Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technologies

Master's Thesis

Next Generation Firewall - An Introductory Use Case

Harsh Ahir

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Bc. Harshkumar Pravinbhai Ahir

Systems Engineering and Informatics
Informatics

Thesis title

Next Generation Firewall – An Introductory Use Case

Objectives of thesis

The ultimate objective of this diploma thesis is to explore the usage and functioning of the Next Generation Firewall and its capabilities inside of an existing and complex network.
Analyzing the topology of a given network and its peripheral devices and appliances will be taken into consideration of this diploma thesis as its primary objective, by monitoring the actual working of the Next Generation Firewall and its relative communications to the other nodes and endpoints within the network as well as incoming and outgoing traffic from external networks including ISPs.
The secondary objective of this diploma thesis is to eventually study and observe the impact and robustness for a corporate organization and how the data of any enterprise can be protected and secured.

Methodology

I will be working with two major methodology styles to achieve the desired objectives: First a theory part, where I will observe and determine the internal workings of a basic firewall concepts and its impact on the network, including the structure of a network topology with a diagram.

Secondly, the practical part will consist of how an enterprise or an organization is utilizing the full potential of a Next Generation Firewall by securing its most important data structures and information, by comparing a traditional firewall against a Next Generation Firewall.

The proposed extent of the thesis

60-80p

Keywords

NGFW, firewall, network, security, data, information, NIPS, topology, cyber attack, vulnerability, protocols, enterprise security

---

Recommended information sources

COMER, D E. *Computer networks and Internets : with Internet applications.* Upper Saddle River: Prentice Hall, 2009. ISBN 0-13-091449-5.

DOROGOVTSEV, S N. – MENDES, J F F. *Evolution of networks : from biological nets to the Internet and WWW.* Oxford ; New York: Oxford University Press, 2003. ISBN 0198515901.

DUNN CAVELTY, M. – KRISHNA-HENSEL, S F. – MAUER, V. *The resurgence of the state : trends and processes in cyberspace governance.* Aldershot, England ; Burlington, VT: Ashgate, 2007. ISBN 9780754649472.

GUTMANN, P. *Cryptographic security architecture : design and verification.* Berlin: Springer, 2004. ISBN 978-1-4419-2980-8.

HAYDEN, L. *IT security metrics : a practical framework for measuring security & protecting data.* New York: McGraw Hill, 2010. ISBN 978-0-07-171340-5.

MCMILLAN, T. – EBRARY, INC. *Cisco networking essentials : e-book.* Indianapolis, Ind.: John Wiley & Sons, Inc., 2012. ISBN 978-1-118-09759-5.

SENTHILKUMAR, P. – MUTHUKUMAR, M. – JAWAHAR, M. *Fundamentals of computer networks and data communications : principles and paradigm.* Beau Bassin (Mauricius): Lambert, 2020. ISBN 978-6202516075.

Expected date of thesis defence

2021/22 SS – FEM

The Diploma Thesis Supervisor

Ing. Martin Havránek, Ph.D.

Supervising department

Department of Information Technologies

Electronic approval: 9. 8. 2021

doc. Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 19. 10. 2021

Ing. Martin Pelikán, Ph.D.

Dean

Prague on 05. 03. 2022

Declaration

I declare that I have worked on my master's thesis titled "**Next Generation Firewall - An Introductory Use Case**" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the master's thesis, I declare that the thesis does not break any copyrights.

In Prague on 28.12.2022 _____

Acknowledgement

I would like to thank my thesis supervisor Mr. Martin Havránek for his extraordinary support and guidance. And I also would like to thank my parents, grandparents, friends and colleagues for their lovely support throughout my whole course of study.

Next Generation Firewall - An Introductory Use Case

Abstract

Traditional firewalls were unable to differentiate between different forms of web traffic and simply followed internet protocols. Due to their inability to analyse the contents of network packets and discern between legitimate business applications and threats, they were forced to accept or reject all traffic. SSL traffic cannot be examined or decoded by a traditional firewall. A firewall is a piece of hardware or software that prevents unauthorized access to a computer system for the purposes of this issue statement. A next-generation firewall (NGFW) is a system security architecture that is based on hardware or software that has security features to identify and stop attacks at the application, port, and convention levels. Since the firewall is the first line of defence against such attacks and business system security is essential, firewall technology has evolved to address the problem. Traditional firewalls have failed because they lack granular insight into identifying distinct types of web activity and are unable to inspect the information payload of system packets. The overall goal is to investigate how the Next Generation Firewall is used and how it functions within a large and complicated network. It can be determined that the Next-Generation Firewall performs much better in terms of neutralising attacks launched by external users on a company network compared to traditional firewall. It can improve the security of data communication networks against external network attacks.

Keywords: NGFW, firewall, network, security, data, information, NIPS, topology, cyber-attack, vulnerability, protocols and enterprise security.

Firewall nové generace – příklad použití

Abstrakt

Tradiční firewally nebyly schopny rozlišovat mezi různými formami webového provozu a jednoduše se řídily internetovými protokoly. Kvůli své neschopnosti analyzovat obsah síťových paketů a rozlišovat mezi legitimními obchodními aplikacemi a hrozbami byli nuceni přijmout nebo odmítnout veškerý provoz. Provoz SSL nemůže být zkoumán nebo dekódován tradičním firewallem. Firewall je část hardwaru nebo softwaru, která brání neoprávněnému přístupu k počítačovému systému pro účely tohoto prohlášení o problému. Firewall nové generace (NGFW) je architektura zabezpečení systému, která je založena na hardwaru nebo softwaru, který má bezpečnostní funkce pro identifikaci a zastavení útoků na úrovni aplikace, portu a konvence. Vzhledem k tomu, že firewall je první linií obrany proti takovým útokům a zabezpečení obchodního systému je zásadní, technologie firewallu se vyvinula, aby tento problém řešila. Tradiční firewally selhaly, protože postrádají podrobný přehled o identifikaci různých typů webové aktivity a nejsou schopny kontrolovat informační zátěž systémových paketů. Celkovým cílem je prozkoumat, jak se používá brána firewall nové generace a jak funguje v rámci velké a komplikované sítě. Je možné určit, že firewall nové generace funguje mnohem lépe, pokud jde o neutralizaci útoků spuštěných externími uživateli v podnikové síti, než tradiční firewall. Může zlepšit zabezpečení datových komunikačních sítí proti externím síťovým útokům.

Klíčová slova: NGFW, firewall, síť, bezpečnost, data, informace, NIPS, topologie, kybernetický útok, zranitelnost, protokoly a podniková bezpečnost.

Table of content

List of Figures

1 Introduction

A firewall is a network security device that monitors incoming and outgoing network traffic and permits or stops data packets. Its goal is to close the gap between incoming traffic from your internal network and external sources (like the ISPs or vendors) in order to block malicious traffic from cybercriminals and viruses.

In order to block attacks, firewalls thoroughly examine incoming traffic in accordance with pre-established criteria and filter traffic from erroneous or suspect sources. Firewalls keep an eye on the traffic at terminals, which are access points for computers and are where data is transferred to and from external devices. For example, "Source address 172.18.1.1 is allowed to access location 172.18.2.1 with a 22 hole". Think of IP addresses as housing, and port numbers as indoor rooms. Only trusted people (source addresses) are not allowed to enter the house (physical address) at all — and then re-filtered so that people inside the house are only allowed access to certain rooms (ports), depending on their owners. , a child, or a visitor. The owner is allowed in any room (any hole), while children and guests are allowed in a certain set of rooms (certain holes).

A firewall can be software or hardware, although it is best to have both. A virtual firewall is a component of a device located between your network and gateway, whereas a software firewall is a program installed on each computer that regulates traffic through port numbers and applications. The most popular sort of protection, firewall filters, examine packets and block them from flowing if they do not adhere to a predetermined safety criterion. This kind of firewall verifies the IP addresses for the package source and destination. If packets similar to those of the law are "allowed" on the firewall, it means that it is trusted to enter the network.

Package filter firewalls are divided into two categories: stateful and stateless. Firewalls check packets apart and have no context, which makes them easy criminals. In contrast, solid firewalls remember information about transmitted packets and are considered extremely secure. Although package protection walls may work well, they ultimately provide basic protection and can be extremely limited for example, they cannot determine if the content of the submitted application will adversely affect the access application. If a malicious request enabled at a trusted source address can lead to, say, deleting the site, the firewall will have no way of knowing that. Next-generation fire hoses and proxy firewalls are well-equipped to detect such threats.

NGFW incorporates traditional firewall technologies and additional functions, such as encrypted traffic testing, antivirus systems, anti-virus and more. Most notable include deep packet testing (DPI). Although firewalls look only at package titles, in-depth package testing explores the data inside the package itself, allowing users to effectively identify, segment, separate, or configure malicious data packets.

Proxy firewalls filters network traffic at the application level. Unlike basic firewalls, a proxy creates a link between the last two systems. The client must send the request to the firewall, which is then analyzed by a set of security rules and then approved or blocked. Most significantly, proxy protection walls use both in-depth and in-depth package testing to identify malicious traffic while monitoring traffic for 7-level protocols like HTTP and FTP.

Using a firewall to translate network addresses, which hides private IP addresses, several devices with different network addresses are able to connect to the Internet. As a result, attackers scanning the network to locate IP addresses are unable to capture certain information, providing greater protection from attack. NAT fire shortcuts are like proxy protection walls because they act as a link between the computer team and the external traffic.

Multi-layer fire test walls filters packets from network, transport, and system layers, and compares them to known trusted packets. Like NGFW firefighters, SMLI scans the entire package and allows them to pass only if they pass each layer individually. These firewalls check packets to determine the state of the connection (hence the name) to ensure that all initiated communications occur only with trusted sources.

An application and protocol decoding engine that carries out Deep Packet Inspection is the foundation upon which the Next Generation Firewall is constructed and set up (DPI). To allow or reject application communication between network entities such as individual hosts, servers, subnets, and networks, firewall and NAT rules are defined.

An NGFW is typically used by network administrators to establish security zones based on corporate tasks including administration, sales, IT, and R&D personnel, among others. Alternatively, they might use an NGFW to implement security based on the traditional three zone approach - public zone, private zone and de-militarized zone (DMZ). Typical configuration could involve many network entity definitions (often involving several networks per zone), including several hundred rules to control access between hosts, networks, zones, and the Internet.

2 Objectives and Methodology

2.1 Objectives

The ultimate objective of this diploma thesis is to explore the usage and functioning of the Next Generation Firewall and its capabilities inside of an existing and complex network.

Analysing the topology of a given network and its peripheral devices and appliances will be taken into consideration of this diploma thesis as its primary objective, by monitoring the actual working of the Next Generation Firewall and its relative communications to the other nodes and endpoints within the network as well as incoming and outgoing traffic from external networks including ISPs.

The secondary objective of this diploma thesis is to eventually study and observe the impact and robustness for a corporate organization and how the data of any enterprise can be protected and secured.

2.2 Methodology

I will be working with two major methodology styles to achieve the desired objectives: First a theory part, where I will observe and determine the internal workings of a basic firewall concepts and its impact on the network, including the structure of a network topology with a diagram.

Secondly, the practical part will consist of how an enterprise, or an organization is utilizing the full potential of a Next Generation Firewall by securing its most important data structures and information, by comparing a traditional firewall against a Next Generation Firewall.

3 Literature Review

3.1 Need for Firewalls

In the early days of the internet, a small but enthusiastic community made it theory mission to advocate transparency and encourage collaboration via sharing (A history and survey of network firewalls, 2002). Morris Worm shattered this perspective. Even if you take the Morris worm of out equation, inclusion and acceptance attitude and branching out would result in the failure of the transparent, bankable group of users (Improving Network Security: Next Generation Firewalls and Advanced Packet Inspection Devices, 2012). Clifford Stoll observed that modification of agents in Germany with his platform and Bill Cheswick's "Evening with Berferd", where he set up a basic "jail" for the threat actor, are two examples of threat that either succeeded or tried during the same time phase. The threat actors were not successful to change the jail's actual networks, but they did not fail in fooling the "inmates" that they had done so (Network firewalls, 2006). Cheswick was good at tailing the attacker's actions, understand their actions, and alert the system administrators of the hacked networks. Such incidents triggered the conclusion of a functioning and running Internet. By, Steve Bellovin had figured out multiple attacks while checking the network close to the AT&T firewall. The inescapable conclusion was that there were many malicious and unreliable individuals online. Because not everyone can be trusted, when networks are joined, there is often a varying level of trust on both sides of the connection (Forcepoint).

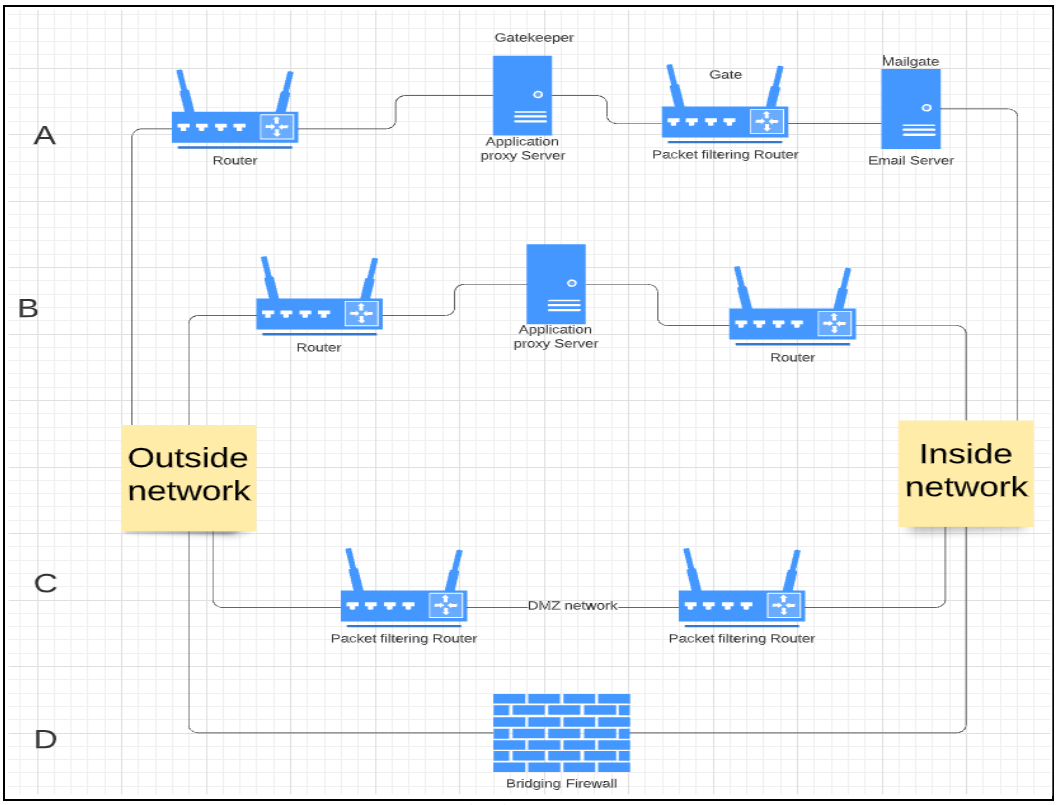

Figure 1 : Need for firewall – Own Processing

Operating system security concerns: Insecure operating system settings have a long history. For instance, because Windows 95 and Windows 98 automatically allowed file sharing, which was a risk that many viruses exploited. Many companies correctly decide not to safeguard the hardware behind their firewall because protecting the entire user system is a continuous and expensive endeavour (What is a Next-Generation Firewall, 2022). The remaining equipment may be in danger if the internal mechanism has been compromised. A personal firewall can be purchased to protect a single device connected to the Internet. Rather than attempting to safeguard the operating system as a whole, these security sites simply avoid certain types of communication. When a laptop or a home computer is outside its normal firewall, such firewalls are commonly used. The machine's network visibility is the trust threshold in this scenario (Detection of slow port scans in flow-based network traffic, 2018).

Information Inaccessibility: The installation of national firewalls is the second example of network security. Instead of protecting them from threats, this step makes sure that online activities of users are restricted. The Children's Internet Protection Act's usage of filters that have been approved by the US is similar in outlook (CHIPA). In lieu of this policy, all the content on the internet must travel via strainers before it can be consumed by schools, libraries, or other non-profit institutions (Network firewalls, 2006).

Information Loss Protection: The firewall reduces information leakages as all data on the network must travel through it. Thus, avoiding illegal or covert leakage of external data is an important step for the success of companies on the internet.

Protocol Monitoring: Firewalls, as defined in the security policies, monitor the network traffic policy that decides what data is allowed to pass through the network. These protocols are implied upon to operating systems, endpoints, and/or the legitimate traffic.

Audit: In the event of a network hack, investigation procedures (other than the firewall) can be applied to determine what exactly happened (Network firewalls, 2006). Additionally, staff recruitment through non-professional work network resources has been subjected to audit methodologies (Rengaraju, et al., 2017).

3.1.1 Next Generation Firewalls?

A standard firewall constantly checks network flow structure. It drops and monitors traffic as per the rules set and allowed or restricts the traffic according to state, port, and protocol. NGFW has also these tools in its arsenal and some more to prevent access control plus latest threats like complex malware and security attacks (What is a Next-Generation Firewall, 2022).

According to Gartner, a Next Generation Firewall must include the following features:

- Standard inspection tools to monitor security workflow
- An in-built and combined intrusion detection and prevention system (IPS & IDS)
- Application monitoring and recognition to identify and dismantle problematic applications
- Repository of threat intel

- Ability to upgrade itself with upcoming versions of threat modeling
- Capability for responding to complex security scenarios

3.1.2 Important things in NGFW?

The best NGFW points for main advantage for small and big companies:

1: Modern security measure and breach prevention

A firewall's primary aim is to keep your data secure by defending its networks. The prowess of your firewall is to swiftly identify complicated malware that should be removed because no preventative measure can be fixated to be 100 percent fool-proof (What is a Next-Generation Firewall, 2022). Invest in a firewall that has features listed below:

- Proactive approach to prevent attacks before they happen
- Integrated best-in-class next-generation intrusion prevention system (IPS) that scans URL for stopping access to multiple URLs and swiftly identify and eradicate silent attacks
- Aggresive malware security with combined tools to check file patterns in real time to quickly identify and eradicate threats
- A top-notch threat intelligence platform that provides the firewall the most latest information to squash upcoming threats

2: Access to the full network's visibility

You need to see from what you need to protect yourself from. To effectively identify malicious behavior and shut it down, you need to keep an eye on what is always happening in your systems. Your firewall has to feed you an exhaustive knowledge of what is happening and complete view of your networks so you can monitor (What is a Next-Generation Firewall, 2022):

- Threats are mostly targeting people, hosts, networks, and machines
- It's important to note that the initial indication of a threat, its last known locations across your infrastructure, and its live intentions
- Working sites and softwares
- Information/file transfers, network routes, and more

3: Flexible management and deployment options

Your firewall has to be configured to your precise standards, which caters the need for any sized organisations (What is a Next-Generation Firewall, 2022)

- Including but not limited to select between an on prem hardware and fixed administration of all devices

- Deploy a virtual firewall either on personal endpoints or in the vendor systems
- Enable characteristics that are tailor made for your company policies. Provide additional services to quickly gain access to more secure and robust tools
- A plethora of speeds should be catered

4: The shortest detection period

It is a very time consuming matter to detect an attack within the industry standard range of 100 to 200 days (What is a Next-Generation Firewall, 2022). A next generation firewall ought to be able to:

- Immediately respond to live attacks
- Precisely acknowledge the attacks or breach as soon as possible
- Triage events by priority so you can act quickly and take promising action to eradicate threats
- Run your opeartions smoothly by absorbing standard regulations that are easy to handle and that are intelligently monitored all over your network and firm

5: Automation and product integration

It is advisable to not use a contained tool as your next-generation firewall. It should be interactive and support with the other tools of your security posture (What is a Next-Generation Firewall, 2022). Select a firewall that:

- Works in perfect harmony with other softwares setup within the same company
- Proactively distributes threat intel, events, policy, and contextual data, web, endpoint, and network security tools
- Orchestrate security protocols like assesment, policy monitoring and editing, and user authentication

3.2 What is the difference between NGFW and Traditional FW

A network firewall's primary function is to operate as a barrier between a trusted internal network and an untrustworthy external network, most commonly the Internet. Traditional firewalls do this by filtering traffic according to ports and protocols. They frequently have network address translation (NAT) capabilities, which hides a device's true IP address and makes internal resource publicly available. Traditional firewalls are from another age, and they are no longer capable of managing traffic and dealing with the numerous problems posed by today's security landscape and proliferation of web applications and SaaS services (Abubakar, et al., 2020). Not only have fraudsters perfected strategies to get around traditional firewall's all or nothing approach.

However, most IT security threats today originate from within the network. By including capabilities like malware filtering, SSL and SSH inspection, intrusion prevention,

application identification and filtering, and the ability to access external intelligence sources, among others, next-generation firewalls overcome the limitations of conventional firewalls (Neupane, et al., 2018) (What is a Next-Generation Firewall, 2022).

1: Application identification and filtering: NGFWs can identify and apply not only filter data based on exclusive applications, preventing inappropriate software from easily avoiding normal traffic procedures by using unusual ports, but also deploying ports and protocols.

2: SSL and SSH Inspection: NGFWs can check SSL and SSH encrypted traffic and provide extra security against malicious applications that enumerate encryption to hide their activity from standard firewalls because they usually have a full web proxy service. This is possible because NGFWs may ideal out during an encrypted HTTPS session.

3: Intrusion prevention: Because NGFWs are capable of advanced intrusion and prevention, they are also known as unified threat management systems (UTM). NGFWs with intrusion prevention capabilities use signatures to identify network activity that reflects well-known and generic attacks.

4: Malware Filtering: Malware should ideally be filtered out before it has a chance to access the network, which is exactly what NGFWs with malware filtering employing basic signature-based analysis do. While signature-based malware scanning has its limits, it is an effective initial line of defence against generic threats.

