

ASA/PIX/FWSM: Handling ICMP Pings and Traceroute

Document ID: 15246

Introduction

Prerequisites

Requirements

Components Used

Conventions

Network Diagram

Send a Ping Through the PIX

PIX/ASA Software Versions 7.x

PIX Software Versions 5.0.1 Through 6.3.3

PIX Software Versions 4.2(2) to 5.0.1

PIX Software Versions 4.1(6) to 4.2(2)

Send Pings to the PIX's Own Interfaces

The traceroute Command Inbound Through the PIX

Make the Firewall Show Up in a Traceroute in ASA/PIX

Example

Error Message – 313005

ICMP Message Types (RFC 792)

Information to Collect if You Open a Service Request

Related Information

Introduction

Internet Control Message Protocol (ICMP) pings and traceroute on the PIX Firewall are handled differently based on the version of PIX and ASA code.

Inbound ICMP through the PIX/ASA is denied by default. Outbound ICMP is permitted, but the incoming reply is denied by default.

Note: ASA/PIX does not support ICMP redirects, because it does not support asymmetric routing.

Note: The information in the Make the Firewall Show Up in a Traceroute in ASA/PIX section of this document applies to ASA versions 8.0(3) and later. Versions prior to 8.0(3) do not support the configuration explained in this section due to the bug CSCsk76401 (registered customers only) .

Prerequisites

Requirements

There are no specific prerequisites for this document.

Components Used

The information in this document is based on these software and hardware versions:

- PIX software versions 4.1(6) and later

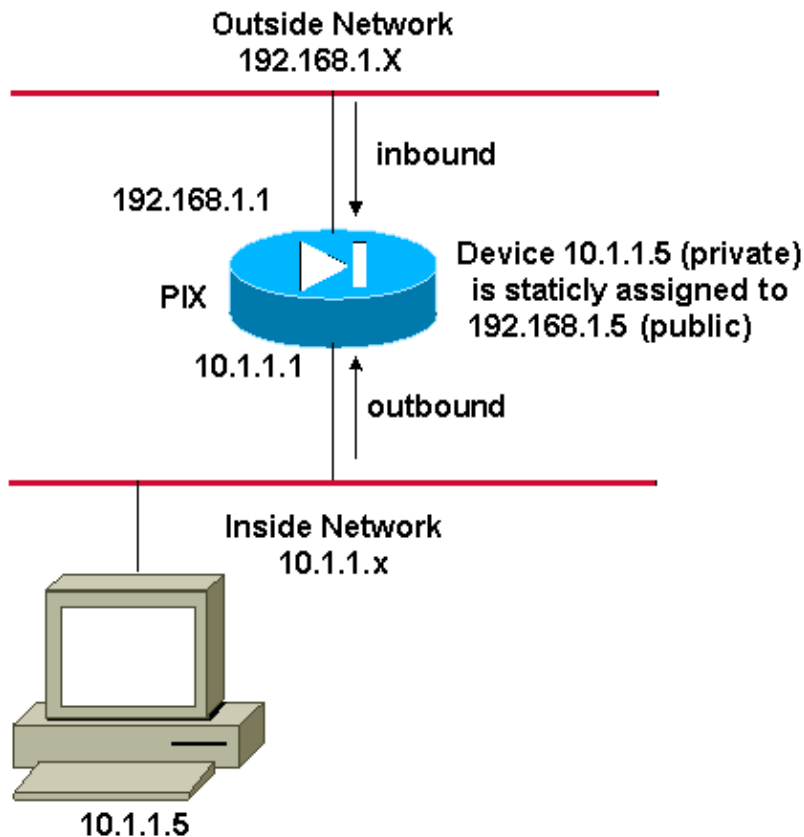
- Cisco ASA 5500 Series Security Appliance that runs 7.x and later versions for ICMP Pings
- Cisco ASA 5500 Series Security Appliance that runs 8.0(3) and later versions for Traceroute in ASA

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.

Conventions

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

Network Diagram



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.

Send a Ping Through the PIX

PIX/ASA Software Versions 7.x

Pings Inbound

Pings initiated from the outside, or another low security interface of the PIX, are denied by default. The pings can be allowed by the use of static and access lists or access lists alone. In this example, one server on the inside of the PIX is made accessible to external pings. A static translation is created between the inside address (10.1.1.5) and the outside address (192.168.1.5).

```
pix(config)#static (inside,outside) 192.168.1.5 10.1.1.5 netmask 255.255.255.255
pix(config)#access-list 101 permit icmp any host 192.168.1.5 echo
pix(config)#access-group 101 in interface outside
```

Pings Outbound

There are two options in PIX 7.x that allow inside users to ping hosts on the outside. The first option is to setup a specific rule for each type of echo message.

