

# Deploy a Palo Alto Firewall in Exoscale cloud



06/01/2022

Limited distribution only

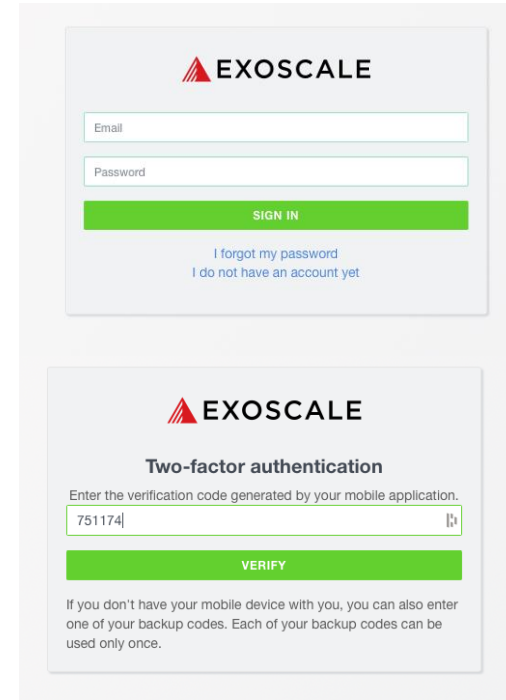


# Connect to Exoscale platform

Go to the Exoscale website (<https://www.exoscale.com>) and click on “Log in”



Enter your credentials and click on “Sign in”

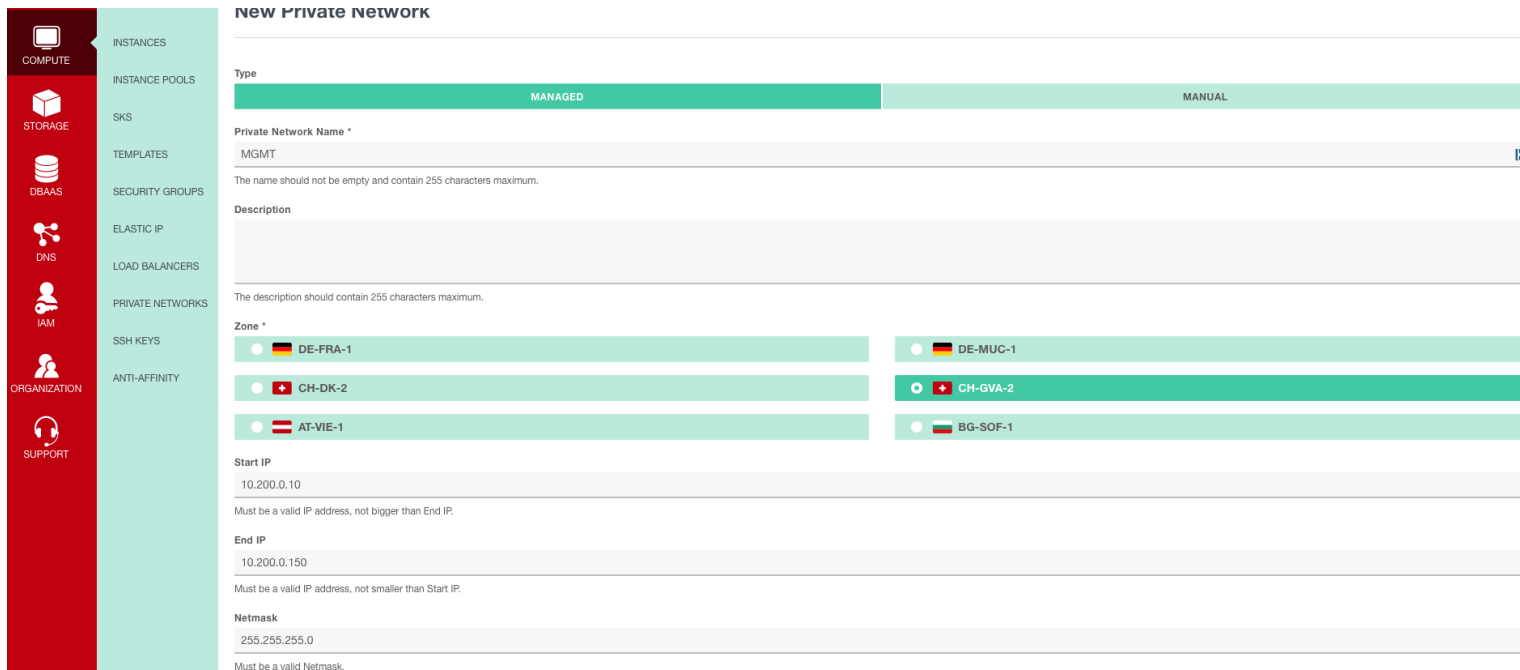
The image shows the Exoscale login and two-factor authentication form. The top section is for logging in, with fields for Email and Password, a "SIGN IN" button, and links for "I forgot my password" and "I do not have an account yet". The bottom section is for two-factor authentication, with a "Two-factor authentication" heading, a text prompt "Enter the verification code generated by your mobile application.", a text input field containing "751174", a "VERIFY" button, and a note about backup codes.

The background features a light gray field with faint, horizontal lines of binary code (0s and 1s). Overlaid on this are large, dark red geometric shapes, specifically concentric squares and rectangles that form a stylized, nested pattern. A diagonal white line cuts across the image from the top-left towards the bottom-right, separating the red shapes into two main sections.

