Anjali Jain

Lab 1: Creating a Zero Trust Environment

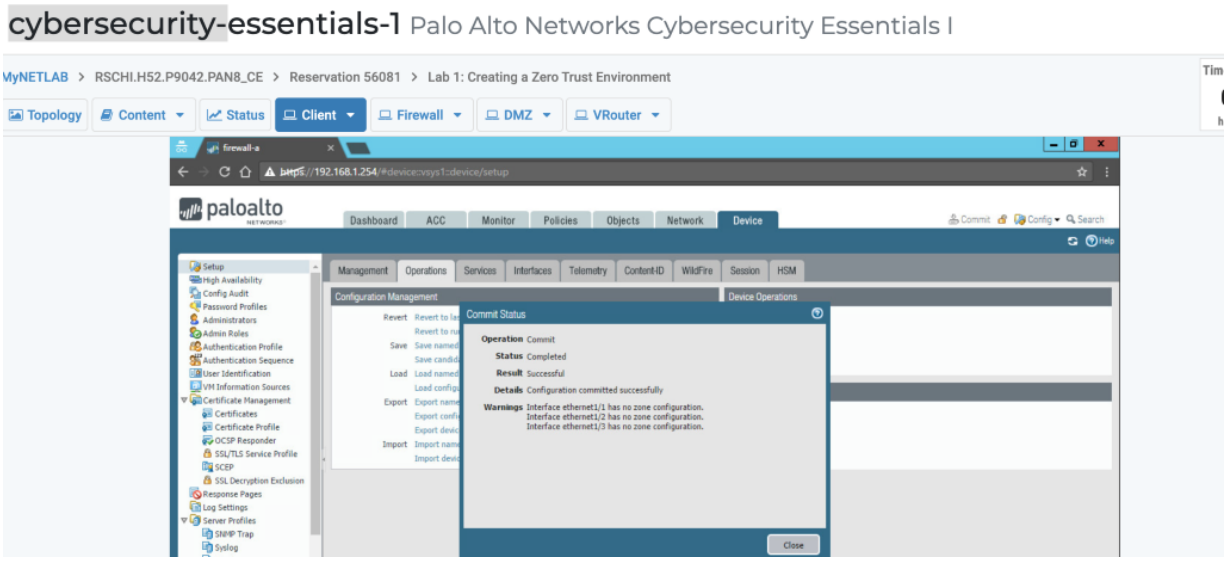
Introduction

In this lab, configure the Firewall with three zones: inside, outside, and dmz. Then, I have applied security policies to these zones to ensure all traffic between zones is being monitored by the Firewall.

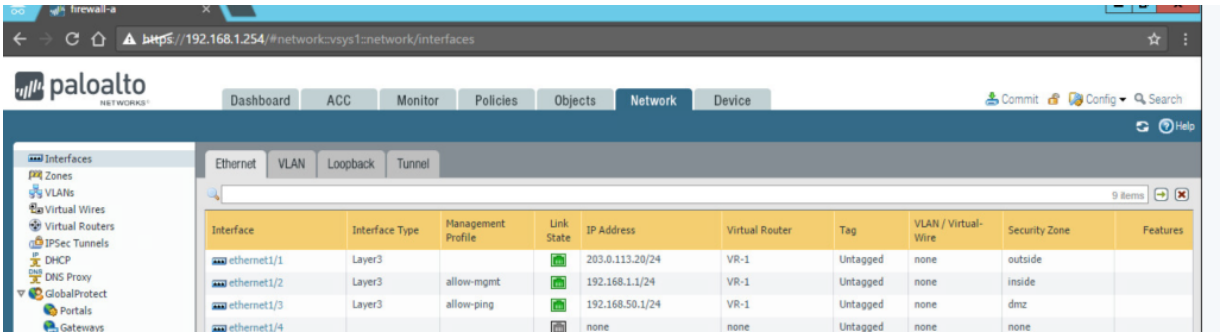
Objective

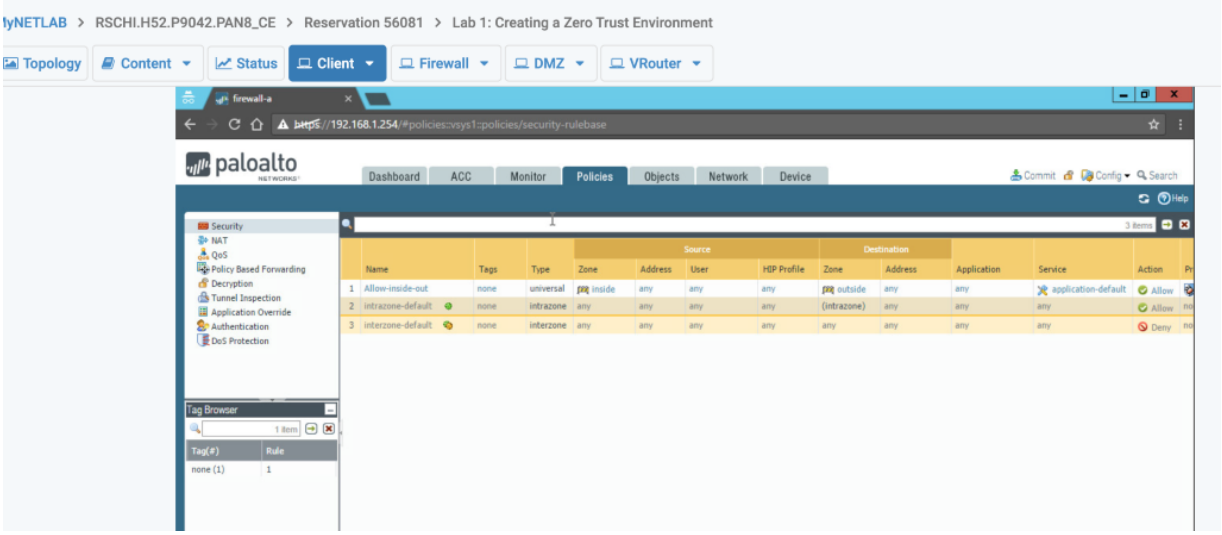
In this lab, perform the following tasks: • Create Zones and Associate the Zones to Interfaces • Create a Security Policy Rule • Create a NAT Policy • Commit and Test the Rules and Policies

