Firewall Defaults, Public Server Rule, and Secondary WAN IP Address

This quick start guide provides the firewall defaults and explains how to configure some basic firewall rules for the ProSafe Wireless-N 8-Port Gigabit VPN Firewall FVS318N to get you up and running fast. For information about more complicated firewall features, and for complete configuration steps, see the *Reference Manual*. This quick start guide contains the following sections:

- *Default Firewall Rules and General Security Settings*
- *Create a Firewall Rule for a Public Server*
- *Create a Firewall Rule for a Secondary WAN IP Address*
- *For More Information*

Note: For more information about the topics covered in this guide, visit the FVS318N support website at *http://support.netgear.com*. You will also find the *Reference Manual* at the support website.

Default Firewall Rules and General Security Settings

The default firewall rules and general security settings should work well for most small business networks, and you do not need change these settings for correct functioning of the wireless VPN firewall. The default settings are listed in the following table.

Table 1. Default firewall rules and general security settings

Security Feature	Default Behavior	Reference Section for More Information in Chapter 5, "Firewall Protection," of the *Reference Manual*
Default inbound LAN WAN firewall rule (communications coming in from the Internet)	All traffic from the WAN is blocked, except in response to LAN requests.	• "Overview of Rules to Block or Allow Specific Kinds of Traffic" • "Configure LAN WAN Rules"
Default outbound LAN WAN firewall rule (communications from the LAN to the Internet)	All traffic from the LAN is allowed.	

Table 1. Default firewall rules and general security settings (continued)

Security Feature	Default Behavior	Reference Section for More Information in Chapter 5, "Firewall Protection," of the *Reference Manual*
Inbound and outbound DMZ WAN firewall rules	None	• "Overview of Rules to Block or Allow Specific Kinds of Traffic" • "Configure DMZ WAN Rules"
Inbound and outbound LAN DMZ firewall rules	None	• "Overview of Rules to Block or Allow Specific Kinds of Traffic" • "Configure LAN DMZ Rules"
Respond to ping on WAN (Internet) ports	Disabled	"Attack Checks"
Stealth mode (prevents responses to port scans from the WAN)	Enabled	
TCP flood (allows all invalid TCP packets to be dropped as protection from a SYN flood attack)	Enabled	
UDP flood (prevents more than 20 simultaneous, active UDP connections from a single device on the LAN)	Enabled	
Respond to ping on LAN ports	Disabled	
IPv4 VPN pass-through for IPSec in NAT mode	Enabled	
IPv4 VPN pass-through for PPTP in NAT mode	Enabled	
IPv4 VPN pass-through for L2TP in NAT mode	Enabled	
IPv6 VPN pass-through for IPSec	Enabled	
Multicast pass-through for IGMP (allows multicast packets from the WAN to be forwarded to the LAN)	Disabled	
Jumbo frames (allow multiple smaller packets to be combined into a single larger packet)[1]	Disabled	
Session limits	Disabled	"Set Limits for IPv4 Sessions"
TCP expiration time-out without traffic	1800 seconds	
UDP expiration time-out without traffic	120 seconds	
ICMP expiration time-out without traffic	60 seconds	
Session Initiation Protocol (SIP) support for the Application Level Gateway (ALG)	Disabled	"Manage the Application Level Gateway for SIP Sessions"
Source MAC address filtering	Disabled	"Enable Source MAC Filtering"
IP address-to-MAC address bindings	Disabled	"Set Up IP/MAC Bindings"
Port triggering rules	None	"Configure Port Triggering"

Table 1. Default firewall rules and general security settings (continued)

Security Feature	Default Behavior	Reference Section for More Information in Chapter 5, "Firewall Protection," of the *Reference Manual*
Universal Plug and Play (UPnP)	Disabled	"Configure Universal Plug and Play"
Bandwidth profiles	None	"Create Bandwidth Profiles"
Content filtering	Disabled	"Configure Content Filtering"
Proxy server blocking	Disabled	
Java applets blocking	Disabled	
ActiveX controls blocking	Disabled	
Cookies blocking	Disabled	
Blocked keywords	None	
Trusted domains	All domains	

