Cisco ASA의 QoS 컨피그레이션 예

목차

소개

이 문서에서는 QoS(Quality of Service)가 Cisco ASA(Adaptive Security Appliance)에서 작동하는 방식에 대해 설명하고 다양한 시나리오에 대해 이를 구현하는 방법에 대한 몇 가지 예를 제공합니다.

모든 트래픽이 제한된 대역폭의 공정한 공유를 얻을 수 있도록 개별 흐름과 VPN 터널 흐름 모두에

대해 선택한 네트워크 트래픽에 속도 제한을 제공하도록 보안 어플라이언스에서 QoS를 구성할 수 있습니다.

이 기능은 Cisco 버그 ID CSCsk06260과 통합되었습니다.

사전 요구 사항

요구 사항

Cisco는 MPF(Modular Policy Framework)에 대한 지식을 보유하고 있는 것을 권장합니다.

사용되는 구성 요소

이 문서의 정보는 버전 9.2를 실행하는 ASA를 기반으로 하지만 이전 버전도 사용할 수 있습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

QoS는 특정 유형의 인터넷 트래픽에 우선 순위를 부여할 수 있는 네트워크 기능입니다.인터넷 사용자가 모뎀에서 DSL(Digital Subscriber Line) 및 케이블과 같은 고속 광대역 연결로 액세스 포인트를 업그레이드함에 따라, 언제든지 단일 사용자가 사용 가능한 대역폭의 대부분을 흡수할 수 있을 가능성이 증가하므로 다른 사용자는 굶주리게 됩니다.한 사용자 또는 사이트 간 연결이 대역폭의 공정한 점유율보다 많은 것을 소비하지 않도록 QoS는 모든 사용자가 사용할 수 있는 최대 대역폭을 제어하는 폴리싱 기능을 제공합니다.

QoS는 네트워크의 기능을 통해 다양한 기술을 통해 선택된 네트워크 트래픽에 더 나은 서비스를 제공하여 기본 기술의 대역폭이 제한된 전체 서비스를 최상으로 제공합니다.

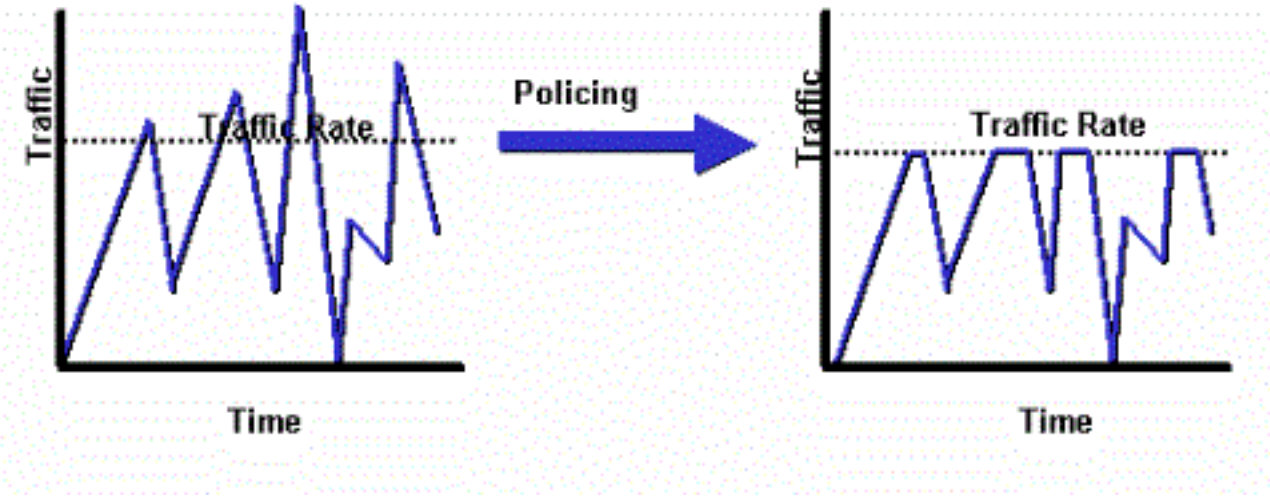
보안 어플라이언스의 QoS의 기본 목표는 개별 플로우 또는 VPN 터널 흐름 모두에 대해 선택한 네트워크 트래픽에 속도 제한을 제공하여 모든 트래픽이 제한된 대역폭의 공정한 공유를 얻도록 하는 것입니다.플로우는 다양한 방법으로 정의할 수 있습니다.보안 어플라이언스에서 QoS는 소스 및 대상 IP 주소, 소스 및 대상 포트 번호, IP 헤더의 Type of Service(ToS) 바이트의 조합에 적용할 수 있습니다.

