

Securing Networks with
Cisco FTD

Chapter 16

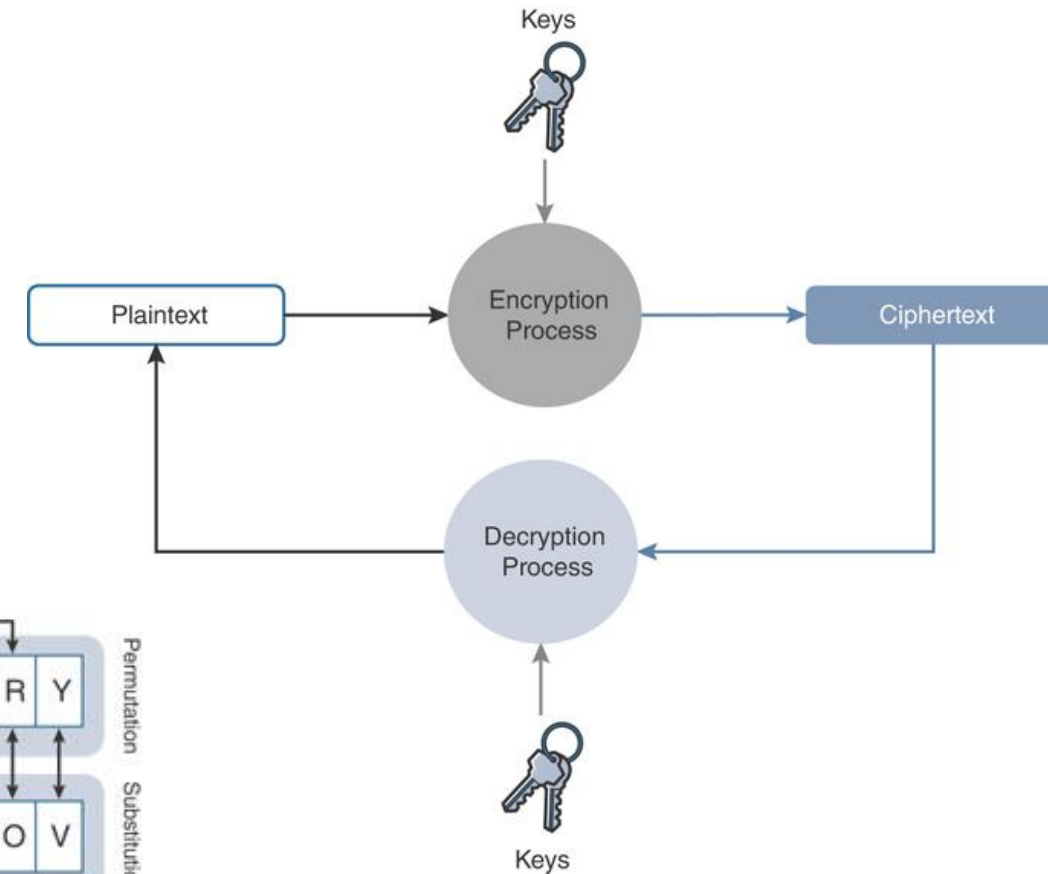
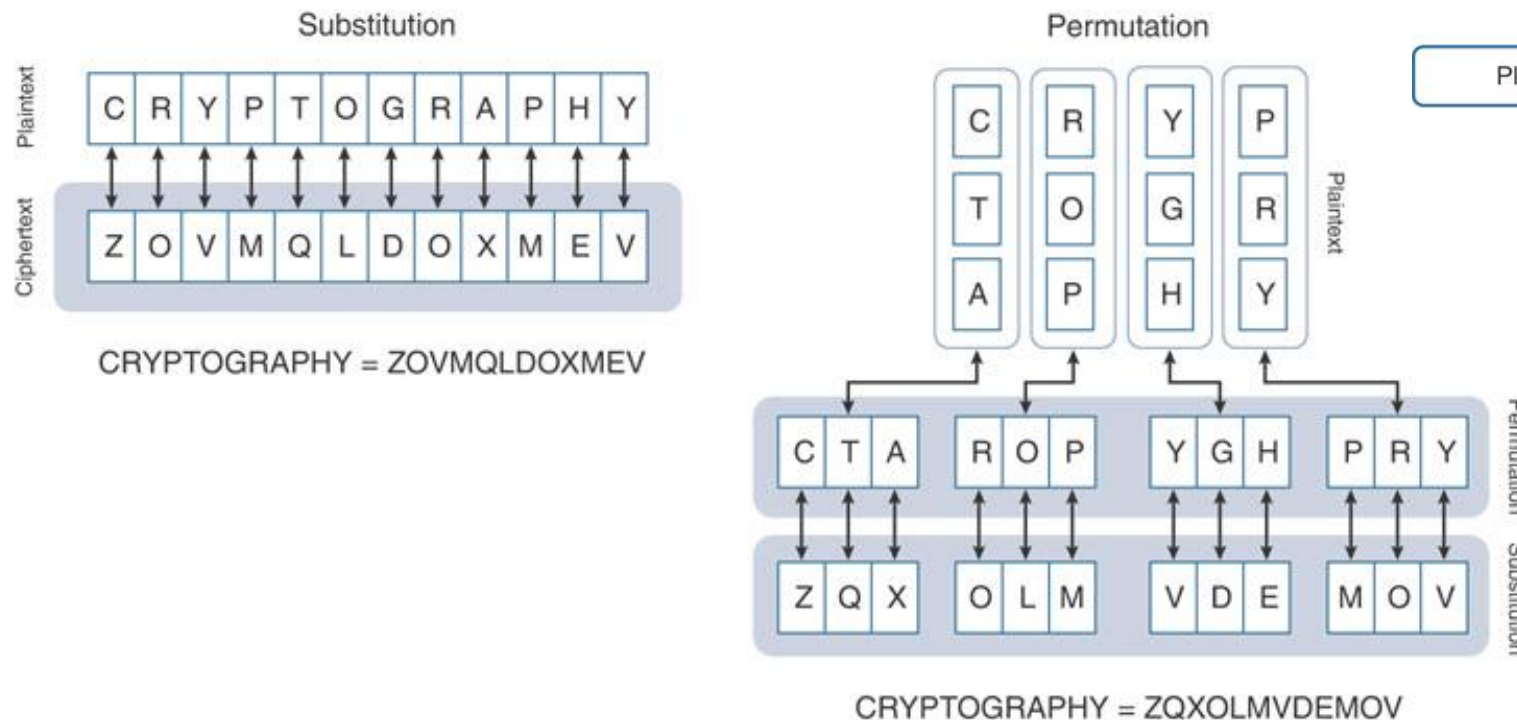
Traffic Decryption Policy

