



NETWORK SECURITY FUNDAMENTALS V2

Lab 2: Configuring Virtual IP Addresses

Document Version: **2022-12-23**

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

| | |
|---|----|
| Introduction | 3 |
| Objective | 3 |
| Lab Topology..... | 4 |
| Lab Settings..... | 5 |
| 1 Configuring Virtual IP Addresses..... | 6 |
| 1.0 Load Lab Configuration | 6 |
| 1.1 Configure a Virtual IP Address..... | 11 |

Introduction

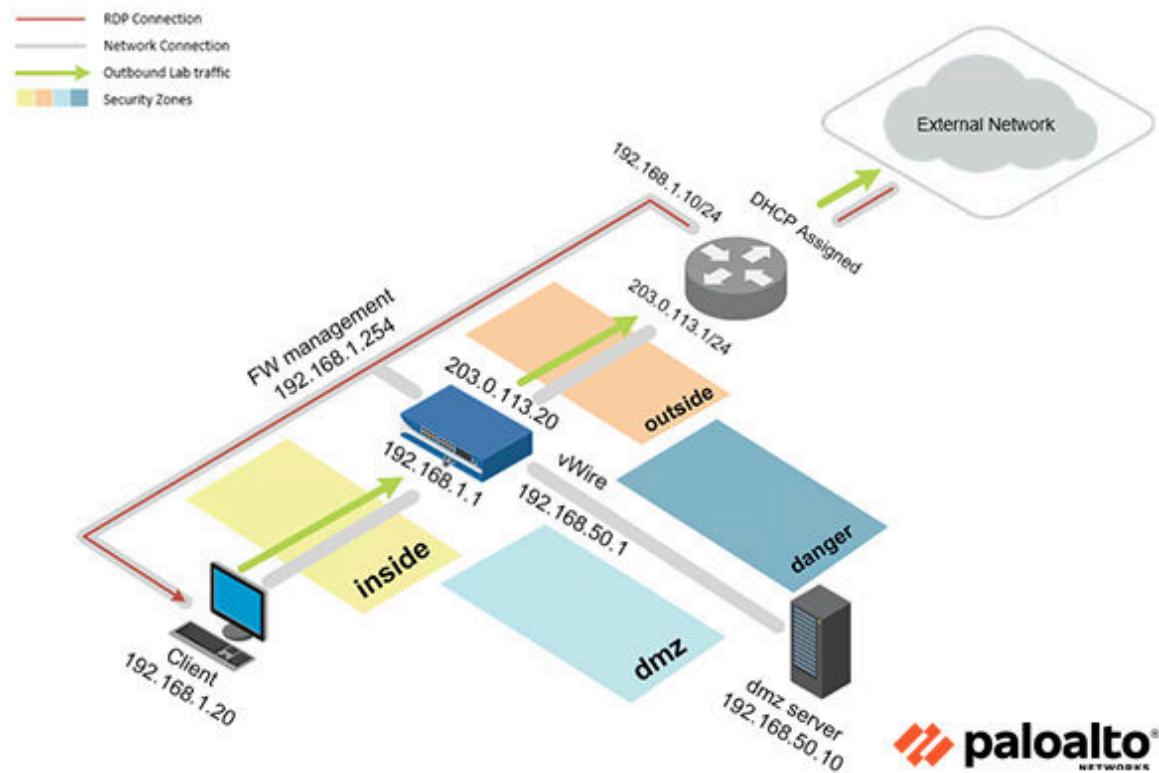
In this lab, you will configure the Palo Alto Networks Firewall inside interface with a virtual IP address.

Objective

In this lab, you will perform the following tasks:

- Configure a Virtual IP Address
- Configure a Virtual IP Address on another subnet

Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

| Virtual Machine | IP Address | Account (if needed) | Password (if needed) |
|-----------------|---------------|------------------------|-------------------------|
| Client | 192.168.1.20 | lab-user | PaloAlt0! |
| DMZ | 192.168.50.10 | root | PaloAlt0! |
| Firewall | 192.168.1.254 | admin | PaloAlt0! |

1 Configuring Virtual IP Addresses

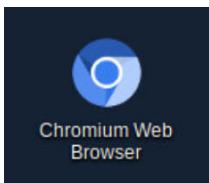
1.0 Load Lab Configuration

In this section, you will load the Firewall configuration file.

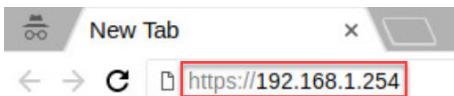
1. Click on the **Client** tab to access the Client PC.



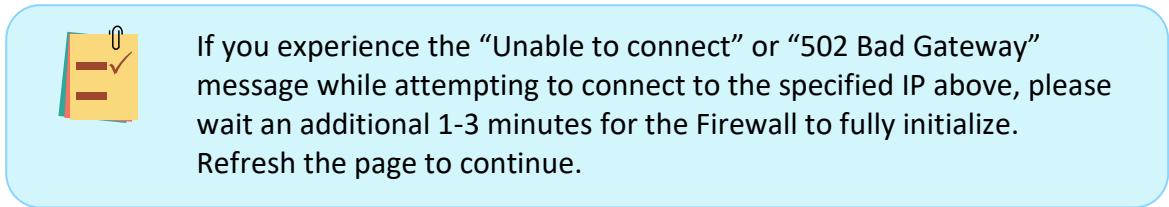
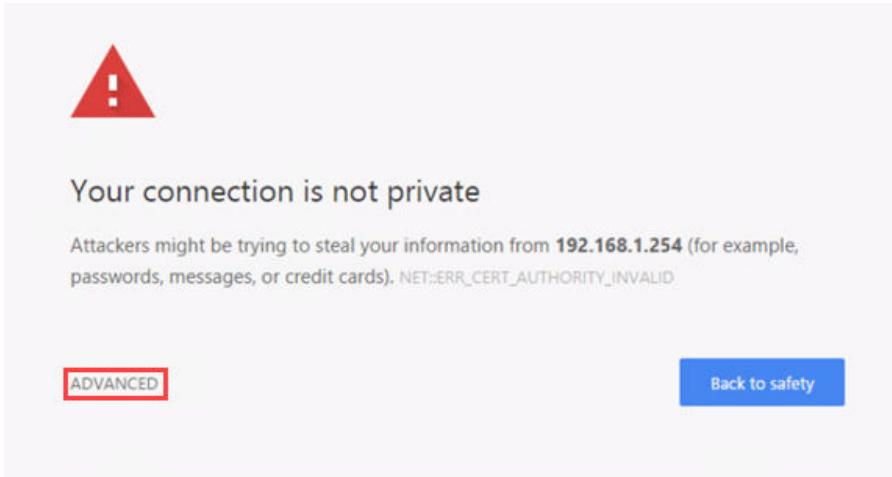
2. Log in to the Client PC as username `lab-user`, password `Pal0Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.



