QoS nos exemplos da configuração ASA Cisco

Índice

Introdução

Este documento explica como o Qualidade de Serviço (QoS) trabalha na ferramenta de segurança adaptável de Cisco (ASA) e igualmente fornece diversos exemplos em como executá-la para encenações diferentes.

Você pode configurar QoS na ferramenta de segurança a fim fornecer a taxa que limita no tráfego

de rede selecionado, porque fluxos do indivíduo e de túnel VPN fluxos, a fim assegurar-se de que todo o tráfego obtenha sua parte justa de largura de banda limitada.

A característica foi integrada com identificação de bug Cisco CSCsk06260.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento da política modular Framwork (MPF).

Componentes Utilizados

A informação neste documento é baseada em um ASA que execute a versão 9.2, mas as versões anterior podem ser usadas também.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

QoS é uns recursos de rede que permitam que você dê a prioridade aos determinados tipos de tráfego do Internet. Como os usuários do Internet promovem seus Access point do Modems às conexões de faixa larga de alta velocidade como o digital subscriber line (DSL) e os cabografam, os aumentos da probabilidade que a um momento determinado, um usuário único pôde poder absorver a maioria, se não toda a, largura de banda disponível, assim morrendo de fome os outros usuários. A fim impedir que toda a uma conexão do usuário ou da site para site consuma mais do que sua parte justa de largura de banda, QoS fornece uns recursos de vigilância que regulem a largura de banda máxima que qualquer usuário pode usar.

QoS refere a capacidade de uma rede de proporcionar o melhor serviço ao tráfego de rede selecionado sobre várias Tecnologias para os melhores serviços totais com a largura de banda limitada das tecnologias subjacentes.

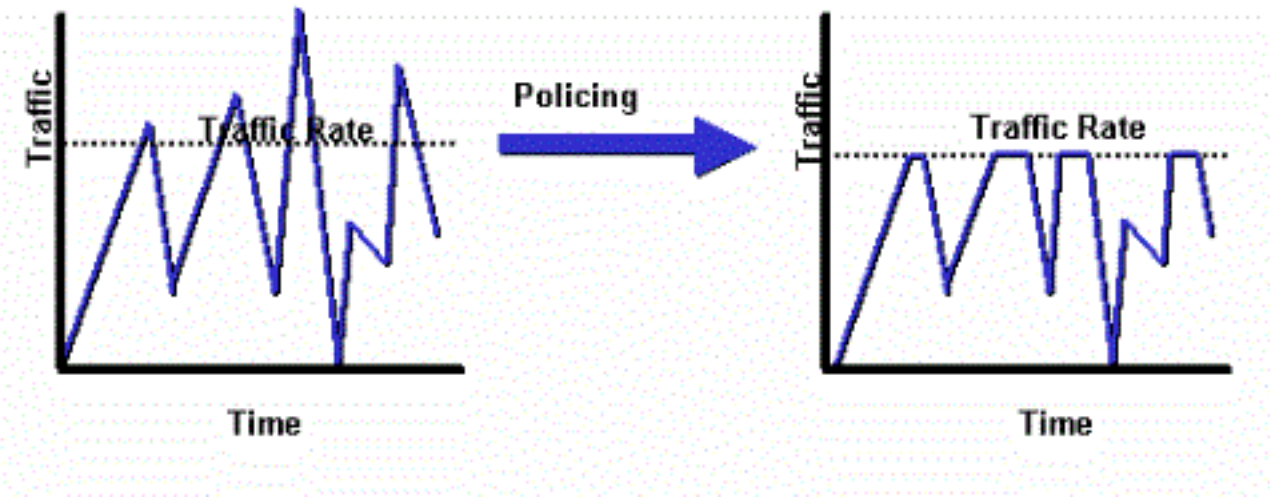
O objetivo principal de QoS na ferramenta de segurança é fornecer a taxa que limita no tráfego de rede selecionado para que o fluxo individual do fluxo ou do túnel VPN siga que todo o tráfego obtém sua parte justa de largura de banda limitada. Um fluxo pode ser definido em um número de maneiras. Na ferramenta de segurança, QoS pode aplicar-se a uma combinação de origem e aos endereços IP de destino, ao número de porta de origem e de destino, e ao byte do Tipo de serviço (ToS) do cabeçalho IP.