A) pan8-ce-lab-01 code committed

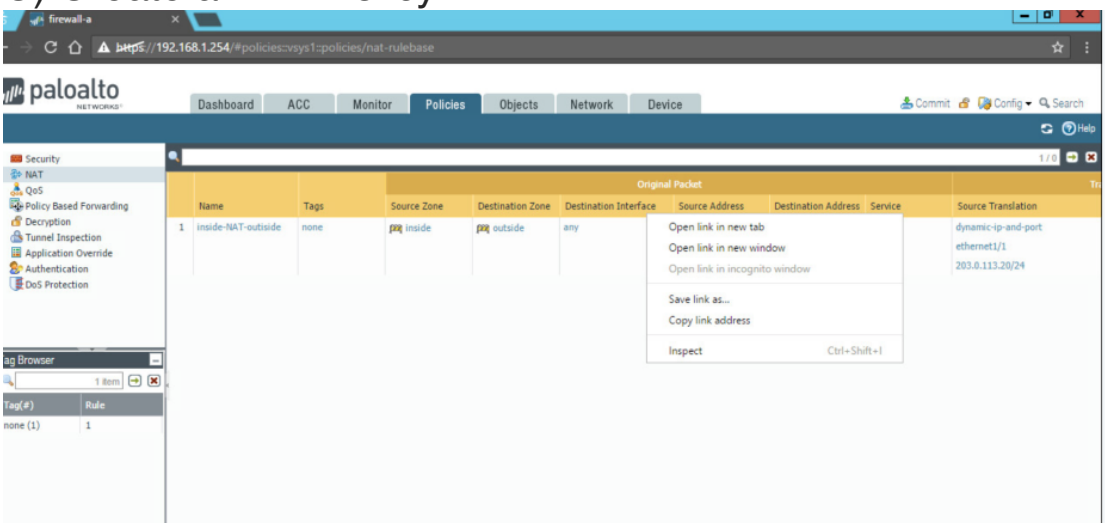


B) Create Zones and Associate the Zones to Interfaces



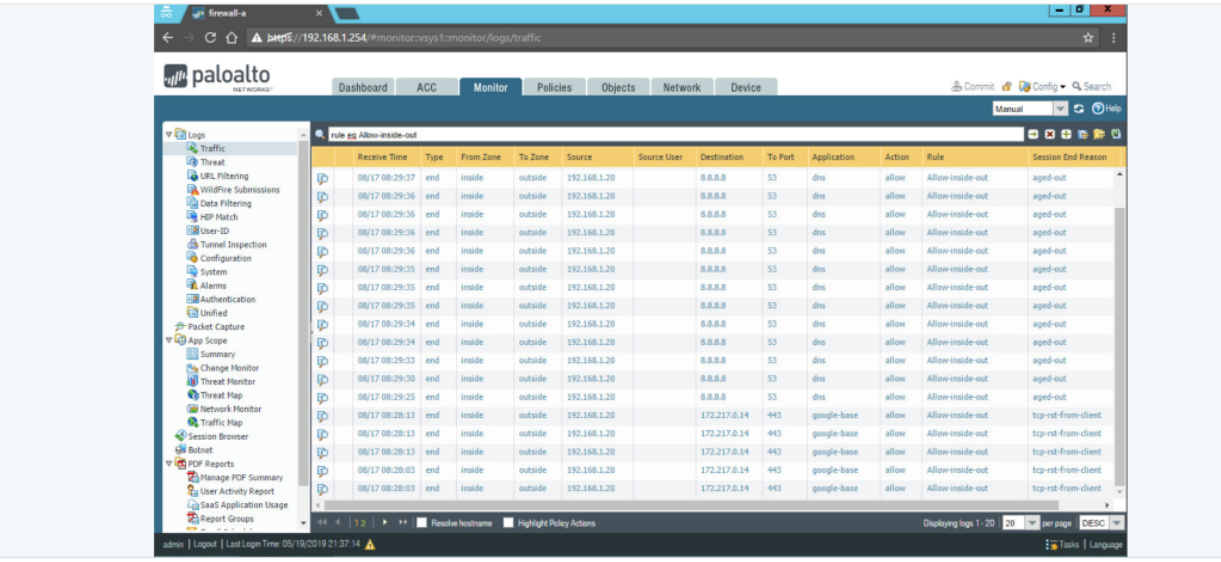


C) Create a NAT Policy



D) Commit and Test the Rules and Policies In this section, I will create a basic NAT policy to NAT traffic from the inside zone to the outside zone.

cybersecurity-essentials-1 Palo Alto Networks Cybersecurity Essentials I



Lab 2: Configuring Authentication

Introduction

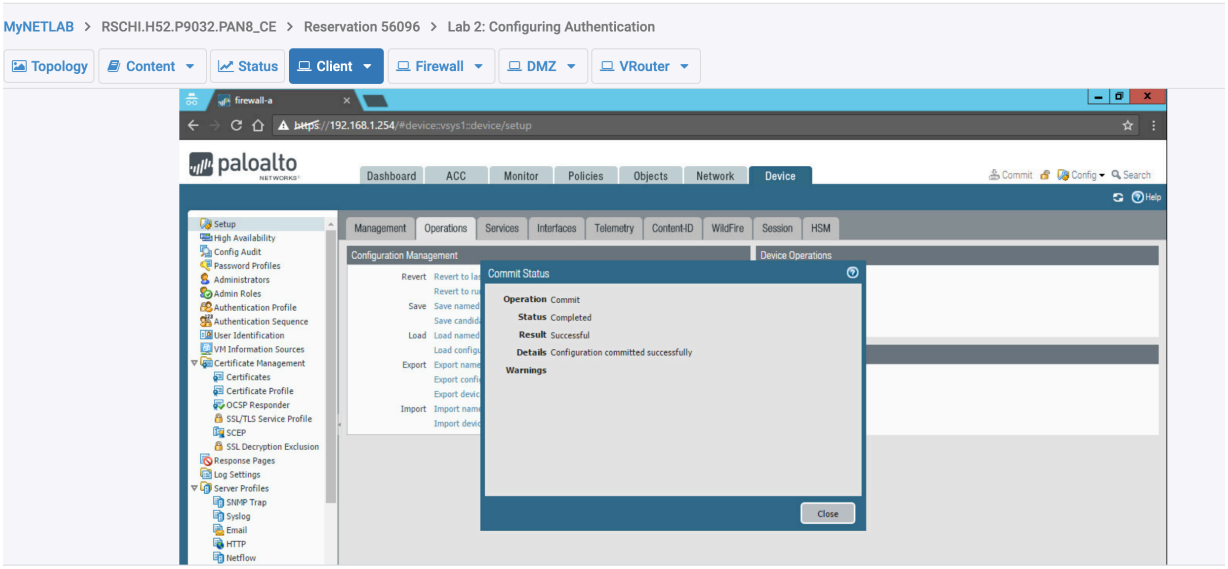
In this lab, configure the Firewall to use a Captive Portal to authenticate users by using a local user account and Authentication Policy.

Objective

In this lab, perform the following tasks: • Configure a Local User Account and Authentication Profile • Enable the Captive Portal and Enable Web-Form based Logins • Create an Authentication Policy • Commit and Test Authentication Policy

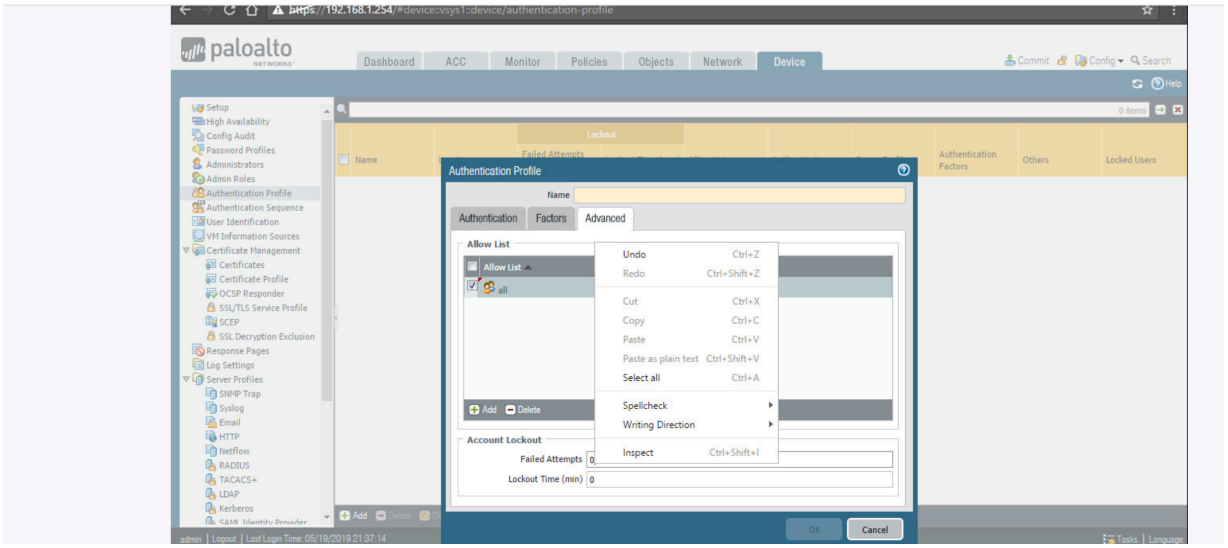
A) commit the changes for this lab.

cybersecurity-essentials-1 Palo Alto Networks Cybersecurity Essentials I

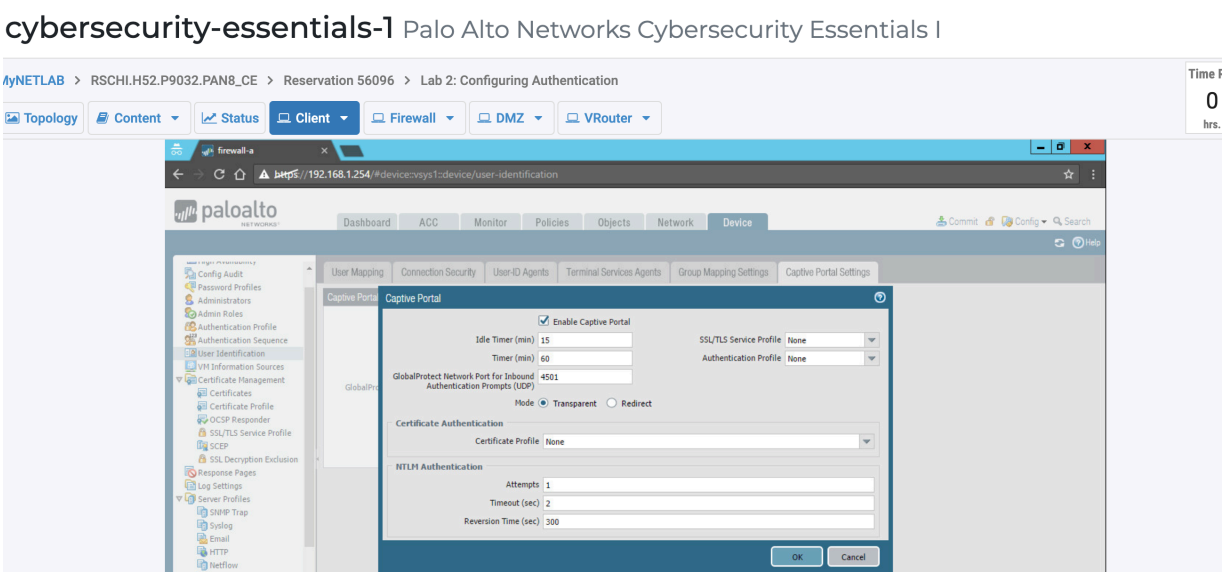


B) Configure a Local User Account and Authentication Profile

cybersecurity-essentials-1 Palo Alto Networks Cybersecurity Essentials I



c) Enable the Captive Portal and Enable Web-Form based Logins



d) Default-web form cloned

Lab 3: Using Two-Factor Authentication to Secure the Firewall

Introduction

In this lab, we will configure the Firewall to use two-factor authentication using a certificate, along with a username and password.