5: Getting information from beyond the firewall: NGFWs can receive dynamic information from a cloud server to aid in the detection of malicious programmes by checking for unusual behaviour, such as a web server making outbound connections to weird IP addresses.

6: Benefits of NGFW over traditional firewall: NGFW provide considerably more complete network security while decreasing infrastructure difficulties and largely eliminating the need for a separate security solution by integrating standard firewall functions with intrusion presentation and virus screening. Operational costs can be considered decreased, and the overall system becomes more robust, with fewer infrastructural complications. Network speed is also increased by streamlining infrastructure since fewer security devices and services are used to route data, each of which makes performance claims that may or may not be true in practice. Most significantly, NGFWs have the necessary application knowledge in today's world of cloud computing and modern cyber threats. Granular control and the ability to create policies based on the user and the application are no longer sufficient because network communication has become substantially more complex.

3.3 Top 5 pre-requirements for NGFW

To be referred to as NGFW, a system must be able to comply with at least 5 fundamental requirements.

1: Deep packet inspection, which is already possible on modern firewalls, must be supported. Confirm that the NGFW checks all files, including encrypted files, for risks. To improve performance, some systems may allow huge files to pass.

2: Application intelligence is required by the system. In other words, it must be able to determine which programmes are using http and https ports, as well as what they are doing. As new apps become available, vendors must be able to provide updates.

3: Performance is a problem because an NGFW must be able to dig deeper into what is going on. All the system's functions must be performed at wire speed. A system with insufficient processing power will become a network bottleneck and/or miss abnormalities it is looking for. Many companies are developing specific hardware devices to run their software due to the requirements of these systems. The processing must be done in real time.

4: A NGFW must have excellent reporting skills that are simple to comprehend. You have no way of knowing whether the system is operating as planned unless you can analyse what is happening with it. More information than only the source and destination IP addresses and ports is required. You can't optimise something if you can't see what's going on.

5: It must be managed most system problems are caused by human mistake and incorrect configuration. Examine the system to see if each instance is controlled independently or if several NGFWs may be managed from a single location.

3.4 Modern NGFW

Initially, application monitoring and deep packet inspection were the primary reasons for NGFW implementation (the first is impossible without the latter). Apps include not only traditional “fat” applications, but also web-based micro-applications. Posting, video, and conversation in social network are examples (Ali, et al., 2020).

Almost all current NGFW, on the other hand, have a lot more features:

- Application control
- URL filtering
- VPN
- Intrusion Prevention System
- Anti-virus
- Anti-spam

Some solutions have additional functionality:

- DLP
- Sandboxing
- Log analyzer and correlation unit

Because of the vast number of functions available, there are implementation issues. The number of applications situations would be significantly reduced if you purchased a proxy server (IronPort, for example). The same can be said for anti-spam technologies that are

narrowly targeted. Regarding the “combinations” like current NGFW and what should be mentioned and how should to be used, so considering at a few examples of scenarios and to discuss about how best is to execute them. All subsequent conclusions are very subjective, depending solely on personal experience and adhering to set of “best practises”.

3.4.1 NGFW as a perimeter Firewall

A perimeter firewall is a type of security software that protect the link between a business' private network and external networks like the internet. A perimeter firewall can be configured as either software, hardware, or both to function as the first line of defence in enterprise security. Once implemented, a perimeter firewall examines packets entering and leaving a private network and accepts or denies them in accordance with pre-established rules (Hunter, 2021).

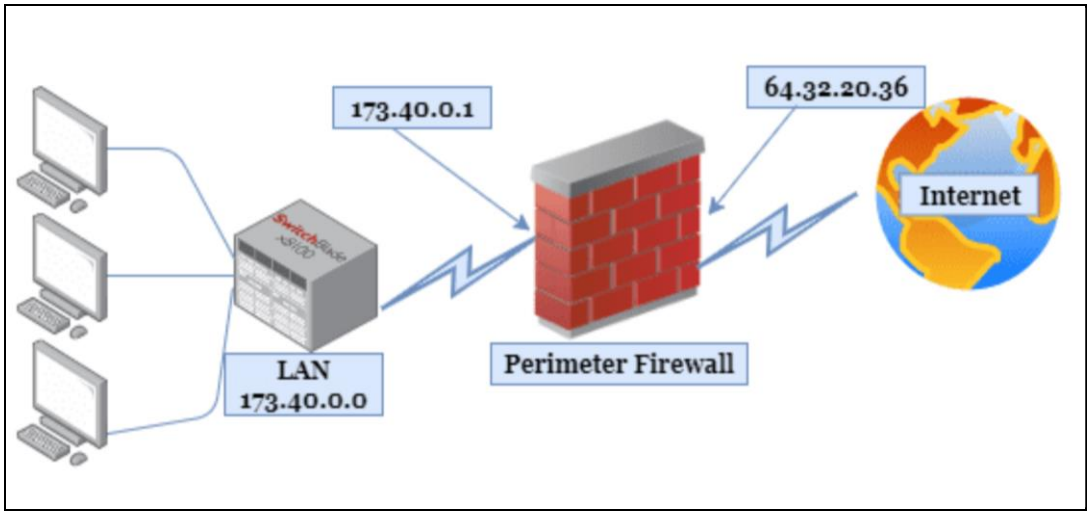

Figure 2 : Perimeter Firewall I

Source: (Hunter, 2021)

The easiest and more correct implementation option. NGFW for this and thought to stand on the edge of the network.

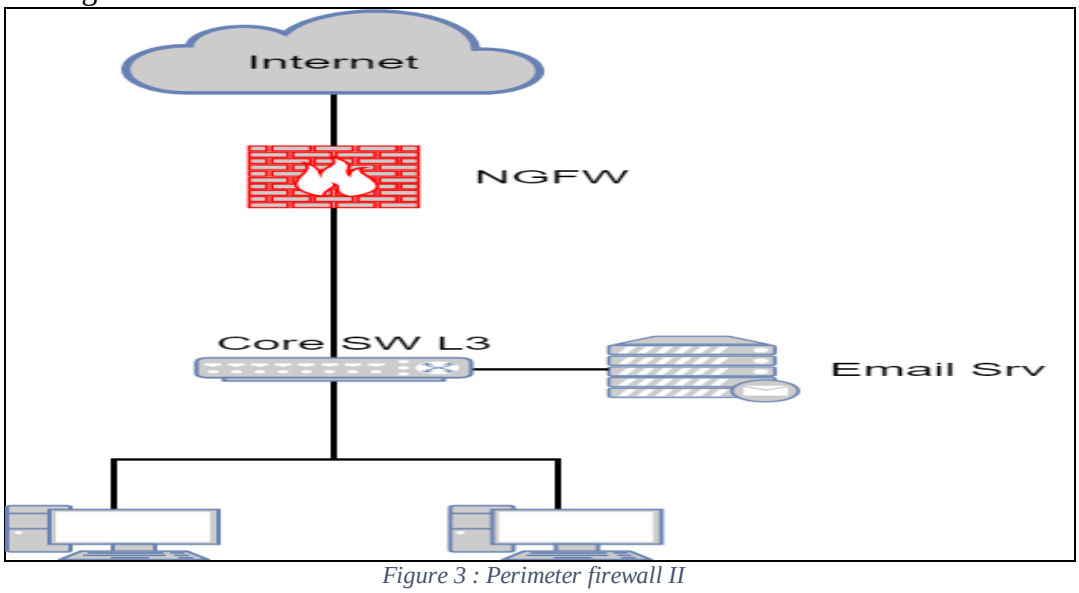

Figure 3 : Perimeter firewall II

Source: (Hunter, 2021)

Benefits of perimeter firewall:

- There's no need for a specialised proxy server. Most NGFWs can work in proxy mode, but for all local networks, all necessary functionality is available I "default route" mode. I set the default gateway and then forgot about it. There are no explicit proxies in the browsers of the users.
- IPS is on by default, and inline mode is enabled immediately. If you're afraid of difficulties, you can choose the Detect option. There's no need to consider how to wrap traffic through a specialised IPS device and how to swiftly reroute traffic if something goes wrong.
- Web traffic antivirus, including HTTPS traffic (with SSL inspection enabled).
- Antivirus protection for email traffic examine the attachments and connections.
- Anti-spam functionality.
- The ability to swiftly put the functional "sandbox" into place (sandbox). Almost all modern NGFW can activate the sandbox (cloud or local).
- All information security incidents are reported in one place.

The scheme has been substantially simplified, as you can see. Several traditional network protection methods have been removed. On the other hand, this is benefit (administration is easier), but on the other side, it is a disadvantage (a single point of failure). We won't argue about which is superior just now. We're just talking about the idea.

What to look in a next NGFW that will protect the network's perimeter:

- The mail check functionality should receive the most attention here (of course, if you are going to remove the current anti-spam solution). An MTA (mail transfer agent) is required for full-fledged mail handling by NGFW. In fact, NGFW replaces SMTP-relay in this mode, allowing for thorough inspection of mail traffic. Verification of investments in the sandbox is included. If there isn't an MTA, at least an SMTP relay should be available.
- Even if the MTA is present in NGFW, consider the mail filtering options carefully. The availability of quarantine is one of the most significant aspects (or ways to organise it).
- Of course, HTTPS inspection should be provided. Only one name from NGFW remains without this function.
- The number of apps that NGFW can identify. Check to see if the solution you've picked determines the applications require (including web applications).

Possible limitations or problems:

A router, rather than a ME, is frequently utilised as an edge device. In this situation, the existing scheme can make advantage of capability that isn't available on the NGFW in its purest form (various WAN technologies, routing protocols, etc.). This should be considered and meticulously planned before the deployment. It might make sense to keep the router and utilise it in parallel (for example, for organising a WAN network).

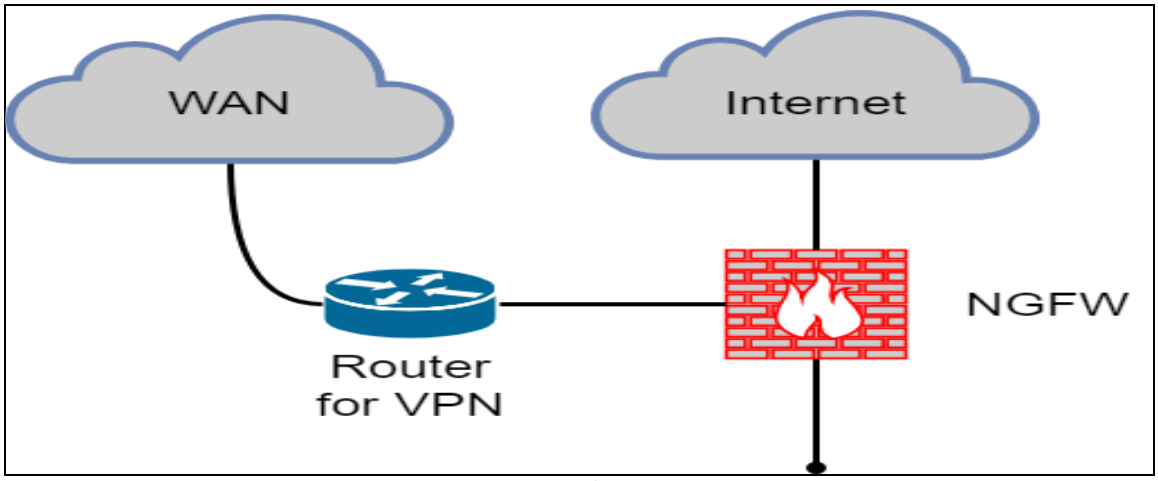

Figure 4 : Perimeter firewall III

Source: (Hunter, 2021)

Summary:

As I previously stated, the NGFW on the network perimeter option is perfect when used properly. However, keep in ind that NGFW is not a router. The normal funtions (bgp, gre, ip sla and so on) may be missing or just partially functional.

3.4.2 NGFW as a proxy server

A proxy firewall, which secure network resources by filtering communications at the application layer, is the most secure sort of firewall. The type of apps that can run on a network are restricted by a proxy firewall, sometimes referred to as an application firewall or a gateway firewall. This increases security but reduces functionality and speed. Application protocol traffic cannot be examined or decrypted by conventional firewalls. They frequently utilize an intrusion prevention system (IPS) or antivirus solution to prevent assaults, but these solutions only cover a small percentage of the threat landscape that businesses currently face (Myriam Dunn, 2007).
Oddly enough but it is also a fairly common option. Although NGFW was not developed as proxy. Typical scheme:

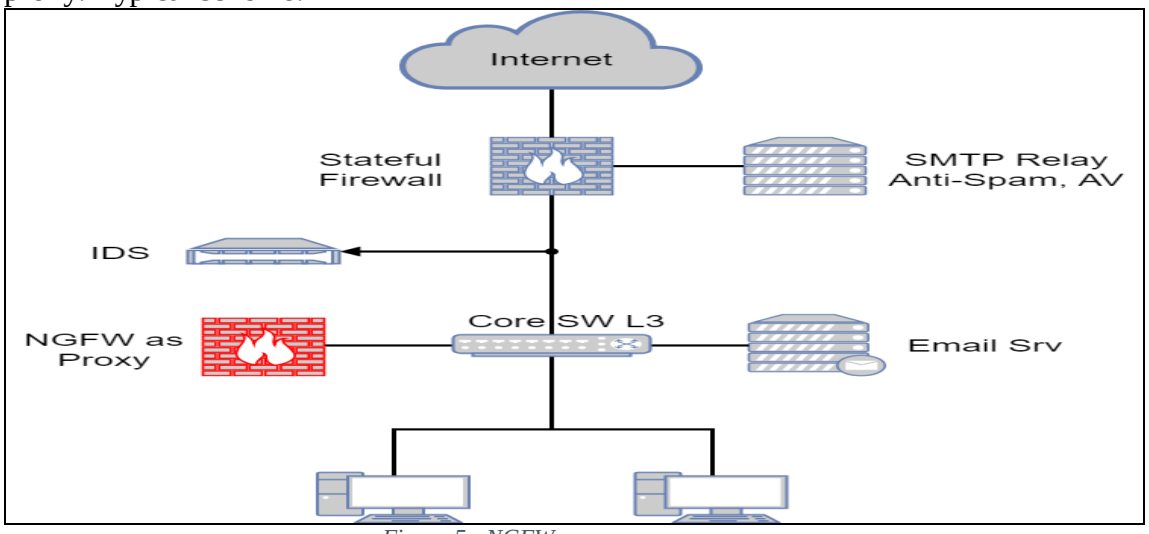

Figure 5 : NGFW as proxy server

Source: (Sudonull, 2019)

The advantage of proxy firewall:

- The implementation timeframe.
- Removed the old proxy and completed the task. There’s no need to make any changes to the current scheent or route.
- This is probably where the benefits end. Although the advantages are frequently stated, many companies find that they must make a decisoin based on them.

When selecting NGFW to as a proxy, keep the following things in mind:

- The user authenticaton mechanisim is the most crucial consideration here (NTLM, Kerberos, Captive Portal, etc.). Verify that the solution you’ve chosen supports the current authorization mechanism or can replace it with somethng suitable.
- Make sure you’re comfortable with the built in reporting features of NGFW (consumed traffic, visited resources, etc.).
- Traffic control options include Quality of Service (QoS), speed (shaping), and amount of downloading traffic limits (limiting).

Possible limitations or issue that may arise:

- First and foremost, keep in mind that NGFW in proxy mode is generally always a stripped-down functionality. You won't be able to use it completely. Especially when it comes to email traffic monitoring.
- Reduced bandwidth. In proxy mode, almost all NGFW solutions show decreased speed per user.
- You will continue to be required to use IPS. Because some of your traffic may pass through the proxy and onto the Internet.

Summary:

Personal recommendation: if there is a way to avoid using "NGFW as proxy," do so. The major drawback is the inability to perform a comprehensive mail check (technically, this can be done, but it will be a "crutch").

3.4.3 NGFW as core

A popular choice for small networks. The NGFW "hangs up" all traffic (internet, local, and server). The L3 switch is either not there or is not in use for routing.

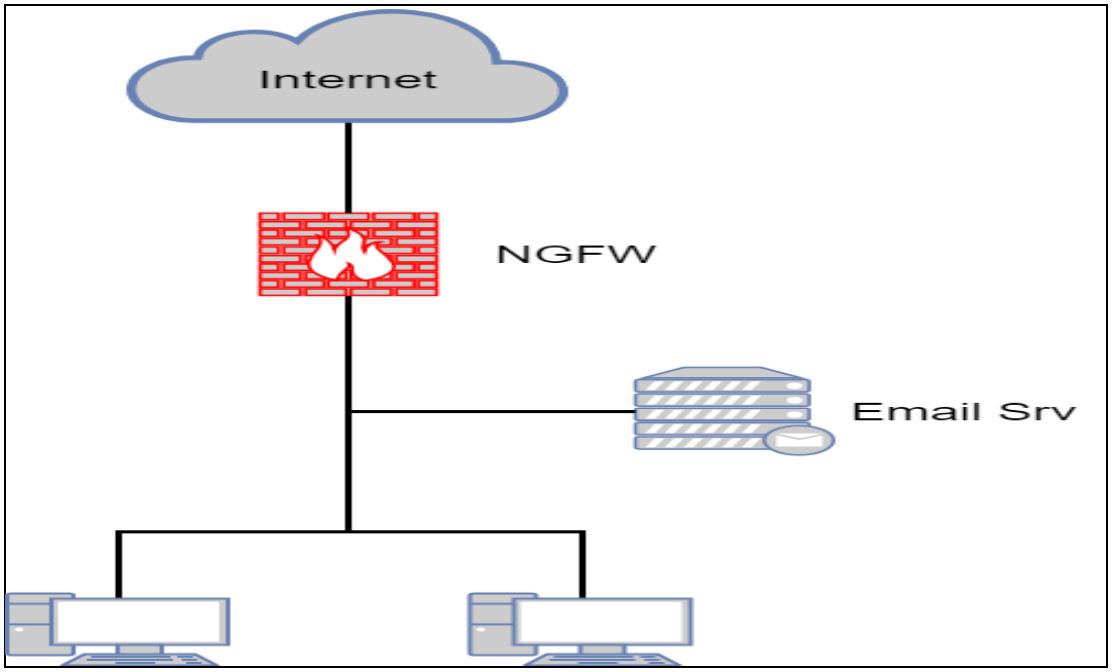

Figure 6 : NGFW as core

Source: (Sudonull, 2019)

The following are some of the benefis of this option:

- Ease of administration. All of your access lists are in one location.
- Quick deployment NGFW is typically placed in this manner in topologies where the ME was previously the network's core.
- All of the benefits of the "NGFW on the network perimeter" option.

When selecting the NGFW in “kernel” mode, what to look for :

Almost everything about the "NGFW on the network perimeter" is the same. However, in this case, the presence of the MTA function is worth paying special attention to. It is preferable to avoid using an additional device such as an SMTP relay in such a small network. It's preferable if your NGFW includes this feature.

Possible limitations or problems:

- A single point of failure could be the major issue. Remember to factor in your local traffic when choosing a device so that the NGFW model you choose can handle the load.
- In terms of change, the network is less adaptable. Less traffic control means fewer routing devices.

Summary

Perhaps this is ideal for small companies. Of course, if you accept the risk of a single point of failure.

3.4.4 NGFW as bridge mode

This is a less common alternative, yet it still happens more frequently than we'd want. The current network logic is unaffected in this instance, traffic at the second level is routed through NGFW, which is in bridge mode:

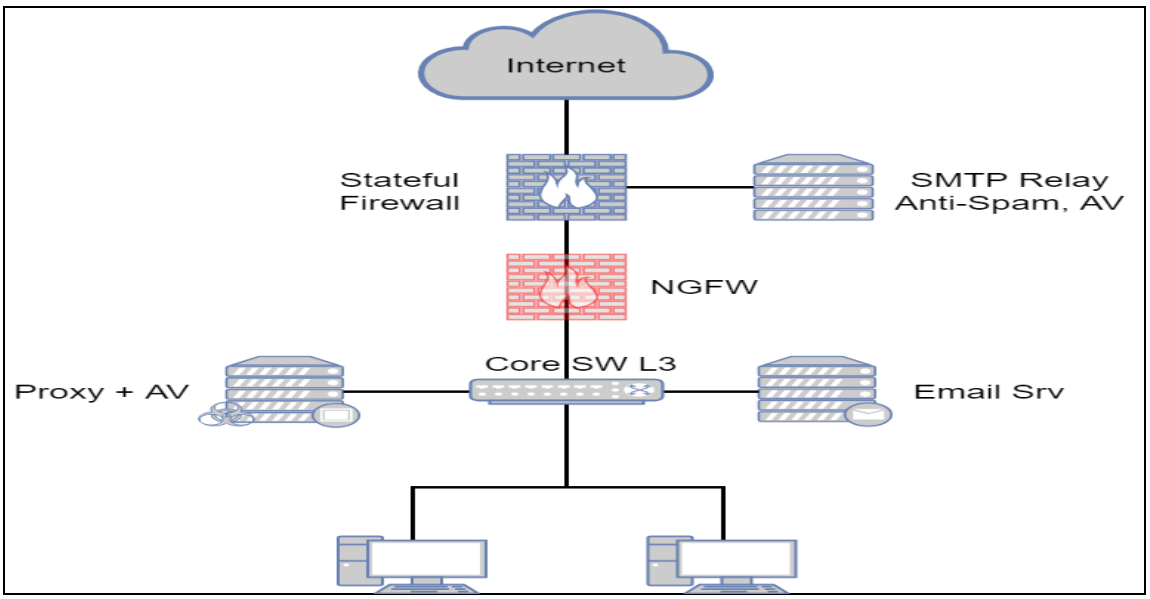

Figure 7 : NGFW as bridge mode

Source: (Sudonull, 2019)

In this instance, leaving a third-party IPS in place makes no sense (especially for monitoring the traffic). NGFW is well capable of doing its duty. This approach is most commonly utilised in more complex infrastructures where topology changes are either difficult or undesirable for some reason.

