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.

Data	Dashboard AC Ethernet VLAN Lo	CC Monito	or Policies	Obje	ects Network	Device	Click arrow	on one of th you will mo to get the l	ne columns in g ost likely have to MAC of the Inte	old and hover ove select MAC Add rface to display	r the Iress	
En Virtual Wires	<u></u>	10		10		0				10	11	- 6
Virtual Routers Piper Tunnels	Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	MAC Address	Tag	VLAN / Virtual- Wire	Security Zone	Features	Comment
E DHCP	ethemet1/1	Layer3	Ping		Dynamic-DHCP Client	VirtualRouter-Trust	and the second second	Untagged	none	WAN-Untrust		WAN
DNS Proxy	ethernet1/2	Layer3	LAN_Trust_Inter			VirtualRouter-Trust	Contraction of the	Untagged	none	LAN-Trust		LAN-Trust
GlobalProtect Portals	ethernet1/3			曲	none	none		Untagged	none	none		
🖲 Gateways	a ethernet1/4			m	none	none		Untagged	none	none		
MDM	and ethernet1/5			m	none	none		Untagged	none	none		
Clientless Anns	ethernet1/6			m	none	none		Untagged	none	none		
Clientless App Groups	ethernet1/7			m	none	none		Untagged	none	none		
& QoS	ethernet1/8	Layer3	Ping	m		VirtualRouter-Trust	and the second second	Untagged	none	DMZ-Untrust		DMZ-NETWORK

Vow 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 modern/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.

ANs									
rtual Wires	🔲 Name	Туре	Interfaces / Virtual Systems	Zone Protection Profile	Packet Buffer Protection	Log Setting	Enabled	Included Networks	Excluded Networks
rtual Routers	LAN-Trust	layer3						any	none
Sec Tunnels	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 Interfac	ce				0
Interface Na	me e	thernet	/2		
Comm	ent				
Interface T	ype L	ayer3			
Netflow Pro	file N	lone			•
Config IPv	4	IPv6	Advanced		
Assign Inte	rface	То			
Virtual	Interface Name ethemet1/2 Comment Interface Type Layer3 Netflow Profile None Config IPv4 IPv6 Advanced Assign Interface To Virtual Router None	~			
Securit	y Zone	LAN-	ust	~	
				OK	

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.

hernet Interface		C
Interface Name	ethernet1/2	
Comment		
Interface Type	Layer3	*
Netflow Profile	None	~
Config IPv4	IPv6 Advanced	
+ Add - Delete	192.168.2.254/24	
🕂 Add 📄 Deletv IP address/netmask. Ex	Move Lip C Move Dears 192.168.2.254/24	

🗹 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.

hernet Interfac	e .	
Interface Nan	ne ethernet1/2	
Comme Interface Tvi	nt laver3	
Netflow Prof	ile None	
Config IPv4	IPv6 Advanced	
Link Setting	5	
Link Speed	auto 💌 Link Duplex auto 💌 Link State auto	*
Other Info	ARP Entries ND Entries NDP Proxy LLDP	
Managen	nent Profile Ping	*
	MTU [576 - 1500]	
Adjust 1	CP MSS	
IPv4 MSS	s Adjustment 40	
IPv6 MSS	Adjustment 60	
	ок	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.

Comment WAN Interface Interface Type Layer3	
Interface Type Layer3	
Netflow Profile None	
Config IPv4 IPv6 Advanced	
Assign Interface To	Internet in
Virtual Router None	*
Security Zone WAN-Untrust	•

🗹 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.

Interface Na	ne ethernet1/1	
Comme	MAN Interface	
Interface Ty	De Layer3	-
Netflow Pro	ile None	
Config IPV2	IPVb Advanced	
	IPVb Advanced Fype Static PPPoE DHCP Client Image: Static Control in the state of the state o	
Default Route M	IPVb Advanced Type Static PPPoE DHCP Client Image: Enable Image: Automatically create default route pointing to default gateway provided by server etric 10	

🗵 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.

