

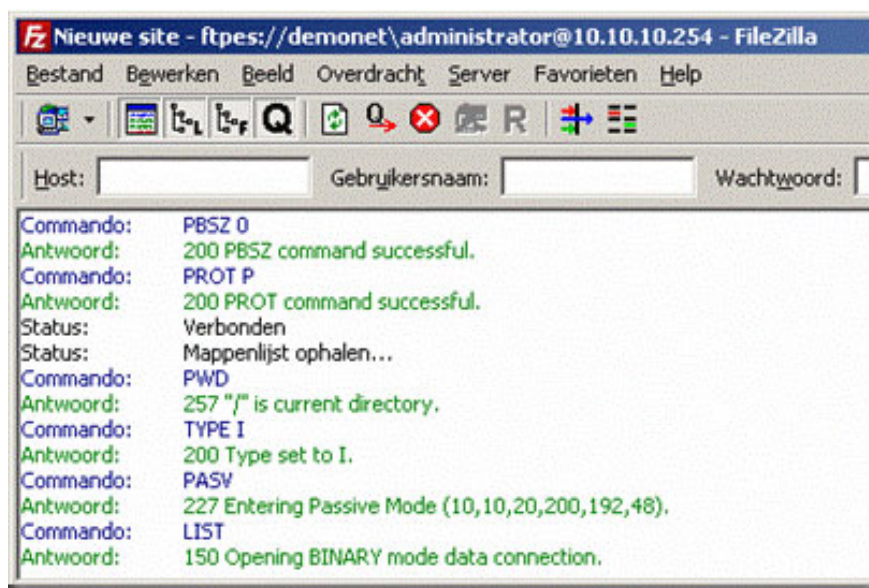
FTP security with Firewall ISA 2006 (Part 2)

In the previous section we explored the issue with the FTP server using the ISA 2006 firewall system.

In the previous section, we explored the issue with the FTP server using the ISA 2006 firewall system. When using a network adapter, we can confirm that TLS (Transport Layer Security) from the workstation rejected by the ISA firewall system.

The ISA firewall has an application layer filter that supports FTP connections, but this filter cannot be configured (unlike an SMTP filter). Because the built-in FTP application layer filter on ISA firewall does not support TLS, users need to disable this filter for all rules or certain rules. It is best to disable it on certain rules so that SecureNAT workstations can use the FTP protocol for external access. After turning off the FTP application filter, the FTP connection on the FTP server is secured by the ISA firewall system. However, users need to take an extra step when securing the FTP connection, which is secure data transfer via FTP channel. This section will delve into the method of data transfer via secure FTP links.

After authenticating the FTP server, we need to list the directories and transfer files. This operation is performed via the secondary data channel.



As you can see above, the authentication process is still in progress, but the system still hangs 150 connections to the Opening Binary mode data, and if it continues to wait we will receive a Time out message.

