QoS en los ejemplos de la configuración de ASA de Cisco

Contenido

Introducción

Este documento explica cómo el Calidad de Servicio (QoS) trabaja en el dispositivo de seguridad adaptante de Cisco (ASA) y también proporciona varios ejemplos en cómo implementarlo para diversos escenarios.

Usted puede configurar QoS en el dispositivo de seguridad para proporcionar la tarifa que limita en el tráfico de la red seleccionada, porque los flujos del individuo y los flujos del túnel VPN, para asegurarse de que todo el tráfico consigue su reparto justo del ancho de banda limitado.

La característica fue integrada con el Id. de bug Cisco CSCsk06260.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de la directiva modular Framwork (MPF).

Componentes Utilizados

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

QoS es una función de red que permite que usted dé la prioridad a los tipos determinados de tráfico de Internet. Como los usuarios de Internet actualizan sus Puntos de acceso de los módems a las conexiones de banda ancha de alta velocidad como el Digital Subscriber Line (DSL) y telegrafían, los aumentos de la probabilidad que en cualquier momento, un único usuario pudo poder absorber la mayoría, si no todo el, ancho de banda disponible, así muriendo de hambre a los otros usuarios. Para evitar que cualquier una conexión del usuario o del sitio a localizar consuma más que su reparto justo del ancho de banda, QoS proporciona una característica de regulación de tráfico que regule el ancho de banda máximo que cualquier usuario puede utilizar.

QoS refiere a la capacidad de una red para proporcionar un mejor servicio al tráfico de la red seleccionada sobre las diversas Tecnologías para los mejores servicios totales con el ancho de banda limitado de las tecnologías subyacentes.

El objetivo principal de QoS en el dispositivo de seguridad es proporcionar la tarifa que limita en el tráfico de la red seleccionada para que el flujo individual del flujo o del túnel VPN siga que todo el tráfico consigue su reparto justo del ancho de banda limitado. Un flujo se puede definir de varias maneras. En el dispositivo de seguridad, QoS puede aplicarse a una combinación de origen y a los IP Address de destino, al número del puerto de origen y de destino, y al byte del Tipo de servicio (ToS) del encabezado IP.

Hay tres clases de QoS que usted puede implementar en el ASA: Policing, shaping, y espera de la prioridad.

Regulación del tráfico

Con el policing, el tráfico sobre un límite especificado se cae. El policing es una manera de asegurarse de que ningún tráfico excede la velocidad máxima (en los dígitos por segundo) esa usted la configuración, que se asegura de que nadie flujo de tráfico o clase pueda asumir el control el recurso entero. Cuando el tráfico excede la velocidad máxima, el ASA cae el tráfico en exceso. La vigilancia también fija la sola ráfaga de tráfico más grande permitida.

Este diagrama ilustra lo hace qué Vigilancia de tráfico; cuando las relaciones del tráfico alcanzan el Máximo configurado de tarifa, se cae el tráfico en exceso. El resultado es una velocidad de salida que tiene la apariencia de un diente de sierra, con crestas y depresiones.

Este ejemplo muestra cómo estrangular el ancho de banda al 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 de tráfico se utiliza para hacer juego el dispositivo y conectar las velocidades, que controla la pérdida del paquete, el Retraso variable, y la saturación del link, que puede causar el jitter y retrasar. El modelado de tráfico en el dispositivo de seguridad permite que el dispositivo limite el flujo de tráfico. Este mecanismo mitiga el tráfico sobre el “límite de velocidad” e intenta enviar el tráfico más adelante. El shaping no puede ser con certeza tipos de tráfico configurados. El tráfico formado incluye el tráfico que pasa a través del dispositivo, así como el tráfico que es originado del dispositivo.

Este diagrama ilustra lo hace qué modelado de tráfico; conserva los paquetes en exceso en una cola y después programa el exceso para la transmisión posterior sobre los incrementos del tiempo. El resultado del diseño del tráfico es una velocidad atenuada del paquete de salida.

> Nota: El modelado de tráfico se soporta solamente en las Versiones de ASA 5505, 5510, 5520, 5540, y 5550. Los modelos multifilares (tales como el 5500-X) no soportan el shaping.

Con el modelado de tráfico, se hace cola (mitigado) y se envía el tráfico que se excede cierto límite durante el timeslice siguiente.

El modelado de tráfico en el Firewall es el más útil si un dispositivo ascendente impone un bottlneck ante el tráfico de la red. Un buen ejemplo sería un ASA que tiene 100 interfaces de Mbit, con una conexión ascendente a Internet vía un módem de cable o un T1 que termina en un router. El modelado de tráfico permite que el usuario configure la producción saliente máxima en

una interfaz (la interfaz exterior por ejemplo); el Firewall transmite el tráfico fuera de esa interfaz hasta el ancho de banda especificado, y después intenta mitigar el tráfico excesivo para la transmisión más adelante cuando el link se satura menos.

El shaping se aplica a todo el tráfico total ese las salidas la interfaz especificada; usted no puede elegir formar solamente ciertos flujos de tráfico.

