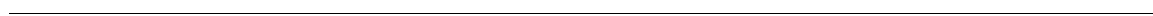




Service Managed Gateway™

How to Configure a Firewall

Issue 1.3
Date 10 March 2006



1	Introduction	3
1.1	What is a firewall?.....	3
1.2	The benefits of using a firewall	3
2	How to configure firewall settings on your SMG	5
2.1	Enabling a firewall.....	5
2.2	Configuring firewall settings	6
2.3	Configuring traffic direction permissions	7
2.4	Specifying local server addresses.....	9
2.5	Enabling Firewall filters.....	12
2.6	Enabling logging services	14
2.7	Saving your configuration	17

© 2007 Virtual Access (Irl) Ltd. This material is protected by copyright. No part of this material may be reproduced, distributed, or altered without the written consent of Virtual Access. All rights reserved. All trademarks, service marks, registered trademarks and registered service marks are the property of their respective owners. Virtual Access is an ISO 9001 certified company.



1 Introduction

1.1 What is a firewall?

A firewall is a system or device that increases network security by policing access to and from a private network. Its principal functions are to block and permit specific or unauthorized traffic between networks. It does this by evaluating incoming and outgoing data packets according to a specified set of security criteria.

A firewall can consist of hardware, software, or a combination of both. It is typically implemented on the router or SMG that separates the private network from the public network. A network that has multiple entry points therefore requires a firewall at each point. Firewalls may also be positioned within networks to protect groups of devices within networks.

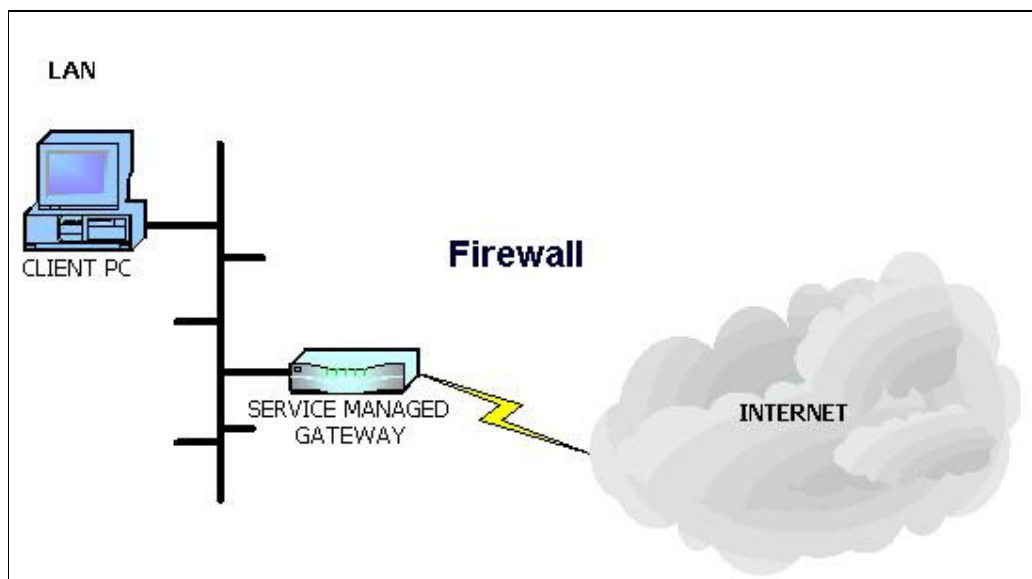


Figure 1: A firewall on a network

It's easy to configure a firewall on your Service Managed Gateway using the Firewall Wizard in the SMG's embedded web. This wizard allows you to easily specify security criteria for the firewall to use while inspecting incoming and outgoing packets.

1.2 The benefits of using a firewall

There are several advantages to configuring and using a firewall on a local network. These include increased security without large administrative overheads and enforcement of network policies such as appropriate Internet access.

A firewall can protect against attacks on the local network, by screening traffic using predefined security filters. In this way the firewall can block mischievous and suspicious packets and warn of potentially dangerous traffic between networks.

Note: On its own, a firewall may not be sufficient to protect sensitive data on a network. Instead, a firewall should form part of a comprehensive security policy.

A firewall represents a single point at which incoming and outgoing data can be inspected. This reduces the administrative load of maintaining security on the local network.

A firewall can prevent calls to specified addresses and services from the local network. This means that you can configure a firewall to prevent local network users from accessing inappropriate material from other networks, such as the Internet. This can represent a convenient way of enforcing an internal company restriction on Internet access.

2 How to configure firewall settings on your SMG

Before you can specify firewall criteria on your Service Managed Gateway, you must first configure an Internet connection. You set this up using the Connection Wizard (see the appropriate Application and Configuration Guide for the connection type).

