KB-Palo Alto Out of The Box Setup For Internet Connectivity With Double NAT

Friday, September 29, 2023

Use Case/Audience:
You want to use a Palo Alto sitting behind a residential class modem/router combo and you are going to operate the modem in "router mode" meaning you are not passing the public IP address through from the modem/router combo device to the outside interface of the Palo Alto. Rather, the traffic egressing the Palo Alto will NAT to another "private" subnet which will NAT again when egressing the modem/router combo.

This is different than some of the guides I have found on the internet to get basic PA setup operational (out of the Ebay box) to get out to the internet because most guides I've come across don't give a configuration option to use double NAT when modem/router is not in bridge mode. This allows you to have devices maintain direct connection to the modem/router network and create an additional network(s) via the Palo Alto for labbing etc. without affecting connectivity of all the other devices on the network. A great topology if you have anyone that works from home or don't want to kill a smart TV connection and make everyone in the house mad.   :(

☑ Decide which interface will be your outside (WAN) interface and which will be inside (LAN).
☑ Log into the Palo Alto and click the Network tab at the top and in the left menu choose Interfaces.
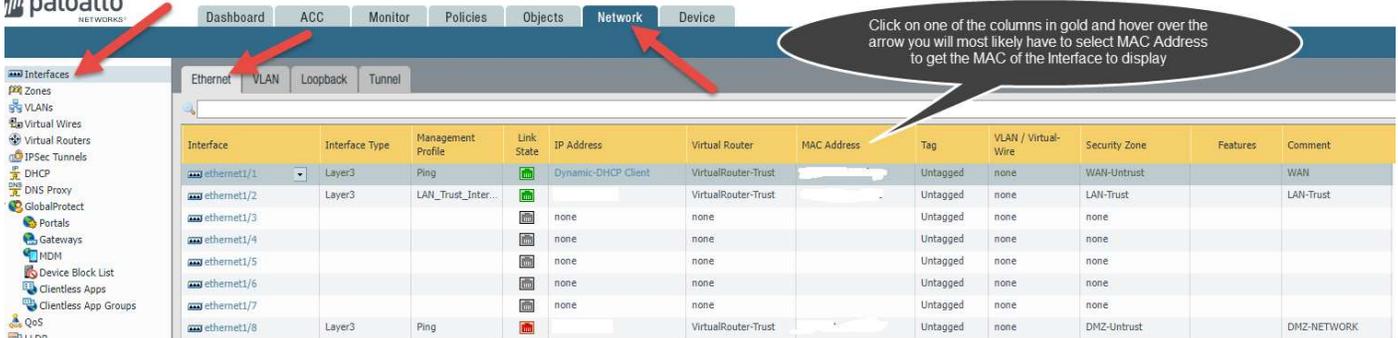
☑ Now that you have the MAC address of your WAN interface, log into your modem/router combo find a place where you can configure a DHCP reservation. It may not have that verbiage, will probably say something like "add device". Add the reservation and choose an address you'd like the Palo Alto WAN interface to have. The reason for this is that the WAN interface will not be set statically it will pull DHCP from the modem/router combo device.
☑ Now we'll configure internal and external zones.
☑ Go to Network menu from the top and on the left menu go to Zones, click add and create two zones one for LAN and one for WAN. Be sure to set the Type as Layer 3. Don't attempt to assign interfaces yet.
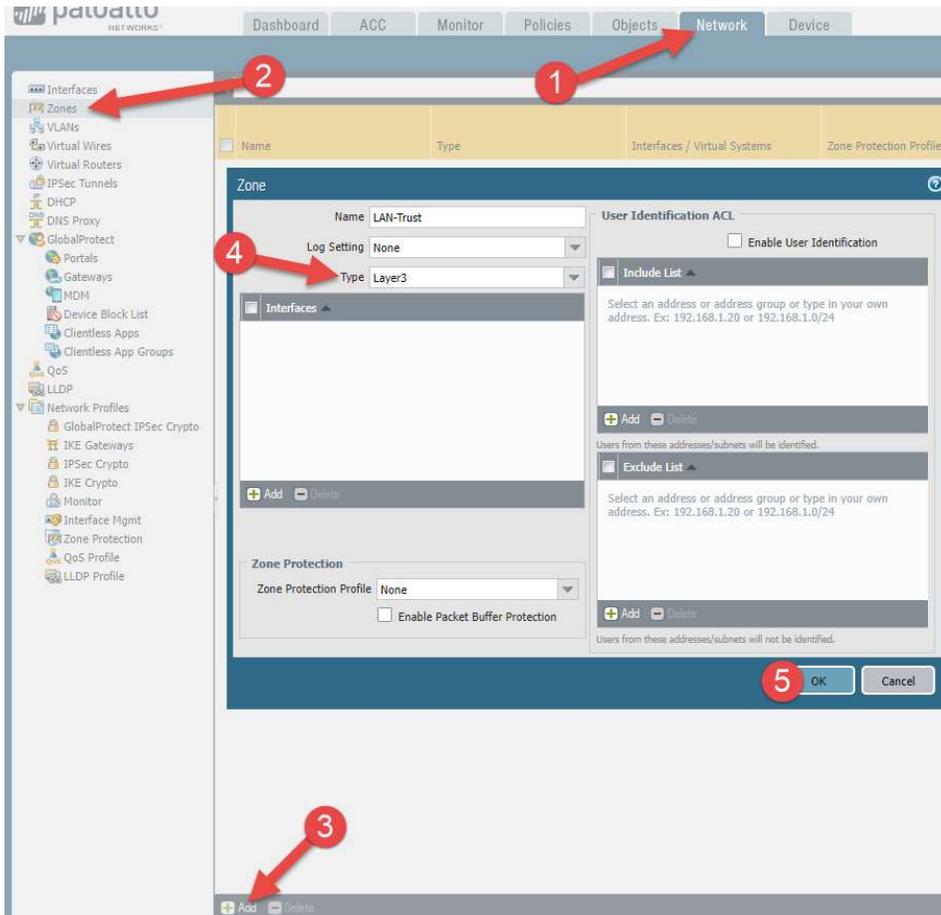
☑ Now we have two zones that should be showing up in the zones menu. Example below.

Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
DHCP
DNS Proxy
GlobalProtect

Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Packet Buffer Protection	Log Setting	Enabled	Included Networks	Excluded Networks
LAN-Trust	layer3						any	none
WAN-Untrust	layer3						any	none

✔ Go to the interfaces menu shown on the left.
✔ Click on the interface that is going to be your LAN interface. Change the Interface Type to Layer 3, Leave the virtual router as none, select the security zone that you created for LAN, then click the IPV4 tab.

Ethernet Interface

Interface Name ethernet1/2
Comment
Interface Type Layer3
Netflow Profile None

Config | IPv4 | IPv6 | Advanced

Assign Interface To
Virtual Router None
Security Zone LAN-Trust

OK   Cancel

✔ Leave the radio button selected for Static, then in the IP section below click Add. Choose the address for the LAN interface. If you are creating a simple network this will most likely be your default gateway for devices sitting behind the Palo Alto. Next click the Advanced tab.

Ethernet Interface

Interface Name ethernet1/2
Comment
Interface Type Layer3
Netflow Profile None

Config | IPv4 | IPv6 | Advanced

Type ● Static   ○ PPPoE   ○ DHCP Client

IP
☑ 172.16.10.1/24

⊕ Add ⊖ Delete ⬆ Move Up ⬇ Move Down
IP address/netmask. Ex. 192.168.2.254/24

OK   Cancel

✔ Change the Management Profile to "Ping". If there is no management profile created, you can choose add new and make sure only the Ping option is selected. This will be helpful for testing troubleshooting later if needed. Finally, click OK to save the configuration.

Ethernet Interface

Interface Name ethernet1/2
Comment
Interface Type Layer3
Netflow Profile None

Config | IPv4 | IPv6 | Advanced

Link Settings
Link Speed auto   Link Duplex auto   Link State auto

Other Info | ARP Entries | ND Entries | NDP Proxy | LLDP

Management Profile Ping
MTU [576 - 1500]
☐ Adjust TCP MSS
IPv4 MSS Adjustment 40
IPv6 MSS Adjustment 60

