Ejemplos de QoS en la Configuración de Cisco ASA

Contenido

Introducción

Este documento explica cómo funciona la Calidad de servicio (QoS) en el Cisco Adaptive Security Appliance (ASA) y también proporciona varios ejemplos sobre cómo implementarla en diferentes escenarios.

Puede configurar QoS en el dispositivo de seguridad para proporcionar limitación de velocidad en el tráfico de red seleccionado, tanto para los flujos individuales como para los flujos de túnel VPN, a fin de garantizar que todo el tráfico obtenga su justa cuota de ancho de banda limitado.

La función se integró con el ID de bug de Cisco CSCsk06260.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento del marco de políticas modular (MPF).

Componentes Utilizados

La información de este documento se basa en un ASA que ejecuta la versión 9.2, pero también se pueden utilizar versiones anteriores.

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.

Antecedentes

QoS es una función de red que permite dar prioridad a determinados tipos de tráfico de Internet. A medida que los usuarios de Internet actualizan sus puntos de acceso de módems a conexiones de banda ancha de alta velocidad, como Digital Subscriber Line (DSL) y cable, aumenta la probabilidad de que, en un momento dado, un solo usuario pueda absorber la mayor parte, si no la totalidad, del ancho de banda disponible, con lo que los demás usuarios se quedarán sin servicio. Para evitar que una conexión de usuario o de sitio a sitio consuma más de lo que le corresponde en ancho de banda, QoS proporciona una función de regulación que regula el ancho de banda máximo que cualquier usuario puede utilizar.

QoS hace referencia a la capacidad de una red para proporcionar un mejor servicio al tráfico de red seleccionado a través de diversas tecnologías para ofrecer los mejores servicios generales con un ancho de banda limitado de las tecnologías subyacentes.

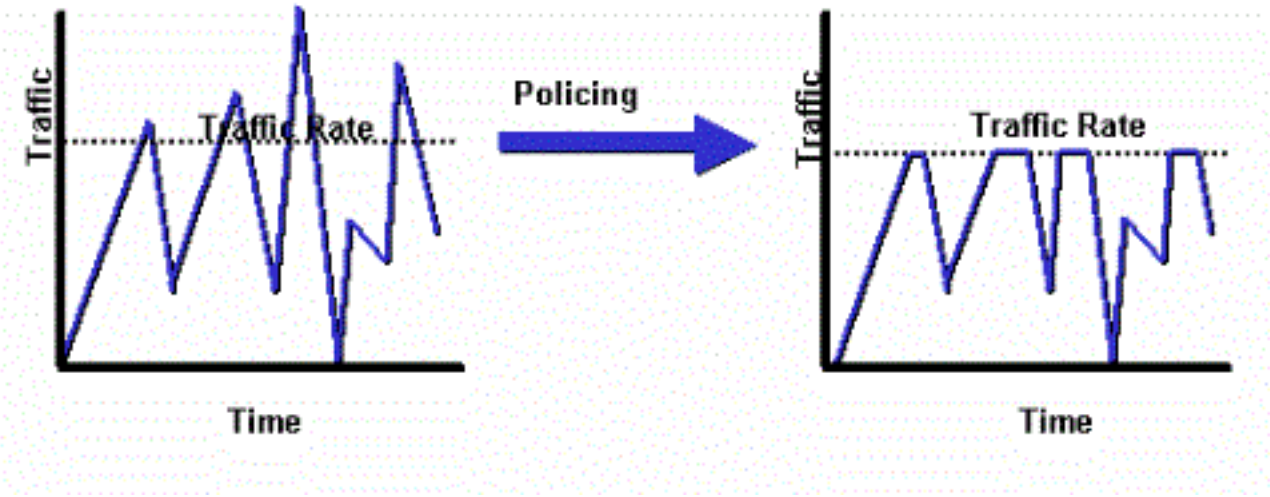
El objetivo principal de QoS en el dispositivo de seguridad es proporcionar limitación de velocidad en el tráfico de red seleccionado tanto para el flujo individual como para el flujo de túnel VPN para garantizar que todo el tráfico obtenga su justa cuota de ancho de banda limitado. Un flujo se puede definir de varias maneras. En el dispositivo de seguridad, QoS se puede aplicar a una combinación de direcciones IP de origen y de destino, número de puerto de origen y de destino y byte de tipo de servicio (ToS) del encabezado IP.

