NETGEAR

Firewall Defaults and Some Basic Rules

ProSecure UTM Quick Start Guide

This quick start guide provides the firewall defaults and explains how to configure some basic firewall rules for the ProSecure Unified Threat Management (UTM) Appliance. For information about more complicated firewall features, and for complete configuration steps, see the *ProSecure Unified Threat Management (UTM) Appliance Reference Manual*, available at *http://downloadcenter.netgear.com*.

This quick start guide contains the following sections:

Default Firewall Rules and General Security Settings

The default firewall rules and general network security settings should work well for many business networks, and you do not need to change these settings for correct functioning of the UTM. The default settings are listed in the following table.

Table 1. Default firewall rules and general security settings

Security Feature	Default Behavior	This column lists sections in Chapter 5, "Firewall Protection," of the reference manual. You can find more information in these sections.
LAN WAN firewall rules (menu path: Network Security > Firewall > LAN WAN Rules)		
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	This column lists sections in Chapter 5, "Firewall Protection," of the reference manual. You can find more information in these sections.
DMZ WAN firewall rules (menu path: Network Security > Firewall > DMZ WAN Rules)		
Inbound and outbound DMZ WAN firewall rules	None configured	• "Overview of Rules to Block or Allow Specific Kinds of Traffic" • "Configure DMZ WAN Rules"
LAN DMZ firewall rules (menu path: Network Security > Firewall > LAN DMZ Rules)		
Inbound and outbound LAN DMZ firewall rules	None configured	• "Overview of Rules to Block or Allow Specific Kinds of Traffic" • "Configure LAN DMZ Rules"
VLAN firewall rules (menu path: Network Security > Firewall > VLAN Rules)		
VLAN firewall rules	None configured	"VLAN Rules"
WAN and LAN security checks and VPN pass-through (menu path: Network Security > Firewall > Attack Checks)		
Respond to ping on Internet ports	Disabled	"Attack Checks, VPN Pass-through, and Multicast Pass-through"
Enable Stealth mode (prevents port scans from the WAN)	Enabled	
Block TCP flood (allows all invalid TCP packets to be dropped as protection from a SYN flood attack)	Disabled	
Block UDP flood (prevents more than 20 simultaneous, active UDP connections from a single device on the LAN)	Disabled	
Respond to ping on LAN ports	Disabled	
IPSec (NAT filtering for IPSec tunnels)	Enabled	
PPTP (NAT filtering for PPTP tunnels)	Enabled	
L2TP (NAT filtering for L2TP tunnels)	Enabled	
Session limits (menu path: Network Security > Firewall > Session Limit)		
Session limits	Disabled	"Set Session Limits"
TCP expiration time-out without traffic	1200 seconds	
UDP expiration time-out without traffic	180 seconds	
ICMP expiration time-out without traffic	8 seconds	

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

Security Feature	Default Behavior	This column lists sections in Chapter 5, "Firewall Protection," of the reference manual. You can find more information in these sections.
Multicast pass-through (menu path: Network Security > Firewall > IGMP)		
IGMP pass-through for (allows multicast packets from the WAN to be forwarded to the LAN)	Enabled	"Attack Checks, VPN Pass-through, and Multicast Pass-through"
SIP ALG and VPN scanning (menu path: Network Security > Firewall > Advanced)		
Session Initiation Protocol (SIP) support for the Application Level Gateway (ALG)	Disabled	"Manage the Application Level Gateway for SIP Sessions and VPN Scanning"
Scanning of VPN traffic	Disabled	
Intrusion prevention system (menu path: Network Security > IPS)		
Intrusion prevention system	Disabled	"Use the Intrusion Prevention System"
Source MAC address filtering (Menu Path: Network Security > Address Filter > Source MAC Filter)		
Source MAC address filtering	Disabled	"Enable Source MAC Filtering"
IP/MAC address binding (menu path: Network Security > Address Filter > IP/MAC Binding)		
IP address-to-MAC address bindings	Disabled	"Set Up IP/MAC Bindings"
Port triggering (menu path: Network Security > Port Triggering)		
Port triggering rules	None	"Configure Port Triggering"
Universal plug and play (menu path: Network Security > UPnP)		
Universal Plug and Play (UPnP)	Disabled	"Configure Universal Plug and Play"

