Harri Lehmonen

Improving Network Security with Watchguard UTM Firewall

Helsinki Metropolia University of Applied Sciences

Master's Degree

Information Technology

Master's Thesis

1 March 2017

PREFACE

This Master’s thesis contains information about how small and midsize businesses can improve their network security without spending too much money to acquire it.

One of the hardest challenges nowadays is to make customers aware that different kinds of security threats are not just something that we read from the news. They are all around us and some preventive measures must be taken before they hit one’s company.

There are many different vendor’s appliances to be utilized. In this case the Watchguard UTM device was studied.

I want to thank Etevä Tietopalveluyhtiö for giving me the chance to do this thesis. I also want to thank our customers who have been a part of this study.

Special thanks go to Ville Jääskeläinen who instructed me with this thesis. Also, thank you Tero Vesimäki for your insights.

Vantaa March 1 2017

Harri Lehmonen

Author(s)	Harri Lehmonen
Title	Improving Network Security with Watchguard UTM Firewall
Number of Pages	54 pages + 1 appendices
Date	1 March 2017
Degree	Master’s Degree
Degree Programme	Information Technology
Instructor(s)	Ville Jääskeläinen, Principal Lecturer, Metropolia Tero Vesimäki, System Architect, Etevä Tietopalveluyhtiö

After working many years in close contact with end customers, the author has noticed that Finnish small and mid-size businesses are not paying as much attention to network security threats as they should. Even though different kind of security threats are probably present and reported often in news, very basic security practices are discarded and no resources are spent advancing the issue.

The topic of this thesis is Improving Network Security with Watchguard’s UTM Firewall. It focuses on how to gain more security with as simple a mean as replacing the old firewall with a new firewall with UTM features. UTM stands for Unified Threat Management and it is a set of features that work within the firewall to investigate passing traffic in order to find anomalies and threats.

In this thesis, first different kind of threats are presented. After that various UTM modules are described, followed by the best practices about how to install the Watchguard firewall. The customer’s current environment was investigated, a proof of concept with a new firewall with UTM features was deployed with the best practice information and details that were agreed on with the customer.

After the deployment, data was gathered for a couple of months. The gathered data was then analyzed and multiple findings of viruses and intrusions were discovered. Also botnets and bad URL’s were blocked. The findings were clear evident of the proof of concept and supported the recommendation about the purchase. The final deployment was made and the customer was pleased with the new security system. The customer continues to invest on improving their security in general.

Keywords	Firewall, UTM, Watchguard, Network Security

Contents

Abbreviations/Acronyms

CPU	Central Processing Unit
DDOS	Distributed Denial of Service
DLP	Data Loss Prevention
HIPAA	Health Insurance Portability and Accountability Act
IP	IP Address
IPS	Intrusion Prevention System
IT	Information Technology
MEM	Memory
NGFW	Next-Generation Firewall
OSI	Open Systems Interconnection Reference Model
PCI DSS	Payment Card Industry Data Security Standard
POP3	Post Office Protocol version 3
SHDLS	Single-pair High-speed Digital Subscriber Line
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTM	Unified Threat Management
VOD	Virus Outbreak Definition
XSS	Cross-site Scripting

1 Introduction

Based on a 10 years' experience of the author in the managed service provider industry and working very closely with small and mid-size business, lots of customers have been seen who lack basic security function in their private networks. Times have changed from when the firewall was just a simple piece of equipment on the border of the customer's network. Technology has gone forward for those who will try to gain hacking a non-secure network, but for also those who are trying to protect it.

According to large Internet Security Threat Report made by Symantec they alone have discovered more than 460 million new unique pieces of malware in 2015 [1]. According to the study made by the University of Phoenix in 2014, organizations were spending 46 billion dollars in cyber security. The cost defending against threats and what breaches cost to companies were increased more than 20% per year [2]. At the same time, McAfee estimates that global cyber activity estimated to cost $300 billion to $1 trillion loss per year compared to the drug trafficking estimate of $600 billion [3]. The global cyber activity was projected to reach $2 trillion yearly loss by 2019 according to Forbes author Steve Morgan [4].

Most organization users or decision-makers were not willing to pay extra or they were relaying on their luck when it comes the security. Technical persons saw the risks, but were not capable to communicate clearly with executives. At the same time teaching individuals about the best practises of how to get along with different security related issues was effective, but the same time very time consuming. Threats are constantly changing so yesterday's lectures may not apply today, or have slightly changed appearances. Even the smallest changes in security will improve the overall status of security and will make human mistakes easier to control and possible security breach attempts harder to accomplish.

In this master's thesis today's security threats are explored and explained and then evaluated how one can easily eliminate some of them. The term UTM means Unified Threat Management which was a set of security features that are applied into the traffic when it passes the firewall which was located at the border of an office interior network. Watchguard has spent years polishing their products, which were in fact composed of different well-known suppliers products and then combined them into one compact product that does it all.

Differences between traditional and UTM firewall are examined and also what different options or UTM features are available. The evaluation was made about what advantages they bring or if they are over appreciated. The best practice of configuring the UTM features to get most out of them is also gone through in the study, as well as applying the customer's needs and the environment itself where the UTM firewall was used.

1.1 Business Problem

The need for the present study laid in one of the commissioner's long-time customer's network - they still had an old traditional firewall. It lacked every modern-day security features. It also had very limited logging and reporting features and it merely told if someone had tried to login to the firewall using a wrong root/admin username. Any logging about security rules was missing, so basically, one had no idea what was happening in the firewall or in the network.

Another reason for the study was that different security measures had already been tried to be implemented to the customer's environment, but they did not improve the overall security status sufficiently. Also, the constant education of risks and behaviour altering was discovered to be time consuming and a very ineffective way to spread the knowledge. A new way to get more security without using valuable time and to automate some of the processes would be the best solution.

1.2 Objective

The objective of the study was to create an action plan that would indicate how one can improve their customers' network and infrastructure security by deploying a Watchguard UTM firewall. The main goal was to gain more security and to show what advantages the new UTM firewall would bring.

Another objective was to bring more logging and reporting features. These were not only for the technical support to indicate and evaluate risks, to make changes to configuration and to keep eye on what happens in the network, but for also for corporate executives to show what security measures have been taken and that way to support the acquisition by bringing more value to it.

1.3 Method

The research method in qualitative. A proof of concept was made in the customer's premises to gain actual information about their use and weather the product and the features improve their overall security state and therefore justifies the acquisition.

1.4 Research Design

The paper starts with an introduction to network security, listing the most important security threats with short descriptions. After that, basic user security practises are discussed along with how firewalls have developed over the years. Next, different firewall UTM features are explained specifying the benefits they bring regarding network security. Then the study moves on to explaining the best practises of firewall installation considering the UTM features taking a short glance at logging features.

Next, the study focuses on analysing the current state in the customer's environment based on information collected and mapped and on the customer's needs. Also, requirements for the new systems are listed. After that, the study moves on to explaining the deployment plan and the customer specific configuration based on the best practises.

After that, the data collected over several months about the firewall's activity is presented. The data is then analysed and the findings are explained and evaluated. Finally, the outcome and proposition of the security solution made to the customer are introduced. The study ends with the discussion and conclusions.

2 Network Security

Network security landscape has changed significantly during the past years. Different kinds of cyberthreats are almost part of everyday news. Most of the time these news deal with large multinational organizations. It brings a question if these large organizations with enormous IT budgets cannot properly protect themselves, what about the small and midsize businesses?

Finnish Chambers of Commerce published a study in 2015 which focused specifically on Finnish companies. 748 Finnish companies were interviewed for the study. Most of the companies were small companies with less than 50 employees. The study clearly showed that Finnish companies are not sufficiently prepared to cyber security.

The study showed that when Finnish companies had been interviewed, the three-top reasons for why they had not accomplished a sufficient cyber security level were:

1. User disregard to cyber security and cyber threats
2. Insufficient information about cyber threats
3. Maintaining the know-how of cyber-threats for current employees

According to the same article, 48% of the Finnish companies do not have no plan if a cyber-attack occurs. [5]

From that article one can draw a couple of conclusions. First, the users' knowledge about different kinds of threats must be increased. The training and instructing must include concrete examples of what to do and what not to do. One cannot rely merely on news and that way demonstrate what has been done wrong. It was recommended that a security strategy dictating guidelines for the users was made.

Secondly, some kind of automation must be deployed to handle at least the most common threats in order to bring more security. Small companies seldom have their own IT department or even one person that handles IT matters. Usually IT was outsourced to a 3rd party support. That is a reason why technology must be quite simple, but still it has to be efficient and include different kinds of features that are needed.

2.1 Security Threats

As the use of the Internet has rapidly grown, it has left lots of room for abuse and misuse. Even though anti-malware technologies have been developed there are far too many grey areas where criminals can do their malicious acts. At the time this thesis was written, hackers had done viscous acts mainly for publicity and maybe to gain large amounts of money. But now it was obvious that hackers have been more and more focused on organizations of every size or human individuals from whom they can profit.

A clear example of an organization targeted attack is different variants of crypto lockers. Crypto locker is a term for malware that is used to encrypt the end-user's computer or the whole computing environment. The malware itself is usually delivered as an attachment in an email. After encryption, a ransom is usually demanded in exchange of the decryption information. They are not specifically targeted and rely more on someone somewhere getting affected and paying the ransom.

The latest individual targeted threat is called a spear-phishing attack. It means that the hacker has found out some level of detail about a certain person and uses this as leverage to gain more useful information, such as credit card or bank account information or passwords. Information that is used against that individual is gathered from social media and these scams are usually carried out via email or even SMS.

The latest comer in the security threat landscape is Malware for hire. That way, almost anyone can hire a service to attack with different types of malware a certain party. That makes the usage of malware very simple as one does not need to know the technical details or even have the skills to use it. It is enough if one has the money to pay for it. This type of attack makes malware very targeted, as the buyer usually already knows how to use the purchased assets.

Within the scope of this thesis it was impossible to through every kind of security threat or malware there was. Below are listed the most common types of malware with a short description. [8] [9]

Virus – Usually a program that runs when activated in the destination system. Multiplies in order to contaminate more systems. Normally has some kind of objective as destroy or steal data.

Worm – Uses network to contaminate different systems. Self-replicated. Usually eats or destroys the file system.

Trojan Horse – Uses usually legitimate software that is imbedded with malicious code. Can be used widely from spying to taking control of the whole system. Acts also as a backdoor to the system.

Zombie or Bot – Is a single computer or a system that is affected of some sort malware. Can be remotely controlled and used without user’s knowledge.

Botnet – Group of Zombies or Bots that can be remotely controlled for example to DDOS-attack.

Rootkit – A piece of software or code that is buried deep in to the operating system or software. Can be used as a backdoor or can be activated in desired time. Very hard to detect as the code can be passive long periods of time.

Spyware - Usually uses malicious program that was installed to the system without user knowing about it. Can use key logger to steal usernames, passwords or banking information. Can also be used for surfing cookies to excavate information. Sends information to the attacker.

Adware – Passive component that is installed to a computer when visiting affected website. Usually don’t cause much damage and is more of a disturbance.

Ransomware – Usually email based malware that contaminates a computer or whole system by encrypting files system and then asks for a ransom. Very common these days and lucrative to attackers.

Scareware – Like ransomware, but doesn’t do anything but tries to scare users to pay some kind of a fee.

Crimeware – Is used to steal person’s identity to gain monetary benefit. Can use key logger or other means to steal information. Usually acts in a background.

Most of the malware detections are based on signatures. As a new code or file is detected as malicious, a signature is created against it, to recognise it again. There is a problem that the first time a malicious program or code is released it will go through every defence system until it has been recognized and a signature has been build. This same problem is with different variants of malware which will passed the defence until properly identified.

This problem was tried to be revised many years ago, by creating technologies such as heuristic detection. Heuristic detection means that the code is compared to a previously identified malicious code and it is then classified as a variant.

The second, newer approach to these unknown files without a signature, was a cloud based sandboxing with full system emulation. In this way, the unknown sample can be sent to this cloud service. In the cloud service the file or code will be run in different sandboxed environments to see if something triggers it and what it is.

Another attack type worth mentioning is injection attacks. In an injection attack the attacker disrupts the normal data stream of the user by injecting code or scripts to it. This is commonly done by inserting an extra part to the code segment where only should be data. This allows the attacker to control and perform action on the used program. The most common injection attack is SQL injection.

Cross site scripting XSS vulnerabilities can also been considered as injection attack. In XSS the attacker uses malicious scripts that are either inserted to the website code or executed from a 3rd party source on a trusted “good known” website. Usually the user’s browsers have no way of knowing that an XSS exploit has taken place. The most common sources of the attack are JavaScript, ActiveX and Flash. [10]

In Watchguard’s whitepaper [6] made in 2011 they referred to Gartner’s study in which they showed that exploits were not only found on bad reputation websites. They showed that even many legitimate websites such as MSNBC, ZDNet, United Nations, Honda, MySpace, and Excite.com had been compromised. In addition malware can be found in:

- 60% of the top 100 sites
- 75% of legitimate web sites
- 1% of Google search results

In Symantec’s study, [1] 78% of all webpages in 2015 were considered to be vulnerable, that means that if they were exploited they could have allowed execution of malicious code. Furthermore 15% of those were considered to be critical. Together with unpatched browsers and plugins this could have led to an end-to-end attack.

2.2 Basic User Security

By far the best way to protect against different kind of security threats and any other kind of threat is education. The more the customers or employees are educated the more they know and the more they can be prepared for different kind on anomalies and then act on them. There are only a couple of problems in education. Firstly, the education itself is very time consuming. When living and working in very hectic society, education of this sort is usually considered pointless. Secondly, it is very hard to reach all of the employees. It is important to educate every person in the organization as they all are using the same tools no matter what their job description is. Nowadays attacks can be well targeted so no one is safe. The third point is that as the threats are constantly changing it is very hard to keep the education up-to-date, so some kind of a basic level of knowhow should be established.

One way to control the environment is to make strict boundaries on how to act in the IT environment. Below is described a few ways that have a positive effect on gaining more security:

- Restrict the way users can download files – deny downloading of known file types including executables (.exe, .com), dynamic-link library (.dll) and compressed archives (.zip) and only allow downloading them in separate request.

- Restrict or deny the use of removal drives as they pose a huge security risk. Apply some sort of removal media policy such as Microsoft Windows Bit Locker. Use anti-virus software to scan any removal media before using it on a computer that is attached to corporate network.

- For email attachment, use at least the anti-virus software email attachment scanning feature. More secure solution is a 3rd party email cyber solution that includes anti-virus, malware and zero-hour features.

There are of course ways the IT department can make the working environment a little safer and establish a baseline of security without any kind of security hardware.

- The most important thing is to keep everything up-to-date at all times. A big part of the security vulnerabilities come from software not being up-to-date. So, operating systems, browsers and software that are frequently used should be always kept up-to-date.

- Some kind of antivirus software should always be installed. That is a very cheap, easy and simple way to keep up basic security. The software should contain adequate features e.g. anti-virus, anti-spyware, anti-rootkit and preferably a firewall feature. Also, regular anti-virus scans should be applied to the environment to make sure the environment stays clean.

- Extra attention should be paid to browsers. They should always be kept up-to-date. Additionally, some sort of a popup-blocker should be used. Popups can contain malicious code that can be run without the user's attention. Also, one should pay attention to the behaviour of browser cookies as they can include personal information about the user.

- A very useful action the IT personnel can take is to make software restrictions. That way they can control what software is used on the customer's computers and minimize the chance that any invalidated and not wanted, possibly harmful software is used in the environment. That way the IT professionals will have control over what software to update in order to keep the environment in the best condition possible.

2.3 Firewall Evolution

Firewalls have been used in IT to secure internal and perimeter networks for over 20 years. Over the year’s firewalls have evolved and more features have been added to them to gain more control and security to network traffic. The main function of a firewall is to keep unwanted people outside the internal or perimeter network.

The first generation firewalls are considered as packet-filter firewalls. It is one of the simplest forms of firewall. It functions based on a pre-defined rule-set. Packets are accepted or denied according to those rules. The rules include the source and destination IP address and the source and destination TCP/UDP port. The first generation firewalls typically do not differ from switches used for routing traffic. They act the same as the routing decision was based on a pre-made access-list. Packet filtering operates mainly on the three first layers of the OSI model.

In the second generation firewalls there is stateful inspection of packets included. This means that the firewall operates up to the OSI layer 4 (transport layer). This way the firewall can determine if the packet is part of an existing connection or if the connection is new. The firewall keeps track of these “states” of connection.

Both the packet-filtering and the stateful inspection are good ways to bring more security to the network. The problems were that both of them are too static and they do not make any decision about the nature of the traffic. This is why more complex techniques are needed to bring more security.

The third generation firewalls are so called proxy firewalls. They are also called application proxies or gateway firewalls. They act as a proxy between the user and the internet or vice versa. The most important function is to intercept, analyse and make a decision based on the traffic. They operate on the OSI layer 7 (application).

The next step in the evolution is a firewall that combines several useful technologies in one product. They are called NGFW - Next Generation firewalls or UTM – Unified Threat Management Firewalls. Both of the acronyms mean more or less the same. The idea is that the device is more than a firewall and includes techniques that help to make a network safer. [11] Next, the security features of UTMs are introduced more in detail.

2.4 UTM Security Features

Almost every UTM firewall includes the same set of features. Common to them is that the different features of the firewalls are not directly produced by the firewall maker itself, but the feature set is merely a collection of the best programs available combined together. This divides the firewall into two – hardware and software.

Below is described the basic features of a Watchguard UTM firewall and how the features are meant to function. Almost every module relies on cloud based signatures that are constantly kept up-to-date. [12]

Intrusion Prevention (IPS) – This can be divided in to two parts. The first part is a firewall-based IPS. A firewall-based IPS scans traffic and detects any anomalies and malformed packets from the traffic. It is a real-time scanning service, so it takes a little of computing power. The second part is called a signature-based IPS, it relies on existing patterns and signatures and scans them from the traffic stream. It requires less computing power. Both provide an effective way to block common network attacks.

Webblocker URL Filtering – Webblocker functions in two ways. Firstly, it relies on a centralized database which contains lots of internet sites that have a bad reputation. That way users are automatically denied access to certain internet sites that might have malicious content. The second part is manual listing of sites or categories that are not allowed to be accessed. These sites may contain pornography, gambling or other illegal content or content that is otherwise irrelevant.

Gateway antivirus – The antivirus function checks for viruses, trojans, worms and other malware directly from the traffic. This way the malicious content never ends up to the end-user’s computer. The antivirus feature relies on signature based detection and it uses heuristics to detect malware.

Reputation enabled defense service – This is a real-time service that automatically blocks access to internet sites that have a bad reputation. It collects information from multiple sources.It also lowers the need of anti-virus by blocking the access altogether. It includes botnet detection which automatically blocks traffic from and to known botnets. The reputation enabled defense service is quite similar to the Webblocker module, but it differs in that it is a completely automatic service. The only change that can be made is that the URL rated score that indicates reputation can be changed.

Spamblocker – Spam blocker can be used in front of an email server. It effectively blocks spam from SMTP and POP3 traffic. Spamblocker relies on Recurrent Pattern Detection technology which instantly detects any outbreaks as they appear.

Application control – With Application control one can determine what programs the user is allowed to use when accessing the internet from a corporate network. Every IP packet includes information about the program that was used. That way one can restrict or even deny the use of certain programs. This was an easy way to apply corporate policies and to add security to the network by denying unwanted programs. Also, it was easy way to reduce bandwidth use.

Some additional features that are not part of the basic security feature set are listed below.

APT Blocker – ATP Blockers is a newer technique built to fight against new threats that do not yet have signatures. It functions as follows - if an unknown file is received at the firewall level and it does not have a signature yet, the file is sent to the sandboxed cloud environment where it is tested in different environments with different actions. A signature is generated to the file whether it is clean or infected. If the file is clean it is passed through to the user. If the file contains malicious components, it is blocked. This is a very efficient way detecting ransomware, zero-day threats and evolved malware.

Host Ransomware Prevention – Ransomware Protection is the newest module in the Watchguard feature set. It is design to prevent ransomware before the encryption of host systems starts. The key feature is an agent that is installed to host systems and which acts as host sensor. This module works closely together with other modules such as APT Blocker and Webblocker.

Data loss prevention (DLP) – The data loss prevention module is meant to prevent sensitive data leaking from the corporation. A firewall scans the traffic that passes through it and detects if sensitive information is sent. This includes social security numbers, phone numbers, credit card numbers, bank account information etc. It has built in rules and is compliant to HIPAA - Healthcare related information and PCI DSS - Payment Card Industry Data Security Standard.

This list gives insight of most common features and operation. Different firewall vendors might have more features or the features can be named differently.

2.5 Benefits of UTM

With UTM features one can prevent lots of different exploits including malware, injections, files and code without signatures, malicious sites and much more. These attacks or threats can be intended and targeted or unintended, nevertheless without these features and reporting attached to it, IT is blind to see what happens in the network.

One still needs to remember that security is like an onion with many different layers and UTM features just bring one more security layer. There are still several threats that the UTM features alone cannot completely protect, including careless and disgruntled employees, mobile devices, unpatched devices, USB drives etc. For complete security to be achieved a solid information security plan should be made.

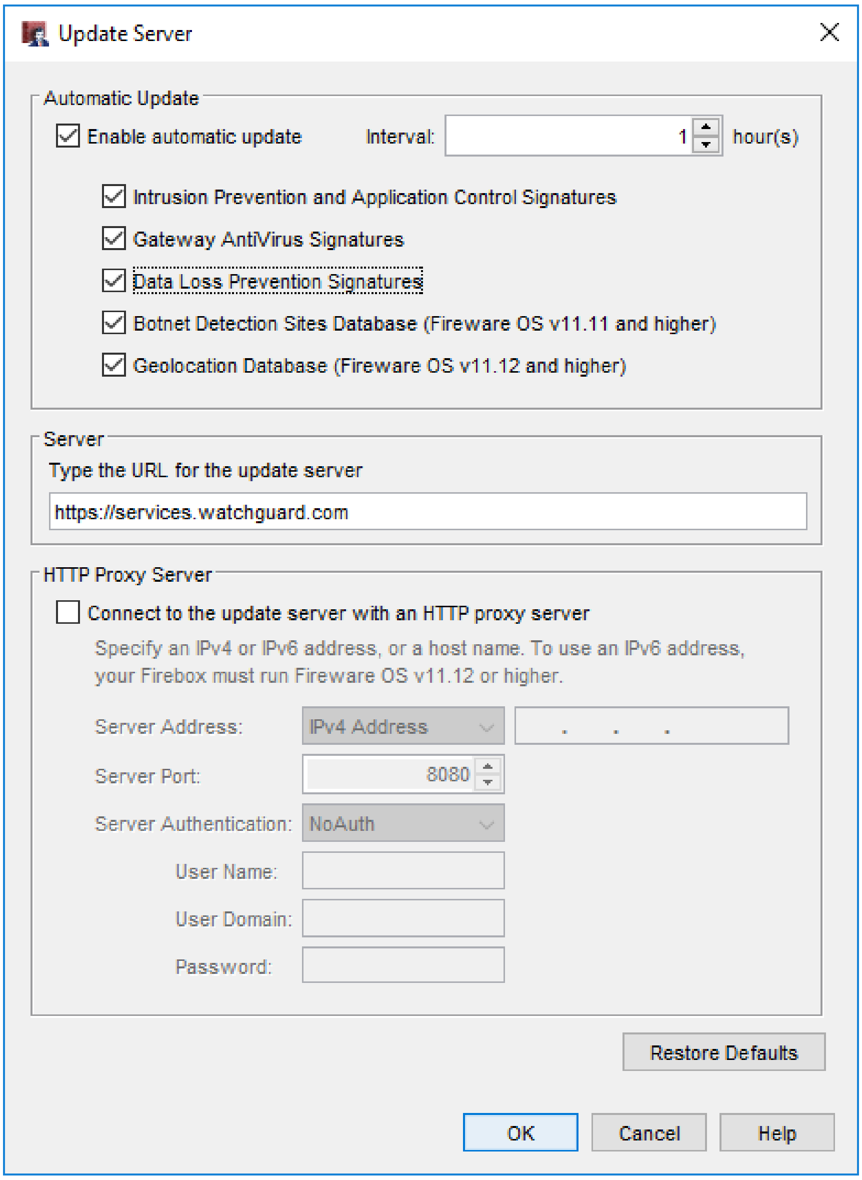
There are many different vendors offering firewalls with UTM features. Unfortunately, there is no good way to compare them as there are no independent studies to be found. There are sponsored studies made by companies such as Gartner which only deals with one certain feature or a single manufacturer’s devices. Because there is no study where different manufacturers models or features would be compared in the same manner, the studies are not independent enough to be relied on.

