An assignment report on

PaloAlto Final Assignment

Submitted for fufillment of award of

Internet Communications Technologies

advanced diploma

By
Chance Page
and
Cody Tremblay
26/11/2024

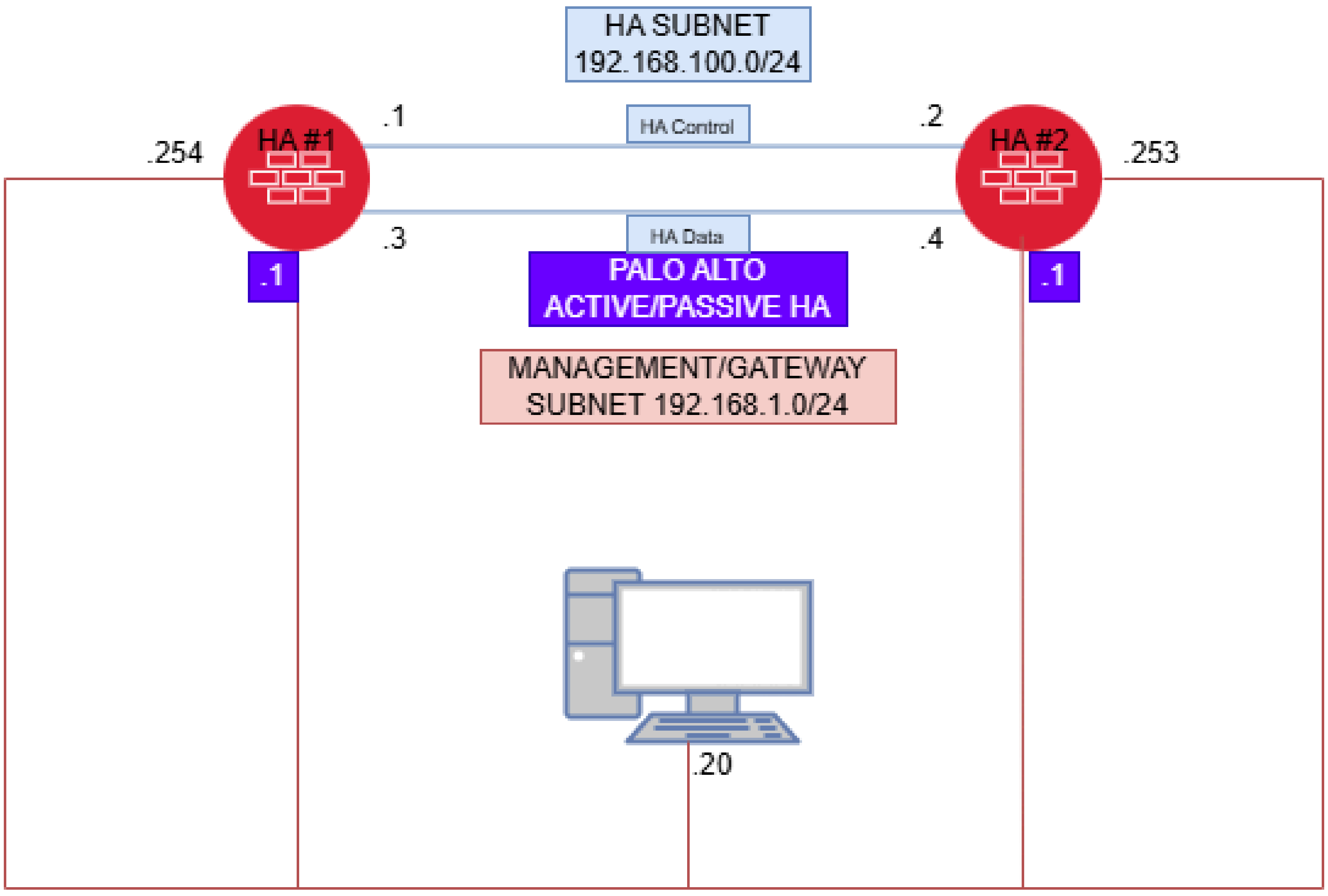
Sheridan College
Faculty of Applied Science & Technology
Professor. Sebastian Maniak
Applied Network Security
TELE33776

Table of Contents

Introduction

High Availability (HA) is a critical feature that addresses issues related to reliability and resilience in a networking environment. It achieves this by adding physical redundancy to the infrastructure, ensuring constant and consistent connectivity in the event of a hardware failure. HA utilizes the fundamentals of the control and data planes to synchronize and manage connectivity within the network, ensuring that all devices maintain secure pathways.

Network Topology



Above is the topology used to simulate the functionality of HA and how it operates. A virtual computer was directly connected to two firewalls configured for high availability. HA #1 was designated (by design) as the primary firewall, while HA #2 is the passive firewall. In this state, HA #1 serves as the firewall the computer communicates with. In the event of a hardware failure or interruption, the connection is switched over to HA #2 to maintain uptime. Two HA links were configured between the firewalls in order implement control and data transmission between the two devices.

Preamble

In this lab, we tested HA failover by pinging the firewall's gateway instead of relying on the firewall propagating traffic through it, to avoid errors and simplify the process. Initially, both firewalls were duplicates of each other because we were using VMware for the simulation. This setup was problematic since the MAC addresses and serial keys needed to be changed, which we did. Instead of having one firewall on one computer's VMware and another firewall on another computer's VMware, we chose to use the same VMware session. This avoided the need to create a VPN link or similar between the two.

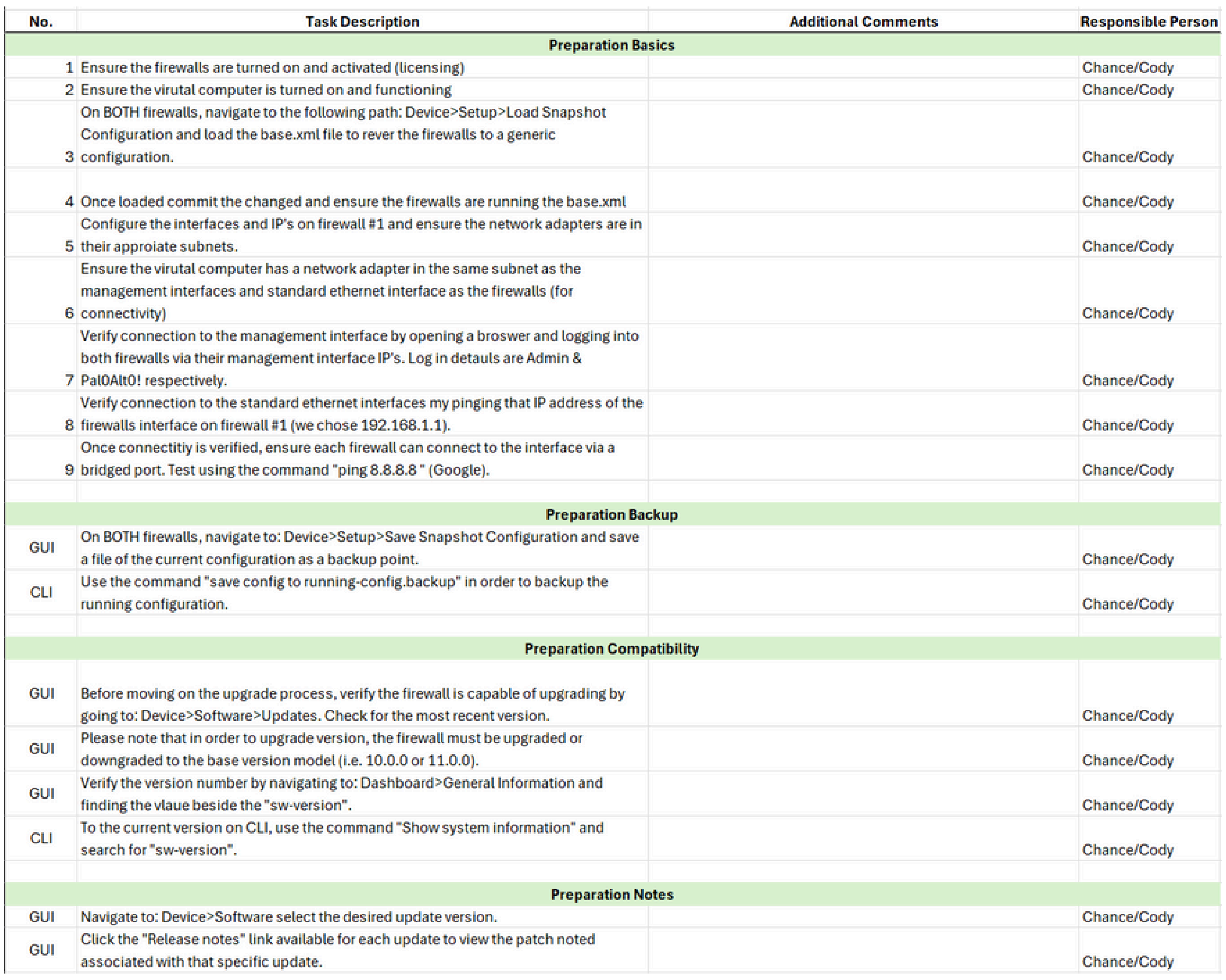
We did not upgrade the firewall to the latest version because it would have required multiple upgrades in sequence. To avoid time constraints, we only upgraded to the next available version.

