MÄLARDALEN UNIVERSITY
SWEDEN

A COMPARATIVE STUDY OF PALO ALTO NETWORKS & JUNIPER NETWORKS NEXT-GENERATION FIREWALLS

FOR A SMALL ENTERPRISE NETWORK

Mälardalen University Sweden
School of Innovation, Design and Engineering

Thesis for the Degree of Bachelor in Computer Network Engineering

Authors: Simon Persson & Andreas Malmgren
Examiner: Mats Björkman
Supervisor: Hossein Fotouhi
Company Supervisor: [REDACTED]

2016-06-08

Abstract

This thesis is a comparative study of two Next-Generation Firewalls (NGFWs) with the aim to conclude which one is the most suitable for a small enterprise network. The network in question is Company A's Office A[1]. Office A is in the process of upgrading their internal network and with the upgrade a new NGFW will be implemented. The two NGFW platforms that have been researched per Company A's request are Juniper Networks' SRX-series firewalls and Palo Alto Networks' (PAN) PA-series, with focus on the SRX1500 and PA-3020 for a fair comparison. To be able to evaluate different platforms and appliances, the concept of NGFW and what it constitutes has been researched and presented. Both of the NGFW platforms have been tested and compared in terms of ease-of-use and cost analysis. The testing focused on the respective web-interfaces and shows no significant differences between the two NGFWs at a first glance in terms of functionality. However, PAN's web-interface does objectively feel more up-to-date and provides application visibility natively, which Juniper offers as a separate service as part of the centralised management platform, which is excessive for Office A's network. The research and collection of data has been conducted based on Office A's needs and requirements. Third-party research has been collected from NSS Labs and Gartner and serves as a basis for the evaluation. The future network of Office A introduces new services and the general usage will mainly consist of office oriented application based traffic. The evaluation of the research of the two NGFWs and the collection of data, in the context of Office A's network, shows that the PA-3020 would be favoured. The key points are as follows:

- PAN's NGFWs are built specifically for application awareness whereas Juniper are new in the NGFW market and has recently started to add the more advanced application awareness features.
- PAN offers a one-box solution suited for smaller networks such as Office A whereas a Juniper implementation would require additional hardware (VM's) to obtain similar features.
- PAN offers more features in terms of user identification which is a key factor in enabling a true context aware security environment seamlessly integrated and invisible to the users.
- No major difference in cost if a similar set of features are to be implemented, based on non-rebated list prices (additional hardware not included).

[1] Note: Due to confidentiality, the name and details of the company has been anonymised throughout the report.

TABLE OF CONTENTS

List of Figures

List of Tables

1 INTRODUCTION

Current development in the firewall sector is pushing additional protection onto the firewalls with more focus on application-based protection. Some of the need for application-based protection can be attributed to the evolution of Web 2.0 [**1**], where web-based applications and web-based services are becoming increasingly dominant. This is important because web-based services and applications use HTTP and HTTPS as a means of transport which is indistinguishable to a traditional firewall. The more advanced protection services typically requires a high amount of resources resulting in poor network performance, but as better hardware is developed the trend is moving previously separate security services onto the same device. The term Next-Generation Firewalls (NGFWs) is now being heavily pushed by the firewall industry. However, there are no industry defined requirements for a NGFW, but a widely accepted definition has been published by Gartner [**2**]. The NGFWs are similar to their predecessors, Unified Threat Management (UTM) -systems, with the difference of integrating the different technologies and security services achieving multi-gigabit throughput [**3**]. Another important distinction is the requirement of application-aware security. These hardware and software achievements have allowed enterprise networks to adopt the single security device solution previously only available to small and medium businesses (SMBs).

With a wide range of competing firewall manufacturers and the push for NGFWs, it is common for companies to replace out-dated firewalls with newer firewalls better suited for their modern needs and facilitate modern internet speeds. This often means a different firewall platform, which includes a change of operating system and how the device implements the technologies. When migrating or upgrading a firewall, the future firewall candidates needs to be researched and analysed in the context of the intended network. Since the implementation of firewall technologies may differ between manufacturers, an important step in migrating or upgrading a firewall is researching and investigating how to properly utilise and implement new functionality to the new platform, as well as the ease-of-use and cost of the upgrade. To choose a firewall is not a simple task, as the majority of high-end firewalls are similar in what they claim to provide in terms of service and security, with some proprietary differences.

Company A[2] is a company specialised in networking and communication solutions and has recently started working with Palo Alto Networks (PAN) [**4**], a network security company specialised in firewalls. Company A is also a customer of Juniper Networks [**5**], who also manufacture firewalls and, in addition, network equipment ranging from switches to routers for various implementation needs. Currently, the entirety of the internal network infrastructure, with the exception of basic connectivity and security, resides in the Office B branch of Company A. Company A's Office A has made the decision to move Company A's Office A's internal network from the Office B branch to the Office A headquarters. In doing so, the internal network is expected to grow significantly with new services and technologies needed to be implemented. Their current infrastructure will not be able to facilitate the growth of new services and will require upgrades, including the firewall solution. Company A has decided that their new firewall will be a NGFW, specifically either PAN's PA-3020 or Juniper's SRX1500 due to their suitability of performance, functionality and price range in the context of their future network.

[2] Note: Due to confidentiality, the name and details of the company has been anonymised throughout the report

2 PROBLEM FORMULATION

The current firewall, a Juniper SSG-140, used by Company A's Office A is out-dated and marked as End of Life by Juniper [**6**]. This along with the planned future upgrades of the internal network of Office A calls for a firewall upgrade. The choice will be between PAN's PA-3020 and Juniper's SRX1500. The thesis aims to conclude which of the two platforms suits Office A's needs and requirements the best. To determine this, the platforms and respective features needs to be researched, analysed and compared. An analysis of Office A's current and future internal network will be required to put the research of the platforms in context. Furthermore, a platform migration[3] will be needed regardless of firewall as the Juniper SSG-140 is a ScreenOS-based platform, the SRX-series runs JunOS and the PA-series runs PAN-OS. A comparison and assessment of the ease-of-use of JunOS and PAN-OS is necessary, as this will be an integral part of the future network upgrade. This will include both objective and subjective observations of management, features, migration and configuration from a neutral stand-point as these are all new environments for the authors. Since the upgrade will introduce a NGFW to Office A, an understanding of NGFW and its features is required.

As Company A has expressed specific interest in Juniper and PAN, the firewall solution should only consider these two manufacturers, per request from Company A. The thesis' target audience is IT professionals and members of the networking community with at least moderate understanding of the current practices and technologies.

3 BACKGROUND

A firewall is the security gateway to a private computer network and is a crucial component in the protection against unwanted traffic and malicious attacks. A physical firewall refers to a physical device connected to the network performing traffic filtering on ingoing and outgoing packets to and from the network. In contrast, a host-based firewall performs protection on a single device, which could be a personal computer. The norm is having a physical firewall at the edge of a network controlling what traffic is allowed both in and out of the network through a predetermined set of rules as well as a host-based firewall. Network security is crucial in today's networks due to more and more services becoming digital and the need to protect information is growing. With cloud-services becoming the norm, moving data and services locally to the cloud for access introduces new security concerns. Current state-of-practice for network security is a multi-layered approach referred to as defense in depth [**7**] where protection is not only located in one place in a network. This means that a range of security solutions should be used including perimeter firewalls at the edge, Intrusion Prevention System (IPS), monitoring systems, secure web gateway, host-based firewalls and antivirus as well as physical security of all critical network devices. Although firewalls and their services are just one part of the defense in depth approach, it is one of the most critical.

[3] The original intent of the thesis was to explore the migration process from the ScreenOS-based platform to both the JunOS and PAN-OS platforms. However, due to the vast differences between the technologies, this was not viable and would not yield any conclusive results. To compare the two platforms, testing of their performance was also planned, but this proved to be much more difficult than anticipated. In its stead, professional studies of the relevant platforms were used.

3.1 Open Systems Interconnection

The OSI-model [**8**] is a way to standardise how computing systems are built in regards to how they communicate. It is used as a model when designing communication methods for applications to provide interoperability between different systems by using standards. It comprises of 7 different layers each describing a function in the communication process.

The relevant layers in networking are usually layer 2, 3 and 4 and as of recently in network security, a full inclusion of layers 3 through 7.

- Layer 2 - Data Link: Error control on a physical link to link basis.
- Layer 3 - Network: Routing and traffic control. Where the IP-protocols are located.
- Layer 4 - Transport: TCP/UDP-protocol, handles transmission of data segments for reliable communication.
- Layer 5 – Session management between communicating nodes. FTP-protocol, HTTP(S)-protocol and the SSH-protocol operates in this layer.
- Layer 7 - Application: Typically refers to what kind of application is communicating, such as HTTP.

These layers are continuously referenced to when explaining where certain security features operate at.

3.2 Traditional Firewall

Traditional firewalls are generally focused on network security along with protecting the clients, but to a lesser degree. The protection offered is usually focused on layer 3 and layer 4 of the OSI model but can include some limited protection of layer 7.

3.2.1 Stateless Operation

A stateless firewall treats each packet individually with no regards to previous sent or received packets. The effect is a pure static port-based firewall which can only filter packets based on header information, which is source and destination IP as well as port-number and protocol.

3.2.2 Stateful Operation

A stateful firewall allows for remembering the state of a specific session [**9**]. A session is when, for example, a TCP three-way-handshake has been performed and thus established a connection between two end nodes through possibly multiple networks. The stateful firewall tracks packets whenever sessions are established and will remember established sessions in a state table. When a packet arrives that belongs to an established session the packet is allowed without the need to look further into the packet. An example of this would be a user on the inside trying to establish a TCP connection with a server on the outside. The firewall would see the request coming from inside the network and dynamically allow for the return traffic for the specific session to be passed through back into the network. If the server would have tried to initiate the session, the traffic would be blocked.

3.2.3 Security Zones

Security Zones is a fundamental concept in regards to architectural network security [**10**]. The most common zones used with firewalls are Trust zone, Untrust zone and Demilitarized Zone (DMZ), where variations of the names can occur to fit the administrator’s preference. The Trust zone often refers to the private network that the firewall is protecting and considers a trusted network, whereas the Untrust zone often refers to any untrusted network such as the internet. The DMZ is a zone used to share resources, such as a web-server, with untrusted networks. Zones are separated at the firewall and are distinguished by the firewall's interfaces. A firewall then enforces rules based on what security zone the traffic is sourced from or destined to, or both.

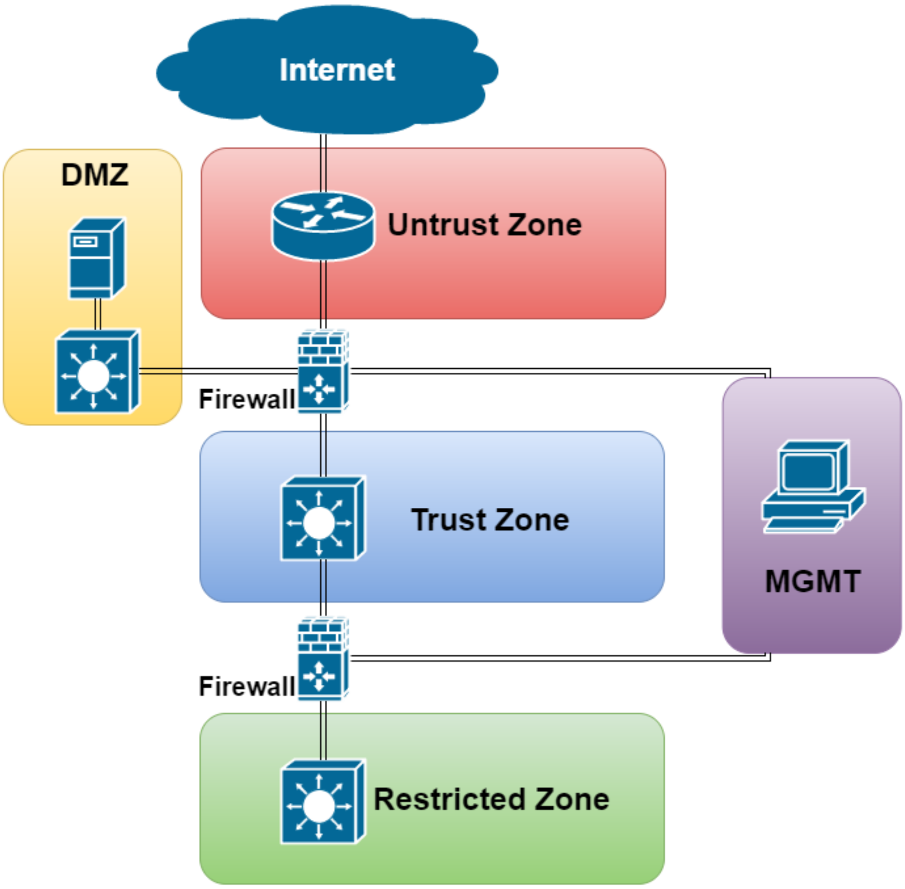


Figure 1 - Example of Logical Security Zones

It is common to add additional separation with more logical security zones when the need arises. An example could be adding another high security zone "Restricted zone" as shown in Figure 1 which could be a zone with a higher level of security compared to the standard Trust zone. The purpose of such a zone would be to facilitate sensitive data that is only available for certain employees and add another layer of defense in accordance to the defense in depth approach. Typically a Management zone exists which grants a higher level of out-of-band access to all of the zones, such as allowing the use of SSH. There is not a one best security model that applies for every network, there are however guidelines and general best practices depending on the purpose of the network.

3.2.4 Security Policies

Security policies are rule-sets that determine how traffic is allowed to pass between security zones. Default behaviour in most firewalls is to allow traffic between the same zone called intra-zone traffic flows whereas inter-zone is traffic flows between different zones and is by default denied. Security policies are used to deny or allow certain traffic based on parameters that can be source/destination zones, IP-addresses, applications, ports or protocols.

3.2.5 Security Policy Approaches

There are some common policy approaches when deciding how to secure a network. They can have drawbacks as well as advantages and needs to be implemented carefully in regards to security concerns and what kind of network is to be protected.

Whitelist approach

The whitelist approach is configuring the rule-sets to specifically allow certain applications/protocols and denying everything else. This is a maximum security approach but can cause problems and management issues due to everything being initially blocked unless specifically allowed.

Blacklist approach

The blacklist approach is configuring the rule-sets to specifically block certain applications/protocols and allowing everything else. This is a more lenient approach blocking known security concerns but allowing everything else, which can cause a security issues.

Hybrid approach

A hybrid approach combines the whitelist and blacklist approach. With this approach it is possible to allow certain applications but deny a subset of an application instead of using a deny all or allow all approach. However, this requires a more advanced set of security features allowing for application awareness and more advanced policies.

3.2.6 Stateful Protocol Analysis

Stateful protocol analysis [**11**] was one of the first methods of providing protection against attacks performed in layers higher than layer 3/4. Stateful protocol analysis enables basic IPS functionality to a firewall's stateful inspection. Stateful protocol analysis is the process of comparing Regular Expression (REGEX) signatures of expected benign vendor-defined protocol behaviour to identify deviations. With the help of databases containing expected behaviour of how protocols and applications interact, the device monitors requests and its corresponding response with a profile of what is expected and any deviations will be flagged. The purpose of flagging a deviation is to perform an action or execute further analysis, if available. The advantage of stateful protocol analysis is adding stateful-capabilities to regular protocol analysis to determine suspicious activity, through knowing the state of the session. An example would be an FTP-session, which in its initial state would only support certain commands such as username and password, whilst when later authenticated would support other commands such as a get request to initiate a file transfer.

3.2.7 Problems with Traditional Firewalls

While traditional stateful firewall functionality is still needed and wanted to a certain extent, it is no longer enough [**12**]. The threats have evolved to a point where the traditional stateful firewalls are unable to stop them. Web-based applications and services are the norm which causes security concerns forcing more protection in the higher layers 4 through 7 where traditional firewalls provide limited protection. Additional security devices are needed to protect a network adding more management and complexity. These additional security devices are, at least, IPS and a secure web gateway.

3.3 Intrusion Prevention System

Intrusion Prevention System (IPS) is a technology used inline to detect and prevent malicious traffic from entering a network. Inline means that the device is placed within the flow of the traffic, such as a choke-point between the traditional firewall and the internal network, where all traffic must pass as shown in Figure 2. When a detection occurs, the IPS can perform actions such as denying the specific packet, connection or host from entering the network by dropping the packet or session as well as notifying the administrator of the attack. Another important aspect is the ability to log the event appropriately. Historically, IPS has been notorious for false positives as the trade-off would be false negatives - which are generally worse [**13**]. However, by placing the IPS behind a firewall, the traffic is already filtered once, reducing the amount of false detections entirely by reducing the amount of traffic to filter.

