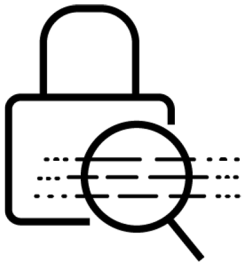
BLOCK THREATS IN ENCRYPTED TRAFFIC



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

paloalto NETWORKS

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

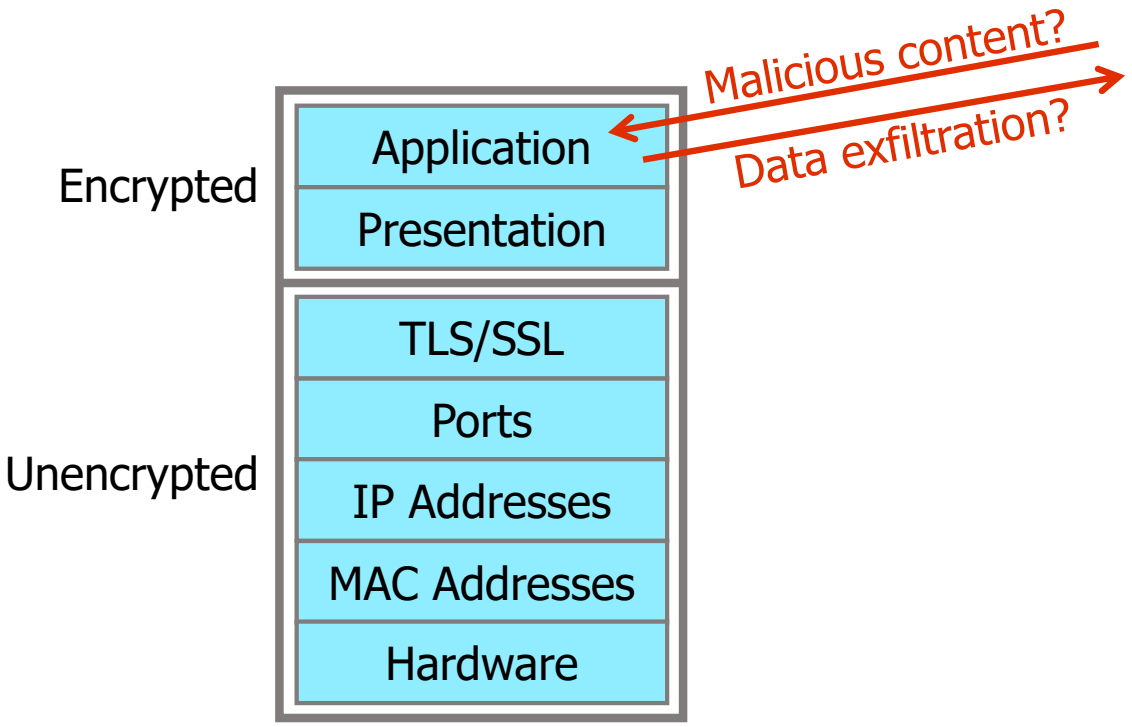
SSH decryption

Master key management

Other decryption methods and features

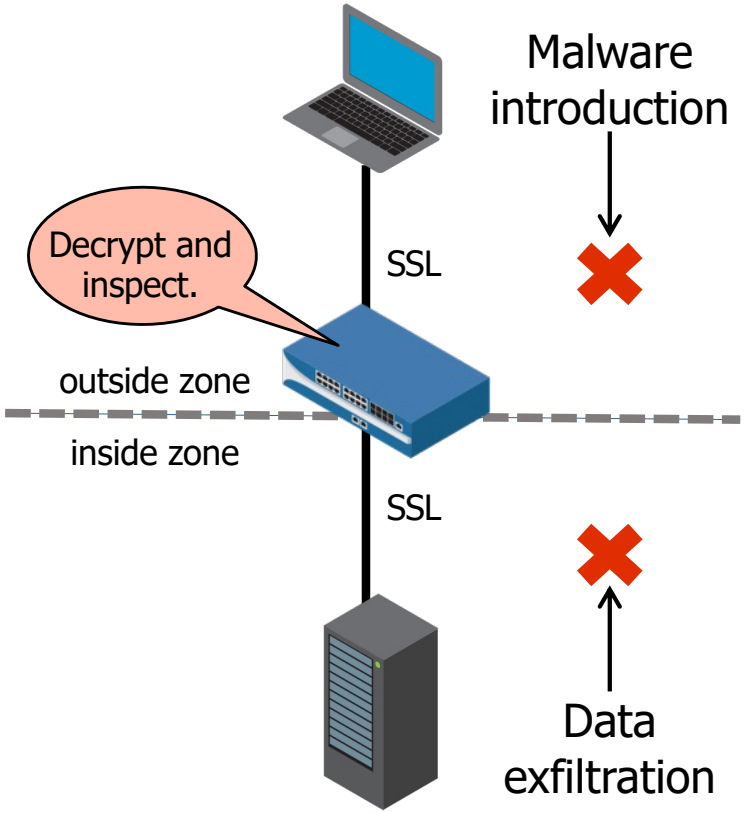
Why Decrypt Network Traffic?

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



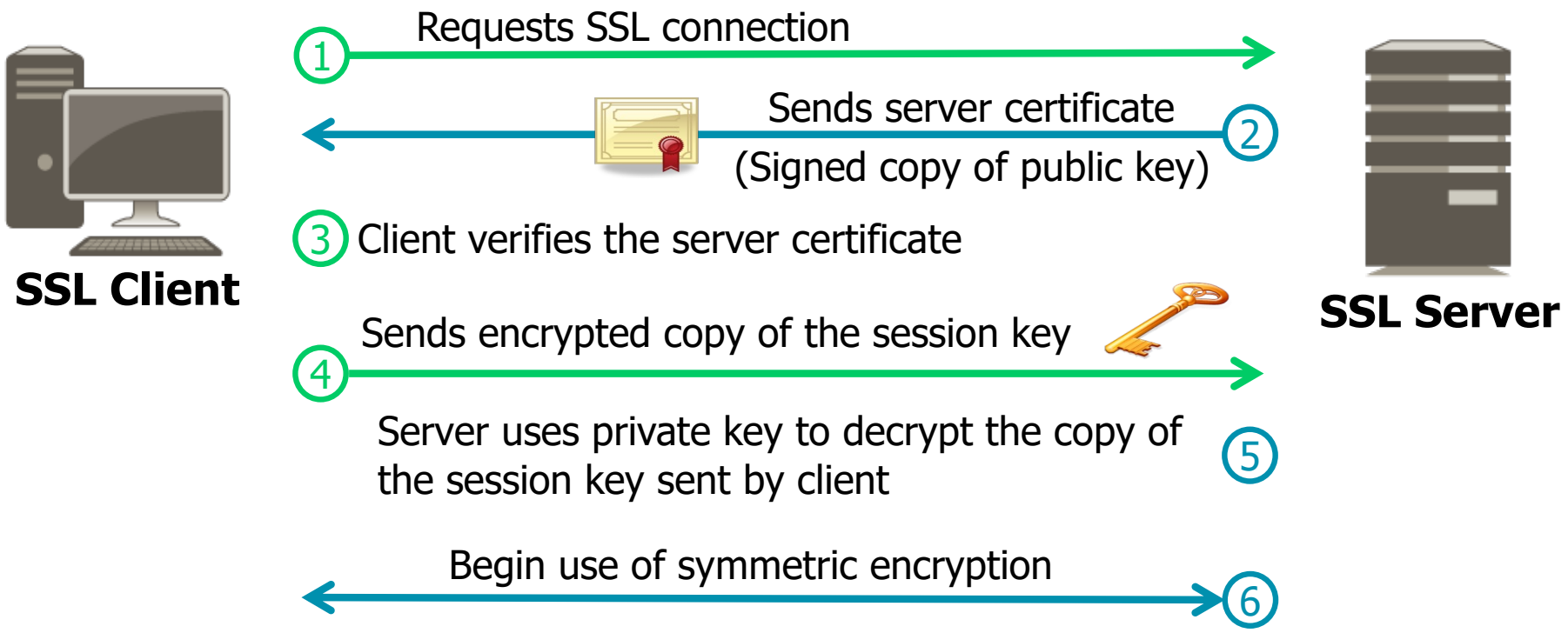
Importance of SSL/TLS

- 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

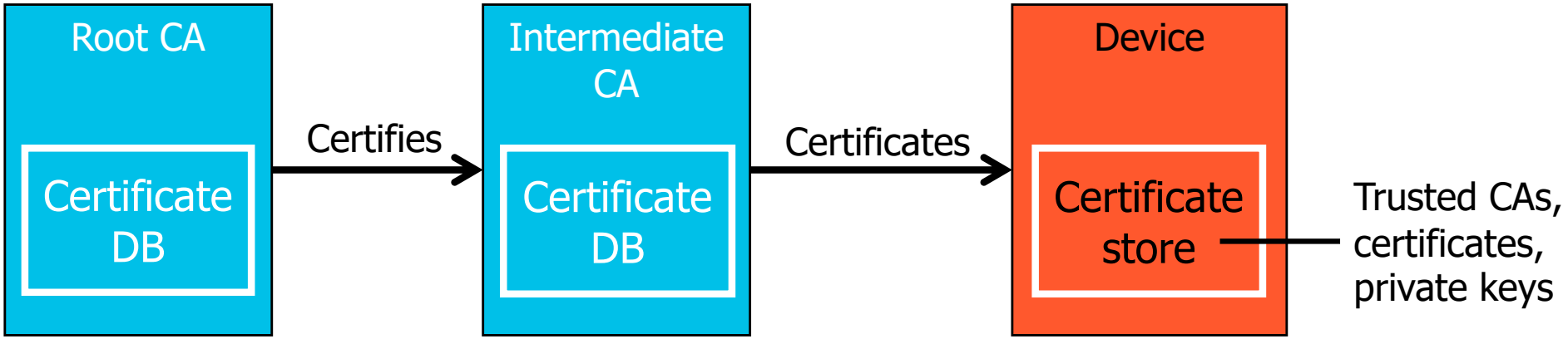
Master key management

Other decryption methods and features

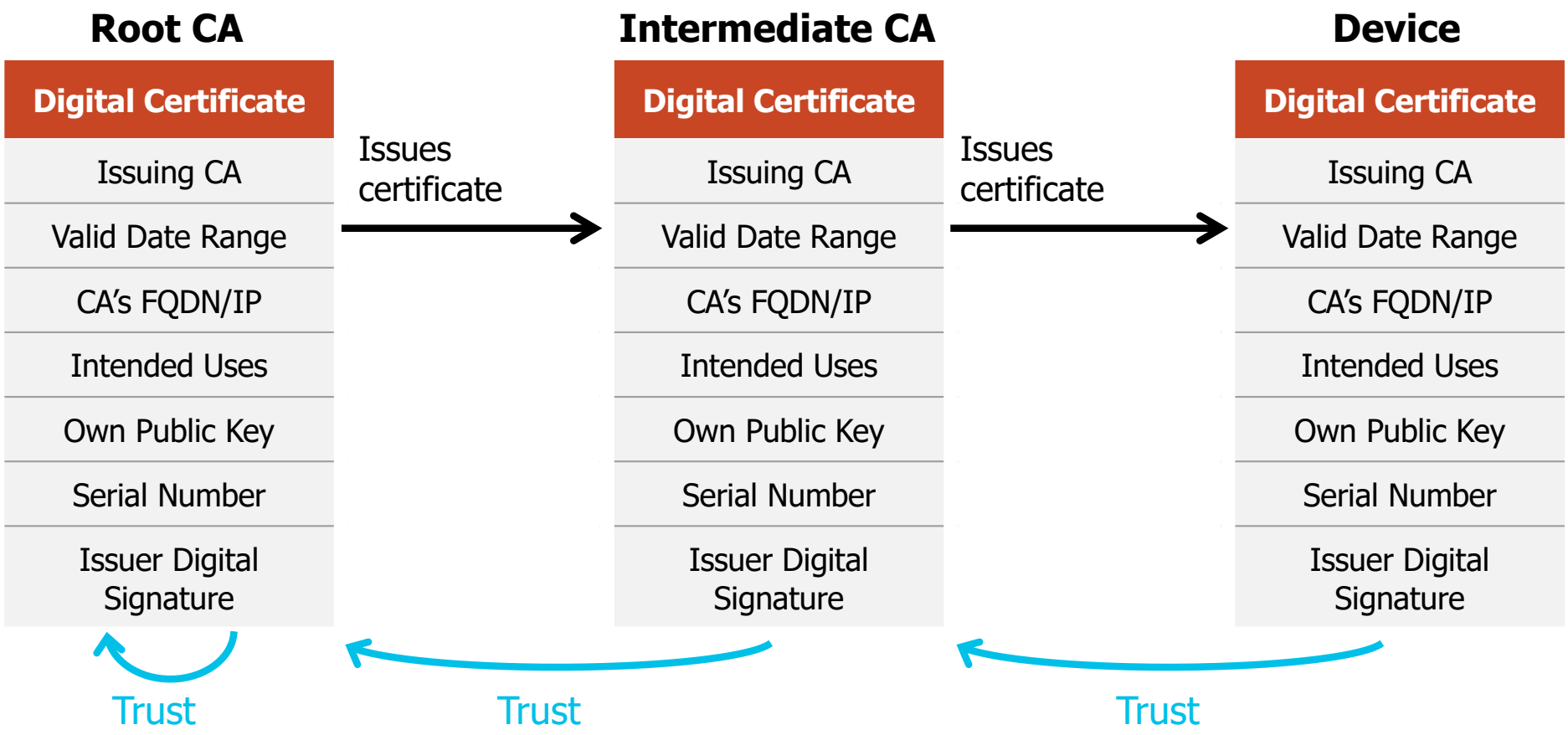
paloalto NETWORKS

Public Key Infrastructure (PKI)

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

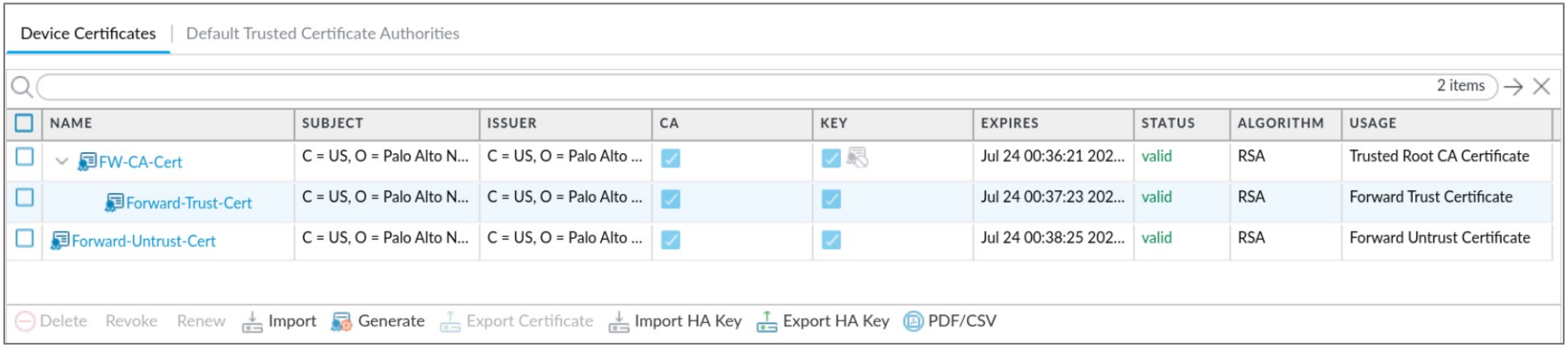


Certificate Chain of Trust



Certificate Management in the Web Interface

Device > Certificate Management > Certificates

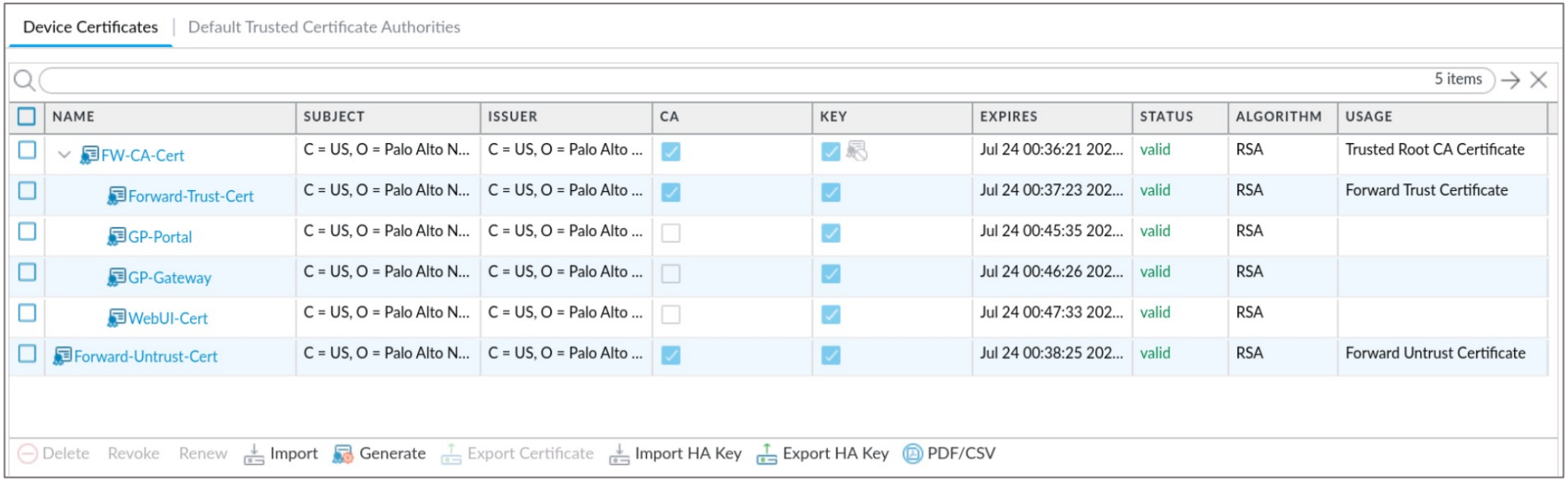


Types of operations:

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

Certificate Hierarchy

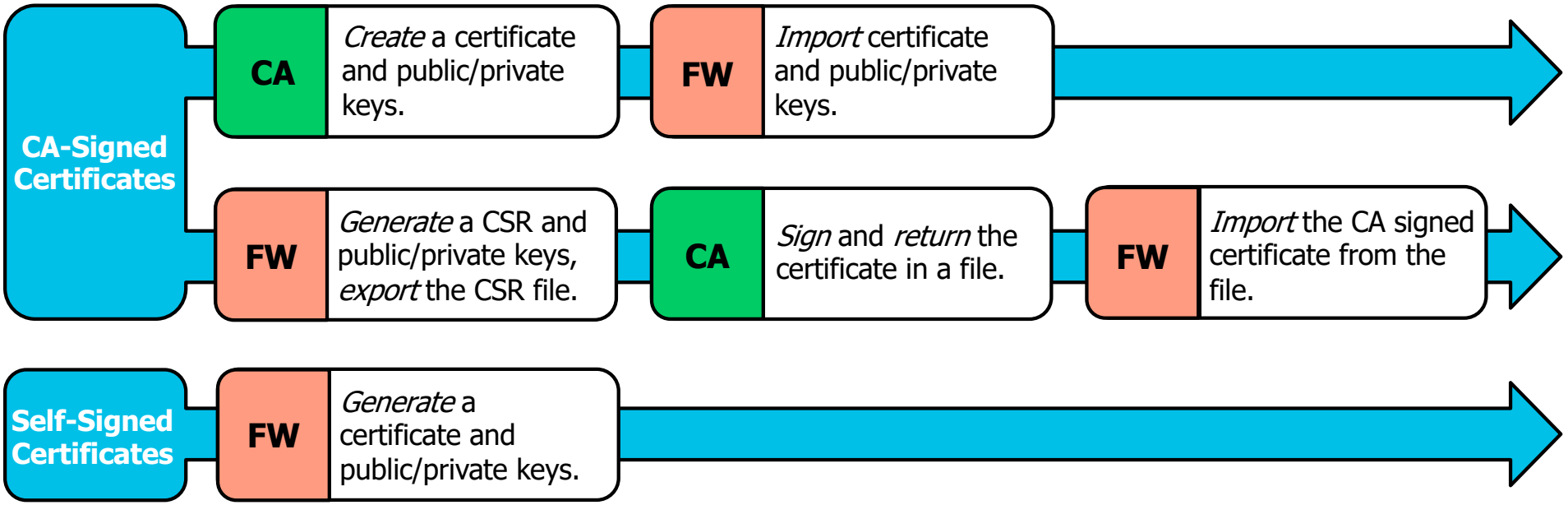
Device > Certificate Management > Certificates



Nested hierarchy visually illustrates the certificate chain of trust.

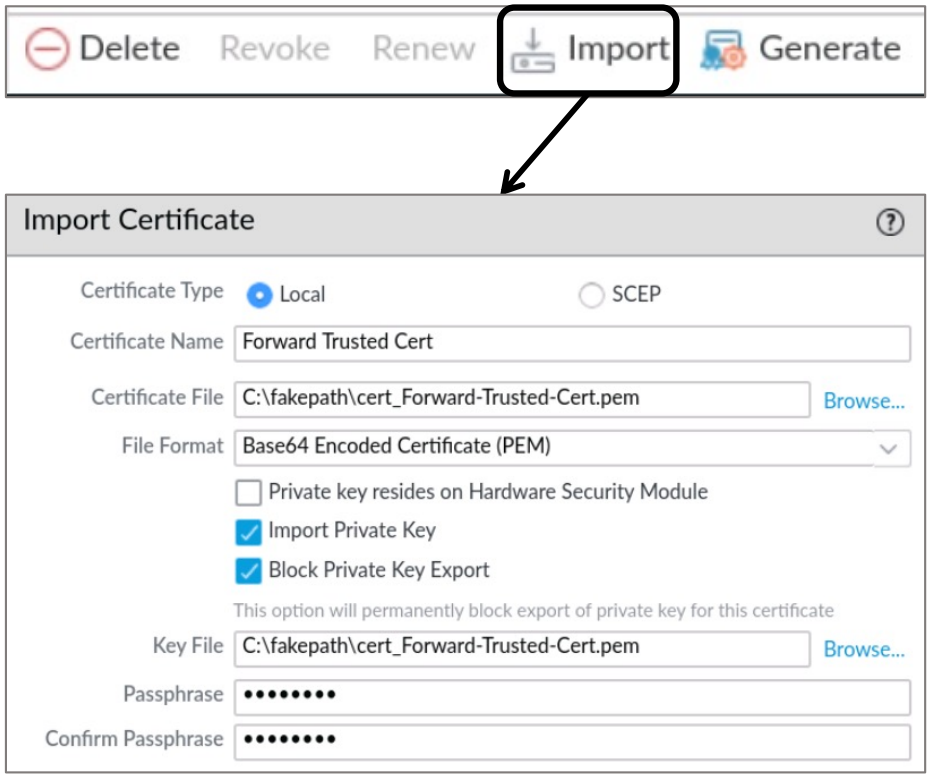
Certificate Creation Overview

Methods to obtain required certificates and public/private keys:



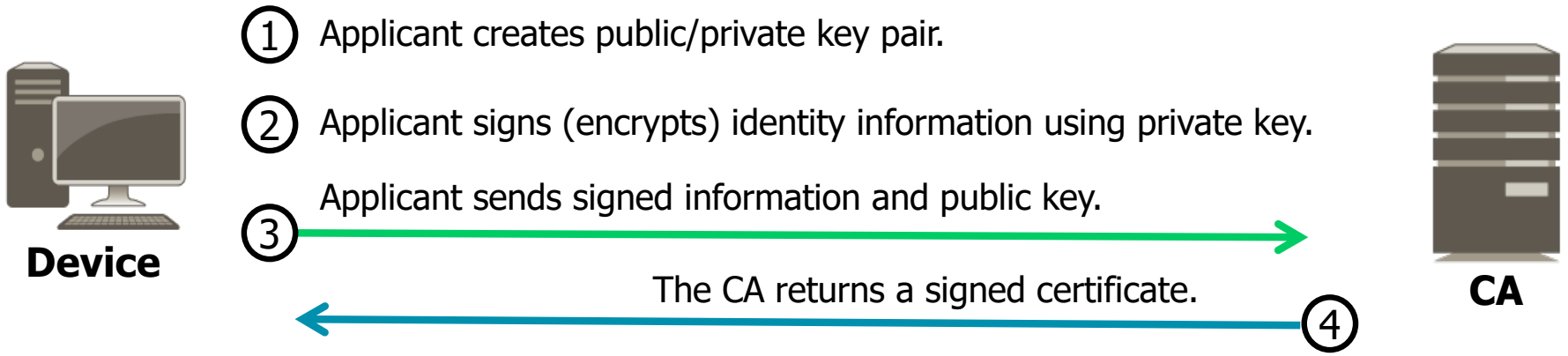
Import a CA Certificate

- 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.



Certificate Signing Request (CSR)

Message sent to CA to acquire a certificate

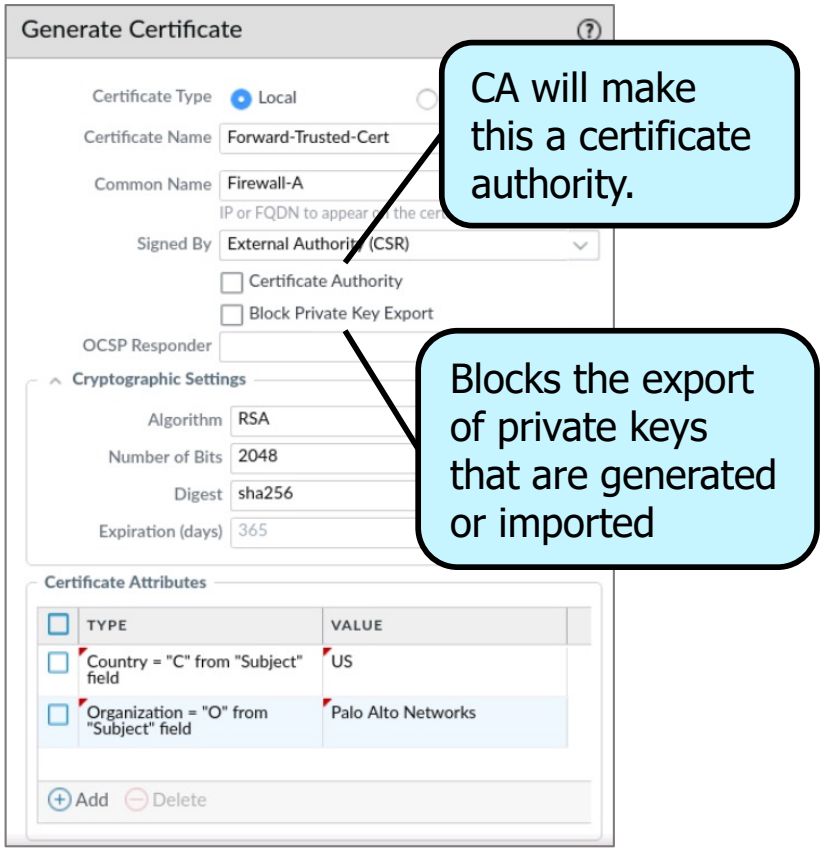


Advantages:

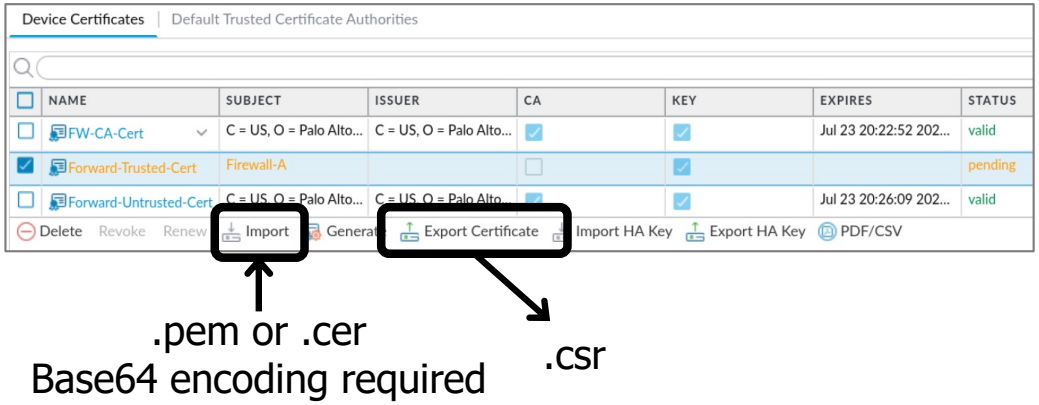
- Device is part of PKI and benefactor of chain of trust.
- Private key never leaves device.

Generate a CSR for the CA-Signed Certificate

Device > Certificate Management > Certificates > Add

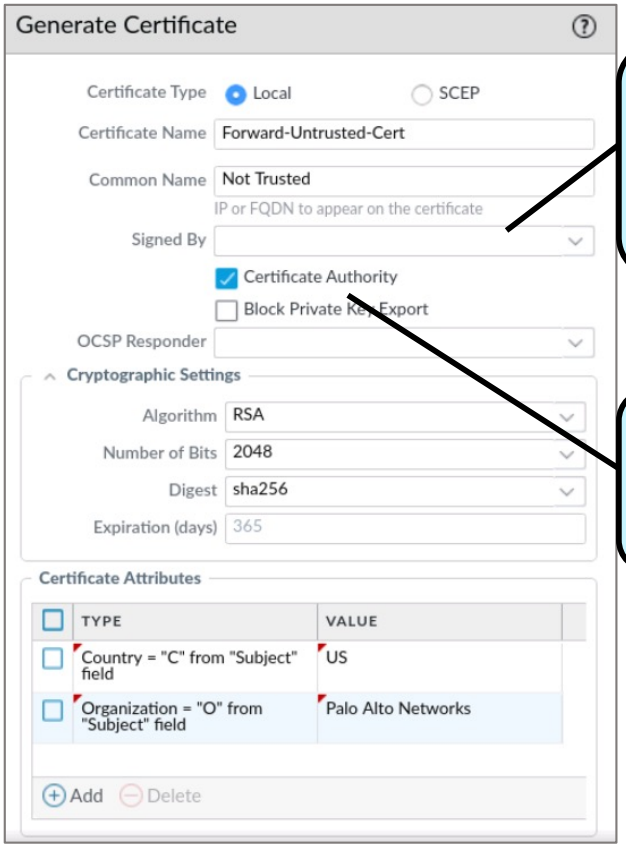


1. Generate a CSR.
2. Export the CSR file to the signing CA.
3. CA returns the signed intermediate CA certificate.
4. Import the signed intermediate CA certificate to the firewall.