**Customer order**

# Create private networks

Define new private networks if needed (you reuse the existing)



**NEW PRIVATE NETWORK**

Type

MANAGED MANUAL

Private Network Name \*

MGMT

The name should not be empty and contain 255 characters maximum.

Description

The description should contain 255 characters maximum.

Zone \*

DE-FRA-1 DE-MUC-1

CH-DK-2 CH-GVA-2

AT-VIE-1 BG-SOF-1

Start IP

10.200.0.10

Must be a valid IP address, not bigger than End IP.

End IP

10.200.0.150

Must be a valid IP address, not smaller than Start IP.

Netmask

255.255.255.0

Must be a valid Netmask.

# Create a new instance from the public template

Go in “Compute > Instance” on the Exoscale Dashboard, and click on “Add”

**Instances**

START | STOP | REBOOT | DESTROY

Instance Display Name	OS Template	Disk	Security Group	Instance Type	IP Address	Zone	Status
-----------------------	-------------	------	----------------	---------------	------------	------	--------

☐ Instance Display Name

OS Template / Disk

Security Group

Instance Type

IP Address

Zone

Status

FILTER INSTANCES DISPLAY NAMES

**ADD**

- Add a Hostname
- Choose Template
- Choose the zone (Datacenter)

**New Instance**

Current balance: CHF 64.95 SCRT-TESTKO ?

**Hostname**

FW-PaloAltoNetworks-Active

Name of the resource, can be up to 253 characters, must begin with a letter, end with a letter or a number, and contain only letters, digits and the '-' char.

**Template**

FILTER TEMPLATE NAMES

PA-VM-KVM-10.1.0	2021-10-07 08:05:07
Palo Alto Network FW - 10.1.3	2022-01-24 10:12:43

**Zone**

CH-DK-2	CH-GVA-2
DE-FRA-1	DE-MUG-1
AT-VIE-1	BG-SOF-1

**Your Instance:**

FW-PaloAltoNetworks-Active

**ZONE**

CH-GVA-2

**TEMPLATE**

Palo Alto Network FW - 10.1.3

**INSTANCE TYPE**

Standard - Medium  
2 CPU + 4 GB RAM

**DISK SIZE**

100 GB SSD

**SSH KEY**

test1

**SECURITY GROUPS**

default

**CREATE**

# Create a new instance from the public template (cont'd)

- Choose the VM size

Instance Type

	CPU	RAM
STANDARD >	Micro	1 512 MB
STORAGE	Tiny	1 1 GB
MEMORY	Small	2 2 GB
CPU	<b>Medium</b>	<b>4 4 GB</b>
GPU	Large	4 8 GB
GPU2	Extra-Large	4 16 GB
	Huge	8 32 GB
	Mega	12 64 GB <b>ENABLE</b>
	Titan	16 128 GB <b>ENABLE</b>
	Jumbo	24 225 GB <b>ENABLE</b>

Your Instance:  
FW-PaloAltoNetworks-Active

ZONE  
CH-GVA-2

TEMPLATE  
Palo Alto Network FW - 10.1.3

INSTANCE TYPE  
Standard - Medium  
2 CPU - 4 GB RAM

DISK SIZE  
100 GB SSD

SSH KEY  
test1

SECURITY GROUPS  
default

**CREATE**

# Create a new instance from the public template (cont'd)

- Choose the Disk size
- Choose a keypair\*
- Choose default Security groups
- Choose private Networks\*

**Disk**

100 GB 200 GB 400 GB

**Keypair**

You have no keypairs at the moment.  
If you wish, you may create one here.

We strongly encourage you to use keypairs instead of a plain password. [Read more on the Exoscale documentation.](#)

**Security Groups**

☒ default

**Private Networks**

☐ test ☒ INSIDE

☒ DATACENTER ☒ MGMT

**IPv6**

☐ Enable IPv6

**Anti-Affinity Groups**

**User Data**

Your Instance:

**FW-PaloAltoNetworks-Active**

**ZONE**

 CH-GVA-2

**TEMPLATE**

 Palo Alto Network FW - 10.1.3

**INSTANCE TYPE**

Standard - Medium  
2 CPU • 4 GB RAM

**DISK SIZE**

100 GB SSD

**SECURITY GROUPS**

default

**PRIVATE NETWORKS**

MGMT - DATACENTER - INSIDE

**CREATE**

\* not mandatory

# VM deployment

## The VM is deploying

INSTANCES

INSTANCE POOLS

SKS

TEMPLATES

SECURITY GROUPS

ELASTIC IP

LOAD BALANCERS

PRIVATE NETWORKS

SSH KEYS

ANTI-AFFINITY

### FW-PaloAltoNetworks-Active

MOVE | SCALE | OPEN CONSOLE

▶ START | ◻ STOP | ↺ REBOOT | ↻ REINSTALL | ✕ DESTROY

STOPPED

OS Template

Palo Alto Network FW - 10.1.3

Zone

CH-GVA-2

Instance IP

IPv4:

ENABLE IPV6 ON THIS INSTANCE

Instance ID

39ddb557-2d44-4ead-b483-ccaa9b7245be

Instance Type: Medium

4 GB / 2 x 2198 MHz

Disk

100 GB

Instance Hostname

FW-PaloAltoNetworks-Active

Instance Display Name

FW-PaloAltoNetworks-Active

Reverse DNS

None set yet.

