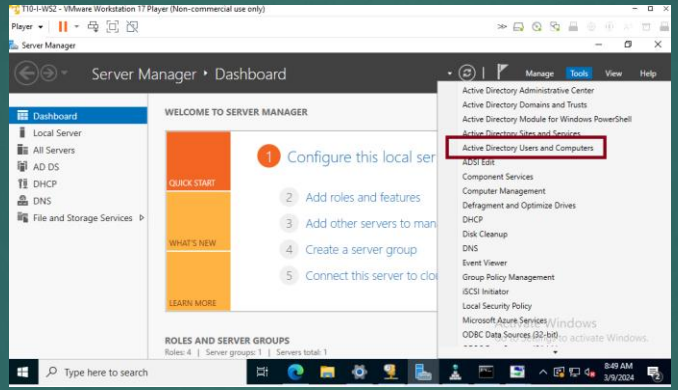
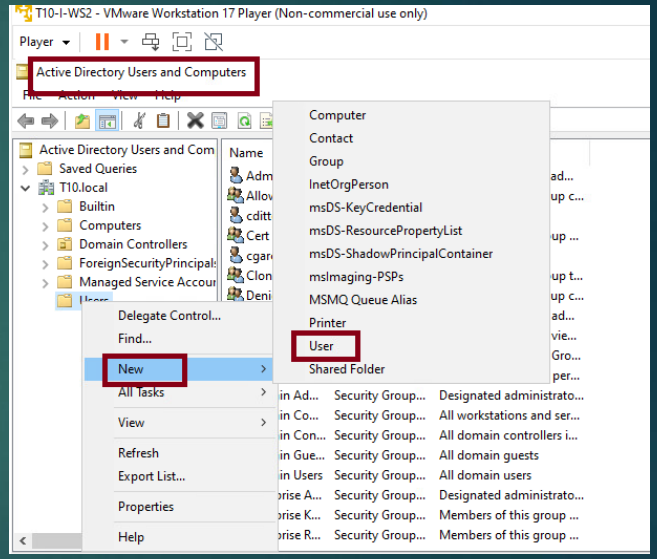
IPsec VPN site to site

By Christopher Ditto, Carlos Gerez, and Mark Riley Slik

Create a user for the Team 15 in Active Directory

Since we had created a domain with a domain controller, we manage the new users centrally from Users and Computers in Active Directory

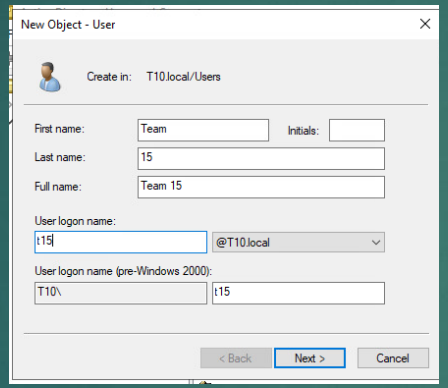


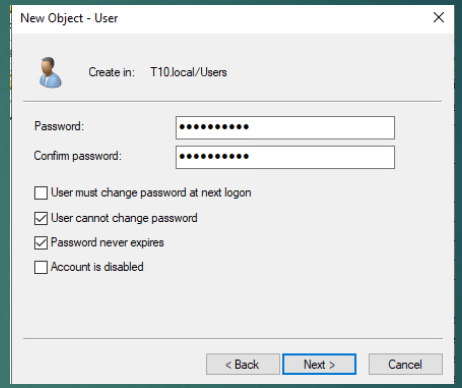


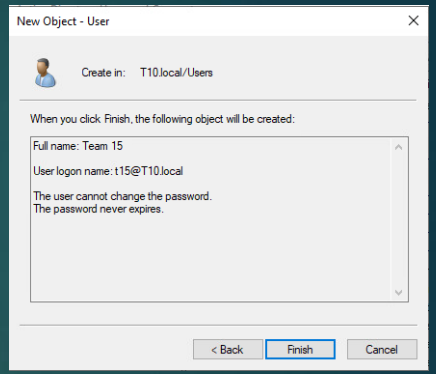
Create a user for the Team 15 in Active Directory

Then we create a new user that can be used on any endpoint on the DMZ zone.