2.1 Enabling a firewall

To configure firewall settings on your Internet-connected Service Managed Gateway, you must first enable the firewall on your SMG. To do this, click the Fast Start icon on the start page:

On the welcome page that opens, click the **Security** button.

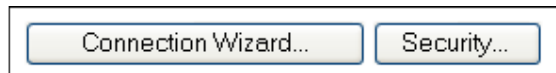


Figure 2: The buttons on the Fast.Start home page

The Security Settings page appears:

Security Settings for your Service Managed Gateway

Firewall Available ▼

VPN Enabled ▼

Secure Management Access Only ▼

Allow Internet Access when VPN enabled ▼

System password

Re-enter password

Local read-only password

Re-enter password

Allow remote logins ▼

Use system password for ▼

Figure 3: The Security Settings page

In the Firewall Enabled field, select 'yes' from the drop-down menu. Now click **OK** and reload your SMG when prompted.

Note: Remember to first configure your Internet connection. The Firewall wizard will not function correctly unless this connection has been configured.

Once your SMG has reloaded, click the Fast Start icon on the start page to go to the Welcome page again, where an additional button called Firewall Wizard appears.

2.2 Configuring firewall settings

When you have enabled the Firewall wizard (see above), click the fast start icon to open the Welcome page. The Firewall Wizard button should appear.

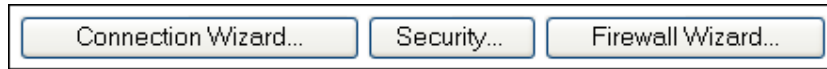


Figure 4: The buttons that are on the Welcome page after you have enabled the Firewall wizard

Click the **Firewall Wizard** button. This opens the Firewall Options page of the Firewall Wizard:

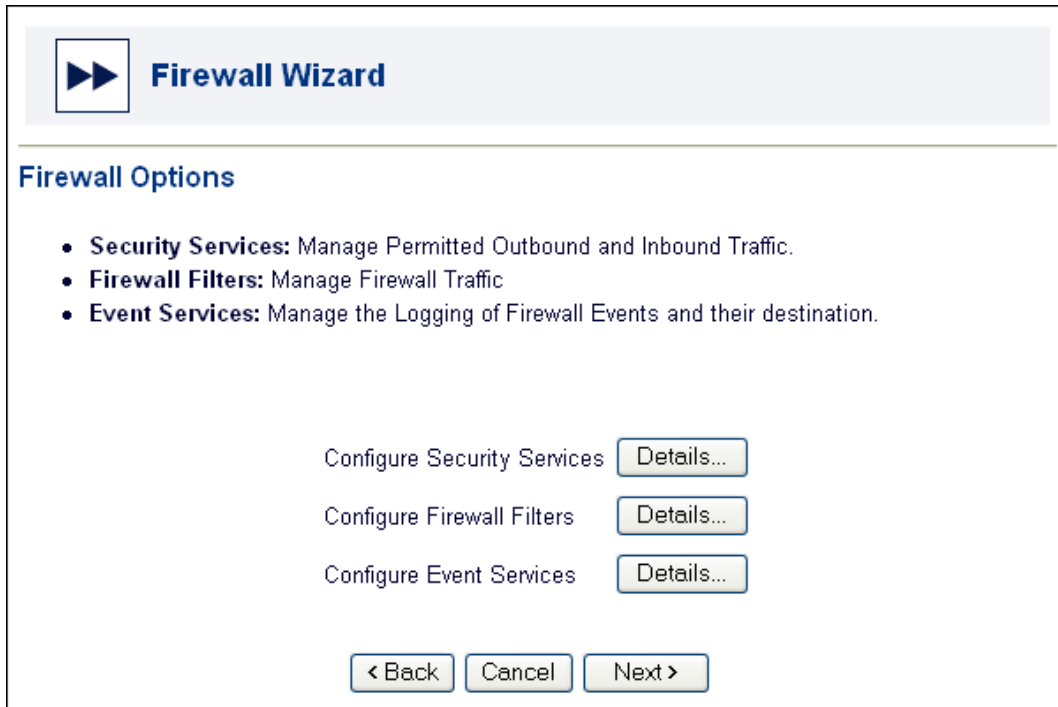


Figure 5: The Firewall Options page

This page contains three fields:

- **Configure Security Services** – use this to set incoming and outgoing traffic permissions to and from server IP addresses
- **Configure Firewall Filters** – use this to configure security criteria for filtering traffic
- **Configure Event Services** – use this to specify whether events related to firewall services are logged, and if they are, where the logged information is stored.

Enable Security Services

To control access permissions between local servers and outside networks, click **Details** next to Configure Security Services.



