SE Boot Camp – Decryption

SE Boot Camp

PAN-OS 8.0

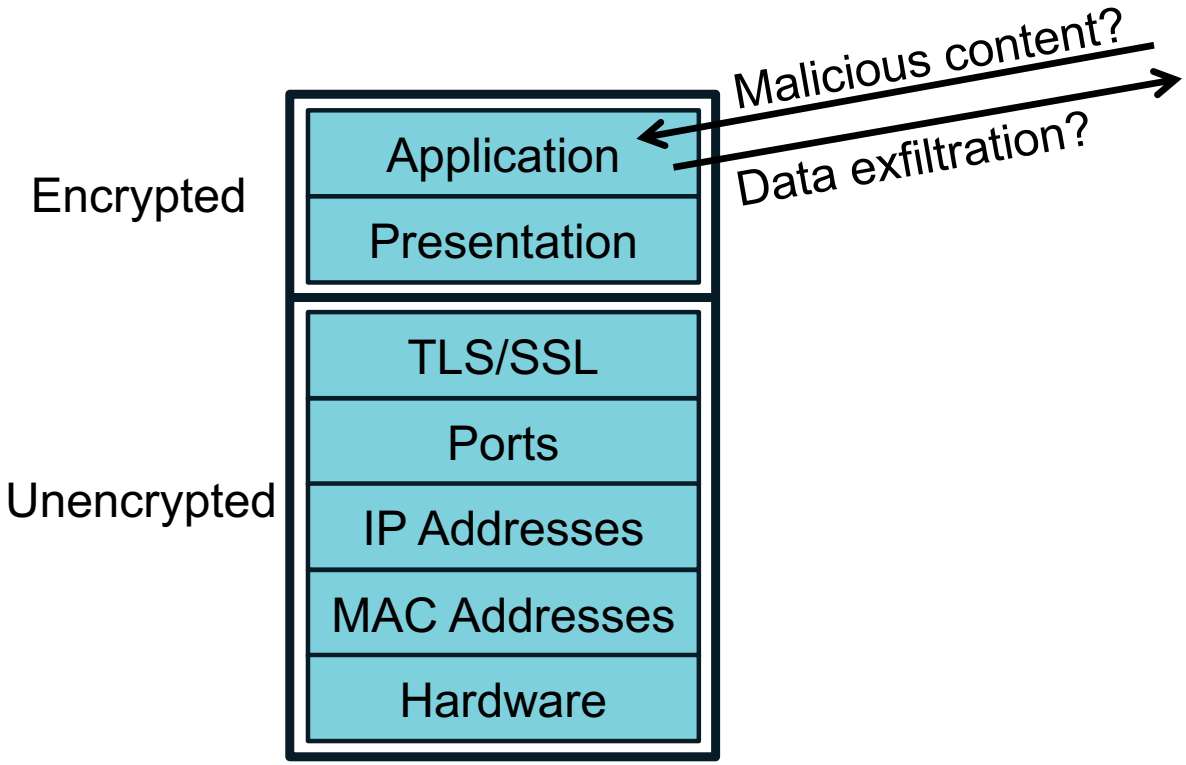
Agenda

- Decryption concepts
- Certificate management
- SSL Forward Proxy decryption
- SSL Inbound Inspection
- Other decryption topics:
  - Unsupported applications
  - No decryption
  - Decryption port mirroring
  - Hardware security modules
  - Troubleshooting SSL session terminations

Decryption Concepts

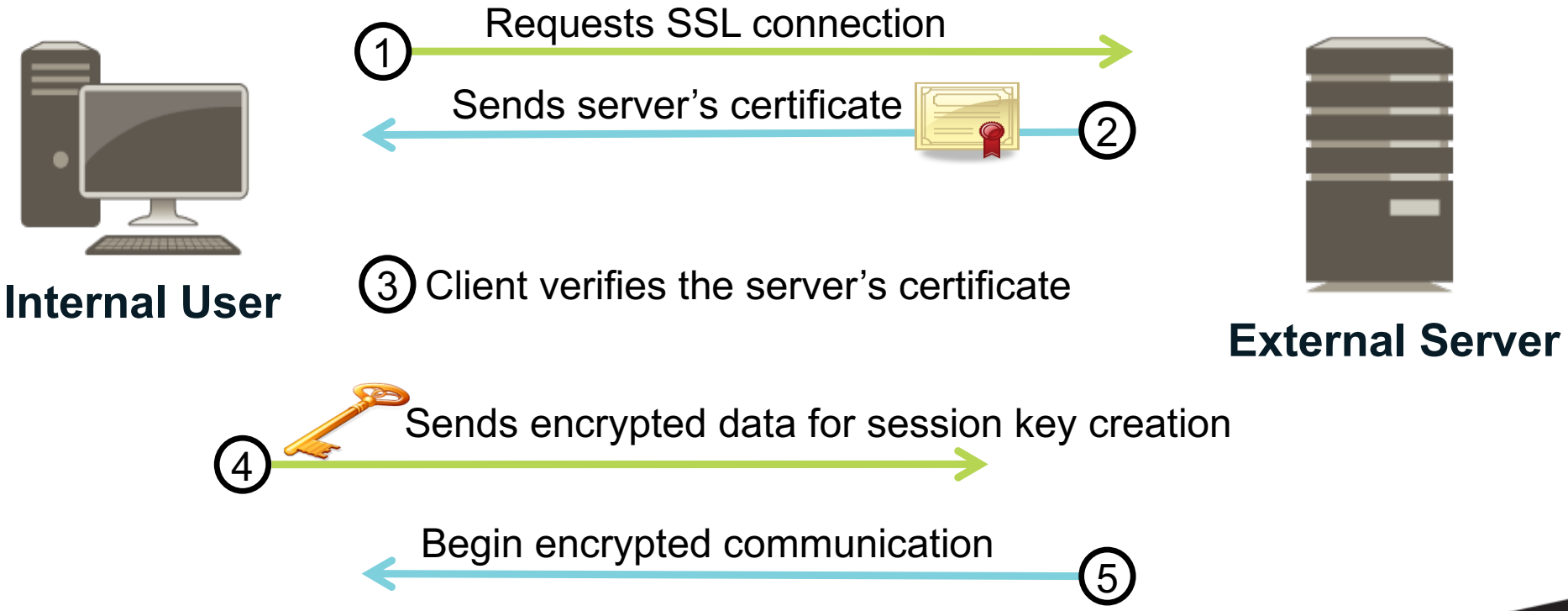
Why Decrypt Network Traffic?

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



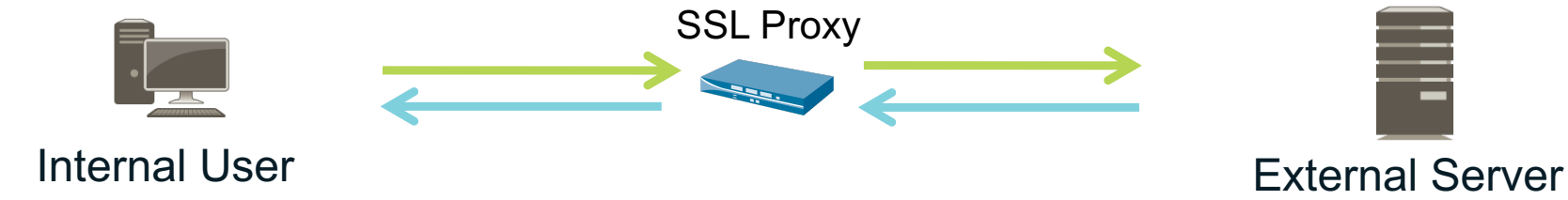
SSL/TLS Session Overview

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

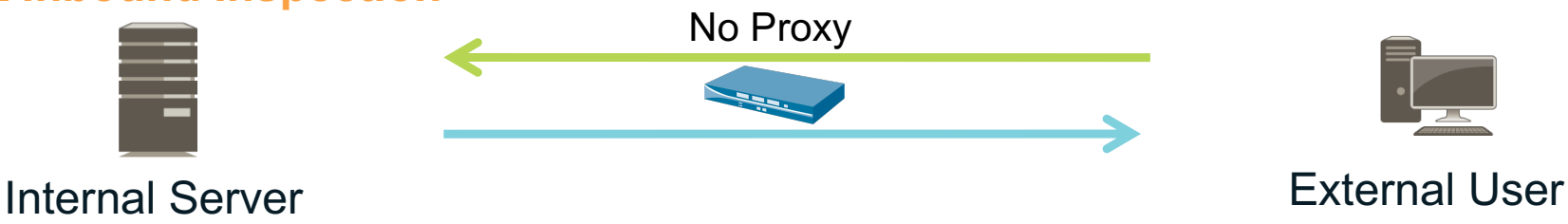


Firewall Decryption Types

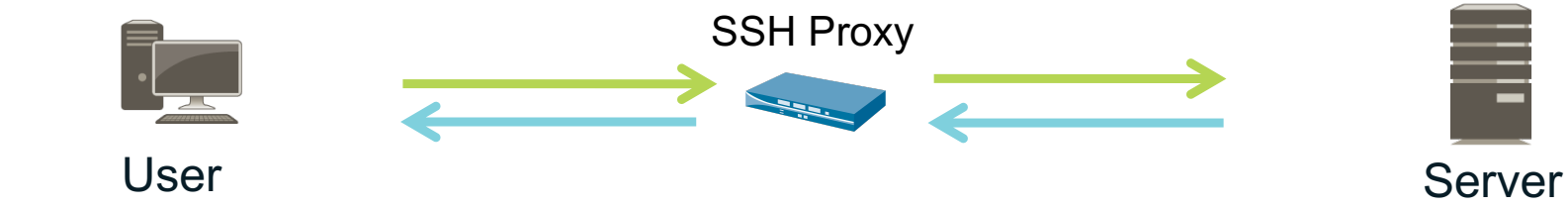
SSL Forward Proxy (Outbound)



