QoS sur les exemples de configuration de Cisco ASA

Contenu

Introduction

Ce document explique comment le Qualité de service (QoS) travaille à l'appliance de sécurité adaptable Cisco (ASA) et fournit également plusieurs exemples sur la façon dont l'implémenter pour différents scénarios.

Vous pouvez configurer QoS sur les dispositifs de sécurité afin de fournir la limitation de débit sur le trafic de réseau sélectionné, parce que des écoulements de personne et des écoulements de tunnel VPN, afin de s'assurer que tout le trafic obtient sa partie équitable de bande passante limitée.

La caractéristique a été intégrée avec l'ID de bogue Cisco CSCsk06260.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de la stratégie modulaire Framwork (MPF).

Composants utilisés

Les informations dans ce document sont basées sur une ASA qui exécute la version 9.2, mais des versions antérieures peuvent être aussi bien utilisées.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

QoS est une caractéristique de réseau qui te permet pour accorder la priorité à certains types de trafic Internet. Pendant que les internautes améliorent leurs Points d'accès des Modems aux connexions haut débit ultra-rapides comme la ligne d'abonné numérique (DSL) et le câble, les augmentations de probabilité qu'à un moment donné, un seul utilisateur pourrait pouvoir absorber les la plupart, sinon toute la, bande passante disponible, de ce fait privant les autres utilisateurs de nourriture. 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 y a trois genres de QoS que vous pouvez implémenter sur l'ASA : Maintenant l'ordre, formant, et s'alignant prioritaire.

Réglementation du trafic

Avec le maintien de l'ordre, le trafic au-dessus d'une limite spécifiée est abandonné. Le maintien de l'ordre est une manière de s'assurer qu'aucun trafic ne dépasse le débit maximum (dans le bits/seconde) ce vous configurent, qui s'assure que l'aucune circulation ou classe ne peut assurer la ressource entière. Quand le trafic dépasse le débit maximum, l'ASA relâche le trafic excédentaire. Le maintien de l'ordre également place la plus grande rafale de trafic simple permise.

Ce diagramme montre quelle Réglementation du trafic fait ; quand le débit de trafic atteint le débit maximum 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 affiche comment étrangler la bande passante au Mbits/s 1 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
```

Formation du trafic

La formation du trafic est utilisée afin d'apparier le périphérique et les vitesses de liaison, qui contrôle la perte de paquets, le retard variable, et la saturation de lien, qui peut entraîner le jitter et retarder. Le trafic formant sur les dispositifs de sécurité permet au périphérique pour limiter l'écoulement du trafic. Ce mécanisme met en mémoire tampon le trafic au-dessus de la « vitesse limite » et des tentatives d'envoyer le trafic plus tard. La formation ne peut pas être configurée pour certains types de trafic. Le trafic formé inclut le trafic traversant le périphérique, aussi bien que le trafic qui est originaire du périphérique.

Ce diagramme montre quel trafic la formation fait ; il retient des paquets excédentaires dans une file d'attente et puis programme l'en excès pour la transmission postérieure au-dessus des incréments de temps. Le résultat du formatage de trafic est un débit en sortie en douceur de paquets.

> Remarque: La formation du trafic est seulement prise en charge sur des versions 5505, 5510, 5520, 5540, et 5550 ASA. Les modèles multicores (tels que le 5500-X) ne prennent en charge pas la formation.

Avec le trafic formant, le trafic qui dépasse une certaine limite est aligné (mis en mémoire tampon) et envoyé pendant le prochain timeslice.

Le trafic formant sur le Pare-feu est le plus utile si un périphérique en amont impose un bottlneck au trafic réseau. Un bon exemple serait une ASA qui a 100 interfaces de Mb, avec une connexion à Internet en amont par l'intermédiaire d'un modem câble ou de t1 qui se termine sur un routeur. La formation du trafic permet à l'utilisateur pour configurer le débit sortant maximum sur une interface (l'interface extérieure par exemple) ; le Pare-feu transmet le trafic hors de cette interface jusqu'à la bande passante spécifiée, et puis le tente de mettre en mémoire tampon le trafic excessif pour la transmission plus tard quand le lien moins est saturé.

La formation est appliquée à tout l'ensemble du trafic ce des de sortie l'interface spécifiée ; vous ne pouvez pas choisir de former seulement certaine circulation.

> Remarque: La formation est faite après cryptage et ne tient pas compte de la hiérarchisation sur la base de paquet interne ou de groupe de tunnels pour le VPN.

Cet exemple configure le Pare-feu afin de former tout le trafic sortant sur l'interface extérieure 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 file d'attente à priorité déterminée, vous pouvez placer une classe du trafic spécifique dans la file d'attente à faible latence (LLQ), qui est traitée avant la file d'attente standard.

> Remarque: Si vous donnez la priorité au trafic dans le cadre d'une stratégie de mise en forme, vous ne pouvez pas utiliser des détails de paquet interne. Le Pare-feu peut seulement exécuter LLQ, à la différence des Routeurs qui peuvent fournir une Mise en file d'attente et des mécanismes plus sophistiqués de QoS (mise en file d'attente pondérée (WFQ), Mise en file d'attente pondérée basée sur les classes (CBWFQ), et ainsi de suite).

La stratégie QoS hiérarchique fournit un mécanisme pour que les utilisateurs spécifient la stratégie QoS d'une mode hiérarchique. Par exemple, si les utilisateurs veulent former le trafic sur une interface et en outre dans le trafic formé d'interface, fournissez la file d'attente à priorité déterminée pour le trafic VoIP, puis les utilisateurs peut spécifier une stratégie de mise en forme du trafic au dessus et une stratégie de file d'attente à priorité déterminée dans le cadre de la stratégie de forme. Le support hiérarchique de stratégie QoS est limité dans la portée. La seule option permise est :

- Le trafic formant au niveau supérieur
- Priorité s'alignant au prochain niveau

> Remarque: Si vous donnez la priorité au trafic dans le cadre d'une stratégie de mise en forme, vous ne pouvez pas utiliser des détails de paquet interne. Le Pare-feu peut seulement exécuter LLQ, à la différence des Routeurs qui peuvent fournir une Mise en file d'attente et des mécanismes plus sophistiqués de QoS (WFQ, CBWFQ, et ainsi de suite).

Cet exemple emploie la stratégie QoS hiérarchique afin de former tout le trafic sortant sur l'interface extérieure à 2 Mbits/s comme l'exemple de formation mais il spécifie également que les paquets vocaux avec le Differentiated Services Code Point (DSCP) évaluent « E-F », aussi bien que le trafic de Protocole Secure Shell (SSH), recevra la priorité.

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

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

Une classe au match dscp E-F :

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

Une classe au trafic de SSH du match port TCP/22 :

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

Une carte de stratégie pour appliquer la hiérarchisation de la Voix et le SSH trafiquent :

