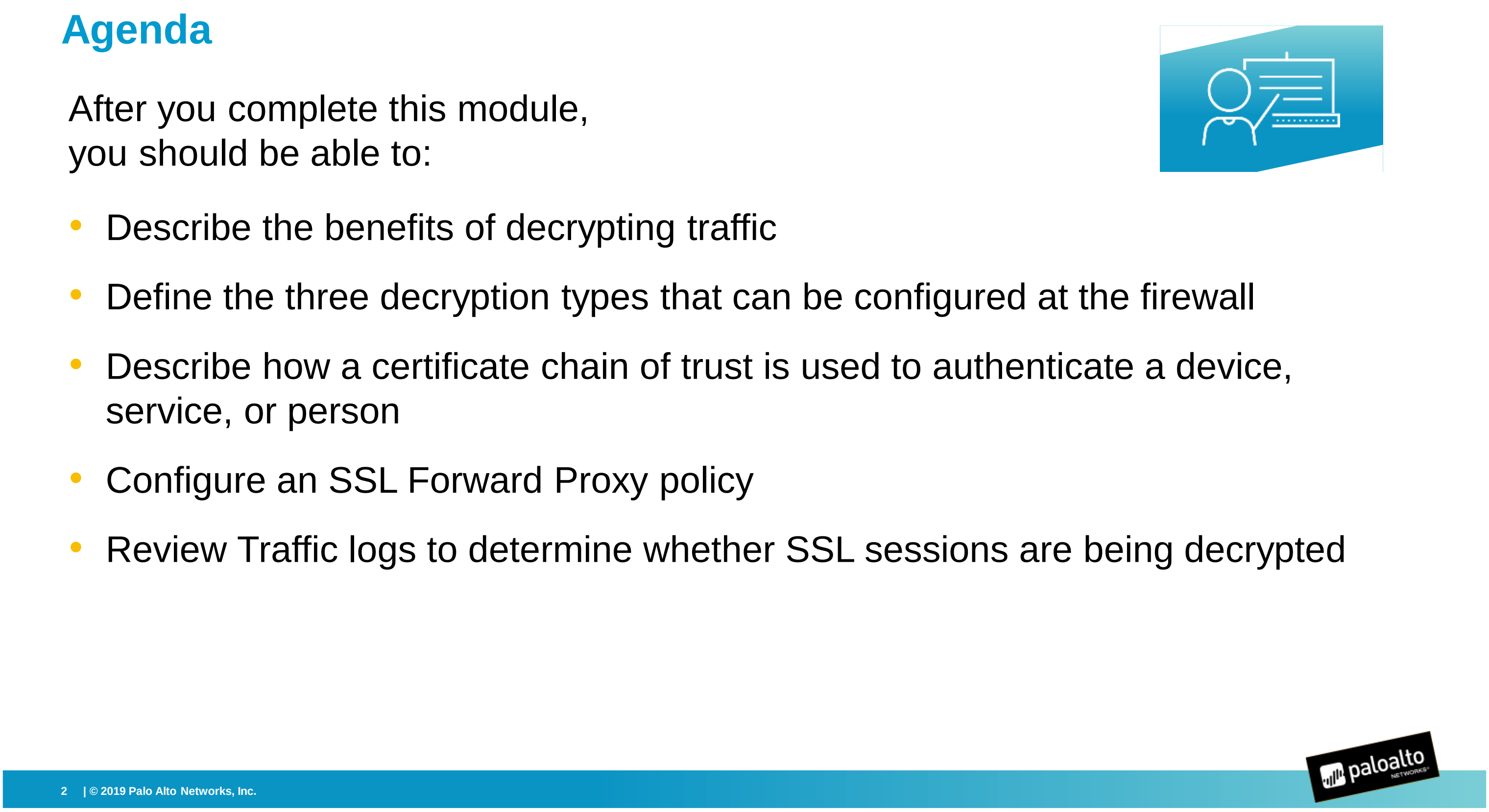
DECRYPTION

EDU-210 Version A
PAN-OS® 9.0

DETECT THREATS IN SSL

- Decryption concepts
- Certificate management
- SSL forward proxy decryption
- SSL inbound inspection
- Other decryption topics



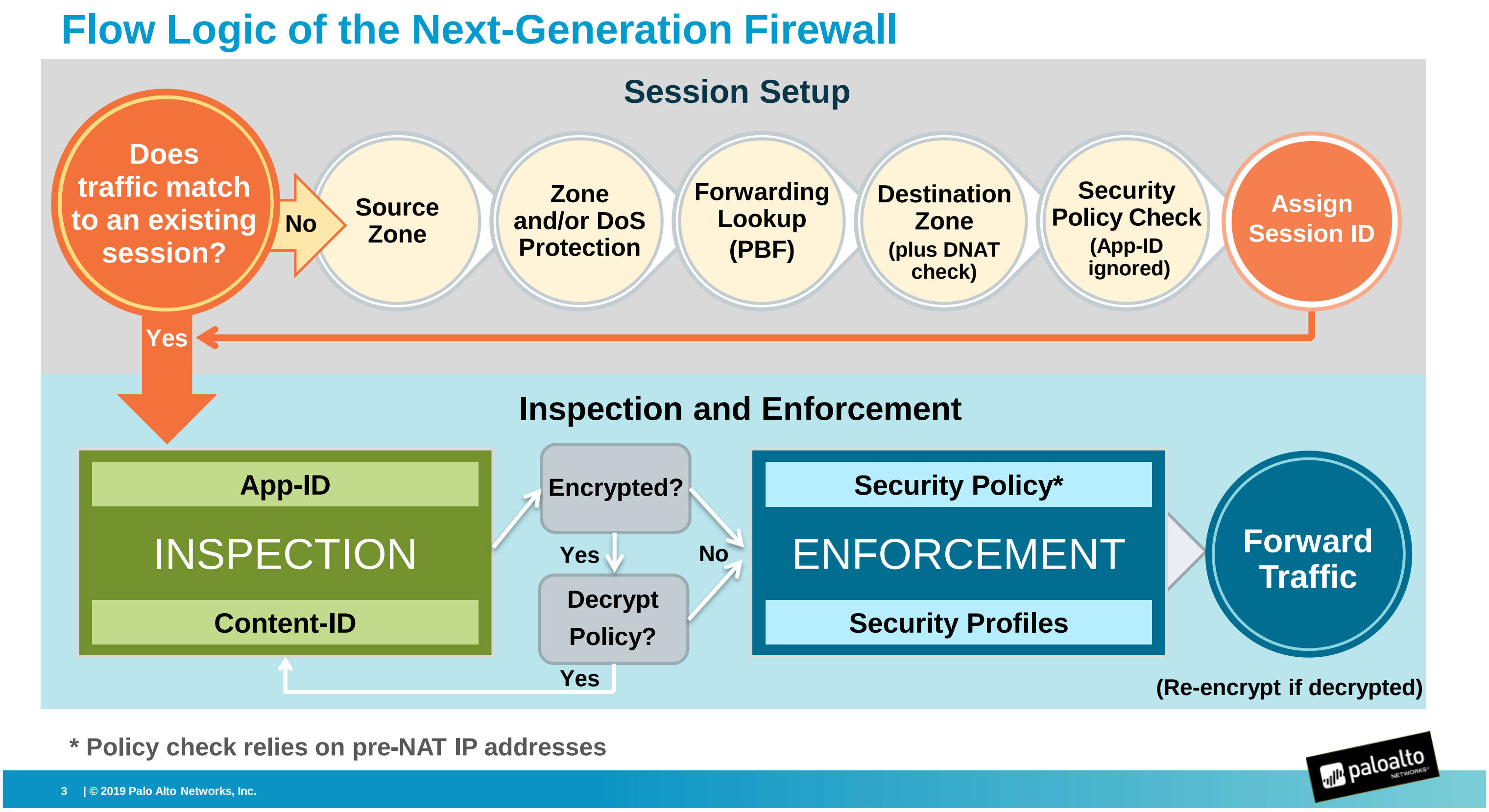
Agenda

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

- Describe the benefits of decrypting traffic
- Define the three decryption types that can be configured at the firewall
- Describe how a certificate chain of trust is used to authenticate a device, service, or person
- Configure an SSL Forward Proxy policy
- Review Traffic logs to determine whether SSL sessions are being decrypted

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

- Describe the benefits of decrypting traffic
- Define the three decryption types that can be configured at the firewall
- Describe how a certificate chain of trust is used to authenticate a device, service, or person
- Configure an SSL Forward Proxy policy
- Review Traffic logs to determine whether SSL sessions are being decrypted



Flow Logic of the Next-Generation Firewall

Session Setup

Does traffic match to an existing session?

No

Source Zone

Zone and/or DoS Protection

Forwarding Lookup (PBF)

Destination Zone (plus DNAT check)

Security Policy Check (App-ID ignored)

Assign Session ID

Yes

Inspection and Enforcement

App-ID

INSPECTION

Content-ID

Encrypted?

Yes

No

Decrypt Policy?

Yes

Security Policy*

ENFORCEMENT

Security Profiles

Forward Traffic

(Re-encrypt if decrypted)

* Policy check relies on pre-NAT IP addresses

3 | © 2019 Palo Alto Networks, Inc.

Encrypted sessions can be used to insert malicious content or to exfiltrate sensitive data. To better protect your organization, the firewall should be configured to decrypt and examine encrypted SSL/TLS and SSH network traffic.

For more information about the packet handling sequence inside of a PAN-OS® device, see the *Packet Flow Sequence in PAN-OS* document available on the Palo Alto Networks Support website at https://live.paloaltonetworks.com/docs/DOC-1628.

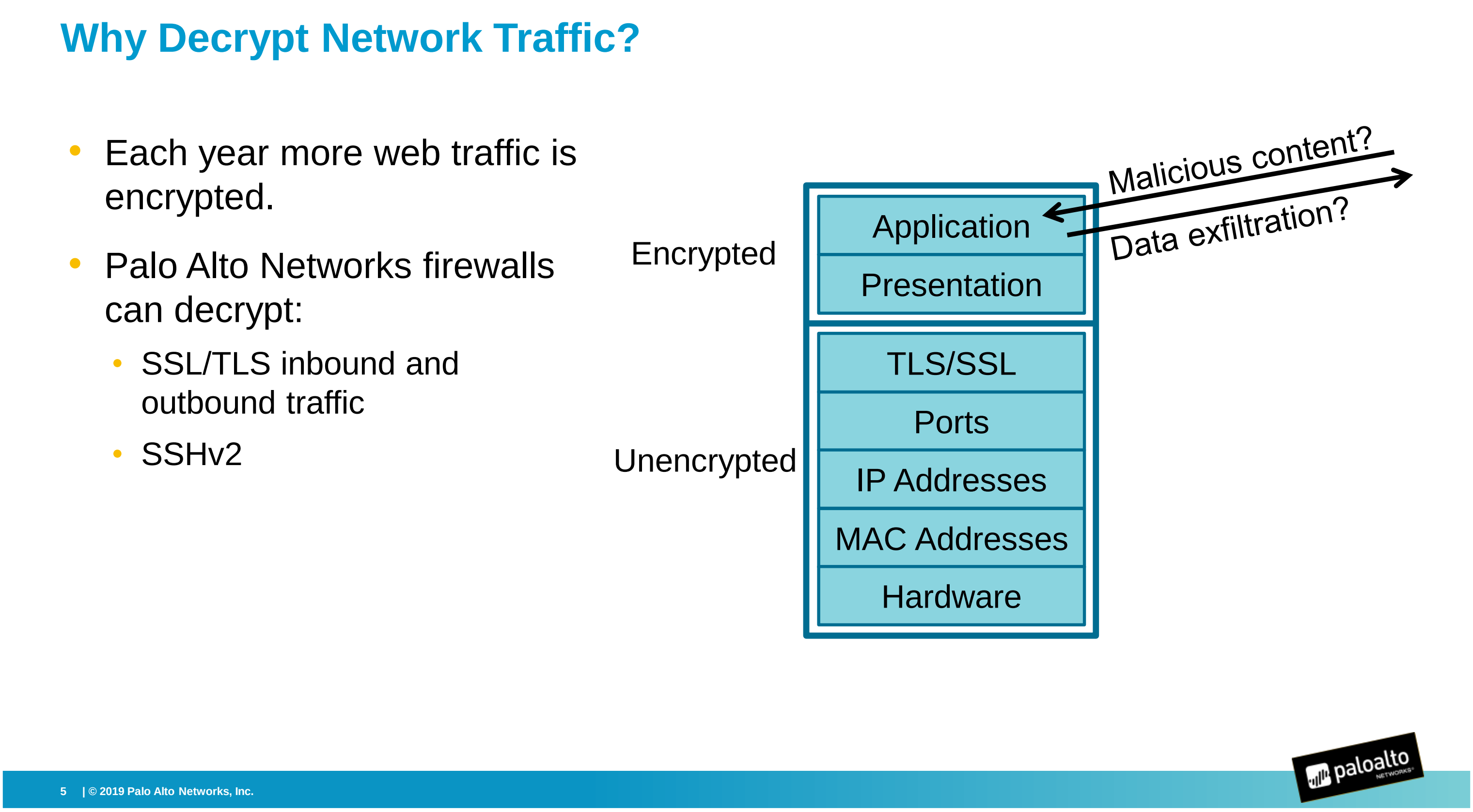
Decryption concepts

Certificate management

SSL forward proxy decryption

SSL inbound inspection

Other decryption topics



Why Decrypt Network Traffic?

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

Encrypted

Application

Presentation

Unencrypted

TLS/SSL

Ports

IP Addresses

MAC Addresses

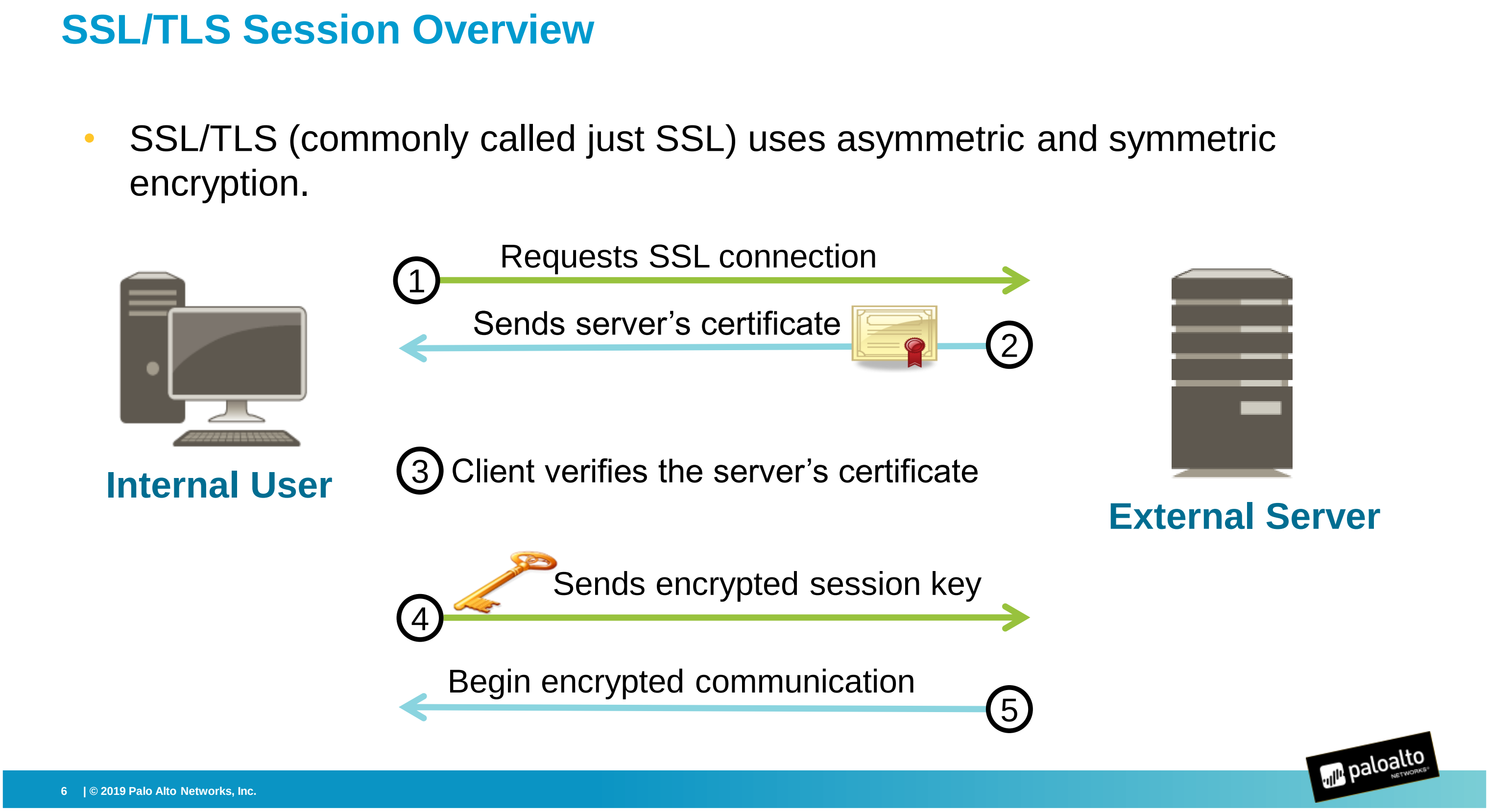
Hardware

Malicious content?

Data exfiltration?

Each year more web traffic is encrypted. Palo Alto Networks firewalls provide the capability to decrypt and inspect network traffic for visibility, control, and granular security. Decryption on a Palo Alto Networks firewall includes the capability to enforce Security policy on decrypted traffic, where otherwise the encrypted traffic might not be blocked and shaped according to your configured security settings. Use decryption on a firewall to prevent malicious content from entering your network or to prevent sensitive content from leaving your network concealed as encrypted traffic.

A Palo Alto Networks firewall can decrypt SSHv2 and SSL/TLS inbound and outbound network traffic.



SSL/TLS Session Overview

- SSL/TLS (commonly called just SSL) uses asymmetric and symmetric encryption.

Internal User

External Server

1 Requests SSL connection

2 Sends server's certificate

3 Client verifies the server's certificate

4 Sends encrypted session key

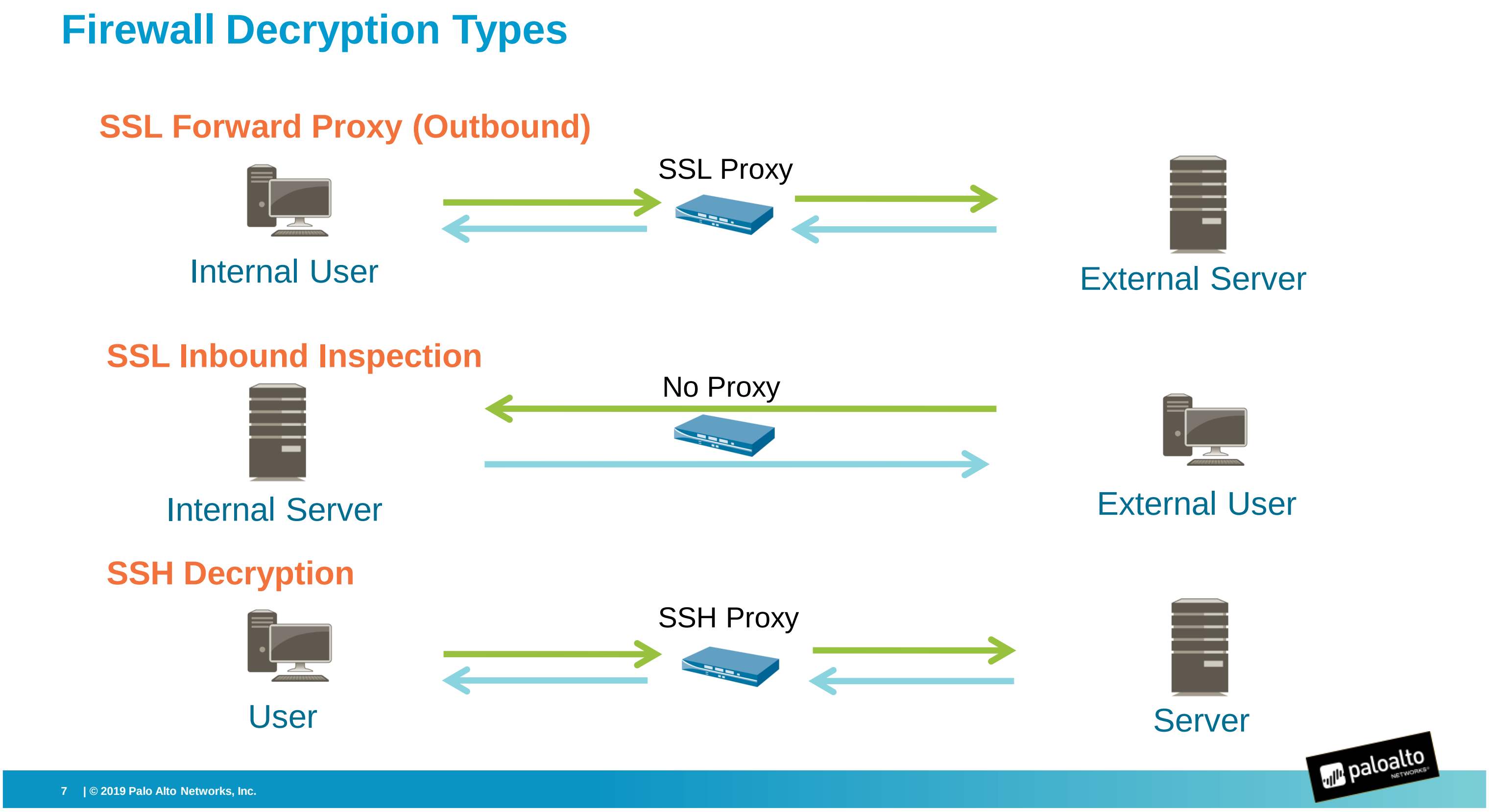
5 Begin encrypted communication

The SSL/TLS protocol encrypts an HTTPS connection between a client and a server where no pre-existing secure channel is present. SSL/TLS commonly is referred to as just SSL.

