

Anjali Jain

Lab 1: Creating a Zero Trust Environment

Introduction

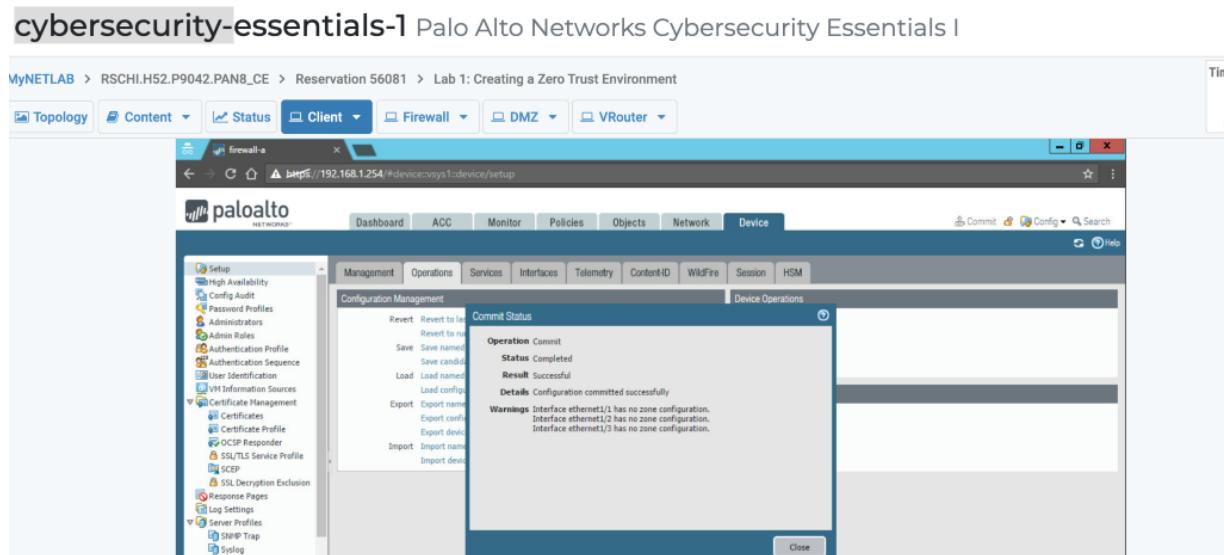
In this lab, configure the Firewall with three zones: inside, outside, and dmz. Then, I have applied security policies to these zones to ensure all traffic between zones is being monitored by the Firewall.

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

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features
ethernet1/1	Layer3		Up	203.0.113.20/24	VR-1	Untagged	none	outside	
ethernet1/2	Layer3	allow-mgmt	Up	192.168.1.1/24	VR-1	Untagged	none	inside	
ethernet1/3	Layer3	allow-ping	Up	192.168.50.1/24	VR-1	Untagged	none	dmz	
ethernet1/4			Up	none	none	Untagged	none	none	

lyNETLAB > RSCHI.H52.P9042.PAN8_CE > Reservation 56081 > Lab 1: Creating a Zero Trust Environment

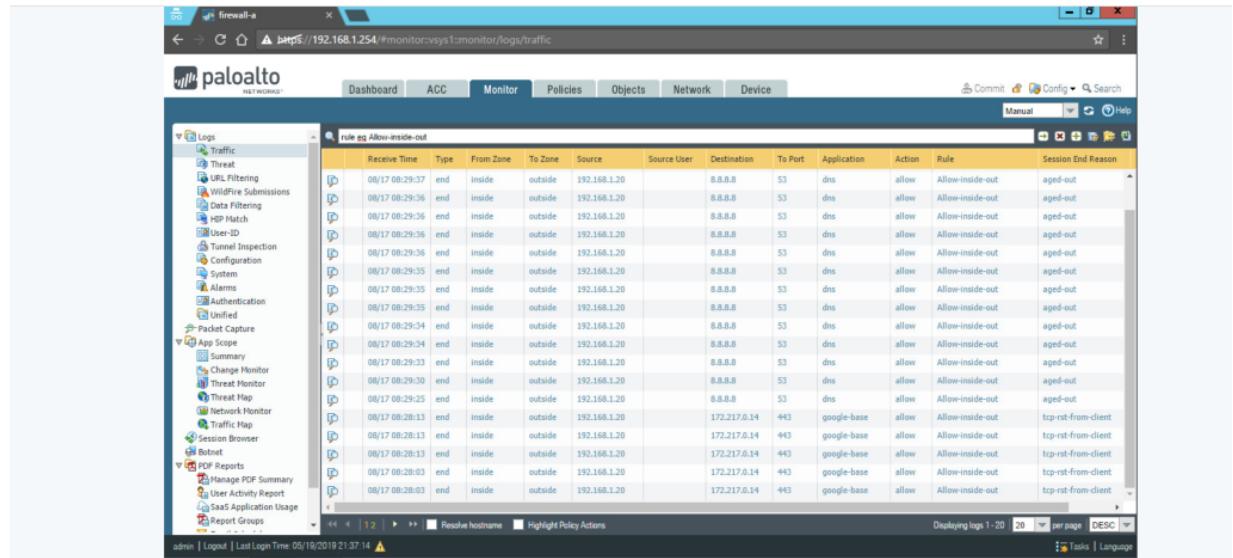
Name	Tags	Type	Zone	Address	User	HDP Profile	Destination	Application	Service	Action	Priority
1 Allow-inside-out	none	universal	px inside	any	any	any	px outside	any	any	application-default	Allow
2 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	application-default	Allow
3 interzone-default	none	interzone	any	any	any	any	any	any	any	application-default	Deny