Challenges

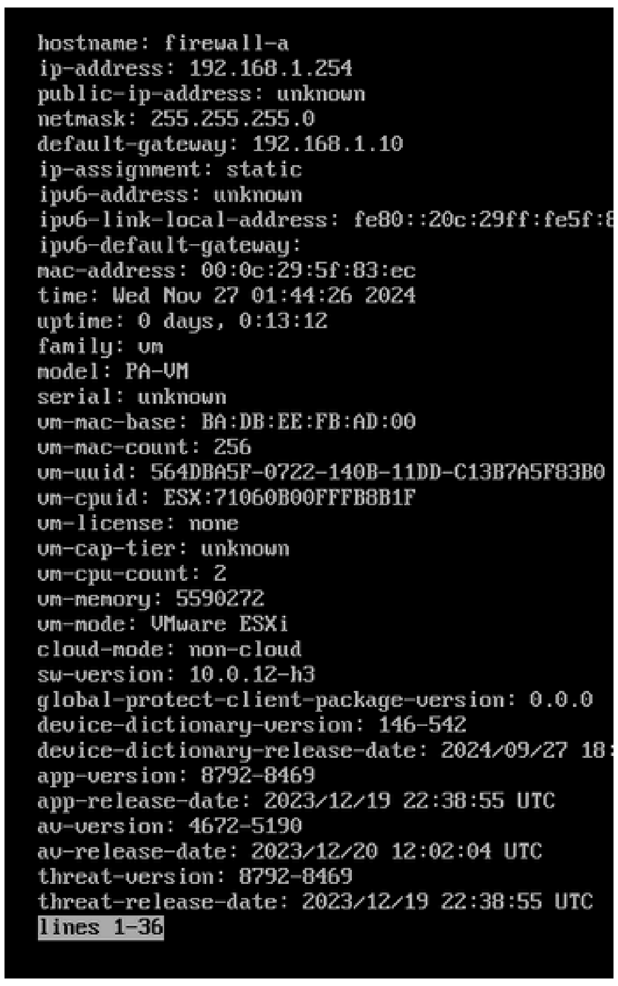
Implementing High Availability (HA) in a network environment presents several challenges. One key issue is ensuring the proper synchronization of configurations, session states, and data across HA pairs. Additionally, HA involves several critical components within its configuration, which, if incorrectly configured or modified, can lead to downtime and failover problems. For instance, during this lab, we encountered issues with MAC resolution related to the direct connection to the virtual computer, as well as control plane connectivity between the firewalls. These issues were traced back to misconfigurations of the network adapters and IP subnet addressing among the devices. Furthermore, it is imperative to define HA prioritization to ensure the active and passive structure aligns with the desired configuration. We observed an issue where the firewalls were not consistently maintaining their statuses, which we determined was due to a lack of proper prioritization during the election process.

Preparation

The preparation for this lab involves the deployment of two firewall units and a virtual computer. During this phase, the user will be guided through the process of directly connecting the virtual computer to both firewall devices. The initial step is to verify the connectivity between the devices to ensure that communication is properly established. Additionally, the user will be instructed to configure a backup point, which serves as a precautionary measure in case of configuration corruption or the need to revert to previous settings. This backup ensures that, in the event of an issue, the user can restore the devices to a known working state, minimizing downtime and preserving network integrity.



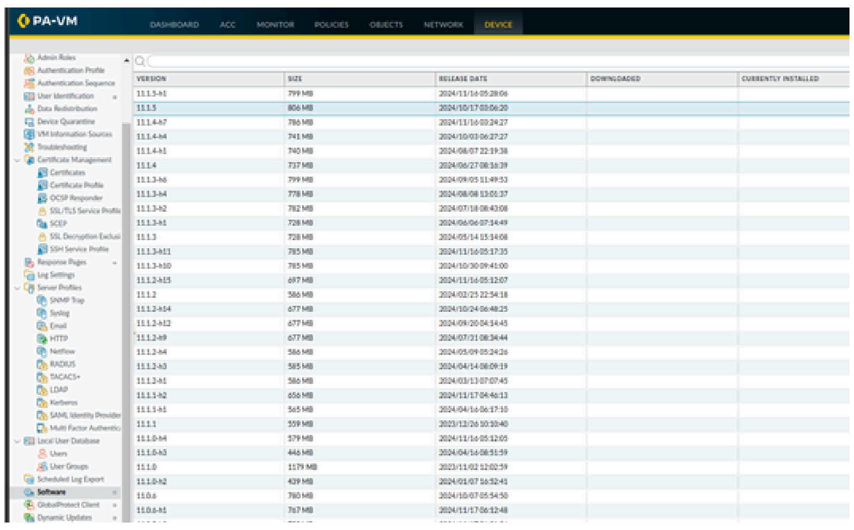
No.	Task Description	Additional Comments	Responsible Person
Preparation Basics			
1	Ensure the firewalls are turned on and activated (licensing)		Chance/Cody
2	Ensure the virutal computer is turned on and functioning		Chance/Cody
3	On BOTH firewalls, navigate to the following path: Device>Setup>Load Snapshot Configuration and load the base.xml file to rever the firewalls to a generic configuration.		Chance/Cody
4	Once loaded commit the changed and ensure the firewalls are running the base.xml		Chance/Cody
5	Configure the interfaces and IP's on firewall #1 and ensure the network adapters are in their approiate subnets.		Chance/Cody
6	Ensure the virutal computer has a network adapter in the same subnet as the management interfaces and standard ethernet interface as the firewalls (for connectivity)		Chance/Cody
7	Verify connection to the management interface by opening a broswer and logging into both firewalls via their management interface IP's. Log in detauls are Admin & Pal0Alt0! respectively.		Chance/Cody
8	Verify connection to the standard ethernet interfaces my pinging that IP address of the firewalls interface on firewall #1 (we chose 192.168.1.1).		Chance/Cody
9	Once connectitiy is verified, ensure each firewall can connect to the interface via a bridged port. Test using the command "ping 8.8.8.8 " (Google).		Chance/Cody
Preparation Backup			
GUI	On BOTH firewalls, navigate to: Device>Setup>Save Snapshot Configuration and save a file of the current configuration as a backup point.		Chance/Cody
CLI	Use the command "save config to running-config.backup" in order to backup the running configuration.		Chance/Cody
Preparation Compatibility			
GUI	Before moving on the upgrade process, verify the firewall is capable of upgrading by going to: Device>Software>Updates. Check for the most recent version.		Chance/Cody
GUI	Please note that in order to upgrade version, the firewall must be upgraded or downgraded to the base version model (i.e. 10.0.0 or 11.0.0).		Chance/Cody
GUI	Verify the version number by navigating to: Dashboard>General Information and finding the vlaue beside the "sw-version".		Chance/Cody
CLI	To the current version on CLI, use the command "Show system information" and search for "sw-version".		Chance/Cody
Preparation Notes			
GUI	Navigate to: Device>Software select the desired update version.		Chance/Cody
GUI	Click the "Release notes" link available for each update to view the patch noted associated with that specific update.		Chance/Cody



```
hostname: firewall-a
ip-address: 192.168.1.254
public-ip-address: unknown
netmask: 255.255.255.0
default-gateway: 192.168.1.10
ip-assignment: static
ipv6-address: unknown
ipv6-link-local-address: fe80::20c:29ff:fe5f:8
ipv6-default-gateway:
mac-address: 00:0c:29:5f:83:ec
time: Wed Nov 27 01:44:26 2024
uptime: 0 days, 0:13:12
family: vm
model: PA-VM
serial: unknown
vm-mac-base: BA:DB:EE:FB:AD:00
vm-mac-count: 256
vm-uuid: 564DBA5F-0722-140B-11DD-C13B7A5F83B0
vm-cpuid: ESX:71060B00FFFB8B1F
vm-license: none
vm-cap-tier: unknown
vm-cpu-count: 2
vm-memory: 5590272
vm-mode: VMware ESXi
cloud-mode: non-cloud
sw-version: 10.0.12-h3
global-protect-client-package-version: 0.0.0
device-dictionary-version: 146-542
device-dictionary-release-date: 2024/09/27 18:
app-version: 8792-8469
app-release-date: 2023/12/19 22:38:55 UTC
av-version: 4672-5190
av-release-date: 2023/12/20 12:02:04 UTC
threat-version: 8792-8469
threat-release-date: 2023/12/19 22:38:55 UTC
lines 1-36
```

CLI

WEB-GUI



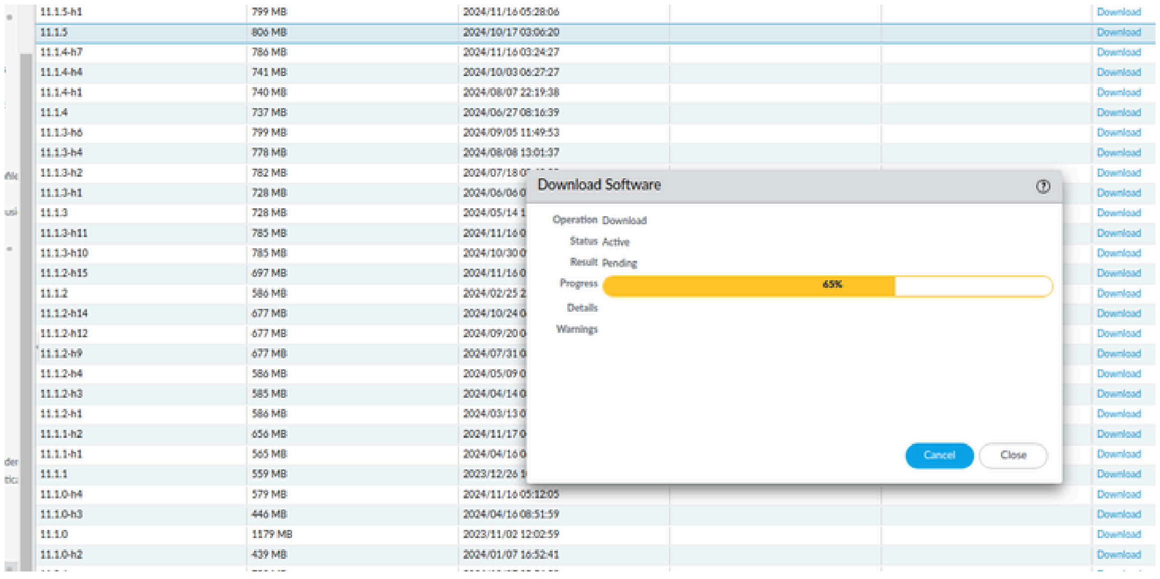
VERSION	SIZE	RELEASE DATE	DOWNLOADED	CURRENTLY INSTALLED
11.1.5-h1	799 MB	2024/11/16 05:28:06		
11.1.5	806 MB	2024/10/17 03:06:20		
11.1.4-h7	786 MB	2024/11/16 03:24:27		
11.1.4-h4	741 MB	2024/10/03 06:27:27		
11.1.4-h1	740 MB	2024/08/07 22:19:38		
11.1.4	737 MB	2024/06/27 08:16:39		
11.1.3-h6	799 MB	2024/09/05 11:49:53		
11.1.3-h4	778 MB	2024/08/08 13:01:37		
11.1.3-h2	782 MB	2024/07/18 08:43:08		
11.1.3-h1	728 MB	2024/06/06 07:14:49		
11.1.3	728 MB	2024/05/14 15:14:08		
11.1.3-h11	785 MB	2024/11/16 05:17:35		
11.1.3-h10	785 MB	2024/10/30 09:41:00		
11.1.2-h15	697 MB	2024/11/16 05:12:07		
11.1.2	586 MB	2024/02/25 22:54:18		
11.1.2-h14	677 MB	2024/10/24 06:48:25		
11.1.2-h12	677 MB	2024/09/20 04:14:45		
11.1.2-h9	677 MB	2024/07/31 08:34:44		
11.1.2-h4	586 MB	2024/05/09 05:24:26		
11.1.2-h3	585 MB	2024/04/14 08:09:19		
11.1.2-h1	586 MB	2024/03/13 07:07:45		
11.1.1-h2	656 MB	2024/11/17 04:46:13		
11.1.1-h1	565 MB	2024/04/16 06:17:10		
11.1.1	559 MB	2023/12/26 10:10:40		
11.1.0-h4	579 MB	2024/11/16 05:12:05		
11.1.0-h3	446 MB	2024/04/16 08:51:59		
11.1.0	1179 MB	2023/11/02 12:02:59		
11.1.0-h2	429 MB	2024/01/07 16:52:41		
11.0.6	780 MB	2024/10/07 05:54:50		
11.0.6-h1	767 MB	2024/11/17 06:12:48		

Upgrade Process

This process outlines the steps for downloading, installing, and verifying an upgraded version of the Palo Alto firewall software (PAN-OS) using the Web-GUI. It begins by checking the current PAN-OS version and downloading the latest compatible firmware from the Palo Alto Networks support portal. The user then uploads the software image to the firewall, initiates the upgrade, and applies the new version, which typically requires a reboot of the firewall. After the upgrade, it is crucial to verify that the new PAN-OS version has been applied correctly, ensuring all firewall services are functioning as expected.

