QoS in den Cisco ASA-Konfigurationsbeispielen

Inhalt

Einführung

In diesem Dokument wird die Funktionsweise von Quality of Service (QoS) auf der Cisco Adaptive Security Appliance (ASA) erläutert. Darüber hinaus enthält es einige Beispiele für die Implementierung in verschiedenen Szenarien.

Sie können QoS auf der Sicherheits-Appliance konfigurieren, um eine Ratenbegrenzung für

ausgewählten Netzwerkverkehr sowohl für einzelne Datenflüsse als auch für VPN-Tunnelflüsse bereitzustellen, um sicherzustellen, dass der gesamte Datenverkehr seinen angemessenen Anteil an begrenzter Bandbreite erhält.

Die Funktion wurde in die Cisco Bug-ID CSCsk06260 integriert.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse des modularen Richtlinien-Frameworks (MPF) zu verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einer ASA, die Version 9.2 ausführt, frühere Versionen können jedoch ebenfalls verwendet werden.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

QoS ist eine Netzwerkfunktion, mit der Sie bestimmten Arten von Internetdatenverkehr Priorität einräumen können. Wenn Internetnutzer ihre Access Points von Modems auf Hochgeschwindigkeits-Breitbandverbindungen wie DSL (Digital Subscriber Line) und Kabel aufrüsten, steigt die Wahrscheinlichkeit, dass ein einzelner Benutzer zu einem beliebigen Zeitpunkt den Großteil, wenn nicht sogar alle, der verfügbaren Bandbreite beanspruchen kann, wodurch die anderen Benutzer benachteiligt werden. Um zu verhindern, dass ein Benutzer oder eine standortübergreifende Verbindung mehr als den angemessenen Anteil an Bandbreite beansprucht, bietet QoS eine Richtlinienfunktion, die die maximale Bandbreite regelt, die ein Benutzer verwenden kann.

QoS bezieht sich auf die Fähigkeit eines Netzwerks, ausgewählten Netzwerkverkehr mithilfe verschiedener Technologien einen besseren Service bereitzustellen, um die besten allgemeinen Dienste mit begrenzter Bandbreite der zugrunde liegenden Technologien bereitzustellen.

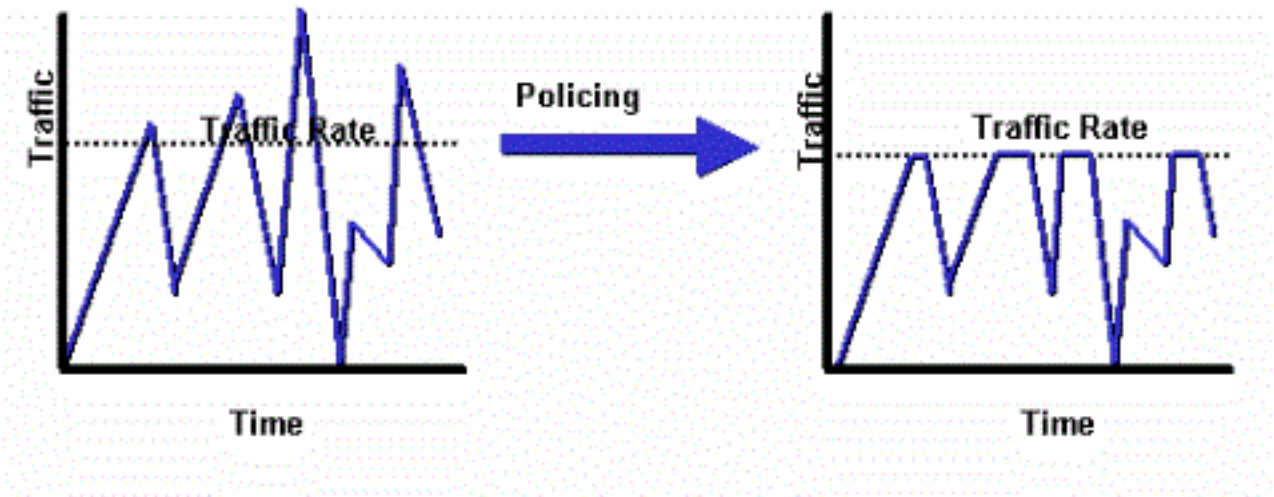
Das Hauptziel von QoS in der Security Appliance ist die Bereitstellung einer Ratenbegrenzung für ausgewählten Netzwerkverkehr, sowohl für den einzelnen Fluss als auch für den VPN-Tunnelfluss, um sicherzustellen, dass der gesamte Datenverkehr einen angemessenen Anteil an begrenzter Bandbreite erhält. Ein Fluss kann auf verschiedene Weise definiert werden. In der Sicherheits-Appliance kann QoS auf eine Kombination aus Quell- und Ziel-IP-Adressen, Quell- und Ziel-Portnummer und dem ToS-Byte (Type of Service) des IP-Headers angewendet werden.

