Firewall VPN 600/2 – 1200/2
User Manual

Don’t get hacked, get… HotBrick

Copyright Notice

Disclaimer

HotBrick Incorporated shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from furnishing this material, or the performance or use of the product.

HotBrick Incorporated reserves the right to change the product specification without notice. Information in this document may change without notice.

Trademarks

Microsoft, Windows 98, ME, 2000, NT, XP are registered trademarks of the Microsoft Corporation. All other brand and product names mentioned herein may be registered trademarks of their respective owners.

Customers should ensure that their use of this product does not infringe upon any patent rights. Trademarks mentioned in this publication are used for identification purposes only and are properties of their respective companies.

Table of Contents

1. Initial Setup

The Firewall VPN 600/2 - 1200/2 is configurable for a variety of network environments, and will automatically reconfigure itself, if possible, to avoid collision with your existing networks.

Each HotBrick box contains the following:

- 1 HotBrick 1200/2 Firewall VPN or 1 HotBrick 600/2 Firewall VPN
- 1 Power Cord
- 2 Patch Cables (1 red cross over cable, 1 blue straight-thru patch cable)
- 2 Mounting Brackets
- 4 Mounting Screws

Connect either a 568A or 568B standard straight-thru network patch cable plug from one of the LAN ports of the Firewall VPN 600/2 - 1200/2 to the network card of a client computer.

1. Plug in the power cable into your Firewall VPN 600/2 - 1200/2.

2. Power on your client computer.

3. Verify you client computer has the following network setup.

Windows 2000 Professional

Start→Settings→Network and Dial-up connections→Local Area Connection (Figure 1.1)

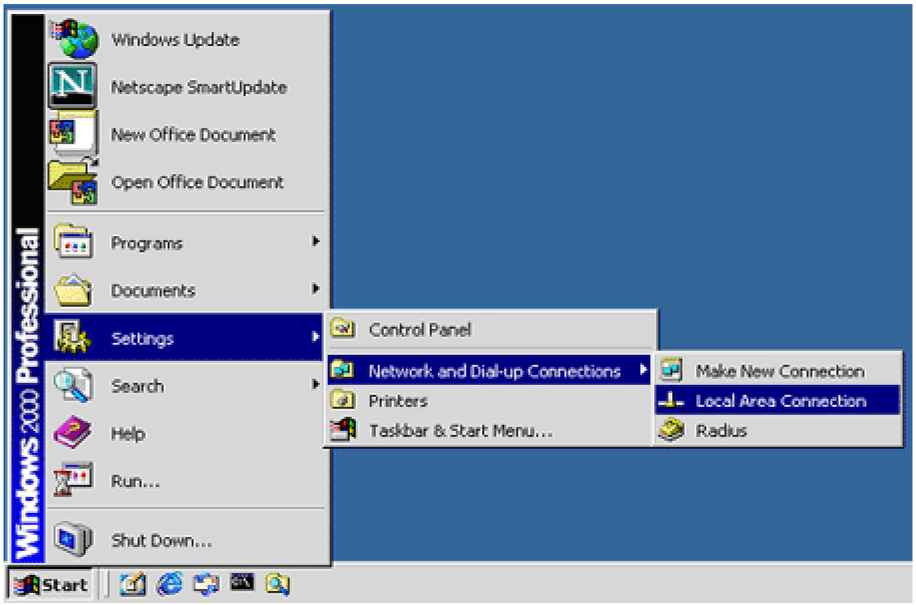
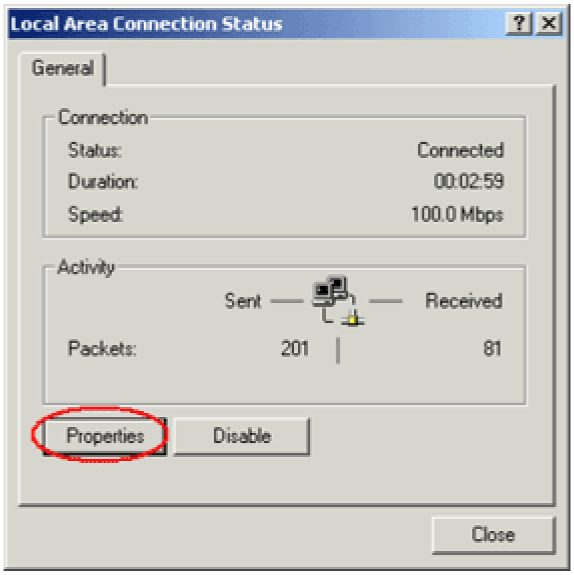


Figure 1.1
Windows 2000 Professional, Network configuration

This will bring up a window like Figure 1.2.



Local Area Connection Status

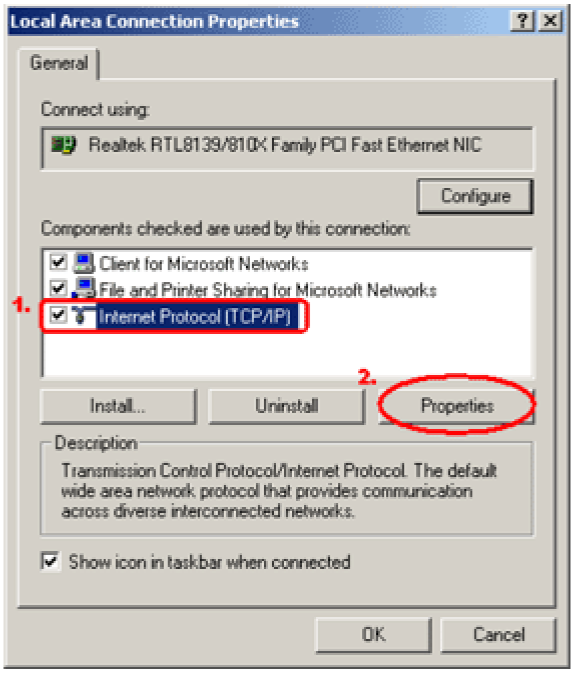
General

Connection
Status: Connected
Duration: 00:02:59
Speed: 100.0 Mbps

Activity
Sent — — Received
Packets: 201 | 81

Figure 1.2
Windows 2000 Professional, Local Area Connection Status, Properties button circled.

Click on the properties button to bring up a window like Figure 1.3. First click on Internet Protocol (TCP/IP), then click the properties button.



Local Area Connection Properties

General

Connect using:
Realtek RTL8139/810X Family PCI Fast Ethernet NIC

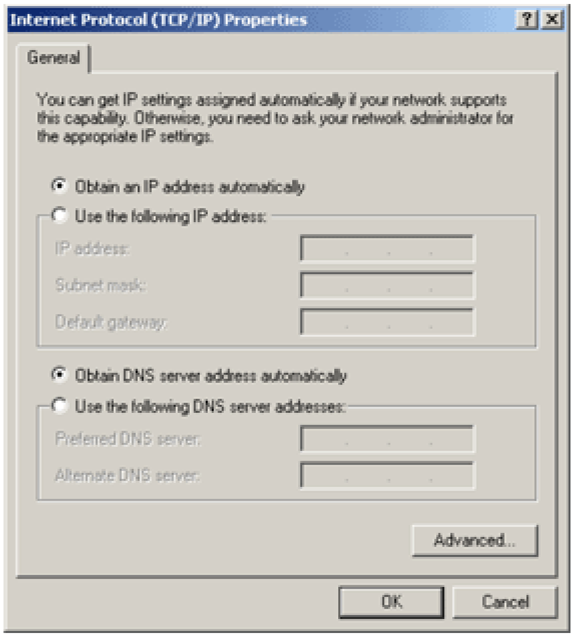
Components checked are used by this connection:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in taskbar when connected

Figure 1.3
Windows 2000 Professional, Local Area Connection Properties, TCP/IP marked, Properties button circled.

This should bring up the Internet Protocol (TCP/IP) Properties page, please make sure that both "Obtain an IP address automatically," and "Obtain DNS server address automatically" are both selected.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

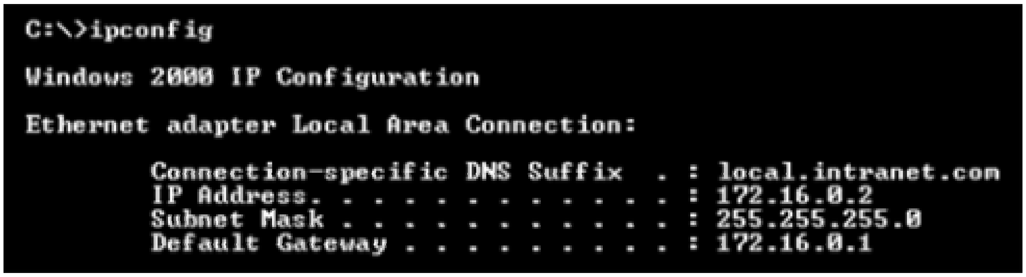
Alternate DNS server:

Figure 1.4
Windows 2000 Professional, Internet Protocol (TCP/IP) Properties

The Firewall VPN 600/2 - 1200/2 will automatically assign your computer an IP address, netmask and gateway.

You can verify this by opening a command or Ms-Dos prompt on your windows machine and typing ipconfig into the command line. You should see something like Figure 1.5.

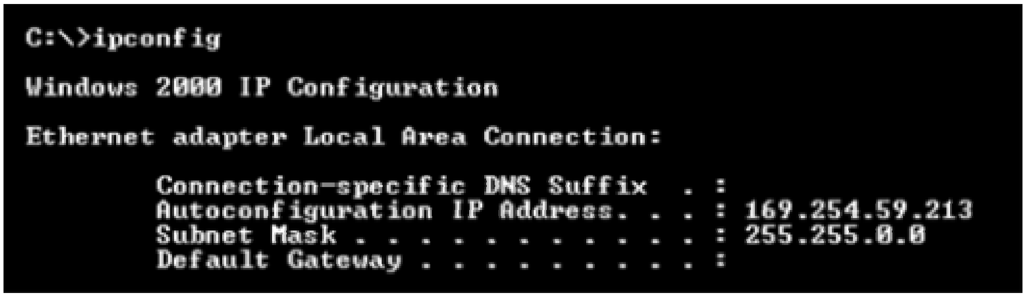
*Note: The default configuration for the Firewall VPN 600/2 - 1200/2 is to allocate a 192.168.1.1/24 IP address with a gateway of 192.168.1.1. If that does not work use 172.16.0.1



```
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : local.intranet.com
        IP Address. . . . . . . . . . . . : 172.16.0.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.16.0.1
```

Figure 1.5
Verify your setup using the command line and typing ipconfig

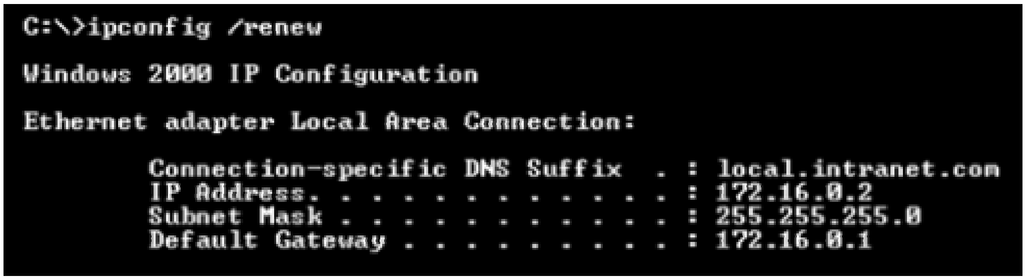
If you fail to receive an IP address, netmask, and gateway, the result from ipconfig may look something like Figure 1.6. To remedy this, please reboot your client computer, and try the previous steps again.



```
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Autoconfiguration IP Address. . . : 169.254.59.213
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . :
```

Figure 1.6
If your computer fails to receive DHCP, this is what may appear when you type ipconfig

More advanced windows users can try typing ipconfig /renew as seen in Figure 1.7.



```
C:\>ipconfig /renew

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : local.intranet.com
        IP Address. . . . . . . . . . . . : 172.16.0.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.16.0.1
```

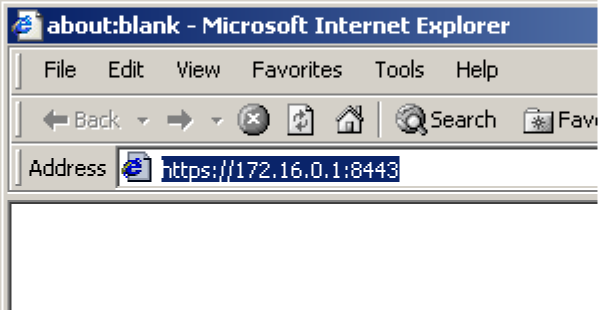
Figure 1.7
Renew your DHCP allocation using ipconfig /renew

If this should still fail, you can try manually configuring your client computer.

2. Logging In

Once you have physically connected the necessary network cables and powered up both the Firewall VPN 600/2 - 1200/2 and the client machine, and verified your network setup on the client computer, you need to open a SSL enabled web browser that can handle forms and connect to the web GUI of the Firewall VPN 600/2 - 1200/2

Using the gateway IP that is displayed when you type ipconfig, open up a browser, and type in (in the case shown before) https://172.16.0.1:8443 into the URL field. If you have some other gateway, such as 192.168.1.1, type https://192.168.1.1:8443 into the URL field.

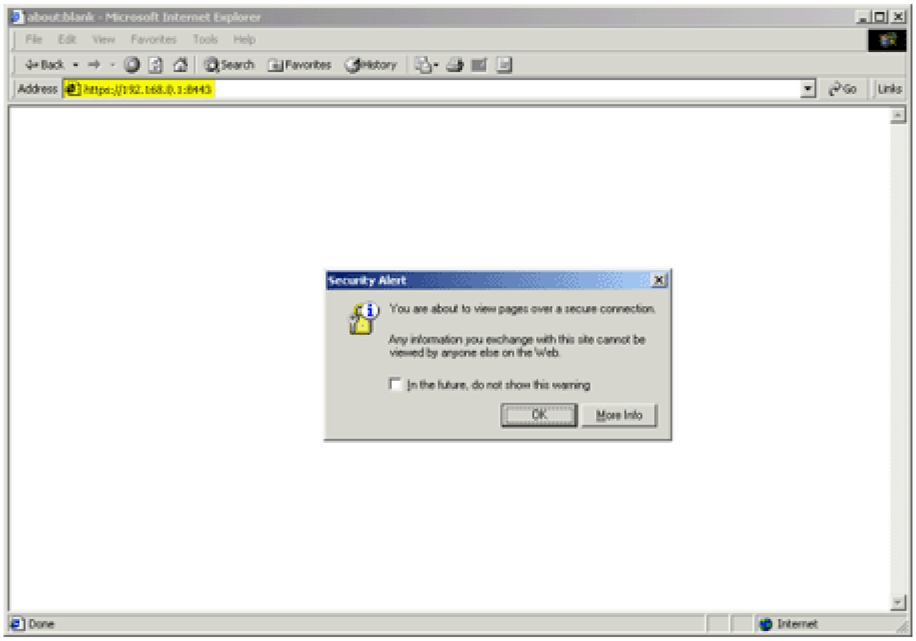


about:blank - Microsoft Internet Explorer

Address: https://172.16.0.1:8443

Figure 2.1
Type https://172.16.0.1:8443 or other gateway IP address shown when you type ipconfig

You will see a Security Alert popup dialog box (Figure 2.2) warning you that you are switching to a secure connection, followed by a second Security popup dialog box warning about the details of the actual security certificate (Figure 2.3). Click through these dialog boxes answering in the affirmative and you will see the login interface (Figure 2.4).



about:blank - Microsoft Internet Explorer

Address: https://192.168.0.1:8443

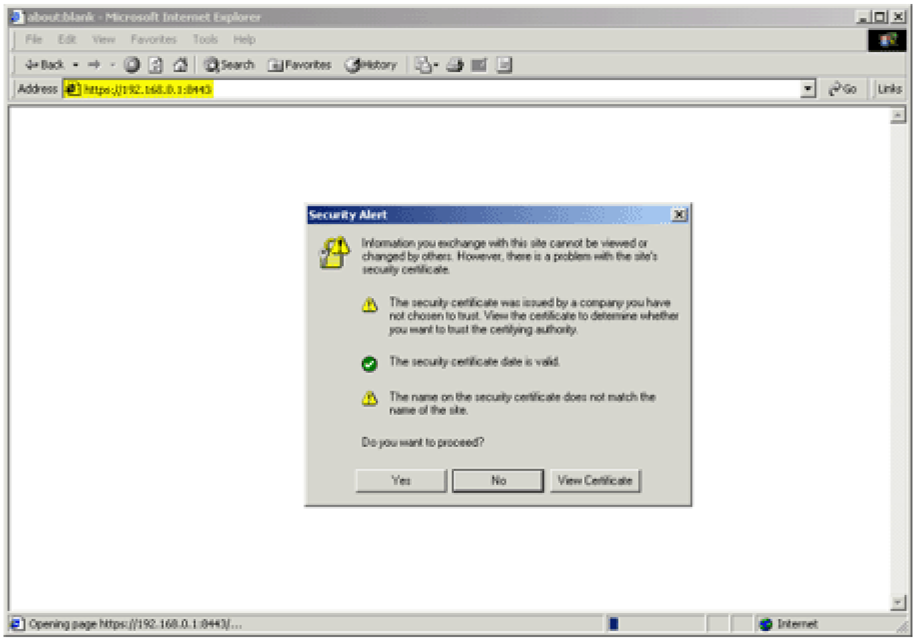
Security Alert

You are about to view pages over a secure connection.

Any information you exchange with this site cannot be viewed by anyone else on the Web.

□ In the future, do not show this warning

Figure 2.2
Secure connection security alert with URL highlighted.


about:blank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address https://192.168.0.1:8443
Go Links

Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The name on the security certificate does not match the name of the site.

Do you want to proceed?

Figure 2.3
Security certificate security alert with URL highlighted

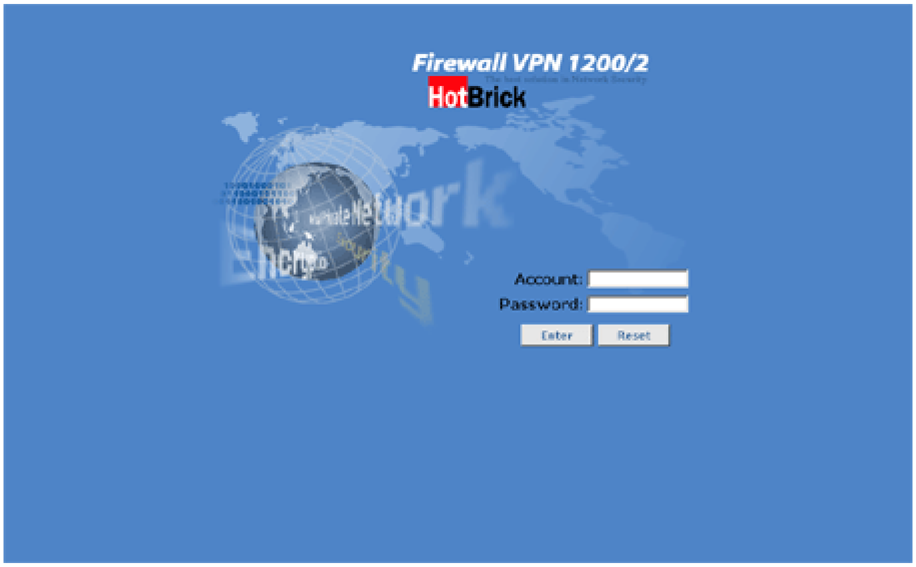
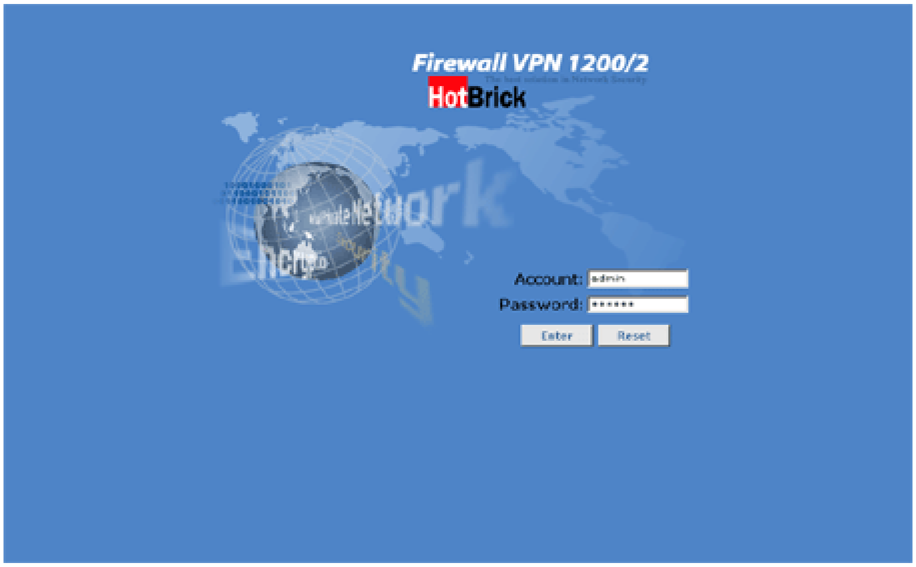


Figure 2.4
Firewall VPN 600/2 - 1200/2 login interface

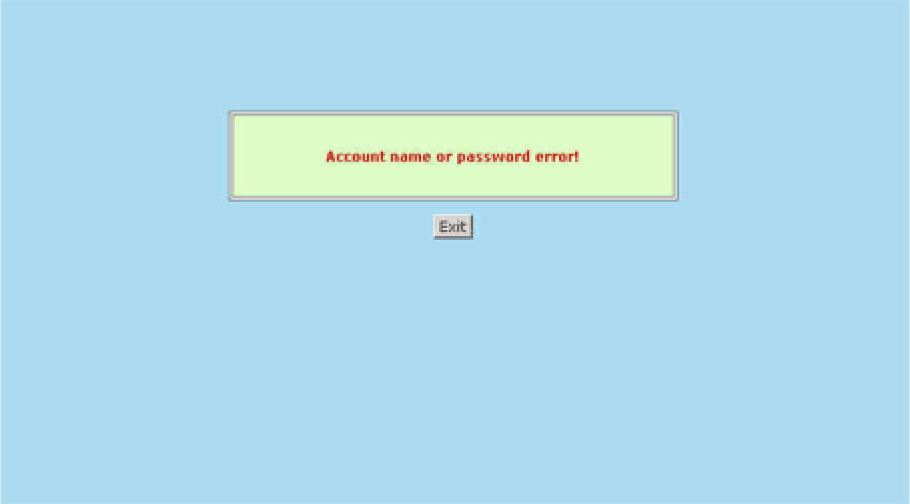
The default login is "admin" with a password "123456" (Figure 2.5). If you should enter any of the above incorrectly, the Firewall VPN will let you know (Figure 2.6).



Account: admin

Password: ******

Figure 2.5
Firewall VPN1200 login interface with default login entered

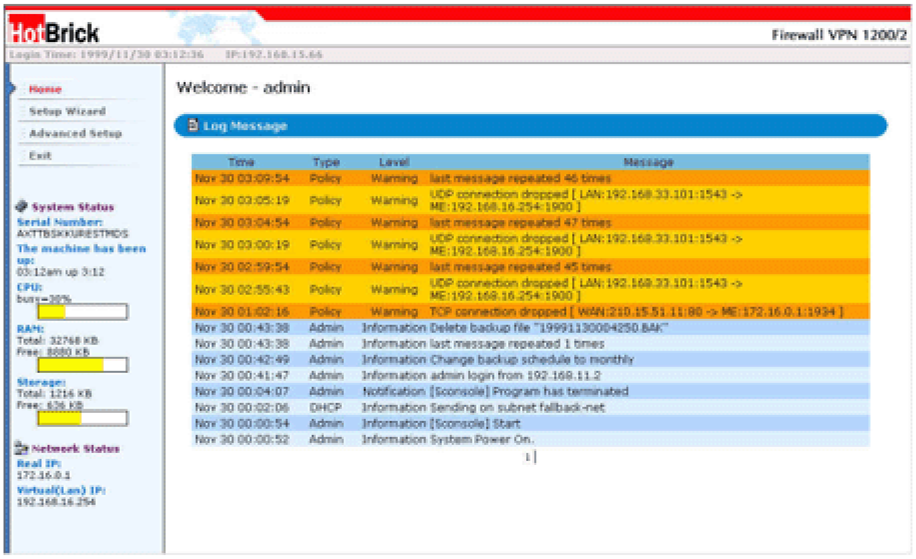


Account name or password error!

Figure 2.6
Incorrect account or password

3. Changing the Administrator Account and Password

Once you have logged in, the first thing you should do is change the administrator password and/or the administrator account name. To do this from the default login screen, click on the Advanced Setup button on the left panel to access the advanced menus (Figure 3.1).



System Status
Serial Number: AXTTBSKKURESTMDS
The machine has been up: 03:12am up 3:12
CPU: busy=30%
RAM: Total: 32768 KB Free: 8080 KB
Storage: Total: 1216 KB Free: 636 KB
Network Status
Real IP: 172.16.0.1
Virtual(Lan) IP: 192.168.16.254

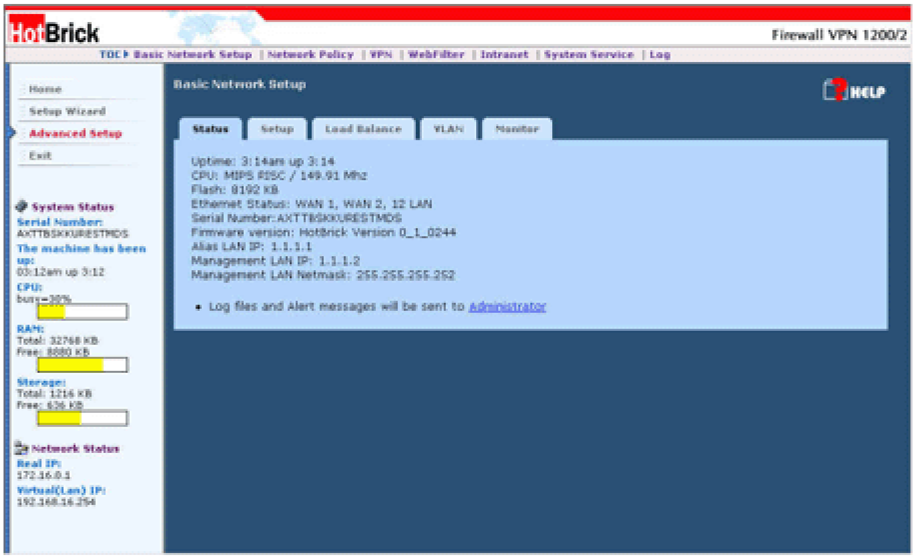
Welcome - admin

Time	Type	Level	Message
Nov 30 03:09:54	Policy	Warning	last message repeated 46 times
Nov 30 03:05:19	Policy	Warning	UDP connection dropped [LAN:192.168.33.101:1543 -> ME:192.168.16.254:1900]
Nov 30 03:04:54	Policy	Warning	last message repeated 47 times
Nov 30 03:00:19	Policy	Warning	UDP connection dropped [LAN:192.168.33.101:1543 -> ME:192.168.16.254:1900]
Nov 30 02:59:54	Policy	Warning	last message repeated 45 times
Nov 30 02:55:43	Policy	Warning	UDP connection dropped [LAN:192.168.33.101:1543 -> ME:192.168.16.254:1900]
Nov 30 01:02:16	Policy	Warning	TCP connection dropped [WAN:210.15.51.11:80 -> ME:172.16.0.1:1934]
Nov 30 00:43:38	Admin	Information	Delete backup file "19991130004250.BAK"
Nov 30 00:43:38	Admin	Information	last message repeated 1 times
Nov 30 00:42:49	Admin	Information	Change backup schedule to monthly
Nov 30 00:41:47	Admin	Information	admin login from 192.168.11.2
Nov 30 00:04:07	Admin	Notification	[Sconsole] Program has terminated
Nov 30 00:02:06	DHCP	Information	Sending on subnet fallback-net
Nov 30 00:00:54	Admin	Information	[Sconsole] Start
Nov 30 00:00:52	Admin	Information	System Power On.

