

UTM Basic Firewall Configuration

This guide describes how to configure basic firewall rules in the UTM to protect your network. The firewall then can provide secure, encrypted communications between your local network and a remote network or computer. For information about other firewall features and for complete configuration steps, see the *ProSecure Unified Threat Management (UTM) Appliance Reference Manual* at: <http://downloadcenter.netgear.com>.

This guide contains the following sections:

- *About Firewall Protection*
- *Use Rules to Block or Allow Specific Kinds of Traffic*
- *Configure Other Firewall Features*
- *Create Services, QoS Profiles, and Bandwidth Profiles*
- *Set a Schedule to Block or Allow Specific Traffic*
- *Use the Intrusion Prevention System*
- *What to Do Next*

About Firewall Protection

A firewall protects one network such as your LAN from another such as the Internet while allowing communication between the networks. It protects your network from hacker intrusions or attacks and controls the types of traffic between networks.

Use Rules to Block or Allow Specific Kinds of Traffic

Firewall rules are used to block or allow specific traffic passing through it from one network to another. You can configure up to 800 rules on the UTM. Inbound rules (WAN to LAN) restrict access by outsiders. The firewall selectively allows only specific outside users to access specific resources on your network. Outbound rules (LAN to WAN) determine what outside resources users on your network can access.

The UTM firewall has two default rules, one for inbound traffic and one for outbound. The default rules are:

- **Inbound.** Block all access from outside except responses to requests from the LAN side.
- **Outbound.** Allow all access from the LAN side to the outside.

The firewall rules for blocking and allowing traffic on the UTM can be applied to LAN WAN traffic. See the reference manual for descriptions of demilitarized zone (DMZ) configuration.

Table 1. Number of supported firewall rule configurations

Traffic rule	Maximum number of outbound rules	Maximum number of inbound rules	Maximum number of supported rules
LAN WAN	300	300	600
DMZ WAN (see note)	50	50	100
LAN DMZ (see note)	50	50	100
<i>Total Rules</i>	400	400	800

The demilitarized (DMZ) port is a dedicated port that can be used to forward unfiltered traffic to a selected node on your network. The DMZ port is not be discussed in this guide. See the reference manual for more information.

Service-Based Rules

The rules to block traffic are based on the traffic category of service:

- **Outbound rules (service blocking).** Outbound traffic is allowed unless the firewall is configured to disallow it.
- **Inbound rules (port forwarding).** The firewall blocks inbound traffic unless the traffic is in response to a request from the LAN side. The firewall can be configured to allow this otherwise blocked traffic.
- **Customized services.** Additional services can be added to the list of services in the factory defaults list. These added services can then have rules defined for them to either allow or block that traffic. See the reference manual for more information.
- **Quality of Service (QoS) priorities.** Each service has a priority that impacts its quality of performance and tolerance for jitter or delays. You can change the QoS priority, which changes the traffic mix through the system. See the reference manual for more information.

Outbound Rules (Service Blocking)

The UTM allows you to block the use of Internet services by computers on your network. This feature is called service blocking. The steps to configure outbound rules are described in the following sections.



WARNING:

Allowing services opens security holes in your firewall. Enable only those services (ports) that are necessary for your network.

The following table describes the fields that define the rules for outbound traffic and that are common to most Outbound Service screens.

Table 2. Outbound rules overview

Setting	Description	Outbound Rules
Service (also referred to as Service Name)	The service or application this rule covers. If the service or application does not display in the list, you must define it using the Services screen (see Add Customized Services on page 20).	All rules
Action (also referred to as Filter)	The action for outgoing connections this rule covers. <ul style="list-style-type: none"> • BLOCK always • ALLOW always <p>Note: The default rule allows any outbound traffic your rules do not block.</p> <p>Note: ALLOW rules are useful only if a BLOCK rule already blocks the traffic. That is, you wish to allow a subset of traffic that another rule currently blocks. Similarly, BLOCK rules are useful only if an ALLOW rule already covers the traffic. That is, you wish to block a subset of traffic that another rule blocks.</p>	All rules
Select Schedule	The time schedule the rule uses. By default, there is no schedule assigned (that is, None is selected from the Schedule drop-down list), and the rule is in effect all the time. For information about creating schedules, see Set a Schedule to Block or Allow Specific Traffic on page 31.	All rules
LAN Users	These settings determine which computers on your network the rule affects. The options are: <ul style="list-style-type: none"> • Any. All computers and devices on your LAN. • Single address. Enter the required address in the Start field to apply the rule to a single device on your LAN. • Address range. Enter the required addresses in the Start and End fields to apply the rule to a range of devices. • Group. Select the LAN group to which the rule applies. See the reference manual. • IP Group. Select the IP group to which the rule applies. See the reference manual. 	LAN WAN rules

Table 2. Outbound rules overview (continued)

Setting	Description	Outbound Rules
WAN Users	<p>The settings that determine which Internet locations the rule affects, based on their IP address. The options are:</p> <ul style="list-style-type: none"> • Any. All Internet IP addresses this rule affects. • Single address. Enter the required address in the Start field. • Address range. Enter the required addresses the Start and End fields. • IP Group. Select the IP group to which the rule applies. Use the IP Groups screen to assign IP addresses to groups. See the reference manual. 	LAN WAN rules
Users Allowed	<ul style="list-style-type: none"> • The settings that determine the users or groups on the network that this rule affects. You can select a local user, local group, or custom group. For information about setting up custom groups, see the reference manual. 	LAN WAN rules
QoS Profile	<p>The priority assigned to IP packets of this service. The priorities depend on Type of Service (ToS), which is defined in the Internet Protocol Suite standards, RFC 1349. The QoS profile determines the priority of a service, which, in turn, determines the quality of that service for the traffic passing through the firewall.</p> <p>The UTM marks the Type of Service (ToS) field, which is defined in the QoS profiles that you create. For more information, see Create Quality of Service Profiles on page 22.</p> <p>Note: There is no default QoS profile on the UTM. After you have created a QoS profile, it can become active only when you apply it to a nonblocking inbound or outbound firewall rule.</p>	LAN WAN rules
Log	<p>The settings that determine whether the traffic this rule affects is logged. The options are:</p> <ul style="list-style-type: none"> • Always. Always log traffic defined in this rule, whether it matches or not. This setting is useful when you are debugging rules. • Never. Never log traffic defined in this rule, whether it matches or not. 	All rules
Bandwidth Profile	<p>Bandwidth limiting determines how the data is sent to and from your host. The purpose of bandwidth limiting is to provide a solution for limiting the outgoing and incoming traffic. This setting prevents LAN users from consuming all the bandwidth of the Internet link. For more information, see Create Bandwidth Profiles on page 25. Bandwidth limiting occurs in the following ways:</p> <ul style="list-style-type: none"> • For outbound traffic. On the available WAN interface in the primary WAN mode and auto-rollover mode, and on the selected interface in load balancing mode. • For inbound traffic. On the LAN interface for all WAN modes. 	LAN WAN rules
Traffic Meter Profile	<p>Select a traffic meter profile to measure and control traffic that is downloaded, uploaded, or both. The traffic meter profile applies only to traffic that this rule covers. Depending on the configuration of the traffic meter profile, when traffic has reached its configured limit, traffic is either logged or blocked. For information about creating traffic meter profiles, see Create Traffic Meter Profiles on page 28.</p>	LAN WAN rules

Table 2. Outbound rules overview (continued)

Setting	Description	Outbound Rules
Application Control	<p>Select an application control profile to allow, block, or log traffic for entire categories of applications, for individual applications, or for a combination of both. The application control profile applies only to traffic to which this rule applies.</p> <p>To create an application control profile, select + Create New from the Application Control drop-down list. The Add or Edit Application Control Profile pop-up screen displays.</p> <p>For information about creating and enabling application control profiles, see the reference manual.</p>	LAN WAN rules
NAT IP	<p>This setting specifies the source address of the outgoing traffic on the WAN is assigned the address of the WAN interface or a different interface. You can specify these settings only for outbound traffic on the WAN interface. See the reference manual for more information. The options are:</p> <ul style="list-style-type: none"> • WAN Interface Address. All the outgoing traffic on the WAN is assigned to the address of the specified WAN interface. • Single Address. All the outgoing traffic on the WAN is assigned to the specified IP address, for example, a secondary WAN address that you have configured. <p>Note: The NAT IP option is available only when the WAN mode is NAT. The IP address specified must be in the WAN subnet.</p>	LAN WAN rules

Inbound Rules (Port Forwarding)

If you have enabled Network Address Translation (NAT), your network presents only *one* IP address to the Internet, and outside users cannot directly access any of your local computers (LAN users). (For information about configuring NAT, see the reference manual.) However, by defining an inbound rule you can make a local server (for example, a web server or game server) visible and available to the Internet. The rule informs the firewall to direct inbound traffic for a particular service to one local server based on the destination port number. This process is also known as port forwarding.

Whether or not DHCP is enabled, how the computer accesses the server LAN address impacts the inbound rules. For example:

- If your ISP assigns the external IP address (DHCP enabled), the IP address might change periodically as the DHCP lease expires. Consider using Dynamic DNS so that external users can always find your network (see the reference manual).
- If DHCP assigns the IP address of the local server computer, the address might change when the computer is rebooted. Use the Reserved (DHCP Client) feature in the LAN Groups screen to keep the computer IP address constant (see the reference manual).
- Local computers must access the local server using the computer's local LAN address. Attempts by local computers to access the server using the external WAN IP address fail.

