navbar
Strip_TechNotes

Establishing Connectivity Through Cisco PIX Firewalls

Help us help you.

Please rate this et:

- Excellent
- Good
- Average
- Fair
- Poor

his et sle::rle:

- Yes
- No
- Just browsing

estis r ireet:

(256 character limit)

Send

Contents

- **Introduction**
  - Hardware and Software Versions
- **Network Diagram**
- **How Connectivity Through the PIX Works**
- **Configuring Connectivity Through the PIX**
- **Troubleshooting Connectivity Problems**
- **`conduit` and `access-list` Command Syntax**
  - PIX Software Release 4.1
  - PIX Software Release 4.2.x and Later
  - PIX Software Release 5.0.x and Later
- **Related Information**

Introduction

When a PIX firewall is configured initially, it has a default security policy: everyone on the inside can get out, and nobody from the outside can get in. If your site requires a different security policy, you can allow outside users to connect to your web server through the PIX.

Once you have established basic connectivity through the firewall, you can make configuration changes to the firewall. Make sure any configuration changes you make to the PIX firewall are in compliance with your site's security policy.

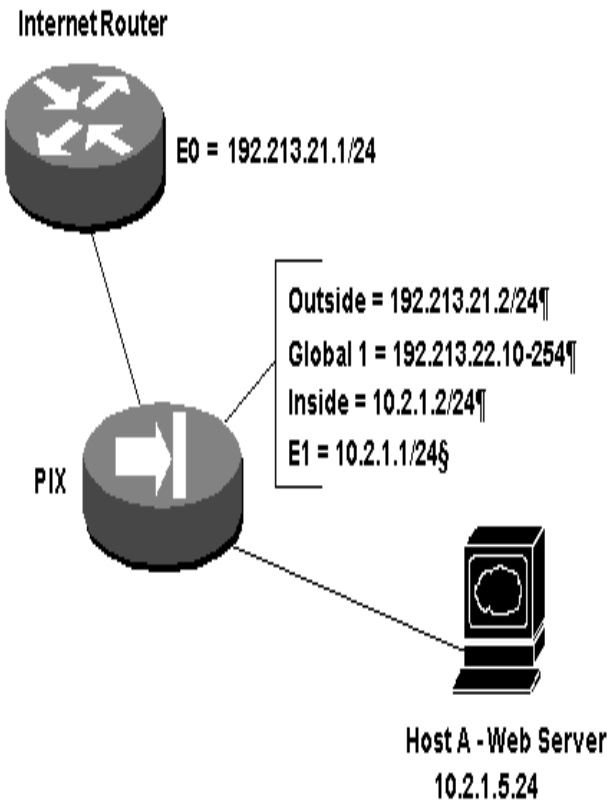
Hardware and Software Versions

The information in this document is based on the software and hardware versions below.

- PIX Firewall Software Releases 5.0.x and later

Note: Earlier versions of the PIX software used the **conduit** command instead of the **access-list** command. Either command works in PIX Firewall Software Releases 5.0.x and later.

Network Diagram



How Connectivity through the PIX Works< /h2>

In the illustration above, Host A is the web server with an internal address of 10.2.1.5. The web server is assigned an external (translated) address of 192.213.22.5. Internet users must point to 192.213.22.5 in order to access the web server. The DNS entry for your web server should be that address. No other connections are allowed from the Internet.

Configuring Connectivity Through the PIX

For more information about command syntax, see the `conduit` and `access-list` Command Syntax section below.

1. **Set up a global pool for the internal hosts to use when they access the Internet.**

```
global (outside) 1 192.213.22.10-192.213.22.254 net
```

2. **Direct internal addresses to select from the global 1 pool.**

```
nat (inside) 1 0.0.0.0 0.0.0.0
```

3. **Assign a static translated address for the internal host to which Internet users will have access.**

```
static (inside,outside) 192.213.22.5 10.2.1.5 0 0
```

4. **Use the access-list command to allow outside users through the PIX firewall. Always use the translated address in the access-list command.**

```
access-list 101 permit tcp any host 192.213.22.5
access-group 101 in interface outside
```

Troubleshooting Connectivity Problems

If Internet users cannot access your web site, try the following steps:

1. **Make sure you have entered the following addresses correctly:**
   - **Valid external address**
   - **Correct internal address**
   - **External DNS has translated address**

2. **Use the show static command to make sure that static translation is enabled.**

3. **Check to see that the default route on the web server is pointing to the inside interface of the PIX.**

4. **Use the logging console debug command to check the log files to see if denies are occurring. (Look for the translated address and see if you see any denies.)**

5. **If the network is not busy, you can capture the traffic with the following command. (Note: This command generates a significant amount of output. It can cause a router to hang or reload under heavy traffic loads.)**

   ```
   debug packet outside dst 192.213.22.5 proto tcp dpo
   ```

   This command captures packets coming from any external host toward the web server. You must be on the console to see if the packets are getting to the PIX.

6. **If packets are making it to the PIX, make sure your route to the web server from the PIX is correct. (Check the route commands in your PIX configuration.)**

7. **If everything appears to be correct, and users still cannot access the web server, open a case with the Technical Assistance Center (TAC).**

`conduit` and `access-list` Command Syntax

PIX Software Release 4.1

The syntax of the conduit command changed between PIX Software Releases 4.1 and 4.2. The syntax for the conduit command in PIX software release 4.1 is as follows:

conduit [(*internal_if_name, external_if_name*)] *global_ip port*[*-port*] *protocol foreign_ip* [*netmask*]

Example: conduit (inside,outside) 192.213.22.5 80 tcp 0 0

PIX Software Release 4.2.x and Later

The syntax is as follows:

conduit permit|deny *protocol global_ip global_mask [operator port [port]] foreign_ip foreign_mask [operator port [port]]*

PIX Software Release 5.0.x and Later

The access-list command was introduced in PIX Software Release 5.0. The syntax for the access-list command is as follows:

access-list *acl_name* [deny | permit] *protocol source source_netmask destination destination_netmask*

Example: access-list 101 permit tcp any host 192.213.22.5 eq www

To *apply* the access list, you must include the following syntax in your configuration:

access-group *acl_name in interface interface_name*

Related Information

- **More PIX Technical Tips**
- **PIX Firewall documentation**
- **Cisco PIX Firewall Product Information**

All contents are Copyright © 1992--2001 Cisco Systems Inc. All rights reserved. Important Notices and Privacy Statement.