Dell Network Security: A Super Massively Scalable Network Firewall

Overview

As Network Security requirements have evolved, the response has been to scale up hardware to meet performance requirements. The trade-off has become increasingly larger, complex, power-hungry, virtualized systems that are expensive to purchase and operate while increasing the impact in failure modes and providing a single attack point for DDOS and other firewall evasion techniques.

This document will describe a network-based model for scaling a Next Generation Firewall (NGFW) to approach or surpass existing or forthcoming models while providing increased performance, better TCO and increased resiliency.

How Massive Is Super?

Dell 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, Dell Network Security solutions deliver unsurpassed price/performance -- high security effectiveness, low-latency, high throughput and low TCO.

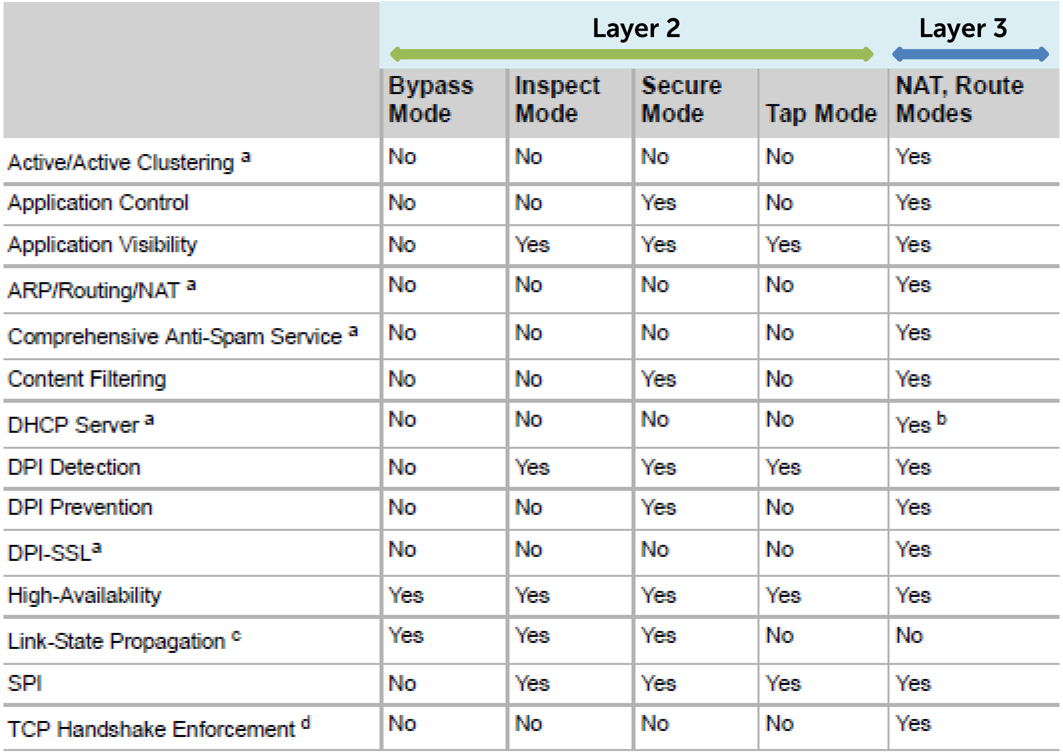
Competing architectures require increasingly massive processing capacity to provide similar levels of price/performance with the result being larger and larger platforms that consume more power, take up more rack space and cost more to purchase and operate. In typical HA deployments (1+1) a failure of one large device also results in a massive reduction in capacity (50%). Furthermore, DDOS or other attacks can be easily targeted to this single point, increasing the likelihood of failures. This is not a winning combination.

Using a network-based architecture, non-massive (1/2U) standard NGFW platforms can be deployed to scale infinitely, with similar or better TCO, better performance and increased resiliency to both failures and attacks. A fully-meshed L2 (transparent) architecture can consist of up to 16 NGFW devices all fully-active, providing up to 320Gbps of performance with typical failure modes that only impact 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, the devices don't' have to be massive to scale massively.

