DECRYPTION

EDU-210 Version A
PAN-OS® 9.0

DETECT THREATS IN SSL

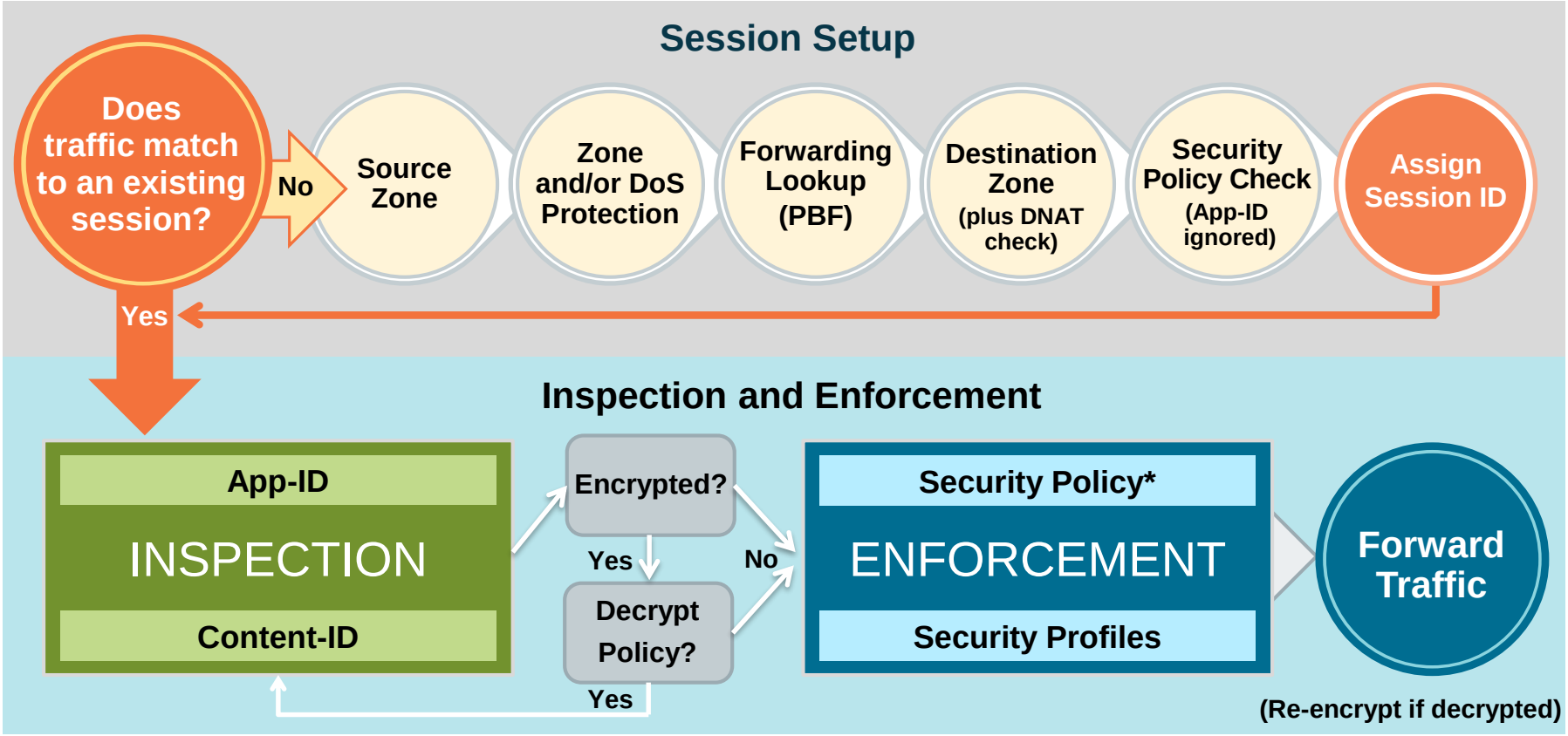
- Decryption concepts
- Certificate management
- SSL forward proxy decryption
- SSL inbound inspection
- Other decryption topics

