

ASA 8.3 and Later: Enable FTP/TFTP Services Configuration Example

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Network Diagram](#)

[Related Products](#)

[Conventions](#)

[Background Information](#)

[Advanced Protocol Handling](#)

[Configure Basic FTP Application Inspection](#)

[Example Configuration](#)

[Configure FTP Protocol Inspection on Non-Standard TCP Port](#)

[Configure Basic TFTP Application Inspection](#)

[Example Configuration](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

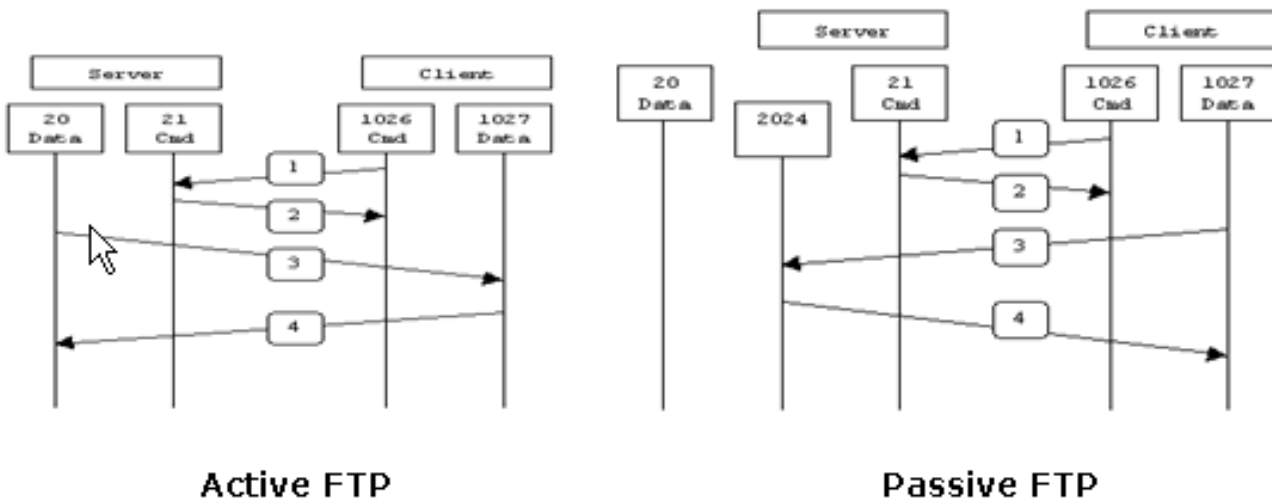
[Introduction](#)

This document explains the steps required for users outside of your network to access FTP and TFTP services in your DMZ network.

File Transfer Protocol (FTP)

There are two forms of FTP:

- Active mode
- Passive mode



Active FTP :

command : client >1023 -> server 21

data : client >1023 <- server 20

Passive FTP :

command : client >1023 -> server 21

data : client >1023 -> server >1023

In Active FTP mode, the client connects from a random unprivileged port ($N > 1023$) to the command port (21) of the FTP server. Then the client starts to listen to port $N+1$ and sends the FTP command port $N+1$ to the FTP server. The server then connects back to the specified data ports of the client from its local data port, which is port 20.

In Passive FTP mode, the client initiates both connections to the server, which solves the problem of a firewall that filters the incoming data port connection to the client from the server. When an FTP connection is opened, the client opens two random unprivileged ports locally ($N > 1023$ and $N+1$). The first port contacts the server on port 21. But instead of then issuing a **port** command and allowing the server to connect back to its data port, the client issues the **PASV** command. The result of this is that the server then opens a random unprivileged port ($P > 1023$) and sends the **port P** command back to the client. The client then initiates the connection from port $N+1$ to port P on the server to transfer data. Without the **inspection** command configuration on the Security Appliance, FTP from inside users headed outbound works only in Passive mode. Also, users outside headed inbound to your FTP server are denied access.

Refer to [PIX/ASA 7.x: Enable FTP/TFTP Services Configuration Example](#) for the same configuration on Cisco Adaptive Security Appliance (ASA) with versions 8.2 and earlier.

Trivial File Transfer Protocol (TFTP)

TFTP, as described in [RFC 1350](#), is a simple protocol to read and write files between a TFTP server and client. TFTP uses UDP port 69.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- There is basic communication between required interfaces.
- You have a configured the FTP server located in your DMZ network.