Figure 6: Configure Security Services

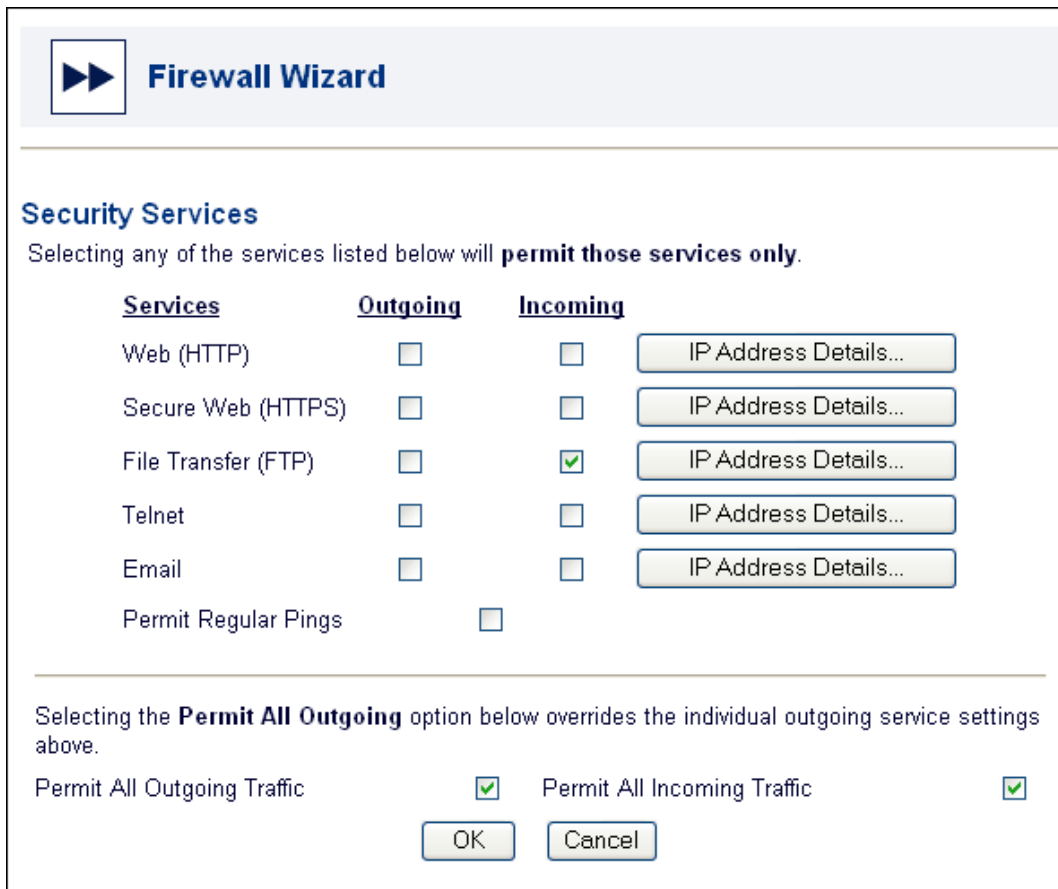


Figure 7: The Security Services pop-up window.

2.3 Configuring traffic direction permissions

By default, all outgoing connections are permitted and all incoming connections are blocked. You can see this in Figure 7.

To allow incoming traffic through the firewall, you either check the individual traffic types or check the Permit All Incoming Traffic box. (The Permit All Incoming Traffic checkbox refers only to the services outlined on this page of the wizard.)

To limit the permission or direction of services, you check or uncheck the specific Outgoing and Incoming checkboxes associated with each service as appropriate:

▶▶ **Firewall Wizard**

Security Services

Selecting any of the services listed below will **permit those services only**.

Services	Outgoing	Incoming	
Web (HTTP)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	IP Address Details...
Secure Web (HTTPS)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	IP Address Details...
File Transfer (FTP)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	IP Address Details...
Telnet	<input type="checkbox"/>	<input type="checkbox"/>	IP Address Details...
Email	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	IP Address Details...
Permit Regular Pings	<input type="checkbox"/>		

Selecting the **Permit All Outgoing** option below overrides the individual outgoing service settings above.

Permit All Outgoing Traffic

 Permit All Incoming Traffic

Figure 8: The Security Services pop-up window. Outgoing web, secure web, FTP, and email are permitted. Incoming web and email are permitted.

