Chapter 3

Deploying Juniper Firewalls

Solutions in this chapter:

- Managing Your Juniper Firewall
- Configuring Your Firewall for the First Time
- Configuring System Services

☑ Summary

☑ Solutions Fast Track

☑ Frequently Asked Questions

Introduction

In this chapter we will look at the basics of deploying a Juniper firewall. The Juniper firewall has a large number of configuration options. Before you can deploy a device, you must first understand how to manage it, so in the first section of this chapter we look at the various methods of managing your Juniper firewall. Each option and best known procedure is discussed. Strong system security is important, but no more so than preventing intruder attacks.

There are many management options available on the Juniper firewall. Of these options, there are, effectively, two ways to manage the device directly. The first is from the *command line interface* (CLI). Many people still prefer this method of device management. Fully comprehending the command line interface allows you to better understand the Juniper firewall. There are specific functions that can only be done from the command line interface. Many of these commands are not commonly used, but are switches to enable or disable specific system features.

The second firewall management option is the *Web User Interface* (WebUI). This streamlined interface is user friendly and intuitive, allowing anyone to jump in and manage the firewall with ease. Even command line junkies will use the WebUI to reference the configuration, or to see a configuration more clearly.

Since a firewall is a core component of the network, we will focus heavily on how to configure your device to interact with the network. This covers *zone configuration* and Internet protocol (*IP) address assignment*. Properly configuring the network is crucial to the functionality of your network entity. Each type of zone and interface is documented to explain the available configuration options. Finally, we will configure various system services available from your Juniper firewall.

Managing Your Juniper Firewall

The first step in learning about firewalls is how to effectively manage them. In this section, we will look at the various management configuration options. The core configuration component for the firewall is the CLI. Even if you are using the WebUI it still ultimately generates the CLI configuration for you. While not required to memorize the CLI, it will greatly help if you do.

When managing your firewall you are required to authenticate to the device. Securing your management access is key to your network security. If you lose control of your access points, you lose control to your network. Creating a strong authentication policy for your administrators is essential for the effectiveness of your firewalls.

There may be times when you mistakenly erase parts of your configuration, or lose your configuration altogether. We will review how to recover from this type of mistake. Losing access to your device can be devastating. With so many different passwords to remember, you can easily forget how to gain access to your Juniper firewall. Even the most experienced administrators can find themselves in this predicament. However, several methods of recovery have been documented.

Finally, we will look at how to update the operating system on your Juniper device. Staying current with software revisions is very important. It provides you with security-related fixes as well as new software enhancements. For each type of management option, there is a specific way to update ScreenOS. Some options may be more effective then others, depending on your needs. At the completion of this section you should be familiar with WebUI and CLI. Knowing this is a requirement for managing your Juniper firewall.

Juniper Management Options

Every Juniper management option centers around two forms of management: the WebUI and the CLI. There is a third type of management, an enterprise class of security, called the NetScreen Security Manager (NSM). Because NSM's configuration options are extensive, NSM is outside of the scope of this book.

Serial Console

The *Serial Console* is a nine-pin female serial connection. This option gives you CLI access to the firewall. Serial Console is used to initially connect to your device, and to conduct *out-of-band management*. Out-of-band management is management that is not network based, such as access via modem. There are certain benefits to using a serial console that you do not get from using any other type of connection. The console provides a secure, physical, and dedicated access. Network connectivity issues cannot interrupt this type of connection, and no one can intercept your management traffic. It is completely secure because of its direct connection.

When configuring over a serial port, you are not using any type of network connectivity. In the case when you need to change Internet Protocol (IP) addressing on the firewall, and guarantee connectivity, using the serial console is an excellent option. With, and only with, serial console can you view and interact with the booting process. This cannot be accomplished remotely because the operating system (OS) has not started, and it is unable to provide management services. Many devices from UNIX servers, as well as other embedded devices, use serial consoles to provide serial console management. Most of the devices use an RJ-45 serial cable with a DB9 female connector. However some older devices use a DB9 female to DB9 male straight through serial cable. Table 3.1 outlines the proper connection settings when connecting with a serial terminal, or serial terminal emulator.

Table 3.1 The Serial Terminal Settings

Setting	Value
Speed	9600 bps
Character Size	8 Bit
Parity	None
Stop Bit	1
Flow Control	None

Telnet

A second form of CLI management is *Telnet*. Telnet is a protocol that has been used for years, and it is like a network based version of a serial console. However, it lacks many of the advantages of a serial console. First of all, it is a very unstable connection. The connection is made over the network in clear text format. This means that the transmitted data is not encrypted in any way, thereby allowing easy access to your login and password. Most client operating systems provide an easy to use Telnet client. A Telnet connection is not an ideal configuration for managing your device from a remote location. You can have a maximum of two active concurrent Telnet sessions. Most operating systems come with a built-in Telnet client. If not, you can use a program called *Tera Term*. Its download location can be found in the Resources section at the end of this chapter.

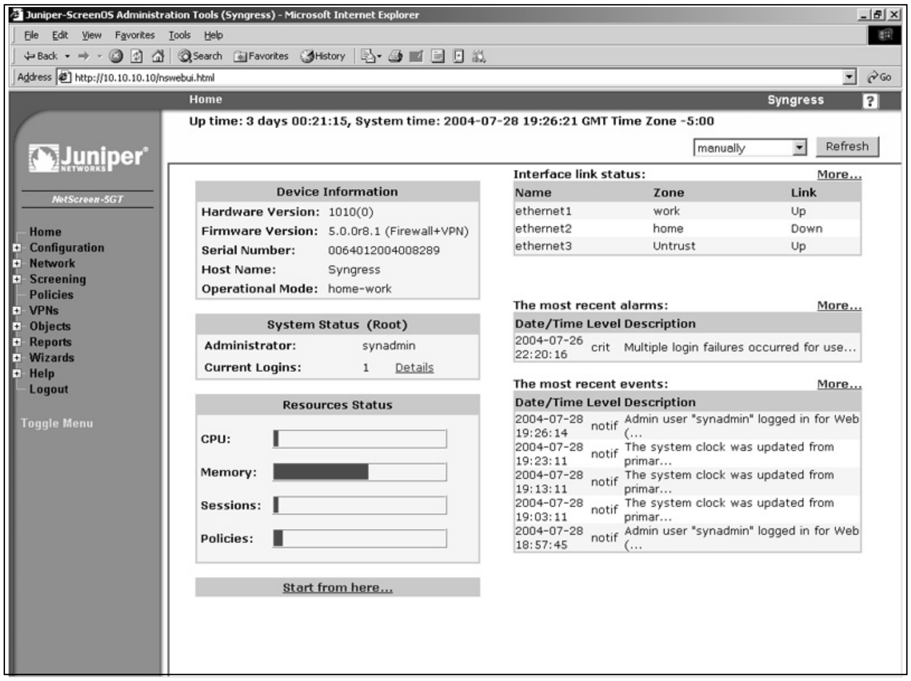
Secure Shell

The third form of command line management is *secure shell* (SSH). Like Telnet, SSH is a remote command line session. When using SSH, Telnet's security concerns are not an issue. Secure Shell provides an encrypted command line session to the Juniper firewall. It also provides protection from IP spoofing, and Domain Name System (DNS) spoofing attacks. SSH has two versions, v1 and v2. The versions are not backwardly compatible. Version two is more popular because of its higher level of security. You are required to have a client that is compatible with the version of SSH that you are using. Many UNIX based operating systems include clients, but Windows based operating systems do not. You can use a client named *PuTTY* for Windows. It is free, and it is easy to use. Information on the PuTTY client can be found in the Resources section at the end of this chapter.

WebUI

The Web user interface is the easiest type of management to use. Because of its simple point-and-select nature, it gives the end user a jumpstart into the management of the Juniper firewall. You can see in Figure 3.1 that the interface is very straightforward. On the left-hand side of the browser is the menu column. From here you can choose from the various configuration options. This menu can be either Dynamic Hypertext Markup Language (DHTML) based, the default, or Java based. The functionality is the same, but the look and feel is slightly different. By default, the WebUI is configured to work over only the Hypertext Transfer Protocol (HTTP). It can, however, be configured to work over Hypertext Transfer Protocol Secure (HTTPS). This provides a mechanism to secure your Web management traffic. Most of the popular Web browsers such as Internet Explorer, or Firefox work well with it.

Figure 3.1 Web User Interface


Juniper-ScreenOS Administration Tools (Syngress) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://10.10.10.10/nswebui.html
Go
Home
Syngress
?
Juniper NETWORKS
NetScreen-5GT
Home
Configuration
Network
Screening
Policies
VPNs
Objects
Reports
Wizards
Help
Logout
Toggle Menu
Refresh
Start from here...

Up time: 3 days 00:21:15, System time: 2004-07-28 19:26:21 GMT Time Zone -5:00

manually

Device Information	
Hardware Version:	1010(0)
Firmware Version:	5.0.0r8.1 (Firewall+VPN)
Serial Number:	0064012004008289
Host Name:	Syngress
Operational Mode:	home-work

System Status (Root)		
Administrator:	synadmin	
Current Logins:	1	Details

Resources Status

CPU:

Memory:

Sessions:

Policies:

Interface link status: More...

Name	Zone	Link
ethernet1	work	Up
ethernet2	home	Down
ethernet3	Untrust	Up

The most recent alarms: More...

Date/Time	Level	Description
2004-07-26 22:20:16	crit	Multiple login failures occurred for use...

The most recent events: More...

Date/Time	Level	Description
2004-07-28 19:26:14	notif	Admin user "synadmin" logged in for Web (...
2004-07-28 19:23:11	notif	The system clock was updated from primar...
2004-07-28 19:13:11	notif	The system clock was updated from primar...
2004-07-28 19:03:11	notif	The system clock was updated from primar...
2004-07-28 18:57:45	notif	Admin user "synadmin" logged in for Web (...

The NetScreen Security Manager

The NetScreen Security Manager (NSM) is a separate tool that can be used to manage a Juniper firewall device. The NSM is an application that runs on either a Solaris server, or a Red Hat Linux server. It requires a separate license, and it is licensed based on how many devices you want to manage. This product is used most effectively when you need to manage several devices at the same time. It uses an object-oriented management design.

Administrative Users

When connecting to a Juniper firewall for management purposes, you must always authenticate to the firewall. There are several types of users that you can employ to connect a Juniper firewall. The first user is the *root user*. This user is the principal user of the Juniper firewall device. The root user has the most power of any user on a Juniper firewall. There is only one root user per device. By default, the root user's name is *netscreen* and the default password is *netscreen*. It is highly recommended that you immediately change the login name and password. The root user has the greatest number of administrative privileges of any device. The *root user administrative privileges* are listed below:

- Add, remove, and manage all other administrators
- Create and manage virtual systems
- Create, delete, and manage virtual routers
- Add, delete, and manage security zones
- Assign security zones to interfaces
- Perform asset recovery
- Set the device to Federal Information Processing Standards (FIPS) mode
- Reset the device to default settings
- Manage the device's firmware
- Load configuration files
- Perform management on the root system

The next level of administrator is *read/write*. Read/write is very similar to the root user; however, read/write users cannot create other administrators. This type of access is most useful when you want to distribute administrative privileges to others, yet control access. The Juniper firewall provides a very detailed audit log of the actions of each administrator. You should capitalize on this by creating administrative users for each person who administers your firewall. This way you can identify the user with the modification. There is no reason to share an administrator user account between two users. The read/write administrative privileges include:

- Create and manage virtual systems
- Create, delete, and manage virtual routers
- Add, delete, and manage security zones
- Assign security zones to interfaces
- Perform asset recovery
- Set the device to FIPS mode
- Reset the device to default settings
- Manage the device's firmware
- Load configuration files
- Perform management on the root system

The next type of user is the *read-only* administrator. This user has limited access to the system. As the name suggests, the user can only view the configuration, and they are unable to modify the system in any way. This is useful if you want to assign a technical writer to document your configurations, or if you want to give anyone limited access to the device to perform troubleshooting on the network. The following list includes the limited privileges of the read-only administrator.

- Read-only privileges in the root system
- Read-only privileges in all virtual systems

On some devices you can have *virtual systems*. A virtual system acts as its own separate security domain. Virtual system administrators have permission only on a specific system. The virtual system administrator privileges are shown in the following list.

- Create and manage auth, Internet Key Exchange (IKE), Layer 2 tunneling protocol (L2TP), Extended Authentication (Xauth), and Manual Key users
- Create and manage services
- Create and manage policies
- Create and manage addresses
- Create and manage virtual private networks (VPNs)
- Modify the virtual system administrator login password
- Create and remove virtual system read-only administrators

The last type of user is the *virtual system read-only administrator* who has almost the same privileges as a read-only administrator. The difference is that they can see only the configuration of a single, specified virtual system.

Becoming familiar with the privileges associated with the different types of administrator can give you the tools to create an efficient strategy for delegating authority on your system. Do not be afraid to create many different administrative users for your Juniper device. This will provide you with granular access to your system. Again, all users' actions are logged. This log provides a detailed list of access for each user. This can be helpful when determining issues related to a particular administrator, or in determining whether or not an administrator account has been compromised. Chapter 6 reviews the use of external authentication sources for administrative users. This can provide additional security in cases where you use technologies such as *SecurID* to remove the use of a single static password.

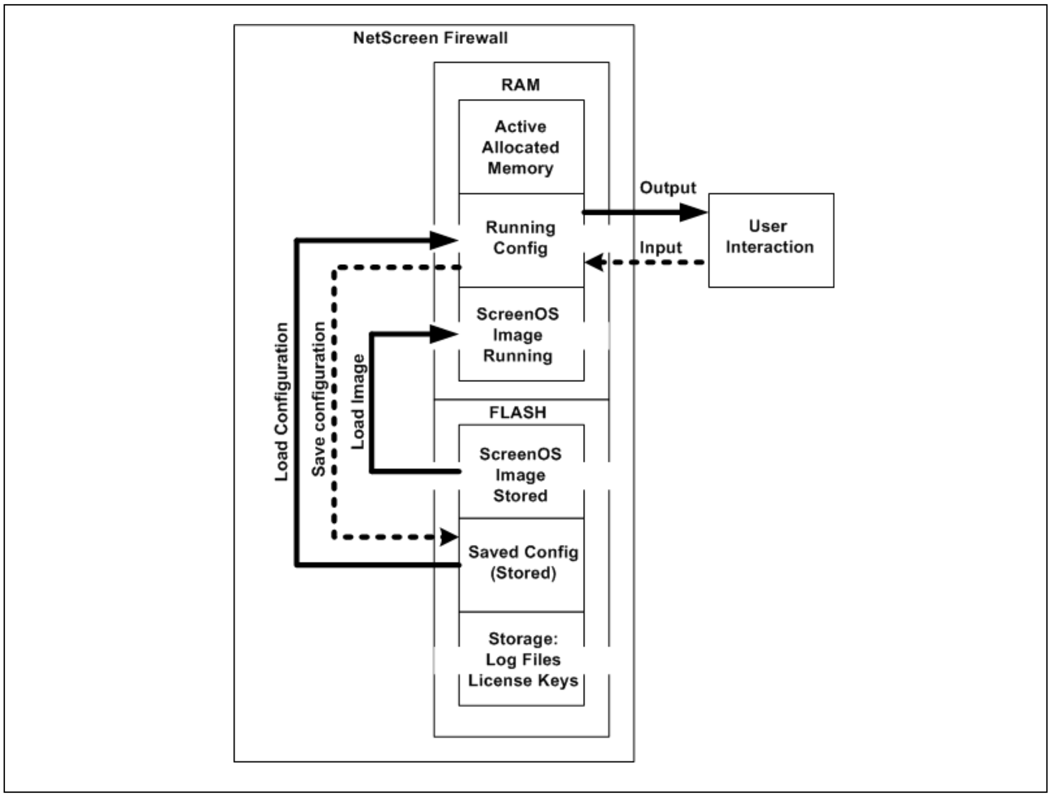
The Local File System and the Configuration File

Each Juniper firewall device has a similar design for its internal system components. Long-term storage on the device is stored into *flash memory*. Flash memory is a non-volatile memory that retains information after the system is turned off. Some devices have a Compact Flash (CF), Secure Digital Memory (SD) card slot, or a universal serial bus (USB) port for external storage. This is flash memory, but it is removable. The internal flash is not removable. All component information that Juniper needs to store is in flash memory, including ScreenOS log files, license keys, attack databases, and virus definitions.

Each Juniper device also contains random access memory (RAM). This is a volatile type of memory that is cleared whenever the system is powered off, or reset. When the Juniper device powers on, and after the power on self test (POST) is completed, the ScreenOS image is loaded into RAM. After ScreenOS is up and functional, it loads the saved configuration file from flash memory. The configuration that is stored in RAM is called the *running configuration*.

Whenever you make a change to the configuration, it is always saved to the running configuration. If you make changes to your configuration but fail to save it, the file would revert to the last saved configuration whenever you reset or rebooted your device. When you remove power to the device, and then restore power, it causes a return to previously saved configuration. When using the CLI, your configuration must be *manually* saved. This can be done by using the *save* command. The save command is simply **save**. By typing that command, your running configuration is saved as the *saved configuration*, which is stored in flash memory. The file system components are shown in Figure 3.2.

Figure 3.2 File System Components



Using the WebUI is even easier. The WebUI *automatically* saves your configuration after every change. However, when using the CLI, if you exit your session or attempt to reset the device, you will be notified that your configuration has changed. At that point you are given the option of saving the configuration. The Juniper device is much more user friendly than other devices when it comes to advising you that your configuration has changed, and offering you the option to save it.

There are times when flash may not provide you with the type of storage that you need. You may require long term storage of log files, or perhaps a backup of your configuration file. There are two ways to accomplish this:

- When using the command line, you can apply the command **get config** to view your configuration, then copy and paste it into a simple text document.
- From the command line, you can copy the configuration to a Trivial File Transfer Protocol (TFTP) server. TFTP is a simple type of File Transfer Protocol (FTP) server. It requires no authentication, but only specification of the filename you are placing on the server. To save your configuration to a TFTP server, use the command **save config to tftp <*a.b.c.d*> <*file*>,** where <*a.b.c.d*> is the IP address of the TFTP server, and <*file*> is the filename you want use for the save.

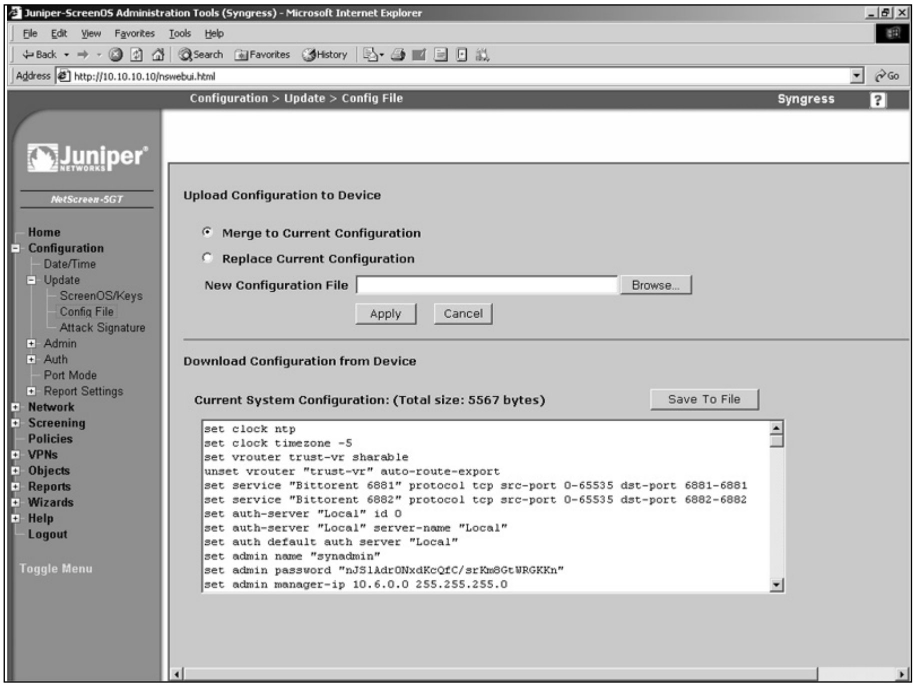
Depending on the data that is being transferred from the file system, you may prefer a more secure option than TFTP. You can use *secure copy* (SCP) to transfer files as well. Secure copy is similar to secure shell. It requires a special client in order to interact with it. Many UNIX systems include this feature. Windows has many clients. I prefer the **PuTTY Secure Copy (**PSCP) software, which is part of the *PuTTY* freeware secure shell clients. In the following example we will turn on SCP, and copy a file from the Juniper firewall to our UNIX system.

```
From the CLI:
Syngress-> set scp enable
Syngress-> get scp
SCP is enabled
SCP is ready
Syngress-> get file
    flash:/envar.rec                  98
    flash:/golerd.rec               1220
    flash:/burnin_log1             10240
    flash:/burnin_log0             10240
    flash:/dhcpservl.txt              52
    flash:/ns_sys_config           1092
    flash:/dnstb.rec                   1
    flash:/license.key               395
    flash:/$lkg$.cfg                 922
    flash:/expire.rec                 23
    flash:/attacks.sig                 198833
Syngress->
From the UNIX Host:
UNIX-Host:~ syngress$ scp synadmin@10.6.0.1:license.key license.txt
The authenticity of host '10.6.0.1 (10.6.0.1)' can't be established.
DSA key fingerprint is f9:a7:4c:53:4c:0a:cc:5a:50:6b:eb:df:42:42:63:c0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.6.0.1' (DSA) to the list of known hosts.
synadmin@10.6.0.1's password:
license.key                                   100%  395     4.8KB/s   00:00
UNIX-Host:~ syngress$ cat license.txt
1k=d2f5fb8aa5b9a000&n=capacity_key
k=2JQcSPh1ogana6h82NJeAfDwgb3aiOXT2UFcm9OFQDkuK4iT6YfKefMZjTODboIN2JQ0oWnWWX+nKkY
SMytB8gF1ID7tWXI9lvZ11JURDENckexZ7IwtmRmDEh+YT3dJvDSOAYeGuuWFtGYE5tVnPfZq6cnlO254
GPPm5HJ3qTG4sRBSRR/QFqL6WAnfnoSpByJu/Xr9vxx9GSU4fTMGLFkWsbRP5cVpTGWmyOBapFfn1qWzu
/bMLzDkox8zUHFZ2NcNCOSGOk5PvCMcZwOaADRIFqJj1oh4u7+toY37gdrEM5sQqmELemAlUi90dhLPl7
jsTy1R/V0/ourYn00XcMw==&n=di_db_key
UNIX-Host:~ Syngress$
```

As you can see, we enabled SCP, allowing us to view all of the files stored in flash memory. Next we went over to the UNIX host and copied the file from the Juniper device to the local UNIX system. Finally, we used the **cat** command to concatenate the contents of the file so you can see them. SCP can be effective and easy to use for removing files from Juniper devices.

