Kalle Kokko

Next-generation firewall case study

Bachelor's thesis
Information Technology

2017

South-Eastern Finland
University of Applied Sciences

Tekijä	Tutkinto	Aika
Kalle Kokko	Insinööri (AMK)	Joulukuu 2017

Opinnäytetyön nimi	
Tapaustutkimus seuraavan sukupolven palomuureista	57 sivua 91 liitesivua

Toimeksiantaja

Kaakkois-Suomen Ammattikorkeakoulu XAMK Oy

Ohjaaja

Yliopettaja Martti Kettunen

Tiivistelmä

Tämän opinnäytetyön tavoitteena on tutkia seuraavan sukupolven palomuuria sekä sen tarjoamia palomuuraustekniikoita. Työn on myös määrä luoda opetusmateriaalia nykyisille ja uusille Kaakkois-Suomen Ammattikorkeakoulun opiskelijoille.

Opetusmateriaalin on tarkoitus toimia XAMK:n Virtuaalilaboratoriossa virtuaalisilla laitteilla fyysisten sijaan. Opetusmateriaalin on myös tarkoitus tukeutua vahvasti Palo Alto Networksin tarjoamaan harjoitusmateriaaliin. Virtuaalilaboratorion ansiosta riippuvuus fyysistä laitteista katoaa. Virtuaalilaboratorio myös mahdollistaa laitteiden ja niiden toiminnallisuuden tarjoamisen entistä useammalle opiskelijalle samanaikaisesti riippumatta sijainnista.

Seuraavan sukupolven palomuurit ovat suhteellisen uusi ilmiö. Kyseiset laitteet pystyvät tunnistamaan kulkevan liikenteen ohjelmapohjaisesti, riippumatta käytettävästä portista, protokollasta tai suojauksesta. Seuraavan sukupolven palomuurit tarjoavat yritysten tietoturvatiimeille paremmat työkalut sallia ja estää jo valmiiksi piiloutuvaa sekä välttelevää liikennettä.

Työssä käytettiin Palo Alto Networksin tarjoamaa seuraavan sukupolven virtuaalista palomuurilaitetta sekä Ciscon ASAv virtuaalipalomuuria. Työ keskittyi pääasiallisesti Palo Alto Networksin laitteen toimintoihin ja sen tarjoamiin palomuuraustekniikoihin. Laitteen kaikkia teknologioita ei tämän opinnäytetyön puitteissa päästy hyödyntämään täyteen potentiaaliinsa, mutta opinnäytetyö tarjoaa pohjan jatkokehitysmahdollisuuksille tuleville vastaaville töille.

Opinnäytetyö oli onnistunut ja sen myötä luotiin kattava tapaustutkimus liittyen Palo Alto Networksin palomuurin toimintoihin. Työohje käsittelee palomuurilaitteen perustoimintoja ja kehittyneempiä toimintakonsepteja. Työn tekovaiheessa ei ollut mahdollisuutta yhdistää virtuaalilaitteita Internetiin, joka rajoitti suodatettavan sovellusliikenteen mahdollista määrää ja erinäisten Palo Alto Networksin tarjoamien pilvipalveluteknologioiden hyödyntämisen tämän työn puitteissa. Virtuaalilaboratorion kehittyessä myös demonstraatiomahdollisuudet kehittyvät.

Asiasanat

seuraavan sukupolven palomuuri, virtualisointi, NGFW, tietoturva, Palo Alto Networks

Author	Degree	Time
Kalle Kokko	Bachelor of Engineering	December 2017
Thesis title Next-generation firewall case study		57 pages 91 pages of appendices
Commissioned by South-Eastern Finland University of Applied Sciences XAMK Ltd.		
Supervisor Martti Kettunen, Principal Lecturer		

Abstract

The objective of this Bachelor's thesis is to research a next-generation firewall and the firewalling techniques it offered. There is also a need to create case study material for the students of South-Eastern University of Applied Sciences regarding the given firewall.

The case study material was to function virtually in XAMK's Virtual laboratory instead of physical appliances. The case study material was to be heavily based on practice material provided by Palo Alto Networks. Because of the Virtual laboratory the dependency for physical devices in teaching is voided. It also gives the ability to serve more students simultaneously, regardless of location.

Next-generation firewalls are a relatively new phenomenon. The given appliances can identify traffic flowing across networks on application-basis, regardless of port, protocol or encryption in use. Next-generation firewalls give security teams of enterprises much more comprehensive tools to allow and block evasive traffic.

A Palo Alto Networks virtual next-generation firewall appliance and a Cisco ASAv virtual firewall appliance were used in this thesis. The thesis itself focused mainly on Palo Alto Networks firewall appliance and advanced technologies they offer. All of the said technologies couldn't be fully utilized to their full extent possible, but this thesis offers a solid basis to complementary theses for future development.

The thesis was successful and a rather comprehensive case study guide was created regarding the Palo Alto Networks firewall appliance features. The case study covers the appliance's basic functions and more advanced operation concepts. Whilst making the case study there was no way to connect laboratories to Internet, which limited the range of possible application traffic data flowing across networks, and cloud-based services offered by Palo Alto Networks to be utilized within the limits of this thesis. As the Virtual laboratory develops, so does the demonstration possibilities.

Keywords

next-generation firewall, virtualization, NGFW, information security, Palo Alto Networks

CONTENTS

ABBREVIATIONS

ACC	Application Visibility & Control
App-ID	Application Identification
ARP	Address Resolution Protocol
ASDM	Adaptive Security Device Manager
AV	Anti-Virus
CLI	Command Line Interface
DB	Database
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DoS	Denial of Service
GUI	Graphical User Interface
HA	High Availability
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange version 2
IPsec	Internet Protocol Security
KVM	Kernel-based Virtual Machine
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
NAT	Network Address Translation
NGFW	Next-Generation Firewall
OS	Operating System

PA	Palo Alto
PAT	Port Address Translation
QoS	Quality of Service
RAM	Random Access Memory
SA	Security Association
SNMP	Simple Network Management Protocol
SOHO	Small Office/Home Office
SSH	Secure Shell
SSL	Secure Sockets Layer
TCB	Transport Control Block
TCP	Transport Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UI	User Interface
URL	Uniform Resource Locator
User-ID	User Identification
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network
WF	WildFire (Appliance)

1 INTRODUCTION

As Internet expands and technologies behind it develop rapidly so does the applications that generate traffic traversing it. The said traffic is not only Web surfing, but applications being accessed by network users for both personal and business use. Many of the said applications improve user and business productivity, while some consume large amounts of bandwidth, pose needless security risks, and increase business liabilities. (Miller 2011.)

As Internet develops, so does the threat landscape. Applications have become evasive and utilize, e.g., encryption to ensure the privacy and protection of data that is being sent via untrusted networks. Enterprises have also simultaneously utilized different kinds of security solutions, e.g., IPSs, proxies and other complex appliances alongside traditional firewalls to enhance their security policies. Such networks containing complex interconnected security devices are troublesome to manage and are expensive to maintain in the long run, not to mention issues regarding scalability. (Miller 2011.)

To fight against such developing and increasing threat landscape, next-generation firewalls are deployed on enterprise networks to give security teams freedom to enhance and enforce company's security policies. Next-Generation firewalls utilize the basic, port-based, technologies of traditional firewalls, but utilize more advanced and heuristic technologies in conjunction, e.g., URL filtering and sandboxed environments to fight against unknown threats. (Miller 2011.)

The goal of this bachelor's thesis is to research, to design and to create case study material regarding next-generation firewalls for students of the South-Eastern University of Applied Sciences by utilizing virtual laboratories. The case study material is to be heavily based on teaching material provided by Palo Alto Networks.

The case study is to provide understanding about fundamental firewalling technologies and best practices. The main goal was to teach students to think of networks surrounding firewall as indistinct security zones. There was also the need to be an emphasis on security policy management.

Besides giving basic understanding about the NGFW appliance itself the basic configuration emphasizes the importance of zones regarding interface configuration. The basic policies consist of allowing traffic to flow between trusted, untrusted and DMZ networks although so that DMZ and untrusted networks aren't allowed to initiate traffic to trusted network. Trusted network is allowed to initiate connections to untrusted network and the traffic is allowed to return if not detected as malicious. This includes and demonstrates the implicit deny rule of firewalls; everything is denied by default if not explicitly allowed by another rule.

The more advanced features were to consist of proprietary technologies (see chapter 4) provided by the NGFW appliance retailers. Most of such technologies vary greatly between retailers. Also, reporting of logs was to be taken into consideration to emphasize the importance of incident reporting which is usually defined by company policies. Also, it is considered the best practice that firewall reporting is reviewed at regular intervals.

All the contents of case study are further discussed in chapter 5.5.

2 FIREWALLS

Firewalls are designed to filter network traffic, enforce various security policies and protect the network against external attacks. Firewalls act as security gateways which inspect the ingress and egress traffic between LAN and WAN networks. By default, all firewalls filter and allow traffic to flow if it matches a specific rule exception. Otherwise all traffic will be denied by an implicit deny-all rule that is the final and absolute rule of a firewall. (Stewart 2014, 44-45.)

As Stewart mentions; “Listing the types of firewalls is almost like listing the taxonomy of the animal kingdom in biology. The variations, models, and versions are numerous. In addition, opinions vary about what is and is not a firewall.” (2014, 66.)

2.1 Traditional Firewalls

Traditional firewalls or legacy firewalls at their most basic level control traffic flow between a trusted network and an untrusted or public network. The most commonly deployed ones today are port-based or variations of such a firewall appliance. (Miller 2011, 6.) Miller also (2011, 6) phrases it; “These firewalls are popular because they are relatively simple to operate and maintain, generally inexpensive, have good throughput, and have been the prevalent design for more than two decades”. As the given devices are dependent on port-based filtering, understanding of TCP/UDP is mandatory.

Traditional firewalls operate typically using either stateless or stateful method for the flowing traffic. The statelessly monitored traffic simply checks over each packet individually and is not able to discern a traffic “flow”. Statefully monitored traffic is kept track of where the flow is within its lifetime. (Wilkins, 2014.) TCP streams are an example of such a stateful traffic and is explained in chapter 3.1.

The following sub-chapters list and explain the ideas behind some of the most common categorizations of traditional firewalls.

2.1.1 Personal Firewalls

Personal firewalls are designed and implemented to protect a single host from unauthorized access. Personal firewalls also integrate additional capabilities such as antivirus software monitoring, behavioral analysis and intrusion detection for added protection. (andy 2007.)

Also, as andy (2007) mentions; “Whereas personal firewalls make immense sense in the SOHO and home user market because they provide the end user protection as well as control of the policy, in the enterprise the issues are more complex. Perhaps the biggest concern for enterprise users with regard to personal firewalls is the ability to provide a centralized policy control mechanism for the firewall. The need to centralize policy control is critical to the use of personal firewalls in an enterprise environment to minimize the administrative burden.”

Personal firewalls, which are mostly application-level (software) firewalls, today are offered as commercial and open-source by a plethora of companies and providers, e.g., Symantec, Comodo, Check Point, Malwarebytes.
Although personal firewalls are quite capable of analyzing and preventing threats from outside network, enterprises need to centralize and enforce their own policies and because of this hardware network firewalls are usually mandatory in such environments.

2.1.2 Network Firewalls

Enterprises deploy network firewalls, in addition to personal firewalls to enforce and centralize their own policies and control the flow of traffic in-between outside and inside network.

Network firewalls are commonly classified in three different types;

Packet-filtering firewalls which are either static or stateful (dynamic).
In static filtering, the firewall uses a static or fixed set of rules to filter network traffic. The rules can focus on source or destination IP address, source or destination port number, IP header protocol field value, ICMP types, fragmentation flags, and IP options. Static filtering mainly focuses on Network Layer (Layer 3) of OSI, but can also include elements of Transport Layer (Layer 4). (Stewart 2014, 69.)

Stateful filtering (dynamic filtering) addresses the issue of more complex malicious traffic by determining whether or not a current packet is part of an existing session, and allow / deny decisions are made based on this determination. A state is a session of communication which refers to the Transport Layer (Layer 4) protocol TCP's (see chapter 3.1) virtual circuits established through the three-way handshake. However, stateful inspection systems can also track communications in Layers 5-7. The track of current sessions is kept in a state table stored in memory. (Stewart 2014, 69-70.)
Although being engineered to address the aforementioned issue, stateful filtering is still vulnerable by design, as the header contents can be manipulated to make malicious traffic look to be a part of an existing valid session. Even if the firewall can keep advanced details about the session, such as sequencing and acknowledge numbers (see chapter 3.1), a hacker can eavesdrop the traffic and learn the logic behind them to for prediction attacks. (Stewart 2014, 70.)

Circuit-level gateways (or Circuit proxies) which focus filtering on the initial setup process of a session, state, or circuit. This given form of filtering focuses on layers from 3 to 5 and functions similarly to application proxies, as it acts as a middleman (See Figure 1.) between the communication of a client and a server. This prevents direct connection existing between the client and server to protect the network. (Stewart 2014, 71.)

Circuit proxies make allow or deny decisions on the initiation of the session, state, or circuit and after a circuit is allowed, no further filtering takes place. All of the communication from there on is unfiltered and unmonitored, at least by the circuit proxy itself. (Stewart 2014, 71.)

The filtering rules of circuit proxies are quite similar to those of static packet filtering. The rules decide to allow and block on the basis of IP addresses, port numbers, domain names and networks. The firewall can function on the basis of either blocking all and allowing exceptions or allow all and deny exceptions. (Stewart 2014, 71.)

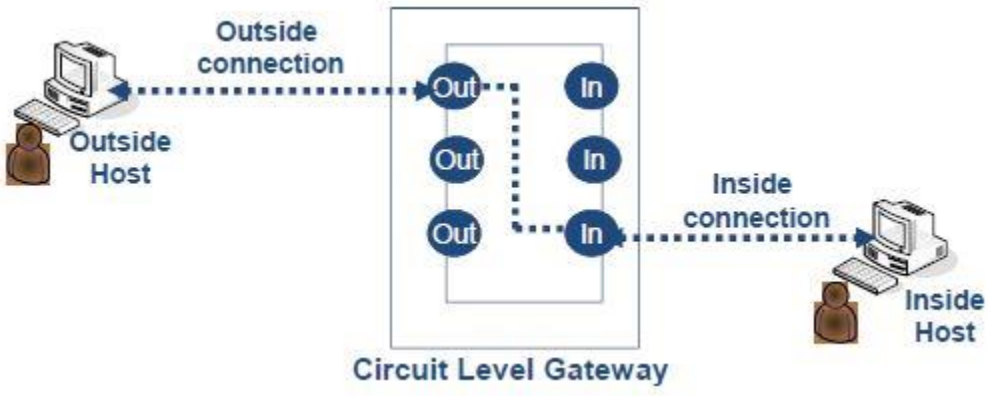

Figure 1. Circuit Level Gateway Firewall (Bankexamstoday 2015)

Application-level gateways act as an application-specific version of a packet filter. However, unlike a static packet filter that is only able to inspect the header of a packet or segment, an application proxy is able to inspect traffic fully at any layer, including the application payload. Although given the name firewall or gateway, application proxy acts as the middleman in-between traffic just like circuit-level proxies (See Figure 2.) and thus grants the firewall the ability to inspect application-specific elements of the traffic, e.g., e-mail, Web, file transfer, database access, VoIP and other TCP/IP sub-protocols are available. (Stewart 2014, 70-71.)