Initiation of an SSL session follows this basic flow:

1. A client requests an SSL connection.
2. The server responds with its certificate that contains its identity and public key.
3. The client uses the PKI to validate the server's certificate and server's public key.
4. If the certificate is valid, the client uses the server's public key to encrypt a symmetric session key and send it to the server.
5. The server uses its private key to decrypt the session key. Both sides use the session key to encrypt communications.

The communication partners periodically might need to establish a new session and rekey the communication. The process of rekeying new or existing sessions is known as Perfect Forward Secrecy, or PFS, and provides assurances that if a private key is compromised, any recorded former sessions cannot be decrypted. PFS support for SSL Forward Proxy was added in PAN-OS 7.1. PFS support for SSL Inbound Inspection was added in PAN-OS 8.0.



Firewall Decryption Types

SSL Forward Proxy (Outbound)

SSL Proxy

Internal User

External Server

SSL Inbound Inspection

No Proxy

Internal Server

External User

SSH Decryption

SSH Proxy

User

Server

7 | © 2019 Palo Alto Networks, Inc.

You can configure SSL Forward Proxy decryption on the firewall, which decrypts SSL traffic between an internal host and an external web server. In this configuration the firewall acts as an SSL proxy. With SSL Forward Proxy, a connection is formed between an internal user and the firewall, while a separate but related SSL connection is formed between the firewall and the external web server.

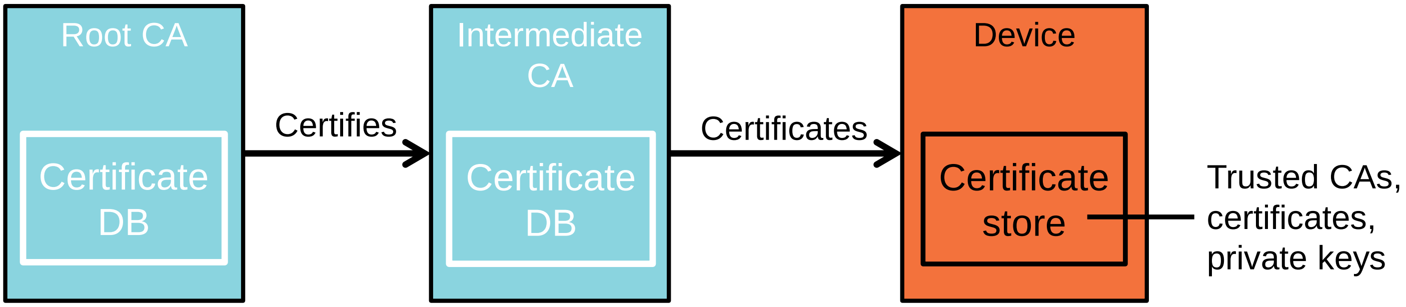
As an example of the usefulness of SSL Forward Proxy decryption, consider a scenario where an internal user will connect via an encrypted connection to Facebook. The company policy is to allow employees to read Facebook but to prevent facebook-chat and facebook-posting. If SSL decryption is enabled for the Facebook application, company policy can be implemented easily with the firewall. If SSL decryption is not enabled, then the firewall cannot identify which application is inside the SSL connection, nor can it recognize that application shifts are occurring within the connection.

You also can configure SSL Inbound Inspection decryption on the firewall, which decrypts SSL traffic coming from external users to internal servers. To configure SSL Inbound Inspection, you must have access to the server’s private key and certificate. In this configuration the firewall does not act as an SSL proxy. An SSL connection is formed directly between the external user and the internal server. The firewall decrypts and inspects only the traffic flowing through it. The firewall can apply Security policy and Security Profiles to the SSL connection and block disallowed traffic.

You can configure SSH Decryption, which can decrypt outbound and inbound SSH traffic. If an SSH tunnel (port forwarding) is discovered, the SSH connection is blocked to ensure that SSH is not being used to tunnel disallowed applications and content. You also can apply a Decryption Profile to your Security policy rules to control normal, non-port-forwarded SSH traffic.

Public Key Infrastructure (PKI)

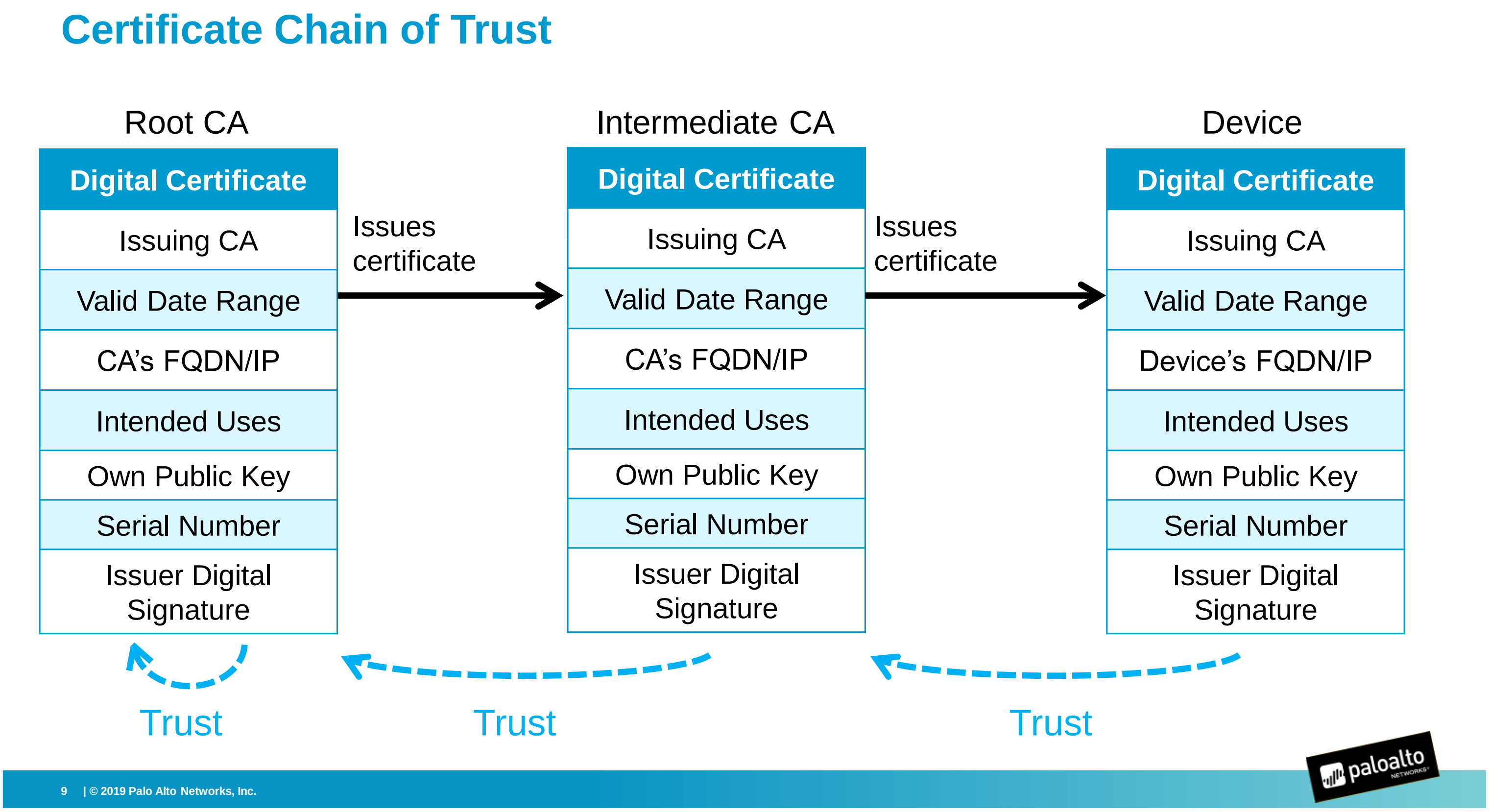
- Solves the problem of secure identification of public keys
- Uses digital certificates to verify public key owners
- Typical PKI components:



The public key infrastructure solves the problem of verifying the identity of a public key owner. PKI is the set of hardware, software, policies, and standards used to create, manage, distribute, and revoke public keys and digital certificates. A PKI digital certificate is a method of packaging and distributing public keys in such a way that proves the identity of their owners. Palo Alto Networks firewalls support X.509-format certificates.

A PKI certificate authority (CA) provides services that authenticate devices, services, and people by issuing the certificates that confirm their identity and public key. CAs are arranged in a hierarchical fashion, similar to a file system. The root CAs form the top level of the hierarchy and intermediate CAs form the second and lower levels. An intermediate CA is certified by a root CA to issue certificates or to certify additional lower-level intermediate CAs. Each CA has a certificate database that stores certificates, revokes certificates, stores certificate requests, and issues certificates.

Devices use a certificate store to store their private keys and the certificates they have been issued. They also maintain a list of trusted CAs. This list of trusted CAs can be updated by a user or by a device software update. If the certificate of the issuing CA is not added to a client's certificate store, the client receives a warning message when browsing to secure sites verified by that CA.



Certificate Chain of Trust

Root CA	Intermediate CA	Device
Digital Certificate	Digital Certificate	Digital Certificate
Issuing CA	Issuing CA	Issuing CA
Valid Date Range	Valid Date Range	Valid Date Range
CA’s FQDN/IP	CA’s FQDN/IP	Device’s FQDN/IP
Intended Uses	Intended Uses	Intended Uses
Own Public Key	Own Public Key	Own Public Key
Serial Number	Serial Number	Serial Number
Issuer Digital Signature	Issuer Digital Signature	Issuer Digital Signature

9 | © 2019 Palo Alto Networks, Inc.

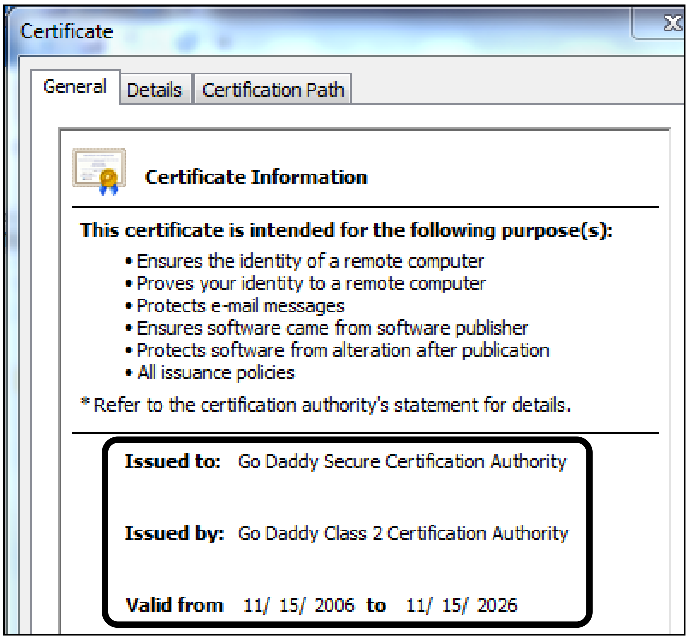
The certificate chain of trust is a hierarchical list of certificates used to authenticate a device, service, or person.

In the example, the chain begins with the device’s certificate. Each certificate in the chain is digitally signed by the entity identified by the next-higher certificate in the chain.

The chain terminates with a root CA certificate. The root CA certificate is always self-signed by the root CA itself. A root certificate is a self-signed certificate because the issuing authority is itself. These root CAs form the basis for all PKI deployments.

The device can verify the owner of a public key if the device’s list of trusted CAs includes a root CA in the chain of trust. For example, a browser can check to determine which authority issued an intermediary certificate, retrieve the intermediary’s certificate from that higher authority, and verify the intermediary certificate. This process continues until a root CA is encountered in the chain. In practice, this process is rarely more than two or three hops.

Certificate Example



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

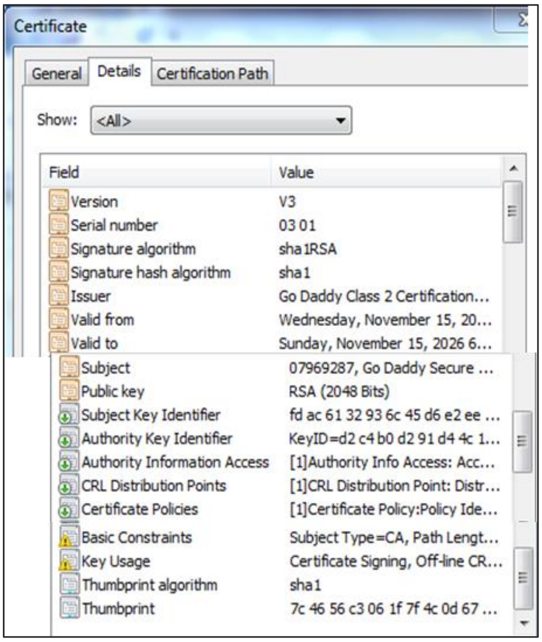
- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Protects e-mail messages
- Ensures software came from software publisher
- Protects software from alteration after publication
- All issuance policies

* Refer to the certification authority's statement for details.

Issued to: Go Daddy Secure Certification Authority

Issued by: Go Daddy Class 2 Certification Authority

Valid from 11/ 15/ 2006 **to** 11/ 15/ 2026



Certificate

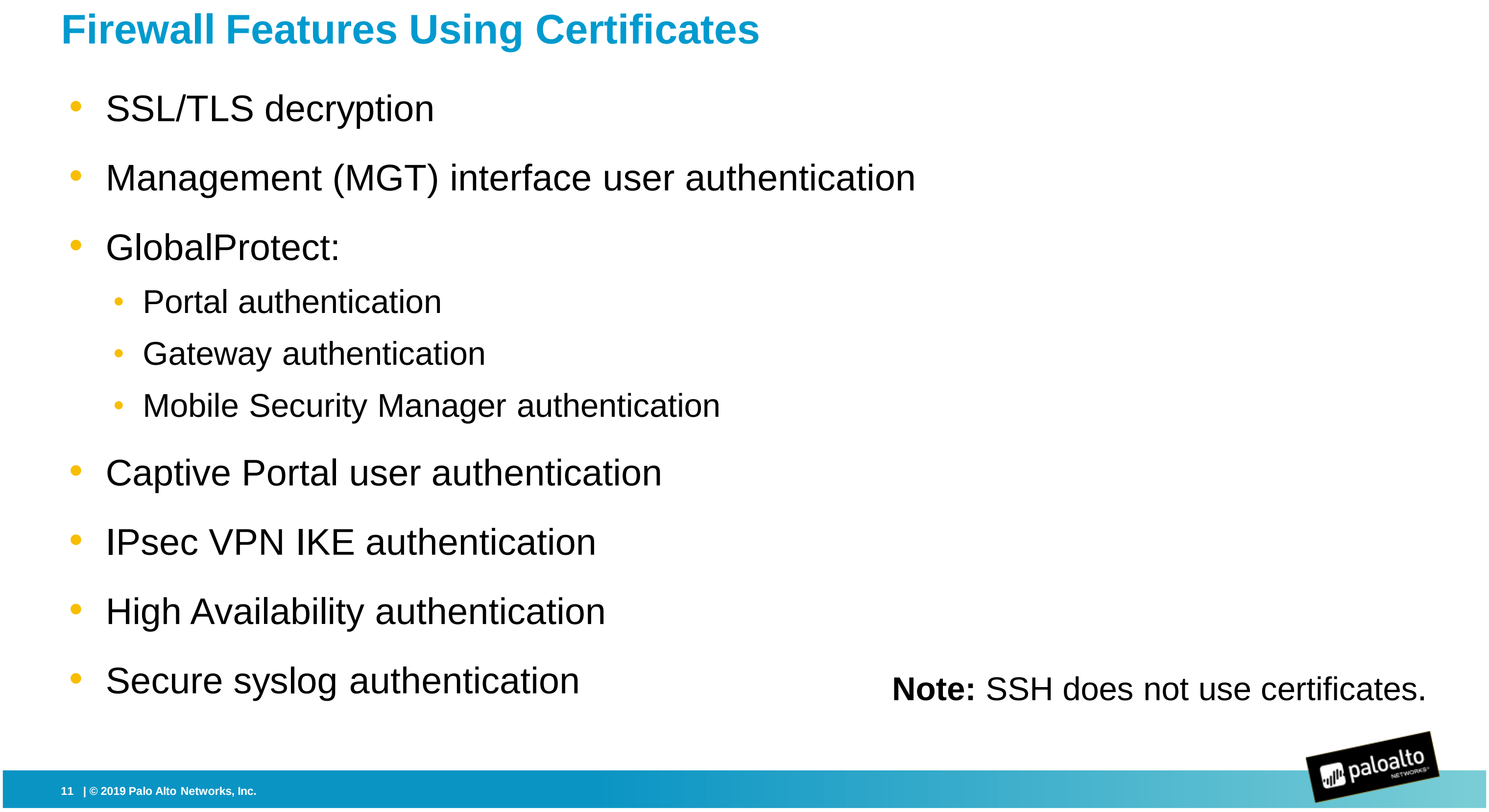
Show: <All>

Field	Value
Version	V3
Serial number	03 01
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	Go Daddy Class 2 Certification...
Valid from	Wednesday, November 15, 20...
Valid to	Sunday, November 15, 2026 6...
Subject	07969287, Go Daddy Secure ...
Public key	RSA (2048 Bits)
Subject Key Identifier	fd ac 61 32 93 6c 45 d6 e2 ee ...
Authority Key Identifier	KeyID=d2 c4 b0 d2 91 d4 4c 1...
Authority Information Access	[1]Authority Info Access: Acc...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Basic Constraints	Subject Type=CA, Path Lengt...
Key Usage	Certificate Signing, Off-line CR...
Thumbprint algorithm	sha1
Thumbprint	7c 46 56 c3 06 1f 7f 4c 0d 67 ...

You can rely on a certificate and the information and public key it contains when the issuing CA is trusted and the signature hash value in a certificate is valid. An issuing CA computes a hash value for critical information in a certificate and includes that hash value in the certificate. The receiving entity can recompute and compare the hash value to ensure that a certificate has not been intercepted and altered by a malicious third party.

