A Guided Tour of EnGarde Secure Linux

A Guided Tour of EnGarde Secure Linux

Table of Contents

List of Figures

Chapter 1. Getting Started with EnGarde Secure Linux

EnGarde Secure Linux is a complete package of open source Internet services designed to take the work and uncertainty out of setting up and maintaining a highly secure Internet presence. A server-only system, EnGarde Secure Linux begins with secure default settings across-the-board and boots initially with all but a few critical services disabled, allowing you to select and run only the services you will actually use. Configuration and management of EnGarde is handled securely and remotely using Guardian Digital's custom-designed WebTool browser-based administration utility. Updates and security patches are easily applied through WebTool, via a secure connection to the Guardian Digital Secure Network (GDSN). Drawing on the combined resources of Guardian Digital's professional security team and the open source security community, EnGarde Secure Linux builds security layer-upon-layer, beginning with a comprehensive set of security policies that control access to every process and service, and including state-of-the-art open source host and network intrusion detection, along with security-aware system logging and encryption of critical communications. EnGarde Secure Linux offers all of the services needed to safely offer both public Internet services and essential local services, from Web and mail services to FTP, DNS, and DHCP. Other services can be added by drawing on a vast collection of open source software packages, many of which have been packaged by Guardian Digital for installation using WebTool. All of EnGarde's services are managed seamlessly from anywhere through Guardian Digital's custom browser-based WebTool administration utility.

This Guided Tour will take you through installing and configuring some of EnGarde's essential services, including Web, mail and FTP, pausing occasionally to point out how EnGarde helps you maintain a secure environment. When you are finished, you will have set up and configured an Apache Web server, a Postfix mail server, a vsftpd FTP server and will be able to manage them from a remote PC's browser using the Guardian Digital WebTool administration utility.

1.1. The Basics

EnGarde Secure Linux creates a server-only environment that uses standard open source tools to build a secure online presence. Because EnGarde uses its own custom system management tool, Guardian Digitals WebTool, for all configuration and system management tasks, you will not need to use any command-line tools to use EnGarde. However, to use the services that EnGarde provides such as Web, SMTP, DNS and FTP you will need a working knowledge of the basic administration of these services. A basic knowledge of sound security practices will also be helpful. Even though EnGarde, through WebTool, enforces security and guides you in maintaining secure configurations, a basic understanding of security tools and policies will help you understand the security policies WebTool enforces. For example when it requires you to specify user and IP address access when enabling services like FTP.

1.2. What You'll Need

The hardware requirements for EnGarde Secure Linux are modest, but you will need to dedicate a computer for use as an EnGarde server since the server cannot be installed on a drive partition. If you wish to simply try EnGarde without installing it to your hard drive, you may choose to create a "LiveCD" EnGarde environment on a bootable CD during installation.

To fully evaluate EnGarde Secure Linux you will need the following items:

- A "server" system to install EnGarde Secure Linux on.
  - An i686 or greater processor (i686 version), or an AMD64/EM64T processor (x86_64 version)
  - 512 megabytes of RAM
  - A 10 gigabyte IDE, SCSI, or Serial ATA hard drive
  - An Ethernet (10/100/1000) adapter

- A "client" system, typically a desktop, to manage your EnGarde Secure Linux system from.
  - A web browser, such as Internet Explorer or Mozilla Firefox, which supports SSL/TLS.
- An Ethernet network
  - Both machines should be on the same network segment and should have unique IP addresses.
  - The "server" system should have Internet access (so you can evaluate the GDSN).

Assemble all of the above in one place, connect them all to the network, then boot the server system up off of the EnGarde Secure Linux CD. Once this is all done you may proceed to Chapter 3. If you have a firewall, the "server" machine should be able to communicate with updates.guardiandigital.com on port 443/tcp (HTTPS) for GDSN access.

> **Note:** If you do not have a second machine to install EnGarde Secure Linux on (the "server" above), you may wish to use something like VMware Server (http://www.vmware.com/products/server/) for your evaluation.

Chapter 2. Key Features and Benefits

EnGarde Secure Linux offers many unique advantages as a platform for secure Internet services, the most important of which are highlighted below.

- **Secure Server-Only System**

  EnGarde is designed as a secure Internet services platform providing only those services that can be offered securely over a public network, including Web, mail, FTP, DNS, and SSH. EnGarde also does not include a desktop environment.

- **Broad Support for Server Hardware**

  EnGarde focuses on hardware critical to dedicated servers, from interface cards to hardware RAID and supports both Intel and AMD processors, including both AMD and Intel 64-bit systems.

- **Simple & Secure Remote Management using WebTool**

  All standard system administration tasks such as creating users and groups and configuring network interfaces and all EnGarde services from Web and mail to FTP and DNS are seamlessly and securely maintained through the Guardian Digital WebTool browser-based system administration utility.

- **SELinux Mandatory Access Control**

  EnGarde re-architects the Linux security model using SELinux to prevent and contain even "zero-day" attacks. Instead of merely relying on the default Linux kernel Discretionary Access Controls (DAC), EnGarde employs and makes very heavy use of SELinux Mandatory Access Controls (MAC).

- **Consistent Security Updates through the GDSN**

  EnGarde users receive updates and security patches through Guardian Digital WebTool directly from the Guardian Digital Secure Network.

- **Integrated Firewall**

  Host and network firewalls are easily configured through WebTool.

- **Commercial-Grade Host and Network Intrusion Detection**

  EnGarde supports both the AIDE host intrusion detection system, which notifies you when critical system files on your machine are modified, and the Snort network intrusion detection system which allows you to monitor and mitigate network attacks in real-time.

- **Downloadable LiveCD version**

  For those who would like to try EnGarde without installing to a hard drive, EnGarde allows its installation CD to run as a complete, bootable EnGarde Secure Linux server.

Chapter 3. Installing EnGarde Secure Linux

Installing EnGarde Secure Linux is rather straight-forward. For the purposes of your evaluation you have two options: installing EnGarde Secure Linux onto your hard disk or running EnGarde Secure Linux as a LiveCD. This chapter will walk you through both of these scenarios and by the end of this chapter you'll be ready to perform initial configuration of your EnGarde Secure Linux server.

3.1. Secure Out-Of-The Box

Many system installations, both open source and proprietary, leave the system vulnerable as soon as the installation is complete and connected to a public network. EnGarde Secure Linux reduces this immediate vulnerability by separating installation of EnGarde on the server from its configuration and administration over a remote encrypted connection and by carefully restricting the services that are turned on by default. EnGarde further enhances initial security of the installation by leaving out unneeded features such as a graphical subsystem or a compiler that could lead to a rapid system compromise.

3.2. Installation Overview

The EnGarde Secure Linux installation disc lets you set up both a bootable, "LiveCD" server environment or a complete hard drive installation of EnGarde Secure Linux. Both proceed quickly and require very little information from the user. This section of the Tour will guide you through both the setup of the LiveCD environment, comprising the first few screens, and then the full hard drive installation and configuration using the WebTool system administration tool.

3.3. The EnGarde LiveCD Environment

The first few screens you will see after booting your machine from the EnGarde installation CD allow you to create a "LiveCD" environment. This lets you boot from the EnGarde installation CD and run EnGarde without altering your PC's hard drive. All that is required is that you choose a password for the server's root account and WebTool administration login, and, optionally, enter basic network information. Once you have provided this information, you will be presented with a screen that allows you to continue with a hard drive installation, or to begin using your LiveCD server immediately.