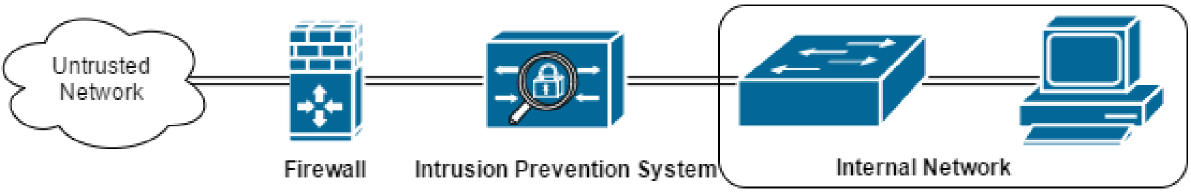


Figure 2 - Example of an inline IPS implementation

Detection methods used by an IPS are a combination of signature-based detection, anomaly-based detection and stateful protocol analysis. Signature-based detection refers to matching of signatures against a signature database of known attack patterns. Anomaly-based detection requires the process of recording a template of network activity such as bandwidth and protocol usage and applying it to detect any deviations from normal activity. A negative aspect would be if an attack is performed during the creation of the template and therefore would be considered normal network activity. Stateful protocol analysis is the same as the previously mentioned traditional firewall technique, although enhanced by the other detection methods as they are interwoven in the way the IPS detects an attack. This means for a single packet, the IPS can use any or all detection methods.

3.4 Secure Web Gateway

A secure web gateway [**14**] is a collection of security solutions which aim to protect user-initiated web traffic. As user-initiated web traffic is generally permitted, it is not heavily inspected by the firewall or the IPS in the same sense that a secure web gateway can inspect the traffic. A secure web gateway solution typically contains URL filtering, antivirus, SSL decryption, application awareness and Data Loss Prevention (DLP).

3.4.1 URL-Filtering

URL-filtering offers another layer of protection or simply a way to enforce company policies. The aim is to deny access to certain websites or categories of websites that are considered to be a threat to security or productivity. URL-filtering uses databases with URLs that are categorised in a manner which an administrator can deny access to gambling sites, where the database for “gambling” contains more than one URL to known gambling sites. Another aspect of URL-filtering is the ability to block dynamic advertisements on websites as they are usually not integrated with the web server providing the wanted content, but imported as an object and retrieved from a third-party web server that may not be trusted.

3.4.2 Antivirus

Antivirus is achieved through inspecting the data of the traffic and using pattern matching to identify malware, either through individual packets or by buffering the individual packets and performing a complete scan of the entire file.

3.4.3 Decryption

The more advanced security devices claim to be able to perform decryption on SSL/TLS-based web traffic (HTTPS). However, while this is true, it is not decryption in the purest sense as a benevolent attack is actually being executed. The different forms of decryption can best be described with three subcategories; SSL Proxy, SSH Proxy and SSL Inbound Inspection [**15**].

SSL Proxy and SSH Proxy shown in Figure 3 are similar in the sense that the security device performs a man-in-the-middle attack on the traffic by establishing either an SSL or SSH connection between both the internal host and the server residing across the proxy device. This is done to enable the device to decrypt and analyse the traffic within the perceived secure connection between the host and the web-server or network device. In addition, SSL Proxy also provides extended security as rogue CA-certificates installed on a host device will never be used to authenticate a server's certificate as the SSL Proxy device is the one authenticating the server certificate and is able to reject them before reaching the host device. The SSL Proxy device will then sign the server certificate with its own certificate and if implemented correctly on the host device, the SSL Proxy will be integrated seamlessly and unbeknownst to the user.

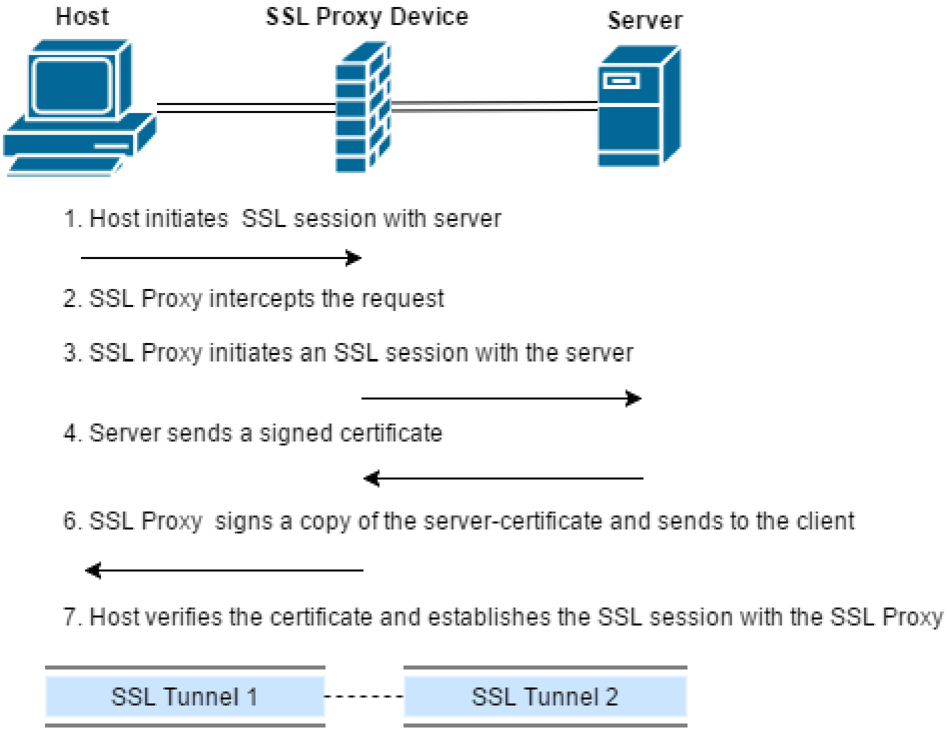

Host
SSL Proxy Device
Server
1. Host initiates SSL session with server
2. SSL Proxy intercepts the request
3. SSL Proxy initiates an SSL session with the server
4. Server sends a signed certificate
6. SSL Proxy signs a copy of the server-certificate and sends to the client
7. Host verifies the certificate and establishes the SSL session with the SSL Proxy
SSL Tunnel 1
SSL Tunnel 2

Figure 3 - SSL proxy operation

SSL Inbound Inspection shown in Figure 4 is performed through obtaining the SSL/TLS certificate used by a server within the network and decrypting any traffic bound for this server. This does not require a dual-tunnel to be set up as the private key is given to the proxy device. As an example, this is favourable as to protect and analyse traffic bound for an internal SSL-VPN, without exposing the device for unnecessary threats coming from the general internet. This also means that the certificate is not only stored in one place, which essentially doubles the potential area of attack. However, if the proxy device is breached, the certificate would be the least of the administrator's concerns. There are also other ways to mitigate certificate theft by storing the certificate in a Hardware Security Module (HSM), not directly accessible if the device is breached.

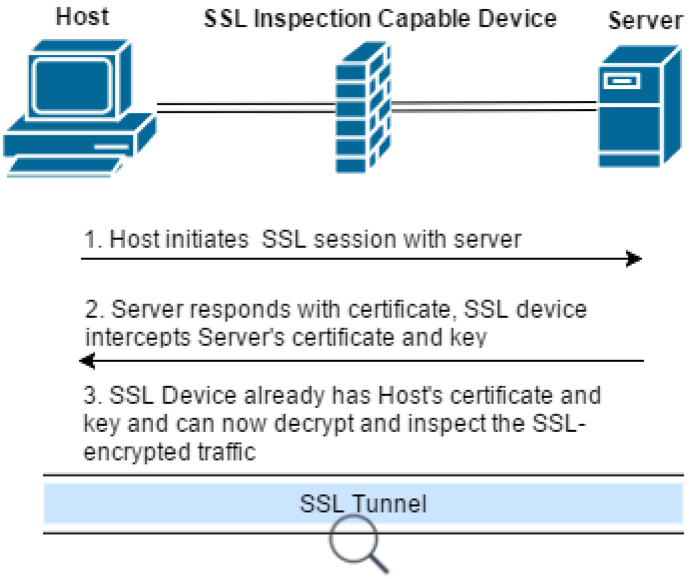

Host
SSL Inspection Capable Device
Server
1. Host initiates SSL session with server
2. Server responds with certificate, SSL device intercepts Server's certificate and key
3. SSL Device already has Host's certificate and key and can now decrypt and inspect the SSL-encrypted traffic
SSL Tunnel

Figure 4 - SSL Inbound Inspection operation

A certificate is an established chain-of-trust between someone, such as a website, and a trusted Certificate Authority (CA), who has validated the identity of the website through signing the web server's certificate with its own Root Certificate, usually by extension of intermediating certificates [**16**]. The certificate contains identity information along with a public key used to encrypt session negotiations sent by the user, which the server uses its own private key to decrypt. The key-pair is asymmetric, which means the private key and the public key are not the same, to ensure the identity of the recipient or sender, the website, depending on which direction the data is being sent. The continuing session uses a symmetric key pair negotiated through the previous step, as asymmetric encryption is resource intensive.

3.4.4 Application Awareness

Application-aware traffic classification is the extension required to provide web 2.0 compatibility. It allows the device to classify traffic based on the application being used rather than the port or protocol it uses. This is done through looking beyond the header and into the data packet itself, matching on data signatures or applying heuristics to determine the application. It provides even more granularity to the protection of a network, the ability to be able to present statistics on application usage and general network performance enhancement [**17**].

3.4.5 Data Loss Prevention

Data Loss Prevention (DLP) is the process of denying or preventing data breaches or data exfiltration of specific or general data [**18**]. DLP covers three main areas: in-use, in-motion and at-rest. In-motion is the main concern for network security devices as it is the last-line of defence against a data leak. In-motion DLP can be achieved through application-aware content filtering or through scanning the content of a file-transfer. At its basic level, in regards to network security, DLP comes in the form of denying users the right to upload to certain web-servers such as a video to YouTube, photos to Facebook or attaching files when sending an email from a private email address. A more advanced method is scanning file transfers for critical information such as credit card numbers and personally identifiable information to prevent monetary and identity theft. This is vital for a business which store customers' information with a real world example being the Sony PlayStation data breach of

2011 [**19**] where personally identifiable information of registered PlayStation Network accounts was extracted.

3.5 Logging

Logging is the process of recording and documenting device and network activity. The activity does not have to be a malicious attack being prevented or detected; it also includes standard benign activity such as the authorisation of network access. Logging is essential to network security as it provides feedback to the network administration that the security equipment actually performs as configured [**20**]. Logs are stored and analysed to serve as a tool for detecting improvements needed, as network security is not a one-time implementation - it is an on-going process.

3.6 Problems with Discrete Security Devices and Solution

All of the previously mentioned security features are wanted and needed in all larger networks. To implement them knowledge is required in several areas; the technologies themselves and several security platforms. Typically small and medium businesses (SMBs) did not have the resources to implement full-fledged network security with all these discrete security devices along with the management required as pictured in Figure 5.

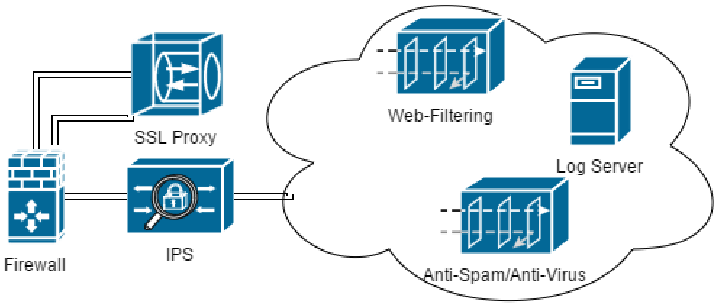


Figure 5 - Multiple Security Devices Solution

This gave way for the Unified Threat Management (UTM) -system [**21**] pictured in Figure 6 which bridged the gap between extensive and expensive network security primarily suitable for SMBs. UTMs are not suitable for larger networks as the trade-off of colocation and unified management is reduced throughput coupled with bad scalability [**3**].

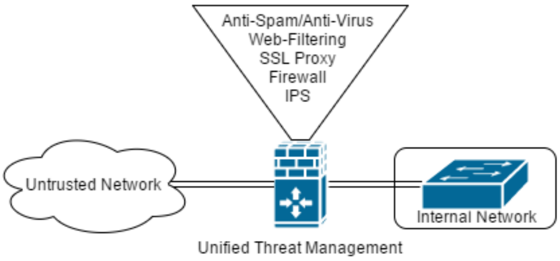


Figure 6 - UTM Solution

4 METHODOLOGY

The focus of the thesis is a comparative study on Juniper's SRX-series and PAN's PA-series in regards to NGFW features along with the challenge of determining which is better suited for Company A's Office A's future network. To accomplish a fair comparison and evaluation, research is conducted on both platforms. The research includes gathering technical and general vendor documentation and reviewing previous research done on the relevant models. An investigation of the meaning, features and concepts involved in a NGFW as well as the different vendor's proprietary features is required to provide a fair base for the evaluation. The research has mainly been aimed at gathering relevant information based on Office A's internal network requirements, but not exclusively, and focused on NGFW features. Office A's internal network and its requirements has been analysed to be able to conduct a fair comparison of the features of the different firewalls. This information has been gathered with the help of Office A's employees.

Since the firewall upgrade will include a migration of platform, the migration process has been investigated using resources of best-practice in regards to migrating. The relevant models; the current in-place SSG-140 running ScreenOS, Palo Alto's PA 3020 running PAN-OS and Juniper's SRX1500 running JunOS are tested and compared from an ease-of-use perspective to see which platform has accomplished an easy to use NGFW, which is vital for a security solution to mitigate human error. These tests have been performed on the equipment Office A provides in their own lab along with available demos of virtualized environments for the NGFWs.

5 CASE STUDY

This section contains our findings of PAN's and Juniper's NGFW, their features and a comparison of tests, costs as well as analysis of reports made by third-parties on both platforms.

5.1 MIGRATION

When upgrading firewalls from a traditional port-based firewall to the application-aware NGFWs there are some considerations to be made. Planning and analysing every step of the process is important to complete the project efficiently and to mitigate errors. A common way to successfully complete a project is to follow a method.

5.1.1 PDCA

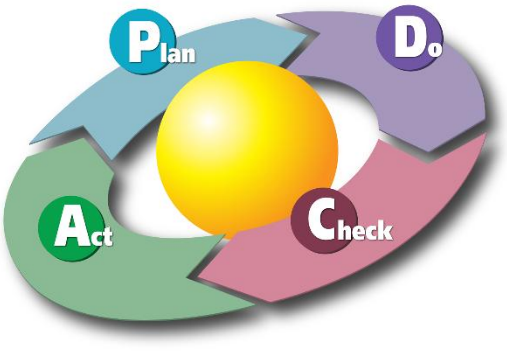


Figure 7 - Plan-do-check-act (PDCA) [22]

The Plan-Do-Check-Act (PDCA) is a methodology that is widely used and can be applied to most projects. It consists of four stages, as the name states, plan, do, check and act. It is meant to help see a project through in a planned and structured manner [**23**]. The process can be cycled numerous times during different stages of a project. When applied to planning a migration of firewalls the first stages can look like the following demonstrated in Table 1.

Table 1 - Preparation Phase PDCA Cycle

Plan	Auditing the existing implementation of the firewall such as configuration, services and policies. As well as general security concerns. Researching the new NGFW and its features and how to implement them. Planning how the existing policies will be implemented on the new platform with extended features.
Do	Convert the old policies and services to the new platform. Implement the new features.
Check	Test the new implementation.
Act	Change or add based on previous step.

A new cycle can then be used with the same principles to cover the necessary practical steps of implementing the new NGFW; however this is not to be performed in this thesis. Table 2 shows an example of an implementation PDCA cycle.

Table 2 - Implementation Phase PDCA cycle

Plan	Plan the actual physical migration Plan testing of implementation
Do	Implement the firewall
Check	Test the new implementation Check that it is working as intended
Act	Change or add based on previous step.

The contents of the thesis is limited to the Plan stage in the preparation phase (Table 1) to be able to decide what NGFW suits the network the best.

5.2 Next-Generation Firewall

In summary, a Next-Generation Firewall (NGFW) is a firewall with more advanced security features integrated within the device. The term is relatively new and is not industry defined. This means there are different interpretations of what constitutes a NGFW.

5.2.1 Definition & Features

In 2009 Gartner released a document defining the NGFW [**2**]. According to this definition there are a set of features considered to be the minimum for a NGFW.

Besides standard firewall features the key ones are:

Integrated IPS

Older types of firewall often offer this as a feature, but it is usually a limited IPS and doesn't compare to the advanced stand-alone IPS devices available. The NGFW definition requires an integrated advanced IPS. The requirement states that the IPS is not supposed to be a stand-alone IPS simply built into the firewall, where the firewall performs its operations separately to the IPS. The firewall and the IPS are supposed to be integrated in a single flow of packet processing where the firewall can enforce rules based on input from the IPS.

