Securing Networks with

Cisco FTD

Chapter 16

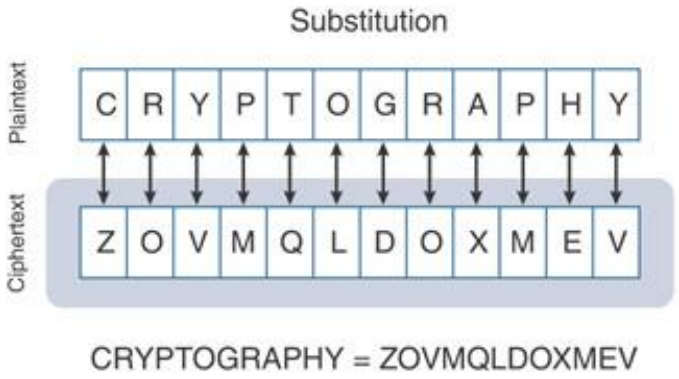
Traffic Decryption Policy

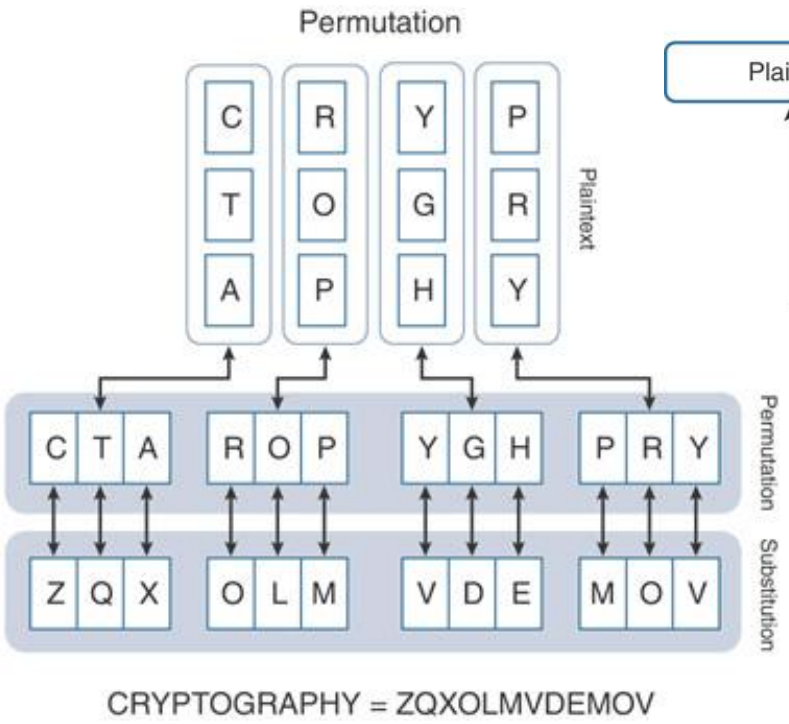
Mohsen Kheradmand

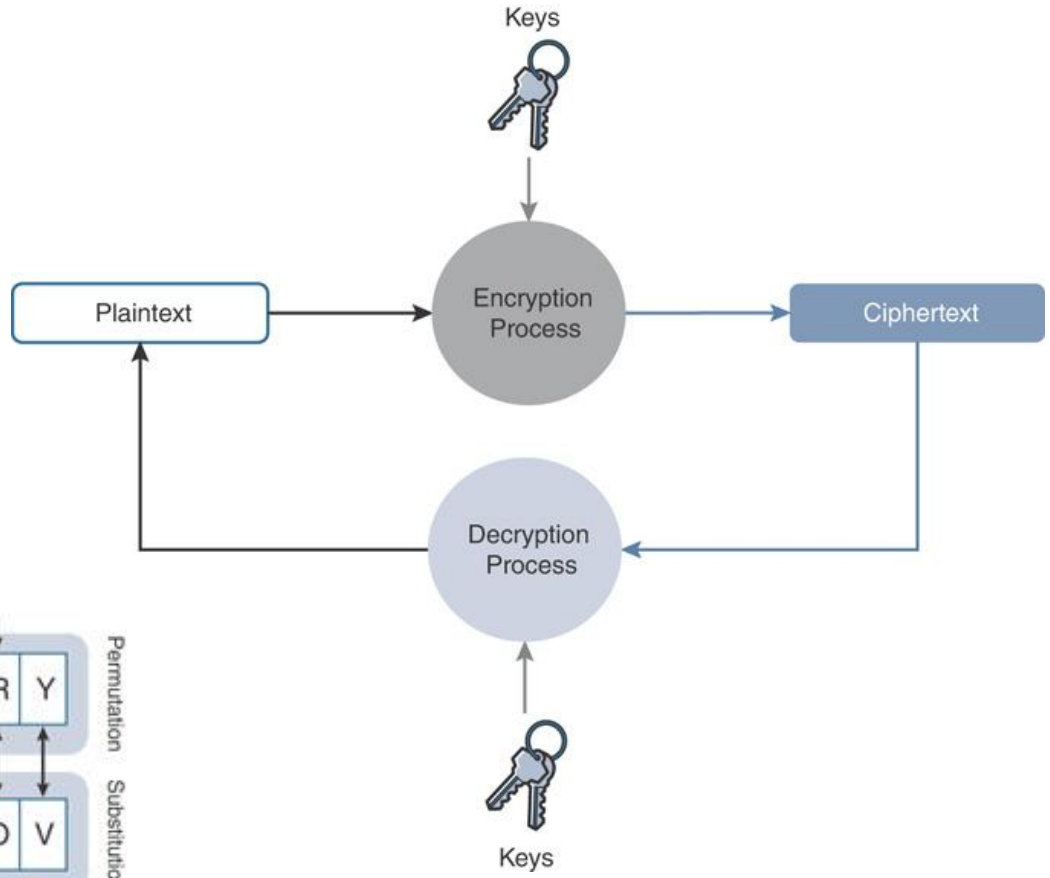
Traffic decryption

- 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