If you chose the LiveCD option, your EnGarde LiveCD server is fully configured and ready to use. Web, mail, DNS, FTP and other services are already installed and ready to be configured, enabled, and accessed using the network information you provided during setup. To access the LiveCD, point the web browser on the "client" machine to:

```
https://192.168.10.100:1023/
```

Replace *192.168.10.100* with the IP address you assigned during the LiveCD configuration. After you accept the SSL certificate you may log in using the username "*admin*" and the password you chose during the LiveCD configuration. You may now manage your EnGarde LiveCD server using Guardian Digital WebTool as described in Chapter 5. Please note that any changes you make to your LiveCD configuration will be lost when you reboot your LiveCD server.

If you choose instead to perform an EnGarde server installation, you are now ready to begin installing and configuring EnGarde to your hard drive.

3.4. Hard Disk Installation

The EnGarde server hard drive installation takes only a few more steps than the EnGarde LiveCD setup. After choosing which language you wish to use, you will be asked to choose a target drive for the installation and can choose to permit automatic partitioning of the drive, or to conduct manual partitioning. You will next be asked to choose which service packages you wish to install, for example a basic Web server and its supporting database server, a DNS server, an email server, or firewall services.

Once this is done you will be asked to input basic network configuration information, or to accept a default IP address and subnet. Make a note of this network information since you will need it to configure and manage your EnGarde server from another PC on the same subnet. The installation will now proceed to completion. When you reboot, you will be ready to log in to your new server using Guardian Digital WebTool and begin initial configuration.

Chapter 4. Initial Configuration using Guardian Digital WebTool

Now that your EnGarde server is installed and running, you are ready to connect to your new server from another PC on your network and configure the server using the Guardian Digital WebTool system administration utility. When you are done performing the basic configuration and reboot your server, you will be ready to set up and run individual services including your Web, mail and FTP servers.

By the end of this chapter you will have a fully configured EnGarde Secure Linux system and will be ready to begin your evaluation.

4.1. Logging In To EnGarde Secure Linux

You must now verify that your EnGarde server is connected to a network and can be accessed from the PC you will be using to configure the server. From your PC, type the following URL into your PC's Web browser:

```
https://192.168.10.100:1023/
```

Replace *192.168.10.100* with the IP address you assigned during installation. After you accept the SSL certificate you may log in using the username *admin* and the password *lock&%box*. Please note that the URL is http**s**, which denotes the security of SSL.

You are now ready to proceed with the initial configuration of your server.

4.2. Passwords and Trusted Hosts

This section allows you to set the system passwords and specify the IP addresses and/or networks that may access WebTool on this machine. Enter suitable passwords for the *Root* account on the server and for *WebTool* itself. They should be different passwords. Next you may change WebTool's default language. Finally, define which hosts and/or networks are permitted to access the WebTool administration tool on this server. You should keep this list as small as possible; the more people you open up access to, the greater the threat. You may enter individual IP addresses (e.g. 192.168.1.90) or entire networks (e.g. 192.168.1.).

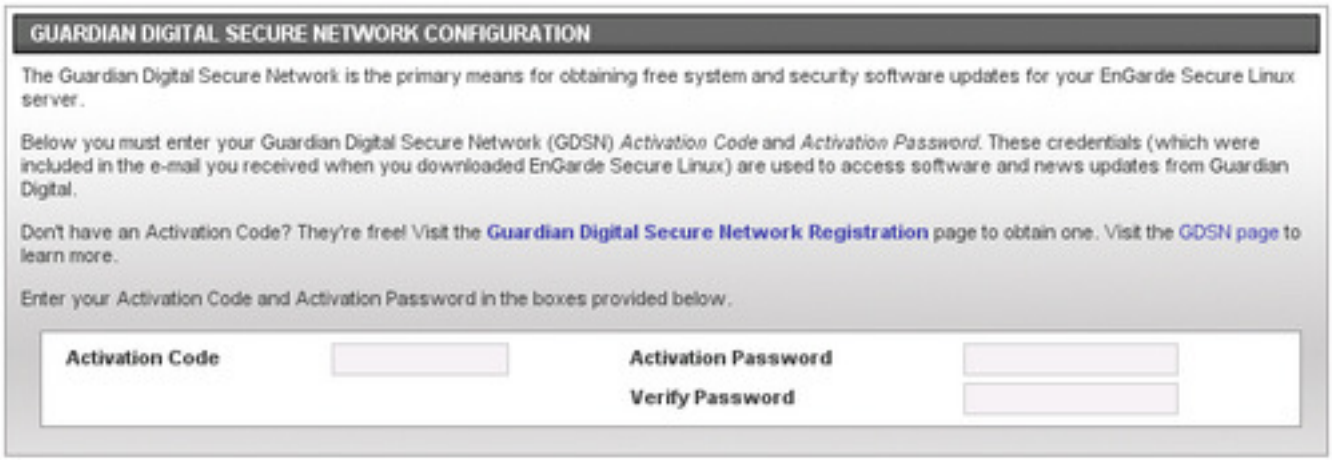
Figure 4-1. Passwords And Access Control

4.3. Guardian Digital Secure Network Configuration

The next step of initial configuration is to configure the Guardian Digital Secure Network (GDSN). The GDSN Is the primary means for obtaining free system and security software updates for your EnGarde Secure Linux server. You should have received an Activation Code and Activation Password in the email you received when you downloaded EnGarde Secure Linux -- enter that here.

If you do not have an Activation Code you can always obtain one (http://www.engardelinux.org/modules/index/register.cgi) from Guardian Digital.

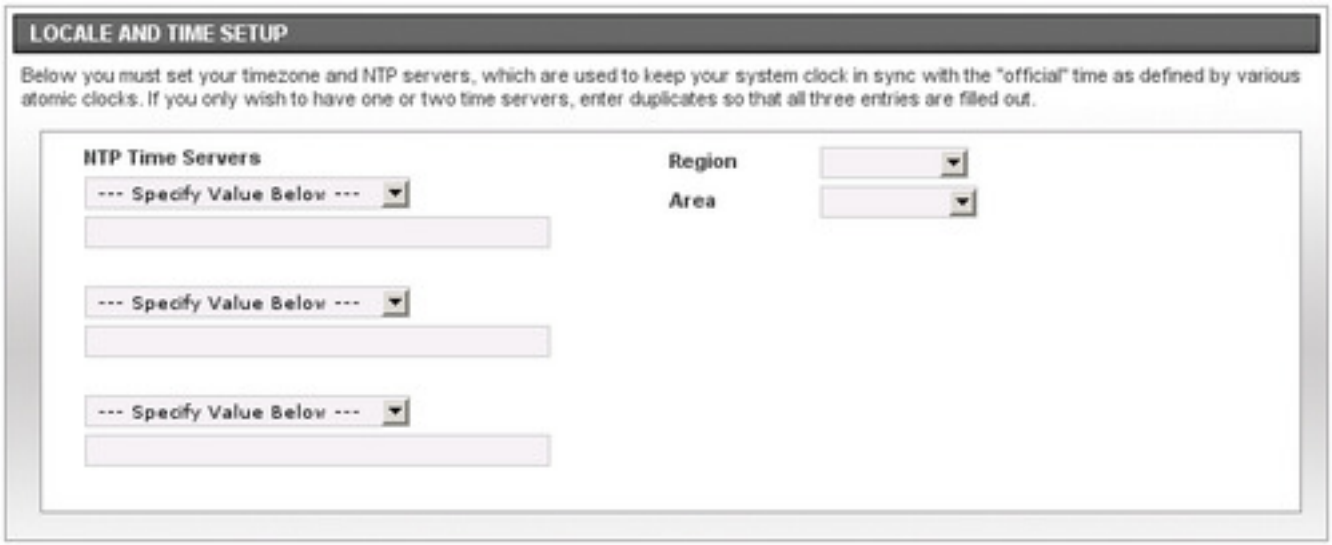
Figure 4-2. Guardian Digital Secure Network Configuration



4.4. Locale and Time Setup

This section allows you to define where in the world your machine is and how to keep its system clock accurate. EnGarde uses the Network Time Protocol (NTP) to synchronize its system clock with time servers on the Internet. Enter three time servers or select three from the drop-down menus (e.g. *pool.ntp.org*). To set up your system locale you must first select your *Region* from the drop-down (e.g. *U.S.*) and then your *Area* from the bottom drop-down (e.g. *Eastern*).