Upon Deeper Inspection

For the purposes of this paper, the Network-based firewall will be deployed in Transparent (Layer 2) mode. This validated and supported architecture consists of Dell Networking S5000 series ingress/egress layer (1U, 10/40GE converged switch) and Dell SonicWALL SuperMassive 9400 series security layer (1U, 20Gbps SPI, 8Gbps IPS, 4.5Gbps DPI firewall) platforms. The table below identifies which security layer services are supported in Layer 2 vs. Layer 3 modes:



	Layer 2				Layer 3
	Bypass Mode	Inspect Mode	Secure Mode	Tap Mode	NAT, Route Modes
Active/Active Clustering [a]	No	No	No	No	Yes
Application Control	No	No	Yes	No	Yes
Application Visibility	No	Yes	Yes	Yes	Yes
ARP/Routing/NAT [a]	No	No	No	No	Yes
Comprehensive Anti-Spam Service [a]	No	No	No	No	Yes
Content Filtering	No	No	Yes	No	Yes
DHCP Server [a]	No	No	No	No	Yes [b]
DPI Detection	No	Yes	Yes	Yes	Yes
DPI Prevention	No	No	Yes	No	Yes
DPI-SSL[a]	No	No	No	No	Yes
High-Availability	Yes	Yes	Yes	Yes	Yes
Link-State Propagation [c]	Yes	Yes	Yes	No	No
SPI	No	Yes	Yes	Yes	Yes
TCP Handshake Enforcement [d]	No	No	No	No	Yes

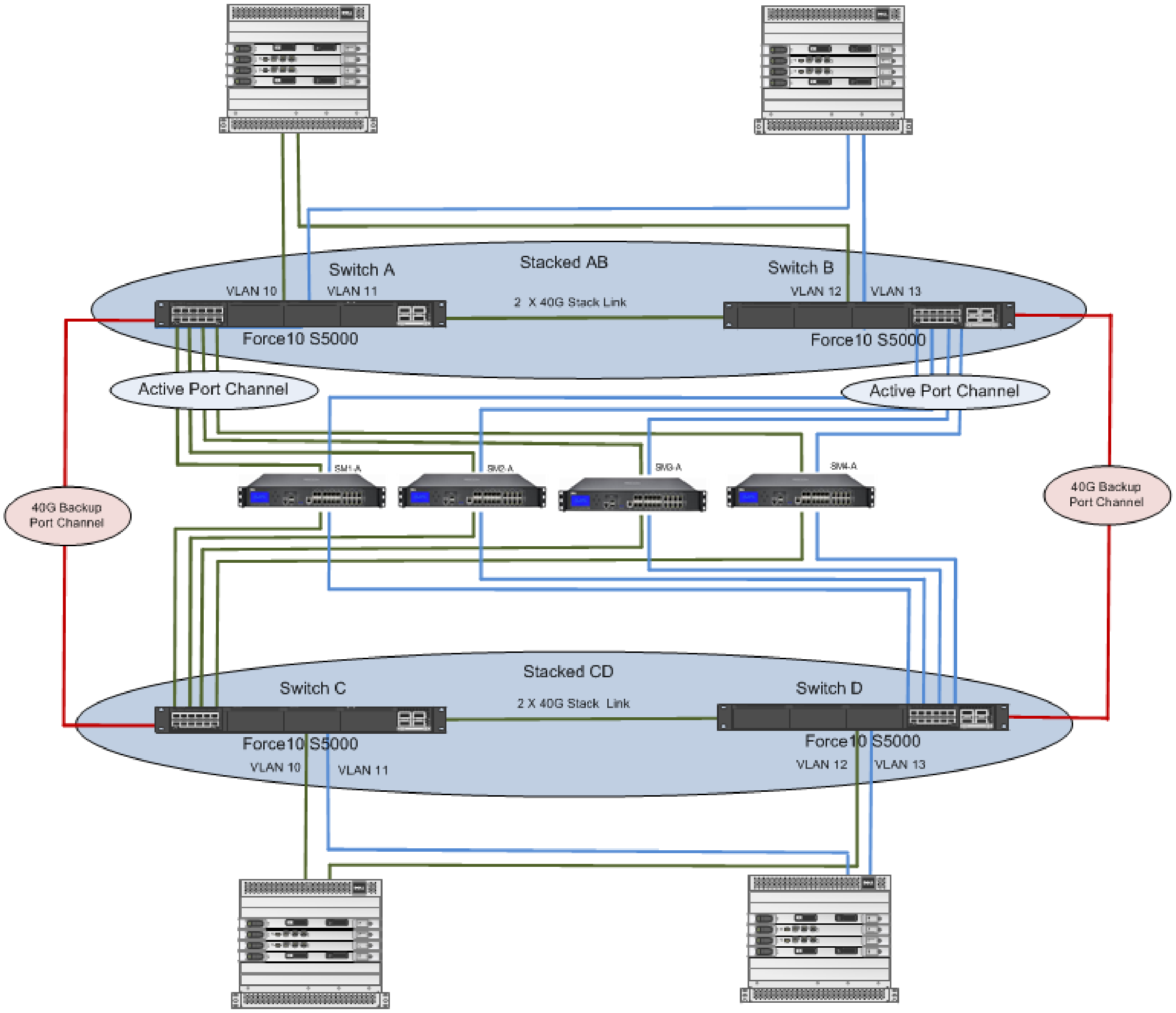
Ingress/egress connections can be made using 40GE or 10GE links as required. Security layer connections will be made using 10GE links. The ingress/egress switches will provide load-balancing and persistence of a given (IP Source/Destination) flow to a specific firewall in the security layer.

