BaseWall VPN 6000 user manual

version 33 (2005-11-11)

Title: BaseWall VPN 6000 user manual
Revision: 33 (05-11-11)

Table of Contents

1 Installation

1.1 Requirements

To insure a smooth installation of your BaseWall VPN 6000, we should make sure to have all the necessary equipment and information ready. To configure your firewall for the first time we will need:

1x BaseWall VPN 6000

1x Standard power cord (bundled with BaseWall VPN 6000)

2x UTP RJ45 cables (one is bundled with BaseWall VPN 6000)

1x UTP RJ45 cross cable or UTP hub/switch for initial configuration

1x PC or notebook computer

If we are to set up your firewall to handle one or more Internet connections, we will also need:

Connection details provided by your Internet Service Provider (ISP)

1.2 Getting to know your BaseWall VPN 6000

1.2.1 Front

1. LCD display
2. Serial port
3. WAN1 port
4. WAN1 connection LED
5. WAN2 port
6. WAN2 connection LED
7. FLEX1 port
8. FLEX1 connection LED
9. FLEX2 port
10. FLEX2 connection LED
11. FLEX3 port
12. FLEX3 connection LED
13. FLEX4 port
14. FLEX4 connection LED

1.2.2 Back

15. Power socket
16. Power switch

1.3 Hardware installation

➔ Use the power cord to connect the BaseWall VPN 6000's power socket (15) to a standard wall power outlet.

➔ Switch the firewall on, using the power switch (16), on the back of the device.

Booting the hardware for the first time may take up to 1 minute.

When the firewall is switched on and ready, you should hear 3 short beeps. If you have not heard 3 beeps within 1 minute of switching on the device, please refer to section 1.13 (Errors and recovery).

➔ Use an UTP RJ45 cross cable to connect the firewall's FLEX1 port (7) to a network connector on your PC or notebook. It is also possible to create a 2 computer LAN with the use of a UTP hub or switch.

➔ Switch on the PC or notebook.

The FLEX1 connection LED above the FLEX1 port (8) should come on. If this LED does not come on, please refer to section 1.13 (Errors and recovery).

1.4 Connecting to the management interface

Your BaseWall VPN 6000 is highly configurable by means of a powerful management interface. Once the device is properly set up you will be able to access this interface from any machine in your local network (provided you know the right password). For the initial setup of the firewall we will make use of the same management interface. However, because the device is not set up to connect with a local network or Internet connection, it must first be configured using a single PC or notebook.

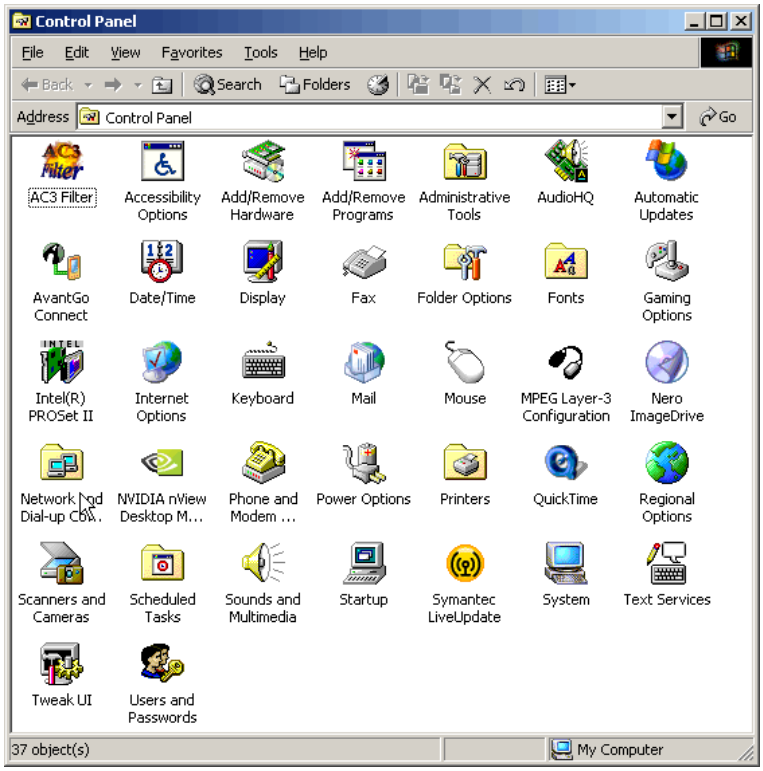
1.4.1 Configure a notebook or PC to use DHCP

If you are to use the firewall's management interface from your notebook or PC, then both are to be connected and using a common network setup. The fastest way to effect this is to have your PC or Notebook computer configure it's network settings automatically by means of DHCP (Dynamic Host Configuration Protocol). As this is done in a slightly different manner by various operating systems, the following sections will detail the procedure for enabling DHCP in *Windows*® 2000, *Windows*® XP (or *Windows*® 2003) and *Mac OS X*® respectively.

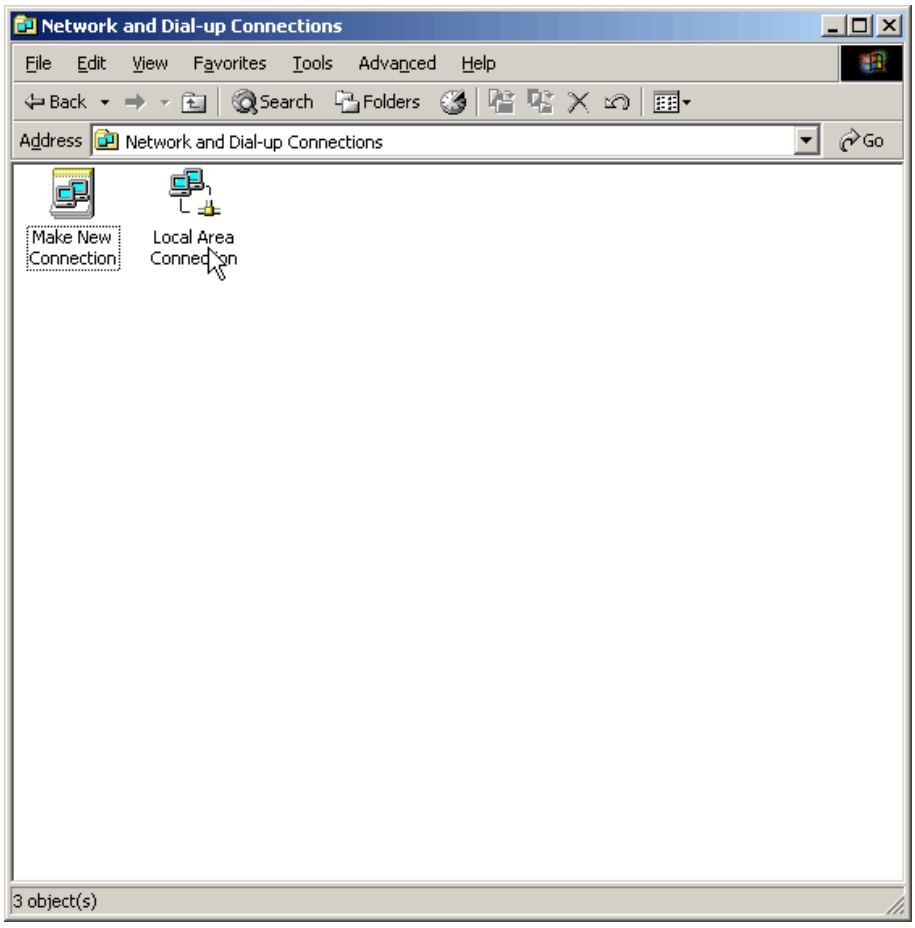
Enabling DHCP using Windows® 2000

➔ Using the *Windows*® “Start” menu (and Settings sub menu), open the “Control Panel”.

➔ In the “Control panel”, double click the “Network and Dial-up Connections” icon.



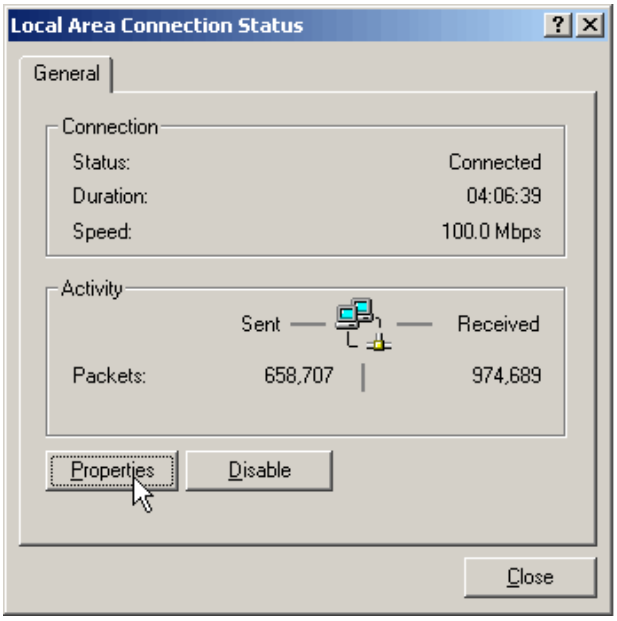
The window “Network and Dial-up Connections” should open.



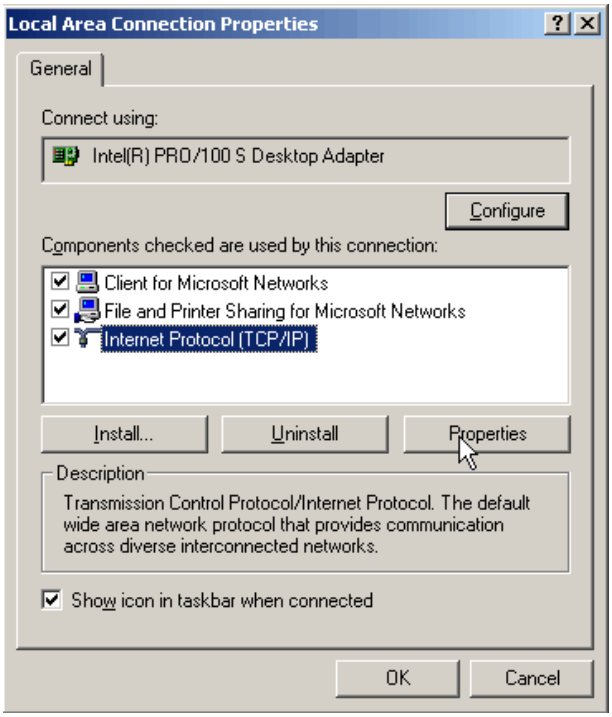
➔ In the “Network and Dial-up Connections” window, double click the “Local Area Connection” icon.

The “Local Area Connection Status” window should open.

➔ In the “Local Area Connection Status” window, click the “Properties”button.



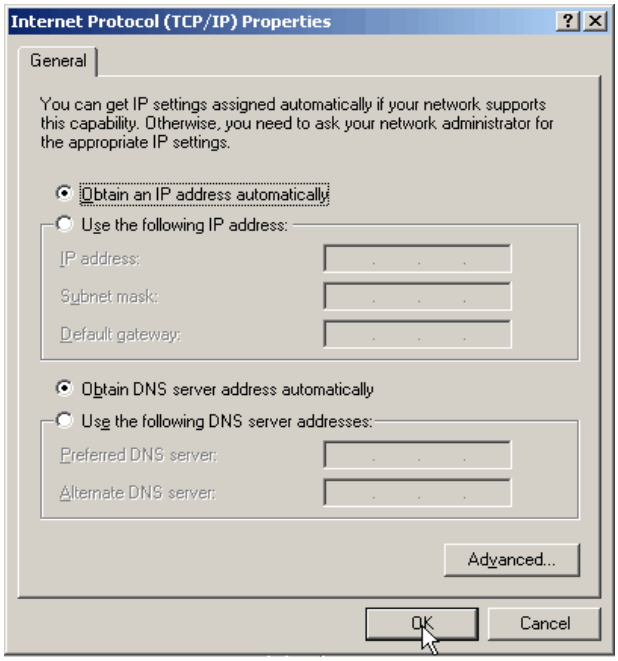
The “Local Area Connection Properties” window should open.



➔ In this window, select “Internet Protocol (TCP/IP)” (the blue line in the example below).

➔ Click the “Properties” button.

The window “Internet Protocol (TCP/IP) Properties” should open.



➔ Make sure settings in this window are as specified in the example above (check “Obtain an IP address automatically” and “Obtain DNS server address automatically”.

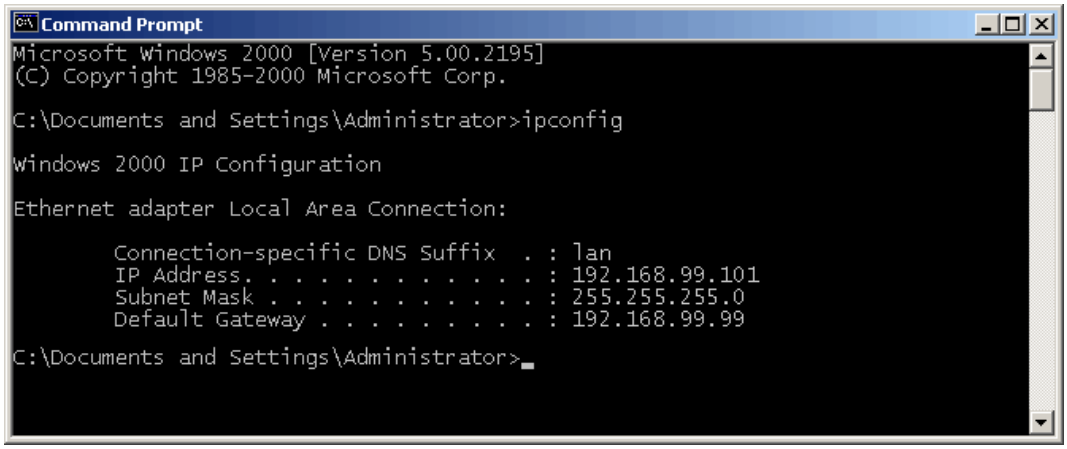
➔ Click the “OK” button to confirm your changes.

➔ To verify your settings, open a “Command Prompt” (From the “Start” menu, through “Programs”, in the “Accessories” sub menu).

➔ In the command prompt type:

```
ipconfig
```

The output should look like this:



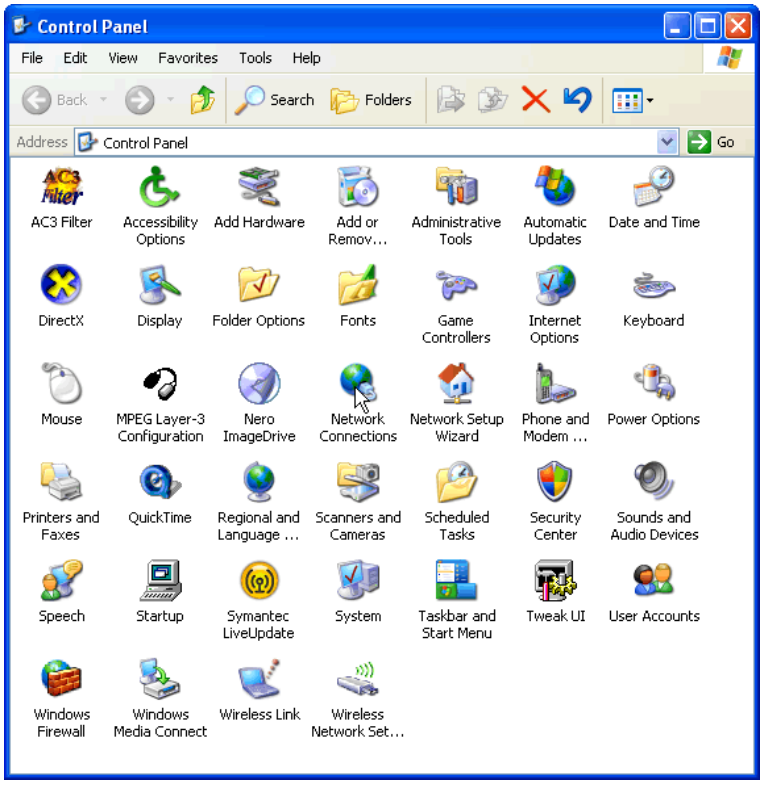
➔ If the “IP Address” line does not list an address starting with 192.168.99, please try typing:

```
ipconfig /renew
```

This should force the PC or Notebook to request a new network address. If you still fail to get an “IP Address” in the correct range, please refer to section 1.13 (Errors and recovery).

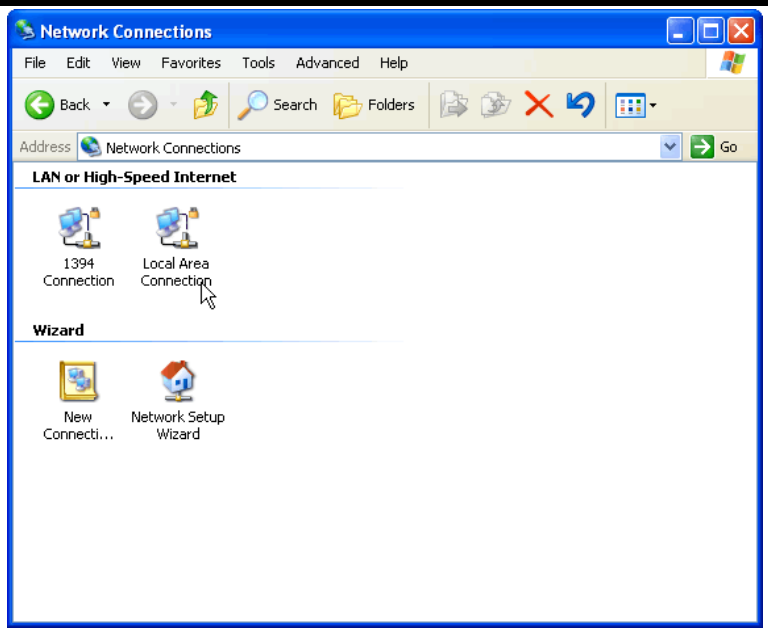
Enabling DHCP using Windows® XP

➔ Using the *Windows*® “Start” menu (and Settings sub menu), open the “Control Panel”.



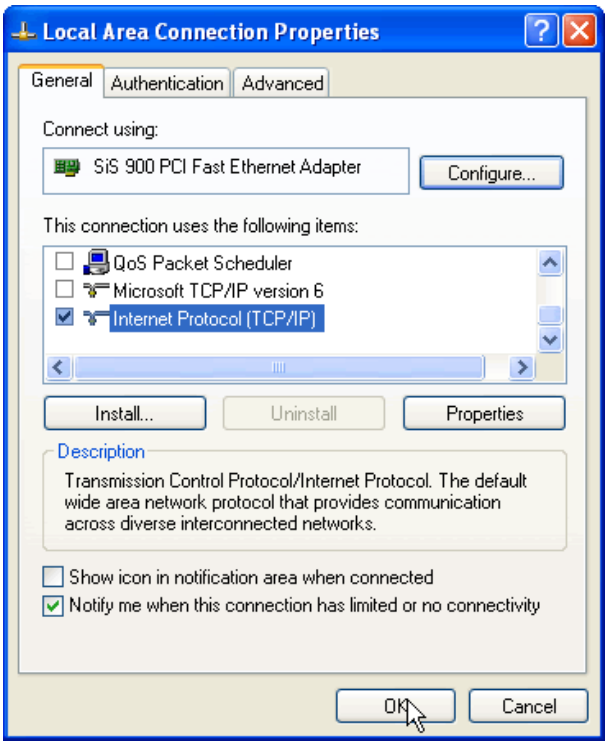
➔ In the “Control Panel”, double click the “Network Connections” icon.

The “Network Connections” window should open.



➔ In the “Network Connections” window, double click the “Local Area Connection” icon.