☐ Untagged Subinterface

OK   Cancel

✔ Next, click on the interface that you've selected for WAN. Change the Interface Type to Layer 3. Leave the Virtual Router as none. Change the security zone to the zone you created for WAN.
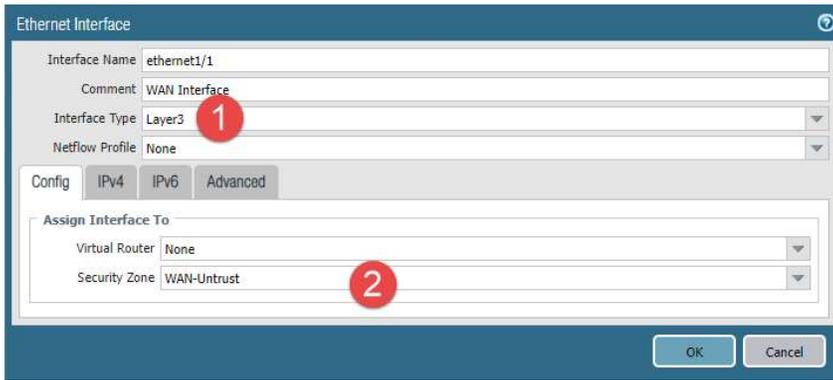
✅ Click on the IPV4 tab and change the radio button to DHCP Client. Make sure both tick boxes are ticked. Set the Default Route Metric to 10. Then click OK.
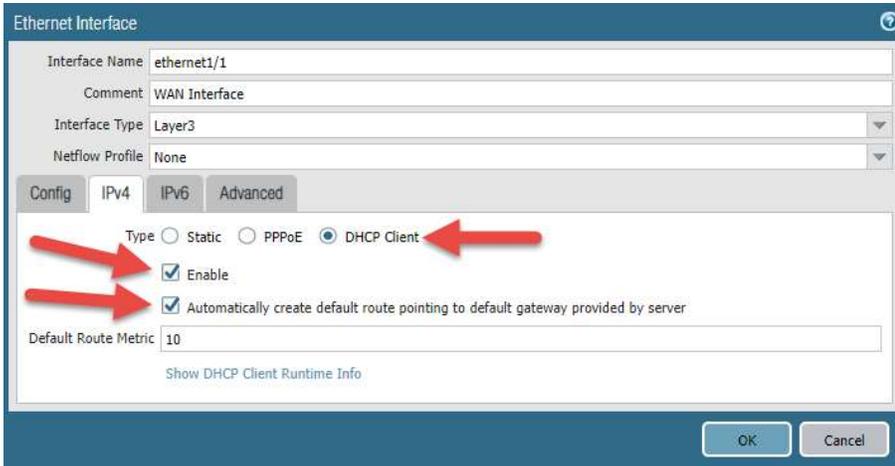
✅ Now go to the Virtual Routers menu on the left side. Click Add at the bottom. In the Router Settings, give your router a name, Add both your WAN and LAN interfaces into the virtual router. Then click on the Static Routes menu.
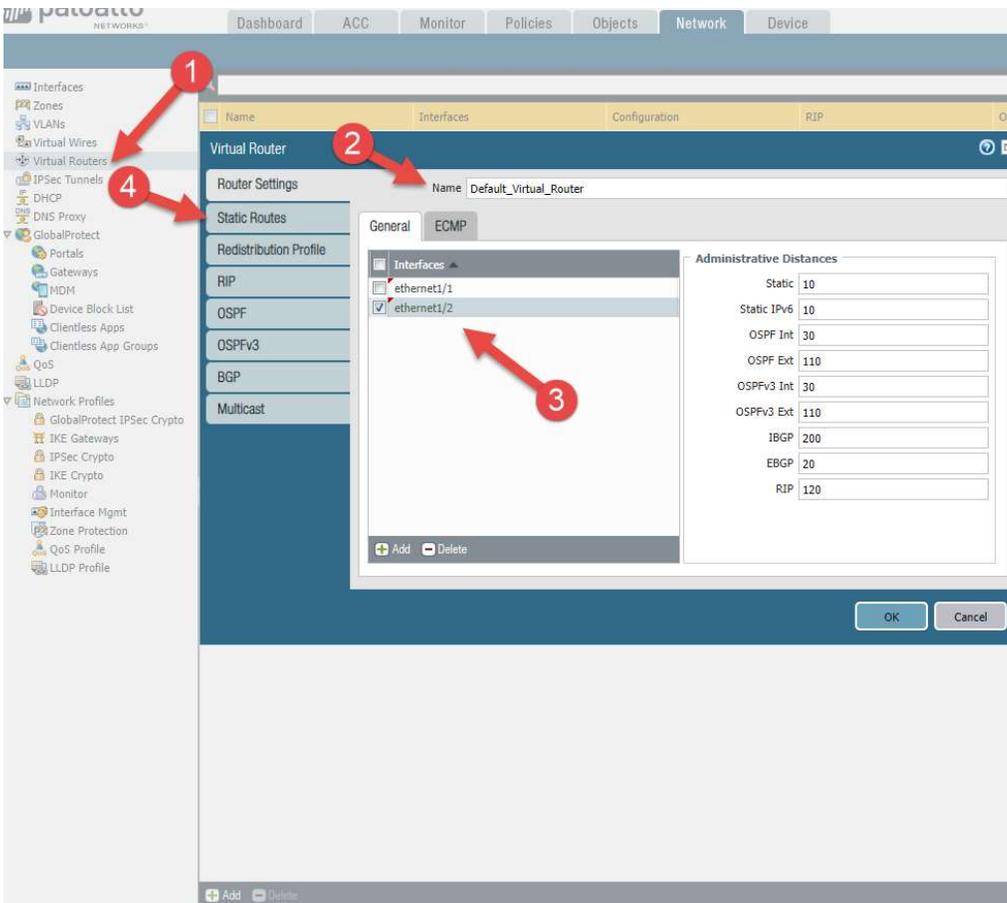
✅ Click Add to add static route. We are creating the route that will route traffic destined for the LAN network and send that traffic to the LAN interface. Give the route a name. In the destination field, input your network that you've

