

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.

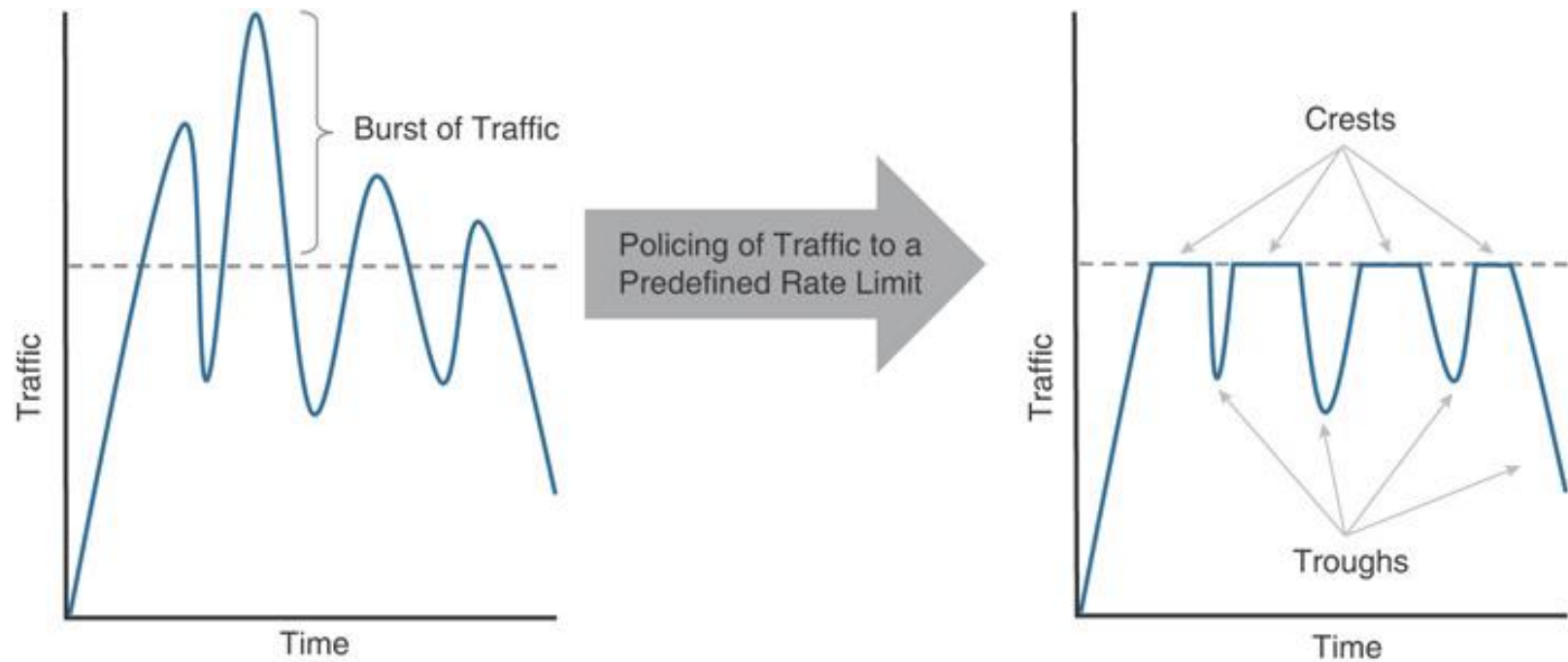
- **Packet loss:**

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.)