Application awareness and full stack visibility

Application awareness refers to the ability to recognise what kinds of applications are being used in the network by being able to inspect up to the application layer. The ability to recognise applications based on application layer information presents new opportunities to granularly control traffic based on applications that were previously not recognisable by older types of firewalls. Application awareness is very important in today's networks.

Extrafirewall intelligence

The ability to implement rules based on external sources such as user-based rules with information from Active Directory.

Centralised Management

Centralised management is another important feature for NGFWs that offers easier and better management of large networks and systems. Most NGFW vendors offer their own centralised management.

Logging

Logging is a core element to any security implementation, whether it is network related or not. Gartner's definition of a NGFW places heavy emphasis on the importance of easy-to-read graphs and tables which summarises the information gathered through logging. This places further emphasis on a well-structured Graphical User Interface (GUI) for an effective network security implementation. Log-management is sometimes an overlooked part of network administration but an important one. Logs can help troubleshoot, prevent threats and monitor a network. As activity on today's networks is constantly escalating, the amount of logs generated and handled can be immense and it is common to have specialised equipment for log-management. Therefore log-management is yet another important feature that NGFWs should offer and can help identifying things such as what applications are used the most and which user is doing what.

5.2.2 Context awareness

Application awareness is the core of what is considered a NGFW. It was one of the first requirements of becoming a NGFW along with IPS functionality at wire-speed. However, the term application awareness has somewhat surpassed its initial value and has now been improved by context awareness, which not only includes application awareness, but also provides context as in who, what, when and how. Who is the user trying to initiate a session, what is the application and recipient, when is a time-stamp and how is the device used by the user itself. Through extensive knowledge of the intended use, the NGFW can apply even more granular policies and special requirements for access which can be essential to preserve data confidentiality. An example could be a specific software patch needed to access certain network resources due to exploitable security vulnerabilities.

5.2.3 Integrating UTM Functionality

The major difference between UTMs and NGFWs is, as previously mentioned, the integration rather than just the colocation of the technologies allowing for multi-gigabit throughput while simultaneously not impeaching on security breadth. Historically, SMBs have not had the same need for gigabit throughput as the bottleneck would be their internet connection rather than the security. However, with the ever growing market of cloud services and the availability of gigabit ISP connections, even SMBs can require high throughput to facilitate the services provided beyond their internal network. The new NGFW claim to integrate UTM-functionality within the firewall while simultaneously meeting throughput demands that standalone UTM-devices could not match. The definition of what constitutes UTM functionality within a NGFW may vary depending on the vendor. Juniper's SRX-series defines their integrated UTM as host-based protection such as antivirus and web-filtering. PAN does not use the term UTM as they try to define themselves as something not related to UTMs, the functionalities are however equivalent.

5.2.4 NGFW Advantages

- High throughput with activated application layer protection
- Single device suitable for enterprises
- Simpler management
- Reduces management
- Scalability

5.2.5 Juniper SRX-Series

The SRX-series is Juniper's line of next-generation firewalls. They offer a wide range of SRX-models suited for branch-office environments up to data-centre environments. The SRX-models are relatively new in the NGFW market. The SRX, as most firewalls, uses the concept of zones to logically separate different security zones of a network.

J-web

J-web is Junipers web-interface that was introduced in 2004 and has been under continuous development since. The web-interface is meant to simplify management and configuration for administrators and can also supply graphs of information that are otherwise not available using the CLI. The web-interface uses the NetConf protocol to communicate with the devices to apply configuration made via the web-interface. The NetConf protocol is defined in [**24**].

Junos Space

Junos Space is a Network Management Solution (NMS) [**25**] that aims to automate and simplify management for a range of devices offered by Juniper. It offers centralised network management for efficient and scalable management. Junos Space consists of three different software components: Junos Space Network Management Platform, Junos Space Management Applications and Junos Space Software Development Kit (SDK).

Junos Space Network Management Platform offers management centralised services such as inventory management, configuration templates, configuration file management and software image management.

Junos Space Management Applications consists of multiple applications that offer a wide range of services for monitoring, reporting and troubleshooting as well as management. The Junos Space SDK provides the ability for customers to create their own applications for specific needs.

Junos Space Security Director [**26**] is an application for Junos Space providing centralised security management for SRX-devices. With the help of the Security Director, granular policies and application security can be applied in a scalable manner. Security Director policies take precedence over local policies. The Security Director in unison with the Log Director also provides application visibility providing administrators insight into what applications are being used in the network. Junos Space Log Director is an application for Junos Space for centralised and scalable log-management as well as monitoring of devices. The application receives information and logs from the Log Collector which in turn receives logs from all SRX-devices across the network.

Juniper Sky Advanced Threat Prevention

NGFWs offer integrated threat prevention such as anti-malware and IPS, they are however limited to signature-databases bound to packet inspection. Juniper's Sky Advanced Threat Prevention (Sky ATP) [**27**] is a cloud-based service dedicated to malware and virus detection and prevention and is integrated with the SRX1500. The Sky ATP performs even deeper inspection of suspicious content with multiple antivirus engines. It can also perform analysis in a sandbox environment to test and observe potential threats to determine whether malicious files have been identified. If a legitimate threat has been identified, the information and signature is cached and sent to the SRX-device to automatically and dynamically stop the threat as well as distribute new signatures to all Sky ATP enabled networks. There are two versions of licensing for Juniper's Sky Advanced Threat Prevention; free and premium. The free version is available to customers with software support contracts and allows executable (EXE) files with a limit to 2500 files a day per device. The premium licence can be purchased and performs a more advanced inspection of a wide range of file-types with a limit of 10 000 files a day per device. Currently Sky ATP is only available on the SRX1500 model. To receive the updated security feeds, a Spotlight Secure Connector VM needs to be installed and integrated as a specialised node in Junos Space Security Director.

AppSecure

With the increase of more web-based applications running over port 80, the traditional way of identifying services and applications based on ports is no longer sufficient. AppSecure is a suite of services dedicated to identifying applications and then performing some kind of action such as blocking it, applying QoS or simply gathering statistics on the application. The suite consists of modules that perform different functions. The Application Identification (AI) is the central part of the suite identifying applications and then the modules can perform actions based on them. The AI can identify applications in a few different ways such as patterns in the application layer.

Summary of the modules from [**28**]:

AppTrack – Logging and statistics of applications traversing the SRX
AppFW – Enforcing rules on applications: permit, deny, redirect. Possible to mix rules and allow Facebook web but deny Facebook applications such as games.
AppQoS – Quality of Service engine to apply QoS rules based on applications.
UserFW – Firewall rules applied on a per-user basis (Active Directory).
SSL Forward Proxy – Creates SSL sessions between the hosts and the hosts' targets allowing the SRX to inspect the traffic.

The modules are configured using rule-sets with matching criteria.

Application Identification (AI)

The AI is the central part of the AppSecure suite that identifies applications. Without the AI all of the other components would not have any information to work with. The AI uses five different methods for identifying applications.

- Signature-based matching
- Heuristic matching
- Predictive session matching

- Application system cache
- Level3/4 application entries

User Firewall (UserFW)

UserFW is the user identification available natively on the SRX platform. User identification is primarily done through Windows Management Instrumentation (WMI) polling the Microsoft Active Directory server for login events, mapping user and correlating groups to an IP address. The WMI client does not support multiple users on a single PC, which would include remote desktop users through Windows Terminal Server. Other methods available are Unified Access Control (UAC) integration with the Pulse Secure Network Access Control (NAC) and captive portal for HTTP traffic.

Application Firewall (AppFW)

AppFW is the part of the suite that enforces rules on application information passed on from the AI. It can function as an extension of the normal stateful firewall operation. The stateful engine handles the normal procedures of handling sessions based on IP-addresses, ports, protocols and zone-restrictions while in addition the AppFW can apply application and user-based rules on top of these rules.

AppTrack

AppTrack is a logging and statistics feature aimed to provide an insight in what applications are traversing the network along with information about session statistics of the applications. It can be implemented as a standalone feature without any other application-aware features. It is implemented on zones and exported via syslog for analysis.

Application Layer Gateway (ALG)

The ALG is a gateway operating in the application layer for certain applications or protocols. Its purpose is to aid some applications to properly work through the firewall that otherwise has a tendency to get blocked by the stateful engine. The problem of the protocols can be the behaviour of how it handles multiple sessions with ports. As the stateful engine is keeping track of what ports the session is using, it can block genuine use of port changes that are characteristic of some protocols. The ALG solves the problem by inspecting the control-channel of the protocols and “pin-holing” the applications and their ports using NAT-functions to circumvent the nature of the stateful engine [**29**].

The applications that are supported are however limited. Commonly the ALG uses the protocols’ RFCs to determine appropriate use which can cause issues if amendments are made to a protocol’s operation.

Intrusion Prevention System

As a NGFW the SRX has an integrated IPS. Even though the AppSecure suite can control what applications are allowed to communicate it does not provide protection against viruses that can be present in allowed applications. Along with the regular operation of a stateful firewall that permits or denies traffic based on allowed ports and IP-addresses, which still is an important defense, modern networks also require the use of an IPS.

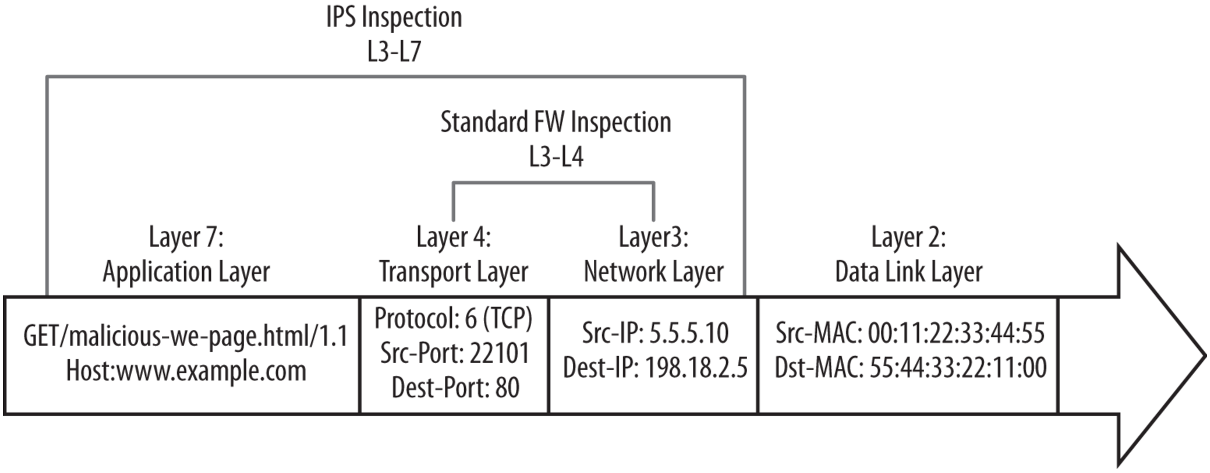


Figure 8 - IPS Inspection vs. Standard FW Inspection [**30**]

The IPS' role is identifying malicious activity in the payload of packets at the application layer, as shown in Figure 8, that the other features cannot detect. Actions include dropping malicious traffic and informing the firewall component to block the IP from where the malicious traffic originates.

The SRX IPS can detect malicious traffic in a few ways with attack objects. Attack Objects consist of two types; protocol anomaly Attack Objects and signature-based Attack Objects [**31**].

Protocol anomaly Attack Objects looks for anomalies in the protocols being inspected using RFCs as a reference. If a protocol is being used in a way that the RFC does not match, it may be a sign of a malicious attack.

Signature-based Attack Objects consist of a range of patterns that can be used to detect certain known attacks. These two Attack Objects are provided and updated by Juniper through licences but it is possible to create custom Attack Objects.

AppDDoS

Application DDoS is a relatively new form of DDoS-attack that is targeting application services. The AppDDoS protection service within the IPS of the SRX can mitigate these forms of attacks [**31**]. The characteristics of AppDDoS are somewhat similar to standard DDoS attacks, by abusing applications hosted by servers to disrupt them. Since the attack is essentially traffic that has been approved by the firewall to communicate with a server providing application services other forms of detection is needed.

The AppDDoS protection is configured to protect certain servers. The IPS inspects traffic as normal and monitors connection thresholds, if a certain amount of connections has been reached within a timeframe the traffic is then monitored for matching of contexts. The contexts are basically different types of thresholds that can be configured within an AppDDoS profile that also contains information about what application is to be protected. If the threshold(s) of the context is reached actions are then enforced that can close connections and block future attempts from the same source. It is also possible to apply rate-limiting for sessions reaching the thresholds.

UTM

The SRX-series offer a built in UTM. In the SRX UTM is defined as any application layer inspection that is not the IPS according to Juniper [**32**].

The UTM consists of:

- Antispam - Filters unwanted e-mails based on block-lists.
- Antivirus - Protection against different kinds of viruses using signature databases. The antivirus features offers scanning with Kaspersky's engine, Sophos engine or Juniper's express engine.
- Web filtering - Blocks certain websites based on their categories, or individually chosen websites.
- Content filtering - Content filtering is a form of data loss prevention that can filter certain types of files not allowed to pass as well as filter based on MIME-types.

The relevant model for a fair comparison with PAN is the SRX-1500. Table 3 shows technical specifications according to Juniper's data sheet for the device.

Table 3 - Juniper SRX 1500 Technical Datasheet [**33**]

Firewall Throughput (stateful)	Up to 9 Gbps
Application Visibility and Control	4 Gbps
Recommended IPS	3 Gbps
NGFW Features (IPS + AppID)	1,5 Gbps
Connections per second	50 000

5.2.6 Palo Alto Networks PA-series

PAN classifies their different NGFW security features into three different main categories: App-ID, User-ID and Content-ID. Threat Prevention is the fourth category which utilises the functionality of the previous three to enforce the network security policies set by the administration.

App-ID

App-ID is the five-step process of application traffic classification within PAN-OS. The steps are executed as defined in [**15**]:

1. A policy check to identify if the traffic is allowed at its most basic level such as source and destination IP. If traffic is not allowed, it is dropped and no further ID is performed.
2. Signature-based detection to identify the application based on unique characteristics of the application or session. Port-number is also identified to determine if standard or non-standard ports are used. Another policy-check is performed based on the basic application findings and, if allowed, further application analysis and threat scanning is performed.
3. If the previous application identification attempts detect SSL or SSH encryption and a decryption policy exist, the traffic will be decrypted and tried again.
4. Decoders for known protocols are applied to determine if any tunnelling applications are being used such as BitTorrent over HTTP and if they conform to the overlaying protocol's specifications. Decoders are also responsible for mapping dynamic port usage for protocols such as FTP as well as support for NAT traversal. This is the ALG-functionality within the Palo Alto NGFW. Policies are applied accordingly and if allowed, further threat scanning and content-ID is performed. Available protocol decoders as of update 424: HTTP, HTTPS, DNS, FTP, IMAP SMTP, Telnet, IRC (Internet Relay Chat), Oracle, RTMP, RTSP, SSH, GNU-Debugger, GIOP (Global Inter-ORB Protocol), Microsoft RPC, Microsoft SMB (also known as CIFS).
5. Heuristics or behavioural analysis may be used for applications not able to be identified through signatures and protocol analysis.

User-ID

User-ID enables the NGFW to integrate directory services to map users and their corresponding groups with firewall policies [**15**]. Directory service integration is, however, only part of the puzzle. To be able to enforce the policies, the device has to be able to map the User-ID to an IP address which can be done through several means, both internal and external. The base of User-ID requires mainly a Windows domain to be used within the network.

Server Monitoring

Server monitoring requires a User-ID agent running on either a Windows-based domain server or integrated within PAN-OS. This method monitors login events through the logs on Microsoft Exchange Servers or domain controllers. The events can be Kerberos ticket grants or renewals, file and print server connections or Exchange server access. To be able to use the logs, correct logging configuration for successful account login is required on the target devices. This method is the recommended base-method of User-ID mapping as the majority of network users will use at least some the services generating a successful account login event.

Client Probing

Client probing is useful in an environment where IP addresses changes regularly. Natively on the PAN-OS User-ID agent, probing can be configured using Windows Management Instrumentation (WMI). This does limit the possibilities of probing as NetBIOS probing is not supported and requires an external Windows-based User-ID agent. Probing is the act of asking every learned IP address periodically to validate the user of the system, which is done by default every 20 minutes (probing itself is not on by default). Another advantage of Client Probing is when a new IP address is learned by the firewall for which it has no User-ID, a request can be sent to the agent and a probe can immediately be sent to map the User-ID with the IP address. The downside to client probing is the extra network traffic it produces and grows in the same manner as the number of known IP addresses in the internal network.

Port Mapping

In a virtualised environment, such as Microsoft Terminal Server or Citrix environments, many users use the same IP address and are distinguished by the source-port used when sending the traffic. A user-to-address mapping in this type of environment is not possible and to solve this Palo Alto Networks Terminal Services Agent must be installed on the target device to serve as a mediator between the virtualised environment and the firewall. PAN-OS also offers an XML API for terminal servers not supporting the proprietary software and can be used to send user mapping information from local events, most commonly login and logout events.