ASA에서 구현할 수 있는 QoS에는 세 가지 종류가 있습니다.폴리싱, 셰이핑 및 우선순위 큐잉.

트래픽 폴리싱

폴리싱을 사용하면 지정된 제한을 초과하는 트래픽이 삭제됩니다. 폴리싱은 어떤 트래픽도 사용자가 구성하는 최대 속도(비트/초)를 초과하지 않도록 하는 방법으로, 어떤 트래픽 흐름이나 클래스도 전체 리소스를 인수할 수 없도록 합니다.트래픽이 최대 속도를 초과하면 ASA는 초과 트래픽을 삭제합니다.또한 폴리싱은 허용되는 최대 단일 트래픽 버스트를 설정합니다.

이 다이어그램은 트래픽 폴리싱이 수행하는 작업을 보여줍니다.트래픽 속도가 구성된 최대 속도에 도달하면 초과 트래픽이 삭제됩니다.그 결과 출력은 크레스트 및 트러스트가 있는 톱니처럼 나타납니다.



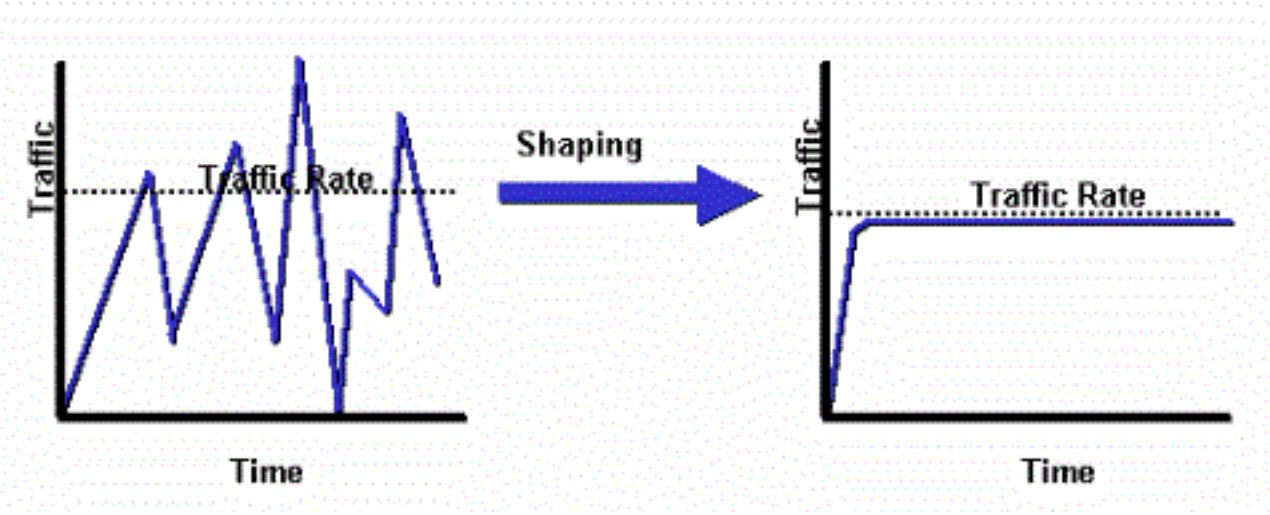
다음 예에서는 아웃바운드 방향의 특정 사용자에 대해 대역폭을 1Mbps로 제한하는 방법을 보여줍니다.

```
ciscoasa(config)# access-list WEB-LIMIT permit ip host 192.168.10.1 any
ciscoasa(config)# class-map Class-Policy
ciscoasa(config-cmap)# match access-list WEB-LIMIT
ciscoasa(config-cmap)#exit

ciscoasa(config)# policy-map POLICY-WEB
ciscoasa(config-pmap)# class Class-Policy
ciscoasa(config-pmap-c)# police output 1000000 conform-action transmit exceed-
action drop
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit

ciscoasa(config)# service-policy POLICY-WEB interface outside
```

트래픽 셰이핑

트래픽 셰이핑은 장치 및 링크 속도를 일치시키기 위해 사용됩니다. 이는 패킷 손실, 변수 지연 및 링크 채도를 제어하여 지터와 지연을 일으킬 수 있습니다. 보안 어플라이언스의 트래픽 셰이핑을 통해 디바이스에서 트래픽 플로우를 제한할 수 있습니다.이 메커니즘은 "속도 제한"을 초과하는 트래픽을 버퍼링하고 나중에 트래픽을 전송하려고 시도합니다.특정 트래픽 유형에 대해서는 셰이핑을 구성할 수 없습니다.셰이핑된 트래픽에는 디바이스를 통과하는 트래픽과 디바이스에서 제공하는 트래픽이 포함됩니다.