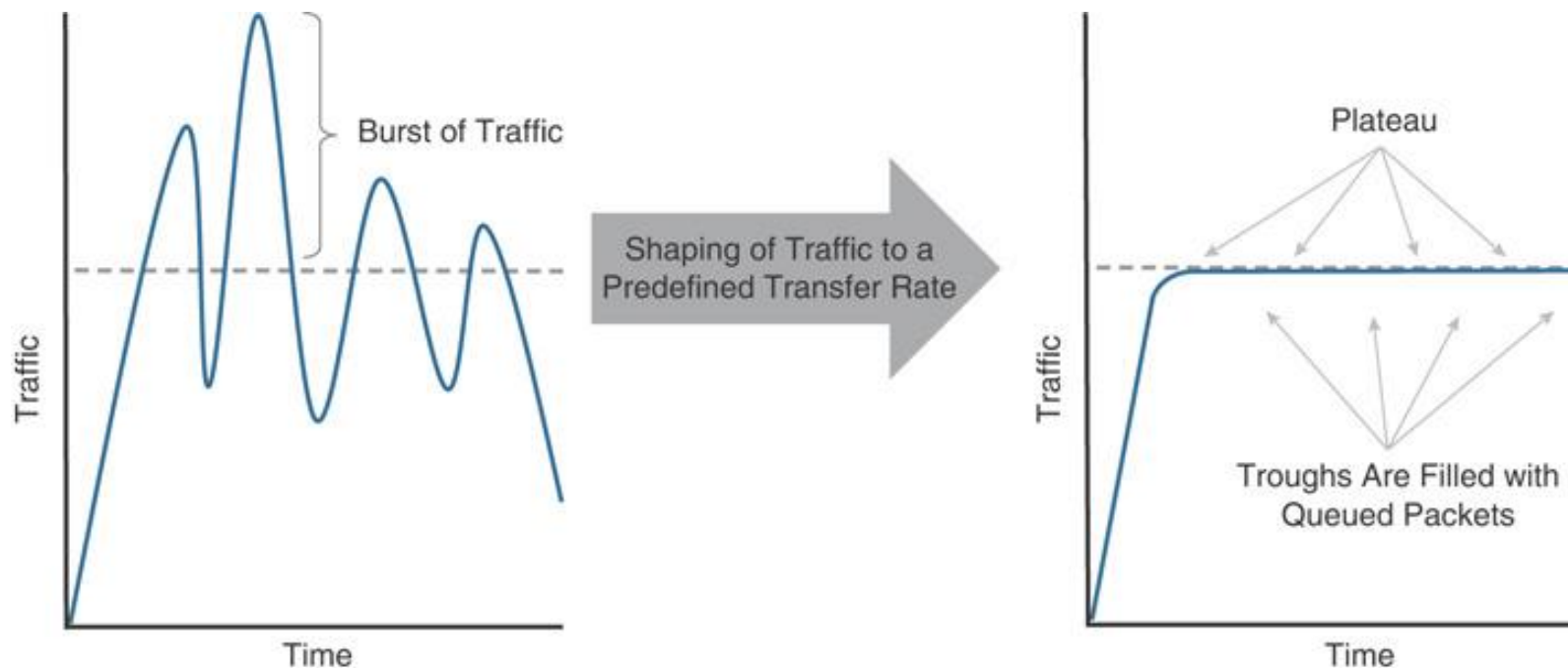
Traffic Policing Method
Dropping Excessive Traffic



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.)