You can block all traffic by unchecking all Outgoing, Incoming, Permit All Outgoing Traffic, and Permit All Incoming Traffic checkboxes:

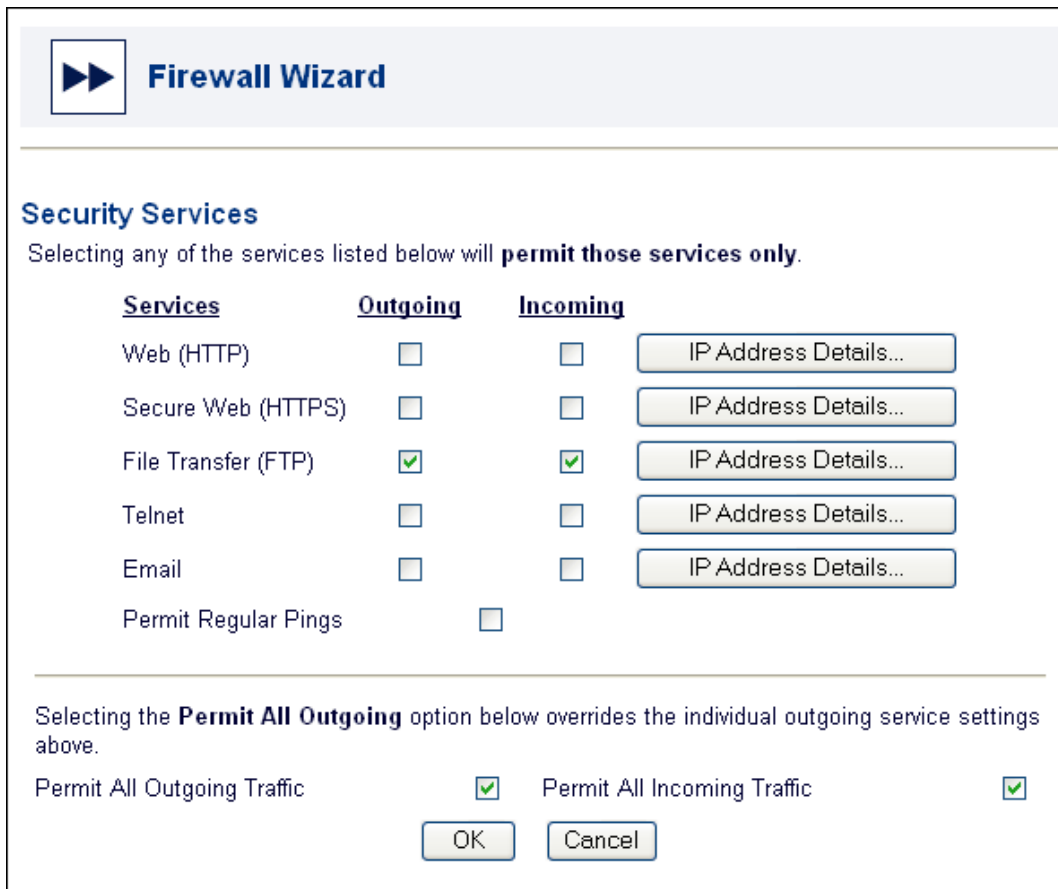


Figure 9: The Security Services pop-up window

Note: If you uncheck all boxes, packets can still be routed on the local (internal) LAN.

You can configure additional options through the Expert View on your Service Managed Gateway. Contact your vendor for more details.

2.4 Specifying local server addresses

For each service listed on the Security Services page, you can specify between one and four local server addresses for permitted incoming traffic. These IP addresses have no relevance to the outgoing traffic.

If IP Address Translation (IPAT) is enabled, you specify a single default host IP address for each service type (this will be reflected in the wizard interface). All incoming traffic on a particular service type will be sent to this specified host because the IPAT translates the 'public' IP address to the one specified on the LAN.

If IPAT is not enabled on your Service Managed Gateway, you may specify up to four local server host addresses (this will be reflected in the wizard interface). A client outside the private network can establish a connection of the specified service type to any of these specified IP addresses on the private network.

To specify one or more local server addresses, you click the **IP Address Details** button associated with each service and enter the appropriate IP address or addresses.

You can enter separate host addresses for each service type if required. Alternatively, you can use the same addresses for some or all services.

Note: the screenshots here reflect an environment where IPAT is not enabled. If IPAT is enabled on your SMG, you may enter only one IP address.

Web (HTTP)

Click the top **IP Address Details** button. The Local HTTP Server window opens.

Local HTTP Server

Primary Server:

Local Server 1 IP Address . . .

Additional Servers:

Local Server 2 IP Address . . .

Local Server 3 IP Address . . .

Local Server 4 IP Address . . .

Figure 10: The HTTP IP Details pop-up window

Enter the IP addresses of each local server and click **OK** to close the window and return to the Security Services page.

Secure web (HTTPS)

Click the second **IP Address Details** button from the top. The Local HTTPS Server window opens:

Local HTTPS Server

Primary Server:

Local Server 1 IP Address . . .

Additional Servers:

Local Server 2 IP Address . . .

Local Server 3 IP Address . . .