이 다이어그램은 트래픽 셰이핑의 기능을 보여줍니다.큐에서 초과 패킷을 보존한 다음 시간 증가에 따라 나중에 전송하기 위해 초과 시간을 예약합니다.트래픽 셰이핑의 결과는 매끄러운 패킷 출력 속도입니다.



참고:트래픽 셰이핑은 ASA 버전 5505, 5510, 5520, 5540 및 5550에서만 지원됩니다.멀티코어 모델(예: 5500-X)은 셰이핑을 지원하지 않습니다.

트래픽 셰이핑에서는 특정 제한을 초과하는 트래픽이 대기열에 추가되고(버퍼링) 다음 시간 내에 전송됩니다.

방화벽의 트래픽 셰이핑은 업스트림 디바이스에서 네트워크 트래픽에 병목 현상이 있는 경우 가장 유용합니다.예를 들어 100Mbit 인터페이스가 있는 ASA는 케이블 모뎀을 통해 인터넷에 업스트림 연결되거나 라우터에서 종료되는 T1을 사용합니다.트래픽 셰이핑을 사용하면 인터페이스에서 최대 아웃바운드 처리량을 구성할 수 있습니다(예: 외부 인터페이스).방화벽은 해당 인터페이스에서 지정된 대역폭까지 트래픽을 전송한 다음, 링크가 포화 상태가 낮은 경우 나중에 전송을 위해 과도한 트래픽을 버퍼링하려고 시도합니다.

셰이핑은 지정된 인터페이스를 통과하는 모든 집계 트래픽에 적용됩니다.특정 트래픽 흐름만 셰이핑하도록 선택할 수는 없습니다.

참고:셰이핑은 암호화 후 수행되며 VPN에 대한 내부 패킷 또는 터널 그룹 기반에서 우선 순위를 지정할 수 없습니다.

다음 예에서는 외부 인터페이스의 모든 아웃바운드 트래픽을 2Mbps로 셰이핑하기 위해 방화벽을 구성합니다.

```
ciscoasa(config-pmap)#policy-map qos_outside_policy
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# shape average 2000000
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit

ciscoasa(config-pmap-c)# service-policy qos_outside_policy interface outside
```

우선순위 대기열 처리

우선 순위 큐잉을 사용하면 표준 대기열 이전에 처리되는 LLQ(Low Latency Queue)에 특정 트래픽 클래스를 배치할 수 있습니다.

참고:셰이핑 정책에 따라 트래픽의 우선 순위를 지정하는 경우 내부 패킷 세부 정보를 사용할 수 없습니다.더 정교한 큐잉 및 QoS 메커니즘(WFQ(Weighted Fair Queuing), CBWFQ(Class-Based Weighted Fair Queueing) 등을 제공할 수 있는 라우터와 달리 방화벽은 LLQ만 수행할 수 있습니다.

계층적 QoS 정책은 사용자가 계층적 방식으로 QoS 정책을 지정할 수 있는 메커니즘을 제공합니다.예를 들어, 사용자가 인터페이스에서 트래픽을 셰이핑하고 더 셰이핑된 인터페이스 트래픽 내에서 VoIP 트래픽에 대해 우선순위 큐잉을 제공하려는 경우 사용자는 맨 위에 트래픽 셰이핑 정책을 지정하고 셰이프 정책에서 우선 순위 큐잉 정책을 지정할 수 있습니다.계층적 QoS 정책 지원은 범위가 제한됩니다.허용되는 유일한 옵션은 다음과 같습니다.

- 최상위 레벨에서 트래픽 셰이핑
- 다음 레벨에서 우선순위 대기열 처리

참고:셰이핑 정책에 따라 트래픽의 우선 순위를 지정하는 경우 내부 패킷 세부 정보를 사용할 수 없습니다.더 정교한 큐잉 및 QoS 메커니즘(WFQ, CBWFQ 등)을 제공할 수 있는 라우터와 달리 방화벽은 LLQ만 수행할 수 있습니다.

이 예에서는 계층적 QoS 정책을 사용하여 외부 인터페이스의 모든 아웃바운드 트래픽을 쉐이핑 예와 같이 2Mbps로 셰이핑하지만, DSCP(Differentiated Services Code Point) 값 "ef" 및 SSH(Secure Shell) 트래픽이 우선 순위를 받도록 지정합니다.