This new user at logon will be identified as t15@T10.local



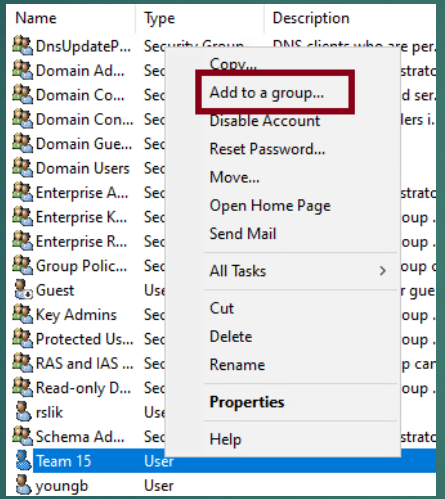


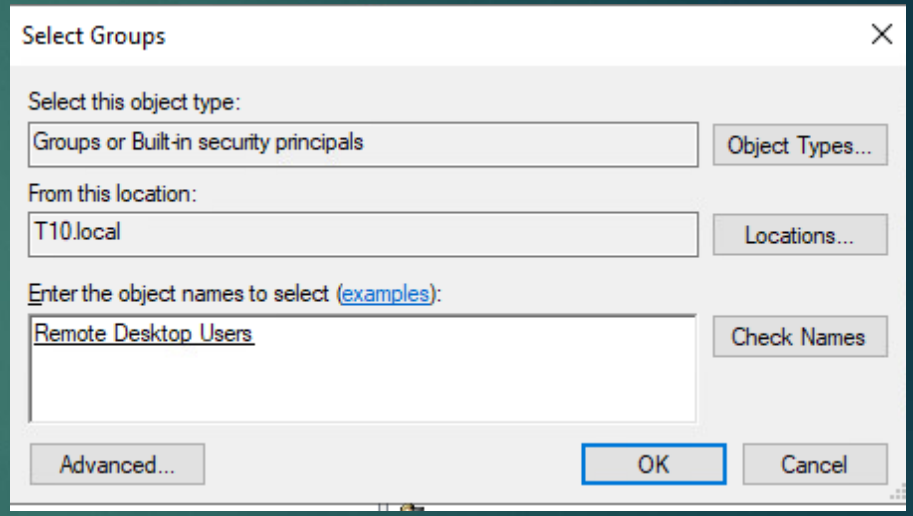


Create a user for the Team 15 in Active Directory

We add the new user to the Remote Desktop Users. The new username is

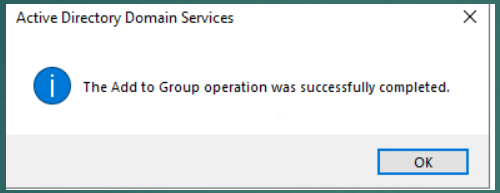
Team 15.

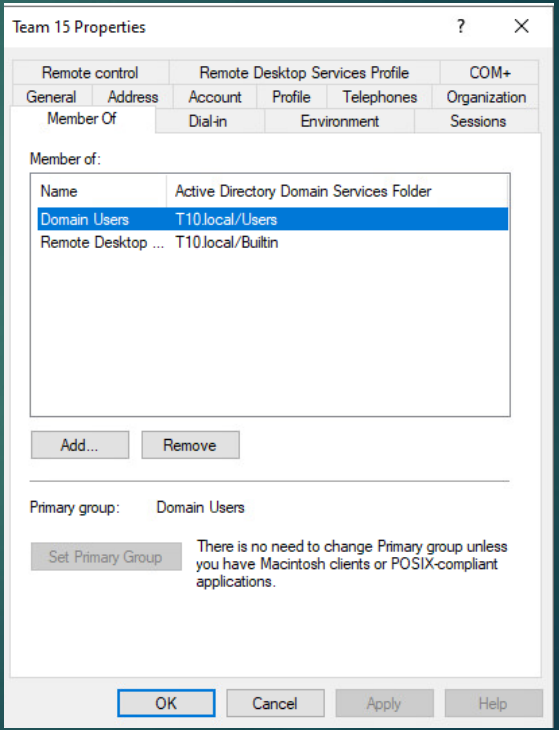




Create a user for the Team 15 in Active Directory

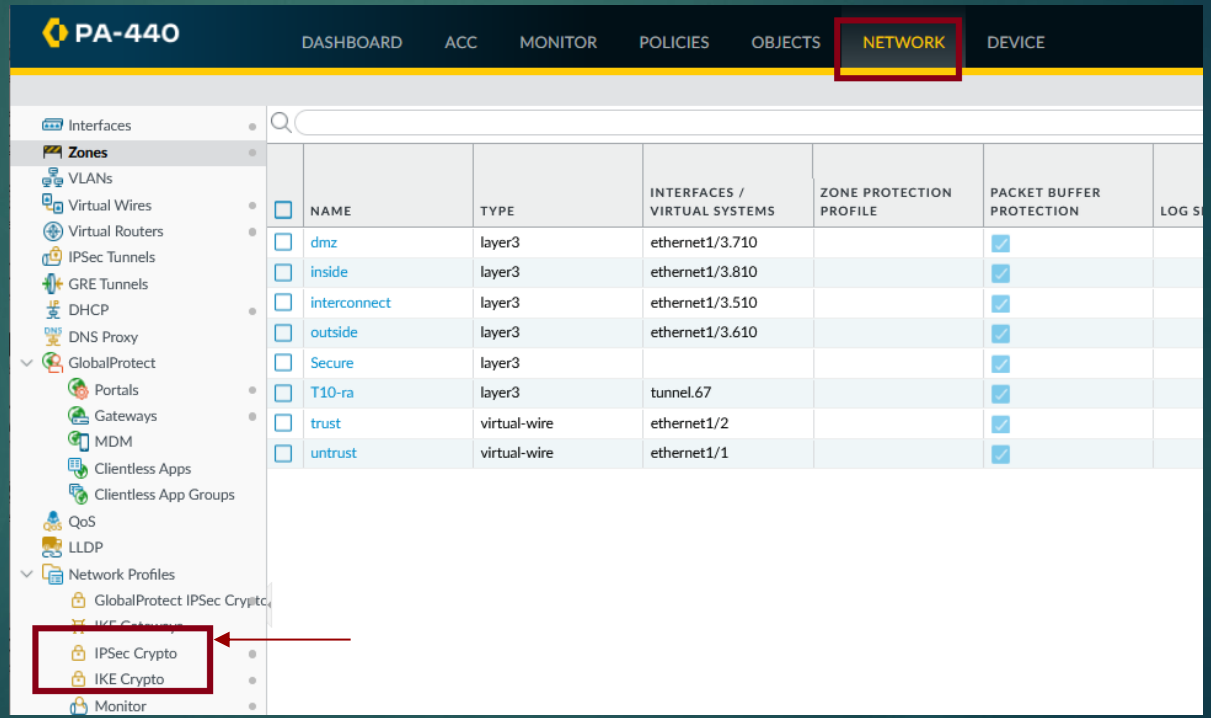
This is how the final team 15 properties should look.