Usually when application proxy is deployed, all client software is reconfigured to point its communications to the proxy server rather than the actual resource server. The application proxy reassembles the request packets before sending them to the resource server. The application proxy maintains two connections, one between itself and the client and a second between itself and the resource server, thus being able to inspect every aspect of an application's communications through disassembling and reassembling content of the application payloads. This is known as deep packet inspection. (Stewart 2014, 71.)

As Stewart (2014) emphasizes;

> *"The primary limitation of application proxy firewalls is that each unique application will need its own dedicated application proxy. Generic proxy systems are usually ineffective."*

Although firewalls are commonly placed in such three main categories, many of them have characteristics that place them in more than one classification.

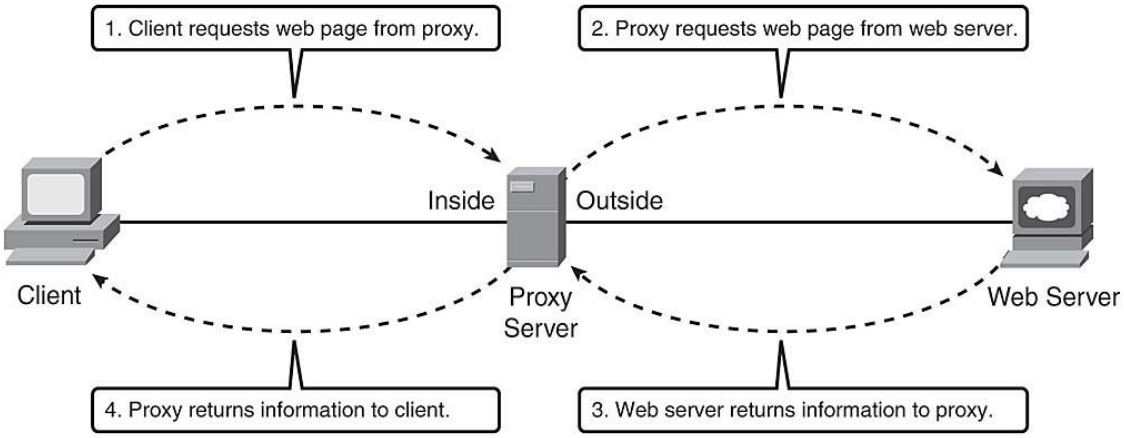

Figure 2. Proxy firewall session establishment (Blair, R. & Durai, A. 2009)

2.2 Next-Generation Firewalls

As Miller (2011, 12-13) states;

> *"In the rapid pace of the Internet Age, nearly two decades means the basic technology behind port-based firewalls is medieval. In fact, network security is often likened to the Dark Ages — a network perimeter is analogous to the walls of a castle, with a firewall controlling access — like a drawbridge. And like a drawbridge that is either up or down, a port-based firewall is limited to just two options for controlling network traffic: allow or block. —*
>
> *— IT organizations have tried to compensate for deficiencies in traditional port-based firewalls by surrounding them with proxies, intrusion prevention systems, URL filtering, and other costly and complex devices, all of which are equally ineffective in today's application and threat landscape."*

As mentioned afore, traditional types of firewalls themselves don't offer as liable security as they once did. Internet and network related threats have evolved tremendously and a new generation of security devices are necessary to prevent e.g., data leakages and DDoS attacks.

Next-Generation Firewall devices process data streams based on applications and thus allowing distinguishing and granularly controlling otherwise evasive network traffic, although requiring multi-factor approach to determine applications identity regardless of port, protocol or encryption (Miller, 2011).

The given thesis will mainly cover Palo Alto Networks' Next-Generation Firewalls and technologies they offer and are further discussed in following chapters.

3 NETWORK PROTOCOLS AND VULNERABILITIES

A network protocol defines rules and conventions for communication between network devices. Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received. (Mitchell 2017.)

Several standardization communities and organizations have been established since the global research of packet radio and packet switched networks in the early 1960's. Most notable of these organizations is ARPANET. (Leiner et al. s.a.; Defense Advanced Research Projects Agency s.a.)

All network protocols lean heavily on The Open Systems Interconnection (OSI) conceptual model which was produced by International Organization for Standardization (ISO) in 1984 (Kucharik 2002).

The most relevant networking and Internet protocols regarding firewall operation and the given bachelor's thesis are explained and discussed in the following sub-chapters. Some of the most common and relevant vulnerabilities are covered as well.

3.1 TCP

The Transmission Control Protocol (TCP) is intended for use as a highly reliable host-to-host protocol between hosts in packet-switched computer communication networks, and in interconnected systems of such networks. (Postel 1981a, 1.) The header of a TCP packet can be seen in Figure 3.

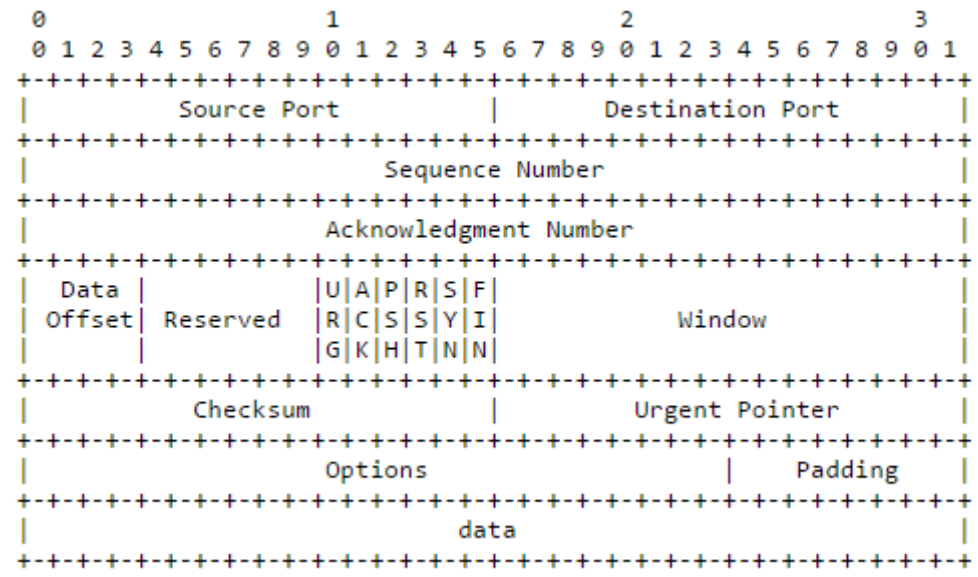

Figure 3. TCP Header (Postel, J. 1981a)

TCP traffic flow may be divided into three phases: 3-way handshake (connection establishment), transmission of data (data transfer) and closing of the established virtual circuit (connection termination). In the following figure 4. is presented the said TCP traffic and all three phases of a TCP session.

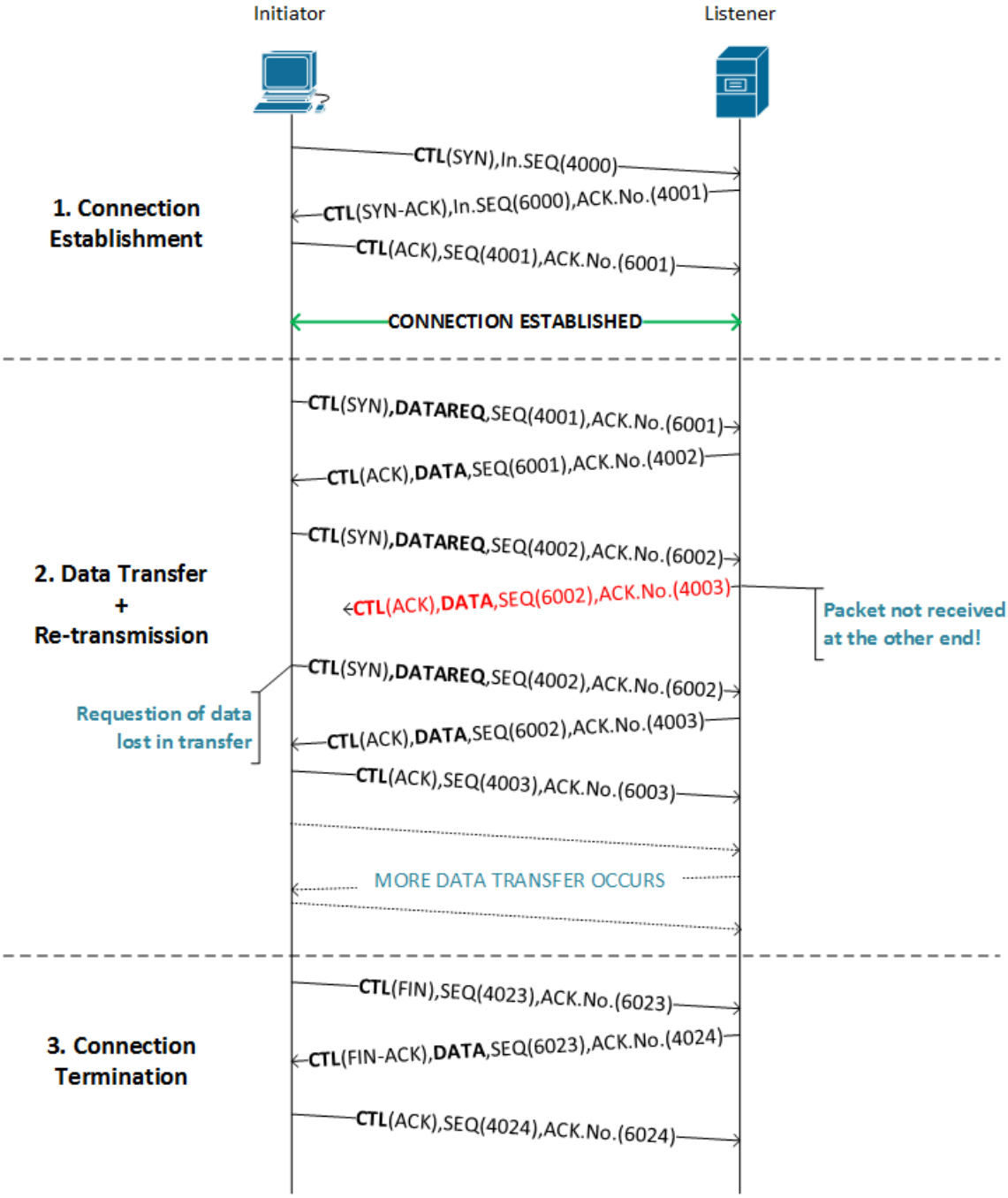

Figure 4. TCP 3-way handshake

3.1.1 Port Scanning

Port scanning occurs when a remote host sends IP packets containing ‘TCP SYN’ segments to different destination ports of a server or another host device. After the host receives the ‘SYN/ACK’ packet it resets the connection as it doesn’t need to establish a full connection. The purpose of such an attack is to scan the available services and identify vulnerable targets. (Juniper Networks 2016.) Port scanning itself is just the reconnaissance part of an attack and the basic operating model can be seen in figure 5.

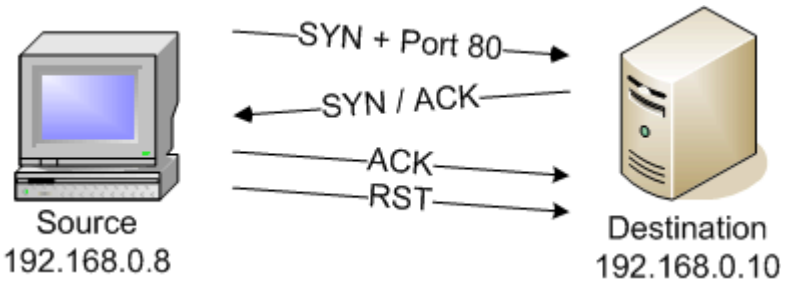

Figure 5. Port Scanning in action for port 80. (Messer, J. 2007)

3.1.2 TCP Split Handshake

TCP Split Handshake is a technique used by attackers that exploits TCP’s three-way handshake’s (See chapter 3.1) slightly different but legitimate variant of four-way handshake. The given variant can be seen in figure 6.

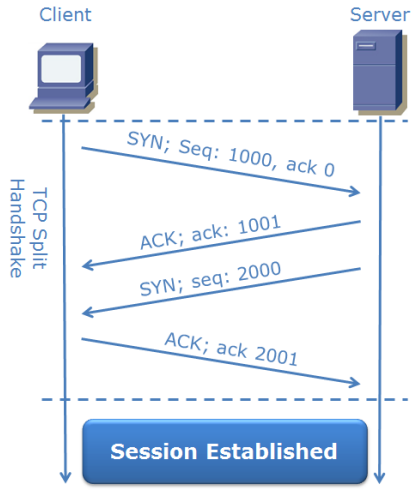

Figure 6. Four-Way Handshake (Passeri 2011)

3.1.3 TCP SYN Flood attack

TCP SYN Flooding abuses the basic design of TCP connection establishment through TCP Packet data structure (see chapter 3.1) that is known as Transmission Control Block (TCB). TCB contains information about local and remote socket numbers, sent and received buffers, security and priority values, and the current segment in the queue. It also manages sent and received sequence numbers. (Omnisecu s.a..) This kind of attack is a clear potential DoS attack and the goal is to deplete the backlog of target system (Wesley s.a.).

As seen in figure 7, the attacker sends a flood of SYN packets to target destination with a bogus IP address, so that when the server receives the requests it will open the given port and send a SYN-ACK flagged packets to bogus destinations which never sends ACK packet back. The connections are left open and the host stores TCB's of the connection information to its memory and potentially overflows it, thus leaving no available kernel memory for potential legitimate customers.