C) Create a NAT Policy

Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation
1 inside-NAT-outside	none	px inside	px outside	any				dynamic-ip-and-port ethernet1/1 203.0.113.20/24

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



The screenshot shows the Palo Alto Networks Firewall interface. The left sidebar has a tree view with categories like Logs, Threat, URL Filtering, Data Filtering, User-ID, Tunnel Inspection, Configuration, Authentication, and PDF Reports. The main pane displays a table titled "rule eq Allow-inside-out" with columns: Receive Time, Type, From Zone, To Zone, Source, Source User, Destination, To Port, Application, Action, Rule, and Session End Reason. The table lists numerous entries from 08/17 08:29:37 to 08/17 08:29:35, mostly for dns traffic from 192.168.1.20 to 8.8.8.8. The interface includes a toolbar at the top with tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, Device, and a search bar. At the bottom, there are buttons for Commit, Config, and Help.

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.

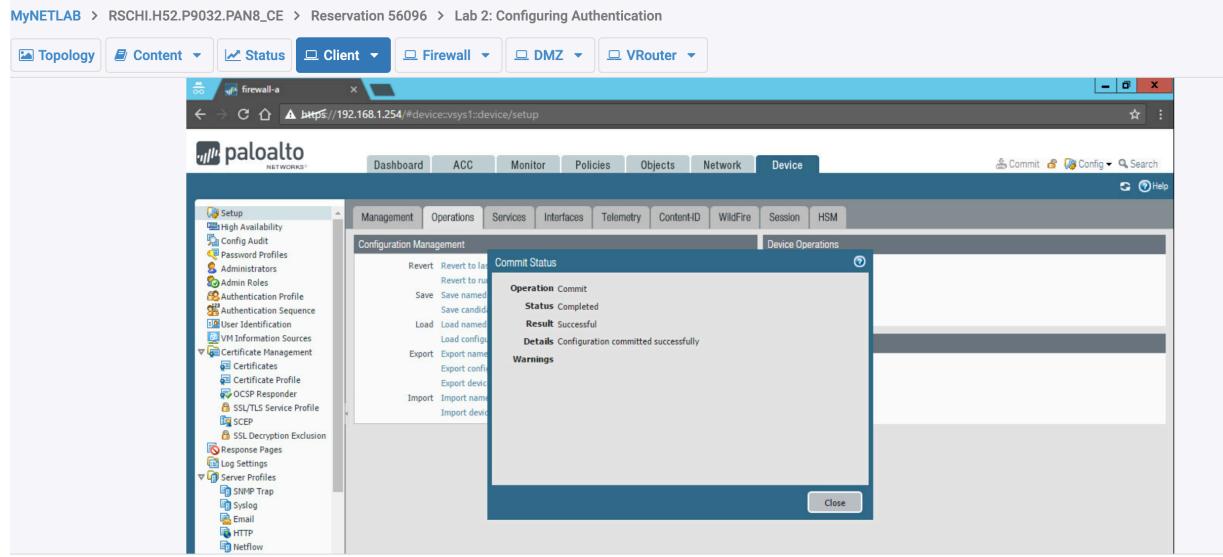
Objective

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

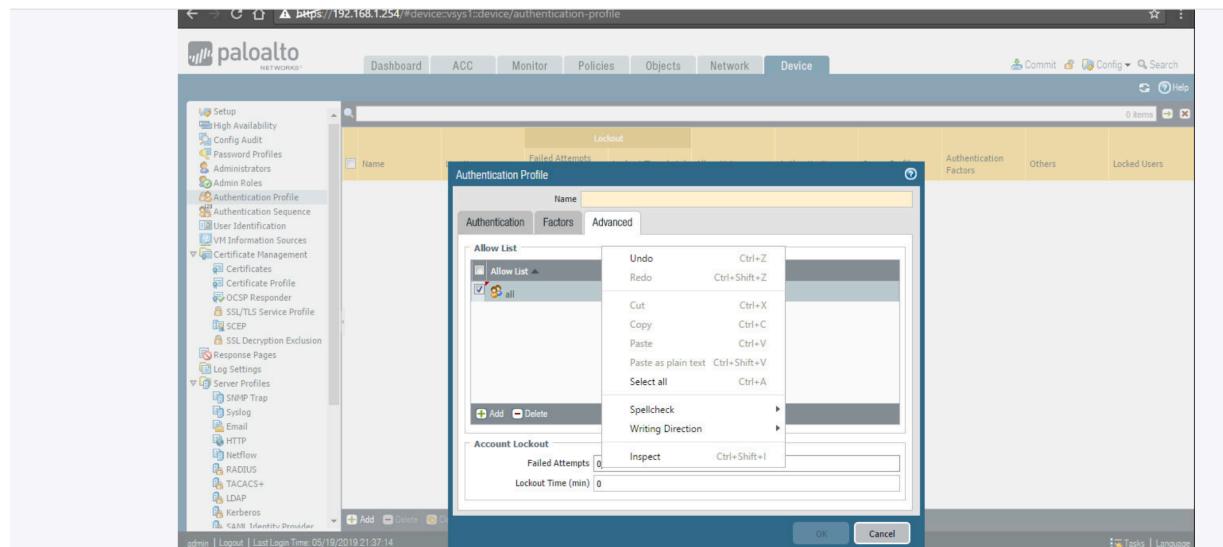
A) commit the changes for this lab.

