
UTM: How to Open FTPS traffic to a Passive mode FTP Server behind the SonicWALL (SW10094)

Title

UTM: How to Open FTPS traffic to a Passive mode FTP Server behind the SonicWALL

Resolution

Article Applies To:

Gen6: NSA E10800, NSA E10400, NSA E10200, NSA E10100

Gen5: NSA E8510, E8500, NSA E7500, NSA E6500, NSA E5500, NSA 5000, NSA 4500, NSA 3500, NSA 2400, NSA 2400 MX, NSA 240, NSA 220, NSA 220 /W. NSA 250M, NSA 250M /W.

Gen5 TZ Series: TZ 100, TZ 100 Wireless, TZ 200, TZ 200 W, TZ 210, TZ 210 W, TZ 215, TZ 215 W. TZ 105, TZ 105 W, TZ 205, TZ 205 W

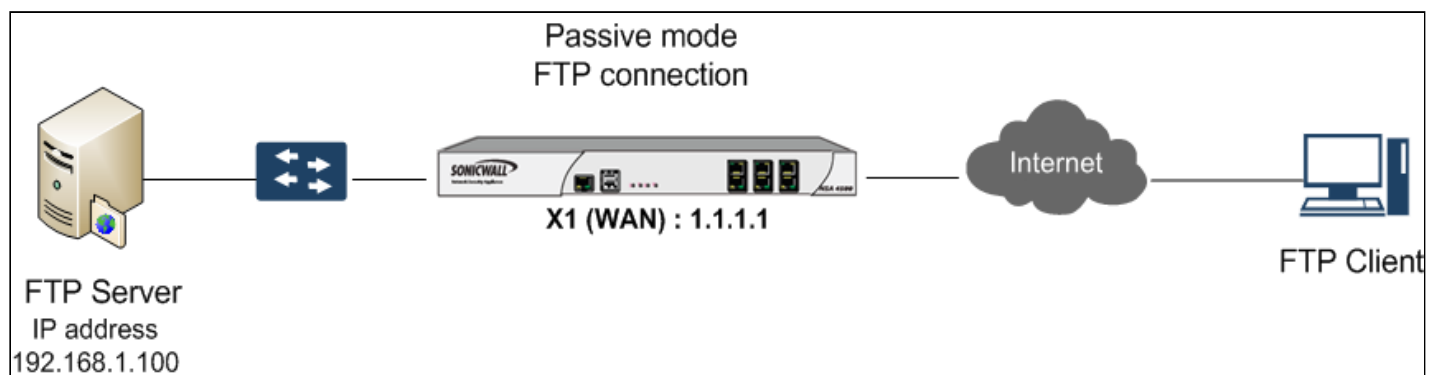
Gen4: PRO series: PRO 5060, PRO 4100, PRO 4060, PRO 3060, PRO 2040, PRO 1260.

Gen4: TZ series: TZ 190, TZ 190 W, TZ 180, TZ 180 W, TZ 170, TZ 170 W, TZ 170 SP, TZ 170 SP Wireless

Firmware/Software Version: All SonicOS Enhanced versions.

Services: Firewall Access Rules, NAT Policies

Feature/Application:



[Click To See Full Image.](#)

In FTPS (FTP over SSL/TLS) connections, SonicWALL will be unable to scan the PORT or PASSV commands to determine the Data ports used. In such cases we must configure the server to listen on a fixed range of Data ports and open the ports in the SonicWALL. Unlike FTP, in FTPS we must also ensure that the external IP is defined in the FTP server Passive mode settings.

This article describes the configuration required in the SonicWALL to allow a FTP client on the WAN

