Firewall VPN Router

Quick Installation Guide

M73-APO09-380

Firewall VPN Router Overview

The Firewall VPN Router provides three 10/100Mbit Ethernet network interface ports which are the Internal/LAN, External/WAN, and DMZ port. It also provides an easily operated software WebUI that allows users to set system parameters or monitor network activities using a web browser.

Firewall VPN Router security feature

Some functions that are available in the firewall are: Packet Filter, Proxy Server, Hacker invasion alarm, Packet monitor log, Policy, etc.

Firewall VPN Router installation

This product is a hardware firewall. Therefore the installation is much easier than a software firewall. First the user has to prepare three network cables, and connect them to the internal, external and DMZ connectors respectively. The internal interface has to connect to the office's internal network on the same HUB/Switch. The external interface has to connect with an external router, DSL modem, or Cable modem. The DMZ interface connects to an independent HUB/Switch for the DMZ network.

Firewall VPN Router function setting

The Firewall VPN Router has a built in WEBUI (Web User Interface). All configurations and management are done through the WEBUI using an Internet web browser.

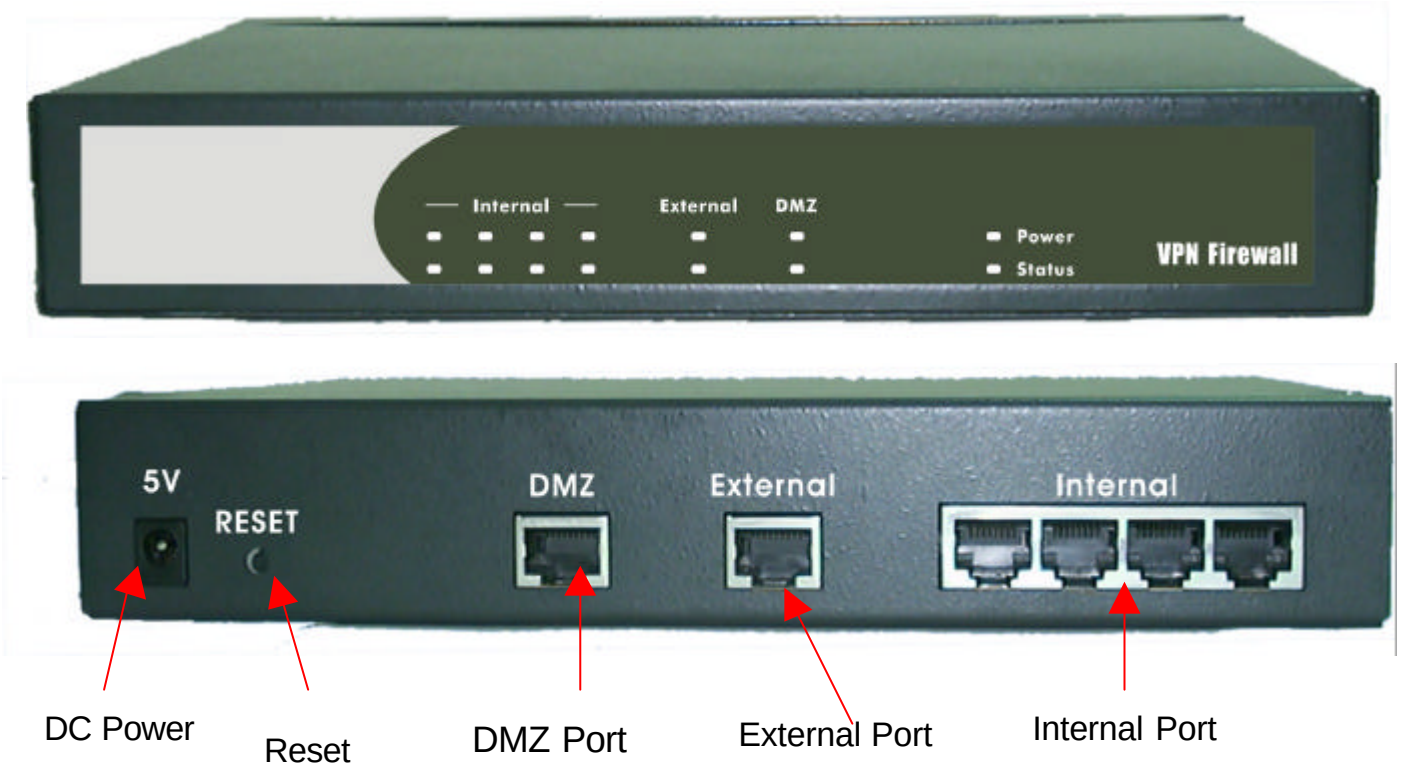
Firewall VPN Router monitoring function

The firewall provides monitoring functions which contains traffic log, event log, traffic alarm, event alarm, and traffic statistics. Traffic alarm records the packets of hacker invasions. Not only does the firewall log these attacks, it can be set up to send E-mail alerts to the Administrator automatically for immediate hacker's invasion crisis management.