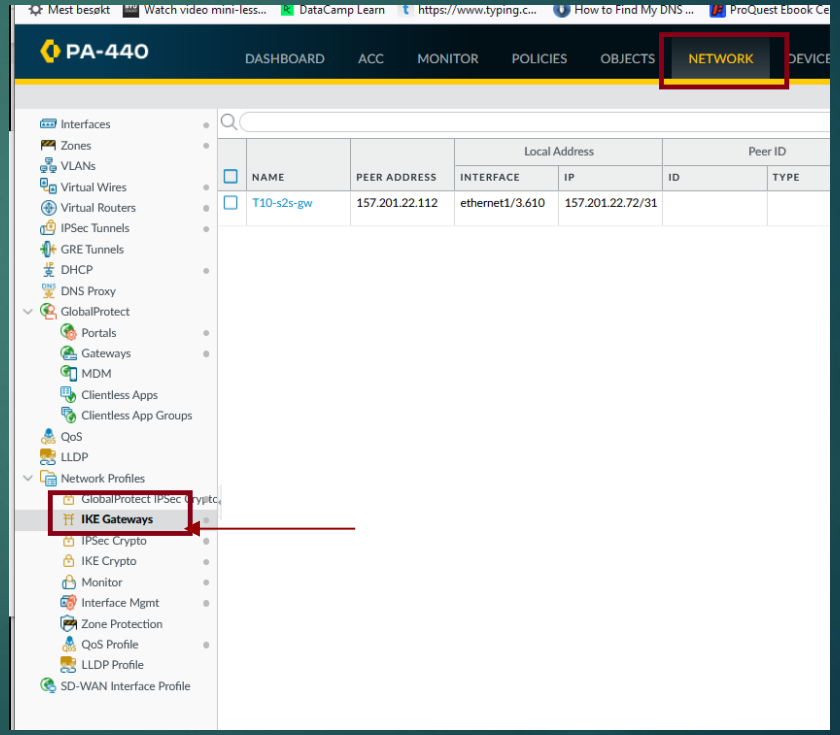
Configuration of IPSec on Palo Alto Firewall

Create an IKE gateway with default values for the tunnel. We see that we have in the side menu, default values for cryptographic management that we will use.



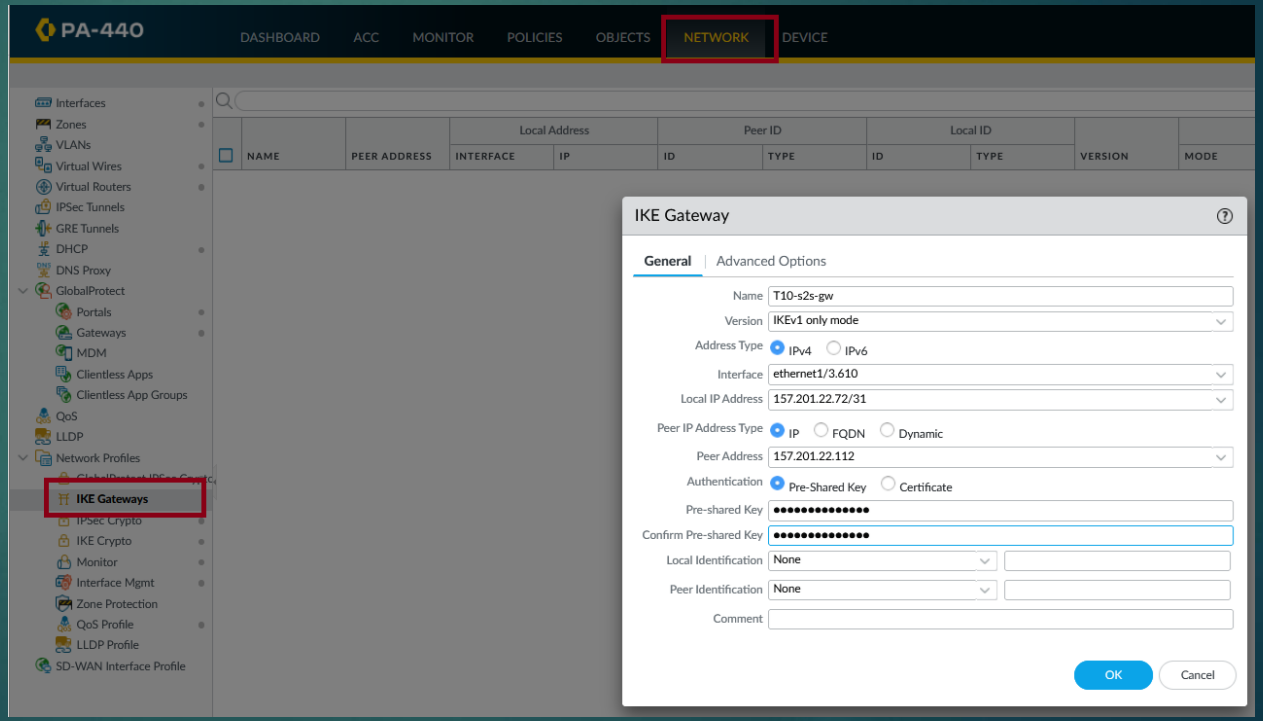
Configuration of IPSec on Palo Alto Firewall

Create an IKE gateway. Start in the IKE gateways tab on the side menu.



