

The PIX and the traceroute Command

Document ID: 25708

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Network Diagram

The traceroute Command Outbound Through the PIX

- Microsoft
- Cisco IOS or UNIX
- The User View

The traceroute Command Inbound Through the PIX

- Microsoft
- Cisco IOS or UNIX
- The User View

Use the traceroute Command to Get to the PIX Interfaces

Use the traceroute Command from the PIX

Troubleshoot

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document discusses permitting and debugging the **traceroute** command through the PIX. The **traceroute** command (which can be known as **tracert** on a PC, **trace** or **traceroute** on Cisco IOS® Software, or **traceroute** on UNIX) can be used to troubleshoot connectivity. The **traceroute** command can operate differently based on the operating system of the source device (the box that does the trace). Refer to Using the **traceroute** Command on Operating Systems for more information about operating systems and how the **traceroute** command works.

The examples in this document show how to permit these commands through the PIX:

- The Microsoft **traceroute** command (which relies on Internet Control Message Protocol [ICMP])
- The Cisco IOS or UNIX **traceroute** command (which relies on a combination of User Datagram Protocol (UDP) and ICMP)

Note: The PIX started to support the initiation of the **traceroute** command from software version 7.2(1) and later. See the Use the traceroute Command from the PIX section for further information.

Prerequisites

Requirements

There are no specific requirements for this document.

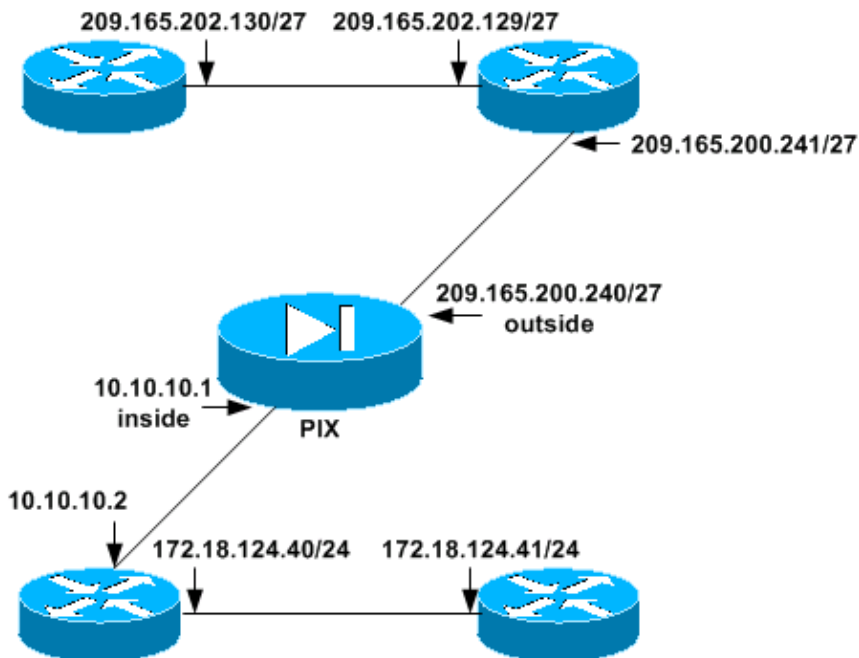
Components Used

This document is not restricted to specific software and hardware versions.

Conventions

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

Network Diagram



The traceroute Command Outbound Through the PIX

There must be static or global statements in order to allow the address translation. In this example, the translation is from 172.18.124.41 to 209.165.202.246. Therefore, the static statement is:

```
static (inside, outside) 209.165.202.246 172.18.124.41
```

In addition to the static or global statements, conduits or access control lists (ACLs) are also added.

Microsoft

Outbound ICMP is permitted by default. In PIX versions 4.2.2 and later, inbound ICMP "unreachable," "time-exceeded," and "echo-reply" responses must be explicitly permitted via conduits or ACLs:

```
conduit permit icmp host 209.165.200.246 any unreachable
conduit permit icmp host 209.165.200.246 any time-exceeded
conduit permit icmp host 209.165.200.246 any echo-reply
```

In PIX version 5.0.1 or later, ACLs can be used instead of conduits (not in conjunction with conduits) in order to perform the same function:

```
access-group 101 in interface outside
access-list 101 permit icmp any host 209.165.200.246 unreachable
```

```
access-list 101 permit icmp any host 209.165.200.246 time-exceeded
access-list 101 permit icmp any host 209.165.200.246 echo-reply
```

This allows only these return messages through the firewall when an inside user does a **ping** or **trace route** to an outside host. The other types of ICMP status messages might be hostile and the firewall blocks all other ICMP messages.