2.6 Watchguard UTM Installation / Best Practise

The next section describes how to configure the Watchguard UTM firewall according to the best known practice. The basic firewall configuration rules and internal network settings are described only if they are necessary in setting up the UTM features. All the settings should always be configured and are not customer dependent.

Some basic settings should always be configured before setting any other features. These include the automatic update feature which will automatically update certain signature definitions The automatic definitions include Signatures for Intrusion Prevention, Application Control, Gateway Antivirus, Data loss Prevention along with Botnet and Geolocation databases.

From the update server, the enable automatic update with 1 hour interval must be configured. Also, all the different module updates must be enabled. (Figure 1)



Update Server

Automatic Update

☑ Enable automatic update   Interval: 1 hour(s)

☑ Intrusion Prevention and Application Control Signatures

☑ Gateway AntiVirus Signatures

☑ Data Loss Prevention Signatures

☑ Botnet Detection Sites Database (Fireware OS v11.11 and higher)

☑ Geolocation Database (Fireware OS v11.12 and higher)

Server

Type the URL for the update server

https://services.watchguard.com

HTTP Proxy Server

□ Connect to the update server with an HTTP proxy server

Specify an IPv4 or IPv6 address, or a host name. To use an IPv6 address, your Firebox must run Fireware OS v11.12 or higher.

Server Address: IPv4 Address . . .

Server Port: 8080

Server Authentication: NoAuth

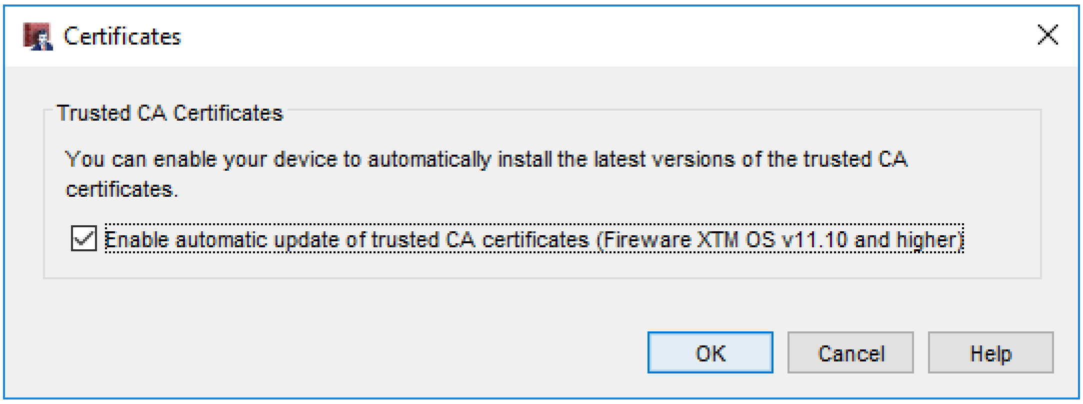
User Name:

User Domain:

Password:

Figure 1. Update Server settings

Another automatic update feature that should be enabled is the Automatic update of certificate. (Figure 2)


Certificates

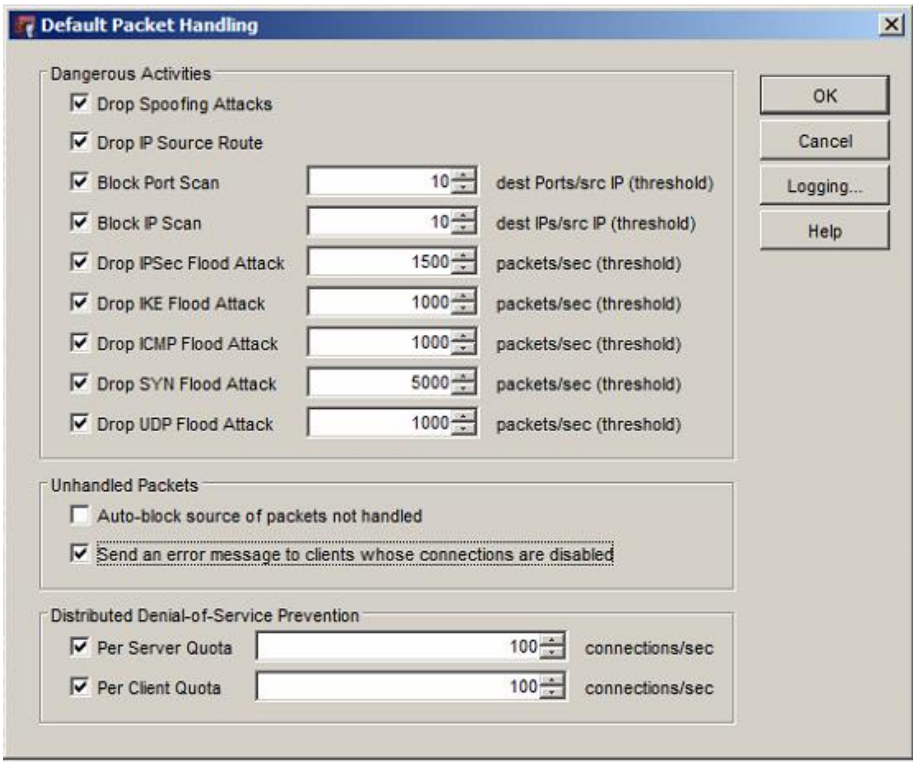
Trusted CA Certificates

You can enable your device to automatically install the latest versions of the trusted CA certificates.

☑ Enable automatic update of trusted CA certificates (Fireware XTM OS v11.10 and higher)

Figure 2. Auto update certificates

To strengthen the firewall settings, extra attention must be paid to default packet handling policies. All *Dangerous Activities* tick boxes should be selected to avoid the very basic type of network attacks. Packets that are not handled, must not be blocked automatically, because this can lead to a situation where a legit source of traffic gets blocked when sending packets that for example have no policy associated. Also the user should be informed if connections are disabled. (Figure 3)


Default Packet Handling

Dangerous Activities

☑ Drop Spoofing Attacks
☑ Drop IP Source Route
☑ Block Port Scan 10 dest Ports/src IP (threshold)
☑ Block IP Scan 10 dest IPs/src IP (threshold)
☑ Drop IPSec Flood Attack 1500 packets/sec (threshold)
☑ Drop IKE Flood Attack 1000 packets/sec (threshold)
☑ Drop ICMP Flood Attack 1000 packets/sec (threshold)
☑ Drop SYN Flood Attack 5000 packets/sec (threshold)
☑ Drop UDP Flood Attack 1000 packets/sec (threshold)

Unhandled Packets

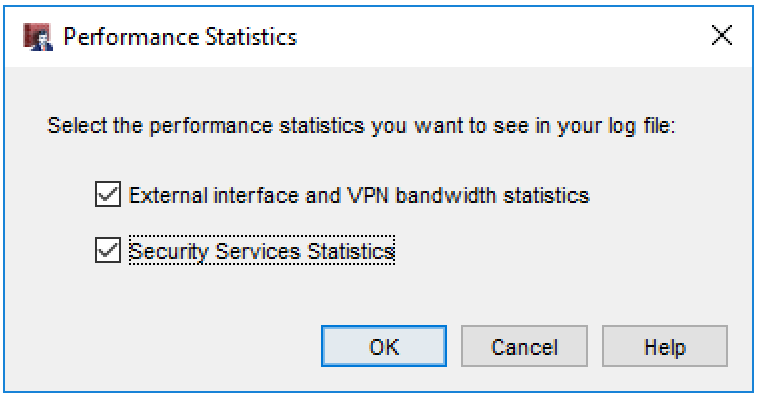
□ Auto-block source of packets not handled
☑ Send an error message to clients whose connections are disabled

Distributed Denial-of-Service Prevention

☑ Per Server Quota 100 connections/sec
☑ Per Client Quota 100 connections/sec

Figure 3. Default Packet Handling

It is important to collect performance statistics in a way that one can get accurate statistics about the traffic passing the firewall and about UTM features. (Figure 4)



Performance Statistics

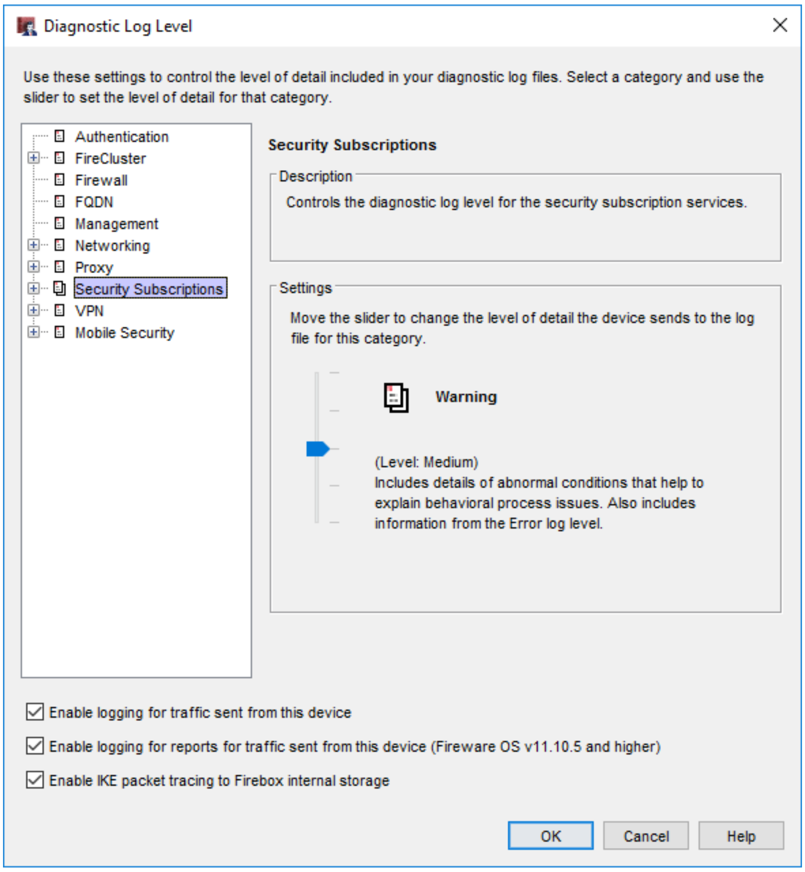
Select the performance statistics you want to see in your log file:

☑ External interface and VPN bandwidth statistics

☑ Security Services Statistics

Figure 4. Performance Statistics

The diagnostic level needs some changes, too. Logging for the sent traffic must be enabled (all tick boxes as shown below in Figure 5). Also, the diagnostic level itself for the Security Subscription must be raised from *Error* to *Warning*. That way a better logging level is achieved.



Diagnostic Log Level

Use these settings to control the level of detail included in your diagnostic log files. Select a category and use the slider to set the level of detail for that category.

Security Subscriptions

Description

Controls the diagnostic log level for the security subscription services.

Settings

Move the slider to change the level of detail the device sends to the log file for this category.

Warning

(Level: Medium)
Includes details of abnormal conditions that help to explain behavioral process issues. Also includes information from the Error log level.

☑ Enable logging for traffic sent from this device

☑ Enable logging for reports for traffic sent from this device (Fireware OS v11.10.5 and higher)

☑ Enable IKE packet tracing to Firebox internal storage

Figure 5. Diagnostic Log Level

In order to use the different kind of UTM features the traffic should not only pass the firewall, but it should also pass a certain type of proxy that should be added to the firewall's traffic policies. (Figure 6)

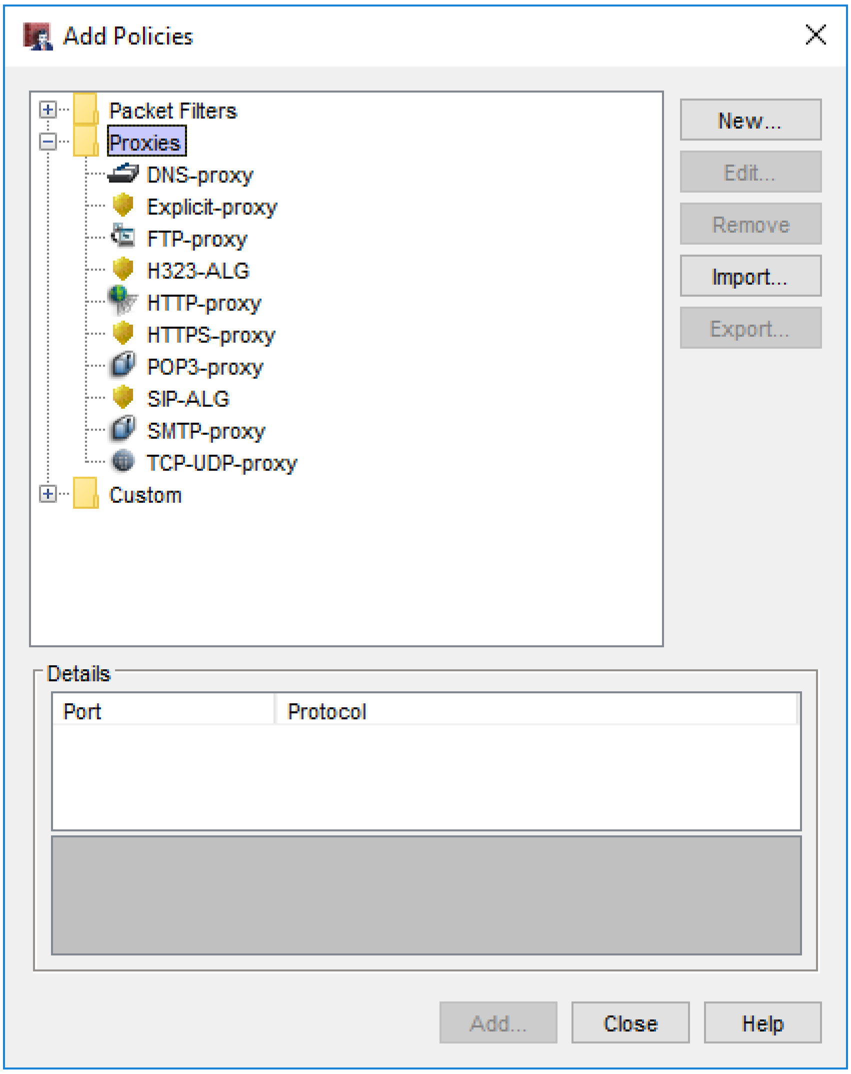
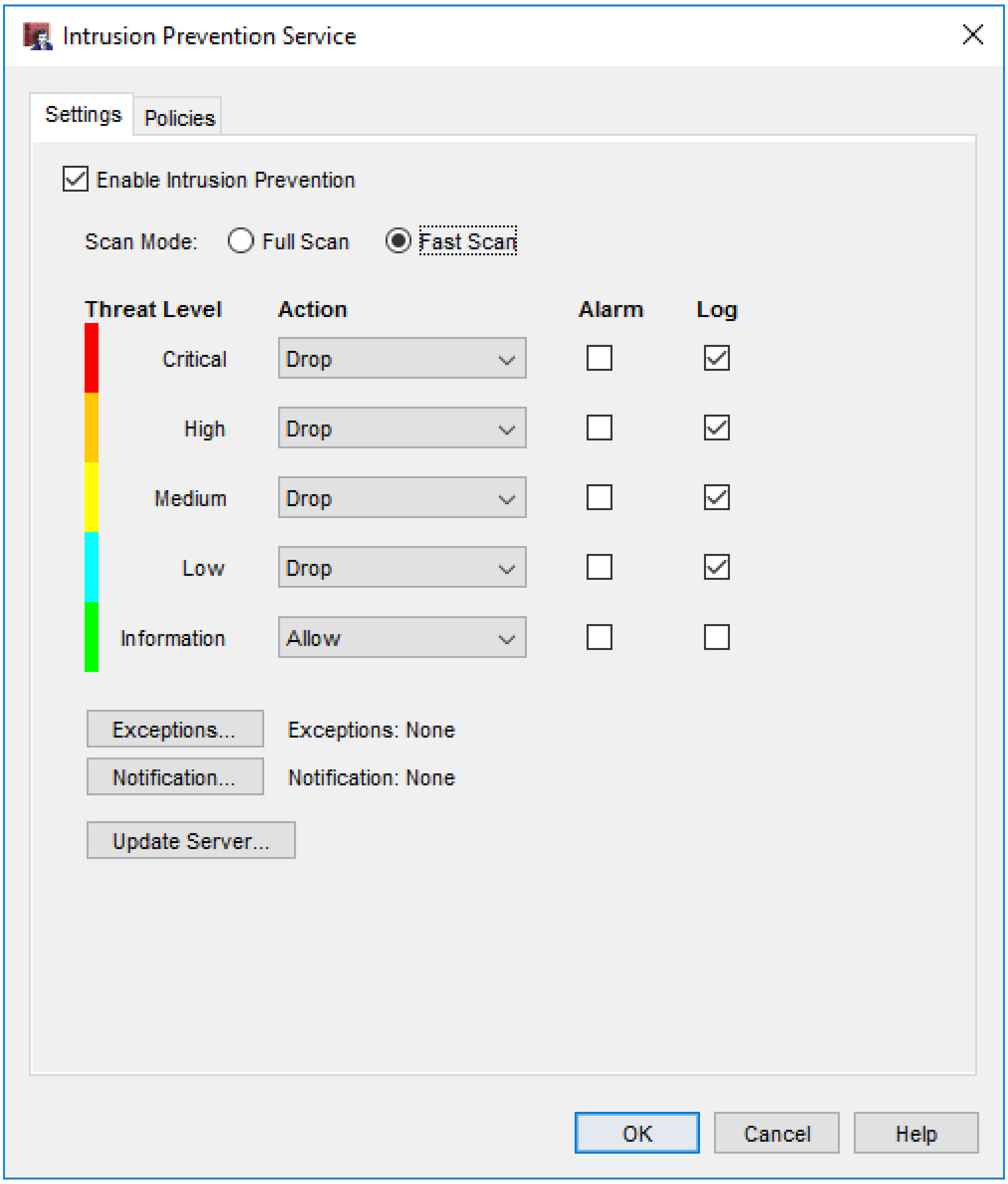


Figure 6. Adding policies

After the desired application proxies have been selected and policies have been modified to allow or deny traffic from a certain client to internet, different features can be applied to that traffic policy.

Intrusion Prevention (IPS) – After Enabling IPS, the feature it will automatically be enabled to all existing and new firewall rule policies. Default settings need no adjusting at this time, since fast scan is suitable for most environments. Full scan demands more calculation power and can affect the performance of the firewall. (Figure 7)



☑ Enable Intrusion Prevention

Scan Mode: ○ Full Scan ● Fast Scan

Threat Level	Action	Alarm	Log
Critical	Drop	□	☑
High	Drop	□	☑
Medium	Drop	□	☑
Low	Drop	□	☑
Information	Allow	□	□

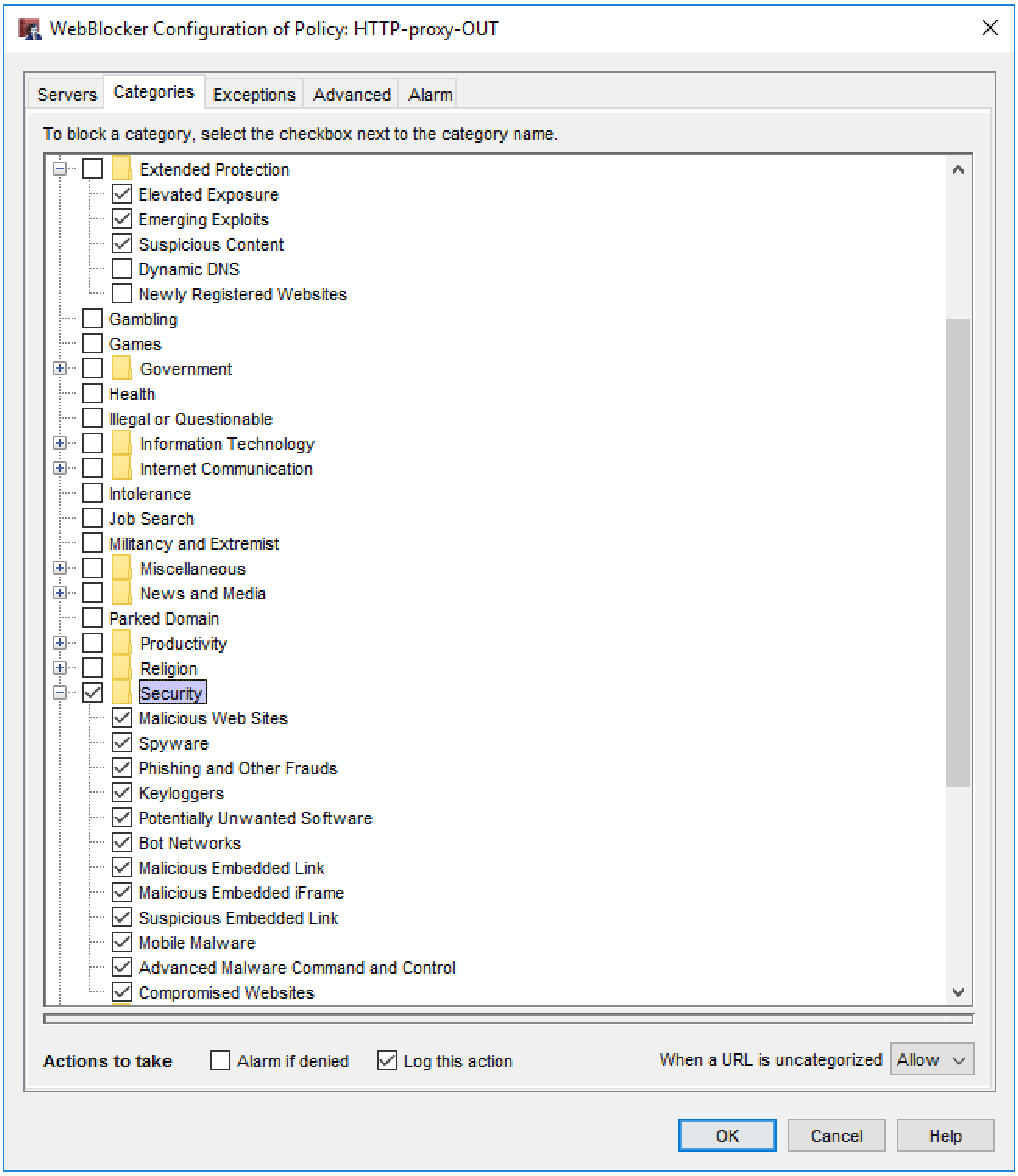
Exceptions... Exceptions: None

Notification... Notification: None

Update Server...

Figure 7. Intrusion Prevention Service

Webblocker URL Filtering – From the Webblocker settings, the Websense cloud option was used for Webblocker lookups. It has 130 different categories to choose from. Various settings can be applied, for example if the Websense service was unavailable, access to denied categories was allowed or denied. Also, an exception list can be built to always grant access to certain important pages. It was possible to setup an access phrase and give it to users who need access to the denied sites although all other users' access was denied. The following categories (see Figure 8) should at least be turned on to gain more security – from Extended Protection: Elevated Exposure, Emerging Exploits and Suspicious Content and all items from Security category.



WebBlocker Configuration of Policy: HTTP-proxy-OUT

To block a category, select the checkbox next to the category name.