The “ingress” layer will consist of dual S5000 switches deployed in a stack, allowing both switches to share a control plane and be fully active forwarders.

The “security” layer will consist of 2 x n SuperMassive 9400 firewalls deployed in a standalone configuration. Ingress and Egress layer connections will be made using load-balanced 10GE links in a Link Aggregation Groups (LAG) port-channel, 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 will be 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 as traffic can originate in either direction.

Redundant Firewall/Switch configuration
Using Stacked\Mesh topology



In the above design, security layer links are shown in a single active port-channel with dual links to each firewall; however, they can be configured as needed to support scaling or additional VLAN's for ingress/egress. The reference design also includes a bypass port-channel which serves to back-up the active links. If the security layer fails or must be taken out of service, it can be quickly and easily bypassed using this method.

For resiliency purposes, a minimum of two firewalls should be deployed. Based on the Dell Networking S5000 and Dell SuperMassive 9400, the maximum performance and size/power requirements of the firewall cluster are:

Units	Model	SPI/Gbps	IPS/Gbps	DPI/Gbps	Conn/sec	Conn/total	Rack Units	Power/Watts
2	SM9400	40	16	9	260,000	2,500,000	6	1400
3	SM9400	60	24	14	390,000	3,750,000	7	1600
4	SM9400	80	32	18	520,000	5,000,000	8	1800
5	SM9400	100	40	23	650,000	6,250,000	9	2000
6	SM9400	120	48	27	780,000	7,500,000	10	2200
7	SM9400	140	56	32	910,000	8,750,000	11	2400
8	SM9400	160	64	36	1,040,000	10,000,000	12	2600
9	SM9400	180	72	41	1,170,000	11,250,000	13	2800
10	SM9400	200	80	45	1,300,000	12,500,000	14	3000
11	SM9400	220	88	50	1,430,000	13,750,000	15	3200
12	SM9400	240	96	54	1,560,000	15,000,000	16	3400
13	SM9400	260	104	59	1,690,000	16,250,000	17	3600
14	SM9400	280	112	63	1,820,000	17,500,000	18	3800
15	SM9400	300	120	68	1,950,000	18,750,000	19	4000
16	SM9400	320	128	72	2,080,000	20,000,000	20	4200

1 - All figures calculated from published specifcations and List Pricing

2 - SPI = Stateful Inspection (traditional firewall)

3 - App/IPS = Application Control with Intrusion Prevention

4 - DPI = Deep Packet Inspetion with Anti-Malware

The above table demonstrates that theoretical performance scales linearly and is only limited, in practice, by the ability to generate traffic levels, as firewalls can be added until the ingress/egress layers exhaust their 10GE security layer interfaces. In addition, latency remains consistent (~2us ingress, ~30us security, ~2us egress) regardless of utilization levels.