Components Used

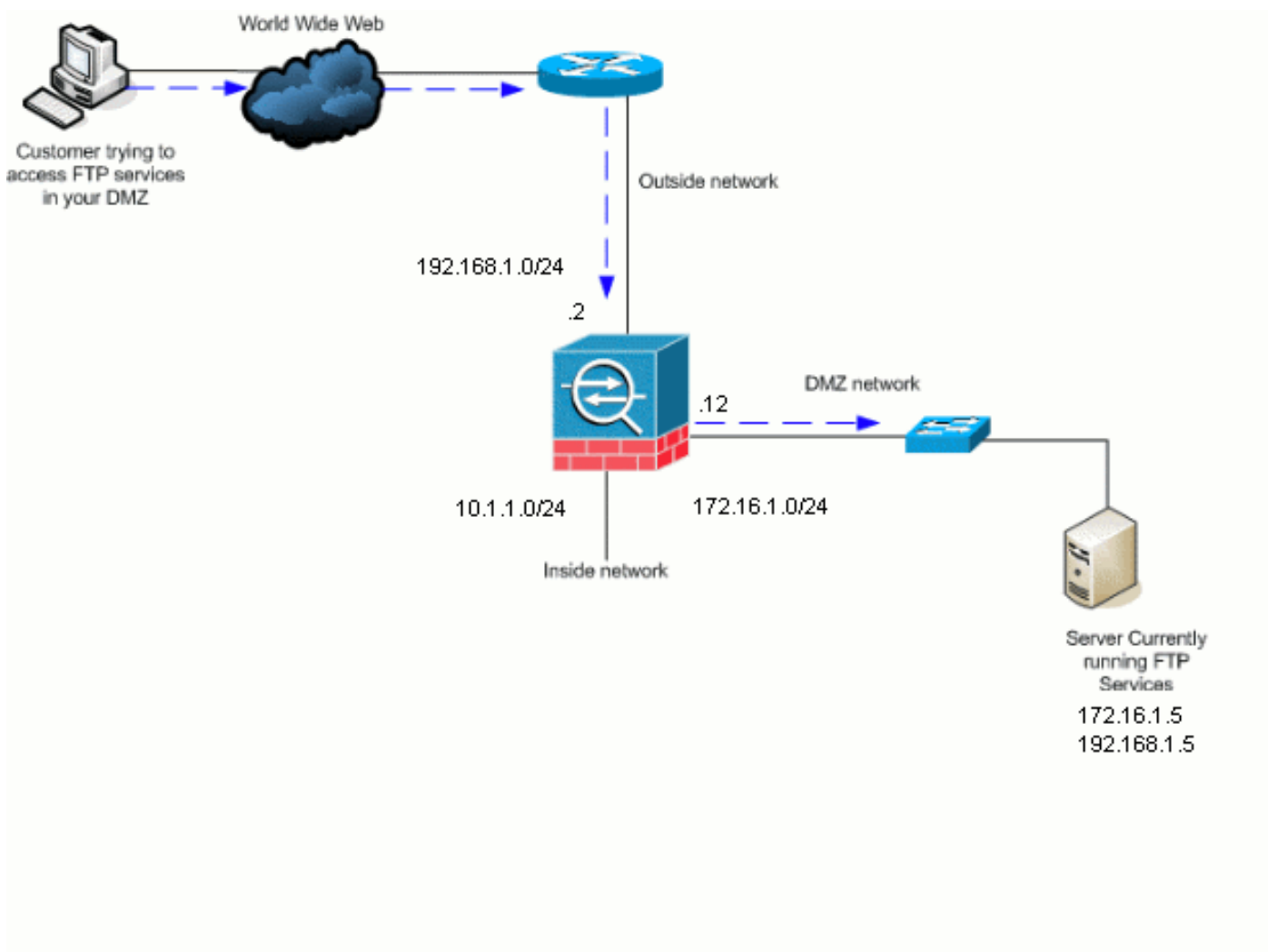
The information in this document is based on these software and hardware versions:

- ASA 5500 Series Adaptive Security Appliance that runs the 8.4(1) software image
- Windows 2003 Server that runs FTP services
- Windows 2003 Server that runs TFTP services
- Client PC located on the outside of the network

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Network Diagram

This document uses this network setup:



Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which have been used in a lab environment.

[Related Products](#)

This configuration can also be used with Cisco Adaptive Security Appliance 8.3 and later.

[Conventions](#)

Refer to the [Cisco Technical Tips Conventions](#) for more information on document conventions.