To prevent tampering of the hash value and other critical information in the certificate, the issuing CA encrypts the information with its own private key. The receiving entity uses the issuing CA’s public key to decrypt the information to recompute and compare the hash value. Because only the issuing CA knows its own private key, encryption of certificate information using its private key is essentially an act of digitally signing the certificate.

If the certificate of the issuing CA is not added to a client’s certificate store, the client receives a certificate warning message when browsing to secure websites verified by that CA.

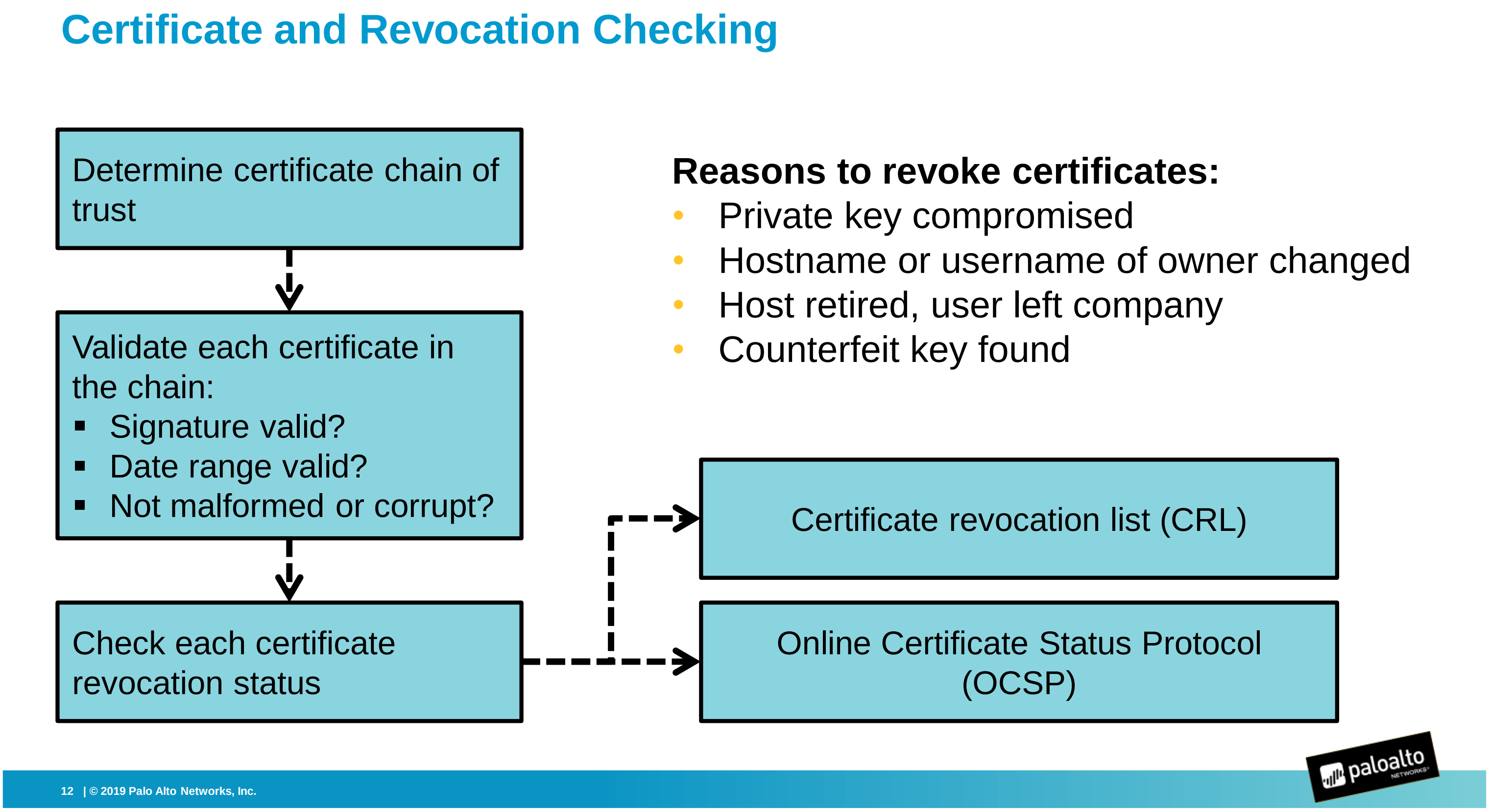


Firewall Features Using Certificates

- SSL/TLS decryption
- Management (MGT) interface user authentication
- GlobalProtect:
  - Portal authentication
  - Gateway authentication
  - Mobile Security Manager authentication
- Captive Portal user authentication
- IPsec VPN IKE authentication
- High Availability authentication
- Secure syslog authentication

Note: SSH does not use certificates.

Palo Alto Networks firewalls use certificates for many purposes. This module describes the use of certificates for SSL/TLS decryption of inbound and outbound network traffic. However, a firewall can use certificates for all of the other authentication functions listed.



Certificate and Revocation Checking

Determine certificate chain of trust

Validate each certificate in the chain:
- Signature valid?
- Date range valid?
- Not malformed or corrupt?

Check each certificate revocation status

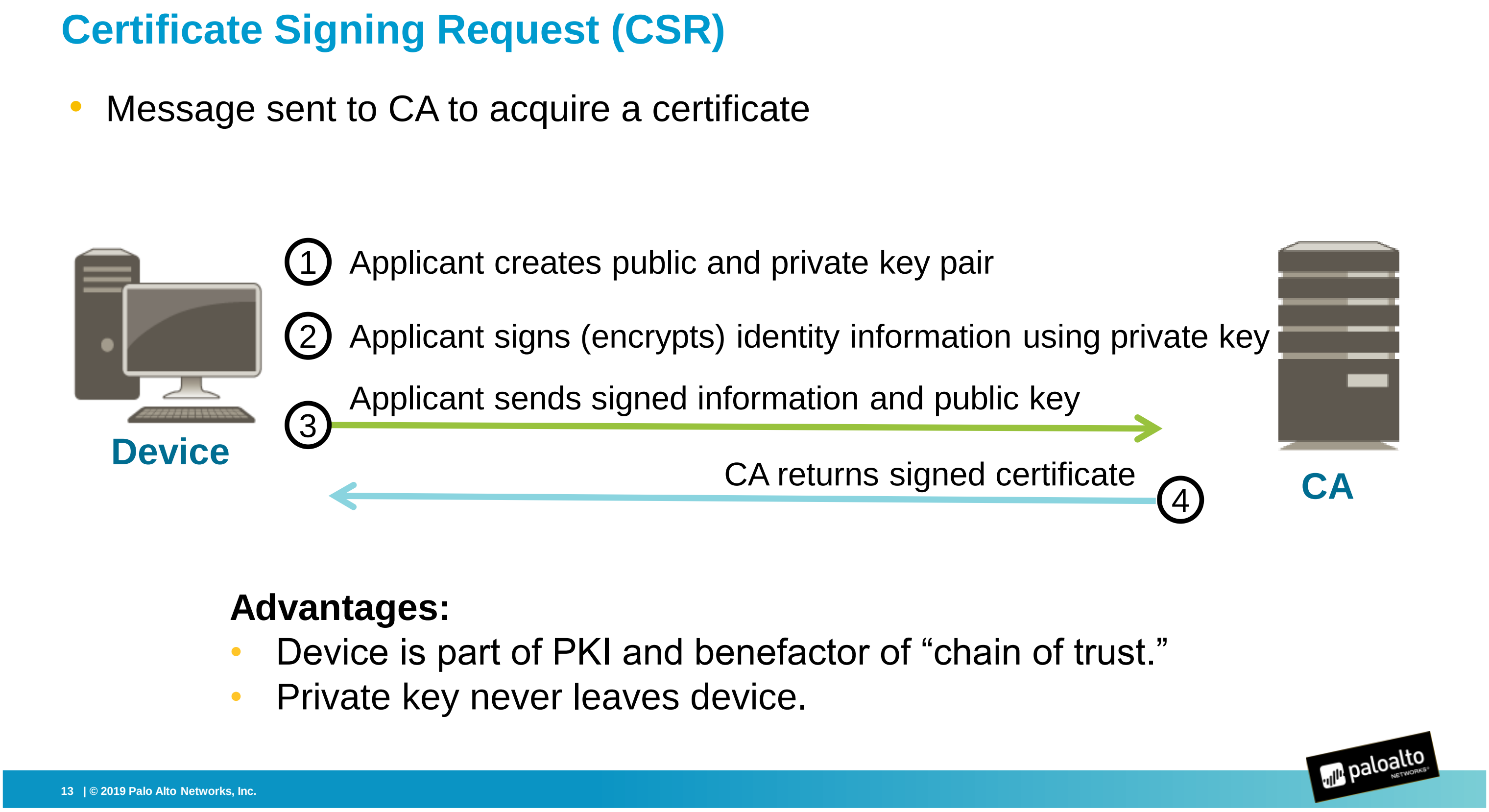
Certificate revocation list (CRL)

Online Certificate Status Protocol (OCSP)

Reasons to revoke certificates:
- Private key compromised
- Hostname or username of owner changed
- Host retired, user left company
- Counterfeit key found

All certificates in the chain of trust must be checked before an SSL/TLS connection can be considered secure. Before it can check the certificates, the SSL client must determine the chain of trust. Then the SSL client must validate each certificate in the chain. If the signatures are valid, then the SSL client must check the revocation status of each certificate in the chain. Two tools are available to check certificate revocation status: CRLs and OCSP. A firewall can use CRL or OCSP to verify certificate revocation status for Captive Portal, GlobalProtect components, IPsec VPNs, MGT port access, and SSL decryption.

A certificate might need to be invalidated before its expiration date because the certificate owner’s private key might have been compromised, the hostname or username of the certificate owner might change, a host could be retired or a user can leave the company, or a counterfeit key might need to be invalidated. The list of revoked certificates is stored on the CAs in their certificate database.



Certificate Signing Request (CSR)

- Message sent to CA to acquire a certificate

1 Applicant creates public and private key pair

2 Applicant signs (encrypts) identity information using private key

3 Applicant sends signed information and public key

4 CA returns signed certificate

Advantages:

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

13 | © 2019 Palo Alto Networks, Inc.

Some devices, including a Palo Alto Networks firewall, can submit a CSR to a CA. To submit a CSR, the device generates a public and private key pair, and identity information, and then submits the public key and identity information to a CA using a CSR file. The CA uses the information in the CSR file to create a certificate signed with the CA’s signature. The signed certificate is sent back to the device.

The advantages of using CSRs is that the device becomes part of the existing PKI infrastructure and its certificate chain of trust. Another advantage is that the device’s private key never leaves the device. The primary disadvantages are that the device must be capable of generating a CSR and that there is some administrative overhead compared to a device using a self-signed certificate.

Decryption concepts

Certificate management

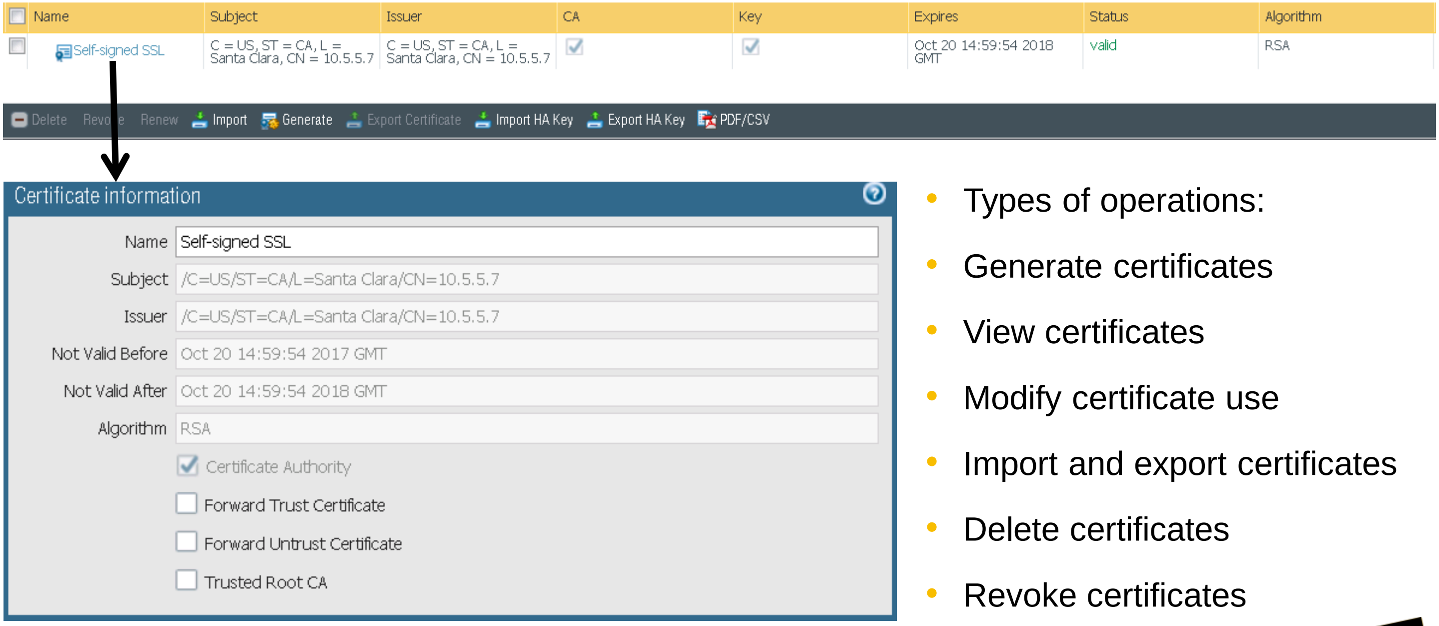
SSL forward proxy decryption

SSL inbound inspection

Other decryption topics

Certificate Management in the Web Interface

Device > Certificate Management > Certificates



□	Name	Subject	Issuer	CA	Key	Expires	Status	Algorithm
□	Self-signed SSL	C = US, ST = CA, L = Santa Clara, CN = 10.5.5.7	C = US, ST = CA, L = Santa Clara, CN = 10.5.5.7	☑	☑	Oct 20 14:59:54 2018 GMT	valid	RSA

Certificate information

Name	Self-signed SSL
Subject	/C=US/ST=CA/L=Santa Clara/CN=10.5.5.7
Issuer	/C=US/ST=CA/L=Santa Clara/CN=10.5.5.7
Not Valid Before	Oct 20 14:59:54 2017 GMT
Not Valid After	Oct 20 14:59:54 2018 GMT
Algorithm	RSA

☑ Certificate Authority

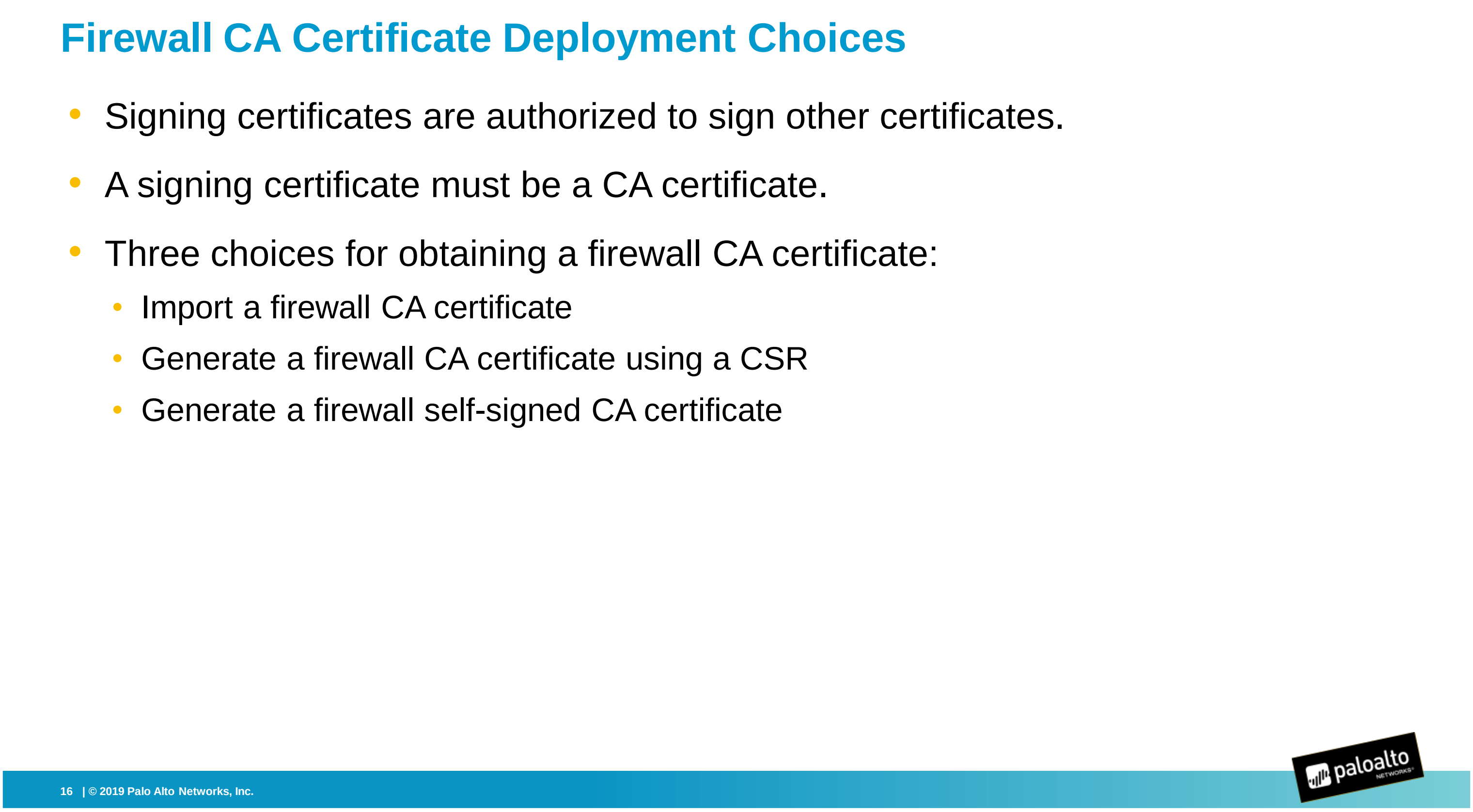
□ Forward Trust Certificate

□ Forward Untrust Certificate

□ Trusted Root CA

- Types of operations:
- Generate certificates
- View certificates
- Modify certificate use
- Import and export certificates
- Delete certificates
- Revoke certificates

The web interface includes certificate management for the firewall at **Device** > **Certificate Management** > **Certificates**. You now can use the web interface to generate and display certificates, or to generate CSRs. You also can import certificates from a third-party or internal CA and export certificates to other devices. You also can modify certificates to meet specific use requirements on the firewall. Certificates issued by the firewall also can be revoked using this interface.



Firewall CA Certificate Deployment Choices

- Signing certificates are authorized to sign other certificates.
- A signing certificate must be a CA certificate.
- Three choices for obtaining a firewall CA certificate:
  - Import a firewall CA certificate
  - Generate a firewall CA certificate using a CSR
  - Generate a firewall self-signed CA certificate

16 | © 2019 Palo Alto Networks, Inc.

Each certificate is authorized for different uses. For example, a signing certificate is authorized to sign other certificates. A signing certificate must be a CA certificate. The firewall requires a signing certificate to support features such as SSL Forward Proxy or GlobalProtect.

You can obtain the initial firewall certificate from a third-party CA. The advantage of this choice is that the third-party CA certificate is signed by a root CA, and all the end clients likely already will trust the root CA. This root CA trust means that the end clients also will trust the third-party CA and the certificate that it issued to the firewall. The primary disadvantage of this choice is that most third-party CAs do not issue signing certificates, and signing certificates are required for SSL operation.

