



MS-Exchange Firewall Configuration

This appendix explains how you can configure the PIX Firewall to support Microsoft Exchange by creating **access-list** command statements for NetBIOS and TCP. The example that follows will work for two Windows NT Servers; one on the inside network of the PIX Firewall, and the other on the external network from where you want to send and receive mail. Once Microsoft Exchange is functioning across the PIX Firewall, users can send and receive mail with mail clients on platforms other than Windows NT.

Before starting, complete the following:

- Determine the PIX Firewall's global address you will use in the **static** command statement.
- Have previously installed Microsoft Exchange on both Windows NT systems.
- Select the Windows NT system from the Administrator login.
- Determine the IP address, computer name, and domain name of each Windows NT system. Click **Start>Settings>Control Panel>Network** and click the entry for the Ethernet adapter. Then click **Properties**. The information you need appears on the IP Address tab and DNS Configuration tab.

This appendix includes the following sections:

- [Configuring the Microsoft Exchange Servers](#)
- [Configuring the PIX Firewall](#)
- [Configuring the Outside Server](#)
- [Configuring the Inside Server](#)
- [Configuring Both Systems After Rebooting](#)

Configuring the Microsoft Exchange Servers

The information that follows describes the configuration required for two Windows NT systems to pass mail across the PIX Firewall.



Note

To use the procedure that follows, you should be completely familiar with Microsoft Exchange and the administrative functionality of your Windows NT Server.

To help understand the procedure discussed in this appendix, [Table C-1](#) lists the host names, their IP addresses, and the domains.

Table C-1 Names and Addresses

System	Name	IP Address	Domain
Outside Windows NT Server	outserver	209.165.201.2	pixout
Inside Windows NT Server	inserver	192.168.42.2	pixin
PIX Firewall outside interface	None	209.165.201.1	None
PIX Firewall inside interface	None	192.168.42.1	None

The PIX Firewall **static** command statement uses 209.165.201.5 as its global address. An administrative domain is created with the Microsoft Exchange Administrator application named **CISCO** in this example. This domain includes both servers.

The sections that follow show how to configure the Microsoft Exchange servers and the PIX Firewall. Complete each section before moving to the next.

Configuring the PIX Firewall

Follow these steps to configure the PIX Firewall:

-
- Step 1** Create **static** and **access-list** commands to permit the outside server access to the inside server via the global address in the PIX Firewall.

For example:

```
static (inside,outside) 209.165.201.5 192.168.42.2 0 0
access-list acl_out permit tcp host 209.165.201.2 host 209.165.201.5 eq 139
access-list acl_out permit udp host 209.165.201.2 host 209.165.201.5 eq 137
access-list acl_out permit udp host 209.165.201.2 host 209.165.201.5 eq 138
access-list acl_out permit tcp host 209.165.201.2 host 209.165.201.5 eq 135
access-group acl_out in interface outside
```

The **static** command statement permits the inside server, 192.168.42.2 to be accessible from the outside at global address 209.165.201.5. The **access-list** commands give the outside server, 209.165.201.2, access to the inside server's global address, 209.165.201.5. Port 139 gives access to NetBIOS over TCP. Access to UDP ports 137 and 138 is also required.

The last **access-list** command statement for TCP port 135 permits the outside server to come in via MSRPC (Microsoft Remote Procedure Call), which uses TCP.

The **access-group** command statement binds the **access-list** command statements to the outside interface.

- Step 2** The **static** command statement in Step 1 also allows outbound initiation, but requires an **established** command statement to allow back connections:

```
established tcp 135 permitto tcp 1024-65535
```

This command statement allows the RPC back connections from the outside host on all high ports (1024 through 65535) to deliver mail.

- Step 3** Enter the **syslog console** command statement so that you can watch for messages after you configure the two servers.
-

Configuring the Outside Server

Follow these steps to configure the outside Microsoft Exchange server:

-
- Step 1** On the outside Microsoft Exchange server, click the **Network** entry in the **Start>Settings>Control Panel**. In the Ethernet adapter **Properties** section, set the primary WINS (Windows Internet Name System) address to the IP address of the outside system, in this case, 209.165.201.2. Set the secondary WINS address to the global address from the **static** command statement, 209.165.201.5.
- Step 2** Also in the **Network** entry, click **Services>Computer Browser**. Ensure that the outside server is the master browser for the server's outside domain, which in this case, is **pixout**.
- Step 3** Click **Start>Programs>WINS Manager**. Click **Mappings>Static Mappings**. Add a static mapping for the inside server's domain, **pixin**, with the global address from the **static** command statement, 209.165.201.5. Also add a unique mapping for the inside server's name, **inserver**, and set it as well to the global address from the **static** command statement. Then save the new information and exit the WINS Manager.
- Step 4** Next, establish a trusted, trusting relationship between the outside server's domain, **pixout** and the inside server's domain, **pixin**.
- Click **Start>Programs>Administrative Tools>User Manager for Domains**.
 - Click **Policies>Trust Relationship** and then click **Trusting Domain**.
 - Add a trusting domain for the inside server's domain and assign a password to it.
 - Establish a trusted domain for **pixin** by clicking **Trusted Domain**.
- Step 5** Exit the application and reboot the Windows NT system.
-

Configuring the Inside Server

Follow these steps to configure the inside Microsoft Exchange server:

-
- Step 1** On the inside server, click **Settings>Control Panel>Network**, set the primary WINS address to the address of that system, 192.168.42.2, and set the secondary WINS address to the inside address of the PIX Firewall, 192.168.41.1.
- In the **Network** entry, click **Services>Computer Browser**. Ensure that the inside server is the master browser for the domain, which in this case, is **pixin**.
- In the **Network** entry, click **Protocols>TCP/IP Protocol>WINS Configuration**. Set the primary and secondary WINS address to that of the inside server, in this case, 192.168.42.2. On the **Default Gateway** tab, set the address to the inside address of the PIX Firewall, in this case, 192.168.42.1.
- Step 2** Click **Start>Programs>WINS Manager**, and specify a static mapping for the outside server's domain, **pixout**, and a unique mapping for the outside server, **outserv**. Set both to the address of the outside server, 209.165.201.2.
- On the **Server** menu, click **Replication Partners** and add a **Pull Partner** for the outside server, in this case, 209.165.201.2. This permits pulling the outside server's database to the inside server's local database. This incorporates the two server's databases so that user information is shared across the firewall. Use the default options in the remainder of this dialog box.
- You can view the information you entered by clicking **Mappings>Show Database**.

- Step 3** Establish a trusted, trusting relationship between the inside server's domain, **pixin** and the outside server's domain, **pixout**.
- Click **Start>Programs>Administrative Tools>User Manager for Domains**.
 - Click **Policies>Trust Relationship** and click **Trusting Domain**.
 - Add a trusting domain for the outside server's domain and assign a password to it.
 - Establish a trusted domain for **pixout** by clicking **Trusted Domain**.
- Step 4** Exit the application and reboot the Windows NT system.
-

Configuring Both Systems After Rebooting

After rebooting, follow these steps to configure both the inside and outside servers:

-
- Step 1** After the systems are usable, on the inside server, click **Start>Find>Computer** and look up the outside server, in this case, by entering `\\outserv`. Then go to the outside server and find **inserv**.
- Step 2** On each server, configure Microsoft Exchange by clicking **Start>Programs>Microsoft Exchange Administrator** to connect to the other server. Declare a network name, in this case, **CISCO** on both servers. On each server, declare the site name to be the respective server's domain name. In this case, on the inside server, the site name is **pixin**. On the outside server, it is **pixout**.
- Click **File>Connect to Server** to connect to the other server.
- Step 3** From the Administrator application, configure the site connector. Double-click your site name in the **Configure/Connections** field and the Connections list appears. Ensure you have a site connector installed. If you followed the defaults when you installed Microsoft Exchange, this should be present. If not, add the site connector for the server's respective domains, just as you did in Step 2. For the **cost**, use the default. For the **Messaging Bridge Head**, use the name of that server. For the **Target Server**, use the name of the other server. You can ignore the **Address Space** field.
- Step 4** Once both sites are connected, the Administrator application should show the other site available for access. Ensure that at least one username is specified on each server that you can use as a test login.
- Step 5** Then test email from a mail client with the username. The global address list in the address book should list the other server and users on either side. Send the email message.
-

On the PIX Firewall, you should now be able to see syslog messages indicating a MSRPC connection. If you are sending mail from the inside network to the outside network, you should see a MSRPC connection going from the inside server to the outside server on port 135. Then you should see another high-port connection being built between the outside server and the inside server. Your email should flow through almost immediately.