SSL Inbound Inspection

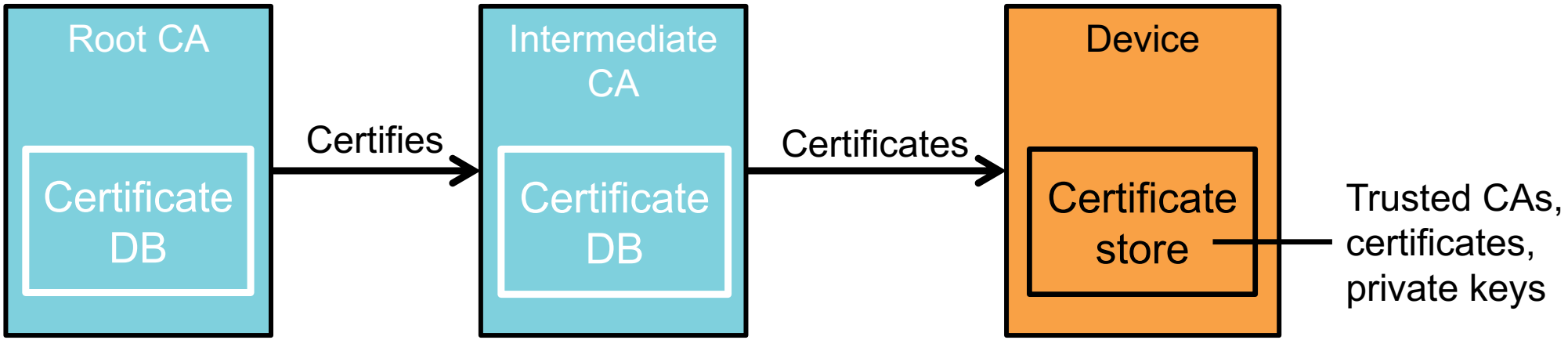


SSH Decryption

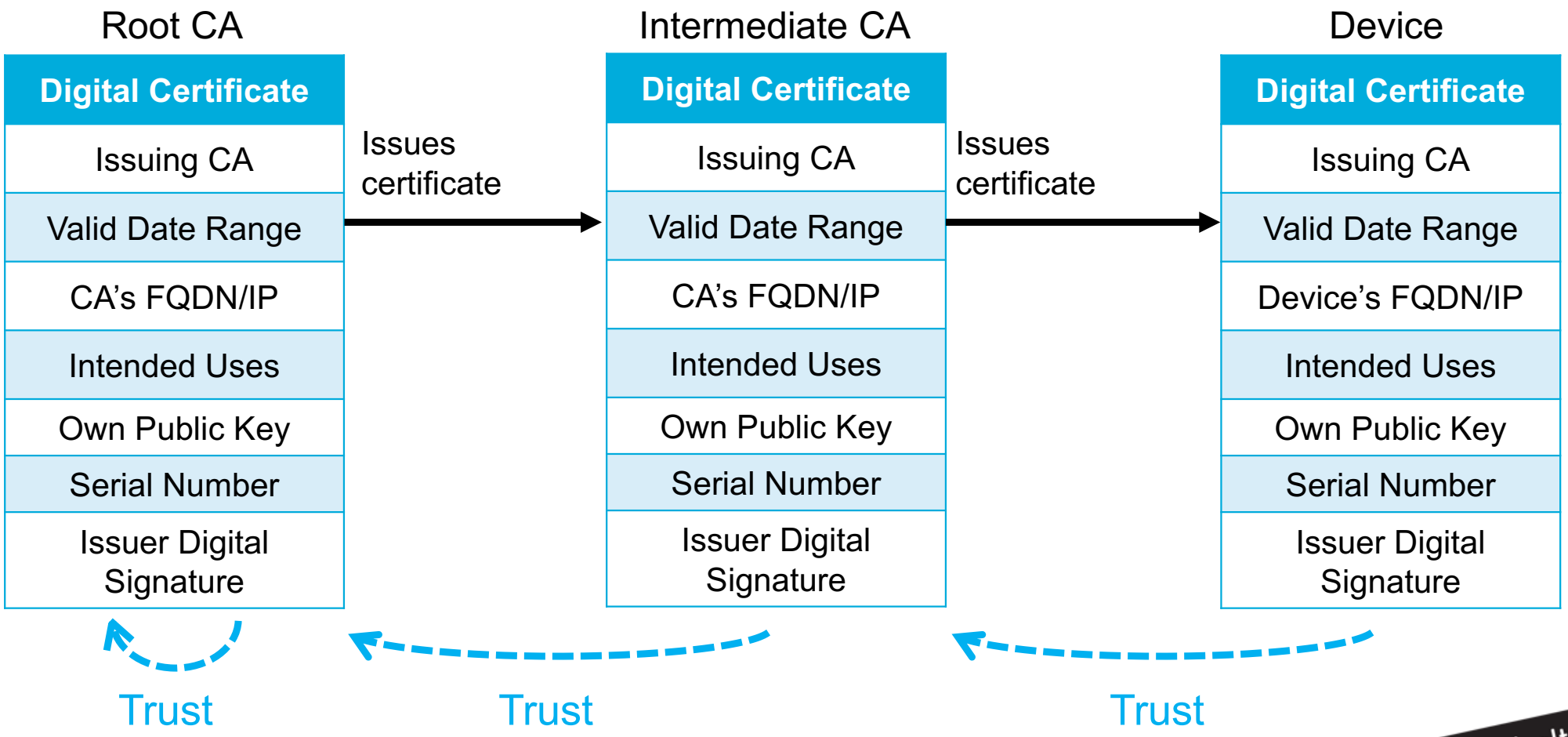


Public Key Infrastructure (PKI)

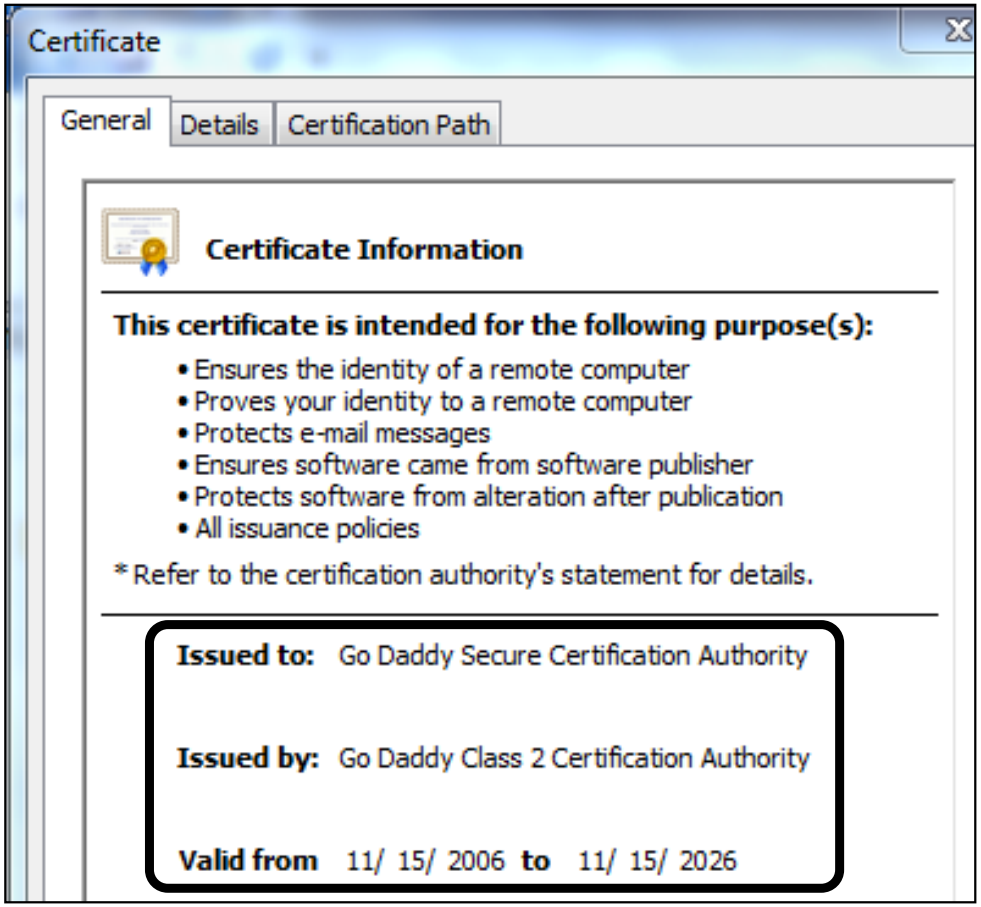
- Solves the problem of secure identification of public keys
- Uses digital certificates to verify public key owners
- Typical PKI components:

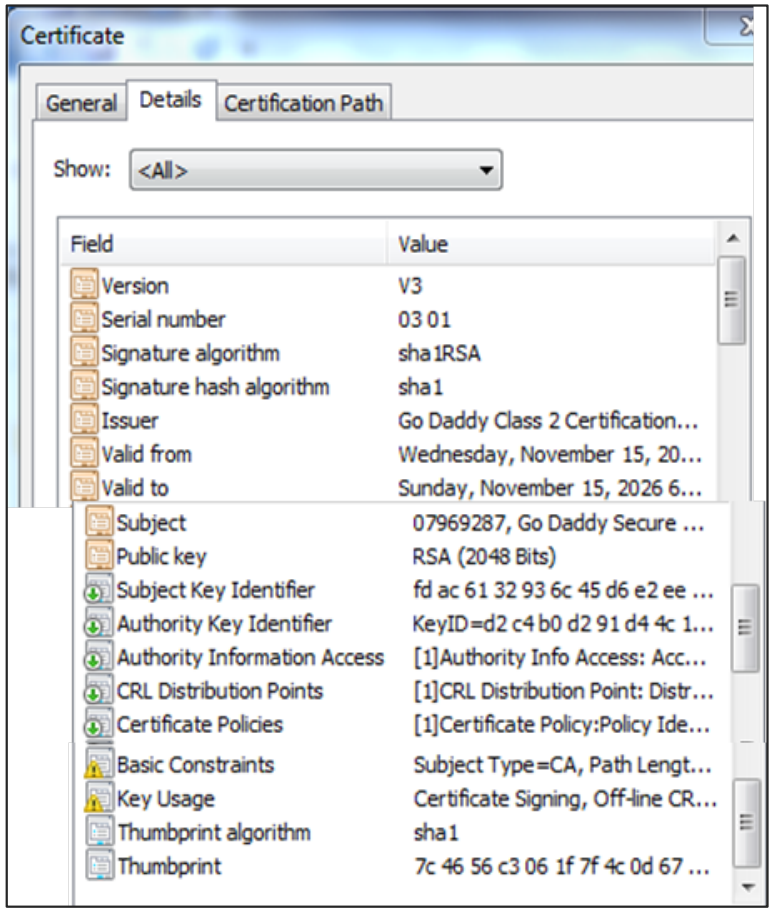


Certificate Chain of Trust



Certificate Example



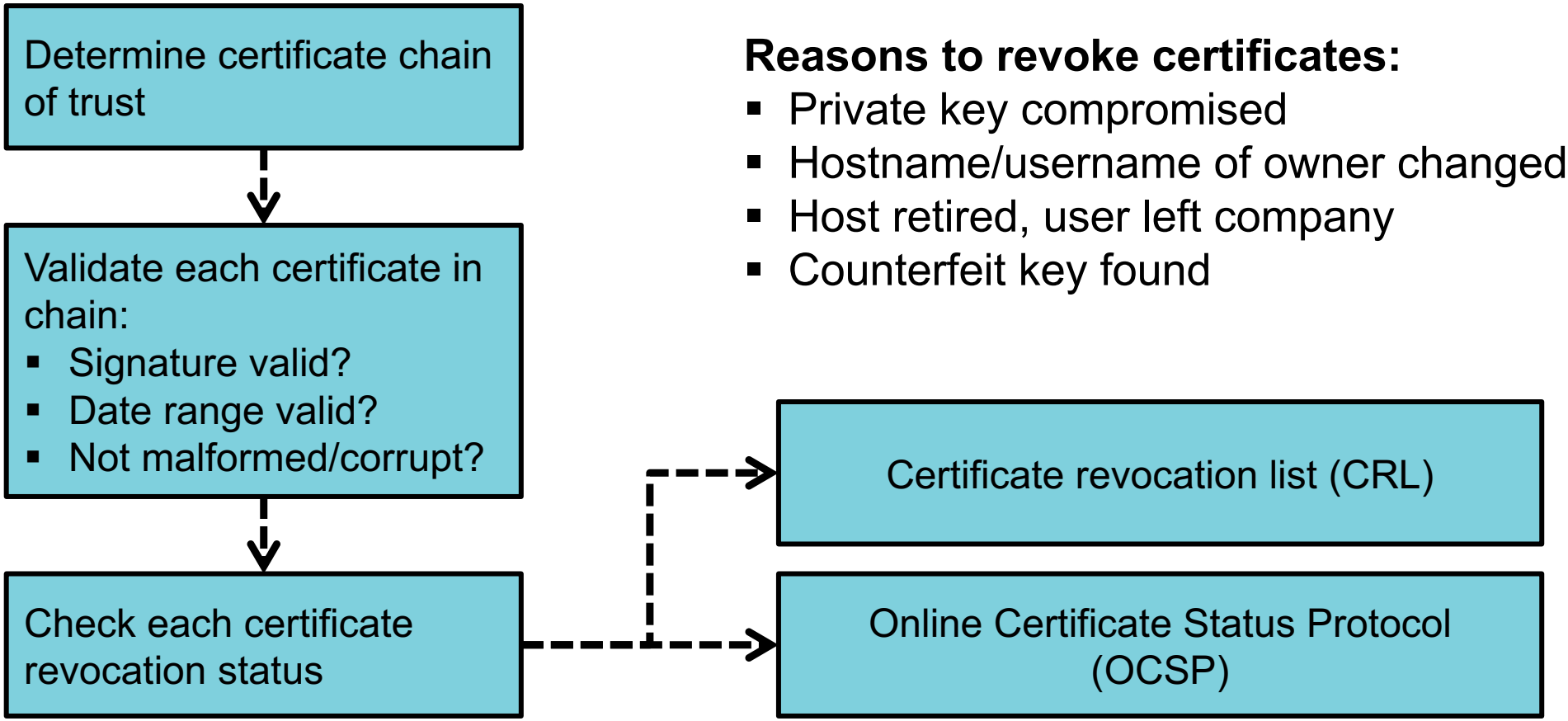


Firewall Features Using Certificates

- 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

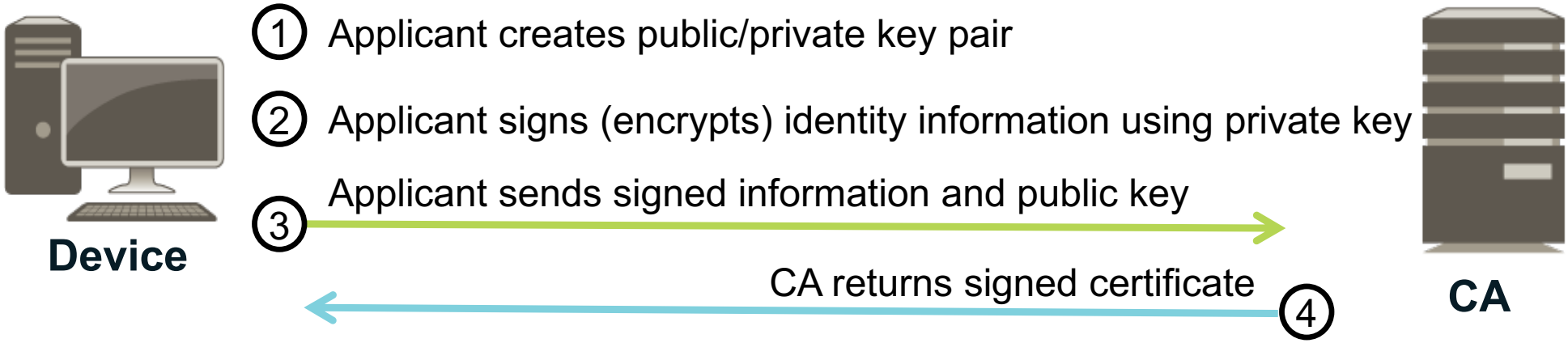


Reasons to revoke certificates:

- Private key compromised
- Hostname/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

Certificate Management

Certificate Management in the WebUI

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	✓	✓	Nov 8 20:56:03 2017 GMT	valid	RSA

Delete Revoke Renew Import Generate Export Import HA Key Export HA Key

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	Nov 8 20:56:03 2016 GMT
Not Valid After	Nov 8 20:56:03 2017 GMT
Algorithm	RSA

- [x] Certificate Authority
- [ ] Forward Trust Certificate
- [ ] Forward Untrust Certificate
- [ ] Trusted Root CA

Types of operations:

- Generate certificates
- View certificates
- Modify certificate use
- Import/export certificates
- Delete certificates
- Revoke certificates

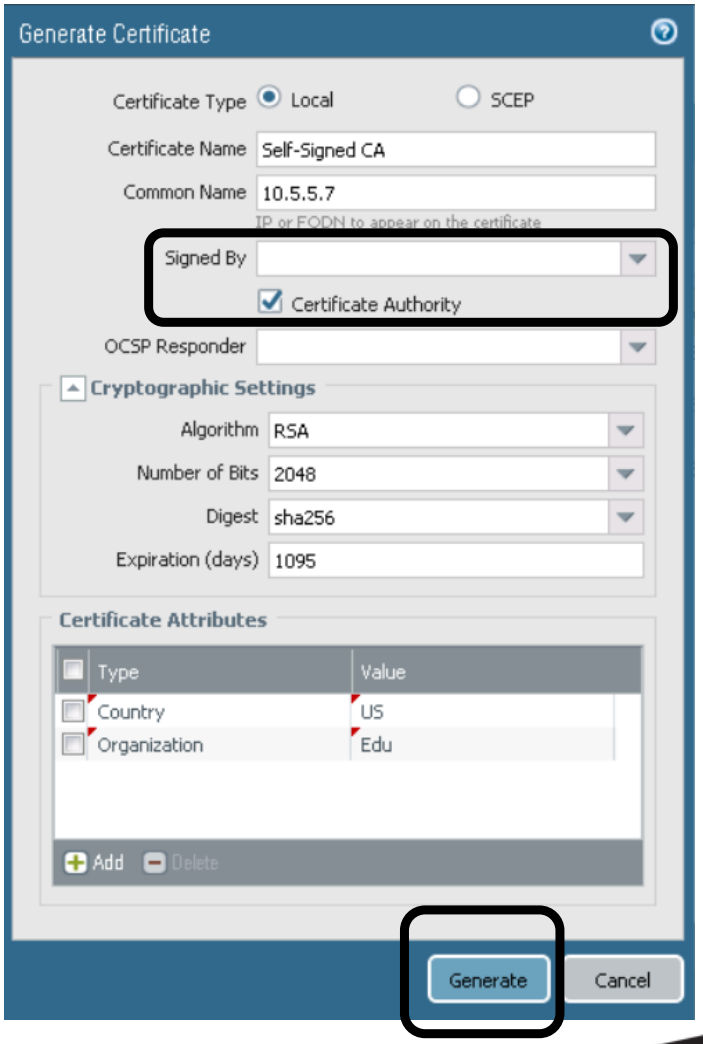
Firewall CA Certificate Deployment Choices

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

Generate Self-Signed CA Certificate

Method 1:

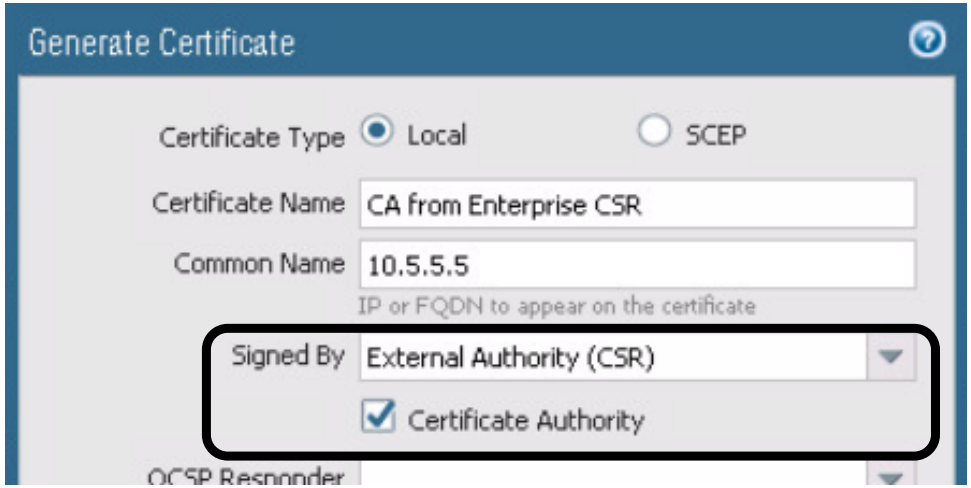
- Create a self-signed firewall CA certificate:
  - Use **Device > Certificate Management > Certificates > Generate**
- Fill out the form and click **Generate**
- Creates a self-signed CA certificate
- Creates public/private keys

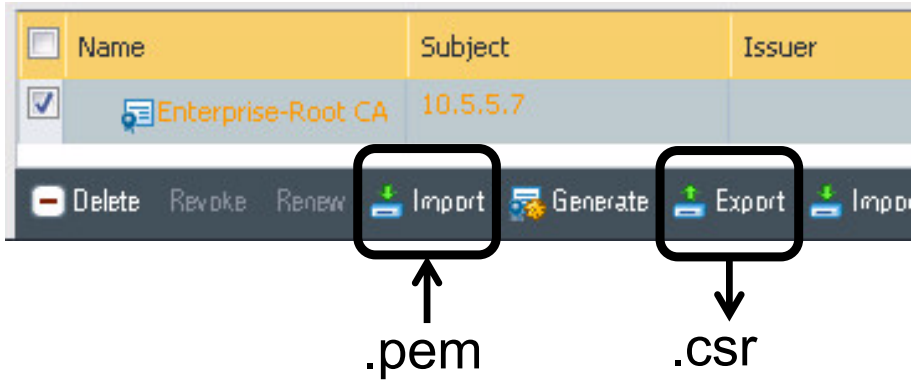


Generate CA Certificate Using CSR

Method 2:

- Generate a firewall CA certificate to be signed by an internal CA:
  - Use **Device > Certificate Management > Certificates > Generate**
  - Fill out the form and click **Generate**
- **Export** public/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

