SONICWALL™

A Massively Scalable Approach to Network Security

A super massively scalable network firewall that delivers strong performance and security at a low TCO

Abstract

As network security requirements have evolved, traffic has increased, and 40 Gbps and higher core networking technologies have been more widely adopted, the response by many organizations has been to scale up their hardware to continue to meet their performance requirements. However, this strategy is proving unsustainable. A growing number of complex and power-hungry virtualized systems increases both capital and operating expenses (CapEx and OpEx), while increasing the impact of failures and providing a single attack point for denial-of-service attacks and other firewall evasion techniques.

This document offers a better approach: a network-based model for scaling a next-generation firewall (NGFW) to approach or surpass existing or forthcoming solutions for enterprise network security — while providing better performance, increased resiliency and lower total cost of ownership (TCO).

Introduction

Devices don't have to be massive to scale massively

To meet modern security requirements, many network security architectures require increasingly massive processing capacity — resulting in larger and larger platforms that consume more power, take up more rack space, and cost more to purchase and operate. Moreover, these network security solutions fail to deliver the reliability and security organizations need. In typical high availability (HA) deployments (1+1), failure of one large device results in a massive — 50 percent — reduction in capacity. Plus, denial-of-service or other attacks can be easily targeted to this single point, increasing the likelihood of failures. This is not a winning combination.

Fortunately, there is a better approach. Using a network-based architecture, non-massive standard 1U or 2U NGFW platforms can be deployed to scale infinitely — with similar or better TCO, better performance, and increased resiliency to both failures and attacks. In fact, a fully meshed Layer 2 (transparent)

Using a network-based architecture, standard NGFW platforms can be deployed to scale infinitely — with similar or better TCO, better performance, and increased resiliency to both failures and attacks than the massive firewall alternative.

architecture can comprise up to 16 fully active NGFW devices, providing up to 640 Gbps of deep packet inspection with failure modes that typically impact only n-1 of overall capacity.

There are additional benefits to the model, including the freedom to choose components based on price/performance, availability or other preferences. With this architecture, your devices don't have to be massive to scale massively.

SonicWall Network Security platforms

SonicWall Network Security platforms employ a patented multi-core network processor architecture and Reassembly-free Deep Packet Inspection (RFDPI) engine. Together with our cloud-assist gateway anti-virus/malware technology, Network Security solutions deliver unsurpassed price/performance by delivering strong security, low latency and high throughput at a remarkably low TCO. This tech brief explains how.

Architecture details

Security services supported by different deployment modes

For the purposes of this paper, we will examine deploying a network-based firewall in transparent (Layer 2) mode. This validated and supported architecture consists of Networking S-series ingress and egress layers and SonicWall SuperMassive 9000 series security layer platforms. Table 1 identifies which security layer services are supported in different modes.

	Bypass mode	Inspect mode	Secure mode	Tap mode	L2 bridge, transparent, NAT & route modes
Active/Active clustering[1]	No	No	No	No	Yes
Application control	No	No	Yes	No	Yes
Application visibility	No	Yes	Yes	Yes	Yes
ARP/Routing/NAT[1]	No	No	No	No	Yes
Comprehensive anti-spam service[1]	No	No	No	No	Yes
Content filtering	No	No	Yes	No	Yes
DHCP server[1]	No	No	No	No	Yes[2]
DPI detection	No	Yes	Yes	Yes	Yes
DPI prevention	No	No	Yes	No	Yes
DPI-SSL[1]	No	No	Yes	No	Yes
High availability	Yes	Yes	Yes	Yes	Yes
Link-state propagation[3]	Yes	Yes	Yes	No	No
Stateful packet inspection	No	Yes	Yes	Yes	Yes
TCP handshake enforcement[4]	No	No	No	No	Yes
Virtual groups[1]	No	No	No	No	Yes

