

FUNCTIONAL TESTING OF BYOD FEATURES WITH NEXT-GENERATION FIREWALL

PAN-OS Version 5.0.x

Pauli Laine

Master's Thesis
December 2013

Master's Degree Programme in Information Technology



JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES



Tekijä(t) Laine, Pauli	Julkaisun laji Opinnäytetyö	Päivämäärä 1.12.2013
	Sivumäärä 142	Julkaisun kieli Englanti
	Luottamuksellisuus () saakka	Verkojulkaisulupa myönnetty (X)
Työn nimi BYOD-toiminnallisuuden testaaminen uuden sukupolven palomuurilla		
Koulutusohjelma Kyberturvallisuus		
Työn ohjaaja(t) Rantonen, Mika Hautamäki, Jari		
Toimeksiantaja(t) NCC Rakennus Hovi, Jori		
Tiivistelmä <p>Opinnäytetyön tavoitteena oli testata uuden sukupolven palomuuriratkaisulla toteutettavia etäkäyttötapoja eri päätelaitteilla ja käyttöjärjestelmillä. Yksi keskeinen tavoite oli useiden erilaisten etäyhteystapojen mahdollistaminen samanaikaisesti siten, että tietoturvan näkyvyys ei heikkene millään vaihtoehdoista nykyisiin ratkaisuihin verrattuna. Asiaa lähestyttiin teoreettiselta näkökulmalta kuvaten aluksi IT:n kehitystä viime vuosina. Tämän jälkeen tarkasteltiin tietoturvan ja erilaisten etäkäyttömenetelmien kannalta perinteisillä menetelmillä tehtyjä ratkaisuja sekä uudempien etäkäyttöratkaisujen ominaisuuksia. Siinä missä perinteiset ratkaisut perustuvat yksittäisiin palveluihin tai toiminnallisuuksiin, jotka eivät kommunikoi toinen toistensa kanssa, uuden sukupolven ratkaisut perustuvat uudenaiseen arkkitehtuuriin, jossa eri toiminnollisuudet sulautuvat yhteen, muodostaen yhden loogisen kokonaisuuden.</p> <p>Opinnäytetyössä esitetään teoria tietoliikenneverkon rajalla olevien useiden perinteisiin menetelmiin perustuvien laitteiden korvaamisesta yhdellä uuden sukupolven ratkaisulla. Empiirisellä tutkimuksella testattiin uuden sukupolven palomuuriratkaisun tuomia ominaisuuksia ja niiden toiminnallisuuksia etäkäytössä. Teorian, käytännön kokemuksen ja empiirisen testauksen tuloksena päädyttiin lopputulokseen, jossa yritys voi korvata tietoliikenneverkon reunalla olevat laitteistot ja palvelut joko kokonaan tai osittain yhdellä kahdennettulla uuden sukupolven palomuuriratkaisulla. Tämä mahdollistaa uudenlaisten kontrollien käytön etäkäyttömenetelmissä sekä tuo uudenlaista tietoturvan kokonaiskuvaa ja näkyvyyttä, jollaista on työläs saavuttaa perinteisillä ratkaisulla. Näin saavutettavissa olevista eduista muodostuu kokonaiskuva, joka mahdollistaa tietoturvatason säilymisen ja jopa paranemisen perinteisiin menetelmiin verrattuna.</p>		
Avainsanat (asiasanat) BYOD, NGFW, uuden sukupolven palomuri, etäkäyttö, mobiililaitteet, Android, iOS		
Muut tiedot Palomuurin arkkitehtuuri, single pass parallel processing, SP3		



Author(s) Laine, Pauli	Type of publication Master's Thesis	Date 1 st December 2013
	Pages 142	Language English
	Confidential () Until	Permission for web publication (X)
Title Functional Testing of BYOD Features with Next-Generation Firewall		
Degree Programme Cyber Security		
Tutor(s) Rantonen, Mika Hautamäki, Jari		
Assigned by NCC Construction Hovi, Jori		
Abstract <p>The objective of the thesis was to test different kind of remote access methods with different mobile devices and platforms leveraging Next-Generation FireWall features. The most essential objective was to enable several different remote access methods simultaneously without the expense of the overall security visibility that cannot be deteriorated compared to the existing methods. A theoretical approach was chosen to briefly illustrate the evolution of IT during the past years. The same method was chosen to illustrate the security perspective and the variety of remote access methods utilizing traditional technology approaches and the Next-Generation FireWall's features. Where traditional technology solutions are based on a single functionalities or services that are not integrated with each other, Next-Generation architecture is based on many functionalities integrated into one single device solution, forming a one logical solution.</p> <p>The thesis introduces a theory of replacing several devices based on traditional technology solutions with a Next-Generation FireWall platform. Empirical research method was chosen to test the Next-Generation FireWall's remote access solutions and features. The outcome of combining the theory, practical experience and empirical research was that a company can replace the devices based on traditional technology solutions on the border of the network entirely or partially with one logical Next-Generation FireWall solution. This enables new control methods in remote access environment and permits the total visibility of the security perspective, which is laborious to achieve with traditional technology solutions. The benefits achieved with this approach forms a security visibility that does not deteriorate the overall security visibility; instead the overall security may improve compared to traditional technology solutions.</p>		
Keywords BYOD, NGFW, Next-Generation Firewall, Remote Access, Mobile devices, Android, iOS		
Miscellaneous FireWall architecture, single pass parallel processing, SP3		

Acknowledgements

I want to thank you my tutors Mika Rantonen and Jari Hautamäki for feedback and guidance during the thesis. I also want to thank NCC Construction Finland for permitting the use of resources and equipment for the past year. Especially, thank you my family, for supporting my studies during my work and outside working hours.

Acronyms

AD	Active Directory
AES	Advanced Encryption Standard
AP	Access Point
API	Application Programming Interface
APT	Advanced Persistent Threat
ASIC	Application Specific Integrated Circuit
BYOD	Bring Your Own Device
BYODT	Bring Your Own Device and Technology
BYOE	Bring Your Own Everything
CA	Certificate Authority
C&C	Command&Control (also known as CC)
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COBIT5	Control Objectives for Information and Related Technology
CRO	Chief Risk Officer
CRMO	Chief Risk Management Officer
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
CYOD	Choose Your Own Device
GP	Global Protect
GUI	Graphical User Interface
HIP	Host Identification Protocol
(H)IDS	(Host-based) Intrusion Detection System
(HI)IPS	(Host-based) Intrusion Prevention System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secured
HYOD	Have Your Own Device
IPsec	IP Security Architecture
ISP	Internet Service Provider
JAR	Java ARchive
LB	Load Balancer
LAN	Local Access Network
LAN2LAN	LAN to LAN (also know as L2L)
MDM	Mobile Device Management
NAT	Network Address Translation
NGFW	Next-Generation FireWall
(N)IDS	(Network-based) Intrusion Detection System
(NI)IPS	(Network-based) Intrusion Prevention System
OYOD	Own Your Own Device
OSI	Open Systems Interconnection
PAT	Port Address Translation
PDF	Portable Document Format
PMO	Project Management Office
QoS	Quality of Service
REST	Representational State Transfer
SD	Service Desk

SCCM	System Center Configuration Manager
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SME	Subject Matter Expert
SP3	Single Pass Parallel Processing
SSL	Secure Socket Layer
SSO	Single Sign-On
TCO	Total Cost of Ownership
UTM	Universal Threat Management
VPN	Virtual Private Network
WLAN	Wireless Access Network
WPA-2	Wi-Fi Protected Access
WSUS	Windows Server Update Services
XML	Extensible Markup Language

Table of Contents

1 INTRODUCTION	5
1.1 Scope.....	6
1.2 The Objective of the Research.....	7
1.3 Structure of the Thesis.....	7
2 LITERATURE REVIEW	8
2.1 Evolution of IT Organization	8
2.2 Evolution of Internet-related Threats	10
2.3 Evolution of Network Perimeter	11
2.4 BYOD Surveys	12
2.5 NGFW Surveys	21
3 THEORY OF REPLACING THE SERVICES	31
3.1 Traditional way of doing Remote Access	31
3.2 Traditional way of doing BYOD.....	33
3.3 Remote Access and BYOD with NGFW	33
3.4 Architectural Differences between Traditional FW's and NGFW's	37
3.5 MDM (Mobile Device Management).....	51
4 EMPIRICAL STUDY: TESTING THE FUNCTIONALITIES	52
4.1 Testing Environment and Equipment.....	52
4.2 Test Plan and Tested Functionalities	53
4.3 Installations and Tests	58
4.3.1 Android Installation with Global Protect Client	58
4.3.2 Android Usage with Global Protect Client.....	62
4.3.3 iPad installation with Global Protect Client.....	70
4.3.4 iPad usage with Global Protect Client	72
4.3.5 Windows7 Installation with Global Protect Client	76
4.3.6 Windows7 Usage with Global Protect Client	78
4.3.7 QoS Testing.....	84
4.3.8 Geographical location usage	85
4.3.9 HIP Matching	86
4.3.10 Threat Identification.....	89
4.3.11 WildFire Reports during the Test Period.....	95
4.3.12 Custom Applications.....	118
4.3.13 Updates	121
5 RESULTS	124
6 CONCLUSIONS AND DISCUSSION	129
6.1 Answering the Research Questions.....	131
6.2 Validity and Credibility of the Study	133
6.3 Areas for Further Research.....	134
References	136
Appendices.....	141
Appendix A: Application Usage and Threat Report – February 2013	142

1 INTRODUCTION

Companies have been allowing remote access to the end users for years to provide access to the corporate resources. Remote access needs for end users has been evolved ever since it has been technically possible to arrange. First, it was introduced for maintenance purposes only and afterwards for end users, but with technology-dependent solutions and limited support and functionalities. Later on, more user-friendly solutions have been evolved with standardized protocols, like IPsec (IP Security Architecture) using VPN (Virtual Private Network) technology. Traditionally, this has been arranged by using corporate devices, which is usually a laptop, configuring the remote access using the technology that the corporate provides and signing a contract or a remote access policy. Corporate IT manages and supports remote access service and has the total responsibility. This traditional way of doing remote access is still very common in today's business.

For the past years there has been a great deal of discussion about BYOD (Bring Your Own Device) for another method of remote access. There are also several acronyms for similar usage, such as CYOD (Choose Your Own Device), HYOD (Here is Your Own Device), OYOD (On Your Own Device) and BYODT (Bring Your Own Device and Technology). The differences between these terms are so insignificant (JGRSC, 2013) that we can talk about BYODT to refer all of these methods except HYOD. HYOD is similar to traditional way of doing remote access where corporate has total control of device, access and data and has total responsibility and support of the concept. All the other acronyms refer to the model, where neither end user nor corporate has total control of the device, access or data and neither party shares the total responsibility or support. Instead, all of them are shared between the end user and the company.

BYODT will provide flexibility to the user when certain job-related functions can be done remotely with one's own, familiar device, instead of a corporate device, but this also introduces risks if not done securely. The same end user's device now shares the job-related data and personal data, which both have different kind of data classi-

fication and retention. Additional security needs to be in place, to address risks that the end user's device and data expose when it is outside corporate premises and especially in personal use, since corporate data usually have more strict data classification criteria than a user's personal data. Security adds complexity since the network connection and the user's device needs to be secured. Increased security also decreases usability and user-friendliness. Increased security means that user authentication and Need-to-Know or Least Privilege must be in place to meet the security demands for remote access defined by the corporate itself to protect its data. Leveraging BYODT in corporate environment is a direct consequence of Consumerization of IT. BYODT devices were first designed for consumers' use and therefore their security features were slightly different than devices designed for corporate use. Today, they are more mature and security and manageability features will meet the corporate demands on many mobile platforms. BYODT devices have become more and more common in corporate environments worldwide.

1.1 Scope

Building a remote access that is easy enough for the users, secured from end-to-end and not too complicated to manage, is challenging. This is the case, because increasing security affects the end user experience and ease of use negatively. Also, bigger environment and multiple solutions create more complexity and maintenance tasks. So far, companies have built up their IT infrastructure with devices that usually do one or few purposes or services only. As the services has been expanded over the years, the number of devices has been increased, which creates more complexity and administration tasks. The scope of this research is to leverage the functionalities in Next-Generation Firewall (NGFW) so that many of those purposes and services can be replaced with one single device, which would be seen as more simplified environment and without degradation of security, performance and latency. In addition, better overall security visibility and easier maintenance tasks can be achieved. The scope will be limited to one NGFW product and two remote access solutions. One remote access solution is based on BYODT method and another based on traditional

remote access method. Remote access devices will be Samsung's phone with Android Operating System (OS), Apple's iPad with iOS and a laptop with Windows 7.

1.2 The Objective of the Research

The objective of this research is functional testing of Next-Generation Firewall (NGFW) to find out if NGFW can support traditional remote access method and BYOD technologies at the same time without compromising IT Security and in order to achieve better visibility of IT related risks. The objective also includes finding out if NGFW environment can simplify traditional network infrastructure. The research method was empirical research for the functionality tests of NGFW product and literature research for BYOD and NGFW solutions. The research questions were:

- Do NGFW functionalities work as expected?
- Can traditional remote access and BYOD Technologies be supported with only one (logical) NGFW device?
- Can the IT Environment be simplified using NGFW?
- Can security still be measured and not degraded with NGFW?

1.3 Structure of the Thesis

Chapter two introduces the backgrounds of the perimeter network evolution in the companies for the past years and the existing literature of BYOD models and researches. It also introduces some NGFW surveys and some implementation examples and surveys. Even though NGFWs has existed since 2005, and many companies have implemented them in their environments, not so many implementation researches have been made or are publicly available.

Chapter three introduces a traditional way of implementing perimeter security and remote access, as well as a theory for implementing and replacing the traditional network perimeter including remote access system with NGFW solution. Architectur-

al differences between traditional network devices and Palo Alto Networks NGFW device are also introduced.

Chapter four presents the testing environment, testing plan and tested functionalities with different platforms. The results are presented in chapter five.

The final chapter is chapter six, which presents conclusions and discussion about the thesis and answers the research questions with areas of further research.

2 LITERATURE REVIEW

2.1 Evolution of IT Organization

Companies' network and infrastructure has been growing and becoming more complicated in the 2000s and afterwards especially in medium-sized and large companies. There are many reasons for this concerning business itself and the consequences effecting IT infrastructure and services directly. Business itself expands, collaborates and changes constantly and sometimes rapidly, which means that the IT infrastructure and services must adapt to the changes as well. Since business changes always have possibilities and threats, they will affect the IT and therefore these changes have also an effect on the infrastructure. In the early 2000 IT Department was driven by CFO (Chief Financial Officer) or CIO (Chief Information Officer) and IT expenses were more constant and predictable. In the mid of 2000, new positions were introduced, like CSO (Chief Security Officer), CISO (Chief Information Security Officer) CRO (Chief Risk Officer) and CRMO (Chief Risk Management Officer). Organization hierarchies changed to become more complex and governance and bureaucracy increased. In the late 2000, PMO (Project Management Office) was already introduced in many companies and took responsibility of project management, project portfolios and processes was designed to be more productive. IT department, among others, was starting to utilize SD (Service Desk) and ticketing systems to han-

dependencies among systems, projects and incidents. Reporting became more important to mid-level managers and follow-up of expenses was started, Service Levels were agreed to services and SLAs (Service Level Agreements) with partner, including contracts and sanctions. Partners and consultants were more utilized, since systems became complicated and SME's (System Matter Experts) were more often needed to trouble-shoot problems and incidents. Then Cloud-Based Services and virtualization were introduced and got immediate interest because they offered a variety of services with low cost expectations. This contributed to outsourcing of IT Services partially or most of the services and even different partners, which created more fragmentation and inefficiencies. That is because information must reach all parties and collaboration and teamwork must work seamlessly over the company borders. At the same time, application landscape started to move towards more browser-based form and started to shift from internal networks to the internet and some of them were encrypted. The total landscape of the network and security was fragmented over the years and maintaining systems became more complicated, since more parties and administrators were involved.

A Centralized Management System and Network Monitoring System were needed to manage changes and monitor network and events and to increase response times. Also, SIEM (Security Incident and Event Management) was needed to handle the great amount of events and log entries to intelligently filter only essential information. However, the outsourced IT Services were not always able to be monitored, at least on a satisfied level. Internal and independent audits and regulation compliances were paid more attention to. When organizational and technical landscape changed rapidly sometimes into even different directions, business alignment suffered resulting in poor operability of the IT services. Today, business changes are best controlled and managed in the management level with top-to-bottom approach which should eventually affect the operational level. Thus, active and utilitarian organization hierarchy, right key-persons, encouraging and recognizing atmosphere, strong cooperation between departments and training are key elements to successfully handle changes throughout organization in reasonable timeframe. COBIT5 (Con-

Control Objectives for Information and Related Technology) can be a helpful framework for enterprises to plan, implement and maintain security for remote devices including BYODT. Operational level problems and solutions includes technology and architectural point of view which can be handled with the right training of skilled staff with effective practices and processes with bottom-to-top approach, which requires good communication skills in management level.

2.2 Evolution of Internet-related Threats

In addition to business related changes, IT related changes have increased more rapidly after 2000 and it seems to be an ongoing trend today. Increased threats towards a variety of applications and different operating systems have become more common today than in early 2000s. Vulnerabilities are discovered in almost all applications and platforms so rapidly that there is barely enough time to patch them before new vulnerabilities are discovered. Unwanted programs, like malware, trojans and viruses that exploit vulnerabilities are published more rapidly than in early 2000s. For the past years, APT (Advanced Persistent Threats) and targeted attacks has taken place for more sophisticated electronic espionage and spying of government or company secrets. Unwanted programs are not created by individuals or groups anymore, since they have become extremely sophisticated and organized by entities that have capability and means to produce ones (Mandiant, 2013, The Guardian 2013). These all are commonly used to refer as cyber threats, which have been raised by one of the largest concerns almost in every business (Lloyd's, 2013). People's behavior has also changed since past years. Today, Social Media and Web 2.0 play a more significant part in people's life, and Social Media itself introduces risks and vulnerabilities that need to be addressed by the company, since companies' resources are used to access Social Media, and Social Media, in turn, can be used to gain information of company users and to conduct targeted attacks. This behavior has also changed the remote access thinking. Consumerization of IT has introduced the BYODT approach, which indeed will introduce threats to the remote access environment. The funda-

mental feature of BYODT is that a user and company share the same device and data. The device is user's property and data is divided into user's personal data and company's data, which both usually have different kind of data classification and retention. This is the major difference between traditional remote access and BYODT and it generates the most significant concerns between these two methods.

2.3 Evolution of Network Perimeter

In early 2000, every company had a FW (FireWall) in the border of the network and every workstation and server had antivirus (AV) programs to address unwanted programs, which was considered a satisfactory combination at that time. The FW filters traffic based on the ports and protocols that the administrator had configured, usually allowing business related traffic to communicate between internal and DMZ (De-Militarized Zone) networks and denying traffic from the internet. The AV program inspects the files in the clients and servers for unwanted software just to make sure nothing gets past the firewall or out-of-band threats, such as files from CD-ROM and USB drives to name some. Then, gateway level protection was a new technology that was becoming a more common solution to gain layered protection to email and un-encrypted www-traffic in addition to AV protection in end points. Yet, they both based on different AV vendors, instead of a new technology solution.

In the mid of 2000, IDS/IPS (Intrusion Detection System/Intrusion Prevention System) solution was introduced. HIDS (Host-based Intrusion Detection System) and NIDS (Network-based Intrusion Detection System) as well as HIPS (Host-based Intrusion Prevention System) and NIPS (Network-based Intrusion Prevention System) was introduced by different security- and AV vendors. Where IDS could detect the threat or attack IPS could prevent it, since IDS was only monitoring traffic and anomalies, whereas IPS was connected in-line to have the ability to reset the connection when anomalies were detected. So, in-line topology needs to be built as fault-tolerance to prevent SPFs (Single point of Failure) in the network. To address SPFs, a LB (Load Bal-

ancers) was commonly used to balance traffic loads to two or more devices. Soon after IDS/IPS technologies, UTM (Universal Threat Management) was introduced. UTM was the first try to implement all or most of the previously mentioned technologies into one box to lower down the device complexity and costs, especially in the branch offices. However, when all those technologies and numerous functionalities are put into one device to the hardware that is not built to do that, the latency and performance will collapse. Another consequence was also that the functionalities had to be greatly reduced, since one box can have only a limited amount of configurations and features with the hardware used at that time. That is the main reason why UTM products are not so common today.

At this point, in the late 2000, centralized logging and monitoring was introduced to handle incidents and events from a variety of sources and platforms. Network protocols, like SNMP, SYSLOG and Netflow were used. Since the amount of logs increased and was hard to manage, intelligence was needed and SIEM was a solution to filter out and correlate many log entries to fewer meaningful alarms or alerts. The latest innovation is the NGFW product, and the first NGFW product shipped out at 2007. NGFWs continued what UTM could not handle. The only way doing it was to build the hardware completely all over again. With purpose-built hardware, NGFWs could take the challenge of implementing many services into one box without any or only minor latency and performance degradation. Some of the innovations were application identification based on behavior regardless of the evasion tactics, identifying users regardless of IP address, scanning the content to address targeted attacks and data leakage and introducing sandbox technology based on cloud-based or private platform.

2.4 BYOD Surveys

Utilization of BYOD technologies in the classroom introduced positive learning atmosphere, according to a literature research in Michigan University (Vanwelsenaers 2012, 22-23). It also improved student engagement, interaction with peers and

communication and extended the place and time of learning. If these opportunities can be achieved in the student society by supporting BYOD technologies, then there is potential to enable them by using BYOD in working life as well. Any technology solution or other method that is supporting productivity and positive learning atmosphere is most likely worth of investment, since a happy, innovated and motivated employee is the most productive employee. Of course BYOD includes risks that cannot be forgotten and needs careful considerations before implementation. The whole lifecycle of BYOD technologies needs to be considered at the first place. There were eight key findings in a research by Educause Center for Applied Research for The Consumerization of Technology and the BYOE Era of Higher Education (Dahlstrom & diFilipo, 2013, 4-5, 37):

1. Unmanaged proliferation of devices could result in a situation, where too many devices access campus networks too fast and institutions find more opportunities lost than taken
2. IT leaders express support for BYOE to promote happy and productive faculty and staff
3. Doing before planning is actually the norm – yet policies are in place where they matter most, such as security and end-user behaviors
4. Security practices should be invested in managing risks and raising user awareness
5. BYOE cost savings can be elusive with the cost to upgrade IT infrastructure
6. IT infrastructure should be considered as a BYOD middleware, which should be robust and nimble at the same time
7. Support strategies need to consider the lag between BYOE ubiquity and do-it-yourself support and therefore adapt to BYOE environments
8. Utilizing mobile technologies is a priority, but how to best do so, remains uncommon.

The recommendations included that one should not count on savings, but if any, then invest on infrastructure. It also estimates that user-provisioned technologies

will proliferate and they do very little to change the basic best practices in security. Data and access to the data should be secured rather than devices and more collaboration should be done inside organization not forgetting user-awareness. (Dahlstrom & diFilipo, 2013, 4-5, 37). Investing in the infrastructure is far-reaching and many security features do not differ so much from the current solutions that companies already have, however people's behaviors are more difficult to affect. Although this research has been in the higher education institutes and among students and teachers, there is still valuable information and experience for companies to develop, since students who practiced with BYOD will be (and already are) in the working life. There is competition of good employee in the industry in every field.

According to a research of University of Oregon, Competitive advantage and cost-savings are factors when developing BYOD Strategy in Higher Education (Emery, 2012, 90-97). It also states that IT policy needs to be more specific than traditional IT policy to address data network security and the control over it. BYOD policy needs to be designed in collaboration with users and "IT must educate user as to the dangers and limitations of using their personal devices at work" (Emery, 2012, 91). A factor to consider related to data security was found that "a competitive edge promised by mobility can be wasted if consumer-owned mobile devices are not adequately protected against mobile device security threats" (Emery, 2012, 94). Appropriate safeguards were to implement an access control based on user identification, device type and access type or location and leveraging the six factors: segregation of data, device registration, remote access to a mobile device, data encryption, strong passwords and VPN. (Emery, 2012, 90-97.) The importance of policies cannot be overstated, since users must be familiar with policies and acceptable behaviors with BYOD devices. Infrastructure is easier to upgrade and manage. If BYOD is being used prior to policies and appropriate procedures, then it is much more difficult and time consuming to try to change behaviors and attitudes when users are already familiar with their own usage which may not be the correct way of accessing, using and distributing corporate data.

A research was made by Journal of Business Management & Social Sciences Research about BYOD for 88 respondents in different kind of business sectors like IT, Consultancy, educational institutes and others. Since 88 respondents out of 136 samples were aware of BYOD policy, only 88 were taken into consideration for data analysis and interpretation. It concluded that 45 % of respondents agreed that BYOD is lucrative for the organization and only 4 % fully disagree with this view. It also revealed that if BYOD has some threats and risks, few of the advantages overshadowed its risks and most of the respondents felt that BYOD should be still applied in the organizations; however with definitely some security measures. 45% of respondents named Corporate IT Security as the major threat of BYOD, the second was Lack of control over devices and the third was Complexity of set up. (Nisharika, 2012, 7-10.) 45% of BYOD users feel that supporting BYOD technologies is lucrative, but 35% of the users does not even know that a BYOD policy exists. User-awareness and education needs to be taken care of continually and with several methods to achieve the best possible coverage among end users. If the device is the property of end user, as it usually is in BYOD solutions, then the end user is most likely more motivated and concerned with security threats and countermeasures. Contractual liabilities in the policies are also one motivation factor with end users commitments.

Nucleus Research made a research of "Understanding the Hard ROI of BYOD" in April 2013. It states that companies must consider six major areas in understanding ROI of BYOD: Device costs, voice and data costs, helpdesk costs, mobile developer costs, enterprise mobility management software and the productivity obtained specifically through personally-owned devices. Device costs are only a small fraction of the total costs of enterprise mobility. "Voice and data costs reimbursement above 40\$ per month implies a company is deliberately giving up money to support BYOD". Help Desk costs vary depending on the outsourcing model. For example, for one employee to device support for every 1000 devices is 5\$ per month when Tier 1 (basic settings and device support) is moved to IT Help Desk and Tier 2 (advanced trouble-shooting, mobile applications and other mobile problems) is outsourced. But depending on the organization, this can vary 50\$ per month. Fully-loaded cost of a mobile developer

was estimated to be at 150,000\$ yearly. This can lead to significant benefits, including increased productivity. Mobility management methods must protect corporate data in compliance-based market to avoid potential liability issues, regardless of corporate or personal ownership. If an employee needs a specific technology to do their work effectively, the business should invest in that technology; however if the value of mobile technology cannot justify a corporate investment, then why does the employee need it at all. The major winners of BYOD are Telecom Carriers from the financial perspective and the losers are the ones that are supporting technology strategy and those responsible for risk and compliance in the companies. (Nucleus Research, 2013.) Intangible or indirect costs are hard to calculate, such as ROI of BYOD or productivity, however practices also vary in every company, country and culture. But if the productivity increases, the potential can be huge and yet hard to calculate. Therefore it can be challenging to justify this for decision makers who want to see cost-effect solutions and savings instead of estimates that cannot be based on facts or cannot even be calculated with any accuracy. Personalities and relationships have a major role between decision making level and CIO. Direct costs like infrastructure costs, including maintenance costs and license costs, are easier to calculate.

A thesis made by Viitamäki at Metropolia of "Aruba BYOD or Citrix VDI as Solution for Multinational Enterprise" (Viitamäki, 2013, 25-26, 46-47), points out that if application or virtual desktop is not designed for touch screens, it is not realistic to assume that it would be user-friendly. This is the case, when serving Windows based application or virtual desktops to iPads or iPhones without separate key boards. They are also prone to network problems, like all real-time applications. Citrix installation was multistage and Citrix licenses were found opaque since users and Windows servers needed to be licensed separately. Citrix was found to be secure, since information is not saved on end users' device, instead in the corporate resources. ClearPass' challenges were found to be complex roles and policies which may effect to complex rollout. 802.1X support is a prerequisite for the company's routers and switches prior to rollout. The design of the network is essential in ClearPass' case and the rollout needs the most design work than installations. (Viitamäki, 2013, 25-26, 46-47.)

Choosing the right technology solution is essential, since it plays a major role in every environment. Therefore, companies need to compare different solutions in their needs to verify that the solution and the support chain operate as expected and it is customizable and scalable for 3-5 years' needs, including BYOD solutions and technologies.

Gartner, the world's leading information technology research and advisory company, predicts that by 2017, half of the employers will require employees to supply their own device for work purposes and enterprises that offer only corporate-liable programs will soon be the exception. This may take place in the USA, however the rest of the world will follow subsequently. (Gartner, 2013.) This estimate is in line with Check Point's survey. It sponsored a global survey conducted by Dimensional Research of 790 IT professionals in the USA, Canada, UK, Germany and Japan. The result was that BYOD is growing dramatically in enterprises of all size and the BYOD movement has dramatically increased the expensive security incidents. Some of the key findings were also, that 79% of the companies reported security incidents in the past year and 52% of large companies reported costs of mobile security incidents last year exceeded \$500, 000. 45% of businesses with less than 1000 employees reported costs exceeding \$100,000. Half of the respondents cited that Android perceived with greatest security risk compared to other platforms and 66% stated that a careless employee is a greater security risk than cybercriminals. 63% of the responded companies do not manage corporate information on personal devices at all. (Dimensional Research, 2013.) BYOD technologies will be more common in near future and preparing infrastructure, people and policies will take time. It is expensive to choose not to manage data or mobile devices, when some of the most common risks are realized.

ISACA (Information Systems Audit and Control Association), an independent, non-profit and global association, conducted a survey at November 2012 for more than 4,500 of its members in 83 countries, including 980 members in Europe. The results of the IT Risk/Reward Barometer show slowly growing acceptance of BYOD in the workplace. In Europe 28% of organizations freely allowed personal mobile devices for

work, in North America 34%, Africa 38% and Oceania 48%. There was a 20-percent-point drop in enterprises that prohibit BYOD down from 58% to 38%, in Europe. The survey also revealed that enterprises will lose on average 12,000 euros in productivity due to an employee shopping online during work hours in November and December, according to nearly quarter of those surveyed. A quarter also believes that employees will spend more than a full work day shopping online during work hours using personal computer or smartphone. (ISACA, 2012.)

According to ISACA's 2012 IT Risk/Reward barometer, Globally in Europe, Africa, Canada, North and Latin America, India and Australia and New Zealand, top three security controls were found to be needed in every organization:

- A password management system
- Remote wipe capability
- Encryption

They all share another similarity: enterprises still do not have a security policy in place for BYOD. It seems that BYOD has generalized more rapidly among users than administrative operations and it has been dismantled somewhat uncontrolled in the organizations. Bureaucracy like policy changes and approvals cannot take too much time since BYOD may spread uncontrolled in the organization meanwhile. This would introduce potentially great risks to the organization, since it is most likely unaware of the situation. The following employee activities were seen to pose a particularly high risk to the enterprise:

- Storing work passwords on a personal device
- Losing work-supplied computer or a smart phone
- Using an online file-sharing service for work documents
- Downloading personal files onto a work-supplied device

When in Europe and Africa BYOD was cautiously accepted, Canadians were more allowing despite the concerns of BYOD related risks. In Latin American BYOD was seen increasingly risky and the Indians were remained wary, since almost half of the enterprises prohibit BYOD. Australia and New Zealand, on the other hand, have growing acceptance of BYOD. (ISACA, 2012). Online shopping was predicted to increase in the future and especially in the holiday seasons. Online shopping was seen to increase IT risks in every continent. (ISACA, 2010, 2011.) There are similarities in every continent concerning BYOD and its risks. Therefore it is possible to implement solutions, technologies and policies to adapt BYOD usage, even in multi-cultural, global enterprises. Local exceptions may need to be done in order to support global policies and standards inside the company. Reasons can be legislations, size or location of the branch offices, criticality or sensitivity of the location or the local know-how (or absence of it) that plays a significant role in the wholeness. Handling of security incidents must be managed rapidly and effectively, since IT security threats tends to transform towards Advanced Targeted Threats which are harder to detect.

A survey made by ISACA of APT (Advanced Persistent Threat) Awareness Study at 2012 from 1,551 individuals results that 87.3% of respondents think that BYOD combining with rooting or jailbreaking makes a successful APT attack more likely. It also reveals that antivirus, anti-malware and traditional network perimeter are the most used technologies to thwart APTs, instead of many defensive approaches. Also, 53.4% of respondents believe that APTs do not differ from traditional threats and one in five enterprises have experienced an APT attack. (ISACA, 2012.) If there is no understanding in the companies, how APTs differ from traditional threats, then it explains why no additional actions have not been taken into account and why companies stick to the traditional countermeasures – and usually fail to detect or prevent APTs.

It is clear that young generation adapts new technology more naturally and effectively because they have already adopted new technology at the very early stage. In addition, more institutes and schools are leveraging BYODT or similar technologies.

Thus, supporting BYODT kind of technologies could be a far-reaching investment for corporates, since new generation will already be familiar with new technology when entering the work life, while the older generation will be minority. Since the new generation interacts with social media and new technology in their daily life, it could be a good strategy for companies with low middle age to start shifting towards BYOD. It has been seen that office hours and outside office hours are not so precise anymore depending somewhat on the job description. Work can be done at a different time of the day or night or even in one's personal time, regardless of the office location or need to be physically in the office. So, there may be benefits to mix personal and business time by leveraging BYODT. Even personnel would spend time on work hours with personal issues, like shopping online they would probably work equally or more outside working hours. These kinds of individuals will likely gain the most out of BYODT.

It is hard to make comprehensive and somewhat accurate estimation of BYOD ROIs, productivities or intangible costs, because there are just so many uncertainties and pieces of expenses which all effects to the total cost of BYOD, such as roaming costs, domestic data and voice costs. Globally increasing traffic amount drives telecom carriers to upgrade their infrastructure which will eventually increase data costs for end users and companies. If the company pays, reimburses or owns the end user's voice and data interface, the Subscriber Identity Module (SIM) card, this will be a considerable part of the mobile costs for a company. Security controls and threat counter-measures for the end user device, communication path and the gateways needs to be planned for BYOD, including logging, monitoring, capacity planning and AAA (Authentication, Authorization and Accounting). If the existing remote access method company is currently using, does not provide sufficient capabilities, then these will cause costs in terms of increased license costs and possible hardware and support costs. Then, there is human factors concerning personnel, and how will they choose to adapt BYOD in real-life and is it implemented correctly, is it still usable in the user's point of view and can they access applications they need today and in the near future? And if they can, are they developed for touch screen and smartphone use.

BYODT is not so different if compared to partners, support or 3rd party remote access to corporate resources. Companies have typically implemented VPN solution, SSL-VPN access or Citrix solution for a partner's remote connection. Whichever solution is used, it is most likely the same solution as the company's own remote users have. Partners have always had their own workstations for remote access and only in rare cases a company provides them a company workstation. This is a BYOD model, since partners have total control of their own devices and a company can only authenticate the 3rd party users and limit their network access and of course log and monitor their actions. Partners have their own policies to follow in addition to other company policies, remote agreements, NDAs and contracts with other companies. These contractual procedures in administrative level have been the only possible controlling method, since device control in operational level is the responsibility of the partner.

2.5 NGFW Surveys

Using only traditional FWs in the border of the network has not been sufficient for at least ten years anymore. AV has also been seen inefficient to detect new malware and variants not only because of encryption, polymorphism and metamorphism behavior of viruses, but also the exponentially rising speed of new variants (Rissanen, 2012). Functionalities provided by NGFW solutions have been implemented more and more, to address these kinds of threats that traditional FW cannot detect (Osterman Research, 2013). Osterman Research conducted a survey for 209 organizations, 106 from United States and Canada and 103 from EU (UK, France and Germany). Survey was about NGFW management adoption and practices in medium- to large-size organizations in different industries. 19% of North American companies and 17% European reported that majority of their FWs are NGFWs and during the next 12 month 44% US' and 47% EUs responded expect the majority of their infrastructures to be NGFWs. The primary reasons were to improve their protection

against complex threats, limit access to internal and external applications, and improve network performance, see Figure 1.

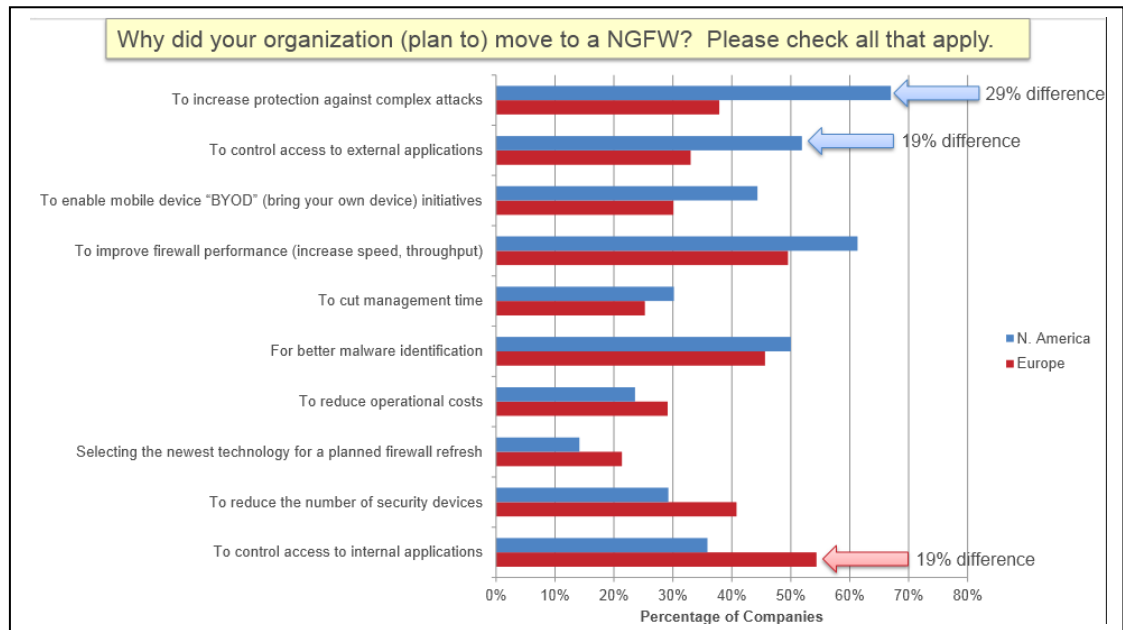


FIGURE 1. Reasons to move from traditional FW to NGFW (Osterman Research, 2012, 5)

93% of the organizations use/plan to use IPS module of their NGFW and 62% in active prevention mode. The key functionalities used or anticipated by organizations adopting NGFW are illustrated in Figure 2. Standard firewall capabilities will remain after migration because of backward compatibility, but their existence will be minority after migration, since more and more enhanced functionalities, like application identification, IPS, user group mappings and content and threat prevention capabilities will be used to replace traditional capabilities.