Generate a Self-Signed Certificate

Device > Certificate Management > Certificates > Add

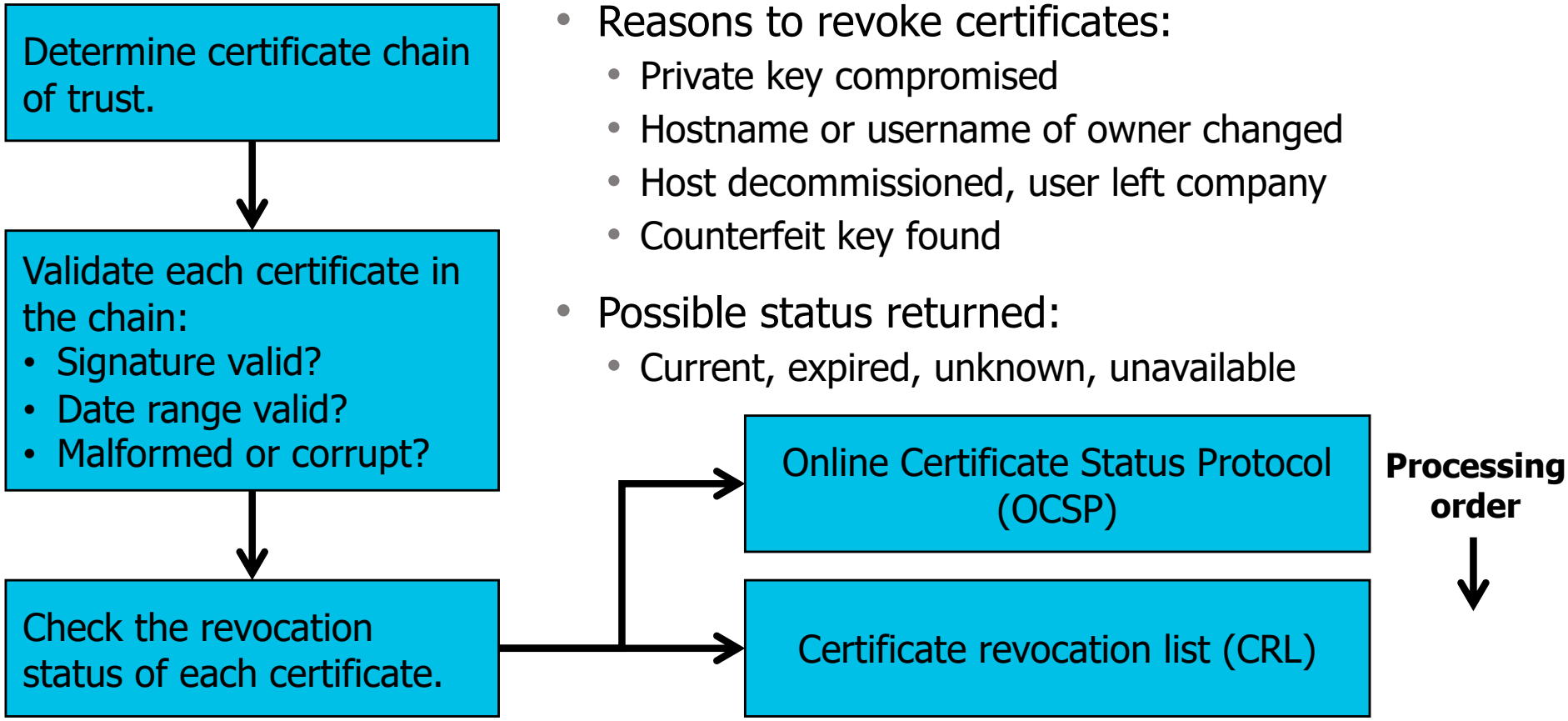


Leave blank to create a self-signed certificate.

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.

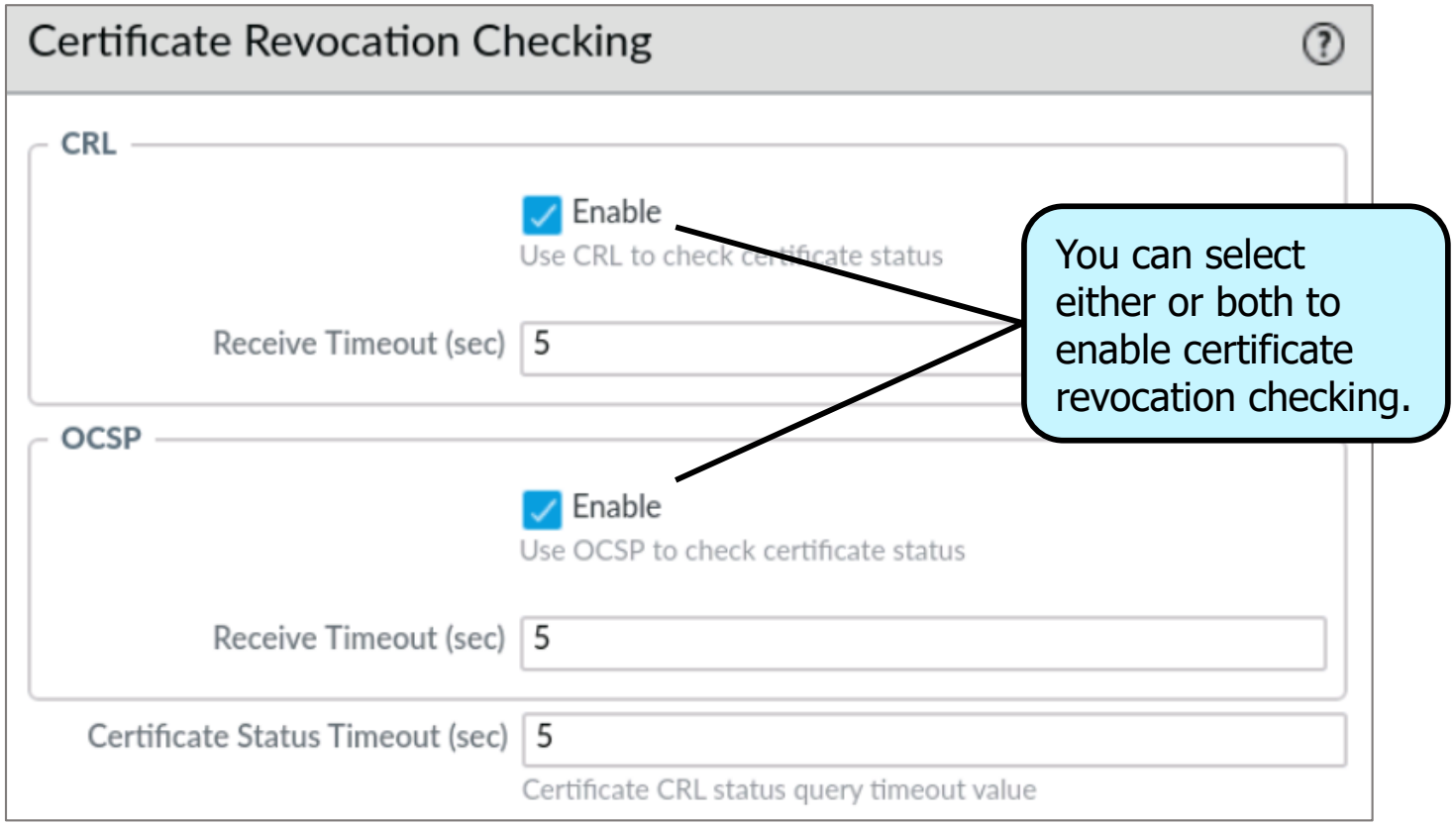
Certificate Checking and Revocation



- Reasons to revoke certificates:
  - Private key compromised
  - Hostname or username of owner changed
  - Host decommissioned, user left company
  - Counterfeit key found
- Possible status returned:
  - Current, expired, unknown, unavailable

Configuring SSL Decryption Certificate Revocation Checking

Device > Setup > Session > Certificate Revocation Checking



SSL/TLS review

Certificate management

SSL/TLS decryption

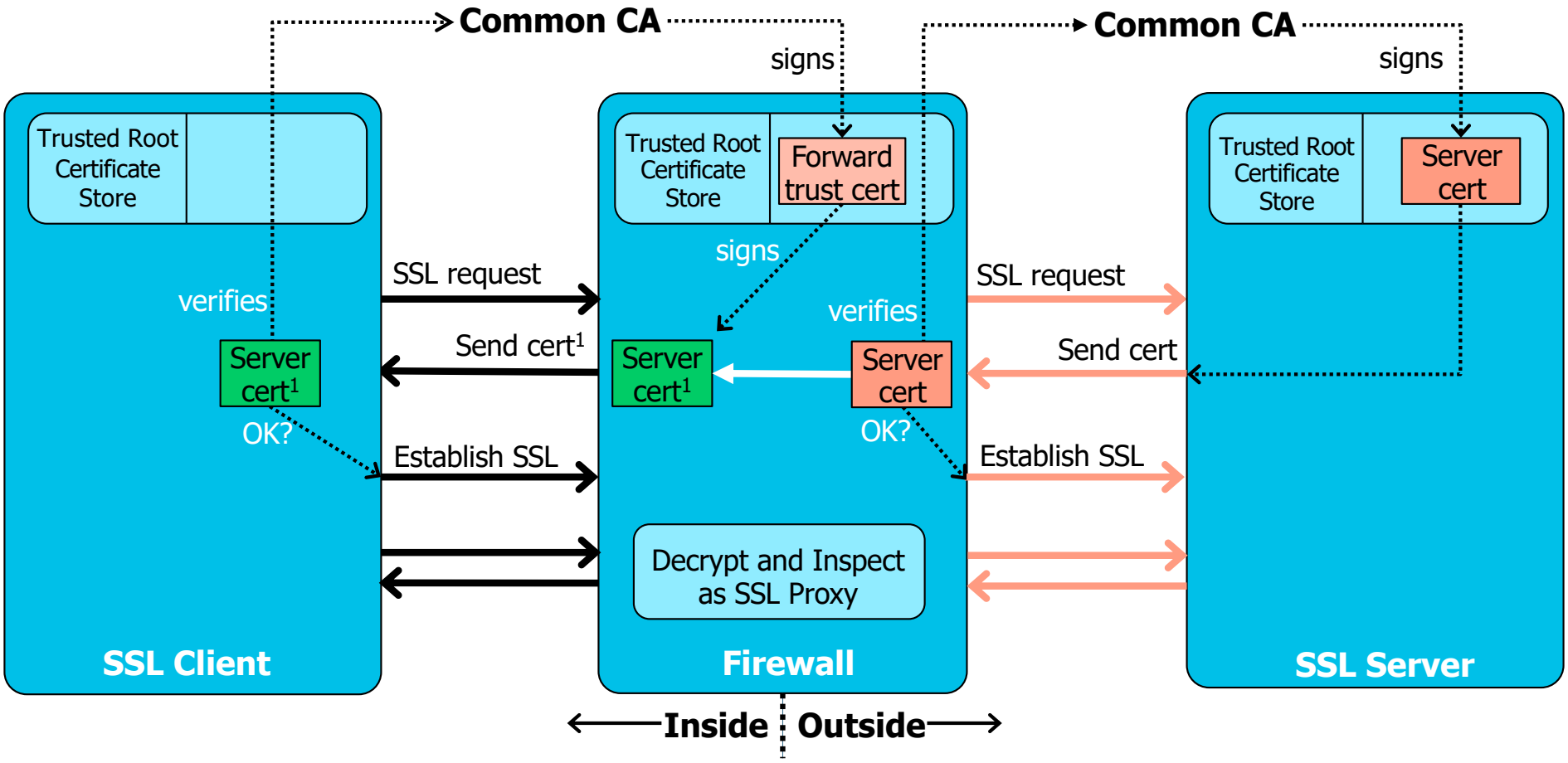
Decryption considerations

SSH decryption

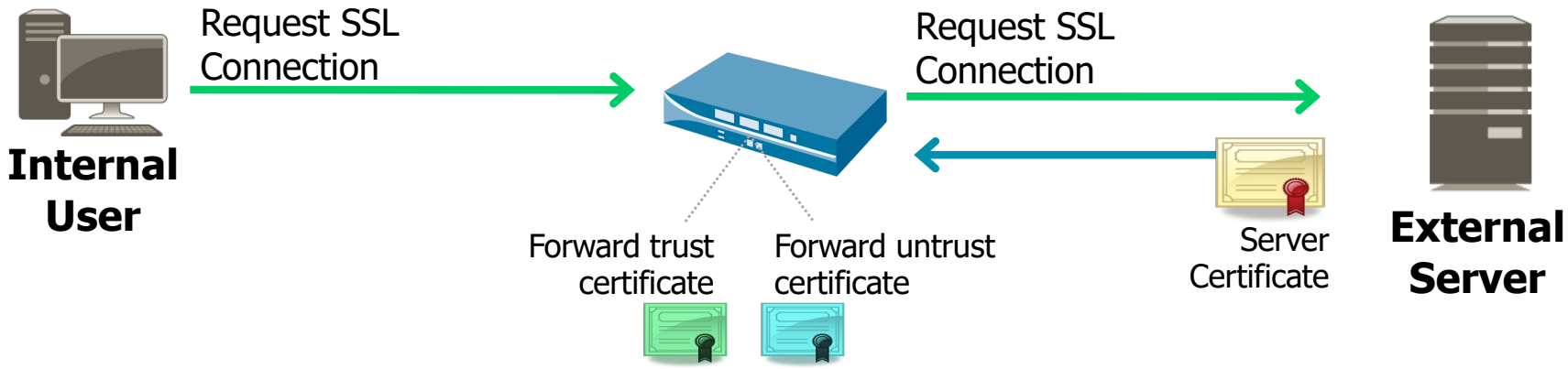
Master key management

Other decryption methods and features

SSL Forward Proxy Review



Forward Trust and Forward Untrust Certificates



Firewall signs a copy of a server certificate with a forward trust certificate.

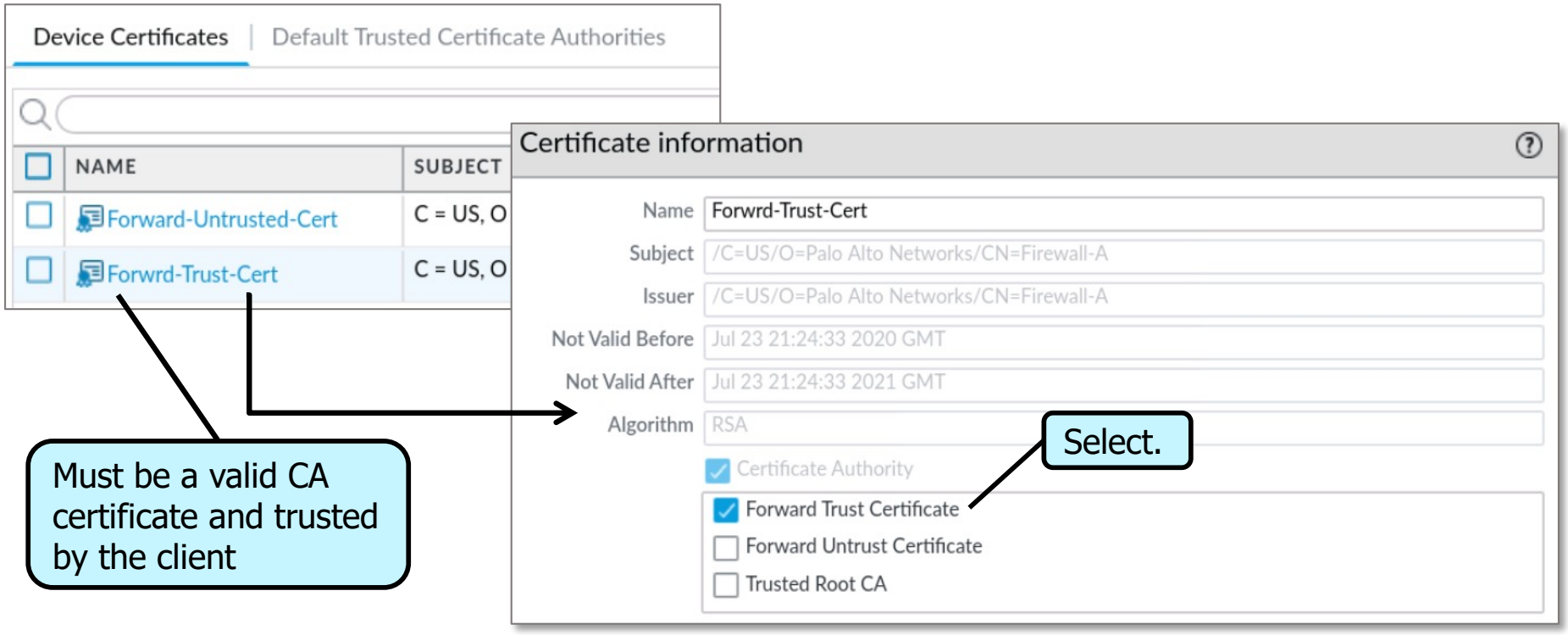
If server certificate is trusted

Firewall signs a copy of a server certificate with a forward untrust certificate.