SSH command

Stopped instances can't be accessed.

SSH Password

RESET PASSWORD

Your password is not available anymore.  
Passwords are available only for the duration of your session.  
We encourage you to use keypairs instead. [Read more on the Exoscale documentation.](#)

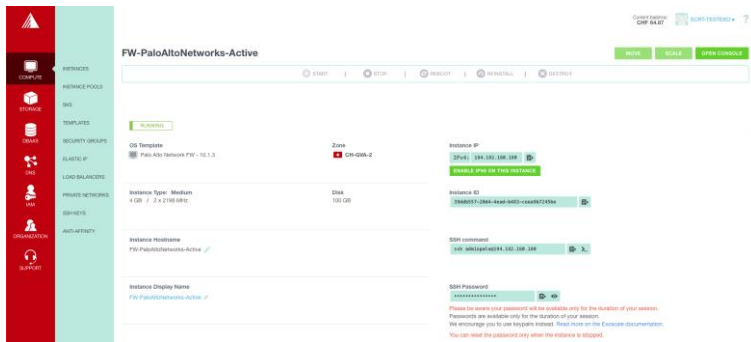
Anti-Affinity Groups

Your instance is not attached to any Anti-Affinity group.



# Palo Alto Networks Management

The VM is running after 5-10 minutes, copy the public IP address or the ssh command and try a connection



SSH command

```
ssh adminpalo@194.182.160.180
```

The login is not valid, the correct user is **admin**

```
sharkmo@CHWSME001 ~ % ssh admin@194.182.160.180
(admin@194.182.160.180) Password:

Number of failed attempts since last successful login: 0

admin@PA-VM>
```

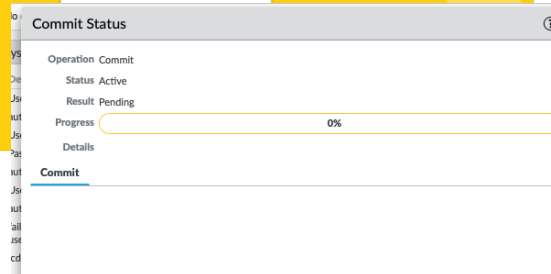
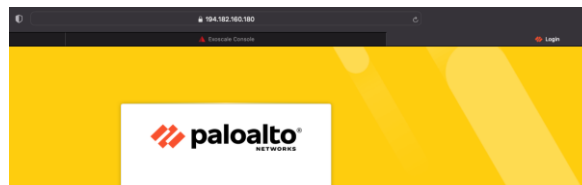
Instance IP

IPv4: 194.182.160.180

ENABLE IPV6 ON THIS INSTANCE

The default credentials are **admin / admin**

Change the password and make a commit



# Create an Interface Management Profile

In “Network > Interface Mgmt”, create a profile “PingOnly” and enable the service ping

Interface Management Profile

Name: PingOnly

Administrative Management Services

- ☐ HTTP
- ☐ HTTPS
- ☐ Telnet
- ☐ SSH

Network Services

- ☒ Ping
- ☐ HTTP OCSP
- ☐ SNMP
- ☐ Response Pages
- ☐ User-ID
- ☐ User-ID Syslog Listener-SSL
- ☐ User-ID Syslog Listener-UDP

PERMITTED IP ADDRESSES

+ Add - Delete

Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64

OK Cancel

# Create an Interface Management Profile

In “Network > Interface Mgmt”, create a profile “HTTPS-SSH-Ping” and enable the service https, ssh and ping

Interface Management Profile

Name: HTTPS-SSH-Ping

Administrative Management Services

- ☐ HTTP
- ☒ HTTPS
- ☐ Telnet
- ☒ SSH

Network Services

- ☒ Ping
- ☐ HTTP OCSP
- ☐ SNMP
- ☐ Response Pages
- ☐ User-ID
- ☐ User-ID Syslog Listener-SSL
- ☐ User-ID Syslog Listener-UDP

PERMITTED IP ADDRESSES

+ Add - Delete

Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64

OK Cancel

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Interfaces

NAME	PING	TELNET	SSH	HTTP	HTTP OCSP	HTTPS	SNMP	RESPONSE PAGE
HTTPS-SSH-Ping	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PingOnly	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

# Create Zones

In “Network > Zones”, create 3 zones (Outside, Datacenter, Inside)

**Zone Configuration:**

- Name: Inside
- Log Setting: None
- Type: Layer3
- INTERFACES: (Empty list)
- User Identification ACL: ☐ Enable User Identification, INCLUDE LIST (Empty)
- Device-ID ACL: ☐ Enable Device Identification, INCLUDE LIST (Empty)
- Zone Protection: Zone Protection Profile: None, ☒ Enable Packet Buffer Protection

**PA-VM Dashboard:** DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, DEVICE

**Zones Table:**

NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING
<input type="checkbox"/> Datacenter	layer3			<input checked="" type="checkbox"/>	
<input type="checkbox"/> Inside	layer3			<input checked="" type="checkbox"/>	
<input type="checkbox"/> Outside	layer3			<input checked="" type="checkbox"/>	

# Configure the interface ethernet1/1

In “Network > Interfaces”, attach the management profile “HTTPS-SSH-Ping” to the interface ethernet1/1 and set the interface in L3 in DHCP mode

