PA 410

*Palo Alto Initialization and SOHO*

Adv Cisco Cybersecurity – Lab 7

Jason Liu

Cybersecurity – Mr. Mason & Mr. Hansen

Period 5

*Lab 7: Palo Alto PA-410 – Initial and SOHO Configuration*

**Purpose**

The objective of this lab is to initialize and to set up a Palo Alto, PA-410, firewall for Small Office Home Office (SOHO) configuration. Its abilities are nuanced from the PA-220 of the first Cybersecurity labs, and thus another objective is to understand its unique licensed features.

**Background Information**

Palo Alto’s PA-410 is the first of the 400 series lineup, being both the smallest and the most accessible. This series, along with many of Palo Alto’s products, are considered Next-Generation Firewalls (NGFW), meaning not only does it use traditional firewall features, but also is considered a strong networking device with advanced filtering, monitoring, and inspection functions. It provides greater control and utility for the work that may be necessary in an industry environment.

The operating system (OS) for this series, as well as all for all Palo Alto network NGFWs, is the PAN-OS. PAN-OS natively classifies all traffic to a user regardless of location or device. This means it tracks applications, content, and threats to each individual user so that security policies, or rulesets that define sessions, can act timely and responsively. The OS also hosts the webGUI, an intuitive management interface where the majority of the firewall should be configured on.

Specific to this series, it advertises its lineup to be the first Machine Learning firewalls, identifying and stopping phishing attempts and other threats. Machine Learning processes are cloud-delivered and natively integrated on the firewall, which provides fast feedback of potential threats. It is a licensed function. It can also make security policy recommendation and even policy auto-configurations to adapt to new devices in environments, such as items belonging to the Internet of Things (IoT). The IoT consists of all ranges of devices that connect to a mainstream database via internet to retrieve data and information, such as smart refrigerators, voice AI, washing machines, and more. With new Machine Learning functions, it can automatically detect and analyze their device onto the network while simultaneously applying the security policy based on their potential threat. This saves time and reduces the change of human error.

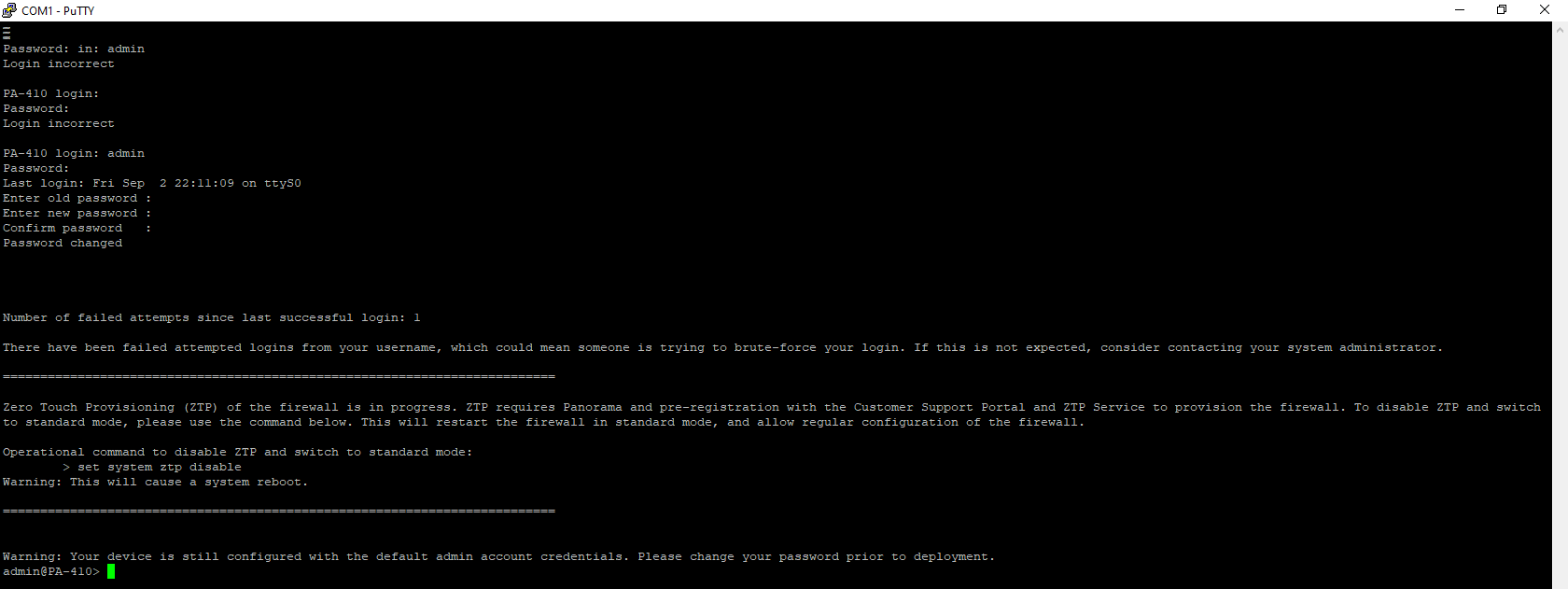
These firewalls avoid using the port as the basis of its policy decisions. This means that policies are based on the application and can span multiple port interfaces which detect and identify the traffic traversing the network regardless of protocol, encryption, or other techniques. In general, all of Palo Alto’s features serve the same purpose of identifying and categorizing all traffic and applications to enforce the security of users. It is highly recognized in industry standards for its ability to maximize security and prevent malicious activity via both its integrated and cloud-delivered (licensed) features.