Mohsen Kheradmand

Traffic decryption

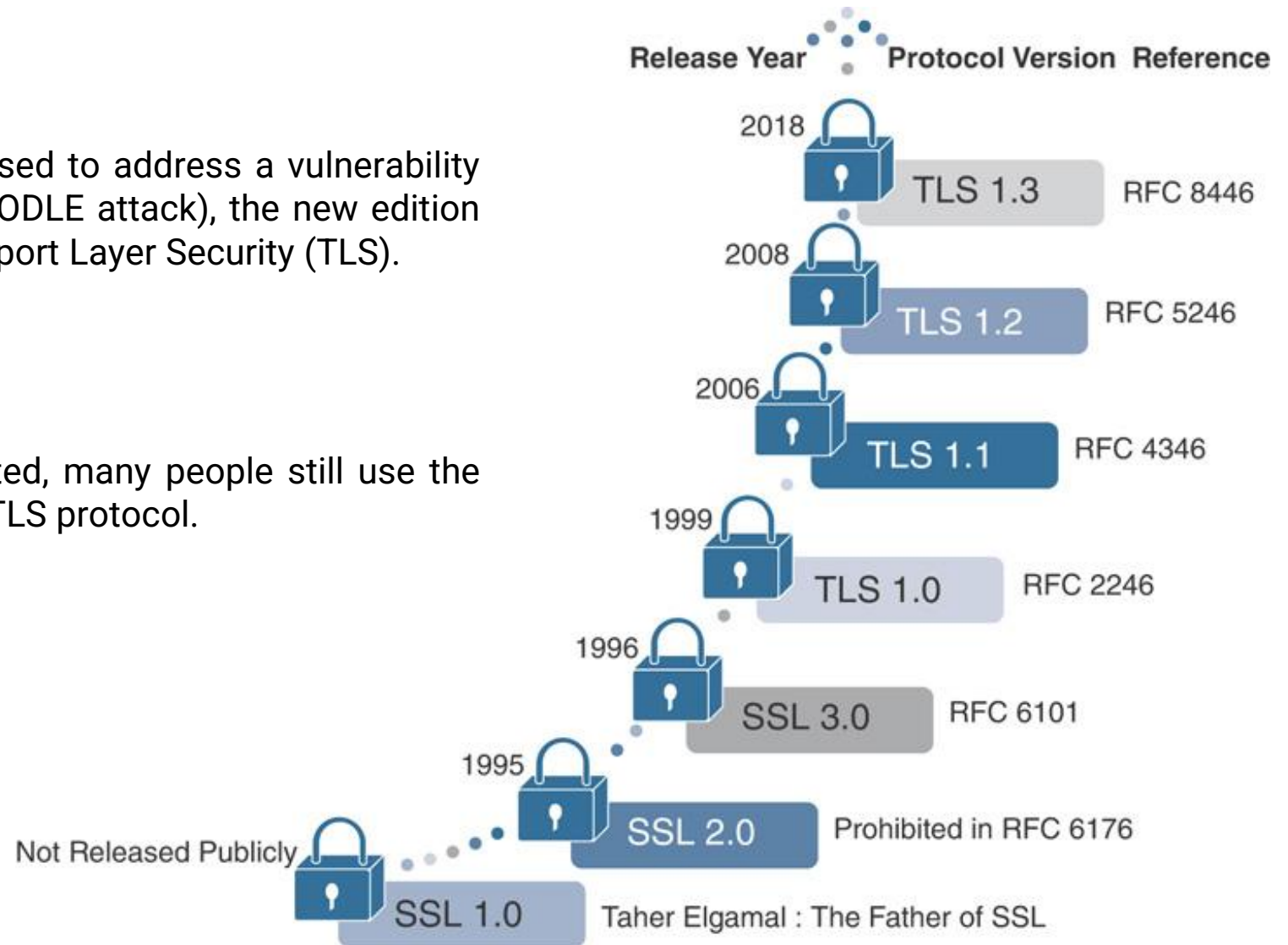
- Malware and ransomware can remain invisible when they traverse over an encrypted tunnel
- FTD can decrypt the encrypted traffic, inspect the decrypted traffic and finally re-encrypt the traffic like a MITM

✓ Concept of Encryption and Decryption Using a Simple Cipher

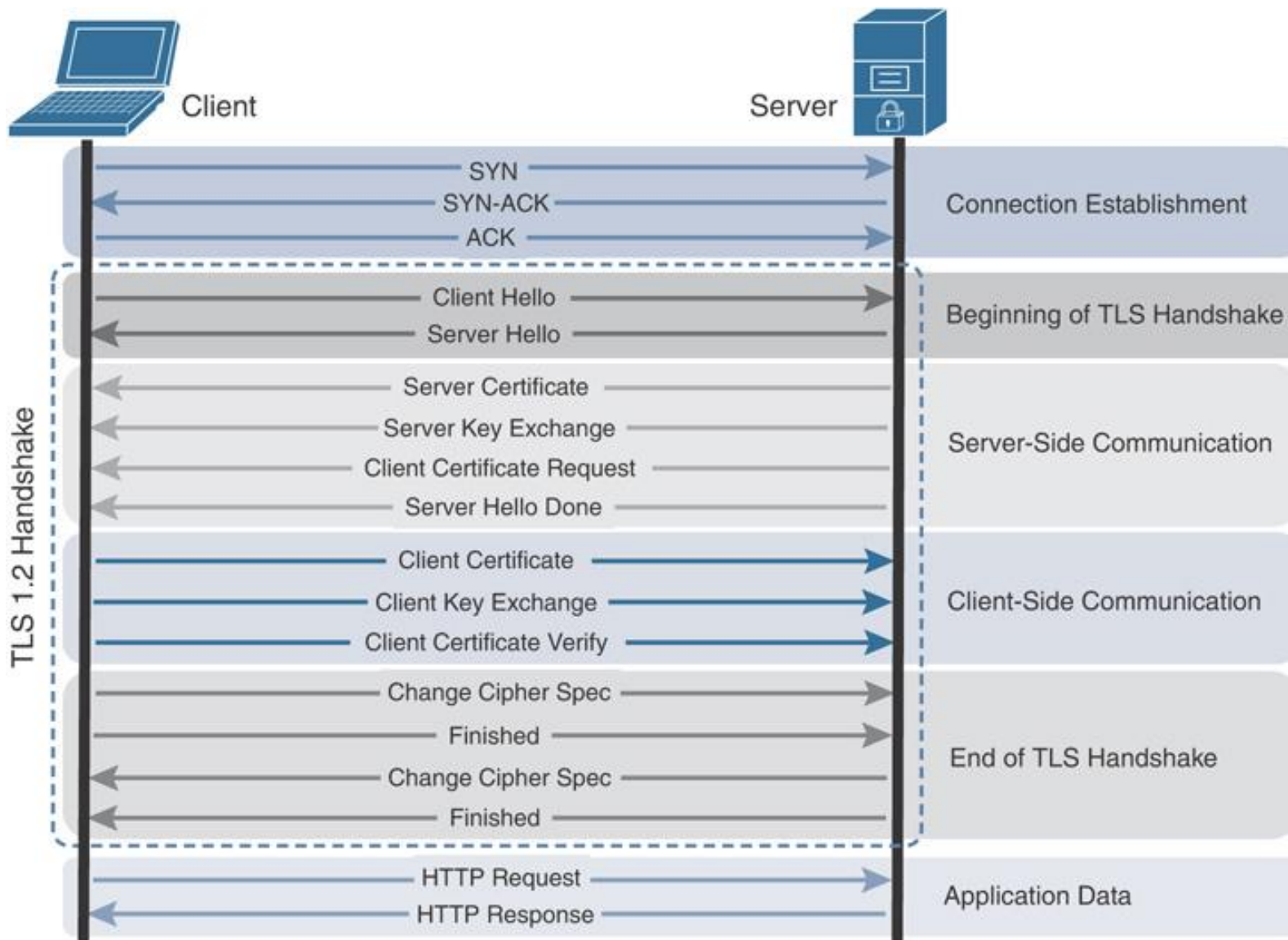


Overview of SSL and TLS Protocols

- When SSL protocol version 3 was revised to address a vulnerability with a MITM attack (known as the POODLE attack), the new edition of the protocol was renamed the Transport Layer Security (TLS).
- Although the SSL protocol is deprecated, many people still use the term SSL to refer to its successor, the TLS protocol.