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

Flow Logic of the Next-Generation Firewall



* Policy check relies on pre-NAT IP addresses

Decryption concepts

Certificate management

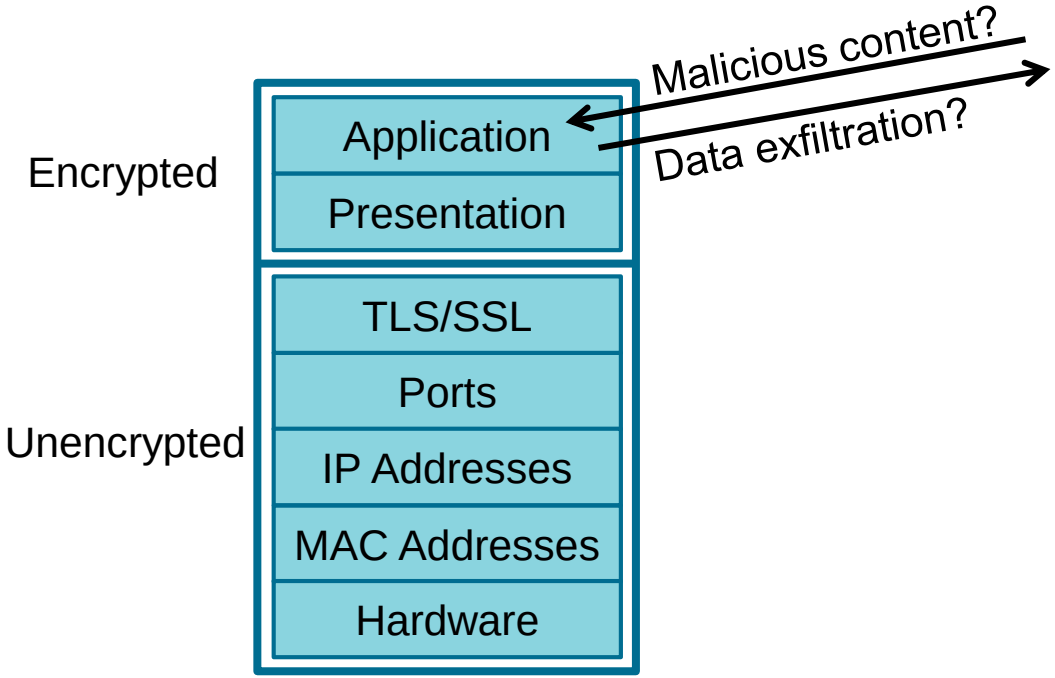
SSL forward proxy decryption

SSL inbound inspection

Other decryption topics

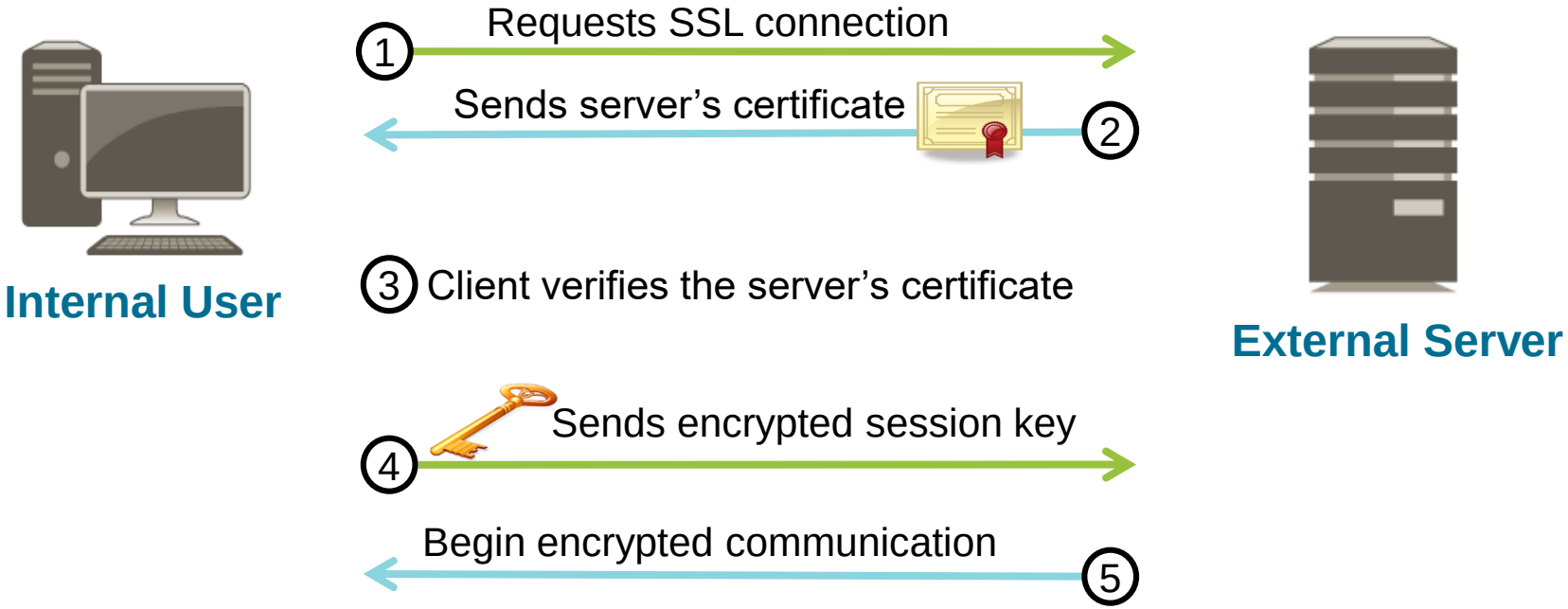
Why Decrypt Network Traffic?

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



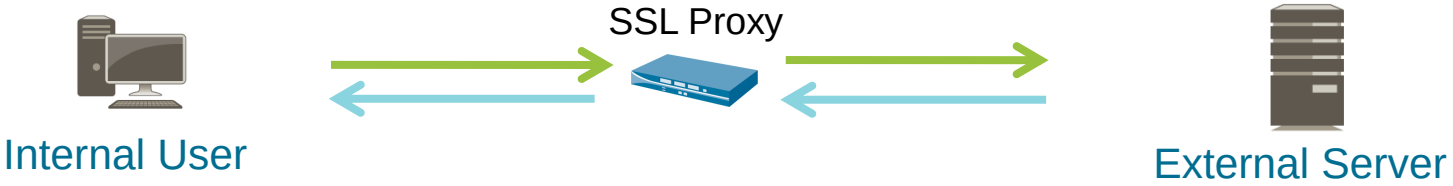
SSL/TLS Session Overview

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

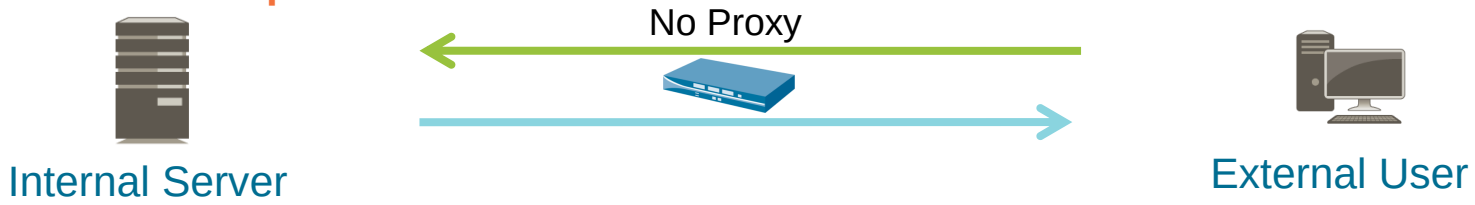


Firewall Decryption Types

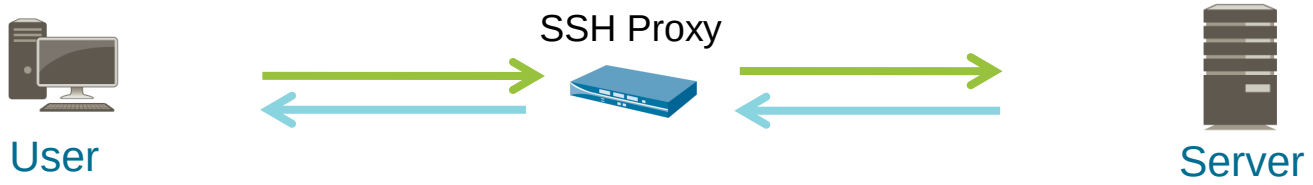
SSL Forward Proxy (Outbound)