Es gibt drei Arten von QoS, die Sie auf der ASA implementieren können: Policing, Shaping und Priority Queueing.

Traffic Policing

Bei der Richtlinienvergabe wird Datenverkehr über einen festgelegten Grenzwert verworfen. Mit der Richtlinienvergabe wird sichergestellt, dass kein Datenverkehr die maximale Rate (in Bit/Sekunde) überschreitet, die Sie konfigurieren. Dadurch wird sichergestellt, dass kein Datenverkehrsfluss oder eine Klasse die gesamte Ressource übernehmen kann. Wenn der Datenverkehr die maximale Rate überschreitet, verwirft die ASA den überschüssigen Datenverkehr. Zudem wird durch Richtlinienvergabe die größte zulässige einzelne Datenverkehrsflut festgelegt.

In diesem Diagramm wird veranschaulicht, wie Datenverkehrsrichtlinien funktionieren. Wenn die Datenverkehrsrate die konfigurierte Höchstgeschwindigkeit erreicht, wird überschüssiger Datenverkehr verworfen. Das Ergebnis ist eine Ausgangsrate, die als Sägezahnspur mit Scheiteln und Tiefen erscheint.



In diesem Beispiel wird gezeigt, wie die Bandbreite für einen bestimmten Benutzer in ausgehender Richtung auf 1 Mbit/s gedrosselt wird:

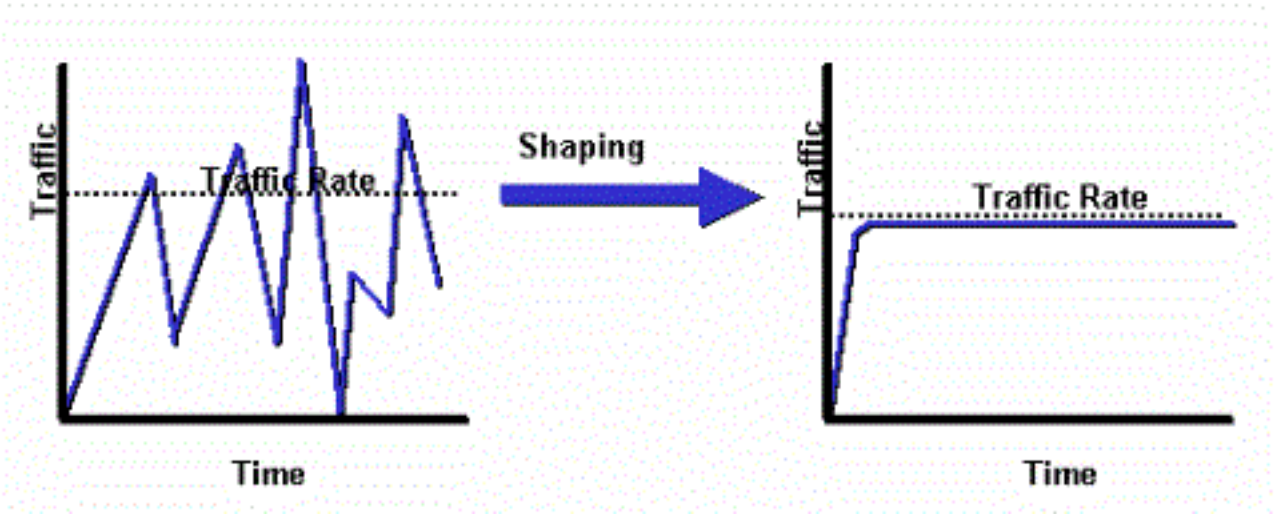
```
ciscoasa(config)# access-list WEB-LIMIT permit ip host 192.168.10.1 any
ciscoasa(config)# class-map Class-Policy
ciscoasa(config-cmap)# match access-list WEB-LIMIT
ciscoasa(config-cmap)#exit

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
```

Traffic Shaping

Das Traffic Shaping wird verwendet, um Geräte- und Verbindungsgeschwindigkeiten abzugleichen, wodurch Paketverluste, variable Verzögerungen und Link-Sättigung gesteuert werden, was Jitter und Verzögerungen verursachen kann. Durch Traffic Shaping auf der Security Appliance kann das Gerät den Datenverkehrsfluss einschränken. Dieser Mechanismus puffert den

Datenverkehr über die "Geschwindigkeitsbegrenzung" und versucht, den Datenverkehr zu einem späteren Zeitpunkt zu senden. Das Shaping kann für bestimmte Arten von Datenverkehr nicht konfiguriert werden. Der geformte Datenverkehr umfasst Datenverkehr, der durch das Gerät geleitet wird, sowie Datenverkehr, der vom Gerät stammt.