Syslog

Syslog monitoring is similar to Server monitoring in the sense that it parses log-files for authentication-events from general Network Access Control (NAC) mechanisms. This type of User-ID mapping is arguably the most effective method as some type of NAC is always used within a secure network environment. Examples would be 802.1x authentication for wired or wireless access and is integrated with the syslog implementation of the network.

Captive Portal

Captive Portal is a security mechanism which forces users to login in order to access web-based services. This is done through the web browser and is independent to the OS used by the user.

GlobalProtect

PAN's GlobalProtect can be integrated with User-ID to provide user mapping information for VPN-based users directly.

PAN-OS XML API

As previously stated, if other methods are incompatible with providing sufficient User-ID mapping, PAN-OS XML API may be used to implement User-ID compatibility. This is done by creating a script and utilising the PAN-OS XML API commands to send the necessary data appropriately.

Content-ID

Content-ID [**34**] is PAN's common name for general NGFW functionality including DLP, URL-filtering, anti-malware and Command and Control detection. The purpose of Content-ID is to identify the content of the traffic passing through the NGFW through pattern-matching from a wide range of databases such as WildFire, Microsoft Active Protections Program (MAPP), private Malware and Vulnerability research and custom signatures allowing for specific internal requirements such as for DLP.

Threat Prevention

Threat Prevention [**15**] is the general protection provided by the NGFW and uses the functionality of App-ID, User-ID and Content-ID to enforce security policies.

Wildfire

WildFire [**15**] is PAN's Virtual Sandbox environment used to automatically detect and create signatures for unknown malware. WildFire can be used to execute several file types or visit an unknown website in a virtualised environment and observes the process for any suspicious activity which could indicate an attempted attack. If found malicious, any URL would be added to the Palo Alto Networks Database (PAN-DB) and categorised as malware and any executable file type would have a signature made and added to the PAN-DB of known malicious signatures and available to their customers. A WildFire-subscribed customer would get the signature in as low as 5 minutes and Threat Prevention subscribed customer would receive the signatures in 24-48 hours as part of the antivirus update.

WildFire has two available implementations where one is the cloud-based service and the other is the WF-500 appliance hosted within the customer's network. The two implementations can be used simultaneously if, for example, private documents are not allowed to leave the private network whilst other threats are sent to the public cloud. Furthermore, there are certain file types not supported by the WF-500 such as Android Application Package (APK) files. WildFire supports email link analysis by allowing the firewall to extract the link within the email and forward the URL and session information without forwarding the email itself.

The full list of supported file types are as follows [**35**]:

- PE - Portable Executable files. This includes .exe, .dll, .FON (Microsoft font files, .exe files with only font resources) and general compiled executable code. Forwarding of PE-files does not require a WildFire subscription
- APK - Android Application Package (APK) files. Not supported in the WildFire private cloud
- Flash - Adobe Flash files and embedded Flash content
- JAR - Java Archive
- PDF - Portable Document Format

- MS-OFFICE - Microsoft Office files
- HTTP/HTTPS links within emails

Table 4 shows performances and technical specifications for the PA-3020 according to Palo Alto's datasheet.

Table 4 - PA-3020 Technical Datasheet [**36**]

Firewall throughput (App-ID enabled)	2 Gbps
Threat prevention throughput (IPS+App-ID)	1 Gbps
New sessions per second	50 000

Licenses

Relevant licenses from [**15**].

- Threat Prevention: Provides anti-malware, vulnerability protection and basic WildFire support.
- Decryption Mirroring - Provides the ability to mirror decrypted traffic to a traffic collection tool for analysis and/or archiving.
- URL Filtering: Allows the creation of security policies based on URL-filtering as well as database subscription.
- Virtual Systems: License required to enable multiple virtual systems on the PA-3000 series firewalls.
- WildFire: Extended premium WildFire support.

Panorama

Panorama [**37**] is PAN's centralised management platform and utilises a similar web-interface available on the NGFW itself, the addition being able to administer multiple NGFWs at once. Administrators are able to create and apply templates of various scales catering to the network needs depending on role and placement of the NGFW. Local policy changes do take precedence over Panorama policies. Panorama is available through the PAN M-series appliances or as a VM.

Single Pass Parallel Processing Architecture

Single Pass Parallel Processing (SP3) Architecture [**38**] is PAN's solution to achieve high throughput by only performing each action on a single packet only once. It is comprised of two components, the Single Pass software and the Parallel Processing hardware. This is what completes the integration of the different technologies rather than just colocation as UTMs repeatedly performed the same action on a packet due to the lack of cooperation between the technologies. An example would be the worst case scenario where forward lookup and protocol identification would be performed for firewall policies, IPS and URL-filtering independently.

5.3 Company A's Current Network

Office A is acting as a branch office to Office B, meaning Office A's network is small with only a few network devices providing basic connectivity and security. Security consists of the Juniper SSG-140 firewall at the edge along with a Blue Coat ProxySG as a secure web gateway.

Services

Currently, Office A internally only provides a Domain Controller for their Active Directory environment and a Microsoft Lync server for mail services.

Juniper SSG-140

The Juniper SSG140 is a security appliance made by Juniper and runs on the operating system called ScreenOS and is geared toward a branch-office deployment. The SSG140 has some characteristics in common with an NGFW, such as an integrated IPS but is not considered an NGFW. It is however important to note that the IPS, its deep inspection and signatures is limited and does not compare to newer integrated IPS in the SRX or PA series. This kind of IPS is sometimes referred to as "IPS lite" [**39**] compared to "full IPS" that the NGFWs offer. The IPS is a part of the UTM-system and uses protocol anomaly detection and stateful protocol signatures. The signatures are available as a paid service shown in Table 6 and come in different packs based on the different needs a company might have. Juniper decided to move their firewall solutions from a separate operating system namely ScreenOS, to the same operating system their routers and switches use, JunOS. Juniper announced in 2015 that this product is considered "End of Life" (EOL) which means the product is being phased out and will no longer be available for purchase and vendor-support will eventually cease [**6**].

Table 5 showing technical specifications for SSG-140.

Table 5 - Technical Datasheet SSG-140 [**40**]

Firewall throughput	350 Mbps
Maximum concurrent sessions	48,000
Signature Database (IPS)	200,000+
Firewall packets per second	90,000

Table 6 - Licenses for SSG-140 [**40**]

Base	Signatures for protection against worms targeted against client/server
Client	Protection for clients
Server	Protection for servers
Worm mitigation	A more comprehensive defense against worm attacks

Blue Coat ProxySG

The Blue Coat ProxySG provides secure web gateway functionality in the form of SSL proxy, anti-malware, user-ID directory service integration, application awareness and data loss prevention. The Blue Coat is considered a web security gateway. Since the SSG-140 does not offer modern IPS functionality a separate device is needed to complement the firewall.

5.4 Company A's Future Network

Currently, Office A is acting as a branch office connected to the headquarters in Office B where the main network infrastructure resides. Company A has decided to upgrade the network in the Office A to handle its own network infrastructure. Company A is by definition a small business with around 100 employees overall and around 30 in Office A. Company A has decided that the new network design will follow an enterprise model for high flexibility, scalability and availability.

New services to be introduced with the upgrade.

- Active Directory
- SSL-VPN (Pulse Secure)
- File server
- FTP-server
- Print server
- Sales system
- Finance system

- Service desk system

The network upgrade will introduce new services hosted on-site. The plan is for the network to handle all of the internal operations of Company A for both Office A and another office, Office C.

Topology

The new network topology introduces a couple of new security zones. Figure 9 shows how the network will be logically segmented into four security zones. The topology is a logical overview of the intended network. The APS is a DoS-mitigating device.

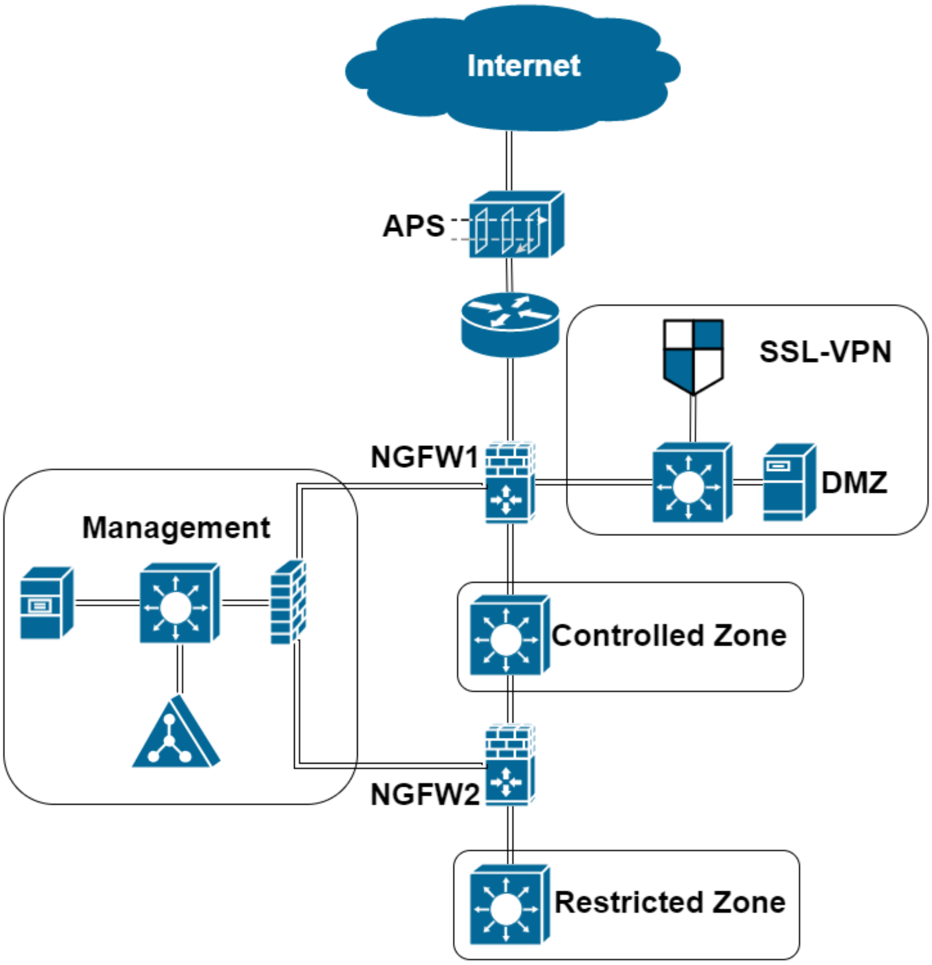


Figure 9 – Company A's future logical security topology

The different zones have different roles, with the roles comes policies that dictate how devices located in a zone can communicate with devices in another zone.

Controlled Zone represents the general internal network.

- Employees/Clients
- Printers
- Print-server
- Service-desk system

DMZ representing shared resources with Internet and the internal network

- Web-server
- SSL-VPN

Management Zone

- Active Directory
- Syslog

Restricted Zone: This zone is regarded a high security zone containing sensitive data and information.

- File & FTP server
- Backup
- Systems for sales and finance

Requirements

As the new network will handle a considerable more amount of activity and services the choice of the new firewall must be made accordingly.

Some key requirements for the new network regarding the future firewall are as follows:

- High availability
  - Office A is planning on using two firewalls in a high availability setup
- Application visibility & context awareness
  - Office A is mainly an office handling sales and finance systems and development of cloud-services. This means there is an emphasis on application security.
- High throughput with IPS features activated

5.5 COMPARISON & RESULTS

When testing and analysing products, it can be helpful to follow guidelines. The SANS institute "Real-World Testing of Next-Generation Firewalls"-white paper [**41**] puts forth some common steps for testing a NGFW functionality. The relevant areas for this section are:

- Ease of installation
- Ease of use
- Usability of management console or interface
- Ability to detect attacks
- High availability, throughput and accuracy
- Price
- Support

In this section the relevant points are the ease of installation, ease of use and usability of management interface will be explored on both platforms. Both firewalls web-interfaces will be tested by configuration some basic security.

5.5.1 Platform Testing

Generally, most of the configuration on network devices is done with the help of the Command Line Interface (CLI) of the device in question. This is true for firewalls too, but due to advancements in firewall technologies and the integration of previously separate technologies, configurations are becoming increasingly complex. The need for a web-interface as a visual aid to enhance the holistic view is perhaps even more important than the extensive features available since if not configured correctly, the device will not operate properly. This is especially true for NGFWs due to their multistep protection suite integrating a multitude of different technologies to achieve network security and business productivity.

Another important factor is the emphasis on application control and visibility, web-interfaces if done properly can help visualise application usage and network flows. Web-interfaces for network devices have been around for a long time but not much focus or effort has been made for user-friendly GUIs. This is changing and can be an important feature for buyers of firewalls. This section will compare and highlight differences in the platforms implementations of their CLI as well as their web-interfaces. A general basic configuration will be configured to test how JunOS J-Web and Palo Alto's PAN-OS web-interface manages to aid an administrator and then be subjectively judged from an inexperienced point of view.

Ease of installation / Initial configuration

The two devices initial setup and configuration is identical. After mounting both devices and powering them on two choices are offered, configure the device via web-interface or the CLI. To configure the device with the CLI a computer is connected with an RJ-45 cable and a DB-9 adapter to the console port on the device.

To configure via the web-interface a computer is connected to the management port with an RJ-45 cable. An IP address for the computers Ethernet-connection is then configured to be in the 192.168.1.0/24 network. Both the SRX and PA device management IP address is preconfigured with 192.168.1.1. After the network configuration on the computer the web-interface is available via a web-browser "http://192.168.1.1". In both cases a login is required, with the default admin login "root" with no password for the SRX and login "admin" password "admin" for Palo Alto.

Usability of interface

Due to the history of the two vendors they share a lot of common features and architecture. This section will explore the CLI and web-interface of PAN-OS and JunOS.

Command Line Interface

Both JunOS and PAN-OS have two CLI modes; operational mode and configuration mode. Operational mode, the default mode when connecting to the devices where the administrator can monitor and troubleshoot along with viewing the current status of the device. To enter configuration mode the command "`configure`" is entered.

In the configuration mode is where the entire device's configuration is made.

Table 7 - Comparison of action and command in CLI

	Configure items	**Show information**	**Apply configuration**
JunOS	set	show	commit
PAN-OS	set	show	commit

Basic use of the CLI is as shown in Table 7 very similar. Command usage is hierarchical in both systems and can be demonstrated using paths in the configuration hierarchy.

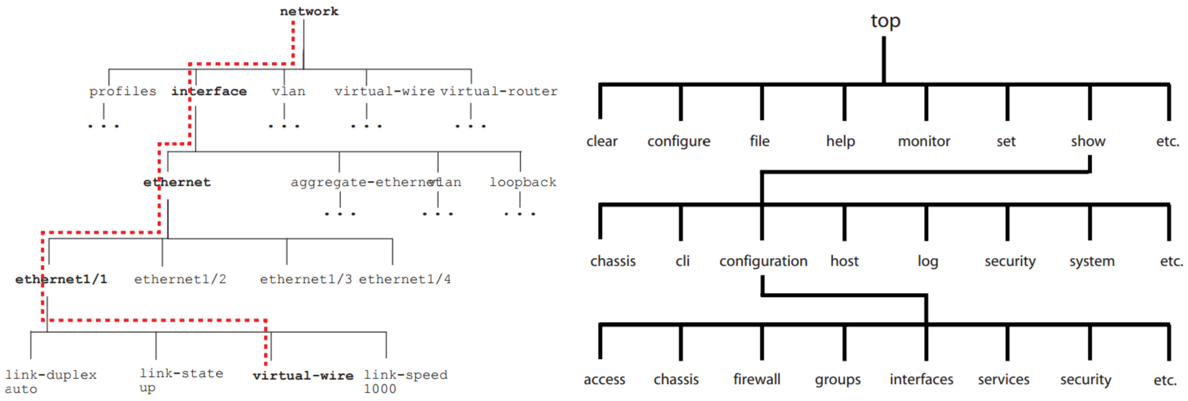


Figure 10 - Hierarchy of the CLI, PAN-OS (left) [**42**] *and JunOS (right)* [**43**]

An example how a *set* command looks like in configuration mode (Table 8) demonstrates how the hierarchy is navigated when configuring an IP address on an interface.

Table 8 - JunOS CLI Command Example

JunOS	`set interfaces ge-0/0/0 unit 0 family inet address 1.1.1.1/24`

Traversing through the hierarchical tree starting at interfaces where all of the interfaces are available. Further under the interfaces multiple options appear all the way down to the bottom of the hierarchical tree where IP address is configured.

The same configuration in PAN-OS (Table 9) looks slightly different but the idea is the same starting at the top hierarchy tree for networking, moving down to interfaces and their options all the way down to the IP address. The differences are mainly name-conventions and where certain options and required inputs are placed in the hierarchy.