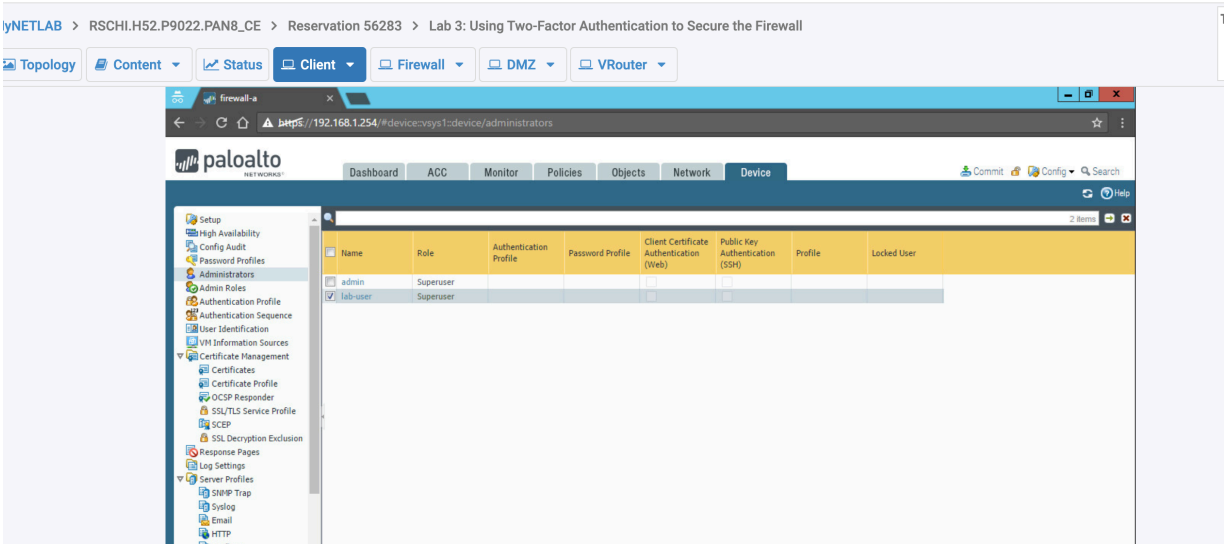
Objective

In this lab, perform the following tasks: • Create a Local User Account • Generate Certificates

• Create a Certificate Profile • Export Certificate and Commit • Test Connectivity and Import Certificate on the Client

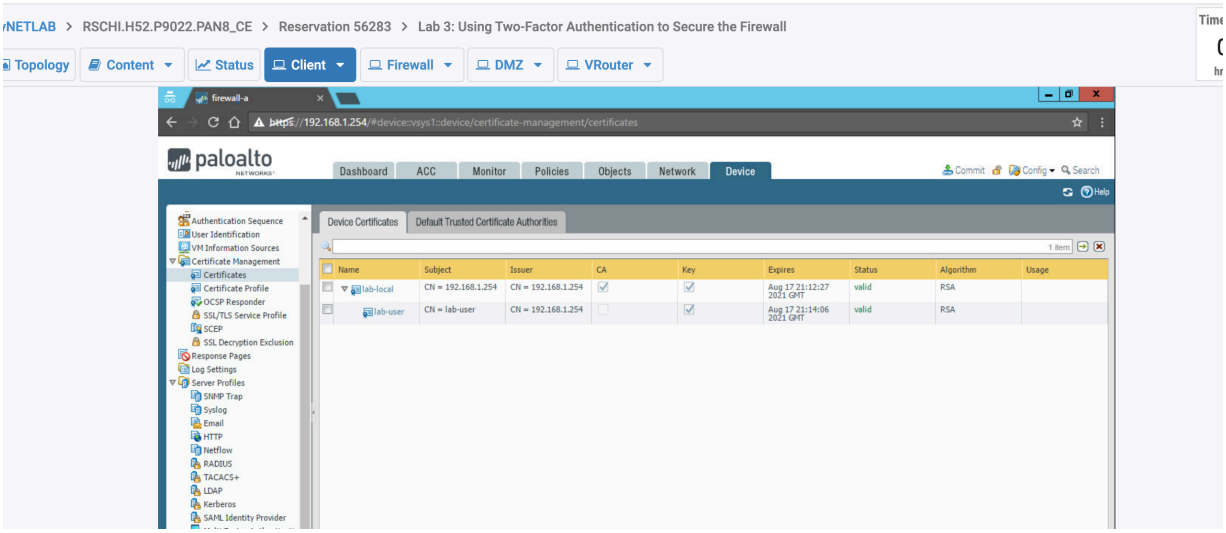
3 Commit the changes to the lab config, Commit of the config done.

3.1 Create Local User Account



3.2 Generate Certificates

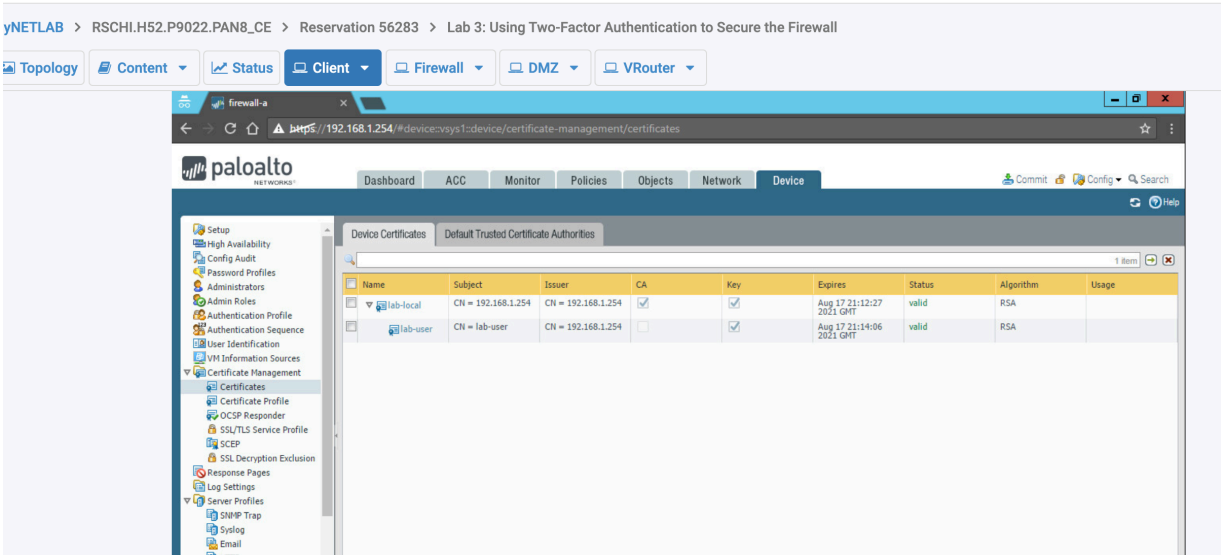
Generate two certificates. The first is a self-signed Root Certificate Authority (CA) certificate, which is the top-most certificate in the certificate chain. The Firewall can use this certificate to automatically issue certificates for other uses. In this lab, use the Root CA certificate to generate a certificate for use on the Client machine that is associated with local user account, lab-user.



3.3 Create a Certificate Profile In this section, create a certificate profile. A certificate profile defines user and device authentication for multiple services on the Firewall. The profile specifies which certificates to use, how to verify certificate revocation status and how that status constrains access. In this lab, the certificate profile is created to tell the Firewall to use the common-name of the certificate as a username. Then tell the Firewall to use this Certificate Profile to authenticate users.

