QoS nos exemplos de configuração do Cisco ASA

Contents

Introduction

Este documento explica como a Qualidade de Serviço (QoS - Quality of Service) funciona no Cisco Adaptive Security Appliance (ASA - Cisco Adaptive Security Appliance) e também fornece vários exemplos de como implementá-lo em diferentes cenários.

Você pode configurar a QoS no Security Appliance para fornecer limitação de taxa no tráfego de rede selecionado, para fluxos individuais e fluxos de túnel VPN, a fim de garantir que todo o tráfego obtenha sua parcela justa de largura de banda limitada.

O recurso foi integrado ao bug da Cisco ID CSCsk06260.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do Modular Policy Framework (MPF).

Componentes Utilizados

As informações neste documento são baseadas em um ASA que executa a versão 9.2, mas versões anteriores também podem ser usadas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

QoS é um recurso de rede que permite que você dê prioridade a determinados tipos de tráfego da Internet. À medida que os usuários da Internet atualizam seus pontos de acesso de modems para conexões de banda larga de alta velocidade, como DSL (Digital Subscriber Line) e cabo, a probabilidade aumenta de que, em um determinado momento, um único usuário possa absorver a maior parte, se não toda, da largura de banda disponível, deixando os outros usuários morrendo de fome. Para impedir que qualquer usuário ou conexão site a site consuma mais do que sua parcela justa de largura de banda, a QoS fornece um recurso de vigilância que regula a largura de banda máxima que qualquer usuário pode usar.

QoS refere-se à capacidade de uma rede de fornecer um melhor serviço para o tráfego de rede selecionado em várias tecnologias para os melhores serviços gerais com largura de banda limitada das tecnologias subjacentes.

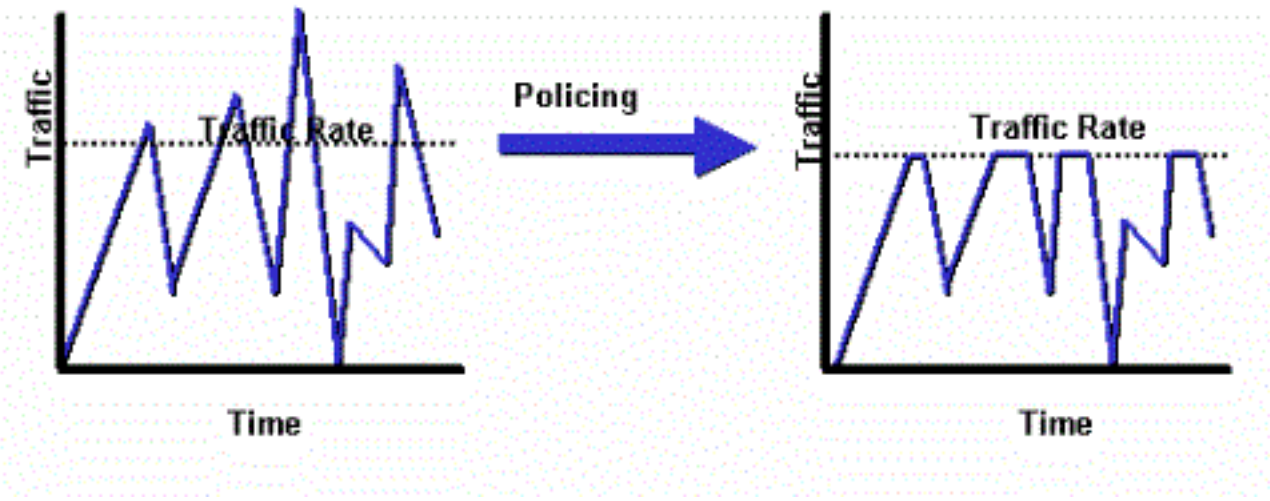
O objetivo principal da QoS no Security Appliance é fornecer limitação de taxa no tráfego de rede selecionado para fluxo individual ou fluxo de túnel VPN para garantir que todo o tráfego obtenha sua parcela justa de largura de banda limitada. Um fluxo pode ser definido de várias maneiras. No Security Appliance, a QoS pode se aplicar a uma combinação de endereços IP origem e destino, número de porta origem e destino e byte Tipo de serviço (ToS) do cabeçalho IP.