**Lab Summary**

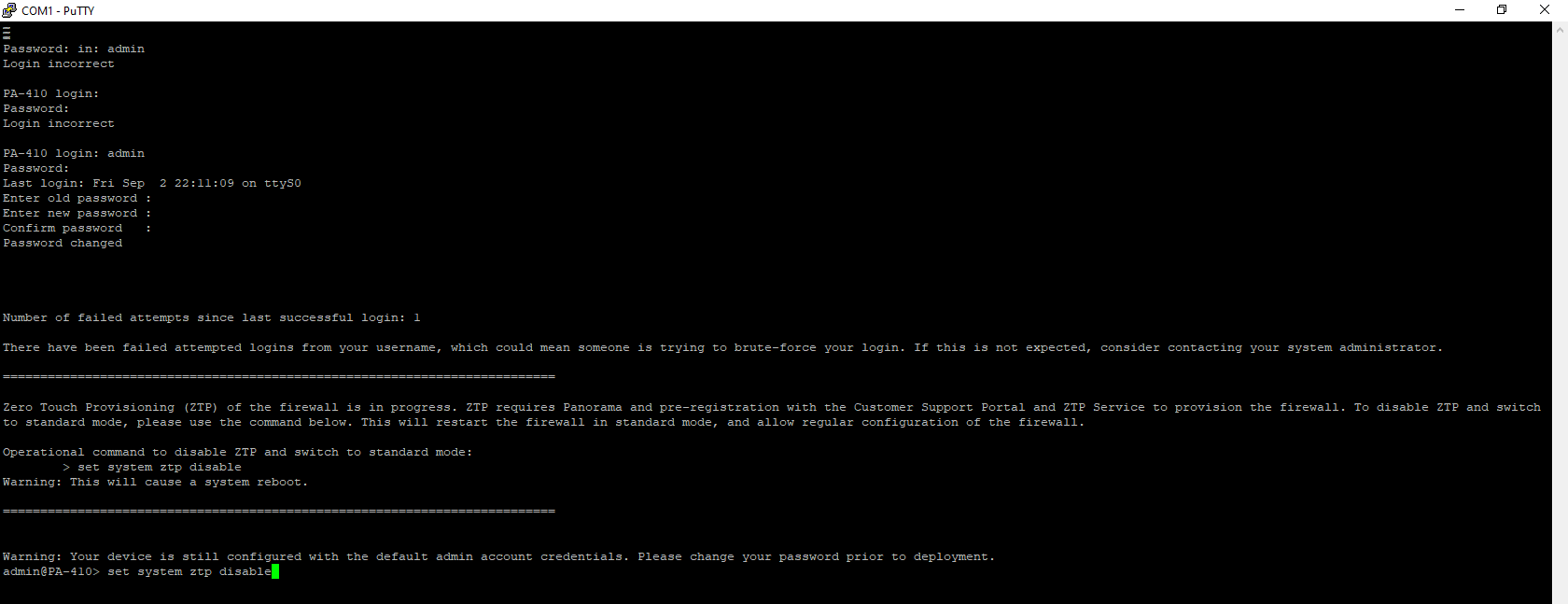
Ending the stalemate of *Lab 6: Cisco ASA 5505* with the introduction of factory fresh PA-410s to the CISCO labs, it was a well-timed break to implement something new. As the PA-410 were completely unopened, there was no need to factory reset these firewalls this time, compared to the used PA-220s in *Lab 1: Factory Reset*. Upon powering the device using the barrel head power cord given in the provided packaging, its initial startup prompts were almost identical to the PA-220, such as having default credentials of *admin* for both username and password fields, as well as requiring an initial change in password. The only difference was its prompt for Zero Touch Provisioning (ZTP). The alternate option was standard mode. We entered the command “set system ztp disable” to enter via standard mode. This action rebooted the firewall but minor errors occurred at this time (see *Problems)*. After successful transition to standard mode, other configurations were intended to be completed on Palo Alto’s useful web Graphical User Interface (webGUI). Changing the PC’s IP address to be on the management IP subnet of 192.168.1.0/24 and entering the default management IP address of 192.168.1.1, one may enter the webGUI on the PC via a browser. Mozilla Firefox was used. Like the credentials, the management IP addressing information may be changed in configuration and must be committed to the firewall, or in other words, to save the changes to the startup configuration.

Luckily, Palo Alto GUI menus and basic configuration are identical between the 200 and 400 series. This means that the SOHO configuration after initial login for the PA-410 is identical as the one done for the PA-220. Recompleting SOHO served as good practice. The process comprised of configuring Layer 3 and Layer 2 Security Zones, the Ethernet interfaces, VLANs and VLAN assignment, the Security Profile Group, and more. The procedure we followed is based on the online documentation for the PA-200 series: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFkCAK>.

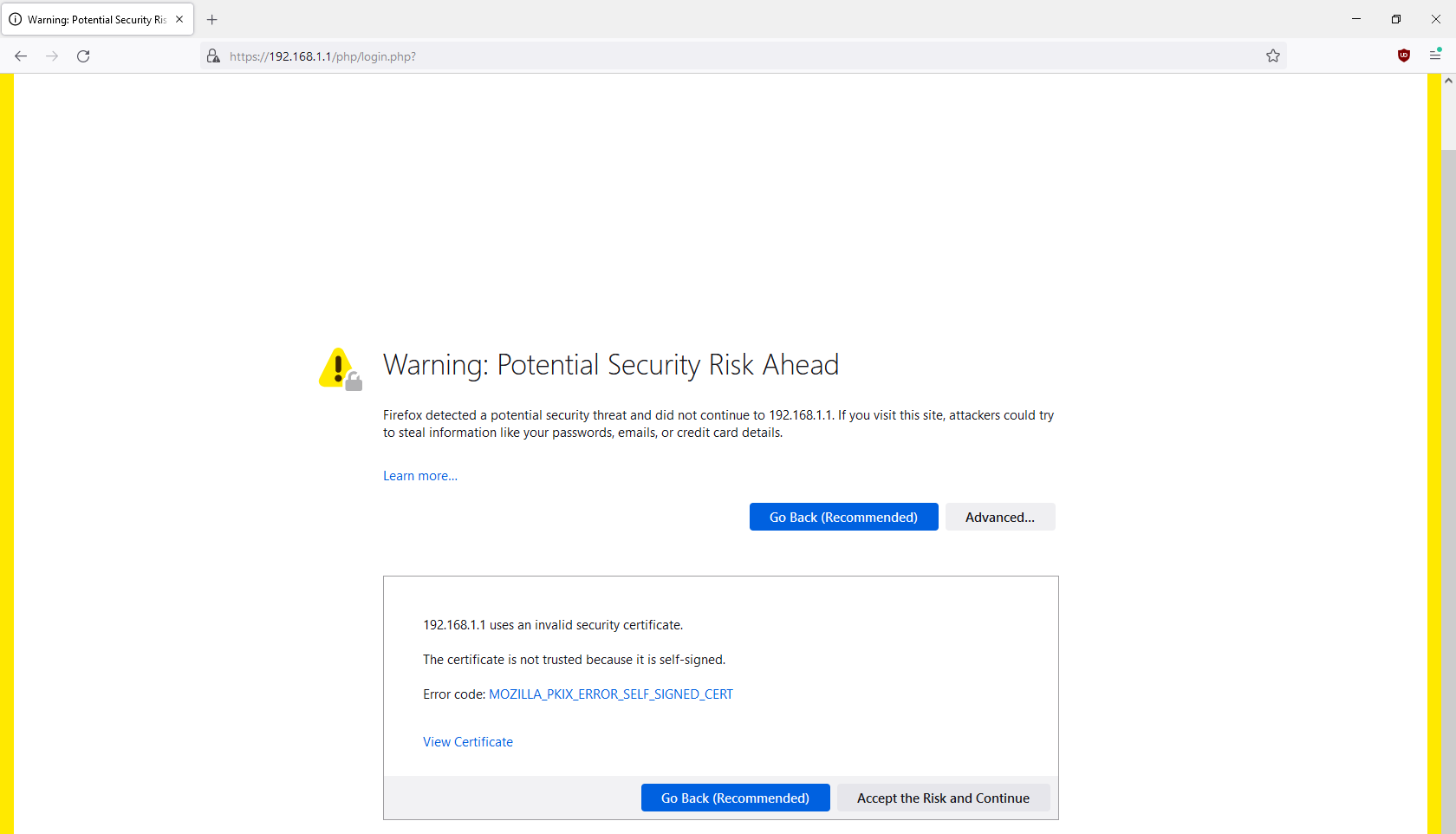
It is important to note that many additional and licensed features were unable to be used as licenses have not yet been obtained for these devices. Basic SOHO, however, can still be implemented throughout.

