

22: Rate Limiting

2020年1月5日 19:08

目录

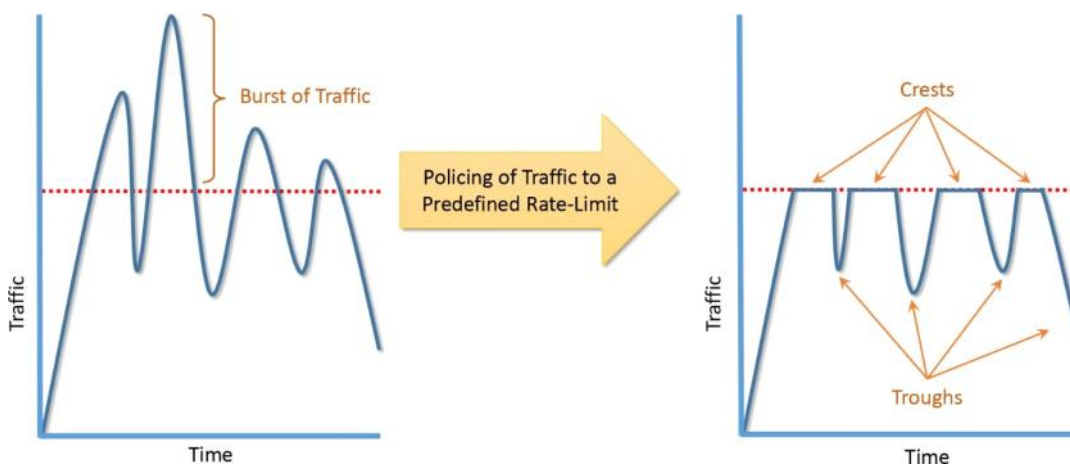
1. 流量限速介绍
2. QOS Rule Best Practices
3. 配置速率限制
4. 验证限速，以及CLI校验

1: 流量限速介绍

- 当ACP（接入控制策略/规则）对流量执行了Trust/Permit行为后，可以用FTD对流量进行限速。
- 如果是Prefilter policy对流量进行Fastpath，FTD无法对具体流量类型做出详细速度限制
- 对流量执行限速是一种管理网络带宽的办法，可以确保关键业务应用提供合理的QOS（服务质量）

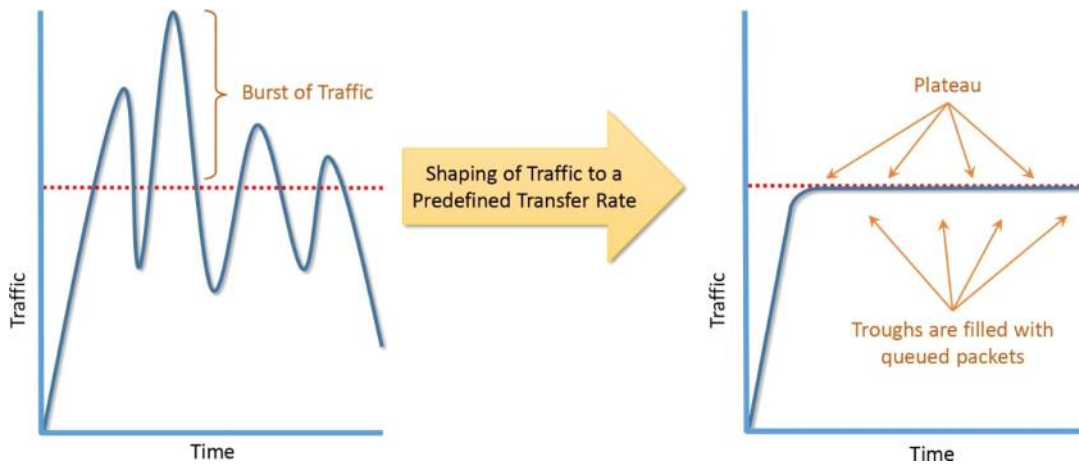
FTD可以通过实时流量限速机制来限制流量的速率，当流量达到预定义限制时，FTD可以丢弃超出的流量（FTD6.1之前不支持流量整形，流量整形可以将超出的流量排列在缓存里，而不是丢弃，以备将来传输。现在是否支持待定）