No.	Task Description	Additional Comments	Responsible Person
	Upgrade Process Download		
GUI	On BOTH firewalls, navigate to: Device>Software and select the load recent version in the bottom left corner.		Chance/Cody
GUI	Once loaded Select the version that is closest to the top of the software running list.		Chance/Cody
GUI	Find the download link to the right of the version that is desired and ensure it completes the process.		Chance/Cody
	Upgrade Process Installation		
GUI	Once the download is complete, find and selec the "install" button to the right of the version that was downloaded.		Chance/Cody
GUI	Verify the installation process completes.		Chance/Cody
GUI	Please note that if you receive an installation error, verify that the base upgrade version is installed first. For example, if you are trying to upgrade to 11.13.0 you will need to installed 11.0.0 first.		Chance/Cody
	Upgrade Process Reboot		
GUI	Once the installation completed on the Web-GUI, you will be prompted to restart the deivce.		Chance/Cody
GUI	Before restarting, ensure that no device on the network require connectivity and all user are aware of the downtime.		Chance/Cody
GUI	Additionallty, ensure the firewall is not processing any other tasks before rebooting by checking the "task manager" in the bottom right corner.		Chance/Cody

The Download Process

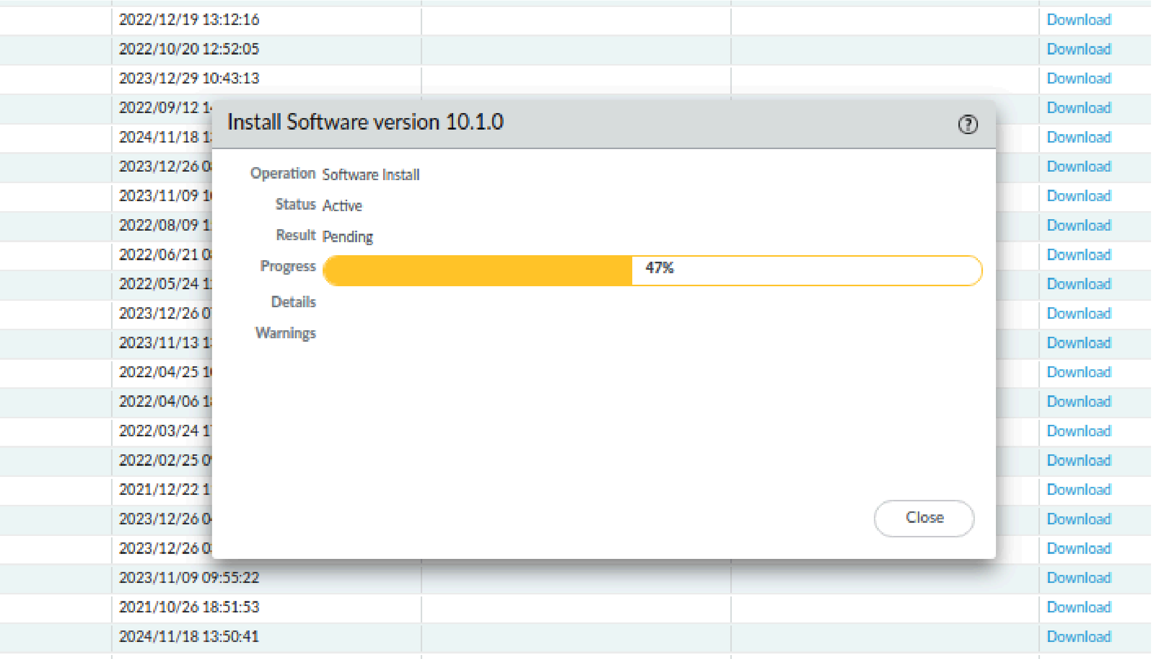


11.1.5-h1	799 MB	2024/11/16 05:28:06	Download
11.1.5	806 MB	2024/10/17 03:06:20	Download
11.1.4-h7	786 MB	2024/11/16 03:24:27	Download
11.1.4-h4	741 MB	2024/10/03 06:27:27	Download
11.1.4-h1	740 MB	2024/08/07 22:19:38	Download
11.1.4	737 MB	2024/06/27 08:16:39	Download
11.1.3-h6	799 MB	2024/09/05 11:49:53	Download
11.1.3-h4	778 MB	2024/08/08 13:01:37	Download
11.1.3-h2	782 MB	2024/07/18 0	Download
11.1.3-h1	728 MB	2024/06/06 0	Download
11.1.3	728 MB	2024/05/14 1	Download
11.1.3-h11	785 MB	2024/11/16 0	Download
11.1.3-h10	785 MB	2024/10/30 0	Download
11.1.2-h15	697 MB	2024/11/16 0	Download
11.1.2	586 MB	2024/02/25 2	Download
11.1.2-h14	677 MB	2024/10/24 0	Download
11.1.2-h12	677 MB	2024/09/20 0	Download
11.1.2-h9	677 MB	2024/07/31 0	Download
11.1.2-h4	586 MB	2024/05/09 0	Download
11.1.2-h3	585 MB	2024/04/14 0	Download
11.1.2-h1	586 MB	2024/03/13 0	Download
11.1.1-h2	656 MB	2024/11/17 0	Download
11.1.1-h1	565 MB	2024/04/16 0	Download
11.1.1	559 MB	2023/12/26 1	Download
11.1.0-h4	579 MB	2024/11/16 05:12:05	Download
11.1.0-h3	446 MB	2024/04/16 08:51:59	Download
11.1.0	1179 MB	2023/11/02 12:02:59	Download
11.1.0-h2	439 MB	2024/01/07 16:52:41	Download

Download Software

Operation Download
Status Active
Result Pending
Progress 65%
Details
Warnings

The Installation Process



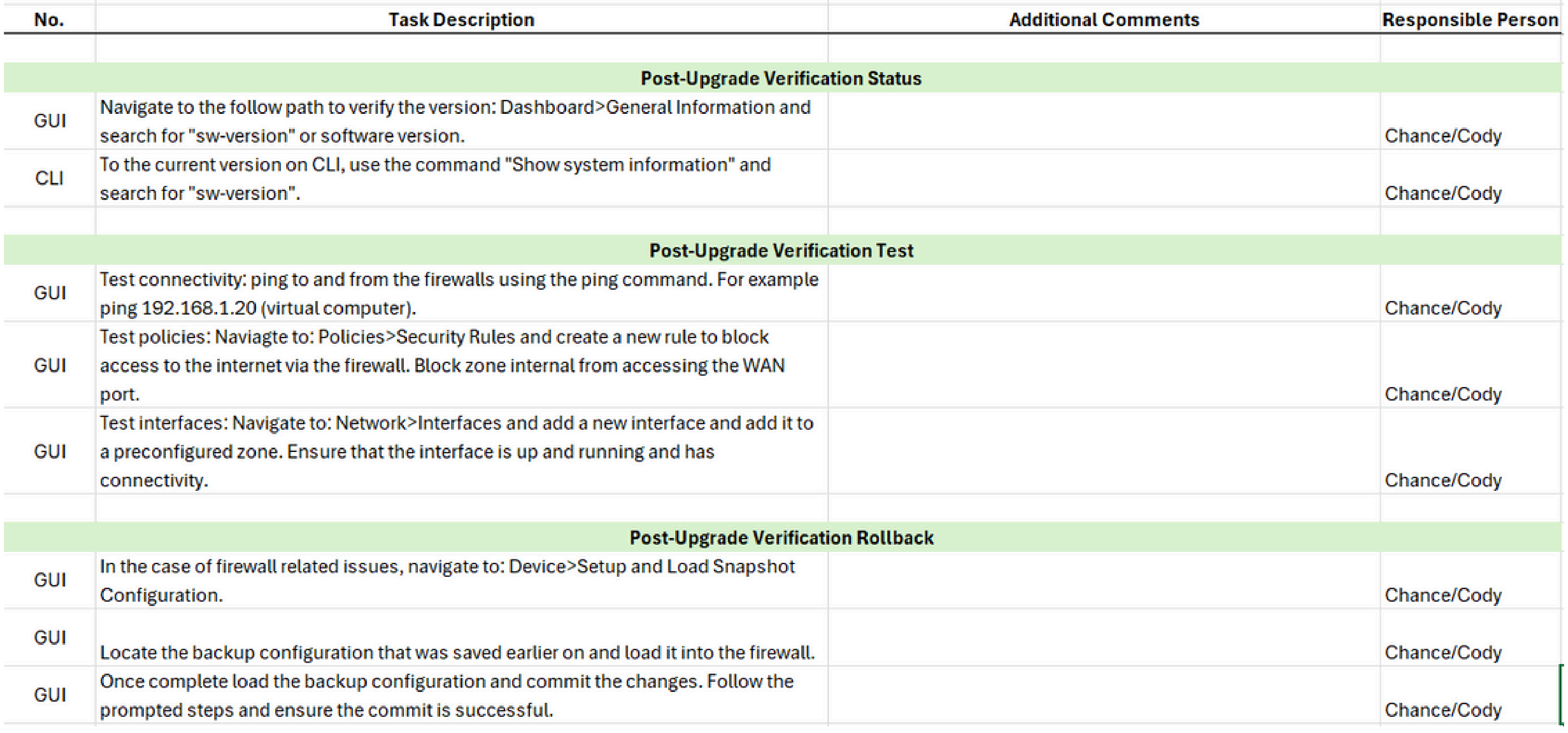
2022/12/19 13:12:16	Download
2022/10/20 12:52:05	Download
2023/12/29 10:43:13	Download
2022/09/12 1	Download
2024/11/18 1	Download
2023/12/26 0	Download
2023/11/09 1	Download
2022/08/09 1	Download
2022/06/21 0	Download
2022/05/24 1	Download
2023/12/26 0	Download
2023/11/13 1	Download
2022/04/25 1	Download
2022/04/06 1	Download
2022/03/24 1	Download
2022/02/25 0	Download
2021/12/22 1	Download
2023/12/26 0	Download
2023/12/26 0	Download
2023/11/09 09:55:22	Download
2021/10/26 18:51:53	Download
2024/11/18 13:50:41	Download

Install Software version 10.1.0

Operation Software Install
Status Active
Result Pending
Progress 47%
Details
Warnings

Post-Upgrade

This process provides a comprehensive approach to verifying and testing a Palo Alto firewall after a software upgrade. Post-upgrade verification begins by confirming the current software version through both the graphical user interface (GUI) and command-line interface (CLI). The next steps involve testing the firewall's functionality, including checking network connectivity, verifying security policies by testing access controls, and ensuring proper operation of network interfaces. If issues are detected, the procedure includes rolling back to a previously saved configuration, restoring the firewall to its prior state, and committing the changes to ensure the system is functioning correctly. This ensures that the firewall operates as expected after the upgrade and allows for a quick recovery in case of any issues.