**Ethernet Interface** ⓘ

Interface Name: ethernet1/1  
Comment:   
Interface Type: Layer3  
Netflow Profile: None

Config | IPv4 | IPv6 | SD-WAN | Advanced

Assign Interface To

Virtual Router: default  
Security Zone: Outside

OK Cancel

**Ethernet Interface** ⓘ

Interface Name: ethernet1/1  
Comment:   
Interface Type: Layer3  
Netflow Profile: None

Config | IPv4 | IPv6 | SD-WAN | **Advanced**

Link Settings

Link Speed: auto Link Duplex: auto Link State: auto

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

Management Profile: HTTPS-SSH-Ping

MTU: [576 - 1500]

☐ Adjust TCP MSS

IPv4 MSS Adjustment: 40  
IPv6 MSS Adjustment: 60

☐ Untagged Subinterface

OK Cancel

- Add the default virtual router
- Add the “Outside” zone

**Ethernet Interface** ⓘ

Interface Name: ethernet1/1  
Comment:   
Interface Type: Layer3  
Netflow Profile: None

Config | **IPv4** | IPv6 | SD-WAN | Advanced

☐ Enable SD-WAN

Type: ☐ Static ☐ PPPoE ☒ DHCP Client

☒ Enable

☒ Automatically create default route pointing to default gateway provided by server

☐ Send Hostname system-hostname

Default Route Metric: 10

Show DHCP Client Runtime Info

OK Cancel

# Configure the interface ethernet1/2

In “Network > Interfaces”, attach the management profile “PingOnly” to the interface ethernet1/2 and set the interface in L3 in DHCP mode

The screenshot shows the 'Ethernet Interface' configuration window with the 'Config' tab selected. The 'Interface Name' is 'ethernet1/2'. The 'Interface Type' is 'Layer3'. The 'Netflow Profile' is 'None'. The 'Assign Interface To' section shows 'Virtual Router' set to 'default' and 'Security Zone' set to 'Datacenter'. There are 'OK' and 'Cancel' buttons at the bottom right.

The screenshot shows the 'Ethernet Interface' configuration window with the 'Advanced' tab selected. The 'Link Settings' section shows 'Link Speed' set to 'auto', 'Link Duplex' set to 'auto', and 'Link State' set to 'auto'. The 'Other Info' section shows 'Management Profile' set to 'PingOnly' and 'MTU' set to '40'. There are 'OK' and 'Cancel' buttons at the bottom right.

- Add the default virtual router
- Add the “Datacenter” zone

The screenshot shows the 'Ethernet Interface' configuration window with the 'IPv4' tab selected. The 'Type' is 'DHCP Client'. The 'Default Route Metric' is '10'. There are 'OK' and 'Cancel' buttons at the bottom right.

# Configure the interface ethernet1/3

In “Network > Interfaces”, attach the management profile “PingOnly” to the interface ethernet1/3 and set the interface in L3 in DHCP mode

**Ethernet Interface** ⓘ

Interface Name: ethernet1/3  
Comment:   
Interface Type: Layer3  
Netflow Profile: None

Config | IPv4 | IPv6 | SD-WAN | Advanced

Assign Interface To

Virtual Router: default  
Security Zone: Inside

OK Cancel

**Ethernet Interface** ⓘ

Interface Name: ethernet1/3  
Comment:   
Interface Type: Layer3  
Netflow Profile: None

Config | IPv4 | IPv6 | SD-WAN | **Advanced**

Link Settings

Link Speed: auto Link Duplex: auto Link State: auto

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

Management Profile: PingOnly  
MTU: [576 - 1500]

☐ Adjust TCP MSS  
IPv4 MSS Adjustment: 40  
IPv6 MSS Adjustment: 60

☐ Untagged Subinterface

OK Cancel

- Add the default virtual router
- Add the “Inside” zone

**Ethernet Interface** ⓘ

Interface Name: ethernet1/3  
Comment:   
Interface Type: Layer3  
Netflow Profile: None

Config | **IPv4** | IPv6 | SD-WAN | Advanced

☐ Enable SD-WAN

Type ☐ Static ☐ PPPoE ☒ DHCP Client

☒ Enable  
☒ Automatically create default route pointing to default gateway provided by server  
☐ Send Hostname: system-hostname

Default Route Metric: 10

[Show DHCP Client Runtime Info](#)

OK Cancel

# Palo Alto Networks Interfaces summary

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Interfaces

- Zones
- VLANs
- Virtual Wires
- Virtual Routers
- IPSec Tunnels
- GRE Tunnels
- DHCP
- DNS Proxy
- GlobalProtect
- Portals
- Gateways
- MDM

Ethernet | VLAN | Loopback | Tunnel | SD-WAN

Q

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	UPSTREAM NAT
ethernet1/1	Layer3	HTTPS-SSH-Ping		Dynamic-DHCP Client	default	Untagged	none	Outside		Disabled
ethernet1/2	Layer3	PingOnly		Dynamic-DHCP Client	default	Untagged	none	Datacenter		Disabled
ethernet1/3	Layer3	PingOnly		Dynamic-DHCP Client	default	Untagged	none	Inside		Disabled
ethernet1/4				none	none	Untagged	none	none		Disabled
ethernet1/5							none	none		Disabled