**Procedure**

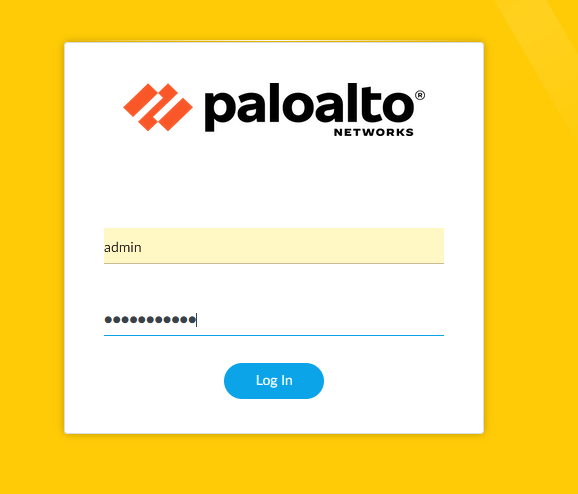
The initial prompt. It will ask to change the password. Default credentials are *admin*.

****

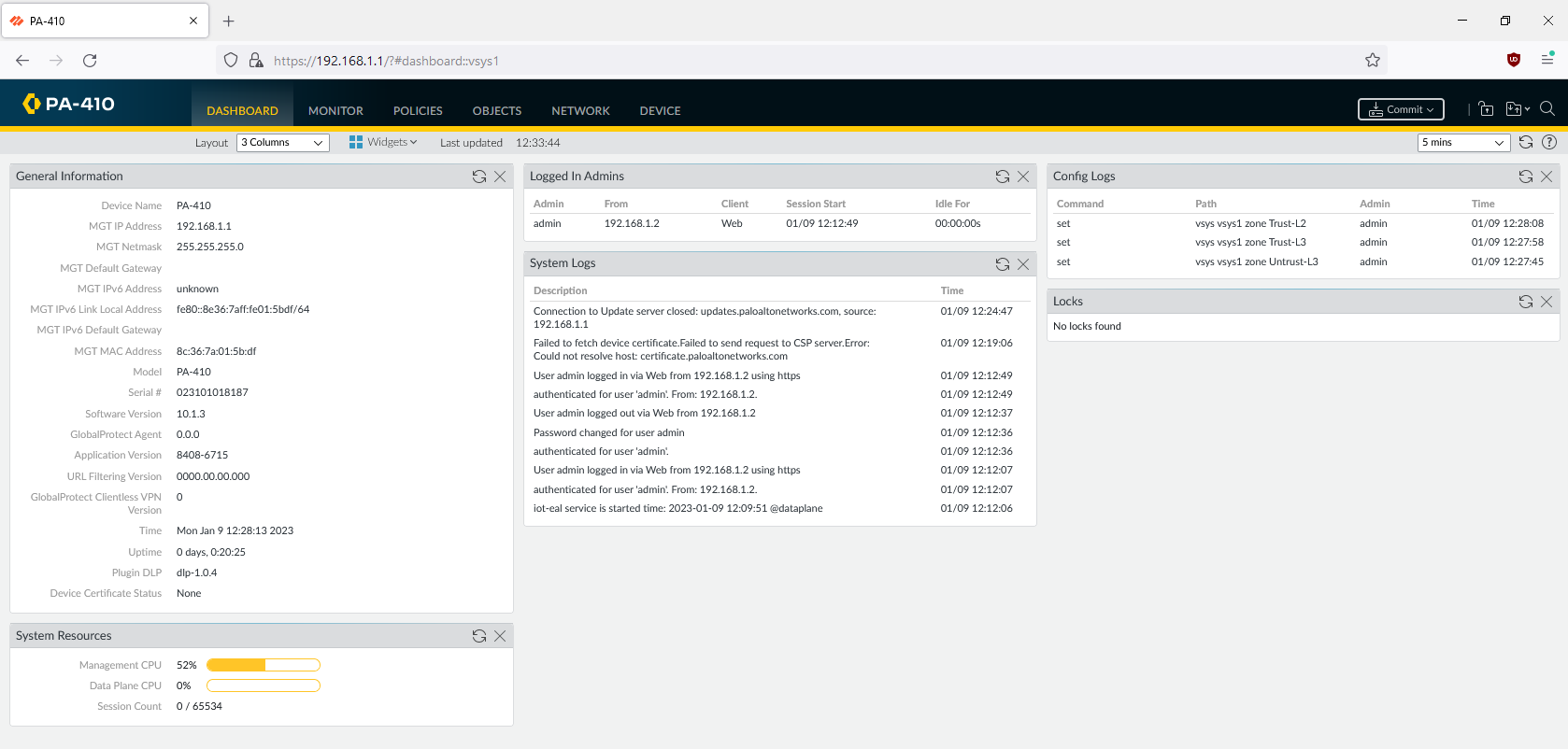
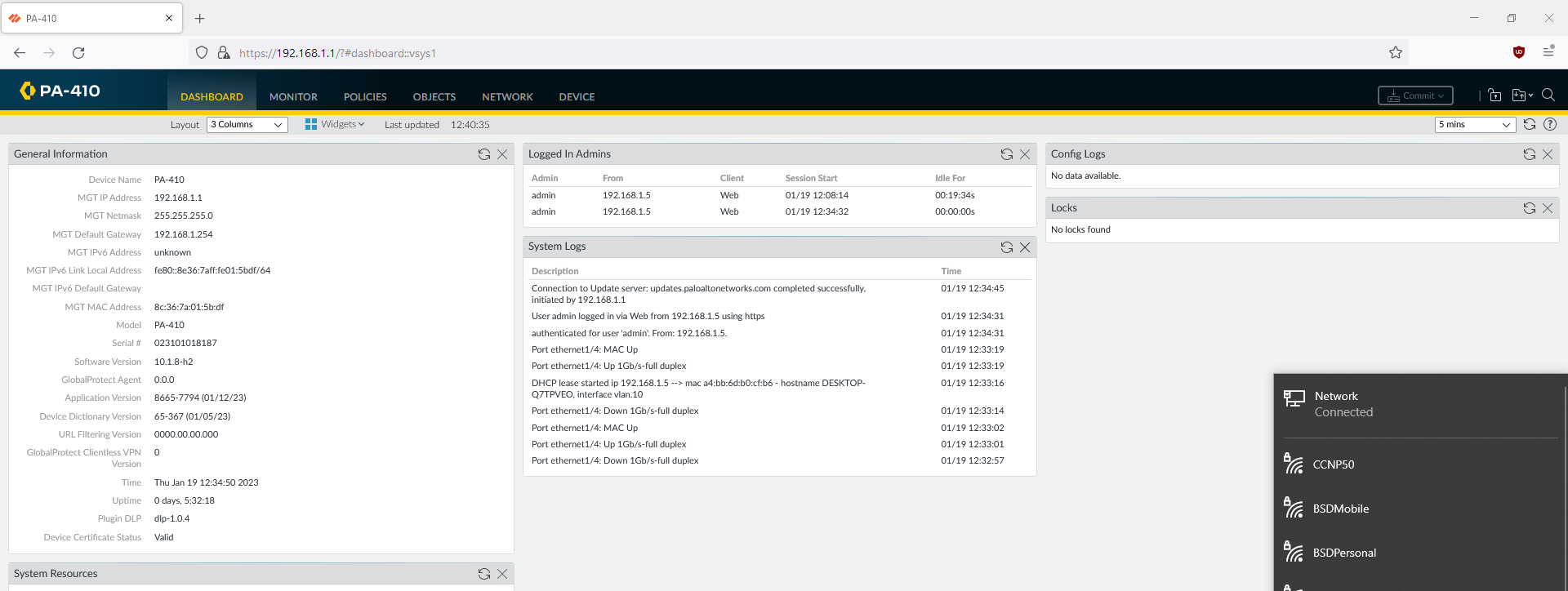
Disabling ZTP with the given ZTP command - “set system ztp disable”. This will reboot the firewall.

