

LIS4774 Information Security

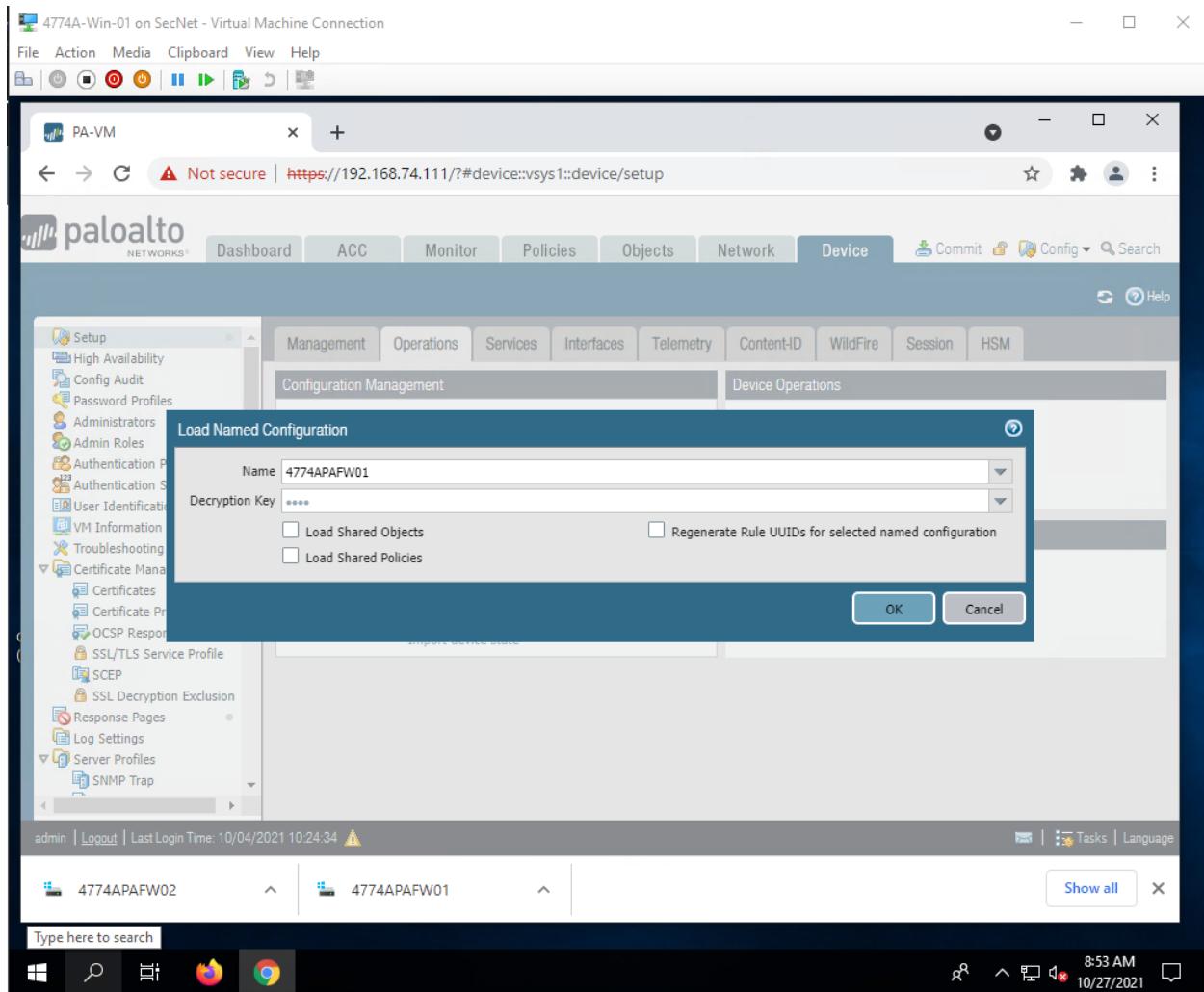
Dr. Metcalfe

October 28, 2021

Group A: Mehmet Can Ozmen, Joshua France, Aiden Talavera, Adam MacDougall, Jordan Northup, Joshua Flashman

Lab 8 - PANFW-9.1.9 Firewall 1

Loaded pre-configured firewall configuration into firewall



Added policy administrator role Monitor, Network, and Device manually disabled.

The screenshot shows the Palo Alto Networks Web UI interface. The main window title is "Admin Role Profile" for "policy-admins-role". The "Name" field is set to "policy-admins-role" and the "Description" field is "Policy Administrators". The "Web UI" tab is selected, showing a list of permissions:

- Report (disabled)
- Log (disabled)
- Configuration (disabled)
- Operational Requests (disabled)
- Commit (disabled)
- User-ID Agent (disabled)
- Export (disabled)
- Import (disabled)

A legend at the bottom indicates: Enable, Read Only, Disable. The "OK" and "Cancel" buttons are at the bottom right of the dialog. On the left, the navigation menu includes "Setup", "High Availability", "Config Audit", "Password Profiles", "Administrators", "Admin Roles" (selected), "Authentication Profiles", "Authentication Sequences", "User Identification", "VM Information Source", "Troubleshooting", "Certificate Management" (expanded), "Certificates", "Certificate Profile", "OCSP Responder", "SSL/TLS Service", "SCEP", "SSL Decryption Engine", "Response Pages", "Log Settings", "Server Profiles", and "SNMP Trap". The top status bar shows "4774A-Win-01 on SecNet - Virtual Machine Connection" and the URL "https://192.168.74.111/#device::vsys1::device/admin-roles". The bottom status bar shows "admin | Logout | Last Login Time: 10/04/2021 10:24:34".

Policy Administrator Role added to Admin Roles

The screenshot shows the Palo Alto Networks Device Admin Roles page. The left sidebar navigation includes: Setup, High Availability, Config Audit, Password Profiles, Administrators, Admin Roles (selected), Authentication Profile, Authentication Sequence, User Identification, VM Information Sources, Troubleshooting, Certificate Management (Certificates, Certificate Profile, OCSP Responder, SSL/TLS Service Profile, SCEP, SSL Decryption Exclusion), Response Pages, Log Settings, Server Profiles (SNMP Trap). The main content area displays a table of admin roles:

Name	Description	Role	CLI Role
auditadmin	Audit Administrator for Common Criteria	device	
cryptoadmin	Crypto Administrator for Common Criteria	device	
securityadmin	Security Admin for Common Criteria	device	
policy-admins-role	Policy Administrators	device	

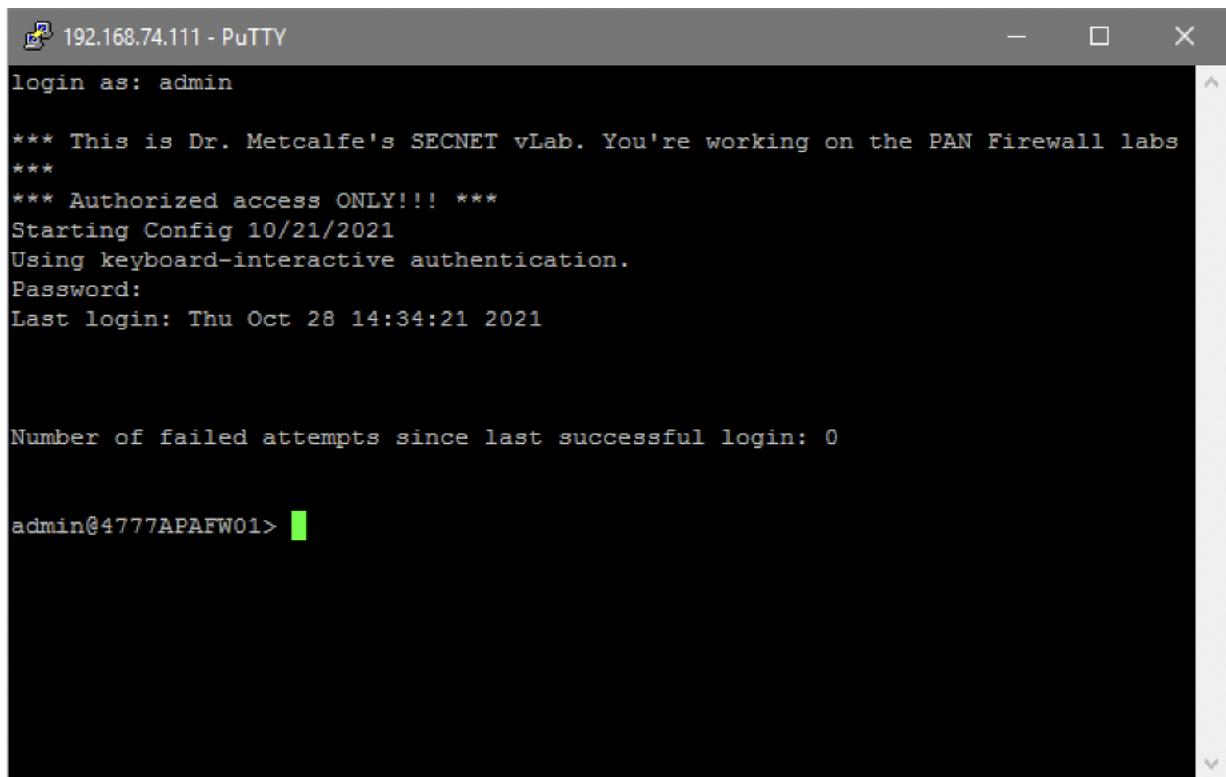
At the bottom of the page, there are buttons for Add, Delete, Clone, PDF/CSV, and a Show all link.

Custom Policy Administrator account created

The screenshot shows the Palo Alto Networks Device Manager interface. The title bar indicates the connection is to a virtual machine named "PA-VM". The top navigation bar includes File, Action, Media, Clipboard, View, Help, and tabs for PA-VM, Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. The Device tab is selected. The main content area displays a table of administrators. A search bar at the top right shows "2 items". The table columns are Name, Role, Authentication Profile, Password Profile, Client Certificate Authentication (Web), Public Key Authentication (SSH), Profile, and Locked User. Two rows are present: one for "admin" (Superuser) and one for "policy-admin" (Custom role-based administrator). The "policy-admin" row has a checked checkbox in the first column. The left sidebar contains a navigation tree with sections like Setup, Administrators, Admin Roles, and Certificate Management.

Name	Role	Authentication Profile	Password Profile	Client Certificate Authentication (Web)	Public Key Authentication (SSH)	Profile	Locked User
admin	Superuser			<input type="checkbox"/>	<input type="checkbox"/>		
policy-admin	Custom role-based administrator			<input type="checkbox"/>	<input type="checkbox"/>	policy-admins-role	

Figure 2.4: Signing into PAFW01 using PuTTY



The screenshot shows a PuTTY terminal window titled "192.168.74.111 - PuTTY". The session is logged in as "admin". The terminal displays a welcome message from Dr. Metcalfe's SECNET vLab, stating that you're working on the PAN Firewall labs and that authorized access is ONLY!!!. It also shows the starting configuration date as 10/21/2021, the authentication method as keyboard-interactive, and the last login details. It then displays the number of failed attempts since the last successful login (0) and ends with the prompt "admin@4777APAFW01>".

```
192.168.74.111 - PuTTY
login as: admin

*** This is Dr. Metcalfe's SECNET vLab. You're working on the PAN Firewall labs
*** Authorized access ONLY!!!
Starting Config 10/21/2021
Using keyboard-interactive authentication.
Password:
Last login: Thu Oct 28 14:34:21 2021

Number of failed attempts since last successful login: 0

admin@4777APAFW01>
```