3.4 Export Certificate and Commit

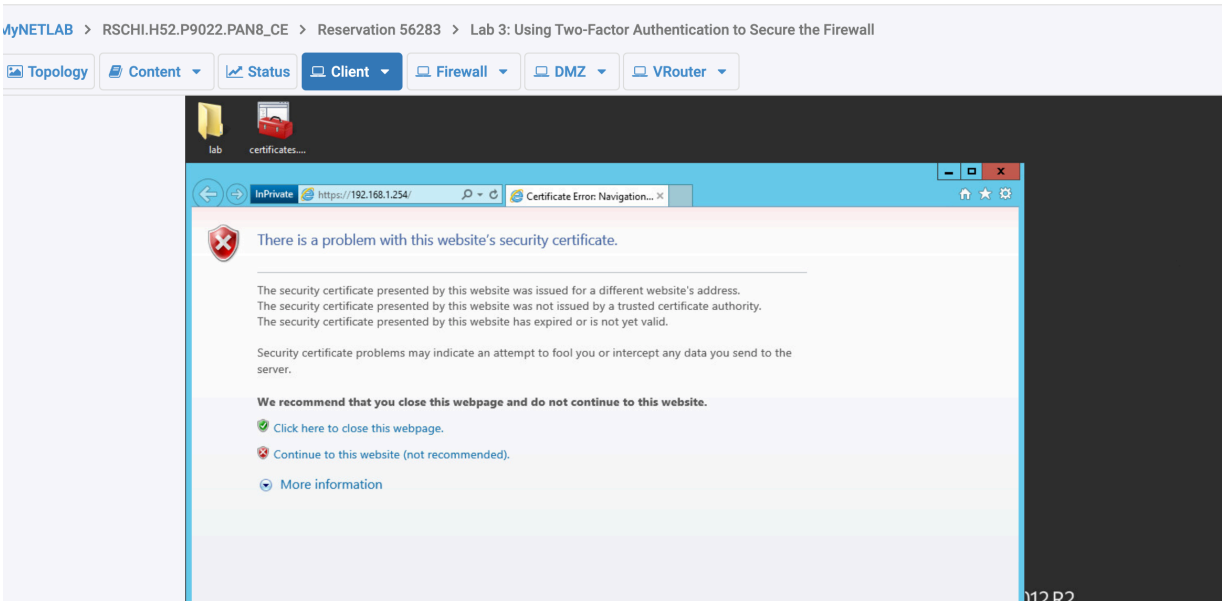
In this section, export the lab-user certificate you generated on the Firewall. Then commit changes, causing the Firewall to start using certificates for authentication.



3.5 Test Connectivity and Import Certificate on the Client

In this section, test connectivity to the Firewall. Then, you will import the labuser certificate on the Client machine and try again. Access to the 192.168.1.254 due to certificate error.

cybersecurity-essentials-1 Palo Alto Networks Cybersecurity Essentials I

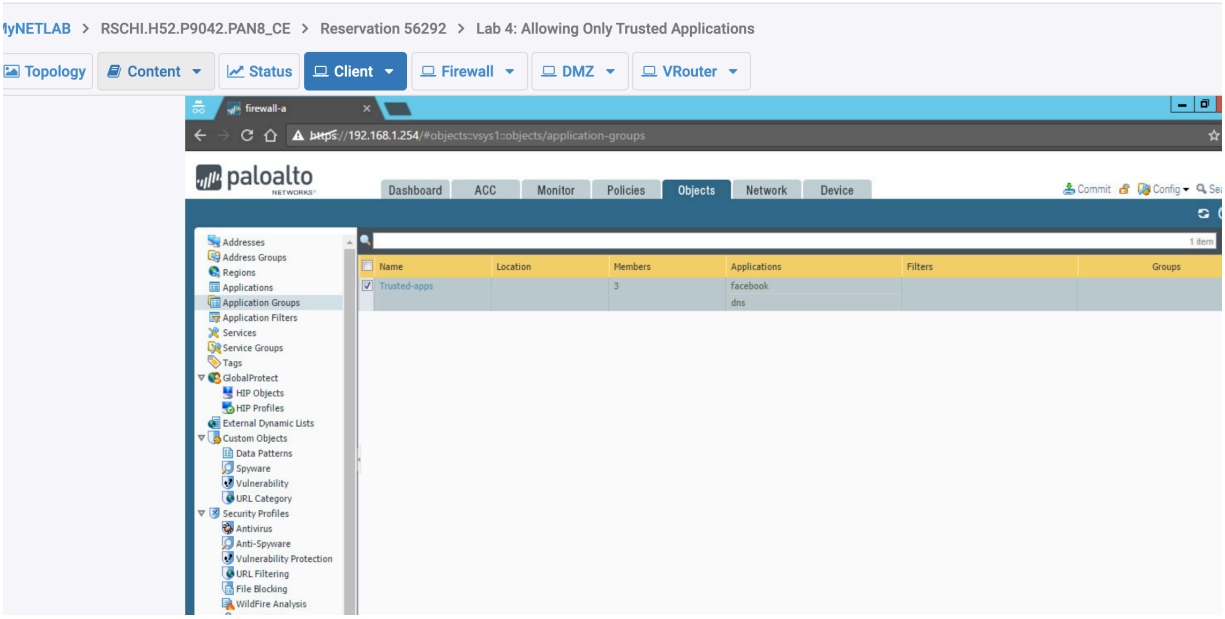


Lab 4: Allowing Only Trusted Applications

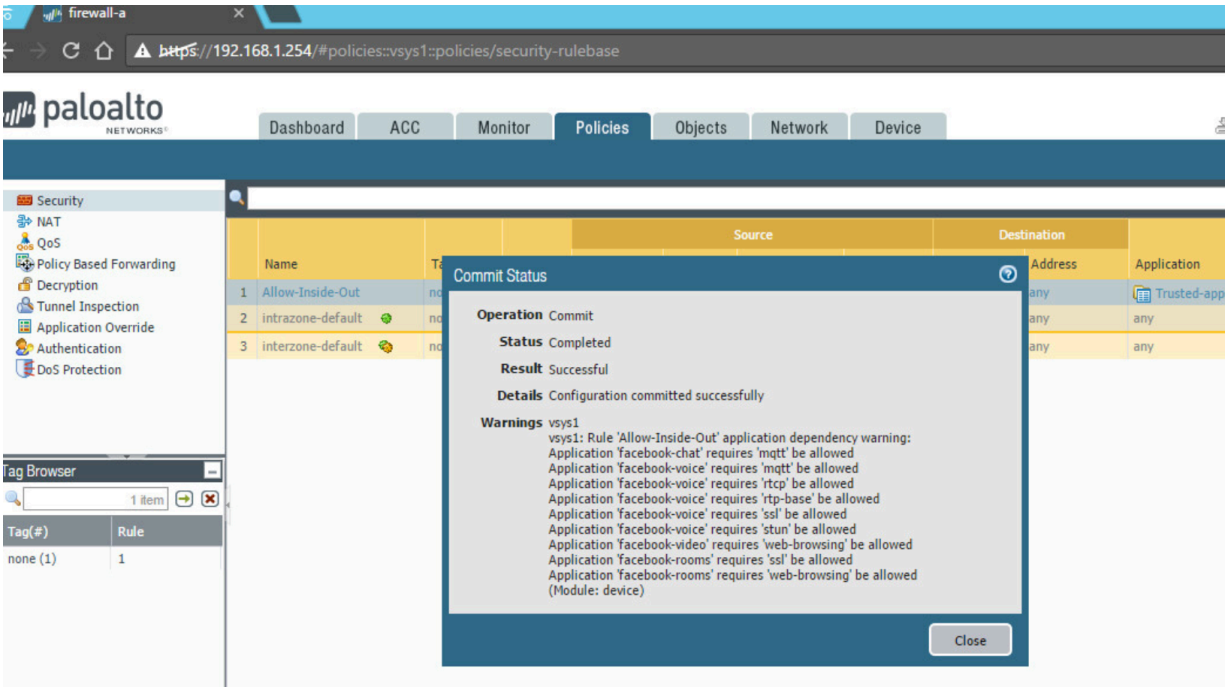
==========

Introduction In this lab, you will configure the Firewall to only allow trusted applications by creating an application group and adding it to an existing security policy. Objective In this lab, you will perform the following tasks: • Create an Application Group • Modify Security Policy • Commit and Test