Note: The UTM always blocks denial of service (DoS) attacks. A DoS attack does not attempt to steal data or damage your computers, but overloads your Internet connection so you cannot use it (that is, the service becomes unavailable).

Note: When the Block TCP Flood and Block UDP Flood check boxes are selected on the Attack Checks screen, multiple concurrent connections of the same application from one host or IP address trigger the UTM's DoS protection. DNS queries from the same computer can produce multiple connections. See *Attack Checks and VPN Pass-through* on page 16.

Note: For more information about protecting the UTM from incoming threats, see *Use the Intrusion Prevention System* on page 33.

The following table describes the fields that define the rules for inbound traffic and that are common to most Inbound Service screens.

Table 3. Inbound rules overview

Setting	Description	Inbound Rules
Service (also referred to as Service Name)	The service or application this rule affects. If the service or application does not display in the list, you must define it using the Services screen (see <i>Add Customized Services</i> on page 20).	All rules
Action (also referred to as Filter)	The action for outgoing connections this rule covers: <ul style="list-style-type: none"> • BLOCK always • ALLOW always <p>Note: Any inbound traffic is allowed unless a rule blocks it.</p> <p>Note: ALLOW rules are useful only if a BLOCK rule already covers the traffic. You can allow a subset of traffic that another rule blocks. Similarly, BLOCK rules are useful only if an ALLOW rule already covers the traffic. You can block a subset of traffic in the ALLOW rule.</p>	All rules
Select Schedule	The time schedule assigned to this rule. By default, there is no schedule assigned (that is, None is selected from the Schedule drop-down list), and the rule is in effect all the time. For information about creating schedules, see <i>Set a Schedule to Block or Allow Specific Traffic</i> on page 31.	All rules

Table 3. Inbound rules overview (continued)

Setting	Description	Inbound Rules
Send to LAN Server	<p>The LAN server address determines which computer on your network is hosting this service rule. (You can also translate this address to a port number.) The options are:</p> <ul style="list-style-type: none"> • Single address. Enter the required address in the Start field to apply the rule to a single device on your LAN. • Address range. Enter the required addresses in the Start and End fields to apply the rule to a range of devices. 	LAN WAN rules
Translate to Port Number	<p>If you want to assign the LAN server to a specific port, you can enable this setting and specify a port number.</p>	LAN WAN rules
WAN Destination IP Address	<p>The settings that determine the destination IP address applicable to incoming traffic. This address is the public IP address that maps to the internal LAN server.</p> <p>On the multiple WAN port models, it can be either the address of a WAN interface or another public IP address (when you configure a secondary WAN address). On the single WAN port models, it can be either the address of the single WAN interface or another public IP address (when you have configured a secondary WAN address). You can enter an address range. Enter the required addresses in the Start and End fields to apply the rule to a range of devices.</p>	LAN WAN rules
LAN Users	<p>The settings that determine which computers on your network the rule covers. The options are:</p> <ul style="list-style-type: none"> • Any. All computers and devices on your LAN. • Single address. Enter the required address in the Start field to apply the rule to a single device on your LAN. • Address range. Enter the required addresses in the Start and End fields to apply the rule to a range of devices. • Group. Select the group to which the rule applies. Use the LAN Groups screen to assign computers to groups. See the reference manual. • IP Group. Select the IP group to which the rule applies. Use the IP Groups screen to assign IP addresses to groups. See the reference manual. • For LAN WAN inbound rules, this field does not apply when the WAN mode is NAT because your network presents only <i>one</i> IP address to the Internet. 	LAN WAN rules
WAN Users	<p>The settings that determine which Internet locations the rule covers, based on their IP address. The options are:</p> <ul style="list-style-type: none"> • Any. This rule covers all Internet IP addresses. • Single address. Enter the required address in the Start field. • Address range. Enter the required addresses in the Start and End fields. • IP Group. Select the IP group to which the rule applies. Use the IP Groups screen to assign IP addresses to groups. See the reference manual. 	LAN WAN rules

Table 3. Inbound rules overview (continued)

Setting	Description	Inbound Rules
Users Allowed	These settings determine which user or group on the network the rule affects. You can select a local user, local group, or customer group. To create a custom group, select + Create New from the Users Allowed drop-down list on a firewall screen that lets you add or edit a rule. You can find the + Create New link under the Custom Groups heading on such a screen. For information about setting up custom groups, see the reference manual.	LAN WAN rules
QoS Profile	The priority assigned to IP packets of this service. The Type of Service (ToS) in the Internet Protocol Suite standards, RFC 1349 defines the priorities. The QoS profile determines the priority of a service, which, in turn, determines the quality of that service for the traffic passing through the firewall. The UTM marks the Type of Service (ToS) field as defined in the QoS profiles that you create. For more information, see Create Quality of Service Profiles on page 22. Note: There is no default QoS profile on the UTM. After you have created a QoS profile, it can become active only when you apply it to a nonblocking inbound or outbound firewall rule.	LAN WAN rules
Log	These settings determine whether packets this rule covers are logged. The options are: <ul style="list-style-type: none"> • Always. Always log traffic that this rule covers, whether it matches or not. This approach is useful when you are debugging your rules. • Never. Never log traffic that this rule covers, whether it matches or not. 	All rules
Bandwidth Profile	Bandwidth limiting determines how the data is sent to and from your host. The purpose of bandwidth limiting is to limit outgoing and incoming traffic, thus preventing LAN users from consuming all the bandwidth of the Internet link. For more information, see Create Bandwidth Profiles on page 25. Bandwidth limiting occurs in the following ways: <ul style="list-style-type: none"> • For outbound traffic. On the available WAN interface in the primary WAN mode and auto-rollover mode, and on the selected interface in load balancing mode. • For inbound traffic. On the LAN interface for all WAN modes. 	LAN WAN rules

Table 3. Inbound rules overview (continued)

Setting	Description	Inbound Rules
Traffic Meter Profile	Select a traffic meter profile to measure and control traffic that is downloaded, uploaded, or both. The traffic meter profile applies only to traffic that this rule covers. Depending on the configuration of the traffic meter profile, when traffic has reached its configured limit, traffic is either logged or blocked. For information about creating traffic meter profiles, see <i>Create Traffic Meter Profiles</i> on page 28.	LAN WAN rules
Application Control	Select an application control profile to allow, block, or log traffic for entire categories of applications, for individual applications, or for a combination of both. The application control profile applies only to traffic that this rule covers. To create an application control profile, select + Create New from the Application Control drop-down list. The Add or Edit Application Control Profile pop-up screen displays. For information about creating and enabling application control profiles, see the reference manual.	LAN WAN rules

Note: Some residential broadband ISP accounts do not allow you to run any server processes (such as a web or FTP server) from your location. Your ISP might periodically check for servers, and if it discovers any active servers at your location, it might suspend your account. If you are unsure, see the acceptable use policy of your ISP.

Order of Precedence for Rules

As you define a new rule, it is added to a table in a Rules screen as the last item in the list, as shown in the following figure.