SSL Inbound Inspection

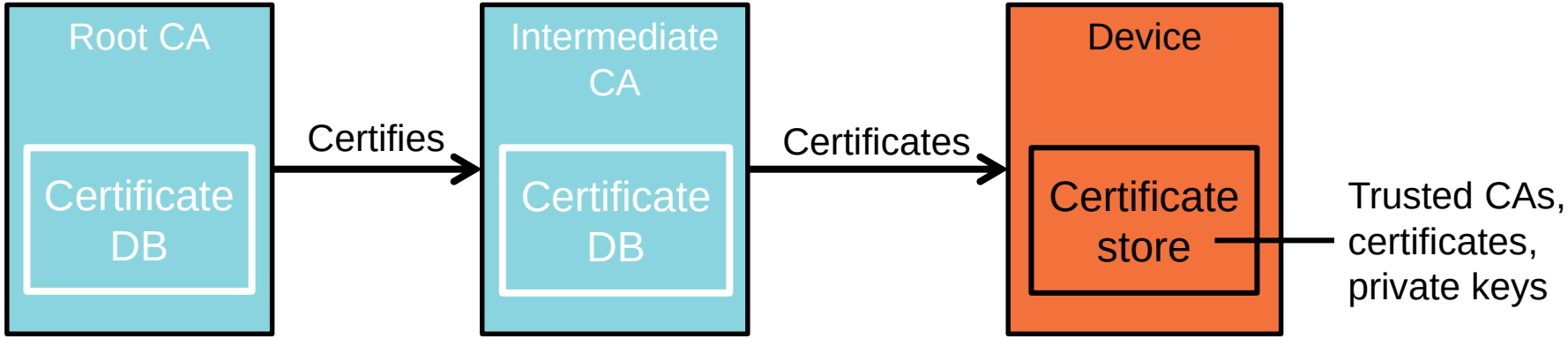


SSH Decryption

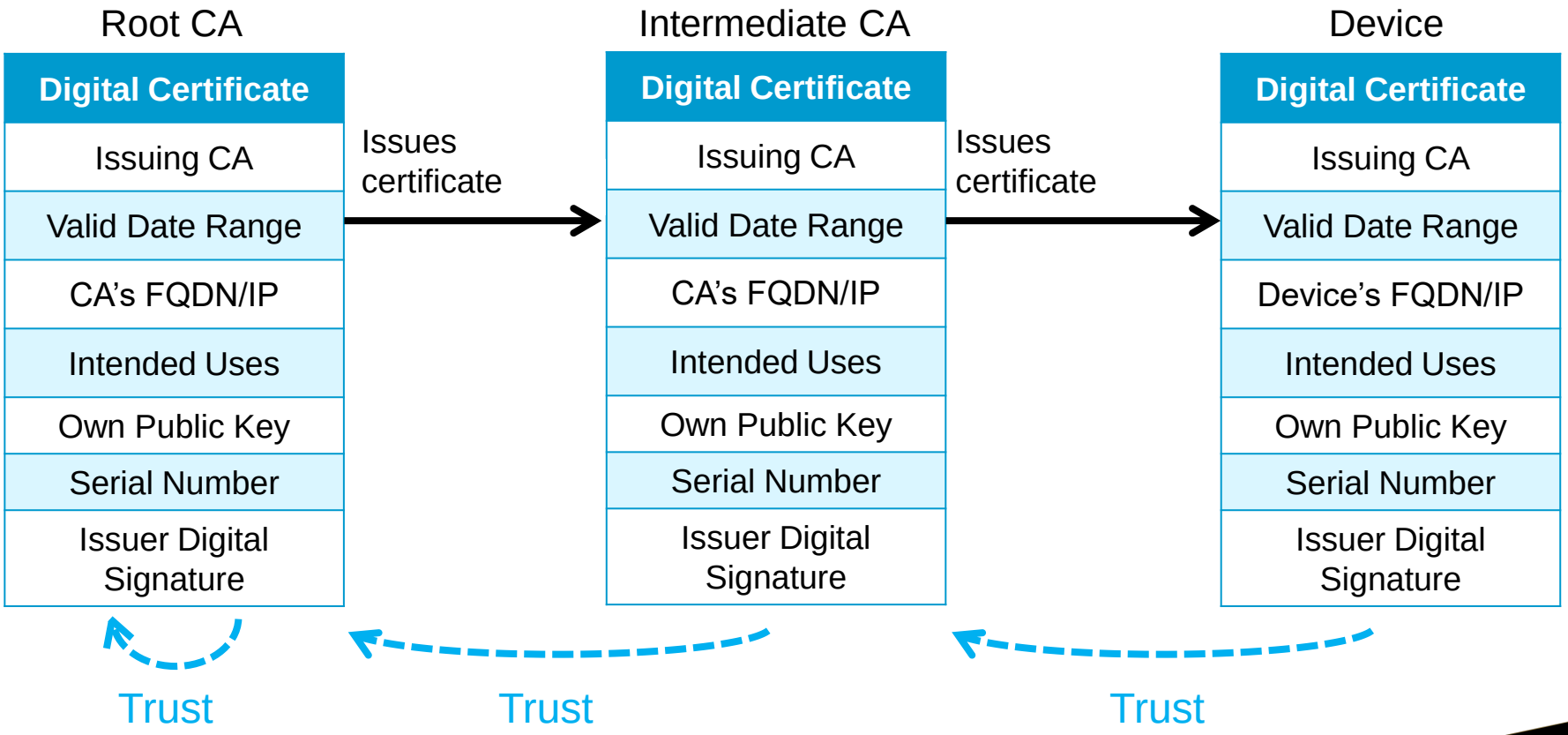


Public Key Infrastructure (PKI)

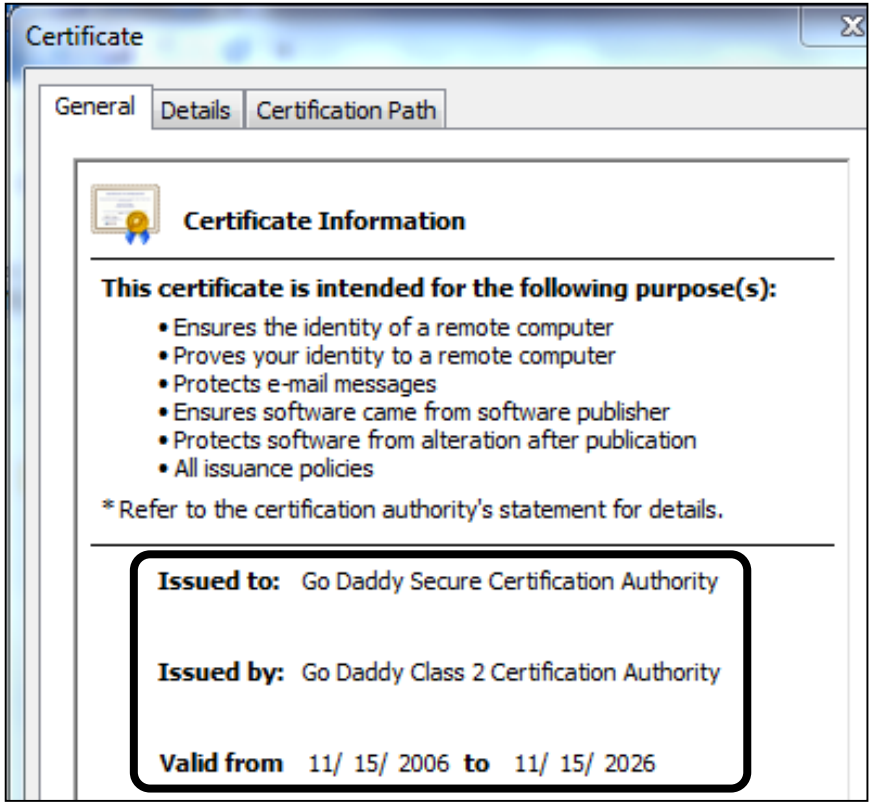
- Solves the problem of secure identification of public keys
- Uses digital certificates to verify public key owners
- Typical PKI components:

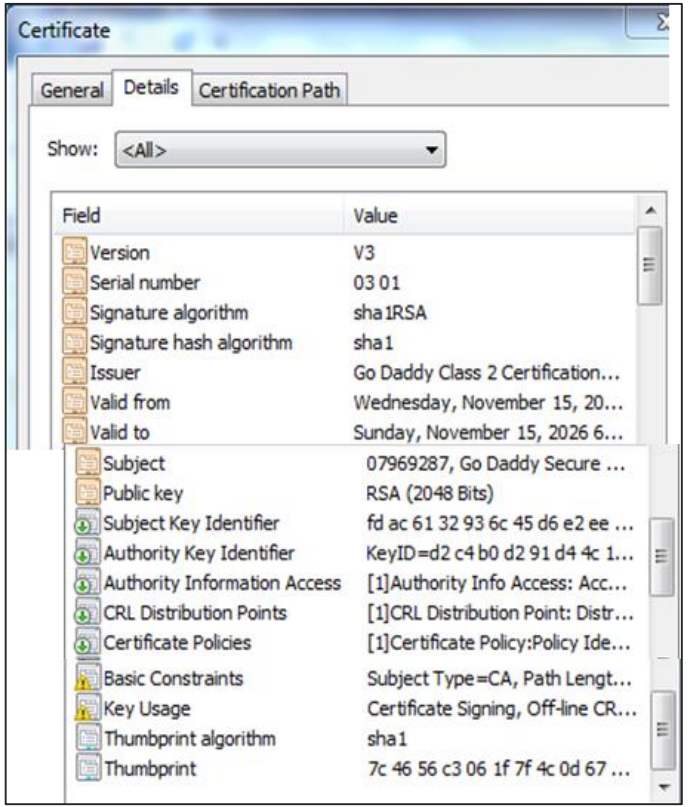


Certificate Chain of Trust



Certificate Example





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.

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

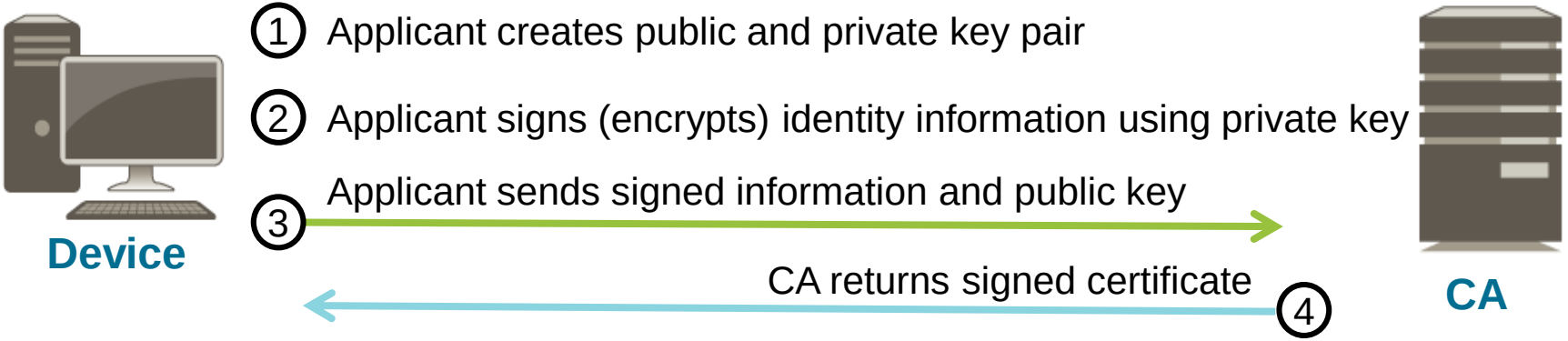
Certificate revocation list (CRL)

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

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.