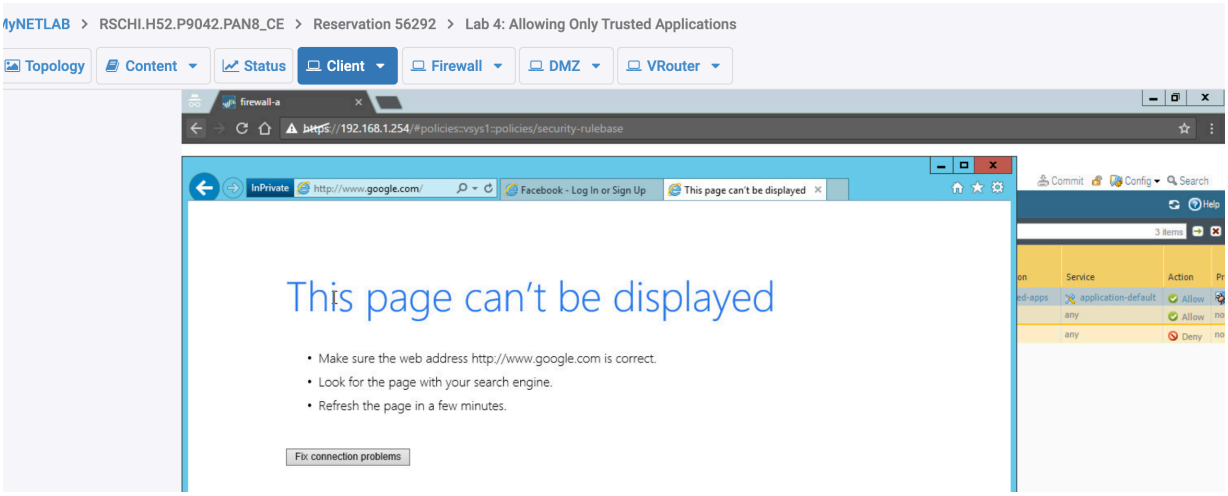
4.1 4.1 Create an Application Group
In this section, you will create an application group. To simplify the creation of security policies, applications requiring the same security settings can be combined by creating an application group.

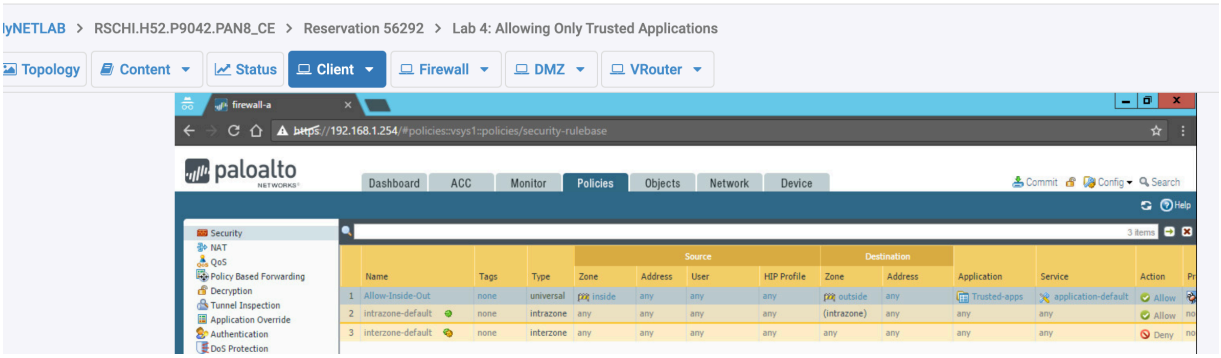


4.2 Modify Security Policy In this section, you will modify the Allow-Inside-Out security policy to only allow the applications in the application group, Trusted-Apps, you created earlier.



4.3 Commit and Test In this section, you will commit changes to the Firewall. Then, you will test the security policy you modified earlier. Next, you will add an additional application to the application group, Trusted-Apps. Finally, you will verify the additional application is allowed.





Lab 5: Managing Certificates

Introduction

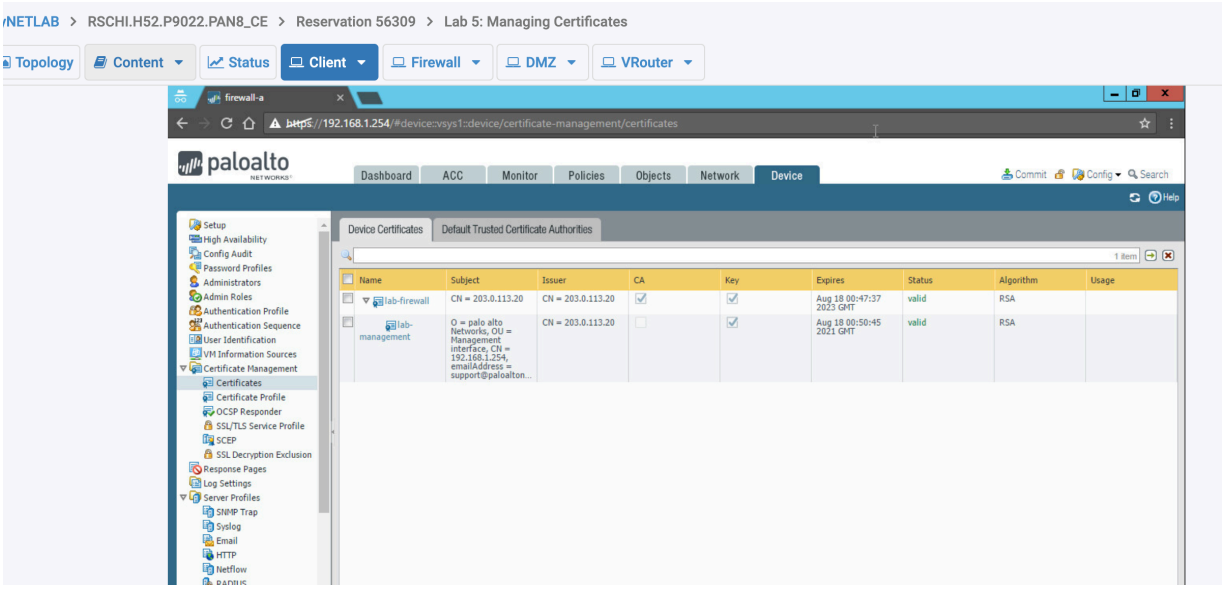
In this lab, generate a Self-Signed Root Certificate Authority (CA) certificate and replace the certificate for inbound management traffic. Then, you will import the root CA certificate on the Client machine.

Objective

You will perform the following tasks: • Generate Certificates • Replace the Certificate for Inbound Management Traffic • Export Certificate and Commit • Test Connectivity and Import Certificate on the Client

5.1 Commit the lab config and save changes
5.2 Generate Certificates

In this lab generate two certificates. The first is a self-signed Root Certificate Authority (CA) certificate, which is the top-most certificate in the certificate chain. The Firewall can use this certificate to automatically issue certificates for other uses. In this lab, use the Root CA certificate to generate a new certificate for the Firewall to use for Inbound Management Traffic, replacing the default certificate issued specifically for this lab environment.

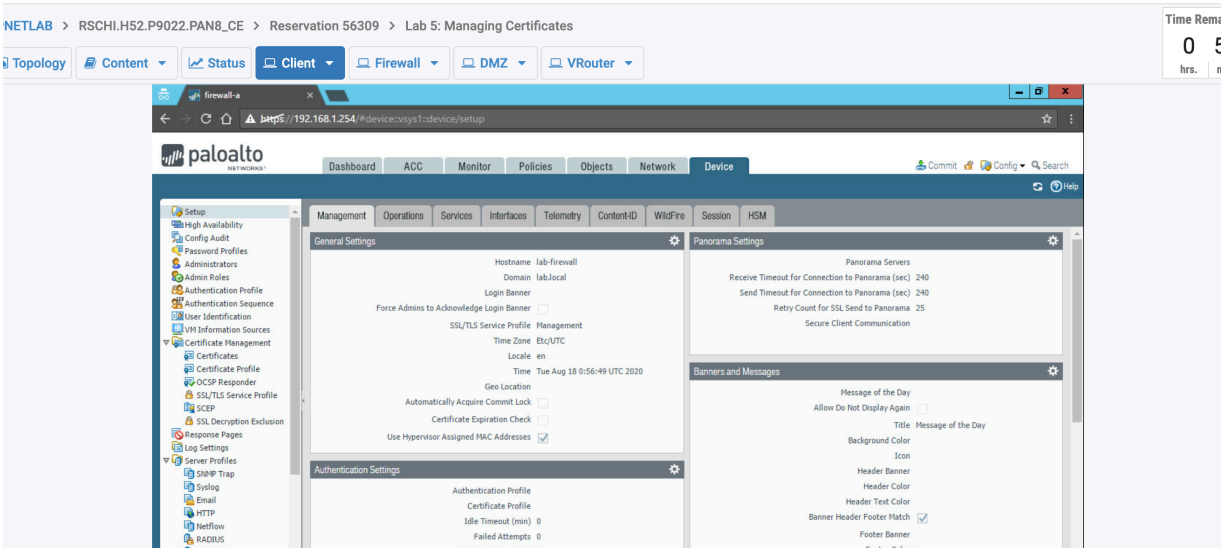


5.3 Replace the Certificate for Inbound Management Traffic

In this section, you will replace the certificate for inbound management traffic. When you boot the Firewall for the first time, it automatically generates a default certificate that enables HTTPS access to the web interface over the management (MGT) interface. To improve the security of inbound management traffic, you will configure a SSL/TLS Service Profile to replace the default certificate with the lab-management certificate you specifically created for this purpose. Then, you will apply the SSL/TLS Service Profile to inbound management traffic.

