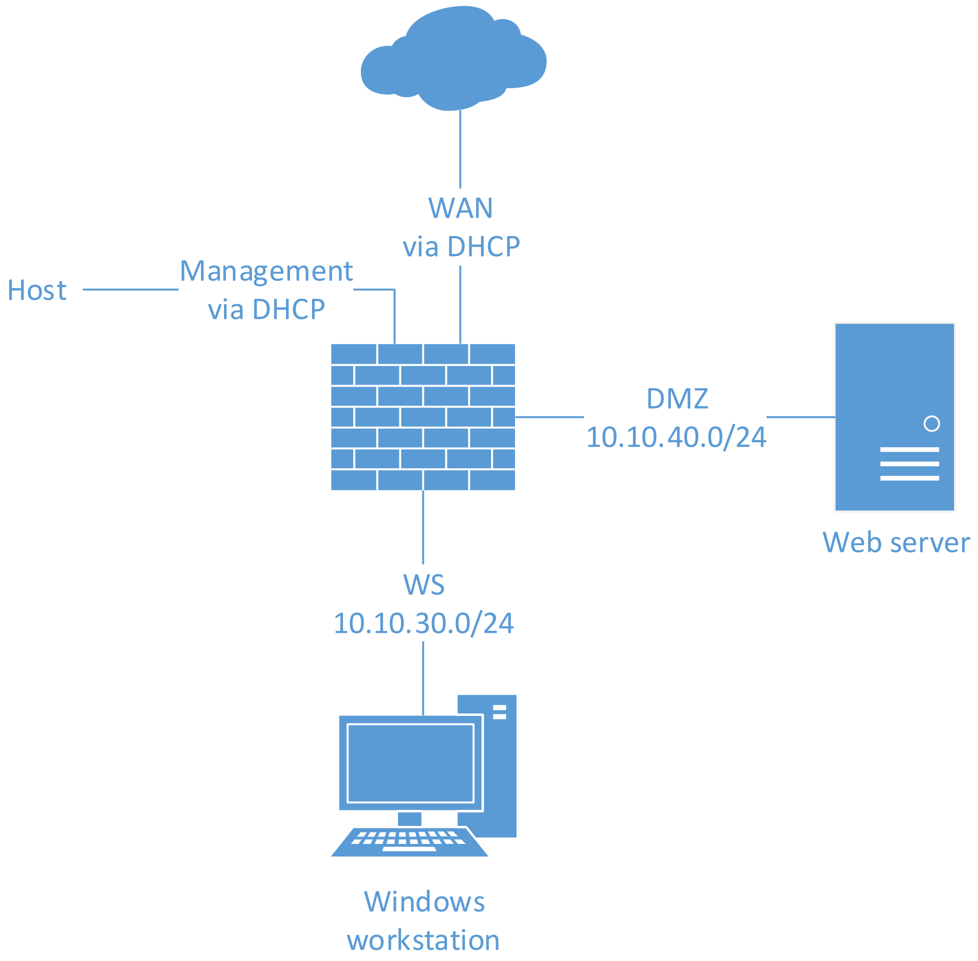
Lab12 – Paloalto basics

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, Windows workstation, and the web server VMs from \\ghost.labranet.jamk.fi\virtuaalikoneet\TTKS\PANOS_LABRA. Then, import the Paloalto.ova image to VirtualBox. Check that interfaces are set as following:

Paloalto:

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

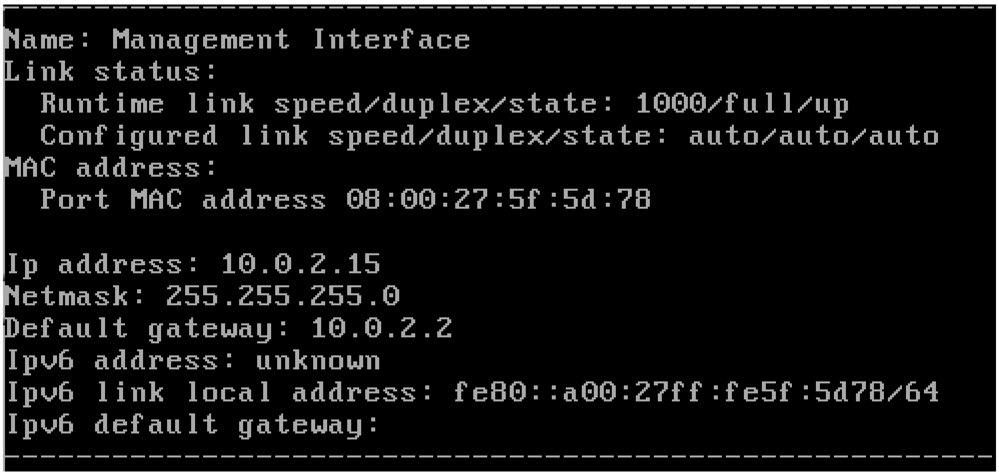
Other VM networks:

- Workstation VM: Internal Network (WM)
- 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

- 

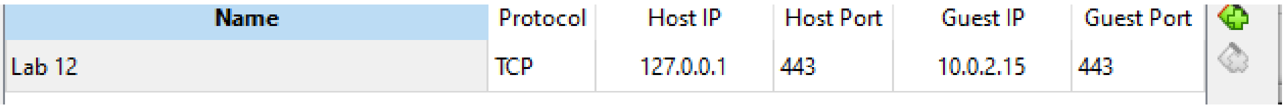
```
-------------------------------------------------------
Name: Management Interface
Link status:
  Runtime link speed/duplex/state: 1000/full/up
  Configured link speed/duplex/state: auto/auto/auto
MAC address:
  Port MAC address 08:00:27:5f:5d:78

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:fe5f:5d78/64
Ipv6 default gateway:
-------------------------------------------------------
```

- ***ip = 10.0.2.15***
- ***default gateway = 10.0.2.2***

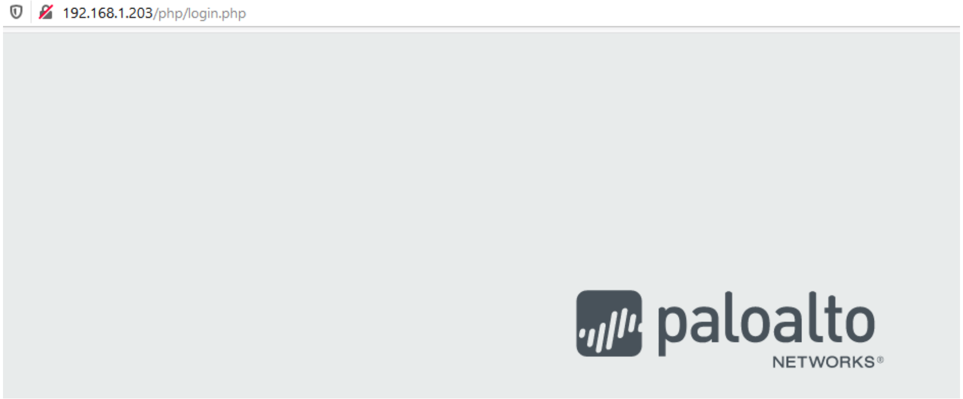
It is worth of noticing that it takes a while before you can actually login, be patient! Before we can access and manage Paloalto we need to create a new port forwarding rule. On VirtualBox, select ***Paloalto VM***, ***Settings***, ***Network***, ***Adapter 1***, ***Advanced***, ***Port Forwarding***.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

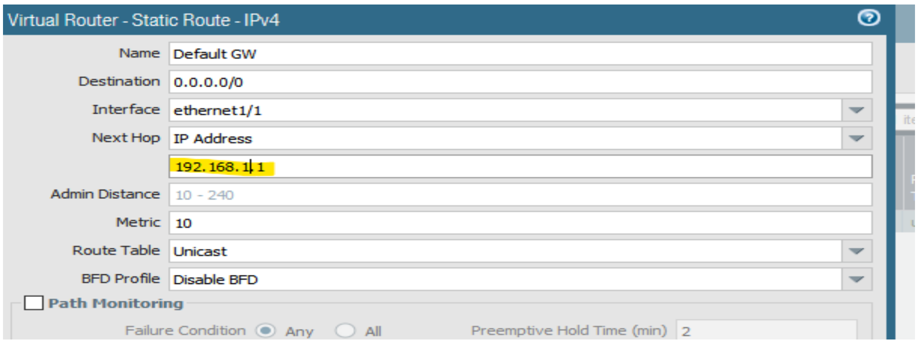
Now we should be able to connect to the Paloalto's web-based graphical user interface using host machine's browser and https://localhost as a URL. Remember to use HTTPS! Before retrieving the login page, the browser should inform you that the connection isn't secure. Add exception.



192.168.1.203/php/login.php

- en päässyt tuolla localhostilla, mutta pääsin oman sisäverkon ip-osoitteella, jota paloalto käyttää

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!



Virtual Router - Static Route - IPv4

Name	Default GW
Destination	0.0.0.0/0
Interface	ethernet1/1
Next Hop	IP Address
	192.168.1.1
Admin Distance	10 - 240
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

□ Path Monitoring

Failure Condition ● Any ○ All   Preemptive Hold Time (min) 2

- hostin default gateway on 192.168.1.1

Boot up both the Windows 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 a Windows workstation's browser. Do the same with the web server. There isn't browser, but try the following command:

wget iltasanomat.fi

- *molemmilla pääsin läpi*

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

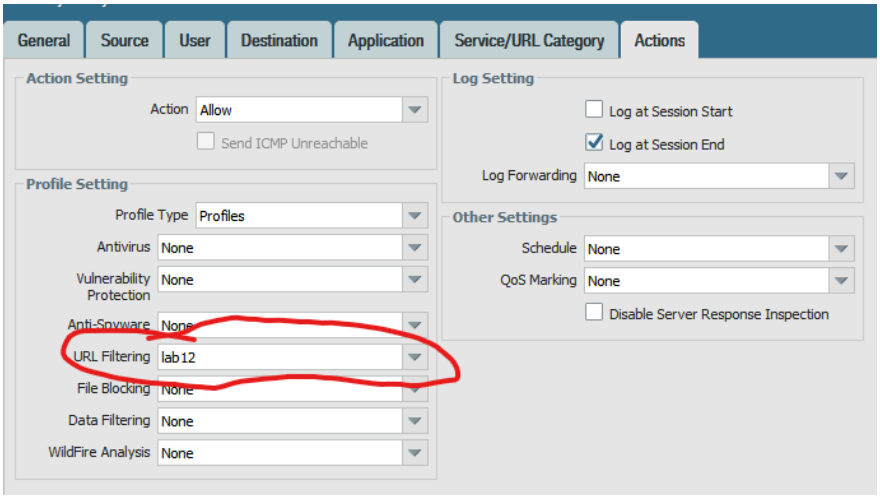
License + URL FILTERING

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).

- VM-50

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.

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!



Action Setting

Action: Allow

□ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: None

Vulnerability Protection: None

Anti-Spyware: None

URL Filtering: lab12

File Blocking: None

Data Filtering: None

WildFire Analysis: None

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Other Settings

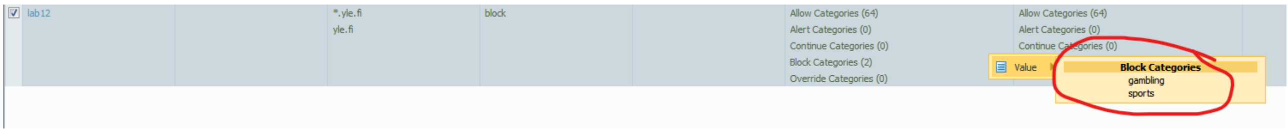
Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

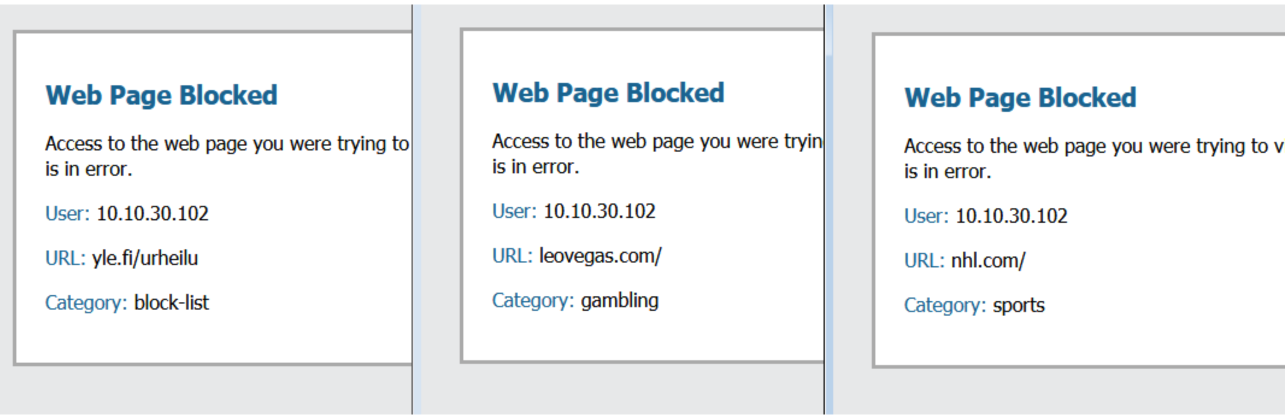
- lab 12 sääntö asetettu Default-allow-any profileen

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***).



☑ lab12		*.yle.fi yle.fi	block		Allow Categories (64) Alert Categories (0) Continue Categories (0) Block Categories (2) Override Categories (0)	Allow Categories (64) Alert Categories (0) Continue Categories (0)

- molemmat blokit olikin jo valmiiksi asetettu, ei näytä päästävän millekään ylen subdomaineistakaan.



Web Page Blocked

Access to the web page you were trying to is in error.

User: 10.10.30.102

URL: yle.fi/urheilu

Category: block-list

Web Page Blocked

Access to the web page you were tryin is in error.

User: 10.10.30.102

URL: leovegas.com/

Category: gambling

Web Page Blocked

Access to the web page you were trying to v is in error.

User: 10.10.30.102

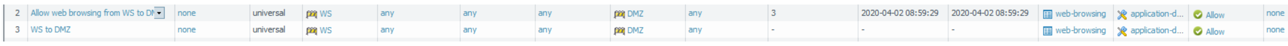
URL: nhl.com/

Category: sports

- lisäsin testiksi itse vielä urheilusivut blokkilistalle

- **Firewall Rules**

Web server has Apache running on it, so create a new security policy rule which allows you to browse from Windows 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.



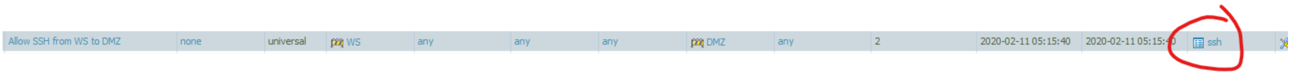
2	Allow web browsing from WS to DM	none	universal	WS	any	any	any	DMZ	any	3	2020-04-02 08:59:29	2020-04-02 08:59:29	web-browsing	application-d...	Allow	none
3	WS to DMZ	none	universal	WS	any	any	any	DMZ	any	-	-	-	web-browsing	application-d...	Allow	none

- Tämä oli valmiina kanssa. Oman saa tehtyä lisäämällä uuden säännön add, painikkeesta ja asetamalla sourceksi zoneksi WS, destination zoneksi DMZ, sekä applicationiksi web-browsing

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

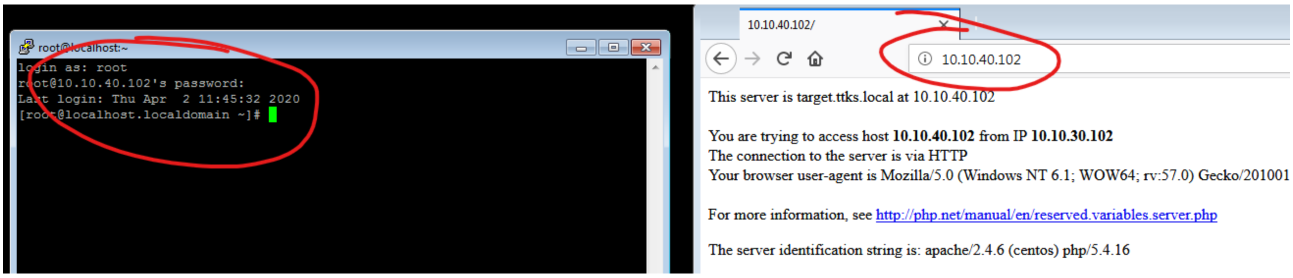
- sama homma, kun edellisessä mutta applicationiksi ssh

-



Allow SSH from WS to DMZ	none	universal	WS	any	any	any	DMZ	any	2	2020-02-11 05:15:40	2020-02-11 05:15:40	ssh

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

- 

root@localhost:~

```
login as: root
root@10.10.40.102's password:
Last login: Thu Apr  2 11:45:32 2020
[root@localhost.localdomain ~]#
```

10.10.40.102/

10.10.40.102

This server is target.ttks.local at 10.10.40.102

You are trying to access host **10.10.40.102** from IP **10.10.30.102**
The connection to the server is via HTTP
Your browser user-agent is Mozilla/5.0 (Windows NT 6.1; WOW64; rv:57.0) Gecko/201001

For more information, see http://php.net/manual/en/reserved.variables.server.php

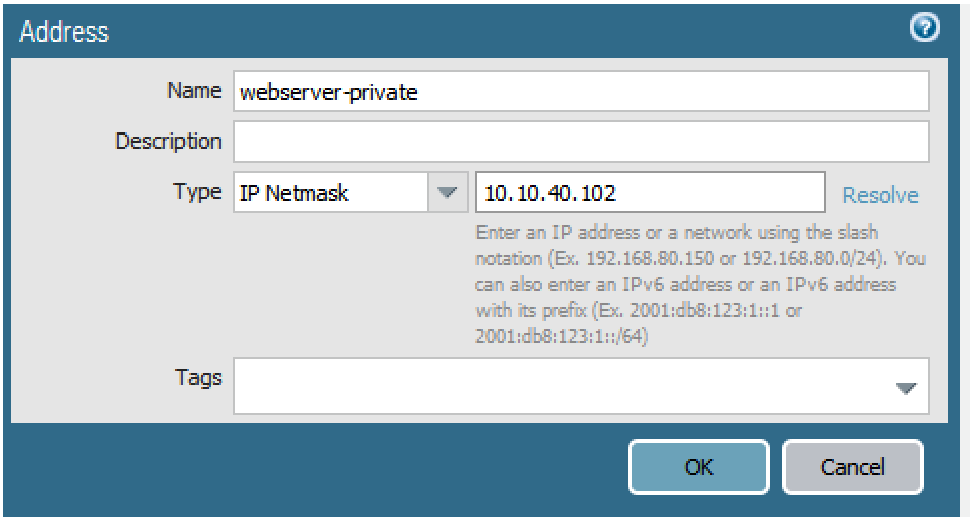
The server identification string is: apache/2.4.6 (centos) php/5.4.16

- **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.

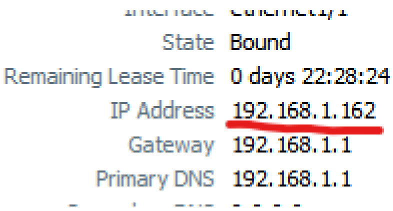


Address

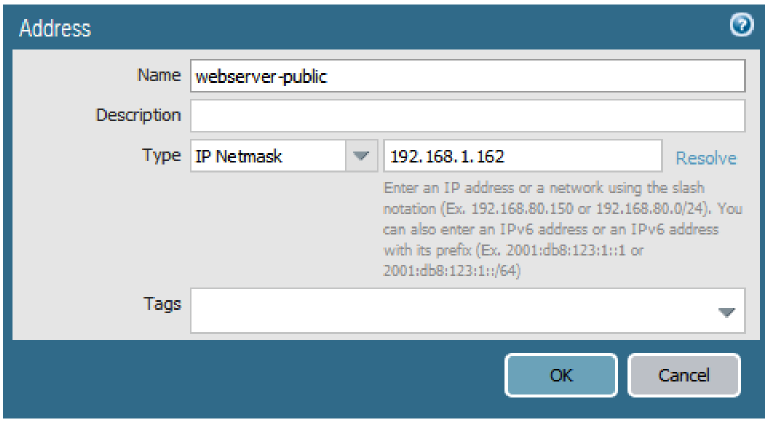
Name	webserver-private
Description	
Type	IP Netmask 10.10.40.102
Tags	

Enter an IP address or a network using the slash notation (Ex. 192.168.80.150 or 192.168.80.0/24). You can also enter an IPv6 address or an IPv6 address with its prefix (Ex. 2001:db8:123:1::1 or 2001:db8:123:1::/64)

- private object



Interface	ethernet1/1
State	Bound
Remaining Lease Time	0 days 22:28:24
IP Address	192.168.1.162
Gateway	192.168.1.1
Primary DNS	192.168.1.1



Name: webserver-public

Description:

Type: IP Netmask — 192.168.1.162

Enter an IP address or a network using the slash notation (Ex. 192.168.80.150 or 192.168.80.0/24). You can also enter an IPv6 address or an IPv6 address with its prefix (Ex. 2001:db8:123:1::1 or 2001:db8:123:1::/64)

Tags:

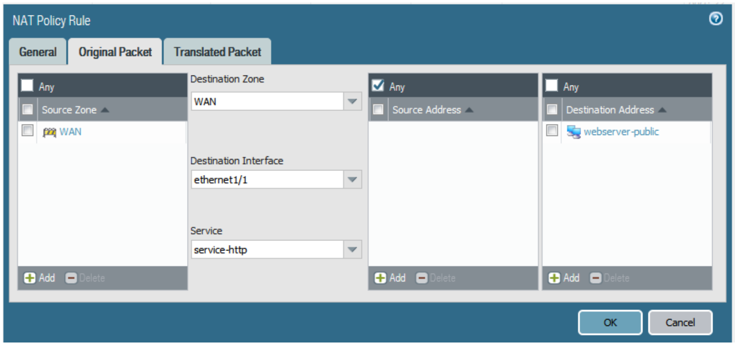
- public object

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

<u>NAT rule</u>

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



□ Any
Source Zone ▲
□ WAN

Destination Zone: WAN

Destination Interface: ethernet1/1

Service: service-http

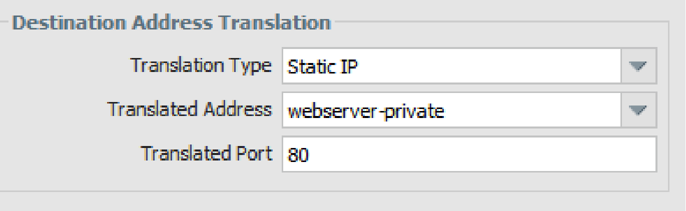
☑ Any
Source Address ▲

□ Any
Destination Address ▲
□ webserver-public

- Wan to DMZ

Translated Packet – Destination Address Translation:

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



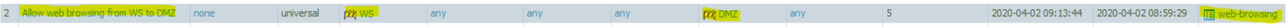
Translation Type: Static IP

Translated Address: webserver-private

Translated Port: 80

Security rule

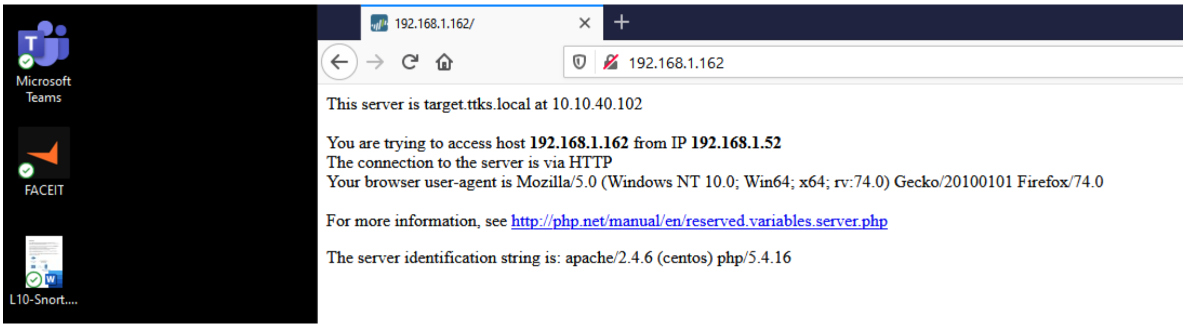
General – Name: Allow WWW NAT from WAN to DMZ
Source – Source Zone: WAN
Destination – Destination Zone: DMZ
Destination – Destination Address: webserver-public
Application – Applications: web-browsing



2	Allow web browsing from WS to DMZ	none	universal	WS	any	any	any	DMZ	any	5	2020-04-02 09:13:44	2020-04-02 08:59:29	web-browsing

- security rule

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).



This server is target.ttks.local at 10.10.40.102

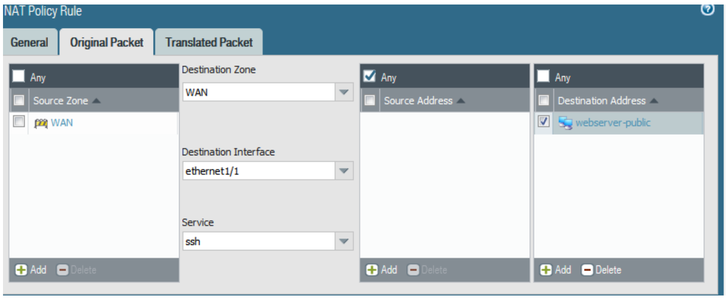
You are trying to access host **192.168.1.162** from IP **192.168.1.52**
The connection to the server is via HTTP
Your browser user-agent is Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0

For more information, see http://php.net/manual/en/reserved.variables.server.php

The server identification string is: apache/2.4.6 (centos) php/5.4.16

- **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.

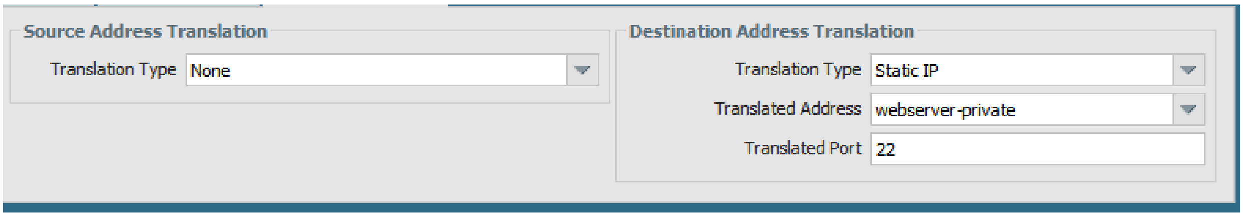


□ Any
□ Source Zone
□ WAN

Destination Zone: WAN
Destination Interface: ethernet1/1
Service: ssh

☑ Any
□ Source Address

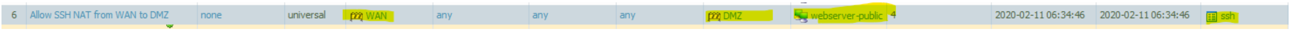
□ Any
□ Destination Address
☑ webserver-public



Source Address Translation
Translation Type: None

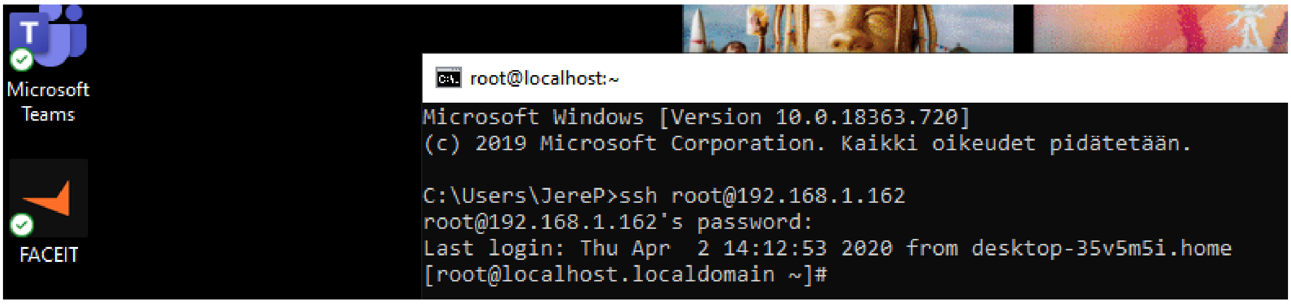
Destination Address Translation
Translation Type: Static IP
Translated Address: webserver-private
Translated Port: 22

- Nat policyn asetukset



6	Allow SSH NAT from WAN to DMZ	none	universal	WAN	any	any	any	DMZ	webserver-public	4	2020-02-11 06:34:46	2020-02-11 06:34:46	ssh

- security rulen asetukset



```
Microsoft Windows [Version 10.0.18363.720]
(c) 2019 Microsoft Corporation. Kaikki oikeudet pidätetään.

C:\Users\JereP>ssh root@192.168.1.162
root@192.168.1.162's password:
Last login: Thu Apr  2 14:12:53 2020 from desktop-35v5m5i.home
[root@localhost.localdomain ~]#
```

- Toimii!