Firewall VPN Router

Quick Installation Guide

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

Administration	Allows user to set system administration options: Such as user name, password and email alert
Configuration	Configure firewall;perform system update;define IP addresses for each port, and set route tables.
Address	Allows user to assign names to IP addresses, subnets and networks.
Service	Allows the user create Service groups
Schedule	Allows scheduling to be set for the firewall policies.
Policy	Allows user to creale Policies that control what can pss through the firewall.
Outgoing	
Incoming	
External To DMZ	
Internal To DMZ	
DMZ To External	
DMZ To Internal	
VPN	Define Virtual Private Network configuration.
Content Filtering	Content filtering includes URL Blocking and general filtering.
Virtual Server	Configure Virtual IP Addresses
Log	Virw log details for each policy in which logging is enabled. View system events.
Alarm	View alarm information for each policy in which alarm thresholds are met.
Statistics	View statistcs for each policy
Status	Diskplays the status information for the FW-100

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

Enter Netv	vork Passwor	d <u>? ×</u>
? >	Please type yo	ur user name and password.
(J	Site:	192.168.1.1
	Realm	Firewall Administration Tools
	<u>U</u> ser Name	admin
	<u>P</u> assword	****
	🔲 <u>S</u> ave this p	bassword in your password list
		OK Cancel

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.