****

Entering the webGUI using the management IP of 192.168.1.1

****

Entering new created password to enter the webGUI.

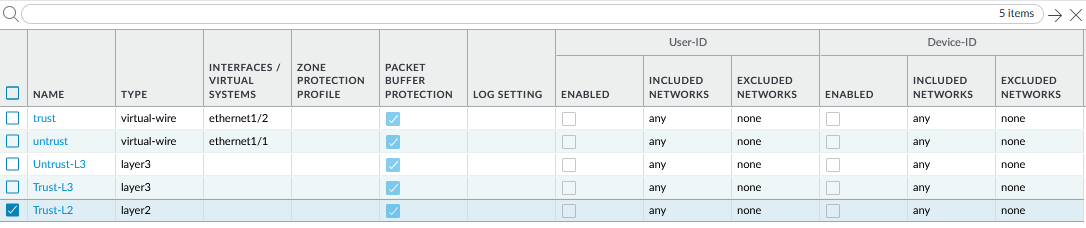
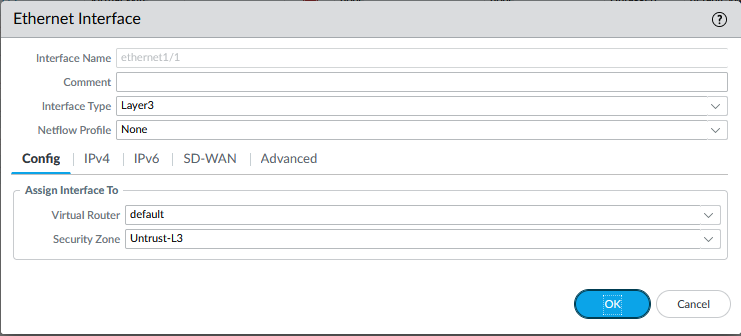
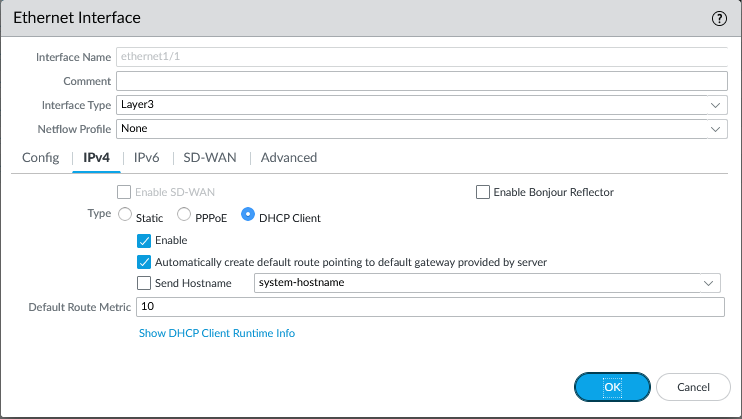
****

The main dashboard. After SOHO configuration (see below), ethernet connection to the internet should be connected.

BELOW IS PROCEDURE CITED FROM *LAB 2: SOHO (PA-220)*

REFERENCE FOR SOHO CONFIGURATION

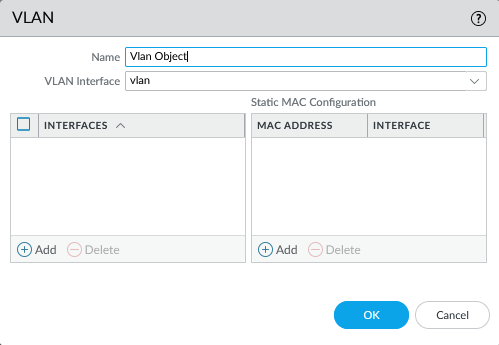
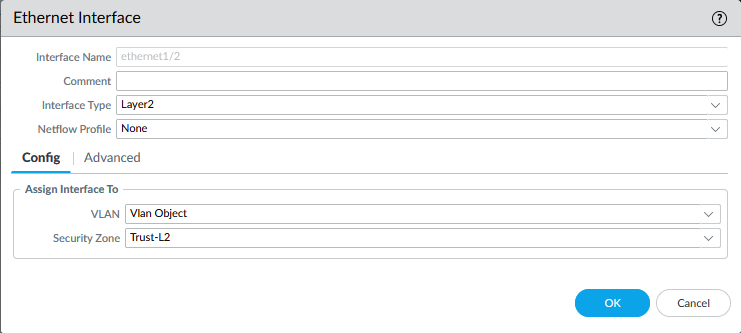
SEE “Problems” SECTION FOR ADDITIONAL PA-410 INFO

****

As it is a Layer 3 interface, IPv4 must be configured. Choose it to be a DHCP client.

