

BLOCK THREATS IN ENCRYPTED TRAFFIC



YOU CAN'T ANALYZE WHAT YOU CAN'T SEE

- SSL/TLS review
- Certificate management
- SSL/TLS decryption
- Decryption considerations
- SSH decryption
- Master key management
- Other decryption methods and features

EDU-210 Version B
PAN-OS® 10.0

 **paloaltonetworks**[®]

Learning Objectives

After you complete this module,
you should be able to:

- Review fundamental SSL concepts and operation
- Create and manage certificates using the web interface
- Configure SSL/TLS forward proxy decryption
- Configure SSL/TLS inbound inspection decryption
- Prevent decryption for specific traffic
- View information and troubleshoot SSL/TLS issues using the CLI and logs
- Identify decryption configuration considerations
- Configure SSH decryption
- Manage the firewall master key
- List other available decryption methods





SSL/TLS review

Certificate management

SSL/TLS decryption

Decryption considerations

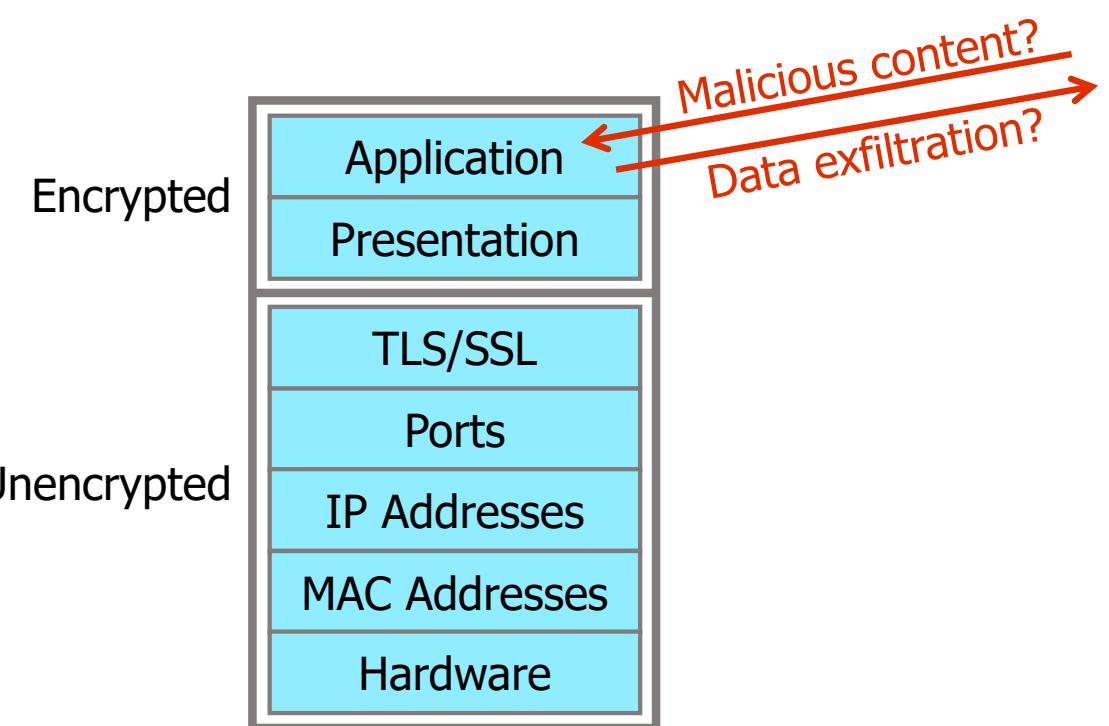
SSH decryption

Master key management

Other decryption methods and features

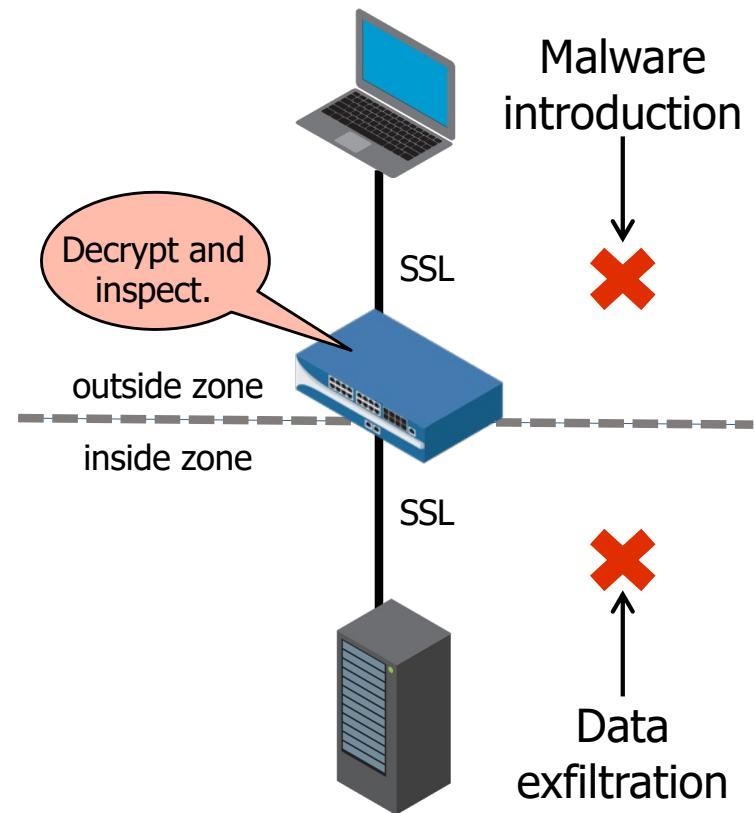
Why Decrypt Network Traffic?

- Most web traffic is encrypted.
- Palo Alto Networks firewalls can decrypt:
 - SSL/TLS inbound and outbound traffic
 - SSHv2



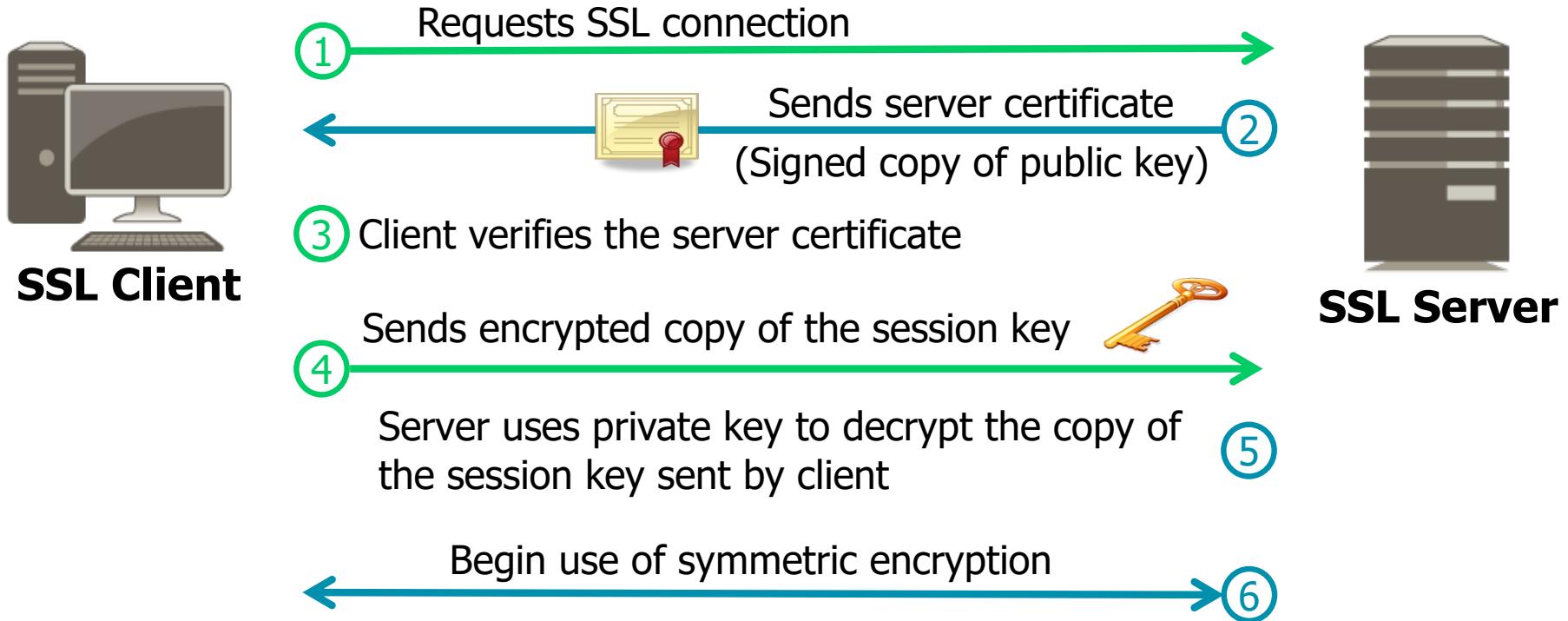
Importance of SSL/TLS

- SSL/TLS secures network communication across a shared network:
 - Encrypts for data privacy
 - Uses hashes for data integrity
 - Uses certificates for authentication
- SSL/TLS decryption helps to prevent:
 - Malware introduction
 - Data exfiltration



SSL/TLS Operation Review

SSL/TLS uses digital certificates to validate identity.