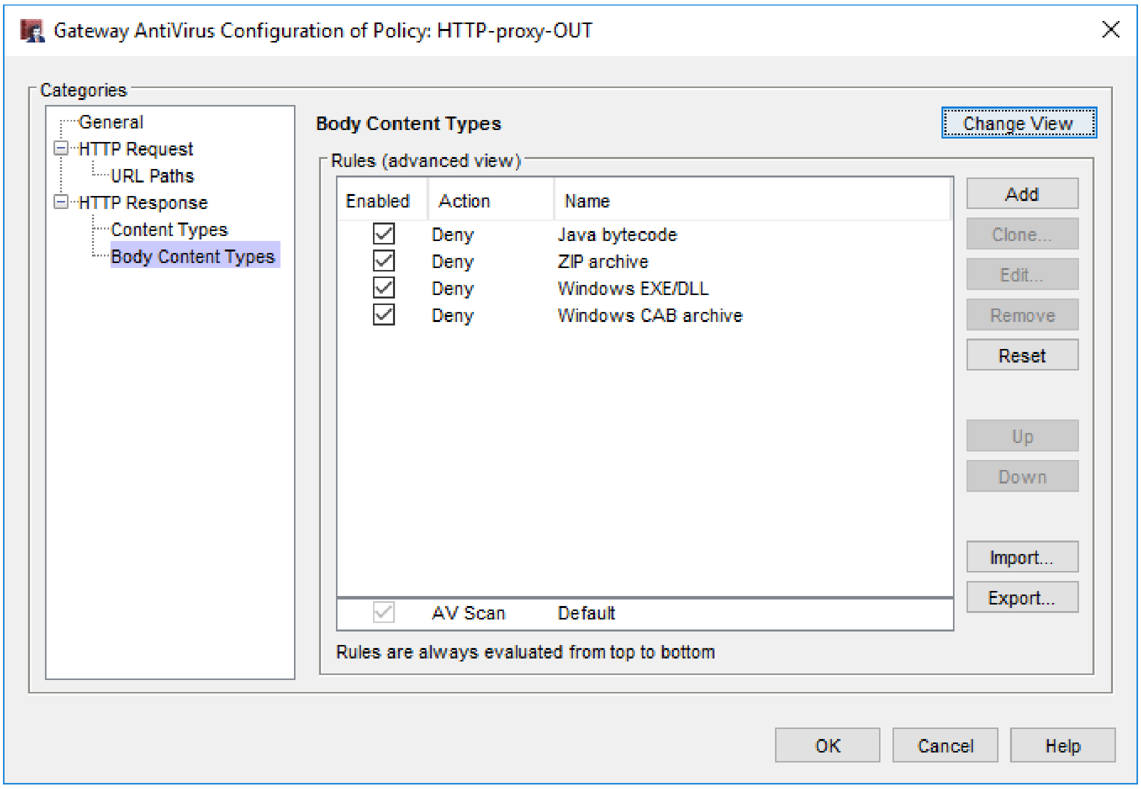
- □ Extended Protection
  - ☑ Elevated Exposure
  - ☑ Emerging Exploits
  - ☑ Suspicious Content
  - □ Dynamic DNS
  - □ Newly Registered Websites
- □ Gambling
- □ Games
- □ Government
- □ Health
- □ Illegal or Questionable
- □ Information Technology
- □ Internet Communication
- □ Intolerance
- □ Job Search
- □ Militancy and Extremist
- □ Miscellaneous
- □ News and Media
- □ Parked Domain
- □ Productivity
- □ Religion
- ☑ Security
  - ☑ Malicious Web Sites
  - ☑ Spyware
  - ☑ Phishing and Other Frauds
  - ☑ Keyloggers
  - ☑ Potentially Unwanted Software
  - ☑ Bot Networks
  - ☑ Malicious Embedded Link
  - ☑ Malicious Embedded iFrame
  - ☑ Suspicious Embedded Link
  - ☑ Mobile Malware
  - ☑ Advanced Malware Command and Control
  - ☑ Compromised Websites

Actions to take □ Alarm if denied ☑ Log this action

When a URL is uncategorized: Allow

Figure 8. WebBblocker Settings

Gateway antivirus – Antivirus was an important feature since it scans the traffic and removes malicious code directly from the traffic without users even knowing it. From the settings scanning for compressed archives must be enabled. From the content types one can check that various types of application are run AV check if traffic was matched. These include for example text, picture and PDF-files. Also, the downloading of the most common types of harmful files should be denied. These include ZIP archives, EXE/DLL files and windows CAB archives. (Figure 9)



Body Content Types

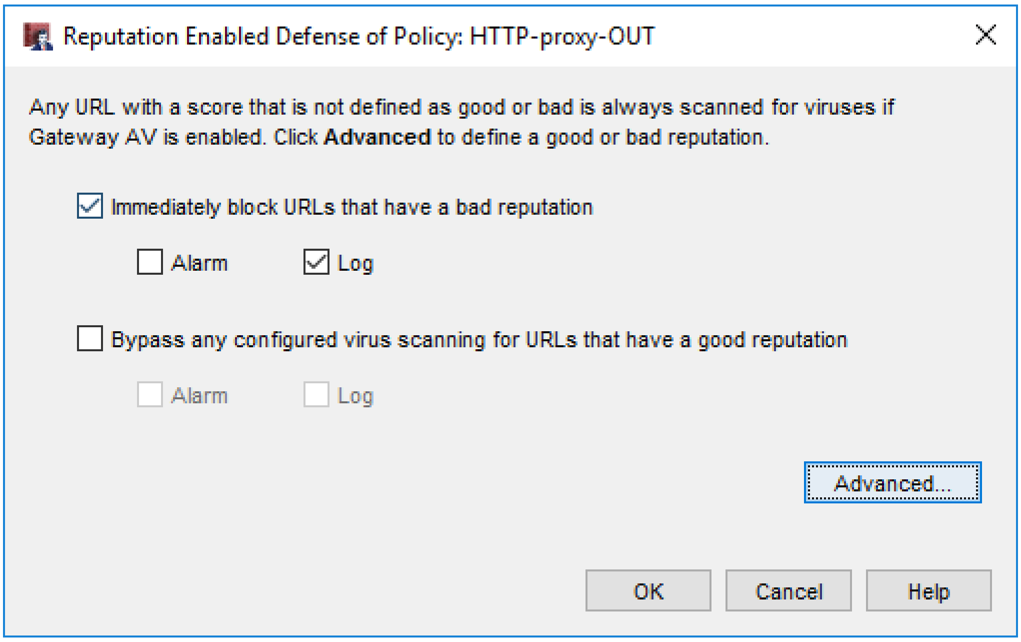
Rules (advanced view)

Enabled	Action	Name
☑	Deny	Java bytecode
☑	Deny	ZIP archive
☑	Deny	Windows EXE/DLL
☑	Deny	Windows CAB archive
☑	AV Scan	Default

Rules are always evaluated from top to bottom

Figure 9. Anti-Virus Body Content Types

Reputation enabled defense service – From Reputation enabled defense blocking of URLs that have bad reputation must be configured to be on, that way the chance of any infection was minimized. Bypassing of good reputation URLs should not be disabled, since even good reputation sites can have malicious code imbedded. (Figure 10)



Reputation Enabled Defense of Policy: HTTP-proxy-OUT

Any URL with a score that is not defined as good or bad is always scanned for viruses if Gateway AV is enabled. Click **Advanced** to define a good or bad reputation.

☑ Immediately block URLs that have a bad reputation

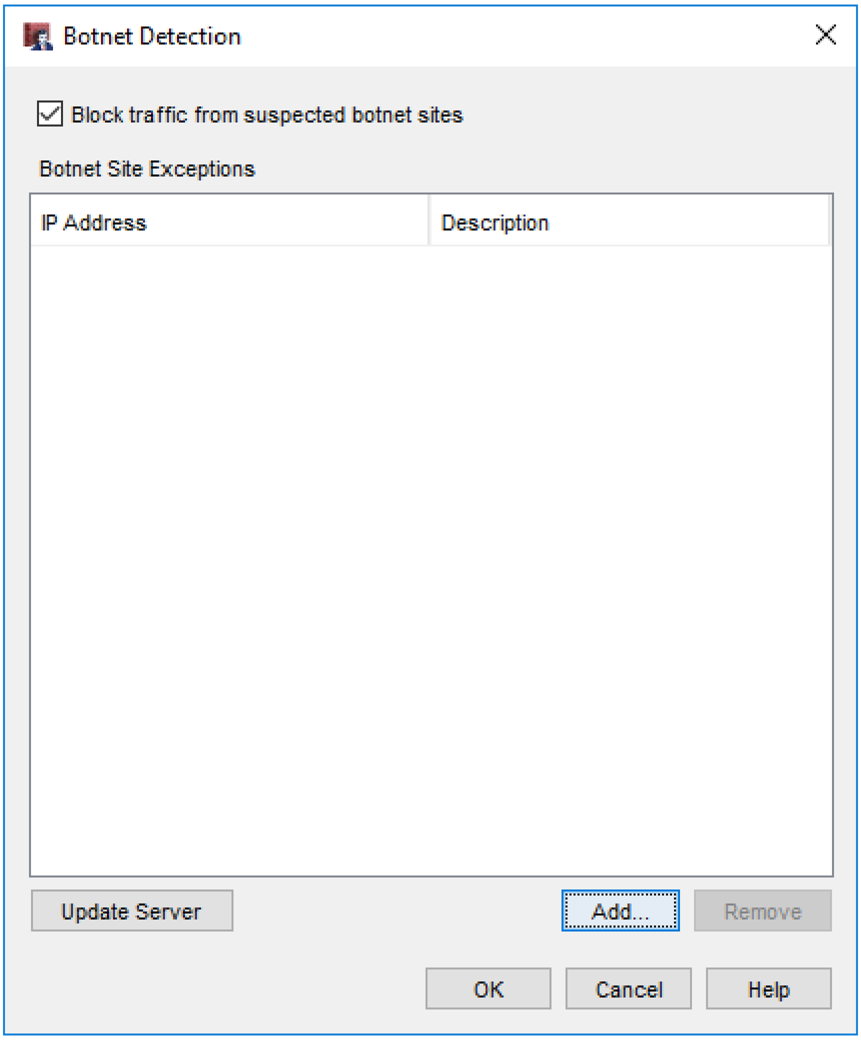
□ Alarm ☑ Log

□ Bypass any configured virus scanning for URLs that have a good reputation

□ Alarm □ Log

Figure 10. Reputation Enabled Defense settings

Botnet detection should also be turned on, so that it automatically blocks traffic from all known botnets. (Figure 11)



Botnet Detection

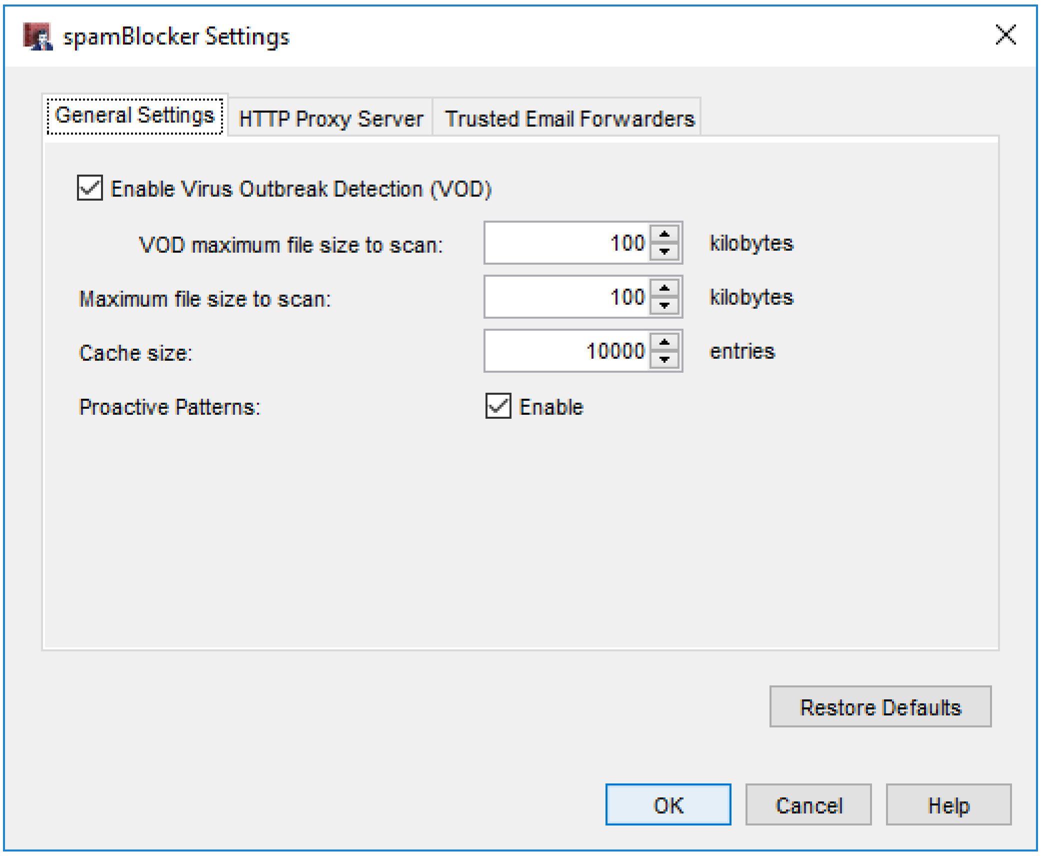
☑ Block traffic from suspected botnet sites

Botnet Site Exceptions

IP Address	Description

Figure 11. Botnet Detection settings

Spamblocker – For Spamblocker to work, one needs to have some kind of an SMTP server in the internal network. Inbound policy needs to be created to allow the traffic to pass the firewall from a certain external IP address to certain internal IP address. After the basic rule was made, the configuration of Spamblocker could be started. First the Virus Outbreak Detection (VOD) needs to be enabled.(Figure 12)



spamBlocker Settings

☑ Enable Virus Outbreak Detection (VOD)

VOD maximum file size to scan: 100 kilobytes

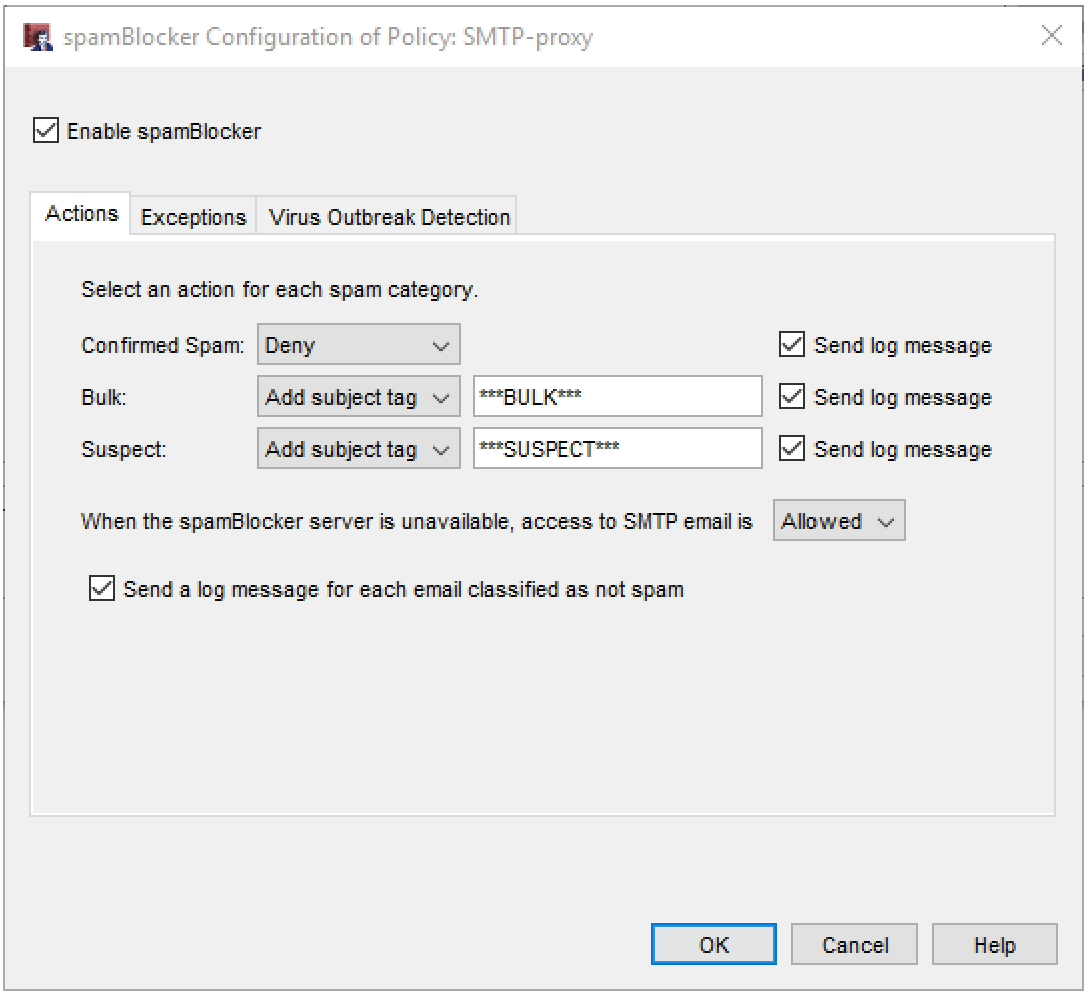
Maximum file size to scan: 100 kilobytes

Cache size: 10000 entries

Proactive Patterns: ☑ Enable

Figure 12. spamBlocker general settings

From the actions the behaviour of suspected spam must be reconfigured. With a default setting the suspected spam was automatically denied. It needs to be enabled and a certain tag needs to be inserted in order to users to receive a suspected spam, too. In the exception page a certain domain can be whitelisted so that emails received from that domain are always accepted. For all actions a log message must be recorded in case a mail flow needs to be examined at later times. (Figure 13)



spamBlocker Configuration of Policy: SMTP-proxy

☑ Enable spamBlocker

Select an action for each spam category.

Confirmed Spam: Deny ☑ Send log message

Bulk: Add subject tag ***BULK*** ☑ Send log message

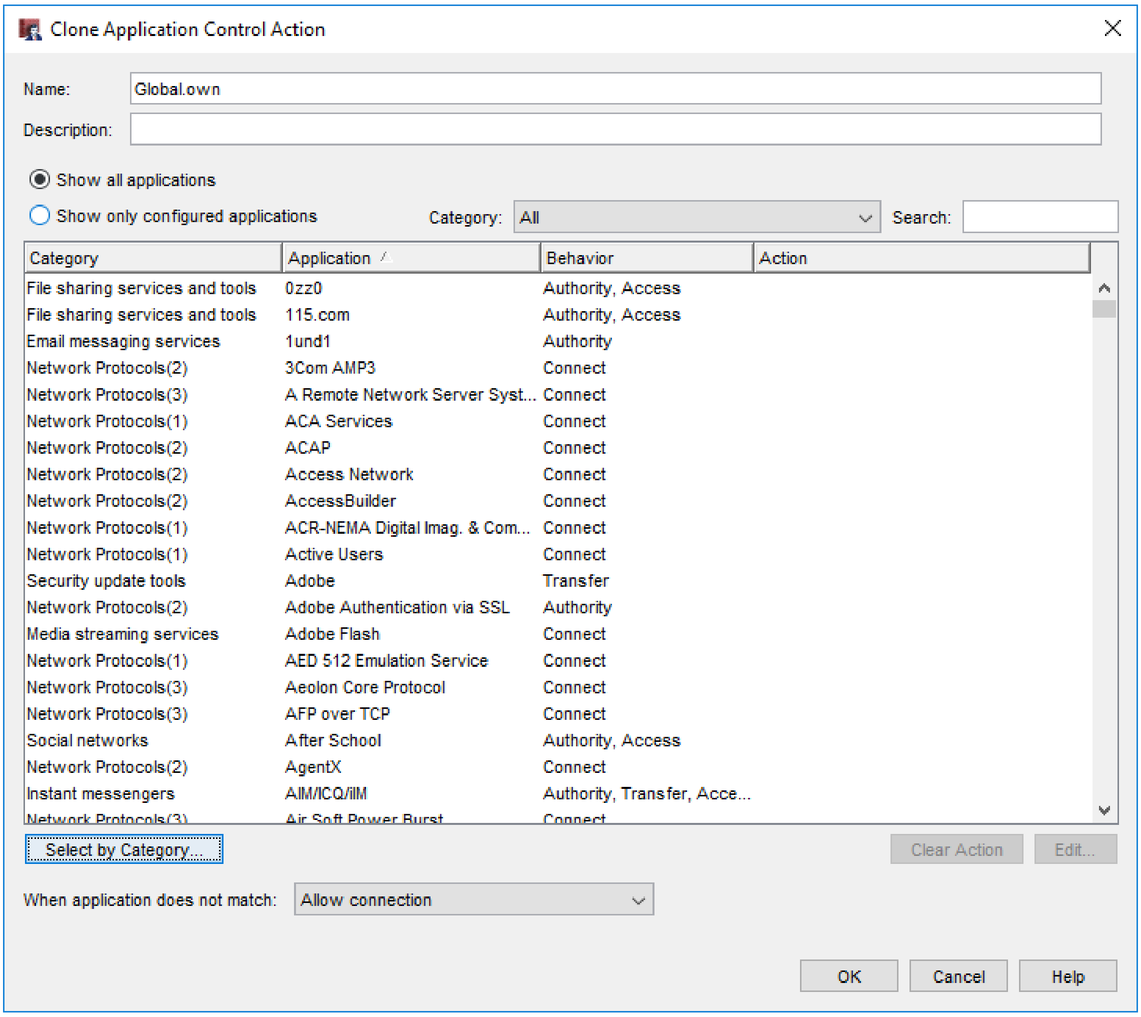
Suspect: Add subject tag ***SUSPECT*** ☑ Send log message

When the spamBlocker server is unavailable, access to SMTP email is Allowed

☑ Send a log message for each email classified as not spam

Figure 13. spamBlocker policy settings

Application control – When starting to configure Application polies the default policy should be cloned. This will ease the work if any new policies need to be applied at any later time. From the configuration, applications can be controlled by categories or by the application itself. It was very easy for example to deny any traffic that was in the category *Online Games*, that way any gaming that uses the internet is prohibited from the local network. The same kind of deny policy can be made for example for *Google Drive* if corporate rules dictate that it should not be used and it proposes a security threat. (Figure 14)



Name: Global.own

Description:

● Show all applications

○ Show only configured applications

Category: All

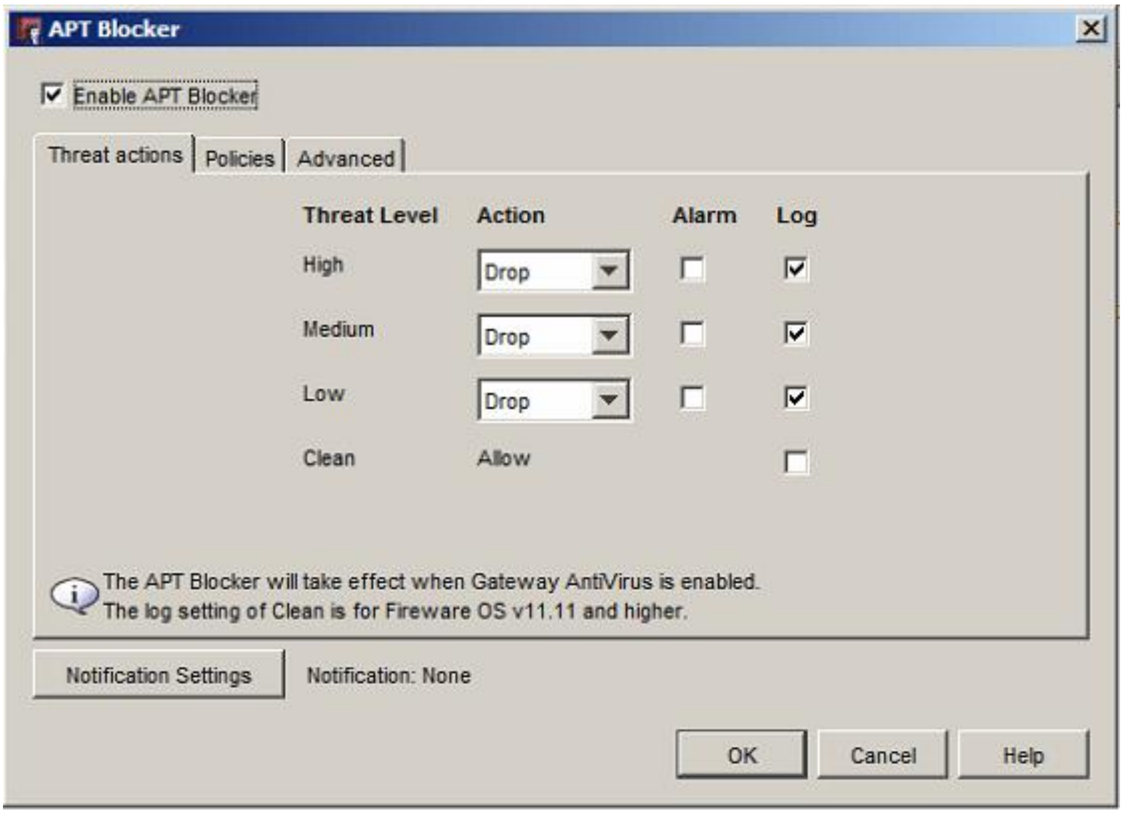
Search:

Category	Application	Behavior	Action
File sharing services and tools	0zz0	Authority, Access	
File sharing services and tools	115.com	Authority, Access	
Email messaging services	1und1	Authority	
Network Protocols(2)	3Com AMP3	Connect	
Network Protocols(3)	A Remote Network Server Syst...	Connect	
Network Protocols(1)	ACA Services	Connect	
Network Protocols(2)	ACAP	Connect	
Network Protocols(2)	Access Network	Connect	
Network Protocols(2)	AccessBuilder	Connect	
Network Protocols(1)	ACR-NEMA Digital Imag. & Com...	Connect	
Network Protocols(1)	Active Users	Connect	
Security update tools	Adobe	Transfer	
Network Protocols(2)	Adobe Authentication via SSL	Authority	
Media streaming services	Adobe Flash	Connect	
Network Protocols(1)	AED 512 Emulation Service	Connect	
Network Protocols(3)	Aeolon Core Protocol	Connect	
Network Protocols(3)	AFP over TCP	Connect	
Social networks	After School	Authority, Access	
Network Protocols(2)	AgentX	Connect	
Instant messengers	AIM/ICQ/iIM	Authority, Transfer, Acce...	
Network Protocols(3)	Air Soft Power Burst	Connect	

When application does not match: Allow connection

Figure 14. Application Control settings

APT Blocker – APT Blocker can only be used when Gateway Anti-virus feature is enabled and it can only be used in the same policies that the Anti-virus was enabled in. (Figure 15)



☑ Enable APT Blocker

Threat Level	Action	Alarm	Log
High	Drop	□	☑
Medium	Drop	□	☑
Low	Drop	□	☑
Clean	Allow		□

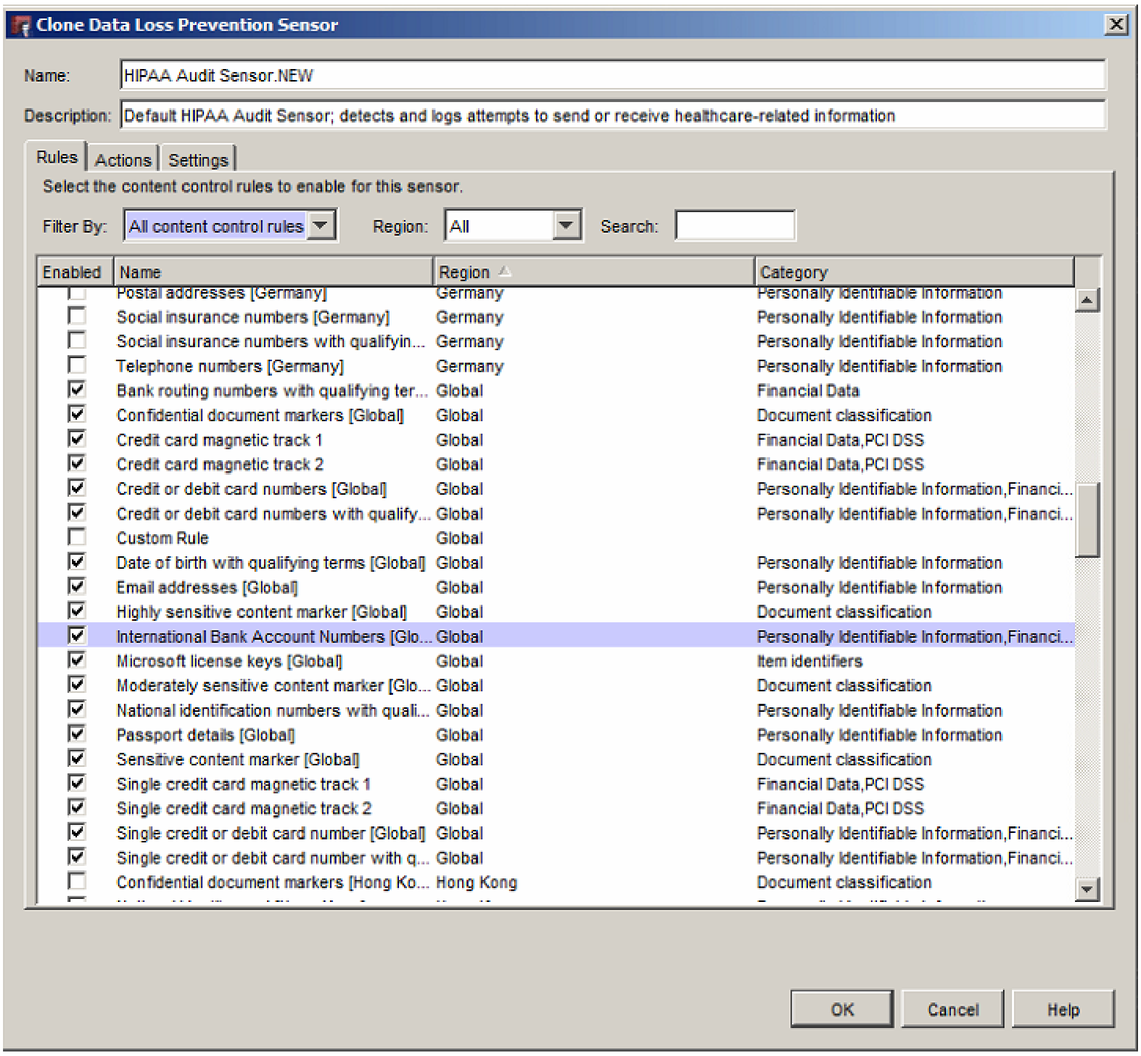
The APT Blocker will take effect when Gateway AntiVirus is enabled.
The log setting of Clean is for Fireware OS v11.11 and higher.

Notification: None

Figure 15. APT Blocker settings

Data loss prevention (DLP) – Data Loss Prevention has two separate Sensors: HIPAA Audit for Healthcare related information and PCI Audit for Payment Card Industry information. Before starting modifying the polices, the default Policy must be cloned and attached to the existing traffic policy. After cloning, the default policy rules need editing. For default installation, only the *Global* rules are selected.

From the settings, an action can be selected if earlier specified content was found in an email or non-email traffic. If desired information was found in the traffic include allow, drop and block. In addition, email traffic scanning has an option to lock the message, strip the content from the message or even quarantine the message. In either case, it was important for the selected logging to be enabled. (Figure 16)



Clone Data Loss Prevention Sensor

Name: HIPAA Audit Sensor.NEW

Description: Default HIPAA Audit Sensor; detects and logs attempts to send or receive healthcare-related information

Select the content control rules to enable for this sensor.

Filter By: All content control rules

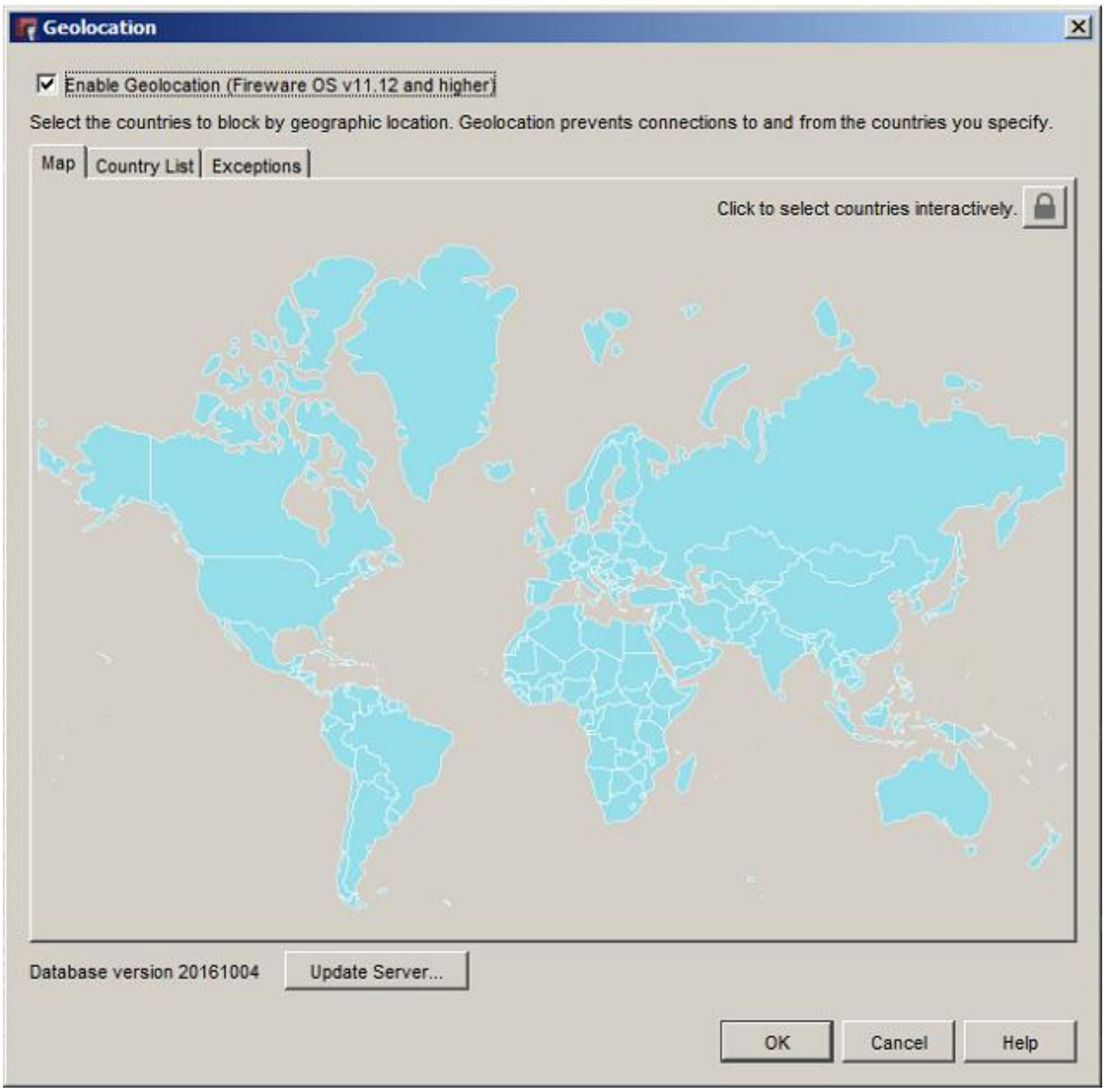
Region: All

Search:

Enabled	Name	Region	Category
□	Postal addresses [Germany]	Germany	Personally Identifiable Information
□	Social insurance numbers [Germany]	Germany	Personally Identifiable Information
□	Social insurance numbers with qualifyin...	Germany	Personally Identifiable Information
□	Telephone numbers [Germany]	Germany	Personally Identifiable Information
☑	Bank routing numbers with qualifying ter...	Global	Financial Data
☑	Confidential document markers [Global]	Global	Document classification
☑	Credit card magnetic track 1	Global	Financial Data,PCI DSS
☑	Credit card magnetic track 2	Global	Financial Data,PCI DSS
☑	Credit or debit card numbers [Global]	Global	Personally Identifiable Information,Financi...
☑	Credit or debit card numbers with qualify...	Global	Personally Identifiable Information,Financi...
□	Custom Rule	Global	
☑	Date of birth with qualifying terms [Global]	Global	Personally Identifiable Information
☑	Email addresses [Global]	Global	Personally Identifiable Information
☑	Highly sensitive content marker [Global]	Global	Document classification
☑	International Bank Account Numbers [Glo...	Global	Personally Identifiable Information,Financi...
☑	Microsoft license keys [Global]	Global	Item identifiers
☑	Moderately sensitive content marker [Glo...	Global	Document classification
☑	National identification numbers with quali...	Global	Personally Identifiable Information
☑	Passport details [Global]	Global	Personally Identifiable Information
☑	Sensitive content marker [Global]	Global	Document classification
☑	Single credit card magnetic track 1	Global	Financial Data,PCI DSS
☑	Single credit card magnetic track 2	Global	Financial Data,PCI DSS
☑	Single credit or debit card number [Global]	Global	Personally Identifiable Information,Financi...
☑	Single credit or debit card number with q...	Global	Personally Identifiable Information,Financi...
□	Confidential document markers [Hong Ko...	Hong Kong	Document classification

Figure 16. Data Loss Prevention settings

Geolocation – From the Geolocation feature one can deny any traffic to and from a certain country. For the default installation, no countries are selected. (Figure 17)



☑ Enable Geolocation (Fireware OS v11.12 and higher)

Select the countries to block by geographic location. Geolocation prevents connections to and from the countries you specify.

Click to select countries interactively.

Database version 20161004

Figure 17 Geolocation settings

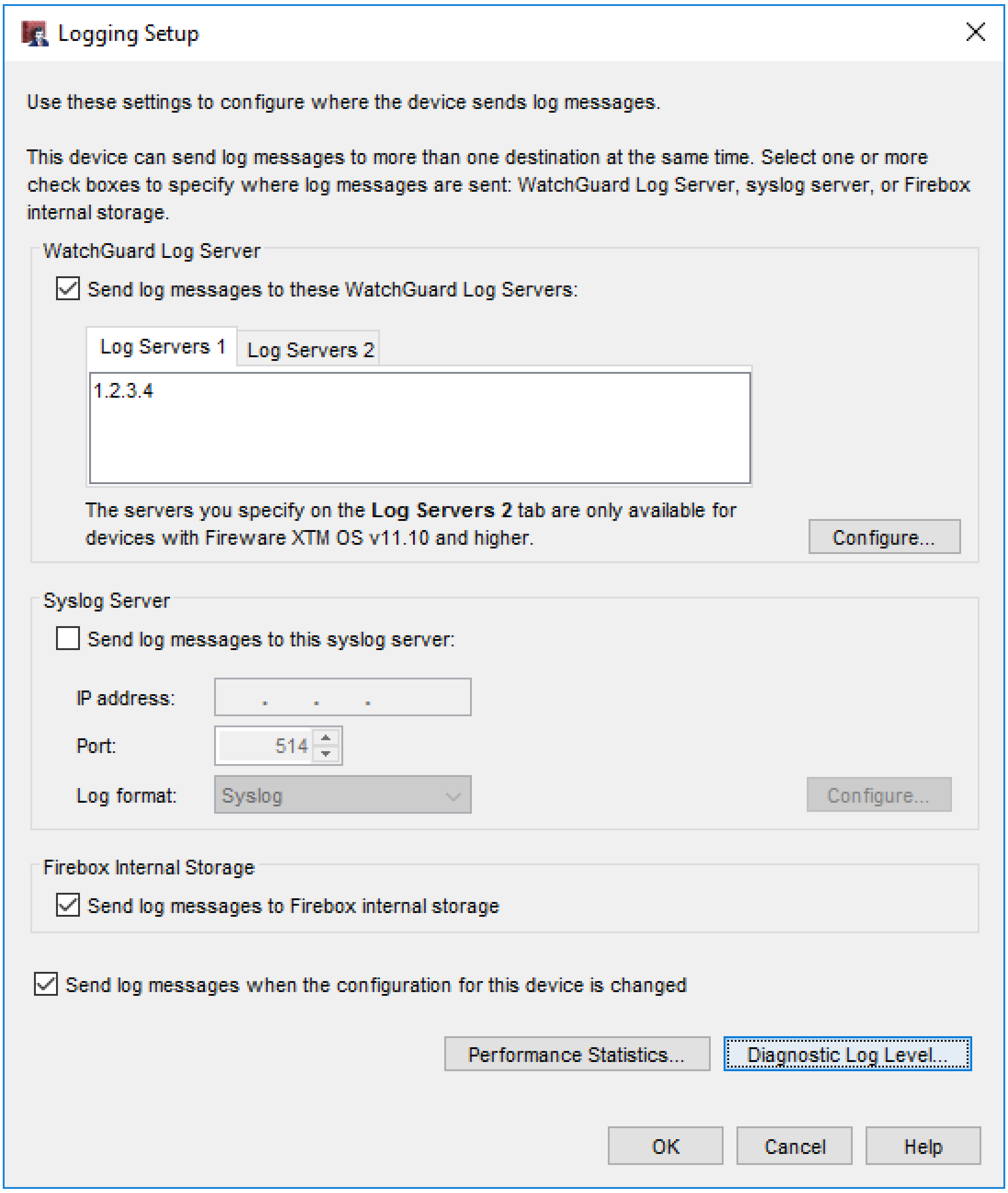
2.7 Logging

The next thing to configure was the logging feature which was a very important feature. Without logging, there is no way to find out if any of the modules have worked and produced a log entry. To produce enough data for adequate logging, all logging options according to the UTM module best practice should be configured. In addition, logging should be enabled in every incoming and outgoing rule of the firewall even if no application proxies are used.

In the present study, mainly the Watchguard device’s own logs were used. This logging feature is imbedded in the Watchguard firewall’s *System Manager* feature. In the System Manager one can see an overview of the device or drill down to the Firewall’s hardware to see the CPU or MEM usage or gather diagnostic logs. The Subscription Service tab shows the statistics from UTM modules since the last restart of the device.

Watchguard has developed separate products for gathering the logs from the Watchguard devices. This is an extremely efficient solution if one has many Watchguard firewalls from which one wants to gather data. The Dimension, which the product is called, is easily accessed with a web browser and it shows all gathered data in an understandable way. From the security point of view, it has very good capabilities to understand what happens in the network. Different reports can be viewed directly from the portal or they can be exported to PDF to hand over to a client. These reports include for example top blocker clients, top blocked destinations, top blocked applications and categories and top blocked protocols. In addition every UTM module has their own service log. From the logs one can browse in time to see when and what kinds of threats have taken place.

For the logging to properly work the Dimension server’s IP address and shared secret must be entered to the logging settings of the firewall. (Figure 18)



Logging Setup

Use these settings to configure where the device sends log messages.

This device can send log messages to more than one destination at the same time. Select one or more check boxes to specify where log messages are sent: WatchGuard Log Server, syslog server, or Firebox internal storage.

WatchGuard Log Server

☑ Send log messages to these WatchGuard Log Servers:

1.2.3.4

The servers you specify on the **Log Servers 2** tab are only available for devices with Fireware XTM OS v11.10 and higher.

Syslog Server

☐ Send log messages to this syslog server:

IP address: . . .

Port: 514

Log format: Syslog

Firebox Internal Storage

☑ Send log messages to Firebox internal storage

☑ Send log messages when the configuration for this device is changed

Figure 18. Logging settings

3 Security Features and Requirements of Case Company

In this chapter the former state of the customer’s environment is described. A short interview with the organization executives was conducted in order to determine what was the current knowledge about the overall security and what were their expectations. After the analysis of the current state was done and the interviews conducted the guidelines were established for the new system. Lastly, a deployment plan was made in cooperation with the customer.

3.1 Analysis and Current State of Customer’s Environment

The analysis of the environment was started with a short interview with the organization decision-makers and the person who was in charge of IT related decisions and purchases. The interview consisted of questions which aimed to examine the current situation.

The questions asked were as follows:

- Do you know what security features are in use at the company?
- Can you give examples of common known security risks?
- What was the biggest security threat that the organization faces?
- How do you see cyber-attacks happening in this company?
- How can you gain more security to the environment?

The answers received were quite in line with each other. Separate answers are not listed here, but instead a summary of all answers was made.

The persons interviewed all knew quite a lot on what security features were in use. Some of them are quite standard in the company as they have been in use for many years. These features are all listed later in this chapter.

A very decent list of common known threats was received. The threats were not introduced by their proper names, but still one can see that there was knowledge behind them. The list included among other things email scams (Nigerian letters, fake email UPS) and different kinds of website related issues. Different kinds of threats such as a crypto locker was mentioned as it had been spotted on the news.

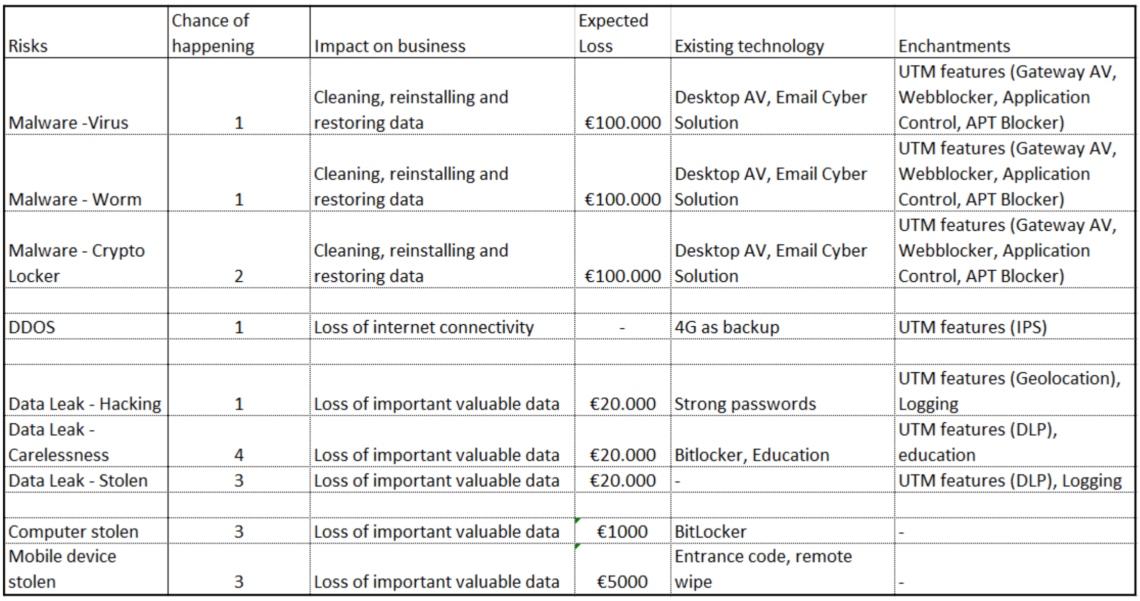
As the biggest security risk the interviewees answered to be their own employees. In more detail, losing or stealing data that was valuable to the company and that way harm the company. Losing data can be caused by carelessness or accidentally. More risks were found in malware and end-devices. Downtime caused by any of these threats was acknowledged, but determined as marginal as the chance of that happening was considered small.

The possibility that any cyber-attacks would happen to the company was considered very small. The fact that malicious emails occasionally come through was not considered as a problem and the personnel was trusted enough to detect the scams and report them to the helpdesk. No other kinds of attacks were mentioned.

For increasing the security of the environment no good ideas were received. Some sort of security device was proposed, but the employees were not able to describe the function of the device. Mobile devices were mentioned as there has been news that Android devices have many security risks.

At the same time as the interviews were held, a table of common risks and their impact to business was put together. In the table, all the risks discovered during the interviews were listed and then estimated what the impact and possible loss to the company would be. The same table includes information if there was any existing technology in place and what could be a new solution to fight against that certain risk. The chance of the risk taking place was approximated on a scale from 1 to 5, where 5 is most likely to happen. (Table 1)

Table 1. List of potential threats and their characteristics



Risks	Chance of happening	Impact on business	Expected Loss	Existing technology	Enchantments
Malware -Virus	1	Cleaning, reinstalling and restoring data	€100.000	Desktop AV, Email Cyber Solution	UTM features (Gateway AV, Webblocker, Application Control, APT Blocker)
Malware - Worm	1	Cleaning, reinstalling and restoring data	€100.000	Desktop AV, Email Cyber Solution	UTM features (Gateway AV, Webblocker, Application Control, APT Blocker)
Malware - Crypto Locker	2	Cleaning, reinstalling and restoring data	€100.000	Desktop AV, Email Cyber Solution	UTM features (Gateway AV, Webblocker, Application Control, APT Blocker)
DDOS	1	Loss of internet connectivity	-	4G as backup	UTM features (IPS)
Data Leak - Hacking	1	Loss of important valuable data	€20.000	Strong passwords	UTM features (Geolocation), Logging
Data Leak - Carelessness	4	Loss of important valuable data	€20.000	Bitlocker, Education	UTM features (DLP), education
Data Leak - Stolen	3	Loss of important valuable data	€20.000	-	UTM features (DLP), Logging
Computer stolen	3	Loss of important valuable data	€1000	BitLocker	-
Mobile device stolen	3	Loss of important valuable data	€5000	Entrance code, remote wipe	-

Before starting this project, the following security features were already in place to increase the security. Some of them have been in place for several years and some of them have been adapted recently.

Email protection - Cyber email security protection for email traffic, usually 3rd party provided service which includes anti-virus, anti-malware and zero-hour protection. Blocks directly unwanted definite spam messages. Separates bulk marketing emails and normal email by seizing bulk emails to email gateway. This way only appropriate work emails reach end-users. Users receives message digest for seized emails once a day.

Desktop Anti-Virus - F-Secure desktop anti-virus was already installed to all of the workstations and laptops. It includes anti-virus and anti-malware protection. It also includes personal firewall which was taken in use when computer was not used in the internal office network. The status of F-Secure installations and virus protection was monitor from F-Secures cloud portal.

Administrative rights - Local administrative rights were stripped from all standard users. All software installations to the computer were denied by regular users. All software installations were installed remotely by the helpdesk service. In this way it was minimized the chance that a user would install something inappropriate to the system that might cause unwanted behaviour.