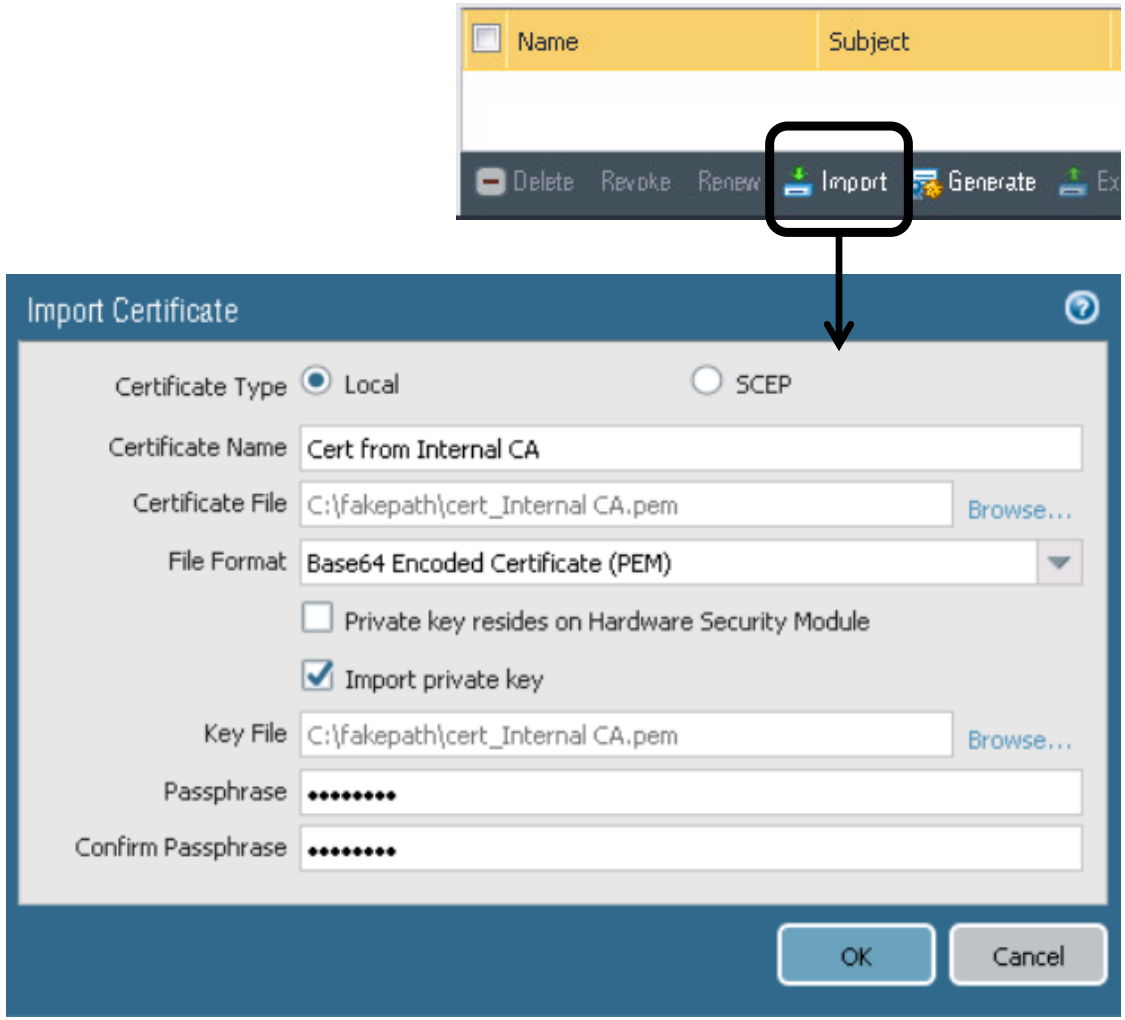




Import CA Certificate

Method 3:

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



Certificate Hierarchy

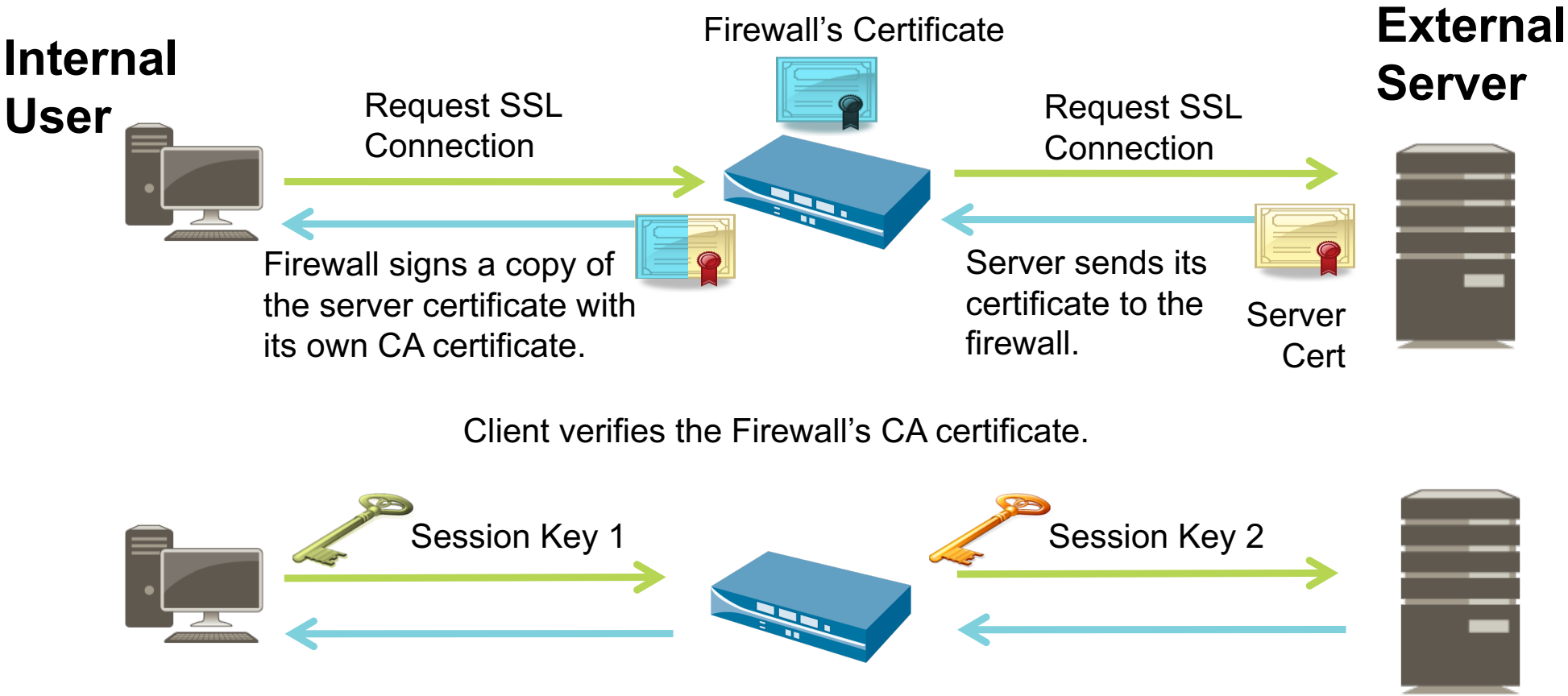
Device > Certificate Management > Certificates

Device Certificates | Default Trusted Certificate Authorities

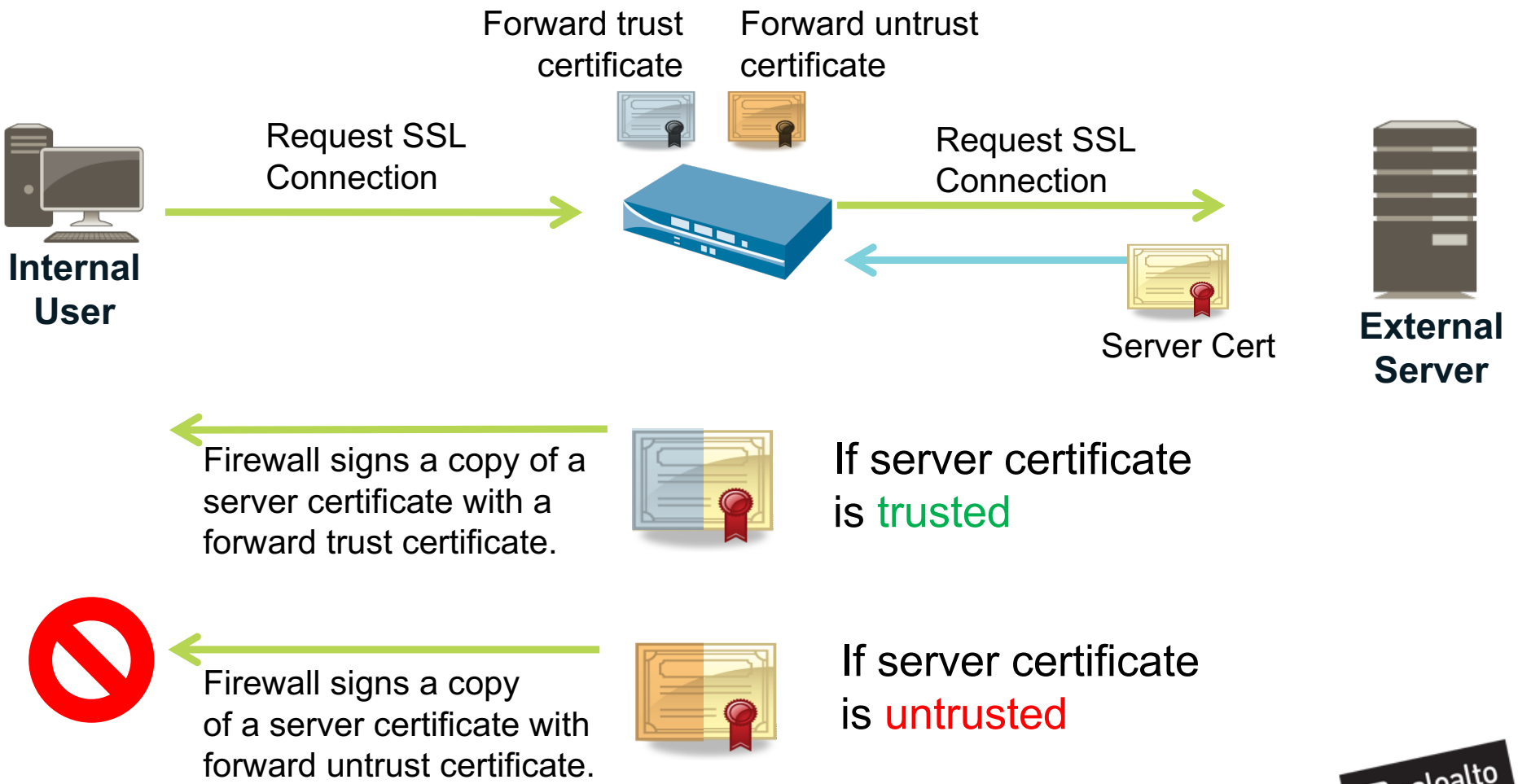
Name	Subject	Issuer	CA	Key	Expires	Status
Student-11-Cert	CN = 172.16.11.1	CN = 172.16.11.1	✓	✓	Sep 20 21:12:57 2016 GMT	valid
FTCert	C = US, CN = 172.16.11.1	CN = 172.16.11.1		✓	Oct 21 23:30:59 2016 GMT	valid
NetwCA	CN = NetCA.com	CN = NetCA.com	✓	✓	Dec 13 23:55:59 2016 GMT	valid
NetDefaultCA	CN = NetwCA.com	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