Há três tipos de QoS que você pode executar no ASA: Policiando, dando forma, e filas de prioridade.

Vigilância de tráfego

Com policiamento, o tráfego sobre um limite especificado é deixado cair. Policiar é uma maneira de assegurar-se de que o sem tráfego exceda a taxa máxima (nos bit/em segundo) essa você configure, que se assegura de que ninguém fluxo de tráfego ou classe possam tomar sobre o recurso inteiro. Quando o tráfego excede a taxa máxima, o ASA deixa cair o tráfego excedente. Policiar igualmente ajusta o único estouro de tráfego o maior permitido.

Este diagrama ilustra que Policiamento de tráfego faz; quando a taxa de tráfego alcança a máxima configurada de taxa, o tráfego excedente está deixado cair. O resultado é uma taxa de saída que aparece como um dente de serra com picos e depressões.



Este exemplo mostra como estrangular a largura de banda ao 1 Mbps para um usuário específico na direção externa:

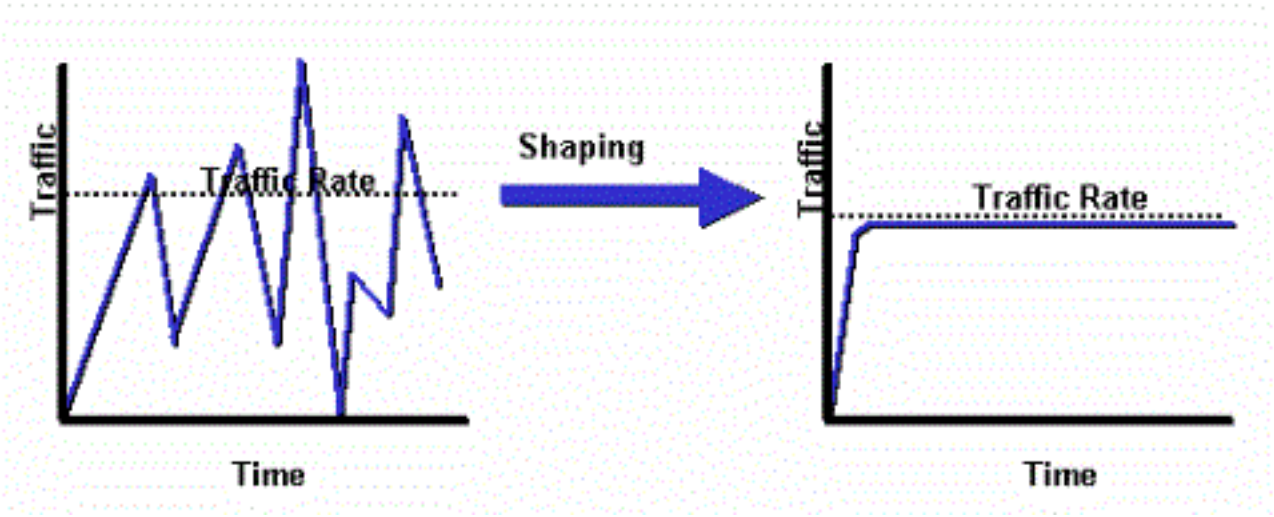
```
ciscoasa(config)# access-list WEB-LIMIT permit ip host 192.168.10.1 any
ciscoasa(config)# class-map Class-Policy
ciscoasa(config-cmap)# match access-list WEB-LIMIT
ciscoasa(config-cmap)#exit

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

O modelagem de tráfego é usado a fim combinar o dispositivo e ligar velocidades, que controla a perda de pacotes, o retardo variável, e a saturação do link, que pode causar o tremor e o atrasar. O modelagem de tráfego na ferramenta de segurança permite que o dispositivo limite o fluxo do tráfego. Este mecanismo protege o tráfego sobre de “o limite velocidade” e tenta enviar mais tarde o tráfego. Dar forma não pode ser com certeza tipos de tráfego configurados. O tráfego dado forma inclui o tráfego que passam através do dispositivo, assim como o tráfego que é originado do dispositivo.

Este diagrama ilustra que modelagem de tráfego faz; retém pacotes adicionais em uma fila e

programa então o excesso para uma transmissão mais atrasada sobre incrementos do tempo. O resultado da modelagem de tráfego é uma taxa de saída de pacote facilitada.



> Nota: O modelagem de tráfego é apoiado somente nas versões ASA 5505, 5510, 5520, 5540, e 5550. Os modelos Multicore (tais como o 5500-X) não apoiam dar forma.

Com modelagem de tráfego, o tráfego que excede um determinado limite é enfileirado (protegido) e enviado durante o timeslice seguinte.

O modelagem de tráfego no Firewall é o mais útil se um dispositivo ascendente impõe um bottlneck no tráfego de rede. Um bom exemplo seria um ASA que tivesse 100 relações de Mbit, com uma conexão de upstream ao Internet através de um modem a cabo ou de um T1 que terminasse em um roteador. O modelagem de tráfego permite que o usuário configure a taxa de transferência de partida máxima em uma relação (a interface externa por exemplo); o Firewall transmite o tráfego fora dessa relação até a largura de banda especificada, e tenta então proteger mais tarde o tráfego excessivo para a transmissão quando o link é saturado menos.

Dar forma é aplicado a todo o tráfego agregado esse saídas a interface especificada; você não pode escolher dar forma somente a determinados fluxos de tráfego.

> Nota: Dar forma é feito após a criptografia e não permite a prioridade na base do pacote interno ou do grupo de túneis para o VPN.

Este exemplo configura o Firewall a fim dar forma a todo o tráfego de saída na interface externa ao 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
```