```
   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 s'appliquer la formation à tout le trafic et pour relier le trafic prioritaire de Voix et 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
```

Reliez enfin la stratégie de mise en forme à l'interface sur laquelle pour former et donner la priorité au trafic sortant :

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

QoS pour le trafic par un tunnel VPN

QoS avec IPsec VPN

Selon le Type de service (ToS) RFC 2401 des bits dans l'en-tête IP d'origine sont copiés sur l'en-tête IP du paquet chiffré de sorte que des stratégies QoS puissent être imposées après cryptage. Ceci permet les bits DSCP/DiffServ à utiliser pour la priorité n'importe où dans la stratégie QoS.

Maintien de l'ordre sur un tunnel d'IPsec

Le maintien de l'ordre peut également être fait pour les tunnels VPN spécifiques. Afin de sélectionner un groupe de tunnels sur lequel pour maintenir l'ordre, vous utilisez la commande de **<tunnel> de groupe de tunnels de correspondance** dans votre class-map et la commande d'**adresse de destination de match flow ip**.

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

Le maintien de l'ordre d'entrée ne fonctionne pas à ce moment où vous utilisez l'ordre de **groupe de tunnels de correspondance** ; voir le pour en savoir plus de l'ID de bogue Cisco CSCth48255. Si vous essayez de faire l'entrée maintenant l'ordre avec l'adresse de destination de match flow ip, vous recevez cette erreur :

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

Le maintien de l'ordre d'entrée ne semble pas fonctionner à ce moment où vous utilisez le **groupe de tunnels de correspondance** (ID de bogue Cisco CSCth48255). Si le maintien de l'ordre d'entrée fonctionne, vous devriez utiliser un class-map sans **adresse d'adresse de destination de match flow ip**.

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

Si vous essayez de maintenir l'ordre la sortie sur un class-map qui n'a pas l'**adresse de destination d'IP de correspondance**, vous recevez :

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

Il est également possible d'exécuter QoS sur les informations intérieures d'écoulement avec l'utilisation du Listes de contrôle d'accès (ACL), DSCP, et ainsi de suite. En raison de la bogue précédemment mentionnée, ACLs sont la manière de pouvoir faire l'entrée maintenant l'ordre en ce moment.

> Remarque: Un maximum de 64 policy-map peut être configuré sur tous les types de plate-forme. Employez les différents class-map dans les policy-map afin de segmenter le trafic.

QoS avec Secure Sockets Layer (SSL) VPN

Jusqu'à la version 9.2 ASA, l'ASA n'a pas préservé les bits de tos.

Le Tunnellisation de VPN SSL n'est pas pris en charge avec cette fonctionnalité. Voir le pour en savoir plus de 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)#
```

> Remarque: Quand les utilisateurs avec téléphone-VPN emploient le Transport Layer Security de client et de datagramme d'AnyConnect (DTLS) pour chiffrer leur téléphone, le classement par ordre de priorité ne fonctionne pas parce qu'AnyConnect ne préserve pas l'indicateur de DSCP dans l'encapsulation DTLS. Référez-vous à la demande d'amélioration CSCtq43909 pour des détails.