1.1: 展示了FTD使用限速机制对流量进行速率限制时，流量模式的波峰和波谷



1.2: 整形机制对流量进行速率限制时的流量图（FTD不支持目前）

整形机制会缓存超出的流量以备将来传输，所以会一直填满波谷

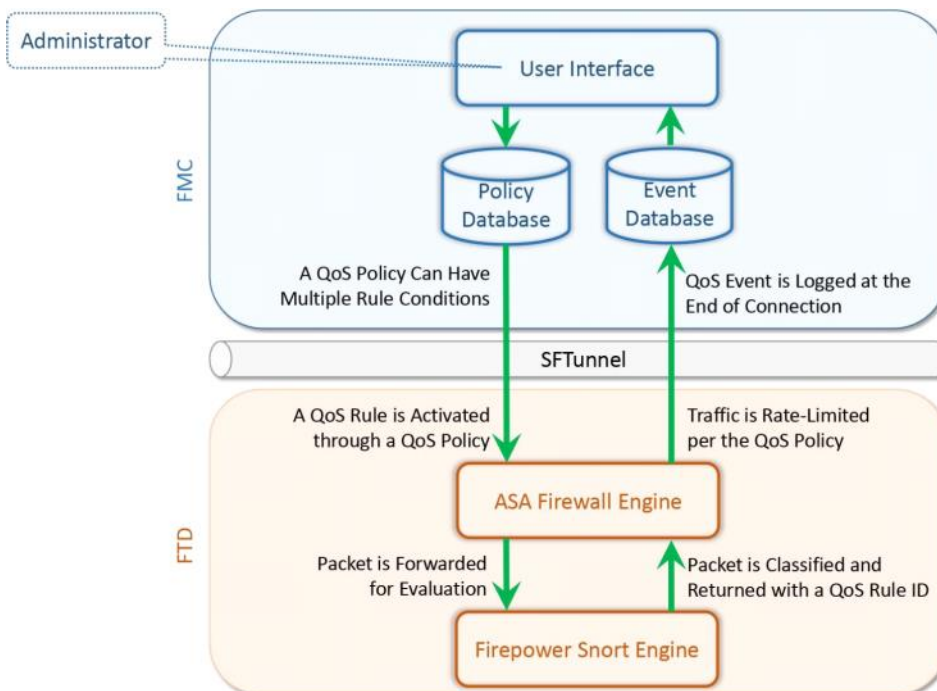


1.3: FTD的QOS说明

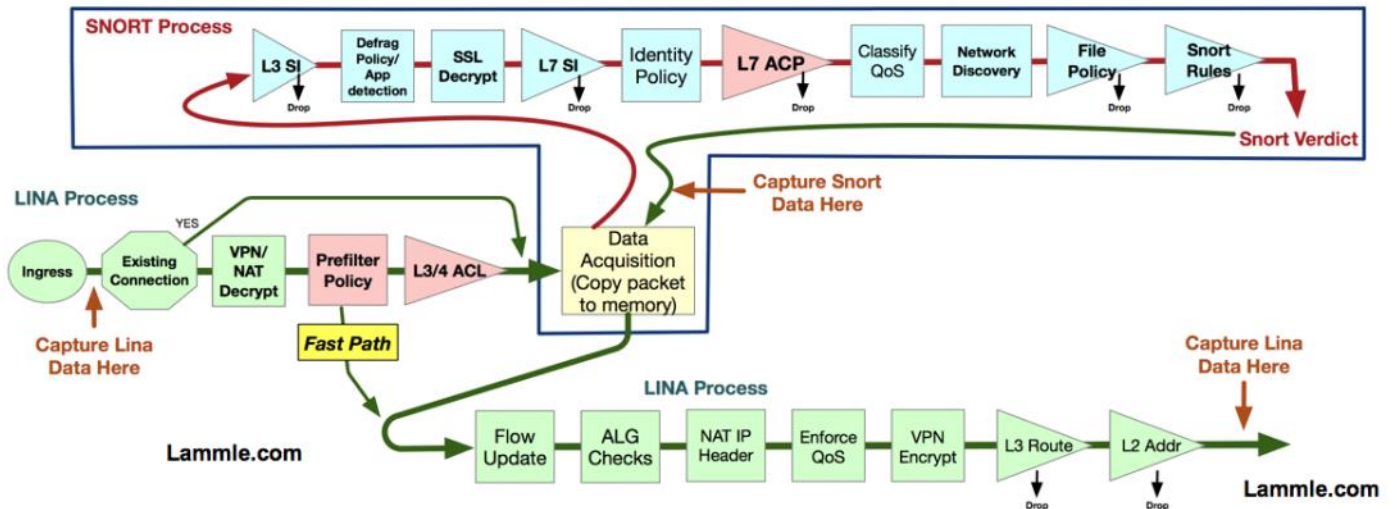
- 每台FTD只可以应用一个QOS Policy，每个Policy中可以多个QOS rule。
- 每个QOS Rule必须关联源目接口，接口必须是路由接口。
- QOS可以设置上传/下载速率限制，并且QOS可以基于高级参数定义QOS规则，比如SGT/IP/Port/APP/URL/User等
- 一个QOS Policy可以拥有32个QOS Rule
- Inline/switch/passive模式都不支持QOS策略
- QOS Policy don't have own log, you must open log in ACP setting

1.4: FTD设备的QOS工作流程

Firepower引擎会对QOS rule进行评估并对流量分类（因为QOS策略可以L7的所以可能用到Snort），数据包匹配QOS Rule后，Firepower引擎把规则ID发给防火墙引擎LINA，LINA根据QOS rule设定的上传/下载速率对流量进行限制。如下图所示