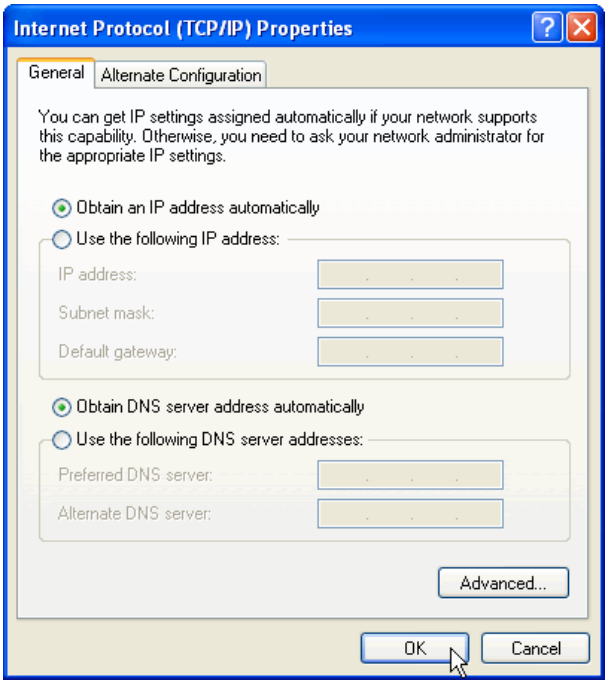
The “Local Area Connection Properties” window should open.



➔ In the “Local Area Connection Properties” window, select “Internet Protocol (TCP/IP)” (the blue line in the above example).

➔ Then press “Properties”.

The “Internet Protocol (TCP/IP) Properties window should open.



➔ In the “Internet Protocol (TCP/IP) Properties” window, make sure settings are as in the above example (“Obtain an IP address automatically” and “Obtain DNS server address automatically”are selected).

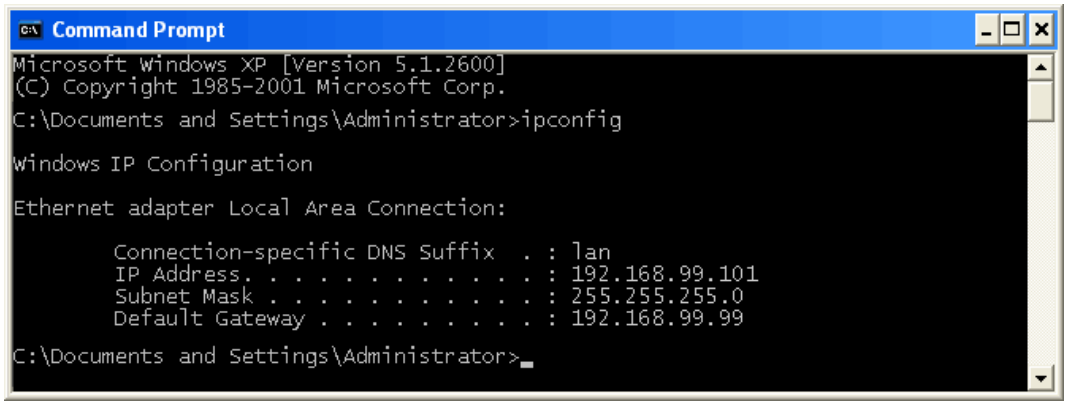
➔ Press the “OK” button to confirm your new settings.

➔ To verify your settings, open a “Command Prompt” (From the “Start” menu, through “All Programs”, in the “Accessories” sub menu).

➔ In the command prompt type:

```
ipconfig
```

The output should look like this:



➔ If the “IP Address” line does not list an address starting with 192.168.99, please try typing:

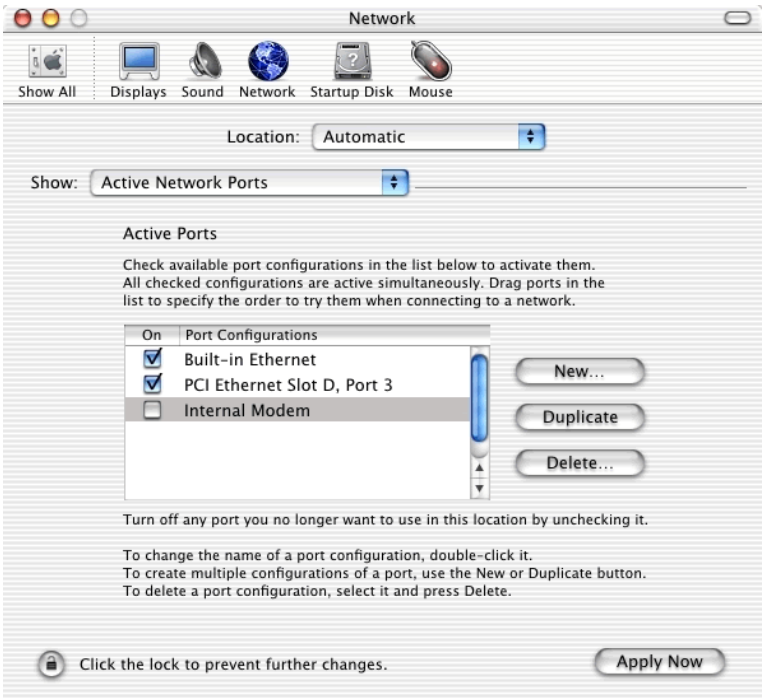
```
ipconfig /renew
```

This should force the PC or Notebook to request a new network address. If you still fail to get an “IP Address” in the correct range, please refer to section 1.13 (Errors and recovery).

Enabling DHCP using Mac OS® X

➔ From the *Apple*® menu, choose “System Preferences”, then “Network”.

The Network window should open.



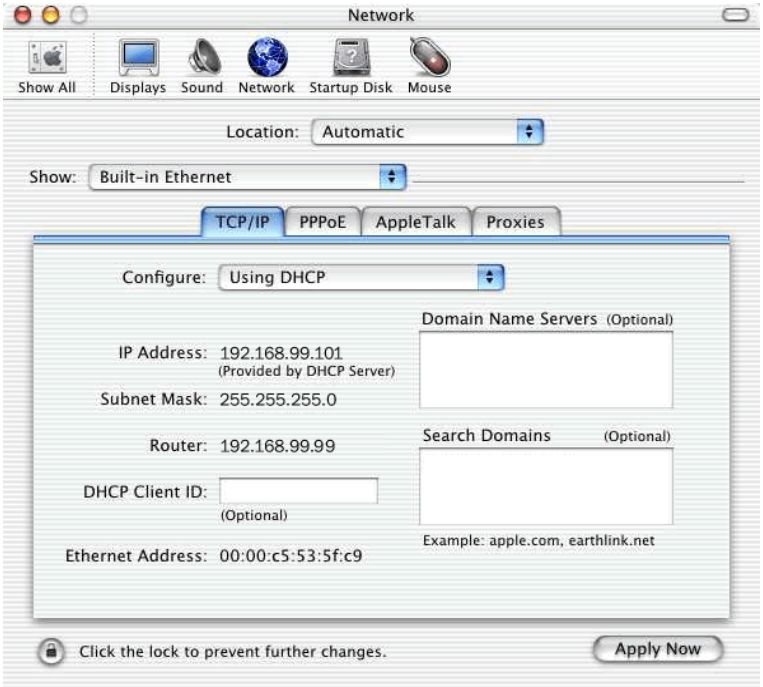
➔ In the “Network” window, make sure the “Show” box is set to show “Active Network Ports”.

➔ Drag “Built-in Ethernet” to the top of the list.

➔ Set the “Show” box to “Built-in Ethernet”.

➔ Now select the “TCP/IP” tab.

➔ Switch the “Configure” box to “Using DHCP”.



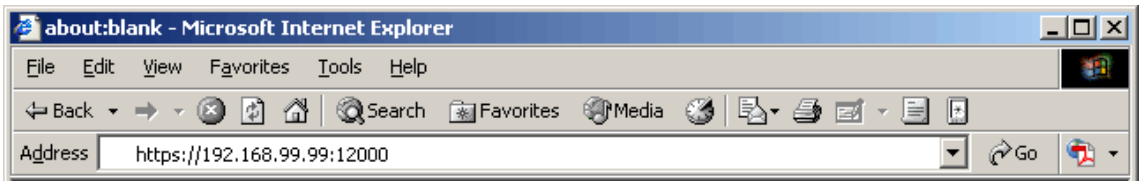
➔ Verify that the “IP address”, “Subnet Mask” and “Router” settings are as shown (192.168.99.101, 255.255.255.0 and 192.168.99.99 respectively).

➔ Click “Apply Now” to confirm your changes.

1.4.2 Log in on the firewall management interface

➔ Open a web browser on the PC or Notebook you have just configured

➔ Enter the address “ https://192.168.99.99:12000”into the address bar.



➔ When prompted for a user name and password, enter “admin” (user name) and “password” (as password).

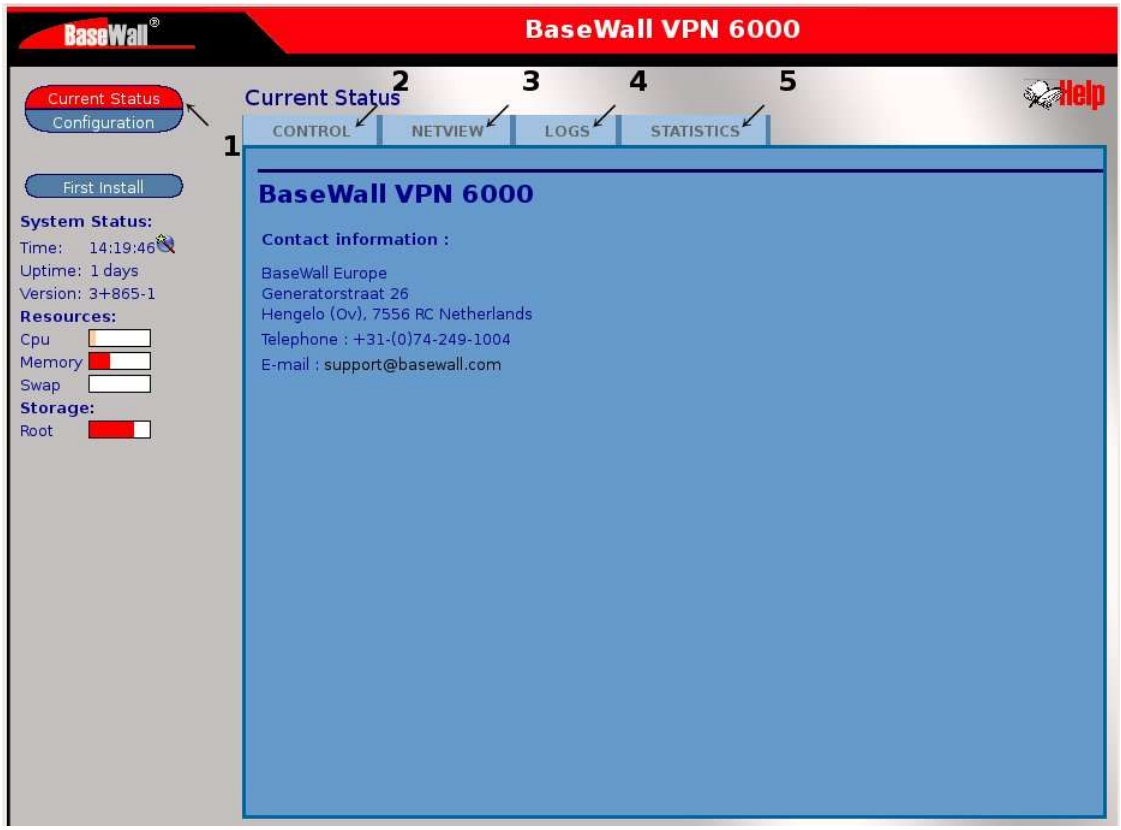
➔ Click “OK”.

If you get a “timeout”, “not found” or “permission denied” error, please refer to section 1.13 (Errors and recovery).

1.5 Basic screen layout

Once you have logged in to the firewall's management interface, you should see the following welcome screen.

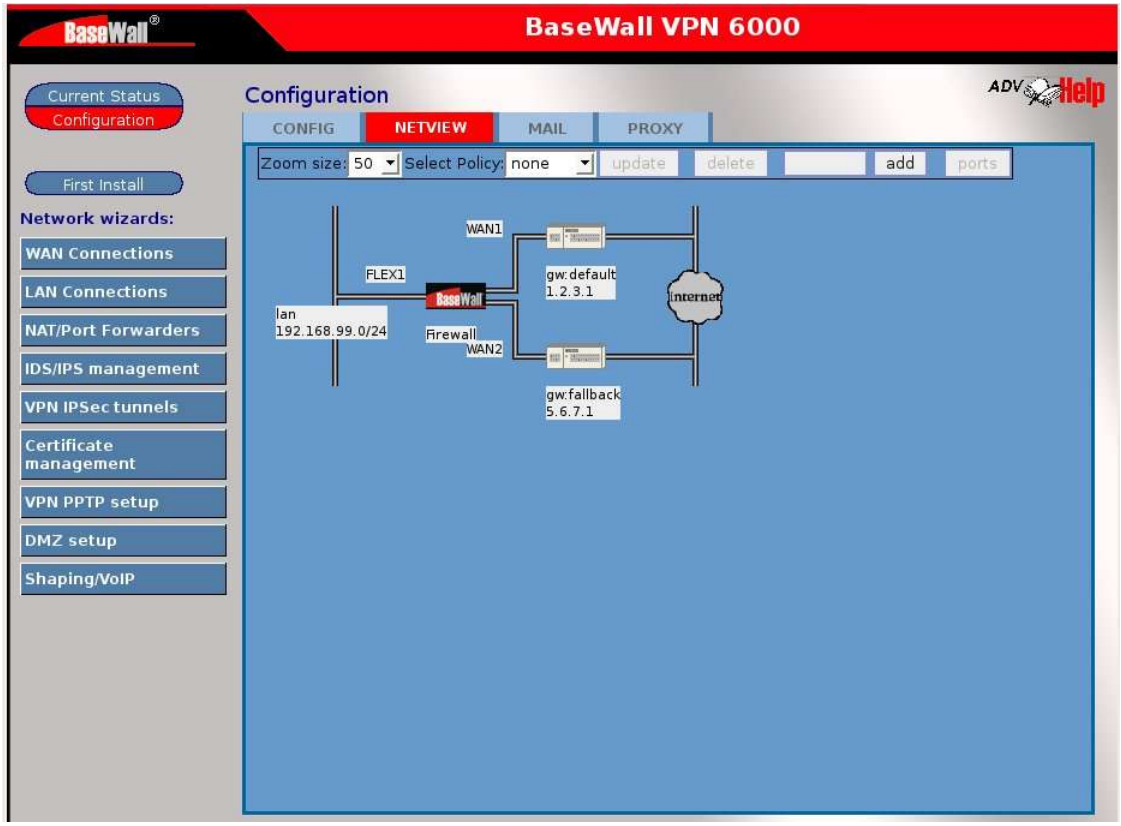
The firewall has two modes of operation. One shows the current status of the firewall and one is for configuration.



A red area in the upper left-hand corner of the screen indicates we are looking at the “Current Status”(1) of the firewall. Tabs labeled “CONTROL”(2), “NETVIEW”(3), “LOGS”(4) and “STATISTICS”(5) provide access to other screens in the “Current Status” context.

The system status on the left hand side of the screen, about half-way to the bottom displays some statistics concerning the operation of your firewall's hardware. These statistics are updated once every 10 seconds, to insure the accuracy of the information.

Pushing the Configuration button switches the interface into configuration mode. The configuration is not directly activated. When witching back to “Current Status” or pushing “Unapplied changes” button changes the actual configuration of the firewall.



The configuration window has a different layout. The left bar now contains a list of wizards and there are now different tabs “CONFIG”, “NETVIEW”, “MAIL” and “PROXY”. The current windows shows the factory configuration of the firewall. With the current network 192.168.99.0 where the firewall occupies the 192.168.99.99 ip address. There are 2 Internet connections defined but with initial values. After the “First install” wizard the picture should show the correct addresses for your situation.

1.6 Running the “First install” wizard

The “First install” wizard was intended to allow you to quickly and efficiently tailor the BaseWall VPN 6000 to match your network's needs and settings. Whenever you start a “First install” wizard, all current configuration data will be lost.

At a first installation this should not pose a problem. However, if you ever feel you should change important configuration data at a later stage, you are encouraged to use the “Local Area Networks” or “Internet Connections” wizards from the “Configuration” context instead.

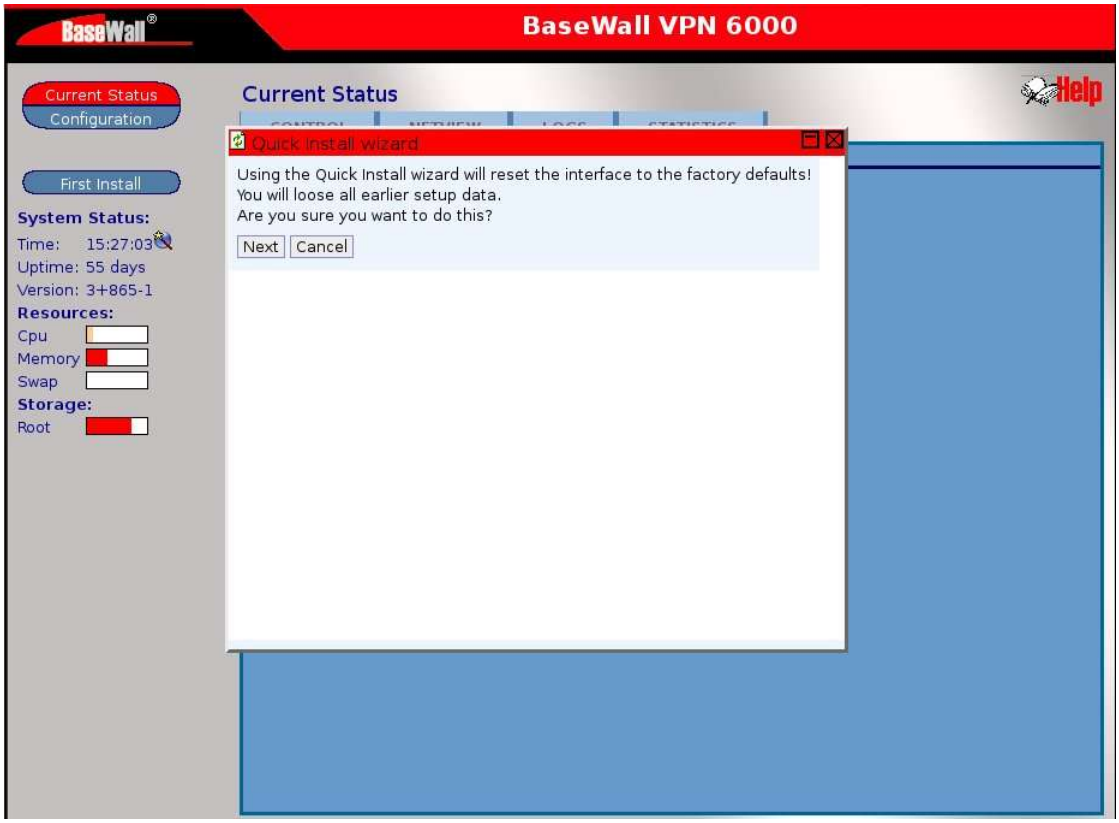
You may start the “First install” wizard by pressing the red “First install” text, in the left hand side of the screen, between “Current Status” and “Configuration”.

➔ Start the “First install wizard”

When you start the “First install” wizard, a warning screen signals the start of this wizard. The screen is there to prevent you from inadvertently starting the “First install” wizard at a later time, thereby deleting all your current network

settings. However, for a first install, we do not consider this a problem.

➔ Click “next”.



1.6.1 Setting up your LAN connection

The first step after starting the wizard is to set up your LAN (Local Area Network) connection. This is the connection between the firewall and your local network. As a firewall, the BaseWall VPN 6000 should serve as a buffer between your Internet connections (WAN or Wide Area Network connections) and your local network (or LAN).

The “First Install” wizard will allow you to enter network settings specific to your local network. First we enter a label to use for the local network. Default setting is “lan”, which seems sensible. In more complex network environments, with more than one LAN you may opt to use a more descriptive name (like “public lan” or “accounting lan” instead). In any case, make sure the names you use are unique throughout your organization, to avoid confusion arising from identical network names for different networks.

➔ Enter a network name for your local network

The next values to enter are an internal IP Address for the firewall (in the context of the LAN) and a net mask. Together, the IP Address and the net mask define a network address for the local network. In our example we use an IP Address of 192.168.0.1, with a net mask of 24 (bits). A net mask of 24 (=3*8) means that the first three numbers from the IP Address will be part of the network address, so all addresses in the network start with 192.168.0. If you

already have a local network, then this network address should have a predefined value (if uncertain, contact your network administrator). In this case, please note that BaseWall VPN 6000 displays the net mask as a number of bits, not in the 255.255.255.0 format.