If you are using WebUI, you can access **Configuration | Update | Config File** and then select the button labeled **Save To File**. This will allow you to save the configuration to your local PC as shown in Figure 3.3. Alternatively, from this same screen you can select the text in the text window, then copy and paste the configuration to a text file. As you have seen from these files, the config files are a collection of commands. The configuration file operates similar to manually typing these commands in line by line. This is great because it requires that you understand only one format. It also allows you to easily modify saved configuration files to reflect changes. Becoming familiar and comfortable with the use of the CLI cannot be stressed enough. In the next section, we will examine the configuration of the device, and the commands available to administer the device.

Figure 3.3 WebUI Save Screen



Upload Configuration to Device

● Merge to Current Configuration

○ Replace Current Configuration

New Configuration File

Download Configuration from Device

Current System Configuration: (Total size: 5567 bytes)

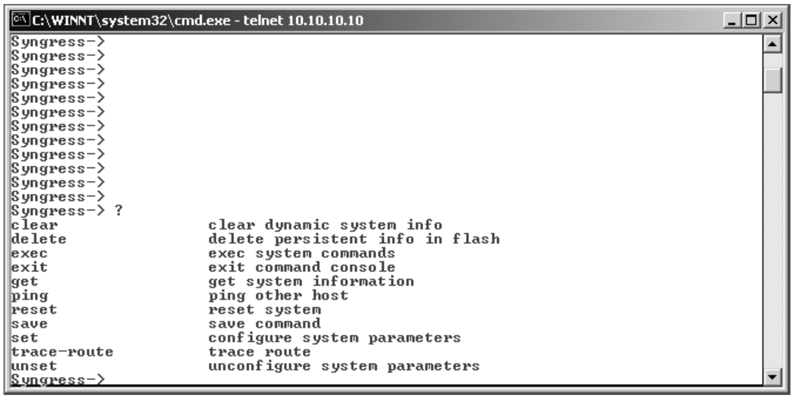
```
set clock ntp
set clock timezone -5
set vrouter trust-vr sharable
unset vrouter "trust-vr" auto-route-export
set service "Bittorent 6881" protocol tcp src-port 0-65535 dst-port 6881-6881
set service "Bittorent 6882" protocol tcp src-port 0-65535 dst-port 6882-6882
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set admin name "synadmin"
set admin password "nJS1AdrONxdKcQfC/srKm8GtWRGKKn"
set admin manager-ip 10.6.0.0 255.255.255.0
```

Using the Command Line Interface

The command line interface is at the core of configuring your Juniper firewall device. No matter which method you use to manage your firewall, the CLI commands control the device, and a thorough understanding the CLI is crucial to effective management. The NSM generates the same commands that you may manually enter via the CLI. CLI commands are straightforward, and easy to learn. Other devices use cryptic commands, or commands that seem to do one thing, but actually perform an unrelated action. When this firewall was designed, the engineers took the need for simplicity into consideration. In Figure 3.4, an example of the help screen is shown. This gives you an idea of the information provided by the *Help* command.

Figure 3.4 shows an example of the command line. The prompt shows the device's current *host* name. This is very useful if you have several devices that are not readily distinguishable from the command line. Starting at the root, there are literally thousands of command options. Memorizing this great number of commands could be a daunting task. However, there is an easy-to-use built-in help system. From anywhere on the command line, simply type **?** to access the Help system, which will list most available commands. Some are not listed; however, these specific commands will be discussed in later sections.

Figure 3.4 Command Line Session Using Help



```
Syngress->
Syngress->
Syngress->
Syngress->
Syngress->
Syngress->
Syngress->
Syngress->
Syngress->
Syngress->
Syngress->
Syngress->
Syngress-> ?
clear                  clear dynamic system info
delete                 delete persistent info in flash
exec                   exec system commands
exit                   exit command console
get                    get system information
ping                   ping other host
reset                  reset system
save                   save command
set                    configure system parameters
trace-route            trace route
unset                  unconfigure system parameters
Syngress->
```

From here there are several *base commands*, including *clear, exec, exit, get, ping, reset, save, set, trace-route,* and *unset***.** Under each one of these commands are subcommands.

An example is in order. We will explore the command used to retrieve information from the device, the **get** command. If we wanted to look at system information device such as *uptim*e, *serial number*, and *configuration information*, we would use the **get system** command. At the end of any get command you can do one of three things.

- You can press **Enter** and have the information displayed in your terminal window.
- You can redirect the output to a TFTP server much as we did earlier when we saved the configuration. You would use this command **get system > tftp <*a.b.c.d*> <*string*>** to send the output to a TFTP server, where <*a.b.c.d*> is the IP address of the TFTP server, and <*string*> is the filename you want to save.
- You can also use the pipe (**|**) to match output. If you were to use the *get system* command to search for the serial number of your device, you would use the command: **get system | include "Serial Num"**. This would then display only the serial number, and omit the rest of the data. You can also exclude specific information. You would use the same procedure as described earlier, but substitute the term **exclude** for **include**. This helps filter the information provided from a get command.

The next command we will examine is the *set* command. This command is used to set a configuration in the current running configuration. Suppose you wanted to set the hostname of your Juniper device to *Syngress*. You would use the *set hostname Syngress* command to cause your prompt to appear as **Syngress->**. This prompt appears only in the *running* configuration. If you want to ensure that this is the default prompt for your device, simply save the configuration: use the command *save* to commit the running configuration to the saved configuration. The *set* command is used throughout this book; therefore, there will be ample exposure.

It is important that you familiarize yourself with the five, system-controlling commands: *save, exec, exit, delete,* and *reset.* Each of these commands performs a system task. The *save* command can be used to perform functions other than the obvious. The *save* command is used to save files to, and from, the local system. The *reset* command is used to *reboot* the Juniper device. There are several suboptions that allow you to reboot without being prompted to confirm the configuration. You can also force a reboot with a choice of saving the running configuration, or discarding it. This way, when you want to reboot the system you do not have to answer prompts before the reboot. This is helpful if placed inside a configuration script.

The *exec* command is powerful and multi-purposed. The *exec* command runs a command on the system. For example, the command **exec save software from flash to tftp 1.2.3.4 CurrentOS.bin** would save the current version of ScreenOS to a TFTP server. So it would be much like copying a file in DOS or UNIX shell from one location to another. This is an example of the type of function that the *exec* command can provide.

The *delete* command allows you to manage your local system by deleting several types of stored information. This can range from you local stored SSH information to files on the local flash file system. For example, if you wanted to delete a file named *old_data* that was stored in flash memory, you would use the following command: **delete file flash:old_data**. This would delete that file permanently from flash memory.

The *exit* command serves one purpose: to exit your current session. When you use this command, your current CLI session is terminated. If you have made unsaved configuration changes, you will be prompted to save them before you exit.

The *clear* command allows you to clear current data from memory. This can include dozens of options anywhere from the current local DNS cache to the current sessions passing though the firewall. This is useful if you want to remote this information, and to then to accumulate it again. Sessions are a perfect example of something that you may want to clear. You would want to clear you session table if you were troubleshooting a connectivity problem, and you wanted to see the session recreated in your debugging logs. This is as easy as typing **clear session** at the command line, and pressing **Enter** to clear all sessions. You could also selectively delete your sessions depending on your needs.

There are two commands that you can use to for troubleshooting purposes, *ping* and *trace-route*. Though you may have used these before on other operating systems, *ping* is a tool to test *connectivity* between two systems. You use *ping* to verify that your firewall can see a specific host. The *ping* command can be used with options other than host. You can also specify how many ping packets you want to send, as well as the size and the timeout for each packet. To use the *ping* command, just type *ping***,** and then the hostname or IP address of the device you want to contact. The other command is *trace-route*. *Trace-route* is similar to *ping*, but it is designed to determine the IP addresses of all routers in the path from your network to the specified remote host.

When using the command line, there are a few special commands that you can use to make things easier for the end user. We previously covered the *?* command for getting help. This can be used for every subcommand, as well as partial commands, to list available options for that command. The *help* command is very useful, and it should be used often. Next is the **Tab** key, which is used to provide command completion. For example, you can type **set add,** and then press **Tab** to have the command completed for you. This results in the command *set address*. If there is more then one match to the command, both matches will be listed, and you can select the appropriate one. You must continue to type the individual characters of the command until it becomes a unique entity in order for command completion to work. This is universal for the CLI on the Juniper device. This is the same functionality provided by the UNIX *bash shell*. Table 3.2 displays other special key combinations.

Tools & Traps…

Command Line Interface Quandaries

When you use the command line there are occasions where some functions do not appear to be functioning, or where some commands do not seem to cause the expected action. For example, sometimes **Tab** completion will not work. Though frustrating, luckily there are only a few situations in which this can happen. One such situation is when you attempt to use **Tab** completion with the name of an interface. Each time you press the **Tab** key, you see the same line again and again. You can use the question mark to bring up the interface list.

The other situation occurs when you use **Tab** completion to complete the name of a zone. You will get the same results as with interface completion. The command line allows use of truncated commands rather your having to type the complete command name.

For example, rather than typing the command *get interface ethernet3* you could use the command *g int e3*. For the first command we type only the letter g. The first command that it matches with the g is get. Since no other command matches it, ScreenOS interprets the g as the get command. The second command we typed was *int*, and the third was *e3*, which corresponded to ethernet3. The more you use the command line, the more familiar you will become with the short, or truncated, version of the commands.

As you can see, each command is separated by a space. However, if a space between two command line entries is *required*, you simply surround the space/text with quotes. For example, the command *set snmp location Dearborn, MI* would fail. However, if we used the command *set snmp location "Dearborn, MI"*, the text enclosed in double quotation marks would count as a single word.

Table 3.2 Special Key Combinations for the CLI

Special Key	Action
Up-arrow key	Recalls previous command
Down-arrow key	Recalls next command
Control+A	Brings cursor to beginning of the current line
Control+E	Brings the cursor to the end of the current line
Ctrl+C	This is the escape sequence
Left-arrow key	Move cursor back one position
Right-arrow key	Move cursor forward one position
Tab	Completes partially typed command
Question mark (?)	Displays Help and command options

The command line interface environment offers *you* the capability to tailor commands specifically for your purposes. In fact, the more advanced options, such as *debugging*, can only be carried out from the CLI. Administrators generally find the WebUI easier to use at first; however, they soon realize the power of the CLI.

Using the Web User Interface

The Web User Interface (WebUI) is a simple to use tool for managing your Juniper firewall. It is intuitive, and it allows those with little firewall experience to easily control a Juniper device. Figure 3.1 shows the main WebUI page following authentication. The menu bar on the left is where you select configuration options. The current status is displayed on the right-hand side of the screen. On this screen, there are six different boxes: *Device Information, System Status, Resource Status, Interface Link Status, The most recent alarms, and The most recent events.*

Each box reports the status of current events. Current uptime, and the current system time are displayed at the top of the screen. The *Device Information* box shows information such as the hardware version, current firmware version, serial number, host name, and its current operations mode. The *System Status* box performs as its name suggests. It shows the current number of logins to the device, and it shows the login identities. The *Resources Status* displays in a bar graph format, four device resources: CPU, memory, sessions, and policies. If you hover the mouse pointer over any of the bars in the graph, it will display the numerical values for that bar. These are the core performance metrics of the Juniper device. As we discussed earlier, the memory bar graph will read higher then you would expect it to do, because ScreenOS preallocates memory for performance.

If you look at the box entitled *Interface Link Status*, you will see the status of all interfaces. This is handy for determining which interface is up, and which is down. *The most recent alarms* list performs as its name suggests. Finally, as its name implies, *The most recent events* box lists the most recent events. Some boxes in the upper right-hand corner have more hyperlinks, which takes you directly to the detail page for each item.

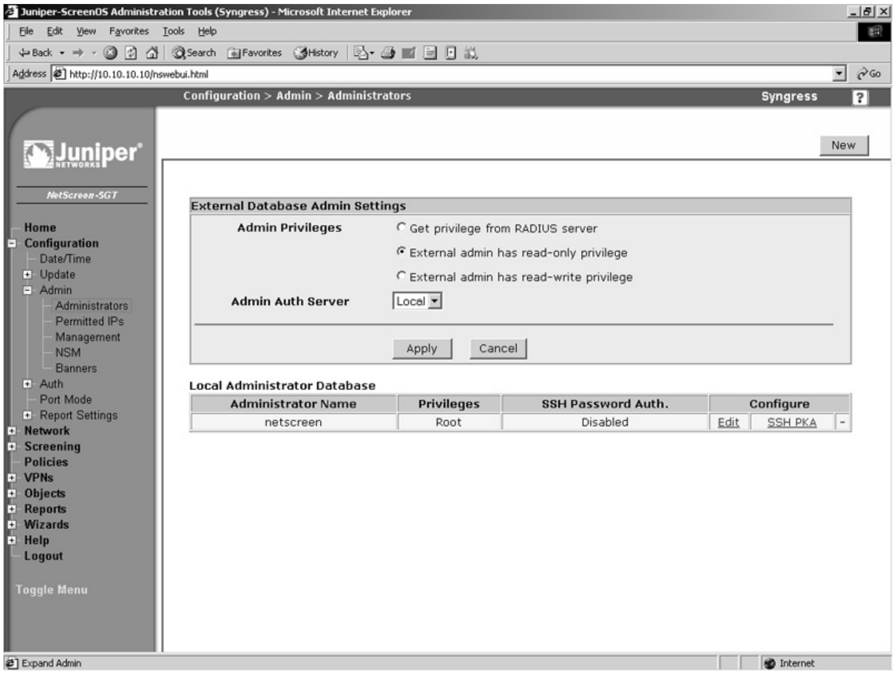
Securing the Management Interface

Now that you understand management of the Juniper firewall device, it is time to *secure* management access to your device. The last thing you want to do is leave the door wide open for an intruder to control your device. There are some easy steps that you can take to prevent this. First, you should change the *root username* and *password*. Everyone who owns a Juniper firewall is aware of the default login and password to the device.

Use the following steps to change the root username and password via the WebUI.

1. Select **Configuration** | **Admin** | **Administrators**. A screen similar to Figure 3.5 will be displayed.

Figure 3.5 WebUI Administrators Screen



External Database Admin Settings

Admin Privileges
○ Get privilege from RADIUS server
● External admin has read-only privilege
○ External admin has read-write privilege

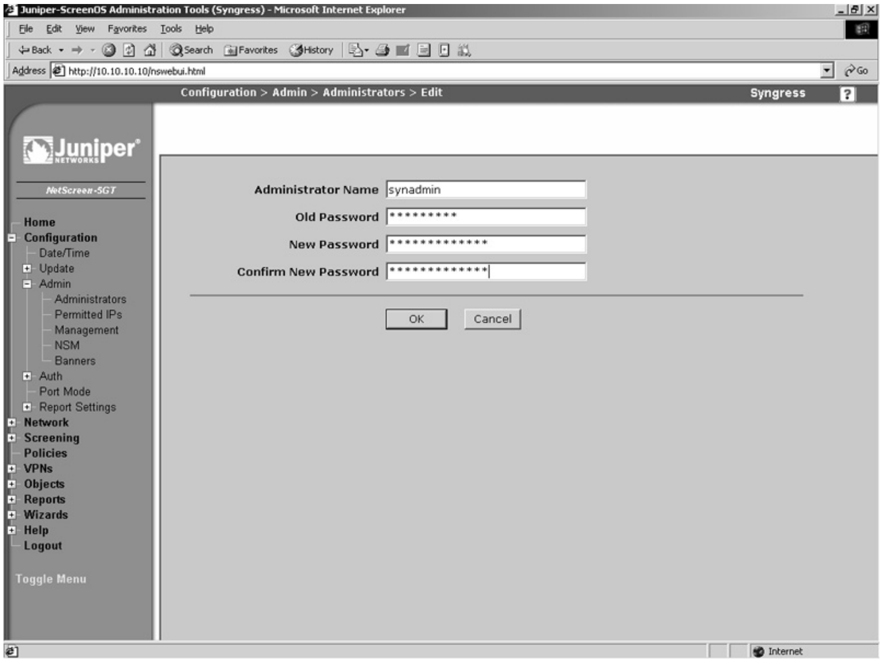
Admin Auth Server: Local

Local Administrator Database

Administrator Name	Privileges	SSH Password Auth.	Configure		
netscreen	Root	Disabled	Edit	SSH PKA	-

2. Press the **Edit** link for the user with *root* privileges. In our example, the *root* user is the only username entry. A screen similar to that in Figure 3.6 will be displayed. Figure 3.6 is identical to Figure 3.5, with the exception that Figure 3.6 must be replaced with a screenshot of the Edit screen.

Figure 3.6 Edit Administrator



Administrator Name synadmin

Old Password *********

New Password *************

Confirm New Password *************

3. Change the **Administrator Name** from **Juniper** to **synadmin**.
4. Enter **Juniper** in the **Old Password** field.
5. Enter the new password in the **New Password** and **Confirm New Password** fields.
6. Press **OK**

Use the following steps to change the root username and password via the CLI:

1. Enter the following command to change the admin name:

```
Syngress-> set admin name synadmin
```

   You will see the following message:

```
Password has been restored to default "Juniper". For security reasons,
please change password immediately.
```

2. Enter the following command to change the password:

```
Syngress-> set admin password password
```

3. Use the following command to verify the changes:

```
Syngress-> get admin user
```

You will see an output similar to the following:

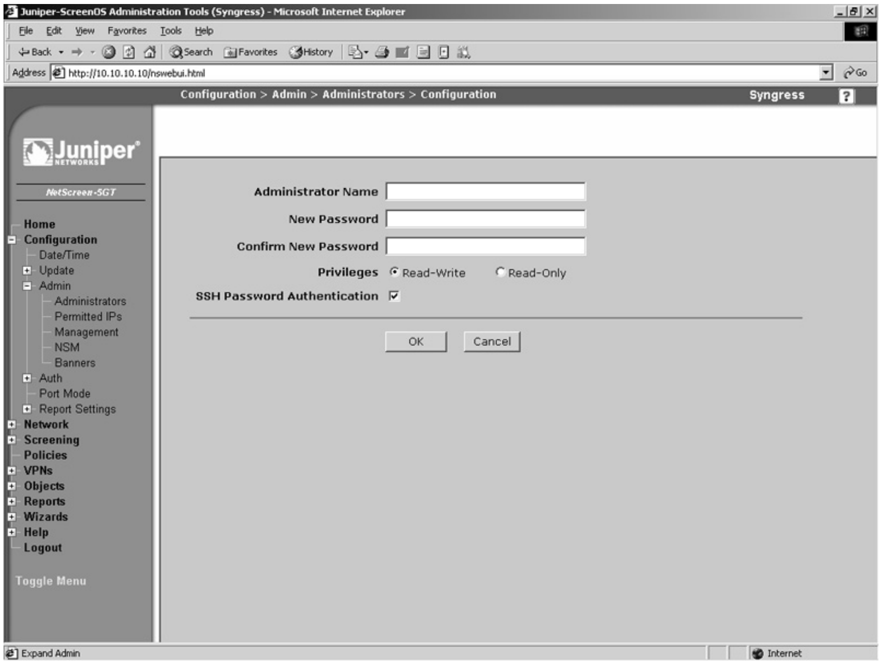
```
Name                             Privilege
-------------------------------- ---------------
synadmin                         Root
Syngress->
```

The device now has its root users name set to **synadmin,** and its password has been changed. It is suggested that you create a password of a minimum of eight characters. The maximum number of characters allowed in the password is thirty-one.

It is also suggested that you create a read-write administrator to use for regular maintenance. If that administrator is compromised, there will be no direct root access to the device. Use the following steps to create a read-write administrator via the WebUI:

1. Select **Configuration** | **Admin** | **Administrators** | **New**. The screen shown in Figure 3.7 will appear.

Figure 3.7 Administrator Configuration



Juniper-ScreenOS Administration Tools (Syngress) - Microsoft Internet Explorer

Address http://10.10.10.10/nswebui.html

Configuration > Admin > Administrators > Configuration

Administrator Name

New Password

Confirm New Password

Privileges ● Read-Write ○ Read-Only

SSH Password Authentication ☑

OK Cancel

2. Use the **Administrator Name** field to enter the new name. In this example, **backupadmin**.

3. Enter this user's password in the **New Password** and **Confirm New Password** fields.
4. Enable the **Read-Write** option.
5. Press **OK**.

Use the following to create a read-only administrator via the WebUI.

1. Select **Configuration** | **Admin** | **Administrators** | **New**.
2. Use the **Administrator Name** field to enter the new name. In this example, **roadmin**.
3. Enter this user's password in the **New Password** and **Confirm New Password** fields.
4. Enable the **Read-Only** option.
5. Press **OK**.

