

PIX/ASA 7.x: QoS for VoIP Traffic on VPN Tunnels Configuration Example

Document ID: 82310

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Background Information

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document provides a sample configuration for Quality of Service (QoS) for Voice over IP (VoIP) traffic on VPN tunnels that terminate on the PIX/ASA Security Appliances.

The primary goal of QoS in the security appliance is to provide rate limiting on selected network traffic, for both individual flow and VPN tunnel flow, in order to ensure that all traffic gets its fair share of limited bandwidth. Refer to PIX/ASA 7.x and Later: Bandwidth Management (Rate Limit) Using QoS Policies for more information.

Note: QoS is not supported on a **subinterface**, only on the main interface itself. If you configure QoS on an interface itself, all the sub-interfaces are also affected by the QoS.

Prerequisites

Requirements

This document assumes that the necessary LAN-to-LAN (L2L) IPsec VPN configurations are made on all the devices and work properly.

Components Used

The information in this document is based on a Cisco PIX 500 Series Security Appliance that runs software version 7.x.

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.

Related Products

This configuration can also be used with the Cisco Adaptive Security Appliance (ASA) 5500 Series Security Appliance that runs software version 7.x.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

QoS is a traffic-management strategy that allows you to allocate network resources for both mission-critical and normal data, based on the type of network traffic and the priority you assign to that traffic. QoS ensures unimpeded priority traffic and provides the capability of rate-limiting (policing) default traffic.

For example, video and VoIP are increasingly important for inter-office communication between geographically dispersed sites, using the infrastructure of the Internet as the transport mechanism. Firewalls are key to network security as they control access, which includes the inspection of VoIP protocols. QoS is the focal point to provide clear, uninterrupted voice and video communications, while still providing a basic level of service for all other traffic that passes through the device.

For voice and video to traverse IP networks in a secure, reliable, and toll-quality manner, QoS must be enabled at all points of the network.

The implementation of QoS allows you to:

- Simplify network operations by collapsing all data, voice, and video network traffic onto a single backbone with the use of similar technologies.
- Enable new network applications, such as integrated call center applications and video-based training, that can help differentiate enterprises in their respective market spaces and increase productivity.
- Control resource use by controlling which traffic receives which resources. For example, you can ensure that the most important, time-critical traffic receives the network resources (available bandwidth and minimum delay) it needs, and that other applications that use the link get their fair share of service without interfering with mission-critical traffic.

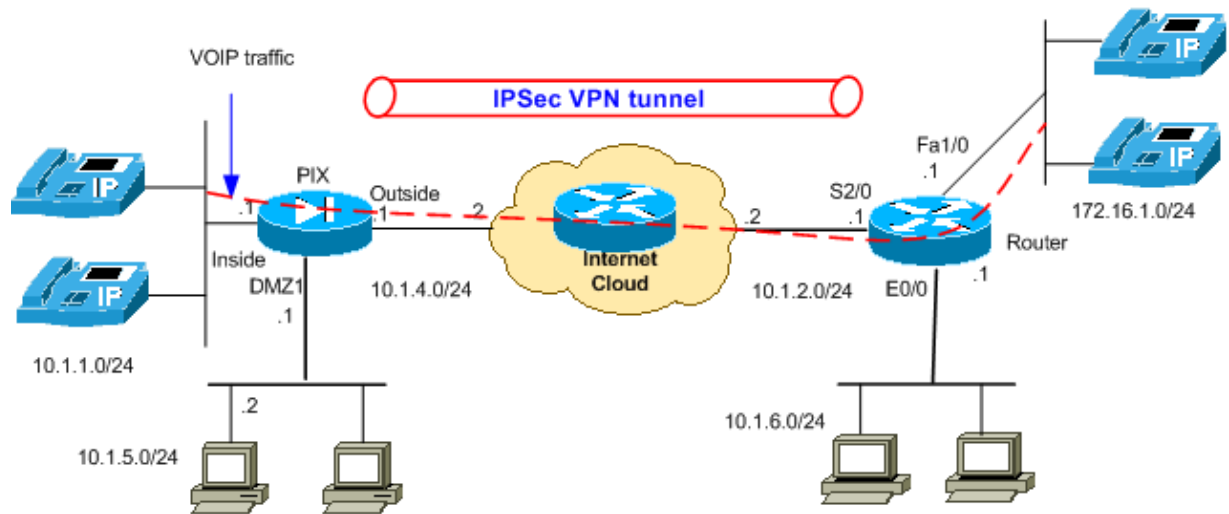
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which have been used in a lab environment.

Note: Ensure that IP phones and hosts are placed in different segments (subnets). This is recommended for a good network design.

Configurations

This document uses these configurations:

- QoS Configuration based on Differentiated Services Code Point (DSCP)
- QoS based on DSCP with VPN Configuration
- QoS Configuration based on Access Control List (ACL)
- QoS based on ACL with VPN Configuration
- Router with VPN Configuration

QoS Configuration based on DSCP

```

!--- Create a class map named Voice.
PIX(config)#class-map Voice

!--- Specifies the packet that matches criteria that
!--- identifies voice packets that have a DSCP value of "ef".
PIX(config-cmap)#match dscp ef

!--- Create a class map named Data.
PIX(config)#class-map Data

!--- Specifies the packet that matches data traffic to be passed through
!--- IPsec tunnel.
PIX(config-cmap)#match tunnel-group 10.1.2.1
PIX(config-cmap)#match flow ip destination-address

```

```

!--- Create a policy to be applied to a set
!--- of voice traffic.

PIX(config-cmap)#policy-map Voicepolicy

!--- Specify the class name created in order to apply
!--- the action to it.

PIX(config-pmap)#class Voice

!--- Strict scheduling priority for the class Voice.

PIX(config-pmap-c)#priority
PIX(config-pmap-c)#class Data

!--- Apply policing to the data traffic.

PIX(config-pmap-c)#police output 200000 37500

!--- Apply the policy defined to the outside interface.

PIX(config-pmap-c)#service-policy Voicepolicy interface outside
PIX(config)#priority-queue outside
PIX(config-priority-queue)#queue-limit 2048
PIX(config-priority-queue)#tx-ring-limit 256

```

Note: The DSCP value of "ef" refers to expedited forwarding which matches voip-rtp traffic.