The advantages of this option:

- The implmenetation timeframe. You only need to rewrite the wire or “wrap” the VLAN, you don’t need to change the network logic.
- Fewer hops mean less network logic.

What to look for when choosing NGFW in “bridge” mode:

- On the restrictions of the “bridge” mode!
- It is desirable to have bypass modules so that traffic goes through the device, even if it is turned off.

Possible limitations or problems:

There are numerous pitfalls in this area. I have yet to come across a single NGFW solution that works well in bridge mode. Maybe I didn’t have any kuck. However, I simply relate my personal experience in this research. In addition of the official (documented) funtionality

constraints, unofficial limitations in the form of bugs and a slew of issues are always present. It all depends on the functions you utilise in bridge mode, of course. There will be almost no problems if you merely configure the firewall. Be prepared for shocks if you have enable features like IPS, Application control, HTTPS inspection, or even Sandboxing.

Summary:

As with the proxy, it is advisable to avoid the bridge mode. If this is not possible, then it is highly desirable to test this mode on your infrastructure.

3.4.5 Virtual NGFW or piece of hardware

Another frequently asked question when preparing for NGFW. Select a virtual or appliance-based solution. There is no one-size-fits-all solution. It all depends on your current infrastructure, funding, and network logic-changing capabilities (Bul'ajoul, et al., 2019). However, we do provide some broad advice for various implementation options:

- A NGFW at the network's perimeter. The appliance is unquestionably the finest option. Because the network perimeter must have a physical separation, this is logical. If you insist on a virtual solution, NGFW should be installed on a dedicated server that is physically isolated from the local network. You receive the same appliance; the only difference is that instead of using the vendor's "hardware", you use your own server with a hypervisor.
- As a proxy, use NGFW. It makes no difference which option you select. A virtual solution, in my opinion, would be a preferable and practical choice.
- The network's core is the NGFW. As stated in the opening paragraph, there are several basic needs. Because NGFW is directly connected to the Internet, it must be physically segregated from the company's servers - either as an appliance or as a virtual machine on a dedicated server. Because NGFW also serves as the kernel in this situation, you'll need to know how many physical ports you'll need and which ones (1g, 10g, optics). It also has a significant impact on the decision.
- In bridge mode, NGFW. A hardware device is strongly suggested for this choice, as bypass modules are preferred (traffic will pass even when the device is turned off).

Advantages of a virtual solution:

- The primary benefits of a virtual solution are the ease of maintenance (backup, snapshot), as well as the speed with which it can be deployed.
- It is also frequently cheaper and more scalable. Licensing is usually depending on the number of cores used. You can just buy a few cores if necessary.

Disadvantage of the virtual solution:

- There is no hardware warranty. If the server goes down, you'll have to deal with it on your own. If you're safe, you'll need to communicate with the IT department. Surprisingly, this is a major issue in many businesses.

In this case of appliances, the reverse is true. Furthermore, more physical ports are accessible right out of the box.

3.4.6 Fault Tolerance

NGFW implementations almost unversally support two clustering modes:

- A high level of availability. One node in the cluster is active and directs traffic, while the other is passive and in hot standby, ready to take over if the first fails.
- Load Sharing is a technique that allows you to share your computer's resources. Both nodes are up and running, and traffic is split between them.

When it comes to designing and executing NGFW, many indiciduals rely significantly on Load sharing mode. Numerous tests have shown that adequate traffic balancing is impossible to achieve. And the most you'll give Load Sharing is a 15% reduction in device load, not more. At the same time, this mode nearly always has some constraints that High Availability does not have. Make a point of reading them. When selecting a device, keep in mind that only one "piece of hardware" should be able to handle all traffic.

Summary

Use High Availability mode.

3.5 What NGFW can do to protect us from today’s security threats

Using a classical/traditional firewall to combat modern security threats is like playing professional football in the twenty-first century while wearing a 1930s leather helmet. You'll get some basic protection, but you'll still be vulnerable to significant harm. Traditional firewalls regulate traffic based on ports, protocols, and IP address. They can’t tell the difference between sorts of online traffic, whether it’s a danger or a genuine business application and apply security controls to prohibit or allow it. They’re also incapable of analysing network packet data payloads (Firewalls: A study on Techniques, Security and Threats, 2019).

Today’s threats, on the other hand, are usually web based and launched through applications. These malwares can bypass earlier firewalls by infiltrating across the https (80) and https (443) ports. Organizations may be required to ban all applications and apply security controls to prohibit or allow it. They’re also incapable of analysing network packet data payloads. Modern security threats include complex malware, stealth bots, and zero-day vulnerabilities. These threats are intelligent enough to disable security defences, steal data, and linger in your network while you wait for more instructions. These are the kind of assaults that a modern firewall can stop.

A next-generation firewall (NGFW) that is application aware may distinguish between various apps and put in place fine-grained security controls at the application layer. While approved applications are permitted into the network, deep packet inspection and intrusion prevention techniques are employed to check the contents of traffic for dangers, enabling more informed banning decisions based on incredibly specific criteria. A NGFW's

enhanced features not only lower the chance of a breach, but they also block or limit the use of non-business apps, which can cause bandwidth bottlenecks and stifle employee productivity. From the viewpoint of personal devices, multiple strategies can be applied and setup, prioritising the most business critical applications and software's receiving the highest attention.

Usually, NGFW is sometimes mixed and matched with some combination of software and hardware as a platform to centrally manage security incidents and threats, firewalls, antivirus, IPS, URL blocking, monitoring, and more into a unified security device. Together, these two techniques can offer genuinely all-encompassing network security. It's critical to consider the architecture, performance impact, and manageability when selecting an NGFW for your company. Understand the hardware and software architecture, including how it will be developed and integrated, as well as how it will deliver the results your company requires. Find out if an NGFW has any effect on network performance. Ensure that throughput is tested after all security elements have been activated and the proper number of connections have been established (Gutmann, 2004).

A Next-Generation Firewall (NGFW) entails very detailed policies and rules that enable more granular, strong security controls, yet it should be simple to configure, implement, and maintain. The importance of simple, centralised management cannot be overstated. Is your firewall more like a polycarbonate shell, vinyl nitrile foam padding, and a titanium facemask, or an old leather helmet. Allow Technologist to assist you in determining your organization's security requirements and selecting and deploying the appropriate NGFW solution.

3.6 NGFW architecture

An application and protocol decoding engine that does Deep Packet Inspection is the foundation upon which the NGFW is constructed and set up. To allow or reject application communication between network elements, such as specific hosts, servers, subnets, firewall, and NAT rules are defined.

An NGFW is typically used by a network administrator to create security zones depending on organizational tasks like administration, sales, IT and R&D personnel, and among others. Instead, they might deploy an NGFW to implement security using the conventional three-zone strategy (public zone, private zone and demilitarized zone). A typical configuration may have several hundred rules to regulate access between hosts, network, zones, and the internet, as well as numerous definitions of network entities (typically involving multiple networks per zone) (Telesis).

3.6.1 Balancing network security with performance

Concerns about network security coverage vary frequently among network administrators. Others need a fair level of protection with a minimum amount of delay and a maximum amount of throughput, while some demand the largest amount of border protection for their corporate network. A network administrator must determine the security/performance trade-off that best meets their demands.

3.6.2 Proxy versus Stream

Proxy-based processes and stream-based processes are the two main groups of components that make up a threat management system. With the help of application-level inspection and scanning, both types of processes concentrate on providing reliable and secure network protection. However, each has a specific function that affects network latency and performance in a different way.

Proxy-based Processes	Stream-based Processes
In this process the security device serves as a proxy for the data's destination during this process. Before sending the file to its destination, the security device will receive it, reconstruct it and examine for threats.	The packets inspect via stream.

NGFW security policies:

Network security component	Security policies
Next-Generation Firewall (NGFW)	• Application control • Web filtering • IP Reputation • Malware Protection • Antivirus • IPS Engine • External link request for 3rd party • URL Filtering (What is a Next-Generation Firewall, 2022)

3.6.3 Proxy-Based threat scanning

Using a proxy antivirus engine, proxy-based threat scanning retrieves the stored object data from the threat signature database files and compares it to various established threat signatures. It can take a lot of memory and CPU resources to carry out object file download, re-order and reassembly, scanning, and object file re-transfer operations. Proxying the TCP session also reduces overall data throughput.

Anti-virus file scanning

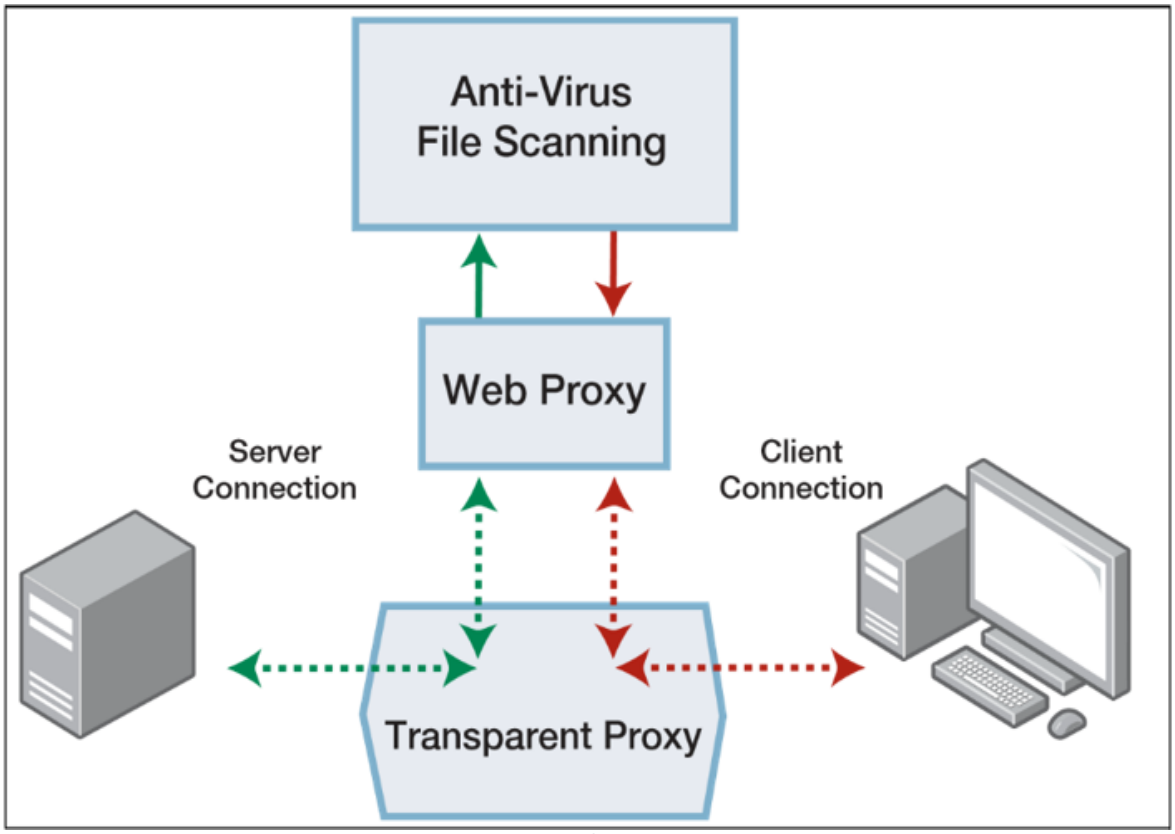

Figure 8 : Anti-virus file scanning

Source: (Telesis)

Project-based object scanning

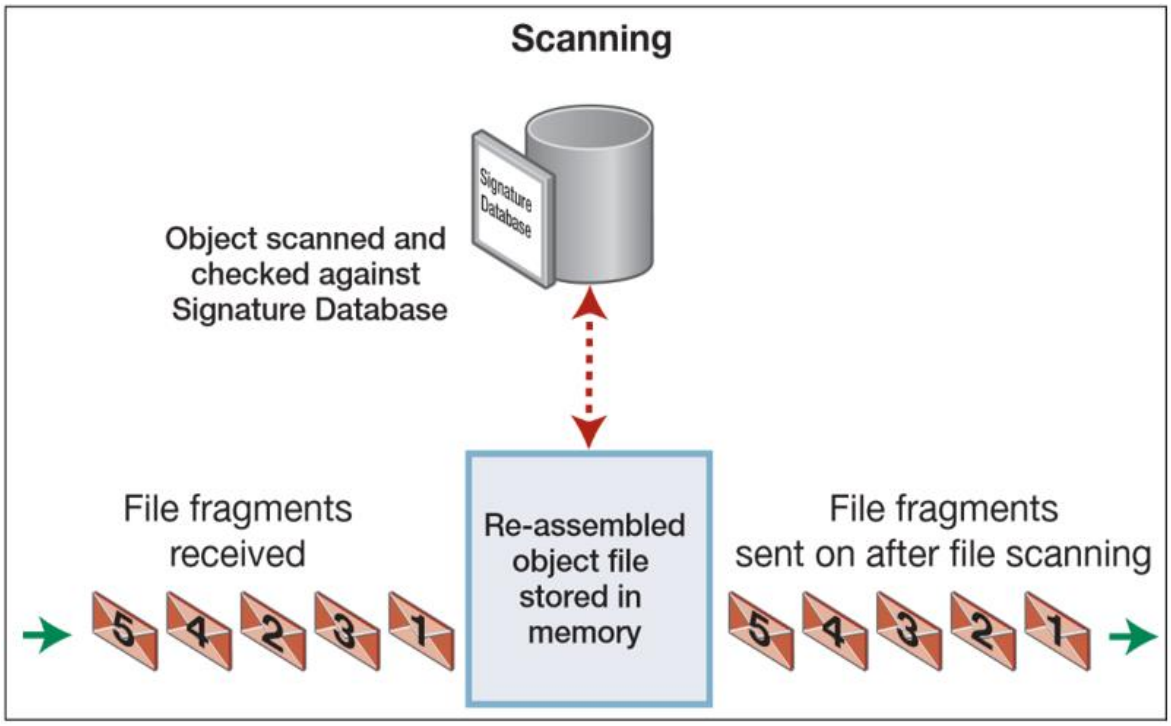

Figure 9 : Project-based object scanning

Source: (Telesis)

By its very nature, proxy-based scanning provides the finest detection; nevertheless, it also consumes more resources and process considerably more slowly than stream-based scanning. Proxy-based engines must serve as a middleman and end each and every client session, create an associated session with the destination server, and trasparently monitor the associated session state. Multiple simultaneous sessions may be managed by a single user connection to a single website

3.6.4 Stream-based threat scanning

Contrarily, stream-based scanning threats data in the order in which it arrives. Because they do not naturally suffer from the need to proxy connections and do not need to wait to receive, store, and scan full object data transfers before forwarding across a security boundary, stream-based engines are built for maximum throughput with the least amount of latency. As it comes in, data is scanned using a layer-by-layer method.

The more data (for a given data stream) that passes through the device, the more thoroughly it is scanned in real time against different threat signatures. This scanning begins with source/destination IP against an IP Reputation list (if IP Reputation is configured), moves on to Layer 7 application data information (like HTTP/1.1 Get requests embedded in HTTP packets), and finally moves to embedded user data. (Intrusion Prevention And Detection in Small to Medium-Sized Enterprises, 2017).

3.6.5 Performance considerations

Imagine a network of users browsing websites with lots of images that must be downloaded into system memory, scanned, and sent in order to display all of a web page's contents (McMillan, 2012).

Proxy-Based Engines: All of these distinct sessions TCP connection states must be simultaneously managed (proxied) by the proxy engine. These operations can consume a significant amount of system resources, such as system memory and CPU cycles, at the expense of other programs. However, it also enables the device to fully download, store, and thoroughly scan an entire object file transfer for dangerous threats and embedded viruses against a threat signature database. This may result in longer latency for client to server traffic. By virtue of how they function, proxy-based engines provide the highest level of protection against threat vectors.

Stream-Based Engines: When opposed to proxy-based engines, stream-based security scanning engines use substantially less CPU and system memory. This is so that whole files can pass via the security device without having to be downloaded. Additionally, file pieces do not need to be put back together before scanning, fragmentation, and forwarding.

3.6.6 SSL Inspection

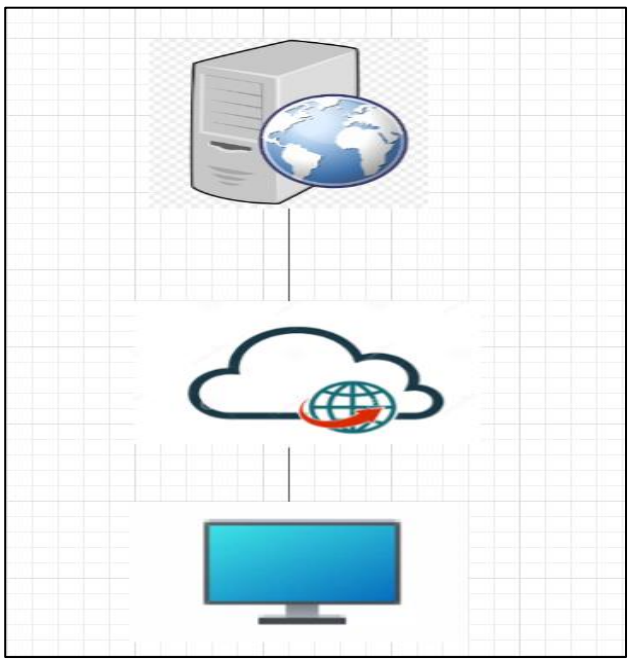

Figure 10 : Without SSL inspection - Own processing

On the left-hand side user is accessing website without SSL inspection which is very serious web security vulnerability since attackers can place themselves in middle of user's browser and server and interrupt sensitive data in transit. Such attack is called as man-in-middle attack. For example, user is trying to reach website which collects personal information such as login credentials, credit/debit card details, contact details, etc. must have SSL inspection otherwise data will be leaked, and the user will be hacked easily even the content of the site is very good.

Figure 11 : With SSL inspection - Own processing

On the left-hand side user is accessing website with SSL inspection which helps user with privacy, data integrity, authentication, enhance image, secure transaction between customers and business, secure FTP service, secure access control panel, etc. SSL verifies that a website has digital certificate which is signed by an authority trusted like GlobalSign, GoDaddy, etc. There are three methods of SSL inspection: Terminal Access point (TAP) mode, Next-Generation Firewall and Proxy. Network connections pass via NGFW with only packet level visibility, which restricts threat detection. NGFW only detect a small portion of malware, it can be distributed in fragments. When essential features like threat prevention are enabled, they frequently perform poorly and need for bolt-on proxy capability.

3.7 Option available on the NGFW

NGFW combine the benefit of both proxy and strem-based protection options.

Users can configure a mix of:

- Proxy-based Antivirus checking for multiple file object kinds during HTTP file transfer (for example, zip and image files associated with a website).
- Proxy-based Web control to classify and filter URL lookups in order to help block access to known harmful and phishing websites.
- A range of stream-based threat protection tools, including URL filtering, malware protection, intrusion detection and prevention, and IP reputation.

NGFW controls the system resources devoted to proxybased scanning. Currently, for proxy-based Anti-virus:

- Objects up to 10 MB per file can be individually scanned.
- Up to 100 MB of objects can be concurrently scanned.

In order to scan within an embedded data flow, antivirus software can extract nested object files up to a maximum depth of three. Up to 10MB-sized files that have been extracted and decompressed can be scanned. If an object file cannot be scanned for whatever reason, the user can decide what alternative actions to take, such as log or allow, should be taken (for example if it is too large). When a scan fails, the default response is to deny (Surantha, 2019).

3.7.1 URL Filtering Versus Web Control

Some threat protection tasks can be completed using either a stream-based approach or a proxy-based approach. Controlling which websites users are permitted to view is an example of this. This can be accomplished via a stream-based approach, in which the NGFW stores lists of websites that are authorized and forbidden and refers to those lists whenever it processes packets that are trying to access a web service. Alternately, it can be done using a proxy, in which case the NGFW extracts the information from the packets and sends it to an outside service, which then makes a determination regarding the compatibility of the website the user is trying to access (Comer, 2009).

NGFWs implement both methods:

- The stream-based method is called URL filtering.
- The proxy-based method is called Web Control

URL Filtering: A service that uses streams is URL filtering. A user-defined list (in which up to 1,000 blacklist/whitelist URL entries can be created) or a downloadable list (comprising many thousands of known harmful website URLs that can be updated often) are the two methods used to filter URLs. In order to match URLs against white and black lists in real time, GET, HEAD, POST, PUT, and DELETE HTTP requests are parsed to extract URLs. An organization may use URL filtering to block access to a particular (or user-defined) set of URLs via a low latency stream-based service. Without affecting

performance, network administrators are permitted to statically specify their own black-listed and white-listed URLs.

Web Control: A proxy-based web categorization service is called Web-control. To offer real-time protection, this function makes use of an outside categorization service. The categorization service provider continuously updates its list of phishing and harmful websites in real-time. The external categorization service's categorization replies are cached by the NGFW. Performance is enhanced and unnecessary and repetitive external URL lookups are avoided. A limited list of user-defined URLs that might be pertinent to a business organization can be specifically accessed using up to 50 user-defined category match criteria. For instance, doing so enables a company to manually bypass the external categorization service's restrictions and provide access to a URL that would have otherwise been denied (Hybrid intrusion detection and signature generation using DeepRecurrent Neural Networks, 2020).

Summary

Web control, by its very nature, offers the best defense against harmful and phishing websites that are dynamically and continually changing at the expense of the latencies associated with a proxy service, whereas URL filtering may carry a slight risk of exposure to threats in between updates. If URL filtering and Web control are both turned on at the same time, URLs will first be examined using URL filtering lists before being categorized using Web control. A connection can be blocked by either function. The choice of one feature to block a connection cannot be reversed by another feature.