1	0.000000	10.10.10.100	10.10.10.254	TCP	1161 > ftp [SYN] Seq=0 Len=0 MSS=1460
2	0.003978	10.10.10.254	10.10.10.100	TCP	ftp > 1161 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
3	0.004057	10.10.10.100	10.10.10.254	TCP	1161 > ftp [ACK] Seq=1 Ack=1 Win=65535 Len=0
4	0.006226	10.10.10.254	10.10.10.100	FTP	Response: 220 Microsoft FTP Service
5	0.008081	10.10.10.100	10.10.10.254	FTP	Request: AUTH TLS
6	0.008950	10.10.10.254	10.10.10.100	FTP	Response: 234 AUTH command ok. Expecting TLS N
7	0.015181	10.10.10.100	10.10.10.254	FTP	Request: \026\003\002\0000\001\000\000k\003\0
8	0.016377	10.10.10.254	10.10.10.100	FTP	Response: \026\003\001\0000\002\000\000F\003\0
9	0.019925	10.10.10.100	10.10.10.254	FTP	Request: \026\003\001\0000\206\020\000\000\202\
10	0.215226	10.10.10.254	10.10.10.100	TCP	ftp > 1161 [ACK] Seq=658 Ack=234 Win=64007 Len=0
11	0.215283	10.10.10.100	10.10.10.254	FTP	Request: \024\003\001\0000\001\001\026\003\001\
12	0.216334	10.10.10.254	10.10.10.100	FTP	Response: \024\003\001\0000\001\001\026\003\001\
13	0.219289	10.10.10.100	10.10.10.254	FTP	Request: \027\003\001\0000\340\332\215nL2\2370\
14	0.220224	10.10.10.254	10.10.10.100	FTP	Response: \027\003\001\000P\277\325P\001\220\
15	0.223986	10.10.10.100	10.10.10.254	FTP	Request: \027\003\001\0000\320\333\205\005=\347
16	0.227943	10.10.10.254	10.10.10.100	FTP	Response: \027\003\001\0000\366\233\332\377e16
17	0.228412	10.10.10.100	10.10.10.254	FTP	Request: \027\003\001\0000\240\036\017r3y2\22
18	0.231986	10.10.10.254	10.10.10.100	FTP	Response: \027\003\001\000P\301\246\204\213\03
19	0.232491	10.10.10.100	10.10.10.254	FTP	Request: \027\003\001\0000 o{\304\274
20	0.235743	10.10.10.254	10.10.10.100	FTP	Response: \027\003\001\0000\242\306\2449\350>
21	0.236187	10.10.10.100	10.10.10.254	FTP	Request: \027\003\001\0000\220\212\271\ao\004h4
22	0.238942	10.10.10.254	10.10.10.100	FTP	Response: \027\003\001\0000LA\F\204\236b\346\3
23	0.243065	10.10.10.100	10.10.10.254	FTP	Request: \027\003\001\0000\260\1255\226u\253\3
24	0.246364	10.10.10.254	10.10.10.100	FTP	Response: \027\003\001\0000\241\315\327\304\24
25	0.246976	10.10.10.100	10.10.10.254	FTP	Request: \027\003\001\0000\320\31\332\000A\353\A
26	0.249689	10.10.10.254	10.10.10.100	FTP	Response: \027\003\001\0000\320x\377\037\036G\
27	0.250212	10.10.10.100	10.10.10.254	FTP	Request: \027\003\001\0000\220yx\363\361\207+2
28	0.253164	10.10.10.254	10.10.10.100	FTP	Response: \027\003\001\000Pq
29	0.257210	10.10.10.100	10.10.10.254	FTP	Request: \027\003\001\000p\3155>\272\236\265I\
30	0.260000	10.10.10.100	10.10.10.200	TCP	1162 > 49198 [SYN] Seq=0 Len=0 MSS=1460 Win=0
31	0.261274	10.10.10.254	10.10.10.100	FTP	Response: \027\003\001\0000r2\273\3437\370\3
32	0.445111	10.10.10.100	10.10.10.254	TCP	1161 > ftp [ACK] Seq=1762 Ack=134 Win=64182 Len=0
33	1.179254	10.10.10.100	10.10.20.200	TCP	1162 > 49198 [SYN] Seq=0 Len=0 MSS=1460 Win=2
34	8.763370	10.10.10.254	10.10.10.100	FTP	Response: \027\003\001\0000\002\2122/\336\230

As mentioned in the previous section, we can check TCP in the 3 packets containing connection information, then the FTP authentication process will start, and at the bottom of the monitoring window you will see some packets saved. Store connection information via data channel.

# Frame 30 (66 bytes on wire, 66 bytes captured)				
# Ethernet II, Src: Vmware_c7:bf:ee (00:0c:29:c7:bf:ee), Dst: vmware_2f:5d:83 (00:0c:29:2f:5d:83)				
# Internet Protocol, Src: 10.10.10.100 (10.10.10.100), Dst: 10.10.20.200 (10.10.20.200)				
# Transmission Control Protocol, Src Port: 1162 (1162), Dst Port: 49198 (49198), Seq: 0, Len: 0				

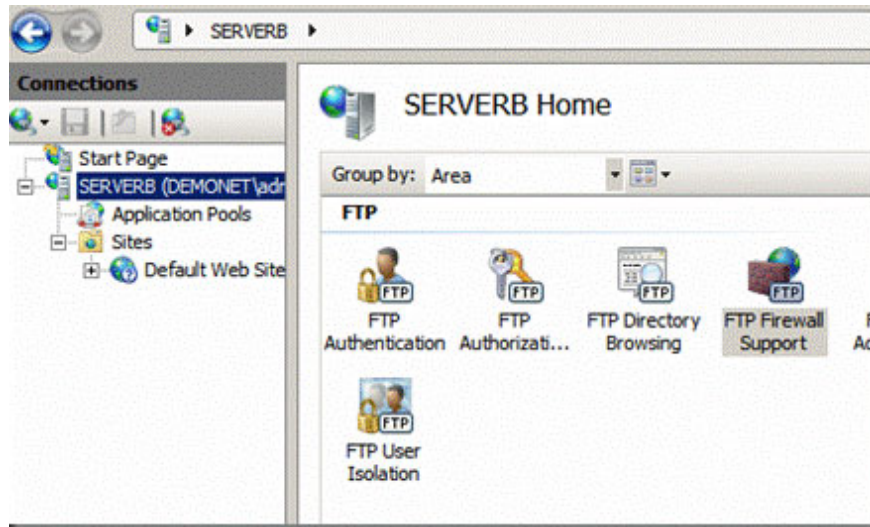
FTP data channel is the second TCP connection connection channel. During authentication, the FTP server sends the FTP client information about the secondary dynamic connection port that needs to be opened. After that, this workstation opens a port on this secondary port and establishes a data connection. Remember that this secondary port is a random high dynamic port. Before Windows Vista was released, high ports could be selected in the range of 1024 to 5000. But when Windows Vista was released, Microsoft changed the random port selection, which is why you see the port. Randomly here is set to 49198 TCP. Windows Vista and Windows Server 2008 use dynamic port ranges from 49152 to 65535.