Configuration of IPSec on Palo Alto Firewall

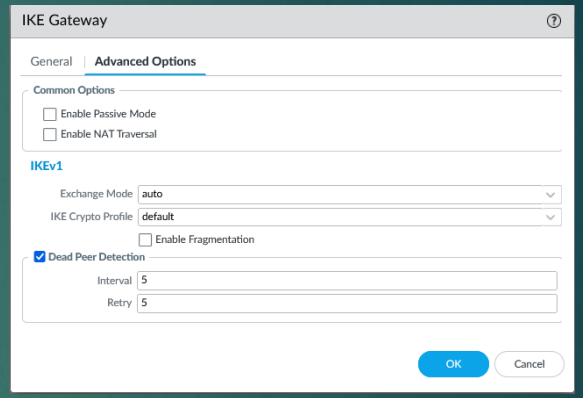
Create an IKE gateway, give a name, leave the default version, and choose the 3.600 outside interface of your team. Local Ip address is the outside address of our team. Peer address is the other team extern ip address. The preshared Key is the password we agreed between the teams.



Configuration of IPSec on Palo Alto Firewall

In advance options left the defaults values.

Your final Ike Gateway should look the one in this picture.



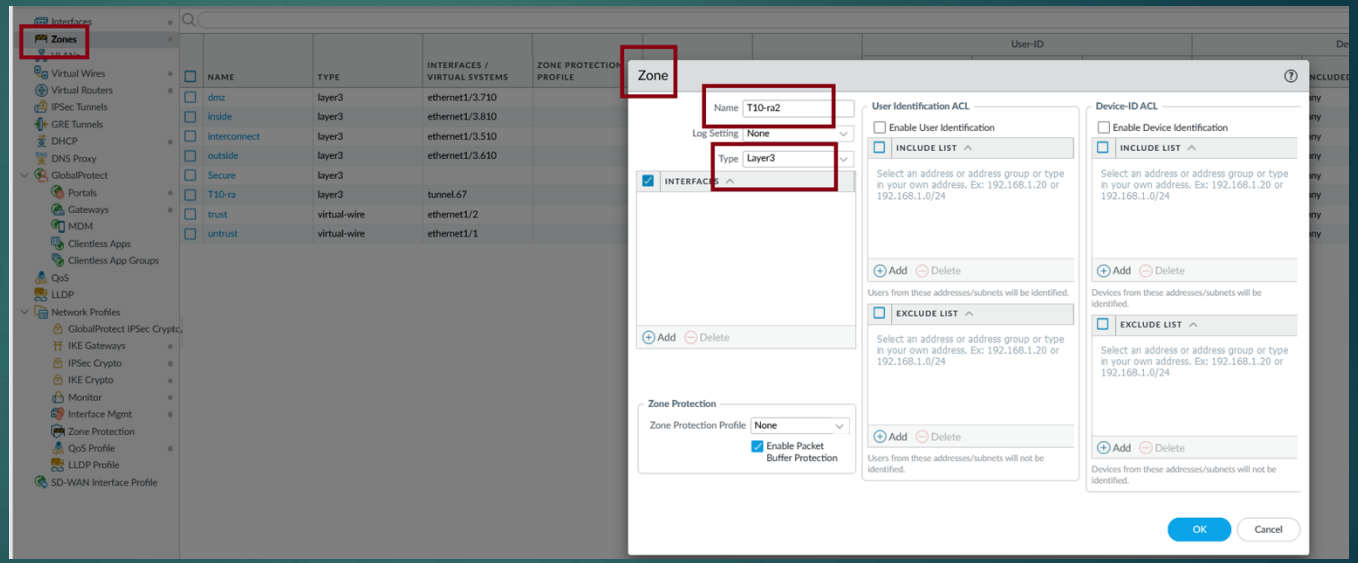
			Local Address		Peer ID		Local ID			IKE Advanced Options				
	NAME	PEER ADDRESS	INTERFACE	IP	ID	TYPE	ID	TYPE	VERSION	MODE	PASSIVE MODE	NAT TRAVERSAL	CRYPTO PROFILE	DPD
☑	T10-s2s-gw	157.201.22.112	ethernet1/3.610	157.201.22.72/31					ikev1	auto			default	enabled/default/default

Configuration of IPSec on Palo Alto Firewall

Add a new layer 3 zone.

On Network choose Zones and add a new layer 3 zone.

Give it a name and choose Layer 3 in Type.

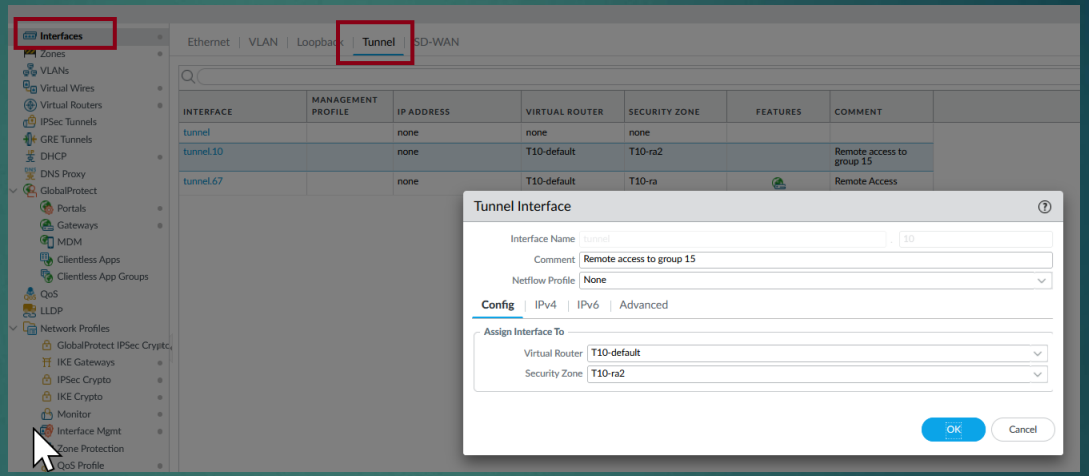


Configuration of IPSec on Palo Alto Firewall

Create a new interface tunnel.