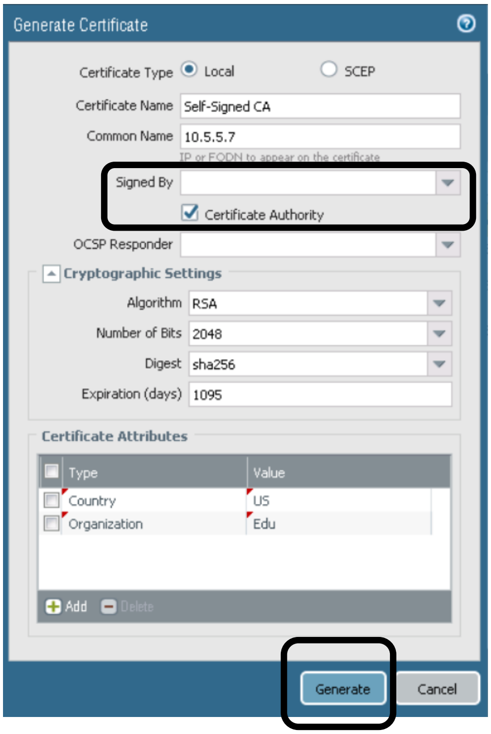
If you already have deployed an internal CA, you can have it issue a signing certificate to the firewall. The advantage of this choice is that the end clients in the enterprise likely already have had the internal CA certificate added to their certificate stores. Because they trust the internal CA, they also will trust the certificate that it issued to the firewall.

Each Palo Alto Networks firewall can generate free, self-signed CA signing certificates. If you generate a self-signed CA certificate, then the firewall can generate any other necessary certificates. The primary disadvantage is that a self-signed CA certificate will not be trusted by any of the end clients until the CA certificate has been installed in their certificate stores. Automated methods exist to distribute a CA certificate to multiple clients; for example, in a Microsoft environment, CA certificates can be distributed to clients using Group Policy. A security warning window appears in a client’s browser window when the web browser cannot establish a certificate chain of trust.

Generate Self-Signed CA Certificate

Method 1:

- Create a self-signed firewall CA certificate:
  - Use **Device > Certificate Management > Certificates > Generate**
- Complete the form and click Generate
- Creates a self-signed CA certificate
- Creates public and private keys



Generate Certificate

Certificate Type ● Local ○ SCEP

Certificate Name Self-Signed CA

Common Name 10.5.5.7

IP or FQDN to appear on the certificate

Signed By

☑ Certificate Authority

OCSP Responder

Cryptographic Settings

Algorithm RSA

Number of Bits 2048

Digest sha256

Expiration (days) 1095

Certificate Attributes

Type	Value
Country	US
Organization	Edu

To create a self-signed CA certificate in the web interface, be sure to leave the **Signed By** field blank and to select the **Certificate Authority** check box. The blank **Signed By** field indicates that this is a self-signed certificate. Selection of the **Certificate Authority** check box enables this certificate to be a signing certificate that can be used to sign other certificates.

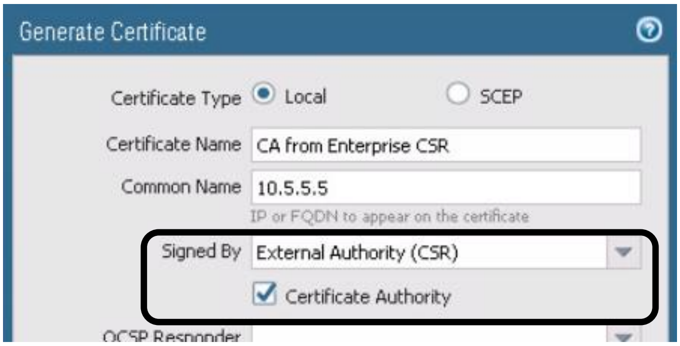
The **Common Name** can be the FQDN or IP address of the firewall, or a label that uniquely identifies the purpose of the certificate. Note that you also can configure an **OCSP Responder** for each certificate. You also can change the cryptographic settings used to generate the certificate and add a variety of **Certificate Attributes** that are used to further identify the owner of the certificate.

After you click **Generate**, the new certificate appears in the list of certificates in the certificate management interface.

Generate CA Certificate Using CSR

Method 2:

- Generate a firewall CA certificate to be signed by an internal CA:
  - Use **Device > Certificate Management > Certificates > Generate**
  - Complete the form and click Generate
- Export public and private keys to .csr file
- Send .csr to internal CA for signing
- CA returns .pem file
  - Use Import to import signed CA certificate .pem file



Generate Certificate

Certificate Type ● Local ○ SCEP

Certificate Name: CA from Enterprise CSR

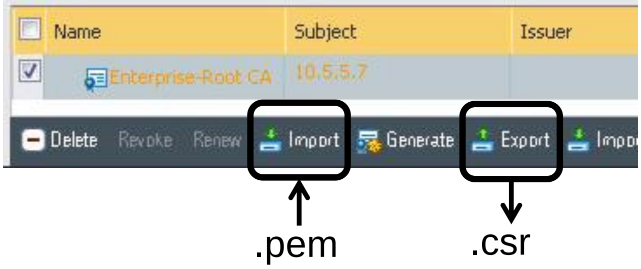
Common Name: 10.5.5.5

IP or FQDN to appear on the certificate

Signed By: External Authority (CSR)

☑ Certificate Authority

OCSP Responder



□	Name	Subject	Issuer
☑	Enterprise-Root CA	10.5.5.7	

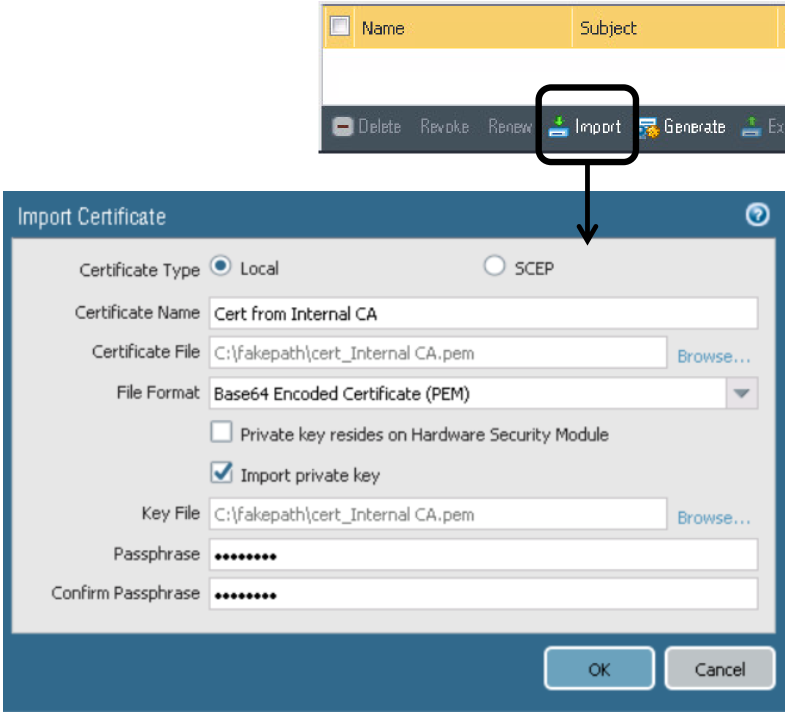
If you have an internal CA, then you can use it to help create the firewall's CA certificate. To create a public and private key and a CSR using the web interface, ensure that you select **External Authority (CSR)** for the **Signed By** field. If the certificate will be a signing certificate capable of signing other certificates, then select the **Certificate Authority** check box. The **Common Name** must be the FQDN or IP address of the firewall. You also can configure an **OCSP Responder** for each certificate, change the cryptographic settings used to generate the certificate, and add a variety of **Certificate Attributes** that are used to further identify the owner of the certificate, although the fields to change these settings are not shown in the screenshot. After you have the form completed, click the **Generate** button. A new, but unsigned, certificate appears in the certificate management window.

Select the check box of the new certificate in the certificate management interface and click **Export** to generate a .csr file. Send this .csr file to your internal CA. The internal CA will sign the certificate and then create a .pem file. Use the web interface to **Import** the .pem file into the firewall. With a firewall CA certificate in place, you can use the web interface to create any other required certificates, and they can be signed by the firewall's CA certificate.

Import CA Certificate

Method 3:

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



Import Certificate

Certificate Type ● Local ○ SCEP

Certificate Name: Cert from Internal CA

Certificate File: C:\fakepath\cert_Internal CA.pem Browse...

File Format: Base64 Encoded Certificate (PEM)

□ Private key resides on Hardware Security Module

☑ Import private key

Key File: C:\fakepath\cert_Internal CA.pem Browse...

Passphrase: ••••••••

Confirm Passphrase: ••••••••

OK Cancel

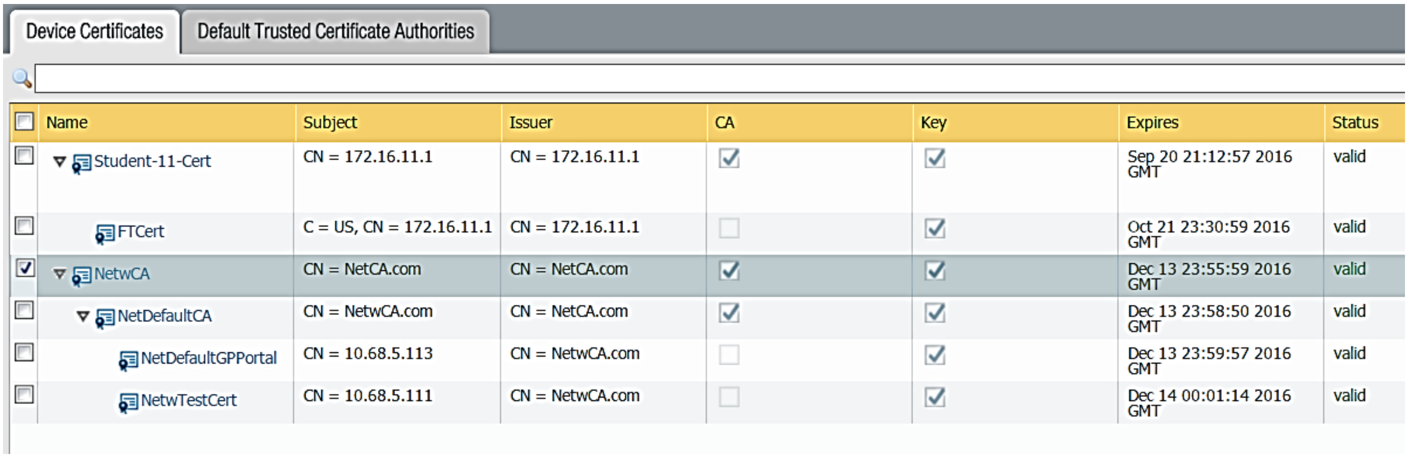
A firewall CA certificate and public and private key pair can be created on an internal CA and imported into the firewall. Ensure that you have a secure network because the firewall’s private key will be transferred over the network.

After the file containing the certificate and keys has been created by the internal CA, use the form shown here to import the files. A PKCS12 file contains both the certificate and private key in the same file. A PEM file containing the certificate will not contain the private key. The private key would have to be transferred in a separate file.

With a firewall CA certificate in place, you can use the web interface to create any other required certificates, and they can be signed by the firewall’s CA certificate.

Certificate Hierarchy

Device > Certificate Management > Certificates



☐	Name	Subject	Issuer	CA	Key	Expires	Status
☐	▽ Student-11-Cert	CN = 172.16.11.1	CN = 172.16.11.1	☑	☑	Sep 20 21:12:57 2016 GMT	valid
☐	FTCert	C = US, CN = 172.16.11.1	CN = 172.16.11.1	☐	☑	Oct 21 23:30:59 2016 GMT	valid
☑	▽ NetwCA	CN = NetCA.com	CN = NetCA.com	☑	☑	Dec 13 23:55:59 2016 GMT	valid
☐	▽ NetDefaultCA	CN = NetwCA.com	CN = NetCA.com	☑	☑	Dec 13 23:58:50 2016 GMT	valid
☐	NetDefaultGPPortal	CN = 10.68.5.113	CN = NetwCA.com	☐	☑	Dec 13 23:59:57 2016 GMT	valid
☐	NetwTestCert	CN = 10.68.5.111	CN = NetwCA.com	☐	☑	Dec 14 00:01:14 2016 GMT	valid

To help you manage certificates, PAN-OS software organizes the certificate listings as a hierarchical list. This format simplifies the process of determining which certificates are related by grouping certificates under their CA certificates on the system.

In the example, an administrator is preparing to deploy a GlobalProtect environment. To enable certificates to correctly authenticate GlobalProtect components to each other, the same CA must issue all the certificates. The web interface display makes this check simple.

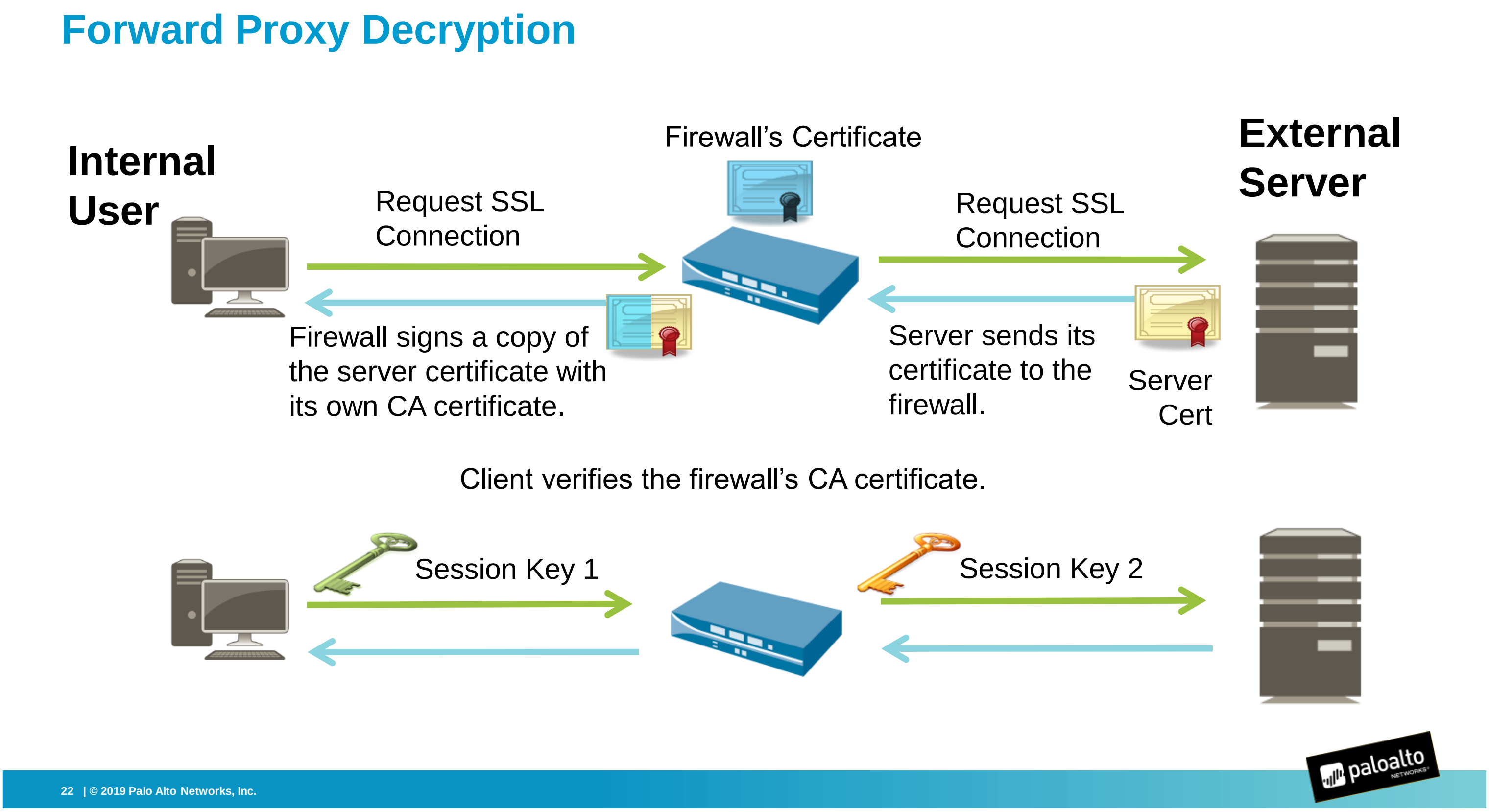
Decryption concepts

Certificate management

SSL forward proxy decryption

SSL inbound inspection

Other decryption topics



Forward Proxy Decryption

Internal User

External Server

Firewall's Certificate

Request SSL Connection

Request SSL Connection

Firewall signs a copy of the server certificate with its own CA certificate.

Server sends its certificate to the firewall.

Server Cert

Client verifies the firewall's CA certificate.

Session Key 1

Session Key 2

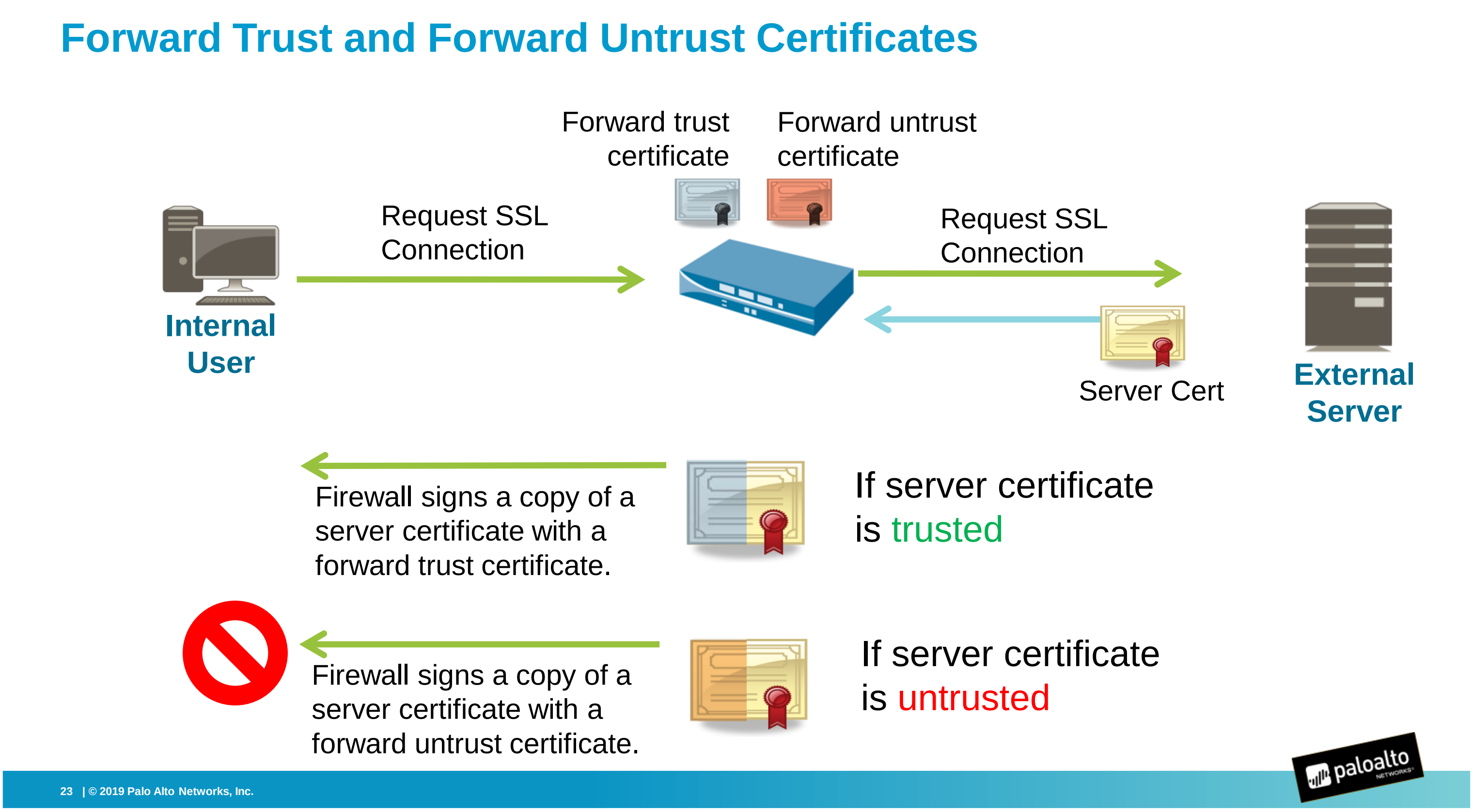
22 | © 2019 Palo Alto Networks, Inc.