[Background Information](#)

The Security Appliance supports application inspection through the Adaptive Security Algorithm function. Through the stateful application inspection used by the Adaptive Security Algorithm, the Security Appliance tracks each connection that traverses the firewall and ensures that they are valid. The firewall, through stateful inspection, also monitors the state of the connection to compile information to place in a state table. With the use of the state table in addition to administrator-defined rules, filtering decisions are based on context that is established by packets previously passed through the firewall. The implementation of application inspections consists of these actions:

- Identify the traffic.
- Apply inspections to the traffic.
- Activate inspections on an interface.

[Advanced Protocol Handling](#)

[FTP](#)

Some applications require special handling by the Cisco Security Appliance application inspections function. These types of applications typically embed IP addressing information in the user data packet or open secondary channels on dynamically assigned ports. The application inspection function works with Network Address Translation (NAT) to help identify the location of embedded addressing information.

In addition to the identification of embedded addressing information, the application inspection function monitors sessions to determine the port numbers for secondary channels. Many protocols open secondary TCP or UDP ports to improve performance. The initial session on a well-known port is used to negotiate dynamically assigned port numbers. The application inspection function monitors these sessions, identifies the dynamic port assignments and permits data exchange on these ports for the duration of the specific sessions. Multimedia and FTP applications exhibit this kind of behavior.

The FTP protocol requires some special handling due to its use of two ports per FTP session. The FTP protocol uses two ports when activated for transferring data: a control channel and a data channel that uses port 21 and 20, respectively. The user, who initiates the FTP session over the control channel, makes all data requests through that channel. The FTP server then initiates a request to open a port from server port 20 to the user's computer. FTP always uses port 20 for data channel communications. If FTP inspection has not been enabled on the Security Appliance, this request is discarded and the FTP sessions do not transmit any requested data. If FTP inspection is enabled on the Security Appliance, the Security Appliance monitors the control channel and tries to recognize a request to open the data channel. The FTP protocol embeds the

data-channel port specifications in the control channel traffic, requiring the Security Appliance to inspect the control channel for data-port changes. If the Security Appliance recognizes a request, it temporarily creates an opening for the data-channel traffic that lasts for the life of the session. In this way, the FTP inspection function monitors the control channel, identifies a data-port assignment, and allows data to be exchanged on the data port for the length of the session.

The Security Appliance inspects port 21 connections for FTP traffic by default through the global-inspection class-map. The Security Appliance also recognizes the difference between an active and a passive FTP session. If the FTP sessions support passive FTP data transfer, the Security Appliance, through the **inspect ftp** command, recognizes the data port request from the user and opens a new data port greater than 1023.

The FTP application inspection inspects FTP sessions and performs four tasks:

- Prepares a dynamic secondary data connection
- Tracks the FTP command-response sequence
- Generates an audit trail
- Translates the embedded IP address using NAT

FTP application inspection prepares secondary channels for FTP data transfer. The channels are allocated in response to a file upload, a file download, or a directory listing event, and they must be pre-negotiated. The port is negotiated through the **PORT** or **PASV** (227) commands.

TFTP

TFTP inspection is enabled by default.

The security appliance inspects TFTP traffic and dynamically creates connections and translations, if necessary, to permit file transfer between a TFTP client and server. Specifically, the inspection engine inspects TFTP read requests (RRQ), write requests (WRQ), and error notifications (ERROR).

A dynamic secondary channel and a PAT translation, if necessary, are allocated on a reception of a valid RRQ or WRQ. This secondary channel is subsequently used by TFTP for file transfer or error notification.

Only the TFTP server can initiate traffic over the secondary channel, and at most one incomplete secondary channel can exist between the TFTP client and server. An error notification from the server closes the secondary channel.

TFTP inspection must be enabled if static PAT is used to redirect TFTP traffic.

Configure Basic FTP Application Inspection

By default, the configuration includes a policy that matches all default application inspection traffic and applies inspection to the traffic on all interfaces (a global policy). Default application inspection traffic includes traffic to the default ports for each protocol. You can only apply one global policy, so if you want to alter the global policy, for example, to apply inspection to non-standard ports, or to add inspections that are not enabled by default, you need to either edit the default policy or disable it and apply a new one. For a list of all default ports, refer to the [Default Inspection Policy](#).

1. Issue the **policy-map global_policy** command.`ASA(config)#policy-map global_policy`

2. Issue the [class inspection default](#) command. `ASA(config-pmap)#class inspection_default`
3. Issue the [inspect FTP](#) command. `ASA(config-pmap-c)#inspect ftp` There is an option to use the [inspect FTP strict](#) command. This command increases the security of protected networks by preventing a web browser from sending embedded commands in FTP requests. After you enable the *strict* option on an interface, FTP inspection enforces this behavior: An FTP command must be acknowledged before the Security Appliance allows a new command. The Security Appliance drops a connection that sends embedded commands. The **227** and **PORT** commands are checked to ensure they do not appear in an



error string. **Warning:** The use of the *strict* option might cause the failure of FTP clients that are not strictly compliant with FTP RFCs. Refer to [Using the strict Option](#) for more information on the use of the *strict* option.

