QoS sur les exemples de configuration Cisco ASA

Contenu

Introduction

Ce document explique le fonctionnement de la qualité de service (QoS) sur l'appliance de sécurité adaptative (ASA) de Cisco et fournit également plusieurs exemples sur la façon de l'implémenter pour différents scénarios.

Vous pouvez configurer la QoS sur l'appliance de sécurité afin de fournir une limitation de débit sur le trafic réseau sélectionné, à la fois pour les flux individuels et les flux de tunnel VPN, afin de vous assurer que tout le trafic reçoit sa juste part de bande passante limitée.

Cette fonctionnalité a été intégrée à l'ID de bogue Cisco CSCsk06260.

Conditions préalables

Conditions requises

Cisco recommande que vous connaissiez le cadre de politique modulaire (MPF).

Components Used

Les informations de ce document sont basées sur un ASA qui exécute la version 9.2, mais les versions antérieures peuvent également être utilisées.

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.

Informations générales

La QoS est une fonctionnalité réseau qui vous permet de donner la priorité à certains types de trafic Internet. À mesure que les utilisateurs d'Internet mettent à niveau leurs points d'accès des modems vers des connexions haut débit à haut débit telles que la ligne d'abonné numérique (DSL) et le câble, la probabilité augmente qu'à un moment donné, un seul utilisateur puisse absorber la plupart, sinon la totalité, de la bande passante disponible, privant ainsi les autres utilisateurs. Afin d'empêcher n'importe quel une utilisateur ou connexion de site à site de consommer plus que sa partie équitable de largeur de bande, QoS fournit une fonctionnalité de régulation qui règle la largeur de bande maximale que n'importe quel utilisateur peut utiliser.

QoS se rapporte à la capacité d'un réseau à fournir un meilleur service à un trafic de réseau sélectionné parmi diverses technologies pour les meilleurs services globaux avec une largeur de bande limitée des technologies sous-jacentes.

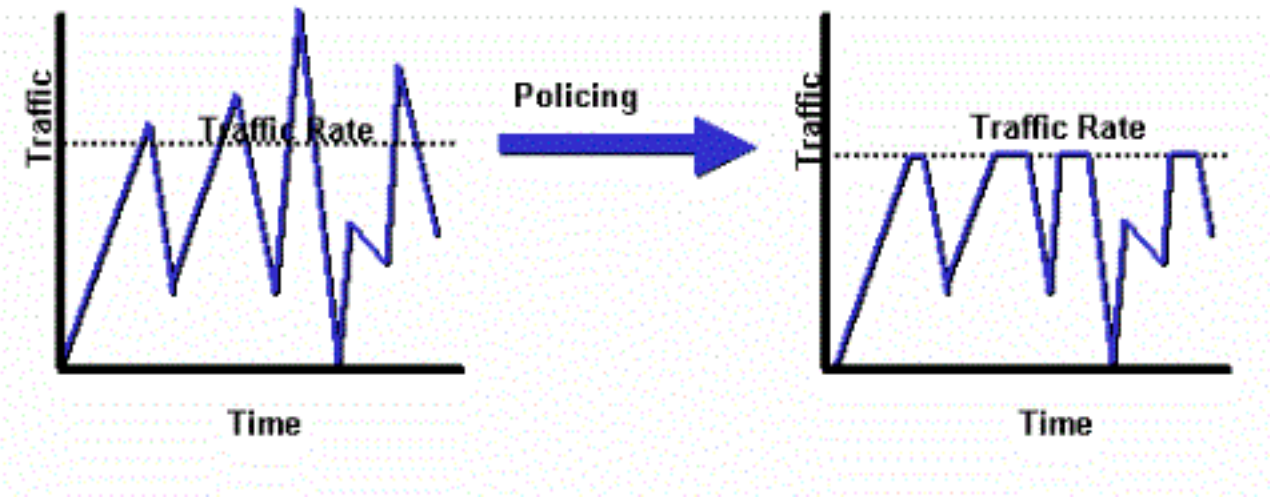
L'objectif principal de la QoS dans l'appliance de sécurité est de fournir la limitation de débit sur le trafic de réseau sélectionné, aussi bien pour le flux individuel que pour le flux du tunnel VPN, afin de s'assurer que l'ensemble du trafic dispose d'une partie équitable de largeur de bande limitée. Un flux peut être défini de plusieurs façons. Dans l'appliance de sécurité, QoS peut s'appliquer à une combinaison des adresses IP source et de destination, des numéros de port de destination et l'octet de Type de service (ToS) de l'en-tête IP.