Firewall VPN Router supporting protocols

The Firewall VPN Router supports all the TCP, UDP and ICMP protocols, such as HTTP, TELNET, SMTP, POP3, FTP, DNS, PING, etc. System Administrators can set up proprietary protocols according to operating requirements.

Hardware Description



DMZ Port: Use this port to connect to the company's server(s), which needs direct connection to the Internet (FTP, SNMP, HTTP, DNS).

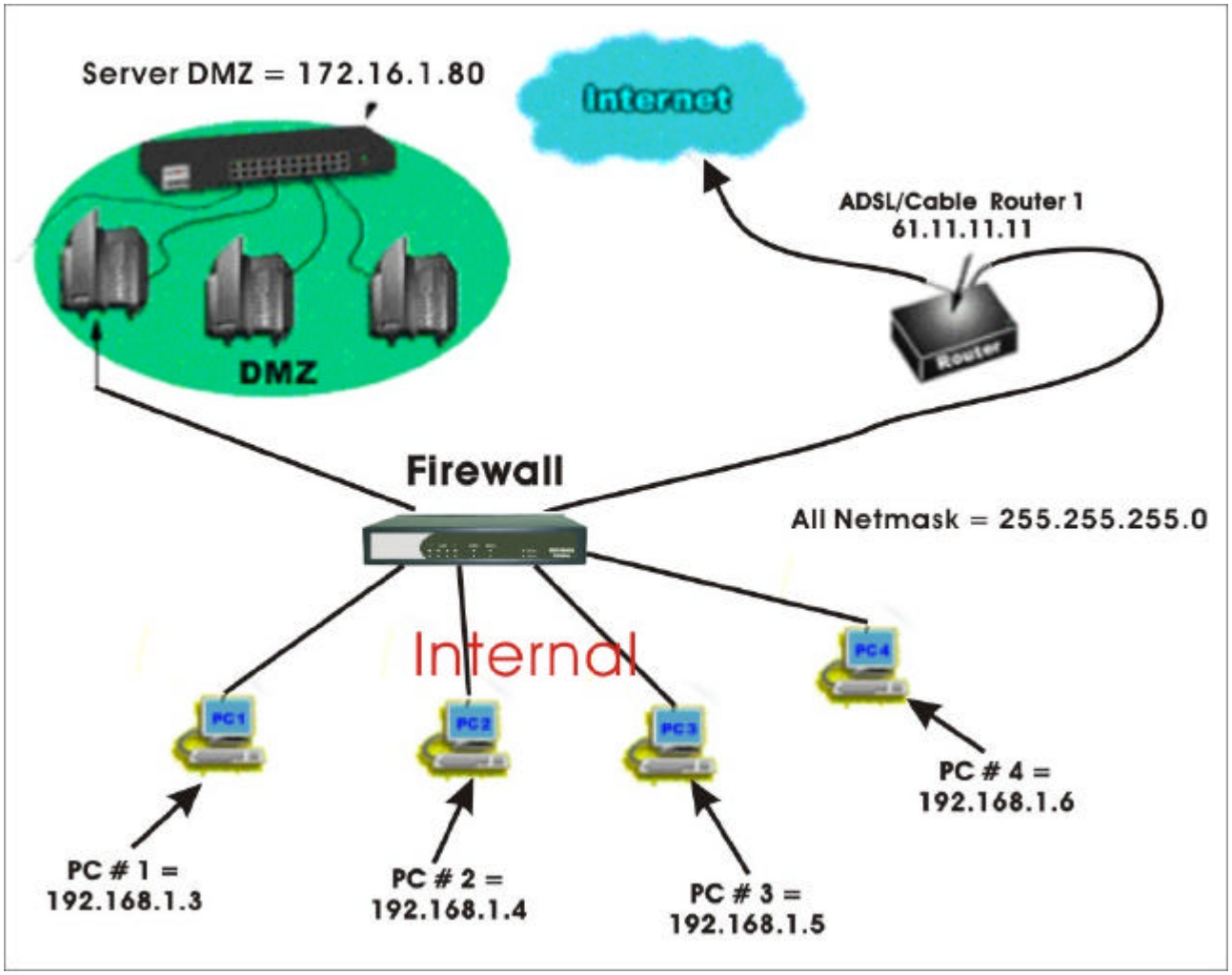
External Port (WAN): Use this port to connect to the external router, DSL modem, or Cable modem.

