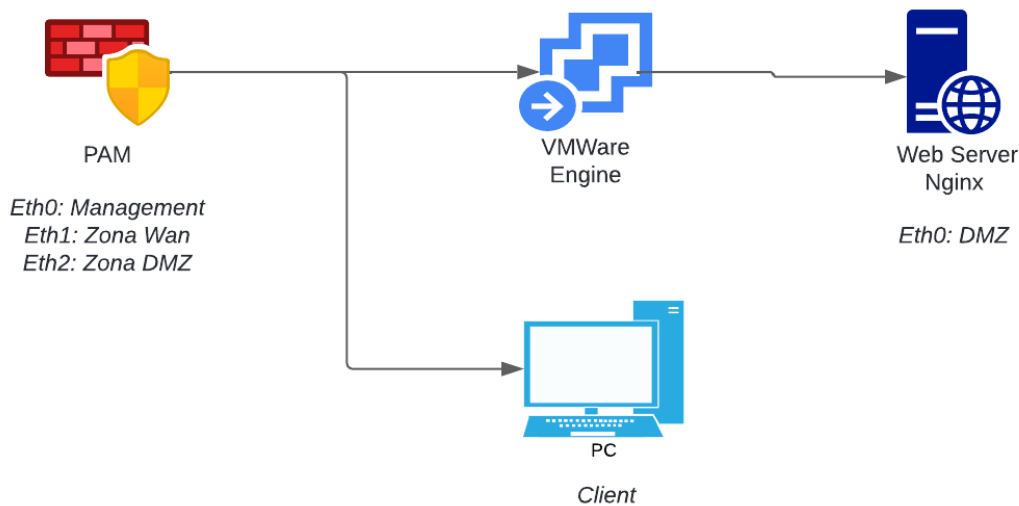


Laboratorio

Palo Alto y Ubuntu server con Enginx

El laboratorio tiene como objetivo simular un entorno de red en el que un servidor Ubuntu, ubicado en una zona DMZ, necesita tener acceso a Internet para descargar actualizaciones y permitir el acceso a un servicio web seguro (HTTPS). Además, se deben implementar políticas de seguridad y reglas de NAT para gestionar el tráfico entre las zonas DMZ y WAN, asegurando que el tráfico sea permitido o bloqueado según las necesidades de la red.



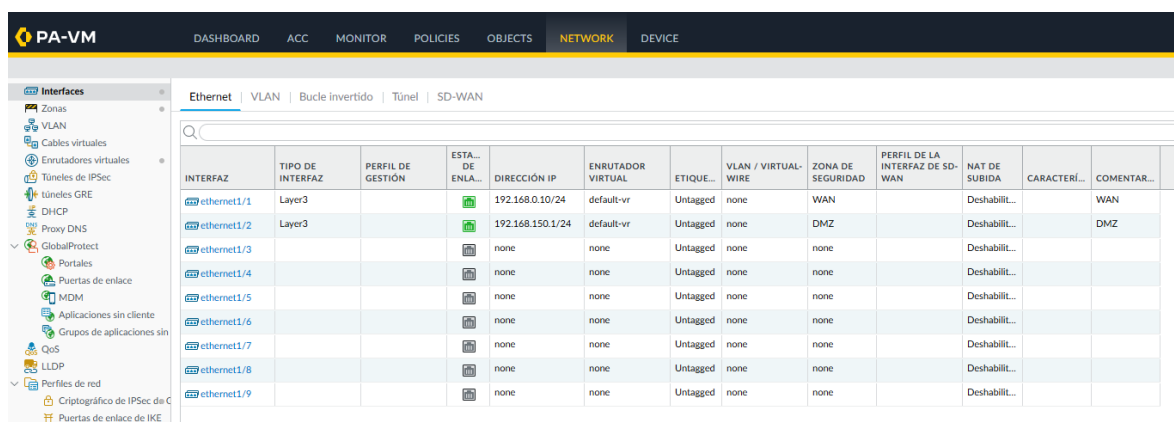
01 | Topología del Laboratorio

Palo Alto VM:

Componente	Interfaz	Fusión	IP Asignada	Zona	Descripción
Palo Alto VM	eth0	Management	192.168.162.128	Management	Administración del firewall
Palo Alto VM	ethernet1/1	WAN	192.168.0.10	WAN	Conectada a la red externa (Internet)
Palo Alto VM	ethernet1/2	DMZ	192.168.150.1	DMZ	conectada al servidor Ubuntu
Ubuntu Server VM	eth0	DMZ	192.168.150.2	DMZ	conectada a la zona DMZ, a través de Palo Alto

Configuración de Interfaces

La correcta configuración de interfaces en Palo Alto y el servidor Ubuntu es fundamental para garantizar que las diferentes zonas de red puedan comunicarse entre sí y con el exterior. El objetivo es configurar las interfaces de red para que el tráfico pueda fluir de manera controlada desde la DMZ (donde está el servidor Ubuntu) hacia Internet a través de la interfaz WAN.