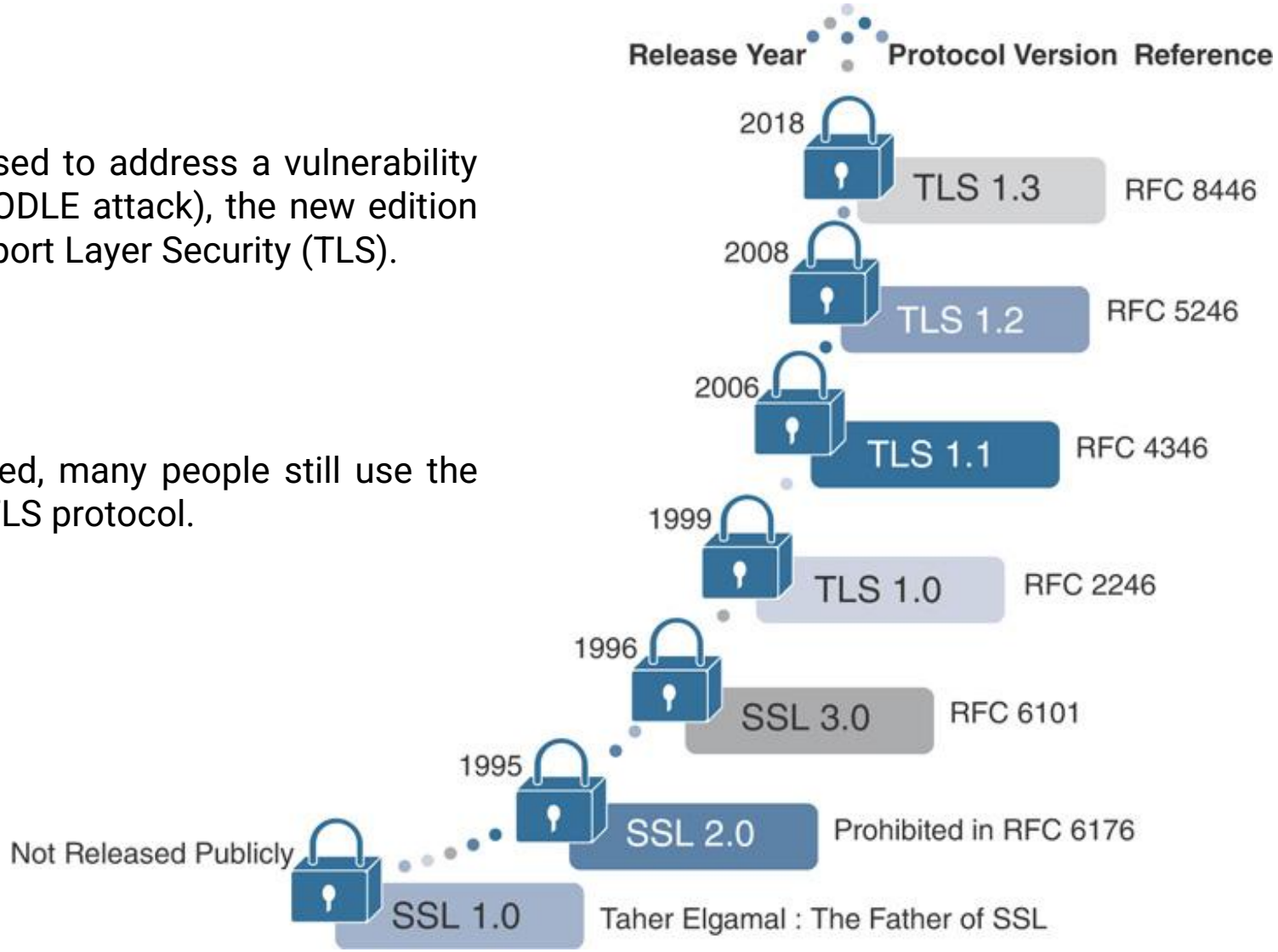


MohsenKheradmand

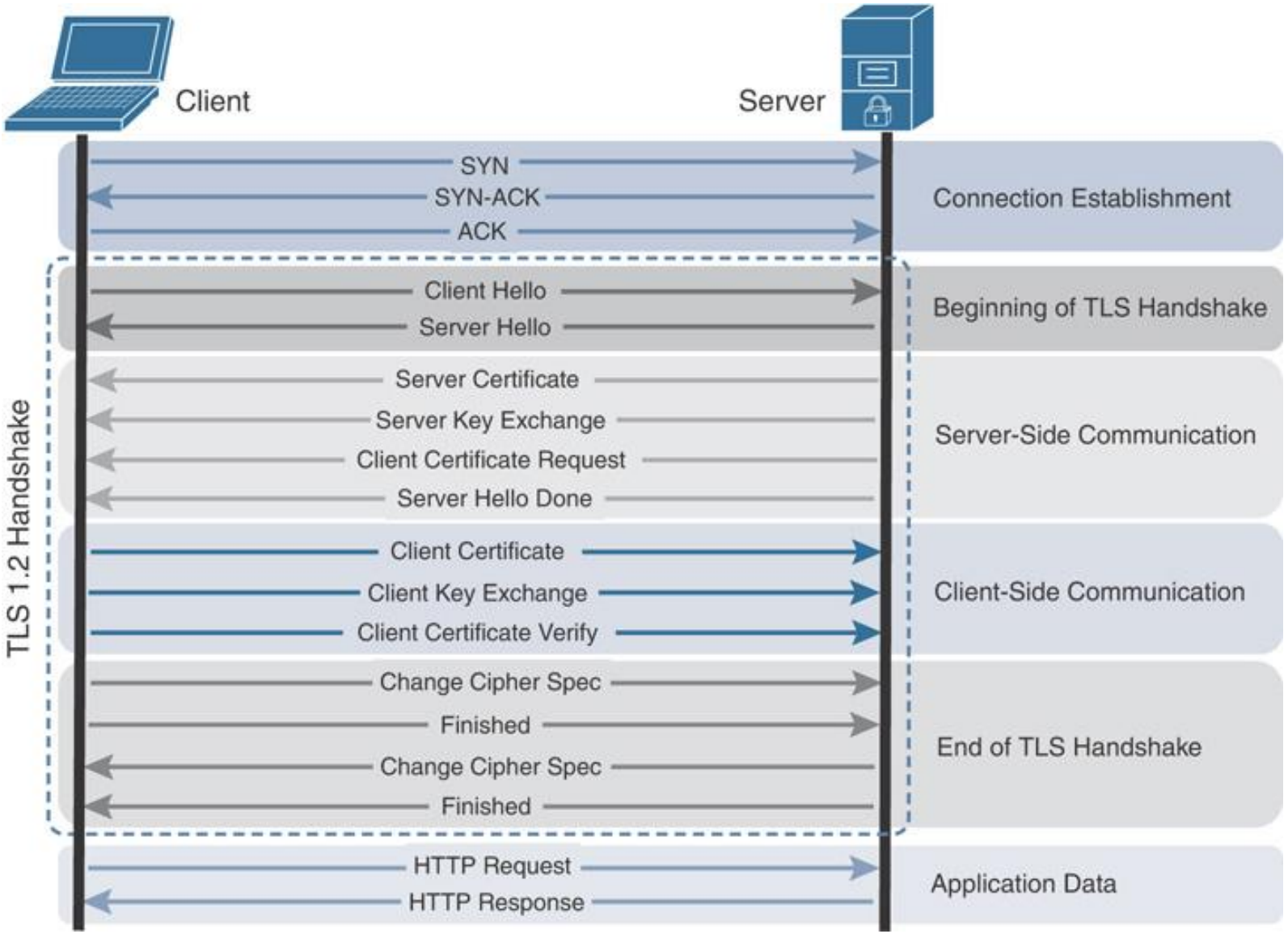
Overview of SSL and TLS Protocols

- 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



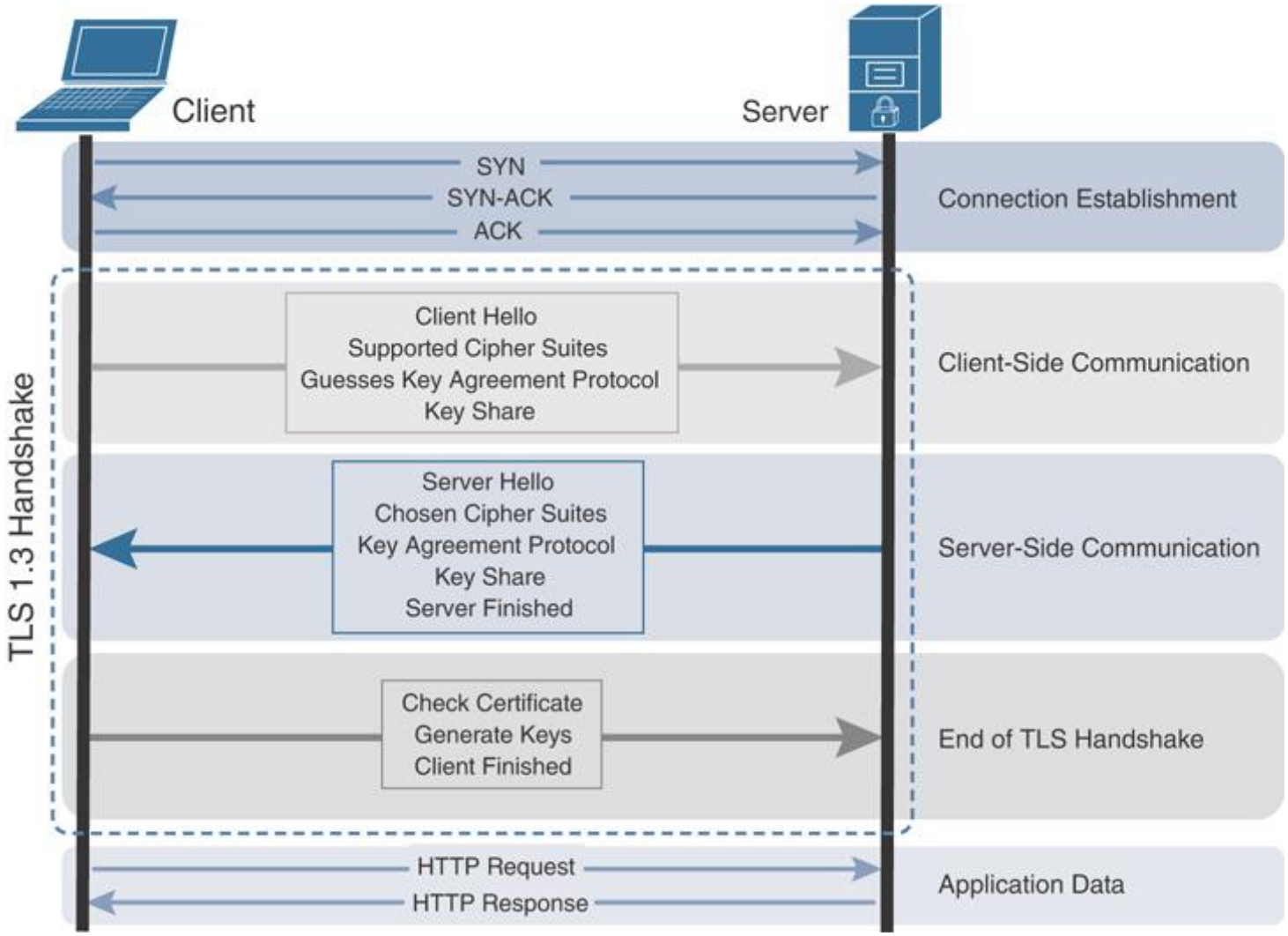
✓ TLS 1.2 requires two round trips to complete its handshake.