Figure 2.5: Taking Lock and not allowing commits

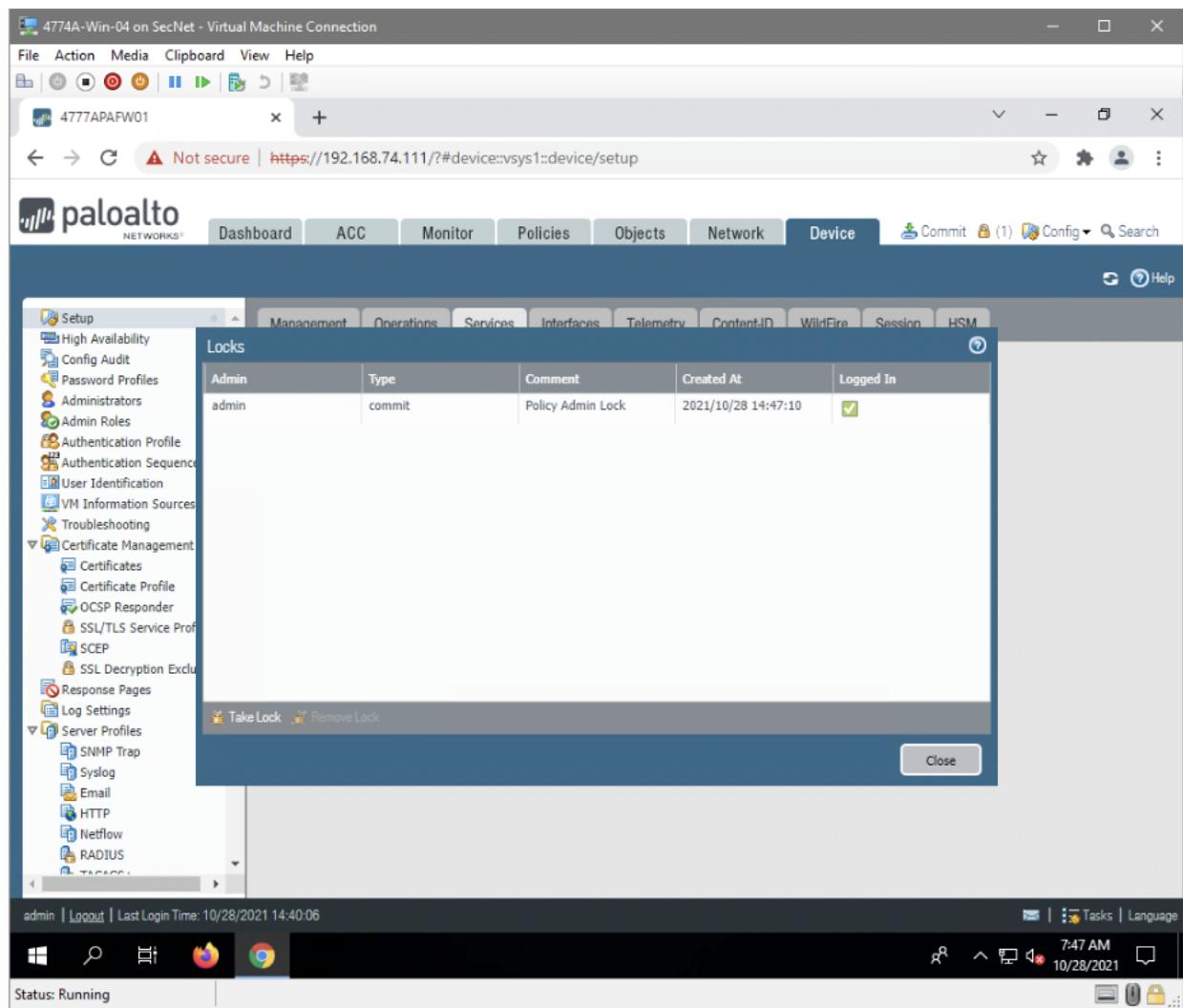


Figure 2.6: Verify the Update Server and DNS Server

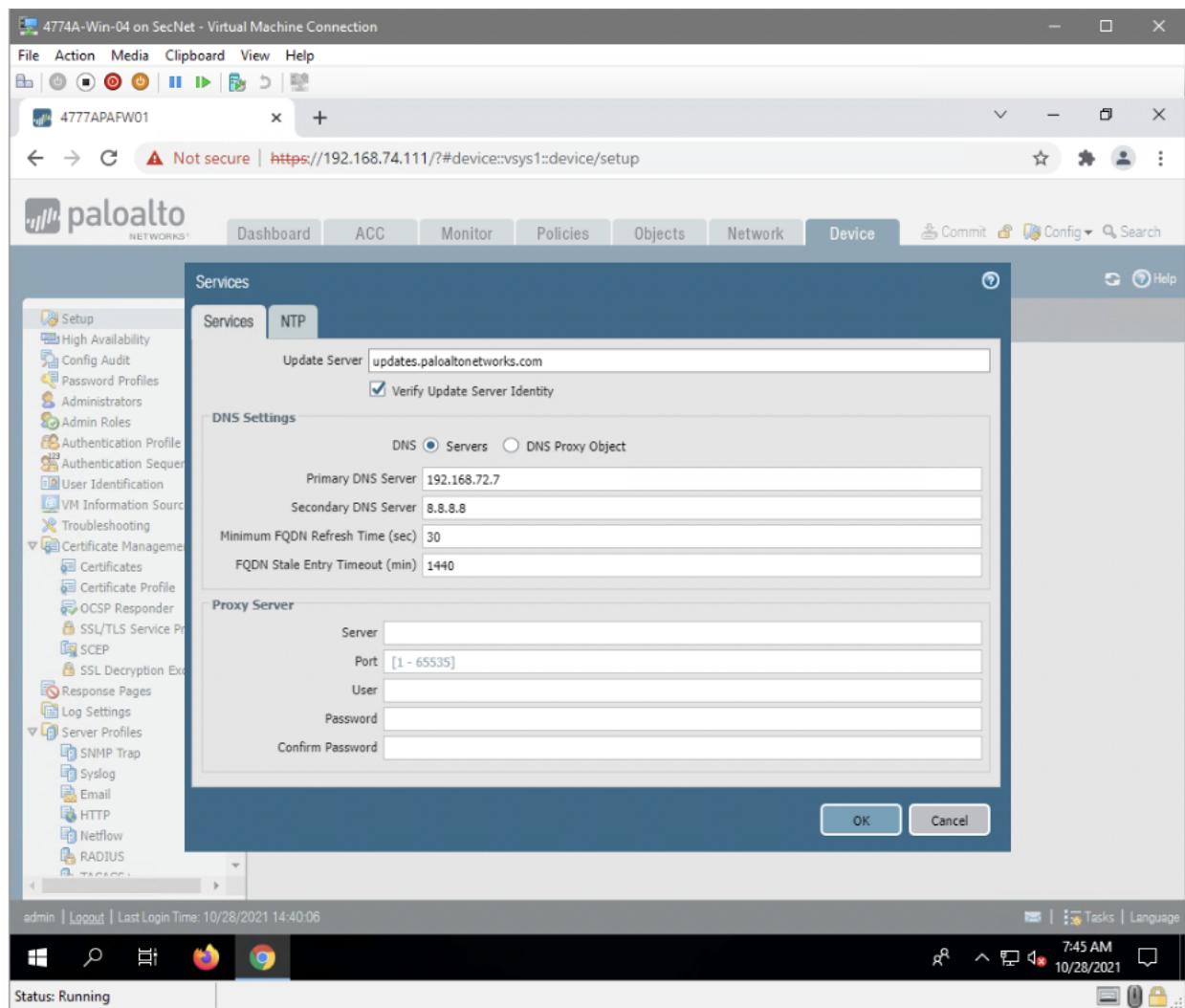


Figure 2.7: Configuring and scheduling dynamic updates

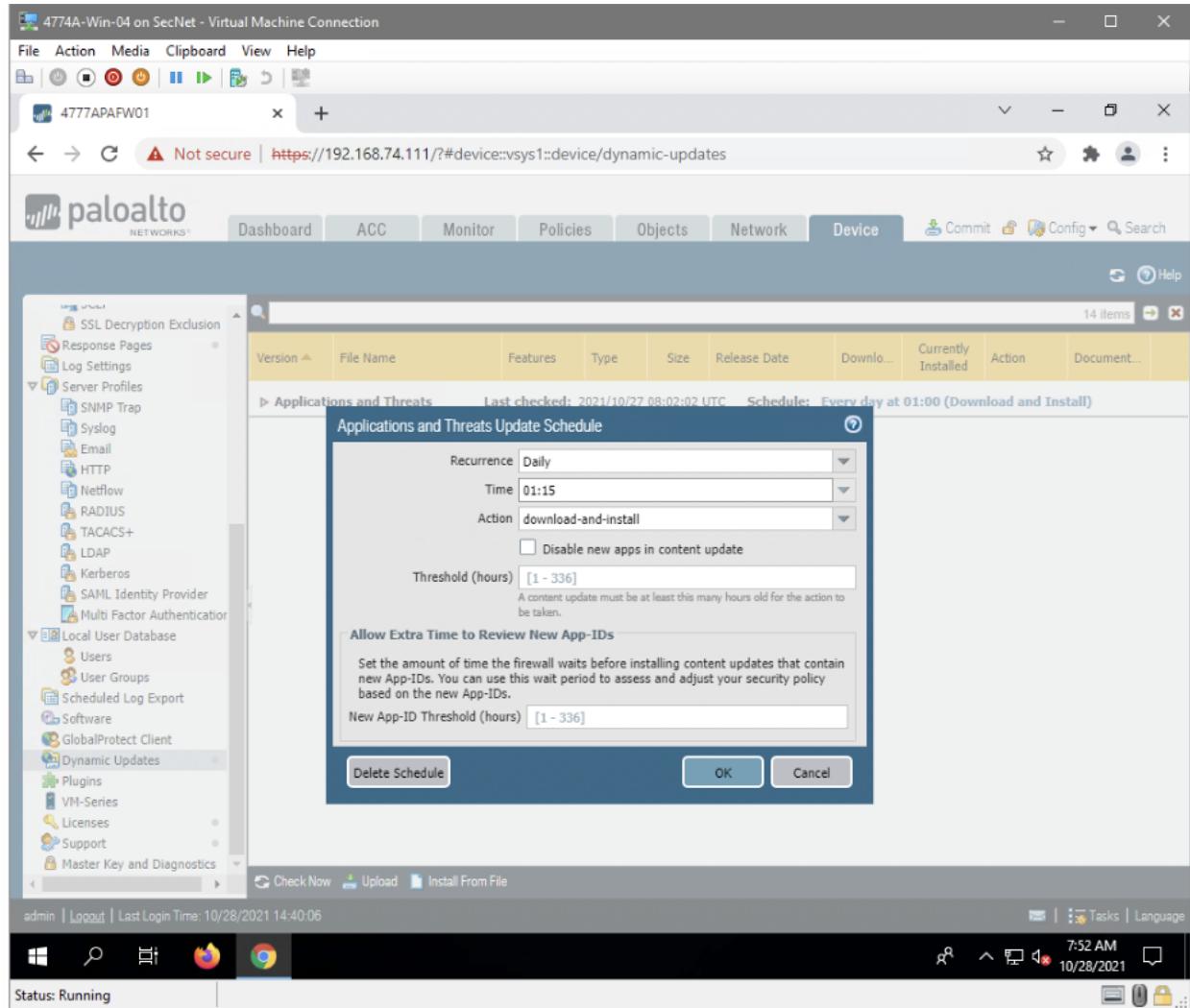


Figure 5: Pushing / Committing all changes so they save

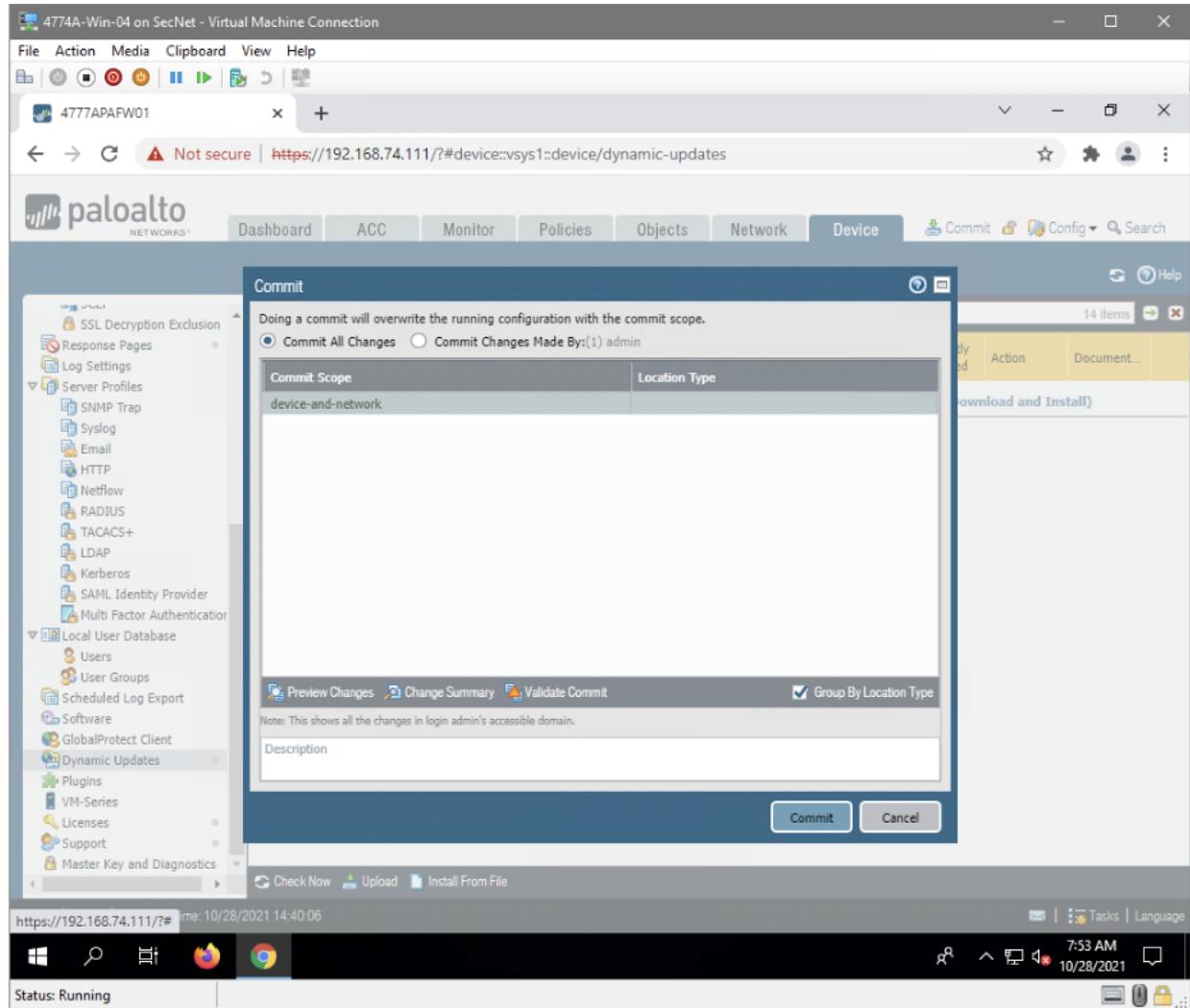


Figure 3: Loading Lab Configuration

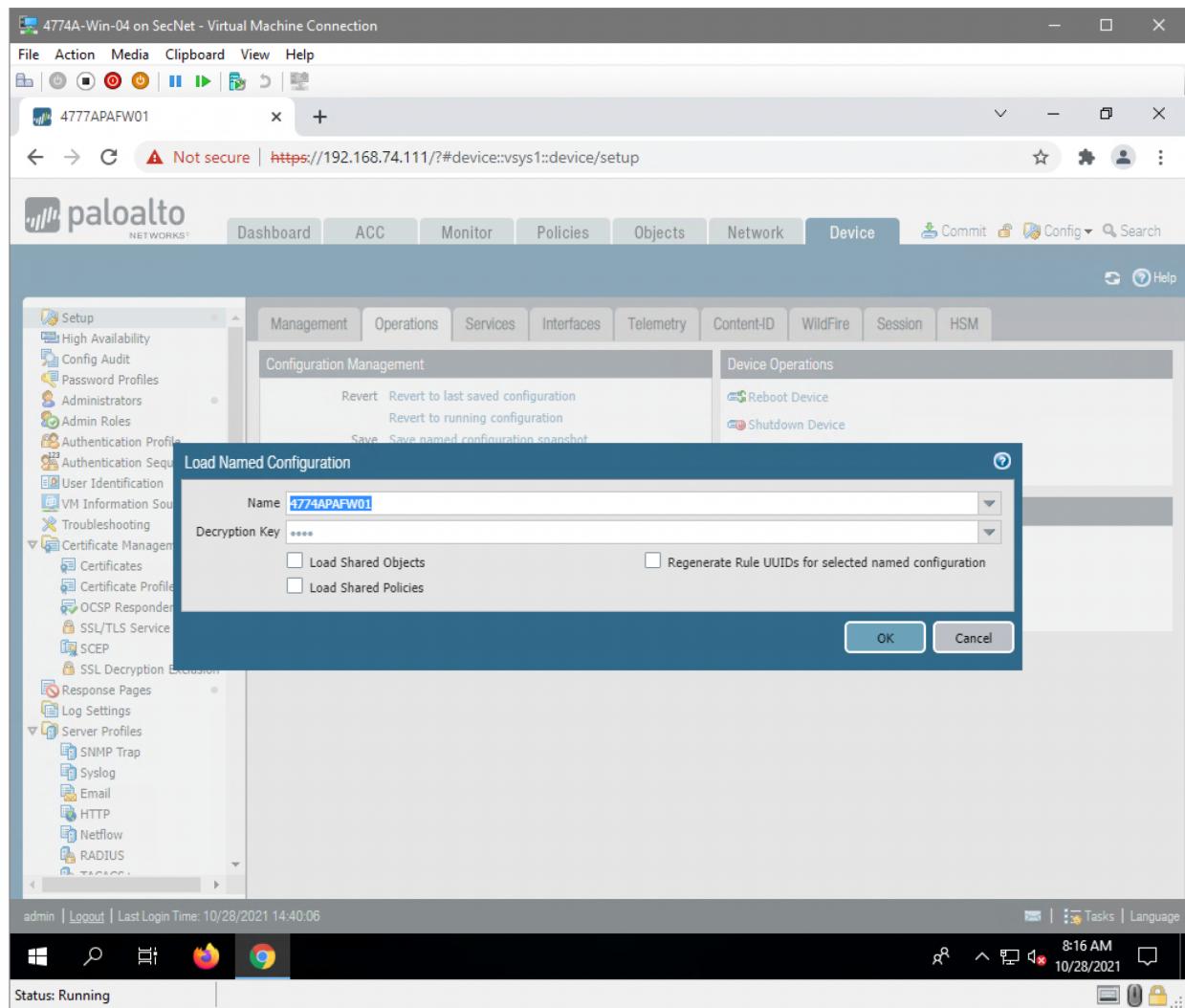


Figure 3.1: Adding new security zone with Layer3 fw

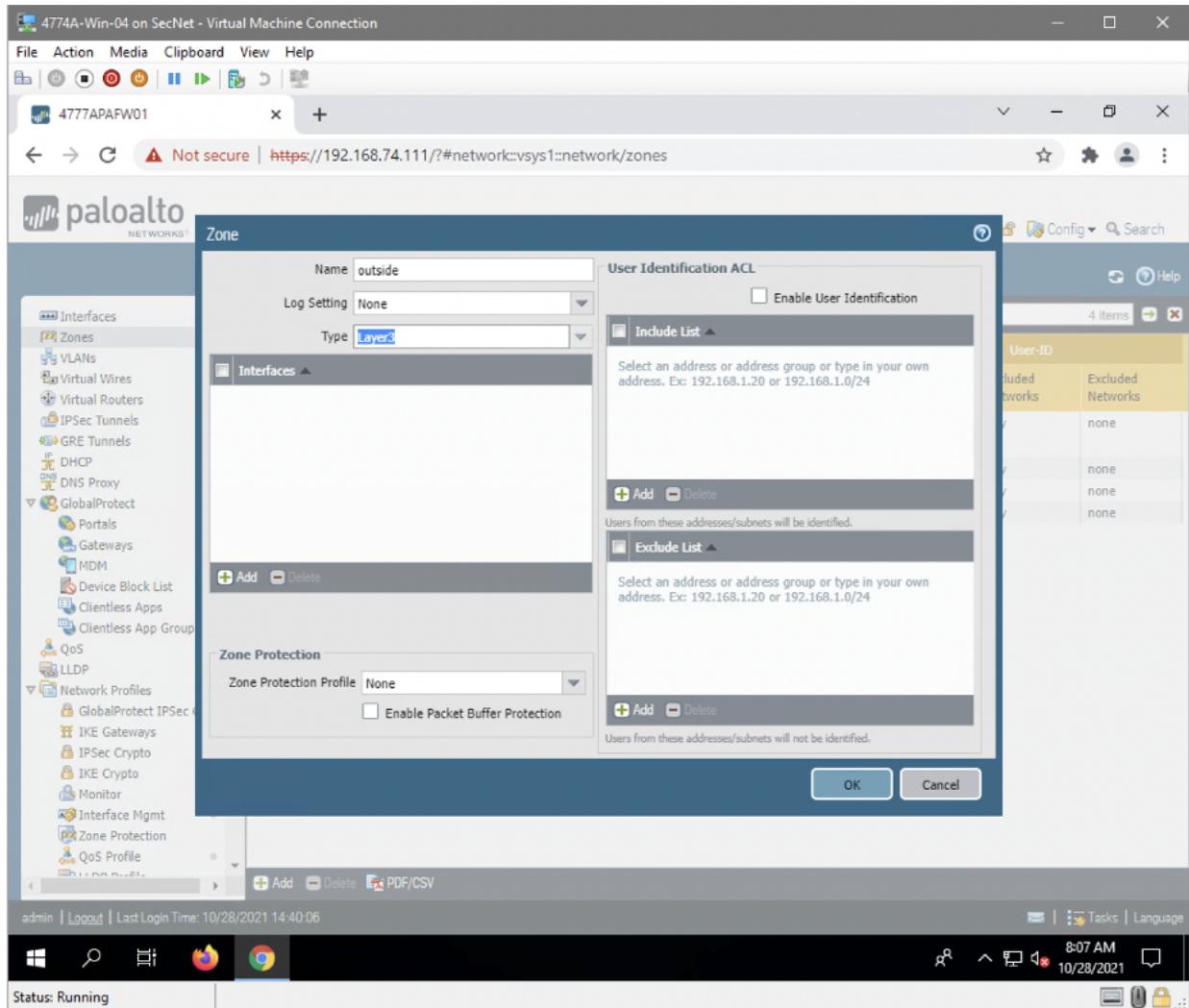


Figure 3.2: Creating Interface Management Profiles

The screenshot shows the Palo Alto Networks interface management profile creation screen. The left sidebar navigation menu includes: Interfaces, Zones, VLANs, Virtual Wires, Virtual Routers, IPsec Tunnels, GRE Tunnels, DHCP, DNS Proxy, GlobalProtect (Portals, Gateways, MDM, Device Block List, Clientless Apps, Clientless App Groups), QoS, LLDP, and Network Profiles (GlobalProtect IPSec Cr, IKE Gateways, IPSec Crypto, IKE Crypto, Monitor, Interface Mgmt, Zone Protection, QoS Profile). The 'Interface Mgmt' item is currently selected. The main content area displays a table titled 'Interface Management Profiles' with two items listed:

Name	Ping	Telnet	SSH	HTTP	HTTP OCSP	HTTPS	SNMP	Response Pages	User-ID	User-ID Syslog Listener-SSL	User-ID Syslog Listener-UDP	Permitted IP Addresses
ping-response-pages	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
ping	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							

Below the table are buttons for 'Add', 'Delete', 'Clone', and 'PDF/CSV'. The bottom status bar shows 'Status: Running' and the date/time '10/28/2021 14:40:06'.

Figure 3.3: Configuring Ethernet Interfaces and Adding New Security Zones

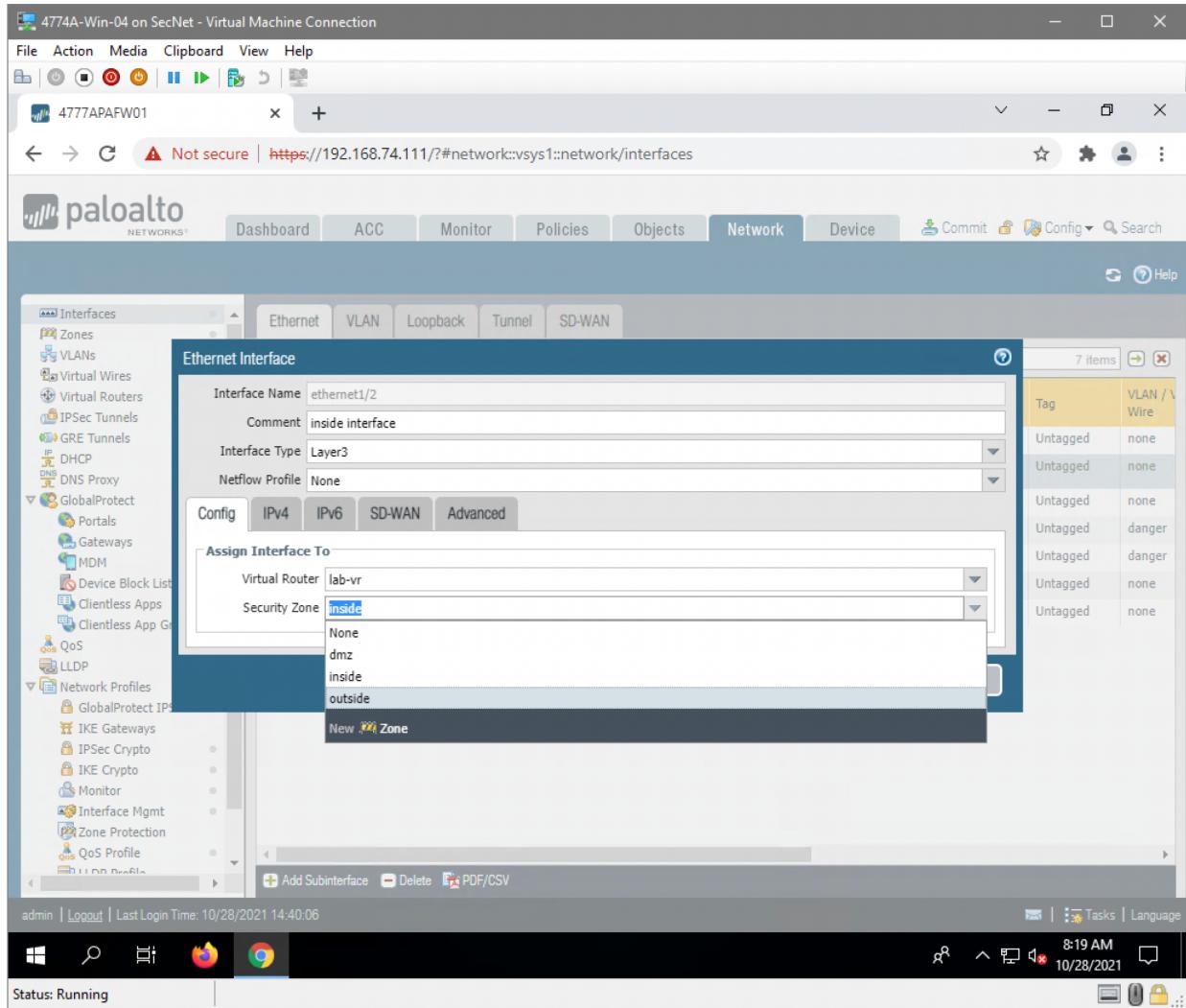


Figure 3.3.2: Configuring Ethernet Interfaces and setting up all of them to filter

The screenshot shows the Palo Alto Networks GlobalProtect interface. The left sidebar navigation menu includes: Interfaces, Zones, VLANs, Virtual Wires, Virtual Routers, IPSec Tunnels, GRE Tunnels, IP, DHCP, DNS Proxy, GlobalProtect (selected), Portals, Gateways, MDM, Device Block List, Clientless Apps, Clientless App Groups, QoS, LLDP, and Network Profiles. The main content area displays a table of Ethernet interfaces:

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Wire
ethernet1/1	Layer3		green	Dynamic-DHCP Client	lab-vr	Untagged	none
ethernet1/2	Layer3	ping-response-pages	green	10.20.111.254/24	lab-vr	Untagged	none
ethernet1/3	Layer3	ping	green	10.21.111.254/24	lab-vr	Untagged	none
ethernet1/4	Virtual Wire		red	none	none	Untagged	danger
ethernet1/5	Virtual Wire		red	none	none	Untagged	danger
ethernet1/6			red	none	none	Untagged	none
ethernet1/7			red	none	none	Untagged	none

At the bottom of the interface, there are buttons for 'Add Subinterface', 'Delete', and 'PDF/CSV'. The status bar at the bottom shows 'Status: Running' and the system clock '10/28/2021 14:40:06'.