NETWORKS'	Dashboard /	ACC Monitor	Policies Objects	Network Devi	be	
Interfaces						
VLANs	Name	Interfaces	Configura	tion	RIP	OS
Ex Virtual Wires	Virtual Router	2				0 🗆
PSec Tunnels	Router Settings	Name Defaul	t_Virtual_Router			
DNS Proxy	Static Routes	General FCMP				
♥ 🧐 GlobalProtect	Redistribution Profile			Administrative Di	stances	
Gateways	RIP	Interfaces ethemet1/1		Static	10	
Device Block List	OSPF	ethernet1/2		Static IPv6	10	
Clientless Apps	OSPFv3			OSPF Int	30	
A QoS	BGP			OSPF Ext	110	
V Retwork Profiles	Multicast	1	3	OSPEv3 Int	30	
GlobalProtect IPSec Crypto	maniause			IBGP	200	
A IPSec Crypto				EBGP	20	
Monitor				RIP	120	
Real Interface Mgmt						
QoS Profile		🕂 Add 🖃 Delete				
LLDP Profile						
					ок	Cancel
	🕂 Add 😑 Delete					

Z 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)

Virtual Router						0 🗉		
Router Settings	10							
Static Routes	vo					_		
Redistribution Profile		-		_	0 ili	ims 🔿 🗙		
RIP			Next Hop			Paula		
OSPF Name	Destinati Interface	Тура	Value	Distance	Metric	Table		
OSPFv3	Virtual Router - Sta	atic Route -	IPv4					0
BGP	Name	e To_LAN_N	letwork					
Multicast	Destination	n 172.16.10	0.0/24					
	Interface	e ethernet1	/2					-
	Next Ho	p None						~
	Admin Distance	e 10 - 240						
	Metri	c 10						
Add 5	Route Table	e Unicast						4
	Failu	ring ire Condition	💿 Any 🔘	All Pr	eemptive Hol	d Time (min) 2		
	Rame Name	Enable	Source	e IP D		Ping Interval(sec)	Ping Count	
	🕀 Add 🔘 🛁							
						OK	Cano	cel

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.

hernet Interface				0
Interface Name Comment	ethernet1/1 WAN Interface			
Interface Type	Layer3			
Netflow Profile	None			
Config IPv4	IPv6 Advanced			
Тур	e 🔿 Static 🔿 PPPoE 💿 DHCP Client	Dynamic IP Interface S	tatus	1
Default Route Metri	Enable Automatically create default route poin 10 Show DHCP Client Runtime Info	Interface State Remaining Lease Time IP Address Gateway Primary DNS Secondary DNS Primary WINS Secondary WINS Secondary WINS Primary NIS Secondary NIS POP3 Server SMTP Server DNS Suffix DHCP Options	ethemet1/1 Bound 0 days 23:53:49 192.168.1.21 192.168.1.1 192.168.1.1 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.00 0.0.00 0.0.00 0.0.00 0.0.00 0.0.000000	

- 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.
- Once DHCP is displaying the correct address we move on to verify the automatically generated rou
 Go to Network -> Virtual Routers. Click on the link on the right side that says More Runtime Stats.

	Dashboard A(C Monitor	Policies Ob	bjects Network	Device					🍰 Commit 🛭 😭 🖓 Config 👻 🔍 Search
										😒 🔞 Help
Interfaces	۹.									1 item
VLANs	🛄 Name	Interfaces		Configuration	RIP	OSPF	OSPFv3	BGP	Multicast	Runtime Stats
2 Virtual Wires	Default_Virtual_Router	ethernet1/1		Static Routes: 1						More Runtime Stats
Virtual Routers		ethemet1/2		ECMP status: Disabled						
nth IPCer Tunnels										

🗹 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.

paloalto Device Dashboard ACC Monitor Policies Objects Network ٩, Interfaces 2 Zones Name RIP OSPF Interfaces Configuration VI ANS Default_Virtual_Router ethernet1/1 Static Routes: 1 En Virtual Wires ethernet1/2 ECMP status: Disabled Virtual Routers 1 IPSec Tunnels Virtual Router - Default_Virtual_Router 0 🗖 DHCP DNS Proxy Routing RIP OSPF OSPFv3 BGP Multicast BFD Summary Information 🛡 🔇 GlobalProtect S Portals Forwarding Table Static Route Monitoring Route Table 🖲 Gateways MDM 🗗 Display Address Family IPv4 and IPv6 W Route Table () Unicast O Multicast B Device Block List Clientless Apps 6 items 📑 🙁 Clientless App Groups Fla 🚴 QoS 0.0.0.0/0 192.168.1.1 AS ethernet1/1 LLDP 172.16.10.0/24 0.0.0.0 S ethernet1/2 Vetwork Profiles 10 172.16.10.0/24 172,16.10.1 AC GlobalProtect IPSec Crypto ethernet1/2 172.16.10.1/32 AH TH IKE Gateways 0.0.0.0 IPSec Crypto 192.168.1.0/24 192.168.1.21 AC ethernet1/1 A IKE Crypto 192.168.1.21/32 0.0.0.0 AH A Monitor Minterface Momt Zone Protection A QoS Profile LLDP Profile Close