Il existe trois types de QoS que vous pouvez mettre en oeuvre sur l'ASA : Réglementation, mise en forme et mise en file d'attente par priorité.

Contrôle du trafic

Avec la réglementation, le trafic dépassant une limite spécifiée est abandonné. La réglementation est un moyen de s'assurer qu'aucun trafic ne dépasse le débit maximal (en bits/seconde) que vous configurez, ce qui garantit qu'aucun flux de trafic ou classe ne peut prendre en charge la totalité de la ressource. Lorsque le trafic dépasse le débit maximal, l'ASA abandonne le trafic excédentaire. La réglementation définit également la plus grande rafale de trafic autorisée.

Ce diagramme illustre ce que fait la réglementation du trafic ; lorsque le débit du trafic atteint le débit maximal configuré, le trafic excédentaire est abandonné. Le résultat est un débit en sortie qui apparaît en dents de scie avec des hauts et des bas.



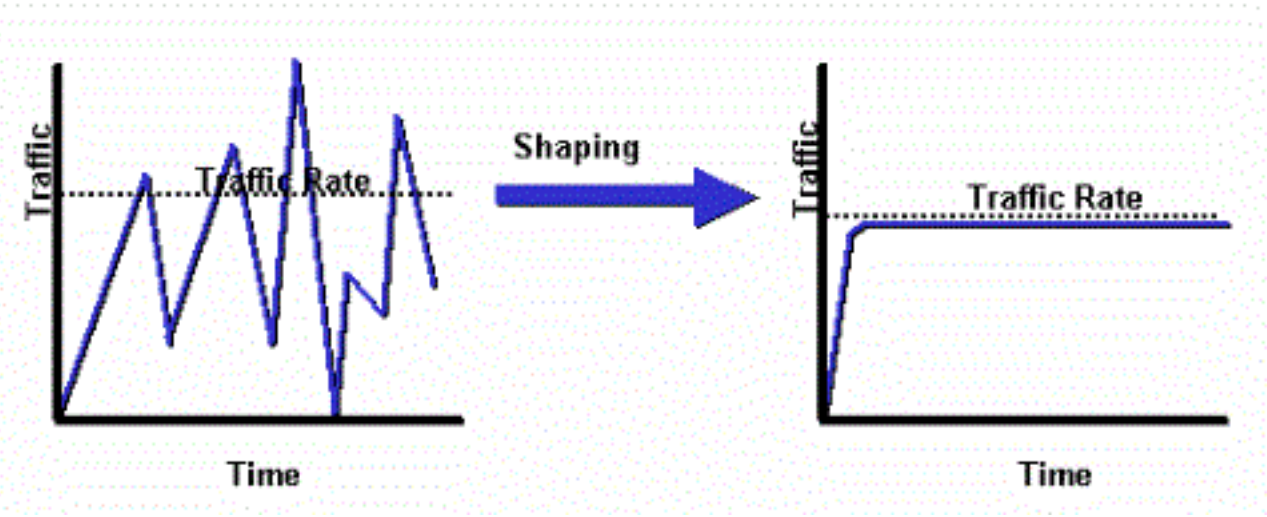
Cet exemple montre comment réduire la bande passante à 1 Mbits/s pour un utilisateur spécifique dans la direction sortante :

```
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
```

Modélisation du trafic

Le formatage du trafic est utilisé afin de correspondre aux vitesses de périphérique et de liaison, qui contrôle la perte de paquets, le délai variable et la saturation de liaison, qui peuvent provoquer gigue et retard. Le formatage du trafic sur l'appliance de sécurité permet au périphérique de limiter le flux du trafic. Ce mécanisme met le trafic en mémoire tampon au-dessus de la « limite de vitesse » et tente d'envoyer le trafic plus tard. La mise en forme ne peut pas être configurée pour certains types de trafic. Le trafic en forme comprend le trafic passant par le périphérique, ainsi que le trafic provenant du périphérique.

Ce schéma illustre ce que fait le formatage du trafic. il conserve les paquets excédentaires dans une file d'attente, puis planifie l'excédent pour une transmission ultérieure par incréments de temps. Le résultat du formatage de trafic est un débit en sortie en douceur de paquets.



> **Note**: Le formatage du trafic est uniquement pris en charge sur les versions ASA 5505, 5510, 5520, 5540 et 5550. Les modèles multicoeurs (tels que le modèle 5500-X) ne prennent pas en charge le formatage.

Avec le formatage du trafic, le trafic qui dépasse une certaine limite est mis en file d'attente (mis en mémoire tampon) et envoyé au cours de la prochaine période.

