IT Technology Network
SS3

Paloalto Networks Academy

Lillebaelt Academy
University of Applied Sciences
IT and Electronics Engineer
3 semester IT-Network

Authors:

Fernando Coello Kjartansson

Abdalmannan Shek Nasan

Wednesday 07 December 2016

Table of Contents

Network overview (HLD)

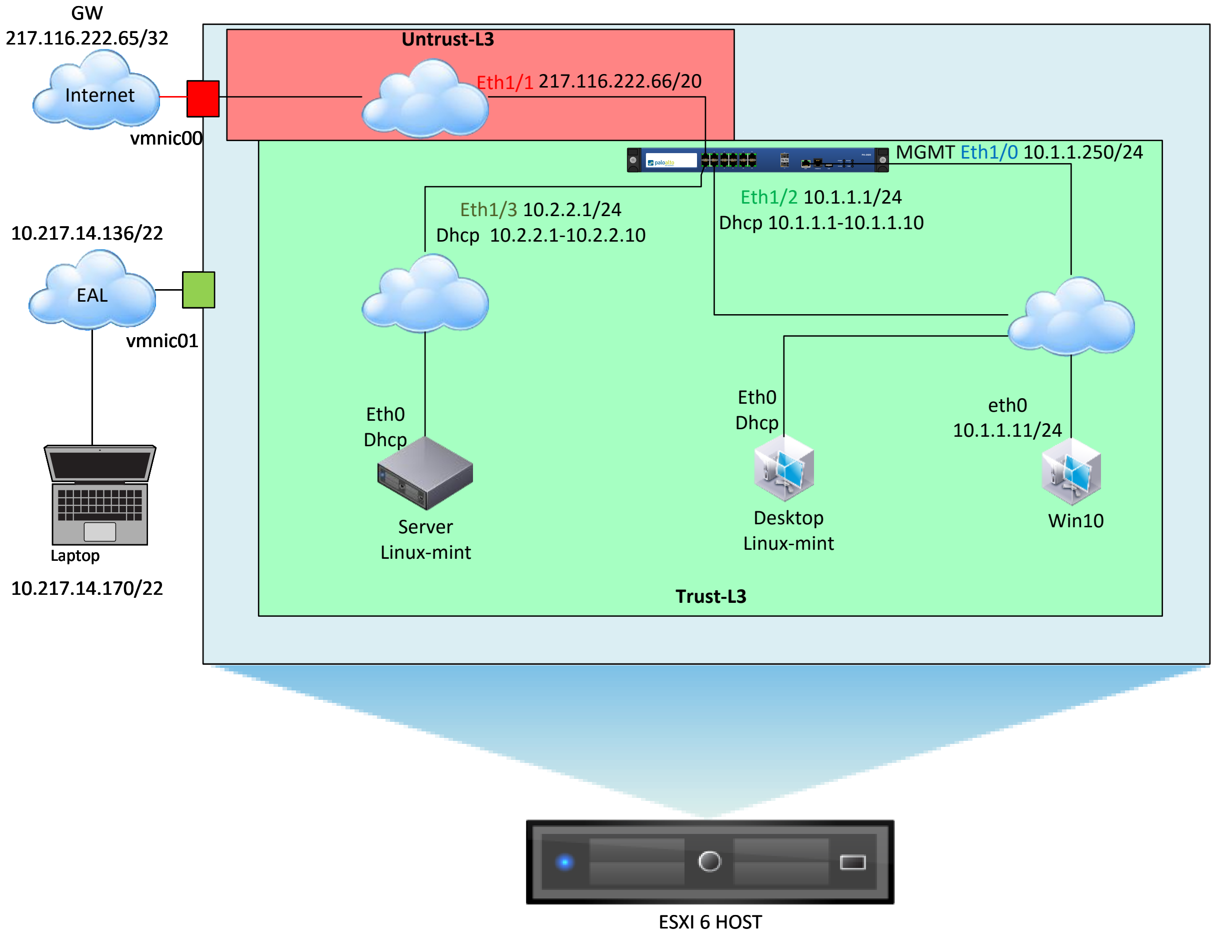


Figure 1.Network Topology

In Figure 2 we have the topology we needed to achieve this Paloalto Network Training.

We run the hole system in a EXSI 6 host that contains the following virtual machines: Paloalto PAM-OS, Windows 10, Linux-mint (Desktop) and Linux-mint (Server).

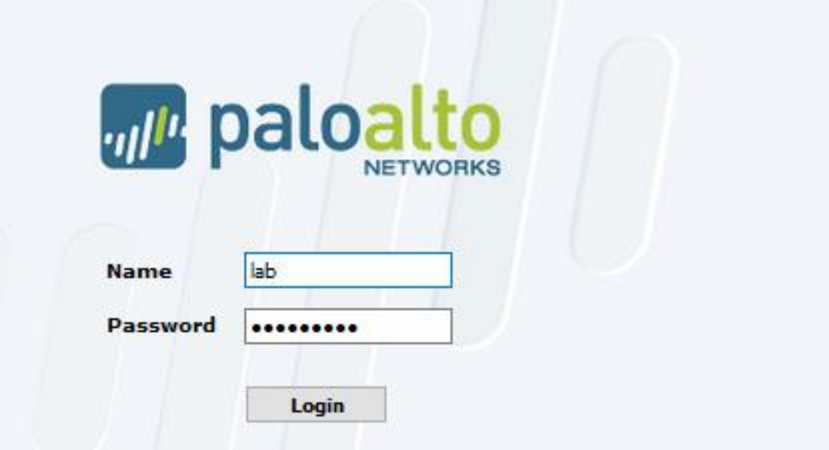
The EXSI 6 have two physical nics:

> **vmnic00**: connected directly to internet and represented with a red color.
>
> **vmnic01**: connected to EAL network and configured as a “vkernel-port -group”. That mean this NIC is only intended for manage ESXI 6 host and the VMs whiting the host. But the VMs are not able to connect to EAL network.

Tasks

Lab 1. Initial Configuration

At this lab, we Connected VM-plaoalto-100 with VM-Windows 10 we use management interface, we Clear the firewall logs them Applied a baseline
configuration to build successive labs we Created a new admin account and tested the configuration locks.
We Checked that the licenses are valid and we updated the software
Note: you need to configure DNS server on firewall for added license key

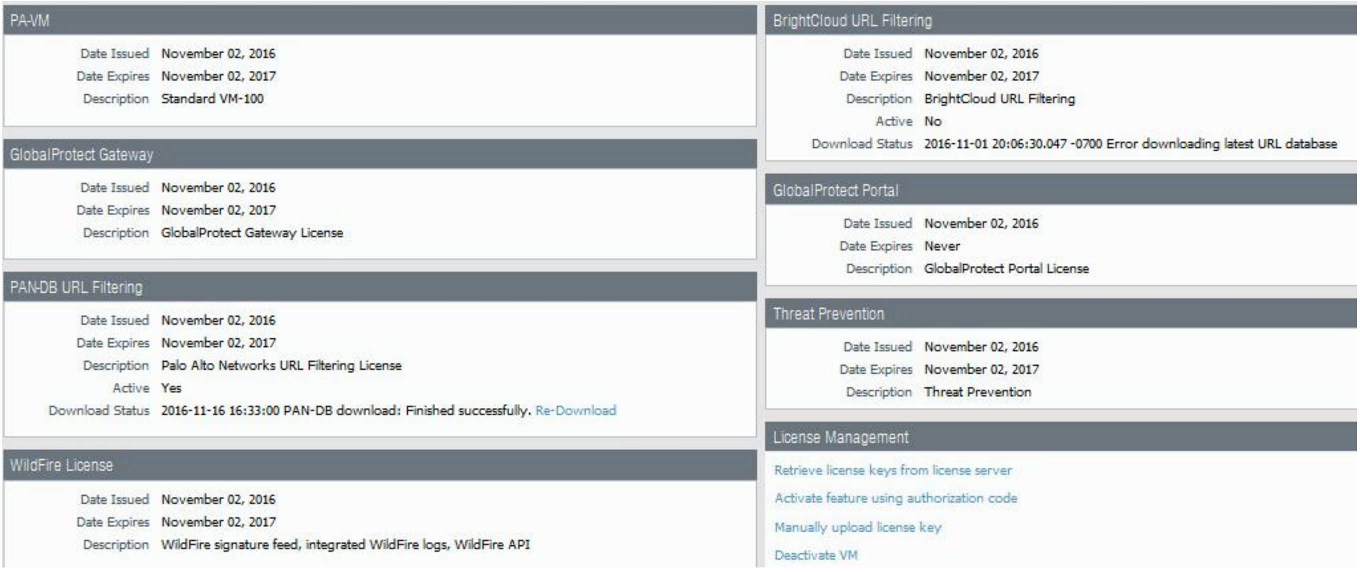


Name lab

Password •••••••••

Figur 1 screen shot from browser

Figure1 We created user called **lab.**



PA-VM
Date Issued November 02, 2016
Date Expires November 02, 2017
Description Standard VM-100