No.	Task Description	Additional Comments	Responsible Person
	Post-Upgrade Verification Status		
GUI	Navigate to the follow path to verify the version: Dashboard>General Information and search for "sw-version" or software version.		Chance/Cody
CLI	To the current version on CLI, use the command "Show system information" and search for "sw-version".		Chance/Cody
	Post-Upgrade Verification Test		
GUI	Test connectivity: ping to and from the firewalls using the ping command. For example ping 192.168.1.20 (virtual computer).		Chance/Cody
GUI	Test policies: Naviagte to: Policies>Security Rules and create a new rule to block access to the internet via the firewall. Block zone internal from accessing the WAN port.		Chance/Cody
GUI	Test interfaces: Navigate to: Network>Interfaces and add a new interface and add it to a preconfigured zone. Ensure that the interface is up and running and has connectivity.		Chance/Cody
	Post-Upgrade Verification Rollback		
GUI	In the case of firewall related issues, navigate to: Device>Setup and Load Snapshot Configuration.		Chance/Cody
GUI	Locate the backup configuration that was saved earlier on and load it into the firewall.		Chance/Cody
GUI	Once complete load the backup configuration and commit the changes. Follow the prompted steps and ensure the commit is successful.		Chance/Cody

Overview of HA

High availability (HA) is a critical concept in networking, ensuring that services remain accessible even in the event of hardware or software failures. It applies to various network devices, including servers, firewalls, and other infrastructure components. Essentially, HA provides a backup system to take over when the primary device fails.

For example, consider a web server setup where you have two web servers. Traffic can either be balanced between the two servers, or one server can act as a backup, ready to take over if the primary server fails. This automatic switch ensures continuous service delivery.

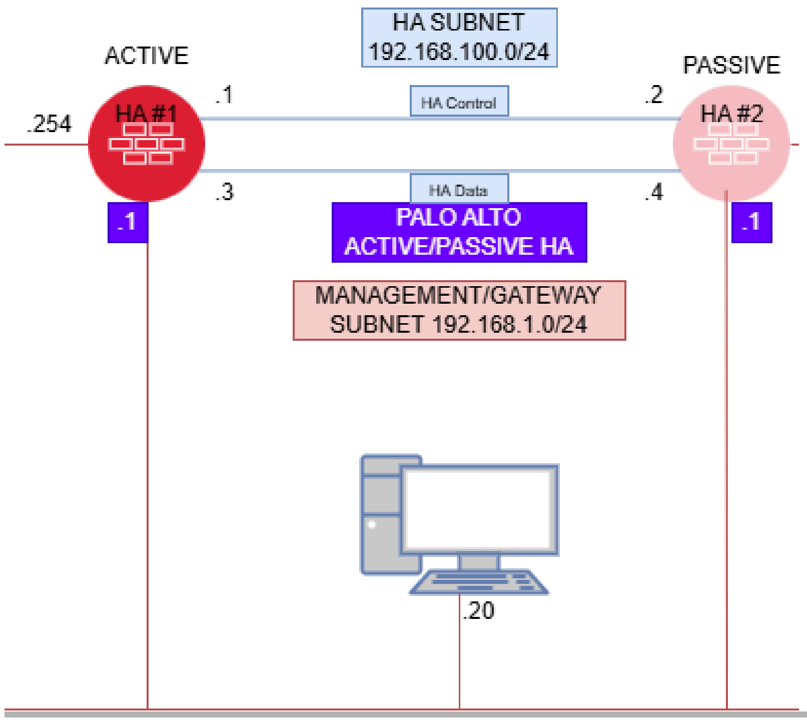
This concept is also applicable to our Palo Alto Firewalls. Palo Alto supports two HA modes:

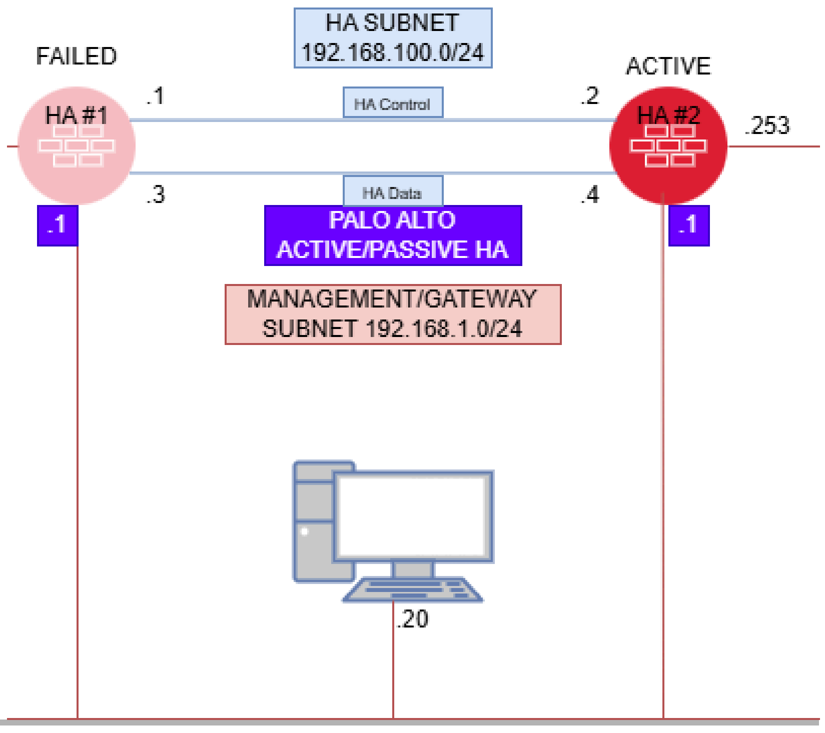
- Active/Passive: In this mode, one firewall is actively handling traffic while the other is on standby, ready to take over if the active firewall fails. This setup ensures that there is always a backup available without splitting the load.

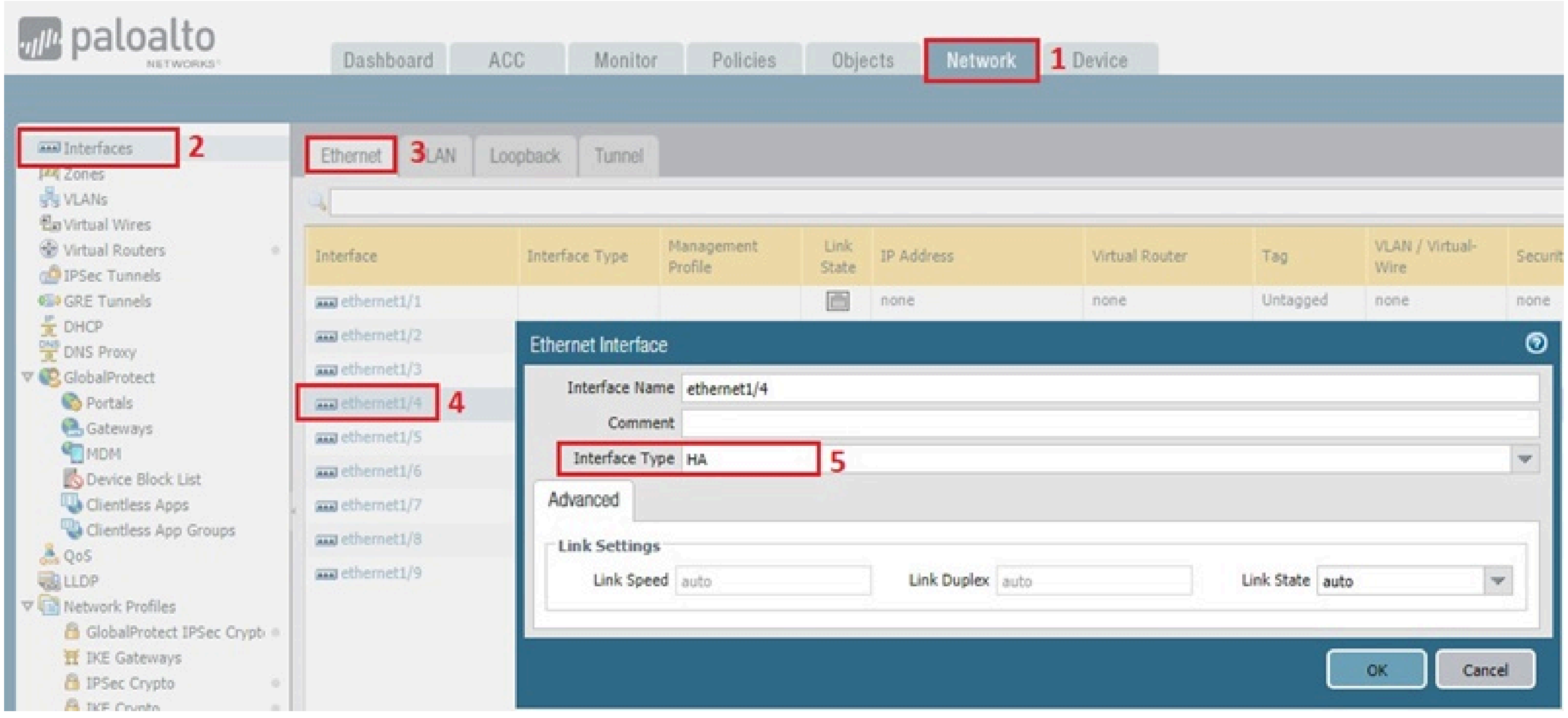
- Active/Active: Both firewalls are active and share the load, providing redundancy and load balancing. If one firewall fails, the other seamlessly continues to handle the traffic.