By default, the application layer filter of the ISA firewall system will monitor this random port (used for secondary connections by open ports, dynamically when the client connects to the FTP server). However, since we need to turn off this application filter to execute the Auth TLS command, we will replace the FTP application filter on the ISA firewall system with another filter.

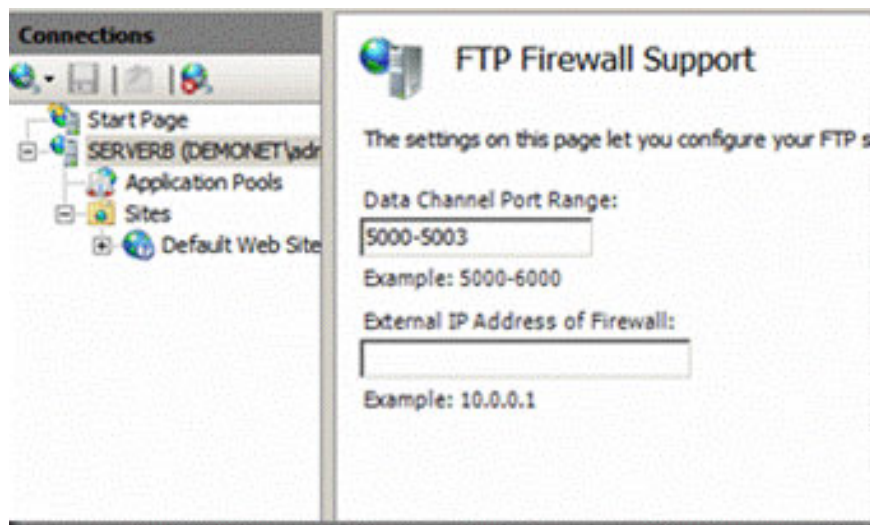
Step 1

First you need to apply the FTP server method to assign random ports to remove unnecessary ports and control which ports are being used. Then, you also need to tell the FTP server which public IP address belongs to the ISA firewall system.

Do this in the IIS configuration window. To install for static ports you have to do it on the server (not on the website level). In this window, double-click the **FTP Firewall Support** icon.

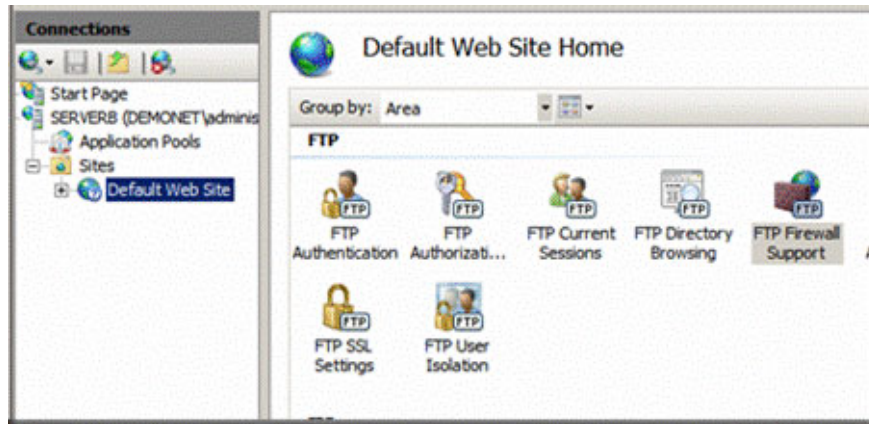


In the **FTP Firewall Support** window, you can enter any port area. For example enter the area **5000-5003** and then click **Apply** .