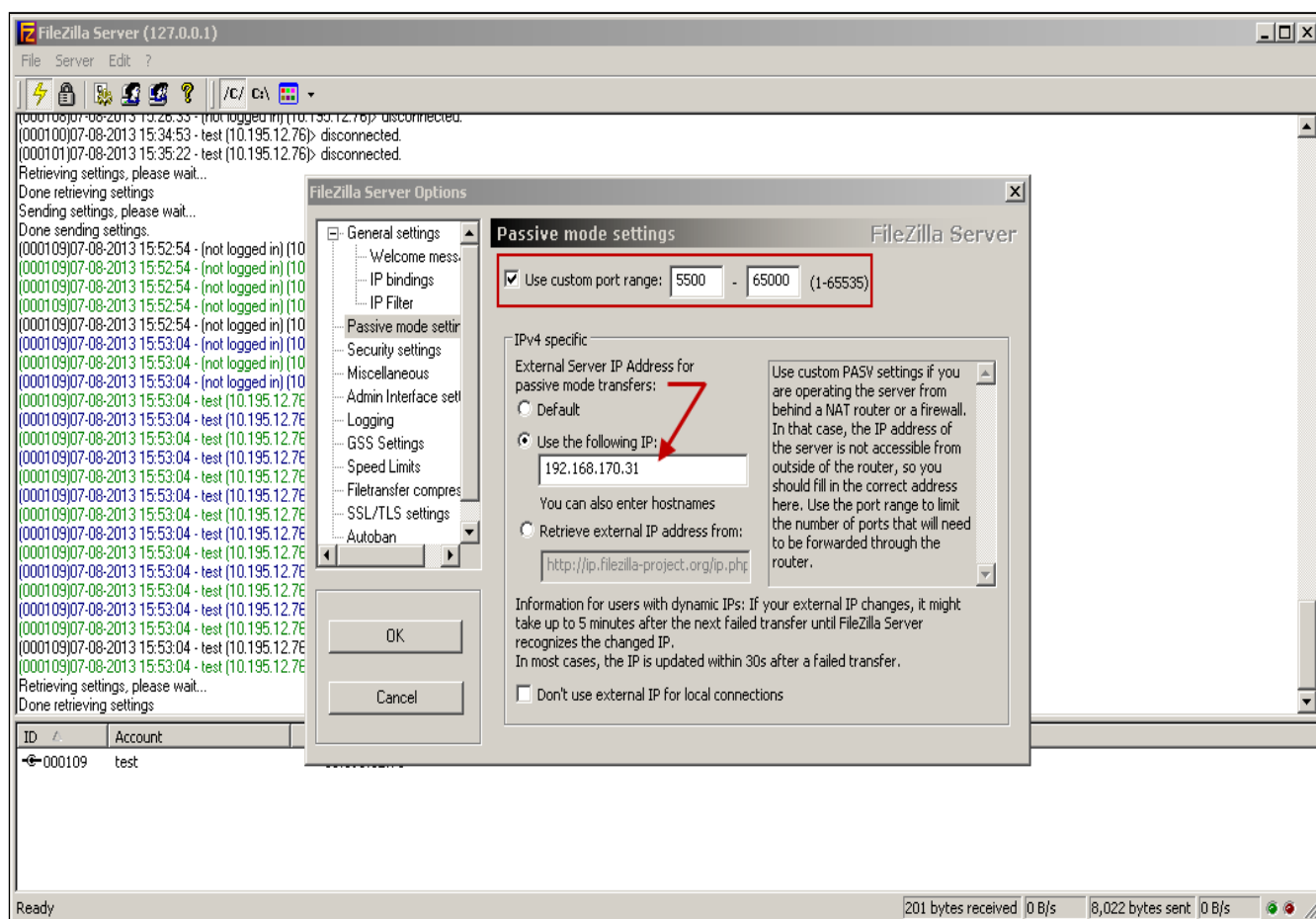
(internet) to connect over SSL/TLS to a server configured in Passive mode behind the SonicWALL. For the purpose of this article a FileZilla FTP server is shown.

Procedure:

FTP Server (FileZilla) Configuration

In FTP Passive mode, when the server responds to the PASV command from the client with its private IP address and Data port it is listening on, the SonicWALL changes the private IP address to that of the SonicWALL's WAN IP before forwarding the packet to the client. However, in FTPS the SonicWALL cannot make such a modification as the traffic is encrypted. Therefore, the FTP server must be manually set with the publically visible (NATted) WAN IP address.