The firewall detects a failure of the other one when either the link goes down or a heartbeat ping is not successful consecutively. Then, the passive firewall will kick in and start delivering traffic.

Below are 2 diagrams of how 2 firewalls will switch over, the active one will fail and the passive one will turn active.







Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Securit
ethernet1/1				none	none	Untagged	none	none
ethernet1/2								
ethernet1/3								
ethernet1/4								
ethernet1/5								
ethernet1/6								
ethernet1/7								
ethernet1/8								
ethernet1/9								

Ethernet Interface

Interface Name: ethernet1/4

Comment:

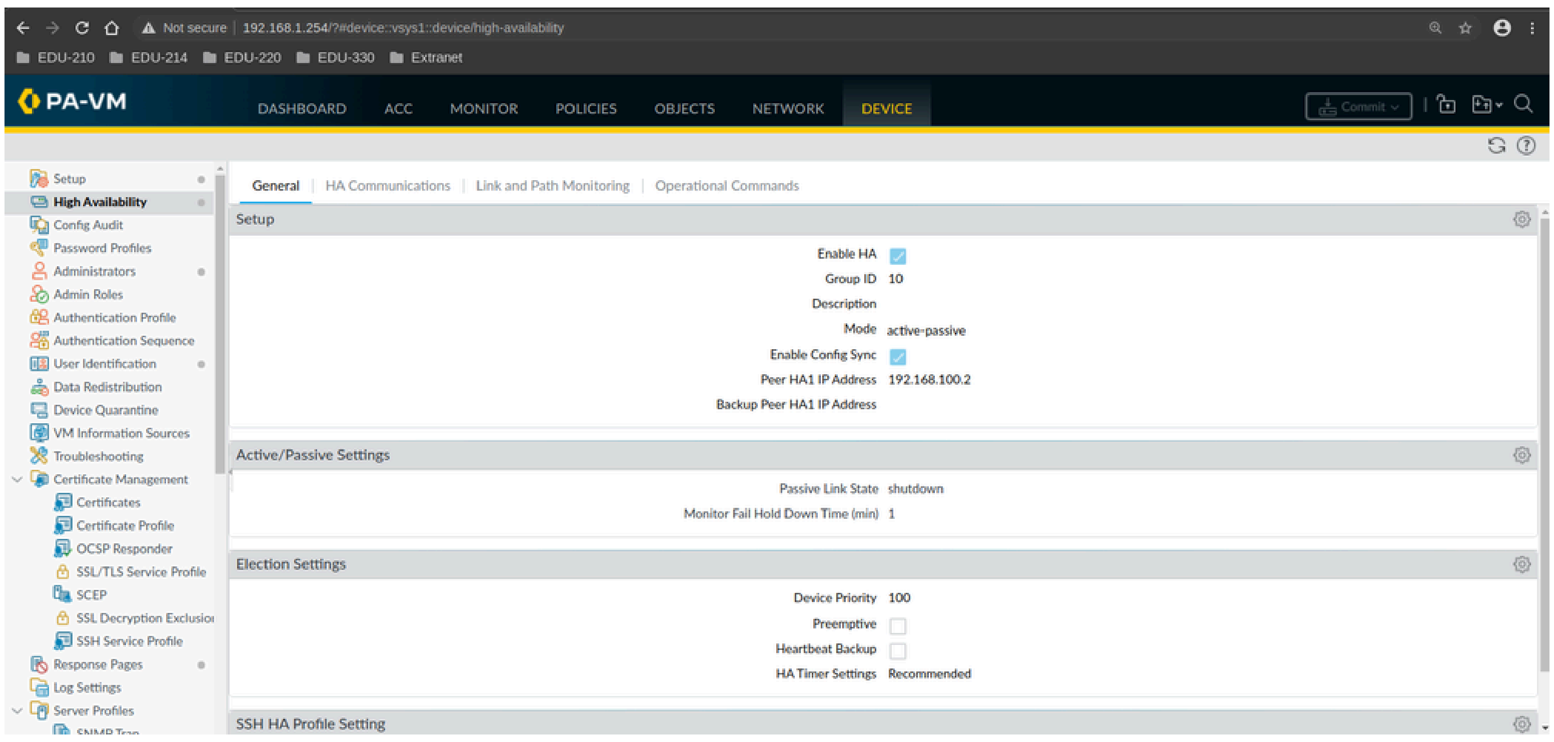
Interface Type: HA

Link Settings

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

"First, you will need to enable two interfaces on your firewall to be of interface type HA. One will be for data, and the other for control links. This is crucial for HA to work. You will need to do this on both firewalls. Most Palo Alto firewalls actually have dedicated HA interfaces, so this step may not be necessary.

Configuring HA#1



Setup

Enable HA ☑
Group ID 10
Description
Mode active-passive
Enable Config Sync ☑
Peer HA1 IP Address 192.168.100.2
Backup Peer HA1 IP Address

Active/Passive Settings

Passive Link State shutdown
Monitor Fail Hold Down Time (min) 1

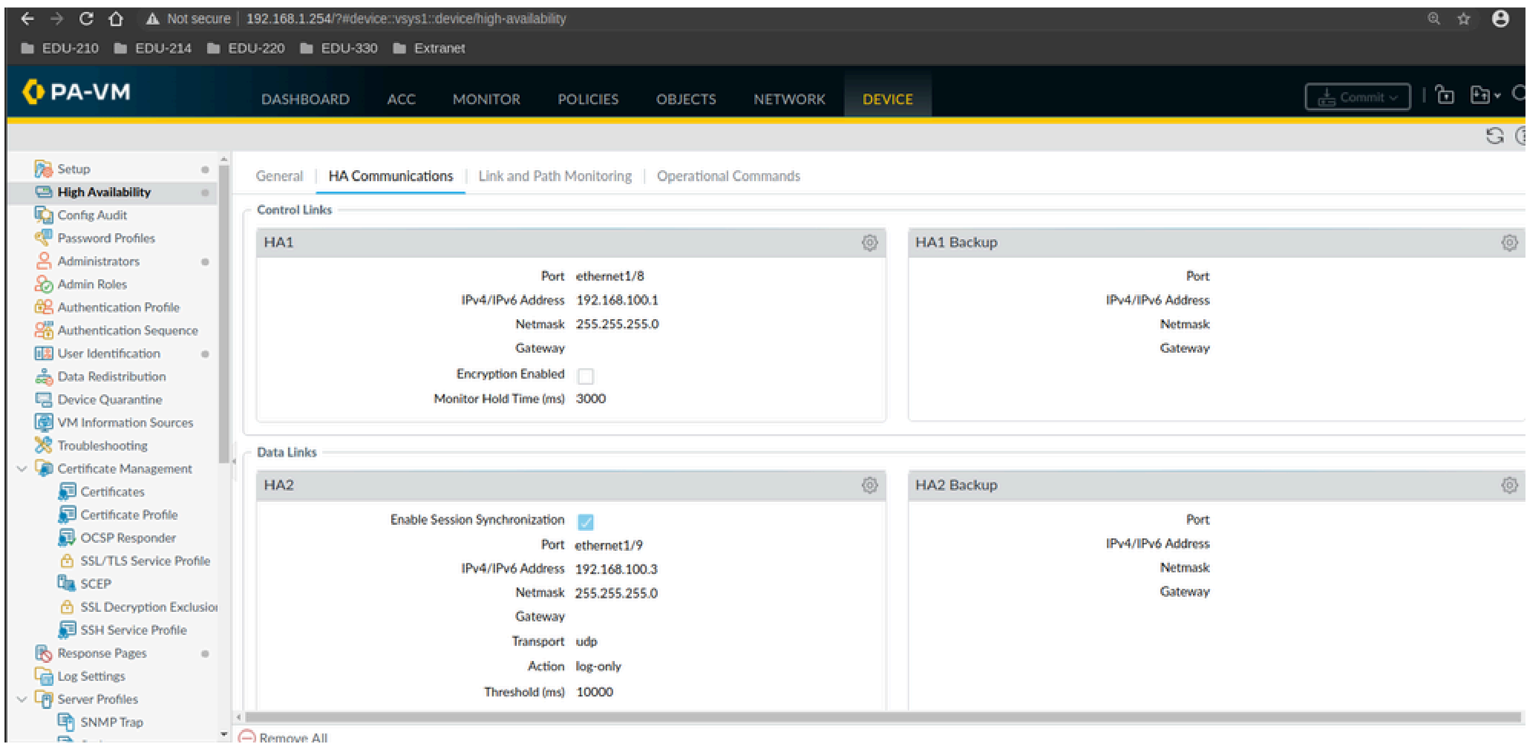
Election Settings

Device Priority 100
Preemptive □
Heartbeat Backup □
HA Timer Settings Recommended

SSH HA Profile Setting

Configuring Palo Alto Firewall HA#1

- Go to Device and select High Availability.
- Enable High Availability (HA).
- Choose an ID for the HA group.
- Enter the peer IP address of the passive Palo Alto firewall.
- Adjust the priority—a higher priority means that HA will be active.
- Set the mode to Active/Passive.