Considérations de QoS

Voici quelques points à considérer au sujet de QoS.

- Il est appliqué par le cadre de stratégie modulaire (MPF) de mode stricte ou hiérarchique : Maintien de l'ordre, formant, LLQ.

  Peut seulement influencer le trafic qui est déjà passé du network interface card (NIC) au DP (le chemin de données)Inutile de combattre des dépassements de capacité (ils se produisent trop tôt) à moins qu'appliqué sur un périphérique contigu

- Le maintien de l'ordre est appliqué sur l'entrée après qu'on permette le paquet et sur la sortie avant le NIC.

  Juste après que vous réécrivez une adresse de la couche 2 (L2) sur la sortie

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

  Utile avec la bande passante limitée de liaison ascendante (de tels Ethernets as1Gigabit (GE) lient au modem 10Mb)Non pris en charge sur les modèles performants ASA558x

- La file d'attente à priorité déterminée pourrait mourir de faim le trafic de meilleur effort.

  Non pris en charge sur 10GE relie sur des sous-interfaces ASA5580 ou VLANLa taille de sonnerie d'interface peut être encore accordée 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 :

> Remarque: 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 l'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
```

Remarque: La valeur DSCP de « E-F » se rapporte à l'expédition expédié qui apparie le trafic de 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 l'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
```

> Remarque: Utilisez le Command Lookup Tool (clients enregistrés seulement) afin d'obtenir plus d'informations que les commandes les ont utilisées dans cette section.

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

police de show service-policy

Afin de visualiser le qos statistics pour la Réglementation du trafic, utilisez la commande de **show service-policy** avec le mot clé de **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
```

priorité de show service-policy

Afin de visualiser des statistiques pour les stratégies de service qui implémentent la commande **prioritaire**, utilisez la commande de **show service-policy** avec le mot clé **prioritaire** :

```
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
```

forme de show service-policy

```
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
```

affichez les statistiques de priority-queue

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 affichent aux statistiques pour chacun des deux la file d'attente de meilleur effort (SOYEZ) et le LLQ. Cet exemple affiche l'utilisation de la commande de **statistiques de priority-queue d'exposition** pour l'interface nommée dehors, et la sortie de 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 cet état statistique, la signification des éléments de ligne est comme suit :

- Les « paquets lâchés » dénote le nombre total de paquets qui ont été lâchés dans cette file d'attente.
- Les « paquets transmettent » dénote le nombre total de paquets qui ont été transmis dans cette file d'attente.
- Les « paquets mis en file d'attente » dénote le nombre total de paquets qui ont été alignés dans cette file d'attente.
- « La longueur en cours Q » dénote la profondeur en cours de cette file d'attente.
- « La longueur maximum Q » dénote la profondeur maximum qui s'est jamais produite dans cette file d'attente.

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Dépannez

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

Informations supplémentaires

Voici quelques bogues introduites par le trafic formant la caractéristique :

ID de bogue Cisco CSCsq08550	Le trafic formant avec des causes de queue prioritaire trafiquent la panne l'ASA
ID de bogue Cisco CSCsx07862	Le trafic formant avec le retard et les baisses de queue de paquet de caus prioritaire
ID de bogue Cisco CSCsq07395	Ajouter formant la service-stratégie échoue si le policy-map a été édité

FORUM AUX QUESTIONS

Cette section apporte une réponse à une des questions fréquemment posées en vue de les informations qui sont décrites dans ce document.

Est-ce que marquages de QoS sont préservés quand le tunnel VPN est traversé ?

Oui. Les marquages de QoS sont préservés dans le tunnel pendant qu'ils traversent les réseaux du fournisseur si le fournisseur ne les élimine pas en transit.

> **Conseil** : Référez-vous au DSCP et à la section de conservation de DiffServ de l'*ouvrage 2 CLI : Guide de configuration CLI de Pare-feu de gamme de Cisco ASA, 9.2* pour plus de détails.

Informations connexes

- Guide de configuration CLI de Pare-feu de gamme de Cisco ASA, qualité de service
- Application des stratégies QoS
- Compréhension des caractéristiques non prises en charge dans le VPN SSL sans client
- Configuration QoS
- Support et documentation techniques - Cisco Systems