SSL/TLS review



Certificate management

SSL/TLS decryption

Decryption considerations

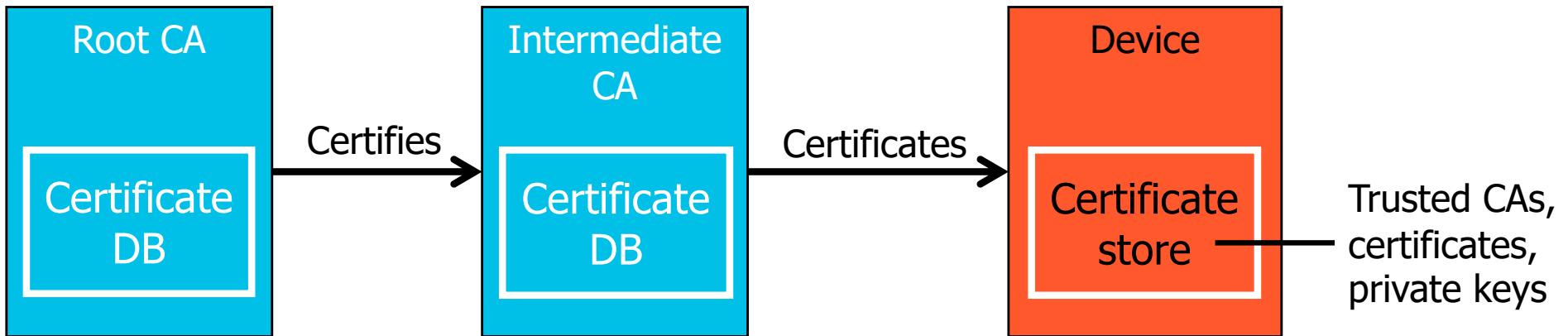
SSH decryption

Master key management

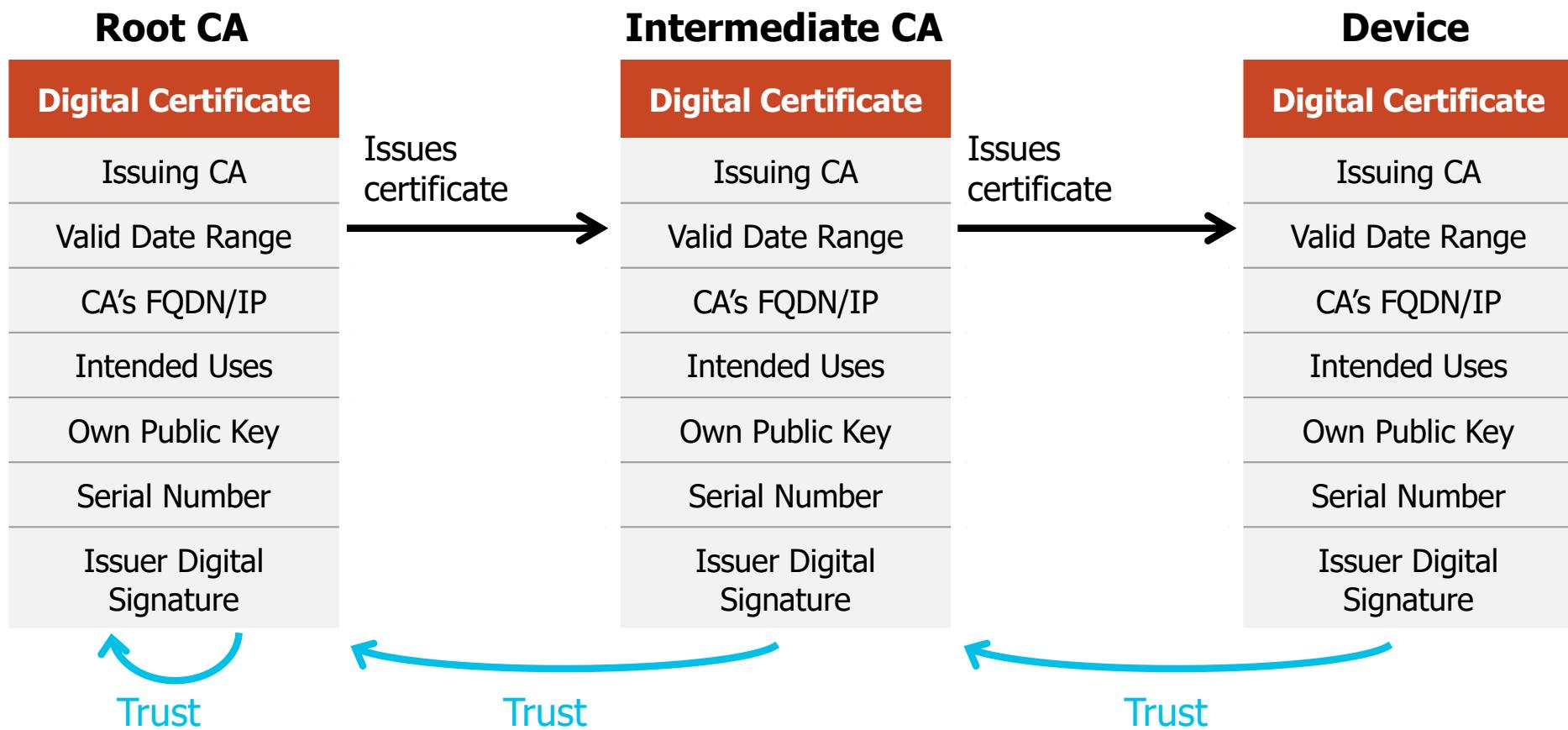
Other decryption methods and features

Public Key Infrastructure (PKI)

- Solves the problem of secure identification of public keys
- Uses digital certificates to verify public key owners
- Typical PKI components:



Certificate Chain of Trust



Certificate Management in the Web Interface

Device > Certificate Management > Certificates

NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGORITHM	USAGE
FW-CA-Cert	C = US, O = Palo Alto N...	C = US, O = Palo Alto ...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jul 24 00:36:21 202...	valid	RSA	Trusted Root CA Certificate
Forward-Trust-Cert	C = US, O = Palo Alto N...	C = US, O = Palo Alto ...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jul 24 00:37:23 202...	valid	RSA	Forward Trust Certificate
Forward-Untrust-Cert	C = US, O = Palo Alto N...	C = US, O = Palo Alto ...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jul 24 00:38:25 202...	valid	RSA	Forward Untrust Certificate

Delete Revoke Renew Import Generate Export Certificate Import HA Key Export HA Key PDF/CSV

Types of operations:

- Generate certificates
- View certificates
- Modify certificate use
- Import and export certificates
- Delete certificates
- Renew and revoke certificates

Certificate Hierarchy

Device > Certificate Management > Certificates

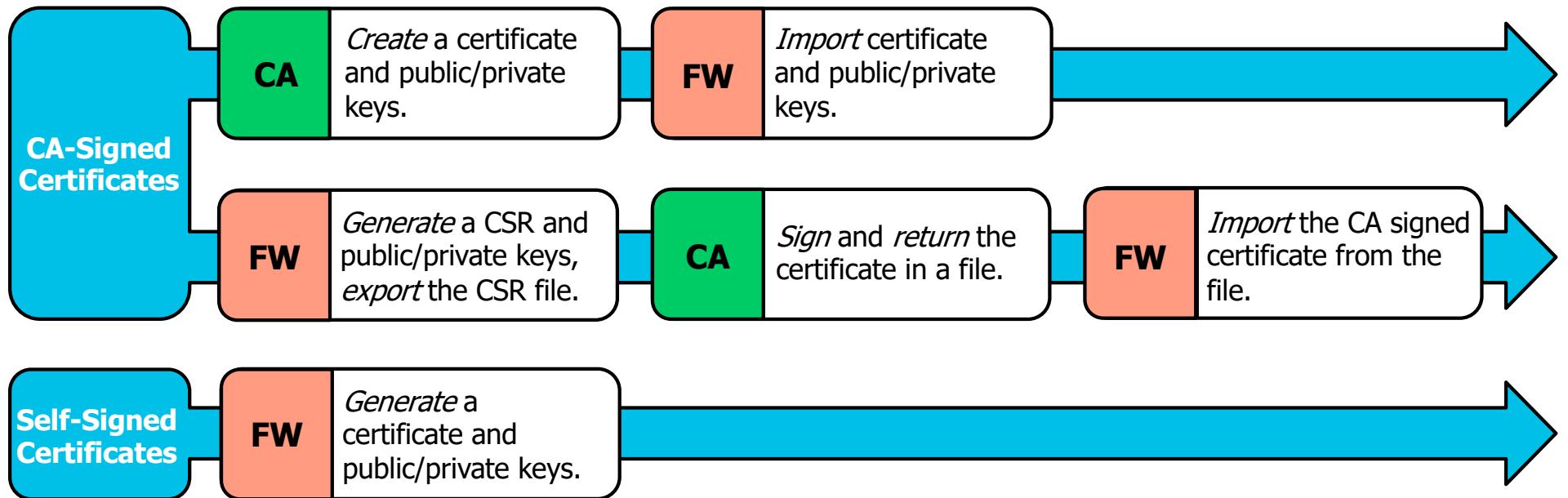
Device Certificates Default Trusted Certificate Authorities									
<input type="text"/> 5 items X									
	NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGORITHM	USAGE
<input type="checkbox"/>	FW-CA-Cert	C = US, O = Palo Alto N...	C = US, O = Palo Alto ...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 	Jul 24 00:36:21 202...	valid	RSA	Trusted Root CA Certificate
<input type="checkbox"/>	Forward-Trust-Cert	C = US, O = Palo Alto N...	C = US, O = Palo Alto ...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jul 24 00:37:23 202...	valid	RSA	Forward Trust Certificate
<input type="checkbox"/>	GP-Portal	C = US, O = Palo Alto N...	C = US, O = Palo Alto ...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Jul 24 00:45:35 202...	valid	RSA	
<input type="checkbox"/>	GP-Gateway	C = US, O = Palo Alto N...	C = US, O = Palo Alto ...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Jul 24 00:46:26 202...	valid	RSA	
<input type="checkbox"/>	WebUI-Cert	C = US, O = Palo Alto N...	C = US, O = Palo Alto ...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Jul 24 00:47:33 202...	valid	RSA	
<input type="checkbox"/>	Forward-Untrust-Cert	C = US, O = Palo Alto N...	C = US, O = Palo Alto ...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jul 24 00:38:25 202...	valid	RSA	Forward Untrust Certificate

Delete Revoke Renew Import Generate Export Certificate Import HA Key Export HA Key PDF/CSV

Nested hierarchy visually illustrates the certificate chain of trust.

Certificate Creation Overview

Methods to obtain required certificates and public/private keys:



Import a CA Certificate

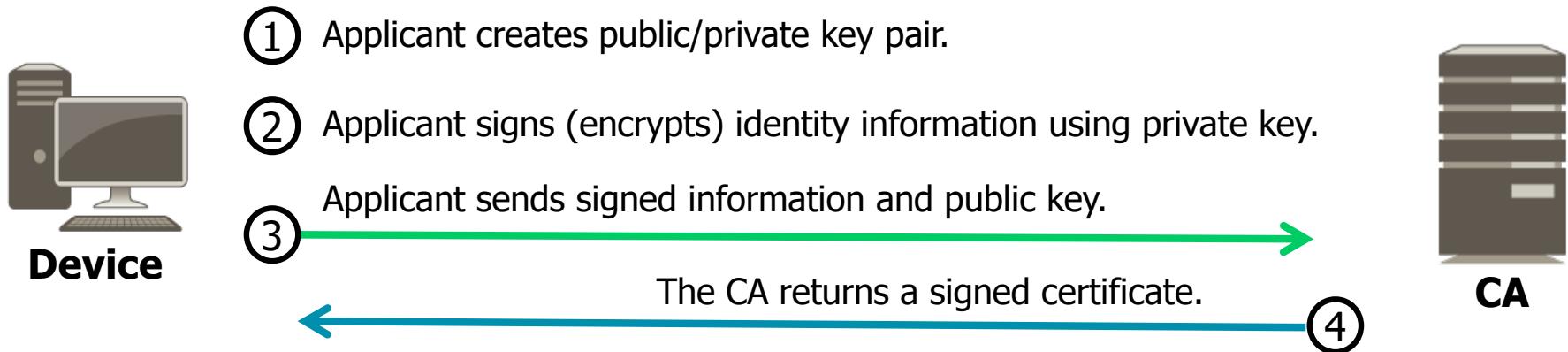
- Use an internal CA to create:
 - Firewall CA certificate
 - Public/private key pair
- Use **Device > Certificate Management > Certificates > Import.**
- Complete the form and click **OK**.
- Imports certificate and public/private keys into the firewall.

The screenshot shows the 'Import Certificate' dialog box. At the top, there are several buttons: Delete, Revoke, Renew, Import (which is highlighted with a black box and has an arrow pointing down to the dialog), and Generate. The dialog itself has the following fields:

- Certificate Type: Local (radio button selected), SCEP (radio button unselected)
- Certificate Name: Forward Trusted Cert
- Certificate File: C:\fakepath\cert_Forward-Trusted-Cert.pem (with a Browse... button)
- File Format: Base64 Encoded Certificate (PEM)
- Checkboxes:
 - Private key resides on Hardware Security Module (unchecked)
 - Import Private Key (checked)
 - Block Private Key Export (checked)
- Note: This option will permanently block export of private key for this certificate
- Key File: C:\fakepath\cert_Forward-Trusted-Cert.pem (with a Browse... button)
- Passphrase: (redacted)
- Confirm Passphrase: (redacted)

Certificate Signing Request (CSR)

Message sent to CA to acquire a certificate



Advantages:

- Device is part of PKI and benefactor of chain of trust.
- Private key never leaves device.

Generate a CSR for the CA-Signed Certificate

Device > Certificate Management > Certificates > Add

Generate Certificate

Certificate Type Local

Certificate Name Forward-Trusted-Cert

Common Name Firewall-A

Signed By External Authority (CSR)

Cryptographic Settings

- Algorithm RSA
- Number of Bits 2048
- Digest sha256
- Expiration (days) 365

Certificate Attributes

TYPE	VALUE
Country = "C" from "Subject" field	US
Organization = "O" from "Subject" field	Palo Alto Networks

+ Add - Delete

1. Generate a CSR.
2. Export the CSR file to the signing CA.
3. CA returns the signed intermediate CA certificate.
4. Import the signed intermediate CA certificate to the firewall.

NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS
FW-CA-Cert	C = US, O = Palo Alto...	C = US, O = Palo Alto...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jul 23 20:22:52 202...	valid
Forward-Trusted-Cert	Firewall-A		<input type="checkbox"/>	<input checked="" type="checkbox"/>		pending
Forward-Untrusted-Cert	C = US, O = Palo Alto...	C = US, O = Palo Alto...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jul 23 20:26:09 202...	valid

Import Export Certificate

.pem or .cer
Base64 encoding required

.csr

Generate a Self-Signed Certificate

Device > Certificate Management > Certificates > Add

Generate Certificate

Certificate Type: Local SCEP

Certificate Name: Forward-Untrusted-Cert

Common Name: Not Trusted

Signed By: [dropdown]

Certificate Authority

Block Private Key Export

OCSP Responder: [dropdown]

Cryptographic Settings

Algorithm: RSA

Number of Bits: 2048

Digest: sha256

Expiration (days): 365

Certificate Attributes

TYPE	VALUE
Country = "C" from "Subject" field	US
Organization = "O" from "Subject" field	Palo Alto Networks

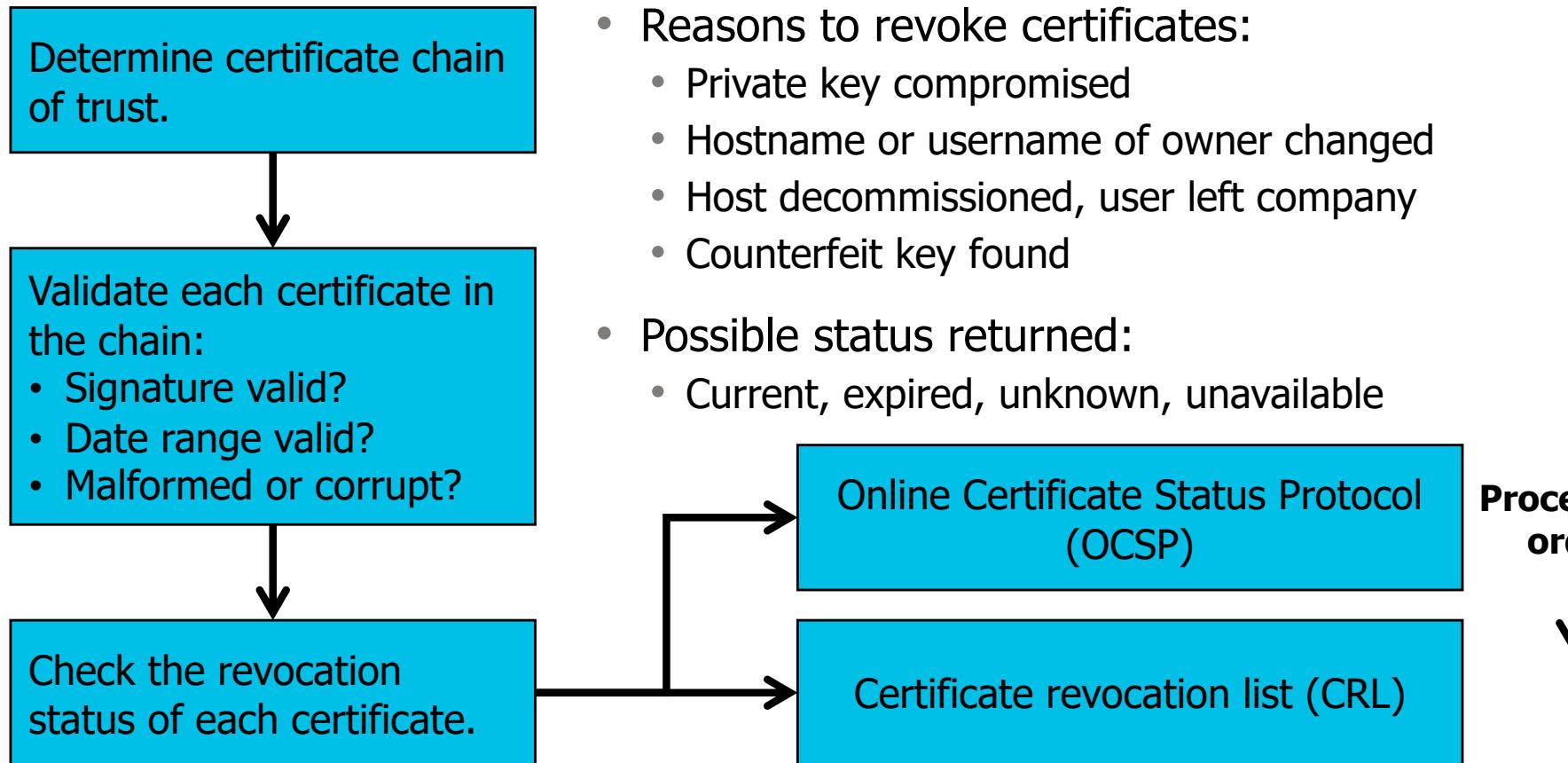
+ Add - Delete

Leave blank
to create a
self-signed
certificate.

Select to
create a CA
certificate.

- Configure a self-signed certificate:
 - The **Signed By** field must be blank.
- Generate** creates a certificate and public/private key pair.

Certificate Checking and Revocation



Configuring SSL Decryption Certificate Revocation Checking

Device > Setup > Session > Certificate Revocation Checking

Certificate Revocation Checking

CRL

Enable
Use CRL to check certificate status

Receive Timeout (sec)

OCSP

Enable
Use OCSP to check certificate status

Receive Timeout (sec)

Certificate Status Timeout (sec)
Certificate CRL status query timeout value

You can select either or both to enable certificate revocation checking.

SSL/TLS review

Certificate management

SSL/TLS decryption

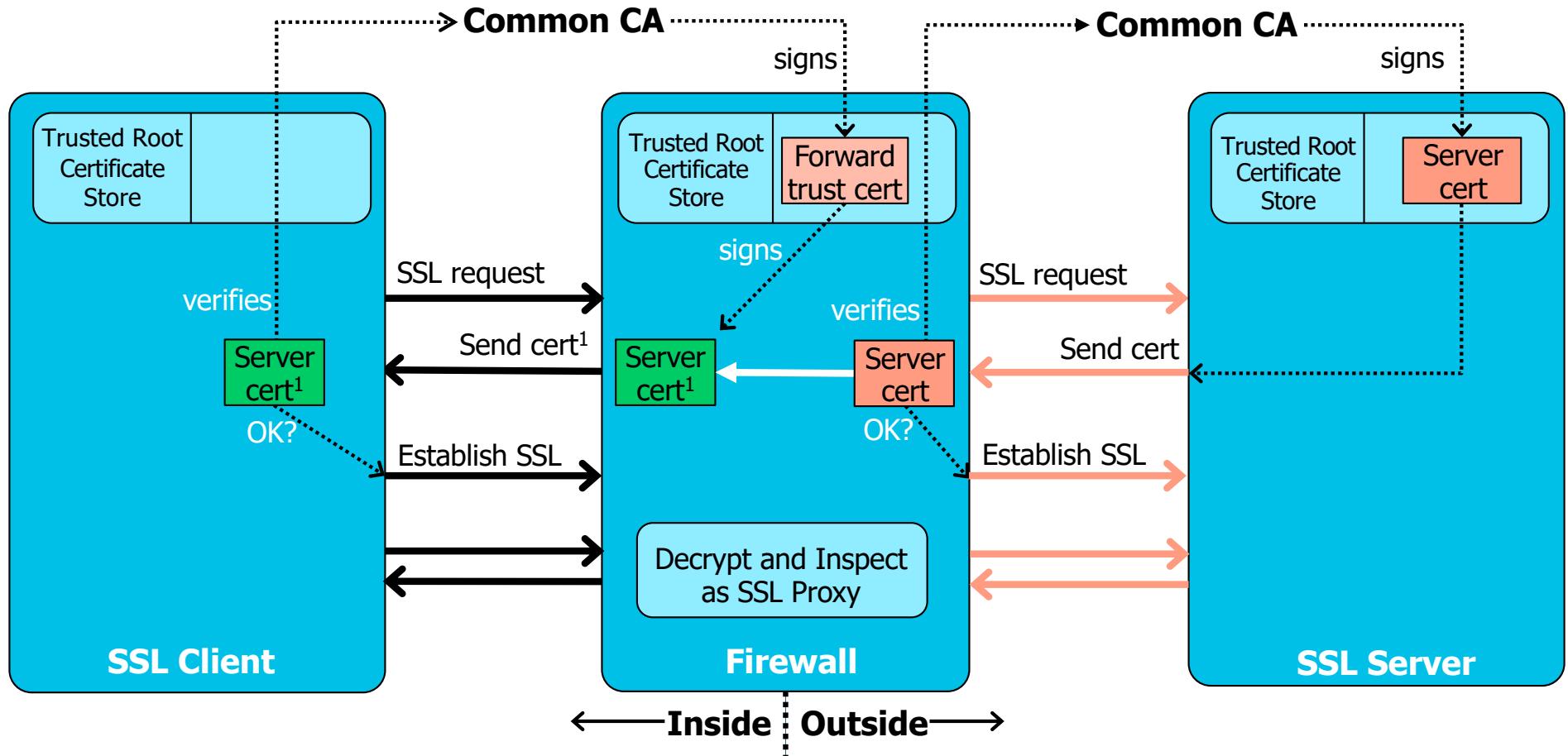
Decryption considerations

SSH decryption

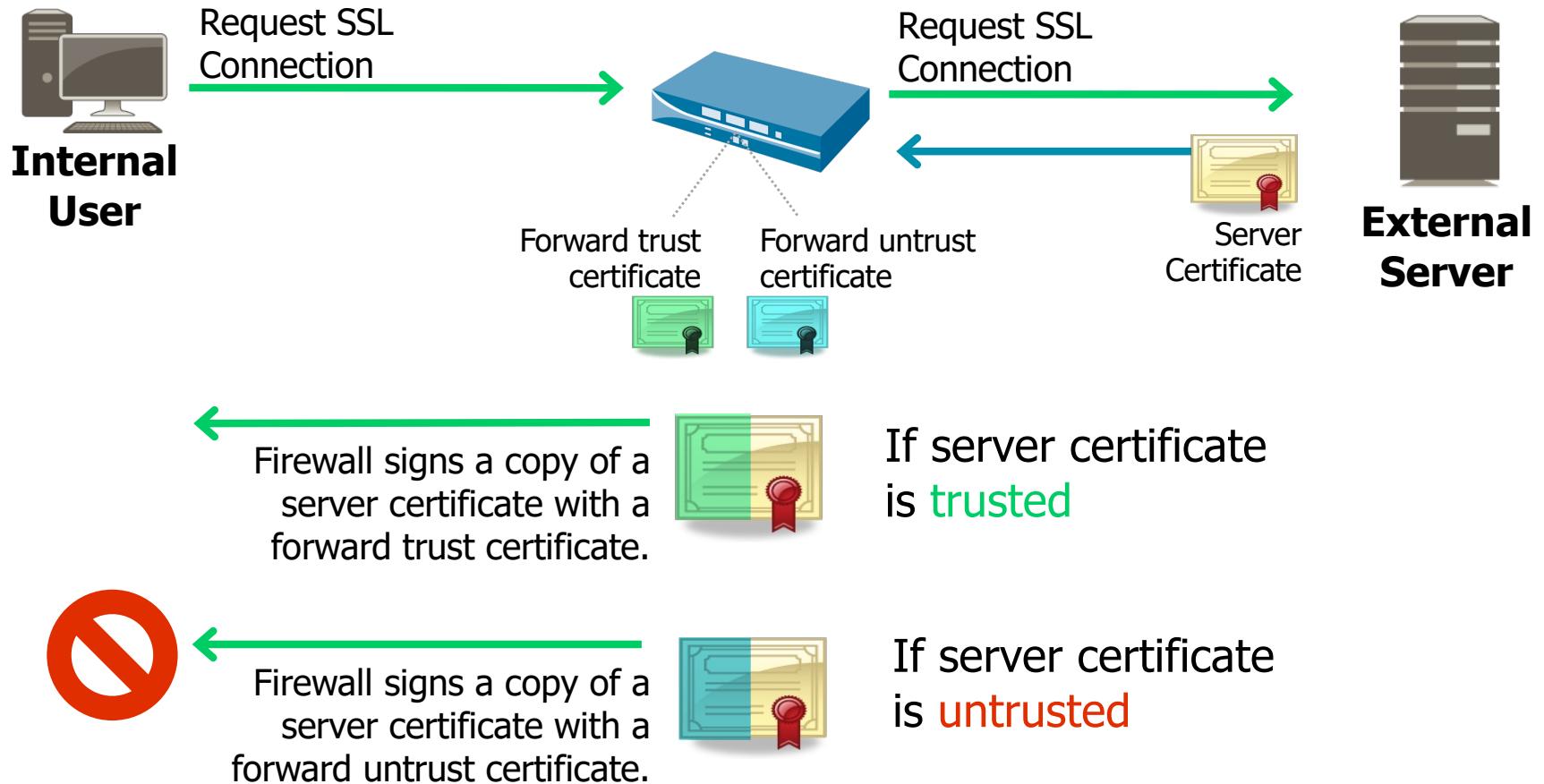
Master key management

Other decryption methods and features

SSL Forward Proxy Review



Forward Trust and Forward Untrust Certificates



Configure a Forward Trust Certificate

Device > Certificate Management > Certificates

The screenshot shows the 'Certificates' page under 'Device Management'. On the left, a table lists certificates: 'Forward-Untrusted-Cert' and 'Forwd-Trust-Cert'. An annotation with a callout says: 'Must be a valid CA certificate and trusted by the client'. An arrow points from this callout to the 'Forwd-Trust-Cert' row. A second annotation with a callout says 'Select.' and points to the 'Forward Trust Certificate' checkbox in the 'Certificate information' panel on the right.