If you do not have a local network, then you need to pick an address for your local network first. There are a number of possible network addresses set aside for use in a local network. The table below lists the possible IP addresses, their net masks and uses:

Network Address	***Net mask***	***Internal IP addresses***	***maximum addresses***
192.168.0.0	16	192.168.x.n	65 thousand
172.16.0.0	12	172.16-31.x.n	1 million
10.0.0.0	8	10.x.y.n	16 million

Where x, y can denote any *predefined* number between 0 and 255, n may be any number between 1 and 254.

Users who intend to use the BaseWall VPN 6000 to connect their local network to another LAN by means of a VPN tunnel (or indeed, anyone wishing to leave this option open) will do well to choose a different network address for each LAN (for example 192.168.0.0, 192.168.1.0, 192.168.2.0 etc.).

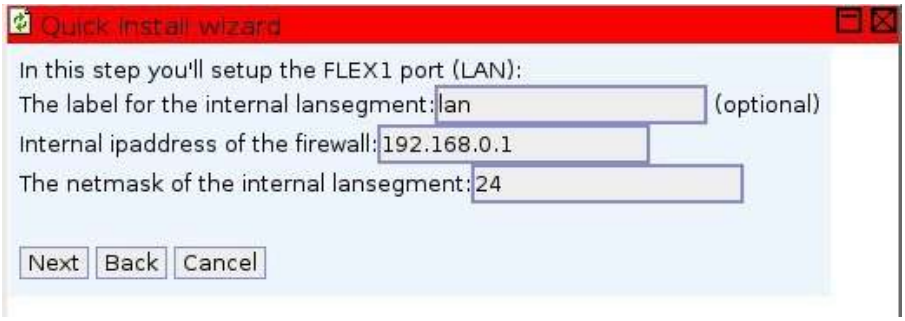
As an example only, we will make use of a 192.168.0.0 network in this user manual. We will set the firewall's internal IP address to 192.168.0.1 and the net mask value to 24 (as befits a 192.168.0.x network).

➔ Enter a firewall IP address.

➔ Enter the corresponding net mask.

➔ Write down the IP address and net mask values for later reference.

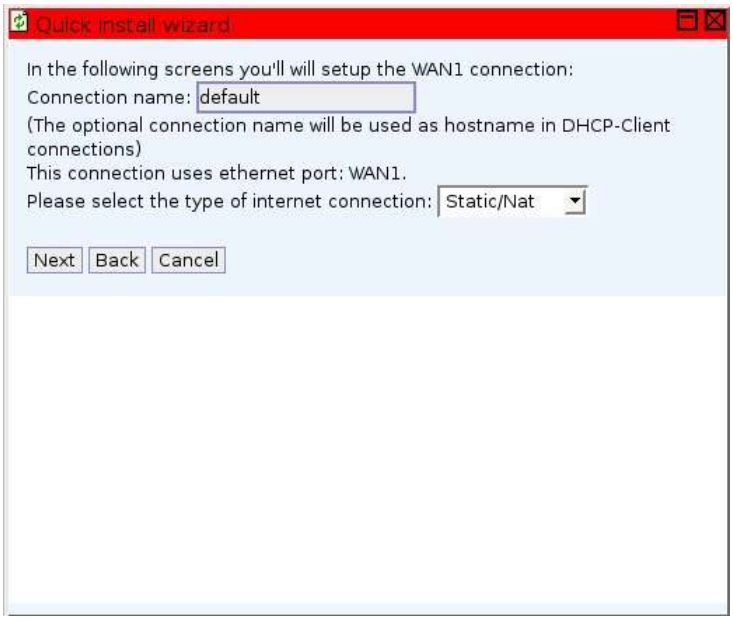
➔ Click “next” to continue



1.6.2 Setting up your default Internet connection

The next step in the wizard is to set up your WAN (Wide Area Network) connections. These are your connections to the Internet. The BaseWall VPN 6000 allows for two WAN connections, one default connection and one fall back. The default connection we name WAN1 (and we will eventually connect the modem or router to the WAN1 network port). The fall back connection we name WAN2 (and like with WAN1, the modem or router for this network connection, if any, will be connected to the WAN2 port).

First we will setup your WAN1 Internet connection.



In this screen we can enter a name for the WAN1 (default) Internet connection. Per default, this name is set to “default”. (WAN2 is named “fall back” per default). Any name can be entered here. You are encouraged to use a descriptive name for the Internet connection. For example “MyISP DSL” or “AOL dial in”. This way, it will be easier to tell two separate Internet connections apart in the future.

➔ Enter a “Connection name” for your default Internet connection.

The type of Internet connection to choose is slightly more complicated. Different types of Internet connections will require different values. As a consequence, the next screen in the “First install” wizard will look slightly different, based on the choice you make here.

If you have an Internet connection by means of an ISDN router or a cable or DSL modem, you will generally be able to choose “DHCP”. Choosing “DHCP” is the easiest possible configuration. Choosing DHCP will allow you to skip the next screen in the “First install” wizard entirely. You do not have to enter any connection details as these can be automatically configured.

However, when you have a routed subnet or a fixed IP address for your Internet connection and have been provided with an IP address, a net mask and a

standard gateway address by your Internet service provider (ISP), please choose “Static/NAT” instead. Be sure to have the connection details provided by your ISP at hand, because you will need these in the next screen.

Some Internet providers may have you authenticate before connecting to the Internet, preferring to use PPTP or PPPoE. If you have such a connection, choose “PPTP/PPPoE”. Like with a Static/NAT connection, setting up a PPTP/PPPoE Internet connection will require connection details provided by your ISP.

When in doubt about the type of Internet connection to choose, please contact your ISP.

➔ Select the type of Internet connection appropriate to your situation.

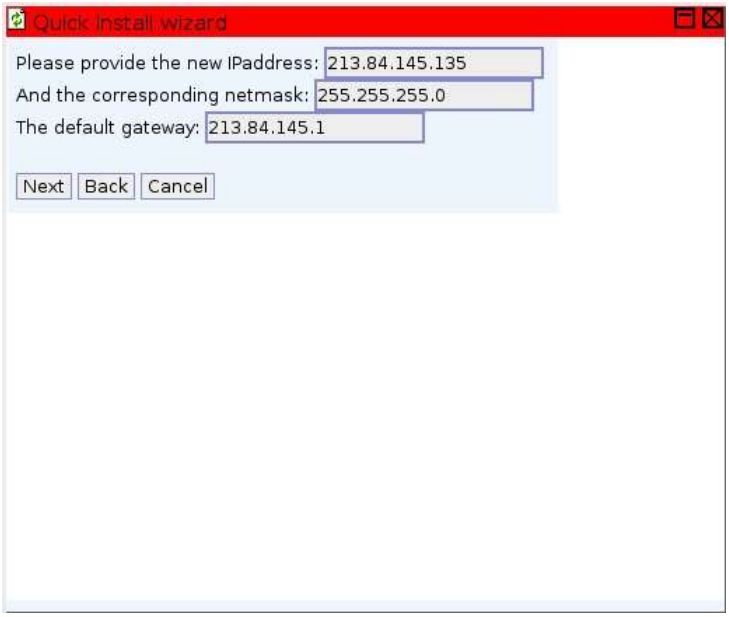
➔ Press “next” to continue.

Setting up WAN1 using DHCP

The easiest way to connect WAN1 to the Internet is using DHCP. Generally, when choosing DHCP, no further settings are required for an Internet connection. After pressing “next” you will directly be offered the opportunity to set up your WAN2 interface (fall back Internet connection).

Setting up WAN1 using a Static/Nat connection

When using a single static IP address or a routed subnet for your network connection, you will have been provided with an IP number, a net mask and a default gateway by your ISP. After choosing “Static/Nat” as type of Internet connection, the next screen will offer the opportunity to enter this data.



➔ Enter the IP address, net mask and gateway address.

If you are in any way unsure about the correct number to enter, please contact your ISP for confirmation.

Setting up WAN1 using a PPTP or PPPoE connection

PPTP or PPPoE Internet connections are not identical, but since both require user authentication, the options to enter are much the same.

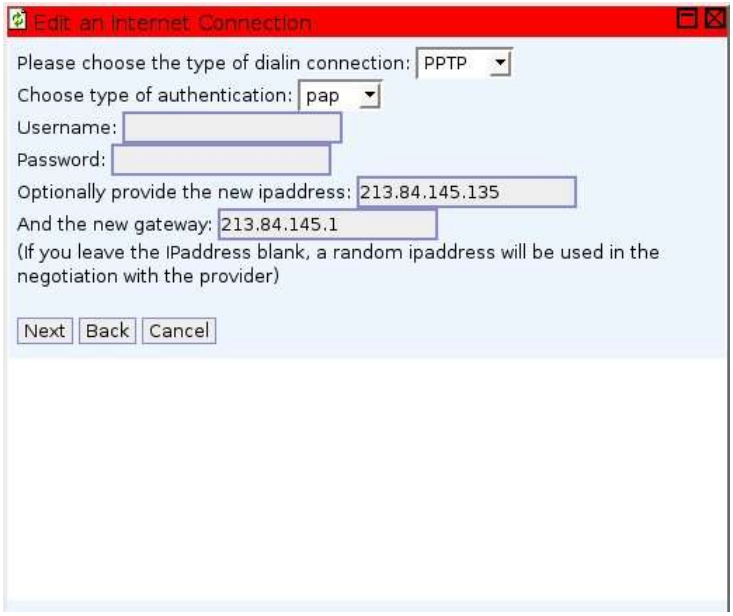
➔ Enter the type of Internet connection (PPTP or PPPoE) after the text “Please choose the type of connection”.

(in the example screen below, we use PPTP. Please remember that this procedure also applies for PPPoE connections).

➔ Enter the user name and password provided by your ISP in the corresponding fields.

If you do not know the correct type of connection, user name and/or password, please contact your ISP for these details.

Some ISP's also require you request a specific IP address of gateway. If such is the case, you can put these values in the *optional* IP address and gateway fields. Most users may simply leave these fields empty.



➔ If required, fill in the “new IP address” and “new gateway” fields

➔ Press “next” to continue.

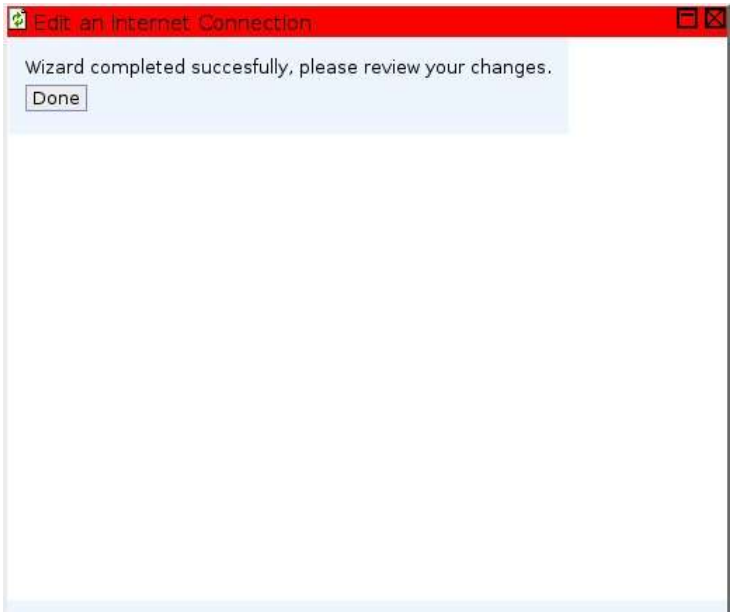
1.6.3 Setting up your fall back Internet connection

Next, you will be asked to set up your fall back Internet connection (WAN2). Setting up a fall back Internet connection is much the same as setting up your default connection (covered in the previous paragraph). Therefore we will not include a detailed description here.

If you do not have a fall back Internet connection, or do not wish to use one, please choose “DHCP” as the type of Internet connection for WAN2. Your firewall will automatically detect the absence of a connection on WAN2 and will not make use of this connection.

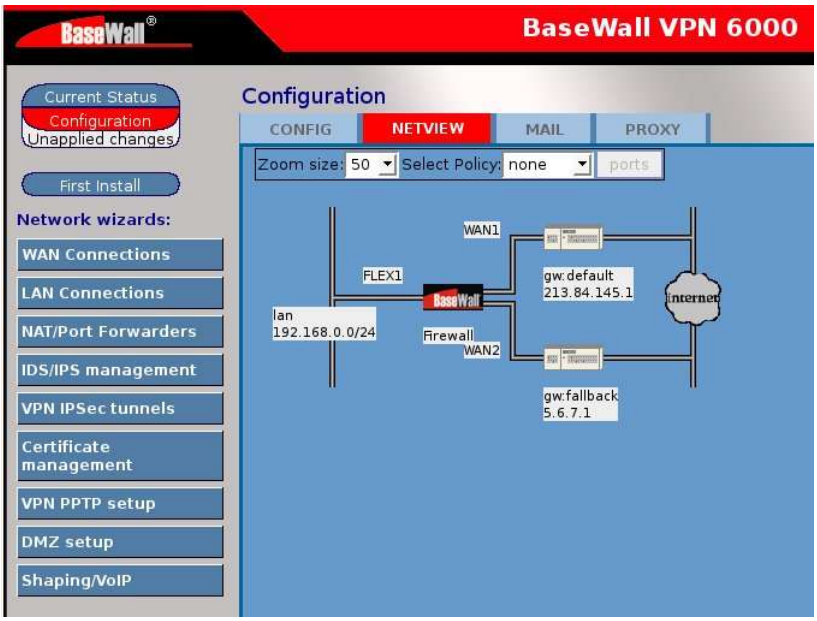
1.6.4 Confirming and applying results

After we have set up our LAN and our default and fall back Internet connections, the “First Install” wizard is done.



➔ In the final confirmation screen, click “done” to close the wizard.

The top left-hand corner of the screen of our firewall's management interface should now show the text “Unapplied changes”. Changes made in the “First install” wizard are only made permanent once you click this text.



Please note that when you do this, your firewall's IP address will probably change. Since the IP address of the firewall will change, the address we used to log in to the management interface will no longer point to the firewall. Hence we will lose our connection to the firewall temporarily. To log in to the

management interface after applying changes, we will need the firewall's new IP address.

➔ Make sure you have the firewall's new IP address (in the local network) written down.

➔ Click “Apply changes”

If you used the “First install” wizard to alter the firewall's IP address on the local network, the we will lose our connection to the firewall after applying changes. The next paragraph deals with re-establishing the connection.

1.6.5 Connecting to the firewall's management interface

After we've applied the changes made in the “First install” wizard, we may loose our connection to the firewall's management interface because (according to the firewall's new local network settings) our PC or notebook is no longer on the same local network as the firewall is. If such is the case, then we have to make a new connection to the firewall before we can proceed.

The first step towards this is to obtain a new network address, which is valid according to the firewall's local network settings. A good way to do this is to reboot the PC or notebook. (Experienced system administrators may opt to renew their machine's DHCP lease instead. Remember to verify the addresses you obtain by this method).

➔ Reboot the PC or notebook

➔ After rebooting the computer, start a web browser.

➔ In the address bar of your web browser, type “https://”, followed by the IP address of the firewall (which you have written down), followed by “:12000”. In our example this would lead to the address https://192.168.0.1:12000. Then press enter.

➔ When prompted for a user name and password, enter “admin” (user name) and “password” (as password), then click “OK”.

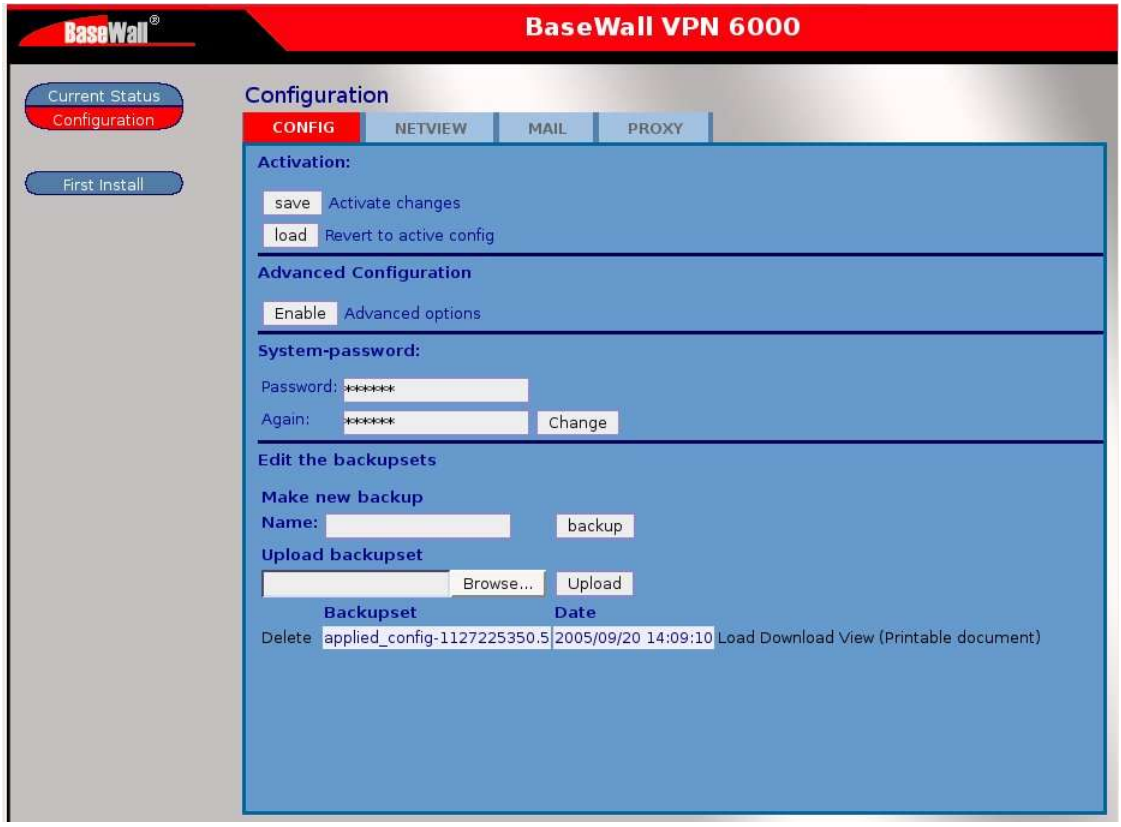
If you get a “timeout”, “not found” or “permission denied” error, please refer to section 1.13 (Errors and recovery).

1.7 Backup sets

The new settings you've just applied have been stored in the firewall as current configuration, but also as a “backup set”. A “backup set” is a snapshot of the BaseWall VPN 6000's configuration in a single file. These backup sets can be uploaded to the firewall, or downloaded from the firewall. Thus it is possible to send or receive an entire firewall configuration in a single file. You can also store a backup set on another computer or backup medium, as a backup of the BaseWall VPN 6000's configuration.

Operations on backup sets are performed in the “Config” tab of the “Configuration” context.

Under the heading “Edit the backup sets” you will find the stored backup sets as well as buttons for possible operations on the backup sets.



At the moment we have one stored backup set (“applied-config-1127225350.5” in the above example). Pressing “Delete” (before the name of the backup set, on the left), will delete the backup set from the firewall's memory. This will not affect the firewall's current settings, but is still inadvisable. On the right hand side of the backup set's name we find the other options, “Load” (which restores the firewall's configuration to the values stored in the backup set), “Download” (which we can use to download a backup set with the firewalls current settings to our computer) and “View” which gives a summary of firewall settings in the selected backup set.

➔ Click “download” to download a copy of the backup set we've just made to your computer.

Whenever you contact support personnel about a problem with your configuration, they may ask you to send a backup set containing your current firewall settings.

1.8 Advanced configuration

The wizards on the firewall are able to handle most of the configuration of the firewall. But when the configuration from the wizards in not enough the advanced configuration can provide access to the underlying rules of the firewall. Chapter 18 till 21 describe the extra options that will become available in the advanced configuration modus.

1.9 Changing the administrator's password

No system can be secure using a factory default password. Before we deploy the BaseWall VPN 6000 in a real network environment we therefore advise you change the administrator's password.

A good administrator's password is at least eight characters long, contains letters (preferably in both upper- and lower case) as well as numbers or non-alphanumeric characters. It can not be found directly in any dictionary but should still be memorable to those in the know.

➔ Think up a good administrator password

It is essential that you not forget this password. You will not be able to manage your firewall without it. It is strongly recommended you file at least one copy of your password (in a sealed envelope) to a safe or to your direct superior.