Internal Port (LAN): Use this port to connect to the internal network of the office.

Reset: Reset the Firewall VPN Router to the original default settings.

DC Power: connect one end of the power supply to this port, the other end to the electrical wall outlet.

Connecting Example:



Firewall:

Internal Port = 192.168.1.1

External Port = x.x.x.x (provided by ISP)

DMZ Port = 172.16.1.254

Connection Type: 10/100 Mbps Cable Connection

【Internal 1 Port】= **192.168.1.3**

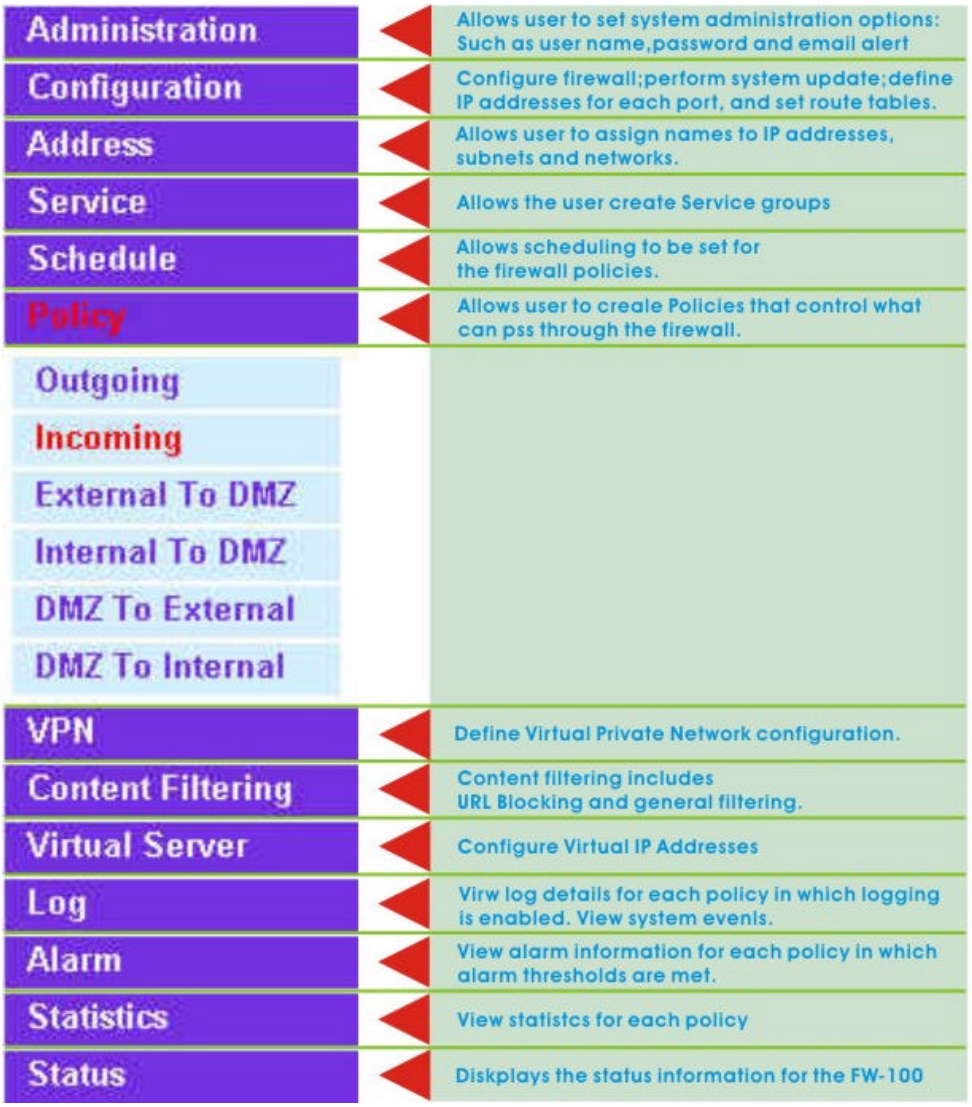
【Internal 2 Port】= **192.168.1.4**

【Internal 3 Port】= **192.168.1.5**

【Internal 4 Port】= **192.168.1.6**

【External Port】 = **61.11.11.11**
【DMZ Port】 = **172.16.1.254**

Firewall VPN Router Software (management tool) description



Firewall VPN Router management tool：WebUI

The main menu functions are located on the left-hand side of the screen, and the display window will be on the right-hand side. The main functions include 12 items, which are: Administrator, Configuration, Address, Service, Schedule, Policy, VPN, Virtual Server, Log, Alarm, Statistics, and Status.