1 |

Figure 3.1
Default login screen with Advanced Setup button circled

The advanced menus are a series of links across the top in alphabetical order, matched with tabs specific to the selected menu. The default page showing when you click on the Advanced Setup button will be the Basic Setup menu with the Status tab selected (Figure 3.2).



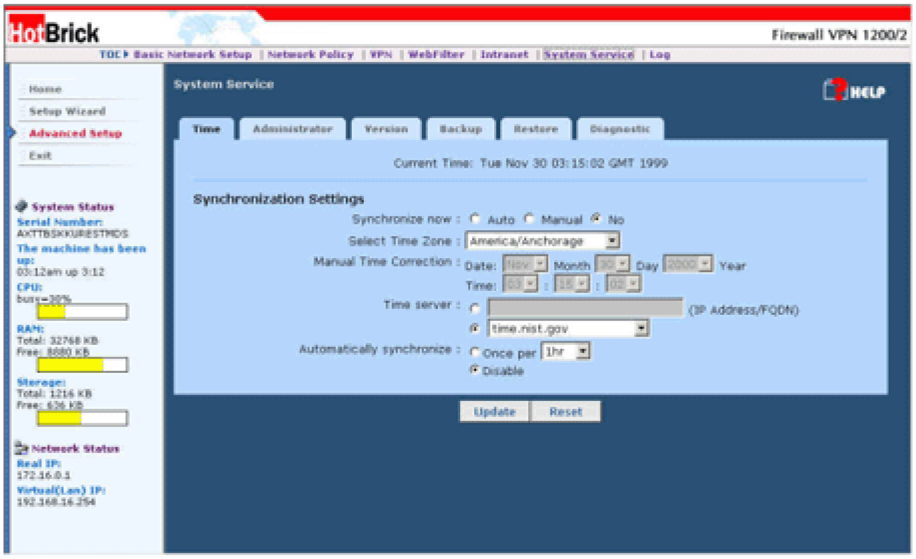
System Status
Serial Number: AXTTBSKKURESTMDS
The machine has been up: 03:12am up 3:12
CPU: busy=30%
RAM: Total: 32768 KB Free: 8080 KB
Storage: Total: 1216 KB Free: 636 KB
Network Status
Real IP: 172.16.0.1
Virtual(Lan) IP: 192.168.16.254

Uptime: 3:14am up 3:14
CPU: MIPS RISC / 149.91 Mhz
Flash: 8192 KB
Ethernet Status: WAN 1, WAN 2, 12 LAN
Serial Number: AXTTBSKKURESTMDS
Firmware version: HotBrick Version 0_1_0244
Alias LAN IP: 1.1.1.1
Management LAN IP: 1.1.1.2
Management LAN Netmask: 255.255.255.252

- Log files and Alert messages will be sent to Administrator

Figure 3.2
Default Advanced Setup page with advanced menus circled

From here, click on the System Service menu link to bring up the System Service tabs. The default tab showing will be the Time tab which allows you to configure the Firewall VPN's clock. You are looking for the Administrator tab (Figure 3.3). Click on it to bring up Figure 3.4.



System Status
Serial Number: AKTTBSKKURESTMDS
The machine has been up: 03:12am up 3:12
CPU: busy=30%
RAM: Total: 32768 KB Free: 8880 KB
Storage: Total: 1216 KB Free: 636 KB

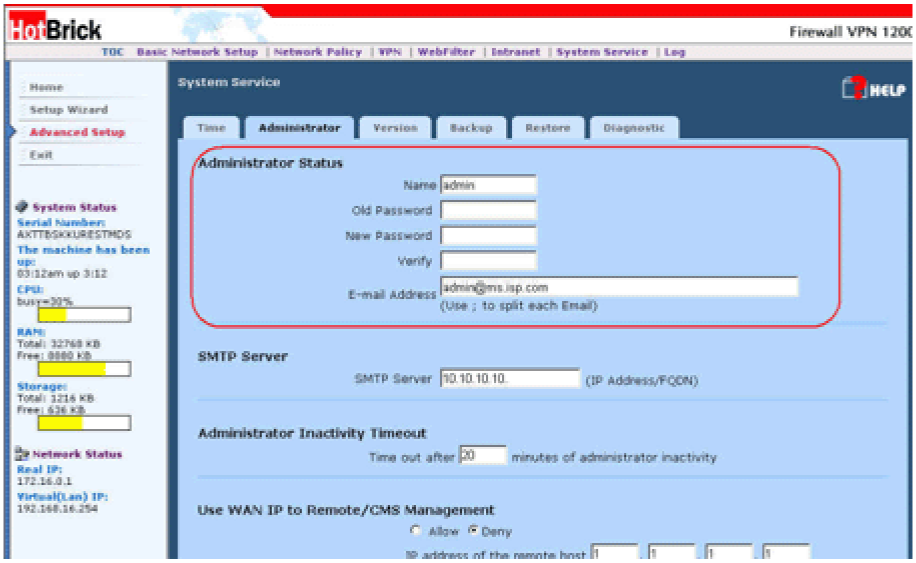
Network Status
Real IP: 172.16.0.1
Virtual(Lan) IP: 192.168.16.254

Current Time: Tue Nov 30 03:15:02 GMT 1999

Synchronization Settings

Synchronize now : ○ Auto ○ Manual ● No
Select Time Zone : America/Anchorage
Manual Time Correction : Date: Nov Month 30 Day 2000 Year
Time: 03 : 15 : 02
Time server : ○ (IP Address/FQDN)
● time.nist.gov
Automatically synchronize : ○ Once per 1hr
● Disable

Figure 3.3
System Service tabs with Administrator tab circled.



System Status
Serial Number: AKTTBSKKURESTMDS
The machine has been up: 03:12am up 3:12
CPU: busy=30%
RAM: Total: 32768 KB Free: 8880 KB
Storage: Total: 1216 KB Free: 636 KB

Network Status
Real IP: 172.16.0.1
Virtual(Lan) IP: 192.168.16.254

Administrator Status

Name admin
Old Password
New Password
Verify
E-mail Address admin@ms.isp.com
(Use ; to split each Email)

SMTP Server

SMTP Server 10.10.10.10. (IP Address/FQDN)

Administrator Inactivity Timeout

Time out after 20 minutes of administrator inactivity

Use WAN IP to Remote/CMS Management

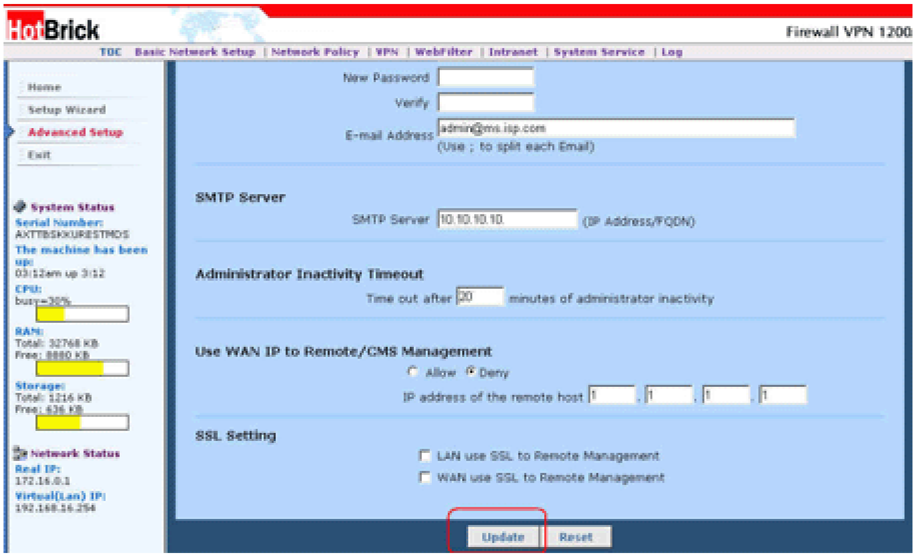
○ Allow ● Deny
IP address of the remote host 1 . 1 . 1 . 1

Figure 3.4
Administrator tab with Administrator Status block marked.

Once on this tab, you can see immediately the first item on the page is the Administrator account information (Figure 3.4). This should be fairly self-explanatory; Name is the current login name of the administrator, Old Password is the old password, New Password is the password you want to change the old password to, Verify is a second New Password field to be sure you have not mistyped it the first time, and E-mail Address is the email address of the administrator, to which critical email messages from the

Firewall VPN will be sent. Make any changes to these fields as you like. These changes are not final until you scroll down and click on the Update button (Figure 3.5). The Firewall VPN will verify it has performed the change (Figure 3.6). Click Exit to return to the Administrator tab. Note: You may change the administrator login name and the email address without entering a password. Changing the password is the only function that requires a reconfirmation of the old password. Additionally, the administrator login name cannot have any slashes ("/" or "\") or spaces and is limited to 16 characters, while the password cannot have any spaces, backslashes ("\"), or periods and is limited to 12 characters.

Congratulations, you have performed your first Firewall VPN customization!


HotBrick
Firewall VPN 1200
TOC | Basic Network Setup | Network Policy | VPN | WebFilter | Intranet | System Service | Log
Home
Setup Wizard
Advanced Setup
Exit
Update
Reset

System Status
Serial Number: AXTTBSKKURESTMDS
The machine has been up: 03:12am up 3:12
CPU: busy=30%
RAM: Total: 32768 KB Free: 8880 KB
Storage: Total: 1216 KB Free: 636 KB
Network Status
Real IP: 172.16.0.1
Virtual(Lan) IP: 192.168.16.254

New Password:
Verify:
E-mail Address: admin@ms.isp.com
(Use ; to split each Email)

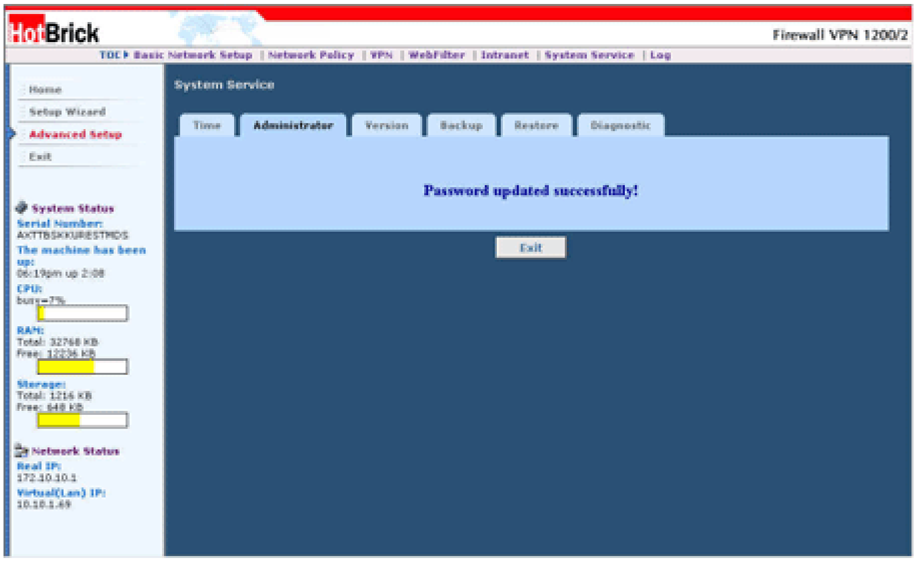
SMTP Server
SMTP Server: 10.10.10.10 (IP Address/FQDN)

Administrator Inactivity Timeout
Time out after 30 minutes of administrator inactivity

Use WAN IP to Remote/CMS Management
○ Allow ● Deny
IP address of the remote host 1 . 1 . 1 . 1

SSL Setting
□ LAN use SSL to Remote Management
□ WAN use SSL to Remote Management

Figure 3.5
Administrator tab with Update button circled.



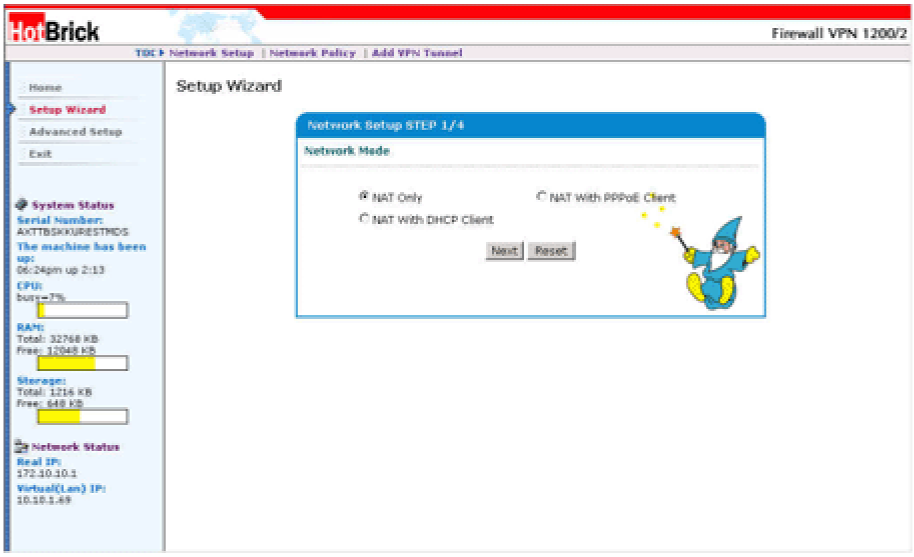
System Status
Serial Number: AXTTBSKKURESTMDS
The machine has been up: 06:19pm up 2:08
CPU: busy=7%
RAM: Total: 32768 KB Free: 12236 KB
Storage: Total: 1216 KB Free: 648 KB
Network Status
Real IP: 172.10.10.1
Virtual(Lan) IP: 10.10.1.69

Password updated successfully!

Figure 3.6
Password Updated Confirmation Screen

4. Configuring the Firewall VPN for Your Network

To configure your Firewall VPN for the first time we recommend using the Setup Wizard, which can be accessed at any time from a similarly named button on the left menu (figure 4.1).



System Status
Serial Number: AXTTBSKKURESTMDS
The machine has been up: 06:24pm up 2:13
CPU: busy=7%
RAM: Total: 32768 KB Free: 12048 KB
Storage: Total: 1216 KB Free: 648 KB
Network Status
Real IP: 172.10.10.1
Virtual(Lan) IP: 10.10.1.69

Setup Wizard

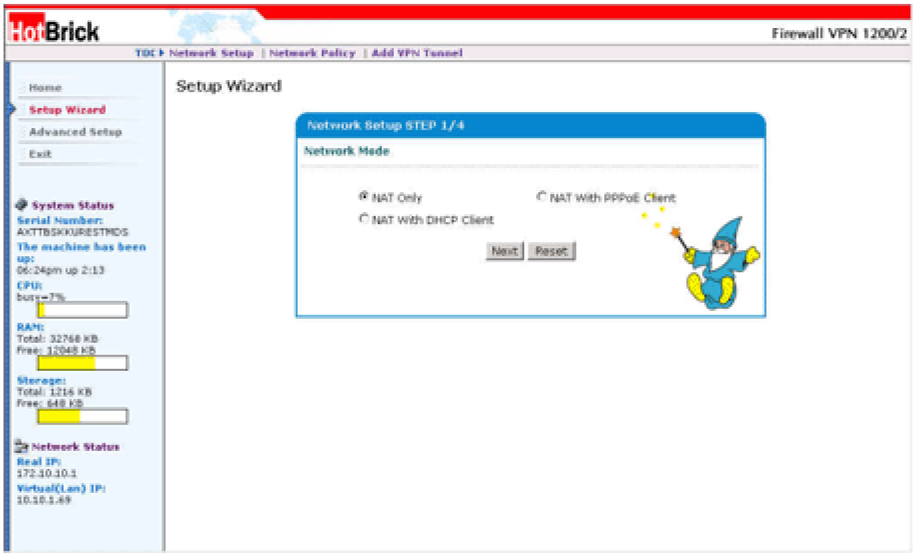
Network Setup STEP 1/4

Network Mode

● NAT Only ○ NAT With PPPoE Client
○ NAT With DHCP Client

Figure 4.1
System Service menu, Administrator tab with the Setup Wizard button circled.

Clicking on the Setup Wizard button will bring up the first of four major steps to configuring your Firewall VPN, Network Mode (Figure 4.2). You might notice along the top there are different menus, Network Setup, Network Policy, and Add VPN Tunnel. These menus lead to different wizards covering the major aspects of your Firewall VPN; network configuration, Firewall rules, and adding new VPN tunnels respectively.



System Status
Serial Number: AXTTBSKKURESTMDS
The machine has been up: 06:24pm up 2:13
CPU: busy=7%
RAM: Total: 32768 KB Free: 12048 KB
Storage: Total: 1216 KB Free: 648 KB
Network Status
Real IP: 172.10.10.1
Virtual(Lan) IP: 10.10.1.69

Setup Wizard

Network Setup STEP 1/4

Network Mode

● NAT Only ○ NAT With PPPoE Client
○ NAT With DHCP Client

Figure 4.2
Setup Wizard, Network Setup Step 1/4, Network Mode.

The network modes are defined as follows.

NAT Only:

This mode refers to the network configuration in which the Firewall VPN external IP and DMZ IP's share the same subnet, but the LAN uses a private addressing scheme for its IP's. This is one of the most common network configurations for fixed external IP's on broadband connections; with the only major difference between implementations is how LAN IP addresses are handled.

NAT with PPPoE Client:

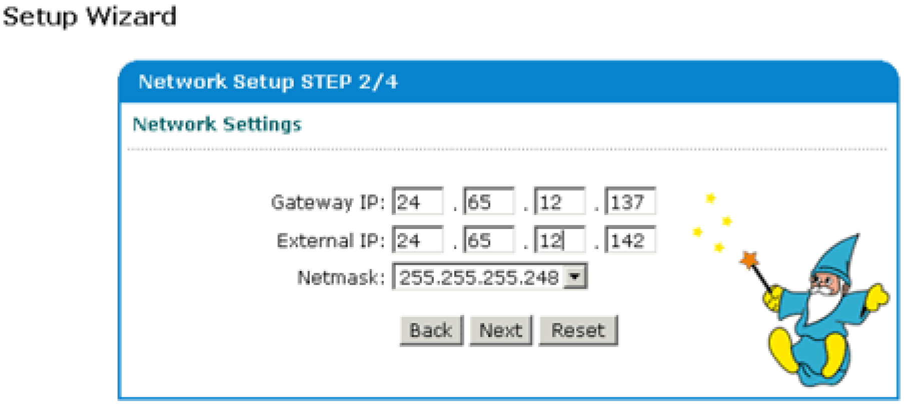
This mode is similar to the NAT only network configuration except that your ISP configures the gateway IP address and Firewall VPN external IP and netmask. There is no DMZ in this configuration, since PPPoE only supports the auto-configuration of a single "dial-up" machine by the ISP. This is increasingly becoming a common network configuration for the home user subscribing to ADSL.

NAT with DHCP Client:

This mode is similar to the NAT with PPPoE Client network configuration except that instead of using PPPoE, the Firewall VPN obtains its gateway, external IP and netmask from a DHCP server. This is not to be confused for using DHCP in your own LAN, but rather DHCP for configuring your external real IP of the Firewall VPN. Like the PPP and PPPoE configurations, there is no DMZ.

Depending on the type of network mode you choose, your second step, the configuration of real IPs of your Firewall VPN, will vary.

If you selected NAT only, your second step (Figure 4.3a) will again consist of filling in the blanks corresponding to information given to you by your ISP.



Setup Wizard

Network Setup STEP 2/4

Network Settings

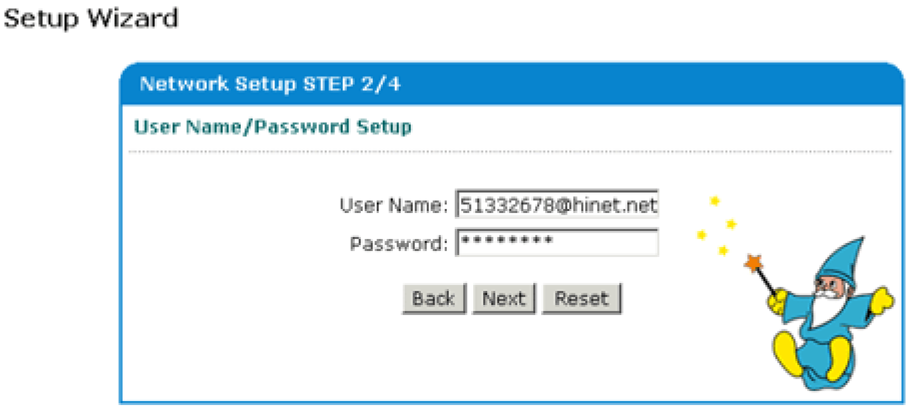
Gateway IP: 24 . 65 . 12 . 137

External IP: 24 . 65 . 12 . 142

Netmask: 255.255.255.248

Figure 4.3a
Setup Wizard, Network Setup 2/4, Network Settings, NAT Only, sample settings.

Selecting NAT with PPPoE Client will bring you to a screen where you enter your user name and password to log into your ADSL provider (Figure 4.3b).



Setup Wizard

Network Setup STEP 2/4

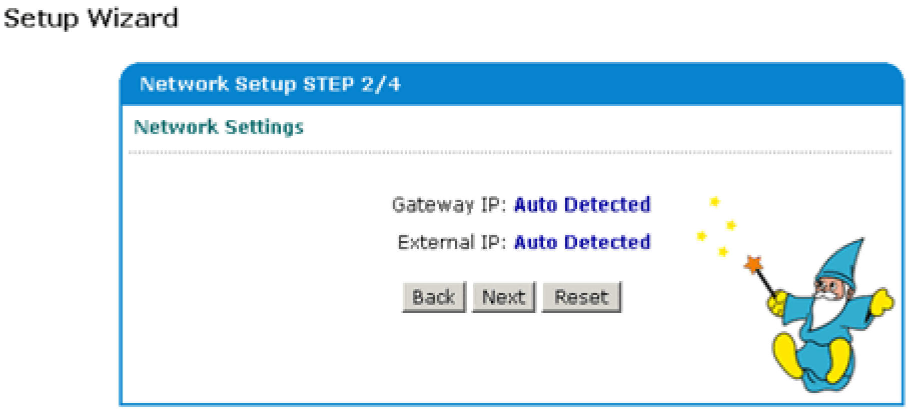
User Name/Password Setup

User Name: 51332678@hinet.net

Password: *********

Figure 4.3b
Setup Wizard, Network Setup 2/4, Network Settings, NAT with PPPoE Client, sample settings

Selecting NAT with DHCP Client, luckily means that there is no configuration needed in this step. Click on Next to continue (Figure 4.3d).



Setup Wizard

Network Setup STEP 2/4

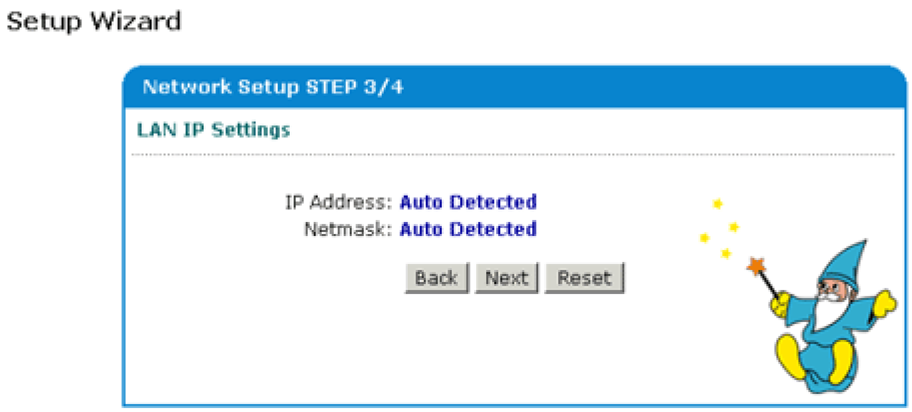
Network Settings

Gateway IP: Auto Detected

External IP: Auto Detected

Figure 4.3d
Setup Wizard, Network Setup 2/4, Network Settings, NAT with DHCP Client

The third step is for configuring the internal IP of the Firewall VPN. Naturally for Standard Transparent mode, which has no internal IP, this step needs no configuration (Figure 4.4a). However for all NAT modes, this step is the same. You may notice the Firewall VPN is already configured for a 192.168.0.1/16 network (Figure 4.4b). Simply change these values to match your internal network needs. All computers connecting to the LAN ports of the Firewall VPN require the IP entered here as their gateway.



Setup Wizard

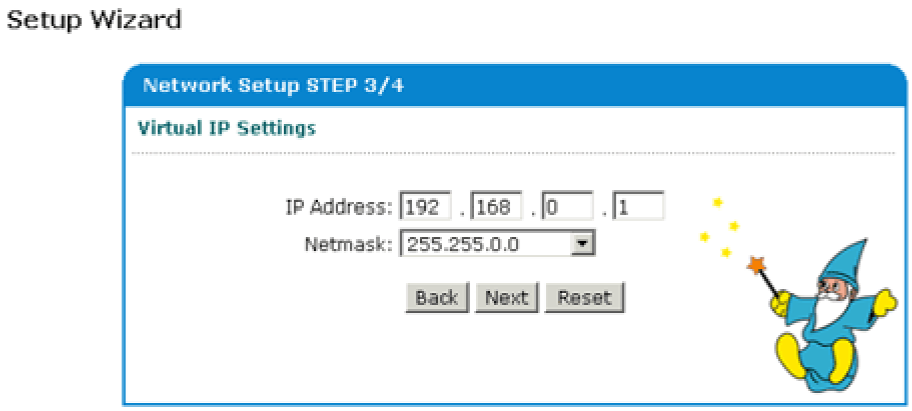
Network Setup STEP 3/4

LAN IP Settings

IP Address: Auto Detected

Netmask: Auto Detected

Figure 4.4a
Setup Wizard, Network Setup 3/4, Network Settings, Standard Transparent



Setup Wizard

Network Setup STEP 3/4

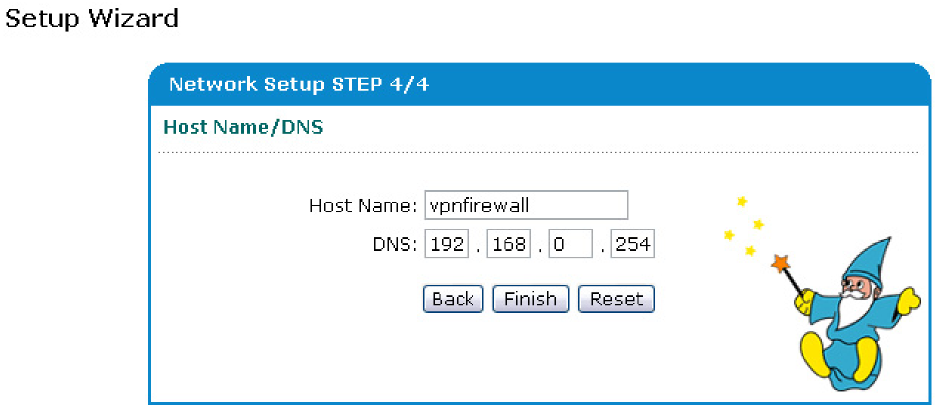
Virtual IP Settings

IP Address: 192 . 168 . 0 . 1

Netmask: 255.255.0.0

Figure 4.4b
Setup Wizard, Network Setup 3/4, Network Settings, all NAT modes

The fourth and final step for configuring the network setup of the Firewall VPN is setting the Firewall VPN's hostname and primary DNS. The hostname cannot have any uppercase or otherwise non-alphanumeric characters. Once you have filled in this information, click Finish to finalize your network configuration.



