Securing Networks with

Cisco FTD

Chapter 18

Quality of Service (QoS)

Mohsen Kheradmand

Quality Of Service

Converged Network Quality Issues

- Lack of bandwidth:

  Multiple flows compete for a limited amount of bandwidth.

  Solution : Limiting the rate of traffic to manage the bandwidth of a network and to ensure quality of service (QoS)

- End-to-end delay (fixed and variable):

  Packets have to traverse many network devices and links that add up to the overall delay

- Variation of delay (jitter):

  Sometimes there is a lot of other traffic, which results in increased delay.

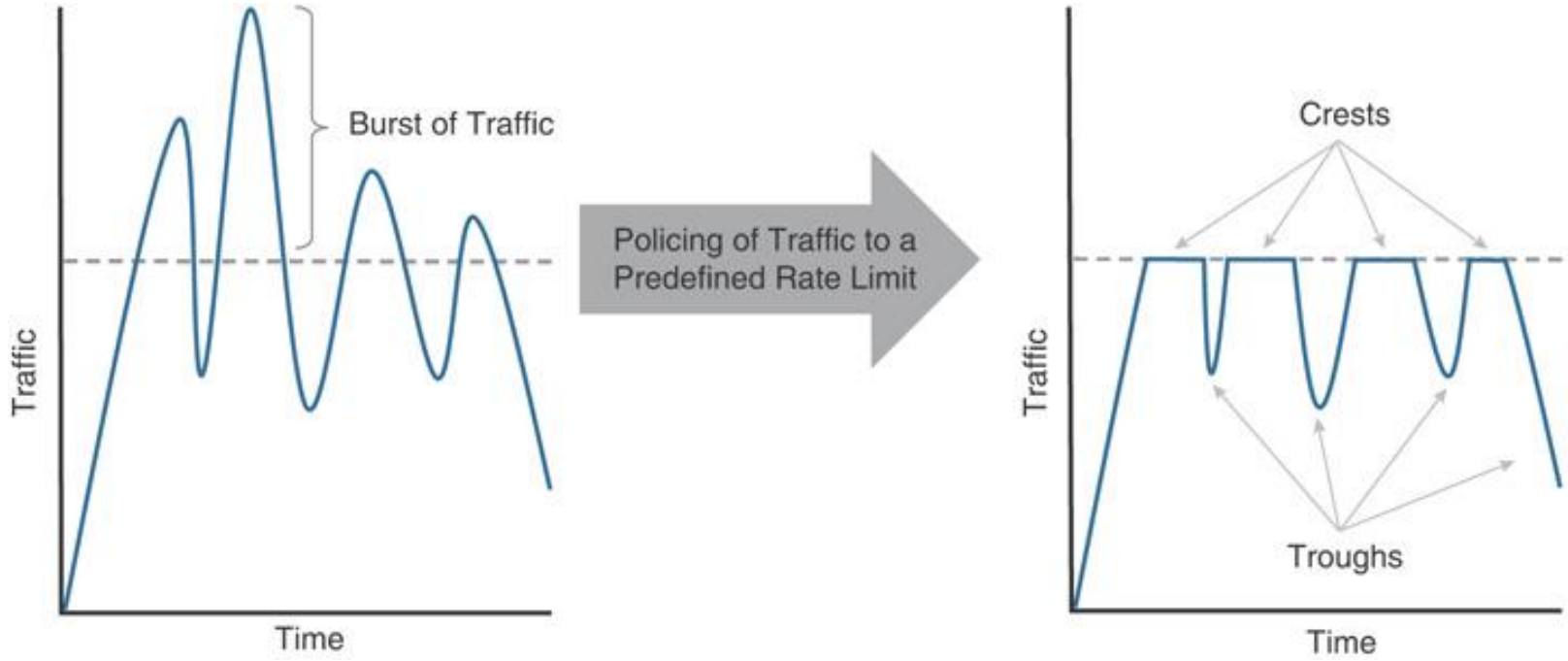
- Packet loss:

  Packets may have to be dropped when a link is congested.

Quality of Service Essentials

- A threat defense implements the traffic policing mechanism to limit the rate of traffic
- The threat defense drops excessive traffic when the traffic rate reaches a predefined limit
- The threat defense does not support traffic shaping (queues excessive traffic in a buffer rather than dropping it for later transmission.)

