## **C:\Users\RoRo\Desktop\bus1_logo.jpg**

**Lebanese University**

**Faculty of Economics and Business Administration**

**First Branch**

Network Cybersecurity Attacks: Monitoring and Prevention

Case: LU Head Office Intrusion Prevention System

**For Obtaining a BA Degree in Business Computer**

**Prepared By:**

**Hussein Tarhini**

**20161212**

**Committee Members:**

**Dr. Mustapha Sarji (Supervisor)**

**Dr. Ali El-Moussaoui (Co-Supervisor)**

**Academic Year 2019-2020**

Table of contents:

[**Acknowledgment**](#_Toc57467386) III

[**Abstract** IV](#_Toc57467386)

[**1.** **Chapter1**:**Introduction** 1](#_Toc57467386)

[**2.** Chapter2:**Cyberattacks and NGN Firewalls** 3](#_Toc57467387)

### 2.1 Reconnaissance ………………………………………………………………………………………………………………………..3

### 2.2 Weaponization ……………………………………………………………………………………………………………………….. 5

### 2.3 Delivery …………………………………………………………………………………………………………..…........................5

### 2.4 Exploitation ……………………………………………………………………………………………………….……………………..5

### 2.5 Installation…………………………………………………………………………………………………………………………….….6

### 2.6 Command and control ……………………….………………………………………………………………………………...... 7

### 2.7 Actions on the objective……………………………………………………………………………………………………........8

### 2.7 Next Generation Firewall………………………………………………………………………………………………..…….... 9

[**3.** Chapter3**:Lebanese University Case Study** 10](#_Toc57467388)

[3.1 Lebanese University infrastructure 10](#_Toc57467389)

[3.2 Lebanese University NGNFirewall 11](#_Toc57467390)

[3.2.1 PaloAlto Firewall Overview 11](#_Toc57467391)

#### A- Policy Types ……………………………………………………………………………………………………………………….. 12

#### B-Monitoring logs …………………………………………………………………………………………………………………… 13

[3.2.2 LU Palo-Alto 22](#_Toc57467392)

#### Existing Security Policy………………………………………………………………………………………………………………. 22

##### A-Existing Policy Object URL filtering …………………………………………………………………………………….. 28

##### B-Existing Policy Object DOS Protection…................................................................................... 35

##### C- Existing Policy Object File Blocking…………………………………………………………………………………….. 38

[**4.** Chapter4:**Enhancement to exiting LU policy** 40](#_Toc57467393)

[4.1 URL filtering Policy Object enhancement 40](#_Toc57467394)

[4.2 DOS Protection Policy Object enhancement 49](#_Toc57467397)

[4.3 File Blocking Policy Object enhancement 53](#_Toc57467397)

[**5. Chapter5:Conclusion** 55](#_Toc57467400)

[References 57](#_Toc57467401)

**Acknowledgement**

At the beginning of this project, I want to acknowledge all those who gave a hand in completing this modest work. Without their help, this report would have been much harder. So my sincere thanks to them for their cooperation and support.

I would like to thank **Dr. Mustapha Sarji**, my honorable Supervisor who gave me the opportunity to work on Lebanese university security system. I would also like to thank **Dr. Jawad khalife** head of the cybersecurity department in the Lebanese university for the guidance and help he provided on this project. At last, I would like to mention that this report gave me the chance to work on a real cybersecurity machine, which helped me to acquire clear insight about the real life of security process. It was a thoroughly enjoyable experience.

**Abstract**

The Lebanese University is one of the top ranked universities in Lebanon. Same as other

Organizations it faces the danger of cyberattacks. To avoid cyberattacks it must adopt a cybersecurity System that is capable of protecting it. This project is about creating a Next Generation Firewall policy that will help securing the university and at the same

Time will not affect the needed resources for the accomplishment of Employees work,

After studying this Policy from Every aspect, we recommended some changes to

Enhance the applied policy with mentioning the reasons for this recommendation.

After applying the modifications, we reached a point where the Lebanese cybersecurity System was upgraded and capable to face cyberattacks using a better

**CHAPTER 1: INTRODUCTION**

This project case study is the Lebanese University it is the only public institution in

Lebanon carrying out the functions of the public higher education with its various

Majors and degrees, scientific research and continuous training. Due to the evolvement

Of covid19 pandemic the Lebanese university as other universities for the sake of its

Students and staff switched for having administrative work and learning done online.

This Exposed the University to Cybercriminals, they tend to take advantage of any

Vulnerability in the system and use it for attacking the university network for stealing

Data, destroying data, breaking down the network extra…

This view aroused a conclusion that my project will build on it that States the Essential

Need for securing every aspect Of Information and data against Cyberattacks Using

Cybersecurity. For whom who don’t know what cybersecurity is, cybersecurity refers to

A range of Systems, procedures and practices designed to secure Networks, computers,

Programs and data from attacks, harm or unauthorized access.

The report will cover four main topics; each will get elaborate in a separate chapter

Chapter 2 will mention the definition of cyberattacks and the tools that used to protect against cyberattacks then we will choose one of those tools and focus our work on.

Chapter 3 will contain an overview of the case study related to the Lebanese university; we will inform the reader with the needed information about the Lebanese university network infrastructure. Then mention the next generation firewall type used in the university and what are the features of this next generation fire wall that make it so special, then will get to the policies being used to protect against cyberattacks.

Chapter 4 will focus on enhancing the existing Lebanese university policies if needed. Moreover, if it is in need we will explain how it concluded.

Chapter 5 will be the conclusion it will contain an overview of the work we have done discuss its reliability and how it helped upgrading the Lebanese University cyber security system.

# **CHAPTER 2: CYBERATTACKS AND NGFW**

*CYBERATTACKS:*

Cyberattack is an attempt to acquire unauthorized access for damage or harm to a

Machine or a computer system.

With the evolvement of cybersecurity nowadays, cyberattacks also evolved especially in

Their Strategy from a direct attack against a high-value server to a patient, multistep

Process that blends Exploits, malware, Stealth and evasion in a coordinated network

Attack (“Low and Slow”).

The Cyberattack Lifecycle (see Figure1) illustrates the sequence of events that an

Attacker goes through to infiltrate a network and steal valuable data. Blocking of just

One-step breaks the chain can effectively defend an organization’s network and data

Against an attack.

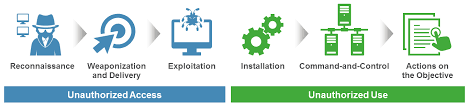


Figure 1 the Cyberattack Life cycle (Verizon Enterprise Solutions, 2018)

1. **Reconnaissance:** Like common offenders, aggressors meticulously arrange their

Cyberattacks. They research, distinguish, and select targets, regularly extricating open

Information from focused on employees’ social media profiles or from corporate

Websites, which can be valuable for social designing and phishing plans. Assailants will

Moreover, Use different apparatuses to scan for network vulnerabilities, services and

Applications that they can misuse, such as:

* **Network analyzers** (also known as packet analyzers, protocol analyzers, or packet sniffers) used to monitor and capture raw network traffic (packets). Examples include tcp dump and Wireshark (formerly Ethereal).
* **Network vulnerability** regularly comprise of a suite of devices counting password crackers, port scanner, and vulnerability scanner and are utilized to test an organization for vulnerabilities (counting arrangement mistakes) that can be misuse
* **Password crackers**. Utilized to perform brute-force word reference assaults against secret word hashes. Example John the Ripper and THC Hydra.
* **Port scanners**: utilized to test for open TCP or UDP (counting ICMP) ports on an endpoint. Examples include Nmap (“network mapper”) and Nessus.
* **Web application vulnerability scanners**: utilized to check web applications for vulnerabilities such as cross-site scripting, SQL injection, and directory traversal. Examples include Burp Suite and OWASP Zed Attack Proxy (ZAP).
* **Wi-Fi vulnerability scanners** are utilized to check wireless networks for vulnerabilities (counting open and misconfigured access points), to capture wireless network traffic, and to crack wireless passwords. Examples include Aircrack-ng and Wifite.

Breaking the Cyberattack Lifecycle at this stage of an assault starts with proactive and

Effective Client security mindfulness preparing that centers on subjects such As social

Engineering strategies (for illustration, phishing, piggybacking, and shoulder surfing),

Social Media (for case, security and protection issues), and organizational Security

Policies (For illustration, password requirements, remote access, and Physical

Security). Another critical countermeasure is nonstop checking and review of Arrange

Traffic Stream to identify and avoid unauthorized harbor and helplessness Filters have

Sweeps and other suspicious action. Compelling alter and setup Administration

Processes offer Assistance guarantee that recently conveyed applications and Endpoints

Are legitimately Configured (for illustration, debilitating unneeded ports and

Administrations) and Maintained. (Verizon Enterprise Solutions, 2018)

2**. Weaponization:** Next, attackers decide which strategies to utilize to

Compromise a Target endpoint. They may select to insert intruder code inside

Apparently harmless Files such as a PDF or Microsoft Word record or mail message.

Breaking the Cyberattack Lifecycle at this stage of an assault is challenging since

Weaponization regularly happens inside the attacker’s network. In any case,

Examination of Artifacts (both malware and weaponized) can give imperative danger

Insights to enable successful zero-day protection when delivery (the next step) is

Attempted. (Verizon Enterprise Solutions, 2018)

3. **Delivery**. Attackers next attempt to deliver their weaponized payload to a target

Endpoint, for example, via email, instant messaging (IM), and drive-by download (an

End User’s web browser is redirect to a webpage that automatically downloads

Malware to The endpoint in the background), or infected file share.

Breaking the Cyberattack Lifecycle at this stage of an assault requires visibility into

All Network activity (counting remote and mobile devices) to successfully square

Malicious or Risky websites, applications, and IP addresses to anticipate known and

Obscure malware in expansion to exploits. (Verizon Enterprise Solutions, 2018)

4. **Exploitation**. After a weaponized payload conveyed to a target endpoint, it must be

Activated. An end user may unwittingly trigger an exploit, for case, by clicking A

Malicious link or opening an infected attachment using an e-mail, or an attacker may

Remotely trigger an exploit against a known server vulnerability on the target network

Breaking the Cyberattack Lifecycle at this stage of an assault, as amid the

Reconnaissance stage starts with proactive and compelling end-user security

Mindfulness Training that centers on themes such as malware anticipation and mail

Security. Other Important security countermeasures incorporate vulnerabilities and

Patch management; Malware location and anticipation; danger insights (counting

Known and obscure Threats); blocking unsafe, unauthorized, or unneeded applications

And Administrations; overseeing File or catalog authorizations and root or director

Benefits; and logging and monitoring organization activity. (Verizon Enterprise Solutions, 2018)

5**. Installation**. Following, an aggressor will raise benefits on the compromised

Endpoint, for case, by setting up remote shell access and installing rootkits or other

Malware. With remote shell access, the aggressor has control of the endpoint and

Can execute commands in advantaged mode from a command line interface (CLI), as in

Case physically sitting before the endpoint. The assailant will at that point move along

The target’s network, executing assault code, recognizing other targets of Opportunity,

Besides, compromising extra endpoints to set up persistence.

The key to breaking the Cyberattack Lifecycle at this stage of an assault is to constrain

Or Restrict the attacker’s movement inside organization network. Use network

Segmentation and a Zero trust model that screens and assesses all activity between

Zones or Segments and granular control of applications that permitted on the

Organization network. (Verizon Enterprise Solutions, 2018)

6. **Command and control**. Attackers build up encrypted communication channels back

To command-and-control (C2) servers over the web so that they can alter their Attack

Destinations and strategies as extra targets of opportunity recognized inside the victim

Network, or to avoid any modern security countermeasures that the Organization May

Endeavor to send in case assault artifacts found. Communication is Basic to An assault

Since it empowers the aggressor to remotely coordinate the assault and execute the

Attack targets. C2 activity must be in this manner versatile and stealthy for an assault

To Succeed. Assault communication activity is as a rule covered up with Different

Methods and Tools, including:

* **Encryption** with SSL, SSH (Secure Shell), or some other custom or proprietary encryption.
* **Circumvention** via proxies, remote access tools, or tunneling. In some instances, use of cellular networks enables complete circumvention of the target network for attack C2 traffic.
* **Port evasion** using network anonymizers or port hopping to traverse any available open ports.
* **Fast Flux** (or Dynamic DNS) to proxy through multiple infected endpoints or multiple ever-changing C2 servers to reroute traffic and make determination of the true destination or attack source difficult.
* **DNS tunneling** used for C2 communications, as well as data infiltration (for example, sending malicious code, commands, or binary files to a victim) and data exfiltration.