Table 9 - PAN-OS CLI Command Example

PAN-OS	`set network interface ethernet ethernet1/1 layer3 ip 1.1.1.1/24`

As seen in Table 10 and 11, the output of the configuration is similar yet again.

Table 10 - JunOS Configuration Output Example

```
interfaces {
        ge-0/0/0 {
                unit 0 {
                        family inet {
                                address 192.168.1.2/24;
                        }
                }
        }
}
```

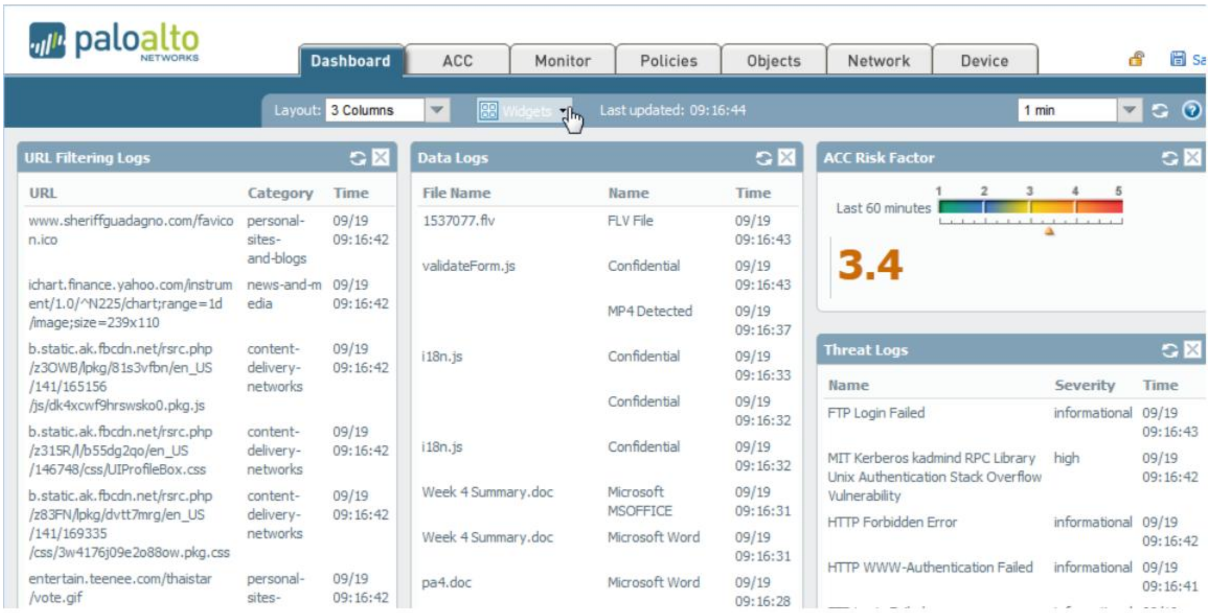
Table 11 - PAN-OS Configuration Output Example

```
network {
      interface {
            ethernet {
                  ethernet1/1 {
                        layer3 {
                              ip {
                                    1.1.1.1/24;
                              }
                        }
                  }
            }
      }
}
```

Web-interface

This section is dedicated to introducing the web-interfaces configuring some basic security features highlighting the differences of the two platforms. It will serve as a basis for a subjective comparison by the authors with the perspective of ease of use for an inexperienced administrator.

The PAN-OS dashboard (Figure 11) is made out of widgets that show certain information such as system information and logs. It is easily configurable by simply closing the widgets or adding them through the drop-down menu to the administrators liking. The layout can be customised and the widgets can be dragged to any position.



Layout: 3 Columns

Last updated: 09:16:44

1 min

URL Filtering Logs

URL	Category	Time
www.sheriffguadagno.com/favicon.ico	personal-sites-and-blogs	09/19 09:16:42
ichart.finance.yahoo.com/instrument/1.0/^N225/chart;range=1d/image;size=239x110	news-and-media	09/19 09:16:42
b.static.ak.fbcdn.net/rsrc.php/z3OWB/lpkg/81s3vfbn/en_US/141/165156/js/dk4xcwf9hrswsko0.pkg.js	content-delivery-networks	09/19 09:16:42
b.static.ak.fbcdn.net/rsrc.php/z315R/l/b55dg2qo/en_US/146748/css/UIProfileBox.css	content-delivery-networks	09/19 09:16:42
b.static.ak.fbcdn.net/rsrc.php/z83FN/lpkg/dvtt7mrg/en_US/141/169335/css/3w4176j09e2o88ow.pkg.css	content-delivery-networks	09/19 09:16:42
entertain.teenee.com/thaistar/vote.gif	personal-sites-	09/19 09:16:42

Data Logs

File Name	Name	Time
1537077.flv	FLV File	09/19 09:16:43
validateForm.js	Confidential	09/19 09:16:43
	MP4 Detected	09/19 09:16:37
i18n.js	Confidential	09/19 09:16:33
	Confidential	09/19 09:16:32
i18n.js	Confidential	09/19 09:16:32
Week 4 Summary.doc	Microsoft MSOFFICE	09/19 09:16:31
Week 4 Summary.doc	Microsoft Word	09/19 09:16:31
pa4.doc	Microsoft Word	09/19 09:16:28

ACC Risk Factor

Last 60 minutes 1 2 3 4 5

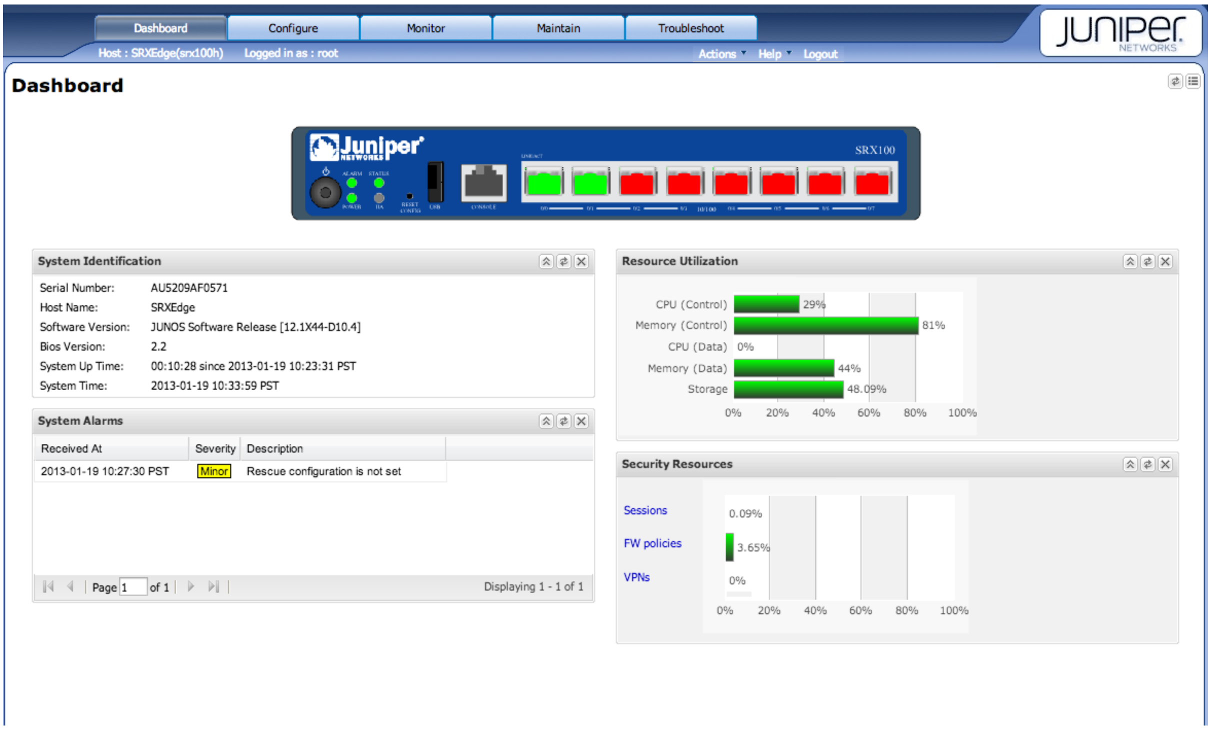
3.4

Threat Logs

Name	Severity	Time
FTP Login Failed	informational	09/19 09:16:43
MIT Kerberos kadmind RPC Library Unix Authentication Stack Overflow Vulnerability	high	09/19 09:16:42
HTTP Forbidden Error	informational	09/19 09:16:42
HTTP WWW-Authentication Failed	informational	09/19 09:16:41

Figure 11 - PAN-OS Web-interface Dashboard [**44**]

The SRX J-web dashboard (Figure 12) is similar in functionality with different widgets containing information about system status and alarms with the options to customise. The interfaces on the picture showing what model is operating are clickable for fast configuration of interfaces. Similarly to PAN-OS the widgets can also be moved by dragging them.



System Identification

Serial Number:	AU5209AF0571
Host Name:	SRXEdge
Software Version:	JUNOS Software Release [12.1X44-D10.4]
Bios Version:	2.2
System Up Time:	00:10:28 since 2013-01-19 10:23:31 PST
System Time:	2013-01-19 10:33:59 PST

System Alarms

Received At	Severity	Description
2013-01-19 10:27:30 PST	Minor	Rescue configuration is not set

Page 1 of 1 Displaying 1 - 1 of 1

Figure 12 - JunOS Web-interface Dashboard [**45**]

The dashboards of the two web-interfaces are similar in layout, options and information. The SRX J-Web appears to have problems conforming to the web-browser's window size when resizing the browser window. The PAN-OS web-interface offers a few more options of widgets in the dashboard.

At the top of both web-interfaces there are multiple tabs. Each of the tabs serves different purposes and are logically separated based on functions such as policies, monitoring and the dashboard.

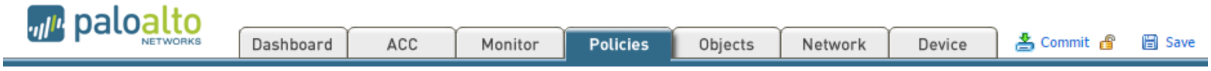


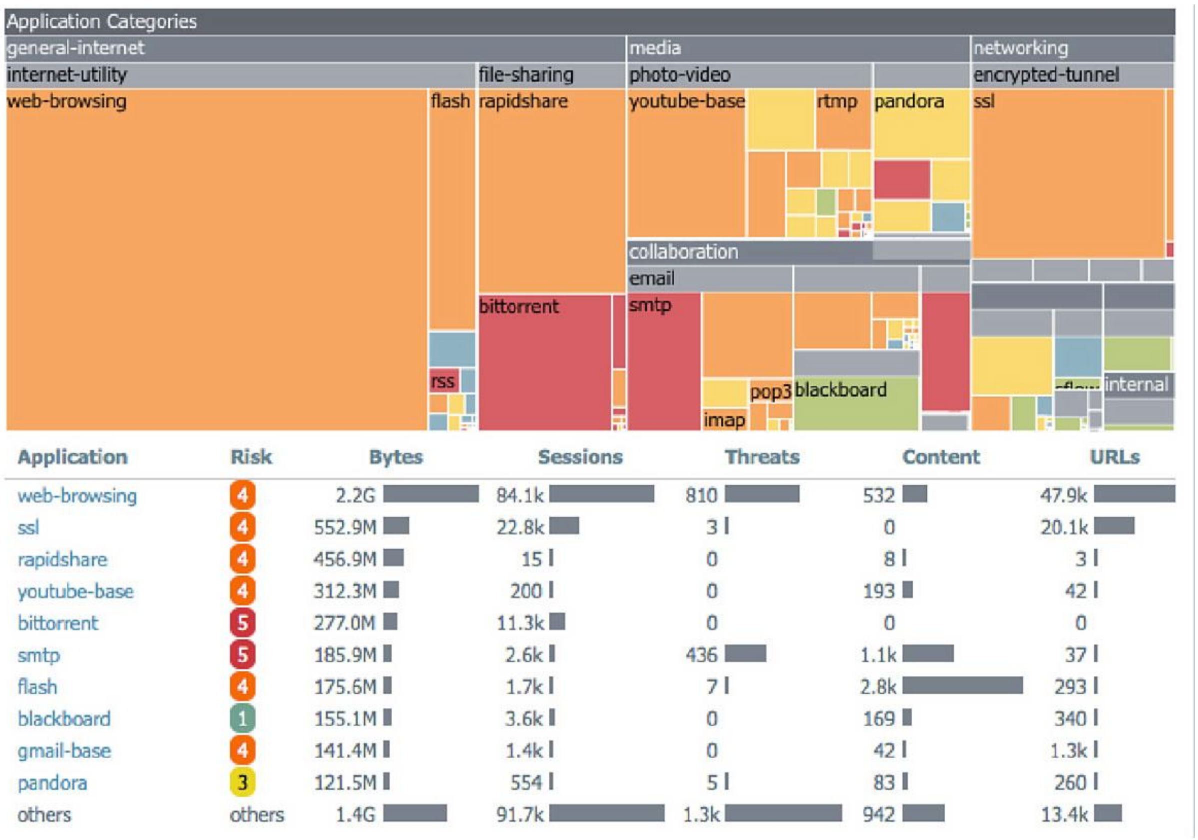
Figure 13 - PAN-OS Web-interface Top-level Tabs

The PAN-OS (Table 13) web-interface has seven tabs named after their function with one being the previously covered dashboard.

- The Network tab handles all network configurations such as interface configuration, tunnels and zones.
- The Policies tab is for configuration of security policies between zones, NAT rules, QoS rules, DoS protection, policy based forwarding and decryption.
- The Objects tab is for configuring and viewing the applications database, application filters, security profiles for anti-virus, URL filtering and file blocking. Amongst many other forms of objects
- The monitor tab is for monitoring of logs of different kinds such as threat logs, traffic logs, application monitoring.
- The Application Command Center (ACC) tab contains information and visibility with graphics for the network traffic, threat activity and blocked activity. It is possible to customise it extensively since the tabs inside the ACC are widgets.

- The Device tab is for configuring and viewing system settings such as administrative users, syslog, licenses and other management services.

The ACC tab (Figure 14) is a highly customisable monitoring tool tailored for application visibility. With the help of Palo Alto’s application identification the ACC tab can show multiple detailed statistics on application usage providing a clear view of the network without the need of third-party devices. The SRX-series does not offer anything similar within the SRX-device itself.



Application	Risk	Bytes	Sessions	Threats	Content	URLs
web-browsing	4	2.2G	84.1k	810	532	47.9k
ssl	4	552.9M	22.8k	3	0	20.1k
rapidshare	4	456.9M	15	0	8	3
youtube-base	4	312.3M	200	0	193	42
bittorrent	5	277.0M	11.3k	0	0	0
smtp	5	185.9M	2.6k	436	1.1k	37
flash	4	175.6M	1.7k	7	2.8k	293
blackboard	1	155.1M	3.6k	0	169	340
gmail-base	4	141.4M	1.4k	0	42	1.3k
pandora	3	121.5M	554	5	83	260
others	others	1.4G	91.7k	1.3k	942	13.4k

Figure 14 - PAN-OS Web-interface ACC [**46**]

The J-web interface has five tabs (Figure 15) with one being the previously covered dashboard.