For example:

```
access-list 101 permit icmp any any echo-reply
access-list 101 permit icmp any any source-quench
access-list 101 permit icmp any any unreachable
access-list 101 permit icmp any any time-exceeded
access-group 101 in interface outside
```

This allows only these return messages through the firewall when an inside user pings to an outside host. The other types of ICMP status messages might be hostile and the firewall blocks all other ICMP messages.

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, hosts on all inside interfaces can ping hosts on the outside and the firewall allows the replies to return. This also gives you the advantage of monitoring the ICMP traffic that traverses the firewall. In this example, **icmp inspection** is added to the default global inspection policy.

For example:

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

Pinging Another Interface

The **management-access** command allows users to connect to the management-access interface from the outside ONLY when the user is connected to PIX/ASA using a full tunnel IPsec VPN or SSL VPN client (AnyConnect 2.x client, SVC 1.x) or across a site-to-site IPsec tunnel.

The inside interface of the PIX cannot be accessed from the outside, and vice-versa, unless the management-access is configured in global configuration mode. Once management-access is enabled, Telnet, SSH, or HTTP access must be configured for the desired hosts.

```
pix(config)#management-access inside
pix(config)#show running-config management-access
management-access inside
```

PIX Software Versions 5.0.1 Through 6.3.3

Inbound ICMP through the PIX is denied by default; outbound ICMP is permitted, but the incoming reply is denied by default.

Note: Version 6.3.3 is the most recent version of code available at the time of publication. For later versions, refer to the release notes for any possible changes.

Pings Inbound

Inbound ICMP can be permitted with either a **conduit** statement or an **access-list** statement, based on which you use on the PIX. Do *not* mix conduits and access lists.

This example shows how to permit ICMP of device 10.1.1.5 inside (static to 192.168.1.5) by all devices outside:

```
static (inside,outside) 192.168.1.5 10.1.1.5 netmask 255.255.255.255 0 0

!--- and either

conduit permit icmp 192.168.1.5 255.255.255.255 0.0.0.0 0.0.0.0 echo

!--- or

access-list 101 permit icmp any host 192.168.1.5 echo
access-group 101 in interface outside
```

Pings Outbound

Responses to outbound ICMP can be permitted with either a **conduit** statement or an **access-list** statement, based on which you use on the PIX. Do *not* mix conduits and access lists.

This example shows how to permit responses to ICMP requests initiated by device 10.1.1.5 inside (static to 192.168.1.5) from all devices outside:

```
static (inside,outside) 192.168.1.5 10.1.1.5 netmask 255.255.255.255 0 0

!--- and either

conduit permit icmp 192.168.1.5 255.255.255.255 0.0.0.0 0.0.0.0 echo-reply
conduit permit icmp 192.168.1.5 255.255.255.255 0.0.0.0 0.0.0.0 source-quench
conduit permit icmp 192.168.1.5 255.255.255.255 0.0.0.0 0.0.0.0 unreachable
conduit permit icmp 192.168.1.5 255.255.255.255 0.0.0.0 0.0.0.0 time-exceeded

!--- or

access-list 101 permit icmp any host 192.168.1.5 echo-reply
access-list 101 permit icmp any host 192.168.1.5 source-quench
access-list 101 permit icmp any host 192.168.1.5 unreachable
access-list 101 permit icmp any host 192.168.1.5 time-exceeded
access-group 101 in interface outside
```

PIX Software Versions 4.2(2) to 5.0.1

Inbound ICMP through the PIX is denied by default. Outbound ICMP is permitted, but the incoming reply is denied by default.

Pings Inbound

Inbound ICMP can be permitted with a conduit statement.

This example shows how to permit ICMP of device 10.1.1.5 inside (static to 192.168.1.5) by all devices outside:

```
static (inside,outside) 192.168.1.5 10.1.1.5 netmask 255.255.255.255 0 0
conduit permit icmp 192.168.1.5 255.255.255.255 0.0.0.0 0.0.0.0 echo
```

Pings Outbound

Responses to outbound ICMP can be permitted with a conduit statement.

This example shows how to permit responses to ICMP requests initiated by device 10.1.1.5 inside (static to 192.168.1.5) from all devices outside:

```
static (inside,outside) 192.168.1.5 10.1.1.5 netmask 255.255.255.255 0 0
conduit permit icmp 192.168.1.5 255.255.255.255 0.0.0.0 0.0.0.0 echo-reply
conduit permit icmp 192.168.1.5 255.255.255.255 0.0.0.0 0.0.0.0 source-quench
conduit permit icmp 192.168.1.5 255.255.255.255 0.0.0.0 0.0.0.0 unreachable
conduit permit icmp 192.168.1.5 255.255.255.255 0.0.0.0 0.0.0.0 time-exceeded
```

PIX Software Versions 4.1(6) to 4.2(2)

Inbound ICMP through the PIX is denied by default. Outbound ICMP is permitted by default.