In PIX 7.x, another option is to configure ICMP inspection. This allows a trusted IP address to traverse the firewall and allows replies back to the trusted address only. This way, all inside interfaces can ping outside and the firewall allows the replies to return. This also gives you the advantage of monitoring the ICMP traffic that traverses the firewall.

For example:

```
policy-map global_policy
  class inspection_default
    inspect icmp
```

Refer to the command reference for more information about the **inspect icmp** command.

Cisco IOS or UNIX

Outbound ICMP and UDP is permitted by default, as are responses to outbound UDP. In PIX versions 4.2.2 and later, inbound ICMP "time exceeded" and "unreachable" responses must be explicitly permitted via conduits or ACLs:

```
conduit permit icmp host 209.165.200.246 any unreachable
conduit permit icmp host 209.165.200.246 any time-exceeded
```

In PIX version 5.0.1 or later, ACLs can be used instead of conduits (not in conjunction with conduits) in order to perform the same function:

```
access-group 101 in interface outside
access-list 101 permit icmp any host 209.165.200.246 unreachable
access-list 101 permit icmp any host 209.165.200.246 time-exceeded
```

The User View

This output is an example of an outbound **traceroute** command through a PIX. Note that you do not see the inside interface of the PIX but do see the "near interfaces" of each router between the tracing device and the destination.

```
goss-cl-2513#trace 209.165.202.130

Type escape sequence to abort.
Tracing the route to 209.165.202.130

 0 172.18.124.40 0 msec 0 msec 4 msec
 1 209.165.200.241 12 msec 8 msec 96 msec
 2 209.165.202.130 104 msec 8 msec *
```

In PIX 7.0, if NAT is enabled, you are unable to see the IP addresses of the PIX interfaces and the real IP addresses of the intermediate hops. However, in PIX 7.0, NAT is not a must and can be disabled with the **no nat-control** command. If the NAT rule is removed, you are able to see the real IP address, provided that the real IP address is a routeable one.

The traceroute Command Inbound Through the PIX

In order to use the **traceroute** command to get to a device inside the PIX, there must be a static mapping to the inside device. In this example, the static mapping is:

```
static (inside, outside) 209.165.202.246 172.18.124.41
```

In addition to the static or global statements, conduits or ACLs are also added.

Microsoft

In PIX versions 4.2.2 and later, an inbound ICMP "echo" must be explicitly permitted:

```
conduit permit icmp host 209.165.200.246 any echo
```

In PIX versions 5.0.1 or later, ACLs can be used instead of conduits (not in conjunction with conduits) in order to perform the same function:

```
access-group 101 in interface outside  
access-list 101 permit icmp any host 209.165.200.246 echo
```

Cisco IOS or UNIX

Inbound UDP must be permitted. Because the source and destination ports are random, all UDP is permitted to the device:

```
conduit permit udp host 209.165.200.246 any
```

In PIX versions 5.0.1 or later, ACLs can be used instead of conduits (not in conjunction with conduits) in order to perform the same function:

```
access-group 101 in interface outside  
access-list 101 permit udp host 209.165.200.246 any
```

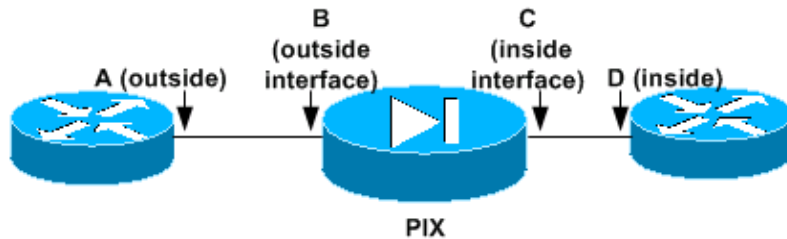
The User View

This output is an example of an inbound **traceroute** command through a PIX. The two entries for the global address are because there are two hops beyond the PIX to the inside device. However, the PIX does not divulge the actual IP address of the inside device (the static mapping), nor do you see the IP address of the PIX in the listing.

```
goss-e4-2513a#trace 209.165.200.246  
  
Type escape sequence to abort.  
Tracing the route to 209.165.200.246  
  
 1 209.165.202.129 4 msec 4 msec 8 msec  
 2 209.165.200.246 4 msec 0 msec 4 msec  
 3 209.165.200.246 8 msec 4 msec *
```

Use the traceroute Command to Get to the PIX Interfaces

The PIX is not seen in the list of routes on outbound or inbound **traceroute** commands. But can you issue a **traceroute** command to get to the PIX interfaces?



With this diagram as an example, you can see that the UDP and ICMP traffic necessary for the **traceroute** to work from A to C is not possible because you cannot send UDP or ICMP traffic from the outside to the private address of the PIX inside interface, and setting up a static for the inside interface is not valid. A **traceroute** from D to B is not possible either because the PIX outside interface does not respond to UDP or ICMP from the inside. Therefore, issuing a **traceroute** command from A to C or D to B does not work.