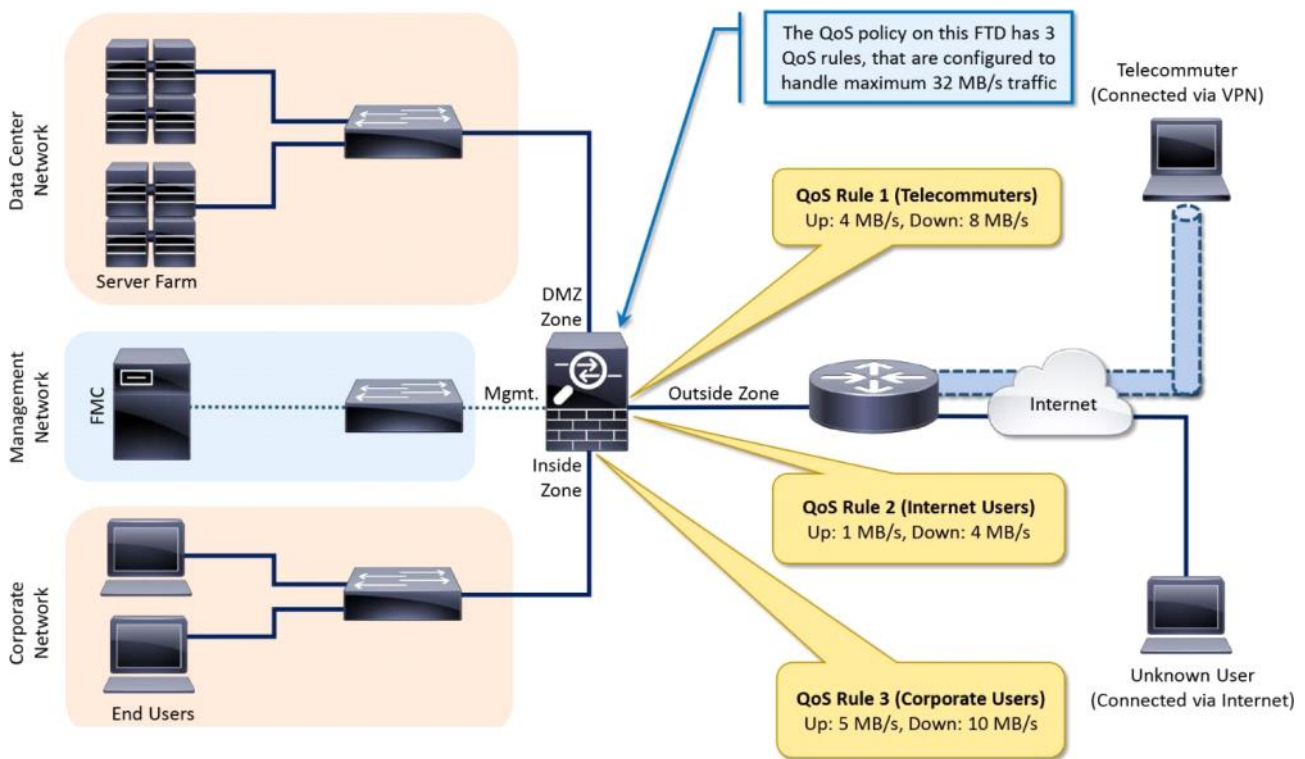
整体数据包在FTD设备的转发流程



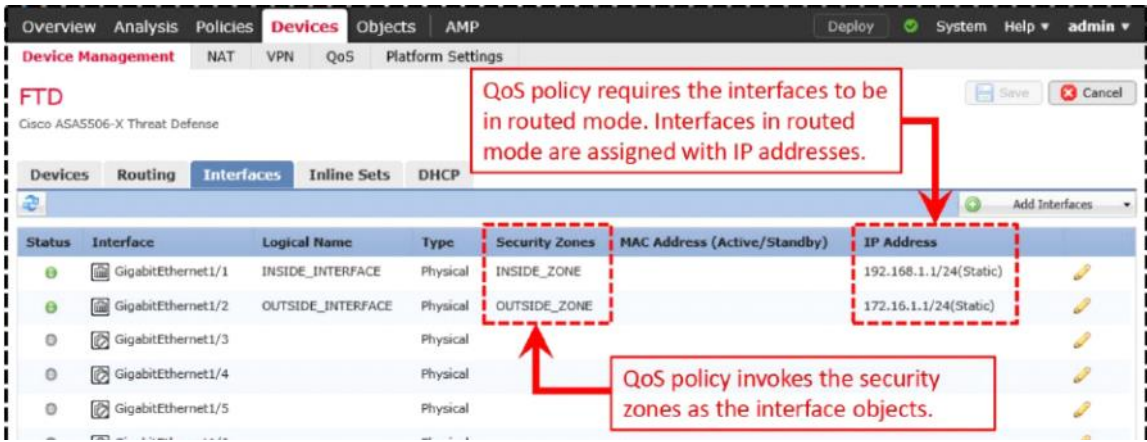
2: QOS rule Best Practices

QoS一个Policy 32个rule最大，尽可能使用贴近源的位置（更精细化）使用QoS规则，避免无用流量消耗网络和系统资源

如下示例，FTD通过一个QoS Policy启用不同的QoS Rule，流量来自不同的源网络，根据不同QoS Rule进行限速不同的用户类型不同的速率，远程/上网用户/企业用户