➤ Detail View of TLS 1.2 Handshakes



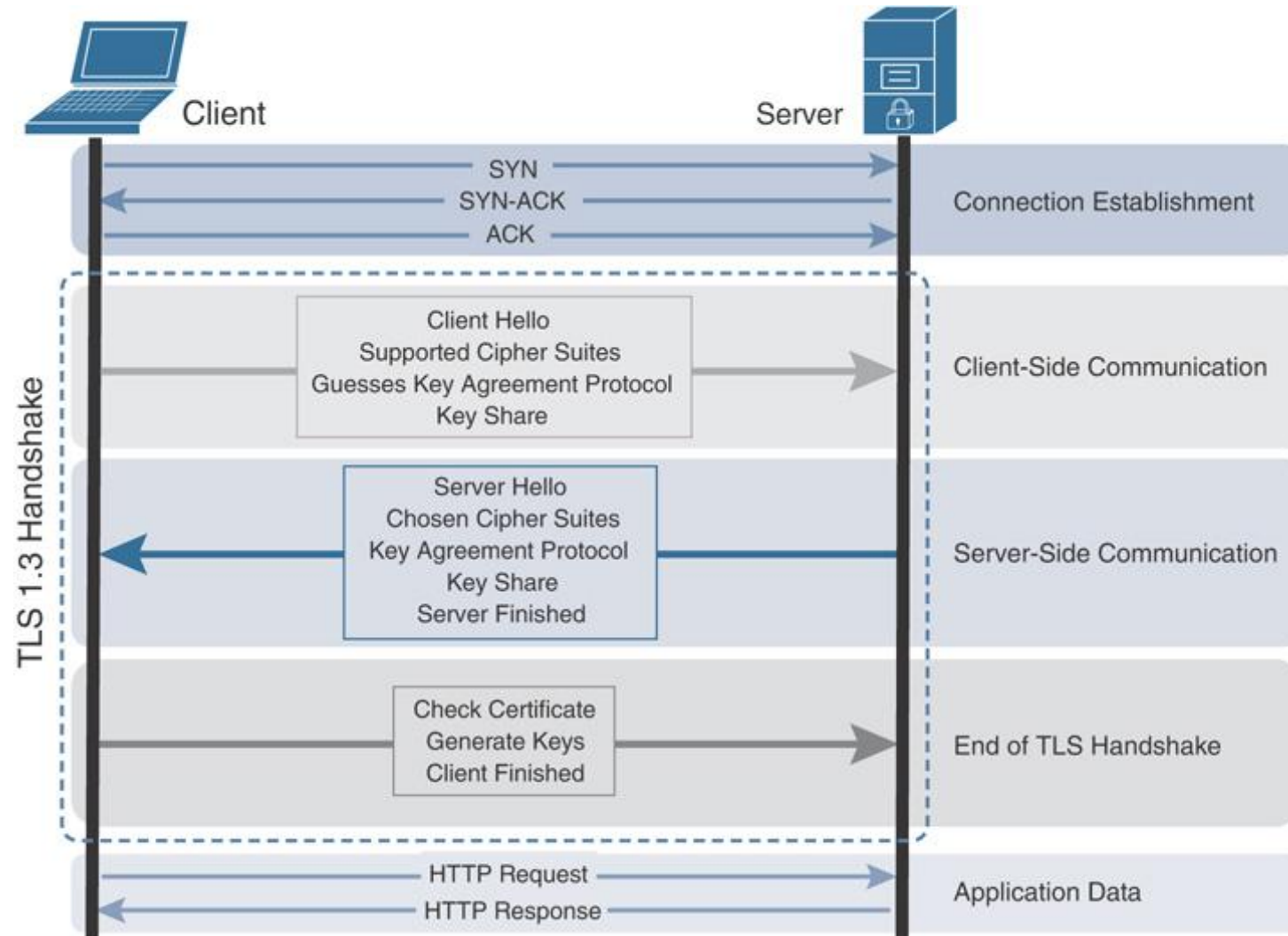
- Secure Firewall uses the handshake to determine the exact protocol version used in an encrypted session

- 1) TCP three- way handshake (SYN, SYN-ACK, ACK)
- 2) start TLS Hello message between the client and server
- 3) Negotiate the security parameters they can support and exchange encryption keys
- 4) End of TLS handshake and begin Data request/response

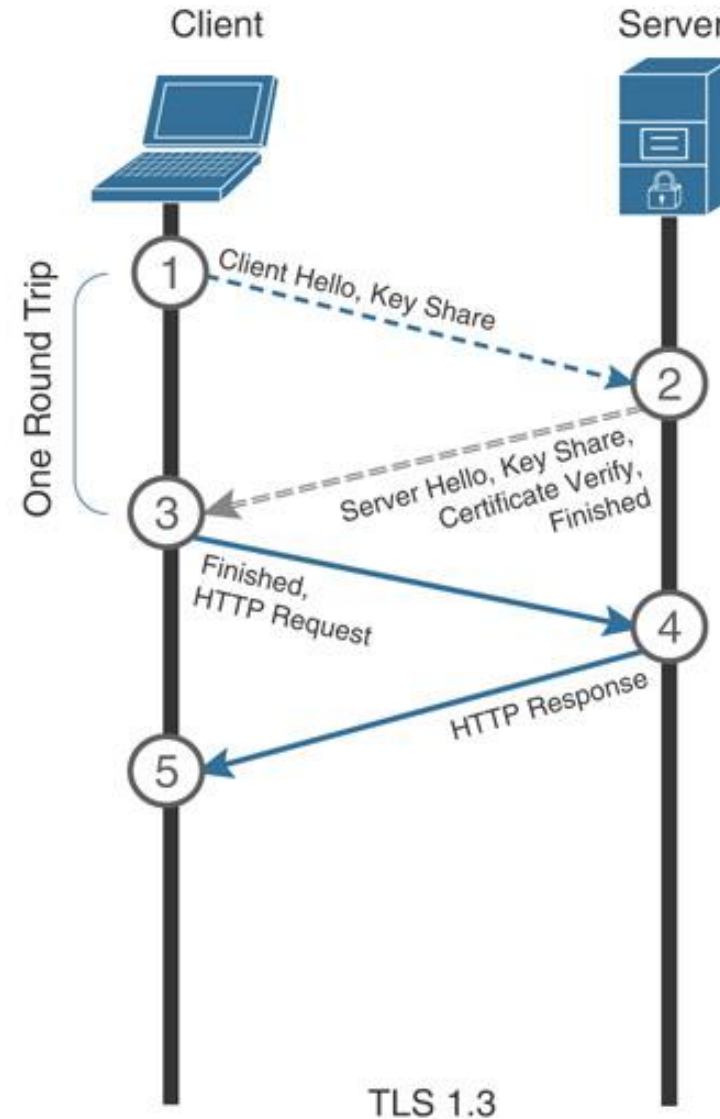
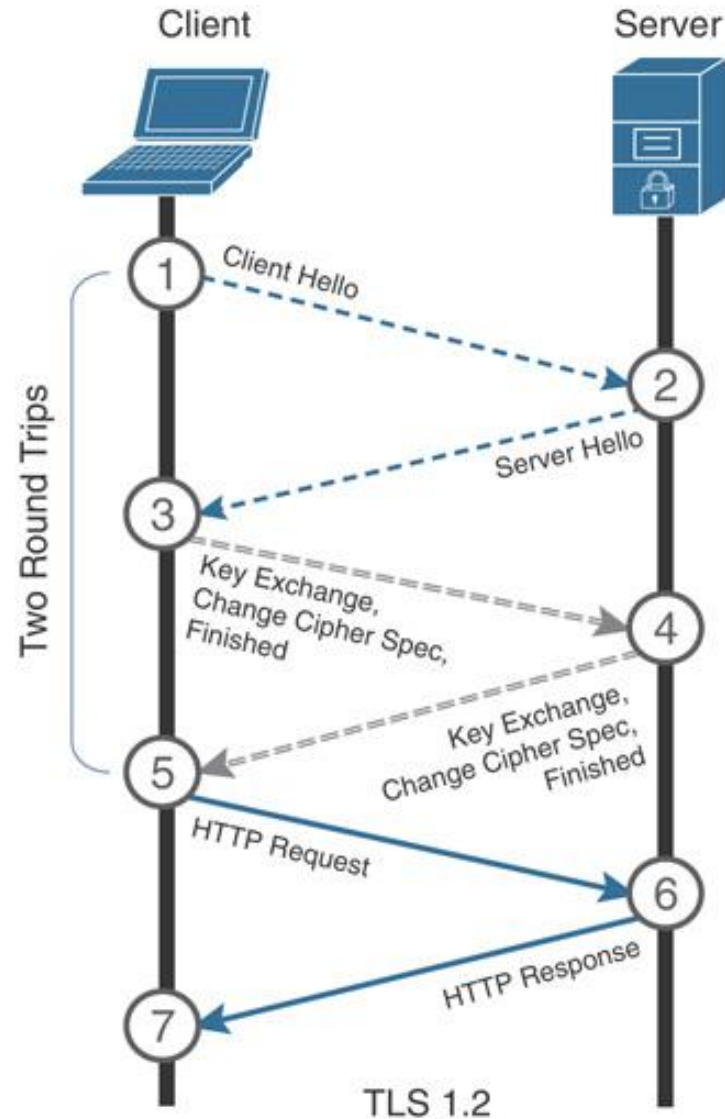
✓ TLS 1.2 requires two round trips to complete its handshake.