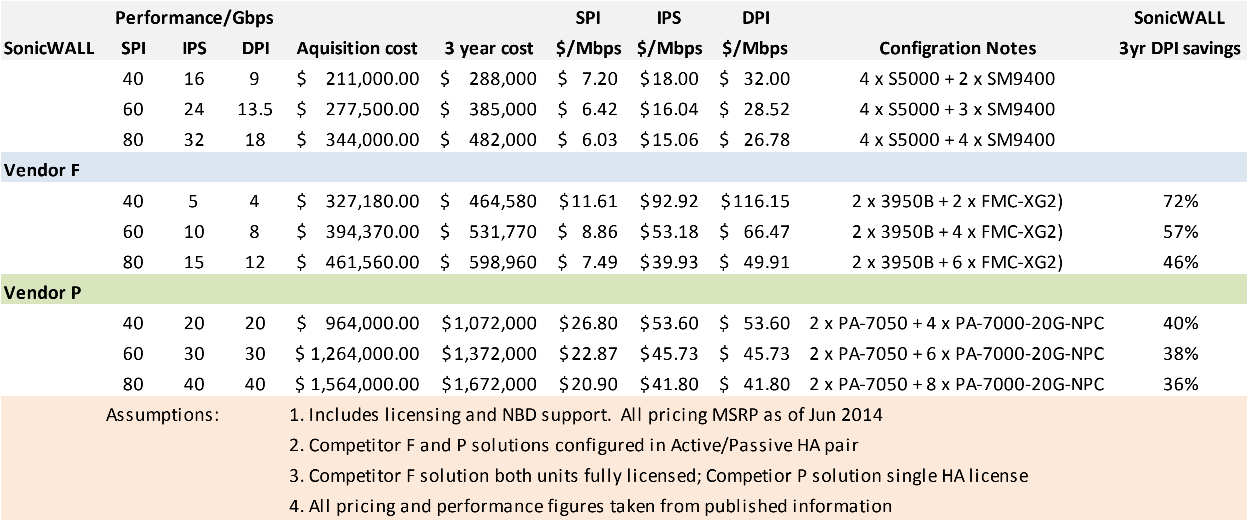
In contrast, other massive, virtualized firewalls have finite scalability, consume ever increasing rack space/power and cannot provide consistent performance (especially in virtualized environments) as utilization increases.

Conclusion

An evaluation of Next Generation Firewall solutions should include consideration for features, **DPI performance, security effectiveness and TCO in price per protected/Mbps**

Dell SonicWALL is an award-winning, industry recognized leader with **over 2 million firewalls shipped** – over 1 million of which are deployed in customers worldwide and 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.

The below table compares price per protected/Mbps, acquisition cost and TCO of a network-based firewall with 10/40GE support vs. competitive "legacy" chassis based models:



	Performance/Gbps					SPI	IPS	DPI		SonicWALL
SonicWALL	SPI	IPS	DPI	Aquisition cost	3 year cost	$/Mbps	$/Mbps	$/Mbps	Configration Notes	3yr DPI savings
	40	16	9	$ 211,000.00	$ 288,000	$ 7.20	$18.00	$ 32.00	4 x S5000 + 2 x SM9400	
	60	24	13.5	$ 277,500.00	$ 385,000	$ 6.42	$16.04	$ 28.52	4 x S5000 + 3 x SM9400	
	80	32	18	$ 344,000.00	$ 482,000	$ 6.03	$15.06	$ 26.78	4 x S5000 + 4 x SM9400	
Vendor F										
	40	5	4	$ 327,180.00	$ 464,580	$11.61	$92.92	$116.15	2 x 3950B + 2 x FMC-XG2)	72%
	60	10	8	$ 394,370.00	$ 531,770	$ 8.86	$53.18	$ 66.47	2 x 3950B + 4 x FMC-XG2)	57%
	80	15	12	$ 461,560.00	$ 598,960	$ 7.49	$39.93	$ 49.91	2 x 3950B + 6 x FMC-XG2)	46%
Vendor P										
	40	20	20	$ 964,000.00	$1,072,000	$26.80	$53.60	$ 53.60	2 x PA-7050 + 4 x PA-7000-20G-NPC	40%
	60	30	30	$ 1,264,000.00	$1,372,000	$22.87	$45.73	$ 45.73	2 x PA-7050 + 6 x PA-7000-20G-NPC	38%
	80	40	40	$ 1,564,000.00	$1,672,000	$20.90	$41.80	$ 41.80	2 x PA-7050 + 8 x PA-7000-20G-NPC	36%
	Assumptions:			1. Includes licensing and NBD support. All pricing MSRP as of Jun 2014						
				2. Competitor F and P solutions configured in Active/Passive HA pair						
				3. Competitor F solution both units fully licensed; Competior P solution single HA license						
				4. All pricing and performance figures taken from published information						

This table demonstrates that a Dell SonicWALL network-based firewall has clear financial advantages using a "pay-as-you-grow" model vs. paying for a large under-utilized chassis model up front. **The Dell SonicWALL solution has a 3 year cost up to 72% lower than Competitor F, and up to 40% lower than Competitor P** with far greater scalability.

Furthermore, the Dell SonicWALL solution has 40GE ingress/egress built-in to the solution and provides investment protection from day one.

The evolution of network security requirements, increasing traffic levels and subsequent move to 10/40Gbps core networking technology has driven the industry to respond with ever larger, power-hungry and expensive security solutions. Dell SonicWALL is proposing an **alternative solution** in this paper which **addresses security, resiliency and performance requirements** while **lowering costs** and providing **10/40GE capability today** – a winning combination.

Appendix 1: Network Firewall Ingress/Egress Layer sample configuration

There are several configuration options for the ingress/egress layer, including:

- Layer 2 (transparent) mode using a single LAG with bypass
  - Supports up to 16 interfaces (160Gbps) to security layer
  - Can be deployed with/without redundant links to each firewall
- Layer 2 (transparent) mode using multiple LAGs with bypass
  - Allows segmentation for virtualized infrastructure
  - Supports up to 16 interfaces (160Gbps) per LAG to security layer
  - Can be used to segment and scale out large environments