Commit Status

Operation Commit

Status Active

Result Pending

Progress 0%

Details

Commit



# Palo Alto Networks Interfaces summary

After the commit, the interfaces are enable and you could see the IPs from the DHCP range define in the Private networks selected during deployment

The screenshot displays the Palo Alto Networks PA-VM Network configuration interface. The top navigation bar includes DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK (selected), and DEVICE. The left sidebar shows a tree view of network objects, with 'Interfaces' expanded. The main content area shows a table of Ethernet interfaces.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	UPSTREAM NAT	FEATURES
ethernet1/1	Layer3	HTTPS-SSH-Ping	🟢	Dynamic-DHCP Client	default	Untagged	none	Outside		Disabled	
ethernet1/2	Layer3	PingOnly	🟢	Dynamic-DHCP Client	default	Untagged	none	Datacenter		Disabled	
ethernet1/3	Layer3	PingOnly	🟢	Dynamic-DHCP Client	default	Untagged	none	Inside		Disabled	
ethernet1/4			🟡	none	none	Untagged	none				
ethernet1/5			🟡	none	none	Untagged	none				

Below the table, three 'Dynamic IP Interface Status' panels are shown for interfaces ethernet1/1, ethernet1/2, and ethernet1/3. Each panel displays the interface name, state (Bound), remaining lease time, IP address, gateway, and DNS settings.

On the right, the 'Private Network' section provides details for each instance. It includes a search bar and lists three managed private networks: INSIDE, DATACENTER, and MGMT. Each network entry shows its MAC address and IP address.

**Dynamic IP Interface Status (ethernet1/1):**

- Interface: ethernet1/1
- State: Bound
- Remaining Lease Time: 0 days 3:56:49
- IP Address: 10.200.0.136
- Gateway: 0.0.0.0
- Primary DNS: 0.0.0.0
- Secondary DNS: 0.0.0.0
- Primary WINS: 0.0.0.0

**Dynamic IP Interface Status (ethernet1/2):**

- Interface: ethernet1/2
- State: Bound
- Remaining Lease Time: 0 days 3:56:34
- IP Address: 10.99.0.43
- Gateway: 0.0.0.0
- Primary DNS: 0.0.0.0

**Dynamic IP Interface Status (ethernet1/3):**

- Interface: ethernet1/3
- State: Bound
- Remaining Lease Time: 0 days 3:56:23
- IP Address: 10.0.0.28
- Gateway: 0.0.0.0

**Private Network Details:**

- INSIDE - [MANAGED]**  
MAC: 0a:c3:fe:07:2c:b0  
IP Address: 10.0.0.28
- DATACENTER - [MANAGED]**  
MAC: 0a:ef:32:07:2d:37  
IP Address: 10.99.0.43
- MGMT - [MANAGED]**  
MAC: 0a:bd:80:08:1b:34  
IP Address: 10.200.0.136

# Swap Interface to move the public IP on the ethernet1/1

From Exoscale, the public interface is always the first hypervisor interface. You need to move the Public IP from Mgmt to ethernet1/1 within the Palo Alto Networks Virtual Machine

To do this, a special CLI command must be executed in the Palo Alto Networks VM in SSH (Reboot mandatory):

**# set system setting mgmt-interface-swap enable yes**

```
admin@PA-VM> set system setting mgmt-interface-swap enable yes
<Enter> Finish input

admin@PA-VM> set system setting mgmt-interface-swap enable yes
Warning: System restart required to take effect changes. Management interface will swap after restart. Do you want to continue? (y or n)

Reboot system to take effect new changes. After reboot use IP address of eth0 (external to VM)

admin@PA-VM> █
```

```
admin@PA-VM> request restart system
Executing this command will disconnect the current session. Do you want to continue? (y or n)

Broadcast message from root (pts/0) (Mon Jan 24 11:17:58 2022):

The system is going down for reboot NOW!
Connection to 194.182.160.180 closed.
sharkmo@CHWSMME001 ~ % █
```

Launch a Terminal and ping the public IP (in this documentation 194.182.160.180)



As you could see, the public IP 194.182.160.180 has moved on the ethernet1/1

In case of issue with default routes given by DHCP Exoscale, try to shut ethernet1/2 and ethernet 1/3 and then commit (Exoscale console mode)

```
admin@PA-VM# set network interface ethernet ethernet1/2 link-state down
[edit]
admin@PA-VM# set network interface ethernet ethernet1/3 link-state down
[edit]
admin@PA-VM# commit
```

## Now the Ping works

```
admin@PA-VM> show interface
all Show all interface information
ethernet1/1 ethernet1/1
ethernet1/2 ethernet1/2
ethernet1/3 ethernet1/3
hardware Show all hardware interface information
logical Show all logical interface information
management Show management interface information
<value> <name> interface name
```

```
admin@PA-VM> show interface all
```

```
total configured hardware interfaces: 3
```

name	id	speed/duplex/state	mac address
ethernet1/1	16	10000/full/up	06:4b:ea:00:0f:49
ethernet1/2	17	10000/full/up	0a:ef:32:07:2d:37
ethernet1/3	18	10000/full/up	0a:c3:fe:07:2c:b0

```
aggregation groups: 0
```

```
total configured logical interfaces: 3
```

name	id	usys	zone	forwarding	tag	address
ethernet1/1	16	1	Outside	vr:default	0	194.182.160.180/22
ethernet1/2	17	1	Datacenter	vr:default	0	10.99.0.43/24
ethernet1/3	18	1	Inside	vr:default	0	10.0.0.28/24

```
admin@PA-UM>
```