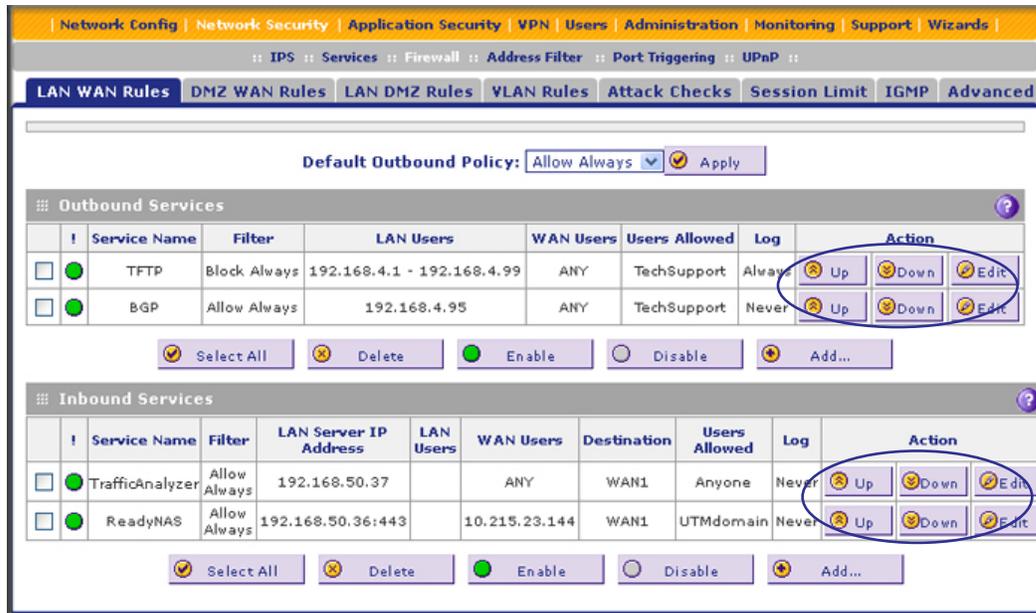


Figure 1. LAN WAN Rules screen showing rules precedence

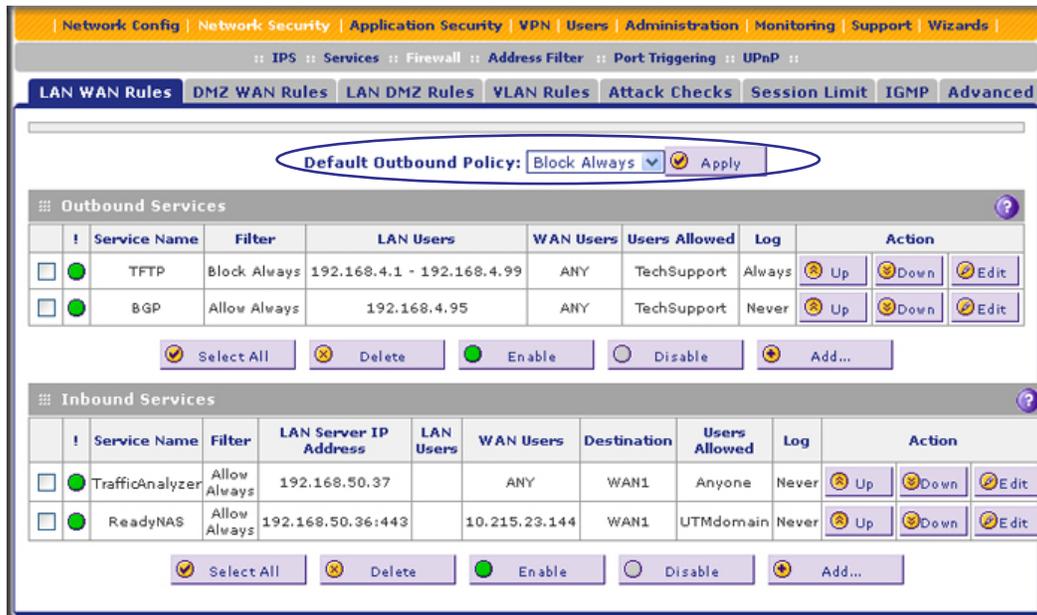
For any traffic attempting to pass through the firewall, the rules apply to the information in the order shown in the rules table, beginning at the top and proceeding to the bottom. In some cases, the order of precedence of two or more rules might be important in determining the disposition of a packet. For example, place the most strict rules at the top (rules with the most specific services or addresses). The Up and Down table buttons in the Action column allow you to relocate a defined rule to a new position in the table.

Set LAN WAN Rules

The default outbound policy is to allow all traffic to the Internet to pass through. Firewall rules can then be applied to block specific types of traffic from going out from the LAN to the Internet (outbound). This feature is also referred to as service blocking. You can change the default policy of Allow Always to Block Always to block all outbound traffic. These policy rules allow you to enable only specific services to pass through the UTM.

➤ To change the default outbound policy:

1. Select **Network Security > Firewall**. The Firewall submenu tabs display, with the LAN WAN Rules screen in view.
2. From the Default Outbound Policy drop-down list, select **Block Always**.



3. Next to the drop-down list, click the **Apply** table button.

➤ **To change an existing outbound or inbound service rule:**

In the Action column to the right of to the rule, click one of the following table buttons:

- **Edit.** Allows you to change the definition of an existing rule. Depending on your selection, either the Edit LAN WAN Outbound Service screen or Edit LAN WAN Inbound Service screen displays, containing the data for the selected rule.
- **Up.** Moves the rule up one position in precedence.
- **Down.** Moves the rule down one position in precedence.

➤ **To enable, disable, or delete one or more rules:**

1. Select the check box to the left of each rule that you want to enable, disable, or delete, or click the **Select All** table button to select all rules.
2. Click one of the following table buttons:
 - **Enable.** Enables the rule or rules. The ! status icon changes from a gray circle to a green circle, indicating that the selected rule or rules are enabled. (By default, when a rule is added to the table, it is automatically enabled.)
 - **Disable.** Disables the rule or rules. The ! status icon changes from a green circle to a gray circle, indicating that the selected rule or rules are disabled.
 - **Delete.** Deletes the selected rule or rules.

LAN WAN Inbound Service Rules

The Inbound Services table lists all existing rules for inbound traffic. If you have not defined any rules, no rules are listed. By default, all inbound traffic (from the Internet to the LAN) is

blocked. Remember that allowing inbound services opens potential security holes in your firewall. Enable only those ports that are necessary for your network.

➤ **To create an inbound LAN WAN service rule:**

1. In the LAN WAN Rules screen, click the **Add** table button under the Inbound Services table. The Add LAN WAN Inbound Service screen displays:

The screenshot shows the 'Add LAN WAN Inbound Service' configuration window. At the top, a status bar indicates 'Operation succeeded.' Below this, the window title is 'Add LAN WAN Inbound Service'. The configuration area contains the following fields and options:

- Service: ANY (dropdown)
- Action: BLOCK always (dropdown)
- Select Schedule: NONE (dropdown)
- Send to Lan Server: Single Address (dropdown)
- Start: [][][][] (input fields)
- End: [][][][] (input fields)
- Translate to Port Number: (checkbox)
- WAN Destination IP Address: WAN1 (dropdown)
- Start: [][][][] (input fields)
- End: [][][][] (input fields)
- LAN Users: Any (dropdown)
- Start: [][][][] (input fields)
- End: [][][][] (input fields)
- WAN Users: Any (dropdown)
- Start: [][][][] (input fields)
- End: [][][][] (input fields)
- Users Allowed: Anyone (dropdown)
- QoS Profile: None (dropdown)
- Log: Never (dropdown)
- Bandwidth Profile: NONE (dropdown)
- Traffic Meter Profile: NONE (dropdown)
- Application Control: NONE (dropdown)

At the bottom of the window, there are two buttons: 'Apply' and 'Reset'.

2. Enter the settings as explained in *Table 3* on page 6.
3. Click **Apply** to save your changes. The new rule is now added to the Inbound Services table.

Inbound Rule Examples

LAN WAN Inbound Rule: Host a Local Public Web Server

If you host a public web server on your local network, you can define a rule to allow inbound web (HTTP) requests. These requests can be from any outside IP address to the IP address of your web server at any time of the day.

The screenshot shows the configuration interface for adding a LAN WAN inbound service. The window title is "Add LAN WAN Inbound Service" and it displays a success message "Operation succeeded." at the top. The configuration fields are as follows:

- Service: HTTP
- Action: ALLOW always
- Select Schedule: NONE
- Send to Lan Server: Single Address
- Start: 192.168.1.99
- End: (empty)
- Translate to Port Number:
- WAN Destination IP Address: WAN1
- Start: (empty)
- End: (empty)
- LAN Users: Any
- Start: (empty)
- End: (empty)
- WAN Users: Any
- Start: (empty)
- End: (empty)
- Users Allowed: Anyone
- QoS Profile: None
- Log: Never
- Bandwidth Profile: NONE
- Traffic Meter Profile: NONE
- Application Control: NONE

At the bottom of the window are "Apply" and "Reset" buttons.

Figure 2. Add a LAN WAN inbound service

LAN WAN Inbound Rule: Allow Videoconference from Restricted Addresses

If you want to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office, you can create an inbound rule (see the following figure). In the example, CU-SeeMe connections are allowed only from a specified range of external IP addresses.