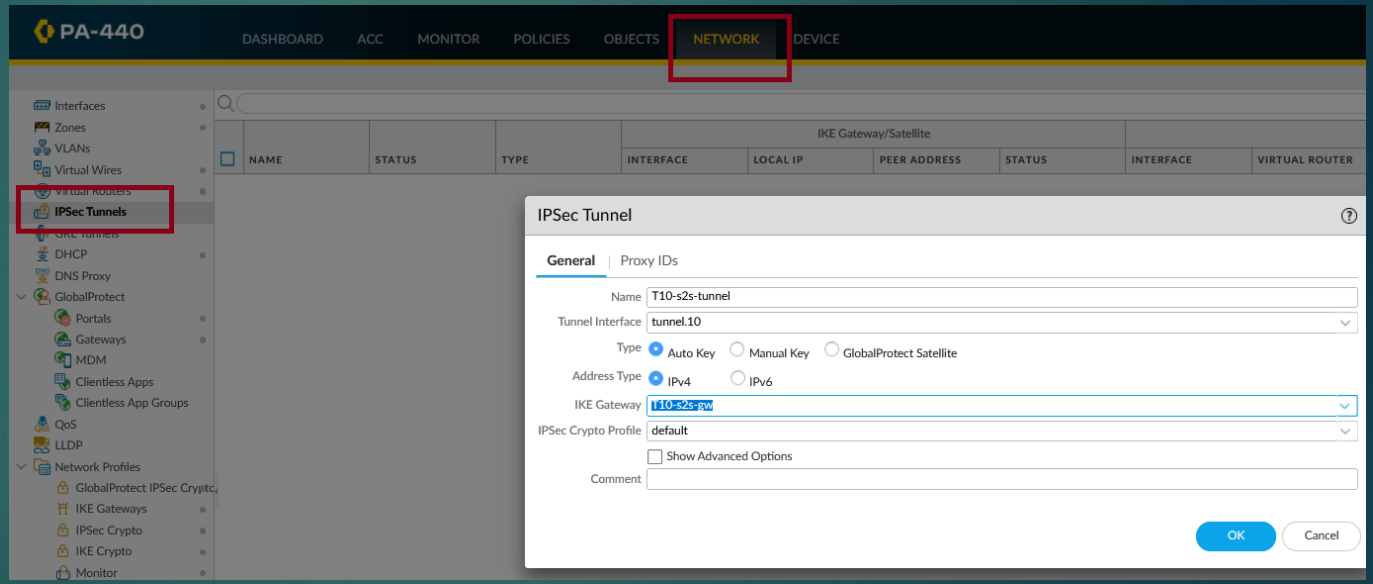
Go to Network and choose Interfaces, then Tunnel to create a new tunnel.

Give it a name, use the default virtual router and add the newly created zone.



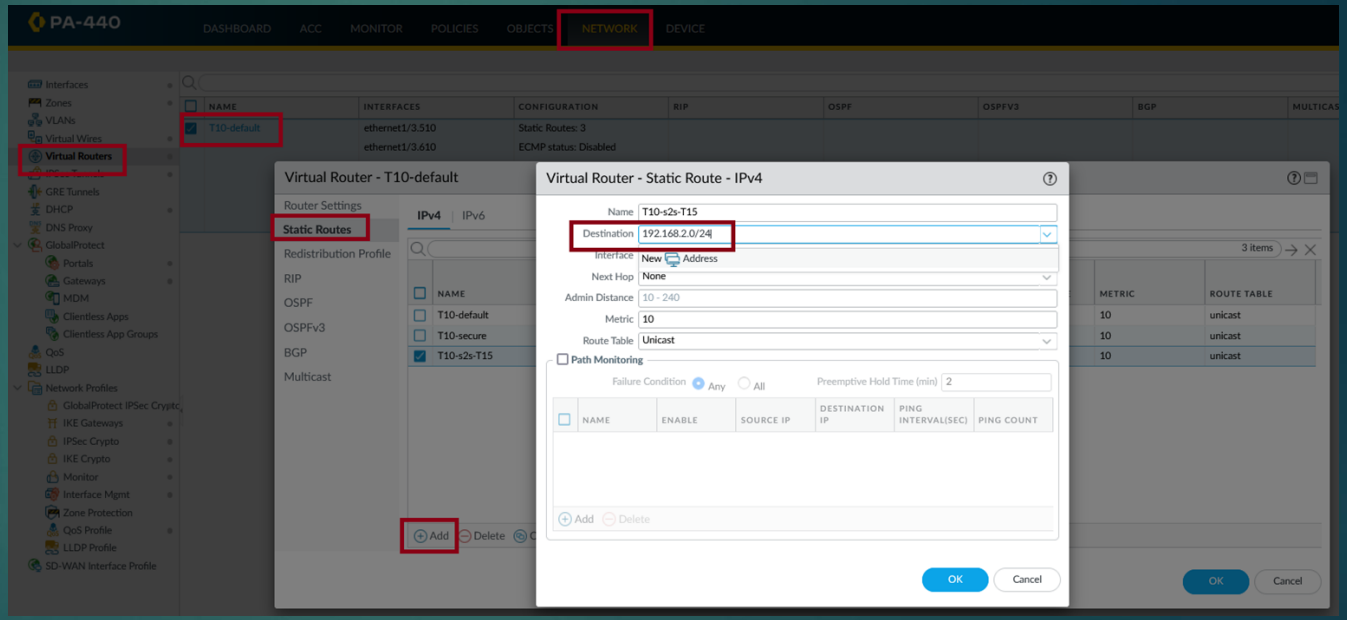
Configuration of IPSec on Palo Alto Firewall

Create an ipsec tunnel . On Network choose IPSec Tunnels and add the information, name tunnel interface already created, and IKE Gateway also previously created.