Enter the following command to create a read-write administrator via the CLI:

```
Syngress-> set admin user backupadmin password %so%back privilege all
```

Verify the entry by using the *get admin user* command. The output will look like the following:

```
Name                             Privilege
-------------------------------- ---------------
synadmin                         Root
backupadmin                      Read-Write
```

Enter the following command to create a read-only administrator via the CLI:

```
Syngress-> set admin user roadmin password n0tru$t privilege read-only
```

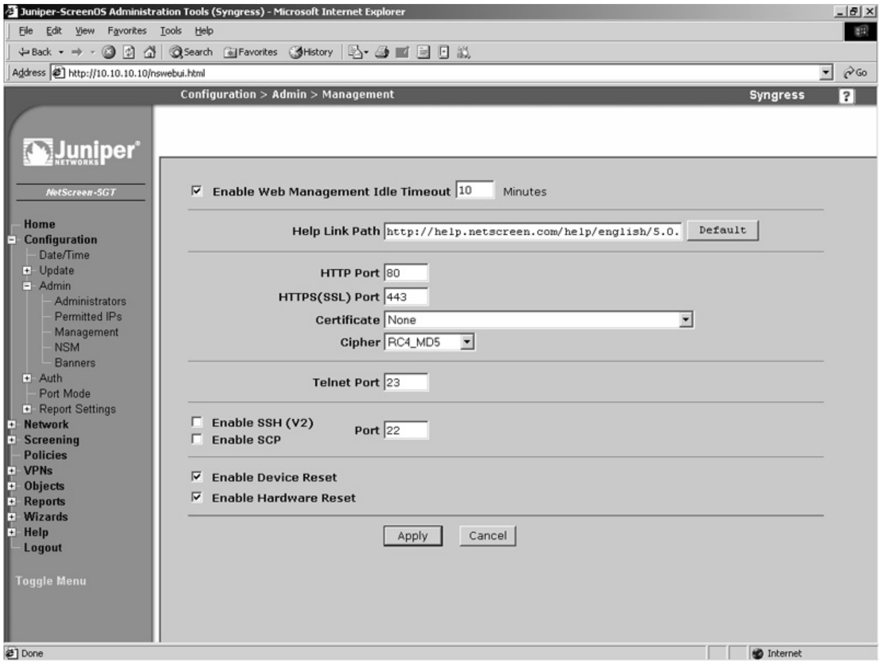
Verify the entry by using the *get admin user* command. The output will look like the following:

```
Name                             Privilege
-------------------------------- ---------------
synadmin                         Root
backupadmin                      Read-Write
roadmin                          Read-Only
```

Another option that you should configure is the *idle timeout*. I have been to many locations where you only have to connect to the console to have a *privileged* account ready and waiting for you. This opportunity exists because the previous user left the console unattended, and they failed to log out. This is a common setup for a serious security breach. Anyone with a little know-how can cause trouble on your network if allowed to connect to your system with readily available privileged access. In order to avoid this situation, set the *idle timeout* to a reasonable amount of time. The default is ten minutes for the console, Telnet, SSH, and WebUI sessions. Use the following steps to set the console, Telnet, and WebUI sessions to timeout after five minutes via the WebUI:

1. Select **Configuration** | **Admin** | **Management**. A screen similar to the one shown in Figure 3.8 will appear.

Figure 3.8 Admin Management



☑ Enable Web Management Idle Timeout 10 Minutes

Help Link Path http://help.netscreen.com/help/english/5.0. Default

HTTP Port 80

HTTPS(SSL) Port 443

Certificate None

Cipher RC4_MD5

Telnet Port 23

☐ Enable SSH (V2)
☐ Enable SCP
Port 22

☑ Enable Device Reset

☑ Enable Hardware Reset

Apply Cancel

2. Ensure the **Enable Web Management Idle Timeout** option is enabled and type **5** in the corresponding text field.
3. Press **Apply**.

You can also modify the console timeout option via the CLI by typing **set console timeout 5**. Note that a timeout value of **0** will disable the timeout feature. Use the **get console** command to verify the change. The output will resemble the following:

```
Console timeout: 5(minute), Page size: 22/22, debug: buffer
privilege 250, config was changed and not saved!
ID State  Duration Task Type   Host
 0 Login       660 13433716 Telnet 10.254.5.32:49401
 1 Logout        0 13435768 Local
 2 Logout        0 13424824 Local
 3 Logout        0 13410460 Local
```

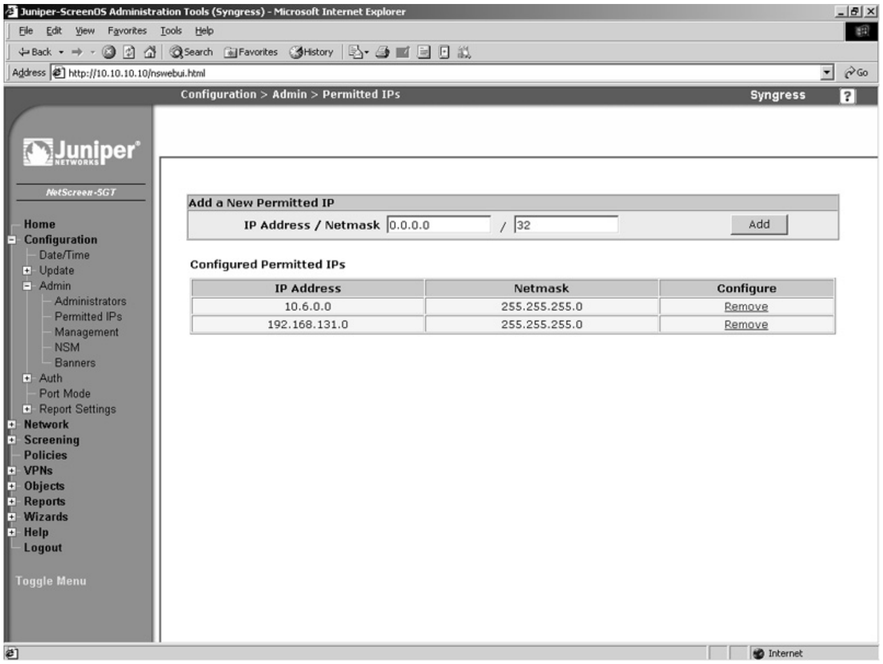
To set the admin authentication timeout, type **set admin auth timeout 5**. Use the *get admin auth* command to verify the setting. The output will resemble the following:

```
Admin user authentication timeout: 5 minutes
Admin user authentication type: Local
```

The next step is to limit system access to your firewall. By specifying *permitted* IP addresses, you can limit which IP addresses are authorized to perform management services. You are limited to a total of six entries for both network and host entries. Once you enable this setting, it immediately takes effect. If you set this up remotely, ensure that you add your own IP address and/or source network. Use the following steps to create a permitted IP address entry via the WebUI:

1. Select **Configuration** | **Admin** | **Permitted IPs**. A screen similar to that shown in Figure 3.9 will be displayed.

Figure 3.9 Permitted IPs



Add a New Permitted IP

IP Address / Netmask 0.0.0.0 / 32

Configured Permitted IPs

IP Address	Netmask	Configure
10.6.0.0	255.255.255.0	Remove
192.168.131.0	255.255.255.0	Remove

2. Use the available text fields to enter the IP address and netmask, and then select **Add**. You can remove an IP address from the list by selecting its **Remove** link. Note that if the list contains no IP addresses, any IP address will be able to access the firewall.

To add a permitted IP address via the CLI, type the command **set admin manager-ip *ipaddress***, where *ipaddress* is the full IP address using dotted quad (###.###.###.###) notation. You can verify the setting by entering **get admin manager-ip**. To remove an IP address entry via the CLI, type the command **unset admin manager-ip *ipaddress***.

Secure Shell is highly suggested over Telnet, as we discussed earlier when we were looking at our different management options. However, SSH must be enabled before you can use it. Again earlier we looked at using SSH version two. In the following code snippet we enable SSH version two in either the CLI, or the WebUI. After enabling SSH it may take several minutes for the SSH servers to be enabled. This is because the SSH keys are generating during this time.

Use the following steps to enable SSH via the WebUI:

1. Select **Configuration | Admin | Management**.
2. Enable the **Enable SSH (v2)** option.
3. Press **Apply**.

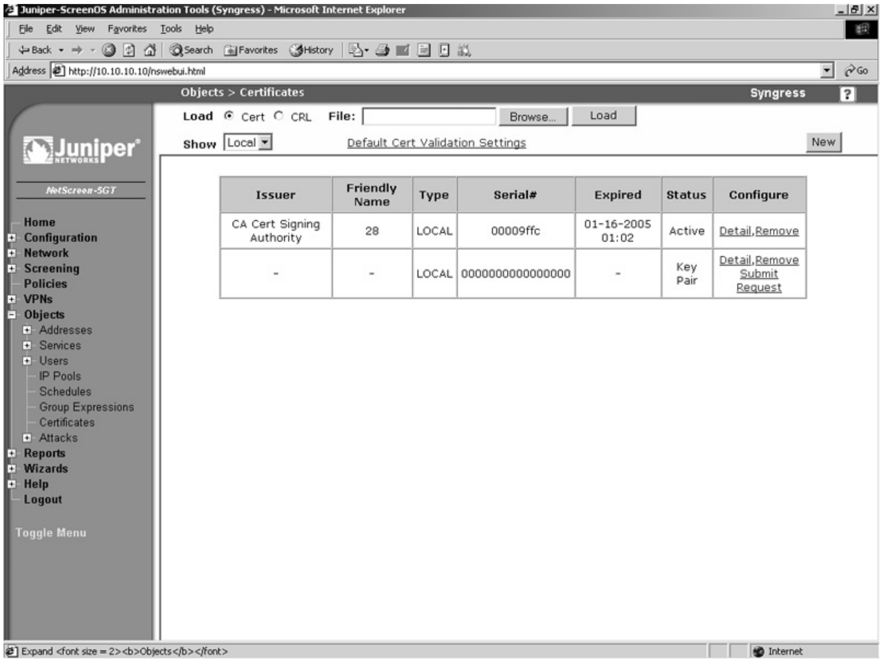
To enable SSH via the CLI, type the command **set ssh version v2**. To set version 1 rather than version 2, simply replace **v2** in the command with **v1**.

It is strongly recommended that you use SSL when using the WebUI. In general, it is very easy to set up and configure. Included in ScreenOS 5.2 and later is a self-signed certificate. WebUI allows you to turn on SSL right out of the box. You can also generate a certificate signing request (CSR) and submit it back to a certificate authority (CA) to get the certificate signed. Once you have the signed certificate, you can load it back onto your Juniper device. We will review how to generate the CSR, and how to load the certificate. However, signing a certificate varies based upon which certificate authority you choose. If you are using your device from your company's network, you should use a certificate purchased from a reputable Web site such as www.verisign.com or www.godaddy.com. Either site can provide you with a certificate. However, if you want to get a signed certificate for testing purposes, go to www.cacert.org to get a free one.

Use the following steps to generate a certificate request. Note that this example includes company-specific information that you should substitute with your own information.

1. Access **Objects | Certificates**. The screen will display the existing certificates (Figure 3.10).
2. Press **New**. The New Request screen will be displayed as shown in Figure 3.11.
3. Enter your **Name**, **Phone**, **Unit/Department**, **Organization**, **County/Locality**, **State**, **Country**, **Email**, **IP Address**, and Fully Qualified Domain Name (**FQDN**).
4. Select the Rivest, Shamir, and Adelman (**RSA)** option.
5. Select **1024** or **2048** from the **Create new key pair** drop-down list: the higher the number, the more secure the certificate.

Figure 3.10 Certificates

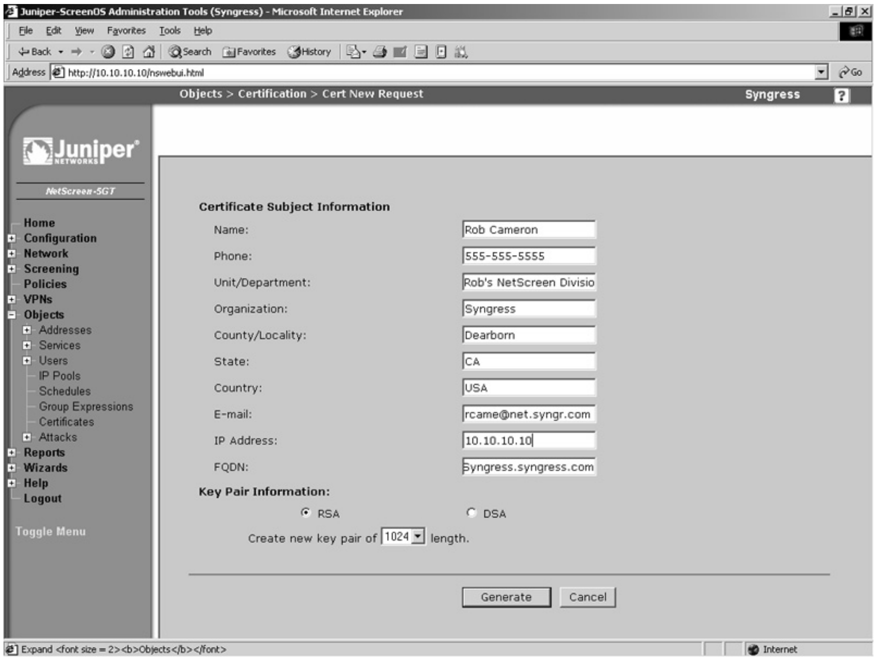

Juniper-ScreenOS Administration Tools (Syngress) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://10.10.10.10/nswebui.html
Go
Juniper NETWORKS
NetScreen-5GT
Home
Configuration
Network
Screening
Policies
VPNs
Objects
Addresses
Services
Users
IP Pools
Schedules
Group Expressions
Certificates
Attacks
Reports
Wizards
Help
Logout
Toggle Menu
Objects > Certificates
Syngress
Browse...
Load
New
Default Cert Validation Settings
Expand <font size = 2><b>Objects</b></font>
Internet

Load ● Cert ○ CRL File:

Show Local

Issuer	Friendly Name	Type	Serial#	Expired	Status	Configure
CA Cert Signing Authority	28	LOCAL	00009ffc	01-16-2005 01:02	Active	Detail,Remove
-	-	LOCAL	0000000000000000	-	Key Pair	Detail,Remove Submit Request

Figure 3.11 New Certificate Request


Juniper-ScreenOS Administration Tools (Syngress) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://10.10.10.10/nswebui.html
Go
Juniper NETWORKS
NetScreen-5GT
Home
Configuration
Network
Screening
Policies
VPNs
Objects
Addresses
Services
Users
IP Pools
Schedules
Group Expressions
Certificates
Attacks
Reports
Wizards
Help
Logout
Toggle Menu
Objects > Certification > Cert New Request
Syngress
Generate
Cancel
Expand <font size = 2><b>Objects</b></font>
Internet

Certificate Subject Information

Name:	Rob Cameron
Phone:	555-555-5555
Unit/Department:	Rob's NetScreen Divisio
Organization:	Syngress
County/Locality:	Dearborn
State:	CA
Country:	USA
E-mail:	rcame@net.syngr.com
IP Address:	10.10.10.10
FQDN:	Syngress.syngress.com

Key Pair Information:

● RSA ○ DSA

Create new key pair of 1024 length.

6. Press **Generate**. In several minutes a new page will displayed that contains a section of text.
7. Copy the text contents from "-----BEGIN CERTIFICATE REQUEST----" to "-----END CERTIFICATE REQUEST-----".
8. Supply this to your certificate authority. They, in turn, will supply you with a certificate file.
9. Access **Objects** | **Certificates** and select **Browse**. Choose the certificate file from the CA and select **Load**. The certificate is now active and loaded.
10. Access **Configuration** | **Admin** | **Management**. Select the certificate from the **Certificate** field.

Use the following steps to request and set up a certificate via the CLI using your own personal and company information.

1. Enter the following commands to request a certificate:

```
Syngress-> set admin mail server-name 123.123.123.100
Syngress-> set pki x509 dn country-name US
Syngress-> set pki x509 dn email rob@Juniper.com
Syngress-> set pki x509 dn ip 123.123.123.123
Syngress-> set pki x509 dn local-name "Dearborn"
Syngress-> set pki x509 dn name "Rob Cameron"
Syngress-> set pki x509 dn org-name "Rob's Juniper division"
Syngress-> set pki x509 dn org-unit-name Books
Syngress-> set pki x509 dn phone 555-555-5555
Syngress-> set pki x509 dn state-name CA
Syngress-> set pki x509 cert-fqdn manage.Juniper.com
Syngress-> set pki x509 dn default send-to rob@Juniper.com
Syngress-> exec pki rsa new-key 1024
```

2. The certificate will be e-mailed to the address you originally specified. Copy the contents starting with "-----BEGIN CERTIFICATE REQUEST----" and ending with "----END CERTIFICATE REQUEST----".
3. Supply this information to your certificate authority. They, in turn, will supply you with a certificate file. The CA may also supply you with a local certificate and a certificate revocation list (CRL). A CRL contains a list of all revoked certificates. These are certificates that the CA has signed that are no longer valid.
4. To import these files, use the following commands:

```
Syngress-> exec tftp 123.123.123.100 cert-name newcer.cer
Syngress-> exec tftp 123.123.123.100 cert-name localpro.cer
Syngress-> exec tftp 123.123.123.100 crl-name notrust.crl
```

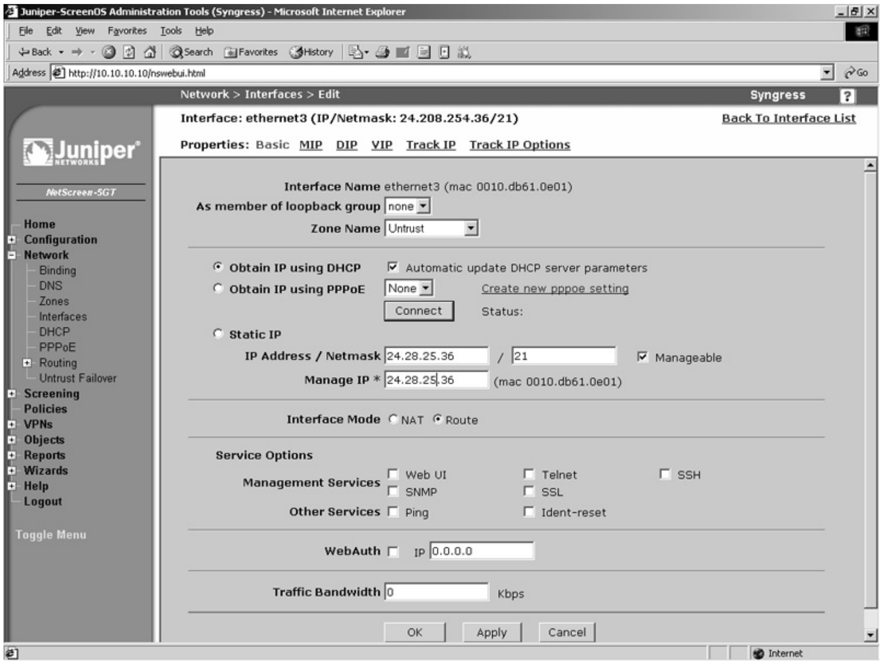
```
Syngress-> set ssl encrypt 3des sha-1
Syngress-> set ssl cert 1
Syngress-> set ssl enable
```

Now that we have the access restricted to specific hosts, there are several more options we can utilize to enhance the security. The first option is to disable unnecessary management services. Management services are bound to individual interfaces. It is important to restrict them to the bare minimum. This can be done easily from either the WebUI or the CLI. In this case, we are using a Juniper-5GT so we will be modifying the *untrust* interface. We are going to enable the WebUI, SSL for the WebUI, and SSH. We will use only the WebUI with SSL and SSH because they are secured.

Use the following steps to disable unnecessary management services via the WebUI:

1. Access **Network | Interfaces**. Press the **Edit** link for the entry titled **untrust.** A screen similar to Figure 3.12 will be displayed.

Figure 3.12 Editing Network Interfaces



Juniper-ScreenOS Administration Tools (Syngress) - Microsoft Internet Explorer

Address http://10.10.10.10/nswebui.html

Network > Interfaces > Edit

Interface: ethernet3 (IP/Netmask: 24.208.254.36/21)

Properties: Basic MIP DIP VIP Track IP Track IP Options

Interface Name ethernet3 (mac 0010.db61.0e01)
As member of loopback group none
Zone Name Untrust

● Obtain IP using DHCP ☑ Automatic update DHCP server parameters
○ Obtain IP using PPPoE None Create new pppoe setting
Connect Status:
○ Static IP
IP Address / Netmask 24.28.25.36 / 21 ☑ Manageable
Manage IP * 24.28.25.36 (mac 0010.db61.0e01)

Interface Mode ○ NAT ● Route

Service Options
Management Services □ Web UI □ Telnet □ SSH □ SNMP □ SSL
Other Services □ Ping □ Ident-reset

WebAuth □ IP 0.0.0.0

Traffic Bandwidth 0 Kbps

2. Ensure that **WebUI**, **SSH**, and **SSL** are all enabled, and ensure the remaining option are disabled.
3. Press **Apply**.

```
To disable unnecessary management services via the CLI, type the following
commands:
```

```
Syngress-> unset interface untrust manage ping
Syngress-> unset interface untrust manage snmp
Syngress-> unset interface untrust manage telnet
Syngress-> set interface untrust manage ssh
Syngress-> set interface untrust manage web
Syngress-> set interface untrust manage ssl
```

Use the *get interface trust* command to verify the settings.The output should resemble the following:

```
Interface untrust:
  number 1, if_info 88, if_index 0, mode route
  link up, phy-link up/full-duplex
  vsys Root, zone Untrust, vr trust-vr
  dhcp client enabled
  PPPoE disabled
  *ip 123.208.123.254/24   mac 0010.db61.1231
  gateway 123.208.123.1
  *manage ip 123.208.123.254, mac 0010.db61.1231
  route-deny disable
  ping disabled, telnet disabled, SSH enabled, SNMP disabled
  Webenabled, ident-reset disabled, SSL enabled
  webauth disabled, webauth-ip 0.0.0.0
  OSPF disabled  BGP disabled  RIP disabled
  bandwidth: physical 100000kbps, configured 0kbps, current 0kbps
             total configured gbw 0kbps, total allocated gbw 0kbps
  DHCP-Relay disabled
  DHCP-server disabled
```

Next, you can change the local port that your management services listen on.This can help prevent your services from being detected if someone were to scan for open services. Telnet (TCP 23), SSH (TCP 22), WebUI (TCP 80), and WebUI SSL (TCP 443) can each be changed to a different port number. Use the following steps to change the ports via the WebUI:

1. Access **Configuration** | **Admin** | **Administrators**.
2. Specify new port numbers for Telnet, SSH, WebUI and WebUI SSL. Note that port numbers must be in the range 1024-32767.
3. Press **Apply**.