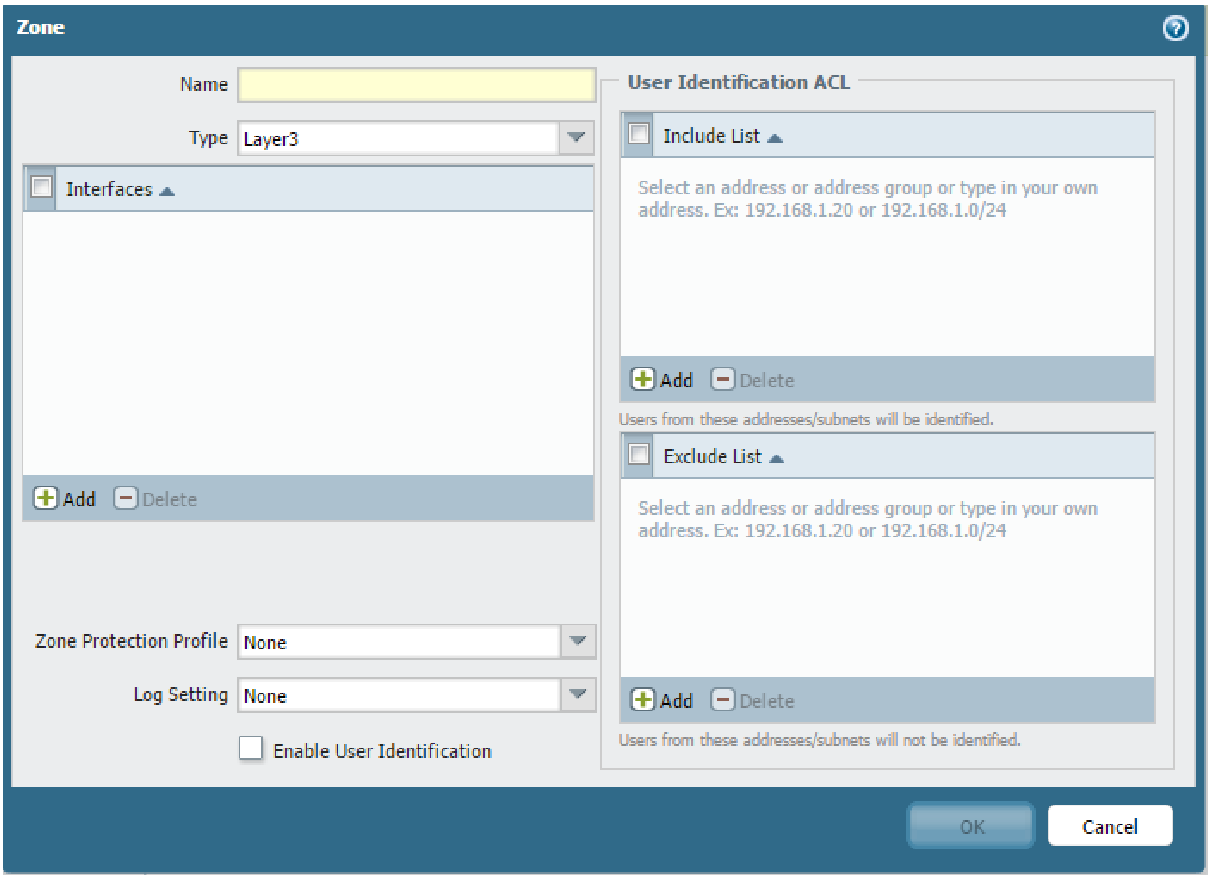
Figure 15 - JunOS Web-interface Top-level Tabs

- The Configure tab is where the entire configuration is made. Inside this tab there are numerous sub tabs divided by their function area such as interfaces, routing and security that it itself contains configuration options for the IPS, security policies and the UTM.
- The Monitor tab contains several different areas of monitoring such as security monitoring for policies, NAT logs and routing logs.
- The Maintain tab is for managing the device such as licensing information and software upgrades.
- The Troubleshoot tab contains a number of features for troubleshooting such as ping (ICMP), traceroute and an option to use the CLI via the web-interface.

The main difference is that JunOS J-web interface has basically all configuration options under one tab where PAN-OS has separated some configuration options based on their roles in either Policies, Objects or the Network tab.

Creating a security zone

With the zone creation window security zones are configured and the process is straight-forward on both platforms with the minimum requirements of interface attached, a name for the zone and for JunOS the type of zone is entered in the text-boxes. PAN-OS zone creation window shown in Figure 16 and J-web in Figure 17.



Name

Type Layer3

Zone Protection Profile None

Log Setting None

□ Enable User Identification

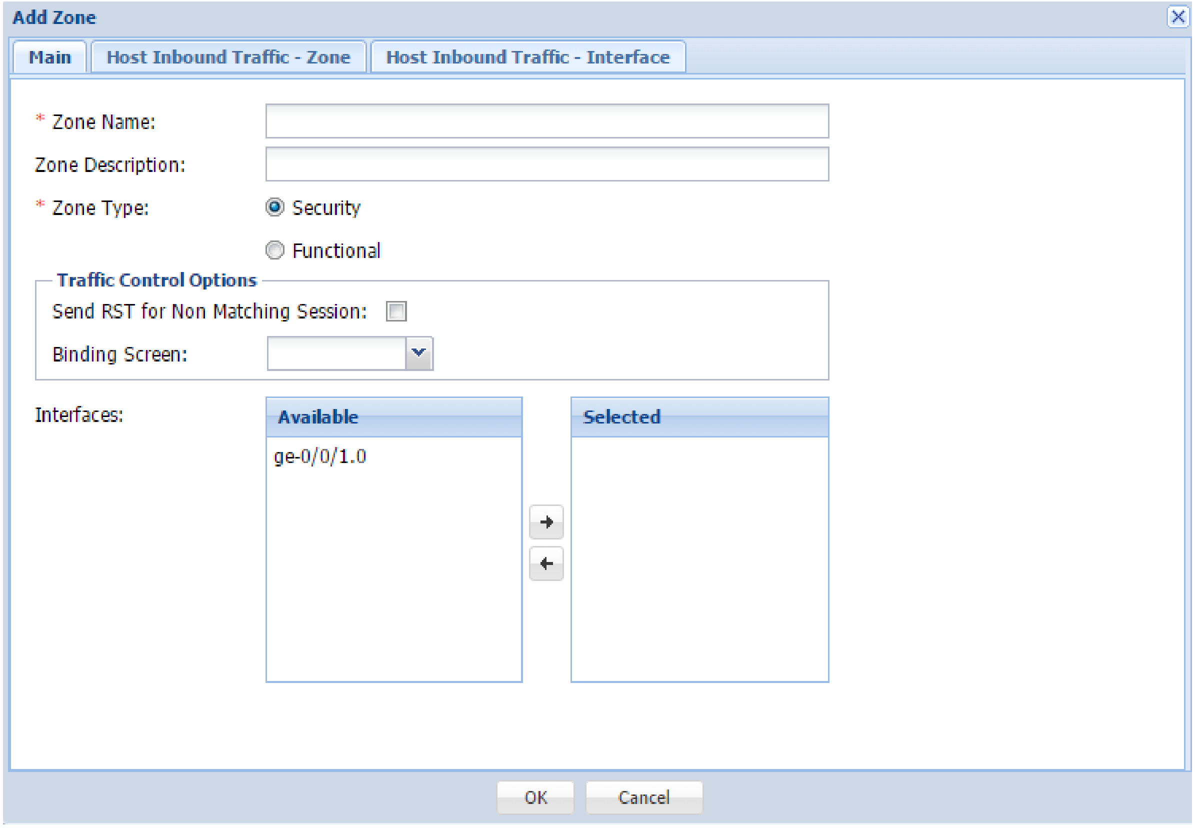
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will be identified.

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will not be identified.

Figure 16 - PAN-OS Web-interface Create Zone


Add Zone

Main | Host Inbound Traffic - Zone | Host Inbound Traffic - Interface

* Zone Name:

Zone Description:

* Zone Type: ● Security ○ Functional

Traffic Control Options

Send RST for Non Matching Session: □

Binding Screen:

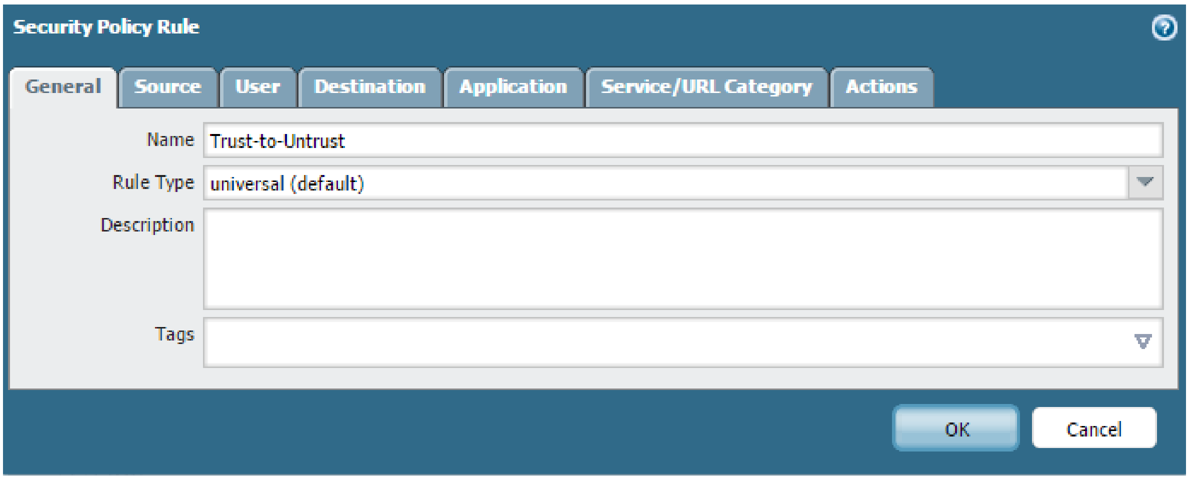
Interfaces:

Available	Selected
ge-0/0/1.0	

Figure 17 - JunOS Web-interface Zone Creation

Creating a policy

The PAN-OS web-interface policy rule creator (Figure 18) consists of seven tabs to configure the different parts of a policy.


Security Policy Rule

General | Source | User | Destination | Application | Service/URL Category | Actions

Name: Trust-to-Untrust

Rule Type: universal (default)

Description:

Tags:

Figure 18 - PAN-OS Web-interface Policy Rule Creation

When for example a service is to be selected for the policy the administrator is given the possibility to define a new service directly in the window as opposed to going into Objects>Services>Add, as seen in Figure 19.

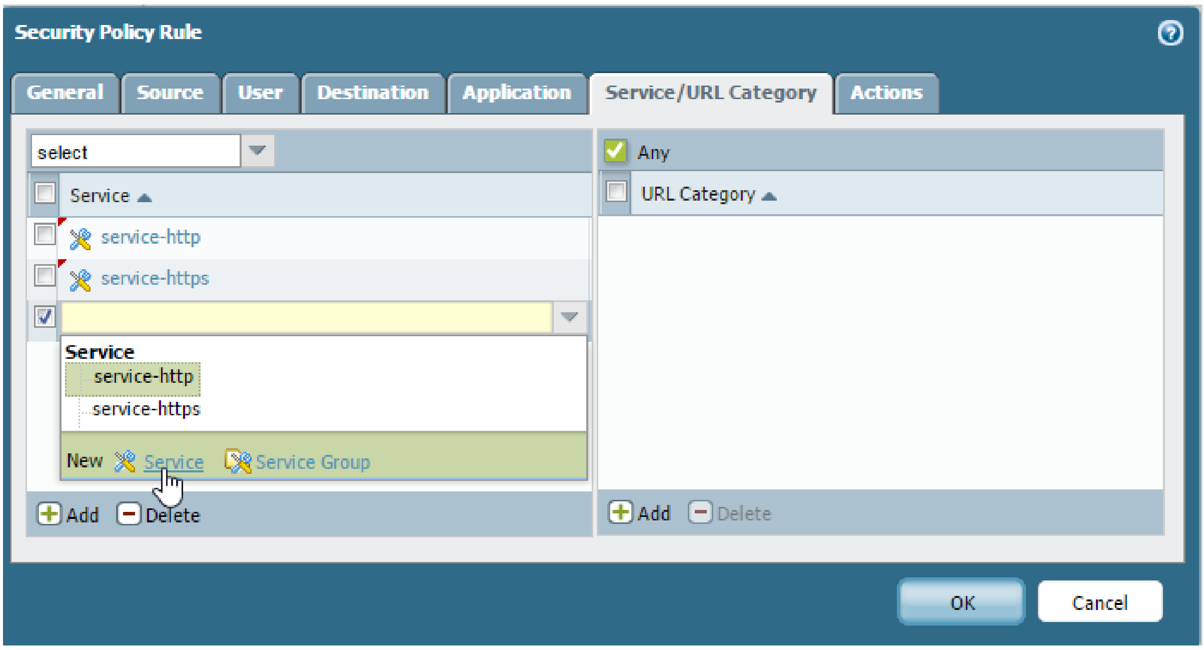
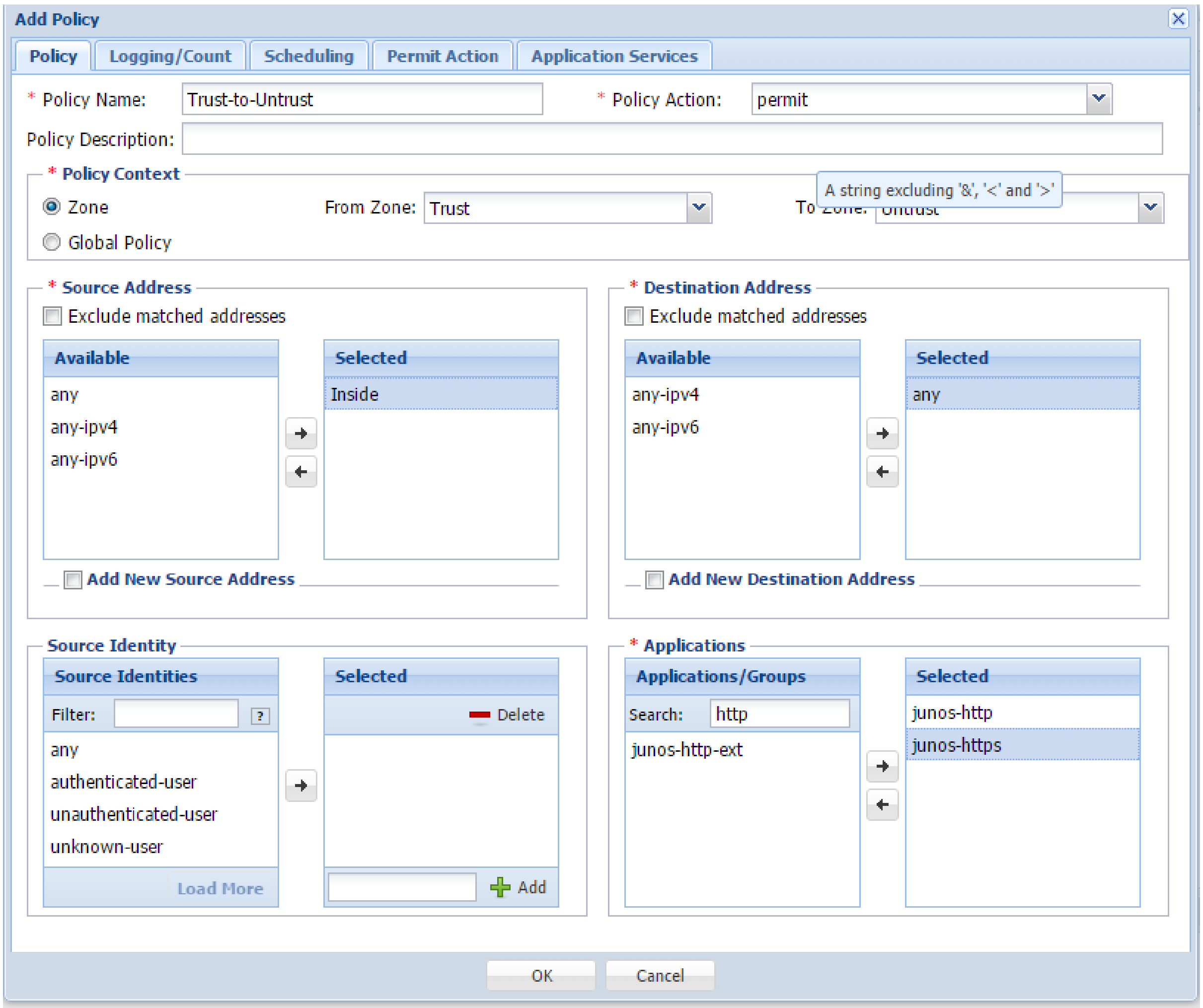


Figure 19 - PAN-OS Web-interface Security Policy Service

The policy creator (Figure 20) in JunOS j-Web shows most of the configuration choices directly in the main window giving the administrator a clear view of details of the policy.



* Policy Name: Trust-to-Untrust

* Policy Action: permit

Policy Description:

● Zone

From Zone: Trust

To Zone: Untrust

Source Address – Selected: Inside

Destination Address – Selected: any

Applications – Search: http

Applications – Selected: junos-http, junos-https

Figure 20 - JunOS Web-interface Policy Creation

Most of the configurations of various features are made in a similar fashion on the two web-interfaces. The main differences are navigating the web-interface and where different options are located.

5.5.2 Gartner

Gartner Magic Quadrant by Gartner Inc. is a process where analysts collaborate and produce market research reports in different areas of technology. Gartner uses a five-step research process [**47**] with proven methods to provide fair and independent analysis of products.

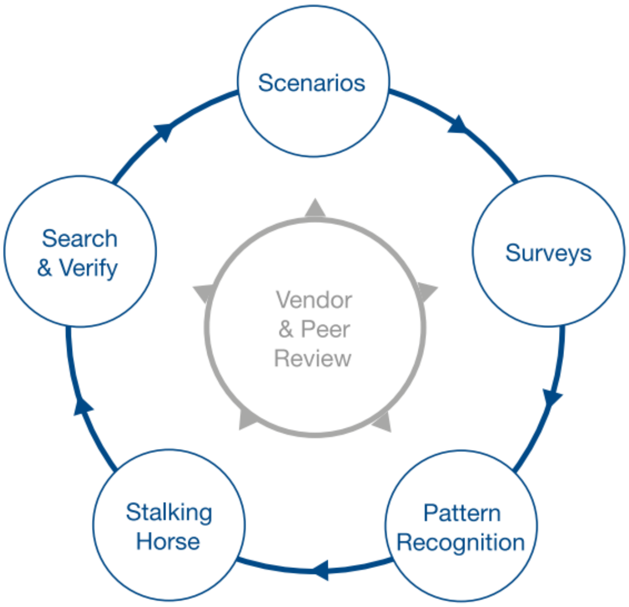


Figure 21 - Gartner Research Process [**47**]

In 2015 Gartner published a Magic Quadrant (MQC) report for enterprise network firewalls [**48**] analysing seventeen vendors with two of them being Juniper Networks and Palo Alto Networks. The result of the report shows where vendors are placed in four categories presenting strengths and weaknesses. The analysis is based on two criteria; completeness of vision and ability to execute.