UPUE-CVCEUU Attentionetine Excitigeneitine Excitigeneitine Interface	Advanisesion Internal interface Configuration Transparent Mode NAT Mode Interface NAT Mode Interface NAT Mode Interface NAT Mode Interface NAT Mode Interface Interfa
Automation C Transparent Mode Interface © Transparent Mode Multiple NAT P Address US20031 Backer Alert P Address US2032830 Poulo Enable IP Ping IW WebUI EMS Proxy External Interface Dynamic DMS C PPPoE (ADSL User) Address 0 Dynamic IP Address Schedule P Address 20122-2000 Policy P Address 20122-2000 Policy P Address 20122-2000 VPN Contant Effection 0 Dynamic IP Address Policy P Address 20122-2000 VPN Remark 205253280 Contant Effection Default Gateway p11222000 VPN Default Gateway p11222000 Virial Sorrer Domain Name Server 1 p283012 Varial Sorrer Domain Name Server 2 p283012 Varial Sorrer DM2 Interface C Transparent Mode © NAT Mode P Ndress p32002 Virial Sorrer DM2 Interface P Ping Virial Sorrer DM2 Interface C Transparent Mode © NAT Mode P Ndress p320252830 P Address PS2003 En	Funding allow C Transparent Mode Interface © Transparent Mode Multiple NAT IP Address IP Address IP 20011 Inacker Aint IP Address Backer Aint IP Address Bysamic DMS C PPPOE (ADSL User) Address C Dynamic IP Address Schobile IP Address Schobile IP Address VP8 Internask Content Filtering Default Gateway Viriand Server Domain Name Server 1 Leg Domain Name Server 2 Adares Enable Statistio Enable
Interface © NAT Mode Multiple NAT IP Address IP (00.1) Route Table IP Address IP (00.1) Route Table IP Ping IP WebUI ENDPOE Enable IP Ping IP WebUI ENS Proxy External Interface IP Ping IP WebUI ENS Proxy External Interface IP Ping IP WebUI ENS Proxy External Interface IP Ping IP WebUI Schedule IP Address 20.223000 IP Address Pulicy IP Address 20.223000 IP Address Pulicy IP Address 20.223000 IP Address VPN Default Gateway III.2223000 IP Address VPN Default Gateway III.223000 IP Address Virial Sorver Domain Name Server 1 IP 80011 IP 80011 Alam Enable IP Ping IP WebUI Statistics IP Address IP 20011 IP Address IV Address IP 20021 IP 80011 IP 80011 Statistics IP Address IP 80011 IP 80011	Instalace NAT Mode Matigin NAT P Address IS2(011) P Address IS2(011) P Address IS2(011) P Address IS2(011) P Address IS2(011) P Address P Ping P WebUI IS2(011) P Ping P WebUI IS2(011) IS2(011) P Ping P WebUI IS2(011) IS2(011)
Multiple NAT IP Address [52:00.1] Backer Alart Netmask [25:25:25:30] Peute Table IP Ping IP WebUI ENS Proxy External Interface Bynamic DNS C PPPoE (ADSL User) Anteres C Dynamic IP Address Schedele IP Address Pulicy P Address Pulicy IP Address Pulicy I	Mailingin MAT IP Address [52:08].1 Backer Alart Netmask [25:25:25:25:0 Prote Table IP Ping IF WebUI EMS Proxy Escend Intiofface IP Ping Bysamic DMS C PPPOE (ADSL User) Address Address C Dynamic IP Address (Cable Modern User) Schoolen P Address PI122:20:121 VPR Paddress PI122:20:121 VPR Netmask 25:25:25:25:0 VPR Default Gateway PI122:20:121 Vanual Server Domain Name Server 1 162:25:11 Leg Domain Name Server 2 162:35:10:1 Statistics Enable IF Ping Statistics DMZ Interface DMZ Interface
Netmask 253,253,2530 Peute Table P Ping P WebUI ENS Proxy External Interface Bysamic DNS C PPPOE (ADSL User) Anterese C Dynamic IP Address (Cable Modern User) Schwölz P Address Pulicy Default Gateway Pinz Sorver Domain Name Server 1 Leg Domain Name Server 2 Statistics Enable DM2 Interface C Transparent Mode C NAT Mode IP Address IP Address Statistics	National Factor Netmask DSS25/23/230 Route Table IP Ping IP WebUI Enable IP Ping IP WebUI EMS Proxy Interface Interface Bysemic DMS C Dynamic IP Address (Cable Modern User) Interface Schoole P Address III.222/20120 VPR Policy III.222/20120 VPR Netmask DSS25/25/2010 VPR Default Gateway III.222/20120 Vinual Server Domain Name Server 1 I/22/20120 Values Enable IP Ping IP WebUI Statesi DMZ Interface IMZ Ping IP WebUI
Encode Food Enable IP Ping IP WebUI ENS Proxy External Interface Bysamic DNS C PPPoE (ADSL User) Address C Dynamic IP Address (Cable Modern User) Schedule P Address Pulicy IP Address Pulicy IP Address Pulicy P Address Pulicy IP Address Pulicy IP Address Pulicy Default Gateway Ping IP WebUI VPN Default Gateway Castern Filterian Default Gateway Virial Server Domain Name Server 1 Domain Name Server 2 IEXXI0.1 Alama Enable Societies IP Ping State P Address Castern Kitesian IP Castern Filterian Opmain Name Server 1 IP 2000.1 Virial Server IP Ping State IP Ping State IP Ping VebUI State State IP Ping P Address IP Ping IP Address IP Ping P Address IP Ping P Address IP Ping P Address IP Ping Enable IP Ping <td>Enable IF Ping IF WebUl ENSProxy External Intorface Bysemic DMS C PPPoE (ADSL User) Address C Dynamic IP Address (Cable Modem User) Schobile P Address Schobile IP Address VPR Paties VPR Default Gateway Vinual Server Domain Name Server 1 Les Domain Name Server 2 Statistics Enable Statistics DM2 Interface</td>	Enable IF Ping IF WebUl ENSProxy External Intorface Bysemic DMS C PPPoE (ADSL User) Address C Dynamic IP Address (Cable Modem User) Schobile P Address Schobile IP Address VPR Paties VPR Default Gateway Vinual Server Domain Name Server 1 Les Domain Name Server 2 Statistics Enable Statistics DM2 Interface
ENS Proxy External Interface Bysamic DNS C PPPoE (ADSL User) Address C Dynamic IP Address (Cable Modern User) Schedule © Static IP Address Policy IP Address VPN Default Gateway Cardenin Filterian Default Gateway Domain Name Server 1 IP 283510 Alame Enable IP Ping Statietics IP Address Statietics IP Address Virbus IP Address P Address ISS(00.31) Netmask ISS(252350) Enable IP Ping IP WebUI	EMS Proxy External Interface Bysemic DMS C PPPoE (ADSL User) Address C Dynamic IP Address (Cable Modem User) Service C Static IP Address Schöele IP Address Policy IP Address VPR Netmask VPR Default Gateway Vinual Server Domain Name Server 1 Leg Domain Name Server 2 Atlans Striktics Striktics Enable VIL Ping