Enter the following commands to set the port numbers via the CLI:

```
Syngress-> set admin ssh port 1024
Syngress-> set admin port 32000
```

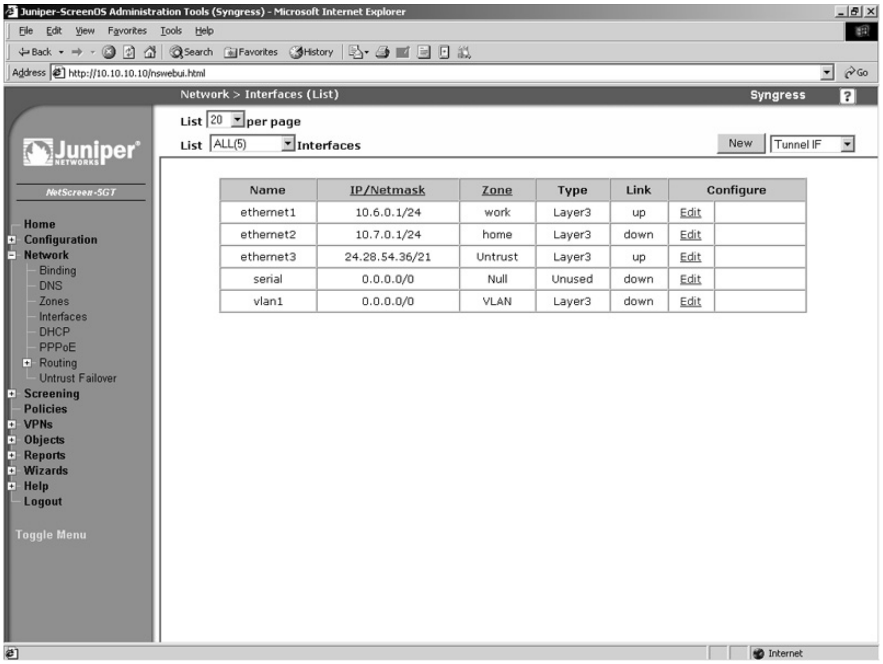
```
Syngress-> set admin telnet port 4000
Syngress-> set ssl port 5000
```

So far, we have explored interface IP address management, and it is simple to determine the IP address of the firewall. If the IP address is known, it can be used to connect to it and to manage your device. However, you can set up a management IP, which is configured directly on the interface. For this example we will be using a Juniper-5GT, and we will be modifying the *untrust* interface.

Use the following steps to set up a management IP via the WebUI:

1. Access **Network | Interfaces (List)**. The screen shown in Figure 3.13 will be displayed.

Figure 3.13 Network Interfaces List



Address http://10.10.10.10/nswebui.html

List 20 per page

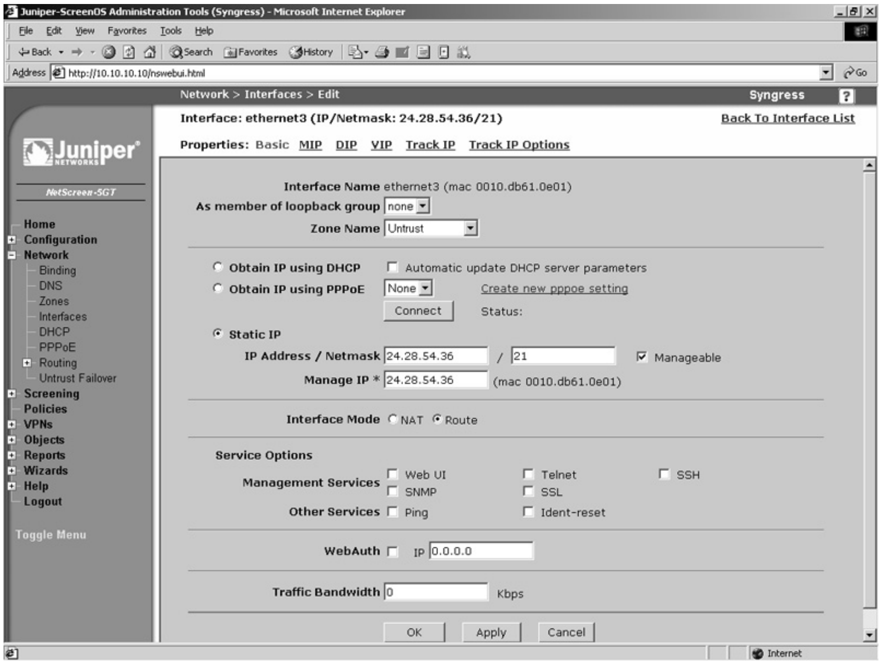
List ALL(5) Interfaces

Tunnel IF

Name	IP/Netmask	Zone	Type	Link	Configure	
ethernet1	10.6.0.1/24	work	Layer3	up	Edit	
ethernet2	10.7.0.1/24	home	Layer3	down	Edit	
ethernet3	24.28.54.36/21	Untrust	Layer3	up	Edit	
serial	0.0.0.0/0	Null	Unused	down	Edit	
vlan1	0.0.0.0/0	VLAN	Layer3	down	Edit	

2. Press the **Edit** link for the *untrust* entry. A screen similar to the one shown in Figure 3.14 will be displayed.
3. Use the **Manage IP *** field to enter the new IP address.
4. Press **Apply**.

Figure 3.14 Edit Network Interface



Network > Interfaces > Edit

Interface: ethernet3 (IP/Netmask: 24.28.54.36/21)

Properties: Basic MIP DIP VIP Track IP Track IP Options

Interface Name ethernet3 (mac 0010.db61.0e01)

As member of loopback group none

Zone Name Untrust

○ Obtain IP using DHCP □ Automatic update DHCP server parameters

○ Obtain IP using PPPoE None

Status:

● Static IP

IP Address / Netmask 24.28.54.36 / 21 ☑ Manageable

Manage IP * 24.28.54.36 (mac 0010.db61.0e01)

Interface Mode ○ NAT ● Route

Service Options

Management Services □ Web UI □ Telnet □ SSH □ SNMP □ SSL

Other Services □ Ping □ Ident-reset

WebAuth □ IP 0.0.0.0

Traffic Bandwidth 0 Kbps

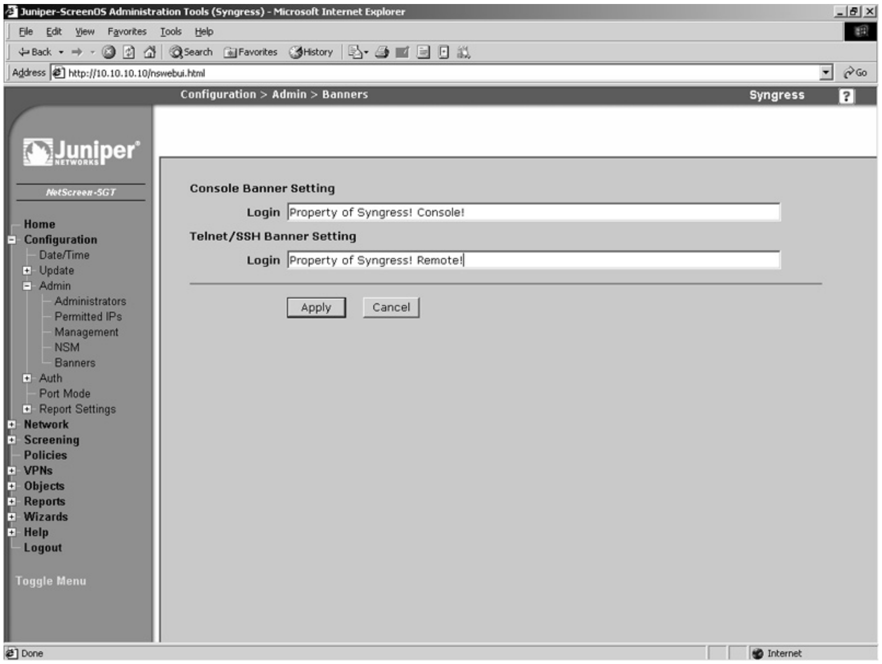
To set up a management IP via the CLI, type the command **set interface untrust manage-ip *ipaddress***.

For remote command line access you can set up customized login banners. This is useful to provide a legal warning, or a help message. This can also identify specific penalties for unauthorized access. There are two limitations to using banners. First, you are limited to a single line. Second, you are limited to 127 characters. A banner can be configured for both console and remote Telnet sessions. This option can be configured from either the CLI, or the WebUI.

From the WebUI:

1. Access **Configuration** | **Admin** | **Banners**. A screen similar to Figure 3.15 will be displayed.
2. Use the **Console Banner Setting Login** field to enter the login banner text that will be displayed for users using the console.
3. Use the **Telnet/SSH Banner Setting Login** field to enter the login banner text that will be displayed for users using Telnet or SSH.
4. Press **Apply**.

Figure 3.15 Banners



Console Banner Setting

Login: Property of Syngress! Console!

Telnet/SSH Banner Setting

Login: Property of Syngress! Remote!

Use the following CLI command to set the banner for console users.

```
Syngress-> set admin auth banner console login "Only permitted individuals are
allowed to use this access. If you are not permitted please disconnect!"
```

Use the following CLI command to set the banner for Telnet users.

```
Syngress-> set admin auth banner telnet login "Authorized users only!!! All
actions are logged!!!"
```

Finally, there are three options that can be configured only from the command line that can enhance security. Two of these options will not save your system, but since they are new to the 5.0 ScreenOS release, they are worth mentioning. First, you can enforce a minimum length for administrative user passwords. Second, you can restrict how many unsuccessful login attempts that a user can have before they are kicked out of the system. The default is three and it does not lock out the user. The same person could Telnet back in to try again. Finally, you can restrict the root user to access from the console only. This can prevent anyone from gaining root access to the device unless they have physical access to it.

Use the following CLI commands to set a minimum password length, limit access attempts, and restrict root user access to the console, respectively.

```
Syngress-> set admin password restrict length 8
Syngress-> set admin access attempts 2
Syngress-> set admin root access console
```

The ideas in this section will help to secure your device. Security is all about mitigating risk. With these management security procedures in place, you significantly lower the chances of incurring a security breach. You can mix and match the configurations that work best for your environment.

Updating ScreenOS

Juniper Networks is committed to providing a secure and robust operating system for Juniper firewall products. From time to time Juniper will publish a new version of ScreenOS. This may include security updates, feature enhancements, or both. It is very important that you maintain the currency of the software on your firewall. It is a core component of your network security platform, and it has to be secure. There are several methods available to upgrade ScreenOS. First, we will focus on the command line methods where you can not only update your OS, but you can back up your operating system as well. You are required to use a Trivial File Transfer Protocol (TFTP) server when you use the CLI. Use the following command to back up your software:

```
Syngress-> save software from flash to tftp ipaddress 5.0.0r8.1-5GT.bin
```

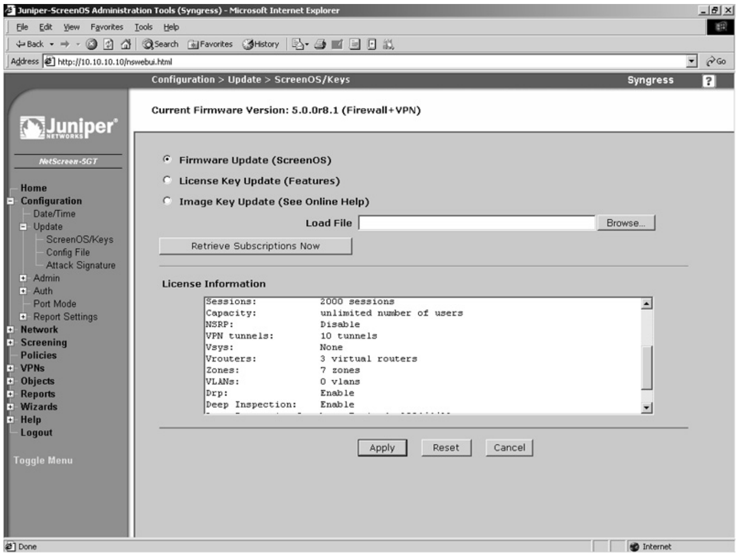
```
       Use the following command to update the software:
```

```
Syngress-> save software from tftp 1.2.3.4 5.0.0r8.1-5GT.bin to flash
```

You can also use the WebUI to update the firmware. However, as we mentioned before, you cannot download the current software from the WebUI.

1. Access **Configuration** | **Update** | **ScreenOS/Keys**. A screen similar to Figure 3.16 will be displayed.

Figure 3.16 ScreenOS/Keys



Juniper-ScreenOS Administration Tools (Syngress) - Microsoft Internet Explorer

Address http://10.10.10.10/nswebui.html

Configuration > Update > ScreenOS/Keys

Current Firmware Version: 5.0.0r8.1 (Firewall+VPN)

● Firmware Update (ScreenOS)
○ License Key Update (Features)
○ Image Key Update (See Online Help)

Load File

License Information

```
Sessions:          2000 sessions
Capacity:          unlimited number of users
NSRP:              Disable
VPN tunnels:       10 tunnels
Vsys:              None
Vrouters:          3 virtual routers
Zones:             7 zones
VLANs:             0 vlans
Drp:               Enable
Deep Inspection:   Enable
```

2. Enable the **Firmware Update (ScreenOS)** option.
3. Press **Browse** and locate and select the previously downloaded firmware file, which is stored on the local system.
4. Press **Apply**. It may take several minutes to update the system with the new OS.

System Recovery

There may be times when your Juniper firewall runs into problems from which you cannot recover.Three scenarios are covered in this section. One of the major issues is *configuration management*.There may be scenarios that cause you to make changes where you are unsure of the repercussions. For example, you may be adding a new route, or a new policy that could wreak havoc on your network, though you are actively running on a successful configuration. In cases where you need a backup copy of a correctly functioning configuration file, you can use the *configuration rollback feature*.

The configuration rollback feature allows you maintain a backup configuration file that you can use in case your primary configuration file, saved or running, runs into problems. The configuration rollback cannot be performed from the WebUI. Use the following steps to save your system configuration.

1. Use the command *get file* to get a list of files in flash memory.
2. Enter the command **save config to last-known good**. A new file called $lkg$.cfg will be created. This file is your rollback configuration file. It is a saved copy of the *running* configuration at the time you executed the command. That file stays on the system unless you explicitly call the *delete* command to remove it. This means that even if you reset the configuration to the defaults, you still have this configuration available for use.

To restore a previously saved system configuration, type the command **exec config rollback**. Note that this process *forces* your device to reboot.

As long as the file exists, you can use this restoration process at any time. There is one additional way to use configuration rollback. If you are working on a new configuration that could possibly cause you to lose access to your system for any reason, configuration rollback can be placed in *watching* mode. In this mode, if the device is reset, it will automatically reset the configuration to the stored rollback configuration. This is a life saver in cases where you need to ensure the safe restoration of your device's provided networking services.

To put the rollback in watching mode, type the command **exec config rollback enable**. The command prompt will include the text "rollback enabled". To turn this mode off, type **exec config rollback disable**.

Now that we have discussed how to recover your configuration, we need to look at another scenario. What if you lose your root password? This is a tough situation to recover from, because you have lost all access to the system. There are two methods to recover from this error. Both methods require you to have console access to the device. In the first scenario, you would log into the serial console using the *serial number* of the device as the username and password. Once you do this, you will be notified that you will lose your configuration and all your settings. If you have performed proper configuration management, you will be fine. Note; even the configuration rollback file is deleted. So you must have saved your configuration somewhere other than the system if you want to be able to use it to restore service in an emergency.

The following shows a typical serial number login and the resulting messages.

```
login: 00642120012308289
password:
!!! Lost Password Reset !!! You have initiated a command to reset the device to
factory defaults, clearing all current configuration and settings. Would you like
to continue?  y/[n] y


        !! Reconfirm Lost Password Reset !! If you continue, the entire
        configuration of the device will be erased. In addition, a permanent
        counter will be incremented to signify that this device has been reset.
        This is your last chance to cancel this command. If you proceed, the
        device will return to factory default configuration, which is: System IP:
        192.168.1.1; username: netscreen, password: netscreen. Would you like to
        continue?  y/[n] y
```

Another way to access a system when you have forgotten the root password is to use the *reset button* located on the exterior of the system. To use this type of configuration use the following procedure:

1. Use a pin, place it in the resent hole, push and hold for at least four to six seconds. The status LED will blink amber once per second.
2. Wait for the status LED to begin blinking, and then remove the pin from the reset hole.
3. Wait one to two seconds, and replace the pin in the reset hole, push and hold for at least four to six seconds.
4. Wait for the status LED to turn red, and then eventually to begin blinking green before you release the pin from the reset hole.

Doing this will reset the system, and you will lose all your configurations. This is done for security purposes. These are both powerful methods available to recover your device; however, you may want to disable these options. You may not want someone to be able to walk up to your device and reset your configuration. Both methods can be disabled. However, if you disable them, the device will be unrecoverable if you lose the root password. Therefore, do not lose your root password unless you want to physically return the device to Juniper Networks.

To disable the ability to log in using the serial number, type **unset admin device-reset**. To re-enable this feature, type **set admin device-reset**. To disable the device's reset button, type **unset admin hw-reset**. To re-enable this feature, type **set admin hw-reset**.

In the previous section we looked at ways to upgrade ScreenOS. However, there are many ways in which the image can be corrupted during upload. More than likely, the file was damaged *before* you uploaded it. To restore your system to a functional configuration, you must have serial console access to the system, and a TFTP server on the local network to the device. During the boot process, a prompt will be displayed four times. The prompt will say, "Hit any key to run loader. Press any key, and you will be asked for the file you want to load, the IP address you want to assign to your device, and the IP address of the TFTP server. The interface that receives the IP address you assign is one of the following depending on what type of device you have: Trust, E1, or E1/1. If the file can be found on the TFTP server, it will be loaded into flash, and your device will reboot. When the device reboots it will load the new OS image.

```
Juniper NS-5GT Boot Loader Version 2.1.0 (Checksum: 61D07DA5)
Copyright (c) 1997-2003 Juniper Technologies, Inc.

Total physical memory: 128MB
    Test - Pass
    Initialization.... Done

Hit any key to run loader
Hit any key to run loader
Hit any key to run loader

Serial Number [0123012123008289]: READ ONLY
HW Version Number [1010]: READ ONLY
Self MAC Address [0010-db61-1230]: READ ONLY
Boot File Name [ns5gt.5.0.0r8.1]:
Self IP Address [192.168.1.1]:
TFTP IP Address [192.168.1.31]:

Save loader config (56 bytes)... Done
```

Configuring Your Firewall for the First Time

Now that you are familiar with the basics of managing your Juniper firewall, it is now time to configure your firewall. This section discusses basic configuration requirements to make your system functional on your network. There are three basics for getting your device up and running on the network. The first thing you need is a *zone.* We touched on zones in the previous chapter. In this section we will explore how to use existing zones, create new zones, and how to bind zones to interfaces. The primary type of zone that exists is the *security zone*, but there are several other types of zones that can be used. It is important to know how each type of zone functions, because it determines how an interface will function. Some zones may never be used; however, being aware of their existence is important.

There are several types of interface on a Juniper firewall.You will always have physical interfaces because they are required in order to connect to the network. Juniper also offers several other types of interfaces. These interfaces provide different functions, and they are not all physical devices.These types of interfaces include *subinterfaces*, *management interfaces*, *high availability interfaces*, and *tunnel interfaces*. Each type of interface was designed to provide a specific function on the Juniper device. We will look at each interface type, its function, and how you can leverage their special abilities on your network.

Your newly configured interface will require an IP address if you want it to interact with your network. In Chapter 1 we discussed IP addressing. It is assumed that you are already familiar with IP addressing, and that you have used it on at least one type of system. The process is similar for every device because each system operates on the IP standard. A Juniper firewall is no exception.

Some Small Office Home Office (SOHO) class devices have a configuration mode called *port mode*.The SOHO devices have five physical interfaces. By default, there is one external *untr*ust interface and four *trus*t interfaces. However, you can change the port mode number to modify the distribution of ports.This feature can be used to extend the value of the SOHO class devices. In this section we will also look at the various options you can use when configuring a network interface using the built-in PPPoE client.

Types of Zones

There are three types of zones on a Juniper firewall. Each zone provides its own specific function, and each is used for a specific purpose.The *security zone* is the most commonly used zone type.The other two zone types are used much less commonly. One of these types is the *tunnel zone*.This type of zone is used for creating route-based VPNs.The other type of zone is the *function zone*.This zone is used for special purposes in high availability. Each type of zone is used to bind to an interface.

Security Zones

A security zone is used to break your network into logical segments.At a minimum, you need to define two security zones. Most Juniper firewall devices come with predefined zones that you can use.These zones are usually trust, untrust, and demilitarized zone (DMZ); however, this varies from device to device.You need to use two zones because this will allow you to separate your network into two parts. Each Juniper firewall can use only a limited number of zones. On some devices you can only have a few, while on the higher-end firewalls you could have several hundred zones.There is another type of security zone called a layer two zone, which is covered in a later chapter.

Tunnel Zones

Tunnel zones are used with tunnel interfaces.Tunnel interfaces are a special type of virtual interface that can terminate VPN traffic.Tunnel interfaces are first bound to the tunnel zone.

Then the tunnel zone is bound to a security zone, which is in turn bound to a physical interface. Tunnel zones are covered in depth in Chapters 11 and 14.

Function Zones

There are five types of function zone, and each is used to provide a single, unique function. The first type is the *null zone*. The null zone is used as a placeholder for interfaces that are not bound to a zone. The next type of function zone is the management (MGT) zone. This zone is used on out-of-band management interfaces. The high availability (HA) function zone is used for high availability interfaces. There are no configurable options for the HA zone. The *self zone* is used to host management connections. When using the remote management protocols to connect to, and manage, your Juniper device, you are connecting to the self zone. The last type of zone is the *virtual local area network* (VLAN) zone. It is used to host the VLAN1 interface. The VLAN1 interface is used to manage a Juniper firewall that is running in transparent mode.

Virtual Routers

As we have discussed, any device that uses the IP protocol must have a routing table that determines how to send information from one place to another. Juniper takes this idea to a whole new level by allowing you to have multiple routing tables, or virtual routers. Each virtual router has its own routing table that is complete and separate routing domain from other virtual routers. In this chapter, we will discuss the trust virtual router, and how to configure routes in it. A full explanation of routing is covered in Chapter 7.

Types of Interfaces

A Juniper firewall can contain several types of interfaces. An interface allows traffic to enter a zone and leave a zone. If you want an interface to pass traffic, you need to *bind* it to a zone. Once you bind an interface to a zone, you can apply an IP address to it. There are four types of interfaces: security zone interfaces, function zone interfaces, tunnel interfaces and loopback interfaces. As you can see, each type of interface has a corresponding zone type, except for the loopback interface, which is a special type of interface.

Security Zone Interfaces

Security zone interfaces are used primarily for passing traffic from one zone to another. In this category any type of interface related to physical interfaces or virtual interfaces belongs in this category. This is the interface that you will more commonly work with.

Physical Interfaces

Every Juniper firewall has some kind of physical interface. Physical interfaces are used to connect the firewall to the network. The naming convention of the physical interfaces varies based on the platform used. On the SOHO class of Juniper appliances, the interface names are based upon the zones. For example, the internal interface is named trust and the external interface is named untrust. On the Juniper-25 through the Juniper-208 products, the interfaces are named beginning with the media type, *Ethernet,* and then specified by the port number, such as *Ethernet1.* Juniper firewalls that are systems are named using the media type, slot number, and then the port number. For example, *Ethernet2/1* would be an Ethernet interface in slot number two, and port number one. The Juniper-500, ISG-2000, Juniper-5200, and Juniper-5400 belong to this category. Physical interfaces can be assigned a single primary IP address.

There are some situations where you may need to have multiple IP address on an interface. You can add multiple secondary IP addresses on each physical interface. When a secondary IP address is added, the Juniper firewall automatically adds a route between the two IP address segments. In this way you can connect the two segments. The route will automatically be removed if you delete the secondary IP address. If you want to segment these two networks, you can disable routing between the two. This will drop packets between the two, but the routing table will not be modified.

Secondary IP addresses have some restrictions as well. First, subnets between the multiple secondary interfaces *cannot* overlap. Secondly, interfaces in the untrust zone are unable to use multiple secondary IP addresses. If you choose to manage your firewall with the secondary IP address, it inherits the management properties of the primary interface. The secondary interface is unable to have a gateway, which means anything connecting to that interface *must* be on that local network.

Subinterfaces

Subinterfaces are used primarily with VLANs. For example, if you had a network that contained several VLANs, a Juniper firewall could act as a central point to connect between the separate VLANs. Each subinterface acts like a physical interface. All of the subinterfaces that are bound to a physical interface can use only the bandwidth that is provided by that interface. So if you have a single 100Mbps interface and several subinterfaces, they can only share the maximum bandwidth of that 100Mbps interface. The properties of a subinterface are otherwise identical to that of a physical interface. However, each subinterface *must* be assigned to a different VLAN and they *must* have a different IP subnet than all of physical interfaces, and the other subinterfaces defined on the firewall.

Aggregate Interfaces

When you create an aggregate interface you are binding multiple physical interfaces together to create one super interface. This interface acts as if it were a single physical interface. It provides cumulative bandwidth. So if you bound two 1-gigabit interfaces together, you would have a combined throughput of 2Gbps for that interface. If one of the interfaces were to fail, the remaining interface would continue to carry the traffic. However, that remaining interface can only carry as much traffic as the interface is rated for. So if you had two gigabit interfaces bound together, and you lost one, you would lower your maximum throughput to 1Gbps. This feature is only available on the Juniper-5200, and the Juniper-5400 system.

Redundant Interfaces

The redundant interface is much like the aggregate interface, but has only one of the two benefits of the aggregate interface. Redundant interfaces are *unable* to combine their bandwidth, and they provide redundancy only in case of a failure.

VLAN1 Interface

The VLAN1 interface is used for one purpose. When you configure a Juniper firewall to operate in transparent mode, the physical interfaces do not have IP addresses. You need a way to manage the firewall, and to terminate VPNs. The VLAN1 interface is a virtual security interface that can have an IP address assigned to it. This allows you to remotely manage your firewall, and to have an IP address to terminate VPNs. Using a Juniper firewall in transparent mode is covered in Chapter 9.

Virtual Security Interfaces

The last type of security interface is the virtual security interface (VSI). This type of interface is used when two Juniper devices are used in a high availability configuration. The two firewalls are combined to create a single entity called a virtual security device (VSD). Each device in the cluster defines a physical interface to create a VSI. This VSI has its own MAC address, its own IP address, and it operates like a physical interface. Configuring and using VSIs and VSDs are covered in Chapter 14.

Function Zone Interfaces

Function zone interfaces are special interfaces that are used for a single purpose, or task. These interfaces are dedicated to that task, and they cannot be used to do anything else.

Management Interfaces

Some Juniper firewalls contain an interface dedicated for management of the device. This interface is called the MGT interface. It allows you to separate the management of the device from the rest of the network by using this special interface. It is ensures that you will have bandwidth for management applications. Because the interface does not pass general-purpose traffic, it provides additional security by being dedicated only to management.

HA Interfaces

On Juniper systems, Juniper-500 and later models, each device contains two HA interfaces, HA1, and HA2. These interfaces are used exclusively for high availability. One interface passes control messages to each device. The second HA interface is used for traffic synchronization. If one of the interfaces fails, the remaining HA interface would provide both services. You must use a minimum of 100Mbps interfaces for high availability interfaces.

Some devices that can function in a HA cluster do not have dedicated interfaces for high availability. You can use a *virtual* HA interface, which is bound to a physical interface. This allows you to use the high availability configurations even though you do not have a dedicated interface to do so.

Tunnel Interfaces

A tunnel interface is used as a gateway to a VPN. This allows you to create a VPN configuration, and to bind that VPN to the tunnel interface. If you want to pass traffic to the VPN, you simply create a route on your firewall to point to the tunnel interface for the remote network. The VPN will be automatically established, and traffic will be encrypted before being sent to the remote gateway. Tunnel interfaces are used only for VPNs. VPNs are explained in Chapter 11.

Loopback Interfaces

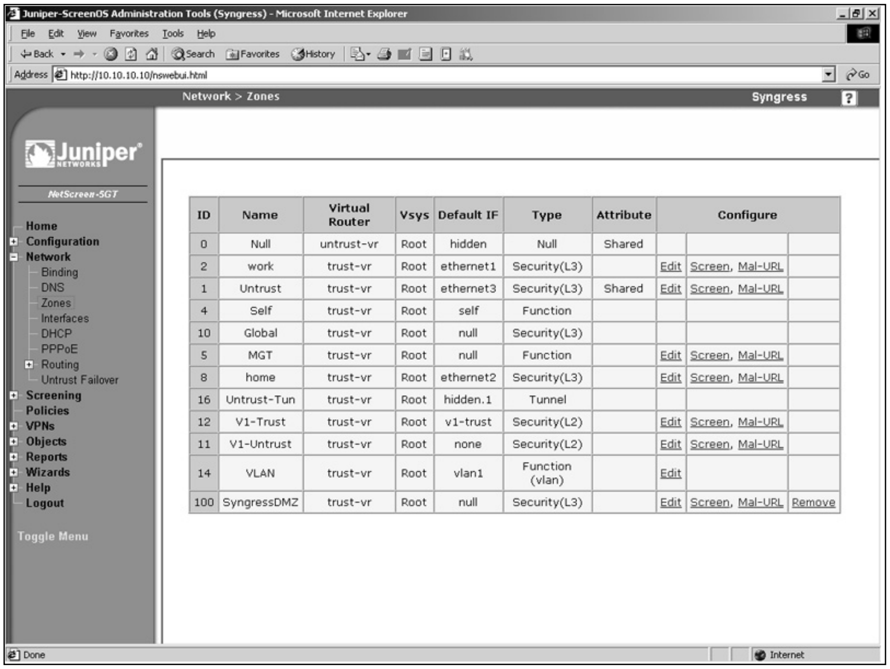
The last type of interface is the loopback interface. The loopback interface is a special interface that exists logically inside the firewall. A loopback interface is assigned to a zone, and it is not accessible from other zones unless you specify a policy to permit that traffic. A loopback interface can be used to manage your firewall.

Configuring Security Zones

Security zones are the core for creation of policies in the Juniper firewall. Policies are discussed in the next chapter. It is important that you become an expert on managing security zones. Once you have the security zones created and configured, it will be much easier for you to effectively create policies. As mentioned before, there will be several predefined security zones on your firewall. These are typically trust, untrust, and DMZ. The trust zone is designed for the internal protected network. The untrust zone is designed typically for the Internet or other undesirable places. The DMZ zone is used for your DMZ network. The trust zone and untrust zone have some unique properties that will be discussed later in this chapter. The predefined zones cannot be deleted, but they can be *modified*. In ScreenOS version 5.4 and later, these zones no longer count toward the upper limit of your device. Previously, you were allowed eight zones on the device, and three (Trust, Untrust, and DMZ) were already taken. You can now create eight user zones for the device.

First, we will inspect zone configurations on our device. This can be done from both the command line as well as the WebUI. To view the zones using the WebUI, access **Network | Zones**. A screen similar to the one shown in Figure 3.17 will be displayed.

Figure 3.17 Network Zones



ID	Name	Virtual Router	Vsys	Default IF	Type	Attribute	Configure		
0	Null	untrust-vr	Root	hidden	Null	Shared			
2	work	trust-vr	Root	ethernet1	Security(L3)		Edit	Screen, Mal-URL	
1	Untrust	trust-vr	Root	ethernet3	Security(L3)	Shared	Edit	Screen, Mal-URL	
4	Self	trust-vr	Root	self	Function				
10	Global	trust-vr	Root	null	Security(L3)				
5	MGT	trust-vr	Root	null	Function		Edit	Screen, Mal-URL	
8	home	trust-vr	Root	ethernet2	Security(L3)		Edit	Screen, Mal-URL	
16	Untrust-Tun	trust-vr	Root	hidden.1	Tunnel				
12	V1-Trust	trust-vr	Root	v1-trust	Security(L2)		Edit	Screen, Mal-URL	
11	V1-Untrust	trust-vr	Root	none	Security(L2)		Edit	Screen, Mal-URL	
14	VLAN	trust-vr	Root	vlan1	Function (vlan)		Edit		
100	SyngressDMZ	trust-vr	Root	null	Security(L3)		Edit	Screen, Mal-URL	Remove

To view the zones using the CLI, type the command **get zone**. You will see each zone listed in an output similar to the following:

```
Total 10 zones created in vsys Root - 5 are policy configurable.
Total policy configurable zones for Root is 5.
----------------------------------------------------------------------
  ID Name                Type    Attr    VR           Default-IF    VSYS
   0 Null                Null    Shared untrust-vr   hidden        Root
   1 Untrust             Sec(L3) Shared trust-vr     untrust       Root
   2 Trust               Sec(L3)        trust-vr     trust         Root
   4 Self                Func           trust-vr     self          Root
   5 MGT                 Func           trust-vr     null          Root
  10 Global              Sec(L3)        trust-vr     null          Root
  11 V1-Untrust          Sec(L2)        trust-vr     None          Root
  12 V1-Trust            Sec(L2)        trust-vr     v1-trust      Root
  14 VLAN                Func           trust-vr     vlan1         Root
  16 Untrust-Tun         Tun            trust-vr     hidden.1      Root
----------------------------------------------------------------------
```

Both the WebUI and the CLI look very similar regarding the way that zones are displayed. Both show the following information:

- **ID** The ID is used when doing debugging. It is important to understand where to locate the zone ID.
- **Name** The name is used as a label for the zone.
- **Type** This tells you what type of zone this is. As you can see, there are several of the zone types we have mentioned.
- **Attr** This specifies any additional attributes for the zone. *Shared* means that the zone is shared among all local virtual systems. By default, untrust and null are shared.
- **VR** This specifies which virtual router that the zone is operating in.
- **Default-IF** This identifies which interface is bound to the zone by default.
- **VSYS** This lists which vsys, or virtual system, the zone is bound to.

It is a simple task to create a new zone. However, before doing so, you should know the following information:

- **Name** A descriptive name for your zone. If you have a DMZ for Webservers, naming it WebDMZ is more helpful than if you chose DMZ02. This is a personal preference; however, if you are creating a layer two security zone, the zone must be prefixed with ***L2-***
- **Type of zone** You can create three types of zones: security layer three zones, security layer two zones, and tunnel zones.

This is the minimum information you would need to configure a zone. There are some additional options that can be configured on a zone.

- **Screen** Screen options are defense options that protect against specific attacks, and malicious traffic. Chapter 10 covers this topic in more detail.
- **Malicious URL protection** This feature provides pattern matching for HTTP traffic. It allows you to identify malicious universal resource locators (URLs) and to block those requests.
- **Block Intra-Zone Traffic** If this option is selected, it will allow you to block traffic between two interfaces bound to the same zone.
- **If TCP non SYN, send RESET back** This option is valid only for layer three security zones and tunnel zones. If this option is enabled, the Juniper firewall will send a RESET TCP packet to any host that sends a TCP segment with a TCP flag set to something other than SYN, and that does not belong to an existing session. If you have SYN checking enabled, from CLI type **set flow tcp-syn-check**, the unsolicited SYN packet is dropped, and the session initiator is notified to reset the TCP connection without initializing a new session in the session table. If the Juniper firewall were to skip sending the RESET notice, the system attempting to

initiate the session would continually send SYN packets until its connection attempt timed out. If SYN checking is disabled, the Juniper firewall passes the SYN packet to the end system if a policy permits it. This is useful for blocking packets that can be used in different types of network scans. If you are unsure if this will help you, it is best to leave it at the default setting.

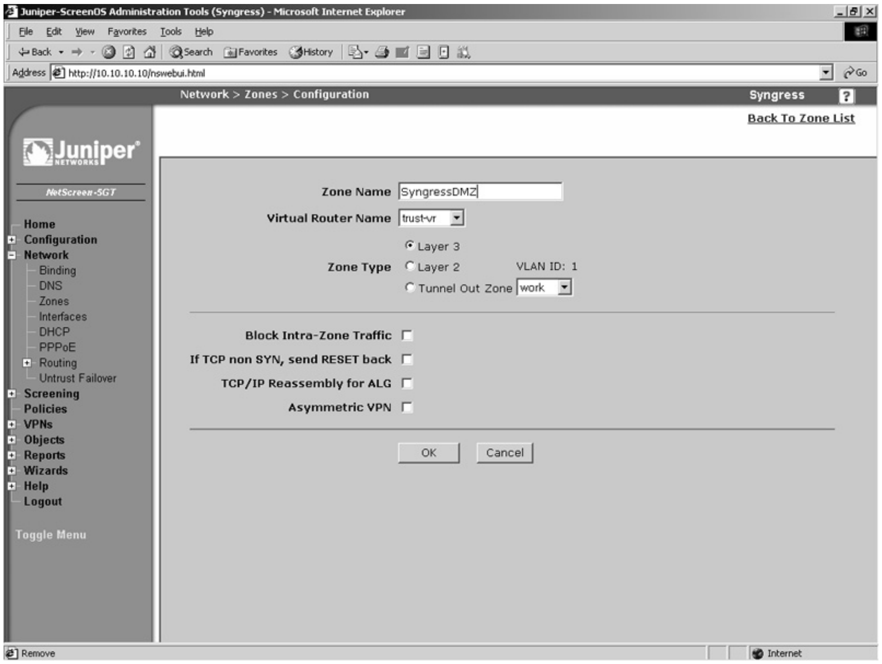
- **IP/TCP Reassembly for ALG (Application Layer Gateway)** If this option is selected, the Juniper firewall will reassemble fragmented HTTP and FTP packets before they are inspected. This will allow for more efficient enforcement for the Mal-URL engine to inspect the traffic. If you are not using the Mal-URL feature, leave this option off.
- **Shared Zone** This option is only available if you have a Juniper device that supports virtual systems. This option enables the zone to be shared among all virtual systems. Once you enable this option, you cannot disable it. You must either delete the zone, or disable all virtual systems, in order to disable it.
- **IP Classification** This option is used only with virtual systems. If this option is selected, the firewall will associate all traffic with this zone to a specific virtual system.
- **WebUI** (layer two zones only) Selecting this option enables management for the WebUI on this zone.
- **SNMP** (layer two zones only) Select this option to enable Simple Network Management Protocol (SNMP) services on this zone.
- **Telnet** (layer two zones only) Select this option to enable Telnet management on this zone.
- **SSL** (layer two zones only) Selecting this option enables SSL WebUI management on this zone.
- **SSH** (layer two zones only) Selecting this option enables SSH management on this zone.
- **NSM** (layer two zones only) Selecting this option enables NSM management on this zone.
- **Ping** (layer two zones only) Selecting this option enables *ping* from the firewall in this zone.
- **Ident-reset** (layer two zones only) Some services such as SMTP and FTP send an ident, or identification request. If you have Ident-reset enabled, it will reset this ident request and allow you access to that service.
- **WebAuth** (layer two zones only) Selecting this option enables Web authentication when traffic passes through the interface to which this zone is bound.

Generally, you would define the name for the new zone, and specify its type. However, it is always a good idea to familiarize yourself with available options when creating a new zone.

As we step through the zone creation process, we will focus on layer three zones, and the other zone types will be covered in later chapters. Use the following steps to create a zone using the WebUI:

1. Access **Network | Zones** and select **New**. A screen similar to Figure 3.18 will be displayed.

Figure 3.18 Create a New Zone



Zone Name: SyngressDMZ

Virtual Router Name: trust-vr

Zone Type: ● Layer 3 ○ Layer 2 VLAN ID: 1 ○ Tunnel Out Zone work

Block Intra-Zone Traffic □

If TCP non SYN, send RESET back □

TCP/IP Reassembly for ALG □

Asymmetric VPN □

2. Enter the **Zone Name**.
3. Ensure **trust-vr** is selected in the **Virtual Router Name** drop-down list.
4. In the **Zone Type** section, select the **Layer 3** option.
5. Press **OK**.

To create a zone using the CLI, type the command **set zone name *name***, where *name* is the name for the zone.

Once a zone is created, you can modify all of its properties except for its name. To change the name, you must delete the zone, and then re-create it using the desired name. Use the following steps to delete a zone using the WebUI:

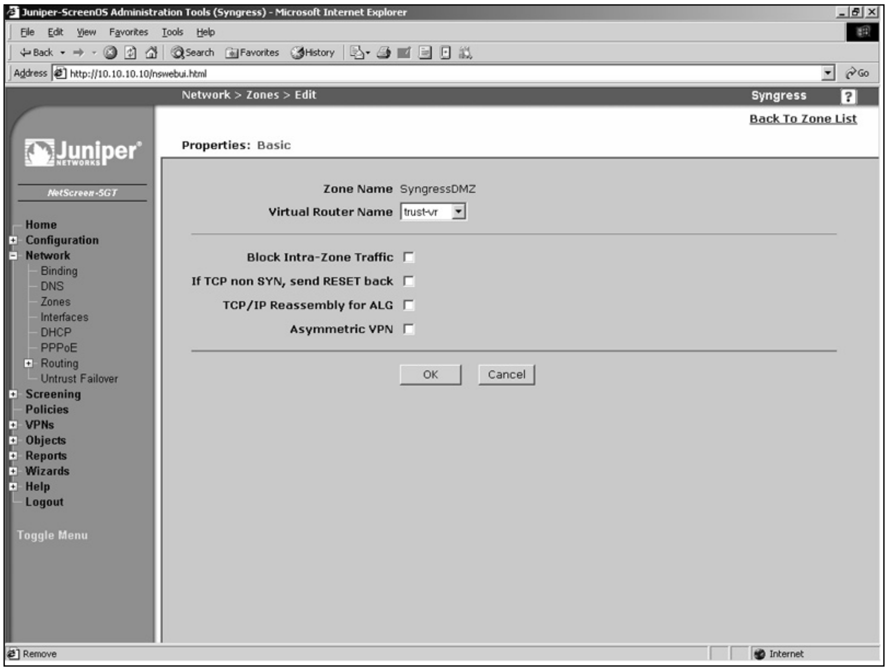
1. Access **Network** | **Zones** and select the **Remove** link of the zone you wish to delete.
2. Press **OK** to confirm.

To remove a zone using the CLI, type the command **unset zone *name***, where *name* is the name of the zone you wish to remove.

Use the following steps to modify an existing zone via the WebUI:

1. Access **Network** | **Zones** and select the **Edit** link of the zone you wish to modify. A screen similar to the one shown in Figure 3.19 will be displayed.

Figure 3.19 Edit a Zone



Network > Zones > Edit

Properties: Basic

Zone Name SyngressDMZ

Virtual Router Name trust-vr

Block Intra-Zone Traffic ☐

If TCP non SYN, send RESET back ☐

TCP/IP Reassembly for ALG ☐

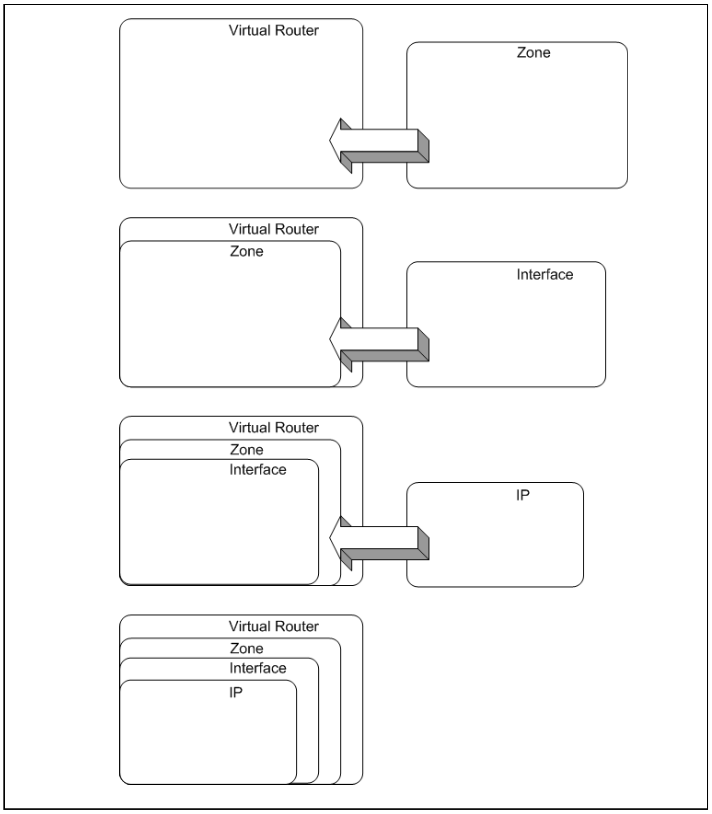
Asymmetric VPN ☐

2. Change the desired fields and select **OK**.

Configuring Your Firewall for the Network

When configuring a Juniper device, there are several steps you should perform before it can interact with the network. A physical interface must first be bound to a zone before it can be assigned an IP address. Figure 3.20 depicts the relationship between a zone and an interface. A zone is a *parent* to a physical interface, and the IP address is a *child* to the physical interface.

Figure 3.20 Zone Interface/IP Relationship



Binding an Interface to a Zone

First we will bind an interface to a zone. In this case we will use a NetScreen-5GT, and we will bind the trust zone to the trust interface. This can be done using either the WebUI or the CLI. However, to change the zone you must first remove the IP address by setting it to **0.0.0.0/0.** Afterward, you can select a new zone.

From the WebUI:

1. Access **Network** | **Interfaces**.
2. Press the **Edit** link for the **trust** interface.
3. Select **Trust** from the **Zone Name** drop-down list.
4. Press **OK**.

To bind an interface to a zone using the CLI, type the command **set interface *interfacename* zone *zonename***, where *interfacename* is the name of the interface you wish to bind, and *zonename* is the name of the zone you wish to bind the specified interface to.

Setting Up IP Addressing

We will now assign an IP address of 192.168.0.1 with a twenty-four-bit subnet mask to the interface. This can be done using either the WebUI or the CLI. If you want to modify the IP address of an interface, it is the accomplished using the same steps that you would use to set it up for the first time.

From the WebUI:

1. Access **Network | Interfaces** and select the **Edit** link for the **trust** interface, or whichever interface you want to bind.
2. Select the **Static IP** option.
3. Enter **192.168.0.1,** or whichever IP address you want to assign, in the IP address text field, and type **24, or another numerical value to represent the bits,** in the netmask text field.
4. Press **OK**.

To assign an IP address to an interface using the CLI, type the command **set interface *interfacename* ip *ipaddress netmask***, where *interfacename* is the name of the interface, *ipaddress* is the IP address you want to assign, and *netmask* is the netmask.

Configuring the DHCP Client

Here we take the Juniper-5GT and set the untrust interface to receive an IP address from the Dynamic Host Configuration Protocol (DHCP). This will allow the Juniper firewall to be plugged into any cable modem, DSL, or internal network to seamlessly receive an IP address.

From the WebUI:

1. Access **Network | Interfaces** and select the **Edit** link for the **untrust** interface, or whichever interface you want to configure.
2. Select the **Obtain IP using DHCP** option.
3. Enable the **Automatic update of DHCP server parameters** option.
4. Press **OK**.

To set this configuration using the CLI, type the command **set interface *interfacename* dhcp client enable**, where *interfacename* is the name of the interface you wish to configure.

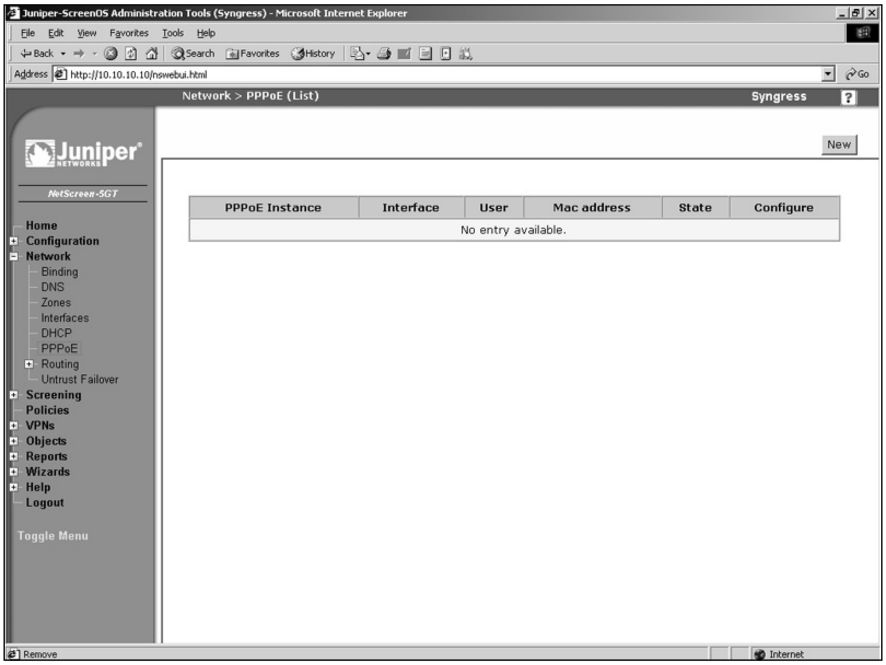
Using PPPoE

Some DSL service providers require the use of a protocol called Point-to-Point Protocol over Ethernet (PPPoE). This requires an additional configuration. You must configure a PPPoE instance, bind to an interface, and then configure the interface to use PPPoE to negotiate the connection. You will then get an IP address from PPPoE, just as you would with DHCP.

From the WebUI:

1. Access **Network | PPPoE**. A screen similar to Figure 3.21 will be displayed.

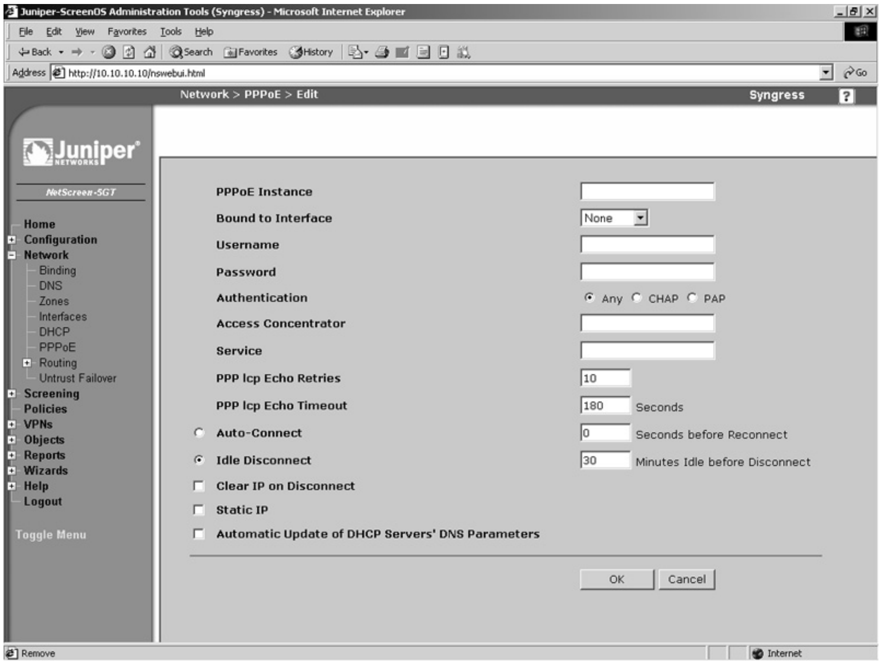
Figure 3.21 Network PPPoE



PPPoE Instance	Interface	User	Mac address	State	Configure
No entry available.					

2. Press **New**. A screen similar to the one shown in Figure 3.22 will be displayed.
3. Use the PPPoE Instance field to enter the name.
4. Choose **untrust** from the **Bound to Interface** drop-down list, or whichever interface you wish to bind.
5. Enter your ISP-provided username and password in the **Username** and **Password** fields, respectively.
6. Select the **Any Authentication** option.
7. Enable the **Automatic Update of DHCP Servers' DNS Parameters** option.
8. Press **OK**.

Figure 3.22 Network | PPPoE | Edit



PPPoE Instance
Bound to Interface: None
Username
Password
Authentication: ● Any ○ CHAP ○ PAP
Access Concentrator
Service
PPP lcp Echo Retries: 10
PPP lcp Echo Timeout: 180 Seconds
○ Auto-Connect: 0 Seconds before Reconnect
● Idle Disconnect: 30 Minutes Idle before Disconnect
□ Clear IP on Disconnect
□ Static IP
□ Automatic Update of DHCP Servers' DNS Parameters

To create a PPPoE connection via the CLI, type the command **set pppoe name "*name*" username "*username*" password "*password*"**, ensuring that you include the quotation marks, and where *name* is the name of the interface, *username* is your ISP-provided username, and *password* is your ISP-provided password.

Interface Speed Modes

By default, all of the ports on your Juniper firewall are auto-sensing. This means they negotiate Ethernet settings such as speed and duplex. Regardless of the auto-sensing feature, you will want to hard code these settings to ensure that you are getting proper performance out of your network. This configuration can be done only from the CLI. In the following example, we will hard code the trust interface port 4 interface to 100Mbps full duplex.

```
Syngress-> get interface trust port phy
Port 1:  link is down, 10 Mbps, forced to half duplex
Port 2:  link is down, 10 Mbps, forced to half duplex
Port 3:  link is down, 10 Mbps, forced to half duplex
Port 4:  link is up, 100 Mbps, auto negotiated to full duplex
Syngress-> set int trust port 4 phy full 100mb
Syngress-> get interface trust port phy
Port 1:  link is down, 10 Mbps, forced to half duplex
Port 2:  link is down, 10 Mbps, forced to half duplex
Port 3:  link is down, 10 Mbps, forced to half duplex
Port 4:  link is up, 100 Mbps, forced to full duplex
```

Port Mode Configuration

Some devices in the SOHO product line support *port mode*. These devices contain one untrust, or external port, and four internal ports. By default, the four internal ports are called trust, and they are bound to the trust zone. However, there are four other modes you can use; however, the *extended* mode requires an additional license. When you change between port modes, this removes your existing configuration. If you clear your configuration by using the *unset all* command, the port mode setting will be unaffected. In Table 3.3 you can see the differences between the different modes.

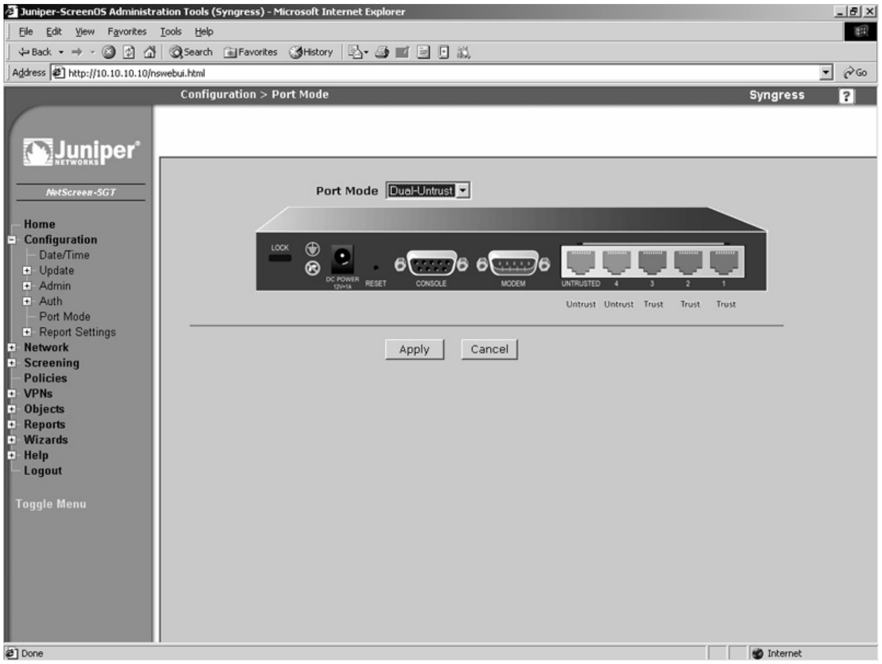
Table 3.3 Port Modes

Port	Trust-Untrust		Home-Work		Dual Untrust		Combined		Extended	
	Int	Zone	Int	Zone	Int	Zone	Int	Zone	Int	Zone
Untrusted	Untrust	Untrust	Eth3	Untrust	Eth3	Untrust	Eth4	Untrust	Eth3	Untrust
1	Trust	Trust	Eth1	Work	Eth1	Trust	Eth1	Work	Eth1	Trust
2	Trust	Trust	Eth1	Work	Eth1	Trust	Eth2	Home	Eth1	Trust
3	Trust	Trust	Eth2	Home	Eth1	Trust	Eth2	Home	Eth2	DMZ
4	Trust	Trust	Eth2	Home	Eth2	Untrust	Eth3	Untrust	Eth2	DMZ
Modem	Serial	Null	Serial	Null	Serial	N/A	N/A	N/A	Serial	Untrust

Port	DMZ-Dual-Untrust		Dual-DMZ	
	Int	Zone	Int	Zone
Untrusted	Eth4	Untrust	Eth5	Untrust
1	Eth1	Trust	Eth1	Trust
2	Eth1	Trust	Eth2	DMZ
3	Eth2	DMZ	Eth3	DMZ2
4	Eth4	Untrust	Eth4	Untrust
Modem	Serial	Null	Serial	Null

You can change the port mode settings from either the CLI or the WebUI. You can see the port mode WebUI configuration in Figure 3.23.

Figure 3.23 Port Mode Configuration



Port Mode Dual-Untrust

Use the following steps to change the port mode settings via the WebUI:

1. Access **Configuration | Port Mode**.
2. Select the desired mode from the **Port Mode** drop-down list.
3. Press **Apply**, then select **OK** to confirm.Your current configuration will be erased and the device will reboot.

To change modes using the CLI, type the command **exec port-mode combined** and press **y** to confirm.Your current configuration will be erased, and the device will reboot.

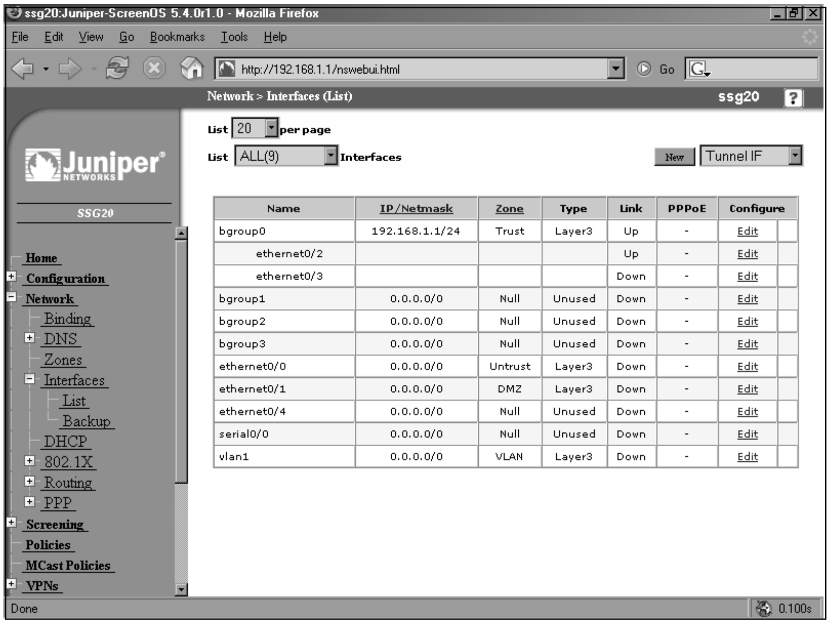
Bridge Groups

The SSG 5 and SSG 20 firewalls offer the option of configuring *bridge groups*.This new option replaces port modes.The bridge group option is more flexible because you are not subject to the limitations of the port mode.You can configure up to four bridge groups per unit.Another benefit is that you can also bind wireless interfaces to a bridge group.The wireless interfaces were previously independent of the LAN interfaces.You could not have the same IP subnet on the LAN and the Wireless LAN (WLAN) at the same. However, bridge groups allow you to bridge them together.The best part is you do not have to reboot the unit for this to take effect.

Use the following steps to change the bridge group settings via the WebUI:

1. Access **Network | Interfaces | List.**
2. Select the Bridge Group you want to edit and select **Edit** from the **Configure** column (see Figure 3.24).
3. Under the Bridge Groups **properties** section at the top select **Bind Port.**
4. You can now select and deselect the interfaces you want to add to the bridge group by selecting the checkbox to the right of the interface name.

Figure 3.24 Bridge Group Configuration



List 20 per page

List ALL(9) Interfaces

Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure
bgroup0	192.168.1.1/24	Trust	Layer3	Up	-	Edit
ethernet0/2				Up	-	Edit
ethernet0/3				Down	-	Edit
bgroup1	0.0.0.0/0	Null	Unused	Down	-	Edit
bgroup2	0.0.0.0/0	Null	Unused	Down	-	Edit
bgroup3	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/0	0.0.0.0/0	Untrust	Layer3	Down	-	Edit
ethernet0/1	0.0.0.0/0	DMZ	Layer3	Down	-	Edit
ethernet0/4	0.0.0.0/0	Null	Unused	Down	-	Edit
serial0/0	0.0.0.0/0	Null	Unused	Down	-	Edit
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit

Use the following commands to add an interface to a bridge group via the CLI:

```
Syngress-> get int

A - Active, I - Inactive, U - Up, D - Down, R - Ready

Interfaces in vsys Root:
Name           IP Address        Zone        MAC            VLAN State VSD
serial0/0      0.0.0.0/0         Null        0014.f69b.e3cd    -   D   -
eth0/0         0.0.0.0/0         Untrust     0014.f69b.e3c0    -   D   -
eth0/1         0.0.0.0/0         DMZ         0014.f69b.e3c5    -   D   -
eth0/4         0.0.0.0/0         Null        0014.f69b.e3c8    -   D   -
bgroup0        192.168.1.1/24    Trust       0014.f69b.e3c9    -   U   -
```

```
  eth0/2       N/A              N/A         N/A              -   U   -
  eth0/3       N/A              N/A         N/A              -   D   -
bgroup1        0.0.0.0/0        Null        0014.f69b.e3ca   -   D   -
bgroup2        0.0.0.0/0        Null        0014.f69b.e3cb   -   D   -
bgroup3        0.0.0.0/0        Null        0014.f69b.e3cc   -   D   -
vlan1          0.0.0.0/0        VLAN        0014.f69b.e3cf   1   D   -
null           0.0.0.0/0        Null        N/A              -   U   0
Syngress-> set int bg0 port e0/4
Syngress-> get int

A - Active, I - Inactive, U - Up, D - Down, R - Ready

Interfaces in vsys Root:
Name           IP Address       Zone        MAC            VLAN State VSD
serial0/0      0.0.0.0/0        Null        0014.f69b.e3cd   -   D   -
eth0/0         0.0.0.0/0        Untrust     0014.f69b.e3c0   -   D   -
eth0/1         0.0.0.0/0        DMZ         0014.f69b.e3c5   -   D   -
bgroup0        192.168.1.1/24   Trust       0014.f69b.e3c9   -   U   -
  eth0/2       N/A              N/A         N/A              -   U   -
  eth0/3       N/A              N/A         N/A              -   D   -
  eth0/4       N/A              N/A         N/A              -   D   -
bgroup1        0.0.0.0/0        Null        0014.f69b.e3ca   -   D   -
bgroup2        0.0.0.0/0        Null        0014.f69b.e3cb   -   D   -
bgroup3        0.0.0.0/0        Null        0014.f69b.e3cc   -   D   -
vlan1          0.0.0.0/0        VLAN        0014.f69b.e3cf   1   D   -
null           0.0.0.0/0        Null        N/A              -   U   0
Syngress->
```

Bridge Group Caveats

As with any new features there are a few caveats with the bridge group feature. It is important to point these out these potential problem areas before you get tripped up by one of them:

- Policies cannot be configured between ports in a bridge group (Bgroup). Traffic is switched locally and is not processed by the ScreenOS engine
- You cannot bind Eth0 and wireless port into the same Bgroup interface. This restriction applies only to Eth0 port.
- Spanning tree is not supported. Make sure you do not create a loop in network; otherwise, there will be broadcast storm.

- Transparent mode is not supported *if* Wired and Wireless port are in the *same* Bgroup.
- ScreenOS will allow creation of a VLAN subinterface on a Bgroup while wireless port is bound to this Bgroup. However, after the VLAN subinterface is created it will include only Ethernet ports in the Bgroup. Wireless port will not be a member port.

Configuring Basic Network Routing

When you want to connect to a remote network, you must inform your firewall of its location. You do this by adding network routes to your firewall. These routes tell the firewall where the remote network can be found. In this section we will discuss adding a static route to access a remote network. We will also be adding a default route. A default route is also known as the *route of last resort*. So if a packet on a device needs to get to a location, and no other routes on the device are able to identify the next gateway to send it to, it will use the default gateway. When a system is determining which route to use, it will always use the most specific route first.