created for your LAN be sure to use the network ID plus subnet (CIDR format) to capture traffic destined for any address in the subnet. Leave Next Hop as None. (shown below)
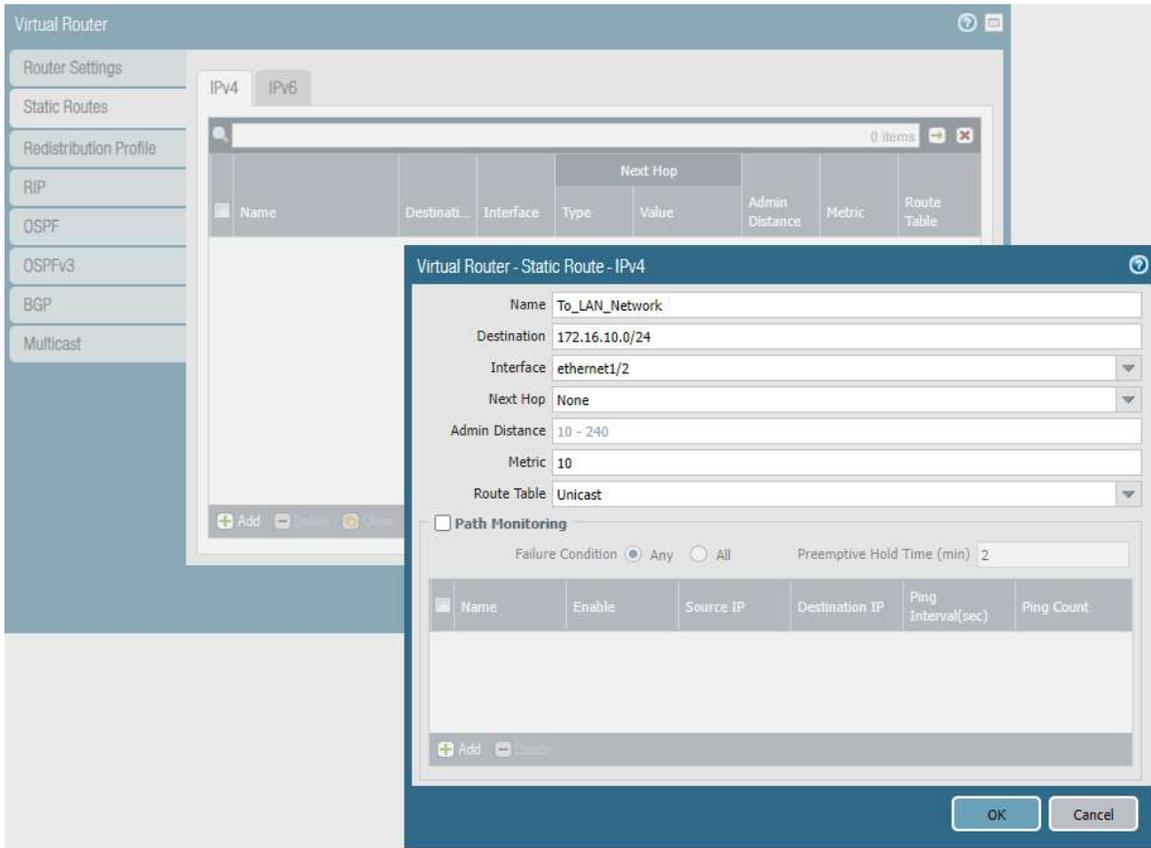
- ✓ Click OK and OK again to save these changes. Now we are going to commit our config up to this point to the firewall. Click commit at the top right of the window and wait for the commit to process.
- ✓ Before moving on to the next part of the config we need to verify that our config up to this point is working correctly.
- ✓ This is the point that you want to make sure that your WAN and LAN physical connections are in place if not done already.
- ✓ Go to Network -> Interfaces -> (select WAN interface) -> IPV4 Then click the link at the bottom that says Show DHCP Client Runtime Info.
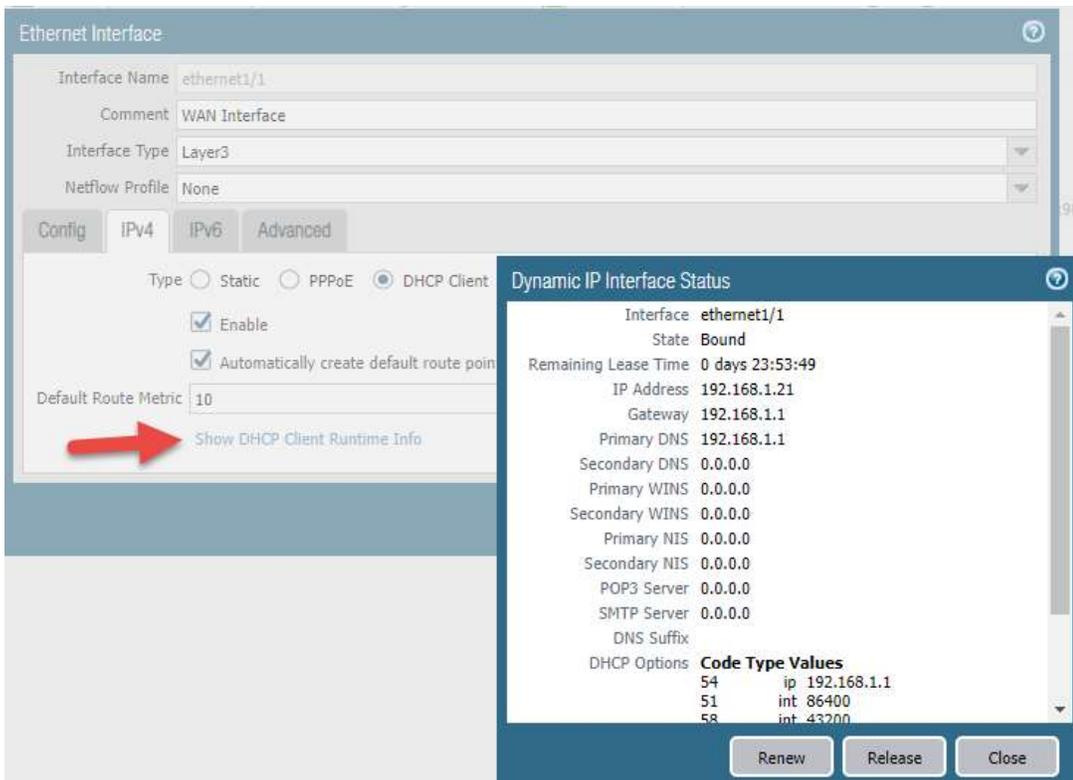
- ✓ The address observed should be the DHCP reservation we configured at the beginning of this guide on the modem/router combo device. If there is no address displayed and you just connected the cable