GlobalProtect Gateway
Date Issued November 02, 2016
Date Expires November 02, 2017
Description GlobalProtect Gateway License

PAN-DB URL Filtering
Date Issued November 02, 2016
Date Expires November 02, 2017
Description Palo Alto Networks URL Filtering License
Active Yes
Download Status 2016-11-16 16:33:00 PAN-DB download: Finished successfully. Re-Download

WildFire License
Date Issued November 02, 2016
Date Expires November 02, 2017
Description WildFire signature feed, integrated WildFire logs, WildFire API

BrightCloud URL Filtering
Date Issued November 02, 2016
Date Expires November 02, 2017
Description BrightCloud URL Filtering
Active No
Download Status 2016-11-01 20:06:30.047 -0700 Error downloading latest URL database

GlobalProtect Portal
Date Issued November 02, 2016
Date Expires Never
Description GlobalProtect Portal License

Threat Prevention
Date Issued November 02, 2016
Date Expires November 02, 2017
Description Threat Prevention

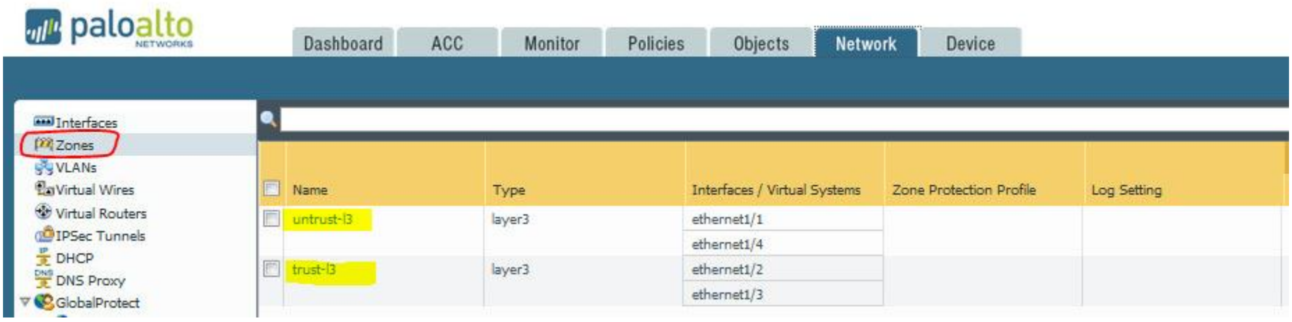
License Management
Retrieve license keys from license server
Activate feature using authorization code
Manually upload license key
Deactivate VM

Figur 2 screen shot show license key

Figure2 After you include license key you go to Device and choose license you will see what its active and how long is active

Lab 2. Basic Interface Configuration

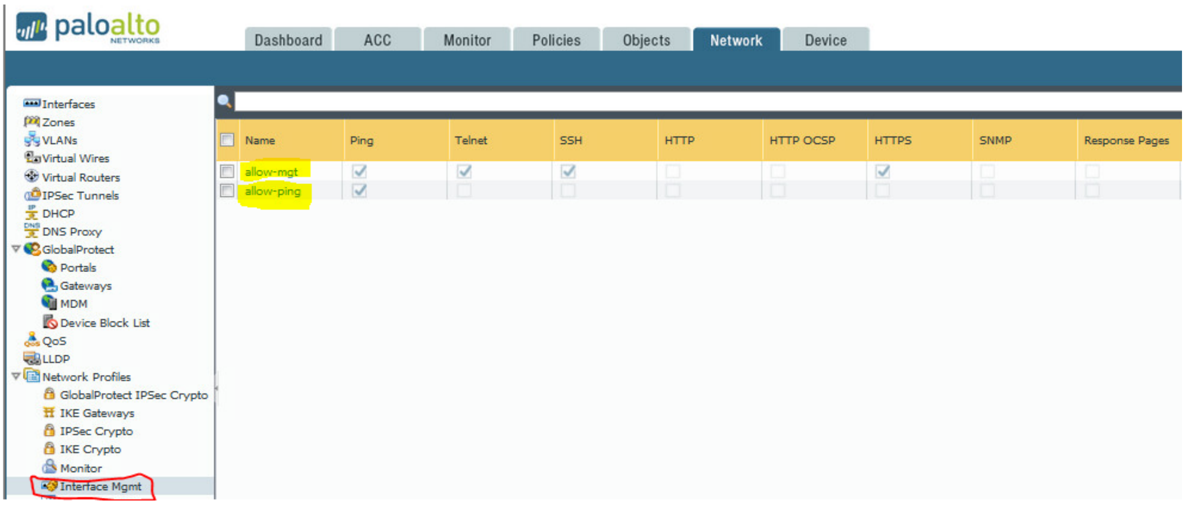
In this lab, we created two zones, Trust-L3 and Untrust-L3, the interface in the Trust-L3 Zone will provided DHCP addresses to these internal clients.
the Untrust-L3 zone, connected to cloud internet
The interface in Untrust-L3 configured to respond to pings and the interface in Trust-L3 provided all management services.
Note: you need Virtual router and Nat to make NAT Policy between to zones



□	Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Log Setting
□	untrust-l3	layer3	ethernet1/1 ethernet1/4		
□	trust-l3	layer3	ethernet1/2 ethernet1/3		

Figur 3screen shot show zones

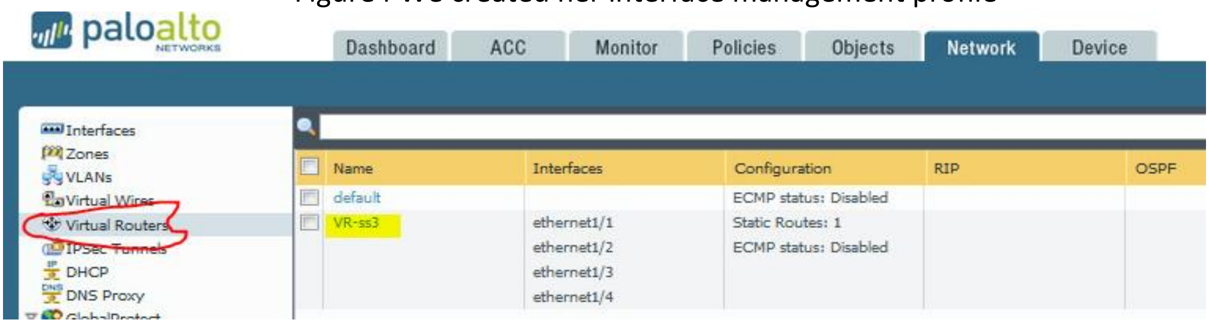
Figure3 we created 2 zones and called untrust-l3 and trust-l3



□	Name	Ping	Telnet	SSH	HTTP	HTTP OCSP	HTTPS	SNMP	Response Pages
□	allow-mgt	☑	☑	☑	□	□	☑	□	□
□	allow-ping	☑	□	□	□	□	□	□	□

Figur 4 screen shot for management profile

Figure4 We created her interface management profile



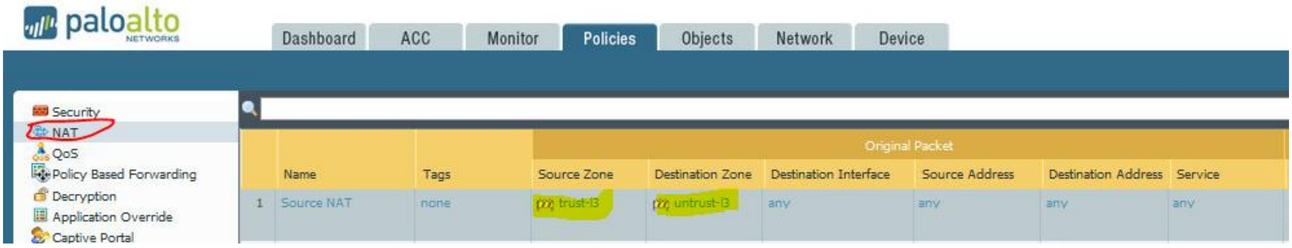
□	Name	Interfaces	Configuration	RIP	OSPF
□	default		ECMP status: Disabled		
□	VR-ss3	ethernet1/1 ethernet1/2 ethernet1/3 ethernet1/4	Static Routes: 1 ECMP status: Disabled		