Dieses Diagramm veranschaulicht die Funktion von Traffic Shaping. Es behält überzählige Pakete in einer Warteschlange und plant die Überschreitung für eine spätere Übertragung über Zeitabschnitte. Das Ergebnis des Traffic Shaping ist eine optimierte Paketausgaberate.



> **Hinweis:** Traffic Shaping wird nur auf den ASA-Versionen 5505, 5510, 5520, 5540 und 5550 unterstützt. Multicore-Modelle (wie der 5500-X) unterstützen kein Shaping.

Beim Traffic Shaping wird Datenverkehr, der einen bestimmten Grenzwert überschreitet, in die Warteschlange gestellt (gepuffert) und während der nächsten Zeitüberschreitung gesendet.

Traffic Shaping auf der Firewall ist besonders dann nützlich, wenn ein Upstream-Gerät dem Netzwerkverkehr einen Engpass aufbürdet. Ein gutes Beispiel wäre eine ASA mit 100-Mbit-Schnittstellen, die über ein Kabelmodem oder T1, das an einem Router angeschlossen ist, eine Upstream-Verbindung zum Internet hat. Traffic Shaping ermöglicht es dem Benutzer, den maximalen ausgehenden Durchsatz auf einer Schnittstelle (z. B. der externen Schnittstelle) zu konfigurieren. Die Firewall überträgt den Datenverkehr von dieser Schnittstelle bis zur angegebenen Bandbreite und versucht dann, den übermäßig hohen Datenverkehr für die Übertragung zu einem späteren Zeitpunkt zu puffern, wenn die Verbindung weniger ausgelastet ist.

Shaping wird auf den gesamten aggregierten Datenverkehr angewendet, der die angegebene Schnittstelle ausführt. Sie können nicht auswählen, nur bestimmte Datenverkehrsflüsse zu gestalten.

> **Hinweis:** Das Shaping wird nach der Verschlüsselung durchgeführt und ermöglicht keine Priorisierung auf der Basis von internen Paketen oder Tunnelgruppen für VPN.

In diesem Beispiel wird die Firewall so konfiguriert, dass der gesamte ausgehende Datenverkehr an der externen Schnittstelle auf 2 Mbit/s umgestellt wird:

```
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
```

Prioritätswarteschlange

Bei Prioritätswarteschlangen können Sie eine bestimmte Verkehrsklasse in die Low Latency Queue (LLQ) einfügen, die vor der Standardwarteschlange verarbeitet wird.

> **Hinweis:** Wenn Sie den Datenverkehr unter einer Shaping-Richtlinie priorisieren, können Sie keine inneren Paketdetails verwenden. Die Firewall kann LLQ nur ausführen, im Gegensatz zu den Routern, die anspruchsvollere Warteschlangen- und QoS-Mechanismen (Weighted Fair Queueing (WFQ), Class-Based Weighted Fair Queueing (CBWFQ) usw.) bereitstellen.

Die hierarchische QoS-Richtlinie bietet einen Mechanismus, mit dem Benutzer die QoS-Richtlinie hierarchisch angeben können. Wenn Benutzer beispielsweise den Datenverkehr an einer Schnittstelle und darüber hinaus innerhalb des Shaping-Schnittstellendatenverkehrs gestalten möchten, eine Prioritätswarteschlange für den VoIP-Datenverkehr bereitstellen, können die Benutzer eine Traffic Shaping-Richtlinie oben und eine Prioritätswarteschlangenrichtlinie unter der Shaping-Richtlinie angeben. Die hierarchische QoS-Richtlinienunterstützung ist im Umfang begrenzt. Es ist nur folgende Option zulässig:

- Traffic Shaping auf oberster Ebene
- Prioritätswarteschlange auf der nächsten Ebene

> **Hinweis:** Wenn Sie den Datenverkehr unter einer Shaping-Richtlinie priorisieren, können Sie keine inneren Paketdetails verwenden. Die Firewall kann LLQ nur ausführen, im Gegensatz zu den Routern, die anspruchsvollere Warteschlangen- und QoS-Mechanismen (WFQ, CBWFQ usw.) bereitstellen können.