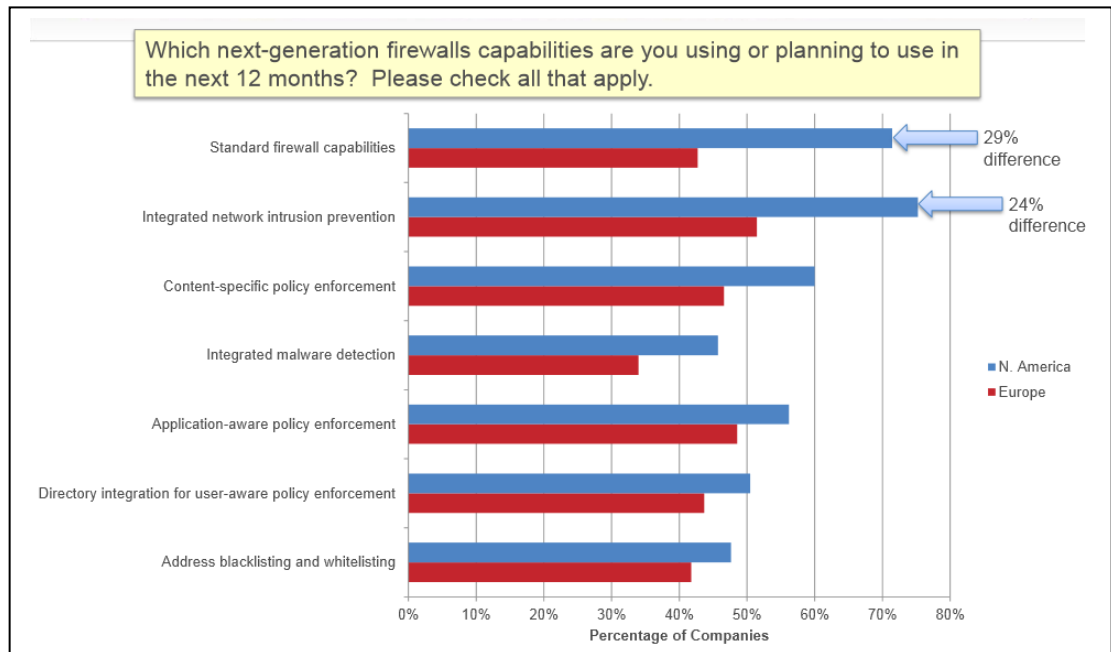


FIGURE 2. NGFW capabilities adopted or anticipated by companies (Osterman Research, 2012, 8)

Migration from traditional FW to NGFW is a big step because of enhanced features that will replace the traditional method and that will apply to the production controls of the traffic. For example, traditionally allowing HTTP would allow almost every single application that used TCP port 80. In NGFW with application identification, the company needs to know what application will be allowed through 80 or regardless of the port, as long as it is HTTP traffic. Thus, after implementation there are dozens of applications that needs to be permitted in order to get them replaced if compared to the traditional method. For example, Adobe has 11 different application characteristics. “adobe-connect” will permit all the three characteristics of adobe connect application and allowing only “adobe-meeting” would allow only adobe-meeting functionalities, without any file transfer or remote control functionality, see Figure 3.

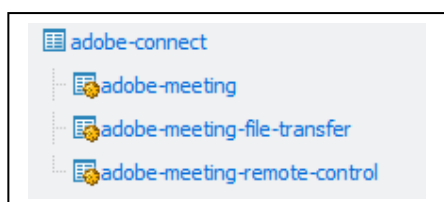


FIGURE 3. Application identification characteristics for Adobe Connect

Other similar applications using HTTP are numerous such as, dropbox, google’s applications and features, FTP, facebook, twitter, webex etc. All of these NFGW capabilities (including application identification) can be seen in Figure 4 with the following characteristics:

- Validating the correct operation of next-gen firewalls
- Planning the architecture changes to minimize impact on operations
- Creating new, more granular policies based on applications, users, content types
- Converting traditional firewall configurations to the new NGFW configurations
- Changing processes related to auditing, change management, reporting

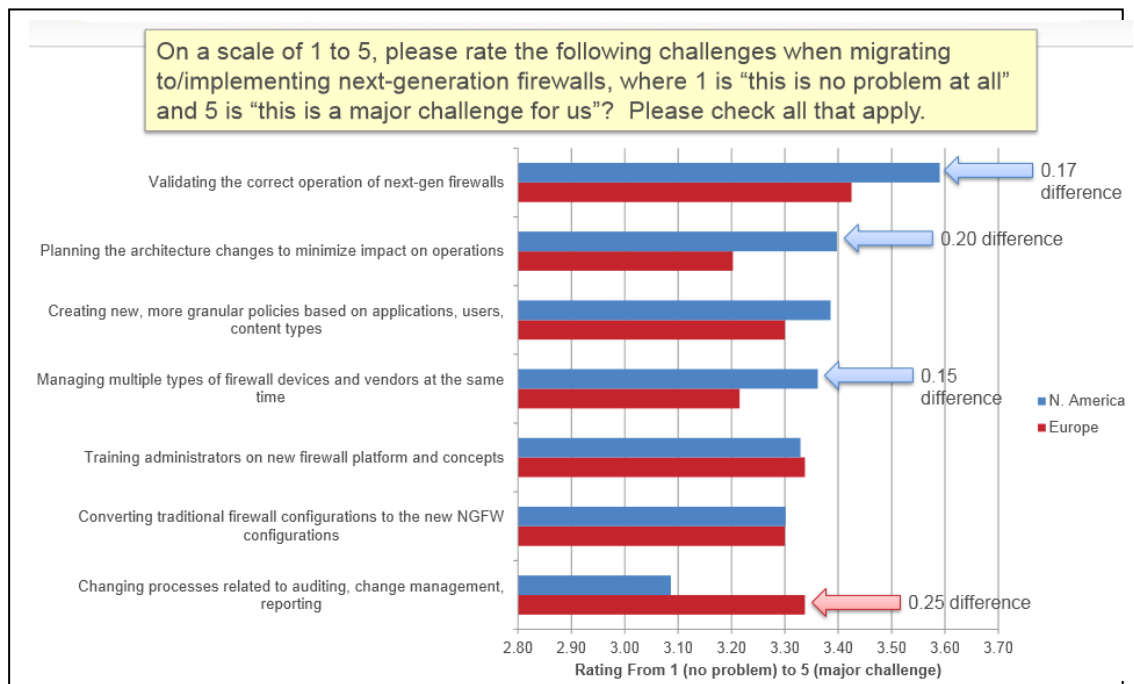


FIGURE 4. Migration characteristics to consider when migrating to NGFW (Osterman Research, 2012, 10)

After migration, the management of the NGFW is somewhat similar to traditional FW, however the control methods will be different from the traditional ones. Figure

5 illustrates the distribution of the top three challenges in on-going management of NGFW. In Europe NGFWs are more used to control an internal application than in North America (Figure 1). North America uses traditional FW simultaneously with NGFW more than in Europe (Figure 5) and also for troubleshooting time is spent more than Europe. Troubleshooting connectivity issues seem to be less challenging in Europe than in North America, while training administrators on a new firewall platform and concepts are ranked as almost similar challenges in Europe and North America (Figure 4). The survey also summarizes, that in Europe FW changes per month are twice more than in North American organizations, 273 vs. 123. All of this could indicate that in Europe, there are more trained and educated IT personnel than in North America.

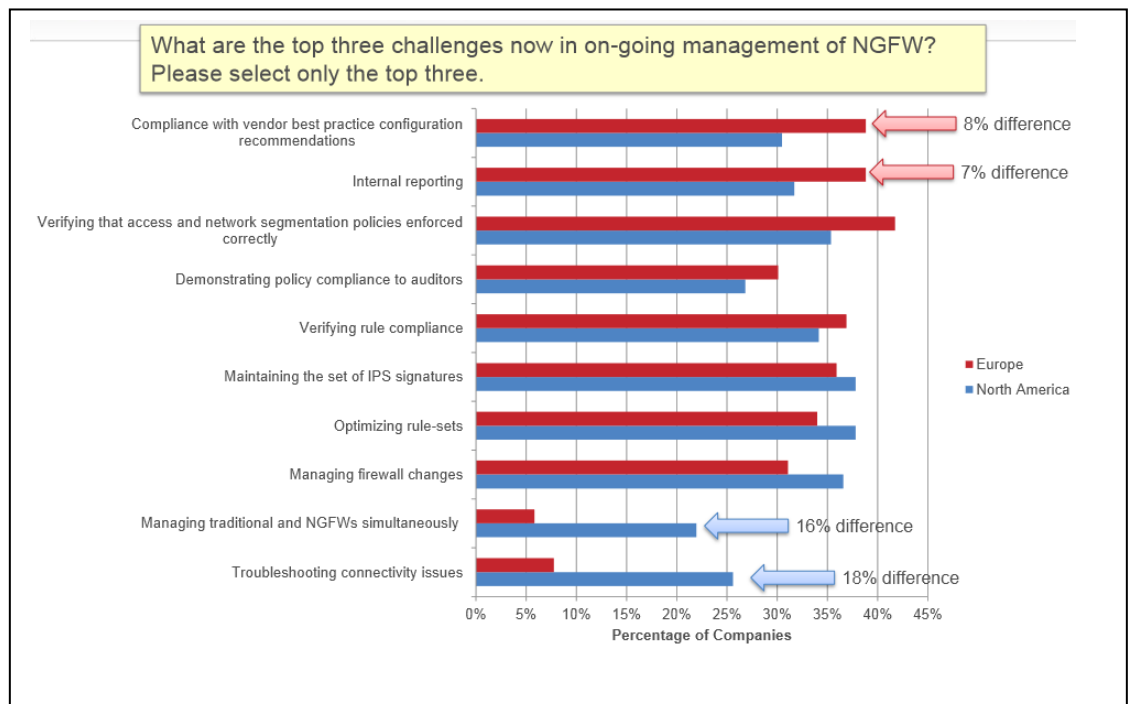


FIGURE 5. Top three challenges in on-going management of NGFW (Osterman Research, 2012, 12)

3,056 Enterprises worldwide have used Palo Alto's NGFW during May 2012 and December 2012 and an Application Usage and Risk Report have been generated from that data by Palo Alto Networks (Palo Alto Networks, 2013). The data included 12.6 petabytes of data, 1,395 applications with 5,300 unique critical, high and medium

severity threats. No survey was made, only raw data was collected from live traffic.

Key findings were as follows:

- Applications that are commonly viewed as top threats are not. That is because 339 social networking, video and filesharing applications represent 20% of the bandwidth; however, displayed only 0.4% of the threat log. Exploits were commonly detected in social networking by ratio of 49:1 and Facebook's 3rd party applications and widgets were 228 times greater in number than other social media applications. FTP and WebDAV represented the highest number of filesharing threat (mostly exploits) logs and were the 4th and 6th most heavily used filesharing application.
- Out of 1,395 applications found, only 10 were responsible for 97% of all exploit logs observed and out of 10 applications, 9 are internal applications and represented 82% of the exploit logs. Exploits focused on the internal applications, like database, active directory, RPC etc.
- Malware relies on custom applications, since custom or unknown UDP traffic represented 55% of all malware traffic and was the number one type of traffic associated with the malware communication (Figure 6). Leading malware families continue to customize their command-and-control traffic; however, in contrast, exploits were only a small percentage of custom/unknown traffic.
- Encrypted traffic, SSL, represented 5% of all bandwidth and the 6th highest volume of malware logs within known applications. It was used primarily on command-and-control traffic. Total application count that used SSL in some way was 356 and 85 out of them did not use standard SSL ports, instead most of them used port hopping, the second most TCP/80 (for HTTP) and 3rd other ports than default, TCP/443. HTTP proxy was the 7th highest volume of malware logs.

Unknown or custom traffic exists in every organization, typically in range of 8-10% of all traffic. It can be an internally developed application, a not yet identified commercial application or a threat. It presents a low volume of traffic but high volume of risk. It is significant for enterprises for determining and then managing a small volume but high risk traffic for controlling threats. This is because attackers and their malware will usually customize existing applications and protocols to fit the attacker's needs. While unknown/custom-UDP and TCP traffic is the largest part of malware logs, malware also masks itself to more traditional paths, such as DNS, IRC, SSL and Web-Proxies. Custom traffic was observed in use in variety of very popular malware families including: Zero Access Botnet, Conficker, The Poison Ivy RAT and the IMDDOS denial of Service Botnet. Web-Browsing, DNS and SSL were the top three, which have both the most frequency of use and volume with the highest concentration of malware logs. And when viewed in tandem with malware data they are found commonly and can utilize any port. (Palo Alto Networks, 2013, 3-5, 11, 13-14.)

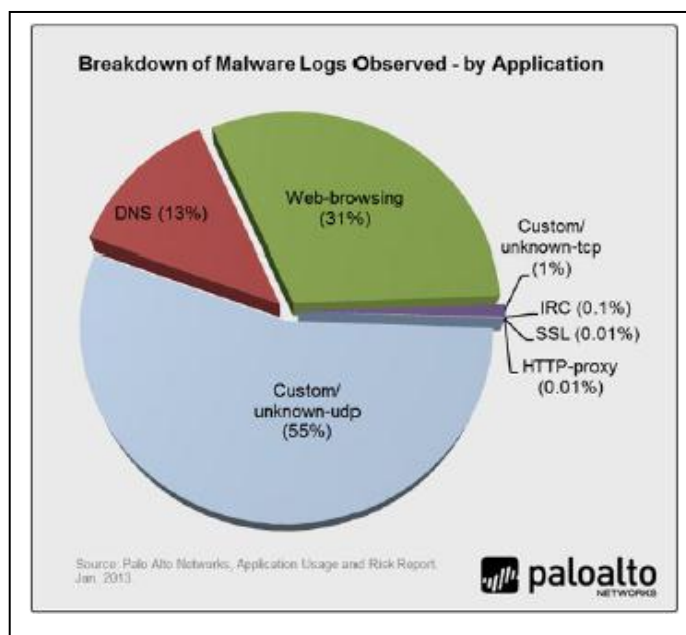


FIGURE 6. Applications with the highest concentration of malware logs (Palo Alto Networks, 2013, 13)

Exploits in custom traffic were a small percentage, but 83% of them were classified as critical and the remaining 17% as either high or medium. Critical exploits are the most dangerous ones, since they can take near total control of the system by infecting the target with malware as part of ongoing persistent attack. The majority of the exploits used in custom traffic was targeting IIS web-servers, SQL databases or were used in cross-site scripting attacks. (Palo Alto Networks, 2013, 14-15.)

Most of the vulnerabilities of internal applications (97%) were found only by 10 applications out of 1,395. And 9 out of these 10 applications are considered as internal applications or infrastructure applications that internal applications are highly dependent on and they are all high-value assets. This indicates that critical resources attacked from inside the network continue to be the rule of the attacking strategy and not the exception. Therefore, enterprises need to monitor the internal networks for threats in addition to perimeter security and monitoring, see Figure 7. (Palo Alto Networks, 2013, 11.)

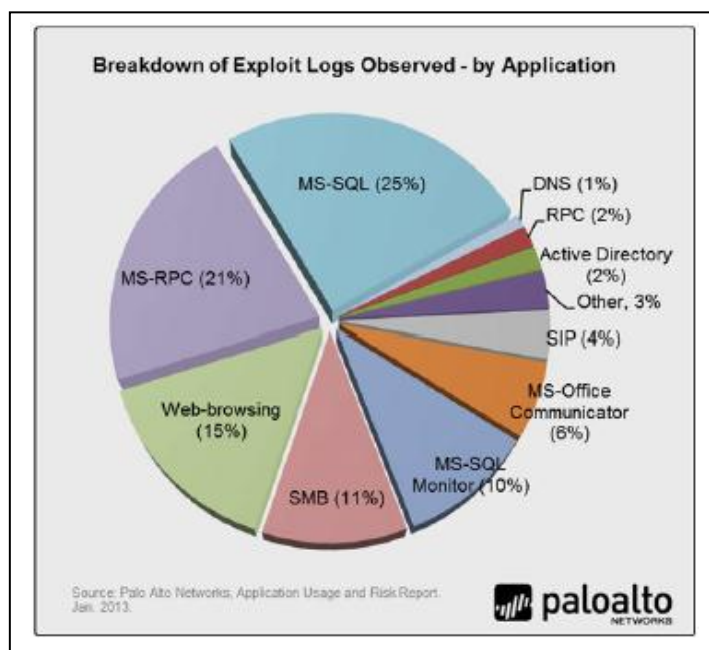


FIGURE 7. Top 10 applications based on criticality (Palo Alto Networks, 2013, 11)

A summary of the report can be seen as a figure in the Appendix 1.

Palo Alto Networks analyzed more than 1,000 real-world enterprise networks for 3 months. The focus was on 26,000 malware samples that were completely undetected by 6 fully updated enterprise AV products at the time they were found in the customer networks. Key findings were:

- 94% of unknown malware was delivered via web browsing or proxies
- It took 20 days for traditional AV to deliver coverage for malware for web and 5 days for email.

The analysis showed that 70% of unknown malware had indicators in the payload or traffic that can be used to improve protections. The indicators were as follows:

- 40% of malware can be blocked with payload-based signatures, if delivered in time
- 30% of malware generates unknown traffic, which can be blocked, if unknown traffic is blocked
- 30% of malware traffic can be blocked, if concerned files or traffic to or from fast-flux domains or newly registered domains or DNS servers

The most common technique to avoid end-point security was for the malware to sleep a long period of time to avoid analysis. More sophisticated behavior focused on disabling security measures and internal checks within the operating systems. (Palo Alto Networks, 2013b.)

By replacing traditional technology solutions, like IDS/IPS, Proxy + ICAP integrated AV and URL Filtering solution and VPN GW/SSL-VPN to one NGFW solution, potential benefits are numerous. Many of them are intangible like reduced license costs, support costs and less hidden dependencies between security devices, smaller latencies and better performances without capacity or resource bottlenecks. The outcome can be less troubles and problems and less time is spent trouble-shooting and therefore more time is available to the efficient working. There are also significant advantages

in administration tasks, like simplified network topology and lesser devices to administer, backup and configuring tasks. Also, more security features and controls can be used in almost any kind of combination to gain more advanced control over the traffic with wider security monitoring in a single system. Gaining knowledge of the content of the internal network's data in addition to perimeter data is utmost important. Comprehensive monitoring includes applications usage combined with threats and risks monitoring. (Laine, 2012.)

3 THEORY OF REPLACING THE SERVICES

3.1 Traditional way of doing Remote Access

Figure 8 illustrates a typical medium- and large sized IT infrastructure in the border of the network. Black arrows illustrate the flow of events and logs generated by the device or administrator. Client location varies between the LAN and the internet. Traditionally, VPN technology is used when client location is on the internet and it is common also that VPN connection is established by the user. Then, during VPN connection attempt, authentication occurs by challenging the user a userid and password request and then possible two-factor authentication follows. Userid with password and/or two-factor authentication combination can be also replaced by a smart card or certificates, but the userid and password combination is the most used method, because it is the simplest and cheapest one to use – and the most insecure, if used alone. After successful authentication, the connection is established and job-related work can start. If there is any personal-related work that the user would like to do, then the company policy will define what can be done and what is prohibited.

Usually, when a VPN connection is terminated, the internet access is useless for personal work, since the corporate security settings prevents any other connections, except VPN connection to the company's VPN gateway. Therefore personal computer based usage is separated from company issued computers to the personal computers. Remote access built solely with traditional technology holds one significant challenge that should be addressed. Once the user or partner establishes a remote access connection and connects to a remote server to the company's internal or DMZ network, security measures should be in place to prevent leapfrogging from server to server. This is a challenge with traditional technology, since application identification and user identification in different servers through remote access connection are not achieved easily. It is challenging to identify different sessions generated by the same user from different client and servers because user identification information is not

transferred within different sessions and protocols. Therefore, traditional network technology cannot address this problem easily, because it cannot differentiate users' sessions from each other if they are coming from the same server, for example. User identification is essential, since a policy can be tied to the user's identity and usually requirements are quite the same for the user regardless of the access method, location or even the device. The traditional method has never had to address external MDM (Mobile Device Management) solution, since end devices have always been under corporate IT department and support has been provided by IT support systems already in place, like Microsoft Windows Server Update Services (WSUS), System Center Configuration Manager (SCCM), remote desktop software (like Netop or DameWare) or some other 3rd party product.

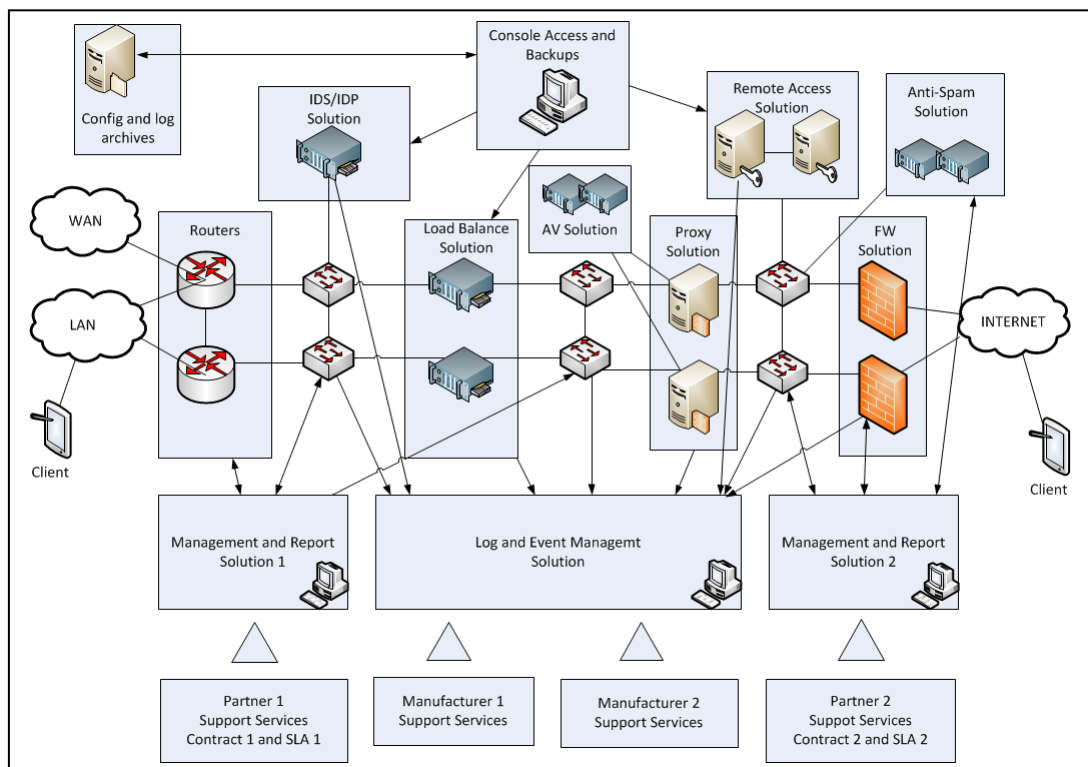


FIGURE 8. High-level design of traditional perimeter network

3.2 Traditional way of doing BYOD

Introducing BYOD into traditional kind of network infrastructure will cause IT department to face real challenges, since the traditional model does not support BYOD in any way. If there is no real application identification, user identification and end-device identification in place, then there is a missing control in place. For partner's remote connection BYOD has been working because of limited number of partners, limited connections needs and some additional contractual procedures. But still there are caveats, such as preventing effectively leapfrogging in a technical way can even prohibited in contracts. Using traditional control methods to BYOD environment limits the controlling BYOD. Since there are many ways to use BYOD and traditional control methods are limited, based only on port or protocol restrictions and user authentication, a comprehensive BYOD environment may not be achieved with this combination. Even MDM does not help much, since it only controls device settings, however it does not control traffic.

3.3 Remote Access and BYOD with NGFW

Figure 9 illustrates a traditional network perimeter with red circles and dotted line red circles. Red circles illustrate services and devices that can be completely replaced by NGFW and dotted line circles illustrates partially or completely replaced services, depending on the company's current setting.

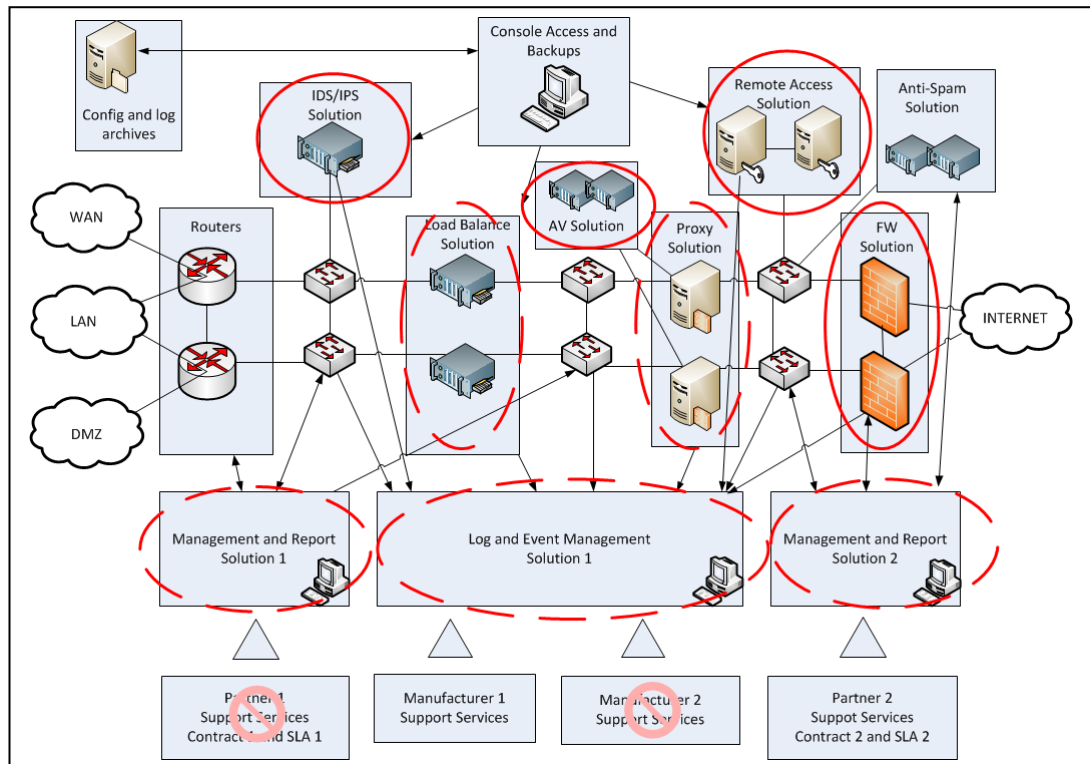


FIGURE 9. Overlapping services and devices between traditional FW and NGFW

IDS/IPS systems can be replaced completely depending on how complex these rules are. For IDS and not too complex IPS configuration, both can be completely replaced with NGFW. Since NGFW and IDS/IPS are a bit different technology they are not 100% comparable, but the same features are found in both devices. Load balancers cannot be replaced at all, since NGFW does not include load balancer. However, if load balancers are for network perimeter devices only, and network devices are completely replaced, they are left unused and can be therefore terminated. If they are used for servers or other services in addition to network perimeter devices, they cannot be completely replaced, but instead moved to another zone, perhaps closer to the servers.

Proxies are used for user authentication, group mapping, content filtering, AV integration, logging and alerting, caching the content, restricting access, content rewriting, SSL decryption and encryption and similar purposes. The only feature that cannot be replaced in proxy server is cache service. Since internet has become more and

more dynamic, encrypted and password-protected, the significance of a cache has become less important, since proxy server cannot cache those features. Thus, in many cases proxy server including AV integration can be completely replaced. NGFW will completely replace traditional FW and remote access services run by VPN Client or VPN LAN2LAN solution, or any other IPsec functionality. If remote access has been implemented using SSL-VPN solution, it cannot be replaced. SSL-VPN offers features for HTTP and HTTPS services and some authentication features for browsers, but these can be replaced with application identification and user identification in NGFW. A company should balance benefits and costs between SSL-VPN versus VPN with NGFW to avoid double costs for similar services in the environment.

After implementation, high-level design can be seen as illustrated in Figure 10. Using the functionalities in NGFW will enable more advanced control of the traffic, based on application or application filters, user or user groups, time and date or recurring time or date, threat or content, HIP (Host Information Profile) and it also controls BYOD technologies in addition to traditional technologies.

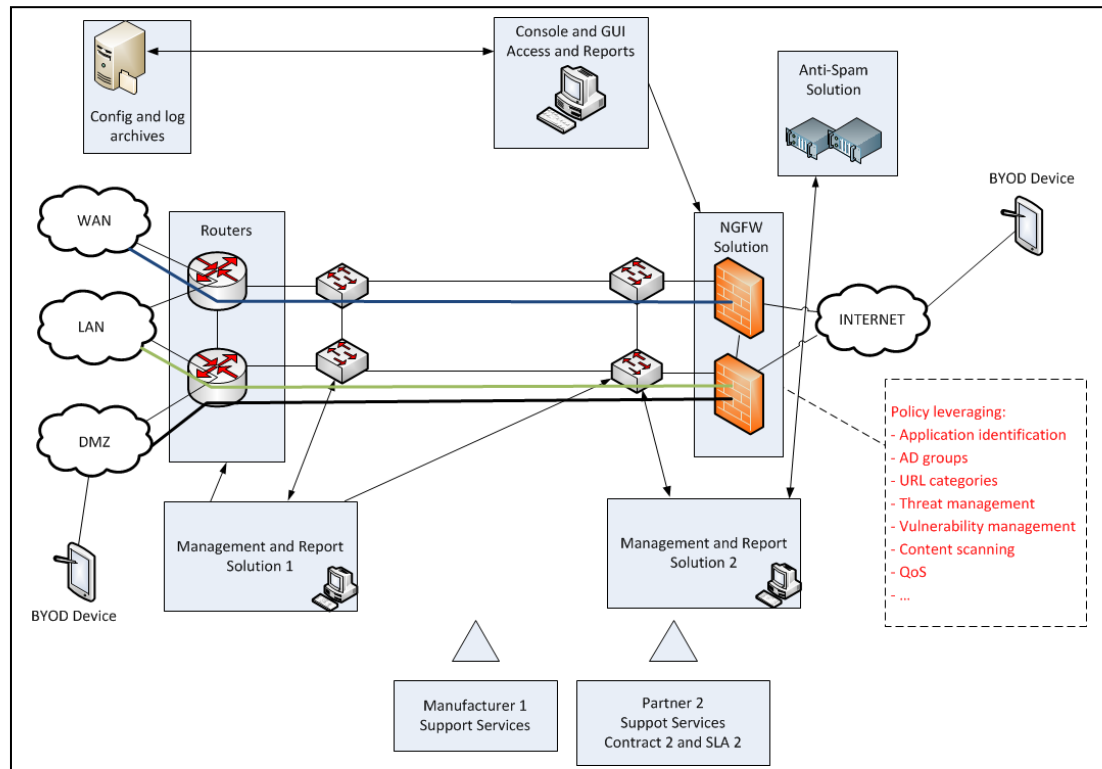


FIGURE 10. Traditional FW solution replaced by NGFW solution

Replacing FW with NGFW introduces also some application installations. There are so called User-ID Agent and Terminal Services Agent. User-ID Agent functionalities can also be carried out with the firewall itself, which polls for AD (active directory)'s DC (domain controller)'s security logs to notice any user authentications in the AD environment. This information is then replicated to the NGFW, which now knows the User's IP address, userid and AD group memberships. This information can be used in the security policies. Terminal Services Agent does the same for MS Terminal Services and Citrix Metaframe Presentations Servers. When there are multiple users logged in, it distinguishes the user's sessions each other. This information is also replicated to the NGFW and used in the security policies. This is an effective technical countermeasure against leapfrogging. Similar User-ID functionalities can be done to MS Exchange environment to once again to feed the information to NGFW. This is effortless solution to identify users that cannot be found anywhere in the domain, such as users using personal devices to access corporate email system directly from the internet.

As soon as NGFW has been installed, the WildFire functionality should be enabled to compare the defined traffic between company and the internet with wildfire to gain extra security and to get the latest updates from the WildFire. This can be as fast as with 15 minutes interval, if using WildFire license. Without a license WildFire is still available, but updates are pushed from the Palo Alto network approximately once a day. WildFire license includes a capability to feed information to the WildFire Cloud Services from different servers/services, like company mail gateways, to the wildfire. This feature leverages xml API (Application Programming Interface) in the NGFW. The server/service sends the hash of the file to the Wildfire and if the hash has been seen before by the WildFire, then the information is already known and replicated back to the NGFW. If it has not been seen, then the file is sent to the WildFire to get the feedback of its behavior, whether benign or malware. Then, the update is available not only to the company itself, but all the other customers as well. This way, the

“WildFire community” protects itself by sharing the protection information to gain extra security.

3.4 Architectural Differences between Traditional FWs and NGFWs

Traditional FireWall technology was implemented more than 20 years ago. It has evolved from packet filtering to stateful Inspection FireWall and today they include Content Inspection Capabilities, such as IDS/IPS features, signatures for malicious traffic behavior and viruses. The functionalities have evolved during the years, but the most important feature has not; the architecture.

The traditional FireWall architecture consists of the hardware components and the core software inside the Central Processing Unit (CPU). The only change in the platform is that the server hardware has changed to higher performance hardware and some of them with efficient Application Specific Integrated Circuit (ASIC) circuits. When the processing is done with the hardware, it is always more efficient than by software with the CPU. However, the industry standard and general-purpose processors are not sufficient anymore, which affects the processing capacity negatively, because they cannot process the traffic more than a small minority of packets traversing the device at a time (Metzler, 2007, 1-2).

The traditional FireWalls are based on stateful inspection, which means that they identify traffic based on the state of the connection. The attributes that form the state of the session includes source and destination port, protocol, source and destination IP addresses and the sequence numbers. The most CPU-intensive task is the start of the session and traditional FireWalls identify and classify the traffic by the start of the session information including the port and protocol information, not by inspecting the content of the packets (Metzler, 2007, 1). The less-intensive task for CPU is to check whether a packet belongs to an existing session or not. After the session is initialized by the CPU, the session is established and the rest of the packets of

the same session will be processed with hardware and only minimum need of the CPU's time is needed.

Because all of the Content Inspection Capabilities that requires deep packet inspection are done in the CPU, the overall performance collapses when the traffic increases, since more content are inspected. This is the reason why all the traditional FireWalls struggles to process CPU-intensive traffic with deep packet inspection turned on, with any accuracy of guaranteed performance. It also affects to all of the remaining traffic, because the degradation in performance causes delays to all traffic traversing through the FireWall, not just the content inspected traffic. VoIP is one example of latency-critical application that suffers if network latency is varying too much.

This CPU processing problem has been tried to circumvent by creating a specialized blades or dedicated expansion modules for existing hardware to provide CPU intensive tasks with additional CPU processing unit. It may be temporary solution, but only postpone the inevitable: traditional technology will need to redevelop in order to manage the continually growing traffic amounts and to detect and prevent advanced threats in the traffic. In order to address both, the architecture needs to be different to face the traffic amounts and the internal logic needs to be redeveloped to detect the behavior of the traffic and address application and threats accordingly. The traditional way of inspecting the start of the session information only, is not sufficient anymore. It takes more than just the initialization phase to correctly identify the application, since application can change the port ranges or do other range of functions over a single connection (Metzler, 2007, 2).

This architectural problem lead to the situation where the whole implementation and architecture needed to redesigned in order to achieve real performance improvements. This means special-purpose programmable hardware in the platform and identifying correctly the application traversing the firewall, which both have a big role in the architecture. They also need to have ability to create custom applications, track port-hopping and dynamic ports and look over the IP header information

into the payload of the packet to look for identifiers (Metzler, 2007, 4). They also need to perform SSL decryption/re-encryption, segregate application functionalities (e.g. facebook-apps, facebook-chat, webex-chat, webex-file-sharing etc.), identify users and tie events and traffic to them and create reports and alerts – all of this at multigigabit throughput (Metzler, 2007, 4). In addition, it cannot be too complex for inputting a rule set or analyzing it for a HelpDesk level analyst (Metzler, 2007, 4).

The advantage of application identification is that it prevents forged applications to traverse through the NGFW, but also unnecessary load of IPS module, since only allowed and correctly behaved applications are passed to the IPS module, instead of all traffic. In addition to application identification, if the architecture is also built on layer 7 in the Open System Interconnect (OSI) model, then the result is more powerful than layer 4-based architecture. The application layer is in layer 7 in OSI model and stateful inspection features are in layer 4. If the architecture relies on layer 4 and has added features (modules) for layer 7, the combined results usually show in poor performance and visibility (Palo Alto, 2010, 11).

Table 1 summarizes the features between Palo Alto Networks architecture and traditional FW architecture.

TABLE 1. Differences between Palo Alto Networks and UTM or IPS-based products
(Palo Alto, 2010b, 4)

	Palo Alto Networks	UTM (FW + IPS)	Impact
Primary traffic classification mechanism	App-ID™: the application identity is determined irrespective of the port, protocol, or SSL encryption.	Stateful inspection: by port and network protocol. Application protocol is (often wrongly) assumed	UTM: Applications adhere to neither port nor protocol associations. Classification by port is ineffective, offers no visibility and poor control. Palo Alto Networks: App-ID™ enables comprehensive visibility and fine-grained control.
Primary security policy element	The application's identity.	Port numbers and protocols believed to be associated with specific traffic.	UTM: Allow port 80, block port 5605. Effectively, this policy blocks nothing because ports can no longer enable appropriate levels of control. Palo Alto Networks: The actual identity of the application is used in policy: e.g., allow Gmail, block BitTorrent and UltraSurf.
Application identity visibility	Complete picture of all application traffic is displayed graphically; used as primary policy element; viewed in logging and reporting.	Limited to IPS log filtering and reporting.	UTM: Log viewing is an "after the fact exercise" providing data too late. The data is incomplete, because it only reflects the applications expressly searched for. Palo Alto Networks: The application identity – what it does, how it works, and who is using it – is the primary policy element.
Application control model	Positive control: allow only what has been configured, block all else – ideal for enabling secure use.	Negative control: Block what has been configured, allow all else – cumbersome to enable secure use.	UTM: Coarse-grained model forces IT admins to say "No" too often. Palo Alto Networks: Employees are given more application freedom, with IT ensuring "safe enablement" to improve the company bottom line while protecting the network.
Enterprise directory services integration	Displayed graphically; as a policy element; in logging and reporting.	Integration is for authentication purposes only; or it is limited to secondary policy element.	UTM: Using IP addresses in lieu of users and groups makes positive control of applications nearly impossible. Palo Alto Networks: Able to enable applications is based on users and groups in addition to, or regardless of, IP address.
Visibility and control of SSL traffic (inbound and outbound)	Yes.	No.	UTM: Typically, all SSL traffic is uncontrolled, un-scanned, and invisible to traditional security infrastructure – and IT administrators. Palo Alto Networks: Incorporates policy-based decryption and inspection of SSL traffic (both inbound and outbound), ensuring total visibility.