We change the administrator's password from the “Configuration” context.

➔ Click on the red text “Configuration” on the left hand side of the screen to enter the “Configuration” context.

➔ Activate the “Config” tab by clicking it.

➔ Under the heading “System password”, next to “Password”, enter your new administrator's password.

➔ Enter the same password again one line lower (next to Again:).

➔ Click “change” to change the password.

After changing the administrator's password, your own login (based on the previous administrator password) will also expire. It will therefore be necessary to provide a user name and password again before continuing.

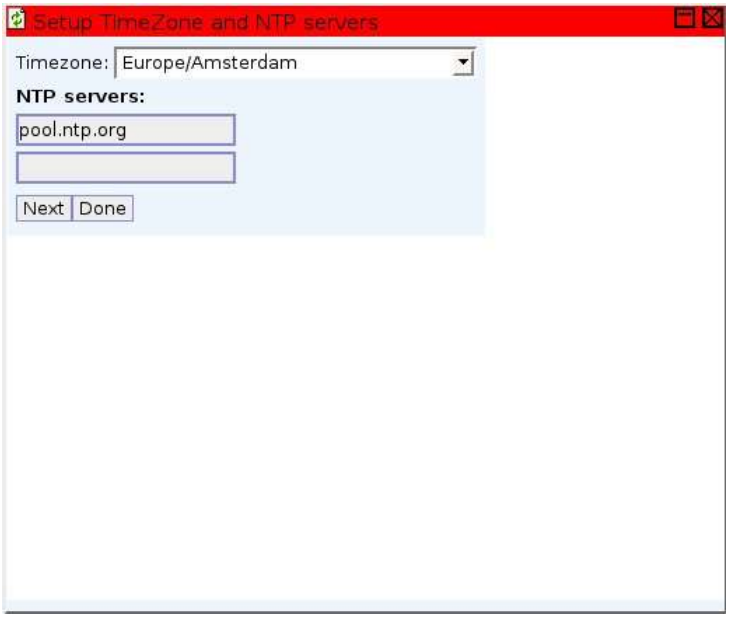
➔ Log in with the user name “admin” and the password you have just entered.

1.10 Setting the firewall's time and date

The configuration of your BaseWall VPN 6000 is not fully complete until you have set the correct time and date. It is customary for computers connected to the Internet to use the network time protocol (NTP) to regularly update their date and time.

- ➔ Click on the red text “Current Status” on the left hand side of the screen to enter the “Current Status” context.
- ➔ Once in the “Current Status” context, find the current time on the left hand side, about half way to the bottom.
- ➔ Press the globe and magic wand icon right of the time indicator

The “Setup TimeZone and NTP servers” window will open.



- ➔ From the “Timezone” menu, choose your timezone.
- ➔ Enter at least one valid NTP server under “NTP servers:” (for example us.pool.ntp.org)
- ➔ Click “next” to continue
- ➔ Click “done” to confirm your changes

Your BaseWall VPN 6000 will now use the Internet connections to keep it's internal clock and calendar synchronized.

1.11 (Optionally) disable the firewall's DHCP server

Per default, the BaseWall VPN 6000 is set to use a DHCP server to automatically configure network addresses of computers in you local network. This could, potentially, cause problems if you have another DHCP server running in your network. Any local network may only contain one DHCP server at a time.

If you wish the BaseWall VPN 6000 to serve as DHCP server, make sure you disable any other DHCP servers in your local network.

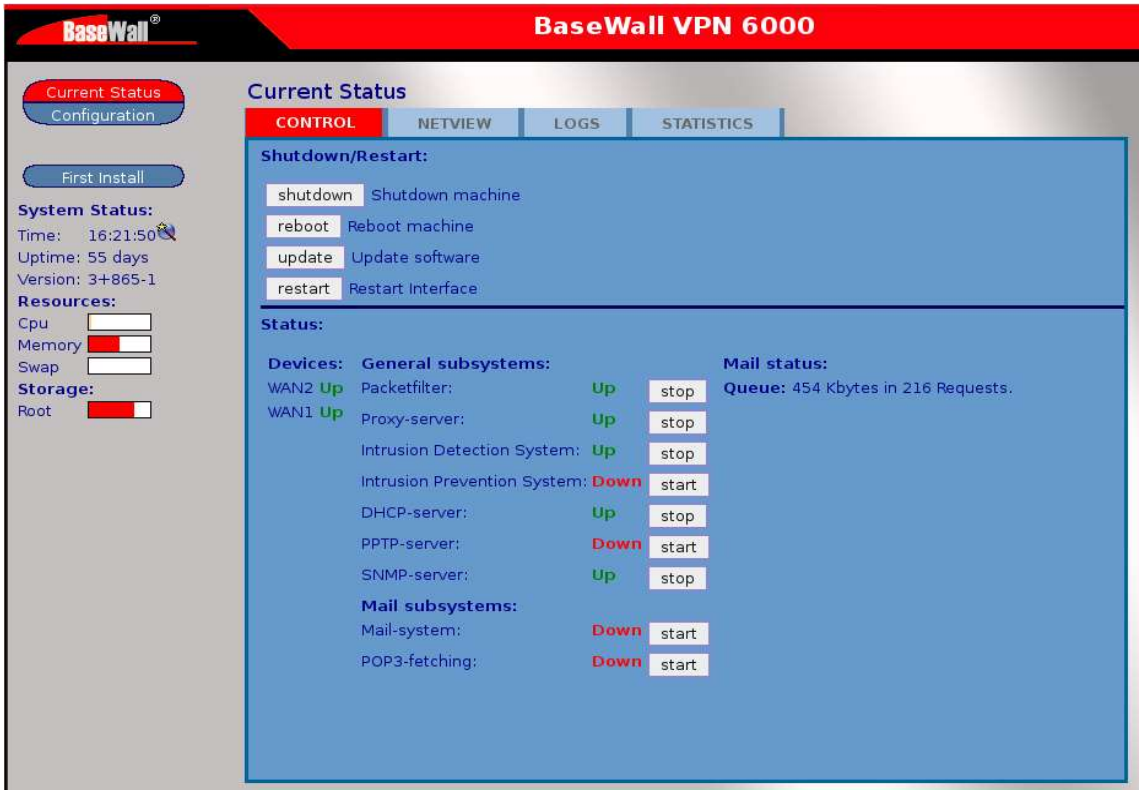
If you wish to keep your existing DHCP server active, we must deactivate the BaseWall VPN 6000's built-in DHCP server before connecting the firewall to your local network.

If you need to disable the BaseWall VPN 6000's built-in DHCP server:

➔ Click on the red text “Current Status” on the left hand side of the screen to enter the “Current Status” context.

➔ Activate the “Control” tab by clicking it once.

➔ In the “Control” page, in the “Subsystems” table, find the line that says “DHCP Server” and click on the corresponding “Stop” button.



1.12 Connecting LAN and WAN cables

Now that we have everything set up correctly, we can perform the final step in the hardware installation of the BaseWall VPN 6000. The firewall is now fully ready to be deployed.

- ➔ Power down the firewall (using the power switch on the back of the device).
- ➔ Power down your notebook or laptop.
- ➔ Detach the network cables from the PC or notebook and the firewall.
- ➔ Using one of the bundled RJ45 UTP cables, connect the WAN1 interface to the router or modem used for your primary (default) Internet connection.
- ➔ If you make use of a secondary (fall back) Internet connection, connect the WAN2 interface to the modem or router used for your secondary (fall back) Internet connection.
- ➔ Using one of the bundled RJ45 UTP cables, connect the FLEX1 interface on the firewall to the switch, router or hub you will use for your local network.
- ➔ Power up the firewall (using the power switch on the back of the device).
- ➔ Check for three beeps to indicate the device has booted up correctly. If you do not hear the three beeps, please refer to section 1.13 (Errors and recovery).
- ➔ Check that WAN1, WAN2 (if in use) and FLEX1 connection LED's (above the corresponding network ports) light up. If one does not, please refer to section 1.13 (Errors and recovery).

1.13 Errors and recovery

Symptom: ***Check/Solution:***

I did not hear three beeps.

Check power cable and insure wall socket has power. Power off the device. Wait 30 seconds. Switch the device on again. If the device fails to beep again the hardware may be at fault. Contact your sales representative for support.

The FLEX1 connection LED doesn't light up when I connect my notebook/PC

Check the cable connection. Make sure you use the network cables bundled with your BaseWall VPN 6000. Verify that both your PC/notebook and your firewall have power and are switched on.

I use an operating system other than Windows 2000/Windows XP/Mac OS X. How am I to enable DHCP on my system?

That information falls outside of the scope of this manual. Please contact your system administrator for support.

DHCP configuration of my system yields the wrong IP Address

If the address you obtain starts with 169.254., or if you get no address at all, then the connection between the firewall and your PC/notebook may be at fault. Check the connection LED for the FLEX1 port to insure that the device is properly connected.

If the address you obtain starts with anything BUT 169.254 then you may have connected you PC or notebook (and probably the firewall too) to an existing network. Please connect the notebook/PC directly to the firewall's FLEX1 port.

My license key is incorrect

Please write down the hard disk serial number mentioned in the “Setup License Keys” dialog and contact your sales representative for a valid license key.

I can't connect to the firewall's management interface

Make sure you have entered the correct address. Initially (before running the “First Install” wizard) this should be https://192.168.99.99:12000.

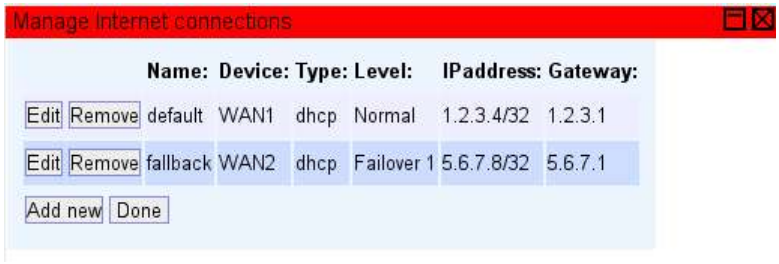
After you've run the first install wizard this should be https://<your_firewall's_ip_address>:12000 (https://192.168.0.1:12000 in our example).

(Where <your_firewall's_ip_address> denotes the new IP address you entered for the firewall).

Make sure your web browser supports HTTPS. If you are unsure about this, upgrade your web browser to the latest stable version.

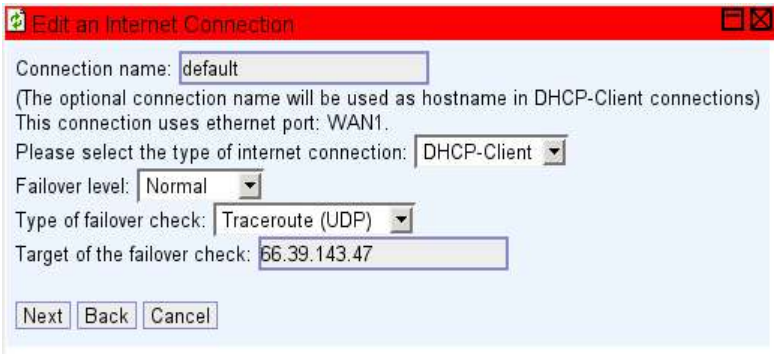
2 Wizard: Internet connections

The wizard “Internet connections” is intended to help you manage your Internet connection settings. With it you can add a new Internet connection or modify an existing one. You can open the wizard “Internet connections” from the firewall's management interface, by entering the “Configuration” context and clicking the text “Internet connections” right below the “Setup subsystems” heading on the left-hand side of the page. This should make the window “Manage Internet Connections” appear.



2.1 Adding an Internet connection

To add a new Internet connection, click the “Add new” button from the “Manage Internet connections” window. The window's title will change to “Setup Internet connection”.



In this screen we can enter a name for the new Internet connection. Any name can be entered here. You are encouraged to use a descriptive name for the Internet connection. For example “MyISP DSL” or “AOL dial in”. This way, it will be easier to tell two separate Internet connections apart in the future.

➔ Enter a “Connection name” for your new Internet connection.

Optionally, we will be able choose an Ethernet port for our new Internet connection. Valid choices for Ethernet ports are “WAN1”, “WAN2” and “FLEX1” through “FLEX4” (corresponding to the Ethernet ports with these labels on the front of your BaseWall VPN 6000).

➔ Select the Ethernet port we will use for this connection.

Determining the type of Internet connection is slightly more complicated.

Different types of Internet connections will require different values to be entered in the next screen of the dialog. As a consequence, the next screen in the dialog will look slightly different, based on the choice you make here.

If you have an Internet connection by means of an ISDN router or a cable or DSL modem, you will generally be able to choose “DHCP-Client”. Choosing “DHCP-Client” is the easiest possible configuration. Choosing DHCP-Client will allow you to skip the next screen in the dialog entirely. You do not have to enter any connection details as these can be automatically configured.

However, when you have a routed subnet or a fixed IP address for your Internet connection and have been provided with an IP address, a net mask and a standard gateway address by your Internet service provider (ISP), please choose “Static/NAT” instead. Be sure to have the connection details provided by your ISP at hand, because you will need these in the next screen.

Some Internet providers may have you authenticate before connecting to the Internet, preferring to use PPTP or PPPoE. If you have such a connection, choose “PPTP/PPPoE”. Like with a Static/NAT connection, setting up a PPTP/PPPoE Internet connection will require connection details provided by your ISP.

When in doubt about the type of Internet connection to choose, please contact your ISP.

➔ Select the type of Internet connection appropriate to your situation.

In normal operation, your firewall will only use one Internet connection at a time. Nevertheless, when this Internet connection fails, it may be necessary to have a secondary connection to fall back on. Your BaseWall VPN 6000 supports up to 4 different backup Internet connections. Whenever an Internet connection fails, operation is taken over by the connection with the next lowest “Failover level”. Your regular Internet connection has failover level “Normal”. This is the lowest “Failover level”. If the connection with “Failover level” “Normal” should fail, operation is taken over by any connection you have with a “Failover level” of “Failover 1”. If this connection should fail, your Internet connection is made using the connection with a “Failover level” of “Failover 2” and so on.

➔ Select your new connection's “Failover level”

Your BaseWall VPN 6000 supports several means of determining whether a connection is operational. All available means involve attempting to connect to a certain host on the Internet. If a connection can be made then the associated Internet connection is operational. If no connection to the host can be made, then the associated Internet connection may be (temporarily) unavailable and your firewall's Internet connection should be made using the connection with the next lowest “Failover level”. Possible types of checking whether to switch to a failover connection include “None” (no check, don't use any failover for this connection), “Ping ICMP”, “Ping UDP”, “Traceroute ICMP” and “Traceroute UDP”. Generally, all of these should yield the same results. Since some firewalled hosts may limit the use of “Ping” or the ICMP protocol we recommend you use “Traceroute UDP”.

➔ Select your new connection's “Type of failover check”

The best way to check if a certain Internet connection is available is try and connect to a machine that is always on. Otherwise our firewall would assume the Internet connection to be unavailable whenever the host we tried to connect to was switched off. The machine we try to connect to should also be located on the other side of our Internet connection. Even with our firewall or our firewall's ISP disconnected from the Internet, connections to a machine in our own LAN or our ISP's internal network would still be possible. The “Target of the failover check” should therefore ideally be a machine located outside of our ISP's network on the actual Internet.

➔ Select your new connection's “Target of the failover check”

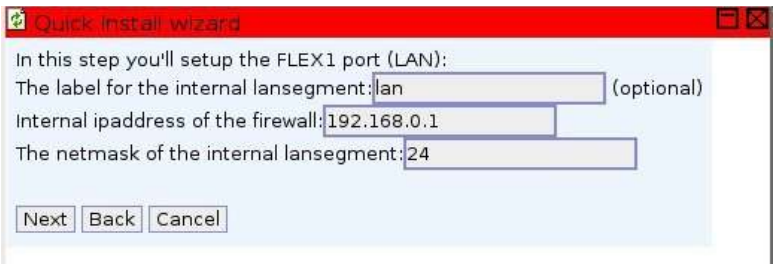
➔ Click the “Next” button to continue.

2.1.1 Setting up a new Internet connection using DHCP

The easiest way to establish the new Internet connection is to use DHCP-Client. Generally, when choosing DHCP-Client, no further settings are required for an Internet connection. After pressing “next” you will be returned to the “Manage Internet connections” screen.

2.1.2 Setting up a new Static/Nat Internet connection

When using a single static IP address or a routed subnet for your network connection, you will have been provided with an IP number, a net mask and a default gateway by your ISP. After choosing “Static/Nat” as type of Internet connection, the next screen will offer the opportunity to enter this data.



➔ Enter the IP address, net mask and gateway address.

➔ Click the “Next” button to return to the “Manage Internet connections” screen.

If you are in any way unsure about the correct number to enter, please contact your ISP for confirmation.

2.1.3Setting a PPTP or PPPoE Internet connection

PPTP or PPPoE Internet connections are not identical, but since both require user authentication, the options to enter are much the same.

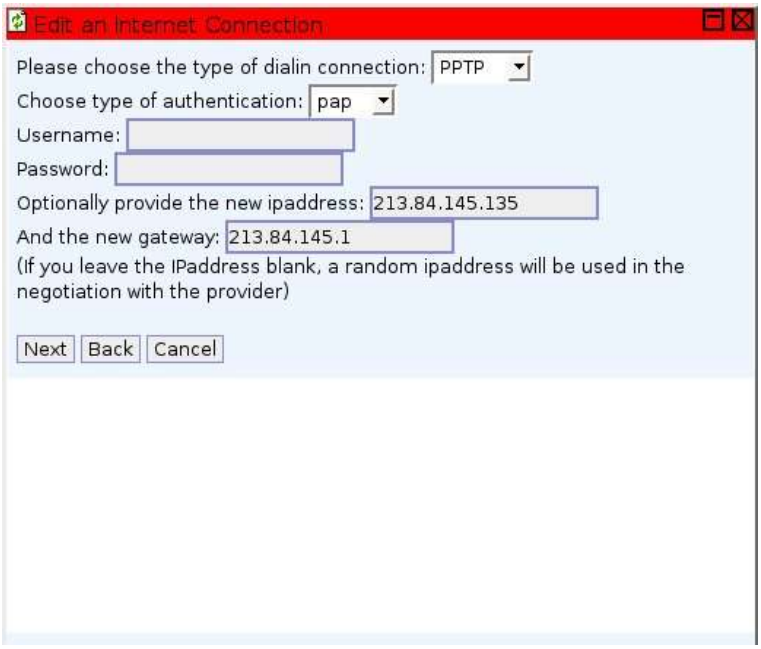
➔ Enter the type of Internet connection (PPTP or PPPoE) after the text “Please choose the type of connection”.

(in the example screen below, we use PPTP. Please remember that this procedure also applies for PPPoE connections).

➔ Enter the user name and password provided by your ISP in the corresponding fields.

If you do not know the correct type of connection, user name and/or password, please contact your ISP for these details.

Some ISP's also require you request a specific IP address of gateway. If such is the case, you can put these values in the *optional* IP address and gateway fields. Most users may simply leave these fields empty.



➔ If required, fill in the “new IP address” and “new gateway” fields.

➔ Click the “Next” button to return to the “Manage Internet connections” screen.

2.2 Editing an existing Internet connection

To edit an existing Internet connection, click the “Edit” button next to the connection in the “Manage Internet connections” screen. The window “Edit an Internet connection” appears. From here on, complete the dialog as if you were adding a new connection (see page 31, Adding an Internet connection).

3 Wizard: Local Area Networks (LAN)

The basic configuration we have reached in the prior chapters of this manual allows for one local network (or LAN). While this may be sufficient in many situations there are a number of possible reasons for segregating local networks (or subnets).

Some departments may have different information needs or working hours from others. Wireless networks may need a tighter security policy than wired networks do. The BaseWall VPN 6000 is equipped with four FLEX ports which can be used for extra Internet connections, extra LAN's or a DMZ at your option.

This chapter covers setting up additional Local Area Networks (or LANs)

3.1 Adding a LAN

To add a Local Area Network (LAN) to your configuration, in the “Configuration” context, click the “Local Area Networks (LAN)” text under the “Setup Subsystems” heading to the left of the screen.