기능을 활성화할 인터페이스에서 우선순위 큐를 생성합니다.

```
ciscoasa(config)#priority-queue outsideciscoasa(config-priority-queue)#queue-limit
2048ciscoasa(config-priority-queue)#tx-ring-limit 256
```

DSCP EF와 일치하는 클래스:

```
   ciscoasa(config)# class-map Voice
ciscoasa(config-cmap)# match dscp ef
ciscoasa(config-cmap)# exit
```

포트 TCP/22 SSH 트래픽을 매칭하는 클래스:

```
   ciscoasa(config)# class-map SSH
ciscoasa(config-cmap)# match port tcp eq 22
ciscoasa(config-cmap)# exit
```

음성 및 SSH 트래픽의 우선 순위를 적용하기 위한 정책 맵:

```
   ciscoasa(config)# policy-map p1_priority
ciscoasa(config-pmap)# class Voice
ciscoasa(config-pmap-c)# priority
ciscoasa(config-pmap-c)# class SSH
ciscoasa(config-pmap-c)# priority
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
```

모든 트래픽에 셰이핑을 적용하고 우선 순위가 지정된 음성 및 SSH 트래픽을 연결하기 위한 정책 맵:

```
   ciscoasa(config)# policy-map p1_shape
```

```
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# shape average 2000000
ciscoasa(config-pmap-c)# service-policy p1_priority
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
```

마지막으로 아웃바운드 트래픽을 구성하고 우선 순위를 지정할 인터페이스에 쉐이핑 정책을 연결합니다.

```
   ciscoasa(config)# service-policy p1_shape interface outside
```

VPN 터널을 통한 트래픽에 대한 QoS

IPsec VPN을 사용하는 QoS

원래 IP 헤더의 RFC 2401 ToS(Type of Service) 비트가 암호화 후 QoS 정책을 적용할 수 있도록 암호화된 패킷의 IP 헤더에 복사됩니다.이렇게 하면 QoS 정책의 모든 위치에서 우선 순위에 DSCP/DiffServ 비트를 사용할 수 있습니다.

IPsec 터널의 폴리싱

특정 VPN 터널에 대한 폴리싱을 수행할 수도 있습니다.폴리싱할 터널 그룹을 선택하려면 class-map 및 match **flow ip destination address** 명령에서 **match tunnel-group <tunnel>** 명령을 사용합니다.

```
 class-map tgroup_out
match tunnel-group ipsec-tun
match flow ip destination-address
policy-map qos
class tgroup_out
police output 1000000
```

match tunnel-**group** 명령을 사용할 때 입력 폴리싱이 현재 작동하지 않습니다.자세한 내용은 Cisco 버그 ID CSCth48255를 참조하십시오.match flow ip destination-address로 입력 폴리싱을 수행하려고 하면 다음 오류가 발생합니다.

```
   police input 10000000
ERROR: Input policing cannot be done on a flow destination basis
```

match tunnel-group(Cisco 버그 ID CSCth48255)을 사용할 때 입력 폴리싱이 현재 작동하지 않는 것으로 나타납니다. 입력 폴리싱이 작동하는 경우 **match flow ip destination-address 주소** 없이 클래스 맵을 사용해야 합니다.

```
  class-map tgroup_in
match tunnel-group ipsec-tun
policy-map qos
class tgroup_in
police input 1000000
```

match ip destination 주소가 없는 클래스 맵에서 출력을 폴리싱하려고 하면, 다음과 같은 메시지가 표시됩니다.

```
   police output 10000000
ERROR: tunnel-group can only be policed on a flow basis
```

또한 ACL(Access Control Lists), DSCP 등을 사용하여 내부 흐름 정보에서 QoS를 수행할 수도 있습니다.앞서 언급한 버그로 인해 ACL은 현재 입력 폴리싱을 수행할 수 있는 방법입니다.

> **참고:**모든 플랫폼 유형에 최대 64개의 정책 맵을 구성할 수 있습니다.트래픽을 분할하려면 정책 맵 내에서 다른 클래스 맵을 사용합니다.

SSL(Secure Sockets Layer) VPN을 사용하는 QoS

ASA 버전 9.2까지 ASA는 ToS 비트를 보존하지 않았습니다.