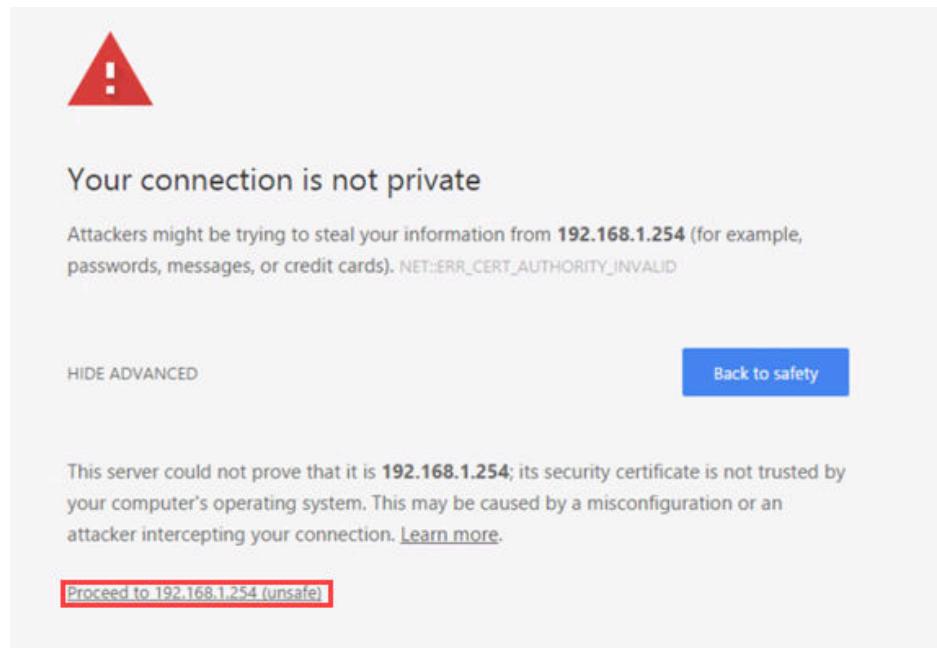
4. In the *Chromium* address field, type `https://192.168.1.254` and press **Enter**.



5. You will see a “*Your connection is not private*” message. Click on the **ADVANCED** link.



6. Click on **Proceed to 192.168.1.254 (unsafe)**.



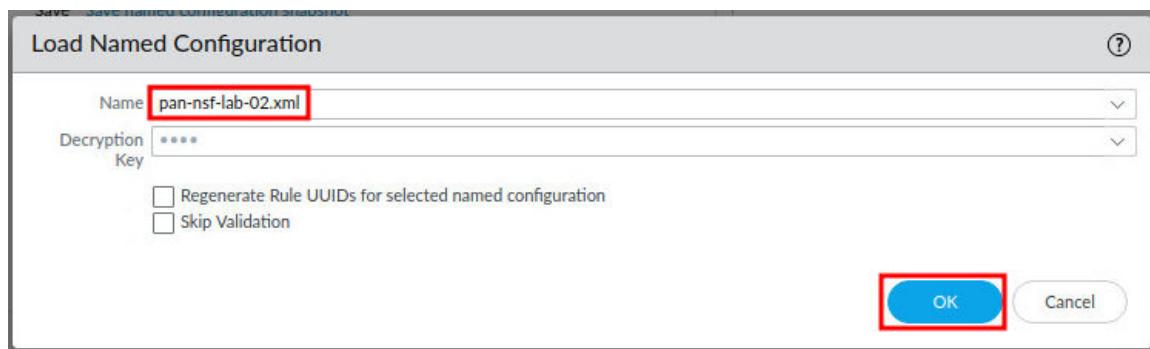
7. Log in to the Firewall web interface as username admin, password PaloAlt0!.



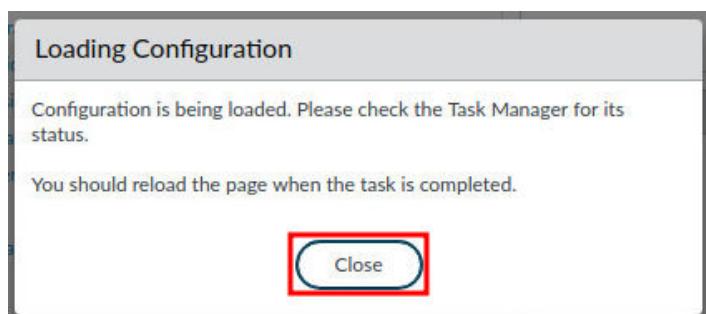
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

The screenshot shows the PA-VM web interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The DEVICE tab is selected. On the left, a sidebar menu under the 'Setup' icon includes options like High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, Data Redistribution, Device Quarantine, VM Information Sources, Troubleshooting, Certificate Management (Certificates, Certificate Profile, OCSP Responder), and Miscellaneous (Custom Log, SNMP Set). The main content area has tabs for Management, Operations (which is selected and highlighted in red), Services, Interfaces, Telemetry, Content-ID, WildFire, Session, and Help. Under the Operations tab, there's a 'Configuration Management' section with several options: Revert (Revert to last saved configuration, Revert to running configuration), Save (Save named configuration snapshot, Save candidate configuration), Load (Load named configuration snapshot, Load configuration version), Export (Export named configuration snapshot, Export configuration version, Export device state), and Import (Import named configuration snapshot, Import device state). The 'Load named configuration snapshot' option is highlighted with a red box.

9. In the *Load Named Configuration* window, select **pan-nsf-lab-02.xml** from the *Name* dropdown box and click **OK**.