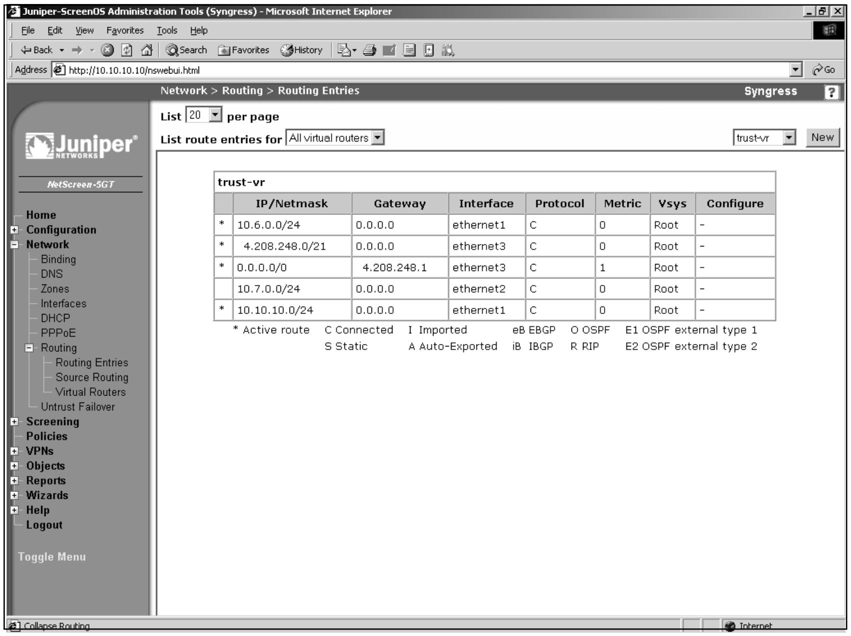
In this example we add a static route on our Juniper firewall to determine the next *hop* for the 192.168.1.0/24 network. For this example, we use only the trust-vr. Chapter 7 covers routing with virtual routers. Adding routes can be accomplished from either the WebUI or the CLI. When you add a route, there are several pieces of information you need to know beforehand:

- **Remote network** Identify the remote network route that you want to add. In our example we will be using 192.168.1.0/24. You can also add routes for single hosts such as 192.168.1.20/32.
- **Interface or virtual router** The interface is whichever physical interface on which the gateway is located.
- **Next hop gateway** You need to know which system can take your packets to the specified remote network. This device must be capable of connecting to the remote network, or if not, it must know where the remote network can be located.
- **Metric** The metric is a preference number, with the lowest number having the highest priority. All directly connected networks have a metric of zero. All static routes have a default metric of one. There may be cases in which you need to add the same route twice, the preferred route with the lower metric and the less preferred route with the higher metric. If the first route is unavailable, the firewall will use the next route.

Our first example of adding a static route in the WebUI.

1. Access **Network | Routing | Routing Entries**. A screen similar to the one shown in Figure 3.25 will be displayed.

Figure 3.25 Routing Entries



List 20 per page

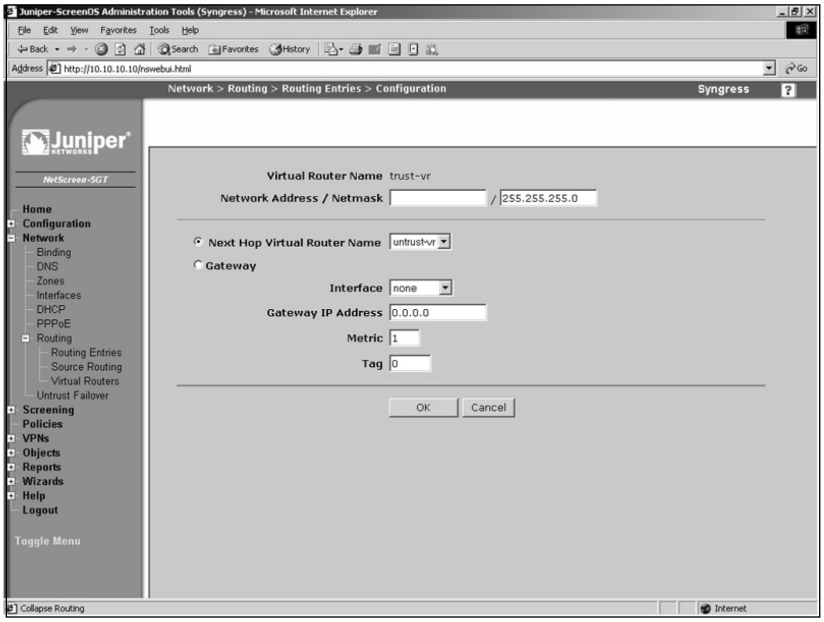
List route entries for All virtual routers — trust-vr — New

trust-vr

	IP/Netmask	Gateway	Interface	Protocol	Metric	Vsys	Configure
*	10.6.0.0/24	0.0.0.0	ethernet1	C	0	Root	-
*	4.208.248.0/21	0.0.0.0	ethernet3	C	0	Root	-
*	0.0.0.0/0	4.208.248.1	ethernet3	C	1	Root	-
	10.7.0.0/24	0.0.0.0	ethernet2	C	0	Root	-
*	10.10.10.0/24	0.0.0.0	ethernet1	C	0	Root	-

* Active route C Connected I Imported eB EBGP O OSPF E1 OSPF external type 1
S Static A Auto-Exported iB IBGP R RIP E2 OSPF external type 2

Figure 3.26 Configure a Routing Entry



Virtual Router Name trust-vr

Network Address / Netmask [ ] / 255.255.255.0

● Next Hop Virtual Router Name untrust-vr

○ Gateway

Interface none

Gateway IP Address 0.0.0.0

Metric 1

Tag 0

OK Cancel

2. Use the drop-down list in the upper right-hand corner to select the virtual router and select **New**. In our example, we will select **trust-vr**. A screen similar to the one shown in Figure 3.26 will be displayed.
3. Enter the **Network Address/Netmask**.
4. Select the **Gateway** option.
5. Use the **Interface** drop-down list to select the interface (gateway) that is the next hop and use the **Gateway IP Address** field to enter the gateway's IP address.
6. Press **OK**.

To add a static route using the CLI, type the command **set route *ipaddress/netmask* interface *interfacename* gateway *gatewayip***, where *ipaddress* is the virtual router's IP address, *netmask* is the virtual router's netmask, *interfacename* is the next hop gateway, and *gatewayip* is the IP address of the next hop gateway.

To remove a static route via the WebUI, access **Network | Routing | Routing Entries** and select the **Remove** link of the route you wish to delete. Press **OK** to confirm.

The most important and most used route on a firewall is the default route, or route of last resort. This route is used when no other route matches the traffic. Typically this route will point to your Internet router. If you are running either DHCP or PPPoE, your default route will likely come from that source. However, there may be times when you need to add your own default route. This can be done from either the WebU or the CLI. It is much like adding a static route.

From the WebUI:

1. Access **Network | Routing | Routing Entries**.
2. Select your virtual router from the drop-down list in the upper right-hand corner and select **New**.
3. Enter **0.0.0.0** in the **Network Address** field and type **0** in the **Netmask** field.
4. Select the **Gateway** option.
5. Use the **Interface** drop-down list to select the interface that acts as the next hop gateway and enter the **Gateway IP Address**.
6. Press **OK**.

To remove the static route using the CLI, type the command **set route 0.0.0.0/0 interface *interfacename* gateway *gatewayip***, where *interfacename* is the next hop gateway and *gatewayip* is the gateway's IP address.

Configuring System Services

On your Juniper firewall there are some other notable devices to configure. Configuring the time is very important for being able to correlate information in the logs to a specific time;

therefore, configuration of the local clock is critical. Also, the firewall executes specific events at given times. If the time is configured improperly, this can prevent events from occurring at the correct time.

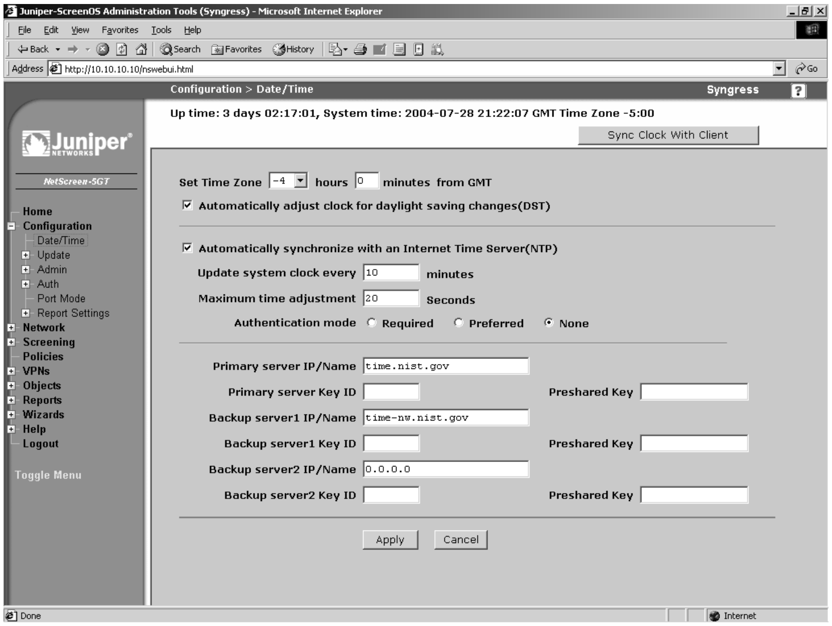
Most Juniper firewalls contain a built-in DHCP server. Typically, you can have a server on each interface. This allows you to manage your internal IP addressing from a single location. All Juniper firewalls are able to query DNS servers. This allows them to resolve hostnames to IP addresses. It is important to have working DNS servers configured on your firewall in case you want to use the network to synchronize time to an NTP server.

There is a great deal of information generated by your firewall in the form of logs. Because all Juniper firewalls have limited space for storing logs, you may want to be able to send this logging information to a remote system. We will look at how to configure, and use, two separate remote log repositories. Finally, we will look at license keys. These keys unlock the features of your firewall device. We will investigate how license keys work and how to update your license key.

Setting the Time

Every Juniper device contains an internal clock that runs continually while the device is powered on. You can manually set the clock from either the WebUI or the CLI. Ideally, you would configure your firewall to contact a timeserver using the Network Time Protocol (NTP) To ensure that the clock is set to the correct time, the steps shown in Figure 3.27 replicate the time configuration page from the WebUI, and it is used to manually set the time on your firewall,.

Figure 3.27 Date/Time Configuration



Up time: 3 days 02:17:01, System time: 2004-07-28 21:22:07 GMT Time Zone -5:00

Set Time Zone -4 hours 0 minutes from GMT

☑ Automatically adjust clock for daylight saving changes(DST)

☑ Automatically synchronize with an Internet Time Server(NTP)

Update system clock every 10 minutes

Maximum time adjustment 20 Seconds

Authentication mode ○ Required ○ Preferred ● None

Primary server IP/Name	time.nist.gov		
Primary server Key ID		Preshared Key	
Backup server1 IP/Name	time-nw.nist.gov		
Backup server1 Key ID		Preshared Key	
Backup server2 IP/Name	0.0.0.0		
Backup server2 Key ID		Preshared Key	

From the WebUI:

1. Access **Configuration | Date/Time**.
2. Use the **Set Time Zone** fields to specify the difference between your time zone and GMT (Greenwich Mean Time).
3. Enable the **Automatically adjust clock for daylight saving changes (DST)** option.
4. Press **Apply**.
5. Press the **Sync Clock with Client** button and select **Yes** to confirm.

```
    To set the timezone and date/time using CLI, type the following commands:
```

```
Syngress-> set clock timezone vv
Syngress-> set clock MM/DD/YYYY hh:mm:ss
```

Where vv in the first command is the difference between local time and Greenwich Mean Time (GMT) (expressed as + or -, for example, +3 or –5), and where MM/DD/YYYY is the month, date, and year, and e hh:mm:ss is the hour, minute, and second.

Setting up timeservers to sync with the NTP protocol allows up to subsecond accuracy for time synchronization. NTP is a free service, and every system should use it. The only time you should not use it is when you want the firewall to generate no traffic. NTP can be configured from either the CLI, or the WebUI. However, you can force NTP synchronization only from the CLI. Figure 3.26 shows the time screen that contains the NTP settings.

From the WebUI:

1. Access **Configuration | Date/Time**.
2. Enable the **Automatically synchronize with an Internet Time Server (NTP)** option.
3. Enter **time.nist.gov** in the **Primary server IP/Name** field.
4. Enter **time-nw.nist.gov** in the **Backup server1 IP/Name** field.
5. Press **Apply**.

To synchronize the time via the CLI, type the following commands:

```
Syngress-> set ntp timezone -5
Syngress-> set ntp server time.nist.gov
Syngress-> set ntp server backup1 time-nw.nist.gov
Syngress-> set clock ntp
Syngress-> exec ntp update
```

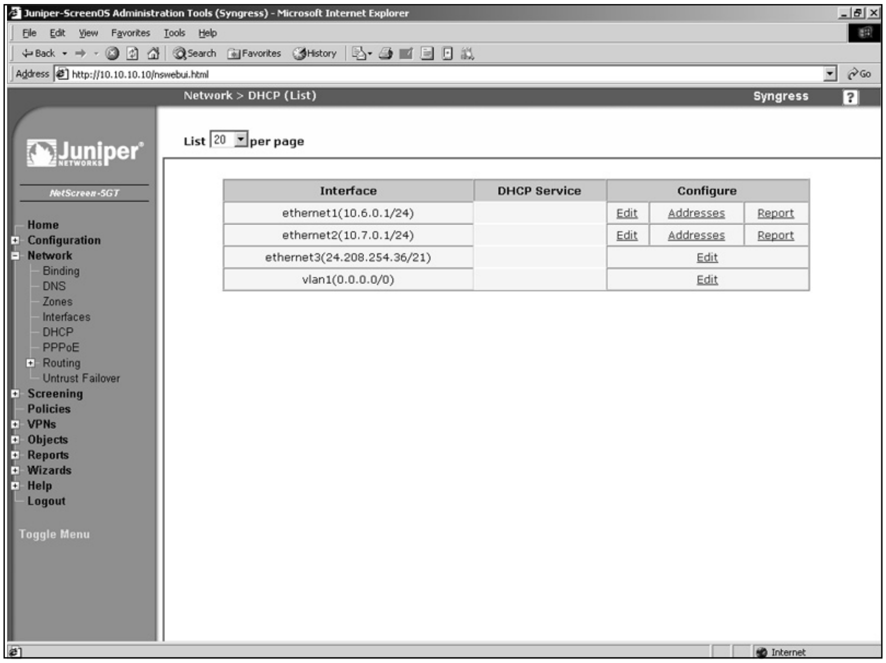
When asked if you want to update the system clock, press **y** for yes.

Finally, you can use Secure Network TimeProtocol (SNTP). This provides MD5-based authentication of each packet to ensure that the packet is from the specified server. To use authentication, you must assign a key ID, and a preshared key for every timeserver you configure. Additionally, you must configure whether authenticaton is required, or simply preferred.

DHCP Server

Juniper firewall devices can act as a DHCP server to allow the firewall to control IP address allocation on the network. Any Juniper device is capable of hosting up to eight DHCP servers. The server can assign IP addresses from a pool, or from a reserved list based on MAC address. Another feature of the DHCP server on the Juniper firewall is that it can determine whether another DHCP server is running on the network. This can prevent a conflict between two servers concurrently handing out IP addresses. In our example, we will set up a DHCP server on the Eth2 interface of a Juniper-5GT. We will assign a pool of IP addresses as shown in Figure 3.28, and create one reservation based upon MAC address. DHCP servers can be configured from either the WebUI or the CLI.

Figure 3.28 DHCP List



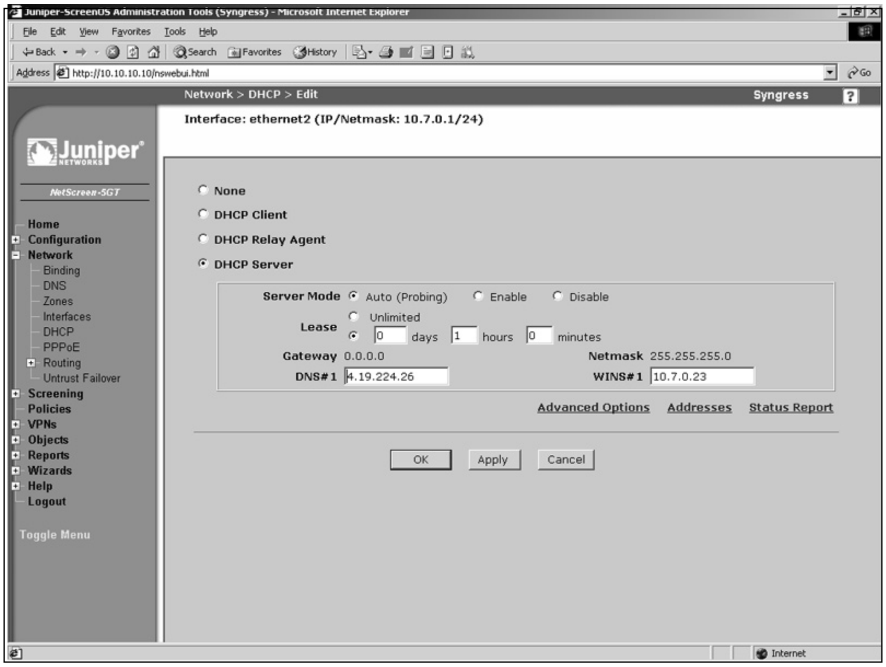
List 20 per page

Interface	DHCP Service	Configure		
ethernet1(10.6.0.1/24)		Edit	Addresses	Report
ethernet2(10.7.0.1/24)		Edit	Addresses	Report
ethernet3(24.208.254.36/21)		Edit		
vlan1(0.0.0.0/0)		Edit		

From the WebUI:

1. Access **Network | DHCP**.
2. Locate the Ethernet2 interface and select its **Edit** link. A screen similar to the one shown in Figure 3.29 will be displayed.

Figure 3.29 Edit a DHCP Entry



Network > DHCP > Edit

Interface: ethernet2 (IP/Netmask: 10.7.0.1/24)

○ None
○ DHCP Client
○ DHCP Relay Agent
● DHCP Server

Server Mode ● Auto (Probing) ○ Enable ○ Disable

Lease ○ Unlimited
● 0 days 1 hours 0 minutes

Gateway 0.0.0.0 Netmask 255.255.255.0

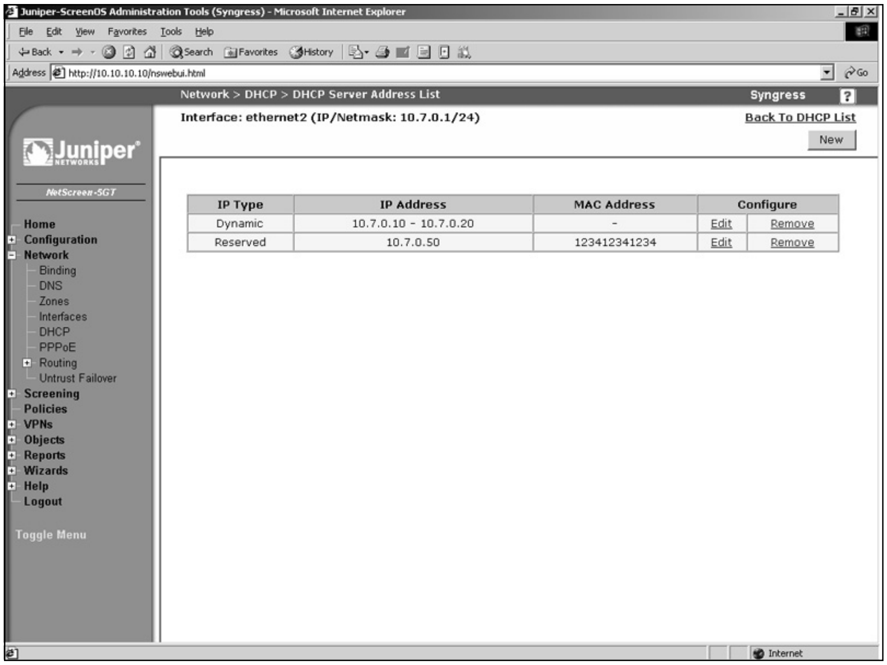
DNS#1 4.19.224.26 WINS#1 10.7.0.23

Advanced Options Addresses Status Report

OK Apply Cancel

3. Enable the **DHCP Server** option.
4. For **Server Mode**, enable the **Auto (Probing)** option.
5. In the **Lease** section, select the option button that allows you to enter a specific time, and then enter the desired **days**, **hours**, and **minutes**.
6. Use the **DNS#1** field to enter the IP address of the primary DNS server.
7. Use the **WINS#1** field to enter the IP address of the primary WINS server.
8. Press **OK**. The DHCP list will be displayed.
9. Locate the ethernet2 interface in the list and select its **Addresses** link. A screen similar to the one shown in Figure 3.30 will be displayed.
10. Press **New**.
11. Ensure the **Dynamic** option is selected.
12. Use the **IP Address Start** field to enter the first IP address in the address pool.
13. Use the **IP Address End** field to enter the last IP address in the address pool.
14. Press **OK**. The DHCP Server Address List screen will be displayed.
15. Press **New**.
16. Select the **Reserved** option.

Figure 3.30 DHCP Server Address List



Network > DHCP > DHCP Server Address List

Interface: ethernet2 (IP/Netmask: 10.7.0.1/24)

IP Type	IP Address	MAC Address	Configure	
Dynamic	10.7.0.10 - 10.7.0.20	-	Edit	Remove
Reserved	10.7.0.50	123412341234	Edit	Remove

17. Use the **IP Address** field to enter the IP address that you wish to reserve.
18. Use the **Ethernet Address** field to enter the MAC address of the device for which you wish to reserve the specified IP address.
19. Press **OK**.