이 기능에서는 SSL VPN 터널링이 지원되지 않습니다.자세한 내용은 Cisco 버그 ID CSCsl73211을 참조하십시오.

```
   ciscoasa(config)# tunnel-group a1 type webvpn
ciscoasa(config)# tunnel-group a1 webvpn-attributes
ciscoasa(config-tunnel-webvpn)# class-map c1
ciscoasa(config-cmap)# match tunnel-group a1
ciscoasa(config-cmap)# match flow ip destination-address
ciscoasa(config-cmap)# policy-map p1
ciscoasa(config-pmap)# class c1
ciscoasa(config-pmap-c)# police output 100000
ERROR: tunnel with WEBVPN attributes doesn't support police!

ciscoasa(config-pmap-c)# no tunnel-group a1 webvpn-attributes
ciscoasa(config)# policy-map p1
ciscoasa(config-pmap)# class c1
ciscoasa(config-pmap-c)# police output 100000
ciscoasa(config-pmap-c)#
```

> **참고:**phone-vpn을 사용하는 사용자가 AnyConnect 클라이언트 및 DTLS(Datagram Transport Layer Security)를 사용하여 전화기를 암호화할 경우 AnyConnect가 DTLS 캡슐화에서 DSCP 플래그를 보존하지 않으므로 우선 순위가 작동하지 않습니다.자세한 내용은 개선 요청 CSCtq43909를 참조하십시오.

QoS 고려 사항

다음은 QoS에 대해 고려해야 할 몇 가지 사항입니다.

- 엄격한 또는 계층적 방식으로 MPF(Modular Policy Framework)를 통해 적용됩니다.폴리싱, 쉐이핑, LLQ

  NIC(Network Interface Card)에서 DP(Data Path)로 이미 전달된 트래픽에만 영향을 줄 수 있습니다.인접한 디바이스에 적용되지 않는 이상 오버런(너무 일찍 발생)을 퇴치할 필요가 없음

- 패킷이 허용된 후 및 NIC 이전의 출력에 폴리싱이 적용됩니다.

출력에 레이어 2(L2) 주소를 다시 쓴 직후에

- 인터페이스의 모든 트래픽에 대한 아웃바운드 대역폭을 형성합니다.

  제한된 업링크 대역폭(예: 10Mb 모뎀에 대한 1기가비트 이더넷(GE) 링크)에 유용합니다.고성능 ASA558x 모델에서는 지원되지 않음

- 우선 순위 큐잉은 최선의 노력을 요하는 트래픽을 방해할 수 있습니다.

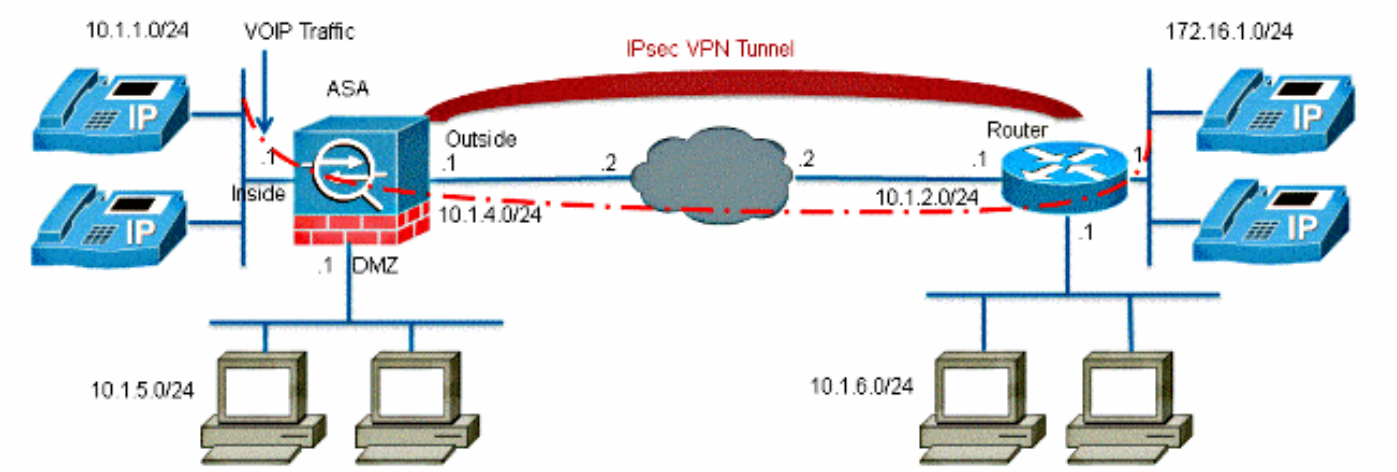
  ASA5580 또는 VLAN 하위 인터페이스의 10GE 인터페이스에서 지원되지 않음최적의 성능을 위해 인터페이스 링 크기를 더 조정할 수 있음

구성 예

VPN 터널의 VoIP 트래픽에 대한 QoS 컨피그레이션 예

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



참고:IP 전화기와 호스트가 서로 다른 세그먼트(서브넷)에 배치되었는지 확인합니다. 이 기능은 올바른 네트워크 설계에 권장됩니다.