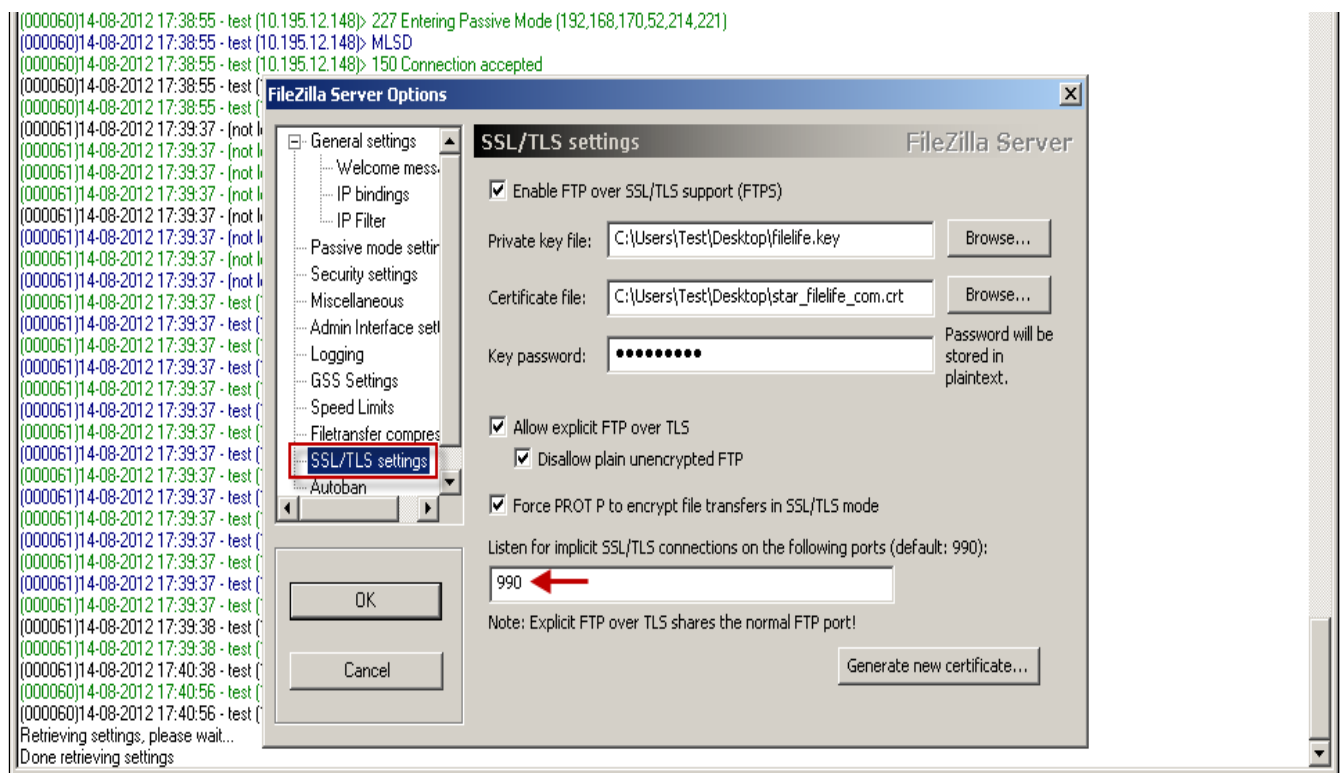
In the following screenshot the server has been manually configured to listen on a port between TCP 55000-65000 for its Data connection and its WAN IP address has been manually configured.



[Click To See Full Image.](#)

The following configuration enables SSL/TLS on TCP port 990.





[Click To See Full Image.](#)

SonicWALL Configuration

Create Service Objects

Login to the SonicWALL management GUI.

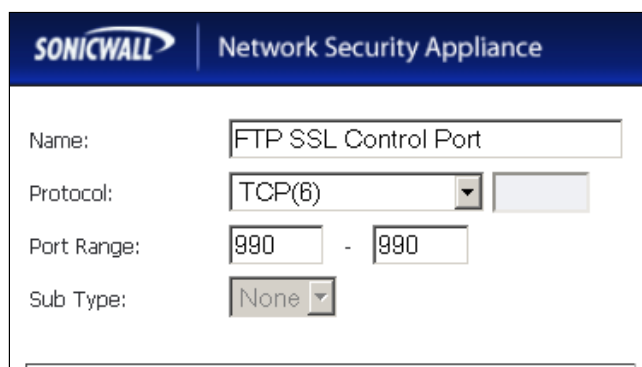
Navigate to the **Network > Services** page.

Create the following service objects.