5.3 Export Certificate and Commit

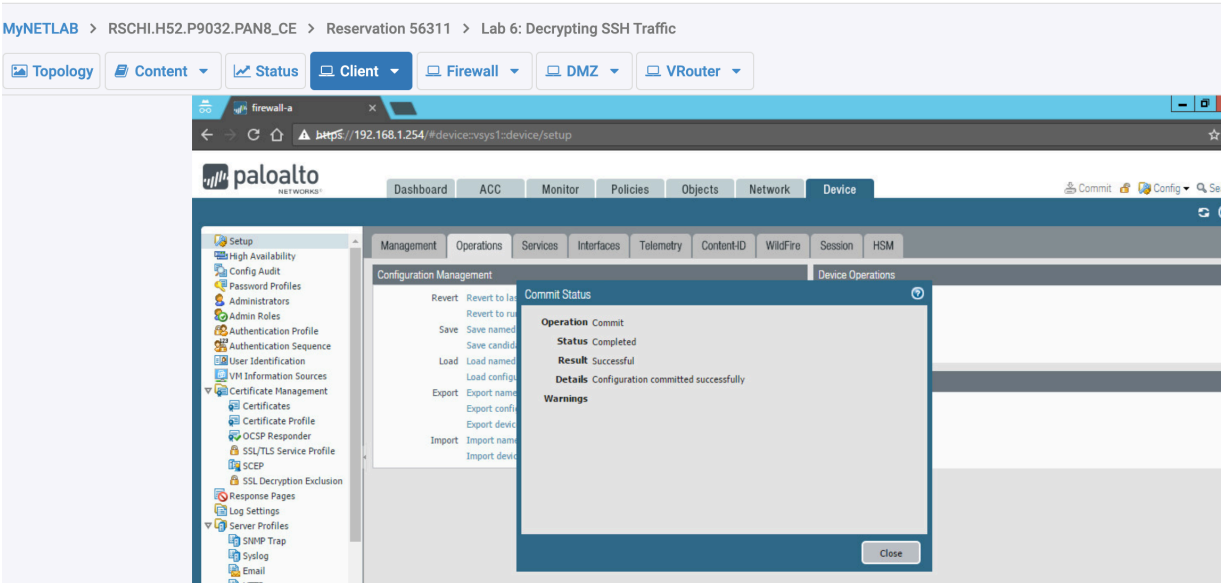
In this section, you will export the root CA certificate, lab-firewall. Then, you will commit your changes to the Firewall.



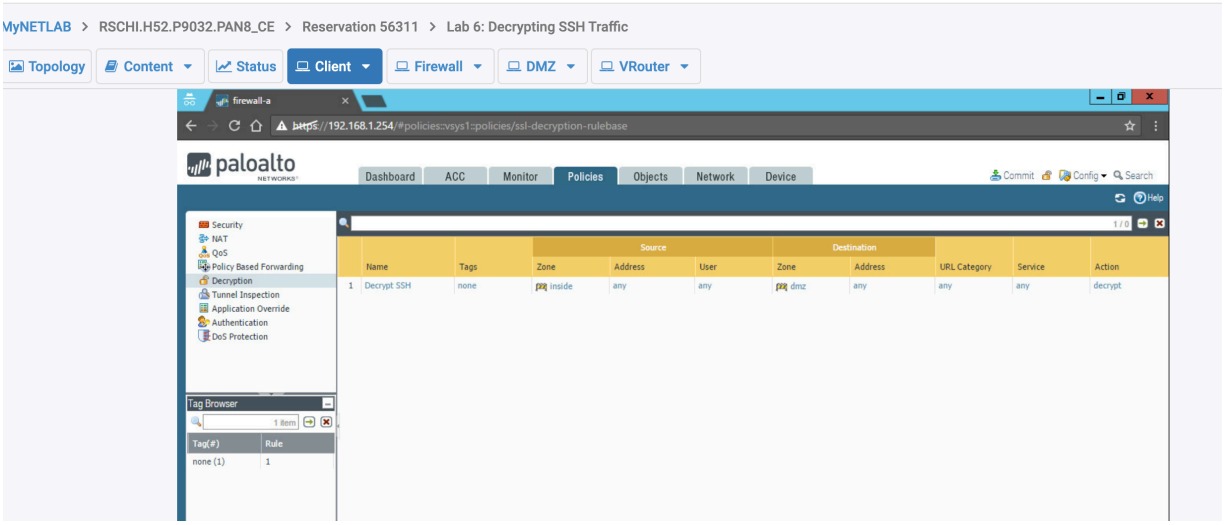
Lab 6: Decrypting SSH Traffic

Introduction In this lab, you will decrypt SSH traffic by creating a decryption policy. Then, you will use PuTTY to SSH to the DMZ server (traffic-generator) and monitor the traffic logs on the Firewall, to show the SSH session has been decrypted. Objective In this lab, you will perform the following tasks: • Create a Decryption Policy and Commit • Create a SSH session with PuTTY and Verify Decryption Is Working • Disable Decryption Policy

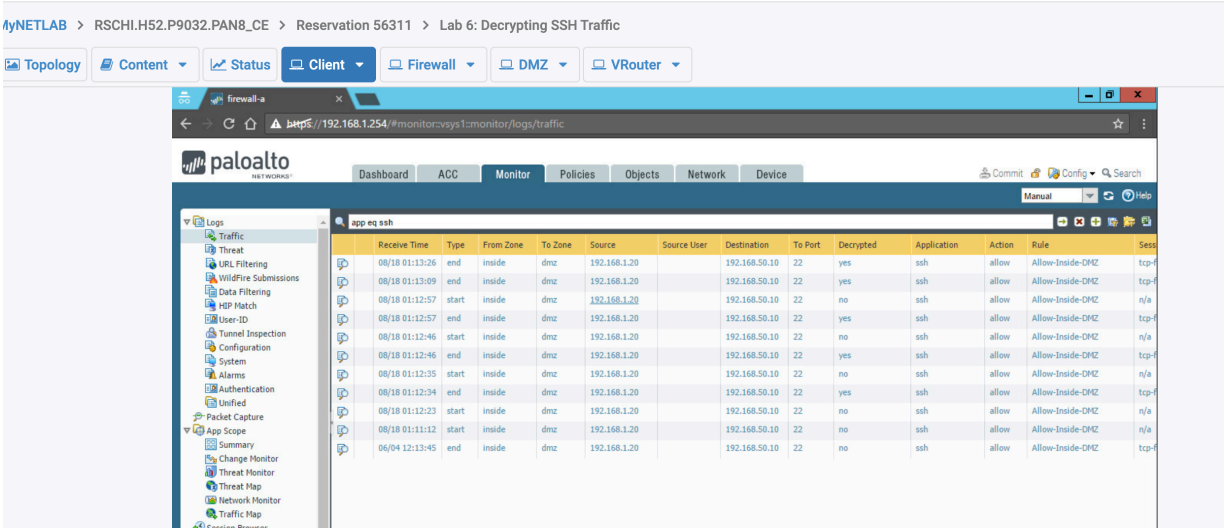
cybersecurity-essentials-1 Palo Alto Networks Cybersecurity Essentials I



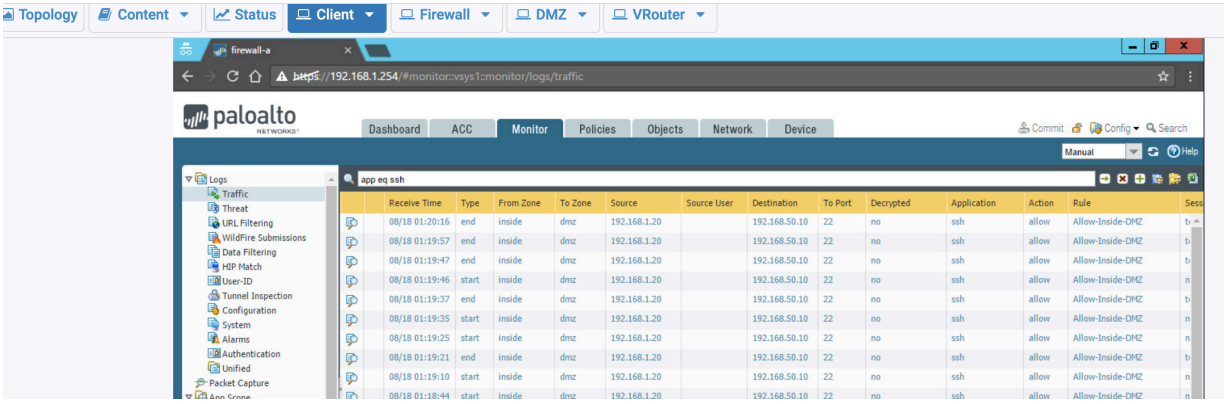
6.1 Create a Decryption Policy and Commit In this section, you will create a decryption policy. Decryption Policies allow administrators to stop threats that would otherwise remain hidden in encrypted traffic and help prevent sensitive content from leaving an organization. Then, you will commit your changes to the Firewall.