Hay tres tipos de QoS que puede implementar en el ASA: Regulación, Modelado y Colocación en Cola Prioritaria.

Regulación del tráfico

Con la regulación del tráfico, se descarta el tráfico por encima de un límite especificado. La regulación de tráfico es una manera de asegurar que ningún tráfico exceda la velocidad máxima (en bits/segundo) que se configura, lo que asegura que ningún flujo de tráfico o clase pueda tomar el control de todo el recurso. Cuando el tráfico excede la velocidad máxima, el ASA descarta el exceso de tráfico. La regulación también establece la mayor ráfaga de tráfico permitida.

Este diagrama ilustra lo que hace la regulación del tráfico; cuando la velocidad de tráfico alcanza la velocidad máxima configurada, se descarta el tráfico excesivo. El resultado es una velocidad de salida que tiene la apariencia de un diente de sierra, con crestas y depresiones.



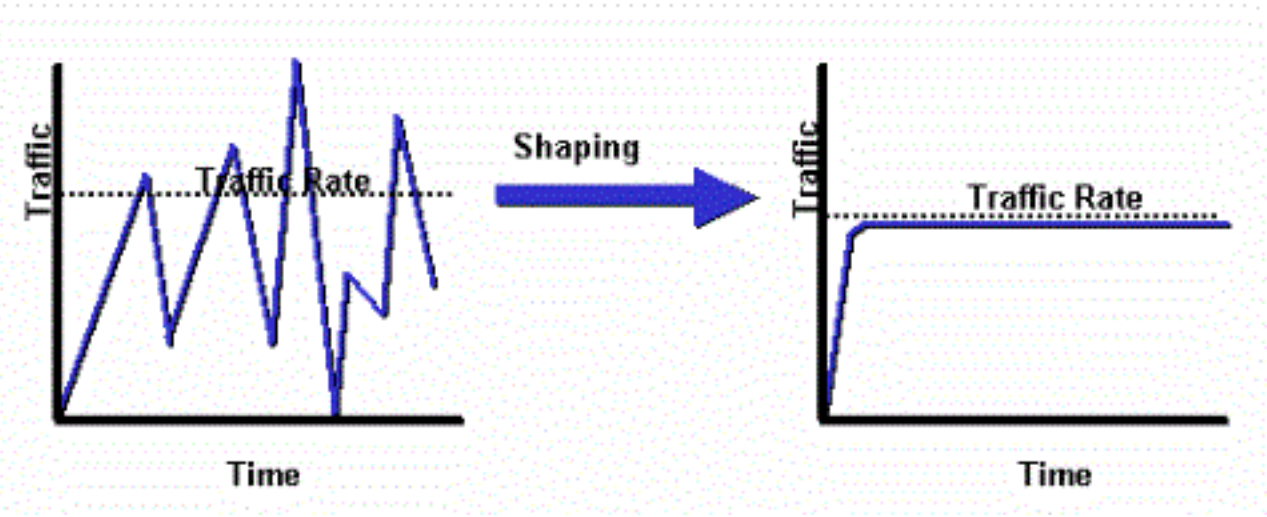
Este ejemplo muestra cómo limitar el ancho de banda a 1 Mbps para un usuario específico en la dirección saliente:

```
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
```

Modelado de tráfico

El modelado del tráfico se utiliza para hacer coincidir las velocidades del dispositivo y del link, que controla la pérdida de paquetes, el retraso variable y la saturación del link, lo que puede causar fluctuación y retraso. El modelado del tráfico en el dispositivo de seguridad permite al dispositivo limitar el flujo de tráfico. Este mecanismo almacena el tráfico en el búfer sobre el "límite de velocidad" e intenta enviar el tráfico más tarde. El modelado no se puede configurar para ciertos tipos de tráfico. El tráfico modelado incluye el tráfico que pasa a través del dispositivo, así como el tráfico que se origina del dispositivo.

Este diagrama ilustra lo que hace el modelado del tráfico; retiene los paquetes excedentes en una cola y luego programa el exceso para una transmisión posterior en incrementos de tiempo. El resultado del diseño del tráfico es una velocidad atenuada del paquete de salida.



