Next Generation Firewalls: Top 9 Revisited

Miguel (Mike) O. Villegas,
CISA, CISSP, GSEC, CEH, PCI QSA, PA-QSA
Vice President K3DES, LLC

Core Competencies – C32

Abstract

Recent security breaches to some of the largest and seemingly more secure environments beg the question whether existing protection mechanisms are sufficient to deter unauthorized access to critical assets. Traditional firewalls, anti-virus and intrusion prevention systems appear to have lost their usefulness. In reality, they are still very much in use; however, more robust and effective solutions are needed to keep up with those that threaten our network infrastructures.

Next-Generation Firewalls are integrated network platforms that consist of in-line deep packet inspection (DPI) firewalls, Intrusion Prevention Systems, Application Inspection and Control, SSL/SSH inspection, website filtering, and Quality of Service (QoS)/bandwidth management in the network to protect the network against latest sophisticated attacks. This session will cover NGFW features, uses, business case and vendor offerings. It will also provide the participant with a roadmap on how to audit and manage a NGFWs. After completing this session, participants will be able to:

1. Better understand what is a Next Generation Firewall?
2. Gain knowledge in how do they differ from UTM?
3. Better understand what are NGFW features and how do they work?
4. Better understand how to make a business case for a NGFW
5. Gain knowledge in how to audit and manage a NGFW

The products presented in this session are for informational purposes only and does not reflect an endorsement or recommendation on the part of the presenter. Attendees are advised to perform their own due diligence in selecting the right solution for their institutions.

Table of Contents

- NGFW Primer
- Need for NGFW
- Case for NGFW
- NGFW Vendors
- NFGW Audit

NGFW PRIMER


ISACA
Trust in, and value from, information systems
San Francisco Chapter
CyberSizeIT
SF ISACA FALL CONFERENCE
NOVEMBER 9-11, 2015
HOTEL NIKKO-SAN FRANCISCO

NGFW Primer

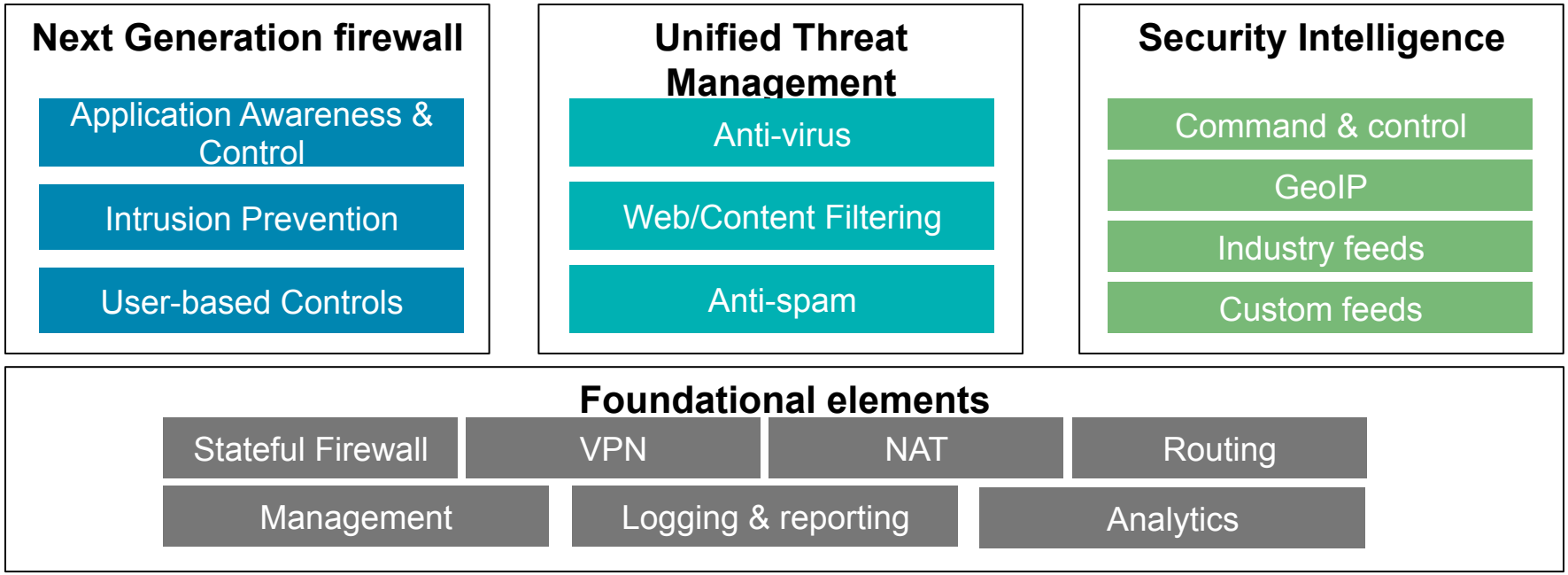
NGFWs are integrated network security platforms that consist of:

- in-line deep packet inspection (DPI) firewalls,
- Intrusion Prevention Systems (IPS),
- application inspection and control,
- SSL/SSH inspection,
- website filtering and
- quality of service (QoS)/bandwidth management

The presenter of this session has interviewed and researched NGFWs for 9 NGFW vendors in October 2014 listed in the 2014 Gartner Magic Quadrant.