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

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

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

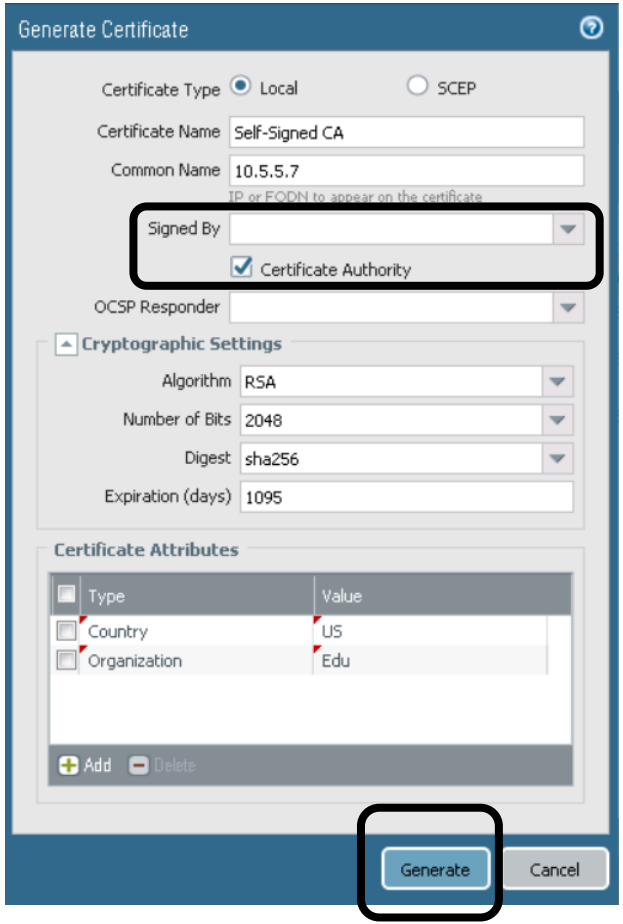
Firewall CA Certificate Deployment Choices

- 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

Generate Self-Signed CA Certificate

Method 1:

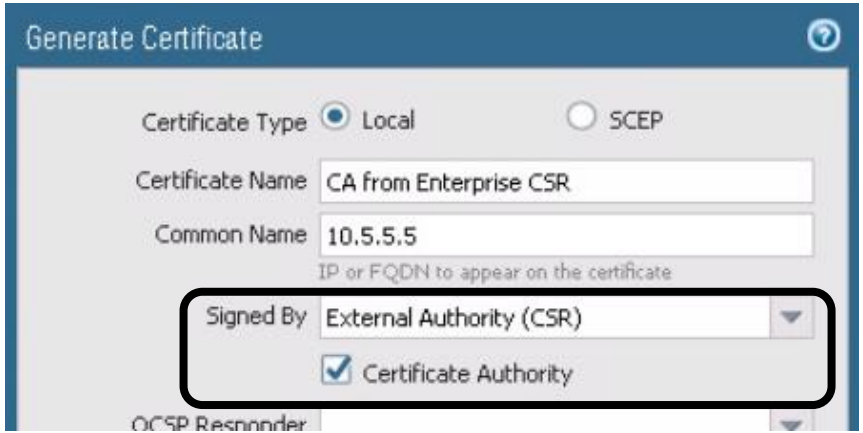
- Create a self-signed firewall CA certificate:
  - Use **Device > Certificate Management > Certificates > Generate**
- Complete the form and click Generate
- Creates a self-signed CA certificate
- Creates public and private keys



