# Quali tipi di proxy FTP sono supportati da WSA?

## Sommario



## Introduzione

In questo documento vengono descritti i tre tipi di proxy FTP supportati da Web Security Appliance (WSA) e vengono forniti esempi di log degli accessi.

## Quali tipi di proxy FTP sono supportati da WSA?

Attualmente, Cisco WSA supporta tre metodi di proxy FTP:

- FTP su HTTP
- Tunneling FTP su HTTP
- FTP nativo

Questi metodi utilizzano diverse tecniche per comunicare.

### FTP su HTTP

Questo metodo viene comunemente utilizzato nei browser Web, ad esempio Internet Explorer, Firefox e Opera.  Si tratta di una tecnica unica, in cui la comunicazione "Client -> WSA" viene effettuata esclusivamente in HTTP e "WSA -> Internet" utilizza FTP per comunicare.  Dopo aver ricevuto la risposta dal server FTP, WSA determina se l'oggetto richiesto è una directory o un file. Se l'oggetto a cui si accede è una directory, WSA compone una directory scritta in HTML che viene quindi inoltrata al client.  Se l'oggetto richiesto è un file, WSA scarica il file e lo invia al client.

Di seguito è riportato un esempio di quanto verrebbe visualizzato nel log degli accessi per FTP su 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,-,-,-,->
```

### Tunneling FTP su HTTP

Questo metodo richiede di consentire la maggior parte delle porte in Web Security Manager > Criteri di accesso > Protocolli e agenti utente > Porte HTTP CONNECT. In genere, i server FTP devono aprire le porte comprese tra 49152 e 65535, ma in molti casi utilizzano le porte 1024 - 65535. Queste porte vengono utilizzate quando il client FTP esegue il comando **PASV** quando stabilisce il proprio canale dati.

Se tutto va bene, nel log degli accessi verranno visualizzate due voci:

```
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,-,-,-,-,- -,-> -
```

Questi log mostrano che sia il canale di controllo (prima riga di log) che il canale dati (seconda riga di log) sono stati stabiliti correttamente.

Filezilla è un esempio di applicazione che supporta questo tipo di transazione. Per abilitare questa funzione su Filezilla, scegliere **Modifica > Impostazioni > Impostazione proxy** e impostare il tipo di proxy su HTTP 1.1. Se necessario, immettere altri dettagli.

In entrambi i metodi, Client - WSA richiede solo che la porta proxy sia aperta e WSA - Internet richiede che tutte le porte in uscita siano aperte.

## FTP nativo

Con questo metodo il client FTP si connette al server WSA sulla porta 21 o sulla porta 8021, a seconda che il proxy sia stato implementato rispettivamente in modalità trasparente o in modalità esplicita. La comunicazione tra il client FTP e il WSA si basa esclusivamente su FTP. Per l'FTP nativo i dettagli di connessione possono essere visualizzati nei log del proxy FTP. Il trasferimento effettivo dei file e l'elenco delle directory possono comunque essere ancora visualizzati nel log degli accessi.

Di seguito sono riportati alcuni esempi di ciò che sarebbe visualizzato nel log degli accessi per 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,-,-,-,-> -
```