➤ Detail View of TLS 1.3 Handshakes

- TLS 1.3 complete the handshake in just in one round trip
- TLS 1.3 also deprecates obsolete and vulnerable ciphers and algorithms, such as RC4, DES, and MD5

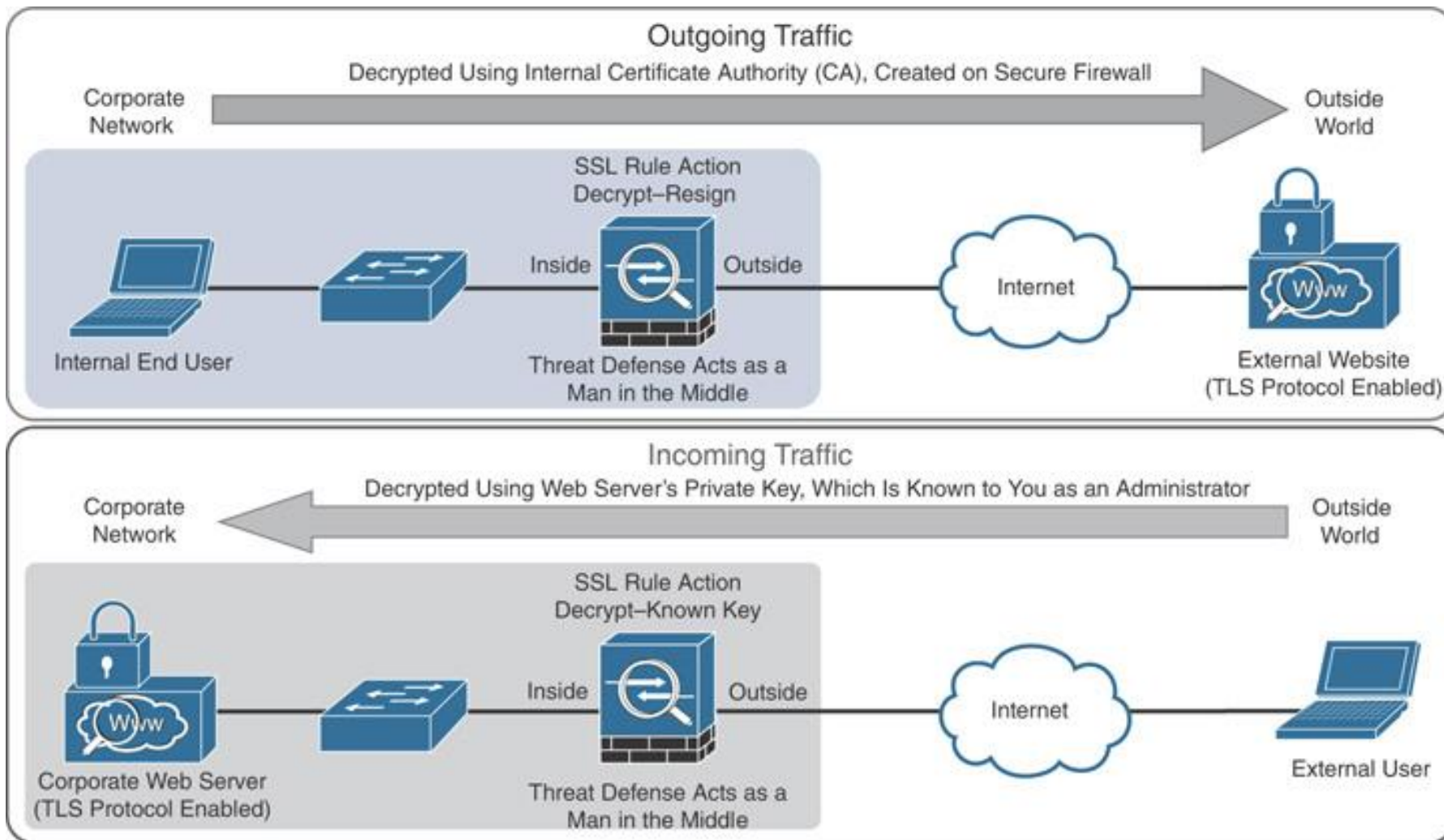


➤ Round Trips Comparison by TLS 1.2 and TLS 1.3



Decryption Techniques on Secure Firewall

- To decrypt, inspect, and block encrypted traffic, you need to configure an SSL policy
- Secure Firewall uses that SSL policy before the access control policy rules



Decryption Techniques on Secure Firewall

❑ Secure Firewall offers two techniques to traffic:

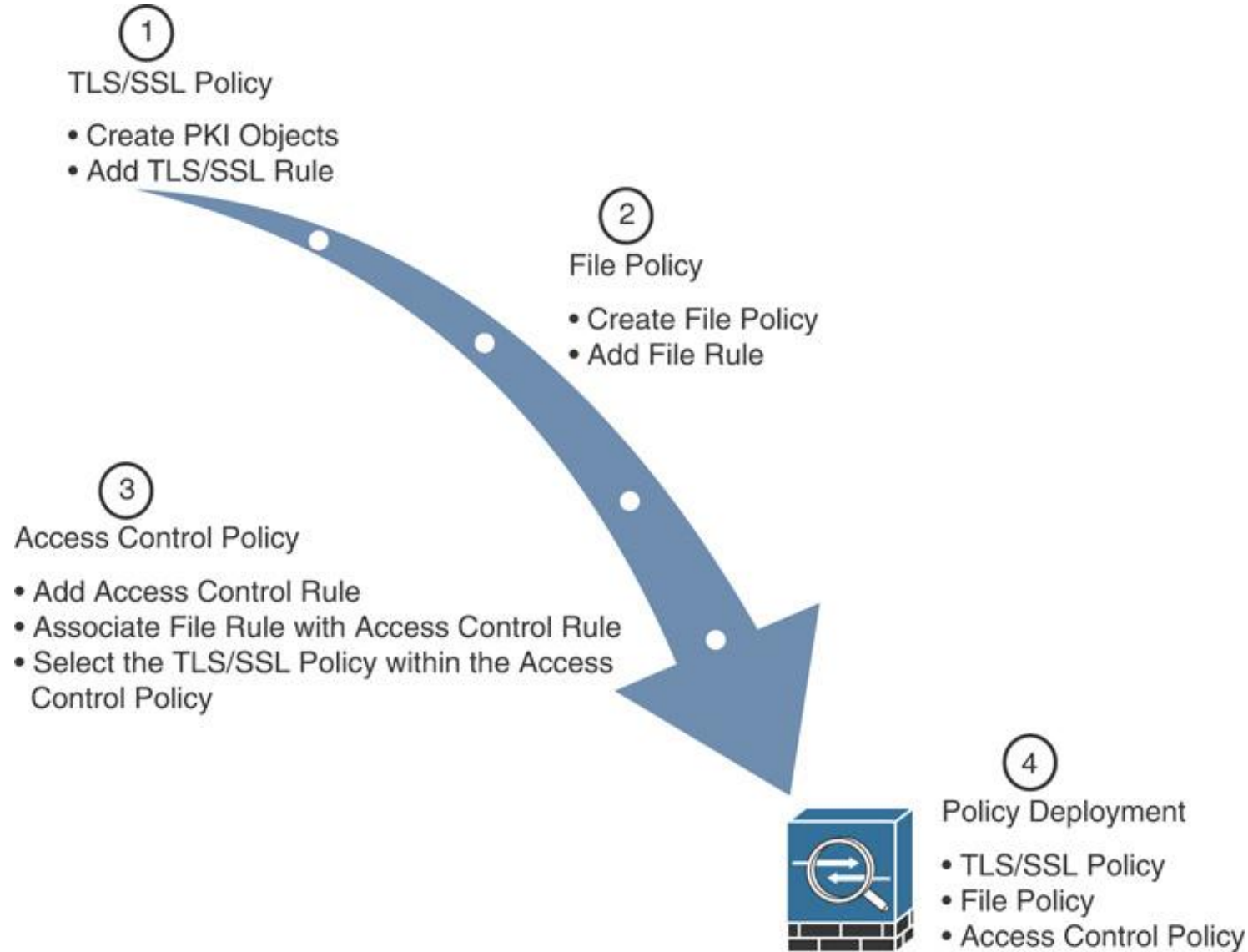
➤ Decryption by resigning (for outgoing traffic) :