Single pass architecture means a common decoder protocol engine for scanning all traffic. Decoding engine pick apart application stream to separate different pieces of the application; start and stop of the file, posting data versus downloading data and were a command is executed. Scanning engine uses this information to scan the content of the files, data, threats and URLs. Since this is the most processing-intensive task, it is done only once by using single pass architecture, see Figure 11 (Palo Alto, 2008, 6).

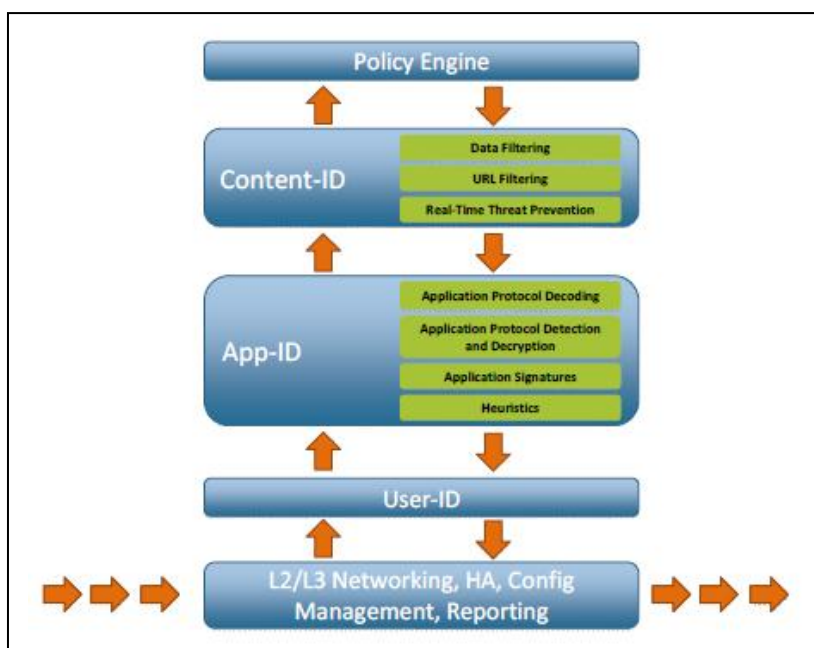


FIGURE 11. Palo Alto Networks single pass architecture (Palo Alto, 2008, 6)

Another difference between Palo Alto architecture and traditional architecture is a stream-based signature engine. This component replaces a file proxy for data, virus and spyware, a signature engine for vulnerability exploits and an HTTP decoder for URL filtering. This single component has the benefit of real-time scanning and only reassembles the small minor of packets when needed, without the need of downloading the entire file in order to scan it. And second, scanning happens only once, instead of multiple times, like traditional technology does (Palo Alto, 2008, 6).

Traditional technology processes the content multiple times, as illustrated in Figure 12 in worst case scenario, where multiple hardware and software are used to perform the same tasks that single pass architecture model does in the Palo Alto architecture. In multi-task architecture, CPU-intensive tasks, e.g. file proxies, application decoding, signature engines and policy enforcement are processed separately, which generates processing overhead, latency introduction and throughput degradation (Palo Alto, 2008, 9).

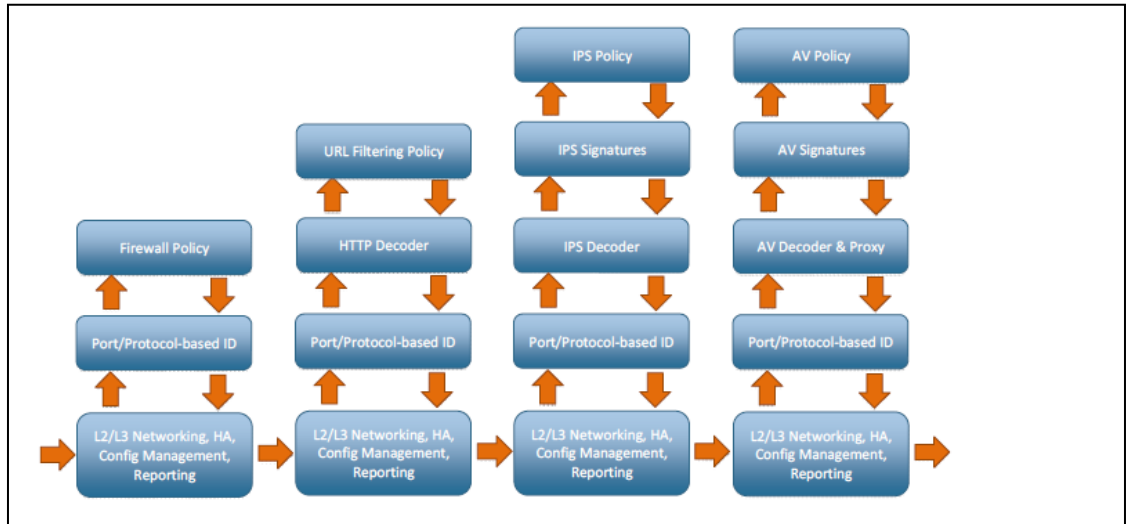


FIGURE 12. Existing solutions multi-pass architecture (Palo Alto, 2008, 9)

In multi-pass architecture, the processing is divided into different engines and content scanning features are proxying files. Therefore, the hardware acceleration is impossible to achieve. Another challenge is the architecture that does not allow to add content scanning with hardware accelerated afterwards, instead of implemented in the architecture and software into the platform (Palo Alto, 2008, 8).

Palo Alto Networks does the hardware acceleration by the platform for the following functionality blocks:

- Networking; Packet routing, flow lookup, stats counting, NAT and similar functions
- User-ID, App-ID and policy engine in multicore security processor for encryption, decryption and decompression
- Content-ID; signature lookup
- control plane; Management functionalities, logging and reporting

These blocks are illustrated in Figure 13 for data plane and control plane.

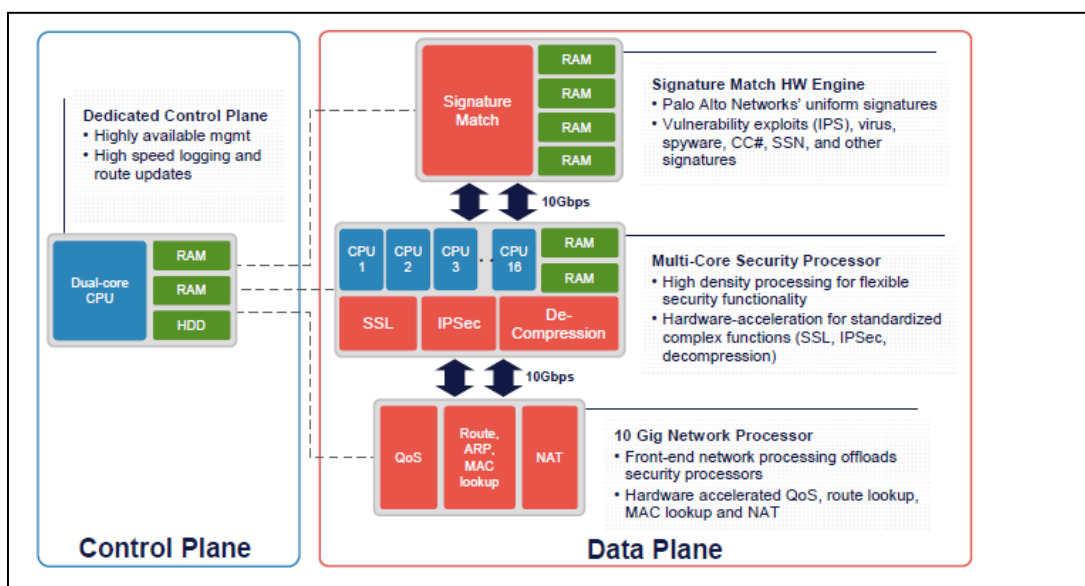


FIGURE 13. Palo Alto Networks platform architecture (Palo Alto, 2008, 8)

There are benefits and trade-offs when changing proxy-based scanning to stream-based scanning. Benefits are:

- Scalability; Stream-based scanning requires significantly less memory and processing power, because it does not need to store the entire file prior to scanning. Therefore it's more feasible for scanning large files
- Low latency; stream-based engine forwards the file as it receives it, which is the fastest way of scanning content
- Common processing; stream-based scanning can process all traffic with one processing engine, whereas file proxy cannot scan vulnerabilities and therefore requires multi-scan approach.

Trade-offs:

- Blocking viruses, spyware or data over traditional email protocols like SMTP cannot be done. Blocking infected attachments will often cause a continuous retransmission of the attachment over SMTP. In addition, it is not possible to quarantine the email message

- Compression operates only for zip and gzip formats without password protection. That is, because these are the only two compression formats that compress in blocks of data instead of the entire file as compressed blocks. However, these are the most common compression algorithms and file type scanning can be used to monitor or block from traversing certain network segments.

Benefits are more significant than trade-offs, because the outcome is guaranteed throughput with increased operational performance, even in multi-gigabit speed (Palo Alto, 2008, 8).

NSS Labs is the world's leading independent information security research and testing organization. Its expert analyses provide unbiased data for information technology professionals in companies that they need to select the right product for their companies. According to NSS Labs' Networks Intrusion Prevention Systems individual product test results for Palo Alto Networks NGFW model PA-4020 at August 2010, PA-4020 blocked 56,6% of attacks for "out-of-the-box" or default configuration and with rapid tuning that consisted of three settings in the policy by Palo Alto Networks engineer, the effectiveness improved to 93,4%. The throughput was informed as 2,000 Mbps of inspected traffic but it was verified to be 2,259 Mbps with "Real World" protocol mix traffic. It also provided an outstanding 3-year Total Cost of Ownership (TCO) including labor. 3-year TCO was calculated as \$80,450 and price per Mbps-protected was \$38. (NSS Labs, 2010, 1).

At April 2011, the same test was done again to the same model by the NSS Labs. This time the throughput was measured 5,207 Mbps, 3-year TCO was calculated \$53,825 and price per Mbps-protected was only \$10. The TCP split handshake spoofing test failed at the first test, but a software update was done and it was verified by NSS Labs to pass the test at the second time. All the other tests were successful at the first try (NSS Labs, 2011, 14). Even the test organization was the same the test methodology versions were different in both tests and the PAN-OS version was also dif-

ferent, which may explain the variation in the test results. At 2012 NSS Labs made a Next-Generation FireWall Group Tests to seven vendors, which only two earned “recommended” rating and Palo Alto’s model PA-5020 was one of them. It passed all the resistance to evasion tests with Methodology Version 4.0, except HTTP evasion, which resisted only 33% of evasion attempts (NSS Labs, 2012, 8). Table 2 illustrates the individual test results.

Table 2. Resistance to evasion (NSS Labs, 2012, 8)

Description	IP Packet Fragmentation	TCP Stream Segmentation	RPC Fragmentation	URL Obfuscation	HTML Evasion	FTP Evasion	TOTAL
Palo Alto Networks PA-5020 PAN-OS 4.0.5	100%	100%	100%	100%	33%	100%	87%

NSS Labs stated “Palo Alto Networks has acknowledged this issue and a public fix should be deployed by the time this report published” (NSS Labs, 2012, 8). The HTTP obfuscation is listed more detailed in Table 3, which shows that they are all codec (encoding) obfuscations.

Table 3. HTTP obfuscation with PA-5020 (NSS Labs, 2012, 24)

3.5.5	HTML Obfuscation	33%
3.5.5.1	UTF-16 character set encoding (big-endian)	0%
3.5.5.2	UTF-16 character set encoding (little-endian)	0%
3.5.5.3	UTF-32 character set encoding (big-endian)	0%
3.5.5.4	UTF-32 character set encoding (little-endian)	0%
3.5.5.5	UTF-7 character set encoding	0%
3.5.5.6	Chunked encoding (random chunk size)	100%
3.5.5.7	Chunked encoding (fixed chunk size)	100%
3.5.5.8	Chunked encoding (chaffing)	100%
3.5.5.9	Compression (Deflate)	100%
3.5.5.10	Compression (Gzip)	100%
3.5.5.11	Base-64 Encoding	0%
3.5.5.12	Base-64 Encoding (shifting 1 bit)	0%
3.5.5.13	Base-64 Encoding (shifting 2 bits)	0%
3.5.5.14	Base-64 Encoding (chaffing)	0%
3.5.5.15	Combination UTF-7 + Gzip	0%

The throughput for 2,000 Mbps device was measured 3,805 Mbps with inspection on, but the connection rates was considered low for a 3,8 Gbps device. However,

connection settings are set for a 2 Gbps device, where the connection rates are appropriate. (NSS Labs, 2012, “).

NSS Labs made a Next-generation Firewall Comparative Analysis at 2013 and the results were published at February 26th. The testing methodology was NSS Labs' Next-Generation FireWall Methodology version 5.2. It stated that 8 out of the 9 products scored over 90% for security effectiveness, while only half of tested vendors scored 90% in this category at 2012. The overall scores for security effectiveness in 2013 ranged from 34.2% to 98.5% compared to 18% to 98.9% in 2012. Also, only 2 of 9 products tested had throughput rates that were significantly less than their vendor's stated claims, while in 2012 5 of the 8 products tested performed well below their advertised speeds. TCO remained fairly stable. Most tested devices costs below \$44 per protected-Mbps. The overall range in 2013 was \$18 - \$124 per protected-Mbps, while in 2012 it was \$30 - \$375 (NSS Labs, 2013).

Top scores for Security Effectiveness and Overall Protection were given to Check Point by NSS Labs at 2013. Test result show that Check Point's Next-Generation FireWall solution provides the best out-of-the-box protection in the industry (Check Point, 2013, 1). See the NGFW Security Value Map in Figure 14. Out-of-the-box means default settings or minimal configuration for the device before connected into production environment. All security devices require additional configuration, when deployment is for large or mid-sized company. Most of the cases existing FireWall's configuration is transferred - to the new FireWall.

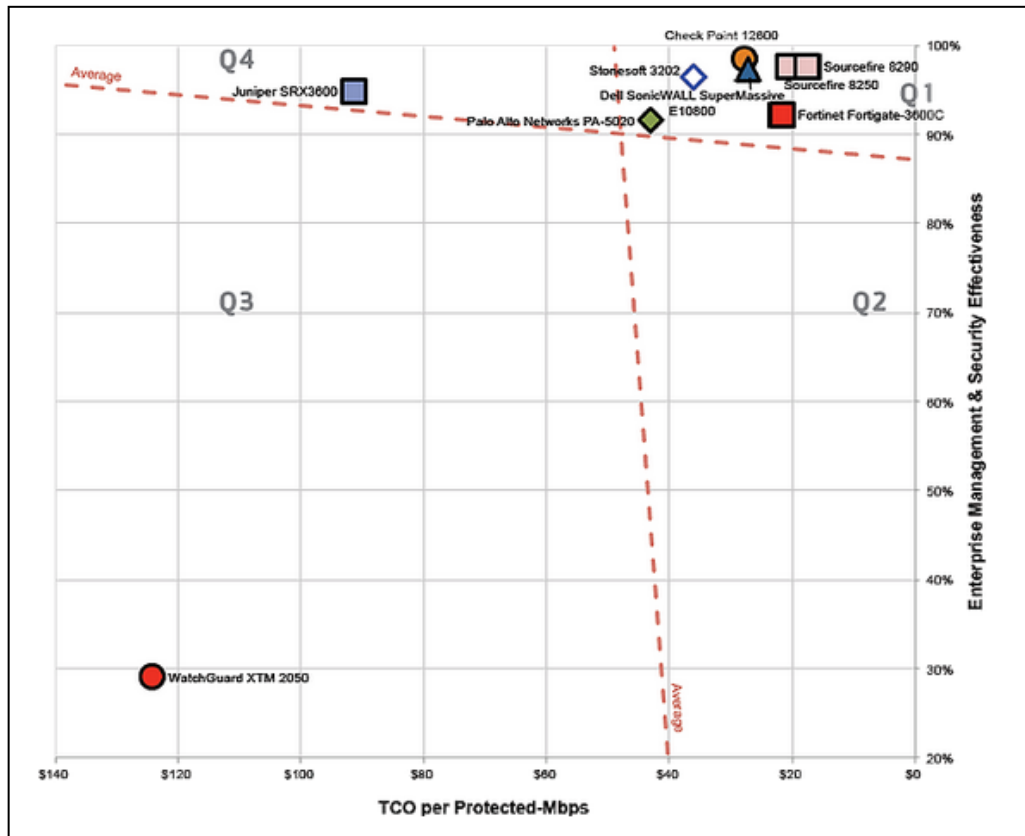


FIGURE 14. 2013 Security Value Map (Check Point, 2013, 1)

According to Security Value Map, most of the other vendors have achieved Palo Alto Networks' head start within the past year, since many of them are in the upper right corner and they are equal or even better position. The essential is to choose from the vendors in the upper right corner, whose differences are relative small. If the security is the only feature that matter, then Check Point or Sourcefire would be the best solution to choose from, since they provide the best Security Value. However, they can change places at the next test. If the benefits brought by the new architectural solution matters in addition to security, then Palo Alto would be the best solution at the small expense of security effectiveness and TCO.

While Check Point has the best Security Value Map, the architecture still matters. According to Check Points' Software Blade Architecture: Achieving the right balance between security and protection and investment:

The architecture also delivers a high level of flexibility without sacrificing performance. Security gateway performance can be guaranteed when multiple blades are deployed by enabling performance thresholds. Thresholds, set by IT personnel, control the provisioning of system resources—such as CPU cycles and system memory—to the IPS Software Blade. (Check Point, 2013, 7).

Figure 15 illustrates this functionality.

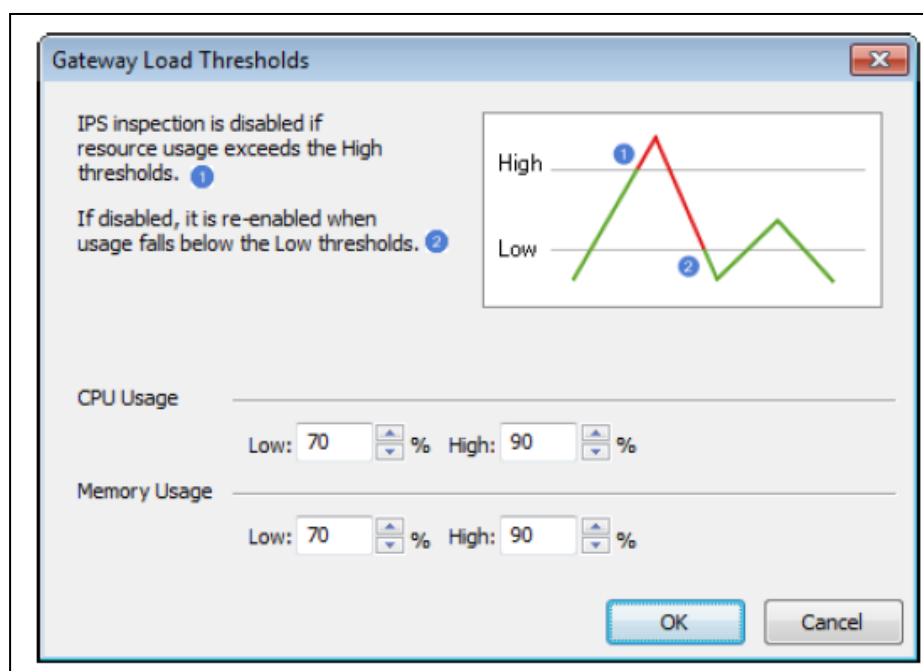


FIGURE 15. Setting usage thresholds to guarantee performance

In the higher resource load, the security gateway either suddenly will suffer performance degradation and stops handling traffic or stops inspecting the traffic until resources are at defined level again. This way, a DoS attack could be used to disable IPS feature and inject malicious traffic into the network. Another more likely example is no more than a normal heavy load in the environment, such as backup system or another bandwidth consuming application that can do the same thing and cause unnecessary risk by disabling IPS inspection. This affects the Security Value Map negatively, depending on how long the resources are overloaded. It also causes degradation in latencies and throughput by filling up Device's TCP buffers, which will end up

packet losses to all the traffic passing the device, since the traffic that cannot fit into the buffers will be discarded.

Even there are unbiased companies that test the functionalities with different kind of test methods, they provide results that are not the same as in the real-life environments. But testing the equipment in controlled environment gives the advantage to make comparative analyses between the devices in the exact same situation and in the exact same way. However, the reality is still different and they cannot be easily verified in the lab environment.

Gartner defines the NGFWs as follows:

Next-generation firewalls (NGFWs) are deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall. An NGFW should not be confused with a stand-alone network intrusion prevention system (IPS), which includes a commodity or nonenterprise firewall, or a firewall and IPS in the same appliance that are not closely integrated. (Gartner, IT Glossary).

According to Gartner's Magic Quadrant for Enterprise Network Firewalls 2013, Palo Alto Networks has a design advantage of "single pass" technology including application identification and IPS features throughout the inspection stream. Competitors, instead, have separate modules forming a serial order processing; from FireWall to IPS and then to the application control (Gartner, 2013). Figure 16 illustrates the situation of network enterprise Firewall market in 2011. Palo Alto Networks has taken the place of visionary, whereas the biggest competitor Check Point Software Technologies is the leader.

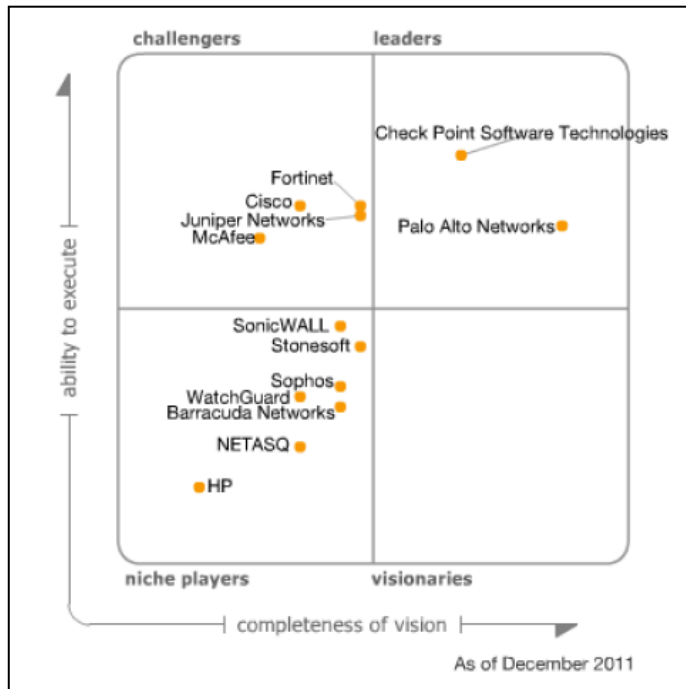


FIGURE 16. Magic Quadrant for Enterprise Network Firewalls 2011 (Gartner, 2011, 1)

When compared to the 2013 statistics, Palo Alto Networks has established its place in visionaries within only in the past few years, headed towards to the upper right corner to the leaders and visionaries. At the same time, the biggest competitor Check Point Software Technologies is still the leader but moving towards the challengers, see Figure 17.

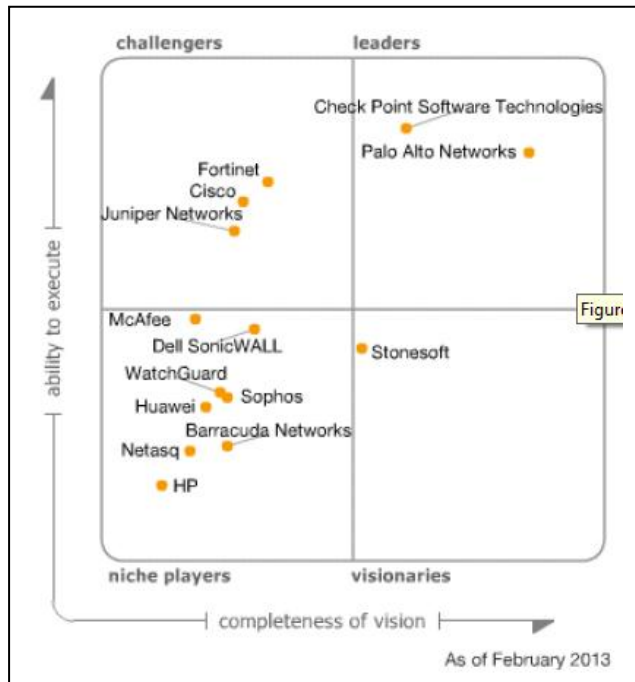


FIGURE 17. Magic Quadrant for Enterprise Network Firewalls 2013 (Gartner, 2013, 2)

Palo Alto Network represents the only vendor in the market that has completely re-designed and rebuilt its product and has also gained the strongest position in the network firewall market. All the other vendors are still built on the traditional Fire-Wall technology solutions.

3.5 MDM (Mobile Device Management)

MDM Solutions is excluded from this thesis, but it is worthwhile to mention that MDM solution is an absolute solution before starting to implement any BYOD solution. MDM can force settings to mobile devices and therefore not only facilitates, but also secures the remote access devices at implementation and change management stages as well as throughout the whole life cycle of a mobile device.

4 EMPIRICAL STUDY: TESTING THE FUNCTIONALITIES

4.1 Testing Environment and Equipment

NGFW vendor was chosen to be Palo Alto Next-Generation Firewall, since it is the only vendor that has not built on traditional hardware technology with serial order processing, instead it is purpose-build hardware with single pass architecture (Gartner, 2013). Palo Alto Next-Generation Firewall model is PA-200, with the most current software image and with full license capabilities: Threat Prevention, URL Filtering with Brightcloud and Pan-DB, Global Protect Portal + Subscription + Gateway License and WildFire Subscription. Mobile devices will be Apple iPad, Samsung Galaxy SII (Android) and Windows 7 Pro laptop, all of them with the most current Global Protect software image. Wireless Access Point (AP) will be Aruba RAP-3 and WAN router is A-Link RR24 and both with the latest software image, see Figure 18.

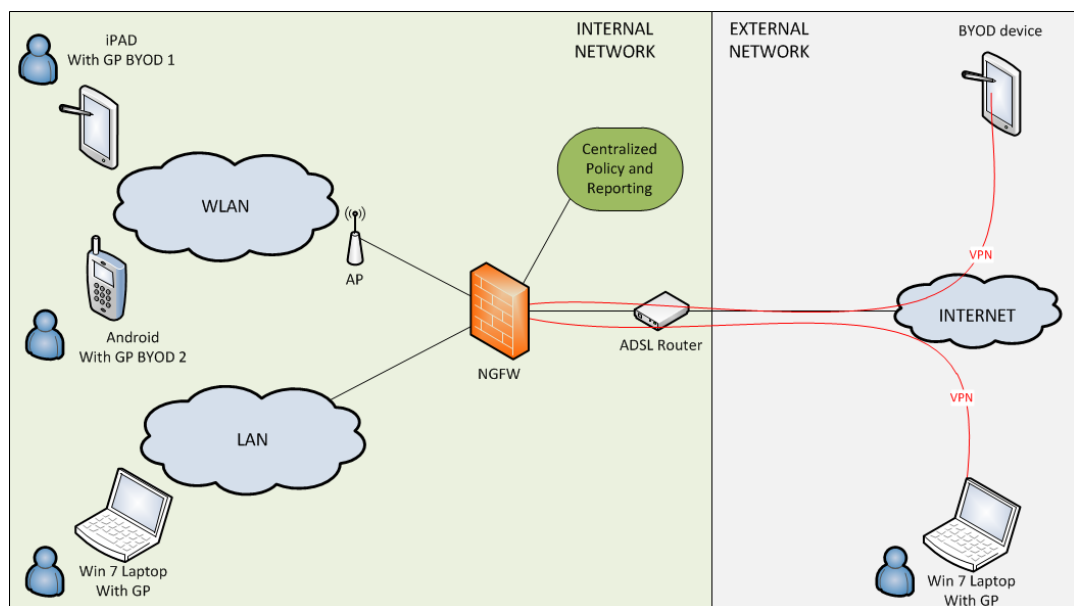


FIGURE 18. Testing environment

Global Protect for Android version: 1.3.2

Android version: 4.1.2, Phone: Samsung Galaxy SII, GT-I9100

Global Protect for Windows version: 1.2.4, 1.2.5 and 1.2.6

Windows version: Windows 7 Professional with SP1

Global Protect for Apple iPad version: 1.3.1

iPAD version: iOS 6.1.3

Pan-OS versions for PA-200: 5.0.4, 5.0.5, 5.0.6, 5.07, 5.08

Aruba RAP-3WN Wireless AP: Version: 6.1.3.4-3.1.0.2_36584

ADSL Router A-Link RR24: Software: 3.7.1 and firmware: 845_AVK_020907.02FA

Some of the functionalities will be tested using NCC's Palo Alto NGFW 5000-series, with version 5.0.x. This is, because some features need a greater amount of real-life data samples that cannot be generated in the lab environment easily, or because of special custom application existence and real-life behavior. Tested functionalities were Custom Application functionality, Threat Profiles, some of the Reports, WildFire statistics and pre-logon feature on VPN functionality.

4.2 Test Plan and Tested Functionalities

Tested functionalities for all mobile devices:

- Global Protect Portal and Gateway (location aware VPN) with user-logon, on-demand and pre-logon modes
- Built-in VPN client provided the mobile device's OS
- SSL-Decryption/Encryption
- Application identification and usage in the policy
- QoS (Quality of Service) filtering
- Geographical location usage
- HIP (Host Identification Profile) for identifying end device
- Threat identification (virus, malware, vulnerabilities, web categories, data filtering, WildFire)
- Reporting functionalities for WildFire and custom reports
- Custom application

- Software and dynamic updates

At first, the PA-200 NGFW was configured with all the features listed above. Internal network was created with DHCP pool in the NGFW. WAN network was created with obtaining interface IP address via DHCP from the ADSL Router, as well as DNS settings provide by the ISP. All IP addresses in the NGFW were private addresses, including WAN interface. Zones were created for Internal (named as Koti), Internet (named as ADSL) and VPN Zone (named as VPN). Threat Detection and WildFire functionality was configured to all traffic by default. NAT was created for outbound traffic from internal networks and another NAT for outbound traffic from VPN zone to separate the NATted traffic from each other in the logs. Global Protect Portal and Gateway was created to the WAN interface address and Country Specific IP addresses (Regions) were configured to allow IPSec VPN and SSL connection to the GP Portal and gateway from Finland and Sweden only. GP modes were tested separately; first user-logon, then on-demand and finally pre-logon. Since GP needs certificates in order to work, the following certificates were created:

- One self-signed Root CA Certificate (KotiRoot)
- One Server Certificate for external VPN Gateway signed by Root CA (KotiOutside2)
- One Server Certificate for internal VPN Gateway signed by Root CA (KotiInside)
- One Device Certificate for Win7 Laptop (KotiLaptop)
- One Device Certificate for iPad (700padlv100...)
- One Device Certificate for Android Phone (PL-SII)
- One Sub-CA Certificate signed by Root CA for SSL Decryption/Encryption (Kotikoti)

Certificates are illustrated in Figure 19.

Name	Subject	Issuer	CA	Key	Expires	Status	Usage
Kotikoti	192.168.12.1	192.168.12.1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Apr 24 18:58:25 2014 GMT	valid	Forward Trust Certificate Forward Untrust Certificate Trusted Root CA Certificate SSL Exclude Certificate
KotiRoot	10.0.0.100	10.0.0.100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 18 15:28:05 2014 GMT	valid	
KotiInside	192.168.12.1	10.0.0.100	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 18 15:30:06 2014 GMT	valid	SSL Exclude Certificate
KotiOutside2	88.114.52.165	10.0.0.100	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 30 07:54:19 2014 GMT	valid	
KotiLaptop	maarit-PC	10.0.0.100	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Aug 9 07:29:10 2014 GMT	valid	
700padlv100-D023DBCF5...	700padlv100-D023DBCF5...	10.0.0.100	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Aug 25 05:05:56 2014 GMT	valid	
SII	PL-SII	10.0.0.100	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Aug 25 05:06:55 2014 GMT	valid	

FIGURE 19. Certificates used during the test.

All the certificates were delivered and installed to the clients to constitute a trust relationship between the clients and portal. Management address was created to the same address space with WAN interface, but with dedicated IP address to the management interface. Management interface cannot be reached from the internet even it is connected to the WAN interface address space, because ADSL router in the front of the NGFW was configured to port forward WAN traffic to the NGFWs WAN interface only. ADSL router had only one public IP address and it was configured to use PAT (Port Address Translation) to the outbound traffic. This enabled the use of private addresses in the NGFW WAN interface and in other network segments. All the inbound traffic originated from the internet to the ADSL router's WAN address was denied except the port forwarded traffic to the public IP.

Also, Security rules were created to the NGFW to allow traffic from the Inside and VPN Zones to the management IP address and also management interface itself has access lists for allowed IP addresses. This way, management interface could not be reached directly from the internet, but with VPN connection it was reached from the internet forcing the traffic to go through the NGFW security policies. ADSL router has one Public IP address in the WAN interface, using DHCP from the operator and LAN interface was configured with DHCP pool where NGFW WAN interface was connect-

ed. Wireless AP (Access Point) was configured and connected to the internal interface of NGFW, using WPA-2 with AES encryption in the wireless radio. This internal WLAN was configured to all mobile devices. WLAN interface of the AP had DHCP pool for wireless clients and by default it was NATing traffic for outbound connection.

Testing period was 6 months for all devices. All the device-specific updates were applied during the test period that was available to each device, including NGFW. Rules and features were fine-tuned whenever needed to achieve desired outcome, resolve problems or correcting misconfigured results.

Connection Methods to Test in the Gateway

There are three different connection methods to choose from:

- User-Logon
- On-Demand
- Pre-Logon

User-Logon method operates in the following way: when user logs on to the device, GP Client attempts to establish a VPN connection automatically to the GP gateway. Combined to Single Sign-on (SSO) option, Windows logon credentials are used to authenticate the user. If Global Protect Portal and Gateway License (subscription) is applied, then the location awareness is automatically on. This way, VPN is established in the external network and is not established in the internal network. Without the license, VPN is always established as soon as user logs on to the computer.

In **On-Demand** method, a user must explicitly initiate the VPN connection to the GP gateway. Credential stored on the GP Client can be used to authenticate the user. This is an ideal solution for partner remote access usage as well as some BYODT deployments. VPN will be disconnected when idle time out exceeds or user disconnects the VPN connection.

Pre-Logon method means that whenever user machine is turned on, regardless of the location, the VPN connection is established prior to user logon, using machine certificates for authentication. This way, client machine can logon directly to AD domain, just like in corporate LAN, which enables AD group policy enforcement, password reset/changes, drive mappings and software deployments downloads – even when the user is not logged in to the machine. It only requires that the machine is turned on and has an internet connection. HIP profiles can be used to limit traffic to or from these pre-logon identified machines, since specific user identification cannot be used prior user logon. When user logs on to the machine, user is identified and user logs in to the domain and the rest of the security policies can be applied to the VPN connection, since user is identified during the logon.

Agent Options

There are several options to choose to enable or disable in the end user's VPN client. The Graphical User Interface (GUI) existence can be enabled or disabled. By enabling this option, user has some visibility for the agent and connection. This should be enabled to provide support in trouble-shooting tasks. It also enables support or end user to temporarily disable the whole client with passcode, comment or using ticketing system by using Agent User Override option. This can be set to disabled as well, to provide read-only view for the user. User can save password –option should be enabled to provide SSO (Single Sign-On) feature. Client upgrade can also be performed transparently or with option to select user to choose it, see Figure 20.

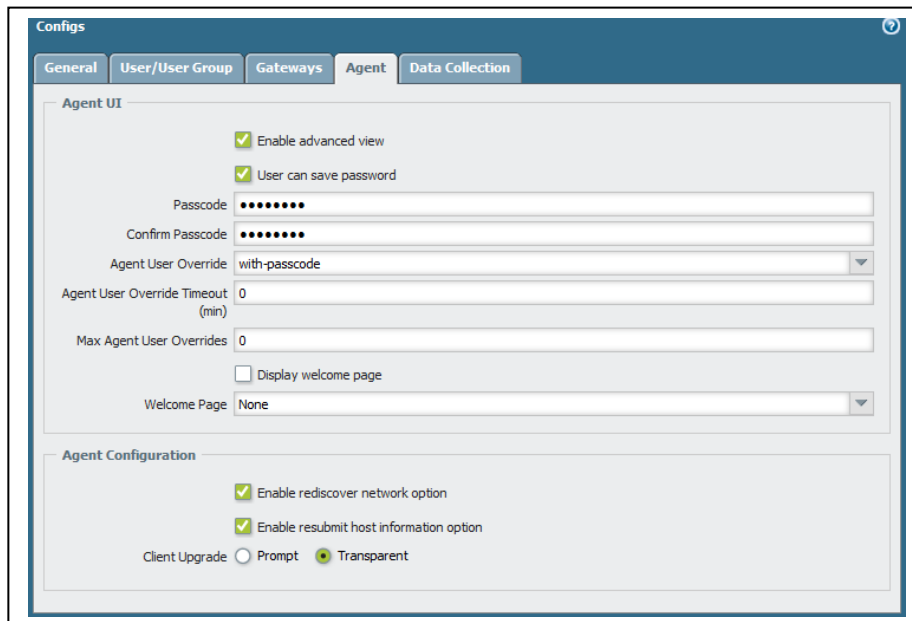


FIGURE 20. Agent options for end user's GUI

When testing the different features, GUI was left on, with a possibility to change all the settings that are changeable. In production environment, GUI provides some visibility to the user, so it should be turned on in read-only mode. The password option may be left on also for administration purposes, or disabled, if the company policy requires the machine to be carried to the office for troubleshooting case or if the remote connection is not so critical service in the company.

4.3 Installations and Tests

4.3.1 Android Installation with Global Protect Client

Android installation was performed from Play Store and there was not any errors encountered during installation of Global Protect (GP) Client. After entering the portal address, username and password with remember me option, the connection was established and fully working (Figure 21). The only negative effect was that user needs to click "I trust this application" every time the device is started up (Figure 22). After clicking OK, the device never asked it again, until the device is rebooted again.

This should be one time feature only, instead of a feature asked after every boot. The default behavior when the gateway is unavailable is that the GP client allows all network connectivity. When the GP gateway is available again, VPN connection is established automatically.