Web Control

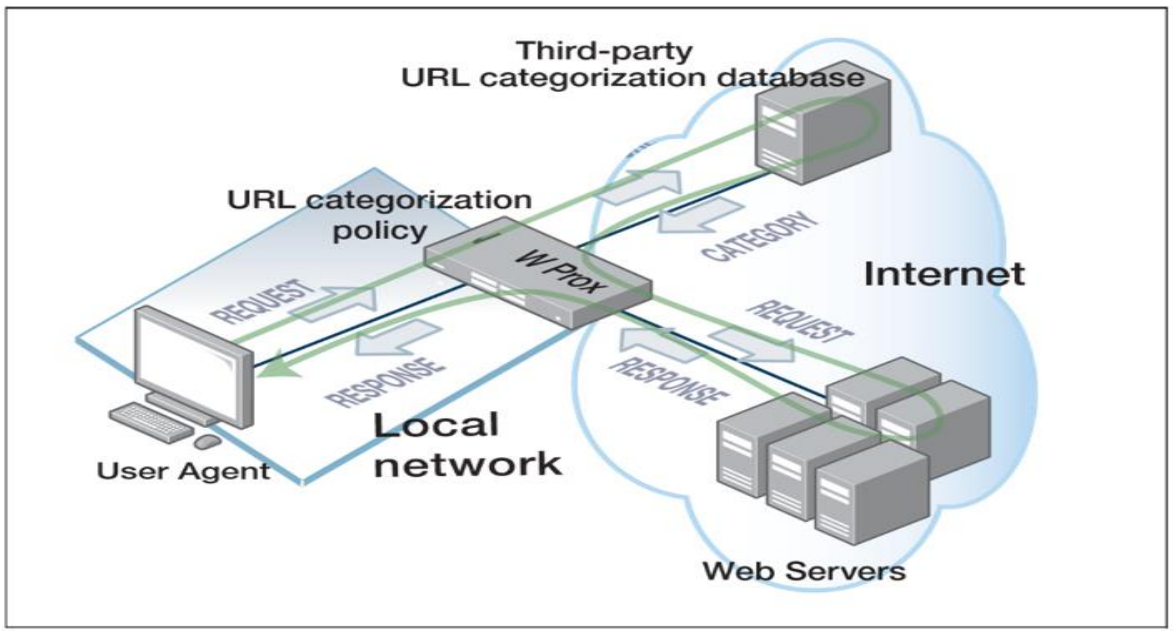

Figure 12 : Web control

Source: (Telesis)

3.7.2 Performance Optimizing Architecture

Characteristics of NGFW and UTM, which are typically offered by a variety of devices, into a single security appliance. As a result, the total cost of ownership is decreased because the network administrator can replace several devices with a single appliance. As they are all enabled within a single security appliance, the network administrator may ask about the impacts of configuring all or combinations of these different protection services. As each security service was used one at a time in certain previous integrated security appliance systems, inconsistent and unpredictable performance was a common issue.

Threat protection with high throughput/low latency is possible with stream-based features. However, as was previously said, when proxy-based measures are also enabled, performance may suffer and latency may rise while proxies are established and data is processed and thoroughly re-scanned via each security feature one at a time. As each security feature is used, this can give rise to legitimate worries about how it will affect performance, connections per second, latency, and other factors. This is especially true if the firewall device's security features are implemented using a traditional processing architecture. Each security process is run separately in such an architecture. As a result, certain operations, including identifying the application contained within a packet, might be repeated several times on the same packet (Silva, et al., 2017).

Process performed separately in series

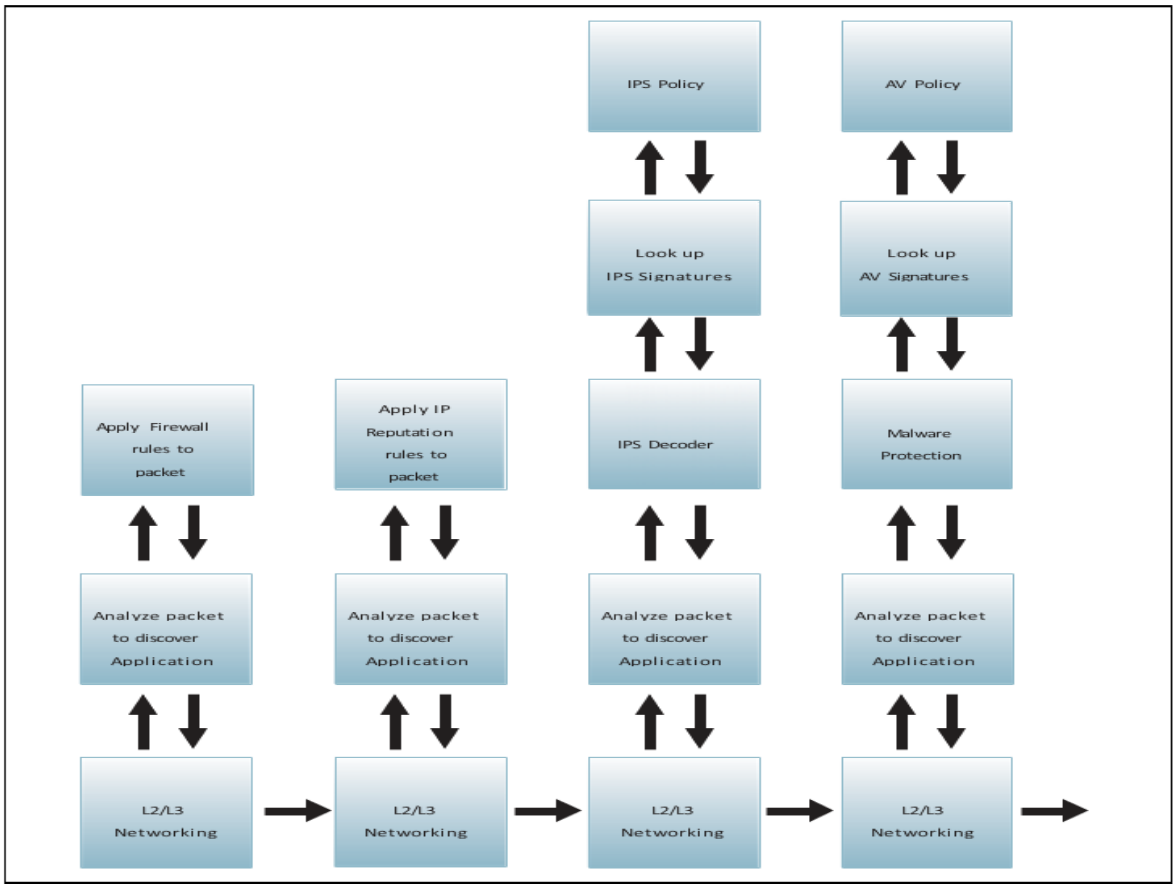

Figure 13 : Network process separately in series

Source: (Telesis)

By combining a multi-core CPU with a more effective architecture model based on many parallel processing channels, NGFW architecture aims to reduce these issues as much as feasible.

3.7.3 Software Architecture – Multiple Parallel Processing Paths

Within the application decoding engine, every data is first classified according to its application, protocol, and content. As a result, each packet is only ever subjected to the analysis process once in order to identify the Application and other characteristics.

Multiple parallel processing paths

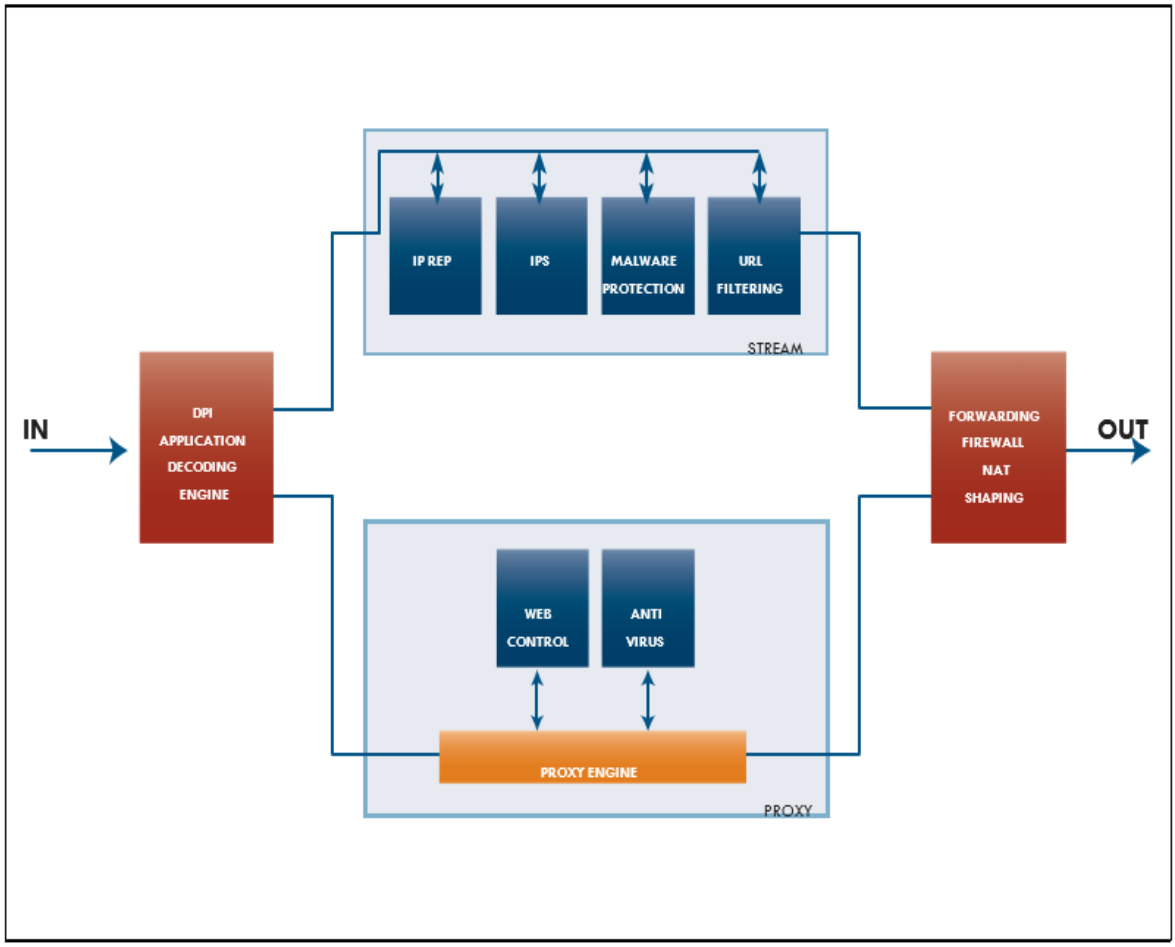

Figure 14 : Parallel processing paths

Source: (Telesis)

Only the proper software data processing path associated with the security feature is used to process content. For instance, if a stream-based feature (such as IP reputation) is enabled along with a proxy-based service (such as HTTP-based antivirus), and the application data is an UDP-based Skype call, the Skype call will not be processed through the proxy service (as the AV service scans HTTP data streams, not UDP data streams). This means that even when using the proxy service, Skype performance won't be impacted.

3.7.4 Hardware Architecture

A specially designed, multi-core Network Services Processing (NSP) CPU is employed to boost performance. The CPU loads balances data to be processed by each CPU core using a core balancing algorithm depending on a range of factors, including protocol, port numbers, and IPv4/IPv6 source address. For instance, running a YouTube video on one CPU core will not influence the throughput of any other application data that is being handled on other cores in an unconnected manner (Erlacher, et al., 2020).

As a result, performance throughput is often tested to reflect real-world usage, with sufficient flows and variance between each flow to guarantee that the load is distributed evenly over all available CPU processing cores. The regular expression engine of the CPU processes signature files. Therefore, hardware-based processing for signature-based file scanning is provided by the CPU. In addition, the CPU offers on-chip hardware (HW) acceleration for IPsec VPN encryption services, increasing security throughput without the requirement for external off-chip co-processing or software encryption of data streams (Senthilkumar, 2020).

On-chip hardware acceleration

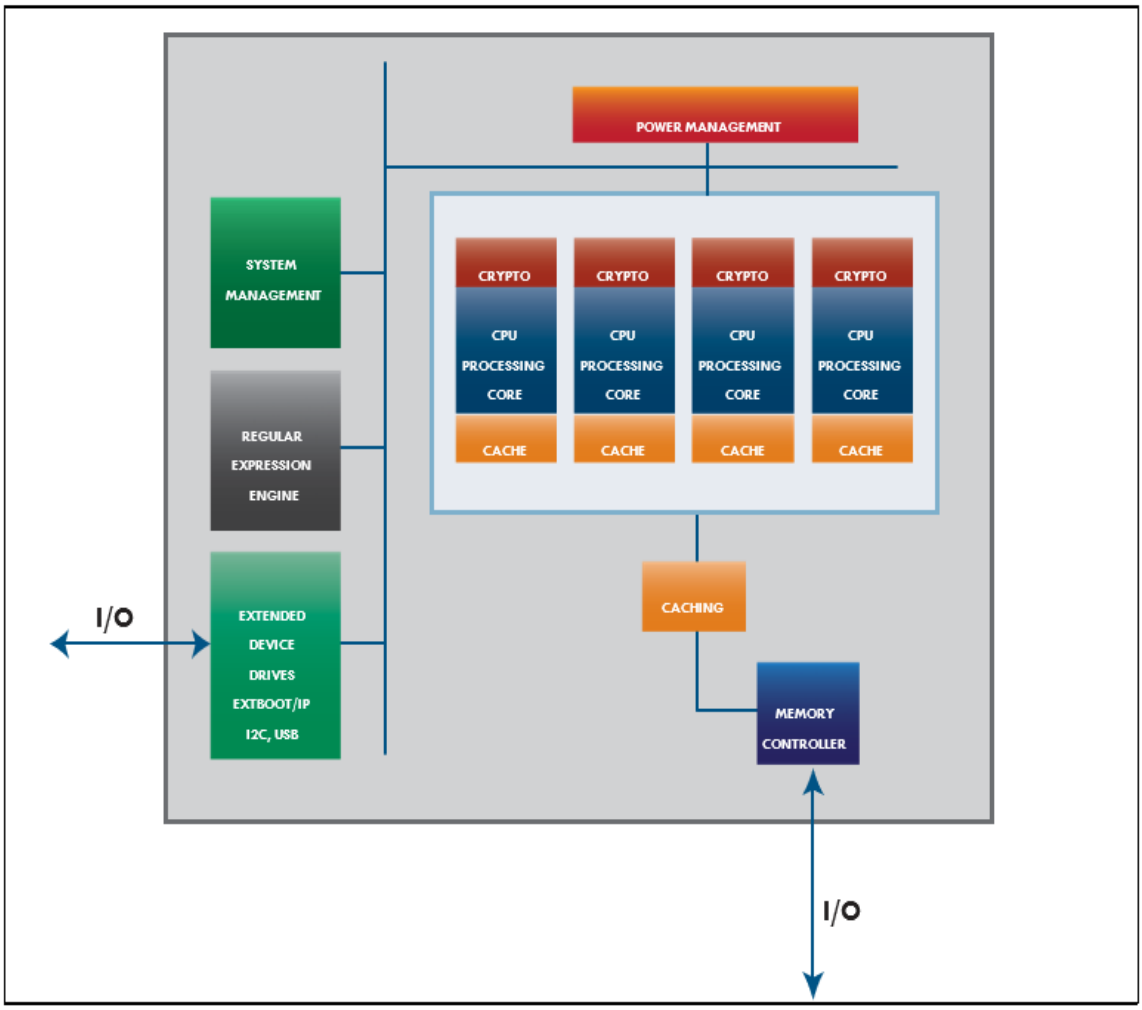

Figure 15 : On-chip hardware acceleration

Source: (Telesis)

3.8 Market overview of NGFW

3.8.1 History of market:

- Firewalls were first proposed in the late 1980s and then implemented as traffic-controlling devices.
- Firewalls have evolved four times, from simple packet filters (that evaluated source, destination, and protocol) to stateful inspectors (that "remembered" the nature of ongoing communications and the origin of the packets involved), proxies (that evaluated packet contents rather than just the packets), and finally, UTMs or Next Generation Firewalls (NGFWs) (Johansen, 2021).

For a more comprehensive firewall, the last edition-orginally known as UTM – began combining functions such as anti-malware and intrusion prevention. While the semantics are still up for debate, UTMs are now commonly referred to as NGFW.

Where it's going:

NGFWs reflect a shift towards more content-aware security, incorporating extra features includes such as:

- Data Leakage Protection (DLP)
- Network Access Control (NAC)
- Application control
- User identity-related controls on top of anti-malware and intrusion prevention and detection (IPS & IDS)

Web application firewalling is being incorporated by more and more manufacturers. As more businesses look for unified solutions for cost savings and resource management, the majority of standalone security solutions, such as DLP, will be replaced by NGFW. This year, some suppliers have already begun to phase out standalones (Generation of DDoS Attack Dataset for Effective IDS Development and Evaluation, 2018).

3.8.2 NGFW Vendor Selection:

While there is some discussion about the semantics of UTMs vs NGFW, the industry remains steady, with long-established suppliers and newer, but equally capable, rivals. Info-tech focused on vendors with extensive skills across several platforms and a strong market and/or reputational presence among mid and large sized business for this Vendor Landscape (Vendor Landscape: Next Generation Firewall).

Included in this Vendor Landscape:

Fortinet: The company that created the term "Unified Threat Management" and was one of the first to increased capabilities.

Barracuda: In terms of features, this is highly competitive solution that is also best kept secret in the space.

Check Point: Look at check point and it's one of the original firewalls companies and remains one of the most well-known.

Cisco: With Cisco's networking market share, the ASA firewall family remains one of the strongest options.

Dell (SonicWALL): Dell is a company that specialises in (SonicWALL). It has emerged as one of the stronger options in terms of features since being bought by Dell in 2012.

Juniper: Since acquiring NetScreen, the company has acquired a strong footing in the firewall sector.

McAfee: The addition of NGFW to the security giant's already extensive product range is a welcome addition.

Palo Alto: The newest arrival to the market among the solutions examined, but nonetheless providing a competitive answer.

Sophos: Cyberoam was purchased in 2014 to add to the company's NGFW portfolio.

WatchGuard: After focusing on the SMB sector for a while, another vendor is expanding into larger markets.

3.8.3 NGFW criteria and weighting factors

Product Evaluation Criteria

Features	The solutions offer both fundamental and sophisticated feature/functionality.
Usability	The administrative and end-user interfaces are simple to use and provide optimized workflow.
Affordability	Given the technology, implementation and running the solution is inexpensive.
Architecture	There are many deployment options and many integration options available.

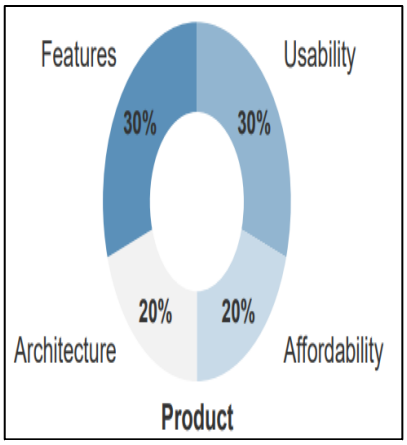

Figure 16 : Product Evaluation Criteria

Source: (Research)

Vendor Evaluation Criteria

Viability	Vendor is successful, knowledgeable, and well-versed in the industry.
Strategy	The vendor is dedicated to the market and has a roadmap for its future product and portfolio.
Reach	Vendor gives worldwide coverage, is capable of selling, and can offer post-sale support.
Channel	Vendor channel method is suitable and powerful by themselves.

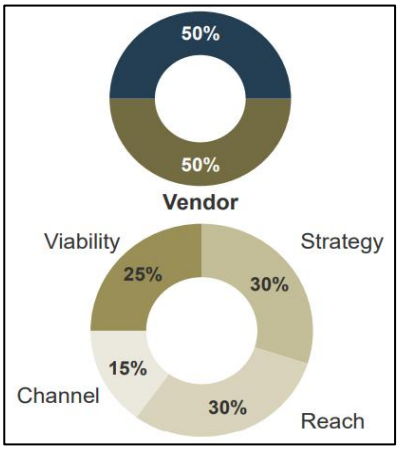

Figure 17 : Vendor Evaluation Criteria
Source: (Research)

3.8.4 Balance Individual strengths to find the best fit for enterprise

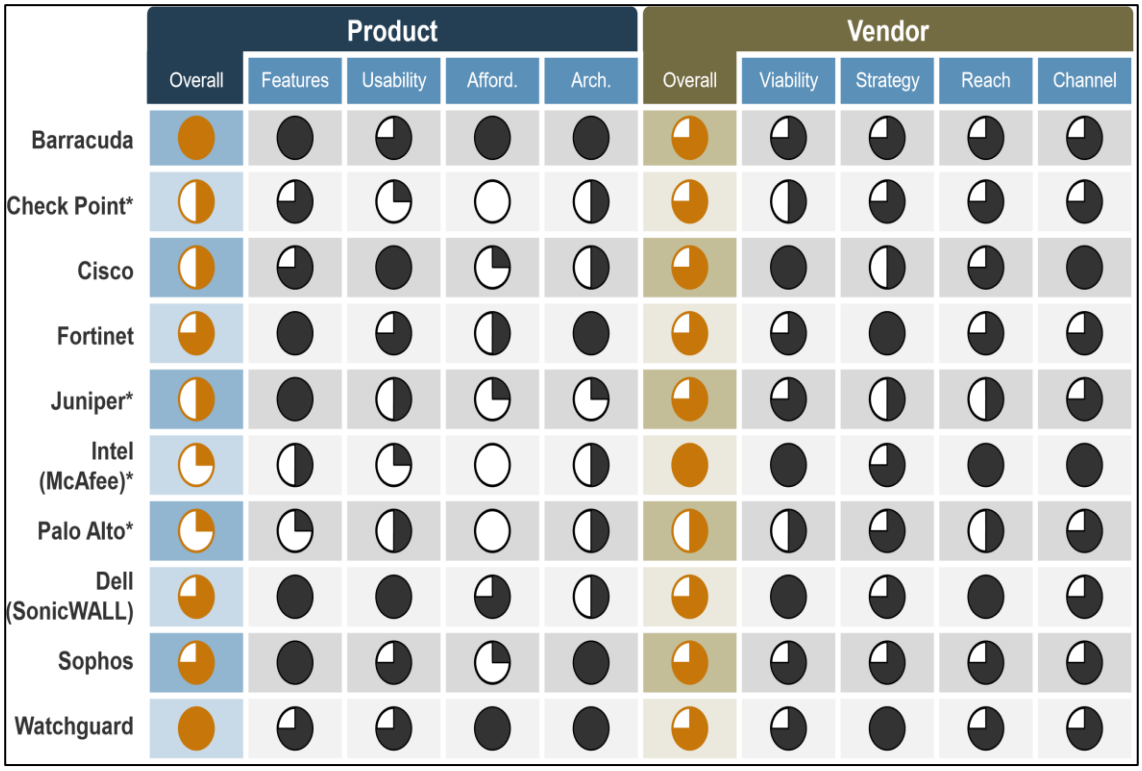

Figure 18 : Firewall vendors strength

Source: (Research)

3.8.5 Advanced features

Feature	What we looked for
Identity-based Control	Mapping of specific security guidelines to protect users as a whole and specific.