The screenshot shows the Palo Alto VM configuration interface. The top navigation bar includes tabs for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK (selected), and DEVICE. The left sidebar lists various configuration categories like Interfaces, Zonas, VLAN, Cables virtuales, Enrutadores virtuales, Túneles de IPsec, DHCP, Proxy DNS, GlobalProtect, Portales, Puertas de enlace, MDM, Aplicaciones sin cliente, Grupos de aplicaciones sin cliente, QoS, LLDP, and Perfiles de red. The main content area is titled 'Ethernet' and shows a table of interfaces.

INTERFAZ	TIPO DE INTERFAZ	PERFIL DE GESTIÓN	ESTADO DE ENLA...	DIRECCIÓN IP	ENRUTADOR VIRTUAL	ETIQUET...	VLAN / VIRTUAL-WIRE	ZONA DE SEGURIDAD	PERFIL DE LA INTERFAZ DE SD-WAN	NAT DE SUBIDA	CARACTERÍSTICA...	COMENTAR...
ethernet1/1	Layer3			192.168.0.10/24	default-vr	Untagged	none	WAN		Deshabilit...		WAN
ethernet1/2	Layer3			192.168.150.1/24	default-vr	Untagged	none	DMZ		Deshabilit...		DMZ
ethernet1/3				none	none	Untagged	none	none		Deshabilit...		
ethernet1/4				none	none	Untagged	none	none		Deshabilit...		
ethernet1/5				none	none	Untagged	none	none		Deshabilit...		
ethernet1/6				none	none	Untagged	none	none		Deshabilit...		
ethernet1/7				none	none	Untagged	none	none		Deshabilit...		
ethernet1/8				none	none	Untagged	none	none		Deshabilit...		
ethernet1/9				none	none	Untagged	none	none		Deshabilit...		

- Palo Alto
 - eth0 (Management): Se configuró con una IP estática 192.168.162.128 para permitir el acceso de administración.
 - eth1/1 (WAN): Configurada inicialmente para obtener una IP por DHCP, con la posibilidad de cambiar a IP estática (192.168.0.10) si el servidor DHCP no funcionaba correctamente.
 - eth1/2 (DMZ): Configurada con la IP 192.168.150.1/24 y conectada directamente al servidor Ubuntu para gestionar el tráfico DMZ-WAN
- Configuración en el Servidor Ubuntu
 - IP Address: 192.168.150.2 asignada manualmente a la interfaz eth0.
 - Gateway: 192.168.150.1 (interfaz de Palo Alto DMZ), para que el tráfico saliente de Ubuntu sea dirigido a Palo Alto.

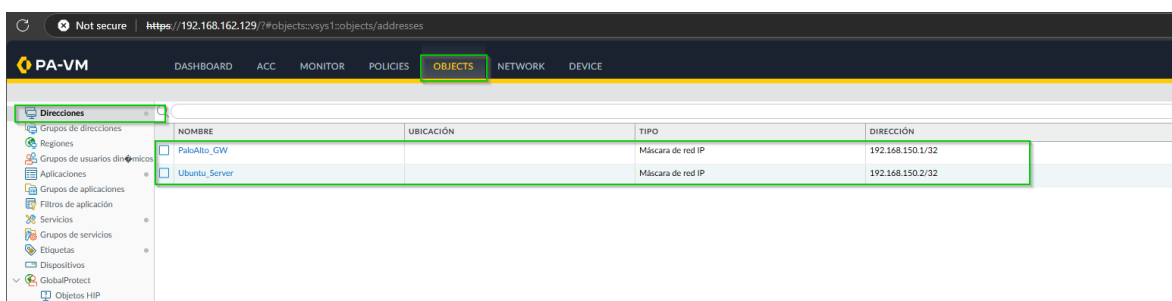
Verificación de Rutas

En el servidor Ubuntu, se verificaron las rutas configuradas para asegurarse de que todo el tráfico saliente se redirige a Palo Alto: ip route

02 | Configuración de los Objetos

En Palo Alto, los objetos permiten simplificar la configuración y administración de las políticas de seguridad, NAT y enrutamiento. En lugar de utilizar direcciones IP estáticas directamente en las reglas, se crean objetos que representan dispositivos o servicios de la red. Esto hace que las configuraciones sean más fáciles de mantener y modificar en el futuro, además de permitir una mayor flexibilidad.