SSL Forward Proxy Decryption

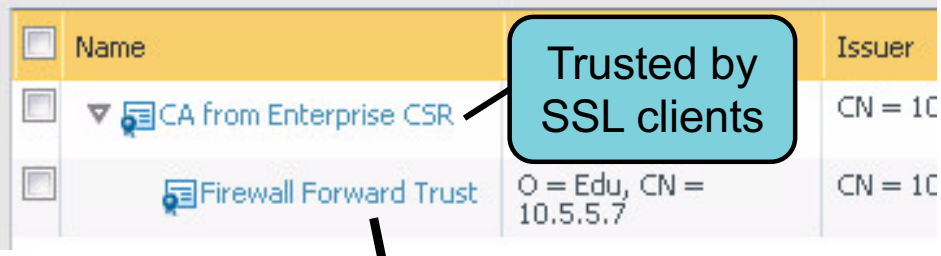
Forward Proxy Decryption



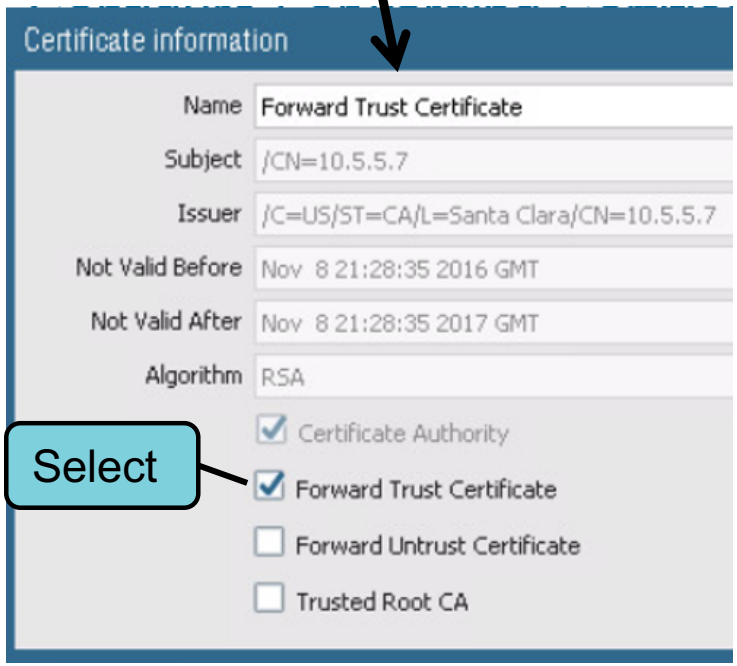
Forward Trust and Forward Untrust Certificates



Configure Forwarding Certificates

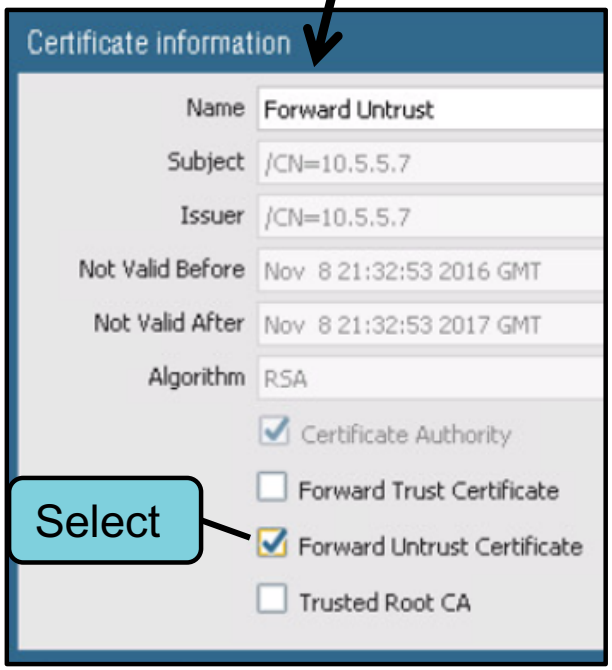


Trusted by SSL clients



Select

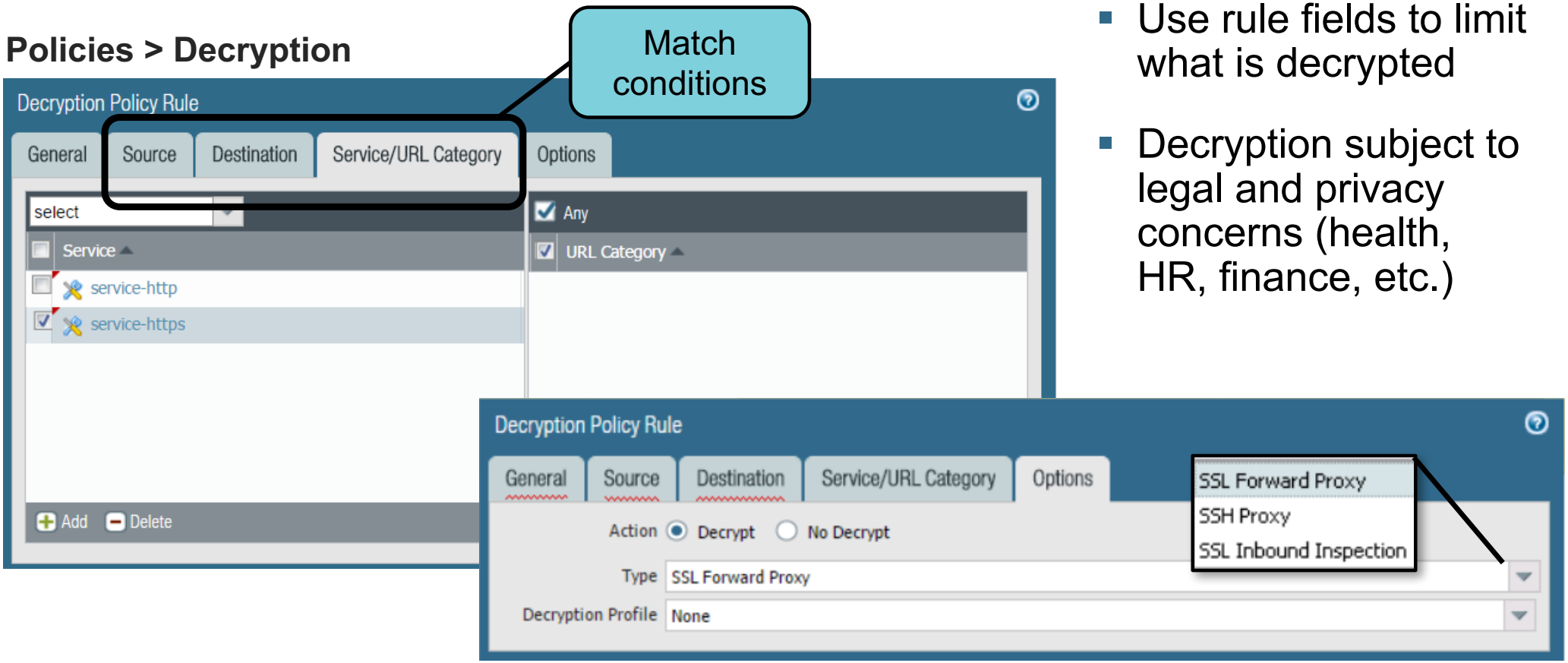
Create self-signed certificate



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 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

Unsupported Mode Checks

- ☑ Block sessions with unsupported versions
- ☑ Block sessions with unsupported cipher su
- ☑ Block sessions with client authentication

Failure Checks

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

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. Chec those sessions instead.

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.

Create the Security Policy Rules

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

Policies > Security

	Source			Destination				
Name	Zone	Address	User	Zone	Address	Application	Service	Action
Allow Web-SSL Traffic	Trust-L3	any	any	Untrust-L3	any	web-browsing	service-http service-https	Allow
Allow SSL Traffic	Trust-L3	any	any	Untrust-L3	any	ssl	application-default	Allow

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

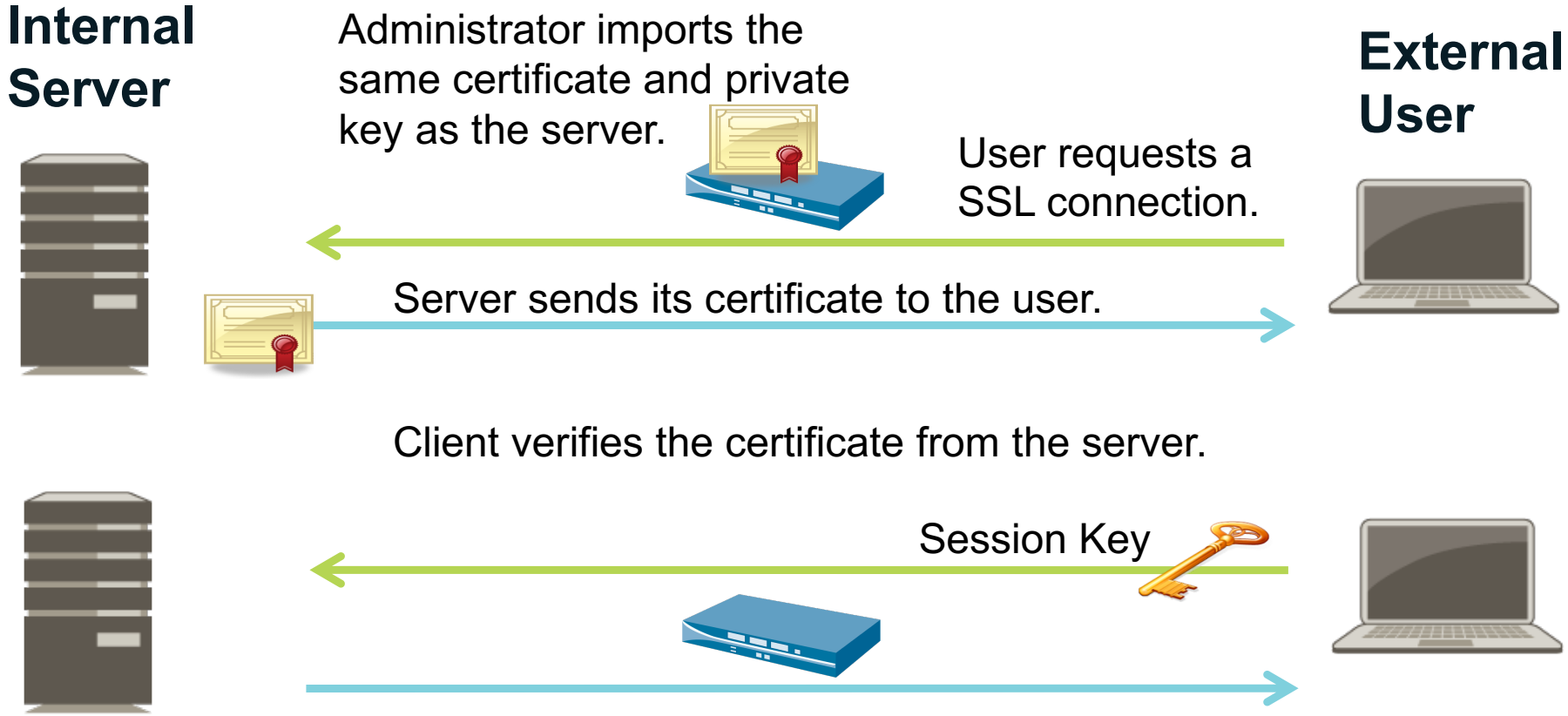
Policies > Decryption

		Source			Destination						
	Name	Zone	Address	User	Zone	Address	URL Category	Service	Action	Type	Decryption Profile
1	Dest IP Addr Bypass	Trust-L3	any	any	UnTrust-L3	203.0.113.38	any	any	no-decrypt	ssl-forward-proxy	Lenient Profile
2	Source User Exception	Trust-L3	any	User123	UnTrust-L3	any	any	any	no-decrypt	ssl-forward-proxy	Lenient Profile
3	URL Exception Bypass	Trust-L3	any	any	UnTrust-L3	any	Decrypt Bypass	any	no-decrypt	ssl-forward-proxy	Lenient Profile
4	Sensitive Category Bypass	Trust-L3	any	any	UnTrust-L3	any	financial-services government health-and-medicine military shopping	any	no-decrypt	ssl-forward-proxy	Lenient Profile
5	Decrypt All Traffic	Trust-L3	any	any	UnTrust-L3	any	any	service-https	decrypt	ssl-forward-proxy	Tight SSL Control