Breaking the Cyberattack Lifecycle at this stage of an assault requires assessment of all

Network activity (counting scrambled communications), blocking of outbound C2

Communications with anti-C2 signatures (along with file and data pattern uploads),

Blocking of all outbound communications to known pernicious URLs and IP

Addresses, blocking of novel assault methods that utilize port evasion methods,

Anticipation of the Use of anonymizers and proxies on the network, observing of

DNS for malicious domains and countering with DNS sinkholing or DNS poisoning, and

Redirection of Malicious outbound communications to honeypots to recognize or square

Compromised Endpoints and analyze assault traffic. (Verizon Enterprise Solutions, 2018)

7. **Actions on the objective**. Attackers regularly have numerous, diverse assault targets

Including information burglary; annihilation or alteration of basic frameworks, systems,

Information and Denial-of-service (DoS). This final arrangement of the Cyberattack

Lifecycle can too utilized by an assailant to develop the early stages of the Cyberattack

Lifecycle against another Target. The 2018 Verizon Information Breach Examinations

Report (DBIR) portrays this Strategy as an auxiliary rationale in, which “[web

Applications] are compromised to help and abet within the assault of another victim.”1

For case, an assailant may compromise a Company is extranet to breach a commerce

Accomplice that is the essential target. Concurring to The DBIR, in 2014 there were

23,244 “Incidents where web applications were compromised with an auxiliary motive.”2

The Assailant turns the assault against the starting Victim organize to a diverse casualty

Organize, in this way making the introductory casualty an unwitting Accomplice.

To halt the lifecycle of a cyber-attack there are numerous instruments that are utilized one

Of the foremost Known instrument is another era firewall. In my extend I will work on

This instrument In the Lebanese university and consider how it utilized productively to

Maintain a strategic distance from cyber-attacks (Verizon Enterprise Solutions, 2018).

*NEXT GENERATION FIREWALL:*

Past days people would have different security components to get the needed protection

You would have an inspection firewall on the internet edge (blocks traffic based on

Network Information such as ip address, network protocol and network port), you would

Have an Intrusion prevention device on the network; you would have an anti-malware

Device in the Environment and web content control for user internet activity. But these

Where All Separate devices eventually people started combining these into a single

Device. Called Next Generation Firewall. This NGFW can look at the traffic and

Determine which Application is using the permitted port now and this device can make

Filtering decisions based on the identity of the application, this gives us as administrators

More power to Create access control and make sure that only the applications that we

Approve are Allowed through the firewall and other applications are blocked, even

If all those Applications are using the same port id. In addition, NGFW Can Make filtering Decisions based on user identity so that the same policy can be applied to the

Connected Device wherever it is connected to regardless of the ip address it has at that

Instance because the same user is using it so we can apply the same policy and it Will

Follow the User around regardless whether they are connecting internally or externally.

There are different kinds of next generation firewalls one of the most known Firewalls

Worldwide is Palo Alto next generation firewall used in the Lebanese University, which

I will discuss through a case study in the following chapter.

# **CHAPTER 3:** **Lebanese University Case Study**

Lebanese university is the only public learning institution in Lebanon it includes 82,000

Individual between employees, instructors and students (lebanese university, n.d.) Every

One of those individuals is in danger of any cyberattack, so the Lebanese university to

Encounter any cyberattack build a cybersecurity topology that we will look at now.

**3.1 Lebanese University infrastructure**

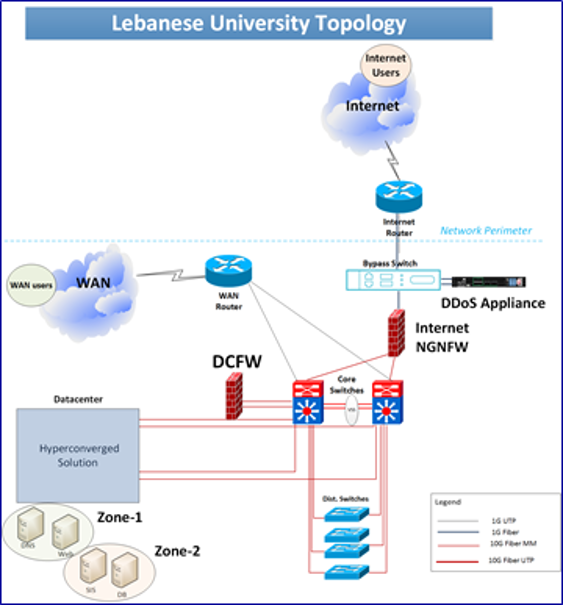


Figure Lebanese University Topology

The Lu network consists of 88 branches on this network there is around 75000 users and

20000 endpoints connected and accepting communication back and forth across the

Network, 2 Internet/WAN providers, 2 High-end Routers, 2 core switches, 2 wlc (wireless

LAN Controller), and 300 AP (Access point).

On the other hand, the CSOC (Cyber Security Operation Center) Technologies for

Protecting The LU network consists of 88 Open source firewalls, 2 next Generation

Firewalls, 1 central EDR (Endpoint Detection and Response), 1 DDOS (Distributed

Denial of Service) Solution, 1 SIEM (Security Information and event management),

One VPN Access Server, 1 LDAP (Lightweight Directory Access Protocol), 1 Email

Filter and at last one web filter (kahlife).

**3.2 Lebanese University NEXT GENERATION Firewall**

As shown in the Lebanese University topology diagram shown above, in addition to the

Huge network that contains thousands of users on a daily basis, there is the Lebanese

University cyber Security Operation Center technologies that we mentioned before.

However, from now on we will focus on one of these important technologies and the

Technology that we have chosen to continue working on is the NGFW.

**3.2.1 Palo Alto Firewall Overview**

Before talking about the firewall I will take few minutes from the reader time to give an

Overview about the founders of this machine that is Palo Alto Networks. It is an American

International Cybersecurity Corporation with its Santa Clara, California headquarters. Its

Key products are a framework that includes sophisticated firewalls and cloud-based

Services that broaden certain firewalls to cover other security aspects. In over 150 nations,

The firm represents over 70,000 organizations. It is the headquarters of the threat analysis

Team of Unit 42 and hosts the conference on Ignite cybersecurity.

The Palo Alto Firewall is a modern approach to network protection, a next-generation

Firewall that allows apps and your company to be safely. Palo Alto provides a real

Firewall breakthrough that allows for unparalleled application enablement, content

Control, not just IP address, by user, at up to 20 Gbps without performance degradation.

The next generation Palo Alto firewall makes applications, regardless of port, protocol

Based on a patent-pending APP-ID technology. Evasive tactics or SSL encryption.

In addition, to scanning content to stop targeted threats and prevent data Leakage.

Therefore, you can safely enable the use of applications, in addition to Maintaining

Complete visibility and control. (palo alto, n.d.)

1. **Policy Type**

A number of policy types that work together to securely allow applications on your network enabled by the Palo Alto Networks next-generation firewall.

|  |  |
| --- | --- |
| Policy Type | Description |
| Security | Determine whether to block or allow a session based on traffic attributes, such as the security zone for the source and destination IP address for the source and destination, application, user, and service. (palo alto, n.d.) |
| NAT | Tell the firewall which packets need translation and how the translation should perform. Both source address and/or port translation and destination address and/or port translation protected by the firewall. (palo alto, n.d.) |
| QOS | Use a given parameter or multiple parameters to classify traffic that needs QOS treatment (either preferential treatment or bandwidth limiting) and assign it a class. (palo alto, n.d.) |
| Policy Based Forwarding | Identify traffic that can use an egress interface that is different from the one usually used based on the routing table. (palo alto, n.d.) |
| Decryption | Identify encrypted traffic for visibility, access, and granular protection that you want to inspect. (palo alto, n.d.) |
| Application Override | Identify sessions that the App-ID engine, which is a Layer-7 inspection, does not want you to process. Traffic matching the override policy of an application causes the firewall at Layer-4 to treat the session as a standard state inspection firewall. (palo alto, n.d.) |
| Authentication | Identify traffic that needs authentication for users. (palo alto, n.d.) |
| DOS Protection | Identify possible denial-of-service (DoS) attacks and in response to rule matches, take defensive measures. (palo alto, n.d.) |

**B-Monitoring logs**

We will mention the logs found in the Palo Alto Next Generation Firewall that are used

For monitoring the network traffic. Every log has a specific functionality that helps the

Firewall to detect any possible cyberattack on our network.

Threat

Threat Logs Show entries when traffic matches one of the firewall security profiles

Attached to the security law. The following information is included in every entry: date

And time. Type a column that describes the threat type, such as "virus" or "spyware."

The threat summary or URL is a name column. Source and destination zones, addresses

And ports, the name of the program, and the name of the security rule applied to the

Flow. And the operation of the alarm (allow or block) and the intensity of the following

Levels (Critical, high, medium, low, informational). Critical is a serious threat that

Results in root compromise of servers, such as those that affect default installations of

Widely distributed applications, and the exploit code is widely accessible to attackers.

High threats that have the potential to become critical but have mitigating factors; they

may be difficult to manipulate, do not lead to high privileges, for example, or may not

have a wide pool of victims. Medium-small threats with minimized effects, low

warning-level threats with very little effect on the infrastructure of an enterprise. They

typically need connections to local or physical networks. Suspicious incidents that do

not pose an immediate threat, but are recorded to call for information attention to deeper

problems (palo alto, n.d.).

Here is a table that contain some of the attacks that we monitored used threat log:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| CONTENT TYPE | TYPE | RULE | SOURCE ZONE | destination | ACTION | URL FILE NAME | CATEGORY |
| vulnerability | THREAT |  | outside | inside | drop |  | any |
| vulnerability | THREAT |  | outside | inside | Reset-both | ul.edu.lb/ | educational-institutions |
| spyware | THREAT | LU-Strict-Out-to-IN-Servers | outside | inside | Reset-both |  | any |
| vulnerability | THREAT |  | outside | inside | drop |  | any |
| spyware | THREAT | LU-Strict-Out-to-IN-Servers | outside | inside | Reset-both |  | any |
| vulnerability | THREAT |  | outside | inside | Reset-both | kerbynet | private-ip-addresses |

URLFiltering

Show URL filter logs that monitor access to websites and whether users can send

website credentials. So you can include which URL categories to block or authorize,

and which credential submissions you want to grant or disable. Alternatively, you can

allow the logging of HTTP URL header options. With URL Filtering allowed, all web

traffic (HTTP and HTTPS) on any port is compared against the URL filtering database

which contains a listing of millions of websites that have been categorized You may use

these categories of URLs as matching criteria to implement security policies and to

securely allow web access and monitor the traffic that your network traverses. You may

also use URL filtering to enforce your users' secure search settings and to avoid

credential phishing(Credential phishing attacks typically impersonate a known brand.

The email will usually contain a connection to a URL that will catch the victim's URL-

based credentials).

What is a PAN-DB ?

PAN-DB: The url filtering cloud database that categorizes site-based websites

Information, characteristics, and safety. A URL can have up to four categories,

including risk categories (high, medium and low), indicating how likely it is that the

web will expose you to attacks, a new version is released every 5 to 10 minutes, so

every time a request is sent to the cloud by the palo alto network firewall, it checks the

latest version number , It updates the system version to the current version if it is

different. As Pan db categorizes firewall sites that can exploit that information in real-

time to implement security policies with url filtering activated.

How url filtering works ?

The firewall checks pan-db for the category of sites and saves it when a user accesses a

url that is not cached(Caching is a tool that stores a copy of a given resource and serves

it back when requested). Since new entries are saved by the firewall, it clears urls that

users have not accessed recently. It also looks for important changes when the firewall

checks pan db for a url, such as urls that previously qualified as benign but are now

malicious.Every 30 minutes ,the firewall checks pan-db for such updates.

Example from test a site to see how PAN-Db categorizes a URL:

* **URL**: https://gestion1.ul.edu.lb/
* **Category**: Educational Institutions
* **Description**: Official websites for schools, colleges, universities, school districts, online classes, and other academic institutions
* **Example Sites**: www.ucla.edu, www.phoenix.edu, www.sfusd.edu
* **Category**: Low Risk
* **Description**: Sites that are not medium or high risk considered as low risk. These sites have displayed benign activity for a minimum of 90 days. The low risk category includes both sites that have a history of only benign activity, and sites found to be malicious in the past, but that have displayed benign activity for at least 90 days.