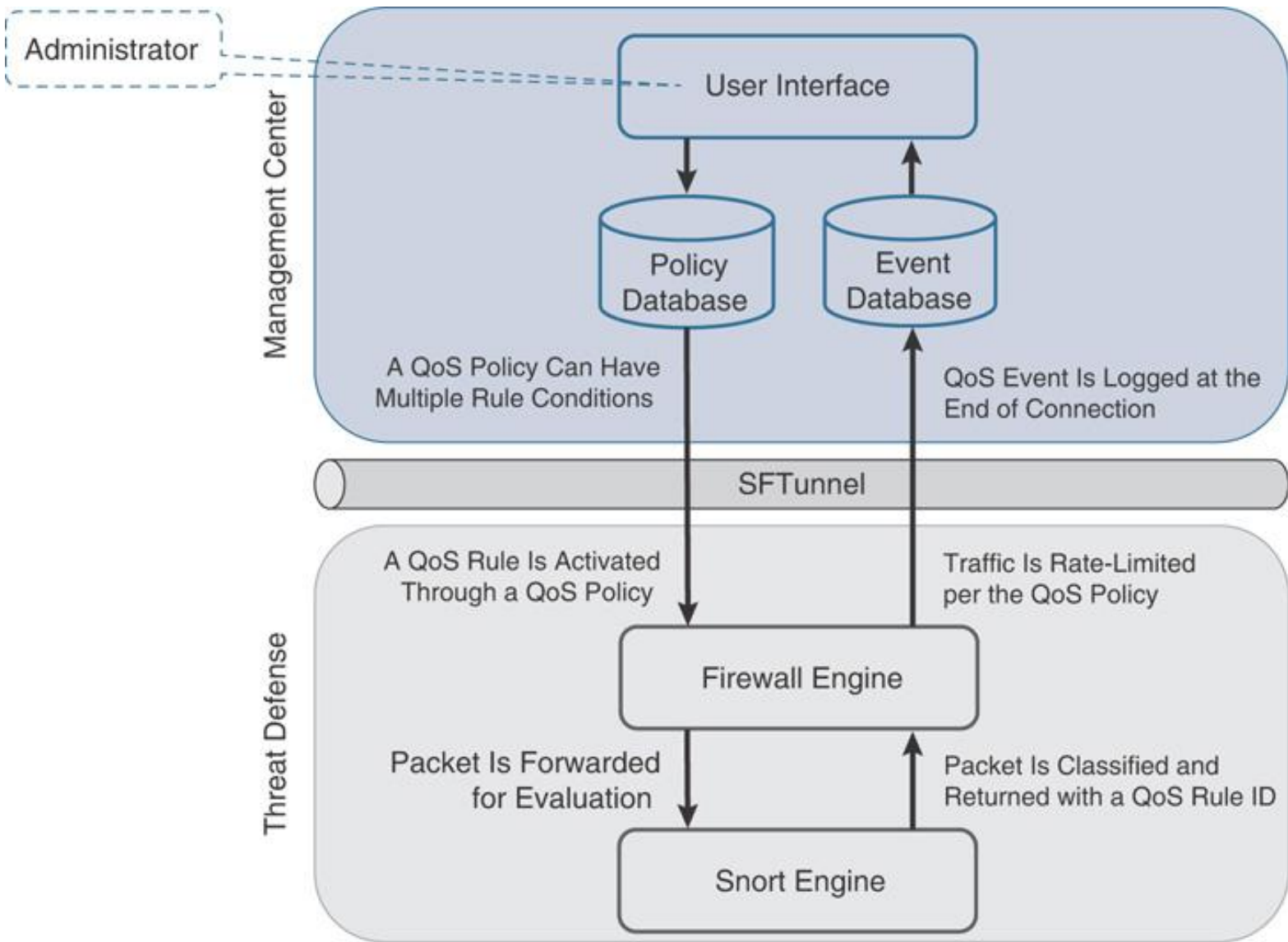
rate-limited by the
shaping mechanism



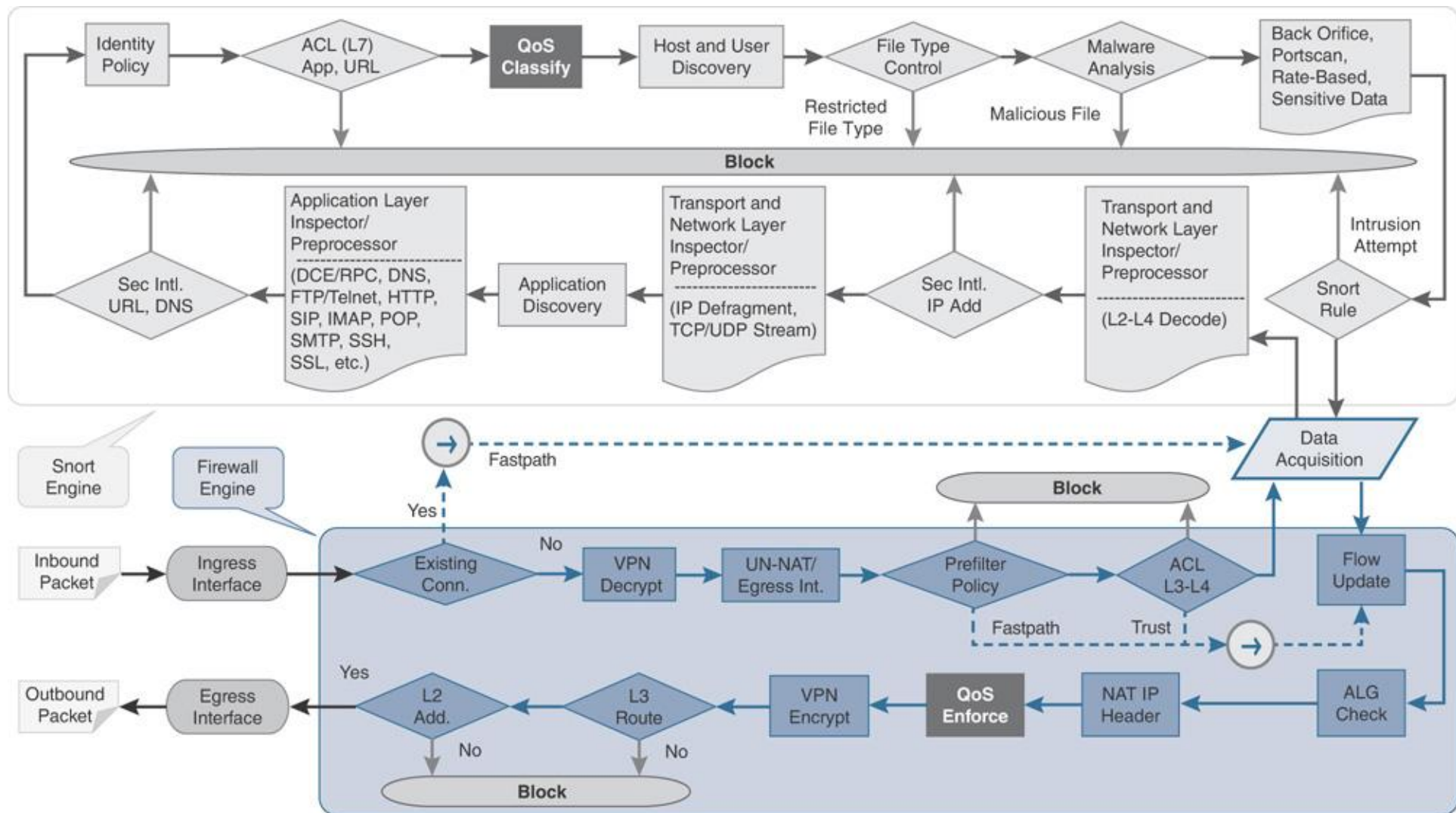
Quality of Service Essentials

- 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.