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

cybersecurity-essentials-1 Palo Alto Networks Cybersecurity Essentials I

The screenshot shows the Palo Alto Networks Firewall configuration interface. The left sidebar contains various configuration categories like GlobalProtect, Applications, Services, and Security Profiles. The main pane is titled 'Captive Portal' under the 'User Mapping' tab. It displays settings for enabling the captive portal, including an idle timer of 15 minutes, a global protect network port of 4501, and authentication prompts for UDP. There are sections for Certificate Authentication and NTLM Authentication, both set to 'None'. Buttons for 'OK' and 'Cancel' are at the bottom right.

d) Default-web form cloned

cybersecurity-essentials-1 Palo Alto Networks Cybersecurity Essentials I

The screenshot shows the Palo Alto Networks Firewall configuration interface. The left sidebar lists various objects including Applications, Services, and Security Profiles. The main pane shows a table of authentication objects. One row is selected, showing 'default-web-form' with 'Predefined' location, 'web-form' authentication method, and no assigned authentication profile. Other rows include 'default-browser-challenge', 'default-no-captive-portal', and 'default-web-form-1'.

Name	Location	Authentication Method	Authentication Profile
default-web-form	Predefined	web-form	
default-browser-challenge	Predefined	browser-challenge	
default-no-captive-portal	Predefined	no-captive-portal	
default-web-form-1		web-form	

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

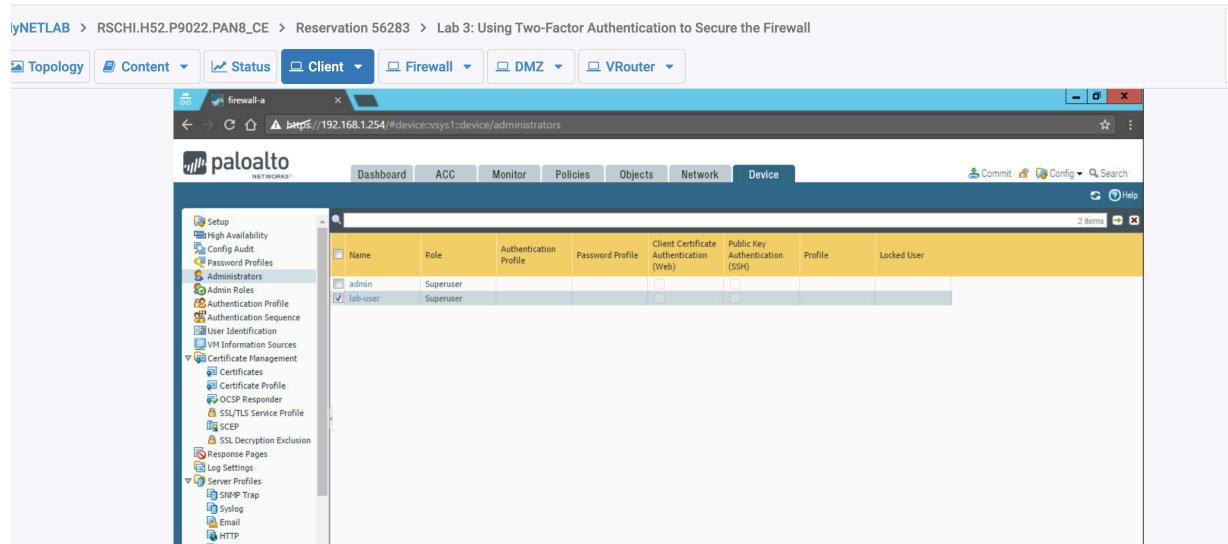
In this lab, perform the following tasks:

- 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



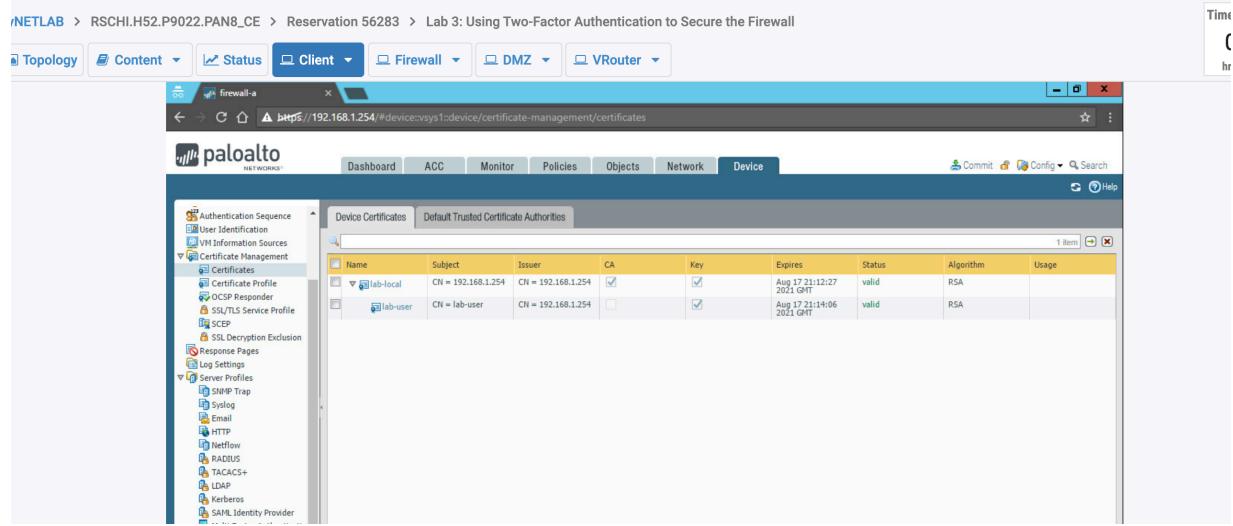
The screenshot shows the Palo Alto Networks Device Manager interface. The left sidebar navigation menu includes 'Setup' (High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, VM Information Sources), 'Certificate Management' (Certificates, Certificate Profile, OCSP Responder, SSL/TLS Service Profile, SCEP, SSL Decryption Exclusion, Response Pages), 'Log Sources' (Log Profiles, SHMP Trap, Syslog, Email, HTTP), and 'System' (Setup, Configuration, Log, Help). The main content area displays a table titled 'Administrators' with the following data:

Name	Role	Authentication Profile	Password Profile	Client Certificate (Web)	Public Key Authentication (SSH)	Profile	Locked User
admin	Superuser						
lab-user	Superuser						

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.

Cybersecurity-essentials-I Palo Alto Networks Cybersecurity Essentials I



The screenshot shows the Palo Alto Networks Device Management interface. The left sidebar has a tree view with 'Certificate Management' selected, which is expanded to show 'Certificates'. Under 'Certificates', there are several items: 'Certificate Profile', 'OCSP Responder', 'SSL/TLS Service Profile', 'SCEP', 'SSL Decryption Exclusion', 'Response Pages', and 'Log Settings'. The main content area has two tabs: 'Device Certificates' (selected) and 'Default Trusted Certificate Authorities'. The 'Device Certificates' tab displays a table with one item:

Name	Subject	Issuer	CA	Key	Expires	Status	Algorithm	Usage
lab-local	CN = 192.168.1.254	CN = 192.168.1.254	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Aug 17 21:12:27 2021 GMT	valid	RSA	
lab-user	CN = lab-user	CN = 192.168.1.254	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Aug 17 21:14:06 2021 GMT	valid	RSA	

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.

cybersecurity-essentials-1 Palo Alto Networks Cybersecurity Essentials I

MyNETLAB > RSCHI.H52.P9022.PAN8_CE > Reservation 56283 > Lab 3: Using Two-Factor Authentication to Secure the Firewall

The screenshot shows the Palo Alto Networks Device Certificate Management interface. On the left, a navigation tree includes Setup, High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, VM Information Sources, Certificate Management, Certificates, Certificate Profile, OCSP Responder, SSL/TLS Service Profile, SCEP, SSL Decryption Exclusion, Response Pages, Log Settings, Server Profiles, SNMP Trap, Syslog, and Email. The 'Certificates' node is selected. The main pane displays 'Device Certificates' and 'Default Trusted Certificate Authorities'. A table lists two certificates:

Name	Subject	Issuer	CA	Key	Expires	Status	Algorithm	Usage
lab-local	CN = 192.168.1.254	CN = 192.168.1.254	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Aug 17 21:12:27 2021 GMT	valid	RSA	
lab-user	CN = lab-user	CN = 192.168.1.254	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Aug 17 21:14:06 2021 GMT	valid	RSA	

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

MyNETLAB > RSCHI.H52.P9022.PAN8_CE > Reservation 56283 > Lab 3: Using Two-Factor Authentication to Secure the Firewall

The screenshot shows a Microsoft Edge browser window with an 'InPrivate' tab open. The address bar shows 'https://192.168.1.254/'. A red shield icon with a white 'X' indicates a security error. The page content reads:

There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website's address.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website has expired or is not yet valid.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.
 Continue to this website (not recommended).
 More information

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.