Filas de prioridade

Com filas de prioridade, você pode colocar uma classe de tráfego específica na fila de latência baixa (LLQ), que esteja processada antes que a fila padrão.

> Nota: Se você dá a prioridade ao tráfego sob uma política moldada, você não pode usar detalhes do pacote interno. O Firewall pode somente executar o LLQ, ao contrário do Roteadores que pode fornecer um Enfileiramento e uns mecanismos de QoS mais sofisticados (enfileiramento considerável tornado mais pesado (WFQ), Class-Based Weighted Fair Queueing (CBWFQ), e assim por diante).

A política de QoS hierárquica fornece um mecanismo para que os usuários especifiquem a política de QoS em uma forma hierárquica. Por exemplo, se os usuários querem dar forma ao tráfego em uma relação e além disso dentro do tráfego dado forma da relação, forneça filas de prioridade para o tráfego voip, a seguir usuários pode especificar uma política do modelagem de tráfego na parte superior e uma política das filas de prioridade sob a política da forma. O apoio hierárquico da política de QoS é limitado no espaço. A única opção permitida é:

- Modelagem de tráfego a nível superior
- Filas de prioridade a nível seguinte

> Nota: Se você dá a prioridade ao tráfego sob uma política moldada, você não pode usar detalhes do pacote interno. O Firewall pode somente executar o LLQ, ao contrário do Roteadores que pode fornecer um Enfileiramento e uns mecanismos de QoS mais sofisticados (WFQ, CBWFQ, e assim por diante).

Este exemplo usa a política de QoS hierárquica a fim dar forma a todo o tráfego de saída na interface externa ao 2 Mbps como o exemplo dando forma mas igualmente especifica que os pacotes de voz com o Differentiated Services Code Point (DSCP) avaliam “ef”, assim como o tráfego do Shell Seguro (ssh), receberá a prioridade.

Crie a fila de prioridade na relação em que você quer permitir a característica:

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

Uma classe para combinar o DSCP ef:

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

Uma classe para combinar o tráfego da porta TCP/22 SSH:

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

Um mapa de política para aplicar a prioridade da Voz e do tráfego 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 dar forma a todo o tráfego e para anexar a Voz prioritária e o tráfego SSH:

```
   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
```

Anexe finalmente a política moldada à relação em que para dar forma e dar a prioridade ao tráfego de saída:

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

QoS para o tráfego através de um túnel VPN

QoS com IPSec VPN

Conforme bit do Tipo de serviço (ToS) do RFC 2401 no cabeçalho de IP original são copiados ao cabeçalho IP do pacote criptografado de modo que as políticas de QoS possam ser reforçadas após a criptografia. Isto permite que os bit DSCP/DiffServ sejam usados para a prioridade em qualquer lugar na política de QoS.