- **Juniper**
- **Palo Alto**
- **Fortinet**
- **Dell Sonicwall**
- **HP Tippingpoint**
- **Cisco**
- **Checkpoint**
- **McAfee**
- **Barracuda**

Next Generation Firewall Primer



Source: Juniper SRX – Next Generation Firewall – November 2014

Traditional Firewalls

- Unlike NGFWs, traditional packet-filtering firewalls only provide protection at Layer 3 (network) and Layer 4 (transport) of the OSI model.
- They include metrics to allow and deny packets by discriminating the source IP address of incoming packets, destination IP addresses, the type of Internet protocols the packet may contain – e.g.,
  - normal data carrying IP packets,
  - ICMP (Internet Control Message Protocol),
  - ARP (Address Resolution Protocol),
  - RARP (Reverse Address Resolution Protocol),
  - BOOTP (Bootstrap Protocol) and
  - DHCP (Dynamic Host Configuration Protocol) -- and routing features.

NGFW Foundational Elements

NGFWs are integrated network security platforms that consist of:

- Stateful Firewall
- Virtual Private Network (VPN)
- Network Address Translation (NAT)
- Routing
- Management
- Logging and Reporting
- Analytics

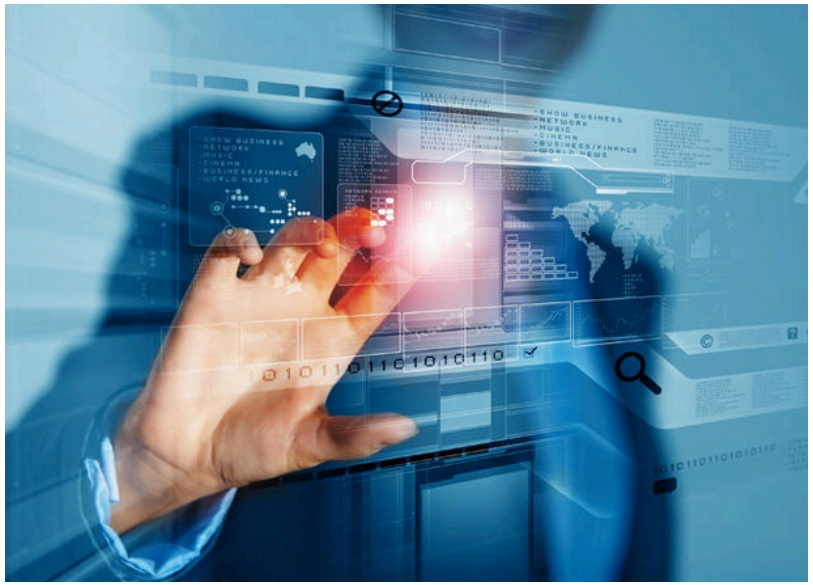
NGFW Additional Elements

NGFWs are integrated network security platforms that also consist of:

- Application Awareness and Control
- Intrusion Prevention
- User based controls
- Anti-Virus
- Web/Content Filtering
- Anti-Spam
- Two-factor authentication
- Active Directory Integration
- Security Intelligence / Threat Intelligence
- Mobile Device Controls
- Data Loss Prevention