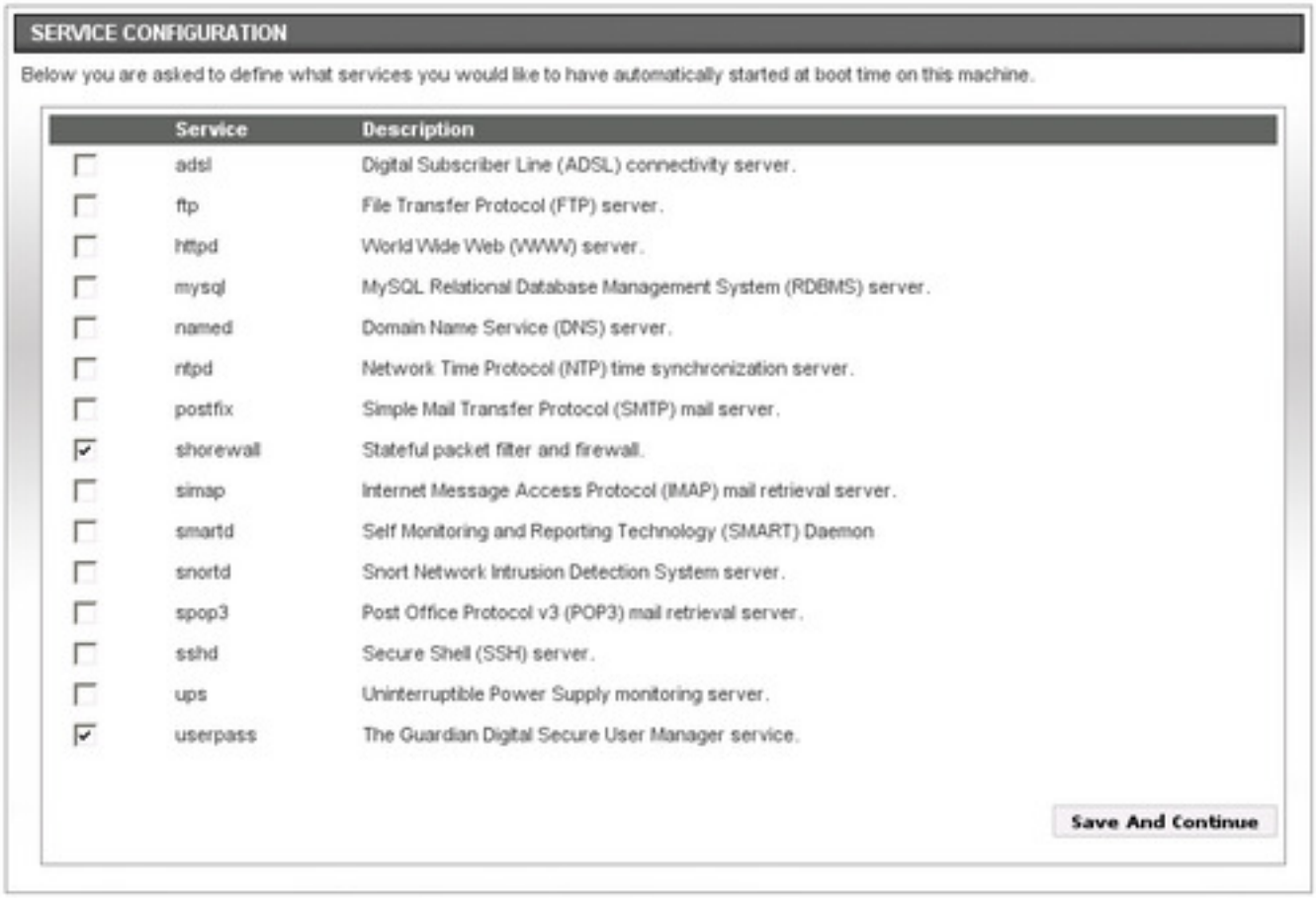
Figure 4-3. Locale and Time Setup



4.5. Service Configuration

This section allows you to define which Internet services will be enabled on this machine. By default all services except for sshd, ntpd, and mysqld (which is configured for localhost only) are disabled. Enable the services you will be using by clicking the checkbox next to their names and leave services that you do not plan on using unchecked; you can always enable them in the *Services Configuration* Module (Section 5.3) later on.

Figure 4-4. Service Configuration



4.6. System Summary and Reboot

Once you have completed your initial configuration you will be brought to a page that summarizes everything you have just entered. Review the information and then click the *Reboot System* button.

Congratulations! Your EnGarde Secure Linux server, once it is finished rebooting, is now fully configured and ready for public access. You may now log back in to your server using WebTool and enter a login name of *admin* and the new password you just chose during initial configuration.

In the following chapters, you will learn how easy it is to configure your EnGarde server to maintain security and to create and customize Web, mail, FTP and other services.

Chapter 5. Secure Administration Using Guardian Digital WebTool

Not just another generic Web-based administration tool, Guardian Digital WebTool is engineered specifically to provide secure remote administration for EnGarde Secure Linux. WebTool provides all the simplicity and convenience you expect from browser-based system administration, from creating users and groups to managing Web access and mail server accounts, while adding the security of carefully restricted default access settings and helping you eliminate unnecessary services.

The goal of this chapter is to introduce the reader to key information such as how to start, stop, and restrict access to services on your EnGarde Secure Linux server. By the end of this chapter you will be able to move forward with your evaluation.

5.1. WebTool Navigation

WebTool navigation is done primarily using the menu bar at the top of the WebTool interface.

Figure 5-1. WebTool Navigation

Use the *LOGOUT* button at the top-right of the interface to log out of WebTool (you are automatically logged out after 15 minutes of inactivity) and use the *GO BACK* button to navigate backwards. Make sure you use the *GO BACK* button instead of the *Back* button in your web browser!

The Menu Bar is broken down into the following sections:

- **Module**

  This menu contains options pertaining to the module that you're currently in. For example, in the *Domain Name Service* module you see options such as *General Configuration*, *Master Zone Listing*, and *Slave Zone Listing* and in the *Firewall Configuration* module you see options such as *Blacklist* and *Firewall Rules*.

- **Services**

  This menu allows you to access the services provided by this EnGarde Secure Linux server, such as DNS, E-Mail and World Wide Web.

- **System**

  This menu allows you to configure your EnGarde Secure Linux system. This menu includes items such as Access Control, Firewall Configuration, and WebTool Configuration.

- **Auditing**

  This menu provides quick access to the Logging and Reporting subsystems of EnGarde Secure Linux.