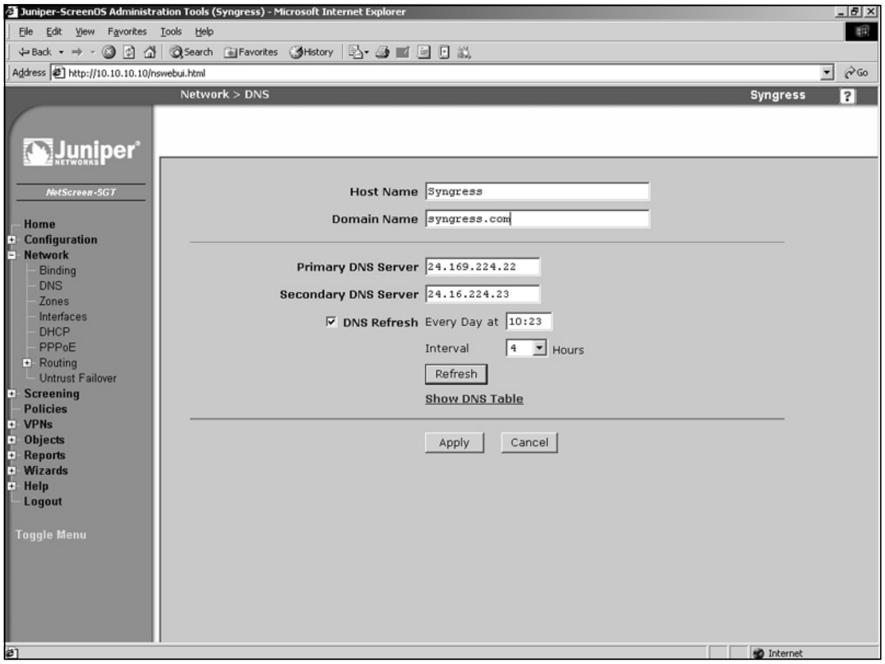
Use the following commands to configure the DHCP server via the CLI:

```
Syngress-> set interface ethernet2 dhcp server auto
Syngress-> set interface ethernet2 dhcp server enable
Syngress-> set interface ethernet2 dhcp server option lease 60
Syngress-> set interface ethernet2 dhcp server option dns1 10.7.0.23
Syngress-> set interface ethernet2 dhcp server option wins1 10.7.0.23
Syngress-> set interface ethernet2 dhcp server option netmask 255.255.255.0
Syngress-> set interface ethernet2 dhcp server ip 10.7.0.10 to 10.7.0.20
Syngress-> set interface ethernet2 dhcp server ip 10.7.0.50 mac 123412341234
```

DNS

Setting up your Juniper firewall as a DNS client is relatively simple.The firewall keeps a local cache of DNS entries, and you must decide when you want the cache to be cleared. DNS can be configured from either the WebUI or the CLI. Figure 3.31 shows the WebUI screen for configuring DNS.The hostname and domain name are also set from this page. If you are using a DHCP, or PPPoE, client on your firewall, the DNS server settings and domain name may be passed down and configured for you.

Figure 3.31 DNS Configuration



Host Name: Syngress

Domain Name: syngress.com

Primary DNS Server: 24.169.224.22

Secondary DNS Server: 24.16.224.23

☑ DNS Refresh Every Day at 10:23

Interval 4 Hours

From the WebUI:

1. Access **Network | DNS**.
2. Enter a **Host Name** and a **Domain Name**.
3. Enter the IP address of the **Primary DNS Server** and the **Secondary DNS Server**.
4. Enable the **DNS Refresh** option and enter the refresh time and frequency.
5. Press **Apply**.

Enter the following commands to configure the DNS server via the CLI:

```
Syngress->set hostname Syngress
Syngress-> set domain syngress.com
Syngress-> set dns host dns1 2.32.23.23
Syngress-> set dns host dns2 2.32.23.24
Syngress-> set dns host schedule 10:23 interval 4
```

SNMP

Simple Network Management Protocol (SNMP) allows remote administrators to view data statistics on a Juniper device. It also allows a Juniper device to send information to a central server. Juniper firewalls support SNMPv1 and SNMPv2c. It also supports the Management Information Base two (MIB II), or standard groups. The SNMP agent supports sending the following traps.

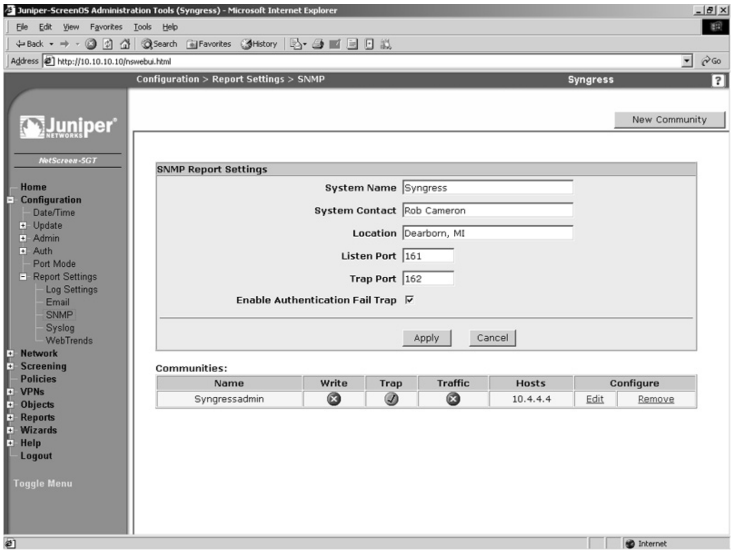
- Cold Start Trap
- Trap for SNMP Authentication Failure
- Traps for System Alarms
- Traps for Traffic Alarms

By default, the SNMP manager requires no configuration. This prevents unauthorized viewing of the system based upon default parameters. To configure your Juniper device for SNMP, you must configure community strings, SNMP host addresses, and permissions. In our configuration example, we will first set up the basic system information, and then we will create a new community. This can be done from either the WebUI or the CLI. You can create up to three communities, with up to eight IP ranges in each. An IP range can consist of a single host, or a network. If you configure a network, those defined IP addresses can poll only the device.

Use the following steps to configure SNMP via the WebUI:

1. Access **Configuration | Report Settings | SNMP**. A screen similar to the one shown in Figure 3.32 will be displayed.

Figure 3.32 SNMP Report Settings



SNMP Report Settings

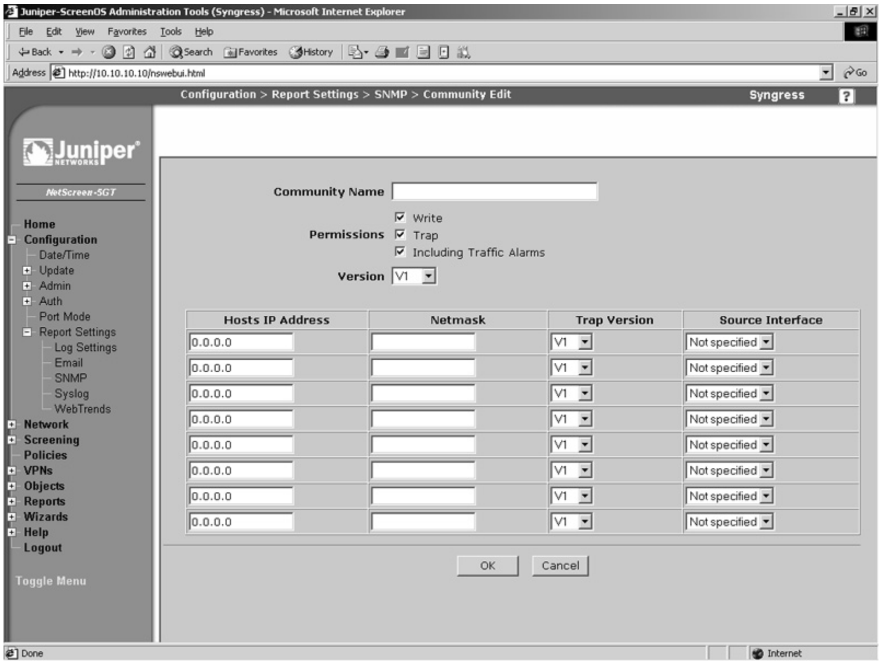
System Name: Syngress
System Contact: Rob Cameron
Location: Dearborn, MI
Listen Port: 161
Trap Port: 162
Enable Authentication Fail Trap ☑

Communities:

Name	Write	Trap	Traffic	Hosts	Configure	
Syngressadmin	☒	✓	☒	10.4.4.4	Edit	Remove

2. Enter the desired **System Name**, **System Contact**, and **Location**.
3. Enter the port numbers of the **Listen Port** and the **Trap Port**.
4. Ensure that the **Enable Authentication Fail Trap** option is enabled.
5. Press **Apply**.
6. Press **New Community**. A screen similar to the one shown in Figure 3.33 will be displayed.

Figure 3.33 New Community


Juniper-ScreenOS Administration Tools (Syngress) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://10.10.10.10/nswebui.html
Go
Configuration > Report Settings > SNMP > Community Edit
Syngress
Juniper NETWORKS
NetScreen-5GT
Home
Configuration
Date/Time
Update
Admin
Auth
Port Mode
Report Settings
Log Settings
Email
SNMP
Syslog
WebTrends
Network
Screening
Policies
VPNs
Objects
Reports
Wizards
Help
Logout
Toggle Menu
OK
Cancel
Done
Internet

Community Name

Permissions ☑ Write ☑ Trap ☑ Including Traffic Alarms

Version V1

Hosts IP Address	Netmask	Trap Version	Source Interface
0.0.0.0		V1	Not specified
0.0.0.0		V1	Not specified
0.0.0.0		V1	Not specified
0.0.0.0		V1	Not specified
0.0.0.0		V1	Not specified
0.0.0.0		V1	Not specified
0.0.0.0		V1	Not specified
0.0.0.0		V1	Not specified

7. Enter a **Community Name**.
8. Enable the **Write** option if you want to allow the remote SNMP user to modify this configuration.
9. Enable the **Trap** option to allow the SNMP agent to send traps to the defined hosts.
10. Enable the **Including Traffic Alarms** option if you wish to force the local SNMP agent to send traffic alarms to the defined hosts.
11. Use the **Version** drop-down list to select the SNMP version that this community will support. The **Any** option will cause the community to support both the v1 and v2c versions.

12. You must define at lease one host, or network, in the lower portion of the screen. To do so, enter the **Host's IP Address** and **Netmask**. Next, select the **Trap Version,** and use the **Source Interface** drop-down list to select the SNMP interface.
13. Press **OK**.

To remove a community, locate it in the community list and select its **Remove** link. Press **OK** to confirm.

To configure SNMP via the CLI, type the following commands:

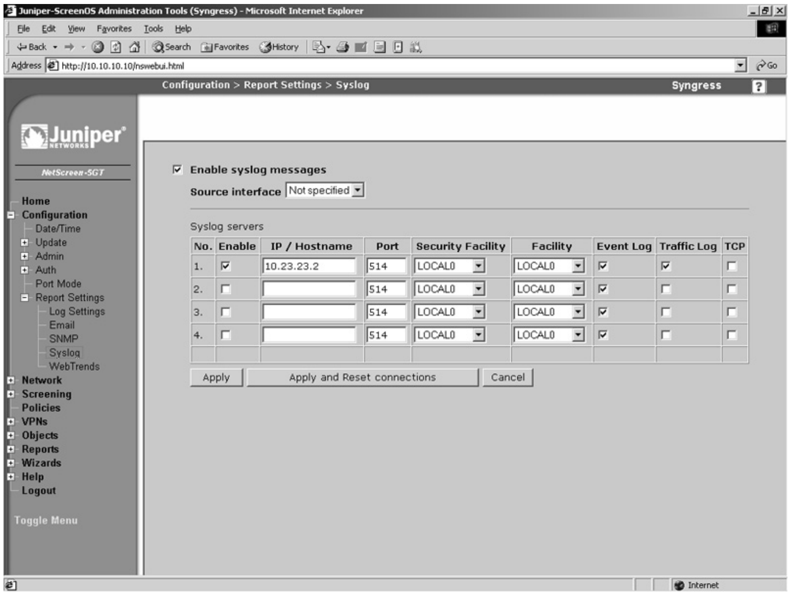
```
Syngress-> set snmp name Syngress
Syngress-> set snmp location "Dearborn, MI"
Syngress-> set snmp community Syngressadmin Read-Only version v2c
Syngress-> set snmp host Syngressadmin 10.4.4.4
```

Syslog

Juniper firewalls generate a great deal of logging. Logged information is contained on the local flash file system using the first-in, first-out (FIFO) method. The first log in will be the first log removed when logging space fills to the limit. If you want to keep your logs for an extended period of time, you must archive them to an external log server. A Juniper firewall can concurrently send information to up to four syslog hosts. Syslog can be configured from either the WebUI or the CLI. Logging is discussed in depth in the next chapter.

Use the following steps to configure the syslog server via the WebUI:

Figure 3.34 Syslog Configuration



Juniper-ScreenOS Administration Tools (Syngress) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://10.10.10.10/nswebui.html
Go
Configuration > Report Settings > Syslog
Syngress
Juniper NETWORKS
NetScreen-5GT
Home
Configuration
Date/Time
Update
Admin
Auth
Port Mode
Report Settings
Log Settings
Email
SNMP
Syslog
WebTrends
Network
Screening
Policies
VPNs
Objects
Reports
Wizards
Help
Logout
Toggle Menu
Apply
Apply and Reset connections
Cancel
Internet

☑ Enable syslog messages

Source interface: Not specified

Syslog servers

No.	Enable	IP / Hostname	Port	Security Facility	Facility	Event Log	Traffic Log	TCP
1.	☑	10.23.23.2	514	LOCAL0	LOCAL0	☑	☑	□
2.	□		514	LOCAL0	LOCAL0	☑	□	□
3.	□		514	LOCAL0	LOCAL0	☑	□	□
4.	□		514	LOCAL0	LOCAL0	☑	□	□

1. Access **Configuration | Report Settings | Syslog**. A screen similar to the one shown in Figure 3.34 will be displayed.
2. Enable the **Enable syslog messages** option.
3. Use the **Source interface** drop-down list to specify the interface from which messages will be sent. If you do not specify an interface here, messages will be sent from the interface closest to the syslog host.
4. In the row labeled **No. 1**, enable the **Enable** checkbox, and type the **IP/Hostname** and **Port** of the remote syslog server.
5. Use the **Security Facility** drop-down list to select the syslog facility to which emergency and critical messages will be sent.
6. Use the **Facility** drop-down list to select the syslog facility to which all other messages will be sent.
7. Enable the **Event Log**, **Traffic Log**, and **TCP** options.
8. Press **Apply**. If you are updating an existing syslog configuration, select **Apply and Reset connections**.

Enter the following commands to configure syslog via the CLI:

```
Syngress-> set syslog config 10.23.23.2 facilities local0 local0
Syngress-> set syslog config 10.23.23.2 port 514
Syngress-> set syslog config 10.23.23.2 log all
Syngress-> set syslog enable
```

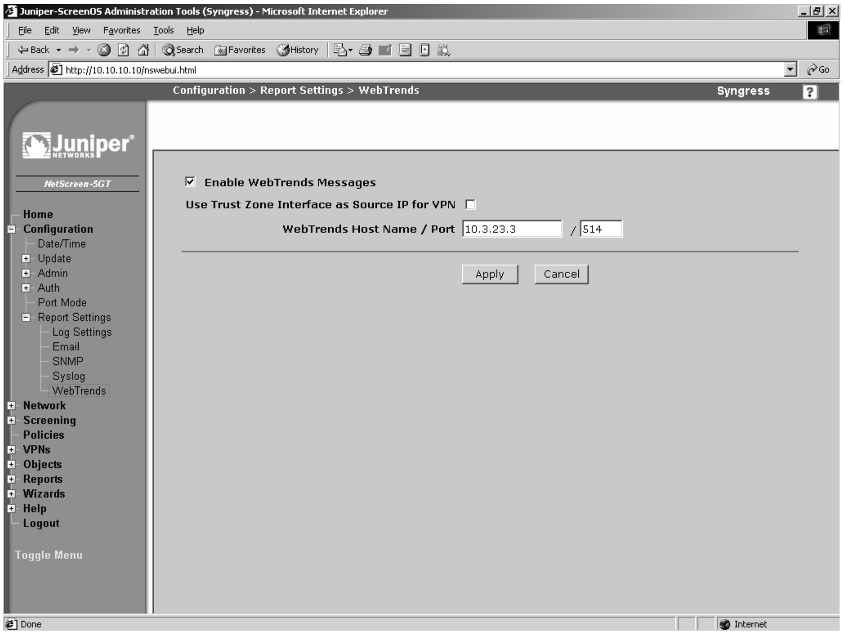
Web Trends

WebTrends firewall suite is a product from the company NetIQ. It is a syslog server that collects all logs, and allows also you to generate graphical reports from the logs. A remote WebTrends server can be configured either from the CLI or the WebUI.

Use the following steps to configure WebTrends via the WebUI:

1. Access **Configuration | Report Settings | WebTrends**. A screen similar to the one shown in Figure 3.35 will be displayed.
2. Enable the **Enable WebTrends Messages** option.
3. Enter the IP address and port number in the **WebTrends Host Name / Port** fields.
4. Press **Apply**.

Figure 3.35 Web Trends Configuration



☑ Enable WebTrends Messages

Use Trust Zone Interface as Source IP for VPN □

WebTrends Host Name / Port 10.3.23.3 / 514

Enter the following commands to configure WebTrends via the CLI:

```
Syngress-> set webtrends host-name 10.3.23.3
Syngress-> set webtrends port 514
Syngress-> set webtrends enable
```

Resources

Windows SSH client *PuTTY*: www.chiark.greenend.org.uk/~sgtatham/PuTTY/
Windows TFTP server Pumpkin: http://kin.klever.net/pumpkin/binaries
Windows Serial/telnet Client Tera Term: http://hp.vector.co.jp/authors/VA002416/teraterm.html

Summary

In this chapter we covered a great deal of information. The purpose of this chapter was to familiarize you with the initial configuration of a Juniper firewall. Before using your firewall, you must understand how to manage it. We explored various methods to manage your firewall. It is important to understand each option available to you. Each option is a separate tool that can be used to control your firewall.

There are two core types of remote management, the WebUI and the CLI. If you are using the serial console, Telnet, or secure shell, you are using the CLI. It is important to be proficient in both management tools. The WebUI is initially easier to use. However, in later chapters you will see that advanced troubleshooting techniques can be carried out only from the command line interface. These techniques are invaluable for more advanced configurations. We also mentioned a third type of management, NetScreen SecurityManager. The NetScreen SecurityManager product is an external source of management, covered in a later chapter.

We also discussed configuring your Juniper firewall to run on the network. Zones are a core part of the Juniper security infrastructure. The security zone is the most commonly used zone, and it is used on every interface, and in every policy. Each interface must be bound to a zone. In the next chapter we focus on basic policy creation and policy theory. We looked at the various types of interface that the firewall supports. The physical interface will be used on each type of Juniper device to interact with the network. The firewall can operate in two modes, layer two and layer three. In this chapter, we focused on layer three configuration of the device. In a later chapter, we focus on the layer two mode, transparent mode.

In the last section of the chapter, we discussed configuration of various system components. Configuring the time on your device is critical, because time is the central reference point used to correlate all events on the firewall. If someone were to break into your network, and your logs were off by several hours, or days, this could mislead your investigation of the break-in. Configuring your logs to be sent to a separate location is also important if you intend to keep your logs on a long-term basis. The syslog server and WebTrends server are powerful options. If you use NetScreen SecurityManager, it also can be used as a central log repository.

Solutions Fast Track

Managing the Juniper Firewall

☑ There are two methods to manage your firewall, the WebUI and the CLI.

☑ Configuration rollback is an important tool for saving a working configuration before you implement changes on your firewall that could potentially disrupt your firewall.

☑ If you use the WebUI the configuration still ends up in the CLI. It is a good idea to memorize the CLI commands because they are at the root of the configuration.

Configuring Your Firewall for the First Time

☑ Security zones are used to identify a logical area of your network.

☑ Physical interfaces can host multiple IP addresses on each interface.

☑ Loopback interfaces are always up when they are configured, and they must be bound to a zone the same as physical interfaces.

Configuring System Services

☑ Setting the system clock is crucial because it is your central point of reference for events that occur on the firewall.

☑ If you need to resolve hostnames to IP addresses, you must configure DNS servers.

☑ A Juniper firewall can hold only so many logs locally, so you must configure an external log server if you want to archive your logs.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Why does Juniper use zones on interfaces? I have used this type of configuration on other devices, and I did not find it to be very effective.

A: Zones are designed to segment areas of the network from each other. On a Juniper firewall, using security zones during policy creation allows, or disallows, traffic from one zone to another. This simplifies policy creation by specifying which zone traffic can travel from and to. Furthermore, it removes the chance of an accidental configuration of access from one system to another. This can easily happen if you use a firewall that does not support zones.

Q: You cover securing the management interface extensively. Are all of those options really required?

A: Because the firewall is such a critical part of your network, you need to ensure its security well. Each option may be used in your network, or perhaps a combination of all of the options makes the most sense in your environment. By understanding all options, you will have the ability to pick and choose between them.

Q: I have looked at the command line interface, and I do not feel that it is very effective to use. Why should I use it when the WebUI is easier and quicker?

A: The WebUI is a very useful tool, and it should be used in conjunction with the CLI. Both have pros and cons. In later chapters, you will need to be proficient in using the command line interface and to be comfortable with its options. Even if you choose to use the WebUI most of the time, I encourage you to use the CLI from time to time so that you are comfortable when you have the need to access it.

Q: You have talked about several options like transparent mode and NetScreen Security Manager. Why did you give so few details on these?

A: These options are complex, and they each deserve separate discussion. There are dedicated chapters for each topic that examine each option in depth.