Setup Wizard

Network Setup STEP 4/4

Host Name/DNS

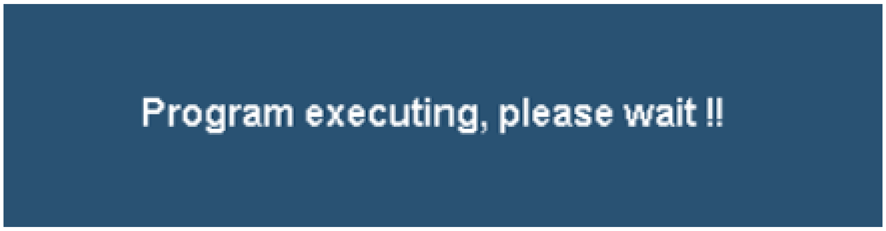
Host Name: vpnfirewall

DNS: 192 . 168 . 0 . 254

Figure 4.5
Setup Wizard, Network Setup 4/4, Network Settings, all modes.

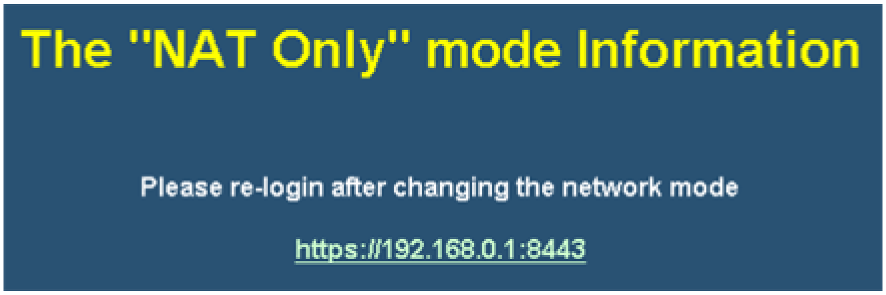
Clicking on finish will bring up a screen that shows text similar to Figure 4.6. You might notice there is a thirty second countdown in the lower left hand status bar. When the countdown is finished, the Firewall VPN will confirm what mode you have selected, and then will ask you to reconnect (Figure 4.7).

Congratulations, your Firewall VPN is now ready to be placed into your network!



Program executing, please wait !!

Figure 4.6
Setup Wizard, Network Setup finalization.



The "NAT Only" mode Information

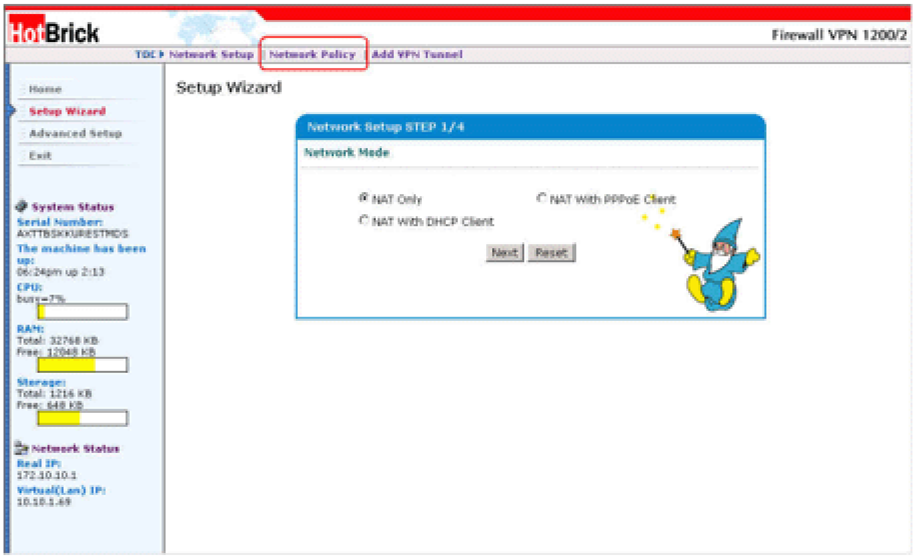
Please re-login after changing the network mode

https://192.168.0.1:8443

Figure 4.7
Setup Wizard, Network Setup Changed, NAT Only, “please reconnect.”

5. Configuring the Firewall VPN

By default, the Firewall VPN is completely open to minimize installation problems. However, this is not optimal in terms of information security. To begin configuring the firewall, click on the Setup Wizard button on the left menu. This will bring up the Network Settings Wizard (Figure 4.2). As noted before, the menus along the top change to reflect the three major wizards for the Firewall VPN. In this case we are interested in the Network Policy link (Figure 5.1).



Setup Wizard

Network Setup STEP 1/4

Network Mode

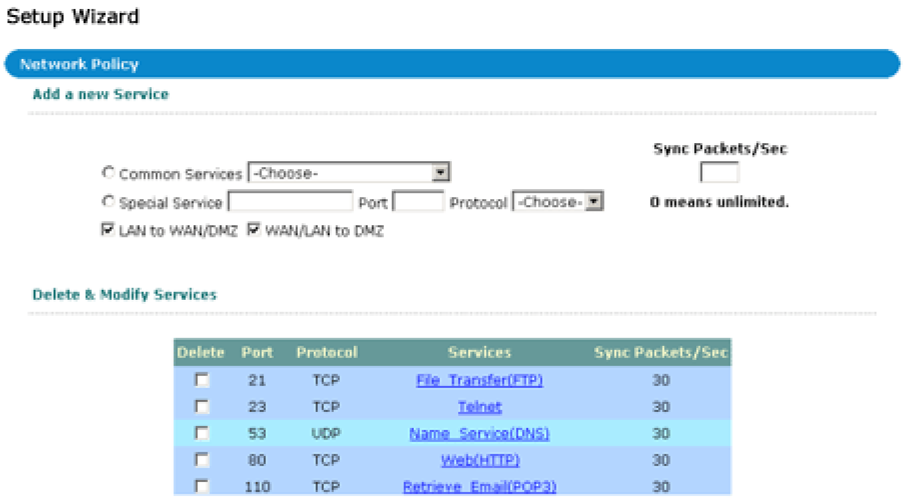
● NAT Only ○ NAT With PPPoE Client
○ NAT With DHCP Client

System Status
Serial Number: AKTTBSKKURESTMDS
The machine has been up: 06:24pm up 2:13
CPU: busy=7%
RAM: Total: 32768 KB Free: 12048 KB
Storage: Total: 1216 KB Free: 648 KB

Network Status
Real IP: 172.10.10.1
Virtual(Lan) IP: 10.10.1.69

Figure 5.1
Setup Wizard, Network Setup screen, Network Policy link circled.

After clicking on the Network Policy link, you will see a screen similar to Figure 5.2. This was designed for quickly adding and removing services, critical for your network needs. Most of the common services can be added via the Common Services radio button and pull down menu (Figure 5.3).



Setup Wizard

Network Policy

Add a new Service

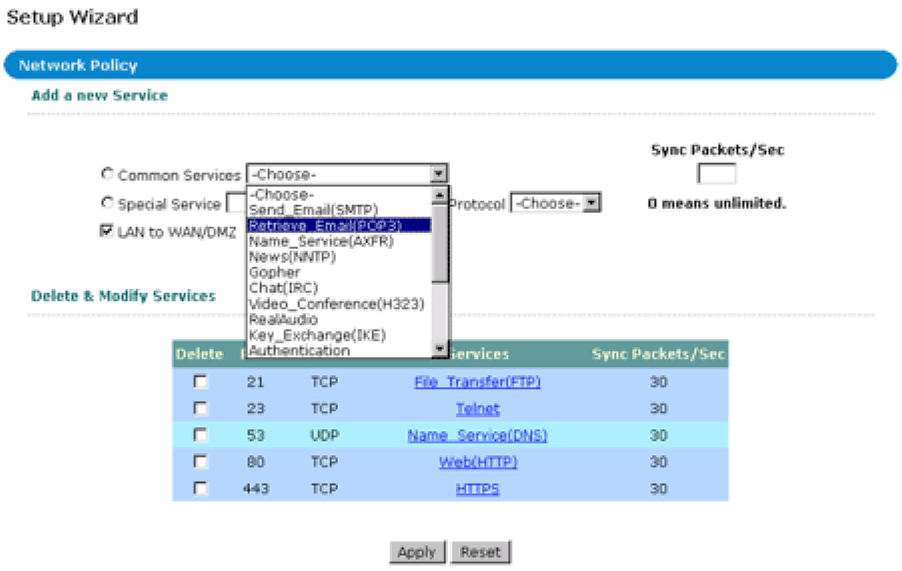
○ Common Services -Choose-
○ Special Service Port Protocol -Choose-
☑ LAN to WAN/DMZ ☑ WAN/LAN to DMZ

Sync Packets/Sec
0 means unlimited.

Delete & Modify Services

Delete	Port	Protocol	Services	Sync Packets/Sec
□	21	TCP	File Transfer(FTP)	30
□	23	TCP	Telnet	30
□	53	UDP	Name Service(DNS)	30
□	80	TCP	Web(HTTP)	30
□	110	TCP	Retrieve Email(POP3)	30

Figure 5.2
Setup Wizard, Network Policy.



Setup Wizard

Network Policy

Add a new Service

○ Common Services -Choose-

○ Special Service

☑ LAN to WAN/DMZ

Protocol -Choose-

Sync Packets/Sec

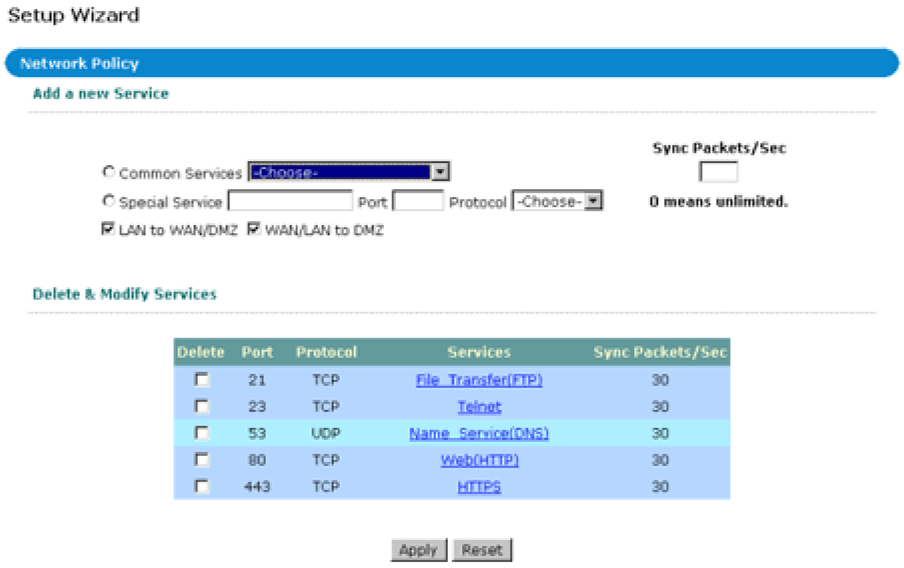
0 means unlimited.

Delete & Modify Services

Delete			Services	Sync Packets/Sec
□	21	TCP	File_Transfer(FTP)	30
□	23	TCP	Telnet	30
□	53	UDP	Name_Service(DNS)	30
□	80	TCP	Web(HTTP)	30
□	443	TCP	HTTPS	30

Figure 5.3
Setup Wizard, Network Policy, Common Services pull down menu

Adding services to the Firewall VPN becomes easy as you select the service and click on the Apply button. As you add each service, the list under Delete & Modify Services will grow (Figure 5.4).



Setup Wizard

Network Policy

Add a new Service

○ Common Services -Choose-

○ Special Service Port Protocol -Choose-

☑ LAN to WAN/DMZ ☑ WAN/LAN to DMZ

Sync Packets/Sec

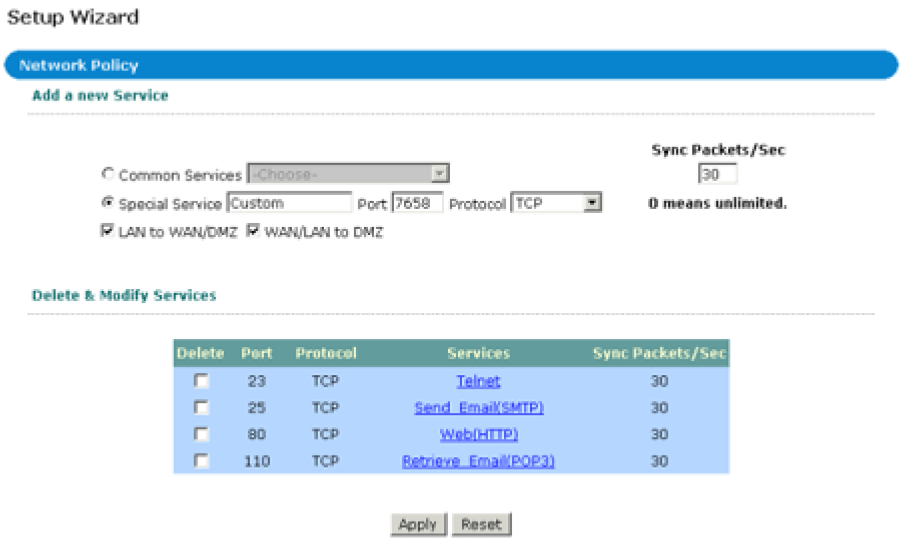
0 means unlimited.

Delete & Modify Services

Delete	Port	Protocol	Services	Sync Packets/Sec
□	21	TCP	File_Transfer(FTP)	30
□	23	TCP	Telnet	30
□	53	UDP	Name_Service(DNS)	30
□	80	TCP	Web(HTTP)	30
□	443	TCP	HTTPS	30

Figure 5.4
Setup Wizard, Network Policy, after adding services.

If a service you want to add is not listed under Common Services, you can add a Special Service. Select the Special Service radio button; fill in a name, the port, and protocol it will use. By default all services are rate limited to thirty initial packets per second. For a small to medium sized company this is more than enough for normal usage (Figure 5.5). Click on Apply to add it to the list.



Setup Wizard

Network Policy

Add a new Service

○ Common Services -Choose-

● Special Service Custom Port 7658 Protocol TCP

☑ LAN to WAN/DMZ ☑ WAN/LAN to DMZ

Sync Packets/Sec 30

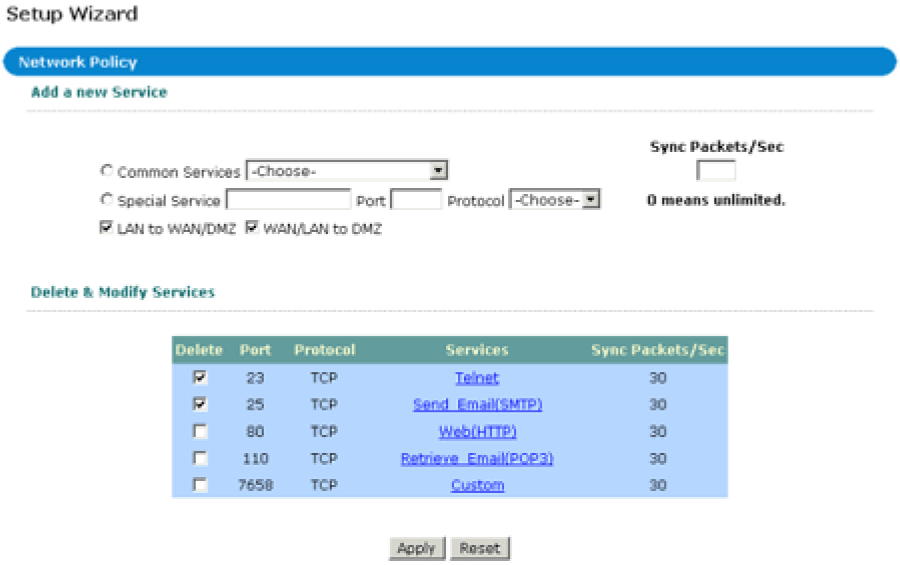
0 means unlimited.

Delete & Modify Services

Delete	Port	Protocol	Services	Sync Packets/Sec
□	23	TCP	Telnet	30
□	25	TCP	Send Email(SMTP)	30
□	80	TCP	Web(HTTP)	30
□	110	TCP	Retrieve Email(POP3)	30

Figure 5.5
Setup Wizard, Network Policy, adding a special service.

After adding the services, you should decide that you no longer want that service, click on the delete checkbox corresponding to the Service and click Apply. You can remove more than one service at a time (Figure 5.6).



Setup Wizard

Network Policy

Add a new Service

○ Common Services -Choose-

○ Special Service Port Protocol -Choose-

☑ LAN to WAN/DMZ ☑ WAN/LAN to DMZ

Sync Packets/Sec

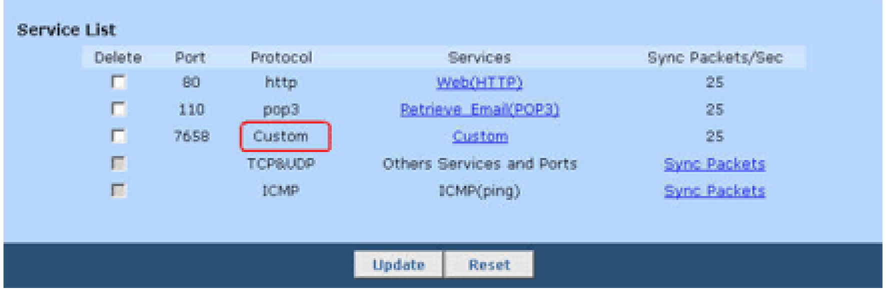
0 means unlimited.

Delete & Modify Services

Delete	Port	Protocol	Services	Sync Packets/Sec
☑	23	TCP	Telnet	30
☑	25	TCP	Send Email(SMTP)	30
□	80	TCP	Web(HTTP)	30
□	110	TCP	Retrieve Email(POP3)	30
□	7658	TCP	Custom	30

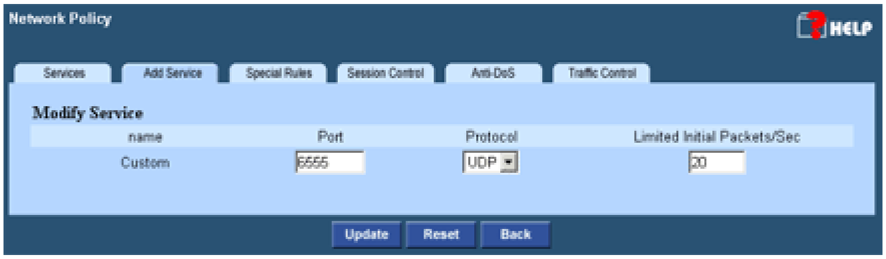
Figure 5.6
Setup Wizard, Network Policy, removing multiple services.

If you only want to modify some of the settings of a service, you can click on the name of the service itself make the changes (Figure 5.7). This will bring you to a service modification page (Figure 5.8). Make you modifications here, and click on Update to finish.


Service List

Delete	Port	Protocol	Services	Sync Packets/Sec
□	80	http	Web(HTTP)	25
□	110	pop3	Retrieve Email(POP3)	25
□	7658	Custom	Custom	25
□		TCP&UDP	Others Services and Ports	Sync Packets
□		ICMP	ICMP(ping)	Sync Packets

Figure 5.7
Setup Wizard, Network Policy, "Custom" service circled.

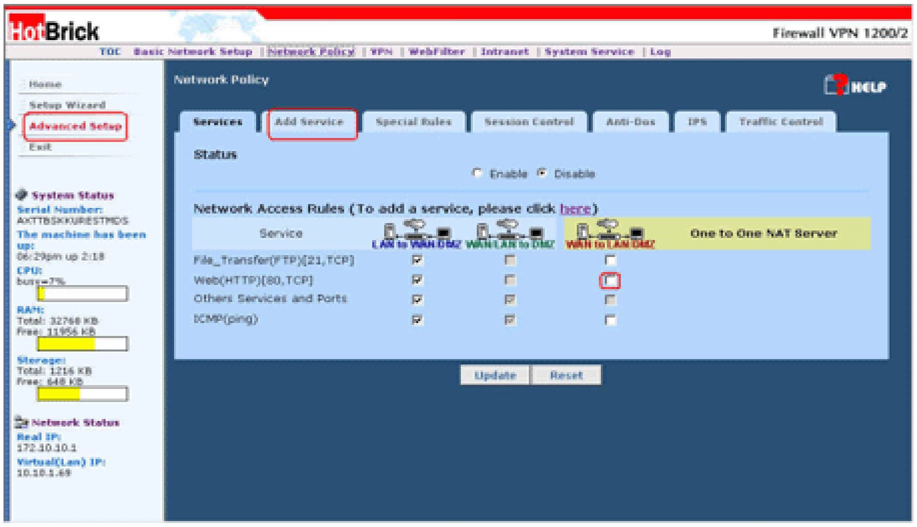


Modify Service

name	Port	Protocol	Limited Initial Packets/Sec
Custom	6555	UDP	20

Figure 5.8
Advanced Setup, Modify Service, "Custom" service modification

Once you are finished, be sure to go to the Advanced Setup, Network Policy menu. The default tab showing will be the Services tab. Then uncheck Others Services and Ports and click Update. This will close the Firewall VPN and only allow the specified services through. (Figure 5.9)



System Status
Serial Number:
AXTTBSKKURESTMDS
The machine has been up:
06:29pm up 2:18
CPU:
busy=7%
RAM:
Total: 32768 KB
Free: 11956 KB
Storage:
Total: 1216 KB
Free: 648 KB

Network Status
Real IP:
172.10.10.1
Virtual(Lan) IP:
10.10.1.69

Status
○ Enable ● Disable

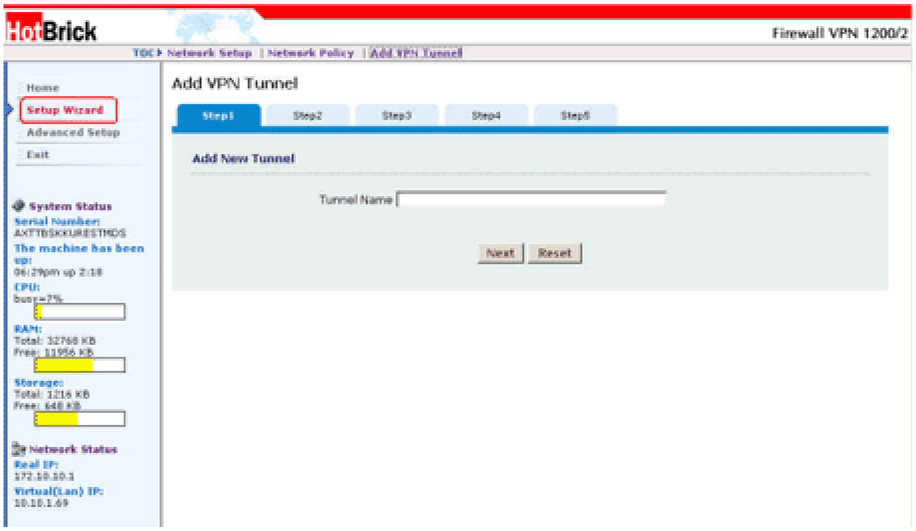
Network Access Rules (To add a service, please click here)

Service	LAN to WAN/DMZ	WAN/LAN to DMZ	WAN to LAN/DMZ	One to One NAT Server
File_Transfer(FTP)[21,TCP]	☑	□	□	
Web(HTTP)[80,TCP]	☑	□	□	
Others Services and Ports	☑	☑	□	
ICMP(ping)	☑	☑	□	

Figure 5.9
Advanced Setup, Network Policy, Services, closing the Firewall VPN

6. Adding a VPN tunnel

Adding a new tunnel can also be done through the Setup Wizard. Click on the Setup Wizard button on the left and then click on the Add VPN Tunnel link along the top. This will bring up the first step of the wizard for adding a new VPN Tunnel (Figure 6.1). This wizard is only for adding simple tunnels that do not require X509 certificates.



System Status
Serial Number:
AXTTBSKKURESTMDS
The machine has been up:
06:29pm up 2:18
CPU:
busy=7%
RAM:
Total: 32768 KB
Free: 11956 KB
Storage:
Total: 1216 KB
Free: 648 KB
Network Status
Real IP:
172.10.10.1
Virtual(Lan) IP:
10.10.1.69

Figure 6.1
Setup Wizard, Add VPN Tunnel, first step

Enter a tunnel name and click Next. This will take you to the second step (Figure 6.2). This step concerns itself with the type of authentication you wish to use. Most simple tunnels use pre-shared keys in which both sides of a VPN connection share the same secret key. More secure is the RSA signature, in which both sides generate a RSA key pair, one private and one public. You share your public key with everyone so that they can encrypt information intended for you with that public key and only your private key can decrypt that information. So if you intend to use an RSA signature to authenticate the VPN you will need the public key of the machine you will connect to and vice versa. Select the type you intend to use and click on Next.

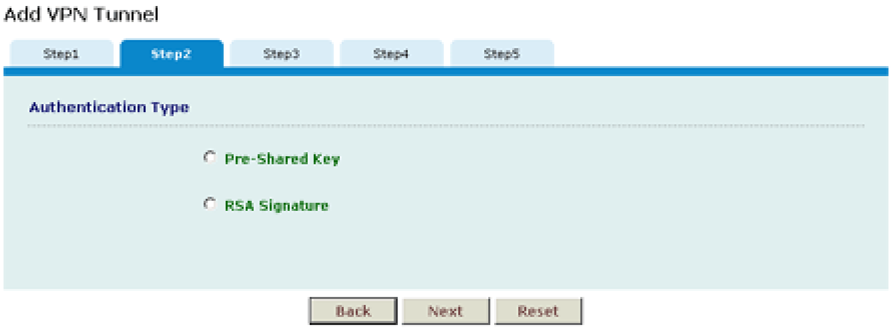
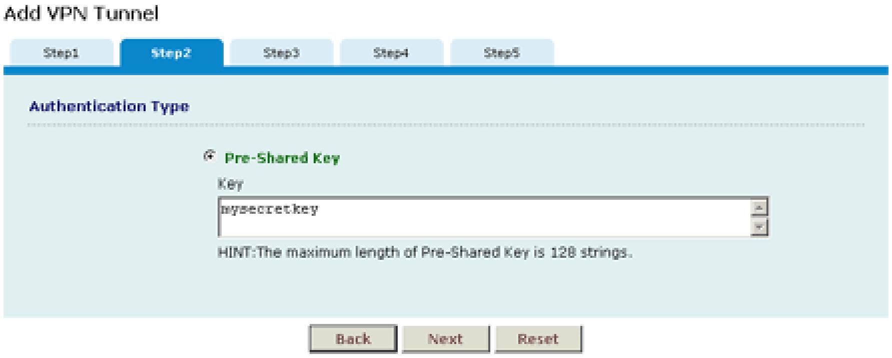


Figure 6.2
Setup Wizard Add VPN Tunnel, second step

Selecting pre-shared key will bring up a screen to enter the pre-shared key (Figure 6.3a). Enter a pre-shared key, hopefully a big more devious than the example, and click Next to continue.



Authentication Type

● Pre-Shared Key

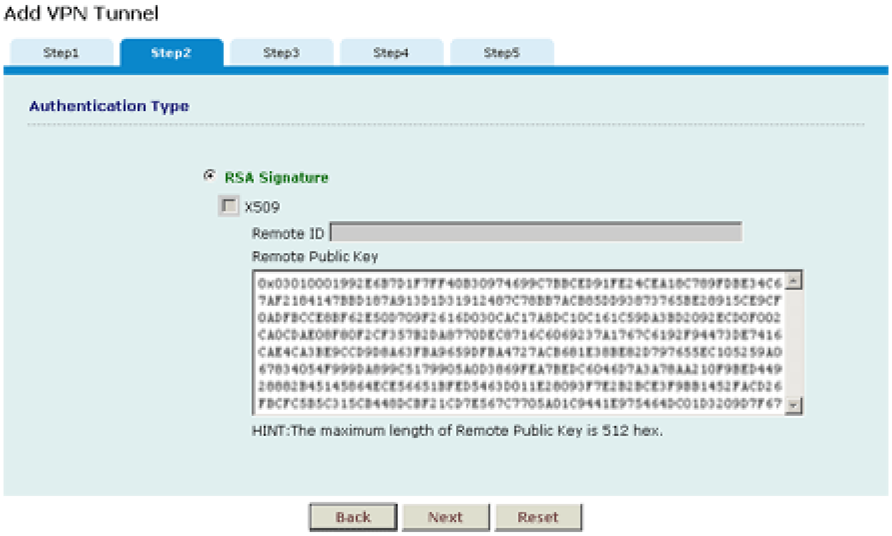
Key

mysecretkey

HINT:The maximum length of Pre-Shared Key is 128 strings.