Há três tipos de QoS que você pode implementar no ASA: Policiamento, modelagem e enfileiramento de prioridade.

Políticas de tráfego

Com a vigilância, o tráfego acima de um limite especificado é descartado. O policiamento é uma forma de garantir que nenhum tráfego exceda a taxa máxima (em bits/segundo) configurada, o que garante que nenhum fluxo ou classe de tráfego possa assumir todo o recurso. Quando o tráfego excede a taxa máxima, o ASA descarta o excesso de tráfego. O policiamento também define a maior intermitência única de tráfego permitida.

Este diagrama ilustra o que a vigilância de tráfego faz; quando a taxa de tráfego atinge a taxa máxima configurada, o tráfego em excesso é descartado. O resultado é uma taxa de saída que aparece como um dente de serra com picos e depressões.



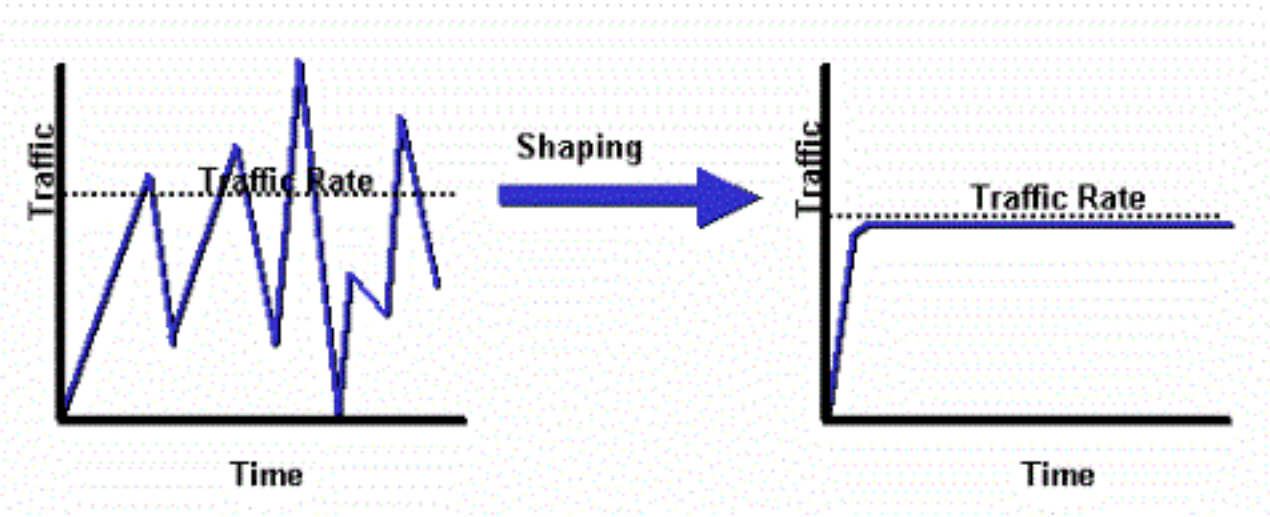
Este exemplo mostra como limitar a largura de banda para 1 Mbps para um usuário específico na direção de saída:

```
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
```

Modelagem de tráfego

A modelagem de tráfego é usada para corresponder às velocidades do dispositivo e do enlace, que controla a perda de pacotes, o atraso variável e a saturação do enlace, o que pode causar instabilidade e atraso. A modelagem de tráfego no Security Appliance permite que o dispositivo limite o fluxo de tráfego. Esse mecanismo coloca o tráfego em buffer no "limite de velocidade" e tenta enviá-lo posteriormente. A modelagem não pode ser configurada para determinados tipos de tráfego. O tráfego modelado inclui o tráfego que passa pelo dispositivo, bem como o tráfego originado do dispositivo.

Este diagrama ilustra o que a modelagem de tráfego faz; ele retém pacotes em excesso em uma fila e agenda o excesso para transmissão posterior em incrementos de tempo. O resultado da modelagem de tráfego é uma taxa de saída de pacote facilitada.



> **Note**: A modelagem de tráfego só é suportada nas versões ASA 5505, 5510, 5520, 5540 e 5550. Os modelos multicore (como o 5500-X) não suportam modelagem.