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

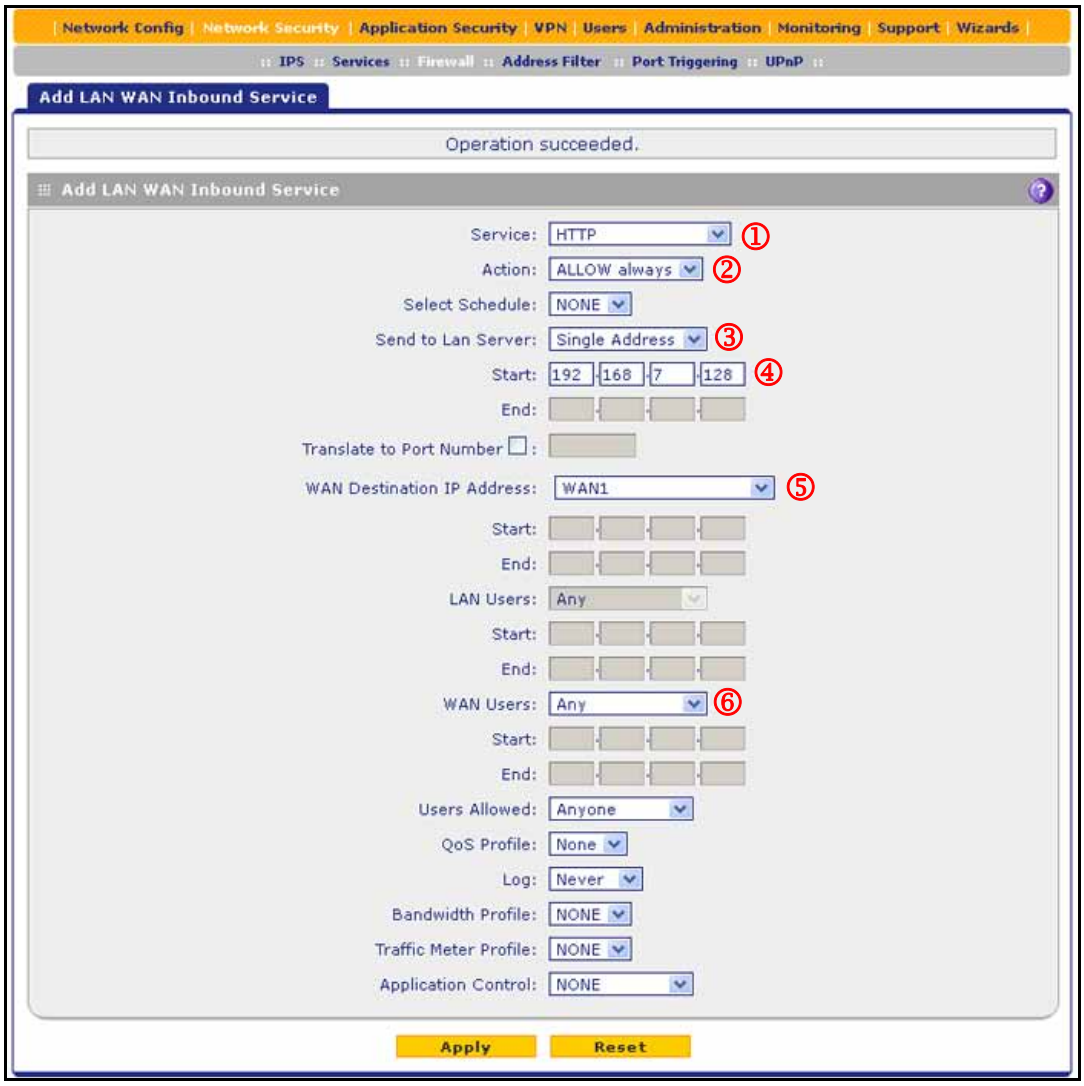

Figure 1.

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.

Table 2. Screen settings for adding public server (continued)

#	Setting	Description
⑤	WAN Destination IP Address	From the drop-down list, select a WAN interface. The available interfaces depend on your UTM model. However, in most situations you would select WAN1.
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.

You first need to configure a secondary WAN address, and then you can create a firewall rule using the new secondary WAN address.

➢ **To configure a firewall rule for a secondary WAN IP address:**

1. Select **Network Config > WAN Settings**. The WAN screen displays.
2. Click the **Edit** button in the Action column of the WAN interface for which you want to add a secondary address. The WAN ISP Settings screen displays.
3. Click the **Secondary Addresses** option arrow at the upper right of the screen. The WAN Secondary Addresses screen displays for the WAN interface that you selected:

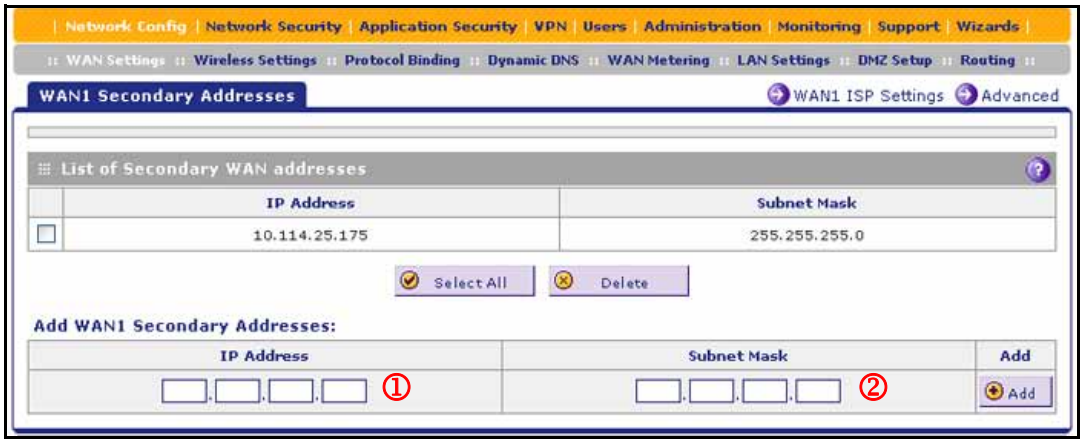

Figure 2.