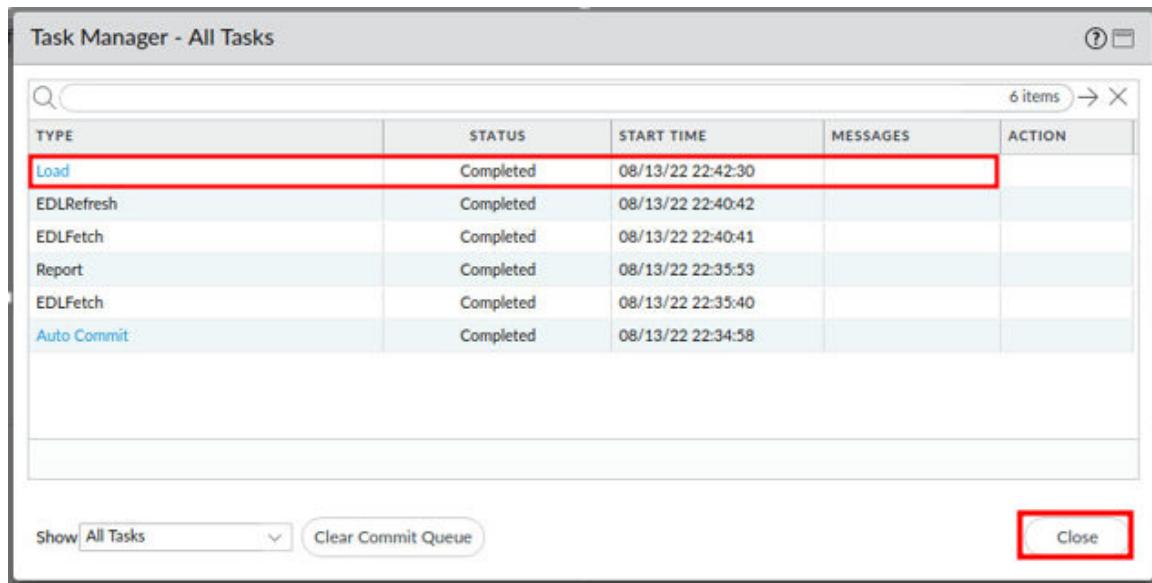
10. In the Loading Configuration window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



11. Click the **Tasks** icon located at the bottom-right of the web interface.



12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

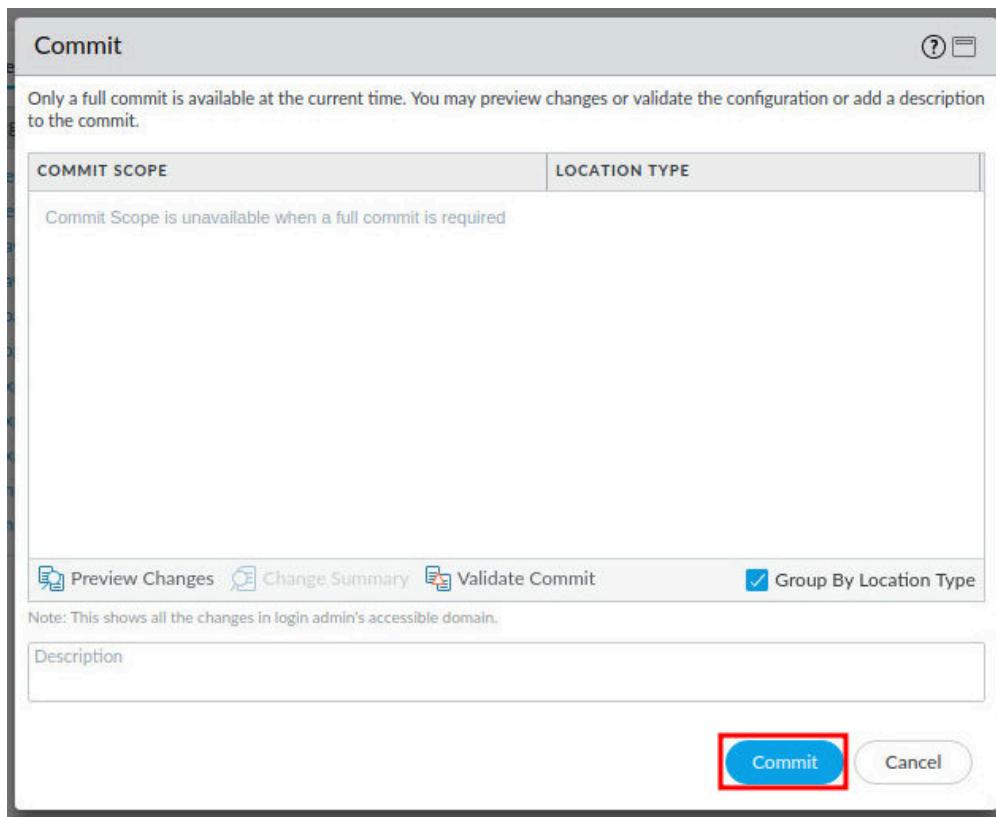


| TYPE | STATUS | START TIME | MESSAGES | ACTION |
|-------------|-----------|-------------------|----------|--------|
| Load | Completed | 08/13/22 22:42:30 | | |
| EDLRefresh | Completed | 08/13/22 22:40:42 | | |
| EDLFetch | Completed | 08/13/22 22:40:41 | | |
| Report | Completed | 08/13/22 22:35:53 | | |
| EDLFetch | Completed | 08/13/22 22:35:40 | | |
| Auto Commit | Completed | 08/13/22 22:34:58 | | |

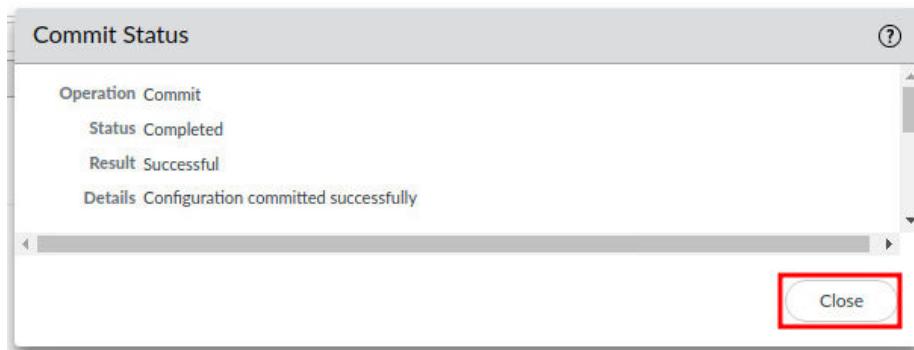
13. Click the **Commit** link located at the top-right of the web interface.