from the Palo Alto WAN interface to an interface on your modem/router combo, click on release followed by renew and that will force the DHCP request broadcast to occur from the Palo Alto WAN interface so that the modem/router combo device gives the DHCP reservation address to the Palo Alto WAN interface.
- ✓ Once DHCP is displaying the correct address we move on to verify the automatically generated route from the WAN interface configuration.
- ✓ Go to Network -> Virtual Routers. Click on the link on the right side that says More Runtime Stats.
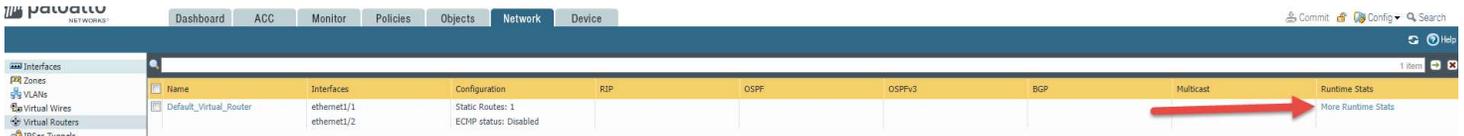
- We are looking for two thing here. The first, a default route that sends traffic to the modem/router combo device's IP address which will automatically route traffic to the internet via next hop address (probably handed to the modem/router combo device by the ISP (public IP address plus gateway address)). Labeled in the picture below "1".
- The second thing we are looking for is a route that sends traffic destined for the modem/router combo device's subnet that sends the traffic to the Palo Alto's WAN interface. Labeled in the picture below "2".