QoS based on DSCP with VPN Configuration

```

PIX#show running-config
: Saved
:
PIX Version 7.2(2)
!
hostname PIX
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet1
 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 transform-set myset esp-des esp-md5-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 transform-set myset
crypto map mymap interface outside

!--- Configuration for IKE policies

crypto isakmp 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 md5
  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.
```

```

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 Configuration based on Access Control List (ACL)

!--- Permits inbound H.323 calls.

```
PIX(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.

```
PIX(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.
PIX(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.
Pix(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.
Pix(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.
Pix(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.
PIX(config)#access-group 100 in interface outside

!--- Create a class map named Voice-IN.
PIX(config)#class-map Voice-IN

!--- Specifies the packet matching criteria which
!--- matches the traffic flow as per ACL 100.
PIX(config-cmap)#match access-list 100

!--- Create a class map named Voice-OUT.
PIX(config-cmap)#class-map Voice-OUT

!--- Specifies the packet matching criteria which
!--- matches the traffic flow as per ACL 105.
PIX(config-cmap)#match access-list 105

!--- Create a policy to be applied to a set
!--- of Voice traffic.
PIX(config-cmap)#policy-map Voicepolicy

!--- Specify the class name created in order to apply
!--- the action to it.
PIX(config-pmap)#class Voice-IN
PIX(config-pmap)#class Voice-OUT

!--- Strict scheduling priority for the class Voice.
PIX(config-pmap-c)#priority
PIX(config-pmap-c)#end
PIX#configure terminal
PIX(config)#priority-queue outside

!--- Apply the policy defined to the outside interface.
```

```
PIX(config)#service-policy Voicepolicy interface outside
PIX(config)#end
```

QoS based on ACL with VPN Configuration

```
PIX#show running-config
: Saved
:
PIX Version 7.2(2)
!
hostname PIX
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet1
 nameif outside
 security-level 0
 ip address 10.1.4.1 255.255.255.0
!
interface Ethernet2
 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 transform-set myset esp-des esp-md5-hmac
crypto map mymap 10 match address 110
crypto map mymap 10 set peer 10.1.2.1
crypto map mymap 10 set transform-set myset
crypto map mymap interface outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash md5
 group 2
 lifetime 86400
tunnel-group 10.1.2.1 type ipsec-l2l
tunnel-group 10.1.2.1 ipsec-attributes
 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
```

Router with VPN Configuration

```
Router#show running-config
Building configuration...

Current configuration : 1225 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
!
!
ip cef
!
!
!
!
!
!
crypto isakmp policy 10
  hash md5
  authentication pre-share
crypto isakmp key cisco123 address 10.1.4.1
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap 10 ipsec-isakmp
  set peer 10.1.4.1
  set transform-set myset
  match address 110
!
!
!
!
interface Ethernet0/0
  ip address 10.1.6.1 255.255.255.0
  half-duplex
!
```

```

interface FastEthernet1/0
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial2/0
 ip address 10.1.2.1 255.255.255.0
 ip access-group 100 in
 no fair-queue
 crypto map mymap
!

ip http server
no ip http secure-server
!
ip route 10.1.0.0 255.255.0.0 Serial2/0
!

!--- Permits inbound IPsec traffic.

access-list 100 permit esp 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 100 permit esp 10.1.6.0 0.0.0.255 10.1.5.0 0.0.0.255
access-list 100 permit udp 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255 eq isakmp
access-list 100 permit udp 10.1.6.0 0.0.0.255 10.1.5.0 0.0.0.255 eq isakmp

!--- ACL entries for interesting traffic.

access-list 110 permit ip 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 110 permit ip 10.1.6.0 0.0.0.255 10.1.5.0 0.0.0.255
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end

```

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show running-config policy-map** Shows the QoS policy map configuration.

```

PIX#show running-config policy-map
!
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

```

- **show service-policy interface outside** Shows the QoS service policy configuration.

```
PIX#show service-policy interface outside
```

```

Interface outside:
  Service-policy: Voicepolicy
  Class-map: Voice
  Priority:
    Interface outside: aggregate drop 0, aggregate transmit 0

```

Troubleshoot

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

Use the **debug** commands in order to troubleshoot the problem.

- **debug h323 {h225 | h245 | ras}** Displays debug messages for H.323.
- **debug sip** Displays debug messages for SIP application inspection.
- **debug skinny** Displays debug messages for SCCP (Skinny) application inspection.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- **Handle VoIP Traffic with the PIX Firewall**
- **Cisco Security Appliance QoS Command Line Configuration Guide**
- **Cisco PIX 500 Series Security Appliance Product Support**

- **Cisco ASA 5500 Series Adaptive Security Appliances Support**
 - **Technical Support & Documentation – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 26, 2008

Document ID: 82310
