Active and Passive FTP Overview and Configuration

File transfer protocol (FTP) is a popular application-layer protocol that is used for file transfers across TCP networks. FTP supports two modes: active and passive. These modes use different connection mechanisms, and each require different firewall configurations to allow access. This article discusses the differences between these modes and the necessary firewall configurations for Cisco Meraki MX Security Appliances.

Active FTP Overview

An active FTP session involves the following steps:

1. The client sends the PORT command to an FTP server. The source port is a random, high-numbered port. The destination port is 21.

2. The server responds with an ACK.

3. The server initiates a connection to the client with source port 20 and the destination port specified in the client’s PORT command.

4. The client sends an ACK to the server. The FTP session has now been established.

Note: Outbound active FTP is supported in MX Firmware version 12.25+ and 13.6+.

MX Configuration for Active FTP

Configuration for inbound active FTP behind an MX appliance is a simple process. Firewall rules must be constructed to allow inbound connections on port 21 and 20. Additional information about constructing firewall rules can be found here, and the following example below details a 1:1 NAT rule that allows inbound connections to an internal FTP server.
By default, MX appliances allow all outbound connections, so no additional firewall configuration is necessary. The following diagram outlines the flow of active FTP traffic, and where the MX comes into play:

**Passive FTP Overview**

Passive FTP is an FTP mode that can be requested by a client to alleviate the issues caused by client-side firewalls. Both the server and the client must support passive FTP for this process to work. When passive FTP is used, the client will initiate the connection to the server. This process is effective because most firewalls allow inbound traffic from sessions initiated by the client. A passive FTP connection follows the following process:

1. The client sends the PASV command to an FTP server on port 21. The source port is a random, high-numbered...
port. The destination port is 21.

2. The server responds with the PORT command. The port command specifies a random, high-numbered (ephemeral) port that the client can connect to.

3. The client initiates a connection to the server on this ephemeral port.

4. The server responds with an ACK. The FTP session has now been established.

Because the client initiates all connections, the client firewall will not block any traffic, as shown below:

---

**MX Configuration for Passive FTP**

Configuration for passive FTP on an MX appliance requires some additional knowledge of the FTP application. Firewall rules must be constructed to allow inbound connections on port 21 and inbound connections on the ephemeral ports used by the client when connecting to the FTP server using a passive connection. An ephemeral port is a temporary, non-registered port used for communication. Ephemeral ports are typically high numbered and outside the range of IANA registered ports.
The documentation about your particular FTP server software should contain information about the ephemeral ports used when passive FTP is requested by a client. For example, Microsoft IIS uses ports 1024 through 65535 by default. With a Microsoft IIS server in the default configuration, firewall rules must allow inbound connections on ports 21 and 1024 through 65535. This configuration will ensure that clients are able to make inbound connections on the passive FTP port provided by the server.

Two firewall rules are necessary for passive FTP to function properly:

- The firewall must allow connections on port 21.
- The firewall must allow connections to the ephemeral ports used by the FTP application.

Additional information about constructing firewall rules can be found here. The following diagram outlines the flow of active FTP traffic, and what additional traffic needs to be allowed by the MX:
Passive FTP Server Configuration Note

When configuring passive FTP, there is typically a field in your server side configuration that effectively tells the client “Use this IP address to connect for the data session.” By default, most FTP server applications will use the server IP for this field. When placed behind a stateful firewall like an MX Security Appliance, this will often be a private LAN address, and result in the client session attempting to connect to a nonexistent IP range to retrieve data.

When placed behind a firewall, this field must be changed to be the public IP that ports are being forwarded from, or the public IP in use for a 1:1 NAT address on the firewall.

Example of what this configuration looks like in FileZilla Server:
**Note:** Microsoft IIS version 6 and earlier do not have a configurable option for server IP, which may cause issues when configuring passive FTP behind any stateful firewall.

### Additional Resources

This article provided an overview of the mechanisms used by active and passive FTP. For a more detailed discussion of passive and active FTP, please consult [this documentation](http://example.com).