Figure 6.3a
Setup Wizard, Add VPN Tunnel, step two, sample pre-shared key.

Selecting a RSA signature will bring up a screen to enter the RSA public key of the remote machine with whom you intend to build a tunnel (Figure 6.3b). Copy and paste in the public key, and click Next to continue. Be careful to watch for new line characters, as they also count as spaces and will cause the Firewall VPN to complain about the key.



Authentication Type

● RSA Signature

□ x509

Remote ID

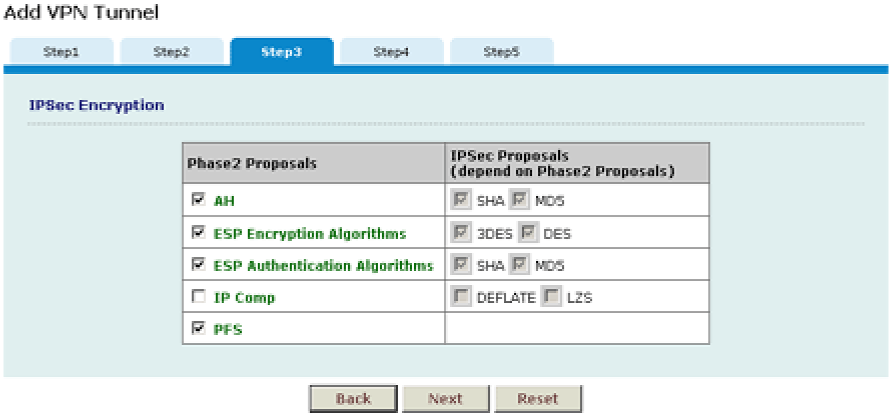
Remote Public Key

```
0x03010001992E4B7D1F7FF40B30974499C7BBCED91FE24CEA10C709FD8E34C6
7AF2104147BBD107A913D1D31912407C70BB7ACB058D93073765BE20915CE9CF
0ADFBCCE0BF62E500709F2616D030CAC17A8DC10C161C59DA3B02092ECD0F002
CA0CDAE08F80F2CF357B2DA0770DEC0716C6069237A1767C6192F94473DE7416
CAE4CA3BE9CCD9D8A63FBA9659DFBA4727ACB601E388E82D797655EC105259AD
67034054F999DA899C51799305A0D3069FEA7BEDC4046D7A3A78AA210F98ED449
20882B45145864ECE56451BFED5463D011E28093F7E2B2BCE3F98B1452FACD26
FBCFC5B5C315CB448DCBF21CD7E567C7705A01C9441E975464DC01D320907F67
```

HINT:The maximum length of Remote Public Key is 512 hex.

Figure 6.3b
Setup Wizard, Add VPN Tunnel, step two, sample remote RSA public key.

The Firewall VPN supports the gamut of VPN protocols; step three allows you to select what protocol you intend to use for this connection. The remote site must support the same protocols you select here. Click Next to continue.



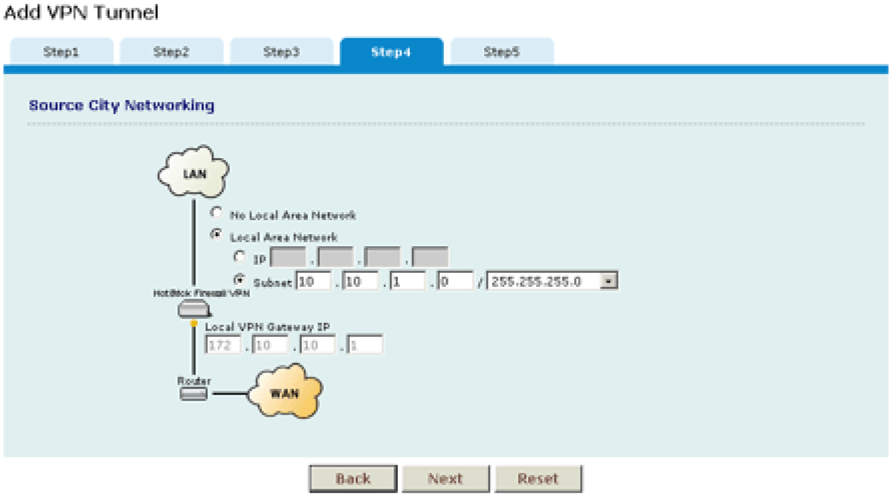
Add VPN Tunnel

IPSec Encryption

Phase2 Proposals	IPSec Proposals (depend on Phase2 Proposals)
☑ AH	☑ SHA ☑ MD5
☑ ESP Encryption Algorithms	☑ 3DES ☑ DES
☑ ESP Authentication Algorithms	☑ SHA ☑ MD5
☐ IP Comp	☐ DEFLATE ☐ LZS
☑ PFS	

Figure 6.4
Setup Wizard, Add VPN Tunnel, step three, selected IPSec encryption protocols.

The fourth step is the network configuration of the Firewall VPN you are currently performing administrative functions upon. The Firewall VPN will attempt to fill in previously entered values; there should be no problem in simply clicking Next to continue.



Add VPN Tunnel

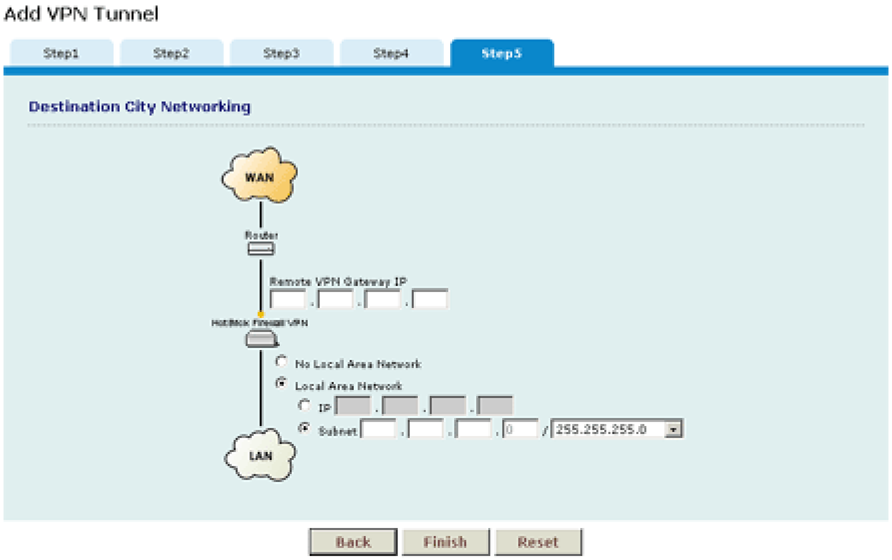
Source City Networking

○ No Local Area Network
● Local Area Network
○ IP _ . _ . _ . _
● Subnet 10 . 10 . 1 . 0 / 255.255.255.0

Local VPN Gateway IP
172 . 10 . 10 . 1

Figure 6.5
Setup Wizard, Add VPN Tunnel, step four, source city networking.

The fifth and last step of adding a new VPN tunnel is the network configuration of the remote site. Since the Firewall VPN does not have any administrative access to the remote site, this information must be completely entered by hand. (Figure 6.6) Click on Finish once you are done to finalize adding a new tunnel. The tunnel will not be created until you hit finish.



Add VPN Tunnel

Destination City Networking

Remote VPN Gateway IP ___ . ___ . ___ . ___

○ No Local Area Network

● Local Area Network

○ IP ___ . ___ . ___ . ___

● Subnet ___ . ___ . ___ . 0 / 255.255.255.0

Figure 6.6
Setup Wizard, Add VPN Tunnel, step five, destination city networking

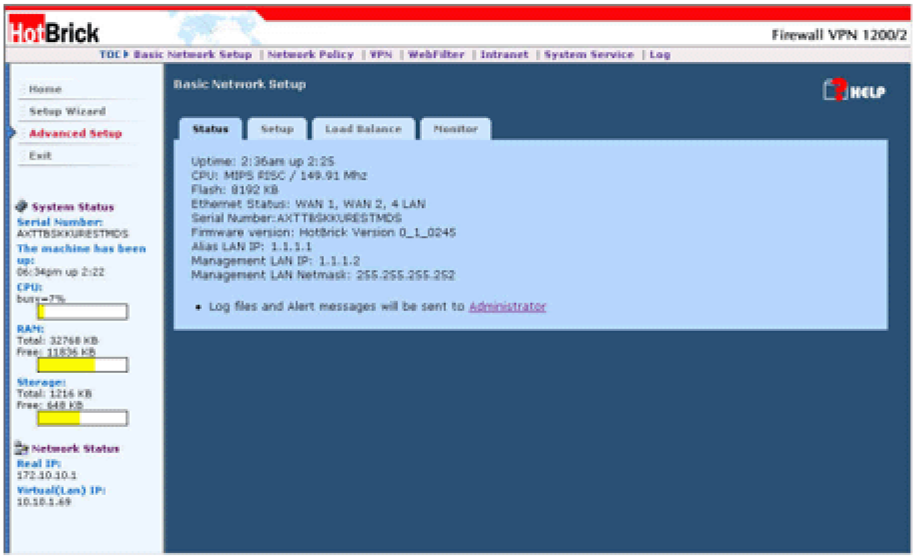
For more information on how to configure the connection for your remote users to your corporate office, please refer to page 43, sections "Configure a VPN Connection to Your Corporate Network in Windows 2000" or "Configure a VPN Connection to Your Corporate Network in Windows XP"

7. Overview of Advanced Setup

Basic Network Setup

Status

This is the first page of the Firewall VPN web administration interface after logging in. This page displays various pieces of information about your Firewall VPN and its current runtime performance. To return to this page later, simply click on the "Basic Setup" menu button.



System Status
Serial Number:
AXTTBSKKURESTMDS
The machine has been up:
06:34pm up 2:22
CPU:
busy=7%
RAM:
Total: 32768 KB
Free: 11836 KB
Storage:
Total: 1216 KB
Free: 648 KB
Network Status
Real IP:
172.10.10.1
Virtual(Lan) IP:
10.10.1.69

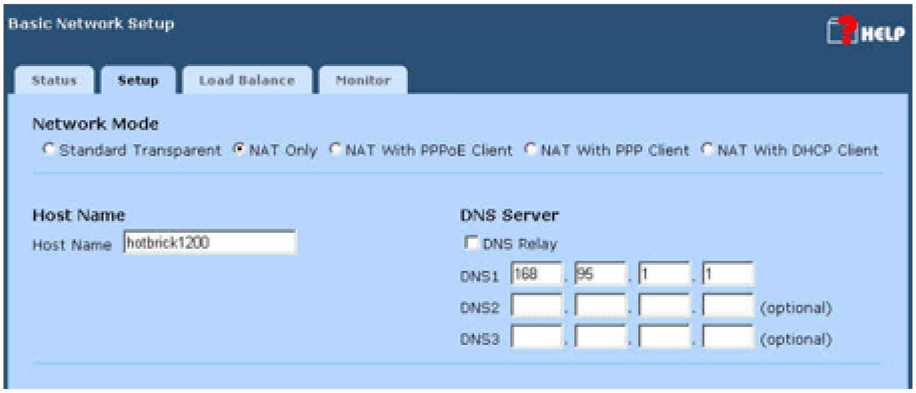
Uptime: 2:36am up 2:25
CPU: MIPS RISC / 149.91 Mhz
Flash: 8192 KB
Ethernet Status: WAN 1, WAN 2, 4 LAN
Serial Number:AXTTBSKKURESTMDS
Firmware version: HotBrick Version 0_1_0245
Alias LAN IP: 1.1.1.1
Management LAN IP: 1.1.1.2
Management LAN Netmask: 255.255.255.252

- Log files and Alert messages will be sent to Administrator

Figure 7.1

Setup

The next tab under the Basic Setup menu button is the Setup tab. This tab allows you to configure the Firewall VPN to conform to your internal network. The first option is the Network Mode. Please refer to section 4. "Configuring the Firewall VPN for Your Network" for more detail about each mode.



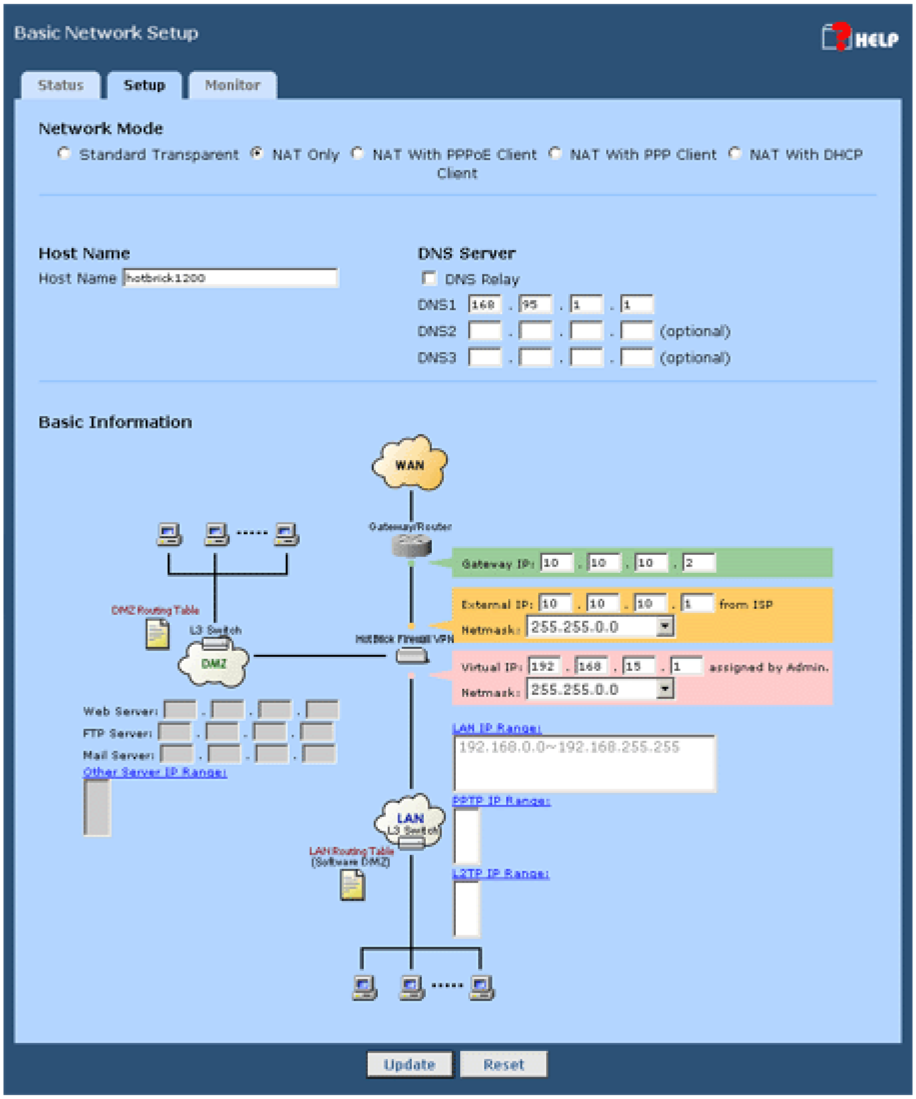
Network Mode
○ Standard Transparent ● NAT Only ○ NAT With PPPoE Client ○ NAT With PPP Client ○ NAT With DHCP Client

Host Name
Host Name hotbrick1200

DNS Server
□ DNS Relay
DNS1 168 . 95 . 1 . 1
DNS2 . . . (optional)
DNS3 . . . (optional)

Figure 7.2
Network Modes

You might note that the network picture below changes from mode to mode, this is because of the nature of each mode lends itself to different network configurations.



Basic Network Setup

HELP

Status | Setup | Monitor

Network Mode

○ Standard Transparent ● NAT Only ○ NAT With PPPoE Client ○ NAT With PPP Client ○ NAT With DHCP Client

Host Name

Host Name: hotbrick1200

DNS Server

□ DNS Relay

DNS1: 168 . 95 . 1 . 1

DNS2: . . . (optional)

DNS3: . . . (optional)

Basic Information

Gateway IP: 10 . 10 . 10 . 2

External IP: 10 . 10 . 10 . 1 from ISP

Netmask: 255.255.0.0

Virtual IP: 192 . 168 . 15 . 1 assigned by Admin.

Netmask: 255.255.0.0

Web Server: . . .

FTP Server: . . .

Mail Server: . . .

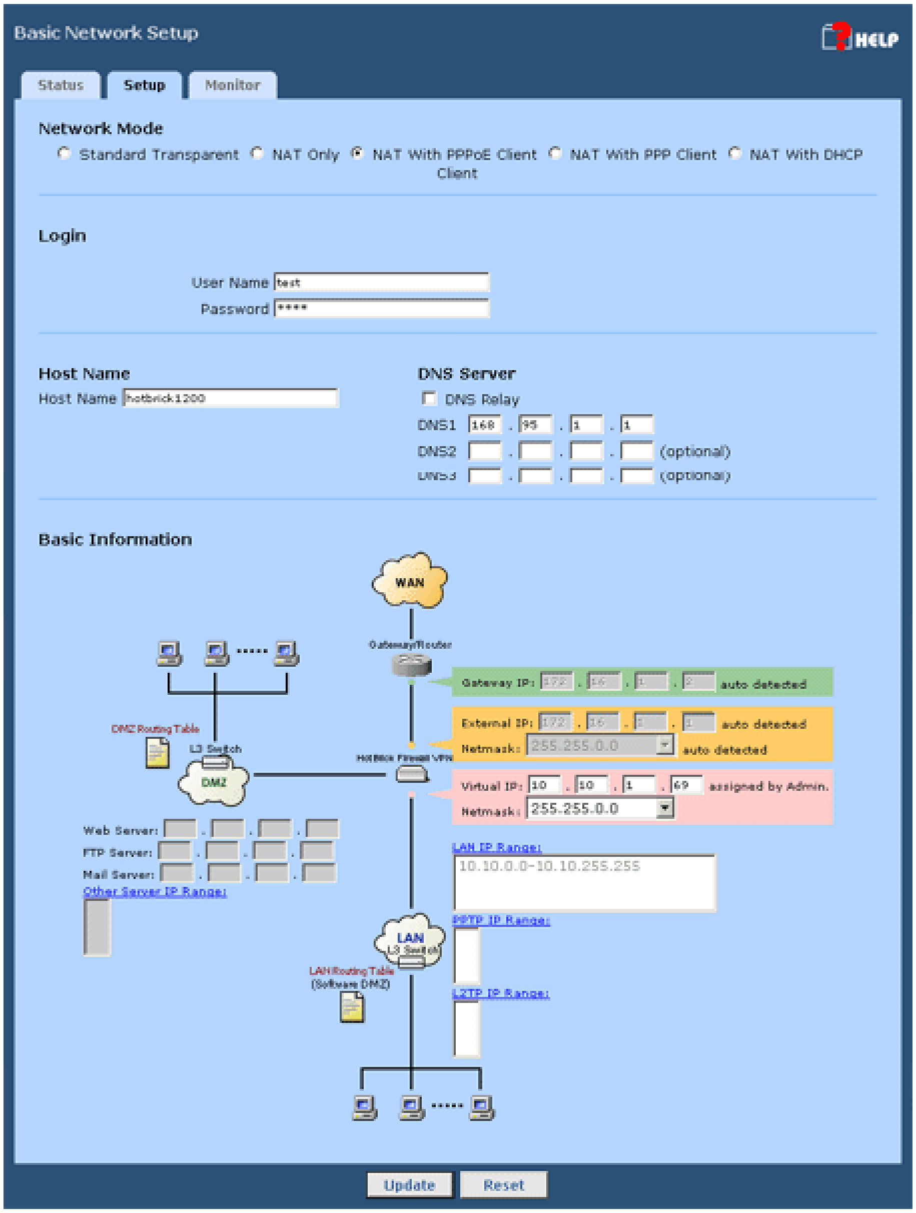
Other Server IP Range:

LAN IP Range: 192.168.0.0~192.168.255.255

PPTP IP Range:

L2TP IP Range:

Figure 7.3
NAT Only Mode



Network Mode

○ Standard Transparent ○ NAT Only ● NAT With PPPoE Client ○ NAT With PPP Client ○ NAT With DHCP Client

Login

User Name: test

Password: ****

Host Name

Host Name: hotbrick1200

DNS Server

□ DNS Relay

DNS1: 168 . 95 . 1 . 1

DNS2: . . . (optional)

DNS3: . . . (optional)

Basic Information

Gateway IP: 172 . 16 . 1 . 2 auto detected

External IP: 172 . 16 . 1 . 1 auto detected

Netmask: 255.255.0.0 auto detected

Virtual IP: 10 . 10 . 1 . 69 assigned by Admin.

Netmask: 255.255.0.0

Web Server: . . .

FTP Server: . . .

Mail Server: . . .

Other Server IP Range:

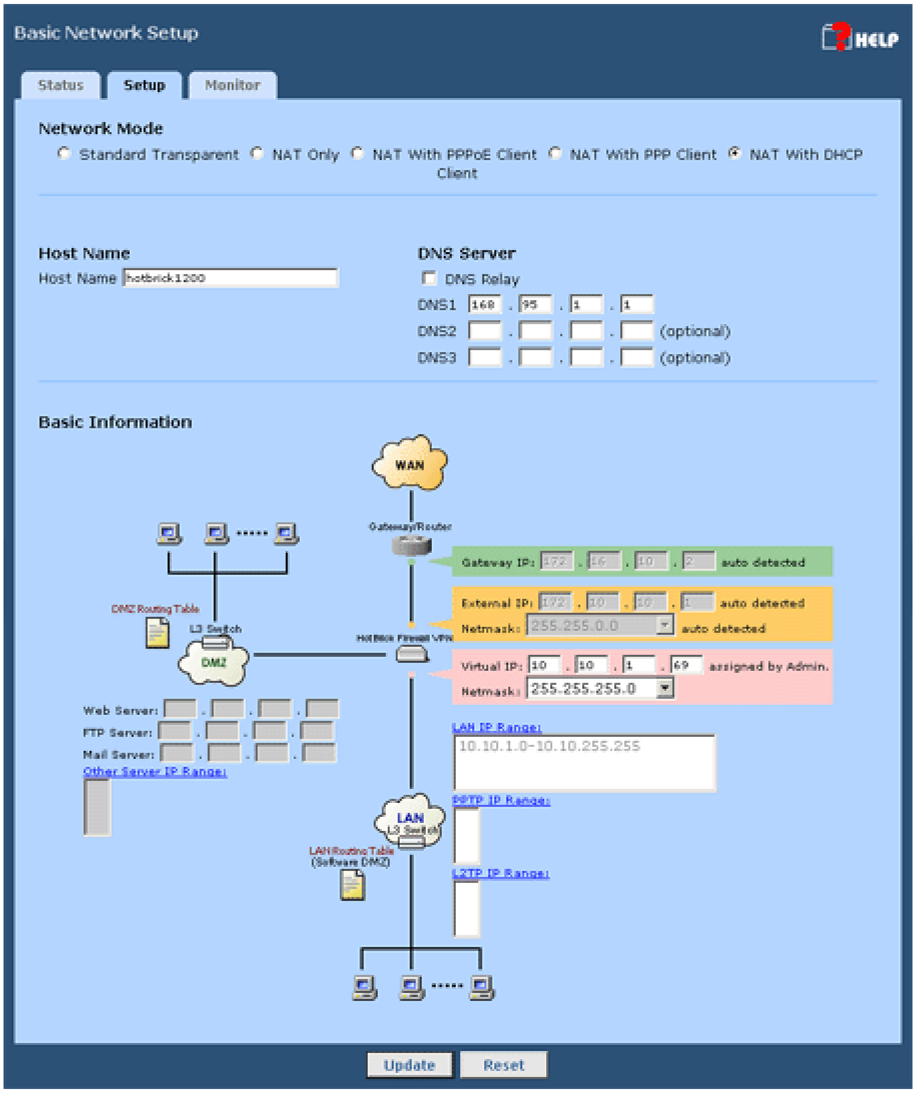
LAN IP Range:

10.10.0.0-10.10.255.255

PPTP IP Range:

L2TP IP Range:

Figure 7.4
NAT with PPPoE Client



Basic Network Setup

Network Mode
○ Standard Transparent ○ NAT Only ○ NAT With PPPoE Client ○ NAT With PPP Client ● NAT With DHCP Client

Host Name
Host Name: hotbrick1200

DNS Server
□ DNS Relay
DNS1: 168 . 95 . 1 . 1
DNS2: . . . (optional)
DNS3: . . . (optional)

Basic Information

Gateway IP: 172 . 16 . 10 . 2 auto detected
External IP: 172 . 10 . 10 . 1 auto detected
Netmask: 255.255.0.0 auto detected
Virtual IP: 10 . 10 . 1 . 69 assigned by Admin.
Netmask: 255.255.255.0

Web Server: . . .
FTP Server: . . .
Mail Server: . . .
Other Server IP Range:

LAN IP Range:
10.10.1.0-10.10.255.255

PPTP IP Range:

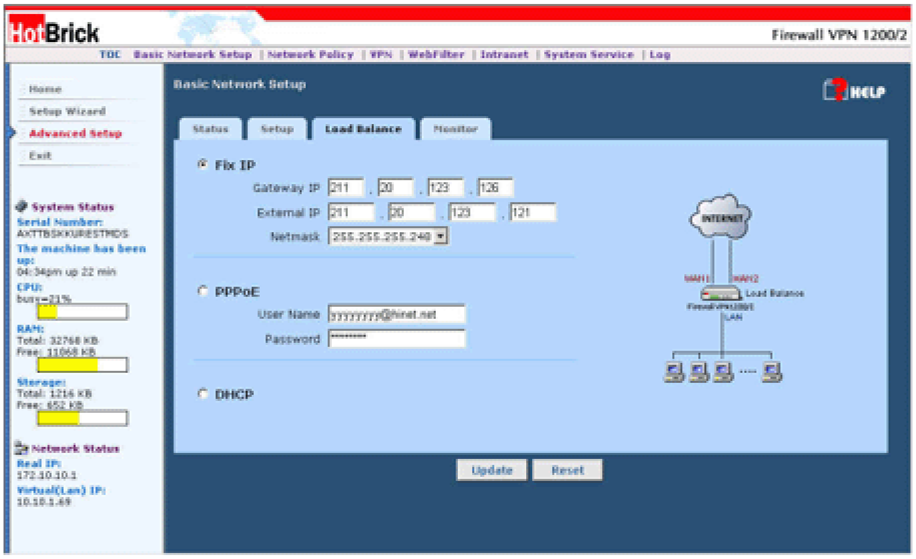
L2TP IP Range:

Figure 7.5
NAT with DHCP Client

Load Balance

This function allows you to setup network for "Load Balance". The Firewall VPN's "Load Balance" function can select one of the Fixed IP, PPPoE or DHCP. The load balance in HotBrick works in the following way:

1. When you have both of your connections active, HotBrick will be constantly checking in which of the connections is faster at that time. For example, if the link in the WAN1 is having a lot of traffic then when the requests from your users will be directed preferably to the WAN2. It also works the other way around.
2. If for whatever reason your connection in either of the WAN connections is down, then the remaining connection will maintain your access to the Internet.



