Integrating Cisco Secure PIX Firewall and IP/VC Videoconferencing Networks

An IP/VC Application Note

Jonathan Roberts

Network Consultant Engineer

Enterprise Voice, Video Business Unit

September 24, 2001

EDCS-154011

Table of contents

Introduction

This paper explains how to set up the Cisco Secure PIX firewall for use in Cisco IP/VC H.323 deployments. The configuration that will be shown below will be a two-interface PIX 515 running version 6.01 and utilizing NAT. The goals of this paper are:

1. Describe the issues with firewalls and H.323
2. Describe how to set up the firewall to allow H.323 video traffic to pass
3. Describe how to allow a terminal outside the firewall to register with a GK on the inside of the firewall.
4. Describe how to allow a terminal outside the firewall to communicate with a terminal on the inside of the firewall.

Where appropriate, this paper refers to existing procedures in the following Cisco user guides:

Cisco IP/VC Videoconferencing Design Guide

Managing Cisco Network Security

This guide assumes the user has basic PIX knowledge. For detailed PIX configuration steps, see the online documentation below:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_60/index.htm

Use the following link to download PIX code:

http://www.cisco.com/kobayashi/sw-center/internet/pix.shtml

Note: *For those who are new to the Cisco IP/VC videoconferencing product family and the Cisco Secure PIX Firewall, it is highly recommended that you first review the users guides referenced above, as this paper is designed to enhance your understanding of the products beyond that of the new user.*

Issues with Firewalls and H.323

What makes H.323 so cumbersome to run through a firewall is its use of multiple data ports for a single call. For an H.323 call to take place it must first open an H.225 connection on TCP port 1720, using Q.931 signaling. After this has taken place, the H.245 management session is established. While this can take place on a separate channel from the H.225 setup it can also be done using H.245 tunneling, which takes the H.245 messages and embeds them in the Q.931 messages in the previously established H.225 channel.

At this point the H.245 session opens dynamically assigned ports for the UDP-based RTP/RTCP video and audio data streams. These ports can range from 1024 to 65535. Since these ports are not known in advance, and since it would defeat the purpose of a firewall to open all these ports, a firewall must be able to "snoop" the H.323 data stream in order to open the additional ports needed for the call. This is also known as stateful inspection.

An additional problem encountered with most firewalls is the use of NAT (see "What is NAT" below for more information). Within H.323, the H.225 and H.245 signaling channels make heavy use of the embedded IP address. An example could be the following: A terminal has a private address of 10.1.1.125, which gets translated to 206.165.202.125 when it tries to place a call to an H.323 terminal with an IP address of 206.165.201.78 on the outside network. The terminal on the outside will still receive the private address within the H.225 signaling stream. Since this is a non-routable address, an attempt to make a connection back will fail. One way to get around this problem is to use an H.323-aware NAT firewall, which can rewrite the addresses in the signaling payload.

What is the Cisco Secure PIX Firewall?

Formerly known as the PIX Firewall, the Cisco Secure PIX Firewall series is the highest-performance, enterprise-class firewall product line within the Cisco firewall family. The integrated hardware/software PIX Firewall series delivers high security without impacting network performance, scaling to meet the entire range of customer requirements.

What is NAT?

Network Address Translation (NAT) is designed for IP address simplification and conservation, as it enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT can operate on the PIX or a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into globally unique addresses before packets are forwarded onto another network. As part of this functionality, NAT can be configured to advertise only one address for the entire network to the outside world. This provides additional security, effectively hiding the entire internal network from the world. NAT has the dual functionality of security and address conservation and is typically implemented in remote access environments.

There are three types of NAT available to the PIX.

-Static NAT – Static NAT is when each host on the internal network is permanently or statically mapped to an address on the external network. Because this in not a dynamic assignment process, a certain amount of administrative overhead is involved with this method.

-Dynamic NAT – Dynamic NAT intercepts traffic from a host on the internal network and maps it to an externally registered Internet Protocol (IP) address available from a pool of addresses maintained by the PIX Firewall. All translations are stored in a table to allow the traffic to make its way back to the internal host.

-PAT – Think of PAT as the port traffic version of NAT. Traffic is identified and routed through a single IP address assigned to an external interface on the firewall. PAT maps the source address of internal host connections to a single IP address on the external interface. The PIX Firewall selects and assigns the packets a new (TCP or UDP) source number. The port remapping is tracked by the PIX Firewall to ensure that traffic has a circuitous route.

Implementing NAT for use with in-bound H.323 traffic

For the purpose of this paper we will look at using a Static NAT environment, since this will allow outside callers to easily connect to systems on the inside of the firewall. The reason for choosing this is simple. If we were to use Dynamic NAT, after a user-configurable timeout period, during which there have been no translated packets for a particular address mapping, the entry is removed from the translation table and that address is freed for use by another inside host. By contrast, if we use Static NAT, you will give an inside host a permanent outside address and no time outs will occur. This will be especially useful for gatekeeper interaction.