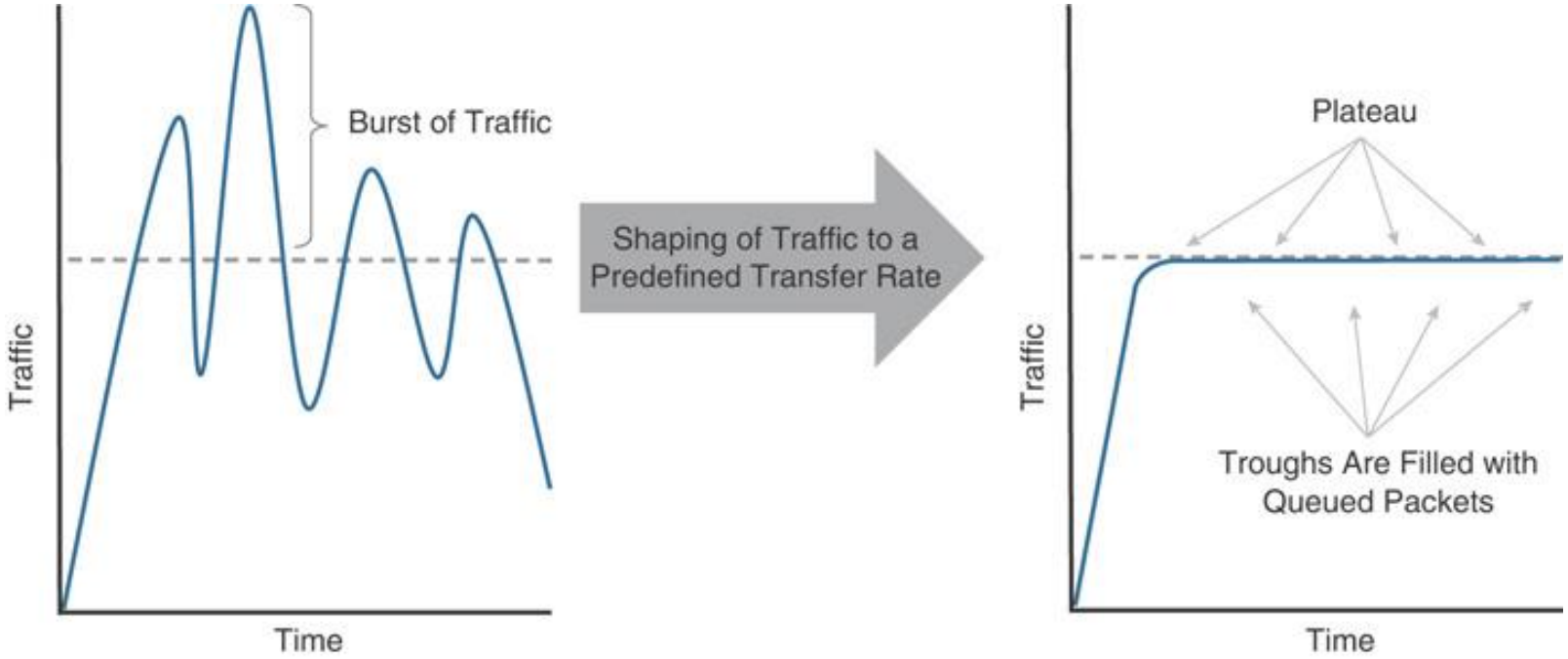
Traffic Policing Method
Dropping Excessive Traffic



Quality of Service Essentials

- A threat defense implements the traffic policing mechanism to limit the rate of traffic
- The threat defense drops excessive traffic when the traffic rate reaches a predefined limit
- The threat defense does not support traffic shaping (queues excessive traffic in a buffer rather than dropping it for later transmission.)