Use an SSL Forward Proxy Decryption policy to decrypt and inspect SSL/TLS traffic from internal users to external web servers. SSL Forward Proxy decryption prevents malware concealed as SSL encrypted traffic from being introduced to your organization's network. It also helps to prevent the exfiltration of sensitive data.

A firewall that is configured to decrypt SSL traffic going to an external web server functions as a forward proxy. In this scenario, the firewall intercepts the SSL client's request for the server's certificate. The firewall then contacts the server and requests the server's certificate. The server responds to the firewall with its certificate, which the firewall verifies. The resulting secure SSL connection is between the firewall and the server. Then the firewall signs the server's certificate with the firewall's certificate and sends it to the SSL client. The SSL client verifies the firewall's certificate that was used to sign the server's certificate, and the result is another secure connection between the firewall and the SSL client. The SSL client uses the proxy connection to the server through the firewall.

By default the firewall dynamically chooses the key size to use to establish an SSL Forward Proxy session for a client, based on the key size used by the destination server. You can configure a static key size for SSL Forward Proxy sessions between the firewall and clients regardless of the key size used by the destination server.

Be aware of the following points when configuring and using SSL Forward Proxy. The validity date on the firewall certificate is taken from the validity date on the destination server certificate. The firewall acts as a proxy for the SSL connection, not the underlying traffic. Packet capture functionality executes before decryption, which means that a packet capture, or pcap, file will contain encrypted data.



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.

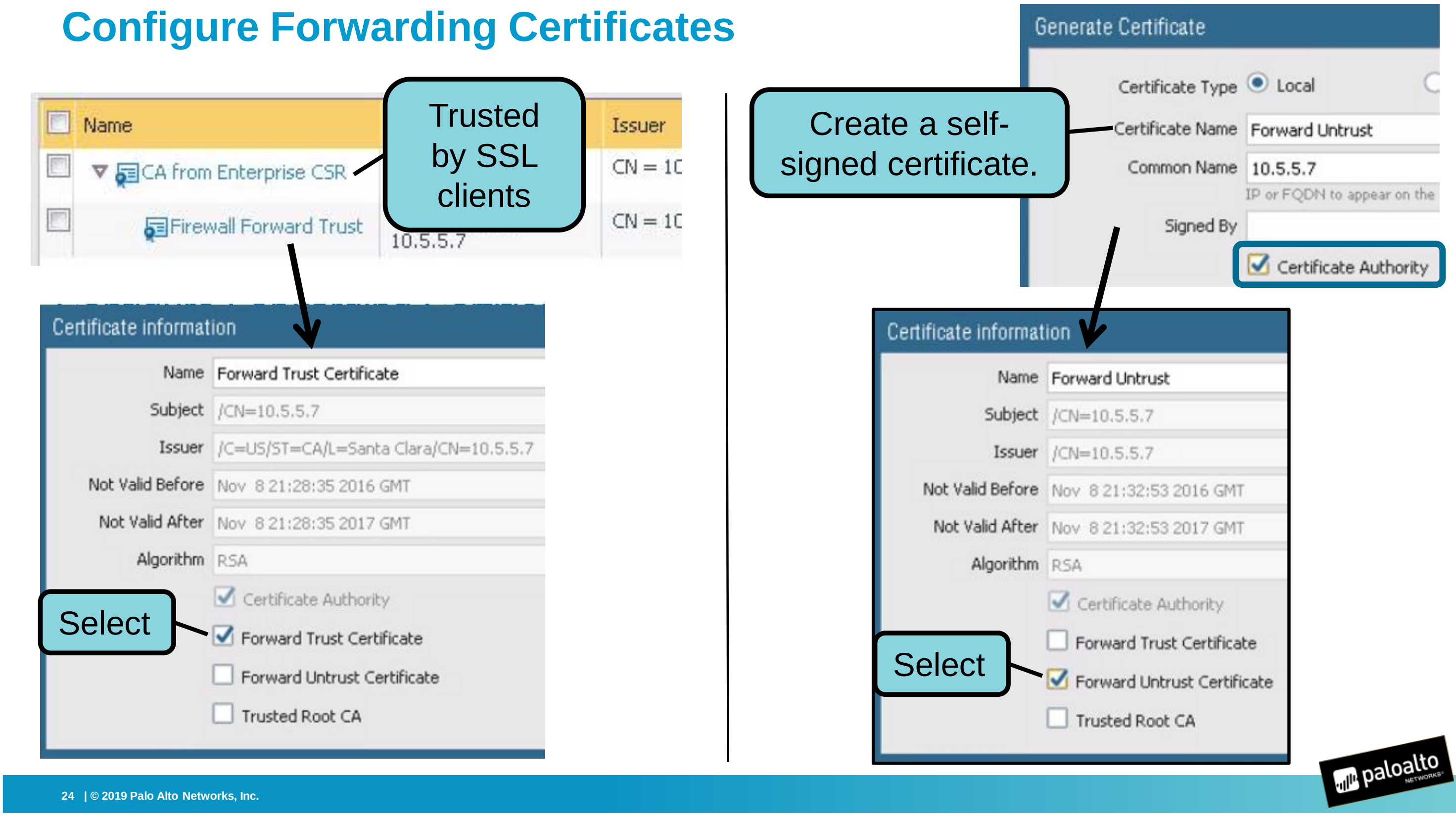
If server certificate is untrusted

23 | © 2019 Palo Alto Networks, Inc.

With SSL Forward Proxy decryption, the firewall resides between the internal SSL client and external web server. As a trusted third party, the firewall uses its forward trust or forward untrust certificates to inform the SSL client whether the firewall has verified the validity of the web server’s certificate.

When an SSL client initiates a session with an external server, the firewall intercepts the SSL request and forwards its own SSL request to the server. The server’s certificate is sent to the firewall. If the server’s certificate is signed by a CA that the firewall trusts, then the firewall creates a copy of the server’s certificate signed by the firewall’s *forward trust* certificate. If the server’s certificate is signed by a CA that the firewall does not trust, the firewall creates a copy of the server’s certificate and signs it with its *forward untrust* certificate. In either case the firewall sends the signed certificate to the SSL client. If a forward untrust certificate was used, the SSL client sees a block page warning that the website it is trying to connect to is not trusted by the firewall that is acting as an SSL Proxy. The user can choose to proceed or terminate the session.

Configure Forwarding Certificates



□ Name	Issuer
□ ▽ CA from Enterprise CSR	CN = 1C
□ Firewall Forward Trust 10.5.5.7	CN = 1C

Certificate information

Name: Forward Trust Certificate
Subject: /CN=10.5.5.7
Issuer: /C=US/ST=CA/L=Santa Clara/CN=10.5.5.7
Not Valid Before: Nov 8 21:28:35 2016 GMT
Not Valid After: Nov 8 21:28:35 2017 GMT
Algorithm: RSA

☑ Certificate Authority
☑ Forward Trust Certificate
□ Forward Untrust Certificate
□ Trusted Root CA

Generate Certificate

Certificate Type: ● Local ○
Certificate Name: Forward Untrust
Common Name: 10.5.5.7
IP or FQDN to appear on the
Signed By:
☑ Certificate Authority

Certificate information

Name: Forward Untrust
Subject: /CN=10.5.5.7
Issuer: /CN=10.5.5.7
Not Valid Before: Nov 8 21:32:53 2016 GMT
Not Valid After: Nov 8 21:32:53 2017 GMT
Algorithm: RSA

☑ Certificate Authority
□ Forward Trust Certificate
☑ Forward Untrust Certificate
□ Trusted Root CA

The first step to configure SSL Forward Proxy decryption is to configure a forward trust certificate on the firewall. The forward trust certificate can be signed by an internal CA or by a firewall CA. Or you can create a firewall self-signed forward trust certificate, but every SSL client will have to have this certificate installed in their certificate store. Otherwise they will get certificate warning errors.

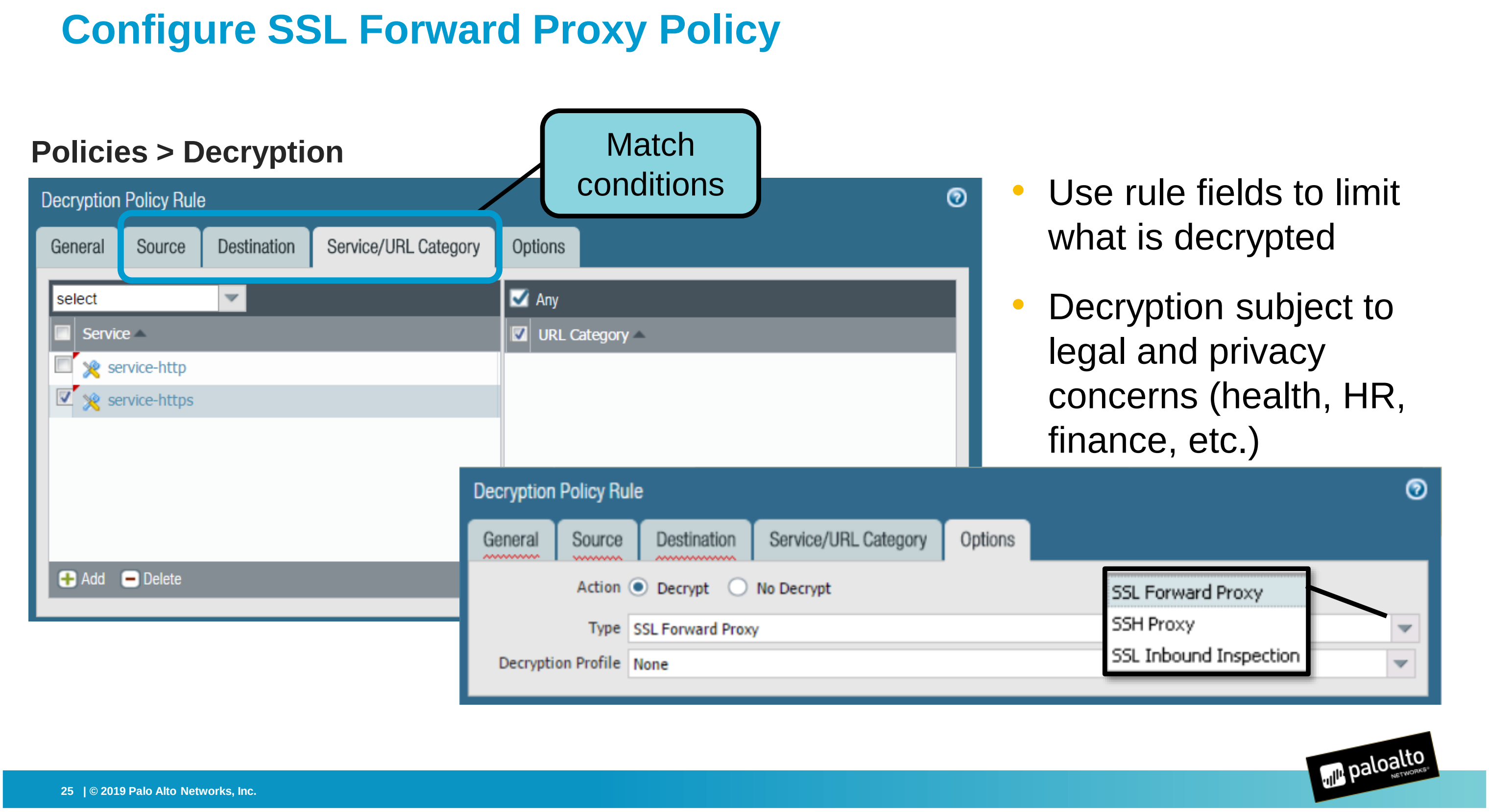
Use the certificate management interface to create a firewall certificate to use as a forward trust certificate. In the example, the Firewall Forward Trust certificate was signed by the CA from the internal CSR certificate, which is why it appears as a child of the CA from the internal CSR certificate. The CA from the internal CSR certificate is trusted by the SSL clients, which means that the clients will trust the Firewall Forward Trust certificate.

Click to open the certificate after it has been created and select the **Forward Trust Certificate** check box, which enables the firewall to use the certificate as its forward trust certificate during SSL Forward Proxy decryption.

Palo Alto Networks recommends that you also configure a forward untrust certificate, which ensures that an SSL client will receive a browser block page when the firewall does not trust the CA of the server to which the client is attempting to connect. This certificate should not be trusted by the SSL clients or they will not get a browser certificate warning when they try to connect to an untrusted server. To ensure that this certificate is not trusted by clients, the certificate should not be issued by a trusted CA nor should it be copied to an SSL client's certificate store.

To create a forward untrust certificate, generate a new certificate on the firewall. This certificate should not be trusted by SSL clients but must still have the capability of signing other server certificates. For these reasons, generate a self-signed certificate that is not signed by any SSL client-recognized CA. Also, do not copy this certificate to the SSL client's certificate stores. However, to ensure that this certificate still can sign the server certificates, select the **Certificate Authority** check box.

After you have generated the new self-signed certificate, click the certificate to open it in the certificate management interface. After the certificate opens, select the **Forward Untrust Certificate** check box to configure it as a forward untrust certificate.



Configure SSL Forward Proxy Policy

Policies > Decryption

Match conditions

- Use rule fields to limit what is decrypted
- Decryption subject to legal and privacy concerns (health, HR, finance, etc.)

Action ● Decrypt ○ No Decrypt

Type SSL Forward Proxy

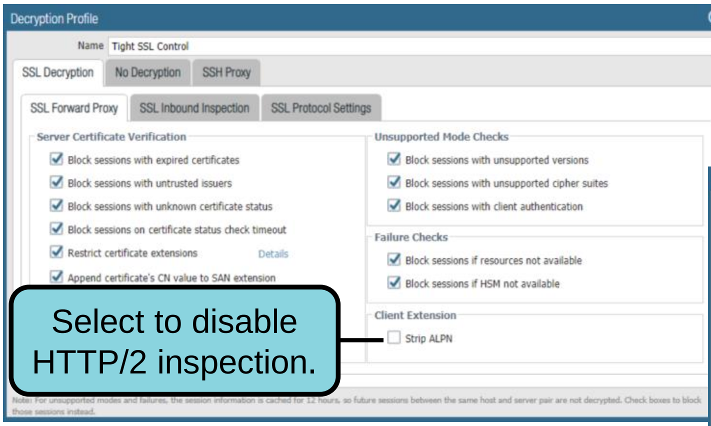
Decryption Profile None

SSL Decryption Policy rulesets are similar to the other rulesets in PAN-OS software. The rules are parsed from top to bottom, comparing network traffic to each rule. When the traffic matches a particular rule, the actions defined in that rule are taken and no further rules are checked.

Not all traffic should be decrypted. Some traffic cannot legally be decrypted, depending on local laws and regulations concerning health records, financial records, and other privacy concerns.

Forward Proxy Decryption Profile

Objects > Decryption > Decryption Profile



Decryption Profile

Name: Tight SSL Control

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

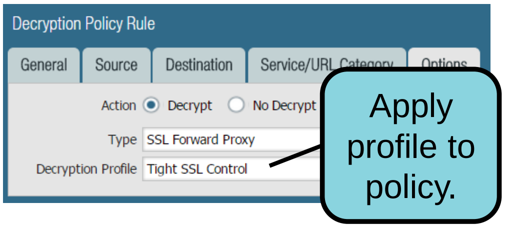
Failure Checks
- ☑ Block sessions if resources not available
- ☑ Block sessions if HSM not available

Client Extension
- □ Strip ALPN

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.

Select to disable HTTP/2 inspection.

Policies > Decryption



Decryption Policy Rule

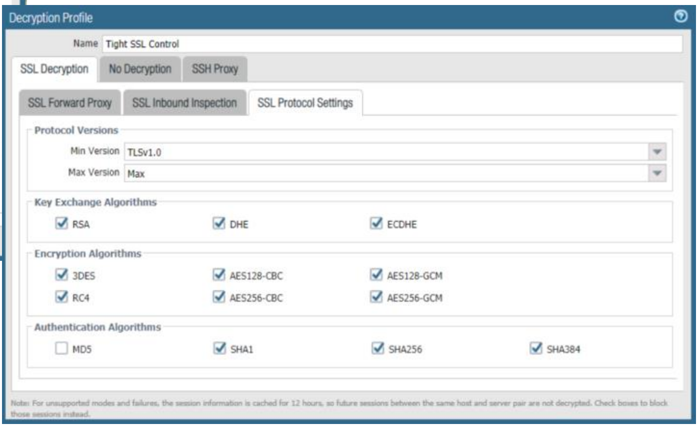
General | Source | Destination | Service/URL Category | Options

Action: ● Decrypt ○ No Decrypt

Type: SSL Forward Proxy

Decryption Profile: Tight SSL Control

Apply profile to policy.



Decryption Profile

Name: Tight SSL Control

SSL Decryption | No Decryption | SSH Proxy

SSL Forward Proxy | SSL Inbound Inspection | SSL Protocol Settings

Protocol Versions
- Min Version: TLSv1.0
- Max Version: Max

Key Exchange Algorithms
- ☑ RSA ☑ DHE ☑ ECDHE

Encryption Algorithms
- ☑ 3DES ☑ AES128-CBC ☑ AES128-GCM
- ☑ RC4 ☑ AES256-CBC ☑ AES256-GCM

Authentication Algorithms
- □ MD5 ☑ SHA1 ☑ SHA256 ☑ SHA384

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.

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

A Decryption Profile enables you to perform checks on decrypted traffic and traffic that you have excluded from decryption. A Decryption Profile enables you to block sessions using unsupported protocols, cipher suites, or sessions that require SSL client authentication. You can block sessions based on certificate status. For example, a certificate could be expired, be signed by an untrusted CA, have extensions restricting the certificate’s use, or have an unknown status. You also can block sessions if the resources to perform decryption are not available or if a hardware security module, or HSM, is not available to sign certificates.

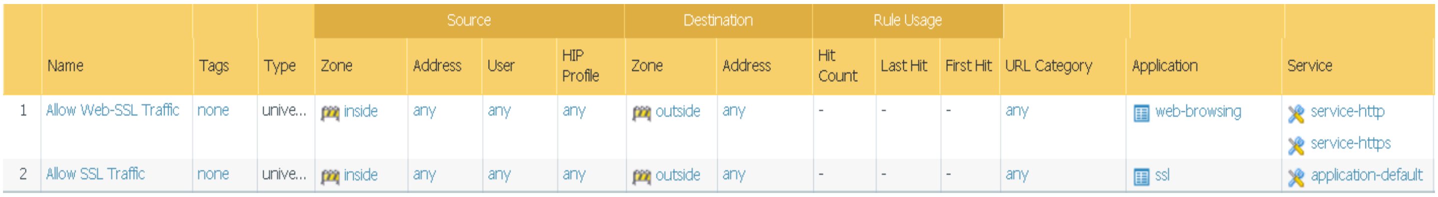
After you create a Decryption Profile, you attach it to a Decryption policy rule. The firewall then enforces the Decryption Profile settings on traffic matched to the Decryption policy rule. Palo Alto Networks firewalls include a default Decryption Profile that you can use to enforce the basic recommended protocol versions and cipher suites for decrypted traffic.

The firewall processes and inspects HTTP/2 traffic by default. The Application-Layer Protocol Negotiation, or ALPN, TLS extension is used to secure HTTP/2 connections. If no value is specified for the ALPN TLS extension, the firewall either downgrades the HTTP/2 traffic to HTTP/1.1 or classifies the traffic as unknown. You can disable HTTP/2 inspection by selecting the **Strip ALPN** check box in the **SSL Forward Proxy** configuration tab.