Nombre del Objeto	Tipo	IPs	Descripción
Ubuntu_Server	Máscara de red IP	192.168.150.2/32	Representa al servidor Ubuntu ubicado en la zona DMZ
PaloAlto_GW	Máscara de red IP	192.168.150.1/32	Representa la puerta de enlace (Gateway) en la DMZ, asignada a Palo Alto



03 | Configuración de Zonas

En Palo Alto, las zonas son un componente clave para aplicar políticas de seguridad y segmentar el tráfico entre las diferentes interfaces de red. Cada interfaz de red (WAN, DMZ, etc.) debe estar asociada a una zona para controlar el tráfico que entra y sale de esas interfaces.

- La interfaz eth1 (WAN) se asigna a una zona llamada WAN. Esto permite gestionar el tráfico de Internet y las conexiones hacia y desde esta interfaz de red.
- La interfaz eth2 (DMZ) se asigna a una zona llamada DMZ. Esta zona se utilizará para el tráfico interno entre el firewall y el servidor Ubuntu.

Not securehttps://192.168.162.129/1/network/vm/zones

PA-VM

DASHBOARDACCMONITORPOLICIESOBJECTSNETWORKDEVICE

Consolid

2 elementos

InterfacesZonesVLANCables virtualesEnrutadores virtualesTúneles de IPSecTúneles GREVPNProxy DNSGlobalProtectPortalesPuentes de enlaceMDMMAplicaciones sin clienteGrupos de aplicaciones sin clienteQoSLLDP

Interfaces

Zones

	NOMBRE	TIPO	INTERFACES / SISTEMAS VIRTUALES	PERFIL DE PROTECCIÓN DE ZONA	PROTECCIÓN DE BÚFER DE PAQUETES	AJUSTE DE LOG	ID de usuario		ID del dispositivo			
							HABILITADO	REDES INCLUIDAS	REDES EXCLUIDAS	HABILITADO	REDES INCLUIDAS	REDES EXCLUIDAS
<input type="checkbox"/>	DMZ	layer3	ethernet1/2				<input type="checkbox"/>	cualquiera	ninguno	<input type="checkbox"/>	cualquiera	ninguno
<input type="checkbox"/>	WAN	layer3	ethernet1/1				<input type="checkbox"/>	cualquiera	ninguno	<input type="checkbox"/>	cualquiera	ninguno

04 | Configuración de Virtual Router

En Palo Alto, el Virtual Router es responsable de dirigir el tráfico entre las interfaces y las zonas configuradas. Si se desea mayor control sobre el enrutamiento, o si se tiene una red más compleja, es posible crear un nuevo Virtual Router además del predeterminado.

NOMBRE	INTERFACES	CONFIGURACIÓN	RIP	OSPF	OSPFV3	BGP	MULTIDIFUSIÓN
default		Estado de ECMP: Deshabilitado					
default-vr	ethernet1/1 ethernet1/2	Rutas estáticas: 1 Estado de ECMP: Deshabilitado					

05 | Configuración de Políticas de Seguridad

Las políticas de seguridad en Palo Alto tienen como objetivo definir qué tipo de tráfico está permitido entre las diferentes zonas de red (DMZ, WAN, etc.). Estas políticas deben estar bien definidas para permitir el acceso de Ubuntu a Internet y permitir conexiones seguras (HTTPS) hacia el servidor Ubuntu desde la red WAN.

Políticas de Seguridad		
Allow_Ubuntu_Internet	Allow_HTTPS_to_Ubuntu	Allow_ICMP_to_GW
Permitir que el servidor Ubuntu acceda a Internet para actualizaciones.	Permitir acceso HTTPS al servidor Ubuntu desde una red WAN.	Permitir pings (ICMP) desde el servidor Ubuntu hacia la puerta de enlace de la DMZ.
<ul style="list-style-type: none"> Source Zone: DMZ. Destination Zone: WAN. Source Address: Ubuntu_Server. Destination Address: Any. Aplicación: Any. Servicio: Any. 	<ul style="list-style-type: none"> Source Zone: WAN. Destination Zone: DMZ. Destination Address: Ubuntu_Server. Aplicación: HTTPS. Servicio: HTTPS. 	<ul style="list-style-type: none"> Source Zone: DMZ. Destination Zone: DMZ. Destination Address: PaloAlto_GW. Aplicación: Ping (ICMP).

