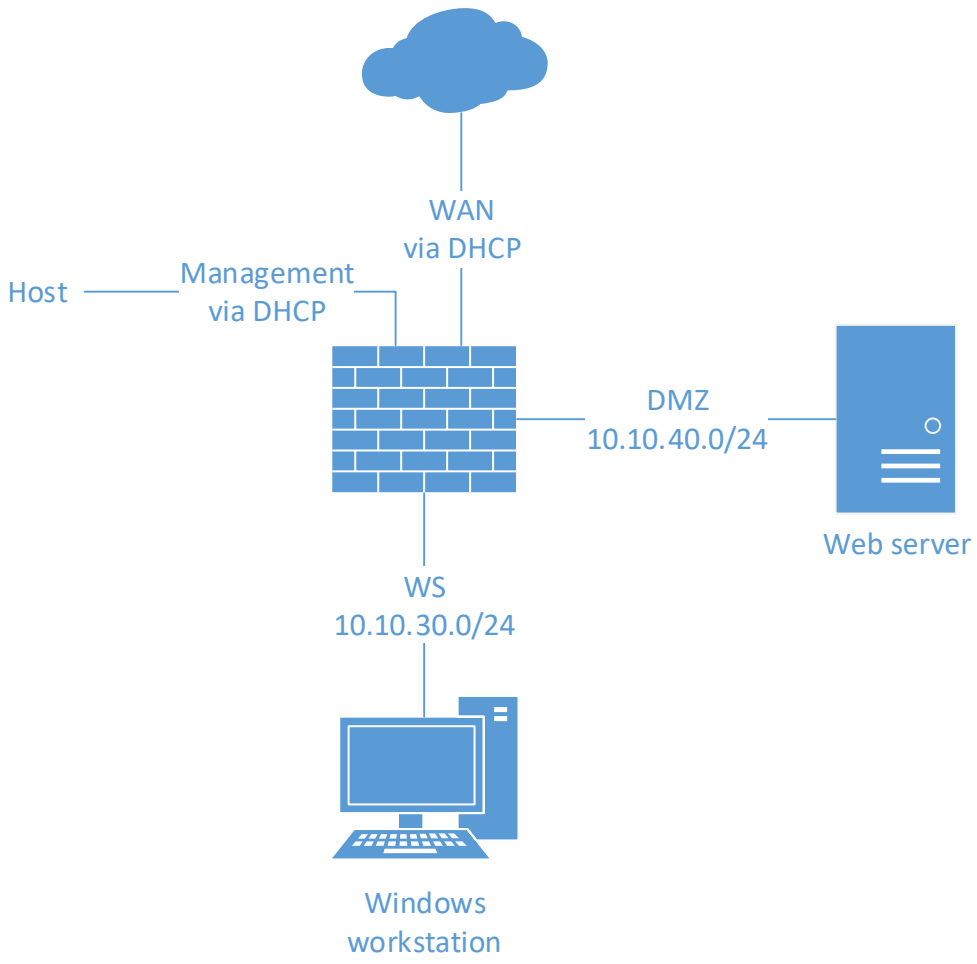
Lab12 – Paloalto basics

Document your commands or take screenshots. Answer questions in english or finnish.

Credentials:

- Paloalto: admin/admin
- Workstation W7: User/Root-66
- Server (Centos7): root/root66

The lab uses the following topology:



Install Paloalto

Retrieve the bundled image consisting pre-installed Paloalto and the web server VMs from \\ghost.labranet.jamk.fi\virtuaalikoneet\TTKS\PANOS_LABRA. Then, import the Paloalto.ova image to VirtualBox. In addition, use i.e. Kali Linux from the previous labs as a workstation. Check that interfaces are set as following:

Paloalto:

- Adapter 1: NAT
- Adapter 2: Bridged
- Adapter 3: Internal Network (WS)
- Adapter 4: Internal Network (DMZ)

Other VM networks:

- Workstation VM: Internal Network (WS)
- Web server VM: Internal Network (DMZ)

Remember to generate new MAC addresses for every interface! (MAC Address Policy)

Find out and what is the management IP address of Paloalto. First, login to the console using credentials admin/admin and then execute the following command:

show interface management

```
Ip address: 10.0.2.15
Netmask: 255.255.255.0
Default gateway: 10.0.2.2
Ipv6 address: unknown
Ipv6 link local address: fe80::a00:27ff:fe04:353e/64
Ipv6 default gateway:
```

ip osoite on 10.0.2.15

It is worth of noticing that it takes a while before you can actually login, be patient! Before we can access and manage Paloalto we need to create a new port forwarding rule. On VirtualBox, select ***Paloalto VM***, ***Settings***, ***Network***, ***Adapter 1***, ***Advanced***, ***Port Forwarding***. Create a new rule with following details:

- Name: Lab 12
- Protocol: TCP
- Host IP: 127.0.0.1
- Host Port: 443
- Guest IP: <management-ip-address>
- Guest Port: 443

Name	Protocol	Host IP	Host Port	Guest IP	Guest Port
Lab 12	TCP	127.0.0.1	443	10.0.2.15	443

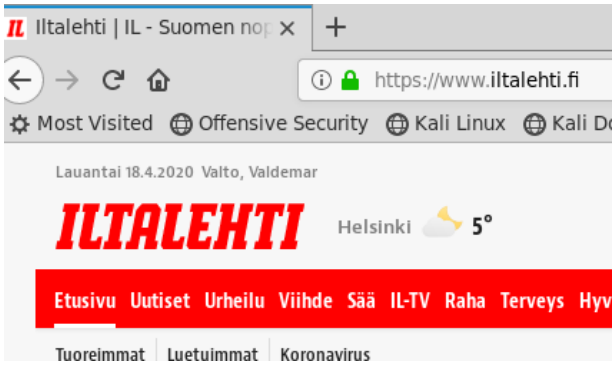
Tein port forward säännöt

Now we should be able to connect to the Paloalto's web-based graphical user interface using host machine's browser and https://localhost as a URL. Remember to use HTTPS! Before retrieving the login page, the browser should inform you that the connection isn't secure. Add exception.

Login to Paloalto from browser using credentials admin/admin. Then, choose ***Network*** tab and ***Virtual Routers*** from there. Select ***default***, ***Static Routes***, and ***Default GW***. Change the Next Hop address to same address that the host machine uses as default gateway. Remember to commit the changes!

vaihdoin osoitteen vastaamaan oman koneen default gatewayta

Boot up both the workstation and the web server VMs. Check that they get an IP address via DHCP. When you get the IP addresses, try to access www.iltalehti.fi with workstation's browser. Do the same with the web server. There isn't browser, but try the following command:



wget iltasanomat.fi

```
Connecting to iltasanomat.fi (iltasanomat.fi)|13.32.43.14|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.is.fi/ [following]
--2020-04-18 20:00:06--  https://www.is.fi/
Resolving www.is.fi (www.is.fi)... 13.32.43.90, 13.32.43.60, 13.32.43.40, ...
Connecting to www.is.fi (www.is.fi)|13.32.43.90|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 134264 (131K) [text/html]
Saving to: 'index.html.2'

100%[===================================>] 134,264      --.-K/s    in 0.1s

2020-04-18 20:00:07 (924 KB/s) - 'index.html.2' saved [134264/134264]

[root@localhost.localdomain ~]# _
```

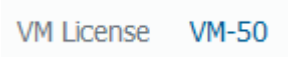
nmnettiyhteydet toimii

If there are wrong DNS Resolvers set for the Paloalto, change them from: ***Device***, ***Setup***, ***Services*** to be:

- 192.168.40.21
- 192.168.40.22

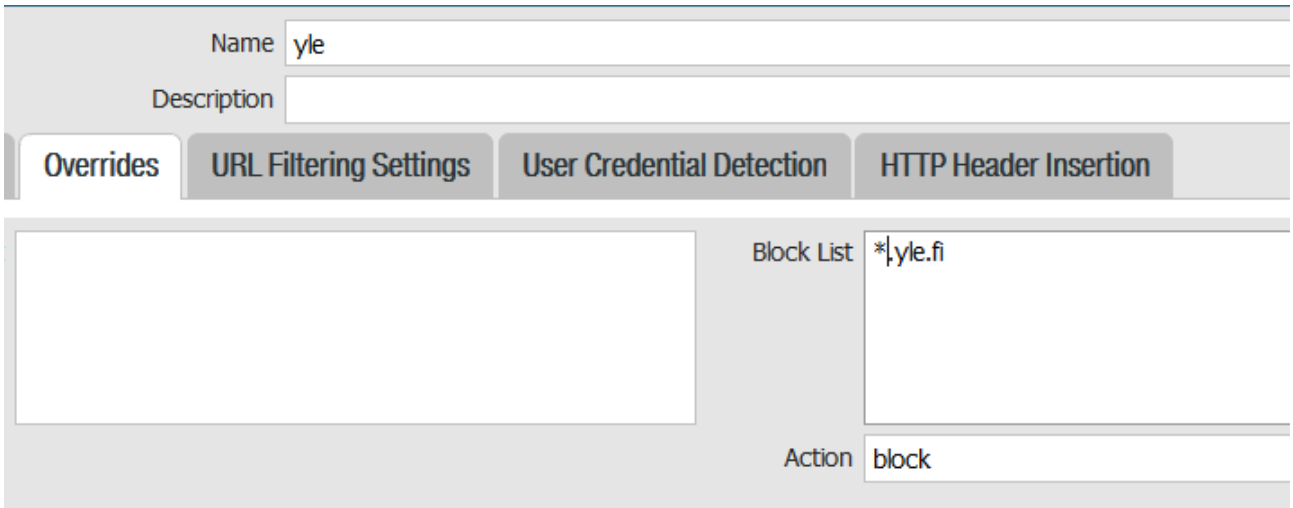
- **License + URL FILTERING**

Next, go to ***Device***, ***Licenses***, ***Activate feature using authorization code***. Use the following authorization code: `I2224713`. It is worth of noticing that the activation will reboot Paloalto. When rebooted, check the version of the license from ***Dashboard*** (VM-xx).



tarkistin lisenssin

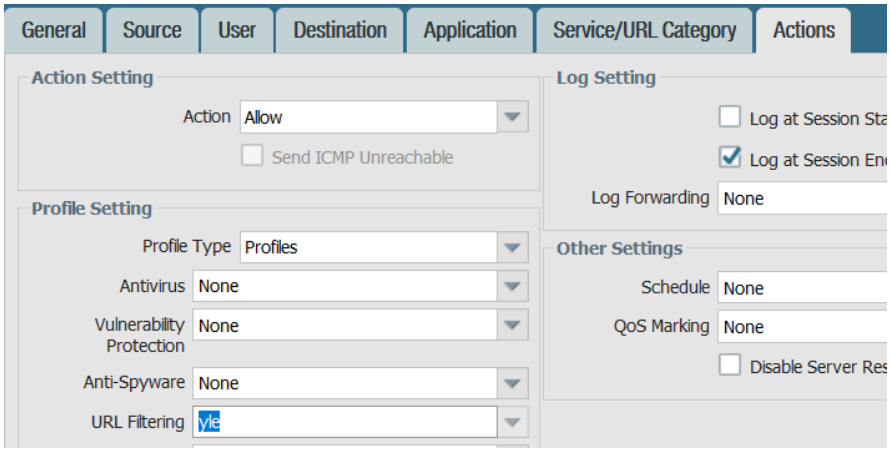
Next, try to figure out how to do URL filtering (Hint: ***Objects***, ***Security Profiles***, ***URL Filtering, +Add, Overrides***). In this lab we want to block yle.fi and all its subdomains. Try also to block site access to specific category i.e. gambling on ***Categories*** tab.