Create the Security Policy Rules

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

Policies > Security



				Source				Destination		Rule Usage					
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	URL Category	Application	Service
1	Allow Web-SSL Traffic	none	unive...	inside	any	any	any	outside	any	-	-	-	any	web-browsing	service-http service-https
2	Allow SSL Traffic	none	unive...	inside	any	any	any	outside	any	-	-	-	any	ssl	application-default

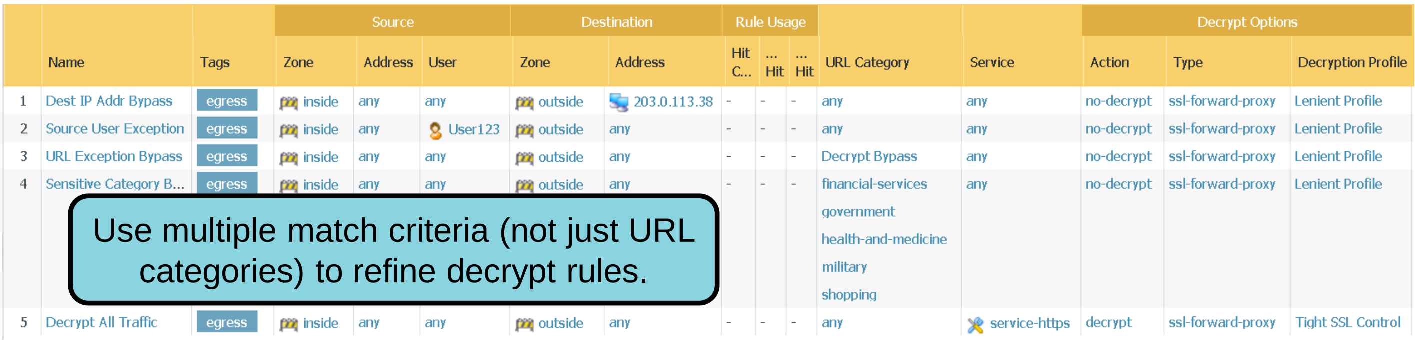
When SSL encrypted traffic first arrives at the firewall, App-ID technology initially identifies the application as ssl. The default port for the ssl application is port 443. If a Security policy rule is configured for the application ssl and the service application-default, then SSL traffic initially will match the rule.

However, after the SSL traffic is decrypted, it might be identified as web-browsing or some other application. If the decrypted traffic is identified as the application web-browsing, it would be identified as web-browsing over port 443. A Security policy rule that allows web-browsing at the service application-default would not match the decrypted traffic because the predefined ports for the web-browsing application are 80 and 8080. For this reason, the Allow Web-SSL Traffic rule service is configured to match the service-http and the service-https rather than application-default. This rule would match web-browsing application traffic at ports 80, 8080, and 443.

Decryption Ruleset Example

- Decrypt everything except sensitive, legally protected traffic
- Create exception rules for specific zones, destination IP, source users, and URL categories
- Attach Decryption Profiles for more granular control

Policies > Decryption



			Source			Destination		Rule Usage					Decrypt Options		
	Name	Tags	Zone	Address	User	Zone	Address	Hit C...	... Hit	... Hit	URL Category	Service	Action	Type	Decryption Profile
1	Dest IP Addr Bypass	egress	inside	any	any	outside	203.0.113.38	-	-	-	any	any	no-decrypt	ssl-forward-proxy	Lenient Profile
2	Source User Exception	egress	inside	any	User123	outside	any	-	-	-	any	any	no-decrypt	ssl-forward-proxy	Lenient Profile
3	URL Exception Bypass	egress	inside	any	any	outside	any	-	-	-	Decrypt Bypass	any	no-decrypt	ssl-forward-proxy	Lenient Profile
4	Sensitive Category B...	egress	inside	any	any	outside	any	-	-	-	financial-services government health-and-medicine military shopping	any	no-decrypt	ssl-forward-proxy	Lenient Profile
5	Decrypt All Traffic	egress	inside	any	any	outside	any	-	-	-	any	service-https	decrypt	ssl-forward-proxy	Tight SSL Control

Use multiple match criteria (not just URL categories) to refine decrypt rules.

Not all SSL traffic should be decrypted. For example, you should not decrypt traffic that is legally protected by privacy laws or has sensitive data such as the traffic going to and from a Human Resources server. In the example, the financial-services, government, health-and-medicine, military, and shopping URL categories have been assigned an action of “no-decrypt.”

You also can create exception rules for specific zones, IP addresses, source users, and custom URL categories. The primary decision often is made on the basis of the URL category. For this reason the URL Filtering and PAN-DB features are important for the Decryption policy. You need a URL Filtering license to use URL categories defined in the PAN-DB database. However, no license is required to create and use your own custom URL categories.

In the example, any SSL traffic to the destination IP address of 203.0.113.38 would not be decrypted. Any SSL traffic from the source user User123 will not be decrypted. Also, any SSL traffic going to the URLs listed in the custom URL category Decrypt Bypass will not be decrypted.

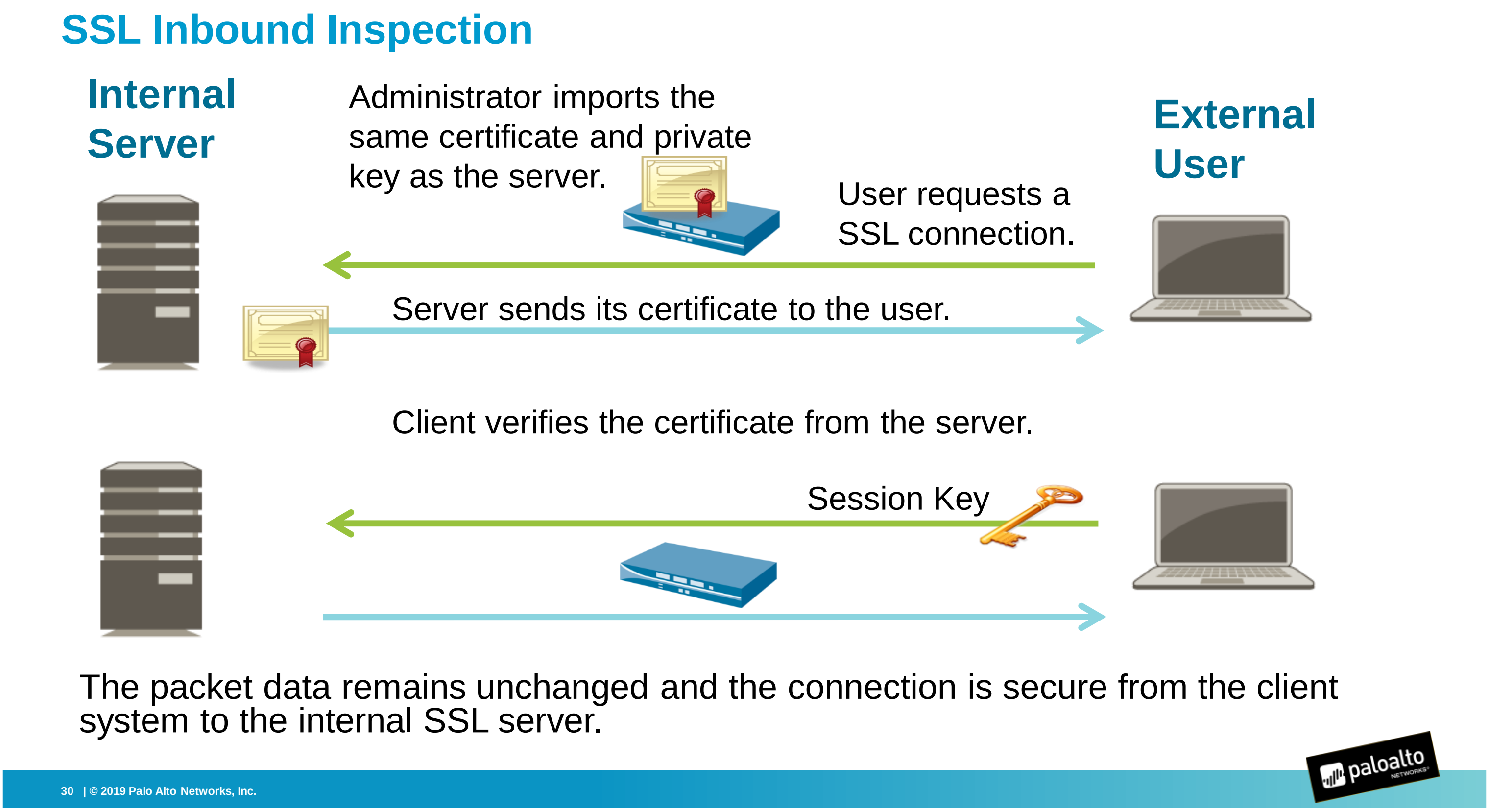
Decryption concepts

Certificate management

SSL forward proxy decryption

SSL inbound inspection

Other decryption topics



SSL Inbound Inspection

Internal Server
Administrator imports the same certificate and private key as the server.
External User
User requests a SSL connection.
Server sends its certificate to the user.
Client verifies the certificate from the server.
Session Key

The packet data remains unchanged and the connection is secure from the client system to the internal SSL server.

30 | © 2019 Palo Alto Networks, Inc.

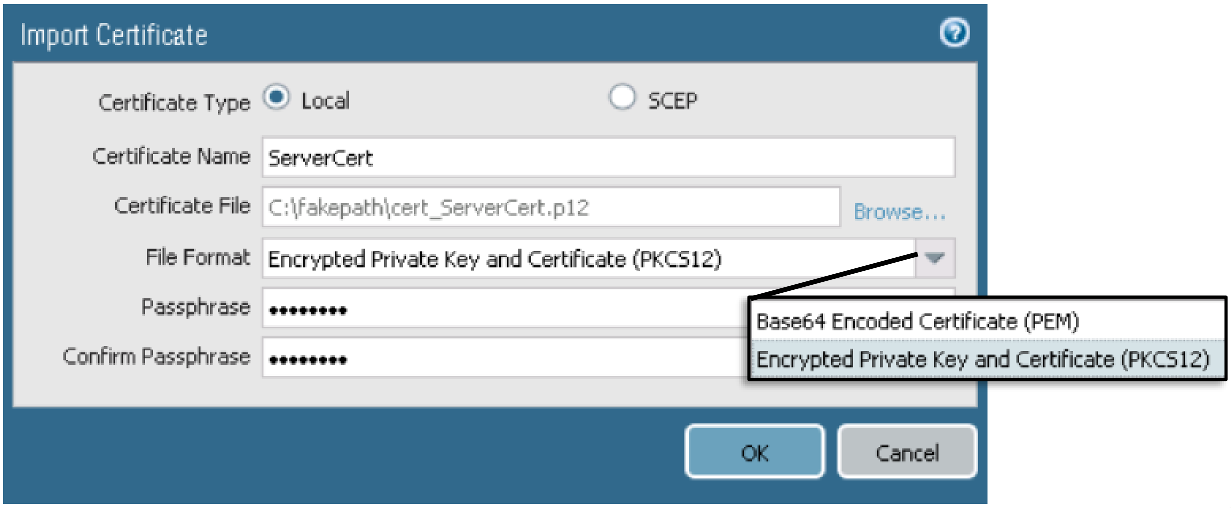
The Palo Alto Networks firewall can inspect inbound SSL traffic for potential threats from external hosts to internal SSL servers. After the inbound traffic has been decrypted and the underlying application and data are exposed, the session can be controlled by Security policy rules and Security Profiles.

Before the firewall can inspect SSL traffic going to an internal server, it needs a copy of the server’s certificate and private key. An SSL Decryption policy rule also must be configured on the firewall to inspect the inbound traffic. After this configuration is complete, the firewall can decrypt and read the traffic before it forwards the traffic to the server. Assuming that the firewall does not block the traffic, it forwards the original encrypted traffic to the internal server. The secure SSL connection remains between the SSL client system and the internal SSL server.

Import Server Certificate and Private Key

- Import the internal server certificate and private key to the firewall

Device > Certificate Management > Certificates > Import



Import Certificate

Certificate Type ● Local ○ SCEP

Certificate Name: ServerCert

Certificate File: C:\fakepath\cert_ServerCert.p12

File Format: Encrypted Private Key and Certificate (PKCS12)

Passphrase: ••••••••

Confirm Passphrase: ••••••••

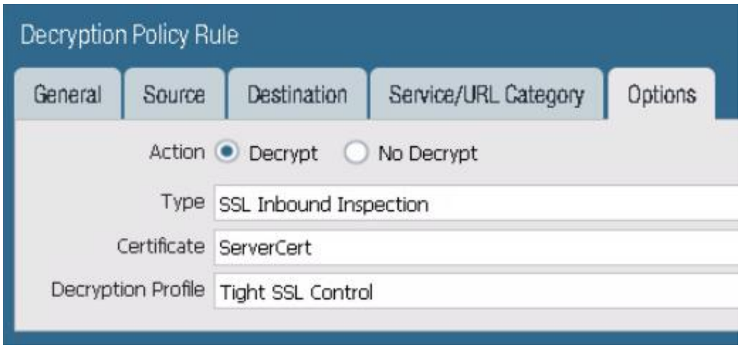
Browse...
Base64 Encoded Certificate (PEM)
Encrypted Private Key and Certificate (PKCS12)
OK
Cancel

Creation of an SSL Inbound Inspection policy is a two-step process, with an optional third step. The first step is to import the internal server’s certificate and private key into the firewall, which enables the firewall to decrypt and inspect traffic going to the internal server.

Configure 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

Action ● Decrypt ○ No Decrypt

Type: SSL Inbound Inspection

Certificate: ServerCert

Decryption Profile: Tight SSL Control

The second step in the configuration of an SSL Inbound Inspection policy is to create the actual Decryption policy rule. You can specify a source zone and IP address, a destination zone and IP address, and a protocol, port, and URL category. Make sure that the destination IP address includes the IP address of the internal server. On the **Options** tab, select **Decrypt** and choose **SSL Inbound Inspection**. For the **Certificate** field, choose the name of the internal server certificate that was imported into the firewall.

An optional third step is to create a Decryption Profile. A Decryption Profile enables you to perform checks on both decrypted traffic and traffic that you have excluded from decryption. You might want to block sessions using unsupported protocols, cipher suites, or sessions that require client authentication. You might want to block sessions based on certificate status, where the certificate is expired, a signature by an untrusted CA, the presence of extensions restricting the certificate use, an unknown certificate status, or a certificate status that cannot be retrieved during a configured timeout period. You might want to block sessions if the resources to perform decryption are not available or if a hardware security module is not available to sign certificates.

After you create a Decryption Profile, attach it to a Decryption policy rule. The firewall then enforces the Decryption Profile settings on traffic matched to the Decryption policy rule. Palo Alto Networks firewalls include a *default* Decryption Profile that you can use to enforce the basic recommended protocol versions and cipher suites for decrypted traffic.

SSL Inbound Inspection uses fewer resources than does SSL Forward Proxy, but each firewall model has a supported limit to the number of imported certificates.

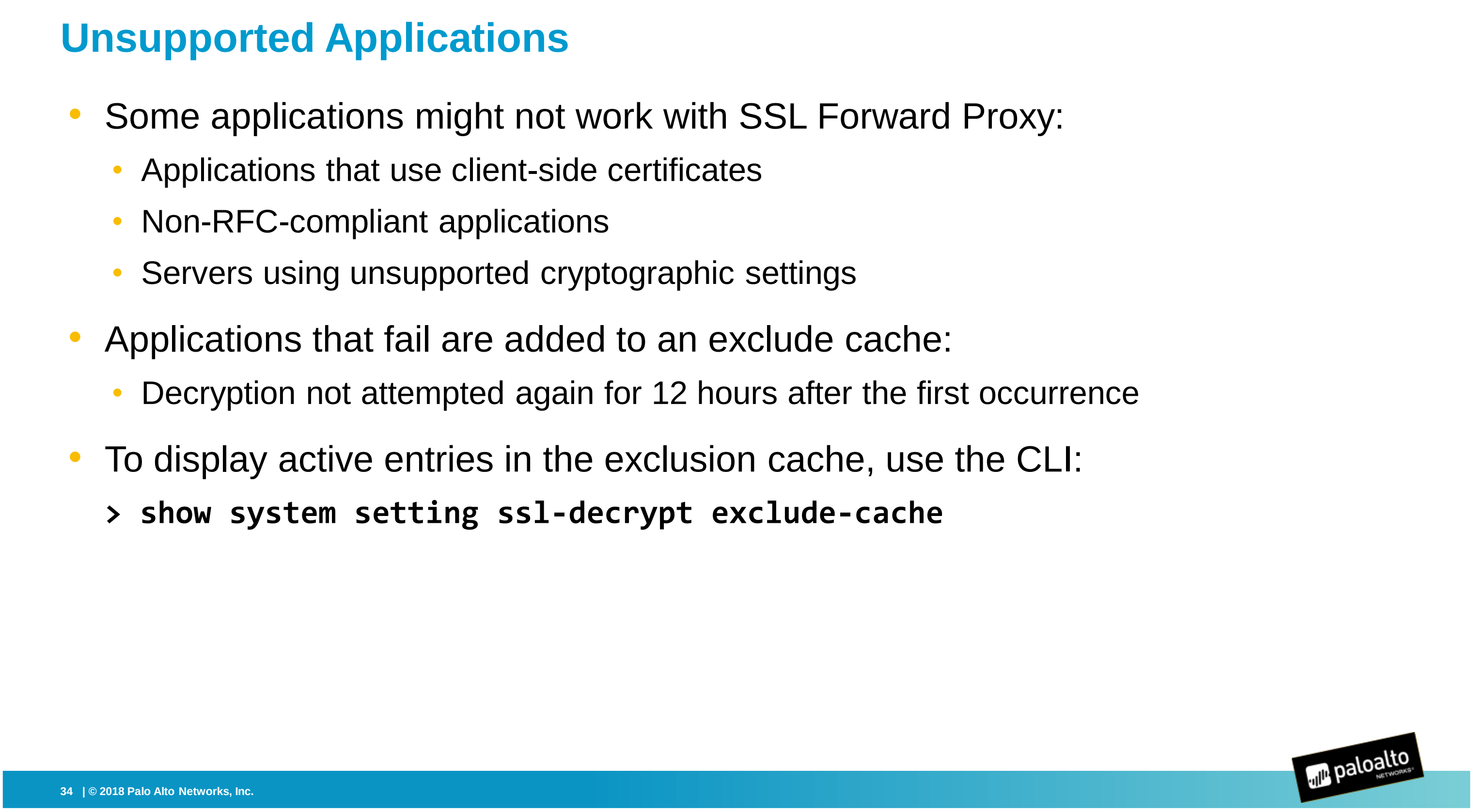
Decryption concepts

Certificate management

SSL forward proxy decryption

SSL inbound inspection

Other decryption topics



Unsupported Applications

- Some applications might not work with SSL Forward Proxy:
  - Applications that use client-side certificates
  - Non-RFC-compliant applications
  - Servers using unsupported cryptographic settings
- Applications that fail are added to an exclude cache:
  - Decryption not attempted again for 12 hours after the first occurrence
- To display active entries in the exclusion cache, use the CLI:

```
> show system setting ssl-decrypt exclude-cache
```

34 | © 2018 Palo Alto Networks, Inc.

Applications use various degrees of SSL for tunneling, privacy, and authentication. Unfortunately, some are not implemented to standards or use capabilities in the standards that are not compatible with Palo Alto Networks SSL decryption capability. SSL decryption also cannot be used when servers require client-side certificates.

When you first implement SSL decryption, use a targeted approach to avoid breaking applications that cannot be successfully decrypted. More aggressive policies can be implemented after the base policy is in place and the full range of applications on the network is known.

When the firewall detects that a session has been broken as a result of the decryption process, it caches the session information and it does not decrypt the next session from that host to the same website. Decryption to that website is not attempted again for 12 hours after the first occurrence. After 12 hours, the firewall attempts to decrypt the traffic from that website again. If decryption fails again, the website is re-added to the cache and the process starts over. To avoid this failure every 12 hours for a site that is known, you can add the site to the decryption exclusion list as shown on the next page.