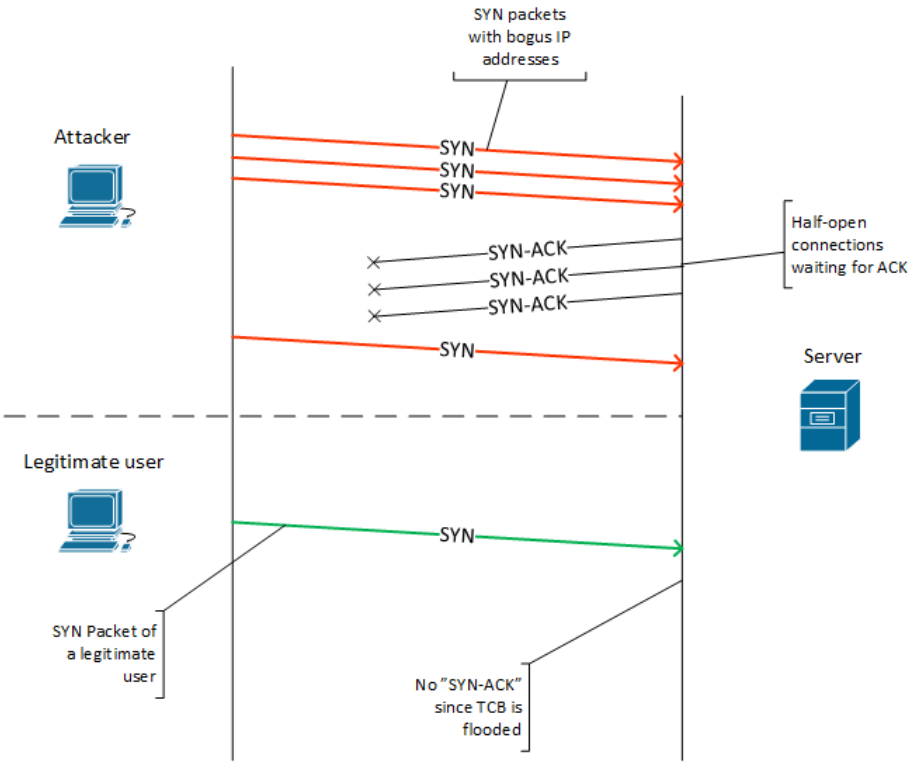

Figure 7. SYN Flood spoofing attack and how it affects legitimate users

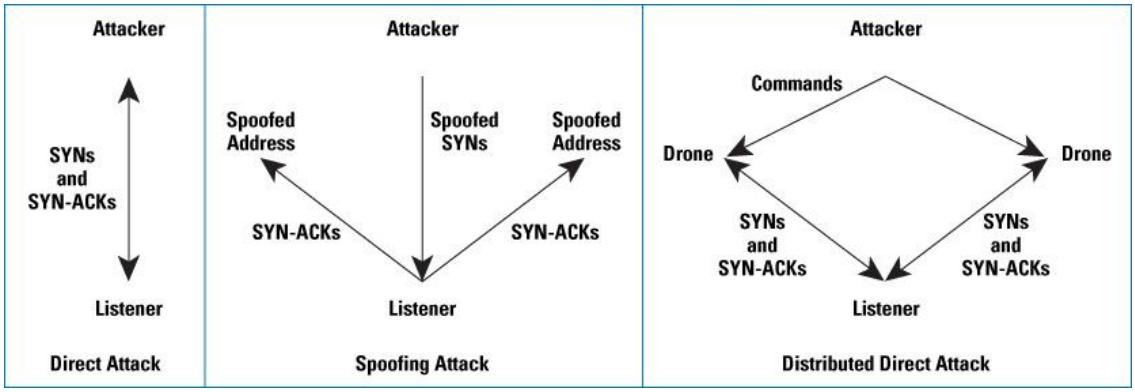

Figure 8. Some variants of SYN Flood attack (Wesley, M., E. & Verizon Federal Network Systems s.a.)

The sort of attack depicted afore is known as a spoofing attack which is much more complex as opposed to a direct one. The main differences can be seen in figure 8. In a direct attack the attacker doesn't spoof IP addresses.
Direct attacks are much easier to defend against as the source is singular.
The most advanced and complex type of attack is considered to be distributed by utilizing "botnets" or "drone armies". The attacker sends commands directly to the attacking bots which allows the attacker to remain untraceable when compared to a direct attack. The effectiveness of the attack can be increased by making each bot utilize IP address spoofing. (Wesley s.a..)

3.2 UDP

The User Datagram Protocol (UDP) is defined to make available a datagram mode of packet-switched computer communication in the environment of an interconnected set of computer networks. UDP provides a procedure for application programs to send messages to other programs with a minimum of protocol mechanism. The protocol is transaction oriented, and delivery and duplicate protection are not guaranteed, unlike in TCP-oriented connections. (Postel 1981a, 1.) UDP is used in situations where it doesn't matter if data is lost in transit; e.g., media streaming, TFTP, internet gaming or VoIP. The header of a UDP packet is shown in figure 9.

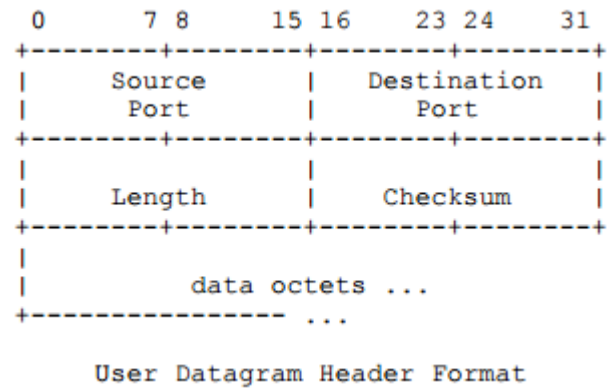

Figure 9. UDP Header (Postel, J. 1980)

3.3 IPv4 & IPv6

IPv4, formerly called just “Internet Protocol”, was designed to be used in interconnected systems of packet-switched computer communication networks. Such networks were called “catenets” which is the today’s equivalent of “LAN”. The purpose of IPv4 is to provide transmission of blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses. The protocol also provides for fragmentation and reassembly of long datagrams. (Postel 1981b.)

The IPv4 packet header is 32 bits long and so are addresses used as well. The IPv4 header and its contents can be observed in figure 10.

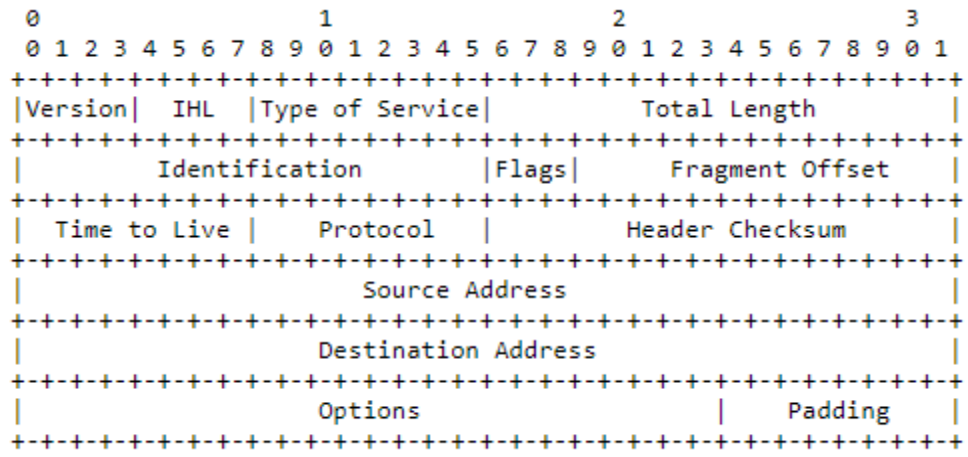

Figure 10. Internet Datagram Header (Postel, J. 1981b)

IPv6 is a newer version of IPv4 and is designed to be a successor for it. The most notable improvement of IPv6 is the expanded addressing capabilities of it; the IP address size is increased from 32 bits to 128 bits and thus supports more levels of addressing hierarchy, a much greater number of addressable nodes, and simpler auto-configuration of addresses. Also some of the IPv4 header fields have been dropped or made optional, to reduce common-case processing cost of packet handling and to limit the bandwidth cost. (Deering & Hinden 1998.)

The contents of IPv6 packet header can be observed in figure 11.

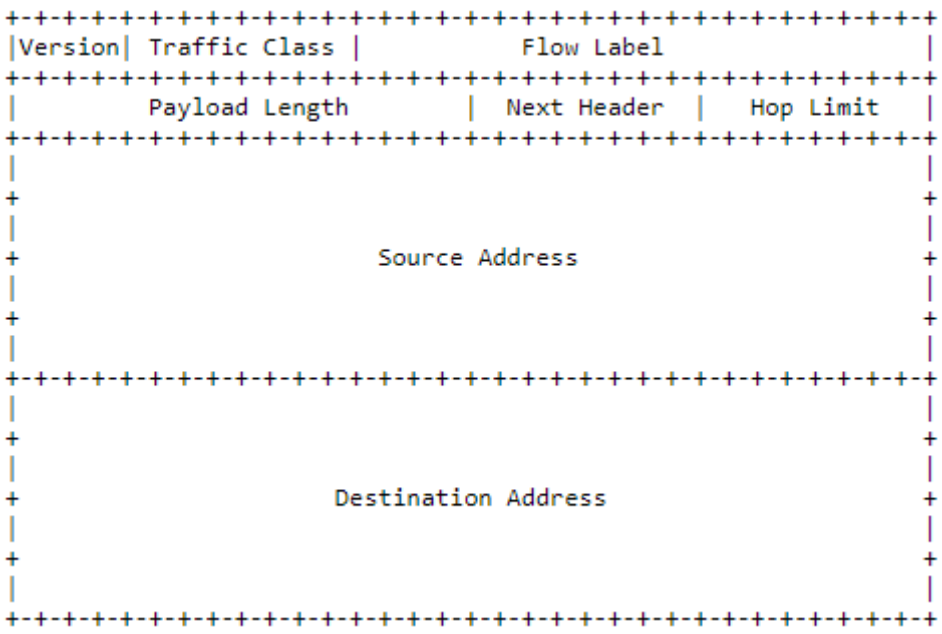

Figure 11. IPv6 Packet Header (Deering, S. & Hinden, R. 1998)

IP Spoofing is based on the design of TCP session sequence numbering (see Chapter 3.1) and IP header (See chapter 3.3) modification itself. Several attacks exploit TCP/IP's design since they need to build sessions, albeit falsely. (Tanase 2003.) The following attacks employ the said protocols as stated by Tanase (2003);

Non-Blind Spoofing takes place when the attacker is on the same subnet as the victim itself. The sequence and acknowledgement numbers can be sniffed, eliminating the potential difficulty of calculating them accurately. The biggest threat of spoofing in this instance would be session hijacking. This is accomplished by corrupting the data stream of an established connection, then re-establishing it based on correct sequence and acknowledgement numbers with the attack machine. (Tanase 2003.)

Blind Spoofing is a more sophisticated attack, because the sequence and acknowledgement numbers are unreachable. In order to circumvent this, several packets are sent to the target machine in order to sample sequence numbers. It was relatively easy to discover the exact formula of sequencing by studying packets and TCP sessions. Today most OS' are implemented with random sequence number generation to make accurate prediction difficult. (Tanase 2003.)

Denial of Service Attack uses IP spoofing to prolong the length of attack. The attack itself is quite difficult to defend against since attackers are most of time only concerned with consuming bandwidth and resources of target. Thus spoofing source IP addresses makes tracing and stopping the DoS as difficult as possible. (Tanase 2003.)

3.4 IPSec

IPsec is a protocol that creates a boundary between unprotected and protected interfaces, for a host or a network. Traffic traversing the boundary is subject to the access controls specified by the user or administrator responsible for the IPSec configuration. (Kent & Seo 2005.)

As Frankel and Krishnan (2011) point out, IPsec suite protocol is composed of the following protocols that perform various security service functions;

Authentication Header (AH) provides integrity protection and data-origin authentication, access control, and, optionally replay protection. A transport mode AH SA, used to protect peer-to-peer communications, protects upper-layer data, as well as those portions of the IP header that do not vary predictably during packet delivery. Tunnel mode AH SA can be used to protect the inner (original) header and the upper-layer data, as well as those portions of the outer (tunnel) header that do not vary unpredictably during packet delivery. AH also does not work in the presence of NAT.

Encapsulating Security Payload (ESP) provides confidentiality (encryption) and/or integrity protection; it also provides data-origin authentication, access control, and, optionally, replay and/or traffic analysis protection. A transport mode ESP SA protects the upper-layer data and the inner header, but not the outer header.

3.5 IKE

IKE is an IPsec standard protocol used to ensure security for VPN negotiation and remote host or network access. IKE defines an automatic means of negotiation and authentication for IPsec SAs which are security policies defined for communication between two or more entities. The given relationship is presented by a key. IKE ensures security for SA communication without the preconfiguration that would otherwise be required. (Rouse 2009.)

IKE itself is not a prequisite of IPsec but it offers number of benefits, including: automatic negotiation and authentication; anti-replay services; certificate authority support; and the ability to change encryption keys during an IPsec session. (Rouse 2009.)

3.6 TLS

The primary goal of TLS protocol is to provide privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. At the lowest level, layered on top of some reliable transport protocol (e.g., TCP), is the TLS Record Protocol. The TLS Record Protocol provides connection security that has two basic properties: connection privacy and connection reliability. Privacy is achieved by using symmetric cryptography for data encryption. The keys for said encryption are generated uniquely for each connection and are based on a secret negotiated by another protocol. Reliability is achieved by including a message integrity check using keyed MAC. Secure hash functions are used for MAC computations. (Dierks & Rescorla 2008.)

As stated by Dierks and Rescorla (2008), the TLS Handshake Protocol provides connection security that has three basic properties:

- **Peer identity authentication** using asymmetric, or public key, cryptography.

- **The negotiation of a shared secret is secure**: the negotiated secret is unavailable to eavesdroppers, and for any authenticated connection the secret cannot be obtained, even by an attacker who can place himself in the middle of the connection.

- **The negotiation is reliable**: no attacker can modify the negotiation communication without being detected by the parties to the communication.

4 PALO ALTO NETWORKS

Palo Alto Networks was founded in 2005 by a former Israeli engineer Nir Zuk. Zuk worked at Check Point Software Technologies in the 1990's and was writing parts of the world's first commercial firewall at the time. Later on, he moved onto building essential chunks of a firewall which was sold by Juniper Networks. (Melby 2013.) As Melby (2013) wrote the statement of Zuk in an interview;

> *"But at both companies, Zuk ended up quitting in a huff--and, in one case, walking away from millions of dollars in unvested stock options. Why? The Israeli engineer felt his best ideas were being blocked by incompetence and office politics. All he ever wanted, he insists, was to build new things."*

With a revenge-like intention Zuk founded a company which sells the first new class of firewall. Ever since Palo Alto Networks has been rapidly gaining an ever-larger share of the network security market. (Melby 2013;Palo Alto Networks 2017g.)

Palo Alto Networks has also acquisitioned some of the rival companies and integrated the technologies they possessed to PA-appliances, such as LightCyber in 2017 (Palo Alto Networks 2017f) and Cyvera (Rao 2014).

The following sub-chapters cover the technologies and advanced features that Palo Alto firewall application solutions offer.

4.1 WildFire

WildFire is engineered to fight against unknown malware and zero-day exploits. WildFire uses dynamic analysis to identify unknown files, that could be identified as zero-day malware, by utilizing virtualized sandboxing environment (Palo Alto Networks 2017n; Palo Alto Networks 2017m). WildFire utilizes a multi-technique approach in its operation that combines dynamic and static analysis, machine learning as well as bare metal analysis environment to detect and prevent even the most evasive and unknown threats (Palo Alto Networks 2017n).

As Palo Alto Networks (2017o) states, the WildFire environment can be either public, private or hybrid-based, depending on which deployment method is preferred by the customer;

- Public cloud utilized traffic forwarding to a publicly hosted WildFire environment to analyze the data. Public cloud environment will generate a new signature to distribute across the globe to all “Threat Prevention” subscribers. The regions are as follows;
    - United States
    - EU; Netherlands
    - Japan
    - Singapore
- Private cloud utilizes a WF-500 appliance on the private network of an enterprise to host private cloud analysis. A single WF-500 appliance can receive and analyze data from up to 100 PA firewalls.
- Hybrid cloud may forward certain traffic to WildFire public cloud and some to a private cloud appliance, thus allowing flexibility of analyzing sensitive content.