- **Wizards** and **Suites** and **Help**

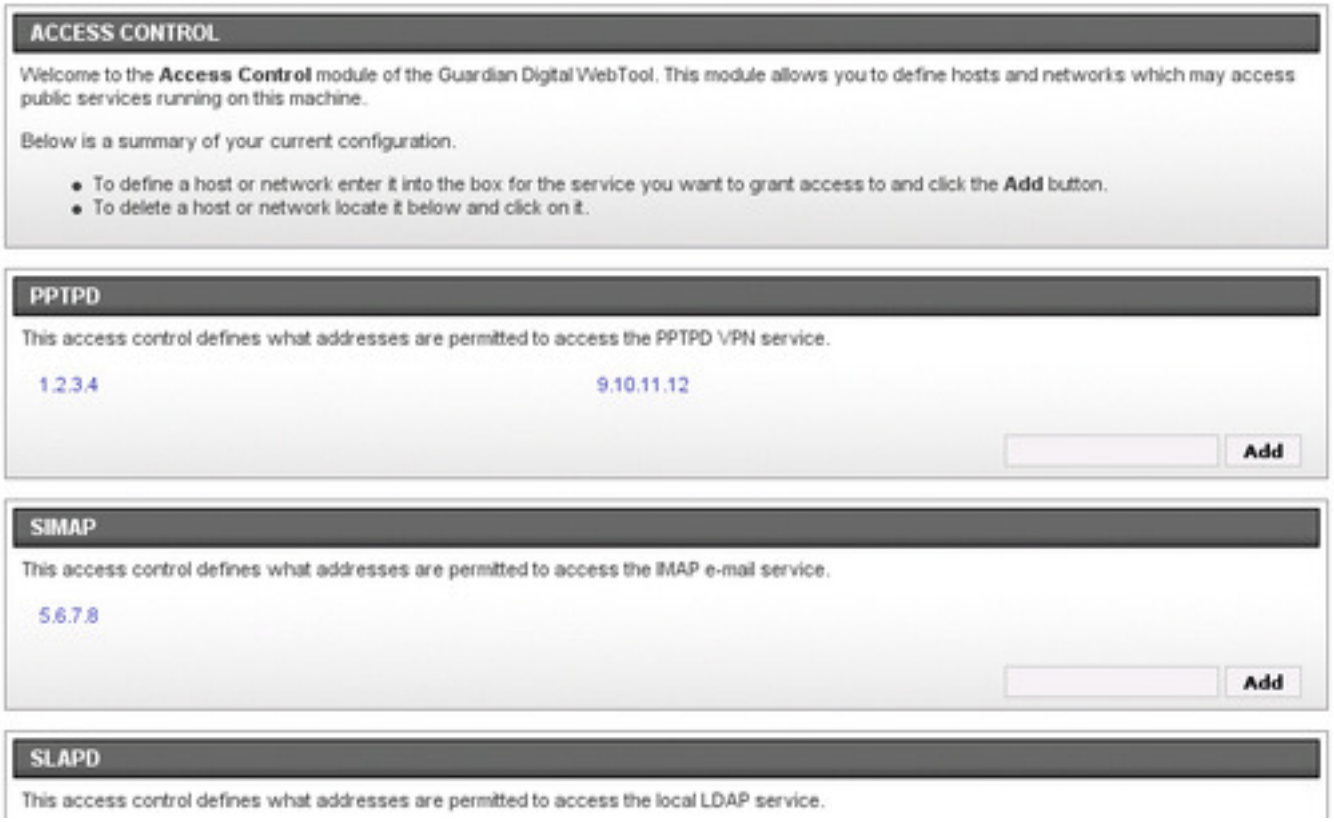
  These menu items are not yet implemented. Help is provided via the WebTool contextual help system.

Now that you know how to get around WebTool, let's take a look at what's inside!

5.2. Controlling Access by IP Address

WebTool management of system and service access control demonstrates EnGarde's unique commitment to secure administration. By default, services like SSH, SPOP/SIMAP, and FTP have no access granted and the administrator must define the machines and networks that will be granted access to each service. This prevents services from being left "wide open" and therefore vulnerable to attack by requiring the administrator to consider and choose the proper scope of access to each service. Access to services is controlled through the *System Access Control Module* by selecting *Access Control* from the *System* menu of WebTool.

Figure 5-2. Access Control

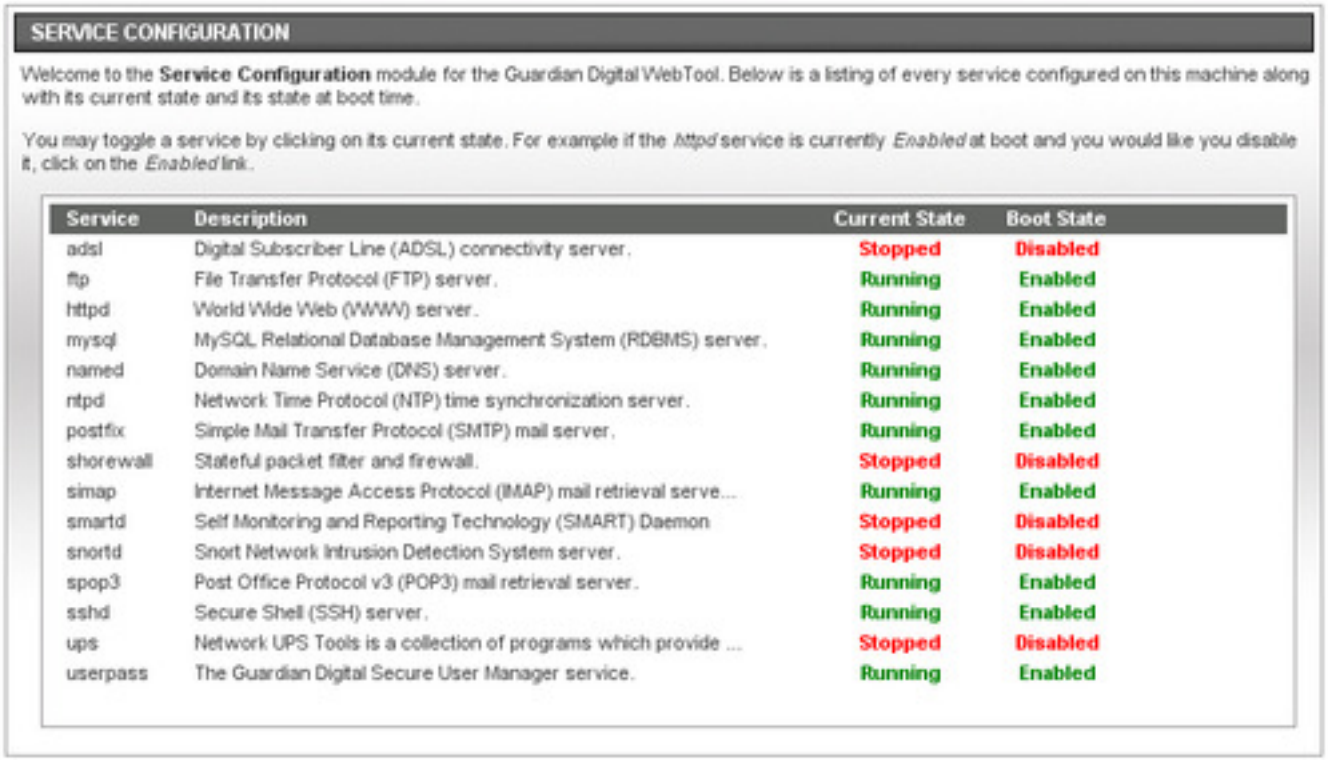


This page shows a listing of the services which you may control access to. To grant access to a service type an address (ie, 192.168.10.100) or a network (ie, 192.168.10.) into the text box for the appropriate service then click the *Add* button. To remove access to a service, simply click the entry you want to delete in the appropriate section and it will be removed immediately.

5.3. Configuring Services

By default, EnGarde disables all services except those few required for basic administration including WebTool and SSH access. You must specifically enable other services through the *Service Configuration Module* shown below. This ensures that the system is not made vulnerable by running unneeded services.

Figure 5-3. Service Configuration



Services can be easily enabled and disabled at any time using this *Services Configuration Module* screen. Click the red or green link to toggle between *Running* or *Stopped* for *Current State*, or between *Enabled* or *Disabled* for the *Boot State*.

Starting from a secure "default-deny" state, you have now chosen the services you need to run and restricted access to each service to only those networks and addresses requiring access. With this fundamental understanding of how to control access to services under your belt you're ready to move on to service configuration.

