Cisco ASA 上での QoS の設定例

目次

概要
前提条件
要件
使用するコンポーネント
背景説明
トラフィック ポリシング
トラフィック シェーピング
プライオリティ キューイング
VPN トンネル経由のトラフィックの QoS
IPSec VPN を使用した QoS
IPSec トンネルに対するポリシング
セキュア ソケット レイヤ（SSL）VPN を使用した QoS
QOS の注意事項
設定例
VPN トンネル上の VoIP トラフィックの QoS 設定例
ネットワーク図
DSCP に基づく QoS 設定
VPN を使用した DSCP に基づく QoS 設定
ACL に基づく QoS 設定
VPN を使用した ACL に基づく QoS 設定
確認
show service-policy police
show service-policy priority
show service-policy shape
show priority-queue statistics
トラブルシューティング
追加情報
FAQ
QoS マークは VPN トンネルが横断されるとき維持されますか。
関連情報

概要

このドキュメントでは、Cisco 適応型セキュリティ アプライアンス（ASA）上での Quality of Service（QoS）の動作について説明し、さまざまなシナリオでの QoS の実装例を紹介します。

セキュリティ アプライアンス上で、選択されたネットワーク トラフィック（個別のフローと VPN トンネル フローの両方）にレート制限を加えるように QoS を設定することによって、限ら

れた帯域幅がすべてのトラフィックに公平に割り当てられるようにすることができます。

この機能は、Cisco Bug ID CSCsk06260 で統合されました。

前提条件

要件

Modular Policy Framwork（MPF）に関する知識を得ておくことをお勧めします。

使用するコンポーネント

このドキュメント内の情報はバージョン 9.2 を実行している ASA に基づいていますが、それ以前のバージョンにも適用できます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

QoS は、インターネット トラフィックの特定のタイプにプライオリティを設定可能なネットワーク機能です。 インターネット ユーザがアクセス ポイントをモデムからデジタル加入者線（DSL）やケーブルなどの高速ブロードバンド接続にアップグレードするほど、利用可能な帯域幅のほとんど（すべてではない）を 1 人のユーザが消費して他のユーザが使用する帯域幅が不足するという事態が起きる可能性が高まります。 特定の 1 ユーザまたはサイトツーサイト接続が適切な割り当て分を超えて帯域幅を消費することを防ぐため、QoS はユーザが使用できる最大帯域幅を管理するポリシング機能を提供します。

QoS は、基盤となるテクノロジーの限られた帯域幅で全体的に最良のサービスを実現するさまざまなテクノロジーによって、特定のネットワーク トラフィックに、より良いサービスを提供するネットワークの機能を指します。

セキュリティ アプライアンスでの QoS の主要な目的は、個別のフローまたは VPN トンネル フローの両方で、特定のネットワーク トラフィックのレートを制限し、限られた帯域幅の中ですべてのトラフィックが適切な割り当て分を得ることができるようにすることです。 フローはさまざまな方法で定義できます。 セキュリティ アプライアンスでは、送信元 IP アドレスと宛先 IP アドレスの組み合せ、送信元ポート番号と宛先ポート番号の組み合せ、および IP ヘッダーの ToS バイトに QoS を適用できます。

ASA 上に実装可能な QoS には、 ポリシング、シェーピング、およびプライオリティ キューイングの 3 種類があります。

トラフィック ポリシング

ポリシングを使用すれば、指定された制限を超えたトラフィックがドロップされます。 ポリシングは、設定された最大レート（ビット/秒単位）を超えるトラフィックが発生しないようにすることによって、1 つのトラフィック フローまたはクラスが全体のリソースを占有しないようにする方法です。 トラフィックが最大レートを超えると、ASA が超過したトラフィックをドロップします。 また、ポリシングでは、許可されるトラフィックの最大単一バーストも設定されます。

次の図に、トラフィック ポリシングの動作を示します。 トラフィック レートが設定された最大レートに達すると、超過したトラフィックがドロップされます。 その結果、出力レートは頂上と谷間のある鋸歯状になります。

次に、特定のユーザの発信方向の帯域幅を 1 Mbps に調整する例を示します。

```
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
```