- Now that we've verified DHCP functionality from the WAN device and our routing table on the Palo Alto, we can move forward with the configuration.
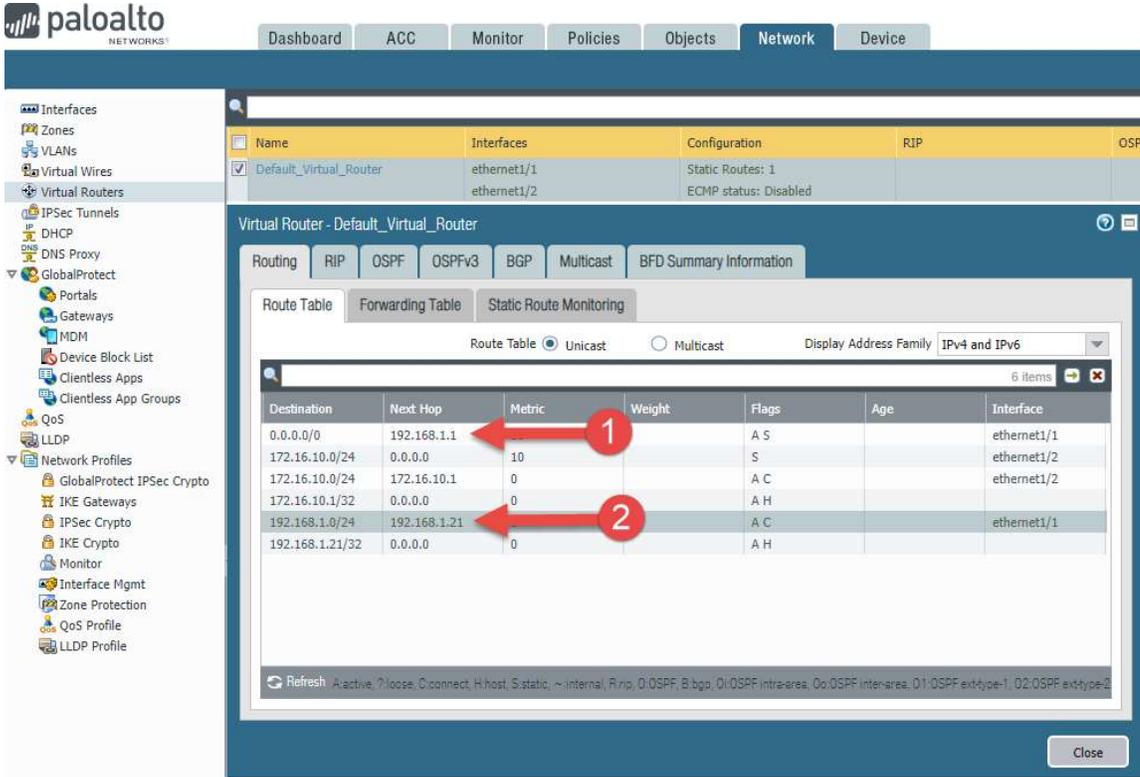
- Go to Objects. Create an Object that encompasses the LAN subnet. Will use this object alias in our NAT/Firewall policies.
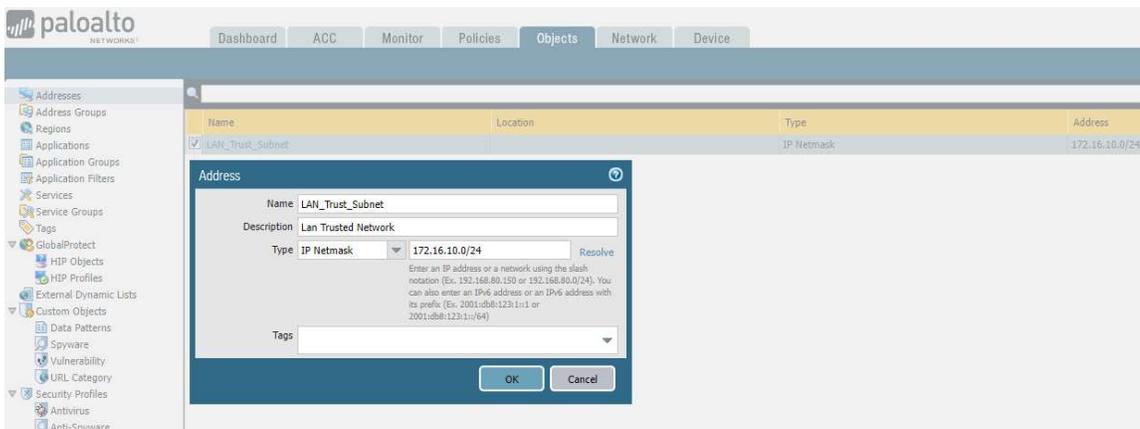
- Now go to Policies -> Security.
- Click in the blank space next to the name that says intrazone-default and down at the bottom of the page click Override.
- Do the same thing for the interzone-default policy.
- Click into both policies, and click on the Actions tab. Tick the box that says Log at Session End. This enables any traffic that is filtered by these policies to show up in the traffic logs which will be useful if any troubleshooting is needed.
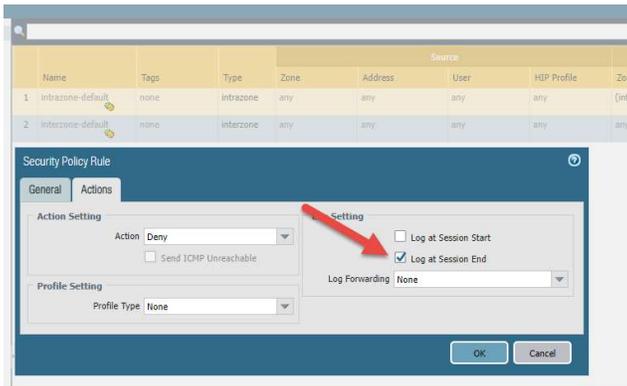
☑ Click OK, then click Add at the bottom to add a new security policy. Configure as pictured below.