Figure 12. is a simplified presentation of WildFire decision flow, where as in figure 13. is a much more detailed presentation of the same flow of decisions.

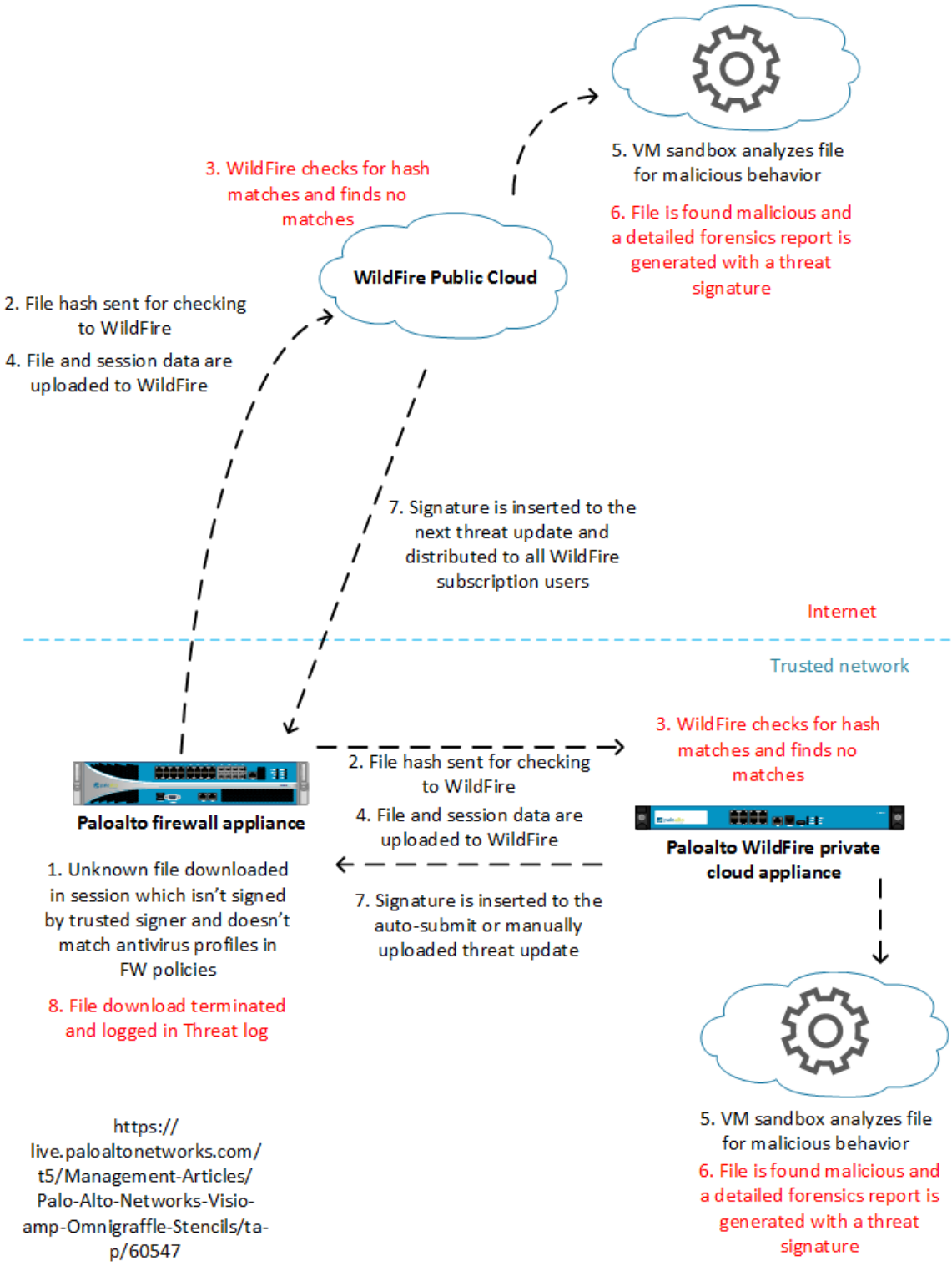

Figure 12. A simplified WildFire decision workflow based on WildFire technical documentation.

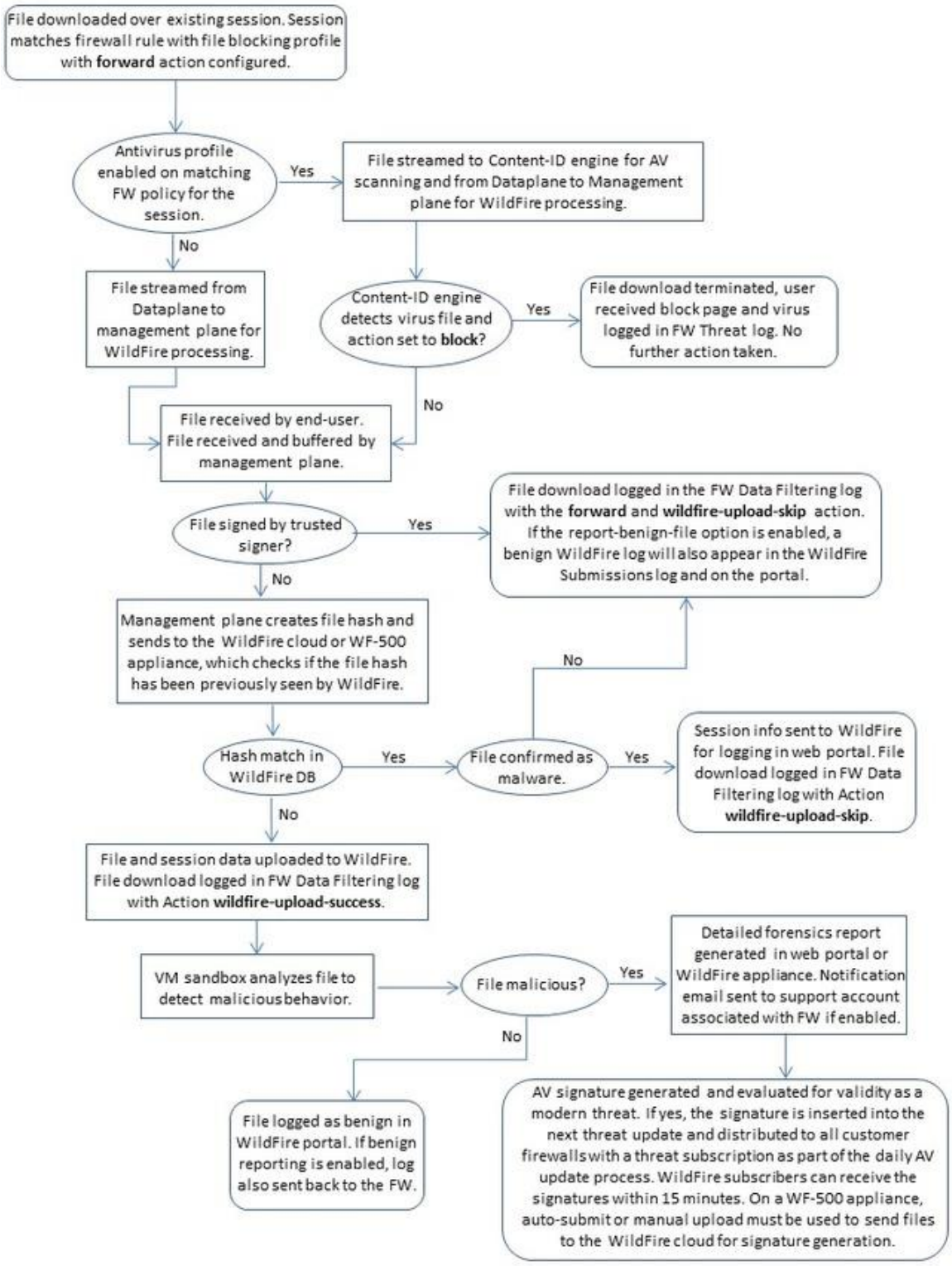

Figure 13. A detailed WildFire Decision Flow (Palo Alto Networks 2017a)

4.2 App-ID

App-ID is engineered to enable the security team of an enterprise to see the applications traversing through network by granularly decoding encrypted data streams. This method gives room for compromise- other than the choice of “either blocking everything or enabling everything”- in comparison to stateless inspection which relies on using source and destination IPs. Stateful inspection also strictly adheres to port-based classifying of TCP/UDP traffic (Palo Alto Networks 2015a).

App-ID also uses stateful inspection as a part of its security policies, but will decrypt the traffic after determining TLS/SSH is in use. After determining such the traffic stream is granularly decrypted and the protocol decoded, be it either unknown or know traffic that needs decoding. In the case of unknown evasive applications heuristics can be applied to further analyze the behavior of the application. Heuristics can check packet length, session rate and packet sources for example to determine malicious application traffic. If the traffic is already identified, no decoding takes place and the policy is enforced and reported in logs.

Figure 14. shows the App-ID traffic classification workflow.

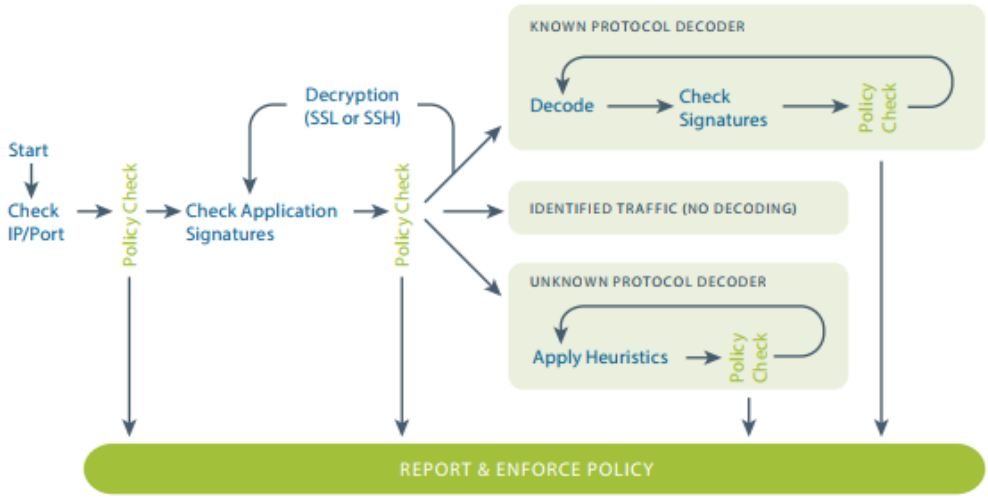

Figure 14. App-ID operating model chart (Palo Alto Networks 2015)

4.3 User-ID

User-ID is used in conjunction with App-ID and Content-ID to give the ability to enable visibility, security policies, reporting, and forensics based on users and groups, instead of IP addresses. User-ID utilizes Microsoft Active Directory and LDAP services to identify traffic of a user and user groups to enforce policies. User-ID also improves visibility of application usage based on groups and users. In case of a security incident, forensics analysis and reporting based on user information provides a lot more complete picture of the given incident. (Palo Alto Networks 2016a.)

Figure 15. is a simplified depiction of how User-ID works.

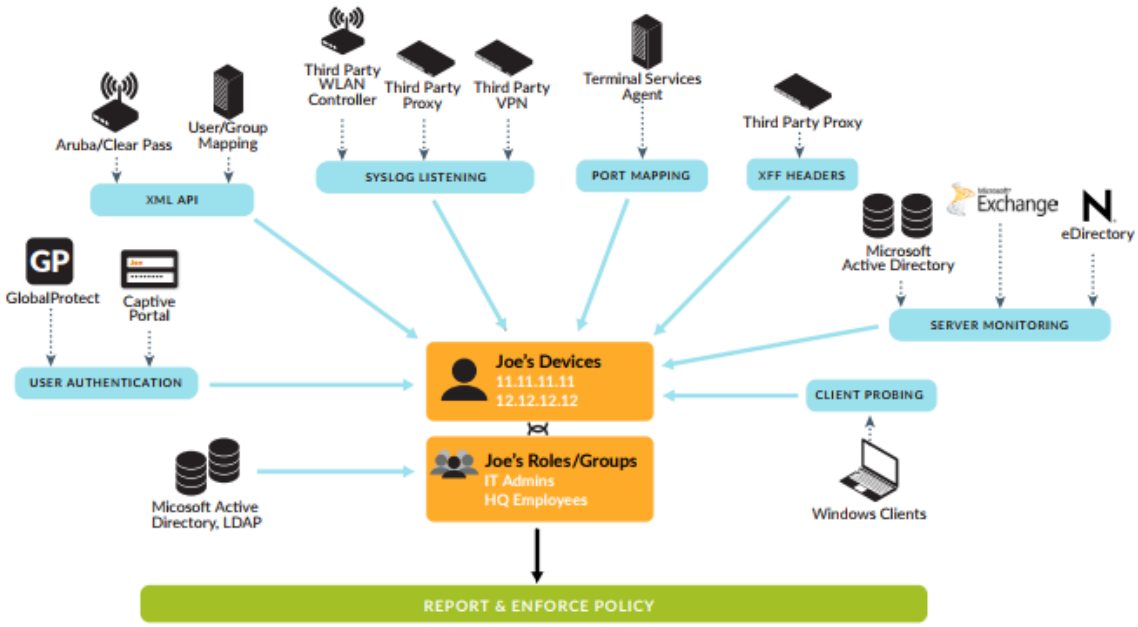

Figure 15. User-ID operating model chart (Palo Alto Networks 2016a)

4.4 GlobalProtect

GlobalProtect is a VPN service that can utilize and enforce all of the aforementioned security technologies whilst operating. It is engineered to give end-users the ability to connect to enterprise network, as it applies security policies to all users regardless of location and device in use. (Palo Alto Networks 2017d.) The one major utility provided by GlobalProtect is the ability to inspect and enforce Host Information Profiles. The given technology offers security team the ability to inspect;

- Operating system and application patch level
- Host anti-malware version and state
- Host firewall version and state
- Disk encryption configuration
- Data backup product configuration
- Customized host conditions (e.g., registry entries and running software)

Besides the given abilities, GlobalProtect also supports clientless SSL VPN for secure access to applications in the data center and the cloud from unmanaged devices. This approach offers convenience and security by providing access to specific applications through a web interface without requiring the user to install a client beforehand or set up a full tunnel (Palo Alto Networks 2017d).

4.5 VM-Series Deployments

Palo Alto Networks offers a wide range of cloud and virtualization environment deployments to secure private, public and hybrid clouds. The virtual environments supported include: VMware® NSX™, ESXi™, vCloud® Air™, Citrix® Netscaler® SDX™, Microsoft® Azure® and Hyper-V®, Amazon® Web Services and KVM with optional support for the OpenStack® plugin. (Palo Alto Networks 2017i; Palo Alto Networks 2017j; Palo Alto Networks 2017k; Palo Alto Networks 2017l.)

The VM-Series deployments function the same way as physical appliances, but are more flexible deployment-wise and can function in the cloud in parallel to other VMs. An example of a VM-series deployment on ESXi can be observed in figure 16.