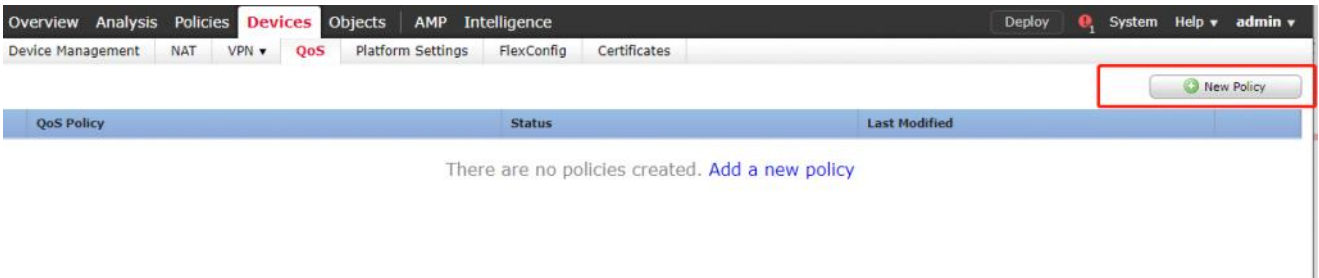
接口必须路由模式，不支持Switch/inline/passive模式接口



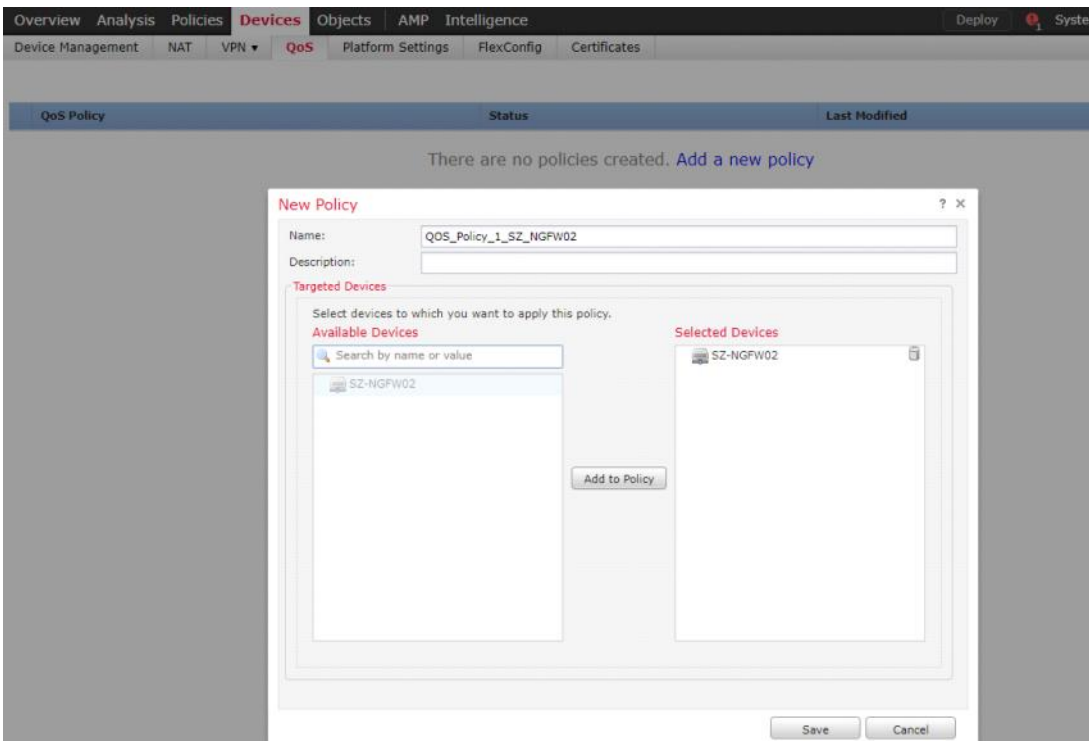
3: Config Rate Limiting

3.1: 配置QOS策略

没有默认的QOS策略，默认所有类型流量优先级一样，创建一条QOS Policy

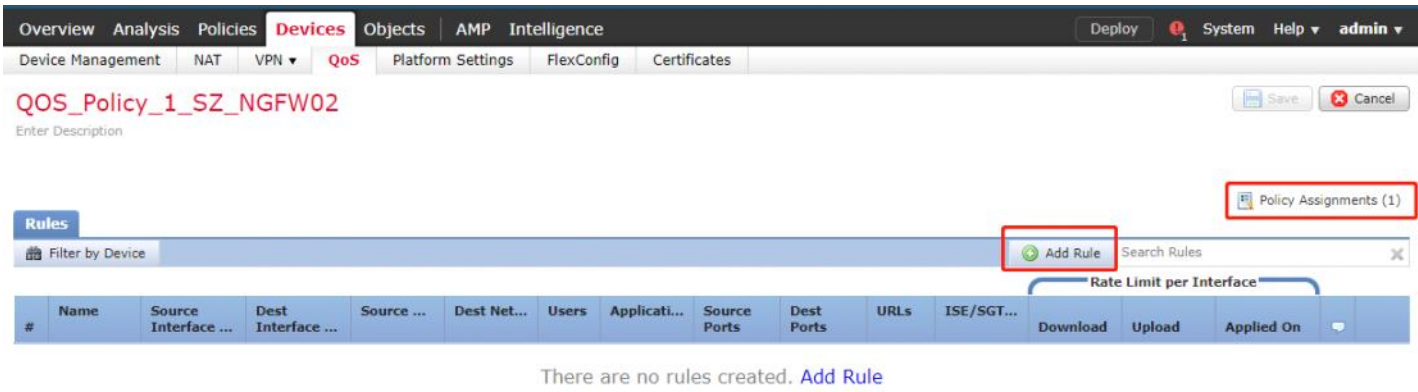


选择要关联该QOS Policy的FTD

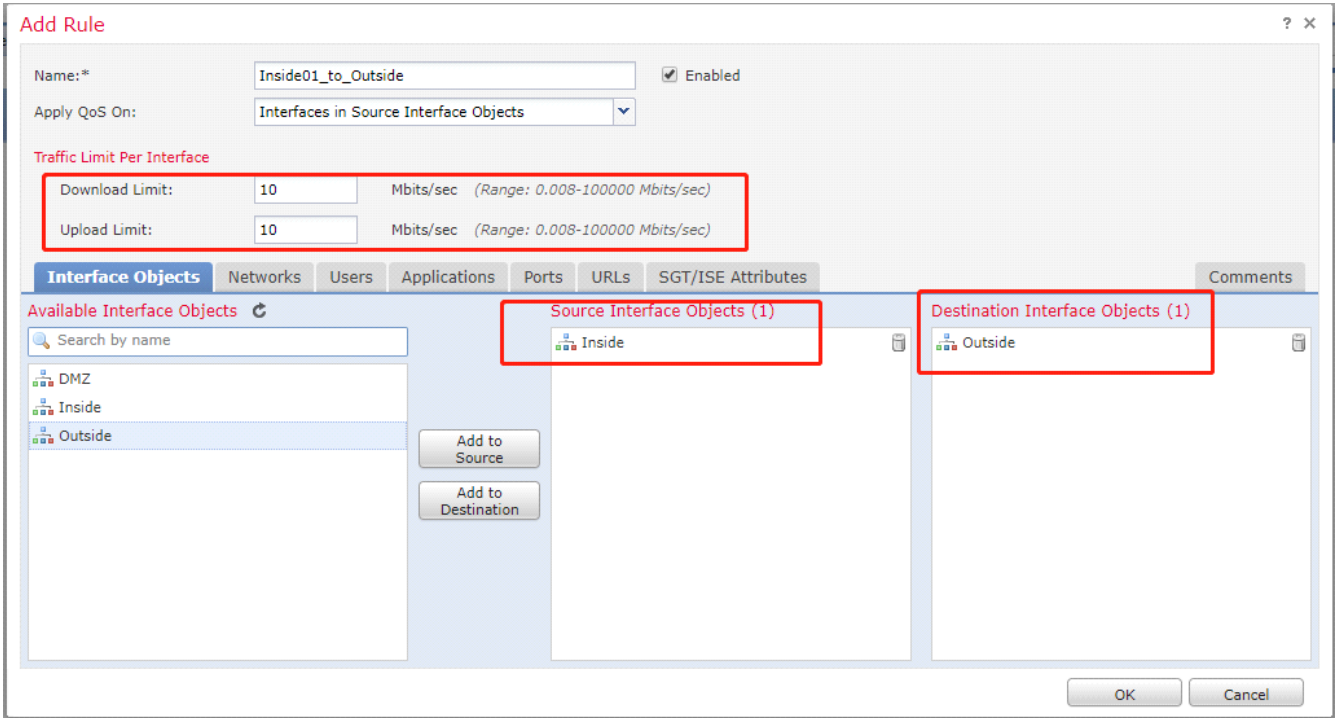


3.2: 创建QOS Rule

3.2.1: 这里还可以看到QOS Policy关联了哪些设备

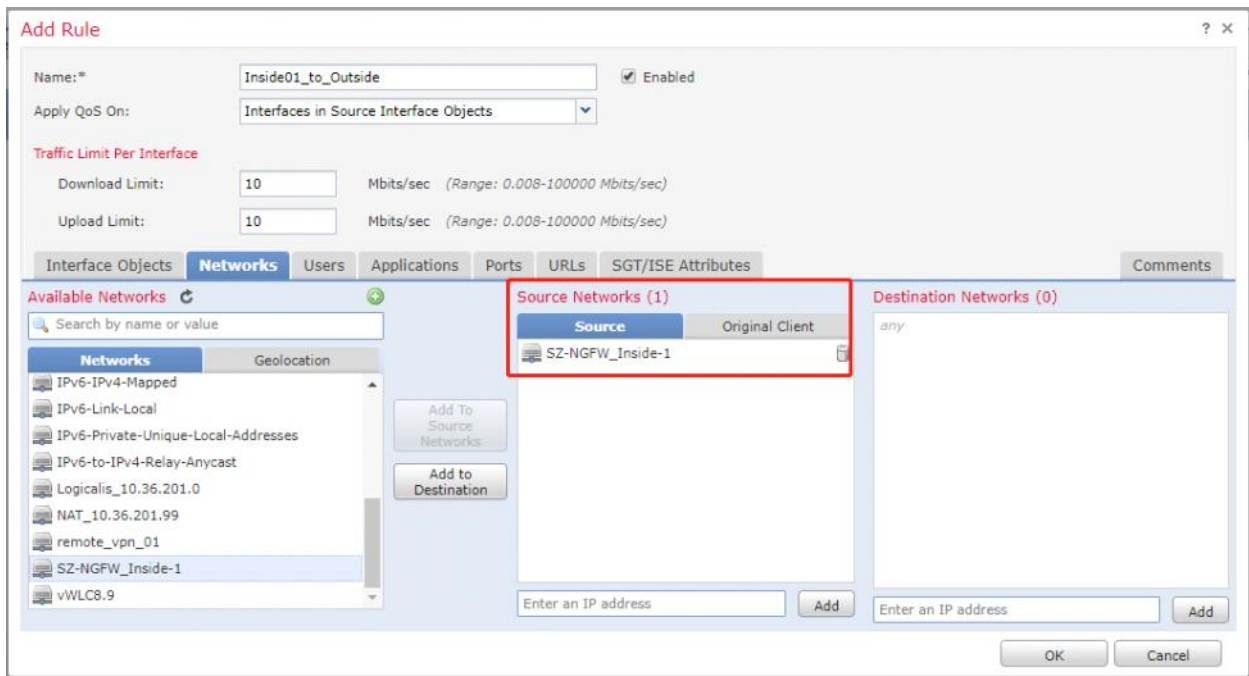