14. In the **Commit** window, click **Commit** to proceed with committing the changes.



15. When the commit operation successfully completes, click **Close** to continue.



The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

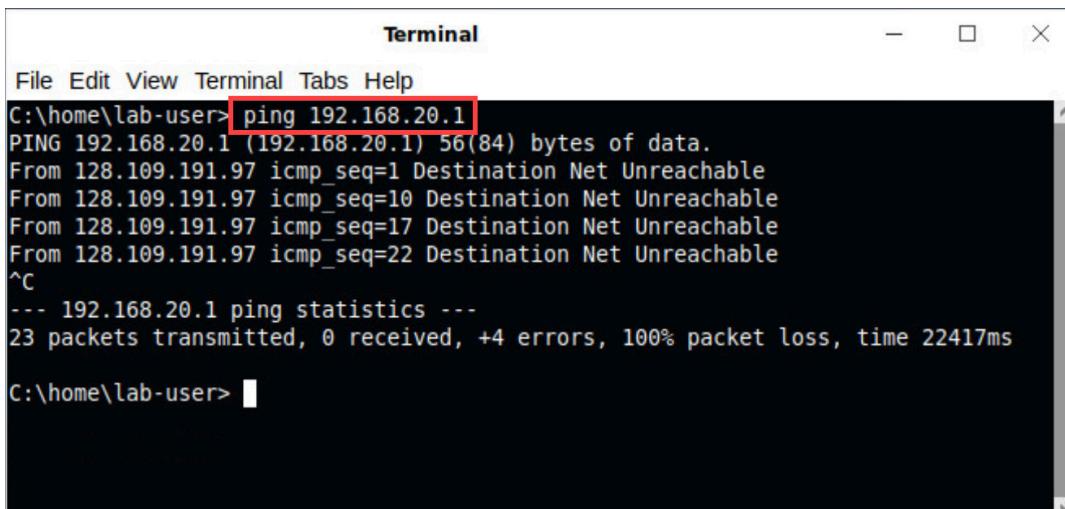
1.1 Configure a Virtual IP Address

In this section, you will configure a virtual IP address **192.168.20.1** on the Firewall. Creating a virtual IP address allows the Firewall to communicate with multiple IP networks from a single physical interface.

1. Refer to the topology and note there is currently nothing assigned with the IP address **192.168.20.1**.
2. You can confirm you cannot reach **192.168.20.1** by utilizing the *ping* utility. Click on the **Xfce Terminal** icon in the taskbar.



3. In the *Terminal* window, try pinging 192.168.20.1 by typing `ping 192.168.20.1` and pressing **Enter**. To stop the ping, type **Ctrl+C**.



```
Terminal
File Edit View Terminal Tabs Help
C:\home\lab-user> ping 192.168.20.1
PING 192.168.20.1 (192.168.20.1) 56(84) bytes of data.
From 128.109.191.97 icmp_seq=1 Destination Net Unreachable
From 128.109.191.97 icmp_seq=10 Destination Net Unreachable
From 128.109.191.97 icmp_seq=17 Destination Net Unreachable
From 128.109.191.97 icmp_seq=22 Destination Net Unreachable
^C
--- 192.168.20.1 ping statistics ---
23 packets transmitted, 0 received, +4 errors, 100% packet loss, time 22417ms

C:\home\lab-user>
```



Notice, you receive **Destination net unreachable** and possibly **Request timed out**. These responses indicate that the Client cannot reach anyone at that IP address. By default, the Client's default gateway is **192.168.1.1**, which is the Firewall inside interface. The responses come from **203.0.113.1**, which means the Firewall had no routes to the **192.168.20.0** network and forwarded those requests to its default gateway **203.0.113.1**. From this information you can reasonably assume **192.168.20.1**, for this lab environment, does not exist on the network.

4. Type `exit` and press **Enter** to close the command prompt.

5. On the Firewall administration page, navigate to **Network > Interfaces > Ethernet**. Click on **ethernet1/2**.

| INTERFACE | INTERFACE TYPE | MANAGEMENT PROFILE | LINK STATE | IP ADDRESS | VIRTUAL RC |
|-------------|----------------|--------------------|------------|-----------------|------------|
| ethernet1/1 | Layer3 | | | 203.0.113.20/24 | VR-1 |
| ethernet1/2 | Layer3 | allow-mgmt | | 192.168.1.1/24 | VR-1 |
| ethernet1/3 | | | | none | none |
| ethernet1/4 | | | | none | none |
| ethernet1/5 | | | | none | none |
| ethernet1/6 | | | | none | none |
| ethernet1/7 | | | | none | none |
| ethernet1/8 | | | | none | none |
| ethernet1/9 | | | | none | none |

6. First, click on the **IPv4** tab. Then, in the bottom-left of the window, click on the **Add** button. Next, type **192.168.20.1/24** in the *IP address* field, press **Enter**. Finally, click the **OK** button.

Ethernet Interface

Interface Name: ethernet1/2

Comment:

Interface Type: Layer3

Netflow Profile: None

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

Enable SD-WAN

Type: Static PPPoE DHCP Client

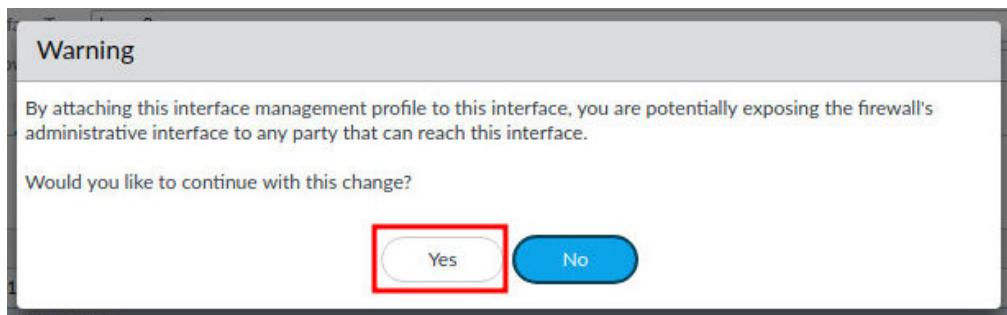
| IP |
|------------------------|
| 192.168.1.1/24 |
| 192.168.20.1/24 |