Com a modelagem de tráfego, o tráfego que excede um determinado limite é enfileirado (colocado em buffer) e enviado durante a próxima fatia de tempo.

A modelagem de tráfego no firewall é mais útil se um dispositivo upstream impõe um gargalo no tráfego da rede. Um bom exemplo seria um ASA com interfaces de 100 Mbit, com uma conexão upstream à Internet através de um modem a cabo ou T1 que termine em um roteador. A modelagem de tráfego permite que o usuário configure o throughput de saída máximo em uma interface (a interface externa, por exemplo); o firewall transmite o tráfego para fora dessa interface até a largura de banda especificada e, em seguida, tenta armazenar em buffer o tráfego excessivo para transmissão posteriormente quando o link estiver menos saturado.

A modelagem é aplicada a todo o tráfego agregado que sai da interface especificada; você não pode escolher moldar apenas determinados fluxos de tráfego.

> **Note**: A modelagem é feita após a criptografia e não permite priorização no pacote interno ou na base de grupo de túneis para VPN.

Este exemplo configura o firewall para modelar todo o tráfego de saída na interface externa para 2 Mbps:

```
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
```

Enfileiramento de prioridade

Com o enfileiramento de prioridade, você pode colocar uma classe específica de tráfego na fila de baixa latência (LLQ), que é processada antes da fila padrão.

> **Note**: Se você priorizar o tráfego em uma política de modelagem, não poderá usar os detalhes do pacote interno. O firewall só pode executar LLQ, diferentemente dos roteadores que podem fornecer mecanismos de QoS e enfileiramento mais sofisticados (Weighted Fair Queueing, WFQ, Class-Based Weighted Fair Queueing, CBWFQ, etc.).

A política de QoS hierárquica fornece um mecanismo para que os usuários especifiquem a política de QoS de forma hierárquica. Por exemplo, se os usuários quiserem modelar o tráfego em uma interface e, além disso, dentro do tráfego de interface modelado, fornecer enfileiramento de prioridade para o tráfego VoIP, os usuários poderão especificar uma política de modelagem de tráfego no topo e uma política de enfileiramento de prioridade sob a política de forma. O suporte hierárquico à política de QoS é limitado no escopo. A única opção permitida é:

- Modelagem de tráfego no nível superior
- Enfileiramento prioritário no próximo nível

> **Note**: Se você priorizar o tráfego em uma política de modelagem, não poderá usar os detalhes do pacote interno. O firewall só pode executar LLQ, diferentemente dos roteadores que podem fornecer mecanismos de QoS e enfileiramento mais sofisticados (WFQ, CBWFQ, etc.).

Este exemplo usa a política de QoS hierárquica para modelar todo o tráfego de saída na interface externa para 2 Mbps, como o exemplo de modelagem, mas também especifica que os pacotes de voz com o valor de Ponto de Código de Serviços Diferenciados (DSCP - Differentiated Services Code Point) "ef", assim como o tráfego de Shell Seguro (SSH - Secure Shell), receberão prioridade.

Crie a fila de prioridade na interface na qual deseja habilitar o recurso:

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

Uma classe para corresponder ao DSCP ef:

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

Uma classe para corresponder ao tráfego TCP/22 SSH da porta:

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

Um mapa de políticas para aplicar a priorização do tráfego de voz e SSH:

```
   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
```

Um mapa de política para aplicar modelagem a todo o tráfego e anexar tráfego de voz e SSH priorizado:

```
   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
```

Finalmente, anexe a política de modelagem à interface na qual moldar e priorizar o tráfego de saída:

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

QoS para tráfego através de um túnel VPN

QoS com VPN IPsec

Conforme RFC 2401, os bits de Tipo de Serviço (ToS) no cabeçalho IP original são copiados para o cabeçalho IP do pacote criptografado para que as políticas de QoS possam ser aplicadas após a criptografia. Isso permite que os bits de DSCP/DiffServ sejam usados para prioridade em qualquer lugar na política de QoS.

Vigilância em um túnel IPsec

A vigilância também pode ser feita para túneis VPN específicos. Para selecionar um grupo de túneis no qual policiar, use o comando **match tunnel-group <tunnel>** em class-map e o comando **match flow ip destination address**.