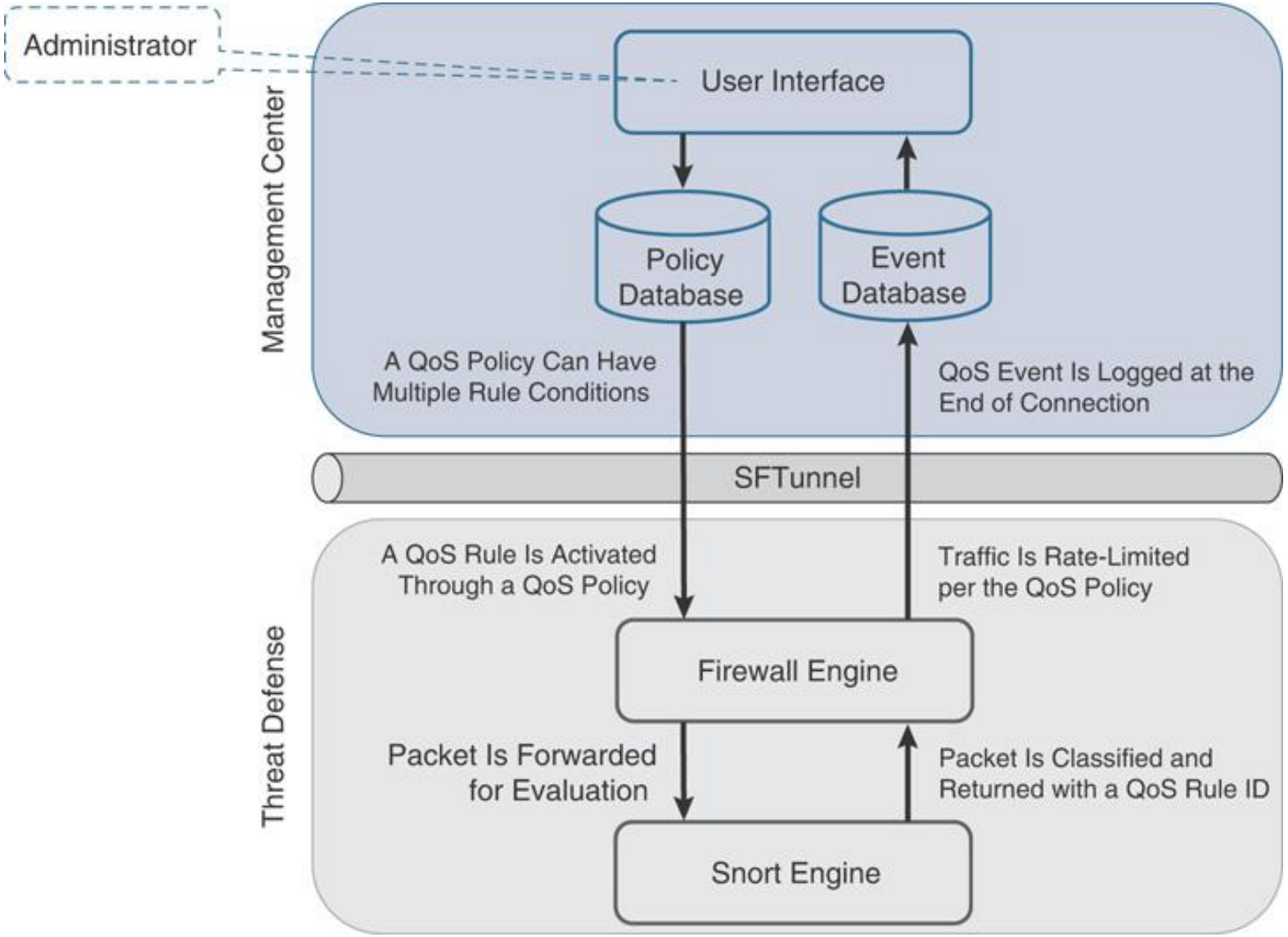
rate-limited by the shaping mechanism



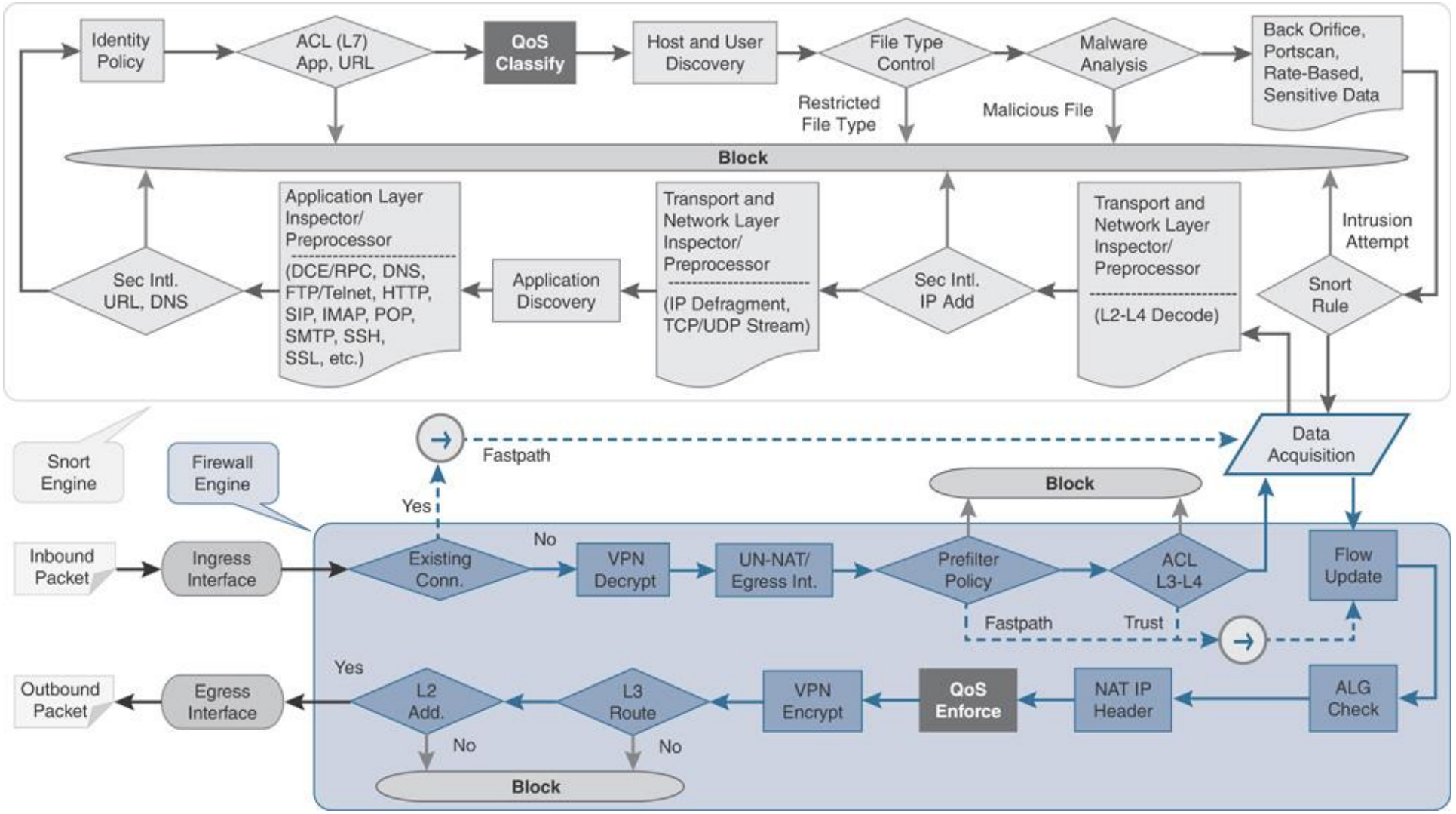
Quality of Service Essentials

- You can activate only one QoS policy on a threat defense at any given time
- However, you can add multiple QoS rules (up to 32 QoS rules) within a single QoS policy.
- Each QoS rule must be associated with a source and destination interface, where both of them have to be routed interfaces
- You cannot apply a QoS policy to an interface that is in inline mode, passive mode, or switched mode.
- You can set separate upload and download speed limits for the traffic
- The QoS rule can be defined based on advanced parameters (IP address, port number, application, URL, user identity , Etc.)
- The Snort engine evaluates a QoS rule and sends the ID of the matching rule to the firewall engine.