- Decrypt outgoing traffic from an internal end-user when the user attempts to connect to an external web server
- Secure firewall acts like a proxy or man-in-the-middle
- Completes the SSL handshake on behalf of the client , perform traffic inspection and re- encrypts the traffic and sends it off to its destination.
- A threat defense builds a TLS tunnel with the internal end-user using a certificate issued by an internal CA.
- Also , a separate TLS tunnel is established simultaneously between the threat defense and the destination website

➤ Decryption using known key (for incoming traffic)

- Decrypt incoming traffic from external sources destined for internal servers
- You can gain access to the internal server's private key and upload it to the management center
- The threat defense can use this private key to decrypt and re-encrypt any incoming traffic

Configuring a Decryption Policy process



Configuring a Decryption Policy process

1) Begin the process by creating public key infrastructure (PKI) objects

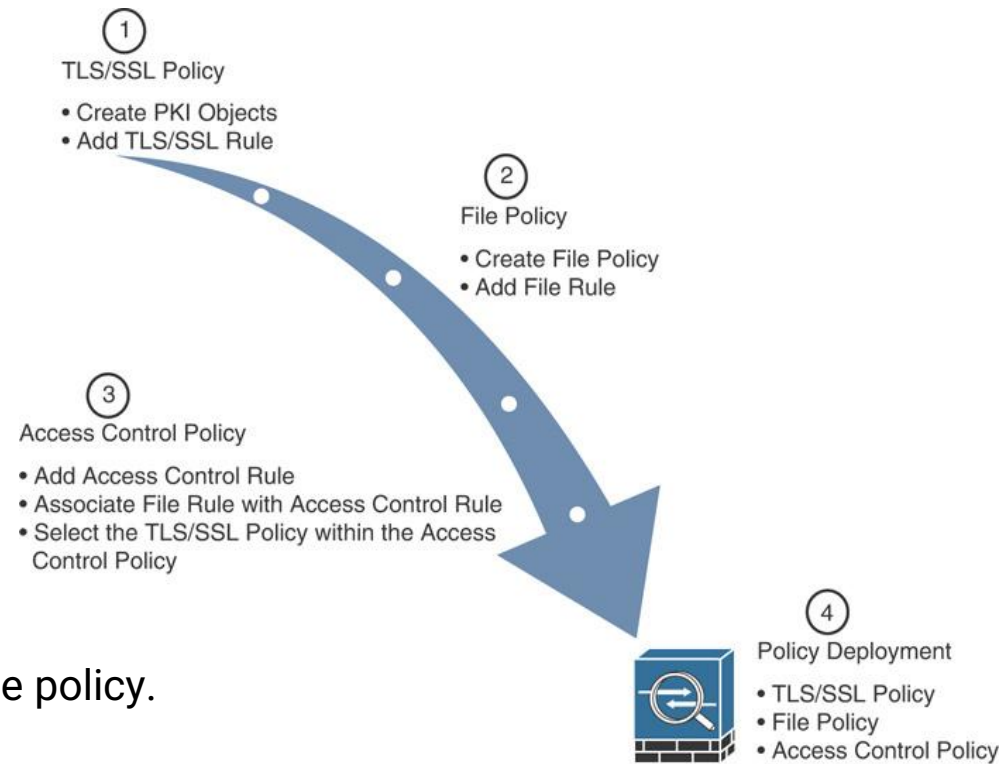
❑ Next, configure an SSL policy using the PKI objects.

2) To use the benefits of traffic decryption, you can also create or reuse a file policy.

❑ Alternatively, an intrusion policy could be used to show deep packet inspection

3) Then , associate your SSL policy with the access control policy

4) Finally deploy the policy to the FTD



PKI Objects

- Objects > Object Management
- PKI > Internal CAs
- Click Generate CA
- Complete the form
- Generate Self-Signed CA

The screenshot displays the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The left sidebar shows a tree view of PKI objects, with 'Internal CAs' selected. The main content area shows the 'Internal CAs' page with a table of existing CAs. A modal dialog box titled 'Generate Internal Certificate Authority' is open, containing the following fields:

- Name: FTD-CA-internal
- Country Name (two-letter code): IR
- State or Province: Tehran
- Locality or City: Tehran
- Organization: Dena
- Organizational Unit (Department): IT
- Common Name: Kheradmand

At the bottom of the dialog, there are three buttons: 'Generate CSR', 'Cancel', and 'Generate self-signed CA'.

Internal Certs Object

- Upload the server certificate and private key to Secure firewall
- FTD uses this object in an SSL rule and select the Decrypt- Known Key action to decrypt matching incoming traffic

PKI

- Cert Enrollment
- External Cert Groups
- External Certs
- Internal CA Groups
- Internal CAs
- Internal Cert Groups
- 1 Internal Certs**
- Trusted CA Groups
- Trusted CAs
- Policy List
- Port
- Prefix List
- Route Map
- Security Intelligence
- Sinkhole
- SLA Monitor
- Time Range
- Time Zone
- Tunnel Zone
- URL
- Variable Set
- VI AN Tag

Internal Certs

2 Add Internal Cert Filter

Internal certificate object represents a server public key certificate belonging to your organization. You can use internal certificate objects and groups in SSL rules, ISE/ISE-PIC connection and captive portal configuration.

Add Known Internal Certificate

Name: Internal_Server_Cert

Certificate Data or, choose a file: Browse...

```
-----BEGIN CERTIFICATE-----
MIIEQzCCAyugAwIBAgIUJtQi5L68xL9XrocpVa+68ReF2kgwDQYJKoZIhvcNAQEL
BQAwZDEkMCIGA1UECwwbSW50cnVzaW9uE1hbmFnZW1ibnQgU3lzdGVtMRswG
QYD
VQQKDBJDaXNjbYBTenXN0ZW1zLCBjb2MxMjE1QzBjbmMxMjE1QzBjbmMxMjE1
MAkG
-----
```

Key or, choose a file: Browse...