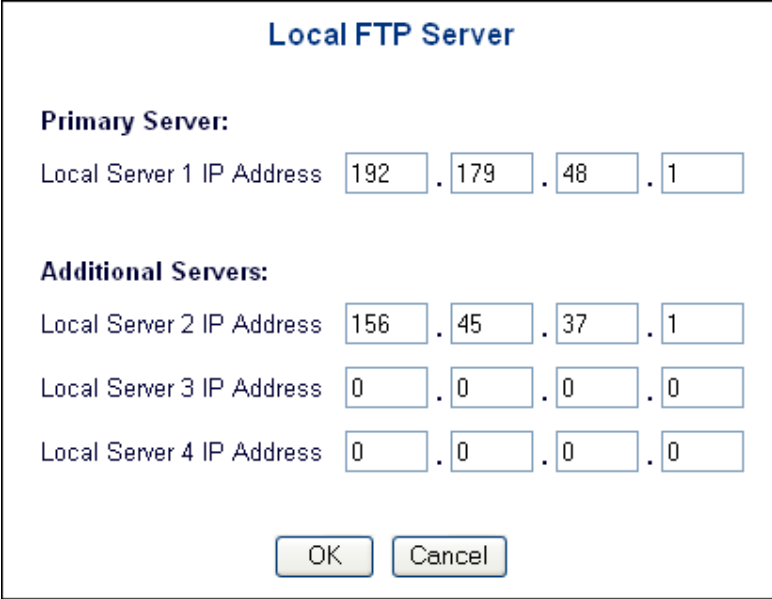
Local Server 4 IP Address . . .

Figure 11: The local HTTPS pop-up window

Enter the IP addresses of each local server and click **OK** to close the window and return to the Security Services page.

File Transfer (FTP)

Click the third **IP Address Details** button from the top. The Local FTP Server window opens:



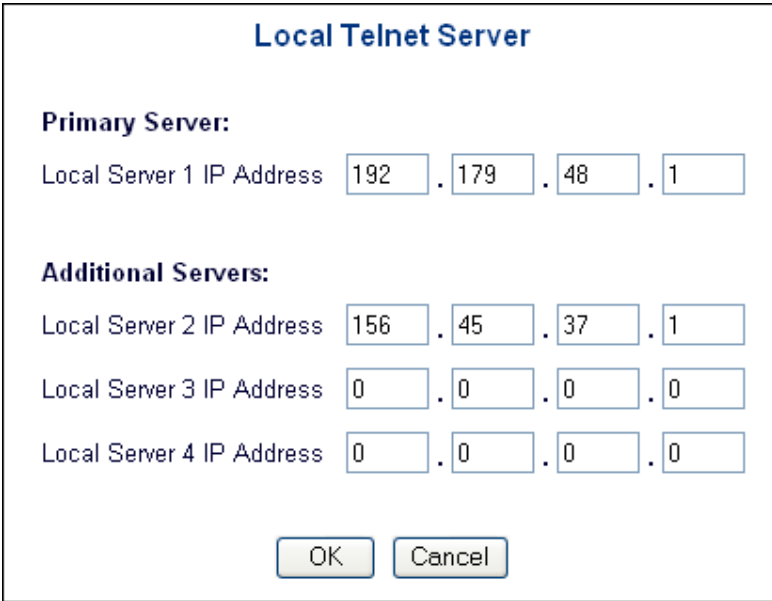
The screenshot shows a window titled "Local FTP Server". It contains two sections: "Primary Server:" and "Additional Servers:". Under "Primary Server:", there is a label "Local Server 1 IP Address" followed by four input boxes containing the values 192, 179, 48, and 1, separated by dots. Under "Additional Servers:", there are three labels: "Local Server 2 IP Address" (156, 45, 37, 1), "Local Server 3 IP Address" (0, 0, 0, 0), and "Local Server 4 IP Address" (0, 0, 0, 0). At the bottom of the window are two buttons: "OK" and "Cancel".

Figure 12: The Local FTP Server window

Enter the IP addresses of each local server and click **OK** to close the window and return to the Security Services page.

Telnet

Click the fourth **IP Address Details** button from the top. The Telnet Server window opens:



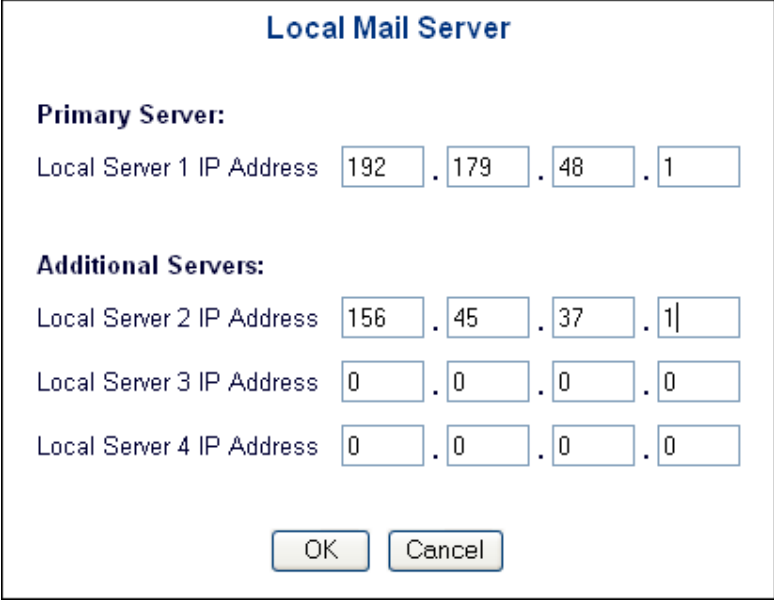
The screenshot shows a window titled "Local Telnet Server". It contains two sections: "Primary Server:" and "Additional Servers:". Under "Primary Server:", there is a label "Local Server 1 IP Address" followed by four input boxes containing the values 192, 179, 48, and 1, separated by dots. Under "Additional Servers:", there are three labels: "Local Server 2 IP Address" (156, 45, 37, 1), "Local Server 3 IP Address" (0, 0, 0, 0), and "Local Server 4 IP Address" (0, 0, 0, 0). At the bottom of the window are two buttons: "OK" and "Cancel".

Figure 13: The Local Telnet Server window

Enter the IP addresses of each local server and click **OK** to close the window and return to the Security Services page.

Email

Click the lowermost **IP Address Details** button. The Local Mail Server window opens:



Local Mail Server

Primary Server:

Local Server 1 IP Address 192 . 179 . 48 . 1

Additional Servers:

Local Server 2 IP Address 156 . 45 . 37 . 1

Local Server 3 IP Address 0 . 0 . 0 . 0

Local Server 4 IP Address 0 . 0 . 0 . 0

OK Cancel

Figure 14: The Local Mail Server window

Enter the IP addresses of each local server and click **OK** to close the window and return to the Security Services page.

Once you have configured all traffic permissions and IP addresses on the Security Services page, click **OK** to return to the Firewall Options page.

2.5 Enabling Firewall filters

You use the Enable Firewall Filters field to define security criteria that the firewall uses to control access of packet types.

To enable firewall filters, click **Details** next to Configure Firewall Filters.



Configure Firewall Filters Details...

Figure 15: Configure Firewall Filters

Figure 16: The Firewall Filters page

Each field on this page refers to a filter that has an associated drop-down list. To enable the filter named in the field, select 'yes' from the drop-down list. To disable it, select 'no'.

Prevent Spoofing – this prevents hackers from sending fake packets to the wide area network (WAN) citing the LAN's destination address

- **Block Broadcast Source** – this stops packets that will broadcast to all addresses on the destination LAN
- **Block Directed Broadcasts** – this stops broadcasts from the source address
- **Protect Interfaces** – this prevents packets from being directed to the Service Managed Gateway in order to protect against direct DOS attacks on the router (This is not relevant where IPAT is enabled.)
- **Block Netbios** and **Block WINS** – these screen packets that identify clients on the network
- **Block Large Pings** – this prevents malicious attacks that flood the network with large packets greater than 1500 bytes
- **Drop Unknown Packets** – this determines if a packet is dropped when it is not part of the existing session or if there are not rules that define what happens to a packet of this type
- **Public LAN outside Firewall** – defines whether traffic from the public LAN interface is treated as trusted or not trusted

When you have configured the firewall filters, click **OK** to return to the Firewall Options page.

2.6 Enabling logging services

The Enable Logging Services drop-down list allows you to specify the severity of firewall events that are logged and where the logged information is stored. Click **Details** next to Configure Event Services.



Figure 17: Configure Event Services

Figure 18: The Logging Services page, where you specify the firewall events that must be logged

On this page, you use the Firewall Target field to select where information logged about the firewall will be stored. You use the remaining fields to determine the level of severity at which events begin to be logged.

Firewall Target

From the drop-down list, choose the site at which logged firewall information will be stored:

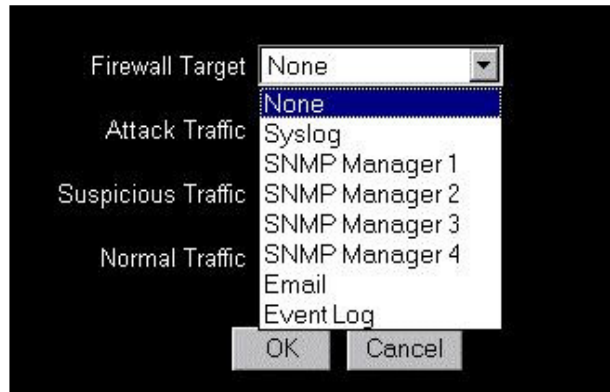


Figure 19: The Firewall Target drop-down list

Note: when you select the firewall target option, you should consider the event severity settings as they affect the amount of logging information generated. See below for more details.