Table 1. The security layer services supported in various modes

[1] *These functions or services are unavailable on interfaces configured in wire mode, but remain available on a system-wide level for any interfaces configured in other compatible modes of operation.*
[2] *Not available in L2 bridged mode.*
[3] *Link state propagation is a feature whereby interfaces in a wire mode pair will mirror the link-state triggered by transitions of their partners. This is essential to proper operations in redundant path networks.*
[4] *Disabled by design in wire mode to allow for failover events occurring elsewhere on the network to be supported when multiple wire mode paths or multiple firewall units are in use along redundant or asymmetric paths.*

Configuring the firewall cluster

Figure 1 illustrates the recommended architecture for the firewall cluster. Ingress and egress connections can be made using 40 GE or 10 GE links as required. Security layer connections are made using 10 GE links. The ingress and egress switches provide load balancing and persistence of a given flow (IP source and destination) to a specific firewall for deep packet inspection in the security layer.

The ingress layer consists of dual Networking S-series switches deployed in a stack, which enables both switches to share a control plane and be fully active forwarders.

The security layer consists of 2 x n SuperMassive 9000 series firewalls deployed in an active configuration. Ingress and egress layer connections are made using load-balanced 10 GE links in port channels, one link from each switch to each firewall. The number of security layer devices can be scaled out as needed to meet performance or resiliency requirements.

The egress layer is configured in the same manner as the ingress layer to ensure persistent and symmetrical packet flows. Note that the ingress and egress layer switch configurations are identical, since traffic can originate in either direction. Support for inbound or outbound network address translation (NAT) can be provided by existing or additional devices in the network.

In the design shown in Figure 1, security layer links are in dual active port-channels to each firewall, one backing up the other in case of switch failure. The reference design also includes a bypass port channel, which serves to back up the active port channels. If the security layer fails or must be taken out of service, it will be quickly bypassed using this method. This design allows for multiple failures at the interface, firewall or switch levels with continuous availability and maintained performance.

The number of security layer devices can be scaled out as needed to meet performance or resiliency requirements.

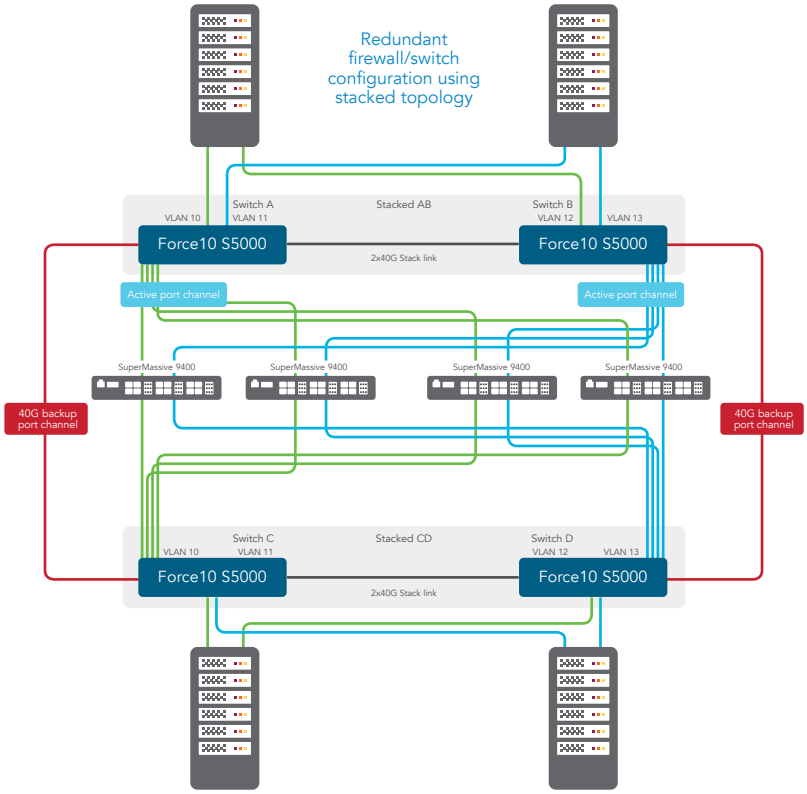

Figure 1. Architecture of a network-based firewall cluster

SONICWALL™

Sizing your firewall cluster

For resiliency purposes, deploy a minimum of two firewalls. To help you determine the best size for your firewall cluster, Table 2 lists the performance and size/power requirements of various size clusters, based on the SuperMassive 9400. You can double these figures by using the SuperMassive 9800 model firewall instead.