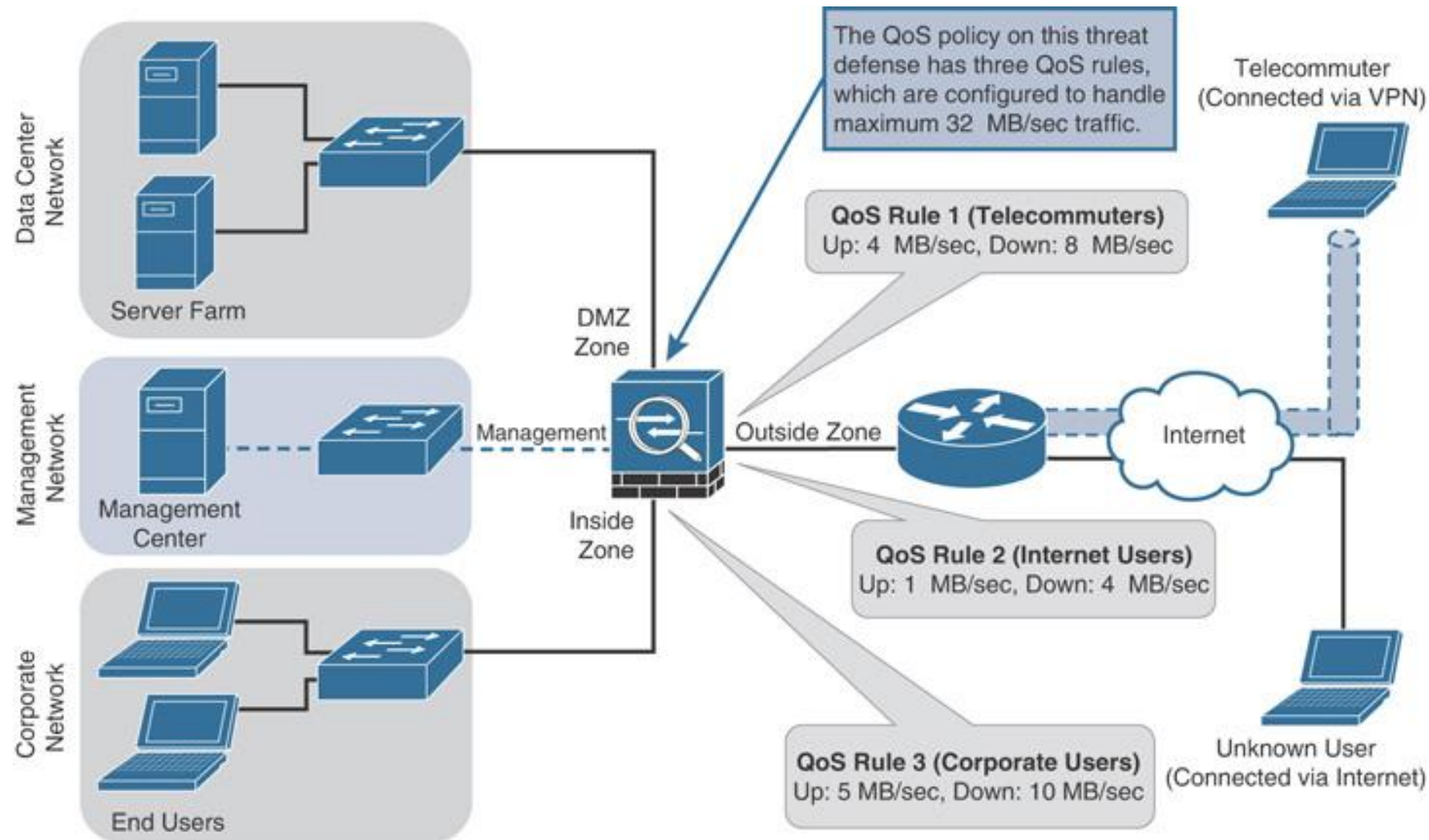
QoS Implementation on the Secure Firewall