Security Policy Rule

General | Source | User | Destination | Application | Service/URL Category | Actions

any ▼ | ☑ Any

☐ Service ▲ | ☐ URL Category ▲

Make sure to change Service to any!

➕ Add ➖ Delete | ➕ Add ➖ Delete

OK | Cancel
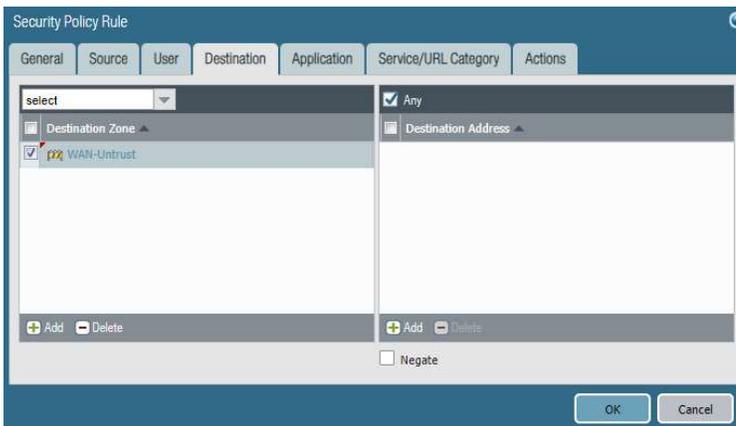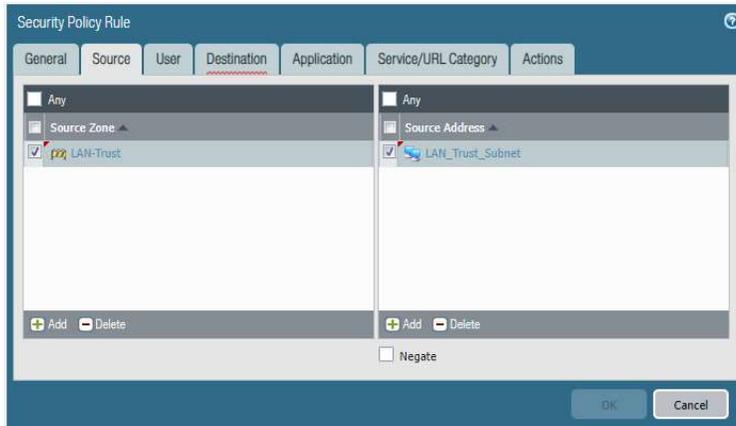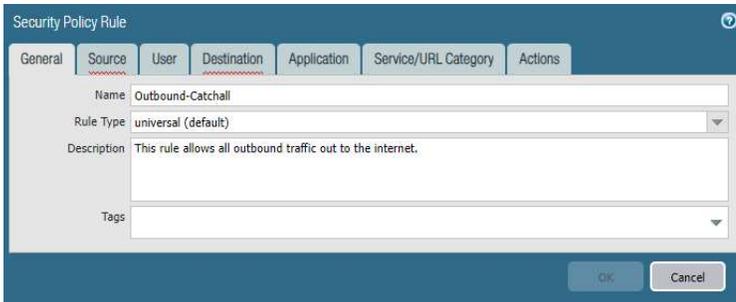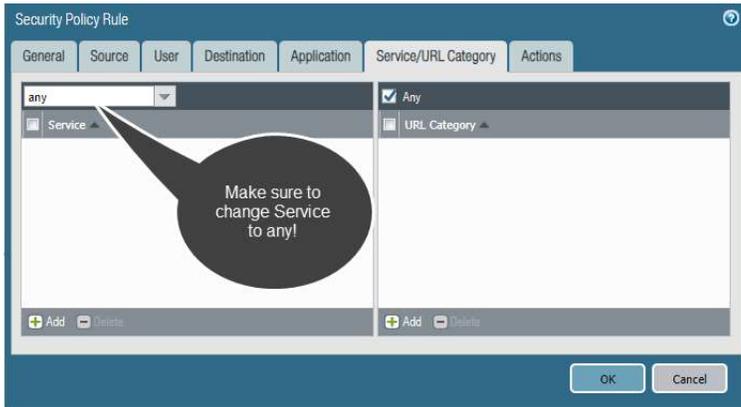
☑ Click OK. Then on the left side menu, click NAT, then click add at the bottom to add a new policy. Then Configure based on the pictures below.

NAT Policy Rule

General | Original Packet | Translated Packet

Name | LAN-To-WAN
Description |
Tags |
NAT Type | ipv4

OK | Cancel

NAT Policy Rule

General | Original Packet | Translated Packet

☐ Any | Destination Zone | ☐ Any | ☑ Any
☐ Source Zone ▲ | WAN-Untrust ▼ | ☐ Source Address ▲ | ☐ Destination Address ▲
☑ 🖧 LAN-Trust | | ☑ 🖳 LAN_Trust_Subnet |
Destination Interface	
any ▼	
Service	
any ▼	

➕ Add ➖ Delete | ➕ Add ➖ Delete | ➕ Add ➖ Delete

OK | Cancel

NAT Policy Rule

General | Original Packet | Translated Packet

Source Address Translation | ☐ **Destination Address Translation**

Translation Type | Dynamic IP And Port ▼ | Translated Address |
Address Type | Interface Address ▼ | Translated Port | [1 - 65535]
Interface | ethernet1/1 ▼
IP Address | None ▼

OK | Cancel

☑ Commit the changes to the firewall.
☑ Now you can plug into the LAN interface and configure the network adapter on your client device with an IP address on the same subnet as the LAN interface of the firewall and you should be able to communicate to the WORLD WIDE WEB! :)