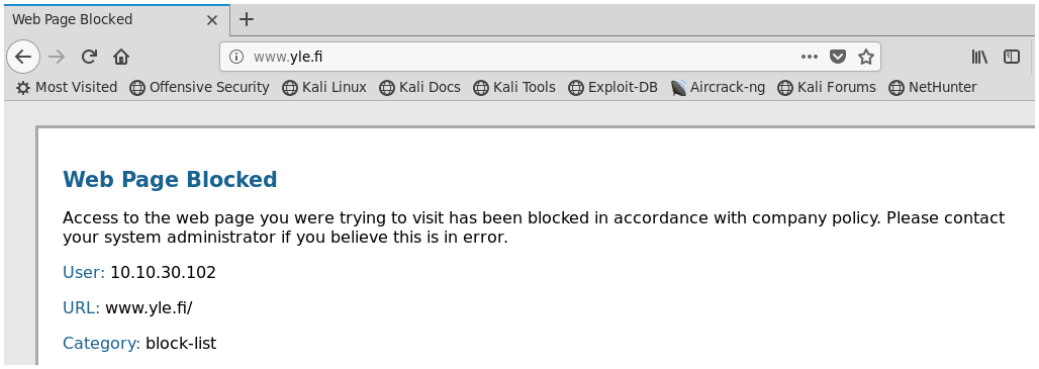
yle blokittu

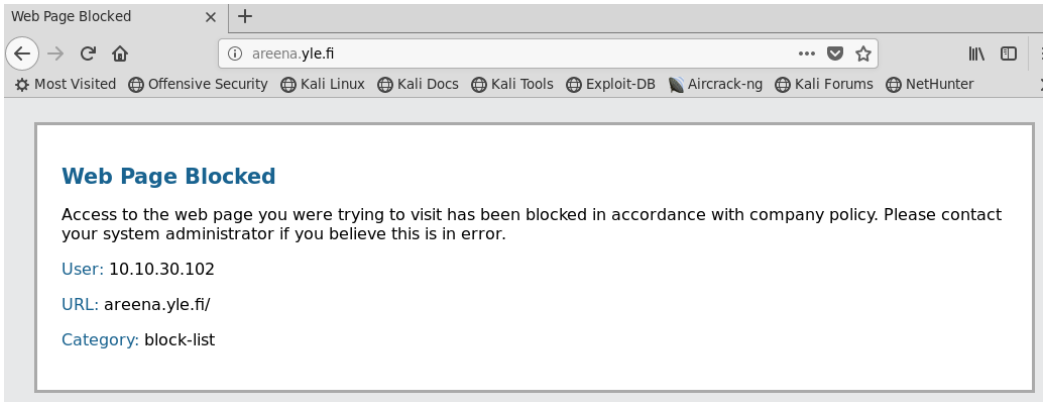
gambling blockitty

Then configure the created URL filtering policy as the profile of ***Default-allow-any*** security policy.

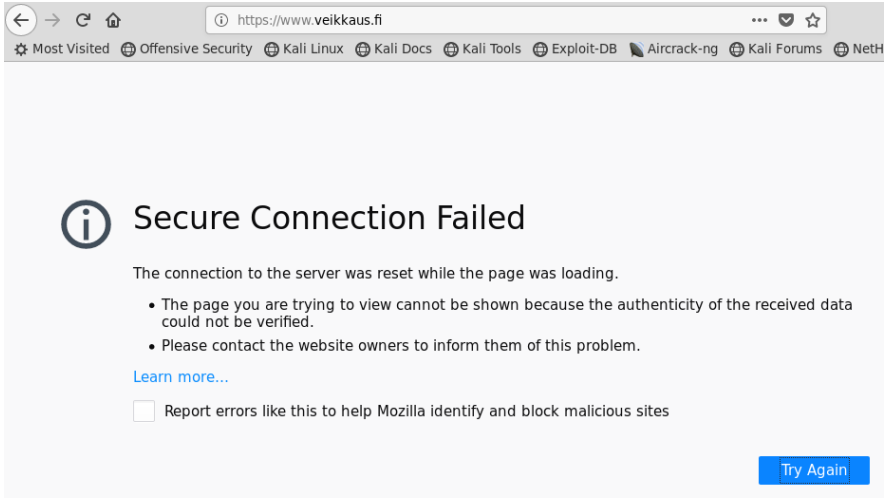


Again, remember to commit your changes to make them effective! Finally, verify effectiveness of your configurations by taking a screenshot from both blocked sites http://www.yle.fi and the site that belongs to the prohibited category. Take also a screenshot from the URL filtering log (***Monitor***, ***Logs***, ***URL Filtering***).





yle blokittu



vissiin toimii koska en pääse millekkään uhkapelisivustolle?

	Receive Time	Category	URL	From Zone	To Zone	Source	Source User	Destination	Application	Action	H
	04/18 16:46:37	block-list	areena.yle.fi/	WS	WAN	10.10.30.102		13.32.43.84	web-browsing	block-url	
	04/18 16:46:34	block-list	www.yle.fi/	WS	WAN	10.10.30.102		13.32.43.60	web-browsing	block-url	
	04/18 16:44:39	block-list	areena.yle.fi/favicon.ico	WS	WAN	10.10.30.102		13.32.43.84	web-browsing	block-url	
	04/18 16:44:39	block-list	areena.yle.fi/favicon.ico	WS	WAN	10.10.30.102		13.32.43.84	web-browsing	block-url	
	04/18 16:44:39	block-list	areena.yle.fi/	WS	WAN	10.10.30.102		13.32.43.84	web-browsing	block-url	
	04/18 16:43:08	block-list	www.yle.fi/areena	WS	WAN	10.10.30.102		13.32.43.60	web-browsing	block-url	
	04/18 16:43:04	block-list	www.yle.fi/	WS	WAN	10.10.30.102		13.32.43.60	web-browsing	block-url	
	04/18 16:39:55	gambling	www.mrgreen.com/	WS	WAN	10.10.30.102		13.32.43.119	ssl	block-url	
	04/18 16:39:55	gambling	www.mrgreen.com/	WS	WAN	10.10.30.102		13.32.43.119	ssl	block-url	
	04/18 16:39:55	gambling	www.mrgreen.com/	WS	WAN	10.10.30.102		13.32.43.119	ssl	block-url	

logeja

- ## Firewall Rules

Web server has Apache running on it, so create a new security policy rule which allows you to browse from workstation to it. You need to make a new security policy rule, which allows web-browsing to be made from WS source zone to DMZ destination zone. Remember to commit the changes.