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

A vigilância de entrada não funciona neste momento quando você usa o comando **match tunnel-group**; consulte o bug da Cisco ID CSCth48255 para obter mais informações. Se você tentar executar a vigilância de entrada com o endereço de destino ip do fluxo de correspondência, você receberá este erro:

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

A vigilância de entrada não parece funcionar neste momento quando você usa **match tunnel-group** (ID de bug da Cisco CSCth48255). Se a vigilância de entrada funcionar, você precisaria usar um mapa de classe sem o **endereço de endereço de destino ip do fluxo de correspondência**.

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

Se você tentar policiar a saída em um mapa de classe que não tenha o **endereço de destino ip correspondente**, você receberá:

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

Também é possível executar QoS nas informações de fluxo interno com o uso de Access Control Lists (ACLs), DSCP e assim por diante. Devido ao bug mencionado anteriormente, as ACLs são a maneira de fazer a vigilância de entrada agora.

> **Note**: Um máximo de 64 mapas de políticas pode ser configurado em todos os tipos de plataforma. Use mapas de classe diferentes dentro dos mapas de política para segmentar o tráfego.

QoS com VPN SSL (Secure Sockets Layer)

Até o ASA versão 9.2, o ASA não preservou os bits ToS.

O tunelamento de VPN SSL não é suportado com esta funcionalidade. Consulte o bug da Cisco ID CSCsl73211 para obter mais informações.

```
   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)#
```

> **Note**: Quando os usuários com phone-vpn usam o cliente AnyConnect e o Datagram Transport Layer Security (DTLS) para criptografar seu telefone, a priorização não funciona porque o AnyConnect não preserva o sinalizador DSCP no encapsulamento DTLS. Consulte a solicitação de aprimoramento CSCtq43909 para obter detalhes.

Configurações de QoS

Aqui estão alguns pontos a serem considerados sobre QoS.

- Ele é aplicado através do Modular Policy Framework (MPF) de forma estrita ou hierárquica: Policiamento, modelagem, LLQ.

  Só pode influenciar o tráfego que já é passado da placa de interface de rede (NIC) para o DP (caminho de dados)Inútil para combater derrapagens (elas acontecem muito cedo), a menos que aplicadas em um dispositivo adjacente

- A vigilância é aplicada na entrada depois que o pacote é permitido e na saída antes da placa de rede.

  Logo após você reescrever um endereço de Camada 2 (L2) na saída

- Ele modela a largura de banda de saída para todo o tráfego em uma interface.

  Útil com largura de banda de uplink limitada (como link 1Gigabit Ethernet (GE) para modem de 10Mb)Não suportado nos modelos ASA558x de alto desempenho

- O enfileiramento de prioridade pode sobrecarregar o tráfego de melhor esforço.

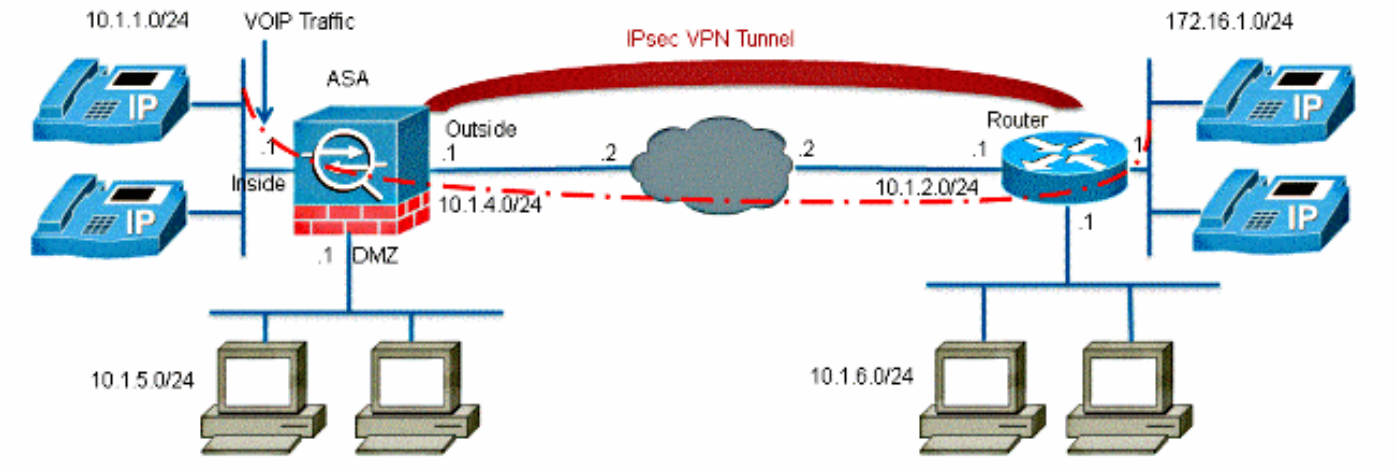
  Não suportado em interfaces 10GE no ASA5580 ou em subinterfaces de VLANO tamanho do anel da interface pode ser ajustado ainda mais para um desempenho ideal