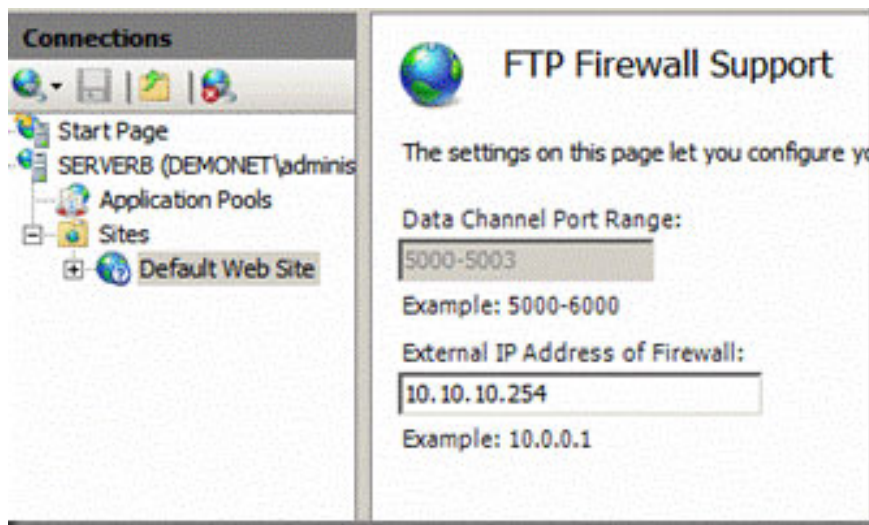


Step 2

Then we must install the IP address on the website level. Expand the **Sites** section and then click **Default Web Site** . Next click on the **FTP Firewall Support** icon.



Enter the newly used public IP address name in the **FTP Server Publishing Rule** of the ISA firewall system, then click **Apply** .



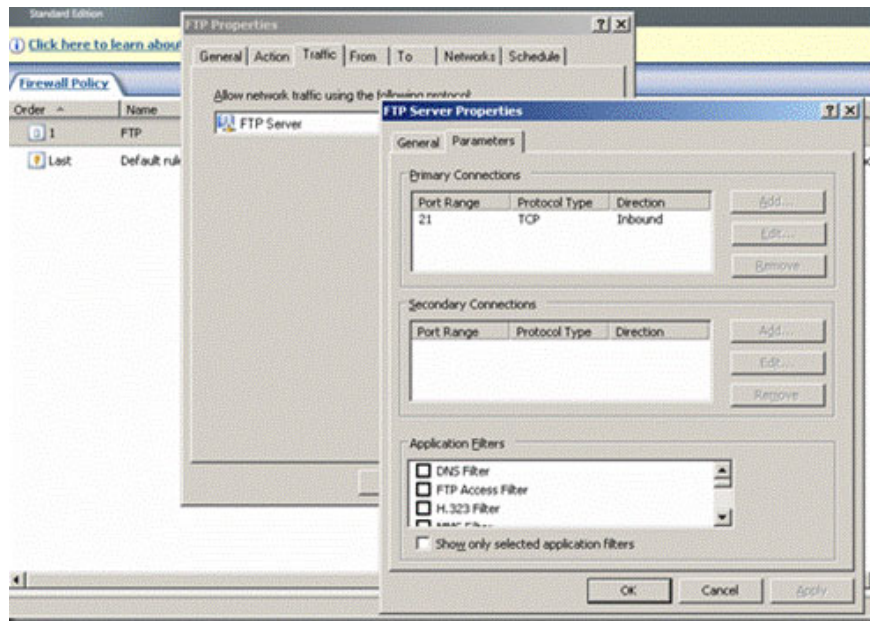
Note: When you click the **Apply** button, the settings you just installed do not apply, relaunch the **Microsoft FTP Service** from the **Service Management Console** .

Link-Layer Topology Discovery Mapper	Creates a ...	Manual	Local Service
Microsoft .NET Framework NGEN v2.0.50727_X86	Microsoft ...	Manual	Local System
Microsoft Fibre Channel Platform Registration Service	Registers t...	Manual	Local Service
Microsoft FTP Service	Enables th...	Started	Automatic
Microsoft iSCSI Initiator Service	Manages I...	Manual	Local System
Microsoft Software Shadow Copy Provider	Manages s...	Manual	Local System
Multimedia Class Scheduler	Enables rel...	Manual	Local System