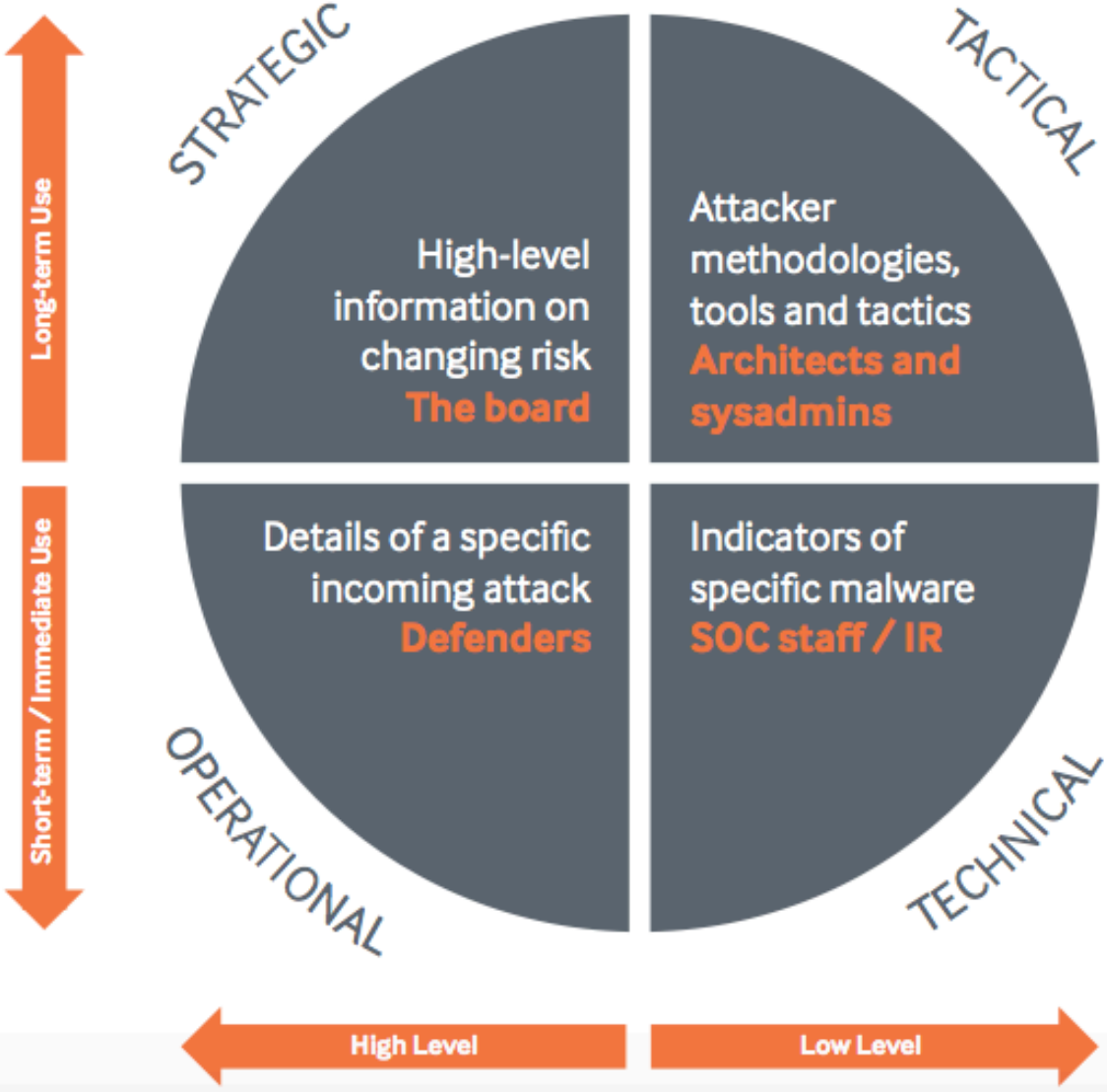
Threat Intelligence

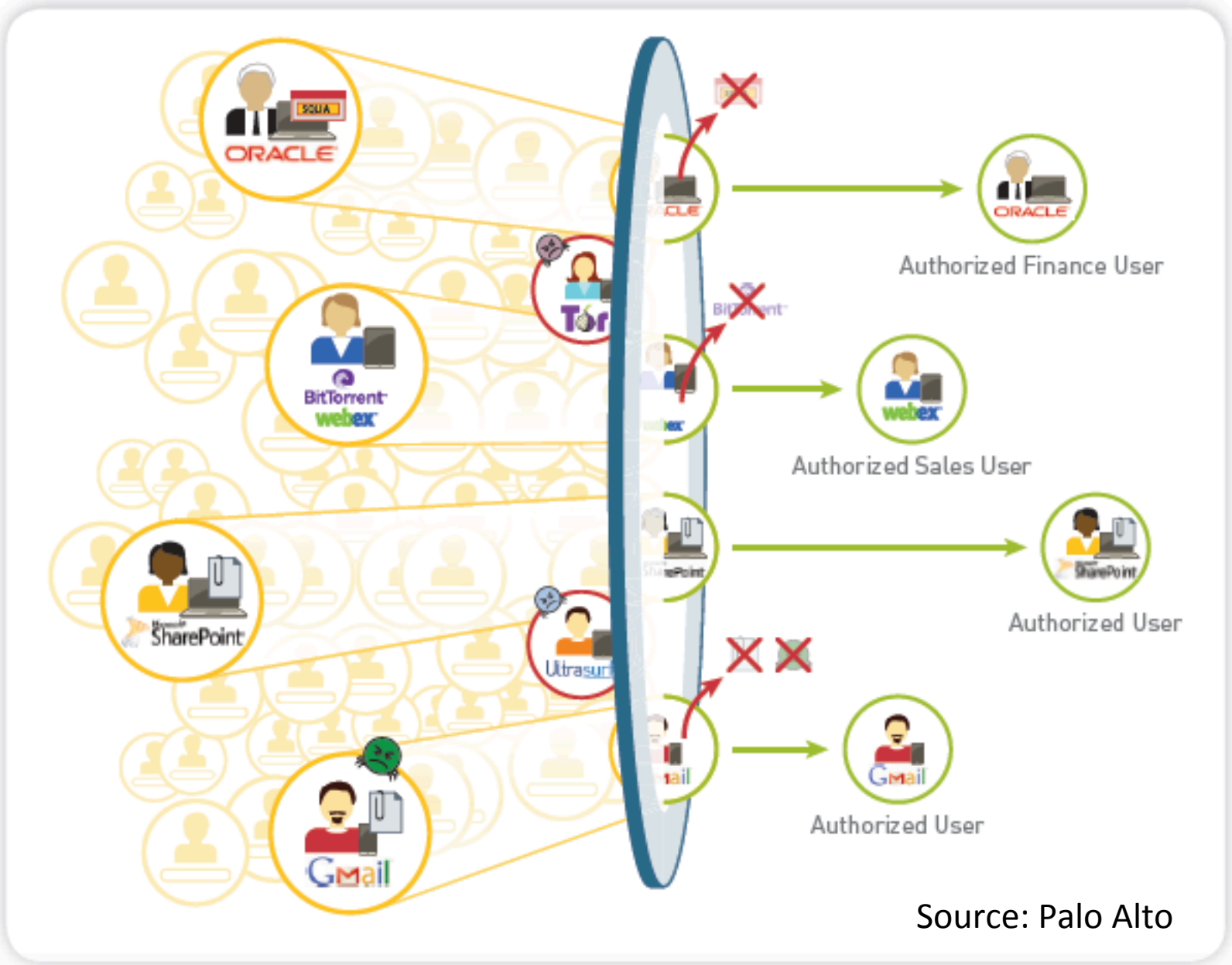
One of the major differentiators that all of these major NGFW companies purport to be working on is threat intelligence that is current, open, continuous, adaptive and automatic.



http://www.zdnet.com/article/new-threat-intelligence-report-skewers-industry-confusion-charlatans/

Figure 3: Subtypes of threat intelligence





Applications, content, users, and devices—all under your control.

Types of Attacks

Malware, also called malicious code, is software designed to gain access to targeted computer systems, steal information or disrupt computer operations.