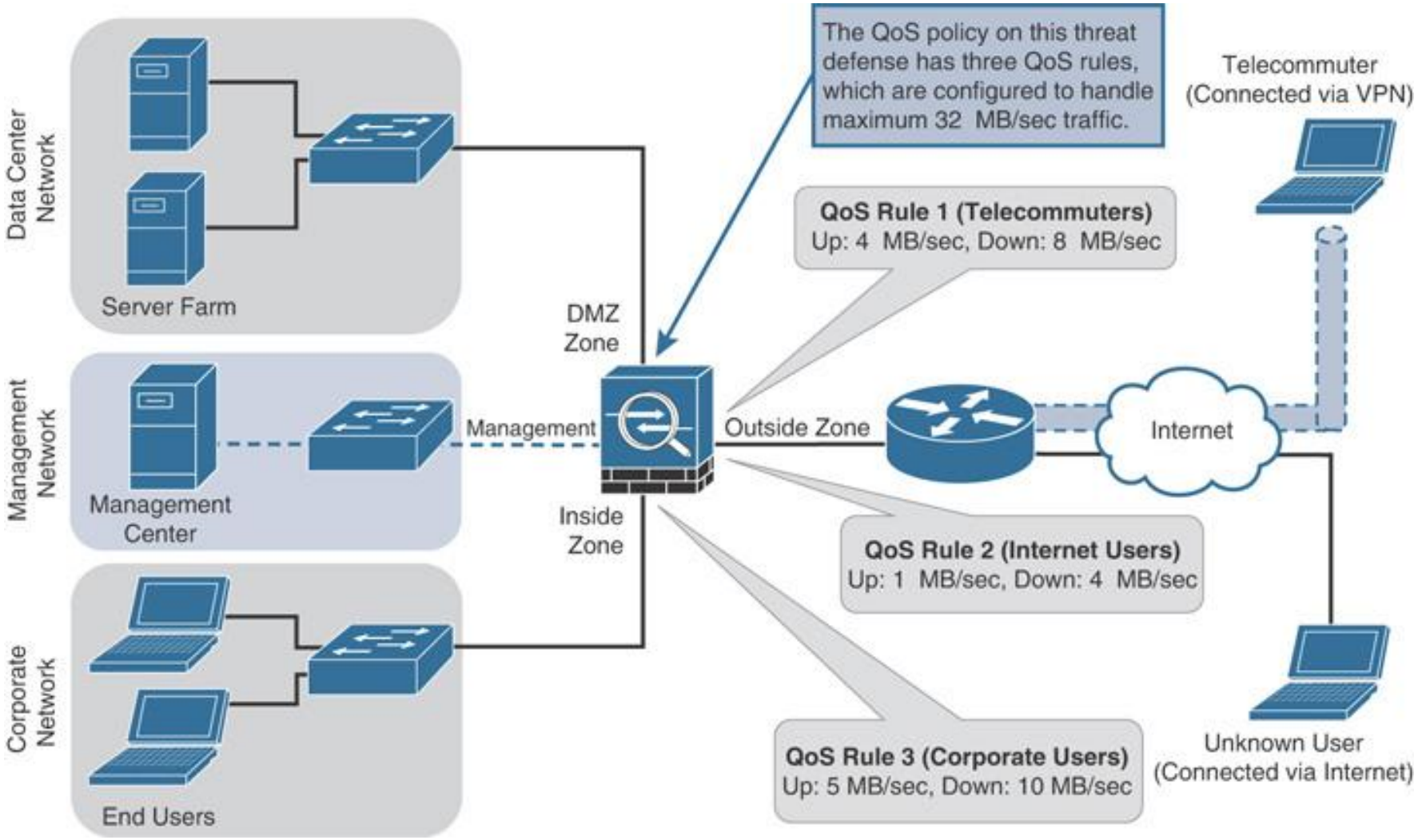
QoS Implementation on the Secure Firewall