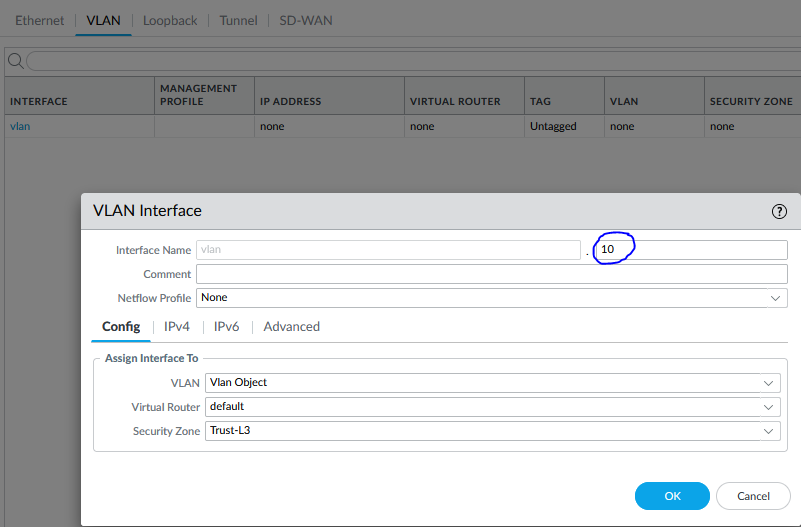
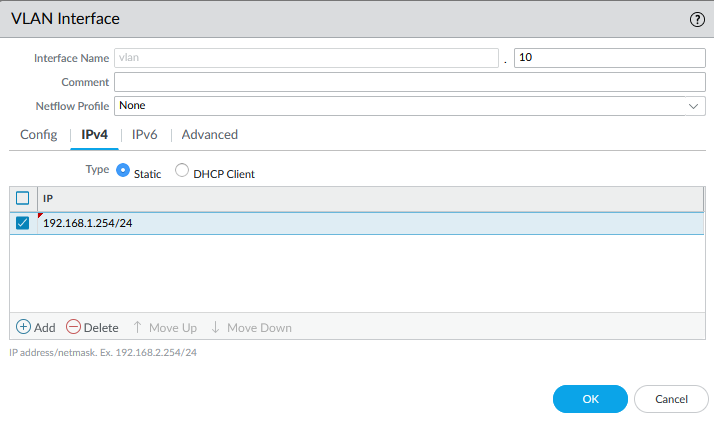
Configure the ethernet1/1 interface to be assigned to the outbound zone.

Create Security Zones. One outbound zone, two inbound zones.

****

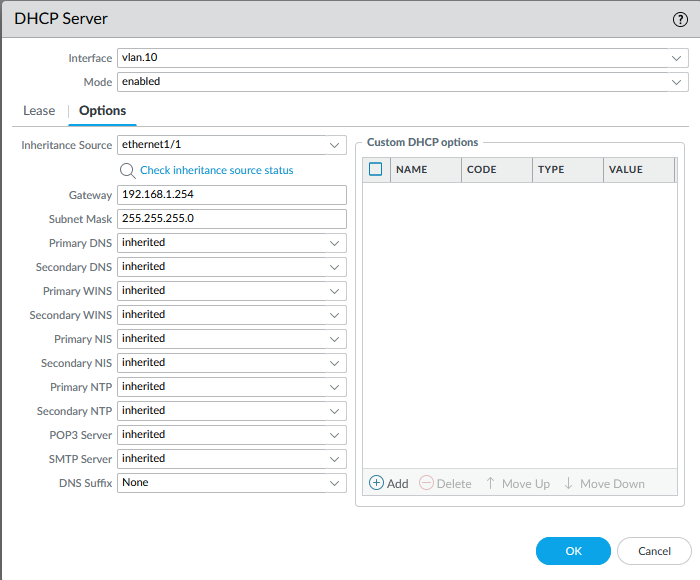
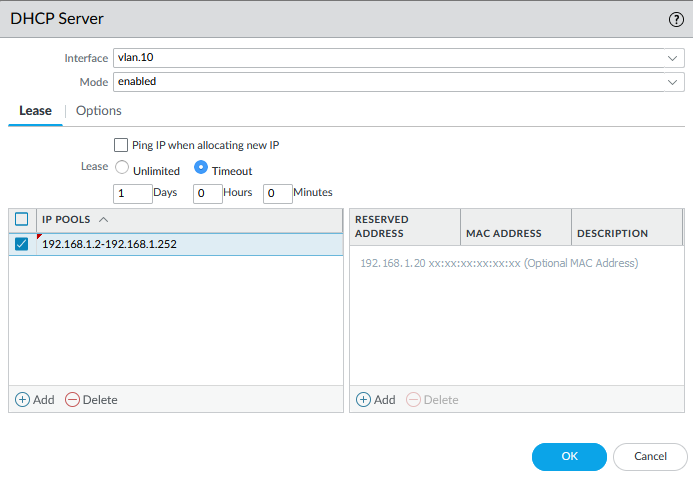
Configure the rest of the Ethernet Interfaces to be Layer 2 and attached to the internal Security Zone and VLAN. Interfaces ethernet1/2, 1/3, and 1/4 were repeated and configured for this lab.

Create a VLAN. This VLAN was named “Vlan Object.” Assign it to a vlan interface.