TCP Port 990 for FTP Control

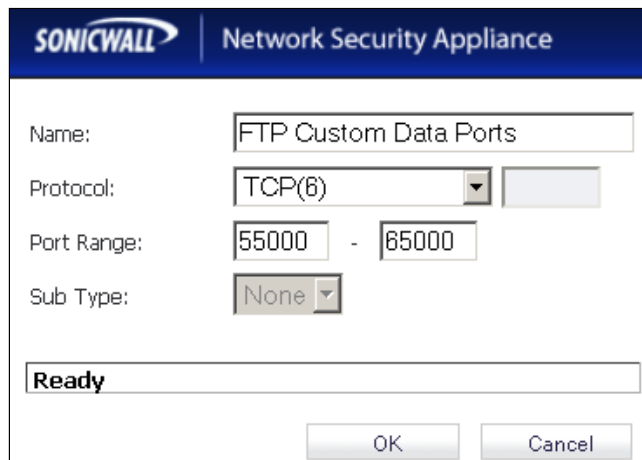
TCP Port range 55000-65000 for FTP Data

Add the newly created objects to a group

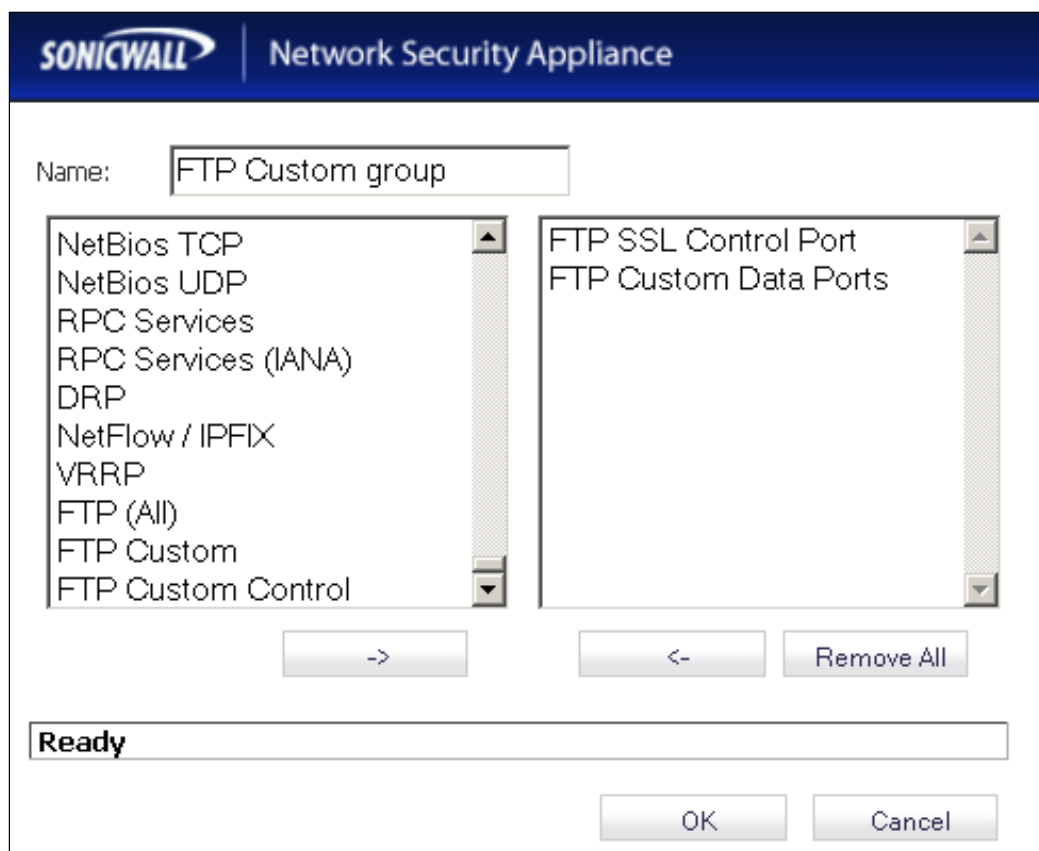




[Click To See Full Image.](#)



[Click To See Full Image.](#)