3.2.2: 限速上传下载均为10Mbit/s, 选择源目接口 (这里限制的是小b 比特字节需要除以8)

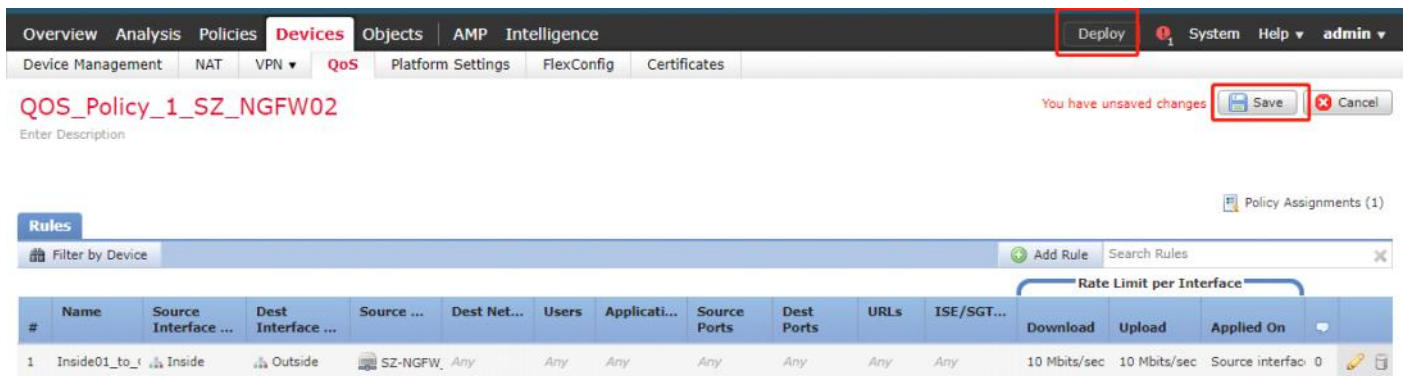


Megabit per Second	Megabyte per Second
1 Mbps	0.125 MB/s
4 Mbps	0.5 MB/s
8 Mbps	1 MB/s
10 Mbps	1.25 MB/s
16 Mbps	2 MB/s
40 Mbps	5 MB/s
80 Mbps	10 MB/s
100 Mbps	12.5 MB/s

3.2.3: 选择源目网络IP段, 这里源inside其中一个段, 目的A11



3.2.4: Save and deploy



备注：QOS策略不会有log选项，ACP里面产生的连接log里会带有QOS策略提示。

4: 校验Rate limiting

4.1: CLI验证FTD获取限速的Policy-map

Show run all可以看到

```

policy-map policy_map_Inside-1
match flow-rule qos 268436487
  police input 10000000 312500
  police output 10000000 312500
!
service-policy global_policy global

```

4.2: 测试网站测试

限速前测试



限速后测试



限速后, 迅雷会员也超不了1.25MB/s, 下载文件是字节=B=Byte。限速限的10Mbps/s



4.3: FMC查看事件

选择连接事件的表格视图

Connection Events (switch workflow)

Info ×
 This user has 1 failed login attempt since the last successful login.