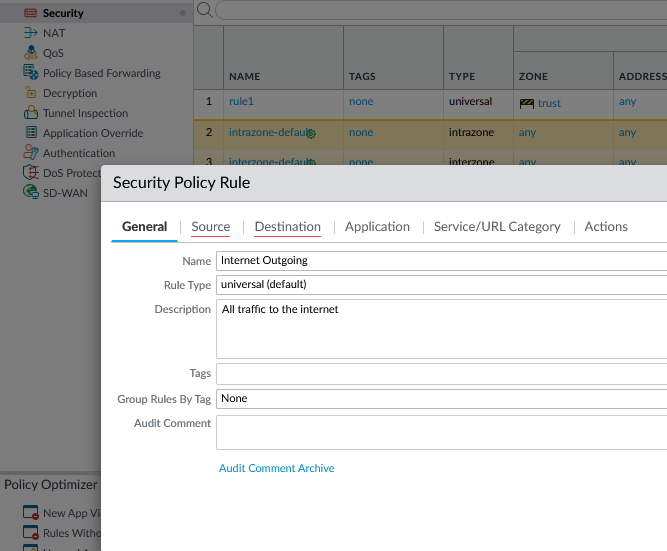
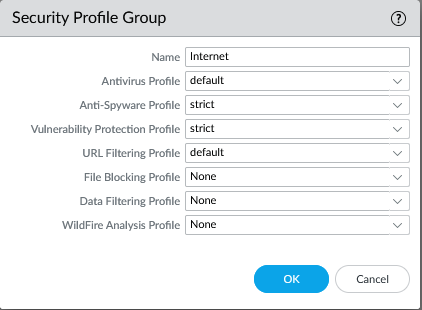
****

Assign an address for the vlan interface. By using the last possible host address in the subnet, it allows DHCP IP pools to be configured easier.

Create a VLAN interface. Do not number it “1” for best practice, as vlan.1 is reserved for other uses in certain circumstances.

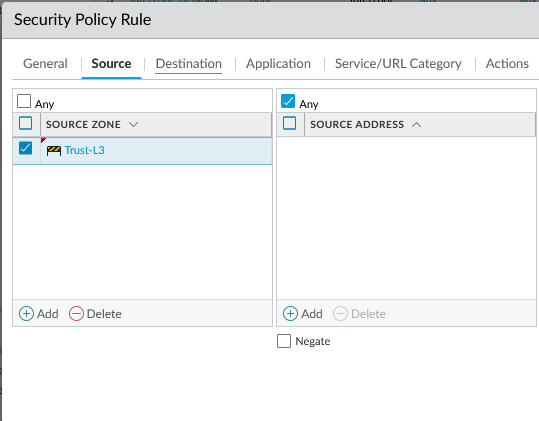
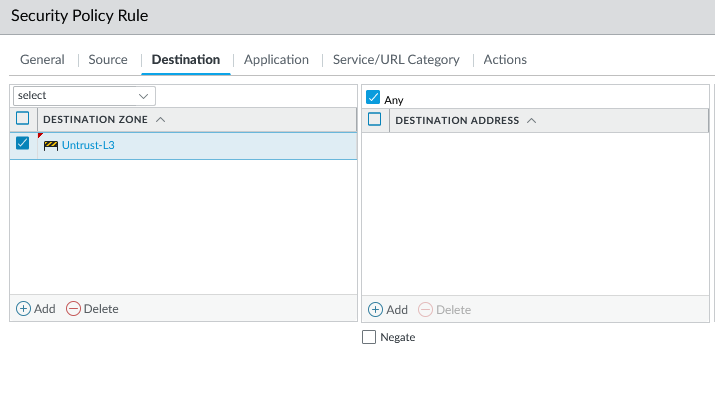
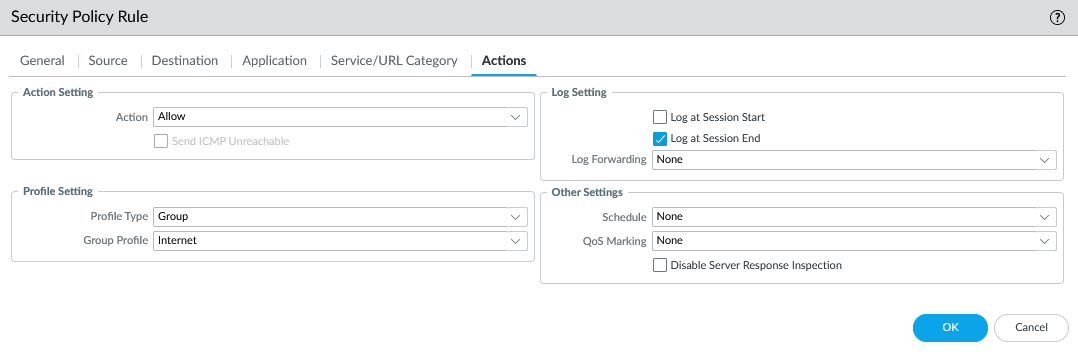
****

Create the DHCP Server to retrieve and inherit information from ethernet1/1, the interface that is tied to the outbound interface. Assign the gateway to the vlan interface IP. Finally, create the IP pool. The rest of the host addresses are used.

****

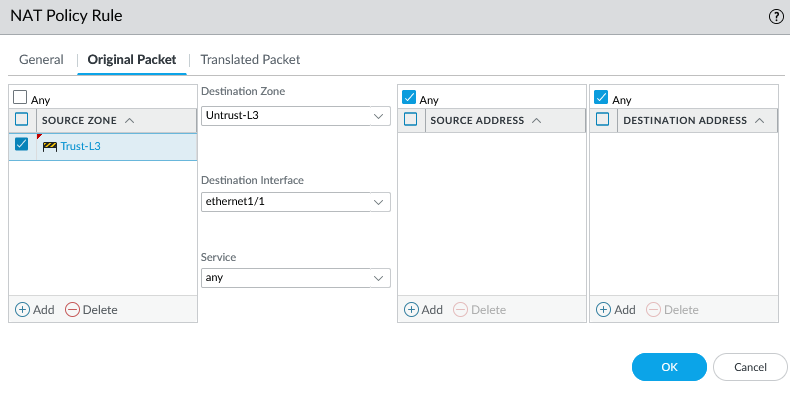
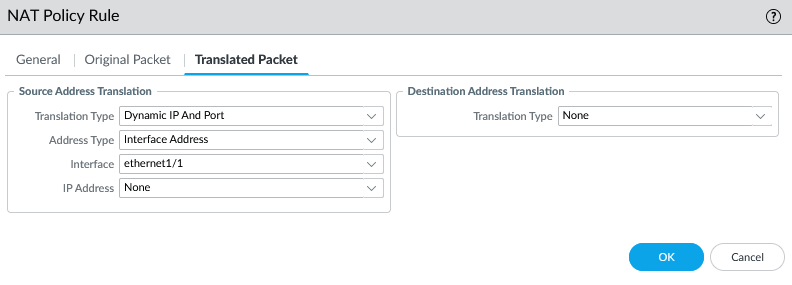
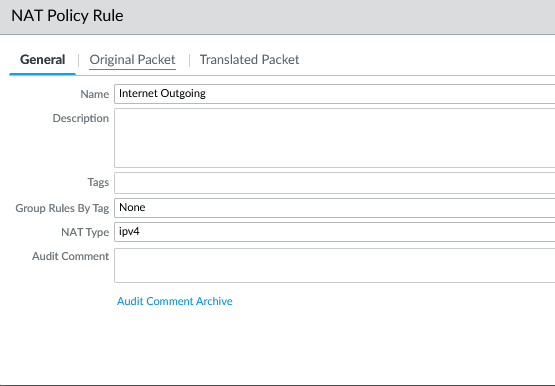
Create a Security Policy Rule. Make it a universal rule as well as giving it an optional brief description.