The screenshot shows the Palo Alto Networks Management Console interface. The top navigation bar includes tabs for Topology, Content, Status, Client (selected), Firewall, DMZ, and VRouter. The URL in the browser is https://192.168.1.254/#objects:vsys1::objects/application-groups. The main content area displays the 'Objects' tab selected under the 'Applications' category. A table lists the 'Trusted-apps' application group, which has three members: facebook and dns. The left sidebar contains a navigation tree with categories like Addresses, Address Groups, Regions, Applications, Application Groups (which is currently selected), Services, Service Groups, Tags, GlobalProtect, External Dynamic Lists, Custom Objects, and Security Profiles.

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.

Commit Status

- Operation:** Commit
- Status:** Completed
- Result:** Successful
- Details:** Configuration committed successfully
- Warnings:** vsys1: Rule 'Allow-Inside-Out' application dependency warning:
Application 'Facebook-chat' requires 'mqtt' be allowed
Application 'Facebook-voice' requires 'mqtt' be allowed
Application 'Facebook-voice' requires 'tcp' be allowed
Application 'Facebook-voice' requires 'tp-base' be allowed
Application 'Facebook-voice' requires 'ssl' be allowed
Application 'Facebook-video' requires 'stun' be allowed
Application 'Facebook-video' requires 'web-browsing' be allowed
Application 'Facebook-rooms' requires 'ssl' be allowed
Application 'Facebook-rooms' requires 'web-browsing' be allowed
(Module: device)

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.

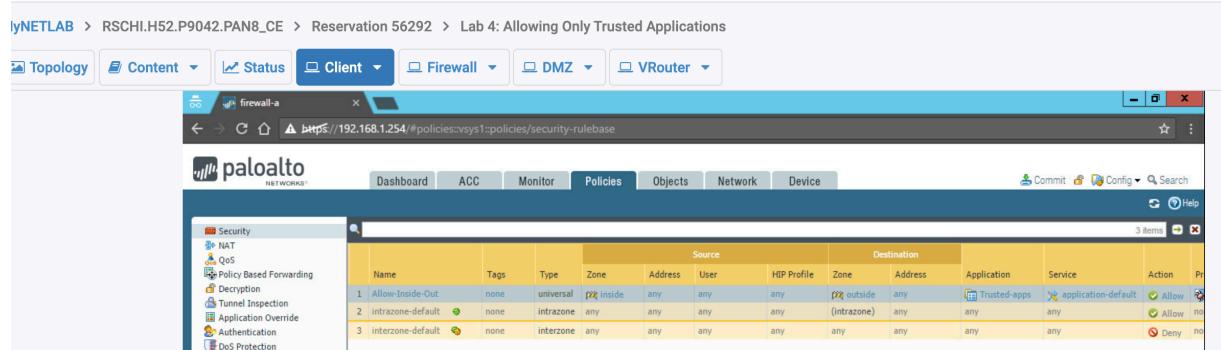
This page can't be displayed

- Make sure the web address <http://www.google.com/> is correct.
- Look for the page with your search engine.
- Refresh the page in a few minutes.

Security Rulebase

Action	Service	Action	Protocol
allow	application-default	allow	any
deny	any	deny	any

cybersecurity-essentials-I | Palo Alto Networks Cybersecurity Essentials I



The screenshot shows the Palo Alto Networks Firewall interface. The top navigation bar includes tabs for Topology, Content, Status, Client, Firewall, DMZ, and VRouter. The main window displays the 'Security' section under the 'Policies' tab. A table titled 'Source' lists three security rules:

Name	Tags	Type	Zone	Address	User	HTTP Profile	Zone	Address	Application	Service	Action	Pr
1 Allow-Inside-Out	none	universal	p ₁ inside	any	any	any	p ₂ outside	any	Trusted-apps	application-default	Allow	80
2 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	no
3 interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny	80

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.

Name	Subject	Issuer	CA	Key	Expires	Status	Algorithm	Usage
lab-firewall	CN = 203.0.113.20	CN = 203.0.113.20	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Aug 18 00:47:37 2023 GMT	valid	RSA	
lab-management	O = palo alto Networks, OU = Management interface, CN = 192.168.1.254, emailAddress = support@paloalto...	CN = 203.0.113.20	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Aug 18 00:50:45 2021 GMT	valid	RSA	