If server certificate is untrusted

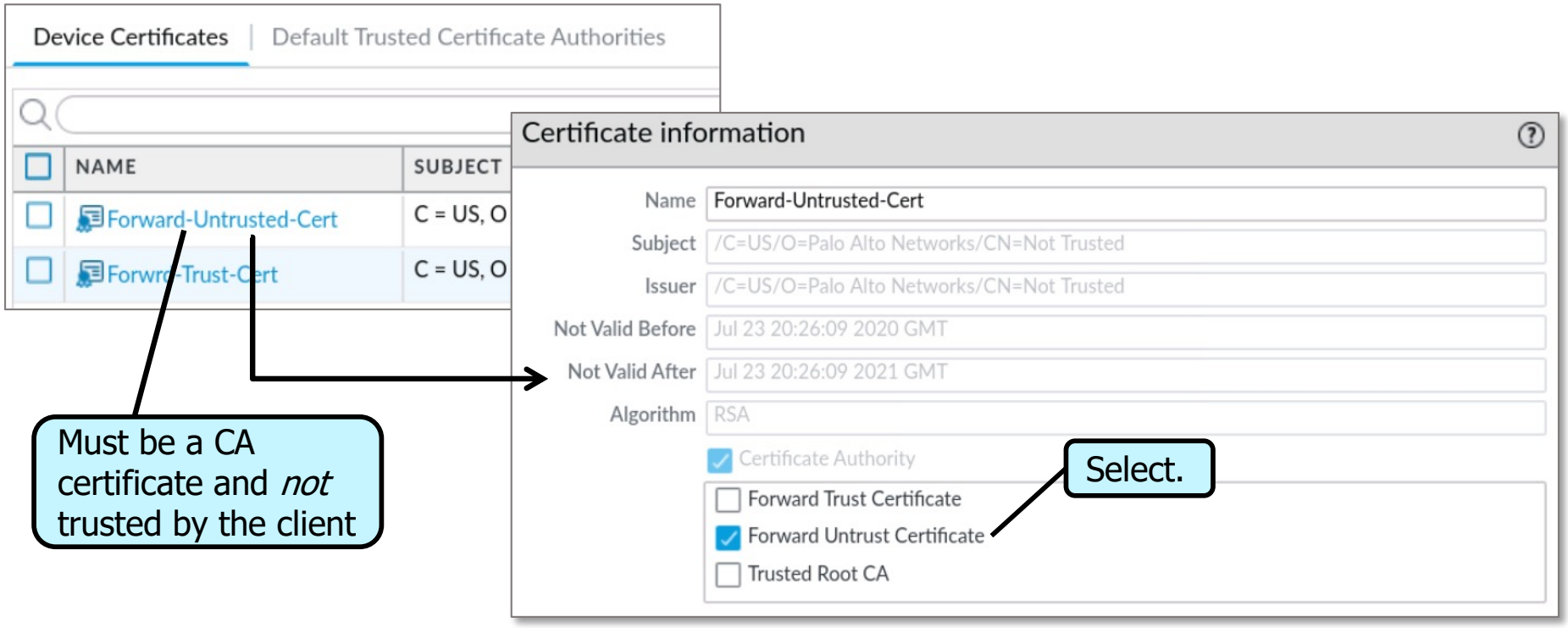
Configure a Forward Trust Certificate

Device > Certificate Management > Certificates



Configure a Forward Untrust Certificate

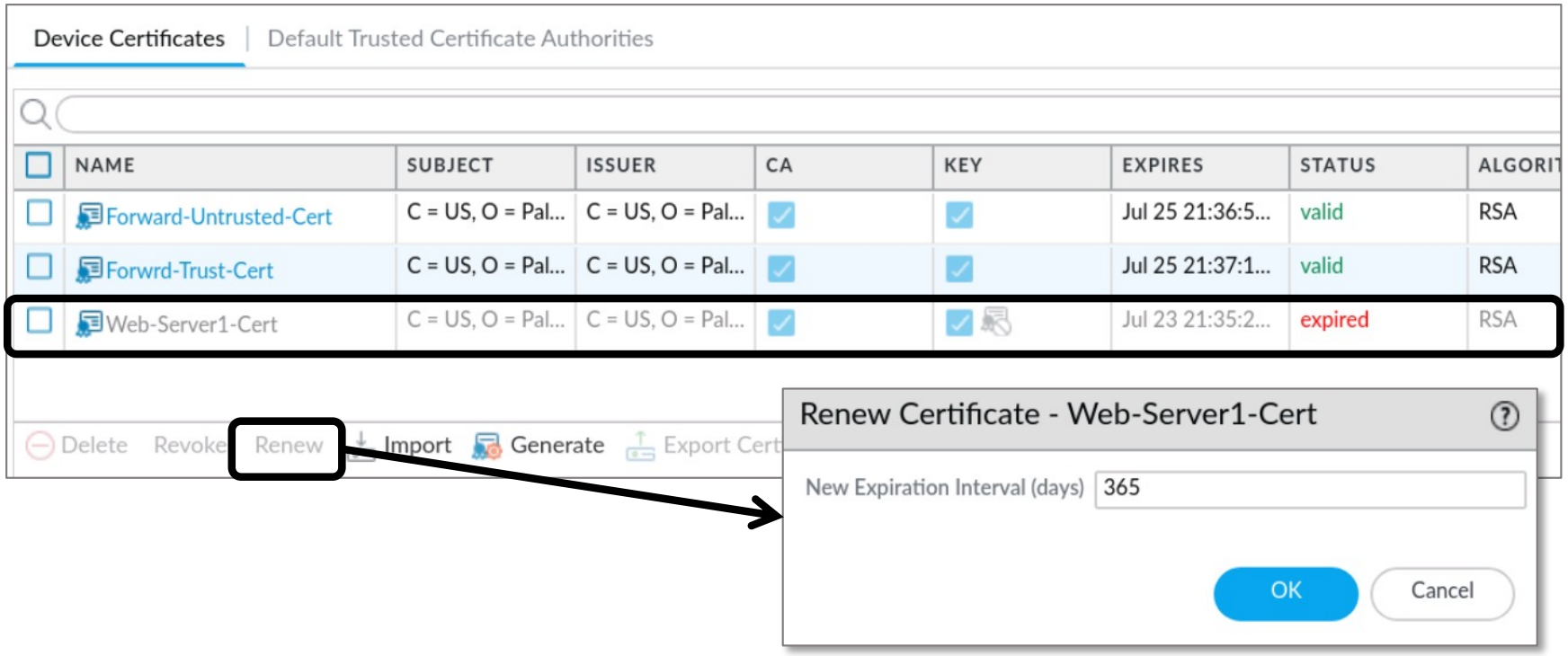
Device > Certificate Management > Certificates



Renew an SSL Forward Untrust Certificate

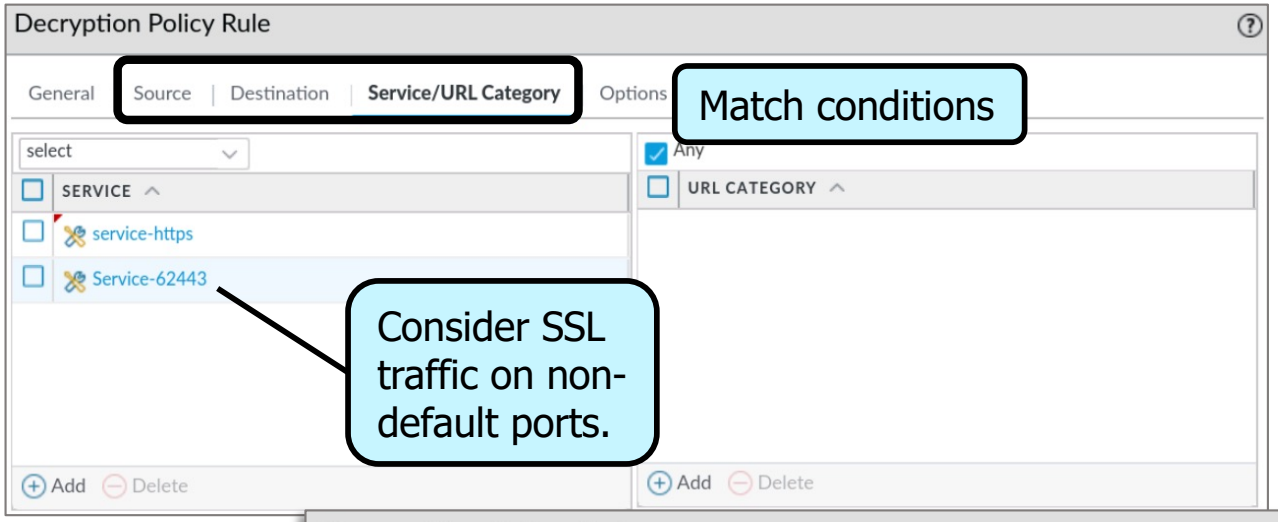
Renews SSL forward untrust certificate issued by the firewall

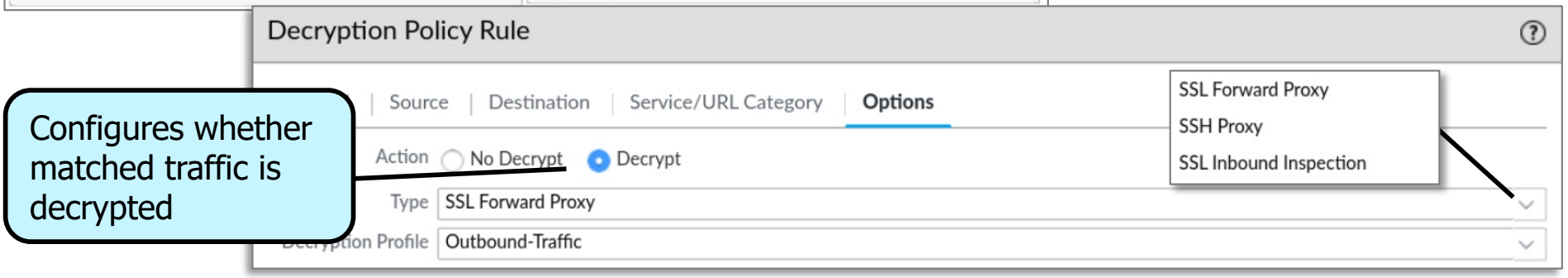
Device > Certificate Management > Certificates



Configure SSL Forward Proxy Decryption Policy

Policies > Decryption

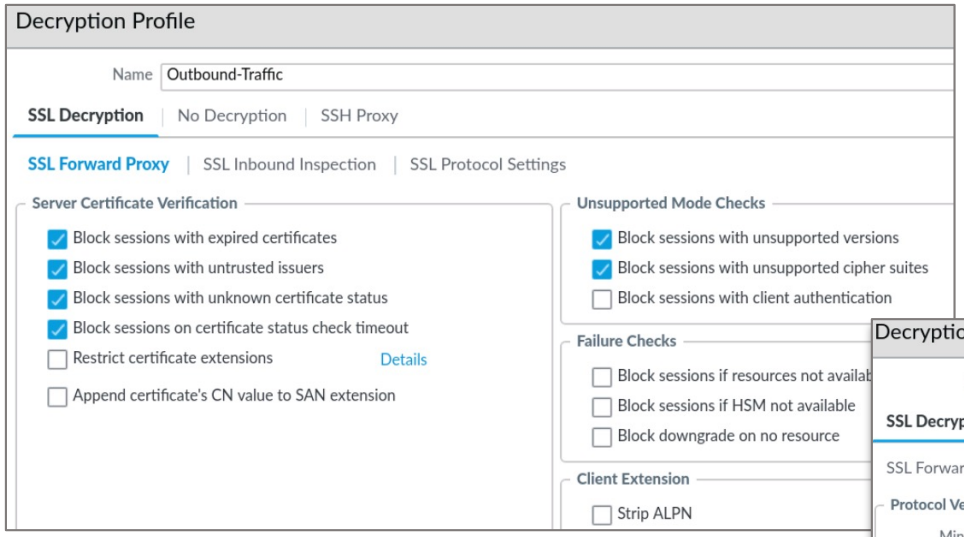




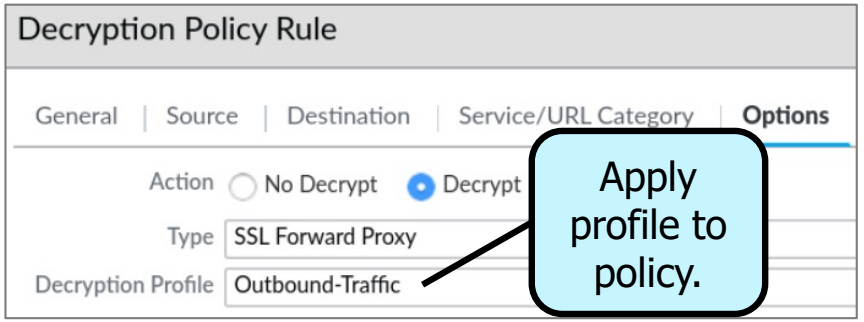
- Use rule fields to control what is decrypted.
- Phase in decryption to minimize user issues.
- Decryption subject to legal and privacy concerns (health, HR, finance, etc.)
- Create a Security policy rule to allow the traffic.