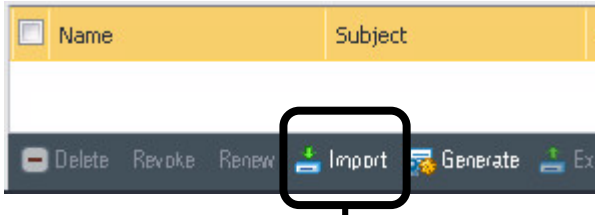
Generate CA Certificate Using CSR

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

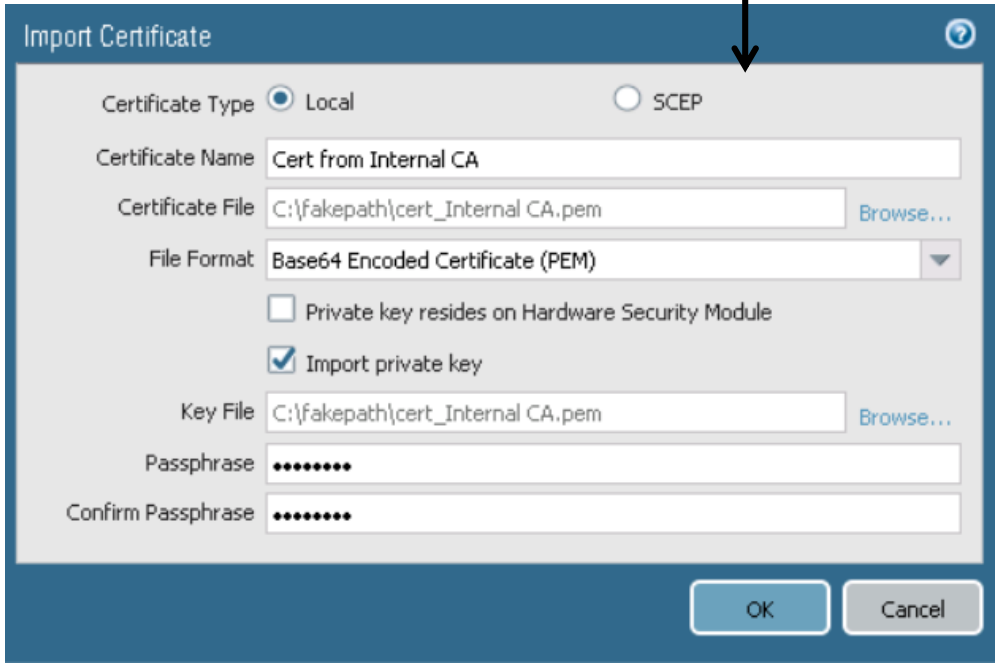


Import CA Certificate



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



Certificate Hierarchy

Device > Certificate Management > Certificates

Device Certificates | Default Trusted Certificate Authorities

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

Decryption concepts

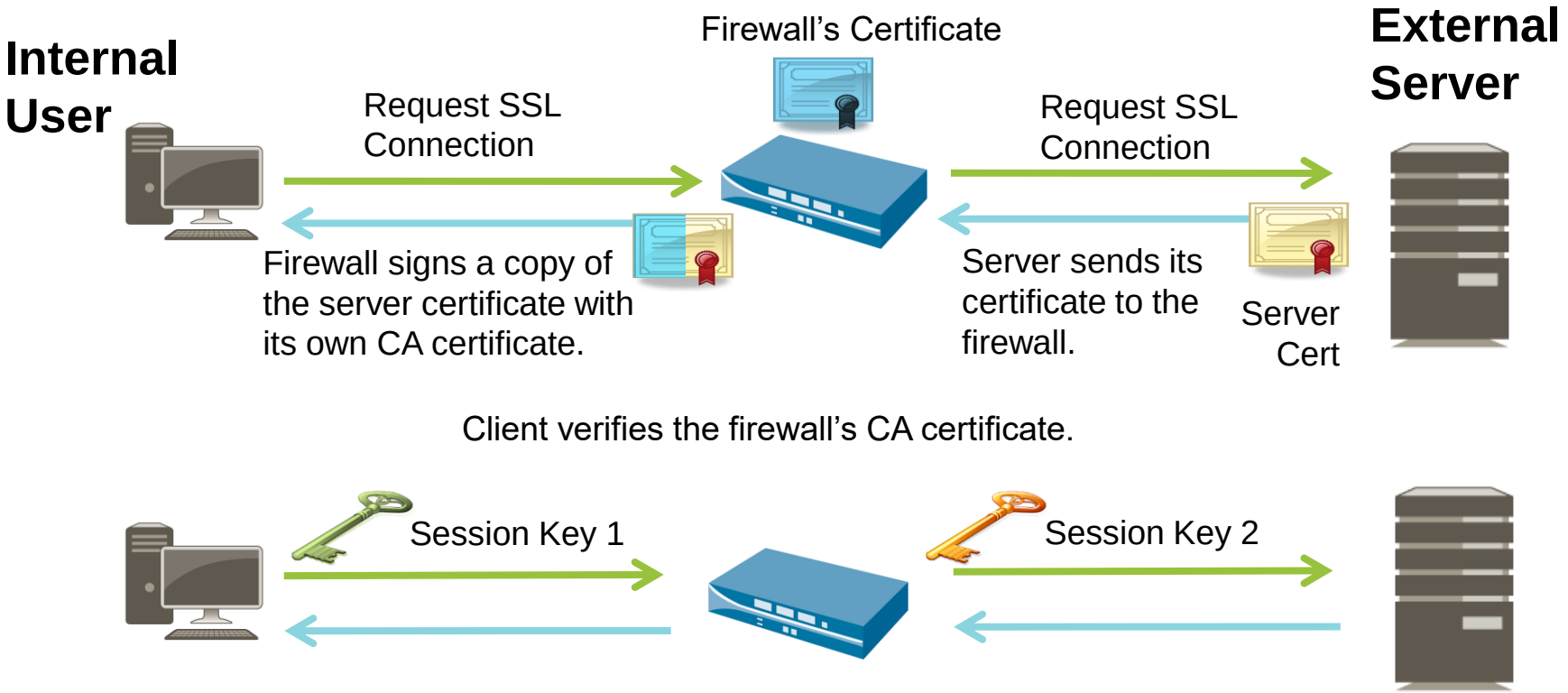
Certificate management

SSL forward proxy decryption

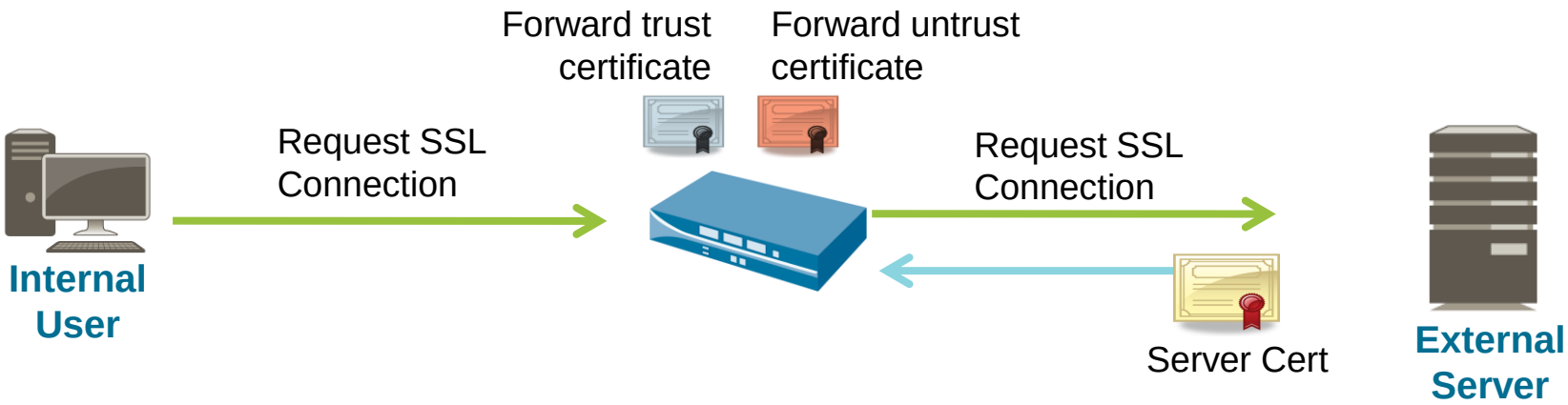
SSL inbound inspection

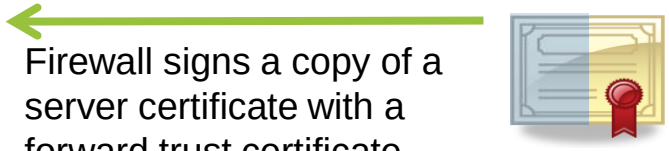
Other decryption topics

Forward Proxy Decryption

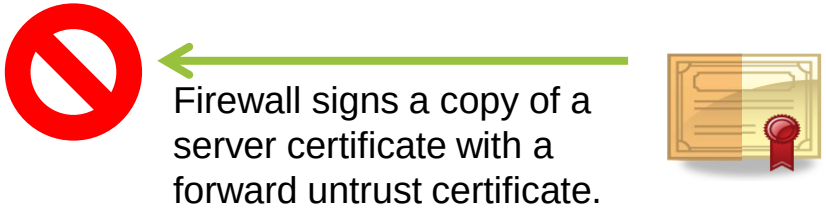


Forward Trust and Forward Untrust Certificates





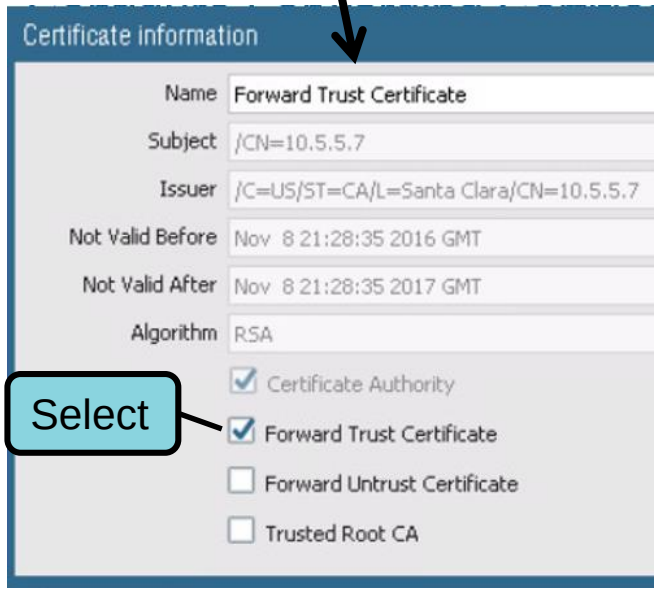
If server certificate is trusted



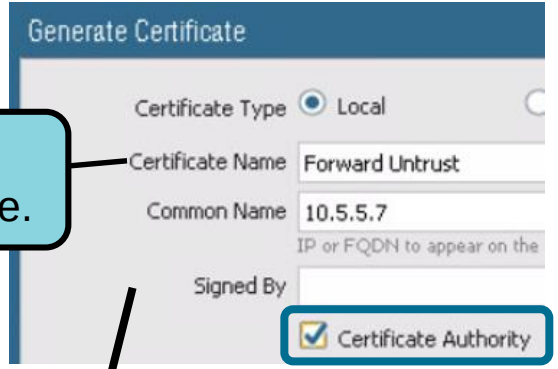
If server certificate is untrusted

Configure Forwarding Certificates