IP Origin													
IP Destino													
NOMBRE	ETIQUETAS	TIPO	ZONA	DIRECCIÓN	USUARIO	DISPOSITIVO	ZONA	DIRECCIÓN	DISPOSITIVO	APLICACIÓN	SERVICIO	ACCIÓN	PERFIL
1. Allow_Ubuntu_Internet	none	universal	DMZ	any	any	any	WAN	any	any	any	application...	Permitir	none
2. Allow_HTTPS_to_Ubuntu	none	universal	WAN	any	any	any	DMZ	any	any	any	service-https	Permitir	none
3. Allow_ICMP_to_GW	none	universal	DMZ	any	any	any	PaloAlto_GW	any	any	any	ping	Permitir	none
4. Intrazone-default	none	Intrazone	any	any	any	any	Intrazone	any	any	any	any	Permitir	none
5. Interzone-default	none	Interzone	any	any	any	any	any	any	any	any	any	Denegar	none

06 | Configuración Nat

La traducción de direcciones de red (NAT) es fundamental para que el tráfico saliente desde la DMZ pueda ser traducido a la IP pública de la interfaz WAN, permitiendo que los dispositivos externos en Internet respondan a las solicitudes del servidor Ubuntu.

Not securehttps://192.168.162.129/?p=policies&vys1p=policies/nat-rulebasePA-VM

DASHBOARDACCMONITORPOLICIESOBJECTSNETWORKDEVICE

192.168.162.129

1 elemento

		Paquete original				Paquete traducido		Uso de reglas					
	NOMBRE	ETIQUETAS	ZONA DE ORIGEN	ZONA DE DESTINO	INTERFAZ DE DESTINO	DIRECCIÓN DE ORIGEN	DIRECCIÓN DE DESTINO	SERVICIO	TRADUCCIÓN DE ORIGEN	TRADUCCIÓN DE DESTINO	RECuento de ACIERTOS	ÚLTIMO ACIERTO	PRIMER ACIERTO
1	NAT_Ubuntu_to_Wi...	none	DMZ	WAN	any	Ubuntu_Server	any	any	dynamic-ip-and-port	ninguno	109	2024-10-20 23:06:19	2024-10-20 21:07:09

07 | Pruebas de Conectividad

Las pruebas de conectividad son esenciales para confirmar que las configuraciones de NAT, políticas de seguridad y rutas están funcionando correctamente. Se realizaron varias pruebas desde el servidor Ubuntu.

Ping desde la PC local a la Ethernet 1/1

```
C:\Users\BayardoCuadra>ping 192.168.0.10

Pinging 192.168.0.10 with 32 bytes of data:
Reply from 192.168.0.10: bytes=32 time=31ms TTL=64
Reply from 192.168.0.10: bytes=32 time<1ms TTL=64
Reply from 192.168.0.10: bytes=32 time=1ms TTL=64
Reply from 192.168.0.10: bytes=32 time=1ms TTL=64





















Ping statistics for 192.168.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 31ms, Average = 8ms
```

Ping de Ubuntu a Internet y al Gateway

```
bcuadra@rootserver:/etc/netplan$
bcuadra@rootserver:/etc/netplan$
bcuadra@rootserver:/etc/netplan$ ping 192.168.150.1
PING 192.168.150.1 (192.168.150.1) 56(84) bytes of data.
^C
--- 192.168.150.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2080ms

bcuadra@rootserver:/etc/netplan$ ping 192.168.150.1
PING 192.168.150.1 (192.168.150.1) 56(84) bytes of data.
64 bytes from 192.168.150.1: icmp_seq=1 ttl=64 time=3.58 ms
64 bytes from 192.168.150.1: icmp_seq=2 ttl=64 time=1.71 ms
64 bytes from 192.168.150.1: icmp_seq=3 ttl=64 time=1.59 ms
64 bytes from 192.168.150.1: icmp_seq=4 ttl=64 time=1.67 ms
64 bytes from 192.168.150.1: icmp_seq=5 ttl=64 time=0.714 ms
64 bytes from 192.168.150.1: icmp_seq=6 ttl=64 time=0.929 ms
^C
--- 192.168.150.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5057ms
rtt min/avg/max/mdev = 0.714/1.698/3.578/0.922 ms
bcuadra@rootserver:/etc/netplan$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=52.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=49.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=58.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=115 time=65.8 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=115 time=61.5 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=115 time=56.0 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=115 time=76.9 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=115 time=53.5 ms
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7010ms
rtt min/avg/max/mdev = 49.248/59.166/76.948/8.325 ms
bcuadra@rootserver:/etc/netplan$
```

Monitor de Palo Alto.