The four categories [**49**]:

Niche Players - Vendors that scored low on both of the criteria, commonly smaller vendors. Can however offer products in niche markets.

Visionaries - Scores low on ability to execute but have good vision. Have a good understanding of the future market but fail to execute.

Challengers - Large vendors that rates high on ability to execute but lower on completeness of vision. Typically established vendors that are unlikely to change their vision.

Leaders - Scoring high on both criteria showing an ability to execute and have a good vision prepared for the future, typically large vendors.

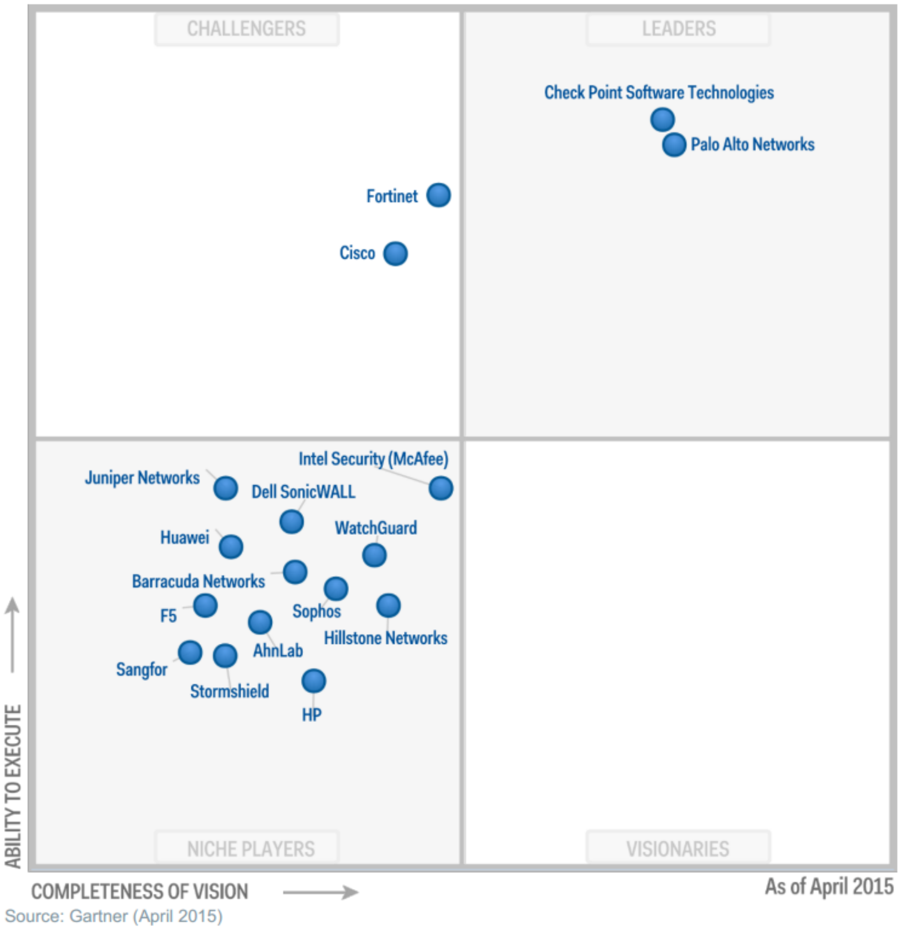


Figure 22 - Gartner MQC Enterprise Firewall Results (April 2015) [**48**]

In the 2015 report PAN was named a leader scoring high on ability to execute and completeness of vision indicating that their technology alongside their vision is amongst the best. Gartner sees Palo Alto as a leader because of consistency in test results for the features and its high focus on NGFW functionality.

Juniper Networks was placed in the niche category scoring relatively high in ability to execute as an established vendor but failed in completeness of vision. According to Gartner, Juniper plays a niche role in firewalls in an enterprise setting due to reports of on-going replacement of Juniper security devices in enterprise networks and that it is mostly chosen because of the Juniper platform instead of its features.

A part of the report is based on a survey made by Gartner that is answered by customers and users of security products with Gartner's opinions and conclusions of the results.

Table 12 - Gartner MGQ Evaluation: Palo Alto & Juniper Networks [**48**]

Gartner MGQ evaluation	**Strengths**	**Cautions**
Palo Alto Networks	-Consistently rated highest in application awareness, high quality of the IPS and ease of use -The integration of the firewall and IPS along with App-ID is regarded highly in	-Marketing from PAN can be overly optimistic about supposed performances of features that may not seem realistic to customers -Gartner is cautious about PAN's

	inspection effectiveness compared to other vendors -Survey shows PAN consistently most mentioned as strongest NGFW vendor -Wildfire advanced threat appliance is very popular with customers removing need of third-party solutions	promises in the endpoint market and the consequences that may arise when trying to enter it -Limited third-party product support -Survey says clients want better log handling at scale, with some complaints about management of scale
Juniper Networks	-Businesses already operating juniper in their infrastructure benefit by using Junos Space for their devices -Higher end SRX models rates highly in performance, benefits data-centres -Offers a range of branch-office devices -Great stateful throughput for the price -Threat intelligence platform with third party support	-Not seen as in the forefront of security development, joining the NGFW market late -Clients expressed need of support for stability improvements -Survey indicates enterprises wants a separate platform for security products -Junipers security market share has been in decline

5.5.3 NSS Labs

NSS labs is an information security company performing analysis and in-depth testing on security products. One area of testing NSS labs performs is on NGFWs. Their testing shows security effectiveness, network performance and a total cost of ownership (TCO). The security configurations done by NSS Labs follows the vendors' own best-practices with out-of-the-box standards. It does not reflect on the ability of the users as it aims to test the product on its capability, rather than the expertise of network security administrators. The TCO is based on initial purchase, maintenance, installation, upkeep and management. With the results of their testing NSS Labs offers a cost analysis based on performance testing and TCO to show where vendors stand in regards to cost per protected Mbps.

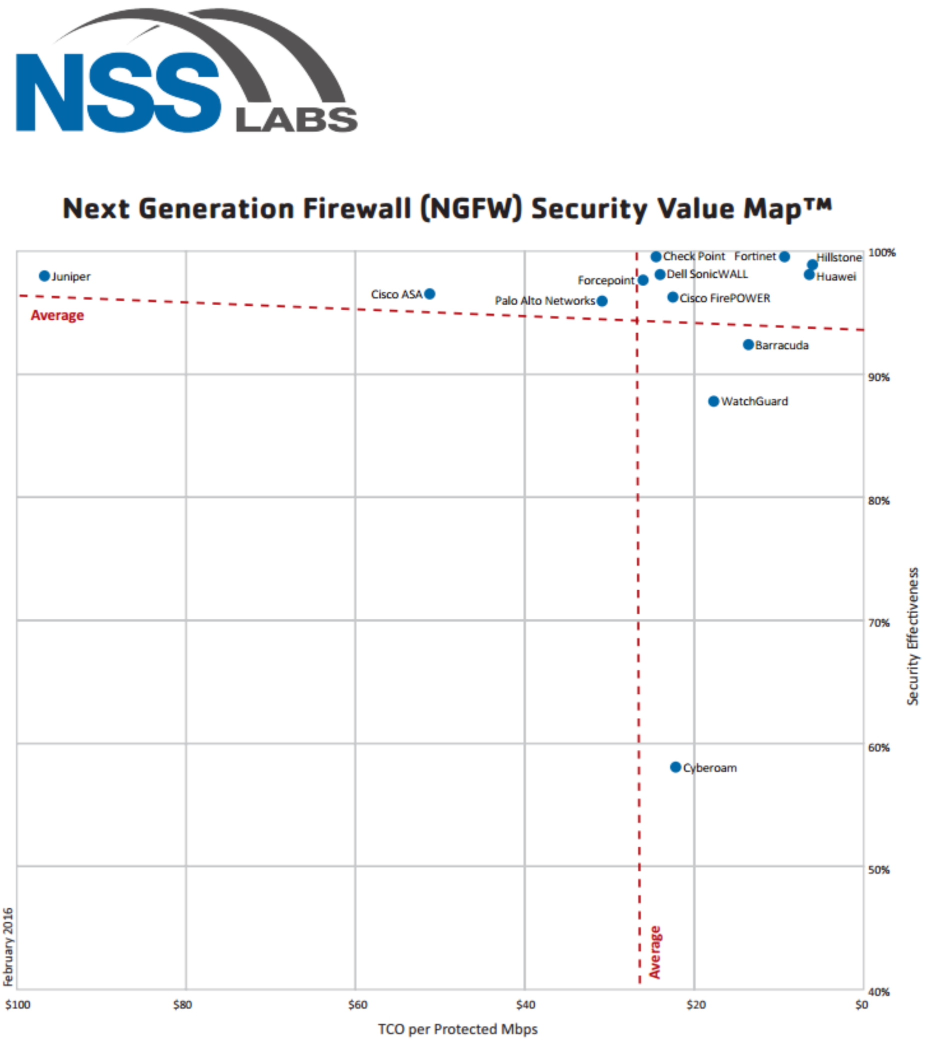


Figure 23 - NSS Labs NGFW SVM 2016 [**50**]

The 2016 NGFW security value map shows a TCO per protected Mbps on the x-axis and security effectiveness on the y-axis.

Juniper were placed a few percentages higher regarding security effectiveness but significantly lower on TCO per protected Mbps. Although Palo Alto's prices are regarded as on the higher end, the testing and criteria used by NSS labs suggests that the prices are well motivated. Juniper does offer much lower prices on hardware and licensing which can be a big factor for customers. However, according to this NSS Labs report, the actual throughput is not reflected well on the per-protected Mbps cost as it is very high compared to other vendors. Table 13 presents the advertised throughput and the achieved throughput by NSS Labs as well as TCO. TCO is calculated by multiplying the TCO per protected Mbps with the achieved throughput and the percentage of protection as it is not presented explicitly in the comparative report [**50**]. The TCO calculation is validated as being correct by the individual PA 7050 [**51**] report published by Palo Alto. Juniper has not published their individual reports.

Table 13 presents the data available through the NSS Labs NGFW Comparative Report SVM [**50**].

Table 13 - NSS Labs Comparative Report SVM (2016) [**50**]

	SRX5400E	PA-7050
Security Effectiveness (overall)	98%	95.9%
NSS Exploit Library		
Server Applications block rate	98.8%	94.4%
Client Applications block rate	99.0%	97.1%
CAWS (Live) Exploit block rate	97.03%	95.96%
Advertised throughput	22 Gbps	60 Gbps
NSS-tested throughput	4.138 Gbps	42.324 Gbps
TCO	$393,358.28	$1,256,938.152
Individual Report TCO	N/A	$1,256,000.00

In addition, both NGFWs fulfilled the following criteria:

- Evasion Techniques - resilience to all evasion techniques
- Stability and Reliability
- Firewall Policy Enforcement
- Applications Control - correctly identified all applications and took appropriate policy action
- User/Group Identity - correctly identified all users and groups and took appropriate policy action

Table 14 presents the data available through the 2014 NSS Labs Next generation firewall product analysis [**52**], which NSS do not recommend to use as it is based on old data. However, it does provide some indication to how the PA-3020 will perform and therefore will be included. Worth noting is that the PAN-OS used is v6.0.5-h3 and the security effectiveness would be more in line with the 2016 NSS report since the PA-3020 uses the same database as the PA-7050. The differences between the products lies within the amount of processing power and available High Availability ports, namely the HA-3 port which is dedicated to exchanging session data when running an active/active HA configuration.

Table 14 - NSS Labs NEXT GENERATION FIREWALL PRODUCT ANALYSIS (2014) PA-3020 [**52**]

	PA-3020
Security Effectiveness (overall)	92.5%
NSS Exploit Library	
Server Applications block rate	93.1%
Client Applications block rate	92.0%
CAWS (Live) Exploit block rate	N/A
Advertised throughput	1 Gbps
"Real World" Protocol Mix Avg.	719 Mbps
Enterprise Perimeter	1 Gbps
Financial	270 Mbps
Education	1 Gbps
Datacenter	1 Gbps
US Mobile Carrier	450 Mbps
EU Mobile Carrier	490 Mbps
3-year TCO	$26,700

Additional Services

To be able to achieve the same level of detail of network usage and the same security features as the PAN appliance does natively, Junos Space with Security Director and Log Director, Log Collector and

Spotlight Secure Connector needs to be installed in three separate VMs (Virtual Machines). Junos Space with Security Director and Log Director enables visualisation comparable to the PAN web-interface with the addition of centralised management of SRX-devices. This implementation requires:

Table 15 - JunOS Space Hardware Requirements

	CPU	**RAM**	**Disk space**
Junos Space with Security Director and Log Director [**53**]	1x 64-bit Quad-core @ 2.66GHz 4x Virtual CPUs	32 GB	100-200 GB
Log Collector [**54**]	8x CPU cores @ 2GHz	16 GB	1 TB +
Spotlight Secure Connector [**55**]	2x CPU cores	8 GB	80 GB
Total:	18 CPU cores	56 GB	1.2 TB +

Junos Space is also available as hardware appliances with the JA1500 and JA2500. The JA1500 is able to run Junos Space and the JA2500 is additionally able to be a Log Collector through a VM subsystem.

Spotlight Secure Connector enables additional security intelligence feeds allowing access to Geo-IP blocking, known C&C IP/URL/domains and known Attacker Fingerprints. Geo-IP blocking is the process of blocking entire IP address ranges linked to specific geographical locations such as continents or countries. Attacker Fingerprints is identifiable information for known devices used with malicious intent. Spotlight Secure Connector and Juniper's Sky ATP is equivalent to PAN's WildFire Cloud service, with the security intelligence feeds being available through the PAN's threat prevention subscription.

PAN's centralised management system Panorama utilises the same web-interface available on the appliances themselves thus does not provide any additional features as they are available natively on the NGFW. Panorama can be deployed as a dedicated device through the PAN M-series or as a VM with the ability to use an M-series appliance as a dedicated Log Collector or store logs locally on the VM itself. For a small deployment (1-10 devices) Panorama requires 4 GB of RAM and 4 CPU cores as a minimum, with a recommended 16 GB of RAM and 8 CPU cores for more than 50 managed devices. Panorama is required to be able to monitor a HA-pair as the logs are not shared between devices and thus will not be available if one fails or within the same web-interface.

5.5.4 Cost Comparison

The costs of appliances are important to consider when choosing a security solution. One needs to weigh the financial costs versus the security gained and evaluate if the resulting conclusion is viable. The prices are provided by Office A and can be seen in Table 16 and Table 17. Worth noting is that the prices are not subjected to any discounts.

Table 16 – SRX1500 Pricings

Product	Description	List price
SRX1500-AC	SRX1500	$11000
SRX1500-JSE	SRX1500 Juniper Secure Edge software	$11000
ND-SRX1500HW	Next Day Support for SRX1500-AC	$713
SUP-SRX1500JSE	Basic Support for SRX1500-JSE	$1650
SRX1500-ATP-1	Sky Advanced Threat Protection 1 year subscription	$8600
SPOT-LOCAL-1400	Spotlight Secure Connector (feed through Sky ATP subscription)	$0
JS-SECDIR-5	Junos Space Security Director for 5 devices	$600
Initial Cost		$33563
Yearly cost		$8600
TCO 3 years		$50763

Table 17 - PA-3020 Pricings

Product	Description	List price
PAN-PA-3020	Palo Alto Networks PA-3020	$16100
PAN-PA-3020-TP	Threat prevention 1 year subscription	$3220
PAN-PA-3020-URL4	PANDB URL filtering 1 year subscription	$3220
PAN-PA-3020-WF	WildFire subscription 1 year subscription	$3220
PAN-SVC-BKLN-3020	Premium support 1 year subscription	$2580
Initial Cost		$28340
Yearly cost		$12240
TCO 3 years		$52820

The price difference is roughly 4% or $2057, which does not include any hardware required to deploy the VMs needed to achieve similar security features or the PAN User-ID agent. Panorama is not included in the cost as a centralised management platform for an active/passive HA deployment would not provide any additional benefit. The one exception is when a failover occurs as the logs are unique per device and not shared between them. In an active/active HA deployment, centralised management could be beneficial, although not cost effective or achieve any greater benefit.

6 EVALUATION

This section is dedicated to evaluating the results from the case study.