[Example Configuration](#)

```

Device Name 1
ASA(config)#show running-config ASA Version 8.4(1) !
hostname ASA domain-name corp.com enable password
WwXYvtKrnjXqGbu1 encrypted names ! interface Ethernet0/0
nameif Outside security-level 0 ip address 192.168.1.2
255.255.255.0 ! interface Ethernet0/1 nameif Inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/2 nameif DMZ security-level 50 ip
address 172.16.1.12 255.255.255.0 ! interface
Ethernet0/3 no nameif no security-level no ip address !
interface Management0/0 no nameif no security-level no
ip address ! !--- Output is suppressed. !--- Permit
inbound FTP control traffic. access-list 100 extended
permit tcp any host 192.168.1.5 eq ftp !--- Permit
inbound FTP data traffic. access-list 100 extended
permit tcp any host 192.168.1.5 eq ftp-data ! !---
Object groups are created to define the hosts. object
network DMZ host 172.16.1.5 object network DMZ-out host
192.168.1.5 !--- Configure manual NAT nat (DMZ,outside)
source static DMZ DMZ-out access-group 100 in interface
outside class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! !---
This command tells the device to !--- use the
"global_policy" policy-map on all interfaces. service-
policy global_policy global prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009 : end
ASA(config)#

```

[Configure FTP Protocol Inspection on Non-Standard TCP Port](#)

You can configure the FTP Protocol Inspection for non-standard TCP ports with these configuration lines (replace XXXX with the new port number):

```

access-list ftp-list extended permit tcp any any eq XXXX
!
class-map ftp-class
  match access-list ftp-list
!
policy-map global_policy
  class ftp-class
    inspect ftp

```

Configure Basic TFTP Application Inspection

By default, the configuration includes a policy that matches all default application inspection traffic and applies inspection to the traffic on all interfaces (a global policy). Default application inspection traffic includes traffic to the default ports for each protocol. You can only apply one global policy. So if you want to alter the global policy, for example, to apply inspection to non-standard ports, or to add inspections that are not enabled by default, you need to either edit the default policy or disable it and apply a new one. For a list of all default ports, refer to the [Default Inspection Policy](#).

1. Issue the [policy-map global_policy](#) command. `ASA(config)#policy-map global_policy`
2. Issue the [class inspection default](#) command. `ASA(config-pmap)#class inspection_default`
3. Issue the [inspect TFTP](#) command. `ASA(config-pmap-c)#inspect TFTP`

Example Configuration

Device Name 1

```

ASA(config)#show running-config ASA Version 8.4(1) !
hostname ASA domain-name corp.com enable password
WwXYvtKrnjXqGbul encrypted names ! interface Ethernet0/0
nameif Outside security-level 0 ip address 192.168.1.2
255.255.255.0 ! interface Ethernet0/1 nameif Inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/2 nameif DMZ security-level 50 ip
address 172.16.1.12 255.255.255.0 ! interface
Ethernet0/3 no nameif no security-level no ip address !
interface Management0/0 no nameif no security-level no
ip address ! !--- Output is suppressed. !--- Permit
inbound TFTP traffic. access-list 100 extended permit
udp any host 192.168.1.5 eq tftp ! !--- Object groups
are created to define the hosts. object network DMZ host
172.16.1.5 object network DMZ-out host 192.168.1.5 !---
Configure manual NAT nat (DMZ,outside) source static DMZ
DMZ-out access-group 100 in interface outside class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtip inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! !--- This command tells the device
to !--- use the "global_policy" policy-map on all
interfaces. service-policy global_policy global prompt
hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009 : end
ASA(config)#

```

Verify


In order to ensure the configuration has successfully taken, use the **show service-policy** command. Also, limit the output to the FTP inspection only using the [show service-policy inspect ftp](#) command.

```
ASA#show service-policy inspect ftp Global Policy: Service-policy: global_policy  
Class-map: inspection_default Inspect: ftp, packet 0, drop 0, reste-drop 0 ASA#
```

Troubleshoot

There is currently no specific troubleshooting information available for this configuration

Related Information

- [Cisco Adaptive Security Device Manager](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Requests for Comments \(RFCs\)](#) 
- [Technical Support & Documentation - Cisco Systems](#)