How to configure the Cisco Secure PIX Firewall to allow H.323 traffic

For this configuration we will assume the following, which is depicted in figure 1:

- The Firewall is a PIX 515 with two interfaces.
- A Gatekeeper with an internal IP address of 10.1.1.10 and an external IP address of 209.165.201.10.
- An H.323 terminal with an internal IP address of 10.1.1.20 and an external IP address of 209.165.201.20.
- A Cisco IP/VC 3510 MCU with an internal IP address of 10.1.1.30 and an external IP address of 209.165.201.30
- An H.323 terminal residing outside the firewall with an IP address of 206.165.201.55

Figure 1: Two Interface PIX with NAT Diagram

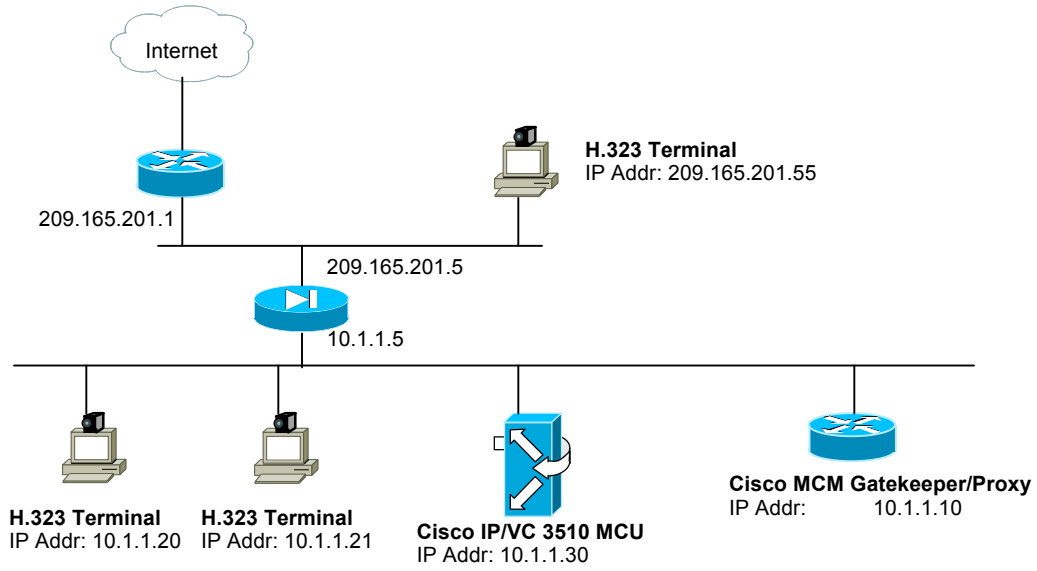

Table 1: Two Interface PIX with NAT Configuration

Configuration	Description
nameif ethernet0 outside security0 nameif ethernet1 inside security100 interface ethernet0 10baset interface ethernet1 10baset	PIX Firewall provides **nameif** and **interface** command statements for the interfaces in the default configuration. Change the default **auto** option in the **interface** command to the specific line speed for the interface card.
Fixup protocol h323 1720	The **fixup protocol** commands let you view, change, enable, or disable the use of a service or protocol through the PIX Firewall. This command will show up in configuration by default.
ip address outside 209.165.201.5 255.255.255.224 ip address inside 10.1.1.5 255.255.255.0	Identify the IP addresses for both interfaces.
arp timeout 14400	Set the ARP timeout to 14,400 seconds (four hours). Entries are kept in the ARP table for four hours before they are flushed.
nat (inside) 1 0 0	Permit all inside users to start outbound connections using the translated IP addresses from the global pool.
global (outside) 1 209.165.201.10-209.165.201.30 global (outside) 1 209.165.201.8	Create a pool of global addresses for use when they exiting the firewall from the protected networks to the unprotected networks. The **global** command statement is associated with a **nat** command statement by the NAT ID, which in this example is 1. Because there are limited IP addresses in the pool, a PAT (Port Address Translation) global is added to handle overflow.
Route outside 0.0.0.0 0.0.0.0 209.165.201.1 1	Sets the outside default route to the router attached to the Internet.
static (inside,outside) 209.165.201.10 10.1.1.10 netmask 255.255.255.255 0 0 static (inside,outside) 209.165.201.20 10.1.1.20 netmask 255.255.255.255 0 0 static (inside,outside) 209.165.201.30 10.1.1.30 netmask 255.255.255.255 0 0	The **static** command creates a permanent mapping (called a static translation slot or "xlate") between a local IP address and a global IP address. Needed in a NAT environment to allow inbound H.323 Calls.
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute	Sets default values for the maximum duration that PIX Firewall resources can remain idle until being freed. Additional users cannot make connections until a connection resource is freed either by a user dropping a connection or by an xlate and conn timer time out.
access-list acl_out permit icmp any any access-group acl_out in interrface outside	Allows inbound and outbound pings.
access-list acl_out permit udp any host 209.165.201.10 eq 1719 access-list acl_out permit tcp any host 209.165.201.20 eq h323 access-list acl_out permit tcp any host 209.165.201.30 eq 2720	The access-list command lets you specify if an IP address is permitted or denied access to a port or protocol. Port 1719 needs to be opened for Gatekeeper traffic, Port 2720 for the Cisco 3510 MCU, and Port 1820 for the Cisco 3520/3525 Gateway.
no snmp-server location no snmp-server contact snmp-server community public	Specifies that SNMP information may be accessed by internal hosts that know the community string, but PIX Firewall does not send trap information to any host.
telnet 10.0.0.100 255.255.255.255 telnet timeout 15	Specifies that host 10.0.0.100 is permitted to access the PIX Firewall console via Telnet and that 15 minutes are allowed before the idle timer runs out and the session is logged off.
mtu outside 1500 mtu inside 1500	Sets the maximum transmission unit value for Ethernet access.