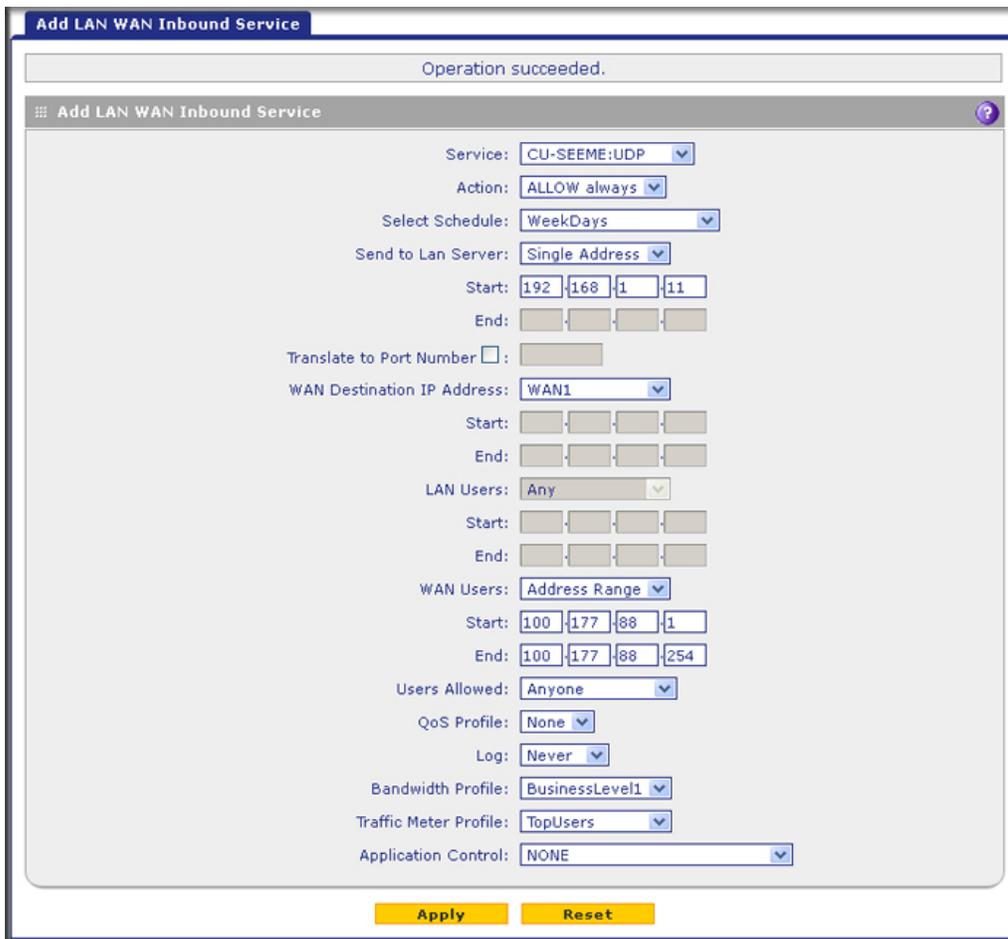


Figure 3. Allow an inbound video service

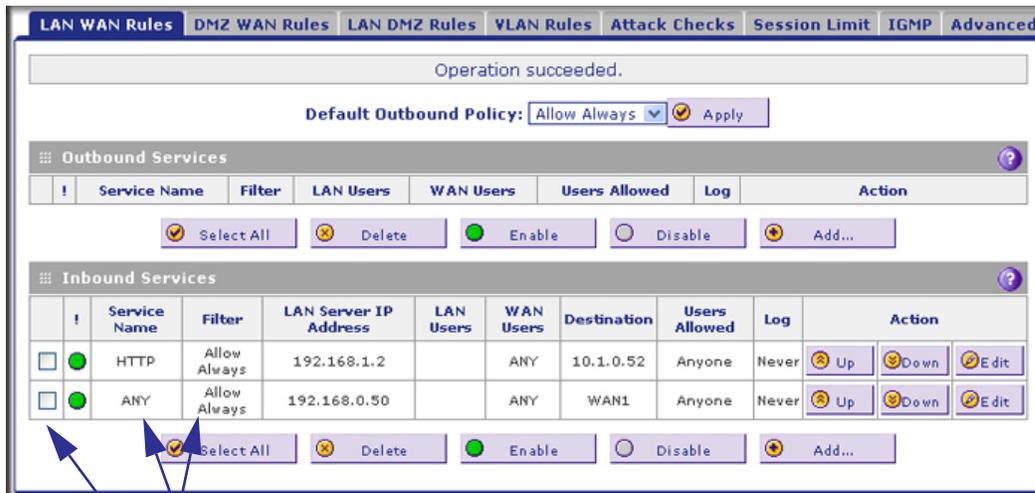
LAN WAN Inbound Rule: Specify an Exposed Host

Specifying an exposed host allows you to set up a computer or server that is available to anyone on the Internet for services that you have not yet defined.

➤ **To expose one of the computers on your LAN as this host:**

1. Create an inbound rule that allows all protocols.
2. Place the rule below all other inbound rules.

See an example in the following figure.



1. Select ANY and Allow Always.
2. Place the rule below all other inbound rules.



WARNING:

For security, NETGEAR strongly recommends that you avoid creating an exposed host. When a computer is designated as the exposed host, it loses much of the protection of the firewall and is exposed to attacks from the Internet. If compromised, the computer can be used to attack your network.

Outbound Rule Example

Outbound rules let you prevent users from using applications such as Instant Messenger, Real Audio, or other nonessential sites.

LAN WAN Outbound Rule: Block Instant Messenger

If you want to block Instant Messenger usage by employees during working hours, you can create an outbound rule to block the application. You can block the application from any internal IP address to any external address according to the schedule that you create in the Schedule screen. See an example in [Figure 4](#).

You can also enable the UTM to log any attempt to use Instant Messenger during the blocked period.

Operation succeeded.

Add LAN WAN Outbound Service

Service: AIM

Action: BLOCK always

Select Schedule: WeekDays

LAN Users: Any

Start: . . .

End: . . .

WAN Users: Any

Start: . . .

End: . . .

Users Allowed: Anyone

QoS Profile: None

Log: Always

Bandwidth Profile: NONE

Traffic Meter Profile: NONE

Application Control: NONE

NAT IP: Auto

Apply Reset

Figure 4. Block Instant Messenger

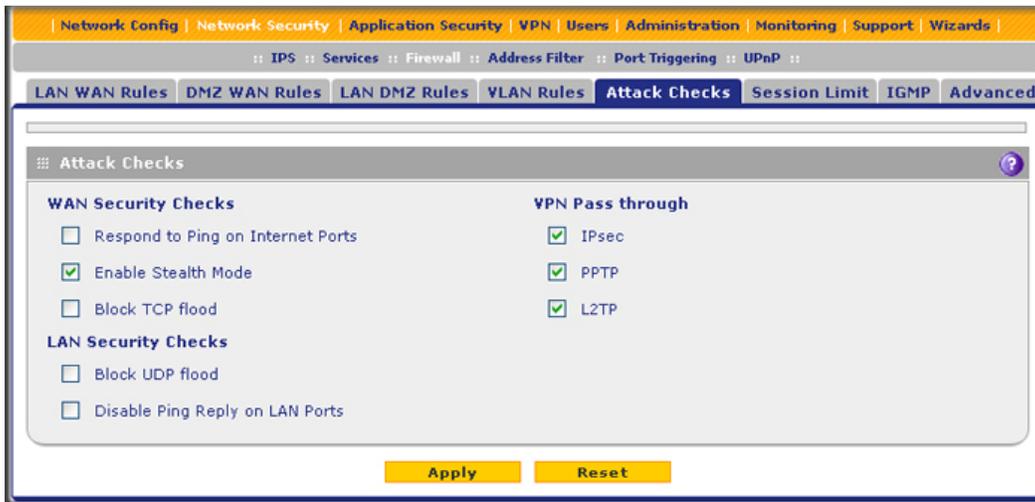
Configure Other Firewall Features

You can configure attack checks, VPN pass-through, and session limits.

Attack Checks and VPN Pass-Through

The Attack Checks screen allows you to protect against common attacks in the LAN and WAN networks. You can also configure VPN pass-through. The various types of attack checks are listed on the Attack Checks screen and defined in [Table 4](#).

- **To enable attack checks for your network environment:**
 1. Select **Network Security > Firewall > Attack Checks**. The Attack Checks screen displays:



2. Enter the settings as explained in the following table:

Table 4. Attack Checks screen settings

Setting	Description
WAN Security Checks	
Respond to Ping on Internet Ports	Select the Respond to Ping on Internet Ports check box to enable the UTM to respond to a ping from the Internet. A ping can be used as a diagnostic tool. Keep this check box cleared unless you have a specific reason to enable the UTM to respond to a ping from the Internet.
Enable Stealth Mode	Select the Enable Stealth Mode check box (which is the default setting) to prevent the UTM from responding to port scans from the WAN, thus making it less susceptible to discovery and attacks.
Block TCP flood	Select the Block TCP flood check box to enable the UTM to drop all invalid TCP packets and to protect the UTM from a SYN flood attack. A SYN flood is a form of denial of service attack in which an attacker sends a succession of SYN (synchronize) requests to a target system. When the system responds, the attacker does not complete the connections, thus leaving the connection half open and flooding the server with SYN messages. No legitimate connections can then be made. By default, the Block TCP flood check box is cleared.

Table 4. Attack Checks screen settings (continued)

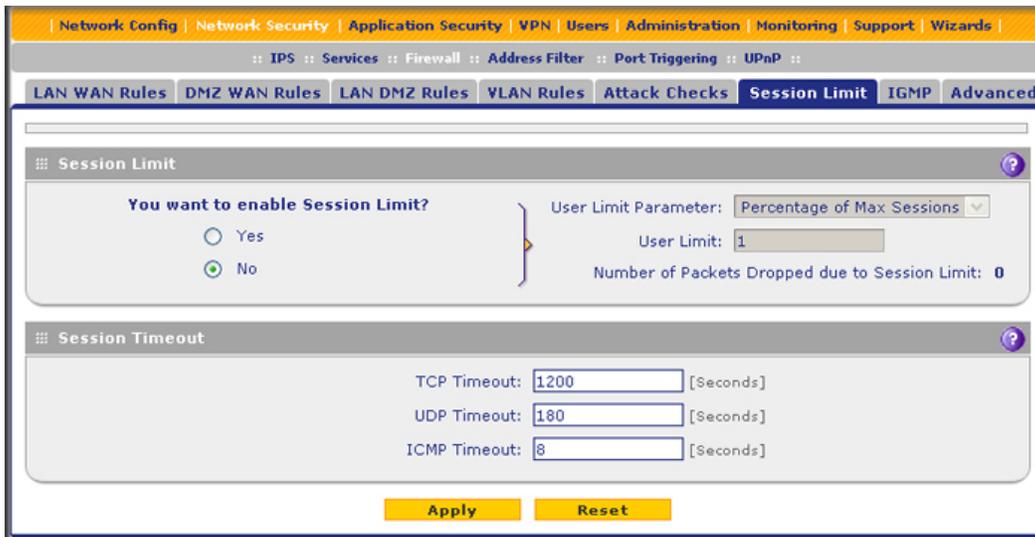
Setting	Description
LAN Security Checks	
Block UDP flood	<p>Select the Block UDP flood check box to prevent the UTM from accepting more than 20 simultaneous, active User Datagram Protocol (UDP) connections from a single device on the LAN. By default, the Block UDP flood check box is cleared.</p> <p>A UDP flood is a form of denial of service attack that can be initiated when one device sends many UDP packets to random ports on a remote host. As a result, the distant host does the following:</p> <ol style="list-style-type: none"> 1. Checks for the application listening at that port. 2. Sees that no application is listening at that port. 3. Replies with an ICMP destination unreachable packet. <p>When the attacked system is flooded, it is forced to send many ICMP packets, eventually making it unreachable by other clients. The attacker might also spoof the IP address of the UDP packets, ensuring that the excessive ICMP return packets do not reach the attacker, thus making the attacker's network location anonymous.</p>
Disable Ping Reply on LAN Ports	<p>Select the Disable Ping Reply on LAN Ports check box to prevent the UTM from responding to a ping on a LAN port. A ping can be used as a diagnostic tool. Keep this check box cleared unless you have a specific reason to prevent the UTM from responding to a ping on a LAN port.</p>
VPN Pass through	
IPSec PPTP L2TP	<p>When the UTM functions in NAT mode, all packets going to the remote VPN gateway are first filtered through NAT and then encrypted according to the VPN policy. For example, if a VPN client or gateway on the LAN side of the UTM wants to connect to another VPN endpoint on the WAN side (placing the UTM between two VPN endpoints), encrypted packets are sent to the UTM. Because the UTM filters the encrypted packets through NAT, the packets become invalid unless you enable the VPN pass-through feature.</p> <p>To enable the VPN tunnel to pass the VPN traffic without any filtering, select any or all of the following check boxes:</p> <ul style="list-style-type: none"> • IPSec. Disables NAT filtering for IPSec tunnels. • PPTP. Disables NAT filtering for PPTP tunnels. • L2TP. Disables NAT filtering for L2TP tunnels. <p>By default, all three check boxes are selected.</p>