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

SSL Inbound Inspection

SSL Inbound Inspection

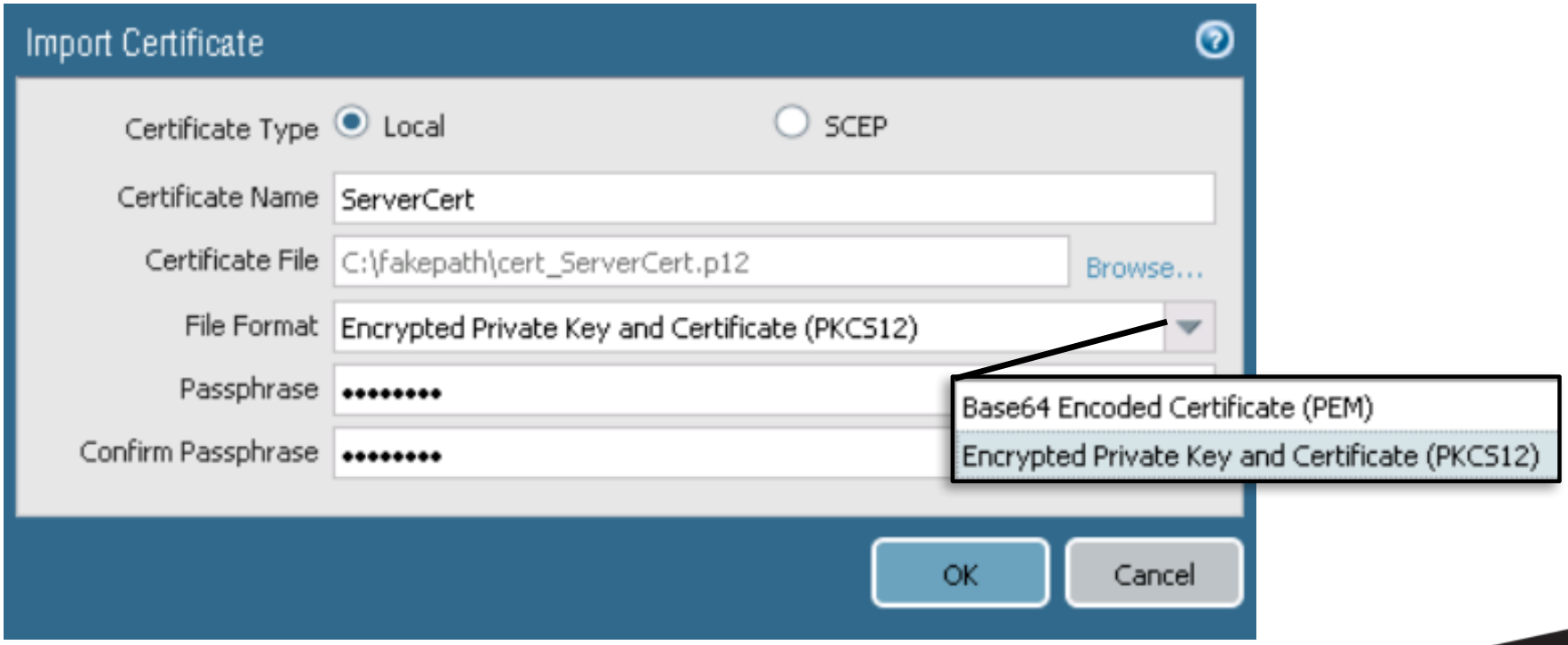


- The packet data remains unchanged and the connection is secure from the client system to the internal SSL server.

Import Server Certificate and Private Key

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

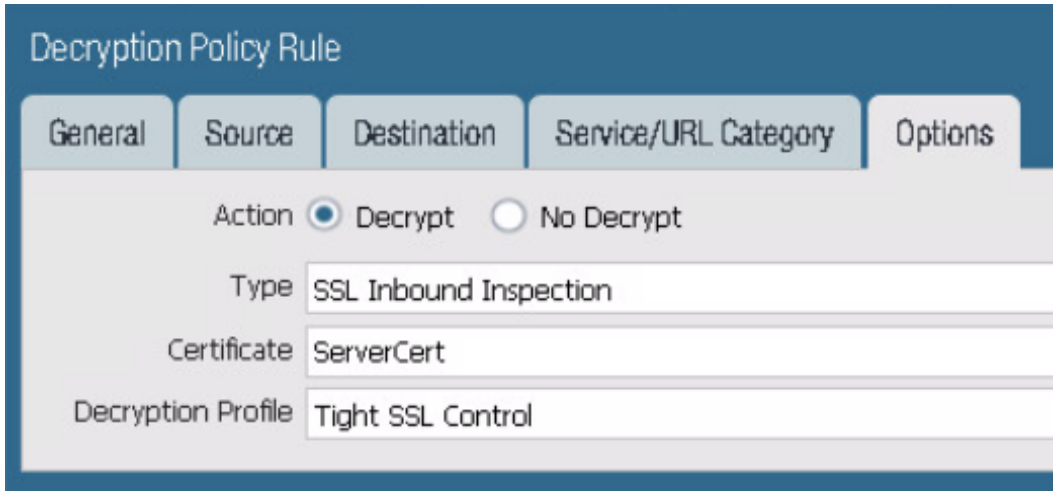
Device > Certificate Management > Certificates > Import



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



Other Decryption Topics

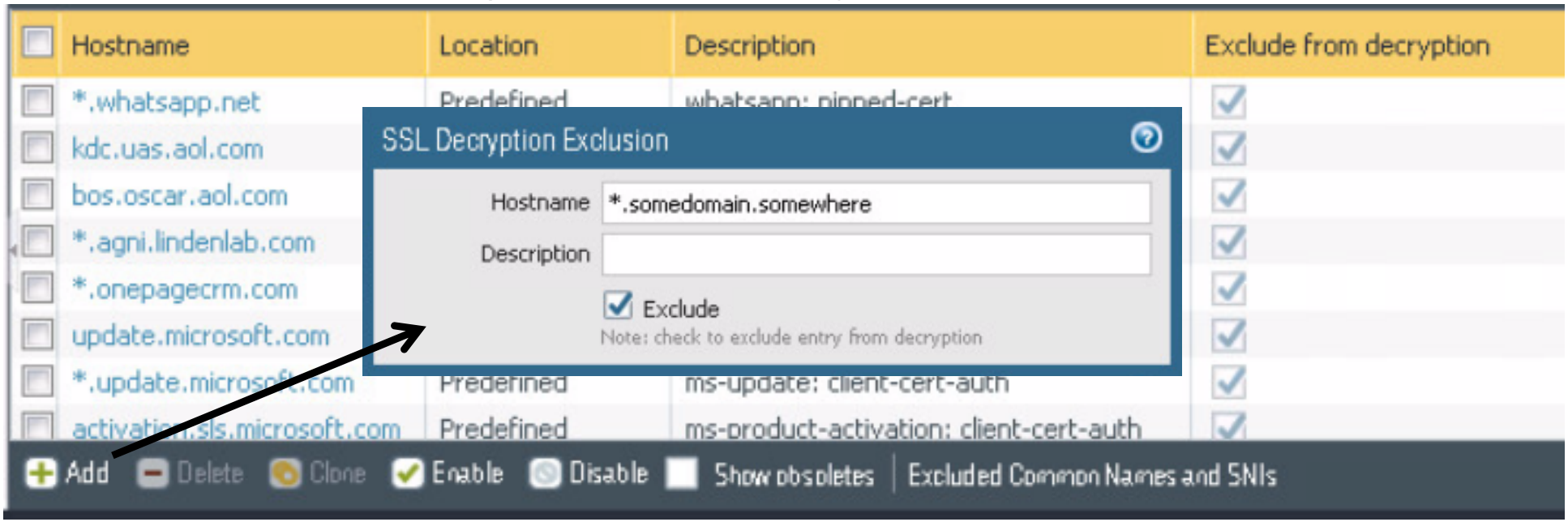
Unsupported Applications

- 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 first occurrence
- To see which websites have been added to the exclusion cache:

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


Decryption Exclusions

Device > Certificate Management > SSL Decryption Exclusion



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

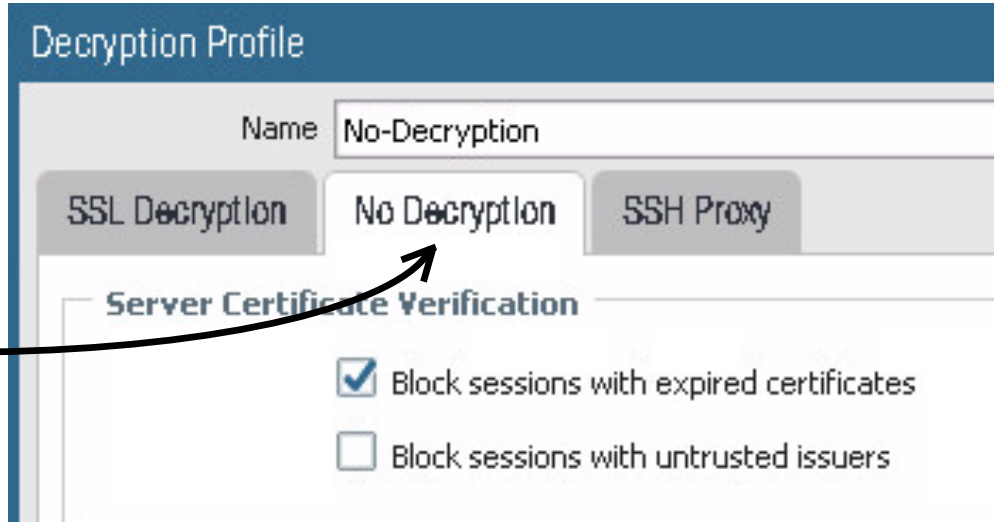
No Decryption

- 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

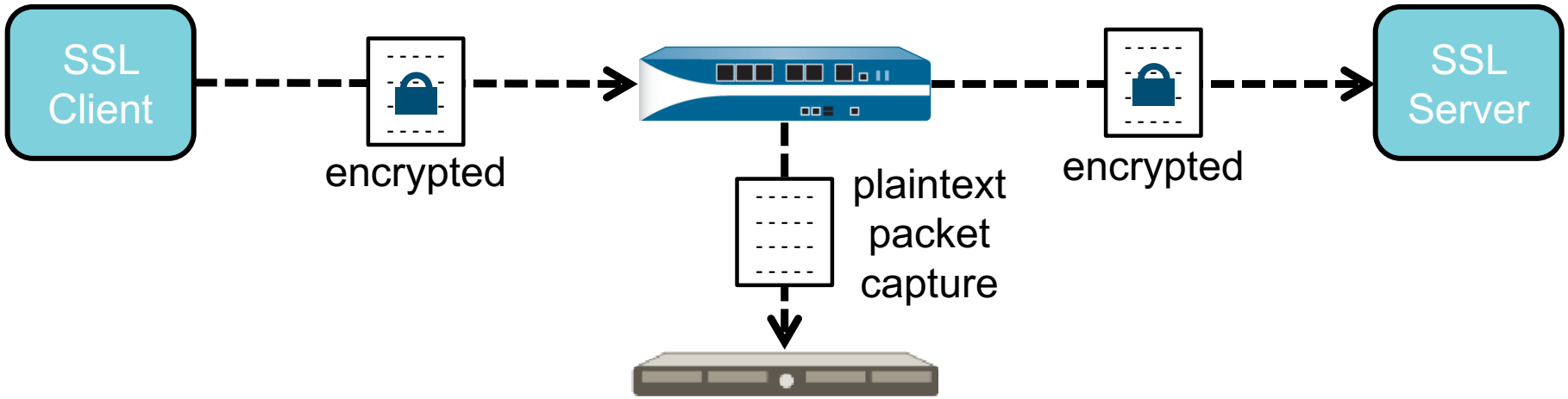
ervice	Action	Type
ıy	no-decrypt	ssl-forwar
ıy	no-decrypt	ssl-forwar

