

Overview

The Fortigate 224B is a fixed configuration firewall appliance that represents Fortinet’s first attempt at a network access control (NAC) product. Fortinet positions themselves as an AV firewall vendor – their entry in the door is the AV “hook”. Their ASIC-based appliance offerings range from low end at 50 Mbps FW to high-end at 40+Gbps and include nearly every security technology possible: AV, FW, VPN, SSL VPN, Web filtering, Anti-Spam, IPS, and now some NAC– 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. The Juniper SSG 140 competes with the FG-224B.

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 by IDC as the next generation security appliance category.
- Strong SMB presence where all-in-one appliances are appealing to those customers.

Juniper SSG 140 Strengths

- **The SSG 140 is a new, purpose-built platform** with improved performance, modular memory, and a wider range of I/O options (see I/O comparison table). Provides significant opportunity to consolidate routing and security thereby reducing capital and operational costs.
 - Fortinet implements their ASIC on an OEM platform from either Portwell or Diversified Technologies (FG5000 series only). This limits the amount of innovation they can implement in order to maximize performance.
- **Flexible I/O options and supporting protocols.** The SSG 140 delivers tremendous flexibility through its 10 fixed interfaces and 4 I/O expansion slots – all of which are supported by LAN protocols and WAN encapsulations. None of the Fortinet small office firewalls provide any modular I/O flexibility.
- **Highest interface density in its class.** With 10 fixed interfaces (8 10/100 + 2 10/100/1000) and 4 interface slots, the SSG delivers the highest interface density in its class.
 - **Lowest cost Gb Ethernet.** No other competitive platform in its class delivers Gb connectivity.
 - **Highest number of I/O expansion slots in its class.** Only FW platform with 4 I/O expansion slots.
- **Integrated security and routing.** The SSG delivers best-in-class security, LAN/WAN interfaces, protocols and encapsulations to deliver powerful option of consolidating multiple devices (FW, Router, Etc).
 - **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 AV/AntiPhishing, Antispyware – West Coast Labs reports Juniper with 99.8% catch-rate vs. Fortinet at 66% (West Coast Labs, November 2006)

Test Results Summary table

Test	Test Description	Malware samples	Juniper AV Engine Detection rate	Fortinet AV Engine Detection rate
Test 1	Wild List	656	656 - 100%	654 - 99.7%
Test 2	Checkmark Anti-Spyware	1011	1008 - 99.7%	767 - 75.8%
Test 3	Checkmark Trojan	445	444 - 99.8%	87 - 19.5%
Test 4	Recently Harvested Spyware	22	22 - 100%	14 - 63.6%
Test 5	Recently Harvested Viruses & Worms	4	4 - 100%	4 - 100%
Test 7	False Positives*	(1362)	0 - 100%	0 - 100%
Test 8	Polymorphic Viruses	200	200 - 100%	23 - 11.5%
Total malware		2,338	2334 - 99.82%	1549 - 66.25%

*100% record - 0% false positive detection

- SurfControl and Websense for Web filtering - Top vendors in the Web Filtering market
 - Symantec for Anti Spam – Leading Anti-Spam Vendor
- **Proven advanced security features.** 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.
 - **VPN Resiliency.** Route-based VPNs leverage dynamic routing and VPN monitoring to deliver secure communications that are resilient to network failures.

- **Centralized management.** Multiple SSGs and all security, routing and UTM features, can be managed centrally via NSM.
- **Complementary offerings.** Best-in-class complementary solutions including: SSL VPN, FW/VPN appliances, application acceleration, and enterprise class routers.

Deployment Comparison

Juniper provides a wider range of deployment options from which to choose.

Deployment Scenario	Juniper Networks SSG 140	Fortinet FG-224B
FW / VPN	Yes	Yes
FW / VPN (HA)	Yes	No
FW / VPN with UTM	Yes	Yes
Secure Router	Yes	No (No WAN requires external router)
Secure Router with UTM	Yes	No (No WAN requires external router)
Network admission control	Yes (UAC)	Yes (Limited)
FW / VPN	Yes	Yes

I/O Comparison

Juniper provides a wider range of I/O options from which to choose.