3. Click **Apply** to save your settings.

Set Session Limits

The session limits feature allows you to specify the total number of sessions that are allowed, per user, over an IP connection across the UTM. The session limits feature is disabled by default.

- **To enable and configure session limits:**
 1. Select **Network Security > Firewall > Session Limit**. The Session Limit screen displays:



2. Select the **Yes** radio button under Do you want to enable Session Limit?
3. Enter the settings as explained in the following table:

Table 5. Session Limit screen settings

Setting	Description
Session Limit	
User Limit Parameter	From the User Limit Parameter drop-down list, select one of the following options: <ul style="list-style-type: none"> • Percentage of Max Sessions. A percentage of the total session connection capacity of the UTM. • Number of Sessions. An absolute number of maximum sessions.
User Limit	Enter a number to indicate the user limit. If the User Limit Parameter is set to Percentage of Max Sessions, the number specifies the maximum number of sessions that are allowed from a single-source device as a percentage of the total session connection capacity of the UTM. (The session limit is per-device based.) If the User Limit Parameter is set to Number of Sessions, the number specifies an absolute value. Note: Some protocols such as FTP and RSTP create two sessions per connection.
Total Number of Packets Dropped due to Session Limit	This parameter is a nonconfigurable counter that displays the total number of dropped packets when the session limit is reached.
Session Timeout	
TCP Timeout	For each protocol, specify a time-out in seconds. A session expires if no data for the session is received during the time-out period. The default time-out periods are 1200 seconds for TCP sessions, 180 seconds for UDP sessions, and 8 seconds for ICMP sessions.
UDP Timeout	
ICMP Timeout	

4. Click **Apply** to save your settings.

Create Services, QoS Profiles, and Bandwidth Profiles

When you create inbound and outbound firewall rules, you use firewall objects such as services, QoS profiles, bandwidth profiles, traffic meter profiles, and schedules to narrow down the firewall rules:

- **Services.** A service narrows down the firewall rule to an application and a port number. You can also narrow down the firewall rule to a group of services. For information about adding services and service groups, see [Add Customized Services](#) on page 20.
- **IP groups.** An IP group is a LAN group or a WAN group to which you add individual IP addresses. You can narrow down the firewall rule to such an IP group. For information about creating IP groups, see the reference manual.
- **QoS profiles.** A Quality of Service (QoS) profile defines the relative priority of an IP packet for traffic that matches the firewall rule. For information about creating QoS profiles, see [Create Quality of Service Profiles](#) on page 22.
- **Bandwidth profiles.** A bandwidth profile allocates and limits traffic bandwidth for the LAN users to which a firewall rule is applied. For information about creating bandwidth profiles, see [Create Bandwidth Profiles](#) on page 25.
- **Traffic meter profiles.** A traffic meter profile measures downloaded or uploaded traffic, or both, for users to which a firewall rule is applied, and logs or blocks traffic that exceeds the preset limit or limits. For information about creating traffic meter profiles, see [Create Traffic Meter Profiles](#) on page 28.

Note: A schedule narrows down the period during which a firewall rule is applied. For information about specifying schedules, see [Set a Schedule to Block or Allow Specific Traffic](#) on page 31.

Add Customized Services

Services are functions server computers perform at the request of client computers. You can configure up to 125 custom services.

For example, web servers serve web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, the requested service uses a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (web server) request.

The Internet Engineering Task Force (IETF) defines the service numbers for many common protocols. These service numbers are published in RFC 1700, *Assigned Numbers*. Service numbers for other applications are typically chosen from the range 1024–65535 by the authors of the application.

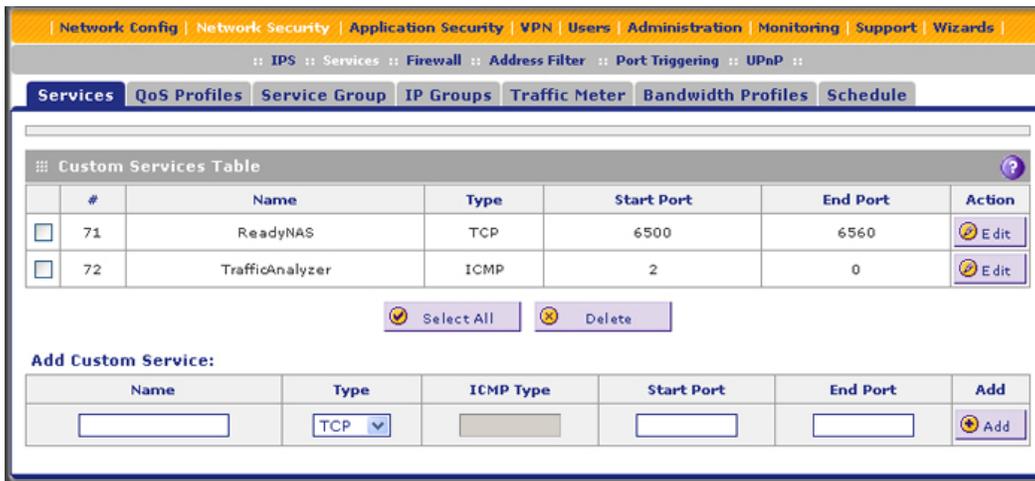
Although the UTM already holds a list of many service port numbers, you are not limited to these choices. Use the Services screen to add additional services and applications to the list for use in defining firewall rules. The Services screen shows a list of services that you have defined, as shown in the following procedure.

To define a new service, first determine which port number or range of numbers the application uses. You can usually determine this information by contacting the publisher of the application, user groups, or newsgroups. When you have the port number information, you can enter it on the Services screen.

You use a customized service as a firewall object to which you apply a firewall rule. Select the customized service from the Service drop-down list on a screen on which you add or edit a firewall rule.

➤ **To add a customized service:**

1. Select **Network Security > Services**. The Services screen displays. The Custom Services table shows the user-defined services. (The following figure shows some examples.)



2. In the Add Customer Service section of the screen, enter the settings as explained in the following table:

Table 6. Services screen settings

Setting	Description
Name	A descriptive name of the service for identification and management purposes.
Type	From the Type drop-down list, select the Layer 3 protocol that the service uses as its transport protocol: <ul style="list-style-type: none"> • TCP • UDP • ICMP

Table 6. Services screen settings (continued)

Setting	Description
ICMP Type	A numeric value that can range from 0 through 40. For a list of ICMP types, go to http://www.iana.org/assignments/icmp-parameters . Note: This field is enabled only when you select ICMP from the Type drop-down list.
Start Port	The first TCP or UDP port of a range that the service uses. Note: This field is enabled only when you select TCP or UDP from the Type drop-down list.
End Port	The last TCP or UDP port of a range that the service uses. If the service uses only a single port number, enter the same number in the Start Port and End Port fields. Note: This field is enabled only when you select TCP or UDP from the Type drop-down list.

3. Click **Apply** to save your settings. The new custom service is added to the Custom Services table.

➤ **To edit a service:**

1. In the Custom Services table, click the **Edit** table button to the right of the service that you want to edit. The Edit Service screen displays:



2. Modify the settings that you wish to change (see the previous table).
3. Click **Apply** to save your changes. The modified service is displayed in the Custom Services table.

➤ **To delete one or more services:**

1. In the Custom Services table, select the check box to the left of each service that you want to disable. You can click the **Select All** table button to select all services.
2. Click the **Delete** table button.

Create Quality of Service Profiles

A Quality of Service (QoS) profile defines the relative priority of an IP packet when multiple connections are scheduled for simultaneous transmission on the UTM. A QoS profile

becomes active only when it is associated with a nonblocking inbound or outbound firewall rule. The UTM processes the traffic matching the firewall rule.