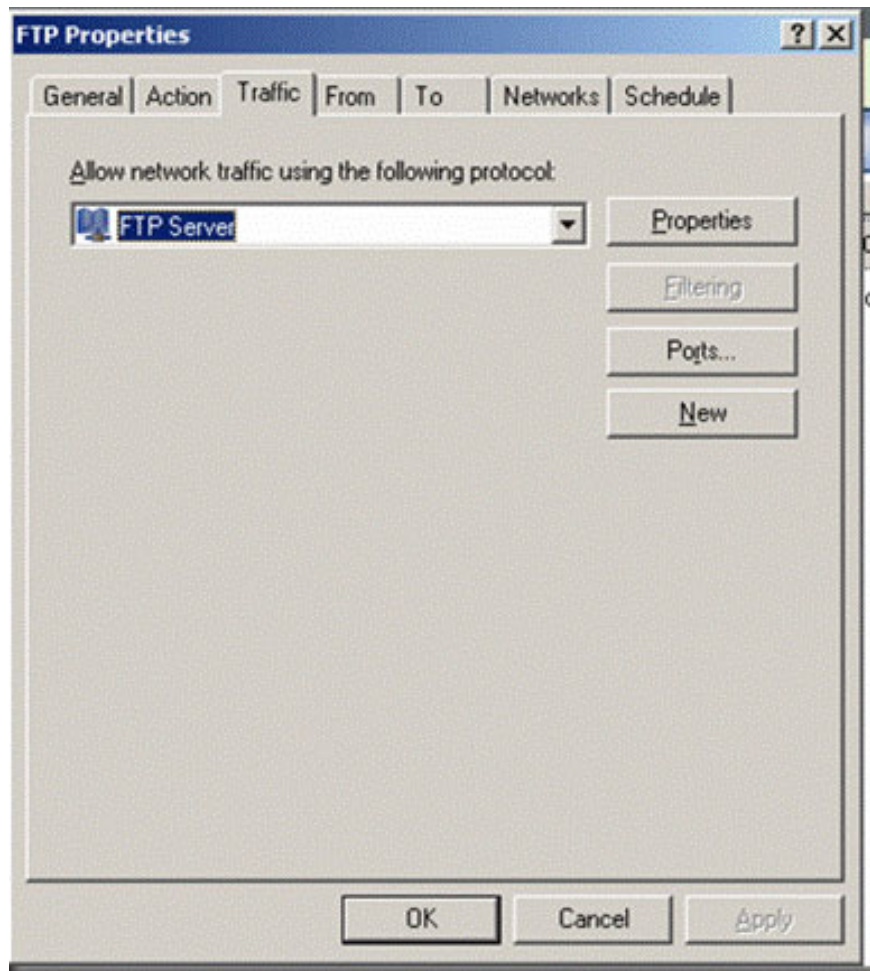
Step 3

The last action to be taken is to configure the **FTP Server Publishing Rule** on the ISA firewall system. Here we

will add the port area that functions as the main connection port. When editing the **FTP Server Publishing Rule**, you will not be able to edit the **Parameters**. That's because the default protocol definition and Microsoft do not allow users to change these definitions.



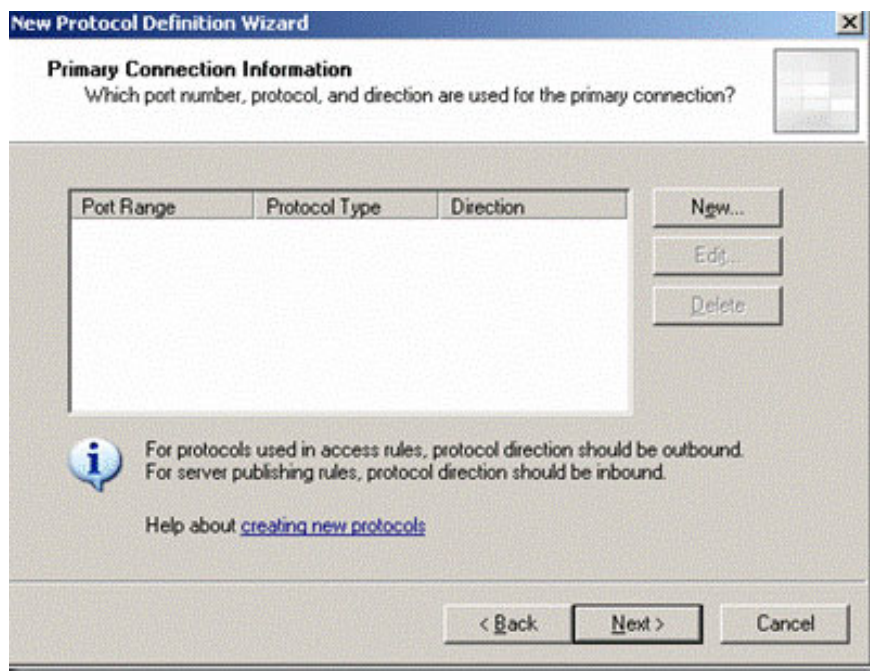
To solve this problem, we will create a separate **Protocol Definition** for **FTPS** server. Please select the **Traffic** tab and then click **New**.