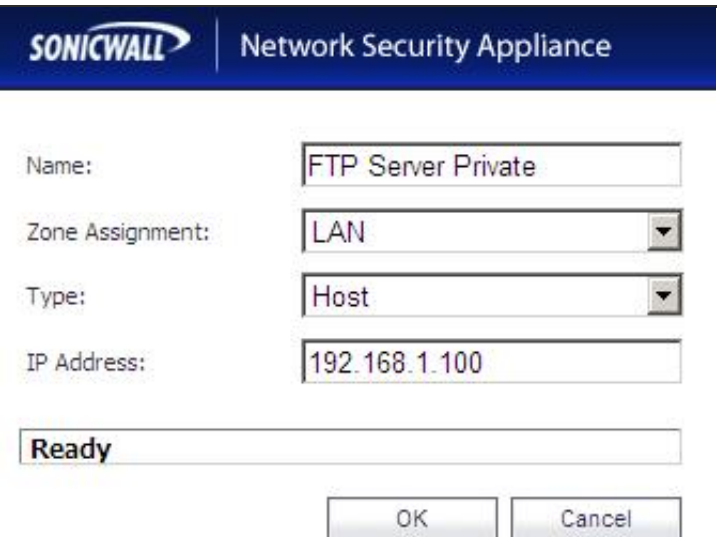
[Click To See Full Image.](#)

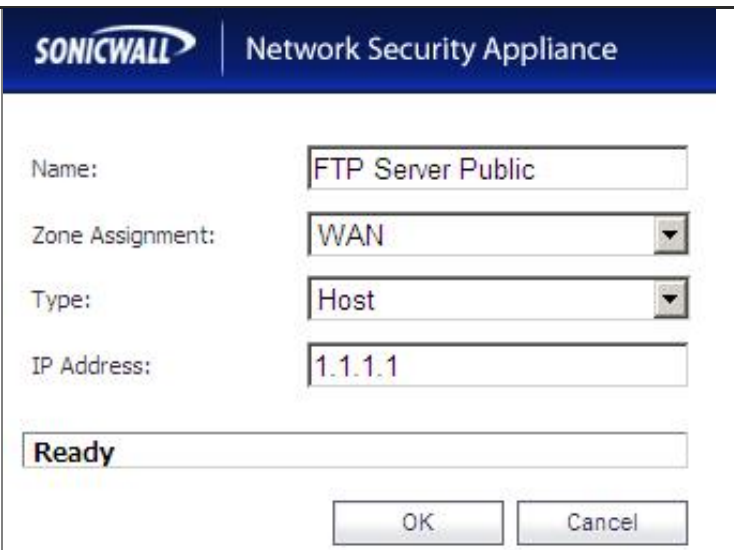
Create Address Objects

Navigate to the **Network > Address Objects** page.

Click the **Add a new address object** button and create two address objects one for **Server IP on LAN** and another for **Public IP** of the server.

Click the **OK** button to complete creation of the new address objects.

Address Object for Server on LAN Name: FTP Server Private Zone Assignment: LAN Type: Host IP Address: 192.168.1.100	
	<p>Click To See Full Image.</p>

