

How to Use Service Redirection

WhistleWare 4.1

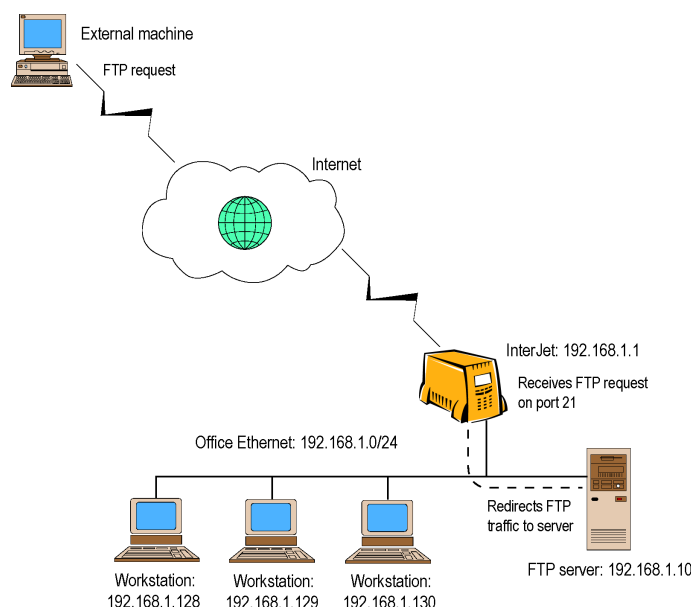
You can provide a public service—such as a Web or FTP server—on a machine that is on your private Office network. Normally, the InterJet firewall prevents access to all machines on your Office network. However, you can configure the InterJet firewall for *service redirection*—also called *port mapping*—which sends all requests from the outside world for a specific service to a machine that you specify. The firewall allows access to only the service that you specify for the machine. With the exception of this service, the firewall continues to protect the machine from all other types of access from outside your network.

Caution: Providing access to a machine on your private network creates a hole in the InterJet firewall. This hole may pose a security risk to your network. Configure the firewall only if you have expertise in networking and TCP/IP protocols.

Example: You have clients with whom you need to exchange files. You installed an FTP server on a machine on your network, and now you want to allow clients to log in to the server from their offices. To make FTP service available to your clients, you must perform the following tasks:

1. First provide the machine running the FTP server with a static, or fixed, IP address.
2. Next, configure the InterJet firewall to allow the machine to provide the service. To do so, you usually map a well-known service identifier—called a *port number*—to the machine's fixed IP address. For this example, you use the port number 21, which identifies FTP service.

Once you complete these tasks, the InterJet firewall redirects all outside requests for FTP service on your network to the machine that you specified. The following figure provides an example of service redirection for an FTP server.



Step 1: Assign a static IP address to the machine.

1. Configure the machine's TCP/IP settings so that it uses a static IP address. Refer to your client machine's operating system documentation for instructions on configuring the machine to use a static IP address.

2. Start your Web browser, then type `interjet` in the **Location** or **Address** box.

The InterJet home page appears, showing the System Agent View.

3. Point to the **Office Net** object.

The Office Network menu appears.

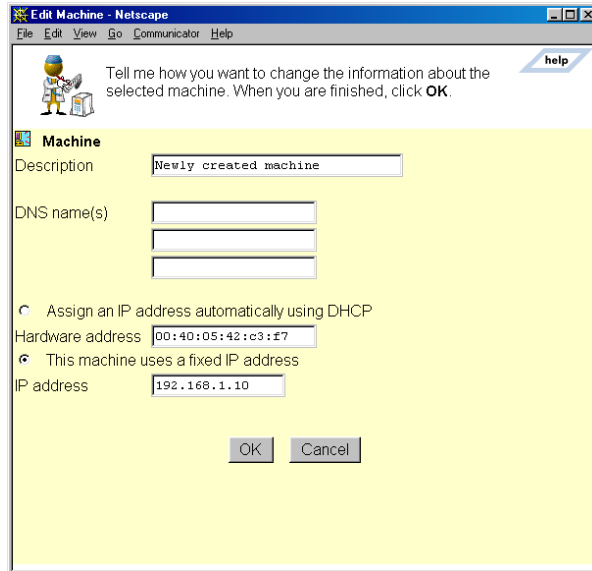
4. Click **Network/Machines List**.