Figur 5 screenshot for virtual router

Figure5 We created her Virtual router

Lab 3. NAT and Security Policy

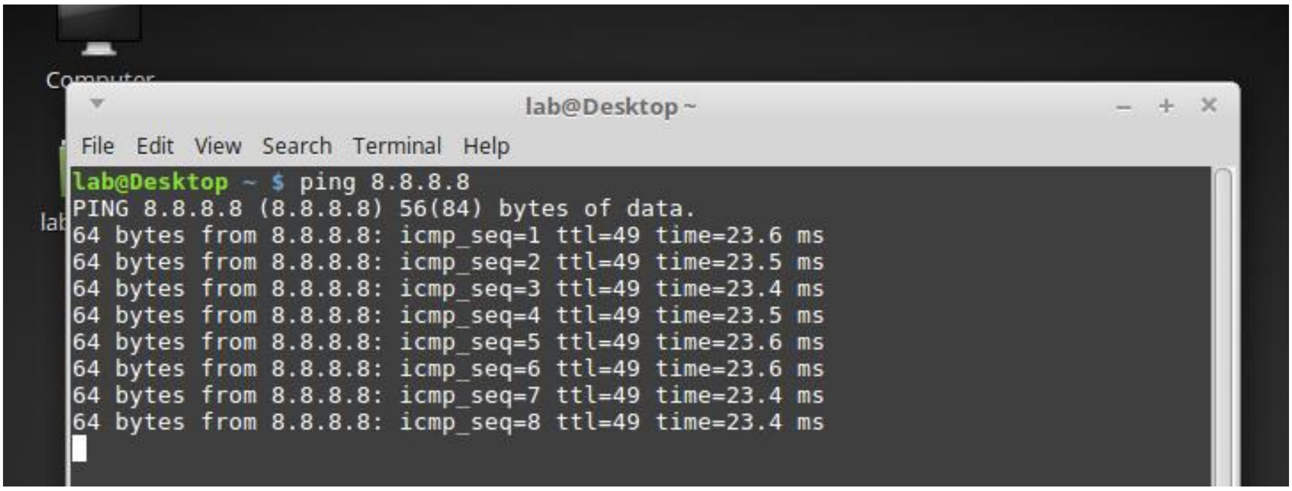
At this lab, we created a Source NAT Policy using the Untrust-L3 IP address as the source address for all outgoing traffic. Then we created a Security Policy to allow traffic from the Trust-L3 Zone to the Untrust-L3 Zone, so paloaltio can access the outside world.



			Original Packet					
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service
1	Source NAT	none	trust-l3	untrust-l3	any	any	any	any

Figur 6 screen shot for NAT source

Figure6 We created source Nat between to zones



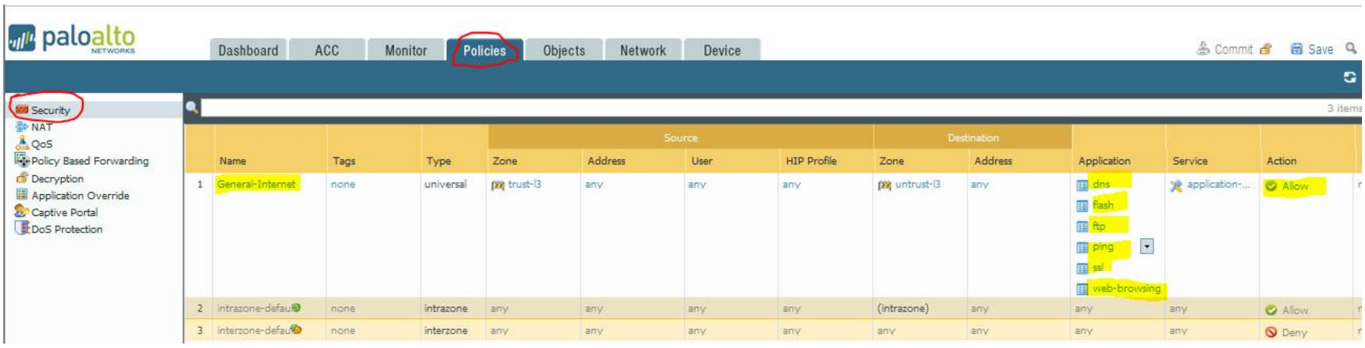
```
lab@Desktop ~ $ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=49 time=23.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=49 time=23.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=49 time=23.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=49 time=23.5 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=49 time=23.6 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=49 time=23.6 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=49 time=23.4 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=49 time=23.4 ms
```

Figure 7 screen shot testing and ping from host in trust-l3

Figure7 Her we testing by ping google after we make NAT

Lab 4. Basic App ID

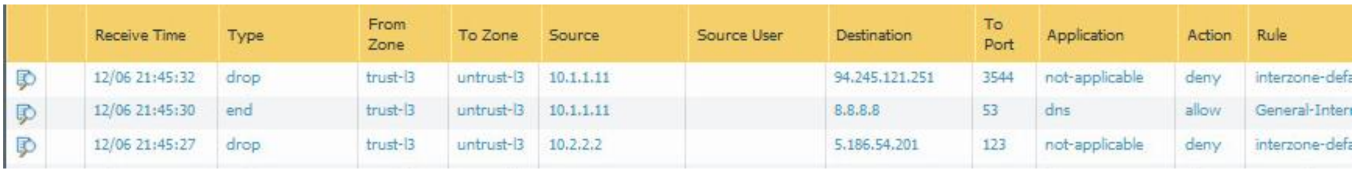
At this lab, we created a Security Policy to selectively enable specific applications to pass from the Trust-L3 to the Untrust-L3 Zone. All other applications blocked.
we Created a Rule named G-NET, which allows users in the Trust-L3 zone to use a set of commonly used applications such as ((dns, flash, ftp, ping, ssl, and web-browsing)). The applications only be permitted on an application’s default port.
All other traffic in and out between Zones blocked



				Source				Destination				
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	General-Internet	none	universal	trust-l3	any	any	any	untrust-l3	any	dns flash ftp ping ssl web-browsing	application-...	Allow
2	intrazone-defau	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow
3	interzone-defau	none	interzone	any	any	any	any	any	any	any	any	Deny

Figur 8 screen shot for security policy

Figure8 a Security Policy to enable specific applications to pass from the Trust-L3 to the Untrust-L3 Zone



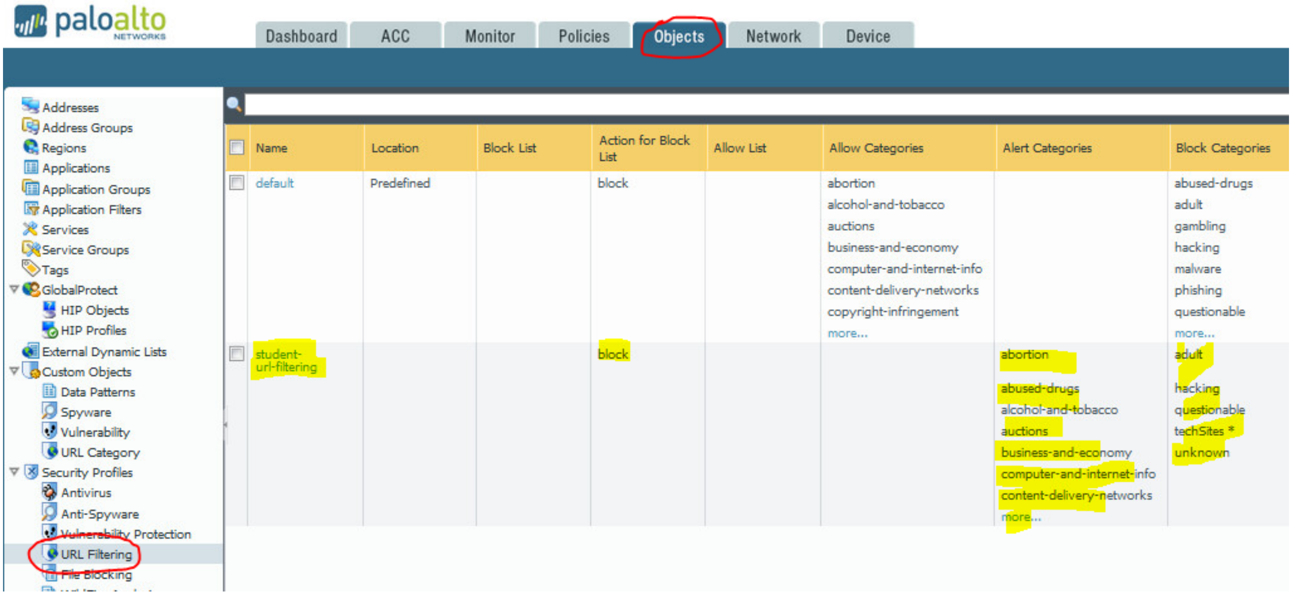
	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule
	12/06 21:45:32	drop	trust-l3	untrust-l3	10.1.1.11		94.245.121.251	3544	not-applicable	deny	interzone-defa
	12/06 21:45:30	end	trust-l3	untrust-l3	10.1.1.11		8.8.8.8	53	dns	allow	General-Intern
	12/06 21:45:27	drop	trust-l3	untrust-l3	10.2.2.2		5.186.54.201	123	not-applicable	deny	interzone-defa