Quick Setup

WebUI Configuration example

STEP 1:

Connect both the Administrator's PC and the Internal (LAN) port of the Firewall VPN Router Firewall to a hub or switch. Make sure there is a link light on the hub/switch for both connections. The Firewall VPN Router has an embedded web server used for management and configuration. Use a web browser to display the configurations of the firewall (such as Internet Explorer 4(or above) or Netscape 4.0(or above) with full java script support). The default IP address of the firewall is **192.168.1.1** with a subnet mask of 255.255.255.0. Therefore, the IP address of the Administrator PC must be in the range between 192.168.1.2 /24– 192.168.1.254/24.

If the company's internal IP Address is not subnet of 192.168.1.0, (i.e. Internal IP Address is 172.16.0.1) the Administrator must change his/her PC IP address to be within the same range of the internal subnet (i.e. 192.168.0.0). Reboot the PC if necessary.

By default, the Firewall VPN Router is shipped with its DHCP Server function enabled. This means the client computers on the internal (LAN) network including the Administrator PC can set their TCP/IP settings to automatically obtain an IP address from the Firewall VPN Router.

The following table is a list of private IP addresses. These addresses may not be used as an External IP address.

10.0.0.0 ~ 10.255.255.255
172.16.0.0 ~ 172.31.255.255
192.168.0.0 ~ 192.168.255.255

STEP 2：

Once the Administrator PC has an IP address on the same network as the Firewall VPN Router, open up an Internet web browser and type in http://92.168.1.1 in the address bar.

A pop-up screen will appear and prompt for a username and password. A username and password is required in order connect to the firewall. Enter the default login username and password of Administrator (see below).

Username: admin

Password: admin

Click OK

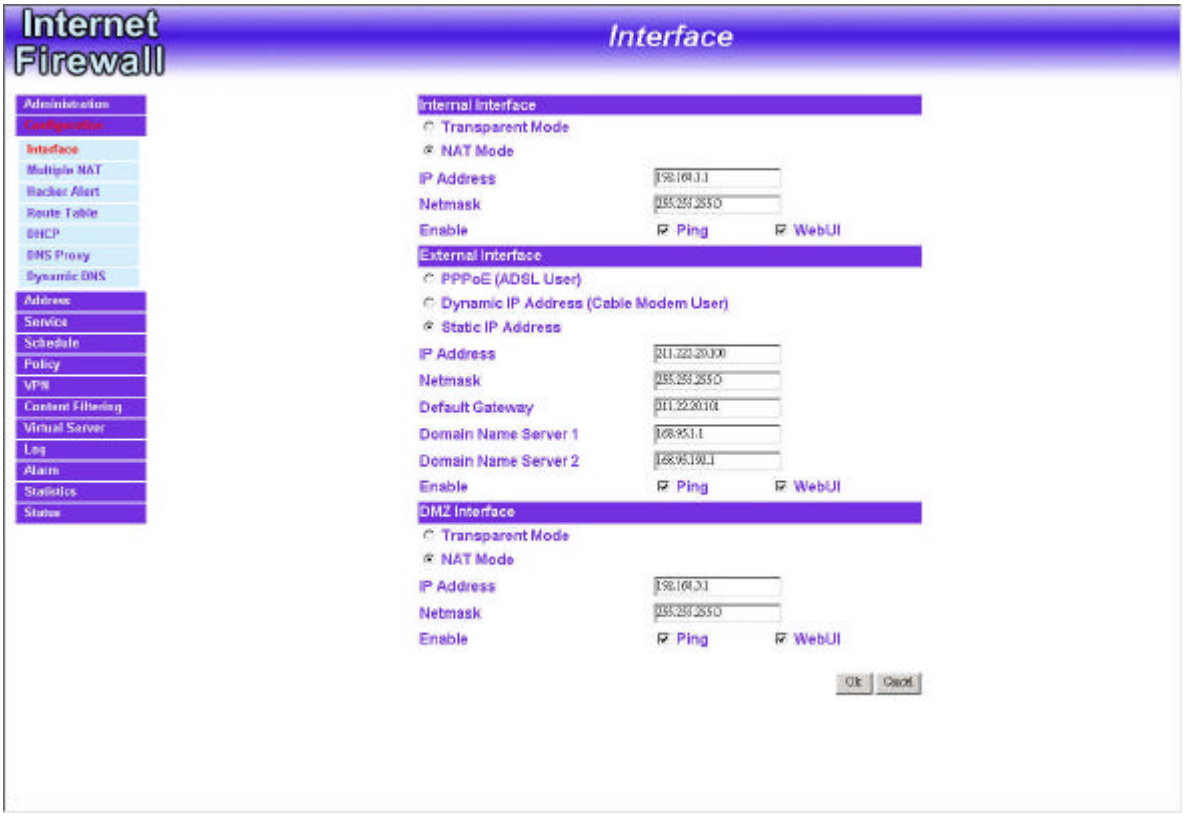
STEP 3:

After entering the username and password, the Firewall VPN Router WEBUI screen will display.