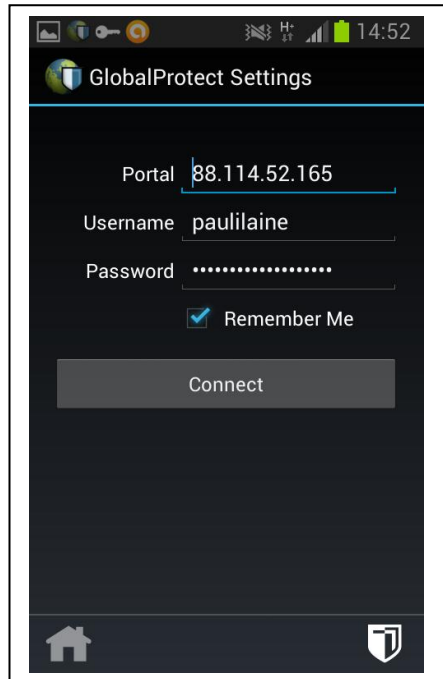


FIGURE 21. GP Portal Settings

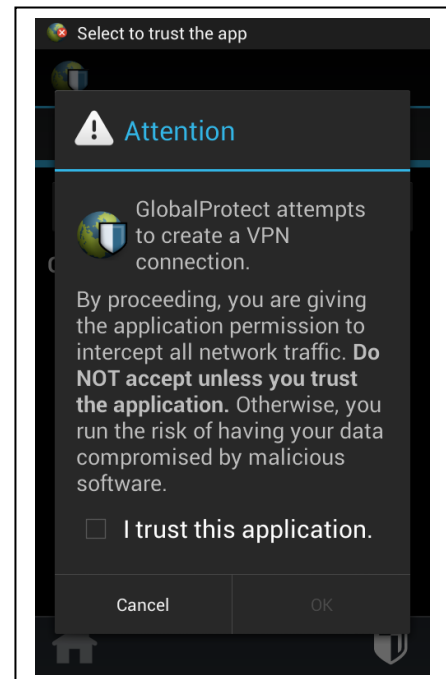


FIGURE 22. Connection establishment

Figure 23 illustrates the situation, when connection has been established to the gateway and location is an external network (internet) and therefore VPN has been automatically turned on. Figure 24 presents the statistics of the VPN connection. IP address has been assigned from the VPN Pool, network is mobile network and Protocol is IPSec, since it is the most efficient transport method, because it is using UDP instead of TCP. If IPSec connection to the gateway cannot be established, then fallback method is SSL, which is usually open in the network. IPSec may be prohibited in some networks by service provider. If the portal's certificates have not been imported to the Android device before connecting to the gateway, the certificate notification will be prompted. This needs user to agree prior to connect to the gateway. After installing the certificates, no prompts were generated; however in an Android

device, this kind of prompt occurred once in the test period, even when the certificates were installed.

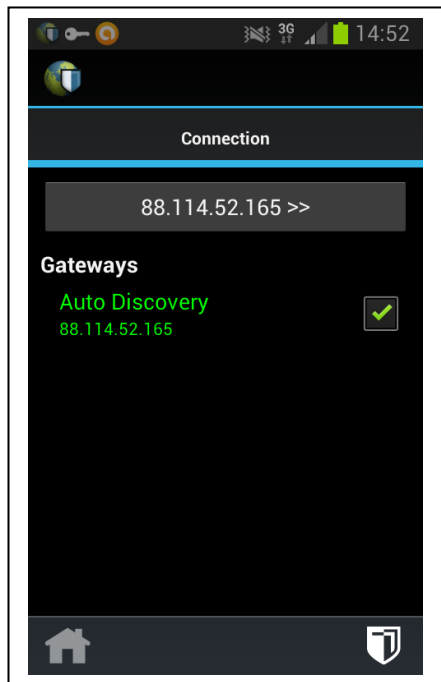


FIGURE 23. Connection established

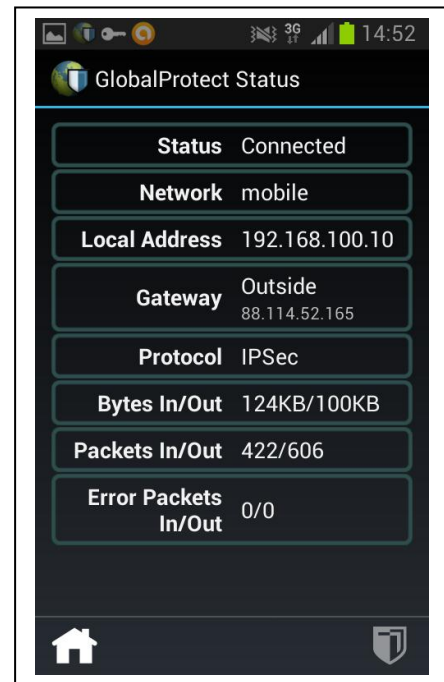


FIGURE 24. VPN Status.

The user can circumvent the VPN connectivity by uninstalling the application, not trusting the application when it asks to trust the application, disabling the application (see Figure 25 and 26) if that is allowed in the gateway parameters (Agent User Override parameter) or with a factory reset. These circumvents can be addressed by the following way:

- Palo Alto Networks changes the (default) behavior of the application from “trust approved by the user during every boot” to “one time only feature”, instead of asked after every boot in the Android version of GP.
- Disabling application by the user is controlled in the gateway using Agent User Override parameter with the password or disabled option. Password must be protected by need-to-know basis and cannot be revealed to end users.
- Uninstalling application can be prevented or detected with MDM solution by password protection or similar controls

- Factory reset is not feasible to be address, since encrypted device remain protected and user will lost all the phone-specific data during the factory reset. Also, company will lose the data in the device and company data and network cannot be accessed until MDM forces the company security settings to the device again.

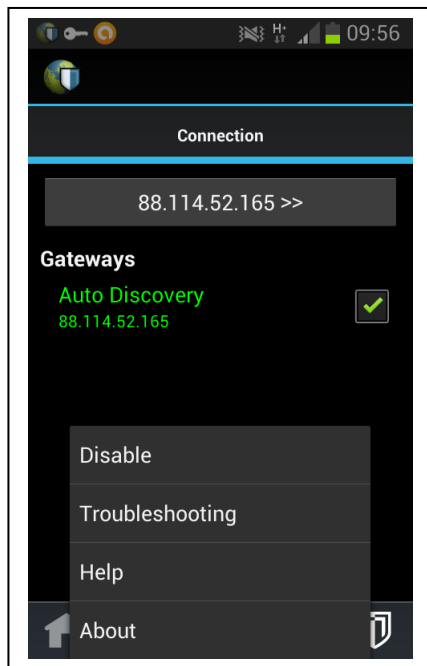


FIGURE 25. Disabling GP

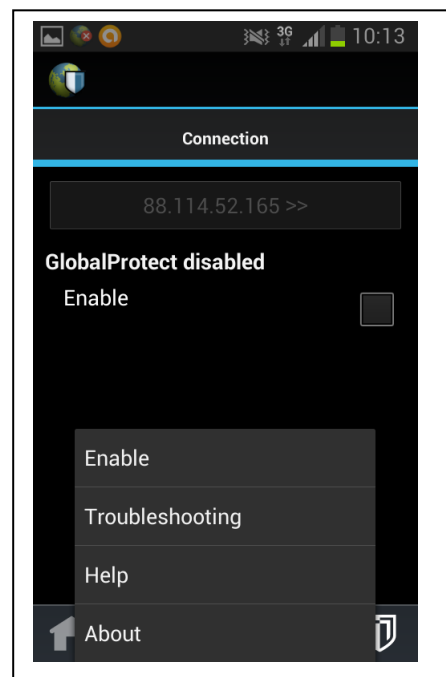


FIGURE 26. Enabling GP

If all of the mentioned improvements are done, GP can be forced with the desired settings for the remote users with some level of confidence that the application is always up and running. Comprehensive protection means that security is addresses in a controlled manner in the NGFW gateway and portal, by the vendor's software and using MDM solution to force and control settings and behavior or the device. In addition, company's processes and agreements should be in place to support user education and responsibilities.

4.3.2 Android Usage with Global Protect Client

In the daily mobile use, GP client is transparent. There is only a small icon on the top left side of the Android bar indicating the network location and VPN status. Figure 27 illustrates the network location as Internet and the key indicates that the VPN is turned on based on the location (outside defined home-network). Figure 28 illustrates the defined home-network, where the VPN is not enabled.

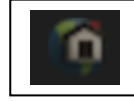


FIGURE 27. Internet-connection with VPN FIGURE 28. Internal-network without VPN

When Wi-Fi was turned on in home location (Figure 29), GP client noticed the new network and whether it is able to connect to its own internal gateway, then the network is considered as internal network and the VPN is disconnected. Once the Wi-Fi is turned off or connected to another network, then connectivity to the internal gateway is lost and VPN will be established to the GP Portal (external gateway), Figure 30). Notifications can be turned off to better support transparency for the user. This can be done from the phones' settings by selecting Settings, Application manager, then selecting GlobalProtect and tapping off the Show notifications -option.

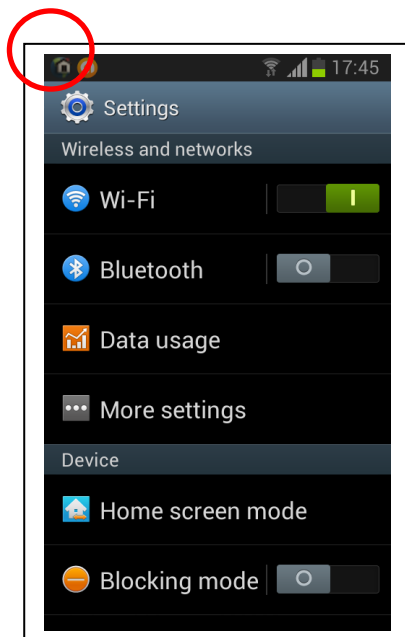


FIGURE 29. Wi-Fi in internal network

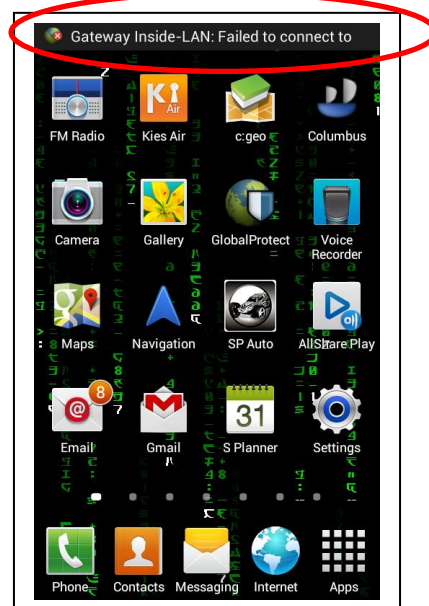


FIGURE 30. Switching to external location

Figure 31 illustrates a management view of NGFW in an Android's phone browser using VPN connection. Management IP address is in private address space and cannot be reachable directly from the internet, only from internal network or via VPN.

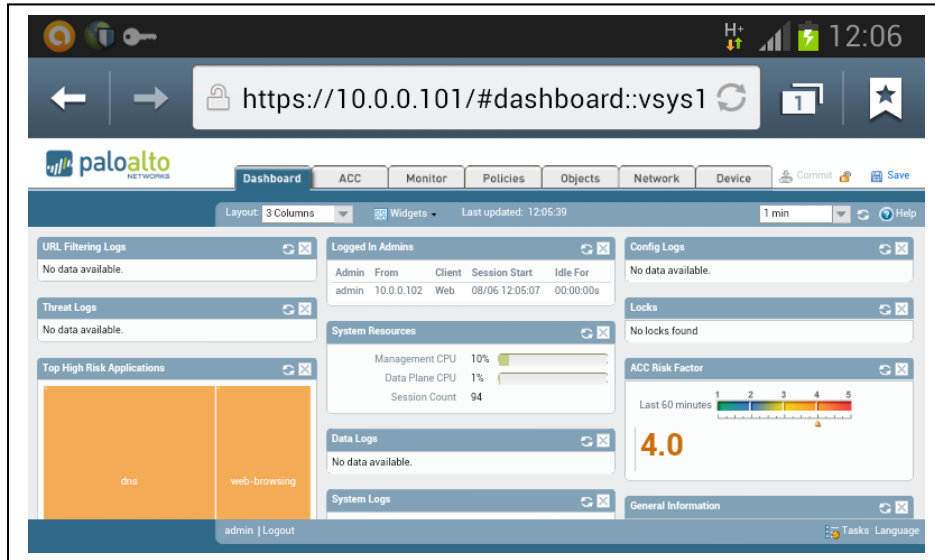


FIGURE 31. Using management interface with VPN enabled.

Testing the functionalities of SSL Decryption/Encryption, a web page was opened from the internet using the VPN connection and Android's web browser. Eicar.org-site has a Test Virus called Eicar that can be tested against company's AV functionality. It can be downloaded using plain (unencrypted) HTTP and more secured (encrypted) HTTPS protocol. Figure 32 illustrates the web site where the test virus can be loaded using SSL (HTTPS).

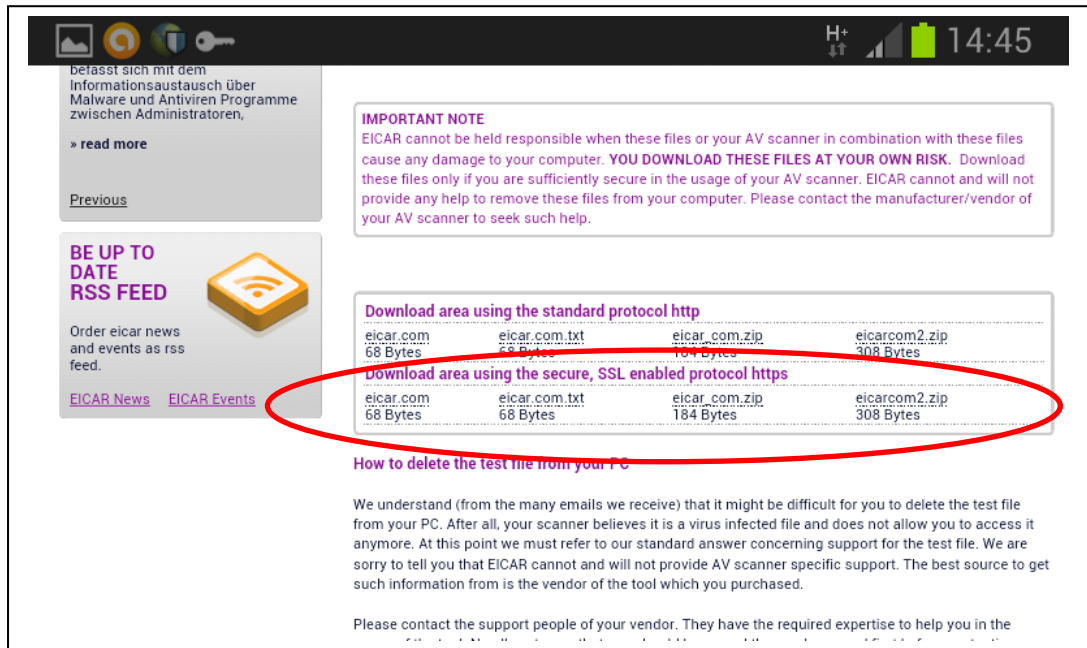


FIGURE 32. Using Android browser to access encrypted web page with SSL

Figure 33 illustrates the message displayed to the user when unwanted programs has been detected and blocked from the user's traffic.

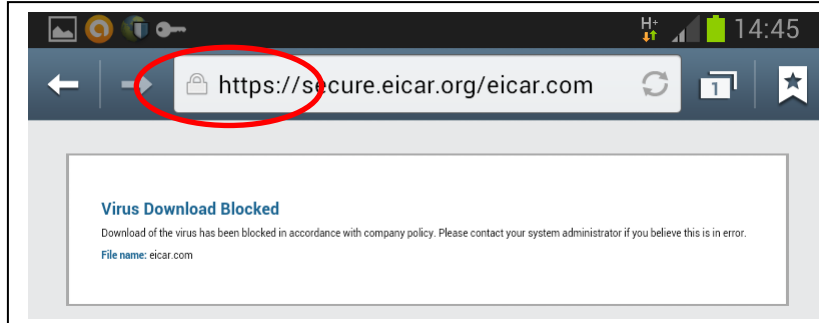


FIGURE 33. Blocked Eicar test virus from encrypted SSL traffic

Eicar was used only to test the correct behavior and configuration of NGFW. Using SSL Decryption/Encryption in the real traffic is more challenging, because user's privacy needs to be protected while unwanted software needs to be blocked. Also, personnel need to be informed before any changes to logging or collecting user's data are done, depending somewhat on country specific privacy laws. Also, collecting user-specific data, users must be informed in advance and they must have a change to accept or decline it and they have the right to know all the details of their records, its

usage, how it is protected and its lifecycle. They have also right to get their information when requested and the records must be deleted if user later on decides to resign from its usage. SSL Encryption/Decryption cannot be done, if applications require browsers to present a client side certificate or if the encryption is proprietary decryption. It is challenging to use SSL Encryption/Decryption efficiently without breaking the functionality of business applications and still decrypt questionable traffic, especially in BYOD environment. During the tests, Apple Store and iTunes connections and Google Maps stopped working when SSL Encryption/Decryption was enabled. Since restriction cannot be done based on the application, instead by categories, those categories must be excluded from the decryption process. After exclusion, functionalities worked again.

Custom categories can help distinguishing the web sites from each other, since wildcards can be used, like *.facebook.com, in addition to “content-delivery-network” category, for example. In Figure 34 a custom category “PL-Exemptions” rule was created to decrypt traffic to the desired domains that overlaps with pre-defined categories in the rule below in “NO-Decrypt2” rule. The last rule will decrypt every SSL-traffic that is not excluded in the rules above. It is important, that Financial-category is not decrypted to prevent decrypting of user’s banking and credit card transactions. Web-email Category is also challenging, since user’s use personal web-based emails for personal usage. Therefore, privacy issues may arise if decrypting Web-email Category, however it also poses a risk, since users tend to receive phishing emails and transfer attachments via encrypted email services and if not decrypted, this poses a risk to the company. Finnish legislation of user’s privacy is determined in the law 13.8.2004/759 and concerning EU countries, in EU’s directive 2002/58/EC.

Name	Tag	Source			Destination		URL Category	Action	Type
		Zone	Address	User	Zone	Address			
NoDecrypt-To-PA-Int...	none	Koti VPN	any	any	ADSL	10.0.0.0/24	any	no-decrypt	ssl-forward-proxy
Decrypt-from-Koti	none	Koti	any	any	ADSL	any	PL-exemptions	decrypt	ssl-forward-proxy
Decrypt-from-VPN	none	VPN	any	any	ADSL	any	PL-exemptions	decrypt	ssl-forward-proxy
NO-Decrypt2	none	Koti VPN	any	any	ADSL	any	computer-and-internet-info content-delivery-networks financial-services music online-storage-and-backup reference-and-research	no-decrypt	ssl-forward-proxy
Decrypt-from-VPN-Rest	none	VPN	any	any	ADSL	any	any	decrypt	ssl-forward-proxy

FIGURE 34. Fine-tuning SSL Decryption/Encryption with categories

Eicar was also downloaded as unencrypted with Android using Avast! Mobile Security product and it did not recognize Eicar test virus downloaded from the internet at eicar.org. Application version was 1.0.2129 and it recognizes 5944 definition with definition version of: 130813-01 updated at 13th of August 2013. Test was done at 14th August 2013.

User-Logon Tests

During the test period, Wi-Fi and Bluetooth tethering could not be used while GP Client was running VPN. Therefore, internet connection cannot be shared with the device running GP with some other devices using Wi-Fi or Bluetooth connection. This prevents unknown devices to share VPN connection that would cause security risks to the company. A personal wireless device and application was tested during testing period. A wireless transmitter was attached to the earphone plug and a radio controlled car was used with iPad and Android phone without any problem with GP Client running VPN connection. iPad and Android have a small application called SP Auto (Figure 30) that loads a car controller board to mobile device touch screen and controls the car using wireless adapter on the earphone plug. Another similar kind of devices and applications (like Radio) can be used together with GP client, since they do not interact with any communication channels of the mobile device, such as bluetooth or Wi-Fi.

When VPN is enabled, it prevents any other direct connections to the client, e.g. remote access connection using Kier Air or similar software. When VPN is turned off in the internal network, these kinds of direct connections to the phone are available again. Thus, in BYOD solution GP will protect the mobile device like any other VPN solution that is configured for Full Tunneling Mode. This means that the company policy applies to the user mobile device 24h per day, 7 days a week. If the company policy conflicts with the user behavior, the company can apply different kind of policies for outside office hours and weekends using scheduled security rules, user groups and HIP rules for different mobile devices. This may limit a user's personal internet usage, depending how internet-usage conflicts with the company policy; however it also provides better security for the user.

Data usage examples for two months are illustrated below, in Figures 35 and 36, taken during User-Logon testing period. Data usage has considerable effect on battery lifetime of a small device, whereas tablets have more capacity on their battery and therefore effect on lifetime is smaller.

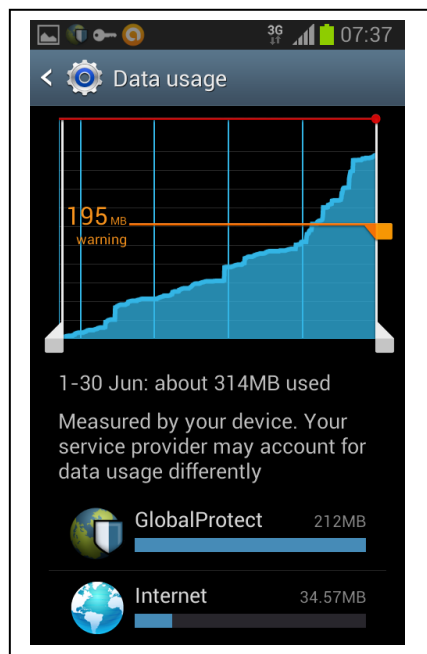


FIGURE 35. Data usage at June

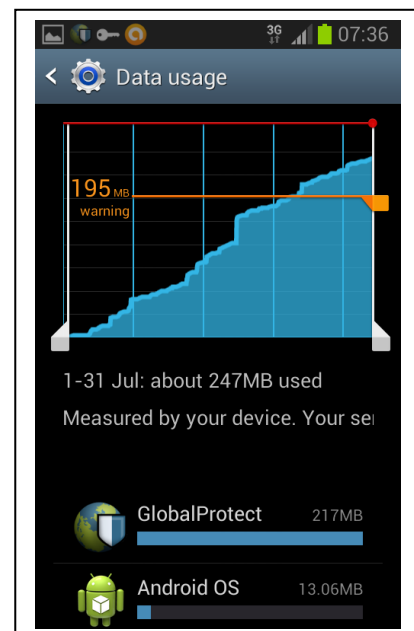


FIGURE 36. Data usage at July

Data usage limits and alerts can be configured to prevent unnecessary data or roaming costs, especially in when abroad. GP Client itself does not generate traffic much more than without VPN, but it will consume some CPU processing power and therefore effects battery consumption. Based on the tests, without GP Client actively turned on, the battery lasts for about 1.5 day before it need to be recharged. With GP Client actively on, it lasts whole day (from 8 am to 8 pm) before it must be recharged. Testing days were typical working days for one person; however phone usages vary much between different people. Testing device's battery was one year old.

On-Demand Tests

When On-Demand mode was selected in the connection method, the Android GP Client changed the behavior with the possibility to connect/disconnect VPN. Thus, VPN must be initiated by the user as illustrated in Figures 37 and 38.

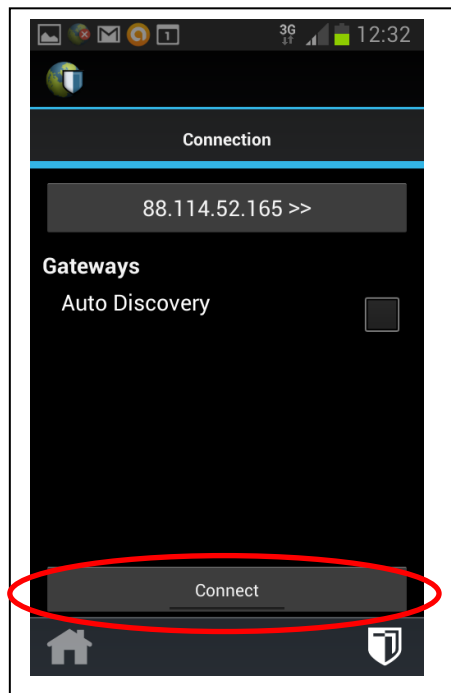


FIGURE 37. On-Demand Mode at disconnected-state

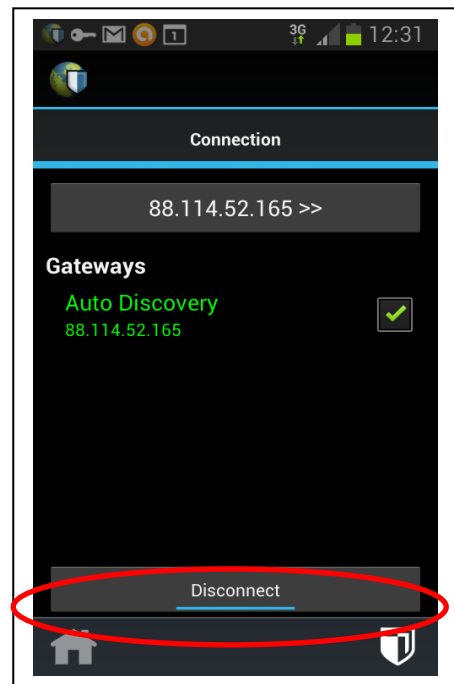


FIGURE 38. On-Demand Mode connected-state

Pre-Logon Tests

Pre-Logon functionality is used only for Windows operating systems and only with machine certificates. However, a test was done with a user certificate generated for user's device, signed by NGFW's root CA. Then, a certificate profile using NGFW's root CA was generated and assigned to the portal. When installing the certificate to the device and applied the Certification Profile to the NGFW, GP worked as in User-Logon tests. However, if the certificate was missing from the device, an error message was displayed, as illustrated in Figure 39 and VPN Connection was not established until the device certificate was installed. Users can install the certificate by clicking the Install-button and selecting the folder where the certificate file exists (if distributed to the user) or choosing to install the certificate later. After installing the certificate, or if the certificate has been distributed to the user, user needs to choose and accept (allow) the certificate when the connection attempts the next time, see Figure 40. This is a one-time functionality and the device remembers the certificate for the future connection attempts and uses it automatically.

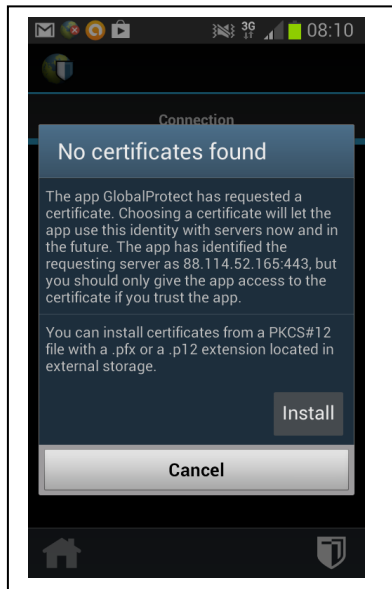


FIGURE 39. Certificate not installed

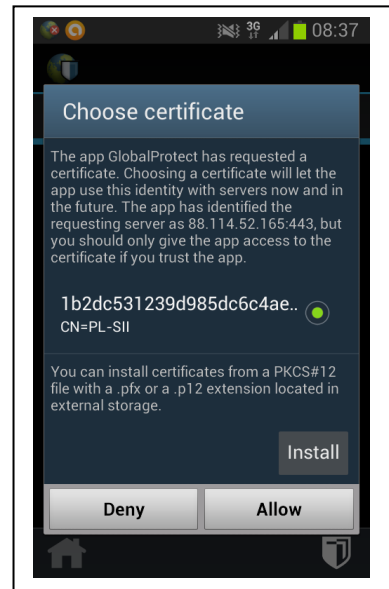


FIGURE 40. Certificate installed

Using certificates limits the connections to the portal and gateway for devices only with a valid certificate installed. If this certificate profile was chosen also to the

gateway and the user-logon was changed to pre-logon mode, the Android GP application crashed when connected to the internal network via Wi-Fi and stayed in the crash-loop until Wi-Fi was disconnected. However, connection using GSM data was operated normally to the WAN portal and gateway. This behavior was tested a few times and the only way to recover was to delete user certificates, reboot the device and reinstall the application. Apple's iOS (iPAD) and Win7 worked normally during this test. This possible bug will be reported to the Palo Alto Networks. Another version of Samsung phone did not crash, so this may be a device model specific bug for Samsung SII GT-I9100 model. The purpose of this test was only to see, that Pre-Logon mode would not affect the devices that cannot do pre-logon.

Android with built-in VPN Client

Android built-in VPN Client was also tested. Built-in VPN Client in Android version 4.1.2 and one version earlier were not able to establish a VPN connection. Version 4.1.2 establishes a VPN connection, but no traffic was seen in or out of the device. The earlier version crashed the software and the phone rebooted every time the VPN connection was established. This build-in VPN Client could have been used for on demand VPN connections. This way user could establish and disconnect the VPN when needed. GP Client offers the same functionality with expanded functionalities, so build-in VPN client test was not tested any further.

4.3.3 iPAD installation with Global Protect Client

Global Protect for iPAD was downloaded and installed from AppStore. No errors or problems were encountered during installation. After entering the portal address, username and password with remember me option, the connection was established and fully working (Figure 41).

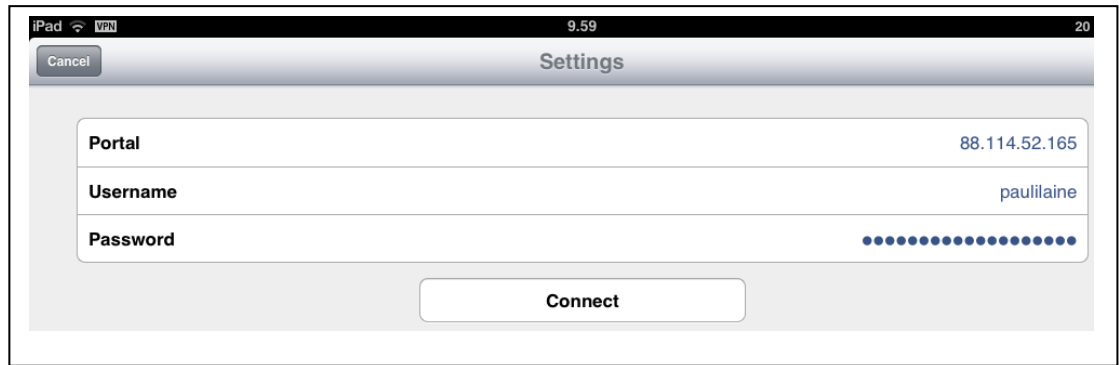


FIGURE 41. GP Settings in iPad

The default behavior when the gateway is unavailable is that the GP client allows all network connectivity. When the GP gateway is available again, VPN connection is established automatically. However, user can circumvent VPN connectivity from the VPN Settings page, by disabling automatic connection establishment (Yhdistä tarvit- taessa), see Figure 42 or completely uninstalling the application. Modifying applica- tion parameters by the user, such as enabling or disabling the GP client, can be pre- vented from the GP gateway.

Next time user is connected to the GP Portal, the settings are obtained automatically from the GP gateway, which will override any user-made changes. So, these settings are centrally managed and forced to the GP Clients. Different GP Client operating modes requires different GP gateways and portals, meaning different Public IP ad- dresses at the gateway. Like in Android, IPSec is the default connection method and SSL is the fallback method. If the certificates are not imported to the iPad, when connecting the first time to the portal, the connection is not established. When the certificates have been imported and installed, the connection will establish without problems.

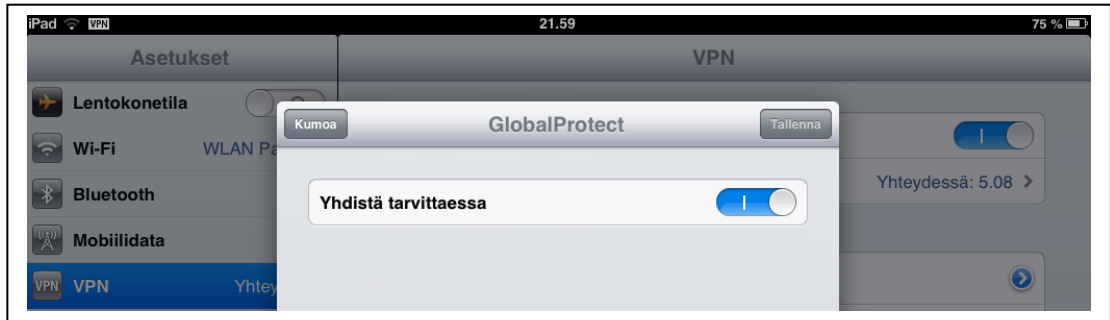


FIGURE 42. GP VPN Settings

4.3.4 iPad usage with Global Protect Client

In the daily mobile use, GP client is transparent, just as it is in Android devices. There is only a small icon on the top left side of the iPad's information bar indicating the network location and VPN status (Figure 43). The VPN icon is displayed in both, internal and external locations, unlike Android, where the icon was different based on the location.



FIGURE 43. VPN indicates that GP is up and running.

FIGURE 44 illustrates the network location as Internet and VPN is turned on based on the location (outside defined home-network). Figure 45 shows the VPN details.



FIGURE 44. Location is Internet and VPN is enabled

Unlike Android's GP Client informed GP specific information in the mobile phone's information bar at the top of the phone, all the information regarding to GP Client is informed under the GP Client's application tab "info". So, user really does not need to be aware of this application – only the "VPN" text is seen in the top left bar.



FIGURE 45. VPN Connection details when connected via Internet

Figure 46 illustrates the defined home-network, where the VPN is not enabled.



FIGURE 46. Location is Internal and VPN is not enabled

The same sites were tested as with Android and also SSL Decryption and Encryption for verifying the correct behavior of the gateway's security policy and that certificate was trusted and no error messages appeared.

User-Logon Tests

Tests and behavior with iPad were uniform with Android. Certification prompts were never shown if the certificates were installed before using GP Client, unlike Android prompted it once even they were installed. If the iPad does not have SIM-card installed and uses only WLAN, there is no need for paying attention to roaming costs. Battery lifetime is much longer than a phone's lifetime, therefore GP Client has a minor effect on it. As in Android's User-Logon Tests at page 66-68, GP prevents local access to the device if using any communication channels like WiFi or Mobile data via SIM card.

On-Demand Tests

When using On-Demand Mode, the possibility to "connect automatically" disappears from the VPN Settings, as seen in Figure 47.



FIGURE 47. VPN Settings in On-Demand mode

User must open the GP Client and touch the connect-button in order to establish a VPN connection to the gateway. VPN disconnects automatically after about a 2-minute idle time or when user chooses to disconnect. This is equal behavior to iPad's built-in VPN Client. This gives a great deal of freedom to the user, since VPN is connected only when access to the corporate data is needed. Thus, any personal communications can take place when disconnecting the VPN and the user-specific personal communication has minimum interaction with corporate network and data.

Pre-Logon Tests

Pre-Logon functionality is used only for Windows operating systems and only with machine certificates. Device certificate is distributed to the client and installed by the user (Figure 48). After installation, GP works as in User-Logon tests and this is the way it should be, since Pre-Logon tests should not affect devices that cannot present machine certificates. If pre-logon fails, then normal authentication follows.



FIGURE 48. Device certificate installation by user

iPAD with built-in VPN Client

Build-in VPN Client works as expected. User needs to enter gateway information and userid and password information in order to establish a connection (Figure 49). At the gateway side, "Enable X-Auth Support" needs to be enabled with group credentials or certificate configured in NGFW in order to support 3rd party IPSec Clients.

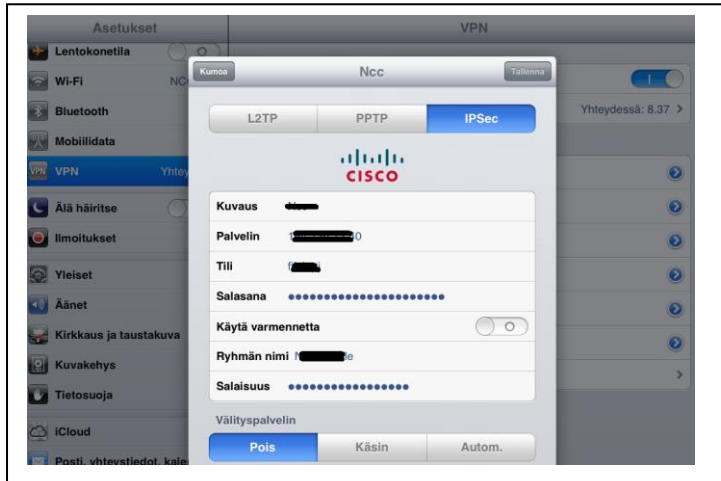


FIGURE 49. Apple iOS native VPN Client

The idle time-out in the device seems to be configured in around 2 minutes. After two-minutes of inactivity, user needs to re-establish the connection. This is a device specific feature, which cannot be changed by the user. Built-in VPN Client can be used together with GP installed on iPad as long as they are not enabled at the same time. This way user can have several different VPN tunnels to several locations or companies. Best result is achieved, when all the VPN tunnels are configured as on-demand mode to prevent them to interference each other's behavior.

4.3.5 Windows7 Installation with Global Protect Client

Windows7 installation and settings were applied and a connection was established without problems. Client needs to have a connection to the Portal and Gateway during installation, in order to test the Client and credentials. Settings are illustrated in Figure 50. Client can be delivered to devices without GUI (Graphical User Interface) and also preconfigure to use the user's logon credentials.

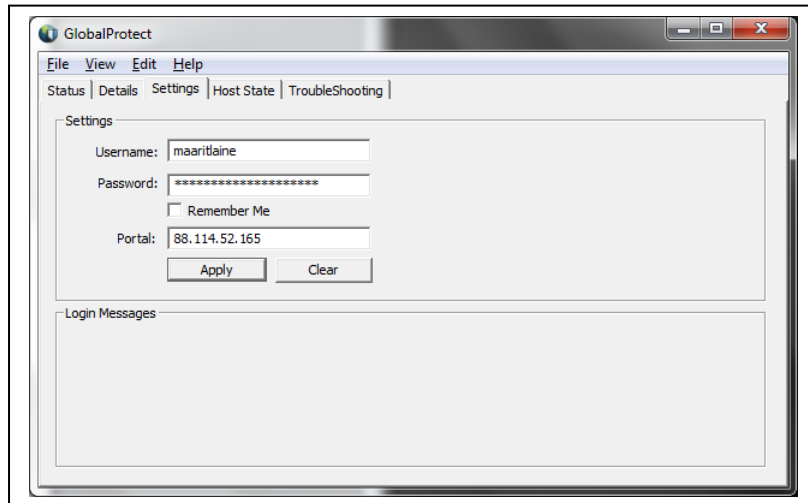


FIGURE 50. Connection Settings with Windows7 GP Client

GP Client is transparent, just like in Android and Apple devices, where only the service icon is displayed located in the lower right corner of the screen, see Figure 51.