- Processing of Packets by Various Components of Security Engines

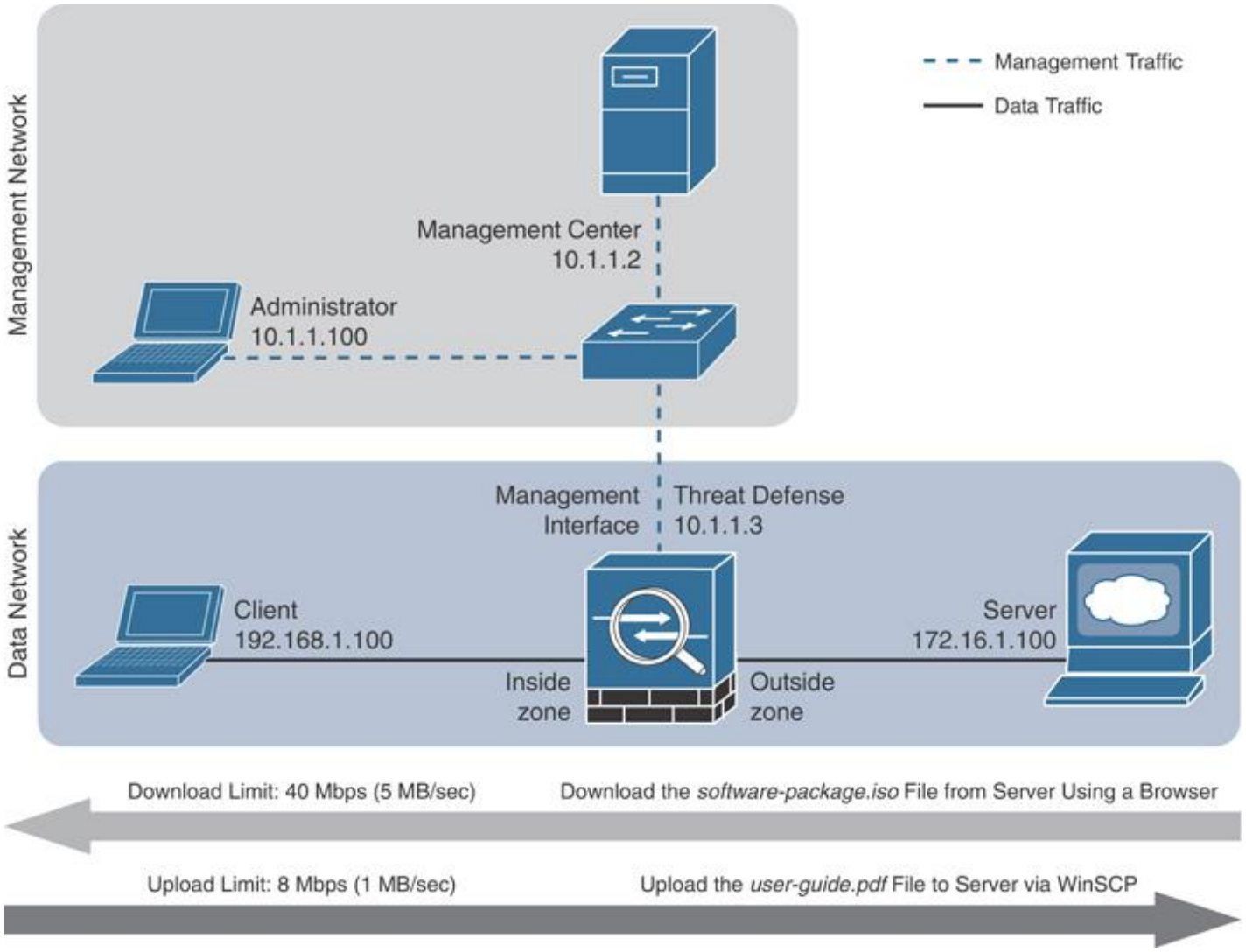


Example of Deploying QOS



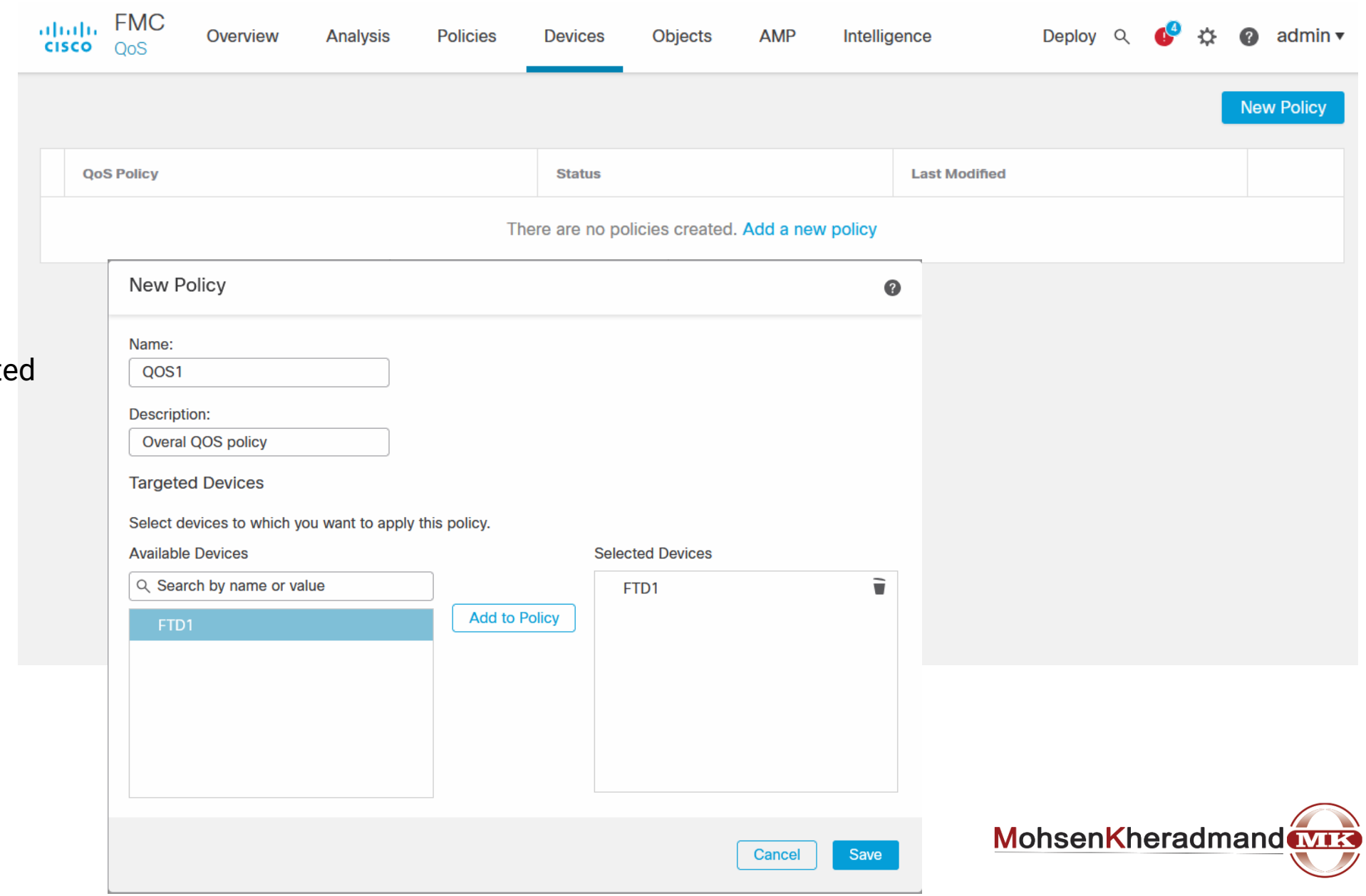
Different QoS Rules Can Be Applied to Different Types of Users