+ Add **- Delete** **↑ Move Up** **↓ Move Down**

IP address/netmask. Ex. 192.168.2.254/24

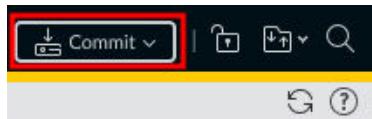
OK **Cancel**

7. In the **Warning** window, click **Yes**.

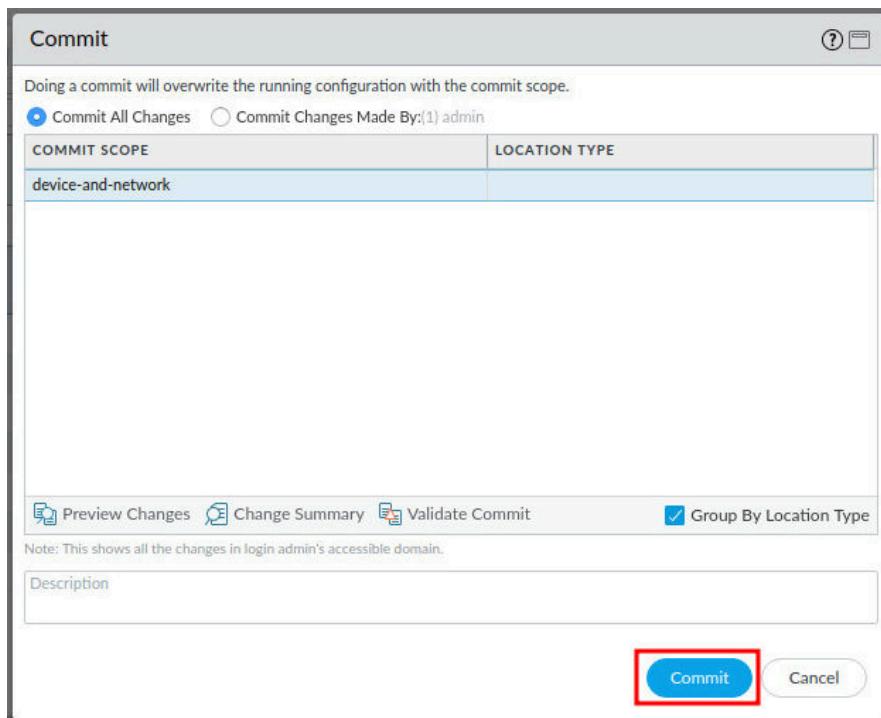


The **Warning** advises that if you attach this interface management profile to this interface, you are potentially exposing the firewall's administrative interface to any party that can reach this interface. For the purpose of this lab, you will bypass this warning knowing that it is not good practice to attach a management profile to a production interface.

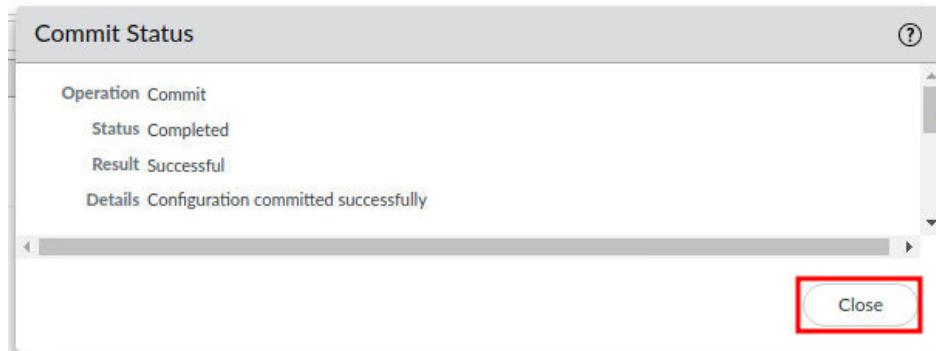
8. Click the **Commit** link located at the top-right of the web interface.



9. In the **Commit** window, click **Commit** to proceed with committing the changes.



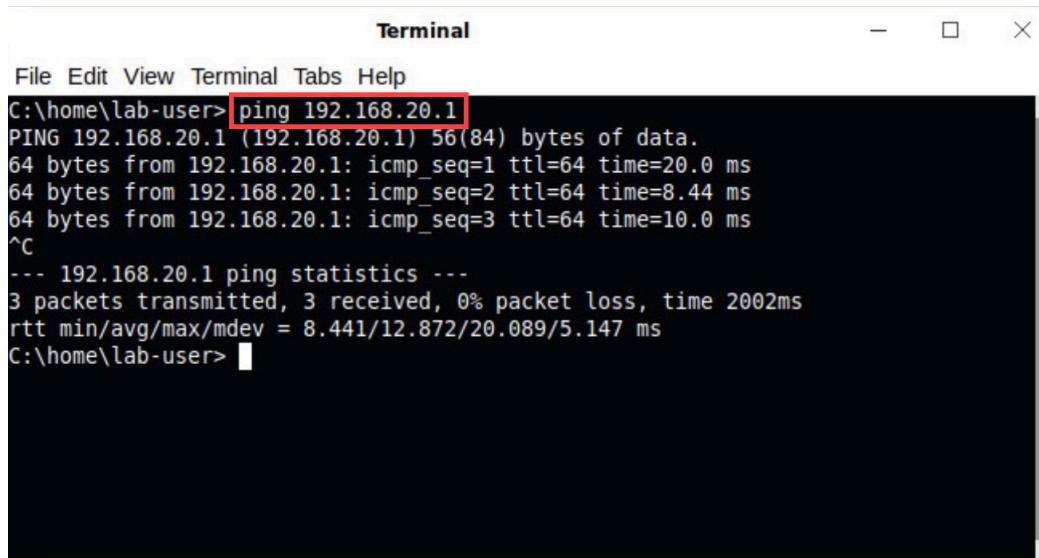
10. When the commit operation successfully completes, click **Close** to continue.



11. Click on the **Xfce Terminal** icon in the taskbar.



12. To confirm the Firewall is configured with IP address 192.168.20.1, type ping 192.168.20.1 and press **Enter**. To stop the ping, click **Ctrl+C**.



```
Terminal
File Edit View Terminal Tabs Help
C:\home\lab-user> ping 192.168.20.1
PING 192.168.20.1 (192.168.20.1) 56(84) bytes of data.
64 bytes from 192.168.20.1: icmp_seq=1 ttl=64 time=20.0 ms
64 bytes from 192.168.20.1: icmp_seq=2 ttl=64 time=8.44 ms
64 bytes from 192.168.20.1: icmp_seq=3 ttl=64 time=10.0 ms
^C
--- 192.168.20.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 8.441/12.872/20.089/5.147 ms
C:\home\lab-user>
```



Notice, you will now receive replies from **192.168.20.1**, the Firewall, even though it is on a different network because it is a virtual network on the Palo Alto interface.

