.

Silver Bullets / Selling Tactics

- **Push the proven enterprise-class ScreenOS** features such as IPS (Deep Inspection), security zones, deployment modes and dynamic routing that have beaten FortiOS regularly
- **Emphasize modular WAN capabilities** that provide longer term investment protection and capacity to consolidate routing and firewall into a single device
- **Point out that Juniper SSG best-in-class components** are all from best-in-class partners – not home grown or public domain offerings. Fortinet’s home-grown components strain R&D, are not best-in-class. Every one of the security components (FW, IPS, VPN, SSL VPN, AV, Anti-Spam, etc., are developed internally, limiting their ability to stay innovative while placing significant strain on their R&D and support efforts.
- **Emphasize Juniper’s robust UTM offering compared to Fortinet’s limited, homegrown UTM capabilities**
 - SSG Antivirus has more than FOUR TIMES the virus coverage than Fortinet’s Anti-Malware database.
 - Antivirus Testing shows many viruses missed by Fortinet Antivirus (Viruses/Malware are easily evaded by the Fortinet Antivirus engine).
- **Lack advanced security features.** Fortinet offering is missing advanced security features such as Route-based VPN support and virtual routers. :
- **Better price performance** – it is up to 47% LESS costly than the FG 400A with similar functionality. The SSG 350M is priced at \$4500, while the FG 400A is priced at \$8495.

Juniper Networks SSG 350M vs. Fortinet FortiGate 400A Competitive Report Card

	Juniper Networks SSG 350M	Fortinet FortiGate 400A
Performance & Capacities		
FW Throughput (Large packets)	550+ Mbps	500 Mbps
FW Throughput (IMIX**)	500 Mbps*	500 Mbps
64 Byte Firewall Packets per second (PPS)	225,000	Not Published
3DES+SHA-1 IPsec VPN Throughput	225 Mbps	150 Mbps
Sessions	48K	400,000
Tunnels	350	2,000
Security Zones	40	Not Published
Stateful FW/VPN HA	Yes	FW only
Security applications		
IPS	Yes	Yes
Integrated Antivirus	Yes	Yes
Adware / Spyware / Keylogger protection	Yes (included at no charge in AV engine)	Yes
Integrated Web Filtering	Yes	Yes
Redirect Web Filtering	Yes	No
Integrated Anti-Spam	Yes	Yes
SSL VPN	Not supported	Yes
Interfaces and Routing		
Fixed interfaces	4 10/100/1000	2CG + 8FE
I/O expansion slots	6	Not supported
Additional I/O options	SFP, 10/100/100, Serial, T1/E1, ADSL2+, G.SHDSL	Not supported
Console/Aux port	Yes	Yes
LAN/WAN Routing	RIPv1/2, OSPF, BGP, Frame Relay, Multilink Frame Relay, PPP, Multilink PPP, HDLC	RIPv1/2, OSPF, BGP
Virtual routers	5	Not supported
VLANs	125	Yes
VoIP termination	Not supported	Not supported
VoIP security	SIP, H.323, MGCP, SCCP	SIP, H.323
QoS	Traffic shaping	Traffic shaping
Price	\$4,500	\$9,995

* IMIX traffic is more demanding than a single packet size performance test and as such is more representative of real-world customer network traffic. The IMIX traffic used is made up of 58.33% 64 byte packets + 33.33% 570 byte packets + 8.33% 1518 byte packets of UDP traffic.

Key Features Comparison ScreenOS 6.0 v FortiOS 3.0

Key Feature/Point	Juniper Networks SSG Family	Fortinet	Why it Matters
LAN and WAN connectivity	LAN and WAN I/O options plus supporting protocols and encapsulations provide unmatched connectivity flexibility in the mid range market	No WAN hardware or encapsulation support whatsoever – limited LAN hardware	Customers are want the ability to extend the investment protection as they move toward next generation networks (broadband, metro Ethernet)
Integrated security policy, network and device level management	Integrated security management for firewall, VPN, NAT, Traffic Management Security policy, network, and device level management and monitoring	Integrated security management for firewall, VPN, NAT, Traffic Management Security policy, network, and device level management and monitoring	To maintain a reasonable administrative cost structure, device management in outlying offices must be easy to perform and consistent in all aspects