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

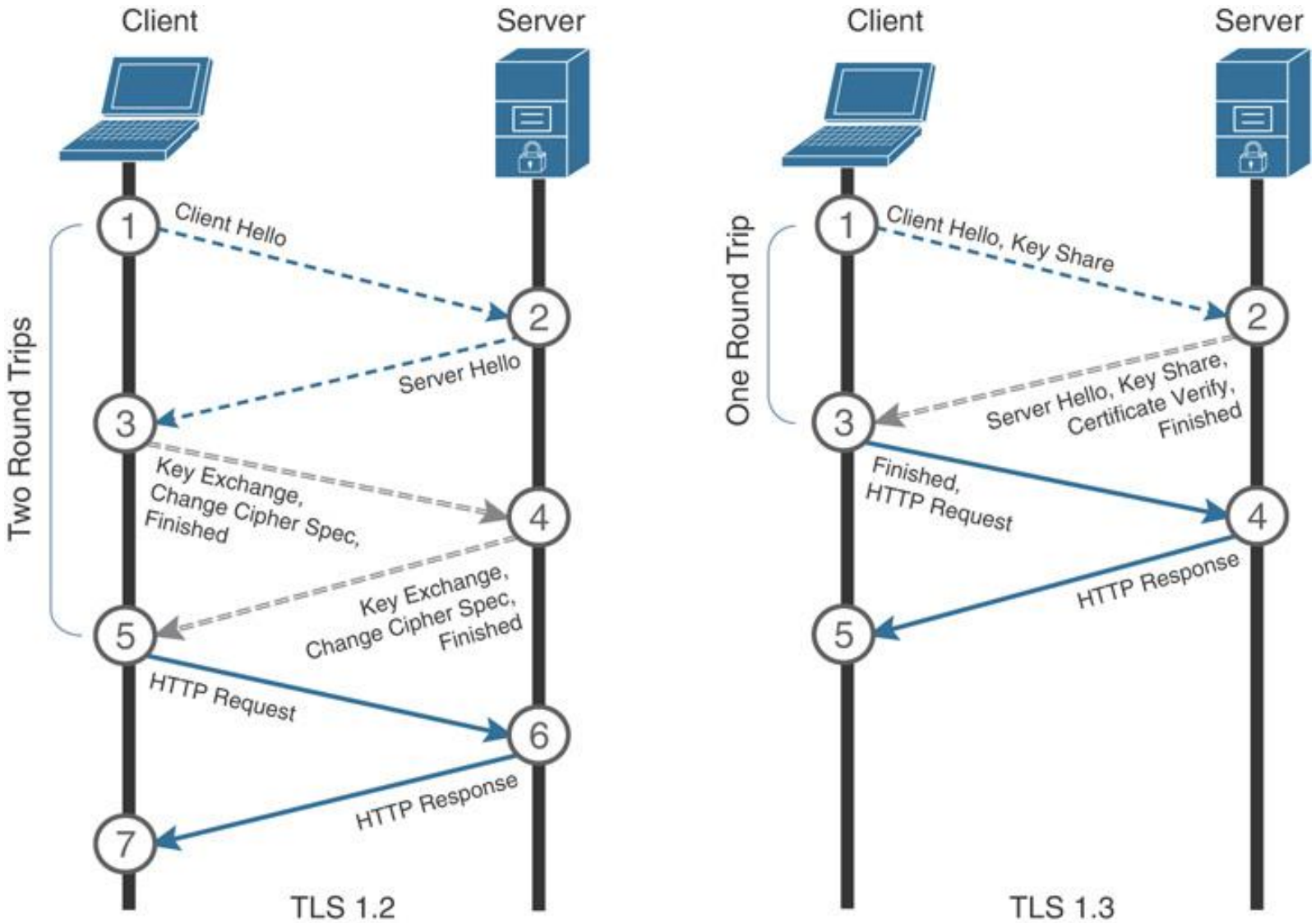
1) TCP three- way handshake (SYN, SYN-ACK, ACK)
2) start TLS Hello message between the client and server
3) Negotiate the security parameters they can support and exchange encryption keys
4) End of TLS handshake and begin Data request/response

➢ 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

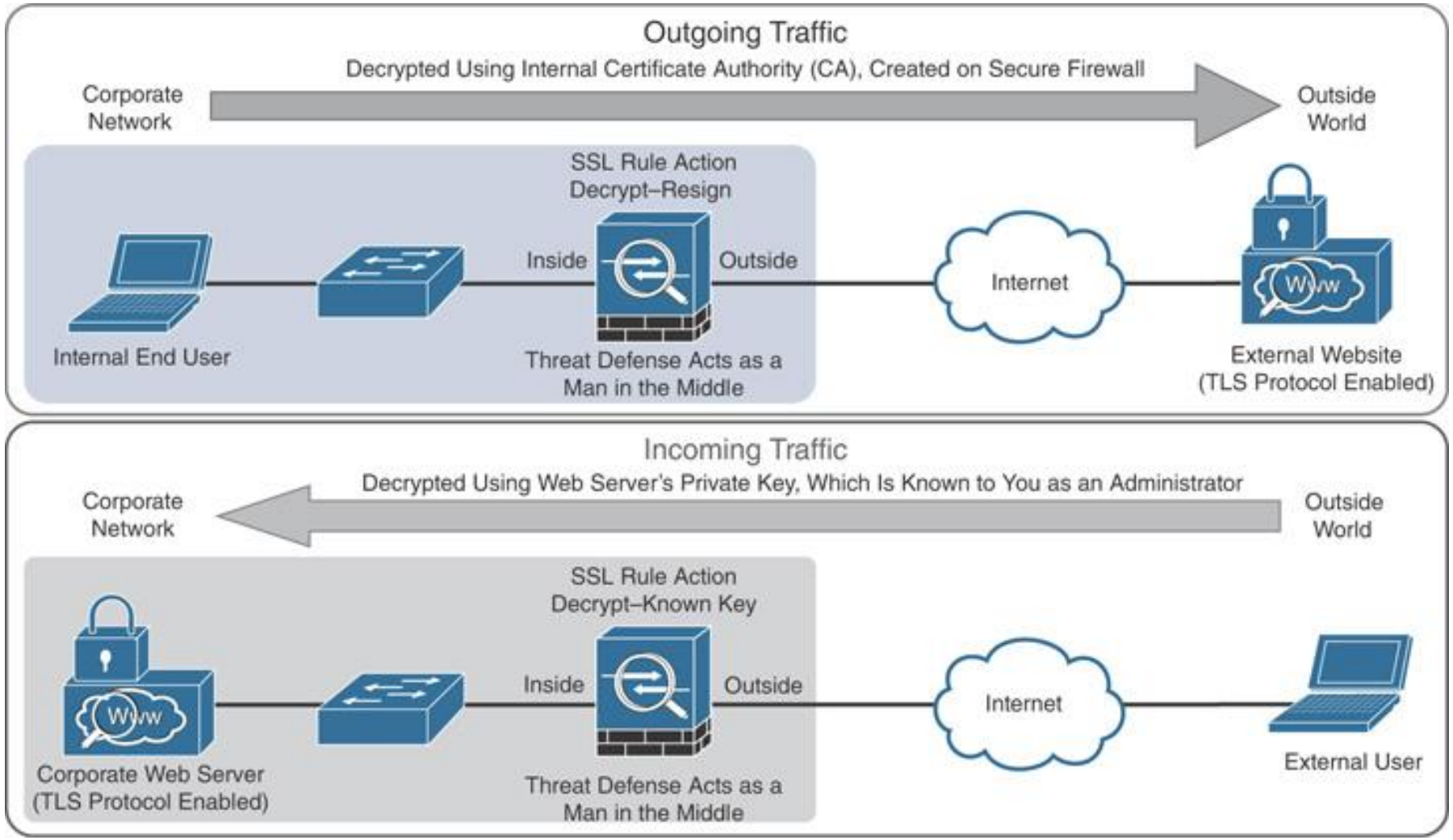


- Round Trips Comparison by TLS 1.2 and TLS 1.3



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



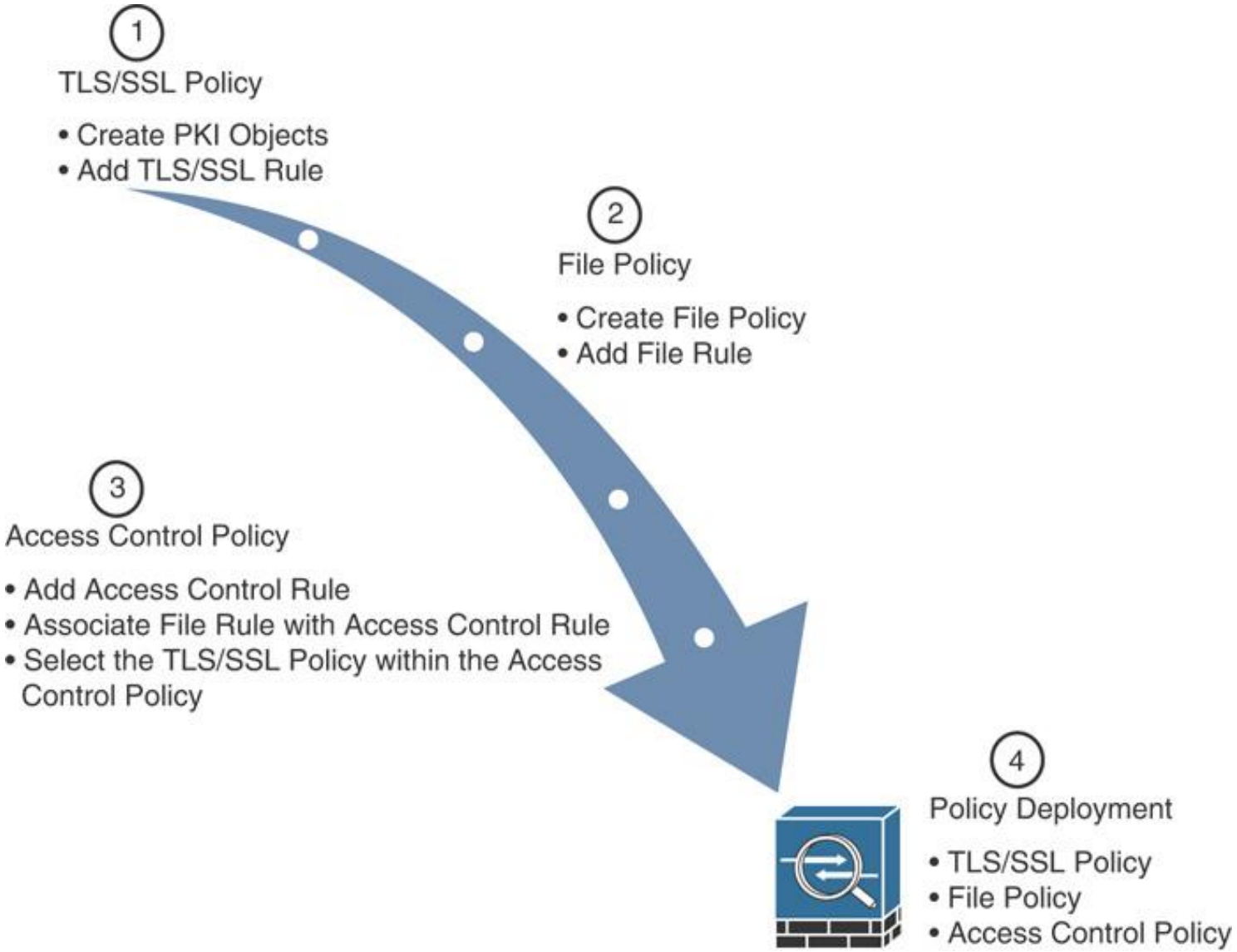
Decryption Techniques on Secure Firewall