이 문서에서는 다음 구성을 사용합니다.

- DSCP 기반 QoS 컨피그레이션
- VPN 컨피그레이션이 포함된 DSCP 기반 QoS
- ACL 기반 QoS 컨피그레이션
- VPN 컨피그레이션을 사용하는 ACL 기반 QoS

DSCP 기반 QoS 컨피그레이션

```
!--- Create a class map named Voice.

ciscoasa(config)#class-map Voice


!--- Specifies the packet that matches criteria that
!--- identifies voice packets that have a DSCP value of "ef".


ciscoasa(config-cmap)#match dscp ef


!--- Create a class map named Data.


ciscoasa(config)#class-map Data


!--- Specifies the packet that matches data traffic to be passed through
!--- IPsec tunnel.


ciscoasa(config-cmap)#match tunnel-group 10.1.2.1
ciscoasa(config-cmap)#match flow ip destination-address


!--- Create a policy to be applied to a set
!--- of voice traffic.


ciscoasa(config-cmap)#policy-map Voicepolicy


!--- Specify the class name created in order to apply
!--- the action to it.


ciscoasa(config-pmap)#class Voice


!--- Strict scheduling priority for the class Voice.

ciscoasa(config-pmap-c)#priority

PIX(config-pmap-c)#class Data


!--- Apply policing to the data traffic.


ciscoasa(config-pmap-c)#police output 200000 37500



!--- Apply the policy defined to the outside interface.


ciscoasa(config-pmap-c)#service-policy Voicepolicy interface outside
ciscoasa(config)#priority-queue outside
ciscoasa(config-priority-queue)#queue-limit 2048
```

```
ciscoasa(config-priority-queue)#tx-ring-limit 256
```

참고:"ef"의 DSCP 값은 VoIP-RTP 트래픽과 일치하는 빠른 전달을 의미합니다.

VPN 컨피그레이션이 포함된 DSCP 기반 QoS

```
ciscoasa#show running-config
: Saved
:
ASA Version 9.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet1
nameif outside
security-level 0
ip address 10.1.4.1 255.255.255.0
!

passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive


!--- This crypto ACL-permit identifies the
!--- matching traffic flows to be protected via encryption.


access-list 110 extended permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0
access-list 110 extended permit ip 10.1.5.0 255.255.255.0 10.1.6.0 255.255.255.0

pager lines 24
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
route outside 0.0.0.0 0.0.0.0 10.1.4.2 1

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart

!--- Configuration for IPsec policies.

crypto ipsec ikev1 transform-set myset esp-3des esp-sha-hmac
crypto map mymap 10 match address 110
```

```
!--- Sets the IP address of the remote end.

crypto map mymap 10 set peer 10.1.2.1

!--- Configures IPsec to use the transform-set
!--- "myset" defined earlier in this configuration.

crypto map mymap 10 set ikev1 transform-set myset
crypto map mymap interface outside

!--- Configuration for IKE policies

crypto ikev1 policy 10

!--- Enables the IKE policy configuration (config-isakmp)
!--- command mode, where you can specify the parameters that
!--- are used during an IKE negotiation.


authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400

!--- Use this command in order to create and manage the database of
!--- connection-specific records like group name
!--- as 10.1.2.1, IPsec type as L2L, and password as
!--- pre-shared key for IPsec tunnels.

tunnel-group 10.1.2.1 type ipsec-l2l
tunnel-group 10.1.2.1 ipsec-attributes

!--- Specifies the preshared key "cisco123" which should
!--- be identical at both peers.


ikev1 pre-shared-key *

telnet timeout 5
ssh timeout 5
console timeout 0
priority-queue outside
queue-limit 2048
tx-ring-limit 256
!
class-map Voice
match dscp ef
class-map Data
match tunnel-group 10.1.2.1
match flow ip destination-address
class-map inspection_default
match default-inspection-traffic

!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
```

```
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
policy-map Voicepolicy
class Voice
priority
class Data
police output 200000 37500
!
service-policy global_policy global
service-policy Voicepolicy interface outside
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

ACL 기반 QoS 컨피그레이션

```
!--- Permits inbound H.323 calls.

ciscoasa(config)#access-list 100 extended permit tcp 172.16.1.0 255.255.255.0
10.1.1.0
255.255.255.0 eq h323

!--- Permits inbound Session Internet Protocol (SIP) calls.

ciscoasa(config)#access-list 100 extended permit tcp 172.16.1.0 255.255.255.0
10.1.1.0
255.255.255.0 eq sip