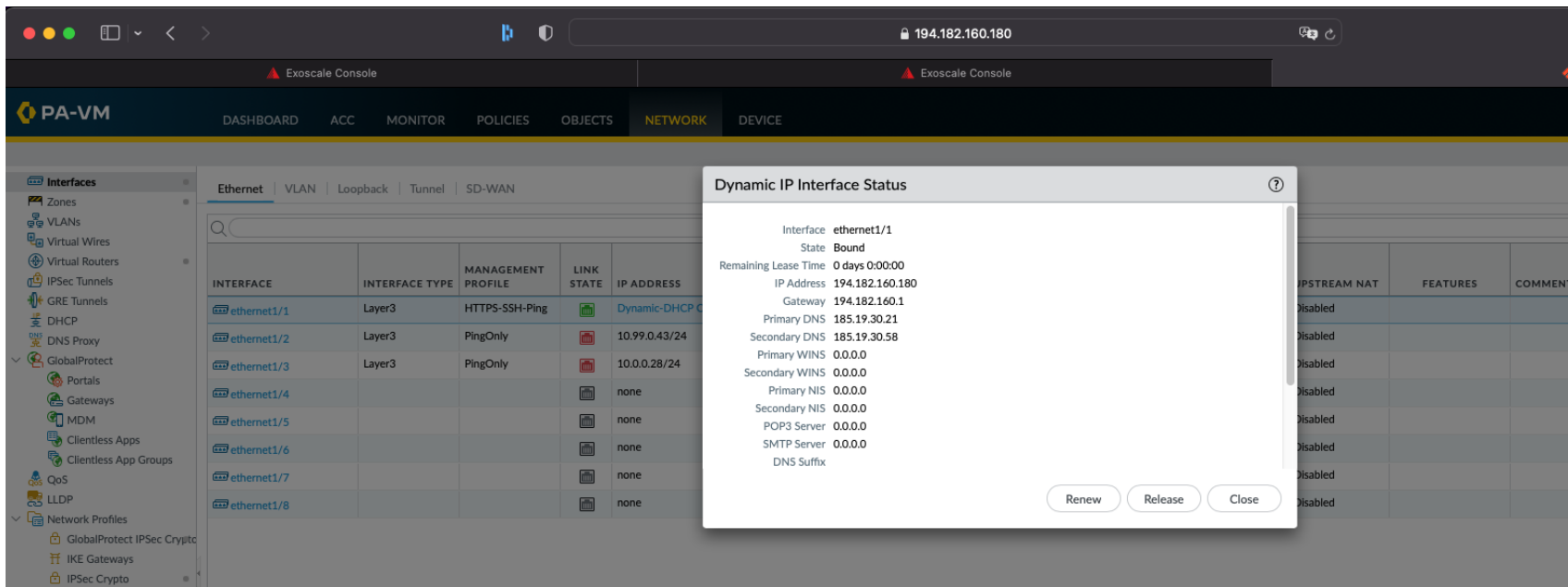
```

sharkmon - ping 194.182.160.180 --70x45
Request timeout for icmp_seq 3387
Request timeout for icmp_seq 3388
Request timeout for icmp_seq 3389
Request timeout for icmp_seq 3390
Request timeout for icmp_seq 3391
Request timeout for icmp_seq 3392
Request timeout for icmp_seq 3393
Request timeout for icmp_seq 3394
Request timeout for icmp_seq 3395
Request timeout for icmp_seq 3396
Request timeout for icmp_seq 3397
Request timeout for icmp_seq 3398
Request timeout for icmp_seq 3399
Request timeout for icmp_seq 3400
Request timeout for icmp_seq 3401
Request timeout for icmp_seq 3402
Request timeout for icmp_seq 3403
Request timeout for icmp_seq 3404
Request timeout for icmp_seq 3405
64 bytes from 194.182.160.180: icmp_seq=3406 ttl=64 time=33.236 ms
64 bytes from 194.182.160.180: icmp_seq=3407 ttl=64 time=31.928 ms
64 bytes from 194.182.160.180: icmp_seq=3408 ttl=64 time=32.442 ms
64 bytes from 194.182.160.180: icmp_seq=3409 ttl=64 time=33.165 ms
64 bytes from 194.182.160.180: icmp_seq=3410 ttl=64 time=31.615 ms
64 bytes from 194.182.160.180: icmp_seq=3411 ttl=64 time=32.864 ms
64 bytes from 194.182.160.180: icmp_seq=3412 ttl=64 time=32.668 ms
64 bytes from 194.182.160.180: icmp_seq=3413 ttl=64 time=32.533 ms
64 bytes from 194.182.160.180: icmp_seq=3414 ttl=64 time=31.615 ms
64 bytes from 194.182.160.180: icmp_seq=3415 ttl=64 time=32.658 ms
64 bytes from 194.182.160.180: icmp_seq=3416 ttl=64 time=33.409 ms
64 bytes from 194.182.160.180: icmp_seq=3417 ttl=64 time=31.264 ms
64 bytes from 194.182.160.180: icmp_seq=3418 ttl=64 time=31.928 ms
64 bytes from 194.182.160.180: icmp_seq=3419 ttl=64 time=32.581 ms
64 bytes from 194.182.160.180: icmp_seq=3420 ttl=64 time=32.318 ms
64 bytes from 194.182.160.180: icmp_seq=3421 ttl=64 time=31.428 ms
64 bytes from 194.182.160.180: icmp_seq=3422 ttl=64 time=31.284 ms
64 bytes from 194.182.160.180: icmp_seq=3423 ttl=64 time=32.205 ms
64 bytes from 194.182.160.180: icmp_seq=3424 ttl=64 time=33.031 ms