トラフィック シェーピング

トラフィック シェーピングは、デバイスとリンクの速度を一致させることで、ジッタや遅延を引き起こす可能性のあるパケット損失、可変遅延、およびリンク飽和を制御するために使用されます。 セキュリティ アプライアンスでトラフィック シェーピングを使用すれば、デバイスでトラフィックのフローを制限することができます。 このメカニズムは、「速度制限」を超えたトラフィックをバッファしておいて、後でその転送を試みます。 シェーピングは、特定のタイプのトラフィック用に設定することはできません。 シェーピング対象のトラフィックには、デバイスを通過するトラフィックだけでなく、デバイスから出力されるトラフィックも含まれます。

次の図に、トラフィック シェーピングの動作を示します。 超過したパケットをキューに入れてから、一定時間の経過後に、その超過パケットを後で伝送するようスケジュールします。 トラフィック シェーピングの結果、パケットの出力レートは平滑化されます。

> **注:** トラフィック シェーピングは、ASA バージョン 5505、5510、5520、5540、および 5550 上でのみサポートされます。 マルチコア モデル（5500-X など）はシェーピングをサポートしません。

トラフィック シェーピングを使用すれば、特定の制限を超過したトラフィックがキューに入れられ、次のタイムスライスで送信されます。

ファイアウォール上のトラフィック シェーピングは、アップストリーム デバイスがネットワーク トラフィックのボトルネックになっている場合に最も有効です。 この例として、ルータ上で終端されたケーブル モデムまたは T1 経由のインターネットへのアップストリーム接続を使用した 100 Mbit インターフェイスを有する ASA を挙げることができます。 トラフィック シェーピングを使用すれば、インターフェイス（外部インターフェイスなど）の最大アウトバウンド スループットを設定することができます。 ファイアウォールは、そのインターフェイスからのトラフィックを指定された帯域幅まで送信し、超過したトラフィックをバッファして後でリンクの飽和状態

が治まってからその伝送を試みます。

シェーピングは、指定されたインターフェイスから出力されるすべての集約トラフィックに適用されます。 特定のトラフィック フローだけをシェーピングするように選択することはできません。

> **注:** シェーピングは、暗号化後に実行され、VPN の内側パケットまたはトンネル グループ単位で優先順位を付けることはできません。

この例では、外部インターフェイス上のすべての発信トラフィックを 2 Mbps にシェーピングするようにファイアウォールを設定します。

```
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
```

プライオリティ キューイング

プライオリティ キューイングを使用すれば、標準キューの前に処理される低遅延キュー（LLQ）に特定のトラフィック クラスを配置することができます。

> **注:** シェーピング ポリシーに基づいてトラフィックに優先順位を付けた場合は、内側パケットの詳細データを使用できません。 より高度なキューイングおよび QoS メカニズム（重み付け均等化キューイング（WFQ）、クラスベース重み付け均等化キューイング（CBWFQ）など）を提供可能なルータと違って、ファイアウォールは LLQ しか実行できません。

階層型 QoS ポリシーは、QoS ポリシーを階層構造で指定するためのメカニズムを提供します。 たとえば、インターフェイス上のトラフィックをシェーピングしてから、シェーピングしたインターフェイス トラフィック内で、VoIP トラフィックにプライオリティ キューイングを適用する場合は、一番上にトラフィック シェーピング ポリシーを指定して、その下にプライオリティ キューイング ポリシーを指定できます。 階層型 QoS ポリシーのサポートは対象範囲が限られています。 使用可能な唯一のオプションは次のとおりです。

- トップ レベルのトラフィック シェーピング
- 次のレベルのプライオリティ キューイング

> **注:** シェーピング ポリシーに基づいてトラフィックに優先順位を付けた場合は、内側パケットの詳細データを使用できません。 より高度なキューイングおよび QoS メカニズム（WFQ、CBWFQ など）を提供可能なルータと違って、ファイアウォールは LLQ しか実行できません。