Policiamento em um túnel de IPsec

Policiar pode igualmente ser feito para túneis específicos VPN. A fim selecionar um grupo de túneis em que para policiar, você usa o comando do **<tunnel> do grupo de túneis do fósforo em** seu mapa de classe e no comando do **endereço de destino do fluxo IP do fósforo**.

```
 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 trabalha neste tempo quando você usa o comando do **grupo de túneis do fósforo**; veja a identificação de bug Cisco CSCth48255 para mais informação. Se você tenta fazer a vigilância de entrada com o endereço de destino do fluxo IP do fósforo, você recebe este erro:

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

A vigilância de entrada não parece trabalhar neste tempo quando você usa o **grupo de túneis do fósforo** (identificação de bug Cisco CSCth48255). Se a vigilância de entrada trabalha, você precisaria de usar um mapa de classe sem o **endereço do endereço de destino do fluxo IP do fósforo**.

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

Se você tenta policiar a saída em um mapa de classe que não tem o **endereço de destino do fósforo IP**, você recebe:

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

Éigualmente possível executar QoS na informação de fluxo interna com o uso do Access Control Lists (ACLs), DSCP, e assim por diante. Devido ao erro previamente mencionado, os ACL são a maneira de poder fazer agora a vigilância de entrada.

> Nota: Um máximo de 64 política-mapas pode ser configurado em todos os tipos de plataforma. Use mapas de classe diferentes dentro dos política-mapas a fim segmentar o tráfego.

QoS com secure sockets layer (SSL) VPN

Até a versão ASA 9.2, o ASA não preservou os bit ToS.

O Tunelamento SSL VPN não é apoiado com esta funcionalidade. Veja a identificação de bug Cisco CSCsl73211 para mais informação.

```
   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)#
```

> Nota: Quando os usuários com telefone-VPN usam a Segurança da camada do cliente e de transporte de datagram de AnyConnect (DTL) para cifrar seu telefone, o prioritisation não trabalha porque AnyConnect não preserva a bandeira DSCP no encapsulamento DTL. Refira a requisição de aprimoramento CSCtq43909 para detalhes.

Configurações de QoS

Estão aqui alguns pontos a considerar sobre QoS.

- Éaplicado através da estrutura de política modular (MPF) na forma restrita ou hierárquica: Policiamento, dando forma, LLQ.

  Pode somente influenciar o tráfego que é passado já do Network Interface Cards (NIC) ao DP (o trajeto de dados)Inútil para lutar excedentes (acontecem demasiado cedo) a menos que aplicado em um dispositivo adjacente

- Policiar está aplicado na entrada depois que o pacote é permitido e na saída antes do NIC.

Right after você reescreve um endereço da camada 2 (L2) na saída

- Dá forma à largura de banda de partida para todo o tráfego em uma relação.

  Útil com largura de banda limitada do uplink (tais Ethernet as1Gigabit (o GE) ligam ao modem 10Mb)Não apoiado em modelos de capacidade elevada ASA558x

- As filas de prioridade puderam morrer de fome o tráfego de melhor esforço.

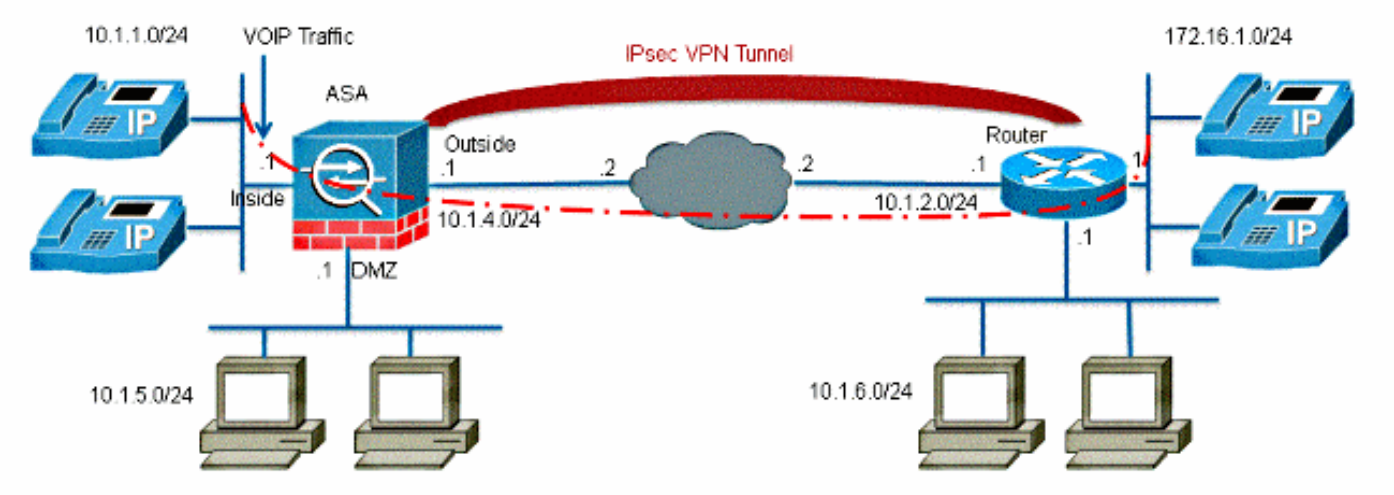
  Não apoiado em 10GE conecta em ASA5580 ou em subinterfaces de VLANO tamanho de toque da relação pode mais ser ajustado para o desempenho ótimo

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:



Nota: Assegure-se de que os Telefones IP e os anfitriões estejam 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 baseada no 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
```