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

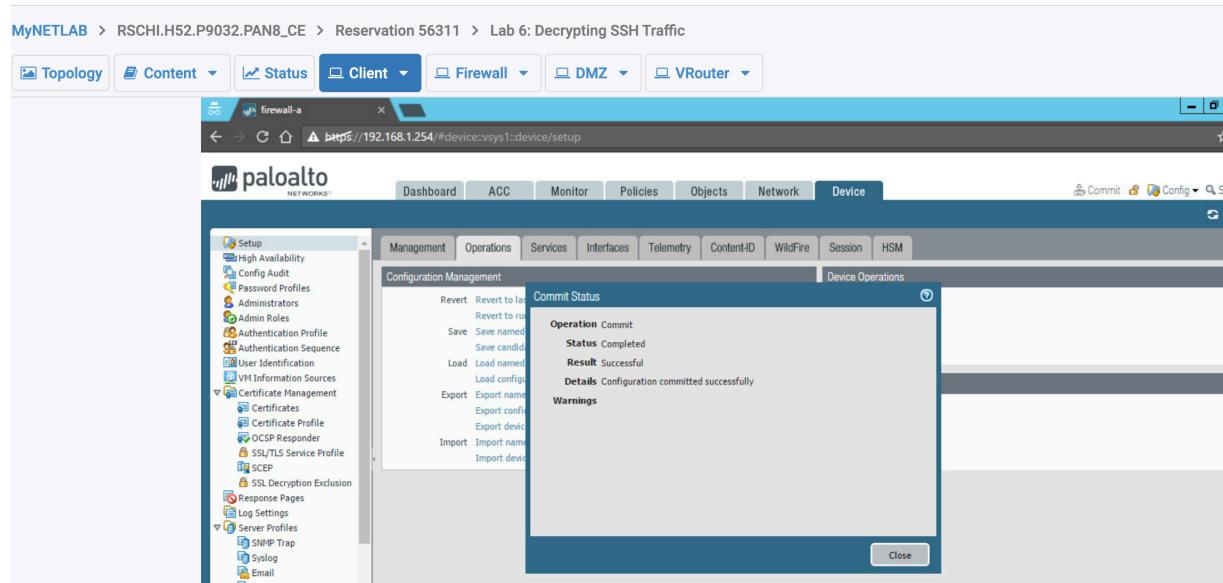
In this section, you will export the root CA certificate, lab-firewall. Then, you will commit your changes to the Firewall.

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.

cybersecurity-essentials-I Palo Alto Networks Cybersecurity Essentials I

MyNETLAB > RSCHI.H52.P9032.PAN8_CE > Reservation 56311 > Lab 6: Decrypting SSH Traffic

The screenshot shows the Palo Alto Networks Firewall interface. The left sidebar has a tree view with 'Security' selected, followed by NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, and DoS Protection. A 'Tag Browser' window is open, showing one item: 'none (1)'. The main content area is titled 'Decryption' and shows a table of rules. The table has columns: Name, Tags, Source, Destination, URL Category, Service, and Action. There is one rule named 'Decrypt SSH' with the action set to 'decrypt'. The source is 'inside' and the destination is 'dmz'. The URL category and service are both 'any'.

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.

MyNETLAB > RSCHI.H52.P9032.PAN8_CE > Reservation 56311 > Lab 6: Decrypting SSH Traffic

The screenshot shows the Palo Alto Networks Firewall interface. The left sidebar has a tree view with 'Logs' selected, followed by Traffic, Threat, URL Filtering, WildFire Submissions, Data Filtering, SIP Match, User-ID, Tunnel Inspection, Configuration, System, Alarms, Unified, Authentication, and Traffic Map. The main content area is titled 'Logs' and shows a table of traffic logs. The table has columns: Receive Time, Type, From Zone, To Zone, Source, Source User, Destination, To Port, Decrypted, Application, Action, Rule, and Sess. The logs show multiple entries for an SSH session between 'inside' and 'dmz' zones, with port 22. The 'Decrypted' column shows 'yes' for most entries, indicating successful decryption.

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.

The screenshot shows the Palo Alto Networks Firewall interface with the URL <https://192.168.1.254/#monitor:vsys1:monitor/logs/traffic>. The left sidebar has a 'Logs' section with 'Traffic' selected, showing various log categories like Threat, URL Filtering, and Wildfire Submissions. The main pane displays a table titled 'app eq ssh' with the following data:

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Decrypted	Application	Action	Rule	Sess
1	08/18 01:20:16	end	inside	dmz	192.168.1.20		192.168.50.10	22	no	ssh	allow	Allow-Inside-DMZ	t
2	08/18 01:19:57	end	inside	dmz	192.168.1.20		192.168.50.10	22	no	ssh	allow	Allow-Inside-DMZ	t
3	08/18 01:19:47	end	inside	dmz	192.168.1.20		192.168.50.10	22	no	ssh	allow	Allow-Inside-DMZ	t
4	08/18 01:19:40	start	inside	dmz	192.168.1.20		192.168.50.10	22	no	ssh	allow	Allow-Inside-DMZ	n
5	08/18 01:19:37	end	inside	dmz	192.168.1.20		192.168.50.10	22	no	ssh	allow	Allow-Inside-DMZ	t
6	08/18 01:19:35	start	inside	dmz	192.168.1.20		192.168.50.10	22	no	ssh	allow	Allow-Inside-DMZ	n
7	08/18 01:19:25	start	inside	dmz	192.168.1.20		192.168.50.10	22	no	ssh	allow	Allow-Inside-DMZ	n
8	08/18 01:19:21	end	inside	dmz	192.168.1.20		192.168.50.10	22	no	ssh	allow	Allow-Inside-DMZ	b
9	08/18 01:19:10	start	inside	dmz	192.168.1.20		192.168.50.10	22	no	ssh	allow	Allow-Inside-DMZ	n
10	08/18 01:18:44	start	inside	dmz	192.168.1.20		192.168.50.10	22	no	ssh	allow	Allow-Inside-DMZ	n