NAME	SUBJECT
Forward-Untrusted-Cert	C = US, O
Forwd-Trust-Cert	C = US, O

Certificate information

Name: Forwd-Trust-Cert
Subject: /C=US/O=Palo Alto Networks/CN=Firewall-A
Issuer: /C=US/O=Palo Alto Networks/CN=Firewall-A
Not Valid Before: Jul 23 21:24:33 2020 GMT
Not Valid After: Jul 23 21:24:33 2021 GMT
Algorithm: RSA
 Certificate Authority
 Forward Trust Certificate
 Forward Untrust Certificate
 Trusted Root CA

Configure a Forward Untrust Certificate

Device > Certificate Management > Certificates

The screenshot shows the 'Certificates' page under 'Device Management'. On the left, a table lists certificates: 'Forward-Untrusted-Cert' and 'Forward-Trust-Cert'. A callout box points to the 'Forward-Trust-Cert' row with the text: 'Must be a CA certificate and *not* trusted by the client'. An arrow points from this row to the 'Certificate information' panel on the right. This panel displays details for the selected certificate, including its name, subject, issuer, validity period, algorithm, and trust settings. A callout box points to the 'Select.' checkbox next to 'Forward Untrust Certificate' in the trust settings section.

NAME	SUBJECT
Forward-Untrusted-Cert	C = US, O
Forward-Trust-Cert	C = US, O

Certificate information

Name: Forward-Untrusted-Cert
Subject: /C=US/O=Palo Alto Networks/CN=Not Trusted
Issuer: /C=US/O=Palo Alto Networks/CN=Not Trusted
Not Valid Before: Jul 23 20:26:09 2020 GMT
Not Valid After: Jul 23 20:26:09 2021 GMT
Algorithm: RSA
 Certificate Authority
 Forward Trust Certificate
 Forward Untrust Certificate
 Trusted Root CA

Must be a CA certificate and *not* trusted by the client

Select.

Renew an SSL Forward Untrust Certificate

Renews SSL forward untrust certificate issued by the firewall

Device > Certificate Management > Certificates

Device Certificates | Default Trusted Certificate Authorities

<input type="checkbox"/>	NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGORIT
<input type="checkbox"/>	Forward-Untrusted-Cert	C = US, O = Pal...	C = US, O = Pal...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jul 25 21:36:5...	valid	RSA
<input type="checkbox"/>	Forwd-Trust-Cert	C = US, O = Pal...	C = US, O = Pal...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jul 25 21:37:1...	valid	RSA
<input type="checkbox"/>	Web-Server1-Cert	C = US, O = Pal...	C = US, O = Pal...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 	Jul 23 21:35:2...	expired	RSA

>Delete Renew Import Generate Export Cert

Renew Certificate - Web-Server1-Cert

New Expiration Interval (days) 365

OK Cancel

Configure SSL Forward Proxy Decryption Policy

Policies > Decryption

The screenshot shows the 'Decryption Policy Rule' configuration window. At the top, there are tabs for General, Source, Destination, Service/URL Category, Options, and a question mark icon. The 'Source' tab is selected. Below the tabs is a 'Match conditions' section with two dropdown menus: 'select' and 'Any'. Under 'select', there are three options: SERVICE, service-https, and Service-62443. A callout bubble points to 'Service-62443' with the text 'Consider SSL traffic on non-default ports.'.

- Use rule fields to control what is decrypted.
- Phase in decryption to minimize user issues.
- Decryption subject to legal and privacy concerns (health, HR, finance, etc.)
- Create a Security policy rule to allow the traffic.

The screenshot shows the 'Decryption Policy Rule' configuration window with the 'Options' tab selected. The 'Action' section has two radio buttons: 'No Decrypt' (unchecked) and 'Decrypt' (checked). The 'Type' section shows 'SSL Forward Proxy' selected. The 'Decryption Profile' section shows 'Outbound-Traffic'. To the right, a dropdown menu is open, showing 'SSL Forward Proxy', 'SSH Proxy', and 'SSL Inbound Inspection'. A callout bubble points to the 'SSL Forward Proxy' option with the text 'Configures whether matched traffic is decrypted'.

Forward Proxy Decryption Profile

Objects > Decryption > Decryption Profile

Decryption Profile

Name: Outbound-Traffic

SSL Decryption: No Decryption | SSH Proxy

SSL Forward Proxy | SSL Inbound Inspection | SSL Protocol Settings

Server Certificate Verification

- Block sessions with expired certificates
- Block sessions with untrusted issuers
- Block sessions with unknown certificate status
- Block sessions on certificate status check timeout
- Restrict certificate extensions [Details](#)
- Append certificate's CN value to SAN extension

Unsupported Mode Checks

- Block sessions with unsupported versions
- Block sessions with unsupported cipher suites
- Block sessions with client authentication

Failure Checks

- Block sessions if resources not available
- Block sessions if HSM not available
- Block downgrade on no resource

Client Extension

- Strip ALPN

Policies > Decryption

Decryption Policy Rule

General | Source | Destination | Service/URL Category | Options

Action: No Decrypt Decrypt

Type: SSL Forward Proxy

Decryption Profile: Outbound-Traffic

- An SSL Forward Proxy policy rule specifies what to decrypt.
- An attached Decryption Profile specifies additional certificate and protocol checks.

Decryption Profile

Name: Outbound-Traffic

SSL Decryption: No Decryption | SSH Proxy

SSL Forward Proxy | SSL Inbound Inspection | **SSL Protocol Settings**

Protocol Versions

Min Version: TLSv1.0

Max Version: Max

SSLv3.0

TLSv1.0

TLSv1.1

TLSv1.2

TLSv1.3

Key Exchange Algorithms

RSA

DHE

Encryption Algorithms

3DES

RC4

AES128-CBC

AES256-CBC

Authentication Algorithms

MD5

SHA1

SHA256

SHA384

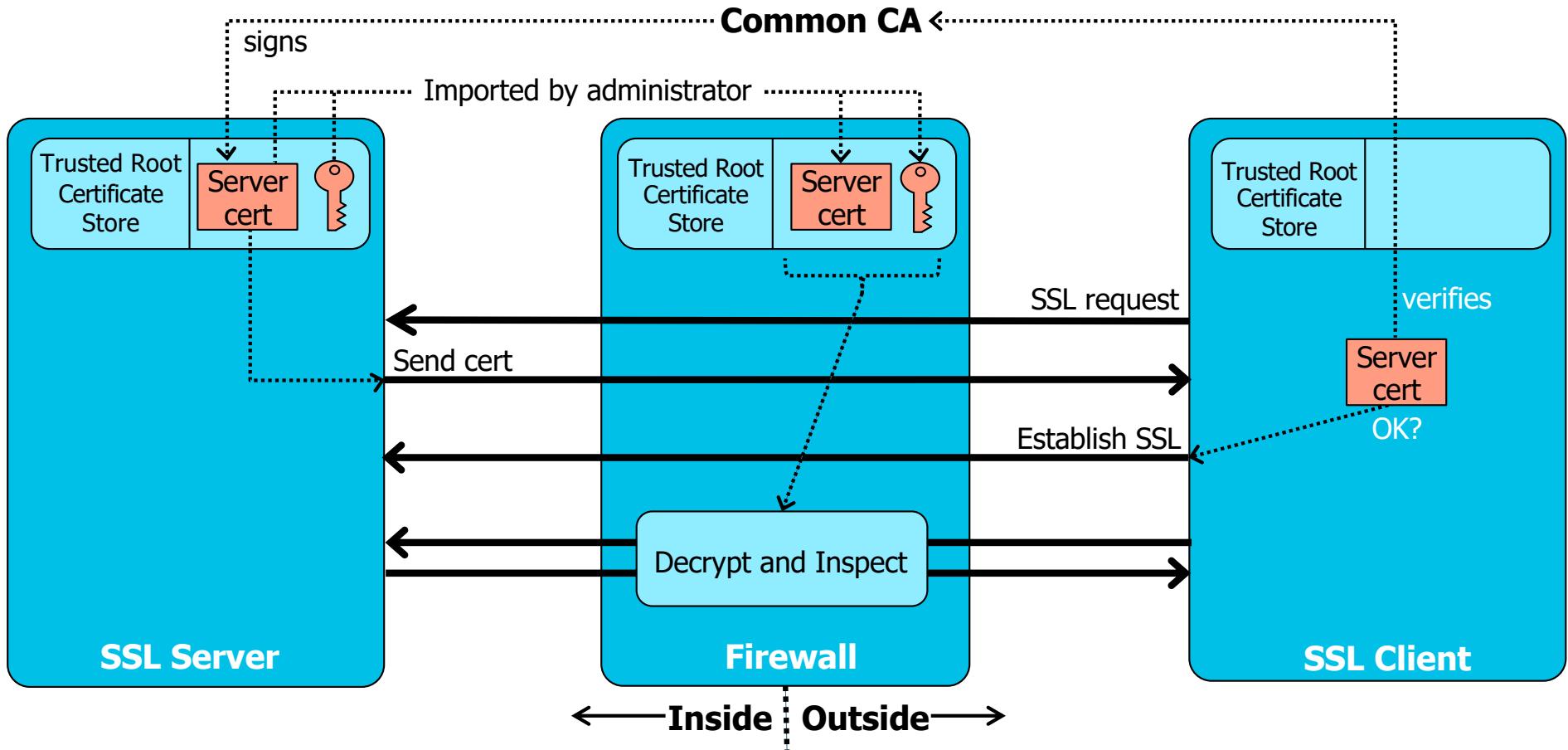
Create the Corresponding Security Policy Rules

- Create a rule to allow application *web-browsing*.
- Create a rule to allow application *ssl*.

Policies > Security

	NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION
				ZONE	ADDRESS	USER	ZONE	ADDRESS				
1	Allow-Web-Traffic	Users_Net	universal	Users_Net	any	any	Internet	any	web-browsing	application-default	any	Allow
2	Allow-SSL-Traffic	Users_Net	universal	Users_Net	any	any	Internet	any	ssl	application-default	any	Allow

SSL Inbound Inspection Review



Import Server Certificate and Private Key

Import the internal server certificate and private key into the firewall.