Figure 3.4: Creating a virtual wire, binding ethernet 1/4 and 1/5 together.

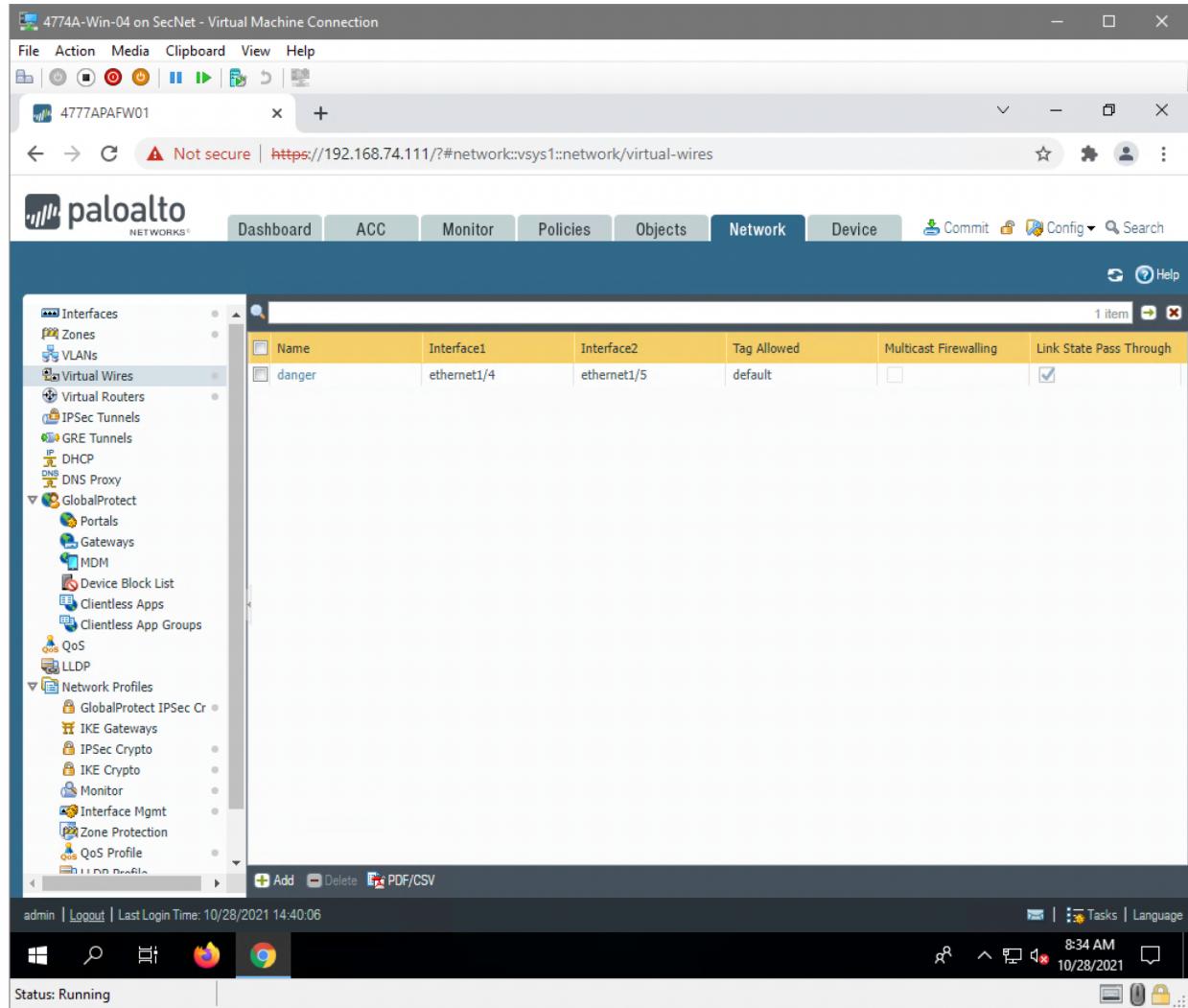


Figure 3.5: Creating virtual router and allowing all 3 interfaces to route traffic to each other.

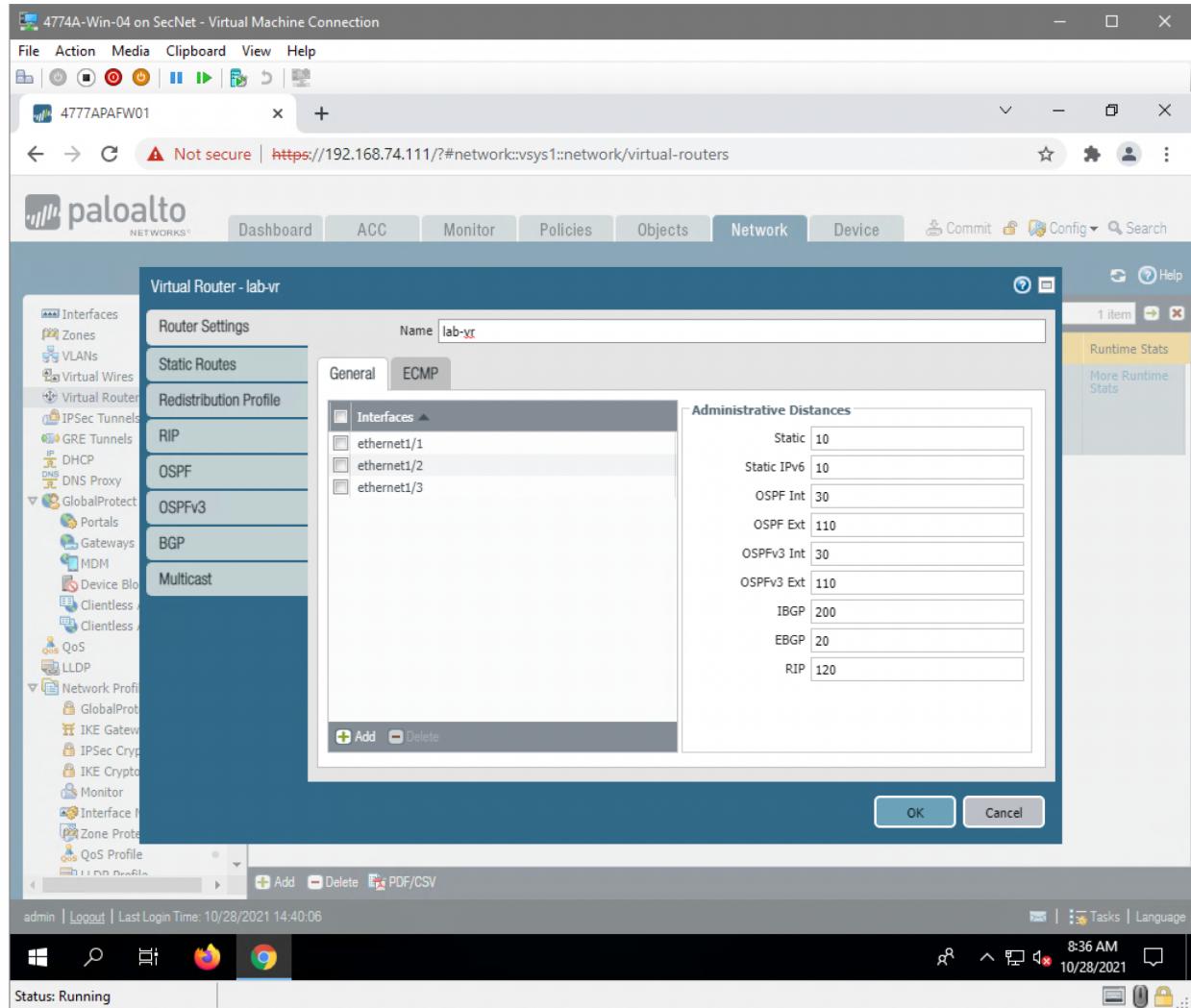


Figure 3-4: Setting static IP address on Interface 1

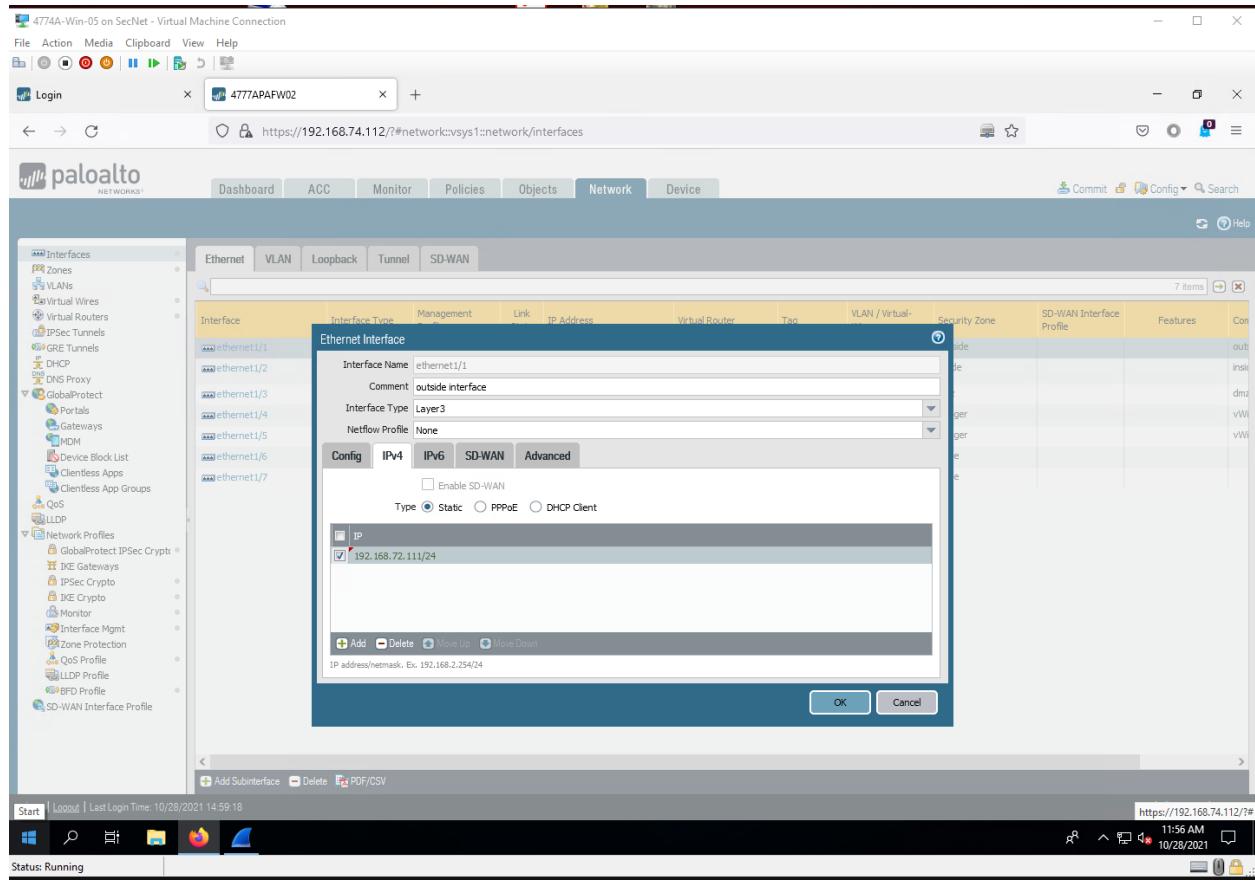
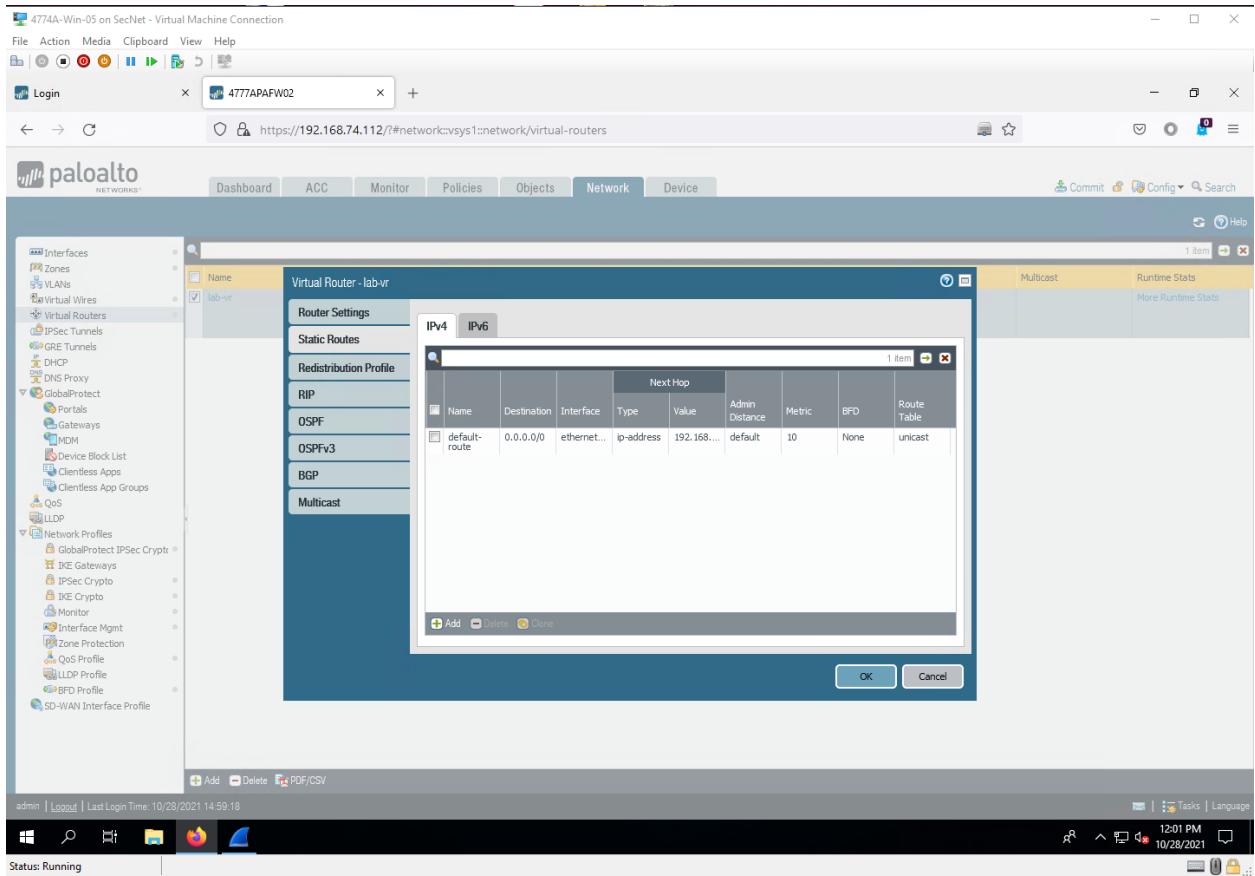
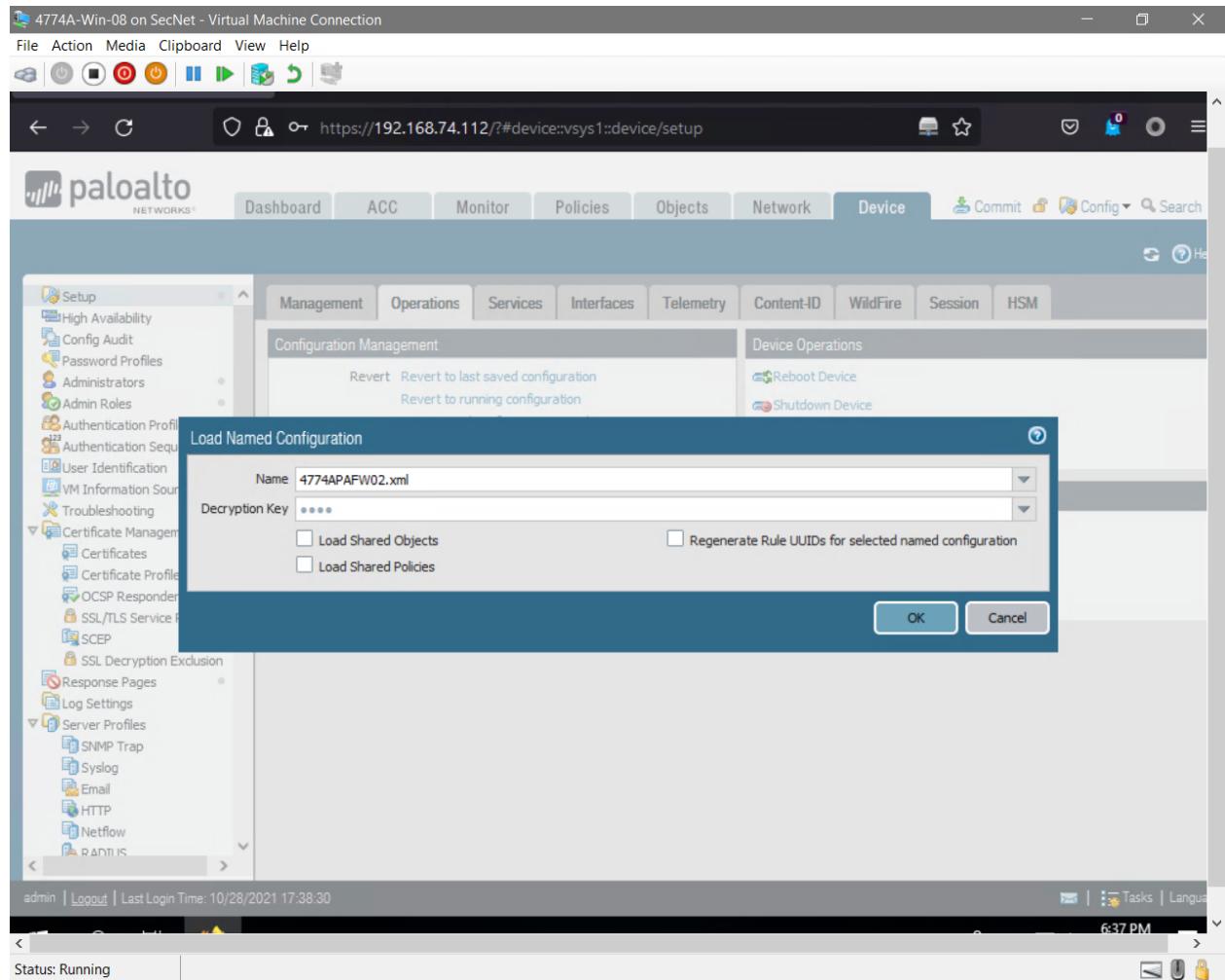