Figur 9 screen shot from monitor traffic

Figure9 All traffic in and out between Zones blocked 10.1.1.11

Lab 5. URL Filtering

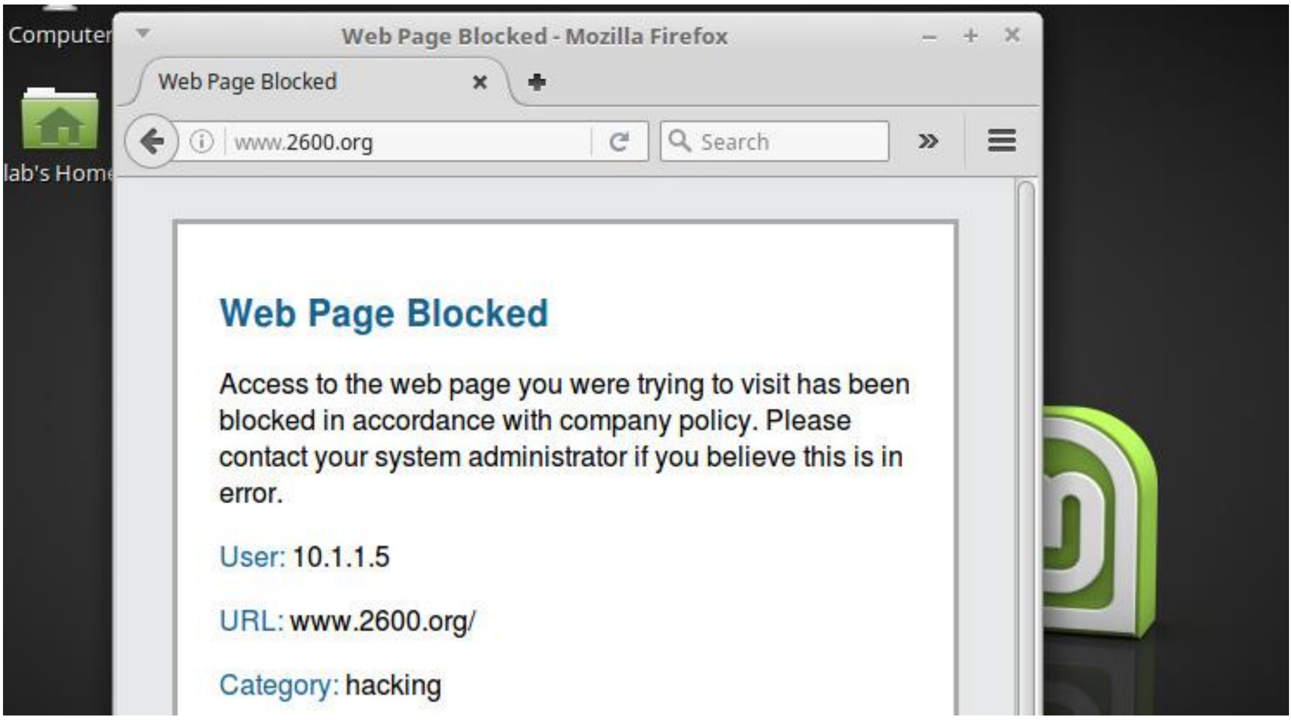
we Configured a custom URL filtering category Tech Sites specifying newegg, cnet, and zdnet. we Blocked these URL categories ((adult-government-hacking-questionable-TechSites-unknown)) we testing by over this site www.2600.org



□	Name	Location	Block List	Action for Block List	Allow List	Allow Categories	Alert Categories	Block Categories
□	default	Predefined		block		abortion alcohol-and-tobacco auctions business-and-economy computer-and-internet-info content-delivery-networks copyright-infringement more...		abused-drugs adult gambling hacking malware phishing questionable more...
□	student-url-filtering			block			abortion abused-drugs alcohol-and-tobacco auctions business-and-economy computer-and-internet-info content-delivery-networks more...	adult hacking questionable techSites * unknown

Figur 10 screen shot for URL File

Figure10 URL filtering file that we created



Web Page Blocked

Access to the web page you were trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: 10.1.1.5

URL: www.2600.org/

Category: hacking

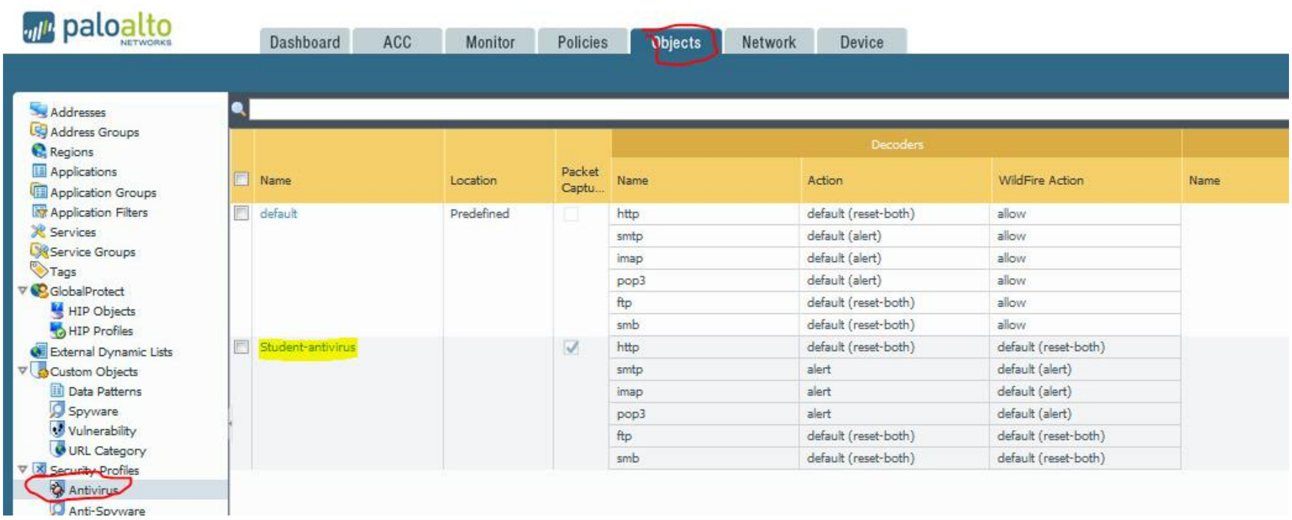
Figur 11 screenshot for testing

Figure 11 Her we tasting by access this site

Lab 6. Anti-Virus & Anti-Spyware Profiles

we Configured a Antivirus Profile and a Antispyware Profile we Assign Profiles to a Security Profile Group we Assign the Security Profile Group to a Policy and we testing by Download Anti Malware Test file and antivirus test file

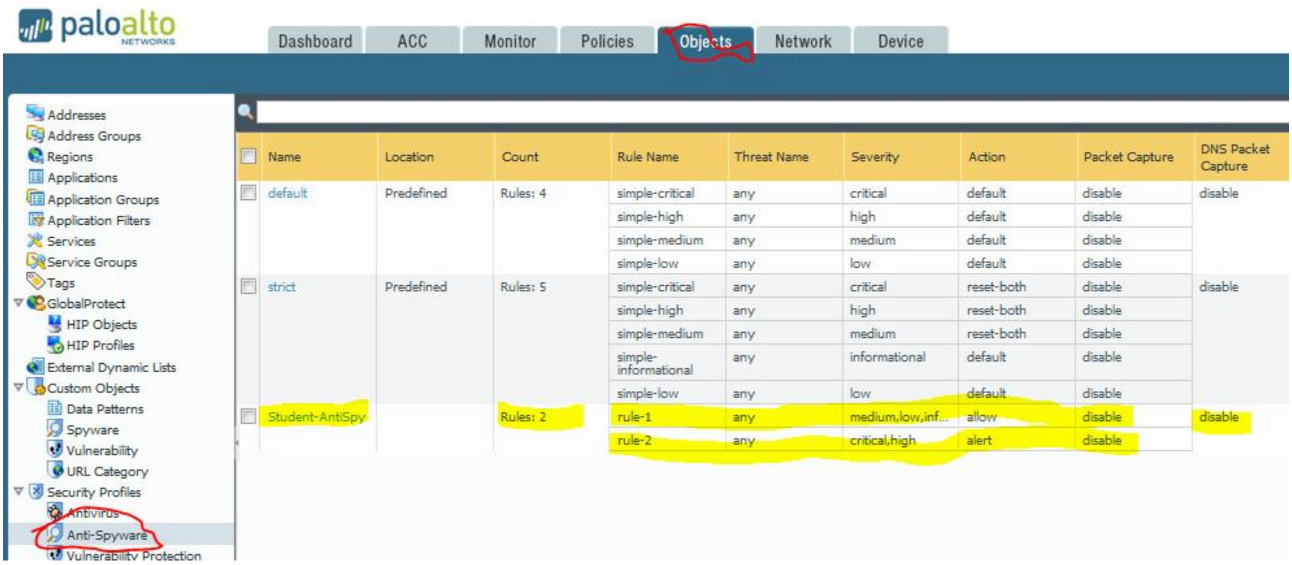
Note: Test the antivirus profile using http and not https because decryption has not been configured on the firewall ye in this case



				Decoders			
□	Name	Location	Packet Captu...	Name	Action	WildFire Action	Name
□	default	Predefined	□	http	default (reset-both)	allow	
				smtp	default (alert)	allow	
				imap	default (alert)	allow	
				pop3	default (alert)	allow	
				ftp	default (reset-both)	allow	
				smb	default (reset-both)	allow	
□	Student-antivirus		☑	http	default (reset-both)	default (reset-both)	
				smtp	alert	default (alert)	
				imap	alert	default (alert)	
				pop3	alert	default (alert)	
				ftp	default (reset-both)	default (reset-both)	
				smb	default (reset-both)	default (reset-both)	