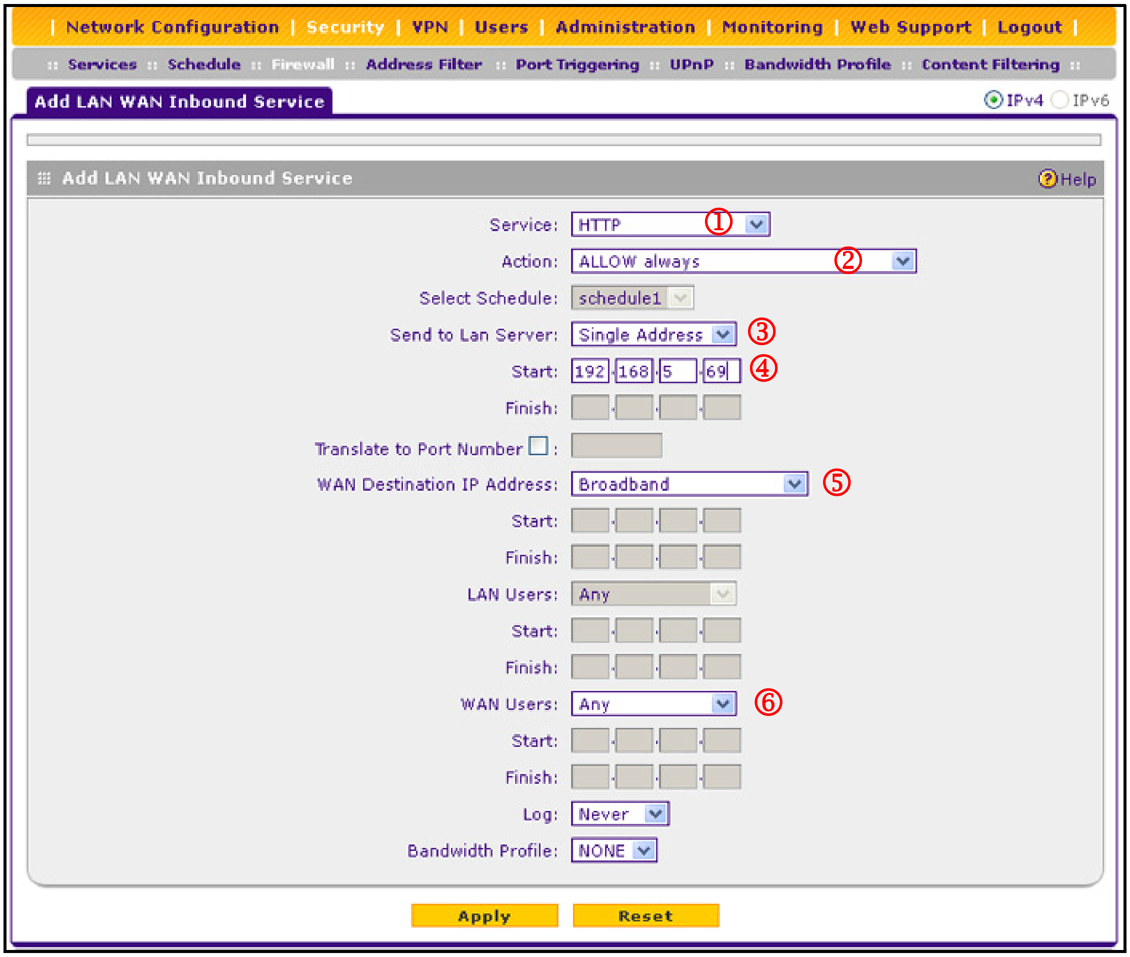
[1] *Jumbo frames are supported on ports 1, 2, 3, and 4 only.*

Create a Firewall Rule for a Public Server

By default, all access from outside is blocked, except responses to requests from LAN users. If you host a public web or FTP server on your LAN, you can define a rule to allow inbound web (HTTP) or FTP requests from any outside IP address to the IP address of your web or FTP server at any time of the day.