Attack, Suspicious, and Normal Traffic

These three fields represent the event severity levels at which you can configure logging to be initiated:

- **Attack Traffic** – this refers to the detection of a manually constructed packet with malicious intent, or a large number of suspicious packets
- **Suspicious Traffic** – this refers to the detection of a large number of broadcast packets or any potentially probing or mischievous packets being sent directly to the router
- **Normal Traffic** – this refers to traffic that could leak sensitive information to unauthorized parties listening on the outside network.

To set an event severity level, select 'yes' from the appropriate drop-down list.

In general if you select 'yes' in the Attack field, fewer events will be logged than if you configure logging to be initiated by packets that are merely suspicious. Usually, if you select 'yes' in the Normal Traffic field, the largest number of logs will be generated.

This has important consequences for the firewall target, and you should select the target accordingly. For example, if you enable the Normal Traffic event severity level, you should set the firewall target as 'syslog', because a large amount of logging information will be generated. On the other hand, if you choose only to receive alerts about Attack Traffic, you could log events to an email account and perhaps trigger a pager. However, if you enabled Suspicious Traffic logging, and the firewall target option was set to this e-mail address, the address could quickly become flooded and unworkable.

Each firewall filter has an associated event severity level:

Large ping	attack
Anti-Spoofing	attack
Broadcast source	attack
Directed broadcast	suspicious
Protected interfaces	suspicious
Netbios	normal
WINS	normal

The severity levels cited here correspond to event severity levels in the Event Forwarding System. You can view parameter in this system in the Expert View:

- Go to the Advanced section on the Fast Start menu
- Click the Expert View option
- In the Configuration table of contents, expand the System folder.
- Expand the Events folder and click 'event filters' to display the Event Filters list.
- Click **add** to add a link.

The screenshot shows the 'Event Filters' configuration page. It features four dropdown menus for configuration: 'Event Class' set to 'CONFIGURATION', 'Target' set to 'Event Log', 'Severity Criterion' set to 'Greater Than', and 'Severity' set to 'Emergency'. Below the 'Severity' dropdown, a list of severity levels is shown, with 'Emergency' selected. The list includes: Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug-Level Messages, and Not Applicable. There are also 'Update' and 'Delete' buttons visible.

Figure 20: The Event Filters page in the Expert Web of the SMG web

The firewall severities map to the event severities as follows:

ATTACK > ALERT SUSPICIOUS > WARNING

NORMAL > DEBUG-LEVEL MESSAGES

When you have completed the logging configuration, click **OK** to return to the Firewall options page.

2.7 Saving your configuration

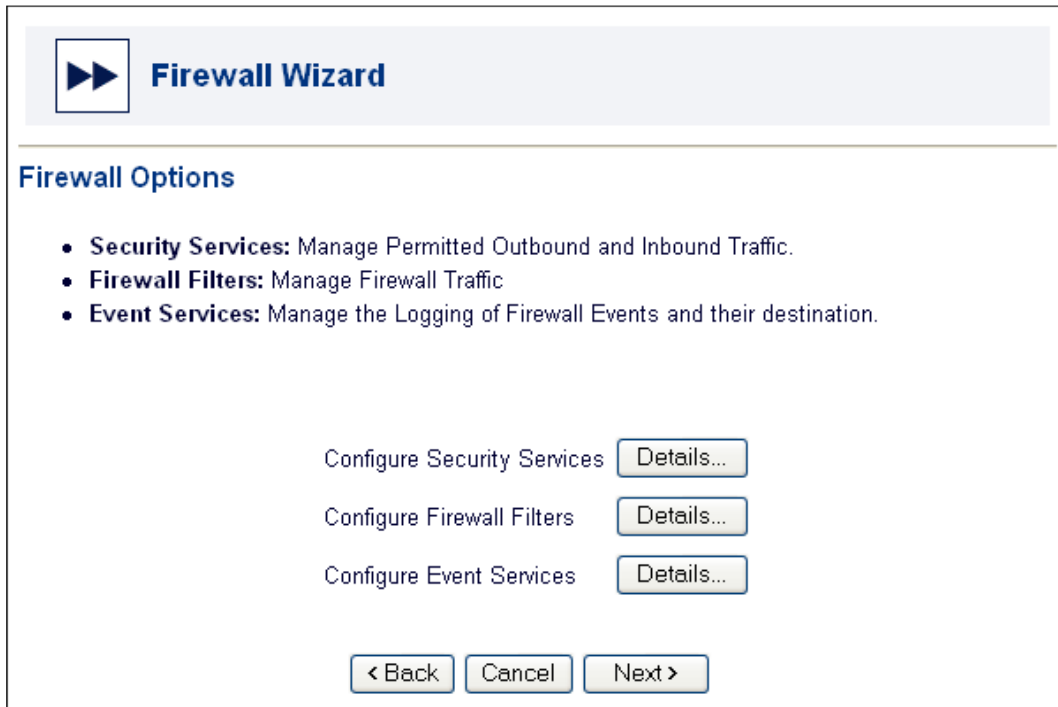


Figure 21: The Firewall Options page

On the Firewall Options page, click **Next** to continue. A page where you can save the new or updated configuration opens.