AppLocker - Windows built-in feature AppLocker was also implemented. It means that only predefined whitelisted applications can be run on computers. This way any 3rd party programs and add-ons that might be ran without installing them to the systems was prohibited. This brings more security when less secure programs are used.

Workstation encryption - Every computer that was used in the organization was encrypted with Windows bit locker hard drive encryption feature. This way, in case of stolen or lost computer, data would still be in safe in encrypted hard drive. Also, bit locker for removable devices was taken in use. This way every USB thumb drive that was attached to the computer must be first formatted to be sure that there was nothing harmful in it. This workaround has complicated the use of thumb drives, because material on thumb drives couldn't been access on corporate computers. This led information to be shared in different channels like email and SFTP, which was in matter of fact better solution since traffic can be monitored better than thumb drives.

Central updates administration - All computers had Windows updates centrally administered. It guarantees that helpdesk has full control what updates are installed and what time. Also, most of the 3rd party software was controlled this same way. 3rd party software updates include the most insecure applications like Adobe, Oracle and different browsers. This way was minimized the risk that was included when user himself controls the updates.

Password policy - Special attention to secure password was paid long before starting this project. The hacking of insecure password was demonstrated to personnel by using internet site that shows how secure user password was. According to howsecureismypassword.net, password with 8 minor case letters was cracked by brute force in 5 seconds. Derived from that test, everybody started to use more complex passwords. Default password policy was also established to include certain number of letters (minor and capital), numbers and special characters.

When starting this project, the customer was using an old out-dated firewall. The firewall itself was end-of-life and was not produced nor supported anymore by the manufacturer. The firewall had insufficient logging and reporting features, which made it more or less useless. The technical specification was also deprecated since the internet connection speed had been increased over the years. Years ago, the customer had a low bandwidth SHDSL line. Nowadays it has been updated to a 100M fibre connection. The only thing that worked as it should, was the stateful inspection of packets and the rules associated. It was self-evident that the firewall should be replaced, the only question was that what features it should support for future use?

The author's organization has been educating the customer organization from time to time to keep them as up-to-date in information security as possible. When a new employee started at the company, a training was held about how the company IT functions as a whole, how the IT equipment was used and what were the predefined company policies. The new employee must sign a form after the training that indicated that he or she has embraced the policies. Also, updating training was held to the personnel after any major IT change to keep everybody up-to-date.

3.2 Requirements for System

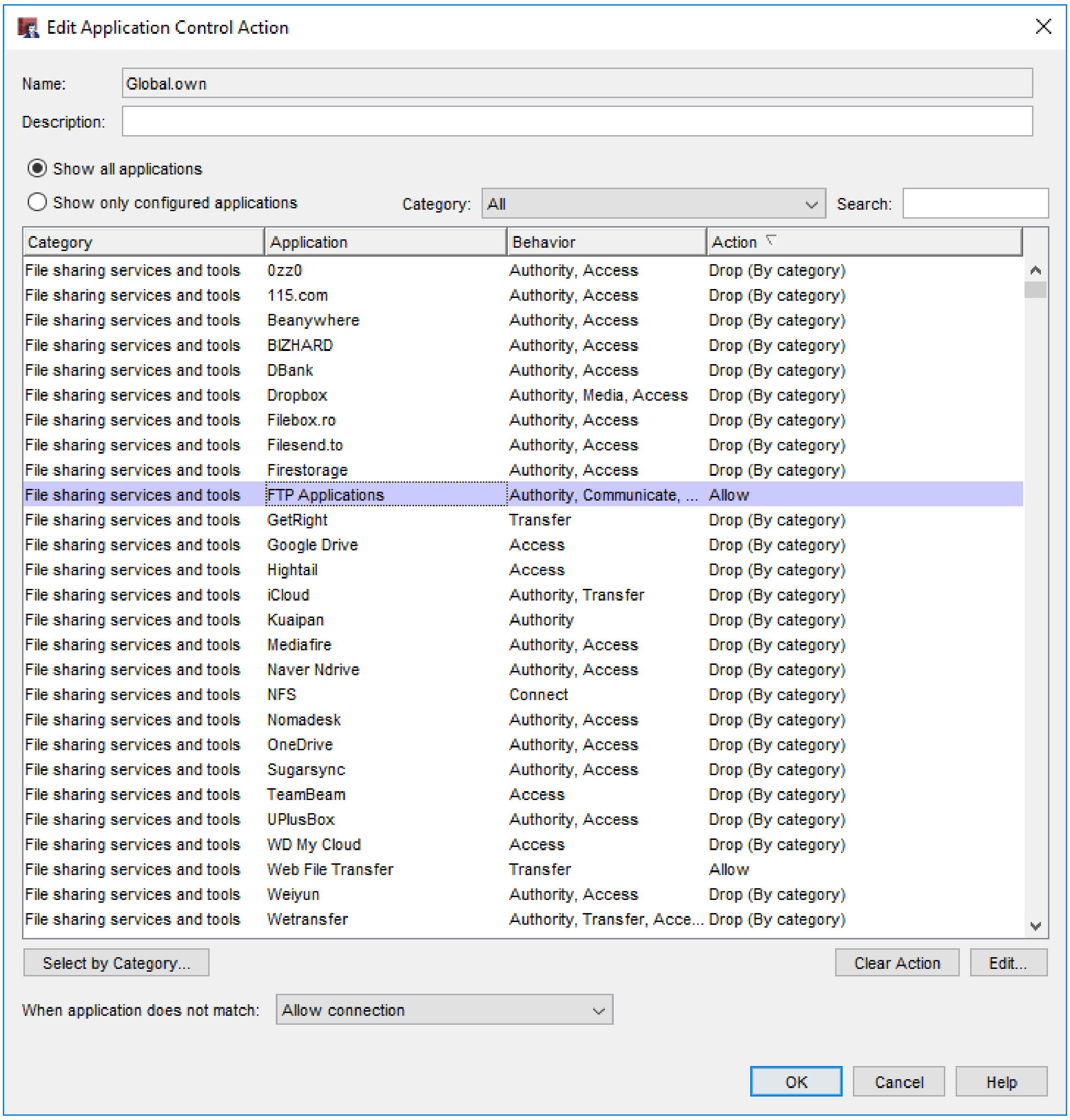
After the interviews had been conducted and the current environment had been analyzed, the requirements for the new system were listed. More security was needed in the network level to automize and prevent certain network threats. Also, the logging level needed to be raised in order to examine what happens in the network. Even though some level of security had been previously established, the customer was eager to see what changes the security features would bring.

Although an anti-virus software was installed to every computer, a decision was made that the gateway anti-virus was taken into use. The customer was using a 3rd party email cyber security service, so the SMTP-proxy feature was decided to be taken off. From other available proxies, FTP, HTTP, HTTPS and TCP-UDP proxies were taken into use. That way most of the traffic generated from the internal network was going through one of the proxies.

3.3 Deployment Plan and Configurations

It was agreed with both sides that the Watchguard UTM firewall was taken in use with the earlier defined best practises. A couple of modifications were made to the best practise guidelines to better suit them to the customer's environment.

Application Control – In the Application Control setting some default actions were modified. As the corporate guidelines dictate, all file sharing services such as OneDrive, Google Drive and Dropbox were denied. The only exception to that rule was that FTP Application and Web File Transfer were accepted. (Figure 19)



Name: Global.own

Description:

● Show all applications

○ Show only configured applications

Category: All

Search:

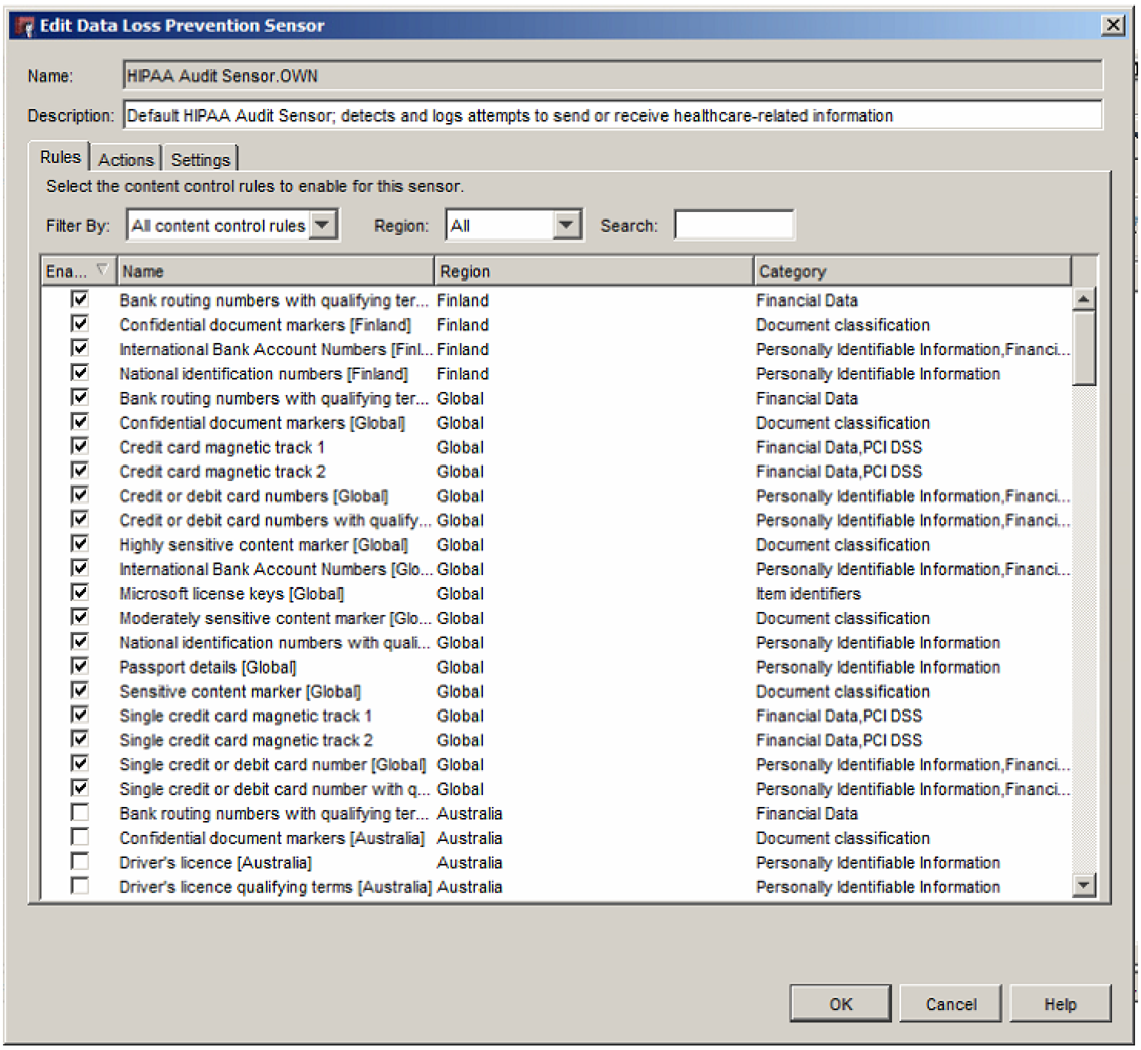
Category	Application	Behavior	Action
File sharing services and tools	0zz0	Authority, Access	Drop (By category)
File sharing services and tools	115.com	Authority, Access	Drop (By category)
File sharing services and tools	Beanywhere	Authority, Access	Drop (By category)
File sharing services and tools	BIZHARD	Authority, Access	Drop (By category)
File sharing services and tools	DBank	Authority, Access	Drop (By category)
File sharing services and tools	Dropbox	Authority, Media, Access	Drop (By category)
File sharing services and tools	Filebox.ro	Authority, Access	Drop (By category)
File sharing services and tools	Filesend.to	Authority, Access	Drop (By category)
File sharing services and tools	Firestorage	Authority, Access	Drop (By category)
File sharing services and tools	FTP Applications	Authority, Communicate, ...	Allow
File sharing services and tools	GetRight	Transfer	Drop (By category)
File sharing services and tools	Google Drive	Access	Drop (By category)
File sharing services and tools	Hightail	Access	Drop (By category)
File sharing services and tools	iCloud	Authority, Transfer	Drop (By category)
File sharing services and tools	Kuaipan	Authority	Drop (By category)
File sharing services and tools	Mediafire	Authority, Access	Drop (By category)
File sharing services and tools	Naver Ndrive	Authority, Access	Drop (By category)
File sharing services and tools	NFS	Connect	Drop (By category)
File sharing services and tools	Nomadesk	Authority, Access	Drop (By category)
File sharing services and tools	OneDrive	Authority, Access	Drop (By category)
File sharing services and tools	Sugarsync	Authority, Access	Drop (By category)
File sharing services and tools	TeamBeam	Access	Drop (By category)
File sharing services and tools	UPlusBox	Authority, Access	Drop (By category)
File sharing services and tools	WD My Cloud	Access	Drop (By category)
File sharing services and tools	Web File Transfer	Transfer	Allow
File sharing services and tools	Weiyun	Authority, Access	Drop (By category)
File sharing services and tools	Wetransfer	Authority, Transfer, Acce...	Drop (By category)

When application does not match: Allow connection

Figure 19. Application control customer settings

Webblocker – Weblocker denied site list was slightly modified from the best configuration. The following categories were added to the denied categories: Adult Material and Gambling.

Data Loss Prevention (DLP) - HIPAA audit sensor was agreed to be taken into use. Both sensors are about the same when considering the options that can be used to identify Finnish information. From the rules, every category related to Finland or Global was selected. (Figure 20)



Name: HIPAA Audit Sensor.OWN

Description: Default HIPAA Audit Sensor; detects and logs attempts to send or receive healthcare-related information

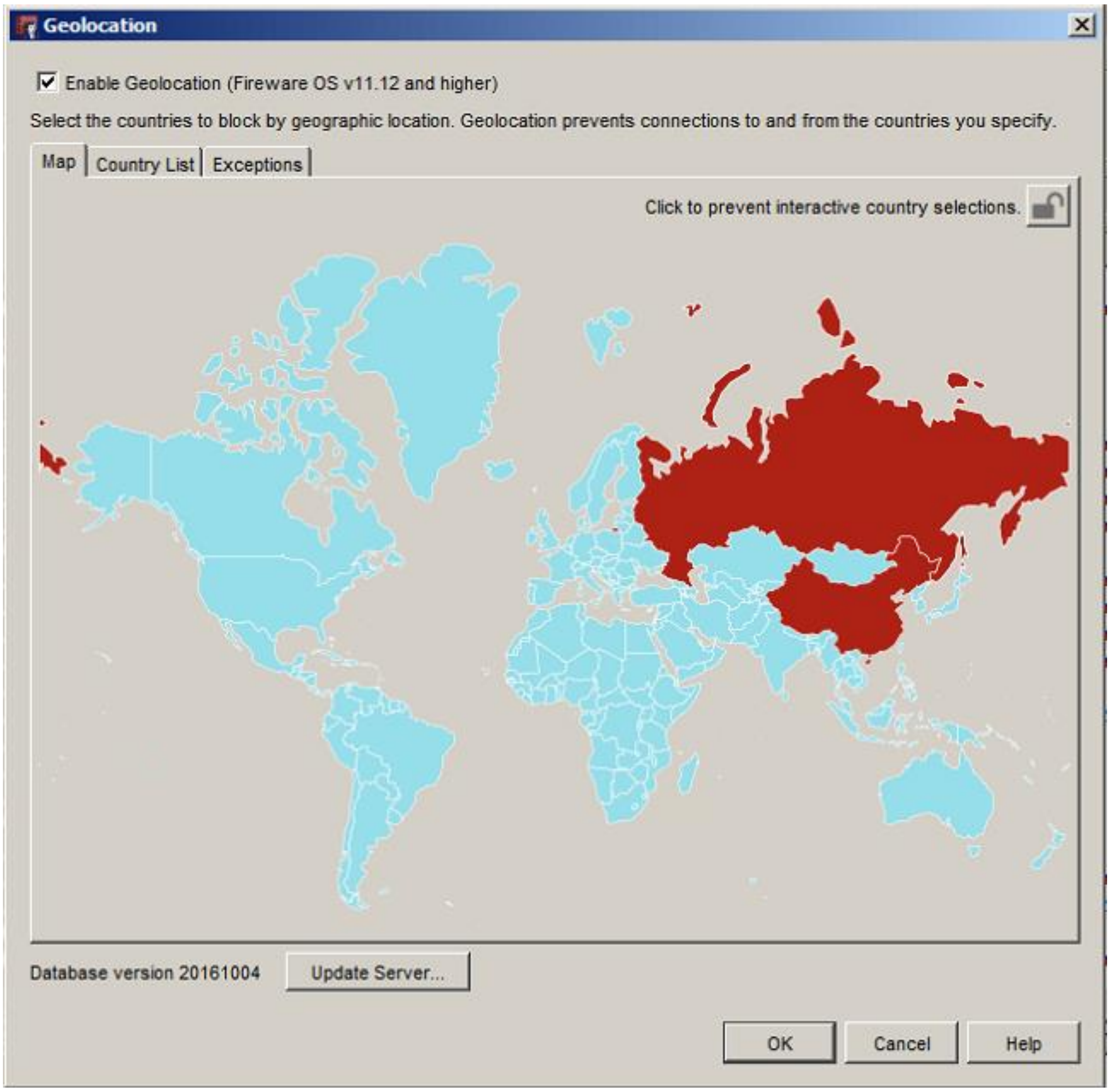
Select the content control rules to enable for this sensor.

Filter By: All content control rules Region: All Search:

Ena...	Name	Region	Category
☑	Bank routing numbers with qualifying ter...	Finland	Financial Data
☑	Confidential document markers [Finland]	Finland	Document classification
☑	International Bank Account Numbers [Finl...	Finland	Personally Identifiable Information,Financi...
☑	National identification numbers [Finland]	Finland	Personally Identifiable Information
☑	Bank routing numbers with qualifying ter...	Global	Financial Data
☑	Confidential document markers [Global]	Global	Document classification
☑	Credit card magnetic track 1	Global	Financial Data,PCI DSS
☑	Credit card magnetic track 2	Global	Financial Data,PCI DSS
☑	Credit or debit card numbers [Global]	Global	Personally Identifiable Information,Financi...
☑	Credit or debit card numbers with qualify...	Global	Personally Identifiable Information,Financi...
☑	Highly sensitive content marker [Global]	Global	Document classification
☑	International Bank Account Numbers [Glo...	Global	Personally Identifiable Information,Financi...
☑	Microsoft license keys [Global]	Global	Item identifiers
☑	Moderately sensitive content marker [Glo...	Global	Document classification
☑	National identification numbers with quali...	Global	Personally Identifiable Information
☑	Passport details [Global]	Global	Personally Identifiable Information
☑	Sensitive content marker [Global]	Global	Document classification
☑	Single credit card magnetic track 1	Global	Financial Data,PCI DSS
☑	Single credit card magnetic track 2	Global	Financial Data,PCI DSS
☑	Single credit or debit card number [Global]	Global	Personally Identifiable Information,Financi...
☑	Single credit or debit card number with q...	Global	Personally Identifiable Information,Financi...
□	Bank routing numbers with qualifying ter...	Australia	Financial Data
□	Confidential document markers [Australia]	Australia	Document classification
□	Driver's licence [Australia]	Australia	Personally Identifiable Information
□	Driver's licence qualifying terms [Australia]	Australia	Personally Identifiable Information

Figure 20. Data Loss Prevention customer settings

Geolocation - The organization in question was mainly working in Europe and it had no business in Russia or China, so traffic from and to those countries was automatically denied. (Figure 21)



Geolocation

☑ Enable Geolocation (Fireware OS v11.12 and higher)

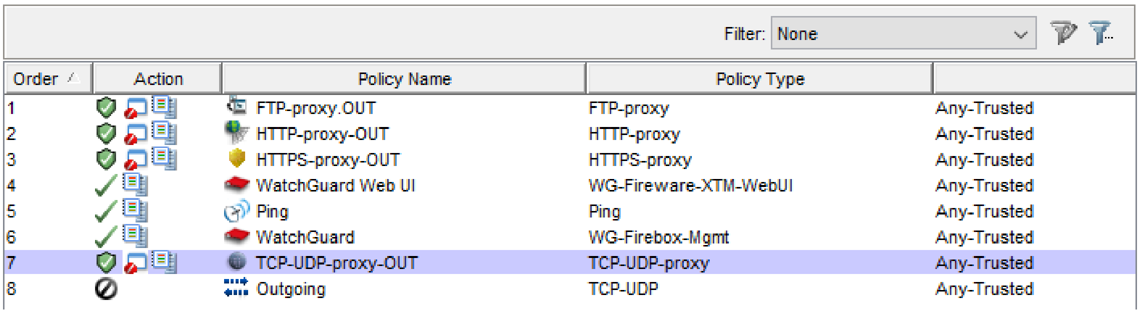
Select the countries to block by geographic location. Geolocation prevents connections to and from the countries you specify.

Database version 20161004

Figure 21. Geolocation customer settings

Logging – Watchguard Dimension was taken into use. It was situated in the service provider’s datacenter. Automatic reports were configured. Those reports contained information about UTM modules and their statistics. The reports were automatically sent to the customer’s responsible IT person. (Sample report Appendix1.)

Following proxies were taken into use: FTP, HTTP, HTTPS and TCP-UDP proxies were taken into use. All the proxies were configured from inside to outside traffic, in other words for outgoing traffic. The customer had no servers or services in their internal network, so no outside to inside – inbound rules were made. Figure 22 below shows that all configured rules have logging on, in addition, also the proxy rules that are indicated with a green shield have application control in use.