- Worm
- Virus
- Network Worm
- Trojan Horse
- Botnets
- Spyware
- Adware
- Ransomware
- Keylogger
- Rootkit

Types of Attacks

- Advanced persistent threats
- Backdoor
- Brute force attack
- Buffer overflow—
- Cross-site scripting (XSS)
- Denial-of-service (DoS) attack
- Man-in-the-middle attack
- Social engineering
- Phishing
- Spear phishing
- Spoofing
- Structure Query Language (SQL) injection
- Zero-day exploit

UTM vs NGFW

Security vendors often differ in their definitions of UTM and NGFWs. Over time, UTM references will likely dissipate -- the same may even happen for NGFWs -- but what's certain is that enhancements to multifunctional security solutions, whatever they're called, will continue.

- UTMs are primarily for SMB
- NGFW are for more larger more complex IT environments

SECURITY PRODUCTS COMPARISON MATRIX

SRX and Firefly Perimeter Features Matrix		SRX100	SRX110	SRX210	SRX220	SRX240	SRX550	SRX650
		Branch / Office	Branch / Office	Branch / Office	Branch / Office	Branch / Office	Branch / Office	Large Office
Performance	Firewall throughput (large packets)	700 Mbps	700 Mbps	850 Mbps	950 Mbps	1.8 Gbps	5.5 Gbps	7 Gbps
	Firewall throughput (IMIX)	200 Mbps	200 Mbps	250 Mbps	300 Mbps	600 Mbps	1.7 Gbps	2.5 Gbps
	IPsec VPN 3DES/AES throughput (large packets)	65 Mbps	65 Mbps	85 Mbps	100 Mbps	300 Mbps	1.0 Gbps	1.5 Gbps
	IPS throughput	75 Mbps	75 Mbps	65 Mbps	80 Mbps	230 Mbps	800 Mbps	1 Gbps
	Antivirus (Sophos AV) throughput	25 Mbps	25 Mbps	30 Mbps	35 Mbps	85 Mbps	300 Mbps	350 Mbps
	Maximum concurrent sessions[2]	32K	32K	64K	96K	256K	375K	512K
	Connections/Sec	1.8K	1.8K	2.2K	2.8K	8.5K	27K	35K
	Interfaces	8x10/100	8x10/100 + 1xVDSL	2 10/100/1000 + 6 10/100, optional PoE, 1 I/O slot supporting SFP, ADSL, ADSL2, ADSL2+, Serial, T1, E1, VDSL	8 10/100/1000, optional PoE, 2 I/O slots supporting SFP, ADSL, ADSL2, ADSL2+, Serial, T1, E1, VDSL	16 10/100/1000, optional PoE, 4 I/O slots supporting SFP, ADSL, ADSL2, ADSL2+, Serial, T1, E1, VDSL	6 10/100/1000 + 4 SFP, 8 I/O slots supporting GbE, PoE, SFP, ADSL, ADSL2, ADSL2+, Serial, T1, E1, VDSL, DS3, E3	4 10/100/1000, 8 I/O slots supporting GbE, PoE, SFP, T1, E1, Serial, DS3, E3
Firewall	DoS and DDoS protection (Layers 3 and 4)	X	X	X	X	X	X	X
	TCP reassembly for fragmented packet protection	X	X	X	X	X	X	X
	Brute force attack mitigation	X	X	X	X	X	X	X
	SYN cookie protection	X	X	X	X	X	X	X
	Zone-based IP spoofing	X	X	X	X	X	X	X
	Malformed packet protection	X	X	X	X	X	X	X
VPN	IPsec VPN	X	X	X	X	X	X	X
NGFW/L7 Security Services	Intrusion Prevention System (IPS)	X	X	X	X	X	X	X
	AppTrack[3]	X	X	X	X	X	X	X
	AppFirewall[3]	X	X	X	X	X	X	X
	AppQoS[4]	X	X	X	X	X	X	X
	AppID (Application Awareness)[5]	X	X	X	X	X	X	X
	User Firewall: On-box[6]	X	X	X	X	X	X	X
	User Firewall: Integrated w/Juniper's Unified Access Control (UAC)	X	X	X	X	X	X	X
	SSL Forward Proxy[7]	X	X	X	X	X	X	X
	SSL Reverse Proxy							
UTM[8]	Antivirus	X	X	X	X	X	X	X
	Antispam	X	X	X	X	X	X	X
	Web filtering	X	X	X	X	X	X	X
	Content filtering	X	X	X	X	X	X	X
Networking	Routing	OSPF, BGP, RIPv1/v2, MPLS, Multicast	OSPF, BGP, RIPv1/v2, MPLS, Multicast	OSPF, BGP, RIPv1/v2, MPLS, Multicast	OSPF, BGP, RIPv1/v2, MPLS, Multicast	OSPF, BGP, RIPv1/v2, MPLS, Multicast	OSPF, BGP, RIPv1/v2, MPLS, Multicast	OSPF, BGP, RIPv1/v2, MPLS, Multicast
	Multiple WAN, WLAN, LAN options	X	X	X	X	X	X	X
Availability	High Availability (A/P, A/A)[11]	X	X	X	X	X	X	X
	Separate Control and Data Planes	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	In-Service SW & HW Upgrade	N/A	N/A	N/A	N/A	N/A	N/A	N/A
NAT	NAT	X	X	X	X	X	X	X
Management	Centralized management	X	X	X	X	X	X	X