Configuring QoS Policy



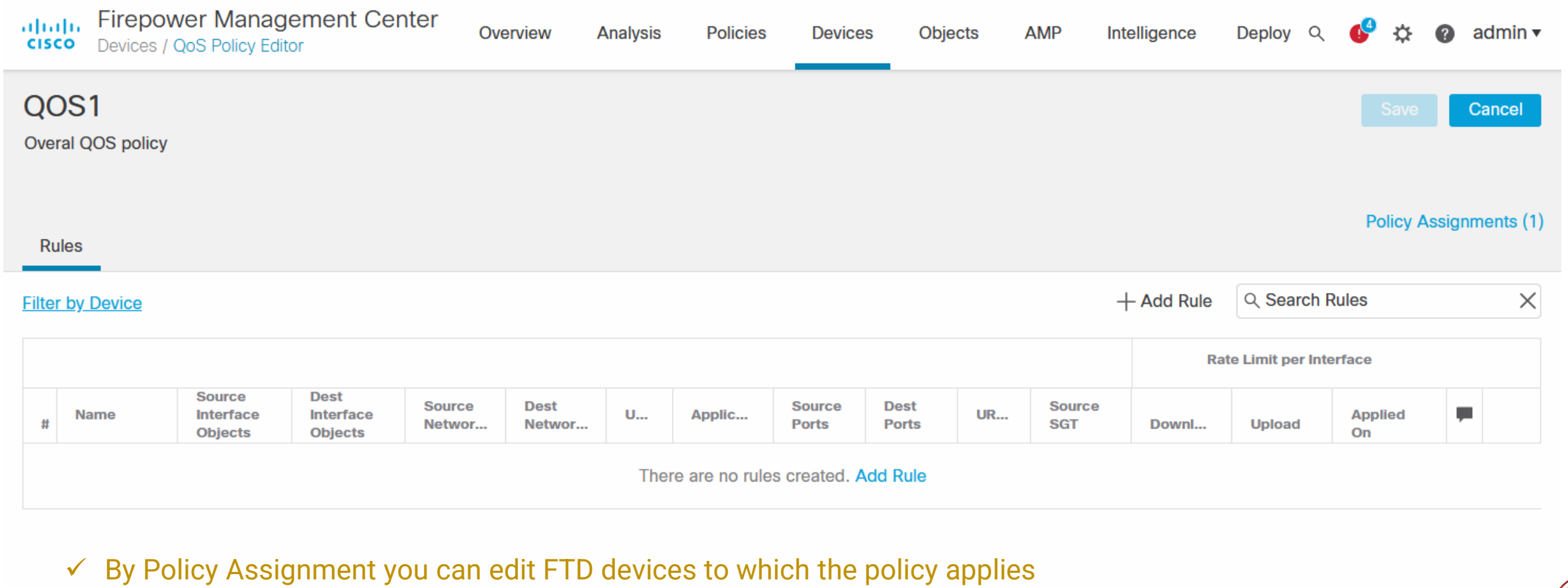
Configuring QoS Policy

- Devices > QoS
- Click the New Policy
- Enter a name for policy
- Add FTD device to selected
- Click save