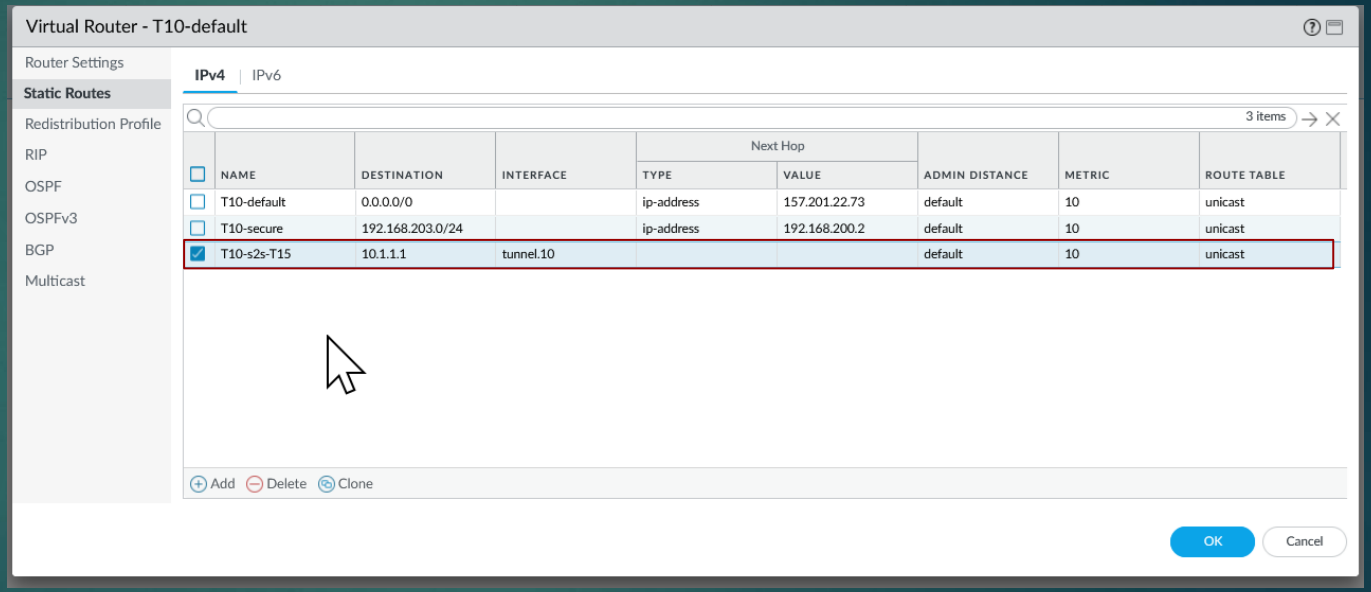
From here on we need to change the addresses with 10.1.1.0 to the range on team 15 DMZ.

Create a static route on the router. Go to Network, Virtual Routers and choose the default router, to add a new Virtual Router-Static Route. Give it a name, You will need the ip range of the DMZ zone of the other team for the destination, add the tunnel interface created before and in next hop none.



Configuration of IPSec on Palo Alto Firewall

The final static route should look like this.



Configuration of IPSec on Palo Alto Firewall

T10-s2s-to-T15	none	universal	dmz	192.168.201.0/24	any	any	T10-ra2	192.168.2.0/24
T10-s2s-from-T15	none	universal	T10-ra2	192.168.2.0/24	any	any	dmz	192.168.201.0/24
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any

				IKE Gateway/Satellite				Tunnel Interface				
	NAME	STATUS	TYPE	INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERFACE	VIRTUAL ROUTER	VIRTUAL SYSTEM	SECURITY ZONE	STATU
	T10-s2s-tunnel	Tunnel Info	Auto Key	ethernet1/3.610	157.201.22.72/31	157.201.22.112	IKE Info	tunnel.10	T10-default (Show Routes)	vsys1	T10-ra2	

Create 2 new rules to allow traffic incoming and outgoing on the zones already created. The second screenshot shows the tunnel ready for testing, you can see this on IPSec Tunnels under Network.

Start the connections from command line.

Access your router from your command line at home when you have the vpn connection up to test and start the tunnels. This test will bring up the connections.

```
Password:
PS C:\WINDOWS\system32> ssh cgerez@10.1.47.10
Password:
Last login: Tue Mar 12 05:28:59 2024 from 10.0.10.8



Number of failed attempts since last successful login: 0



cgerez@PA-440-T10> test vpn ike-sa gateway T10-s2s-gw

Start time: Mar.12 14:04:37
Initiate 1 IKE SA.

cgerez@PA-440-T10> test vpn ipsec-sa tunnel T10-s2s-tunnel

Start time: Mar.12 14:06:03
Initiate 1 IPSec SA for tunnel T10-s2s-tunnel.

cgerez@PA-440-T10>
```

Check the status of the tunnel.