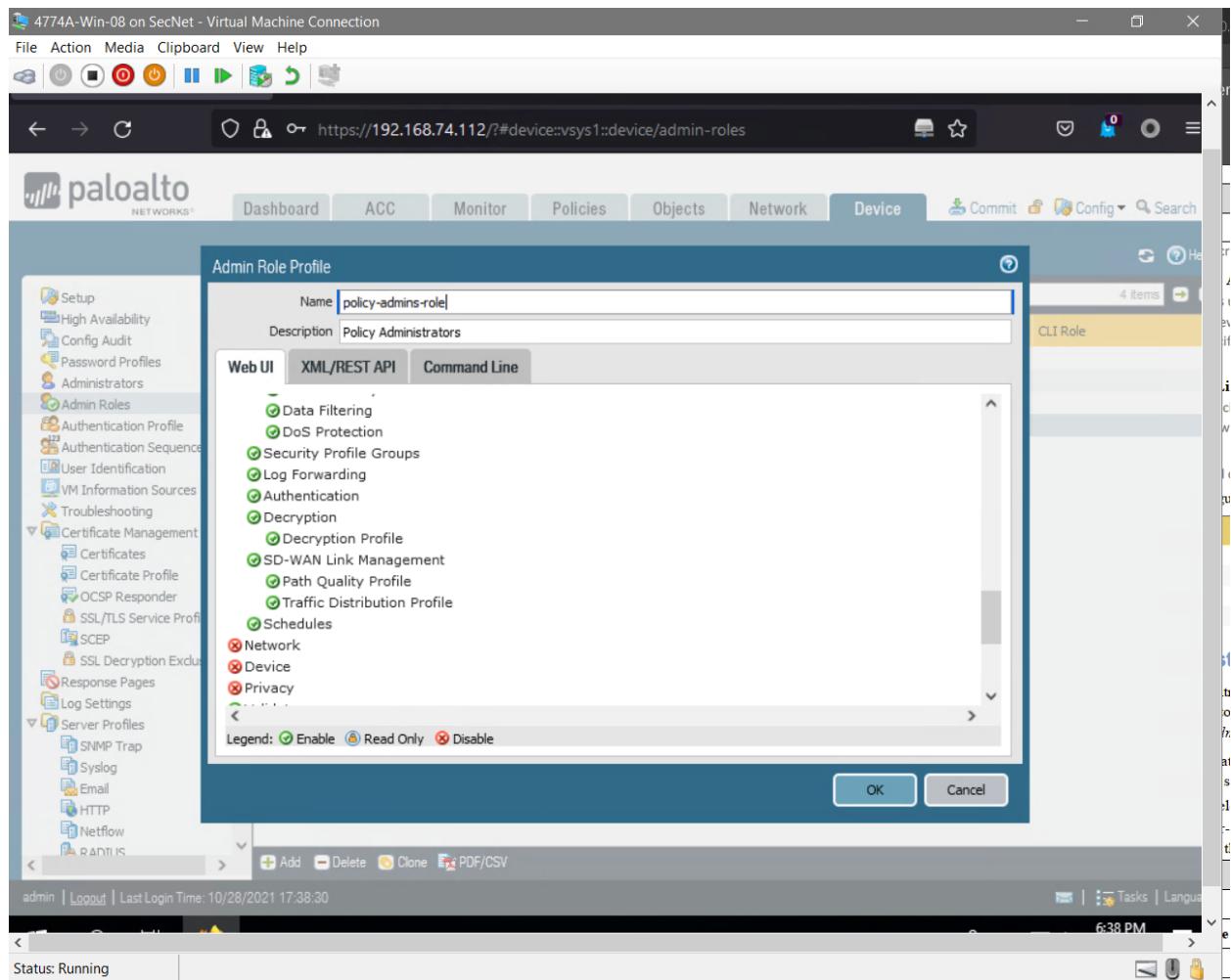
Figure 3-4: Adding static route to virtual router



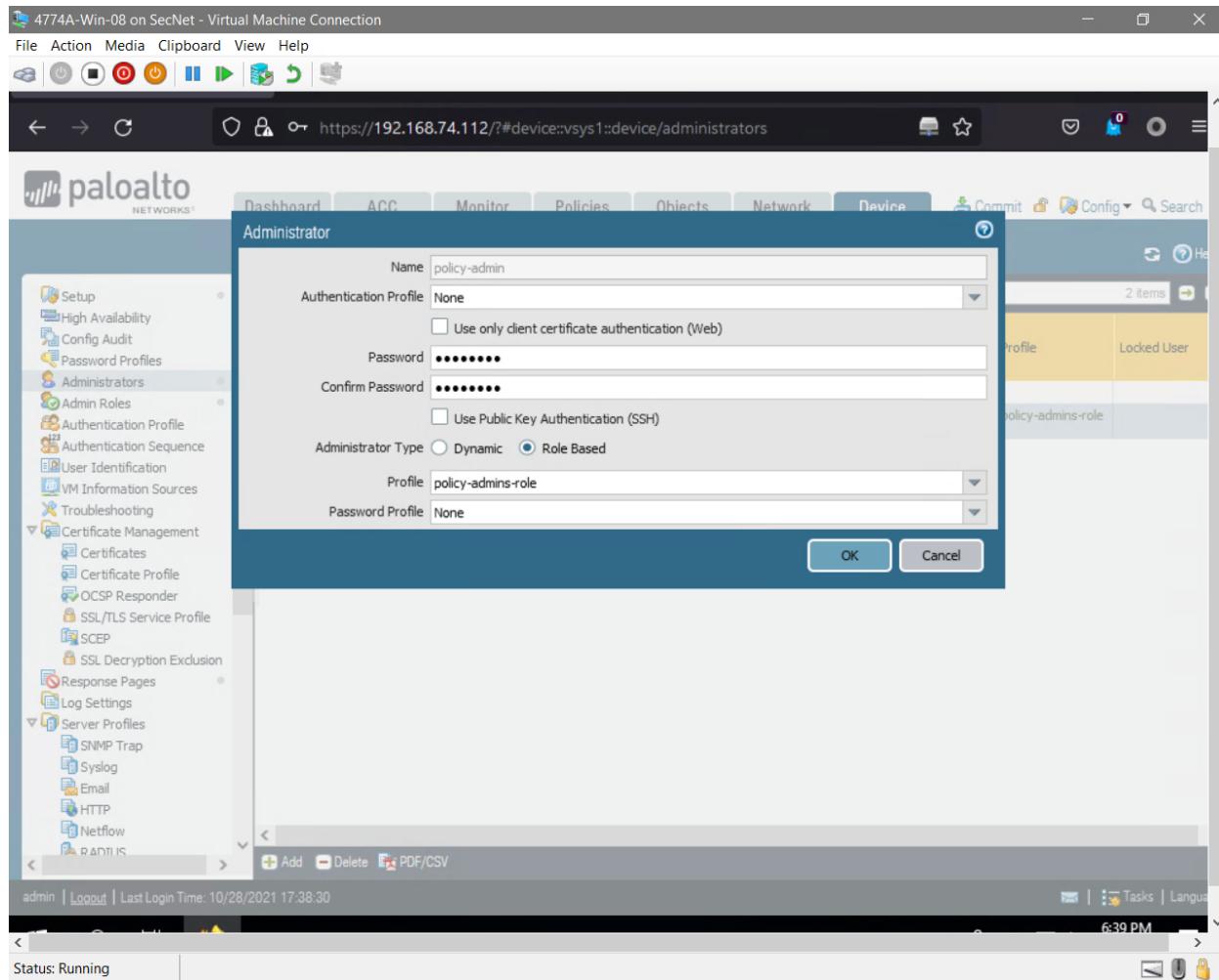
Firewall 2



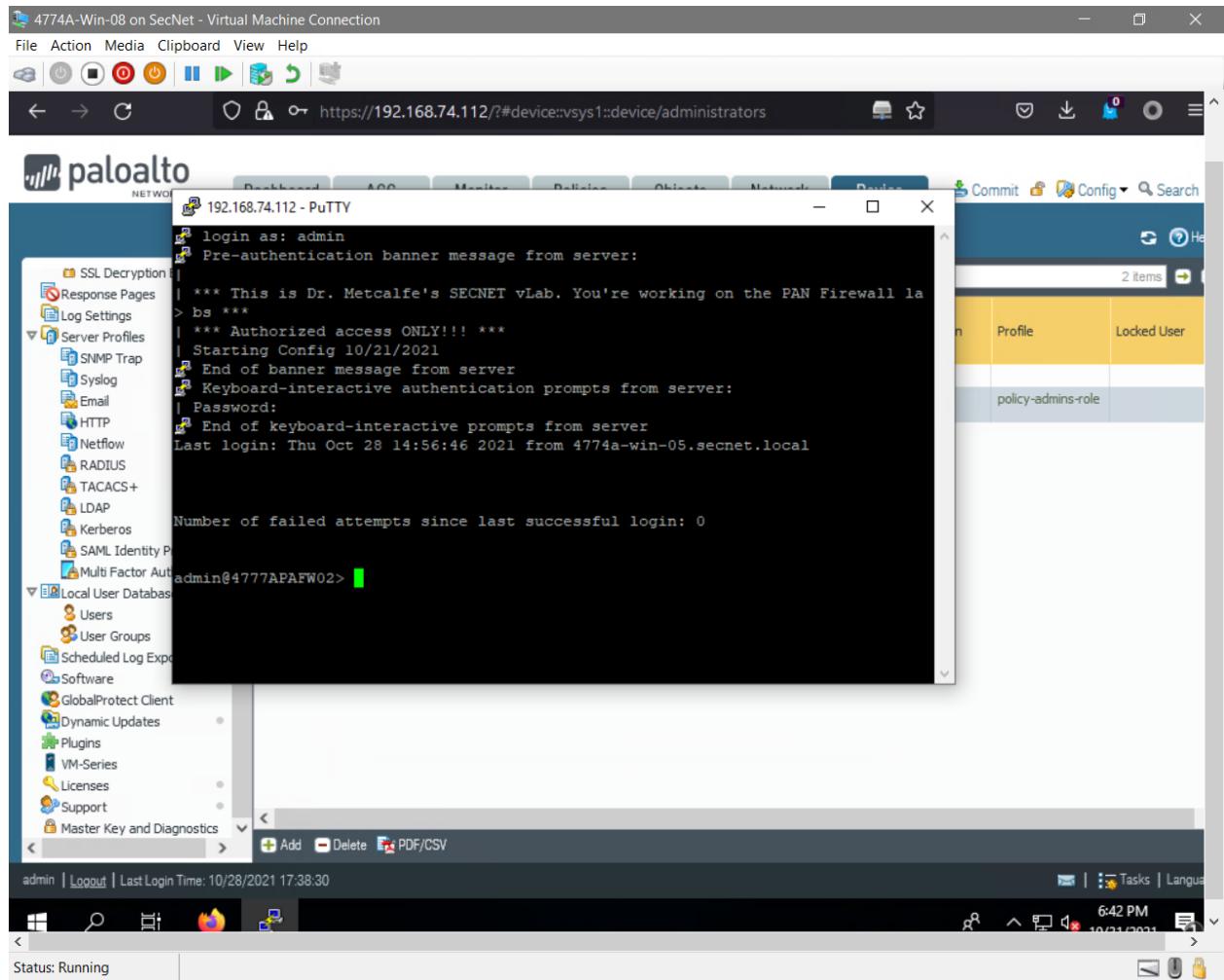
Loaded Firewall 2 configuration file



Added Policy-Admin role



Created Policy-Admin account



Successfully tested admin account. Putty closed automatically successfully when logging into policy-admin due to lack of CLI permission.

4774A-Win-08 on SecNet - Virtual Machine Connection

File Action Media Clipboard View Help

4777APAFW02 https://192.168.74.112/#dashboard::vsys1

paloalto NETWORKS®

Dashboard ACC Policies Objects Commit Config Search

Last updated: 18:52:24

Layout: 3 Columns Widgets 5 mins

General Information

Device Name	4777APAFW02
MGT IP Address	192.168.74.112
MGT Netmask	255.255.255.0
MGT Default Gateway	192.168.74.254
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80::70fa:ff:fe00:2/64
MGT IPv6 Default Gateway	
MGT MAC Address	72:fa:00:00:00:02
Model	PA-VM
Serial #	unknown
CPU ID	HPV:57060500FFFFB8B1F
UUID	D38BD179-AF5D-174E-92BA-56068FDD67BF
VM License	none
VM Mode	Microsoft Hyper-V
Software Version	9.1.9
GlobalProtect Agent	0.0.0
Application Version	8391-6609
URL Filtering Version	0000.00.00.000
GlobalProtect Clientless VPN Version	0
Time	Mon Nov 1 01:52:25 2021
Uptime	3 days, 11:12:16
Plugin VM Version	vsys version 7.0.6

Logged In Admins

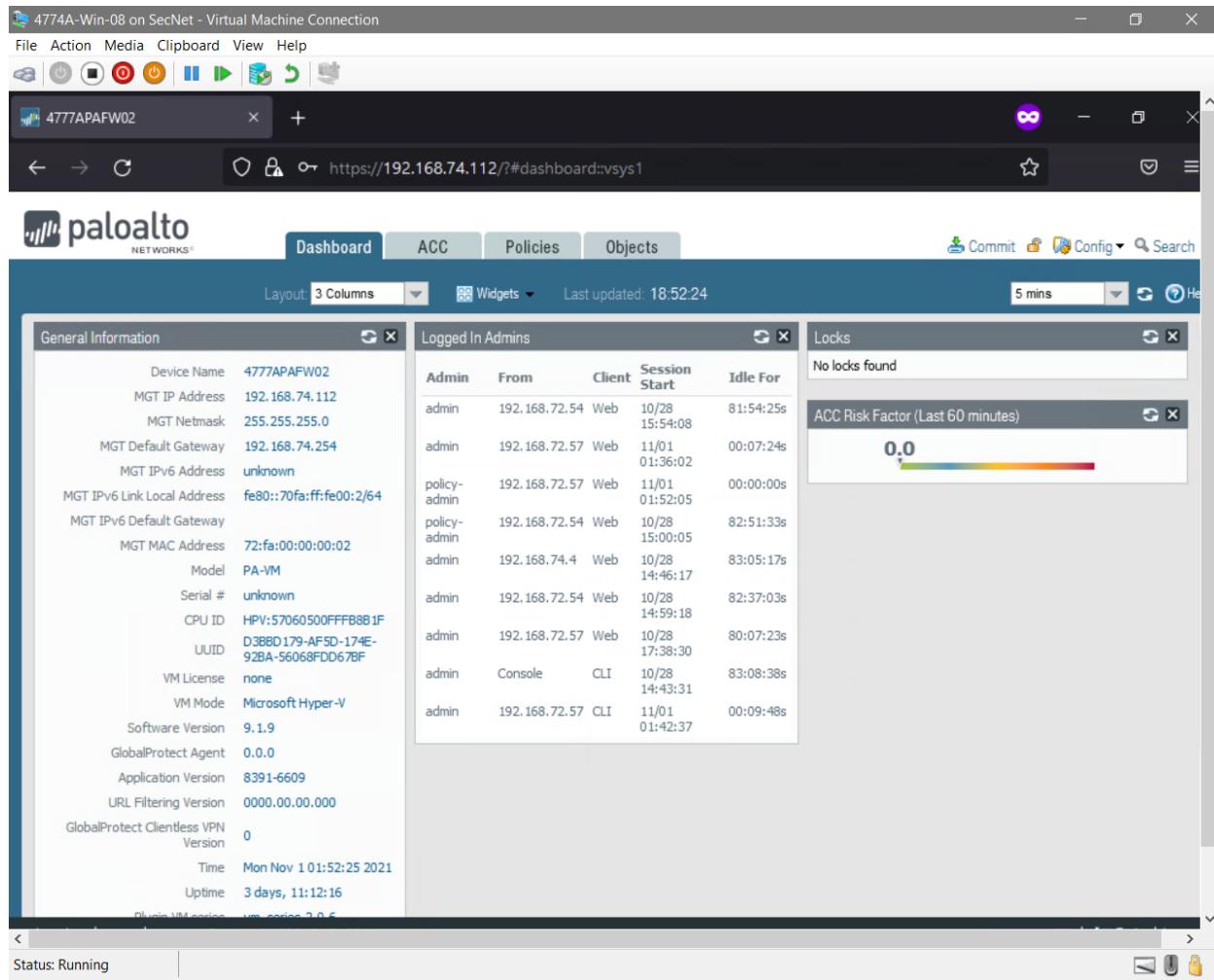
Admin	From	Client	Session Start	Idle For
admin	192.168.72.54	Web	10/28 15:54:08	81:54:25s
admin	192.168.72.57	Web	11/01 01:36:02	00:07:24s
policy-admin	192.168.72.57	Web	11/01 01:52:05	00:00:00s
policy-admin	192.168.72.54	Web	10/28 15:00:05	82:51:33s
admin	192.168.74.4	Web	10/28 14:46:17	83:05:17s
admin	192.168.72.54	Web	10/28 14:59:18	82:37:03s
admin	192.168.72.57	Web	10/28 17:38:30	80:07:23s
admin	Console	CLI	10/28 14:43:31	83:08:38s
admin	192.168.72.57	CLI	11/01 01:42:37	00:09:48s

Locks

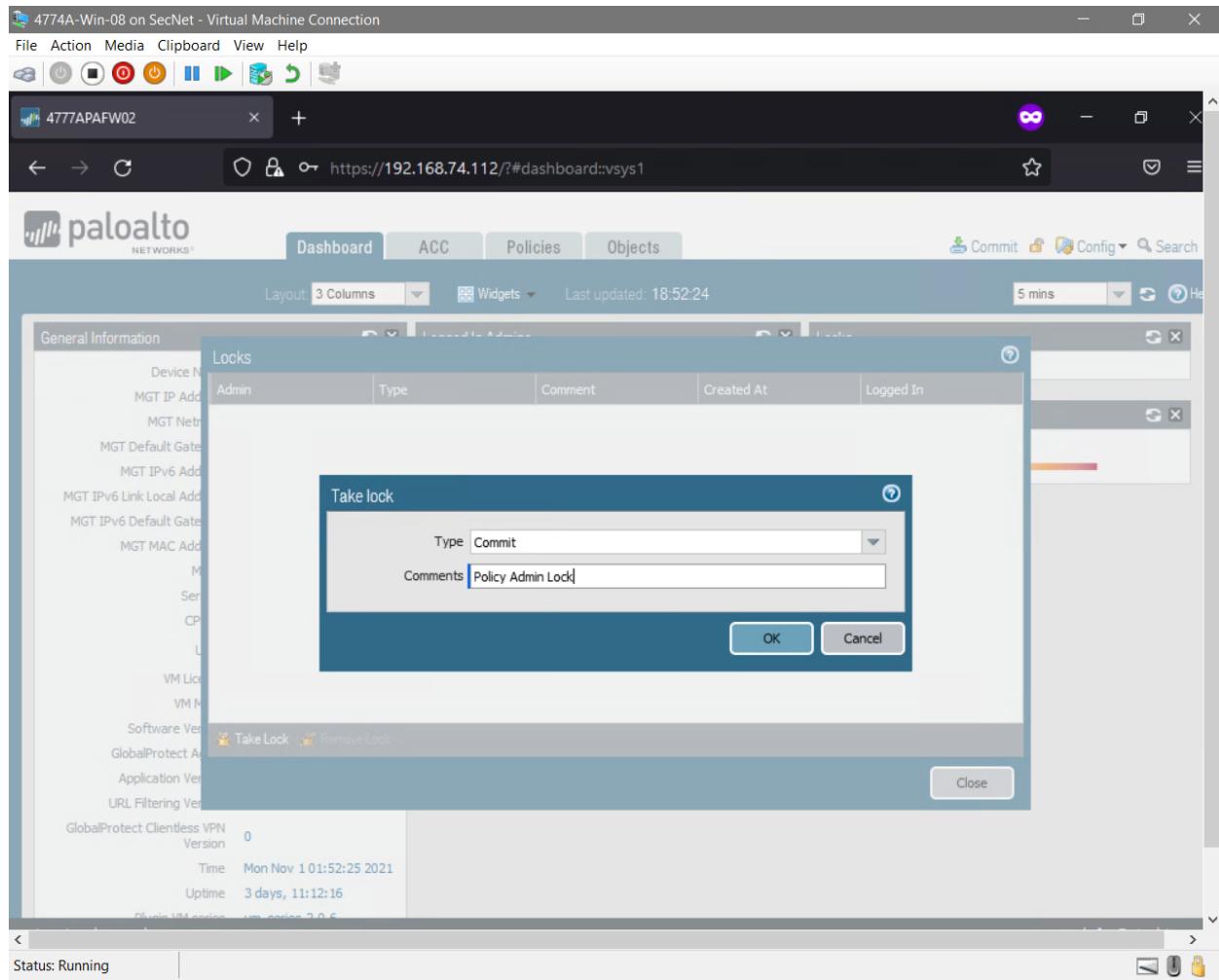
No locks found

ACC Risk Factor (Last 60 minutes)