この例では、階層型 QoS ポリシーを使用して、シェーピングの例と同様に、外部インターフェイス上のすべての発信トラフィックを 2 Mbps にシェーピングしますが、Differentiated Services Code Point（DSCP）値の "ef" を含む音声パケットとセキュア シェル（SSH）トラフィックが優先されるように指定します。

この機能を有効にするインターフェイス上でプライオリティ キューを作成します。

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

DSCP ef を照合するクラス：

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

ポート TCP/22 SSH トラフィックを照合するクラス：

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

音声と SSH トラフィックの優先順位付けを適用するポリシー マップ：

```
   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
```

すべてのトラフィックにシェーピングを適用し、優先順位付けされた音声と SSH トラフィックをアタッチするポリシー マップ:

```
   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
```

最後に、発信トラフィックをシェーピングして優先順位付けするインターフェイスにシェーピング ポリシーをアタッチします。

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

VPN トンネル経由のトラフィックの QoS

IPSec VPN を使用した QoS

RFC 2401 では、オリジナルの IP ヘッダー内の Type of Service (ToS) ビットが暗号化されるパケットの IP ヘッダーにコピーされるため、暗号化後に QoS ポリシーを適用できます。 そのため、DSCP/DiffServ ビットを QoS ポリシーの任意の場所でプライオリティとして使用できます。

IPSec トンネルに対するポリシング

ポリシングは、特定の VPN トンネルに対して実施することもできます。 ポリシングするトンネル グループを選択するには、クラス マップ内の **match tunnel-group <tunnel>** コマンドと、**match flow ip destination address** コマンドを使用します。

```
 class-map tgroup_out
match tunnel-group ipsec-tun
```

```
match flow ip destination-address
policy-map qos
class tgroup_out
police output 1000000
```

match tunnel-group コマンドを使用した場合は、その時点で入力ポリシングが機能するわけではありません。 詳細については、Cisco Bug ID CSCth48255 を参照してください。 match flow ip destination-address を使用して入力ポリシングを実行しようとすると、次のエラーが表示されます。

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

match tunnel-group を使用した場合は、その時点で入力ポリシングが機能していないように見えます（ Cisco Bug ID CSCth48255 ）。 入力ポリシングが機能するには、**match flow ip destination-address address** を使用せずに、クラス マップを使用する必要があります。

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

match ip destination address を含まないクラス マップに基づいて出力をポリシングしようとすると、次のエラーが表示されます。

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

アクセス コントロール リスト（ ACL ）や DSCP などを使用して、内側フロー情報に基づく QoS を実行することもできます。 前述のバグがあるため、現時点では、ACL が入力ポリシングを正しく実行可能な方法です。

> **注:** すべてのプラットフォーム タイプに対して、最大 64 のポリシー マップを設定できます。 トラフィックをセグメント化するには、ポリシーマップ内で複数のクラス マップを使用します。

セキュア ソケット レイヤ（ SSL ）VPN を使用した QoS

ASA バージョン 9.2 までは、ASA で ToS ビットが保存されませんでした。

この機能で SSL VPN トンネリングはサポートされません。 詳細については、Cisco Bug ID CSCsl73211 を参照してください。

```
   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)#
```

注: 電話 vpn を使っているユーザが AnyConnect クライアントと Datagram Transport Layer Security（DTLS）を使用して電話を暗号化する場合は、AnyConnect の DTLS カプセル化で DSCP フラグが保存されないため、優先順位付けが機能しません。 詳細については、機能拡張要求 CSCtq43909 を参照してください。

QOS の注意事項

QoS について考慮すべき点は次のとおりです。

- これは、厳密なまたは階層的な形式（ポリシング、シェーピング、および LLQ）の Modular Policy Framework（MPF）経由で適用されます。

  ネットワーク インターフェイス（NIC）から DP（データ パス）に渡されたトラフィックにのみ影響を与えることができる隣接デバイスに適用されない場合は、オーバーランの対処に使用できない（発生するのが早すぎる）

- ポリシングは、パケットが許可された後の入力時と NIC の前の出力時に適用されます。

  出力時にレイヤ 2（L2）アドレスを書き換えた直後

- インターフェイス上のすべてのトラフィックのアウトバウンド帯域幅をシェーピングします。

  アップリンク帯域幅が制限されている場合に有用（10Mb モデムへの 1Gigabit イーサネット（GE）リンクなど）高性能 ASA558x モデルではサポートされない