Enter a name for **Protocol Definition** on the **Welcome to the New Protocol Definition Wizard** page . Suppose you enter the name **FTPS** (you can enter a custom name). Then click the **Next** button.



Next, click the **New** button on the **Primary Connection Information** page.



In the **New / Edit Protocol Connection** dialog box, select **TCP** for the **Protocol** type. Select **Direction** as **Inbound** value , and set the **Port Range** area to **21** and **To From to 21** values. Done, click **OK** .

New/Edit Protocol Connection

Protocol type: TCP Protocol Number: 6

Direction: Inbound

Port Range
From: 21 To: 21

ICMP Properties
ICMP Code: ICMP Type:

OK Cancel

Click the **New** button again on the **Primary Connection Information** page. Set the **Protocol** type to **TCP** . Select **Inbound** for **Direction** and set the value for the **From** to **5000** and **To** fields to **5003** in the **Port Range** area.

New/Edit Protocol Connection

Protocol type: TCP Protocol Number: 6

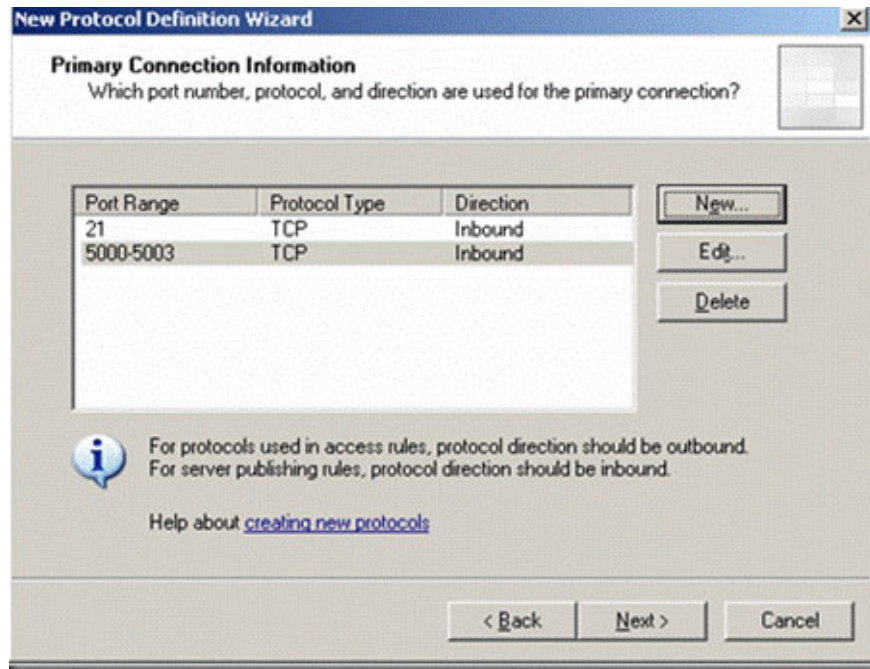
Direction: Inbound

Port Range
From: 5000 To: 5003

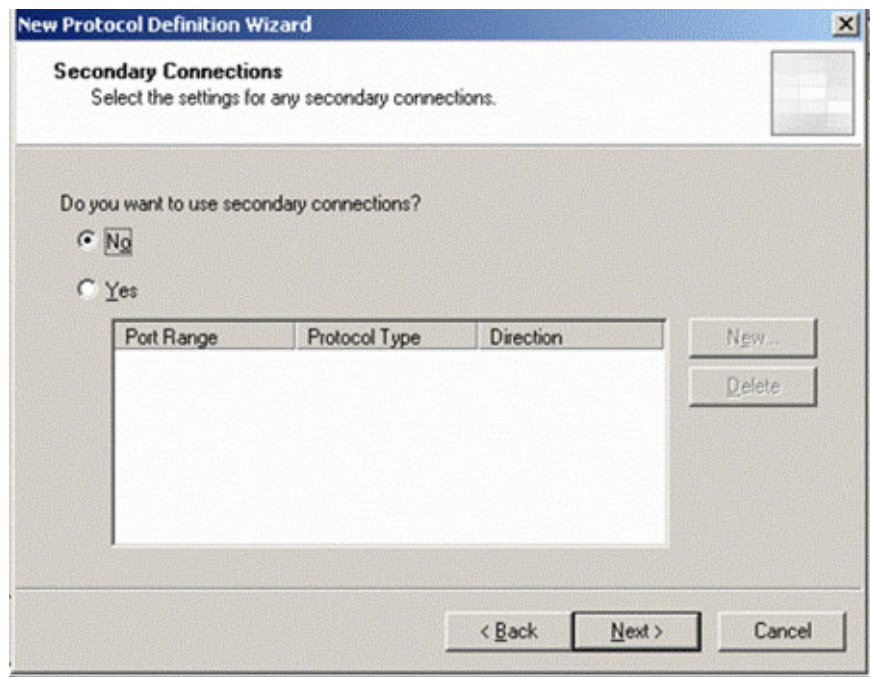
ICMP Properties
ICMP Code: ICMP Type:

OK Cancel

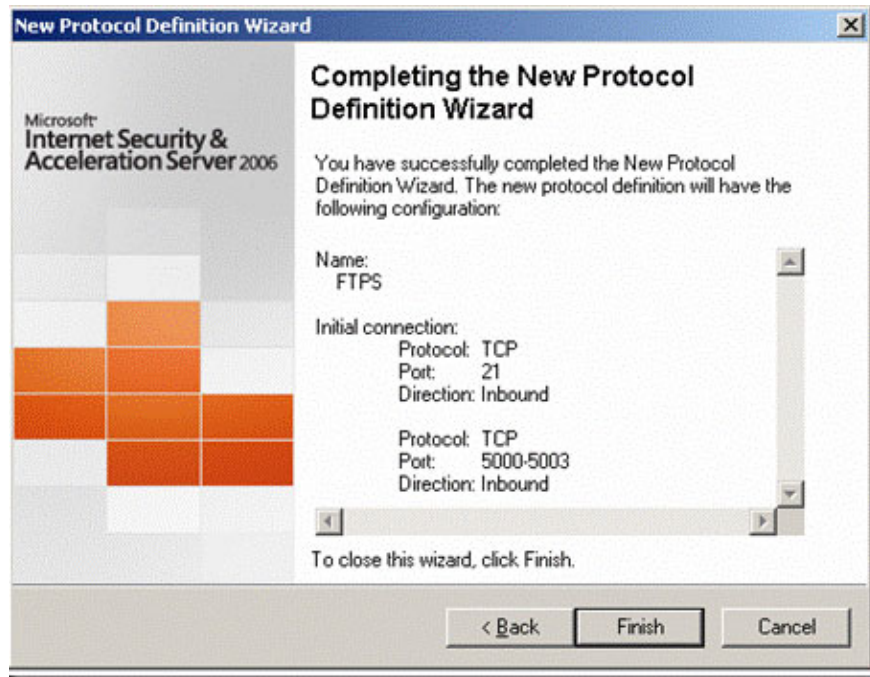
You will then see the new primary connection on the **Primary Connection Information** page. Click **Next** .



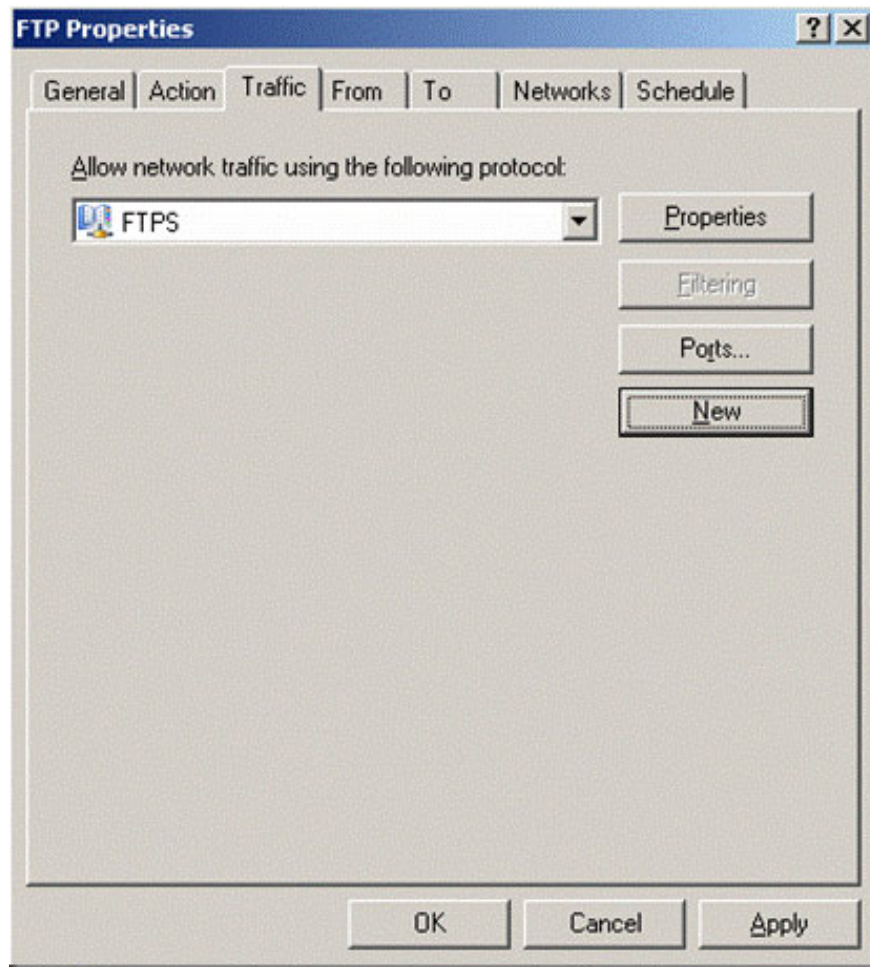
On the **Secondary Connections** page select the radio **No** option and click **Next** .