To display websites that have been cached for 12 hours, use this CLI command:

- `show system setting ssl-decrypt exclude-cache`

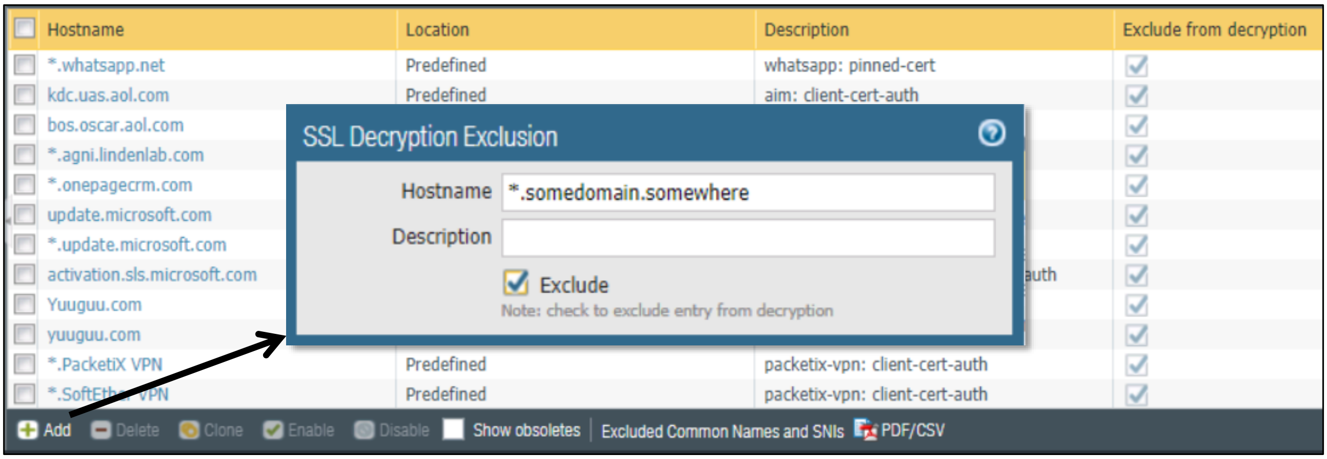
The command output includes the reason that decryption failed. Possible reasons listed include the following:

- `APP_UNSUPPORTED: The application, such as an SSL VPN, is not RFC-compliant.`
- `SSH_ERROR: An SSH application error occurs.`
- `SSH_UNSUPPORTED_ALG: Application-level gateway support is not supported.`
- `SSH_UNSUPPORTED_VERSION: The firewall does not support the SSH version required.`

- **SSL_CLIENT_CERT: The application uses a client certificates.**
- **SSL_EXCLUSION_LIST_MATCH: The SNI or CN matched a username in the exclusion list.**
- **SSL_UNSUPPORTED: The firewall does not support the SSL version required.**
- **SSL_UNSUPPORTED_CIPHER: The server does not support a compatible cipher suite.**

Decryption Exclusions

Device > Certificate Management > SSL Decryption Exclusion



□	Hostname	Location	Description	Exclude from decryption
□	*.whatsapp.net	Predefined	whatsapp: pinned-cert	☑
□	kdc.uas.aol.com	Predefined	aim: client-cert-auth	☑
□	bos.oscar.aol.com			☑
□	*.agni.lindenlab.com			☑
□	*.onepagecrm.com			☑
□	update.microsoft.com			☑
□	*.update.microsoft.com			☑
□	activation.sls.microsoft.com		auth	☑
□	Yuuguu.com			☑
□	yuuguu.com			☑
□	*.PacketiX VPN	Predefined	packetix-vpn: client-cert-auth	☑
□	*.SoftEther VPN	Predefined	packetix-vpn: client-cert-auth	☑

SSL Decryption Exclusion

Hostname: *.somedomain.somewhere

Description:

☑ Exclude

Note: check to exclude entry from decryption

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

Starting with PAN-OS 8.0, you have centralized management for decryption exclusions. You can view predefined decryption exclusions that identify applications that decryption is known to break. Updates and additions to the predefined decryption exclusion list are delivered to the firewall in content updates and are enabled by default. You also can create custom decryption exclusions based on hostname. Hostnames are compared against the Server Name Indication, or SNI, that the client requests or the Common Name, or CN, that is presented in the server certificate. When the hostname matches the SNI or the CN, all traffic originating from or destined to that server is exempt from decryption.

To display the list of websites excluded from decryption, browse to **Device** > **Certificate Management** > **SSL Decryption Exclusion**. To add a website, click **Add**. The **Hostname** field accepts the asterisk wildcard character. In the example, any website in the somedomain.somewhere domain is excluded from decryption. To disable or enable individual exclusions, deselect or select the check box in the **Exclude from decryption** column. To disable or enable multiple exclusions at a time, select multiple exclusion entries using the check box to the left of the **Hostname** column and then click **Disable** or **Enable**.

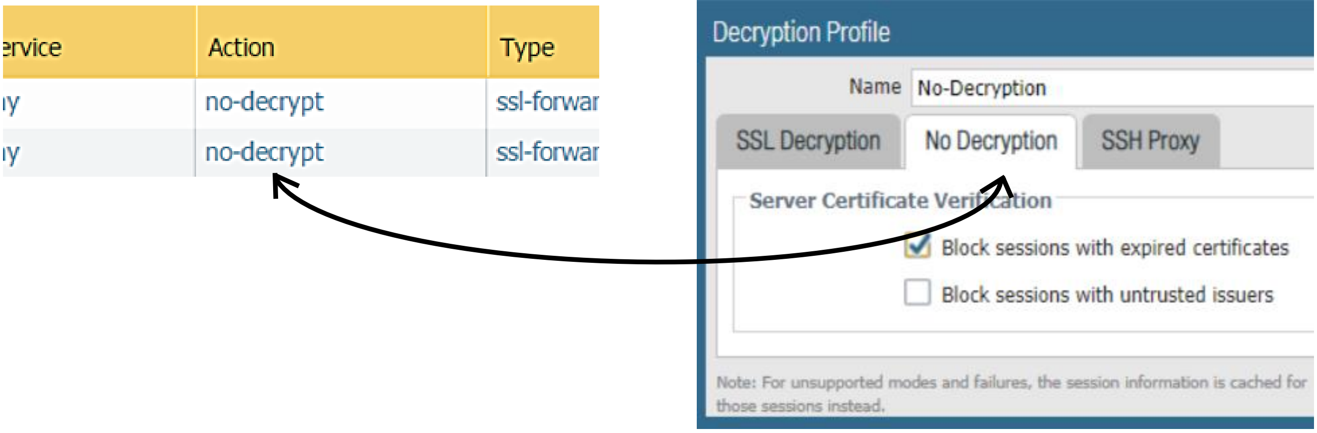
Palo Alto Networks removes decryption exclusions when they become obsolete. However, if a predefined decryption exclusion is disabled, it is not automatically removed from the list. Select **Show obsoletes** to check if there are disabled, predefined exclusions on your list that Palo Alto Networks has determined no longer are needed.

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

Objects > Decryption > Decryption Profile > Add



ervice	Action	Type
iy	no-decrypt	ssl-forwar
iy	no-decrypt	ssl-forwar

Decryption Profile

Name: No-Decryption

Server Certificate Verification

☑ Block sessions with expired certificates

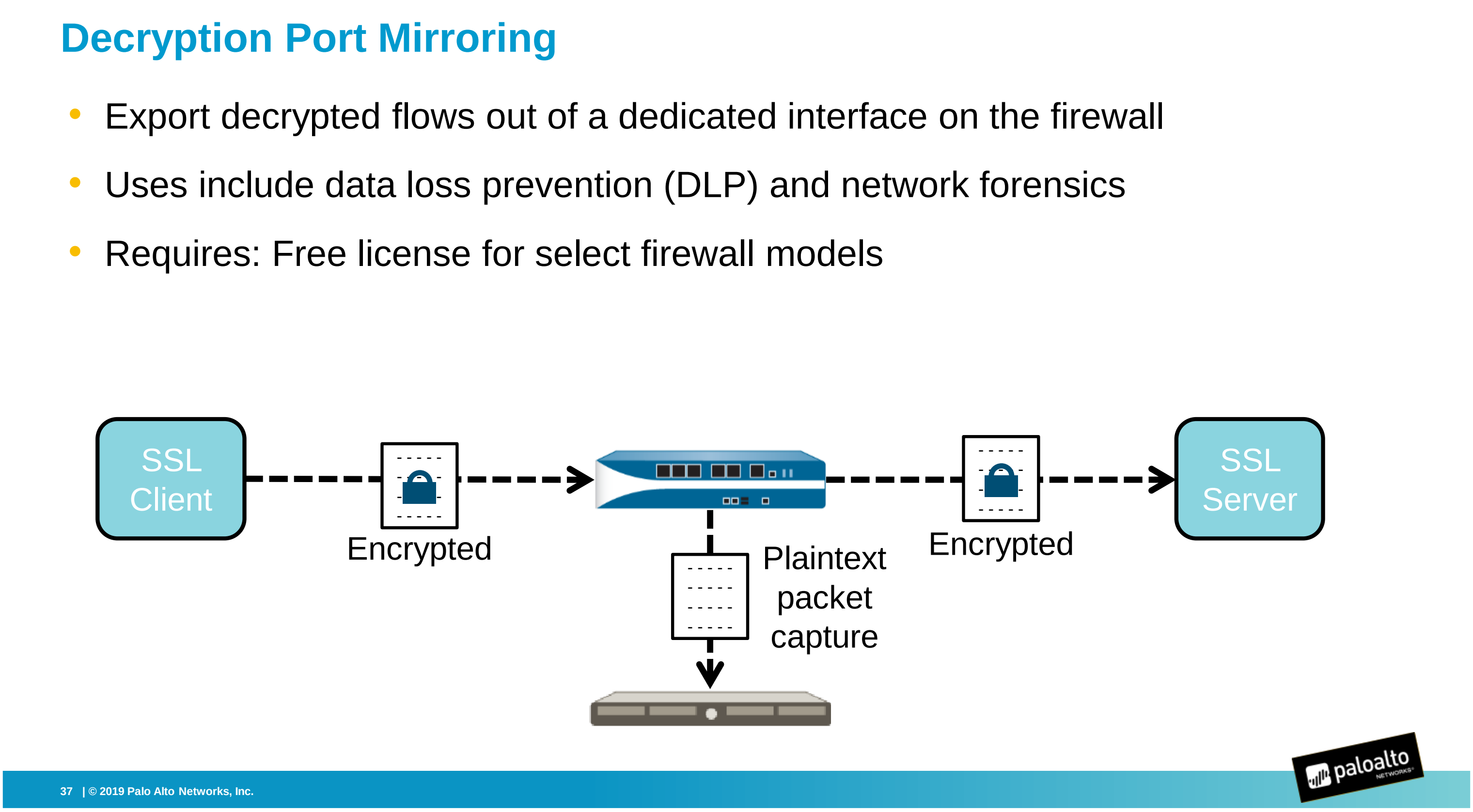
□ Block sessions with untrusted issuers

Note: For unsupported modes and failures, the session information is cached for those sessions instead.

Even if the Decryption policy rule action is “no-decrypt,” the Decryption Profile attached to the rule still can be configured to block sessions with expired or untrusted certificates. To check certificates, click the **No Decryption** tab in the Decryption Profile and select the desired check boxes.

Selection of **Block sessions with expired certificates** terminates the SSL connection if the server certificate is expired. This action prevents a user from being able to accept an expired certificate and continue with an SSL session. Selection of **Block sessions with untrusted issuers** terminates the SSL session if the server certificate issuer is untrusted. The Traffic log records entries for terminated sessions.

For the firewall to perform these certificate checks, it still must act as an SSL proxy even though the application data is not decrypted. The Traffic log for the session will include a decrypted flag, but the application will be listed as ssl instead of web-browsing or an actual application name.



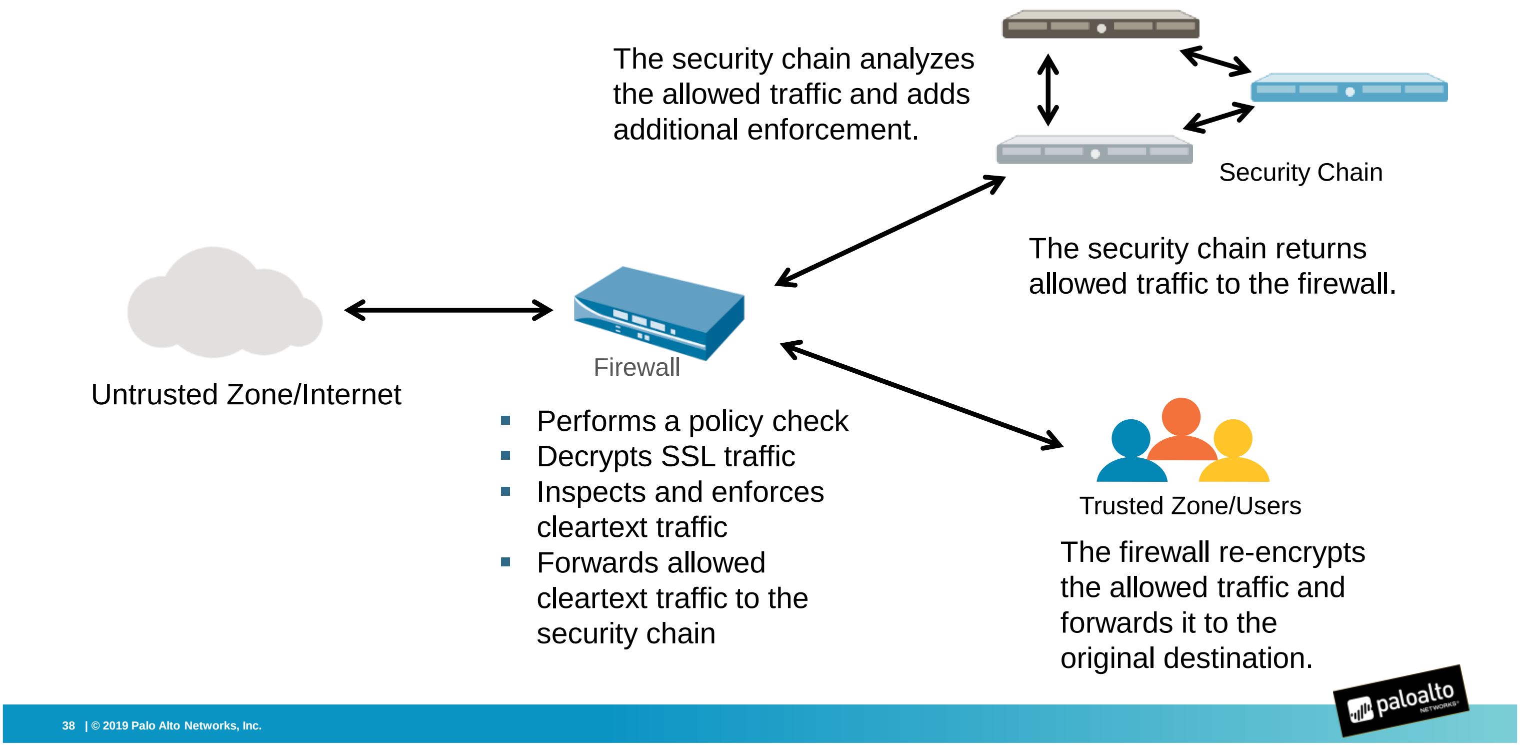
Decryption Port Mirroring

- Export decrypted flows out of a dedicated interface on the firewall
- Uses include data loss prevention (DLP) and network forensics
- Requires: Free license for select firewall models

The decryption port mirroring feature enables a firewall to forward packet captures of decrypted traffic to a traffic collection tool, such as NetWitness or Solera, for archiving and analysis. This feature is necessary for organizations that require comprehensive data capture for forensic and historical purposes or to enhance DLP functionality.

The decryption port mirroring feature is available only on the PA-3000 Series, PA-5200 Series, and PA-7000 Series platforms and requires a free PAN-PA-DECRYPT license to be installed to enable it. This free license is perpetual with no expiration date and can be requested from the Customer Support Portal at support.paloaltonetworks.com.

Decryption Broker



The security chain analyzes the allowed traffic and adds additional enforcement.

The security chain returns allowed traffic to the firewall.

- Performs a policy check
- Decrypts SSL traffic
- Inspects and enforces cleartext traffic
- Forwards allowed cleartext traffic to the security chain

The firewall re-encrypts the allowed traffic and forwards it to the original destination.

38 | © 2019 Palo Alto Networks, Inc.

Palo Alto Networks next-generation firewalls can provide a single, central point for decrypting all of your network traffic. The decryption broker enables the firewall to forward plain, cleartext traffic to a security chain for additional enforcement, which provides complete visibility into network traffic. A security chain is a set of inline, third-party appliances dedicated to perform a specific security function such as an Intrusion Prevention System, or IPS. A single firewall can distribute decrypted sessions to a maximum of 64 security chains, and the firewall can monitor the security chains to ensure that they are effectively processing traffic.

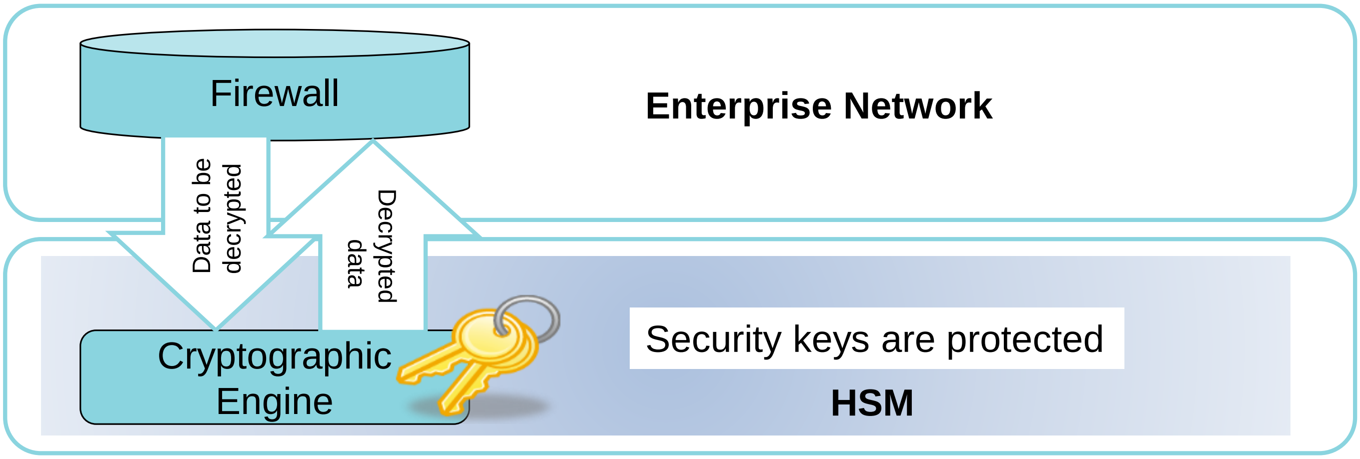
The decryption broker also enables you to simplify your network security deployment. By enabling the decryption broker, you can eliminate the need for a third-party SSL decryption solution and reduce the number of third-party devices performing traffic analysis and enforcement. For networks without a dedicated SSL decryption appliance, the decryption broker reduces latency because the traffic flow is decrypted only once, at the firewall.

In a decryption broker deployment, the firewall provides session distribution to the security chain, ensuring that the security chain devices are not oversubscribed. When the firewall receives traffic back from the security chain, the firewall re-encrypts the traffic and forwards the traffic to its destination.

The decryption broker feature is supported for PA-7000 Series, PA-5200 Series, PA-3200 Series, and VM-Series devices running PAN-OS 8.1 or later, and is supported only with SSL Forward Proxy decryption enabled.

Hardware Security Modules (HSMs)

- Cryptographic devices designed to safeguard security keys



An HSM is a physical device that generates, stores, and manages digital keys. It provides logical and physical protection of the firewall’s private keys from nonauthorized use and potential adversaries.

Use dedicated HSMs to manage the certificate signing functions for SSL Forward Proxy, SSL Inbound Inspection, and master key storage functions.

HSM support generally is required when FIPS 140-2 Level 3 protection for CA keys is required.

Palo Alto Networks firewalls can be used with SafeNet Luna SA 5.2.1 or later HSMs and with Thales nShield Connect 11.62 or later HSMs.

HSM use is supported on the PA-3000 Series, PA-5200 Series, PA-7000 Series, and VM-Series firewalls. It also is supported on the Panorama M-100 and M-500 appliances, and on the Panorama VM.