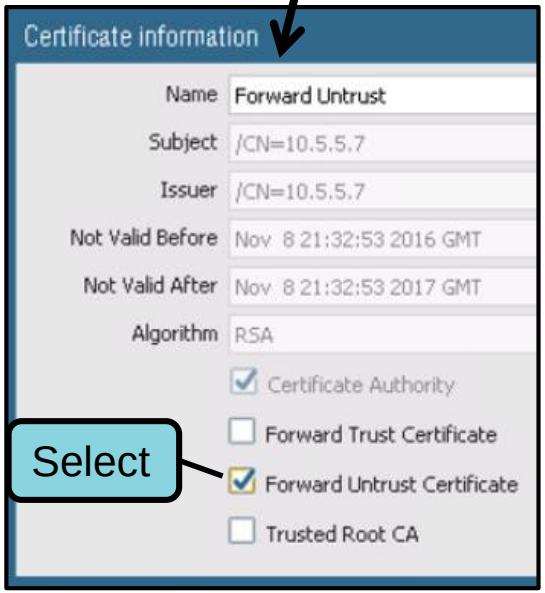
Trusted by SSL clients



Select



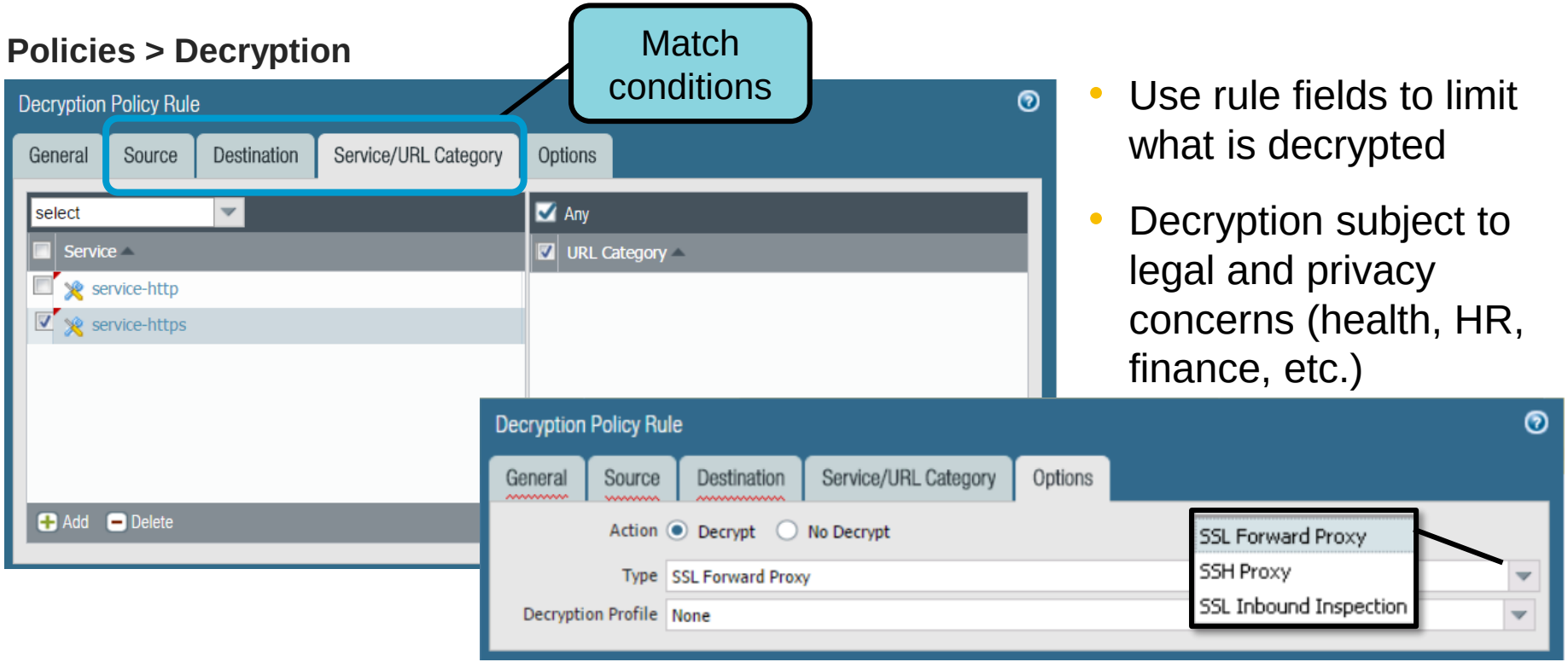
Create a self-signed certificate.



Select

Configure SSL Forward Proxy Policy

Policies > Decryption



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

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

Unsupported Mode Checks
- [x] Block sessions with unsupported versions
- [x] Block sessions with unsupported cipher suites
- [x] Block sessions with client authentication

Failure Checks
- [x] Block sessions if resources not available
- [x] 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

- [x] RSA
- [x] DHE
- [x] ECDHE

Encryption Algorithms

- [x] 3DES
- [x] AES128-CBC
- [x] AES128-GCM
- [x] RC4
- [x] AES256-CBC
- [x] AES256-GCM

Authentication Algorithms

- [ ] MD5
- [x] SHA1
- [x] SHA256
- [x] 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.

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

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.