Go to Objects. Create an Object that encompasses the LAN subnet. Will use this object alias in our NAT/Firewall policies.

ES Groups	۹.		-				
Groups	Name			Location		Туре	Address
ions	LAN_Trust_Subnet					IP Netmask	172.16.10.0
ion Filters	Address	LAN Trust Subr	et		0		
Groups	Description	Lan Trusted Net	work				
otect	Туре	IP Netmask	~	172.16.10.0/24	Resolve		
Ubjects Profiles I Dynamic Lists Objects				Enter an IP address or a network using t notation (Er. 192.168.80.150 or 192.166 can also enter an IPv6 address or an IPv its prefix (Er. 2001.408:123.1:1 or 2001:408.123.1:1:/64)	the slash 3.80.0/24). You 16 address with		
Patterns	Tags				100		

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.

	Name	Tags	Туре	Zone	Address	User	HIP Profile	
	intrazone-default	none	intrazone	any	any	any	any	
			interzone					
ero Ge	Curity Policy Rule eneral Actions Action Setting Action	Denv			setting	any	©	
ec Ge	Curity Policy Rule eneral Actions Action Setting Action	Deny			setting	g at Session Start	• aiy	
Geo	Curity Policy Rule eneral Actions Action Setting Action	Deny	MP Unreachable		setting ↓ La	g at Session Start g at Session End	©	
Geo	Curity Policy Rule eneral Actions Action Setting Action Profile Setting	Deny	MP Unreachable		Setting Log Forwarding None	g at Session Start g at Session End	•	

Click OK, then click Add at the bottom to add a new security policy. Configure as pictured below.

county F	uncy nuic							
General	Source	User	Destination	Application	Service/URL Category	Actions		
	Name	Outbound-	Catchall					
	Rule Type	universal (default)					-
C	Description	This rule a	llows all outbour	id traffic out to t	he internet.			
	Tags							v
	0					ſ	OK	Cance

Security Policy Rule	0		
General Source User Destination	Application	Service/URL Category	Actions
Any		Any	
Source Zone 🔺		Source Address 🔺	
🗹 🕅 LAN-Trust		IAN_Trust_Subr	net
		+ Add - Delete	
		Negate	
			OK Cancel

Security Policy Rule	1	ତ
General Source	User Destination Applic	ation Service/URL Category Actions
select	V	🗹 Any
Destination Zor	1e 🔺	Destination Address
V PR WAN-Untru	st	
🕂 Add 🖃 Delete		🖶 Add 💭 Deleta
		Negate
		OK

Security Policy Rule	Ø
General Source User Destination Application	Service/URL Category Actions
any	🖾 Any
Service	URL Category -
Make sure to change Service to any!	
Add 🖨 Calante	Calente
	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					6
General Original	Packet Translated Packet				
Name	LAN-To-WAN				
Description					
Tags					-
NAT Type	ipv4				¥
				GK	Cancel
NAT Policy Bule					ল
General Original	Packet Translated Packet				
Алу	Destination Zone		Any	🔽 Алу	
Source Zone	WAN-Untrust	~	Source Address	Destination	Address
V COR LAN-Trust			V Subne	£:	
	Destination Interfac	:e			
	any	~			
	Service				
	any	*			_
🕂 Add 🖃 Delete			🕂 Add 🛛 💻 Delete	🕂 Add 🔳 De	ete
				ОК	Cancel
NAT Policy Rule					Q
General Original	Packet Translated Packet				
Source Address T	ranslation		Destination Addres	s Translation	
Translation Type	Dynamic IP And Port		Translated Address		-
Address Type	Interface Address		Translated Port		
Interface	ethernet1/1	*			
IP Address	None	~			
1					
				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 WEBL :)