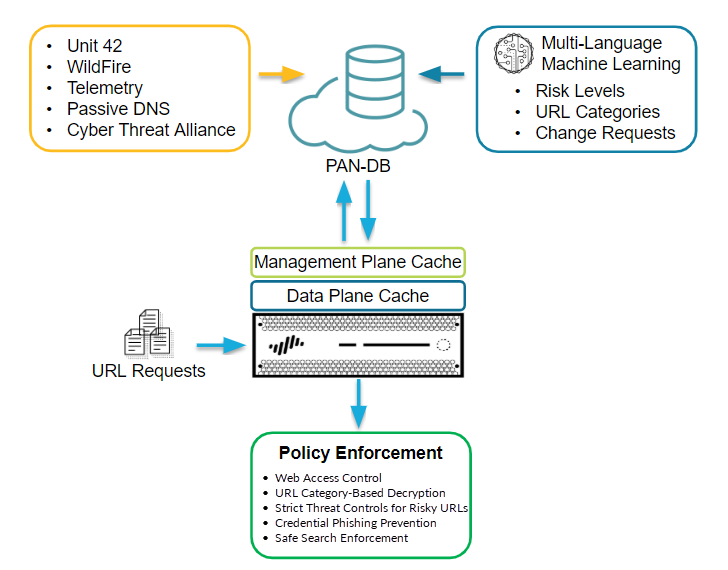


Figure how URL filtering works (palo alto, n.d.)

More URLs are kept in the management plane and it interacts directly with PAN-DB. If

the firewall is unable to locate the category of a URL in the cache and conducts a PAN-

DB lookup, the retrieved category information in the management plane is cached. The

management plane transmits the data to the data plane, which often caches it and uses it

for policy enforcement.

The dataplane holds fewer URLs and receives information from the management plane.

After the firewall checks URL category exception lists and custom URL categories for a

URL, the next place it looks in is the dataplane. Only if the firewall cannot find the URL

categorized in the dataplane it checks the management plane and, if the category

information is not there, then PAN-DB (palo alto, n.d.) .

Here is a table that contain some of the attacks that we monitored used threat log:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| CONTENT  TYPE | TYPE | RULE | SOURCE ZONE | destination | ACTION | URL FILE NAME | Category |
| URL | THREAT | Allow WhatsApp TCP ports outbound-1 | inside | outside | Block-URL | app.  Openo  bjstack.  com/  static  /js/3034  /a.js | malware |
| URL | THREAT | Allow WhatsApp TCP ports outbound-1 | inside | outside | Block-URL | cdn.  special-offers.  online/ | grayware |
| URL | THREAT | Allow WhatsApp TCP ports outbound-1 | inside | outside | Block-URL | cp.esb7  cg54  .ru/diff.  php | command  and  control |
| URL | THREAT | Allow WhatsApp TCP ports outbound-1 | inside | outside | Block-URL | differe  ntia.  ru/  diff.php | malware |
| URL | THREAT | Allow WhatsApp TCP ports outbound-1 | inside | outside | Block-URL | bdcrqgo  nzmwu  ehky  .nl/in.php | command-and-control |
| URL | THREAT | Allow WhatsApp TCP ports | inside | outside | Block-URL | atomictri  vi  a.ru/atomi | malware |

WildFire Submissions

When a firewall in Palo Alto Networks detects an unknown sample (a file or a link),

Included in an email), the firewall will forward the Wildfire study sample automatically.

The sample reveals when evaluated and executed in the Wildfire sandbox based on the

properties, actions, and activities (sandbox is an isolated environment on a network that

mimics end-user operating environments. Sandboxes are used to execute suspicious

code securely without causing damage to the host computer or network), the sample to

be decided by Wildfire (benign, malware, Grayware, or phishing). Samples categorized

as malicious can pose a threat to security. Viruses, worms, Trojans, Remote Access

Tools (RATs), rootkits, and botnets can contain malware . The WildFire cloud produces

and distributes a signature for samples that are known as malware to prevent future

disclosure, the phishing verdict indicates that the site to which the connection directs

users displayed credential phishing activity, whereas the files classified as grayware do

not pose a direct security danger, but may otherwise show obtrusive behavior like adwa

For newly-discovered malware, WildFire produces a signature to detect the malware

and distributes it to all firewalls with active WildFire subscription within minutes. This

allows the detection and prevention of malware detected by a single firewall for all Palo

Alto next-generation firewalls worldwide. Malware signatures frequently coincide with

many versions of the same malware family and block new variants of malware that the

firewall has never seen before. The threat research team of Palo Alto Networks uses the

threat information obtained from malware variants to block malicious IP addresses,

domains, and URLs (palo alto, n.d.)

Here is a table that represent some suspecious attack we monitored using wildfire log:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Content type | TYPE | Rule | Source  zone | destination | action | URL FILE NAME | category |
| wildfire | threat | Allow WhatsApp TCP ports outbound-1 | inside | outside | allow | Your File Is Ready To Download.  apk | malicious |
| wildfire | threat | Allow WhatsApp TCP ports outbound-1 | inside | outside | allow | ZoodMall.  apk | malicious |
| wildfire | threat | Allow WhatsApp TCP ports outbound-1 | inside | outside | allow | Download [3isk TV] مسلسل علي رضا الحلقة متر | malicious |
| wildfire | threat | Allow WhatsApp TCP ports outbound-1 | inside | outside | allow | woo.js | malicious |
| wildfire | threat | allow WhatsApp TCP ports outbound-1 | inside | outside | allow | com-  android-vending-billing-inappbillingservice-crac-1495-36803 | malicious |

Tunnel Inspection

Anywhere on the network where you do not have the opportunity to terminate the tunnel

first the Palo alto firewall will inspect the tunnel material. As long as the firewall is in

the GRE's direction (Generic Routing Encapsulation is a tunneling protocol developed

by Cisco Systems that can encapsulate a wide variety of network layer protocols inside

virtual point-to-point links or point-to-multipoint links over an Internet Protocol

network), IPSec is not encrypted (Ipsec stands for internet protocol and a group is

secure). Protocols used together to set up encrypted communications between devices),

GTP-U (it encapsulates and routes user plane traffic through several signaling

interfaces. GTP-U messages are either user plane or signaling messages) or VXLAN

tunnel (a VXLAN tunnel is set up between certain devices when devices interact inside

a Software Specified Datacenter. In both physical and virtual switches, such tunnels can

be set up), the firewall can inspect the content of the tunnel. Tunnel inspection logs are

like tunnel session traffic logs; they show an entry for the beginning and end of each

tunnel session inspected. The firewall saves only the internal flows in traffic logs to

avoid double counting, and sends tunnel sessions to tunnel inspection logs. The tunnel

inspection log entries include Receive Time (date and time the log was received), the

tunnel ID, monitor tag, session ID, the Security rule applied to the tunnel session,

number of bytes in the session, parent session ID (session ID for the tunnel session),

source address, source user and source zone, destination address, destination user, and

destination zone (palo alto, n.d.) .

**3.2.2 LU Palo-Alto**

1. **Existing Security Policy**

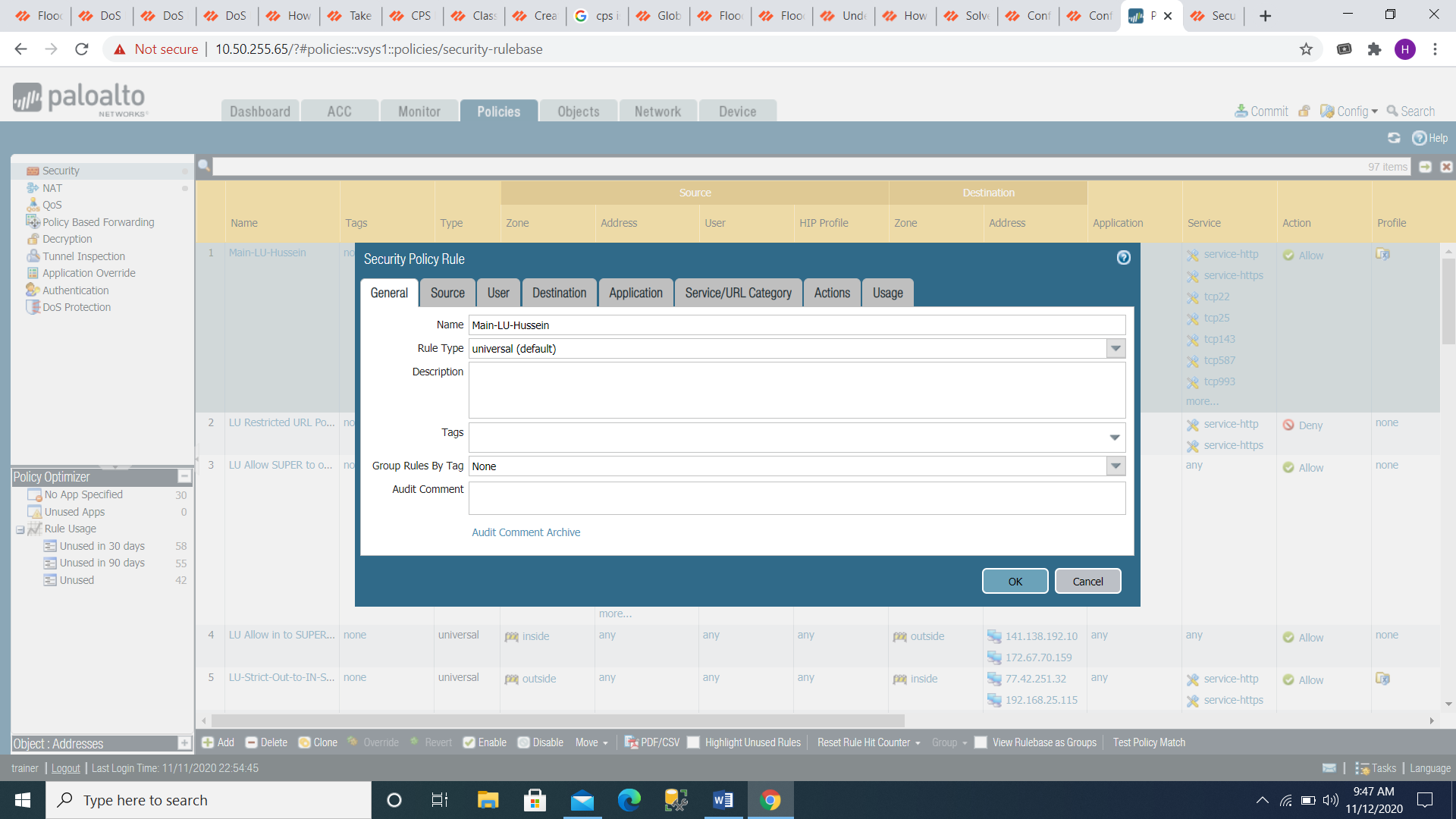


Figure Security Policy Rule General

Rule Type: Universal (Applies the law to all interzone and intrazone traffic matching in

The source and destination zones that have listed.)