> Nota: El shaping se hace después del cifrado y no tiene en cuenta el priorización sobre la base del paquete interno o del grupo de túnel para el VPN.

Este ejemplo configura el Firewall para formar todo el tráfico saliente en la interfaz exterior al 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
```

Espera de la prioridad

Con la cola prioritaria, usted puede poner una clase de tráfico específica en la cola de tiempo de latencia bajo (LLQ), que se procesa antes de la cola estándar.

> Nota: Si usted da prioridad al tráfico bajo política de modelado, usted no puede utilizar los detalles del paquete interno. El Firewall puede realizar solamente el LLQ, a diferencia del Routers que puede proporcionar Datos en espera y mecanismos de Calidad de servicio (QoS) más sofisticados (espera cargada de la feria (WFQ), del Mecanismo de cola de espera equitativo y ponderado basado en clases (CBWFQ), y así sucesivamente).

El jerárquico política de calidad de servicio (QoS) proporciona un mecanismo para que los usuarios especifiquen política de calidad de servicio (QoS) en una moda jerárquica. Por ejemplo, si los usuarios quieren formar el tráfico en una interfaz y además dentro del tráfico formado de la interfaz, proporcione la prioridad que hace cola para el tráfico de VoIP, después a los usuarios puede especificar una directiva del modelado de tráfico en el top y una directiva de la cola prioritaria bajo directiva de la dimensión de una variable. Política de calidad de servicio (QoS) el soporte jerárquico se limita en el alcance. La única opción permitida es:

- Modelado de tráfico en el nivel superior
- Prioridad que hace cola en el nivel siguiente

> Nota: Si usted da prioridad al tráfico bajo política de modelado, usted no puede utilizar los detalles del paquete interno. El Firewall puede realizar solamente el LLQ, a diferencia del Routers que puede proporcionar Datos en espera y mecanismos de Calidad de servicio (QoS) más sofisticados (WFQ, CBWFQ, y así sucesivamente).

Este ejemplo utiliza el jerárquico política de calidad de servicio (QoS) para formar todo el tráfico saliente en la interfaz exterior al 2 Mbps como el ejemplo del shaping pero también especifica que los paquetes de voz con el Differentiated Services Code Point (DSCP) valoran “ef”, así como el

tráfico del Secure Shell (SSH), recibirá la prioridad.

Cree el priority queue en la interfaz en la cual usted quiere habilitar la característica:

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

Una clase para hacer juego el DSCP ef:

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

Una clase para hacer juego el tráfico del puerto TCP/22 SSH:

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

Una correspondencia de políticas para aplicar el priorización de la Voz y del tráfico de 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
```

