SONICWALL

Network Security. 10 Things a Cisco ASA Can't Do

SC MAGAZINE RECOMMENDED

"If you've considered SonicWALL before and didn't take the plunge, now is the time."

Read SC Magazine's article on NSA 240

Top Things the Cisco ASA Can't Do for Your Customers That SonicWALL Will

1. **No 802.11n Wireless** – 802.11g is the fastest you'll get with the Cisco ASAs
2. **No Integrated Deep Packet Inspection** – ASAs require additional IPS and Gateway AV hardware modules
3. **No 3G Wireless Failover** – USB-based 3G is not an option on Cisco ASAs
4. **No Application Intelligence and Control** – No application level bandwidth control and blocking on Cisco ASAs
5. **Limited File Size and Port Scanning** – ASAs are extremely limited; SonicWALLs aren't
6. **No Outbound Malware Blocking** – ASAs only do inbound DPI (when they have a module)
7. **No Clean VPN** – No scanning of threats over IPSec/SSL VPN connections with Cisco ASAs
8. **No Desktop Anti-Virus** – Infected endpoints can connect to the corporate LAN
9. **No Onboard Comprehensive Anti-Spam** – ASAs require an additional hardware module for Anti-Spam
10. **Limited Protocol Inspection** – ASAs select protocols to scan; SonicWALLs scan everything

Selling SonicWALL is easy! Simply match up the Cisco ASA with the corresponding SonicWALL.

If you were selling this Cisco ASA	Now sell this SonicWALL	Part Number
Cisco ASA 5505	SonicWALL TZ 210/TZ 210 Wireless-N SonicWALL NSA 240	01-SSC-8753/01-SSC-8754 01-SSC-8756
Cisco ASA 5510	SonicWALL NSA 2400/2400MX SonicWALL NSA 3500	01-SSC-7020/01-SSC-7100 01-SSC-7016
Cisco ASA 5520	SonicWALL NSA 4500	01-SSC-7012
Cisco ASA 5540	SonicWALL NSA 4500 SonicWALL E-Class NSA E5500 SonicWALL E-Class NSA E6500 SonicWALL E-Class NSA E7500	01-SSC-7012 01-SSC-7008 01-SSC-7004 01-SSC-7000
Cisco ASA 5550	SonicWALL E-Class NSA E5500 SonicWALL E-Class NSA E6500 SonicWALL E-Class NSA E7500	01-SSC-7008 01-SSC-7004 01-SSC-7000

Contact Information

Name:______________________ Phone:______________________ Email:______________________

Learn more at www.sonicwall.com/asareplacement

SONICWALL

10 Things a WatchGuard XTM Firewall Won’t Do for Your Customers

NSA E7500: ★★★★★

“The SonicWALL E-Class Network Security Appliance is a high performance, highly configurable, super UTM”

Read SC Magazine’s article on the NSA E7500

Top 10 Things the WatchGuard XTM Won’t Do for Your Customers That a SonicWALL Will

1. **Limited File Size and Port Scanning** – XTMs can’t scan files greater than 20 MB; SonicWALLs can
2. **Poor UTM Performance** – Testing using Ixia IxLoad showed a substantial loss in performance on tested XTMs running Gateway AV and IPS; SonicWALL showed no degradation
3. **No Application Intelligence and Control** – No application level bandwidth control and blocking on XTMs
4. **Costly Anti-Spam Installation** – SpamBlocker must be installed on a separate server; SonicWALL Comprehensive Anti-Spam Service is run directly on the firewall
5. **Minimal Protocol Inspection** – XTMs scan only 7 protocols and scanning on non-standard ports requires each port to be configured separately as a new rule; SonicWALLs scan everything
6. **Limited Distributed Wireless** – Only the XTM 2 Series integrates wireless and no XTMs support WLAN access points; All SonicWALLs support and/or integrate 802.11n wireless
7. **No Enforced Client or Server AV Support** – Unlike SonicWALL Enforced Client/Server AV, WatchGuard’s client and server AV solutions are not gateway enforced
8. **Advanced Features Cost More** – Over half of the XTM models require the Fireware Pro upgrade for advanced OS features; SonicOS includes every feature
9. **Lack In-house UTM Expertise** – XTMs rely on 3rd parties for Gateway AV, IPS, Anti-Spam and Content Filtering
10. **Increased Management and Cost for 3G Wireless** – XTMs can’t run onboard 3G wireless without purchasing an extra device