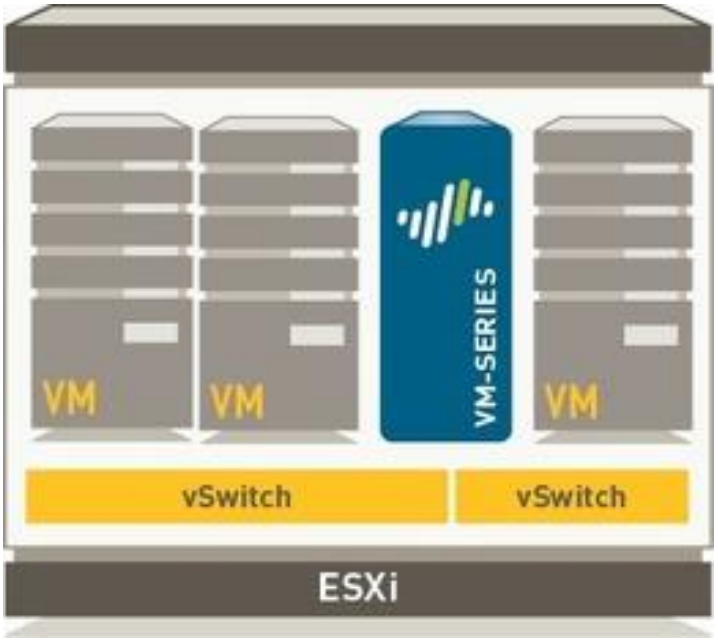

Figure 16. VM-Series deployment on ESXi (Palo Alto Networks 2017k)

4.6 URL Filtering

Palo Alto Networks URL Filtering technology is a service which enables and enforces secure web access through categorization of URLs. Such filtering allows security team to manage web traffic policies to be in line with organizational policies. (Palo Alto Networks 2017h; Palo Alto Network 2017e.)

Palo Alto Networks also offers a real-time URL database which receives updates from WildFire every five minutes to counter and protect against malicious sites, in addition to other advanced identification techniques (Palo Alto Network 2017h; Palo Alto Network 2017e).

4.7 Content-ID

Content-ID by Palo Alto Networks is a single-pass architecture that combines multiple threat-prevention techniques into a single stream-based engine, as seen in Figure 17. The aforementioned techniques are this way handled as one bigger entity that inspects the flowing traffic and give security teams the ability to control application traffic and content. (Palo Alto Networks 2016b.)

Content-ID (Palo Alto Networks 2017c; Palo Alto Networks 2017b) uses App-ID all the time to granularly decode and look for threats within application data streams and thus prevents threats tunneled via already otherwise approved applications, thus acting as a threat prevention mechanism. To reinforce IPS functionality, Content-ID uses the following mechanisms as stated in a tech brief;

- Protocol decoders and anomaly detection
- Stateful pattern matching
- Statistical anomaly detection
- Heuristic-based analysis
- Invalid or malformed packet detection
- IP defragmentation and TCP reassembly
- Custom vulnerability and spyware phone-home signatures

To fight back against unknown malware and zero-day exploits, Content-ID also utilizes WildFire which utilizes cloud-based virtualized sandbox architecture without additional acquisition of hardware (see chapter 4.1).

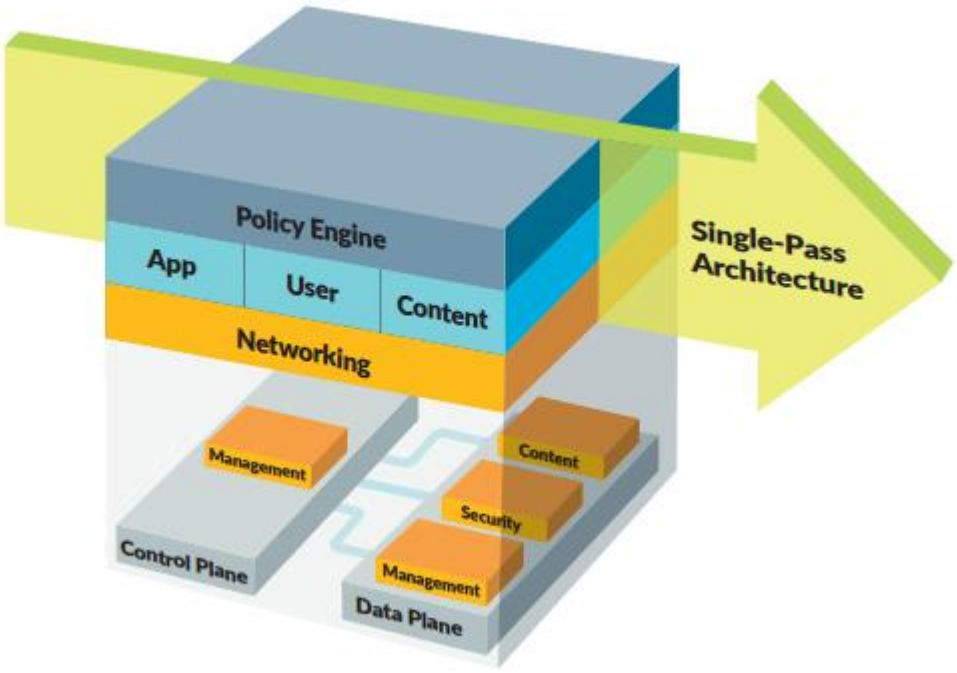

Figure 17. Palo Alto Networks single-pass parallel processing architecture (Palo Alto Networks 2016b)

Content-ID also allows traffic to be analyzed faster by utilizing parallel processing and thus minimizing latency and maximizing throughput. This is a lot faster in comparison to more traditional file-based scanning techniques utilized in most of the firewalls today, as seen in Figure 18.

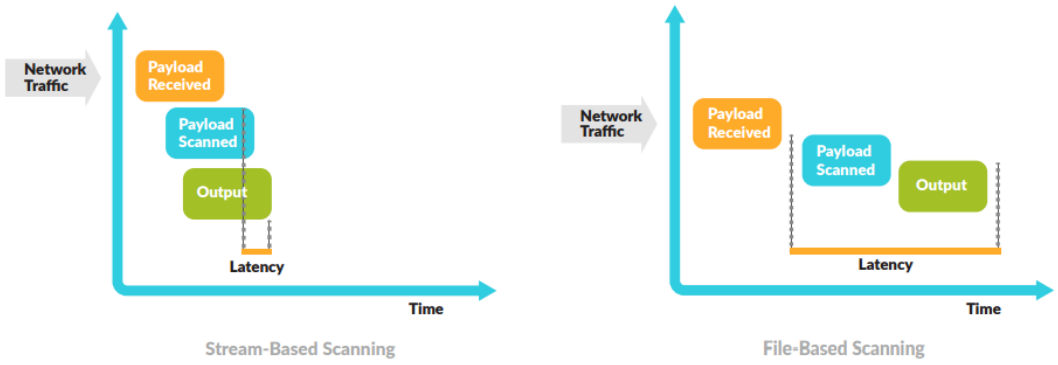

Figure 18. Stream-based scanning's effect on throughput performance (Palo Alto Networks 2016b

5 CASE STUDY

There was a need for case study material. The material was to cover the following; Basic implementation and configuration of network devices, Palo Alto firewall appliance and Cisco ASAv appliance. Also, there was a need to cover more advanced aspects of Palo Alto firewall and focus less on Cisco ASA itself. The case study material was to be heavily based on practice material provided by Palo Alto Networks, but needed revising to serve its purpose in the given scenarios.

The decision to use a virtual environment instead of physical one was because of the possibility to use SIMTERNET (Kankare 2015) as an ISP network. The topology of SIMTERNET itself can be seen in the following figure 19. Also, the possibility to use Virtual Laboratory (Nurmi 2016) provided many benefits as described in chapter 5.1.

Virtual Laboratory is run in "CyberLab" data center by South-Eastern University of Applied Sciences XAMK Ltd. and it encompasses of 12 servers which consist of over 300 cores and 3 TB's of RAM. The Virtual Laboratory itself is a web based application that only requires user to have HTML5-based browser. The application does not require Java or any additional add-ons. (Kettunen 2017.) The Virtual Laboratory can be seen in action in figure 23.

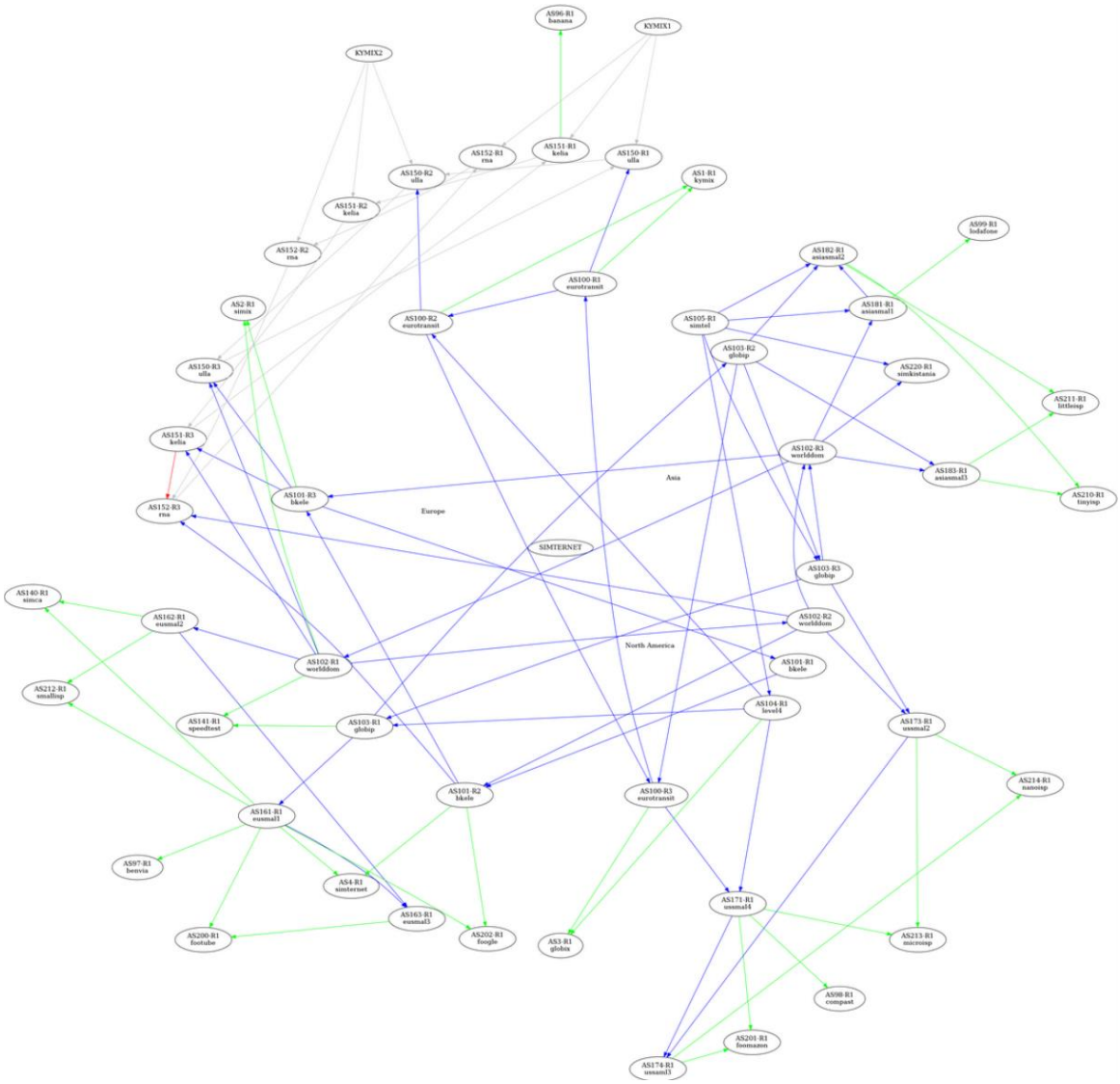

Figure 19. SIMTERNET and its topology (Kankare 2015)

5.1 Benefits of Virtual Laboratory

Working in the Virtual Laboratory (Nurmi 2016) provides many pedagogical and practical benefits for teaching, as Kettunen (2017) mentions; All the case study material that has been done with physical devices before converts to the virtualized environment as well and allows students to have more devices in each case study than previously possible. Also, the laboratories of each student can be easily interconnected to create collaborative study units. If there is a need, the teacher can easily manage, supervise and help with each laboratory session that is running on the servers. As the Virtual Laboratory can be accessed through secure VPN connection, regardless of location, device and time, the flexibility of studying outside of school hours is made possible. (Kettunen 2017.)

There is also a way to simulate packet loss, bit errors and latency increases of individual links between virtual devices. If there is a need the student can also monitor and inspect the traffic of links by using a Wireshark sniffer. This is necessary if there is the need for troubleshooting connectivity problems. (Kettunen 2017.)

5.2 Network Topology

The network topology used in two different case studies can be seen in figure 20. The reason to have both case studies use the same topology is that the devices can be supplied to be pre-configured as necessary considering what is relevant to each of them. The case study consisted of twelve devices; three routers, seven Windows XP end devices of which two provided DMZ HTTP services and a Cisco ASAv and Palo Alto VM-100 firewall appliances.

The link between R2 (Router 2) and SIMTERNET can be an address between 239.0.0.96 – .99 Each address corresponds a different ISP operating inside SIMTERNET. Each ISP in SIMTERNET is interconnected with each other.

The idea was to have two different imaginary enterprise locations. One that has deployed a Cisco ASA firewall and another one that has deployed Palo Alto

firewall appliance. Both of them are interconnected and can access services in SIMTERNET. Also each enterprise hosts their own DMZ web services and has a private IPSec VPN tunnel between each other for Site-to-Site connectivity.