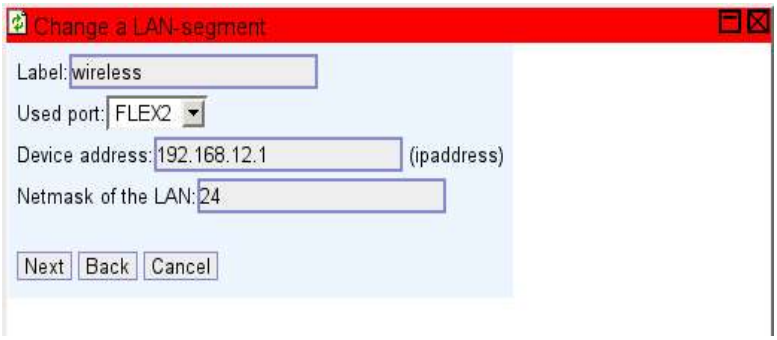
The “Manage LAN-segments” screen will appear. This screen lists the currently configured Local Area Networks. The screenshot below show this screen as it would appear after using the “First install” wizard as described in chapter 1. In the example there we have used the network address 192.168.0.0 with netmask 24 (for an explanation of the meaning and uses of network addresses and netmask, see paragraph 1.6.1, ” Setting up your LAN connection“.

To add a new LAN, lick on the “Add new” button halfway down the window on the left hand side. The window's title will change to “Create new LAN-segment” and you will be prompted to choose a type of local network, either a “Directly connected Lan” (a local network connected to the firewall through one of the FLEX ports) or a “Segmented LAN behind gateway” (a local network not directly connected to one of the FLEX ports, reachable through a segment router).

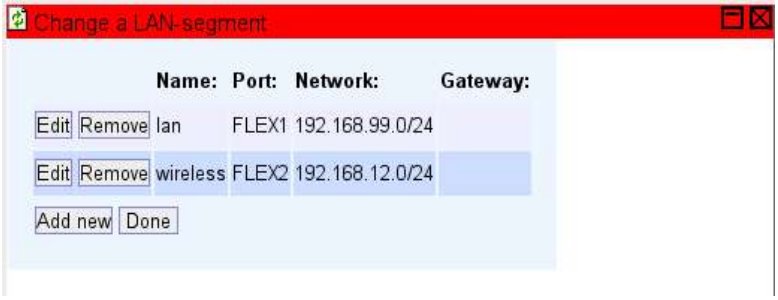
3.1.1 Adding a “Directly Connected Lan”

In this example we choose to add a “Directly connected Lan”. To do this, choose “Directly connected Lan” from the pull down menu and click “Next”. We are then prompted for a label. In the example below, we use the label “wireless” as a convenience since we plan to use this LAN segment for a wireless network. There is no prescribed format for this label. You are encouraged to choose a label describing the LAN you mean to create. Valid examples include department names (“accounting”, “R&D”), network types (“wireless”, “SAN”) or even other features (“floor2”, “meeting rooms”).

You will also be asked to select the network port the Directly Connected Lan will be connected to (FLEX2 in the example) and a device address the firewall will be identified with on this particular LAN. Please note that, since this is a different LAN from the one we created before, it will need it's own, unique network address. The firewall will need it's own unique address on every network it is directly connected to. It is required that the firewall's device address on any LAN is within the valid range of addresses for that LAN. Usually the first address in a LAN is used for the router or firewall (in the example below we choose the address 192.168.12.1).



When you have entered the label, used port, device address and netmask, click “Next” to add this LAN and return to the “Manage LAN-segments” screen.



3.1.2 Adding a “Segmented LAN behind gateway”

Any local network which is not directly connected to the firewall must be reached through some system which *is* a part of an existing local network. (If you must reach a local network through the Internet, this can be done with a VPN tunnel. This is covered in a later chapter). A router or computer on the local network connected to the firewall serves as a gateway to the segmented

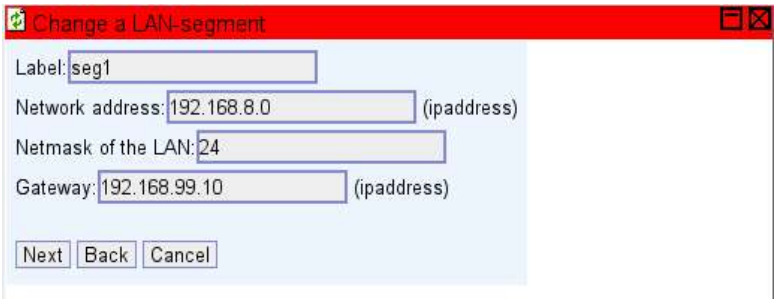
LAN.

To add a “Segmented LAN behind gateway”, in the “Manage LAN segments” window(reached by clicking the “Local Area Networks (LAN)” text under the “Setup Subsystems” heading to the left of the screen in the “Configuration” context), click “Add new”. The “Create new LAN-segment” window appears. For the type of LAN, choose “Segmented LAN behind gateway” and click “Next”.

You are asked to provide a label, a network address, a netmask and a gateway for the segmented LAN. There is no prescribed format for the label. You are encouraged to choose a label describing the segmented LAN or it's purpose. In the below example we use “seg1”.

Like any local network, a segmented LAN has it's own unique network address. For more information on network addresses and their corresponding net masks, see paragraph 1.6.1 “ Setting up your LAN connection“. Enter a network address and a netmask for the segmented LAN. (In the example below we used the network address 192.168.8.0 with the corresponding netmask of 255.255.255.0).

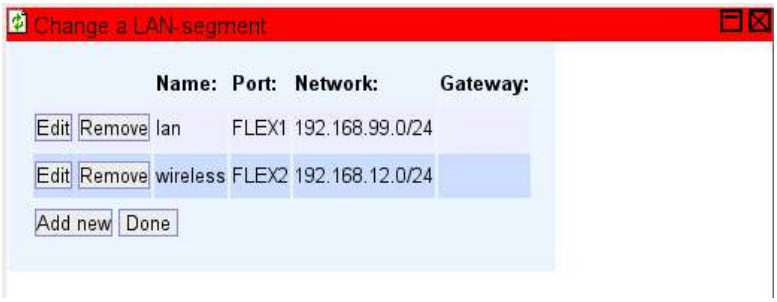
A segmented LAN can be reached through a gateway connected to a LAN connected to the firewall. The address of this gateway machine on the directly connected LAN is the gateway address we need so the firewall will know how to reach the newly defined segmented LAN. Enter the gateway address and click “Next”.



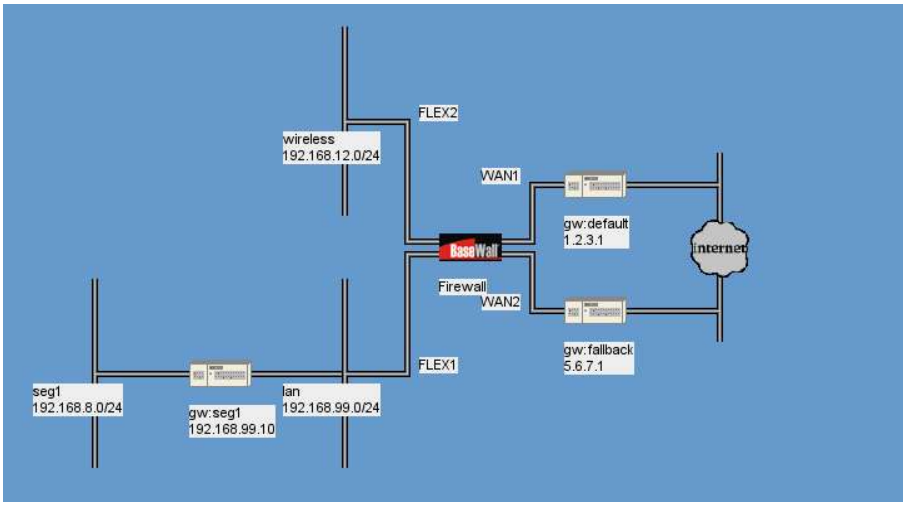
3.2 Modifying or deleting Local Area Networks

To modify an existing LAN (segmented or directly connected), click the “Edit” button left of the LAN's label in the “Manage LAN-segments” screen (reached by clicking the “Local Area Networks (LAN)” text under the “Setup Subsystems” heading to the left of the screen in the “Configuration” context). The steps for modifying a LAN are essentially the same as those for creating a new LAN described in the previous paragraphs.

To delete a LAN, click the “Remove” button left of the LAN's label in the “Manage LAN-segments” screen.



3.3 Viewing the new network layout



4 Wizard: Port forwarders (PNAT)

Most Internet connections will only allow one Internet address (IP address) to be assigned to your firewall. This means that no machine on the internal network (LAN) can be reached directly from the Internet. While this provides some measure of safety to the machines on the internal network, it also effectively prevents these machines from functioning as a server for machines on the Internet. For example any mail-, web- or database servers that you operate on your internal network cannot be reached from the Internet. Hence these machines cannot accept requests or deliveries from machines located on the Internet. In some cases (like the case of a mail server operating on the internal network) this is not the intended behavior. For these cases, port forwarding (PNAT, Port based Network Address Translation) is supported on your BaseWall VPN 6000.

Port forwarding effectively redirects all requests originally sent to a specific Internet address and port of the firewall to a specific port and address on the internal network. This is necessary for every case where a machine or service on the internal network (LAN) must be able to accept connections from the Internet directly. This may be the case for example HTTP (an intranet web server), VoIP (voice over IP) or IP telephony, teleconferencing or peer to peer file transfer software. In the example below we will use the case of HTTP (web-traffic) to a web server on the internal network (LAN).

E-mail delivered to the mail server is offered to the firewall's external Internet address using the TCP protocol on port 80 (which is reserved for HTTP traffic). If the web server on the internal network is to correctly receive this request then all traffic addressed to TCP port 80 of the firewall should be forwarded to TCP port 80 of the internal network's web server. This is what “Port forwarding” (PNAT) is for.

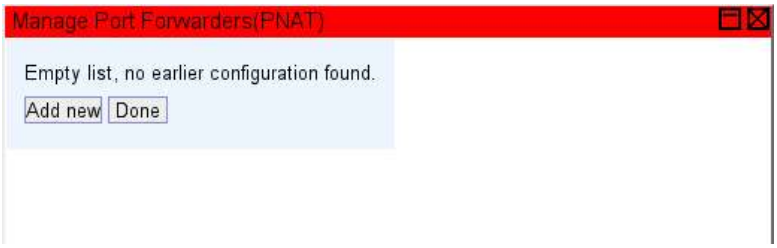
Please bear in mind the fact that, once you have forwarded traffic from any port on the firewall to a machine on the internal network, this machine may be vulnerable to Internet attacks using that specific port. Your firewall cannot entirely protect this system from attacks masquerading as bona-fide Internet traffic. You are advised to run regular system updates and security audits on any machine so exposed to outside influence.

4.1 Managing Port forwarding (PNAT)

To set up port forwarding to a specific machine on your internal network:

➔ Click on the “Port forwarders (PNAT)” text under “Setup subsystems” on the left-hand side of the screen in the “Configuration” context.

The “Manage port forwardings” screen should appear.

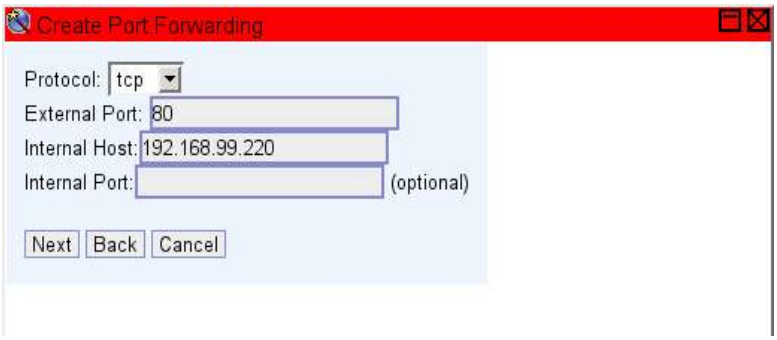


4.2 Adding a port forwarding

To add a port to be forwarded:

➔ Click the “Add new” button in the “Manage Port Forwardings” screen.

The screen should change to the “Create Port Forwarding” view.



As an example we will forward traffic to a web server. Web servers use the HTTP (Hyper Text Transfer Protocol) protocol, on TCP port 80.

➔ Choose the “protocol to forward” (TCP, UDP, TCP/UDP or ICMP). In our example we will use TCP.

➔ Choose the “external port” to forward requests from. This is the port on your firewall that the clients should use to connect to your internal server. In our example we will use port 80 (HTTP).

➔ Choose the “Internal host” to forward the selected port to.

➔ If the port you wish to forward traffic to should differ from the “external port”, enter an “Internal port”. Otherwise leave this field blank.

➔ Press “Next” to confirm.

After adding a port forwarding, the screen will once again change to “Manage Port forwardings” (see above). The newly added port forwarding is added to the list of forwardings displayed.

4.3 Editing a port forwarding

To edit an existing port forwarding:

➔ Open the “Manage port forwardings” screen (as demonstrated in paragraph 4.1 Managing Port forwarding (PNAT)).

➔ Click the “Edit” button next to the line corresponding to the port forwarding you wish to edit.

➔ Modify the forwarding settings as if you created a new forwarding (as described in paragraph 4.2 Adding a port forwarding).

After editing a port forwarding, the screen will once again change to “Manage Port forwardings” (see above).

4.4 Deleting a port forwarding

To remove a port forwarding:

➔ Open the “Manage port forwardings” screen (as demonstrated in paragraph 4.1 Managing Port forwarding (PNAT)).

➔ Click the “Remove” button next to the line corresponding to the port forwarding you wish to delete.

➔ Click “OK” to confirm deletion of the port forwarding.

After deleting a port forwarding, the screen will once again change to “Manage Port forwardings” (see above). The deleted port forwarding should no longer be displayed in the list of forwardings.

5 Wizard: IDS/IPS management

The IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) are two components of vital importance to the security of your BaseWall VPN 6000. Both are enabled by default. The IDS constantly monitors network traffic to- and from your firewall, looking for suspicious network traffic that could be indicative of an (impending) attack. Whenever such suspicious traffic is detected, the IDS will signal the IPS to place the offending Internet host on it's “blacklist”. Hosts on the blacklist are denied access to your firewall and your nternal network. Thus any attacks detected by the IDS are effectively and allmost instantly dealt with. No user intervention is required for this protective feature.

However, a possibility exists that you so often suffer from attacks or misbehaviour from certain hosts on the Internet that you wish to permanently award them a place on your “blacklist” (denying them access to your firewall and internal network). This can be done through the IDS/IPS management wizard.

There is also the theoretical possibility of a host displaying suspicious behaviour which should nevertheless not be blacklisted. External security audits generally qualify as “suspicious” behaviour (from the IDS's point of view) since they often try for known vulnerabilities. In spite of this you may not want to blacklist your IT contact. Whenever a specific host is “allowed” to generate suspicious traffic without the normal repercussion of being awarded a place on the “blacklist”, we place this host on a “whitelist”. Hosts on the “whitelist” are never placed on the “blacklist”, no matter what they do.

5.1 Manage the Intrusion Prevention System

To manage your firewall's IPS:

➔ Click on the “IDS/IPS management” text under “Setup subsystems” on the left-hand side of the screen in the “Configuration” context.

The “Manage the Intrusion Prevention System” screen should appear.

This screen can be used to add hosts (or networks) to the blacklist or whitelist and to remove hosts (or networks) from these lists.

5.2 Adding a host or network to the blacklist

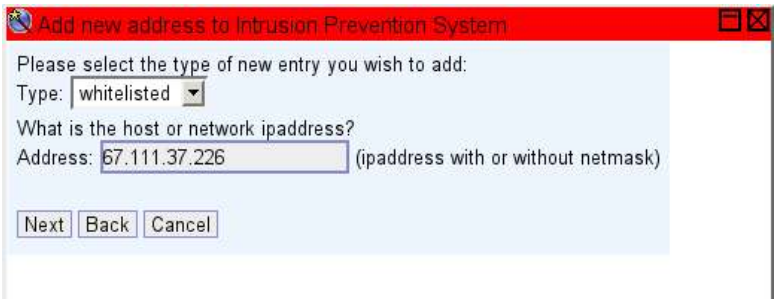
Adding a host or a network to the blacklist effectively prevents any access from the host or network to your firewall and internal network. Adding a host or network to the whitelist instead prevents that host or network from ever being denied access by the IPS (though of coarse other access restrictions my still apply).

To add a host or network to the blacklist or whitelist:

➔ Open the “Manage the Intrusion Prevention System” screen as described in paragraph 5.1 Manage the Intrusion Prevention System.

➔ In the “Manage the Intrusion Prevention System” screen, click the “ Add New” button in the lower left corner of the screen.

The screen will change to the “Add new address to Intrusion Prevention System” view.

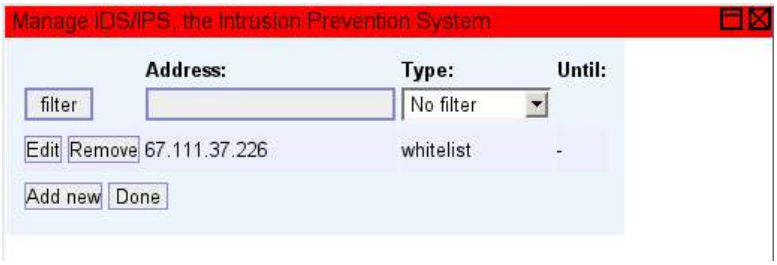


➔ Choose the “Type” of entry to add (“Whitelisted” if you want to add a host or network to the whitelist, “Blacklisted” if you want to add a host or network to the blacklist).

➔ Enter the “Address”. For a single host, this is the host's IP address (in dotted quad format). For a network, this is the network address (in dotted quad format) followed by a slash character (/) and the number of bits in the netmask (between 0 and 32).

➔ Click the “Next” button to continue.

The screen will change to the “Manage the Intrusion Prevention System” view.



5.3 Removing from blacklist or whitelist

To remove a host or network from the blacklist or whitelist:

➔ Open the “Manage the Intrusion Prevention System” screen as described in paragraph 5.1 Manage the Intrusion Prevention System.

➔ Click “Remove” button next to the blacklist or whitelist entry you wish to remove.

6 Wizard: VPN IPSec tunnels

6.1 VPN IPSec tunnels

VPN (Virtual Private Network) IPSec (Internet Protocol Security) tunnels are used to connect two or more LAN's though the Internet in a secure manner. Usually, whenever a company needs to make a common computing or information resource available on multiple locations, a VPN IPSec tunnel is the best solution.

A VPN IPSec tunnel is an encrypted Internet connection between two routers on separate networks. All traffic from one network to the other network is sent over this encrypted connection. This way, other (possibly malignant) Internet users are prevented from reading the encrypted content. Also, other Internet users are prevented from impersonating valid users on any of the local networks (and accessing restricted information in this manner).

Authentication and encryption require that both ends of the tunnel be aware of a common key. Your BaseWall VPN 6000 supports authentication based either on a pre-shared key or on a security certificate.

For a VPN IPSec tunnel to work, both LAN's to be connected do not need to be directly connected to the Internet. However, both will have to have access to a router of firewall that *does* have an active Internet connection. One of these routers will be the BaseWall VPN 6000 we are configuring. The other router or firewall can be any router or firewall that supports VPN IPSec tunnels.

6.2 Managing VPN IPSec tunnels

To manage VPN IPSec tunnels on your firewall:

➔ Click on the “VPN IPSec tunnels” text under “Setup subsystems” on the left-hand side of the screen in the “Configuration” context.

The “List IPSec tunnels” screen should appear.

In the “List IPSec-tunnels screen you have the option of adding, editing or removing IPSec tunnels.

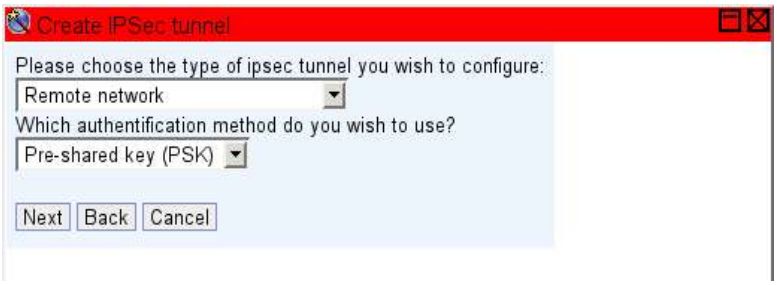
6.3 Adding a VPN IPSec tunnel to a remote network

To add a VPN IPSec tunnel to a remote network:

➔ From the “List IPSec-tunnels” screen, click the “Add new” button.

