

Compatible Systems Tech Notes: FTP vs Filters and NAT

Document ID: 17664

- Introduction**
- Prerequisites**
 - Requirements
- Affected Products**
- Affected Versions**
- More Information**
- Related Information**

Introduction

This document addresses Normal mode and Passive mode FTP servers, Network Address Translation (NAT) and Filtering.

Prerequisites

Requirements

There are no specific requirements for this document.

Affected Products

900i, 1200i, 1220i, 1250i, 1270i, 2600i, 2900i, 2200R, 2220R, 2250R, 2270R, 3500R, 3800R, VSR-2, and VSR-8

Affected Versions

All versions

More Information

There are two types of FTP servers called Normal mode and Passive mode. Normal mode is the original implementation of FTP. A user initiates a connection from their side using a port > 1023 to reach the FTP server on port 21. The server responds to that users port and says it plans to send the data requested right back. Then the server starts a new connection from itself on port 20 back to the > 1023 port on the users end. Normal mode is considered "firewall UNfriendly" because it initiates its own connection with the user.

Passive mode FTP allows the user to initiate all connections. The user begins with a port > 1023 to the server's port 21 and the server lets the user know it is ready to go and gives the user a port > 1023 on the server for the user to call next. The user then initiates a new connection to that > 1023 port on the server that the server just said to use. In this method the user initiates all connections with the server and is considered "firewall friendly".

If you use a private internal network and use NAT to get out to the Internet, then you experience a problem when you access Normal Mode FTP servers on the Internet. Passive Mode FTP servers are firewall friendly and you should have no problems with them. If the FTP server is on your internal network, then you need to do some NAT Mapping in order to get it access. NAT Mapping is the answer to accessing Normal Mode FTP servers on the Internet also. You need to map an external address to every internal address that you wish to use Normal Mode FTP out to the Internet.

If you just have a filter, here are the lines you need to add to allow all types of FTP in and out:

```
#allow established internal connections, required for both FTP Modes
permit 0.0.0.0 0.0.0.0 tcp est
#allow internal access to internet Normal Mode FTP Servers
permit 0.0.0.0 0.0.0.0 tcp src = 20
#allow internet access to an internal FTP Server
permit 0.0.0.0 0.0.0.0 tcp dst = 21
permit 0.0.0.0 0.0.0.0 tcp src > 1023 dst > 1023
```

These should be applied as an input filter on your port closest to the Internet.

Related Information

- [Technical Support & Documentation – Cisco Systems](#)
-

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jun 19, 2007

Document ID: 17664