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

The screenshot shows the Palo Alto Networks Firewall interface under the 'Client' tab. The URL in the browser is <https://192.168.1.254/#objects:vsys1::objects/decryption-profile>. On the left, there is a navigation tree with sections like Applications, Services, and Security Profiles. The main area displays a table for 'SSL Inbound Inspection' with two rows. The columns include Name, Location, Server Certificate Verification, Unsupported Mode Checks, Failure Checks, Key Exchange Algorithms, Protocol Versions, Encryption Algorithms, Authentication Algorithms, and SSH Proxy settings.

Name	Location	Server Certificate Verification	Unsupported Mode Checks	Failure Checks	Key Exchange Algorithms	Protocol Versions	Encryption Algorithms	Authentication Algorithms	No Decryption	SSH Proxy
default	Predefined				RSA DHE ECDHE	Min Version: TLSv1.0 Max Version: Max	3DES RC4 AES128-CBC AES256-CBC AES128-GCM AES256-GCM	SHA1 SHA256 SHA384		
SSI inbound Inspection					RSA DHE ECDHE	Min Version: TLSv1.0 Max Version: Max	3DES RC4 AES128-CBC AES256-CBC AES128-GCM AES256-GCM	SHA1 SHA256 SHA384		

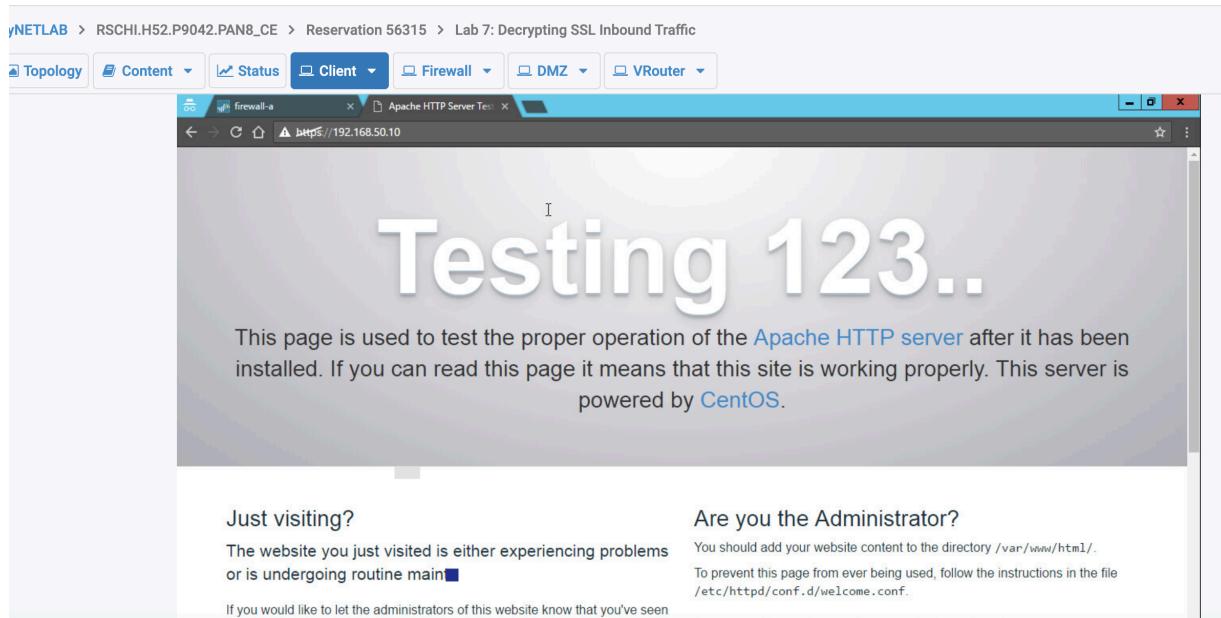
7.3 Create a Decryption Profile In this section, you will create a decryption profile. Decryption profiles allow administrators to perform checks on both decrypted traffic and traffic that would have been excluded from decryption. After a decryption profile is created, it can then be attached to a decryption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

7.4 Create a Decryption Policy

The screenshot shows the Palo Alto Networks Firewall interface under the 'Client' tab. The URL in the browser is <https://192.168.1.254/#policies:vsys1:ssl-decryption-rulebase>. On the left, there is a navigation tree with sections like Security, NAT, QoS, Policy-Based Forwarding, and Decryption. The main area displays a table for 'Decryption' rules with one row. The columns include Name, Tags, Source (Zone, Address, User), Destination (Zone, Address), URL Category, Service, and Action.

Name	Tags	Source	Destination	URL Category	Service	Action
1 Decrypt SSL bound inspection		Inside any any	dmz any any	any	service- http service- https	decrypt

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.