The “List IPSec-tunnels” screen should change tot the “Create IPSec-tunnel” view.

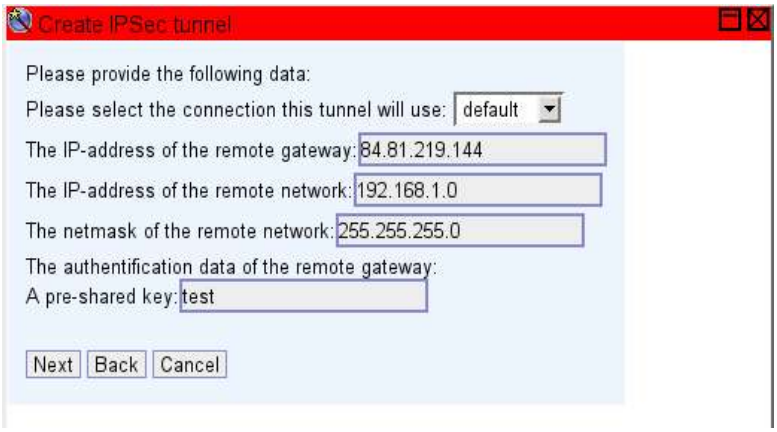
➔ Choose the type of VPN IPSec tunnel you wish to configure. In this example we will connect to a “Remote network”.



➔ Choose the “authentication method” we will use for the VPN IPSec tunnel. (May be either “Pre-shared key (PSK)” or “Certificate” if you have a valid certificate.) In our example we will use a Pre-shared key.

➔ Click the “Next” button.

The “Create IPSec-tunnel” screen will change.



➔ Choose the Internet connection that will be used for this VPN IPSec tunnel (usually your “default” connection).

➔ Enter the Internet IP address of the router or firewall on the other end of the tunnel.

➔ Enter the LAN IP address of the router or firewall on the remote network you wish to connect to.

➔ Enter the net mask of the remote network you wish to connect to.

(Depending on the method of authentication you chose)

➔ Enter a pre-shared key (if you chose to authenticate by means of a pre-shared key like we have in this example).

OR

➔ Enter your certificate's asn1dn subject (if you have chosen to authenticate with a security certificate).

➔ Click the “Next” button.

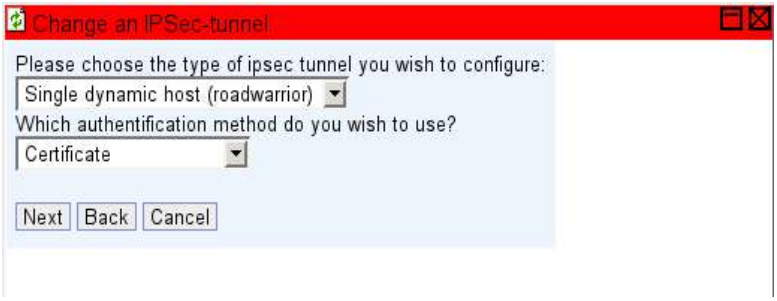
You should be taken back to the “List IPSec-tunnels” view.

6.4 Adding a VPN IPSec tunnel to a single dynamic host

To add a VPN IPSec tunnel to a remote network:

➔ From the “List IPSec-tunnels” screen, click the “Add new” button.

The “List IPSec-tunnels” screen should change tot the “Create IPSec-tunnel” view.

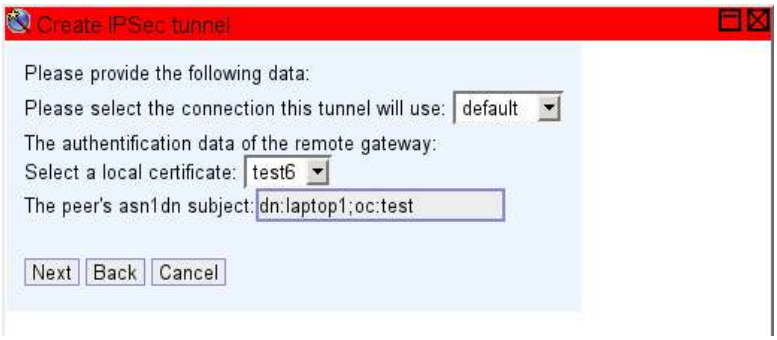


➔ Choose the type of VPN IPSec tunnel you wish to configure. In this example we will connect to a “Single dynamic host (roadwarrior)”.

➔ Choose the “authentication method” we will use for the VPN IPSec tunnel. For security reasons your BaseWall VPN 6000 only supports “Certificate” authentication with “Single dynamic host (roadwarrior)” tunnels.

➔ Click the “Next” button.

➔ The “Create IPSec-tunnel” screen will change.



➔ Choose the Internet connection that will be used for this VPN IPSec tunnel (usually your “default” connection).

➔ Enter your certificate's asn1dn subject (if you have chosen to authenticate with a security certificate).

➔ Click the “Next” button.

You should be taken back to the “List IPSec-tunnels” view.

6.5 Editing a VPN IPSec tunnel

To edit an existing VPN IPSec tunnel:

➔ Open the “List IPSec-tunnels” screen (as demonstrated in paragraph 6.2 Managing VPN IPSec tunnels).

➔ Click the “Edit” button next to the line corresponding to the VPN IPSec tunnel you wish to edit.

➔ Depending on the type of tunnel and authentication, modify the VPN IPSec tunnel settings as if you created a new VPN IPSec tunnel (as described in paragraphs 6.3 Adding a VPN IPSec tunnel to a remote network and 6.4 Adding a VPN IPSec tunnel to a single dynamic host).

After editing VPN IPSec tunnel, the screen will once again change to “List IPSec-tunnels” (see above).

6.6 Deleting a VPN IPSec tunnel

To remove a VPN IPSec tunnel:

➔ Open the “List IPSec-tunnels” screen (as demonstrated in paragraph 6.2 Managing VPN IPSec tunnels).

➔ Click the “Remove” button next to the line corresponding to the VPN IPSec tunnel you wish to delete.

➔ Click “OK” to confirm deletion of the VPN IPSec tunnel.

After deleting a VPN IPSec tunnel, the screen will once again change to “List IPSec-tunnels” (see above). The deleted VPN IPSec tunnel should no longer be displayed in the list of tunnels.

7 Wizard: Certificate management

7.1 Adding Signed Certificate

Add a certificate for the authentification of the firewall in tunnels. Other parties can inspect and check this certificate to be sure that no other machine pretends to be this firewall.

7.2 Adding Certificate Authority

This is an extra Certificate Authority that can sign certificates. There is a standard set of public authorities like VeriSign already in the firewall. Officially signed certificates would normally be automatically validated. But when a certificate from another source in tunnels to this firewall is used the new Authority details should be uploaded here.

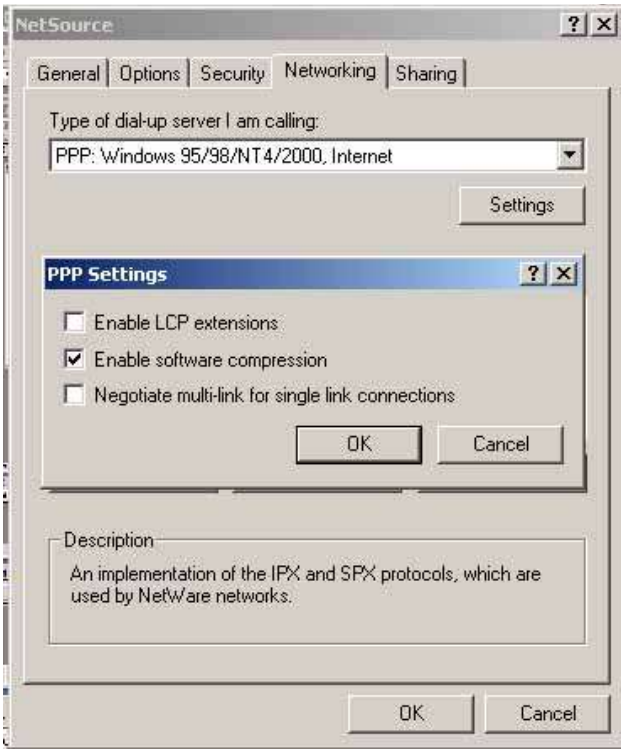
8 Wizard: VPN PPTP/L2TP users

8.1 VPN PPTP/L2TP

Both PPTP and L2TP allow connection to a corporate network by employers. Microsoft Point-to-Point Tunneling Protocol (PPTP) is a revised and more secure implementation of the original PPTP implementation. Layer 2 Tunneling Protocol (L2TP) is an implementation of L2F developed by Cisco in combination with the user authentication available in PPTP.

These protocols allow people to log onto the network with their general user name and password from their home PC or laptop and set up a secure virtual private network (VPN) via the Internet. Computers running Window's XP or Window's 2000 can already connect to both types of networks, older Window PC's only support PPTP and can download free L2TP client software from Microsoft.

Be aware of the fact that the options “LCP extensions”, “software compression” or “Negotiate multi-link” should be turned off. These are patent encumbered extensions on the protocol. And the “optional encryption” option “MS-Chap v2” should be on.



Both these clients can connect to the server once it is configured.

8.2 Setting up PPTP/L2TP

To start using PPTP or L2TP connection's to your network:

➔ Click on the “VPN PPTP/L2TP users” text under “Setup subsystems” on the

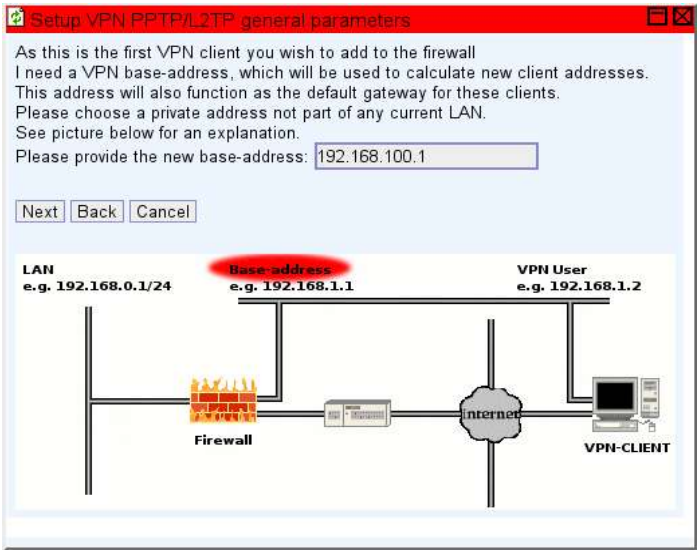
left-hand side of the screen in the “Configuration” context.

The “Setup general VPN parameters” screen should appear.

The client PC's get an extra IP address for this connection. These addresses should not double with any IP range of the internal network's of the firewall or any networks connected to by IPSec tunnels. It is better to choose a base number in the local network ranges like '192.168.100.1' or '10.100.0.1' so this traffic will never by error be routed via the normal Internet connection.

➔ Fill in the base IP address of the VPN users.

➔ Click the “Next” button.



8.3 Managing PPTP/L2TP users

Now it is possible to add user names and passwords for employees to connect to the network.

➔ Click the “Add new” button.

➔ Fill in a user name and a password.

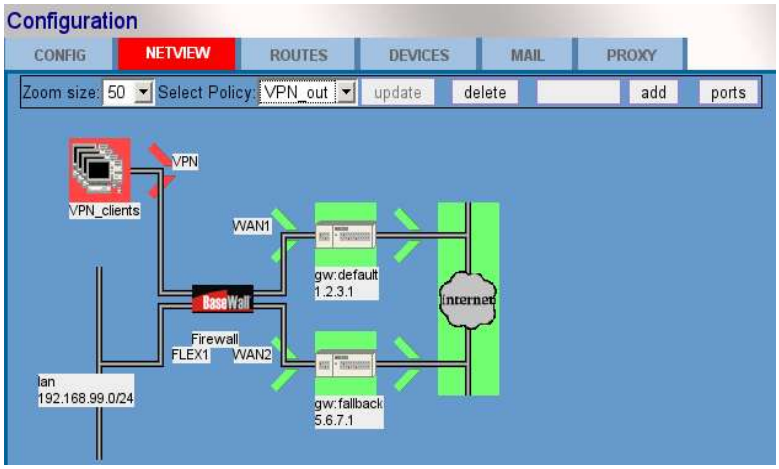
➔ Click the “Next” button.

The first uses is now visible and gets automatically the next IP address higher than the last given address. The base address is used by the BaseWall VPN 6000 side of the connections.

It is possible in this screen to remove users, edit their user name and password again and add extra users.

8.4 Rights of PPTP/L2TP users

The picture in the “Netview” tab is altered to show the new situation. There is now a group of VPN_clients visible. With a right click with the mouse it is possible to show any individual member of this group.



There are 5 more policies added to the policy list.

- “VPN_lan”: rights of the VPN users on the network.
- “lan_VPN”: what does the lan network(s) see from the VPN users.
- “VPN_out”: rights of the VPN users to the Internet.
- “VPN_fw”: firewall services to VPN users like mail boxes.
- “fw_VPN”: traffic originated at the firewall.

These policies are open by default. Add addresses to their port lists to restrict traffic to a specific set of ports.

8.5 Changing the base address

When the network changes in the future and the IP-ranges of the VPN users are possibly doubling another network IP-range it is possible to change the base address with the “Change general PPTP parameters” link. All the current IP-addresses will be changed according to the new base address.

9 Wizard: DMZ setup

9.1 DMZ

A DMZ network layout stands for a virtual Demilitarized Zone. It is used to connect servers to the Internet with a public IP-address and keep them separated from the internal network. When a server gets comprised the internal network is still save behind the firewall. Ideally the servers in the DMZ get no rights to reach the LAN but there are limited rights of the LAN towards the DMZ servers.

The firewall creates a IP-bridge to route all the traffic for DMZ servers directly towards the machines. The IP-address that the servers get on the Internet are directly inputted in the DMZ configuration.

9.2 Create a DMZ segment

➔ Click on the “DMZ setup” text under “Setup subsystems” on the left-hand side of the screen in the “Configuration” context.

One segment can only be connected to a single Internet connection. So with multiple connection enter the connection that should be used.

➔ Choose both the Internet connection and choose a FLEX port as DMZ port on the firewall.

➔ Click the “Next” button.

It is possible from the “Manage DMZ-segments” screen to add extra DMZ's on other ports of the firewall or edit existing DMZ segments.

9.3 Managing DMZ-servers

➔ Click the “Servers” link to access or add servers to a DMZ segment.

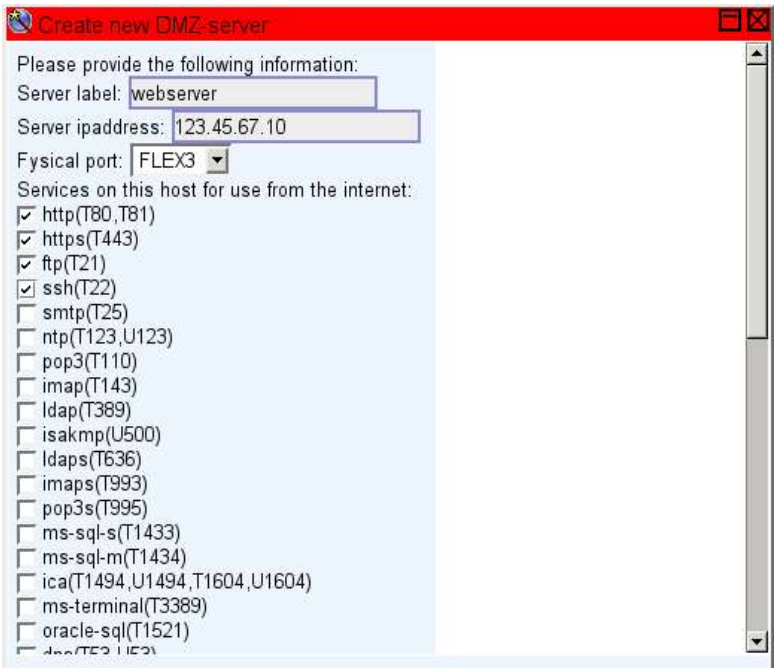
➔ Click the “Add new” button in the “Manage DMZ-servers” screen.

➔ Enter a name as label for the server.

➔ Enter the public IP-address for the server.

➔ Choose the protocols that the server needs to provide for both the Internet and the internal network(s).

➔ Click the “Next” button.



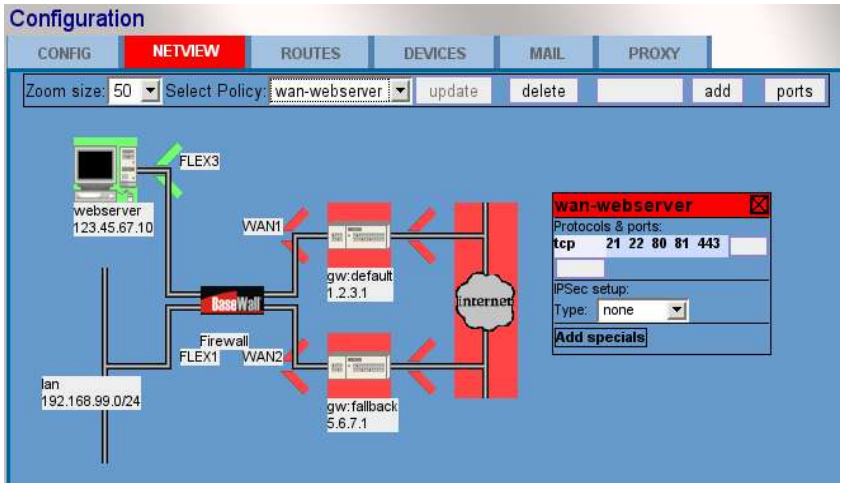
It is possible from the “Manage DMZ-servers” to remove the servers again or edit existing servers.

9.4 Netview picture of DMZ servers

DMZ servers are directly visible from the Internet. There are 3 new policies created for a DMZ server:

- wan-DMZ_server: contains the possible services towards the Internet
- DMZ_server-wan: connections from the DMZ servers on the Internet, initially not restricted.
- lan-DMZ_server: contains possible services towards the internal networks.

The first and the last policy are initially filled and can be edited by the “DMZ setup”wizard. But the choice of services is limited to a common used set. Via the Netview it is possible to allow all other kinds of services of the DMZ servers.



10 Wizard: Shaping/VoIP

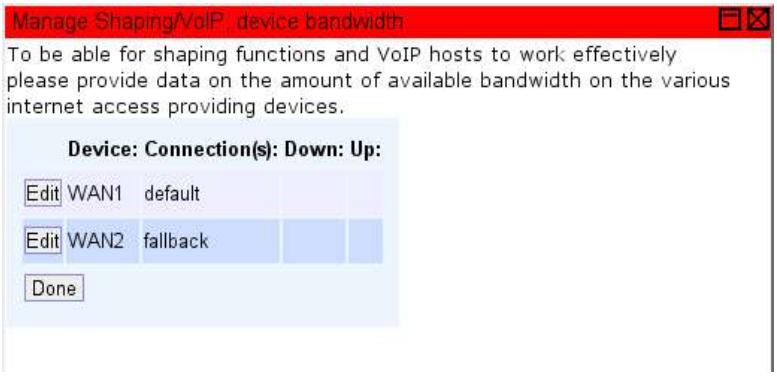
10.1 Shaping

The VPN 6000 can divide the Internet traffic in separate parts. For Voice over IP it is necessary to separate the different computers that use VoIP from the rest of the traffic. It is then possible to reserve some traffic for these computers so that other traffic for example big download cannot block the small but steady stream of voice packages.

When reserved bandwidth isn't completely used the rest becomes available for the other traffic.

10.2 Bandwidth

Most ISP use a simple mechanism to limit the bandwidth use of their customers. When the upload or download stream reaches a limit the total traffic is blocked. So a big download often blocks the sending of packages. It now becomes vital for the shaping to know the limits set by the ISP so it will always limit traffic before the ISP blocks everything. On entering the Shaping/VoIP wizard it checks the shaping statistics on the Internet devices. When there is no bandwidth information known it will ask for it before the VoIP computers can be identified.