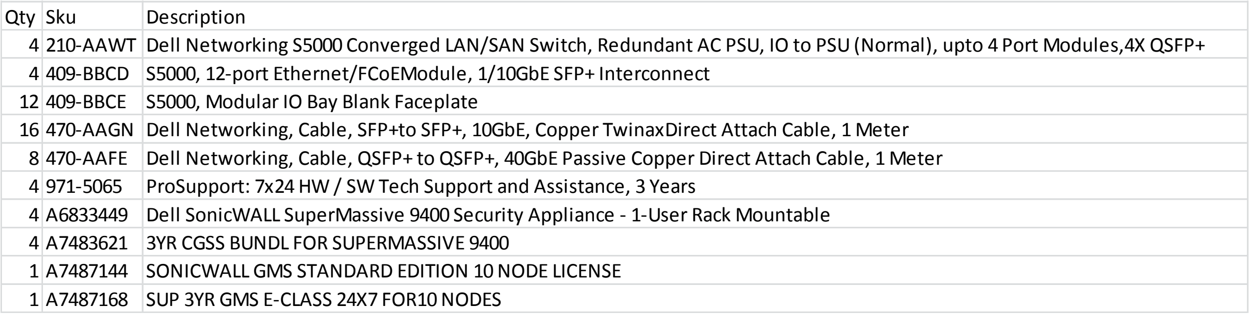
For the purpose of this document, the configuration to upstream/downstream devices (switches and/or routers connected to the network-based firewall) is ignored. The sample partial configuration below provides a transparent mode network-based firewall using dual port-channels (active and backup) with redundant firewall connections and bypass, supporting 20Gbps ingress/egress to each firewall for full SPI, IPS and DPI services.

```
! FTOS Version 9.1(1.0P2)
!
redundancy auto-synchronize full
!
hash-algorithm seed 444444
hash-algorithm lag xor16
!
stack-unit 0 provision S5000
!
stack-unit 0 stack-group 14
!
stack-unit 0 stack-group 15
!
interface TenGigabitEthernet 0/0
 no ip address
!
 port-channel-protocol LACP
  port-channel 1 mode active
 no shutdown
!
interface TenGigabitEthernet 0/1
 no ip address
!
 port-channel-protocol LACP
  port-channel 1 mode active
 no shutdown
!
interface TenGigabitEthernet 0/2
 no ip address
!
 port-channel-protocol LACP
  port-channel 1 mode active
 no shutdown
!
```

```
interface TenGigabitEthernet 0/3
 no ip address
!
 port-channel-protocol LACP
  port-channel 1 mode active
 no shutdown
!
interface fortyGigE 0/48
 no ip address
!
 port-channel-protocol LACP
  port-channel 2 mode active
 no shutdown
!
stack-unit 1 provision S5000
!
stack-unit 1 stack-group 14
!
stack-unit 1 stack-group 15
!
interface TenGigabitEthernet 1/0
 no ip address
!
 port-channel-protocol LACP
  port-channel 1 mode active
 no shutdown
!
interface TenGigabitEthernet 1/1
 no ip address
!
 port-channel-protocol LACP
  port-channel 1 mode active
 no shutdown
!
interface TenGigabitEthernet 1/2
 no ip address
!
 port-channel-protocol LACP
  port-channel 1 mode active
 no shutdown
!
interface TenGigabitEthernet 1/3
 no ip address
!
 port-channel-protocol LACP
  port-channel 1 mode active
 no shutdown
!
interface fortyGigE 1/48
 no ip address
!
port-channel-protocol LACP
  port-channel 2 mode active
 no shutdown
!
interface Port-channel 1
 no ip address
 switchport
 switchport backup interface Port-channel 2
 no shutdown
!
interface Port-channel 2
 no ip address
 switchport
 no shutdown
!
interface Vlan 1
!untagged Port-channel 1-2
!
stack-unit 0 priority 1
!
load-balance ip-selection source-ip dest-ip
!
end
```

Appendix 2: Bill of Materials

The below Bill of Materials is for a network based firewall cluster supporting up to 80Gbps of Stateful Inspection:



Qty	Sku	Description
4	210-AAWT	Dell Networking S5000 Converged LAN/SAN Switch, Redundant AC PSU, IO to PSU (Normal), upto 4 Port Modules,4X QSFP+
4	409-BBCD	S5000, 12-port Ethernet/FCoEModule, 1/10GbE SFP+ Interconnect
12	409-BBCE	S5000, Modular IO Bay Blank Faceplate
16	470-AAGN	Dell Networking, Cable, SFP+to SFP+, 10GbE, Copper TwinaxDirect Attach Cable, 1 Meter
8	470-AAFE	Dell Networking, Cable, QSFP+ to QSFP+, 40GbE Passive Copper Direct Attach Cable, 1 Meter
4	971-5065	ProSupport: 7x24 HW / SW Tech Support and Assistance, 3 Years
4	A6833449	Dell SonicWALL SuperMassive 9400 Security Appliance - 1-User Rack Mountable
4	A7483621	3YR CGSS BUNDL FOR SUPERMASSIVE 9400
1	A7487144	SONICWALL GMS STANDARD EDITION 10 NODE LICENSE
1	A7487168	SUP 3YR GMS E-CLASS 24X7 FOR10 NODES

This bundle is also offered for 40Gbps or 60Gbps configurations and can be customized for desired support levels and further scaling beyond 80Gbps.