Exemplos de configuração

Exemplo de Configuração de QoS para Tráfego VoIP em Túneis VPN

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Note: Assegure-se de que os telefones IP e os hosts sejam colocados em segmentos diferentes (sub-redes). Esta prática é recomendada para um bom design de rede.

Este documento utiliza as seguintes configurações:

- Configuração de QoS Baseada em DSCP
- Configuração de QoS Baseada em DSCP com VPN
- Configuração de QoS com base na ACL
- Configuração de QoS Baseada em ACL com VPN

Configuração de QoS Baseada em DSCP

```
!--- 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
```

Note: O valor de DSCP de "ef" refere-se ao encaminhamento expresso que corresponde ao tráfego VoIP-RTP.

Configuração de QoS Baseada em DSCP com VPN

```
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
```

Configuração de QoS com base na ACL

```
!--- 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
```

Configuração de QoS Baseada em ACL com VPN

```
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
```

> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

show service-policy police

Para visualizar as estatísticas de QoS para vigilância de tráfego, use o comando **show service-policy** com a palavra-chave **police**:

```
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
```

show service-policy priority

Para exibir estatísticas de políticas de serviço que implementam o comando **priority**, use o comando **show service-policy** com a palavra-chave **priority**:

```
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
```

show service-policy shape

```
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
```

show priority-queue statistics

Para exibir as estatísticas da fila de prioridade para uma interface, use o comando **show priority-queue statistics** no modo EXEC privilegiado. Os resultados mostram as estatísticas para a fila de melhor esforço (BE) e para o LLQ. Este exemplo mostra o uso do comando **show priority-queue statistics** para a interface chamada outside e a saída do comando.

```
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#
```

Neste relatório estatístico, o significado das rubricas é o seguinte:

- "Pacotes Descartados" indica o número total de pacotes que foram descartados nessa fila.
- "Transmissão de pacotes" indica o número total de pacotes que foram transmitidos nessa fila.
- "Pacotes Enfileirados" indica o número total de pacotes enfileirados nessa fila.
- "Comprimento atual da fila" indica a profundidade atual desta fila.
- "Comprimento máximo da fila" indica a profundidade máxima que ocorreu nessa fila.

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Additional Information

Aqui estão alguns bugs introduzidos pelo recurso de modelagem de tráfego:

ID de bug da Cisco CSCsq08550	A modelagem de tráfego com enfileiramento de prioridade causa falha de tráfego no ASA
ID de bug da Cisco CSCsx07862	A modelagem de tráfego com enfileiramento de prioridade causa atrasos e quedas de pacotes
ID de bug da Cisco CSCsq07395	A adição da política de serviço de modelagem falhará se o mapa de política tiver sido editado

FAQ

Esta seção fornece uma resposta a uma das perguntas mais frequentes em relação às informações descritas neste documento.

As marcas de QoS são preservadas quando o túnel VPN é atravessado?

Yes. As marcas de QoS são preservadas no túnel à medida que atravessam as redes do provedor se o provedor não as desencapa em trânsito.

> **Tip**: Consulte a seção Preservação de DSCP e DiffServ do *CLI Book 2: Guia de configuração da CLI do firewall Cisco ASA Series, 9.2* para obter mais detalhes.

Informações Relacionadas

- Guia de configuração da CLI do Cisco ASA Series Firewall, Qualidade de serviço
- Aplicando políticas de QoS
- Entendendo os recursos não suportados na VPN SSL sem cliente
- Configurando QoS
- Suporte Técnico e Documentação - Cisco Systems