The View Network/Machines page appears.

5. On the Network/Machines list, click the option button for the machine on which you want to provide a publicly accessible service—in this case, FTP. You can identify this machine by the IP address that you assigned to it.

6. Click **edit**.

The Edit Machine page appears.



7. Type a description for the machine in the **Description** box. For this example, type FTP server.
8. Type a name for the machine in the **DNS name** box.

This is the name by which your clients can refer to the machine. For this example, name the machine `ftpserver`. Once you finish configuring the firewall, your clients can type

ftp://ftpserver.your_domain_name to access the FTP server running on this machine—for example, ftp://ftpserver.whistle.com.

9. Select **This machine uses a fixed IP address**.
10. Click **OK**.

Step 2: Configure the InterJet firewall.

1. In the System Agent View, point to the **Firewall** object.

The Firewall Configuration menu appears.

2. Click **Firewall Holes**.

The Firewall Configuration page appears, showing a firewall configuration table. Each row of settings in the table represents a hole that you can create in the firewall.

Firewall Configuration - Netscape

I manage the firewall for your InterJet. Configure the entries to best suit your organization.

Firewall Configuration

Warning: This page allows you to open holes in the InterJet firewall so that traffic from external machines can reach specified machines on your internal network. An incorrect configuration can pose a security risk to your files or prevent InterJet services from functioning properly.

Use this page only if you are experienced in configuring firewalls.

Number	Allow protocol	On port(s) (TCP or UDP only)	For the external machines	To access the internal machine
1	(None)	N/A	☒ Range of IP addresses: to ☐ Perimeter network ☐ All	mceglia
2	(None)	N/A	☒ Range of IP addresses: to ☐ Perimeter network ☐ All	mceglia
3	(None)	N/A	☒ Range of IP addresses: to ☐ Perimeter network ☐ All	mceglia

OK Cancel

3. Specify the following information for the hole that you want to create in the firewall:

- ♦ **Allow protocol:** Specify the protocol that external machines use to establish a connection with an internal machine.

For this example, select **FTP**.

- ♦ **Port number:** For the TCP/UDP protocols, you must specify the port number that identifies the service or process that you want the internal machine to provide.

For this example, you do not need to specify a port number. Because you selected FTP, the InterJet automatically redirects incoming FTP requests to the well-known port for this

service, which is 21. For a list of some other well-known port numbers, see the table on page 4.

- ◆ **For the external machines:** If you want to specify the external machines that can access the internal machine through the firewall hole, you can type their range of IP addresses in the boxes. You can also allow only machines on your Perimeter network to access the internal machine.

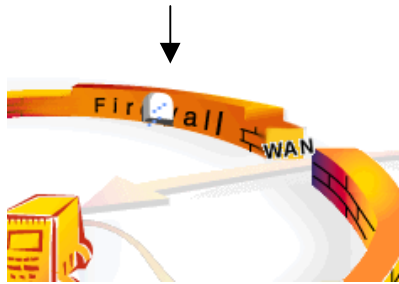
For this example, however, you do not want to limit incoming FTP requests to specific external machines. Therefore, select **All**.

- ◆ **To access the internal machine:** You must select the machine to which you want to provide access through the firewall. The drop-down list includes only those machines on your Office network for which you have provided a static IP address.

For this example, select the machine **ftpserver**.

4. Click **OK** to save your changes to the firewall configuration.

The Firewall object on the System Agent View animates to indicate that a hole is open, as shown in the following figure.



Well-Known Port Numbers for TCP/IP Services

DNS	53
FTP	21
HTTP	80
POP3	110
SMTP	25
Telnet	23

Note: For more information about port numbers, including well-known port numbers for other services, consult a TCP/IP reference text.