**Competitive HotSheet:
Juniper Networks SSG 350M vs. Fortinet FortiGate 400A**



Security zone Architecture	Security zones provide ability to enforce security via logical group functions (i.e. Marketing, Finance, etc) as opposed to specific IP subnets or addresses	Limited zone creation capability	Segmenting the network in a logical, easy to configure and manage manner is critical to protect internal resources from attacks and/or unauthorized use/access
Dynamic Routing Protocol support	Full Supports of RIP v1/2, OSPF and BGP	Hastily implemented and lack of important security features e.g. encrypt OSPF over GRE or IPSec tunnel.	Eases integration of security into existing networks
Dynamic Route based VPN	With multiple VPN tunnels defined to a given location, routing protocols will ensure that the optimal tunnel will be used for traffic dynamically	FortiOS does not offer route based VPN – Policy based VPNs cannot leverage dynamic routing protocols to ease deployment of large hub and spoke deployments.	Outlying offices need maximum reliability at all levels – device, as well as link layer – dynamic route-based VPNs provide this level of resiliency.
Virtual Routers	Support overlapping IP address space and provide greater security than a shared router instance for both trusted and untrusted networks	Not supported.	Isolates and separates public and private IP address for greater security than a shared router
802.1q Virtual LANs	Use VLANs as an alternative means of routing traffic to destination	Use VLANs as an alternative means of routing traffic to destination	Provides another mechanism to route traffic to appropriate security zone
Stateful High Availability for Firewall and VPN	Stateful, sub-second failover for VPN and firewall Warm standby HA on NetScreen-25 Important for central site deployment	High Availability is stateful only for firewall sessions. VPN IKE tunnels must be renegotiated from scratch = downtime	Stateful failover for VPN at remote sites is critical to continued business operations
Traffic Management	Optimize bandwidth on a per-policy basis for specific application and specific tunnels. Supports DSCP marking	No support for DSCP	Able to prioritize application traffic such as VoIP
VoIP	ScreenOS supports ALG for all major VoIP protocols – SIP, MGCP, H.323 (including Avaya extension) and SGCP. ScreenOS also supports all of the major call flows in each protocol – call transfer, conference calls, etc.	FortiOS does not have explicit ALG functions. Instead, one has to build specific policy to support SIP and H.323 traffic. There is no explanation on call flows that is supported by their ALG.	ALGs are back-to-back user agents that can dynamically open and close firewall pinholes to maintain security. ALGs designed specifically to handle demanding applications like VoIP can prevent malicious attacks on VoIP and other systems, as well as prevent severe system outages triggered by malfunctioning VoIP devices.
Antivirus support	Optional File-based Kaspersky antivirus engine and database that can stop viruses, Spyware, adware from penetrating the network User configurable scanning at 3 levels allows user to tailor protection to needs.	Homegrown AV looks only at the wild list.	Kaspersky is a best-in-class vendor, ranking #2 in most market assessments.

Key Feature/Point	Juniper Networks SSG Family	Fortinet	Why it Matters
Anti-Spam support	Optional Anti-Spam solution from Symantec provides best in class gateway-based spam prevention	Anti-Spam uses public domain real-time black lists (RBL) which can be unreliable when used in production	SPAMMERS will commonly change their addresses so using a public domain offering as opposed to a best-in-class offering will provide false sense of security

**Competitive HotSheet:
Juniper Networks SSG 350M vs. Fortinet FortiGate 400A**



Denial of Service protections (prevention)	DoS protections, per interface and configurable per zone	DoS protections applied uniformly (not configurable per interface) on up to 4 interfaces	Per policy management delivers the optimum level of control over network attacks.
Application level attack protection	Deep Inspection application-level attack prevention both Stateful signature and protocol anomaly based Per policy configuration	IPS is snort-like signature-based only. No dedicated IPS (IDP) capability	Stateful signatures and protocol anomalies provide greater accuracy
Web filtering	Integrated Web Filtering option with SurfControl option on NetScreen-HSC up through SSG 500 Series Websense and Surfcontrol redirect support across product line	Uses a homegrown URL filtering	Flexible, best-in-class offerings provide optimum protection.

Fortinet FortiOS 3.0 Assessment

Based on preliminary feedback, the FortiOS 3.0 brings new enterprise and management features, most of which have already been field proven in ScreenOS for several years.

New FortiOS 3.0 Feature	ScreenOS Support?
IM Security – able to stop users from using IM and P2P	ScreenOS can block P2P and IM via Deep Inspection. If companies want to allow employees the ability to use or deny use of key pieces of IM they can do so. Deep Inspection is more granular in its control capability and can allow users to use chat while blocking file transfer – a common attack vector.
IM Logging – it is unclear what this means. It could mean logging the entire message or merely logging the “act” of IM.	ScreenOS can log the preceding and following packets as well as the activity. ScreenOS cannot log the entire message content.
Active Directory Integration	ScreenOS can integrate with AD via Webauth (radius or LDAP) and via FW auth.
Network redundancy – 802.3 AD Link Aggregation	ScreenOS supports this feature already. In addition to the “Redundant Interface” features for enhanced physical link resiliency.
BGP and PIM	BGP and multicast support (PIM) added to ScreenOS 2 years ago
Virtual HA	ScreenOS supports this via virtual systems and HA.