- Secure Firewall offers two techniques to traffic:

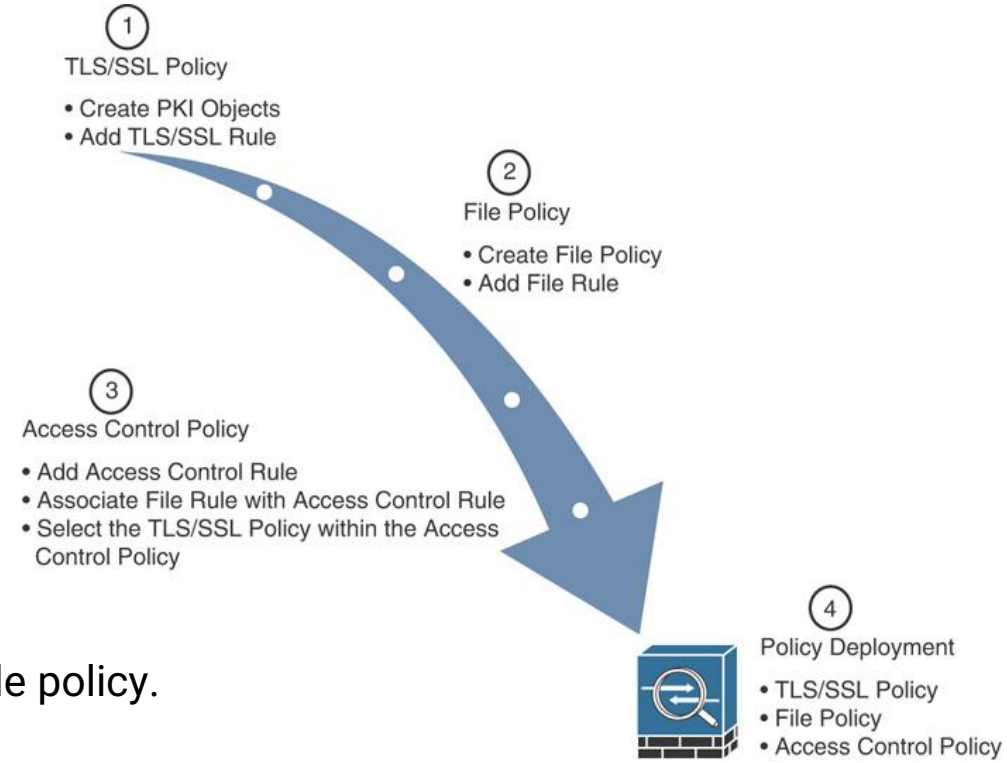
  - Decryption by resigning (for outgoing traffic) :
    - Decrypt outgoing traffic from an internal end-user when the user attempts to connect to an external web server
    - Secure firewall acts like a proxy or man-in-the-middle
    - Completes the SSL handshake on behalf of the client , perform traffic 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.

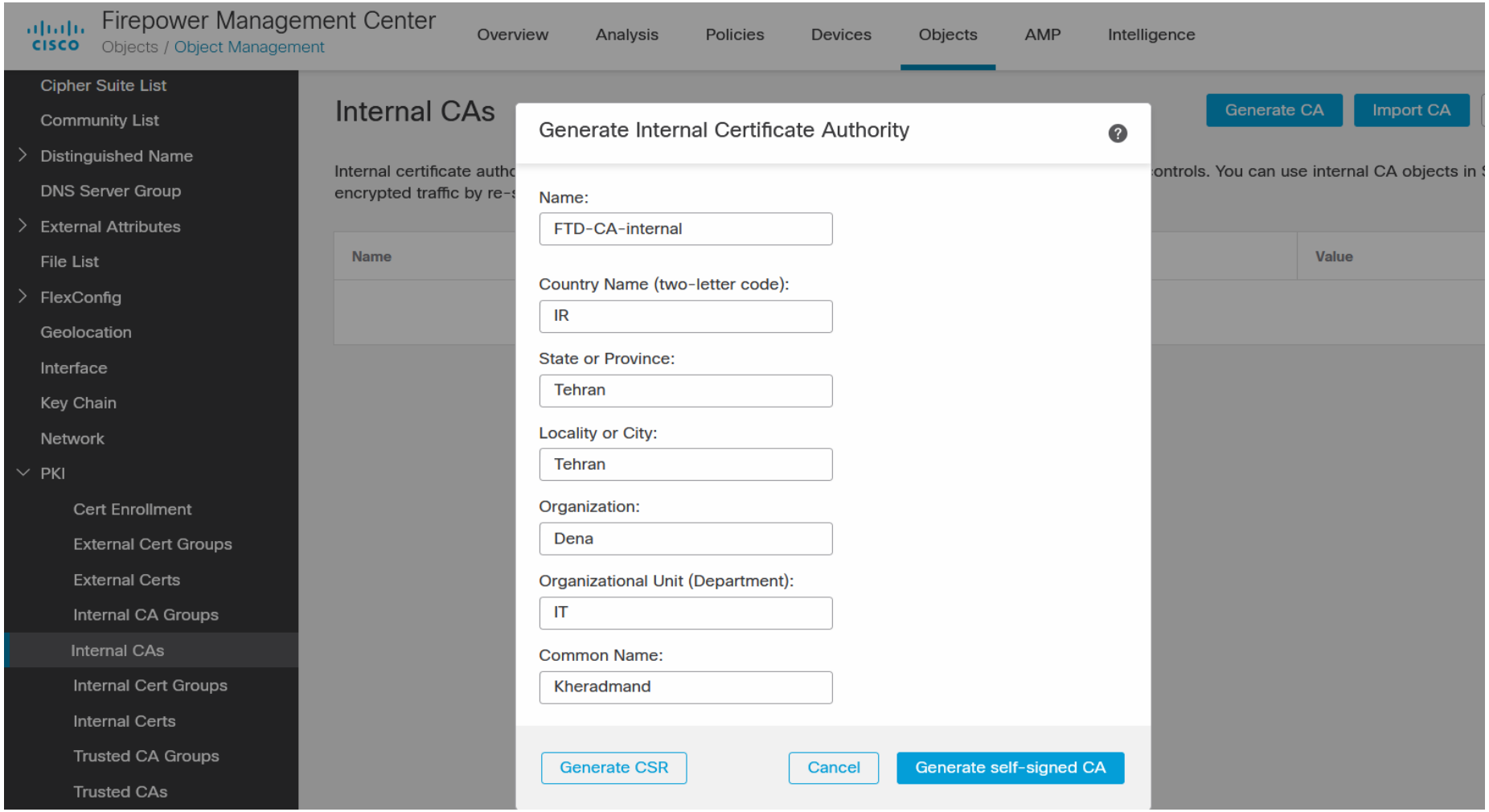
   - ❑ Alternatively, an intrusion policy could be used to show deep packet inspection