Device > Certificate Management > Certificates > Import

Import Certificate

Certificate Type Local SCEP

Certificate Name

Certificate File [Browse...](#)

File Format

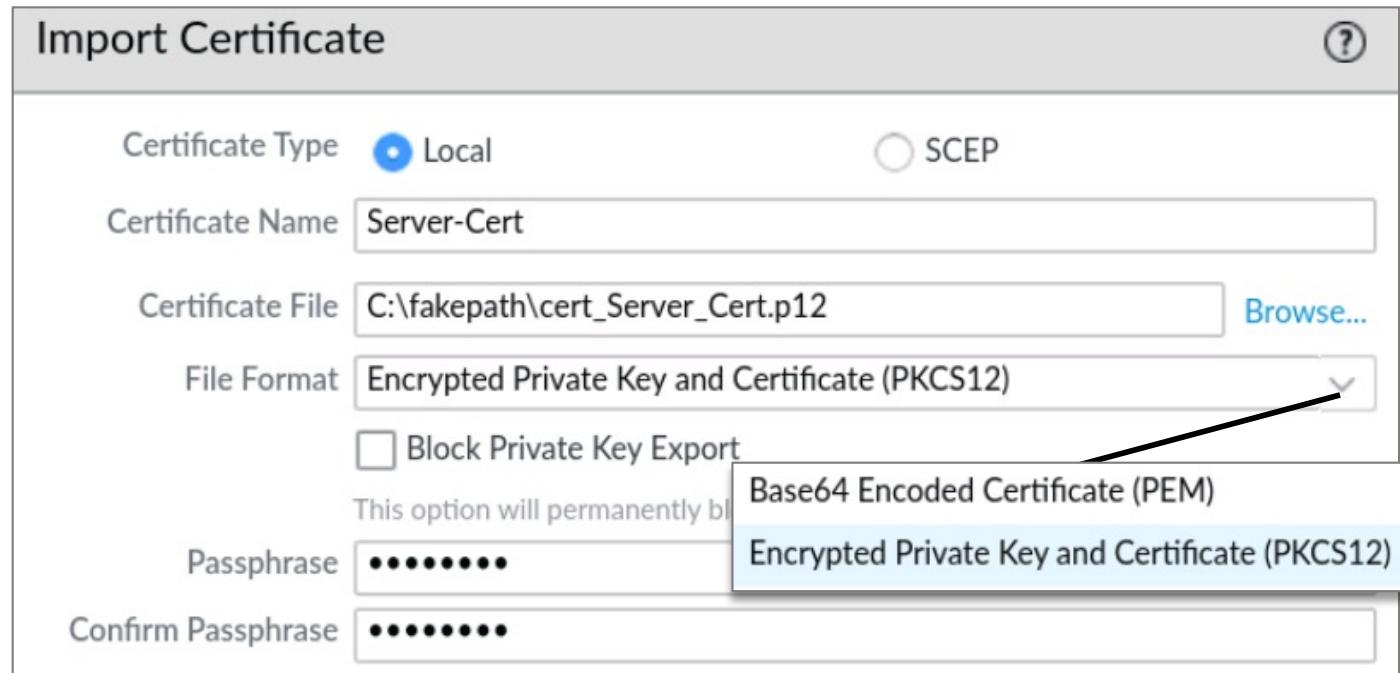
Block Private Key Export
This option will permanently bl

Passphrase

Confirm Passphrase

Base64 Encoded Certificate (PEM)

Encrypted Private Key and Certificate (PKCS12)



Configure an SSL Inbound Inspection Policy

- An SSL Inbound Inspection policy rule specifies what to inspect.
- An attached profile specifies additional protocol and firewall resource checks.
- Create a Security policy rule that allows traffic.

Policies > Decryption > Add

Decryption Policy Rule

General	Source	Destination	Service/URL Category	Options
Action	<input type="radio"/> No Decrypt	<input checked="" type="radio"/> Decrypt		
Type	SSL Inbound Inspection			
Certificate	Server-Cert			
Decryption Profile	Inbound-Traffic			

Imported server certificate

Configure an Inbound Inspection Decryption Profile

Objects > Decryption > Decryption Profile > Add

The screenshot shows the 'Decryption Profile' configuration page. The 'Name' field is set to 'Inbound-Traffic'. Under 'SSL Decryption', the 'SSL Inbound Inspection' tab is selected. In the 'Unsupported Mode Checks' section, two checkboxes are checked: 'Block sessions with unsupported versions' and 'Block sessions with unsupported cipher suites'. In the 'Failure Checks' section, three checkboxes are present but none are checked: 'Block sessions if resources not available', 'Block sessions if HSM not available', and 'Block downgrade on no resource'. A note at the bottom states: 'Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.' A callout bubble points to the 'Block sessions with unsupported cipher suites' checkbox with the text: 'Default setting allows encrypted traffic if firewall is too busy.'

Decryption Profile

Name

SSL Decryption | No Decryption | SSH Proxy

SSL Forward Proxy | **SSL Inbound Inspection** | SSL Protocol Settings

Unsupported Mode Checks

Block sessions with unsupported versions

Block sessions with unsupported cipher suites

Failure Checks

Block sessions if resources not available

Block sessions if HSM not available

Block downgrade on no resource

Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.

Default setting allows encrypted traffic if firewall is too busy.

Decryption Exclusions

Device > Certificate Management > SSL Decryption Exclusion

The screenshot shows a table of SSL Decryption Exclusions. A modal window titled "SSL Decryption Exclusion" is open, displaying a new exclusion entry. The modal fields are: Hostname: *.somedomain.somewhere, Description: Exclusion created for somedomain.somewhere, and Exclude checkbox (which is checked). A note below says "Note: check to exclude entry from decryption". A large black arrow points from the left side of the table towards the "SSL Decryption Exclusion" modal. To the right of the modal, a callout bubble contains the text: "Globally disables decryption regardless of Decryption policy".

<input type="checkbox"/>	HOSTNAME	LOCATION	DESCRIPTION	EXCLUDE FROM DECRYPTION
<input type="checkbox"/>	*.whatsapp.net	Predefined		<input checked="" type="checkbox"/>
<input type="checkbox"/>	kdc.uas.aol.com	Predefined		<input checked="" type="checkbox"/>
<input type="checkbox"/>	bos.oscar.aol.com	Predefined		
<input type="checkbox"/>	*.agni.lindenlab.com	Predefined		
<input type="checkbox"/>	*.service.paloaltonetworks.com	Predefined		
<input type="checkbox"/>	*.threatvault.paloaltonetworks.com	Predefined		
<input type="checkbox"/>	*.onepagecrm.com	Predefined		
<input type="checkbox"/>	update.microsoft.com	Defined		

Actions: Show obsolete | Excluded Common Names and SNI |

- Websites with known decryption problems are pre-populated on the list:
 - Exclusion list updated via content updates
 - You can add websites to the exclusion list.

No Decryption

Even if the Decryption policy rule action is “no-decrypt,” the Decryption Profile can be configured to block sessions with expired or untrusted certificates.

Policies > Decryption

ACTION	TYPE	DECRYPTION PROFILE
no-decrypt	ssl-forward-proxy	No-Decrption
no-decrypt	ssl-forward-proxy	No-Decrption

Objects > Decryption Profile > Add

Decryption Profile

Name

SSL Decryption No Decryption SSH Proxy

Server Certificate Verification

Block sessions with expired certificates
 Block sessions with untrusted issuers

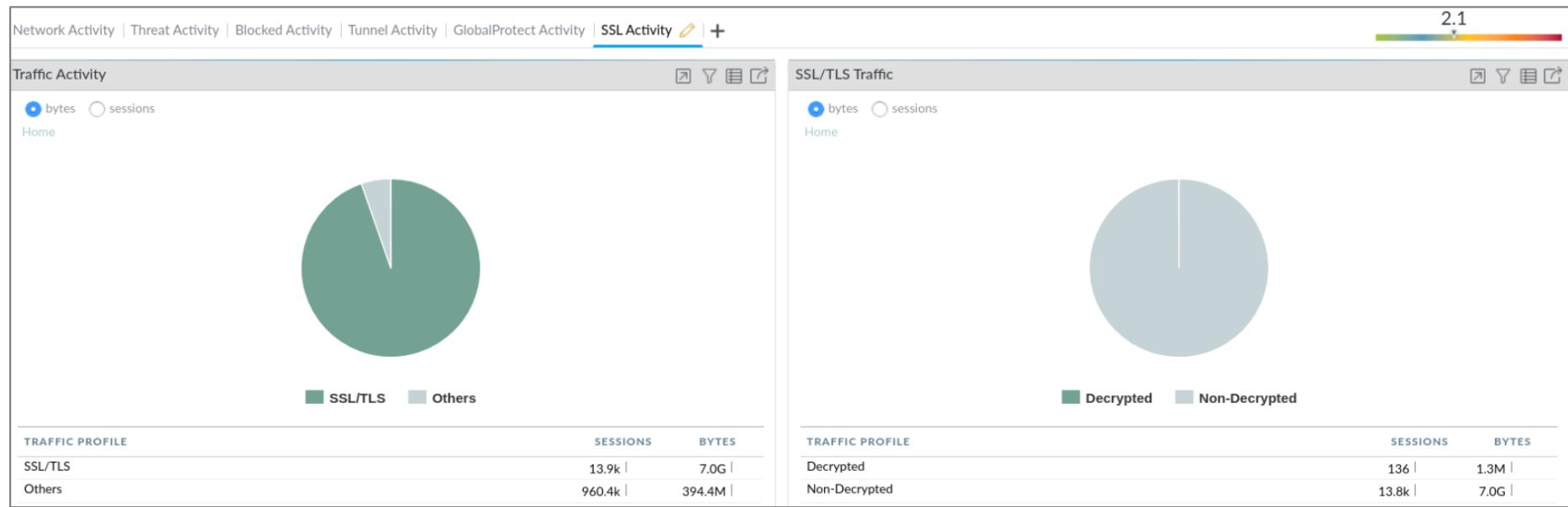
Note: For unsupported modes and failures, the session information is cached for 12 hours, boxes to block those sessions instead.

SSL Decryption Troubleshooting

Monitor > Logs > Decryption

	RECEIVE TIME	APPLICATION	POLICY NAME	SOURCE ZONE	DESTINA... ZONE	PROXY TYPE	SOURCE ADDRESS	DESTINATION ADDRESS	ROOT STATUS	TLS VERSION	KEY EXCHANGE	ENCRYPTION ALGORITHM
1	07/23 18:05:00	web-browsing	Decrypts_User_Traffic	Users_Net	Internet	Forward	192.168.1.20	172.217.12.42	trusted	TLS1.2	ECDHE	AES_128_GCM
2	07/23 17:20:02	web-browsing	Decrypts_User_Traffic	Users_Net	Internet	Forward	192.168.1.20	172.217.1.237	trusted	TLS1.2	ECDHE	AES_128_GCM
3	07/23 17:14:55	web-browsing	Decrypts_User_Traffic	Users_Net	Internet	Forward	192.168.1.20	216.58.193.131	trusted	TLS1.2	ECDHE	AES_128_GCM

ACC > SSL Activity



Troubleshoot SSL Session Terminations

Monitor > Logs > Traffic

The screenshot shows the Palo Alto Networks traffic log interface. On the left, a list of log entries is displayed, with one entry highlighted and a callout box labeled "Session end log entries". On the right, a modal dialog titled "Add Log Filter" is open. Inside the dialog, a search bar contains the query "(session_end_reason eq decrypt-error)". Below the search bar, there are four columns: Connector, Attribute, Operator, and Value. The Connector dropdown is set to "and". The Attribute dropdown is set to "Session End Reason". The Operator dropdown is set to "equal". The Value dropdown is expanded, showing a list of session end reasons: unknown, decrypt-cert-validation, decrypt-unsupport-param, decrypt-error (which is highlighted with a blue box), and split-tunnel. A callout box on the right side of the dialog states "Filter log for SSL-related errors." An arrow points from the "Decrypt Error" value in the Value dropdown to this callout box.

Decryption in the Traffic Log

Monitor > Logs > Traffic

The screenshot shows the 'Traffic' log view in the Palo Alto Networks interface. A specific session is highlighted with a black box around the 'DECRYPTED' column value 'yes'. An arrow points from this highlighted cell to a detailed log view window. In this detailed view, the 'Flags' section has a checkbox labeled 'Decrypted' which is checked, also highlighted with a black box.