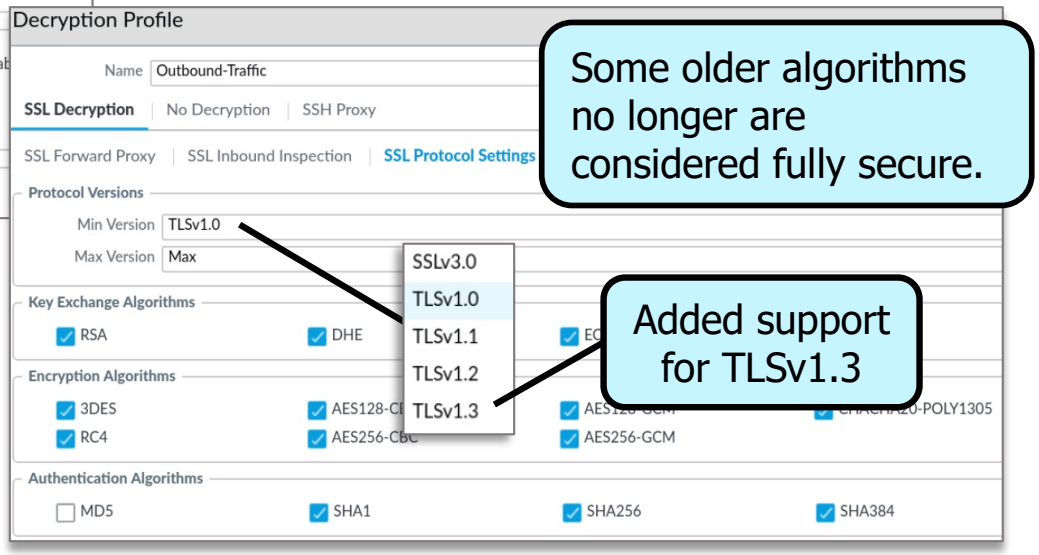
Forward Proxy Decryption Profile

Objects > Decryption > Decryption Profile



Policies > Decryption





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

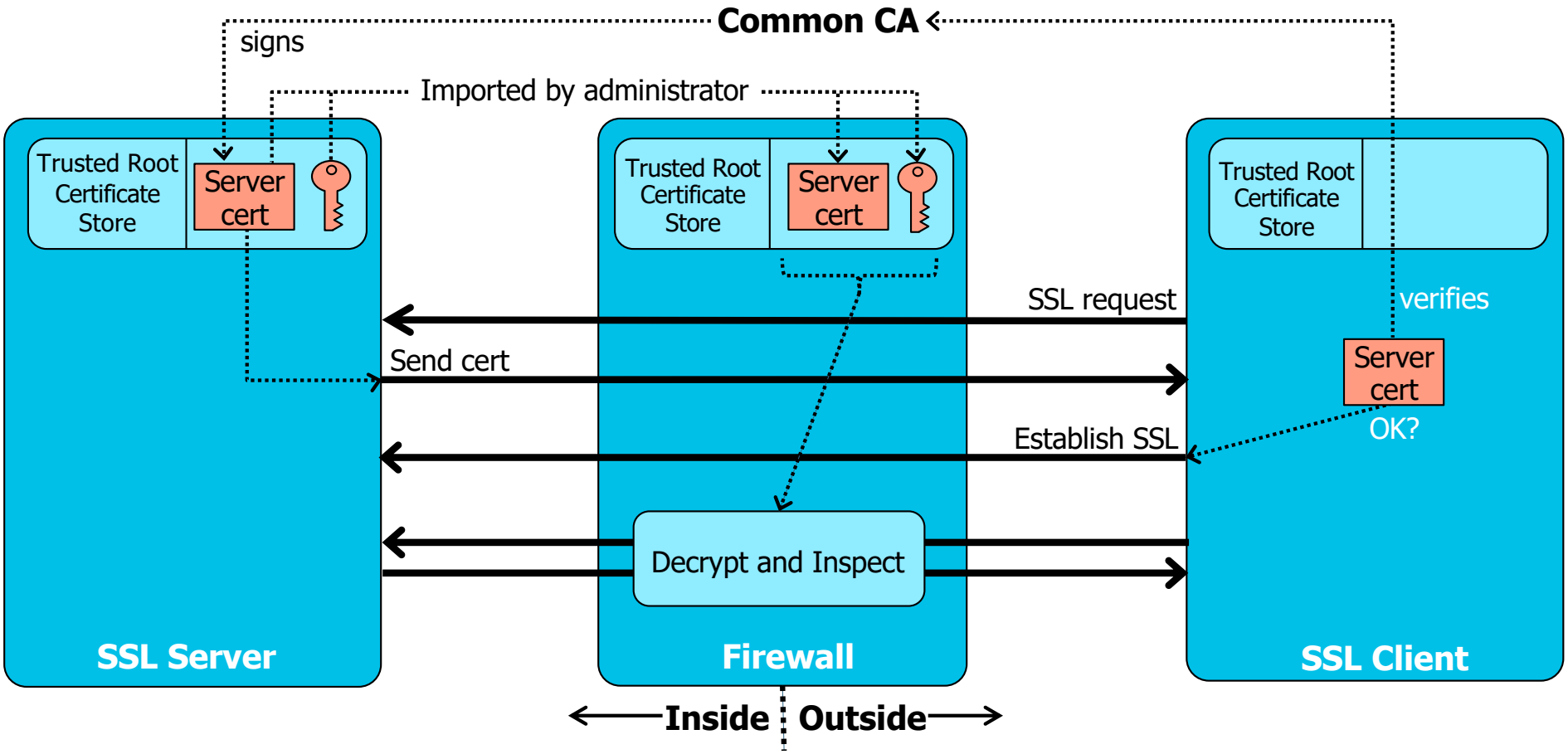
Create the Corresponding Security Policy Rules

- 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

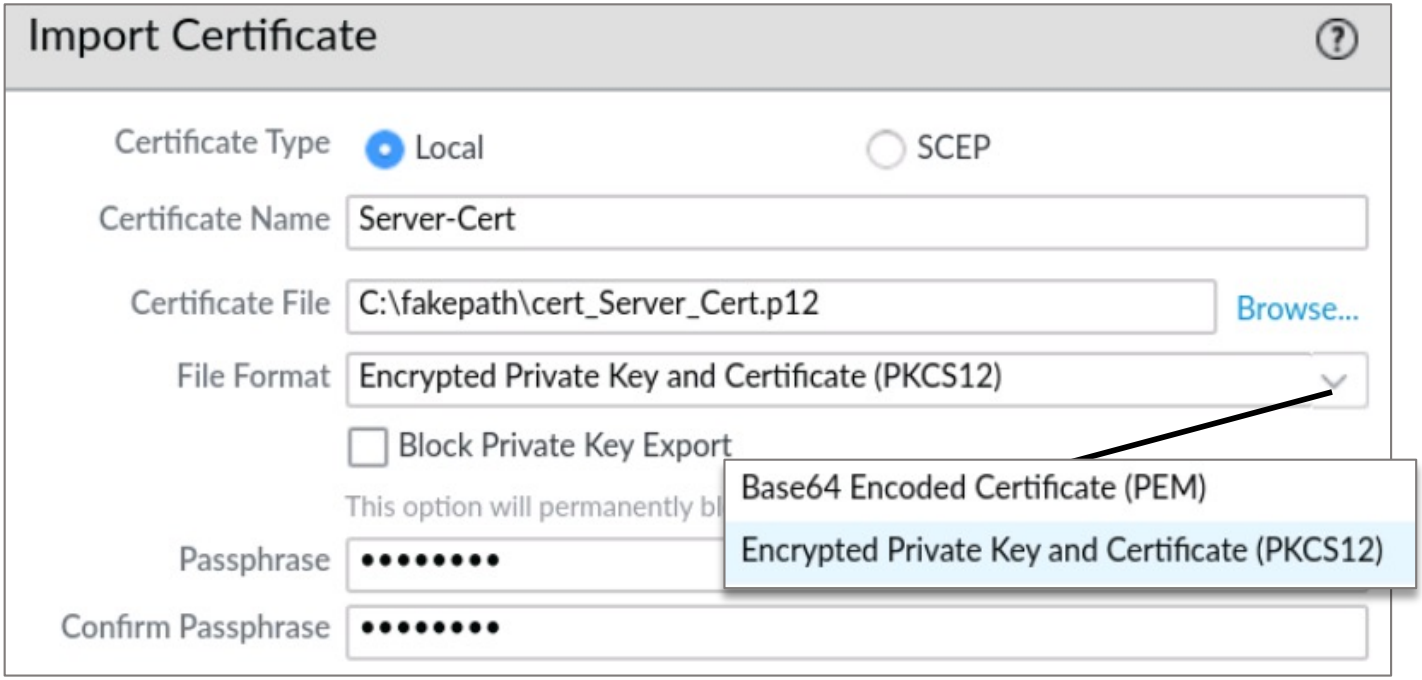
SSL Inbound Inspection Review



Import Server Certificate and Private Key

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

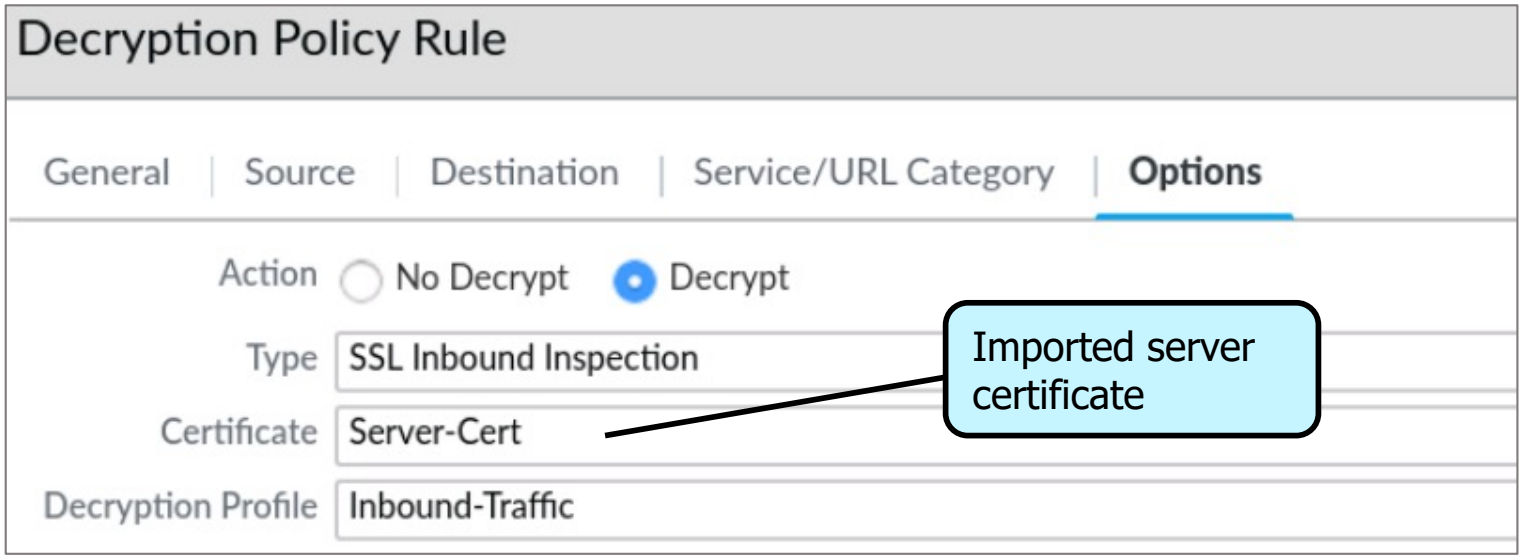
Device > Certificate Management > Certificates > Import



Configure an SSL Inbound Inspection Policy

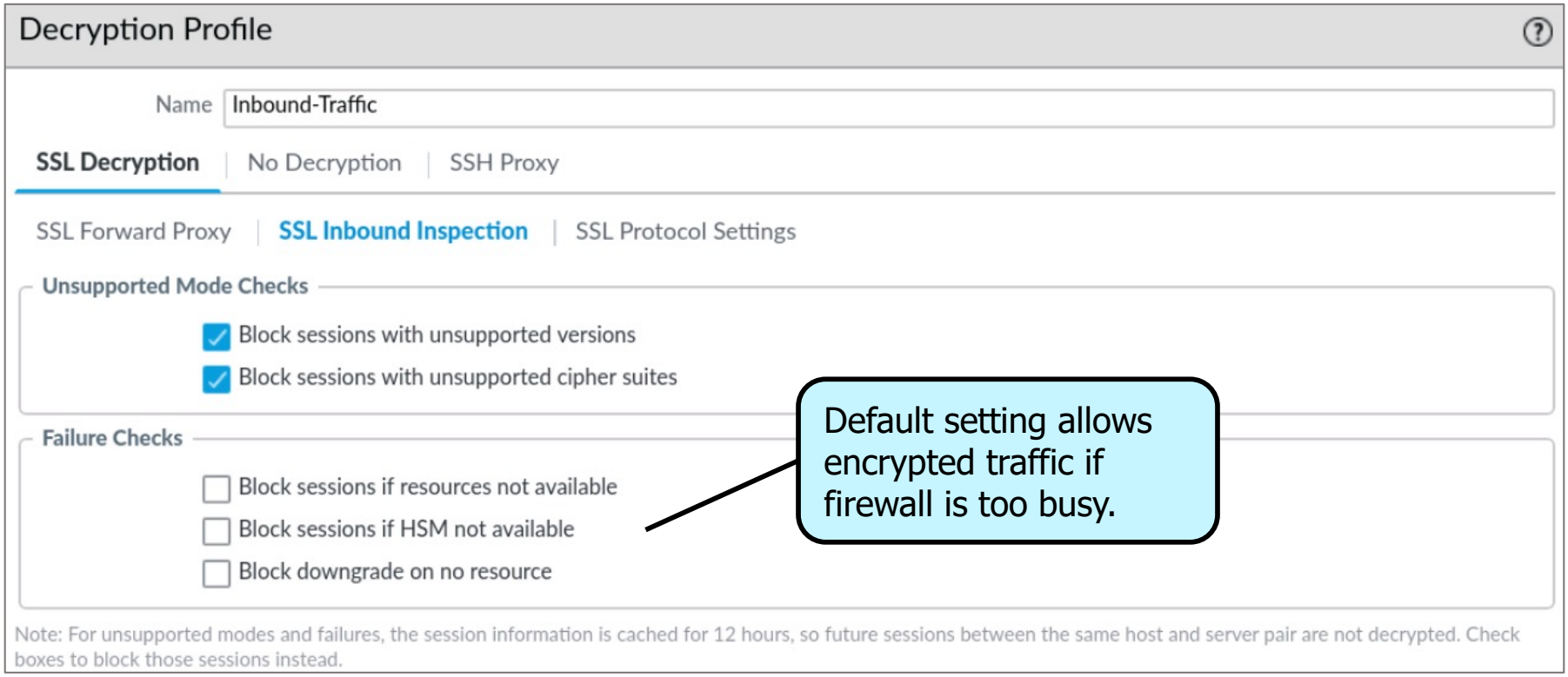
- An SSL Inbound Inspection policy rule specifies what to inspect.
- An attached profile specifies additional protocol and firewall resource checks.
- Create a Security policy rule that allows traffic.

Policies > Decryption > Add



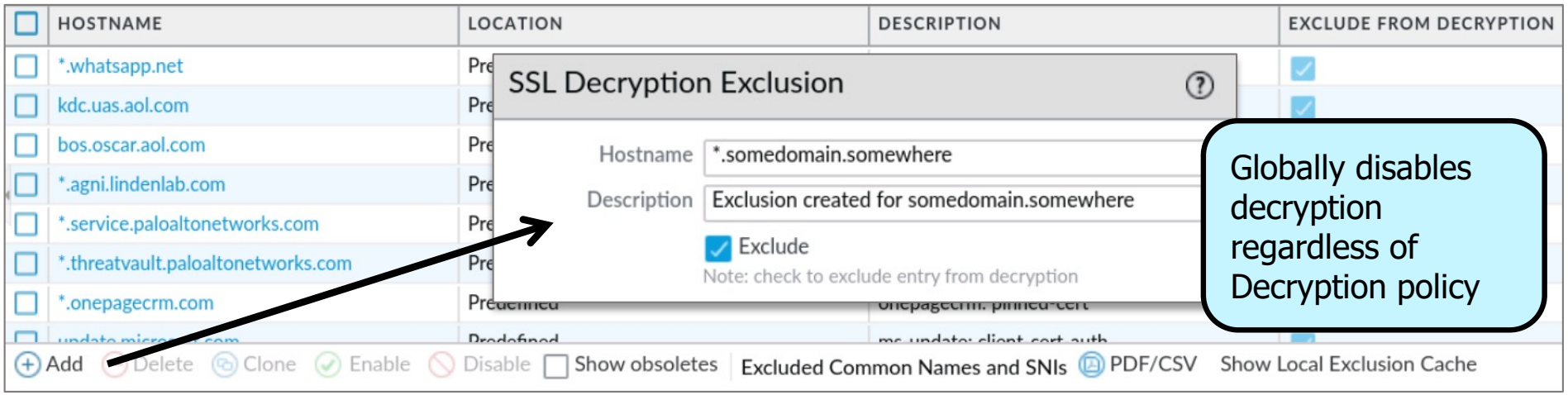
Configure an Inbound Inspection Decryption Profile

Objects > Decryption > Decryption Profile > Add



Decryption Exclusions

Device > Certificate Management > SSL Decryption Exclusion



- 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.