After you have created a QoS profile, you can assign the profile to firewall rules and application control profiles on the following screens:

- Add LAN WAN Outbound Services screen (see the reference manual).
- Add LAN WAN Inbound Services screen (see [LAN WAN Inbound Service Rules](#) on page 11).
- Application Control Policy pop-up screens. You can access these pop-up screens from the Add or Edit Application Control Profile screen (see the reference manual).

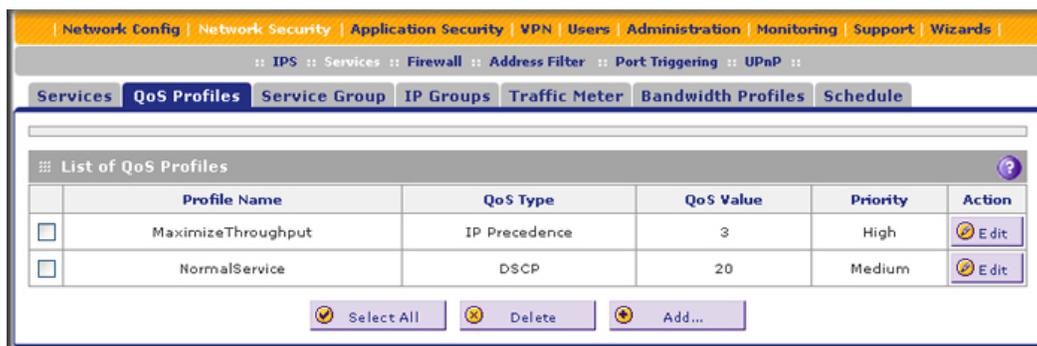
The Type of Service (ToS) in the Internet Protocol Suite standards, RFC 1349 defines the priorities.

There are no default QoS profiles on the UTM. Following are examples of QoS profiles that you *could* create:

- **Normal service profile.** Used when no special priority is given to the traffic. You would typically mark the IP packets for services with this priority with a ToS value of 0.
- **Minimize-cost profile.** Used when data must be transferred over a link that has a lower cost. You would typically mark the IP packets for services with this priority with a ToS value of 1.
- **Maximize-reliability profile.** Used when data must travel to the destination over a reliable link and with little or no retransmission. You would typically mark the IP packets for services with this priority with a ToS value of 2.
- **Maximize-throughput profile.** Used when the volume of data transferred during an interval is important even if the latency over the link is high. You would typically mark the IP packets for services with this priority with a ToS value of 3 or 4.
- **Minimize-delay profile.** Used when the time required (latency) for the packet to reach the destination must be low. You would typically mark the IP packets for services with this priority with a ToS value of 7.

➤ **To create a QoS profile:**

1. Select **Network Security > Services > QoS Profiles**. The QoS Profiles screen displays. The following figure shows some profiles in the List of QoS Profiles table as an example.



- Under the List of QoS Profiles table, click the **Add** table button. The Add QoS Profile screen displays:

- Enter the settings as explained in the following table.

Note: This document assumes that you are familiar with QoS concepts such as QoS priority queues, IP precedence, DHCP, and their values. See the reference manual for more detailed descriptions.

Table 7. Add QoS Profile screen settings

Setting	Description
Profile Name	A descriptive name of the QoS profile for identification and management purposes.
Re-Mark	Select the Re-Mark check box to set the differentiated services (DiffServ) mark in the Type of Service (ToS) byte of an IP header by specifying the QoS type (IP precedence or DHCP) and QoS value. If you clear the Re-Mark check box, the QoS type and QoS value are ignored, and you can configure the QoS priority only.
QoS	From the QoS drop-down list, select one of the following traffic classification methods: <ul style="list-style-type: none"> IP Precedence. A legacy method that sets the priority in the ToS byte of an IP header. DSCP. A method that sets the Differentiated Services Code Point (DSCP) in the Differentiated Services (DS) field (the same as the ToS byte) of an IP header.

Table 7. Add QoS Profile screen settings (continued)

Setting	Description
QoS Value	The QoS value in the ToS or DiffServ byte of an IP header. The QoS value that you enter depends on your selection from the QoS drop-down list: <ul style="list-style-type: none"> For IP precedence, select a value from 0 to 7. For DSCP, select a value from 0 to 63.
QoS Priority	From the QoS Priority drop-down list, select one of the following priority queues: <ul style="list-style-type: none"> Default High Medium High Medium Low

- Click **Apply** to save your settings. The new QoS profile is added to the List of QoS Profiles table.

➤ **To edit a QoS profile:**

- In the List of QoS Profiles table, click the **Edit** table button to the right of the QoS profile that you want to edit. The Edit QoS Profile screen displays.
- Modify the settings that you wish to change (see the previous table).
- Click **Apply** to save your changes. The modified QoS profile is displayed in the List of QoS Profiles table.

➤ **To delete one or more QoS profiles:**

- In the List of QoS Profiles table, select the check box to the left of each QoS profile that you want to delete. You can click the **Select All** table button to select all profiles.
- Click the **Delete** table button.

Create Bandwidth Profiles

Bandwidth profiles determine how data is communicated with the hosts. The purpose of bandwidth profiles is to provide a method for allocating and limiting traffic. Profiles can allocate LAN users sufficient bandwidth while preventing them from consuming all the bandwidth on your WAN link. A single bandwidth profile can be for both outbound and inbound traffic.

For outbound traffic, you can apply bandwidth profiles on the available WAN interfaces in both the primary WAN mode and auto-rollover modes, and in load balancing mode on the interface that you specify. For inbound traffic, you can apply bandwidth profiles to a LAN interface for all WAN modes.

When a device establishes a new connection, the device locates the firewall rule corresponding to the connection.

- If the rule has a bandwidth profile specification, the device creates a bandwidth class in the kernel.

- If multiple connections correspond to the same firewall rule, the connections use the same bandwidth class.

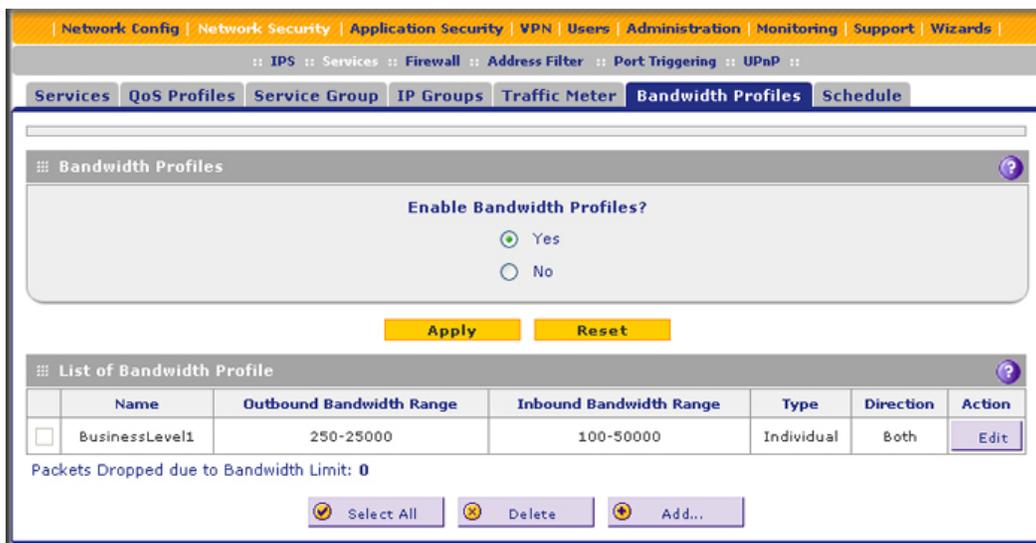
If the classes are per-source IP address classes, an exception occurs for an individual bandwidth profile. The source IP address is the IP address of the first packet that is transmitted for the connection. So for outbound firewall rules, the source IP address is the LAN-side IP address. For inbound firewall rules, the source IP address is the WAN-side IP address. The class is deleted when all the connections that are using the class expire.

After you have created a bandwidth profile, you can assign the profile to firewall rules and application control profiles on the following screens:

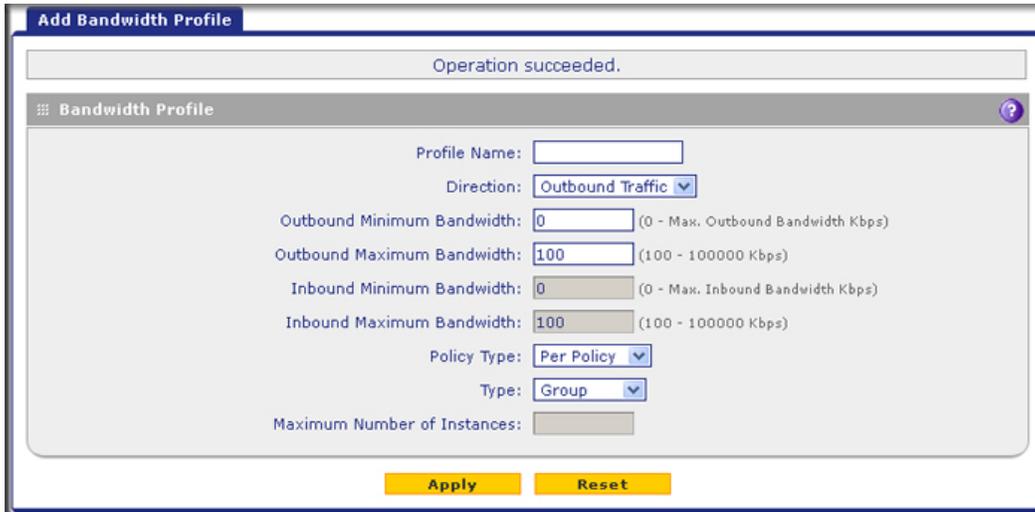
- Add LAN WAN Outbound Services screen (see the reference manual).
- Add LAN WAN Inbound Services screen (see *Figure 2* on page 12).
- Application Control Policy pop-up screens. You can access these pop-up screens from the Add or Edit Application Control Profile screen (see the reference manual).