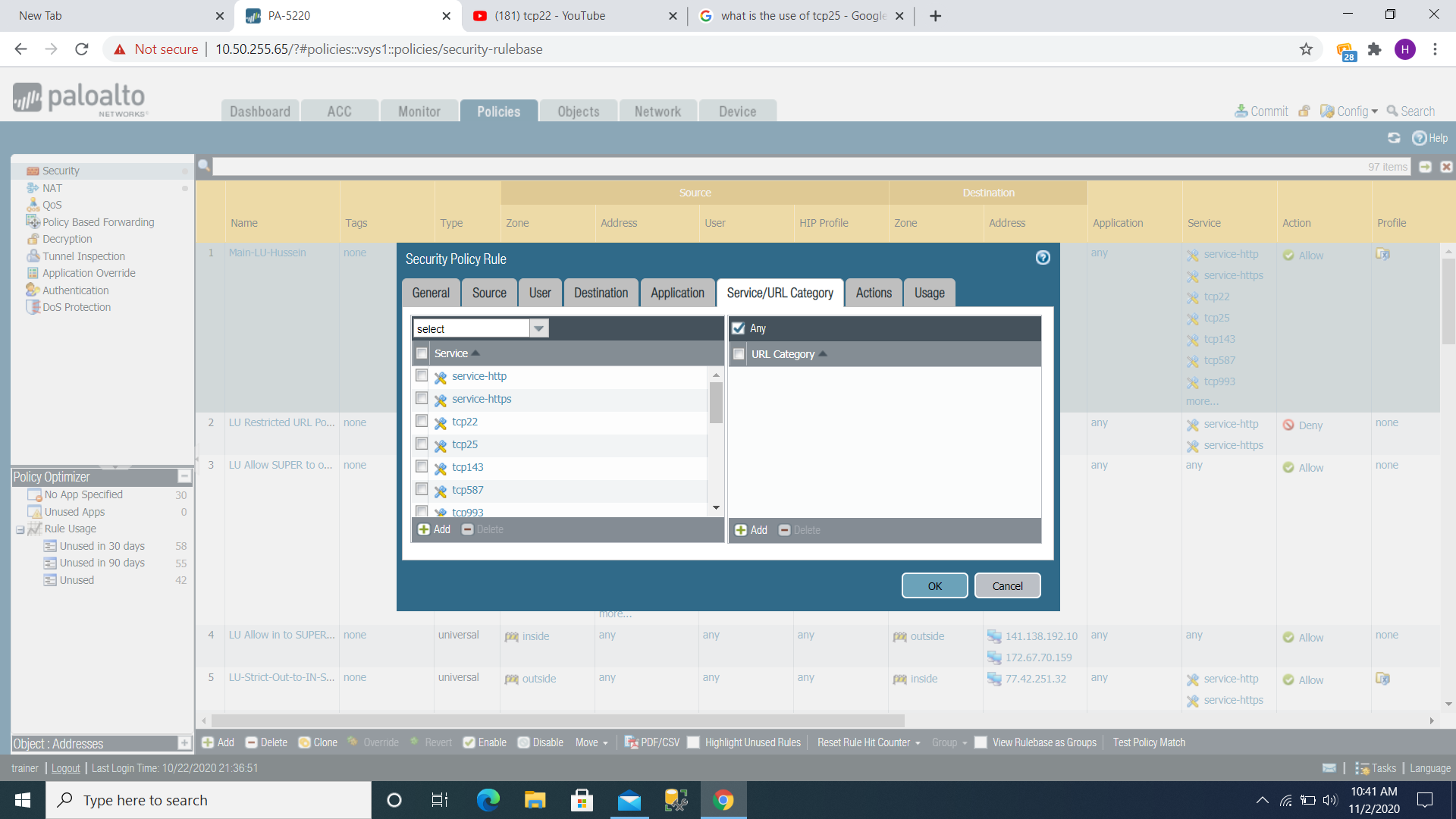


Figure Security Policy Rule Service

***Service allow you to select a Layer 4 (TCP or UDP) port for the application***

Service-http: The Application Server portion is the one that provides facilities for

Deployment of Web applications and usability of deployed Web applications by HTTP clients (wikins, 2012)

Service-https: Data encryption between a client and a server that protects data

Against eavesdropping, information forging, and data tampering. (wikins, 2012)

Tcp22: A software standard to support encrypted data transfer is Secure Shell (SSH).

Between the two PCs, secure logins, file transfers (SCP (Secure, Contain and

Protect), sftp (popular method for securely transferring files over remote systems)) and

Port forwarding. (wikins, 2012)

Tcp25: Used between mail servers and end users to move mail from source to destination to send email to a mail system. (wikins, 2012)

Tcp143: Internet Message Control Protocol (IMAP) is a protocol for mail that used to

Access messages Accessing email on a remote web server from a local client. ... Port

143 – This is the Default IMAP non-encrypted port. (wikins, 2012)

Tcp587: Is the port of mail submission. Where there is an email client or outgoing

Server it should always sent by an email to get route through a proper mail server,

Using SMTP (Simple Mail Transfer Protocol is a set of communication protocols)

Guidelines that permit the transmission of electronic mail over the Internet through

Software) the default port is port 587. (wikins, 2012)

Tcp993: The port you need to use if you want securely communicate with IMAP

(Emails that synchronized between your device and the email server. In addition, to

Sort your messages; you can create your own folders on the server. By using IMAP, you

Can also easily access this folder with Outlook or a smartphone (iPhone/Android/etc.). (wikins, 2012)

Tcp995: This is the port you need if you want to connect securely using POP3 (Post

Office Protocol version 3) (POP3) is a mail protocol used by a local email client to

Receive mail from a remote server. POP3 can copy the mail to the local mail client from

The remote server. Mail is optionally removed after uploading from the server, which

Saves space on the server. (wikins, 2012)

Tcp2082: Default on CPanel. CPanel is a control panel for internet hosting (The

Software offers a graphical interface (GUI) and automation tools designed to simplify

The process of hosting a website to the "end user" website owner, enabling the

Management of a web-hosting server built by CPanel and American Corporate. (wikins, 2012)

Tcp2083: The default SSL (Secure Sockets Layer) cPanel is a cryptographic protocol.

Built to provide the protection of communication over a computer network). (wikins, 2012)

Tcp2401: A revision access control CVS (also known as the Concurrent Versioning System). (wikins, 2012)

Tcp3389: Remote Desktop Protocol Developed by Microsoft Terminal Server (RDP)

Officially registered as a Windows based terminal (Microsoft, which provides a user

With a graphical interface to connect to another device over a network connection)

(WBT). (wikins, 2012)

Tcp5004: Real-time Transport Protocol (RTP) is a protocol used by the network to

Deliver over IP networks, audio and video. (wikins, 2012)

Tcp8080 HTTP alternative port, Apache Tomcat (provides pure HTTP web java)

Jira (a proprietary problem tracking product developed by Atlassian that enables bug

Tracking and agile project management), is a server environment in which Java code

Can run. (wikins, 2012)

Tcp8082: Us-cli CLI is a command line program that accepts text entries for execution.

Functions of operating system. (wikins, 2012)

Tcp8443: Apache Tomcat (provides a pure web server environment for java HTTP in

Which Java code will run), iCal over SSL (is a private calendar created by apple). (wikins, 2012)

Tcp9000: SonarQube Web Server is an open source framework built for continuous

Code quality inspection for automated evaluation with static code review to identify

Glitches, code smells, and security vulnerabilities in 20+ programming languages).

DBGp (is a simple protocol, for use with language tools and engines for the purpose of

Debugging applications), Hadoop (is a series of software utilities from open source that

Facilitates the use of a network of several computers (PHP default port) to solve

Problems involving large quantities of data and computation. (wikins, 2012)

Tcpftp: Two TCP connections for communication used by FTP as a file transfer

Protocol. One to transfer control information and not used for port 21 file sending, only

Control information. Furthermore, the other is a data link on port 20 to send the data

Files between the client and the server. (wikins, 2012)

Udp53: DNS (a domain name system that names computers, utilities, or other Internet-

Connected or private network resources). (wikins, 2012)

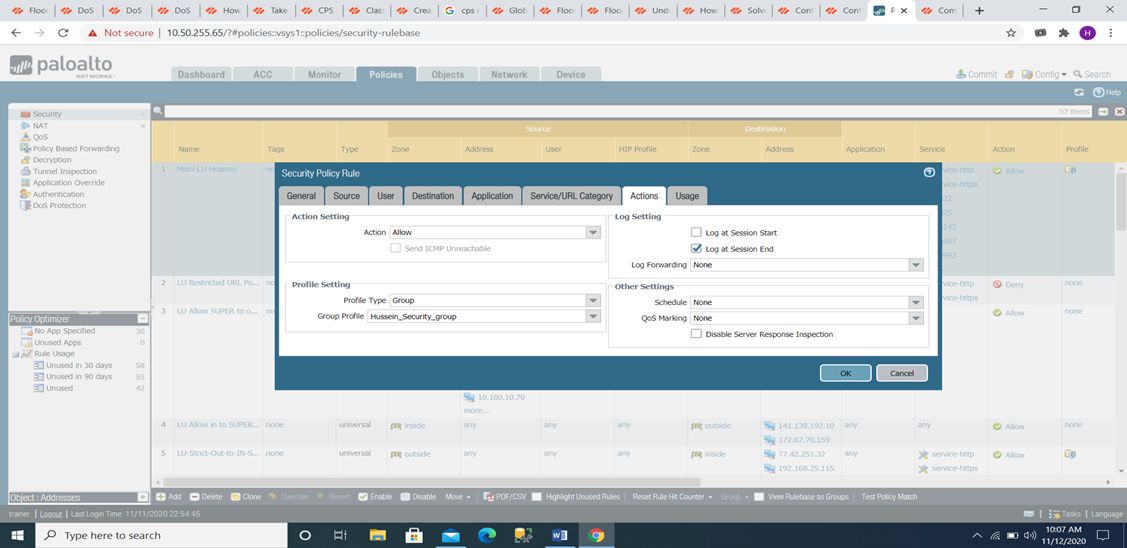


Figure Security Policy Rule Actions

In addition to the mentioned ports this policy contain a group profile that was named

Here Hussein\_Security\_Group, this group profile contains number of objects each

Object has a specific task to make the policy more efficient the used objects in our

Policy are URL Filtering,DOS Protection, and File BLOCKING we will talk about

Every objective we have mentioned now starting by URL Filtering.

**A-Existing URL Filtering Policy object**

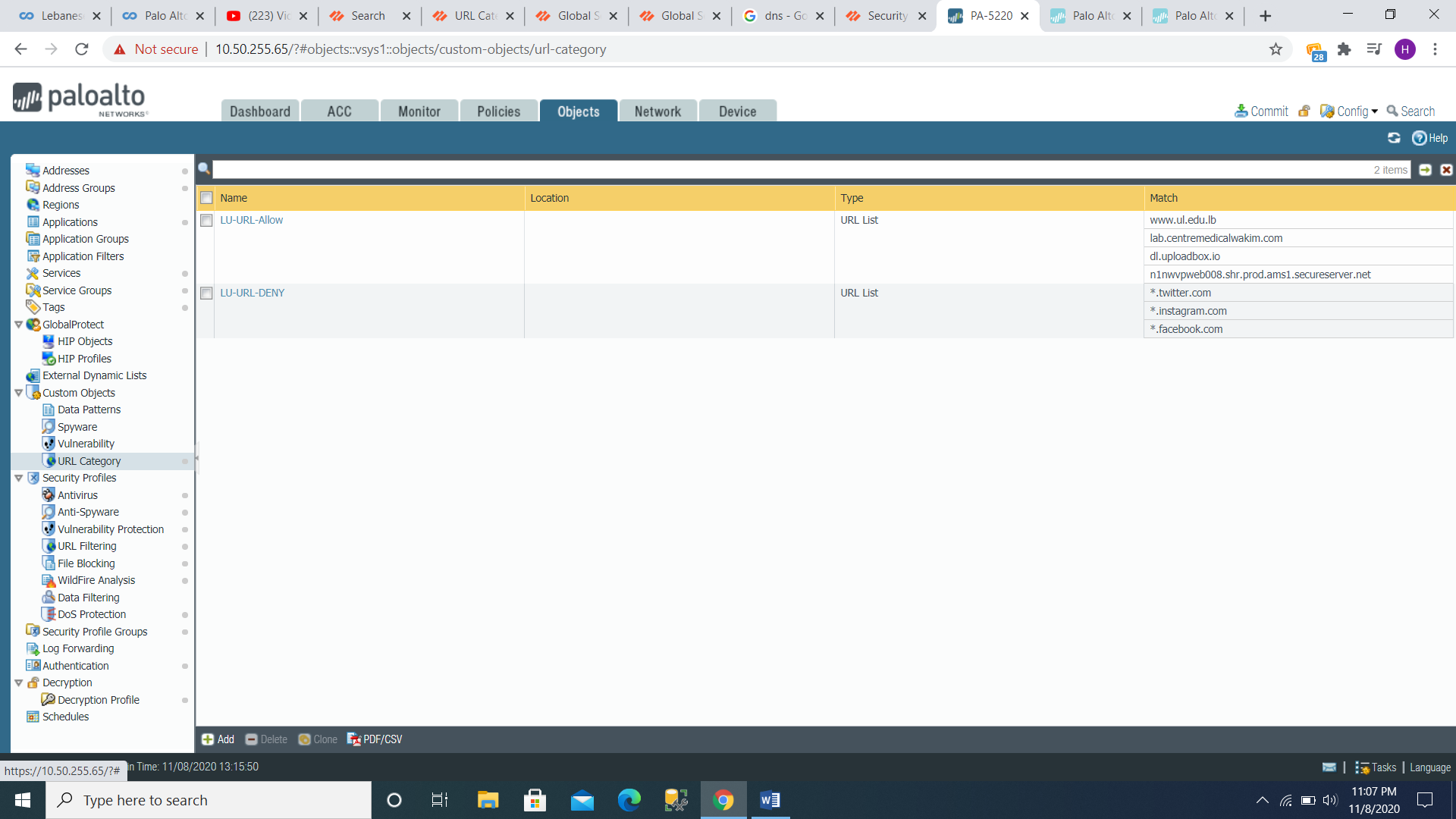


Figure URL Category

Custom URL Categories:

LU-URL-Allow:

1. [www.ul.edu.lb](http://www.ul.edu.lb)
2. lab.centremedicalwakim.com
3. dl.uploadbox.io
4. n1nwvpweb008.shr.prod.ams1.secureserver.net

LU-URL-DENY:

1. \*.twitter.com
2. \*.instagram.com
3. \*.facebook.com

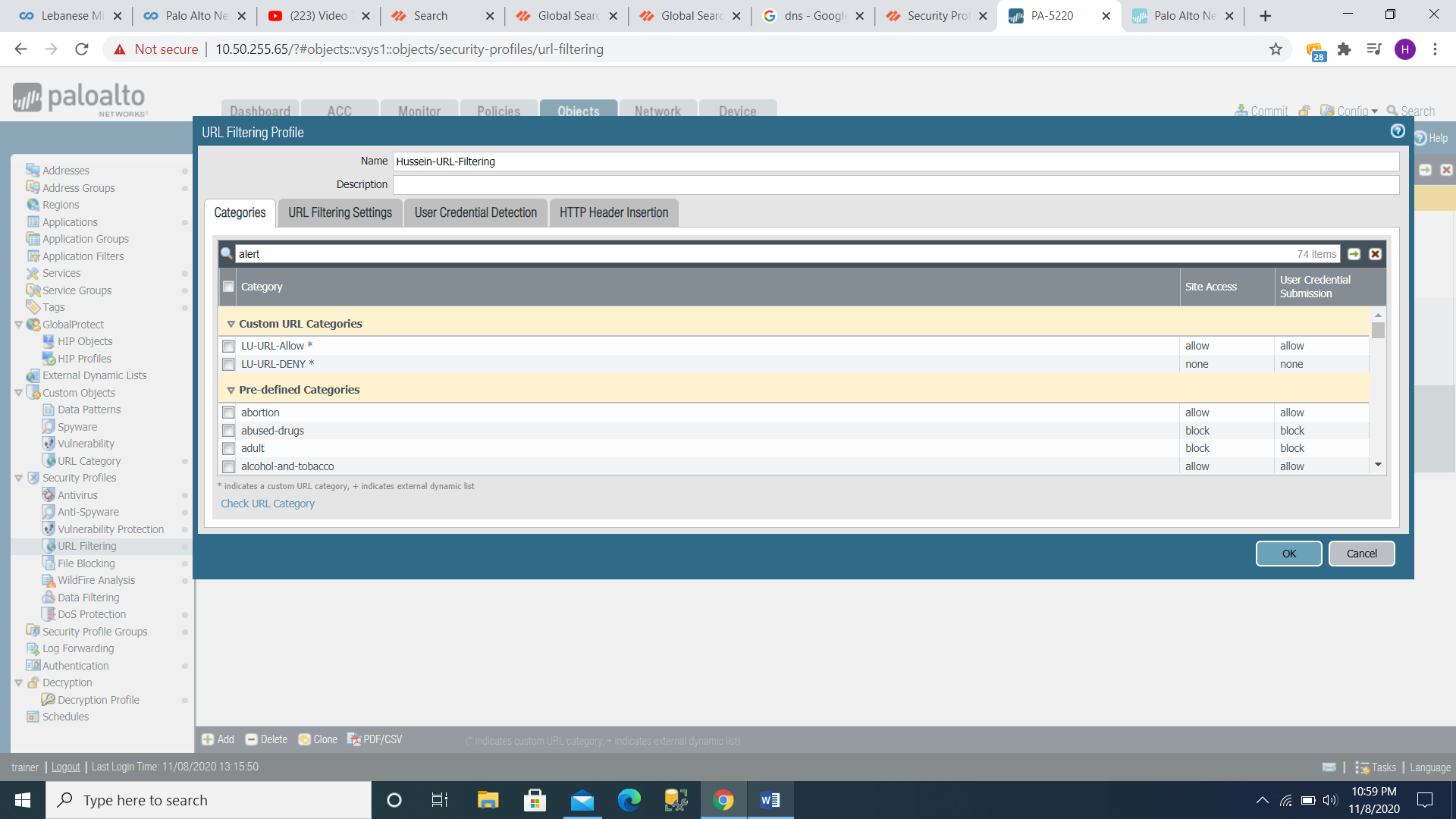


Figure URL Filtering Profile

LU-URL-Allow: this category action is set to allow accessing the previously mentioned

Sites also to submit user credentials.

LU-URL-DENY: this category action is set to none on both site access and user

Credentials submission. None (custom URL category only) the action none allow the

Firewall to inherit the assignment of the URL filter group from the vendor URL

Database. (The PAN category list).

Pre-defined categories:

1. Abortion: this category action is set to allow both site access and user credentials submission.
2. Abused drugs: this category action is set to block both site access and user credentials submission.
3. Adult: this category action is set to block both site access and user credentials submission.
4. Alcohol-and-tobacco: this category action is set to allow both site access and user credentials submission.
5. Auctions: this category action is set to allow both site access and user credentials submission.
6. Business-and-Economy: this category action is set to allow both site access and user credentials submission
7. Command-and-Control: this category action is set to block both site access and user credentials submission.
8. Computer-and- internet-info: this category action is set to allow both site access and user credentials submission.
9. Content-delivery-Networks: this category action is set to allow both site access and user credentials submission.
10. Copyright-infringement: this category action is set to allow both site access and user credentials submission.
11. Cryptocurrency: this category is set to alert site access and allow user credential submission
12. Dating: this category is set to allow both site access and user credential submission.
13. Dynamic-dns: this category action is set to allow both site access and user credentials submission.
14. Educational-institutions: this category is set to allow both site access and user credential submission.
15. Entertainments-and-arts: this category is set to allow both site access and user credential submission.
16. Extremism: this category action is set to allow both site access and user credentials submission.
17. Financial-services: this category is set to allow both site access and user credential submission.
18. Gambling: this category is set to block both site access and user credential submission.
19. Games: this category is set to allow both site access and user credential submission.
20. Government: this category is set to allow both site access and user credential submission.
21. Grayware: this category is set to block both site access and user credential submission.
22. Hacking: this category is set to block both site access and user credential submission.
23. Health-and-medicine: this category is set to allow both site access and user credential submission.
24. High-risk: this category is set to alert site access and allow user credential submission.
25. Home-and-garden: this category is set to allow both site access and user credential submission.
26. Hunting-and-fishing: this category is set to allow both site access and user credential submission.
27. Insufficient-content: this category is set to allow both site access and user credential submission.
28. Internet-communication-and-telephony: this category is set to allow both site access and user credential submission
29. Internet-portals: this category is set to allow both site access and user credential submission.
30. Job-search: this category is set to allow both site access and user credential submission.
31. Legal: this category is set to allow both site access and user credential submission.
32. Low-risk: this category is set to allow both site access and user credential submission.
33. Malware: this category action is set to block both site access and user credentials submission.
34. Medium-risk: this category is set to allow both site access and user credential submission.
35. Military: this category is set to allow both site access and user credential submission.
36. Motor vehicles: this category is set to allow both site access and user credential submission.
37. Music: this category is set to allow both site access and user credential submission.
38. Newly registered domain: this category action is set to alert site access and allow user credential submission.
39. News: this category is set to allow both site access and user credential submission.
40. Not resolved: this category is set to allow both site access and user credential submission.
41. Nudity: this category is set to allow both site access and user credential submission.
42. Online-storage-and backup: this category is set to allow both site access and user credential submission.
43. Parked: this category action is set to allow both site access and user credentials submission.
44. Peer to peer: this category action is set to allow both site access and user credentials submission.
45. Personal-sites-and-blogs: this category action is set to allow both site access and user credentials submission.
46. Philosophy-and-political-advocacy: this category action is set to allow both site access and user credentials submission.
47. Phishing: this category action is set to block both site access and user credentials submission.
48. Private-ip-addresses: this category action is set to allow both site access and user credentials submission.
49. Proxy\_avoidance\_and\_anonymizers: this category action is set to allow both site access and user credentials submission.
50. Questionable: this category action is set to block both site access and user credentials submission.
51. Real estate: this category action is set to allow both site access and user credentials submission.
52. Recreation-and-hobbies: this category action is set to allow both site access and user credentials submission.
53. Reference-and-research: this category action is set to allow both site access and user credentials submission.
54. Religion: this category action is set to allow both site access and user credentials submission.
55. Search-engines: this category action is set to allow both site access and user credentials submission.
56. Sex-education: this category action is set to allow both site access and user credentials submission.
57. Shareware-and-freeware: this category action is set to allow both site access and user credentials submission.
58. Shopping: this category action is set to allow both site access and user credentials submission.
59. Social networking: this category action is set to allow both site access and user credentials submission.
60. Society: this category action is set to allow both site access and user credentials submission.
61. Sports: this category action is set to allow both site access and user credentials submission.
62. Stock-advice-and-tools: this category action is set to allow both site access and user credentials submission.
63. Streaming-media: this category action is set to allow both site access and user credentials submission.
64. Swimsuits-and intimate-apparel: this category action is set to allow both site access and user credentials submission.
65. Training-and-tools: this category action is set to allow both site access and user credentials submission.
66. Translation: this category action is set to allow both site access and user credentials submission.
67. Travel: this category action is set to allow both site access and user credentials submission.
68. Unknown: this category action is set to allow both site access and user credentials submission.
69. Weapons: this category action is set to block both site access and user credentials submission.
70. Web-advertisements: this category action is set to allow both site access and user credentials submission.
71. Web-based-email: this category action is set to allow both site access and user credentials submission.
72. Web hosting: this category action is set to allow both site access and user credentials submission.

**Existing DOS Protection Policy Object:**

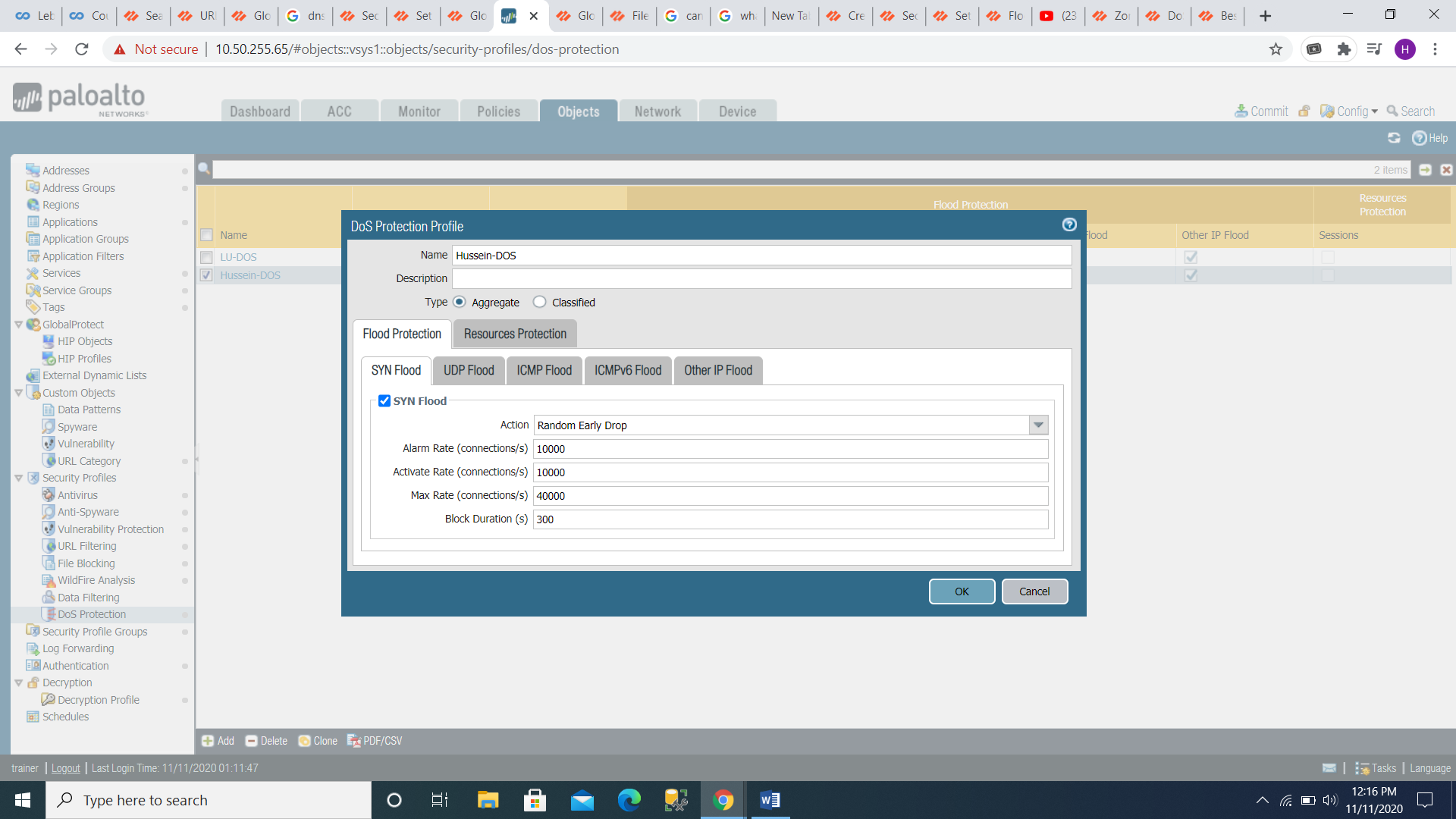


Figure DOS Protection Profile

In a denial-of-service (DoS) attack an attacker attempts to block access to information

Or resources by legitimate users. The intruder may be able to prevent you from

Accessing emails, websites, online accounts (online banking, etc.) or other services that

Depend on the affected device by targeting your computer, servers, routers, network

Connections, or the computers and networks of the sites you are trying to use..