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAykh5r9dUbTPUISNbhgmjWc1sZfQ+qz4Z7B5L8oldv+5DKkM
2LHNFJlqkbUCYBEVMjAaaZPnj/9Vpo9o5Bkl8wSgOkTiQdDd2Gi9jSQc7TWH/0L
kiB5572mqOrXoq2afscyJjk28J4jUNjAguliW/M6UU6wYQSAFof9nUVykajalCcRCzgb
0tmBBFHgF83ldnLRScCkM7a4IzJ7BunCkOWv9HyQw5giaHm3NF
HyRd4Gx3LmlGYhtV9Jy7l/qoH+zux/btVA5MWC76iRvPP7u+8h7d0aBiUXPHI6U
-----
```

☐ Encrypted, and the password is:

3

Cancel Save

Objects > Object Management

1) PKI > Internal Certs

2) Add Internal Cert

- Enter a name for Cert
- Import the internal web server Cert
- Also import the private key of web server

3) Click Save

SSL Policy

- 1) Policies > Access Control > SSL
- 2) click the New Policy
- 3) Enter a name and select Do not decrypt as a default action

The screenshot shows the Cisco Firepower Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Policies' tab is selected. On the right, there are buttons for 'Compare Policies' and 'New Policy'. A modal dialog titled 'New SSL Policy' is open in the center. It contains the following fields and options:

- Name:** A text input field containing 'Decryption Policy'.
- Description:** An empty text input field.
- Default Action:** Three radio button options: 'Do not decrypt' (selected), 'Block', and 'Block with reset'.
- Buttons:** 'Cancel' and 'Save' buttons at the bottom right of the dialog.

The background interface shows a table with columns 'SSL Policy' and 'Last Modified', but it is partially obscured by the dialog box.

- ✓ The default action is used to handle the traffic that does not match any SSL rules

Decryption Policy

Cancel

Trusted CA Certificates

Undecryptable Actions

+ Add Rule

Search Rules

×

Name



SSL

Action

This category is empty

This category is empty

This category is empty

Default Action

☒ Enabled

Standard Rules

w

C

☐ Replace Key Only

Networks

Users

Ports	Category
-------	----------

DN

Cipher Suite

Logging

DMZ

Inside-LAN

Internet

Add to Source

Add to Destination

Source Zones (1)

DMZ

Destination Zones (1)

Internet

Cancel

Add

SSL Policy

4) In the policy editor page, click the Add Rule button

5) Name the SSL rule

6) define the direction of the traffic

7) select an action and PKI object

8) Optionally, enable logging (logging tab)

9) Click Add

Add Rule

Name: Decryption-outgoing ☒ Enabled Insert: into Category Standard Rules

Action: Decrypt - Resign with FTD-CA-internal ☐ Replace Key Only

Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Logging

Available Zones

- DMZ
- Inside-LAN
- Internet

Add to Source Add to Destination

Source Zones (1): DMZ

Destination Zones (1): Internet

Cancel Add

Actions :

- **Decrypt - Resign** : to handle outgoing traffic (flow from inside to the outside zone)
- **Decrypt - Known Key** : to handle incoming traffic (flow from the outside zone to the internal zones)

SSL Policy

10) You can enable logging for any traffic that can match the default action

Logging

☒ Log at End of Connection

Send Connection Events to:

☒ Firepower Management Center

☒ Syslog Server
(Using default syslog configuration in Access Control Logging)

[Show Overrides](#)

☐ SNMP Trap

Select an SNMP Alert Configuration ▼ +

Cancel OK

FMC SSL Policy Editor

Overview Analysis Policies Devices Objects AMP Intelligence Deploy

Decryption Policy

Enter Description

Rules Trusted CA Certificates Undecryptable Actions

+ Add Category + Add Rule QSearch Rules X

Name	Source Zones	Dest Zones	So... Ne...	De... Ne...	VL Ta	Us	A...	S... P...	D... P...	C...	SSL	Action
Administrator Rules												
This category is empty												
Standard Rules												
1	Decrypt_Outgoing	INSIDE_ZON	OUTSIDE_Z	any	any	any	any	any	any	any	any	→ Decrypt - Resig
2	Decrypt_Incoming	OUTSIDE_Z	INSIDE_ZO	any	any	any	any	any	any	any	any	→ Decrypt - Know
Root Rules												
This category is empty												
Default Action												Do not decrypt

Displaying 1 - 2 of 2 rows |< < Page 1 of 1 > > C

Note :

- ✓ SSL rules are evaluated in top-to-bottom order , Place the SSL rules with **Block** and **Do Not Decrypt** actions before the **Decrypt Known Key** and **Decrypt Resign** actions.
- ✓ Place the rules with specific conditions before the rules with broader conditions

Logging Icon for Default Action

SSL Policy

11) Finally, define how Secure Firewall will handle the undecryptable traffic