***Disclaimer**: Statements contained in this document are based on publicly available information as of September 8, 2010*

Selling a SonicWALL is easy! Simply match up the WatchGuard XTM with the corresponding SonicWALL

If You Were Selling This WatchGuard XTM	Now sell this SonicWALL	Part Number
WatchGuard XTM 21/21-W	SonicWALL TZ 100/TZ 100 Wireless-N	01-SSC-8734/01-SSC-8735
WatchGuard XTM 22/22-W	SonicWALL TZ 200/TZ 200 Wireless-N	01-SSC-8741/01-SSC-8742
WatchGuard XTM 23/23-W	SonicWALL TZ 210/TZ 210 Wireless-N	01-SSC-8753/01-SSC-8754
WatchGuard XTM 505	SonicWALL NSA 240	01-SSC-8756
WatchGuard XTM 510	SonicWALL NSA 2400/2400MX	01-SSC-7020/01-SSC-7100
WatchGuard XTM 520	SonicWALL NSA 3500	01-SSC-7016
WatchGuard XTM 530	SonicWALL NSA 4500	01-SSC-7012
WatchGuard XTM 810	SonicWALL E-Class NSA E5500	01-SSC-7008
WatchGuard XTM 820	SonicWALL E-Class NSA E6500	01-SSC-7004
WatchGuard XTM 830	SonicWALL E-Class NSA E7500	01-SSC-7000
WatchGuard XTM 1050	SonicWALL E-Class NSA E8500	01-SSC-8953

Since 1991, SonicWALL is an industry-recognized worldwide leader in network security. With over 1.4 million appliances deployed, SonicWALL protects over 20 million people from malware, intrusions, spyware, spam every day.

Take a Test Drive Today by visiting http://livedemo.sonicwall.com/livedemo.html

SONICWALL

10 Limitations a Fortinet FortiGate Firewall Has That a SonicWALL Doesn't

NSA E7500: ★★★★★

"The SonicWALL E-Class Network Security Appliance is a high performance, highly configurable, super UTM"

Read SC Magazine's article on the NSA E7500

Top 10 Limitations a Fortinet FortiGate Has That Your Customers Should Know About

1. **Limited Proxy-based AV Scanning** – FortiGates using proxy-based AV scanning have file size limitations and performance-limiting intellectual property and hardware. Files larger than the buffer are passed without being scanned or are blocked. SonicWALLs have no such file size limitations.

2. **Basic Application Management** – SonicWALL's running SonicOS 5.6.4 and later with Application Intelligence, Control and Visualization provide a comprehensive set of application management capabilities. FortiGates are limited to very basic allow, block and log. Also, SonicWALLs have 3x as many application signatures as FortiGates.

3. **Inadequate File and Protocol Scanning** – FortiGates scan only a portion of each file for malware across just 11 protocols. SonicWALLs scan the entire file over 50+ protocols.

4. **Poor Distributed Wireless Functionality** – FortiWiFis offer few wireless features. SonicWALLs provide many more such as Lightweight Hotspot Messaging, Wireless Guest Services and others.

5. **Costly Central Management** – Customers need to purchase and run FortiManager and FortiAnalyzer together to get the equivalent features of SonicWALL GMS.

6. **No IPv6 or ICSA Enterprise Firewall Certification** – While FortiGates may support IPv6, SonicWALL NSA and E-Class NSA Series appliances are IPv6 certified. In addition, SonicWALL is the first network security vendor to receive ICSA Enterprise Firewall certification. Fortinet products have no such certification.