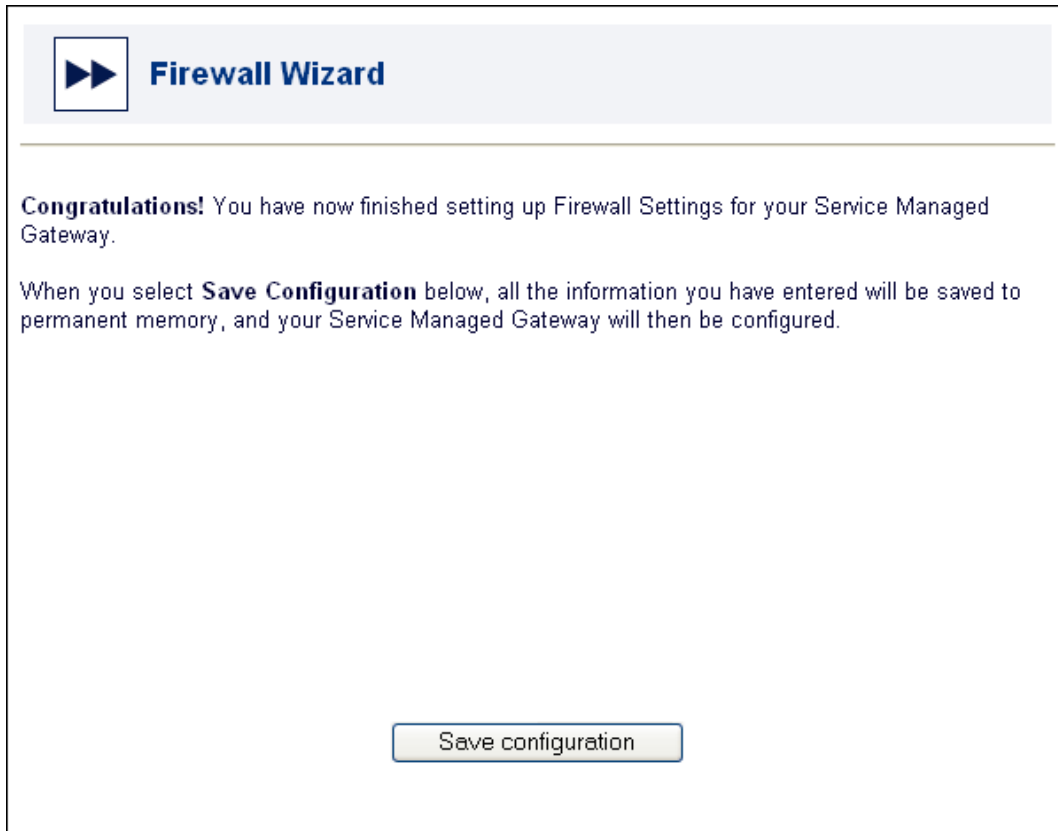


Figure 22: The Congratulations page, where you save your configuration

When you click **Save Configuration**, your SMG reloads and updates its firewall settings. When it has completed the reload, a message appears:

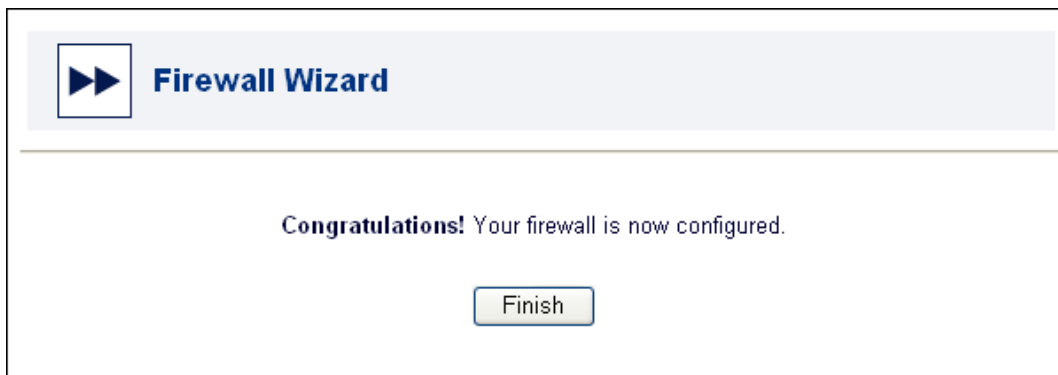


Figure 23: The Finish button

Click **Finish** to close this window and return to the Fast Start menu.