Control Links

HA1

Port ethernet1/8
IPv4/IPv6 Address 192.168.100.1
Netmask 255.255.255.0
Gateway
Encryption Enabled □
Monitor Hold Time (ms) 3000

HA1 Backup

Port
IPv4/IPv6 Address
Netmask
Gateway

Data Links

HA2

Enable Session Synchronization ☑
Port ethernet1/9
IPv4/IPv6 Address 192.168.100.3
Netmask 255.255.255.0
Gateway
Transport udp
Action log-only
Threshold (ms) 10000

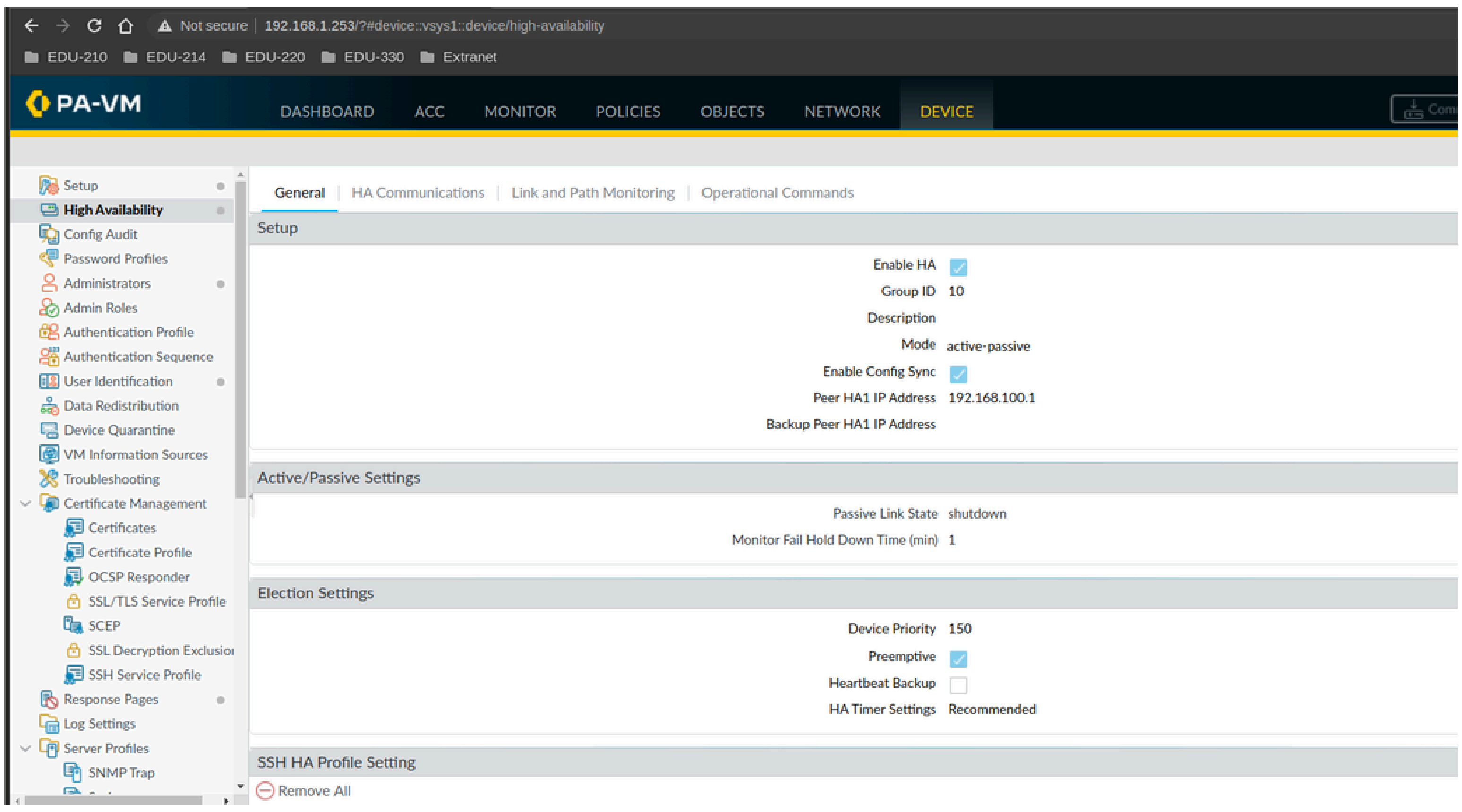
HA2 Backup

Port
IPv4/IPv6 Address
Netmask
Gateway

Configuring Palo Alto HA#1 - Communications Tab

- Choose the interfaces that connect the Palo Alto firewalls to each other.
- Ensure the communication subnet is the same for both data and control links. You can use separate subnets if preferred, but it’s not mandatory.
- Ensure the control link is connected to the control link on the other firewall.
- Ensure the data link is connected to the data link on the other firewall.

Configuring HA#2



Setup

Enable HA ☑
Group ID 10
Description
Mode active-passive
Enable Config Sync ☑
Peer HA1 IP Address 192.168.100.1
Backup Peer HA1 IP Address

Active/Passive Settings

Passive Link State shutdown
Monitor Fail Hold Down Time (min) 1

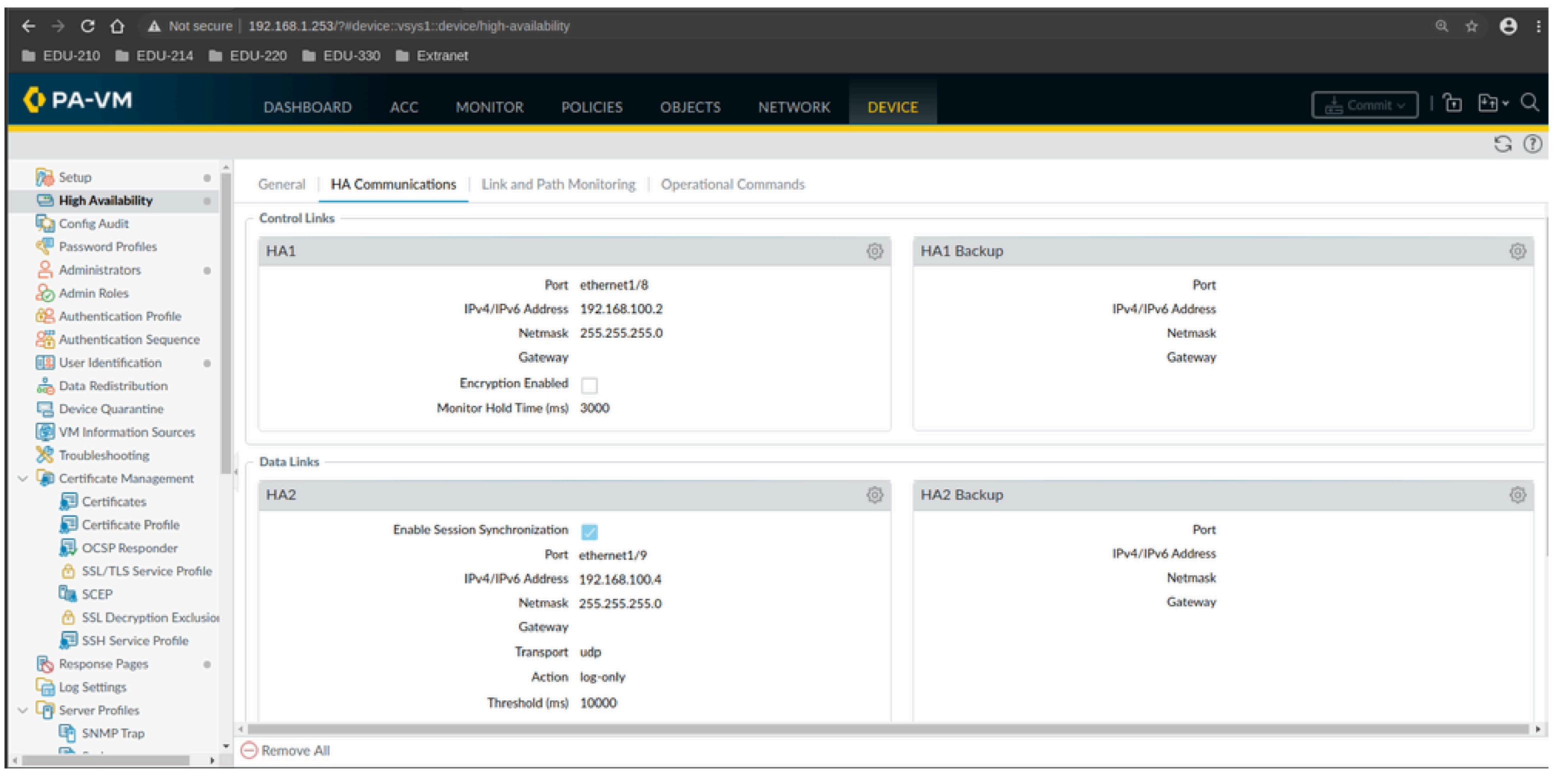
Election Settings

Device Priority 150
Preemptive ☑
Heartbeat Backup □
HA Timer Settings Recommended

SSH HA Profile Setting

Configuring Palo Alto Firewall HA#2

- Go to Device and select High Availability.
- Enable High Availability (HA).
- Choose an ID for the HA group.
- Enter the peer IP address of the primary Palo Alto firewall.
- Adjust the priority—a higher priority means that HA will be active.
- Set the mode to Active/Passive.



Control Links

HA1

Port ethernet1/8
IPv4/IPv6 Address 192.168.100.2
Netmask 255.255.255.0
Gateway
Encryption Enabled □
Monitor Hold Time (ms) 3000

HA1 Backup

Port
IPv4/IPv6 Address
Netmask
Gateway

Data Links

HA2

Enable Session Synchronization ☑
Port ethernet1/9
IPv4/IPv6 Address 192.168.100.4
Netmask 255.255.255.0
Gateway
Transport udp
Action log-only
Threshold (ms) 10000

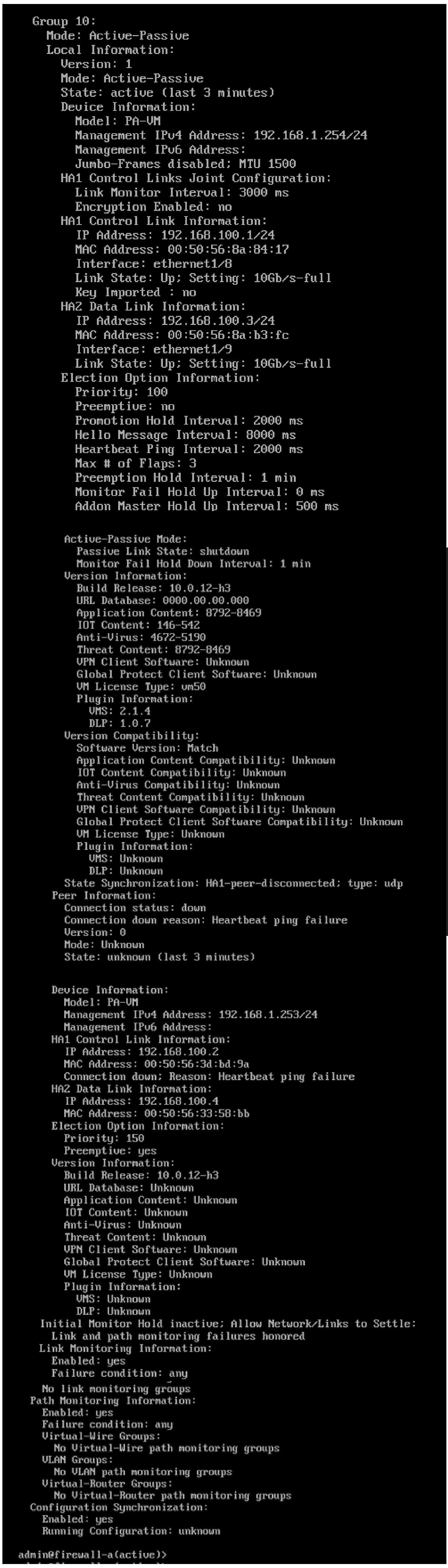
HA2 Backup

Port
IPv4/IPv6 Address
Netmask
Gateway

Configuring Palo Alto HA#1 - Communications Tab

- Choose the interfaces that connect the Palo Alto firewalls to each other.
- Ensure the communication subnet is the same for both data and control links. You can use separate subnets if preferred, but it’s not mandatory.
- Ensure the control link is connected to the control link on the other firewall.
- Ensure the data link is connected to the data link on the other firewall.