- Processing of Packets by Various Components of Security Engines

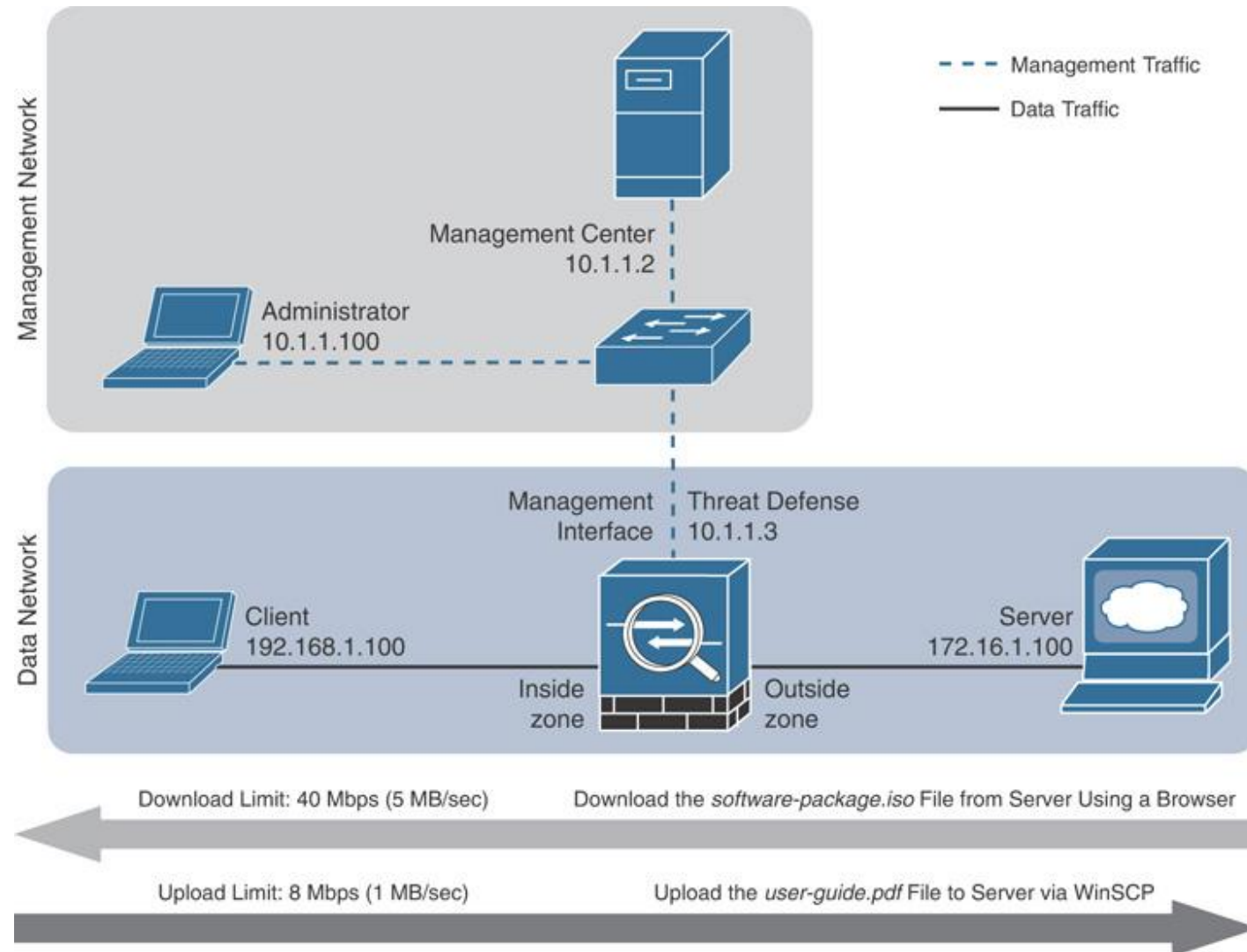


Example of Deploying QoS



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

The screenshot displays the Cisco FMC QoS configuration interface. The top navigation bar includes the Cisco FMC QoS logo and tabs for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The 'Devices' tab is currently selected. A 'New Policy' button is located in the top right corner. Below the navigation bar, a table lists existing QoS policies with columns for 'QoS Policy', 'Status', and 'Last Modified'. A message states 'There are no policies created. Add a new policy'. The 'New Policy' dialog box is open, showing the following fields:

- Name:** QOS1
- Description:** Overall QOS policy
- Targeted Devices:** Select devices to which you want to apply this policy.