The screenshot shows the Cisco FMC (Firewall Management Center) SSL Policy Editor interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies' (selected), 'Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', and a user profile 'admin'. The main heading is 'Decryption Policy'. Below it, there's a 'Enter Description' field and a status bar indicating 'You have unsaved changes' with 'Save' and 'Cancel' buttons. The 'Undecryptable Actions' tab is selected, showing a table of actions for various decryption errors. A 'Revert to Defaults' button is at the bottom of the table.

Decryption Errors	Action
Decryption Errors	Block
Handshake Errors	Block
Session not cached	Inherit Default Action
Unsupported Cipher Suite	Block with reset
Unknown Cipher Suite	Block with reset
SSLv2 Session	Block
Compressed Session	Inherit Default Action

❖ For example, if you do want to deny any SSLv2 traffic, you can select Block action

You can create a file policy rule to invoke in SSL policy

MohsenKheradmand 

Access Control Policy

After you configure an SSL policy and a file policy you must invoke them in the access control policy

 Firepower Management Center

Policies / Access Control / Policy Editor

OverviewAnalysisPoliciesDevicesObjectsAMPIntelligence

Deploy 🔍 2 ⚙️ ? admin ▾

FTD1-Policy

applicable to FTD1

You have unsaved changes Show Warnings Analyze Hit Counts Save Cancel

[Inheritance Settings](#) | [Policy Assignments \(1\)](#)

RulesSecurity IntelligenceHTTP ResponsesLogging⚠️ Advanced

Prefilter Policy: Servers PrefilterSSL Policy: Decryption PolicyIdentity Policy: None

[Filter by Device](#) 🔍 Search Rules X ☐ Show Rule Conflicts ? + Add Category + Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destinat... Dynamic Attributes	Action	
▼ Mandatory - FTD1-Policy (1-3)															
1	DB-SRVs	Any	Any	Any	Servers	Any	Any	Any	Any	Any	Any	Any	Any	➡ Allow	
2	Clients-to-int	Any	Internet	IT-Admins sales-PCs Production	Any	Any	Any	Any	Any	Any	Any	Any	Any	👁 Monitor	
3	IT-to-SRVs	Any	Any	IT-Admins	Servers	Any	Any	Risks: High; AnyDesk	Any	Any	Any	Any	Any	🚫 Block	
▼ Default - FTD1-Policy (-)															
There are no rules in this section. Add Rule or Add Category															

Verification

Example :

- You intend to connect to a web server located at the outside zone with the TLS protocol enabled



- First, log in to the internal end-user computer (IP: 192.168.1.100) and open a browser.
- Using the browser : open the <https://203.0.113.10>
- Attempt to download the EXE file from the site (which is prohibited by file policy)

Verification

Example :

File	Edit	View	Go	Capture	Analyze	Statistics	Telephony	Wireless	Tools	Help
No.	Source	Destination	Protocol	Info						
1	192.168.1.100	203.0.113.10	TCP	57178 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=5957044 TSecr=						
2	203.0.113.10	192.168.1.100	TCP	443 → 57178 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1380 SACK_PERM=1 TSval=						
3	192.168.1.100	203.0.113.10	TCP	57178 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=5957044 TSecr=349875392						
4	192.168.1.100	203.0.113.10	TLSv1.2	Client Hello						
5	203.0.113.10	192.168.1.100	TCP	443 → 57178 [ACK] Seq=1 Ack=555 Win=32768 Len=0 TSval=349875392 TSecr=5957045						
6	203.0.113.10	192.168.1.100	TLSv1.2	Server Hello						
7	192.168.1.100	203.0.113.10	TCP	57178 → 443 [ACK] Seq=555 Ack=106 Win=29312 Len=0 TSval=5957046 TSecr=34987539						
8	203.0.113.10	192.168.1.100	TLSv1.2	Change Cipher Spec, Encrypted Handshake Message						
9	192.168.1.100	203.0.113.10	TCP	57178 → 443 [ACK] Seq=555 Ack=157 Win=29312 Len=0 TSval=5957046 TSecr=34987539						
10	192.168.1.100	203.0.113.10	TLSv1.2	Change Cipher Spec, Encrypted Handshake Message						
11	203.0.113.10	192.168.1.100	TCP	443 → 57178 [ACK] Seq=157 Ack=606 Win=32640 Len=0 TSval=349875395 TSecr=595704						
12	192.168.1.100	203.0.113.10	TLSv1.2	Application Data						
13	203.0.113.10	192.168.1.100	TCP	443 → 57178 [ACK] Seq=157 Ack=965 Win=32384 Len=0 TSval=349875448 TSecr=595706						
14	203.0.113.10	192.168.1.100	TCP	443 → 57178 [PSH, ACK] Seq=157 Ack=965 Win=32768 Len=1368 TSval=349875455 TSecr=						
15	203.0.113.10	192.168.1.100	TLSv1.2	Application Data						
16	192.168.1.100	203.0.113.10	TCP	57178 → 443 [ACK] Seq=965 Ack=2117 Win=34944 Len=0 TSval=5957061 TSecr=3498754						