Receive Time	Type	From Zone	To Zone	Source	Decrypted	Source User	Destination	To Port	Application	Action	Rule	Sess
08/18 01:51:24	end	inside	dmz	192.168.1.20	yes		192.168.50.10	443	web-browsing	allow	Allow-Inside-DMZ	b
08/18 01:51:24	end	inside	dmz	192.168.1.20	yes		192.168.50.10	443	web-browsing	allow	Allow-Inside-DMZ	b
08/18 01:51:05	end	inside	dmz	192.168.1.20	yes		192.168.50.10	443	ssl	allow	Allow-Inside-DMZ	b
08/18 01:50:57	end	inside	dmz	192.168.1.20	yes		192.168.50.10	443	ssl	allow	Allow-Inside-DMZ	b
08/18 01:50:57	end	inside	dmz	192.168.1.20	yes		192.168.50.10	443	ssl	allow	Allow-Inside-DMZ	b
08/18 01:50:57	end	inside	dmz	192.168.1.20	yes		192.168.50.10	443	ssl	allow	Allow-Inside-DMZ	b
08/18 01:50:57	end	inside	dmz	192.168.1.20	yes		192.168.50.10	443	ssl	allow	Allow-Inside-DMZ	b
08/18 01:50:34	end	inside	dmz	192.168.1.20	yes		192.168.50.10	443	ssl	allow	Allow-Inside-DMZ	b

Student Project

Screenshot 1

lyNETLAB > RSCHI.H52.P9072.PAN8_CE > Reservation 56319 > Lab 1: Creating a Zero Trust Environment

The screenshot shows the Palo Alto Networks Firewall interface. The main window displays a table of security policy rules. One rule is selected, showing its detailed configuration. The rule is named 'Allow-Any' and has the following settings:

Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
Allow-Any	none	universal	any	any	any	any	any	any	any	any	Allow

Profile Settings include:

- Profile Type: Profiles
- Vulnerability Protection: default
- Anti-Spyware: default
- URL Filtering: default
- File Blocking: None
- Data Filtering: None
- WildFire Analysis: default

Log Settings include:

- Action Setting: Allow
- Log Setting: Log at Session End (checked)

Other Settings include:

- Schedule: None
- QoS Marking: None
- Disable Server Response Inspection: unchecked

Screenshot 2

cybersecurity-essentials-1 Palo Alto Networks Cybersecurity Essentials I

The screenshot shows the Palo Alto Networks Firewall interface. The main window displays a table of security policy rules. One rule is selected, showing its detailed configuration. The rule is named 'Allow-Any' and has the following settings:

Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
Allow-Any	none	universal	any	any	any	any	any	any	any	any	Allow

Profile Settings include:

- Profile Type: None

Log Settings include:

- Action Setting: Allow
- Log Setting: Log at Session Start (unchecked), Log at Session End (checked)

Other Settings include:

- Schedule: None
- QoS Marking: None
- Disable Server Response Inspection: unchecked

Screenshot 3

Screenshot 4

The screenshot shows the Palo Alto Networks Firewall configuration interface. The top navigation bar includes tabs for Topology, Content, Status, Client, Firewall, DMZ, and VRouter. The active tab is Firewall. Below the navigation is a browser window titled "firewall-a" with the URL <https://192.168.1.254/#policies:vsys1:policies/nat-rulebase>. The main content area displays a "NAT Policy Rule" configuration dialog. The dialog has tabs for General, Original Packet, and Translated Packet, with Original Packet selected. Under Source Address Translation, the Translation Type is set to "Dynamic IP And Port". The Address Type is "Interface Address", the Interface is "ethernet1/1", and the IP Address is "203.0.113.2072". Under Destination Address Translation, there is a checkbox labeled "Destination Address Translation" which is unchecked. The "Translated Address" field is empty, and the "Translated Port" field contains "[1-65535]". Buttons for OK and Cancel are at the bottom right of the dialog.

Screenshot 4

The screenshot shows the Palo Alto Networks Firewall monitoring interface. The top navigation bar includes tabs for Topology, Content, Status, Client, Firewall, DMZ, and VRouter. The active tab is Firewall. Below the navigation is a browser window titled "firewall-a" with the URL <https://192.168.1.254/#monitor:vsys1-monitor/logs/traffic>. The main content area displays a table of traffic logs titled "rule eq 'Allow-Inside-Out'". The table columns are: Receive Time, Type, From Zone, To Zone, Source, Source User, Destination, To Port, Application, Action, Rule, and Session End Reason. The table lists numerous entries from May 19, 2018, at 21:38:24 to 21:37:42, all categorized under the "Allow-Inside-Out" rule. The logs show various types of traffic (ping, dns) between the Inside and Outside zones, primarily originating from 192.168.1.20 and destination 8.8.8.8. The "Action" column consistently shows "allow". The "Session End Reason" column indicates "aged-out" for most entries. The bottom of the screen shows a toolbar with icons for Refresh, Stop, and Help, along with a search bar and a manual link.