Filter: None

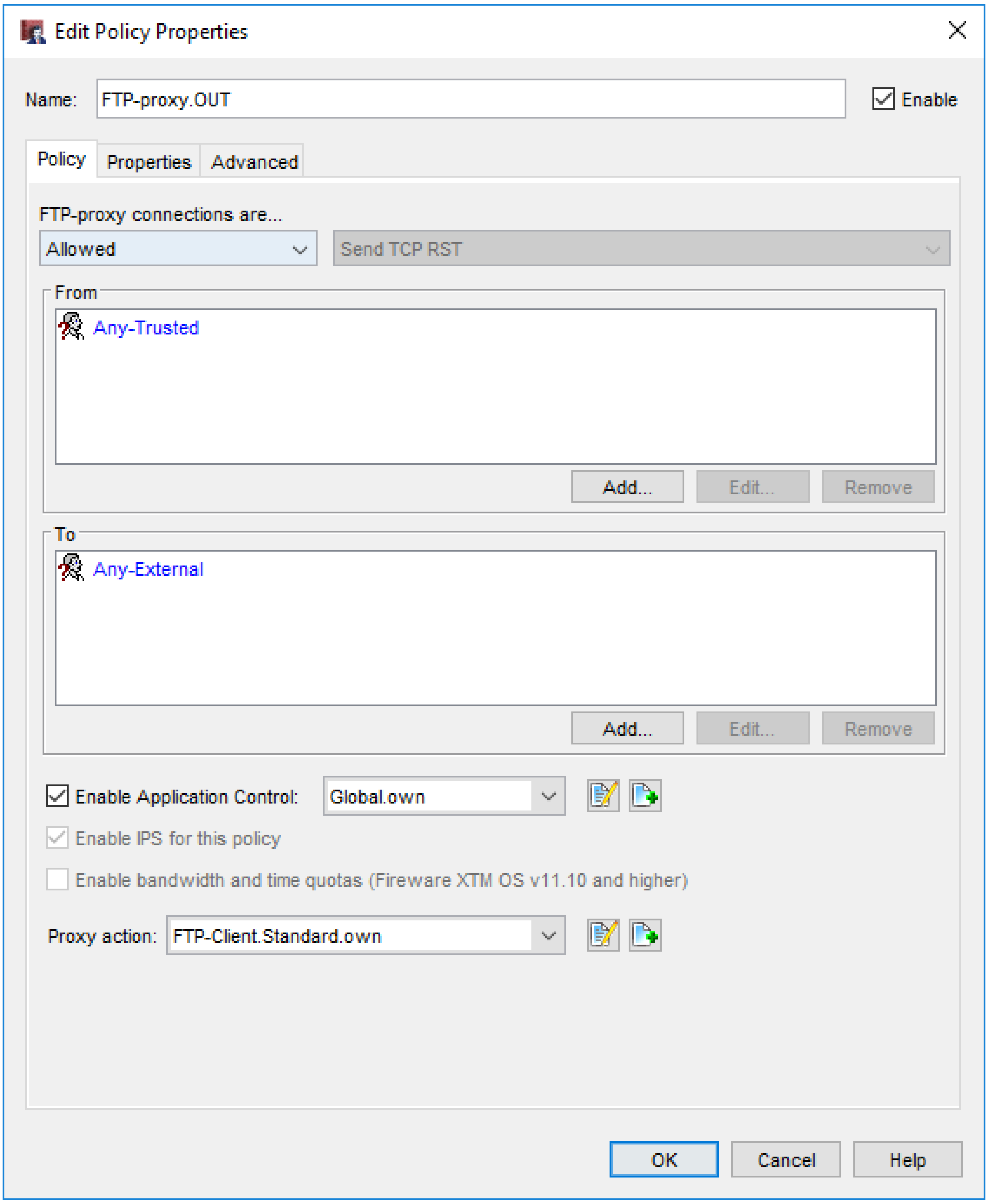
Order	Action	Policy Name	Policy Type	
1	🛡	FTP-proxy.OUT	FTP-proxy	Any-Trusted
2	🛡	HTTP-proxy-OUT	HTTP-proxy	Any-Trusted
3	🛡	HTTPS-proxy-OUT	HTTPS-proxy	Any-Trusted
4	✓	WatchGuard Web UI	WG-Fireware-XTM-WebUI	Any-Trusted
5	✓	Ping	Ping	Any-Trusted
6	✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted
7	🛡	TCP-UDP-proxy-OUT	TCP-UDP-proxy	Any-Trusted
8	⊘	Outgoing	TCP-UDP	Any-Trusted

Figure 22. Customer's firewall policies

All different proxies were configured so that the following features are enabled with the predefined profiles, if applicable:

- Application Control – Global.own
- AntiVirus
- Data Loss Prevention - HIPAA Audit Sensor.OWN
- Webblocker – WebBlocker.1 (HTTP) or WebBlocker.2 (HTTPS)
- APT Blocker

FTP-proxy – The FTP-Proxy modification was started by cloning the default Proxy action. No other changes were made to the rule-set. (Figure 23)



Edit Policy Properties

Name: FTP-proxy.OUT ☑ Enable

FTP-proxy connections are... Allowed Send TCP RST

From: Any-Trusted

To: Any-External

☑ Enable Application Control: Global.own

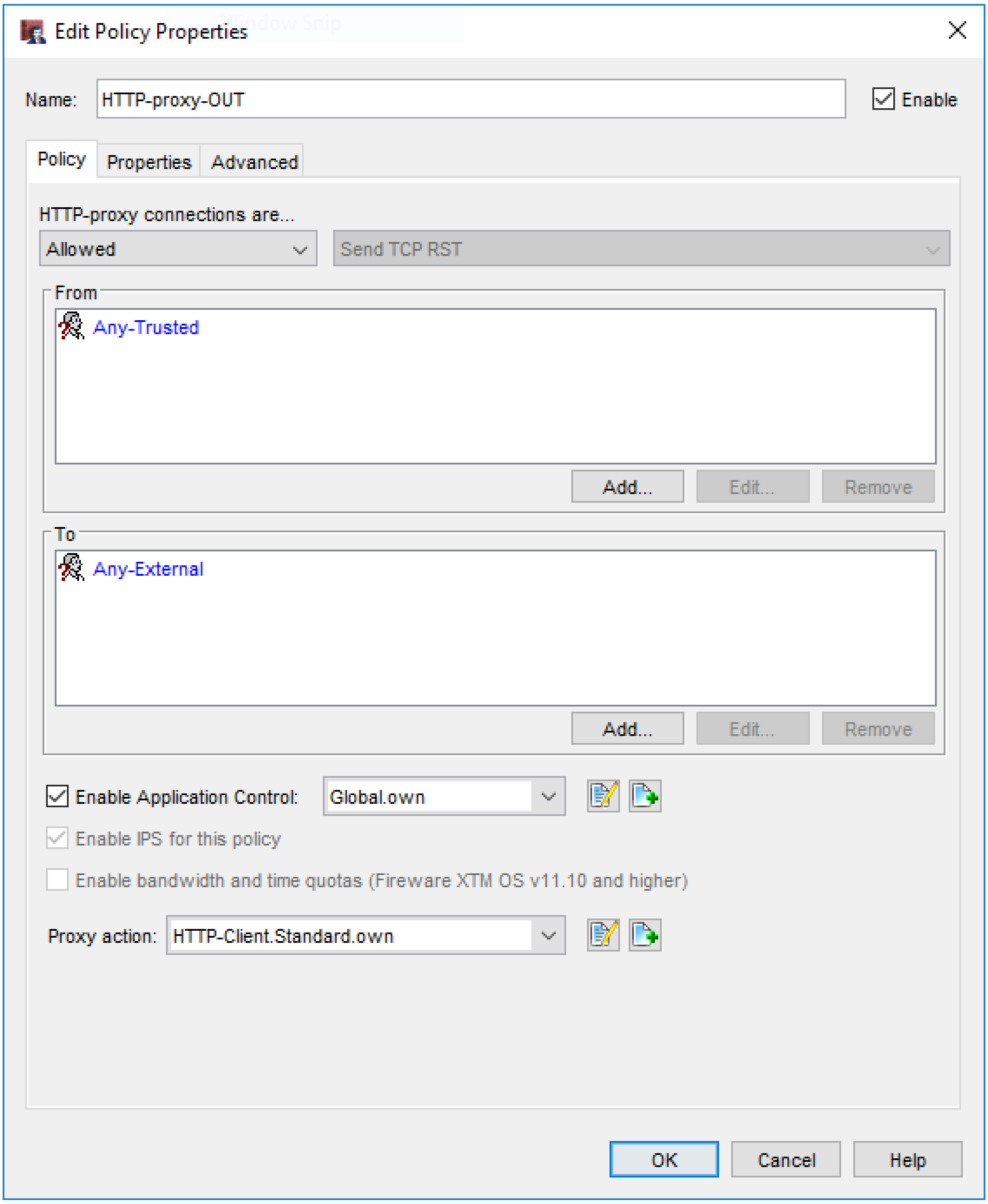
☑ Enable IPS for this policy

☐ Enable bandwidth and time quotas (Fireware XTM OS v11.10 and higher)

Proxy action: FTP-Client.Standard.own

Figure 23. Customer's FTP Proxy settings

HTTP-proxy – The HTTP-proxy setting was modified in the following ways. The proxy action rule-set was modified too by first cloning the default rule-set. Then changes were made, from the rule categories Body Content Types downloading of Java bytecode, ZIP archives, Windows EXE/DLL and Windows CAB archives was denied. (Figure 24)



Edit Policy Properties

Name: HTTP-proxy-OUT ☑ Enable

HTTP-proxy connections are... Allowed Send TCP RST

From: Any-Trusted

To: Any-External

☑ Enable Application Control: Global.own

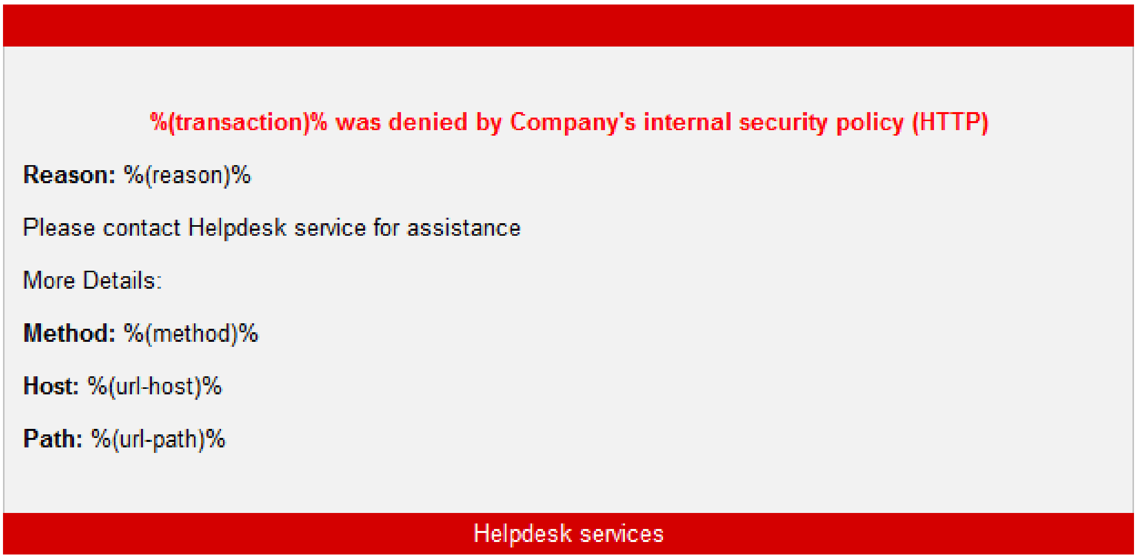
☑ Enable IPS for this policy

□ Enable bandwidth and time quotas (Fireware XTM OS v11.10 and higher)

Proxy action: HTTP-Client.Standard.own

Figure 24. Customer’s HTTP Proxy settings

Lastly from the HTTP proxy actions the Deny message was modified to provide end-users information if the firewall has blocked traffic. Figure 25 below shows what the banner could have been. Actually, the message had more information e.g. the company's real name to show that the message was genuine. In addition it shows the phone and email contact information of the helpdesk services.



%(transaction)% was denied by Company's internal security policy (HTTP)

Reason: %(reason)%

Please contact Helpdesk service for assistance

More Details:

Method: %(method)%

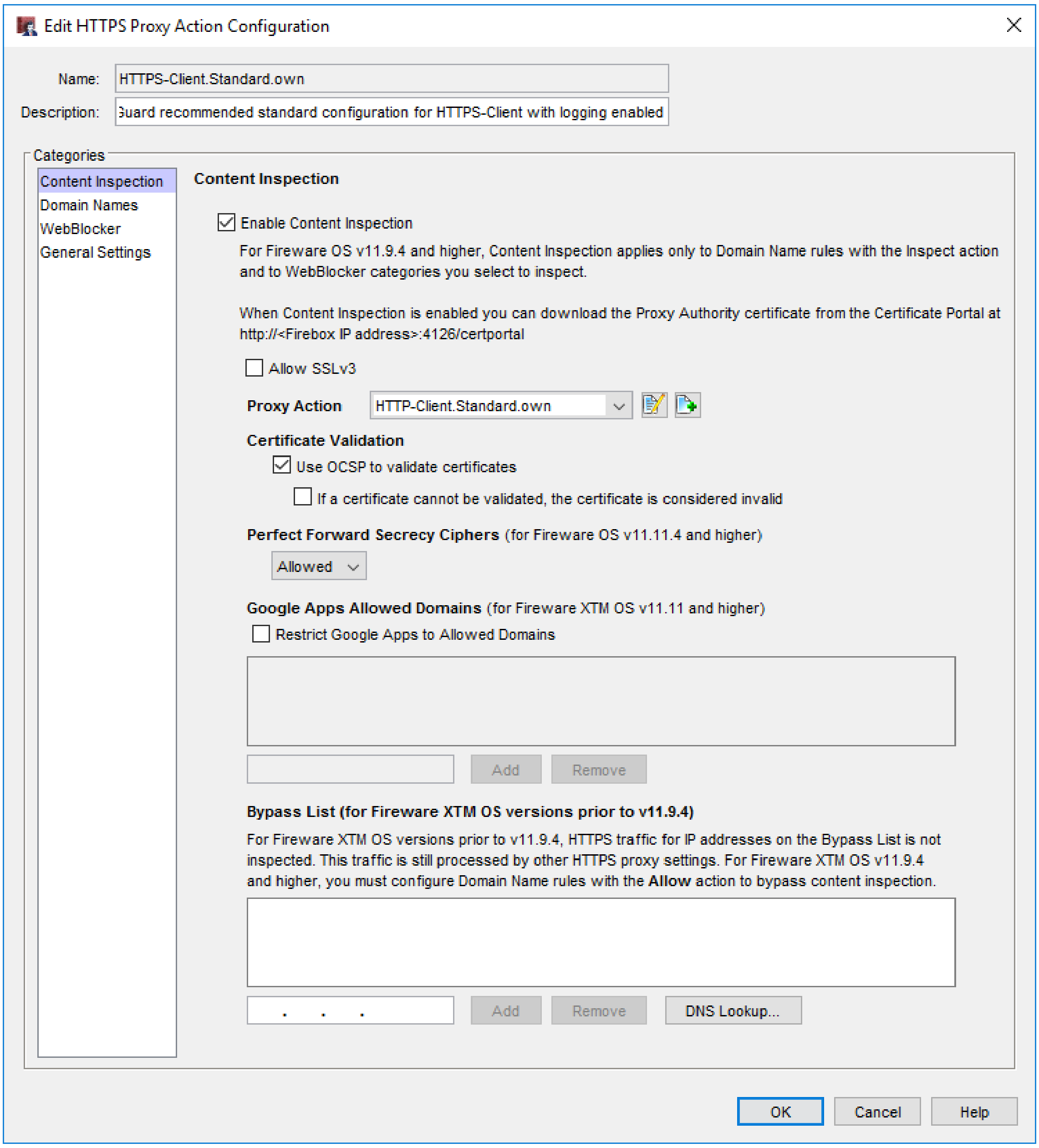
Host: %(url-host)%

Path: %(url-path)%

Helpdesk services

Figure 25. Custom Deny message

HTTPS-proxy – The HTTPS-proxy configurations were started by cloning the default Proxy action rule. From the rule itself, *Enable Content Inspection* was turned on. From the proxy action the HTTP-Client.Standard.own rule was selected to be used to inspecting the traffic inside the HTTPS traffic. (Figure 26)



Edit HTTPS Proxy Action Configuration

Name: HTTPS-Client.Standard.own

Description: 3uard recommended standard configuration for HTTPS-Client with logging enabled

Content Inspection

☑ Enable Content Inspection

For Fireware OS v11.9.4 and higher, Content Inspection applies only to Domain Name rules with the Inspect action and to WebBlocker categories you select to inspect.

When Content Inspection is enabled you can download the Proxy Authority certificate from the Certificate Portal at http://<Firebox IP address>:4126/certportal

□ Allow SSLv3

Proxy Action: HTTP-Client.Standard.own

Certificate Validation

☑ Use OCSP to validate certificates

□ If a certificate cannot be validated, the certificate is considered invalid

Perfect Forward Secrecy Ciphers (for Fireware OS v11.11.4 and higher): Allowed

Google Apps Allowed Domains (for Fireware XTM OS v11.11 and higher)

□ Restrict Google Apps to Allowed Domains

Bypass List (for Fireware XTM OS versions prior to v11.9.4)

For Fireware XTM OS versions prior to v11.9.4, HTTPS traffic for IP addresses on the Bypass List is not inspected. This traffic is still processed by other HTTPS proxy settings. For Fireware XTM OS v11.9.4 and higher, you must configure Domain Name rules with the **Allow** action to bypass content inspection.

Figure 26. Customer’s HTTPS Proxy settings

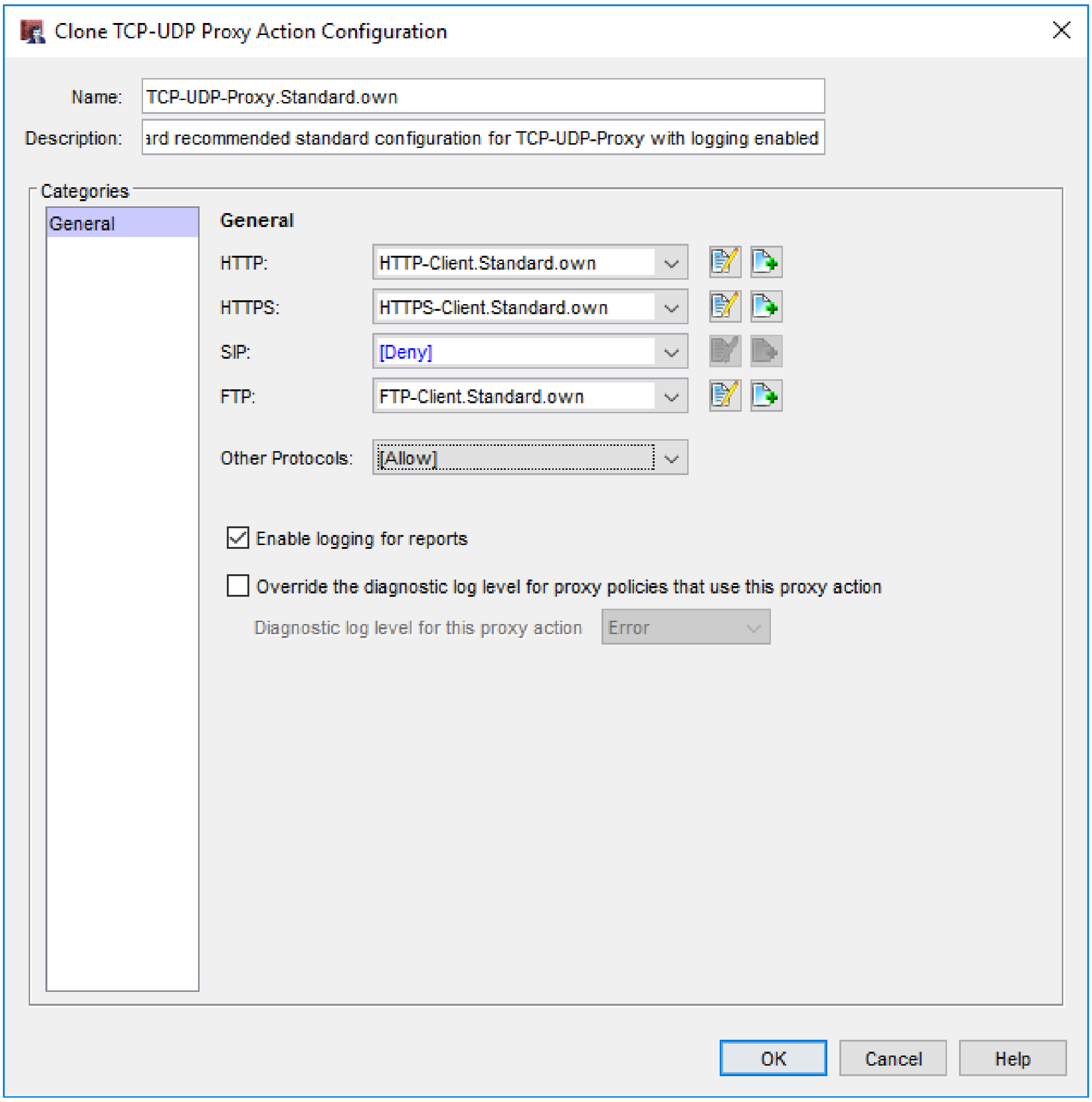
Contrary to the previous versions of firewall software the HTTPS-Proxy did not inspect all of the browsed HTTPS sites by default, but instead the HTTPS sites that would have been wanted to inspect must be manually inserted to the *Domain Names* list. This made the use of the HTTPS inspection a little hard since it required manual work to make the list. A way around this was to enter domain names wildcard from etc. *.fi and *.com. Either way, this had to be made for all domains that were wanted to be inspected.

For the HTTPS content inspection to properly work, the SSL transmission needs to be broken down. In a matter of fact this was a kind of a man in the middle attack, but this time it was used with good intentions. For the traffic interception to correctly work there were two different workarounds.

1. Use the firewall's self-signed certificate to intercept the traffic. The certificate needs to be downloaded from the firewall and then it must be installed to all computers that are used in internal network and sends traffic through the HTTP-proxy rule.
2. Another method was to use corporate Public Key Infrastructure if it was possible. Public Key Infrastructure or PKI means that one needs to have certificate infrastructure in place to publish certificates. Certificates must then be published and enrolled to every computer that was used in corporation. One certificate must be published and then installed to the firewall.

In this case the first option, firewall self-signed certificate, was used mainly because the customer did not have PKI in place and it would have been too complicated to implement it at this point. The certificate was installed to all client computers.

TCP-UDP-proxy – With the TCP-UDP-proxy the intention was that all traffic that was TCP or UDP traffic was going to go through this policy. The policy was automatically positioned as the last firewall rule. This way if rules that came before did not “catch” the traffic, this rule would do so. The default proxy action rule was cloned. From the cloned action configuration HTTP, HTTPS and FTP traffic was modified to use earlier .own rules. (Figure 27)



Clone TCP-UDP Proxy Action Configuration

Name: TCP-UDP-Proxy.Standard.own

Description: ard recommended standard configuration for TCP-UDP-Proxy with logging enabled

Categories

General

General

HTTP: HTTP-Client.Standard.own

HTTPS: HTTPS-Client.Standard.own

SIP: [Deny]

FTP: FTP-Client.Standard.own

Other Protocols: [Allow]

☑ Enable logging for reports

☐ Override the diagnostic log level for proxy policies that use this proxy action

Diagnostic log level for this proxy action: Error

Figure 27. Customer’s TCP/UDP Proxy settings

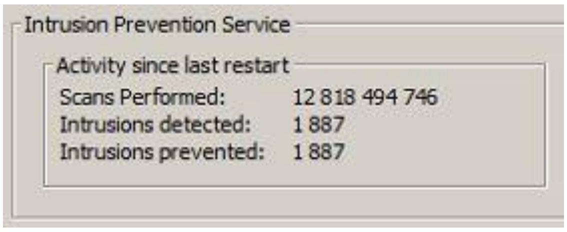
4 Evaluation of New Security Solution

This chapter explains how the new security solution was evaluated by first gathering data about the different security modules of the firewall. Then the findings were listed and analyzed to see the results. After that a proposition about the new security solution was done to the customer.

4.1 Data Gathering and Analysis

The data shown in this chapter was gathered by using the Watchguard firewall's own logging feature. This was possible since the firewall was not restarted during the test period. If the firewall had been restarted the data gathering would have been harder and the Watchguard's Dimension log server should have been used.

Intrusion Prevention (IPS) – The intrusion detection counter showed that it had scanned almost 13 billion packets. In those packets 1887 intrusions were detected. All intrusions were prevented. (Figure 28)



Intrusion Prevention Service

Activity since last restart

```
Scans Performed:        12 818 494 746
Intrusions detected:    1 887
Intrusions prevented:   1 887
```

Figure 28. Intrusion Prevention Service statistics

The most common intrusions that were prevented are listed below in an order where the first intrusion was used the most. This literally shows that different kinds of intrusion attempts have taken place.

WEB GNU Bash Remote Code Execution -1 (CVE-2014-6271)
WEB Apache HTTPD mod_proxy_ajp Denial Of Service (CVE-2011-3348
WEB Apache mod_ssl HTTP Request DOS -1
WEB Apache Struts Wildcard Matching OGNL Code Execution -4 (CVE
WEB Directory Traversal -8
WEB Apache HTTP Server mod_rewrite RewriteLog Command Execution
WEB HTTP Host Header Buffer Overflow
SSL SSLv2 CBC Cipher SSL_RC4_128_EXPORT40_WITH_MD5 (CVE-2016-08
SHELLCODE Egg Hunter -1

WEB Cross-Site Scripting -7

SSL SSLv2 CBC Cipher SSL_CK_RC4_128_WITH_MD5 (CVE-2016-0800)

EXPLOIT Arbitrary Code Injection -1

FILE Invalid XML Version -2

WEB SQL injection attempt -6

WEB SQL injection attempt -25

WEB-CLIENT HTTP Suspicious Div Tag -1

SSL OpenSSL TLS DTLS Heartbeat Information Disclosure -5 (CVE-2

WEB Remote File Inclusion /etc/passwd

WEB SQL injection attempt -10

WEB Remote Shell Command Execution -1

WEB NetBSD tnftp fetch.c fetch_url Command Execution -2 (CVE-20

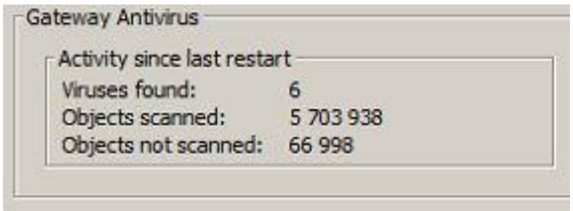
WEB-CLIENT Suspicious HTML Div Tag -2 (Ransomware Attack Vector

WEB-CLIENT Javascript Obfuscation in Exploit Kits - 30 (Ransomw

WEB HTTP Accept-Language Header Buffer Overflow

Webblocker URL Filtering – Blocked URLs did not show in the Watchguard firewall's internal log. For the blocked URLs to be seen Watchguard Dimension has to be used. During the present study, the customer did not visit any pre-defined blocked websites, or at least none could be found in the Dimension logs. This meant that the customer had not used websites that were denied by their categories.