```

# Palo Alto Networks Mgmt on Ethernet1/1

Reconfigure the Datacenter (ethernet1/2) and the Inside (ethernet1/3) interfaces with static IPs in each range and re-enable them



The screenshot shows the Palo Alto Networks VM console interface. The left sidebar contains a navigation menu with categories like Interfaces, Zones, VLANs, Virtual Wires, Virtual Routers, IPsec Tunnels, GRE Tunnels, DHCP, DNS Proxy, GlobalProtect, Portals, Gateways, MDM, Clientless Apps, Clientless App Groups, QoS, LLDP, and Network Profiles. The main panel displays the 'Network' configuration page, specifically the 'Ethernet' tab. A modal window titled 'Dynamic IP Interface Status' is open, showing details for interface 'ethernet1/1'. The interface is in a 'Bound' state with a static IP of 194.182.160.180. The modal also shows lease time, gateway, and DNS settings.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS
ethernet1/1	Layer3	HTTPS-SSH-Ping	Dynamic-DHCP	
ethernet1/2	Layer3	PingOnly		10.99.0.43/24
ethernet1/3	Layer3	PingOnly		10.0.0.28/24
ethernet1/4				none
ethernet1/5				none
ethernet1/6				none
ethernet1/7				none
ethernet1/8				none

**Dynamic IP Interface Status**

Interface: ethernet1/1  
State: Bound  
Remaining Lease Time: 0 days 0:00:00  
IP Address: 194.182.160.180  
Gateway: 194.182.160.1  
Primary DNS: 185.19.30.21  
Secondary DNS: 185.19.30.58  
Primary WINS: 0.0.0.0  
Secondary WINS: 0.0.0.0  
Primary NIS: 0.0.0.0  
Secondary NIS: 0.0.0.0  
POP3 Server: 0.0.0.0  
SMTP Server: 0.0.0.0  
DNS Suffix:

Buttons: Renew, Release, Close

# Allowing traffic from Inside/Datacenter to Outside (Internet)

Add a default route in the default virtual router

Virtual Router - Static Route - IPv4

Name: Default

Destination: 0.0.0.0/0

Interface: ethernet1/1

Next Hop: IP Address

194.182.160.180

Virtual Router - default

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

IPv4 | IPv6

1 item

	NAME	DESTINA...	INTERFA...	TYPE	VALUE	ADMIN DISTANCE	METRIC	BFD	ROUTE TABLE
<input type="checkbox"/>	Default	0.0.0.0/0	ethernet1...	ip-address	194.182...	default	10	None	unicast

Add a NAT rule to translate all packets with the Public IP on the Interface ethernet 1/1

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Security

NAT

	NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION	HIT COUNT
1	Default-To-Internet	none	Inside	Outside	ethernet1/1	any	any	any	dynamic ip-and-port	ethernet1/1	-

Add a security that allow the traffic from Inside/Datacenter zone to Outside zone for testing

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Commit

Security

	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	HIT
1	Default-To-Internet	none	universal	Inside	any	any	any	Outside	any	any	any	any	Allow	none		-
2	Intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow	none	none	957
3	Interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny	none		-

# Use the Linux client to test the outgoing traffic

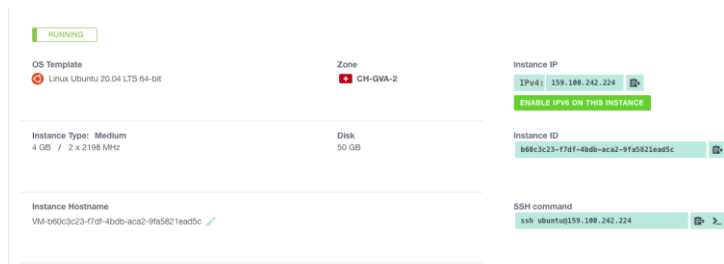
From a Linux client deployed in the datacenter network, configure a specific destination through Palo Alto Network FW (to avoid lose the SSH Control on it)

Username: `ssh ubuntu@159.100.242.224`

Password: `eY5dyaypddqyehj` (To reset when VM stopped)

Let's choose the SCRT website:

([www.scrt.ch](http://www.scrt.ch) - 104.21.29.35, 172.67.171.75)



```
sharkmo@CHWSMME001 ~ % ssh ubuntu@159.100.242.224
ubuntu@159.100.242.224's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-88-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Mon Jan 24 20:42:42 UTC 2022

System load:  0.54               Processes:    132
Usage of /:   4.6% of 48.29GB     Users logged in: 0
Memory usage: 5%                IPv4 address for eth0: 159.100.242.224
Swap usage:   0%

85 updates can be installed immediately.
1 of these updates is a security update.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Oct 18 09:06:41 2021 from 91.175.140.9
ubuntu@VM-b60c3c23-f7df-4bdb-aca2-9fa5821ead5c:~$
ubuntu@VM-b60c3c23-f7df-4bdb-aca2-9fa5821ead5c:~$
ubuntu@VM-b60c3c23-f7df-4bdb-aca2-9fa5821ead5c:~$ sudo -s
root@VM-b60c3c23-f7df-4bdb-aca2-9fa5821ead5c:/home/ubuntu# exit
exit
ubuntu@VM-b60c3c23-f7df-4bdb-aca2-9fa5821ead5c:~$
ubuntu@VM-b60c3c23-f7df-4bdb-aca2-9fa5821ead5c:~$
ubuntu@VM-b60c3c23-f7df-4bdb-aca2-9fa5821ead5c:~$
```