0.0



Successfully logged into policy-admin account on web interface



Added a policy-admin lock

4774A-Win-08 on SecNet - Virtual Machine Connection

File Action Media Clipboard View Help

4777APAFW02 https://192.168.74.112/#dashboard::vsys1

paloalto NETWORKS Dashboard ACC Monitor Policies Objects Network Device Commit Config Search

Last updated: 18:54:39 5 mins

General Information

Device Name	4777APAFW02
MGT IP Address	192.168.74.112
MGT Netmask	255.255.255.0
MGT Default Gateway	192.168.74.254
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80::70fa:ff:fe00:2/64
MGT IPv6 Default Gateway	
MGT MAC Address	72:fa:00:00:00:02
Model	PA-VM
Serial #	unknown
CPU ID	HPPV:57060500FFFFB8B1F
UUID	D38BD179-AF5D-174E-92BA-56068FDD67BF
VM License	none
VM Mode	Microsoft Hyper-V
Software Version	9.1.9
GlobalProtect Agent	0.0.0
Application Version	8391-6609
URL Filtering Version	00000.00.00.00
GlobalProtect Clientless VPN Version	0
Time	Mon Nov 1 01:54:39 2021
Uptime	3 days, 11:14:30
Paloalto VM Version	vsys version 7.0.6

Logged In Admins

Admin	From	Client	Session Start	Idle For
admin	192.168.72.54	Web	10/28 15:54:08	81:56:39s
admin	192.168.72.57	Web	11/01 01:36:02	00:00:00s
policy-admin	192.168.72.54	Web	10/28 15:00:05	82:53:47s
admin	192.168.74.4	Web	10/28 14:46:17	83:07:31s
admin	192.168.72.54	Web	10/28 14:59:18	82:39:17s
admin	192.168.72.57	Web	10/28 17:38:30	80:09:37s
admin	Console	CLI	10/28 14:43:31	83:10:52s
admin	192.168.72.57	CLI	11/01 01:42:37	00:12:02s

Config Logs

Command	Path	Admin	Time
edit	config mgt-config users policy-admin	admin	11/01 01:45:00

Locks

Admin	Type	Created	Logged In
policy-admin	commit	2021/11/01 01:53:41	yes

ACC Risk Factor (Last 60 minutes)

0.0

Data Logs

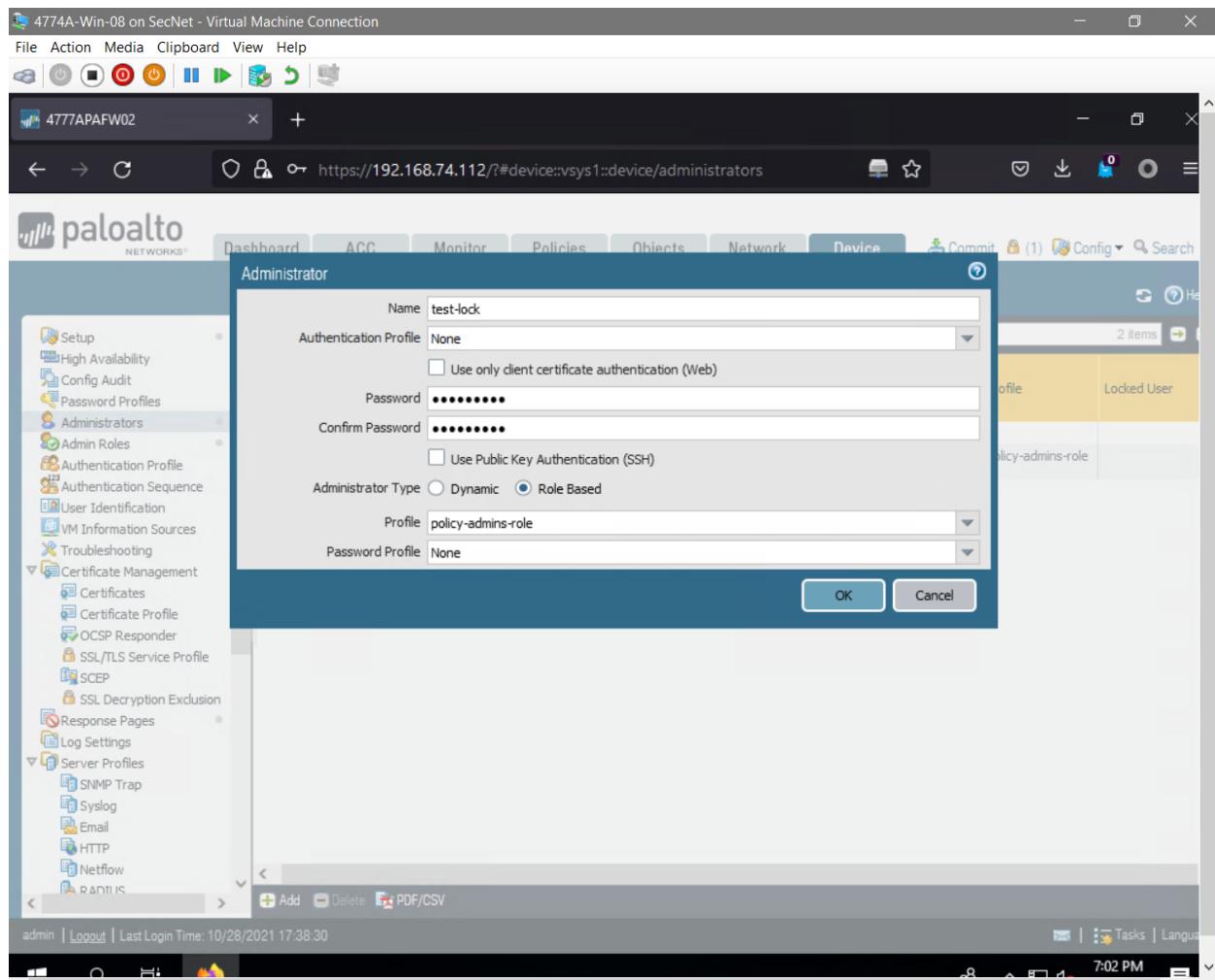
No data available.

System Logs

Description	Time
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.74.112	11/01 01:54:26

Status: Running

Policy admin lock was successful when viewed from main admin account



Added test-lock administrator account

4774A-Win-08 on SecNet - Virtual Machine Connection

File Action Media Clipboard View Help

4777APAFW02 https://192.168.74.112/#device::vsys1::device/administrators

paloalto NETWORKS Dashboard ACC Monitor Policies Objects Network Device Commit Config Search

Administrators

Name	Role	Authentication Profile	Password Profile	Client Certificate Authentication (Web)	Public Key Authentication (SSH)	Profile	Locked User
admin	Superuser			<input type="checkbox"/>	<input type="checkbox"/>		
policy-admin	Custom role-based administrator			<input type="checkbox"/>	<input type="checkbox"/>	policy-admins-role	
test-lock	Custom role-based administrator			<input type="checkbox"/>	<input type="checkbox"/>	policy-admins-role	

Error
Other administrators are holding device wide commit locks.

Close

admin | Logout | Last Login Time: 10/28/2021 17:38:30

Tasks | Language

7:03 PM

The screenshot shows the Palo Alto Networks Device Admin interface. On the left is a navigation tree with various configuration sections like Setup, High Availability, and Certificate Management. The main pane displays a table of administrators with columns for Name, Role, Authentication Profile, Password Profile, Client Certificate Authentication (Web), Public Key Authentication (SSH), Profile, and Locked User. Three rows are visible: 'admin' (Superuser), 'policy-admin' (Custom role-based administrator), and 'test-lock' (Custom role-based administrator). A modal dialog box titled 'Error' is centered over the table, stating 'Other administrators are holding device wide commit locks.' with a 'Close' button. At the bottom of the screen, there's a footer bar with links for admin/logout/last login time, tasks/language, and the current time (7:03 PM).

Unable to commit changes due to commit lock

4774A-Win-08 on SecNet - Virtual Machine Connection

File Action Media Clipboard View Help

4777APAFW02 https://192.168.74.112/#device::vsys1::device/administrators

paloalto NETWORKS Dashboard ACC Monitor Policies Objects Network Device Commit (1) Config Search

Locks

Admin	Type	Comment	Created At	Logged In
policy-admin	commit	Policy Admin Lock	2021/11/01 01:53:41	<input checked="" type="checkbox"/>

Remove lock

Are you sure you want to release commit lock for policy-admin?

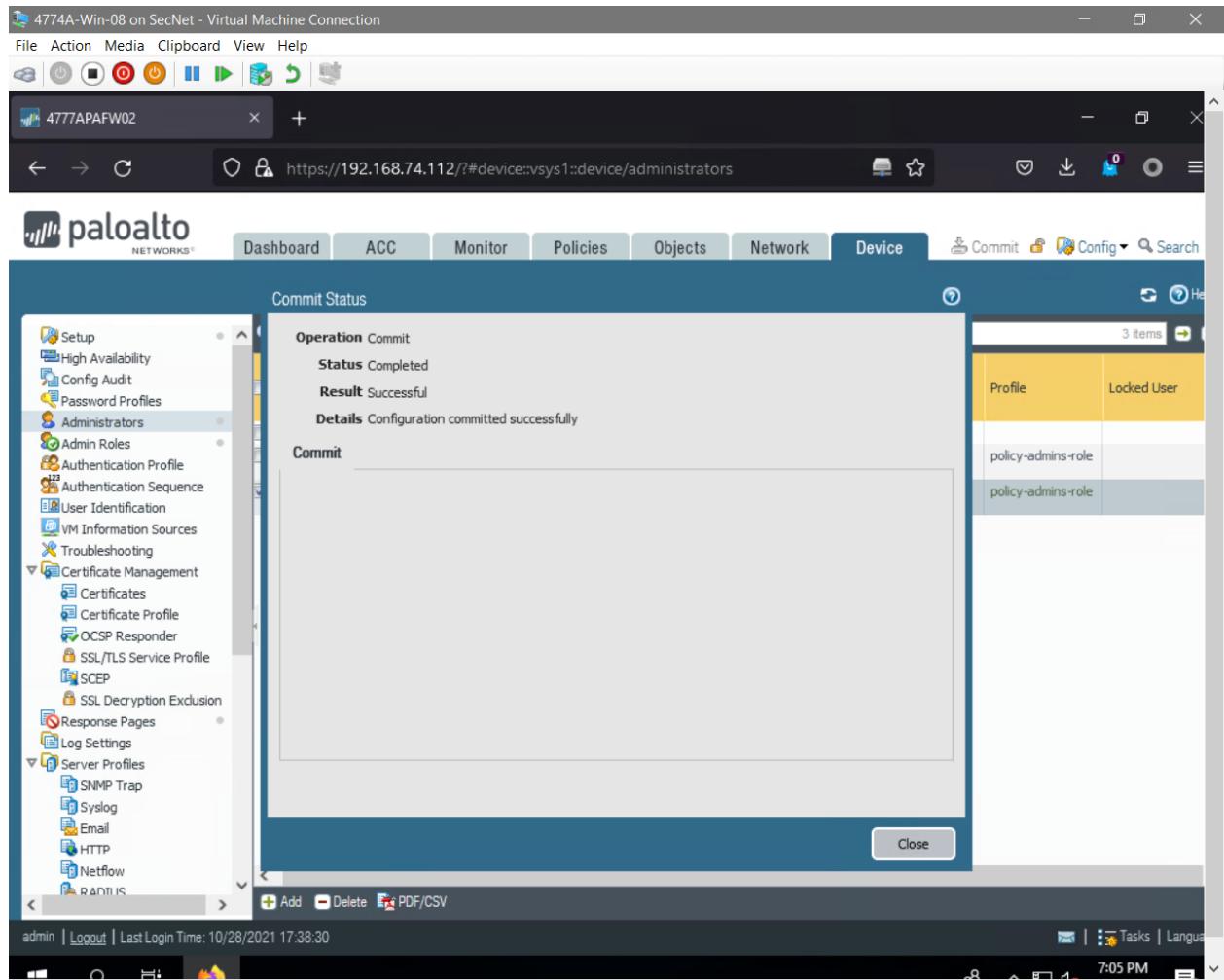
OK Cancel Close

Take Lock Remove Lock

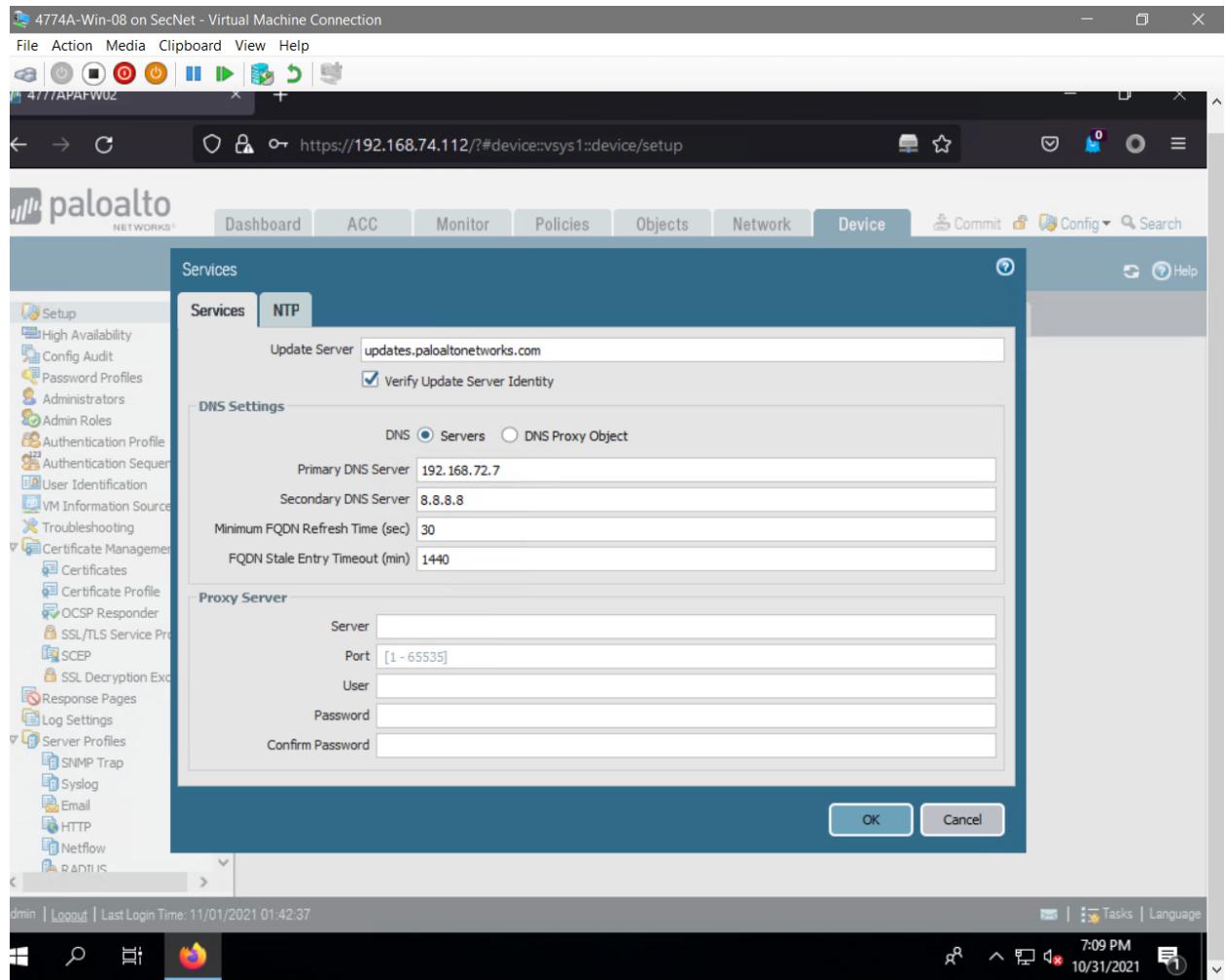
https://192.168.74.112/# Time: 10/28/2021 17:38:30 7:04 PM

The screenshot shows the Palo Alto Networks Device Manager interface. On the left, there's a navigation tree with various configuration sections like Setup, High Availability, and Certificate Management. The 'Device' tab is selected. In the center, a 'Locks' table lists a single entry for 'policy-admin'. A modal dialog box titled 'Remove lock' is displayed, asking 'Are you sure you want to release commit lock for policy-admin?'. The bottom of the screen shows the browser address bar with the URL 'https://192.168.74.112/#' and the system time '10/28/2021 17:38:30'.