FIGURE 51. GP Client icon

Windows GP Client collects information about the host state, e.g. installed AV, Microsoft patches and version information, logon domain, IP addresses in use, network interfaces, registry entries, etc, see Figure 52. This information can be used against the NGFW's security policies to verify what kind of device is connecting to the gateway and make policies according to the HIP information. Different settings can be defined to the HIP profiles, and used to distinguish devices with different access levels, such as corporate devices, BYOD devices and partners' devices.

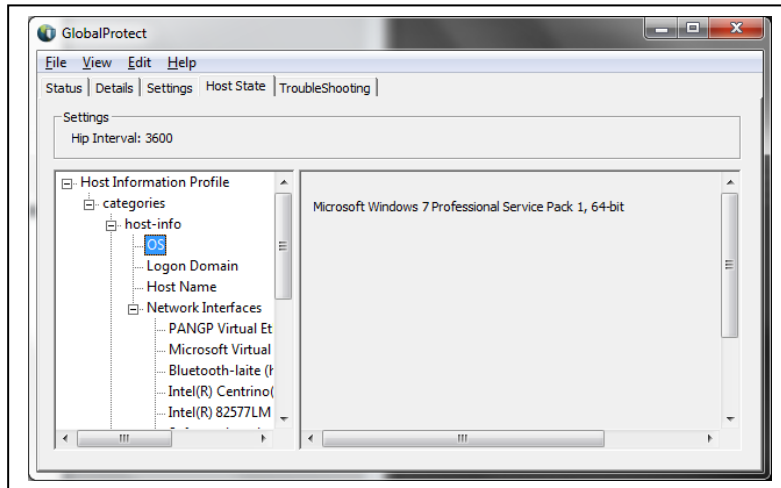


FIGURE 52. Host identification information

4.3.6 Windows7 Usage with Global Protect Client

Discovery works as expected. Every time the network changes, GP Client detects whether internal or external network and establish VPN accordingly, see Figures 53-54. Without GUI, only a small icon is displayed with a splash bubble displaying any changes in the GP Client's connectivity.

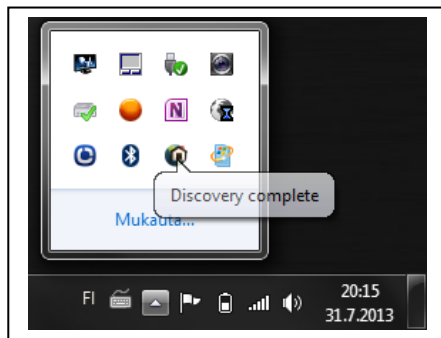


FIGURE 53. Discovery process

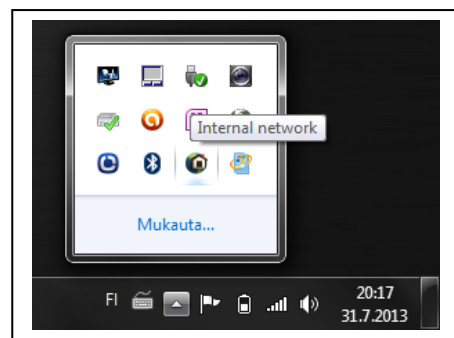


FIGURE 54. Discovery completed

SSL Decryption/Encryption was also tested to verify correct functionality and it worked as expected, see Figures 55-56. A virus was blocked inside SSL traffic and the certificate was fully trusted and user was not asked to trust the certificate. Figure 56 illustrates the certificate chain and Figure 57 illustrates how Subordinate Certificate Authority –type of certificate generates server certificate on-the-fly and signs the

secure.eicar.org –certificate. This way, the traffic can be automatically analyzed by the security policy, and automatic alarms can be generated if critical and/or high threats are detected and the traffic can be prevented before it is delivered to the client.

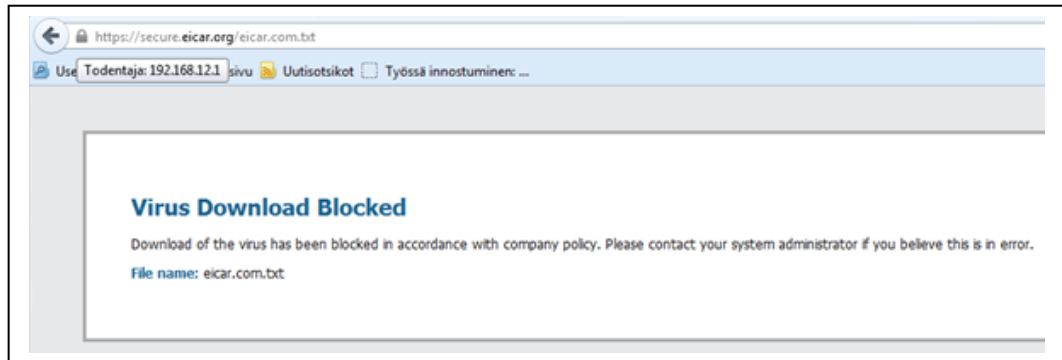


FIGURE 55. Eicar-virus blocked inside SSL traffic

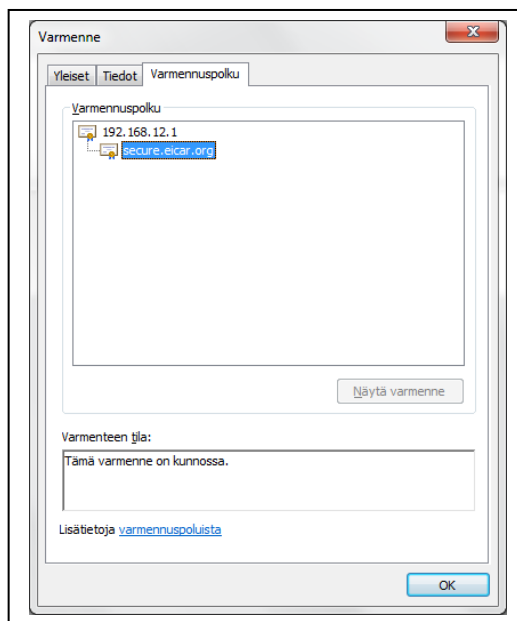


FIGURE 56. Certificate chain

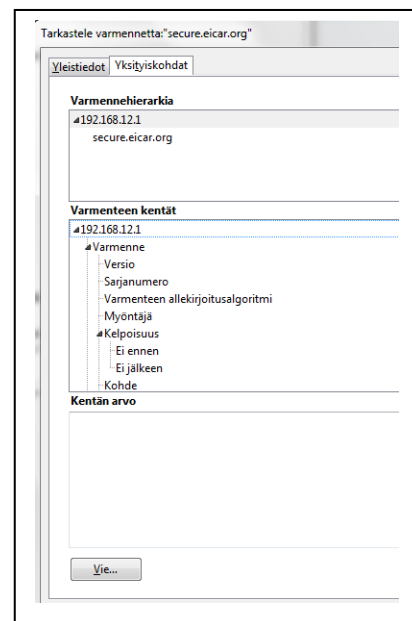


FIGURE 57. Certificate Details

In order to distribute the certificate to the clients, several methods need to be done. In IE (Internet Explorer) distribution is the easiest in corporate environment, since certificates can be delivered using existing methods, like WSUS, SCCM or Group Policy updates. This is because IE uses Windows OS' certificate store, where-as Firefox uses its own database for certificates as well as other Firefox specific settings. Firefox

and Chrome need some additional scripts to deliver the certificates to the users. When using Apple's Safari browser, usually the end user installs the certificate, even when pushed via MDM solution, user still needs to accept the certificate.

User-Logon Tests

In user-logon mode, GP establishes a connection, when user logs on to the computer. It automatically discovers the network and connects to the portal for latest configuration changes or updates and establishes a VPN tunnel to the corporate gateway, if located outside corporate network. If located in the internal network, VPN will not be established. Usually, devices are not connected to two or more different network at the same time. Interfaces are typically prioritized because of routing issues to decide which route will take effect if there are several interfaces available. One of the interfaces must be the default route where traffic is routed unless static entries define differently. This will cause a problem to client connectivity, therefore it is usually solved by disabling WLAN if LAN is available in BIOS settings or alternatively with additional software delivered with the laptop. And, when LAN is not available, WLAN is turned back on which will prevent simultaneous interfaces to be active at the same time.

With mobile devices like phones and tablets, this is not a problem either, since they only have wireless interfaces and once one interface is on, others are shut down. Thus, it is not so important to test VPN functionality with simultaneous interfaces on, since it will establish a VPN connection whenever it discovers to be on the internet. But, if the previous problem exist, that simultaneous interfaces are actively on with different security zones (connections, like internal and internet network), the problem needs to be resolved in the host side, not in the VPN client. In this kind of situation, VPN Client is typically configured to secure the client connection and establish the VPN connection. Overall, user-logon tests were reliable and successful and there were no problems using it with other security products likes AV or FW in the host.

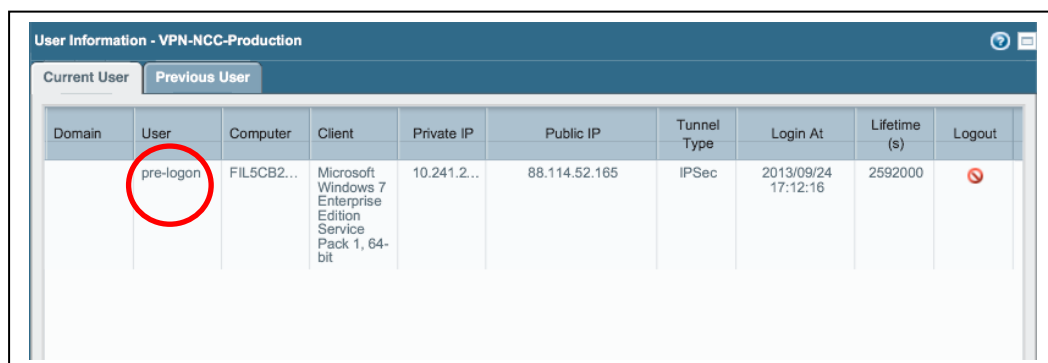
On-Demand Tests

On-demand test worked as reliably as the user-logon test. The gateway was configured to use on-demand, instead of user-logon and next time the client connects to the portal, it will get the updated parameters and works accordingly. After that, user can connect or disconnect VPN by on-demand, when needed. This setting is ideal for partners and GP client works with other VPN products installed in the client's computer, like Juniper Network Connect Virtual Adapter, Cisco Systems VPN Adapter and PAN Virtual Ethernet Adapter.

Pre-Logon Tests

Pre-logon feature requires a machine type of certificate installed into the client enrolled by the Certificate Service in the Windows AD. No other type of certificate is sufficient to test this feature, which limits the Operating System requirement also to the Windows platforms.

Figure 58 illustrates a pre-logon user that has turned on a company laptop and has not yet logged in, or the user has logged off from the computer but the computer still has a network connection to the company. The user cannot be authenticated if he or she is not logged in and therefore the user is not identified; however the computer is authenticated using the machine certificate. This way, a company's computer is under the control of IT services and it can be supported remotely.



User Information - VPN-NCC-Production									
Current User		Previous User							
Domain	User	Computer	Client	Private IP	Public IP	Tunnel Type	Login At	Lifetime (s)	Logout
	pre-logon	FIL5CB2...	Microsoft Windows 7 Enterprise Edition Service Pack 1, 64-bit	10.241.2...	88.114.52.165	IPSec	2013/09/24 17:12:16	2592000	⊘

FIGURE 58. Pre-logon user identified

As soon as the user logs on to computer, he or she can be authenticated and more network level access can be granted defined by the security policy rules. Pre-logout feature offers a domain-level logon, which enables the use of network shares, printers, logon scripts, updates and all the other domain-level services, including the user's password reset remotely by the support team. Therefore, pre-logout feature offers virtually the same services, as if the user were in the office. Figure 50 illustrates the log entries, when the user logs in to the computer. The first four log entries are located at the bottom of Figure 59 and the computer is identified as pre-logout, since the computer was restarted with the internet connection. The rest of the log entries were generated, when the user logged on to the computer and the user was identified with Single Sign-On. Single Sign-On feature enables the VPN connectivity without any user interaction. This way, VPN works seamlessly from the end user perspective.

Time	Type	Severity	Event	Object	Description
7:54	globalprotect	informational	globalprotectgateway-regist-succ	VPN-NCC-Production	GlobalProtect gateway user login succeeded. Login from: 88.114.52.165, User name: [REDACTED]
7:54	globalprotect	informational	globalprotectgateway-config-succ	VPN-NCC-Production	GlobalProtect gateway client configuration generated. User name: filainpj, Private IP: 10.241.217.34, Client version 1.2.5-2, Client OS: Microsoft Windows 7 Enterprise Edition Service Pack 1, 64-bit.
7:54	globalprotect	informational	globalprotectgateway-auth-succ	VPN-NCC-Production	GlobalProtect gateway user authentication succeeded. Login from: 88.114.52.165, User name: [REDACTED]
7:53	globalprotect	informational	globalprotectportal-config-succ	VPN-Portal-NCC-Production	GlobalProtect portal client configuration generated. Login from: 88.114.52.165, User name: [REDACTED], Config name: [REDACTED]
7:53	globalprotect	informational	globalprotectportal-auth-succ	VPN-Portal-NCC-Production	GlobalProtect portal user authentication succeeded. Login from: 88.114.52.165, User name: [REDACTED]
2:16	globalprotect	informational	globalprotectgateway-config-succ	VPN-NCC-Production	GlobalProtect gateway client configuration generated. User name: pre-logout, Private IP: 10.241.217.34, Client version 1.2.5-2, Client OS: Microsoft Windows 7 Enterprise Edition Service Pack 1, 64-bit.
2:16	globalprotect	informational	globalprotectgateway-regist-succ	VPN-NCC-Production	GlobalProtect gateway user login succeeded. Login from: 88.114.52.165, User name: pre-logout.
2:16	globalprotect	informational	globalprotectgateway-auth-succ	VPN-NCC-Production	GlobalProtect gateway user authentication succeeded. Login from: 88.114.52.165, User name from client certificate: pre-logout.
2:05	globalprotect	informational	globalprotectportal-config-succ	VPN-Portal-NCC-Production	GlobalProtect portal client configuration generated. Login from: 88.114.52.165, User name: pre-logout, Config name: [REDACTED]

FIGURE 59. Pre-logout user logs in to the computer

In the pre-logout scenario, it is important to secure the end device with a passcode, a password or some other method during the boot process but also use the idle time or smartcards that locks the computer after a certain period of idle time or if the smartcard is removed. If the company already has a strong authentication, it should

not be changed to worse when implementing a VPN solution. Therefore, it is important to implement a password request before boot, which is something the user knows. Then, taking advantage of the machine certificate which is something the user has, which cannot be accessed without a boot password. Alternatively, a smart-card carrying a certificate secured by a PIN code or password in addition to domain credentials can be utilized during the logon or VPN connection or both. Also, the end device's data should be encrypted either partially for confidential and critical data only or entirely.

Pre-logon configuration in the NGFW included a Certification trust parameters configured in the Certification Profile, which was assigned to the Global Protect Portal and the Gateway, as illustrated in Figures 60 and 61.

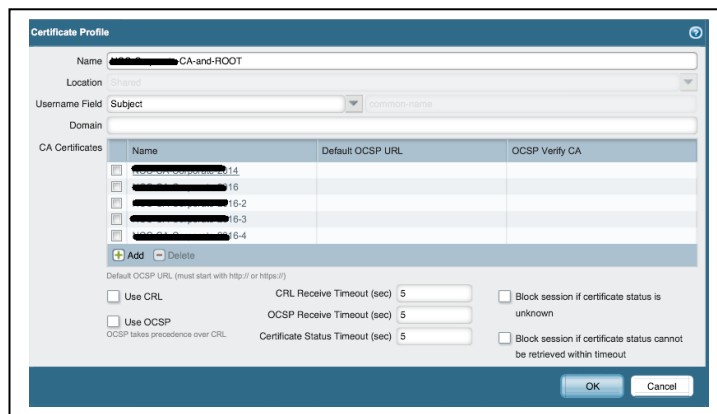


FIGURE 60. Certification Profile defines the trust relationship of the certificates

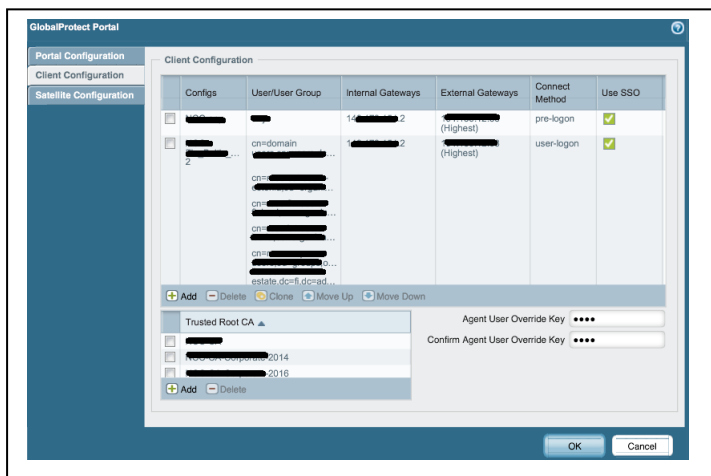


FIGURE 61. Pre-logon and the Trusted Root CA definitions

Pre-logout tests were done in the NCC's environment with a 30-day of trial license, because the test environment did not include a Windows domain and a Certification Service. Therefore the test period was limited to 30 days for pre-logout feature and the PAN-OS version was 5.0.6 and GP Client version was 1.2.5.

4.3.7 QoS Testing

Quality of Service was tested with Youtube application by defining Youtube as class 8 with maximum bandwidth of 1 Mb/s as illustrated in Figure 62.

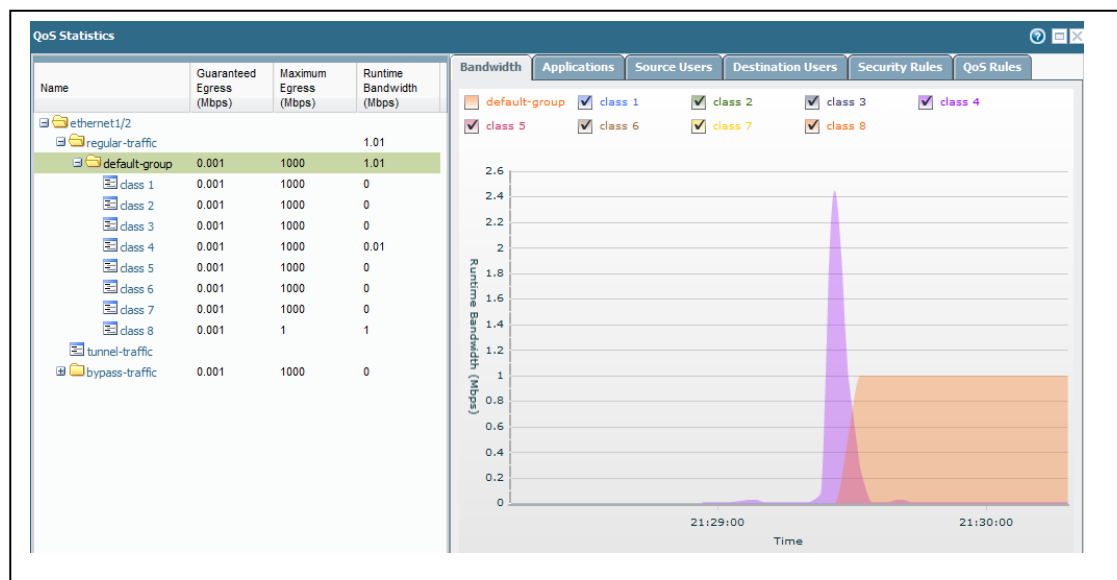


FIGURE 62. QoS example with bandwidth limitation based on application

All the other data are class 4 by default with no maximum bandwidth limitation. Figure 62 illustrates how class 8 cannot exceed 1 Mb/s limit, while class 4 can reach the maximum limit, which is about 2 Mb/s, see the "Runtime Bandwidth" and "Maximum Egress Bandwidth" for both classes. Because of QoS-limit, the downloading will take more time, since bandwidth is less than class 4 with no limit; however, the application is still allowed and fully functional. This helps enterprises to prioritize traffic based on application criticality to guarantee bandwidth to more important applica-

tions while still allowing less important applications in race condition. Figure 63 illustrates how less important applications get less capacity, thus showing in horizontally and more important applications get more capacity and are seen in vertically.

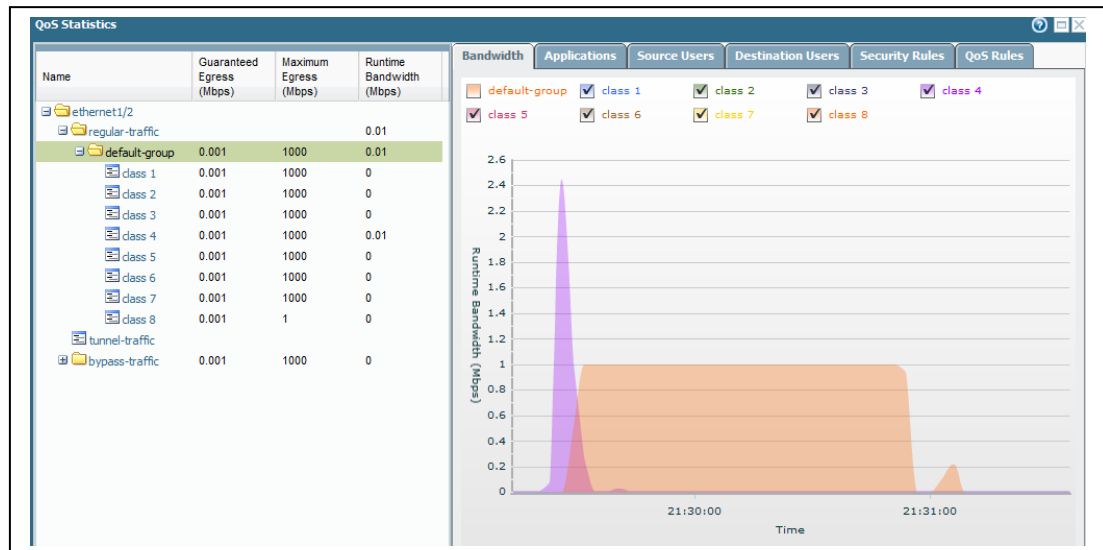


FIGURE 63. Important application gets more bandwidth than less important

4.3.8 Geographical location usage

The use of regions is practical, when limiting traffic from the internet, for remote access users for example, as illustrated in Figure 64. If users are located in the specific countries, they can be allowed and others denied by default. For example, Global Protect gateway can be allowed for IPsec, but portal access can be limited to countries, where company has business or partners. This reduces the noise hitting from the Internet to the perimeter network and false logon attempts to the portal. Combined to the DoS Protection and Zone Protection, it will reduce network scanning, reconnaissance and flooding further.

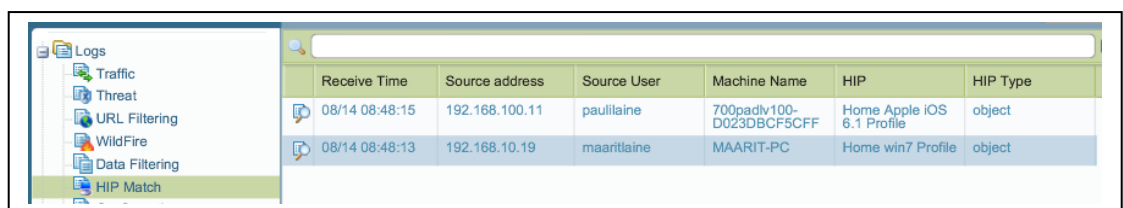
Type	From Zone	To Zone	Source	Source User	Source Country
drop	ADSL	ADSL	199.19.106.225		US
end	ADSL	ADSL	84.230.32.42		FI
end	ADSL	ADSL	84.230.32.42		FI
drop	ADSL	ADSL	190.5.195.24		CO
drop	ADSL	ADSL	162.213.25.40		US
drop	ADSL	ADSL	1.62.100.3		CN
drop	ADSL	ADSL	198.20.69.98		US
drop	ADSL	ADSL	113.107.249.21		CN
end	ADSL	ADSL	84.230.32.42		FI
end	ADSL	ADSL	84.230.32.42		FI
end	ADSL	ADSL	84.230.32.42		FI
end	ADSL	ADSL	84.230.32.42		FI

FIGURE 64. Other regions than Finland are dropped by default, like USA (US)

Drop in the log means dropped connection and end in the log means successful connection.

4.3.9 HIP Matching

HIPs are logged under HIP Match logs, where detailed information of the devices and their appearance times can be seen, as illustrated in figure 65.



Receive Time	Source address	Source User	Machine Name	HIP	HIP Type
08/14 08:48:15	192.168.100.11	paulilaine	700padlv100-D023DBC5CFF	Home Apple iOS 8.1 Profile	object
08/14 08:48:13	192.168.10.19	maartilaine	MAARIT-PC	Home win7 Profile	object

FIGURE 65. HIP logs of remote users' devices

When choosing the first log entry in Figure 56, Apple iPad's HIP information can be seen, as illustrated in Figure 66. It includes userid, assigned VPN IP address and real IP address obtained from the local network, MAC address, device name and OS version.



FIGURE 66. Apple iPad HIP information

Choosing the second log entry, MS Windows7 device HIP information is revealed, as illustrated in Figure 67-69. Just like in Apple iPad, the similar information is revealed, but in case of Windows, all the details about patches, disk encryption, backup etc. are revealed as well and all of this information is available to make use of in the HIP profiles.

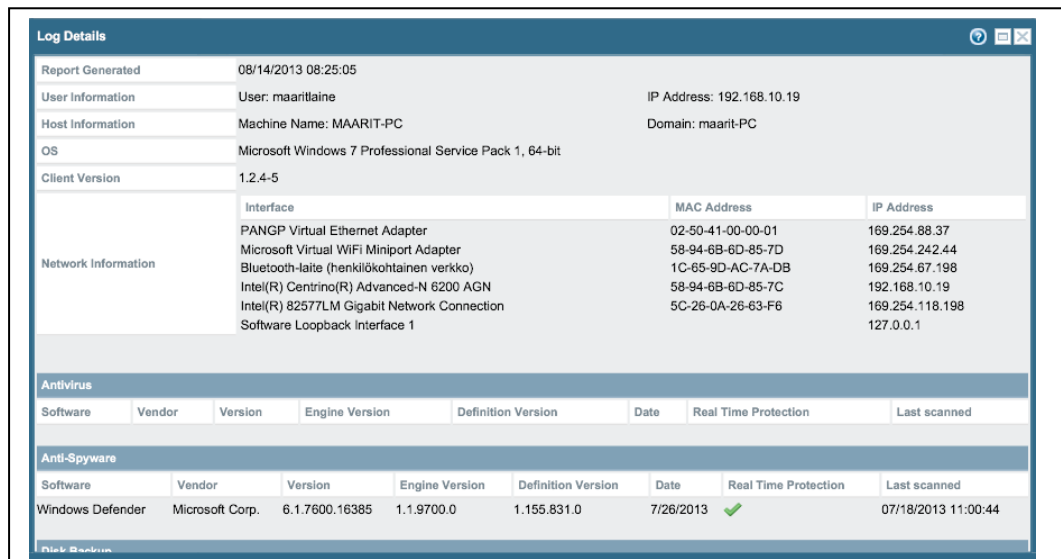


FIGURE 67. MS Windows device HIP information

Log Details			
Disk Backup			
Software	Vendor	Version	Last Backup
Windows Backup and Restore	Microsoft Corp.	6.1.7600.16385	n/a
Disk Encryption			
Software	Vendor	Version	
Firewall			
Software	Vendor	Version	Enabled
Microsoft Windows Firewall	Microsoft Corp.	7	✓
Patch Management			
Software	Vendor	Version	Enabled
Microsoft Windows Update Agent	Microsoft Corp.	7.6.7600.256	n/a
Microsoft Windows AutomaticUpdate	Microsoft Corp.	7.6.7600.256	✓

FIGURE 68 MS Windows device HIP information of FW, encryption and backup

Patch Management			
Software	Vendor	Version	Enabled
Microsoft Windows Update Agent	Microsoft Corp.	7.6.7600.256	n/a
Microsoft Windows AutomaticUpdate	Microsoft Corp.	7.6.7600.256	✓
Missing Patches			
Title	KB Article ID	Severity	
X64-järjestelmien Windows 7:n päivitys (KB2574819)	2574819		
X64-järjestelmien Windows 7:n päivitys (KB2592687)	2592687		
Windows 7 x64 Editionin Platform Update -päivitys (KB2670838)	2670838		
X64-järjestelmien Windows 7 -käyttöjärjestelmän Internet Explorer 10	2718695		
Suojauspäivitys: Microsoft Publisher 2010 (KB2553147) 32-bittinen versio	2553147		2
Suojauspäivitys: Microsoft Visio 2010 (KB2810068) 32-bittinen versio	2810068		2
X64-järjestelmien Windows 7:n tietoturvapäivitys (KB2862966)	2862966		
X64-järjestelmien Windows 7:n tietoturvapäivitys (KB2861855)	2861855		
X64-järjestelmien Windows 7:n tietoturvapäivitys (KB2868623)	2868623		2
X64-järjestelmien Windows 7:n tietoturvapäivitys (KB2849470)	2849470		2
X64-järjestelmien Windows 7:n tietoturvapäivitys (KB2859537)	2859537		2
X64-järjestelmien Windows 7 R2 SP1:n ja Windows Server 2008:n Microsoft .NET Framework 3.5.1:n tietoturvapäivitys (KB2844286)	2844286		
X64-järjestelmien Windows 7:n Internet Explorer 9:n koottu tietoturvapäivitys (KB2862772)	2862772		3
X64-järjestelmien Windows 7:n päivitys (KB2863058)	2863058		
X64-järjestelmien Windows Server 2008 R2:n, Windows Server 2008:n, Windows 7:n, Windows Vistan, Windows Server 2003:n ja Windows XP:n	2840628		2
Microsoft .NET Framework 4:n tietoturvapäivitys (KB2840628)	2840628		
X64-järjestelmien Windows 7:n tietoturvapäivitys (KB2803821)	2803821		3
Windowsin haittaohjelmien poistotyökalu (x64), elokuu 2013 (KB890830)	890830		

FIGURE 69. MS Windows device HIP information of patch management

HIP information was tested in the security policy as follows: Security policy was generated allowing management access to the NFGW and Aruba management interface by defining also certain devices in the HIP column in the “Admin HIP to MGMT” rule. After the rule was tested to work, as illustrated in Figure 70, then additional “Deny MGMT Rest” rule was added to deny the rest of the traffic to the management, as illustrated in Figure 71. The security police operated logically with the rules and Android device could not log in to the management console after the security policy was committed, since only Apple’s iOS 6.1 and Windows7 were allowed.

Log Details										
General		Time								
Session ID	14132	IP Protocol	tcp							
Type	end	Log Action								
Action	allow	Bytes	5,635							
Application	ssl	Bytes Received	3,865							
Rule	Admin HIP to Aruba gw	Bytes Sent	1,770							
Category	private-ip-addresses	Repeat Count	1							
Virtual System	vsys1	Packets	24							
Device	0[REDACTED]486	Packets Received	10							
		Packets Sent	14							
Source		Destination								
Source User	paullaine	Destination User								
Source address	192.168.100.11	Destination address	192.168.12.11							
Source Country	192.168.0.0-192.168.255.255	Destination Country	192.168.0.0-192.168.255.255							
Source Port	61068	Destination Port	4343							
Source Zone	VPN	Destination Zone	Koti							
Inbound Interface	tunnel.1	Outbound Interface	ethernet1/2							
Related Logs (+/- 24 Hours)										
Receive Time	Log	Type	Application	Action	Rule	Bytes	Packets	Severity	Category	URL / Filename
08/14 09:15:39	traffic	end	ssl	allow	Admin HIP to Aruba gw	5,635	24			

FIGURE 70. A log entry of a successful management connection with HIP enabled

Admin HIP to MGMT	none	VPN	any	any	Admin-pad	ADSL	Aruba-instant-gw	ssl	any	✓
Deny MGMT rest	none	VPN	any	any	Admin-win7	Koti	Palo Alto MGMT...	web-browsing	any	✗
..										
DenyRest	none	ADSL	any	any	any	ADSL	Aruba-instant-gw	any	any	✗
		VPN				Koti	Palo Alto MGMT...			

FIGURE 71. Security Policy leveraging the HIP information for management access

4.3.10 Threat Identification

Threats are identified using dynamic updates from Palo Alto and criterions are defined based on the threats' risk levels (severities), threat types or individual threat IDs. Those criteria can then be grouped to a Profile and are leveraged in the Security Policy's Profiles in each Security Rule. Different threat Profiles are:

- Antivirus (using following decoders: FTP, HTTP, IMAP, POP3, SMB, SMTP)
- Anti-Spyware (can be customized in addition to dynamic updates)
- Vulnerability Protection (in CVE-database format)
- URL Filtering (using Palo Alto's database or Bright Cloud's database)

- File Blocking (can be used to send to the WildFire Cloud)
- Data Filtering (using regex-format)
- DoS Protection (flood and resource protection).

Figure 72 illustrates Threat, WildFire, Global Protect and Application updates that are used in the Threat Profiles.

Version	File Name	Features	Type	Size	Release Date	Download...	Currently Installed	Action	Documen...	
Antivirus Last checked: 2013/08/02 06:57:25 Schedule: Every day at 05:30 (download-and-install)										
1070-1491	panup-inc-antivirus-1070-1491		Incremental	12 MB	2013/08/01 09:50:01	✓	✓		Release Notes	✕
1069-1490	panup-inc-antivirus-1069-1490		Incremental	13 MB	2013/07/31 13:41:55	✓ previously		Revert	Release Notes	✕
Applications and Threats Last checked: 2013/08/02 06:57:21 Schedule: Every day at 05:45 (download-and-install)										
386-1889	panupv2-all-contents-386-1889	Apps, Threats	Full	18 MB	2013/07/30 15:08:40	✓	✓		Release Notes	✕
385-1883	panupv2-all-contents-385-1883	Apps, Threats	Full	18 MB	2013/07/23 13:12:11	✓ previously		Revert	Release Notes	✕
GlobalProtect Data File Schedule: Every day at 01:00 (download-and-install)										
WildFire Last checked: 2013/08/02 07:00:54 Schedule: Every 30 Minutes (download-and-install)										
17511-23290	panup-all-wildfire-17511-23290		Full	3 MB	2013/08/01 20:49:01	✓	✓		Release Notes	✕

FIGURE 72. Scheduled dynamic updates

All of these include individual signatures that can be included or excluded from the profiles or defined with another criterion like a threat's severities which all have similar behaviors, like block or allow. These properties have been illustrated in Figures 73-75.

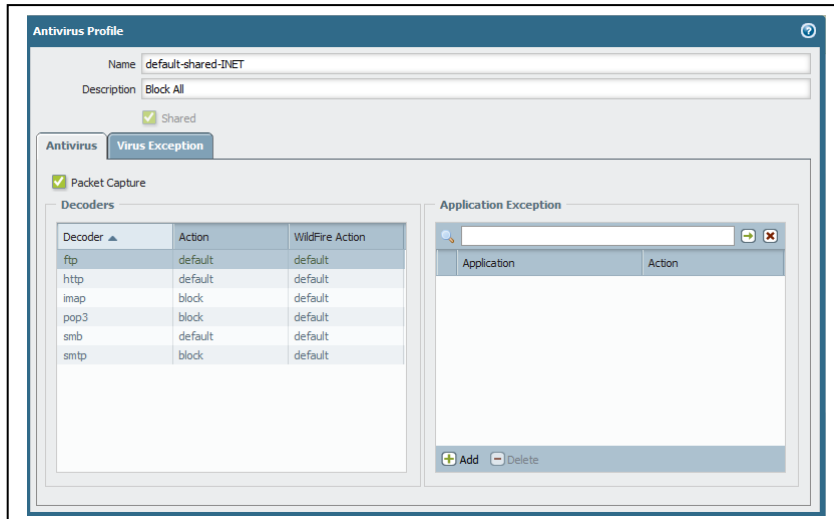


FIGURE 73. Antivirus profile with default and block definitions

Default actions means, that every threat ID has a default action based on the behavior: The more serious the threat, the stricter the default action. It can also be selected manually as allow, alert, block or default.

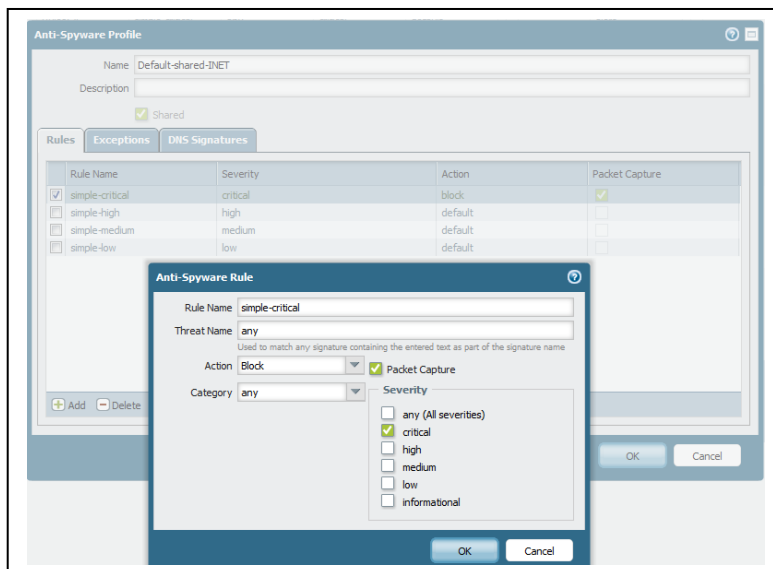


FIGURE 74. Anti-Spyware profile with criterion that blocks all critical threats

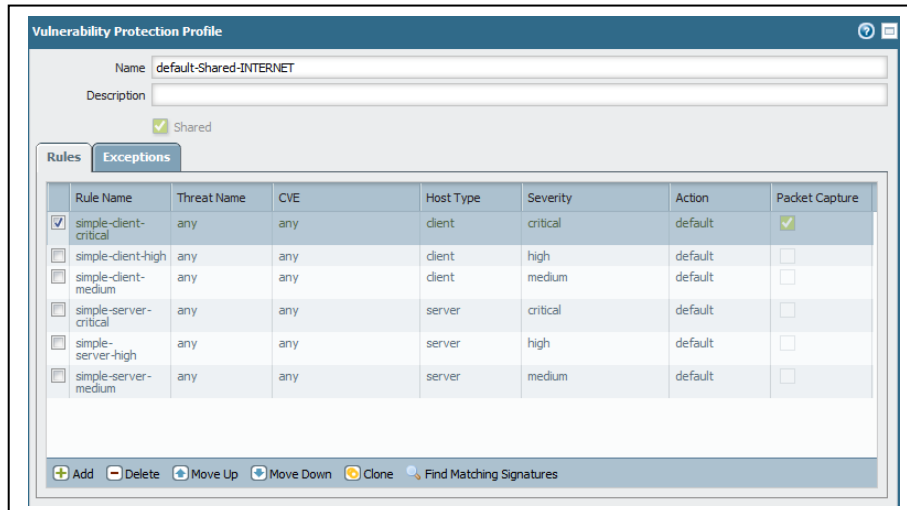


FIGURE 75. Vulnerability Protection profile where critical threats are captured

It is important to remember that in every Profile's Action criteria, Alert means that traffic is allowed and logged, whereas Allowed means allowed, but not logged. So Alert should be always used for allowed traffic to get the log entries, unless specifically not wanted to log traffic. An example of URL Filtering Profile is illustrated in Figure 76.