The 'Available Devices' section contains a search bar with the text 'Search by name or value' and a list of available devices, with 'FTD1' selected. The 'Selected Devices' section shows 'FTD1' as the selected device. An 'Add to Policy' button is located between the two device lists. At the bottom of the dialog box, there are 'Cancel' and 'Save' buttons.

Configuring QoS Policy

- Click Add Rule

 Firepower Management Center

Devices / QoS Policy Editor

OverviewAnalysisPoliciesDevicesObjectsAMPIntelligenceDeploy

Search icon, 4 notifications, Settings, Help, admin

QOS1

Overall QoS policy

SaveCancel

Rules

Policy Assignments (1)

Filter by Device

+ Add Rule

Search Rules

												Rate Limit per Interface			
#	Name	Source Interface Objects	Dest Interface Objects	Source Network...	Dest Network...	U...	Applic...	Source Ports	Dest Ports	UR...	Source SGT	Downl...	Upload	Applied On	
There are no rules created. 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)

Editing Rule - Youtube-BW-Limit ?

Name:* Youtube-BW-Limit ☒ Enabled

Apply QoS On: Interfaces in Source Interface Ob...

Traffic Limit Per Interface

Download Limit: 100 Mbits/sec (Range: 0.008-100000 Mbits/sec)

Upload Limit: 5 Mbits/sec (Range: 0.008-100000 Mbits/sec)

Interface Objects Networks Users Applications Ports URLs SGT/ISE Attributes Comments

Available Interface Objects ⓘ

Search by name

DMZ

Inside-LAN

Internet

Add to Source

Add to Destination

Source Interface Objects (1)

Inside-LAN

Destination Interface Objects (1)

Internet

Cancel OK

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

Add Rule ?

Name:* ☒ Enabled

Apply QoS On: ▼

Traffic Limit Per Interface

Download Limit: **Mbits/sec** (Range: 0.008-100000 Mbits/sec)

Upload Limit: **Mbits/sec** (Range: 0.008-100000 Mbits/sec)

Interface Objects Networks Users Applications Ports **URLs** SGT/ISE Attributes Comments

Categories and URLs ↺ +

Category	URLs
IR-Download	
soft98	
Custom URL	

Reputations

Any

5 - Trusted

4 - Favorable

3 - Neutral

2 - Questionable

1 - Untrusted

☒ Apply to unknown reputation

Selected URLs (1)

https://www.youtube.com ✕

Configuring QoS Policy

- Click Save
- Deploy > Deployment

 Firepower Management Center
Devices / QoS Policy Editor

Overview Analysis Policies **Devices** Objects AMP Intelligence

Deploy     admin ▾

QOS1
Overall QoS policy

Policy Assignments (1)

Rules

[Filter by Device](#) + Add Rule

												Rate Limit per Interface				
#	Name	Source Interface Objects	Dest Interface Objects	Source Networks	Dest Networks	Users	Applicati...	Source Ports	Dest Ports	URLs	Source SGT	Download	Upload	Applied On		
1	Youtube-BW-I	Inside-LAN	Internet	Any	Any	Any	Any	Any	Any	https://ww	Any	100 Mbts/sec	5 Mbts/sec	Source interface	0	

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

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

II 2021-01-11 21:38:00 - 2021-01-18 17:54:14 Expanding

Search Constraints [\(Edit Search\)](#)

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

Jump to...

	☐ First Packet x	Action x	Initiator IP x	Responder IP x	Access Control Rule x	QoS-Applied Interface x	QoS-Dropped Responder Packets x
▼	☐ 2021-01-17 20:37:07	Allow	172.16.1.100	192.168.1.100	Default Action	INSIDE_INTERFACE	0
▼	☐ 2021-01-17 20:27:58	Allow	192.168.1.100	172.16.1.100	Default Action, QoS Rule	INSIDE_INTERFACE	35,931

Page 1 of 1 > > Displaying rows 1-2 of 2 rows

[View](#)
[View All](#)

The QoS Rule Dropped 35,931 Packets Because the Traffic Rate Exceeded the Predefined Limit