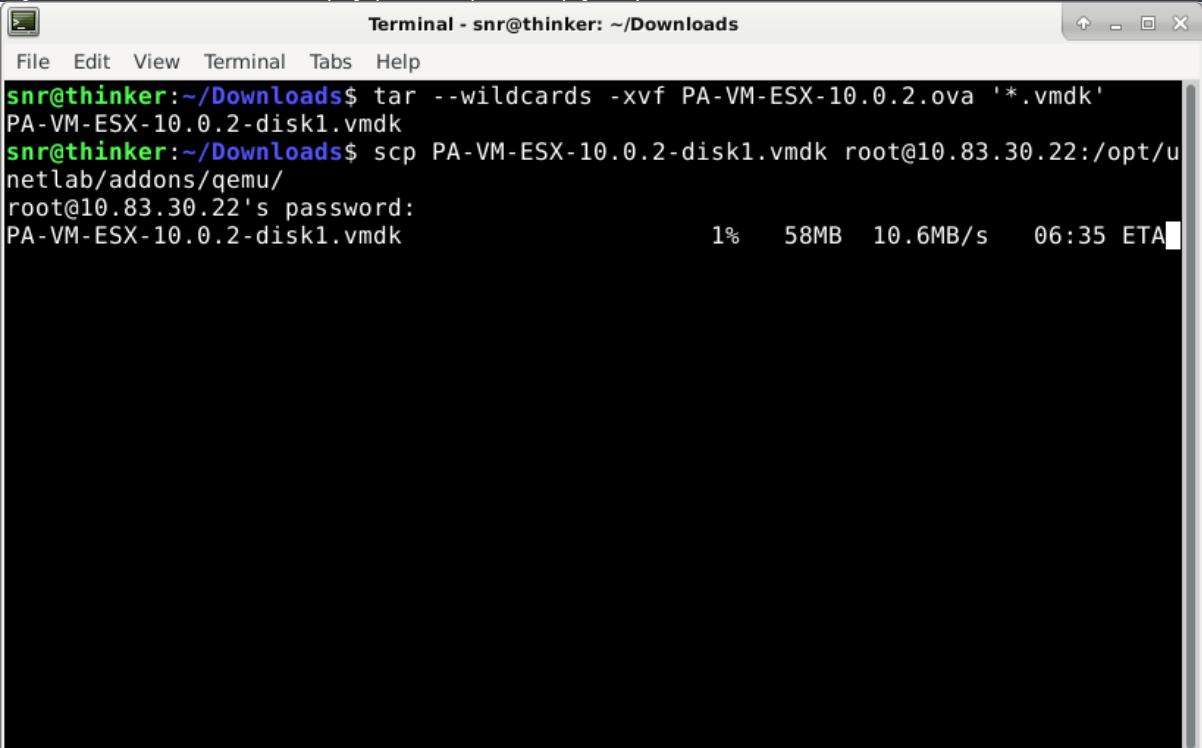


# Running a Palo Alto 10.0.2 VM on EVE-NG

This post will cover using the latest PAN-OS (v10.0.2) ESXi (PAN-OS for VM-Series Base Images) on EVE-NG. First obtain the 10.0.2 OVA file, and then extract the VMDK disk image from it, and upload it to our EVE-NG instance placing the image in the correct folder:

```
tar --wildcards -xvf PA-VM-ESX-10.0.2.ova '*.vmdk'
scp *.vmdk root@10.83.30.22:/opt/unetlab/addons/qemu/
```

A terminal window titled "Terminal - snr@thinker: ~/Downloads" is shown. The terminal output displays the execution of a tar command to extract a VMDK file from an OVA file, followed by an scp command to upload the VMDK file to a remote host. The upload progress bar shows 1% completion, 58MB transferred, a speed of 10.6MB/s, and an estimated time to complete of 06:35.

```
snr@thinker:~/Downloads$ tar --wildcards -xvf PA-VM-ESX-10.0.2.ova '*.vmdk'
PA-VM-ESX-10.0.2-disk1.vmdk
snr@thinker:~/Downloads$ scp PA-VM-ESX-10.0.2-disk1.vmdk root@10.83.30.22:/opt/u
netlab/addons/qemu/
root@10.83.30.22's password:
PA-VM-ESX-10.0.2-disk1.vmdk          1%   58MB  10.6MB/s   06:35 ETA
```