Chapter 6. Setting Up EnGarde Services

Guardian Digital has simplified the task of configuring and managing EnGarde's services by avoiding "generic" browser-based management tools and creating its own secure system management tool, the Guardian Digital WebTool system administration utility. WebTool goes beyond merely providing a consistent interface across Web, mail, DNS and other services to guide you as the administrator towards secure and consistent settings.

This chapter will guide you through setting up a secure SSL-enabled Apache Web server and an associated MySQL database, a Postfix mail server, a vsfptd FTP server, and the rudiments of a BIND DNS server. Along the way, you will see how WebTool guides you in keeping the services secure.

6.1. Setting up a Web Server

WebTool makes creating a secure SSL-enabled Web server just as simple as creating an ordinary insecure Web server. When you have completed this section, you will be operating a new SSL-enabled Web server Virtual Host and its associated database.

To create a new Web server Virtual Host select *World Wide Web Management* from the *Services* menu, then choose *Create New Virtual Host* from the *Modules* menu. All you need to do to create an SSL-enabled Web server is to select *Yes* in response to *Use SSL?* . Enter basic hostname, IP and administrative access information, click *Create New Virtual Host* and your Web server is ready to use.

> **Note:** Please note that due to limitations of the SSL protocol itself, only one SSL-enabled server can be created for a specified IP address. Thus if you only have one IP address you can only have one SSL-enabled Web server.

Figure 6-1. Create New Virtual Host

The *Create Virtual Host* screen also demonstrates the ease with which the administrator can create a MySQL database for use by the new server. Just supply a database username and password and the database is created and linked to the new site, with access to the new database granted only to the specified username. This avoids the many security pitfalls and other headaches associated with "manually" creating and associating a database. The database name will be the hostname separated by underscores, e.g. www_engardelinux_org.

Only one step remains to enable a working SSL-enabled site: creating its new SSL certificate. To do this, select *World Wide Web Management* from the *Services* menu and you will see the screen below.

Figure 6-2. Current Virtual Hosts

Click on the virtual server you just created, scroll down to the *SSL Certificate Management* section and click *Create New Certificate*. You will be presented with a pop up asking for basic contact information, as well as the name of your site (*Authority Name*):

Figure 6-3. Create/Renew SSL Certificate

Fill in the required fields then click the *Create Certificate* button. Finally, navigate back to the main *World Wide Web Management* screen, click the *Restart Apache Web Server Service* button and your new server is up and running. You may now access the virtual host you just created by typing the URL into your browser, for example:

http://www.engardelinux.org/

The next thing to do is to upload content. Once you have completed the procedure in Section 6.3 you can upload your HTML content via FTP to */home/httpd/<site>-<port>/html*. In the example above, you'd upload your content to */home/httpd/www.engardelinux.org-80/html*.

6.2. Setting up a Mail Server

EnGarde Secure Linux provides all the tools needed to set up secure mail services based on the open source Postfix mail server. In this section, you will create and configure a new SMTP server and add mail recipients to it.

Creating a mail server is similar to creating a Web Virtual Host. From the *Services* menu, select *E-Mail Services*, and then click *SMTP Server Management*. Choose *Virtual Mail Domain*s from the *Module* menu to see the screen below:

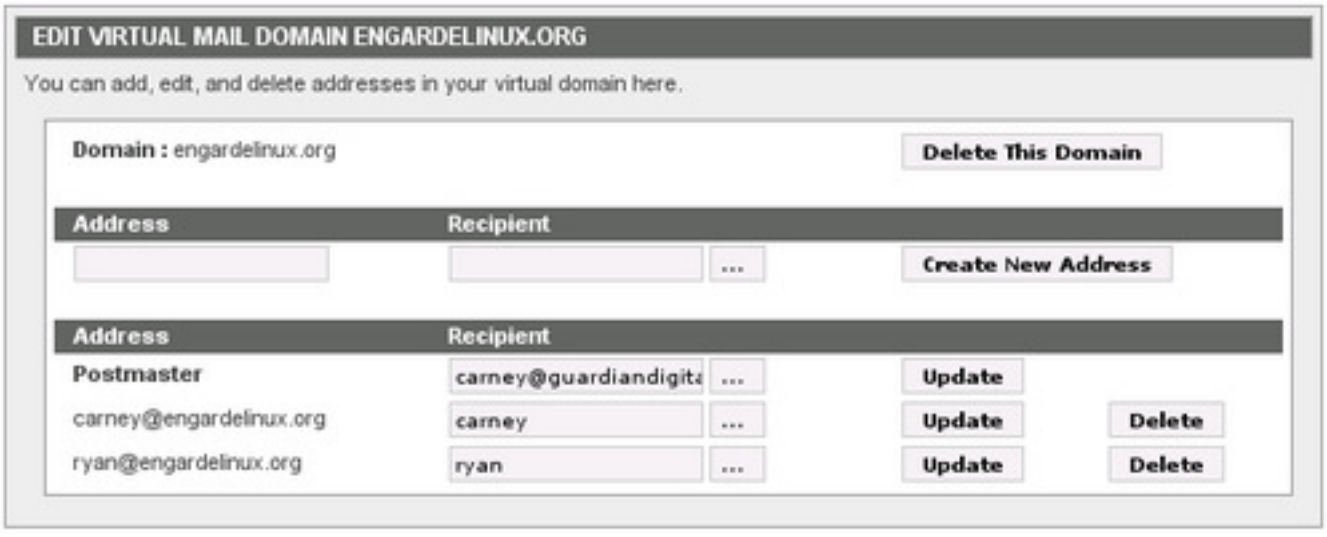
Figure 6-4. Virtual Mail Domain Management

You may now, at your option, enter an email address or local user to receive "postmaster" mail-- mail sent to invalid addresses on your server.

Click *Create New Domain* and your mail domain can begin creating mail recipients.

To begin adding recipients to your new mail domain, while viewing the *Virtual Mail Domain Management* screen above click on the name of the domain you have just created (displayed in the *Active Virtual Domains* box) and you will see the editing window shown below.

Figure 6-5. Edit Virtual Mail Domain



To add a recipient, enter a username in the *Address* box and enter a recipient address (or local username) in the *Recipient* box, then click *Create New Address.*