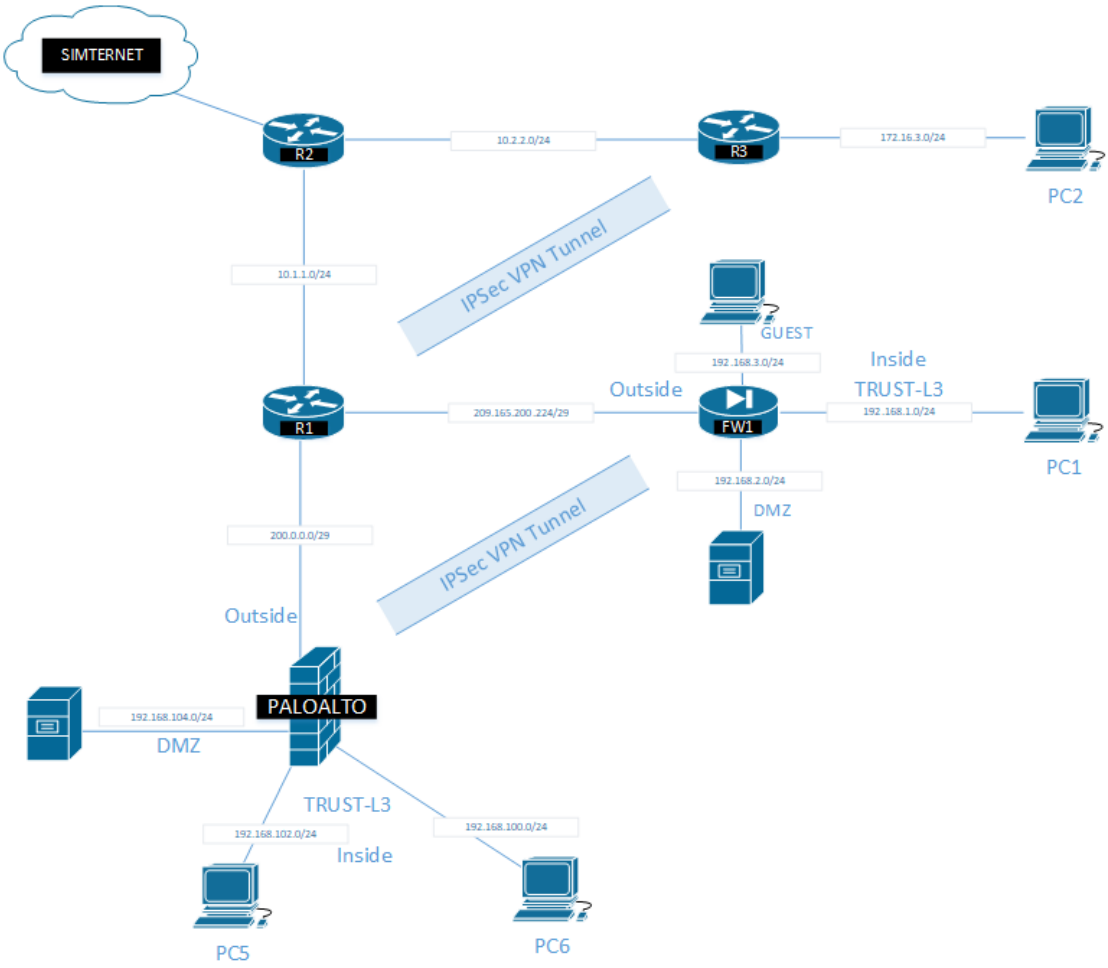

Figure 20. Palo Alto Firewall case study topology

5.3 Virtual Laboratory

The Virtual Laboratory uses ".top" format that is a text file based topology file. The topology of figure 20. (Topology) can be observed as a text file in figure 21.

The corresponding parameters are used as follows:

Text line to be shown in user view:

TEXT [x-coord.] [y-coord.] [Font size] [#Text color as hexadecimal] [#Background color as hexadecimal] [Text to be shown]

Workstations:

WORKS [Name] [x-coord.] [y-coord.] [Text to show on device]

Routers:

ROUTER [Name] [x-coord.] [y-coord.]

Palo Alto Firewall:

PALO_FIREWALL [Name] [x-coord.] [y-coord.] [Text to show on device]

Generic Firewalls:

FIREWALL [Name] [x-coord..] [y-coord..] [Text to show on device]

Link to SIMTERNET:

MCASTVPN [Name] [x-coord..] [y-coord..] [ISP Address 239.0.0.96 - .99] [Text to show on VPN]

Cables to interconnect devices:

CABLE [Device A] [Port] [Device B] [Port] [Text to show on cable]

(The "\n" signifies line break)

```
TEXT 58 67 20px #ffffff #000000 Data Security Equipment Lab 2

WORKS PC1 1025 490 PC-B_(PC1)
WORKS PC2 1025 230 PC-C_(PC2)
WORKS PC3 713 673 PC-A_(PC3)
WORKS PC4 714 327 PC-D_(PC4)
WORKS PC6 532 848 Paloalto_MGMT_(PC6)
WORKS PC5 80 848 Paloalto_INSIDE_(PC5)
WORKS PC7 80 500 Paloalto_DMZ_(PC7)

ROUTER R1 303 484
ROUTER R2 305 222
ROUTER R3 642 226

PALO_FIREWALL CPALO 302 648 PALOALTO
FIREWALL FW1 710 480 ASA_(FW1)

MCASTVPN SIMTERNET 103 134 239.0.0.98 SIMTERNET

CABLE PC2 0 R3 1 172.16.3.0/24
CABLE R3 0 R2 0 10.2.2.0/24
CABLE R2 1 R1 1 10.1.1.0/24
CABLE R1 0 FW1 1 OUTSIDE_ASA\n209.165.200.224/29
CABLE FW1 2 PC1 0 INSIDE_ASA\n192.168.1.0/24
CABLE FW1 3 PC3 0 DMZ_ASA\n192.168.2.0/24
CABLE PC4 0 FW1 4 GUEST_ASA\n192.168.3.0/24
CABLE CPALO 0 PC6 0 MGMT_PALO\n192.168.100.0/24
CABLE CPALO 4 R1 2 OUTSIDE_PALO\n200.0.0.0/24
CABLE PC5 0 CPALO 1 INSIDE_PALO\n192.168.102.0/24
CABLE PC7 0 CPALO 2 DMZ_PALO\n192.168.104.0/24
CABLE SIMTERNET -1 R2 2
```

Figure 21. The topology file of the case study as a “.top” file

Also an installation (".inst") file was made to be used in conjunction with ".top" file to create the laboratories from premade parameters. The installation file and its contents can be observed from figure 22.

The parameters are used as follows:

Topic to be listed in Virtual Laboratory available installations:

TOPIC [Name]

Topology file to be used for laboratory:

TOPOLOGY [Path/To/File.top]

Device and its hardware specifications:

DEVICE [Name] [Path/To/Image.filetype] [RAM] [CPU Cores] [Network Interfaces] [Network Interface Model] [MAC base] [Display Type] [Console Port] [Display Driver] [Snapshot mode on/off]

(MAC base can be "-" to generate one automatically)

Additional configuration lines:

#DISABLE topo_upload (Disables the ability to upload own topology)

#DISABLE topo_select (Disables the ability to select another topology)

```
1  TOPIC Data Security Equipment Lab 2
2  TOPOLOGY Path/To/The/File/lab2.top
3
4  DEVICE Monitor COMMON/monitorv2r3.vmdk 1024 1 1 e1000 - vnc 5907 vmware-svga 1
5  DEVICE R1 COMMON/iosv-156v1.img 512 1 4 e1000 - telnet 9121 cirrus-vga 0
6  DEVICE R2 COMMON/iosv-156v1.img 512 1 4 e1000 - telnet 9122 cirrus-vga 0
7  DEVICE R3 COMMON/iosv-156v1.img 512 1 4 e1000 - telnet 9123 cirrus-vga 0
8  DEVICE FW1 COMMON/asavV2.qcow2 2048 1 5 e1000 - telnet 9124 cirrus-vga 0
9  DEVICE PC1 COMMON/labXPv2.img 2048 1 1 rtl8139 - vnc 9124 vmware-svga 0
10 DEVICE PC2 COMMON/Windows7_Enterprise.qcow2 2048 2 1 e1000 - vnc 9124 vmware-svga 0
11 DEVICE PC3 COMMON/labXPv2.img 1024 1 1 rtl8139 - vnc 9124 vmware-svga 0
12 DEVICE PC4 COMMON/labXPv2.img 1024 1 1 rtl8139 - vnc 9124 vmware-svga 0
13 DEVICE PC5 COMMON/labXPv2.img 1024 1 1 rtl8139 - vnc 9124 vmware-svga 0
14 DEVICE PC6 COMMON/labXPv2.img 2048 1 1 rtl8139 - vnc 9124 vmware-svga 0
15 DEVICE PC7 COMMON/labXPv2.img 1024 1 1 rtl8139 - vnc 9124 vmware-svga 0
16 DEVICE CPALO COMMON/paloalto710_licensed.qcow2 6072 2 8 e1000 00:DF:FE:B2:11 telnet 9112 cirrus-vga 0
17
18 #DISABLE topo_upload
19 #DISABLE topo_select
```

Figure 22. The installation file of the case study

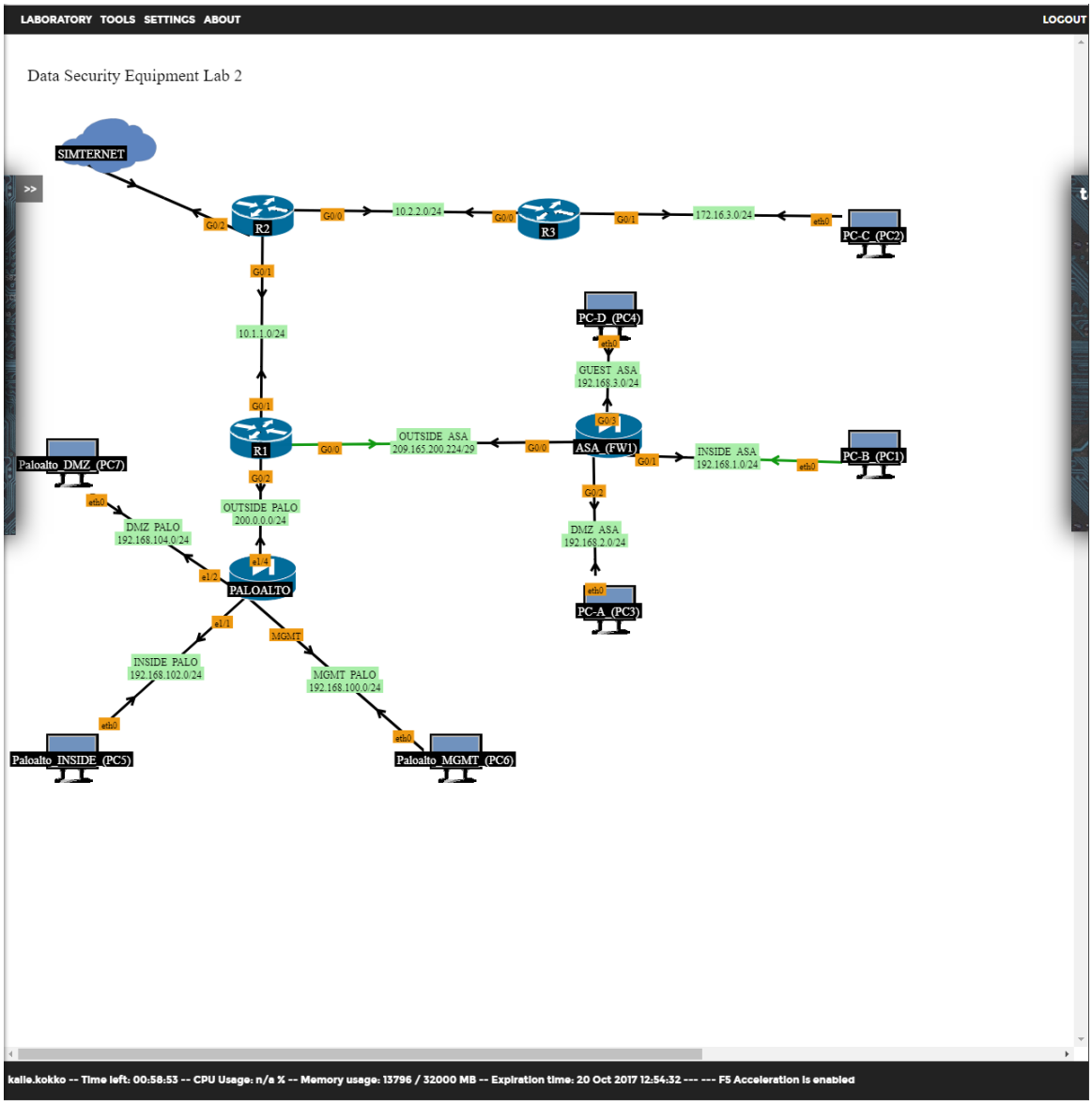

Figure 23. A freshly installed Virtual Laboratory case study instance

5.4 Services in SIMTERNET

The decision of using SIMTERNET as an alternative to real Internet connection meant that more services had to be implemented to test the capabilities of Palo Alto firewall. A simple Linux with Debian as distribution was chosen and implemented in SIMTERNET with the following services: Three different web sites that deliver content as unencrypted and encrypted traffic. The sites were to have video streaming and download services. All the sites are made with HTML5 and CSS and were hosted using Apache 2.

The first web site, “Timekill.com”, is an imaginary web hosting service provider. Timekill consists of simple text, image and link elements. It serves the purpose of being a generally generic site to access and to be distinguished in Palo Alto firewall network monitoring. The site and part of its contents are visible in figure 24.

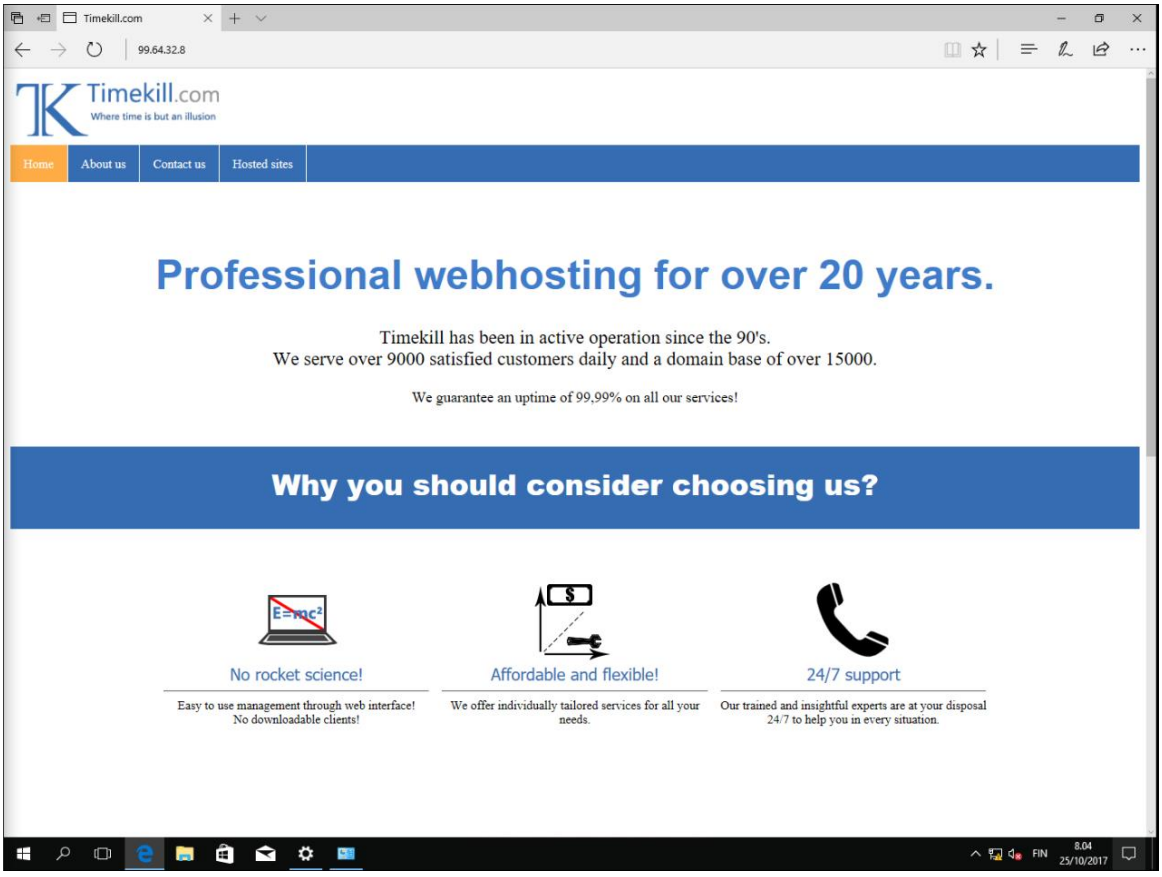

Figure 24. Timekill.com site

The second web site, “Jyytube.com”, serves the purpose of bandwidth consuming video streaming. All the videos are courtesy of Pexels, which are licensed under Creative Commons Zero (CC0) license. The site and its videos can be observed in figure 25.