Removed commit lock created by policy-admin account



Successfully able to commit changes after removing commit lock



Verified the update server and primary/secondary DNS settings

4774A-Win-08 on SecNet - Virtual Machine Connection

File Action Media Clipboard View Help

4/77/APAFW02

https://192.168.74.112/#device::vsys1:device/dynamic-updates

paloalto NETWORKS

Dashboard ACC Monitor Policies Objects Network Device Commit Config Search Help

SSL Decryption Exclusion Response Pages Log Settings Server Profiles

SNMP Trap Syslog Email HTTP Netflow RADIUS TACACS+ LDAP Kerberos SAML Identity Provider Multi Factor Authentication

Local User Database Users User Groups Scheduled Log Export Software GlobalProtect Client Dynamic Updates Plugins VM-Series Licenses Support Master Key and Diagnostics

Check Now Upload Install From File

dmin | Logout | Last Login Time: 11/01/2021 01:42:37

Tasks | Language

7:21 PM 10/31/2021

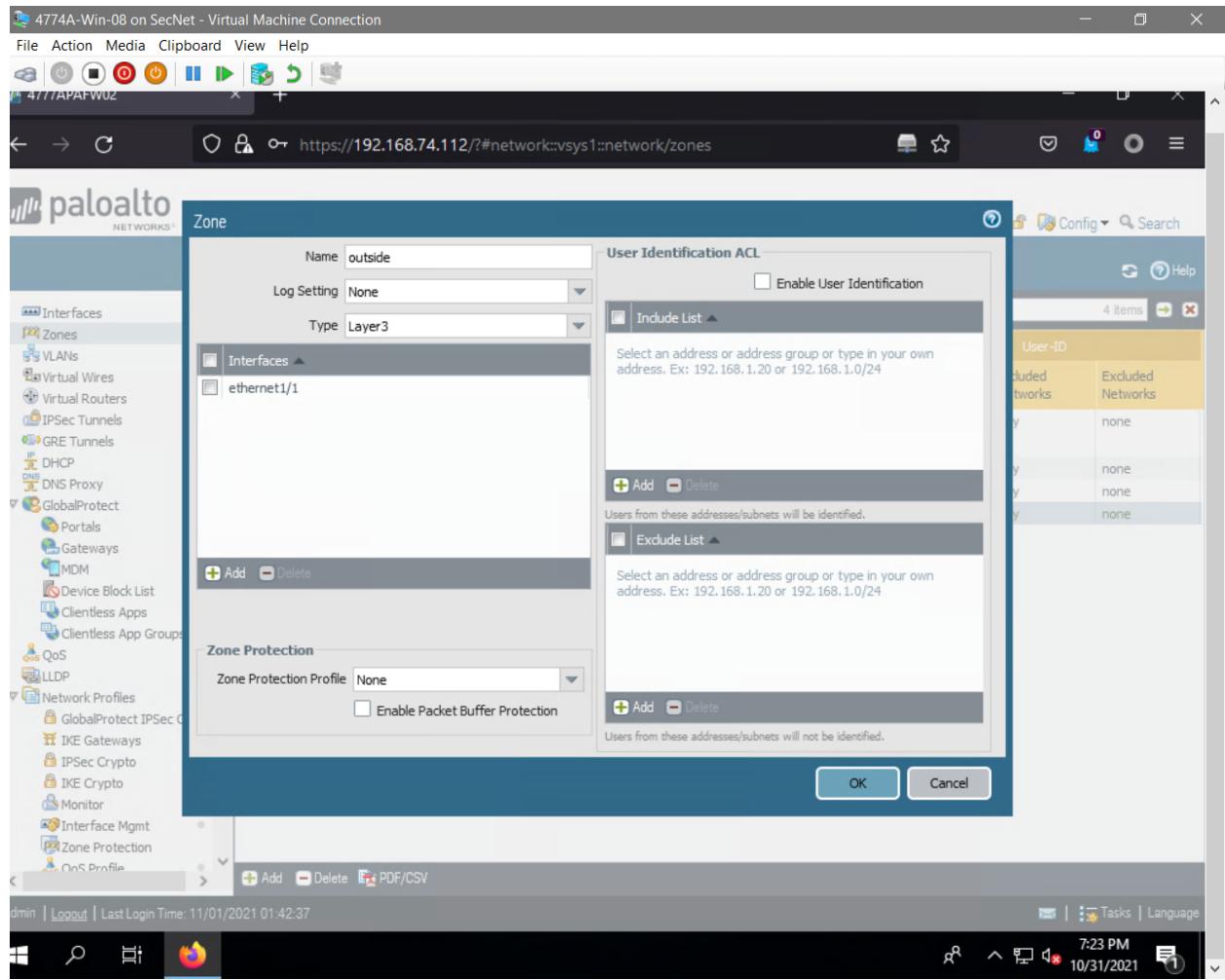
Applications and Threats Update Schedule

Version	File Name	Features	Type	Size	Release Date	Downloaded	Currently Installed	Action	Document...
1.0	AppID_1.0.0.0	Antivirus, Application Control, Intrusion Prevention, Threat Intelligence	Content	~100 MB	2021-10-31 01:15	100%	Yes	download-and-install	

Reurrence: Daily
Time: 01:15
Action: download-and-install
 Disable new apps in content update
Threshold (hours): [1 - 336]
A content update must be at least this many hours old for the action to be taken.
Allow Extra Time to Review New App-IDs
Set the amount of time the firewall waits before installing content updates that contain new App-IDs. You can use this wait period to assess and adjust your security policy based on the new App-IDs.
New App-ID Threshold (hours): [1 - 336]

Delete Schedule OK Cancel

Configured daily updates for Applications and Threats section



Created outside zone

4774A-Win-08 on SecNet - Virtual Machine Connection

File Action Media Clipboard View Help

4774A-Win-08

https://192.168.74.112/#network::vsys1::network/network-profiles/interface-management-profiles

paloalto NETWORKS

Dashboard ACC Monitor Policies Objects Network Device Commit Config Search

Interface Management Profile

Name: ping-and-response-pages

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

User-ID	User-ID	Permitted IP Addresses
Syslog Listener-SSL	Syslog Listener-UDP	

Add Delete OK Cancel

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

Administrator | Logout | Last Login Time: 11/01/2021 01:42:37

Tasks Language

7:25 PM 10/31/2021

Created ping-and-response-pages Interface Management Profile

4774A-Win-08 on SecNet - Virtual Machine Connection

File Action Media Clipboard View Help

Dashboard ACC Monitor Policies Objects Network Device Commit Config Search

paloalto NETWORKS®

Interface Management Profile

Name: ping-only

Administrative Management Services

- HTTP
- HTTPS
- Telnet
- SSH

Network Services

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

Permitted IP Addresses

User-ID Syslog Listener-SSL	User-ID Syslog Listener-UDP	Permitted IP Addresses

Add Delete OK Cancel

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

Network Profiles

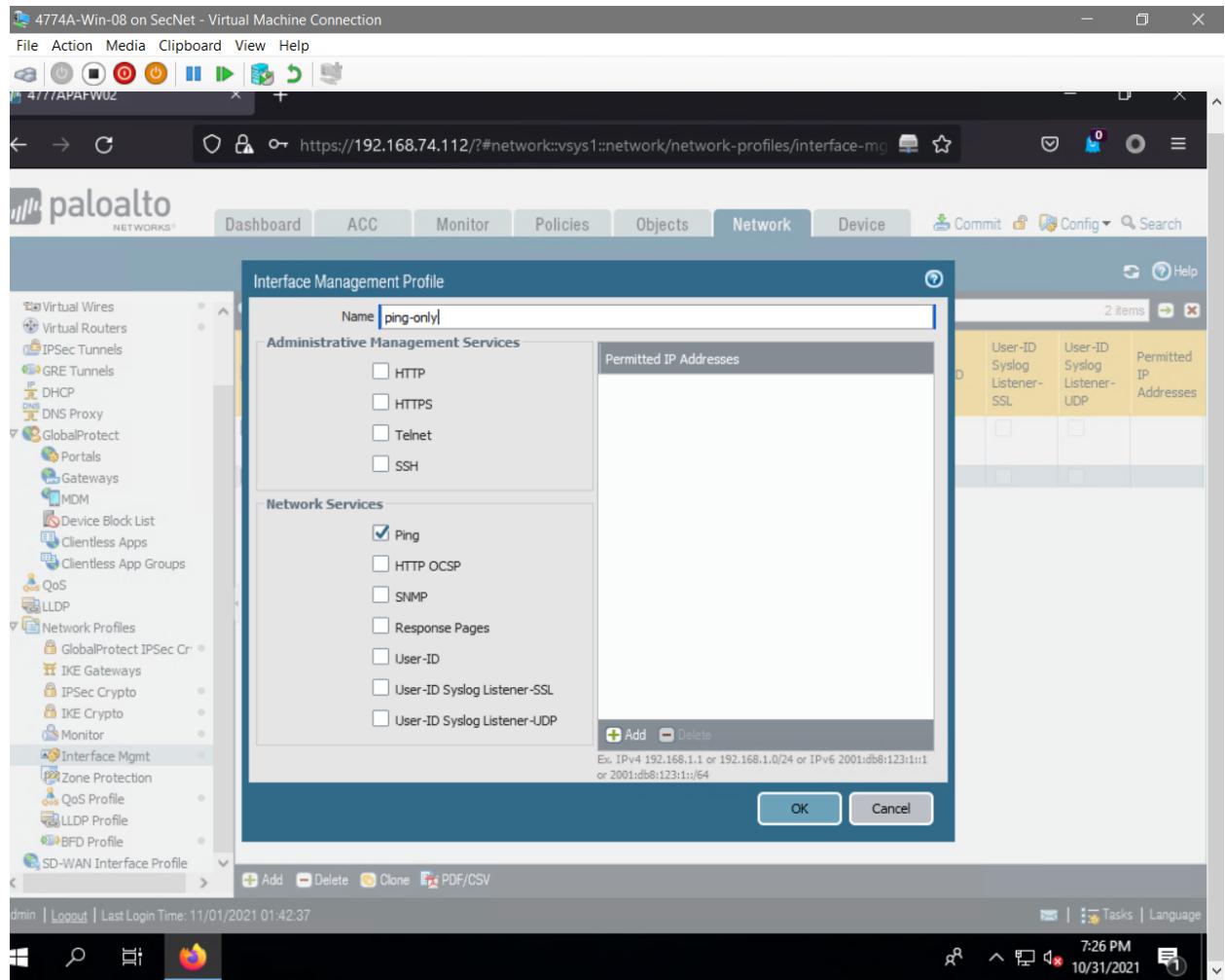
- GlobalProtect IPSec Cr.
- IKE Gateways
- IPSec Crypto
- IKE Crypto
- Monitor
- Interface Mgmt
- Zone Protection
- QoS Profile
- LLDP Profile
- BFD Profile

SD-WAN Interface Profile

admin | Logout | Last Login Time: 11/01/2021 01:42:37

Tasks | Language

7:26 PM 10/31/2021



Created ping-only Interface Management Profile

4774A-Win-08 on SecNet - Virtual Machine Connection

File Action Media Clipboard View Help

Dashboard ACC Monitor Policies Objects Network Device Commit Config Search

paloalto NETWORKS®

Virtual Wires Virtual Routers IPSec Tunnels GRE Tunnels IP DHCP DNS DNS Proxy GlobalProtect Portals Gateways MDM Device Block List Clientless Apps Clientless App Groups QoS LLDP Network Profiles GlobalProtect IPSec Cr IKE Gateways IPSec Crypto IKE Crypto Monitor Interface Mgmt Zone Protection QoS Profile LLDP Profile BFD Profile SD-WAN Interface Profile

Name Ping Telnet SSH HTTP HTTP OCSP HTTPS SNMP Response Pages User-ID User-ID Syslog Listener-SSL User-ID Syslog Listener-UDP Permitted IP Addresses

Name	Ping	Telnet	SSH	HTTP	HTTP OCSP	HTTPS	SNMP	Response Pages	User-ID	User-ID Syslog Listener-SSL	User-ID Syslog Listener-UDP	Permitted IP Addresses
ping-and-response-pages	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
ping-only	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							

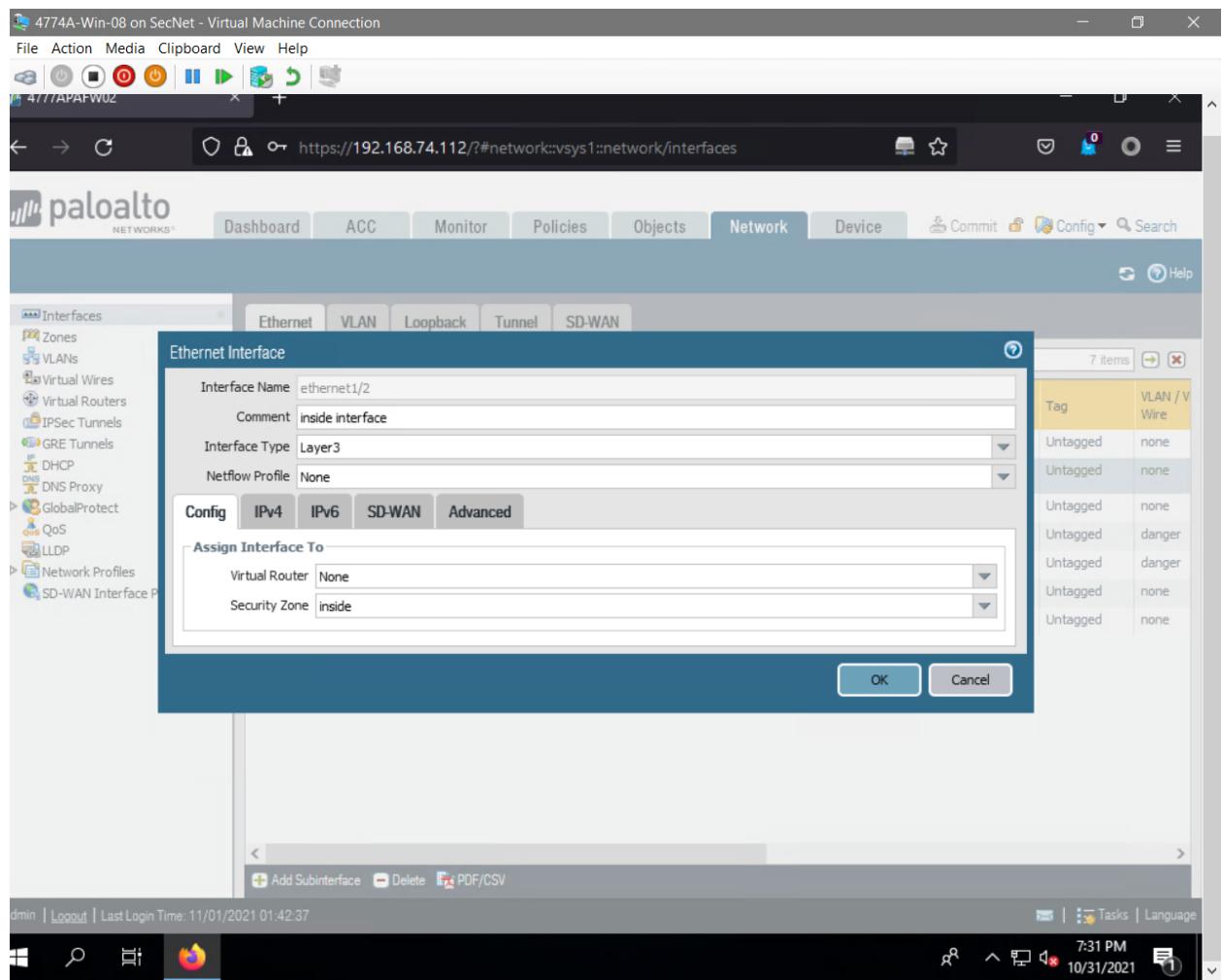
Add Delete Clone PDF/CSV

dmin | Logout | Last Login Time: 11/01/2021 01:42:37

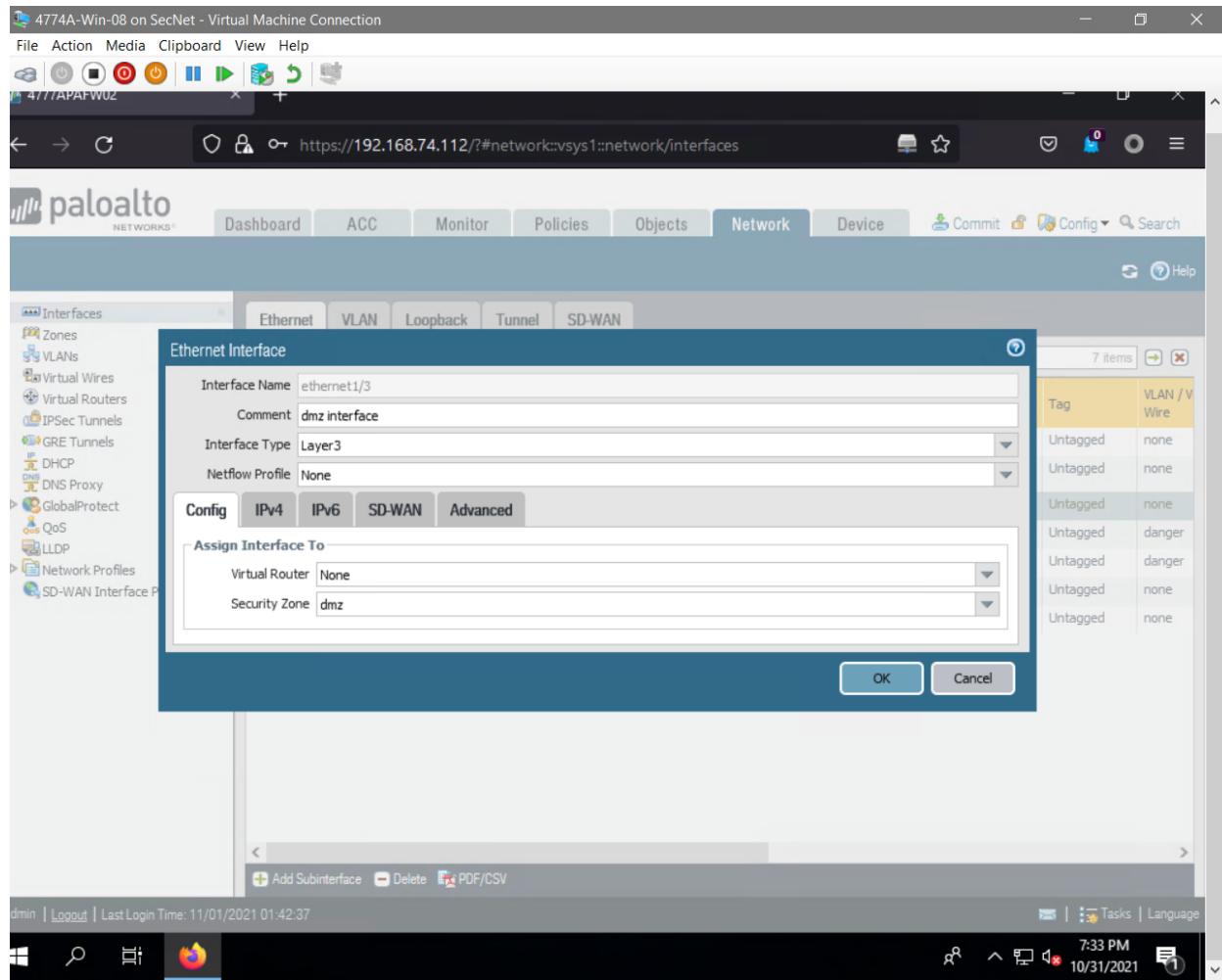
Tasks | Language

7:27 PM 10/31/2021

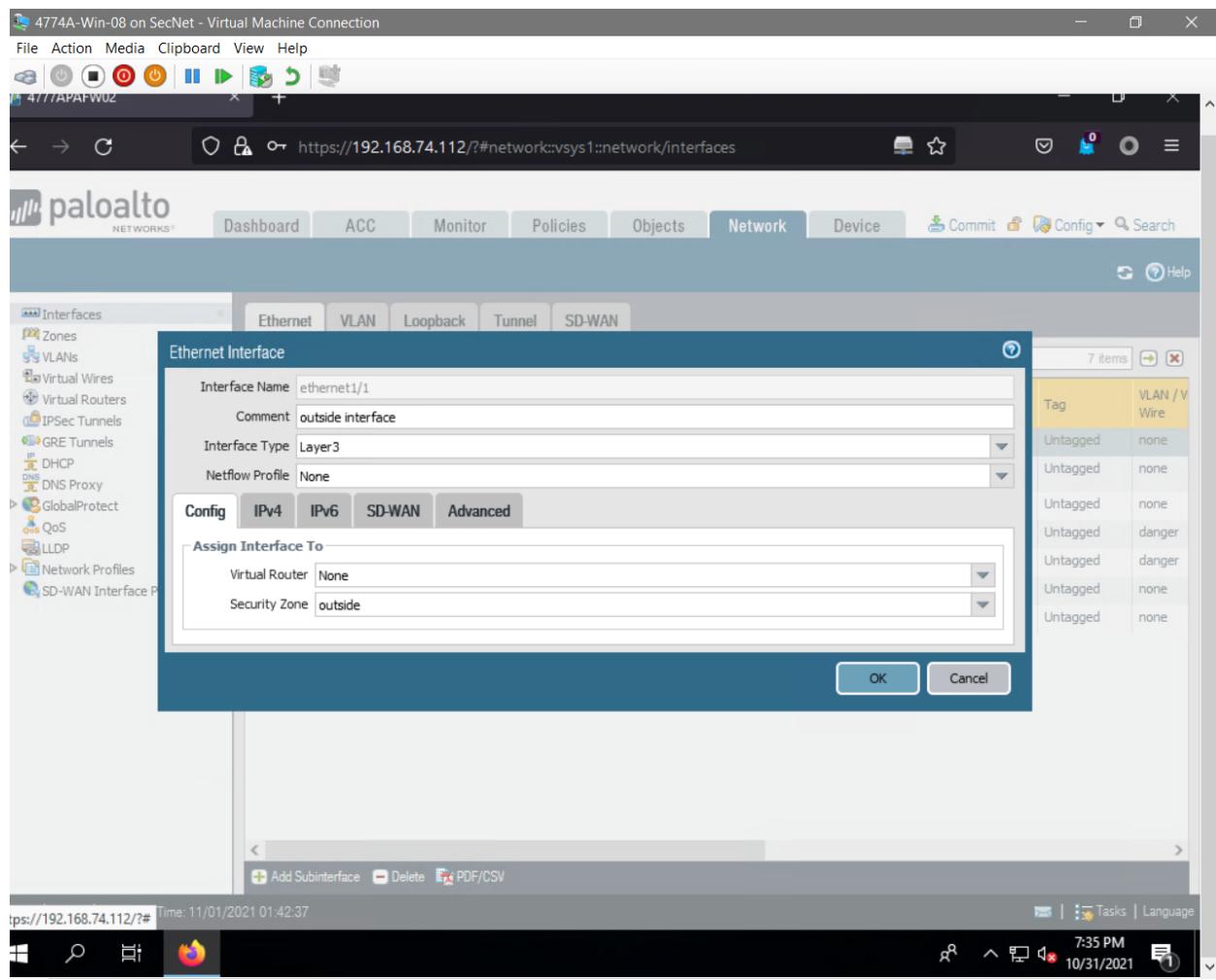
Verified configuration of Interface Management Profiles