System Status
Serial Number:
AXTTBSKKURESTMDS
The machine has been up:
04:34pm up 22 min
CPU:
busy=21%
RAM:
Total: 32768 KB
Free: 11068 KB
Storage:
Total: 1216 KB
Free: 652 KB
Network Status
Real IP:
172.10.10.1
Virtual(Lan) IP:
10.10.1.69

● Fix IP
Gateway IP 211 . 20 . 123 . 126
External IP 211 . 20 . 123 . 121
Netmask 255.255.255.240

○ PPPoE
User Name yyyyyyyy@hinet.net
Password *********

○ DHCP

Figure 7.6
Load Balance

You can also specify in this tab the number of times HotBrick will try to reestablish the connection you have for your PPPoE or DHCP connection if for any reason it goes down. By default number of attempts is 5.

Monitor

This function allows you to get a quick overview of the Firewall VPN's status. By selecting which summary report you want to display and then clicking "Update" you can view the current statistics for the given report. You may select more than one at a time, and they will all be displayed in a single pop up window sequentially. The reports will refresh in the pop up window every seven seconds. To close this pop up window you can click the "Exit" button at the bottom of the page or click on the close window icon for your browser.

Traffic Control

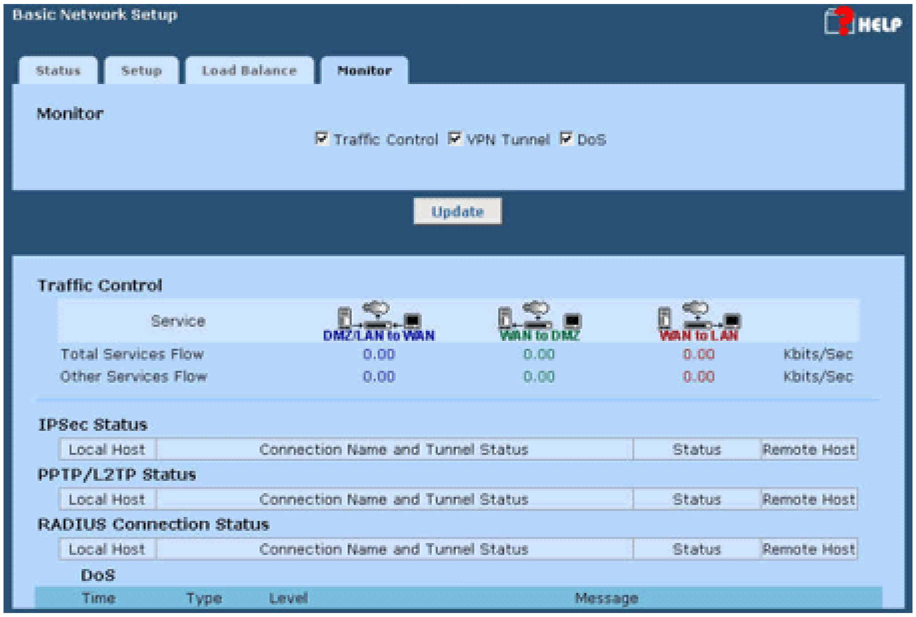
This summary report shows current bandwidth usage statistics for each service listed under the Network Policy Services Tab (This is the default tab that is displayed when you click on the Network Policy menu button).

VPN Tunnel

This summary report shows the current status of all VPN tunnels.

DoS

This summary report shows all logged DoS attacks detected and stopped by the Firewall VPN.



Monitor

☑ Traffic Control ☑ VPN Tunnel ☑ DoS

Traffic Control

Service	DMZ/LAN to WAN	WAN to DMZ	WAN to LAN	
Total Services Flow	0.00	0.00	0.00	Kbits/Sec
Other Services Flow	0.00	0.00	0.00	Kbits/Sec

IPSec Status

Local Host	Connection Name and Tunnel Status	Status	Remote Host

PPTP/L2TP Status

Local Host	Connection Name and Tunnel Status	Status	Remote Host

RADIUS Connection Status

Local Host	Connection Name and Tunnel Status	Status	Remote Host

DoS

Time	Type	Level	Message

Figure 7.7
Monitor with Traffic Control and DoS selected.

Network Policy

This menu button allows for configuration of the Firewall VPN to conform to your organization's security policies and information security needs.

Service

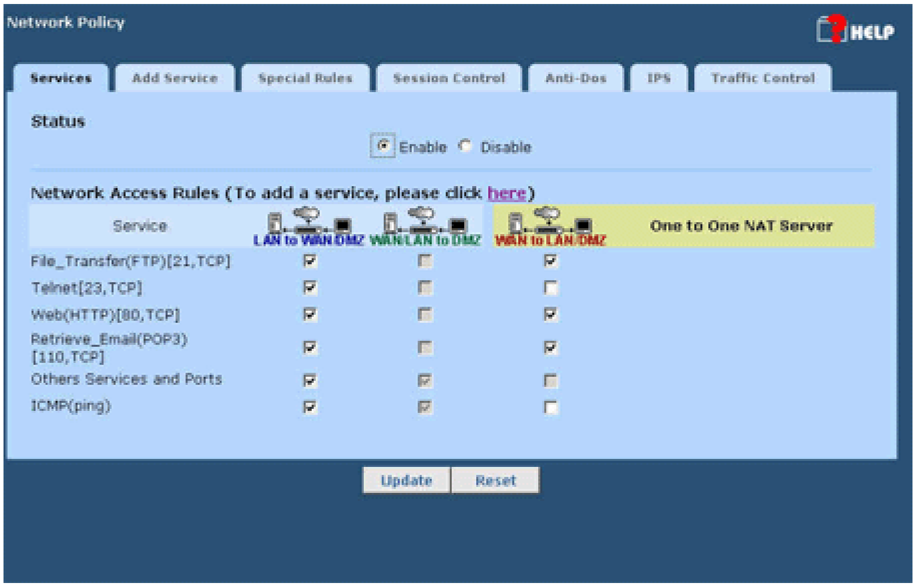
This is the default tab that is displayed when you click on the "Network Policy" menu button. This shows a list of services currently known by the Firewall VPN.

Rules

This list of services known by your Firewall VPN allows for quick enabling and disabling of traffic flows in any given direction through the Firewall VPN. To clarify, these flows, LAN to WAN/DMZ, WAN to LAN/DMZ, and WAN to LAN refer to the capability of the source network to access a server in the destination network. For example, DMZ/LAN to WAN is the direction of network traffic flowing from your local network (DMZ/LAN) to the Internet, referred to as the WAN or wide area network. By clicking the checkbox and thereby enabling this traffic flow for a given service, you allow users from your DMZ or LAN to access that given Internet service from some Internet server. In many cases enabling this flow alone is enough for the typical end-user, since by doing so you do not restrict flow back through the firewall for established TCP connections to Internet servers. Likewise for WAN to DMZ and WAN to LAN, this allows users from the Internet to access servers that you are providing in your DMZ and or LAN, but does not restrict data flowing back to these Internet clients for established connections to your servers.

The final column, "One to One NAT Server," will not show any servers for any services unless you are using one of the NAT modes and add a server into your LAN. The latter of which can be done through the "Add Service" tab, or by clicking on the "Intranet" menu button, then the "One to One NAT" tab. This will be covered in more detail later.

To make changes to this page, and therefore to network policy through the Firewall VPN, simply click on the checkbox desired and click "Update" at the bottom of the list.



Status

● Enable ○ Disable

Network Access Rules (To add a service, please click here)

Service	LAN to WAN/DMZ	WAN/LAN to DMZ	WAN to LAN/DMZ	One to One NAT Server
File_Transfer(FTP)[21,TCP]	☑	□	☑	
Telnet[23,TCP]	☑	□	□	
Web(HTTP)[80,TCP]	☑	□	☑	
Retrieve_Email(POP3)[110,TCP]	☑	□	☑	
Others Services and Ports	☑	☑	□	
ICMP(ping)	☑	☑	□	

Figure 7.8
Network Policy, Services tab

Add Service

This tab allows the administrator to add and remove services from the Firewall VPN. You might note that under "Service List," the Firewall VPN lists all of the known services by increasing port number order, regardless if they are enabled or not. Common services, such as email and web access can be quickly added and removed, since they are included by default into the Firewall VPN database of services. To add such a service, simply click on the radio button for Common Services, select the service desired from the pull down menu, and click on the "Update" button at the bottom of the screen.

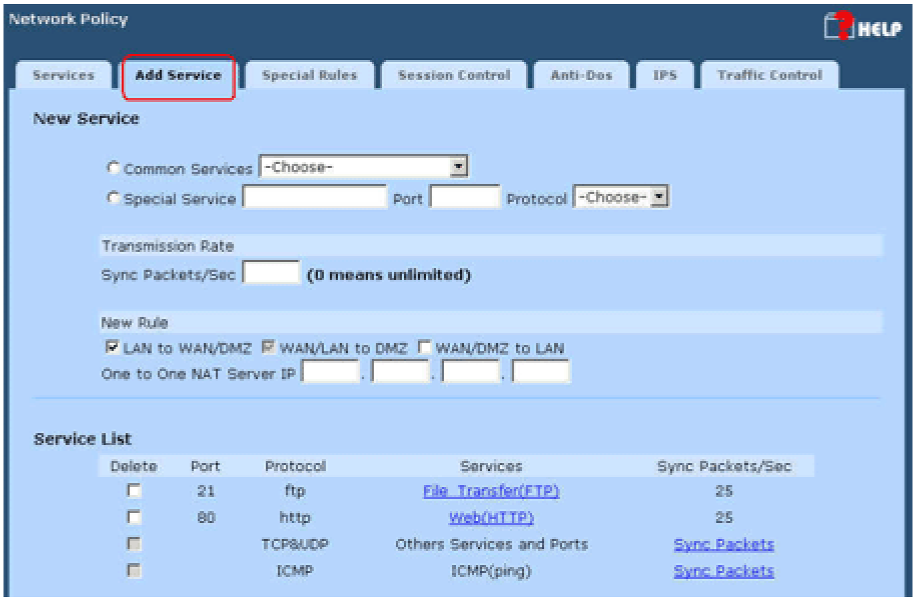
In the event that the service you wish to add is unlisted, you can add the service manually clicking on the Special Service radio button, filling in some name, the port, and the protocol that the service will use. **The name may not have any spaces or dashes**. It might take some investigation to find the correct settings to enable a custom service.

You might notice that the "Transmission Rate" and the "New Rule" fields are filled in with some default values as you select what service or what protocol to use. The "Transmission Rate" field allows you to control possible attacks over a given service by limiting the number of new connections per second. If the value set for "Sync Packets/Sec" is exceeded, then those connections above the threshold will be dropped and logged, under the "Log" menu button. The "New Rule" options allow you to configure the service being added for the directions of traffic you want enabled for the new service.

After adding a new service, it will be added to the list below, for further modification. To modify an existing service, click on the underlined name in this list, and it will bring up a window for changing the port, protocol, and the "Sync Packets/Sec," the number of new connections before the Firewall VPN begins dropping packets for that service. To delete a service from the Firewall VPN database, click on the delete checkbox next to the desired service and click "Update" at the bottom of the screen.

Example: Let's open MSN Messenger ports for file transfer. Per the product documentation you have to open as many TCP ports between 6891 and 6900.

Click in "Special Service", type the a name for it like MSN_Messenger, choose the "Protocol" to TCP, then type the port range separating the lower and the higher ports using a colon, like → 6891:6900. Hit Update and you will see the new service in the "Service List".



New Service

○ Common Services -Choose-
○ Special Service ______ Port ______ Protocol -Choose-

Transmission Rate

Sync Packets/Sec ______ (0 means unlimited)

New Rule

☑ LAN to WAN/DMZ ☑ WAN/LAN to DMZ □ WAN/DMZ to LAN

One to One NAT Server IP ____ . ____ . ____ . ____

Service List

Delete	Port	Protocol	Services	Sync Packets/Sec
□	21	ftp	File Transfer(FTP)	25
□	80	http	Web(HTTP)	25
□		TCP&UDP	Others Services and Ports	Sync Packets
□		ICMP	ICMP(ping)	Sync Packets

Figure 7.9
Network Policy, Add Service tab

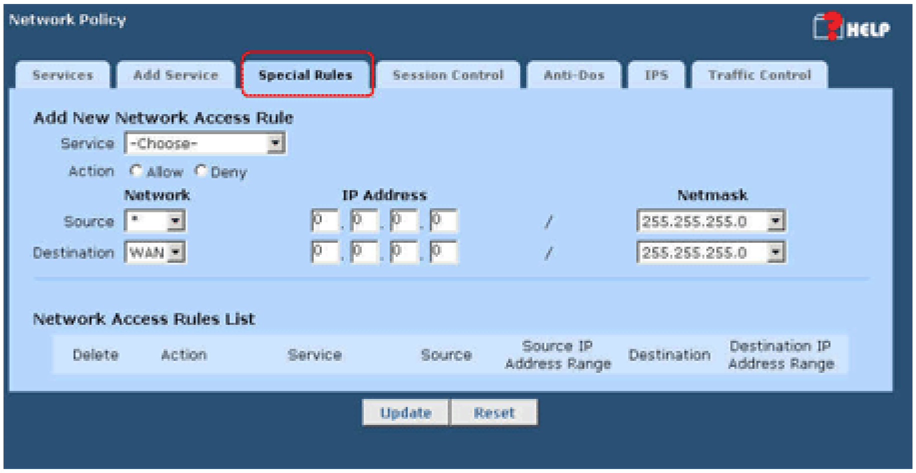
Special Rules

This tab allows the administrator to allow or deny a service from a user or group of users. This page is closely linked with the first "Services" tab. This can be exemplified by enabling some of the traffic flows for "Other Services and Ports" on the "Services" tab, then clicking back to the "Special Rules" tab to view the changes.

To enable a service for a single user or group of users and deny the service to all other users, go back to the "Services" tab, and disable all directions of traffic for the service in question. Then return to the "Special Rules" tab, select the service from the pull down menu, select the "Allow" radio button, and then configure the direction of the traffic. To do the last step requires knowledge from which part of your network you will be attempting to access the service and to which part of the network the service is being served, whether it is the LAN, DMZ, WAN. The character '*', is a wildcard character meaning all networks. Additionally you must know the IP addresses of both the source networks for which you would like to have this service available too and the destination networks from which you expect will be serving this service.

To disable a service for a single user or group of users, and allow the service for all other users, make sure that the service has been enabled on the "Services" tab, and then return to the "Special Rules" tab. Again, select the service from the pull down menu, select the "Deny" radio button, and then configure the direction of the traffic.

To remove any such special rules for a service, simply click on the checkbox next to the specific rule you want to remove and click “Update” at the bottom of the screen.



Network Policy

Add New Network Access Rule

Service: -Choose-

Action: ○ Allow ○ Deny

	Network	IP Address		Netmask
Source	*	0 . 0 . 0 . 0	/	255.255.255.0
Destination	WAN	0 . 0 . 0 . 0	/	255.255.255.0

Network Access Rules List

Delete	Action	Service	Source	Source IP Address Range	Destination	Destination IP Address Range

Figure 7.10
Network Policy, Special Rules

Session Control

This tab allows you to control how the Firewall VPN handles sessions. More specifically, how long the Firewall VPN will wait for each part of a session’s lifespan before closing the connection. For your reference, a simplified diagram of the TCP/IP handshake is provided (Figure 7.12).

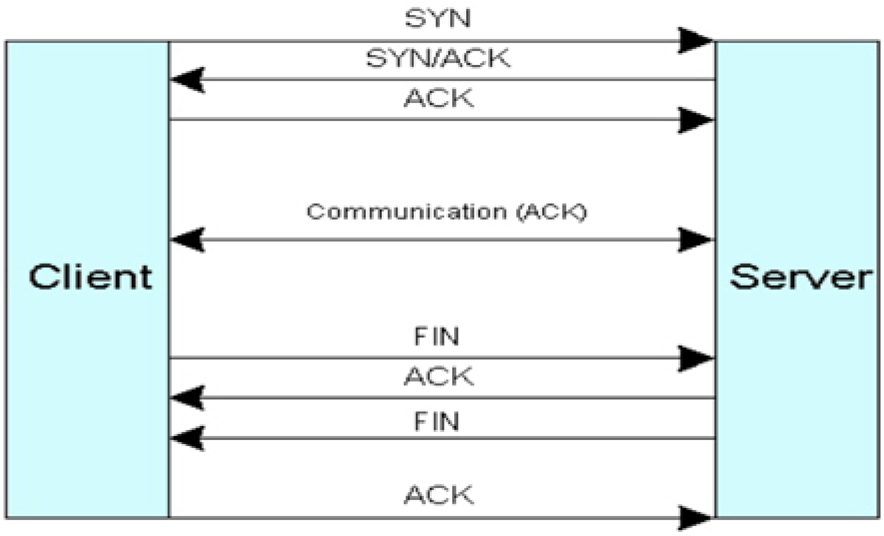


Figure 7.11
TCP/IP handshake diagram

- **TCP SYN-SENT**
  The time you put into this field will be the length of time the Firewall VPN will wait for a

matching SYN-RECV from the remote server before dropping the connection.

- **TCP SYN-RECV**
  This happens when a server in your network transmits a TCP SYN-RECV, Firewall VPN will wait the length time entered here for a TCP ACK, or acknowledgement from the remote client.

- **TCP ESTABLISHED**
  This is the data transfer phase of an establish TCP connection, the firewall will maintain an idle session for only as long as the time entered here.

- **TCP FIN-WAIT**
  The Firewall VPN will wait the time entered for a FIN ACK, or a connection termination acknowledgement from a remote server.

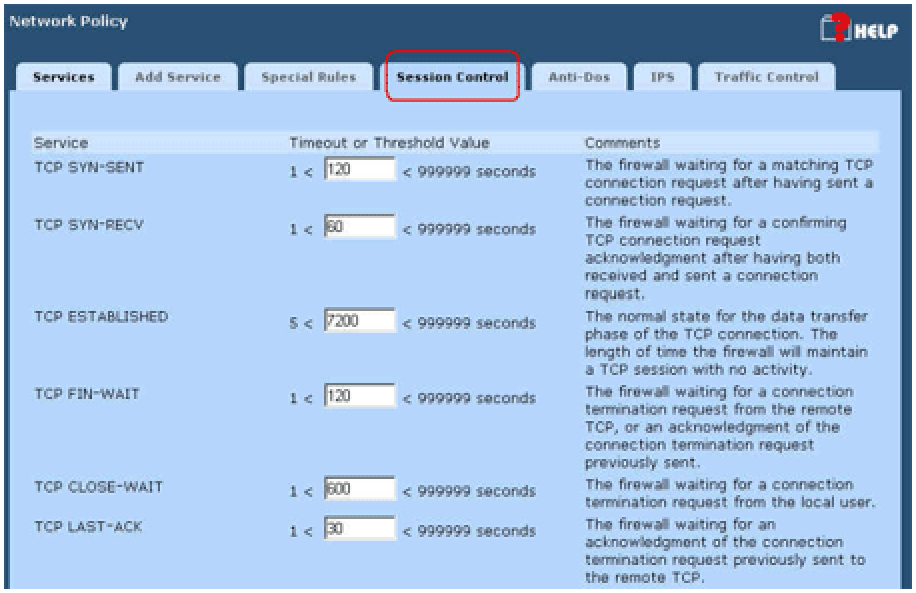
- **TCP CLOSE-WAIT**
  The Firewall VPN will wait the time entered to successfully send a TCP LAST-ACK, or connection termination request to a remote client.

- **TCP LAST-ACK**
  The Firewall VPN will wait the time entered to receive a TCP ACK, or a connection termination acknowledgement, from a remote client.

- **TCP TIME-WAIT**
  The Firewall VPN will wait the time entered to receive a TCP LAST-ACK, or a final connection termination acknowledgement, from a remote server.

- **TCP CLOSED**
  The Firewall VPN will wait the time entered to maintain the TCP connection in closed state.

- **UDP session idle timeout**
  The length of time the firewall will maintain a UDP session with no activity.

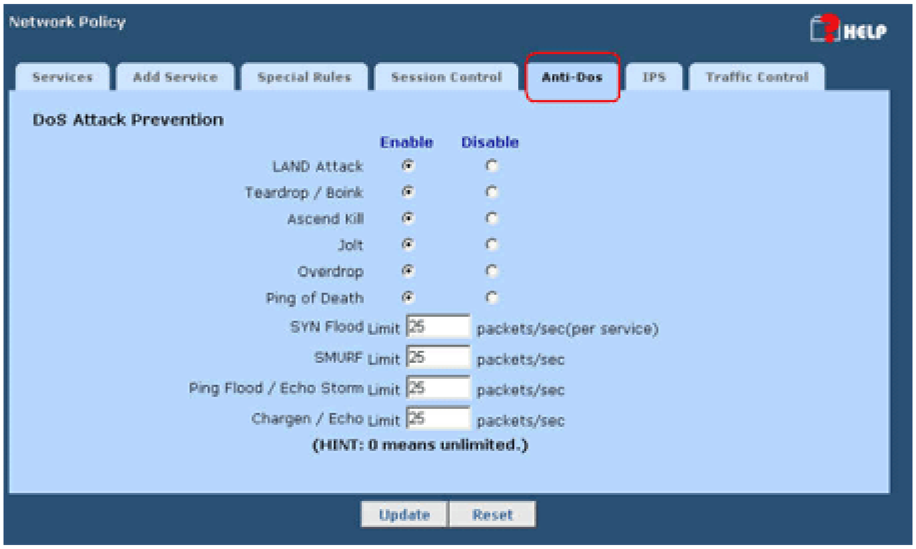


Service	Timeout or Threshold Value	Comments
TCP SYN-SENT	1 < 120 < 999999 seconds	The firewall waiting for a matching TCP connection request after having sent a connection request.
TCP SYN-RECV	1 < 60 < 999999 seconds	The firewall waiting for a confirming TCP connection request acknowledgment after having both received and sent a connection request.
TCP ESTABLISHED	5 < 7200 < 999999 seconds	The normal state for the data transfer phase of the TCP connection. The length of time the firewall will maintain a TCP session with no activity.
TCP FIN-WAIT	1 < 120 < 999999 seconds	The firewall waiting for a connection termination request from the remote TCP, or an acknowledgment of the connection termination request previously sent.
TCP CLOSE-WAIT	1 < 600 < 999999 seconds	The firewall waiting for a connection termination request from the local user.
TCP LAST-ACK	1 < 30 < 999999 seconds	The firewall waiting for an acknowledgment of the connection termination request previously sent to the remote TCP.

Figure 7.12
Network Policy, Session Control

Anti-DoS

This tab allows you to enable the Firewall VPN built-in defenses to common DoS attacks. Disabling is as easy as clicking disable and then Update. You can disable and enable multiple attacks at once. Since the last four attacks are not attacks based on flawed TCP/IP stacks, they are regulated instead by rate limiters. To disable these, set the limit to zero.



DoS Attack Prevention

	Enable	Disable
LAND Attack	●	○
Teardrop / Boink	●	○
Ascend Kill	●	○
Jolt	●	○
Overdrop	●	○
Ping of Death	●	○

SYN Flood Limit 25 packets/sec(per service)

SMURF Limit 25 packets/sec

Ping Flood / Echo Storm Limit 25 packets/sec

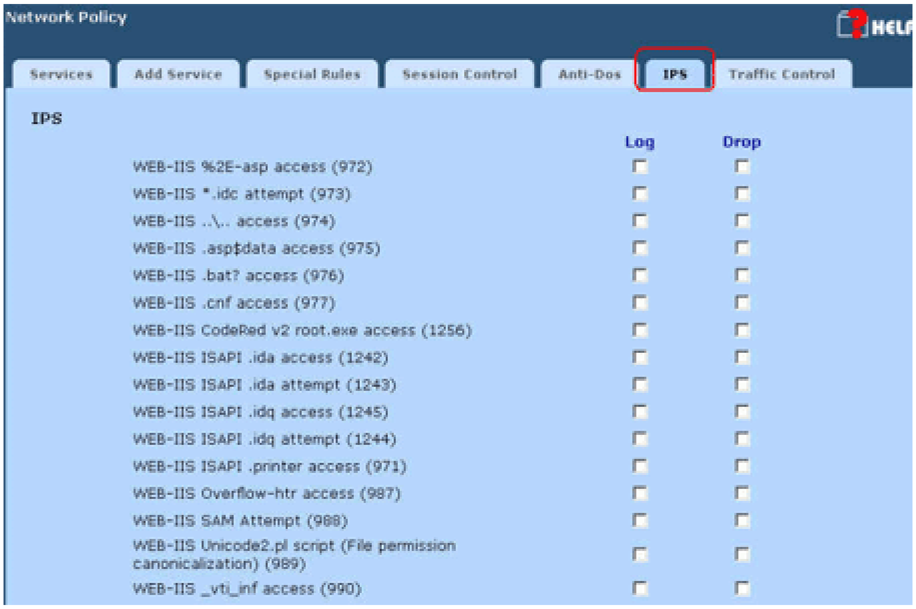
Chargen / Echo Limit 25 packets/sec

(HINT: 0 means unlimited.)

Figure 7.13
Network Policy, Anti-DoS

IPS

This tab allows you to enable the Firewall VPN built-in defenses to common IPS (Intrusion Prevention Systems) attacks. Disabling is as easy as clicking disable and then Update. You can disable and enable multiple attacks at once. Also can select both Log and Drop or one.



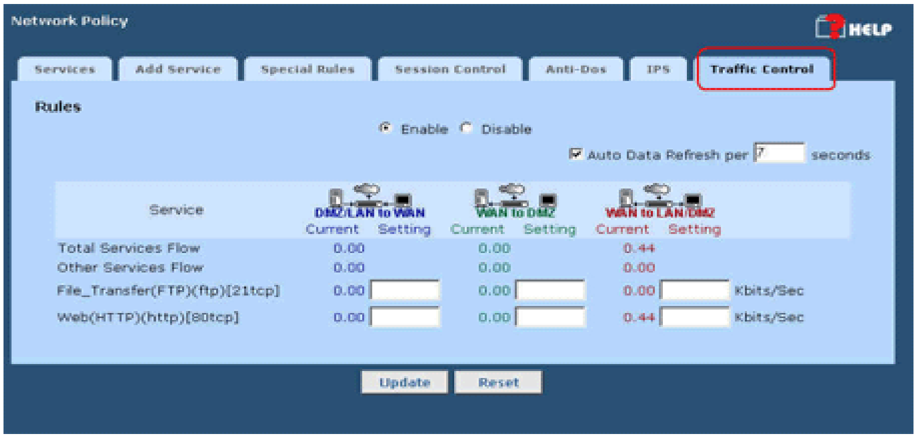
IPS

	Log	Drop
WEB-IIS %2E-asp access (972)	□	□
WEB-IIS *.idc attempt (973)	□	□
WEB-IIS ..\.. access (974)	□	□
WEB-IIS .asp$data access (975)	□	□
WEB-IIS .bat? access (976)	□	□
WEB-IIS .cnf access (977)	□	□
WEB-IIS CodeRed v2 root.exe access (1256)	□	□
WEB-IIS ISAPI .ida access (1242)	□	□
WEB-IIS ISAPI .ida attempt (1243)	□	□
WEB-IIS ISAPI .idq access (1245)	□	□
WEB-IIS ISAPI .idq attempt (1244)	□	□
WEB-IIS ISAPI .printer access (971)	□	□
WEB-IIS Overflow-htr access (987)	□	□
WEB-IIS SAM Attempt (988)	□	□
WEB-IIS Unicode2.pl script (File permission canonicalization) (989)	□	□
WEB-IIS _vti_inf access (990)	□	□

Figure 7.14
Network Policy, IPS

Traffic Control

This tab shows current bandwidth usage for the three directions of traffic flow through the Firewall VPN. It also allows the administrator to set traffic limiters for each individual service, to ensure quality of service. Refer to the section above if you are still unclear about the directions of traffic.