Gateway antivirus – Gateway antivirus had scanned more than 5.7 million packets and in those it found 6 viruses. Measured in percentage this was a really small number, but it showed that there were viruses in the network traffic. (Figure 29)



Gateway Antivirus

Activity since last restart

Viruses found:	6
Objects scanned:	5 703 938
Objects not scanned:	66 998

Figure 29. Gateway Antivirus statistics

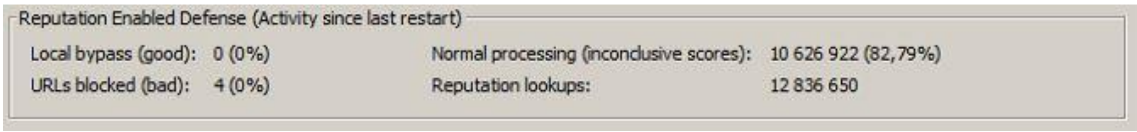
The viruses that had been found were the following:

VOD Zero-Hour Detection: [3] Virus threat HIGH.

JS/Phish

FakeAlert

Reputation enabled defense service – The reputation enabled defense scanned over 10 million URLs in which it found 4 that were considered to have a bad reputation. The service scans all found URLs which meant that if one went to a page which had linked URLs, for example a newspaper frontpage website, the scanned URLs count can rise up to hundreds of scans per webpage. It was surprising that bad URLs were not more numerous than this. This could have meant that the customer did not use that kind of sites that much and only used work related webpages at work. (Figure 30)

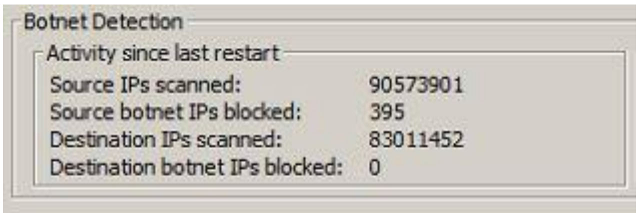


Reputation Enabled Defense (Activity since last restart)

Local bypass (good): 0 (0%)
URLs blocked (bad): 4 (0%)
Normal processing (inconclusive scores): 10 626 922 (82,79%)
Reputation lookups: 12 836 650

Figure 30. Reputation Enabled Defense statistics

Botnet Detection – The Botnet Detection module had scanned over 173 million IP addresses from which 395 IP addresses turned out to be part of the botnets. Only source botnets were blocked, so the assumption was that there was an illegal scanning of the customer's network or attempts to login to the firewall from those IP addresses. (Figure 31)



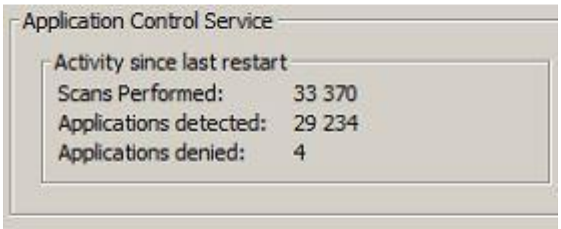
Botnet Detection

Activity since last restart

Source IPs scanned: 90573901
Source botnet IPs blocked: 395
Destination IPs scanned: 83011452
Destination botnet IPs blocked: 0

Figure 31. Botnet Detection statistics

Application control – From the logs it was found that almost 30 thousand different applications were used from the customer's network. From those only 4 were denied. Those 4 different applications were denied by the predefined settings. Those applications were Dropbox, OneDrive, Google Drive and iCloud. (Figure 32)



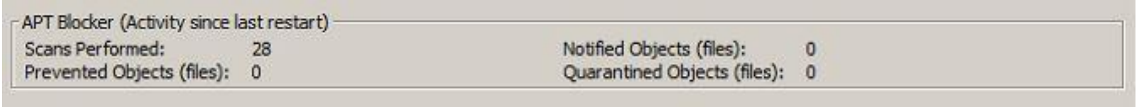
Application Control Service

Activity since last restart

Scans Performed: 33 370
Applications detected: 29 234
Applications denied: 4

Figure 32. Application Control Service statistics

APT Blocker – The ATP Blocker scanned files that were uncertain or which had no signature yet. 28 files were scanned and all of them were determined to be clean. (Figure 33)



APT Blocker (Activity since last restart)

Scans Performed:	28	Notified Objects (files):	0
Prevented Objects (files):	0	Quarantined Objects (files):	0

Figure 33. APT Blocker statistics

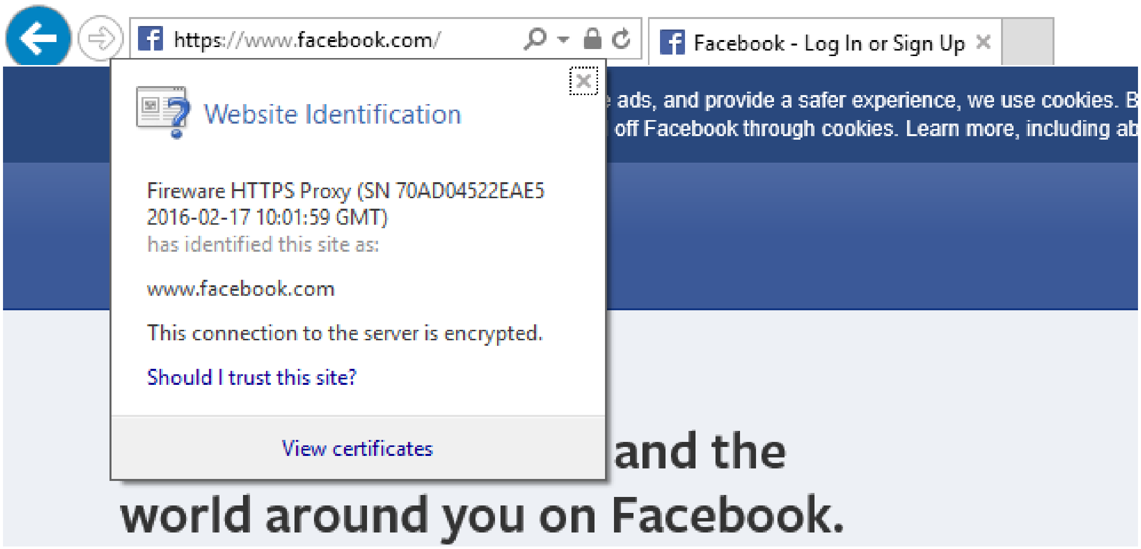
To summarize, all of the used UTM features found several threats and managed to handle them in their own manner. After analysis, evaluation of data will be done.

4.2 Data Evaluation

After the proof on concept had been made and the logs had been gathered and analysed, a couple of remarks were made. First of all, it was eye opening that such amount of traffic, injections and viruses were blocked during the test period. This clearly shows that the threats are real and part of everyday network traffic in one way or another. These same threats had most certainly been present when the old firewall was in place, but there were no tools to do anything about them. There is no way to tell the nature of one certain incident when the old firewall was in use or if the blocked threat with the new firewall is “fatal” or harmless. The most important thing is to have appropriate logging to find out if something abnormal has happened.

A little bit surprising was the fact that even though the firewall was running several months with all the security features on, some modules such as ATP Blocker did not found any threats. This was challenging to explain to the customer since they expected every module to produce results. In the security point of view, it was relieving to see that no zero-hour or unknown viruses had been found. This, however, does not mean that the environment itself has no zero-day threats, they just have not yet surfaced and been found.

Another issue was that the HTTPS proxy was found to be too challenging to be used. In the configuration phase it was described in two different ways to get the HTTPS inspection to work. In either case when users were browsing SSL secured sites, the firewall first intercepted the traffic, decrypted the packets, inspected the packets by the predefined rules and then the firewall passed the packet off to the end-user's browser. At this point the browser showed that the site that had being viewed, showed not the original site certificate, but the certificate that was installed to the firewall. (Figure 35)



Website Identification

Fireware HTTPS Proxy (SN 70AD04522EAE5 2016-02-17 10:01:59 GMT)
has identified this site as:

www.facebook.com

This connection to the server is encrypted.

Should I trust this site?

ads, and provide a safer experience, we use cookies. B
off Facebook through cookies. Learn more, including ab

and the
world around you on Facebook.

Figure 35. Certificate error

This way of showing the identity of the website was found to be misleading and the customer did not like the feature. Because of this the HTTPS proxy was disabled altogether. This lead to the point that HTTPS traffic was not inspected at all. The way the author saw this was that this produces a huge security risk, since more and more websites are using HTTPS encryption on their sites.

After some research was done about the HTTPS packet inspection it was found that it was a generally acknowledged problem that all organizations are facing. In IDC's whitepaper Robert Westervelt [7] revealed that the inspection of HTTPS traffic was indeed a problem and according to their surveys, at least half of all traffic that organizations was facing was encrypted.

4.3 Outcome and Security Solution Proposition

Shortly after the evaluation period was over the outcome of the study was presented to the customer. For that reason, a separate meeting was held. In that meeting the initial starting point with the original problems was first introduced. The deployment of the new firewall with all the used security modules was then covered. The customer was also briefed on what was the purpose of each of the modules.

After that, the gathered logs were handled with the customer together with the explanations of what actions the firewalls security features had exactly taken and why. The findings were thoroughly discussed to see the big picture. The customer was deeply impressed and at the same time confused about the findings. They thought that there was going to be no threats to found, because there was no clear indication of that. Which actually was the inline what they thought in the initial interview. Nevertheless, they were astonished about the amount of different security matters the firewall had covered.

Along with going through the findings with the company executives and IT, a couple of employees were interviewed about the deployment of the new security system. Not much usable information was gathered. The answers indicated that everything was working in their eyes the same as before. No one had seen the red banner (Figure 25) which indicated that they had entered a page that was not safe. This also verifies that no entries were found in logs about this.

After the meeting and final interviews were held, a proposition of acquiring the firewall with the security features that were presented earlier was made. The price of the firewall was around 2200 Euros including three-year support. The price was discussed with the customer and it was perceived that the price divided by three years was roughly 60 Euros per month. That price was ridiculously low compared to how much more security the device brings to the network. It was estimated that with that price at least one major security related incident can be avoided and because of that the purchase was more that justifiable. In addition, more logging was achieved for cases when something unknown has happened and more information was needed to sort it out.

5 Discussion and Conclusions

The need for this thesis originated from a customer that had an old firewall in use. The firewall lacked basic security functions and did not provide accurate logging. Discussion were held with the customer, about how to improve the network security without having to purchase several different appliances to do different jobs and at the same time to avoid spending lots of time and money.

In this thesis, the current state of global network security threats was presented together with different threat types. After that a short description of different UTM features was presented as well as the best practice of configuring the Watchguard firewall.

A short interview was held with the customer to understand their point of view to the security issues. At the same time a deployment plan was made according to the Watchguard best practices and settings that were agreed on with the customer.

A proof of concept was made with firewall installation including the security functions. After several months of operation, data about the usage of the firewall and statistics of the security modules were gathered and analyzed. Evaluation was made according to the collected and analyzed data.

The collected data supported the investment and therefore a proposition to purchase the new firewall was made to the customer. The customer saw the advantages the new security firewall brought and acquired the device and was still using it when this study was finalized.

In the most recent release of Watchguard software a new security feature called Threat Detection and Response was implemented. This feature introduces agents installed to the end-user’s workstations. They work in co-operation with Watchguard’s other modules bringing more security to an otherwise more challenging part of a network – endpoints.

Although the customer was very pleased with the security solution provided, they are still looking for new security features in future and constantly improving their environment. The new Threat Detection and Response feature will be taken in a test use. Also, a mobile phone management and security solution has been evaluated.

References

1 Symantec Internet Security Threat Report. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf (Accessed Oct 2016)

2 Center for Cyber Safety and Education. https://iamcybersafe.org/wp-content/uploads/2017/01/University-of-Phoenix-ISC2-cybersecurity-report.pdf (Accessed Sep 2016)

3 McAfee, The Economic Impact of Cybercrime and Cyber Espionage. https://www.mcafee.com/es/resources/reports/rp-economic-impact-cybercrime.pdf (Accessed Oct 2016)

4 Forbes, Cyber Crime Costs Projected To Reach $2 Trillion by 2019. http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#6839eaf63bb0 (Accessed Oct 2016)

5 Finnish Chamber of Commerce, Kyberturvallisuus 2015 http://www.digipaper.fi/kauppakamari/127242/ (Accessed Jun 2016)

6 Watchguard, Gateway Antivirus. https://www.watchguard.com/docs/tech/wg_gav_tb.pdf (Accessed Nov 2016)

7 https://dsimg.ubm-us.net/envelope/386743/514323/F5%20IDC%20Report%20The%20Blind%20State%20of%20Rising%20SSL%20Traffic.pdf

8 The Truth About Malware. http://www.malwaretruth.com/the-list-of-malware-types/ (Accessed Oct 2016)

9 Vracode, Common Malware Types: Cybersecurity 101. https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101 (Accessed Oct 2016)

10 PHP Security, Injection Attacks. http://phpsecurity.readthedocs.io/en/latest/Injection-Attacks.html (Accessed Sep 2016)

11 TechRepublic, Understand the evolution of firewalls. http://www.techrepublic.com/article/understand-the-evolution-of-firewalls/ (Accessed Oct 2016)

12 Watchguard, Subscriptions Datasheet. http://www.watchguard.com/docs/datasheet/wg_subscriptions_ds.pdf (Accessed Nov 2016)

Watchguard Dimension Log Sample Report

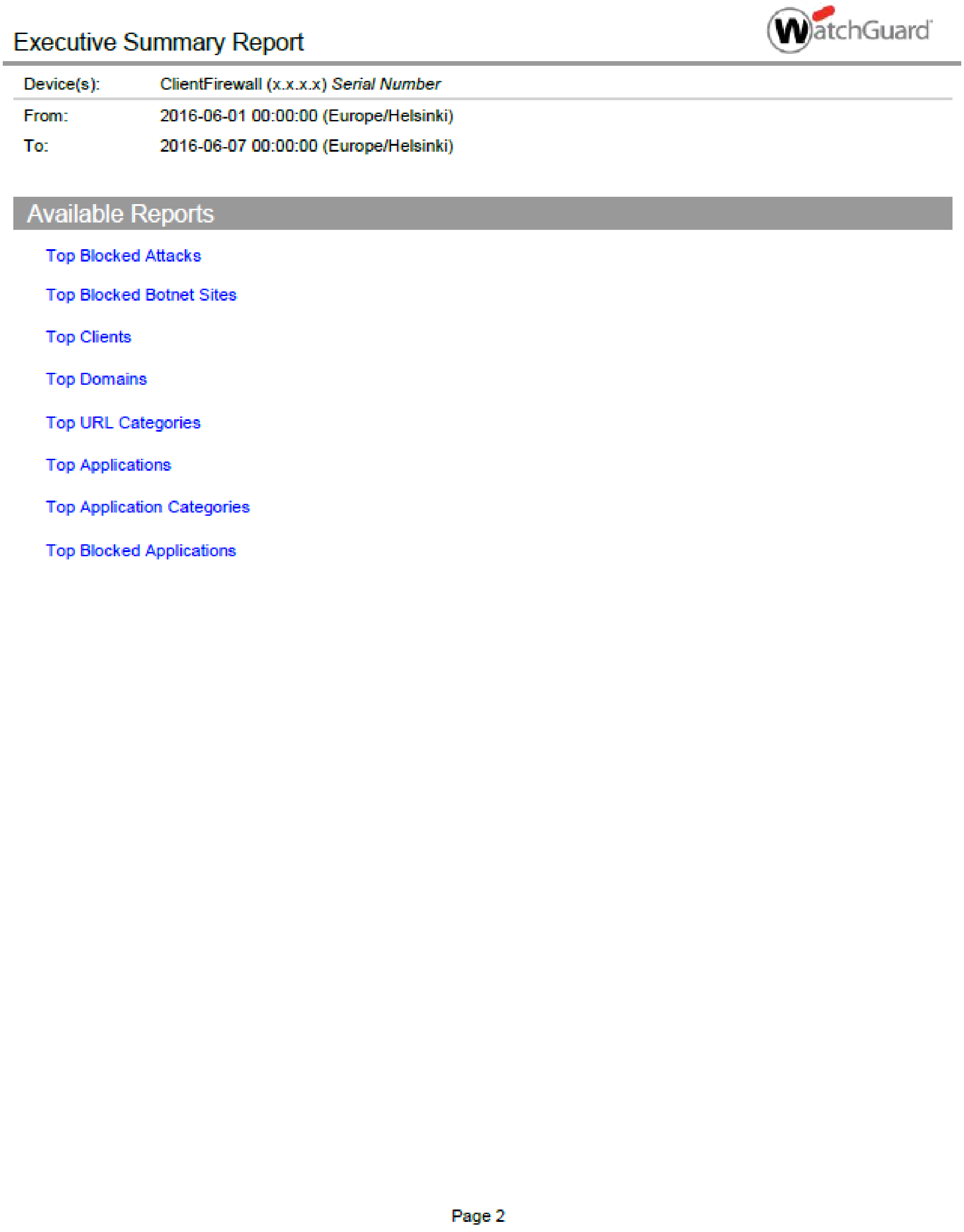
Executive Summary Report

Report generated 2016-06-07 00:02:31 (Europe/Helsinki)

Complete Visibility into network traffic and security events boosts efficiency, productivity, and profitability. The summary report provides the business intelligence that you need to support key goals:

- *Ensure productive use of corporate assets and time throughout the organization.*
- *Audit compliance against acceptable usage policies for Internet usage.*
- *Monitor protection against spyware, malware, and viruses.*

Page 1



Executive Summary Report

Device(s):	ClientFirewall (x.x.x.x) *Serial Number*
From:	2016-06-01 00:00:00 (Europe/Helsinki)
To:	2016-06-07 00:00:00 (Europe/Helsinki)

Available Reports

- Top Blocked Attacks
- Top Blocked Botnet Sites
- Top Clients
- Top Domains
- Top URL Categories
- Top Applications
- Top Application Categories
- Top Blocked Applications

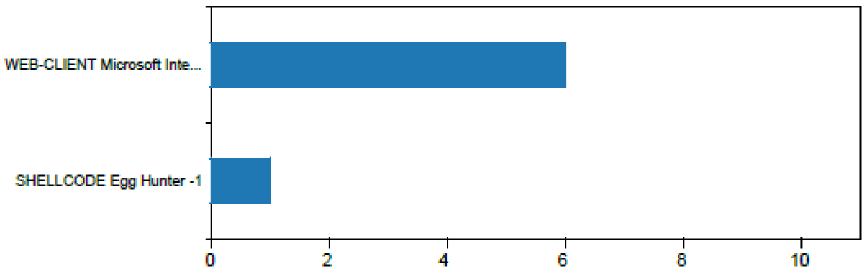
Page 2

Top Blocked Attacks

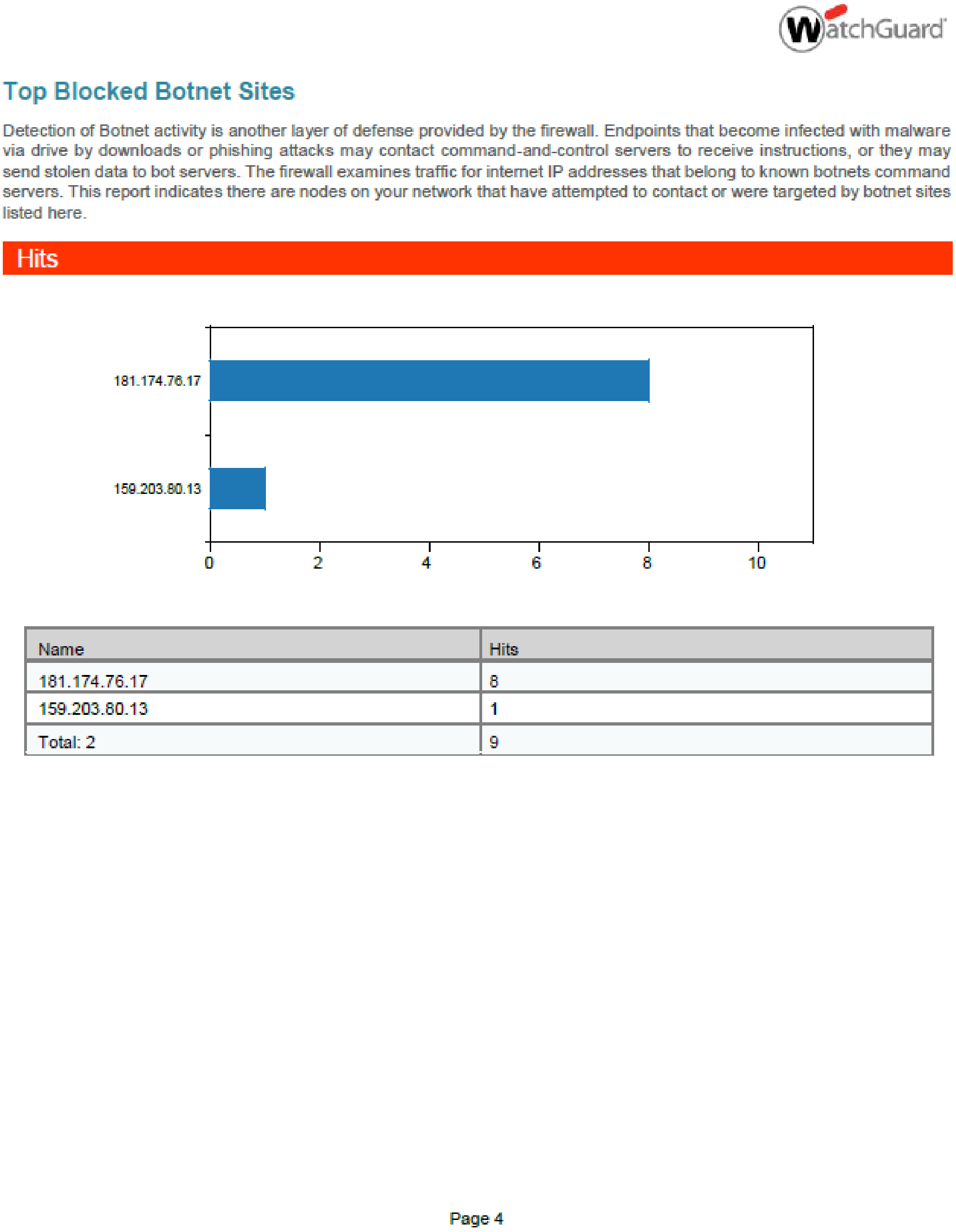
The Intrusion Prevention Service (IPS) provides real-time protection against network threats, including spyware, SQL injections, cross-site scripting, and buffer overflows. Skillful hackers can exploit these vulnerabilities to gain control of computer systems in the network. For example with buffer overflows, the hacker can send input that overflows the allocated memory, enabling them to gain access to the portion of memory where code is executed. Once code is installed, it can be used for theft of company financial data, or botnets could be used to extract company confidential information.

This report details the top intrusion attacks that were blocked at the firewall over the reporting period. More details about each intrusion attack are available at the **WatchGuard Security Portal** (http://www.watchguard.com/SecurityPortal/ThreatDB.aspx)

Hits



Name	Hits
WEB GNU Bash Remote Code Execution -1 (CVE-2014-6271)	6
SHELLCODE Egg Hunter -1	1
Total: 2	7



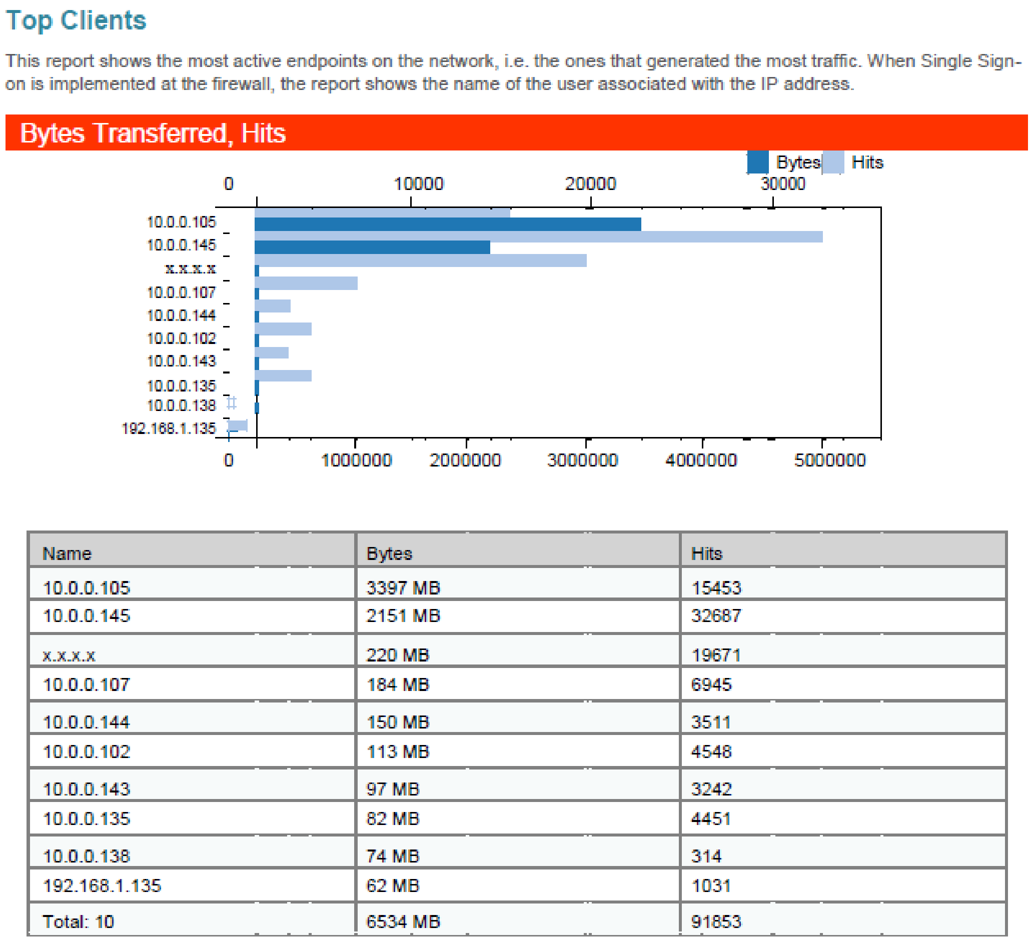
WatchGuard

Top Blocked Botnet Sites

Detection of Botnet activity is another layer of defense provided by the firewall. Endpoints that become infected with malware via drive by downloads or phishing attacks may contact command-and-control servers to receive instructions, or they may send stolen data to bot servers. The firewall examines traffic for internet IP addresses that belong to known botnets command servers. This report indicates there are nodes on your network that have attempted to contact or were targeted by botnet sites listed here.