Bysamic DNS C PPPoE (ADSL User) Address C Dynamic IP Address (Cable Modern User) Schedule C Static IP Address Pulcy IP Address Pulcy PAddress Pulcy Period Patient Patients Pulcy Patients Pulcy PAddress Patient Patients Patient Patient Patient	Bysemic DNS C PPPoE (ADSL User) Address C Dynamic IP Address (Cable Modern User) Scholkle P Address Scholkle IP Address Paticy IP Address VPN Netmask VPN Default Gateway Vinual Server Domain Name Server 1 Leg Domain Name Server 2 Statistics Enable Statesi DM2 Interface
Address C Dynamic IP Address (Cable Modern User) Schoole © Static IP Address Schoole IP Address Pulsy IP Address VPW Netmask Content Filtering Default Gateway Virual Server Domain Name Server 1 Virual Server Domain Name Server 2 Alamn Enable Statistics DMZ Interface C Transparent Mode © NAT Mode IP Address ISS/0001 Netmask ISS/2000	Address C Dynamic IP Address (Cable Modem User) Service Static IP Address School IP Address Policy P Address VPR Netmask Content Filtering Default Gateway Vinual Server Domain Name Server 1 Leg Domain Name Server 2 Statics Enable Striketos DM2 (Interface
Static IP Address PL222000 Static IP Address PL222000 VPN Netmask DS332350 Containt Filtering Default Gateway PL222000 Virial Server Domain Name Server 1 D0953101 Leg Domain Name Server 2 D2630101 Statistics Enable IF Ping Statistics DMZ Interface C Transparent Mode IP Address DS262350 IP Address DS262350 Enable IF Ping PAddress DS262350 Enable IF Ping	Server Patient School PAddress Publicy PAddress Publicy PAddress VPR Netmask Content Filtering Default Gateway Virinual Server Domain Name Server 1 Leg Domain Name Server 2 Alares Enable Striketos DM2 Interface
Palicy IP Address PL222000 VPR Netmask PSS252350 Containt Filtering Default Gateway PL22000 Virtual Server Domain Name Server 1 PR83510 Alama Domain Name Server 2 PR835100 Statistics Enable IF Ping Statistics DMZ Interface C Transparent Mode IP Address IP Address PSL6001 Netmask PSL222300 Enable IF Ping IP Address PSL6001 Netmask PSL22300	Policy IP Address PU1/22/20/20 Policy Netmask 255/255/255/0 VPR Default Gateway PU1/22/20/20 Virianal Server Domain Name Server 1 1/22/20/20 Virianal Server Domain Name Server 2 1/22/20/20 Alaura Enable R* Ping R* WebUI Statese DM2 Interface
VPN Netmask DSISSISSO Contant Filtering Default Gateway D1122010 Virtual Server Domain Name Server 1 D083510 Alama Domain Name Server 2 D0835100 Statistics Enable IF Ping Statistics DMZ Interface C Transparent Mode IP Address IP Address D5232350 Enable IF Ping Vertices IP Address IP Address D5232350 Enable IF Ping	VPR Netmask 255.255.2550 Content Filtering Default Gateway PI1222010 Virial Server Domain Name Server 1 162851.1 Leg Domain Name Server 2 162851.0 Alama Domain Name Server 2 162851.0 Striktics Enable R* Ping R* WebUI Strikting DM2 Interface Vertice
Content Filtering Default Gatewary PI1.22010 Virtual Server Domain Name Server 1 D083510 Alarm Domain Name Server 2 D835100 Alarm Enable IF Ping IF WebUI Statistics DMZ Interface OMZ Interface Ping IF WebUI P Address If8:160.01 Netmask D33232500 Enable IF Ping IF WebUI	Content Filtering Default Gateway p112220101 Virinal Server Domain Name Server 1 1/28251.1 Leg Domain Name Server 2 1/28251.0 Alama Enable R ² Ping R ² WebUI States DM2 Interface Machine
Virtual Server Domain Name Server 1 D8831.1 Leg Domain Name Server 2 D8831.0 Atama Enable IF Ping IF WebUI Statistics DM2 Interface C Transparent Mode © Transparent Mode IN NAME 198100.1 IP Address 198100.1 If WebUI Netmask 298283.2550 If WebUI	Virtual Server Domain Name Server 1 Id8251.1 Leg Domain Name Server 2 Id8251.00.1 Alarma Demain Name Server 2 Id8251.00.1 Statistics Enable R2 Ping R2 WebUI States DM2 Interface R2 Ping R2 WebUI
Let Domain Name Server 2 [2000100] Statistics Statistics DMZ Interface C Transparent Mode A NAT Mode IP Address ISE (60.01 Netmask ID Statistic Enable F Ping F WebUI	Les Domain Name Server 2 L68/81/0/1 Alarma Enable F2 Ping F2 WebUI Statistics DM2 Interface F2 Ping F2 WebUI
Statistics Enable Pring Prebul Statistics DMZ Interface C Transparent Mode C Transparent Mode R NAT Mode IP Address ISE (60.01) ISE (60.01) Netmask DSS 2550 Enable	Statistics Enable Pring Pring PrivebUl Statistics DM2 Interface
States DMZ Interface C Transparent Mode A NAT Mode IP Address IS8:6031 Netmask Enable F Ping F WebUI	Status DMZ Interface
C Transparent Mode R NAT Mode IP Address [SS:0001 Netmask 25:23:25:0 Enable R Ping R WebUI	
	C Transparent Mode
IP Address (158:1613) Netmask (253:253:2550) Enable IP Ping IP WebUI	A NAT Mode
Netmask 233,233 2350 Enable IP Ping IP WebUI	IP Address [198.16(3)]
Enable Ping R WebUI	Netmask 235/257 255/0
	Enable F Ping F WebUI
Ok Cad	OE

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.

Internet Firewall		Outgoing	
Administration	Add New Policy		
Configuration	Source Address	haida_Aay 🛥	
Address	Destination Address	Outlike_Any +	
Service Schedule	Service	ANY	
Policy	Action	FIRMIT .	
Outgoing	Logging	C Enable	
Incoming	erasita Otobeller		
External To DMZ	Staustics	Enable	
Internal To DMZ	Schedule	None -	
DMZ To External	Alarm Threshold	0.0 KBytes/Sec	
VPN			Ol: Cuncel
Content Filtering			
Virtual Server			
Log			
Alarm			
Statistics			

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.

Internet Firewall	Outgoing
Administration Configuration Address Service Schedule Policy Outgoing Incoming External To DM2 Internal To DM2 Internal To DM2 Internal To DM2 OM2 To External DM2 To Internal VPN Content Filtering Virtual Server Log Alarm Statistics States	No. Source Destination Source Any Any Configure Move 1 Inside_Any Any Any Configure Move To New Barty Configure Move To Configure Move To