Rules

● Enable ○ Disable

☑ Auto Data Refresh per 7 seconds

Service	DMZ/LAN to WAN Current	DMZ/LAN to WAN Setting	WAN to DMZ Current	WAN to DMZ Setting	WAN to LAN/DMZ Current	WAN to LAN/DMZ Setting	
Total Services Flow	0.00		0.00		0.44		
Other Services Flow	0.00		0.00		0.00		
File_Transfer(FTP)(ftp)[21tcp]	0.00		0.00		0.00		Kbits/Sec
Web(HTTP)(http)[80tcp]	0.00		0.00		0.44		Kbits/Sec

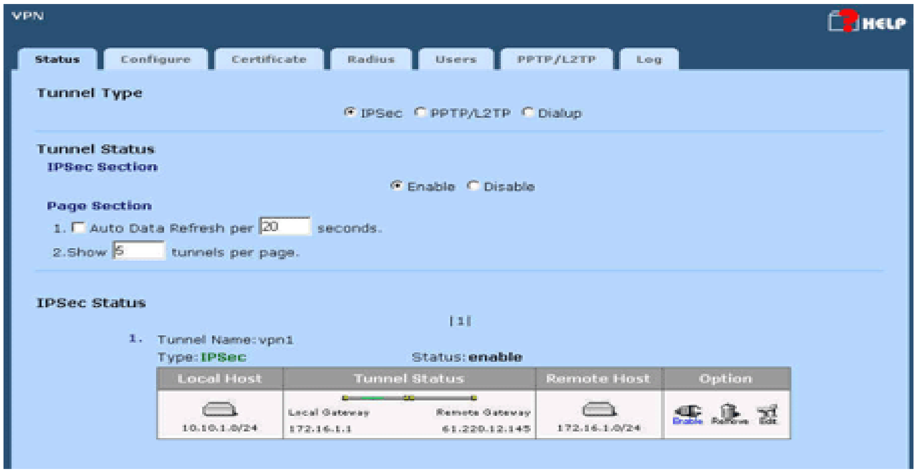
Figure 7.15
Network Policy, Traffic Control

VPN

This menu allows the administrator to manage, add, and delete VPN tunnels that are routed through the Firewall VPN.

Status

This tab allows for quick management of existing VPN tunnels. Selecting the tunnel type will show tunnels corresponding to that type. If you disable the tunnel status, no VPN tunnel can be established with your Firewall VPN and existing tunnels will be shutdown. This is a quick way to shutdown all tunnels.



Tunnel Type

● IPSec ○ PPTP/L2TP ○ Dialup

Tunnel Status

IPSec Section

● Enable ○ Disable

Page Section

1. □ Auto Data Refresh per 20 seconds.

2. Show 5 tunnels per page.

IPSec Status

[1]

1. Tunnel Name: vpn1

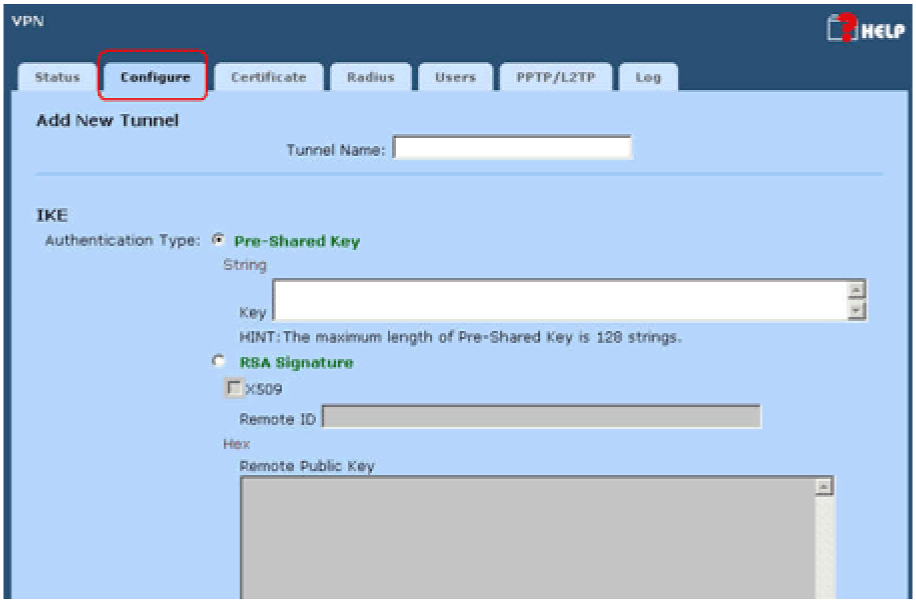
Type: IPSec Status: enable

Local Host	Tunnel Status	Remote Host	Option
10.10.1.0/24	Local Gateway 172.16.1.1 Remote Gateway 61.220.12.145	172.16.1.0/24	Enable Remove Edit

Figure 7.16
VPN, Status tab, two disabled VPN showing, and no refresh

Configure

This tab is for adding new L2TP/IPSec VPN tunnels.



Add New Tunnel

Tunnel Name:

IKE

Authentication Type: ● Pre-Shared Key

String

Key

HINT: The maximum length of Pre-Shared Key is 128 strings.

○ RSA Signature

□ X509

Remote ID

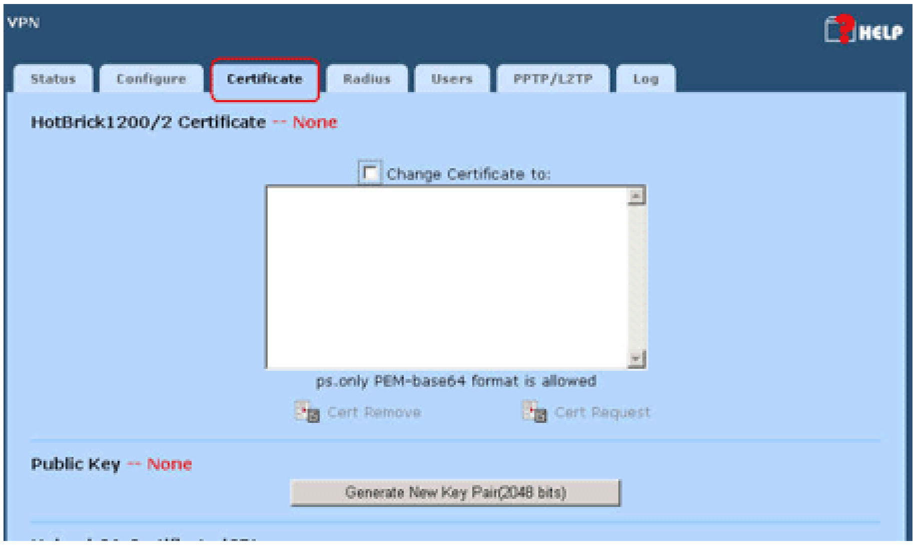
Hex

Remote Public Key

Figure 7.17
VPN, Configure tab

Certificate

This tab is for managing, adding, and deleting certificates from third party certificate authorities.



HotBrick1200/2 Certificate -- None

□ Change Certificate to:

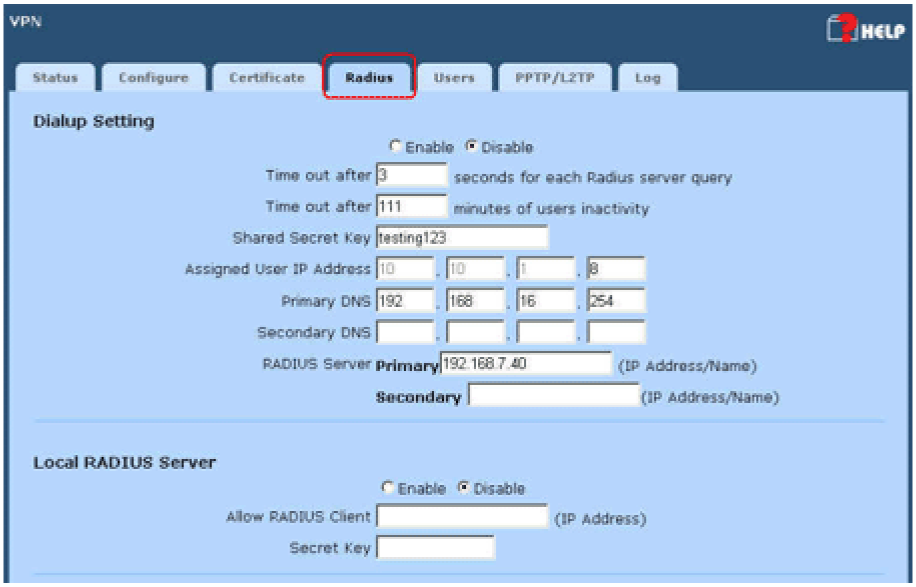
ps.only PEM-base64 format is allowed

Public Key -- None

Figure 7.18
VPN, Certificate tab, sample RSA public key

RADIUS

This tab is for configuring the Firewall VPN to dial into a RADIUS server, to configure the Firewall VPN to be a RADIUS server itself, as well as management of any clients that will use the Firewall VPN as a RADIUS server.



Dialup Setting

○ Enable ● Disable

Time out after 3 seconds for each Radius server query

Time out after 111 minutes of users inactivity

Shared Secret Key testing123

Assigned User IP Address 10 . 10 . 1 . 8

Primary DNS 192 . 168 . 16 . 254

Secondary DNS . . .

RADIUS Server **Primary** 192.168.7.40 (IP Address/Name)

Secondary (IP Address/Name)

Local RADIUS Server

○ Enable ● Disable

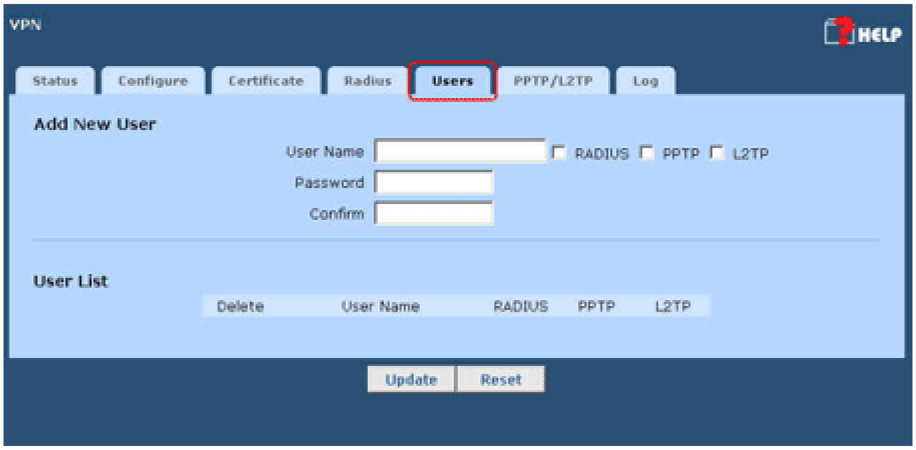
Allow RADIUS Client (IP Address)

Secret Key

Figure 7.19
VPN, RADIUS tab, sample dial-up information for the Firewall VPN to dial another RADIUS server for remote authentication.

Users

This tab is for managing, adding, and deleting of users for all VPN tunnels. You must tell what kind of tunnels your users can access and their password. After you're done creating them, go to the "PPTP/L2TP" tab to configure the tunnel you wish to use if creating a tunnel of that kind.



Add New User

User Name [ ] □ RADIUS □ PPTP □ L2TP
Password [ ]
Confirm [ ]

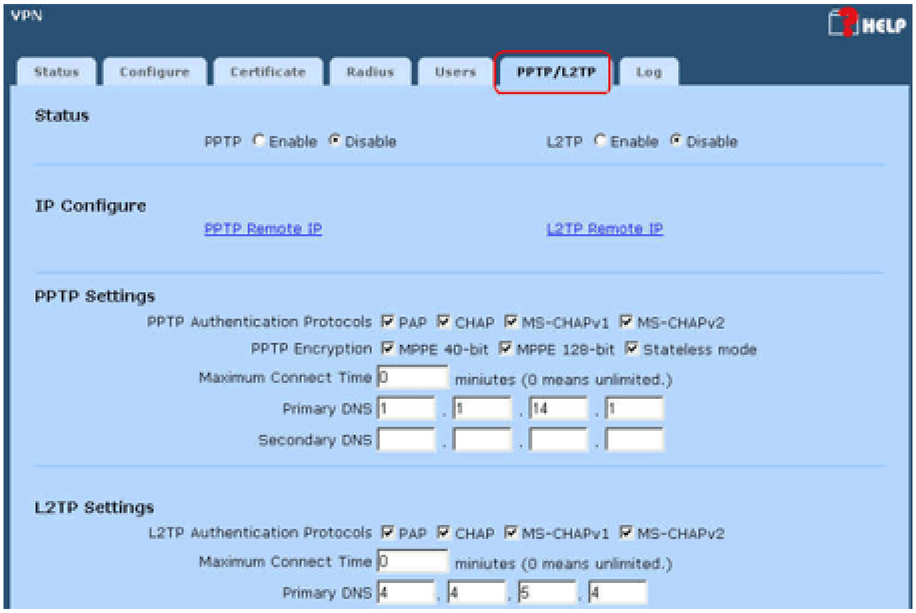
User List

Delete	User Name	RADIUS	PPTP	L2TP

Figure 7.20
VPN, Users tab

PPTP/L2TP

This tab is for management of the PPTP and L2TP settings. To create a PPTP or L2TP tunnel for your remote users, click either in "PPTP Remote IP" or "L2TP Remote IP" and define the ranges that you want to give your remote users when they gain access to your corporate network. Do not forget to change the tunnel status to "Enable" when configuring your PPTP or L2TP tunnel.



Status

PPTP ○ Enable ● Disable   L2TP ○ Enable ● Disable

IP Configure

PPTP Remote IP   L2TP Remote IP

PPTP Settings

PPTP Authentication Protocols ☑ PAP ☑ CHAP ☑ MS-CHAPv1 ☑ MS-CHAPv2
PPTP Encryption ☑ MPPE 40-bit ☑ MPPE 128-bit ☑ Stateless mode
Maximum Connect Time [0] miniutes (0 means unlimited.)
Primary DNS [1] . [1] . [14] . [1]
Secondary DNS [ ] . [ ] . [ ] . [ ]

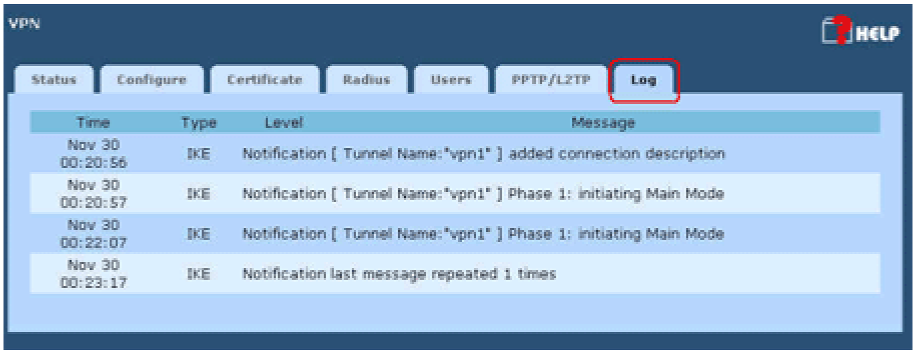
L2TP Settings

L2TP Authentication Protocols ☑ PAP ☑ CHAP ☑ MS-CHAPv1 ☑ MS-CHAPv2
Maximum Connect Time [0] miniutes (0 means unlimited.)
Primary DNS [4] . [4] . [5] . [4]

Figure 7.21
VPN, PPTP/L2TP tab

View Log

This tab is for viewing all logs related to the VPN.



Time	Type	Level	Message
Nov 30 00:20:56	IKE	Notification	[Tunnel Name:"vpn1"] added connection description
Nov 30 00:20:57	IKE	Notification	[Tunnel Name:"vpn1"] Phase 1: initiating Main Mode
Nov 30 00:22:07	IKE	Notification	[Tunnel Name:"vpn1"] Phase 1: initiating Main Mode
Nov 30 00:23:17	IKE	Notification	last message repeated 1 times

Figure 7.22
VPN, View Log tab

How to Configure the HotBrick Firewall VPN Server for Remote User access

The first thing you have to do is decide which kind of encryption you're going to use in the VPN connection you're about to create. You have the option to use either PPTP or L2TP.

After you decide what kind of tunnel will be used, we need to create its users. Let's create PPTP tunnels for this example, but if you plan to use L2TP the steps are the same, just make sure to apply the patches explained at the end of this section about your Windows clients' connections.

1. Click in **Advanced Setup**
2. On the top menu choose **VPN**
3. In VPN, choose the tab **Users**.
4. In this tab you will give them a username, then click in the checkbox VPN, then create and confirm the password. When you're done hit **Update**.

Now let's configure the tunnel:

1. On the top menu choose **VPN**
2. Click in the tab **PPTP/L2TP**.
3. In this tab go to the section **IP Configure**, click in the link **PPTP Remote IP**.
4. In the section **Add PPTP/L2TP IP Range**, choose the radio button **PPTP** and let's use a range of 10 IPs for this example, so let's type 230 to 239 (assuming that the IP schema you have in your network is 192.168.1.X), when you're done hit **Update**.
5. On the top menu choose **VPN**
6. Click in the tab **PPTP/L2TP**.
7. Under the section **Status**, choose the option **Enable** under **PPTP**
8. In the section PPTP Settings, keep all the authentications protocols and PPP encryptions checked. In the Maximum Connect Time leave the as 0, and in the **Primary DNS** and **Secondary DNS** use the information provided by your ISP.
9. Hit **Update**

You're done configuring the HotBrick. Now it's time to configure the client side, just follow the steps for your windows client computer.

Configure a VPN Connection to Your Corporate Network in Windows 2000

To create a VPN connection under Windows 2000, you should:

1. Go to the **Control Panel** and then **Network and Dial-up Connections**
2. Select **Make New Connection**. This will open the **Network Connection Wizard***.*
3. Select the option **Connect to a private network through the Internet** and click **Next**.
4. Because you are already connected to the Internet, click **Do not dial the initial connection**. Click **Next**.
5. In the **Host name** field, enter the IP address for the HotBrick to which you are connecting
6. Select whether you want the connection to be available for all users/accounts on your machine, or just for yourself. Click **Next**.
7. Finally choose a name for the connection and click **Finish**. You can specify for a shortcut to be added to your desktop if required.

Configure a VPN Connection to Your Corporate Network in Windows XP

How to Create a New VPN Connection

1. To open the Network Connections folder, click **Start**, click **Control Panel**, click **Network and Internet Connections**, and then double-click **Network Connections**.
2. Click **Create a new connection**, and then click **Next**. Click **Connect to the network at my workplace**, and then click **Next**.

3. Click **Virtual Private Network connection**, click **Next**. Type a descriptive name for your company, and click **Next**.
4. Because you are already connected to the Internet, click **Do not dial the initial connection**.
5. Type the host IP address for the HotBrick to which you are connecting, and then click **Next**.
6. Choose whether you want this connection to be shared by all users (**Anyone's use**) of this computer, or only for yourself (**My use only**).
7. Click **Next**, and then click **Finish** to end the Setup process.

How to Modify the VPN Connection to use L2TP

1. To open an existing connection, click Start, click Control Panel, click Network and Internet Connections, and then double-click Network Connections.
2. Click the connection, and then click Change settings of this connection.
3. On the **General** tab, you can change the IP address for the HotBrick to which you are connecting if you want or need to.
4. On the **Networking** tab, you can change the type of secure protocol to L2TP IPSec VPN.
5. On the **Security** tab, click in the **Advanced** option, and click in the Settings button.
6. On the drop down menu choose, Requires Encryption (disconnect if the server declines).
7. In **Logon Security**, click in Allow These protocols:
    a. Unencrypted Password (PAP)
    b. Challenge Handshake Authentication Protocol (CHAP)
    c. Microsoft CHAP
    d. Microsoft CHAP Version 2

e. Click OK, and OK again.

Note: If you are creating a L2TP tunnel to your remote office from your client computer, Microsoft has released an update package to enhance the current functionality of the Layer Two Tunneling Protocol (L2TP) and Internet Protocol security (IPSec) on computers that are running Windows XP or Windows 2000. **We strongly recommend that you apply these patches.**

Please review the article number 818043: L2TP/IPSec NAT-T Update for Windows XP and Windows 2000:

http://support.microsoft.com/default.aspx?scid=kb;%5bLN%5d;818043

Also it will be necessary to disable IPSec policy in order for the L2TP tunnel to work, go to the article 258261: Disabling IPSEC Policy Used with L2TP for the step-by-step on how to perform this procedure.

http://support.microsoft.com/default.aspx?scid=kb;en-us;258261

Web Filter

This menu is for filtering web content to conform to your organization's policies. The rules for this can be quite complex but are based on the regular expression engine used on *NIX systems. Additionally, the web filter can support multi byte characters.

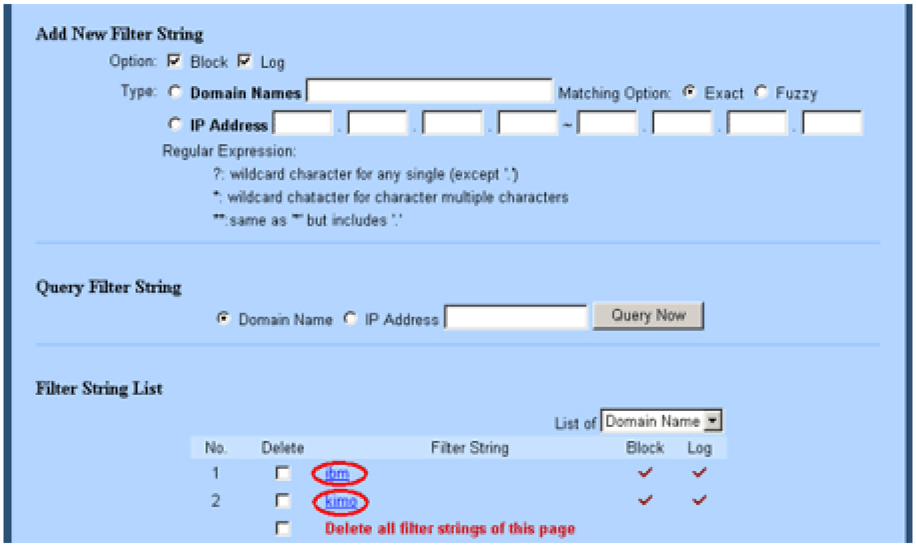
Character	Matches	Examples
\	Quote the next character	\. => .
.	any single character	l.ve => love, live, l-ve, …
?	0 or 1 matches to the preceding character	se?x => sex, sx nc?tu => ntu, nctu
*	0 or more matches to the preceding character. (repeating characters)	ab*c => ac, abc, abbc, abbbc, … zyx* => zy, zyx, zyxx, zyxxx, …

		*rst => st, rst, rrst, rrrst, …
+	1 or more matches to the preceding character. (repeating characters)	W+ => w, ww, www, … h+ => h, hh, hhh, … y+ => y, yy, yyy, …

These regular expressions can be combined for maximum effect to block a range of possible URL and content string matches. For example, foreignaffairs?\.c. can block: foreignaffair.com, foreignaffairs.com, foreignaffairs.cc, foreignaffair.cx, foreignaffair.cc and so on…

URL

This tab is for filtering web content based on its URL, or universal resource locator. You can block a specific domain or use fuzzy logic to block domains with similar names.



Add New Filter String

Option: ☑ Block ☑ Log

Type: ○ **Domain Names** Matching Option: ● Exact ○ Fuzzy

○ **IP Address**

Regular Expression:

?: wildcard character for any single (except '.')

*: wildcard chatacter for character multiple characters

**:same as '*' but includes '.'

Query Filter String

● Domain Name ○ IP Address

Filter String List

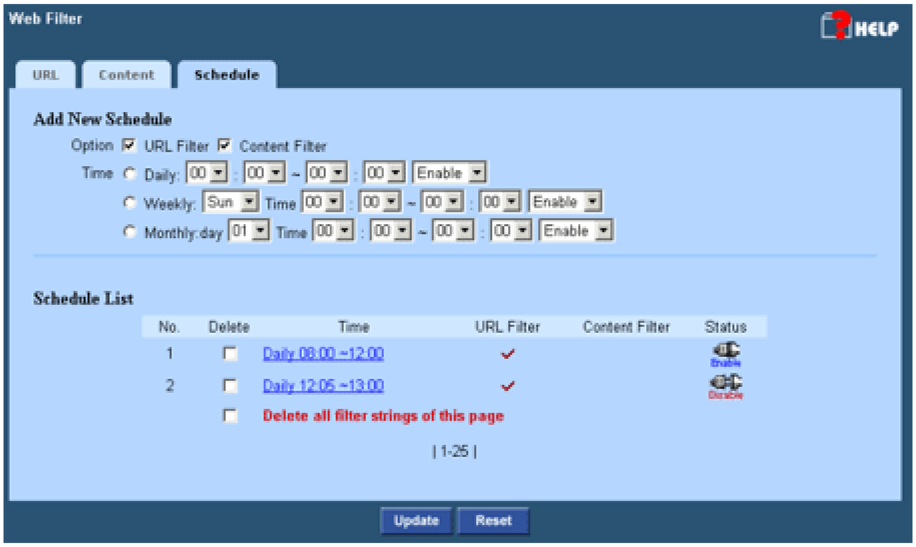
List of Domain Name

No.	Delete	Filter String	Block	Log
1	□	ibm	✓	✓
2	□	kimo	✓	✓
	□	Delete all filter strings of this page		

Figure 7.23
Web Filter, URL Filter tab, sample filters in place

Schedule

This tab is for setting up a schedule to filter content.



Add New Schedule

Option ☑ URL Filter ☑ Content Filter

Time ○ Daily: 00 : 00 ~ 00 : 00 Enable

○ Weekly: Sun Time 00 : 00 ~ 00 : 00 Enable

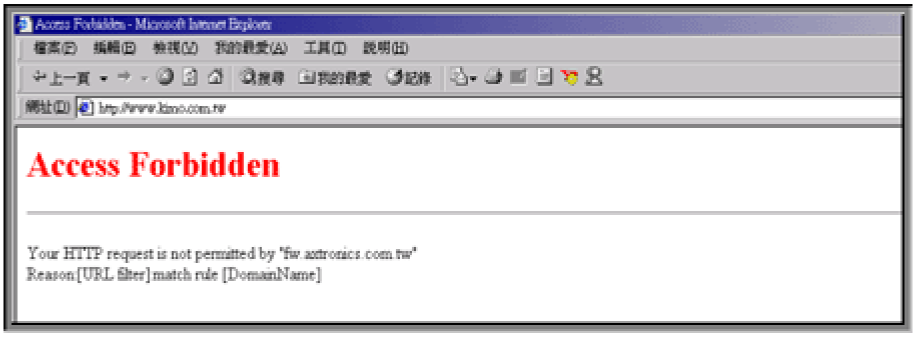
○ Monthly:day 01 Time 00 : 00 ~ 00 : 00 Enable

Schedule List

No.	Delete	Time	URL Filter	Content Filter	Status
1	□	Daily 08:00 ~12:00	✓		Enable
2	□	Daily 12:05 ~13:00	✓		Disable
	□	Delete all filter strings of this page			

| 1-25 |

Figure 7.24
Web Filter, Schedule tab, sample schedules in place


Access Forbidden - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
記錄
網址(D)
http://www.kimo.com.tw

Access Forbidden

Your HTTP request is not permitted by "fw.axtronics.com.tw"
Reason:[URL filter] match rule [DomainName]

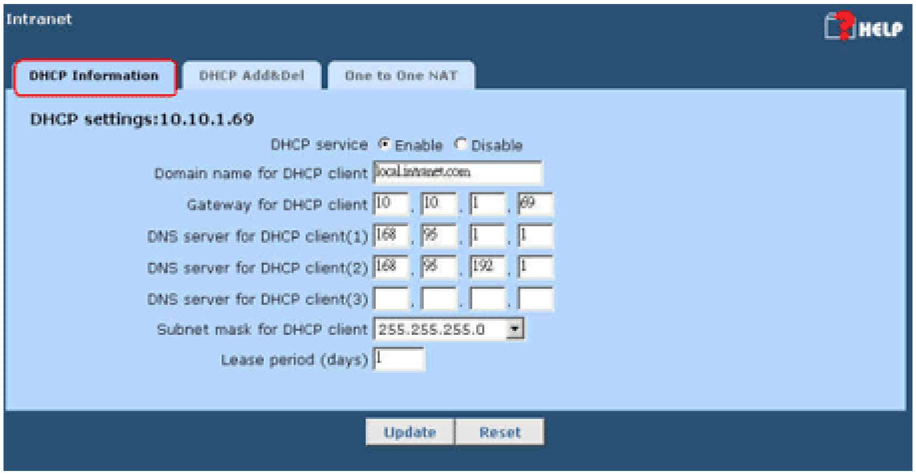
Figure 7.25
Access Forbidden when attempting to access a page that is screened out by the content filter.

Intranet

This menu is for configuring your Intranet, referred to earlier as the LAN, or local area network.

DHCP Information

This tab is for a quick overview and basic configuration of the Firewall VPN's built-in DHCP server.



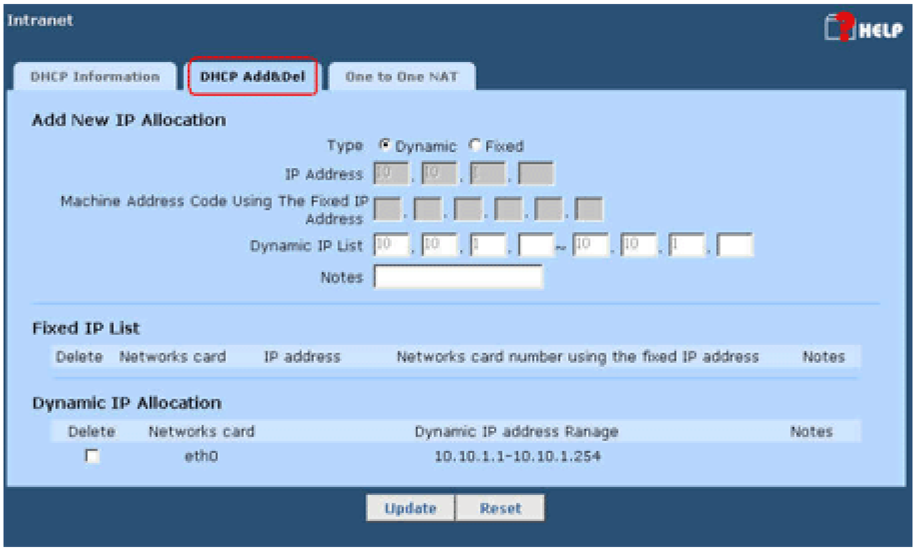
DHCP settings:10.10.1.69

DHCP service	● Enable ○ Disable
Domain name for DHCP client	local.intranet.com
Gateway for DHCP client	10 . 10 . 1 . 69
DNS server for DHCP client(1)	168 . 95 . 1 . 1
DNS server for DHCP client(2)	168 . 95 . 192 . 1
DNS server for DHCP client(3)	. . .
Subnet mask for DHCP client	255.255.255.0
Lease period (days)	1

Figure 7.26
Intranet, DHCP Information tab, sample settings in place.

DHCP Add & Del

This tab is for configuring the Firewall VPN's built-in DHCP server. More specifically, this page allows the administrator to add new ranges to the dynamic IP allocation, or add fixed IP allocations for specific machines.



Add New IP Allocation

Type	● Dynamic ○ Fixed
IP Address	10 . 10 . 1 .
Machine Address Code Using The Fixed IP Address	. . . . .
Dynamic IP List	10 . 10 . 1 . ~ 10 . 10 . 1 .
Notes	

Fixed IP List

Delete	Networks card	IP address	Networks card number using the fixed IP address	Notes

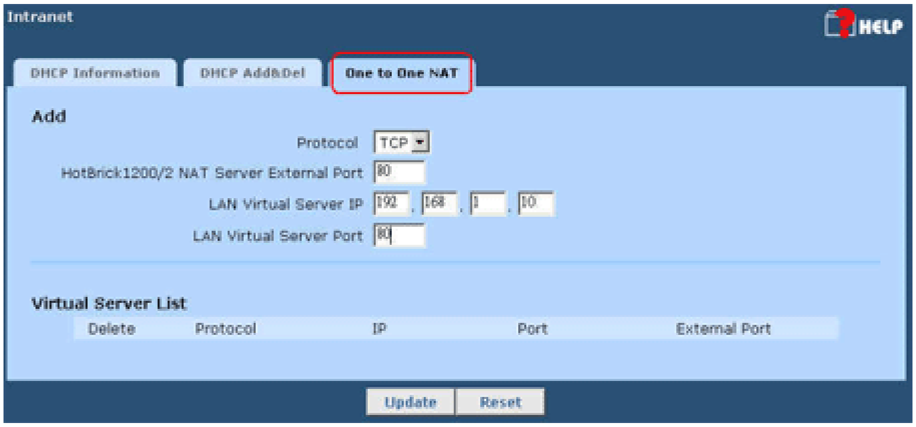
Dynamic IP Allocation

Delete	Networks card	Dynamic IP address Ranage	Notes
□	eth0	10.10.1.1-10.10.1.254	

Figure 7.27
Intranet, DHCP Add&Del tab

One to One NAT

This tab is for configuring the Firewall VPN to allow users from the DMZ or Internet (WAN), to access servers in the Intranet (LAN).



Add

Protocol: TCP
HotBrick1200/2 NAT Server External Port: 80
LAN Virtual Server IP: 192 . 168 . 1 . 10
LAN Virtual Server Port: 80

Virtual Server List

Delete	Protocol	IP	Port	External Port

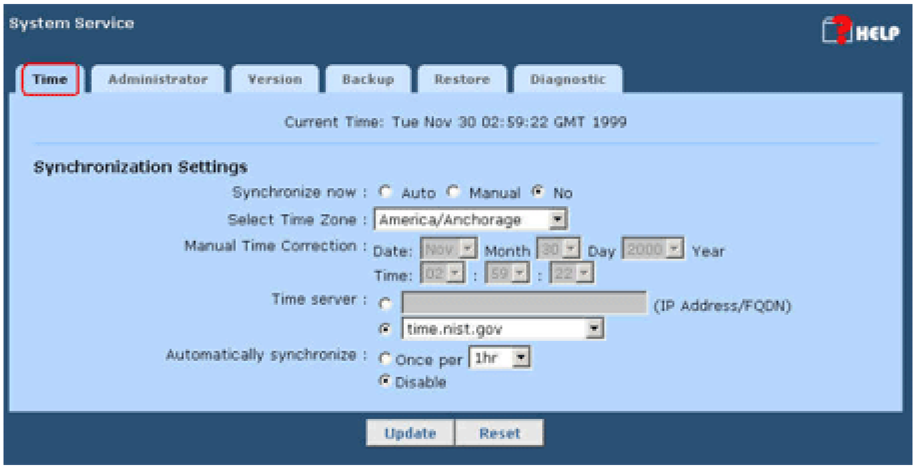
Figure 7.28
Intranet, One to One NAT tab

System Service

This menu is to configure the Firewall VPN’s system. Items such as system time, backup, and version are included in this.

Time

This tab shows the current system time, and allows the administrator to synchronize the time or schedule when they would like synchronization with a network timeserver to take place.



Current Time: Tue Nov 30 02:59:22 GMT 1999

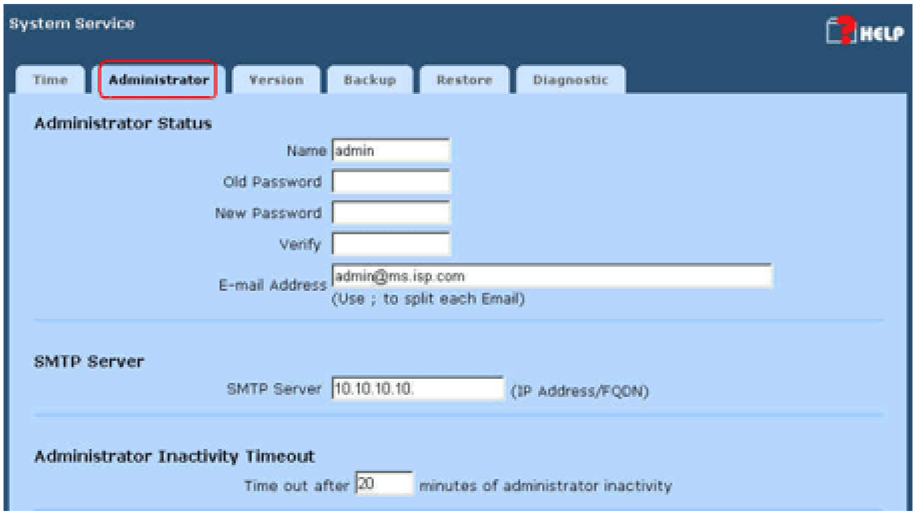
Synchronization Settings

Synchronize now : ○ Auto ○ Manual ● No
Select Time Zone : America/Anchorage
Manual Time Correction : Date: Nov Month 30 Day 2000 Year
Time: 02 : 59 : 22
Time server : ○ (IP Address/FQDN)
● time.nist.gov
Automatically synchronize : ○ Once per 1hr
● Disable

Figure 7.29
System Service, Time tab

Administrator

This tab allows the administrator to change information pertaining to the “Administrator” account. In addition it allows for configuration of remote (Internet) administration of the Firewall VPN.



Administrator Status

Name: admin

Old Password:

New Password:

Verify:

E-mail Address: admin@ms.isp.com
(Use ; to split each Email)

SMTP Server

SMTP Server: 10.10.10.10 (IP Address/FQDN)

Administrator Inactivity Timeout

Time out after 20 minutes of administrator inactivity

Figure 7.30
System Service, Administrator tab

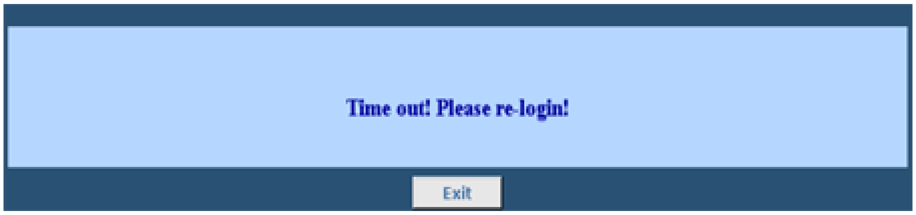
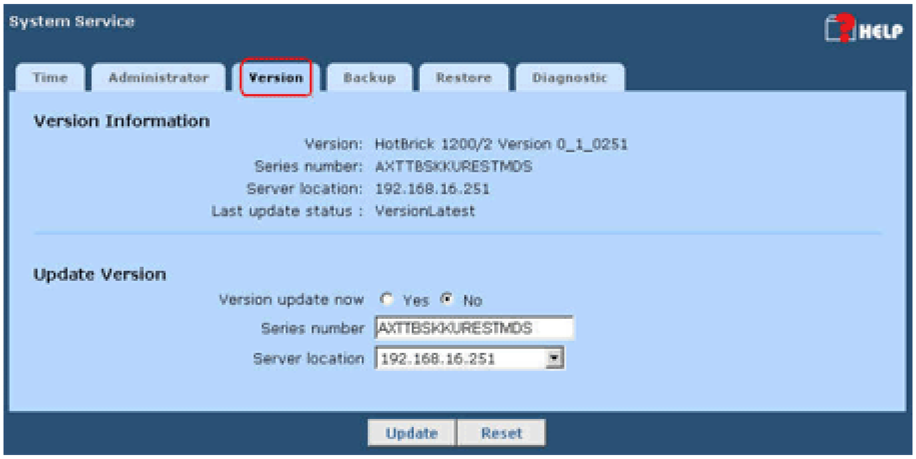

Time out! Please re-login!

Figure 7.31
Time out screen

Version

This tab shows the current version of the Firewall VPN, and allows the administrator to update the Firewall VPN immediately.



Version Information

Version: HotBrick 1200/2 Version 0_1_0251
Series number: AXTTBSKKURESTMDS
Server location: 192.168.16.251
Last update status : VersionLatest

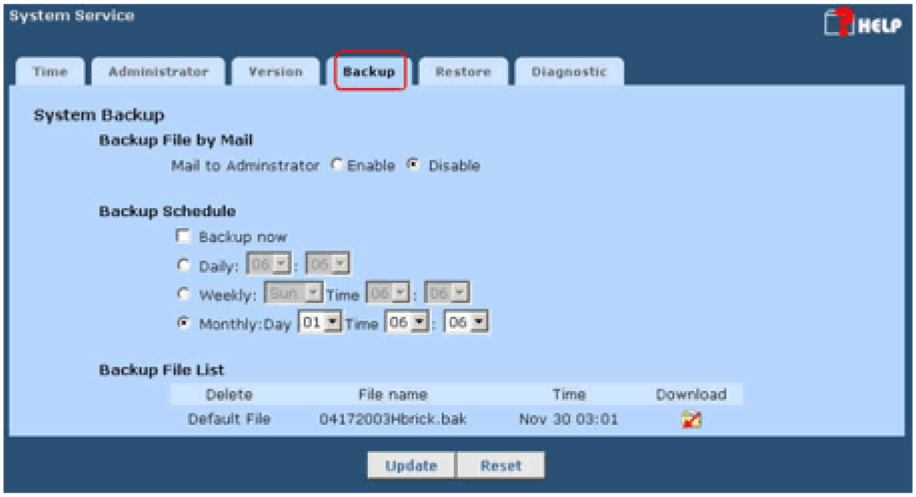
Update Version

Version update now ○ Yes ● No
Series number: AXTTBSKKURESTMDS
Server location: 192.168.16.251

Figure 7.32
System service, Version tab

Backup

This tab allows the administrator to backup critical system configuration files, and then restore the Firewall VPN from a backup.



System Backup

Backup File by Mail

Mail to Adminstrator ○ Enable ● Disable

Backup Schedule

□ Backup now

○ Daily: 06 : 06

○ Weekly: Sun Time 06 : 06

● Monthly:Day 01 Time 06 : 06

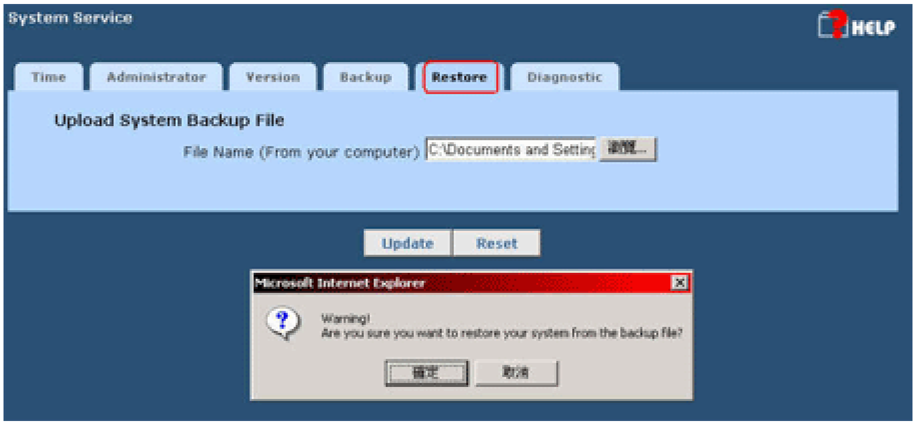
Backup File List

Delete	File name	Time	Download
Default File	04172003Hbrick.bak	Nov 30 03:01	

Figure 7.33
System Service, Backup tab

Restore

This tab allows the administrator upload System Backup File.



Upload System Backup File

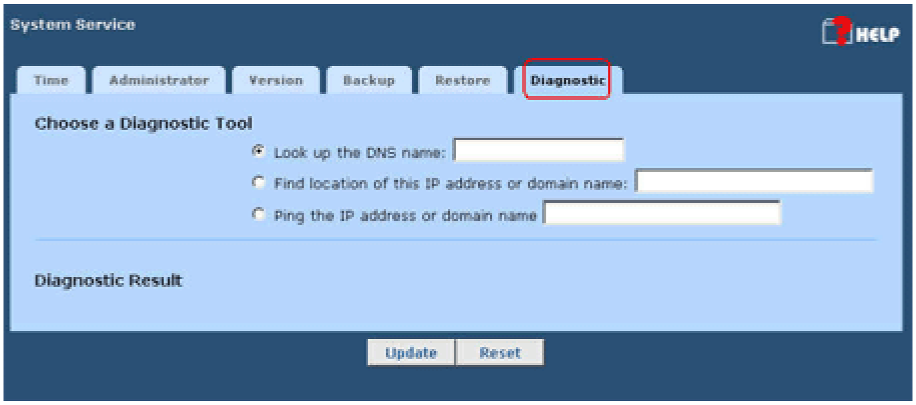
File Name (From your computer) C:\Documents and Setting 瀏覽...

Warning!
Are you sure you want to restore your system from the backup file?

Figure 7.34
System Service, Backup, restoring from a backup file

Diagnostic

This tab allows the administrator to execute standard diagnostic tools from the Firewall VPN.



Choose a Diagnostic Tool

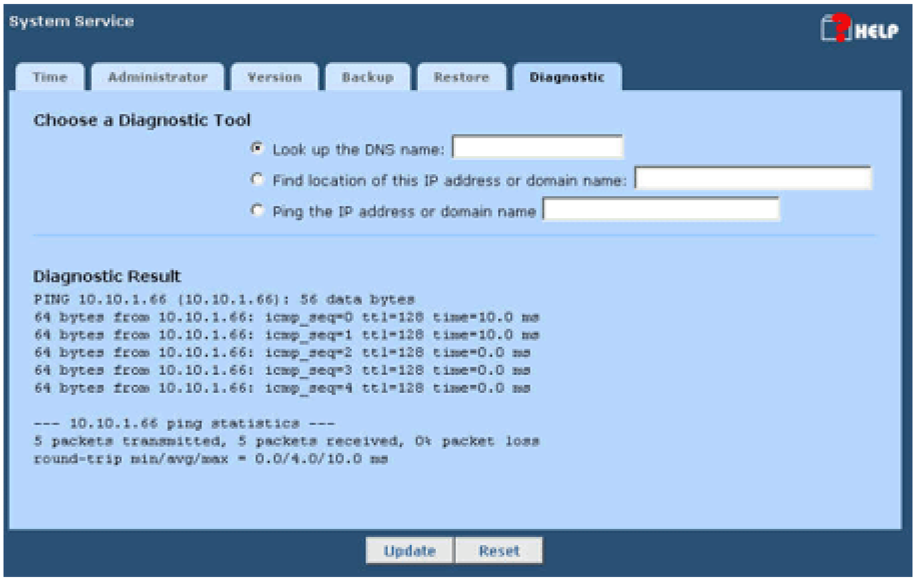
● Look up the DNS name:

○ Find location of this IP address or domain name:

○ Ping the IP address or domain name

Diagnostic Result

Figure 7.35
System Service, Diagnostic tab



Choose a Diagnostic Tool

● Look up the DNS name:

○ Find location of this IP address or domain name:

○ Ping the IP address or domain name

Diagnostic Result

```
PING 10.10.1.66 (10.10.1.66): 56 data bytes
64 bytes from 10.10.1.66: icmp_seq=0 ttl=128 time=10.0 ms
64 bytes from 10.10.1.66: icmp_seq=1 ttl=128 time=10.0 ms
64 bytes from 10.10.1.66: icmp_seq=2 ttl=128 time=0.0 ms
64 bytes from 10.10.1.66: icmp_seq=3 ttl=128 time=0.0 ms
64 bytes from 10.10.1.66: icmp_seq=4 ttl=128 time=0.0 ms

--- 10.10.1.66 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/4.0/10.0 ms
```

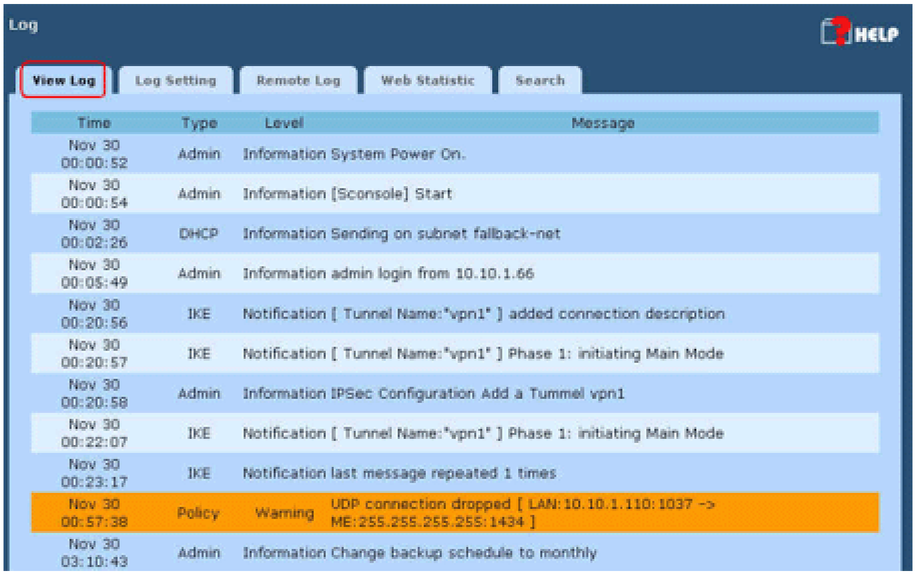
Figure 7.36
System Service, Diagnostic tab, sample ping data

Log

This menu summarizes all of the logs for the Firewall VPN, allowing the administrator to configure, search, and save these logs.

View Log

This tab displays the main log for the Firewall VPN.

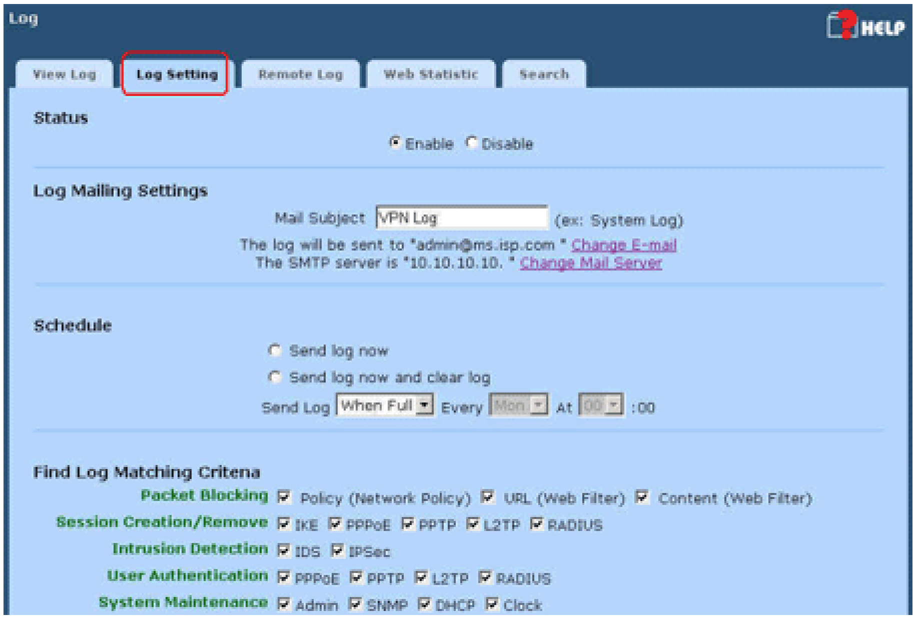


Time	Type	Level	Message
Nov 30 00:00:52	Admin	Information	System Power On.
Nov 30 00:00:54	Admin	Information	[Sconsole] Start
Nov 30 00:02:26	DHCP	Information	Sending on subnet fallback-net
Nov 30 00:05:49	Admin	Information	admin login from 10.10.1.66
Nov 30 00:20:56	IKE	Notification	[Tunnel Name:"vpn1"] added connection description
Nov 30 00:20:57	IKE	Notification	[Tunnel Name:"vpn1"] Phase 1: initiating Main Mode
Nov 30 00:20:58	Admin	Information	IPSec Configuration Add a Tummel vpn1
Nov 30 00:22:07	IKE	Notification	[Tunnel Name:"vpn1"] Phase 1: initiating Main Mode
Nov 30 00:23:17	IKE	Notification	last message repeated 1 times
Nov 30 00:57:38	Policy	Warning	UDP connection dropped [LAN:10.10.1.110:1037 -> ME:255.255.255.255:1434]
Nov 30 03:10:43	Admin	Information	Change backup schedule to monthly

Figure 7.37
Log, View log, sample policy warnings

Log Settings

This tab allows the administrator to configure some of the log settings, such as where the logs will be mailed to, when to send the log, and what should be logged.



Status

● Enable ○ Disable

Log Mailing Settings

Mail Subject VPN Log (ex: System Log)

The log will be sent to "admin@ms.isp.com " Change E-mail
The SMTP server is "10.10.10.10. " Change Mail Server

Schedule

○ Send log now
○ Send log now and clear log
Send Log When Full Every Mon At 00 :00

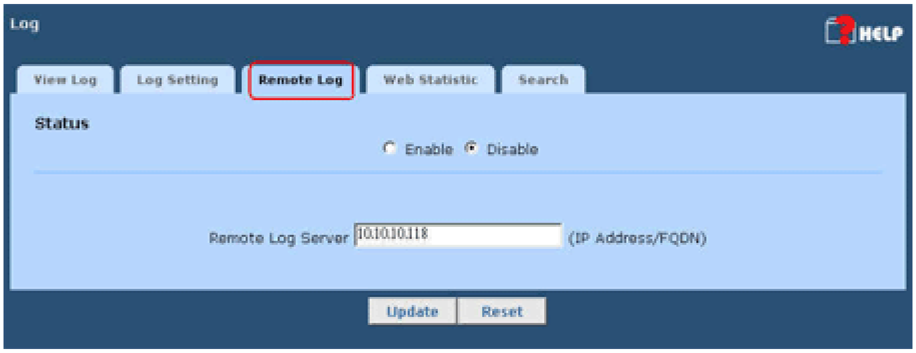
Find Log Matching Critena

Packet Blocking ☑ Policy (Network Policy) ☑ URL (Web Filter) ☑ Content (Web Filter)
Session Creation/Remove ☑ IKE ☑ PPPoE ☑ PPTP ☑ L2TP ☑ RADIUS
Intrusion Detection ☑ IDS ☑ IPSec
User Authentication ☑ PPPoE ☑ PPTP ☑ L2TP ☑ RADIUS
System Maintenance ☑ Admin ☑ SNMP ☑ DHCP ☑ Clock

Figure 7.38
Log, Log Setting tab

Remote Log

This tab allows the administrator to configure remote log settings, such as setup the remote server IP or FQDN.



Status

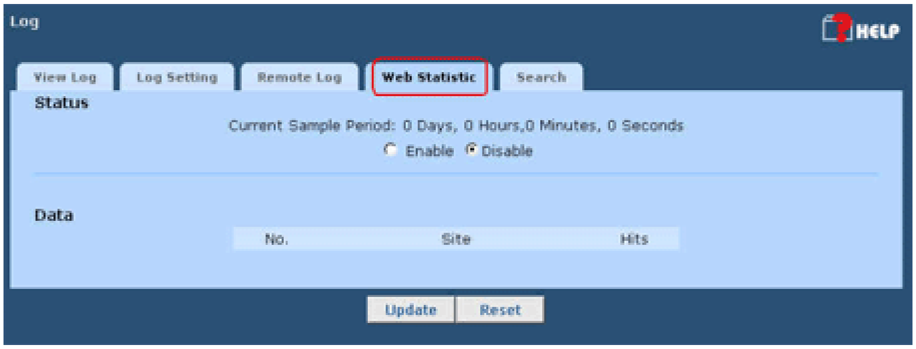
○ Enable ● Disable

Remote Log Server 10.10.10.118 (IP Address/FQDN)

Figure 7.39
Log, Remote Log Setting tab

Web Statistics

This tab allows the administrator to track the most visited web sites.