7. **Lack L2TP Server Support for Handheld Devices** – FortiGates lack L2TP Server, so handhelds are unable to connect to the firewall. SonicWALLs include built-in L2TP Server.

8. **One-way Anti-Spyware Protection** – FortiGates monitor only inbound traffic for spyware, not outbound. SonicWALLs monitor and block spyware in both directions.

9. **Restricted 3G Availability** – Only low-end FortiGates (80 Series and below) have 3G wireless WAN failover. SonicWALL includes 3G across all firewall lines.

10. **Poor Anti-Spam Options** – The FortiGate email filter service is limited to three dynamically-updated techniques (IP Reputation, Message body URL check and Message body content signatures). SonicWALL Comprehensive Anti-Spam Service utilizes 3x as many techniques including those.

***Disclaimer**: Statements contained in this document are based on publicly available information as of December 2, 2010*

If You Were Selling This Fortinet FortiGate	Now sell this SonicWALL	Part Number
FortiGate-30B/FortWifi-30B FortiGate-50B/FortWifi-50B	SonicWALL TZ 100/TZ 100 Wireless-N	01-SSC-8734/01-SSC-8735
FortiGate-60C/FortWifi-60C	SonicWALL TZ 200/TZ 200 Wireless-N	01-SSC-8741/01-SSC-8742
FortiGate-80CM/FortWifi-80CM FortiGate 110B/111B	SonicWALL TZ 210/TZ 210 Wireless-N	01-SSC-8753/01-SSC-8754
FortiGate 200B FortiGate 300A FortiGate 311B FortiGate 800	SonicWALL NSA 2400MX SonicWALL NSA 240/NSA 2400 SonicWALL NSA 3500 SonicWALL NSA 4500	01-SSC-7100 01-SSC-8756/01-SSC-7020 01-SSC-7016 01-SSC-7012
FortiGate 1000A FortiGate 3016B FortiGate 3600A	SonicWALL E-Class NSA E5500 SonicWALL E-Class NSA E6500 SonicWALL E-Class NSA E7500	01-SSC-7008 01-SSC-7004 01-SSC-7000
FortiGate 3810A	SonicWALL E-Class NSA E8500	01-SSC-8953

Established in 1991, SonicWALL is an industry-recognized worldwide leader in network security. With over 1.4 million appliances deployed, SonicWALL protects over 20 million people from malware, intrusions, spyware, and spam every day.

Take a Test Drive Today by visiting http://livedemo.sonicwall.com/livedemo.html

Network Security. 10 Things a Juniper SRX Can't Do

> "If you've considered SonicWALL before and didn't take the plunge, now is the time."
>
> *Read SC Magazine's article on the NSA 240*

Top Things the Juniper SRX Can't Do for Your Customers That a SonicWALL Will

1. **Limited File Size Scanning for UTM** – SRXs can't scan files greater than 20 MB, so Juniper lets malware THROUGH in large files or blocks good content. SonicWALL scans EVERYTHING!

2. **Lacks Ease-of-Use** – No configuration wizards with SRXs, and customers will need to understand the CLI to enable certain features

3. **No Application Intelligence and Control** – No application identification, bandwidth control or blocking is available on Juniper Branch SRXs

4. **No SSL VPN or Virtual Assist** – SRXs don't provide an option for SSL VPN or Virtual Assist

5. **UTM Restrictions** – UTM is only available on high-memory SRX models; others require an expensive memory upgrade to run UTM

6. **Limited Distributed Wireless** – Only three SRXs support WLAN access points; All SonicWALLs support and/or integrate 802.11n wireless

7. **No Clean VPN** – No scanning of threats over IPSec/SSL VPN connections with Juniper SRXs

8. **Minimal Protocol Inspection** – SRXs scan only 5 protocols; SonicWALLs scan everything

9. **Lack UTM In-house Expertise** – SRXs rely on 3rd parties for Gateway AV, Anti-Spyware, Anti-Spam and CFS

10. **3G Wireless Interfaces** – Only one SRX has a built-in 3G interface; Others require additional hardware

***Disclaimer**: Statements contained in this document are based on publicly available information as of May 20, 2010*

Selling SonicWALL is easy! Simply match up the Juniper SRX with the corresponding SonicWALL.