Configuring QoS Policy

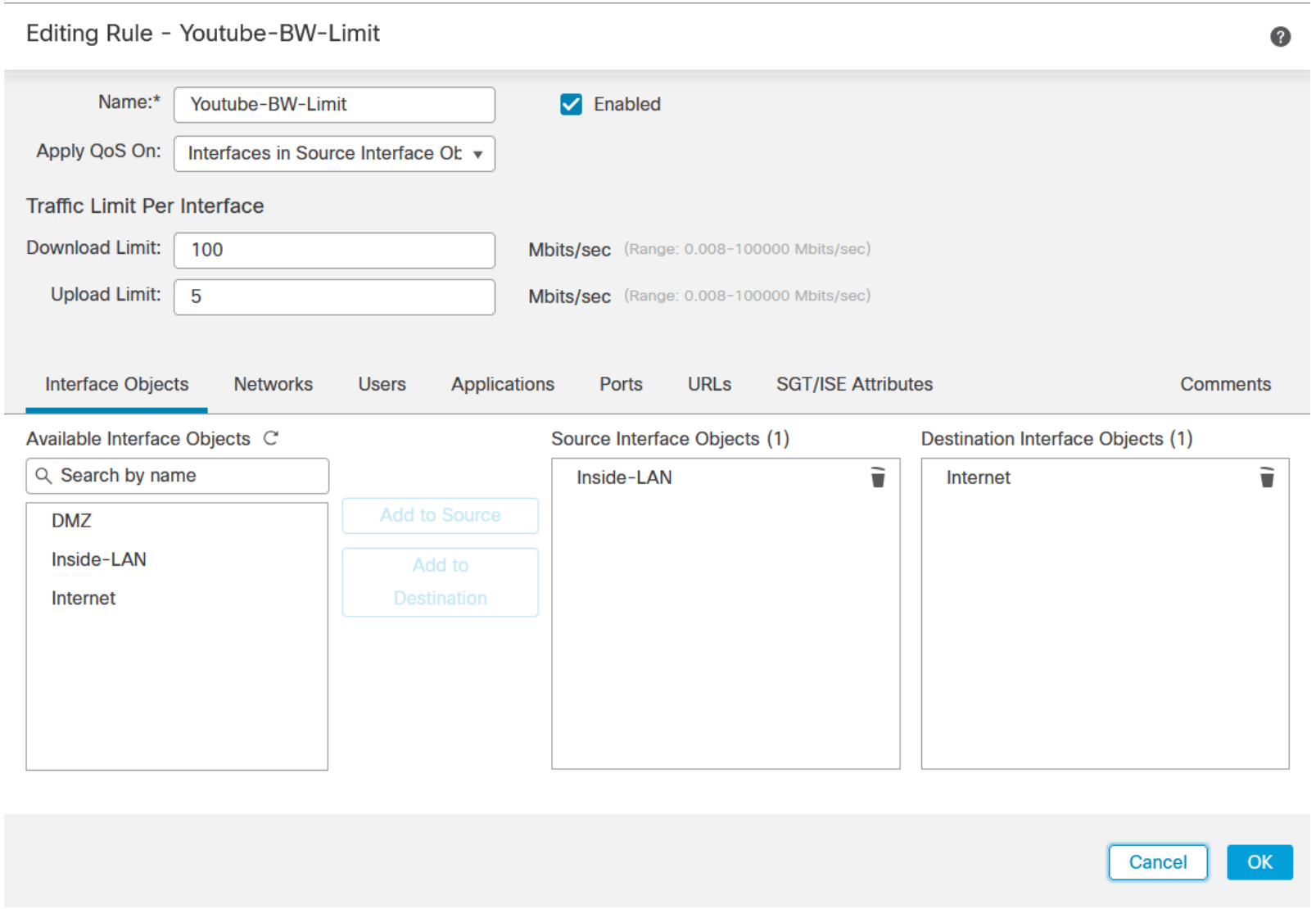
- Click Add Rule



✓ By Policy Assignment you can edit FTD devices to which the policy applies

Configuring QoS Policy

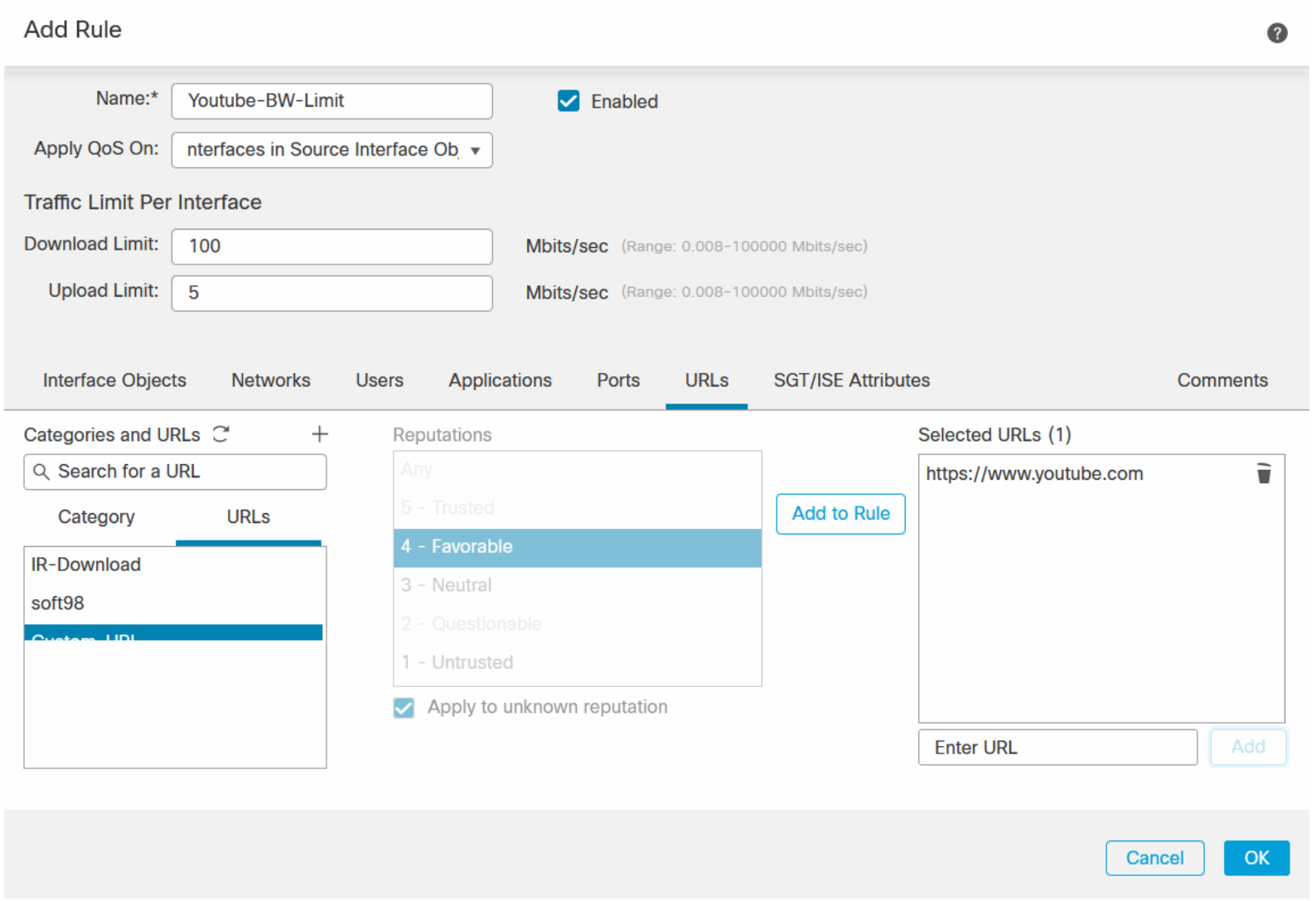
- Enter a name for this Rule
- Select Interface to apply the QOS
- Enter Download and Upload limit
- Select interface Objects (Zone)



Configuring QoS Policy

- Enter a name for this Rule
- Select Interface to apply the QOS
- Enter Download and Upload limit
- Select interface Objects (Zone)
- Enter other parameters :