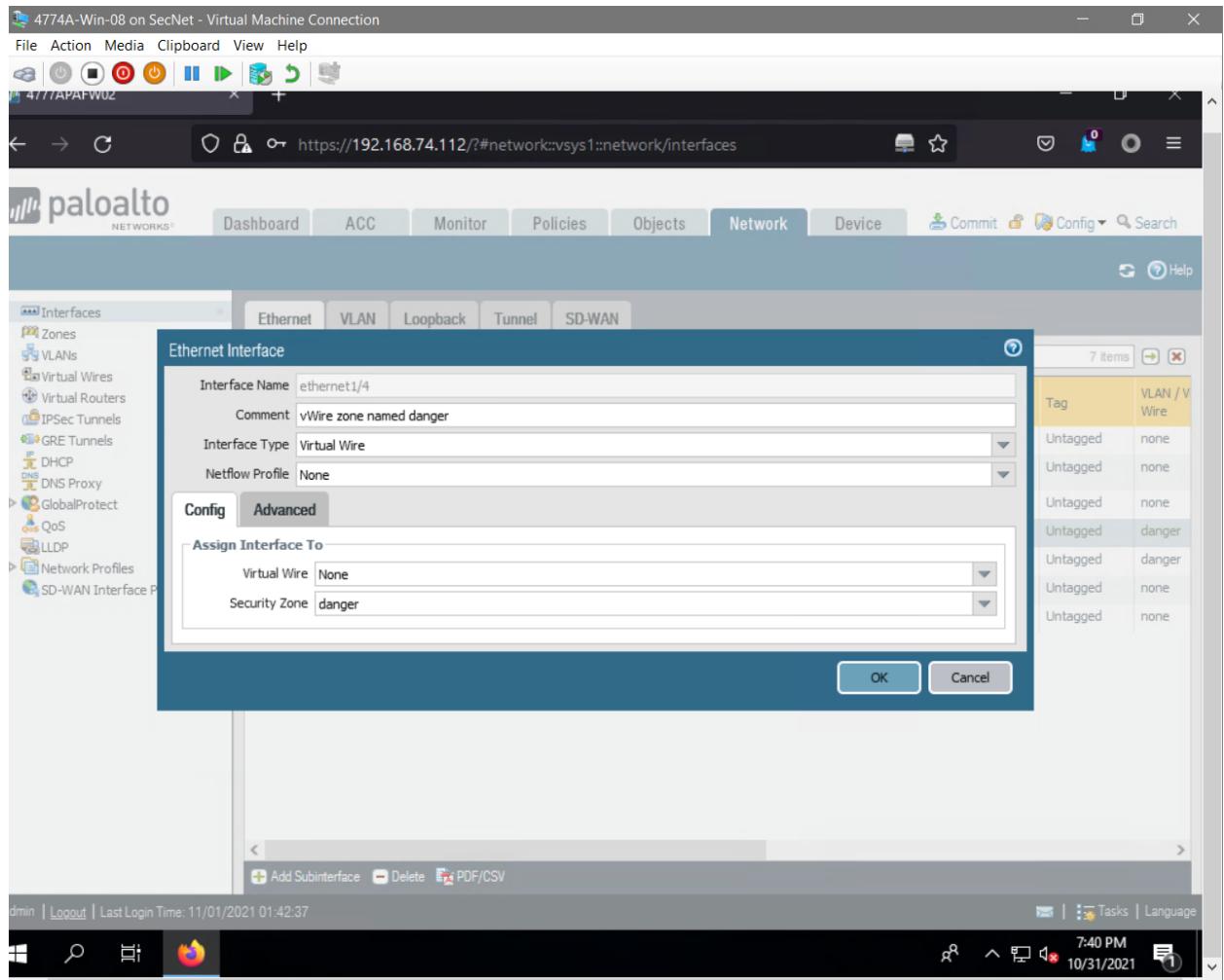
'Inside' Ethernet Interface configured



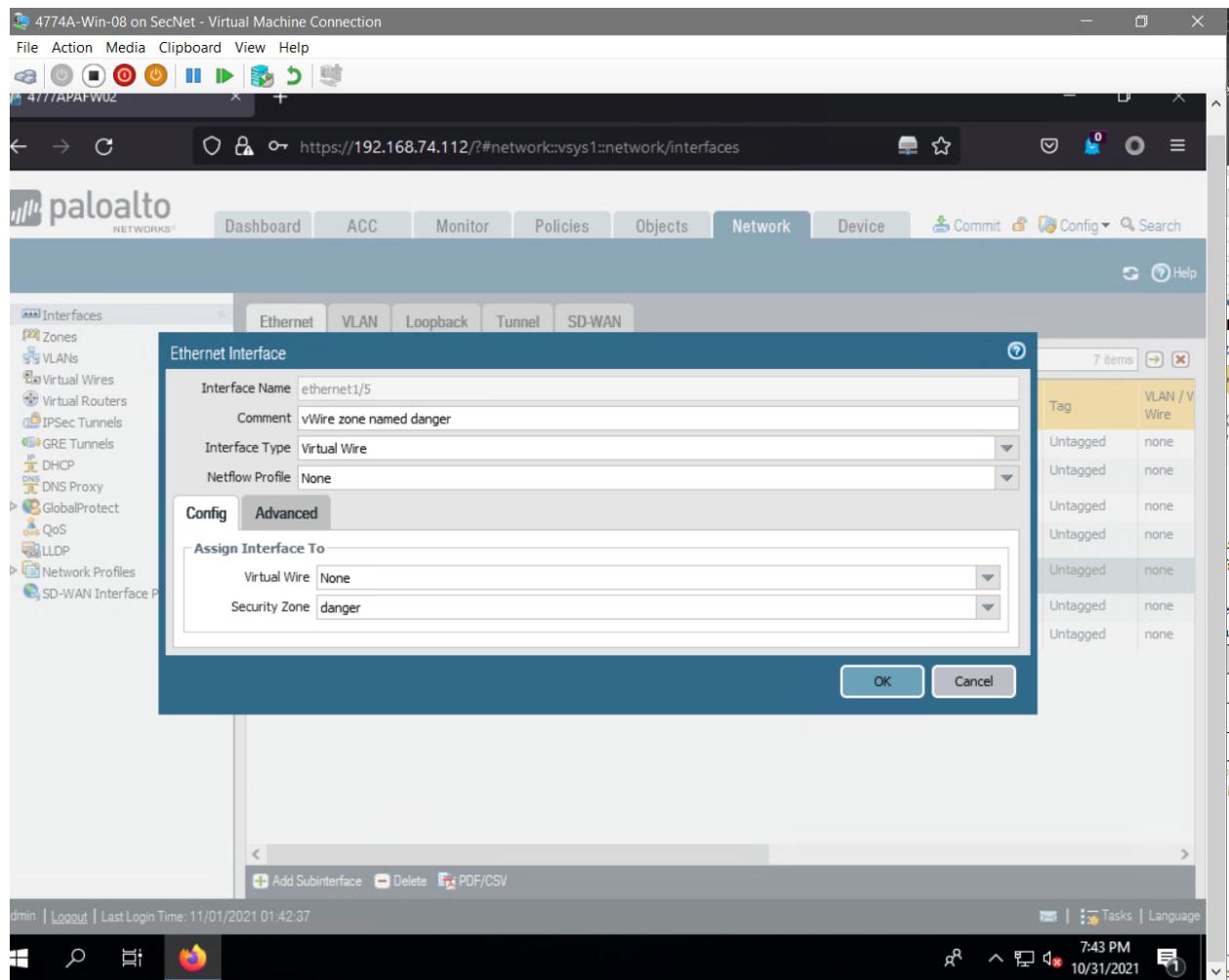
Configured 'dmz' ethernet interface



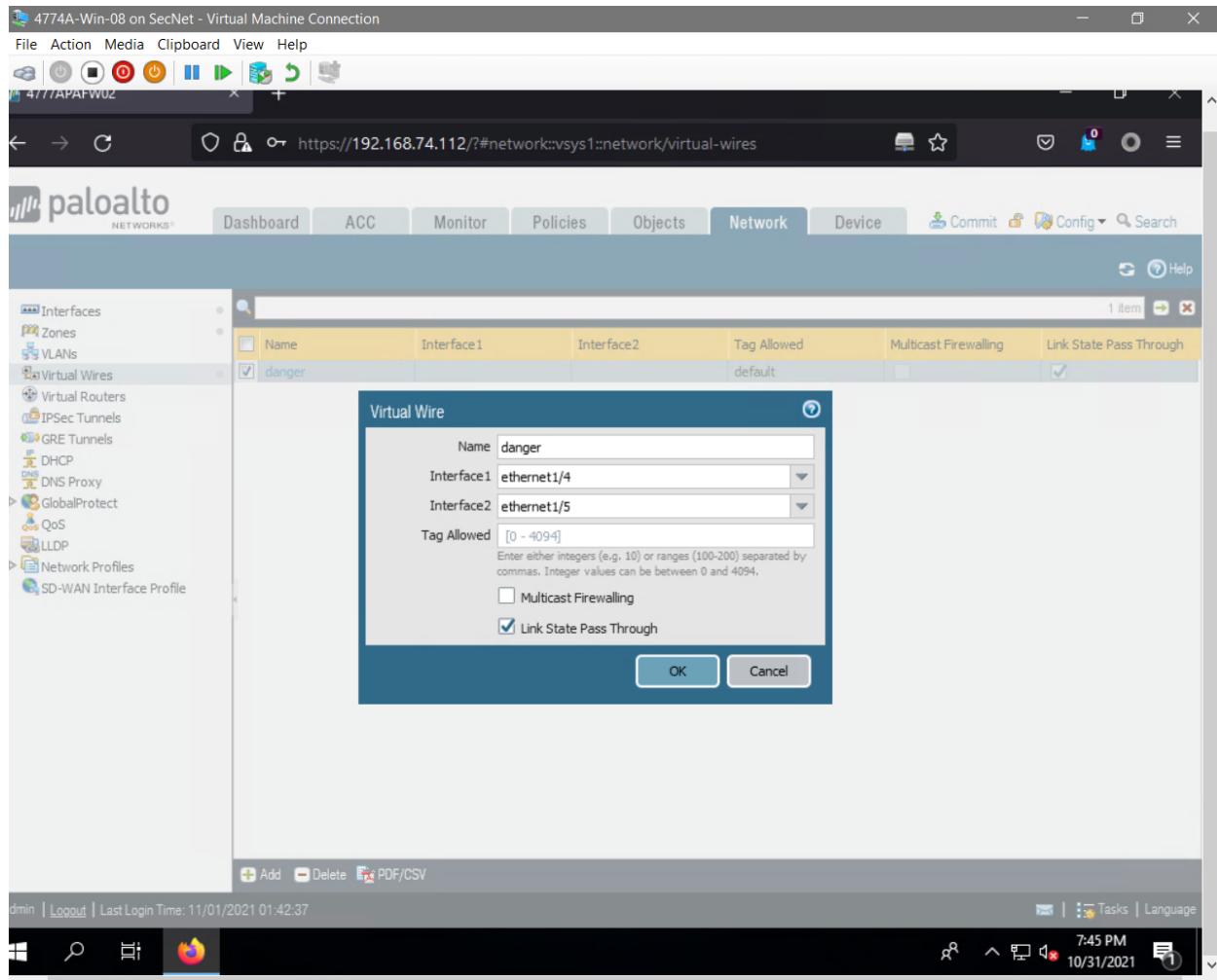
Configured 'outside' Ethernet Interface



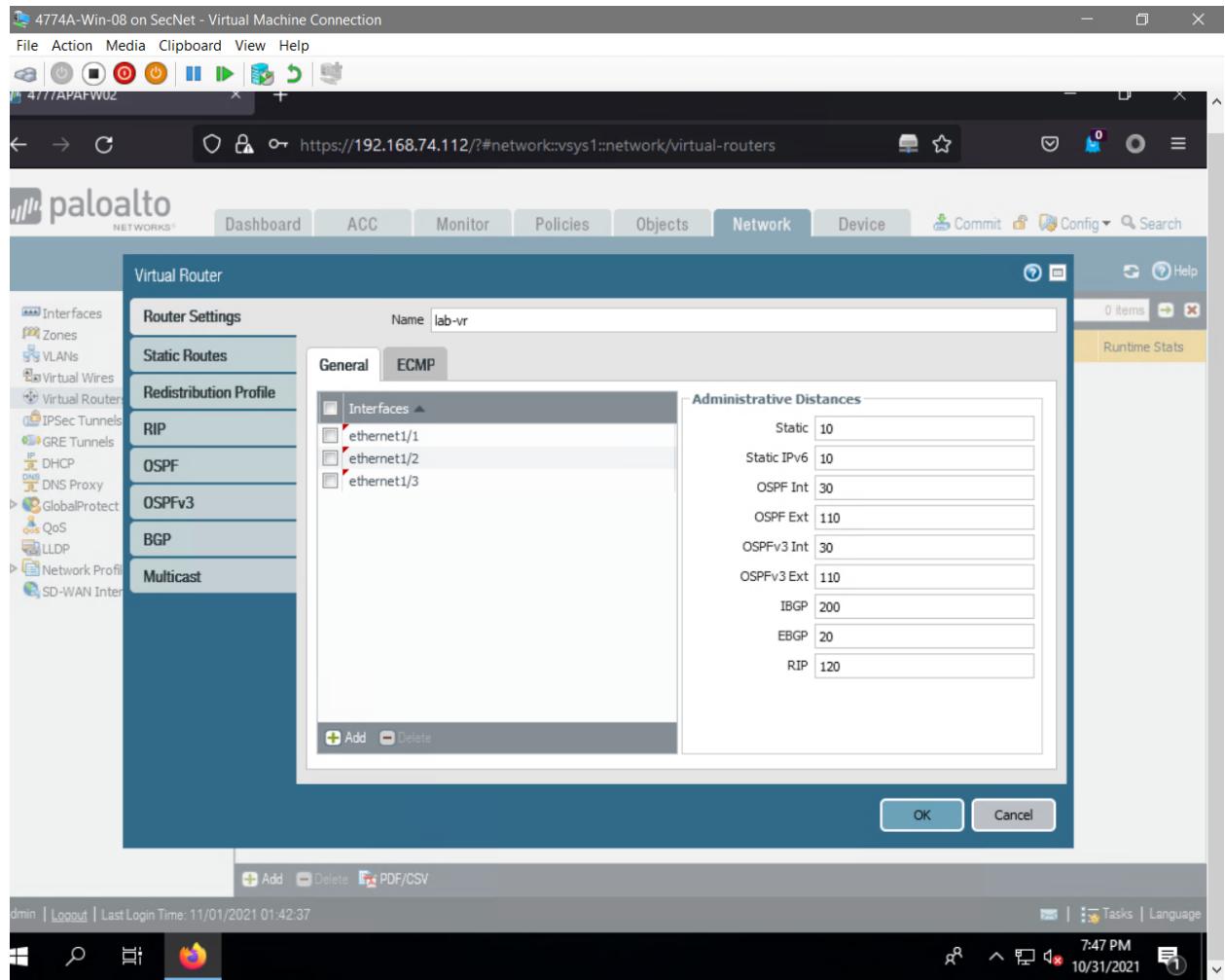
Configured 'vWire zone named danger' Ethernet Interface



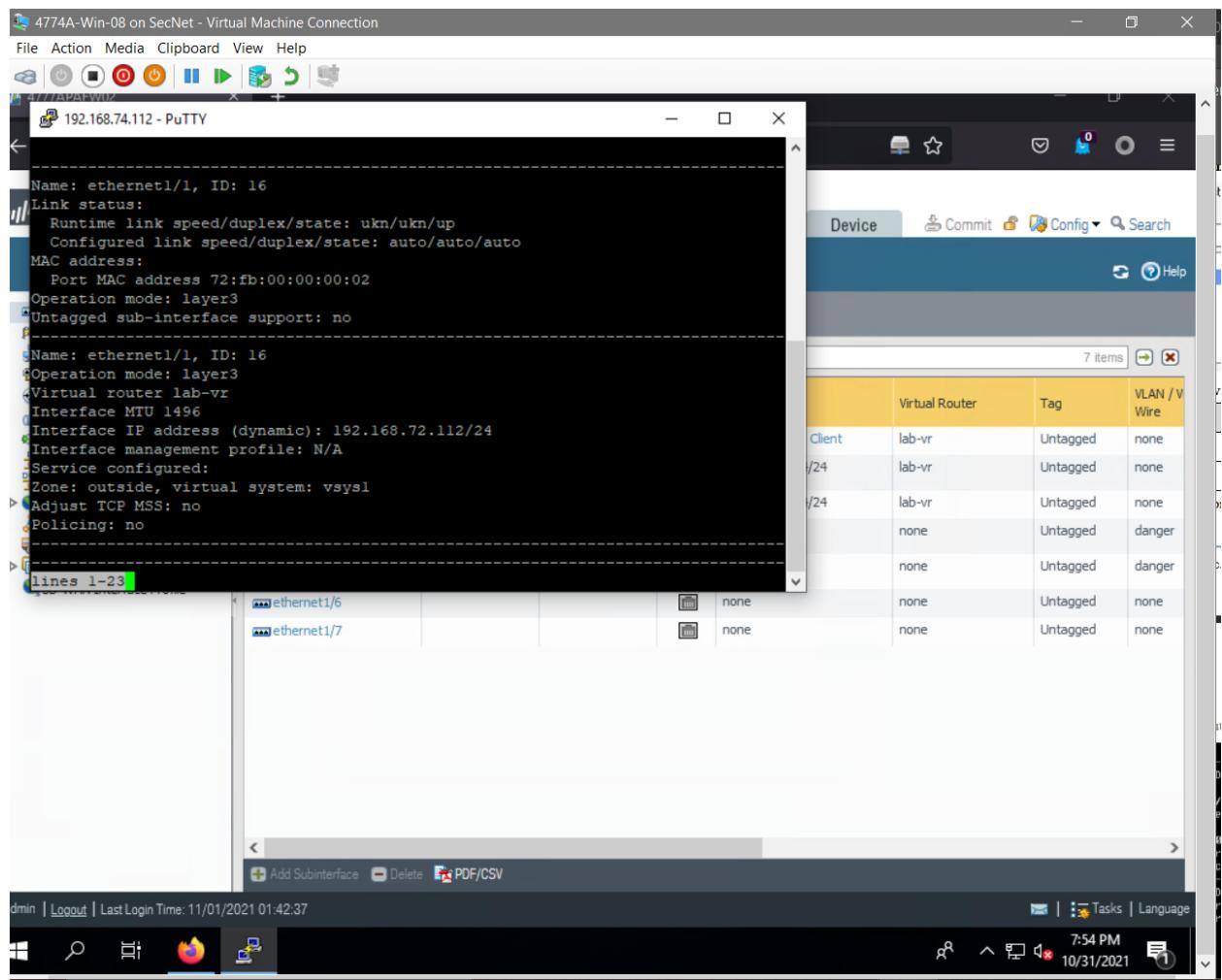
Configured second 'vWire zone named danger' ethernet interface for ethernet1/5