Table 2 demonstrates that performance scales linearly and is limited in practice only by the ability to generate traffic, since firewalls can be added until the ingress and egress layers exhaust their 10 GE security layer interfaces. In addition, latency remains consistent (~2 µs ingress, ~17 µs security, ~2 µs egress) regardless of utilization levels.

In contrast, competing chassis-based firewalls have finite scalability, consume ever-increasing rack space and power, and may not provide consistent performance (especially in virtualized environments) as utilization increases.

Comparing costs

An evaluation of next-generation firewall solutions should consider features, DPI performance, security effectiveness and TCO measured in price per protected/Mbps.

In addition to its security, performance and scalability benefits, a SonicWall network-based firewall has clear financial advantages. Initial deployment is far less expensive with SonicWall's pay-as-you-grow model than paying for large, under-utilized chassis models up front. Moreover, compared to chassis-based competitors, the SonicWall solution's three-year cost is up to 82 percent lower than Cisco, 65 percent lower than Palo Alto Networks and 57 percent lower than Fortinet, as detailed in Table 3.

Units	Model	SPI1/Gbps	APP-IPS2/ Gbps	DPI3/ Gbps	SSL-DPI/ Gbps	Connections/ sec	Maximum Connections (DPI)	RU	Watts
2	SM9400	40	20	9	4	260,000	2,000,000	6	1400
3	SM9400	60	30	13	6	390,000	4,000,000	7	1600
4	SM9400	80	40	18	8	520,000	5,000,000	8	1800
5	SM9400	100	50	22	10	650,000	6,000,000	9	2000
6	SM9400	120	60	26	12	780,000	7,000,000	10	2200
7	SM9400	140	70	31	14	910,000	8,000,000	11	2400
8	SM9400	160	80	35	16	1,040,000	9,000,000	12	2600
9	SM9400	180	90	40	18	1,170,000	10,000,000	13	2800
10	SM9400	200	100	44	20	1,300,000	11,000,000	14	3000
11	SM9400	220	110	48	22	1,430,000	12,000,000	15	3200
12	SM9400	240	120	53	24	1,560,000	13,000,000	16	3400
13	SM9400	260	130	57	26	1,690,000	14,000,000	17	3600
14	SM9400	280	140	62	28	1,820,000	15,000,000	18	3800
15	SM9400	300	150	66	30	1,950,000	16,000,000	19	4000
16	SM9400	320	160	70	32	2,080,000	17,000,000	20	4200

Table 2. SuperMassive 9400

Notes:
All figures calculated using published data
[1] SPI = Stateful inspection (traditional firewall)
[2] App-IPS = Application control with intrusion prevention
[3] DPI = Deep packet inspection with anti-malware
** Assumption 250W per S5000 (4 x 250W per sandwich)*