These Microsoft **traceroute** attempts to the PIX itself work.

- You are able to issue a **traceroute** command from D to C.
- You are able to issue a **traceroute** command from A to B.

These Cisco IOS or UNIX **traceroute** attempts to the PIX itself do *not* work.

- You are not able to issue a **traceroute** command from D to C.
- You are not able to issue a **traceroute** command from A to B.

In PIX version 5.2, the **icmp** command was introduced. This command allows you to modify the behavior of the PIX to ICMP traffic destined to the local interface of the PIX. You are now able to enable/disable ICMP requests received by the PIX.

Configure these commands in order to stop the PIX from responding to a ping attempt from host A:

```
icmp deny host A echo outside
icmp permit any outside
```

The second command (**icmp permit any outside**) is needed, as the default is to deny any ICMP type once the **icmp** command is in use.

Use the traceroute Command from the PIX

The PIX does not support the initiation of the **traceroute** command up through software version 7.1 but started to support this command in version 7.2(1) and later.

The **traceroute** command is used to discover the routes that packets actually take when they travel to their destination. The device (for example, PIX or a router or a PC) sends out a sequence of User Datagram Protocol (UDP) datagrams to an invalid port address at the remote host.

Three datagrams are sent, each with a Time-To-Live (TTL) field value set to 1. The TTL value of 1 causes the datagram to timeout as soon as it hits the first router in the path. This router then responds with an ICMP Time Exceeded Message (TEM) that indicates that the datagram has expired.

Another three UDP messages are now sent, each with the TTL value set to 2, which causes the second router to return ICMP TEMs. This process continues until the packets actually reach the other destination. Since these datagrams try to access an invalid port at the destination host, ICMP Port Unreachable Messages are returned, and indicate an unreachable port. This event signals the traceroute program that it is finished.

This example shows **traceroute** output that results when a destination IP address is specified:

```
PIX#traceroute 192.168.200.225

Tracing the route to 192.168.200.225

 0 10.83.194.1 0 msec 10 msec 0 msec
 1 10.83.193.65 0 msec 0 msec 0 msec
 2 10.88.193.101 0 msec 10 msec 0 msec
 3 10.88.193.97 0 msec 0 msec 10 msec
 4 10.88.239.9 0 msec 10 msec 0 msec
 5 10.88.238.65 10 msec 10 msec 0 msec
 6 172.16.7.221 70 msec 70 msec 80 msec
 7 192.168.200.225 70 msec 70 msec 70 msec
```

Refer to the PIX Software Version 7.2 Command Reference in order to learn more about the **traceroute** command.

Troubleshoot

- Can you issue a **traceroute** command to the devices on either side of the PIX?
- Can you ping from the PIX to the outside device and from the PIX to the inside device?
- Can you ping from the outside device to the PIX and the inside device to the PIX?
- Does the **traceroute** fail from both a PC and a Cisco IOS or UNIX box?
- Where does the **traceroute** fail?
- Do the devices in between have ACLs that might block the traffic?
- Does all traffic fail or just the **traceroute** traffic?
- Are there static device mappings set up for the inbound **traceroute**?
- Does the inside device have a route to the PIX?

Use extreme caution when you add **debug** commands to a heavily loaded PIX. However, based on the amount of traffic through the PIX, debugging can be turned on:

```
debug icmp trace
```

You can also turn on packet debug for one or more interfaces:

```
debug packet inside src 172.18.124.41 dst 209.165.202.130 proto udp both
debug packet outside src 209.165.202.130 dst any proto udp both
```

This output shows a partial debug on an inbound **traceroute**:

```
172.18.124.41 ==> 209.165.202.130
      ttl = 0x1      proto=0x11      chksum = 0xf23d
      -- UDP --
Inbound ICMP time exceeded (code 0) 209.165.200.241 > 209.165.200.243 >
172.18.124.41
172.18.124.41 ==> 209.165.202.130
      ttl = 0x2      proto=0x11      chksum = 0xf138
      -- UDP --
Inbound ICMP unreachable (code 3) 209.165.202.130 > 209.165.200.243 >
```

172.18.124.41

This output shows a partial debug on an outbound **traceroute**:

```
209.165.202.130 ==>      209.165.200.246
      ttl = 0x2          proto=0x11      chksum = 0x7f29
      -- UDP --
153: Outbound ICMP unreachable (code 3) 172.18.124.41 > 209.165.200.246 >
      209.165.202.130
```

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

- [Documentation for PIX Firewall](#)
- [PIX Command Reference](#)
- [PIX Support Page](#)
- [Requests for Comments \(RFCs\)](#)
- [Technical Support & Documentation – Cisco Systems](#)

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

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Dec 11, 2006

Document ID: 25708