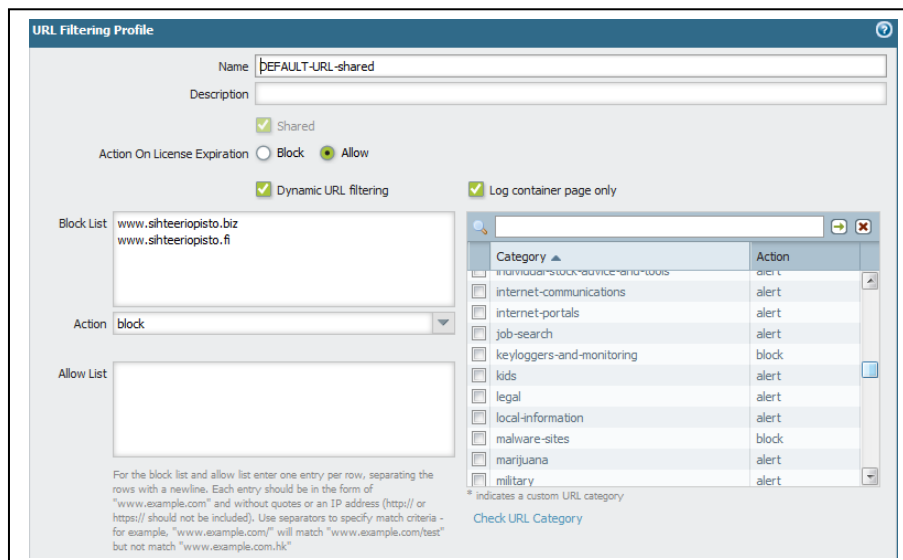


FIGURE 76. URL Filtering with blocked and logged (alert) categories

URL-Filtering uses Bright Cloud or Palo Alto Networks databases. During the past year (24.8.2012 – 30.8.2013) at NCC using Bright Cloud database, 22 false categorized web sites were found that prevented business traffic. They were all categorized as adult-and-pornography category, which they were not. Comparing these sites to Palo Alto Network's database, it categorized 11 of these to right – or close to right – category and 11 for unknown category. Unknown means that the database does not know the category yet, but it will be categorized by the cloud after a while and will be recognized in the future updates and will be pushed to the client by the vendor. In addition, four sites were found to be suspicious: two of them as malware sites and another two for spam sites. One of the spam sites was asked to be re-categorized since it was needed by the business and it was changed to the business-and-economy category. All of these sites were located in Russia, Estonia, Latvia and Finland.

File Blocking and URL Categories work in a similar way as the previous threat protection profiles; however File Blocking Profile also includes the possibility to send the file to the WildFire Cloud, see Figure 77. This should be used as default behavior in Internet traffic, whereas internal traffic may not want to be sent to the cloud, but all the other protection mechanisms should be used internally. As a rule of thumb, all internet-related critical threats in every profile should be blocked packet captured and send to the WildFire if possible. Internally, all critical threats should be blocked, except vulnerabilities may want to be left as alert, instead of blocking mode at least some part of the internal network. This depends somewhat on the company's segmentations, like server's criticalities, DMZ traffic's criticalities and business applications.

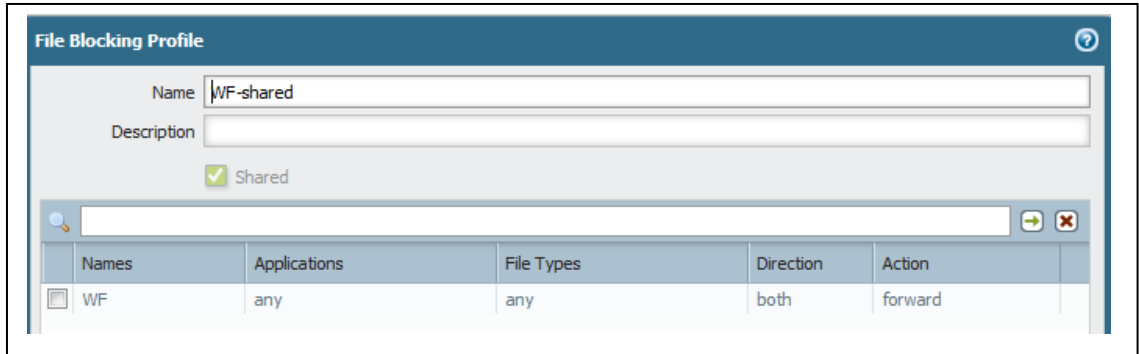


FIGURE 77. File Blocking Profile with all files sent to the WildFire for analysis

Data Filtering is about administrator defined regex strings that can be used as filters in different kind of traffic. Data Pattern for “Luottamuksellinen” (“Confidential”) is illustrated in the Data Filtering Profile in Figure 78. These filters can then be used to block, allow, packet capture and alert desired groups of peoples.

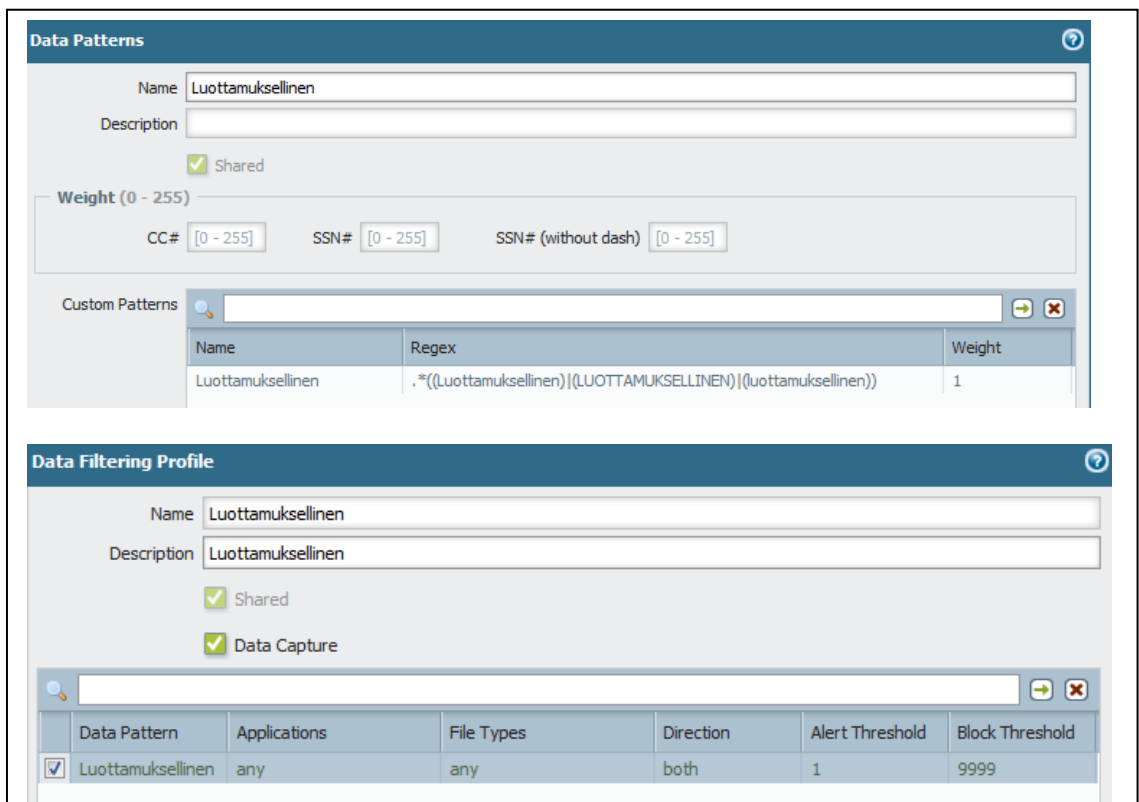


FIGURE 78. Data Pattern in the Data Filtering Profile

Once the Security Profiles are defined, they can be activated in the Security Rules. Different Profiles should be created for at least Internal, DMZ and External (Internet) traffic for easier management of different needs. In Figure 79 there is an example of security rule for Internet traffic, where allowed applications are in one application group and a “Tuotanto-INTERNET” Security Group that consists of Security Profiles of all of the threats: Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking and Data Filtering. DoS Protection needs to be defined in a different Security Policy and cannot be added into the Security Group Profile.

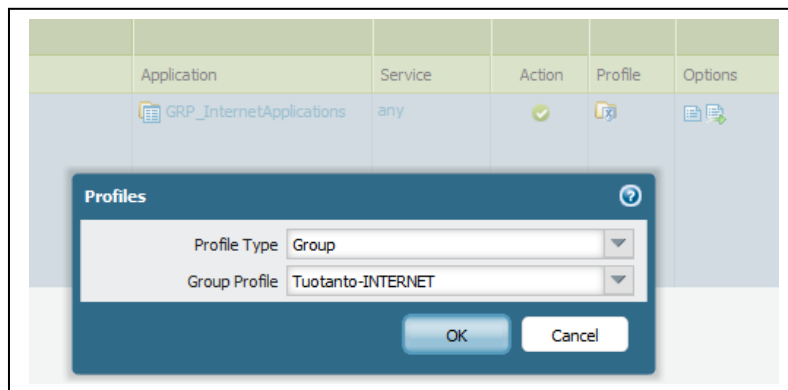


FIGURE 79. Security Group that includes all Security Profiles for Internet traffic

4.3.11 WildFire Reports during the Test Period

After the test environment was set up including WildFire functionality, the ADSL Router was updated to the latest firmware, since it was jamming (halted) regularly. During the search of the latest firmware from the Internet, the following WildFire log entries were encountered at 7th of June 2013, see Figure 80.

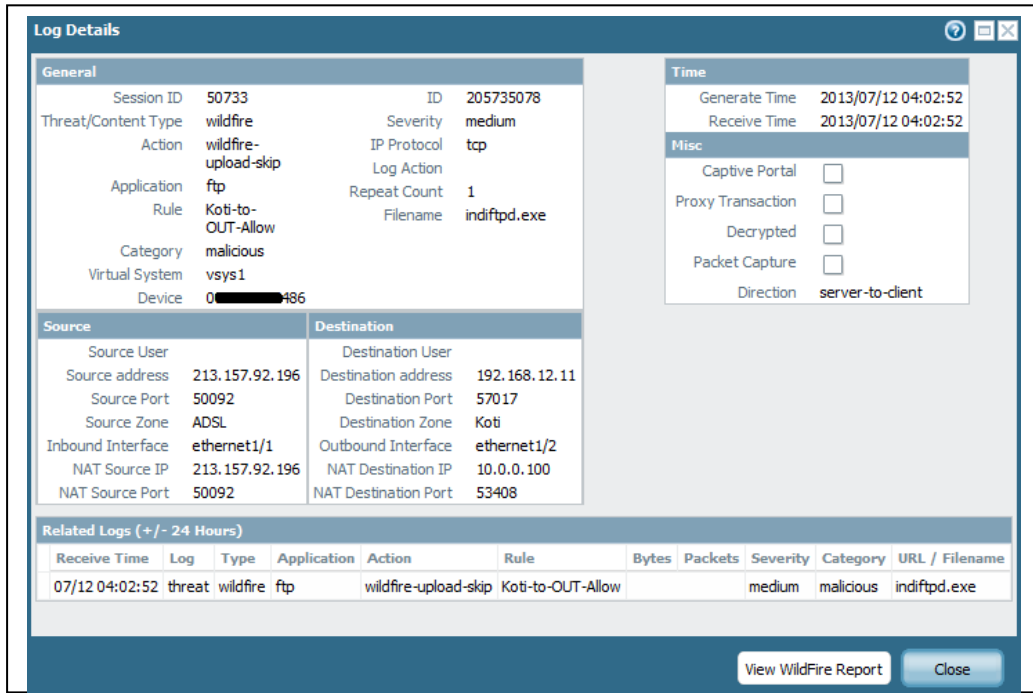


FIGURE 80. Malicious file detected from the traffic

When the log details were further analyzed, the indiftpd.exe file included several files with pv.exe file and a virus in it, called a Win32.neshta.bxs detected at 2nd May 2013, see Figure 81.

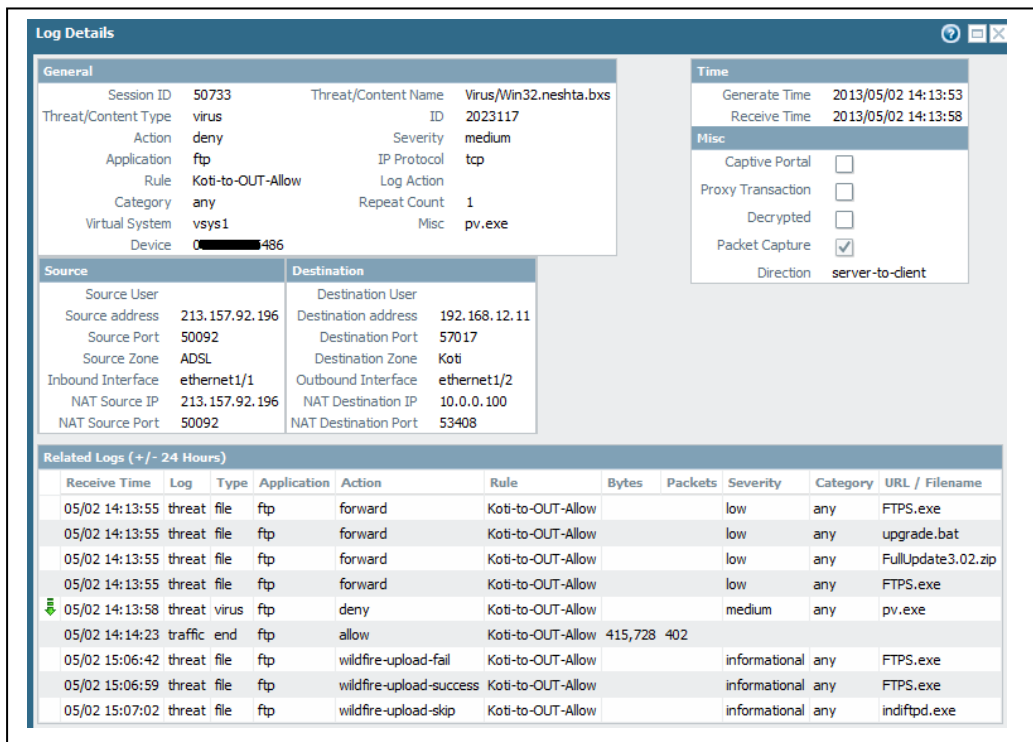


FIGURE 81. Pv.exe contains a malicious file

A packet capture was defined to all critical threats, thus the content can be seen in the NGFW GUI or exporting the network traffic using the Export button, see Figure 82. Exported file is pcap-format which can be viewed with packet capture programs, like Wireshark, for example. Packet capture captures packets only until traffic is terminated by the NGFW, therefore only first packets are captured. If the traffic is configured to allow or alert, then more packets are captured.

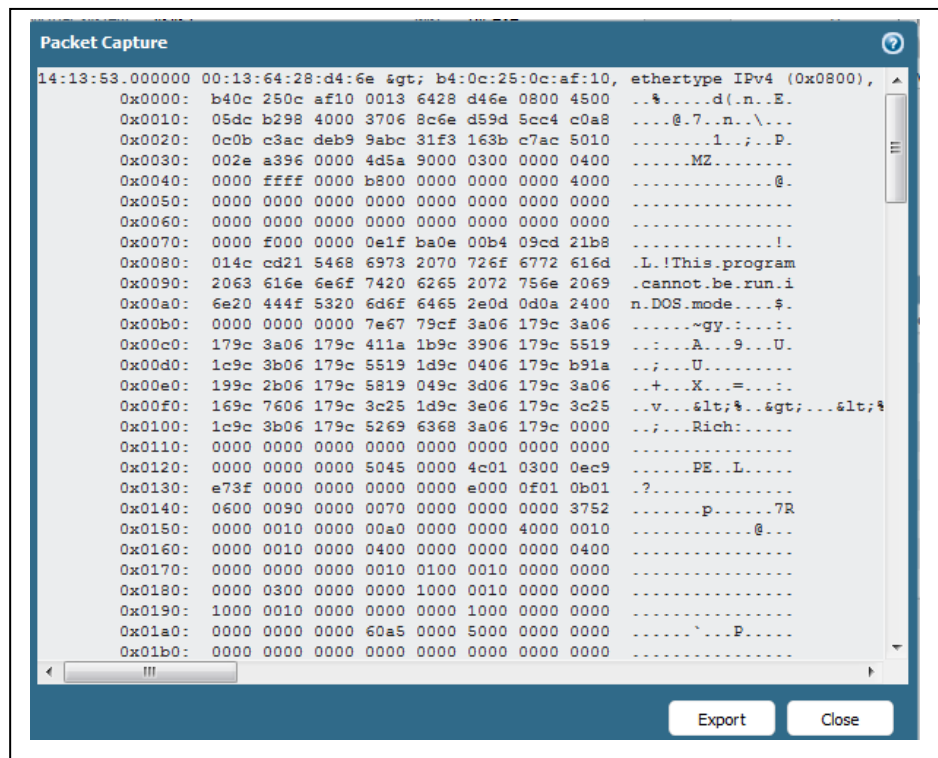


FIGURE 82. Content of the pv.exe

In Figure 83 is the analysis result of the Win32.neshta.bxs. It creates an executable file in the windows folder, which is seen as the most severe threat behavior in this case. All the other behaviors are not malicious and therefore this particular case can be a false positive alert. However, this report is not detailed enough to decide whether it is reliably a virus or not, even there seems to be some malicious behavior.

Virus/Win32.neshta.bxs

Overview

Virus Name	Virus/Win32.neshta.bxs
SHA - 256	c16c2a83aca467bc7954536ca41f61a0fc8a7b6da473555c9fa620422a4a6661
MD5	efcd1c0f3fd7241545fea6b739517cfb
Content Release	
Virus Total	Virus Coverage Information

Behavior Summary

This malware exhibited the following behaviors :

Behavior	Severity
Created or modified files	
Spawned new processes	
Modified WINDOWS registries	
Created an executable file in Windows folder	
Created an executable file in an user document folder	

Process Activity

Process	Parent Process	Action
C:\sample.exe	UNKNOWN	Create
C:\sample.exe	explorer.exe	Create
C:\sample.exe	explorer.exe	Terminate
C:\WINDOWS\system32\userinit.exe	C:\WINDOWS\system32\winlogon.exe	Terminate

File Activity

File	Process	Action
C:\Documents and Settings\Administrator\Application Data\Wplugin.dll	C:\sample.exe	Write
C:\WINDOWS\Wplugin.dll	C:\sample.exe	Write

Registry Modifications

Registry Key	Action
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData	Set

FIGURE 83. Overview of the Win32.neshta.bxs file

To present more confidence and reference to the inspected file, WildFire integrates directly to the Virustotal.com service. Virustotal will compare the result of the given hash of the sample file to its own database. Its database has the information of total 44 of different AV vendors and whether they can detect the file, and if they can then what the signature version is. Figure 84 illustrates how many vendors detect the file (hash) at 13th August 2013.

virustotal

SHA256: c16c2a83aca467bc7954536ca41f61a0fc8a7b6da473555c9fa620422a4a6661

File name: efdc1c0f3fd7241545fea6b739517cfb

Detection ratio: 37 / 44

Analysis date: 2011-09-25 04:53:17 UTC (1 vuosi, 10 kuukautta ago)

[More details](#)

FIGURE 84. 37 AV vendors out of 44 detects the sample file (hash)

Even though the file has been in the database since one year and 10 months, still not all AV vendors can detect it, see Figures 85 and 86.

Analysis File detail Additional information Comments Votes

File identification

MD5	efcd1c0f3fd7241545fea6b739517cfb
SHA1	d8436c6611c3adbb11e7ed96eab8f9c574c1de74
SHA256	c16c2a83aca467bc7954536ca41f61a0fc8a7b6da473555c9fa620422a4a6661
ssdeep	1536:FzdED/TLhhJmaTnUJzoS2RvuFFDUIYkK4cEui1gNNx0eW6QPB/4ZW1ck8zHhTdu8:k7Y2nUJzoihYZ4z1sxtbjUWnoRzNj
File size	152.5 KB (156131 bytes)
File type	Win32 EXE
Magic literal	
TRiD	Win64 Executable Generic (59.6%) Win32 Executable MS Visual C++ (generic) (26.2%) Win32 Executable Generic (5.9%) Win32 Dynamic Link Library (generic) (5.2%) Generic Win/DOS Executable (1.3%)
VirusTotal metadata	
First submission	2011-09-25 04:53:17 UTC (1 vuosi, 10 kuukautta ago)
Last submission	2011-09-25 04:53:17 UTC (1 vuosi, 10 kuukautta ago)
File names	efcd1c0f3fd7241545fea6b739517cfb

FIGURE 85. First and last submission of the hash

Many of the AV vendors have named the malware as “Slugin”, as seen in Figure 86. The green spot under the Result indicates that the AV vendor does not recognize the

variant or it considers it as benign and name of the variant indicates that the vendor detects the variant.

Antivirus	Result	Update
AhnLab-V3	Win32/Slugin	20110924
AntiVir	W32/Slugin.A	20110923
Antiy-AVL	☑	20110924
Avast	Win32:Patched-HO [Trj]	20110924
Avast5	Win32:Patched-HO [Trj]	20110924
AVG	Win32/Slugin.A	20110924
BitDefender	Win32.Slugin.A	20110925
ByteHero	☑	20110923
CAT-QuickHeal	W32.Slugin.A	20110924
ClamAV	Trojan.Spy-59563	20110925
Commtouch	W32/Slugin.B	20110924
Comodo	TrojWare.Win32.Patched.Q	20110925
DrWeb	Win32.Wplugin.2	20110925
Emsisoft	Trojan.Win32.Patched!IK	20110925
eSafe	☑	20110920
eTrust-Vet	Win32/Slugin.A	20110923
F-Prot	W32/Slugin.B	20110924

FIGURE 86. Different AV vendors detect or do not detect the malware sample

37 out of 44 AV vendors detects the file and identifies it either a Trojan Horse or a Virus and only 7 AV vendors do not recognize it or considers it benign. According to both WildFire and Virustotal analysis information, it is reasonable to believe that this particular file is a malware.

When inspecting the Palo Alto Networks Threat Database with the identified malware ID: 2023117 again at 22nd November 2013, the name of the variant has changed from Win32.neshta.bxs to Trojan/Win32.llac.nar with the new WildFire content release version of 1143 dated as 8th November 2013, see Figures 87-89. Figure 87 illustrates the behavior that has been detected with recent WildFire analyze. The file attempts to modify system registry entries and system configuration to enable auto-start capability, which is seen questionable behavior (yellow). It also change Internet

Explorer settings and inject code to another process, which is definitely a malicious behavior.

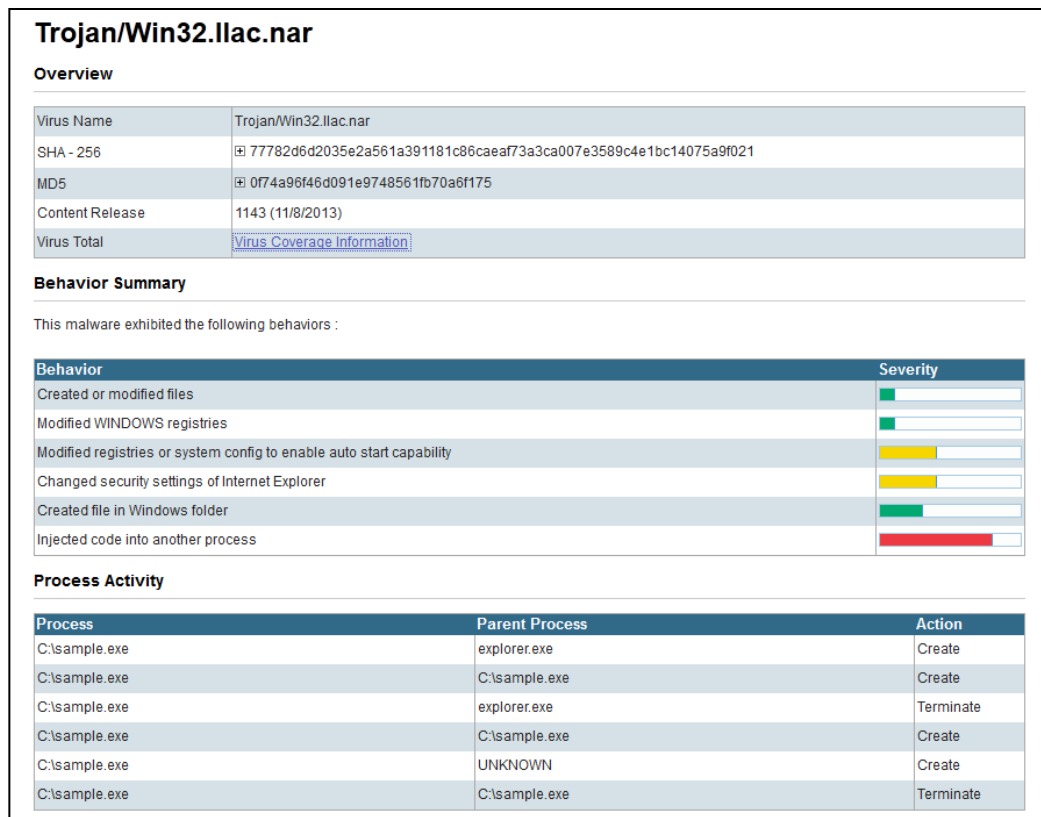


FIGURE 87.

Figure 88 illustrates file activity of the sample, including writing files to the temp, root, Windows and Windows Systems folders and also a Facebook icon file. At the end some of the temp folder's files are deleted. The file (sample) and hashes are different than in the previous analysis, since WildFire analysis has been done to another file with identical behavior and the behavior and virus definition has been updated accordingly.

File Activity		
File	Process	Action
C:\Documents and Settings\Administrator\Local Settings\Temp\XX--XX--XX.bt	C:\sample.exe	Write
C:\Documents and Settings\Administrator\Local Settings\Temp\XX--XX--XX.bt	C:\sample.exe	Delete
C:\Documents and Settings\Administrator\Local Settings\Temp\XX.XX	C:\sample.exe	Write
C:\Documents and Settings\Administrator\Local Settings\Temp\7483-ico-facebook-icon.ico	C:\sample.exe	Write
C:\Documents and Settings\Administrator\Local Settings\Temp\Uu.U.Uu	C:\sample.exe	Write
C:\Documents and Settings\Administrator\Local Settings\Temp\Uu.U.Uu	C:\sample.exe	Delete
C:\Documents and Settings\Administrator\Local Settings\Temp\IWEB.abc	C:\sample.exe	Write
C:\Documents and Settings\Administrator\Local Settings\Temp\XX.XX	C:\sample.exe	Delete
C:\WINDOWS\system32	C:\sample.exe	Write
C:\WINDOWS	C:\sample.exe	Write
C:\	C:\sample.exe	Write
C:\Documents and Settings\Administrator	C:\sample.exe	Write
C:\Documents and Settings\Administrator\Local Settings	C:\sample.exe	Write
C:\Documents and Settings\All Users	C:\sample.exe	Write
C:\Program Files	C:\sample.exe	Write
C:\WINDOWS\system32\CatRoot2	C:\sample.exe	Write
C:\WINDOWS\WinSxS	C:\sample.exe	Write
C:\Documents and Settings\Administrator\Cookies	C:\sample.exe	Write
C:\Documents and Settings\Administrator\Local Settings\History\History.IE5	C:\sample.exe	Write
C:\Documents and Settings\Administrator\Application Data	C:\sample.exe	Write
C:\WINDOWS\SoftwareDistribution	C:\sample.exe	Write

FIGURE 88.

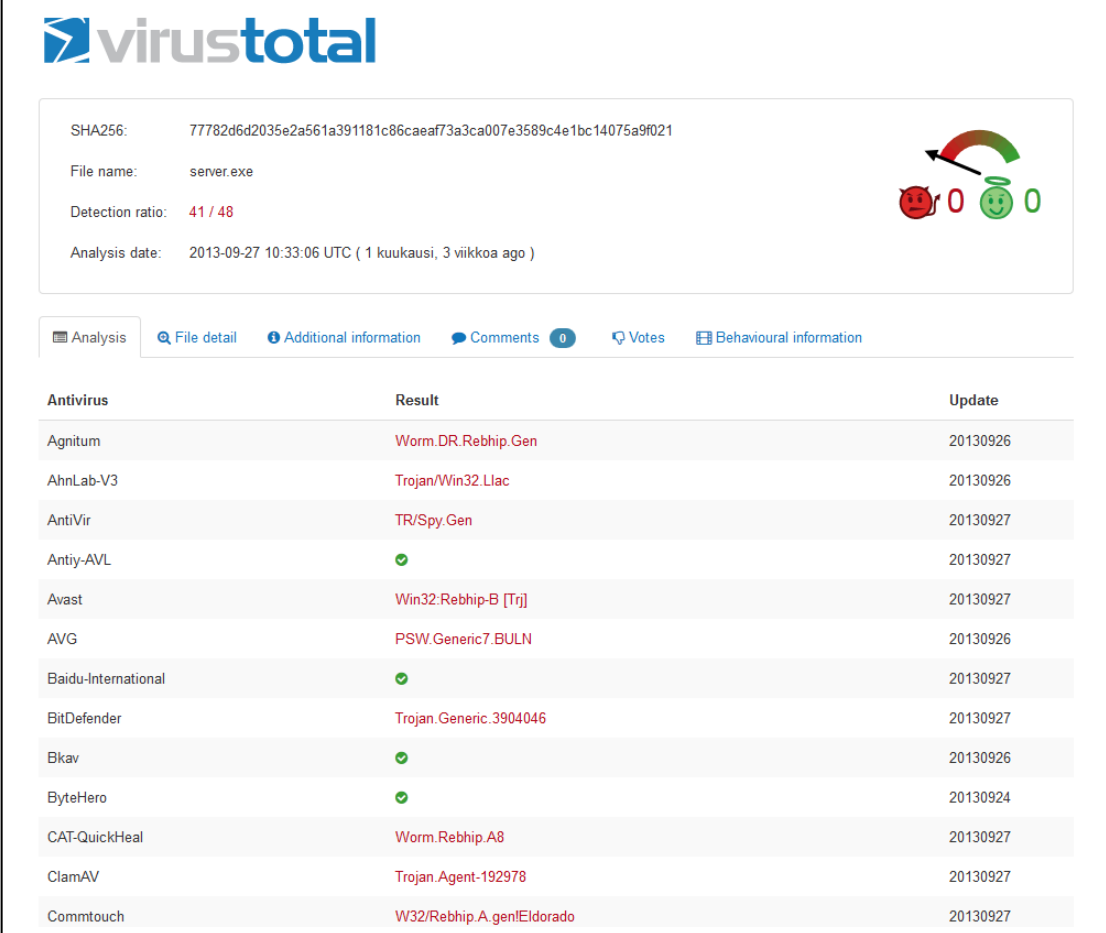
Figure 89 illustrates registry modifications including Internet Explorer's settings, as informed in the Behavior section in Figure 87 "Changed security settings of Internet Explorer" and "Modified Windows Registries".

Registry Modifications	
Registry Key	Action
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Personal	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{e86064ca-57e4-11e0-bef8-806d6172696f}\BaseClass	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Documents	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Desktop	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Desktop	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cookies	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{e86064ca-57e4-11e0-bef8-806d6172696f}\BaseClass	Set
HKCU\Software\admin\NewIdentification	Set
HKCU\Software\admin\NewGroup	Set
HKCU\Software\admin\FirstExecution	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Personal	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Documents	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Desktop	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Desktop	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cookies	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common AppData	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cookies	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\History	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Policies	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Policies	Set
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{FEYUO60N-1275-0F82-28U0-5N1JEI724261}\StubPath	Set

FIGURE 89. Detailed registry setting's modification

Updated WildFire analysis (content release version 1143) is more precious than earlier content release and now it clearly shows that the submitted file is a malware. This information can be compared to the Virustotal information again to get some reference to the analysis. See Figures 90-93 of the result of the Virustotal database.

Figure 90 illustrates the detection ratio with 41 AV vendors out of 48 detects the malicious file as Trojan Horse or a Virus while only 7 vendor does not recognize it or considers it as benign. The file has been re-analyzed, since analysis date has changed to one month and three weeks ago.



SHA256: 77782d6d2035e2a561a391181c86caaf73a3ca007e3589c4e1bc14075a9f021

File name: server.exe

Detection ratio: 41 / 48

Analysis date: 2013-09-27 10:33:06 UTC (1 kuukausi, 3 viikkoa ago)

Analysis | File detail | Additional information | Comments 0 | Votes | Behavioural information

Antivirus	Result	Update
Agnitum	Worm.DR.Rebhip.Gen	20130926
AhnLab-V3	Trojan/Win32.LIac	20130926
AntiVir	TR/Spy.Gen	20130927
Antiy-AVL	✓	20130927
Avast	Win32.Rebhip-B [Trj]	20130927
AVG	PSW.Generic7.BULN	20130926
Baidu-International	✓	20130927
BitDefender	Trojan.Generic.3904046	20130927
Bkav	✓	20130926
ByteHero	✓	20130924
CAT-QuickHeal	Worm.Rebhip.A8	20130927
ClamAV	Trojan.Agent-192978	20130927
Commtouch	W32/Rebhip.A.genIEldorado	20130927

FIGURE 90. Virustotal database results for given file (hash)

The file has been re-analyzed and the behavior has updated but also the first and last submission has been changed, as illustrated in Figure 91.

Analysis		File detail	Additional information	Comments	Votes	Behavioural information
File identification						
Md5	074a96f46d091e9748561fb70a6f175					
SHA1	eecd1b6c8550b562850203b71e225fcb58ec666					
SHA256	77782d6d2035e2a561a391181c86caea73a3ca007e3589c4e1bc14075a9f021					
ssdeep	12288:0UD6jbQGafZyaM8b0QcYqGLyWSKaAS79MEqfGe:0UDaP41MddY/jiSZgfGe					
File size	518.0 KB (530432 bytes)					
File type	Win32 EXE					
Magic literal	PE32 executable for MS Windows (GUI) Intel 80386 32-bit					
TrID	Win32 Executable (generic) (42.5%) Win16/32 Executable Delphi generic (19.5%) Generic Win/DOS Executable (18.9%) DOS Executable Generic (18.8%) Autodesk FLIC Image File (extensions: flc, flt, cel) (0.0%)					
Tags	peexe					
VirusTotal metadata						
First submission	2013-09-27 10:33:06 UTC (1 kuukausi, 3 viikkoa ago)					
Last submission	2013-09-27 10:33:06 UTC (1 kuukausi, 3 viikkoa ago)					
File names	server.exe					

FIGURE 91. First and last submission of the file

The Virustotal's behavioral information identifies the malicious activity as well, as illustrated in Figure 92 and 93. Figure 92 illustrates the Code Injection activity and identifies the injected file as explorer.exe (run also as explorer process) with malicious file's own spawned file and process that it creates in the Created Processes, Opened Files and Read Files section. The Shell command seems not working with the virtual system which made the analysis, since the result of the shell command is failed. Figure 93 illustrates UDP traffic to an IP address that indicates communication traffic which usually is directed to Command and Control (C&C) server to confirm that the client is compromised and ready to serve the C&C server.

Opened files

- C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\XX--XX.txt (successful)
- C:\77782d6d2035e2a561a391181c86caef73a3ca007e3589c4e1bc14075a9f021 (successful)

Read files

- C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\XX--XX.txt (successful)
- C:\77782d6d2035e2a561a391181c86caef73a3ca007e3589c4e1bc14075a9f021 (successful)

Written files

- C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\XX--XX.txt (successful)

Created processes

- C:\77782d6d2035e2a561a391181c86caef73a3ca007e3589c4e1bc14075a9f021 (successful)

Shell commands

- (open) C:\77782d6d2035e2a561a391181c86caef73a3ca007e3589c4e1bc14075a9f021 [(null)] (failed)

Code injections in the following processes

- explorer.exe (successful)
- 77782d6d2035e2a561a391181c86caef73a3ca007e3589c4e1bc14075a9f021 (successful)

Created mutexes

- _x_x_UPDATE_x_x_ (successful)
- _x_x_PASSWORDLIST_x_x_ (successful)
- _x_x_BLOCKMOUSE_x_x_ (successful)
- M40S1YULC5WIUK (successful)
- M40S1YULC5WIUK_PERSIST (successful)
- M40S1YULC5WIUK_SAIR (successful)

Opened mutexes

- ShimCacheMutex (successful)

FIGURE 92. Behavior information

Q Searched windows

CLASS: Shell_TrayWnd
NAME: (null)

Runtime DLLs

- kernel32.dll (successful)
- advapi32.dll (successful)
- user32.dll (successful)
- avicap32.dll (successful)
- gdi32.dll (successful)
- gdiplus.dll (successful)
- mpr.dll (successful)
- msacm32.dll (successful)
- ntdll.dll (successful)
- ole32.dll (successful)

Show all

UDP communications

64.4.10.33:123

FIGURE 93. UDP traffic

These two analyses of the same threat ID provided by the Palo Alto Networks threat database together with Virustotal's database analysis information illustrates the constantly changing threat landscape that the companies are facing on a daily basis. Threats are changing and new signatures and behavior are constantly analyzed, compared and behavior and threat databases are updated to match the recent results. The behavior based analysis and threat information sharing between parties are essential for detecting and preventing zero-day attacks and constantly changing threats. Automatically generated information; e.g. statistics and results of analyses from sandboxed and virtualized environments with different set of OS and software installed that are delivered to the companies, are definitely valuable for identifying threats. They are also a competitive advantage among competitors.

Some general WildFire statistics were taken from the production environment in NCC Finland's network during the past year at 24.8.2012 – 30.8.2013.

Total number of samples:	2294	(100%)
Number of malware samples:	326	(14%)
Number of benign samples:	1968	(86%)

Four different anomalies separated from the samples represented a total of 154 samples. Those were compared to Virustotal's AntiVirus database to see how many AV vendors detect those threats after one year's period, on 30th August 2013.

Anomaly 1, time of occurrence: 24.8.-30.8.2012.