- プライオリティ キューイングはベスト エフォート トラフィックを枯渇させる可能性があります。

  ASA5580 上の 10GE インターフェイスまたは VLAN サブインターフェイス上でサポートされない最適なパフォーマンスのためにインターフェイス リング サイズをさらに調整できる

設定例

VPN トンネル上の VoIP トラフィックの QoS 設定例

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

注: IP 電話機とホストが別々のセグメント（サブネット）に配置されていることを確認します。 これは、適切なネットワーク設計として推奨されています。

このドキュメントでは、次の設定を使用します。

- DSCP に基づく QoS 設定
- VPN を使用した DSCP に基づく QoS 設定
- ACL に基づく QoS 設定
- VPN を使用した ACL に基づく QoS 設定

DSCP に基づく QoS 設定

```
!--- 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
```

注: DSCP 値の "ef" は VoIP-RTP トラフィックを照合する完全優先転送を意味します。

VPN を使用した DSCP に基づく QoS 設定

```
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
```

ACL に基づく QoS 設定

```
!--- 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
```

VPN を使用した ACL に基づく QoS 設定

```
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
```

> **注:** ここで使用されているコマンドの詳細を確認するには、Command Lookup Tool（登録ユーザ専用）を使用してください。

確認

このセクションでは、設定が正常に機能していることを確認します。

show service-policy police

トラフィック ポリシングの QoS 統計情報を表示するには、**show service-policy コマンド**と **police** キーワードを使用します。

```
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

priority コマンドを実装するサービス ポリシーの統計情報を表示するには、**show service-policy コマンド**と **priority キーワード**を使用します。

```
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

インターフェイスのプライオリティ キュー統計情報を表示するには、特権 EXEC モードで **show priority-queue** statistics コマンドを実行します。 ベスト エフォート（BE）キューと LLQ の両方の統計情報が表示されます。 次に、outside という名前のインターフェイスに対して **show priority-queue statistics コマンド**を使用した場合のコマンド出力例を示します。

```
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#
```

この統計情報レポートの項目の意味は、次のとおりです。

- 「Packets Dropped」は、このキューでドロップされたパケットの総数を示します。
- 「Packets Transmit」は、このキューで送信されたパケットの総数を示します。
- 「Packets Enqueued」は、このキューでキューイングされたパケットの総数を示します。
- 「Current Q Length」は、このキューの現在の深さを示します。
- 「Max Q Length」は、このキューで発生した最大深さを示します。

特定の show コマンドが[アウトプット インタープリタ ツール](#)（[登録ユーザ専用](#)）でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

追加情報

ここでは、トラフィック シェーピング機能によって発生したバグを示します。

Cisco bug ID [CSCsq08550](#)	プライオリティ キューイングを使用したトラフィック シェーピングが ASA 上のトラフィック エラーを引き起こす

Cisco bug ID CSCsx07862	プライオリティ キューイングを使用したトラフィック シェーピングがパケットの遅延とドロップを引き起こす
Cisco bug ID CSCsq07395	ポリシー マップを編集するとシェーピング サービス ポリシーが追加できない

FAQ

このセクションは情報に関してこの資料に説明があるほとんどの FAQ の 1 つに返事を提供します。

QoS マークは VPN トンネルが横断されるとき維持されますか。

はい。 QoS マークはトンネルでプロバイダがそれらを送信中に除去しない場合プロバイダー ネットワークを横断すると同時に維持されます。

> **ヒント**： *CLI 本 2 の* DSCP および DiffServ 保持セクションを参照して下さい*: Cisco ASA シリーズ ファイアウォール CLI コンフィギュレーション ガイド、9.2* 詳細については。

関連情報

- Cisco ASA シリーズ ファイアウォール CLI コンフィギュレーション ガイド、Quality of Service
- QoS ポリシーの適用
- クライアントレス SSL VPN でサポートされていない機能の概要
- QoS の設定
- テクニカルサポートとドキュメント - Cisco Systems