Le formatage du trafic sur le pare-feu est particulièrement utile si un périphérique en amont impose un goulot d'étranglement au trafic réseau. Par exemple, un ASA doté d'interfaces 100 Mbit, avec une connexion en amont à Internet via un modem câble ou un modem T1 qui se termine sur un routeur, est un bon exemple. Le formatage du trafic permet à l'utilisateur de configurer le débit sortant maximal sur une interface (l'interface externe par exemple); le pare-feu transmet le trafic de cette interface jusqu'à la bande passante spécifiée, puis tente de mettre en mémoire tampon le trafic excessif pour transmission ultérieurement lorsque la liaison est moins saturée.

Le formatage est appliqué à tout le trafic agrégé qui sort de l'interface spécifiée ; vous ne pouvez pas choisir de seulement modeler certains flux de trafic.

> **Note**: Le formatage est effectué après le chiffrement et ne permet pas la hiérarchisation des paquets internes ou des groupes de tunnels pour le VPN.

Cet exemple configure le pare-feu afin de modeler tout le trafic sortant sur l'interface externe à 2 Mbits/s :

```
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
```

Mise en file d'attente par priorité

Avec la mise en file d'attente par priorité, vous pouvez placer une classe de trafic spécifique dans la file d'attente à faible latence (LLQ), qui est traitée avant la file d'attente standard.

> **Note**: Si vous hiérarchisez le trafic dans le cadre d'une stratégie de formatage, vous ne pouvez pas utiliser les détails des paquets internes. Le pare-feu ne peut exécuter que LLQ, contrairement aux routeurs qui peuvent fournir des mécanismes de mise en file d'attente et de qualité de service plus sophistiqués (WFQ (Weighted Fair Queueing), CBWFQ (Class-Based Weighted Fair Queueing), etc.).

La stratégie QoS hiérarchique fournit un mécanisme permettant aux utilisateurs de spécifier la stratégie QoS de manière hiérarchique. Par exemple, si les utilisateurs veulent modeler le trafic sur une interface et, en outre, dans le trafic de l'interface en forme, fournir une file d'attente prioritaire pour le trafic VoIP, les utilisateurs peuvent spécifier une stratégie de formatage du trafic en haut et une stratégie de mise en file d'attente prioritaire sous la stratégie de forme. La prise en charge de la stratégie QoS hiérarchique est limitée. La seule option autorisée est :

- Formatage du trafic au niveau supérieur
- Mise en file d'attente prioritaire au niveau suivant

> **Note**: Si vous hiérarchisez le trafic dans le cadre d'une stratégie de formatage, vous ne pouvez pas utiliser les détails des paquets internes. Le pare-feu peut uniquement exécuter LLQ, contrairement aux routeurs qui peuvent fournir des mécanismes de mise en file d'attente et de qualité de service plus sophistiqués (WFQ, CBWFQ, etc.).

Cet exemple utilise la stratégie QoS hiérarchique afin de modeler tout le trafic sortant sur l'interface externe à 2 Mbits/s comme l'exemple de formatage, mais il spécifie également que les paquets voix avec la valeur ef du point de code de services différenciés (DSCP), ainsi que le trafic SSH (Secure Shell), doivent recevoir la priorité.

Créez la file d'attente prioritaire sur l'interface sur laquelle vous voulez activer la fonctionnalité :

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

Une classe qui correspond à DSCP ef :

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

Une classe correspondant au trafic TCP/22 SSH du port :

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

Carte de stratégie pour appliquer la hiérarchisation du trafic voix et 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
```

Une carte de stratégie pour appliquer le formatage à tout le trafic et associer le trafic voix et SSH prioritaire :