The List of Secondary WAN addresses table displays the secondary WAN IP addresses added for the selected WAN interface.

4. In the Add WAN Secondary Addresses section of the screen, enter the following settings:
   - **IP Address**. Enter the secondary address that you want to assign to the WAN interface. (①)
   - **Subnet Mask**. Enter the subnet mask for the secondary IP address. (②)
5. Click the **Add** table button in the rightmost column to add the secondary IP address to the List of Secondary WAN addresses table.
6. Select **Network Security > Firewall**. The Firewall submenu tabs display with the LAN WAN Rules screen in view.
7. Click the **Add** table button under the Inbound Services table. The Add LAN WAN Inbound Service screen displays. The following screen shows an example for a secondary WAN IP address:

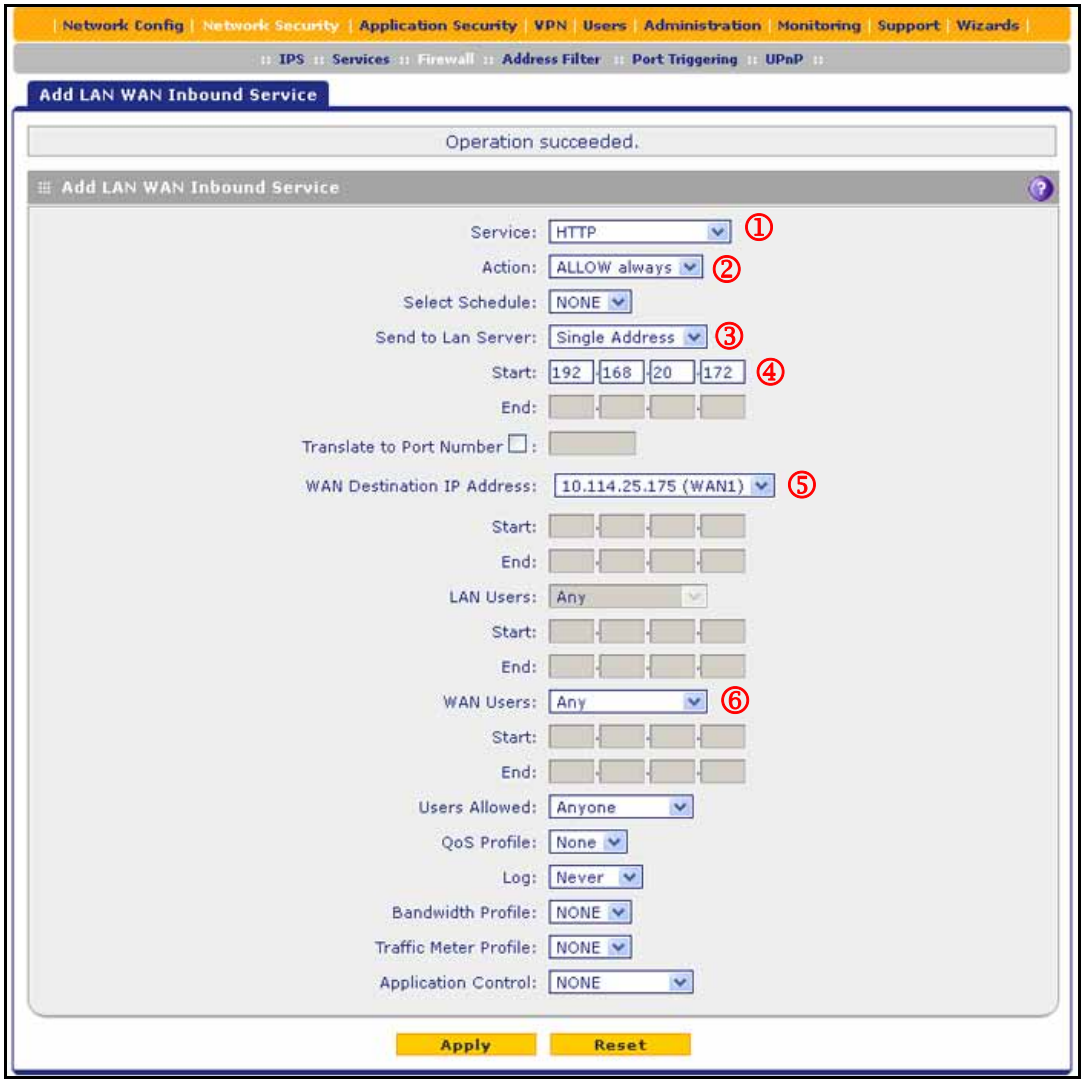

Figure 3.

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

Table 3. Screen settings for 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 the secondary WAN IP address that you added in *Step 4* and *Step 5*.
⑥	WAN Users	From the drop-down list, select **Any**.

9. 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
- Creating services, QoS profiles, bandwidth profiles, and traffic meter profiles
- 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
- Enabling and configuring the intrusion prevention system