Verify HA

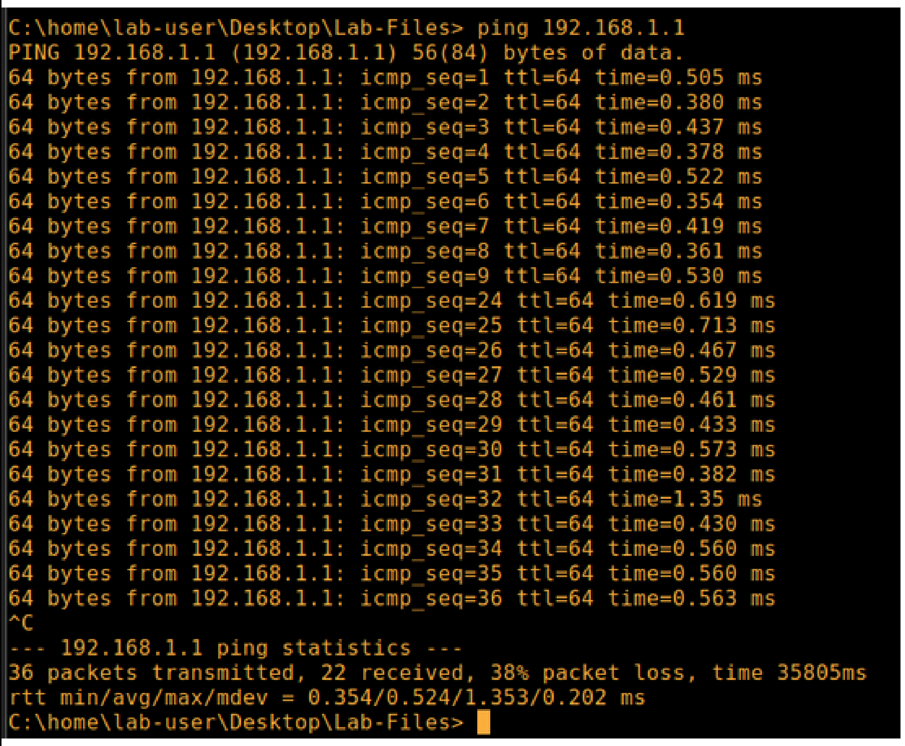


```
Group 10:
  Mode: Active-Passive
  Local Information:
    Version: 1
    Mode: Active-Passive
    State: active (last 3 minutes)
    Device Information:
      Model: PA-VM
      Management IPv4 Address: 192.168.1.254/24
      Management IPv6 Address:
      Jumbo-Frames disabled; MTU 1500
    HA1 Control Links Joint Configuration:
      Link Monitor Interval: 3000 ms
      Encryption Enabled: no
    HA1 Control Link Information:
      IP Address: 192.168.100.1/24
      MAC Address: 00:50:56:8a:84:17
      Interface: ethernet1/8
      Link State: Up; Setting: 10Gb/s-full
      Key Imported : no
    HA2 Data Link Information:
      IP Address: 192.168.100.3/24
      MAC Address: 00:50:56:8a:b3:fc
      Interface: ethernet1/9
      Link State: Up; Setting: 10Gb/s-full
    Election Option Information:
      Priority: 100
      Preemptive: no
      Promotion Hold Interval: 2000 ms
      Hello Message Interval: 8000 ms
      Heartbeat Ping Interval: 2000 ms
      Max # of Flaps: 3
      Preemption Hold Interval: 1 min
      Monitor Fail Hold Up Interval: 0 ms
      Addon Master Hold Up Interval: 500 ms

    Active-Passive Mode:
      Passive Link State: shutdown
      Monitor Fail Hold Down Interval: 1 min
    Version Information:
      Build Release: 10.0.12-h3
      URL Database: 0000.00.00.000
      Application Content: 8792-8469
      IOT Content: 146-542
      Anti-Virus: 4672-5190
      Threat Content: 8792-8469
      VPN Client Software: Unknown
      Global Protect Client Software: Unknown
      VM License Type: vm50
      Plugin Information:
        VMS: 2.1.4
        DLP: 1.0.7
    Version Compatibility:
      Software Version: Match
      Application Content Compatibility: Unknown
      IOT Content Compatibility: Unknown
      Anti-Virus Compatibility: Unknown
      Threat Content Compatibility: Unknown
      VPN Client Software Compatibility: Unknown
      Global Protect Client Software Compatibility: Unknown
      VM License Type: Unknown
      Plugin Information:
        VMS: Unknown
        DLP: Unknown
    State Synchronization: HA1-peer-disconnected; type: udp
  Peer Information:
    Connection status: down
    Connection down reason: Heartbeat ping failure
    Version: 0
    Mode: Unknown
    State: unknown (last 3 minutes)


  Device Information:
    Model: PA-VM
    Management IPv4 Address: 192.168.1.253/24
    Management IPv6 Address:
  HA1 Control Link Information:
    IP Address: 192.168.100.2
    MAC Address: 00:50:56:3d:bd:9a
    Connection down; Reason: Heartbeat ping failure
  HA2 Data Link Information:
    IP Address: 192.168.100.4
    MAC Address: 00:50:56:33:58:bb
  Election Option Information:
    Priority: 150
    Preemptive: yes
  Version Information:
    Build Release: 10.0.12-h3
    URL Database: Unknown
    Application Content: Unknown
    IOT Content: Unknown
    Anti-Virus: Unknown
    Threat Content: Unknown
    VPN Client Software: Unknown
    Global Protect Client Software: Unknown
    VM License Type: Unknown
    Plugin Information:
      VMS: Unknown
      DLP: Unknown
 Initial Monitor Hold inactive; Allow Network/Links to Settle:
   Link and path monitoring failures honored
 Link Monitoring Information:
   Enabled: yes
   Failure condition: any
  No link monitoring groups
Path Monitoring Information:
  Enabled: yes
  Failure condition: any
  Virtual-Wire Groups:
    No Virtual-Wire path monitoring groups
  VLAN Groups:
    No VLAN path monitoring groups
  Virtual-Router Groups:
    No Virtual-Router path monitoring groups
Configuration Synchronization:
  Enabled: yes
  Running Configuration: unknown

admin@firewall-a(active)>
```

Verifying High Availability Connection:

To verify that the HA is properly connected, you can use the following command:

show running-config high-availability
As shown in the screenshot on the **left**, the state is active. The passive link is currently shutdown because it is not active yet. The primary firewall would need to be shut down for the passive link to become active.



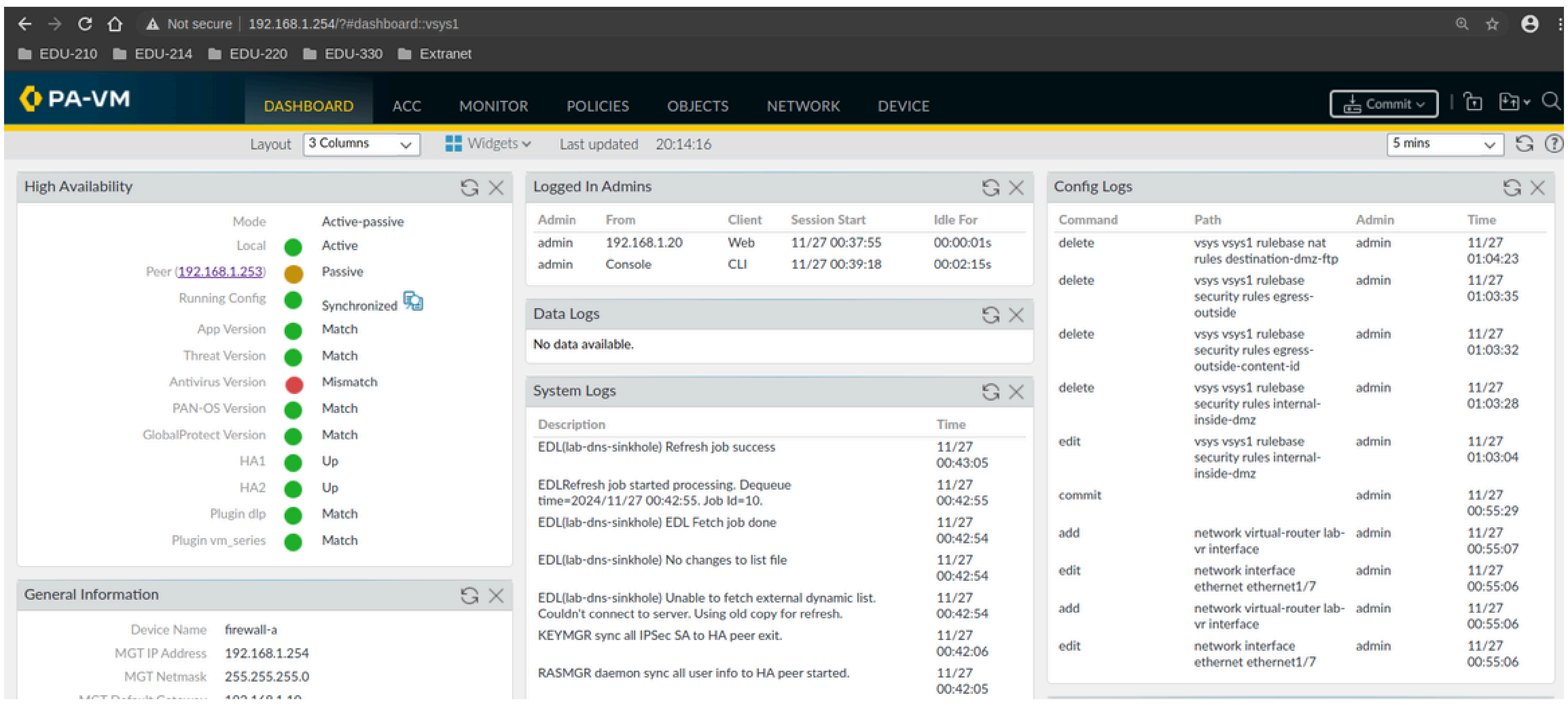
```
C:\home\lab-user\Desktop\Lab-Files> ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.505 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.380 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.437 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.378 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=0.522 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=0.354 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=64 time=0.419 ms
64 bytes from 192.168.1.1: icmp_seq=8 ttl=64 time=0.361 ms
64 bytes from 192.168.1.1: icmp_seq=9 ttl=64 time=0.530 ms
64 bytes from 192.168.1.1: icmp_seq=24 ttl=64 time=0.619 ms
64 bytes from 192.168.1.1: icmp_seq=25 ttl=64 time=0.713 ms
64 bytes from 192.168.1.1: icmp_seq=26 ttl=64 time=0.467 ms
64 bytes from 192.168.1.1: icmp_seq=27 ttl=64 time=0.529 ms
64 bytes from 192.168.1.1: icmp_seq=28 ttl=64 time=0.461 ms
64 bytes from 192.168.1.1: icmp_seq=29 ttl=64 time=0.433 ms
64 bytes from 192.168.1.1: icmp_seq=30 ttl=64 time=0.573 ms
64 bytes from 192.168.1.1: icmp_seq=31 ttl=64 time=0.382 ms
64 bytes from 192.168.1.1: icmp_seq=32 ttl=64 time=1.35 ms
64 bytes from 192.168.1.1: icmp_seq=33 ttl=64 time=0.430 ms
64 bytes from 192.168.1.1: icmp_seq=34 ttl=64 time=0.560 ms
64 bytes from 192.168.1.1: icmp_seq=35 ttl=64 time=0.560 ms
64 bytes from 192.168.1.1: icmp_seq=36 ttl=64 time=0.563 ms
^C
--- 192.168.1.1 ping statistics ---
36 packets transmitted, 22 received, 38% packet loss, time 35805ms
rtt min/avg/max/mdev = 0.354/0.524/1.353/0.202 ms
C:\home\lab-user\Desktop\Lab-Files>
```