➤ **To add and enable a bandwidth profile:**

1. Select **Network Security > Services > Bandwidth Profiles**. The Bandwidth Profiles screen displays. The following figure shows one user-defined profile in the List of Bandwidth Profiles table as an example.



2. Under the List of Bandwidth Profiles table, click the **Add** table button. The Add Bandwidth Profile screen displays:



3. Enter the settings as explained in the following table:

Table 8. Add Bandwidth Profile screen settings

Setting	Description
Profile Name	A descriptive name of the bandwidth profile for identification and management purposes.
Direction	From the Direction drop-down list, select the traffic direction for the bandwidth profile: <ul style="list-style-type: none"> • Outbound Traffic. The bandwidth profile is applied only to outbound traffic. Specify the outbound minimum and maximum bandwidths. • Inbound Traffic. The bandwidth profile is applied only to inbound traffic. Specify the inbound minimum and maximum bandwidths. • Both. The bandwidth profile is applied to both outbound and inbound traffic. Specify both the outbound and inbound minimum and maximum bandwidths.
Outbound Minimum Bandwidth	The outbound minimum allocated bandwidth in Kbps. The default setting is 0 Kbps.
Outbound Maximum Bandwidth	The outbound maximum allowed bandwidth in Kbps. The default setting is 100 Kbps (you cannot configure less than 100 Kbps). The maximum allowable bandwidth is 100,000 Kbps.
Inbound Minimum Bandwidth	The inbound minimum allocated bandwidth in Kbps. The default setting is 0 Kbps.
Inbound Maximum Bandwidth	The inbound maximum allowed bandwidth in Kbps. The default setting is 100 Kbps (you cannot configure less than 100 Kbps); the maximum allowable bandwidth is 100,000 Kbps.

Table 8. Add Bandwidth Profile screen settings (continued)

Setting	Description		
Policy Type	<p>From the Policy Type drop-down list, select how the policy is applied when it is assigned to multiple firewall rules:</p> <ul style="list-style-type: none"> • Per Policy. The policy limits apply to each firewall rule separately. For example, an outbound maximum bandwidth of 25,000 Kbps would apply to each firewall rule to which the policy is assigned. • All Policies. The policy limits apply to all firewall rules. For example, all firewall rules to which the policy is assigned use an outbound maximum bandwidth of 25,000 Kbps. 		
Type	<p>From the Type drop-down list, select the type for the bandwidth profile:</p> <ul style="list-style-type: none"> • Group. The profile applies to all users, that is, all users share the available bandwidth. • Individual. The profile applies to an individual user, that is, each user can use the available bandwidth. 		
	<table border="1"> <tr> <td>Maximum Number of Instances</td> <td>If you select Individual from the Type drop-down list, you must specify the maximum number of class instances that the individual bandwidth profiles can create.</td> </tr> </table>	Maximum Number of Instances	If you select Individual from the Type drop-down list, you must specify the maximum number of class instances that the individual bandwidth profiles can create.
Maximum Number of Instances	If you select Individual from the Type drop-down list, you must specify the maximum number of class instances that the individual bandwidth profiles can create.		

4. Click **Apply** to save your settings. The new bandwidth profile is added to the List of Bandwidth Profiles table.
5. In the Bandwidth Profiles section of the screen, select the **Yes** radio button under Enable Bandwidth Profiles? By default the No radio button is selected.
6. Click **Apply** to save your setting. You now can select the profile when you create or change a firewall rule.

➤ **To edit a bandwidth profile:**

1. In the List of Bandwidth Profiles table, click the **Edit** table button to the right of the bandwidth profile that you want to edit. The Edit Bandwidth Profile screen displays.
2. Modify the settings that you wish to change (see the previous table).
3. Click **Apply** to save your changes. The modified bandwidth profile is displayed in the List of Bandwidth Profiles table.

➤ **To delete one or more bandwidth profiles:**

1. In the List of Bandwidth Profiles table, select the check box to the left of each bandwidth profile that you want to delete. You can click the **Select All** table button to select all profiles.
2. Click the **Delete** table button.

Create Traffic Meter Profiles

Traffic meter profiles allow you to measure and control traffic that users download and upload. When traffic for a profile has reached its configured limit, you can either log or block the traffic. A traffic meter profile differs from the WAN traffic meter (see the reference manual) in that it applies to one or more firewall rules instead of a WAN interface. A single bandwidth

profile can be used for both downloaded and uploaded traffic. When applied to multiple firewall rules, a single profile can be applied to each firewall rule separately, or to all firewall rules together.

After you have created a traffic meter profile, you can assign the profile to firewall rules and application control profiles on the following screens:

- Add LAN WAN Outbound Services screen (see the reference manual).
- Add LAN WAN Inbound Services screen (see *Figure 2* on page 12).
- Application Control Policy pop-up screens. You can access these pop-up screens from the Add or Edit Application Control Profile screen (see the reference manual).

➤ **To add a traffic meter profile:**

1. Select **Network Security > Services > Traffic Meter**. The Traffic Meter screen displays. The following figure shows two profiles in the List of Traffic Meter Profiles table as an example.

Profile Name	Traffic Direction	Limit	Download (MB)	Upload (MB)	Action
<input type="checkbox"/> TopUsers	Both	Download - 500 MB Daily ; Upload - 250 MB Daily	0	0	<input type="button" value="Edit"/> <input type="button" value="Reset"/>
<input type="checkbox"/> OffendingUsers	Both	Download - 1500 MB Daily ; Upload - 500 MB Daily	0	0	<input type="button" value="Edit"/> <input type="button" value="Reset"/>

Note: If a traffic meter profile is assigned to a firewall rule, the *Download (MB)* and *Upload (MB)* columns display the downloaded and uploaded traffic in MB. To reset the traffic meter for a profile, click the **Reset** table button to the right of the profile.

2. Under the List of Traffic Meter Profiles table, click the **Add** table button. The Add Traffic Meter Profile screen displays:

Operation succeeded.

Add Traffic Meter Profile

Profile Name:

Direction:

Download Limit: (MB)

Upload Limit: (MB)

When Limit is reached: Block All Traffic Log Only

Policy Type:

- Enter the settings as explained in the following table:

Table 9. Add Traffic Meter Profile screen settings

Setting	Description
Profile Name	A descriptive name of the traffic meter profile for identification and management purposes.
Direction	From the Direction drop-down list, select the traffic direction for the bandwidth profile: <ul style="list-style-type: none"> Download only. The traffic meter profile is applied only to downloaded traffic. Specify the download limit and measurement period. Upload only. The traffic meter profile is applied only to uploaded traffic. Specify the upload limit and measurement period. Both. The traffic meter profile is applied to both downloaded and uploaded traffic. Specify both the download and upload limits and measurement periods.
Download Limit	Enter the download limit in MB, upload limit in MB, or both. Then, from the drop-down list, for each limit, select the period to which the limit applies: <ul style="list-style-type: none"> Daily. The limit applies to one day and is reset after one day at 00.00 AM. Weekly. The limit applies to one week and is reset on Sunday at 00.00 AM. Monthly. The limit applies to one month and is reset on the first day of the next month at 00.00 AM.
Upload Limit	
When Limit is reached	From the Direction drop-down list, select the action to occur when the limit is reached: <ul style="list-style-type: none"> Block All Traffic. The traffic that you selected from the Direction drop-down list is blocked. Log Only. Traffic is not blocked but logged.
Policy Type	From the Policy Type drop-down list, select how the policy is applied when it is assigned to multiple firewall rules: <ul style="list-style-type: none"> Per Policy. The policy limits apply to each firewall rule separately. For example, a download limit of 1000 MB would apply to each firewall rule to which the policy is assigned. All Policies. The policy limits apply to all firewall rules together. For example, a download limit of 1000 MB applies to all firewall rules to which the policy is assigned.

- Click **Apply** to save your settings. The new traffic meter profile is added to the List of Traffic Meter Profiles table. You now can select the profile when you create or change a firewall rule.

➤ **To edit a traffic meter profile:**

- In the List of Traffic Meter Profiles table, click the **Edit** table button to the right of the traffic meter profile that you want to edit. The Edit Traffic Meter Profile screen displays.
- Modify the settings that you wish to change (see the previous table).
- Click **Apply** to save your changes. The modified traffic meter profile is displayed in the List of Traffic Meter Profiles table.

➤ **To delete one or more traffic meter profiles:**

1. In the List of Traffic Meter Profiles table, select the check box to the left of each traffic meter profile that you want to delete. You can click the **Select All** table button to select all profiles.
2. Click the **Delete** table button.