```
   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
```

Enfin, associez la stratégie de mise en forme à l'interface sur laquelle le trafic sortant doit être formaté et hiérarchisé :

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

QoS pour le trafic via un tunnel VPN

QoS avec VPN IPsec

Conformément à la RFC 2401, les bits de type de service (ToS) de l'en-tête IP d'origine sont copiés dans l'en-tête IP du paquet chiffré afin que les stratégies QoS puissent être appliquées après le chiffrement. Cela permet aux bits DSCP/DiffServ d'être utilisés en priorité n'importe où dans la stratégie QoS.

Contrôle sur un tunnel IPsec

La réglementation peut également être effectuée pour des tunnels VPN spécifiques. Afin de sélectionner un groupe de tunnels sur lequel contrôler, vous utilisez la commande **match tunnel-group <tunnel>** dans votre class-map et la commande **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 réglementation d'entrée ne fonctionne pas pour le moment lorsque vous utilisez la commande **match tunnel-group** ; voir l'ID de bogue Cisco CSCth48255 pour plus d'informations. Si vous essayez d'effectuer la réglementation d'entrée avec la correspondance flow ip destination-address, vous recevez cette erreur :

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

La réglementation des entrées ne semble pas fonctionner pour le moment lorsque vous utilisez **match tunnel-group** (ID de bogue Cisco CSCth48255). Si le contrôle d'entrée fonctionne, vous devez utiliser une carte de classe sans l'**adresse de destination de correspondance ip flow**.

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

Si vous essayez de contrôler la sortie sur une carte-classe qui ne possède pas l'**adresse ip de destination correspondance**, vous recevez :

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

Il est également possible d'effectuer une QoS sur les informations de flux interne à l'aide de listes de contrôle d'accès (ACL), DSCP, etc. En raison du bogue mentionné précédemment, les listes de contrôle d'accès sont le moyen d'effectuer la surveillance des entrées dès maintenant.

> **Note**: Un maximum de 64 cartes-politiques peut être configuré sur tous les types de plate-forme. Utilisez différentes cartes-classes dans les cartes-politiques afin de segmenter le trafic.

QoS avec VPN SSL (Secure Sockets Layer)

Jusqu'à la version 9.2 d'ASA, l'ASA ne conservait pas les bits ToS.

La tunnellisation VPN SSL n'est pas prise en charge avec cette fonctionnalité. Pour plus d'informations, reportez-vous à l'ID de bogue Cisco CSCsl73211.

```
   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**: Lorsque les utilisateurs équipés de téléphone-vpn utilisent le client AnyConnect et le DTLS (Datagram Transport Layer Security) pour chiffrer leur téléphone, la hiérarchisation ne fonctionne pas car AnyConnect ne conserve pas l'indicateur DSCP dans l'encapsulation DTLS. Référez-vous à la demande d'amélioration CSCtq43909 pour plus de détails.

Considérations relatives à la qualité de service

Voici quelques points à prendre en compte à propos de la qualité de service.

- Elle est appliquée par le biais du cadre de politique modulaire (MPF) de manière stricte ou hiérarchique : Contrôle, formatage, LLQ.

  Ne peut influencer que le trafic déjà transmis de la carte d'interface réseau (NIC) au DP (Data Path)Inutile de lutter contre les dépassements (ils surviennent trop tôt), sauf s'ils sont appliqués sur un périphérique adjacent

- La réglementation est appliquée sur l'entrée après que le paquet est autorisé et sur la sortie avant la carte réseau.

  Juste après avoir réécrit une adresse de couche 2 (L2) sur la sortie

- Il forme la bande passante sortante pour tout le trafic sur une interface.

  Utile avec une bande passante de liaison ascendante limitée (liaison 1 Gigabit Ethernet (GE) vers modem 10 Mo)Non pris en charge sur les modèles ASA558x hautes performances

- La mise en file d'attente par priorité risque de priver le trafic au mieux.

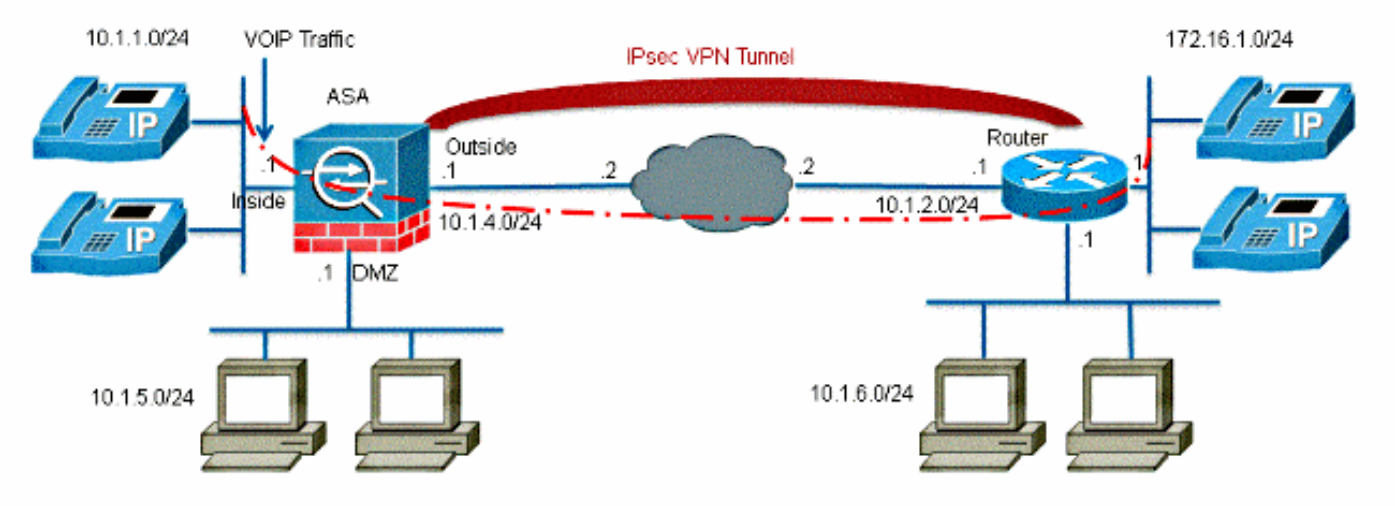
  Non pris en charge sur les interfaces 10GE sur les sous-interfaces ASA5580 ou VLANLa taille de la sonnerie de l'interface peut être ajustée pour des performances optimales