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

4) Finally deploy the policy to the FTD

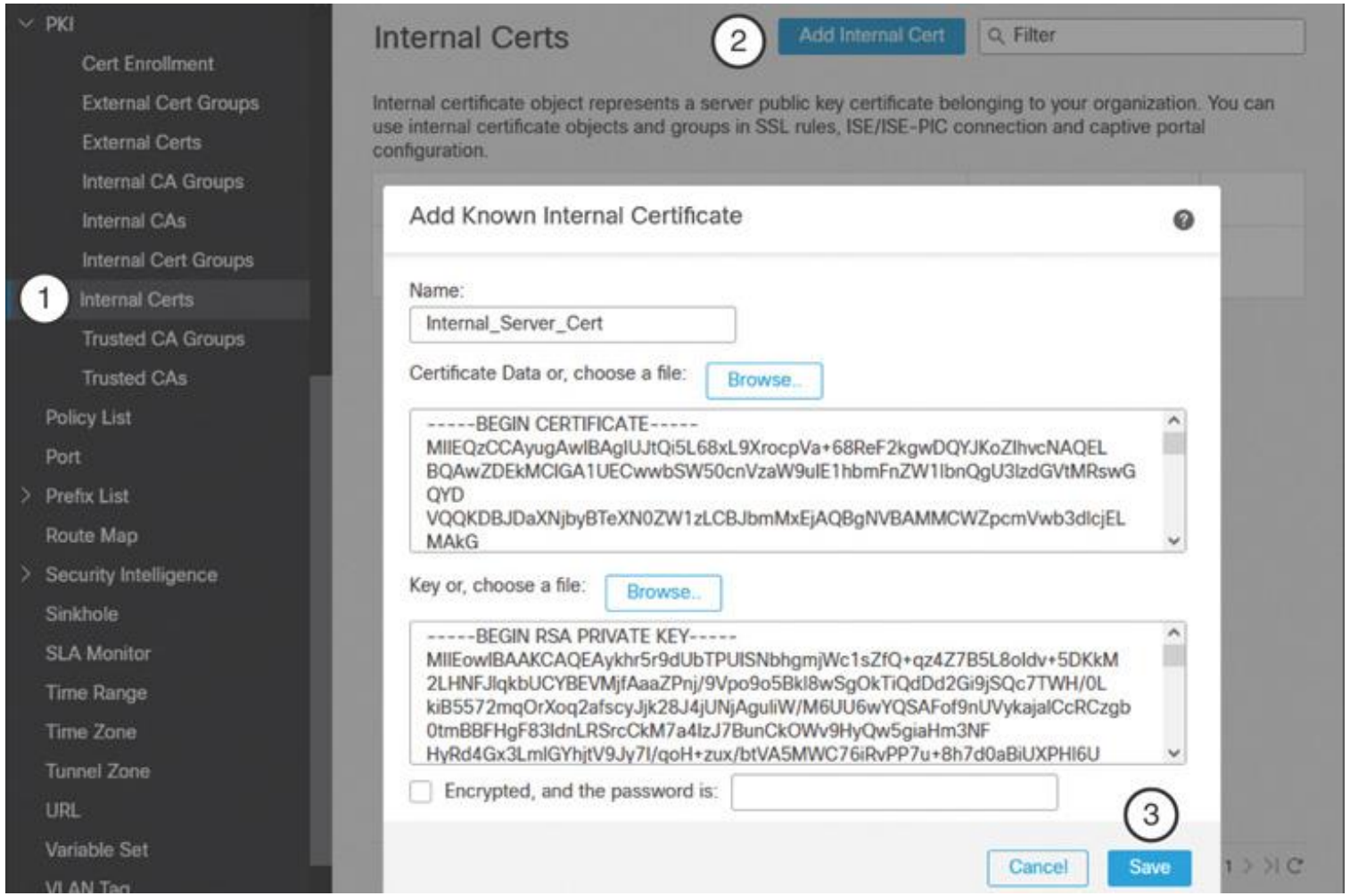
PKI Objects

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



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



Objects > Object Management

1) PKI > Internal Certs

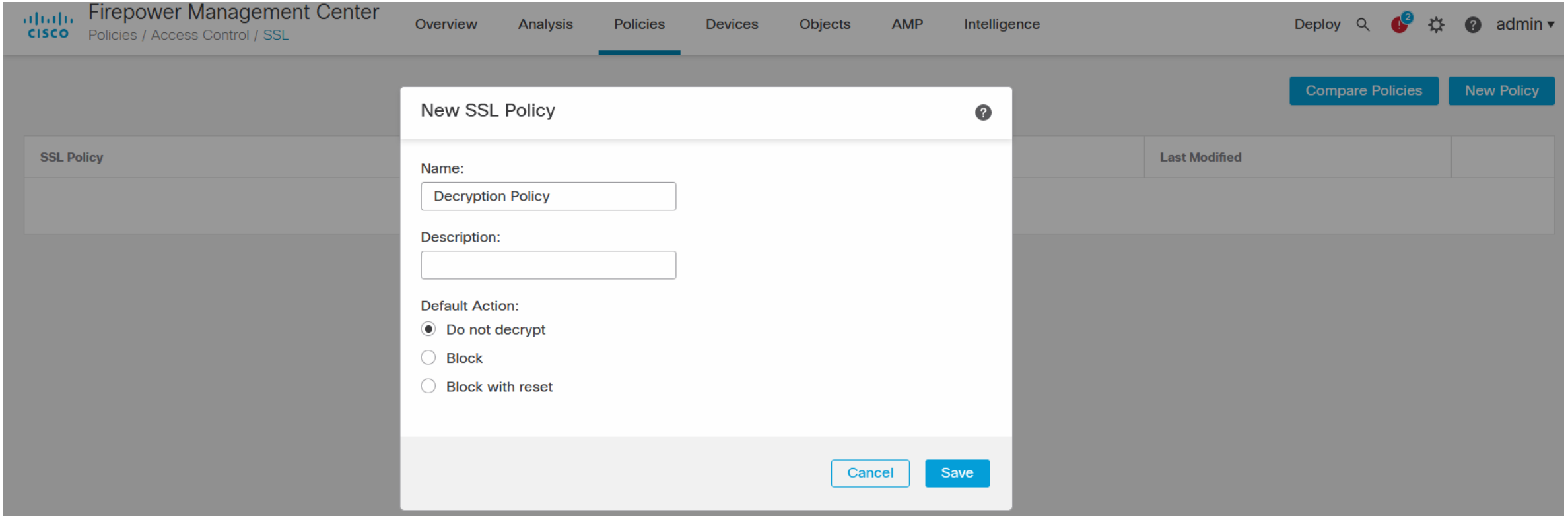
2) Add Internal Cert
   - Enter a name for Cert
   - Import the internal web server Cert
   - Also import the private key of web server

3) Click Save

MohsenKheradmand

SSL Policy

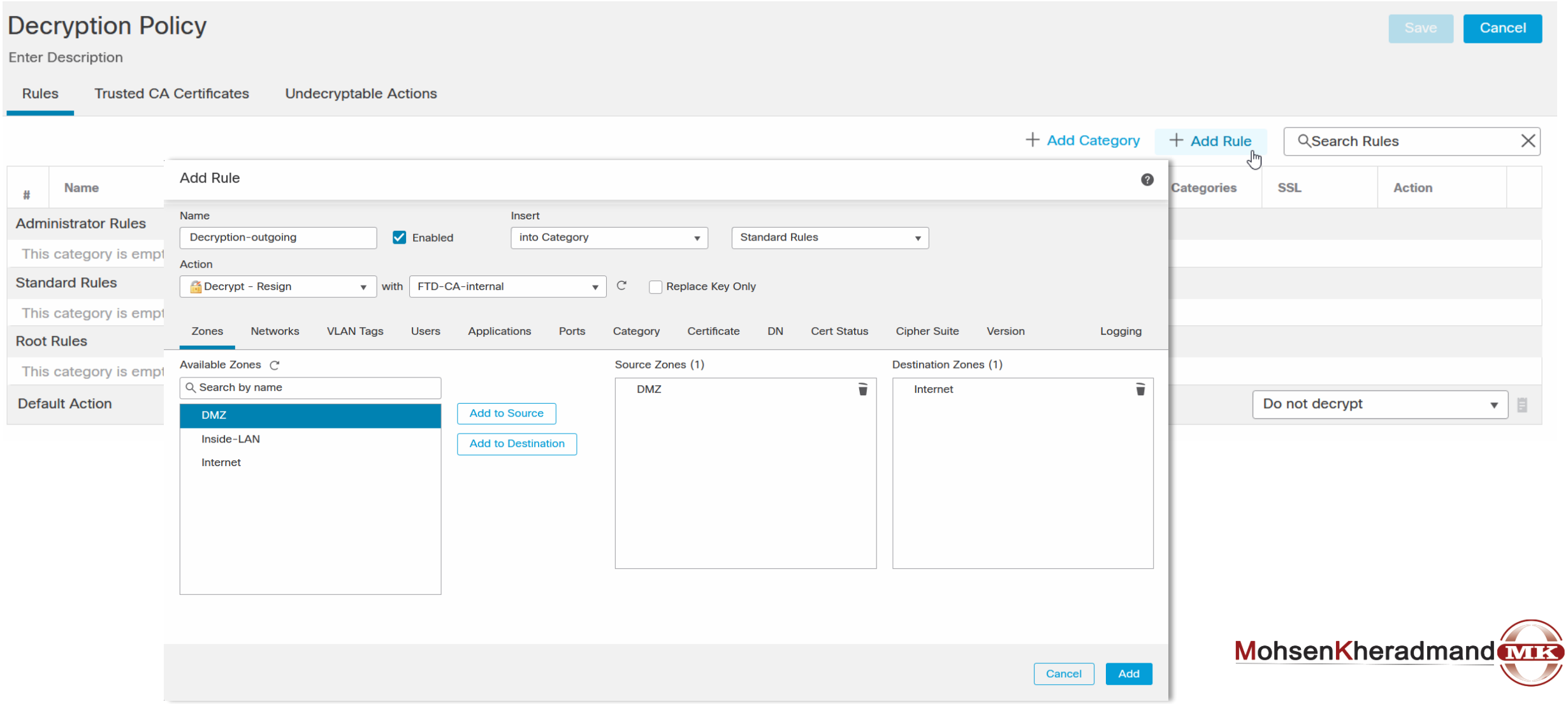
1) Policies > Access Control > SSL
2) click the New Policy
3) Enter a name and select Do not decrypt as a default action