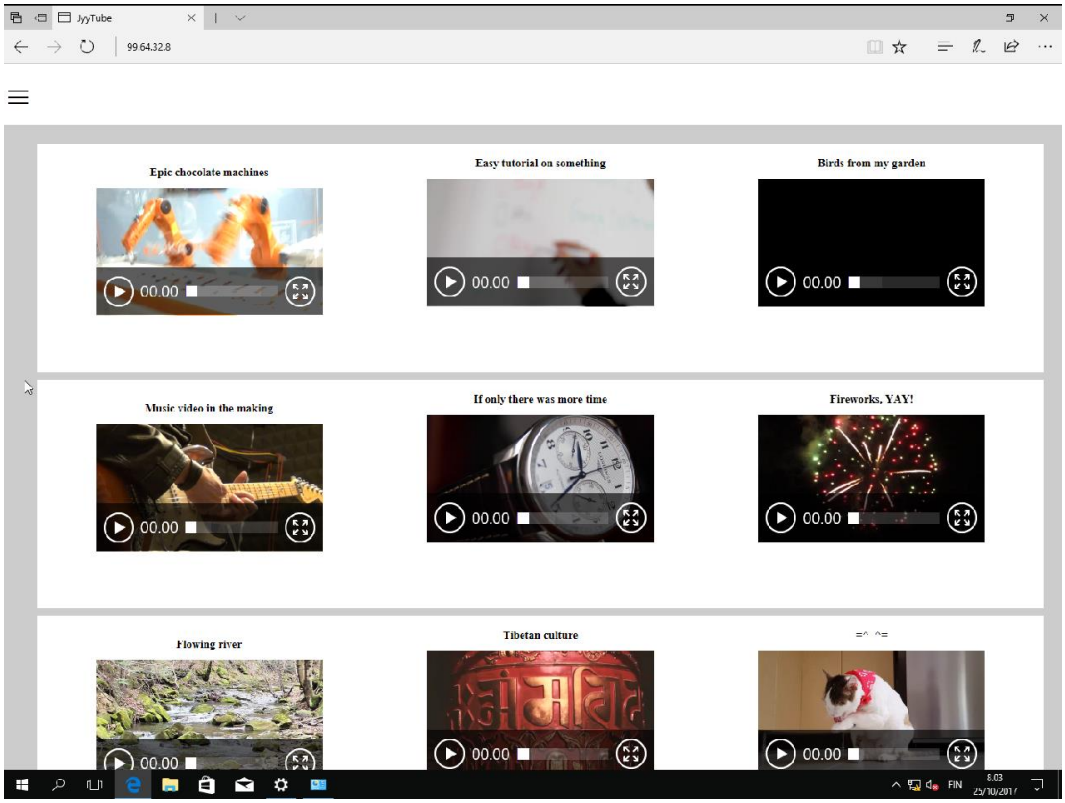

Figure 25. Jyytube.com site

The third web site, “Hacker.com”, serves the purpose of storing downloadable vulnerable files that are used to test firewall’s security capabilities, such as antivirus, anti-spyware and file blocking. Most of the files are test files provided by EICAR (European Institute for Computer Antivirus Research). The “Paloalto testfiles” are provided originally by Palo Alto itself for WildFire and file blocking test purposes. The website can be seen in figure 26.

The files provided by EICAR are designed to be seen by anti-malware as a virus, but it doesn't include any fragments of viral code. If the files themselves are run, a simple DOS program is run and the message "EICAR-STANDARD-ANTIVIRUS-TEST-FILE!" is printed. The file itself is consists entirely of simple ASCII characters, so it can be easily created and modified with a text editor. (EICAR 2017.)

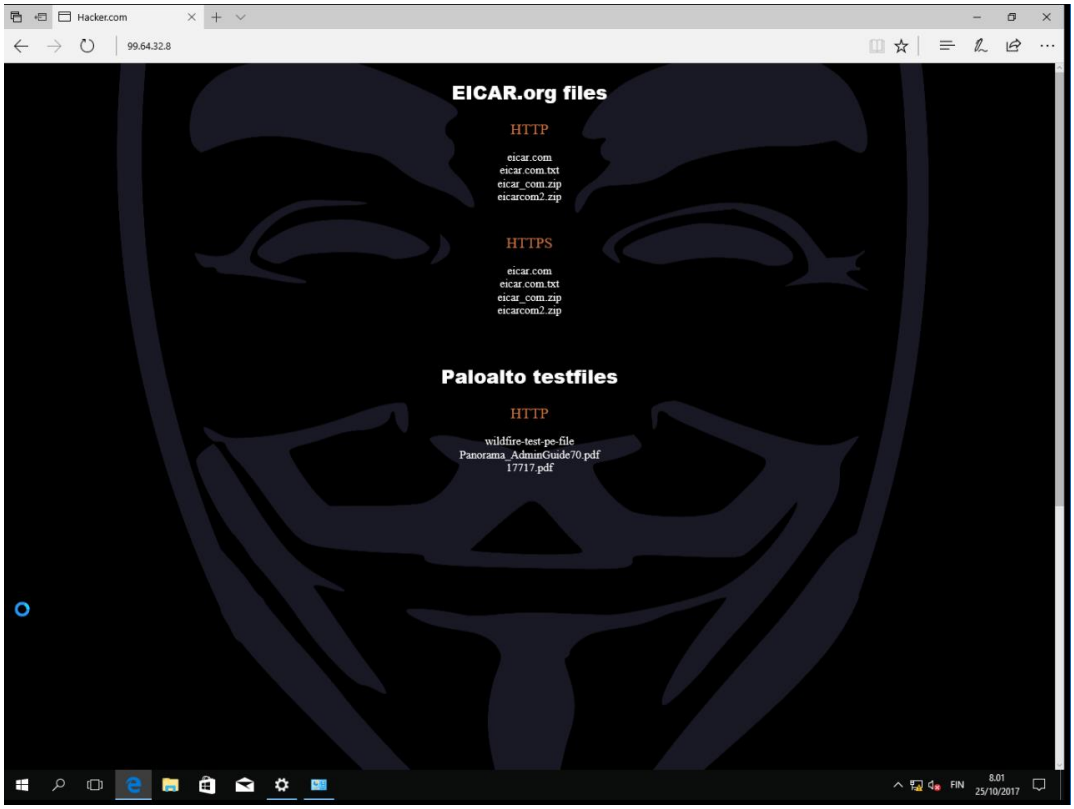

Figure 26. Hacker.com site with downloadable files

5.5 Content of the Case Study

The case study was to cover the basic connectivity configuration which involves basic interface configuration, security zones and simple security policies for connectivity between trusted, untrusted and DMZ networks. The routing between networks is achieved by utilizing virtual routers of PA appliance that create dynamic and static routes between networks. implementation of NAT and DHCP was part of the most basic functions as well. The zones and security policies involving PA appliance in the case study can be seen from figure 27.

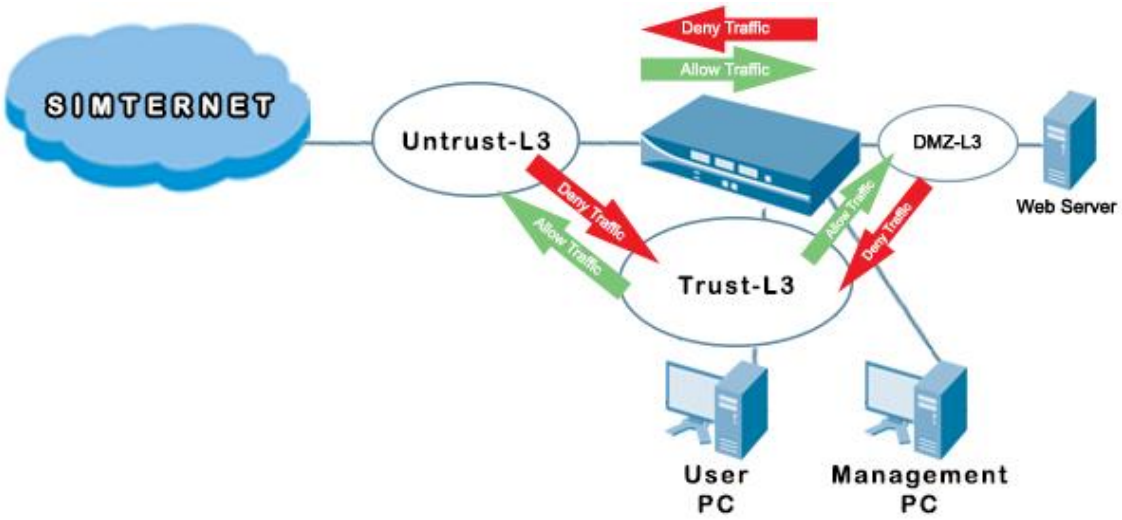

Figure 27. Security zones and security policies involving PA appliance in case study

As the enterprises host DMZ web services, the need to implement “destination NAT” was relevant. It handles the HTTP requests from untrusted network coming to the IP address of the firewall to be redirected to the DMZ network’s subnetted host by utilizing security policies and NAT. All other application requests to DMZ are blocked by implicit deny rule.

The advanced features implemented revolved around the technologies provided by Palo Alto Networks and which are further discussed in chapter 4. Implementation of App-ID ensured that the most fundamental NGFW functionality, application identification, could be demonstrated. In addition to App-ID, decryption and two self-signed certificates, trusted and untrusted, are generated and implemented as well to inspect the evasive traffic flow from liable sources. The self-signed trust certificate is also imported to trusted host devices. File blocking is taken into consideration as well in decryption to enable the scanning and blocking of possibly malicious file types. Figure 28 depicts application traffic that originates from trusted network to be filtered by App-ID.

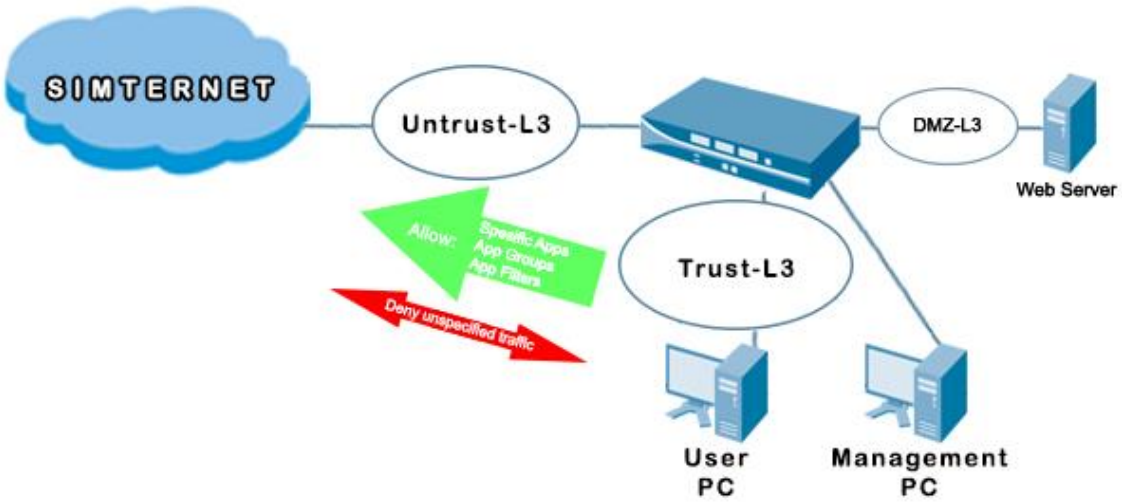

Figure 28. Basic App-ID implementation

The PA appliance works as a forwarding proxy between the web server in untrusted network and the host in trusted network. As figure 14 depicts, if the application traffic is decrypted and identified it is matched with relevant security policies and either blocked or allowed and redirected to host.

Site-to-Site VPN tunneling between PA and Cisco ASAv appliances was covered and implemented. The reason for it was to make possible the access to inside network resources between two physical enterprise locations. Also, the tunneling ensures integrity of data sent between these locations via untrusted network. Figure 20 shows the IPSec VPN tunnel between the enterprise networks traversing via untrusted network.

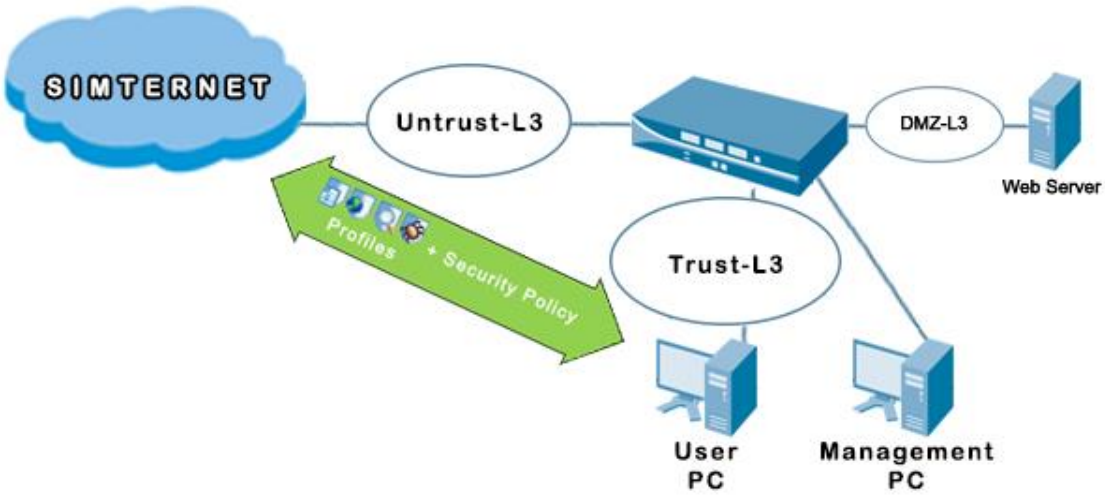

Figure 29. Basic implementation of Content-ID in the case study

The implementation of Content-ID required that custom profiles were created. The given profiles included URL filtering, antivirus and anti-spyware. All the said technologies are joined as one by use of Content-ID, and flexible custom security profile groups. The figure 29 shows the simplified depiction of Content-ID and the said profiles in use.

One of the most important feature for security teams is also covered in the case study; management of logs and generation of reports based on activity. Usually such reports are generated at regular intervals.

6 CONCLUSION

The case study unit was completed, and the needed implementation goals (see chapter 1) were achieved. Also, a rather comprehensive study guide was created, although the timeframe of the original schedule could not be accomplished.