➢ **To configure a public server:**

1. Select **Security > Firewall**. The Firewall submenu tabs display with the LAN WAN Rules screen for IPv4 in view.
2. Click the **Add** table button under the Outbound Services table. The Add LAN WAN Outbound Service screen for IPv4 displays. The following screen shows an example for a public web server:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Add LAN WAN Inbound Service
● IPv4 ○ IPv6
Add LAN WAN Inbound Service
Help
①
②
③
④
⑤
⑥
Apply
Reset

Service:	HTTP
Action:	ALLOW always
Select Schedule:	schedule1
Send to Lan Server:	Single Address
Start:	192.168.5.69
Finish:	
Translate to Port Number □ :	
WAN Destination IP Address:	Broadband
Start:	
Finish:	
LAN Users:	Any
Start:	
Finish:	
WAN Users:	Any
Start:	
Finish:	
Log:	Never
Bandwidth Profile:	NONE

Figure 1.

3. Configure the settings as explained in the following table. The fields that are not mentioned are not required.

Table 2. Screen settings for adding public server

#	Setting	Description
①	Service	From the drop-down list, select **HTTP** for a web server or **FTP** for an FTP server.
②	Action	From the drop-down list, select **ALLOW always**.
③	Send to Lan Server	From the drop-down list, **Single Address**.
④	Start (under Send to Lan Server)	Type the IP address of the web or FTP server on your LAN.
⑤	WAN Destination IP Address	From the drop-down list, select **Broadband** for the WAN interface.
⑥	WAN Users	From the drop-down list, select **Any**.

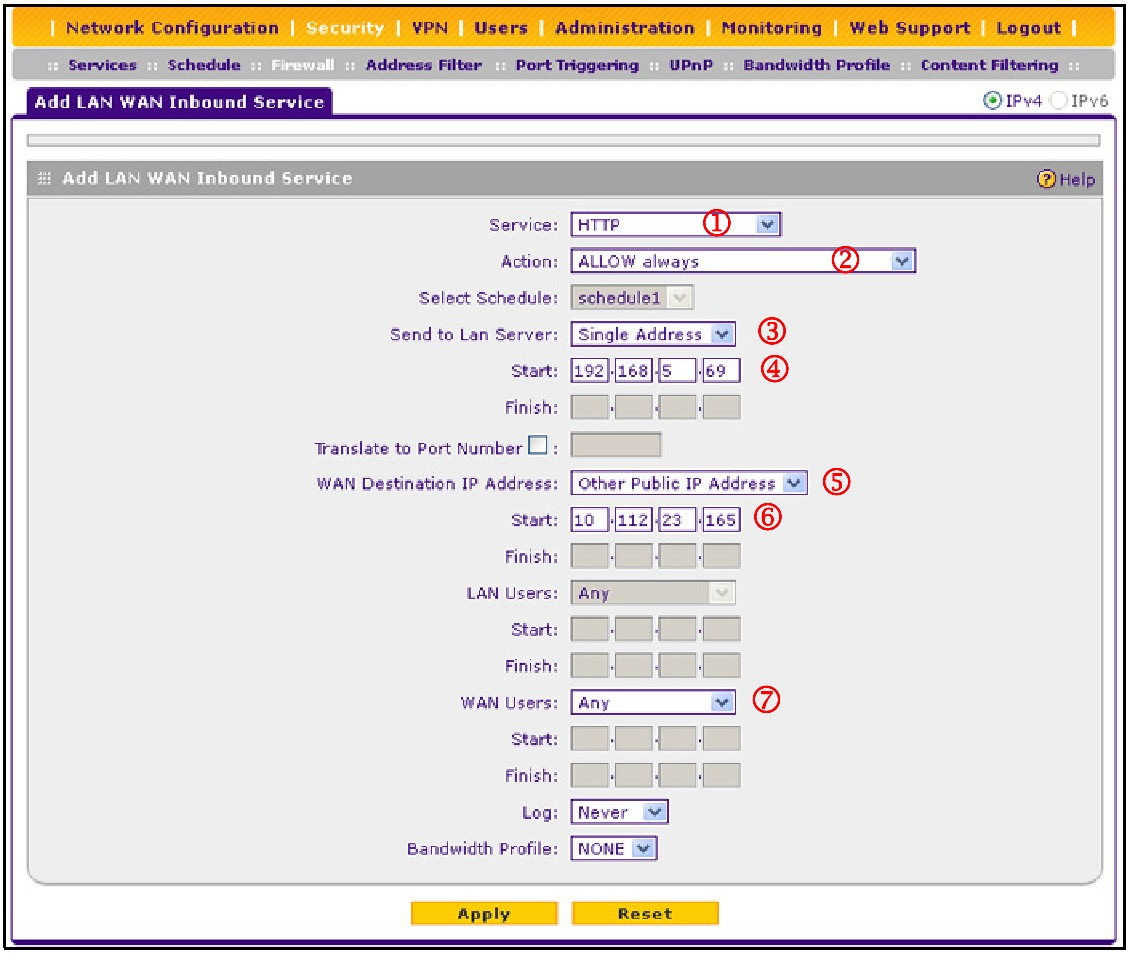
4. Click **Apply** to save your changes. The new rule is added to the LAN WAN Rules screen and is automatically enabled.