Method: SMTP (email)

AV coverage by vendor per variants: 34/42, 39/46, 42/46 (detected/total vendors)

Number of samples: 11

Behavior: Similar threats (malware) were sent via email using three different variants with similar behavior. They all tried to trick a user to click a link or open the attachment disguised as Adobe's PDF (Portable Document Format)-document but was actually executable file format (.exe), which would have infected the client and downloaded some more malware from identified malware domains, if succeeded in infecting the client. These samples were detected four days after WildFire functionality was taken into production, so they may have been seen before WildFire was in use.

Anomaly 2, time of occurrence: 27.8.-12.10.2012

Method: Web browsing (using browser)

AV coverage by vendor per variants: 28/40, 16/40

Number of Samples: 58

Behavior: Two variants tried to infect client machines using the server side scripting language in the destination server. If successful, it would run an executable file in the client's document folder, spawned new processes, created a backdoor, deleted itself,

inject code to another process, registered a file as auto-start from a local directory, modified IE settings and several other unwanted behavior.

Anomaly 3, time of occurrence: 23.-30.10.2012

Method: SMTP (email)

AV coverage by vendor per variants: 42/47, 43/46, 42/47, 40/45, 40/45, 39/46

Number of samples: 74

Behavior: six variants tried to infect client using an attachment in the email that would have stolen the saved passwords of the FireFox. The attachment appeared to be an Adobe PDF document, but it was actually an executable file.

Anomaly 4, time of occurrence: 16.1.-28.1.2013

Method: Web browsing (using browser)

AV coverage by vendor per variants: 32/46, 32/46, 30/46, 28/46, 33/44

Number of samples: 11

Behavior: five variants tried to infect clients by serving a malware in the web server. If the client enters the infected web site, the executable file is downloaded and executed in the user document folder. If succeed, then new processes are spawned, the code is injected to another processes, IE settings are affected, FireFox passwords are stolen, it visits malware sites and attempts to sleep for a long period of time.

Anomalies number one and three represents threats sent to the user through email with a malicious attachment or link included. It is worthwhile to mention the ThreatSim's phishing-for-hire campaigns (Verizon, 2013, 38). It states that running with three emails grants the attacker more than 50% possibility of getting at least one click. Running that campaign twice and the probability rises up to 80%, and sending 10 phishing emails will almost guarantee on getting a click. The inevitability of a click is illustrated in Figure 94. (Verizon, 2013, 38).

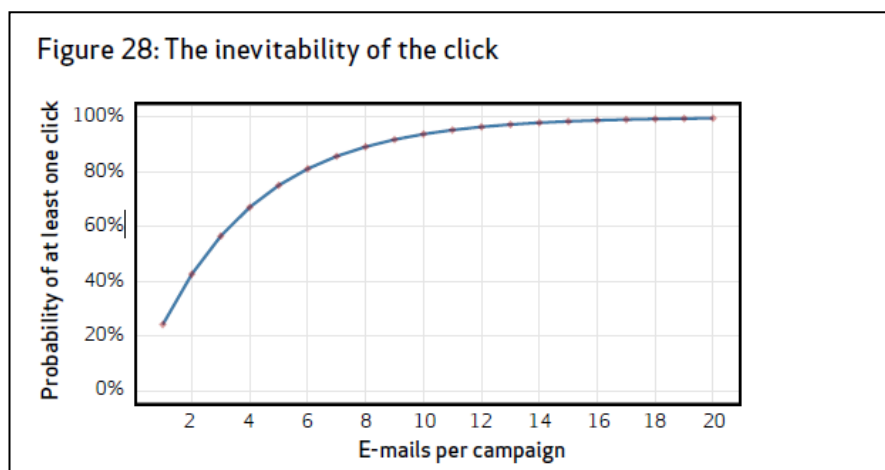


FIGURE 94. Inevitability of a click in a phishing campaign (Verizon, 2013, 38)

The exploit is only possible, if the user actually clicks the link, has a vulnerability on the system, and the malware can be quietly installed without the user awareness and the communication path is available to the attacker (Verizon, 2013, 38).

All the other malware samples represent more evenly distributed behaviors that varied greatly. Some worrying example was seen although, which was at the end of the test period. One backdoor was seen in the Hewlett Packard's BIOS driver during the download from HP's web site (Figure 95).

Log Details

General				Time	
Session ID	636160	Threat/Content Name	Backdoor/Win32.Rbot.nm	Generate Time	2013/08/15 09:21:07
Threat/Content Type	virus	ID	2222844	Receive Time	2013/08/15 09:21:12
Action	deny	Severity	medium	Misc	
Application	ftp	IP Protocol	tcp	Captive Portal	<input type="checkbox"/>
Rule	INT :ONS	Log Action	Critical-Syslog	Proxy Transaction	<input type="checkbox"/>
Category	any	Repeat Count	1	Decrypted	<input type="checkbox"/>
Virtual System	vsys3	Misc	sp62738.exe	Packet Capture	<input checked="" type="checkbox"/>
Device	[REDACTED]			Direction	server-to-client

Source		Destination	
Source User	[REDACTED]	Destination User	[REDACTED]
Source address	15.193.112.142	Destination address	146.162.500.13
Source Port	44985	Destination Port	50013
Source Zone	INTERNET	Destination Zone	-WKS
Inbound Interface	etherne , 140	Outbound Interface	etherne , 30
NAT Source IP	15.193.112.142	NAT Destination IP	[REDACTED]
NAT Source Port	44985	NAT Destination Port	10274

Related Logs (+/- 24 Hours)											
Receive Time	Log	Type	Application	Action	Rule	Bytes	Packets	Severity	Category	URL / Filename	
08/15 09:21:12	threat	file	ftp	forward	INT	ONS		low	any	sp62738.exe	
08/15 09:21:12	threat	file	ftp	forward	INT	ONS		low	any	sp62738.exe	
08/15 09:21:12	threat	virus	ftp	deny	INT	ONS		medium	any	sp62738.exe	
08/15 09:21:40	traffic	end	ftp	allow	INT	ONS	4,688 6				

FIGURE 95. Backdoor in HP BIOS driver file sp62738.exe

File “sp62738.exe” is a HP’s BIOS update for certain models of HP’s laptops. Wild-Fire’s analysis of the file was categorized as malware, see Figures 96-98. There are several behaviors that do not apply to BIOS installation package, e.g. backdoor behavior (listening to a specific port), creates hidden executable in the Windows and Windows system folder, removes itself and visited a malware domain.

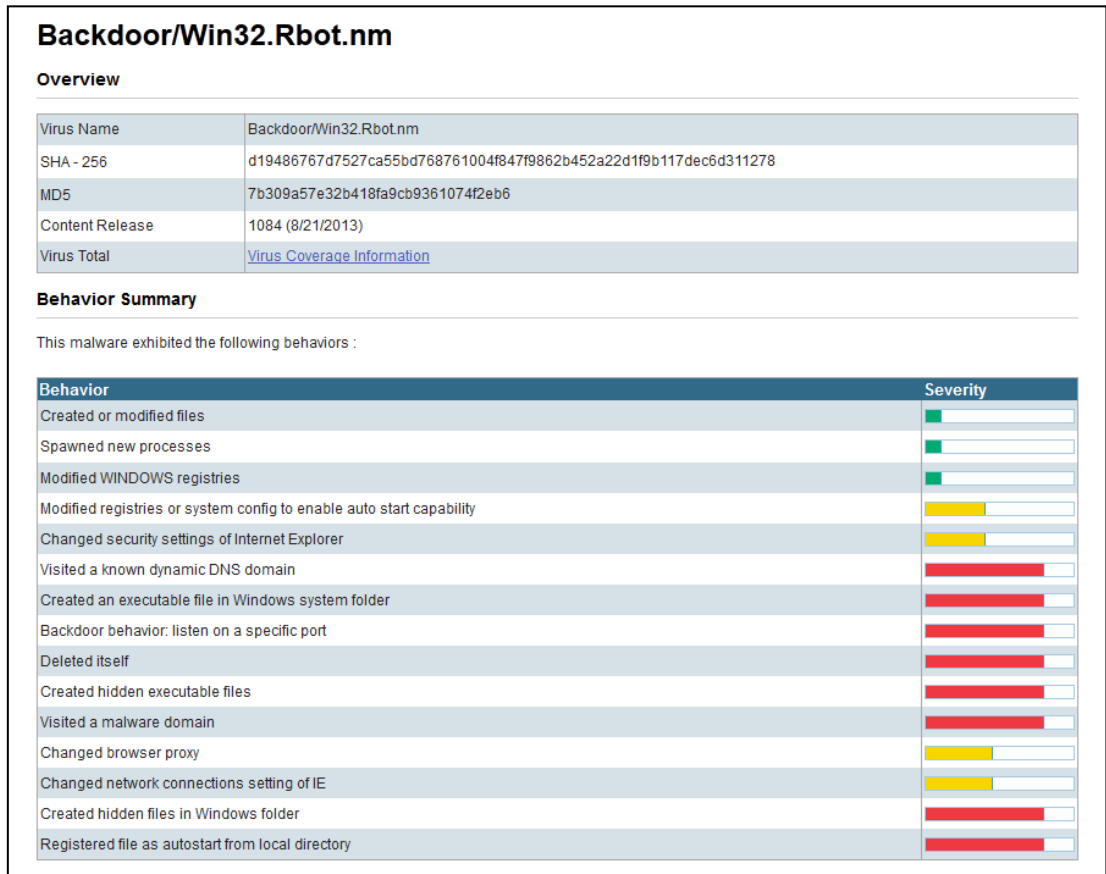


FIGURE 96. Backdoor behavior analyzed by WildFire

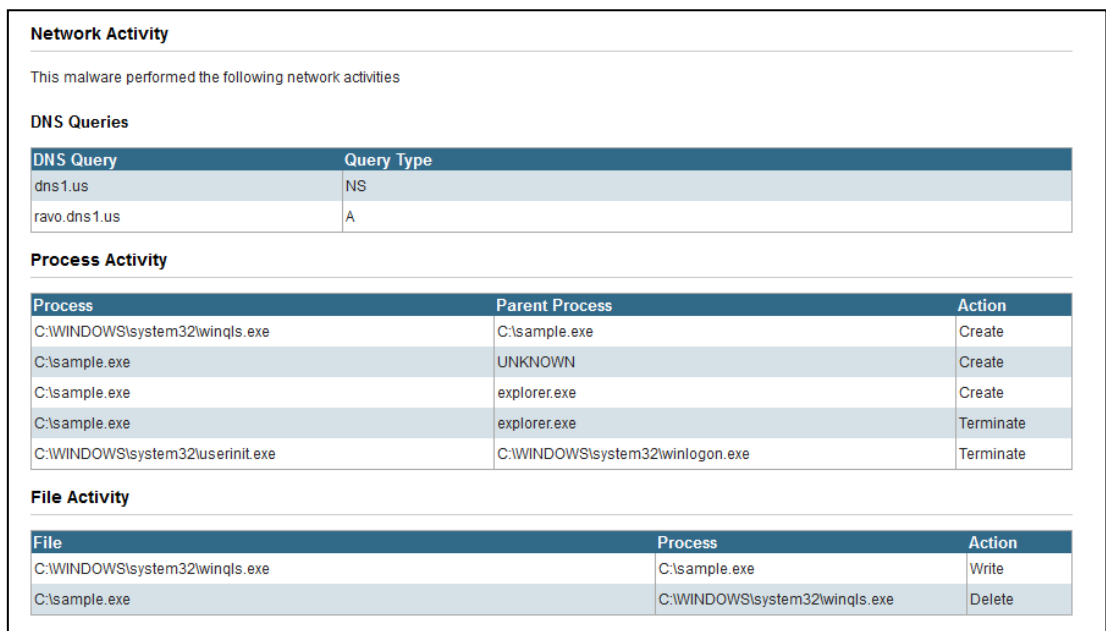


FIGURE 97. Network activity of identified backdoor by WildFire

Registry Modifications	
Registry Key	Action
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Personal	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{e86064ca-57e4-11e0-bef8-806d6172696f}\BaseClass	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Documents	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Desktop	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Desktop	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cookies	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cookies	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\History	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cookies	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\History	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Microsoft IT Update	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Services\Microsoft IT Update	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft IT Update	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Internet.exe	Delete
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common AppData	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\MigrateProxy	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer	Delete
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride	Delete
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL	Delete
HKLM\SYSTEM\ControlSet001\Hardware Profiles\0001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings	Set
HKCU\Control Panel\Keyboard\InitialKeyboardIndicators	Set

FIGURE 98. Registry modifications by identified backdoor by WildFire

36 out of 44 AV vendors detected this backdoor after being 1 week and 2 days in the Virustotal's database. When queried again at 30th August 2013, the same detection ratio still exists, being 2 weeks and 3 days in Virustotal's database (Figure 99-100).

virustotal	
SHA256:	d19486767d7527ca55bd768761004f847f9862b452a22d1f9b117dec6d311278
File name:	9bc8d97a01d259b7250dfd4193f13e4f5b45c766-7b309a57e32b418fa9cb9361...
Detection ratio:	36 / 44
Analysis date:	2013-08-12 20:15:02 UTC (1 viikko, 2 päivää ago)
 More details	

FIGURE 99. Virustotal's detection ratio for a given sample at 22th Aug 2013



FIGURE 100. Virustotal's detection ratio for a given sample at 30th Aug 2013

If this many AntiVirus vendors can detect this specific backdoor so soon, within a week and two days, then it must have been seen within many customer's networks globally. Usually different AntiVirus vendors do not detect malware this rapidly in web traffic.

Predefined Reports and Custom Reports

In addition to WildFire reports, the device itself generates predefined and custom reports defined by the administrator. An example of a predefined report is seen in Figure 101.

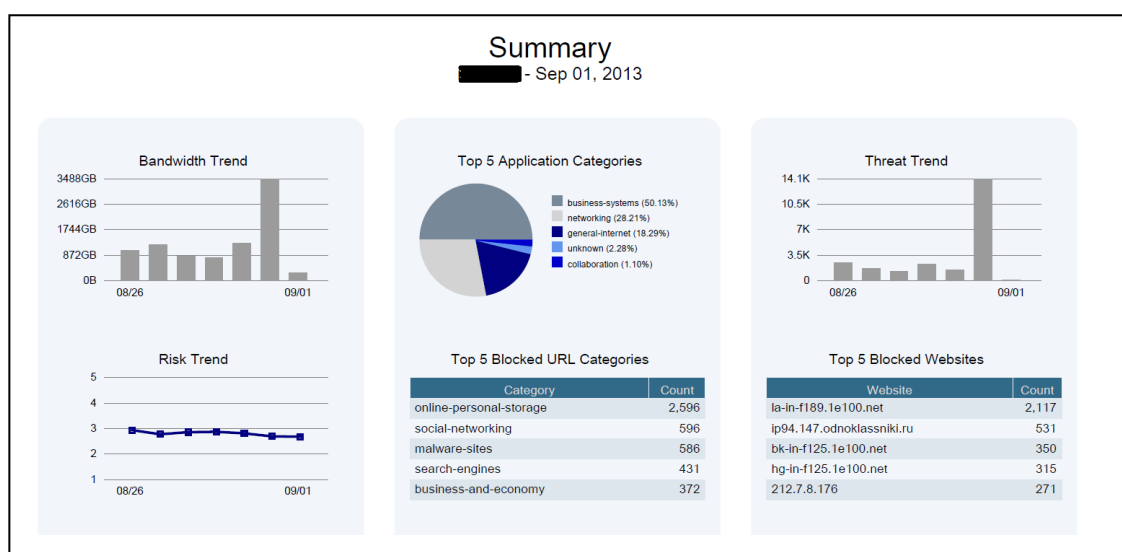


FIGURE 101. Example of a Summary report scheduled by the device

Multiple predefined and custom reports can be scheduled to the email or viewed from the device itself. Figure 102 illustrates a data content report from the past 7 days grouped by the application. On the right pane is the report list per category and below that is a list of different report categories.

Application	Source	Source Host Name	Destination	Destination Host Name	Name	ID	Action	Direction	R.	File Name	Repeat Count
21	62.212.82.94	a330vg.avast.com	192.168.100.10	192.168.100.10	Android Package File Detected	S.	forward	server-to-client	1	resources.arsc	1
22	212.117.161...	ip-sharc-212-117-161-26.as577.net	192.168.100.10	192.168.100.11	Adobe Portable Document Format (PDF)	S.	forward	server-to-client	1	DHG-FBI-AndroidThreats.pdf	1
23	95.211.174.1...	a330vg.avast.com	192.168.100.10	192.168.100.13	Android Package File Detected	S.	forward	server-to-client	1	resources.arsc	1
24	50.7.188.198	a403fs.avast.com	192.168.100.10	192.168.100.11	Android Package File Detected	S.	forward	server-to-client	1	resources.arsc	1
25	109.123.117...	a330vg.avast.com	192.168.100.10	192.168.100.10	Android Package File Detected	S.	forward	server-to-client	1	resources.arsc	1
26	62.142.11.10	www.ncs.fi	192.168.12.11	Aruba-Instant-gw	ZIP	S.	forward	server-to-client	1	AsakasAjurka.jukka.docx	53
27	62.142.11.10	www.ncs.fi	192.168.12.11	Aruba-Instant-gw	ZIP	S.	forward	server-to-client	1	8859-11Q7Ty+F8hyvivoanta_yhdes+E...	20
28	62.142.11.10	www.ncs.fi	192.168.12.11	Aruba-Instant-gw	ZIP	S.	forward	server-to-client	1	=ho-8859-11Q7Ty+F8hyvivoanta_yhdes+E...	17
29	62.142.11.10	www.ncs.fi	192.168.12.11	Aruba-Instant-gw	Adobe Portable Document Format (PDF)	S.	forward	server-to-client	1	Master 2014 este.pdf	3
30	62.142.11.10	www.ncs.fi	192.168.12.11	Aruba-Instant-gw	Adobe Portable Document Format (PDF)	S.	forward	server-to-client	1		2
31	62.142.11.10	www.ncs.fi	192.168.12.11	Aruba-Instant-gw	Microsoft Office 2007 Word Document	S.	forward	server-to-client	1	8859-11Q7Ty+F8hyvivoanta_yhdes+E...	1
32	62.142.11.10	www.ncs.fi	192.168.12.11	Aruba-Instant-gw	Microsoft Office 2007 Word Document	S.	forward	server-to-client	1	AsakasAjurka.jukka.docx	1
33	62.142.11.10	www.ncs.fi	192.168.12.11	Aruba-Instant-gw	Microsoft MSOFFICE	S.	forward	server-to-client	1	Kokouskutsu 1 2013.doc	1
34	62.142.11.10	www.ncs.fi	192.168.12.11	Aruba-Instant-gw	Microsoft Word	S.	forward	server-to-client	1	Kokouskutsu 1 2013.doc	1
35	62.142.11.10	www.ncs.fi	192.168.12.11	Aruba-Instant-gw	Microsoft Office 2007 Word Document	S.	forward	server-to-client	1	=ho-8859-11Q7Ty+F8hyvivoanta_yhdes+E...	1
36	192.168.12.11	Aruba-Instant-gw	62.142.5.5	post.sausalah.fi	ZIP	S.	forward	client-to-server	1	8859-11Q7Ty+F8hyvivoanta_yhdes+E...	20
37	192.168.12.11	Aruba-Instant-gw	62.142.5.5	post.sausalah.fi	ZIP	S.	forward	client-to-server	1	=ho-8859-11Q7Ty+F8hyvivoanta_yhdes+E...	17
38	192.168.12.11	Aruba-Instant-gw	62.142.5.5	post.sausalah.fi	ZIP	S.	forward	client-to-server	1	=ho-8859-11Q7Ty+F8hyvivoanta_yhdes+E...	13

FIGURE 102. Reports viewed using the management interface.

Traffic can be seen as a map where traffic sources or destinations are divided per countries, the color illustrates the risk and the size of the bubble illustrates the traffic amount, as seen in Figure 103. The Atlantic sea represents private addresses.

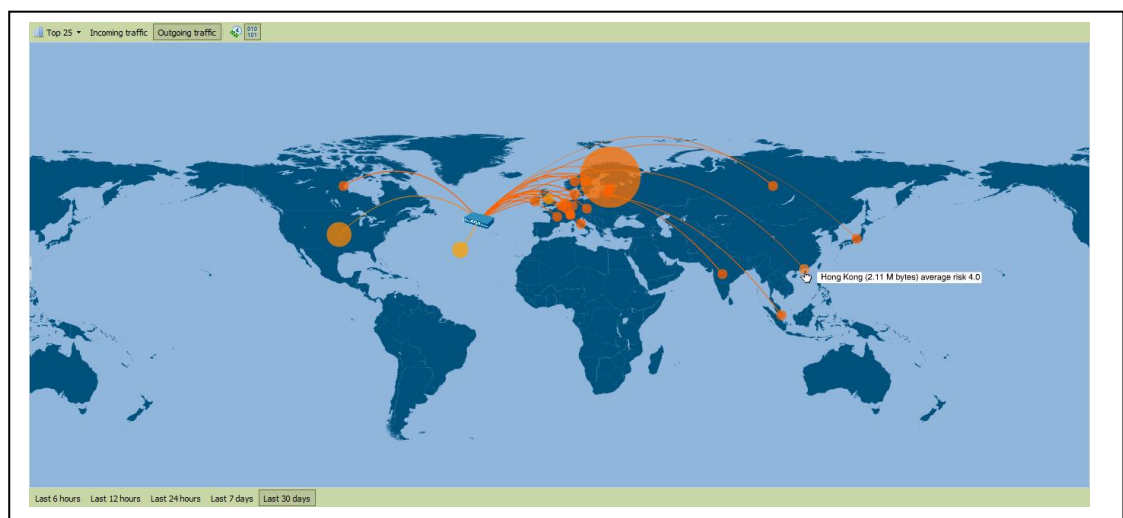


FIGURE 103. Traffic map for past 30 days for outgoing traffic

All reports are generated with active links and filters. Therefore choosing the traffic generated to Hong Kong in Figure 103, for example, will open up an Application Command Center illustrated in Figure 104-105.

Top Applications					
	Risk	Application	Sessions	Bytes	
1	🔗	web-browsing	13	2.0 M	
2	🔗	icmp	4	640	

Top Sources					
	Source Address	Source Host Name	Source User	Bytes	Sessions
1	192.168.12.11	Aruba-instant-gw 🔗		1.9 M	11
2	80.186.141.242	80-186-141-242.elsa-mobile.fi 🔗		640	4
3	192.168.100.11	192.168.100.11 🔗	paulliane	122.3 K	2

Top Destinations					
	Destination Address	Destination Host Name	Destination User	Bytes	Sessions
1	180.150.130.240	i.haymarketmedia.com.au 🔗		2.0 M	8
2	180.150.130.230	www.haymarketmedia.com.au 🔗		21.4 K	5
3	219.73.77.6	n219073077006.netnavigator.com 🔗		640	4

Top Source Countries					
	Source Country	Bytes	Sessions		
1	192.168.0.0-192.168.255.255	2.0 M	13		
2	🇫🇮 Finland	640	4		

FIGURE 104. Traffic map filtered for Hong Kong for past 30 days

Any of the blue colored texts are links to another filter, if more detailed filters are required. For example, selecting web-browsing in Figure 104 will add another filter based on web-browsing application in addition to existing filters, see Figure 105.

Top Destination Countries					
	Destination Country	Bytes	Sessions		
1	🇭🇰 Hong Kong	2.0 M	17		

Top Security Rules					
	Rule	Bytes	Sessions		
1	Kali-to-Out-allow	1.9 M	11		
2	VPN-to-Out	123.0 K	6		

Top Ingress Zones					
	Source Zone	Bytes	Sessions		
1	Kali	1.9 M	11		
2	VPN	123.0 K	6		

Top Egress Zones					
	Destination Zone	Bytes	Sessions		
1	ADSL	2.0 M	17		

URL Filtering					
	Category	Sessions	Bytes		
1	business-and-economy	8	2.0 M		
2	computer-and-internet-info	5	21.4 K		

Threat Prevention					
No matching record					

FIGURE 105. Web-browsing traffic filtered for Hong Kong for past 30 days

Traffic Map and Threat Map can be used in the similar way or in the Traffic Monitor or Threat Monitor view, as illustrated in Figure 106.

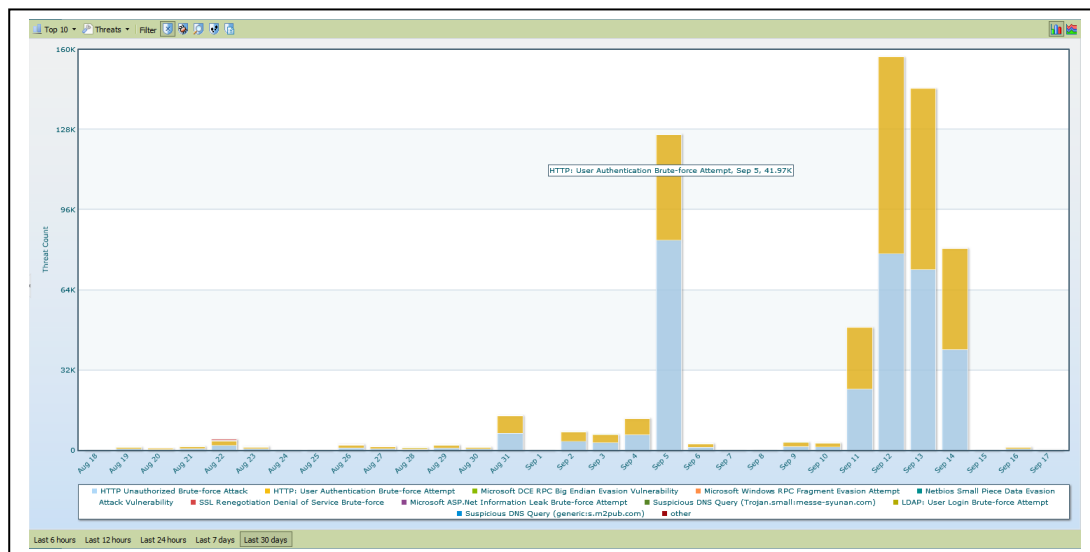


FIGURE 106. Threat Monitor for the past 30 days for top 10 threats

Once again, by selecting a threat it works as an active filter to the next view, where traffic is filtered with a selected threat type, like a User Authenticated Brute-force Attempt in this case. That kind of threats occurred during several days and on Tuesday, September 5th it occurred 41,970 of times. A similar figure as Figure 104-105 will appear, but as filter set to User Authenticated Brute-force Attempt and on Tuesday 5th September.

Browser based web applications can be separated as well, as illustrated in Figure 107. All of these applications use either port 80 known as HTTP or dynamically allocated port or port range or port hopping; however their behavior reveals the true application behind the traffic.

	Application Name	Bytes	Sessions
1	web-browsing	76.0 M	881
2	playstation-network	1.1 M	94
3	google-maps	13.4 M	84
4	gmail-base	828.0 K	80
5	itunes-base	3.7 M	75
6	google-analytics	289.1 K	49
7	panos-global-protect	130.4 K	41
8	linkedin-base	511.6 K	19
9	idoud-base	185.1 K	19
10	facebook-base	357.0 K	18
11	apple-appstore	178.0 M	18
12	facetime	2.2 K	6
13	facebook-social-plugin	73.7 K	4
14	silverlight	463.0 K	3
15	ocsp	9.6 K	3
16	google-app-engine	15.0 K	2
17	google-calendar-base	12.8 K	2
18	apple-maps	5.8 K	1
19	ldap	252	1
20	google-update	3.0 K	1

FIGURE 107. HTTP-Applications separated from the browser based traffic

Sometimes it is convenient to compare traffic behavior between two timelines, taking for example this Monday to last week's Monday or a certain day of the week or month to another day of the week or month. Figure 108 illustrates a change monitor for a given day.

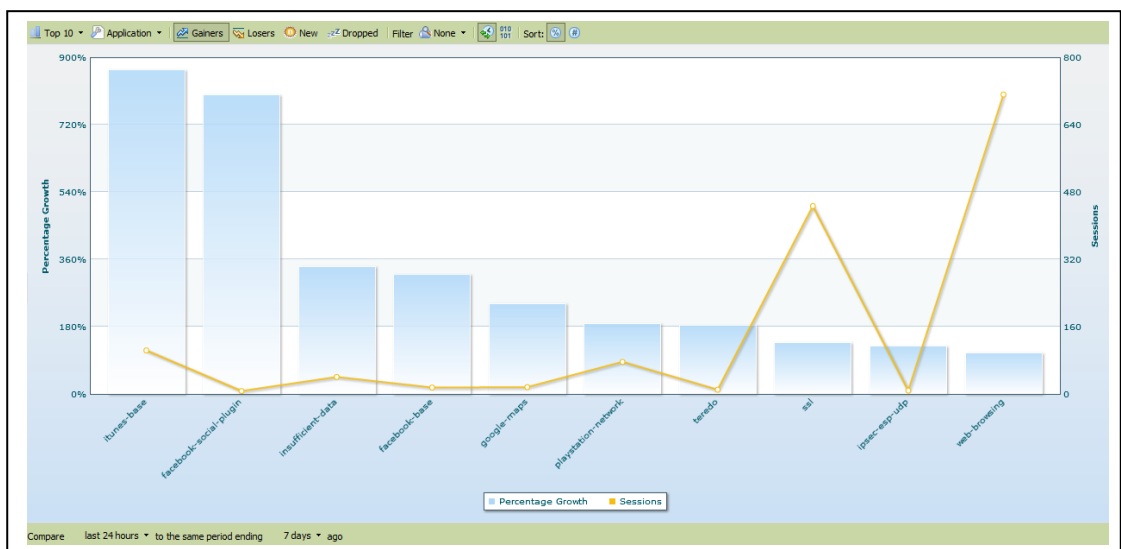


FIGURE 108. Change monitor for a Monday to previous Monday

Change monitor offers a possibility to find behavior on certain days, if some troubles are experienced, e.g. larger traffic amounts or threats on a given day. Filter can be applied to as gainers, losers, applications, new or dropped traffic and so on.

Many general reports are also available, like Top Categories and Top Denied Categories, illustrated in Figures 109 and 110.

	Category	Repeat Count
1	business-and-economy	276.1 K
2	social-networking	182.9 K
3	search-engines	154.4 K
4	content-delivery-networks	139.8 K
5	news-and-media	111.8 K
6	computer-and-internet-info	93.5 K
7	streaming-media	90.7 K
8	entertainment-and-arts	55.9 K
9	web-advertisements	55.6 K
10	travel	51.8 K
11	web-based-email	41.2 K
12	society	34.3 K
13	sports	22.0 K
14	unknown	19.1 K
15	reference-and-research	18.1 K
16	internet-portals	16.8 K
17	shopping	15.4 K
18	financial-services	14.9 K
19	personal-sites-and-blogs	13.3 K
20	games	10.6 K

FIGURE 109. URL Categories

	Category	Repeat Count
1	online-personal-storage	10.2 K
2	malware-sites	4.0 K
3	internet-communications	2.2 K
4	social-networking	1.9 K
5	business-and-economy	1.6 K
6	streaming-media	1.1 K
7	search-engines	919
8	spam-urls	793
9	adult-and-pornography	729
10	computer-and-internet-info	725
11	spyware-and-advare	351
12	personal-sites-and-blogs	347
13	pay-to-surf	154
14	web-based-email	129
15	shareware-and-freeware	68
16	image-and-video-search	60
17	shopping	15
18	computer-and-internet-security	13
19	web-advertisements	5
20	content-delivery-networks	4

FIGURE 110. Blocked URL Categories

An example of custom report is illustrated in Figure 111. There is a list of viruses and spyware for the past week.

Application	Threat/Content Name	ID	Risk	Severity	Source Zone	Source Country	Destina. Zone	Destination Country	Count	
1	dns	Suspicious DNS Query (Trojan.smallmesse-syunan.com)	40	4	MEDIUM	Aruba-VPN-PO...	10.0.0.0-10...	EVRY-S...	Sweden	94
2		Suspicious DNS Query (Trojan.smallmesse-syunan.com)	40	4	MEDIUM	SERVER...	Sweden	ELISA-INTERN...	Finland	43
3		Suspicious DNS Query (Trojan.smallmesse-syunan.com)	40	4	MEDIUM	OFFICE...	Sweden	SERVER...	Sweden	33
4		Suspicious DNS Query (generics.m2pub.com)	40	4	MEDIUM	Aruba-VPN-PO...	10.0.0.0-10...	EVRY-S...	Sweden	10
5		Suspicious DNS Query (Trojan.smallmesse-syunan.com)	40	4	MEDIUM	VPN	10.0.0.0-10...	SERVER...	Sweden	8
6		Suspicious DNS Query (generics.m2pub.com)	40	4	MEDIUM	VPN	10.0.0.0-10...	SERVER...	Sweden	6
7		Suspicious DNS Query (generics.m2pub.com)	40	4	MEDIUM	SERVER...	Sweden	ELISA-INTERN...	Finland	6
8		Suspicious DNS Query (Trojan.smallmesse-syunan.com)	40	4	MEDIUM	GUEST	Sweden	ELISA-INTERN...	Finland	5
9		Suspicious DNS Query (Trojan.Cropper-pykapaxunhentyf.net)	40	4	MEDIUM	OFFICE...	Sweden	SERVER...	Sweden	3
10		Suspicious DNS Query (Trojan.smallmesse-syunan.com)	40	4	MEDIUM	OFFICE...	Sweden	SERVER...	Sweden	2
11	ms-ds-emb		25	1	0	SERVER...	Sweden	SERVER...	Sweden	290
12	google-analytics	Suspicious user-agent strings	10	2	MEDIUM	ELISA-INTERN...	Finland	OFFICE...	10.0.0.0-10...	36
13		Suspicious user-agent strings	10	2	MEDIUM	ELISA-INTERN...	United States	OFFICE...	10.0.0.0-10...	2
14	web-browsing	Suspicious user-agent strings	10	4	MEDIUM	ELISA-INTERN...	Israel	OFFICE...	10.0.0.0-10...	4
15		Virus/Win32.WGeneric.iahj	26	4	MEDIUM	ELISA-INTERN...	Germany	OFFICE...	10.0.0.0-10...	3
16			25	4	0	ELISA-INTERN...	United States	VPN	10.0.0.0-10...	1
17		Virus/Win32.WGeneric.iahj	26	4	MEDIUM	ELISA-INTERN...	Germany	OFFICE...	Sweden	1
18		Suspicious user-agent strings	10	4	MEDIUM	ELISA-INTERN...	France	OFFICE...	10.0.0.0-10...	1
19		Suspicious user-agent strings	10	4	MEDIUM	ELISA-INTERN...	Israel	Aruba-VPN-PO...	10.0.0.0-10...	1
20		Virus/Win32.WGeneric.iahj	26	4	MEDIUM	ELISA-INTERN...	Germany	VPN	10.0.0.0-10...	1
21		JS/Trojan.blacleref.n	25	4	MEDIUM	ELISA-INTERN...	Netherlands	Aruba-VPN-PO...	10.0.0.0-10...	1
22			25	4	0	ELISA-INTERN...	United States	OFFICE...	10.0.0.0-10...	2
23	ftp	Backdoor/Win32.Rbot.rm	22	2	MEDIUM	ELISA-INTERN...	United States	OFFICE...	Sweden	6

FIGURE 111. A list of viruses and spyware for the past week grouped by application

4.3.12 Custom Applications

Sometimes it is necessary to write own customized applications for unknown-TCP or -UDP traffic that cannot be recognized. Alternatively, a packet capture can be made from the traffic and sent to the Palo Alto Networks to write an application identification which is then updated via dynamic updates to all customers. A simple example

of a production environment in NCC of a web-based building automation system, built on an embedded system running on various version of Linux OS. The application was not recognized as web-browsing or similar application, instead unknown TCP traffic, which was blocked by default and only allowed applications were allowed. Therefore, a custom application was written with the following definition based on packed capture, as illustrated on Figures 112-115.

The screenshot shows the 'Application' configuration window with three tabs: 'Configuration', 'Advanced', and 'Signatures'. The 'Configuration' tab is active. It is divided into three sections: 'General', 'Properties', and 'Characteristics'.
- **General:** Name is 'Custom-Fidelix' with a 'Shared' checkbox checked. Description is 'Monitoring of Fidelix Automation system'.
- **Properties:** Category is 'business-systems', Subcategory is 'general-business', Technology is 'browser-based', Parent App is 'web-browsing', and Risk is '4'.
- **Characteristics:** A grid of checkboxes where 'Has Known Vulnerabilities', 'Used by Malware', and 'Prone to Misuse' are checked, while others are unchecked.

FIGURE 112. Custom application example – Configuration

The screenshot shows the 'Application' configuration window with the 'Advanced' tab active. It is divided into three sections: 'Defaults', 'Timeouts', and 'Scanning'.
- **Defaults:** Radio buttons for 'Port', 'IP Protocol', 'ICMP Type', 'ICMP6 Type', and 'None', with 'None' selected.
- **Timeouts:** Three input fields for 'Timeout', 'TCP Timeout', and 'UDP Timeout', all containing '[0 - 604800]'.
- **Scanning (activated via Security Profiles):** Four checked checkboxes for 'File Types', 'Viruses', 'Spyware', and 'Data Patterns'.