Exemples de configuration

Exemple de configuration de QoS pour le trafic VoIP sur les tunnels VPN

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Note: Vérifiez que les téléphones IP et les hôtes sont placés dans des segments différents (sous-réseaux). Ceci est recommandé pour une bonne conception du réseau.

Ce document utilise les configurations suivantes :

- Configuration QoS basée sur DSCP
- Configuration QoS basée sur DSCP avec VPN
- Configuration QoS basée sur ACL
- Configuration QoS basée sur ACL avec VPN

Configuration QoS basée sur 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: La valeur DSCP de « ef » fait référence au transfert accéléré qui correspond au trafic VoIP-RTP.

Configuration QoS basée sur DSCP avec 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
```

Configuration QoS basée sur 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
```

Configuration QoS basée sur ACL avec 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**: Utilisez l'outil de recherche de commandes (clients enregistrés uniquement) afin d'obtenir plus d'informations sur les commandes utilisées dans cette section.

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

show service-policy police

Afin d'afficher les statistiques QoS pour la réglementation du trafic, utilisez la commande **show service-policy** avec le mot clé **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

Afin d'afficher des statistiques pour les stratégies de service qui implémentent la commande **priority**, utilisez la commande **show service-policy** avec le mot clé **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

Afin d'afficher les statistiques de file d'attente prioritaire pour une interface, utilisez la commande show priority-queue statistics en mode EXEC privilégié. Les résultats montrent les statistiques de la file d'attente Best Effort (BE) et de la file d'attente LLQ. Cet exemple montre l'utilisation de la commande **show priority-queue statistics** pour l'interface nommée outside, ainsi que le résultat de la commande.

```
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#
```

Dans ce rapport statistique, la signification des éléments de ligne est la suivante :

- «Paquets abandonnés » indique le nombre total de paquets qui ont été abandonnés dans cette file d'attente.
- «Transmission de paquets » indique le nombre total de paquets qui ont été transmis dans cette file d'attente.
- «Paquets mis en file d'attente » indique le nombre total de paquets qui ont été mis en file d'attente dans cette file d'attente.
- «Longueur de file d'attente actuelle » indique la profondeur actuelle de cette file d'attente.
- «Longueur de file d'attente maximale » indique la profondeur maximale jamais atteinte dans cette file d'attente.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Additional Information

Voici quelques bogues introduits par la fonctionnalité de formatage du trafic :

ID de bogue Cisco CSCsq08550	Le formatage du trafic avec la file d'attente prioritaire entraîne une défaillance trafic sur ASA
ID de bogue Cisco CSCsx07862	La mise en forme du trafic avec la file d'attente prioritaire entraîne un retard e pertes de paquets
ID de bogue Cisco CSCsq07395	L'ajout de la stratégie de service de mise en forme échoue si la carte de strat a été modifiée

Forum aux questions

Cette section fournit une réponse à l'une des questions les plus fréquemment posées au sujet de l'information décrite dans ce document.

Les marquages QoS sont-ils préservés lorsque le tunnel VPN est traversé ?

Oui. Les marquages QoS sont conservés dans le tunnel lorsqu'ils traversent les réseaux du fournisseur si le fournisseur ne les supprime pas en transit.

Astuce : Reportez-vous à la section Préservation DSCP et DiffServ du *CII Book 2 : Guide de configuration de l'interface de ligne de commande du pare-feu de la gamme Cisco ASA, version 9.2* pour plus d'informations.

Informations connexes

- Guide de configuration CLI du pare-feu de la gamme Cisco ASA, Qualité de service
- Application des politiques QoS
- Présentation des fonctionnalités non prises en charge dans le VPN SSL sans client
- Configuration QoS
- Support et documentation techniques - Cisco Systems