6.1 PRESENTATION

The testing and research of the two platforms concludes a migration to either platform will provide the same level of difficulty. The CLI of JunOS is regarded as one of the best in the networking world but PAN-OS share a lot of similarities with JunOS. As Company A is currently implementing Juniper network infrastructure for their customers, their competence in JunOS will make a potential transition to PAN easy for their own network. As firewall configuration can be tedious using the CLI, heavy emphasis on a well-structured web-interface, log-presentation and ease-of-use could be as important as the security features themselves. Basic configuration is performed similarly, but PAN's web-interface is well designed and feature-rich, which Juniper's J-Web is not and requires additional VMs to provide the same features in the form of Junos Space with Security Director and Log Director, Log Collector and Spotlight Security Connector. This does however include centralised management, but for a single HA-implementation with potentially additional situational firewalls, centralised management would be excessive when accounting for cost. The trade-off is when a failover occurs as the logs will not be available on the back-up device but the security policies are already replicated and active. As the intended network for Office A will be relatively small, it should not be necessary to implement the extra features as separate devices or a centralised management system for security devices.

6.2 KEY DIFFERENCES

PAN developed their NGFW solution and based their entire business-model around a security appliance able to handle firewall-functionality, IPS and application awareness. The result is that the logging and management tools were built specifically to handle these three key features natively rather than complemented at a later stage by additional VMs. Key differences are that the PAN appliance is able to log and present data of users linked with network usage through App-ID and User-ID directly in the web-interface available on the device. This makes security and business-related policy decisions easier to implement as it is done through the same platform rather than having to rely on additional VMs. The result is however a single-point-of-failure but in a small environment this can be acceptable and having one device handling all of these features can be preferred.

Another key difference is the available techniques of mapping users to IP addresses. PAN supports a wider range of techniques whereas the SRX is natively limited to WMI polling AD DC event logs, captive portal for HTTP/HTTPS traffic and with the possibility of integration with Pulse Secure NAC, which is also available on the PAN device. This limits the SRX's ability to perform user-mapping dynamically and offers no support for Windows Terminal Server (remote desktop). This favours the PAN appliance as the SRX could potentially cause temporary problems and nuisance for the users requiring multiple instances of inputting credentials as well as the inability to properly map remote desktop users.

6.3 THIRD-PARTY ANALYSIS

According to the survey from Gartner, firewall customers has expressed the want for a different vendor for their security solutions other than the equipment used for their network infrastructure, which favours PAN as the future infrastructure of Company A will be Juniper equipment. As could be seen through the 2016 NSS Labs NGFW Comparative Report testing the PA-7050 and SRX5400E, performance of each appliance in terms of throughput with security and context-awareness features enabled heavily favours the PAN appliance. Even though these are not the intended candidates or equal in terms of vendor provided performance data, the data can be correlated to how the different vendors grade their own equipment in terms of throughput and therefore be applied to the less advanced, in terms of hardware, appliances. The SRX1500 does not have any published NSS Labs tests done as of writing, but it does have an advertised projection of potential NGFW throughput of 1.5 Gbps with an IPS throughput of 3 Gbps. If the 2016 NSS Labs Comparative Report of the SRX5400E is to be considered with its advertised IPS throughput of 22 Gbps and 4.138 Gbps NSS-achieved throughput, the SRX1500 would be projected to achieve 564 Mbps throughput. This is lower than the NSS Labs report for the PA-3020 which achieved 1 Gbps throughput with a typical enterprise-perimeter mix of protocols and an average of 719 Mbps with the "real-world" protocol mixes due to the significantly lower throughput of financial and EU/US mobile carrier mix of protocols. To provide the same correlation treatment, PA-7050 is advertised at 60 Gbps and achieved 42.324 Gbps, which correlates to 705 Mbps for the PA-3020, which is in line with the reported 719 Mbps. This is however only speculative since the SRX1500 is a new appliance and not well documented by third-parties as of writing. If the vendor projections are correct with the 1.5 Gbps throughput of NGFW functionality, the SRX1500 would provide higher throughput in comparison to the PA-3020.

7 Conclusions

Next-Generation Firewall (NGFW) functionality is a necessity of any enterprise network to provide a secure environment protecting the network resources from both external and internal threats as well as providing web 2.0 compatibility. NGFW functionality allows for granular policy controls giving more access to authorised parties in the context of their own choosing. Features previously only available as limited discrete security devices are now available as high throughput consolidated security solutions, bringing simpler management and leaving a smaller margin for human error or incompatible solutions.

Company A is a provider of network and communications solutions and is planning to implement a rigid internal network infrastructure at their branch Office A, which is going to utilise a NGFW. The new network will follow an enterprise network model and the network utilisation consists of office related network activity meaning heavy use web-based application traffic. The new network will be relatively small servicing around 30 employees. This puts emphasis on application awareness and ease of management due to the size and use of the network. The choice between Juniper SRX1500 and Palo Alto (PAN) PA-3020 (vendors requested by Company A) boils down to which one suits the future network the best. The Juniper SRX operates on JunOS that the company has an already-established expertise in while PAN operates on PAN-OS, of which limited knowledge exists. The research and testing shows that there are no significant challenges in regards to choosing either platform as the NGFW solution, as they both operate and are configurable in a similar fashion. PAN devices are however built from the ground-up with application awareness in mind whilst Juniper is a new challenger in the NGFW market, recently adding these features to their already established firewall product-line. PAN offers a one-box solution for management, visibility and logging whereas Juniper offers equivalent features as separate solutions. As the future network is small, PAN becomes a more obvious choice as to minimise management. The cost analysis shows no significant favour for either appliance as the prices for the full set of security features from both vendors are at a ~4% difference (excluding additional hardware costs), according to non-rebated list prices. Third-party research by NSS Labs concludes that the test-achieved throughput of one of PAN's high-end devices reaches 70.5% of advertised throughput while the testing of one of Juniper's high-end devices only reaches 18.8% of advertised throughput with the same full suite of NGFW security features enabled. When applying these percentage differences on the intended devices for Company A's network, PA-3020 and SRX1500, the PAN device would be favoured in terms of throughput. There are no tests done on the SRX1500 since it is new, but it could indicate how the different vendors grade their own products. The SRX1500 has a 50% higher vendor-projected NGFW-throughput compared to the PA-3020. Third-party market research made by Gartner places PAN as a leader in enterprise firewalls where Juniper is placed in a niche-role. Gartner's surveys answered by firewall customers shows PAN is rated highly on their IPS and application-aware features where Juniper is not seen as a contender in the NGFW market but can suit other implementations.

Our recommendation to Company A is to choose the PA-3020 as their NGFW solution based on our research showing that PAN is heavily favoured in enterprise networks due to their NGFW focus, incorporating application visibility and user-identification to a higher degree natively. PAN is a well-established and proven NGFW platform while Juniper is up and coming.

REFERENCES

[1] S. Murugesan, "Understanding Web 2.0," *IEEE IT Professional*, vol. 9, no. 4, pp. 34-41, Jul. 2007.

[2] J. Pescatore and G. Young, "Defining the Next-Generation Firewall," Stamford, Gartner RAS Core Research Note G00171540, 12 October 2009.

[3] Palo Alto Networks. Comparing Palo Alto Networks with UTM Products. [Online]. https://www.paloaltonetworks.de/content/dam/paloaltonetworks-com/en_US/assets/pdf/tech-briefs/paloaltonetworks-vs-utm.pdf

[4] Palo Alto Networks. Palo Alto Networks. [Online]. https://www.paloaltonetworks.com/

[5] Juniper Networks. [Online]. http://www.juniper.net/us/en/

[6] Juniper Networks. (2015, Nov.) NetScreen Security Products Hardware Dates & Milestones. [Online]. http://www.juniper.net/support/eol/ns_hw.html

[7] E. Byres J, "Defense in Depth: A single cyber defense is the weakest form of cyber protection," *InTech Magazine*, Nov. 2012.

[8] H. Zimmermann, "OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection," *IEEE Transactions on Communications*, vol. 28, no. 4, pp. 425-432, Apr. 1980.

[9] X. Li, Z.-Z. Ji, and M.-Z. Hu, "Stateful Inspection firewall session table processing," in *International Conference on Information Technology: Coding and Computing (ITCC'05) - Volume II*, Las Vegas, Apr. 2005, pp. 615-620.

[10] C. Lyons. (2012, Oct.) ENTERPRISE IT SECURITY ARCHITECTURE SECURITY ZONES: NETWORK SECURITY ZONE STANDARDS. [Online]. http://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/network_security_zone_standards.pdf

[11] D. Mudzingwa, "A study of methodologies used in intrusion detection and prevention systems (IDPS)," in *Southeastcon, 2012 Proceedings of IEEE*, Orlando, FL, Mar. 2012, pp. 1-6.

[12] X. Zhang, C. Li, and W. Zheng, "Intrusion prevention system deisgn," in *Computer and Information Technology, 2004. CIT '04. The Fourth International Conference on*, 2004, pp. 386-390.

[13] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," National Institute of Standards and Technology Special Publication 800-94, Feb. 2007. [Online]. http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

[14] Gartner. Secure Web Gateway. [Online]. http://www.gartner.com/it-glossary/secure-web-gateway/

[15] Palo Alto Networks. (2016, May) PAN-OS 7.1 Administrator's Guide. [Online]. https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/71/pan-

os/pan-os.pdf

[16] Robertckl. (2014, Jul.) How does SSL work? What is an SSL handshake?. [Online]. http://www.symantec.com/connect/blogs/how-does-ssl-work-what-ssl-handshake

[17] H. Tegenaw and M. Kifle, "Application Aware Firewall Architecture to Enhance Performance of Enterprise Network," in *AFRICON*, Addis Ababa, 2015, pp. 1-10.

[18] S. Lie and R. Kuhn, "Data Loss Prevention," *IT Professional*, vol. 12, no. 2, pp. 10-13, Mar. 2010.

[19] K. Sangani, "Sony security laid bare," *Engineering & Technology*, vol. 6, no. 8, pp. 74-77, Sep. 2011.

[20] S. M. GadAllah. (2003, Dec.) The Importance of Logging and Traffic Monitoring for. [Online]. https://www.sans.org/reading-room/whitepapers/logging/importance-logging-traffic-monitoring-information-security-1379

[21] Gartner. Unified Threat Management. [Online]. http://www.gartner.com/it-glossary/unified-threat-management-utm

[22] K. Bulsuk. (2008, Nov.) PDCA Cycle [image]. [Online]. https://1.bp.blogspot.com/-SFfhh7kpXXQ/VtQpM50ncfI/AAAAAAAANjA/fJxePV62vb4/s1600/pdca-cycle.png

[23] K. Bulsuk. (2009, Feb.) Taking the First Step with the PDCA (Plan-Do-Check-Act) Cycle. [Online]. http://www.bulsuk.com/2009/02/taking-first-step-with-pdca.html

[24] R. Enns, M. Bjorklund, J. Schoenwaelder, and A. Bierman, "Network Configuration Protocol (NETCONF)," Internet Engineering Task Force (IETF) RFC 6241 ISSN: 2070-1721, 2011.

[25] Juniper Networks. (2016, May) Junos Space. [Online]. https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000297-en.pdf

[26] Juniper Networks. (2016, Mar.) Junos Space Security Director. [Online]. http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000332-en.pdf

[27] Juniper Networks. (2016, Feb.) Juniper Sky Advanced Threat Prevention. [Online]. http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000549-en.pdf

[28] B. Woodberg and R. Cameron, *Juniper SRX Series*. Sebastopol, CA, United States of America: O'Reilly Media, 2013.

[29] Juniper Networks. (2016, Mar.) Application Layer Gateways Feature Guide for Security Devices. [Online]. http://www.juniper.net/techpubs/en_US/junos15.1x49-d40/information-products/pathway-pages/security/security-alg-overview.pdf

[30] B. Woodberg and R. Cameron. (2013) IPS Inspection vs Standard FW Inspection [image]. [Online]. http://orm-chimera-prod.s3.amazonaws.com/1234000001633/images/jsec_1303.png

[31] R. Cameron, B. Woodberg, P. Giecco, T. Eberhard, and J. Quinn, *Junos Security*. Sebastopol, CA, United States of America: O'Reilly Media, 2010.

[32] Juniper Networks. (2013, Nov.) Understanding Unified Threat Management for Branch SRX Series. [Online]. https://www.juniper.net/documentation/en_US/junos12.1x46/topics/concept/security-branch-device-utm-understanding.html

[33] Juniper Networks. (2016, Apr.) SRX1500 Services Gateway. [Online]. http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000551-en.pdf

[34] Palo Alto Networks. (2014) Content-ID. [Online]. https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/content-id-tech-brief

[35] Palo Alto Networks. (2016, May) WildFire Subscription. [Online]. https://www.paloaltonetworks.com/documentation/71/wildfire/wf_admin/wildfire-overview/wildfire-subscription.pdf

[36] Palo Alto Networks. (2016) PA-3000 Series. [Online]. https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3000-series-specsheet

[37] Palo Alto Networks. (2016) Panorama. [Online]. https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/panorama/panorama-ds.pdf

[38] Palo Alto Networks. (2015) Palo Alto Networks Single-Pass Architecture: Integrated, Prevention-Oriented Security. [Online]. https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/white-papers/single-pass-parallel-processing-architecture.pdf

[39] J. Snyder. (2007, Nov.) Juniper, Cisco all-in-one devices hit on intrusion-prevention controls. [Online]. http://www.networkworld.com/article/2288400/lan-wan/juniper--cisco-all-in-one-devices-hit-on-intrusion-prevention-controls.html

[40] Juniper Networks. (2013, Sep.) SSG140 Secure Services Gateway. [Online]. https://www.juniper.net/us/en/local/pdf/datasheets/1000181-en.pdf

[41] E. Cole. (2013, Oct.) Real-World Testing of Next-Generation Firewalls. [Online]. https://www.sans.org/reading-room/whitepapers/analyst/real-world-testing-next-generation-firewalls-34955

[42] Palo Alto Networks. (2016, Apr.) PAN-OS CLI Quick Start. [Online]. https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/70/pan-os/cli-gsg.pdf

[43] C. Gadecki and M. Scruggs, *DAY ONE: EXPLORING THE JUNOS CLI*, P. Ames, Ed. United States of America: Juniper Networks Books, Jan. 2011.

[44] Palo Alto Networks. Monitor the Dashboard [image]. [Online]. https://www.paloaltonetworks.com/etc/framemaker/61/pan-os/pan-os-admin/pan-os-221.gif

[45] B. Woodberg and R. Cameron. (2013, Jun.) Juniper SRX Series [image]. [Online]. http://orm-chimera-prod.s3.amazonaws.com/1234000001633/images/jsec_0302.png

[46] Palo Alto Networks. Application Visibility (ACC) [Image]. [Online]. https://www.paloaltonetworks.com/content/dam/pan/en_US/images/products/applicationvisibility-screenshot1-1170x.jpg

[47] Gartner. (2015) Gartner Research Methodologies. [Online]. http://www.gartner.com/imagesrv/research/methodologies/methodologies_brochure_14.pdf

[48] Gartner. (2015, Apr.) Magic Quadrant for Enterprise Network Firewalls. [Online]. https://www.gartner.com/doc/reprints?id=1-2DVI0YW&ct=150422&st=sb&elqaid=1245&elqat=2&elqTrackId=3fde15b81c9b40618641ac7bb3b9641f%5b5/28/2015

[49] Gartner. (2015) Gartner Magic Quadrant. [Online]. http://www.gartner.com/technology/research/methodologies/research_mq.jsp

[50] T. Skybakmoen and C. Conrad, "NEXT GENERATION FIREWALL COMPARATIVE REPORT - Security Value Map," NSS Labs, 2016.

[51] C. Conrad, "NEXT GENERATION FIREWALL TEST REPORT - Palo Alto Networks PA-7050 v6.0.11-h1," 2016.

[52] C. Conrad and J. Pearce, "NEXT GENERATION FIREWALL PRODUCT ANALYSIS - Palo Alto Networks PA-3020 v6.0.5-h3," 2014.

[53] Juniper Networks. (2016, Apr.) Junos Space Virtual Appliance Deployment and Configuration Guide. [Online]. http://www.juniper.net/techpubs/en_US/junos-space14.1/information-products/topic-collections/junos-space-virtual-appliance-pwp/junos-space-virtual-appliance-pwp-14.1r2.pdf

[54] Juniper Networks. (2015, Jan.) Junos Space Security Director - Logging and Reporting Getting Started Guide. [Online]. http://www.juniper.net/techpubs/en_US/junos-space14.1/logging-reporting/information-products/topic-collections/junos-space-security-director-logging-reporting-getting-started-guide.pdf

[55] Juniper Networks. (2015, Apr.) Configuring Spotlight Secure Connector. [Online]. http://www.juniper.net/techpubs/en_US/release-independent/spotlight-secure/topics/topic-map/secure-connector-installing.html