Next, once SSH'd onto the EVE-NG instance, create a Palo Alto instance folder and place the qcow2 formatted VMDK into it:

```
cd /opt/unetlab/addons/qemu/
mkdir paloalto-10.0.2
/opt/qemu/bin/qemu-img convert -f vmdk -O qcow2 PA-VM-ESX-10.0.2-disk1.vmdk ./paloalto-
10.0.2/virtioa.qcow2
/opt/unetlab/wrappers/unl_wrapper -a fixpermissions
rm ./PA-VM-ESX-10.0.2-disk1.vmdk
```

```
Terminal - root@eve-ng: /opt/unetlab/addons/qemu
File Edit View Terminal Tabs Help
snr@thinker:~/Downloads$ ssh -l root 10.83.30.22
root@10.83.30.22's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.20.17-eve-ng-ukms+ x86_64)

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

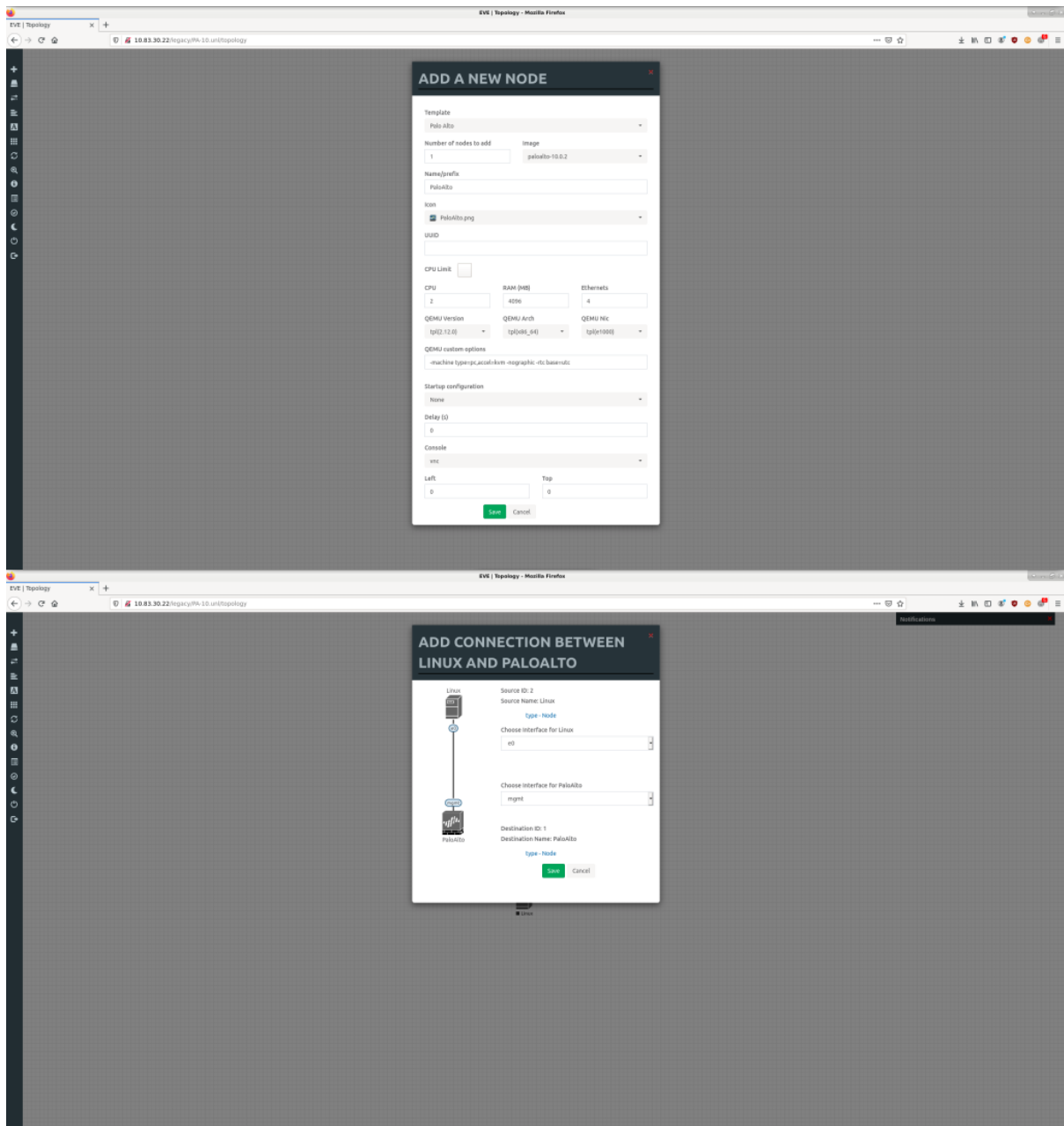
 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

   https://microk8s.io/high-availability
Last login: Fri Dec  4 02:26:30 2020 from 10.83.30.21
root@eve-ng:~# cd /opt/unetlab/addons/qemu/
root@eve-ng:/opt/unetlab/addons/qemu# mkdir paloalto-10.0.2
root@eve-ng:/opt/unetlab/addons/qemu# /opt/qemu/bin/qemu-img convert -f vmdk -O
qcow2 PA-VM-ESX-10.0.2-disk1.vmdk ./paloalto-10.0.2/virtioa.qcow2
root@eve-ng:/opt/unetlab/addons/qemu# /opt/unetlab/wrappers/unl_wrapper -a fixe
rmissions
root@eve-ng:/opt/unetlab/addons/qemu# rm ./PA-VM-ESX-10.0.2-disk1.vmdk
root@eve-ng:/opt/unetlab/addons/qemu#
```