SonicWall Performance/Gbps					SPI	IPS	DPI	SonicWall
9400 units	SPI	IPS	DPI	3 year TCO	$/Mbps	$/Mbps	$/Mbps	3yr DPI savings
2	40	20	9	$254,698	$6	$13	$29	
3	60	30	13	$335,047	$6	$11	$25	
4	80	40	18	$415,396	$5	$10	$24	
5	100	50	22	$495,745	$5	$10	$23	
6	120	60	26	$576,094	$5	$10	$22	
7	140	70	31	$656,443	$5	$9	$21	
8	160	80	35	$736,792	$5	$9	$21	
9	180	90	40	$817,141	$5	$9	$21	
10	200	100	44	$897,490	$4	$9	$20	
Fortinet FortiGate 3700D								
	160	23	7.5	$505,990	$3	$22	$67	57%
	160	23	7.5	$505,990	$3	$22	$67	57%
	160	23	7.5	$505,990	$3	$22	$67	57%
Palo Alto Networks enterprise firewall PA-7050 series								
	40	20	20	$1,302,400	$33	$65	$65	65%
	60	30	30	$1,602,400	$27	$53	$53	60%
	80	40	40	$1,902,400	$24	$48	$48	57%
Cisco ASA 5585-X next-generation firewall								
	40	15	6	$985,544	$25	$66	$164	82%
	40	15	6	$985,544	$25	$66	$164	82%
	40	15	6	$985,544	$25	$66	$164	82%

Table 3. The SonicWall solution has a three-year cost up to 82 percent lower than chassis-based competitors.

Notes:
[1] Includes licensing and NBD support
[2] Performance figures from published data
[3] Competitive solutions configured in Active/Passive HA pair due to Active/Active limitations
[4] Fortinet solution: both units licensed with UTM bundle
[5] Palo Alto Networks solution: threat prevention + HA unit license
[6] Cisco solution: single FirePOWER IPS and apps 3YR AMP and URL subscription
[7] All pricing MSRP as of September 2015 from published data

The three-year cost of the SonicWall solution is up to 82 percent lower than chassis-based competitors.

Comparing total value

SonicWall is an award-winning, industry recognized leader with over two million firewalls shipped – over one million of which are protected through our Global Response Intelligent Defense (GRID) network. Our leading performance and security effectiveness has been validated and recommended by ICSA Labs, NSS Labs, Network World and others. We are consistently rated by the Microsoft Active Protections Program (MAPP) as "MAPP Partners who have released protections within 48 hours of the release of the Microsoft Security Advisory" — further demonstrating our value in protecting customers from real-world threats.

Conclusion

The evolution of network security requirements, along with increasing traffic levels and the adoption of 40 Gbps and higher core networking technologies, have driven the industry to respond with ever larger, more complex, power-hungry and expensive solutions. SonicWall offers an alternative solution that addresses security, resiliency and performance requirements while reducing costs — a winning combination.

Appendix 1: Bill of materials

Table 4 lists a bill of materials for a SonicWall network-based firewall supporting up to 80 Gbps of stateful inspection.

This bundle is also offered for 40 Gbps and 60 Gbps configurations and can be customized for scaling up to 640 Gbps. You can also customize to your desired support levels.

Qty	SKU	Description
4	210-AAWT	Networking S5000 Converged LAN/SAN Switch, Redundant AC PSU, IO to PSU (Normal), up to 4 Port Modules, 4X QSFP+
4	409-BBCD	S5000, 12-port Ethernet/FCoEModule, 1/10GbE SFP+ Interconnect
16	470-AAGN	Networking, Cable, SFP+to SFP+, 10GbE, Copper TwinaxDirect Attach Cable, 1 Meter
8	470-AAFE	Networking, Cable, QSFP+ to QSFP+, 40GbE Passive Copper Direct Attach Cable, 1 Meter
8	450-AASX	Networking, Jumper Cord, 250V, 12A, 2 Meters, C13/C14, US
4	971-5032	ProSupport: Next Business Day Parts Delivery, Initial Year
4	971-5036	ProSupport: 7x24 HW / SW Tech Support and Assistance, 1 year
4	971-5145	Hardware Limited Warranty Initial Year
4	A6833423	SonicWall SuperMassive 9400 Security Appliance with 1-year Total Secure
1	A7487144	SonicWall GMS Standard Edition 10 Node License
1	A7487154	SonicWall GMS E-Class 24x7 Software Support, 1 Year, 10 Nodes

Table 4. Bill of materials for a network-based firewall supporting up to 80 Gbps of stateful inspection

About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
www.sonicwall.com