13. Type exit and press **Enter** to close the command prompt.

14. On the Firewall administration page, click on **ethernet1/2**.

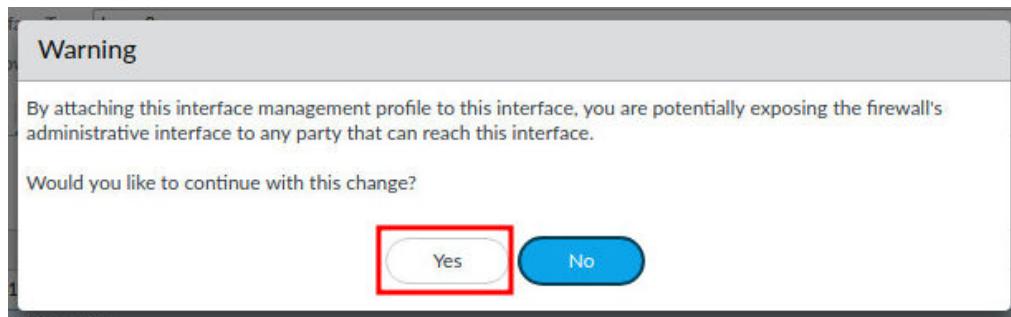
| Ethernet | VLAN | Loopback | Tunnel | SD-WAN |
|-------------|----------------|--------------------|------------|-----------------|
| INTERFACE | INTERFACE TYPE | MANAGEMENT PROFILE | LINK STATE | IP ADDRESS |
| ethernet1/1 | Layer3 | | | 203.0.113.20/24 |
| ethernet1/2 | Layer3 | allow-mgmt | | 192.168.1.1/24 |
| | | | | 192.168.20.1/24 |
| ethernet1/3 | | | | none |
| ethernet1/4 | | | | none |
| ethernet1/5 | | | | none |
| ethernet1/6 | | | | none |
| ethernet1/7 | | | | none |
| ethernet1/8 | | | | none |
| ethernet1/9 | | | | none |

15. Click on the **IPv4** tab. Click on **192.168.20.1/24** to edit the entry. Change to **192.168.20.1/29**. Press **Enter** and click the **OK** button.

Ethernet Interface

| | | | | |
|--|---|-----------------------------|-----------------------------------|----------|
| Interface Name | ethernet1/2 | | | |
| Comment | | | | |
| Interface Type | Layer3 | | | |
| Netflow Profile | None | | | |
| Config | IPv4 | IPv6 | SD-WAN | Advanced |
| <input type="checkbox"/> Enable SD-WAN | | | | |
| Type | <input checked="" type="radio"/> Static | <input type="radio"/> PPPoE | <input type="radio"/> DHCP Client | |
| <input type="checkbox"/> IP | | | | |
| <input type="checkbox"/> 192.168.1.1/24 | | | | |
| <input checked="" type="checkbox"/> 192.168.20.1/29 | | | | |
| <input type="button"/> Add <input type="button"/> Delete <input type="button"/> Move Up <input type="button"/> Move Down | | | | |
| IP address/netmask. Ex. 192.168.2.254/24 | | | | |
| <input type="button"/> OK <input type="button"/> Cancel | | | | |

16. In the *Warning* window, click **Yes**.

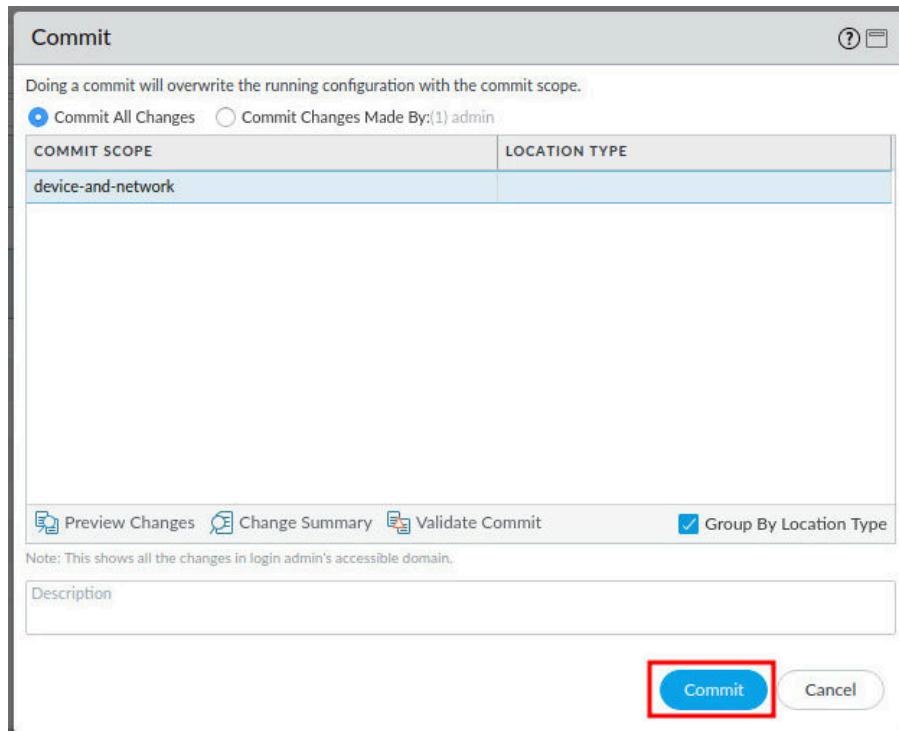


The *Warning* advises that if you attach this interface management profile to this interface, you are potentially exposing the firewall's administrative interface to any party that can reach this interface. For the purpose of this lab, you will bypass this warning knowing that it is not good practice to attach a management profile to a production interface.

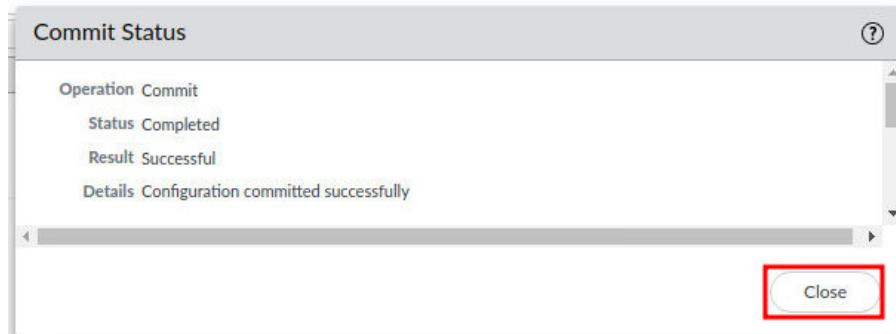
17. Click on the **Commit** link on the top-right of the web interface.