Along the way hardware issues were present with virtual laboratory (Nurmi 2016) itself which were solved quite painlessly in the end. Also, technologies and practices regarding it changed as time progressed. The ease of creating and managing laboratories evolved and most of the text-based configurations of scenarios can be created through the Web GUI itself.

The limiting factor regarding case studies was the limited range of applications in SIMTERNET that could be taken into consideration whilst designing security policies. Thankfully the ability to connect to Internet through VPN has been implemented in the virtual laboratory for future development. This itself affected the capabilities demonstration-wise of PA appliance in use.

The given version of case study covers network that is implemented inside the enterprise network which doesn’t offer as wide spectrum of applications as Internet does. This itself limits the configuration capabilities of the PA appliance case study wise. Thus, the future studies should utilize Internet instead of SIMTERNET in that regard. Also, this would establish a need to implement QoS, GlobalProtect and DoS protection technologies in the case study.

As the case study itself covers the fundamentals of each technology covered, each one should be researched and implemented further to give a more complete understanding and competency regarding the firewall appliance to students, e.g., Security Policies, App-ID, User-ID, Content-ID and WildFire.

WildFire in itself is the single most intriguing technology, which is only covered in theory in the current version of case study. Also, the implementation of User-ID through Windows AD or LDAP would enhance the incident reporting and network monitoring capabilities.

Also, the possibility of supplying two different virtual images of PA appliance would give the possibility to test and implement High Availability (HA) in the future.

The case studies could be revised so that two students host their own enterprise networks, behind a PA appliance(s), inside Virtual Laboratories and interconnect them with VPNs between each other. This implementation method would also establish more cooperation between students.

REFERENCES

andy. 2007. Firewall Taxonomy. Available: http://codeidol.com/community/security/firewall-taxonomy/22986/ [Accessed 26 September 2017].

Deering, S. & Hinden, R. 1998. Internet Protocol, Version 6 (IPv6). Available: https://www.rfc-editor.org/info/rfc2460 [Accessed 18 October 2017].

Defense Advanced Research Projects Agency (DARPA). s.a. ARPANET and the Origins of the Internet. Available: http://www.darpa.mil/about-us/timeline/arpanet [Accessed 29 Apr. 2017].

Dierks, T. & Rescorla, E. 2008. The Transport Layer Security (TLS) Protocol Version 1.2 Available: https://www.rfc-editor.org/info/rfc5246 [Accessed 18 October 2017].

European Insitute for Computer Antivirus Research (EICAR). 2017. Intended Use. Available: http://www.eicar.org/86-0-Intended-use.html [Accessed 1 November 2017].

Frankel, S. & Krishnan, S. 2011. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. Available: https://www.rfc-editor.org/info/rfc6071 [Accessed 20 October 2017].

Juniper Networks. 2016. Understanding TCP Port Scanning. Availble: https://www.juniper.net/documentation/en_US/junos/topics/concept/reconnaissance-deterrence-port-scan-understanding.html [Accessed 10 October 2017].

Kankare, V. 2015. Implementation of a service provider networks study unit based on virtual networking environment. Available: http://www.theseus.fi/handle/10024/91528 [Accessed 17 Oct 2017].

Kent, S. & Seo, K. 2005. Security Architecture for the Internet Protocol. Available: https://www.rfc-editor.org/info/rfc4301 [Accessed 20 October 2017].

Kucharik, A. 2002. Who created the OSI model? Available: http://searchnetworking.techtarget.com/answer/Who-created-the-OSI-model [Accessed 6 June 2017].

Leiner, M., B., Cerf, G., V., Clark, D., D., Kahn, E., R., Kleinrock, L., Lynch, C., D., Postel, J., Roberts, G., L. & Wolff, S. s.a. Brief History of Internet. Available: https://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet [Accessed 29 Apr. 2017].

Kettunen, M. 2017. XAMK-Virtuaalilaboratorio. Available: https://www.ictlab.fi/images/kyberturvallisuus/tekstit/XAMK-Virtuaalilaboratorio.pdf [Accessed 29 Nov. 2017].

Miller, C., L. & CISSP. 2011. Next-Generation Firewalls For Dummies. E-book. Indianapolis: Wiley Publishing, Inc. 6-7, 12-13. Available: http://www.bradreese.com/blog/firewalls-for-dummies.pdf [Accessed 29 Apr. 2017].

Messer, J. 2007. Deciphering Nmap's Port Descriptions. Available: https://www.professormesser.com/nmap/deciphering-nmaps-port-descriptions/ [Accessed 10 October 2017].

Melby, C. 2013. Nir Zuk's Palo Alto Networks Is Blowing Up Internet Security. Forbes. Available: https://www.forbes.com/sites/calebmelby/2013/03/27/nir-zuks-palo-alto-networks-is-blowing-up-internet-security/#756b1039ff92 [Accessed 29 Apr. 2017].

Mitchell, B. 2017. Protocol (network). Available: https://www.lifewire.com/definition-of-protocol-network-817949 [Accessed 29 Apr. 2017].

Nurmi, J. 2016. Implementation of Nested Virtual Laboratory System. Available: http://www.theseus.fi/handle/10024/118489 [Accessed 25 Mar. 2017].

Omnisecu. s.a. Transmission Control Block (TCB). Available: http://www.omnisecu.com/tcpip/tcp-transmission-control-block.php [Accessed 10 October 2017].

Palo Alto Networks. 2011. Firewall Feature Overview. Available: https://media.paloaltonetworks.com/documents/Firewall_Feature_Overview.pdf [Accessed 25 Sept. 2017].

Palo Alto Networks. 2015. App-ID Tech Brief. Available: https://www.paloaltonetworks.com/resources/techbriefs/app-id-tech-brief [Accessed 25 September 2017].

Palo Alto Networks. 2016a. User-ID Tech Brief. Available: https://www.paloaltonetworks.com/resources/techbriefs/user-id-tech-brief [Accessed 25 Sept. 2017].

Palo Alto Networks. 2016b. Content-ID Tech Brief. Available: https://www.paloaltonetworks.com/resources/techbriefs/content-id-tech-brief [Accessed 25 Sept. 2017].

Palo Alto Networks. 2017a. About Wildfire. Available: https://www.paloaltonetworks.com/documentation/60/wildfire/wf_admin/wildfire-overview/about-wildfire [Accessed 25 Sept. 2017].

Palo Alto Networks. 2017b. App-ID. Available: https://www.paloaltonetworks.com/technologies/app-id [Accessed 25 Sept. 2017].

Palo Alto Networks. 2017c. Content-ID. Available: https://www.paloaltonetworks.com/technologies/content-id [Accessed 18 Apr. 2017].

Palo Alto Networks. 2017d. GlobalProtect Datasheet. Available: https://www.paloaltonetworks.com/resources/datasheets/globalprotect-datasheet [Accessed 5 October 2017].

Palo Alto Networks. 2017e. Integrated URL Filtering Datasheet. Available: https://www.paloaltonetworks.com/resources/datasheets/integrated-url-filtering-datasheet [Accessed 27 Nov. 2017].

Palo Alto Networks. 2017f. Palo Alto Networks Completes Acquisition of LightCyber. Available: https://www.paloaltonetworks.com/company/press/2017/palo-alto-networks-completes-acquisition-of-lightcyber [Accessed 29 Apr. 2017].

Palo Alto Networks. 2017g. Palo Alto Networks Reports Fiscal Third Quarter 217 Financial Results. Available: https://www.paloaltonetworks.com/company/press/2017/palo-alto-networks-reports-fiscal-third-quarter-2017-financial-results [Accessed 29 Apr. 2017].

Palo Alto Networks. 2017h. URL Filtering PAN-DB. Available: https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/url-filtering-pandb [Accessed 27 Nov. 2017].

Palo Alto Networks. 2017i. VM-Series. Available: https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series [Accessed 16 October 2017].

Palo Alto Networks. 2017j. VM-Series Deployments. Available: https://www.paloaltonetworks.com/documentation/61/virtualization/virtualization/about-the-vm-series-firewall/vm-series-deployments [Accessed 18 Apr. 2017].

Palo Alto Networks. 2017k. VM-Series Deployments. Available: https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization/about-the-vm-series-firewall/vm-series-deployments [Accessed 16 October 2017].

Palo Alto Networks. 2017l. VM-Series Specsheet. Available: https://www.paloaltonetworks.com/resources/datasheets/vm-series-specsheet [Accessed 16 October 2017].

Palo Alto Networks. 2017m. Wildfire. Available: https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/wildfire [Accessed 6 June 2017].

Palo Alto Networks. 2017n. Wildfire Datasheet. Available: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/wildfire/wildfire-ds.pdf [Accessed 25 Sept. 2017].

Palo Alto Networks. 2017o. Wildfire Deployments. Available: https://www.paloaltonetworks.com/documentation/70/wildfire/wf_admin/wildfire-overview/wildfire-deployments#_10671 [Accessed 25 Sept. 2017].

Passeri, P. 2011. TCP Split Handshake Attack Explained. Available: http://www.hackmageddon.com/2011/04/17/tcp-split-handshake-attack-explained/ [Accessed 16 October 2017].

Postel, J. 1980. User Datagram Protocol. Available: https://www.rfc-editor.org/info/rfc768 [Accessed 18 Apr. 2017].

Postel, J. 1981a. Transmission Control Protocol. Available: https://www.rfc-editor.org/info/rfc793 [Accessed 18 Apr. 2017].

Postel, J. 1981b. Internet Protocol. Available: https://www.rfc-editor.org/info/rfc791 [Accessed 18 October 2017].

Raghu, D. s.a. TCP Connection Establishment and Termination. Available: http://www.masterraghu.com/subjects/np/introduction/unix_network_programming_v1.3/ch02lev1sec6.html [Accessed 29 April 2017].

Appendix 1

LISTS OF FIGURES OR TABLES

Appendix 1

Figure 12. A simplified WildFire decision workflow based on WildFire technical documentation.

Figure 13. A detailed WildFire Decision Flow. Palo Alto Networks. 2017a. About Wildfire. Available: https://www.paloaltonetworks.com/documentation/60/wildfire/wf_admin/wildfire-overview/about-wildfire [Accessed 25 Sept. 2017].

Figure 14. App-ID operating model chart. Palo Alto Networks. 2015 App-ID Tech Brief. Available: https://www.paloaltonetworks.com/resources/techbriefs/app-id-tech-brief [Accessed 25 September 2017].

Figure 15. User-ID operating model chart. Palo Alto Networks. 2016a. User-ID Tech Brief. Available: https://www.paloaltonetworks.com/resources/techbriefs/user-id-tech-brief [Accessed 25 Sept. 2017].

Figure 16. VM-Series deployment on ESXi. Palo Alto Networks. 2017j. VM-Series Deployments. Available: https://www.paloaltonetworks.com/documentation/61/virtualization/virtualization/about-the-vm-series-firewall/vm-series-deployments [Accessed 18 Apr. 2017].

Figure 17. Palo Alto Networks single-pass parallel processing architecture. Palo Alto Networks. 2016b. Content-ID Tech Brief. Available: https://www.paloaltonetworks.com/resources/techbriefs/content-id-tech-brief [Accessed 25 Sept. 2017].

Figure 18. Stream-based scanning's effect on throughput performance. Palo Alto Networks. 2016b. Content-ID Tech Brief. Available: https://www.paloaltonetworks.com/resources/techbriefs/content-id-tech-brief [Accessed 25 Sept. 2017].

Figure 19. SIMTERNET and its topology. Kankare, V. 2015. Implementation of a service provider networks study unit based on virtual networking environment. Available: http://www.theseus.fi/handle/10024/91528 [Accessed 17 Oct 2017].

Figure 20. Palo Alto Firewall case study topology.

Figure 21. The topology file of the case study as a ".top" file.

Figure 22. The installation file of the case study.

Appendix 1

Appendix 2

Device Configurations

R1

```
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ethernet lmi ce
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
no ip domain lookup
ip domain name company.fi
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
redundancy
!
interface GigabitEthernet0/0
 ip address 209.165.200.225 255.255.255.248
 duplex auto
 speed auto
 media-type rj45
 no shut
!
interface GigabitEthernet0/1
 ip address 10.1.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
 media-type rj45
 no shut
!
interface GigabitEthernet0/2
 ip address 200.0.0.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
 media-type rj45
 no shut
!
```

Appendix 2

```
ip forward-protocol nd
!
!
ip http server
ip http authentication local
ip http secure-server
ip nat inside source list 1 interface GigabitEthernet0/2 overload
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1
ip route 192.168.1.0 255.255.255.0 GigabitEthernet0/0
ip route 0.0.0.0 0.0.0.0 dhcp
!
access-list 1 permit 200.0.0.0 0.0.0.255
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 logging synchronous
 login local
 transport input telnet ssh
!
no scheduler allocate
!
do wr
!
```

R2

```
hostname R2
!
interface GigabitEthernet0/0
 ip address 10.2.2.2 255.255.255.252
 ip nat inside
 no shut
!
interface GigabitEthernet0/1
 ip address 10.1.1.2 255.255.255.252
 ip nat inside
 no shut
!
interface GigabitEthernet0/2
 ip address dhcp
 ip nat outside
 no shut
!
no ip http server
no ip http secure-server
ip nat inside source list 1 interface GigabitEthernet0/2 overload
ip route 172.16.3.0 255.255.255.0 10.2.2.1
ip route 200.0.0.0 255.255.255.0 10.1.1.1
ip route 209.165.200.224 255.255.255.248 10.1.1.1
ip route 0.0.0.0 0.0.0.0 dhcp
```

```
!
!
access-list 1 permit 200.0.0.0 0.0.0.255
access-list 1 permit 209.165.200.224 0.0.0.7
access-list 1 permit 172.16.3.0 0.0.0.255
!
do wr
!
```

Cisco ASA

```
hostname CCNAS-ASA
domain-name ccnasecurity.com
enable password cisco
!
interface gig0/1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shut
!
interface gig0/0
nameif outside
security-level 0
ip address 209.165.200.226 255.255.255.248
no shut
!
interface gig0/2
nameif dmz
security-level 70
ip address 192.168.2.1 255.255.255.0
no shut
!
object network inside-net
subnet 192.168.1.0 255.255.255.0
!
object network dmz-server
host 192.168.2.3
!
access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3
!
object network inside-net
nat (inside,outside) dynamic interface
!
object network dmz-server
nat (dmz,outside) static 209.165.200.227
!
access-group OUTSIDE-DMZ in interface outside
!
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
!
```

```
username admin password admin
!
aaa authentication ssh console LOCAL
aaa authentication http console LOCAL
!
http server enable
http 192.168.1.0 255.255.255.0 inside
ssh 192.168.1.0 255.255.255.0 inside
ssh timeout 10
!
class-map inspection_default
match default-inspection-traffic
policy-map global_policy
class inspection_default
inspect icmp
!
crypto key generate rsa modulus 1024
yes
!
wr mem
!
```

Palo Alto Firewall

```
configure
!
set deviceconfig system ip-address 192.168.100.1 netmask 255.255.255.0
!
commit
!
```

Appendix 3/1

Appendix 3

Palo Alto Networks Firewall Case study

HIDDEN