6.2 Create a SSH Session with PuTTY and Verify Decryption Is Working In this section, you will create a SSH session with PuTTY to the DMZ server (trafficgenerator), which travels through internal interface of the Firewall. Then, you will monitor the traffic logs to verify decryption is working.



6.3 Disable the Decryption Policy
disable the decryption policy that was created earlier and verify the Firewall is no longer decrypting the SSH traffic.

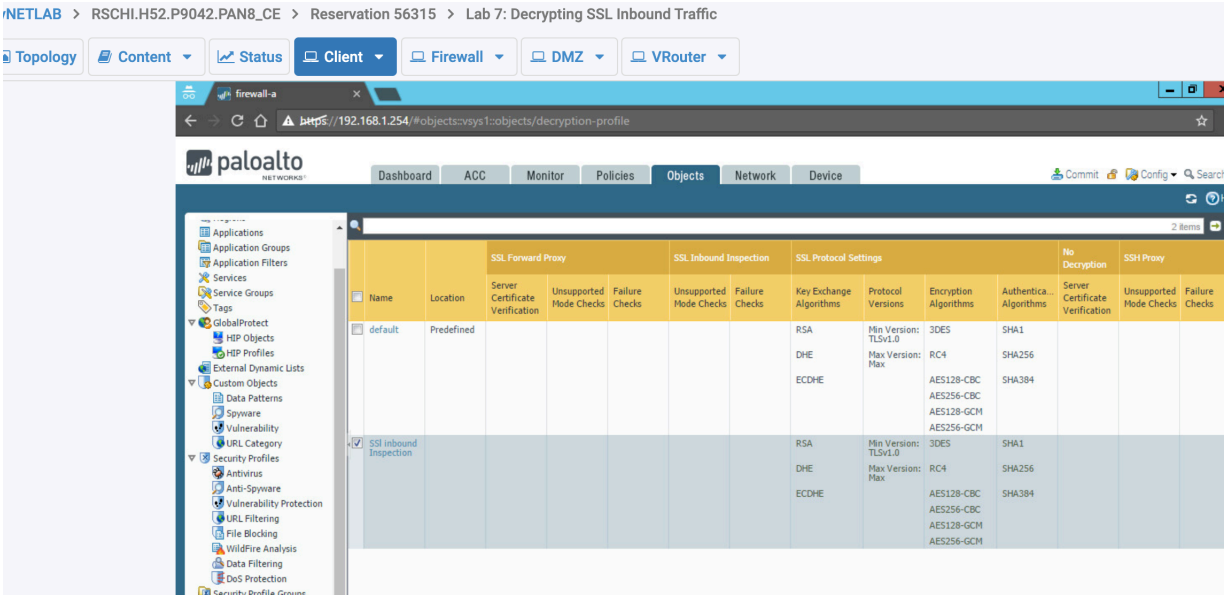


Lab 7: Decrypting SSL Inbound Traffic

Introduction In this lab, you will decrypt SSL inbound traffic and inspect SSL traffic from the Client machine to the DMZ server. When the SSL server certificate is loaded on the Firewall, and an SSL decryption policy is configured for the inbound traffic, the device can then decrypt and read the traffic as it forwards it along. No changes are made to the packet data, and the secure channel is built from the client system to the internal server. The Firewall can then detect malicious content and control applications running over this secure channel. Objective In this lab, you will perform the following tasks: • Download the SSL Certificate from DMZ Server • Import SSL Certificate • Create a Decryption Profile • Create a Decryption Policy • Commit and Test Decryption Policy • Disable Decryption Policy

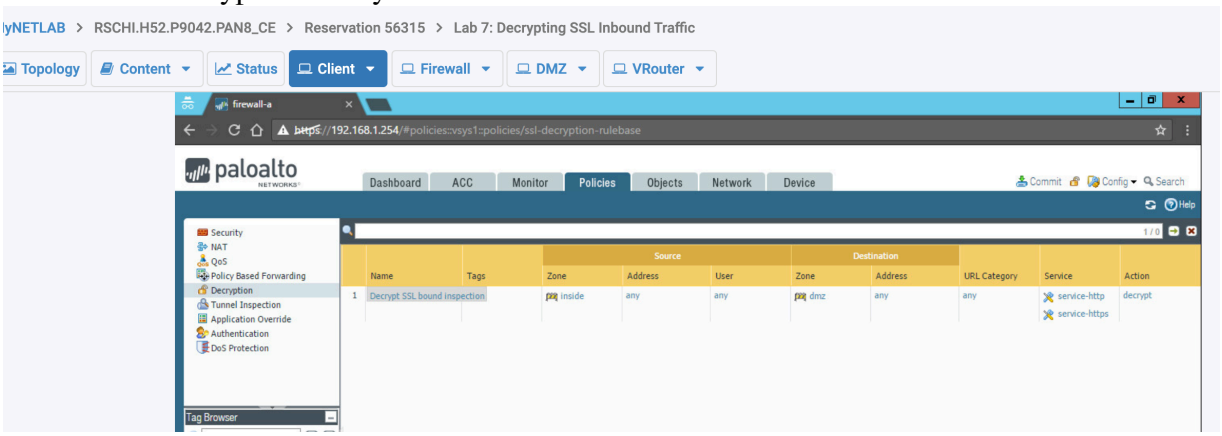
7.1 Download the SSL Certificate from DMZ Server

7.2 Import SSL Certificate In this section, you will import the SSL Certificate you downloaded from the DMZ server to the Firewall. This will later be used to create a decryption profile