Decryption concepts

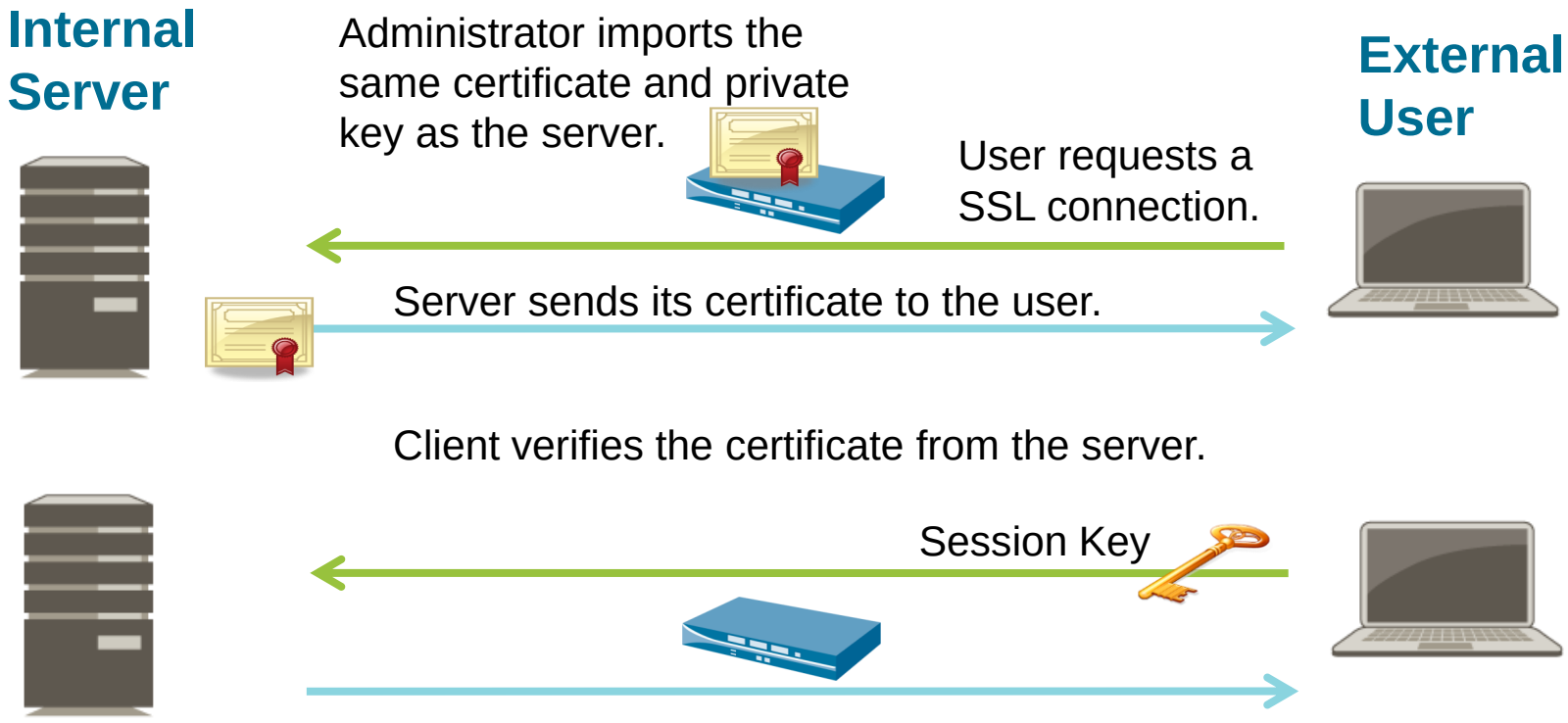
Certificate management

SSL forward proxy decryption

SSL inbound inspection

Other decryption topics

SSL Inbound Inspection

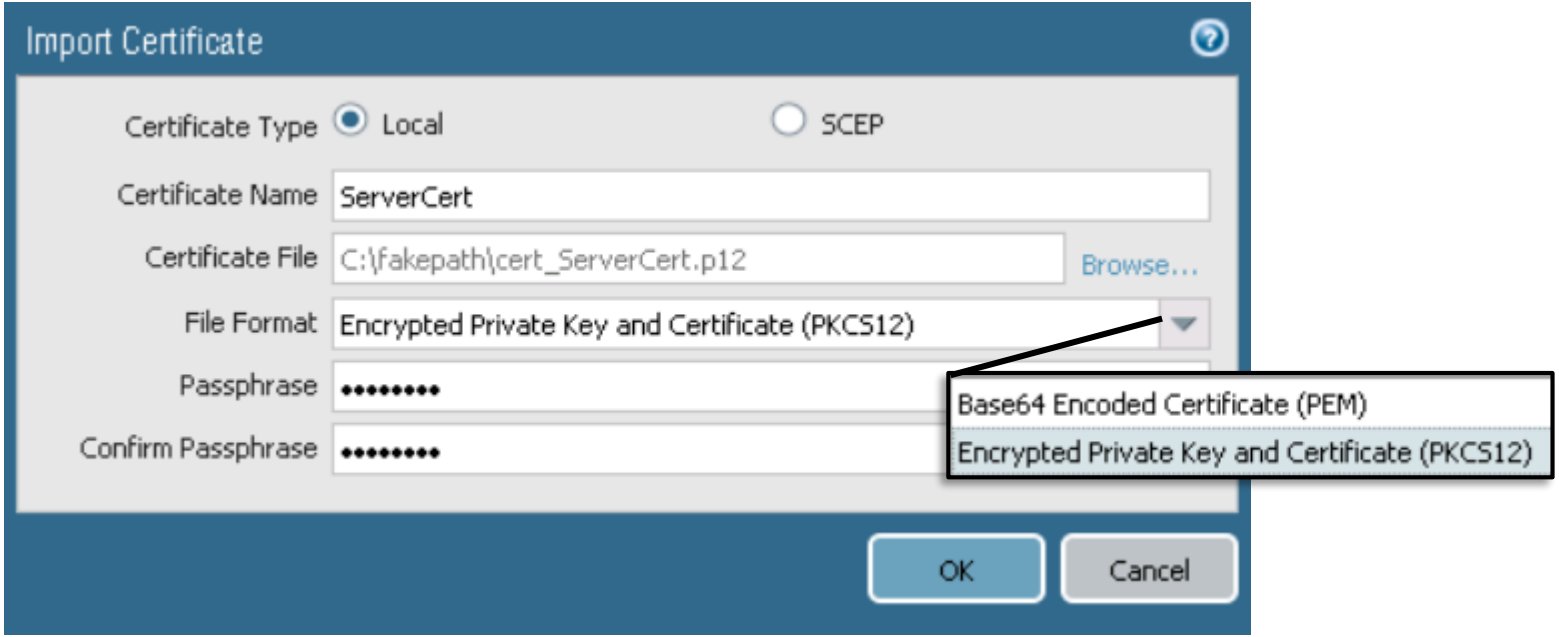


The packet data remains unchanged and the connection is secure from the client system to the internal SSL server.

Import Server Certificate and Private Key

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

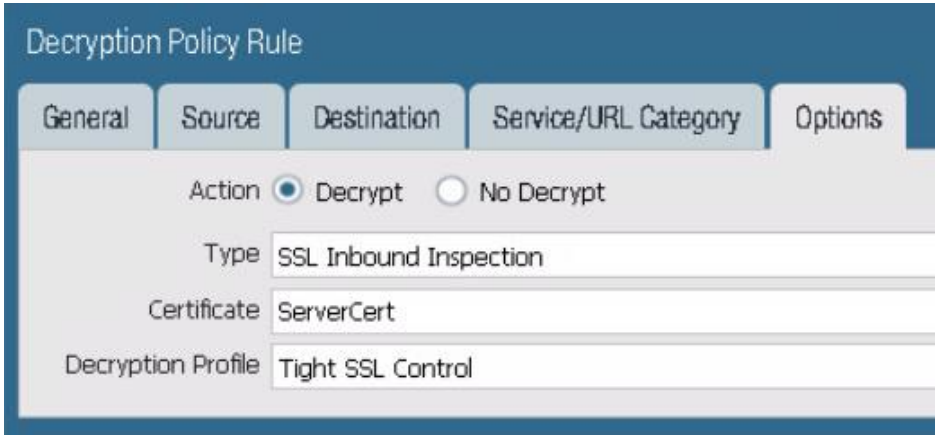
Device > Certificate Management > Certificates > Import