Status

Current Sample Period: 0 Days, 0 Hours,0 Minutes, 0 Seconds

○ Enable ● Disable

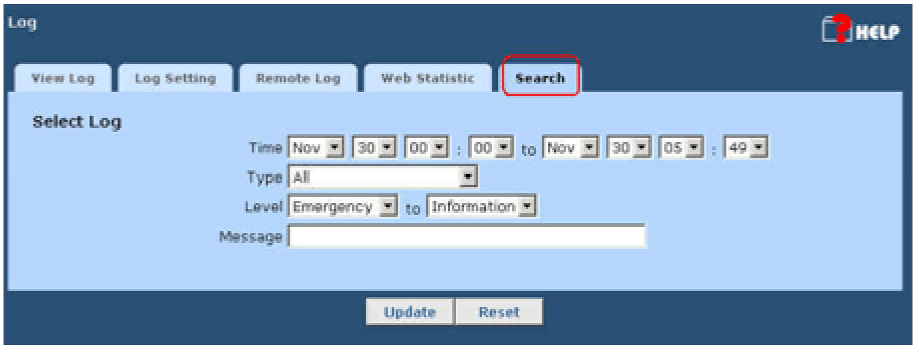
Data

No.	Site	Hits

Figure 7.40
Log, Web Statistic tab

Search

This tab allows the administrator to search the main log.



Select Log

Time Nov 30 00 : 00 to Nov 30 05 : 49

Type All

Level Emergency to Information

Message

Figure 7.41
Log, Search tab, sample search data

Exit

This menu item exits the Firewall VPN web administration interface, returning to the login screen.

Quick Tips

How do I reset my HotBrick to factory defaults if everything else fails?

Press the reset button 5 times in a row (with a half second interval). The box will reboot; since it is a master reboot, it will take approximately 5 minutes.

I have a cable modem and when I connect it to my HotBrick I have no link light. What can be wrong?

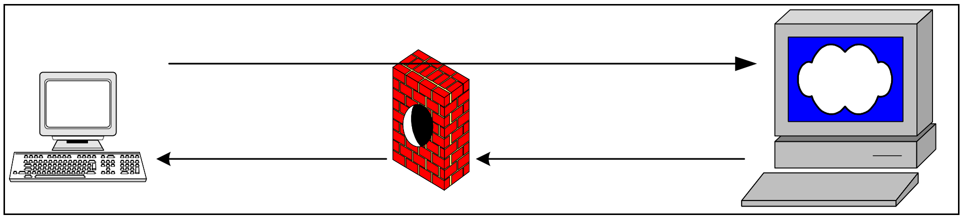
Cable modems are characterized by storing the MAC address of the device they were attached previously. What you have to do it to unplug the cable modem from the HotBrick wan port. Remove the power cable of the cable modem for about 10 seconds. After that plug the power back into the cable modem and wait until its lights go back to their normal behavior. Now, plug to cable modem into the HotBrick WAN port again and it will start to work normally.

How to Use Port Triggering

Port Triggering

If a connection from LAN to Internet matches a rule range, then initiates another special rule mapping wan port (range) to LAN host.

Here we get an example case:



Example case:

A web-based media server need to click movie via browser, then player will be initialized and "receive" movie.

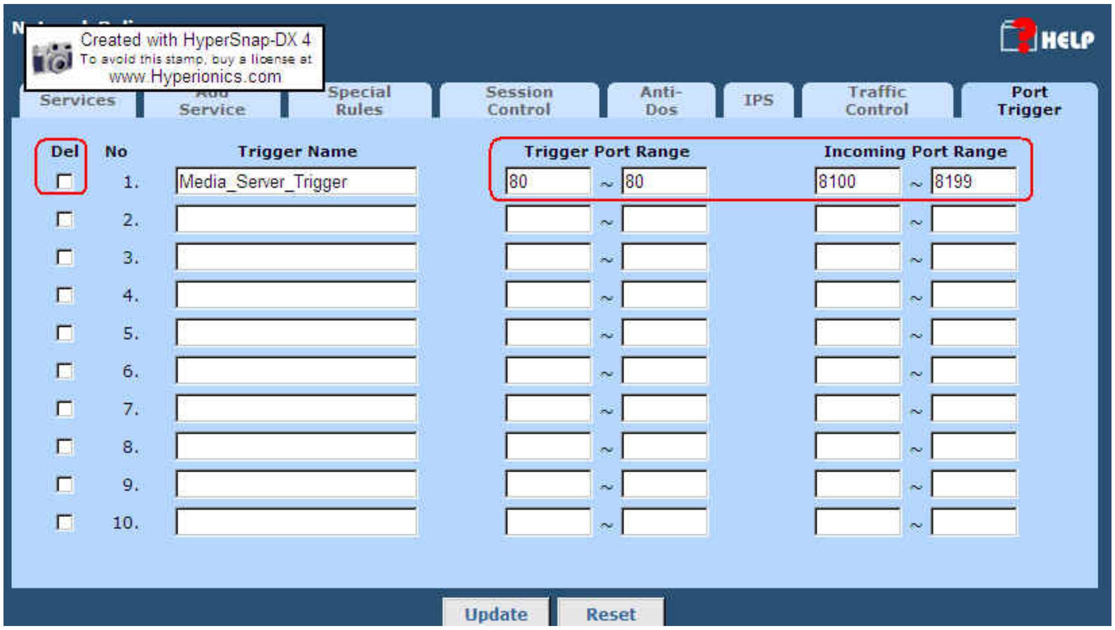
Trigger port	Incoming Port
80	8100~8199

Setting Steps: (Adding entry)

1. GUI location: Advanced Setup → Network Policy → Port Trigger
2. Insert trigger port (could be a range)
3. Insert Incoming port (could be a range)
4. Click update button to apply setting.

Deleting entries:

1. Select "Del" check box in front which item you want to delete.
2. Click update box, the entry and rules will be flushed after executing.



Del	No	Trigger Name	Trigger Port Range	Incoming Port Range
□	1.	Media_Server_Trigger	80 ~ 80	8100 ~ 8199
□	2.		~	~
□	3.		~	~
□	4.		~	~
□	5.		~	~
□	6.		~	~
□	7.		~	~
□	8.		~	~
□	9.		~	~
□	10.		~	~

Note:

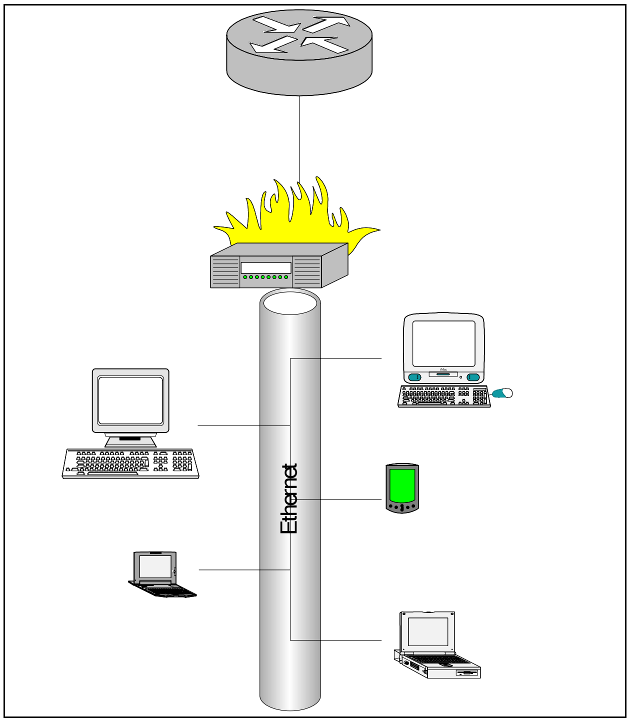
1. Trigger port will be blocked if there’s any blocking rule in firewall setting.
2. If trigger port is free to Internet, Incoming port will not be blocked even if the service is not in allow list of firewall.
3. It doesn’t matter what IP address of Client host IP or remote server IP when setting.
   But connection incoming will only match the source and destination of trigger connection.

   Ex: LAN user 192.168.0.1 trigger TCP 80, Incoming a connection TCP 8100 from 61.62.30.251
   Then only 192.168.0.1 receive incoming data, other packet from another server or to another LAN user will not be send to 192.168.0.1

How to Use Standard Transparent Mode

Standard Transparent mode

This mode means forwarding packets without NAT. This Network mode used on a topology which all in real IP.

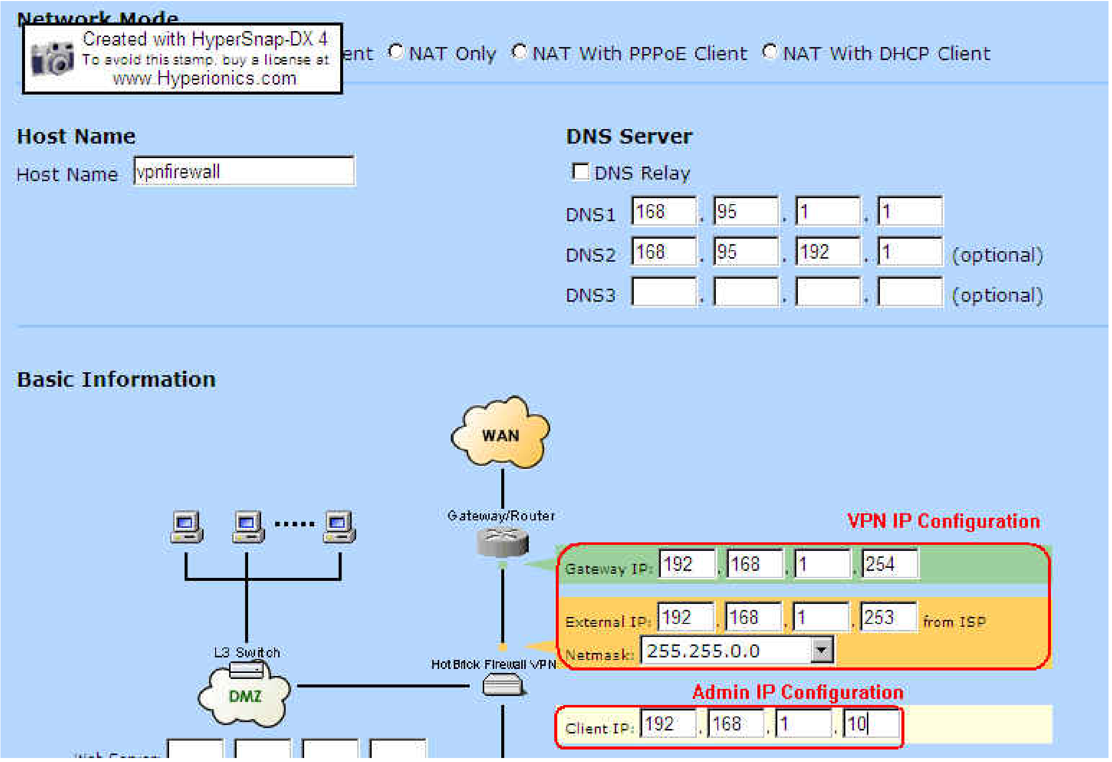


Example case:

1. Router IP 192.168.1.254
2. HotBrick IP 192.168.1.253
3. Client hosts stand behind of HotBrick, IP range start from 192.168.1.10
4. All hosts in this case in 192.168.1.0/16, go to Internet through HotBrick.
5. Admin login from 192.168.1.10

Setting steps:

1. Login GUI management interface
2. Go to Advanced → Setup → Setup → Select "Standard Transparent"
3. Insert gateway and VPN WAN IP into setup screen
4. Insert Client IP in to setup screen
5. Click Update, apply setting.



Network Mode

ent ○ NAT Only ○ NAT With PPPoE Client ○ NAT With DHCP Client

Host Name

Host Name: vpnfirewall

DNS Server

□ DNS Relay

DNS1: 168 . 95 . 1 . 1

DNS2: 168 . 95 . 192 . 1 (optional)

DNS3: . . . (optional)

Basic Information

VPN IP Configuration

Gateway IP: 192 . 168 . 1 . 254

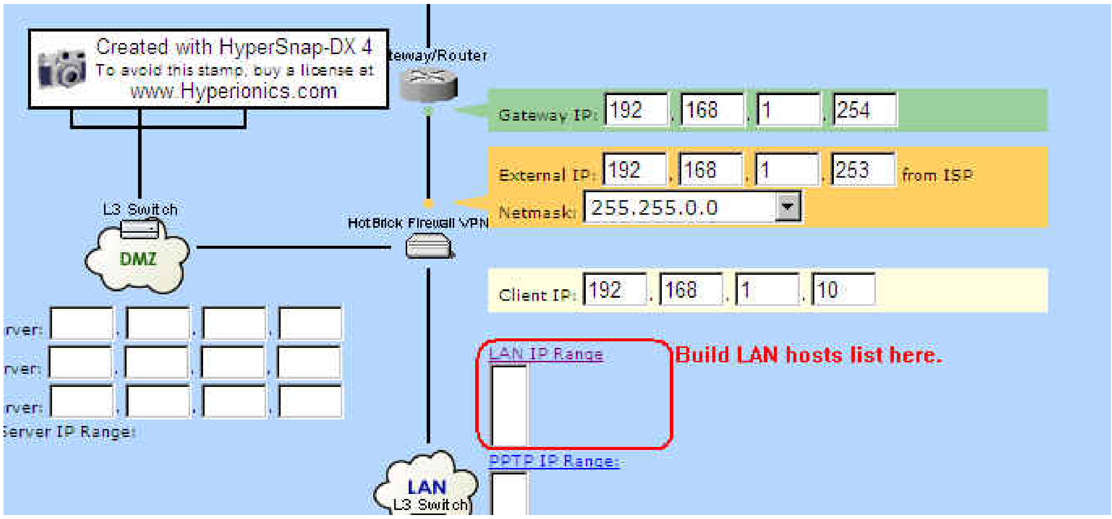
External IP: 192 . 168 . 1 . 253 from ISP

Netmask: 255.255.0.0

Admin IP Configuration

Client IP: 192 . 168 . 1 . 10

6. All routing will be flushed but "Client IP" and "Gateway"
7. Move to "LAN IP range" → Build a LAN hosts list.



Gateway IP: 192 . 168 . 1 . 254

External IP: 192 . 168 . 1 . 253 from ISP

Netmask: 255.255.0.0

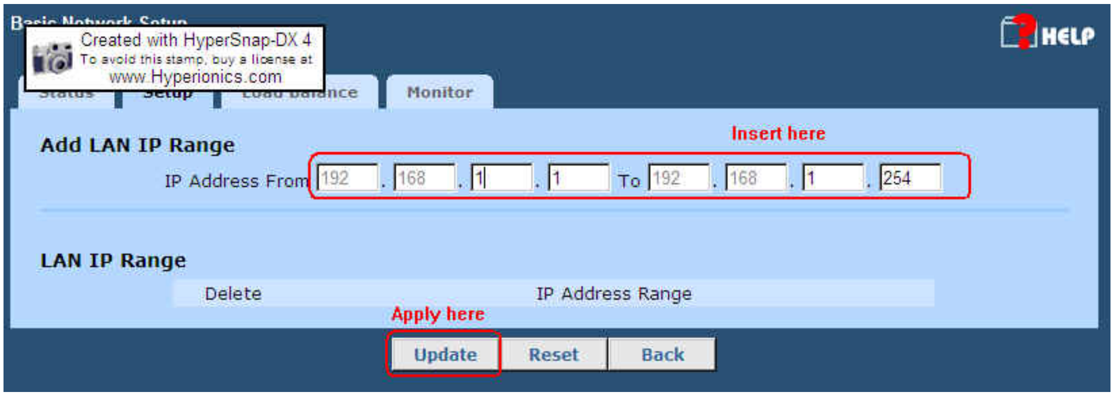
Client IP: 192 . 168 . 1 . 10

LAN IP Range

Build LAN hosts list here.

PPTP IP Range:

8. Insert LAN IP which under HotBrick, by range.



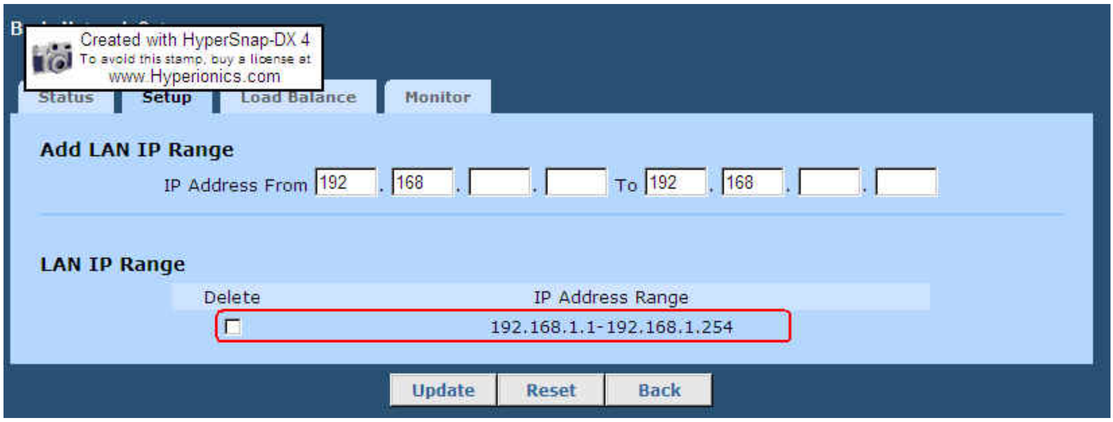
Add LAN IP Range

IP Address From 192 . 168 . 1 . 1 To 192 . 168 . 1 . 254

LAN IP Range

Delete	IP Address Range

9. Make sure LAN IP range exists.



Add LAN IP Range

IP Address From 192 . 168 . . To 192 . 168 . .

LAN IP Range

Delete	IP Address Range
□	192.168.1.1-192.168.1.254

Note:

1. Client IP = Admin IP, Admin login into management GUI only from this source IP.
2. Make sure all exist IP (range) is in LAN IP range or users will unable to access Internet
3. In this release so far (0_1_0471), Admin must modify LAN IP range after switching to Transparent Mode.
   Do not support setup LAN IP range before switching to Transparent Mode.
   (Entry will be flushed after executing.)

APPENDIX A – Commonly Used Ports and Services

Port No.	Protocol	Service Name	Aliases	Comment
7	TCP	echo		Echo
7	UDP	echo		Echo
9	TCP	discard	sink null	Discard
9	UDP	discard	sink null	Discard
13	TCP	daytime		Daytime
13	UDP	daytime		Daytime
17	TCP	qotd	quote	Quote of the day
17	UDP	qotd	quote	Quote of the day
19	TCP	chargen	ttytst source	Character generator
19	UDP	chargen	ttytst source	Character generator
20	TCP	ftp-data		File Transfer
21	TCP	ftp		FTP Control
23	TCP	telnet		Telnet
25	TCP	smtp	mail	Simple Mail Transfer
37	TCP	time		Time
37	UDP	time		Time
39	UDP	rlp	resource	Resource Location Protocol
42	TCP	nameserver	name	Host Name Server
42	UDP	nameserver	name	Host Name Server
43	TCP	nicname	whois	Who Is
53	TCP	domain		Domain Name
53	UDP	domain		Domain Name Server
67	UDP	bootps	dhcps	Bootstrap Protocol Server
68	UDP	bootpc	dhcpc	Bootstrap Protocol Client
69	UDP	tftp		Trivial File Transfer
70	TCP	gopher		Gopher
79	TCP	finger		Finger
80	TCP	http	www, http	World Wide Web
88	TCP	kerberos	krb5	Kerberos
88	UDP	kerberos	krb5	Kerberos
101	TCP	hostname	hostnames	NIC Host Name Server
102	TCP	iso-tsap		ISO-TSAP Class 0
107	TCP	rtelnet		Remote Telnet Service
109	TCP	pop2	postoffice	Post Office Protocol - Version 2
110	TCP	pop3	postoffice	Post Office Protocol - Version 3
111	TCP	sunrpc	rpcbind portmap	SUN Remote Procedure Call
111	UDP	sunrpc	rpcbind portmap	SUN Remote Procedure Call
113	TCP	auth	ident tap	Authentication Service
117	TCP	uucp-path		UUCP Path Service
119	TCP	nntp	usenet	Network News Transfer Protocol
123	UDP	ntp		Network Time Protocol
135	TCP	epmap	loc-srv	DCE endpoint resolution
135	UDP	epmap	loc-srv	DCE endpoint resolution
137	TCP	netbios-ns	nbname	NETBIOS Name Service
137	UDP	netbios-ns	nbname	NETBIOS Name Service
138	UDP	netbios-dgm	nbdatagram	NETBIOS Datagram Service
139	TCP	netbios-ssn	nbsession	NETBIOS Session Service
143	TCP	imap	imap4	Internet Message Access Protocol
158	TCP	pcmail-srv	repository	PC Mail Server
161	UDP	snmp	snmp	SNMP
162	UDP	snmptrap	snmp-trap	SNMP TRAP
170	TCP	print-srv		Network PostScript
179	TCP	bgp		Border Gateway Protocol
194	TCP	irc		Internet Relay Chat Protocol
213	UDP	ipx		IPX over IP
389	TCP	ldap		Lightweight Directory Access Protocol

443	TCP	https	MCom	
443	UDP	https	MCom	
445	TCP			Microsoft CIFS
445	UDP			Microsoft CIFS
464	TCP	kpasswd		Kerberos (v5)
464	UDP	kpasswd		Kerberos (v5)
500	UDP	isakmp	ike	Internet Key Exchange (IPSec)
512	TCP	exec		Remote Process Execution
512	UDP	biff	comsat	Notifies users of new mail
513	TCP	login		Remote Login
513	UDP	who	whod	Database of who's logged on, average load
514	TCP	cmd	shell	Automatic Authentication
514	UDP	syslog		
515	TCP	printer	spooler	Listens for incoming connections
517	UDP	talk		Establishes TCP Connection
518	UDP	ntalk		
520	TCP	efs		Extended File Name Server
520	UDP	router	router routed	RIPv.1, RIPv.2
525	UDP	timed	timeserver	Timeserver
526	TCP	tempo	newdate	Newdate
530	TCP,UDP	courier	rpc	RPC
531	TCP	conference	chat	IRC Chat
532	TCP	netnews	readnews	Readnews
533	UDP	netwall		For emergency broadcasts
540	TCP	uucp	uucpd	Uucpd
543	TCP	klogin		Kerberos login
544	TCP	kshell	krcmd	Kerberos remote shell
550	UDP	new-rwho	new-who	New-who
556	TCP	remotefs	rfs rfs_server	Rfs Server
560	UDP	rmonitor	rmonitord	Rmonitor
561	UDP	monitor		
636	TCP	ldaps	sldap	LDAP over TLS/SSL
749	TCP	kerberos-adm		Kerberos administration
749	UDP	kerberos-adm		Kerberos administration
1109	TCP	kpop		Kerberos POP
1167	UDP	phone		Conference calling
1433	TCP	ms-sql-s		Microsoft-SQL-Server
1433	UDP	ms-sql-s		Microsoft-SQL-Server
1434	TCP	ms-sql-m		Microsoft-SQL-Monitor
1434	UDP	ms-sql-m		Microsoft-SQL-Monitor
1512	TCP	wins		Microsoft Windows Internet Name Service
1512	UDP	wins		Microsoft Windows Internet Name Service
1524	TCP	ingreslock	ingres	Ingres
1701	UDP	l2tp		Layer Two Tunneling Protocol
1723	TCP	pptp		Point-to-point tunneling protocol
1812	UDP	radiusauth		RRAS (RADIUS authentication protocol)
1813	UDP	radacct		RRAS (RADIUS accounting protocol)
2049	UDP	nfsd	nfs	Sun NFS server
2053	TCP	knetd		Kerberos de-multiplexer
2504	UDP	nlbs		Network Load Balancing
9535	TCP	man		Remote Man Server

APPENDIX B – Common Services and Ports

Service Name	UDP	TCP
Browsing datagram responses of NetBIOS over TCP/IP	138	
Browsing requests of NetBIOS over TCP/IP	137	
Client/Server Communication		135
Common Internet File System (CIFS)	445	139, 445
Content Replication Service		560
Cybercash Administration		8001
Cybercash Coin Gateway		8002
Cybercash Credit Gateway		8000
DCOM (SCM uses udp/tcp to dynamically assign ports for DCOM)	135	135
DHCP client		67
DHCP server		68
DHCP Manager		135
DNS Administration		139
DNS client to server lookup (varies)	53	53
Exchange Server 5.0		
Client Server Communication		135
Exchange Administrator		135
IMAP		143
IMAP (SSL)		993
LDAP		389
LDAP (SSL)		636
MTA - X.400 over TCP/IP		102
POP3		110
POP3 (SSL)		995
RPC		135
SMTP		25
NNTP		119
NNTP (SSL)		563
File shares name lookup	137	
File shares session		139
FTP		21
FTP-data		20
HTTP		80
HTTP-Secure Sockets Layer (SSL)		443
Internet Information Services (IIS)		80
IMAP		143
IMAP (SSL)		993
IKE	500	
IPSec Authentication Header (AH)		
IPSec Encapsulation Security Payload (ESP)		
IRC		531
ISPMOD (SBS 2nd tier DNS registration wizard)		1234
Kerberos de-multiplexer		2053
Kerberos klogin		543
Kerberos kpasswd (v5)	464	464
Kerberos krb5	88	88
Kerberos kshell		544
L2TP	1701	
LDAP		389
LDAP (SSL)		636
Login Sequence	137, 138	139
Macintosh, File Services (AFP/IP)		548
Membership DPA		568
Membership MSN		569
Microsoft Chat client to server		6667
Microsoft Chat server to server		6665
Microsoft Message Queue Server	1801	1801
Microsoft Message Queue Server	3527	135, 2101

Microsoft Message Queue Server		2103, 2105
MTA - X.400 over TCP/IP		102
NetBT datagrams	138	
NetBT name lookups	137	
NetBT service sessions		139
NetLogon	138	
NetMeeting Audio Call Control		1731
NetMeeting H.323 call setup		1720
NetMeeting H.323 streaming RTP over UDP	Dynamic	
NetMeeting Internet Locator Server ILS		389
NetMeeting RTP audio stream	Dynamic	
NetMeeting T.120		1503
NetMeeting User Location Service		522
NetMeeting user location service ULS		522
Network Load Balancing	2504	
NNTP		119
NNTP (SSL)		563
Outlook (see for ports)		
Pass Through Verification	137, 138	139
POP3		110
POP3 (SSL)		995
PPTP control		1723
PPTP data		
Printer sharing name lookup	137	
Printer sharing session		139
Radius accounting (Routing and Remote Access)	1646 or 1813	
Radius authentication (Routing and Remote Access)	1645 or 1812	
Remote Install TFTP		69
RPC client fixed port session queries		1500
RPC client using a fixed port session replication		2500
RPC session ports		Dynamic
RPC user manager, service manager, port mapper		135
SCM used by DCOM	135	135
SMTP		25
SNMP	161	
SNMP Trap	162	
SQL Named Pipes encryption over other protocols name lookup	137	
SQL RPC encryption over other protocols name lookup	137	
SQL session		139
SQL session		1433
SQL session		1024 - 5000
SQL session mapper		135
SQL TCP client name lookup	53	53
Telnet		23
Terminal Server		3389
UNIX Printing		515
WINS Manager		135
WINS NetBios over TCP/IP name service	137	
WINS Proxy	137	
WINS Registration		137
WINS Replication		42
X400		102