Nota: O valor DSCP de “ef” refere o Expedited Forwarding a esse tráfego dos fósforos 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 baseada no 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
```

Nota: Use a ferramenta de consulta de comandos (clientes registrados somente) a fim obter mais informação que os comandos se usaram nesta seção.

Verificar

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

mostre a polícia da serviço-política

A fim ver as estatísticas de QoS para o Policiamento de tráfego, use o **comando service-policy da mostra** com a palavra-chave da **polícia**:

```
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
```

mostre a prioridade da serviço-política

A fim ver estatísticas para as políticas de serviços que executam o **comando priority**, use o **comando service-policy da mostra** com as **palavras-chave de prioridade**:

```
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
```

mostre a forma da serviço-política

```
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
```

mostre estatísticas da prioridade-fila

A fim indicar as estatísticas da prioridade-fila para uma relação, use o **comando statistics da prioridade-fila da mostra no** modo de exec privilegiado. Os resultados mostram às estatísticas para ambos a fila do (Be) do melhor esforço e o LLQ. Este exemplo mostra o uso do **comando statistics da prioridade-fila da mostra** para a relação nomeada fora, 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 dos itens de linha é como segue:

- Os “pacotes deixados cair” denotam o número total de pacotes que foram deixados cair nesta fila.
- Os “pacotes transmitem” denotam o número total de pacotes que foram transmitidos nesta fila.
- Os “pacotes enviados à fila” denotam o número total de pacotes que foram enfileirados nesta fila.
- “O comprimento atual Q” denota a profundidade atual desta fila.
- “O comprimento máximo Q” denota a profundidade máxima que ocorreu nunca nesta fila.

A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

Troubleshooting

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

Informações adicionais

Estão aqui alguns erros introduzidos pelos recursos de modelagem de tráfego:

Identificação de bug Cisco CSCsq08550	Modelagem de tráfego com falha do tráfego das causas das filas de prioridade no ASA
Identificação de bug Cisco CSCsx07862	Modelagem de tráfego com retardo do pacote e gotas das causas da de prioridade

Identificação de bug Cisco CSCsq07395	Adicionar dando forma à serviço-política falha se o mapa de política f editado

FAQ

Esta seção dá uma resposta a uma mais frequentemente das perguntas feitas com respeito à informação que é descrita neste documento.

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

Sim. As marcações de QoS estão preservadas no túnel enquanto atravessam as redes de provedor se o fornecedor não as descasca no trânsito.

> Dica: Refira o DSCP e a seção da preservação do DiffServ do *livro 2 CLI: Guia de configuração de CLI do Series Firewall de Cisco ASA, 9.2* para mais detalhes.

Informações Relacionadas

- Guia de configuração de CLI do Series Firewall de Cisco ASA, Qualidade de Serviço
- Aplicando políticas de QoS
- Compreendendo as características não apoiadas nos sem clientes SSL VPN
- Configurando QoS
- Suporte Técnico e Documentação - Cisco Systems