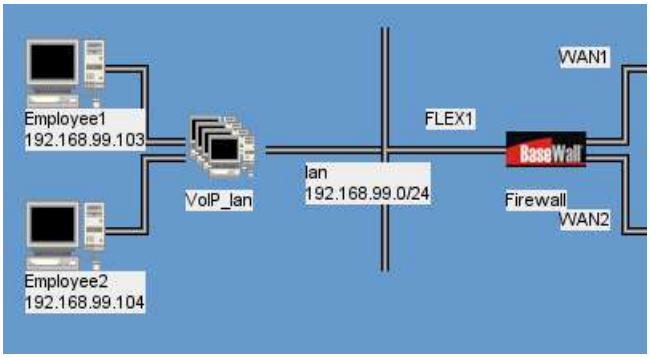


10.3 Hosts

The different IP addresses of the computers with VoIP should be known. All those computer gets a reservation of 3% of the bandwidth. Voice traffic doesn't need much bandwidth but it is very sensitive for delays.

10.4 The Netview

The computers with VoIP bandwidth reserved for them get their own group inside the “Netview”. Normally the computers are invisible but can be made visible by clicking on the group and select “Show subparts”.



11 E-mail

Normally the firewall is configured to accept all email send to one or more mail domains. This domain is the name behind the '@' of an email address. Every mail is accepted, checked and send on towards an internal mail server.

Email send from outside the firewall for unknown domains are automatically dropped and an error notice is send back to the origin of the email.

11.1 First mail domain

Click on the “Mail” tab when in the configuration part of the interface.

➔ Enter the complete host name of the firewall.

De part after the first dot is automatically used as the primary mail domain. Mail that is generated by the firewall due to found email viruses or unwanted email is send with this name as sender.

➔ Enter the DNS host name of the firewall. Often identical to the host name.

Some mail servers are very strict on identification. These servers require the firewall to introduce itself with the exact host name as the (reverse) DNS-record that points to the firewall. This field should be an exact copy of the DNS entry of the firewall.

➔ Enter the IP-address of the mail server of the ISP into the “SMTP/Relay host” field.

This field can be left empty, then the DNS system of the Internet is used to deliver email directly to the recipients system.

➔ Enter the IP-address of the internal mail server into the “Transport mapping” field.

When using the build-in POP3 server, the transport-mapping should be empty or 'local'.

11.2 Administrator mailbox

When dealing with email for a corporation someone should monitor the state of the email system. This task should be given to a person who will be called Postmaster. Whenever an email is dropped or delayed this person will be notified of the occurrence. The postmaster can act on communication problems this way.

It is vitally important that this person has a working, reachable email address. The aliases in the mail screen are both important and dangerous. If they are incorrectly configured there is a large change the mail system runs into problems, like mail loops and/or the loosing of email.

Enter the complete email address of the administrator into the “Root: (system mail)” field. Again: it's important that this email address is reachable and valid.

The other aliases are provided to split the system mail up to several accounts. When this is not wished for, you may leave them on "root", effectively forwarding the mail to the system administrator.

The following sources of system mail are handled by the firewall:

- Postmaster: Basic mail-subsystem notifications. Notifications like overflowing mail boxes or long delivery delays.
- Virus-warning: Notification of blocked mail due to virus content.
- Spam-warning: Notification of blocked mail due to spam content.
- Virus-quarantine: (Optional) This account will receive a copy of the blocked mail, still containing the virus. **Handle with CARE!**
- Spam-quarantine: (Optional) This account will receive a copy of the blocked spam mail.

The warnings about spam (unsolicited e-mail) and viruses can be send in intervals to prevent huge amounts of messages.

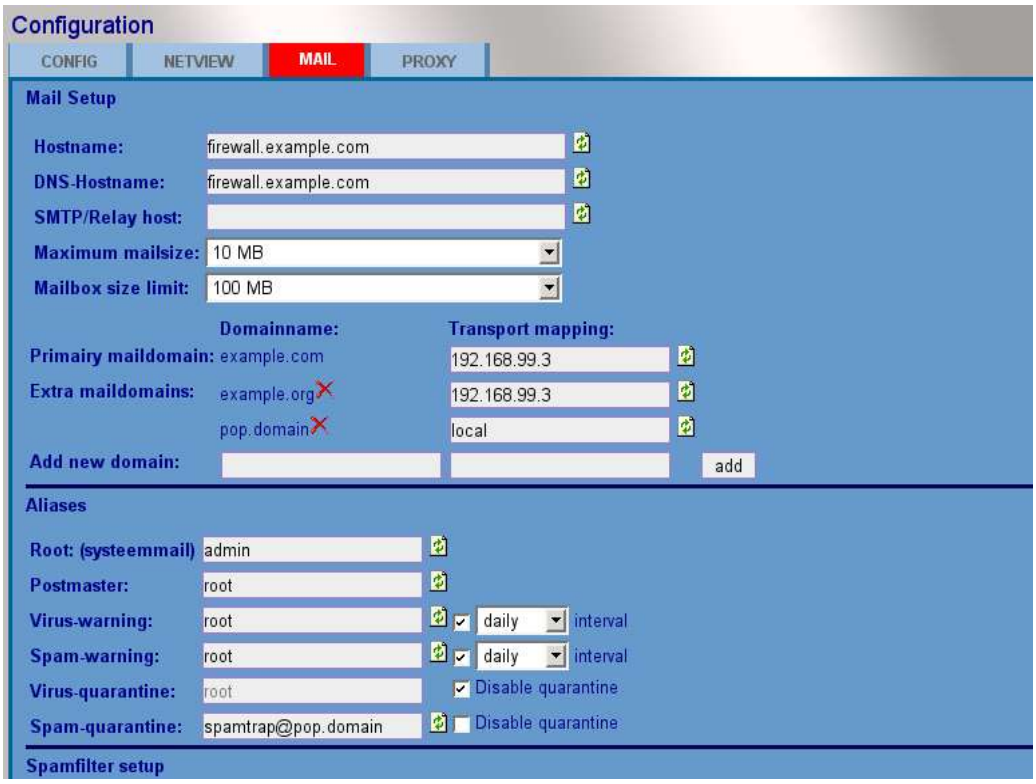
11.3 Secondary mail domains

It is possible to allow email from multiple domains to the firewall. These extra domains can write into the same mailboxes as the primary domain or send the email to a different mail server.

➔ Write the mail domain in the “Add new domain” field.

➔ Write the server name in the corresponding “Transport mapping” field.

It is possible to fill the transport mapping field with “local” to deliver the mail to the internal pop3 mail server of the firewall.



11.4 White and blacklists

Enter an email address or an email domain name into the “Whitelist” field to guarantee the delivery of all email from this source. The spam filter is bypassed for these account.

The field “Blacklist” can be used to block all mail from a source. This is an effective way to block a mail bomb of spam or virus email or a mail loop from a specific address. Mail loops can occur when for example a service of Internet replies to a simple automatic reply as out of office messages.

11.5 Reading external mail boxes

The firewall can be used to read external pop boxes and check the mail before sending it to the internal mail server or make them available to other pop boxes.

➔ Write the pop server name or IP address in the “POP-server” field.

Side note: This field should not be filled with the Host name of the firewall on top of the page.

➔ Write the user name of the mail box into the “Username” field.

➔ Enter the password of the mail box into the “Password” field.

➔ Set the correct domain to deliver the mail to.

When that delivery domain is entered with “local” in the “transport mapping” then the mail is written again to User mail boxes.

11.6 User mail boxes

To let users read from mail boxes on the firewall.

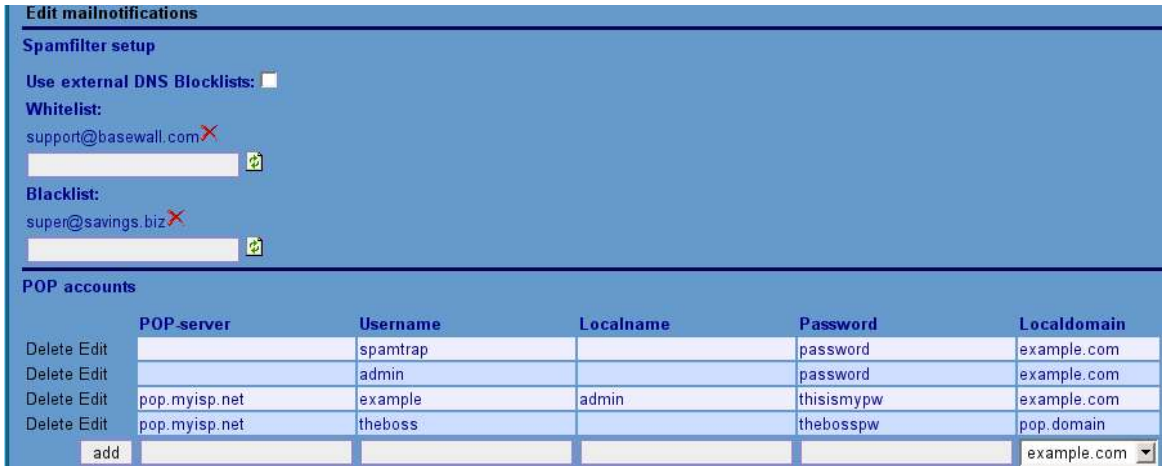
➔ Write the user name in the “Localname” field.

➔ Fill the password into the “Password” field.

When the “POP-server” and “Username” fields are also filled the password internally and externally are the same.

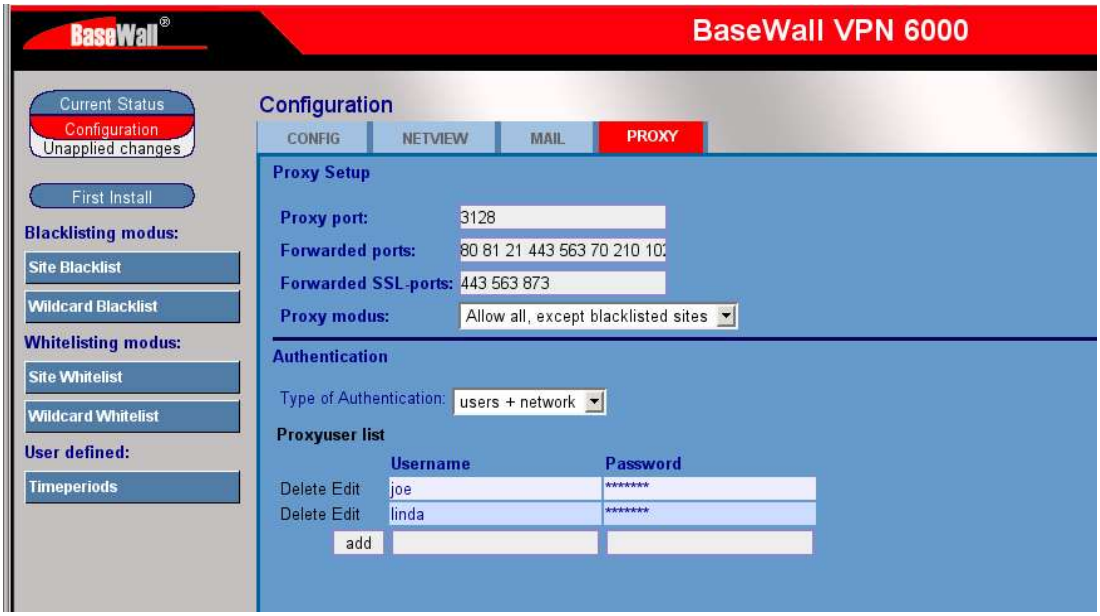
The mailboxes have a size limit set with the “Mailbox size limit” field near the top of the page. This should be a couple of times higher than the “Maximum mailsize” limit. Otherwise the mail system could get stuck with a email that can't be delivered or send to the postmaster. This can hamper the overall working of the mail system.

When mailboxes are first created but didn't receive any mail yet the firewall will show a message “No valid/Maildir found!”. The mailbox is automatically created after the first email for the box is received.



12 HTTP Proxy

The proxy settings are found in the “Proxy” tab in the “Configuration” part of the firewall. The proxy can be used to lower the amount of traffic used by browsing the web. Normally first the “lan-out” policy should be modified to prevent the use of 'http' (port 80) and 'https' (port 143).



The browsers proxy configuration should point to the proxy port and the internal address of the firewall. It is possible to define the used proxy port. The default port is 3128, another common used port is 8080.

The different ports that the proxy caches are listed.

It's possible to deny all site outside the whitelisted sites. The wizard buttons to the left of the screen give access to the current white and blacklisted sites.

Normally all PC's on the internal networks are allowed to use the proxy server on the firewall. This is the “network” method of the “Authentication” field.

When set to “users+network” there should be given a set of user names and passwords on this screen.

13 Netview

The Netview is the central screen of the BaseWall VPN 6000. It shows all the networks and computers that the firewall knows something about. From this screen it is possible to view and change the rights of all these parts on other parts of this virtual “world”.

13.1 Policies

After selecting a policy. Some parts of the network will change color.

- Red: This is the source of the policy.
- Green: This is the destination of the policy.
- Orange: This is both source and destination of the policy.

A policy handles the traffic initiated by the red part of the network towards the green part. This is a service of the Green part towards the network. But some services like a file share on a normal PC are not intended for everybody.

Some policies can span multiple parts of the network like multiple LAN segments and the Internet. This can reduce the number of necessary policies needed to allow traffic to multiple parts of the network.

When there is no policy all traffic through the firewall is blocked. But there can still be traffic through a connection made from the other side. The connection track software makes it possible to identify an established connection so there is no need for any rights of the Internet on the LAN but the LAN can still receive requested web-pages.

13.2 Adding or removing ports

First select the policy of interest. This can be done in a couple of ways:

- Select the correct name in the drop-down menu on top of the page. Then click on the “ports” button.
- Click on a network or host and a menu will open. It shows in sub menu's the policies that affect traffic originated “from” or requested “to” this part of the network.
- Open the “Policy info” screen in the same menu and click on the policy names there.

Inside the newly opened “Protocols & ports” screen is an overview of protocols and ports that currently are allowed (or sometimes explicitly denied ports) by this policy.

To add a protocol insert it's name or protocol number into the field under the possible existing protocols.

To remove a protocol and deny traffic by this policy click on the protocol name twice, it will first show red to prevent unintended deletions.

Add port numbers behind “tcp”, “upd” or “icmp” protocols restricts traffic to only the listed ports. Other protocols don't use ports. When the ports list is

blank every port is allowed. Allowing ports in specific policies add to rights in more general policies. So when a tunnel is created across the Internet. The network behind this tunnel gains the normal rights of the Internet but normally will have more rights.

Ports are deleted the same way as protocols.

When a port is preceded with a “!” sign this port is restricted. With only restricted ports the rest of the ports are still free to use. It is possible for a more specific policy to deny a port that was allowed by a more general policy.

13.3 Adding or removing port ranges

It is possible to open ranges of ports. Some tcp protocols use a range of ports for multiple tasks. To prevent the input of all the subsequent numbers you can enter the lowest port a colon-sign (':') and the highest port to indicate a range.

13.4 Policy overview of a network or host

When clicking with the mouse on a network or host the “Policy info” can be selected. This window is divided in two parts. First all the policies are listed that show the rights of this part of the network in Red. The second half shows the rights of the rest of the network on this part.

First the most general policies are listed and then more specific policies. From the policies the allowed protocol and ports are shown like in the “Protocols & ports” window of that policy.

13.5 Block a host or network

In the menu that opens with clicking on a host or network is also the option “Disable route”. With this option the traffic from and to a specific route can quickly be stopped. This can be used to stop large data streams from parts of the network. But normally a better solution should be sought for network rights.

13.6 IPSec authentication

When clicking with the mouse on a network or host on the other side of the Internet the “IPSec authentication” option can be selected. The following options can be set.

- No IPSec: The traffic from and to this part doesn't need to be encrypted.
- Certificate: The traffic is encrypted and a certificate is used as authorization.

You need to fill in the “Distinguished name” of the other party here. This is part of any certificate.

- Pre shared key: The traffic is encrypted and a shared key is used as authorization.

The rest of the IPSec options are shown in the next Chapter (14 IPSec configuration).

13.7 Road warrior(s) authentication

When clicking with the mouse on the Internet cloud the “Roadwarrior's Auth.” option can be selected.

Roadwarriors are PC's that use IPSec tunnels to connect to the firewall. But it is unknown what IP-address they will use and they can switch to different IP-addresses en reconnect.

The first option can be used to select a certificate to use for the connections to Roadwarriors. These certificates can be set with the “Certificate management” wizard.

There are 2 authentication methods possible for Road worriers:

- The Asn1dn Subject of their certificates. This is the complete “Distinguished name's” of their certificate.
- The Email address that was put into the alternative name of the certificate. This is often shorter that the Asn1dn name.

All the identifiers of Road Warriors that are allowed to connect to the firewall should be entered here.

The rest of the IPSec options for the Road Warriors are the same as for normal tunnels and are handled in the next chapter.

14 IPSec configuration

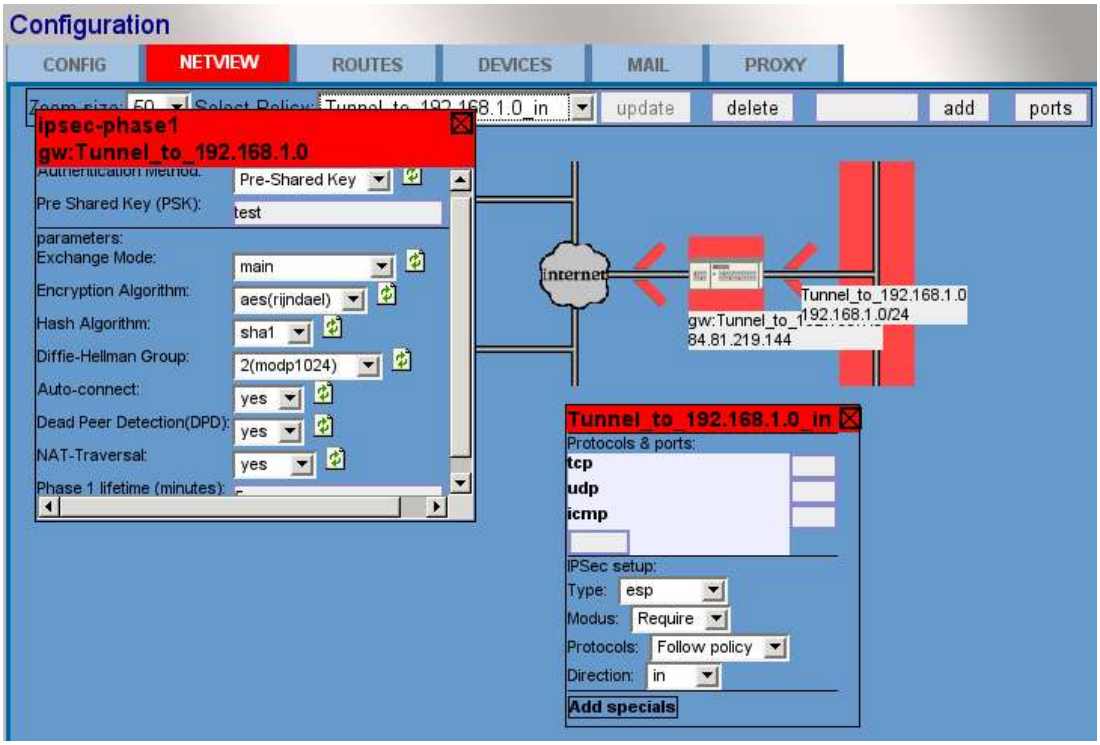
14.1 Identification options

After running the IPSec wizard and after the apply of the configuration the firewall will start the IPSec tunnels when there is traffic towards the remote network or when the remote network tries to connect the tunnel.

The tunnels are configured with sane defaults so in a lot of cases the normal configuration will just work. When there are problems with the tunnels there are several parameters that can alter the way IPSec behaves.

Click on the tunnel gateway computer and select the “IPSec Authentification” option to open the first related screen.

Select the ports on the IPSec policy for the remaining options.



14.2 IPSec options

- ➔ Exchange mode: main or aggressive key exchange, some implementations of IPSec need this option but aggressive is less secure than the default.
- ➔ Encryption Algorithm: aes is the world standard but sometimes others are required.
- ➔ Hash Algorithm: md5 is somewhat older and less secure.
- ➔ Diffie-Hellman Group: need to be the same value as the other side of the IPSec tunnel.
- ➔ Auto-connect: off when the other side should allways op the tunnels

- ➔ Dead peer detection: when the tunnel is not connecting directly the dead peer detection closes the tunnel and tries to connect again. This can give less connectivity when the other side doesn't react right.
- ➔ NAT Traversal: when the tunnel is behind a NAT connection the software detects this and tries to compensate for it. With 'force' it will always assume that it is behind a NAT. This firewall uses the rfc3947 definition.
- ➔ Lifetime: when will the software exchange new keys for the tunnel.