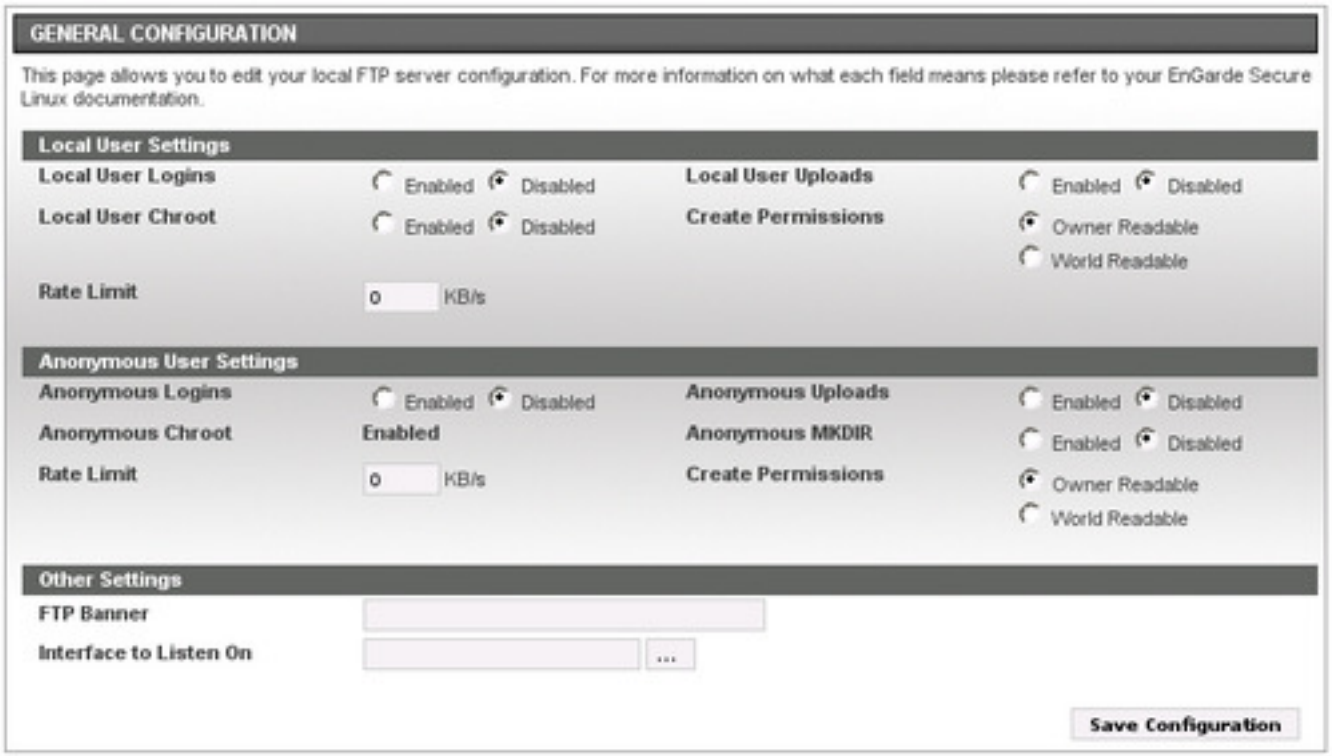
Your mail server is now configured and ready to use. If you have DNS set up properly you should now be able to validate

your changes by sending an email to one of the addresses that you've configured, such as carney@engardelinux.org. If you plan on using your EnGarde Secure Linux server as a mail server, you will probably want to set up SPOP3 and/or SIMAP at this time.

6.3. Setting up an FTP Server

FTP remains the most widely used file transfer protocol, and the method most often used to upload content to websites, despite its use of unencrypted logins and other insecurities. EnGarde offers the most secure FTP server available, vsftpd, and simplifies its use through WebTool. Because of the risks of unrestricted FTP access, EnGarde requires you to first choose the addresses or networks you wish to grant FTP access, by selecting *Access Control* from the *System* menu as described in Section 5.2. Once this is done you may now select *File Transfer Protocol* from the *Services* menu, and then select *General Configuration* from the *Modules* menu to begin configuring your FTP server using the screen below.

Figure 6-6. FTP Server Configuration



In order to use your FTP server to upload files to your EnGarde Web server, you must change the settings above to *Enabled* for *Local User Login*s and *Local User Uploads*, and, optionally, to allow users to create *World Readable* permissions.

The *FTP Server Configuration* module allows you to further restrict FTP access to machines on your private network by restricting the *Interface to Listen On* to your server's internal interface, if applicable.

By default, the *FTP Server Configuration* module disables anonymous FTP logins, an inherently insecure activity. Should you wish to operate a public FTP server, anonymous FTP access can be carefully controlled through a variety of settings as shown in *Anonymous User Settings* above.

EnGarde also permits you to restrict FTP users' system access to only their home directories by setting up chroot access. A complicated process on many systems, this can be accomplished easily in EnGarde by changing the *Local User Chroot* setting, shown above, to *Enabled*.

You have now set up and configured a vsftpd FTP server and learned how to configure it to minimize the FTP protocol's insecurities. To verify that your FTP server is working correctly, try to FTP into it using an FTP client such as WS_FTP.

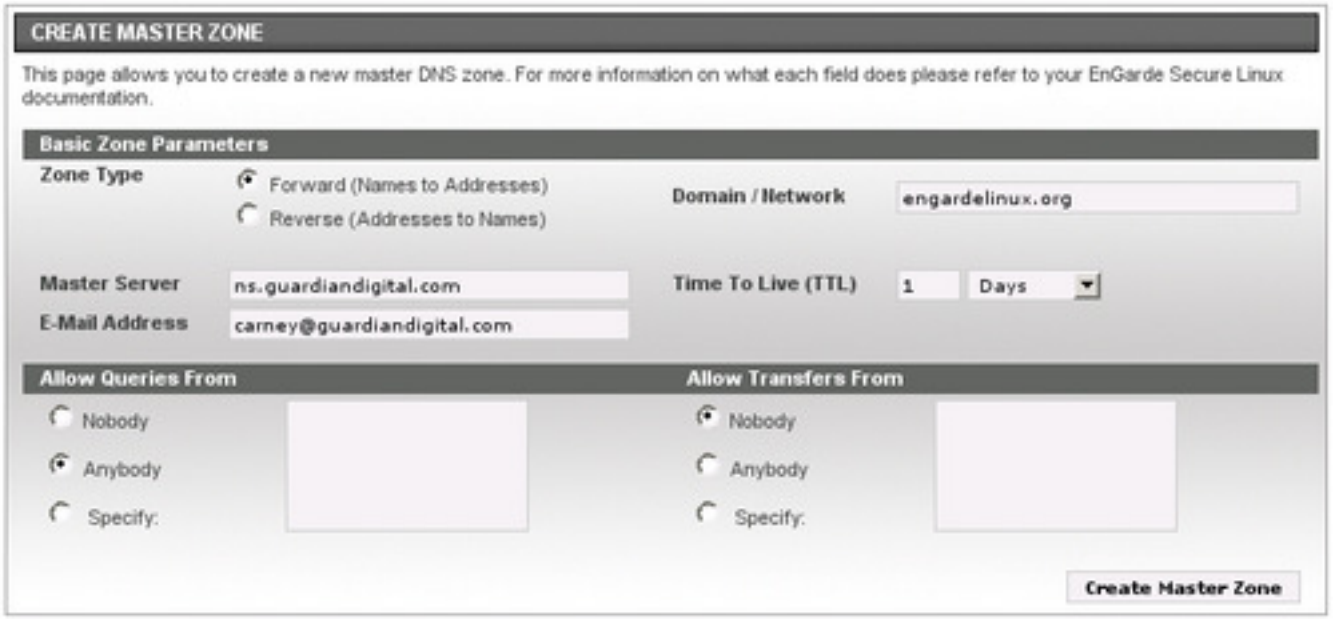
6.4. Setting up DNS Services

Although not all users of EnGarde will need or want to run their own Domain Name server, those who do want complete control of their domain will find it easy to set up a secure DNS server using WebTool. The EnGarde DNS server easily creates and manages both forward and reverse zones and the standard DNS record types, A, PTR, NS, and MX.

To illustrate the simplicity of DNS management in EnGarde, here are the steps you need to take to create a Forward DNS Zone in EnGarde Secure Linux. To configure a complete functioning DNS server, you will also need to create a Reverse DNS zone, and if you are also operating a mail server on your EnGarde server, MX mail records. For details, see the EnGarde Secure Linux 3.0 QuickStart Guide (http://www.engardelinux.org/doc/guides/engarde-quick-start-guide-3.0/engarde-quick-start-guide-3.0/index.shtml)

In WebTool, select *Domain Name Service*s from the *Services* menu and from the *Module* menu choose *Master Zone Listing*, then click *Create Master Zone to view the Create Master Zone module screen.*

Figure 6-7. Create Master Zone



All you need to do to create a working DNS zone is to enter the Domain Name itself and an email address for zone administration. WebTool ensures that the DNS configuration files are correctly and securely written, disallows zone transfers by default, and makes it easy to restrict queries of the DNS server when needed for additional security.