	RECEIVE TIME	DECRYPTED	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
[Icon]	07/23 18:42:32	yes	end	Users_Net	Internet	192.168.1.252	34.96.84.34	443	web-browsing	allow	Users_to_Internet
[Icon]	07/23 18:30:24	yes	end	Users_Net	Internet	192.168.1.254	34.96.84.34	443	web-browsing	allow	Users_to_Internet
[Icon]	07/23 18:27:27	yes									
[Icon]	07/23 18:14:59	yes									
[Icon]	07/23 18:12:40	yes									
[Icon]	07/23 17:59:21	yes									
[Icon]	07/23 17:57:35	yes									

Detailed Log View

Rule UUID d6fede9b-9a48-419a-ac7f-fc0b83993fcf	Zone Users_Net	Interface ethernet1/2	Interface ethernet1/1
Session End Reason aged-out	NAT IP 203.0.113.20	NAT Port 13290	NAT IP 34.96.84.34
Category computer-and-internet-info	X-Forwarded-For IP 0.0.0.0	NAT Port 443	
Device SN			
IP Protocol tcp			
Log Action			
Generated Time 2020/07/23 18:30:24			
Start Time 2020/07/23 18:30:00			
Receive Time 2020/07/23 18:30:24			
Elapsed Time(sec) 10	Type end		
	Bytes 9935		

Flags

Captive Portal	<input type="checkbox"/>
Proxy Transaction	<input type="checkbox"/>
Decrypted	<input checked="" type="checkbox"/>
Packet Capture	<input type="checkbox"/>
Client to Server	<input type="checkbox"/>
Server to Client	<input type="checkbox"/>

Identify Decrypted Network Sessions Using the CLI

- Firewall logs decrypted sessions.
- Decrypted sessions are displayed using web interface or CLI.

```
admin@firewall-a> show session all filter ssl-decrypt yes  
-----  
ID          Application      State   Type Flag  Src[Sport]/Z  
Vsys  
                               Dst[Dport]/Z  
-----  
12033        web-browsing    ACTIVE  FLOW *NS  192.168.1.20  
vsys1  
12055        web-browsing    ACTIVE  FLOW *NS  192.168.1.20  
  
* = decrypted  
NS = Source NAT
```

SSL/TLS review

Certificate management

SSL/TLS decryption



Decryption considerations

SSH decryption

Master key management

Other decryption methods and features

Opt Out of SSL Decryption

Device > Response Pages

TYPE	ACTION
File Blocking Block Page	
GlobalProtect App Help Page	
GlobalProtect Portal Login Page	
GlobalProtect Portal Home Page	
GlobalProtect App Welcome Page	
MFA Login Page	
SAML Auth Internal Error Page	
SSL Certificate Errors Notify Page	
SSL Decryption Opt-out Page	Enabled
URL Filtering and Category Match Block Page	Default
URL Filtering Continue and Override Page	Default

Click to enable.

SSL Inspection

If you proceed with this session then, in accordance with company security policy, SSL encrypted traffic that you initiate will be temporarily decrypted so that it can be inspected for viruses, spyware, and malware.

After inspection, the traffic will be re-encrypted and sent to its destination.

IP: 23.211.85.11

Category: lab-decryption

Would you like to proceed with this session?

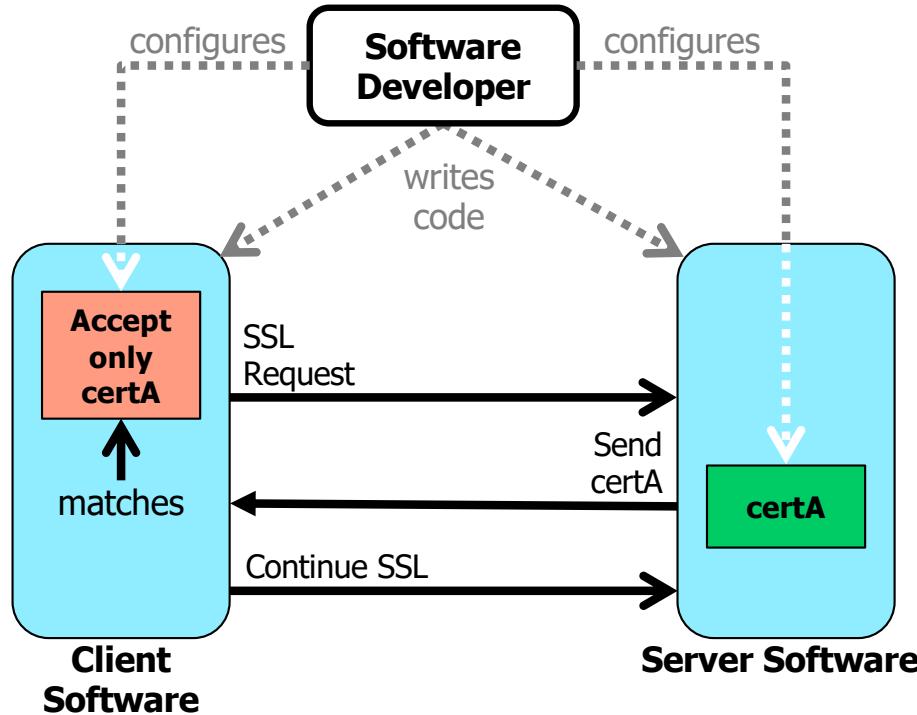
Enables users to refuse connections to decrypted sites

SSL Decryption Policy Considerations

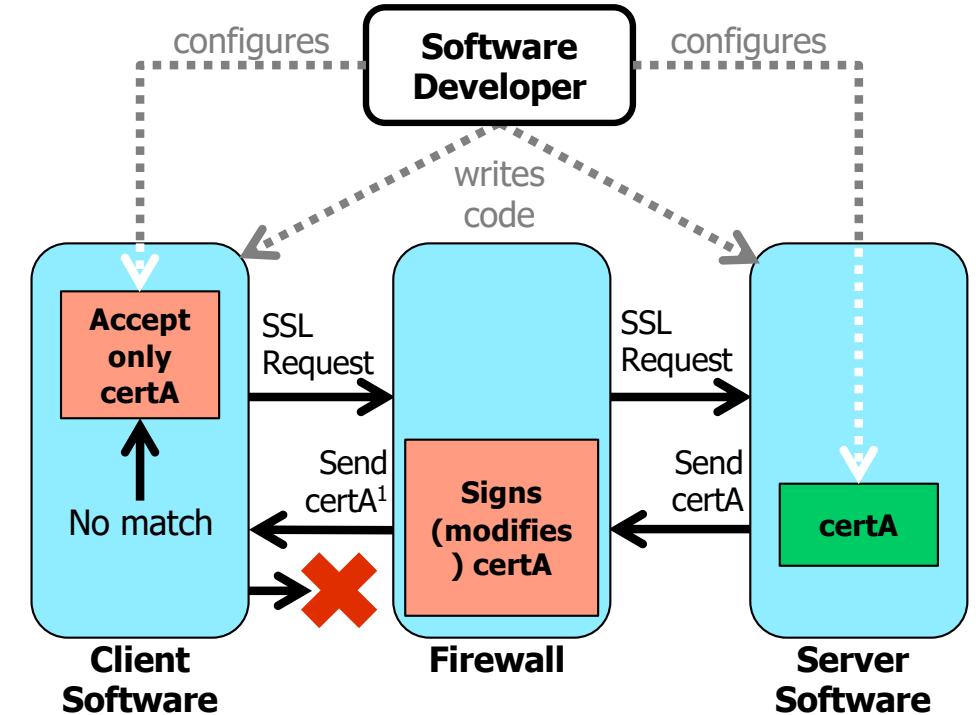
- Certificate or key pinning can affect SSL decryption configuration.
- Client is preconfigured to know which certificate or keys to expect or accept.
- Defeats use of counterfeit or man-in-the-middle keys or certificates.
- Two types of certificate pinning:
 - Static server certificate pinning
 - Static CA certificate pinning
- Dynamic key pinning: HTTP Public Key Pinning (HPKP)

Static Server Certificate Pinning

Server Certificate Pinning – No Firewall



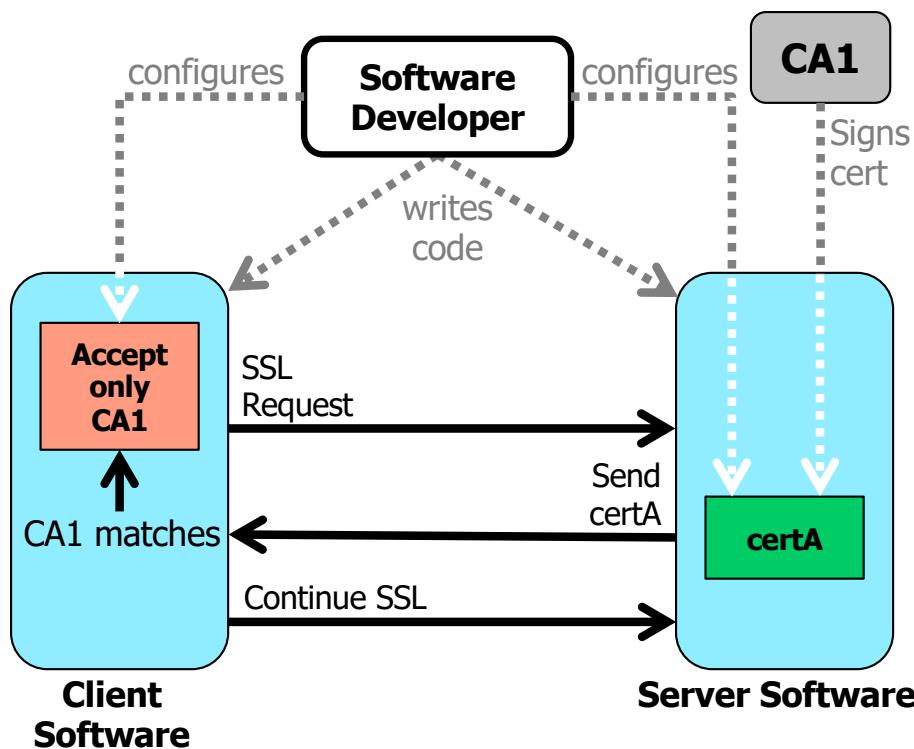
Server Certificate Pinning – With Firewall



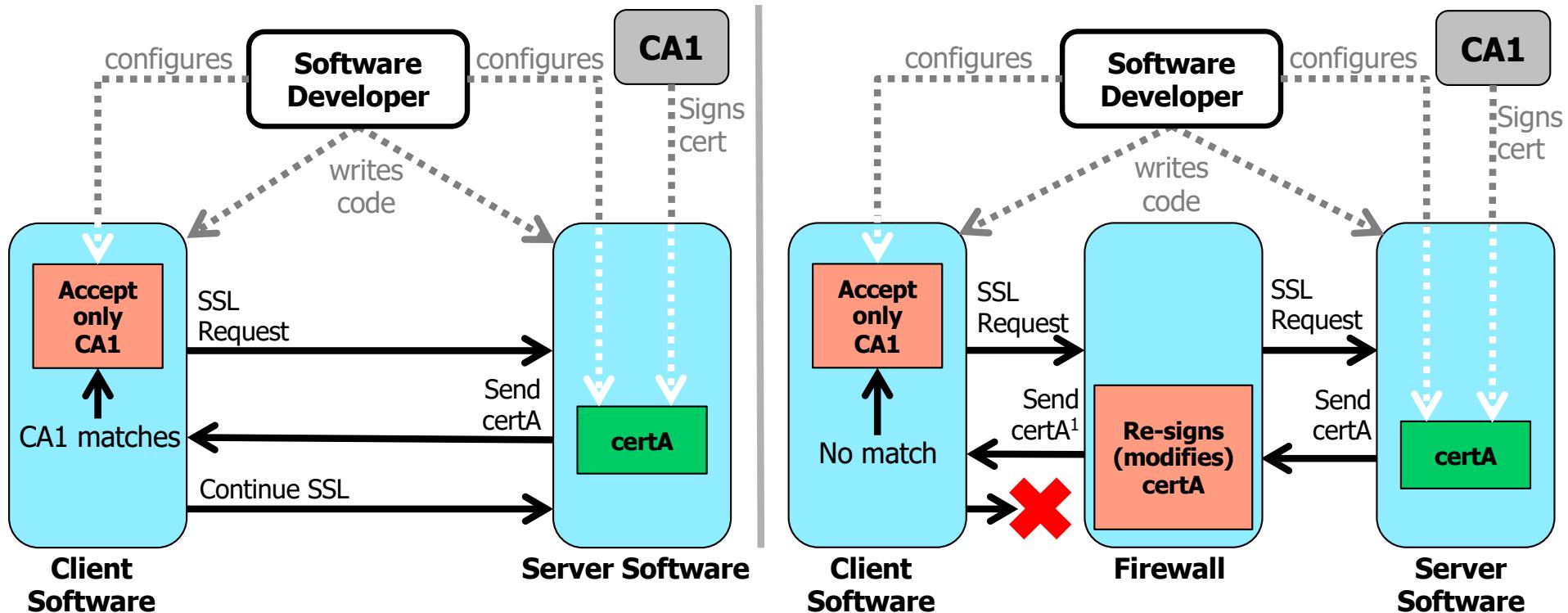
Server certificate pinning prevents MiTM attacks but breaks SSL Forward Proxy decryption.