When an attacker "floods" a network with data, the most common and obvious form

Of DoS attack occurs. When you type a URL in your browser for a specific website, you

Send a request to the computer server of that website to view the page. The server

Can only handle a certain amount of requests at once, so if the server is overwhelm

With requests from an attacker, the request cannot processed. This is a "denial of

Service" since you are unable to access the site. (palo alto, n.d.)

DoS Protection profiles set thresholds for protection against IP flood attacks from new

Sessions and provide resource protection (maximum concurrent session limits for

Specified Endpoints and resources). DoS protection profiles protect against

SYN (tcp), UDP, ICMP, ICMPv6 and other IP flood attacks by specific devices (classified

Profiles) and groups of devices (aggregate profiles).

Type: Aggregate (since we are trying to protect a group of servers in a destination zone

Such as a group of web servers, aggregate profiles apply limits aggregately through all

Connections matched by the corresponding dos protection policy rule to which the

Profile is attached accurate profile rate limits applied before classified rate limits).

**SYN FLOOD (TCP)**

Action: Random Early Drop (This operation causes SYN packets to drop to prevent a

Flood attack such that an alarm created when the flow reaches the warning rate

Threshold. Additionally, when the flow exceeds the active rate threshold, the firewall

Randomly drops individual SYN packets to limit the flow. In addition, when the flow

Exceeds the maximum rate threshold, 100% of incoming SYN packets are dropped to

Limit the flow.

Alarm Rate: 10000

Activate Rate: 10000

Max Rate: 40000

Block Duration: 300

**UDP FLOOD**

Alarm Rate: 10000

Activate Rate: 10000

Max Rate: 40000

Block Duration: 300

**ICMP FLOOD**

Alarm Rate: 10000

Activate Rate: 10000

Max Rate: 40000

Block Duration: 300

**Other IP FLOOD**

Alarm Rate: 10000

Activate Rate: 10000

Max Rate: 40000

Block Duration: 300

**Existing File Blocking Policy Object**

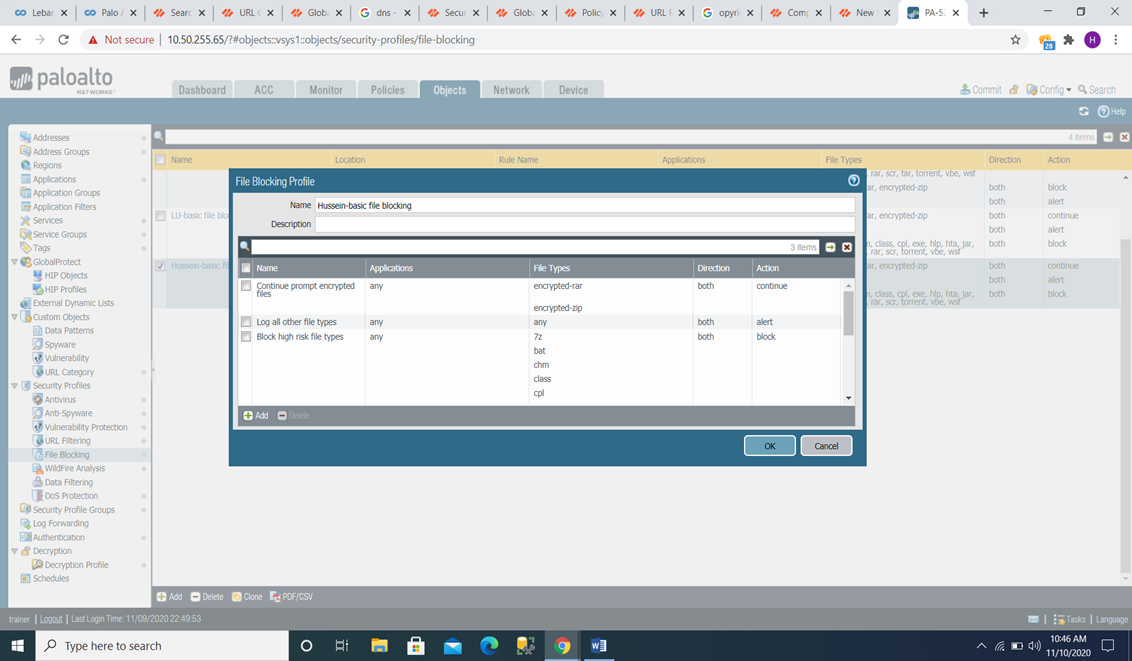
****

Figure File Blocking Profile

The firewall uses file blocking profiles to block specified file types over specific

Applications and in the flow direction of the session defined (inbound/outbound/both).

You can set the upload and/or download profile to warn or block, and you can decide

Which applications are subject to file blocking here are the Lebanese university

1. **Continue prompt encrypted files:**

Applications: any

File Types: Encrypted-rar (Encrypted RAR File)

Encrypted-zip (Encrypted ZIP)

Direction: both

Action: continue

1. **Log all other file types**:

Application: any

File Types: any

Direction: both

Action: alert

1. **Block high risk file types**:

Application: any

File Types: 7z (7z File Detected)

Bat (Windows batch)

Chm (CHM File)

Class (Java class file)

Cpl (CPL file)

Exe (Windows Executable)

Hlp (Windows Help File)

Hta (HTML Application)

Jar (JAR File)

Ocx (ActiveX CAB File)

Pe (Microsoft PE File)

Pif (Windows Program Information File)

Rar (RAR)

Scr (Windows Screen Saver SCR File)

Torrent (Torrent File)

Vbe (VBScript Encoded

Wsf (Windows Script)

Direction: bot

Action: Block

**Chapter4: Enhancement to exiting LU policy**

After mentioning the existing policies in the LU Next Generation Firewall In this

Chapter, we will recommend some enhancement to the mentioned Policies before.

**4.1 URL filtering Policy Object enhancement**

To enhance the url filtering policy we monitored the Lebanese university network

Against any threat figure 11 represents 6 hours of network monitoring.

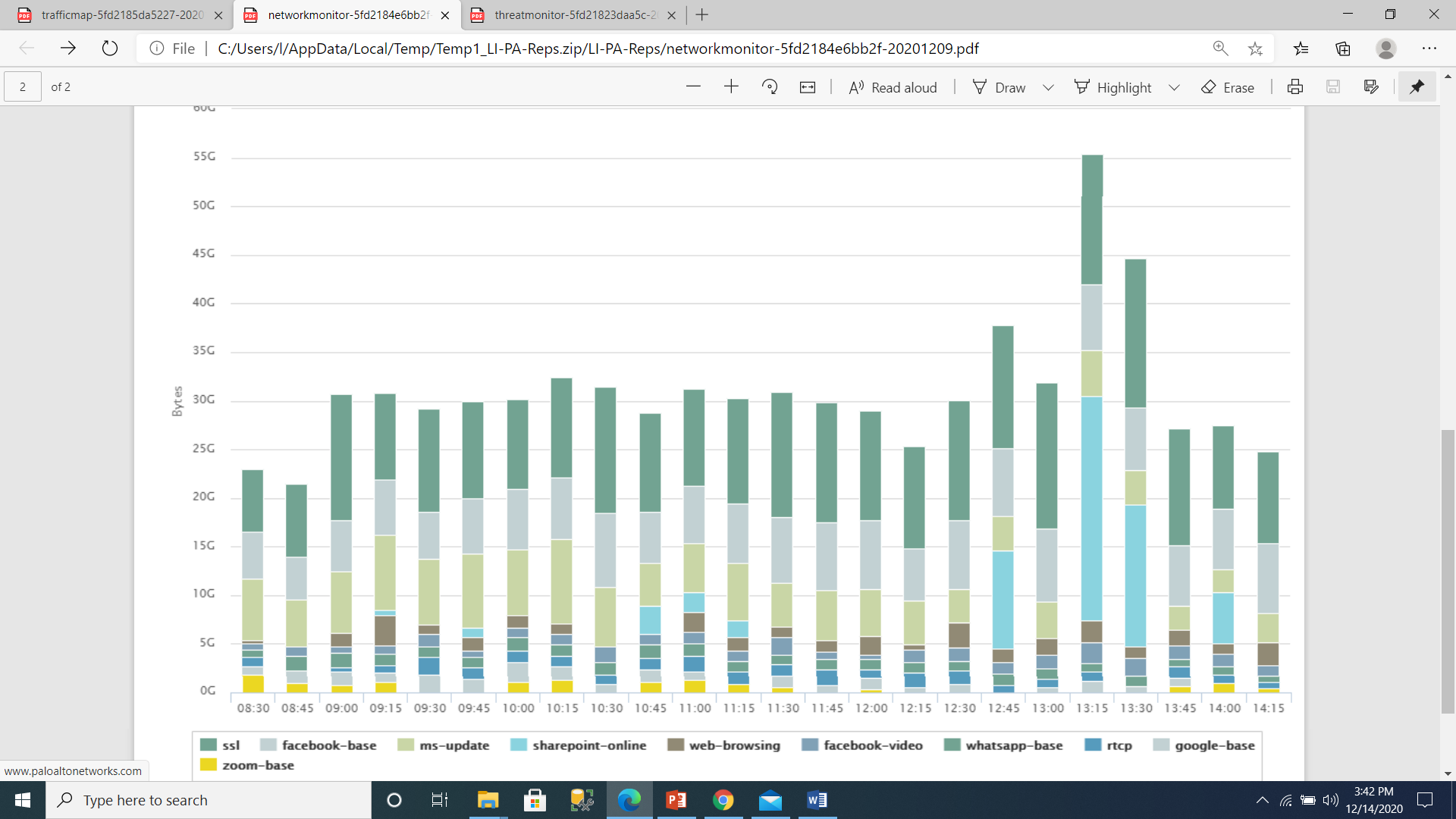


Figure network monitor report

Figure 12 represents threats that we have monitored in the Lebanese university for 6

Hours.