Click *Create Master Zone* and your zone will be created. You are now ready to create Reverse Zones and any necessary DNS records. Don't forget that, unless you plan to use IP addresses only, you will need to create DNS records for each Web, mail, FTP and other services you offer, for example ftp.engardelinux.org for your FTP server. If you are running the EnGarde DNS service, you can do this by selecting *Domain Name Service* from the *System* menu.

6.5. Summary

As you've seen from this chapter setting up services on EnGarde Secure Linux is very easy. Guardian Digital WebTool allows you to set up each service without ever having to edit a configuration file and guides you through selecting safe defaults. Leveraging best-of-breed services such as Apache, Postfix, vsftpd, and BIND, Guardian Digital WebTool and EnGarde Secure Linux provide a solid foundation for your business.

Chapter 7. Consistent Security and the Guardian Digital Secure Network

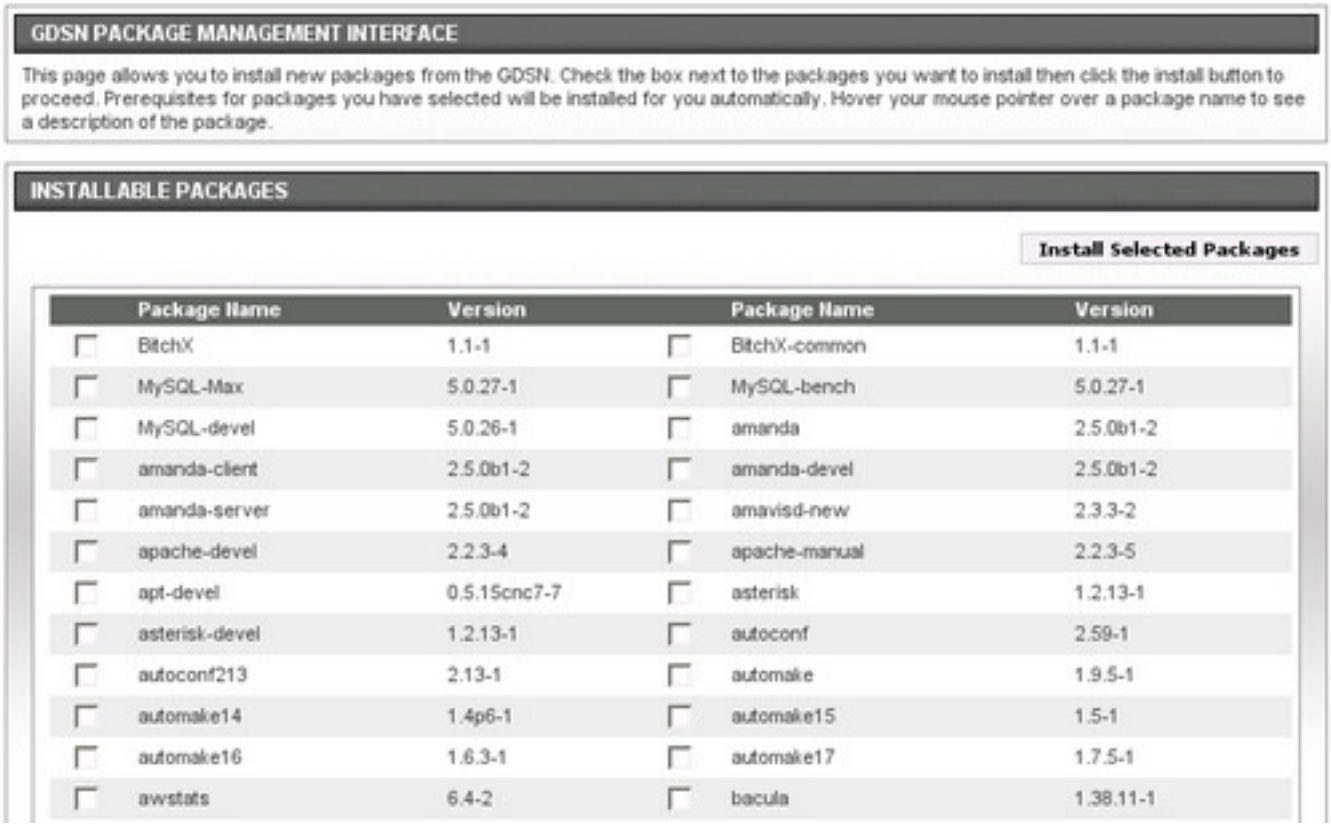
The security of any system is only as good as its maintenance and support. Guardian Digital lifts the burden of maintaining a secure Internet presence by offering each user access to a personal account on the Guardian Digital Secure Network (GDSN).

In this section, you will learn how to access the GDSN to perform system upgrades, apply security patches, and add entire new services to your EnGarde system.

To see what upgrades are available for your EnGarde installation, log into WebTool and select *Guardian Digital Secure Network* from the *System* menu, then select *Update Agent* from the *Module* menu. The *Update Agent* screen will display a list of all pending upgrades to your EnGarde system. Just click the *Proceed with Upgrades* button and your upgrades will be installed.

Installing new packages and services is just as simple. Again select *Guardian Digital Secure Network* from the System menu and then select *Package Management* from the *Module* menu as shown below:

Figure 7-1. GDSN Package Management



Hover your mouse cursor over a Package Name for more information on it and if you decide to install it, it's as easy as clicking a checkbox. For example to install the packages needed to run a BitTorrent server just check the *BitTorrent* box

and click the *Install Selected Packages* button. You will be taken to the *Confirm Package Installation* screen displaying the packages you have chosen where you can complete the BitTorrent installation by clicking the *Install These Packages* button.

This concludes your introduction to the Guardian Digital Secure Network. You now know how easy it is to check for and install upgrades to your EnGarde system and to add services through the *Package Management* module. You should stay on top of package and security updates by checking the *Update Agen*t early and often!