Connectivity Requirement	Juniper Networks SSG 140	Fortinet FG-224B
Fast Ethernet (10/100)	8 x 10/100	24 x 10/100 LAN, 2 x 10/100 WAN
Gb Ethernet (10/100/1000)	2 x 10/100/1000	2 x 10/100/1000
Interface expansion slots	4	Not supported
• T1 Interface Module	2 x T1	Not supported
• E1 Interface Module	2 x E1	Not supported
• Serial Interface Module	2 x Serial	Not supported
• ISDN BRI S/T Interface Module	1 x ISDN BRI S/T	Not supported
• ADSL/2/2+ Interface Modules	1 x ADSL Annex A or B	Not supported
• 4-Wire G.SHDSL Module	1 x 4-Wire G.SHDSL	Not supported
• 6-Port SFP GigE Interface Module	6 x 10/100/1000	Not supported
• 8-Port Copper GigE Interface Module	8 x 10/100/1000	Not supported
• 16-Port Copper GigE Interface Module	16 x 10/100/1000	Not supported

Competing with UTM and NAC features from Fortinet

Fortinet will push Unified Threat Management (UTM) capabilities as the key differentiator to their platform. It is important to look at how the features are developed, implemented and supported.

Fortinet develops and supports ALL of their UTM features INTERNALLY – with only ~650 employees company wide, this places significant strain on their product development and support capabilities. The result is sub-par Fortinet product capability and quality of all UTM features. Juniper is already recognized as the industry leader for firewall, IP Sec VPN, SSL VPN, and IDP. Juniper is the only vendor on the market that partners with Best-In-Class UTM vendors.

- Kaspersky for AV/AntiPhishing, Antispyware – consistently rated #1 in catch testing
- SurfControl and Websense for Web filtering -- Two top vendors in the Web Filtering market
- Symantec for Anti Spam – Leading Anti-Spam Vendor

This means that Juniper has both the best in class technical solution and the best in class support of hundreds of dedicated engineers who are developing and deploying best in class threat management solutions every day.

	ScreenOS	FortiOS
Anti-virus	<ul style="list-style-type: none"> • Juniper partners with Kaspersky, one of the top 3 AV vendors on the market. • Proven records for virus signature updates. 	<ul style="list-style-type: none"> • Home grown virus signature database limited to only the Wild list • No track record for response time in the event of a new virus outbreak. • Does not protect users against virus embedded in webmail and malicious / fictitious news groups servers.
Anti-spam	<ul style="list-style-type: none"> • Partner with prominent anti-spam solution provider – Symantec to filter spam. • Symantec worldwide NOC monitoring spam activities and updating servers. Spam database is updated every 10-15 minutes. • Track open proxies, relays...etc to stop source of spam. 	<ul style="list-style-type: none"> • Home grown spam services (FortiGuard) server. • Based on DNSBL /ORDBL to filter spam -- prone to spoofing and bias of DNS authors.
Web filtering	<ul style="list-style-type: none"> • Juniper partners with the #1 and #2 vendors on the market • Integrated SurfControl engine. • Traffic can also be redirected to external SurfControl or Websense servers. • Malicious URL protecting feature. • Full interpretability to WebTrends servers - system administrator can get crucial information such as bandwidth and security analysis as well as monitor internet usage. 	<ul style="list-style-type: none"> • Internally developed and maintained solution • Filter based on black / white URL list and keywords -- lacks of sophistication. • Servers (FortiGuard) hosted by Fortinet – no track record on server reliability and accuracy.
IPS	<ul style="list-style-type: none"> • Proven best in class capabilities • Multiple levels of threat severities. • Build in brute force protection; system administrator can define corrective actions under attacks. • Easy to manage (adding and removing) IPS signatures base on threat level. • Protect against spyware, adware and keylogger. 	<ul style="list-style-type: none"> • Poor management interfaces. One has to go down to each service category (e.g., telnet, ftp) and examine current value before changes can be made. • IPS signatures do not indicate threat level. Administrator can be mislead and apply incorrect level (information vs. critical) threat coverage. • IPS is snort-like signature-based only. • Not configurable per-policy, but system wide.
NAC	<ul style="list-style-type: none"> • Juniper Networks Unified Access Control solution combines user identity and device security state information with network location information, to create a unique access control policy for each user. The solution can be enabled at Layer 2, using 802.1X, or at Layer 3 using an overlay deployment. UAC 2.0 can also be provisioned in mixed mode, using 802.1X for network admission control and Layer 3 for resource access control. 	<ul style="list-style-type: none"> • FG 224B is Fortinet's first product that supports NAC-like features. There is no tracking record on either the NAC functions or any live Fortinet NAC deployment. There are no other Fortinet products to support NAC (e.g., policy enforcer).

Performance and Price

The Juniper SSG 140 offers significant performance and price advantages over the Fortinet FG-224B.