Create a Firewall Rule for a Secondary WAN IP Address

By default, all access from outside is blocked, except responses to requests from LAN users. As an added security measure, you can configure a secondary WAN IP address to which inbound web (HTTP) requests from any outside IP address can be directed at any time of the day.

➢ **To configure a secondary WAN IP address:**

1. Select **Security > Firewall**. The Firewall submenu tabs display with the LAN WAN Rules screen for IPv4 in view.
2. Click the **Add** table button under the Outbound Services table. The Add LAN WAN Outbound Service screen for IPv4 displays. The following screen shows an example for a secondary WAN IP address:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Add LAN WAN Inbound Service
● IPv4 ○ IPv6
Add LAN WAN Inbound Service
? Help
Apply
Reset

Service: HTTP ①

Action: ALLOW always ②

Select Schedule: schedule1

Send to Lan Server: Single Address ③

Start: 192.168.5.69 ④

Finish:

Translate to Port Number □:

WAN Destination IP Address: Other Public IP Address ⑤

Start: 10.112.23.165 ⑥

Finish:

LAN Users: Any

Start:

Finish:

WAN Users: Any ⑦

Start:

Finish:

Log: Never

Bandwidth Profile: NONE

Figure 2.

3. Configure the settings as explained in the following table. The fields that are not mentioned are not required.

Table 3. Screen settings for a adding secondary WAN IP address

#	Setting	Description
①	Service	From the drop-down list, select **HTTP** for a web server or **FTP** for an FTP server.
②	Action	From the drop-down list, select **ALLOW always**.
③	Send to Lan Server	From the drop-down list, **Single Address**.
④	Start (under Send to Lan Server)	Type the IP address of the web or FTP server on your LAN.
⑤	WAN Destination IP Address	From the drop-down list, select **Other Public IP Address** for the WAN interface.
⑥	Start (under WAN Destination IP Address)	Type the IP address of the secondary WAN address.
⑦	WAN Users	From the drop-down list, select **Any**.

4. Click **Apply** to save your changes. The new rule is added to the LAN WAN Rules screen and is automatically enabled.

For More Information

Chapter 5, “Firewall Protection,” of the *Reference Manual* provides information about the following security topics:

- Overview of rules to block or allow specific kinds of traffic
- Configuring LAN WAN rules
- Configuring DMZ WAN rules
- Configuring LAN DMZ rules
- Configuring other firewall features
- Services, bandwidth profiles, and QoS profiles
- Configuring content filtering
- Setting a schedule to block or allow specific traffic
- Enabling source MAC filtering
- Setting up IP/MAC bindings
- Configuring port triggering
- Configuring universal Plug and Play (UPnP)