Pings Inbound

Inbound ICMP can be permitted with a conduit statement.

This example shows how to permit ICMP of device 10.1.1.5 inside (static to 192.168.1.5) by all devices outside:

```
static (inside), outside) 192.168.1.5 10.1.1.5
conduit 192.168.1.5 8 icmp 0.0.0.0 0.0.0.0
```

!--- The 8 is for echo request; these are from RFC 792.

See the ICMP Message Types (RFC 792) section of this document for more information.

Pings Outbound

Outbound ICMP and responses are permitted by default.

Send Pings to the PIX's Own Interfaces

In PIX Software versions 4.1(6) to 5.2.1, ICMP traffic to the PIX's own interface is permitted. The PIX cannot be configured to not respond. You are not able to ping interfaces on the "far side" of the PIX in any version. Based on the network diagram in this document:

- You are not able to ping 10.1.1.1 from 10.1.1.5.
- You are not able to ping 192.168.1.1 from the outside.
- You are not be able to ping 192.168.1.1 from 10.1.1.5.
- You are not able to ping 10.1.1.1 from the outside.

In PIX Software versions 5.2.1, ICMP is still permitted by default, but PIX ping responses from its own interfaces can be disabled with the **icmp** command (that is, a "stealth PIX").

```
icmp permit|deny [host] src_addr [src_mask] [type] int_name
```

In this example, the PIX cannot send echo replies in response to echo requests:

```
icmp deny any echo outside
```

As with access lists, in the absence of **permit** statements, there is also an implicit deny of all other ICMP traffic.

This command permits pings from the network immediately outside the PIX:

```
icmp permit 192.168.1.0 255.255.255.0 echo outside
```

As with access lists, in the absence of **permit** statements, there is also an implicit deny of all other ICMP traffic.

The traceroute Command Inbound Through the PIX

Problem: The PIX Firewall hides all internal networks in the output of inbound traceroutes.

Resolution:

The PIX does not support the **traceroute** command. When a **traceroute** is issued from the outside, the PIX does not display its own interface IP address nor does it display the IP addresses of the inside networks. The destination address is displayed multiple times for each internal hop.

Traceroutes work only with static Network Address Translations (NATs) and not with Port Address Translation (PAT) IP addresses. For example, a client on the Internet with the address 209.165.202.130 performs a traceroute to a web server on the inside of the PIX with a public address of 209.165.201.25 and a private address of 10.1.3.25. There are two routers between the PIX and the internal web server. The **traceroute** output on the client machine appears this way:

```
Target IP address: 209.165.201.25 Source address: 209.165.202.130
```

```
Tracing the route to 209.165.201.25
 0 209.165.202.128 4 msec 3 msec 4 msec
 1 209.165.201.25 3 msec 5 msec 0 msec
 2 209.165.201.25 4 msec 6 msec 3 msec
 3 209.165.201.25 3 msec 2 msec 2 msec
```

In PIX version 6.3 and later, this behavior can be undone if the **fixup protocol icmp error** command is issued. When this feature is enabled, the PIX creates xlates for intermediate hops that send Internet Control Message Protocol (ICMP) error messages, based on the static NAT configuration. The PIX overwrites the packet with the translated IP addresses.

When NAT is enabled in PIX 7.0, the IP addresses of the PIX interfaces and the real IP addresses of the intermediate hops cannot be seen. However, in PIX 7.0, NAT is not essential and can be disabled with the **no nat-control** command. If the NAT rule is removed, the real IP address can be seen if it is a routeable one.

Configure the PIX/ASA to show its internal network from the outside network:

```
ciscoasa#config t
ciscoasa(config)#access-list internal-out permit icmp any any echo-reply
ciscoasa(config)#access-list internal-out permit icmp any any time-exceeded
ciscoasa(config)#access-list internal-out permit icmp any any unreachable
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#
inspect icmp
```

```
ciscoasa(config-pmap-c)#  
inspect icmp error  
  
ciscoasa(config-pmap-c)#end  
ciscoasa(config)#service-policy global_policy global  
ciscoasa(config)#access-group internal-out in interface outside
```

For more information, refer to the The traceroute Command Inbound Through the PIX section of The PIX and the traceroute Command.