FIGURE 113. Custom Application example – Advanced

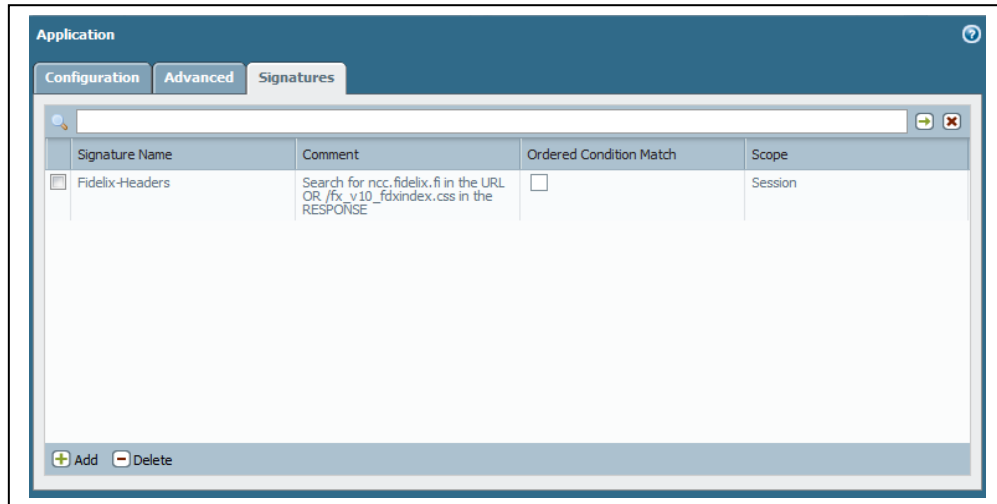


FIGURE 114. Custom Application example – Signatures

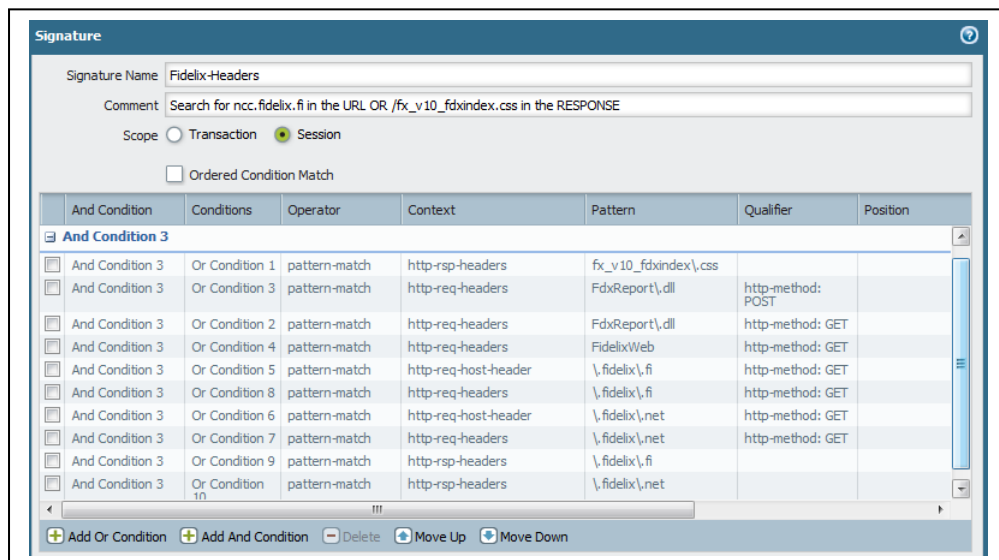


FIGURE 115. Custom Application example – Signatures for Session Scope

In addition to custom application, Application Override Rule was also defined with correct zone, source, and destination definitions for desired ports. This way, the NGFW's default application identification process can be ignored, since any custom made settings are prioritized first to run, prior to App-ID process. This way, any custom made applications are forced to be identified as custom applications. Now, Security Rules can be made to this custom application for desired users or user groups. For this particular application, specific users were defined as sources. Then, a Custom URL Category was made with a Partner's domain specifications in it. This was defined as a destination in the security rule and previously created custom application as

application with all the threat parameters on. The same example can be leveraged in BYOD solutions. This way security is not degraded, since this application override is done to an application that is known to be important for business. It is then examined, a custom application is written based on its behavior, source users are restricted to only need-to-know-basis, destination is limited to the specific domains only by custom category leveraging wildcards (in the format: *.company.com), only specific custom application is allowed and threat monitor is on with the same level as normal internet traffic for all users.

4.3.13 Updates

NGFW software was updated three times from 5.0.4 to 5.0.7. No errors were encountered with any features after the updates were applied, and everything worked normally. The software updates are illustrated in Figure 116.

Version	Size	Release Date	Downloaded	Currently Installed	Action	Release Notes	
5.0.6	180 MB	2013/07/08 16:48:30	✓	✓	Reinstall	Release Notes	☒
5.0.5	180 MB	2013/05/24 22:28:09	✓		Install	Release Notes	☒
5.0.4	180 MB	2013/04/02 22:17:39	✓		Install	Release Notes	☒
5.0.3	180 MB	2013/03/08 21:07:53			Download	Release Notes	
5.0.2	160 MB	2013/01/15 15:25:02			Download	Release Notes	
5.0.1-h1	160 MB	2012/12/10 15:40:22			Download	Release Notes	
5.0.0	259 MB	2012/11/01 19:58:24	✓		Install	Release Notes	☒

FIGURE 116. Software updates with NGFW

Dynamic updates are checked daily and downloaded and installed whenever available. Dynamic updates are illustrated in Figure 117.

Version	File Name	Features	Type	Size	Release Date	Download...	Currently Installed	Action	Documen...
Antivirus Last checked: 2013/09/02 05:30:14 Schedule: Every day at 05:30 (download-and-install)									
1091-1520	panup-inc-antivirus-1091-1520		Incremental	17 MB	2013/08/30 04:00:03	✓	✓		Release Notes <input type="checkbox"/>
1090-1519	panup-inc-antivirus-1090-1519		Incremental	16 MB	2013/08/29 04:00:04	✓ previously		Revert	Release Notes <input type="checkbox"/>
Applications and Threats Last checked: 2013/09/02 05:45:06 Schedule: Every day at 05:45 (download-and-install)									
389-1904	panupv2-all-contents-389-1904	Apps, Threats	Full	18 MB	2013/08/20 14:23:35	✓	✓		Release Notes <input type="checkbox"/>
388-1898	panupv2-all-contents-388-1898	Apps, Threats	Full	18 MB	2013/08/13 15:11:35	✓ previously		Revert	Release Notes <input type="checkbox"/>
GlobalProtect Data File Schedule: Every day at 01:00 (download-and-install)									
13780722...					2013/09/01 21:51:16		✓		
WildFire Last checked: 2013/09/02 13:31:33 Schedule: Every 30 Minutes (download-and-install)									
18896-24793	panup-inc-wildfire-18896-24793		Incremental	3 MB	2013/09/02 02:33:01	✓	✓		Release Notes <input type="checkbox"/>
18895-24792	panup-inc-wildfire-18895-		Incremental	3 MB	2013/09/02 02:04:01	✓ previously		Revert	Release Notes <input type="checkbox"/>

FIGURE 117. Dynamic Updates using scheduling

Global Protect software updates were also updated. They can be deployed automatically to the client per every portal. Thus, internal users can be updated transparently and partners can be prompted to update the client. GP updates can be seen in Figure 118.

Version	Size	Release Date	Downloaded	Currently Activated	Action	Release Notes
1.2.5	23 MB	2013/07/18 17:22:56	✓	✓	Reactivate	Release Notes <input type="checkbox"/>
1.2.4	22 MB	2013/06/09 22:41:49	✓		Activate	Release Notes <input type="checkbox"/>
1.2.3	22 MB	2013/04/26 09:25:26			Download	Release Notes
1.2.2	22 MB	2013/02/23 10:26:41	✓		Activate	Release Notes <input type="checkbox"/>
1.2.1	22 MB	2012/12/19 15:10:58			Download	Release Notes
1.2.0	21 MB	2012/11/02 16:32:22			Download	Release Notes

FIGURE 118. Global Protect version updates

If agent updates for global protect client have been chosen to prompt for user, the following pop-up will occur next time the client connects to the portal, see Figure 119.

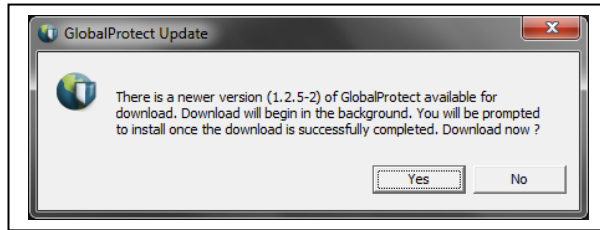


FIGURE 119. Global protect client update

All the updates reduces maintenance work, since no additional actions are needed from the administrators when something changes, e.g. software bugs are fixed and new applications or threats are identified. Customers can also receive updates from the Palo Alto Networks directly via email, when new applications features are added, removed or modified. This way, the administrator can verify that everything is in order and know what will change during the next update without logging in to the system. An example of content release notes is illustrated in Figure 120.

Risk	Name	Category	Subcategory	Technology	Depends On	Previously Identified As	Minimum PAN-OS Version
2	elastic-search	business-systems	management	browser-based	web-browsing	web-browsing	3.1.0
2	memcached	business-systems	database	client-server		unknown-tcp,unknown-udp	3.1.0
4	opendoor	networking	proxy	client-server	ssl	ssl	3.1.0

Risk	Name	Category	Subcategory	Technology	Depends On	Minimum PAN-OS Version
5	bittorrent	general-internet	file-sharing	peer-to-peer	web-browsing	3.1.0
2	citrix-jedi	networking	remote-access	client-server	ssl,web-browsing	3.1.0
2	gotomypc-base(function)	networking	remote-access	client-server	citrix-jedi,ssl,web-browsing	
2	gotomypc-remote-control(function)	networking	remote-access	client-server	citrix-jedi,gotomypc,ssl	3.1.0
4	sip	collaboration	voip-video	peer-to-peer		3.1.0

Name
http
ssl

FIGURE 120. Application and Threat Content Release Notes delivered via email

5 RESULTS

The product and the remote access features are versatile and mature, based on the functional testing's results. There has been product development in the past, since the previous SSL-VPN software called NetConnect is not supported anymore in the 5.0 release. Instead, it is replaced and automatically migrated with Global Protect, which connects using a more efficient method: IPsec or as a fallback option: SSL. Whereas IPsec uses simpler and more efficient UDP, SSL uses slower but more reliable TCP. All the SSL-VPN solutions, such as NetConnect, are based on SSL, even though some solutions may have additional transport methods included.

Overall, a NGFW technology offers three different remote access solutions:

- On-demand method, which is suitable for partners for occasional remote access needs and mobile users for on-demand use. This type of connection can be established with any type of device that supports IPsec protocol without any additional license needs or with Global Protect Client with Global Protect License subscription. The use of Global Protect Clients together with IPsec clients can be combined also. Mobile devices can be laptops with Windows, Linux or Macintosh or they can be smartphones and tablets using Android, iOS or Windows8, with the exception that Windows8 is supported only with Global Protect Client.
- User-logon method with Global Protect Client without the license subscription in the portal. This method provides VPN Client functionality for laptops without the location awareness functionality which means that the IPsec tunnel is always performed regardless the location. IPsec clients are supported with any IPsec-capable device
- Pre-logon method with Global Protect Client with the license subscription in the portal. This method supports all the other methods mentioned above, but also the location awareness functionality with Global Protect Client in the lap-

tops and mobile devices with Android and iOS (windows8 is not yet supported, but other Windows versions are). It also enables the possibility to logon to the domain even the user is behind the remote access connection with windows laptop and a valid machine certificate installed.

Windows OS does not support IPSec termination other than Windows gateway products and therefore a separate VPN client program is required for terminating IPSec to other vendor's gateways. This applies to all Windows platforms from Windows95 to Windows8, which means that it is probably a political decision that has driven to choose this path when developing windows OS. If the VPN gateway is other than Windows platform, a vendor specific VPN client software is recommended for full functionality and in Palo Alto NGFW case, VPN client program is Global Protect Client with or without the license. The mobile environment is not so mature yet, even it has grown rapidly for the past years. The consumerization may be one reason that remote access functionalities have not been developed enough. The consumer does not need remote access outside working hours in their spare time, until they use it for work also. The immaturity can be seen in the devices capability to work reliably with platform provided IPSec client software, if it even exists. Windows8 OS is one example of immature VPN behavior, since it only supports windows based platforms and termination to other vendor's gateways does not support windows specific negotiations or tunneling protocols, such as PPTP, L2TP, MS-CHAP etc. Another example is Samsung Galaxy SII model, which native IPSec VPN client does not work at all, but the same family's SIII and SIV models works without problem. Additional VPN Client software resolves this immaturity problem, but affects the wholeness if mobile environment is relying solely on device's native IPSec client.

Palo Alto Networks' NGFW integrates many services and solutions, such as Proxy, AV, IDP/IPS and SSL-VPN into one, centralized solution. This enables many benefits which results in topological simplicity and greater visibility, and also less risks because of less complexity in the network topology. With an NGFW solution, latencies are smaller, since traffic does not need to be sent between several devices back and

forth in order to achieve the same functionality or result. Instead with purpose-built hardware and innovative technology solution, more efficiency and performance improvements can be achieved even with larger traffic amounts together with a number of different functionalities enabled.

Global Protect solution offers features for remote access solutions for mid-sized and large companies, including branch offices. Remote access methods can be deployed as centralized solution or decentralized solution, depending on the geographical distribution of the company's network and the size of the company. Several remote access methods are supported at the same time with different configurations enabled for different level of zones or classification needs. Satellite configuration offer geographically distributed Global Protect gateways to the Global Protect clients. This way, connecting to the central site it always offers the best (or nearest) Global Protect gateway to choose from, or some additional gateways for stronger authentication needs of stricter security zone for certain users only, for example. Whenever a configuration changes, updated client software is available or a gateway is unavailable, the information is updated to the clients through the Global Protect Portal.

Without a Global Protect Portal and Gateway license User-logon method is available with GP Client for laptops for Mac OS 32- and 64-bit and Windows OS 32- and 64-bit versions (Windows8 is not supported yet). In addition, 3rd party VPN is supported for any device that supports IPsec VPN with Xauth method, e.g. Android OS and Apple's iOS. 3rd party VPN is typically used on-demand mode only, but Apple's iOS supports also split tunneling with company domains routed through the VPN tunnel to the company network. In this scenario, VPN tunnel is established automatically but it supports certificate authentication only and therefore a user certificate is required and must be distributed to the clients prior to connection establishment. A company should carefully estimate whether to allow split tunneling, and if allowed, then control traffic with application identification and threat prevention. Split tunneling introduces risks, since traffic can traverse from outside VPN connection, such as internet, to the company network through the VPN tunnel. Therefore these risks need to

be addressed with minimal networks access and applications allowed, with maximal threat prevention and using need-to-know approach.

With the Global Protect Portal and Gateway license, more features can be enabled. Laptops with GP Client installed recognize the internal network and the Internet and operate in a different manner, depending on the current location of the laptop. In the internal network, VPN is not established and when the location changes to the Internet the VPN is automatically established, without any user interaction if so configured. Strong authentication can be implemented in this phase, if that is a preferred solution for the company. When connection is established automatically with license feature, strong authentication decreases the usability significantly, if user needs to authenticate with another PIN, SMS code or password. Instead, it should be done with a certificate or smartcard that requires user interaction only when inserted or removed to or from the laptop. Alternatively, the additional authentication can be PIN code during boot-up and hibernate using encryption software, such as BitLocker in Windows.

For smartphones and tablets, license feature enables the same functionality for GP Clients as with the laptops. GP Client is available for the most used platforms, which are Windows, Mac OS X, Android and iOS and its different functionalities operated very reliably during the test period, even with the built-in VPN configured in the devices. For the mobile use, license features offer several ways of supporting remote access without at the sacrifice of the security and IT related risks, however it also support laptop usage with location awareness and different gateway selection options that offer extra redundancy for remote services if some of the gateways are unreachable. There is a feature that should be noted when using the GP license and full tunneling on the mobile device; this combination makes Bluetooth and WLAN tethering useless because full tunneling disables local network resources totally. This can be an advantage or disadvantage for a company, depending what is the current mobile policy in the company. If tethering using mobile device is currently used in the company to avoid use of malicious AP's, then there is a conflict with full tunneling

feature in the mobile device and with the policy. One solution would be the use of available WLAN's or additional SIM cards.

WildFire functionality is a competitive advantage among competitors, since it analyses unknown threats safely and in isolated environment separated from the customer's environment and provides detailed information about threats and behavior with integration to the Virustotal Database and its analyses. The traditional way of detecting viruses based on signatures has not been enough for several years anymore, if used as only protection method. Also, layered protection protects better than traditional AV solution solely, but without behavioral analysis its significance is not enough anymore. Behavioral analysis with integrated cloud solution, consisting of virtual environments for Windows and Android including various set of office products and the most vulnerable software (such as Adobes Acrobat Reader) that analyses the viruses and creates the results in addition to existing countermeasures, is essential. Palo Alto Networks also have cooperation with Mandiant and Bit9 for make further use of WildFire information and WildFire itself operates in four time zones already.

Palo Alto Networks provides various reports on-the-box by default, but also tailored reports using regex format via GUI or REST (Representational State Transfer) API interface for external reporting systems to retrieve custom information from the NGFW directly. It simplifies reporting needs and gaining total network visibility by having as much information as possible in one location, whereas traditional systems retrieves or pushes pieces of information from various places of the network and then constructs the total network visibility by network monitoring, log and event management and SIEM systems.

6 CONCLUSIONS AND DISCUSSION

Technology and architecture has a major part when choosing how to build a scalable, multifunctional and long-term solution in the infrastructure. A traditional way of implementing the network solutions and services in the border of the network is complicated in mid-sized and large deployments. NGFW solution will defeat many of those challenges since it simplifies the environment significantly and therefore enables the usage of modern solutions, such as BYODT, and adapts to business changes more efficiently. The architectural advantage of Palo Alto Networks' NGFW is that the throughput is predictable in multi-gigabit speed with purpose-build hardware that has hardware acceleration in layers 4 to 7. The traditional solutions struggle when traffic increases and the outcome is usually low performance with varying latencies and therefore the throughput is not predictable. This is, because the traditional technology is based on layer 4 architecture and layer 7 inspection is done with CPU on "industry standard hardware".

The new architectural model simplifies network topology by reducing the number of different devices and services by replacing them with NGFW's own services. This also affects the following elements by lowering IT related costs depending how many services are completely replaced:

- Licenses and software: Security products' licenses are based on number of clients or servers (AV's, Proxies), end-user amount (AV's, IPS) or simultaneous sessions (FW's, Proxies) in the company
- Management and reporting: Multi-vendor environment usually requires vendor-specific management software and even licenses in some cases. Also, vendor-specific logging, alerting or reporting systems are sometimes needed to provide full support for the vendors' features

- Multi-vendor environment and hardware: Services are typically added when needed and divided to different vendors because of various historical reasons, such as gaining layered protection, dividing risks to different parties, or easier replacement of single service or functionality
- Support and partner: By reducing partners, there are lesser contracts and supporting parties, but also lesser vendors, agreements and SLA's.
- Network visibility: Total network and security visibility is gained through one single solution or lesser solution, which reduces time spent in troubleshooting and finding root-causes, security issues and simplifies alerting and monitoring.

NGFW solution carries one similar risk as traditional solution. If the firmware has a bug, a corruption of the configuration or some sort of fault condition, which causes some or all of the services work in an unexpected manner, then the faulty service or services affects the production significantly and may not be isolated at all until a fix is found by the vendor. In traditional architecture, this can be usually isolated from the network without the significant efforts and production can be continued without that service, however in the NGFW solution this isolation can be harder to achieve, depending on which service is the faulty one. Even if the device is in the cluster and connected through the high availability to the secondary device, the secondary device shares the same software and configuration information and does not provide a backup solution or fix to the firmware related risk. This kind of risk can be more likely when updating to the major firmware or software release and less likely when updating to the minor release. However, this kind of risk has not been encountered in the lifetime of Palo Alto Networks' NGFW products since 2007 and the risk is also equal to the traditional based model's risk.

Traditional based model has many individual services (and usually even by different vendors) that form the wholeness and every clustered individual service carries the

same risk. Therefore, the risk can be even more likely realized since these individual services are cascaded, caused by the serial order processing and the network topology. It is irrelevant to estimate what is the probability of the risk, since every services and vendors carries the same risk, but it is important to understand, that in the traditional model the risk is as many times more likely than the number of individual, cascaded services. Palo Alto Networks NGFW integrates all of those services into one cluster, but they still exist inside the device. Even all integrated services are considered the same risk and probability, at least the software that controls the integrated services is the same, there is only one vendor and processing is done in parallel order, which all lower the overall risk of the wholeness.

Employees and partners utilize more and more several different remote access methods at the same time. Therefore it is advantageous for the company to support as many remote access methods as possible to support varying business needs and devices. A company should not concentrate on limiting or denying the device models and platforms together with strict and complicated policies, instead, investing to the infrastructure that support standards and protocols and is a long-run solution would be advisable.

6.1 Answering the Research Questions

Do NGFW functionalities work as expected?

All the tested functionalities operated as expected. However, one suspected bug was found in the Android platform for certain model of Samsung smartphone in the situation, where mobile client used a certificate installed to Android in order to authenticate to the portal and gateway. This was verified in three times with the same result and the Tech Support File was created from the NGFW and the smartphone and a ticket was generated to the vendor. After testing the functionalities for six months, they worked very reliably all the time in all of the platforms and no other problems,

software freezes or bugs were found in the mobile devices or NGFW product. An improvement suggestion was also made to the vendor concerning Global Protect for Android in the situation described on page 59, Figure 22, to make the application permanently trusted instead of being asked to trust the application during every boot.

Can traditional remote access and BYODT Technologies be supported with only one (logical) NGFW device?

NGFW product used in this test with the Global Protect licenses will give much more comprehensive control methods for supporting different kinds of remote access methods including BYODT than a traditional one. This is only a technological solution, but it can support all the needed features for building up a secure remote access environment. All of this can be achieved with supporting different mobile platforms as long as the mobile platforms supports basic standards like IPsec VPN, but Global Protect Client is also available on several platforms. Upgrading from traditional solutions to the NGFW solution is a long run investment for the infrastructure.

Can the IT Environment be simplified using NGFW?

Companies should carefully estimate what services they are running on their network and what can be replaced with NGFW solution. After all, it is tempting to see how many services can be integrated into one and what hidden or indirect cost benefits there are. Some of the benefits cannot be calculated, but are obvious, such as smaller latencies and faster trouble-shooting times. Benefits depend on the size of the company, since larger enterprises tend to have many solutions to do the same or similar tasks, and those tasks can be replaced ending up with a simpler environment. Replacement process will take time and after six months of switchover, most of the services are typically replaced and after a year, more and more fine-tuning can be achieved to gain more improvements to the monitoring of network and security events.

Can security still be measured and not degraded with NGFW?

Many predefined reports are available and ready to run or schedule. Usually predefined reports are not suitable or detailed enough for different kinds of environments and therefore custom reports are a must for any product to fulfill the needs of different requirements. Custom reports can be generated through the web GUI, but NGFW also supports API that can be used to produce almost any kind of information. The API interface can be used either to push or retrieve the information to or from NGFW. Overall, there are many possibilities to gain visibility to different level of subjects from the information flow that travels through the NGFW. Also, customized alerts and external logging systems are supported to achieve better interoperability with external devices.

6.2 Validity and Credibility of the Study

In mid-sized and large companies distributing of applications, configurations, settings and updates have a significant role. Usually the devices are not similar, because of differences in the hardware, drivers, applications and the age of the OS and hardware. Every time a change is made, there is a risk that the change affects some of the existing functionality. Therefore, it is vital to test changes for a test group of devices before distributing the changes to the rest of the devices. The functionality test of NGFW with only three different platforms and devices does not give any reliable perspective of the distribution phase. There can be bugs in the same platforms but with different hardware than what was revealed in this functionality test of this study. There are also many dependencies in the corporate environment between systems that need to be carefully estimated before considering changing the remote access methods and configurations. Tests, results and assumptions in the thesis do not apply to any other vendors' NGFW product, since Palo Alto Networks' architecture differs from the other vendors' architecture significantly.

6.3 Areas for Further Research

Palo Alto Networks will introduce PAN-OS version 6.0 at the 4th quarter of 2013, which will introduce more enhancements to the GP features and the NGFW itself. WildFire began to support Android packages officially in September 2013. By inspecting Android Application Packages; .apk's, NGFW supports more security visibility and reduces mobile risks, since Android is considered the riskiest mobile platform among the other mobile platforms at the moment (F-secure 2012, 8; F-secure 2013, 8). This is because of the open application platform strategy, whereas Apple's strategy is more controlled and is therefore considered more trustworthy.

In addition of supporting Android packages, other file types supported will be Microsoft Office documents; .doc, .xls, .ppt, Portable Document Format; .pdf and Java Archives; .jar. New features will be available for the customers starting at version 6.0. However, these new file types requires WildFire subscription (license) in the firewall, in order it to forward the files to the WildFire Cloud. Otherwise the FireWall only forwards the PE (Portable Executable) file formats to the cloud, e.g. .cpl, .exe, .dll. WildFire also enables incorrect verdict option for customers to submit to the WildFire Cloud, when they suspect that the sample is False Positive or False Negative. Palo Alto Networks' Threat Team will perform a further analysis on the sample to determine should it be re-classified in the AntiVirus profile, for example. The customer (submitter) will be always informed the results of the analysis. WildFire Analysis Reports can be downloaded directly from the NGFW's GUI. It includes the information of dynamic analysis of each virtual machine where the sample was analyzed. Packet captures generated by the sample file in the WildFire virtual environment can be also downloaded in the GUI. When upgrading to version 6.0, license upgrade of WildFire Subscription will be recommended for the companies using mobile devices and remote access connections for better addressing risks in the mobile environment.

Version 6.0 also introduces DNS Sinkholing and Extended Packet Capturing features. When a computer is connected inside a company network and wants to communicate with servers, it uses company's DNS servers, which converts host names to the valid IP addresses. The IP address is then forwarded to the client, which then establishes a direct connection to the server's IP address. This way, all the DNS queries are originated from the company's DNS servers. This is the reason, why all the other DNS queries are typically denied in the FireWall. But the problem is that FireWall only sees DNS queries coming from the company's DNS servers and not which client was the one that the DNS query was originated from. DNS Sinkholing feature address this problem by forging a response to the DNS query for a known malicious domain. This way the malicious domain name will be resolved to the administrator defined IP address and enables to identify possibly infected clients in the protected network using DNS traffic, even the FireWall cannot see the client's DNS queries. This administrator configured IP address is called Sinkhole IP address and can be used to detect possibly infected clients and identified in the traffic reports also.

DNS Sinkholing can be enabled in the existing profiles and so can Extended Packet Capture feature also. It enables to capture automatically more than just the first packet of the configured trigger. By default it is set to 5 packets, but can be configured from 1 to 50 packets to provide more content in the logs. This is a global setting which will affect to all packet capture settings that are defined to use extended mode in the NGFW's Security Profiles.

References

Check Point Software Technologies Ltd, 2013. Check Point Summary Analysis.

Check Point Software Technologies Ltd, 2010. Check Point Software Blade Architecture – Achieving the right balance between security protection and investment.

Dahlstrom, E. & diFilipo, S., March 25th 2013. The Consumerization of Technology and the Bring-Your-Own-Everything (BYOE) Era of Higher Education, EDUCAUSE Center for Applied Research.

Dimensional Research, June 2013. The Impact of Mobile Devices on Information Security. Referred to 13th September 2013. **Virhe. Hyperlinkin viittaus ei kelpaa..**

Emery S., July 2012. Factors for Consideration when Developing a Bring Your Own Device (BYOD) Strategy in Higher Education. University of Oregon.

F-Secure, 2013. Mobile Threat Report January-March 2013. Referred to 13th September 2013. [http://www.f-secure.com/static/doc/labs_global/Research/Mobile Threat Report Q1 2013.pdf](http://www.f-secure.com/static/doc/labs_global/Research/Mobile%20Threat%20Report%20Q1%202013.pdf).

F-Secure, 2012. Mobile Threat Report Q4 2012. Referred to 13th September 2013. http://www.f-secure.com/static/doc/labs_global/Research/Mobile%20Threat%20Report%20Q4%202012.pdf.

Gartner Inc., February 7th 2013. Magic Quadrant for Enterprise Network Firewalls. ID:G00229302. Referred to 13th September 2013. <http://www.gartner.com/id=2329815>.

Gartner Inc., May 1st 2013. Press release, Stamford, Conn. Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes. Referred to 13th September 2013. <http://www.gartner.com/newsroom/id/2466615>.

Gartner Inc., IT Glossary. Referred to 13th September 2013. <http://www.gartner.com/it-glossary/next-generation-firewalls-ngfws>

Gartner Inc. 14th December 2011. Magic Quadrant for Enterprise Network Firewalls 2011. ID:G00219235. Referred to 15th September 2013.

[Http://www.gartner.com/id=2329815](http://www.gartner.com/id=2329815).

Journal of Global Research in Computer Science (JGRSC), April 2013. Bring Your Own Device (BYOD): Security Risks and Mitigating Strategies, ISSN-2229-371X, Volume 4, No. 4.

Lloyd's Press Release, Wed 10th July 2013. Tax at the Top of Global Business Concerns. Referred to 15th September 2013. [Http://www.lloyds.com/lloyds/press-centre/press-releases/2013/07/tax-at-the-top-of-global-business-concerns](http://www.lloyds.com/lloyds/press-centre/press-releases/2013/07/tax-at-the-top-of-global-business-concerns).

Mandiant, 2013. APT1 Exposing One of China's Cyber Espionage Units. Referred to 15th September 2013. [Http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf](http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf).

ISACA Survey, November 2012: Enterprises in Europe Cautiously Accepting BYOD. Referred to 15th September 2013. [Http://www.isaca.org/About-ISACA/Press-room/News-Releases/2012/Pages/ISACA-Survey-Enterprises-in-Europe-Cautiously-Accepting-BYOD.aspx](http://www.isaca.org/About-ISACA/Press-room/News-Releases/2012/Pages/ISACA-Survey-Enterprises-in-Europe-Cautiously-Accepting-BYOD.aspx).

ISACA Survey, November 2012: ISACA Survey Reveals Cautious Acceptance of BYOD in Africa. Referred to 15th September 2013. [Http://www.isaca.org/About-ISACA/Press-room/News-Releases/2012/Pages/ISACA-Survey-Reveals-Cautious-Acceptance-of-BYOD-in-Africa.aspx](http://www.isaca.org/About-ISACA/Press-room/News-Releases/2012/Pages/ISACA-Survey-Reveals-Cautious-Acceptance-of-BYOD-in-Africa.aspx).

ISACA Survey, November 2012: ISACA Survey Reveals Canadian Enterprises Are Allowing BYOD, Despite Concerns. Referred to 15th September 2013. [Http://www.isaca.org/About-ISACA/Press-room/News-Releases/2012/Pages/ISACA-Survey-Reveals-Enterprises-Are-Allowing-BYOD-Despite-Concerns.aspx](http://www.isaca.org/About-ISACA/Press-room/News-Releases/2012/Pages/ISACA-Survey-Reveals-Enterprises-Are-Allowing-BYOD-Despite-Concerns.aspx).

ISACA Survey, November 2012: Latin American Companies Increasingly Worried About BYOD Risk. Referred to 15th September 2013. [Http://www.isaca.org/About-ISACA/Press-room/News-Releases/2012/Pages/ISACA-Survey-Latin-American-Companies-Increasingly-Worried-About-BYOD-Risk.aspx](http://www.isaca.org/About-ISACA/Press-room/News-Releases/2012/Pages/ISACA-Survey-Latin-American-Companies-Increasingly-Worried-About-BYOD-Risk.aspx).

ISACA Survey, November 2012: ISACA Reveals Enterprises in India Remain Wary of BYOD. Referred to 15th September 2013. [Http://www.isaca.org/About-ISACA/Press-room/News-Releases/2012/Pages/ISACA-Survey-Reveals-Enterprises-in-India-Remain-Wary-of-BYOD.aspx](http://www.isaca.org/About-ISACA/Press-room/News-Releases/2012/Pages/ISACA-Survey-Reveals-Enterprises-in-India-Remain-Wary-of-BYOD.aspx).

ISACA Survey. November 2012: ISACA Survey Reveals Growing Acceptance of BYOD in Australia and New Zealand. Referred to 15th September 2013.

[Http://www.isaca.org/About-ISACA/Press-room/News-Releases/2012/Pages/ISACA-Survey-Reveals-Growing-Acceptance-of-BYOD-in-Australia-and-New-Zealand.aspx](http://www.isaca.org/About-ISACA/Press-room/News-Releases/2012/Pages/ISACA-Survey-Reveals-Growing-Acceptance-of-BYOD-in-Australia-and-New-Zealand.aspx).

ISACA, 2012. ISACA's 2012 IT Risk/Reward Barometer. Referred to 15th September 2013. [Http://www.isaca.org/Pages/2012-Risk-Reward-Barometer.aspx](http://www.isaca.org/Pages/2012-Risk-Reward-Barometer.aspx).

ISACA, 2012: Advanced Persistent Threat Awareness Study Results. Referred to 15th September 2013. [Http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Advanced-Persistent-Threats-Awareness-Study-Results.aspx](http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Advanced-Persistent-Threats-Awareness-Study-Results.aspx).

ISACA Survey, November 2011: BYOD Trend Heightens Online Holiday Shopping Risk. Referred to 15th September 2013. [Http://www.isaca.org/About-ISACA/Press-room/News-Releases/2011/Pages/ISACA-Survey-Bring-Your-Own-Device-Trend-Heightens-Online-Holiday-Shopping-Risk.aspx](http://www.isaca.org/About-ISACA/Press-room/News-Releases/2011/Pages/ISACA-Survey-Bring-Your-Own-Device-Trend-Heightens-Online-Holiday-Shopping-Risk.aspx).

ISACA Survey, November 2011: IT Professionals in Africa Expect Employee Online Shopping to Increase Risk. Referred to 15th September 2013. [Http://www.isaca.org/About-ISACA/Press-room/News-Releases/2011/Pages/ISACA-Survey-IT-Professionals-in-Africa-Expect-Employee-Online-Shopping-to-Increase-Risk.aspx](http://www.isaca.org/About-ISACA/Press-room/News-Releases/2011/Pages/ISACA-Survey-IT-Professionals-in-Africa-Expect-Employee-Online-Shopping-to-Increase-Risk.aspx).

ISACA Survey, November 2011: IT Professionals in Canada Expect Employee's Online Shopping to Increase Risk This Holiday Season. Referred to 15th September 2013. [Http://www.isaca.org/About-ISACA/Press-room/News-Releases/2011/Pages/ISACA-Survey-IT-Professionals-in-Canada-Expect-Employee-Online-Shopping-to-Increase-Risk-This-Holiday-Season.aspx](http://www.isaca.org/About-ISACA/Press-room/News-Releases/2011/Pages/ISACA-Survey-IT-Professionals-in-Canada-Expect-Employee-Online-Shopping-to-Increase-Risk-This-Holiday-Season.aspx).

ISACA Survey, November 2011: IT Professionals in Oceania Predict Increased Online Shopping at Work. Referred to 16th September 2013. [Http://www.isaca.org/About-ISACA/Press-room/News-Releases/2011/Pages/ISACA-Survey-IT-Professionals-in-Oceania-Predict-Increased-Online-Shopping-at-Work.aspx](http://www.isaca.org/About-ISACA/Press-room/News-Releases/2011/Pages/ISACA-Survey-IT-Professionals-in-Oceania-Predict-Increased-Online-Shopping-at-Work.aspx).

ISACA Survey, November 2011: IT Professionals in Latin America Say Online Shopping at Work Increases Risk During the Holiday Season. Referred to 16th September 2013. [Http://www.isaca.org/About-ISACA/Press-room/News-Releases/2011/Pages/ISACA-Survey-IT-Professionals-in-Latin-America-Say-Online-Shopping-at-Work-Increases-Risk-During-the-Holiday-Season.aspx](http://www.isaca.org/About-ISACA/Press-room/News-Releases/2011/Pages/ISACA-Survey-IT-Professionals-in-Latin-America-Say-Online-Shopping-at-Work-Increases-Risk-During-the-Holiday-Season.aspx).

[Survey-IT-Professionals-in-Latin-America-Say-Online-Shopping-at-Work-Increases-Risk.aspx](#).

ISACA Survey, November 2010: IT Professionals in Europe Predict More Online Shopping at Work This Holiday Season. Referred to 16th September 2013.

[Http://www.isaca.org/About-ISACA/Press-room/News-Releases/2010/Pages/ISACA-Survey-IT-Professionals-in-Europe-Predict-More-Online-Shopping-at-Work-This-Holiday-Season.aspx](http://www.isaca.org/About-ISACA/Press-room/News-Releases/2010/Pages/ISACA-Survey-IT-Professionals-in-Europe-Predict-More-Online-Shopping-at-Work-This-Holiday-Season.aspx).

L 13.8.2004/759. Finnish Privacy Law. Referred to 21th September 2013.

[Http://www.finlex.fi/fi/laki/ajantasa/2004/20040759](http://www.finlex.fi/fi/laki/ajantasa/2004/20040759).

Laine, P. 2012. Hakin9, Issue 9, Real-Life Experiences with Next-Generation Firewall.

Metzler, J. 2007. Kubernan Briefs, Vol.1, number 6. Next Generation Firewalls – The Policy and Security Control Point. Referred to 9th October 2013.

https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/white-papers/kubernan-notes-vol1-no6.1.pdf

Nisharika S., Dec 2012. Journal of Business Management & Social Sciences Research, B.Y.O.D. Genie Is Out Of the Bottle – “Devil or Angel”. ISSN No: 2319-5614, Volume 1, No.3.

NSS Labs, February 2013. 2013 Next Generation FireWall Comparative Analysis. Referred to 12th Sptember 2013. <https://nsslabs.com/reports/2013-next-generation-firewall-comparative-analysis>.

NSS Labs Inc, 2012. Next Generation FireWall – Individual Product Test Results. Palo Alto Networks PA-5020. PAN-OS 4.0.5. Methodology Version: 4.0. Referred to 9th October 2013. <http://www.nsslabs.com/research/network-security/firewall-ngfw/>

NSS Labs Inc, April 2011. Network Intrusion Prevention Systems – Individual Product Test Results. Methodology version 3.0.

NSS Labs Inc, August 2010. Network Intrusion Prevention Systems – Individual Product Test Results. Methodology version 6.0.

Nucleus Research, April 2013. Research Note: Understanding the Hard ROI of BYOD, Document N65.

Osterman Research, November 2012. Referred to 20th August 2013. Next-Generation Firewall Management. **Virhe. Hyperlinkin viittaus ei kelpaa..**

Palo Alto Network, February 2013. The Application Usage and Threat Report, 10th Edition. Referred to 20th August 2013. **Virhe. Hyperlinkin viittaus ei kelpaa..**

Palo Alto Networks, March 2013. Modern Malware Review, 1st edition. Referred to 9th August 2013. <http://researchcenter.paloaltonetworks.com/2013/03/introducing-the-modern-malware-review/>.

Palo Alto Networks, 2010. Evasion Techniques and Palo Alto Networks Solution Resilience.

Palo Alto Networks, May 2010. Application Visibility and Control: In the FireWall vs. Next to the FireWall. How Next-Generation Firewalls are Different from UTM and IPS-based Products.

Palo Alto Networks, December 2008, Single Pass Architecture – Palo Alto Networks Architecture Whitepaper.

Rissanen, J. 2012. Next-generation firewall in a corporate network. Referred to 29th September 2013. <http://urn.fi/URN:NBN:fi:amk-201205148149>. Thesis, Lahti University of Applied Sciences. Theseus-portal.

The Guardian, July 31 2013. XKeyscore: NSA tool collects ‘nearly everything a user does on the internet’. Referred to 9th August 2013. <http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>.

Vanwelsenaers, M. Dec 6th 2012. Students Using Their Own Technology Device In The Classroom: Can “BYOD” Increase Motivation And Learning. Michigan University.

Verizon, 2013. 2013 Data Breach Investigation Report. Referred to 27th August 2013. <http://www.verizonenterprise.com/DBIR/2013/>.

Viitamäki, A. 2013. Aruba BYOD or Citrix VDI as Solution for Multinational Enterprise. Thesis, JAMK, University of Applied Sciences. Referred to 29th September 2013. <http://urn.fi/URN:NBN:fi:amk-201305169097>. Thesis, Metropolia University of Applied Sciences. Theseus-portal.

Appendices

Appendix A. Application usage and Threat Report February 2013. Palo Alto Networks

Appendix A: Application Usage and Threat Report – February 2013