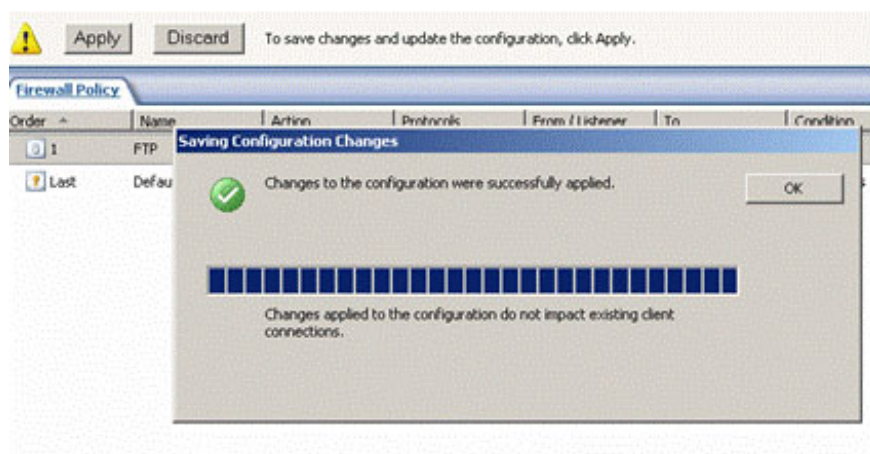
Click the **Finish** button on the **Completing the New Protocol Definition Wizard** page .



On the **Traffic** tab, you will see two **Protocol Definition** displayed in the **Allow network traffic using the following protocol** drop-down list (allowing network traffic to use the following protocol).

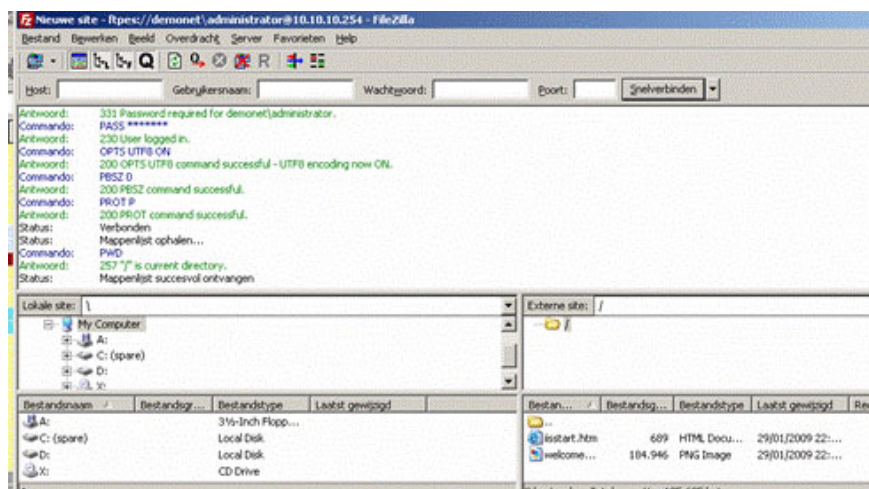


Click **Apply** to save the changes and update the firewall settings. Then click **OK** in the **Saving Configuration Changes** dialog box.



Step 4

Return to the **FTP** workstation and make the connection again. You will then see that the connection was successful.



Conclude

When securing the FTP server, we can establish a connection to authenticate the FTP server using the default FTP Protocol Definition. However, we cannot establish data connection. To support data connectivity, we must first change the FTPS server configuration to limit the high port used to make the connection. In addition, we must also configure the IP address for the FTP server on the external interface of the ISA firewall system that applies to the FTPS Server Publishing Rule. After implementing FTPS server configuration, we changed the FTPS Server Publishing Rule so it will use a new FTP Protocol Protocol Definition. Then the FTPS client was able to connect to the FTPS server.

You finished reading the article "**FTP security with Firewall ISA 2006 (Part 2)**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.