> **Nota:** El modelado de tráfico sólo se admite en las versiones 5505, 5510, 5520, 5540 y 5550 de ASA. Los modelos de varios núcleos (como el 5500-X) no admiten el modelado.

Con el modelado del tráfico, el tráfico que excede un determinado límite se coloca en cola (almacenado en búfer) y se envía durante el siguiente tiempo.

El modelado del tráfico en el firewall es más útil si un dispositivo ascendente impone un cuello de botella en el tráfico de red. Un buen ejemplo sería un ASA que tiene interfaces de 100 Mbit, con una conexión ascendente a Internet a través de un cable módem o T1 que termina en un router. El modelado del tráfico permite al usuario configurar el rendimiento máximo saliente en una interfaz (por ejemplo, la interfaz externa); el firewall transmite el tráfico de esa interfaz hasta el ancho de banda especificado y, a continuación, intenta almacenar en búfer el tráfico excesivo para la transmisión más tarde cuando el link está menos saturado.

El modelado se aplica a todo el tráfico agregado que sale de la interfaz especificada; no puede elegir dar forma a ciertos flujos de tráfico solamente.

> **Nota:** El modelado se realiza después del cifrado y no permite la priorización en el paquete interno o en el túnel-grupo para VPN.

Este ejemplo configura el firewall para modelar todo el tráfico saliente en la interfaz exterior a 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
```

Envío a Cola Prioritario

Con la cola de prioridad, puede colocar una clase específica de tráfico en la cola de baja latencia (LLQ), que se procesa antes de la cola estándar.

> **Nota:** Si da prioridad al tráfico bajo una política de modelado, no puede utilizar los detalles internos del paquete. El firewall sólo puede realizar LLQ, a diferencia de los routers que pueden proporcionar mecanismos de cola y QoS más sofisticados (Weighted Fair Queueing (WFQ), Class-Based Weighted Fair Queueing (CBWFQ), etc.).

La política jerárquica de QoS proporciona un mecanismo para que los usuarios especifiquen la política de QoS de una manera jerárquica. Por ejemplo, si los usuarios desean modelar el tráfico en una interfaz y, además, dentro del tráfico de interfaz modelado, proporcionan cola de prioridad para el tráfico VoIP, los usuarios pueden especificar una política de modelado de tráfico en la parte superior y una política de colocación en cola de prioridad en la política de formas. El alcance del soporte jerárquico de la política de QoS está limitado. La única opción permitida es:

- Modelado del tráfico en el nivel superior
- Cola prioritaria en el siguiente nivel

> **Nota:** Si da prioridad al tráfico bajo una política de modelado, no puede utilizar los detalles internos del paquete. El firewall sólo puede realizar LLQ, a diferencia de los routers que pueden proporcionar mecanismos de QoS y cola más sofisticados (WFQ, CBWFQ, etc.).

Este ejemplo utiliza la política de QoS jerárquica para dar forma a todo el tráfico saliente en la interfaz exterior a 2 Mbps como el ejemplo de modelado, pero también especifica que los paquetes de voz con el valor "ef" del punto de código de servicios diferenciados (DSCP), así como el tráfico de Secure Shell (SSH), recibirán prioridad.

Cree la cola de prioridad en la interfaz en la que desea habilitar la función:

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

Una clase que coincida con el resultado DSCP:

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

Una clase que coincida con el tráfico TCP/22 SSH del puerto:

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

Un mapa de política para aplicar la prioridad del tráfico de voz y 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
```

Un mapa de política para aplicar el modelado a todo el tráfico y adjuntar tráfico de voz y 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
```

Por último, adjunte la política de modelado a la interfaz en la que modelar y priorizar el tráfico saliente:

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

QoS para el tráfico a través de un túnel VPN

QoS con VPN IPsec

Según RFC 2401, los bits de tipo de servicio (ToS) del encabezado IP original se copian en el encabezado IP del paquete cifrado para que las políticas de QoS se puedan aplicar después del cifrado. Esto permite que los bits DSCP/DiffServ se utilicen como prioridad en cualquier lugar de la política de QoS.

Regulación de tráfico en un túnel IPsec

La regulación también se puede realizar para túneles VPN específicos. Para seleccionar un grupo de túnel en el que se debe vigilar, usted utiliza el comando **match tunnel-group <tunnel>** en su mapa de clase y el 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
```