Data Leakage Protection	Restriction on the exist of sensitive, confidential or privileged data.
Network Access Control	Endpoint integration to use to ensure that the security of each connecting device is sufficient.
URL Filtering	Restricting access to hazardous and unsuitable websites during web browsing.
Application Control	Ability to granularly limit which online applications can be used.
Wi-fi Network Control	Ensuring that Wi-Fi networks are capable of and have the same security posture as a perimeter.
WAN Routing & Optimization	WAN traffic can be routed dynamically and supported by QoS and prioritizing features.
Encrypted Data Control	SSL and SFTP traffic native decryption and re-encryption for in-depth inspection.
Web App Firewalling	Being able to defend web servers from threats like SQL injections.

Each vendor offers a different feature set, concentrate on what your organization needs

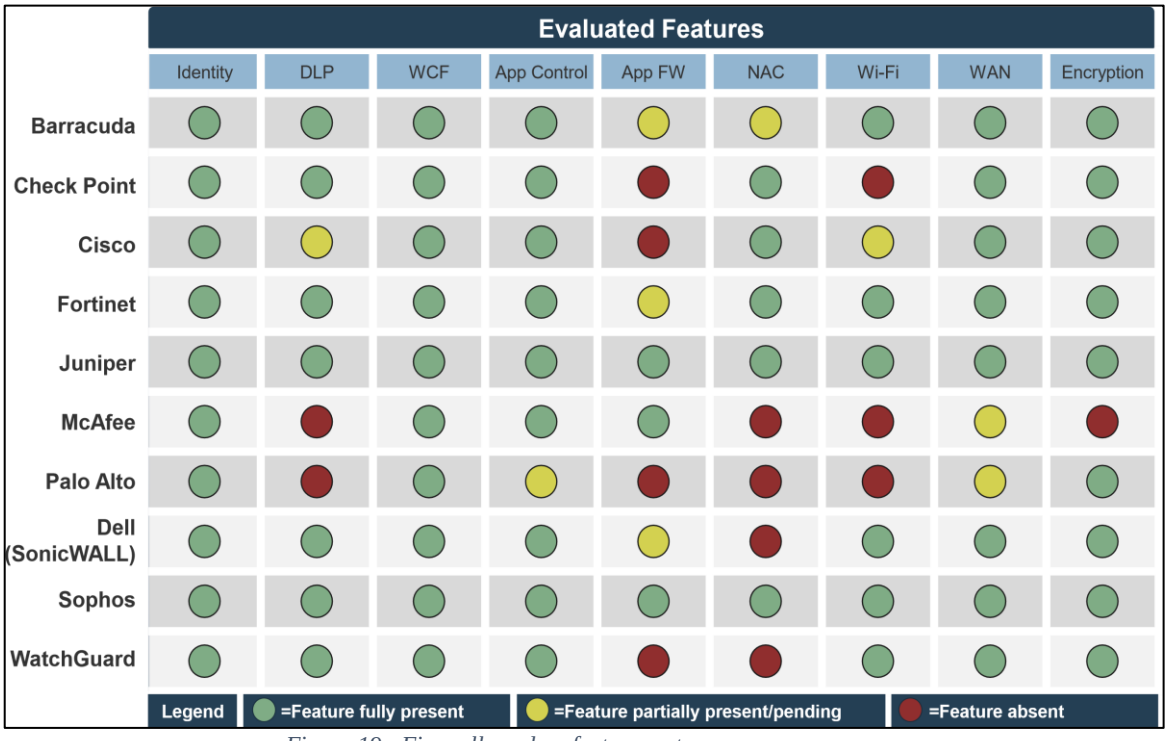

Figure 19 : Firewall vendors features set

Source: (Research)

3.8.6 Scenarios using the 10 NGFW vendors

When checking the devices bundled in each Vendor LandscapeTM, particularly examples are noteworthy. Info-Tech identifies such examples as scenarios and gives importance to them when they are valid, due to their applicability in specific locations, importance, or positives in providing a certain skill (Vendor Landscape: Next Generation Firewall).

1: Fortinet
Fortinet provides the best all-around NGFW solution on the market.

Overview
With its initial FortiGate, Fortinet helped define the UTM space. Even with its enlarged range, Fortinet's firewalls remain its strongest product.

Strengths
Fortinet provides a variety of deployment choices, including hardware appliances, cloud-ready, multi-tenant/virtual domain solutions, and AWS. Organizations are looking beyond hardware in today's diversified market, providing Fortinet a competitive advantage. Despite the fact that Fortinet has only been in the space since 2000, businesses may be assured in its entire stability and strong worldwide expansion – including support alternatives.

Challenges
Fortinet's web application firewall is available as a separate product rather than as a built-in feature of the NGFW.

FortiGate NGFW is feature rich, with flexible deployment options

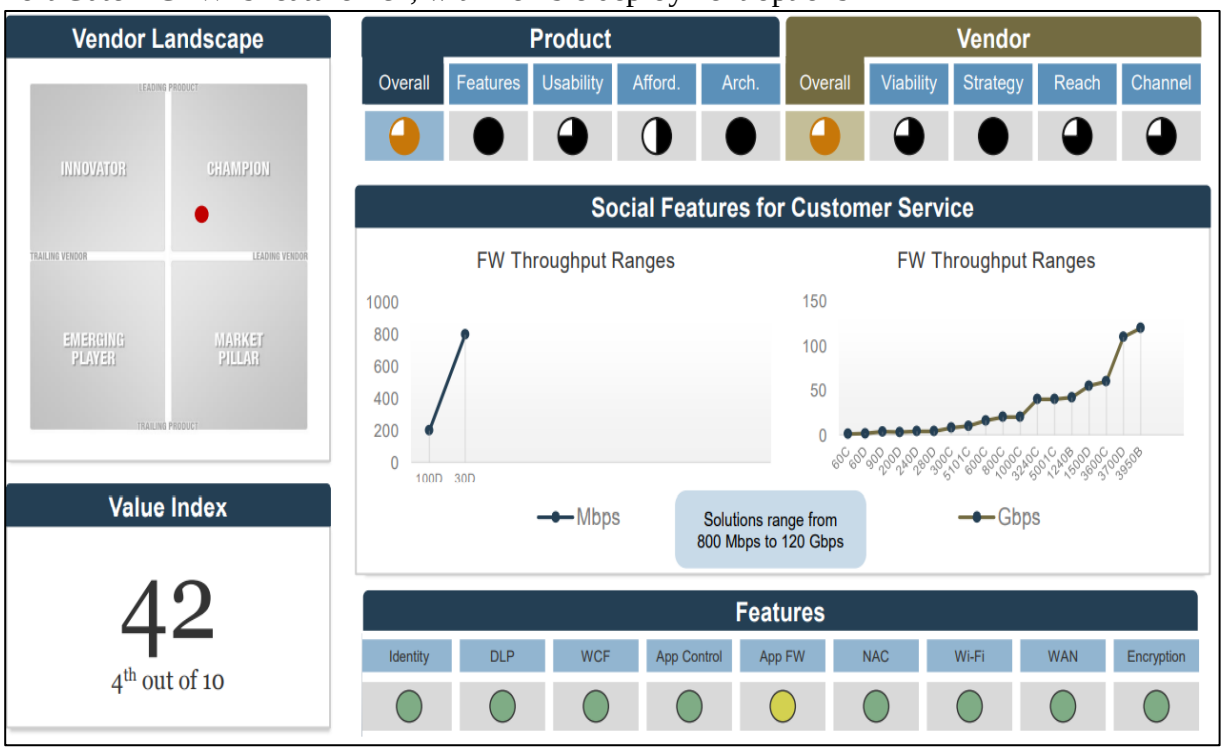

Figure 20 : Fortinet as vendor

Source: (Research)

Info-Tech recommends:
The FortiGate solution from Fortinet is great for companies who want a lot of bells and whistles but don't have the resources to pay for them. From cloud-ready choices to Amazon Web Services, the solution provides a variety of deployment options.

2: Palo Alto
It needs to enhance its NGFW offering to remain competitive.

Overview
Palo Alto launched its first appliance in 2007 and has since become a market standard, with over 17,000 clients in more than 120 countries.

Strengths
Palo Alto has an easy-to-use interface with a clear representative of traffic flow and user activity.

- The PA series includes hardware, software, and virtual platform deployment choices.
- Palo Alto isn't a pure-play vendor, but companies searching for a product that focuses more on NGFW than a broad range of solutions would like the fact that it is a top priority for Palo Alto.

Challenges
The PA Series, as a "newer" manufacturer in the field, lacks some essential advanced features like Wi-Fi Network Control, NAC, DLP, and web application firewalling, preventing it from genuinely competing in terms of total capabilities.
Palo Alto has flexible deployment officies, however it isn’t the best option in a competitve market.

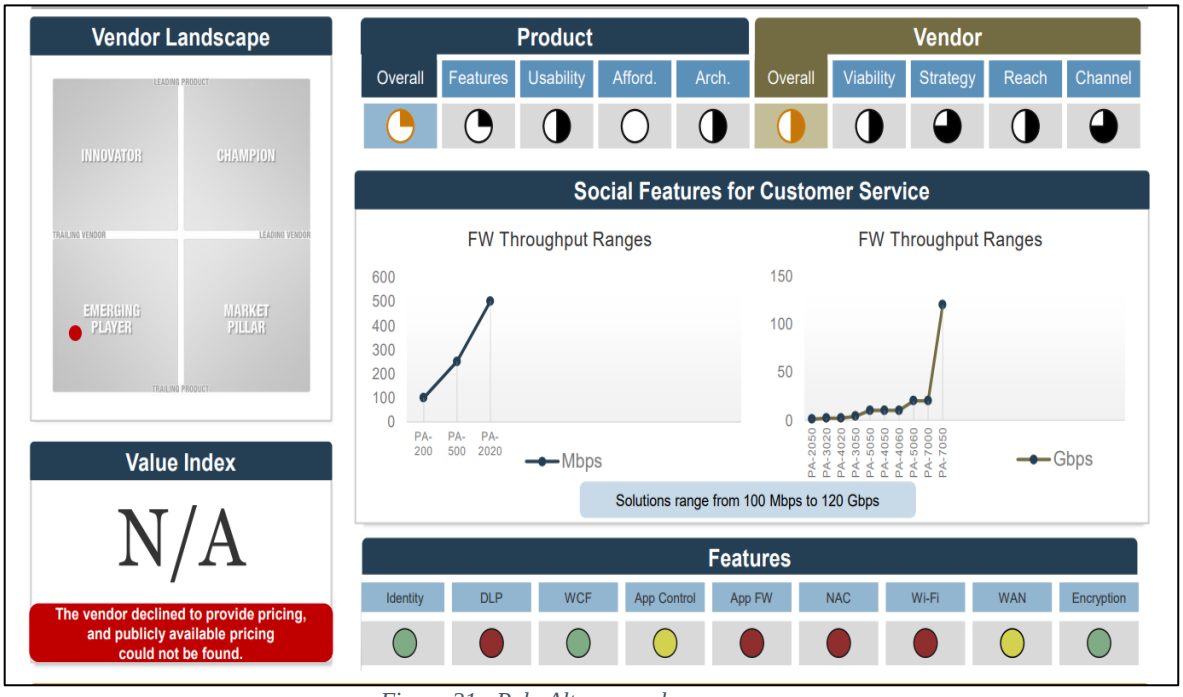

Figure 21 : Palo Alto as vendor

Source: (Research)

Info-Tech recommends:
Despite its concentration on Next-Generation Firewalls, Palo Alto, while a reliable manufacturer, lacks critical advanced functionality. Palo Alto Networks, on the other hand, has strong channel partners like RSA and Citrix, making them an appealing alternative for enterprises interested in that aspect.

3: Cisco
Cisco customers will love the ADA firewall family, which include a variety of deployment options.

Overview
Cisco is one of the largest firewall vendors in the world thanks to it's significant networking market share.

Strengths

- Cisco's ASA firewalls offer an easy-to-configure dashboard, with options for reporting such as identity-based reporting and devicebased reporting.
- Despite Cisco's image as a network vendor, its global presence has earned the ASA series a positive reputation, particularly within Cisco shops.

Challenges
There are no built-in templates for compliance needs such as PCI-DSS, which is a small flaw in the firewall's reporting capabilities.

Cisco makes a good firewall, but its more expensive than the competition.

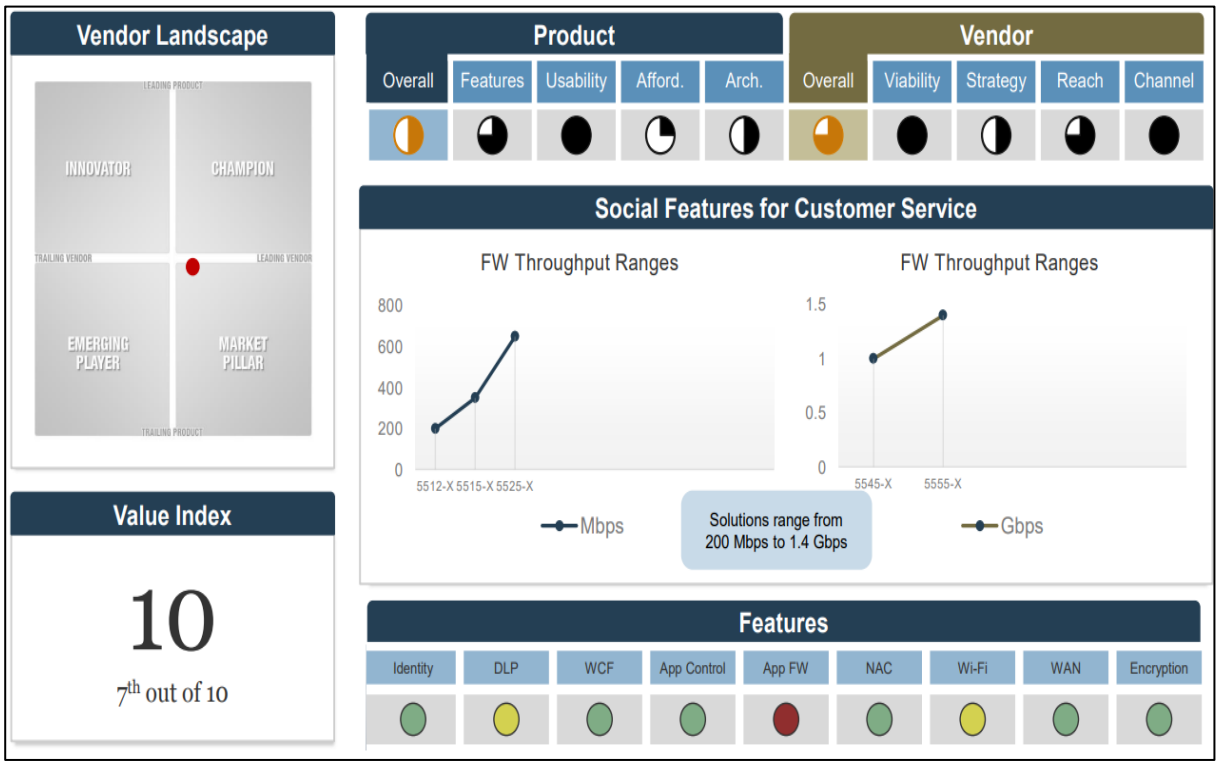

Figure 22 : CISCO as vendor

Source: (Research)

Info-Tech recommends:
Cisco has built a great reputation for its ASA firewalls by leveraging its network presence; but, a lack of deployment alternatives may turn off some enterprises looking for virtual appliances, for example. In any case, Cisco-shop enterprises will find the ASA solutions to be compatible with their existing architecture.

4: Checkpoint
It continues to be the standard for firewalls.

Overview
Checkpoint has been a long-time competitor in the security arena, and its primary focus has always been firewalls.

Strengths

- Checkpoint primary strengths are brand recognition and stability. Check Point's strong position in the market will appeal to organisations searching for industry standards and simple deployment options - hardware, software, or virtual.
- Checkpoint software blade architecture, with each feature available as an add-on blade, can give some companies with the flexibility they want.

Challenges
The software blade architecture has been described by some users as clumsy and complex, despite being one of its benefits.
Despite being one of the earliest firewall vendors, checkpoint has lagged behind in terms of innovation in recent years.

Check point provides some scalability and vendors trustworthiness.

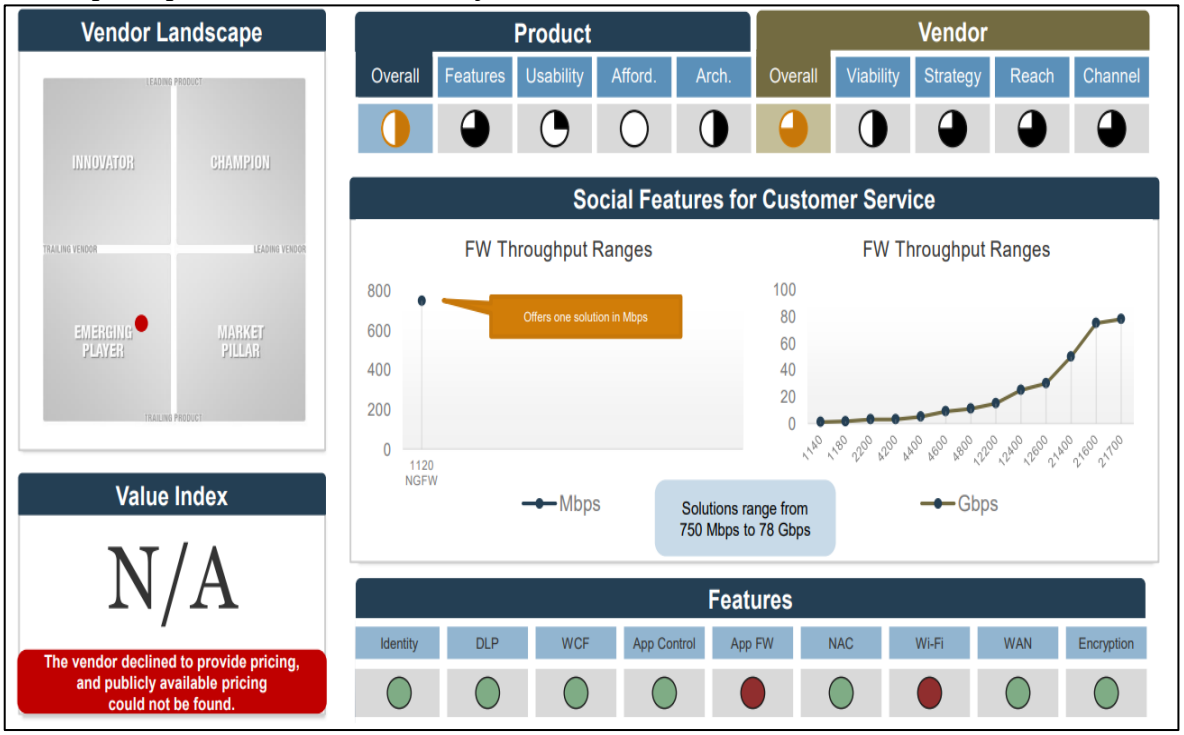

Figure 23 : Checkpoint as vendor

Source: (Research)

Info-Tech recommends:
When it comes to firewalls, Check Point is still at the top of the list. Check Point's Next Generation FW is a strong option for organisations looking for vendor longevity and enjoy Check Point's software blade architecture, which allows you to add whichever features you want.

5: Sophos
The SG series from Sophos is a market leader because to its extensive feature set ad high performance.

Overview
Cyberoam, a next-generation firewall firm, was acquired in 2014, reflecting the corporation's growing focus on the firewall area as they transition to the high-performance SG Series.

Strengths
The SG Series interface is highly configurable for network definitions, offers bandwidth control, a wide range of reporting options, drag-and-drop functionality for rule creation, and more.

Challenges
The Sophos product are often more expensive than similar solutions but, with this solution, you get exactly what you paid for.

Sophos high performance SG series demonstrate a competitive feature set.