Breaking down the PIX configuration

Fixup protocol Command

The first thing that we will look at in the PIX configuration is the H.323 Fixup Protocol. The H.323 fixup on PIX enables users to allow H.323 traffic to pass though the PIX.

The two major functions of the fixup are to:

1. NAT the necessary embedded IPv4 addresses in the H.225 and H.245 signaling channels. Since H.323 messages are encoded in PER encoding format, PIX uses an ASN.1 decoder to decode the H.323 messages.

2. Dynamically allocate the negotiated H245 and RTP/RTCP messages. The PIX administrator must open a conduit for the well-known H.323 port 1720 for the H.225 call signaling, however, he/she doesn't know on what ports the H.245 signaling will take place since the H.245 signaling channel is negotiated between the endpoints in the H.225 signaling. The PIX will dynamically allocate the H.245 channel after inspecting the H.225 messages and then "hookup" the H.245 channel to be fixed up as well. That means whatever H.245 messages pass thru the PIX, the PIX will pass it thru the H.245 fixup, NATing embedded IP addresses and opening the negotiated media channels.

The H.323 ITU standard requires that the H.225 and H.245 messages be preceded by a TPKT header to define the length of the message since it is passed on the reliable connection. Since the TPKT header does not necessarily need to be sent in the same TCP packet as the H.225/H.245 message, PIX must remember the TPKT length in order to process/decode the messages properly. PIX keeps a data structure for each connection, and that data structure contains the TPKT length for the next expected message.

If the PIX needs to NAT any IP addresses, then it will have to change the checksum, the UUIE (user-user information element) length, and the TPKT, IF included with the H225/H245 message.

Each connection with a packet going thru the H.323 fixup will be marked as an H.323 connection and will timeout with the H.323 timeout as configured by the user via the "timeout" command.

Static command

The static command creates a permanent mapping (called a static translation slot or "xlate") between a local IP address and a global IP address. Use the static and access-list commands when you are accessing an interface of a higher security level from an interface of a lower security level; for example, when accessing the inside from a perimeter or the outside interface. The command syntax for this command is as follows:

static [**(***internal_if_name***,** *external_if_name***)**] *global_ip local_ip* [**netmask** *network_mask*] [*max_conns* [*em_limit*]] [**norandomseq**]

In the configuration from Table XX, the static command is implemented in this manner:

static (inside,outside) 209.165.201.10 10.1.1.10 **netmask** 255.255.255.255 0 0
static (inside,outside) 209.165.201.20 10.1.1.20 **netmask** 255.255.255.255 0 0
static (inside,outside) 209.165.201.20 10.1.1.30 **netmask** 255.255.255.255 0 0

For each H.323 terminal, MCU and Gateway on the inside that you would like an external terminal to have access to will require a static entry in the PIX configuration. Likewise, if you would like external terminals to access a gatekeeper on the inside, a static entry will need to be created as well. One way to get around needing to add multiple static entries would be to implement the Cisco Multimedia Conference Manager (MCM).

The Cisco Multimedia Conference Manager (MCM) is a Cisco IOS software component that supplies gatekeeper and proxy functions for an H.323 video network. The Cisco IOS based gatekeeper allows large H.323 video networks to be built and managed on Cisco hardware. The proxy supplies needed functions that are not currently supplied by devices in some IP networks. Functions such as QoS, access to NAT networks, and firewall access are some of the functions that the proxy supplies.