Make the Firewall Show Up in a Traceroute in ASA/PIX

```
ciscoasa(config)#class-map class-default  
ciscoasa(config)#match any
```

!--- This class-map exists by default.

```
ciscoasa(config)#policy-map global_policy
```

!--- This Policy-map exists by default.

```
ciscoasa(config-pmap)#class class-default
```

!--- Add another class-map to this policy.

```
ciscoasa(config-pmap-c)#set connection decrement-ttl
```

*!--- Decrement the IP TTL field for packets traversing the firewall.
!--- By default, the TTL is not decrement hiding (somewhat) the firewall.*

```
ciscoasa(config-pmap-c)#exit  
ciscoasa(config-pmap)#exit  
ciscoasa(config)#service-policy global_policy global
```

!--- This service-policy exists by default.

WARNING: Policy map global_policy is already configured as a service policy

```
ciscoasa(config)#icmp unreachable rate-limit 10 burst-size 5
```

*!--- Adjust ICMP unreachable replies:
!--- The default is rate-limit 1 burst-size 1.
!--- The default will result in timeouts for the ASA hop:*

```
ciscoasa(config)#access-list outside-in-acl remark Allow ICMP Type 11 for Windows tracert  
ciscoasa(config)#access-list outside-in-acl extended permit icmp any any time-exceeded
```

*!--- The access-list is for the far end of the ICMP traffic (in this case
!---the outside interface) needs to be modified in order to allow ICMP type 11 replies
!--- time-exceeded):*

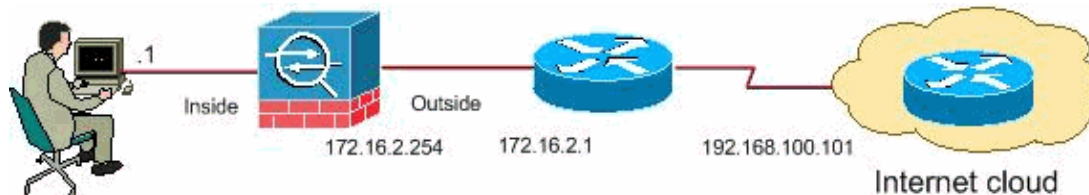
```
ciscoasa(config)#access-group outside-in-acl in interface outside
```

```
!--- Apply access-list to the outside interface.
```

```
ciscoasa(config)#
```

Example

Topology



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

Before you apply the policy change:

```
C:\>tracert -d www.yahoo.com.
```

```
Tracing route to www.yahoo-ht3.akadns.net [192.168.93.52]  
over a maximum of 30 hops:
```

```
 1      1 ms      <1 ms      <1 ms      172.16.2.1
```

```
!--- First shown hop is Router 1
```

```
 2      6 ms      6 ms      5 ms      192.168.100.101  
(etc...)
```

After you apply the policy change:

```
C:\>tracert -d www.yahoo.com.
```

```
Tracing route to www.yahoo-ht3.akadns.net [192.168.93.52]  
over a maximum of 30 hops:
```

```
 1      <1 ms      <1 ms      <1 ms      172.16.2.254
```

```
!--- First shown hop is ASA
```

```
 2      <1 ms      <1 ms      <1 ms      172.16.2.1
```

```
!--- Router 1 is now second hop
```

```
 3      6 ms      6 ms      6 ms      192.168.100.101  
(etc...)
```

Error Message – 313005

Error Message

```
%PIX|ASA-4-313005: No matching connection for ICMP error message:  
icmp_msg_info on interface_name interface. Original IP payload:  
embedded_frame_info icmp_msg_info = icmp src src_interface_name:src_address dst
```

```
dest_interface_name:dest_address (type icmp_type, code icmp_code)
embedded_frame_info = prot src source_address/source_port dst
dest_address/dest_port
```

Explanation

ICMP error packets are dropped by the security appliance because the ICMP error messages are not related to any session already established in the security appliance.

Recommended Action

If the cause is an attack, you can deny the host with ACLs.

ICMP Message Types (RFC 792)

Message Number	Message
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply

Information to Collect if You Open a Service Request

If you still need assistance after following the troubleshooting steps above and want to open a service request with the Cisco TAC, be sure to include the following information for troubleshooting your PIX Firewall.

- Problem description and relevant topology details
- Troubleshooting performed before opening the service request
- Output from the **show tech-support** command
- Output from the **show log** command after running with the **logging buffered debugging** command, or console captures that demonstrate the problem (if available)

Please attach the collected data to your service request in non-zipped, plain text format (.txt). You can attach information to your service request by uploading it using the Service Request Query Tool (registered customers only). If you cannot access the

Service Request Query Tool, you can send the information in an email attachment to attach@cisco.com with your service request number in the subject line of your message.

Related Information

- [RFC 792](#)
 - [Documentation for PIX Firewall](#)
 - [PIX Command Reference](#)
 - [PIX Support Page](#)
 - [Requests for Comments \(RFCs\)](#)
 - [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: Nov 03, 2009

Document ID: 15246