Figur 12 screen shot for antivirus file

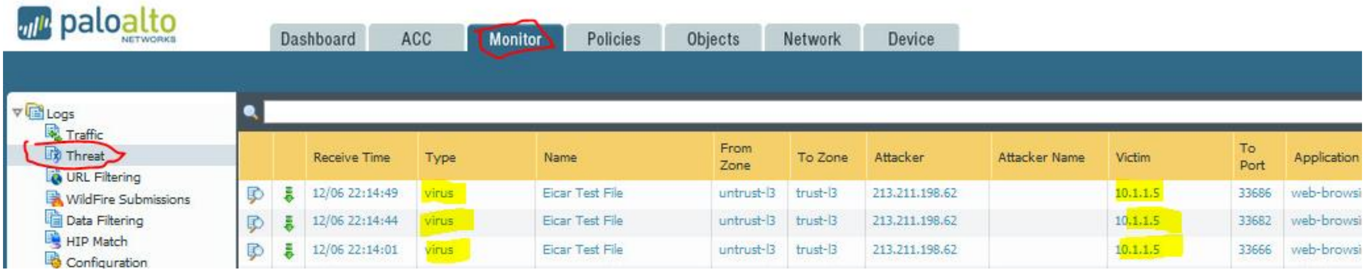
Figure12 show the Antivirus-file we created



□	Name	Location	Count	Rule Name	Threat Name	Severity	Action	Packet Capture	DNS Packet Capture
□	default	Predefined	Rules: 4	simple-critical	any	critical	default	disable	disable
				simple-high	any	high	default	disable	
				simple-medium	any	medium	default	disable	
				simple-low	any	low	default	disable	
□	strict	Predefined	Rules: 5	simple-critical	any	critical	reset-both	disable	disable
				simple-high	any	high	reset-both	disable	
				simple-medium	any	medium	reset-both	disable	
				simple-informational	any	informational	default	disable	
				simple-low	any	low	default	disable	
□	Student-AntiSpy		Rules: 2	rule-1	any	medium,low,inf...	allow	disable	disable
				rule-2	any	critical,high	alert	disable	

Figur 13 screen shot for anti-spyware file

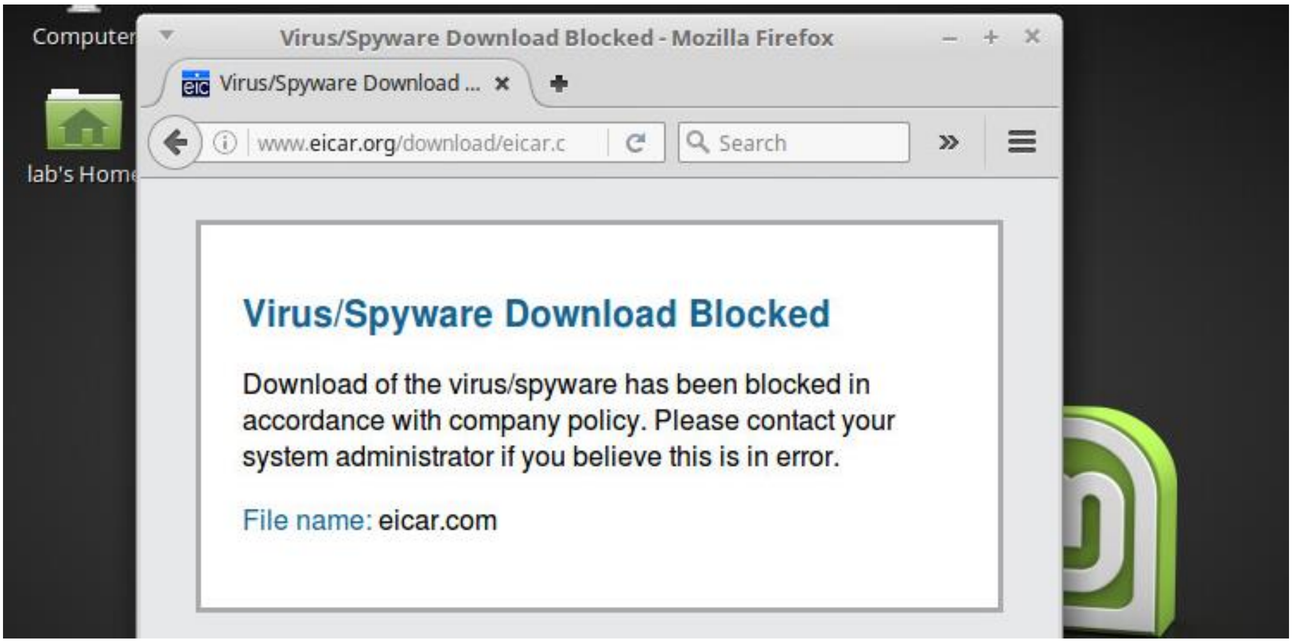
Figure13 show the Anti-spyware-file we created



		Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application
		12/06 22:14:49	virus	Eicar Test File	untrust-l3	trust-l3	213.211.198.62		10.1.1.5	33686	web-browsi
		12/06 22:14:44	virus	Eicar Test File	untrust-l3	trust-l3	213.211.198.62		10.1.1.5	33682	web-browsi
		12/06 22:14:01	virus	Eicar Test File	untrust-l3	trust-l3	213.211.198.62		10.1.1.5	33666	web-browsi

Figur 14 screen shot for monitor traffic

Figure14 Her you can see the cache virus



Computer
lab's Home
Virus/Spyware Download Blocked - Mozilla Firefox
Virus/Spyware Download ...
www.eicar.org/download/eicar.c
Search

Virus/Spyware Download Blocked

Download of the virus/spyware has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