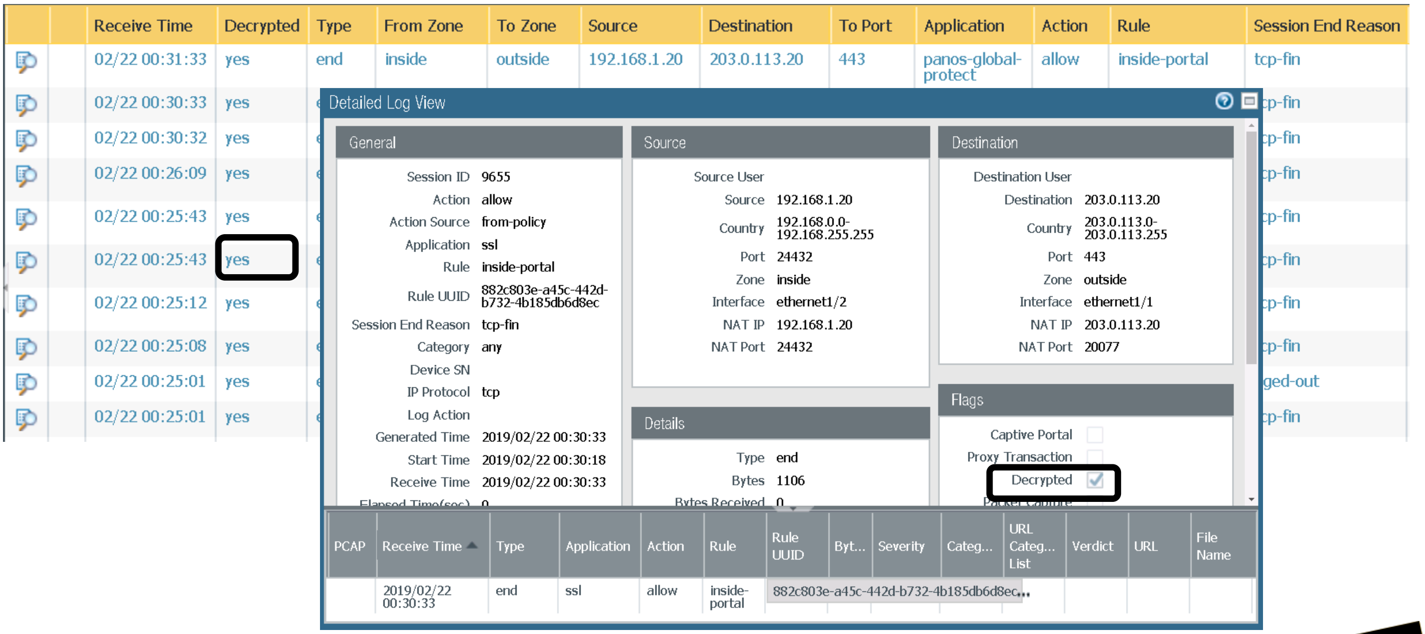
HSM can be used with Palo Alto Networks devices for secure certificate signing in an SSL Forward Proxy deployment, in secure session key decryption in an SSL Inbound Inspection deployment, and in secure decryption of master keys.

Each firewall maintains a default master key that is used to encrypt its private keys, session keys used in asymmetric encryption, and locally stored passwords. To increase the level of master key security, you change the default master key on each firewall and encrypt the master key with a wrapping key that resides on an HSM.

For more information about integrating an HSM with your firewall, see the *PAN-OS Administrator’s Guide Version 9.0* at https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin.html.

Decryption in the Traffic Log

Monitor > Logs > Traffic



	Receive Time	Decrypted	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule	Session End Reason
	02/22 00:31:33	yes	end	inside	outside	192.168.1.20	203.0.113.20	443	panos-global-protect	allow	inside-portal	tcp-fin
	02/22 00:30:33	yes										cp-fin
	02/22 00:30:32	yes										cp-fin
	02/22 00:26:09	yes	e									cp-fin
	02/22 00:25:43	yes	e									cp-fin
	02/22 00:25:43	yes	e									cp-fin
	02/22 00:25:12	yes	e									cp-fin
	02/22 00:25:08	yes	e									cp-fin
	02/22 00:25:01	yes	e									ged-out
	02/22 00:25:01	yes	e									cp-fin

Detailed Log View

General

Session ID	9655
Action	allow
Action Source	from-policy
Application	ssl
Rule	inside-portal
Rule UUID	882c803e-a45c-442d-b732-4b185db6d8ec
Session End Reason	tcp-fin
Category	any
Device SN	
IP Protocol	tcp
Log Action	
Generated Time	2019/02/22 00:30:33
Start Time	2019/02/22 00:30:18
Receive Time	2019/02/22 00:30:33
Elapsed Time(sec)	0

Source

Source User	
Source	192.168.1.20
Country	192.168.0.0-192.168.255.255
Port	24432
Zone	inside
Interface	ethernet1/2
NAT IP	192.168.1.20
NAT Port	24432

Destination

Destination User	
Destination	203.0.113.20
Country	203.0.113.0-203.0.113.255
Port	443
Zone	outside
Interface	ethernet1/1
NAT IP	203.0.113.20
NAT Port	20077

Details

Type	end
Bytes	1106
Bytes Received	0

Flags

Captive Portal	□
Proxy Transaction	□
Decrypted	☑
Packet Capture	

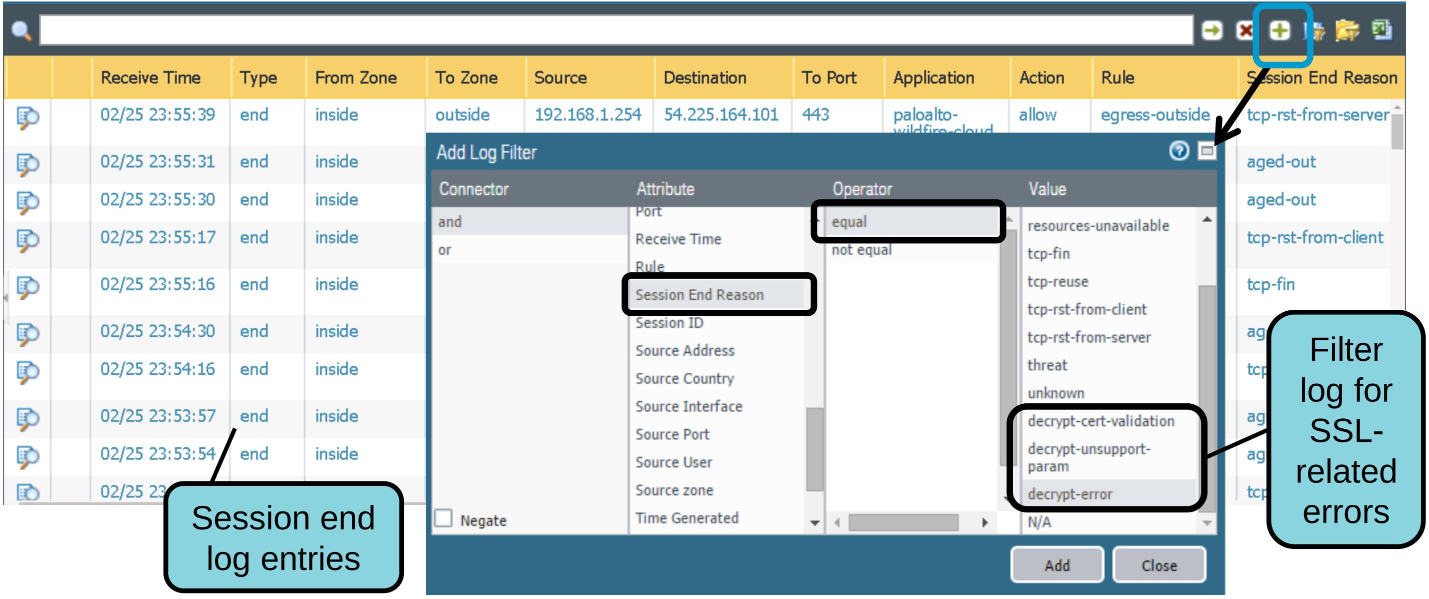
PCAP	Receive Time	Type	Application	Action	Rule	Rule UUID	Byt...	Severity	Categ...	URL Categ... List	Verdict	URL	File Name
	2019/02/22 00:30:33	end	ssl	allow	inside-portal	882c803e-a45c-442d-b732-4b185db6d8ec...							

You can use the Traffic log to determine whether SSL sessions are being decrypted. If the log entry contains a packet capture, the packet capture will be encrypted because packet capture occurs before decryption.

You also can search for decryption traffic by using the log filter (`flag has proxy`).

Troubleshooting SSL Session Terminations

Monitor > Logs > Traffic



Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule	Session End Reason
02/25 23:55:39	end	inside	outside	192.168.1.254	54.225.164.101	443	paloalto-wildfire-cloud	allow	egress-outside	tcp-rst-from-server
02/25 23:55:31	end	inside								aged-out
02/25 23:55:30	end	inside								aged-out
02/25 23:55:17	end	inside								tcp-rst-from-client
02/25 23:55:16	end	inside								tcp-fin
02/25 23:54:30	end	inside								ag
02/25 23:54:16	end	inside								tcp
02/25 23:53:57	end	inside								ag
02/25 23:53:54	end	inside								ag
02/25 23										tcp

Add Log Filter

Connector	Attribute	Operator	Value
and	Port	equal	resources-unavailable
or	Receive Time	not equal	tcp-fin
	Rule		tcp-reuse
	Session End Reason		tcp-rst-from-client
	Session ID		tcp-rst-from-server
	Source Address		threat
	Source Country		unknown
	Source Interface		decrypt-cert-validation
	Source Port		decrypt-unsupport-param
	Source User		decrypt-error
	Source zone		N/A
	Time Generated		

☐ Negate

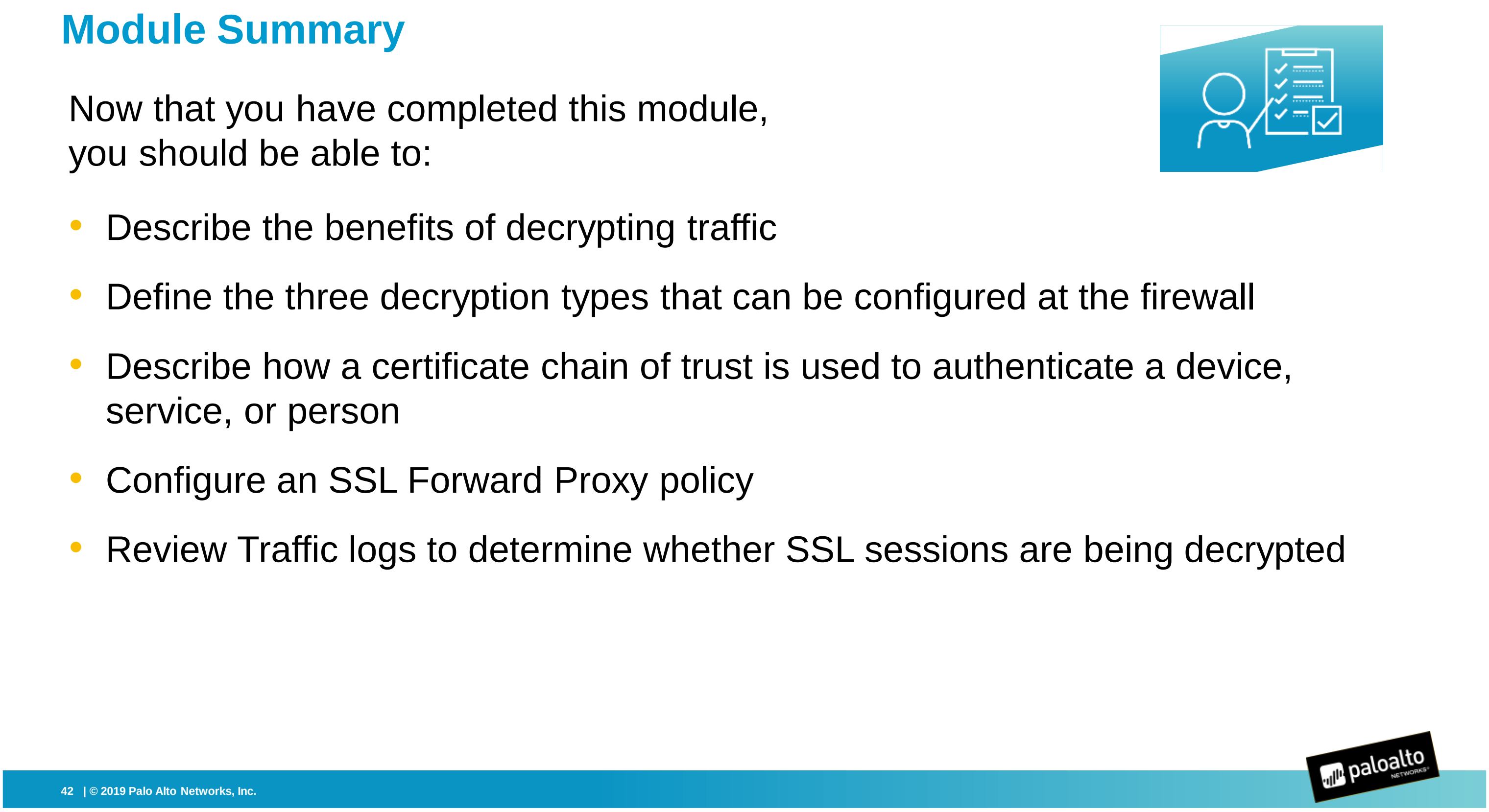
Session end log entries

Filter log for SSL-related errors

SSL sessions can be terminated for reasons that might include expired server certificates, unsupported ciphers or protocol versions, untrusted certificate issuers, and unknown certificate status and SSL timeout events. SSH decryption can be terminated because of unsupported SSH algorithms.

The Traffic log records the start and end of each session. The word “end” in the **Type** column indicates a log entry for the end of a session. The **Session End Reason** column records why a session ended. You can use the **Session End Reason** filter values to filter the list of sessions to display only sessions that ended because of problems specific to SSL. SSL sessions that were terminated because of a Decryption Profile “block” action or the reception or transmission of fatal SSL/TLS alert messages are mapped to one of the following **Session End Reason** values:

- **decrypt-cert-validation:** An SSL session is terminated with this end reason attribute under one or more of the following scenarios:
  - Expired server certificate
  - Untrusted issuer
  - Unknown certificate status
  - Certificate status timeout
  - Client authentication
- **decrypt-unsupport-param:** An SSL session is terminated with this end reason attribute under one or more of the following scenarios:
  - Unsupported protocol version
  - Unsupported cipher
  - Unsupported SSH algorithm
- **decrypt-error:** An SSL session is terminated with this end reason attribute under one or more of the following scenarios:
  - Resources unavailable
  - HSM unavailable
  - SSH errors



Module Summary

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

- Describe the benefits of decrypting traffic
- Define the three decryption types that can be configured at the firewall
- Describe how a certificate chain of trust is used to authenticate a device, service, or person
- Configure an SSL Forward Proxy policy
- Review Traffic logs to determine whether SSL sessions are being decrypted

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

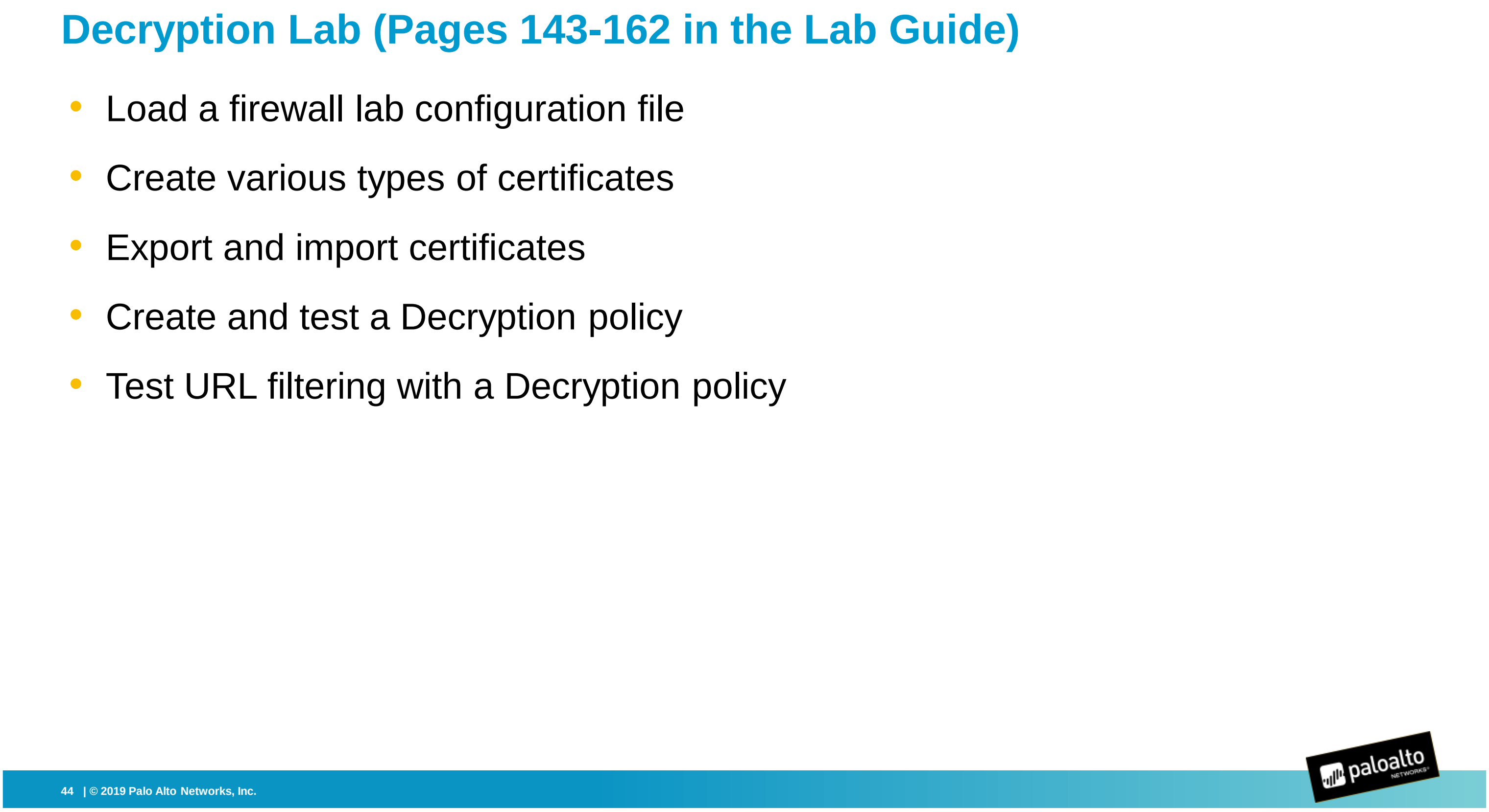
- Describe the benefits of decrypting traffic
- Define the three decryption types that can be configured at the firewall
- Describe how a certificate chain of trust is used to authenticate a device, service, or person
- Configure an SSL Forward Proxy policy
- Review Traffic logs to determine whether SSL sessions are being decrypted

Questions?

43 | © 2019 Palo Alto Networks, Inc.

Review Questions

1. Which three statements are true regarding a public key infrastructure? (Choose three.)
   a. solves the problem of secure identification of public keys
   b. uses digital certificates to verify key owners
   c. relies on the manual distribution of shared keys
   d. has root and intermediate certificate authorities
2. True or false? When the firewall is configured to inspect SSL traffic going to an internal server for which the firewall has the private key, it functions as a forward proxy.
   a. true
   b. false
3. What are two methods of certificate revocation? (Choose two.)
   a. CRL
   b. OCSP
   c. IKE
   d. SSH
4. True or false? When the firewall is configured to decrypt SSL traffic going to external sites, it functions as a forward proxy.
   a. true
   b. false
5. When the firewall detects that a session has been broken as a result of the decryption process, it will cache the session information and will not attempt to decrypt the next session to the same server. How many hours does this cache entry persist?
   a. 8
   b. 12
   c. 18
   d. 24



Decryption Lab (Pages 143-162 in the Lab Guide)

- Load a firewall lab configuration file
- Create various types of certificates
- Export and import certificates
- Create and test a Decryption policy
- Test URL filtering with a Decryption policy

PROTECTION. DELIVERED.

Answers to Review Questions

1. a, b, d
2. b (false)
3. a, b
4. a (true)
5. b