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

2020-01-11 13:32

No Search Constraints (Edit Search)

Jump to... ▾

	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source ICM
↓	2020-01-12 13:31:44		Allow		192.168.44.2		223.6.6.6	CHN	Inside	Outside	6197
↓	2020-01-12 13:31:44		Allow		192.168.44.2		223.6.6.6	CHN	Inside	Outside	5340
↓	2020-01-12 13:31:44		Allow		192.168.44.2		223.6.6.6	CHN	Inside	Outside	6503
↓	2020-01-12 13:31:38		Allow		192.168.44.2		223.6.6.6	CHN	Inside	Outside	5097

This user has 1 failed login attempt since the last successful login.

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

2020-01-11 13:33:29 - 2020-01-12 13:33:29 ⌵
 (Last 1 day) Sliding

Search Constraints (Edit Search)

- Disabled Columns
- Application Protocol Category
 - Application Protocol Tag
 - Client Category
 - Client Tag
 - DNS Record Type
 - DNS Response
 - DNS Sinkhole Name
 - DNS TTL
 - HTTP Referrer
 - HTTP Response Code
 - Netflow Destination Autonomous System
 - Netflow Destination Prefix
 - Netflow Destination TOS
 - Netflow SNMP Input
 - Netflow SNMP Output
 - Netflow Source Autonomous System
 - Netflow Source Prefix
 - Netflow Source TOS
 - Original Client Country
 - Original Client IP
 - QoS Policy**
 - QoS Rule**
 - QoS-Applied Interface**
 - QoS-Dropped Initiator Bytes**
 - QoS-Dropped Initiator Packets**

然后在这个表格视图看连接日志，往右就可以看到是匹配了哪个QoS策略的哪个QoS规则

Prefilter Policy	Tunnel/Prefilter Rule	QoS Policy	QoS Rule	Security Group Tag	Endpoint Profile	Endpoint Location	Device	Ingress Interface	Egress Interface	TCP Flag
x Custom_Bypass_Traffic		QoS_Policy_1_SZ_NGFW02					SZ-NGFW02	Inside-1	Outside	
x Custom_Bypass_Traffic		QoS_Policy_1_SZ_NGFW02					SZ-NGFW02	Inside-1	Outside	
x Custom_Bypass_Traffic		QoS_Policy_1_SZ_NGFW02	Inside01 to Outside				SZ-NGFW02	Inside-1	Outside	
x Custom_Bypass_Traffic		QoS_Policy_1_SZ_NGFW02					SZ-NGFW02	Inside-1	Outside	
x Custom_Bypass_Traffic		QoS_Policy_1_SZ_NGFW02					SZ-NGFW02	Inside-1	Outside	
x Custom_Bypass_Traffic		QoS_Policy_1_SZ_NGFW02					SZ-NGFW02	Inside-1	Outside	
x Custom_Bypass_Traffic		QoS_Policy_1_SZ_NGFW02					SZ-NGFW02	Inside-1	Outside	
x Custom_Bypass_Traffic		QoS_Policy_1_SZ_NGFW02					SZ-NGFW02	Inside-1	Outside	
x Custom_Bypass_Traffic		QoS_Policy_1_SZ_NGFW02	Inside01 to Outside				SZ-NGFW02	Inside-1	Outside	
x Custom_Bypass_Traffic		QoS_Policy_1_SZ_NGFW02					SZ-NGFW02	Inside-1	Outside	
x Custom_Bypass_Traffic		QoS_Policy_1_SZ_NGFW02					SZ-NGFW02	Inside-1	Outside	
x Custom_Bypass_Traffic		QoS_Policy_1_SZ_NGFW02					SZ-NGFW02	Inside-1	Outside	
x Custom_Bypass_Traffic		QoS_Policy_1_SZ_NGFW02					SZ-NGFW02	Inside-1	Outside	
x Custom_Bypass_Traffic		QoS_Policy_1_SZ_NGFW02					SZ-NGFW02	Inside-1	Outside	
x Custom_Bypass_Traffic		QoS_Policy_1_SZ_NGFW02					SZ-NGFW02	Inside-1	Outside	
x Custom_Bypass_Traffic		QoS_Policy_1_SZ_NGFW02					SZ-NGFW02	Inside-1	Outside	
x Custom_Bypass_Traffic		QoS_Policy_1_SZ_NGFW02					SZ-NGFW02	Inside-1	Outside	
x Custom_Bypass_Traffic		QoS_Policy_1_SZ_NGFW02					SZ-NGFW02	Inside-1	Outside	