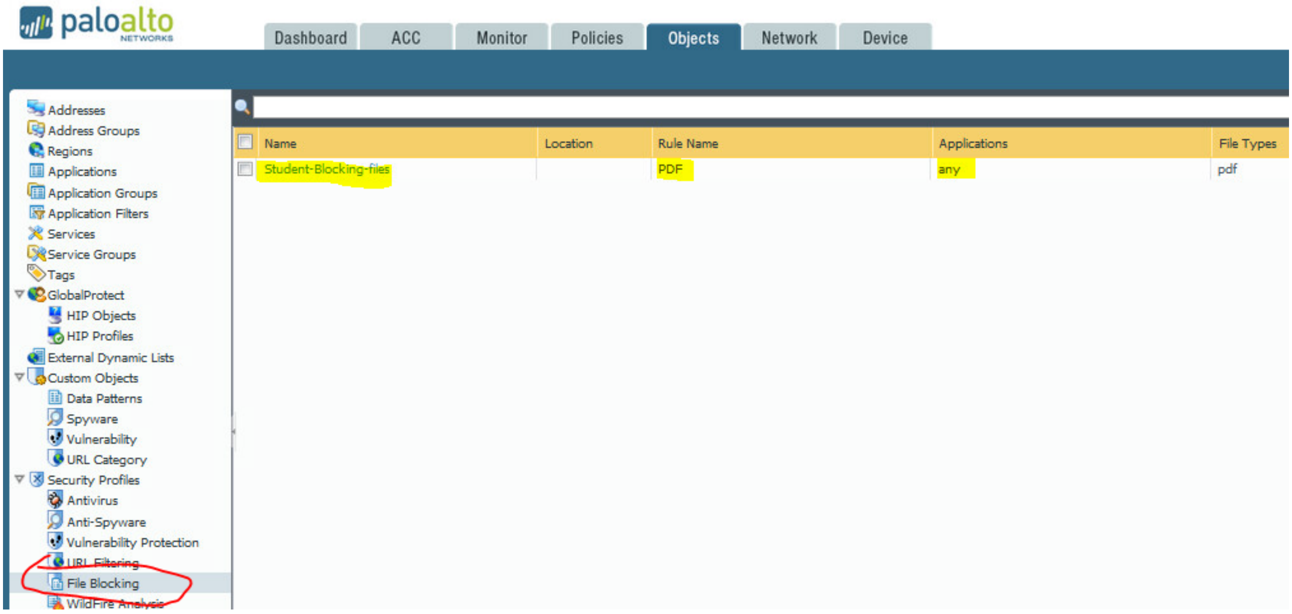
File name: eicar.com

Figur 15 screen shot for testing virus/spyware

Figure15 Her you can see the are blocked Virus/Spyware

Lab 7. File Blocking and Wildfire

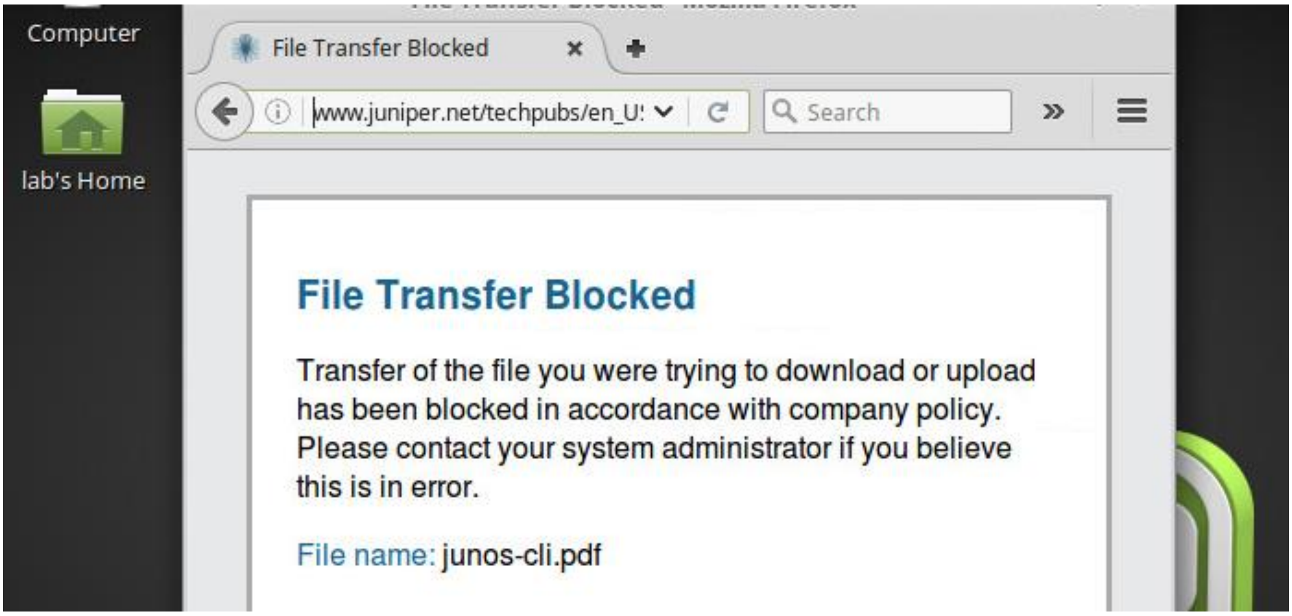
At this lab we Configured downloaded pdf files be automatically blocked.
the Testing we trying by downloaded pdf file



□	Name	Location	Rule Name	Applications	File Types
□	Student-Blocking-files		PDF	any	pdf

Figur 16 screen shot for the blocking file

Figure16 her we created file to block PDF



File Transfer Blocked

Transfer of the file you were trying to download or upload has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

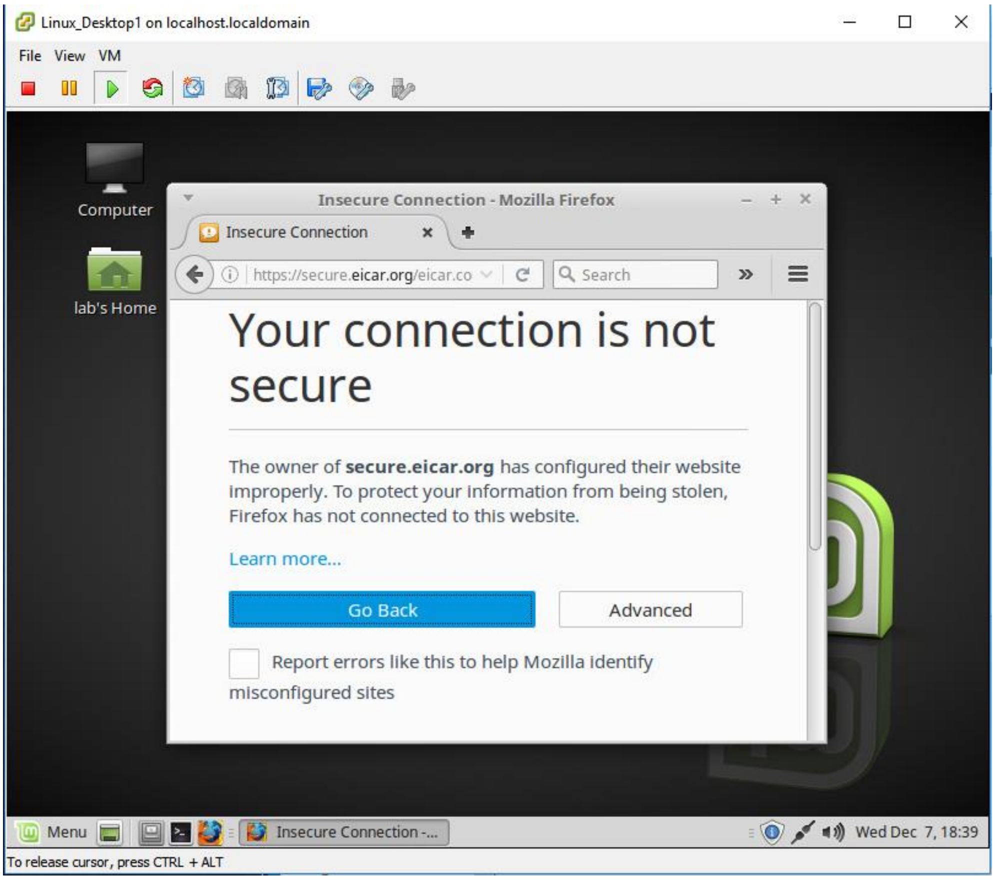
File name: junos-cli.pdf

Figur 17 screen shot show for blocking PDF file

Figure17 we couldn't open pdf file because its blocked

Lab 8. Decryption

In this lab 8 we generate a Certification that is apply to a Decryption Policy Rules and in each rule we can define witch traffic can be allowed and decrypted.
Testing: we testing with a Linux machine open the browser and downloading encrypted and unencrypted traffic and in the browser appear “Untrusted page” where we need to add Exception to accept the Certification we generate in this LAB. Also we also check on Monitor -> traffic the logs generation in PA.


Linux_Desktop1 on localhost.localdomain
File View VM
Computer
lab's Home
Insecure Connection - Mozilla Firefox
Insecure Connection
https://secure.eicar.org/eicar.co
Search
Menu
Insecure Connection -...
Wed Dec 7, 18:39
To release cursor, press CTRL + ALT

Your connection is not secure

The owner of **secure.eicar.org** has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

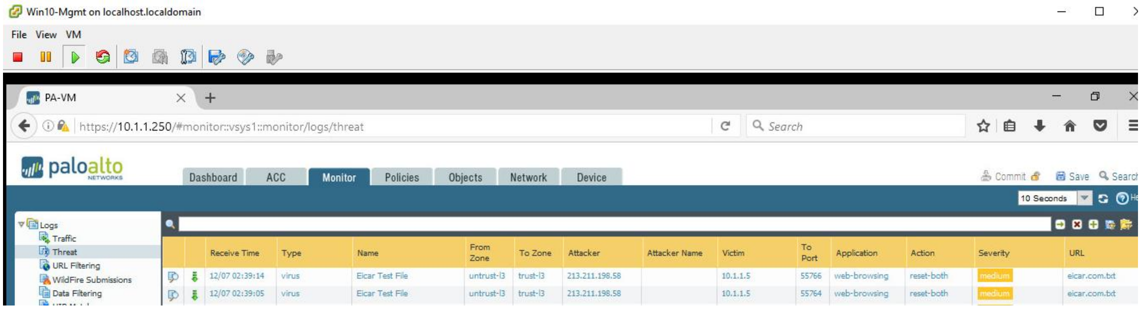
Learn more...