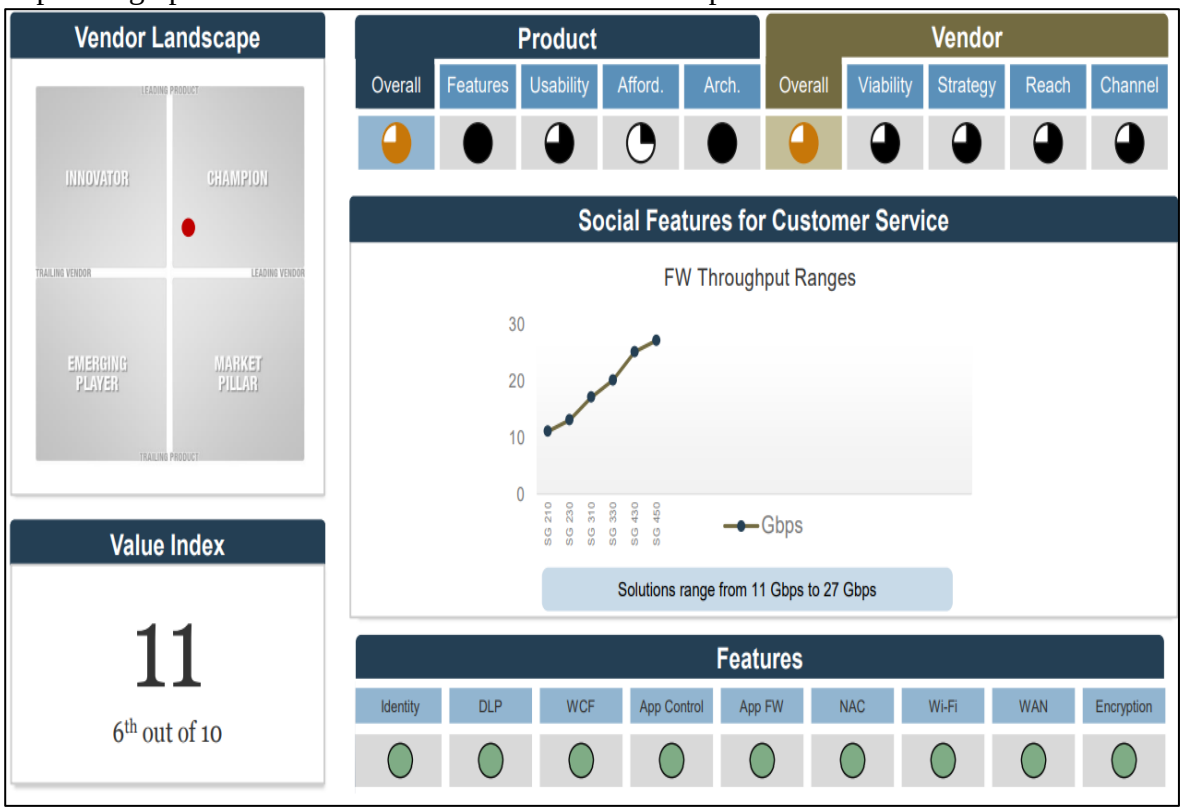

Figure 24 : Sophos as vendor

Source: (Research)

Info-Tech recommends:
All of the advanced features of Sophos' NGFW have been tested. One disadvantage of the seller is that its products are frequently on the expensive side. The comprehensiveness and performance of Sophos' firewalls will be appreciated by enterprises with the correct budget or larger organisations dealing with a lot of data.

6: Dell (SONICWALL)
Dell is one of the greatest all around systems on the market, as well as one of the most cost-effective.

Overview
Dell used its existing presence to develop a strong NGFW strategy after purchasing SonicWALL in 2012.

Strengths
The product's user interface was one of the most user-friendly of the solutions tested. It was interactive, with an appealing and informative geographical map showing the locations of the firewalls. It also offered data transfer reporting to monitor how much it cost the company on a daily basis (ideal for demonstrating product effectiveness).

Challenges
The NGFW series is currently only available in hardware and virtual deployments, restricting the alternatives accessible to enterprises for their NGFW.

The SuperMassive, NSA, and TZ series all offer one of the strongest feature sets in this evaluation

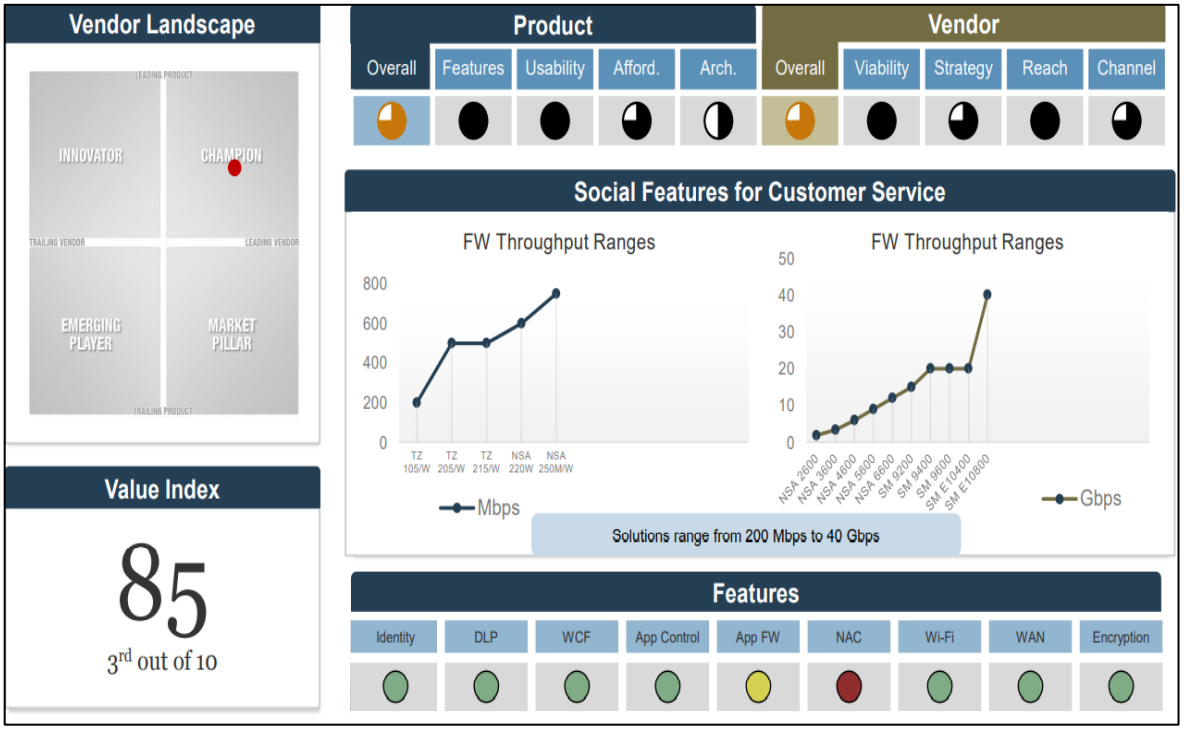

Figure 25 : Dell as vendor

Source: (Research)

Info-Tech recommends:
The one drawback to Dell (SonicWALLotherwise)'s excellent firewalls is that they presently only provide hardware and virtual deployment choices. Dell (SonicWALL) firewall systems, on the other hand, are suitable for enterprises looking for a highly competitive and economical solution.

7: Watchguard
The XTM series from WatchGuard is the best bang for any organization's dollars.

Overview
WatchGuard is a firewalling company that focuses on the needs of small businesses, though not solely. The business is robust, and the items are capable.

Strengths
The XTM series from WatchGuard provides the best bang for your buck, with a reasonable pricing for a reliable and expandable device. The XTM firewall can generate reports at multiple levels (executive dashboard, security dashboard, threat map, etc.), and each dashboard has several clickable components that present detailed event information in a visually appealing manner a distinction from its competitors.

Challenges
Some advanced functions, such as web application firewalling and network access control, are lacking from the XTM series.

In this review, WatchGuard's affordability is unrivalled.

Figure 26 : WatchGuard as vendor

Source: (Research)

Info-Tech recommends:
WatchGuard's XTM series delivers outstanding scalability and a great advanced feature set at a reasonable price, making it a viable solution for any-sized enterprise on a budget.

8: MCAFEE
Its vendor stability is insufficient to compensate for its lack of advanced capabilities.

Overview
McAfee is the world's largest specialised security solutions supplier and is now a wholly-owned division of Intel. It joined the firewall business when it bought Secure Computing in 2008.

Strengths
This vendor has unrivalled viability, reach, and channel skills, making it a vendor that organisations can rely on for a long-term partnership.
McAfee's comprehensive management platform, the ePolicy Orchestrator (ePO), is integrated with the management console. Through a single console, it provides centralised control of the full McAfee stack.

Challenges
Some critical advanced functions, like as DLP, NAC, Wi-Fi network control, and encrypted data inspection, are missing from McAfee's NGFW offering.

Despite being a security behemoth, McAfee is falling behind its firewall competition.

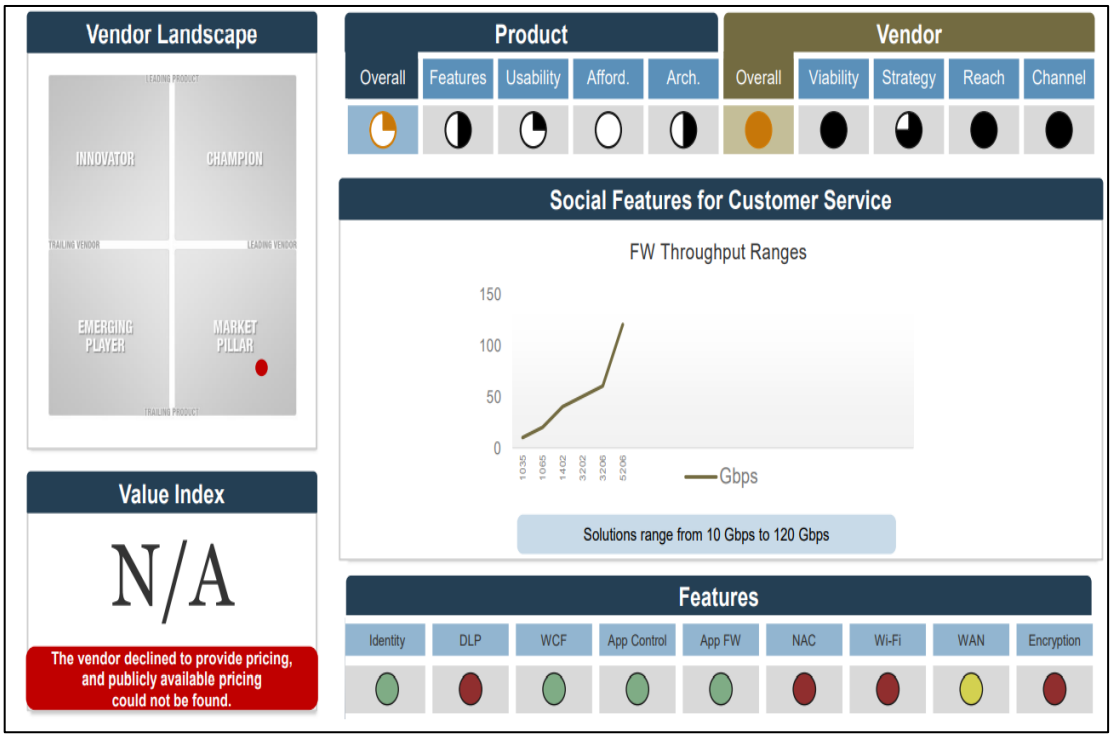

Figure 27 : McAfee as vendor

Source: (Research)

Info-Tech recommends:
The ePO Orchestrator and McAfee's market presence are the company's primary differentiators. Organizations that require convenience will appreciate the opportunity to manage their portfolio from a central location. Aside from that, the NGFW product lacks crucial advanced capabilities that have been available for years in its competitors' products.

9: Barracuda

With its strong solution and sturdy firewall, it's an excellent match for mid-sized businesses.

Overview

Barracuda's business model is based on low-cost, high-function spam and malware "firewalls," and the company has continued to expand its portfolio. It joined the NGFW industry when it bought Phion in 2009.

Strengths

Barracuda has one of the most comprehensive feature sets of the systems tested, including Data Leakage Prevention (DLP) and web application firewalling via its IPS engine.

The software also allows you to take a deep application dive, where admins can actually click on the files and see precisely what their users have been viewing, thanks to a column that provides real-time occurrences and fully customised reporting tools.

Challenges

Barracuda has been attempting to gain market share since entering the NGFW market a little later than its competitors; nonetheless, brand recognition is growing.

Barracuda is an underappreciated competitor with a viable alternative.

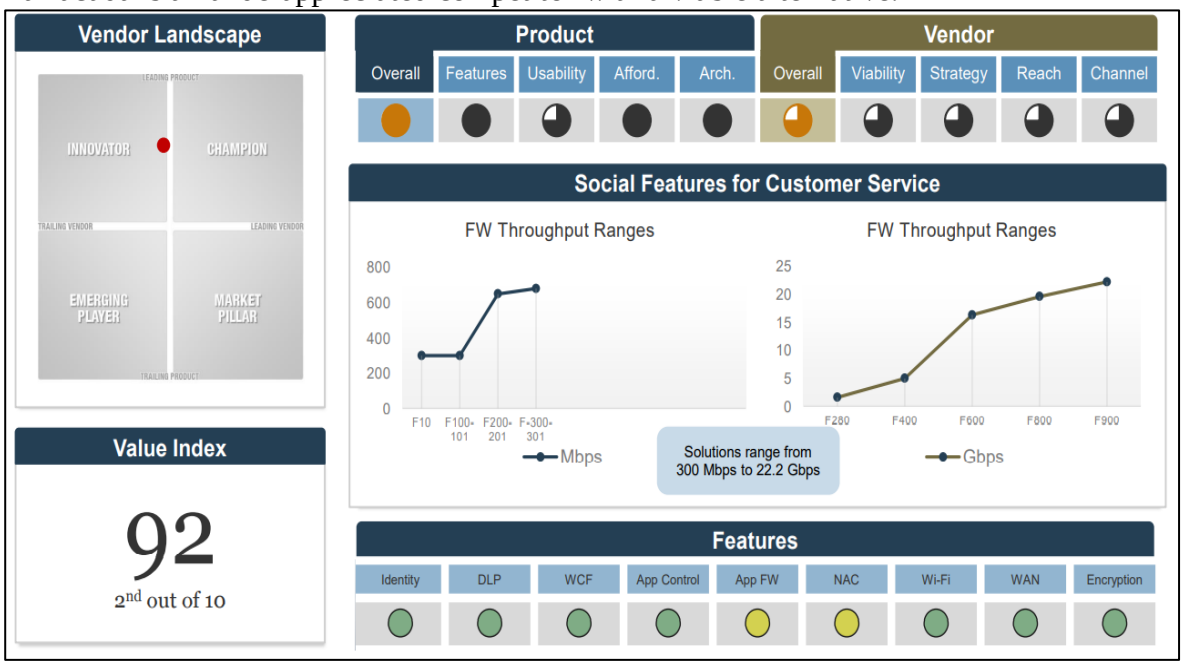

Figure 28 : Barracuda as vendor

Source: (Research)

Info-Tech recommends:
Barracuda may not be top-of-mind when it comes to these products, but organizations are aware of its good reputation in the space. This NGFW solution is ideal for mid-sized organizations looking for an option outside of their traditional choices.

10: Juniper

It's features set and product range make it one of the most robust solutions.

Overview

Juniper Networks is a networking and security firm that specialises on high-performance networking and security. The acquisition of NetScreen in 2004 laid the groundwork for the company's enterprise firewall capabilities, which are just one part of its market-leading security portfolio.

Strengths

The SRX series from Juniper has a comprehensive feature set, providing it a wide range of alternatives for companies seeking for a top-of-the-line solution. Juniper is a long-standing vendor that, although entering the firewall industry in 2004, has firmly established itself in the market thanks to its SRX product and channel strength. Juniper's Junos Central is an online community where clients can participate in training, live webinars, and other educational activities.

Challenges

Juniper has limited deployment options only hardware and software available.
Juniper's SRX series offers a full advanced features set for comprehensive protection.

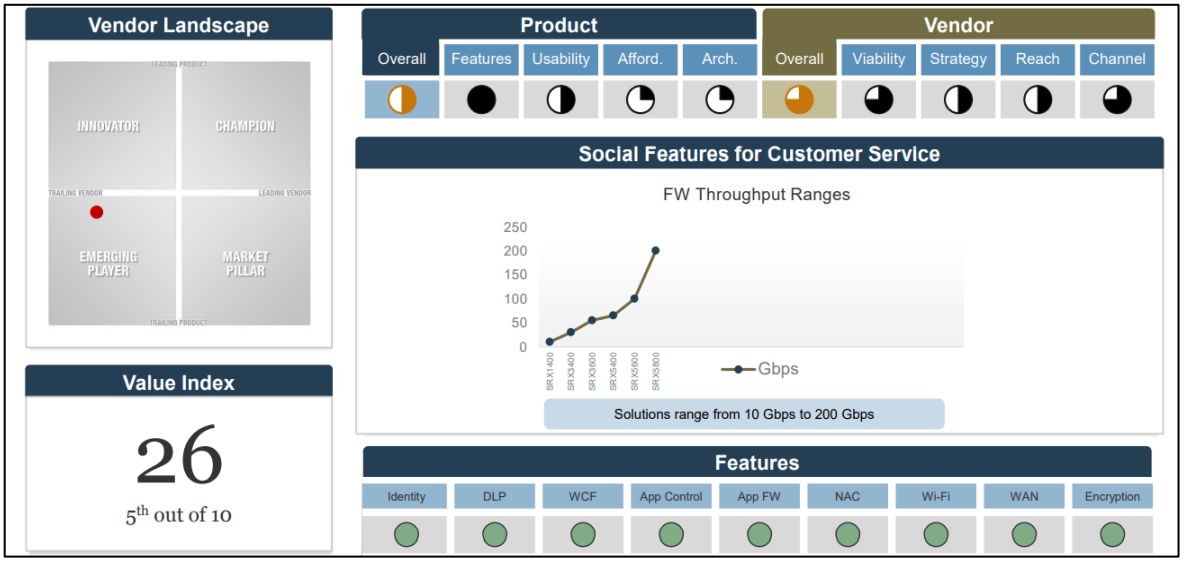

Figure 29 : Juniper as vendor

Source: (Research)

Info-Tech recommends:
Organizations looking for the ability to turn on all NGFW features should add Juniper to their vendor shortlist. One downside is that the scalability of the range is primarily for enterprise-sized organizations and may not appeal to mid-sized.

4 Practical Part

The practical part consists of different network topologies which includes majorly all network appliances used in current and proposed HLD and LLD of an organization. I used NGFW as a technology since it provides robust protection against some popular attack metrics like DDoS, phishing, malware, ransomware, man-in-the middle, etc. The primary justification for choosing NGFW is that it offers cutting-edge functionality for a business, including identity-based control, web app firewalling, data leakage prevention, network access control, URL filtering, application control, WAN routing & optimization, and Wi-Fi network control.
The best NGFW deliver five core benefits to organizations are as follows:

- Advanced breach prevention and security
- Visibility across the whole network
- Possibility for flexible deployment and management
- Shortest time to detect any threats
- Automation and product integration

I have chosen Fortinet as vendor for NGFW since it provides feature rich with flexible deployment options and it has strength to provides a variety of hardware appliances, cloud-ready, multi-tenant/virtual domain solutions, etc. Fotinet also provide wide range of support to all it's vendor in terms of software support, RMA (hardware replacement), technical fault, etc. Their software versions almost have zero vulnerability.

Newer versions of NGFW comprises of firewall part plus the NIPS which is IDS/IPS functionality all togther in one hardware. They are running in mixed mode for monitoring purpose as well as blocking purpose, I have mentioned more deatils about NIPS functionalities in chaper 4.4. Ususally in traditinal firewalls these two things were separated by individul devices, but in these newer versions of NGFWs specially with Fortinet vendor they are mixed and combined into one devices with both capabilties. Also comparing NGFW against traditional firewalls, that why NGFW is best and below are the major key points:

NGFW	**Traditional Firewall**
• Allows inspection of application-level through all layer 7. • Investigates all traffic actively to find threats. • Provides precise control over the functioning of the program. • Anti-malware, IPS and IDS security functions are integrated and managed as a single hardware.	• Keep track of network layer 2 through layer 4 traffic. • Offers no over specific application functionality. • Threats can get through buried in approved traffic. • Other security functions must be deployed and managed separately.

4.1 HLD (High Level Design) of enterprise without using NGFW – current

This High-Level Design is an industry standard and usually all Small-Medium Enterprises follow this type of topology as a baseline, if it is designed without NGFW in their network arsenal. More importantly if the userbase of a certain enterprise is not that hugely significant then most of the enterprises go without an NGFW on their network structure. But because these NGFW are so versatile as well as integral part of security and robustness of managing the network more efficiently, I am trying to portray that why it is important plus inevitable to include a good NGFW in any network design.

The below figured shows the network topology without NGFW of an enterprise where there is no grouping of traffic, so basically all the traffic moves from single point, and it doesn't matter if its internal or external traffic (3rd party traffic).