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

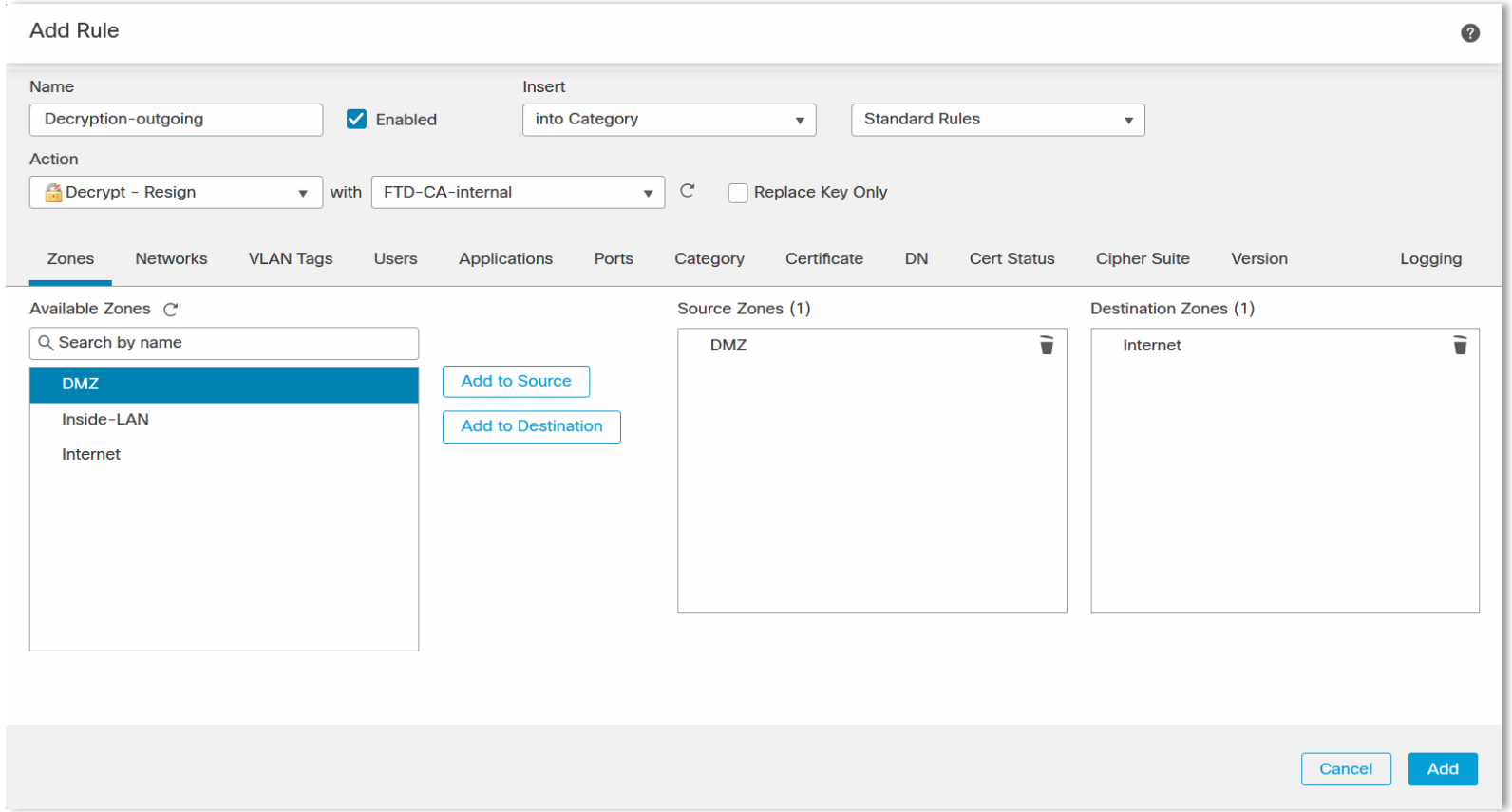
SSL Policy

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



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

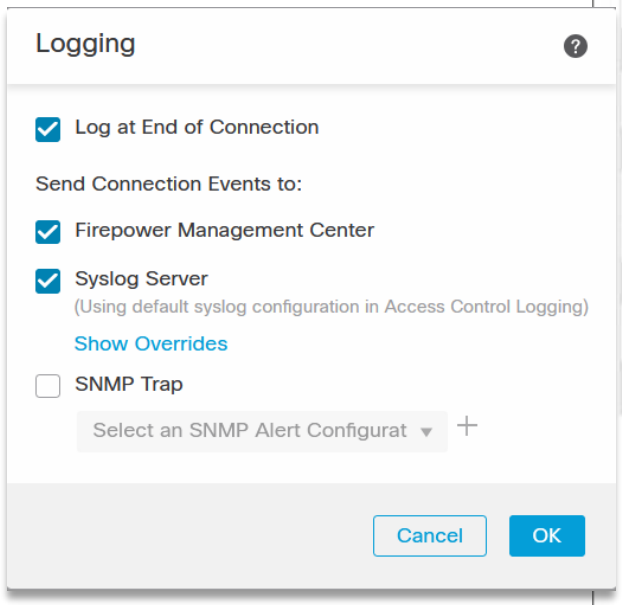


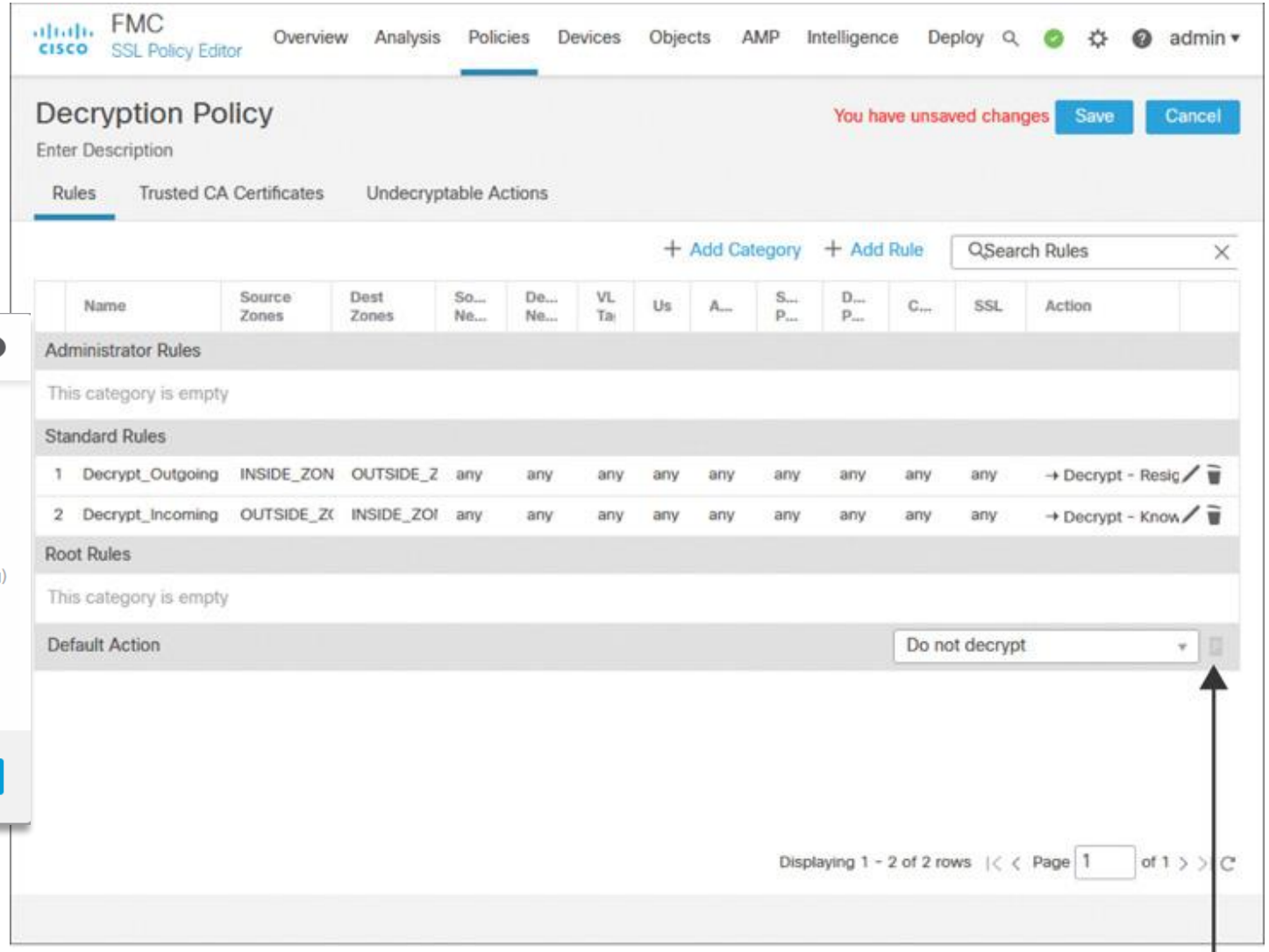
Actions :

