What types of FTP proxy does the WSA support?

Contents

Introduction

This document describes the three types of FTP proxy the Web Security Appliance (WSA) supports and provides examples of the access logs.

What types of FTP proxy does the WSA support?

Currently the Cisco WSA supports three methods of FTP proxy:

- FTP over HTTP
- FTP over HTTP Tunneling
- Native FTP

These methods use different techniques in order to communicate.

FTP over HTTP

This method is commonly used by web browsers, such as Internet Explorer, Firefox, and Opera. It is rather a unique technique where "Client -> WSA" communication is done purely in HTTP, and "WSA -> Internet" uses FTP in order to communicate. Once the WSA receives its response from the FTP server, the WSA determines whether the requested object is a directory or a file. If the object that is accessed is a directory, the WSA composes a directory listing written in HTML which is then forwarded to the client. If the requested object is a file, the WSA downloads the file and streams it to the client.

Here is an example of what you would see in the access log for FTP over HTTP.

```
1219138948.126 18058 192.168.10.100 TCP_MISS/200 1993 GET ftp://ftp.example.com/ -
DIRECT/ftp.example.com text/html DEFAULT_CASE-FTPACCESS <nc,ns,0,-,-,-,-,0,-,-,-,-,->
```

FTP over HTTP Tunneling

This method requires you to allow the majority of the ports under Web Security Manager > Access Policies > Protocols and User Agents > HTTP CONNECT Ports. Typically FTP servers should open ports between 49152 - 65535, but in a lot of cases they use ports 1024 - 65535. These ports are used when the FTP client issues the **PASV** command when it establishes it's data channel.

If everything goes well, you will see two entries in your access log:

```
1219137634.898 10707 192.168.10.100 TCP_MISS/0 160 CONNECT ftp.example.com:21/ -
DIRECT/ftp.example.com - DEFAULT_CASE-FTPACCESS <nc,ns,0,-,-,-,-,0,-,-,-,-,-> -
1219137698.512 287 192.168.10.100 TCP_MISS/0 240 CONNECT 192.168.10.10:57918/ -
DIRECT/192.168.10.10 text/plain DEFAULT_CASE-FTPACCESS <nc,ns,0,-,-,-,-,0,-,-,-,-,-> -
```

These logs show that both the control channel (first log line) and data channel (second log line) have successfully established.

Filezilla is one example of an application which supports this kind of transaction. In order to enable this feature on Filezilla, choose **Edit > Settings > Proxy Setting** and set the proxy type to HTTP 1.1. Enter other necessary details if needed.

In either of these two methods, Client - WSA only needs the proxy port to be open and WSA - Internet needs all outbound ports to be opened.

Native FTP

In this method the FTP client connects to the WSA on port 21 or port 8021, dependent upon whether the proxy has been implemented in transparent mode or explicit mode, respectively. Communication between the FTP client and the WSA is based purely on FTP. For native FTP the connection details can be viewed in the FTP Proxy logs. The actual file transfer and listing of directories can however still be viewed in the access log.

Here are a few examples of what you would see in the access log for Native FTP.

```
1340084525.556 2808 192.168.10.100 TCP_MISS/226 2790 RETR ftp://ftp.example.com/examplefile.txt
- DIRECT/ftp.example.com text/plain DEFAULT_CASE-FTPACCESS <nc,ns,0,-,-,-,-,0,-,-,-,-,-> -
1340084512.590 1013 192.168.10.100 TCP_MISS/230 27 FTP_CONNECT tunnel://ftp.example.com/ -
DIRECT/ftp.example.com - DEFAULT_CASE-FTPACCESS <nc,ns,0,-,-,-,-,0,-,-,-,-,-> -
1340084514.016 1426 192.168.10.100 TCP_MISS/226 413 MLSD ftp://ftp.example.com/ -
DIRECT/ftp.example.com text/plain DEFAULT_CASE-FTPACCESS <nc,ns,0,-,-,-,-,0,-,-,-,-,-> -
```