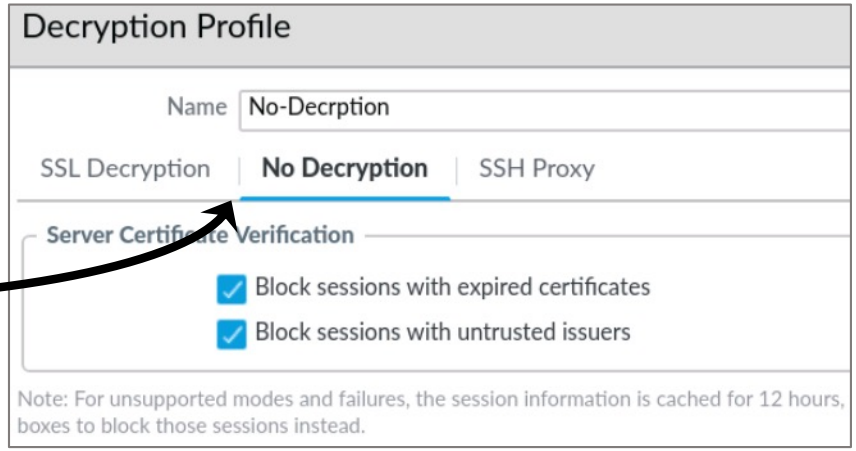
No Decryption

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

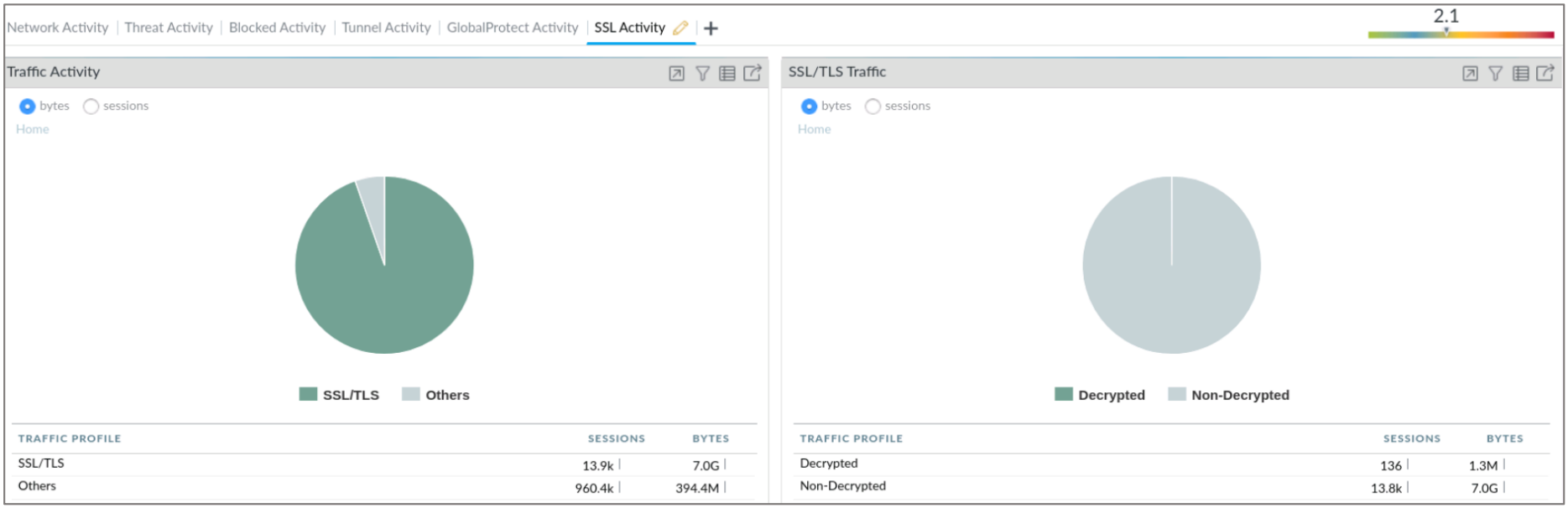


SSL Decryption Troubleshooting

Monitor > Logs > Decryption

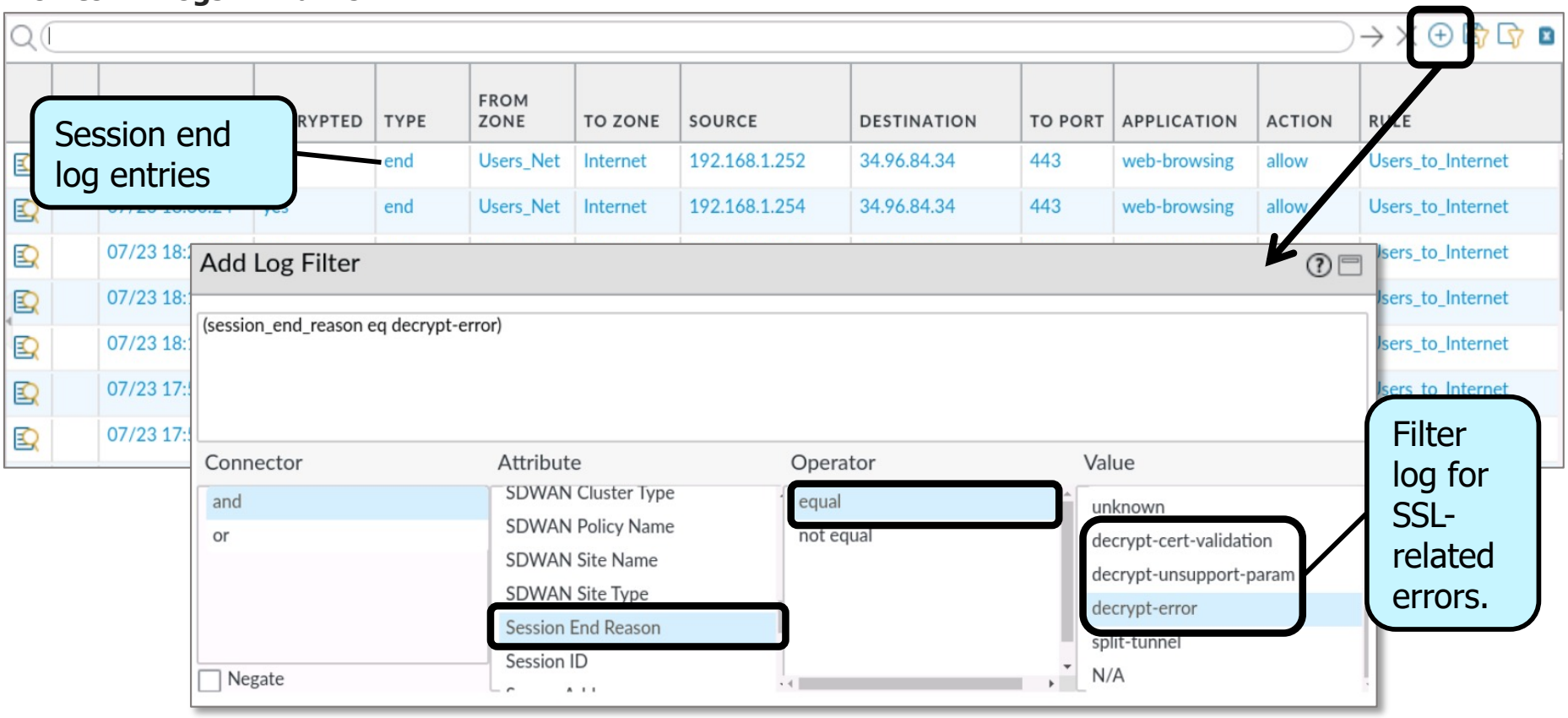
	RECEIVE TIME	APPLICATION	POLICY NAME	SOURCE ZONE	DESTINA... ZONE	PROXY TYPE	SOURCE ADDRESS	DESTINATION ADDRESS	ROOT STATUS	TLS VERSION	KEY EXCHANGE	ENCRYPTION ALGORITHM
	07/23 18:05:00	web-browsing	Decrypts_User_Traffic	Users_Net	Internet	Forward	192.168.1.20	172.217.12.42	trusted	TLS1.2	ECDHE	AES_128_GCM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