Now install a linux desktop VM (linux-ubuntu-mate-x) which we can use to manage the Palo Alto VM, follow these instructions: <https://www.eve-ng.net/index.php/documentation/howtos/howto-create-own-linux-host-image/>

Login into EVE-NG, I will be using the HTML5 console.

Create a new lab and add the newly minted Palo Alto and ubuntu desktop node to it. Connect the linux node `e0` interface to the `mgmt` interface and then power them both up.



Double click on the Palo Alto VM to bring up its console. You will notice that the login prompt will cycle through three different hostnames ('vm', 'PA-HDF' and 'PA-VM') whilst it brings different internal services online. Once the 'PA-VM' prompt is seen, the management plane is accessible and we can log in with the default credentials (admin/admin) .

Now we need to set the management interface IP address:

```
set deviceconfig system ip-address 192.168.1.254 netmask 255.255.255.0
set deviceconfig system type static
commit
```

```
PA-UM login: admin
Password:
Last login: Thu Dec  3 15:17:04 on tty1

Number of failed attempts since last successful login: 0

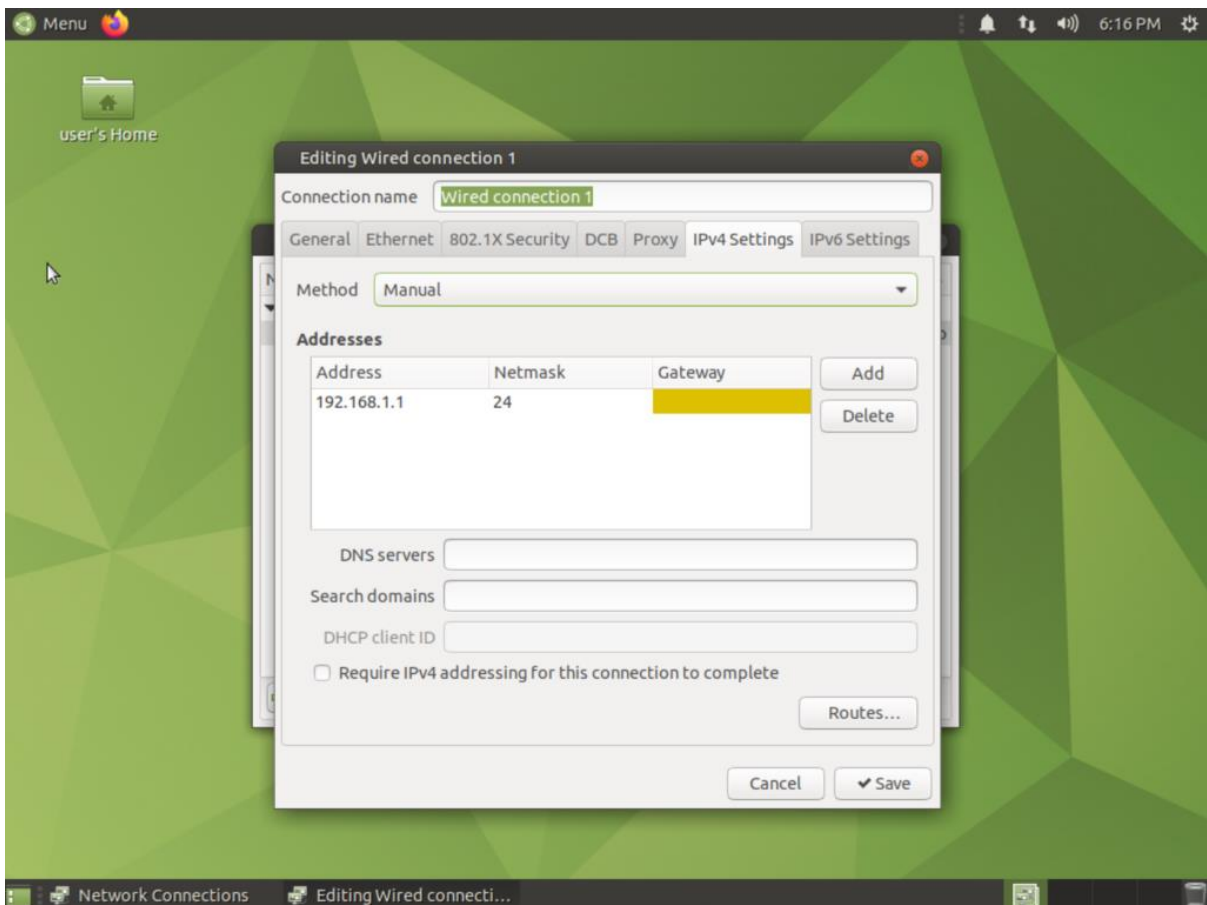
admin@PA-UM> configure
Entering configuration mode
[edit]
admin@PA-UM# set deviceconfig system ip-address 192.168.1.254 netmask 255.255.255.0

[edit]
admin@PA-UM# set deviceconfig system type static

[edit]
admin@PA-UM# commit

Commit job 2 is in progress. Use Ctrl+C to return to command prompt
...55%75%98%._
```

Whilst the commit process is progress, switch to the linux VM and statically assign its network interface with an IP in the 192.168.1.0/24 subnet.