DASHBOARDACCMONITORPOLICIESOBJECTSNETWORKDEVICE																Commit		Manual	
																Manual			
	FECHA DE REGISTRO	NAT IP DESTINO	TIPO	ZONA ORIGEN	ZONA DESTINO	IP ORIGEN	USUARIO DE ORIGEN	GRUPO DE DIRECCIONES DINAMICAS DE ORIGEN	IP DESTINO	GRUPO DE DIRECCIONES DINAMICAS DE DESTINO	GRUPO DE USUARIOS DINAMICOS	PUER... DEST...	APLICACIÓN	ACCIÓN	REGLA	RAZÓN DEL FIN DE SESIÓN	BYTES	ID DE SESIÓN O CONEXIÓN HTTP/2	
	10/21 17:42:44	8.8.4.4	end	DMZ	WAN	192.168.150.2			8.8.4.4			53	dns-base	allow	Allow_Ubuntu_L...	tcp-fin	2.1k	0	
	10/21 17:42:24	91.189.91.82	end	DMZ	WAN	192.168.150.2			91.189.91.82			80	apt-get	allow	Allow_Ubuntu_L...	tcp-fin	185.0k	0	
	10/21 17:41:04	8.8.4.4	end	DMZ	WAN	192.168.150.2			8.8.4.4			53	dns-base	allow	Allow_Ubuntu_L...	tcp-fin	1.5k	0	
	10/21 17:40:59	185.125.190.56	end	DMZ	WAN	192.168.150.2			185.125.190.56			123	ntp-base	allow	Allow_Ubuntu_L...	aged-out	180	0	
	10/21 17:37:53	8.8.4.4	end	DMZ	WAN	192.168.150.2			8.8.4.4			53	dns-base	allow	Allow_Ubuntu_L...	tcp-fin	2.8k	0	
	10/21 17:37:38	8.8.8.8	end	DMZ	WAN	192.168.150.2			8.8.8.8			0	ping	allow	Allow_Ubuntu_L...	aged-out	392	0	
	10/21 17:37:33	91.189.91.47	end	DMZ	WAN	192.168.150.2			91.189.91.47			443	ssl	allow	Allow_Ubuntu_L...	tcp-rst-from-client	23.4k	0	
	10/21 17:37:28	8.8.8.8	end	DMZ	WAN	192.168.150.2			8.8.8.8			0	ping	allow	Allow_Ubuntu_L...	aged-out	980	0	
	10/21 17:37:18	8.8.8.8	end	DMZ	WAN	192.168.150.2			8.8.8.8			53	dns-base	allow	Allow_Ubuntu_L...	aged-out	582	0	
	10/21 17:36:58	8.8.8.8	end	DMZ	WAN	192.168.150.2			8.8.8.8			0	ping	allow	Allow_Ubuntu_L...	aged-out	1.2k	0	
	10/21 17:36:48	8.8.8.8	end	DMZ	WAN	192.168.150.2			8.8.8.8			0	ping	allow	Allow_Ubuntu_L...	aged-out	588	0	
	10/21 17:36:43	8.8.8.8	end	DMZ	WAN	192.168.150.2			8.8.8.8			0	ping	allow	Allow_Ubuntu_L...	aged-out	1.2k	0	
	10/21 17:36:33	8.8.8.8	end	DMZ	WAN	192.168.150.2			8.8.8.8			0	ping	allow	Allow_Ubuntu_L...	aged-out	1.2k	0	
	10/21 17:36:28	8.8.8.8	end	DMZ	WAN	192.168.150.2			8.8.8.8			0	ping	allow	Allow_Ubuntu_L...	aged-out	1.4k	0	
	10/21 17:36:23	8.8.8.8	end	DMZ	WAN	192.168.150.2			8.8.8.8			0	ping	allow	Allow_Ubuntu_L...	aged-out	1.2k	0	
	10/21 17:36:18	8.8.8.8	end	DMZ	WAN	192.168.150.2			8.8.8.8			0	ping	allow	Allow_Ubuntu_L...	aged-out	1.4k	0	
	10/21 17:36:08	8.8.8.8	end	DMZ	WAN	192.168.150.2			8.8.8.8			0	ping	allow	Allow_Ubuntu_L...	aged-out	1.2k	0	
	10/21 17:36:03		end	DMZ	WAN	192.168.150.2			8.8.8.8			0	ping	allow	Allow_Ubuntu_L...	aged-out	980	0	
	10/21 17:35:58		end	DMZ	WAN	192.168.150.2			8.8.8.8			0	ping	allow	Allow_Ubuntu_L...	aged-out	686	0	
	10/21 17:35:53		end	DMZ	WAN	192.168.150.2			8.8.8.8			0	ping	allow	Allow_Ubuntu_L...	aged-out	588	0	

08 | Copias de Seguridad

Para exportar configuraciones;