18. In the *Commit* window, click **Commit** to proceed with committing the changes.



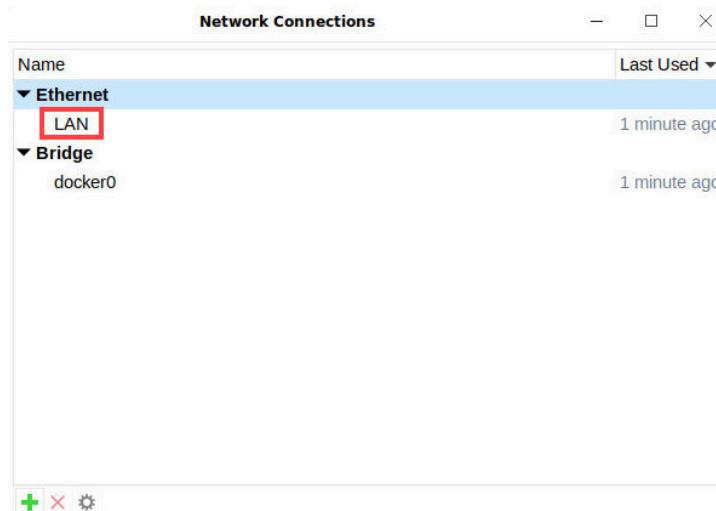
19. When the commit operation successfully completes, click **Close** to continue.



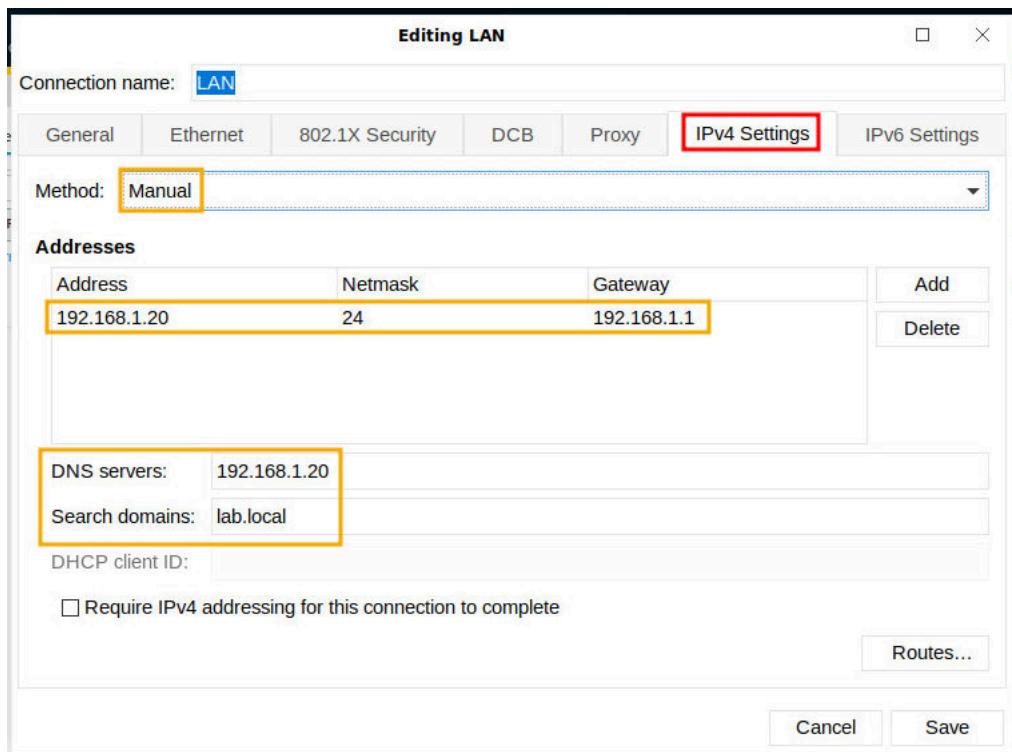
20. Click on the **Connection** icon in the lower-right of the web Client. Next, click on **Edit Connections...**



21. In the *Network Connections* window, double-click **LAN**.



22. In the *Editing LAN* window, click **IPv4 Settings**. Leave the *Editing LAN* window open for the next step.

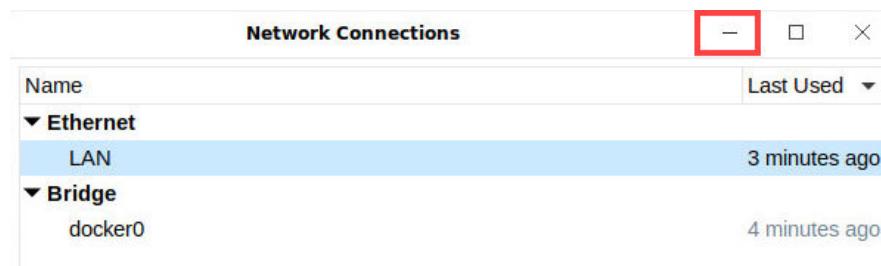


Notice that the method is set to **Manual**. By default, in this lab environment, the Client is configured with a static IP address of **192.168.1.20**, a Netmask of **24** which is **255.255.255.0**, a default gateway of **192.168.1.1**. The DNS server is set to **192.168.1.20** and the search domain is **lab.local**.

23. In the *IP address* field, change it from 192.168.1.20 to 192.168.20.20, and change the *Default Gateway* field to 192.168.20.1. Click the **Save** button to close the *Editing LAN* window.



24. Minimize the *Network Connections* window.



25. Click on the **Xfce Terminal** icon in the taskbar.



26. In the *Terminal* window, type `sudo ip link set ens160 down`. Enter the `PaloAlt0!` password when prompted, and press **Enter**. Leave the *Terminal* window open for the next step.

```
Terminal
File Edit View Terminal Tabs Help
C:\home\lab-user> sudo ip link set ens160 down
[sudo] password for lab-user:
C:\home\lab-user>
```

27. With the *Terminal* window still open, type `sudo ip link set ens160 up` and press **Enter**. Leave the *Terminal* window open for the next step.

```
C:\home\lab-user> sudo ip link set ens160 down
[sudo] password for lab-user:
C:\home\lab-user> sudo ip link set ens160 up
C:\home\lab-user>
```



In the previous two steps, you may need to pause for several seconds to confirm that the link has shut down and come back up. Look for the popups indicating this.