Una correspondencia de políticas para aplicar el shaping a todo el tráfico y para asociar la Voz y el tráfico prioritarios de 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
```

Finalmente asocie la política de modelado a la interfaz en la cual formar y dar prioridad al tráfico saliente:

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

QoS para el tráfico a través de un túnel VPN

QoS con el IPSec VPN

Según los bits del Tipo de servicio (ToS) del RFC 2401 en el encabezado IP original se copian al encabezado IP del paquete encriptado para poder aplicar las directivas de QoS después del cifrado. Esto permite que los bits DSCP/DiffServ sean utilizados para la prioridad dondequiera en política de calidad de servicio (QoS).

Policing en un túnel IPsec

El policing se puede también hacer para los túneles específicos VPN. Para seleccionar a un grupo de túnel en quien limpiar, usted utiliza el comando del **<tunnel> del grupo de túnel de la**

coincidencia en su clase-mapa y el comando del **IP Destination Address del flujo de la coincidencia**.

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

Las Políticas de entrada no trabajan ahora cuando usted utiliza el comando del **grupo de túnel de la coincidencia**; vea el Id. de bug Cisco CSCth48255 para más información. Si usted intenta hacer las Políticas de entrada con el IP Destination Address del flujo de la coincidencia, usted recibe este error:

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

Las Políticas de entrada no aparecen trabajar ahora cuando usted utiliza el **grupo de túnel de la coincidencia** (Id. de bug Cisco CSCth48255). Si las Políticas de entrada trabajan, usted necesitaría utilizar un clase-mapa sin el **direccionamiento del IP Destination Address del flujo de la coincidencia**.

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

Si usted intenta limpiar la salida en un clase-mapa que no tenga el **IP Destination Address de la coincidencia**, usted recibe:

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

Es también posible realizar QoS en la información de flujo interna con el uso del Listas de control de acceso (ACL), DSCP, y así sucesivamente. Debido al bug previamente mencionado, los ACL son la manera de poder hacer las Políticas de entrada ahora.

> Nota: Un máximo de 64 correspondencias de políticas se puede configurar en todos los tipos de plataforma. Utilice diverso class-maps dentro de las correspondencias de políticas para dividir el tráfico en segmentos.

QoS con Secure Sockets Layer (SSL) VPN

Hasta la Versión de ASA 9.2, el ASA no preservó los bits TOS.

El Tunelización SSL VPN no se soporta con estas funciones. Vea el Id. de bug Cisco CSCsl73211 para 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 teléfono-VPN utilizan la Seguridad de la capa del cliente y de transporte de datagrama de AnyConnect (DTL) para cifrar su teléfono, la priorización no trabaja porque AnyConnect no preserva el indicador DSCP en la encapsulación DTL. Refiera al pedido de mejora CSCtq43909 para los detalles.

Consideraciones de QoS

Aquí están algunas puntas a considerar sobre QoS.

- Es aplicado a través del Marco de políticas modular (MPF) en la moda estricta o jerárquica: Policing, shaping, LLQ.

  Puede influenciar solamente el tráfico que se pasa ya del Network Interface Cards (NIC) al DP (el trayecto de datos)Inútil luchar los sobrantes (suceden demasiado temprano) a menos que esté aplicado en un dispositivo adyacente

- El policing se aplica en la entrada después de que el paquete se permita y en la salida antes del NIC.

  Justo después de que usted reescribe un direccionamiento de la capa 2 (L2) en la salida

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

  Útil con el ancho de banda limitado del uplink (tales Ethernetes as1Gigabit (GE) conectan al módem 10Mb)No soportado en los modelos de alto rendimiento ASA558x

- La cola prioritaria pudo morir de hambre tráfico Best-Effort (mejor esfuerzo).

  No soportado en 10GE interconecta en ASA5580 o las subinterfaces del VLANEl tamaño de anillo de la interfaz se puede ajustar más a fondo para el rendimiento óptimo

Ejemplos de Configuración

QoS para el tráfico de VoIP en el VPN hace un túnel el ejemplo de configuración

Diagrama de la red

En este documento, se utiliza esta configuración de red:

> Nota: Asegúrese de que los Teléfonos IP y los host estén puestos en diversos segmentos (subredes). Esto se recomienda para un buen diseño de red.

En este documento, se utilizan estas configuraciones:

- Configuración de QoS basada en el DSCP
- QoS basó en el DSCP con la configuración VPN
- Configuración de QoS basada en el ACL
- QoS basó en el ACL con la configuración VPN

Configuración de QoS basada en el 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” refiere al Expedited Forwarding que haga juego el tráfico VoIP-RTP.

QoS basó en el DSCP con la 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 el 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 basó en el ACL con la 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 herramienta de búsqueda de comandos (clientes registrados solamente) para obtener más información que los comandos utilizaron en esta sección.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

muestre la policía de la servicio-directiva

Para ver las estadísticas de QoS para la Vigilancia de tráfico, utilice el **comando service-policy de la demostración** con la palabra clave de la **policía**:

```
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
```

muestre la prioridad de la servicio-directiva

Para ver las estadísticas para las políticas de servicio que implementan el **comando priority**, utilice el **comando service-policy de la demostración** con la **palabra clave de prioridad**:

```
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
```

muestre la dimensión de una variable de la servicio-directiva

```
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
```

muestre las estadísticas de la prioridad-cola

Para visualizar las estadísticas de la prioridad-cola para una interfaz, utilice el **comando statistics de la prioridad-cola de la demostración** en el modo EXEC privilegiado. Los resultados muestran las estadísticas para la cola de (Be) de mejor esfuerzo y el LLQ. Este ejemplo muestra el uso del **comando statistics de la prioridad-cola de la demostración** para la interfaz nombrada afuera, y la salida de 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 los elemntos de línea es como sigue:

- Los “paquetes caídos” denotan el número total de paquetes que se han caído en esta cola.
- Los “paquetes transmiten” denotan el número total de paquetes que se han transmitido en esta cola.
- Los “paquetes enviados a la cola” denotan el número total de paquetes que se han hecho cola en esta cola.
- La “longitud actual Q” denota la profundidad actual de esta cola.
- La “longitud máxima Q” denota la profundidad máxima que ocurrió nunca en esta cola.

La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

Troubleshooting

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

Información adicional

Aquí están algunos bug introducidos por la Función de modelado del tráfico:

Id. de bug Cisco CSCsq08550	Modelado de tráfico con el error de espera del tráfico de las causas de la priori en el ASA
Id. de bug Cisco CSCsx07862	Modelado de tráfico con el retraso de paquetes y los descensos de espera de l causas de la prioridad
Id. de bug Cisco CSCsq07395	Agregar la servicio-directiva del shaping falla si se ha editado el directiva-mapa

FAQ

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

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

Sí. Las marcas de QoS se preservan en el túnel mientras que atraviesan las Redes proveedora si el proveedor no las elimina adentro transita.

> Consejo: Refiera al DSCP y a la sección de la preservación del DiffServ del *libro 2 CLI: Guía de configuración CLI del Firewall de la serie de Cisco ASA, 9.2* para más detalles.

Información Relacionada

- Guía de configuración CLI del Firewall de la serie de Cisco ASA, calidad de servicio
- Aplicación de las directivas de QoS
- Comprensión de las características no soportadas en el clientless SSL VPN
- Configuración de QoS
- Soporte Técnico y Documentación - Cisco Systems