Go Back | Advanced

□ Report errors like this to help Mozilla identify misconfigured sites

Figur 18 screen shot for testing CA

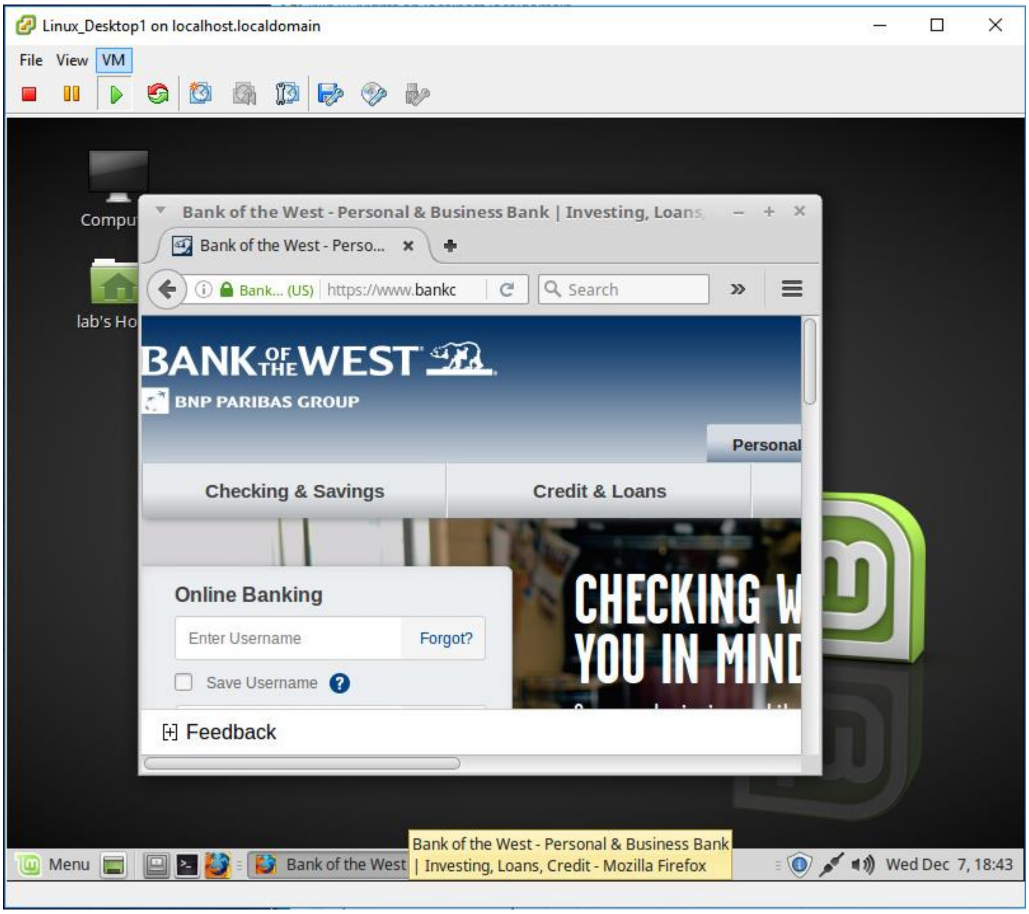
Figure18 We need to accept the CA we generate in PA in the browser.



		Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity	URL
		12/07 02:39:14	virus	Eicar Test File	untrust-l3	trust-l3	213.211.198.58		10.1.1.5	55766	web-browsing	reset-both	medium	eicar.com.txt
		12/07 02:39:05	virus	Eicar Test File	untrust-l3	trust-l3	213.211.198.58		10.1.1.5	55764	web-browsing	reset-both	medium	eicar.com.txt

Figur 19 screen shot for monitor traffic

Figure19 Logs when not allowed encrypted traffic


Linux_Desktop1 on localhost.localdomain
File View VM
Bank of the West - Personal & Business Bank | Investing, Loans,
Bank of the West - Perso...
Bank... (US) https://www.bankc
Search
BANK OF THE WEST
BNP PARIBAS GROUP
Personal
Checking & Savings
Credit & Loans
Online Banking
Enter Username
Forgot?
Save Username
CHECKING W
YOU IN MIND
Feedback
Menu
Bank of the West
Bank of the West - Personal & Business Bank | Investing, Loans, Credit - Mozilla Firefox
Wed Dec 7, 18:43

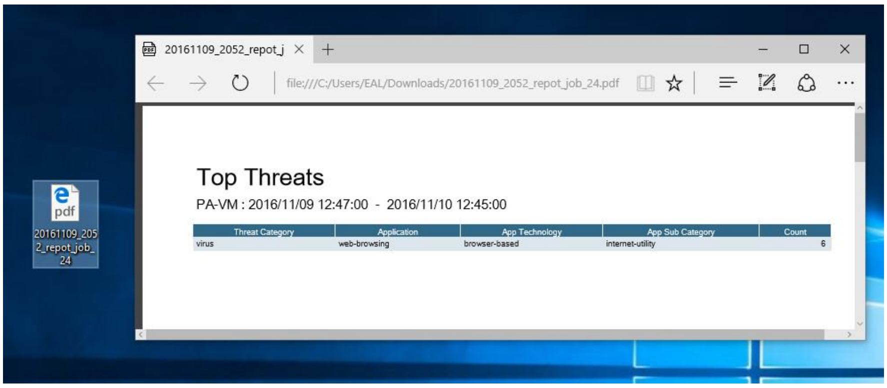
Figur 20 screen shot for testing

Figure20 We allow encrypted if there are financial services

Lab 9. Management and Reporting

In this lab 9 consist in management and generate custom reports, selecting the data we want in this report. We can choose a range of dates, filtering by threats, Applications, etc.

Testing: we create custom report and we exported as a PDF document.


20161109_2052_repot_j
file:///C:/Users/EAL/Downloads/20161109_2052_repot_job_24.pdf
20161109_2052_repot_job_24

Top Threats

PA-VM : 2016/11/09 12:47:00 - 2016/11/10 12:45:00

Threat Category	Application	App Technology	App Sub Category	Count
virus	web-browsing	browser-based	internet-utility	6

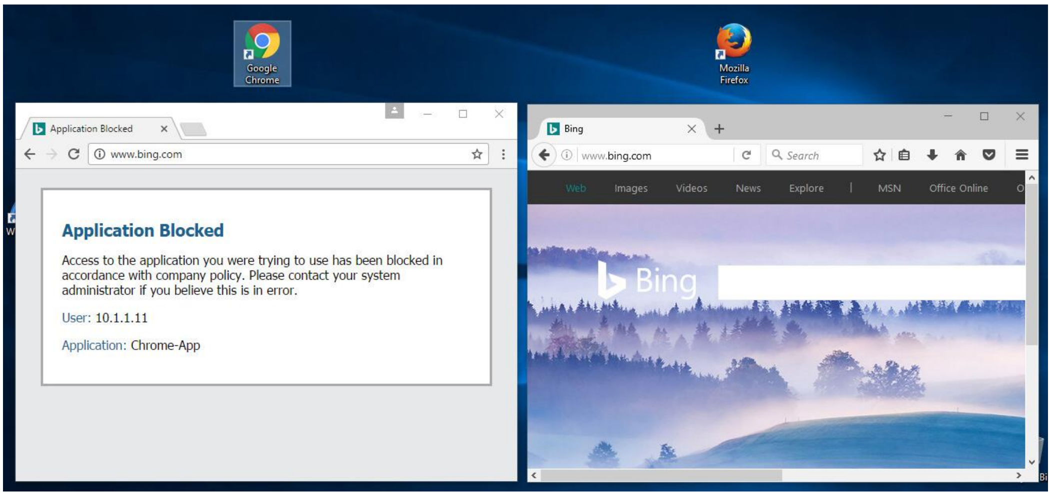
Figur 21screen shot for document we created

Figure21 Example of a PDF report generation by PA.

Lab 10. Custom Apps

In this lab 10 we create a new Application Object Signature. After we configure this object giving all the parameters we need to identify this application we will see that we can chose this object when we define a Security Policy Rule in the Application tab.

<u>Testing</u>: We configure the object to identify Google Chrome, and we tested trying to connect from this application from our desktop 1 getting the message Application Blocked.



Application Blocked

Access to the application you were trying to use has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: 10.1.1.11

Application: Chrome-App

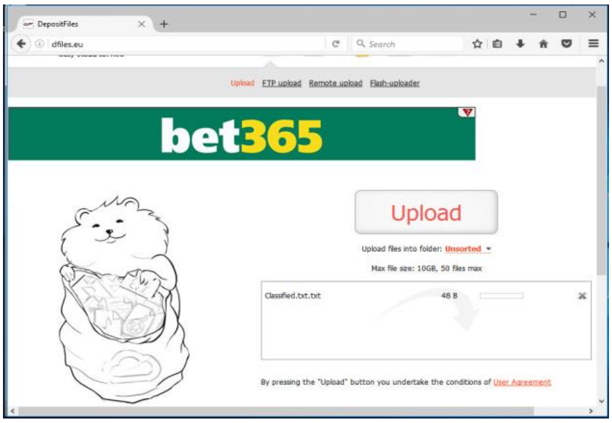
Figur 22 screen shot for application

Figure22 On the right side Chrome “blocked” on the left side Firefox running

Lab 11. Custom Data Patterns

In lab 11 we start creating an Object “Data Pattern” (where we specify the pattern “classified” to be identify) and after another Object “Data Filtering” related to the first Object. Once we have this two object we can choose an Application in our Security Policy Rule to apply the Data Filtering we create before.

<u>Testing</u>: We try to upload a file with “classified” pattern from one of our VM and we don’t get any progress uploading.