28. To ping the virtual IP address on the Firewall, type `ping 192.168.20.1` and press **Enter**. Give the *Terminal* window approximately 1 minute and stop the ping by clicking **Ctrl+C**.

```
Terminal
File Edit View Terminal Tabs Help
C:\home\lab-user> ping 192.168.20.1
PING 192.168.20.1 (192.168.20.1) 56(84) bytes of data.
^C
--- 192.168.20.1 ping statistics ---
45 packets transmitted, 0 received, 100% packet loss, time 45019ms
C:\home\lab-user>
```



The ping will fail because the Firewall's virtual IP address, **192.168.20.1**, has a network mask of **/29** (255.255.255.248). The **192.168.20.0/29** network can only have an IP range of **192.168.20.1 – 192.168.20.6**, with **192.168.20.0** being the network address, and **192.168.20.7** being the broadcast address. For the ping to succeed, the Client, configured for IP address of **192.168.20.20** does not fall in the IP range.

29. Type **exit** and press **Enter** to close the command prompt.
30. Switch back to the *Editing LAN* window. Click on the **IPv4 tab**. Change the *IP address* from **192.168.20.20** to **192.168.20.6** and change the *Netmask* field from **/24 CIDR** to **/29 CIDR**. Click on the **Save** button to save the change.

Editing LAN

Connection name: **LAN**

General Ethernet 802.1X Security DCB Proxy IPv4 Settings **IPv6 Settings**

Method: **Manual**

Addresses

| Address | Netmask | Gateway | Add | Delete |
|---------------------|-----------|--------------|-----|--------|
| 192.168.20.6 | 29 | 192.168.20.1 | | |

DNS servers: **192.168.1.20**

Search domains: **lab.local**

DHCP client ID:

Require IPv4 addressing for this connection to complete

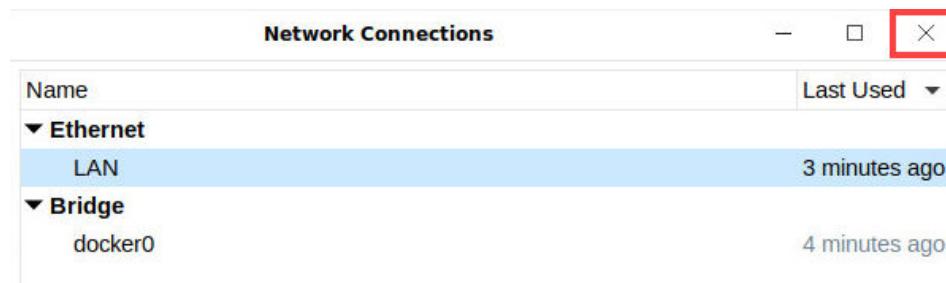
Routes...

Cancel **Save**



Note that CIDR is a condensed representation of an IP address's routing prefix based on subnetting.

31. Click **Close** on the *Network Connections* window.



32. Click on the **Xfce Terminal** icon in the taskbar.



33. In the *Terminal* window, type `sudo ip link set ens160 down`. Enter the `PaloAlt0!` password when prompted, and press **Enter**. Leave the *Terminal* window open for the next step.

```
Terminal
File Edit View Terminal Tabs Help
C:\home\lab-user> sudo ip link set ens160 down
[sudo] password for lab-user:
C:\home\lab-user>
```

34. With the *Terminal* window still open, type `sudo ip link set ens160 up` and press **Enter**. Leave the *Terminal* window open for the next step.

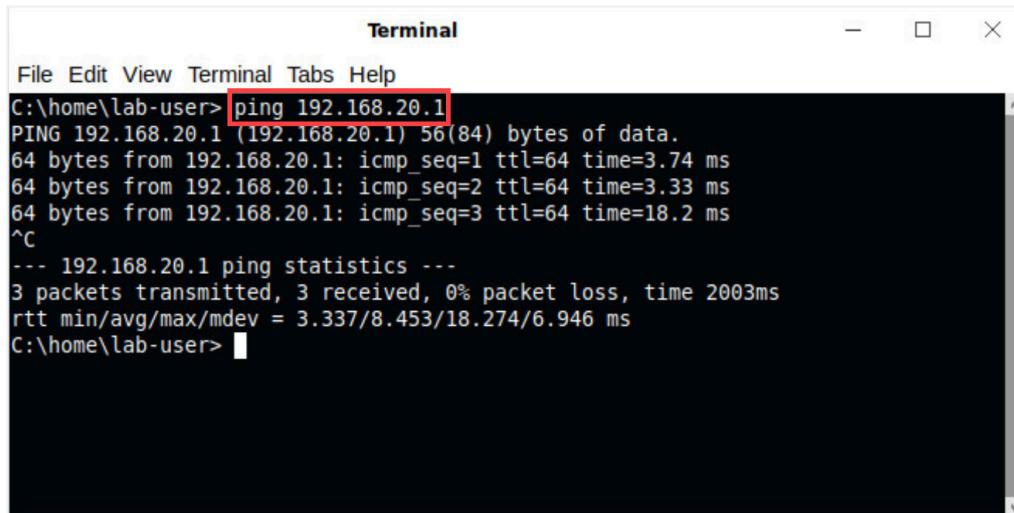
```
C:\home\lab-user> sudo ip link set ens160 down
[sudo] password for lab-user:
C:\home\lab-user> sudo ip link set ens160 up
C:\home\lab-user>
```



In the previous two steps, you may need to pause for several seconds to confirm that the link has shut down and come back up. Look for the popups indicating this.



35. Type `ping 192.168.20.1` and press **Enter**. To stop the ping, press **Ctrl+C**.



A screenshot of a Windows Terminal window titled "Terminal". The window shows the command `ping 192.168.20.1` being typed at the prompt. The output of the ping command is displayed below, showing three successful packets sent to the virtual IP address 192.168.20.1. The terminal window has a standard Windows title bar and a scroll bar on the right side.

```
File Edit View Terminal Tabs Help
C:\home\lab-user> ping 192.168.20.1
PING 192.168.20.1 (192.168.20.1) 56(84) bytes of data.
64 bytes from 192.168.20.1: icmp_seq=1 ttl=64 time=3.74 ms
64 bytes from 192.168.20.1: icmp_seq=2 ttl=64 time=3.33 ms
64 bytes from 192.168.20.1: icmp_seq=3 ttl=64 time=18.2 ms
^C
--- 192.168.20.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 3.337/8.453/18.274/6.946 ms
C:\home\lab-user>
```



The ping will now respond because the Client is in the same network as the Firewall's virtual IP address.

36. The lab is now complete; you may end the reservation.