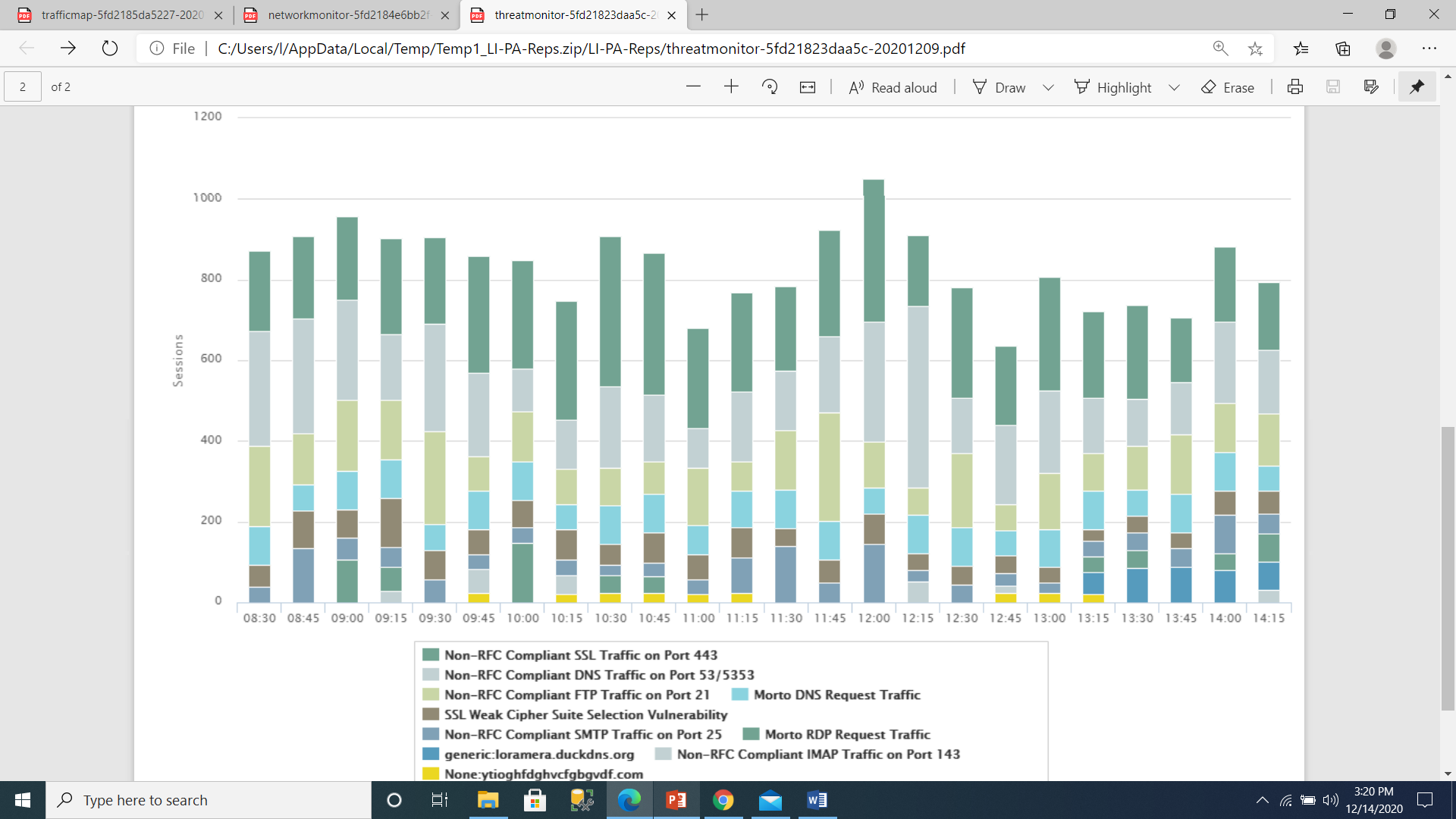


Figure threat monitor report

After studying the network and the threats that it counters we made a conclusion of the

Unneeded categories that could cause a variability for our network that cybercriminals

Can use against us so we made the following enhancement.

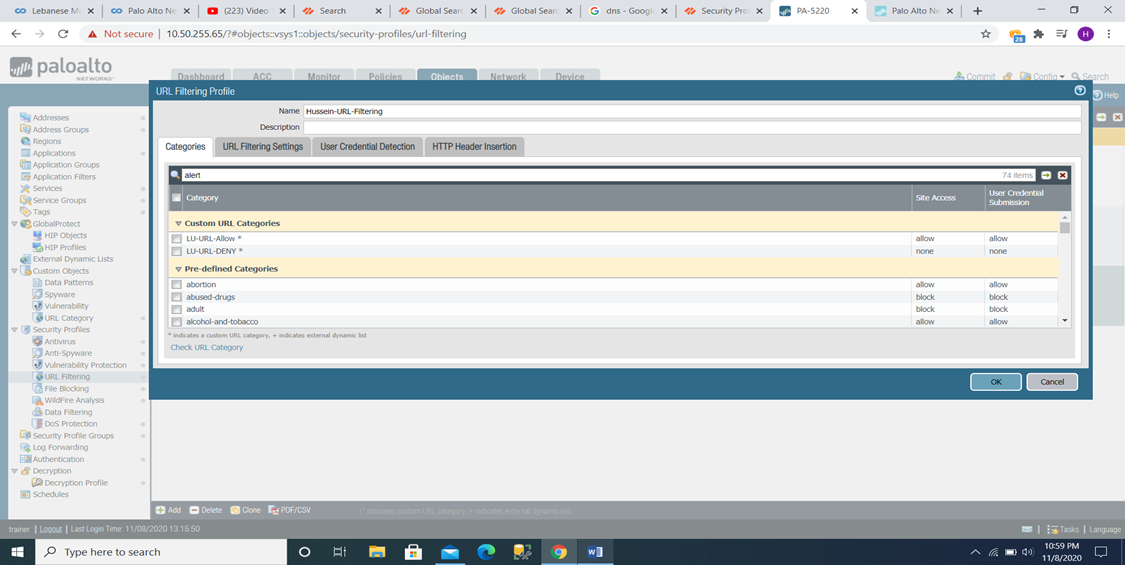


Figure URL Filtering profile with enhancement

1. Abortion: this category action is set to allow both site access and user credentials submission.

Recommendation: This category consist of sites that contain Facts or organizations in

Favor of or against abortion, information on abortion procedures, assistance or advocacy

Platforms for or against abortion, or websites offering information on the

Consequences/effects of or not pursuing an abortion (palo alto, n.d.).

The Recommended policy Action of this category is to block both site access and user

Credential submission.

1. Alcohol-and-tobacco: this category action is set to allow both site access and user credentials submission.

Recommendation: this category consist of sites related the selling, production or use of

Alcohol and/or tobacco products and associated equipment. (palo alto, n.d.)

The recommended Policy action of this category is to block both site access and user

Credential Submission.

1. Copyright-infringement: this category action is set to allow both site access and user credentials submission.

Recommendation: copyright-infringement category contain online sites and websites

Devoted to unlawfully selling images, movies or other downloadable media

Infringement of the copyrights of others. (palo alto, n.d.)

The recommended policy action of this category is to block both site access and user

Credential submission.

1. Cryptocurrency: this category is set to alert site access and allow user credential submission

Recommendation: cryptocurrency category contain websites that promotes crypto

Currencies, exchanges and vendors, this category does not include traditional

Financial services websites that reference crypto currencies, website, that describe

How crypto currencies and block chains work, or websites, that contain embedded

Crypto, currency miners (Grayware). (palo alto, n.d.)

The recommended policy action of this Category is to block both site access and user

Credential submission.

1. Dating: this category is set to allow both site access and user credential submission.

Recommendation: dating category contain Websites that provide dating services online,

Advice and other personal advertising. (palo alto, n.d.)

The recommended policy action of this category is to block both site access and user

Credential submission.

1. Dynamic-dns: this category action is set to allow both site access and user credentials submission.

Recommendation: Intruders for command-and-control communication and other

Malicious purposes also use Dynamic DNS. (palo alto, n.d.)

The recommended policy Action of this category is to block both site access and user

Credential submission.

1. Extremism: this category action is set to allow both site access and user credentials submission.

Recommendation: Extremism category contain Websites that advocate terrorism,

Racism, fascism or other extreme views that discriminate against individuals or groups

Of different ethnic backgrounds, religions or other beliefs. (palo alto, n.d.)

The recommended policy Action of this category is to block both site access and user

Credential submission.

1. Games: this category is set to allow both site access and user credential submission.

Recommendation: Games category contain Sites that include video and computer games

For online play or download, game reviews, tips or cheats, as well as instructional sites

Or non-electronic games, board game sales/trade, or related publications/media. (palo alto, n.d.)

The Recommended policy action of this category is to block both Site access and user

Credential submission.

1. High-risk: this category is set to alert site access and allow user credential submission.

Recommendation: This category contain sites that is Malware, phishing, or C2 sites that

Have shown only benign activity for at least 30 days been previously verified as

Malware, also unknown domains identified as high-risk before PAN-DB completes site

Inspection and categorization sites that are associated with confirmed malicious

Sites. (palo alto, n.d.)

The recommended policy action of this category is to block both site Access and user

Credential submission.

1. Hunting-and-fishing: this category is set to allow both site access and user credential submission.

Recommendation: this category contains sites of Hunting and fishing tips, directions,

Sales and paraphernalia of associated equipment. (palo alto, n.d.)

The recommended policy Action of this category is to block both site access and user

Credential submission.

1. Insufficient-content: this category is set to allow both site access and user credential submission.

Recommendation: this category contains Websites and services which show test pages,

No contents, provide API access that is not intended for display by the end user or

Requires Authentication without having to show any other content suggesting a

Different Categorization. (palo alto, n.d.)

The recommended policy action of this category is to block both site Access and user

Credential submission.

1. Medium-risk: this category is set to allow both site access and user credential submission.

Recommendation: This category contain sites that is previously confirmed to be

Malware, phishing, or C2 sites that have displayed only benign activity for at least 60

Days, unknown IP addresses categorized as medium-risk until PAN-DB completes

Site analysis and categorization. (palo alto, n.d.)

The recommended policy action of this category is to Alert both site access and user

Credential submission.

1. Military: this category is set to allow both site access and user credential submission.

Recommendation: this category contain sites of Military divisions, training, ongoing or

Past activities, or any associated paraphernalia information or comments.

This kind of information does not have any advantage for the Lebanese university. (palo alto, n.d.)

The Recommended policy action of this category is to block both site access and user

Credential submission.

1. Newly registered domain: this category action is set to alert site access and allow user credential submission.

Recommendation: this category contains Recorded domains within the last 32 calendar

Days. (palo alto, n.d.)

The recommended policy action of this category is to block both site Access and

User credential submission.

1. Nudity: this category is set to allow both site access and user credential submission.

Recommendation: nudity category contain sites that contain nudes Regardless of

Meaning or purpose, the human body. (palo alto, n.d.)

The recommended policy action of this category is to block both site access and user

Credential submission.

1. Parked: this category action is set to allow both site access and user credentials submission.

Recommendation: parked category contain Individual-registered domains, sometimes

Later, are found used for credential phishing. These domains may be identical to legal

Domains, e.g. pal0alto0netw0rks.com, to recognize information for credentials or

Personal phishing purposes. (palo alto, n.d.)

The recommended policy action of this Category is to block both site access and user

Credential submission.

1. Peer to peer: this category action is set to allow both site access and user credentials submission.

Recommendation: peer-to-peer category contain sites that provides Access or Peer-to-

Peer Sharing Clients for uploading torrents, media files, or other software applications. (palo alto, n.d.)

The recommended policy action of this category is to alert both site access and user

Credential submission if there is a need for this kind of sites, or Block both site access

And user credential submission.

1. Proxy\_avoidance\_and\_anonymizers: this category action is set to allow both site access and user credentials submission.

Recommendation: proxy-avoidance-and-anonymizers category contain Proxy servers

And other techniques for bypassing URL filtering or tracking. (palo alto, n.d.)

The recommended Policy action of this category is to block both site access and user

Credential Submission.

1. Swimsuits-and intimate-apparel: this category action is set to allow both site access and user credentials submission.

Recommendation: this category contain Sites containing information or images relating

To swimsuits, intimate clothing or other suggestive clothing. I believe that

There is no use for this kind of sites in the Lebanese university. (palo alto, n.d.)

The recommended Policy action of this category is to block both site access and user

Credential Submission.

1. Unknown: this category action is set to allow both site access and user credentials submission.

Recommendation: this category contain websites that are not categorize, Therefore it

Does not exist in the Firewall URL filtering database or in the URL database. When

Deciding on what action to take for unknown traffic, we should be aware that setting the

Blocking action could be very disruptive for users because there could be many valid

Sites that are not yet in the URL database. (palo alto, n.d.)

The recommended Policy action for this Category is to alert both site access and user

Credential Submission, or for a strict policy Block both size access and user credential

Submission. (palo alto, n.d.)

**4.2 DOS Protection Policy Object enhancement**

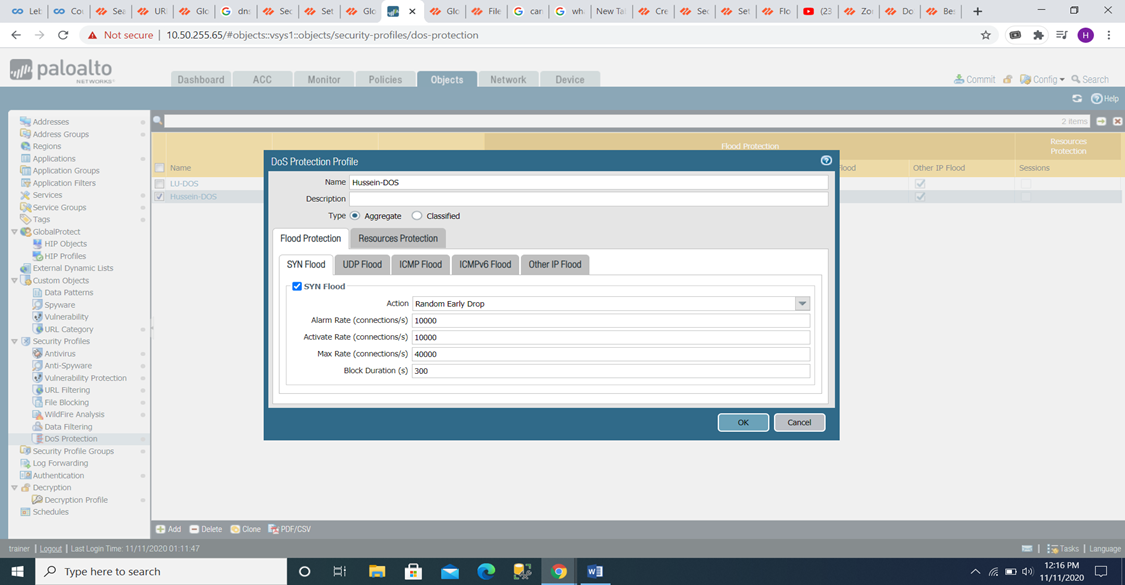


Figure DOS Protection Profile with enhancement

**SYN FLOOD (TCP)**

Alarm Rate: 10000

Recommendation: the Alarm rate should be above the average cps rate of the zone by

15-20%. The average cps rate in our condition is about 350. Therefore, the

Recommended alarm rate between 400 and 420.