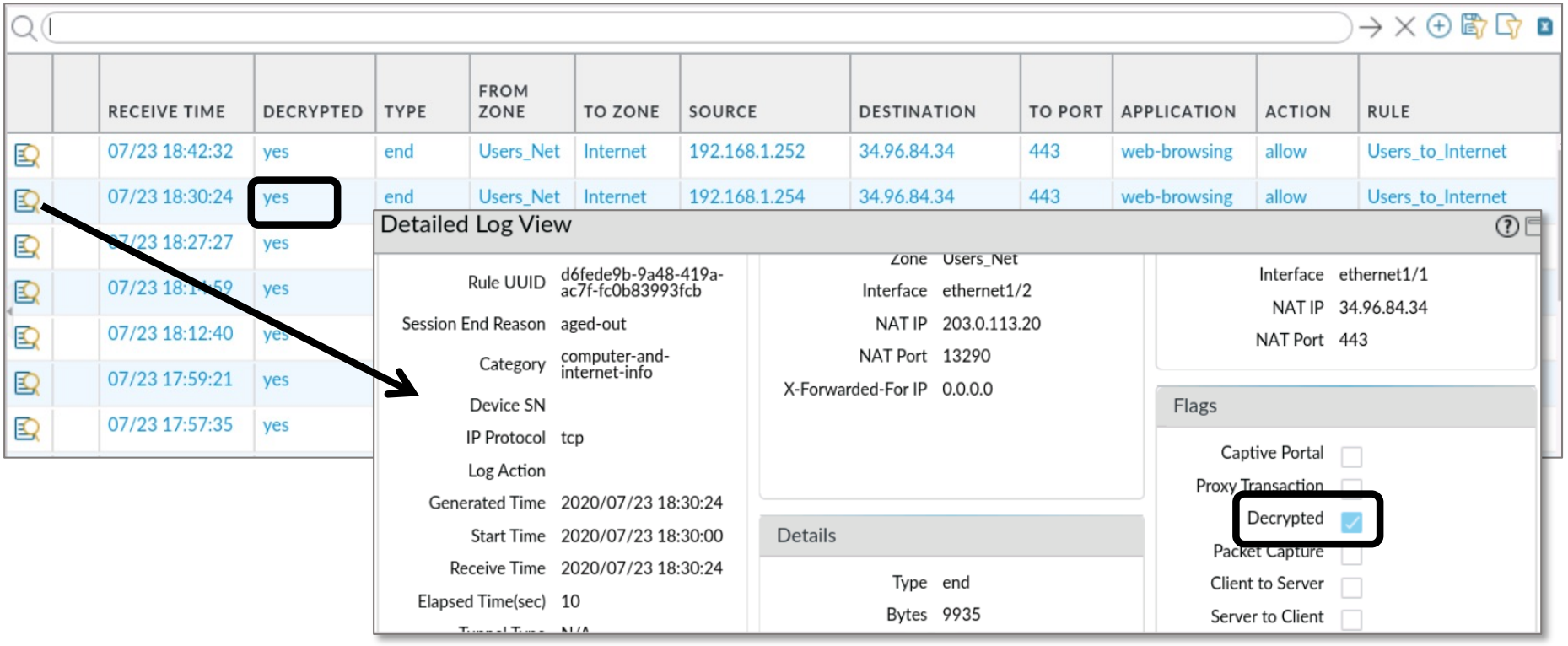
Troubleshoot SSL Session Terminations

Monitor > Logs > Traffic



Decryption in the Traffic Log

Monitor > Logs > Traffic



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   192.168.1.2
vsys1                                            23.211.85.1
12055         web-browsing   ACTIVE   FLOW *NS   192.168.1.2
```

* = decrypted
NS = Source NAT

SSL/TLS review

Certificate management

SSL/TLS decryption

Decryption considerations

SSH decryption

Master key management

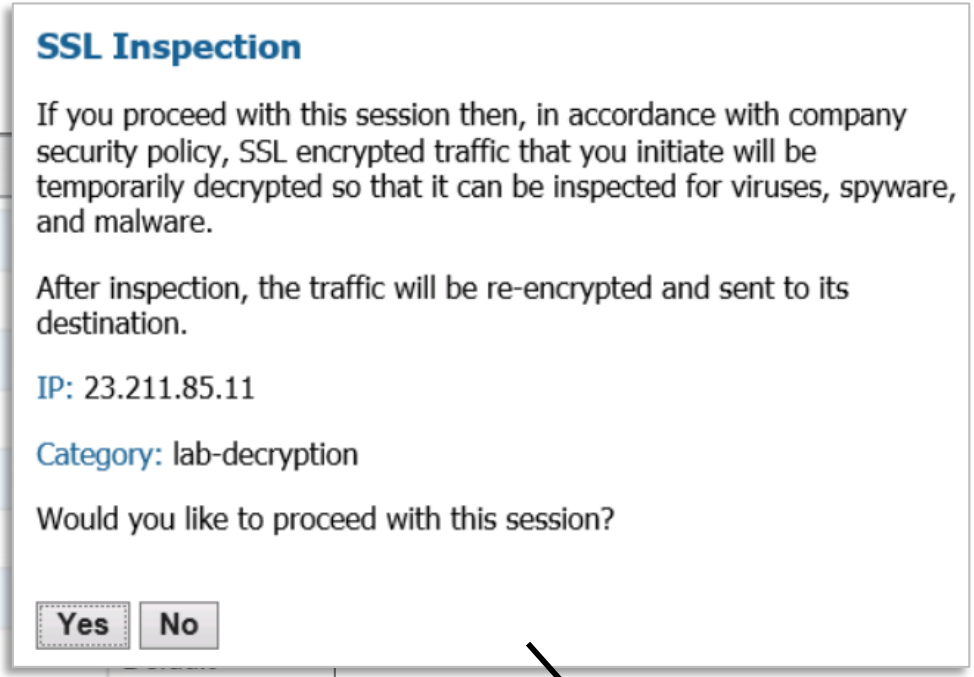
Other decryption methods and features

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	Default
URL Filtering and Category Match Block Page		Default
URL Filtering Continue and Override Page		Default

Click to enable.



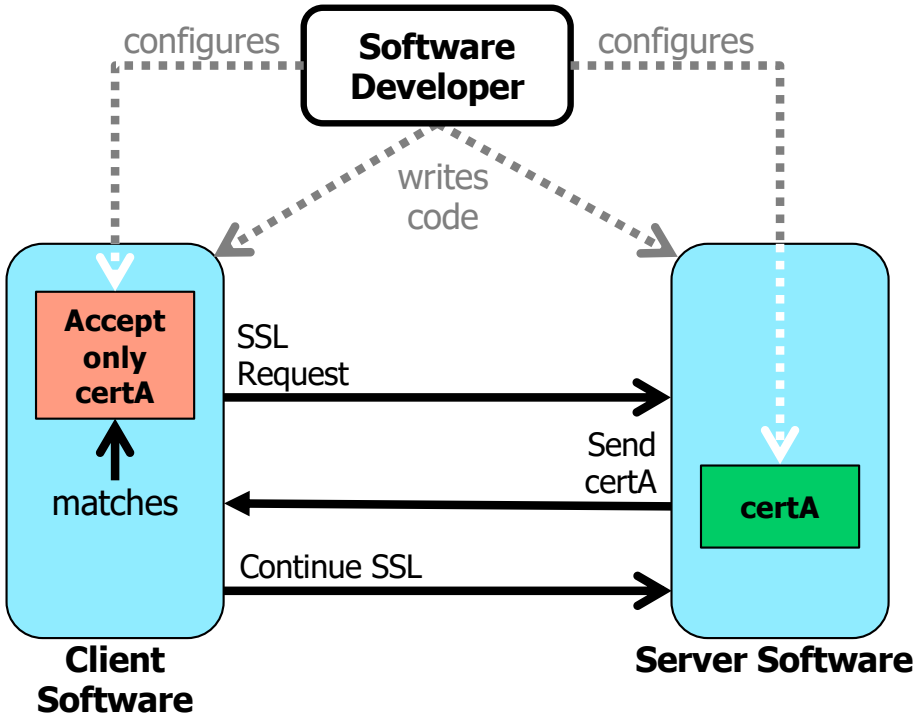
Enables users to refuse connections to decrypted sites

SSL Decryption Policy Considerations

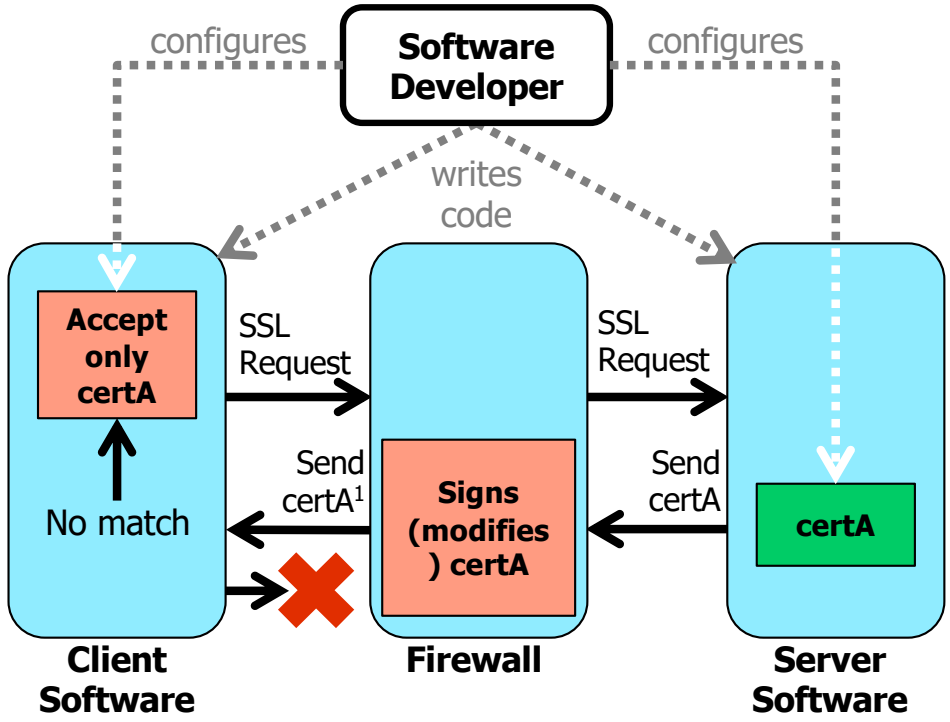
- Certificate or key pinning can affect SSL decryption configuration.
- Client is preconfigured to know which certificate or keys to expect or accept.
- Defeats use of counterfeit or man-in-the-middle keys or certificates.
- Two types of certificate pinning:
  - Static server certificate pinning
  -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

Static Server Certificate Pinning

Server Certificate Pinning – No Firewall



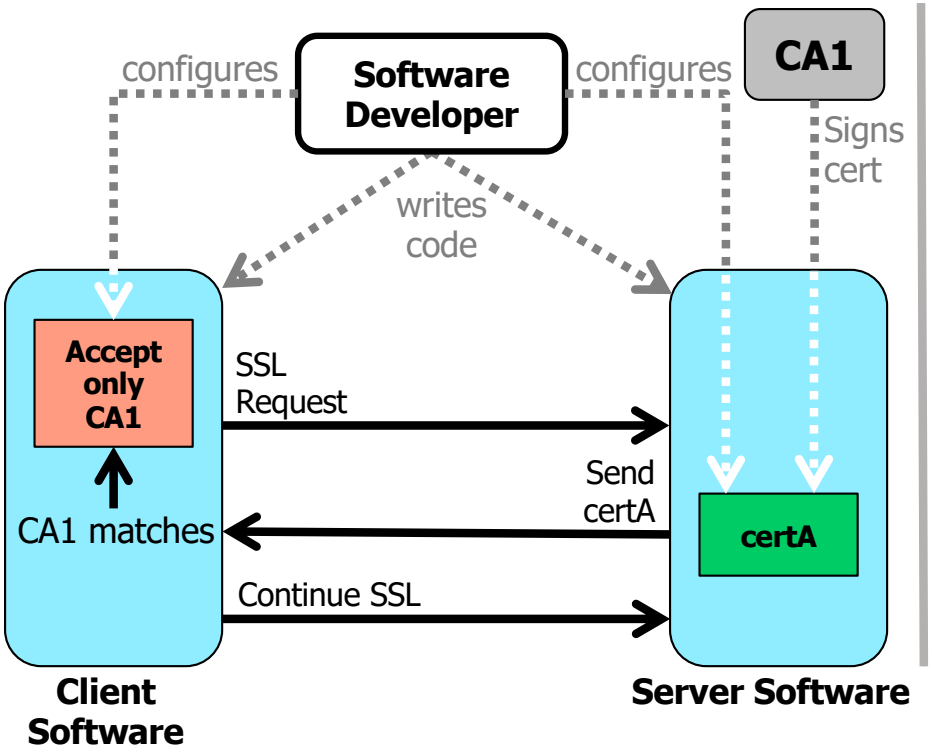
Server Certificate Pinning – With Firewall



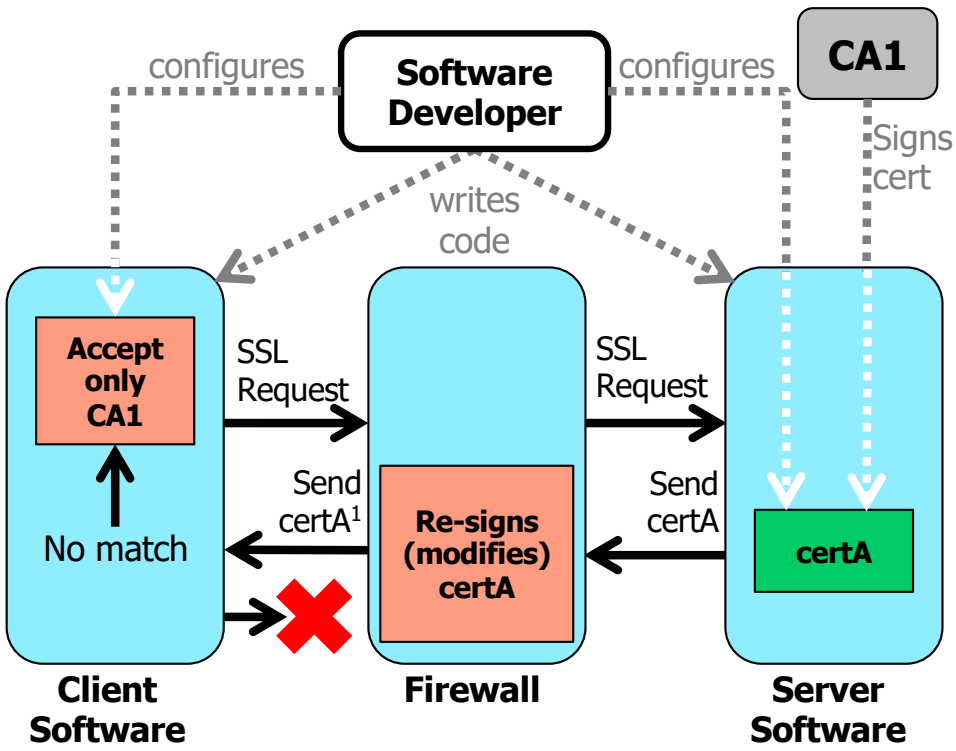
Server certificate pinning prevents MiTM attacks but breaks SSL Forward Proxy decryption.

Static CA Certificate Pinning

CA Certificate Pinning – No Firewall



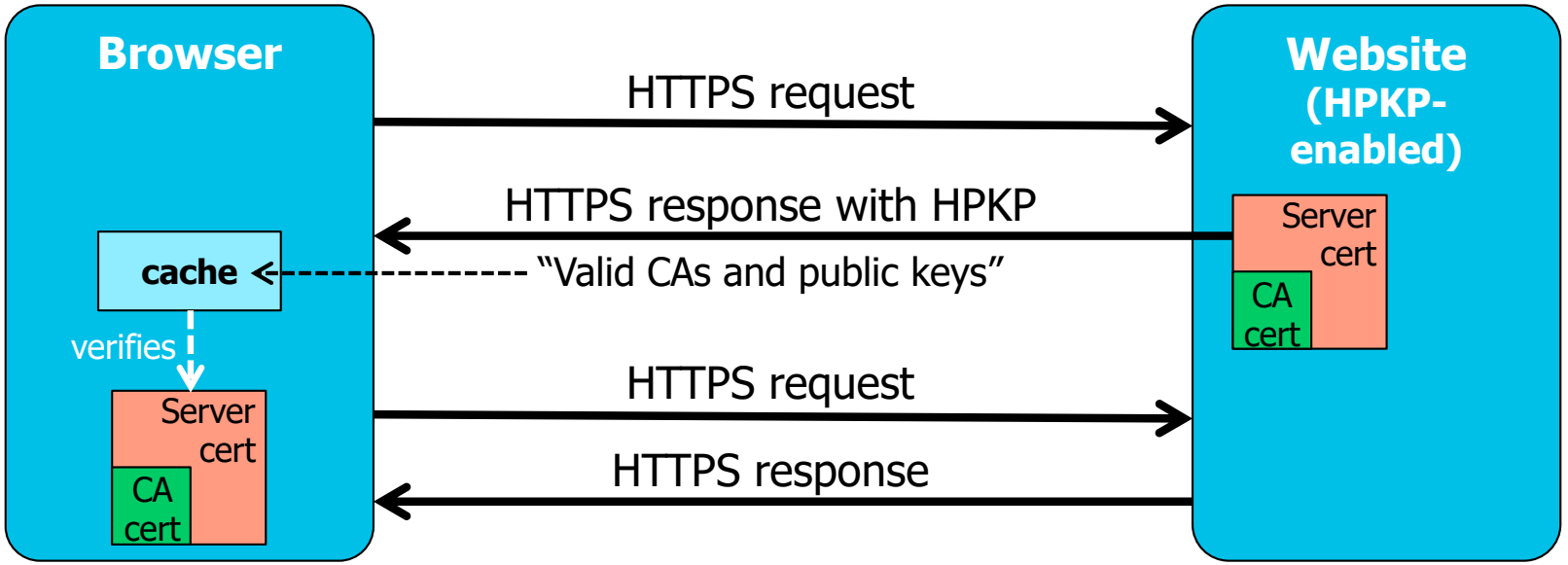
CA Certificate Pinning – With Firewall