- **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





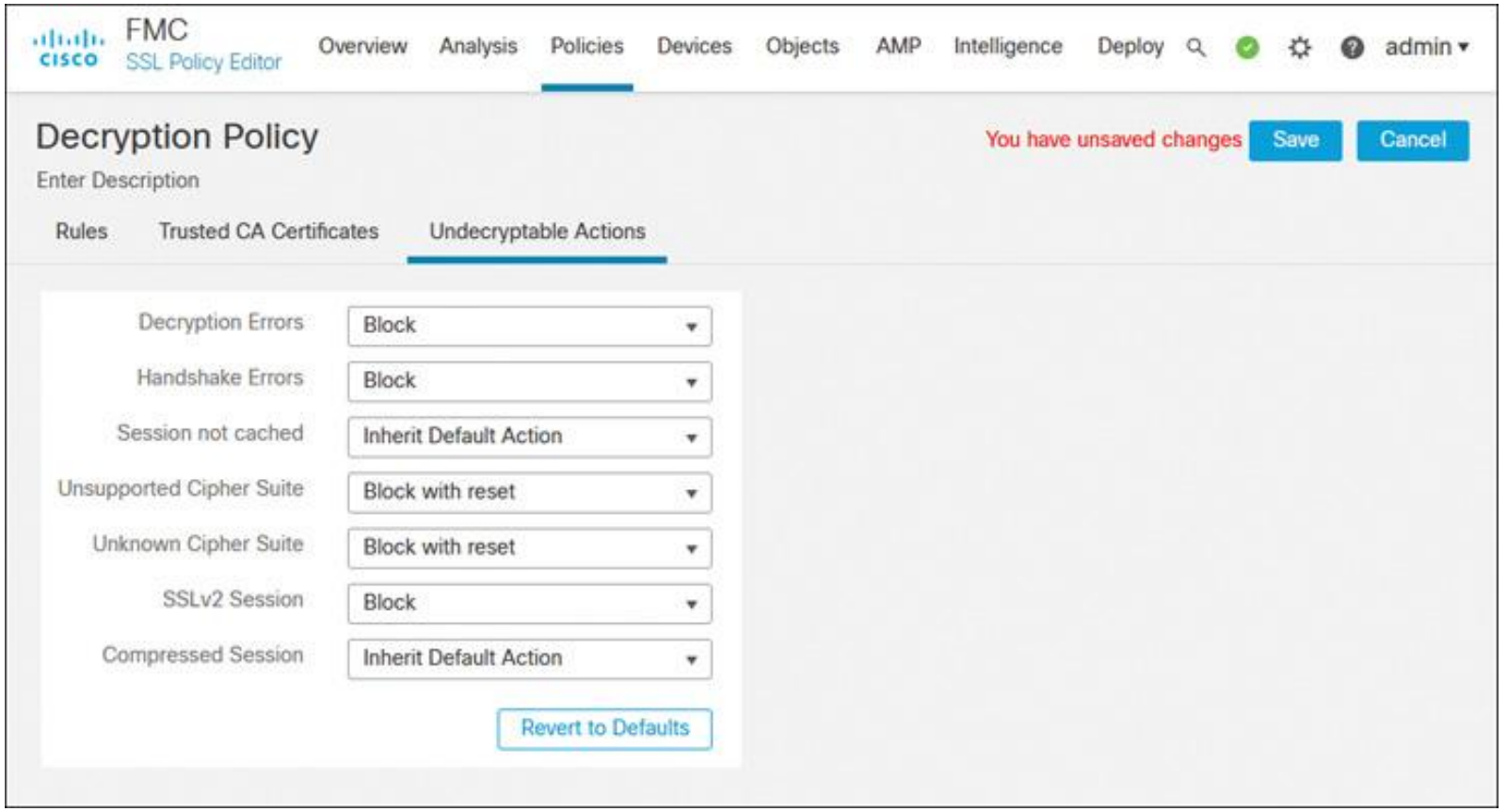
Logging Icon for Default Action

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

SSL Policy

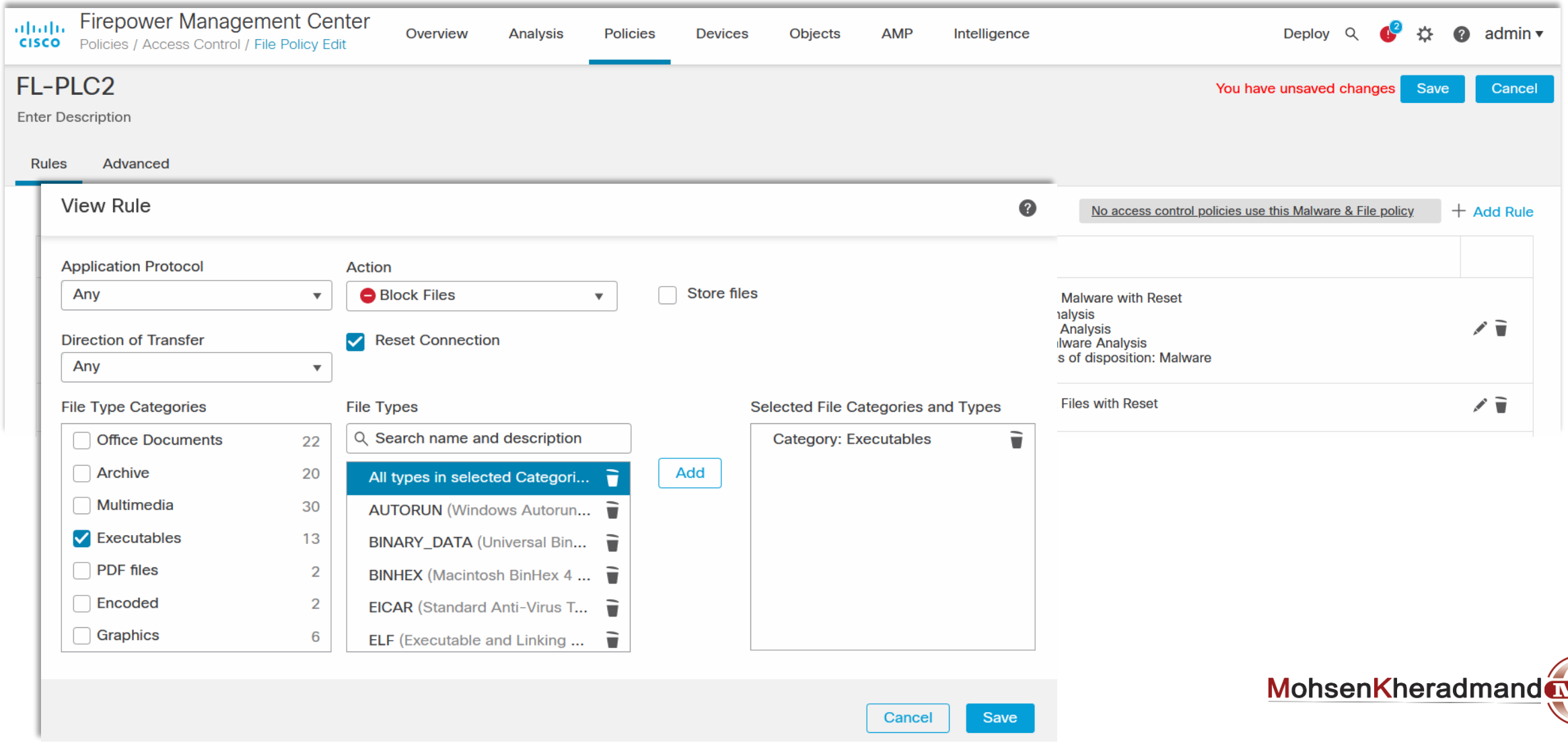
11) Finally, define how Secure Firewall will handle the undecryptable traffic