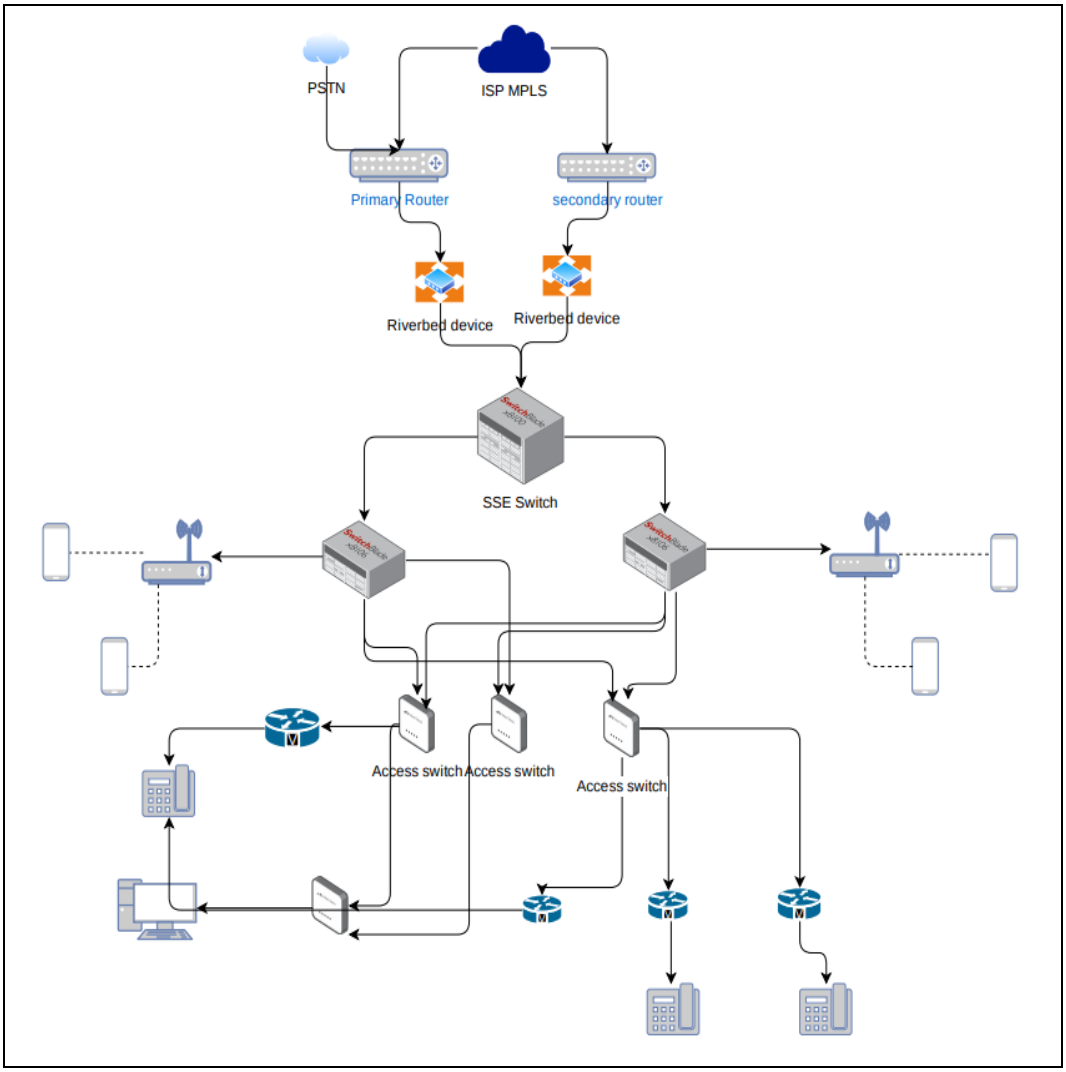

Figure 30 : HLD without NGFW - Own Processing

4.2 HLD (High Level Design) of an enterprise using NGFW – proposed

The below figured shows the network topology with NGFW of an enterprise where there is grouping of traffic, so basically traffic is distributed with different point, and it defines that internal traffic doesn't need to go under monitoring/analysing and 3rd party traffic (external traffic) must go under proper analysing in order to secure the enterprise/organization most important data structure and information.

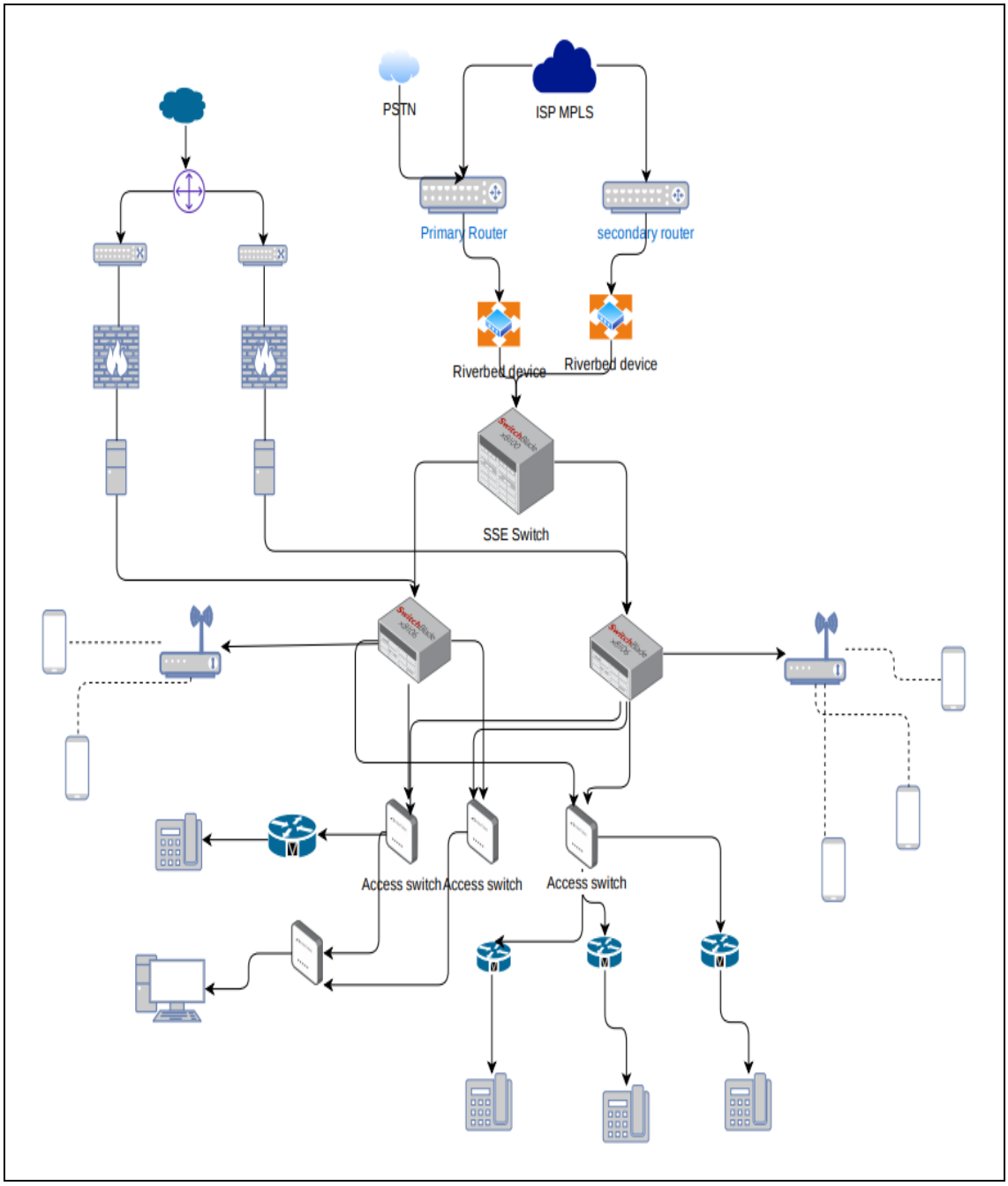

Figure 31 : HLD with NGFW - Own Processing

Cabling details

Sr No.	Between Devices	Cable model
1	Router and Riverbed	Crossover
2	Riverbed and NGFW	Crossover
3	Riverbed and Core Switch	Straight
4	NGFW and Core Switch (L3)	Straight
5	Router and NGFW	Straight

Details of appliances and it's vendor

Sr No.	Appliances	Vendor
1	Router	Cisco
2	Core Switch	Cisco
3	Access Switch	Cisco
4	Riverbed	Cisco
5	NGFW	Fortinet

The NGFW deployed on both MPLS (primary and secondary) and both FortiGate running on 6.4.10 version which we can considered as update to date version for some big organization. To avoid TCP SYN assault, UDP flood attack, DHCP Starvation attack, DDoS attack, and restrictive lateral attack movement, policies will be implemented and configured on the Next-Generation firewall FortiGate. It's also feasible that if a company/organization simply wants to permit a small number of IP addresses, they only need to configure and implement those IP addresses and rules on FortiGate.

using FortiGate's Next-Generation Firewall, a network security technology that can lessen attacks from both internal and external networks. The Intrusion Prevention System (IPS) functionality was integrated into next-generation firewall devices in line mode to protect against attacks on traditional firewall core networks or no firewall protection in the suggested extra devices architecture. To make sure that only clients with registered Media Access Control (MAC) addresses and VLANs can connect to the network or the internet, earlier VLAN and port security divisions are implemented on the access switch

4.3 Tests by using FortiGate

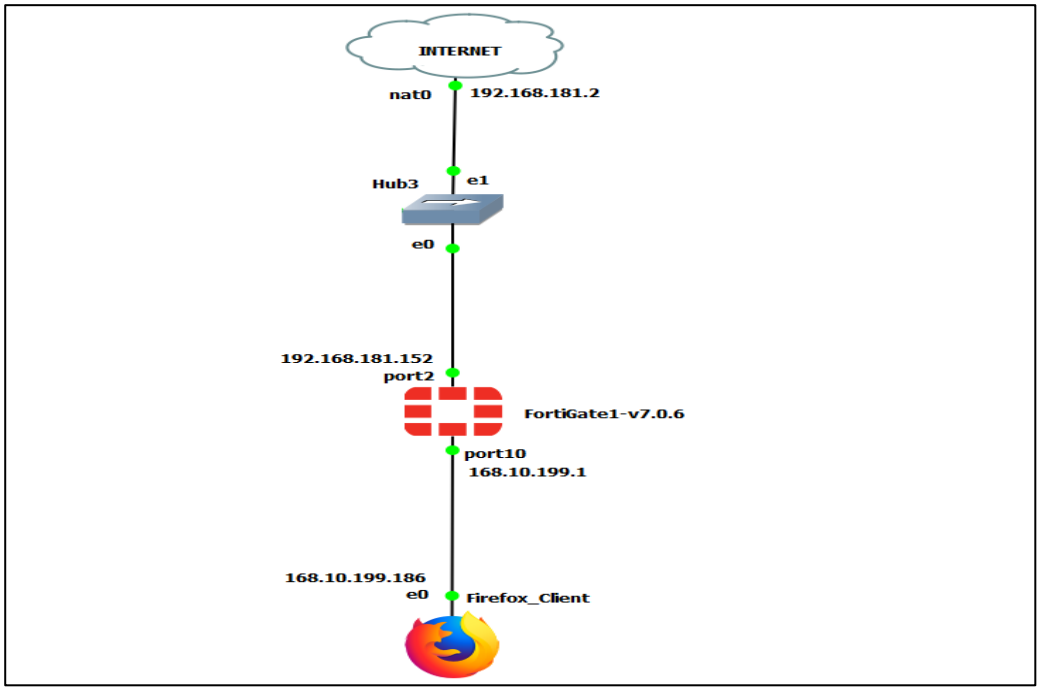

Figure 32 : FortiGate test - own processing

In above figure I have introduced Next-Generation Firewall and carried about below mentioned tests:

SSL Inspection

SSL inspection helps user with privacy, data integrity, authentication, enhance image, secure transaction between customers and business, secure FTP service, secure access control panel, etc.

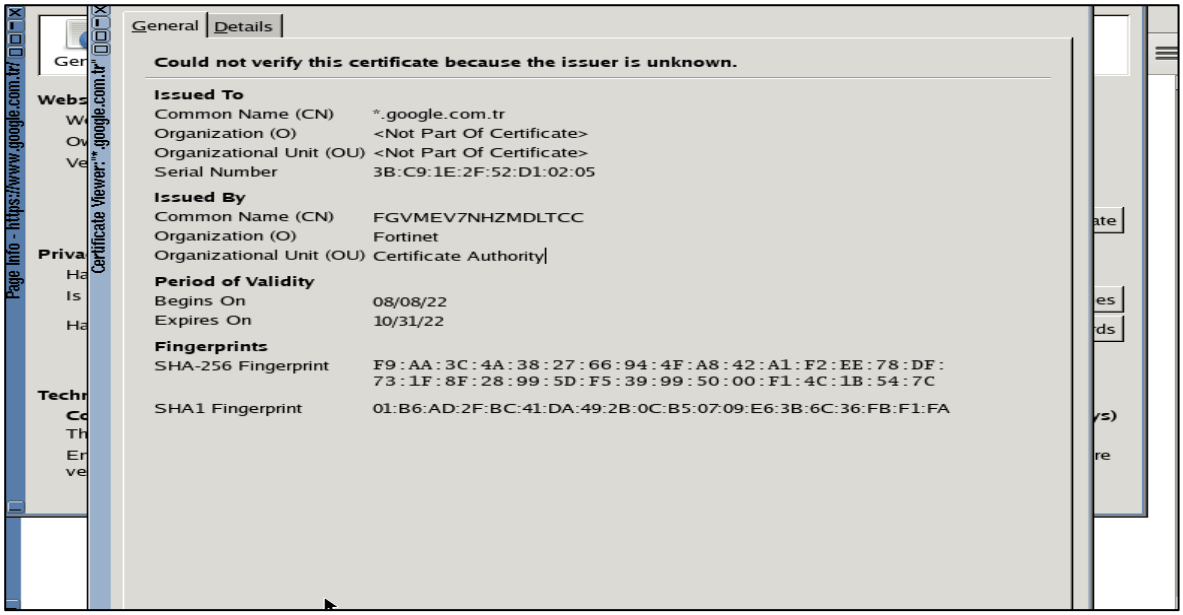

Figure 33 : SSL Insection result I - Own Processing

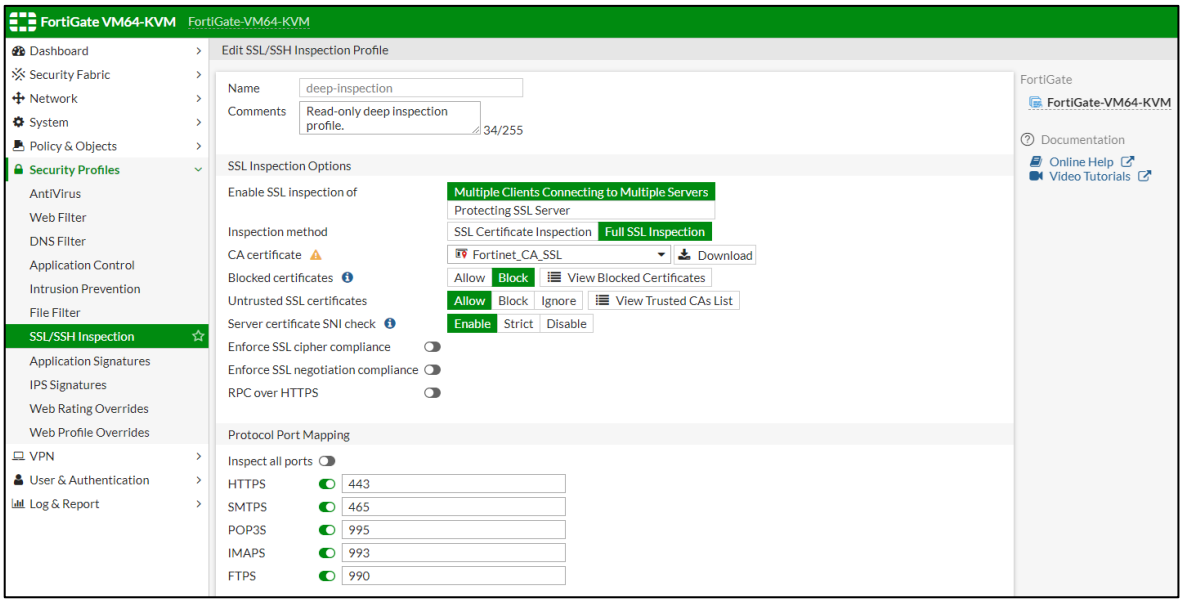

Figure 34 : SSL inspection result II - Own Processing

Web-filter Block

By using this policy organization can be protected by blocking access to malicious, hacked or inappropriate websites.

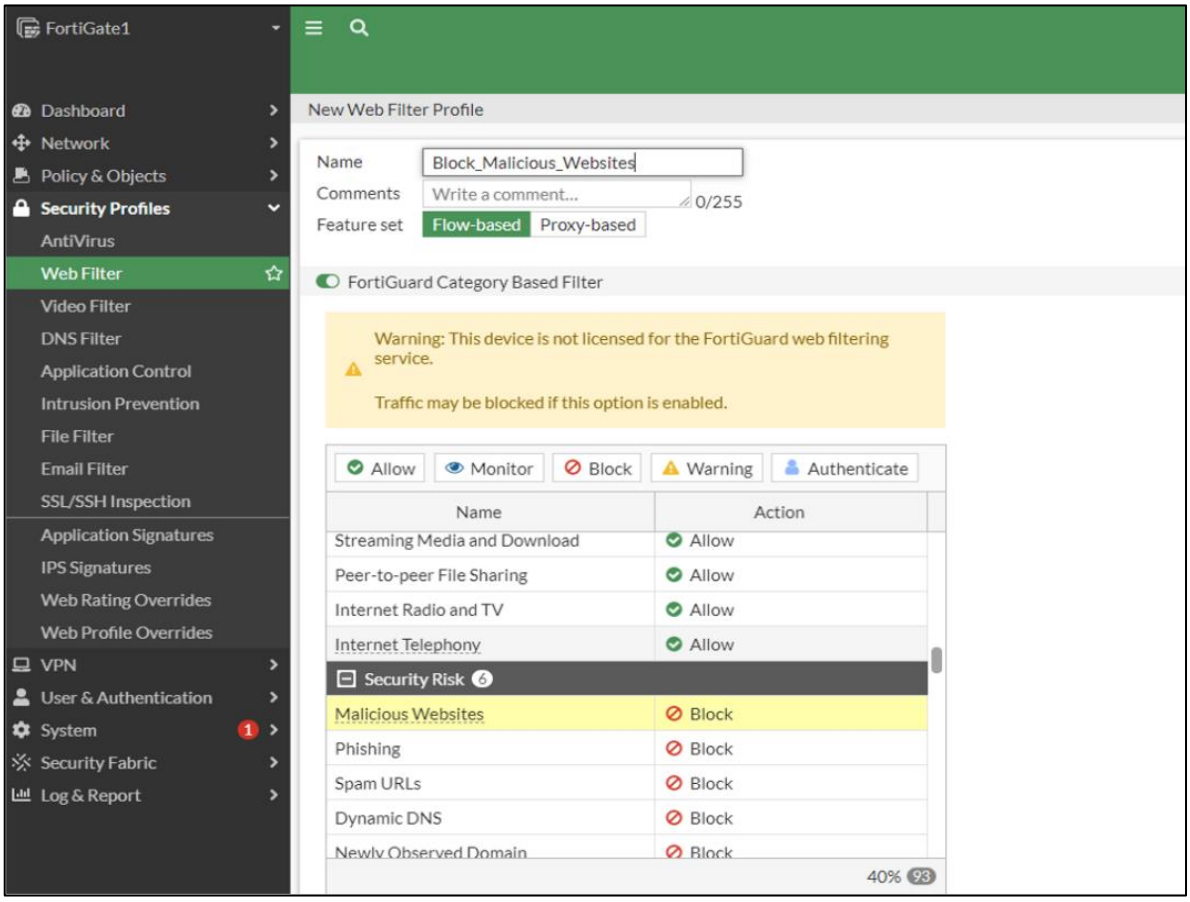

Figure 35 : Web filter result I - Own Processing

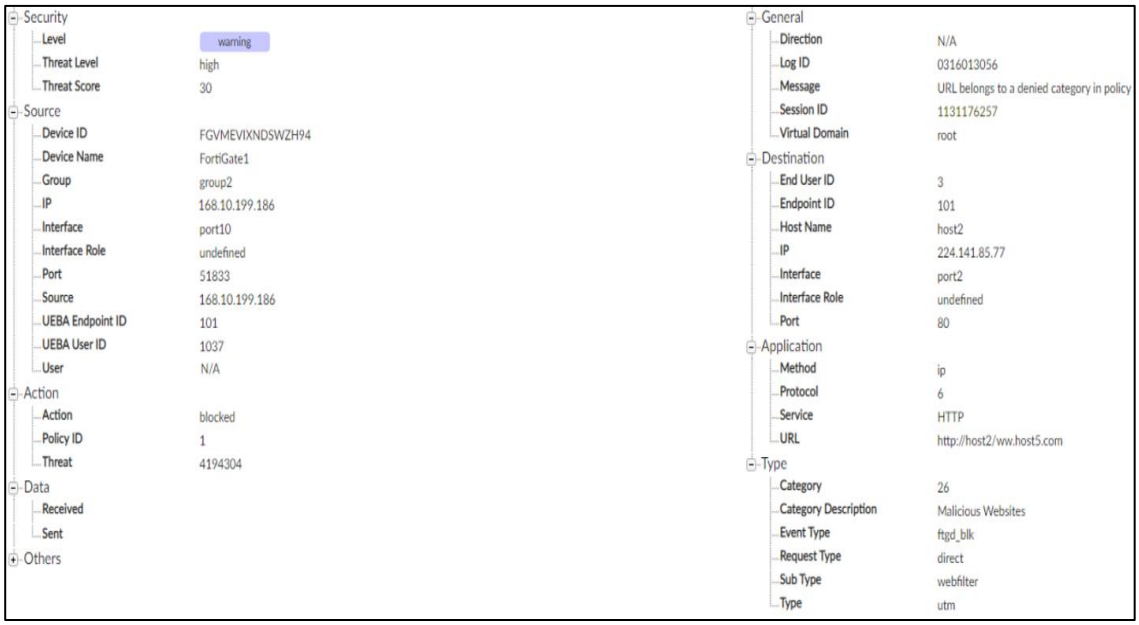

Figure 36 : Web filter result II - Own Processing

Anti-Virus Block

The benefit of this policy is to allow the flexibility of deploying suitable protection according to security needs and infrastructure designs.