SRX and Firefly Perimeter Features Matrix		SRX1400	SRX3400	SRX3600	SRX5400	SRX5600	SRX5800	Firefly Perimeter
		Small-med data center	Med / large data center	Med / large data center	High perf data center	High perf data center	High perf data center	Virtual DC/ Public or Private Cloud
NGFW/L7 Security Services	Intrusion Prevention System (IPS)	X	X	X	X	X	X	X
	AppTrack	X	X	X	X	X	X	
	AppFirewall	X	X	X	X	X	X	
	AppQoS[4]	X	X	X	X	X	X	
	AppID (Application Awareness)	X	X	X	X	X	X	
	User Firewall: On-box[4]	X	X	X	X	X	X	
	User Firewall: Integrated w/Juniper's Unified Access Control (UAC)[4]	X	X	X	X	X	X	
	SSL Forward Proxy	X	X	X	X	X	X	
	SSL Reverse Proxy[4]	X	X	X	X	X	X	
UTM[5]	Antivirus	X	X	X	X	X	X	X
	Antispam	X	X	X	X	X	X	X
	Web filtering	X	X	X	X	X	X	X
	Content filtering	X	X	X	X	X	X	X
Networking	Routing	OSPF, BGP, RIPv1/v2, Multicast	OSPF, BGP, RIPv1/v2, Multicast	OSPF, BGP, RIPv1/v2, Multicast	OSPF, BGP, RIPv1/v2, Multicast	OSPF, BGP, RIPv1/v2, Multicast	OSPF, BGP, RIPv1/v2, Multicast	X
	Multiple WAN, WLAN, LAN options	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Availability	High Availability (A/P, A/A)[11,12]	X	X	X	X	X	X	X
	Separate Control and Data Planes	X	X	X	X	X	X	N/A
	In-Service SW & HW Upgrade	X	X	X	X	X	X	N/A
NAT	NAT	X	X	X	X	X	X	X
Management	Centralized management	X	X	X	X	X	X	X

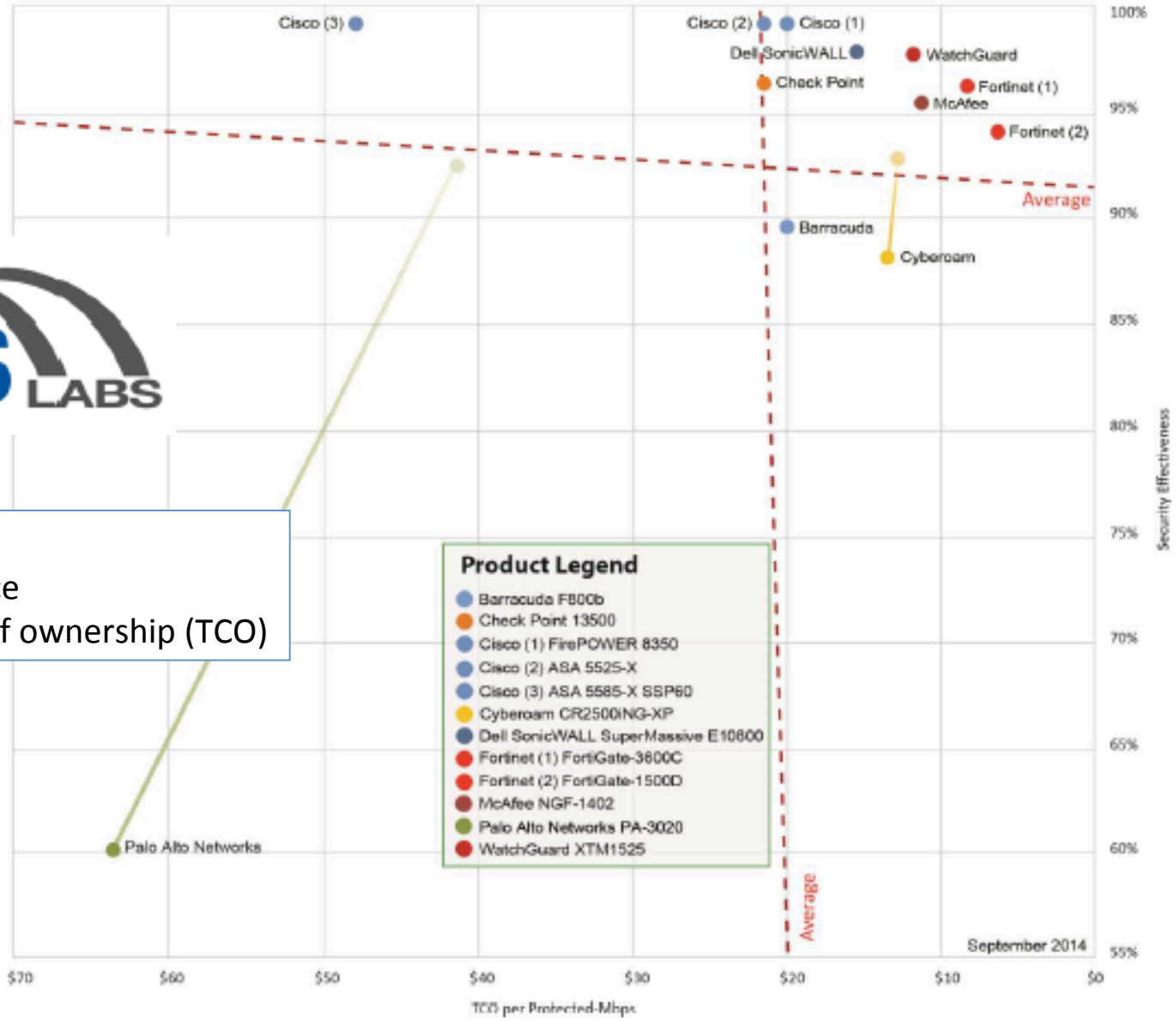
Source: Juniper SRX Datasheet

Gartner Magic Quadrant – April 2015

CHALLENGERS LEADERS

NICHE PLAYERS VISIONARIES

NSS Labs Next Generation Firewall (NGFW) Security Value Map™



NSS LABS

October 7, 2015

- Security
- Performance
- Total cost of ownership (TCO)