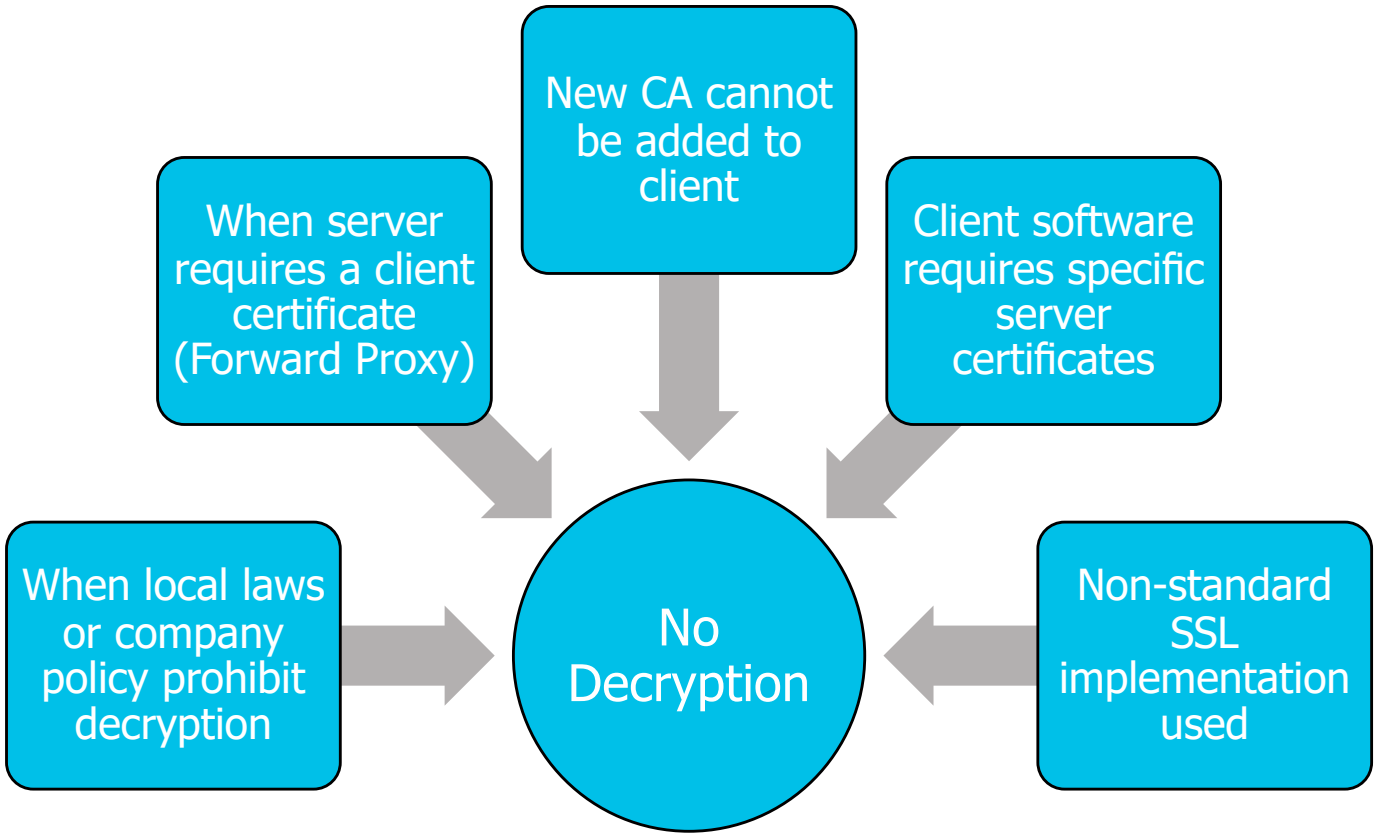
SSL decryption fails unless you can add the firewall's forward trust certificate to the client's list.

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

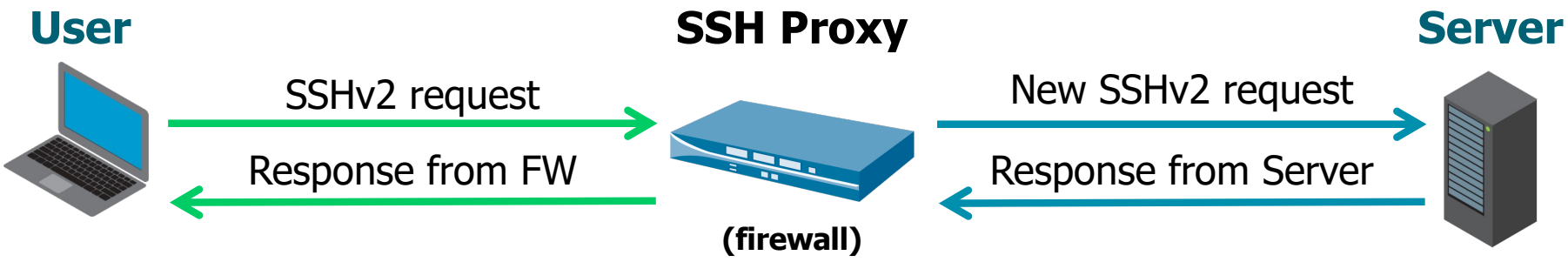
Decryption considerations

SSH decryption

Master key management

Other decryption methods and features

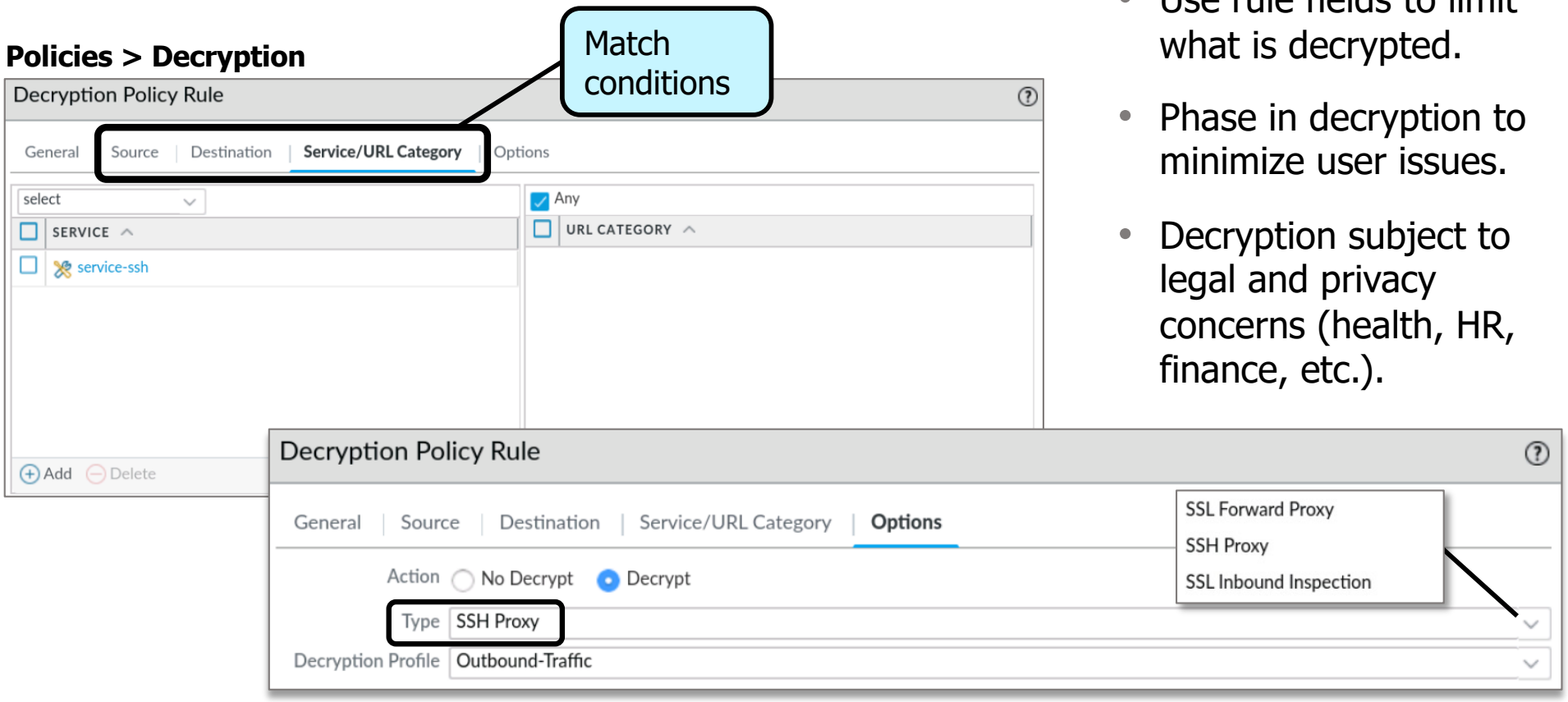
SSH Decryption



- 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

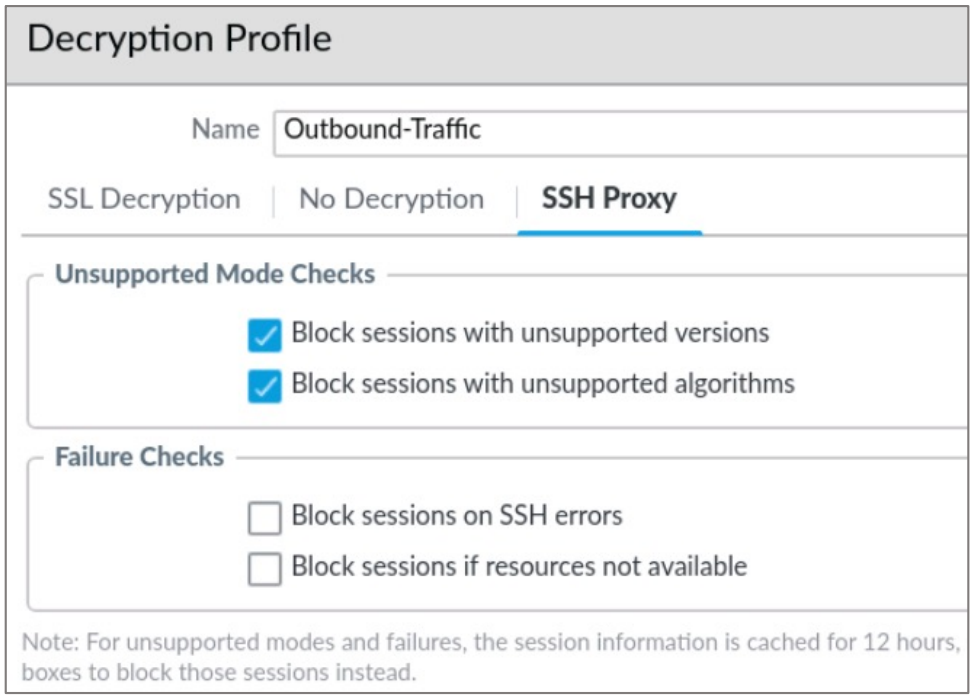
Policies > Decryption



- 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



- 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

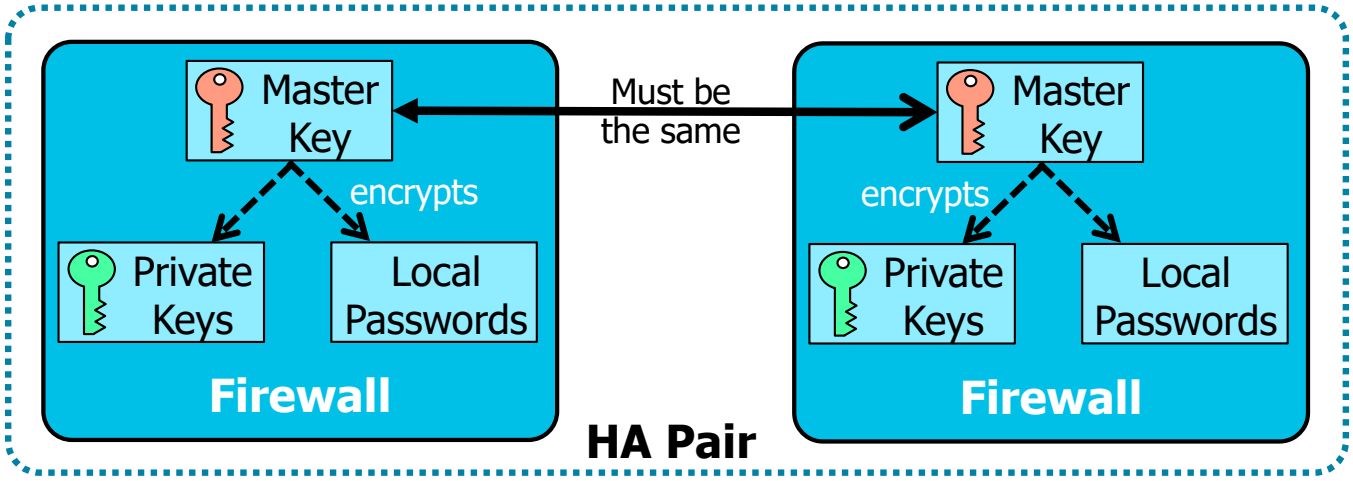
SSH decryption

Master key management

Other decryption methods and features

Firewall Master Key

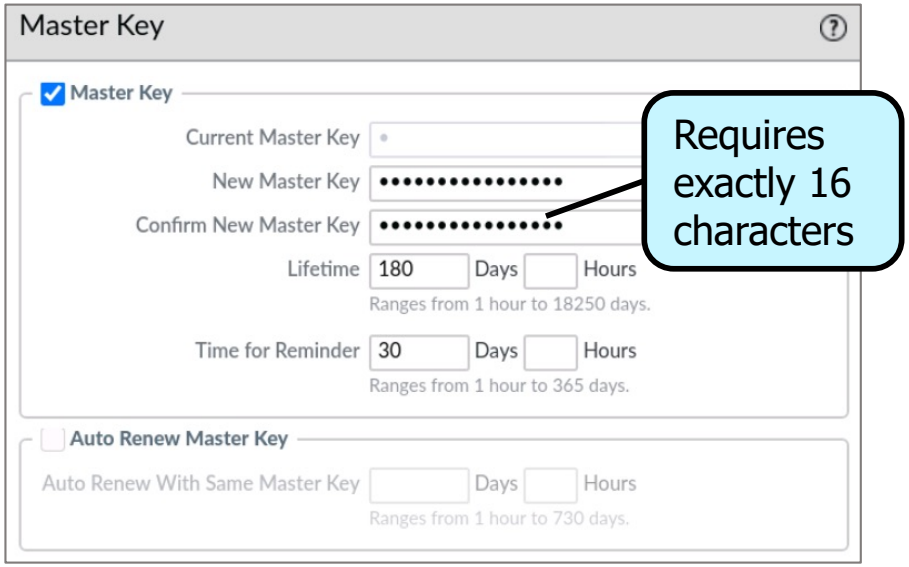
- Firewall master key used to encrypt password and private keys.
- Periodically change master key.
- Must use the same master key in an HA pair.



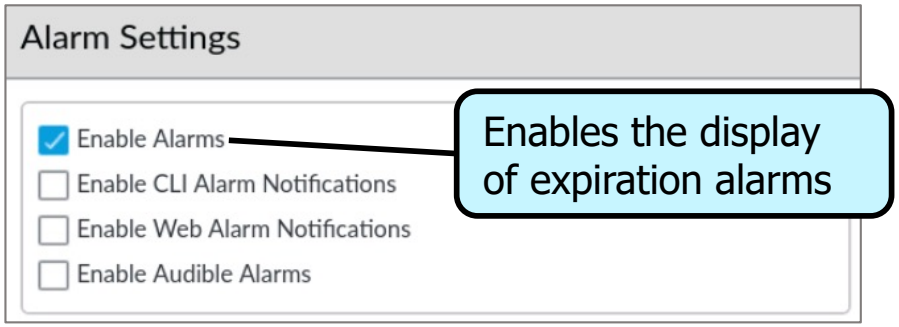
Manage the Master Key

- 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



Device > Log Settings > Alarm Settings



SSL/TLS review

Certificate management

SSL/TLS decryption

Decryption considerations

SSH decryption

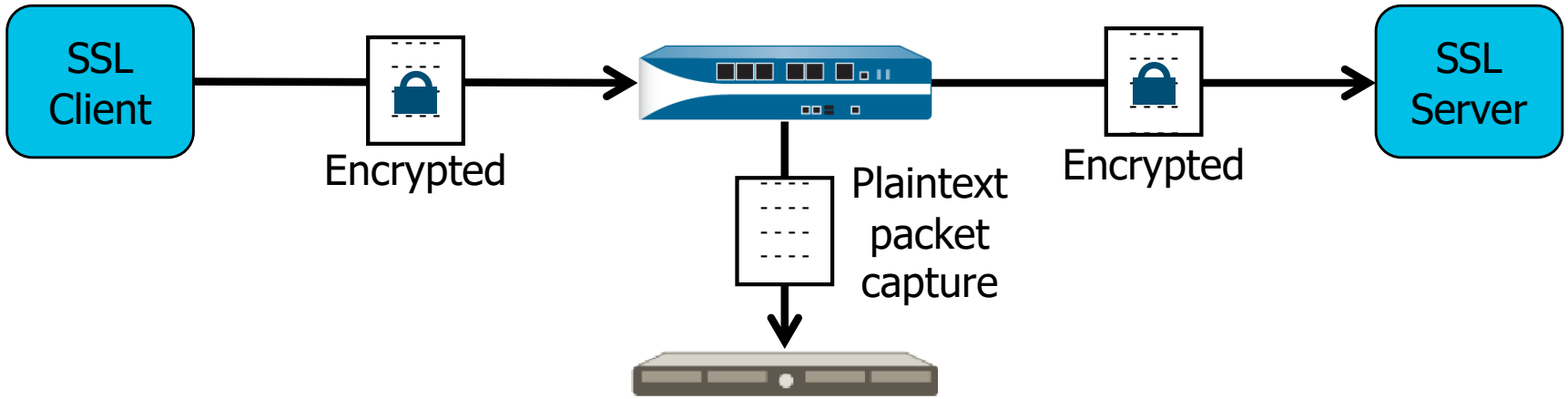
Master key management

Other decryption methods and features

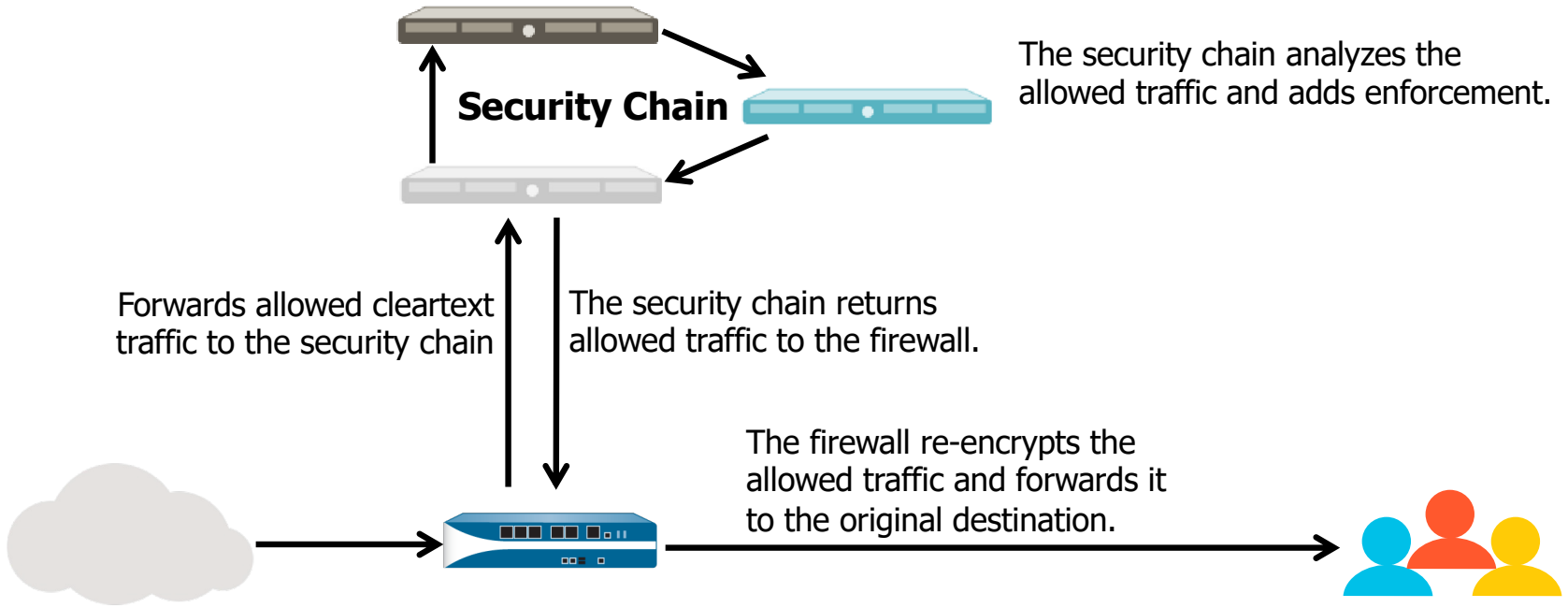
paloalto NETWORKS

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.



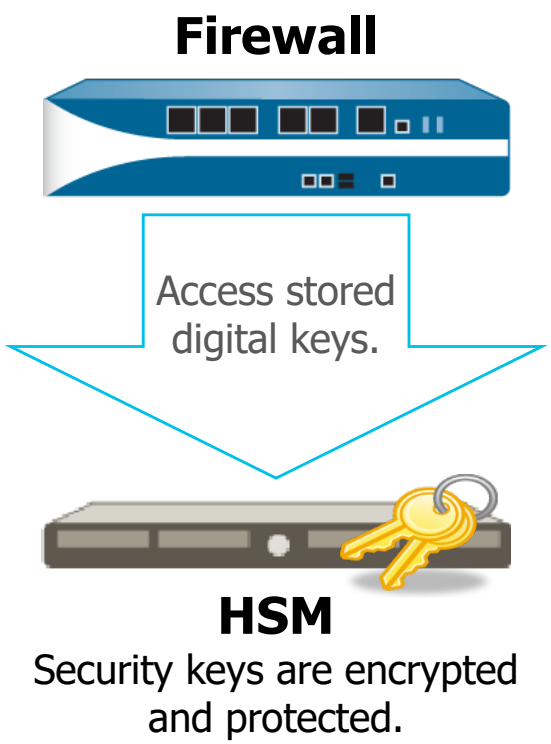
Decryption Broker



- Performs a policy check
- Decrypts SSL traffic
- Inspects and enforces cleartext traffic

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



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.