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 concepts

Certificate management

SSL forward proxy decryption

SSL inbound inspection

Other decryption topics

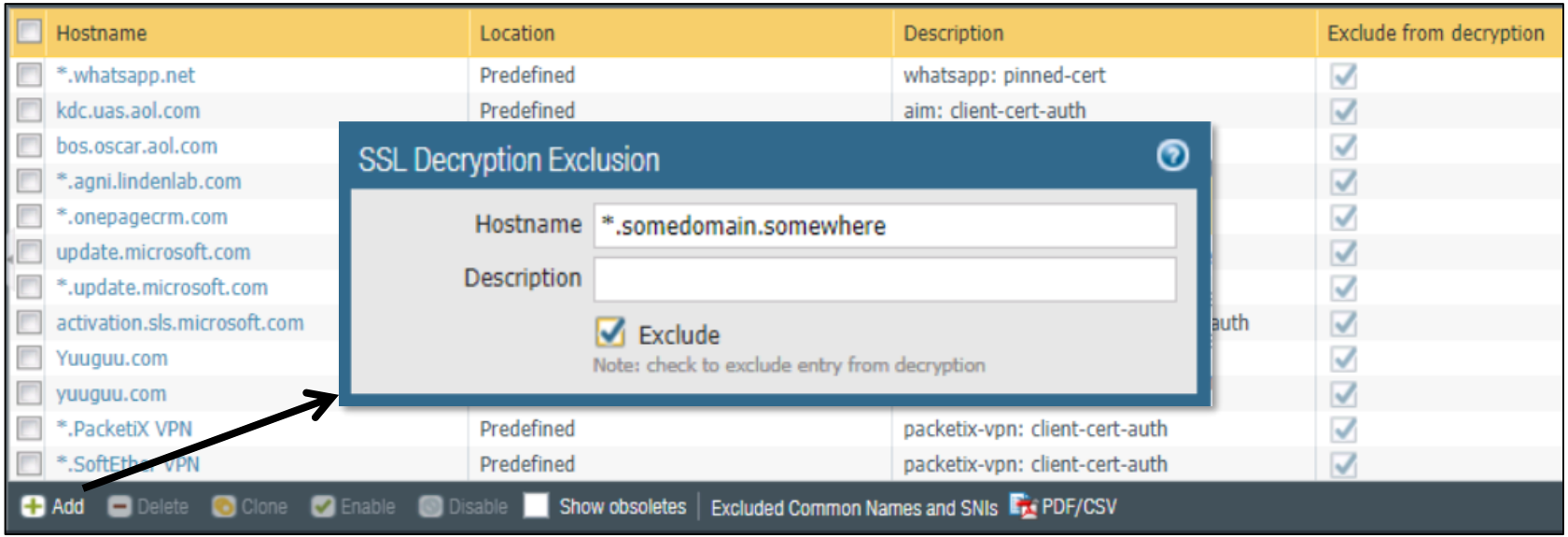
Unsupported Applications

- 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
```


Decryption Exclusions

Device > Certificate Management > SSL Decryption Exclusion



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

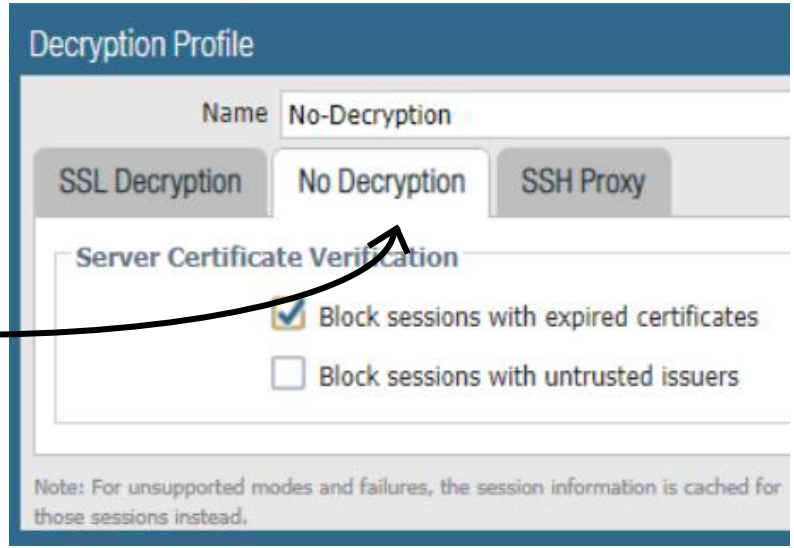
No Decryption

- 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

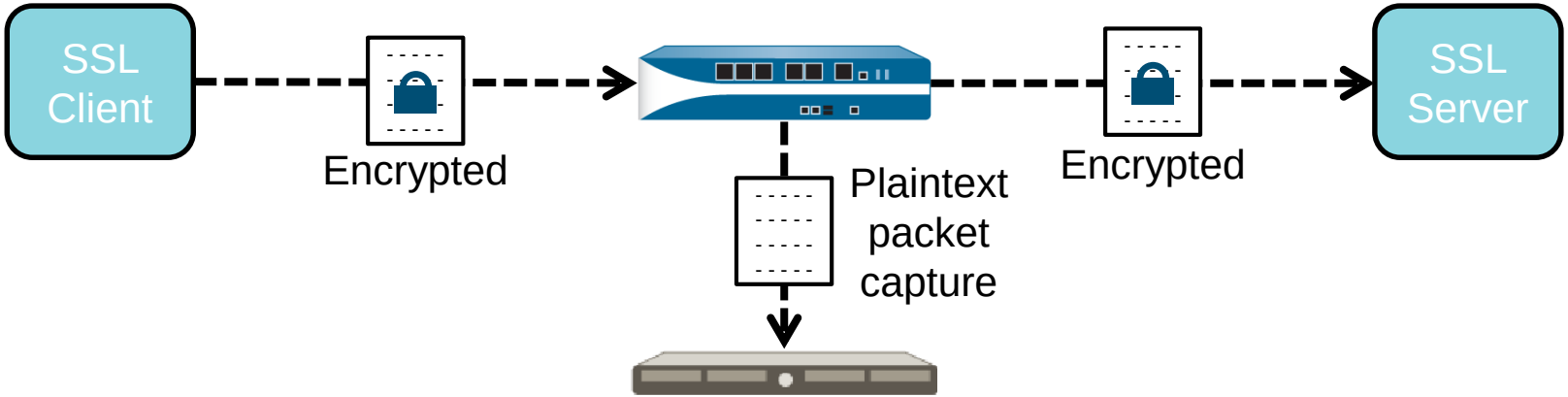
ervice	Action	Type
ıy	no-decrypt	ssl-forwar
ıy	no-decrypt	ssl-forwar

Objects > Decryption > Decryption Profile > Add



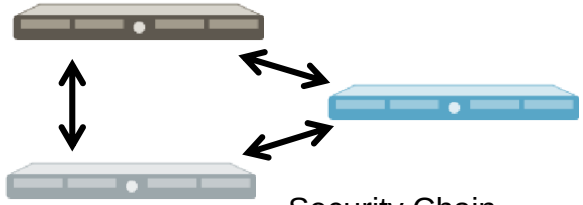
Decryption Port Mirroring

- 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



Decryption Broker

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



Security Chain

The security chain returns allowed traffic to the firewall.

Untrusted Zone/Internet

Firewall

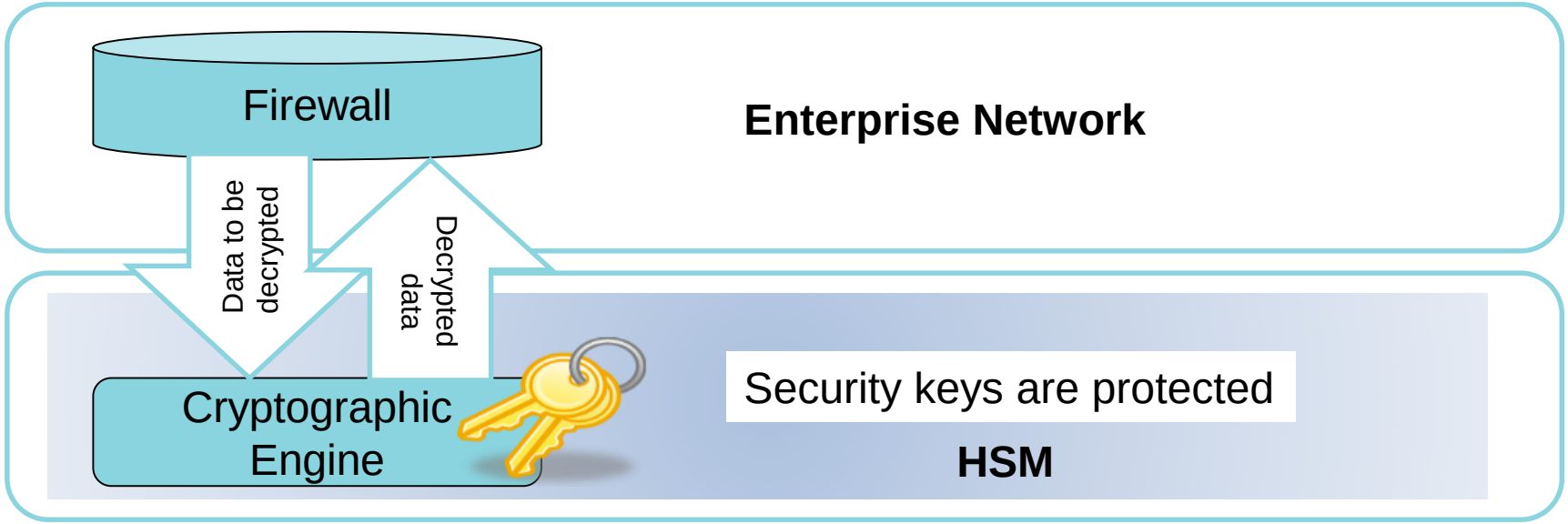
- Performs a policy check
- Decrypts SSL traffic
- Inspects and enforces cleartext traffic
- Forwards allowed cleartext traffic to the security chain

Trusted Zone/Users

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

Hardware Security Modules (HSMs)

- Cryptographic devices designed to safeguard security keys



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	e									cp-fin
		02/22 00:30:32	yes	e									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...							

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		
Negate	Time Generated		N/A

Add Close

Session end log entries

Filter log for SSL-related 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

Questions?

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.

paloalto NETWORKS®