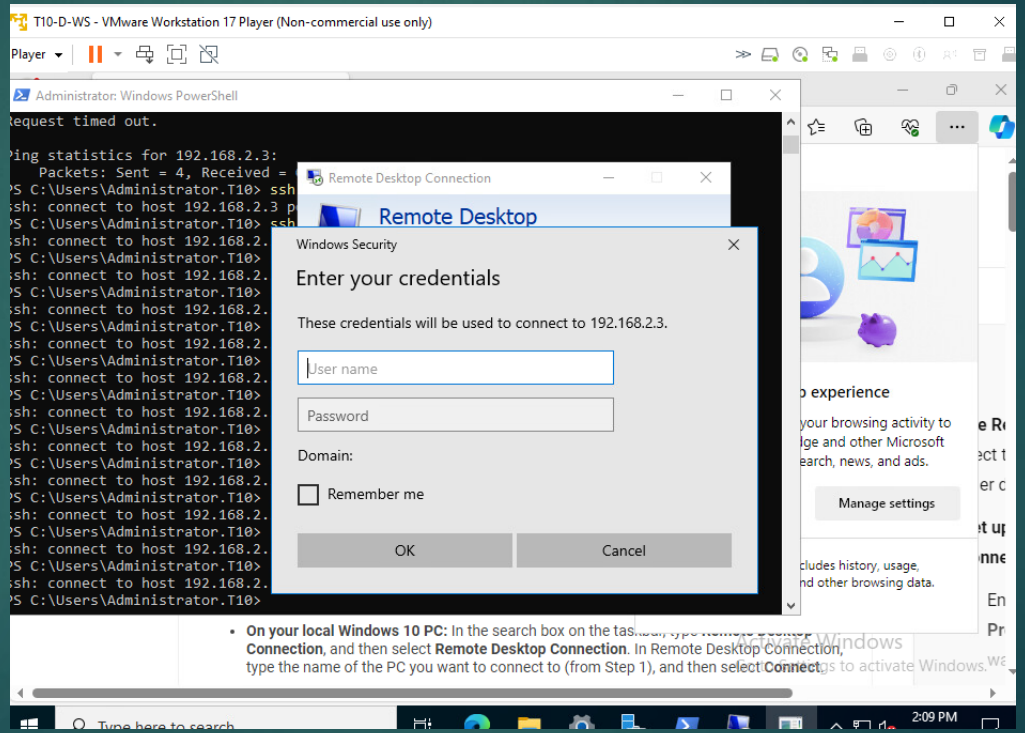
Go to Network, IPSec Tunnel and look at the connections. Green means they are up.

1 it

				IKE Gateway/Satellite				Tunnel Interface					
	NAME	STATUS	TYPE	INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERFACE	VIRTUAL ROUTER	VIRTUAL SYSTEM	SECURITY ZONE	STATUS	C
	T10-s2s-tunnel	Tunnel Info	Auto Key	ethernet1/...	157.201.22...	157.201.22...	IKE Info	tunnel.10	T10-default (Show Routes)	vsys1	T10-ra2		

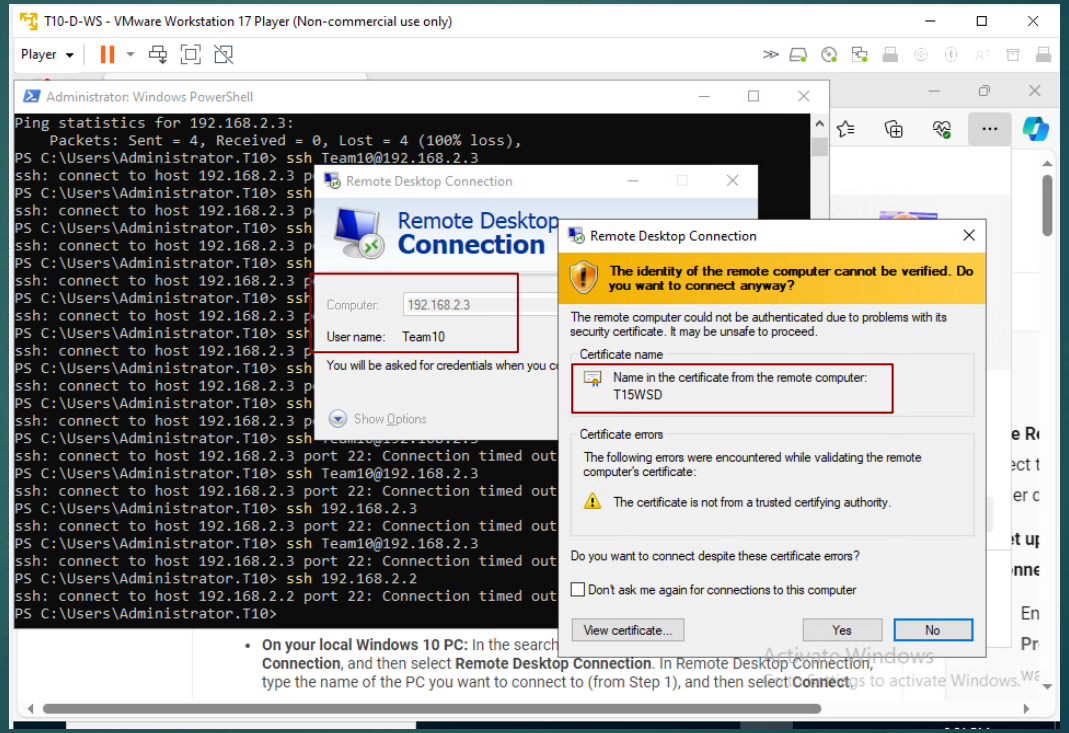
Testing the tunnel with ssh and RDP

Remote desktop from Team 10 DMZ zone towards Team 15 windows machine on DMZ zone.