Upload files into folder: Unsorted

Max file size: 10GB, 50 files max

Classified.txt.txt 48 B

By pressing the "Upload" button you undertake the conditions of User Agreement

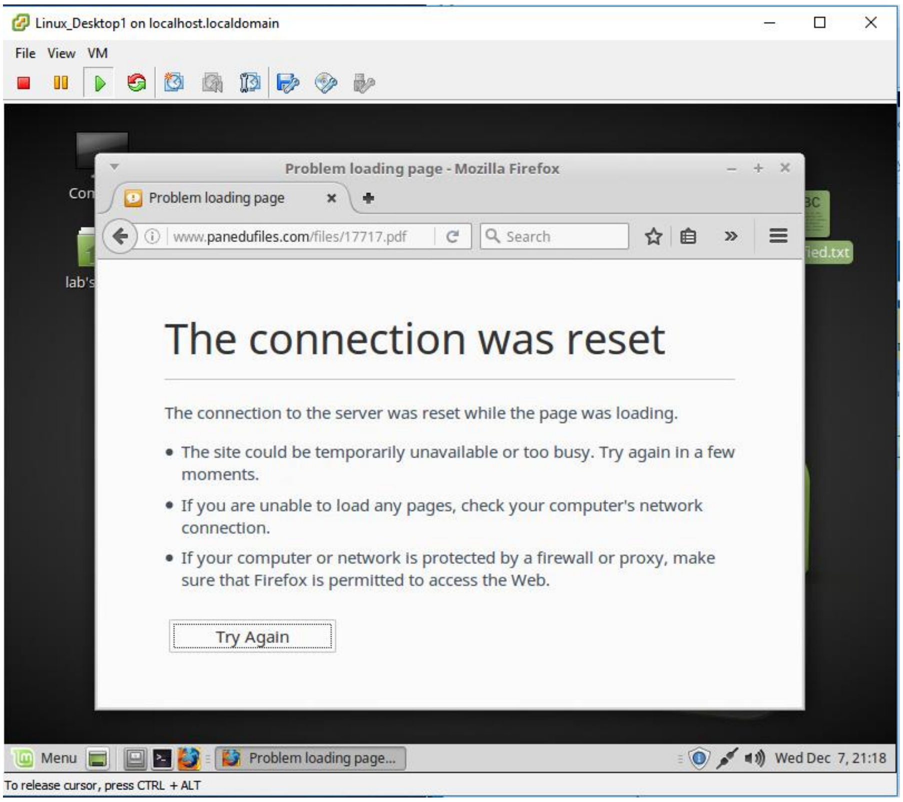
Figur 23 screen shot for testing

Figure23 We don’t get any progress because the file contains the pattern we don’t allow

Lab 12. Custom Vulnerability Signatures

In Lab 12 we create a custom vulnerability signatures in concrete a PDF file. We go to Object-> Custom Objects -> Vulnerability. We fulfill the different parameters we need in the Configuration and Signature section.
Now we need to apply this new object in our Security Policy Rule in the Action tab and commit.

Testing: We try to access to a pdf file from our browser and we get the message “The connection was reset”. If we check on monitor threat, we will see the log as a high severity because we specify it.



Linux_Desktop1 on localhost.localdomain
File View VM
Problem loading page - Mozilla Firefox
Problem loading page
www.panedufiles.com/files/17717.pdf
Search
Menu
Problem loading page...
Wed Dec 7, 21:18
To release cursor, press CTRL + ALT

The connection was reset

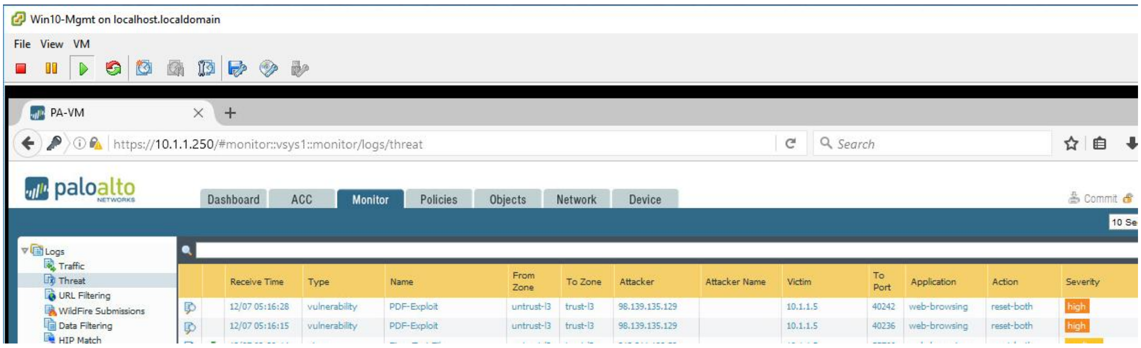
The connection to the server was reset while the page was loading.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again

Figur 24screen shot for testing open PDF

Figure24 We are not able to open this pdf file because we blocked



Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity
12/07 05:16:28	vulnerability	PDF-Exploit	untrust-l3	trust-l3	98.139.135.129		10.1.1.5	40242	web-browsing	reset-both	high
12/07 05:16:15	vulnerability	PDF-Exploit	untrust-l3	trust-l3	98.139.135.129		10.1.1.5	40236	web-browsing	reset-both	high

Figur 25 screen shot for monitor traffic

Figure25 Logs blocking the pdf file and with high severity.

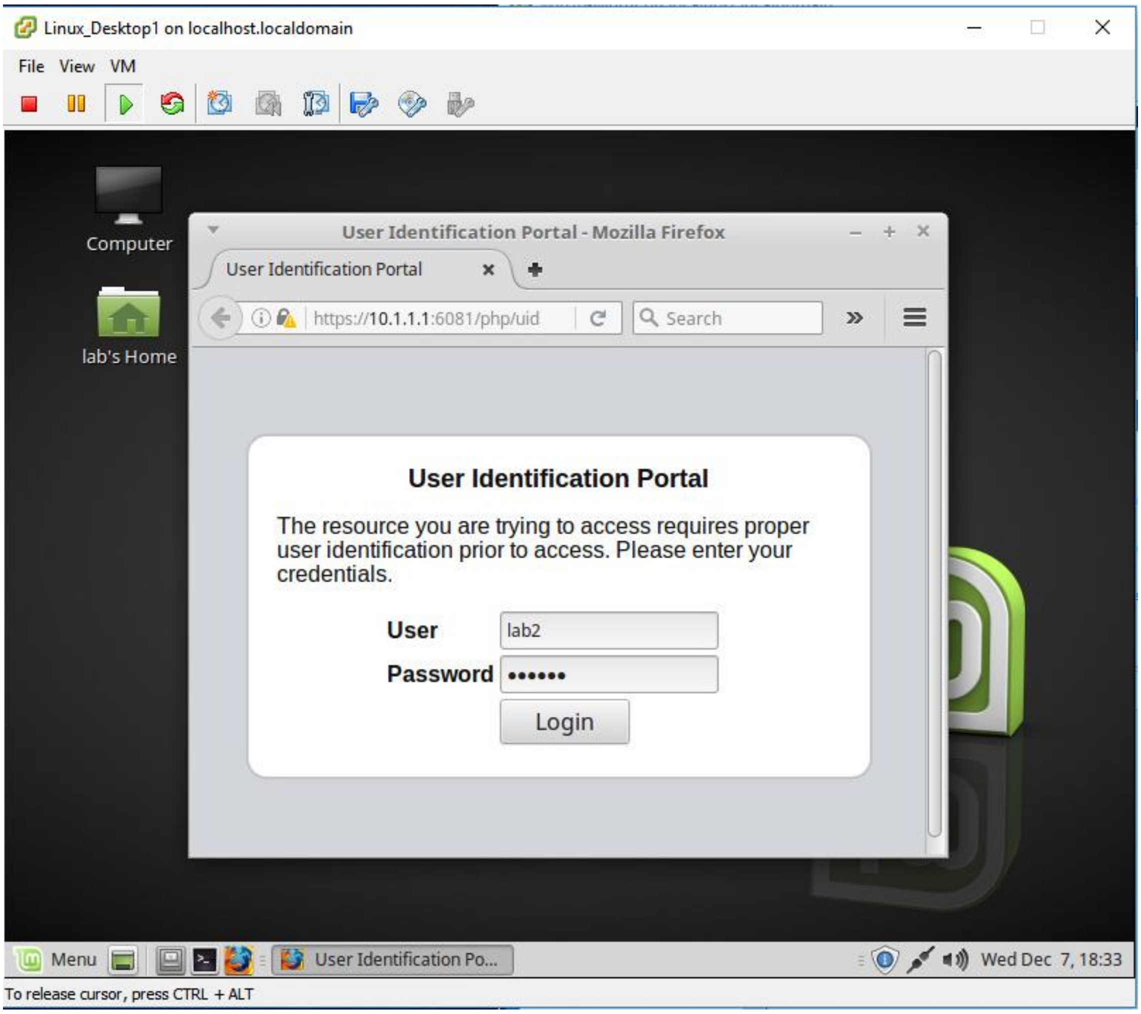
Lab 13. Advanced User-ID

In Lab 13 we start creating ad Local User Database with a user name and password for each user. After we in network we Enable User Identification in Network zones and we choose the zone we want to enable the user identification.

In Device -> User identification section we need to Enable Captive Portal and fill in the parameters we need.

In the end we need to go to Policies -> Captive Portal and specify the source TRUST in this case and the destination UNTRUST choose the Service/URL Category and Action web-form.

Testing: When we open our browser the first that we see is a window asking for a user name and password.



Linux_Desktop1 on localhost.localdomain
File View VM
Computer
lab's Home
User Identification Portal - Mozilla Firefox
User Identification Portal
https://10.1.1.1:6081/php/uid
Search
Menu
User Identification Po...
Wed Dec 7, 18:33
To release cursor, press CTRL + ALT

User Identification Portal

The resource you are trying to access requires proper user identification prior to access. Please enter your credentials.

User lab2

Password ••••••

Login

Figur 26 screen shot show testing for Captive portal

Figure26 Captive portal example