In diesem Beispiel wird die hierarchische QoS-Richtlinie verwendet, um den gesamten ausgehenden Datenverkehr an der externen Schnittstelle wie im Shaping-Beispiel auf 2 Mbit/s zu gestalten. Es wird jedoch auch festgelegt, dass Sprachpakete mit dem DSCP-Wert "ef" (Differentiated Services Code Point) sowie Secure Shell (SSH)-Datenverkehr Priorität erhalten sollen.

Erstellen Sie die Prioritätswarteschlange auf der Schnittstelle, auf der Sie die Funktion aktivieren möchten:

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

Eine Klasse, die DSCP ef entspricht:

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

Eine Klasse, die Port-TCP/22-SSH-Datenverkehr abgleicht:

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

Eine Richtlinienzuordnung zur Priorisierung von Sprach- und SSH-Datenverkehr:

```
   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
```

Eine Richtlinienzuordnung, die das Shaping auf den gesamten Datenverkehr anwendet und priorisierten Sprach- und SSH-Datenverkehr anfügt:

```
   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
```

Fügen Sie schließlich die Shaping-Richtlinie an die Schnittstelle an, auf der ausgehender Datenverkehr geformt und priorisiert werden soll:

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

QoS für Datenverkehr über einen VPN-Tunnel

QoS mit IPsec-VPN

Gemäß RFC 2401 werden Type of Service (ToS)-Bits im ursprünglichen IP-Header in den IP-Header des verschlüsselten Pakets kopiert, sodass QoS-Richtlinien nach der Verschlüsselung durchgesetzt werden können. Auf diese Weise können die DSCP/DiffServ-Bits für die Priorität an einer beliebigen Stelle in der QoS-Richtlinie verwendet werden.

Richtlinienvergabe an einen IPsec-Tunnel

Die Richtlinienvergabe kann auch für bestimmte VPN-Tunnel erfolgen. Um eine Tunnelgruppe auszuwählen, für die Richtlinien festgelegt werden sollen, verwenden Sie den Befehl **match tunnel-group <tunnel>** in Ihrer Klassenzuordnung und den Befehl **match flow ip destination address (Zieladresse für Übereinstimmung).**

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

Die Eingaberichtlinie funktioniert derzeit nicht, wenn Sie den Befehl **match tunnel-group** verwenden. Weitere Informationen finden Sie unter Cisco Bug ID CSCth48255. Wenn Sie versuchen, eine Eingaberichtlinie mit der Zieladresse für den Abgleichstrom zu erstellen, wird folgender Fehler angezeigt:

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

Die Eingabe-Policing scheint derzeit nicht zu funktionieren, wenn Sie **match-Tunnelgruppe** verwenden (Cisco Bug-ID CSCth48255). Wenn die Eingaberichtlinie funktioniert, müssen Sie eine Klassenzuordnung ohne die **Zieladresse für** den **Abgleichstrom-IP-Zieladresse** verwenden.

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

Wenn Sie versuchen, die Ausgabe auf einer Klassenzuordnung zu kontrollieren, die nicht über die **Zieladresse für Übereinstimmung** verfügt, erhalten Sie Folgendes:

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

Es ist auch möglich, QoS für Informationen zum inneren Datenfluss mithilfe von Zugriffskontrolllisten (ACLs), DSCP usw. auszuführen. Aufgrund des oben genannten Fehlers können Zugriffskontrolllisten (ACLs) derzeit die Eingangsüberwachung durchführen.

> **Hinweis:** Auf allen Plattformtypen können maximal 64 Richtlinienzuordnungen konfiguriert werden. Verwenden Sie verschiedene Klassenzuordnungen in den Richtlinienzuordnungen, um Datenverkehr zu segmentieren.

QoS mit SSL-VPN (Secure Sockets Layer)

Bis zur ASA-Version 9.2 wurden die ToS-Bits von der ASA nicht beibehalten.