Figure 1 – NSS Labs Security Value Map (SVM) for Next Generation Firewall (NGFW)

ISA Serving IT Governan
San Francisco Chapter

Key Findings

- Overall *security effectiveness* varied between 60.1% and 99.2%, with 8 of the 12 tested products achieving greater than 95.0%.
- The Cyberoam CR2500iNG-XP failed one Stream Segmentation evasion test.
- The Palo Alto PA-3020 failed the RPC Fragmentation and IP Fragmentation + TCP Segmentation evasion tests.
- *TCO per protected-Mbps* varied from US$6.35 to US$63.66, with most tested devices costing below US$25.00 *per protected-Mbps*.
- *NSS-tested throughput* ranged from 719 Mbps to 18,771 Mbps.
- Average *security effectiveness* rating was 91.5% – 9 devices were rated as above average *security effectiveness*, 3 were rated as below average.
- Average *value* (*TCO per protected-Mbps*) was US$21.80 – 10 devices were rated as above average *value* and two were below average.

Product	Security Effectiveness		Value (TCO Per Protected-Mbps)		Overall Rating
Barracuda F800b	89.70%	Below Average	$20.03	Above Average	Neutral
Check Point 13500	96.40%	Above Average	$21.45	Above Average	Recommended
Cisco ASA 5525-X	99.20%	Above Average	$21.60	Above Average	Recommended
Cisco ASA 5585-X SSP60	99.20%	Above Average	$48.00	Below Average	Neutral
Cisco FirePOWER 8350	99.20%	Above Average	$20.03	Above Average	Recommended
Cyberoam CR2500iNG-XP	88.20%	Below Average	$13.48	Above Average	Neutral
Dell SonicWALL SuperMassive E10800	97.90%	Above Average	$15.46	Above Average	Recommended
Fortinet FortiGate-1500D	94.10%	Above Average	$6.35	Above Average	Recommended
Fortinet FortiGate-3600C	96.30%	Above Average	$8.30	Above Average	Recommended
McAfee NGF-1402	95.50%	Above Average	$11.38	Above Average	Recommended
Palo Alto Networks PA-3020	60.10%	Below Average	$63.66	Below Average	Caution
WatchGuard XTM1525	97.80%	Above Average	$11.87	Above Average	Recommended

Figure 2 – NSS Labs' Recommendations for Next Generation Firewall (NGFW)

31 October 2014

During October 2014 the Palo Alto Networks PA-3020 v6.0.5-h3 was subjected to thorough testing at the NSS facility in Austin, Texas, based on the Next Generation Firewall (NGFW) methodology v5.4 available on www.nsslabs.com. This test was conducted free of charge and NSS did not receive any compensation in return for Palo Alto Networks' participation.

Using the recommended policy, the PA-3020 blocked 93.1% of attacks against server applications, 92.0% of attacks against client applications, and 92.5% overall. The device successfully detected and decoded all evasion techniques. The device also passed all stability and reliability tests.

As a result of these tests the Palo Alto Networks PA-3020 v6.0.5-h3 achieved a 92.5% security effectiveness rating.

Our test engineers are available to speak with you should you have questions about this test or the results.

Sincerely,

Vikram Phatak
Chief Executive Officer
NSS Labs

NEED FOR NGFW

Do we really need a NGFW?

- But “we’ve never had a breach” or “we are not a big target”
- Today there are a large number of disparate standalone products and services forced to work together
- Although effective, appear architecturally desultory, reactive and tactical in nature
- NGFWs offer a good compliment of security solutions in one appliance
- Not all NGFWs are created equal
- 3 factors for establishing a need for a NGFW
  - Is the investment justifiable?
  - Alignment with existing IT strategies
  - Total Cost of Ownership (TCO)

Is the investment justifiable?

- Basic firewall services regulate network connections between computer systems of differing trust levels
- Most enterprises need:
  - IPS/IDS
  - Firewall (deep packet inspection)
  - Anti-virus/Malware protection
  - Application controls
  - VPN
  - Session encryption (TLS 1.2)
  - Wireless security
  - Mobile security

Alignment with existing IT strategies

- Organizations that deploy NGFWs may discover they do not require all the security features these appliances support
- Features required by an enterprise should be determined in advance, as this will influence what NGFW product is bought and which security services to enable
- Some NGFWs have security features built into the appliance at no additional cost
- Some do not activate feature since they have not found them necessary or because they do not fit their business model

For example:

- Large retail companies might opt for a NGFW solution at the corporate headquarters, but go with point solutions in each retail store -- whether from the same vendor or not.
- Online retail businesses that do not have brick and mortar locations typically require robust and, therefore, increasingly integrated network security solutions that focus on QoS, load balancing, IPS, web application security, SSL, VPN and strong firewalls with deep packet inspection.
- Enterprises that are heavily regulated via standards (e.g., PCI, HIPAA, HITECH Act, Sarbanes-Oxley, FISMA, PERC, etc.) would need to also address remote access controls, two-factor authentication, Active Directory integration and, possibly, DLP.

Alignment with existing IT strategies

- Whatever course is taken, information security decisions need to integrated with IT's strategic goals.
- IT, in turn, exists to support the business. IT does not drive the business.
- The business drives the business.
- IT's purpose is to ensure the IT infrastructure (perimeter and core deployments) exist to allow the business to achieve its strategic goals.