Access-list command

The **access-list** command lets you specify if an IP address is permitted or denied access to a port or protocol. In this document, one or more **access-list** command statements with the same access list name are referred to as an "access list." The command syntax for this command is as follows:

access-list *acl_ID* [**deny** | **permit**] *protocol {source_addr | local_addr} {source_mask | local_mask} operator port {destination_addr |remote_addr} {destination_mask | remote_mask} operator port*

In the configuration from Table XX, the access-list is created in this manner:

access-list acl_out **permit** udp any host 209.165.201.10 eq 1719
access-list acl_out **permit** tcp any host 209.165.201.20 eq h323
access-list acl_out **permit** tcp any host 209.165.201.30 eq 2720

Here we are allowing any external unit to access the gatekeeper with an IP address of 209.165.201.10 through port 1719. This will be needed for RAS messages to pass back and forth. Also any external unit may access the H.323 terminal at IP address 209.165.201.20 on port h323 (1720), h323 or 1720 may be used interchangeably. Because of the use of the fixup protocol h323, it will not be necessary to create additional access-list commands to open other ports for H.323 communication. Lastly for the Cisco

IP/VC 3510 MCU with the IP address of 209.165.201.30, port 2720 will need to be opened.

Use the following guidelines for specifying a source, local, or destination address:

-Use a 32-bit quantity in four-part, dotted-decimal format.

-Use the keyword **any** as an abbreviation for an address and mask of 0.0.0.0 0.0.0.0. This keyword is normally not recommended for use with IPSec.

-Use **host** *address* as an abbreviation for a mask of 255.255.255.255.

Use the following guidelines for specifying a network mask:

-Do not specify a mask if the address is for a host; if the destination address is for a host, use the **host** parameter before the address; for example:

access-list acl_out permit tcp any host 192.168.1.1

-If the address is a network address, specify the mask as a 32-bit quantity in four-part, dotted-decimal format. Place zeros in the bit positions you want to ignore.

-Remember that you specify a network mask differently than with the Cisco IOS software **access-list** command. With PIX Firewall, use 255.0.0.0 for a Class A address, 255.255.0.0 for a Class B address, and 255.255.255.0 for a Class C address. If you are using a subnetted network address, use the appropriate network mask; for example:

access-list acl_out permit tcp any 209.165.201.0 255.255.255.224

Access-group command

In order to make sure that the access list is applied to a specific interface, the **access-group** command needs to be entered. The command syntax for this command is as follows:

access-group *acl_ID* **in interface** *interface_name*

In the configuration from Table XX, the access-group is applied to the outside interface in this manner:

access-group acl_out **in interface** outside

The **access-group** command binds an access list to an interface. The access list is applied to traffic inbound to an interface. If you enter the **permit** option in an **access-list** command statement, the PIX Firewall continues to process the packet. If you enter the

deny option in an **access-list** command statement, PIX Firewall discards the packet and generates the following syslog message:

%PIX-4-106019: IP packet from source_addr to destination_addr, protocol protocol received from interface interface_name deny by access-group acl_ID

Always use the **access-list** command with the **access-group** command.

Typical Ports used for H.323 traffic

Port	Protocol	Description	Terminal	MCU	Gateway	Gatekeeper
1300	TCP	H.235 secure signaling	X	X	X	
1503	TCP	T.120 Data	X	X	X	
1718	UDP	Gatekeeper discovery	X	X	X	X
1719	UDP	Gatekeeper RAS	X	X	X	X
1720	TCP	H.323 call set-up	X	X	X	
1731	TCP	Audio call control	X	X	X	
1820	TCP	Cisco IP/VC GW			X	
2720	TCP	Cisco IP/VC MCU		X		
1024-65535	TCP	H.245	X	X	X	
1024-65535	UDP	RTP (video)	X	X	X	
1024-65535	UDP	RTP (audio)	X	X	X	
1024-65535	UDP	RTCP (control)	X	X	X	

Helpful Links

Cisco Secure PIX Configuration Forms
http://www/univercd/cc/td/doc/product/iaabu/pix/pix_60/config/cfgforms.htm

Performance of PIX in H.323
http://wwwin.cisco.com/cmc/cc/pd/fw/sqfw500/tech/h3prf_in.pdf

Microsoft's How to Establish NetMeeting Connections Through a Firewall
http://support.microsoft.com/support/kb/articles/Q158/6/23.asp?LN=EN-US&SD=g

Cisco's PIX Firewall and Stateful Firewall Security
http://www/warp/public/cc/pd/fw/sqfw500/tech/nat_wp.htm

Other Cisco Secure PIX Firewall configuration examples
http://www.cisco.com/warp/customer/707/index.shtml - pix

PIX Top Issues
http://www.cisco.com/warp/customer/110/top_issues/pix/pix_index.shtml

Pix Support Page
http://www.cisco.com/cgi-bin/Support/PSP/psp_view.pl?p=Hardware:PIX

How NAT Works
http://www.cisco.com/warp/public/556/nat-cisco.shtml