Help

Forwarding Rules

Forwarding Rules permits the firewall to forward data traffic for a subnet from one interface to another. When forwarding a subnet, an IP address needs to be assigned to the system to serve as the default router for the subnet. To add an additional IP address to the system, visit the Subinterfaces page.

Add a Forwarding Rule:

Destination IP:	210.XX.XX.91
Destination Mask:	255.255.255.248
Source IP:	10.90.91.23
Source Mask:	255.255.255.128
Input Interface:	WAN
Output Interface:	LAN
Protocol:	Any
Custom Destination Ports:	
Custom Source Ports:	

Add Clear

Enable Firewall for WAN: ☑

Basic WAN Firewall Settings:

These setting apply to services that are running on the V2IU.

Allow HTTP access through firewall: ☑

Set HTTP access port: 80

Note that if you change the HTTP port you will have to access the GUI using the new port

Allow HTTPS access through firewall: ☑

Allow TELNET access through firewall: ☐

Allow SSH access through firewall: ☑

Allow SNMP access through firewall: ☐

Allow TCP Port:

Allow UDP Port:

Trusted Management Addresses:

Apply basic settings configuration only to the following addresses:

Address can be host IP or network/mask, e.g. 10.10.10.1 or 10.10.10.0/24. To delete an entry, highlight and delete it.

Forwarding WAN Firewall Settings:

These settings apply to packets being forwarded to systems running behind the firewall.

Enable Firewall Logging: ☐

Enable PPTP Server Pass-through: ☐

PPTP Server IP Address:
