CONFIGURATION MADE SIMPLE
LET'S CONFIG

You are here: Home » Palo Alto Firewalls » **Palo Alto Zone Based Firewall Configuration LAB**

Palo Alto Zone Based Firewall Configuration LAB

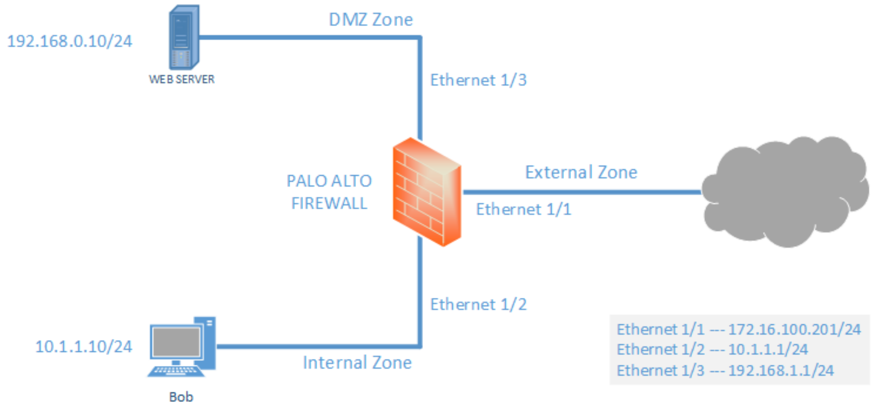
Posted on April 23, 2019 / Under Palo Alto Firewalls / With 0 Comments

Zone based firewall configuration concept in Palo Alto is similar to any other firewall. In this lesson, we will learn to configure Palo Alto Zone Based Firewall. We will be using **PAN OS 8.1.0**, and our firewall management is already configured. If you are new in Paloalto firewall, then you are recommended to check Palo Alto Networks Firewall Management Configuration.

LAB Goals:

- 3 zones for External, Internal and DMZ network and bind with appropriate interfaces
- Internal zone (LAN users) can reach Internet
- DMZ WEB server access from Internal Zone
- External people will be able to access WEB server only through NAT

LAB Diagram:



After completing this LAB, we will develop some knowledge to configure Zone, Virtual Routers, Interface Configuration, Policies, NAT and Routing (Static).

In policy section, we will allow every application and services (any) to make article short and easier for new comers. Later we will discuss in detail. So, let's get started with **Palo Alto Zone Based Firewall Configuration**.

Configuration:

Zone creating and binding to appropriate interfaces

Creating Zone:

To search type and hit enter

Email Subscribe

Name

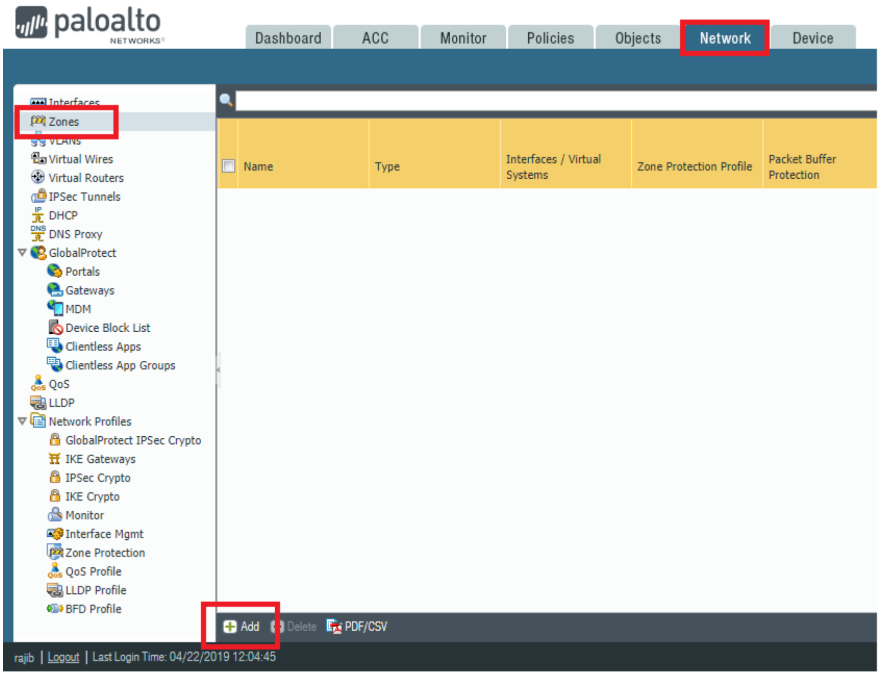
Email

Submit

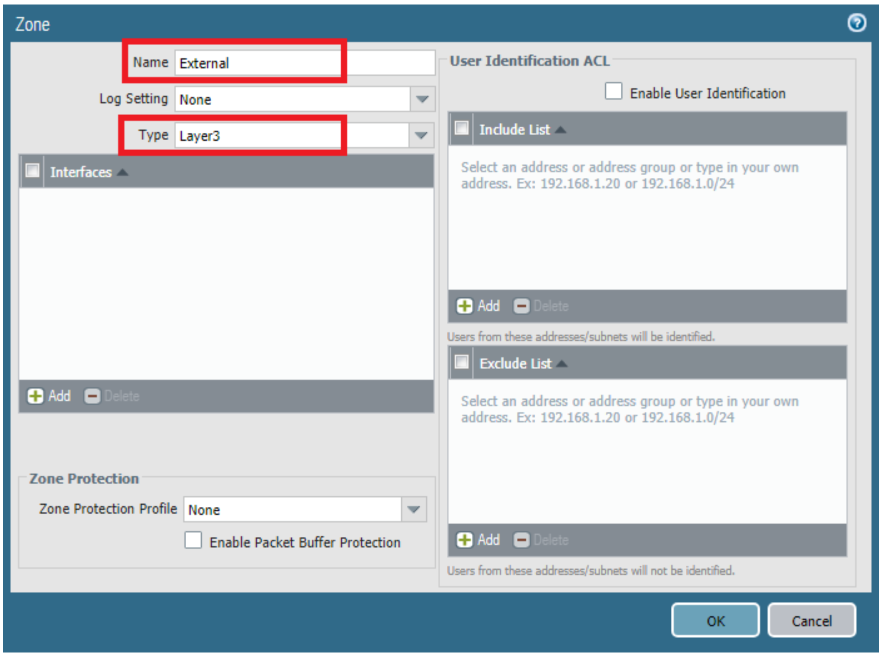
Recent Posts

How to Recover Root Password on Juniper
How to configure Site-to-Site Route based IPSec VPN on Juniper SRX
Errdisable Recovery on Cisco Switches
Managing MAC address table in Cisco
Palo Alto Zone Based Firewall Configuration LAB

To create the zone, we need to go to **Network** >> **Zones** and then click **Add**.



Now, name the Zone and select zone type. Below image shows **External** zone, creating with L3 type. Similarly, we also created other two zones named **Internal** and **DMZ** with L3 zone type.



Zone

Name: External

Log Setting: None

Type: Layer3

Zone Protection Profile: None

□ Enable Packet Buffer Protection

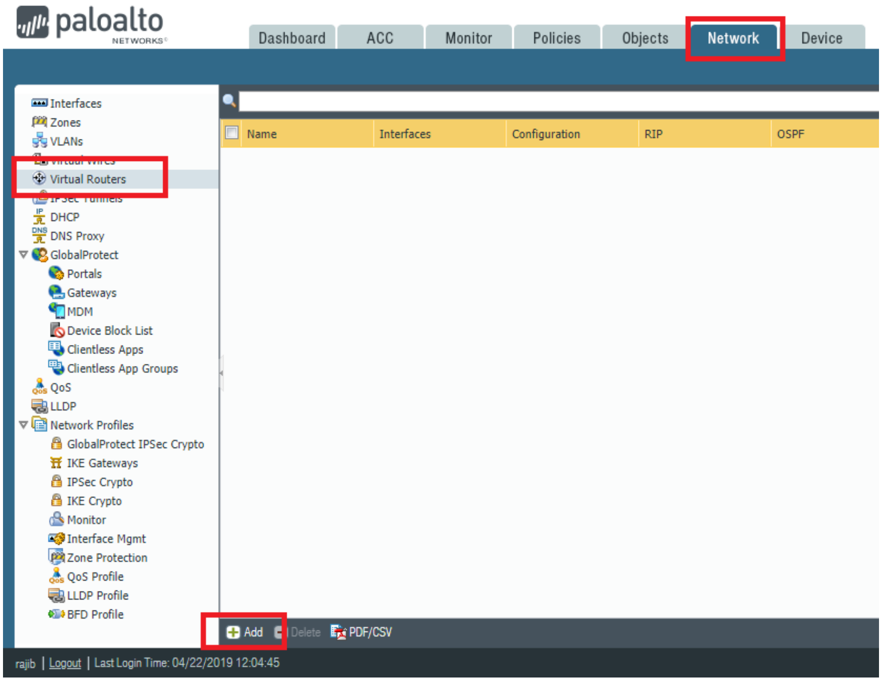
User Identification ACL

□ Enable User Identification

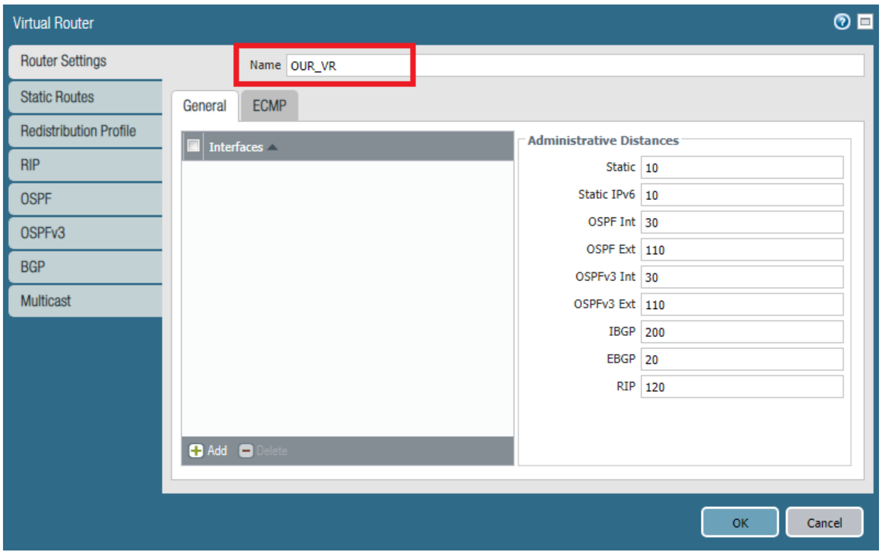
Interfaces
Add
Delete
Zone Protection
Include List
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add
Delete
Users from these addresses/subnets will be identified.
Exclude List
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add
Delete
Users from these addresses/subnets will not be identified.
OK
Cancel

Creating Virtual Routers:

To create virtual routers, we have to go **Network** >> **Virtual Routers** and then click **Add**.



You will find lots of options here, including all the routing configuration. Just name the Virtual Router, rest will be configured later. In our example, we are creating Virtual Routers name **OUR_VR**.



Name OUR_VR

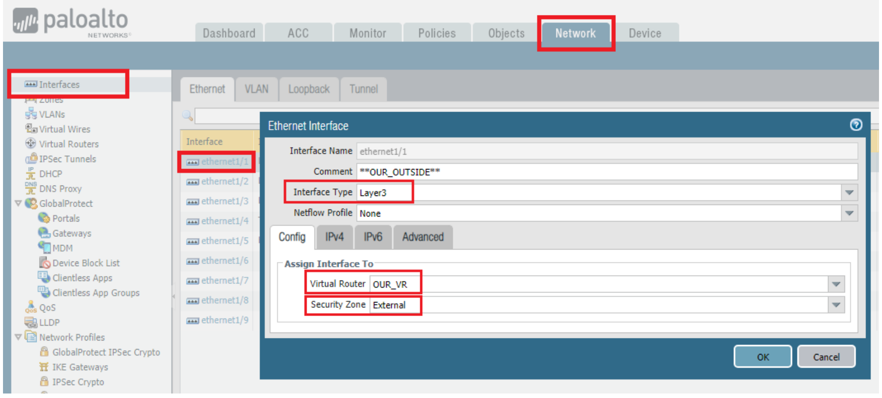
Administrative Distances

Static	10
Static IPv6	10
OSPF Int	30
OSPF Ext	110
OSPFv3 Int	30
OSPFv3 Ext	110
IBGP	200
EBGP	20
RIP	120

Interface Configuration:

For interface configuration, first of all we need to go **Network** >> **Interfaces** and then click on the interfaces.

In our example, **Ethernet 1/1** is our outside interface. So, after clicking **Ethernet 1/1**, we are giving comment (description), Interface type as **Layer3**. Then, we will assign the virtual router **OUR_VR** and zone **External**.



Ethernet Interface

Interface Name: ethernet1/1

Comment: **OUR_OUTSIDE**

Interface Type: Layer3

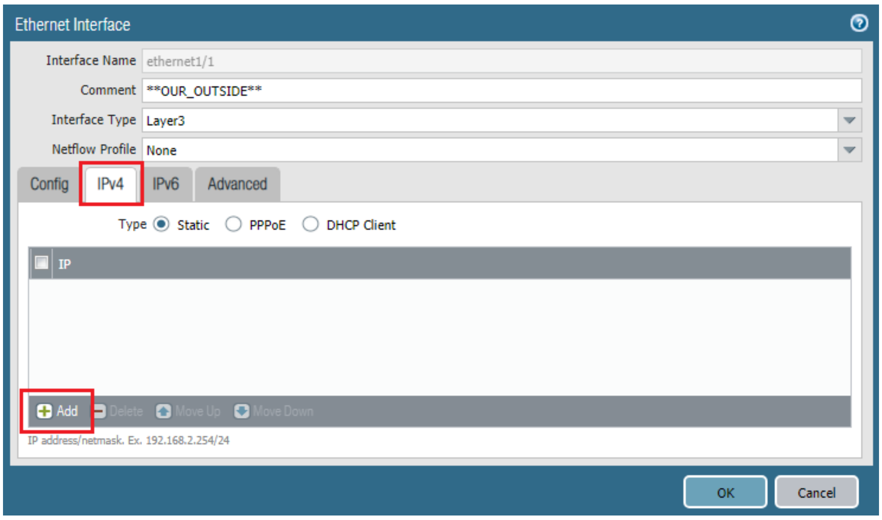
Netflow Profile: None

Assign Interface To

Virtual Router: OUR_VR

Security Zone: External

On the same page, we have to add IP address. We are using IPv4, so we are clicking on **IPv4** and adding the IP address for external interface by clicking **Add**.



Ethernet Interface

Interface Name: ethernet1/1

Comment: **OUR_OUTSIDE**

Interface Type: Layer3

Netflow Profile: None

Type ● Static ○ PPPoE ○ DHCP Client

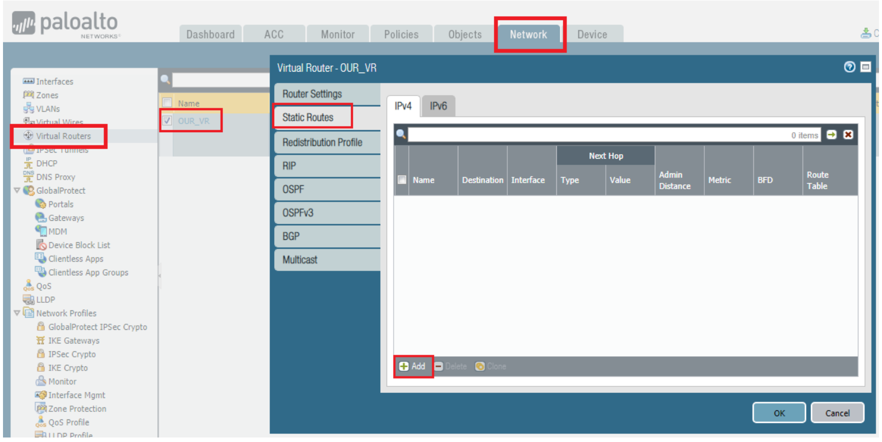
IP address/netmask. Ex. 192.168.2.254/24

Similarly, we need to do the same steps for **Internal** and **DMZ** zone to add IP addresses for them. In our LAB **10.1.1.1/24** is Internal interface IP and **192.168.1.1/24** is DMZ interface IP.

Finally, commit all the configuration by clicking **Commit** from right top corner.

Reaching Internet from Internal Zone

First of all, we need to add routing configuration. To do so, we need to go to **Network** >> **Virtual Routers** and then click newly created virtual router named **OUR_VR**.

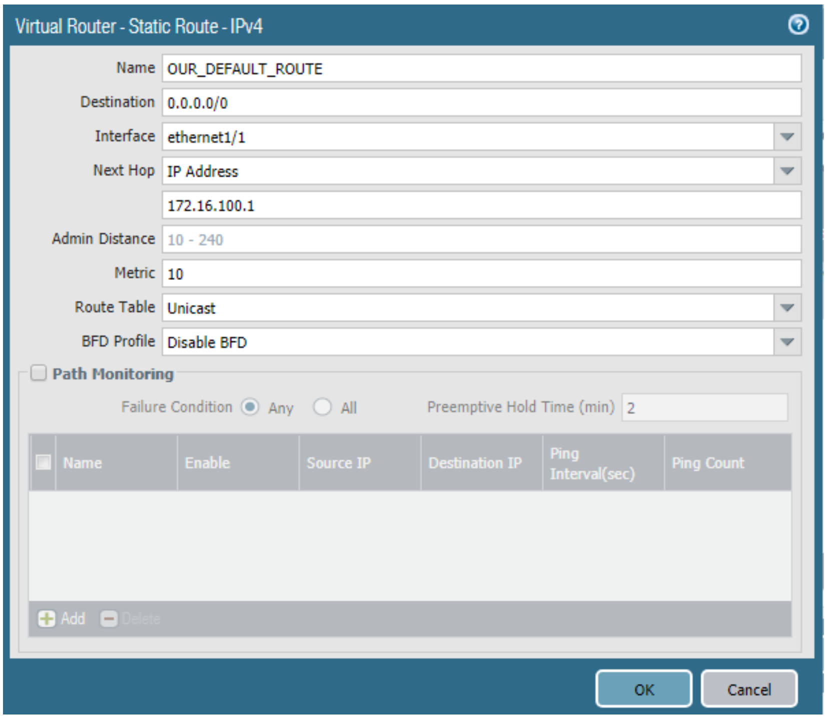


Virtual Router - OUR_VR

0 items

Name	Destination	Interface	Next Hop Type	Next Hop Value	Admin Distance	Metric	BFD	Route Table

Below are the configuration of our LAB setup.



Virtual Router - Static Route - IPv4

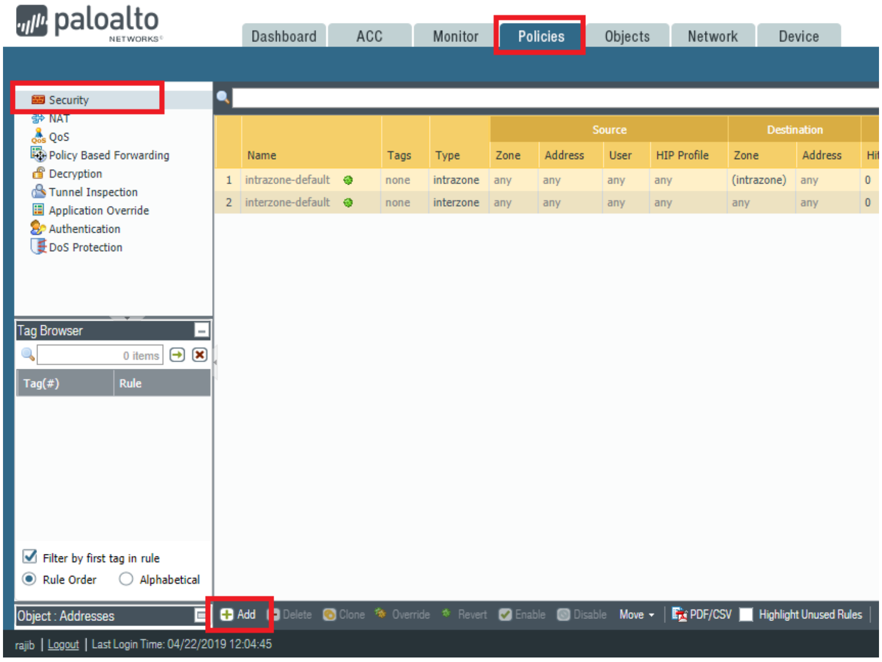
Name	OUR_DEFAULT_ROUTE
Destination	0.0.0.0/0
Interface	ethernet1/1
Next Hop	IP Address
	172.16.100.1
Admin Distance	10 - 240
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

□ Path Monitoring

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

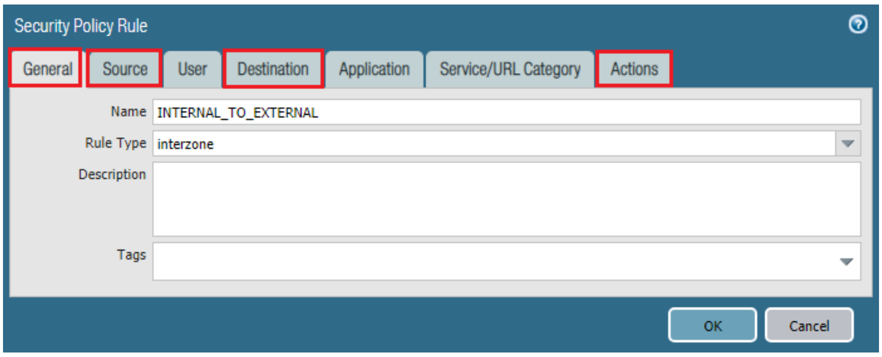
□	Name	Enable	Source IP	Destination IP	Ping Interval(sec)	Ping Count

Now, we need to configure the policy for Inside to Outside communication. By default, interzone communication is blocked.



				Source				Destination		
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hi
1	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	0
2	interzone-default	none	interzone	any	any	any	any	any	any	0

In policy, we need to configure minimum 4 section. We are configuring according below listed information.



Security Policy Rule

Name	INTERNAL_TO_EXTERNAL
Rule Type	interzone
Description	
Tags	

General:

Name: INTERNAL_TO_EXTERNAL

Rule Type: interzone

Source:
Source Zone: Internal
Source Address: 10.1.1.0/24

Destination:
Destination Zone: External
Source Address: any

Action:
Action: Allow

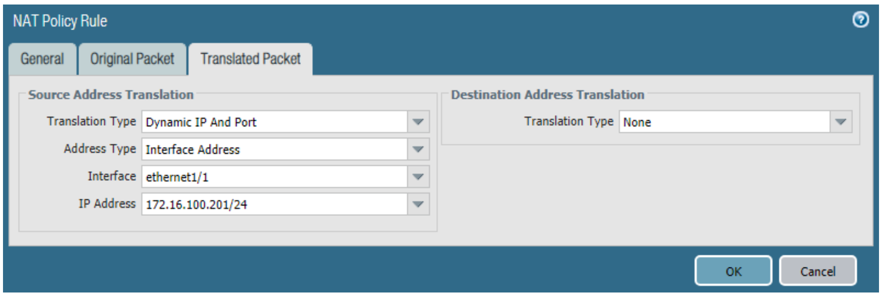
Now, we need to create NAT rule. To create go to **Policies** >> **NAT** and click **Add** to add the NAT rule.

We use below information to create the NAT rule.

General
Name: INTERNAL_TO_INTERNET

Original Packet
Source Zone: Internal
Destination Zone: External
Destination Interface: ethernet 1/1
Source Address: 10.1.1.0
Destination Address: Any

Translated Packet
(Source Address Translation)
Translation Type: Dynamic IP And Port
Address Type: Interface Address
Interface: ethernet 1/1
IP Address: 172.16.100.201/24



Source Address Translation
Translation Type: Dynamic IP And Port
Address Type: Interface Address
Interface: ethernet1/1
IP Address: 172.16.100.201/24

Destination Address Translation
Translation Type: None

Now, we need to commit all the configuration by clicking **Commit**.

Verification:

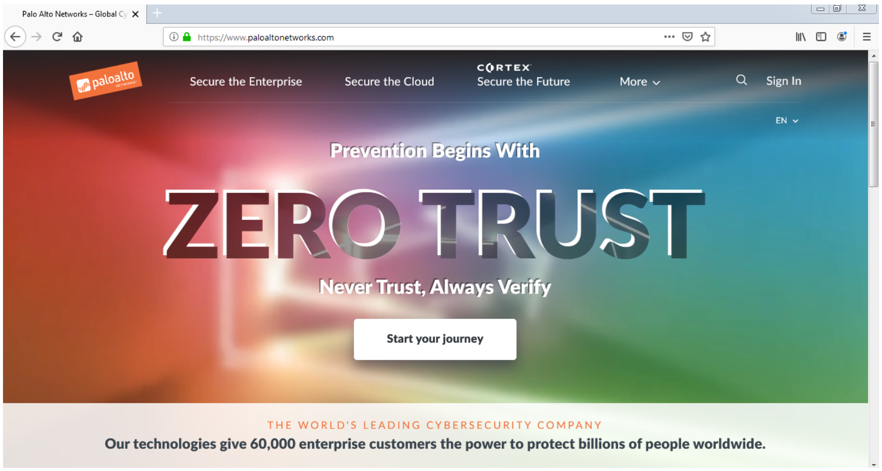
Let’s have a http request to www.paloaltonetworks.com from Internal network.

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6cf7:1072:c575:5
   IPv4 Address. . . . . . . . . . . : 10.1.1.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.1.1.1
```



Our technologies give 60,000 enterprise customers the power to protect billions of people worldwide.

Sure enough, our Internal LAN users BOB can access the internet.

WEB Server configuration on DMZ

DMZ server is connected to ethernet 1/3 interface which belong to DMZ zone. Our WEB server IP is 192.168.1.10. Now, let's create policies for communication between **INTERNAL** and **DMZ** zone.

INTERNAL to DMZ:

General:
Name: INTERNAL_TO_DMZ
Rule Type: interzone

Source:
Source Zone: Internal
Source Address: 10.1.1.0/24

Destination:
Destination Zone: External
Source Address: 192.168.1.0/24

Action:
Action: Allow

DMZ to INTERNAL

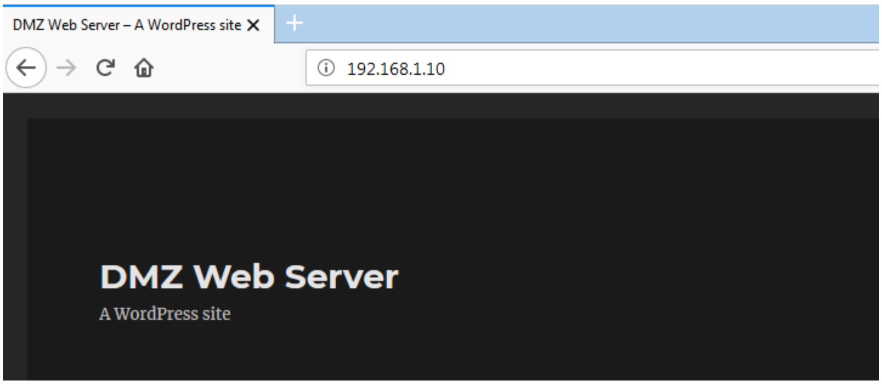
General:
Name: DMZ_TO_INTERNAL
Rule Type: interzone

Source:
Destination Zone: External
Source Address: 192.168.1.0/24

Destination:
Source Zone: Internal
Source Address: 10.1.1.0/24

Action:
Action: Allow

We can verify the result by hitting WEB server IP http://192.168.1.10 from Internal LAN PC (10.1.1.10).



DMZ Web Server – A WordPress site

192.168.1.10

DMZ Web Server

A WordPress site

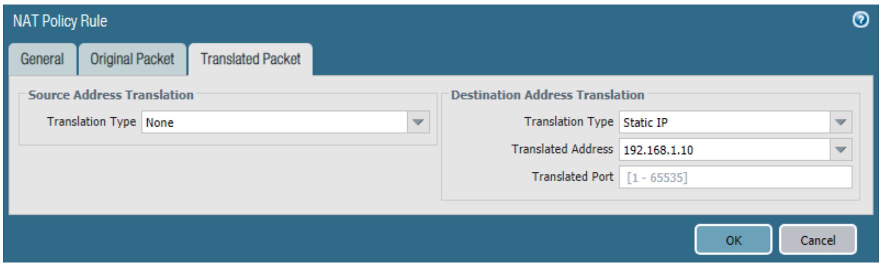
Now, time for External users. We will configure Destination NAT for outside users. To create destination NAT, we have to go **Policies** >> **NAT** and then click **Add** to add the NAT rule.

Below are our NAT configuration.

General
Name: DESTINATION_NAT

Original Packet
Source Zone: External
Destination Zone: External (it's because we will hit external IP)
Destination Interface: ethernet 1/1
Source Address: any
Destination Address: 172.16.100.199 (this is our Outside IP :P)

Translated Packet
(Destination Address Translation)
Translation Type: Static IP
Translated Address: 192.168.1.10



NAT Policy Rule

General | Original Packet | Translated Packet

Source Address Translation

Translation Type: None

Destination Address Translation

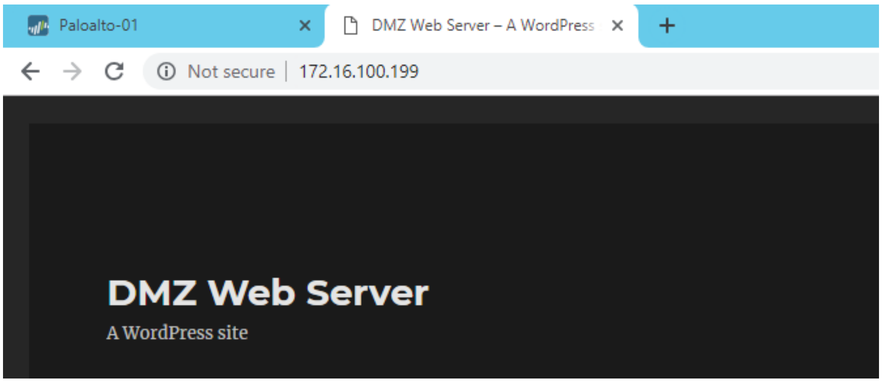
Translation Type: Static IP

Translated Address: 192.168.1.10

Translated Port: [1 - 65535]

Verification:

To verify, let's do a http request to **http://172.16.100.199** which is our WEB server external IP.



Paloalto-01

DMZ Web Server – A WordPress

Not secure | 172.16.100.199

DMZ Web Server

A WordPress site

Result looks perfect. Finally, we can reach WEB server from External Zone.

Written by Rajib Kumer Das

I am Rajib Kumer Das, a network engineer with 7+ years of experience in multi-vendor environment. In my current company, I am responsible to take care critical projects and it's support cases. I do have several vendor certificates and have plans to go further.

Leave a Comment

Your email address will not be published. Required fields are marked *

Name *

Email *

Website

Post Comment

← Managing MAC address table in Cisco

How to upgrade F5 Big-IP software version →