Hits

Name	Hits
181.174.76.17	8
159.203.80.13	1
Total: 2	9

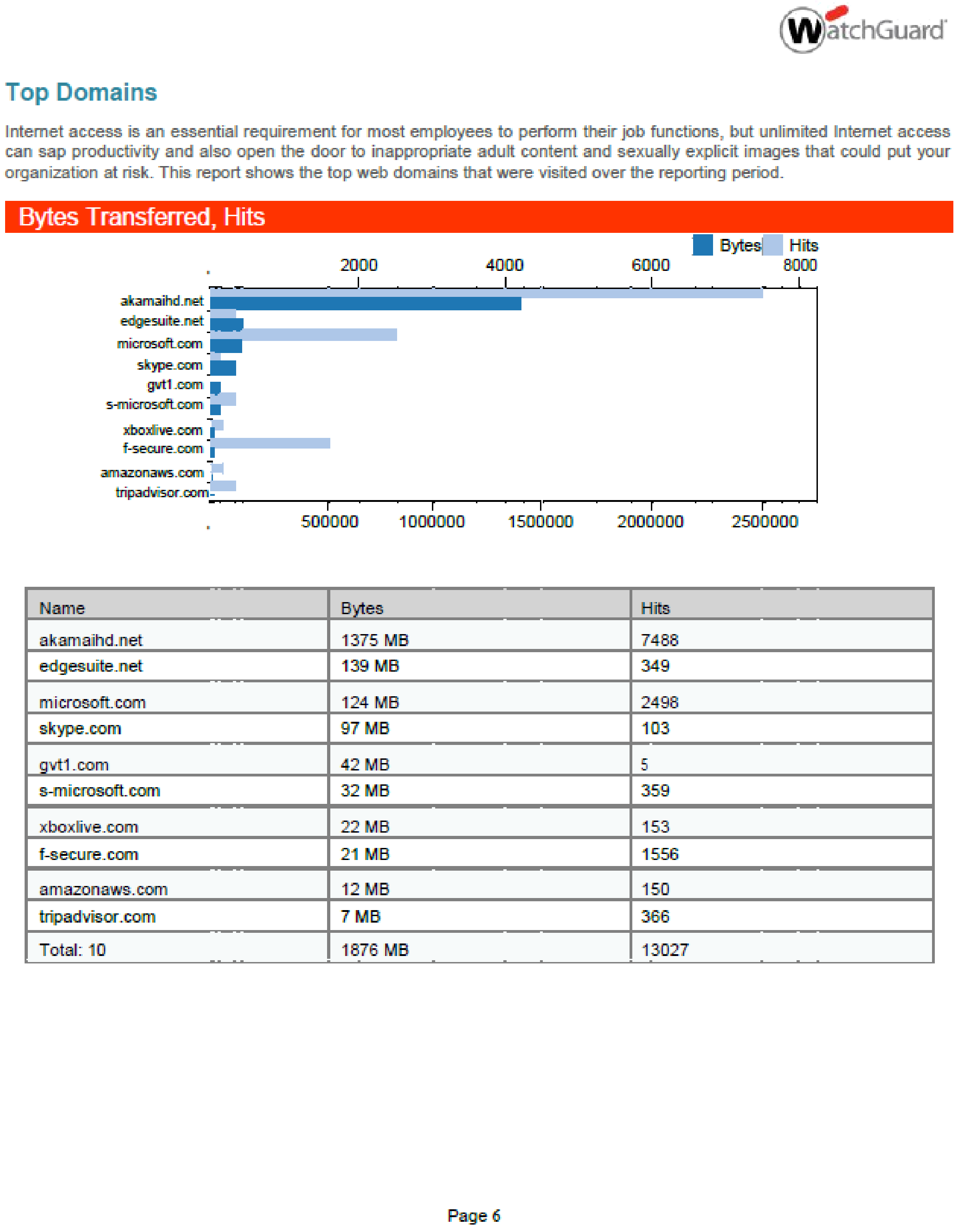


Top Clients

This report shows the most active endpoints on the network, i.e. the ones that generated the most traffic. When Single Sign-on is implemented at the firewall, the report shows the name of the user associated with the IP address.

Bytes Transferred, Hits

Name	Bytes	Hits
10.0.0.105	3397 MB	15453
10.0.0.145	2151 MB	32687
x.x.x.x	220 MB	19671
10.0.0.107	184 MB	6945
10.0.0.144	150 MB	3511
10.0.0.102	113 MB	4548
10.0.0.143	97 MB	3242
10.0.0.135	82 MB	4451
10.0.0.138	74 MB	314
192.168.1.135	62 MB	1031
Total: 10	6534 MB	91853

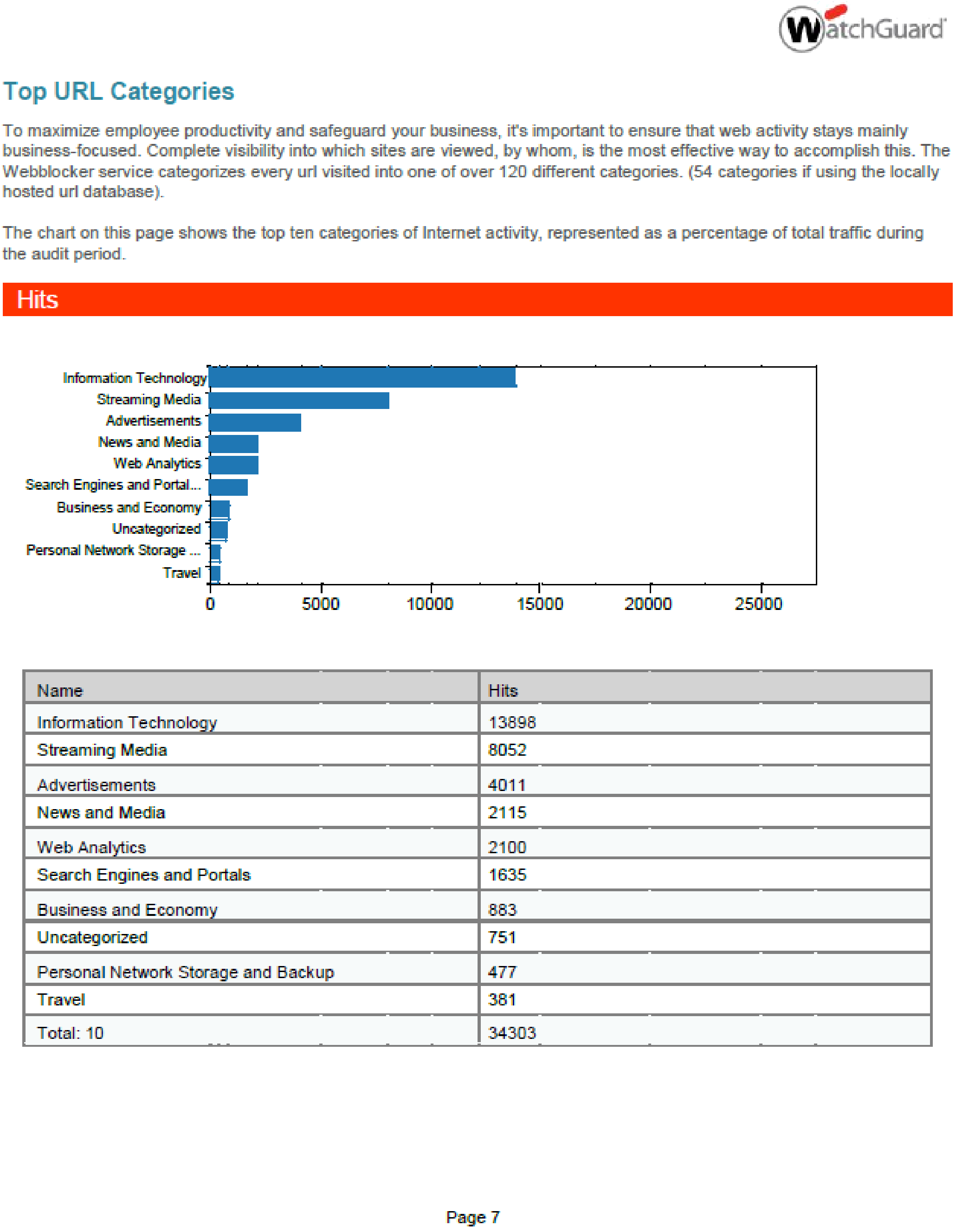


Top Domains

Internet access is an essential requirement for most employees to perform their job functions, but unlimited Internet access can sap productivity and also open the door to inappropriate adult content and sexually explicit images that could put your organization at risk. This report shows the top web domains that were visited over the reporting period.

Bytes Transferred, Hits

Name	Bytes	Hits
akamaihd.net	1375 MB	7488
edgesuite.net	139 MB	349
microsoft.com	124 MB	2498
skype.com	97 MB	103
gvt1.com	42 MB	5
s-microsoft.com	32 MB	359
xboxlive.com	22 MB	153
f-secure.com	21 MB	1556
amazonaws.com	12 MB	150
tripadvisor.com	7 MB	366
Total: 10	1876 MB	13027



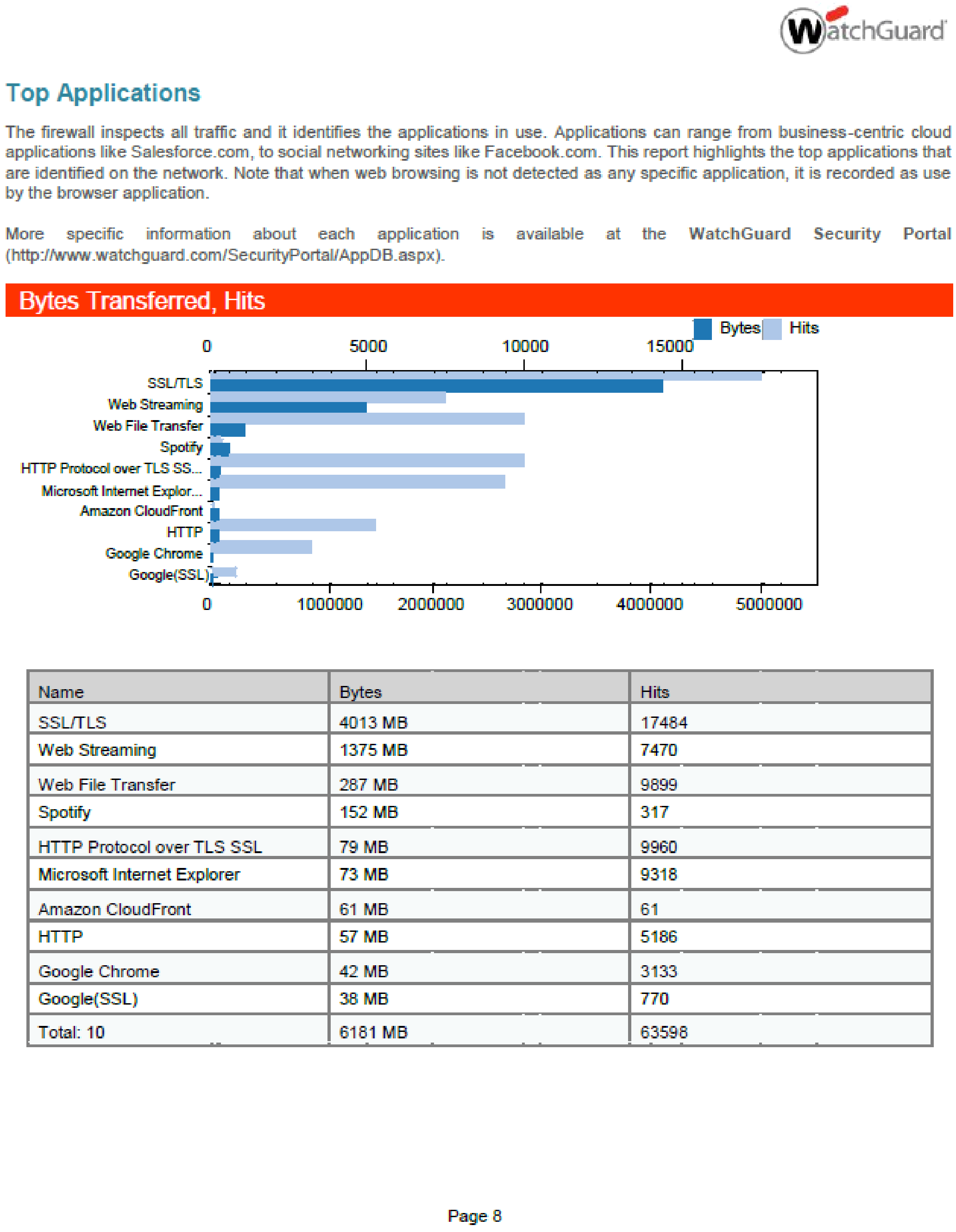
Top URL Categories

To maximize employee productivity and safeguard your business, it's important to ensure that web activity stays mainly business-focused. Complete visibility into which sites are viewed, by whom, is the most effective way to accomplish this. The Webblocker service categorizes every url visited into one of over 120 different categories. (54 categories if using the locally hosted url database).

The chart on this page shows the top ten categories of Internet activity, represented as a percentage of total traffic during the audit period.

Hits

Name	Hits
Information Technology	13898
Streaming Media	8052
Advertisements	4011
News and Media	2115
Web Analytics	2100
Search Engines and Portals	1635
Business and Economy	883
Uncategorized	751
Personal Network Storage and Backup	477
Travel	381
Total: 10	34303



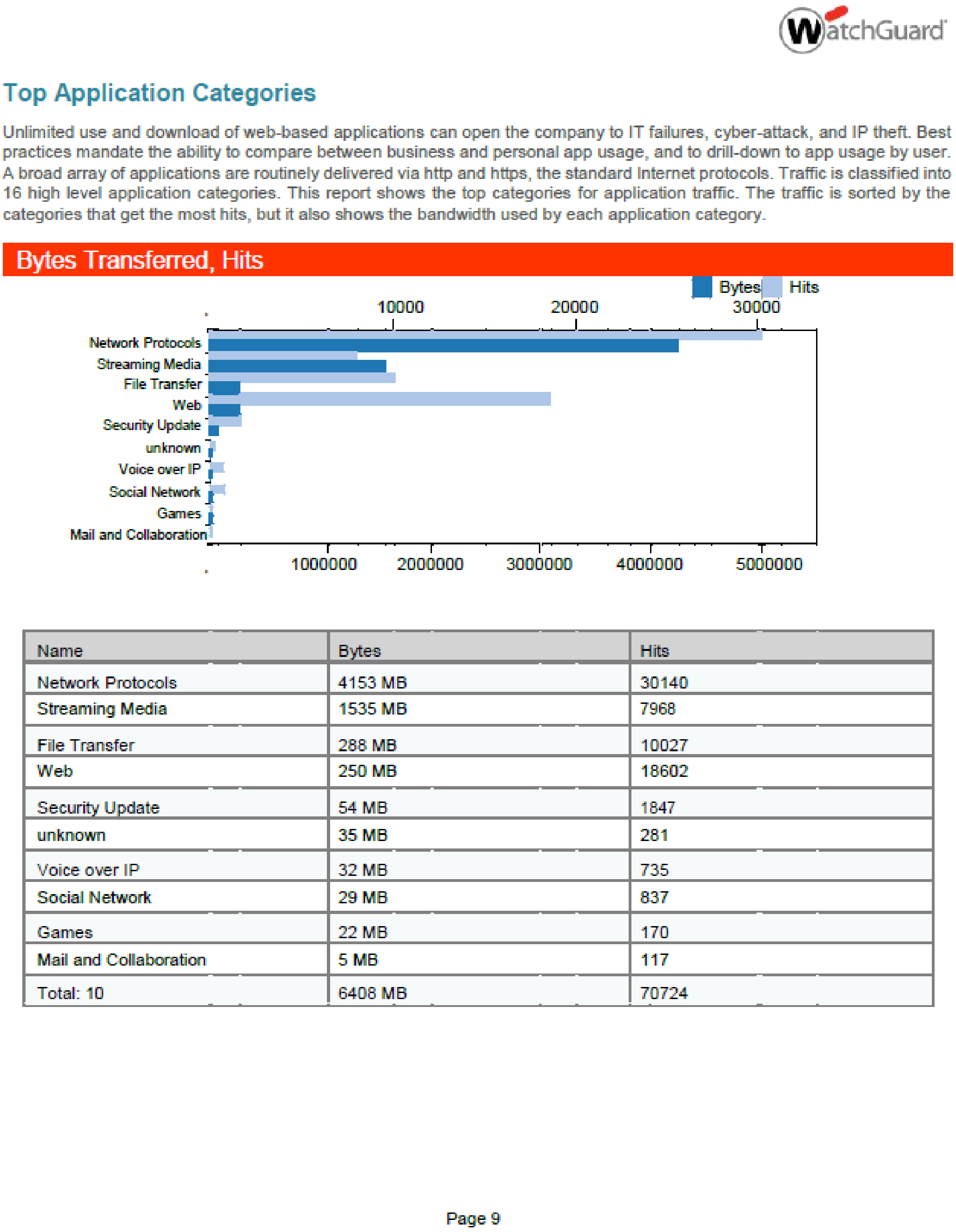
Top Applications

The firewall inspects all traffic and it identifies the applications in use. Applications can range from business-centric cloud applications like Salesforce.com, to social networking sites like Facebook.com. This report highlights the top applications that are identified on the network. Note that when web browsing is not detected as any specific application, it is recorded as use by the browser application.

More specific information about each application is available at the **WatchGuard Security Portal** (http://www.watchguard.com/SecurityPortal/AppDB.aspx).

Bytes Transferred, Hits

Name	Bytes	Hits
SSL/TLS	4013 MB	17484
Web Streaming	1375 MB	7470
Web File Transfer	287 MB	9899
Spotify	152 MB	317
HTTP Protocol over TLS SSL	79 MB	9960
Microsoft Internet Explorer	73 MB	9318
Amazon CloudFront	61 MB	61
HTTP	57 MB	5186
Google Chrome	42 MB	3133
Google(SSL)	38 MB	770
Total: 10	6181 MB	63598



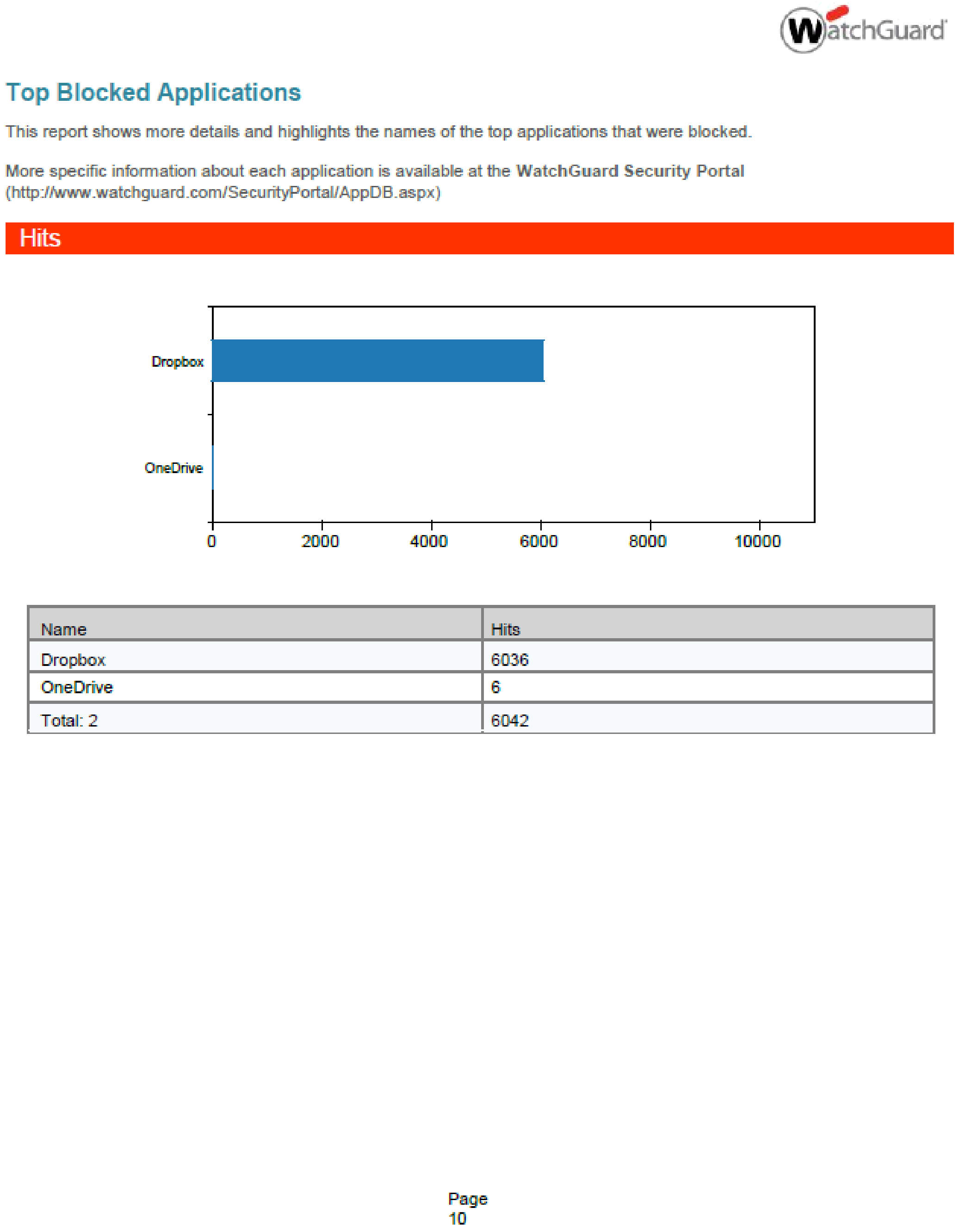
WatchGuard

Top Application Categories

Unlimited use and download of web-based applications can open the company to IT failures, cyber-attack, and IP theft. Best practices mandate the ability to compare between business and personal app usage, and to drill-down to app usage by user. A broad array of applications are routinely delivered via http and https, the standard Internet protocols. Traffic is classified into 16 high level application categories. This report shows the top categories for application traffic. The traffic is sorted by the categories that get the most hits, but it also shows the bandwidth used by each application category.

Bytes Transferred, Hits

Name	Bytes	Hits
Network Protocols	4153 MB	30140
Streaming Media	1535 MB	7968
File Transfer	288 MB	10027
Web	250 MB	18602
Security Update	54 MB	1847
unknown	35 MB	281
Voice over IP	32 MB	735
Social Network	29 MB	837
Games	22 MB	170
Mail and Collaboration	5 MB	117
Total: 10	6408 MB	70724



WatchGuard

Top Blocked Applications

This report shows more details and highlights the names of the top applications that were blocked.

More specific information about each application is available at the **WatchGuard Security Portal** (http://www.watchguard.com/SecurityPortal/AppDB.aspx)

Hits

Name	Hits
Dropbox	6036
OneDrive	6
Total: 2	6042