	Juniper SSG 140	FG-224B
Sessions per Second	8000 sessions per second	4000 sessions per second
Firewall Performance	350Mbs	150Mbs
IPSec VPN Performance	100Mbs	70Mbs
UTM (AV) Performance	40+ Mbs	30Mbs
Price (USD)	\$2,700 - \$3,200	\$5,215

Key Feature Comparison

	SSG 140 (ScreenOS 5.4)	FG-224B/FG300A (FortiOS 3.0)
LAN Interface Density	8 x 10/100 with 2 x 10/100/1000 onboard, plus up to 32 additional 10/100/1000 ports with interface modules	24 x 10/100 with 2 x 10/100/1000. If there are more than 24 clients, an additional Fortigate 224B or Ethernet switch is required, creating a multiple-box solution where an administrator has to be proficient with router and firewall (and potentially an Ethernet switch) configuration and maintenance
WAN options – field upgradeable	SSG 140 has 4 expansion slots that support 2xT1, 2xE1, 1xISDN BRI S/T, and 2xSerial I/O cards	Not supported
WAN Encapsulations	SSG 140 supports PPP, FR and HDLC as well as WAN aggregation across MLPPP, and MLFR	PPPoE, 802.3 supported only on two Ethernet WAN interfaces
NAT and Transparent mode	ScreenOS allows one to define each interface operates in either route or NAT mode.	FortiOS has a system-wide global configuration for the entire system to be in either NAT or transparent mode.
Routing protocols	Full support for OSPF, BGP, RIPv1/2	Hastily implemented and lack a lot of important security related features, e.g., encrypt OSPF over GRE or IPSec tunnel.
Extended Access Control lists	Extended ACL lists allow source IP/port range (TCP, UDP or icmp), destination IP/port range and TOS value to be examined. System administrator can use the ACL to create route or system-wide policy on process (drop or pass) traffic.	FortiOS can only use source / destination IP address and destination port to make policy based routing decisions.
VPN – Dynamic route based	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 VPN's cannot leverage dynamic routing protocols to ease the deployment of large hub and spoke VPN deployments
Virtual Routers	Virtual routers, each with their own address table, delivers separate routing domains to manage public/private IP addresses	Not supported.
VPN – tunnel creation	ScreenOS allows users to establish tunnel from either remote site or HQ site	VPN can only be created from Internal or DMZ to the External interface on FortiOS
VPN - stateful failover	Supported in Active/Passive or Active/Active	Not supported
VPN - Traffic mgmt	Per policy traffic management allows IPSec VPN to be given greater weight (more BW).	All IPSEC traffic have same priority.
VPN Monitoring	ScreenOS offers VPN group or monitoring function to maintain availability of VPN tunnels.	Not supported
VoIP	ScreenOS supports ALG for all major VoIP protocols – SIP, MGCP, H.323 (incl. Avaya extension) and SCCP. 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

QoS	<p>ScreenOS allows system administrator to “condition” the DSCP value of ingress and egress packets. This will allow Juniper firewall to make proper DSCP value marking on packets toward to up-stream / down-stream next hop devices.</p> <p>Juniper allows traffic shaping on each policy. In addition, ScreenOS permits one to set the max ingress / egress bandwidth on each Ethernet interface.</p>	<p>Traffic shaping is only supported on per policy. The algorithm runs in software and is very volatile as it is not a memory or CPU protected procedure and the entire operation of the unit is effected.</p>
Redundancy and backup mode	<p>ScreenOS allows multiple IP addresses with different weight to be tracked. Therefore, one can define policy so that redundant interface in the same zone will kick-in if one or more IP failed to response. ScreenOS allows different type of interfaces – WAN, Ethernet or modem in same zone for backup purpose.</p>	<p>Fortigate only permits modem to be part of dial-back solution. It also does not allow more than one IP addresses to be tracked.</p>
Centralized management	<p>NSM delivers powerful centralized management including templates, rapid deployment and granular logging and reporting.</p>	<p>FortiManager is unstable, lacking key features for large scale deployments, resulting in loss of many big sales.</p>
Real time monitoring	<p>All platforms provide complete logging visibility or export to a 3rd party server for more analysis.</p>	<p>Does not allow one to view the system log in real-time, on-screen format. System administrator has to use FortiAnalyzer, memory (to play back) or syslog server to view the operation status.</p>
Memory upgrade	<p>SSG 140 comes with 256MB RAM and can be upgraded in the field to 512MB</p>	<p>Not supported</p>