Activate Rate: 10000

Recommendation: the Activate Rate should be above the peak of the cps rate of the zone

To begin mitigating potential floods. The average cps rate in our condition is about 350.

Therefore, the recommended Active rate in our condition is 400.

Max Rate: 40000

Recommendation: The Max Rate should be approximately 80-90% of firewall capacity

Per second. The firewall used at the Lebanese University maximum new session per second is about 169,000. Therefore, the recommended Max Rate in our situation is between 135,000 and 152,000.

Block Duration: 300

Recommendation: The block duration is Firewall block packet length of time matching

The DOS Protection policy rule that refers to this profile (Range is 1-21,600; default is

300). If you are more concerned about blocking volumetric attacks, but you are

Incorrectly blocking packets that are not part of an attack, I recommend setting a low

Block duration value if there is a concern that packets are incorrectly identified because

Attack traffic will be blocked unnecessarily, or setting a high block duration value.

**UDP FLOOD**

Alarm Rate: 10000

Recommendation: the Alarm rate should be above the average cps rate of the zone by

15-20%. The average cps rate in our condition is about 350. Therefore, the

Recommended alarm rate between 400 and 420.

Activate Rate: 10000

Recommendation: the Activate Rate should be above the peak of the cps rate of the zone

To begin mitigating potential floods. The average cps rate in our condition is about 350.

Therefore, the recommended Active rate in our condition is 400.

Max Rate: 40000

Recommendation: The Max Rate should be approximately 80-90% of firewall capacity

Per second. The firewall used at Lebanese University maximum new session per second is About 169,000. Therefore, the recommended Max Rate in our situation is between

135,000 and 152,000.

Block Duration: 300

Recommendation: The block duration is Firewall block packet length of time matching

The DOS Protection policy rule that refers to this profile (Range is 1-21,600; default is

300). If you are more concerned about blocking volumetric attacks, but you are

Incorrectly blocking packets that are not part of an attack, I recommend setting a low

Block duration value if there is a concern that packets are incorrectly identified because

Attack traffic will be blocked unnecessarily, or setting a high block duration value

**ICMP FLOOD**

Alarm Rate: 10000

Recommendation: the Alarm rate should be above the average cps rate of the zone by

15-20%. The average cps rate in our condition is about 350. Therefore, the

Recommended alarm rate between 400 and 420

Activate Rate: 10000

Recommendation: the Activate Rate should be above the peak of the cps rate of the zone

To begin mitigating potential floods. The average cps rate in our condition is about 350.

Therefore, the recommended Active rate in our condition is 400

Max Rate: 40000

Recommendation: The Max Rate should be approximately 80-90% of firewall capacity

Per second. The firewall used at Lebanese University maximum new session per second is about 169,000. Therefore, the recommended Max Rate in our situation is between 135,000 and 152,000.

Block Duration: 300

Recommendation: The block duration is Firewall block packet length of time matching

The DOS Protection policy rule that refers to this profile (Range is 1-21,600; default is

300). If you are more concerned about blocking volumetric attacks, but you are

Incorrectly blocking packets that are not part of an attack, I recommend setting a low

Block duration value if there is a concern that packets are incorrectly identified because

Attack traffic will be blocked unnecessarily, or setting a high block duration value

**Other IP FLOOD**

Alarm Rate: 10000

Recommendation: the Alarm rate should be above the average cps rate of the zone by

15-20%. The average cps rate in our condition is about 350. Therefore, the

Recommended alarm rate between 400 and 420.

Activate Rate: 10000

Recommendation: the Activate Rate should be above the peak of the cps rate of the zone

To begin mitigating potential floods. The average cps rate in our condition is about 350.

Therefore, the recommended Active rate in our condition is 400.

Max Rate: 40000

Recommendation: The Max Rate should be approximately 80-90% of firewall capacity

per second. The firewall used at Lebanese University maximum new session per second

is about 169,000. Therefore, the recommended Max Rate in our situation is between

135,000 and 152,000.

Block Duration: 300

Recommendation: The block duration is Firewall block packet length of time matching

The DOS Protection policy rule that refers to this profile (Range is 1-21,600; default is

300). If you are more concerned about blocking volumetric attacks, but you are

Incorrectly blocking packets that are not part of an attack, I recommend setting a low

Block duration value if there is a concern that packets are incorrectly identified because

Attack traffic will be blocked unnecessarily, or setting a high block duration value. (palo alto, n.d.)

**4.3 File Blocking Policy Object enhancement**

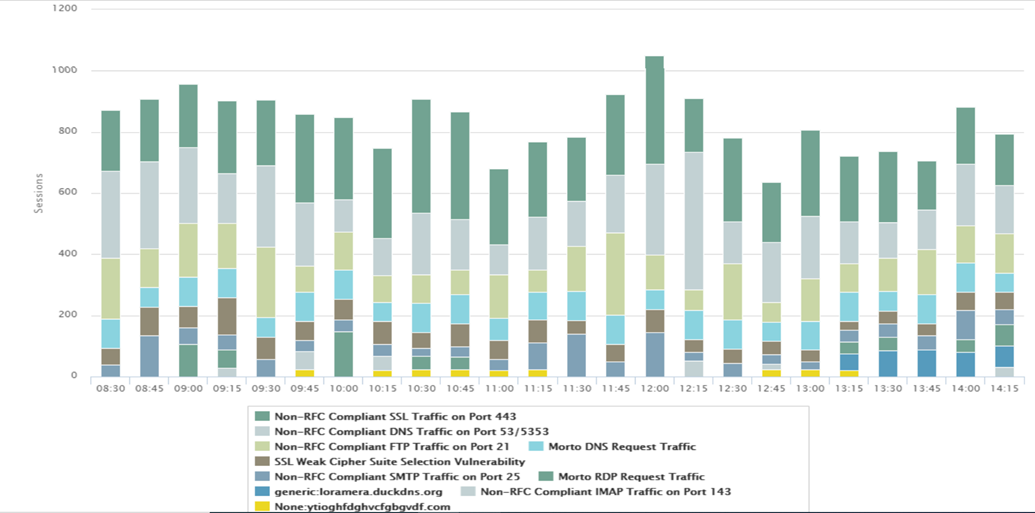


Figure threat monitor report

This graph represents the threat attacks report on the Lebanese university in 6 hours we

To put the enhancement on file blocking policy used threat log monitoring that this

Represent an idea and we used this monitoring log to know the threat files that our

Network is encountering and we concluded some enhancement that are mentioned

Below:

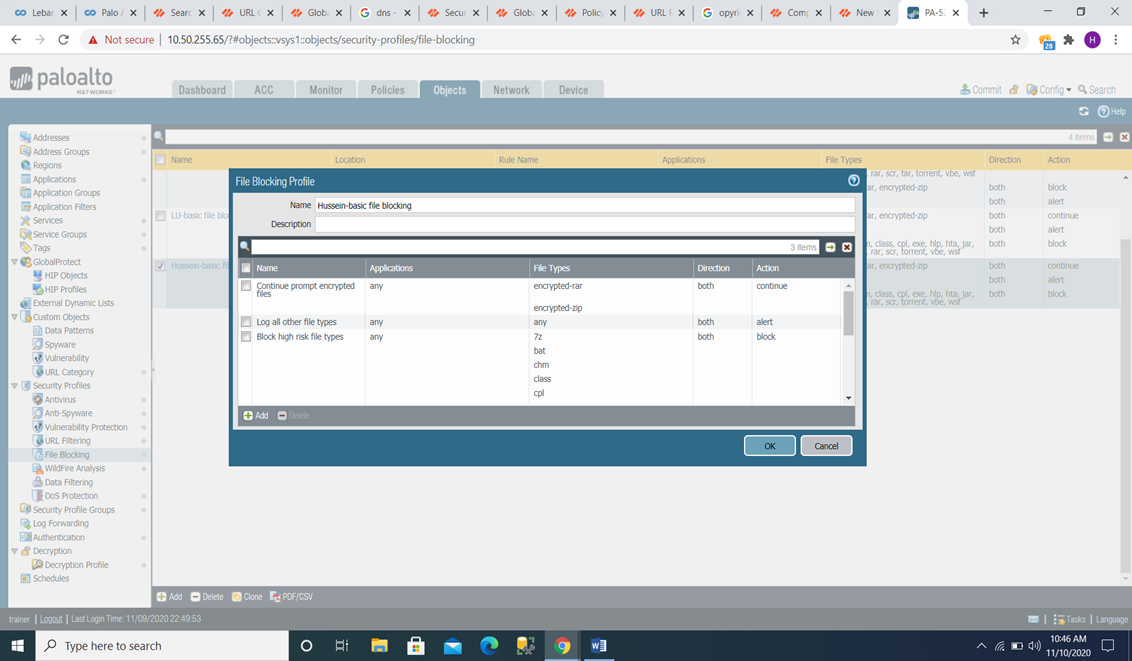


Figure File Blocking Profile with enhancement

The recommendation that will enhance this policy states that Files that are commonly

Included in malware attack campaigns or that do not have a real Upload/Download

Case. PE files (Scr, Cpl, dll, Ocx, Pif, exe), Java files (class, jar), help files (chm, help)

In addition, other potentially malicious file types should be block (including Vbe, Hta,

Wsf, Torrent, 7z, rar, and bat). The security policy named Block High Risk File types

Do not Contain these entire files example it do not contain: Dll (Windows Dynamic

Link Library), exe (Windows Executable).

**Chapter5: Conclusion**

This project studies the Lebanese university cybersecurity system, the project focus on a

Specific tool used in the Cyber Security Operation Center that is the Palo Alto Next

Generation Firewall we worked on a policy that consists of a number of tcp and udp

Ports that considered being harmful to the university Network, it might use by

Cybercriminals to lunch cyberattacks. In addition to the ports the policy contained a

Profile group that contains three objects URL filtering, DOS Protection and File

Blocking.

URL Filtering consisted of sites categories; we have chosen the needed sites categories

For the Lebanese university and blocked the categories that may contain harm toward

The university network and the unneeded categories.

DOS Protection consisted of different ports we calculated for each port specific alarm

Rate; activate Rate, max rate and the block duration with the use of the Palo Alto rules

That uses the Cps (connection per second) zone rate. We measured cps zone rate of

Our network and used it to get the needed rate for each port (alarm rate, activate rate,

Max rate, Block duration).

File Blocking we created three categories of this object that are Continue prompt

Encrypted files this category contained needed encrypted files for the university so it

Grants permission to get access toward the network, Log all other file types this

Category alert about the files that are being send or received to the network, Block high

Risk File type this category contained harmful file types that can used through

Cyberattacks.

This Policy in addition to the enhancement we mentioned in our project increase the university cybersecurity system efficiency those enhancement will be tested for 2 months and we will see if those enhancements are efficient and effective and secure the university cybersecurity system.

As we reached this point, other features can get added to our policy we could specify specific services for each ports and for each application, we can include more objects such as Antispyware, antivirus, vulnerability protection and wildfire analysis. Such features shall solidify the system so that it becomes robust enough to Handel cyberattacks.

**REFERENCES**

[1] [www.paloalto.com](http://www.paloalto.com)

[2] [www.ul.edu.lb](http://www.ul.edu.lb)

[3] Dcs.paloaltonetworks.com

[4] www.dagstuhl.de

[5] [www.nextgensecurityforeducation.com](http://www.nextgensecurityforeducation.com)

[6] Urlfiltering.paloaltonetworks.com

[7] Knowledgebase.paloaltonetworks.com

[8] Secureleaves.wordpress.com

[9] CYBERSECURITY SURVIVAL GUIDE Principles & Best Practices by Lawrence

C. Miller

[10] Understanding DoS Protection in PAN-OS

[11] CompTIA security + by Professor Messer