Set a Schedule to Block or Allow Specific Traffic

Schedules define the time frames under which firewall rules can be applied. You can create multiple schedules and select any one them when defining firewall rules.

➤ **To add a schedule:**

1. Select **Network Security > Services > Schedule**. The Schedule screen displays. The following figure shows two schedules in the List of Schedules table as an example.

Profile Name	Description	Scheduled Days	Scheduled Time of Day	Action
<input type="checkbox"/> WeekDays	7AM-8PM	Mon,Tue,Wed,Thur,Fri,	7. 0 AM - 5. 0 PM; 5. 5 PM - 8. 0 PM	<input type="button" value="Edit"/>
<input type="checkbox"/> WeekendTechSupport	Firewall Schedule	Sat,Sun	All day	<input type="button" value="Edit"/>

2. Under the List of Schedules table, click the **Add** table button. The Add Schedule screen displays:

3. Enter the settings as explained in the following table:

Table 10. Add Schedule screen settings

Setting	Description
Profile Name	A name of the schedule for identification and management purposes.
Description	A description for identification and management purposes.
Scheduled Days	
Select one of the following radio buttons:	
<ul style="list-style-type: none"> • All Days. The schedule is in effect all days of the week. • Specific Days. The schedule is in effect only on specific days. To the right of the radio buttons, select the check box for each day that you want the schedule to be in effect. 	

Table 10. Add Schedule screen settings (continued)

Setting	Description
Scheduled Time of Day	
<p>Select one of the following radio buttons:</p> <ul style="list-style-type: none"> • All Day. The schedule is in effect all hours of the selected day or days. • Specific Times. The schedule is in effect only during specific periods of the selected day or days. To the right of the radio buttons, fill in the Start Time and End Time fields (Hour, Minute). Make a selection from the AM/PM drop-down lists to specify the periods during which the schedule is in effect. <p>Note: To add another period to the schedule, click + (plus). This option allows you to specify two distinctive periods within one 24-hour period.</p>	

4. Click **Apply** to save your settings. The new schedule is added to the List of Schedules table. You now can select the schedule when you create or change a firewall rule.

➤ **To edit a schedule:**

1. In the List of Schedules table, click the **Edit** table button to the right of the schedule that you want to edit. The Edit Schedule screen displays.
2. Modify the settings that you wish to change (see the previous table).
3. Click **Apply** to save your changes. The modified schedule is displayed in the List of Schedules table.

➤ **To delete one or more schedules:**

1. In the List of Schedules table, select the check box to the left of each schedule that you want to delete or click the **Select All** table button to select all schedules.
2. Click the **Delete** table button.

Use the Intrusion Prevention System

The intrusion prevention system (IPS) of the UTM monitors all network traffic to detect, in real time, distributed denial-of-service (DDoS) attacks, network attacks, and port scans, and protects your network from such intrusions. You can set up alerts, block source IP addresses from which port scans are initiated, and drop traffic that carries attacks. You can configure detection of and protection from specific attacks such as web, email, database, malware, and other attacks. The IPS differs from the malware scan mechanism in that it monitors individual packets, whereas the malware scan mechanism monitors files.

The IPS also allows you to configure port scan detection according to your needs and to protect the network from unwanted port scans that could compromise the network security.

The IPS is disabled by default.

➤ **To enable intrusion prevention:**

1. Select **Network Security > IPS**. The IPS screen displays.

2. To enable the IPS, select the **Yes** radio button in the IPS section of the screen. The default setting is **No**.
3. Click **Apply** to save your settings.

Note: When you enable the IPS, the default IPS configuration goes into effect. The default IPS configuration is the configuration that the IPS screen returns to when you press the Factory Default reset button.

➤ **To configure intrusion prevention:**

1. Select **Network Security > IPS**. The IPS screen displays.
2. Enter the settings as explained in the following table:

Table 11. IPS screen settings

Setting	Description
Anomaly Behavior Settings	
Detect Port Scans	Detect the action that is taken when the UTM detects a port scan: <ul style="list-style-type: none"> • Alert. An alert is emailed to the administrator that is specified on the Email Notification screen. • Disable. Port scan detection is disabled. This setting is the default. • Block Source IP for. The IP address of the computer that scans the port is blocked for the duration that you specify in the Seconds field. The default setting is 300 seconds.
Detect DDoS	Detect the action that is taken when the UTM detects a DDoS attack: <ul style="list-style-type: none"> • Alert. An alert is emailed to the administrator that is specified on the Email Notification screen. • Disable. DDoS attack detection is disabled. • Block Source IP for. The IP address of the attacking computer is blocked for the duration that you specify in the Seconds field. The default setting is 300 seconds. This setting is the default.

Table 11. IPS screen settings (continued)

Setting	Description
Security Category Settings	
<p>This section displays the different categories of attacks such as Web, Mail, and Databases. The Action column shows the default settings (Disable, Drop, or Alert).</p> <p>In the Action column for each category, select the actions for individual attacks by making selections from the drop-down lists to the right of the names. You can also select a global action for all attacks for a category. Make a selection from the category top drop-down list. Some of the less familiar web and miscellaneous attacks are explained in Table 12 on page 37.</p> <p>The drop-down lists let you select one of the following actions:</p> <ul style="list-style-type: none"> • Disable. The IPS does not control the application. • Drop. The traffic that carries the attack is dropped, and an alert is logged. • Alert. An alert is logged but the traffic that carries the attack is not dropped. <p>The default action for all attacks is Disabled, except for the following attacks, for which the default action is Drop:</p> <ul style="list-style-type: none"> • Web attacks. XSS, IIS, Apache, PHP, CGI, Web-Client, Web-Attack, Web-Misc. • Databases. SQL-injection. • Misc. ShellCode. 	

3. Click **Apply** to save your settings.

Note: The IPS also scans traffic that passes on the UTM's VLANs and on the secondary IP addresses that you have configured on the LAN Multi-homing screen (see the reference manual).

ProSecure Unified Threat Management (UTM) Appliance

[Network Config](#) | [Network Security](#) | [Application Security](#) | [VPN](#) | [Users](#) | [Administration](#) | [Monitoring](#) | [Support](#) | [Wizards](#) |

:: IPS :: Services :: Firewall :: Address Filter :: Port Triggering :: UPnP ::

IPS

:: IPS ?

Do you want to enable IPS?
 Yes No

:: Anomaly Behavior Settings ?

Detect Port Scans Alert Disable Block Source IP for Seconds

Detect DDoS Alert Disable Block Source IP for Seconds

:: Security Category Settings ?

Category	Name	Action
Web	All Web attacks	- Select -
	XSS	Drop
	IIS	Drop
	Apache	Drop
	PHP	Drop
	CGI	Drop
	Web-Client	Drop
	Web-Attack	Drop
	Web-Misc	Drop
Inappropriate	Disable	
Category	Name	Action
Mail	All Mail attacks	- Select -
	SMTP	Disable
	POP3	Disable
	IMAP	Disable
Category	Name	Action
Databases	All Databases attacks	- Select -
	Oracle	Disable
	MicrosoftSQL	Disable
	MySQL	Disable
	PostgreSQL	Disable
	DB2	Disable
	SQL-injection	Drop

Category	Name	Action
Application	All Application attacks	- Select -
	IM	Disable
	P2P	Disable
	Media	Disable
	Tunnel	Disable
	Game	Disable
	Adobe	Disable
	Apple	Disable
	Microsoft	Disable
Category	Name	Action
Malware	All Malware attacks	- Select -
	Exploit	Drop
	Virus	Disable
	Worm	Disable
	Backdoor	Disable
	Trojan	Disable
	Bot	Disable
Category	Name	Action
Network Protocol	All Network Protocol attacks	- Select -
	FTP	Disable
	ICMP	Disable
	SNMP	Disable
	NNTP	Disable
	SIP	Disable
Category	Name	Action
Misc	All Misc attacks	- Select -
	Policy	Disable
	ProtocolNormalization	Disable
	ShellCode	Drop
	Misc	Disable

- Click **Apply** to save your settings.

The following table explains some of the less familiar attack names in the IPS:

Table 12. IPS: uncommon attack names

Attack Name	Description
Web	
Web-Misc	Detects some specific web attack tools, such as the fingerprinting tool and the password-cracking tool.

Table 12. IPS: uncommon attack names (continued)

Attack Name	Description
Web-Attacks	Detects the web attacks that cannot be placed under other web categories, such as DoS and overflow attacks against specific web services. These web services include IMail Web Calendaring, ZixForum, ScozNet, ScozNews, and other services.
Inappropriate	Detects traffic that involves visiting pornographic websites.
Misc	
Policy	Detects traffic that violates common policies, such as traffic that flows because of certain network installer applications, and traffic that flows when Google SafeSearch is turned off.
ProtocolNormalization	Detects an attempt to set all protocols to their standard formats.
ShellCode	Detects shell code, which can initiate an attack.
Misc	Detects the web attacks that cannot be placed in other categories, such as attacks specifically against SNMP or DNS.

What to Do Next

You can further refine your control using the following features described in the reference manual:

- Groups and hosts
- Services
- Schedules
- Allow or block sites and applications
- Source MAC filtering
- Port triggering
- Content filtering
- Monitor blocked content and malware threats in real time
- Log and email attack and other information to an email address