

V2 Firewall Web Admin Usage

1. Login the V2 web interface like this: <http://xxx.xxx.xxx.xxx> (where xxx.xxx.xxx.xxx is the IP address of the V2)

Uniforce V2 VPN/FW Main Menu

Status

Port 0 (LAN): 10.180.2.5/255.255.255.0
Port 1 (AUX): 192.168.2.1/255.255.255.0
Port 2 (AUX): 192.168.3.1/255.255.255.0
Port 3 (WAN): / GW:218.20.216.1
ADSL 1 (ppp0): 218.19.243.125/255.255.255.255
ADSL 2 (ppp1): /
VPN: IPsec running pluto pid 23236
Copyright 2002-2003 Uniforce System Ltd

Actions

[Reset Config to Factory Default](#)
[Restart System](#)
[Restart VPN Service](#)
[Restart TCP/IP and ADSL Service](#)
[Commit Changes to System Config](#)
[Admin Firewall Rules](#)

Port 0 is LAN - Internal IP: 10.180.2.5, Netmask: 255.255.255.0
Port 3 is WAN – External IP: 218.20.216.1
ADSL 1 is PPPoE : IP: 218.19.243.125, Netmask: 255.255.255.255

2. In Actions part, click **Admin Firewall Rules**

3. You will see the web interface contains the followings: Workstation IP Address, Protocol, Access Port# and Allow/Disallow like this:

	Workstation IP Address	Protocol	Access Port#	Allow/Disallow
1	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	tcp ▾	<input type="text"/> ▾ <input type="text"/>	<input type="radio"/> / <input type="radio"/>
2	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	tcp ▾	<input type="text"/> ▾ <input type="text"/>	<input type="radio"/> / <input type="radio"/>
3	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	tcp ▾	<input type="text"/> ▾ <input type="text"/>	<input type="radio"/> / <input type="radio"/>
4	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	tcp ▾	<input type="text"/> ▾ <input type="text"/>	<input type="radio"/> / <input type="radio"/>
5	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	tcp ▾	<input type="text"/> ▾ <input type="text"/>	<input type="radio"/> / <input type="radio"/>
6	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	tcp ▾	<input type="text"/> ▾ <input type="text"/>	<input type="radio"/> / <input type="radio"/>

4. Workstation IP Address is for the user to enter the IP address. Number of IP address allowed: 50-100
5. Protocol has two options: TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). The user can only select one from each line.
6. Access Port# has the following options: ftp, ssh, telnet, http, pop3, imap. Port# will be assigned automatically by the system based on the selected protocol. The user can only select one from each line.

- The user can only have one choice in Allow/Disallow. Allow means that the firewall will not block the traffic if the IP Address, Protocol and Access Port# of particular line are all matched. Disallow means that firewall will block the traffic if the IP Address, Protocol and Access Port# of particular line are all matched.
- The Submit button at the bottom (see figure) is for the user to save his/her setting. The V2 Firewall settings will be effective after the user clicked the Submit button. The user can entered the web interface again and edit the V2 Firewall settings if necessary.

98	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	tcp	<input type="text"/>	<input type="text"/>	<input type="radio"/> / <input type="radio"/>
99	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	tcp	<input type="text"/>	<input type="text"/>	<input type="radio"/> / <input type="radio"/>
100	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	tcp	<input type="text"/>	<input type="text"/>	<input type="radio"/> / <input type="radio"/>

- Go back the Telnet Interface and type commit in the login part and then press Enter key. The new firewall settings will then be effective. (Note: This step MUST be done, otherwise all the new settings will be lost when the V2 is rebooted)

```

Uniforce V2 VPN/FW Gateway
Build: v2c0000-030309a

Logon as:

reboot - restart box
resvpn - restart just vpn service
resnet - restart all LAN and WAN and ADSL connections
commit - commit config changes to permanent memory
seteth0 - setup LAN port (port 0) LAN
seteth1 - setup aux port 1
seteth2 - setup aux port 2
seteth3 - setup WAN port (port 3) WAN
setppp0 - setup first adsl connection (pppoe)
setppp1 - setup second adsl connection (pppoe)

mreset - set to factory default (* WARNING: all current settings are erased)
login:
    
```

Example of the firewall settings:

	Workstation IP Address	Protocol	Access Port#	Allow/Disallow
1	<input type="text"/> 192 . <input type="text"/> 168 . <input type="text"/> 51 . <input type="text"/> 66	tcp	ssh 22	<input type="radio"/> / <input type="radio"/>
2	<input type="text"/> 192 . <input type="text"/> 168 . <input type="text"/> 51 . <input type="text"/> 66	tcp	telnet 23	<input type="radio"/> / <input type="radio"/>
3	<input type="text"/> 192 . <input type="text"/> 168 . <input type="text"/> 51 . <input type="text"/> 99	tcp	<input type="text"/> / <input type="text"/>	<input type="radio"/> / <input type="radio"/>

V2 Telnet Interface

```
Uniforce V2 VPN/FW Gateway
Build: v2c0000-030309a

Logon as:

reboot - restart box
resvpn - restart just vpn service
resnet - restart all LAN and WAN and ADSL connections
resfw - restart firewall service
commit - commit config changes to permanent memory
seteth0 - setup LAN port (port 0) LAN
seteth1 - setup aux port 1
seteth2 - setup aux port 2
seteth3 - setup WAN port (port 3) WAN
setppp0 - setup first adsl connection (pppoe)
setppp1 - setup second adsl connection (pppoe)

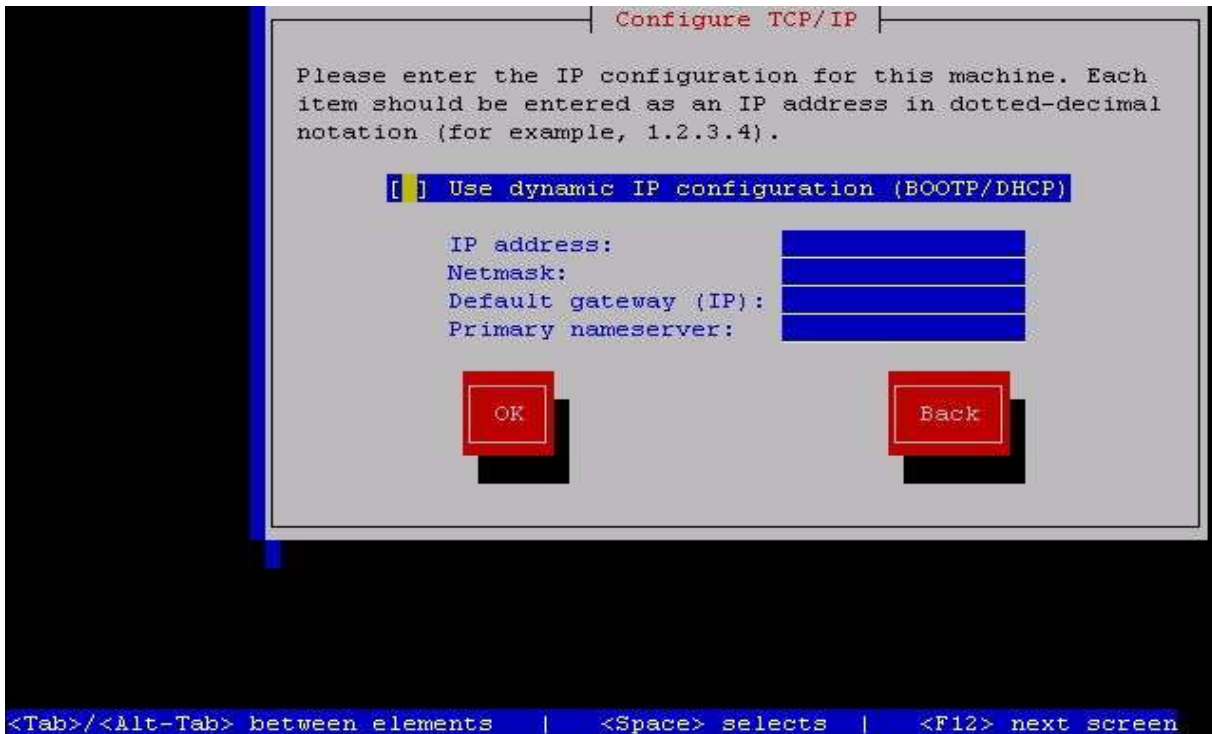
mreset - set to factory default (* WARNING: all current settings are erased)
login:
```

There are 12 commands can be typed

9. reboot : the V2 will be restarted
- 10.resvpn : the V2 will be restarted just VPN service
- 11.resnet : all the LAN, WAN and ADSL connections in V2 will be restarted
- 12.resfw : the firewall service in V2 will be restarted
- 13.commit : save all the changes in configuration to the permanent memory
- 14.seteth0, seteth1, seteth2, seteth3 – the screen will be like this:

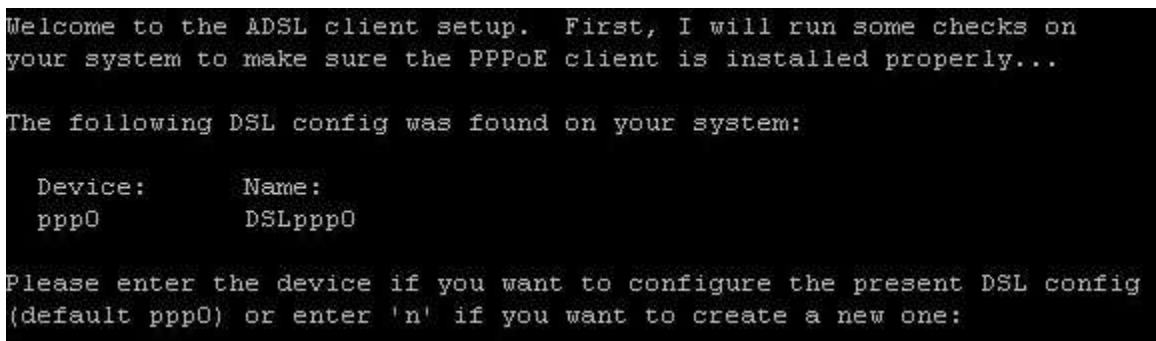


- a. Select Yes to set up networking



b. Configure TCP/IP using dynamic or fixed IP. If dynamic IP is used, just use space bar to select **Use dynamic IP configuration (BOOTP/DHCP)**. If fixed IP is used, the user should enter the correct value for **IP address**, **Netmask**, **Default Gateway (IP)** and **Primary nameserver**. After that, select **OK** to quit the screen.

setppp0, setppp1 : the screen will be like this:



a. Configure the present DSL configuration, default is ppp0



b. Enter the login name, default is user@isp

```
INTERFACE

Enter the Ethernet interface connected to the ADSL modem
For Solaris, this is likely to be something like /dev/hme0.
For Linux, it will be ethX, where 'X' is a number.
(default eth3): eth3
```

c. Enter the Ethernet interface, default is eth3

```
Do you want the link to come up on demand, or stay up continuously?
If you want it to come up on demand, enter the idle time in seconds
after which the link should be dropped.  If you want the link to
stay up permanently, enter 'no' (two letters, lower-case.)
NOTE: Demand-activated links do not interact well with dynamic IP
addresses.  You may have some problems with demand-activated links.
Enter the demand value (default no):
```

d. Enter the demand value, default is no

```
DNS

Please enter the IP address of your ISP's primary DNS server.
If your ISP claims that 'the server will provide dynamic DNS addresses',
enter 'server' (all lower-case) here.
If you just press enter, I will assume you know what you are
doing and not modify your DNS setup.
Enter the DNS information here:
```

e. Enter the DNS information

```
PASSWORD

Please enter your Password:
Please re-enter your Password:
```

f. Enter the password

```
USERCTRL

Please enter 'yes' (two letters, lower-case.) if you want to allow
normal user to start or stop DSL connection (default yes):
```

g. Select your user control, default is yes

```
FIREWALLING

Please choose the firewall rules to use. Note that these rules are
very basic. You are strongly encouraged to use a more sophisticated
firewall setup; however, these will provide basic security. If you
are running any servers on your machine, you must choose 'NONE' and
set up firewalling yourself. Otherwise, the firewall rules will deny
access to all standard servers like Web, e-mail, ftp, etc. If you
are using SSH, the rules will block outgoing SSH connections which
allocate a privileged source port.

The firewall choices are:
0 - NONE: This script will not set any firewall rules. You are responsible
for ensuring the security of your machine. You are STRONGLY
recommended to use some kind of firewall rules.
1 - STANDALONE: Appropriate for a basic stand-alone web-surfing workstation
2 - MASQUERADE: Appropriate for a machine acting as an Internet gateway
for a LAN
Choose a type of firewall (0-2): 0
```

h. Choose firewall type, should select 0 first.

```
Start this connection at boot time
Do you want to start this connection at boot time?
Please enter no or yes (default no):yes
```

i. Select whether start the connection at boot time or not, default is no

```
** Summary of what you entered **
Ethernet Interface: eth3
User name: user@isp
Activate-on-demand: No
DNS: Do not adjust
Firewalling: NONE
User Control: yes
Accept these settings and adjust configuration files (y/n)?
```

j. Confirm your settings

8. mreset : restore to factory default settings (note: all current settings will be lost)