SSL VPN-Tunneling wird von dieser Funktion nicht unterstützt. Weitere Informationen finden Sie unter Cisco Bug ID 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)#
```

Hinweis: Wenn Benutzer mit Telefon-VPN den AnyConnect-Client und Datagram Transport Layer Security (DTLS) zur Verschlüsselung ihres Telefons verwenden, funktioniert die Priorisierung nicht, da AnyConnect das DSCP-Flag in der DTLS-Kapselung nicht behält. Weitere Informationen finden Sie unter Erweiterungsanfrage CSCtq43909.

QoS-Überlegungen

Im Folgenden sind einige Punkte zu QoS aufgeführt, die beachtet werden sollten.

- Sie wird strikt oder hierarchisch über das modulare Richtlinien-Framework (MPF) angewendet: Policing, Shaping, LLQ.

  Kann nur den Datenverkehr beeinflussen, der bereits von der Netzwerkschnittstellenkarte (NIC) an das DP (Datenpfad) übergeben wirdUnnützlich bei der Bekämpfung von Überschreitungen (sie treten zu früh auf), wenn sie nicht auf einem benachbarten Gerät angewendet werden

- Die Richtlinienvergabe wird auf die Eingabe angewendet, nachdem das Paket zugelassen ist, und auf die Ausgabe vor der NIC.

  Direkt nach dem Umschreiben einer Layer 2 (L2)-Adresse auf die Ausgabe

- Es gestaltet die ausgehende Bandbreite für den gesamten Datenverkehr an einer Schnittstelle.

  Nützlich bei begrenzter Uplink-Bandbreite (z. B. 1-Gigabit-Ethernet (GE)-Verbindung mit 10-Mbit-Modem)Keine Unterstützung für leistungsstarke ASA558x-Modelle

- Durch Prioritätswarteschlangen wird möglicherweise bestmöglicher Datenverkehr blockiert.

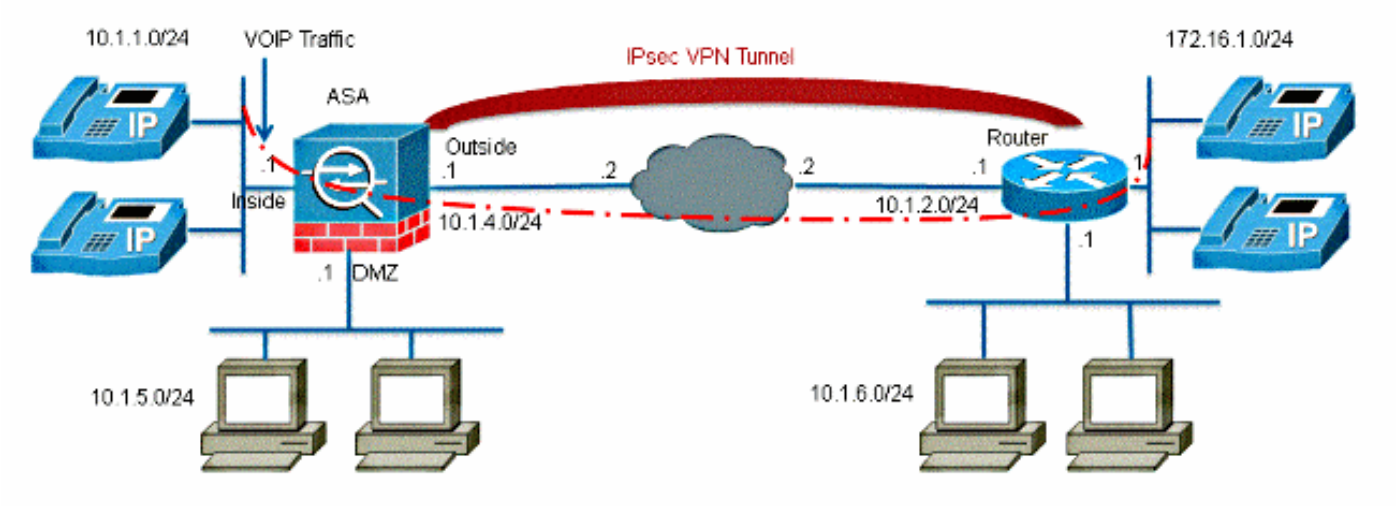
  Nicht unterstützt auf 10GE-Schnittstellen auf ASA5580- oder VLAN-SubschnittstellenDie Ringgröße der Schnittstelle kann für optimale Leistung weiter angepasst werden.

Konfigurationsbeispiele

Konfigurationsbeispiel für QoS für VoIP-Datenverkehr in VPN-Tunneln

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Hinweis: Stellen Sie sicher, dass IP-Telefone und Hosts in verschiedenen Segmenten (Subnetzen) angeordnet sind. Dies wird für ein gutes Netzwerkdesign empfohlen.

In diesem Dokument werden folgende Konfigurationen verwendet:

- QoS-Konfiguration basierend auf DSCP
- QoS basierend auf DSCP mit VPN-Konfiguration
- QoS-Konfiguration basierend auf ACL
- QoS basierend auf ACL mit VPN-Konfiguration

QoS-Konfiguration basierend auf 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
```

Hinweis: Der DSCP-Wert "ef" bezieht sich auf die beschleunigte Weiterleitung, die mit dem VoIP-RTP-Verkehr übereinstimmt.

QoS basierend auf DSCP mit VPN-Konfiguration

```
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
```

QoS-Konfiguration basierend auf 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 basierend auf ACL mit VPN-Konfiguration

```
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
```

> **Hinweis:** Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen über die in diesem Abschnitt verwendeten Befehle zu erhalten.

Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Show Service Policy Police

Um die QoS-Statistiken für die Datenverkehrsüberwachung anzuzeigen, verwenden Sie den Befehl **show service-policy** mit dem Schlüsselwort **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
```

Anzeige der Servicerichtlinienpriorität

Um Statistiken für Dienstrichtlinien anzuzeigen, die den **Priority-**Befehl implementieren, verwenden Sie den Befehl **show service-policy** mit dem **priority-**Schlüsselwort:

```
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
```

Servicerichtlinienform anzeigen

```
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
```

Statistiken zu Prioritätswarteschlangen anzeigen

Um die Statistik der Prioritätswarteschlange für eine Schnittstelle anzuzeigen, verwenden Sie den Befehl **show priority-queue statistics** im privilegierten EXEC-Modus. Die Ergebnisse zeigen die Statistiken für die Warteschlange mit bestmöglicher Leistung (BE) und die LLQ. Dieses Beispiel zeigt die Verwendung des Befehls **show priority-queue statistics** für die Schnittstelle mit dem Namen outside und die Befehlsausgabe.

```
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#
```

In diesem statistischen Bericht sind die Posten im folgenden Sinn definiert:

- "Verworfene Pakete" bezeichnet die Gesamtzahl der Pakete, die in dieser Warteschlange verworfen wurden.
- "Paketübermittlung" bezeichnet die Gesamtzahl der Pakete, die in dieser Warteschlange übertragen wurden.
- "Pakete in Warteschlange gestellt" gibt die Gesamtzahl der Pakete an, die in dieser Warteschlange in Warteschlange gestellt wurden.
- "Aktuelle Q-Länge" kennzeichnet die aktuelle Tiefe dieser Warteschlange.
- "Max Q Length" (Maximale Q-Länge) bezeichnet die maximale Tiefe, die in dieser Warteschlange aufgetreten ist.

Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zusätzliche Informationen

Die Traffic-Shaping-Funktion hat u. a. folgende Fehler hervorgerufen:

Cisco Bug-ID CSCsq08550	Traffic Shaping mit Prioritätswarteschlange verursacht Datenverkehrsausfälle auf ASA
Cisco Bug-ID CSCsx07862	Das Traffic Shaping mit Prioritätswarteschlange verursacht Verzögerungen und Verwerfungen
Cisco Bug-ID CSCsq07395	Das Hinzufügen von Shaping-Service-Richtlinien schlägt fehl, wenn die Richtlinienzuweisung bearbeitet wurde.

Häufig gestellte Fragen

Dieser Abschnitt beantwortet eine der am häufigsten gestellten Fragen zu den in diesem Dokument beschriebenen Informationen.

Werden beim Durchlaufen des VPN-Tunnels QoS-Markierungen beibehalten?

Ja. Die QoS-Markierungen bleiben im Tunnel erhalten, wenn sie die Anbieternetzwerke durchlaufen, wenn der Provider sie nicht beim Transit entfernt.

Tipp: Weitere Informationen finden Sie im Abschnitt DSCP und DiffServ Preserve im *CLI Book 2: Konfigurationsleitfaden für CLI-Konfigurationen der Cisco ASA-Serie, 9.2* für weitere Details.

Zugehörige Informationen

- CLI-Konfigurationsleitfaden für die Firewall der Cisco ASA-Serie, Quality of Service
- Anwendung von QoS-Richtlinien
- Funktionen, die in Clientless-SSL-VPN nicht unterstützt werden
- Konfigurieren von QoS
- Technischer Support und Dokumentation für Cisco Systeme