4.4: FTD上CLI校验

可以看到传输和丢弃的数据包大小

```
> show service-policy police

Interface Inside-1:
Service-policy: policy_map_Inside-1
Flow-rule QoS id: 268436487
Input police Interface Inside-1:
  cir 10000000 bps, bc 312500 bytes
  conformed 85795 packets, 50477711 bytes; actions: transmit
  exceeded 3554 packets, 5075186 bytes; actions: drop
  conformed 311464 bps, exceed 31408 bps
Output police Interface Inside-1:
  cir 10000000 bps, bc 312500 bytes
  conformed 107377 packets, 121416727 bytes; actions: transmit
  exceeded 12424 packets, 17803625 bytes; actions: drop
  conformed 724808 bps, exceed 109792 bps

>
```

```
> show asp drop

Frame drop:
No route to host (no-route) 12
Reverse-path verify failed (rpf-violated) 4
Flow is denied by configured rule (acl-drop) 113745
First TCP packet not SYN (tcp-not-syn) 111
TCP failed 3 way handshake (tcp-3whs-failed) 103
TCP RST/FIN out of order (tcp-rstfin-ooo) 212
TCP packet SEQ past window (tcp-seq-past-win) 3
Output QoS rate exceeded (rate-exceeded) 101322
Slowpath security checks failed (sp-security-failed) 803746
TCPMP Inspect bad icmp code (inspect-icmp-bad-code) 20
DNS Inspect id not matched (inspect-dns-id-not-matched) 14
Snort requested to drop the frame (snort-drop) 122644
Snort instance is down (snort-down) 40
FP L2 rule drop (l2_acl) 7997
Interface is down (interface-down) 3
Blocked or blacklisted by the firewall preprocessor (firewall) 31119
Blocked or blacklisted by the session preprocessor (session-preproc)
Blocked or blacklisted by the file process preprocessor (file-process)

Last clearing: Never

Flow drop:
Last clearing: Never
```

Show conn detail可以看到实时的连接都撞击了QoS策略

```

UDP Inside-1: 192.168.44.2/12345 Outside: 125.68.25.70/9331,
  flags - Nl, qos-rule-id 268436487, idle 0s, uptime 3m1s, timeout 2m0s, bytes 1202496, xlate id 0x2b448ab45300

TCP Inside-1: 192.168.44.2/52245 Outside: 61.170.175.50/13195,
  flags UfrxIO Nl, qos-rule-id 268436487, idle 3m7s, uptime 3m7s, timeout 10m0s, bytes 299, xlate id 0x2b4496b128c0

UDP Inside-1: 192.168.44.2/12345 Outside: 61.128.145.28/8000,
  flags - Nl, qos-rule-id 268436487, idle 36s, uptime 36s, timeout 2m0s, bytes 157, xlate id 0x2b448ab45300

UDP Inside-1: 192.168.44.2/12345 Outside: 222.214.51.254/12345,
  flags - Nl, qos-rule-id 268436487, idle 0s, uptime 3m7s, timeout 2m0s, bytes 1583317, xlate id 0x2b448ab45300

TCP Inside-1: 192.168.44.2/52249 Outside: 124.77.105.199/11709,
  flags UxIO Nl, qos-rule-id 268436487, idle 7s, uptime 3m7s, timeout 1h0m, bytes 804, xlate id 0x2b448ab3eb00

UDP Inside-1: 192.168.44.2/12345 Outside: 120.36.3.129/12679,
  flags - Nl, qos-rule-id 268436487, idle 0s, uptime 3m7s, timeout 2m0s, bytes 4118733, xlate id 0x2b448ab45300

TCP Inside-1: 192.168.44.2/52344 Outside: 61.55.10.54/35571,
  flags UxIO Nl, qos-rule-id 268436487, idle 2m22s, uptime 2m23s, timeout 1h0m, bytes 469, xlate id 0x2b448ab44f00

```

查看Firepower引擎Snort生成的实时调试信息，由于流量匹配QOS rule生成，这个日志很多，实时的，注意取消

```

> system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages

192.168.44.2-52728 > 171.223.111.49-49581 6 AS 1 I 0 Starting with minimum 0, id 0 and SrcZone first with zones 3 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 924, payload -1, client 2000000924, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.44.2-52728 > 171.223.111.49-49581 6 AS 1 I 0 match rule order 1, id 268436487 action Rate Limit
192.168.44.2-52286 > 118.250.106.36-52313 6 AS 1 I 0 Starting with minimum 0, id 0 and SrcZone first with zones 3 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload -1, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.44.2-52286 > 118.250.106.36-52313 6 AS 1 I 0 match rule order 1, id 268436487 action Rate Limit
192.168.44.2-52237 > 59.47.72.254-54321 6 AS 1 I 0 Starting with minimum 0, id 0 and SrcZone first with zones 3 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload -1, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.44.2-52237 > 59.47.72.254-54321 6 AS 1 I 0 match rule order 1, id 268436487 action Rate Limit
192.168.44.2-52237 > 59.47.72.254-54321 6 AS 1 I 0 Starting with minimum 0, id 0 and SrcZone first with zones 3 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload -1, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.44.2-52237 > 59.47.72.254-54321 6 AS 1 I 0 match rule order 1, id 268436487 action Rate Limit
192.168.44.2-52237 > 59.47.72.254-54321 6 AS 1 I 0 Starting with minimum 0, id 0 and SrcZone first with zones 3 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload -1, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.44.2-52237 > 59.47.72.254-54321 6 AS 1 I 0 match rule order 1, id 268436487 action Rate Limit

```

- Ctrl + c可以退出debug
- Undebug all取消
- Debug snort event可以看到firepower引擎

4.5: 清除QOS计数便于排错

- Clear asp drop
- Clear service-policy interface inside