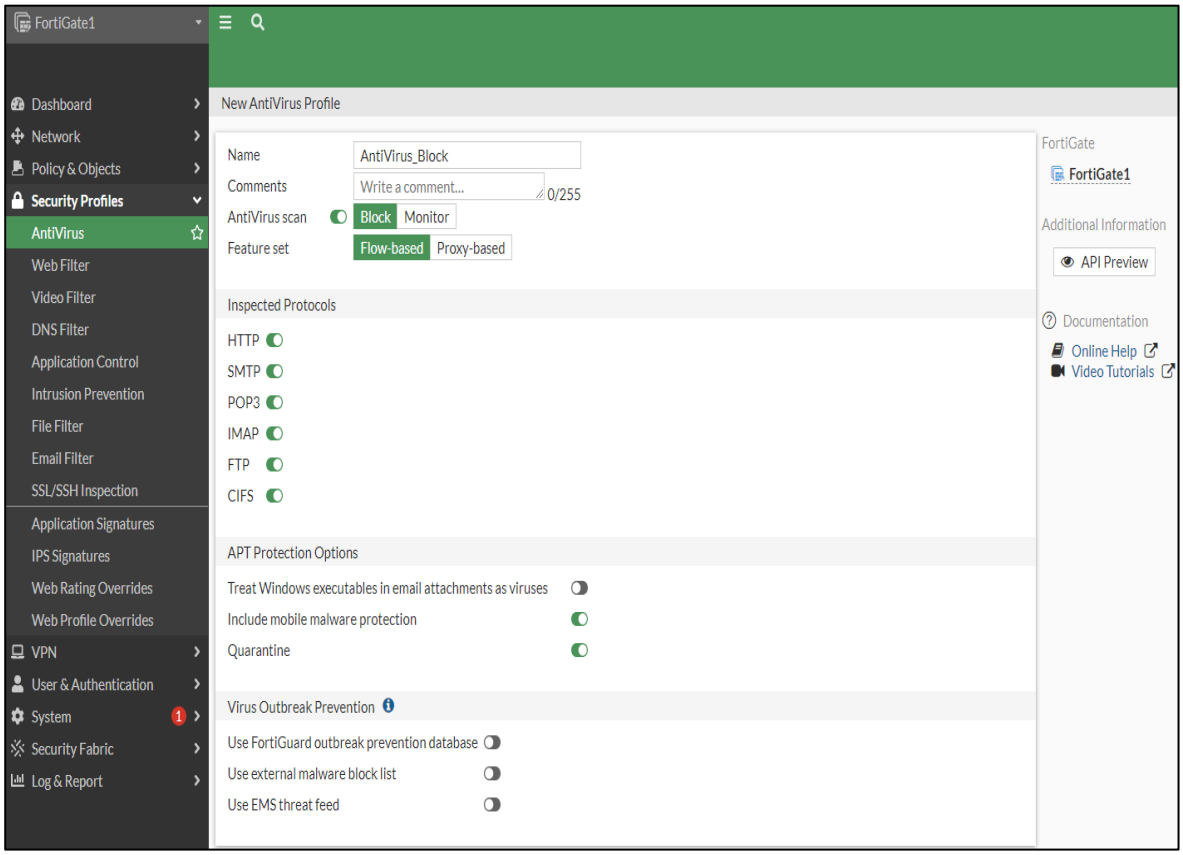

Figure 37 : AntiVirus result I - Own Processing

Figure 38 : AntiVirus result II - Own Processing

Application control Block

Basically, it allows organizations to easily control application usage and meet compliance requirements while also advancing their overall security posture. It also provides usage of trends over time as well as real-time visibility into all applications running on the network.

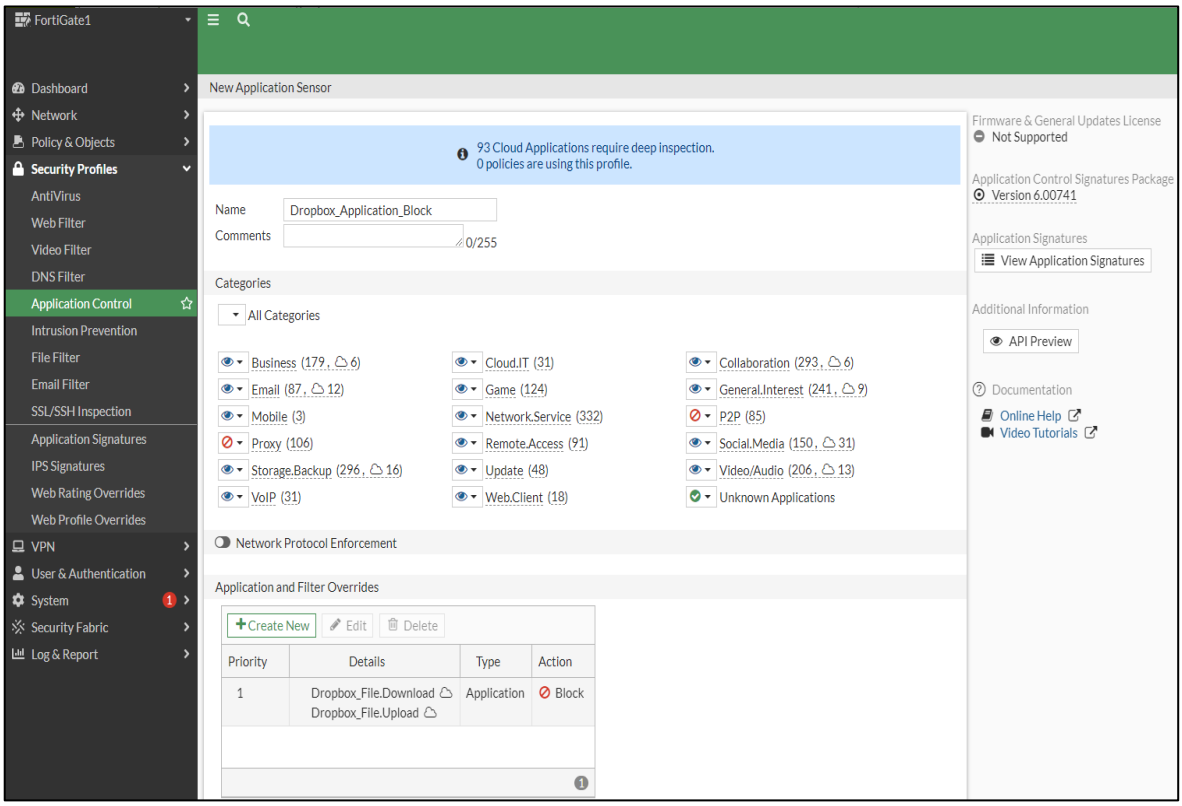

Figure 39 : Application control block I - Own Processing

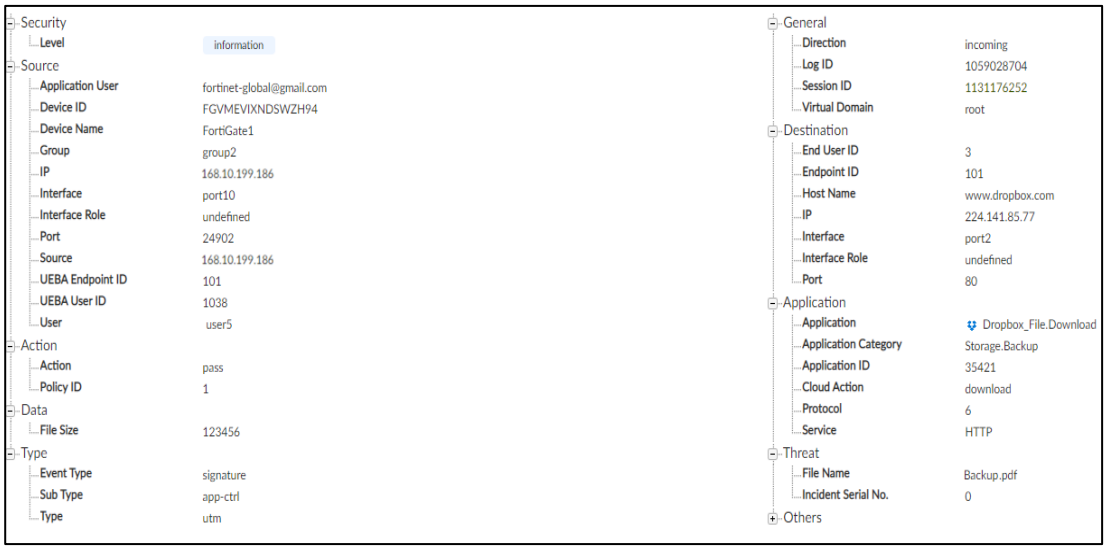

Figure 40 : Application control block II - Own Processing

4.4 Introducing NIPS to enhance more security of enterprise/organization

NIPS – Network Intrusion Prevention System
Below are the few points about NIPS:

- It protects the local LAN from attacks initiated from other locations.
- It prevents malicious network traffic from consuming bandwidth.
- It blocks or allows network traffic based on given network-based criteria, as well as other criteria including applications, users, URLs, IP address reputations, and result of intrusion or malware inspections.

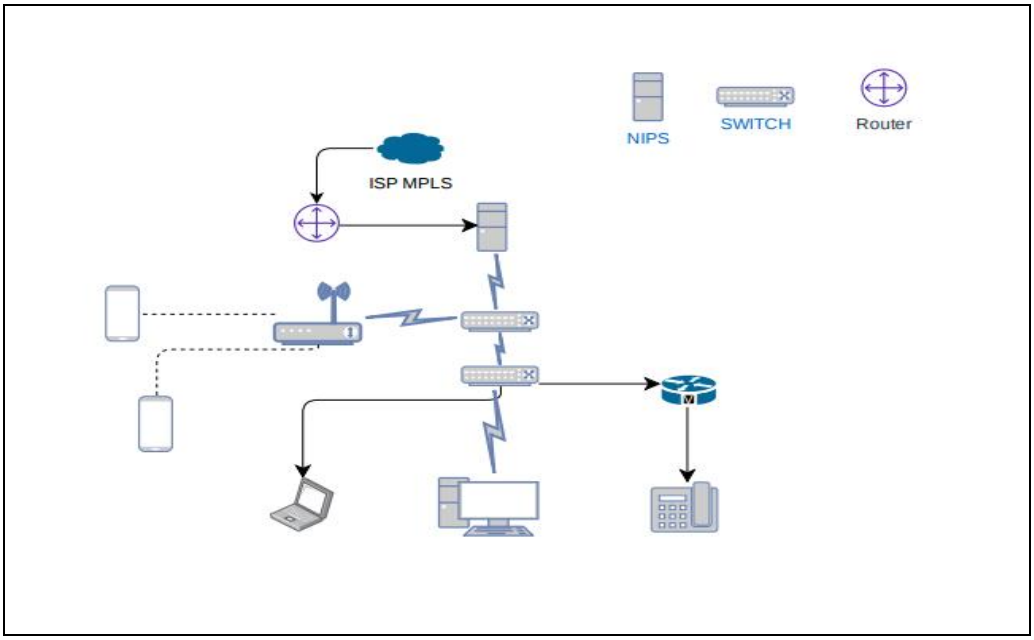

Figure 41 : Introducing NIPS - Own Processing

The enterprise/organization who are having more than 10,000 employees are using some standard form to deploy/introduce NIPS device to their network and the main pre-requisites to deploy NIPS is to have Layer 3 core switch.

Below are the three major stages:

- Installation – this stage includes physical installation of device (racking, power connection, management port connection and initial setup).
- Inlining – this stage includes applying rules to the device, make connection to NIPS device from router to NIPS and then NIPS to switch before this stage there was direct connection from router to switch.
- Blocking – this stage will be cover after few days of analysing the traffic via NIPS engine and from the traffic report organization/enterprise can set rules like what needs to whitelist and blacklisted and after the last stage the NIPS device started protecting the infrastructure and blocking malicious traffic which can be harmful for internal network.

Following are the proprietary commands for Fortinet to deploy both, NGFW as well as NIPS, functionalities on their console:

config system interface
edit (port name)
set ip a.a.a.a/aa
set allowaccess ping https ssh fgfm
next
end

config router static
edit (port number)
set dst ab.ab.ab.ab.ab.ab.ab.ab
set gateway x.x.x.x
set device (port name)
next
end

4.5 Below is the approx. price list of Fortinet devices and license for 1 year

Fortinet model	Hardware Price	Licence for 1 year price
FortiGate 60E	1000 - 1100 USD	700 – 800 USD
FortiGate 80F	1600 - 1700 USD	1300 – 1400 USD

Many businesses and organizations choose "Enterprise Protection (IPS, Advanced Malware Protection, Application Control, Web & Video filtering, Antispam, Security rating, IOT Detection, Industrial Security, FortiConverter SVC, and 24*7 Forticare)" out of the various license types that are offered with various services.

	Firewall	IPS	NGFW	Threat Protection	Interfaces
FortiGate 60E	3 Gbps	400 Mbps	250 Mbps	200 Mbps	Multiple GE RJ45 – PoE/+interfaces
FortiGate 80F	10 Gbps	1.4Gbps	1 Gbps	900 Mbps	Multiple GE RJ45 – PoE – DSL – 3G4G – variants with internal storage - WiFi

5 Results and Discussion

As the goal of this thesis, next-generation firewalls FortiGate will prevent attacks from internal networks on a typical firewall core network. The effectiveness of the testing done with FortiGate's Next-Generation Firewalls gives organizations and businesses the confidence and clarity they need to use these firewalls.

With SSL inspection, web filter blocking, anti-virus blocking, application control blocking, etc., FortiGate can help.

Using Fortinet vendor will be the best option for any enterprise/organization according to my research since it’s having the best functionalities and cost effectiveness.

6 Conclusion

Keeping track of all incoming and outgoing network traffic and accepting or rejecting data packets in accordance with a set of security rules, a firewall is a piece of network security equipment. A firewall can be hardware or software, however having both is ideal. NGFW, proxy firewall, and other types of firewalls are examples of many sorts. A typical firewall monitors network traffic continually. Based on the state, port, and protocol of the traffic, it filters it using settings that the administrator has established. All these different aims are fulfilled by NGFWs. NGFWs can deal with latest threats in terms of modern malicious software and application-layer threats as well as access control. The redefined security, attack prevention, and network-wide monitoring of next-generation firewalls should be bundled together. Along with customizable administration and deployment options, the quickest detecting time, product integration, and automation options are offered.

A trusted internal network and an unreliable external network are separated by traditional and next-generation firewalls, but they accomplish this goal in very different ways. By combining traditional firewall functionality with other types of network device filtering, NGFWs achieve the granular control required to handle the challenges of today's threat landscape, making them the ideal choice for all businesses and organizations that can't afford to take any chances when it comes to cybersecurity.

Market overview shows us the different vendors with extensive skills across several platforms and a strong market and/or reputational presence among mid- and large-sized businesses for this Vendor Landscape.

Based on the results the proposed solutions shows that the Next-Generation firewall FortiGate can prevent attacks from internal users and reduce assaults from internal networks. With the addition of more devices, the Next-Generation firewall FortiGate may improve network security compared to traditional firewalls. This study, however, has several limitations, notably in terms of the type of attack that was investigated. In this study, only network devices with standard firewalls from internal networks were included.

7 References

A history and survey of network firewalls. **Ingham, Kenneth L. 2002.** 2002, Sv. 5.

Abubakar, Rana, a další. 2020. *An Effective Mechanism to Mitigate Real-Time DDoS Attack.* Lahore : IEEE, 2020. Sv. 8. 2169-3536.

Ali, Amir a Yousaf, Muhammad Murtaza. 2020. *Novel Three-Tier Intrusion Detection and Prevention System in Software Defined Network.* Lahore : IEEE, 2020. Sv. 8. 2169-3536.

Barker, Keith a Morris, Scott. 2012. *CCNA Security.* místo neznámé : Cisco Press, 2012. 9780132966061.

Bul'ajoul, Waleed, James, Anne a Shaikh, Siraj. 2019. *A New Architecture for Network Intrusion Detection and Prevention.* Nottingham : IEEE, 2019. Sv. 7. 2169-3536.

Comer, Douglas E. 2009. *Computer Networks and Internets.* New Jearsey : Pretice Hall, 2009. 0-13-091449-5.

Design and Evaluation of Enterprise Network with Converged Services. **Surantha, Nico. 2018.** Tokyo : Bina Nusantara University, 2018.

Detection of slow port scans in flow-based network traffic. **Ring, Markus, Landes, Dieter a Hotho, Andreas. 2018.** Coburg : autor neznámý, 2018.

Erlacher, Felix a Dressler, Falko. 2020. *On High-Speed Flow-Based Intrusion Detection Using Snort-Compatible Signatures.* Berlin : IEEE, 2020. stránky 495-506. 1941-0018.

Firewalls: A study on Techniques, Security and Threats. **Kalpesh, Pooja a Goel, Anjuli. 2019.** Chandigarh : autor neznámý, 2019.

Forcepoint. What is firewall? *Forcepoint.* [Online] [Citace: 10. January 2022.] https://www.forcepoint.com/cyber-edu/firewall.

Generation of DDoS Attack Dataset for Effective IDS Development and Evaluation. **Sabah Alzahrani, Liang Hong. 2018.** Nashville : Journal of Information Security, 2018. 2153-1242.

Gutmann, Peter. 2004. *Cryptographic Security Architecture: Design and Verification.* Berlin : Springer, 2004. 978-1-4419-2980-8.

Hayden, Lance. 2010. *IT security metrics: A practical framework for measuring security & protecting data.* New York : McGraw Hill, 2010. 978-0-07-171340-5.

Hunter, Alex. 2021. Perimeter Firewall: What is it, and how does it work? *Parallels Perimeter firewall.* [Online] 1. June 2021. [Citace: 1. February 2022.] https://www.parallels.com/blogs/ras/perimeter-firewall/#:~:text=A%20perimeter%20firewall%20is%20a,of%20defense%20in%20enterprise%20security.

Hybrid intrusion detection and signature generation using DeepRecurrent Neural Networks. **Kaur, Sanmeet a Singh, Maninder. 2020.** místo neznámé : Springer, 2020.

Improving Network Security: Next Generation Firewalls and Advanced Packet Inspection Devices. **Thomason, Steven. 2012.** 13, Greenville : Global Journals Inc., 2012, Sv. 12. 0975-4172.

Internal Threat Defense using Network Access Control and Intrusion Prevention System. **Surantha, Nico a Andhika, Surya Putra. 2019.** Tokyo : International Journal of Advanced Computer Science and Applications, 2019, Sv. 10.

Intrusion Prevention And Detection in Small to Medium-Sized Enterprises. **Choi, Young B. a Allison, Gregory D. 2017.** 2017.

Johansen, Alison Grace. 2021. What is firewall? Firewalls explained and why you need one. *Norton.* [Online] 17. June 2021. [Citace: 11. January 2022.] https://us.norton.com/internetsecurity-emerging-threats-what-is-firewall.html.

McMillan, Troy. 2012. *Cisco networking essentias.* Indianapolis : Sybex, 2012. 978-1-118-09759-5.
Mendes, S.N. Dorogovtsev and J.F.F. 2003. *Evolution of Networks: From Biological netss to the Internet and WWW.* New York : Oxford University Press, 2003. 0198515901.
Myriam Dunn, Victor Mauer. 2007. *The resurgence of the state: Trends and processes in cyberspace governance.* England : Routledge, 2007. 9780754649472.
Network firewalls. **Ingham, K., & Forrest, S. 2006.** New Mexico : Enhancing computer security with smart technology, 2006.
Neupane, Kishan, Haddad, Rami a Chen, Lei. 2018. *Next Generation Firewall for Network Security: A Survey.* Florida : IEEE, 2018. 978-1-5386-6133-8.
Razzak, Hasina A., a další. 2017. A Methodical Approach to Implement Intrusion Detection System. 2017, Sv. 7, 3.
Rengaraju, Perumalraja, Ramanan, V. Raja a Lung, Chung-Horng. 2017. *Detection and prevention of DoS attacks in Software-Defined Cloud networks.* Taipei : IEEE, 2017. 978-1-5090-5569-2.
Research, Info-Tech. Vendor Landscape: Next Generation Firewall. *Watchguard NGFW Landscape.* [Online] [Citace: 12. December 2021.] https://www.watchguard.com/docs/analysis/Next_Generation_Firewall-Vendor_Landscape.pdf.
Senthilkumar, Dr. P. 2020. *Fundamentals of computer networks and data communications: Princples and Paradigm.* Mauricius : LAP LAMBERT Academic, 2020. 978-6202516075.
Silva, Renato S. a Macedo, Evandro L. C. 2017. *A cooperative approach for a global intrusion detection system for internet service providers.* Brazil : IEEE, 2017. 978-1-5386-1332-0.
Silva, Renato Souza. 2017. *A Cooperative Approach for a Global Intrusion Detection System for Internet Service Providers.* 2017. 1570386330.
Soewito, Benfano a Andhika, Charlie Erwin. 2019. *Next Generation Firewall for Improving Security in Company and IoT Network.* Surabaya : IEEE, 2019. 978-1-7281-3749-0.
Sudonull. 2019. Typical NGFW implementation scenarios. *Sudonull NGFW.* [Online] 2019. [Citace: 25. January 2022.] https://sudonull.com/post/8106-Typical-NGFW-implementation-scenarios.
Surantha, Nico. 2019. *Evaluation of network security based on next generation intrusion prevention system.* Tokyo : autor neznámý, 2019. Sv. 17. 1693-6930.
Technologent. How Next-Generation Firewalls Protect against Today's Security Threats. *Technologent security threats.* [Online] [Citace: 27. January 2022.] https://blog.technologent.com/how-next-generation-firewalls-protect-against-todays-security-threats.
Telesis, Allied. NGFW Architecture. [Online] [Citace: 3. January 2022.] https://www.alliedtelesis.com/sites/default/files/documents/configuration-guides/understanding_ngfw_architecture.pdf.
Vendor Landscape: Next Generation Firewall. **Research, Info-Tech.**
What is a Next-Generation Firewall. **Systems, Cisco. 2022.** místo neznámé : Cisco Systems, 2022.