!--- Permits inbound Skinny Call Control Protocol (SCCP) calls.

ciscoasa(config)#access-list 100 extended permit tcp 172.16.1.0 255.255.255.0
10.1.1.0
255.255.255.0 eq 2000

!--- Permits outbound H.323 calls.

ciscoasa(config)#access-list 105 extended permit tcp 10.1.1.0 255.255.255.0
172.16.1.0
255.255.255.0 eq h323

!--- Permits outbound SIP calls.

ciscoasa(config)#access-list 105 extended permit tcp 10.1.1.0 255.255.255.0
172.16.1.0
255.255.255.0 eq sip

!--- Permits outbound SCCP calls.

ciscoasa(config)#access-list 105 extended permit tcp 10.1.1.0 255.255.255.0
172.16.1.0
255.255.255.0 eq 2000
```

```
!--- Apply the ACL 100 for the inbound traffic of the outside interface.

ciscoasa(config)#access-group 100 in interface outside


!--- Create a class map named Voice-IN.

ciscoasa(config)#class-map Voice-IN

!--- Specifies the packet matching criteria which
!--- matches the traffic flow as per ACL 100.

ciscoasa(config-cmap)#match access-list 100


!--- Create a class map named Voice-OUT.

ciscoasa(config-cmap)#class-map Voice-OUT

!--- Specifies the packet matching criteria which
!--- matches the traffic flow as per ACL 105.

ciscoasa(config-cmap)#match access-list 105


!--- Create a policy to be applied to a set
!--- of Voice traffic.

ciscoasa(config-cmap)#policy-map Voicepolicy

!--- Specify the class name created in order to apply
!--- the action to it.

ciscoasa(config-pmap)#class Voice-IN
ciscoasa(config-pmap)#class Voice-OUT

!--- Strict scheduling priority for the class Voice.

ciscoasa(config-pmap-c)#priority
ciscoasa(config-pmap-c)#end
ciscoasa#configure terminal
ciscoasa(config)#priority-queue outside


!--- Apply the policy defined to the outside interface.

ciscoasa(config)#service-policy Voicepolicy interface outside
ciscoasa(config)#end
```

VPN 컨피그레이션을 사용하는 ACL 기반 QoS

```
ciscoasa#show running-config
: Saved
:
ASA Version 9.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0
```

```
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet1
nameif outside
security-level 0
ip address 10.1.4.1 255.255.255.0
!
interface GigabitEthernet2
nameif DMZ1
security-level 95
ip address 10.1.5.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive


!--- This crypto ACL-permit identifies the
!--- matching traffic flows to be protected via encryption.


access-list 110 extended permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0
access-list 110 extended permit ip 10.1.5.0 255.255.255.0 10.1.6.0 255.255.255.0


!--- Permits inbound H.323, SIP and SCCP calls.

access-list 100 extended permit tcp 172.16.1.0 255.255.255.0 10.1.1.0
255.255.255.0 eq h323
access-list 100 extended permit tcp 172.16.1.0 255.255.255.0 10.1.1.0
255.255.255.0 eq sip
access-list 100 extended permit tcp 172.16.1.0 255.255.255.0 10.1.1.0
255.255.255.0 eq 2000


!--- Permit outbound H.323, SIP and SCCP calls.

access-list 105 extended permit tcp 10.1.1.0 255.255.255.0 172.16.1.0
255.255.255.0 eq h323
access-list 105 extended permit tcp 10.1.1.0 255.255.255.0 172.16.1.0
255.255.255.0 eq sip
access-list 105 extended permit tcp 10.1.1.0 255.255.255.0 172.16.1.0
255.255.255.0 eq 2000
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
access-group 100 in interface outside

route outside 0.0.0.0 0.0.0.0 10.1.4.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec ikev1 transform-set myset esp-3des esp-sha-hmac
crypto map mymap 10 match address 110
```

```
crypto map mymap 10 set peer 10.1.2.1
crypto map mymap 10 set ikev1 transform-set myset
crypto map mymap interface outside
crypto ikev1 policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
tunnel-group 10.1.2.1 type ipsec-l2l
tunnel-group 10.1.2.1 ipsec-attributes
ikev1 pre-shared-key *

telnet timeout 5
ssh timeout 5
console timeout 0
priority-queue outside
!
class-map Voice-OUT
match access-list 105
class-map Voice-IN
match access-list 100
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp

!--- Inspection enabled for H.323, H.225 and H.323 RAS protocols.

inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp

!--- Inspection enabled for Skinny protocol.

inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp

!--- Inspection enabled for SIP.

inspect sip
inspect xdmcp
policy-map Voicepolicy
class Voice-IN
class Voice-OUT
priority
!
service-policy global_policy global
service-policy Voicepolicy interface outside
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
```

```
: end
```

참고:이 섹션에서 사용하는 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

서비스 정책 경찰 표시

트래픽 폴리싱에 대한 QoS 통계를 보려면 **police** 키워드와 함께 **show service-policy** 명령을 사용합니다.