Create a Security Profile group, consisting of many Palo Alto default Profiles. This will be applied to the Security Policies.

****

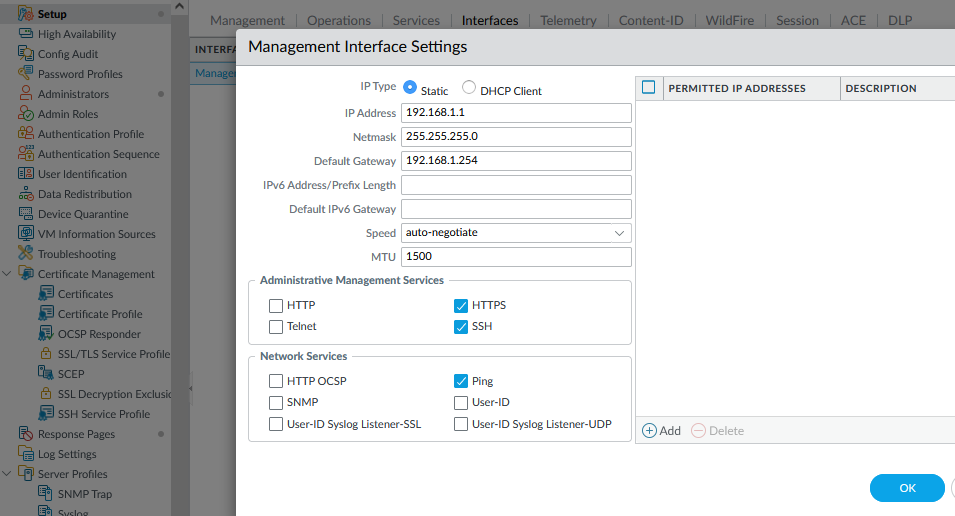
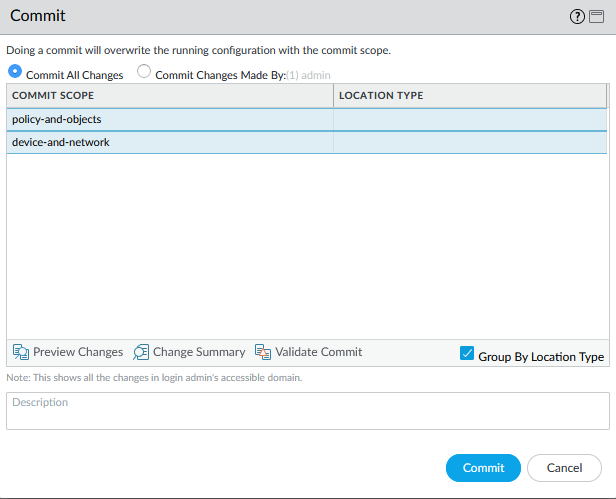
Let it be an “allow” action and assign the profile group.

Assign source and destination zones. It is sourced in the inbound zone, and destination to the outbound zone.

****

Similarly, create a NAT policy rule with the corresponding source inbound and destination outbound zone. The outbound interface is ethernet1/1.

Configure translated packet settings, too, including Translation type and interface.

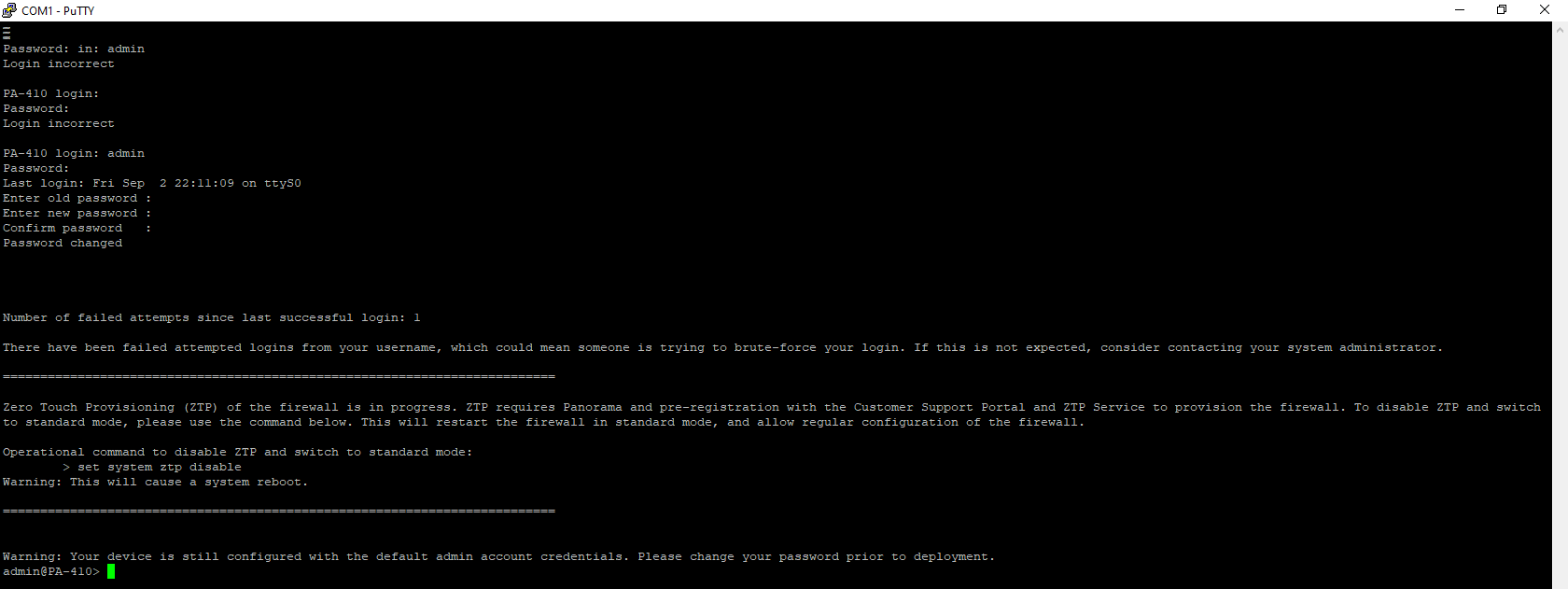
****

Select “Commit” and commit changes to save all configurations to the firewall. The firewall should now be functional. Completion continued in *Problems* section.