Objects > Decryption Profile > Add

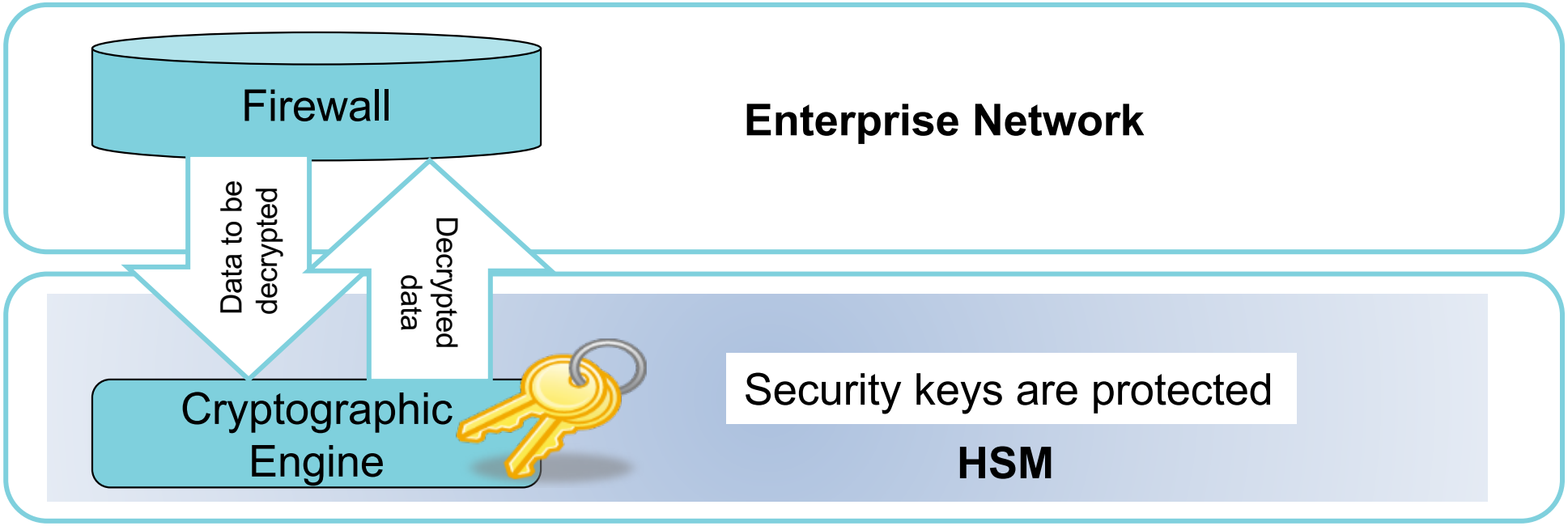


Decryption Port Mirroring

- 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



Hardware Security Modules (HSMs)



- Cryptographic devices designed to safeguard security keys

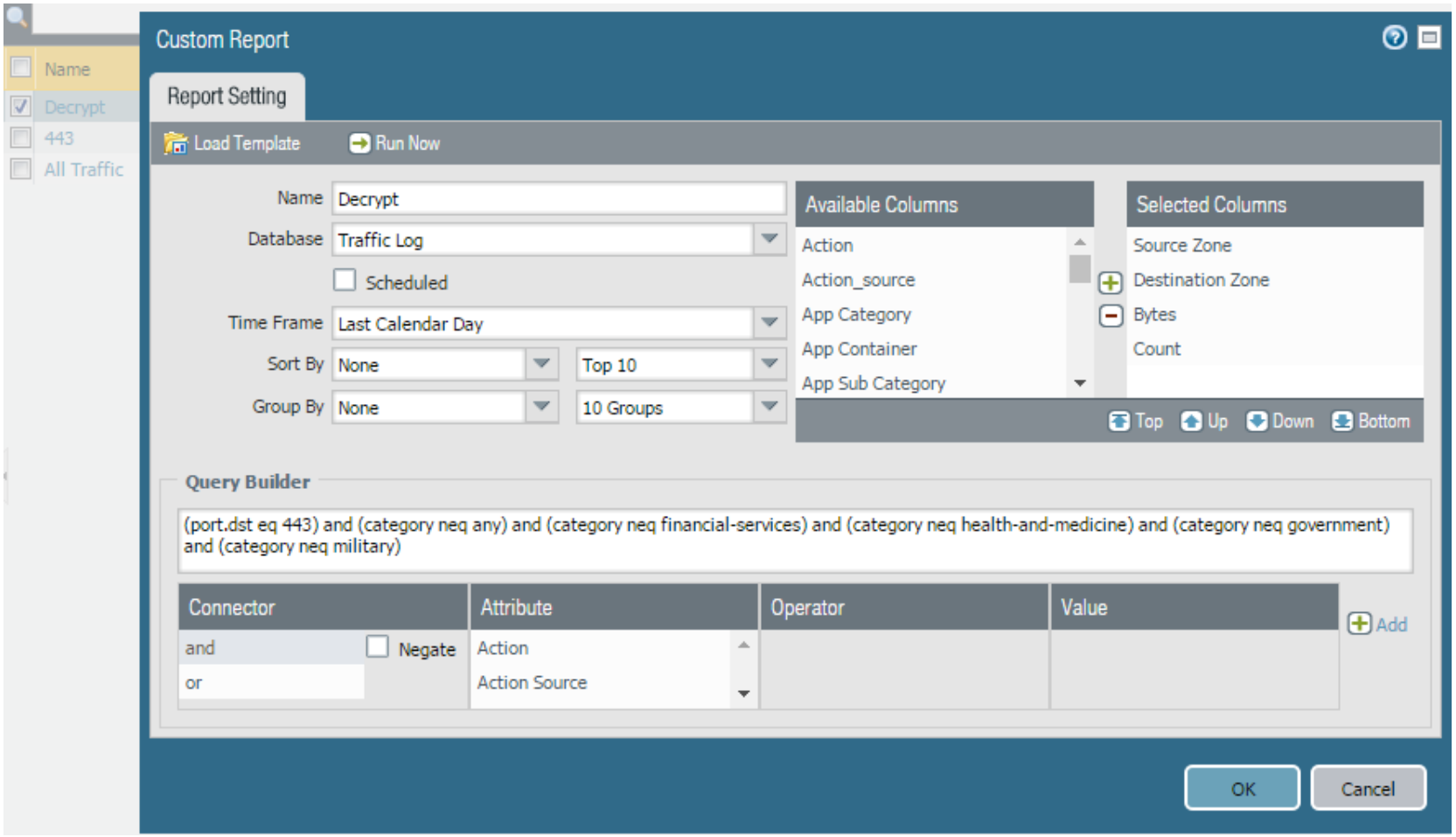
Sizing for Decryption

Calculating SSL Sizing Estimates

- **DO NOT** size based on decrypt-all performance stats!
- First: Calculate % decryption (loose approximation)
    1. Calculate bytes for categories that will be decrypted
    2. Calculate total tcp/443 bytes
    3. % decryption = (Sum of bytes for selected categories / total bytes) x 100

- Use Custom Reports to obtain this percentage.

Decryption Sizing Parameters: Custom Report



Sizing Example

Report Setting | All Traffic | 443 | Decrypt

	From Zone	To Zone	Bytes	Count
1	inside	outside	19.6G	46.6k

Report Setting | All Traffic | 443 | Decrypt

	From Zone	To Zone	Bytes	Count
1	inside	outside	545.2M	7.9k

Report Setting | All Traffic | 443 | Decrypt

	From Zone	To Zone	Bytes	Count
1	inside	outside	547.0M	8.0k

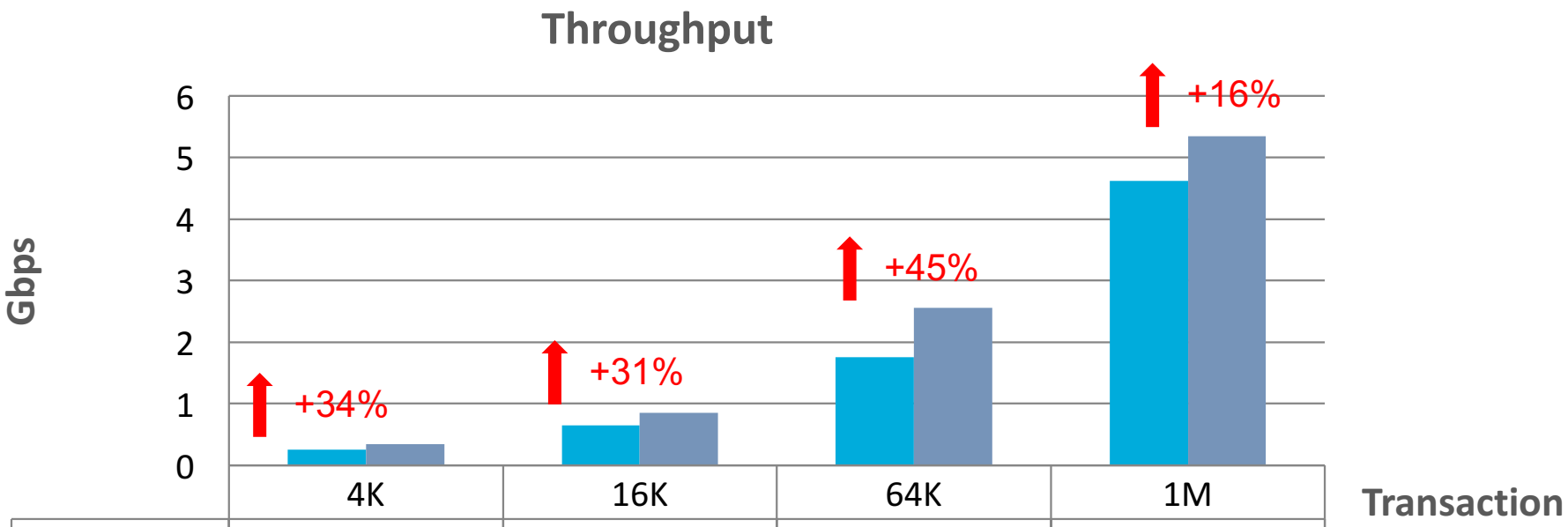
- Calculate bytes for categories that will be decrypted (**545.2M**)
- Calculate total tcp/443 bytes (**547.0M**)
- % decryption = (Sum of bytes for selected categories / total bytes) x 100

545.2M / 547.0M X 100 = 99.67% (3% of Total Traffic)

Note: This is not representative data. Just showing the process. This is heavily skewed home traffic.