SonicWALL is the better channel choice.

Note: Juniper has entered into an OEM agreement with DELL to private label the SRX, MX, EX and JUNOS software product lines. Read More

If you were selling this Juniper SRX	Now sell this SonicWALL	Part Number
Juniper SRX100	SonicWALL TZ 210/TZ 210 Wireless-N SonicWALL NSA 240	01-SSC-8753/01-SSC-8754 01-SSC-8756
Juniper SRX210	SonicWALL NSA 240 SonicWALL NSA 2400/2400MX	01-SSC-8756 01-SSC-7020/01-SSC-7100
Juniper SRX240	SonicWALL NSA 3500	01-SSC-7016
Juniper SRX650	SonicWALL E-Class NSA E5500 SonicWALL E-Class NSA E6500 SonicWALL E-Class NSA E7500	01-SSC-7008 01-SSC-7004 01-SSC-7000
Juniper SRX3400	SonicWALL E-Class NSA E7500	01-SSC-7000

Contact Information

Name:______________________ Phone:______________________ Email:______________________

SONICWALL

Network Security. 10 Things a Palo Alto Networks Firewall Can't Do

SC MAGAZINE RECOMMENDED

"If you've considered SonicWALL before and didn't take the plunge, now is the time."

Read SC Magazine's article on the NSA 240

Top Things a Palo Alto Networks (PAN) Firewall Can't Do for Your Customers That a SonicWALL Can

1. **Limited File Size and Port Scanning** – PAN firewalls can't scan all files sizes for each of their supported protocols; SonicWALLs can!
2. **Minimal Protocol Inspection** – PAN firewalls scan only 6 protocols; SonicWALLs scan everything
3. **Lack UTM In-house Expertise** – PAN firewalls rely on third parties for Gateway AV, Anti-Spyware, Anti-Spam and CFS
4. **No 3G Wireless Failover –** USB-based 3G is not an option on PAN firewalls
5. **Limited Application Identification** – PAN firewalls can only identify certain application types; SonicWALL can identify ANY application
6. **Poor Price Performance** – For the same price point SonicWALL offers 10x the performance of PAN firewalls
7. **No Onboard Comprehensive Anti-Spam** – PAN firewalls don't block spam. SonicWALLs offer Anti-Spam protection as a service or with our enterprise-class Email Security virtual appliance
8. **No Endpoint Enforcement** – SonicWALLs have the ability to enforce and scan clients at the desktop level; PAN firewalls don't
9. **Poor WiFi Security** – SonicWALLs can control hundreds of virtual WAPs while providing application intelligence and control to the WIFI edge; PAN firewalls can't
10. **No Traffic Monitoring Integration** – PAN firewalls don't integrate with industry-standard traffic monitoring protocols like NetFlow; SonicWALLs do

***Disclaimer**: Statements contained in this document are based on publicly available information as of July 12, 2010*

Selling a SonicWALL is easy! Simply match up the Palo Alto Networks firewall with the corresponding SonicWALL

If you were selling PAN Firewall	Now sell this SonicWALL	Part Number
Palo Alto Networks PA-500	SonicWALL NSA 3500	01-SSC-7016
Palo Alto Networks PA-2020	SonicWALL NSA 4500	01-SSC-7012
Palo Alto Networks PA-2050	SonicWALL NSA E5500	01-SSC-7008
Palo Alto Networks PA-4020	SonicWALL E-Class NSA E6500 SonicWALL E-Class NSA E7500	01-SSC-7004 01-SSC-7000
Palo Alto Networks PA-4050	SonicWALL E-Class NSA E7500 SonicWALL E-Class NSA E8500	01-SSC-7000 01-SSC-8866

Contact Information

Name:________________ Phone:________________ Email:________________