14.3 Policy options

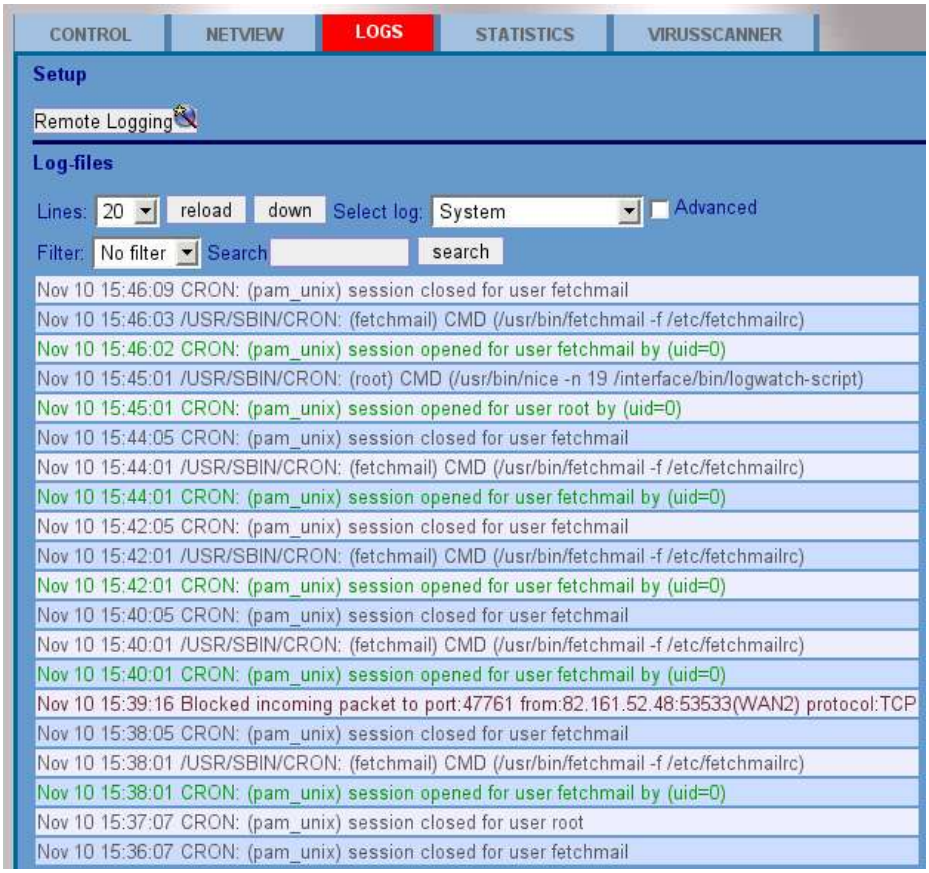
- ➔ Type: the AH is somewhat more secure but NAT Traversal won't work in combination with AH. Only AH without esp doesn't encrypt the data.
- ➔ Modus: when multiple tunnels are defined behind the same host the same keys can be used for those tunnels. Specifically Cisco routers need unique keys for these tunnels.
- ➔ Protocols: set it to any when the other IPSec implementation doesn't know to handle the different protocols.
- ➔ Direction: the traffic allowed in this policy is (in/out/both) of the tunnel.

15 Logs

Select the logs tab to inspect the different logs of the system. Click on “reload” to get fresh data on the screen, sometimes the logs will grow rather quickly.

Push the “down” button to move to the next screen of `older` log messages.

Enter a search term and push the “search” button to find a specific word or phrase in the logs.



There are several different log files on the system:

- System

  Packet blocks, general errors, startup messages of programs.

  Filters:

  PPP – show only internet connection status messages

  DNS – show only internet name request related messages.

- Mail

  Incoming mail, virus checks and sending to mail servers.

  Filters:

  Mail – only show mail handling messages.

  POP-Fetching – show only retrieving mail from external pop boxes.

POP-server – show only the sending from internal defined pop boxes.

- Intrusion Detection

  Show the network security messages.

- IPSec key manager

  Show the securty key exchange of the defined IPSec tunnels.

- Proxyaccess

  Internet questions from internal PC's to the proxy.

- Proxycache

  General squid messages.

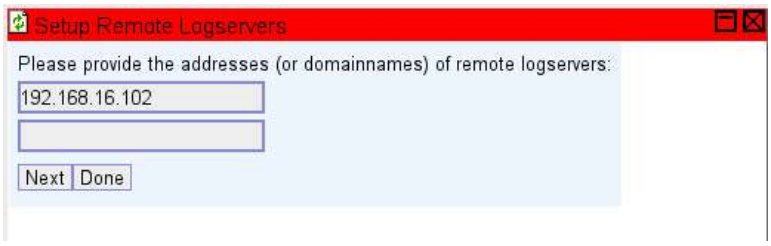
- Proxystore

  State information of the proxy cache.

The logging system supresses some less relevant messages and sometimes shows more readable messages. With the advanced button set to on all messages will be shown without any modification.

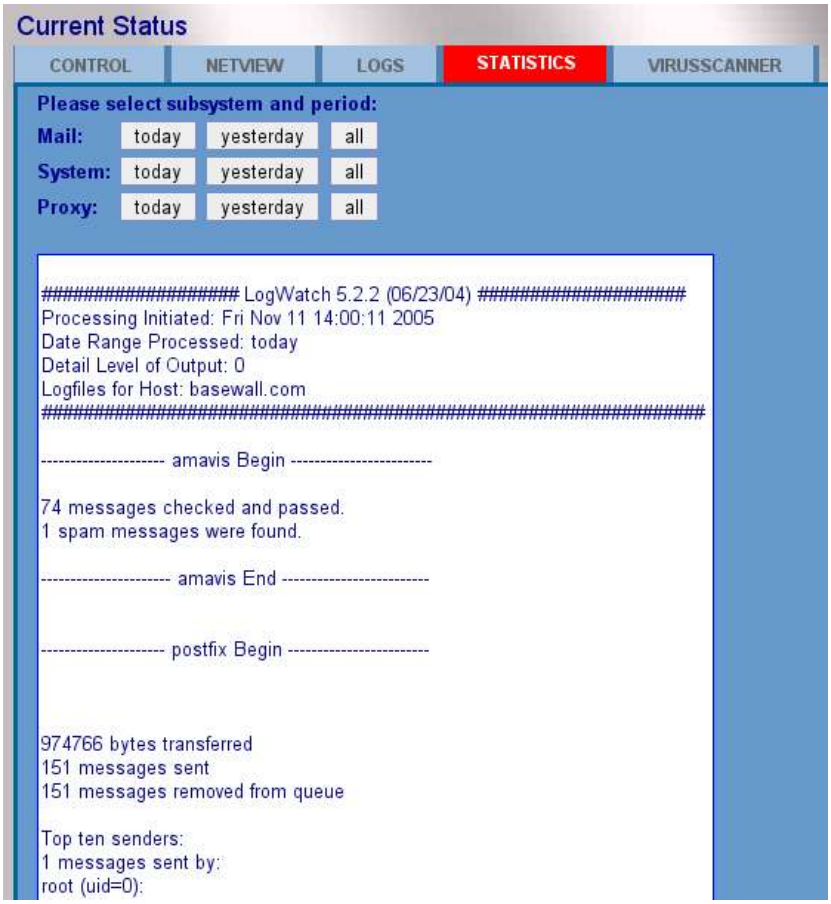
15.1 External logging

Enter an ip-address of a computer where the logs should be send. The information in the logs contains technical information about the firewall and the network behind it and private information about email received and send from the network. So it is vital to build a tunnel to send this information encrypted when it is send to a computer outside the internal network.



16 Statistics

This page shows an analysis of the logs on this machine.

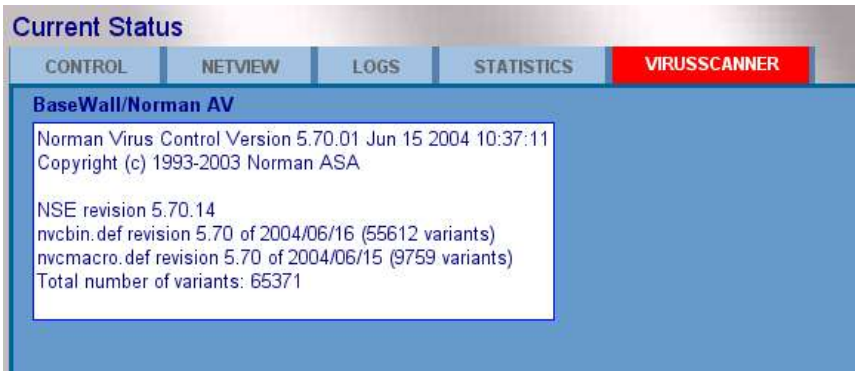


This contains totals and rules out the normal messages. The “all” time shows the logs for roughly a month.

17 Virusscanner status

This is a tab that shows the status of the anti-virus software running on the firewall. It is very important that the latest virus data is loaded and every hour the firewall should update to the latest definitions. When the version of the anti-virus software loaded on the firewall gets too old for the latest database or when the license keys of some virus scanners expire the email will not be checked anymore.

This screen provides the current state of the anti-virus software.



18 Low level device management

18.1 Possible devices

To enter device management activate advanced options in the “Config” tab. Then click on the “Devices” tab.

The different wizards are normally used to add devices to this list.

Here is a description of the devices in use.

- WAN*: Ethernet links reserved for Internet connections
- LAN*: Ethernet links reserved for internal network connections
- DMZ*: Ethernet links reserved for DMZ servers
- FLEX*: Ethernet links for LAN, WAN or DMZ
- PPP*: Dial-in connection, for both cable modems and ADSL.
- VPN: Device for PPtP VPN connections.

18.2 Parameters to devices

Internal

When this check box is checked any network on this device is considered "safe" by the firewall. This is used by all subsystems and is therefor vital to security.

Dhcpd

When checked the dhcpd gives out ip addresses to dhcp client computers.

Dhcp

The network configuration of this device are fetched by the dhcp client software.

Addresses

In this column it's possible to add one or more IP-addresses to the device. There is no particular order and there is no need to add any netmasks to this address as this is automatically calculated from the routes.
When editing an existing device it's possible to click on an address. Depending on the use of the address in any route this will result in the possibility to remove an address or change the address.

Bridgedevs

The routing subsystems provides the possibility to configure an Demilitarized zone(DMZ). This is a network which is under the policy of the firewall, but in routing a part of the larger Internet. This is implemented via Ethernet-bridging. In this column the used Ethernet devices can be entered.

Status

Provides current status information about the device.

18.3 Bandwidth limits on devices

There are a list of bandwidth settings for each device.

Upstream-bandwidth

Provide the upstream bandwidth. This should be 95% of the total available bandwidth so the firewall can fairly handle all questions without the possible chocking of the bandwidth by the Internet Service Provider.

Downstream-bandwidth

Provide 95% of the available downstream bandwidth.

18.4 PPP device options

For PPP devices there are some extra options to initiate the PPP connection.

Username

When defining an PPP device this field appears. It's the user name used to authenticates to the Internet Service Provider(ISP).

Password

Like the user name, to be supplied by the ISP.

Type

Choice between types of PPP connections.

- PPTP: Point-2-Point Tunneling Protocol, used by many ADSL providers
- PPPoE: Point-2-Point over Ethernet, used by many Cable modem providers

19 Low level route management

To enter device management activate advanced options in the “Config” tab. Then click on the “Routes” tab.

These are the routes towards the different networks or hosts known by the firewall. All the routes are shown in the “Netview” as elements. Routes do not allow traffic by themselves for this policies should be added in the “Netview”.

Most routes are created by various wizards. But when a LAN is segmented it is sometimes necessary to add routes by hand.

19.1 Route parameters

Name

The label of the route in netview. Chose any name, everything is allowed. There are some characters that can't be used such as: space ' , = or "

Device

The device to which this route is connected.

Network

This is the endpoint of this route, which can be a host or a network.
When no netmask is given it will default to 32 and point towards a single host. After the route is submitted the netmask will be applied to the IP address and the base network address will be entered. Thus 192.168.99.3/24 will become 192.168.99.0/24.

Gateway

This is the gateway to the network or host. When the route is directly connected to the firewall this can be left empty or identical to the local address.

Local

A route will always bind to a specific local address of the device, choose one when there are multiple IP-addresses defined on the device.

19.2 Edit the mac address of a route

You can set the MAC-address of the Ethernet-card of a host. This may serve two purposes:

- It prevents other computers from using the specified IP address. The MAC-address and the IP address form a pair which will be enforced by the firewall.
- It also provides the possibility to use static leases when the firewall acts as the DHCP server of the network. The host, with this MAC-address, will always get the IP address given in the network column of the route.

19.3 Bandwidth limits to a route

In the column bandwidth setup of a given route can be modified. There are four different numbers. Down means from Internet, up means towards Internet.

For both directions you'll have to specify a upper limit and a lower limit. The upper limit prevents traffic to and from this route to receive a higher bandwidth that specified. The lower limit guarantees a minimum available bandwidth for this traffic. It's impossible to guarantee more bandwidth that 100% on all your routes.

19.4 Groups of routes

When the configuration of the firewall consists of a large amount of routes, the presentation of the network in the “Netview” gets pretty large. This is especially undesirable when many routes serve a similar purpose.

Therefor it's possible to create a group of routes. This group serves as a container of similar routes and can be displayed in the “Netview” as a single entity. Routes can only be combined into groups when they are on the same network.

The group can have a common policy connected to it, but every sub-route within the group can still get a more specific policy.

To add a group you'll have to provide a name for the group and select which route the group will be attached to. After you added the group, you can edit the routes you wish to add to the group, they will receive a pulldown menu in the “group” column. This pulldown menu lists all possible groups for this route. If the group you would like to select is missing the group is probably place in the wrong network.

20 Low level policy management

20.1 Policies

Policies are the core of the network subsystem. Most advanced features are based on policies, combined with various special options. Therefor this paragraph will describe the design of the policy system. In the following paragraph the options will be discussed.

The firewall is designed to block all traffic. It is the function of a policy to allow traffic. If there are no policies, no Internet packets may enter, leave or pass the firewall. A policy consists of several routes, a port list and various specials. Each policy has at least 1 source route and 1 destination route.

You may read a policy like this: “Allow traffic from this address (source route) to that address (destination route) when the used destination port is part of this port list.”

The procedure to allow certain traffic therefor consist of the following steps:

➔ Make sure both source and destination routes exist, if not introduce them.

➔ Create a new policy using these routes.

➔ Modify the policy's port list and options to suit your needs.

Various policy options are available to create advanced setups. These options include: address translation, IPSec encryption, binding to a specific connection, modification of TCP header fields, etc. Each policy can have one or more of these options selected.

20.2 Define a new policy

When the interface is in advanced mode (selectable in the “Config” tab) policies can be created, updated and removed in the “Netview”.

To create a new policy you need to take the following steps:

➔ Make sure no other policy is selected by selecting “none” in the policy selection pulldown menu.

➔ Open the context menu of a relevant source route by clicking on the route.

➔ Select the red button “(De)Select Source”. This will change the route's background to red.

➔ Repeat the two steps for all relevant source routes.

➔ Repeat the process for the relevant destination routes, this time choosing “(De)Select Destination”. These routes will get a green background.

➔ Provide a new name for this policy in the text field next to the “add” button.

➔ Push the “add” button.

➔ Open the port list by selecting the "ports" button.

➔ Modify the port list.

➔ Optionally add specials to the policy, see later in this chapter for the

possibilities.

20.3 Modify a policy

To modify a policy's routes, you can use the following procedure:

➔ Select the policy in the policy selection pulldown menu.

➔ Use the context menu of the relevant routes to select and/or deselect routes.

➔ Use the “update” button to apply these changes to the policy.

20.4 Removing a policy

It's possible to remove a policy by selecting the policy in the policy selection pulldown menu and the push the “delete” button. You will have to acknowledge the removal by pushing the (appearing) “remove” button.

20.5 Specific local addresses

Normally, when you select the firewall as a source or destination of the policy, it doesn't matter which specific local address the traffic is destined for. Therefor any address on all local devices matches the policy.

But for certain setups this behavior is unwanted. For example, if you setup the firewall to provide 1-on-1 NAT translation, mapping a secondary firewall address to an internal host, you need a way to select this secondary address. When an IP address is given in the field below the subject: “Specific local address(es)” this policy will only match traffic using the given address.

20.6 IPSec options

The first option found in the ports screen of a policy is the IPSec setup. Together with the IPSec Authentication of the remote gateway this policy option defines an IPSec tunnel.

The purpose of this option is to change this policy to a description of what traffic should be encrypted. There are two pulldown menu's: IPSec type and Direction.

IPSec type is used to choose between the different types of IPSec. For normal everyday tunnels this will be set to “esp”.

The Direction is used to provide some extra information about the direction of the tunnel. Basically there are two different setups possible. In both setups there are two policies for one tunnel, one defining the traffic going to the remote network, and one defining the traffic coming from the remote network.

Normally the outgoing policy will get a direction of “out” and the incoming policy the direction of “in”. Both in situations where there is a wish to setup different port lists for the different directions it is possible to let one policy define both directions. The other policy can be left on IPSec type “none” in that situation.

20.7 Specials

To add more options to a policy you'll have to push the “Add specials” button. This will provide a pulldown menu with the various options that are available.

20.8 DNAT

To setup a Destination Network Address Transformation you select the DNAT option. Normally a DNAT policy will need to have the firewall (the old destination) and the new target address (the new destination) as destination routes selected. If the firewall is able to detect this policy setup, it will automatically setup the DNAT option with the new target address. If this fails a DNAT entry with new address "---" will appear. By clicking on the address it can be modified.

It is possible to not only translate the destination address, but also translate the destination port. This is accomplished by changing the address in the DNAT entry to: <address>:<newport> for example 192.168.99.4:3390

20.9 SNAT/MASQ

With these two options it is possible to translate the source address of traffic matching this policy. SNAT is used to translate the source to the address given behind the SNAT entry. This address can be modified by clicking on the address. This will provide a pulldown menu with all known local addresses of the firewall. A special case is the usage of MASQ instead of SNAT. When MASQ is used the firewall will automatically translate the source to the first address of the device the packets leave on.

20.10 MSS

The MSS option is used to modify a TCP header field of the passing packets. The modified field is called Maximum Segment Size (MSS). This field indicates the destination of these packets that the reply packets should be smaller than this size. Effectively it will lower the return MTU (Maximum Transfer Unit) of the returning packets. This can be very effective in setups where there are MTU related problems.

20.11 Bind

The Bind option is used for protocol binding. Traffic matching the policy will be routed of the specified Internet connection, effectively binding this traffic to the device. For example mail should always be fetched at the correct Internet Service Provider even if there are multiple Internet connections to choose from.

20.12 Shaping

Similar to the routes, it's also possible to shape traffic according to policies. Again you will be provided with four different numbers. In this case the sum of lower limits of all policies must lower than 100%.

21 Mail handling policies

To be able to see and change mail handling policies activate advanced options in the “Config” tab. Then click on the “Mail” tab.

21.1 Set the policy for virus emails

Behind the “Virus-quarantine” line is the virus policy pulldown menu. It can be set to the following values:

- Bounce: The mail will be blocked and the original sender will receive a non-delivery notification.
- Discard: The mail will be blocked and no non-delivery notification will be send to the original sender (The Virus-warning account will always receive a notification).
- Pass: The mail will not be blocked! **This is not advised for virus mail, your network could get infected!**

21.2 Set the policy for unwanted emails

Behind the “Spam-quarantine” line is the spam policy pulldown menu. It can be set to the following values:

- Bounce: The mail will be blocked and the original sender will receive a non-delivery notification.
- Discard: The mail will be blocked and no non-delivery notification will be send to the original sender (The Spam-warning account will always receive a notification).
- Tag: The mail will be delivered but there will be a header line added with the warning that it is spam.
- Pass: The mail will not be blocked!

21.3 Spamfilter setup

There are two advanced options for spam detection.

Local tests only

This setting controls whether online databases with spam related information will be consulted or not. When this box is checked no network traffic will be generated, making the spam detection somewhat less effective, but considerable faster.

Spam-drop score

This number reflects the score used by the spam-detection system to decide whether to block the mail or let it pass. Mail with a high spam chance get a high value. So a low value here will treat mail easier as spam. In the mail headers of any mail with a spam score above 3.0, this score will be printed.