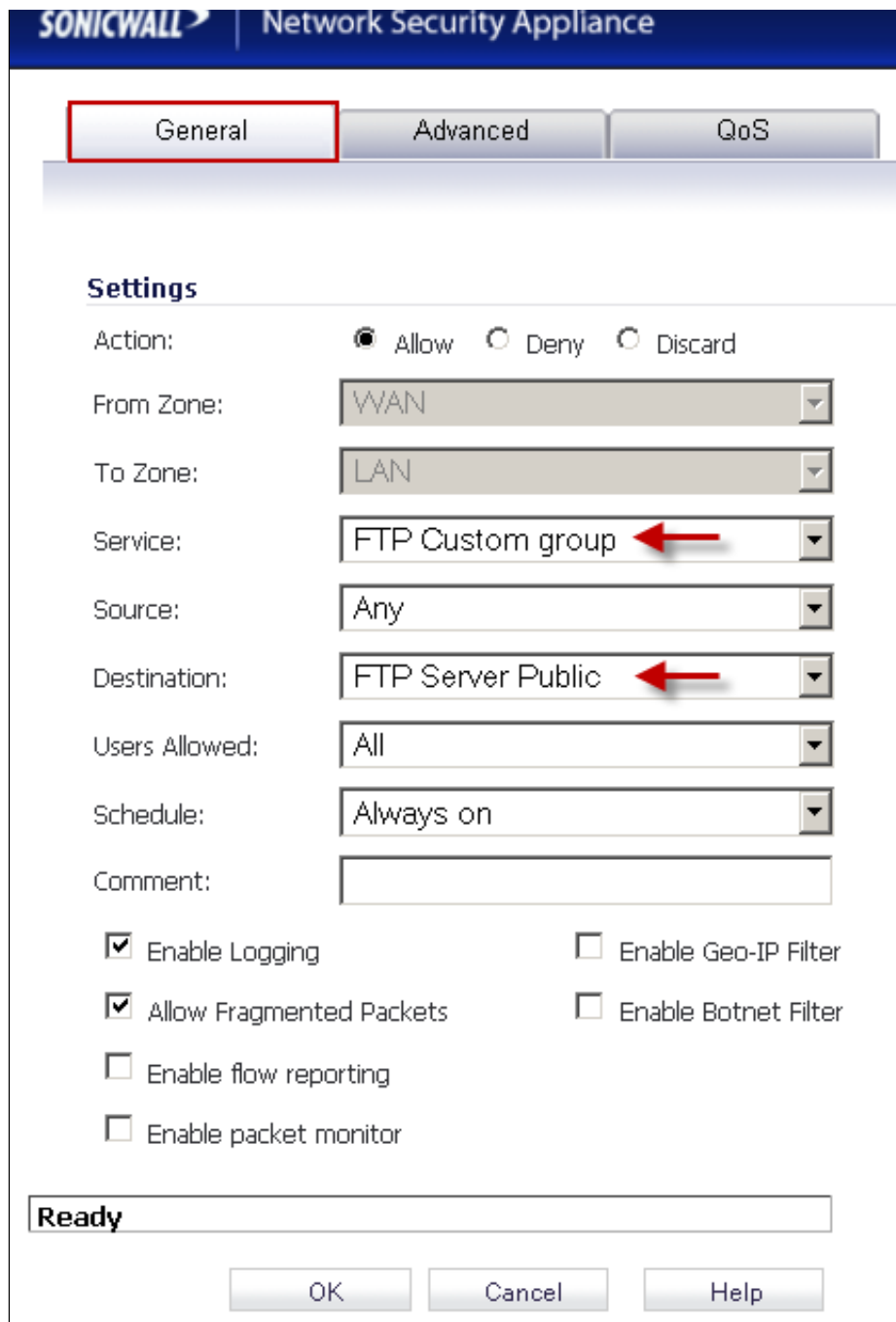
Address Object for Server's Public IP Name: FTP Server Public Zone Assignment: WAN Type: Host IP Address: 1.1.1.1	
	<p>Click To See Full Image.</p>

Create an Access Rule

Navigate to the Firewall > Access Rules page.

Navigate to the WAN > LAN page.

Create the following access rule.

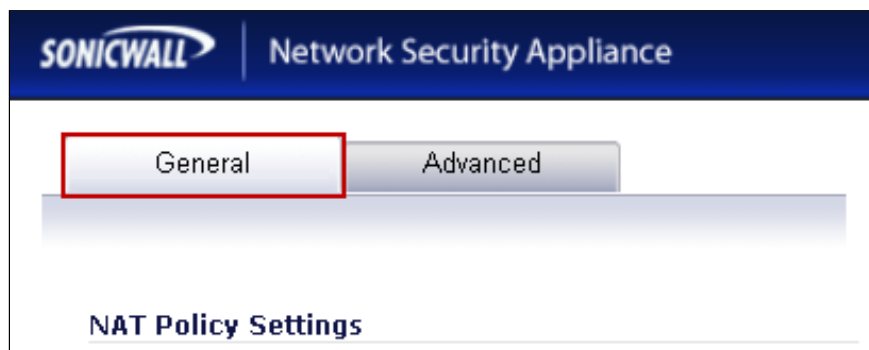


[Click To See Full Image.](#)

Create a NAT Policy

Navigate to the **Network > NAT Policies** page.

Create the following NAT policy.



Original Source:	Any
Translated Source:	Original
Original Destination:	FTP Server Public
Translated Destination:	FTP Server Private
Original Service:	FTP Custom group
Translated Service:	Original
Inbound Interface:	X1
Outbound Interface:	Any
Comment:	
<input checked="" type="checkbox"/> Enable NAT Policy	
Ready	
OK Cancel Help	

[Click To See Full Image.](#)