Web server has also SSH server running on it. Create a new security policy rule so you can take SSH connection from the workstation to web server. Remember to commit the changes.

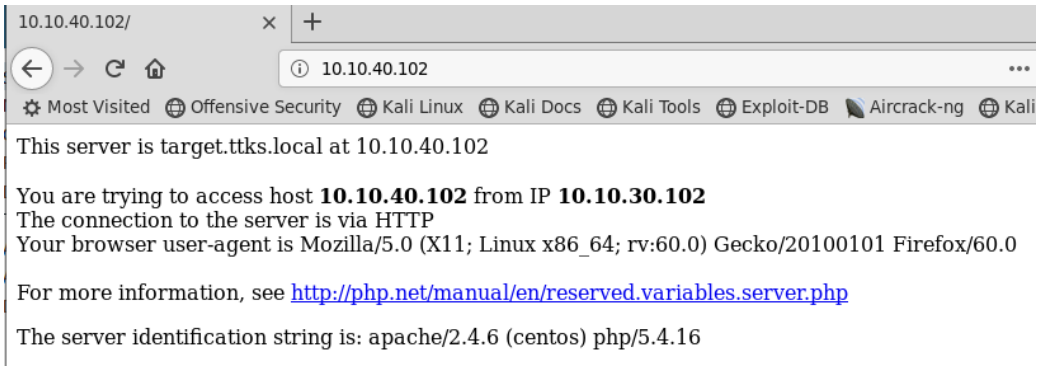
Verify both of the security policy rules with a screenshot. In addition, take a screenshot from both workstation's browser when the web server is accessed, and Putty client after the SSH connection to the web server has been established.

				Source				Destination		Rule Usage	
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit
1	Default-allow-any	none	universal	DMZ WS	any	any	any	WAN	any	10943	2020-04-18 16:57:18
2	ws-to-dmz	none	universal	WS	any	any	any	DMZ	any	3	2020-04-18 16:55:55
3	ws-to-dmz-ssh	none	universal	WS	any	any	any	DMZ	any	0	-

policy rules part1

First Hit	Application	Service	Action	Profile	Options
2020-01-16 05:47:13	any	application-d...	Allow		
2020-04-18 16:55:55	any	application-d...	Allow	none	
-	any	ssh	Allow	none	
2020-04-18 16:57:04	any	any	Allow	none	none
-	any	any	Deny	none	none

part2



yhteys kalilta serverille

- **WWW NAT**

In this lab we configure a port forward -based NAT. Incoming connection to port 80 from the WAN address will be forwarded to the web server.

First you need to create two address objects, so go to ***Objects***, ***Addresses***.

Add two objects, webserver-private and webserver-public, and for the webserver-private object set the IP address to be your web server's IP address. For the webserver-public object set the IP address to be the same that you have on the ethernet1/1 interface (***Network***, ***Interfaces***, ***ethernet 1/1***, ***IPv4***, ***Show DHCP Client Runtime Info***). Again, commit the changes.

To get NAT working properly you need to create two policy rules, NAT and Security, which utilizes the previously created objects.

NAT rule

General – Name: WWW NAT from WAN to DMZ
Original Packet:

- Source Zone: WAN
- Destination Zone: WAN
- Destination Interface: ethernet 1/1
- Service: service-http
- Source Address: any
- Destination Address: webserver-public

Translated Packet – Destination Address Translation:

- Translation Type: Static IP
- Translated Address: webserver-private
- Translated Port: 80

<u>Security rule</u>

General – Name: Allow WWW NAT from WAN to DMZ
Source – Source Zone: WAN
Destination – Destination Zone: DMZ
Destination – Destination Address: webserver-public
Application – Applications: web-browsing

Remember to commit the changes. Verify with screenshot that you can connect to the web server using your host computer's browser and IP address of the ethernet 1/1 interface (port 80).

- **SSH NAT**

Next we want to configure NAT policies also for the SSH. You can use almost the same configurations for the SSH NAT that you used for the WWW NAT; however, some of steps needs to be modified such as the used service, translated port, and application. Verify with a screenshot that you can establish SSH connection to the web server from your host computer using i.e. Putty SSH client.