Try to ping the datacenter interface of the FW from the linux client, it shouldn't work:

```
ubuntu@VM-b60c3c23-f7df-4bdb-aca2-9fa5821ead5c:~$ ping 10.99.0.43
PING 10.99.0.43 (10.99.0.43) 56(84) bytes of data.
^C
--- 10.99.0.43 ping statistics ---
16 packets transmitted, 0 received, 100% packet loss, time 15345ms
ubuntu@VM-b60c3c23-f7df-4bdb-aca2-9fa5821ead5c:~$
```

Try to ping [www.scrt.ch](http://www.scrt.ch) from the linux client, it shouldn't work:

```
ubuntu@VM-b60c3c23-f7df-4bdb-aca2-9fa5821ead5c:~$ ping www.scrt.ch
PING www.scrt.ch (104.21.29.35) 56(84) bytes of data.
^C
--- www.scrt.ch ping statistics ---
36 packets transmitted, 0 received, 100% packet loss, time 35846ms
```

# Use the Linux client to test the outgoing traffic (cont'd)

Modify the eth1/1 network interface with an IP in the datacenter subnet.

```
sudo ifconfig eth1 10.99.0.5
sudo ifconfig eth1 netmask 255.255.255.0
sudo ifconfig eth1 up
```

Try to ping the fw, it should work:

```
ubuntu@VM-b60c3c23-f7df-4bdb-aca2-9fa5821ead5c:~$ ping 10.99.0.43
PING 10.99.0.43 (10.99.0.43) 56(84) bytes of data:
64 bytes from 10.99.0.43: icmp_seq=1 ttl=64 time=3.43 ms
64 bytes from 10.99.0.43: icmp_seq=2 ttl=64 time=1.76 ms
64 bytes from 10.99.0.43: icmp_seq=3 ttl=64 time=1.83 ms
64 bytes from 10.99.0.43: icmp_seq=4 ttl=64 time=0.961 ms
64 bytes from 10.99.0.43: icmp_seq=5 ttl=64 time=1.71 ms
^C
--- 10.99.0.43 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 0.961/1.937/3.427/0.808 ms
ubuntu@VM-b60c3c23-f7df-4bdb-aca2-9fa5821ead5c:~$
```

Try to ping [www.scr.t.ch](http://www.scr.t.ch), it shouldn't work

```
ubuntu@VM-b60c3c23-f7df-4bdb-aca2-9fa5821ead5c:~$ ping www.scr.t.ch
PING www.scr.t.ch (172.67.171.75) 56(84) bytes of data:
^C
--- www.scr.t.ch ping statistics ---
13 packets transmitted, 0 received, 100% packet loss, time 12273ms
```

Add the specifics routes

```
sudo route add 104.21.29.35 gw 10.99.0.43 eth1
sudo route add 172.67.171.75 gw 10.99.0.43 eth1
```

Traffic well went through the firewall, this means the internet through the firewall is working

```
ubuntu@VM-b60c3c23-f7df-4bdb-aca2-9fa5821ead5c:~$ ping www.scr.t.ch
PING www.scr.t.ch (172.67.171.75) 56(84) bytes of data:
64 bytes from 172.67.171.75 (172.67.171.75): icmp_seq=12 ttl=54 time=11.1 ms
64 bytes from 172.67.171.75 (172.67.171.75): icmp_seq=13 ttl=54 time=11.2 ms
64 bytes from 172.67.171.75 (172.67.171.75): icmp_seq=14 ttl=54 time=11.2 ms
64 bytes from 172.67.171.75 (172.67.171.75): icmp_seq=15 ttl=54 time=11.1 ms
64 bytes from 172.67.171.75 (172.67.171.75): icmp_seq=16 ttl=54 time=11.1 ms
64 bytes from 172.67.171.75 (172.67.171.75): icmp_seq=17 ttl=54 time=11.1 ms
```

PA-VM																
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE																
Logs																
Traffic																
Threat																
URL Filtering																
WildFire Submissions																
Data Filtering																
Web Malware																
GlobalProtect																
IP-Tag																
Cisco-IDS																
	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	BYTES
	05/24 12:53:31	end	Datacenter	Outside	10.99.0.5			104.21.29.35			0	ping	allow	Default for Internet	agent-out	568
	05/24 12:53:31	start	Datacenter	Outside	10.99.0.5			104.21.29.35			0	ping	allow	Default for Internet	n/a	568
	05/24 12:53:21	start	Datacenter	Outside	10.99.0.5			104.21.29.35			0	ping	allow	Default for Internet	n/a	568



### Test with google.fr IP

## Add the specific route

```
sudo route add -net 172.217.168.0/24 gw 10.99.0.43 eth1
```

Traffic well went through the firewall, this means the internet through the firewall is working:

[illegible]