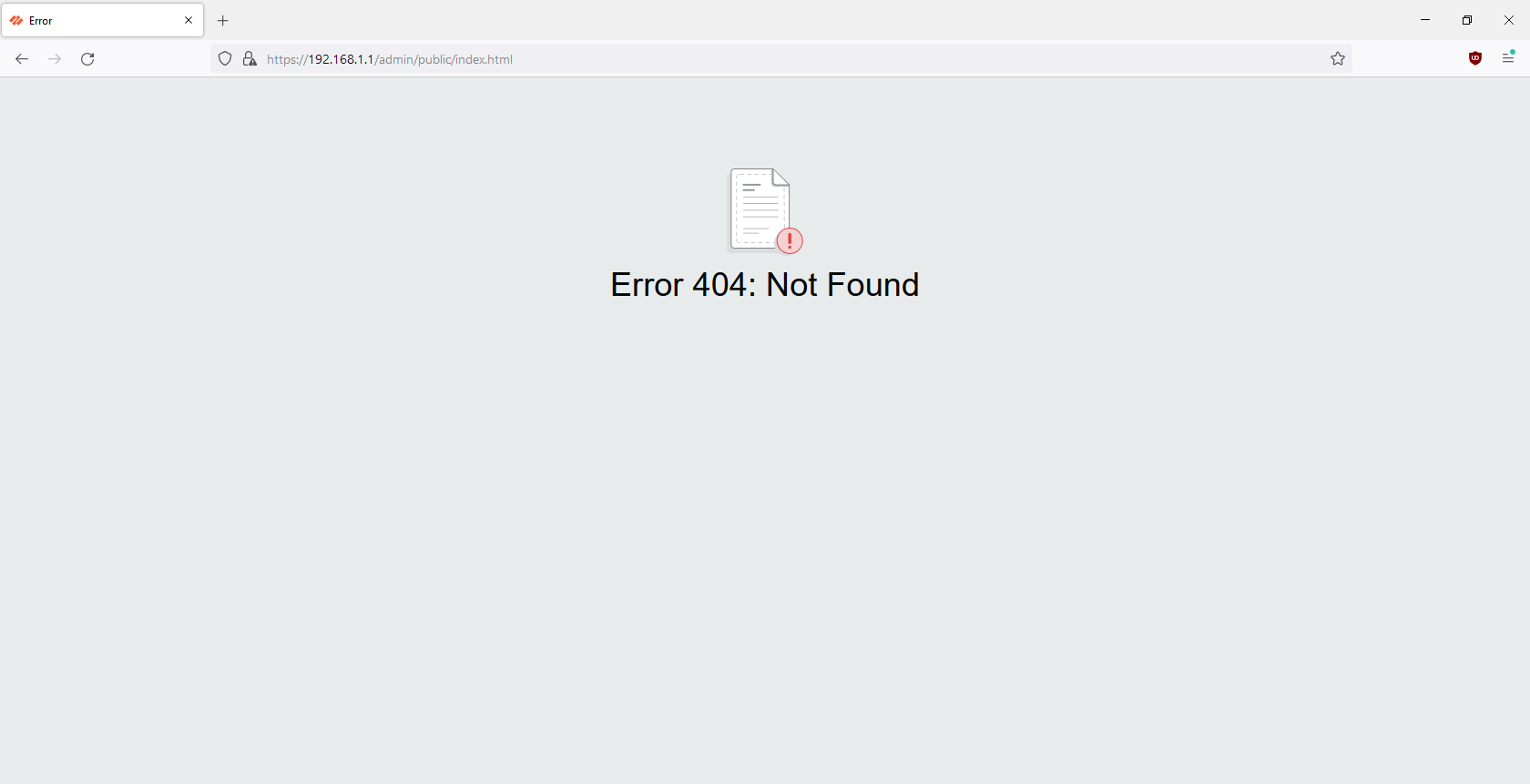
For best practice, configure the Management Interface to a new IP and allow certain administrative management services. We kept the interface address default.

**Problems**

Despite following the SOHO configuration that worked previously, there resurfaced minor problems as well as new ones that are unique to PA-410, such as Zone Touch Provisioning.

 During initial setup, there are sometimes show strange bars that appear like corrupted lines which appear on the console, momentarily freezing the console. However, it does not damage any configurations and did not pose any major issues.

Corrupted lines appeared often in the console.

 After disabling ZTP, the firewall rebooted. However, my lab partner Evan Choi and I were never able to access the webGUI on our PCs again. It would show a web page 404 error. Only one other lab peer had this issue. We solved this issue by testing other NVMe drives and realized that the issue corresponded to the specific storage drive that the PC was booting off of. We then deduced that the web page error was caused by us changing the TLS in a troubleshooting attempt to access the ASDM launcher for *Lab 6: Cisco ASA 5505*. By using other drives, such as a blank and reimaged NVMe drive for the computer to boot off of, where TLS versions were never touched, one can login into the firewall’s webGUI perfectly. Note that “https://”, the secure HTTP, was required on the browser to obtain access.

Unable to access webGUI after disabling ZTP. This is due to TLS version tampering. NVMe drives with proper TLS versions can load normally.

The SOHO configuration was almost complete. Last minor issues reflected configuration hiccups in PA-220’s SOHO, such as virtual wire issues. Deleting the virtual wire, changing the zones it interacts with (to the ones that were created), and reassuring that the PC should obtain DNS and IP address automatically, were all methods to double check the proper functionality of PA-410’s SOHO.

**Conclusion**

This is the first time unpackaging and using a piece of equipment straight out of the box, so it was a good experience going through its contents and using a factory fresh device. Otherwise, startup and configuration was simple and straightforward, following the experience of previous Palo Alto work. As I researched Palo Alto’s technological publications, it gave insight on many new features that the Series 400, and potentially beyond, brings. In conclusion, this lab improves my holistic experience on what buying, using, and implementing a new Palo Alto firewall may be like.