Select the **Configuration** tab on the left menu and a sub-function list will be displayed. Click on **Interface** from the sub-function list, and enter proper Layer 3 network setup information. (for example)

Internal interface	IP Address	192.168.1.1
	NetMask	255.255.255.0
External	IP address	211.222.20.100
	NetMask	255.255.255.0
	Default Gateway	211.222.20.101
DMZ	IP address	192.168.3.1
	NetMask	255.255.255.0

Note: The above figures are only examples. Please fill in the appropriate IP address information provided to you by the ISP.



STEP 4：

Click on the **Policy** tab from the main function menu, and then click on **Outgoing** from the sub-function list.

Click on **New Entry** button.

When the **New Entry** option appears, then enter the following configuration:

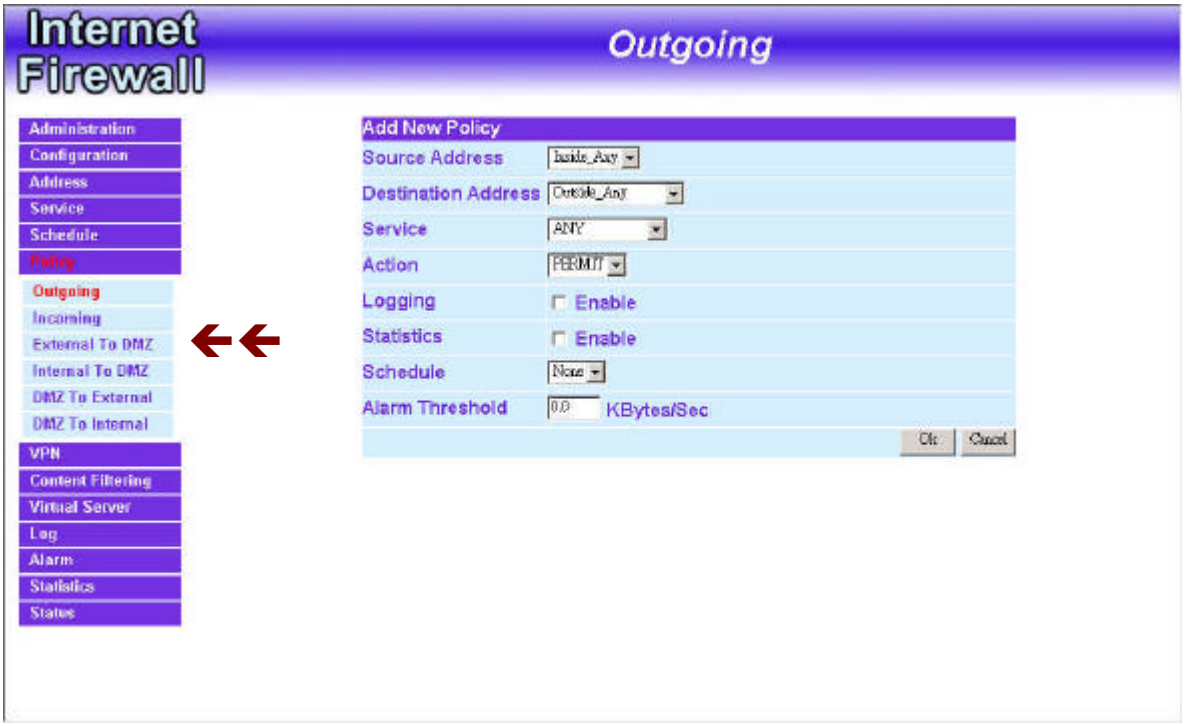
Source Address – select **“Inside_Any”**

Destination Address – select **“Outside_Any”**

Service - select **“ANY”**

Action - select **“Permit”**

Click on **OK** to apply the changes.



STEP 5：

The configuration is successful if you see the screen below. Make sure that all the computers that are connected to the Internal (LAN) port have their Default Gateway IP Address set to the Firewall's Internal IP Address (i.e. 192.168.1.1). At this point, all the computers on the Internal network should gain access to Internet immediately. If a firewall filter function is required, please refer to the Policy section.