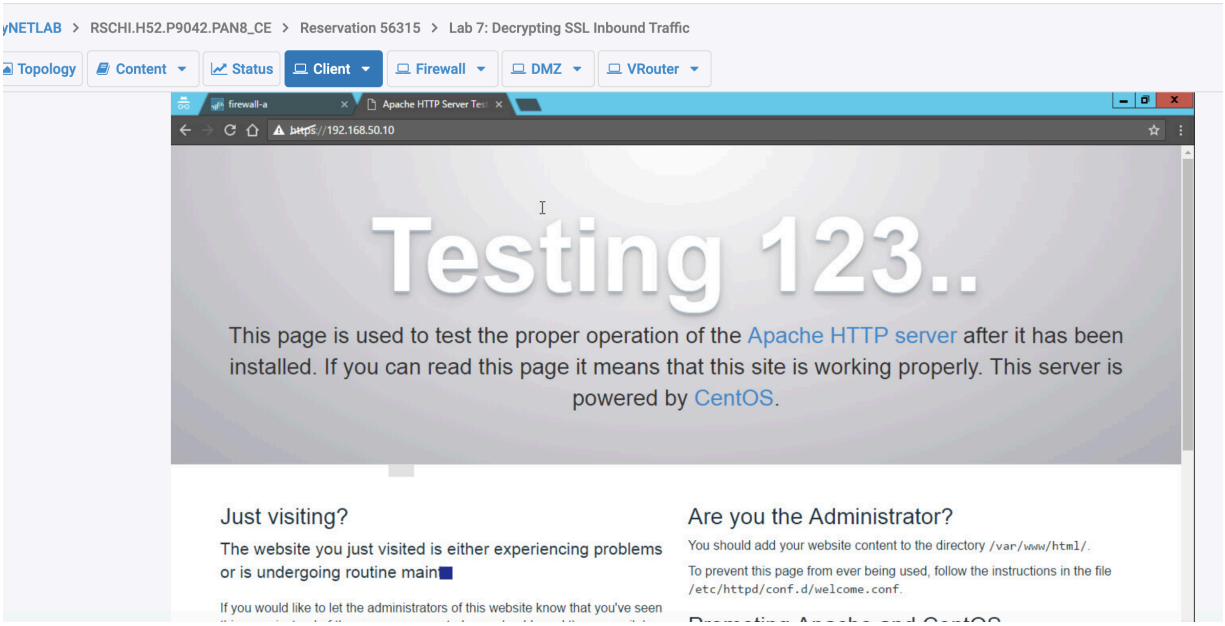


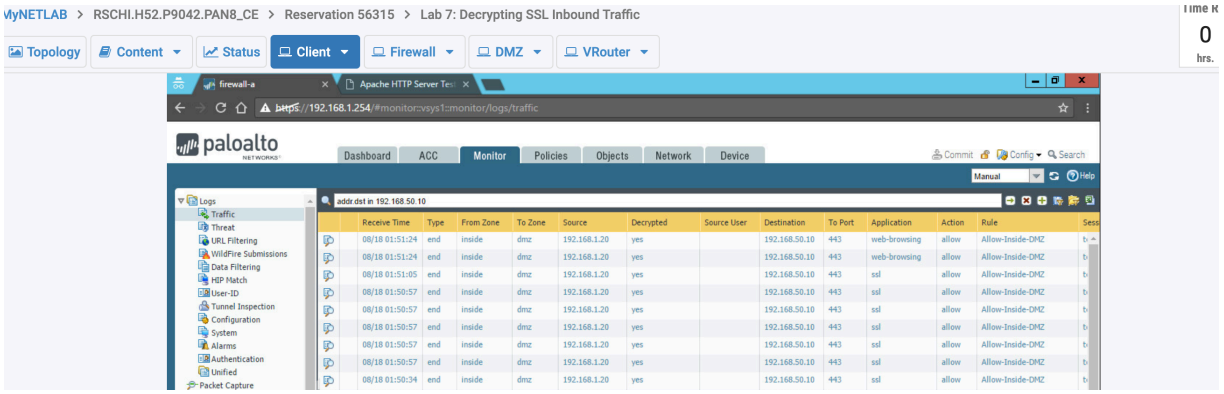
7.3 Create a Decryption Profile In this section, you will create a decryption profile. Decryption profiles allow administrators to perform checks on both decrypted traffic and traffic that would have been excluded from decryption. After a decryption profile is created, it can then be attached to a decryption policy rule that will enforce the profile settings.

7.4 Create a Decryption Policy



7.5 Commit and Test Decryption Policy In this section, you will commit your changes to the Firewall. Then, you will test the decryption policy you created earlier.

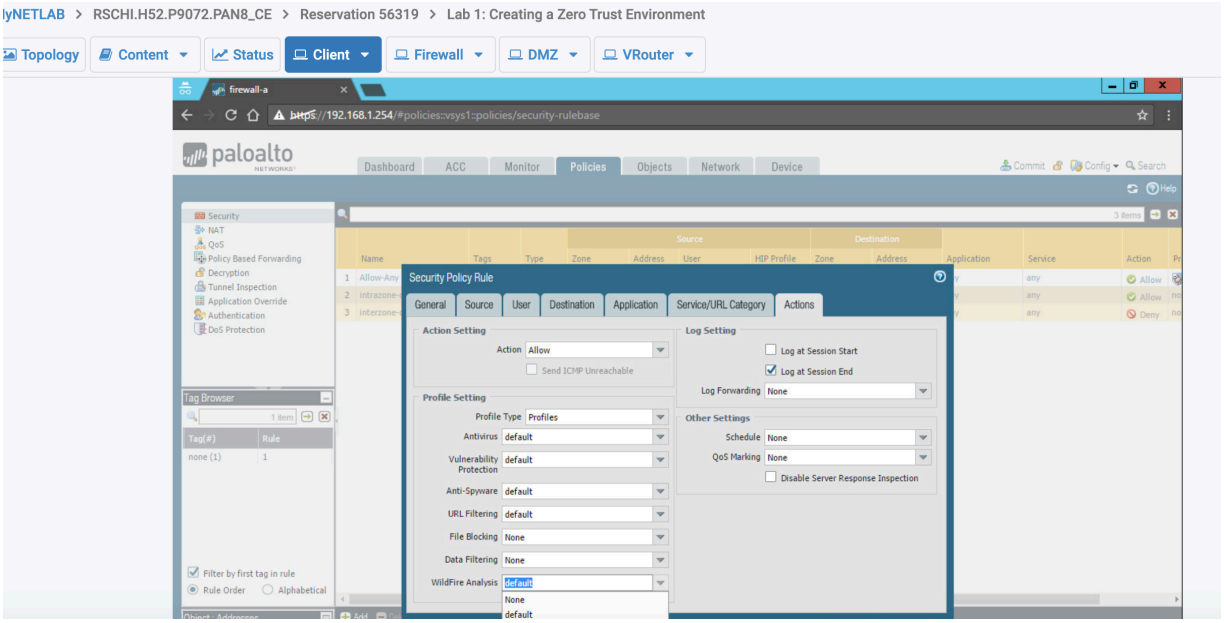




==========

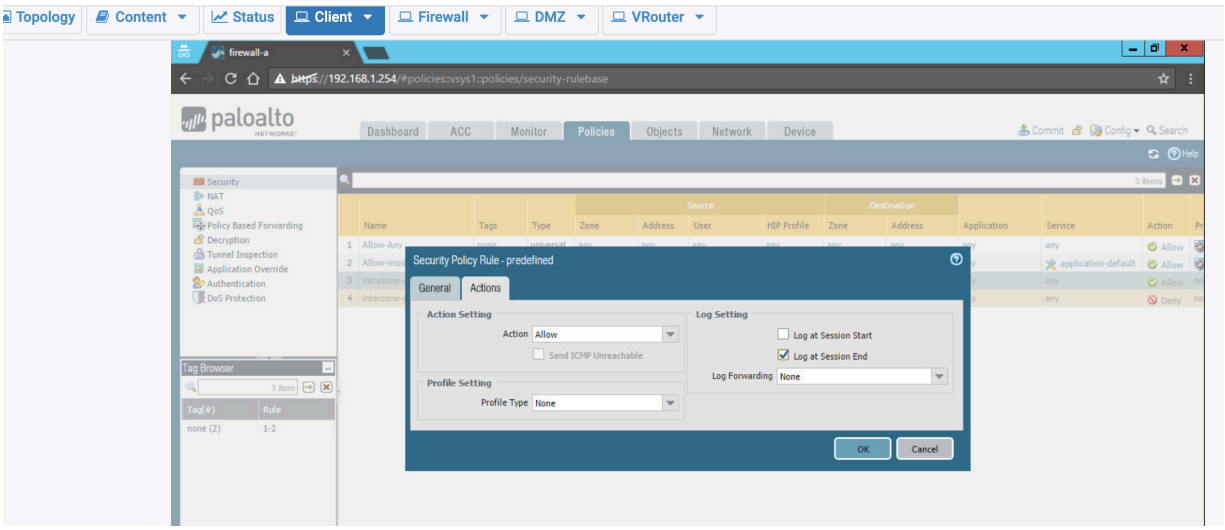
Student Project

Screenshot 1

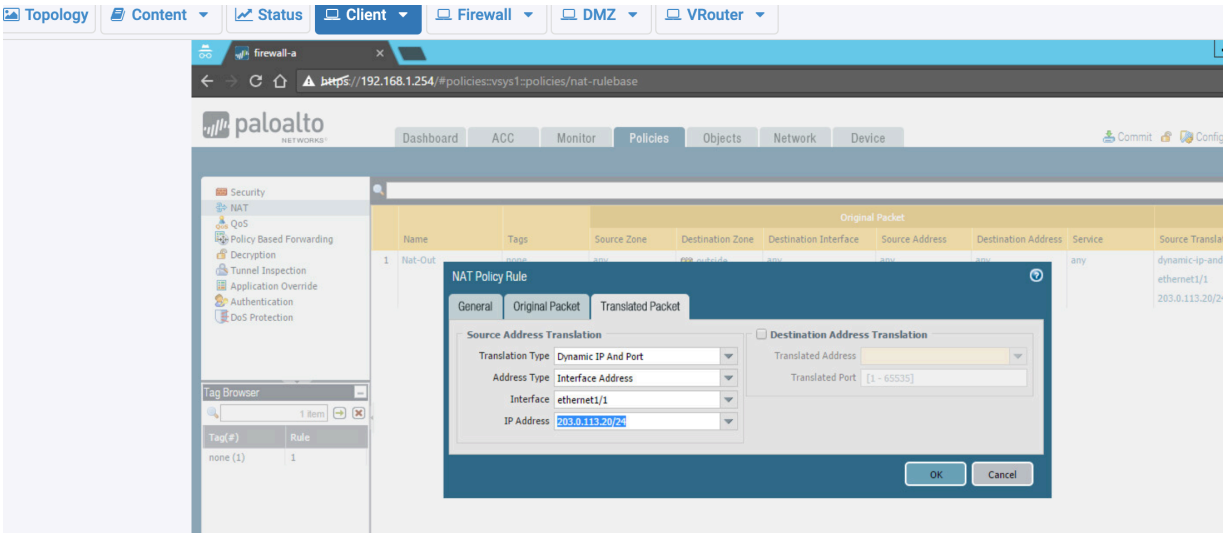


Screenshot 2

cybersecurity-essentials-1 Palo Alto Networks Cybersecurity Essentials I



Screenshot 3



Screenshot 4