Finally use the using a web browser connect to the <https://192.168.1.254>

PA-VM - Mozilla Firefox

PA-VM

https://192.168.1.254/?#dashboard::vsys1

PA-VM | FIREFOX HOME PAGE | BOARD | ACC | MONITOR | POLICIES | OBJECTS | NETWORK | DEVICE

Welcome

**Welcome to PAN-OS 10.0!**

With this release, Palo Alto Networks introduces a machine learning powered next-generation firewall with proactive capabilities for inline malware and web-based attack prevention, integrated IoT Security to detect and protect IoT devices that cannot run endpoint security, telemetry data collection for security policy optimization, identification and quarantine of compromised devices, and more

Highlights include:

**IoT Security**—Use AI and machine-learning (ML) algorithms to dynamically discover and maintain a real-time inventory of your IoT devices, assess risk, detect behavioral anomalies and security threats, and make policy recommendations for firewall enforcement.

**Inline ML for URL Filtering and WildFire**—Use your firewall to proactively analyze:

- Web page content to determine if it contains malicious JavaScript or is being used for credential phishing. Prevent web-based threats from infiltrating your network by providing inline analysis capabilities on the firewall, reducing the possibility of successful attacks using previously unknown malicious JavaScript and various phishing vectors.
- Windows executables and PowerShell scripts on the dataplane. Intercept malware before it can infiltrate your network by providing real-time analysis capabilities on the firewall, reducing the possibility of proliferation of unknown malware variants.

**Telemetry**—Enable telemetry on your next-generation firewalls to collect data on device health and performance, product usage categories, and threat prevention. This data drives ML to help you understand your firewall deployment's health, optimize Security policy rules and eliminate breaches from product misconfigurations.

**GlobalProtect Identification and Quarantine of Compromised Devices**—Control access of compromised devices on your network by tracking devices.

Do not show again

Close

General Information

Time

12/03 16:08:34

12/03 16:08:32

12/03 16:08:22

PA-VM - Mozilla Firefox

PA-VM

https://192.168.1.254/?#dashboard::vsys1

PA-VM | DASHBOARD | ACC | MONITOR | POLICIES | OBJECTS | NETWORK | DEVICE

Layout: 3 Columns | Widgets | Last updated: 18:18:00 | 5 mins

**General Information**

Device Name: PA-VM

MGT IP Address: 192.168.1.254

MGT Netmask: 255.255.255.0

MGT Default Gateway:

MGT IPv6 Address: unknown

MGT IPv6 Link Local Address: fe80::5200:ff:fe01:0/64

MGT IPv6 Default Gateway:

MGT MAC Address: 50:00:00:01:00:00

Model: PA-VM

Serial #: unknown

CPU ID: KVM:63060000DFB8807

UUID: 5D180F7D-662D-49CF-96D4-8D419BD8EBB6

VM License: none

VM Mode: KVM

Software Version: 10.0.2

GlobalProtect Agent: 0.0.0

Application Version: 8334-6362

Threat Version: 8334-6362

Antivirus Version: 3510-4021

Device Dictionary Version: 7-231

**Data Logs**

No data available.

**System Logs**

Description	Time
User admin logged in via Web from 192.168.1.1 using https	12/03 16:17:41
authenticated for user 'admin'. From: 192.168.1.1.	12/03 16:17:41
User admin logged in via Web from 192.168.1.1 using https	12/03 16:13:01
authenticated for user 'admin'. From: 192.168.1.1.	12/03 16:13:01
Commit job succeeded. Completion time=2020/12/03 16:09:14. Jobid=2. User:admin	12/03 16:09:14
Port MGT: Up 1Gb/s Full duplex	12/03 16:09:02
Port MGT: Down 1Gb/s Full duplex	12/03 16:09:00
Config installed	12/03 16:08:57
Dnsproxy object:mgmt-obj was enabled.	12/03 16:08:55
SSLMGR daemon configuration load phase-2 succeeded.	12/03 16:08:54

**Config Logs**

Command	Path	Admin	Time
commit		admin	12/03 16:08:34
set	deviceconfig system type	admin	12/03 16:08:32
set	deviceconfig system	admin	12/03 16:08:22

**Locks**

No locks found

**ACC Risk Factor (Last 60 minutes)**

0.0

admin | Logout | Last Login Time: 12/03/2020 16:13:01 | Session Expire Time: 01/02/2020 16:17:41