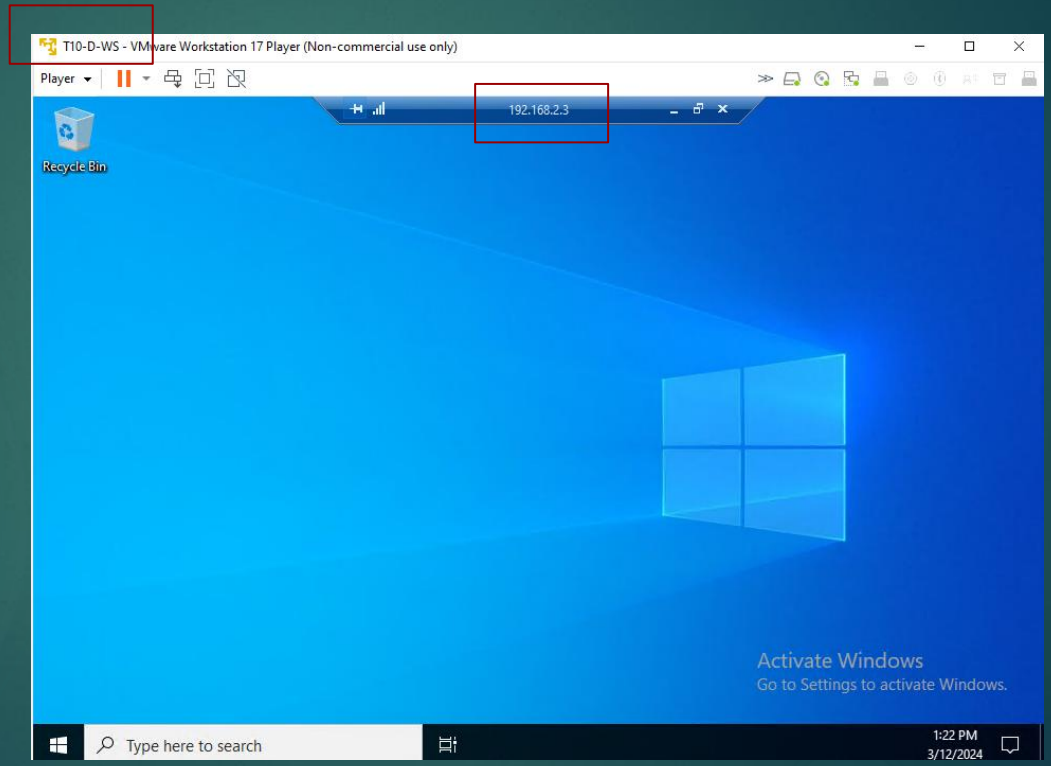
Testing the tunnel with ssh and RDP

Remote desktop from Team 10 DMZ zone towards Team 15 windows machine on DMZ zone.



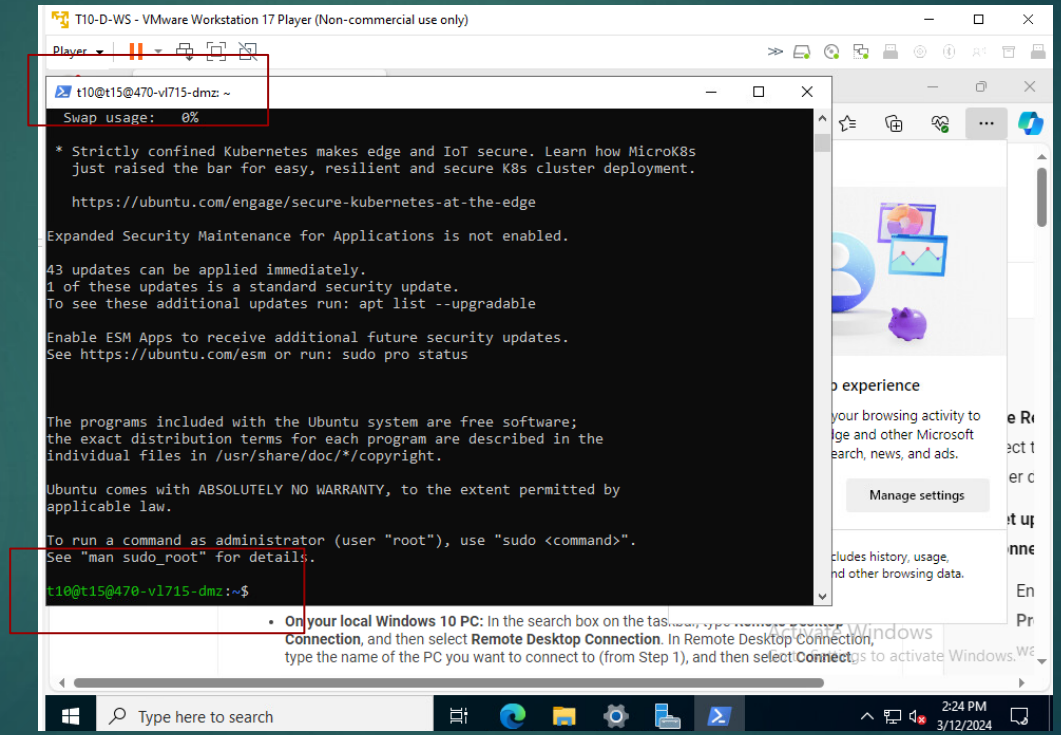
Testing the tunnel with ssh and RDP

Remote desktop from Team 10 DMZ zone towards Team 15 windows machine on DMZ zone.



Testing the tunnel with ssh and RDP

SSH from Team 10 DMZ zone Windows machine towards Team 15 Linux machine on DMZ zone.



Testing the tunnel with ssh and RDP

SSH from Team 10 DMZ zone Linux machine towards Team 15 Linux machine on DMZ zone.