Testing the HA Configuration:

- Connect a client to a firewall interfaces.
- Ensure this client connects to the two firewall interfaces that share the same IP address, with one interface being inactive/passive.
- Ping the firewall using the IP address 192.168.1.1.
- Turn off the active firewall.
- You should notice a brief disruption before the secondary firewall becomes active, as indicated by the ICMP sequence jumping from 9 to 24.

Verify HA

We can also verify that HA is working by checking the web UI. The screenshots below show the primary and secondary firewalls, with one being active and the other being passive. You can see that the configurations are synchronized. The only issue we can see is that the antivirus is mismatched, this would probably be fixed by updating the softwares all the way to the latest ones. In the screenshot we can see all the green dots mean good, HA1 and HA2 are both up an running meaning control and data.



Layout: 3 Columns · Widgets · Last updated 20:14:16 · 5 mins

High Availability

Mode		Active-passive
Local	●	Active
Peer (192.168.1.253)	●	Passive
Running Config	●	Synchronized
App Version	●	Match
Threat Version	●	Match
Antivirus Version	●	Mismatch
PAN-OS Version	●	Match
GlobalProtect Version	●	Match
HA1	●	Up
HA2	●	Up
Plugin dlp	●	Match
Plugin vm_series	●	Match

General Information

Device Name	firewall-a
MGT IP Address	192.168.1.254
MGT Netmask	255.255.255.0

Logged In Admins

Admin	From	Client	Session Start	Idle For
admin	192.168.1.20	Web	11/27 00:37:55	00:00:01s
admin	Console	CLI	11/27 00:39:18	00:02:15s

Data Logs

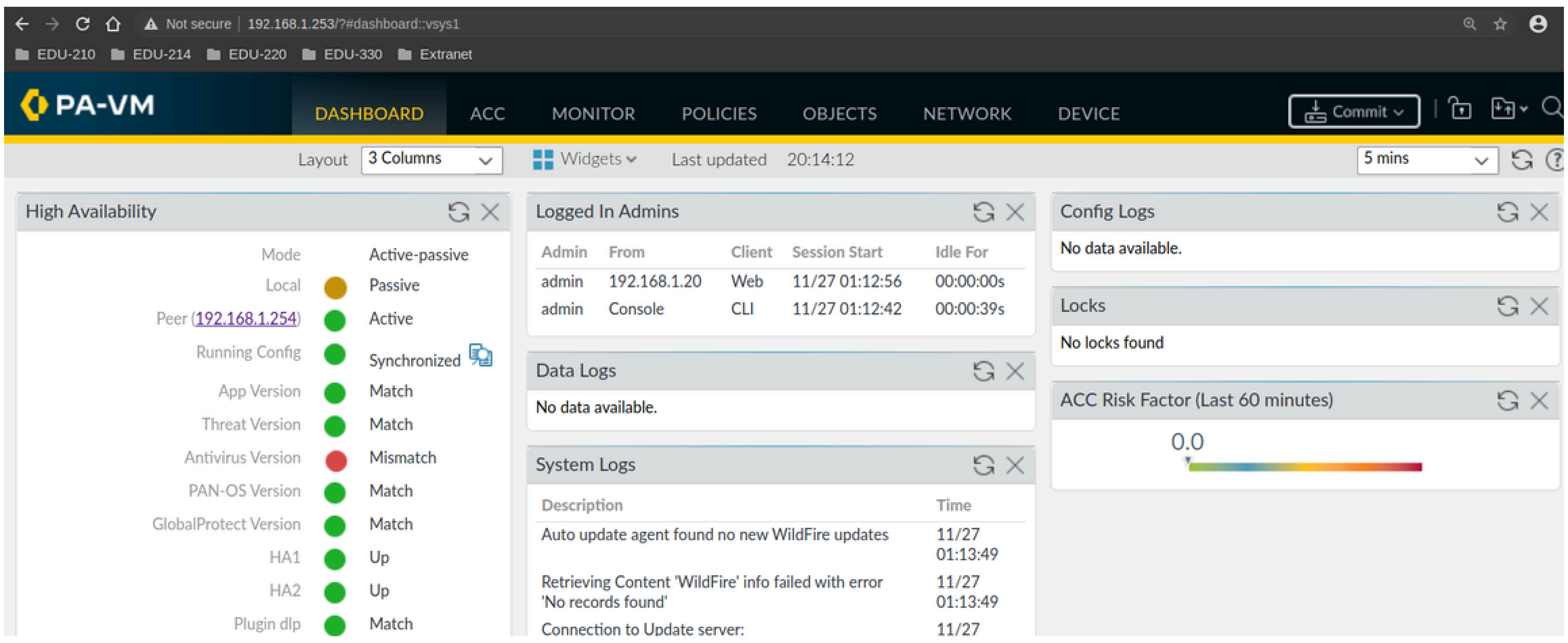
No data available.

System Logs

Description	Time
EDL(lab-dns-sinkhole) Refresh job success	11/27 00:43:05
EDLRefresh job started processing. Dequeue time=2024/11/27 00:42:55. Job Id=10.	11/27 00:42:55
EDL(lab-dns-sinkhole) EDL Fetch job done	11/27 00:42:54
EDL(lab-dns-sinkhole) No changes to list file	11/27 00:42:54
EDL(lab-dns-sinkhole) Unable to fetch external dynamic list. Couldn't connect to server. Using old copy for refresh.	11/27 00:42:54
KEYMGR sync all IPSec SA to HA peer exit.	11/27 00:42:06
RASMGR daemon sync all user info to HA peer started.	11/27 00:42:05

Config Logs

Command	Path	Admin	Time
delete	vsys vsys1 rulebase nat rules destination-dmz-ftp	admin	11/27 01:04:23
delete	vsys vsys1 rulebase security rules egress-outside	admin	11/27 01:03:35
delete	vsys vsys1 rulebase security rules egress-outside-content-id	admin	11/27 01:03:32
delete	vsys vsys1 rulebase security rules internal-inside-dmz	admin	11/27 01:03:28
edit	vsys vsys1 rulebase security rules internal-inside-dmz	admin	11/27 01:03:04
commit		admin	11/27 00:55:29
add	network virtual-router lab-vr interface	admin	11/27 00:55:07
edit	network interface ethernet ethernet1/7	admin	11/27 00:55:06
add	network virtual-router lab-vr interface	admin	11/27 00:55:06
edit	network interface ethernet ethernet1/7	admin	11/27 00:55:06



Layout: 3 Columns · Widgets · Last updated 20:14:12 · 5 mins

High Availability

Mode		Active-passive
Local	●	Passive
Peer (192.168.1.254)	●	Active
Running Config	●	Synchronized
App Version	●	Match
Threat Version	●	Match
Antivirus Version	●	Mismatch
PAN-OS Version	●	Match
GlobalProtect Version	●	Match
HA1	●	Up
HA2	●	Up
Plugin dlp	●	Match

Logged In Admins

Admin	From	Client	Session Start	Idle For
admin	192.168.1.20	Web	11/27 01:12:56	00:00:00s
admin	Console	CLI	11/27 01:12:42	00:00:39s

Data Logs

No data available.

System Logs

Description	Time
Auto update agent found no new WildFire updates	11/27 01:13:49
Retrieving Content 'WildFire' info failed with error 'No records found'	11/27 01:13:49
Connection to Update server:	11/27

Config Logs

No data available.

Locks

No locks found

ACC Risk Factor (Last 60 minutes)

0.0

Common HA Issues

Some common HA issues when setting it up with Palo ALto Firewall HA would be putting the wrong group id causing them not to connect. another issue would be wrong interfaces, if you use the wrong interface for HA when setting up HA in the communications tab they wont sync. Another one would be mismatched firewall software versions which either would not work at all or cause errors. Another would be not putting in your firewalls license key so they wouldnt be licensed. Putting the wrong subnet on the HA link would cause an issue because they cant connect over IP.

Conclusion

In this lab, we explored High Availability (HA) using a virtual computer connected to two firewalls in a primary (HA #1) and standby (HA #2) configuration. This setup ensured continuity during hardware failures by switching connections to the standby firewall. We established two HA links for control and data transmission.

HA is crucial for network reliability by adding redundancy. It maintains connectivity during failures by synchronizing configurations and session states.

Challenges included synchronizing configurations and addressing MAC resolution and control plane connectivity issues due to network adapter and IP misconfigurations. Proper HA prioritization is vital, as we observed inconsistencies without it.

We tested failover by pinging the firewall’s gateway, bypassing traffic propagation. Both firewalls initially had identical setups in VMware, so we changed MAC addresses and serial keys. Using the same VMware session for both avoided needing a VPN link.

We didn't upgrade to the latest version to avoid sequential updates. Instead, we updated to the next available version.

This lab provided key insights into configuring and testing HA on a Palo Alto firewall and will relate to real world situations we come across.