Total Cost of Ownership (TCO)

TCO establishes the right complement of resources -- people and technology.

- **Total cost of technology (TCT):** The cost of technology that is required to deploy, monitor and report on the state of information security for the enterprise.
- **Total cost of risk (TCR):** The cost to estimate and not deploy resources, processes or technology for your enterprise, such as compliance risk, security risk, legal risk and reputation risk.
- **Total cost of maintenance (TCM):** The cost of maintaining the information security program, such as people, skills, flexibility, scalability and comprehensiveness of the systems deployed.

CASE FOR A NGFW

Six Criteria for buying a NGFW

It is clear that regardless of what vendors call their NGFW products, it is incumbent that buyers understand the precise features each NGFW product under consideration includes. Let's look at six criteria:

- Platform Type
- Feature Set
- Performance
- Manageability
- Price
- Support

Platform Type

- How is the NFGW provided?
- Most next-gen firewalls are hardware- (appliance), software- (downloadable) or cloud-based (SaaS).
- Hardware-based NGFWs appeal best to large and midsize enterprises
- Software-based NGFWs to small companies with simple network infrastructures
- Cloud-based NGFWs to highly decentralized, multi-location sites or enterprises where the required skill set to manage them is wanting or reallocated.

Feature Set

- Not all NGFW features are similarly available by vendor.
- NGFW features typically consist of
  - inline deep packet inspection firewalls,
  - IDS/IPS,
  - application inspection and control,
  - SSL/SSH inspection,
  - website filtering and
  - QoS/bandwidth management to protect networks against the latest in sophisticated network attacks and intrusion.
- Additionally, most NGFWs offer threat intelligence, mobile device security, data loss prevention (DLP), Active Directory integration and an open architecture that allows clients to tailor application control and even some firewall rule definitions.

Performance

- Because NGFWs integrate many features into a single appliance, they may seem attractive to some organizations.
- However, enabling all available features at once could result in serious performance degradation.
- NGFW performance metrics have improved over the years, but the buyer needs to seriously consider performance in relationship to the security features they want to enable when determining the vendors they approach and the model of NGFW they choose.

Manageability

- This criterion involves system configuration requirements and usability of the management console
- It considers how the NGFW manages complex environments with many firewalls and users and very narrow firewall change windows
- System configuration changes and the user interface of the management console should be:
  1. **comprehensive** - such that it covers an array of features that preclude the need for augmentation by other point solutions;
  2. **flexible -** possible to exclude features that are not needed in the enterprise environment; and
  3. **easy to use** - such that the management console, individual feature dashboards and reporting are intuitive and incisive.

Price

- NGFW appliance, software and cloud service pricing varies considerably by vendor and model
- Prices range from $599 to $80,000+ per device
- Some are even priced by number of users (e.g., $1,100 for 1-99 users to $100,000 for 5,000 users+).
- All, meanwhile, have separate pricing for service contracts
- If possible, do not pay retail prices
- Most vendors will provide volume discounts (the more users supported the less it costs per user, for example) or discounts with viable prospects of further purchases
- Purchase at month-end and quarter-end. Sales people have goals that can be leveraged for pricing to your advantage

Support

- The 2015 Gartner Magic Quadrant on NGFW also rated support -- with quality, breadth and value of NGFW offerings viewed from the vantage point of enterprise needs.
- Given the critical nature of NGFWs, timely and accurate support is essential. Obtain references and ask to speak with vendor clients without the vendor present.
- Support criteria for NGFWs should address responsiveness ranked by type of service request, quality and accuracy of the service response, currency of product updates, and customer education and awareness of current events.

NGFW VENDORS

NGFW Players

The top nine NGFW vendors are

- Checkpoint
- Dell Sonicwall
- Palo Alto
- Cisco
- Fortinet
- HP TippingPoint
- McAfee
- Barracuda

There are other NGFW vendors but these are the top 9

Questions to consider

Questions to consider when comparing these and other NGFW products include:

- What is their product line?
- Is their NGFW for cloud service providers, large enterprises, SMBs or small companies?
- What are the NGFW features that come with the base product?
- What features need an extra license(s)?
- How is the NGFW sold and priced?
- What differentiates their NFGW from other vendor NGFW products?

What features are available in the NGFW?

Non-common NGFW features vary by vendor. So this is where organizations can start to differentiate which NGFWs will work for them, and which won't. For example:

- Dell SonicWall provides security services such as gateway anti-malware, content filtering and client antivirus and antispyware that are licensed on an annual subscription contract. Dell SecureWorks premium Global Threat Intelligence service is an additional subscription.
- Cisco provides Application Visibility and Control as part of the base configuration at no cost, but separate licenses are required for Next Generation Intrusion Prevention Systems (NGIPS), Advanced Malware Protection, and URL filtering.
- McAfee provides clustering and multi-Link as standard features with McAfee Next Generation Firewall license.

What features are available in the NGFW?

- Barracuda requires an optional subscription for malware protection (AV engine by Avira), threat intelligence and for advanced client Network Access Control (NAC) VPN/SSL VPN features.
- Juniper offers advanced software security services (NGFW/ UTM/IPS/Threat Intelligence Service) shipped with its SRX Series Services Gateways that can be turned on with the purchase of an additional license, which can be subscription-based or perpetual. No additional components are required to turn services on/off.
- Checkpoint provides a full NGFW solution package with all of its software blades included under one license. However, it does not provide mobile device controls or Wi-Fi network control without purchasing a different Checkpoint product.