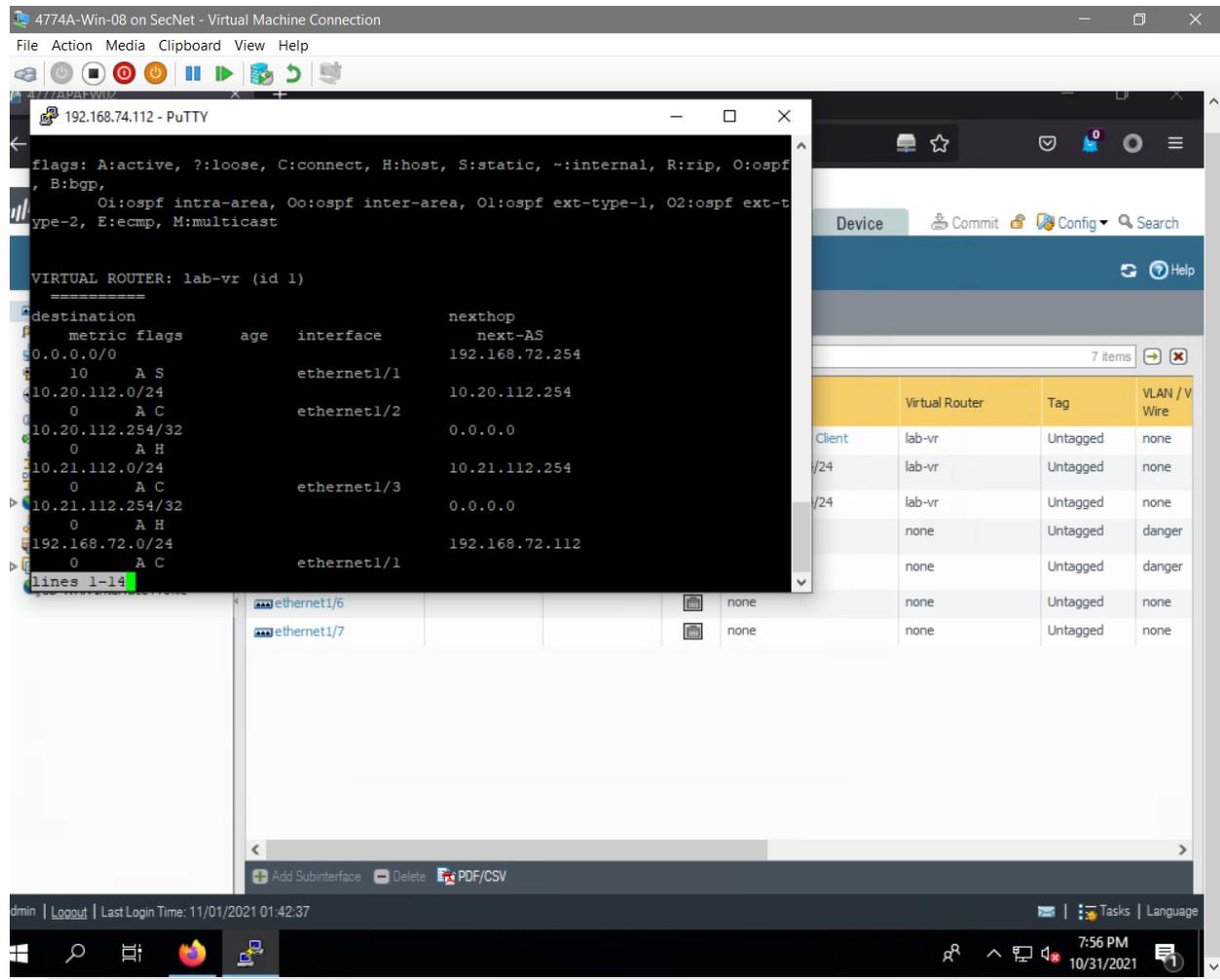
Configured 'danger' virtual wire



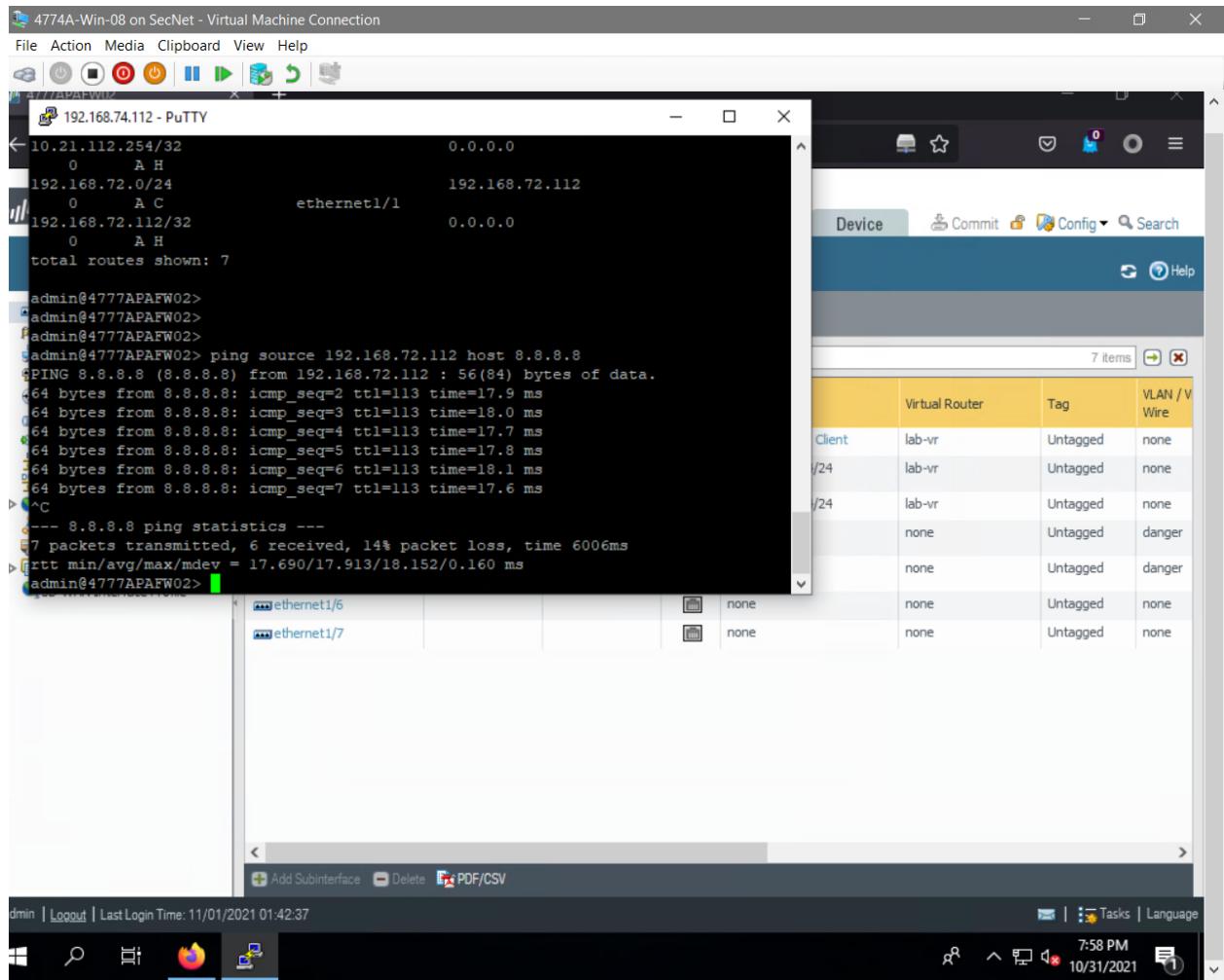
Configured 'lab-vr' virtual router



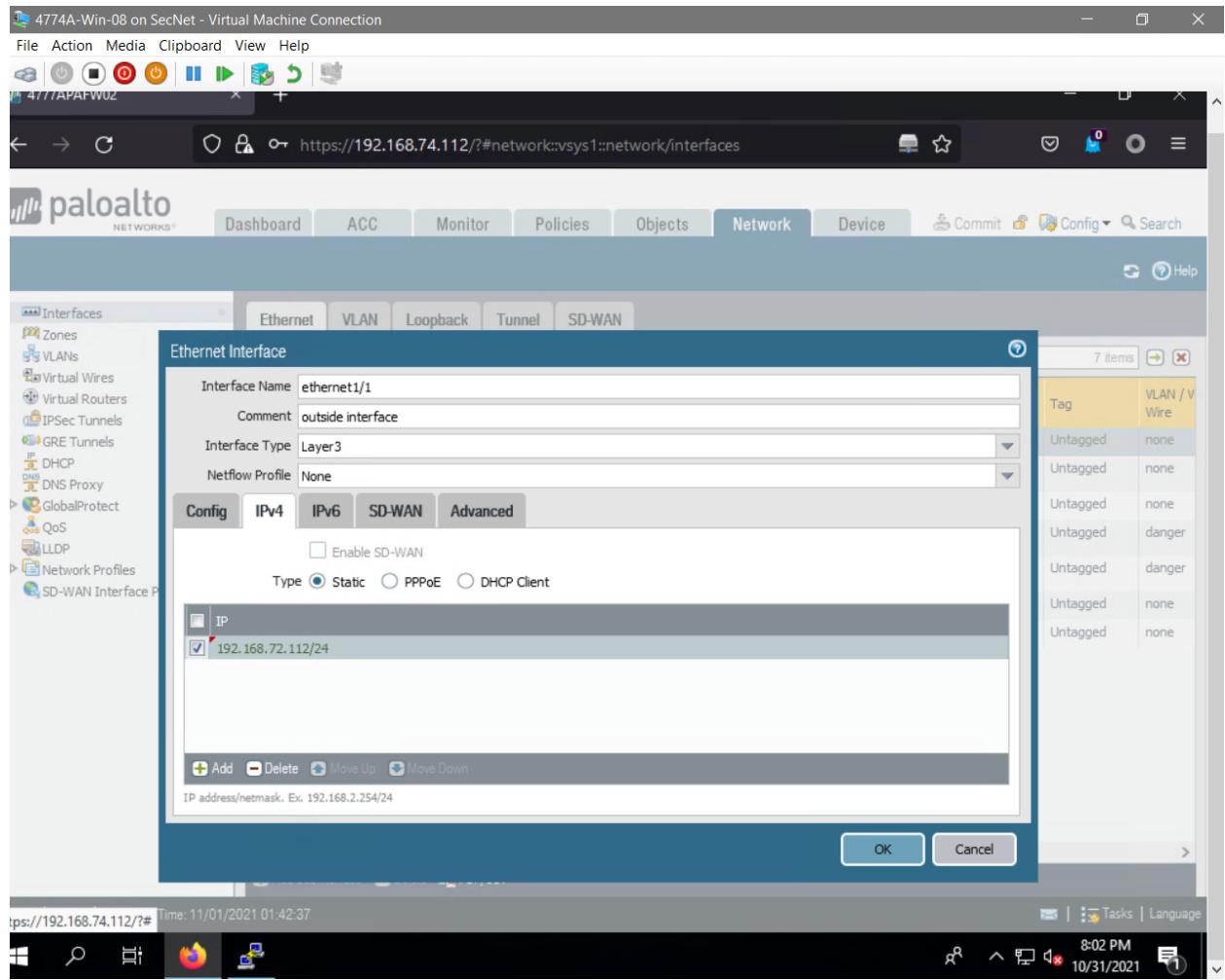
Showing interface in command line for ethernet1/1



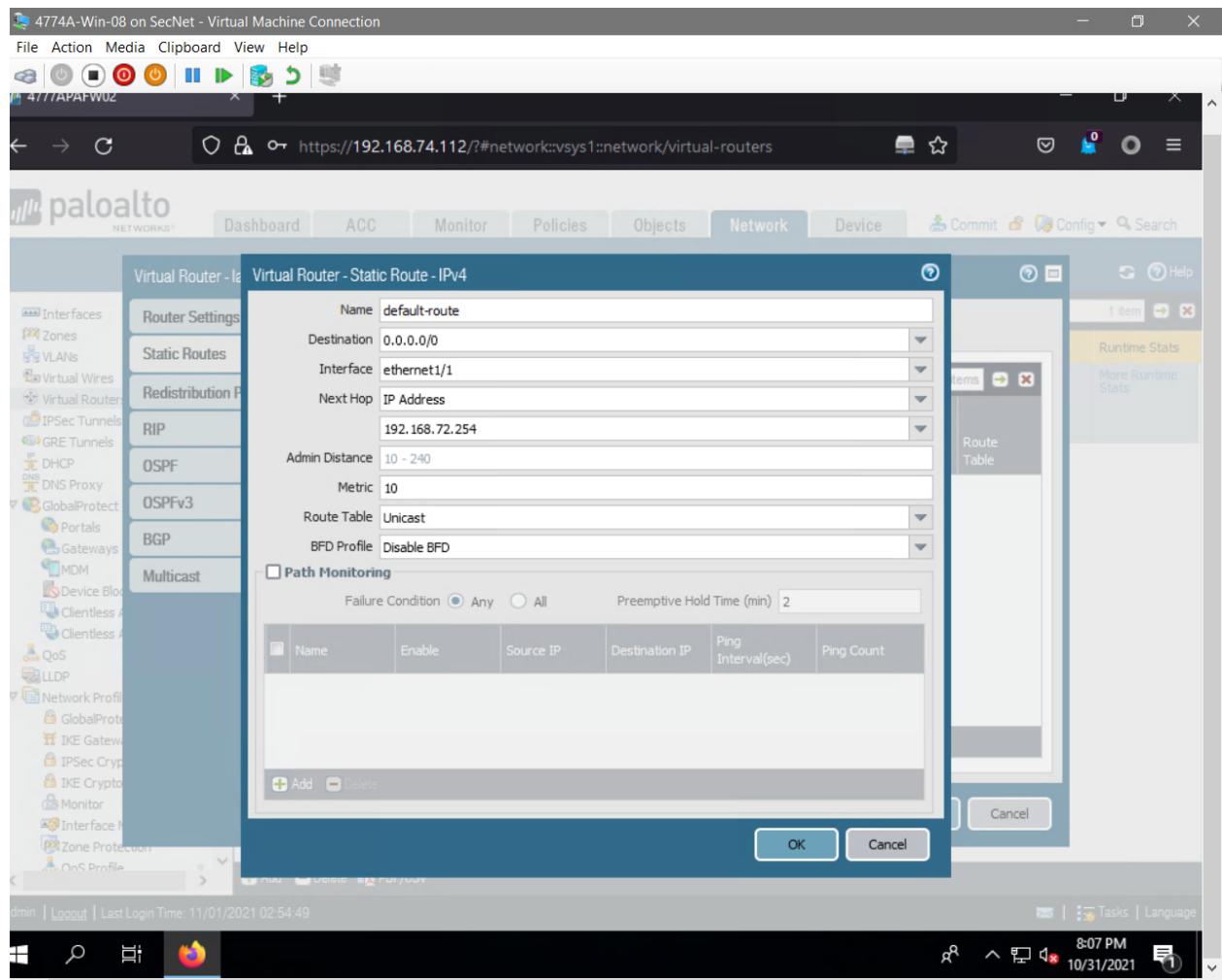
Showing routing route on command line for firewall



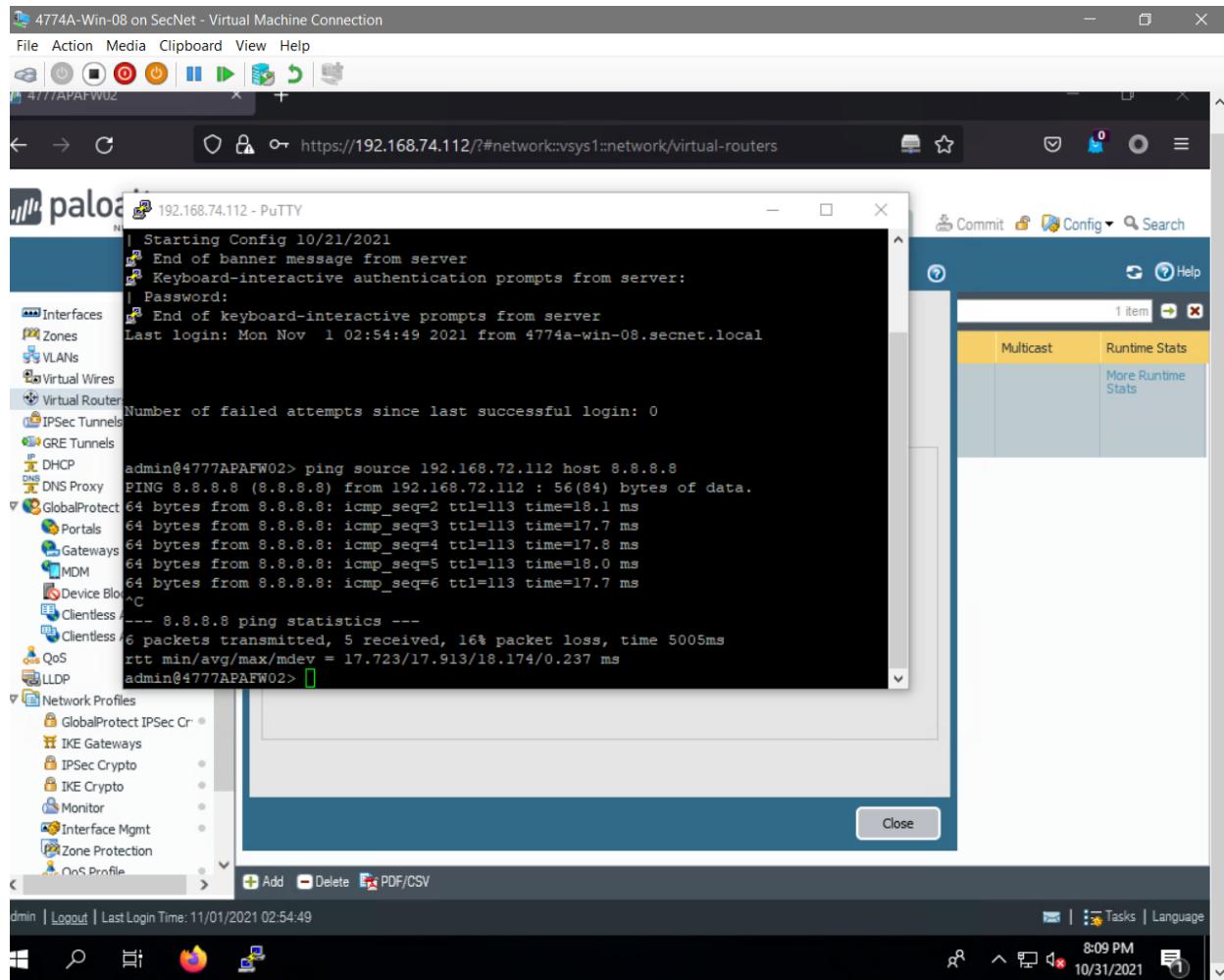
Pinging outside of firewall to verify connectivity to internet



Created new outside ethernet interface with static IP



Added new static route



Pinged source from within firewall CLI, confirming successful configuration