Static CA Certificate Pinning

CA Certificate Pinning – No Firewall



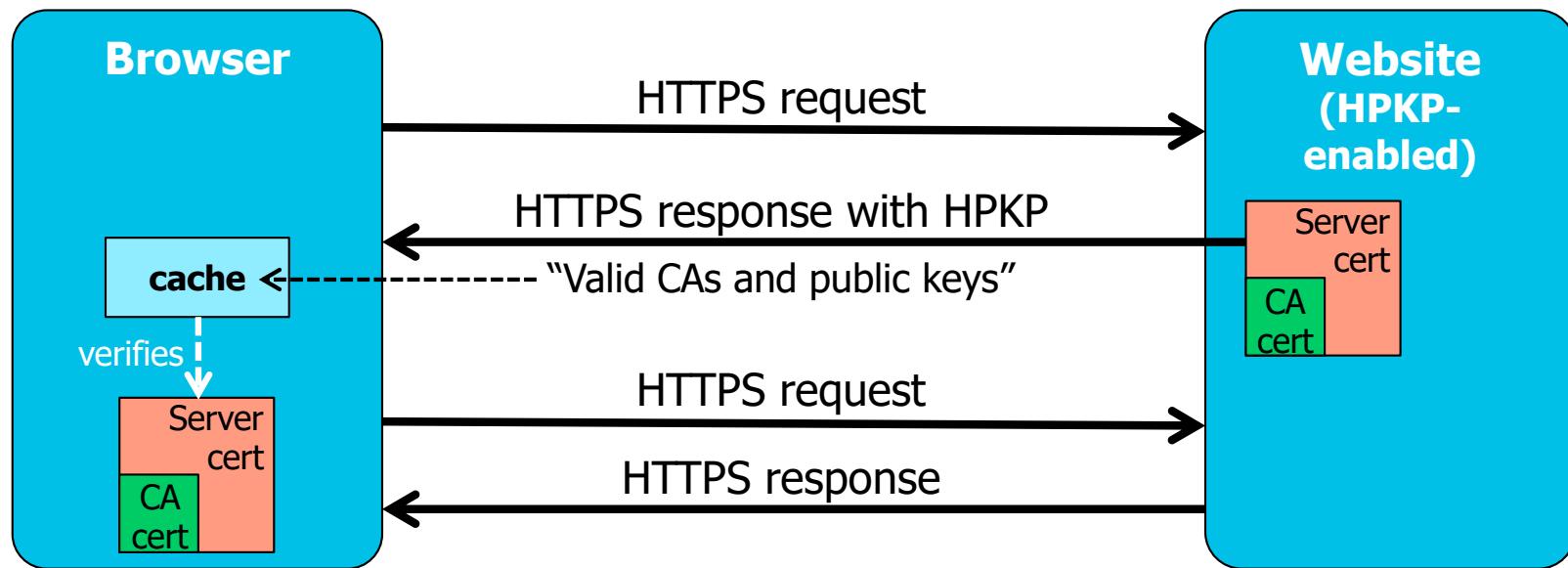
CA Certificate Pinning – With Firewall



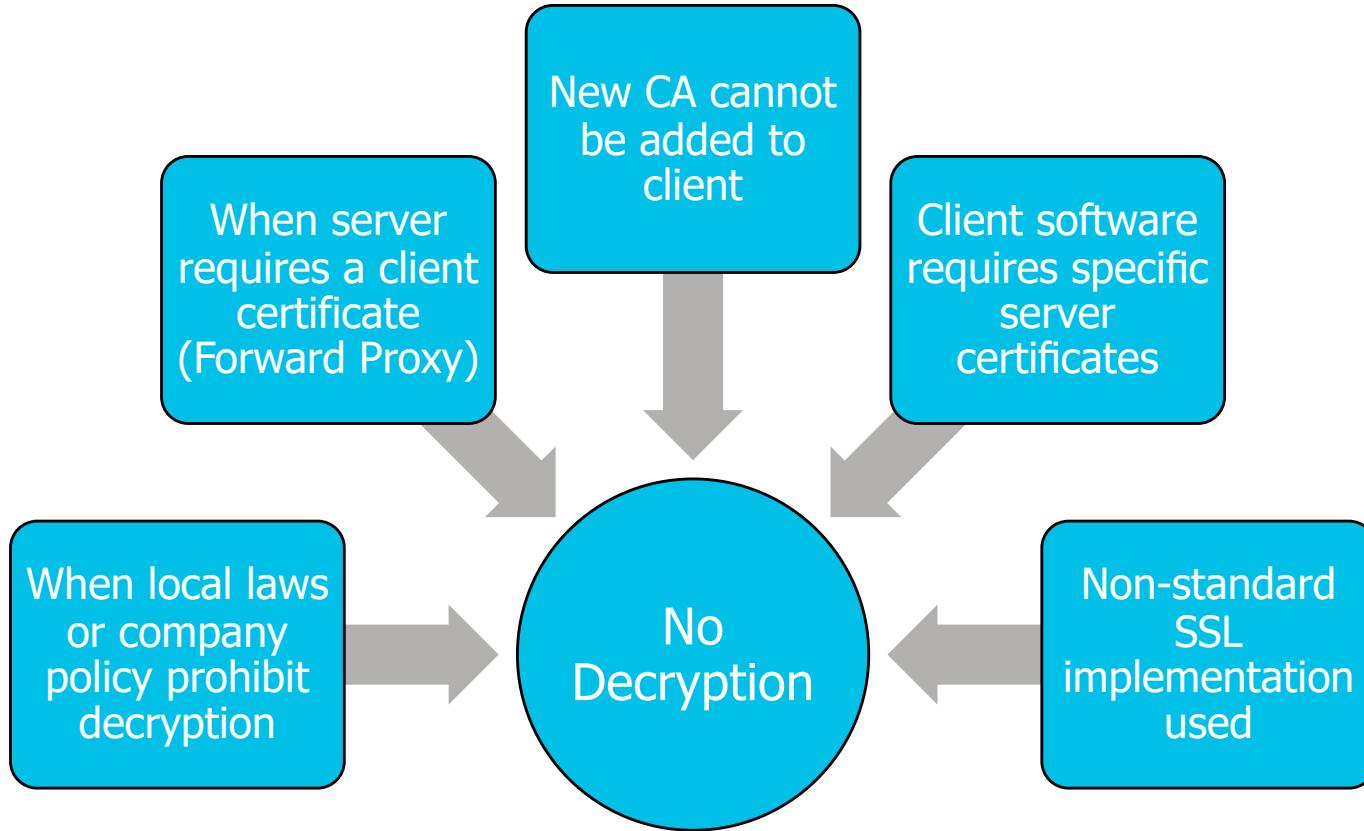
SSL decryption fails unless you can add the firewall's forward trust certificate to the client's list.

Dynamic Key Pinning

- Dynamic key pinning relies on HTTP Public Key Pinning (HPKP).
- HPKP breaks SSL Forward Proxy decryption unless you can update the valid CA list to include the firewall forward trust certificate.



Reasons to Not Configure SSL Decryption



SSL/TLS review

Certificate management

SSL/TLS decryption

Decryption considerations

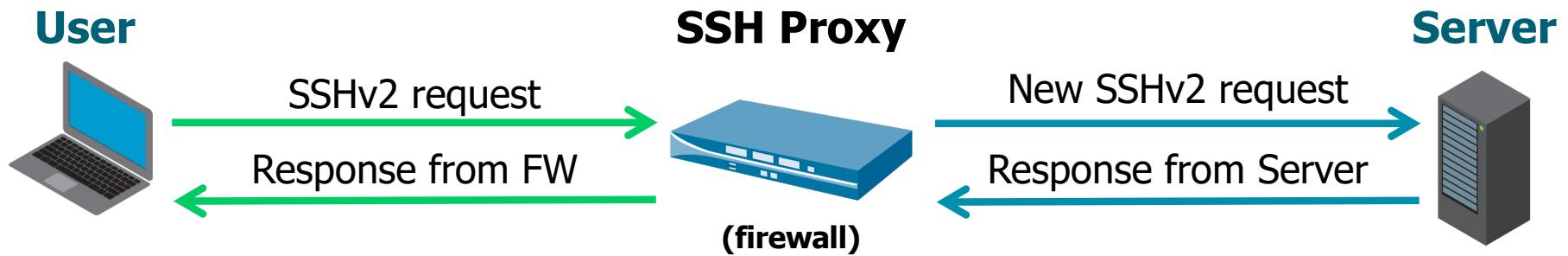


SSH decryption

Master key management

Other decryption methods and features

SSH Decryption



- Decrypts and inspects SSHv2 traffic (to detect SSH-tunneled applications).
- Unsupported with SSH key passwordless login.
- Uses an automatically generated key to decrypt or encrypt traffic.
- All traffic is identified as either *ssh* or *ssh-tunnel*:
 - Control traffic using Security policy rules.

Configure an SSH Proxy Decryption Policy

Policies > Decryption

The screenshot shows the 'Decryption Policy Rule' configuration screen. At the top, there are tabs: General, Source, Destination, Service/URL Category (which is underlined in blue), and Options. Below the tabs, there are two dropdown menus: 'select' and 'SERVICE'. Under 'SERVICE', there is an option 'service-ssh'. On the right side, there is a checkbox labeled 'Any' and another checkbox labeled 'URL CATEGORY' which is currently unchecked. A callout bubble labeled 'Match conditions' points to the 'Service/URL Category' tab.

The screenshot shows the 'Decryption Policy Rule' configuration screen with the 'Options' tab selected. Under the 'Action' section, the 'Decrypt' radio button is selected. Below it, the 'Type' dropdown is set to 'SSH Proxy'. There is also a 'Decryption Profile' dropdown set to 'Outbound-Traffic'. To the right, there is a dropdown menu with three options: 'SSL Forward Proxy', 'SSH Proxy', and 'SSL Inbound Inspection'. A callout bubble labeled 'Match conditions' points to the 'Service/URL Category' tab in the top interface.

- Use rule fields to limit what is decrypted.
- Phase in decryption to minimize user issues.
- Decryption subject to legal and privacy concerns (health, HR, finance, etc.).

SSH Proxy Decryption Profile

Objects > Decryption > Decryption Profile > Add

Decryption Profile

Name	Outbound-Traffic
SSL Decryption	No Decryption
SSH Proxy	
Unsupported Mode Checks	
<input checked="" type="checkbox"/> Block sessions with unsupported versions	
<input checked="" type="checkbox"/> Block sessions with unsupported algorithms	
Failure Checks	
<input type="checkbox"/> Block sessions on SSH errors	
<input type="checkbox"/> Block sessions if resources not available	
Note: For unsupported modes and failures, the session information is cached for 12 hours, boxes to block those sessions instead.	

- Enables additional controls on decrypted SSH traffic
- Recommended to block sessions with unsupported versions or algorithms
- No options selected by default

SSH Traffic and the Security Policy

Add rules to control ssh and ssh-tunnel traffic.