What features are available in the NGFW?

The key message in this comparison is that in addition to the common features, one needs to carefully review those features that require additional licenses and whether they are significant enough to decide on a specific products procurement.

- For example, if you need a DLP feature, those NGFWs that provide it, such as Checkpoint, although offered with over 600 types, you might determine that a full-featured DLP solution might still be required if the Checkpoint is not sufficient.
- The same would apply to web application firewalls (WAF), such as the Dell Sonicwall but again is not a full-featured WAF.

What features are available in the NGFW?

- Another example would be Cisco, although malware protection is available with their network anti-virus/ malware solution, but an additional licenses would be required for their Advanced Malware Protection, NGIPS and URL filtering.
- Barracuda NG Firewall also requires an additional license for Malware Protection (Anti-Virus engine by Avira).
- There are some vendors that provide threat intelligence services as part of the NGFW offering, such as Fortinet, McAfee and HP TippingPoint.
- Juniper's Threat Intelligence Service is shipped with the SRX but needs to be activated with the purchase of an additional license.

How is the NGFW sold, licensed and priced?

- All NGFW products are licensed per physical device. Additional licenses are required for the non-common features stated above.
- Read the T&Cs to determine what services are available in the base NGFW produce and what services require an additional license.
- All NGFW products are priced by scale based on the type of hardware utilized and service contract
- While pricing structure appears disparate, similarities do exist in the lower-end product lines (in other words, the smaller the NGFW need, the simpler the pricing).
- The larger the enterprise and volume purchase potential, the greater the disparity, but also the greater the bargaining power on the part of the customer

Key differentiators between NGFW products

- Checkpoint is the inventor of stateful firewalls. It has the highest block rate of IPS among its competitors, largest application library (over 5,000) than any other, data loss prevention (DLP) with over 600 file types, change management (i.e. configuration and rule changes) that no one else has, and Active Directory integration agent-based or agentless.
- Dell SonicWall has patented Reassembly-Free Deep Inspection (RFDPI) which allows for centralized management for users to deploy, manage and monitor many thousands of firewalls through a single-pane of glass.

Key differentiators between NGFW products

- Cisco ASA with FirePower Services provides an integrated defense solution with greater firewall features detection and protection threat services than other vendors.
- Fortinet lauds its 11-year old in-house dedicated security research team -- FortiGuard Labs -- one of the few NGFW vendors that have its own, since most OEM this activity. Fortinet also purports to have NGFW FortiGate that can deliver five times better performance of comparatively priced competitor products.
- HP TippingPoint is known for its NGFW's simple, effective and reliable implementation. The security effectiveness coverage is high with over 8,200 filters that block known and unknown threats and over 383 zero-day filters in 2014 alone.

Key differentiators between NGFW products

- McAfee NGFW provides “intelligence aware” security controls, advanced evasion prevention and a unified software core design.
- Barracuda purports the lowest total cost of ownership (TCO) in the industry due to advanced troubleshooting capabilities and smart lifecycle management features built into large scaling central management server. The NGFW is also the only one that provides NGFW application control and user identity functions for SMBs.
- Juniper SRX is the first NGFW to offer customers validated (Telcordia) 99.9999% availability of the SRX 5000 line. The SRX Series are also the first NGFW to deliver automation of firewall functions via JunoScript and open API to programming tools. Open attack signatures in the IPS also allow customers to add or customize signatures tailored for their network

How to select the right NGFW

Consider the following criteria in selecting the NGFW vendor and model for your enterprise:

(1) identify the players;
(2) develop a short list;
(3) perform a proof of concept – POC;
(4) make reference calls;
(5) consider cost;
(6) obtain management buy-in; and
(7) work out contract negotiations.
(8) Total cost of ownership (TCO) is also critical.

Lastly, but no less important, consider the skill set of your staff and the business model and growth expectation for your enterprise -- all-important factors in making your decision

NGFW AUDIT


ISACA
Trust in, and value from, information systems
San Francisco Chapter
CyberSizeIT
SF ISACA FALL CONFERENCE
NOVEMBER 9-11, 2015
HOTEL NIKKO-SAN FRANCISCO

Evaluation and Audit of NGFW

- Platform Based – appliance/software/SaaS
- Feature Set – baseline and add-ons
- Performance – NSS Labs results
- Manageability – comprehensive/easy to use
- Threat Intelligence – currency/accuracy/completeness
- TCO – total cost of ownership
- Risk – consider the business model and objectives
- Price – you get what you pay for
- Support – what is support experience?
- Differentiators – what sets them apart?

BIO

Miguel (Mike) O. Villegas is a Vice President for K3DES LLC. He performs and QA's PCI-DSS and PA-DSS assessments for K3DES clients. He also manages the K3DES ISO/IEC 27001:2005 program. Mike was previously Director of Information Security at Newegg, Inc. for five years. Mike is currently a contributing writer for SearchSecurity – TechTarget.

Mike has over 30 years of Information Systems security and IT audit experience. Mike was previously Vice President & Technology Risk Manager for Wells Fargo Services responsible for IT Regulatory Compliance and was previously a partner at Arthur Andersen and Ernst & Young for their information systems security and IS audit groups over a span of nine years. Mike is a CISA, CISSP, GSEC and CEH. He is also a QSA and PA-QSA as VP for K3DES.

Mike was president of the LA ISACA Chapter during 2010-2012 and president of the SF ISACA Chapter during 2005-2006. He was the SF Fall Conference Co-Chair from 2002–2007 and also served for two years as Vice President on the Board of Directors for ISACA International. Mike has taught CISA review courses for over 18 years.