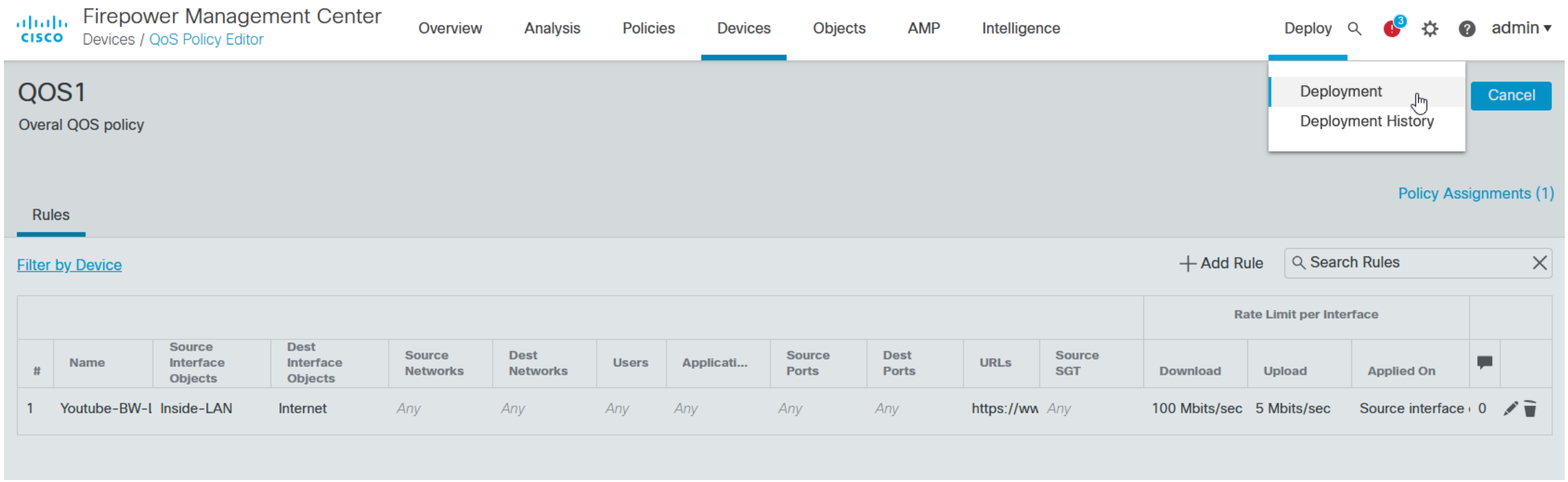
  Network
  Application
  URL
  Users
  …
- Click OK



MohsenKheradmand MK

Configuring QoS Policy

- Click Save
- Deploy > Deployment



Verification Commands

Connect to the FTD via SSH or Telnet:

- Showing the Active QoS Policy

  > show running-config policy-map

- Showing the Active QoS Policy on an Interface

  > show running-config service-policy

- Statistics of Dropped Packets

  > show service-policy police

  > show asp drop

Analyzing QoS Events and Statistics

- Analysis > Connections > Events
- Table View of Connection Events