Policies > Security > Add

	NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION
				ZONE	ADDRESS	USER	ZONE	ADDRESS				
1	Bad-SSH-Traffic	Users_Net	universal	Users_Net	165.35.13.6	any	Extranet	any	ssh	any	any	Deny
2	Block-SSH-Tunnels	Users_Net	universal	Users_Net	any	any	Extranet	any	ssh-tunnel	any	any	Deny
3	Good-SSH-Traffic	Users_Net	universal	Users_Net	any	any	Extranet	any	ssh	application-default	any	Allow

SSL/TLS review

Certificate management

SSL/TLS decryption

Decryption considerations

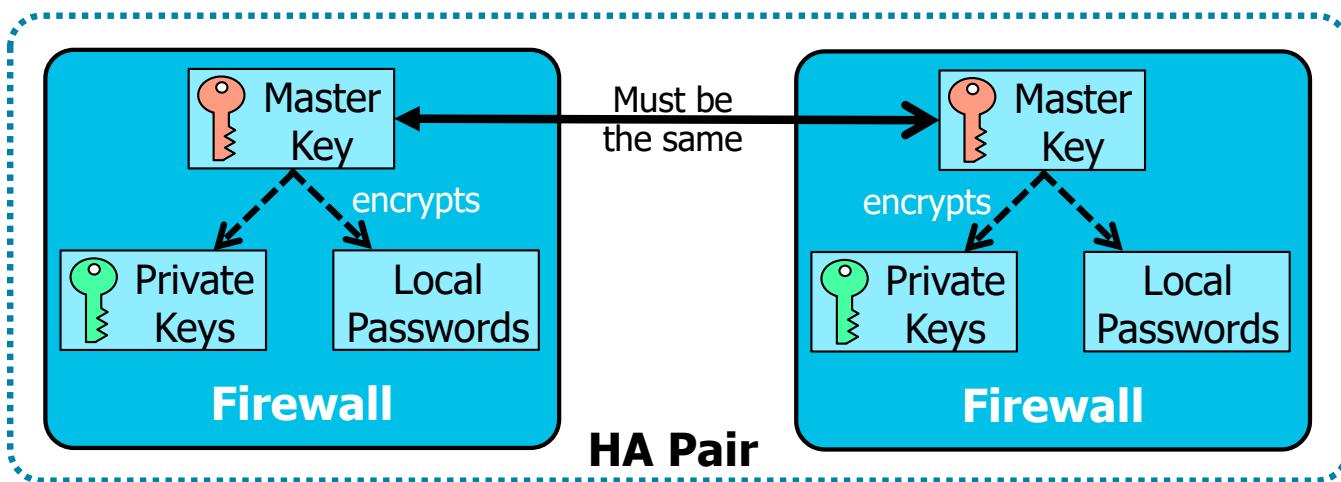
SSH decryption

► **Master key management**

Other decryption methods and features

Firewall Master Key

- Firewall master key used to encrypt password and private keys.
- Periodically change master key.
- Must use the same master key in an HA pair.



Manage the Master Key

- You must commit all pending changes before changing the key.
- A commit is not required after the key is changed.
- Set an expiration warning to avoid being locked out.
- Configure auto-renew as a lockout safeguard.
- If the master key expired, firewall access is available only through the serial console:
 - Perform a factory reset

Device > Master Key and Diagnostics

The screenshot shows the 'Master Key' configuration page. It includes fields for the current master key, new master key (with a note that it must be exactly 16 characters), confirm new master key, lifetime (set to 180 days), time for reminder (set to 30 days), and auto-renew settings. A callout box highlights the 'New Master Key' field with the text 'Requires exactly 16 characters'.

Device > Log Settings > Alarm Settings

The screenshot shows the 'Alarm Settings' configuration page. It includes checkboxes for enable alarms, enable CLI alarm notifications, enable web alarm notifications, and enable audible alarms. A callout box highlights the 'Enable Alarms' checkbox with the text 'Enables the display of expiration alarms'.

SSL/TLS review

Certificate management

SSL/TLS decryption

Decryption considerations

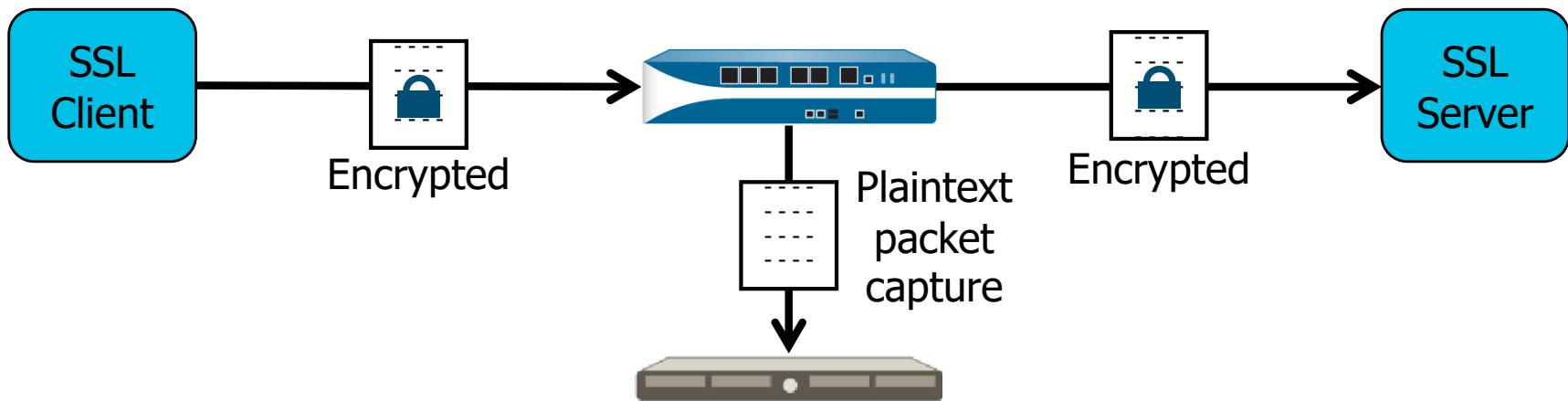
SSH decryption

Master key management

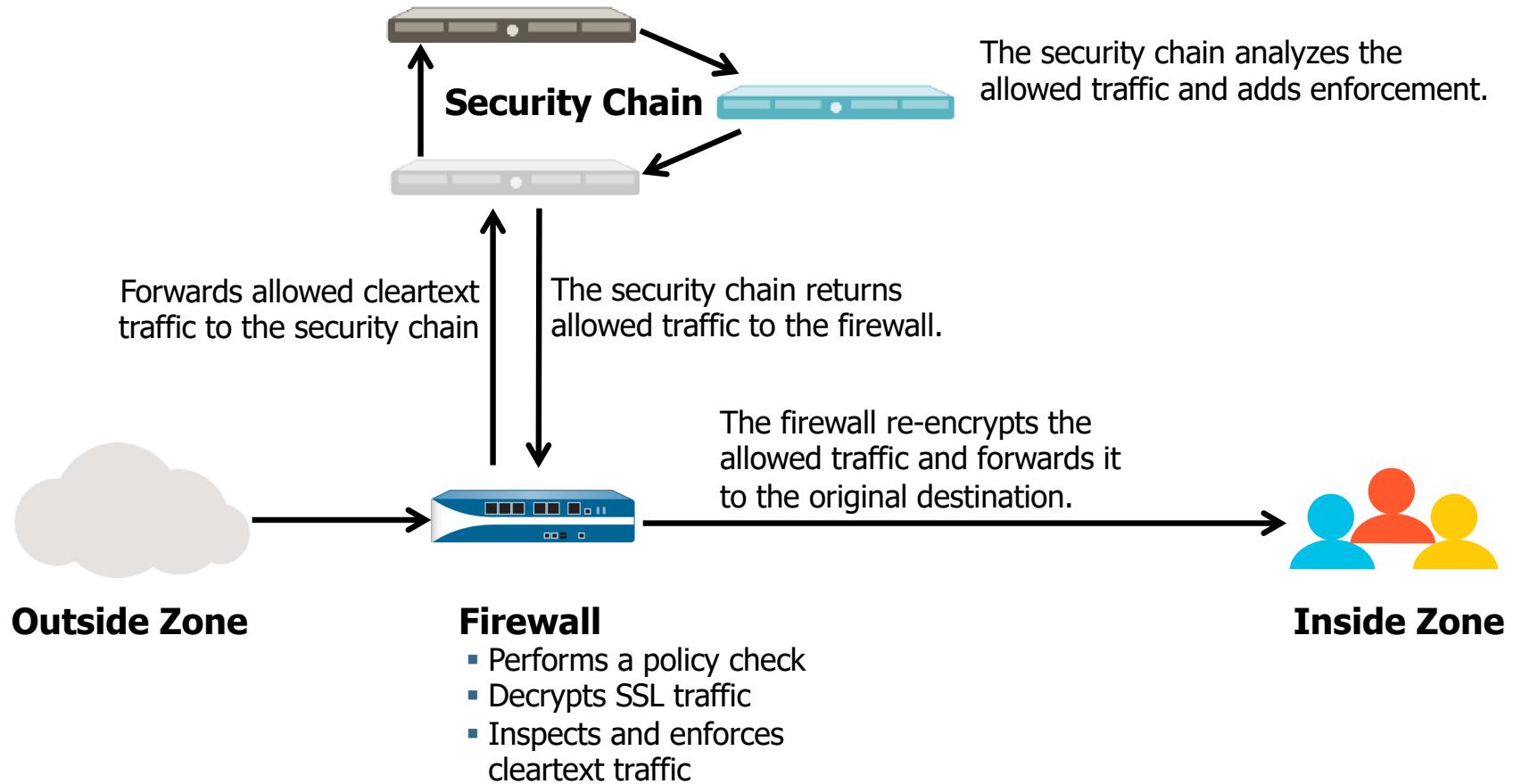
Other decryption methods and features

Decryption Port Mirroring

- Exports decrypted flows out of a dedicated interface on the firewall.
- Use cases include data loss prevention (DLP) and network forensics.
- Requires a free license.

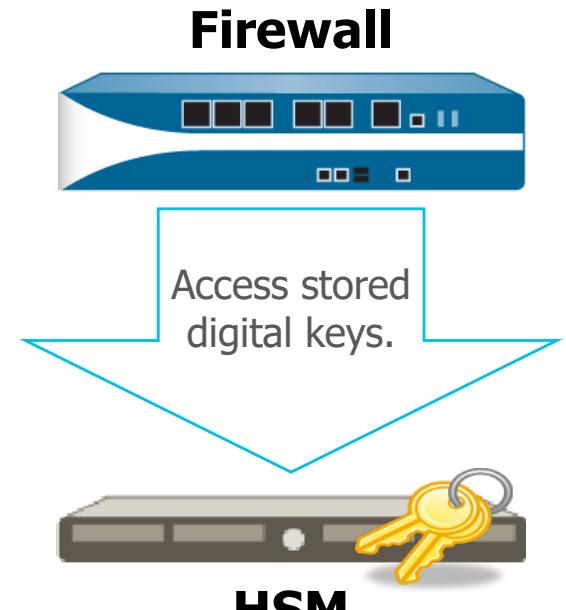


Decryption Broker



Hardware Security Modules (HSMs)

- Physical device designed to safeguard digital keys
- Generates, stores, and manages digital keys
- Used by firewall:
 - SSL Forward Proxy
 - SSL Inbound Inspection
 - Master key storage
 - Private key storage



HSM
Security keys are encrypted
and protected.

Module Summary

Now that you have completed this module,
you should be able to:

- Review fundamental SSL concepts and operation
- Create and manage certificates using the web interface
- Configure SSL/TLS forward proxy decryption
- Configure SSL/TLS inbound inspection decryption
- Prevent decryption for specific traffic
- View information and troubleshoot SSL/TLS issues using the CLI and logs
- Identify decryption configuration considerations
- Configure SSH decryption
- Manage the firewall master key
- List other available decryption methods



Questions



Lab 16: Blocking Threats in Encrypted Traffic

- Test the Firewall Behavior Without Decryption
- Create Self-Signed Certificates for Trusted and Untrusted Connections
- Create and Test a Decryption Policy for Outbound Traffic
- Export the Firewall Certificate
- Test Outbound Decryption with the Imported Certificate
- Review Firewall Logs
- Exclude URL Categories from Decryption
- Test the No-Decryption Rule



**Protecting our
digital way
of life.**