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

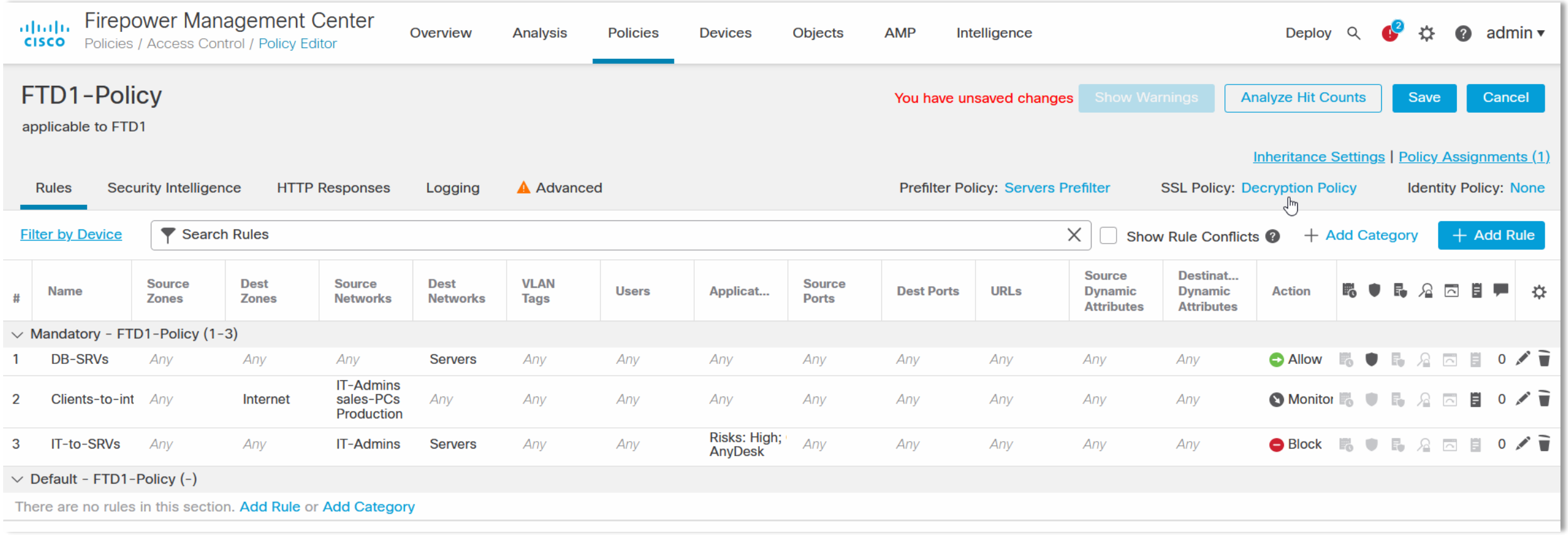
File Policy

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



Access Control Policy

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



Verification

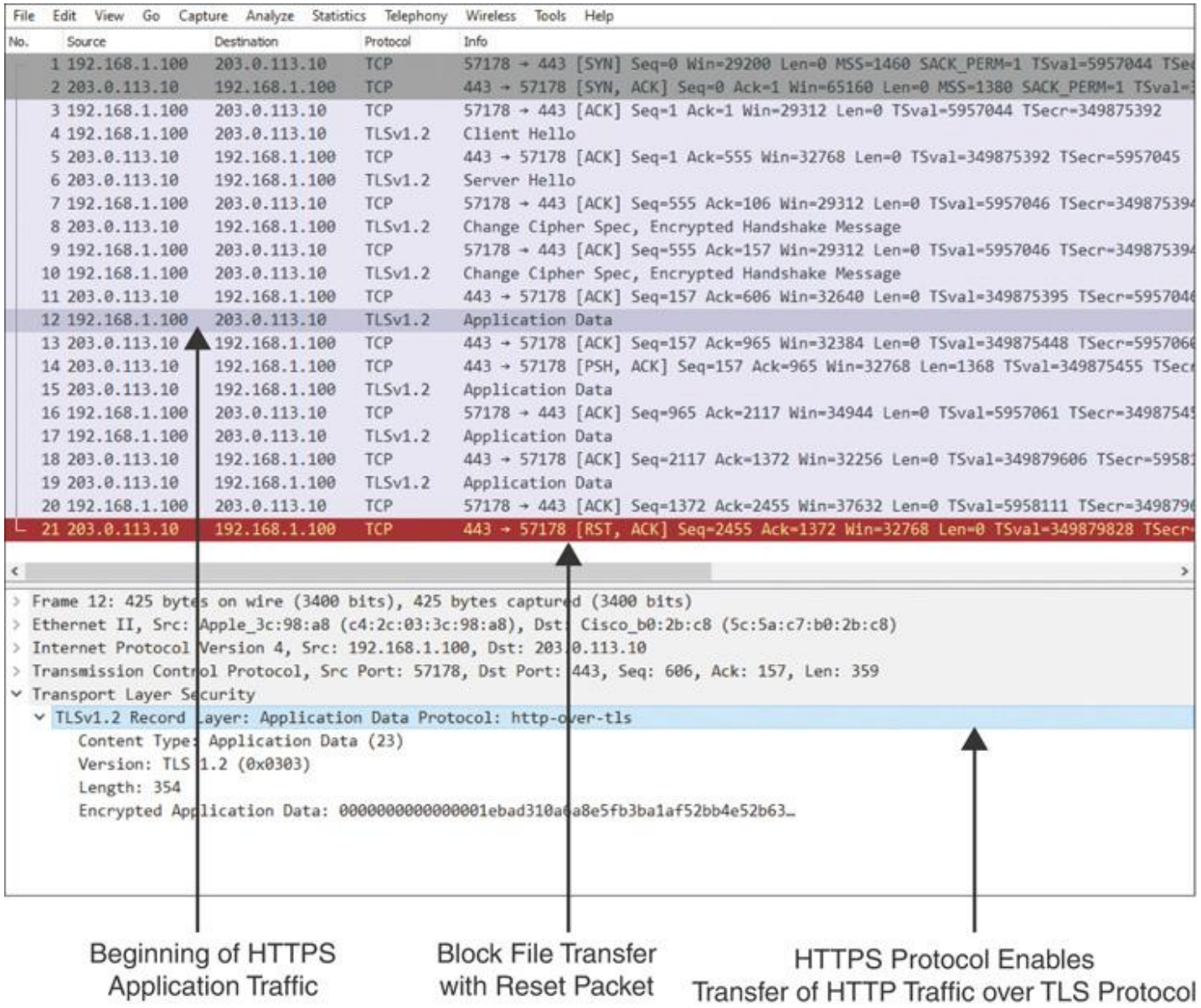
Example :

- 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

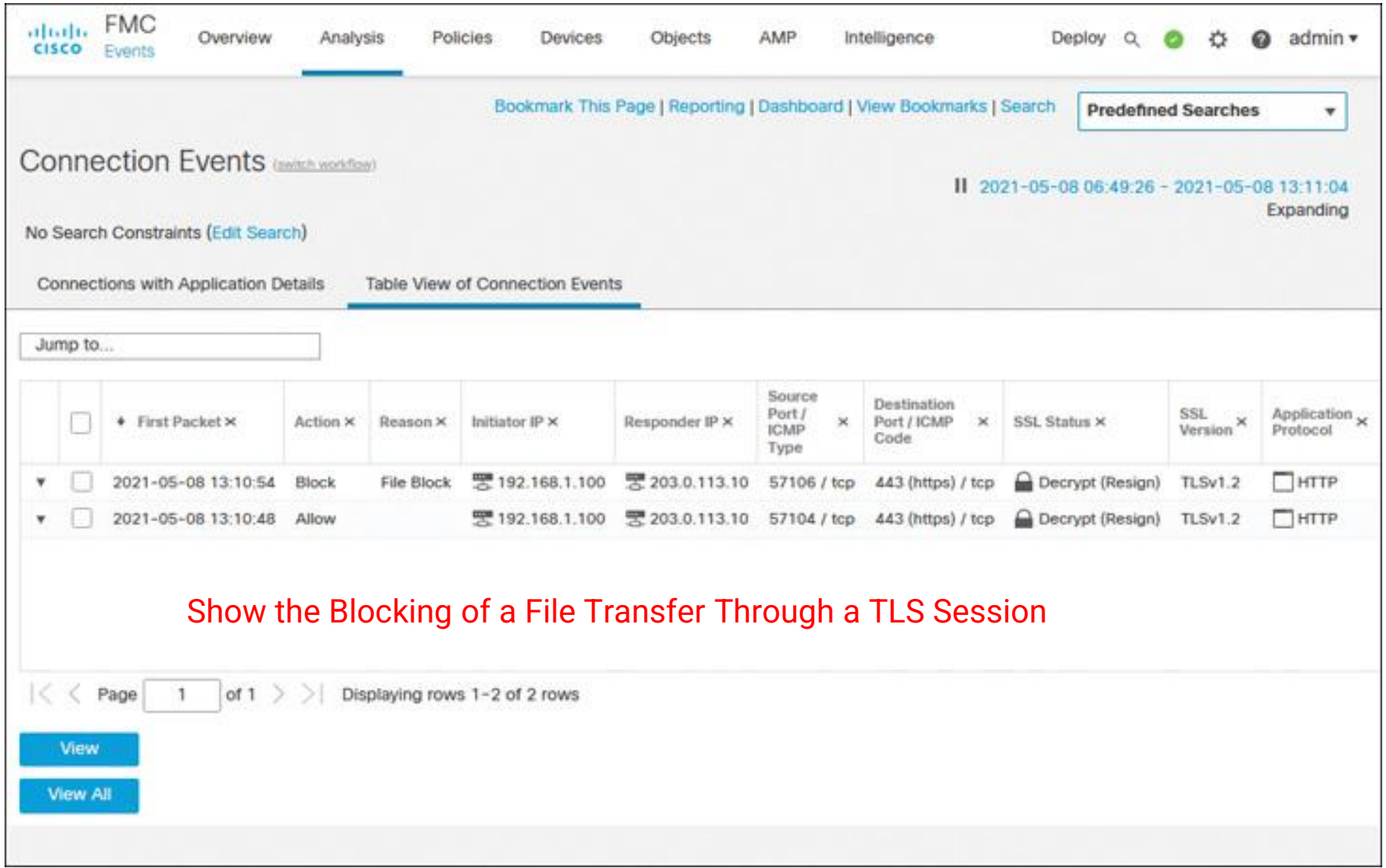
Example :



Capture of an HTTPS session

Verification

Analysis > Connections > Events

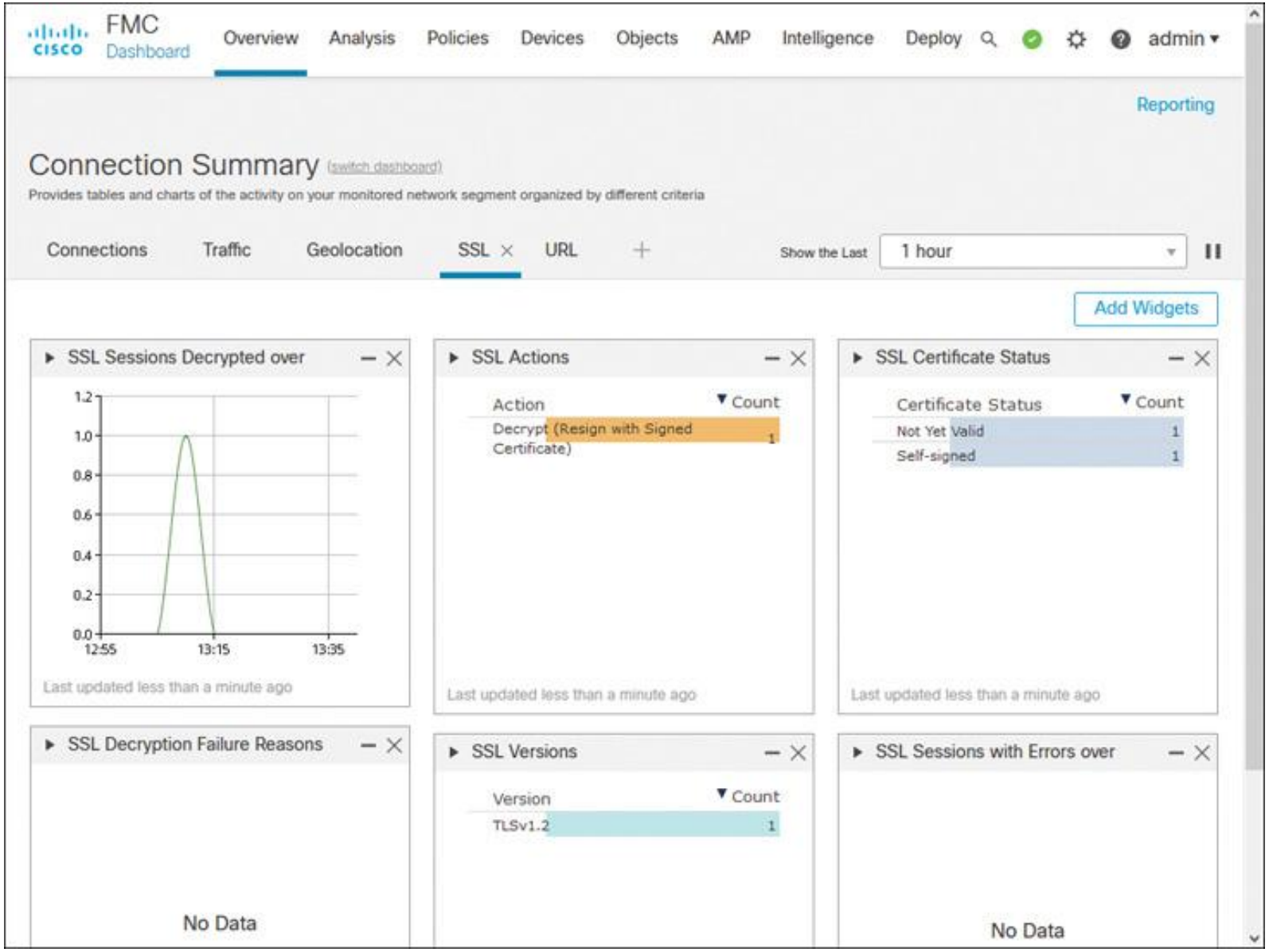


MohsenKheradmand

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