La regulación de entrada no funciona en este momento cuando se utiliza el comando **match tunnel-group**; consulte Cisco bug ID CSCth48255 para obtener más información. Si intenta realizar el control de tráfico de entrada con la dirección ip de destino del flujo coincidente, recibe este error:

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

La regulación de entrada no parece funcionar en este momento cuando utiliza **match tunnel-group** (ID de bug Cisco CSCth48255). Si la regulación de entrada funciona, necesitará utilizar un mapa de clase sin la **dirección ip de destino del flujo coincidente**.

```
  class-map tgroup_in
```

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

Si intenta controlar la salida en un mapa de clase que no tiene la **dirección de destino ip coincidente**, recibirá:

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

También es posible realizar QoS en la información de flujo interno con el uso de listas de control de acceso (ACL), DSCP, etc. Debido al error mencionado anteriormente, las ACL son la manera de poder realizar la regulación de entrada ahora mismo.

> **Nota:** Se puede configurar un máximo de 64 mapas de políticas en todos los tipos de plataforma. Utilice diferentes class-maps dentro de policy-maps para segmentar el tráfico.

QoS con VPN de capa de conexión segura (SSL)

Hasta la versión 9.2 de ASA, el ASA no conservaba los bits ToS.

La tunelización VPN SSL no se soporta con esta funcionalidad. Consulte Cisco bug ID CSCsl73211 para obtener más información.

```
   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:** Cuando los usuarios con vpn de teléfono utilizan el cliente AnyConnect y Datagram Transport Layer Security (DTLS) para cifrar su teléfono, la priorización no funciona porque AnyConnect no conserva el indicador DSCP en la encapsulación DTLS. Refiérase a la solicitud de mejora CSCtq43909 para obtener detalles.

Consideraciones de QoS

A continuación se indican algunos puntos que se deben tener en cuenta sobre QoS.

- Se aplica a través de un marco de políticas modular (MPF) de forma estricta o jerárquica:

Vigilancia, modelado, LLQ.

Sólo puede influir en el tráfico que ya se pasa de la tarjeta de interfaz de red (NIC) al DP (ruta de datos)Inútil para combatir los desbordamientos (se producen demasiado pronto) a menos que se apliquen en un dispositivo adyacente

- La regulación se aplica en la entrada después de que se permita el paquete y en la salida antes de la NIC.

  Justo después de reescribir una dirección de Capa 2 (L2) en la salida

- Configura el ancho de banda saliente para todo el tráfico en una interfaz.

  Útil con ancho de banda de enlace ascendente limitado (como el enlace de 1 Gigabit Ethernet (GE) al módem de 10 Mb)No compatible con los modelos ASA558x de alto rendimiento

- La colocación en cola prioritaria puede provocar el hambre del tráfico de mejor esfuerzo.

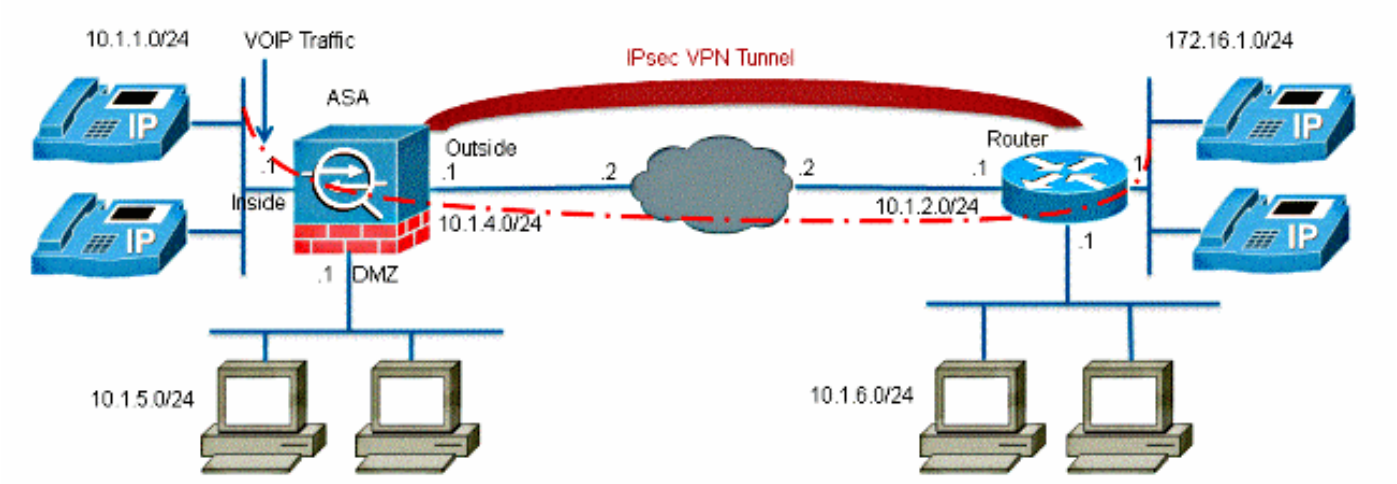
  No se admite en interfaces 10GE en subinterfaces ASA5580 o VLANEl tamaño del anillo de la interfaz se puede ajustar aún más para lograr un rendimiento óptimo

Ejemplos de Configuración

Ejemplo de Configuración de QoS para Tráfico VoIP en Túneles VPN

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Nota: Asegúrese de que los teléfonos IP y los hosts se coloquen en diferentes segmentos (subredes). Esto se recomienda para un buen diseño de red.

En este documento, se utilizan estas configuraciones:

- Configuración de QoS basada en DSCP
- QoS basada en DSCP con configuración VPN
- Configuración de QoS basada en ACL
- QoS basada en ACL con configuración VPN

Configuración de QoS basada en 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: El valor DSCP de "ef" se refiere al reenvío acelerado que coincide con el tráfico VoIP-RTP.

QoS basada en DSCP con configuración 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
```