```
ciscoasa(config)# show ser
ciscoasa(config)# show service-policy police
Interface outside:
Service-policy: POLICY-WEB
Class-map: Class-Policy
Output police Interface outside:
cir 1000000 bps, bc 31250 bytes
conformed 0 packets, 0 bytes; actions: transmit
exceeded 0 packets, 0 bytes; actions: drop
conformed 0 bps, exceed 0 bps
```

서비스 정책 우선 순위 표시

priority 명령을 구현하는 서비스 정책에 대한 통계를 보려면 **priority** 키워드와 함께 **show service-policy** 명령을 사용합니다.

```
ciscoasa# show service-policy priority
Global policy:
Service-policy: qos_outside_policy
Interface outside:
Service-policy: qos_class_policy
Class-map: voice-traffic
Priority:
Interface outside: aggregate drop 0, aggregate transmit 9383
```

서비스 정책 셰이프 표시

```
ciscoasa(config)# show service-policy shape
Interface outside:
Service-policy: qos_outside_policy
Class-map: class-default
shape (average) cir 2000000, bc 16000, be 16000
Queueing
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
```

우선순위 대기열 통계 표시

인터페이스에 대한 우선순위 대기열 통계를 표시하려면 특권 EXEC 모드에서 **show priority-queue statistics** 명령을 사용합니다.결과는 BE(Best-Effort) 대기열과 LLQ 모두에 대한 통계를 보여줍니다.이 예에서는 outside라는 인터페이스에 대해 **show priority-queue statistics** 명령을 사용하고 명령 출력을 보여 줍니다.

```
ciscoasa# show priority-queue statistics outside

Priority-Queue Statistics interface outside

Queue Type = BE
Packets Dropped = 0
Packets Transmit = 0
Packets Enqueued = 0
Current Q Length = 0
Max Q Length = 0

Queue Type = LLQ
Packets Dropped = 0
Packets Transmit = 0
Packets Enqueued = 0
Current Q Length = 0
Max Q Length = 0
ciscoasa#
```

이 통계 보고서에서 라인 항목의 의미는 다음과 같습니다.

- "Packets Dropped"는 이 큐에서 삭제된 패킷의 전체 수를 나타냅니다.
- "Packets Transmit"은 이 큐에서 전송된 패킷의 전체 수를 나타냅니다.
- "Packets Enqueued"는 이 큐에서 대기열에 있는 패킷의 전체 수를 나타냅니다.
- "현재 대기열 길이"는 이 대기열의 현재 깊이를 나타냅니다.
- "최대 대기열 길이"는 이 대기열에서 발생한 최대 깊이를 나타냅니다.

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

추가 정보

다음은 트래픽 셰이핑 기능에 의해 도입된 버그입니다.

Cisco 버그 ID CSCsq08550	우선 순위 큐잉이 있는 트래픽 셰이핑으로 인해 ASA에서 트래픽 오류가 발생다.
Cisco 버그 ID CSCsx07862	우선순위 큐잉을 통한 트래픽 셰이핑으로 인해 패킷 지연 및 삭제
Cisco 버그 ID CSCsq07395	정책 맵이 편집된 경우 쉐이핑 서비스 정책 추가 실패

FAQ

이 섹션에서는 이 문서에 설명된 정보와 관련하여 가장 자주 묻는 질문 중 하나에 대한 답변을 제공합니다.

VPN 터널을 통과할 때 QoS 표시가 유지됩니까?

예.제공자가 전송 중에 QoS 표시를 제거하지 않을 경우 제공자 네트워크를 통과할 때 터널에서 QoS 표시가 보존됩니다.

> **팁:**CLI Book *2*의 DSCP and DiffServ Preservation 섹션을 참조하십시오.*자세한 내용은 Cisco ASA Series Firewall CLI 컨피그레이션 가이드, 9.2*를 참조하십시오.

관련 정보

- Cisco ASA Series Firewall CLI 컨피그레이션 가이드, QoS
- QoS 정책 적용
- 클라이언트리스 SSL VPN에서 지원되지 않는 기능 이해
- QoS 구성
- 기술 지원 및 문서 – Cisco Systems