17	192.168.1.100	203.0.113.10	TLSv1.2	Application Data						
18	203.0.113.10	192.168.1.100	TCP	443 → 57178 [ACK] Seq=2117 Ack=1372 Win=32256 Len=0 TSval=349879606 TSecr=5958						
19	203.0.113.10	192.168.1.100	TLSv1.2	Application Data						
20	192.168.1.100	203.0.113.10	TCP	57178 → 443 [ACK] Seq=1372 Ack=2455 Win=37632 Len=0 TSval=5958111 TSecr=349879						
21	203.0.113.10	192.168.1.100	TCP	443 → 57178 [RST, ACK] Seq=2455 Ack=1372 Win=32768 Len=0 TSval=349879828 TSecr=						
Frame 12: 425 bytes on wire (3400 bits), 425 bytes captured (3400 bits) Ethernet II, Src: Apple_3c:98:a8 (c4:2c:03:3c:98:a8), Dst: Cisco_b0:2b:c8 (5c:5a:c7:b0:2b:c8) Internet Protocol Version 4, Src: 192.168.1.100, Dst: 203.0.113.10 Transmission Control Protocol, Src Port: 57178, Dst Port: 443, Seq: 606, Ack: 157, Len: 359 Transport Layer Security TLSv1.2 Record Layer: Application Data Protocol: http-over-tls Content Type: Application Data (23) Version: TLS 1.2 (0x0303) Length: 354 Encrypted Application Data: 0000000000000001ebad310a0a8e5fb3ba1af52bb4e52b63...										

Capture of an HTTPS session

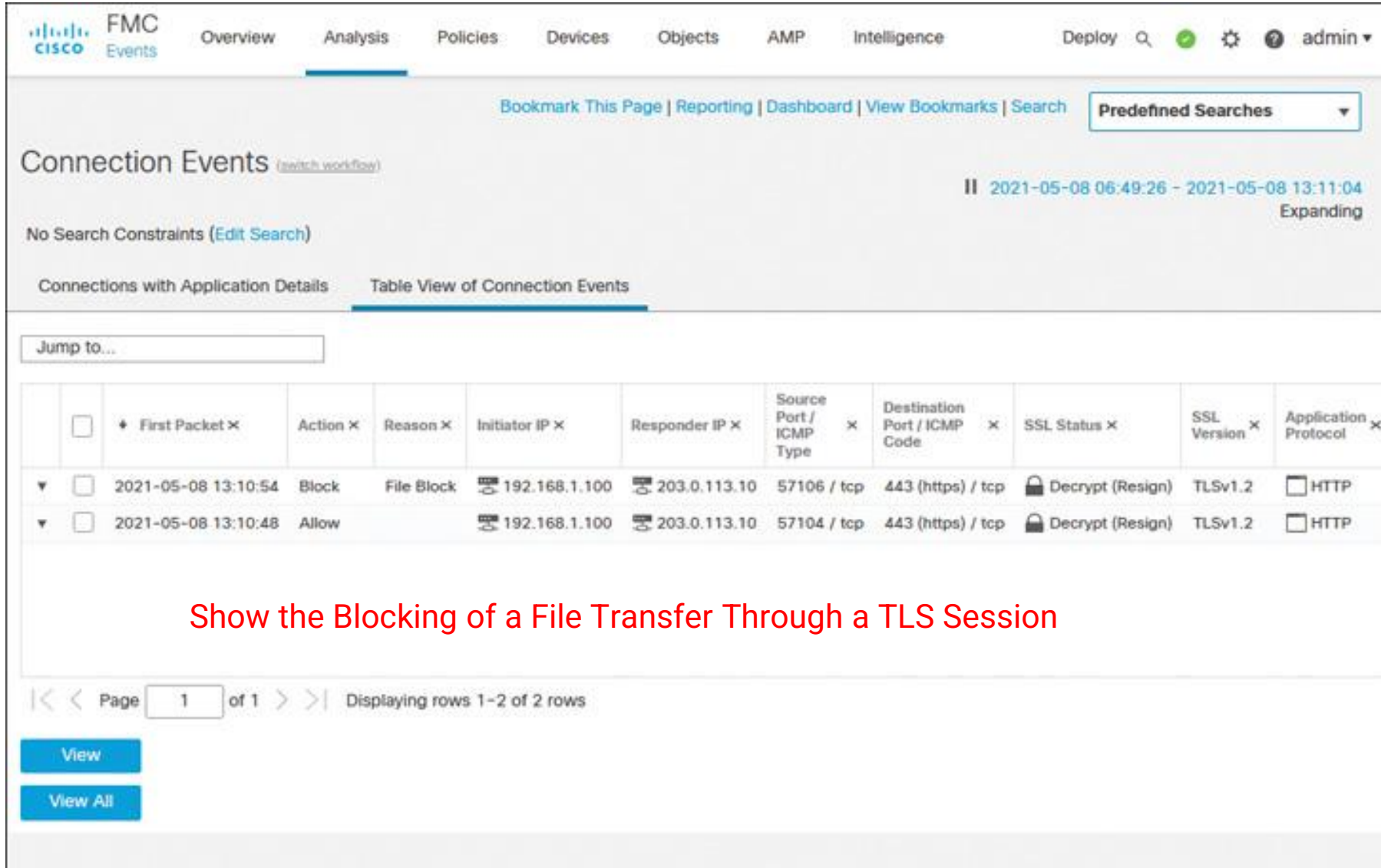
Beginning of HTTPS
Application Traffic

Block File Transfer
with Reset Packet

HTTPS Protocol Enables
Transfer of HTTP Traffic over TLS Protocol

Verification

Analysis > Connections > Events



The screenshot displays the Cisco FMC Events page. The navigation bar includes links for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The main heading is "Connection Events" with a link to "switch workflow". A search bar is present with a "Predefined Searches" dropdown. The table below shows two events:

	☐ First Packet ×	Action ×	Reason ×	Initiator IP ×	Responder IP ×	Source Port / ICMP Type ×	Destination Port / ICMP Code ×	SSL Status ×	SSL Version ×	Application Protocol ×
▼	☐	Block	File Block	192.168.1.100	203.0.113.10	57106 / tcp	443 (https) / tcp	Decrypt (Resign)	TLSv1.2	☐ HTTP
▼	☐	Allow		192.168.1.100	203.0.113.10	57104 / tcp	443 (https) / tcp	Decrypt (Resign)	TLSv1.2	☐ HTTP

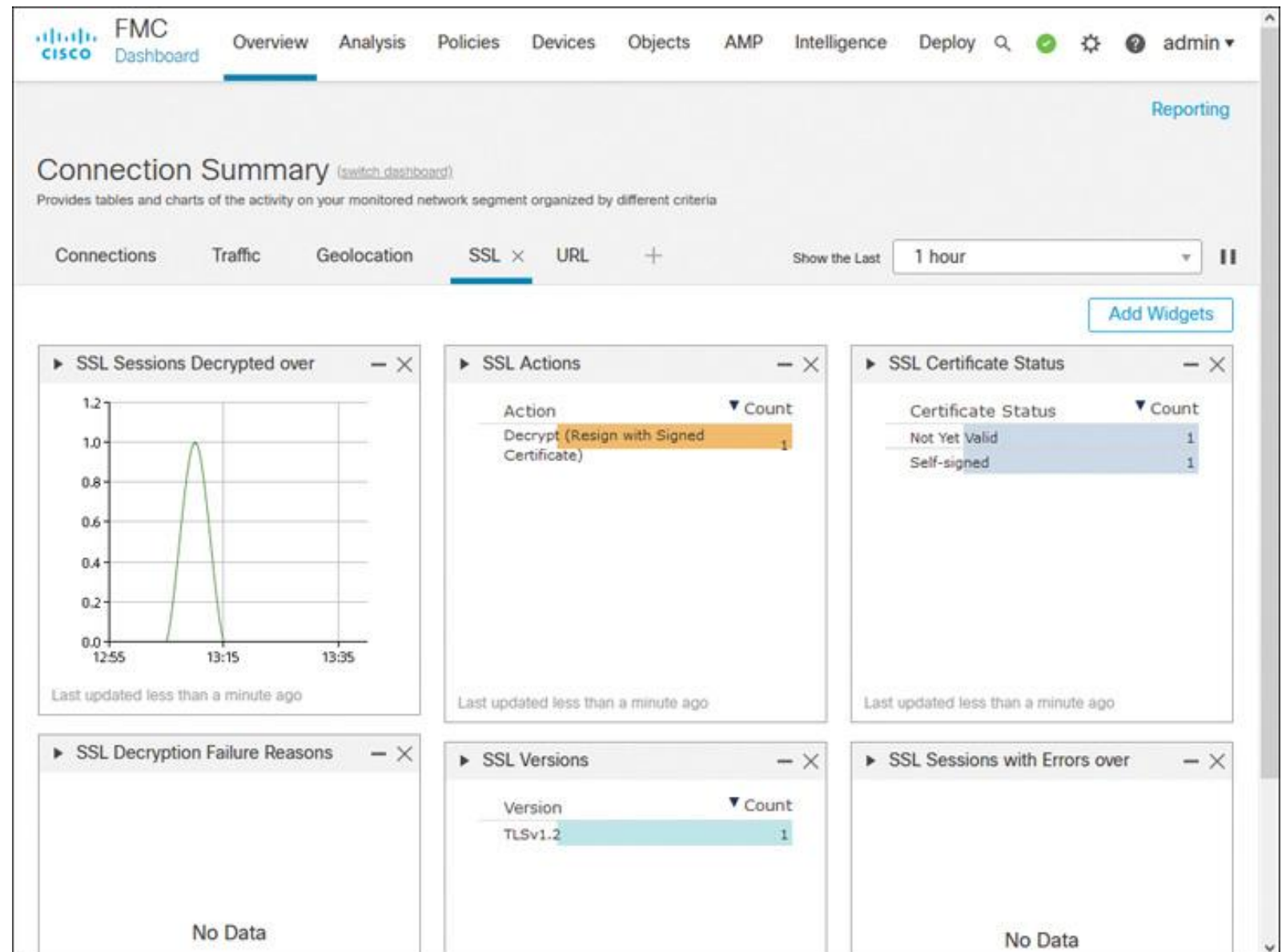
At the bottom, there is a pagination bar showing "Page 1 of 1" and "Displaying rows 1-2 of 2 rows". Below the pagination bar are two buttons: "View" and "View All".

Show the Blocking of a File Transfer Through a TLS Session

Verification

Dashboard Widgets

Show the Blocking of a File Transfer
Through a TLS Session



Verification

Test this example without SSL policy in ACP :

- ✓ Remove the association of the SSL policy from the ACP and redeploy the policy
- ✓ Retry to download the EXE file from the site
 - This time, the file should be downloaded successfully
 - The connection Events are no longer decrypted

Connection Events [\(switch workflow\)](#)

2021-05-08 06:49:26 - 2021-05-08 13:36:01 Expanding

No Search Constraints [\(Edit Search\)](#)

Connections with Application Details **Table View of Connection Events**

Jump to...

	☐	* First Packet ×	Action ×	Reason ×	Initiator IP ×	Responder IP ×	Source Port / ICMP Type ×	Destination Port / ICMP Code ×	SSL Status ×	SSL Version ×	Application Protocol ×
▼	☐	2021-05-08 13:35:24	Allow		192.168.1.100	203.0.113.10	57116 / tcp	443 (https) / tcp			☐ HTTPS
▼	☐	2021-05-08 13:35:24	Allow		192.168.1.100	203.0.113.10	57120 / tcp	443 (https) / tcp			☐ HTTPS
▼	☐	2021-05-08 13:35:24	Allow		192.168.1.100	203.0.113.10	57122 / tcp	443 (https) / tcp			☐ HTTPS
▼	☐	2021-05-08 13:35:24	Allow		192.168.1.100	203.0.113.10	57118 / tcp	443 (https) / tcp			☐ HTTPS
▼	☐	2021-05-08 13:35:24	Allow		192.168.1.100	203.0.113.10	57124 / tcp	443 (https) / tcp			☐ HTTPS
▼	☐	2021-05-08 13:35:24	Allow		192.168.1.100	203.0.113.10	57114 / tcp	443 (https) / tcp			☐ HTTPS
▼	☐	2021-05-08 13:35:12	Allow		192.168.1.100	203.0.113.10	57112 / tcp	443 (https) / tcp			☐ HTTPS
▼	☐	2021-05-08 13:35:12	Allow		192.168.1.100	203.0.113.10	57110 / tcp	443 (https) / tcp			☐ HTTPS
▼	☐	2021-05-08 13:35:11	Allow		192.168.1.100	203.0.113.10	57108 / tcp	443 (https) / tcp			☐ HTTPS
▼	☐	2021-05-08 13:10:54	Block	File Block	192.168.1.100	203.0.113.10	57106 / tcp	443 (https) / tcp	Decrypt (Resign)	TLSv1.2	☐ HTTP
▼	☐	2021-05-08 13:10:48	Allow		192.168.1.100	203.0.113.10	57104 / tcp	443 (https) / tcp	Decrypt (Resign)	TLSv1.2	☐ HTTP

< < Page 1 of 1 > > | Displaying rows 1-11 of 11 rows

[View](#)

[View All](#)

Decrypted Connections

Encrypted Connections