Configuración de QoS basada en 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
```

QoS basada en ACL con configuración 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:** Utilice la Command Lookup Tool (sólo clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

show service-policy police

Para ver las estadísticas de QoS para la regulación del tráfico, utilice el comando **show service-policy** con la palabra clave **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 ver las estadísticas de las políticas de servicio que implementan el comando **priority**, utilice el comando **show service-policy** con la palabra clave **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 mostrar las estadísticas de cola de prioridad para una interfaz, utilice el comando **show priority-queue statistics** en el modo EXEC privilegiado. Los resultados muestran las estadísticas tanto para la cola de mejor esfuerzo (BE) como para la LLQ. Este ejemplo muestra el uso del comando **show priority-queue statistics** para la interfaz denominada outside y el resultado del 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#
```

En este informe estadístico, el significado de las partidas es el siguiente:

- "Paquetes descartados" denota el número total de paquetes que se han descartado en esta cola.
- "Transmisión de paquetes" denota el número total de paquetes que se han transmitido en esta cola.
- "Paquetes puestos en cola" denota el número total de paquetes que se han puesto en cola en esta cola.
- "Longitud actual de Q" denota la profundidad actual de esta cola.
- "Longitud máxima de Q" indica la profundidad máxima que se ha producido en esta cola.

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Additional Information

A continuación se muestran algunos errores introducidos por la función de modelado de tráfico:

Id. de bug Cisco CSCsq08550	El modelado del tráfico con cola prioritaria provoca fallos de tráfico en ASA
Id. de bug Cisco CSCsx07862	El modelado del tráfico con cola de prioridad provoca retrasos y caídas de paquetes
Id. de bug Cisco CSCsq07395	Si se ha editado policy-map, se produce un error en la adición de la política de servicio de modelado

Preguntas frecuentes

Esta sección proporciona una respuesta a una de las preguntas más frecuentes con respecto a la información que se describe en este documento.

¿Se conservan las marcas de QoS cuando se atraviesa el túnel VPN?

Yes. Las marcas de QoS se conservan en el túnel cuando atraviesan las redes del proveedor si el proveedor no las tira en tránsito.

> **Consejo:** Consulte la sección Preservación DSCP y DiffServ del *Libro 2 de CLI: Guía de Configuración de Cisco ASA Series Firewall CLI, 9.2* para obtener más detalles.

Información Relacionada

- Guía de configuración de Cisco ASA Series Firewall CLI, calidad de servicio
- Aplicación de políticas de QoS
- Introducción a las Funciones no Soportadas en Clientless SSL VPN
- Configuración de QoS
- Soporte Técnico y Documentación - Cisco Systems