Performance improvements in Orlando

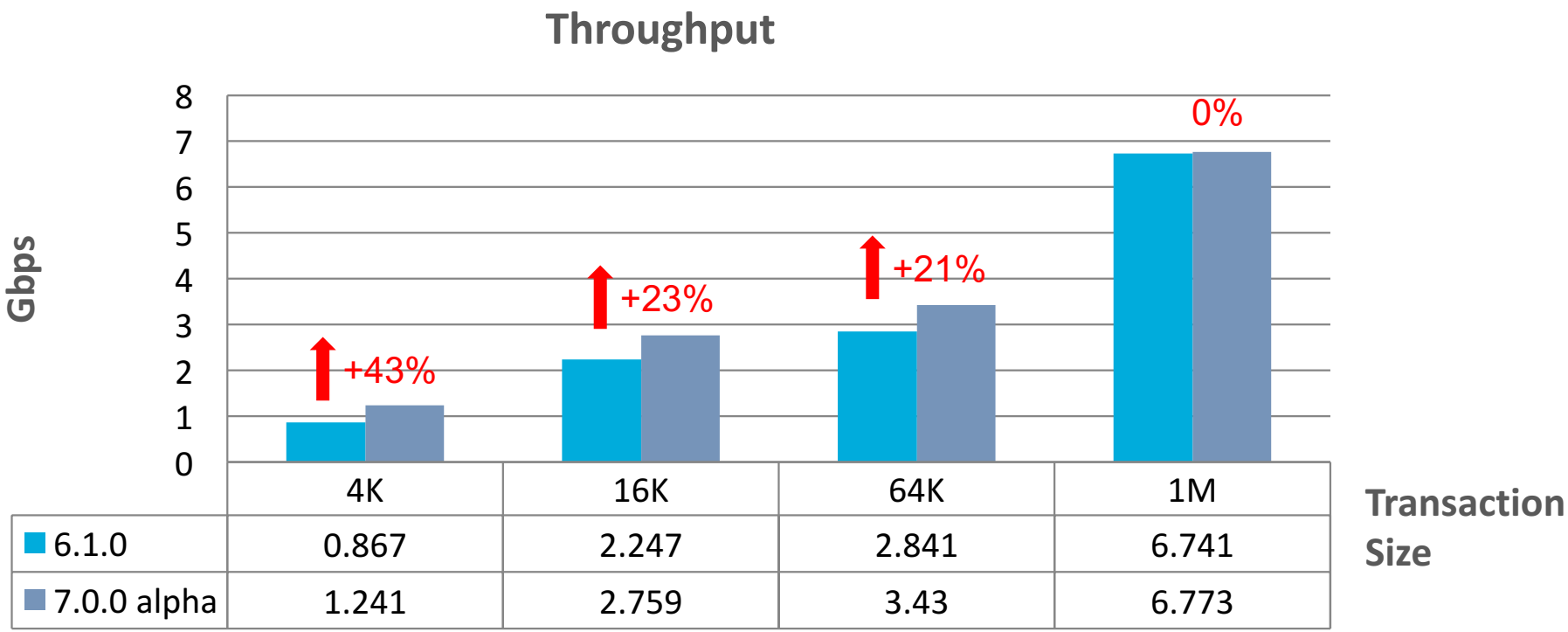
- PA-7050, 1 NPC, Forward Proxy, 2K keys



	4K	16K	64K	1M
6.1.0	0.255	0.651	1.757	4.622
7.0.0 alpha	0.342	0.856	2.555	5.349

Performance improvements in Orlando

- PA-7050, 1 NPC, Inbound, 2K keys



	4K	16K	64K	1M
6.1.0	0.867	2.247	2.841	6.741
7.0.0 alpha	1.241	2.759	3.43	6.773

SSL Specific Sizing Parameters

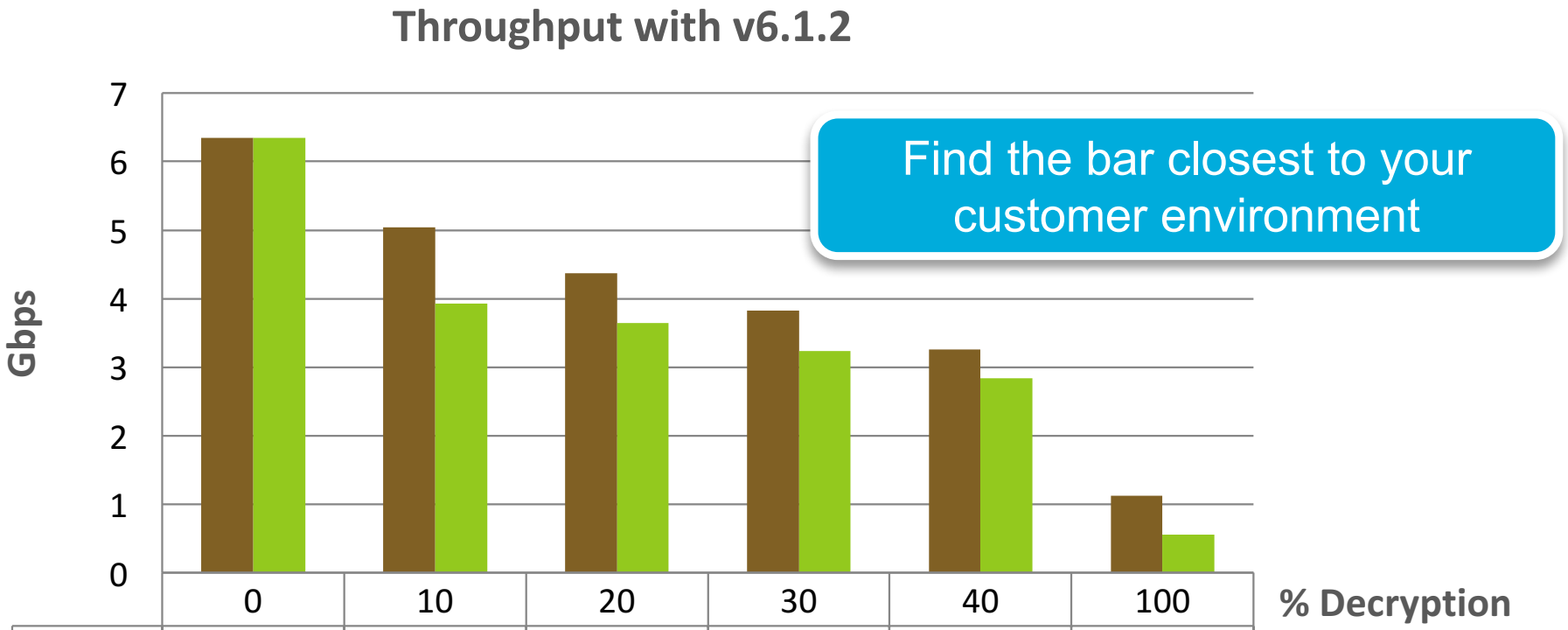
- Average object size for encrypted traffic
  - From custom report calculate avg. object size = total bytes / total sessions
- Find out if the customer intends to turn on threat prevention profiles
- Private keys – 1K vs. 2K

Decryption Sizing Methodology: PA-5060 Forward Proxy

Name	Weight	Seed	Sessions	% Bandwidth	% Flows	# Bytes
BreakingPoint Google Map Search	13.00	Generated	6.00	0.83	0.77	398,672.00
BreakingPoint Microsoft Update	5.00	Generated	4.00	0.32	0.02	5,653,396.00
BreakingPoint Netflix Silverlight	30.00	Generated	5.00	1.93	0.03	21,219,203....
PAN_NGFW_SMTP	70.00	Generated	2.00	4.50	3.16	519,760.00
PAN_NGFW_Exchange_Outlook Email	127.00	Generated	1.00	8.16	5.12	582,505.00
PAN_NGFW_Twitter	42.00	Generated	3.00	2.70	0.21	4,691,130.00
PAN_NGFW_AOL_IM	6.00	Generated	1.00	0.39	0.04	3,144,787.00
PAN_NGFW_SSH	11.00	Generated	1.00			
PAN_NGFW_BitTorrent	118.00	Generated	7.00			
PAN_NGFW_Hotmail	160.00	Generated	3.00			
PAN_NGFW_HTTP	719.00	Generated	1.00			
NGFW_Facebook	100.00	Generated	1.00	6.43	0.70	3,344,463.00
SSL HTTPS 1.1 64K	155.00	Generated	1.00	9.96	16.39	221,903.00

Vary the % of SSL traffic in increments of 10. Test throughput with decryption turned on

Sizing Results (PA-5060 FP)



	0	10	20	30	40	100
1K Key	6.342	5.037	4.366	3.83	3.259	1.121
2K Key	6.342	3.925	3.649	3.235	2.835	0.553

* Threat prevention is configured with default profiles for AV, AS and VP

Sizing Exercise 3 : Internet Perimeter

- Customer now wants to enable SSL Decryption (Forward proxy) for visibility.

- Existing Traffic Profile
  - Corporate has 500 Mbps Internet connection
  - Concerned about Threat Prevention
  - From an evaluation carried out for traffic mix:
    - 8T bytes of sessions to be decrypted.
    - 10T bytes of total SSL traffic
    - 50% of the total traffic is SSL
  - Assume Avg. Transaction size = 64K, 1K key size
  - Assume the following trend for performance degradation due to decryption (this is purely for sake of this exercise – NOT real data)

% of Decrypted Traffic	0	10	20	30	40	100
Throughput %	100	79.4	68.8	60.4	51.4	17.7

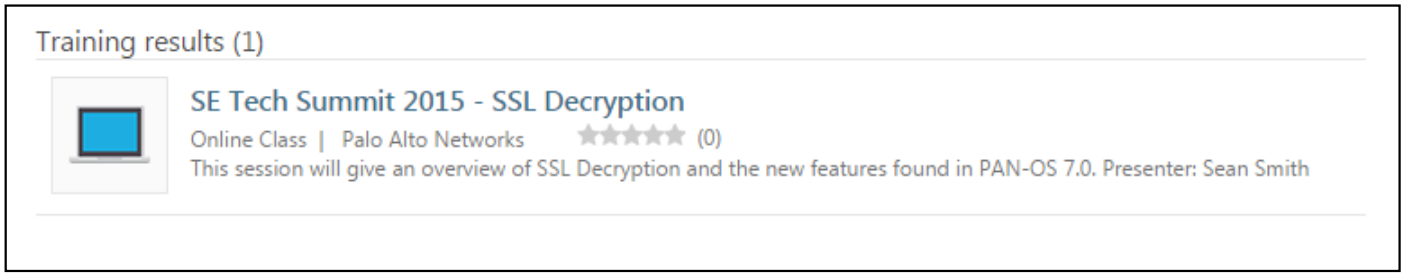
- Determine the **SKUs** required.

Sizing Exercise 4 : Datacenter Perimeter

- Customer wants to enable Decryption for full App visibility and control
- Requirements
  - Requires 3G throughput with Threat prevention
  - 30% Decryption
  - 1K Key size
- Determine the **SKUs** required.

For Further Reference

- For further reference, please refer to the SSL Decryption recording on the Learning Center: https://paloaltonetworks.csod.com/
- Search for SSL Decryption:



Questions?


paloalto
NETWORKS®
Secures the Network