Chapter 8. Layered Security Using Enterprise-Class Open Source Tools

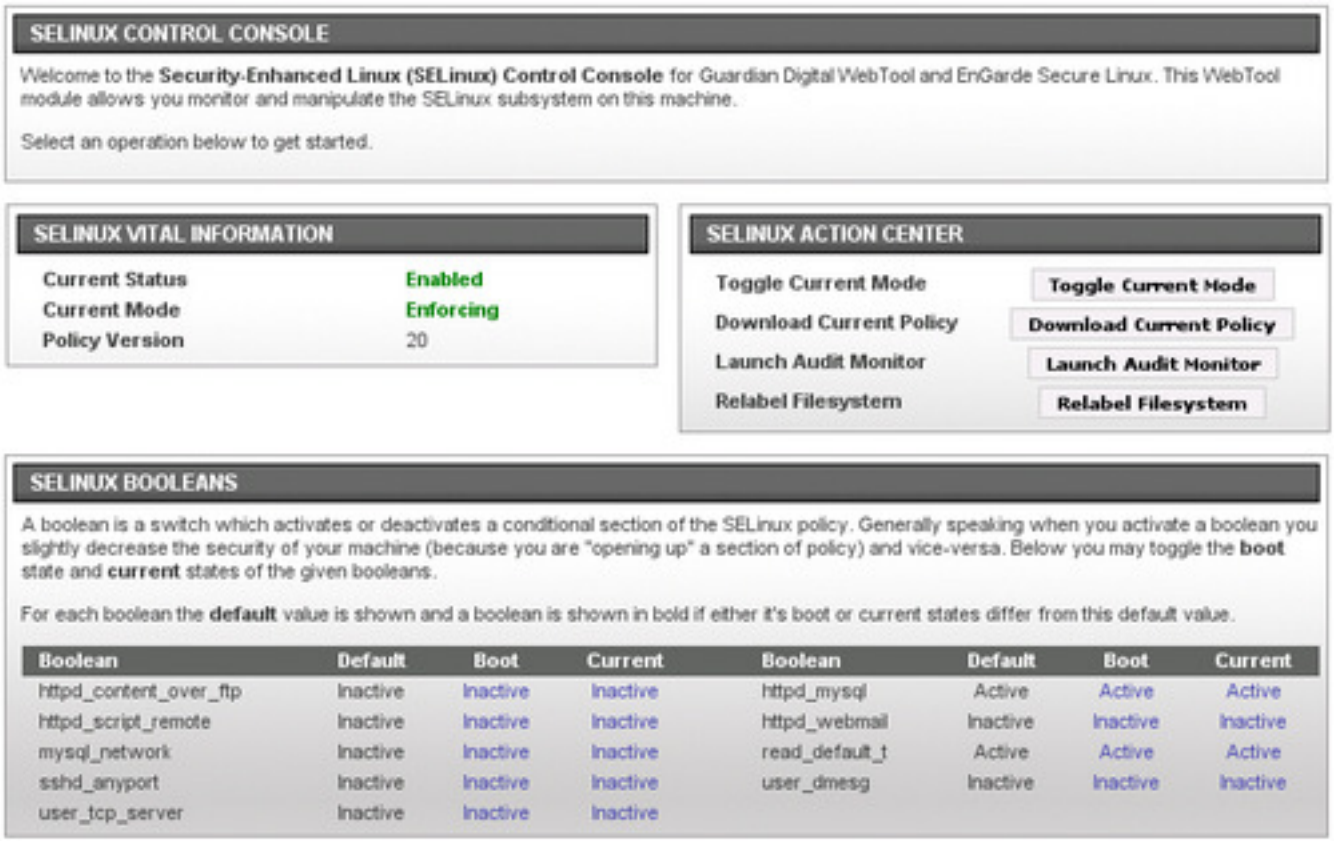
Because any system is only as strong as the weakest link in its security armor, EnGarde Secure Linux defends itself using layers of open source defenses, extending from the Linux kernel out to the boundaries of the public network. In this chapter, you will be introduced to the most of the important of these defensive technologies, beginning with SELinux, and will learn how they are managed through WebTool.

8.1. SELinux and Mandatory Access Control

The greatest weakness of most operating systems, both open source and proprietary is their vulnerability to compromise through the subversion of user privileges leading to compromise of the all-powerful root account, a process sometimes referred to as privilege escalation. EnGarde Secure Linux neutralizes these attacks and prevents rootkit and even "zero-day" attacks by implementing Security-Enhanced Linux (SELinux), a security model that places all processes and applications under the control of individualized security policies that define the actions the process may take and the resources it may access, hence "mandatory" access control rather than merely "discretionary". Unlike many systems that use SELinux, EnGarde comes out-of-the-box with a fully developed SELinux policy for every service and application.

To help you manage the SELinux policy environment, WebTool offers a unique *SELinux Control Console*. To use the console, Select *SELinux Control Console* from the *System* menu:

Figure 8-1. SELinux Control Console



Because Guardian Digital has created a uniquely secure SELinux environment for EnGarde Secure Linux, adding packages not included in EnGarde's base installation or modifying the services you have installed may require you to temporarily disable SELinux policy enforcement or to disable specific restrictions. The *SELinux Control Console* allows you to make these changes easily by using the *Toggle Current Mode* action to turn off policy enforcement while continuing to monitor policy violations; simply click the *Toggle Current Mod*e mode and then click the *Yes, Disable Enforcing Mode* button and your machine will be put into *Permissive Mode*. You will now see the *Current Mode* change from *Enabled* to *Permissive*.

You can also disable certain specific elements of policy by changing the status of policy "boolean" switches. For example you can allow your Web server and its CGI or PHP scripts to communicate with HTTP/HTTPS services on remote machines by toggling the *httpd_script_remote* boolean setting.

The *SELinux Control Console* also illustrates the EnGarde contextual help system found in all WebTool modules. To see specific help text for any field in a module, for example in the *SELinux Boolean* list above, just hold your mouse over a field and an explanatory text box will appear until you roll off of it. [change screenshot to include rollover text box from Boolean list]

8.2. Network and Host Intrusion Detection

Your EnGarde Secure Linux server includes a WebTool-enabled Snort network intrusion detection system. Just select *Intrusion Detection Systems* from the *System* menu, then select the *Network IDS* submenu and designate the interfaces and services you wish to monitor.

You may also at your option install and configure the open source AIDE host intrusion detection system. To install AIDE, use the Guardian Digital Secure Network's *Package Management* module as described above in Chapter 7. Once installation is complete, you can initialize AIDE and begin monitoring your system for suspect changes by selecting the *AIDE Host IDS* menu from the *Network IDS* menu and clicking the *Initialize IDS Database* button.

8.3. Firewall Protection

EnGarde offers firewall protection through the Shorewall open source firewall package, available during initial installation and afterward through the Guardian Digital Secure Network's *Package Management* module (Chapter 7). This flexible system lets you configure firewall protection for the server itself, or to configure EnGarde itself as a standalone multi-homed firewall.

8.4. Configuring EnGarde's Defenses-in-Depth

You have a fundamental understanding of some of the crucial layers in EnGarde Secure Linux security architecture. Having only scratched the surface, you now know how to monitor and manage Mandatory Access Control policies through WebTool's *SELinux Control Console* and have been introduced to WebTool's intrusion detection and firewall module.

Chapter 9. EnGarde Security the Guardian Digital Way

This Guided Tour of EnGarde Secure Linux is now complete. We hope you have seen how EnGarde makes creating a fully secure Internet services environment simple and straightforward. In the course of this Guided Tour you have:

- Set up an EnGarde Secure Linux LiveCD environment
- Installed EnGarde Secure Linux on a hard drive
- Connected a PC to your new server and configured your server using Guardian Digital WebTool.
- Enhanced your new server's security by limiting services and restricting access to services
- Set up and managed an SSL-enabled Web server and MySQL database
- Set up and managed a mail server
- Set up and managed a secure FTP server
- Begun configuration of a DNS server
- Updated your new server using the Guardian Digital Secure Network
- Managed SELinux security policies using the SELinux Control Console

In the course of the Tour, you have seen how EnGarde Secure Linux begins with secure default settings and guides you through maintaining security as new services are added, configured and managed. You are now ready to begin using EnGarde Secure Linux, the premier open source platform for providing secure services in an insecure world.

9.1. Guardian Digital, Inc.

The first full-service open source security company, Guardian Digital has developed and refined EnGarde Secure Linux in both community and commercially-supported versions since 1999. Guardian Digital's team of professional security engineers are constantly evaluating new developments in IT security and incorporating them into EnGarde Secure Linux with the help and support of the community of open source security enthusiasts.

Guardian Digital offers a fully-supported commercial version of EnGarde Secure Linux. For more information on our commercial products, including WebTool-supported suites for Mail, ECommerce and VPN services, visit the Guardian Digital (http://www.guardiandigital.com) site or contact as shown below.

Contact Information:

Guardian Digital, Inc.
165 Chestnut Street
Allendale, NJ 07401
Phone: (201) 934-9230
Fax: (201) 934-9231
Web: http://www.guardiandigital.com/
Email: info@guardiandigital.com (mailto:info@guardiandigital.com)

9.2. Additional Resources

Below are some additional resources which should help you during your evaluation of EnGarde Secure Linux.

- **EnGarde Secure Linux (Community Edition) Home Page** (http://www.engardelinux.org/)

  EnGarde Secure Linux Community Edition is currently available for download under the GNU General Public License from the EnGarde Secure Linux homepage and a worldwide network of mirrors.

- **EnGarde Secure Linux (Community Edition) Documentation** (http://www.engardelinux.org/modules/index/documentation.cgi)

  This is the first place you should go if you have a problem. If you're having trouble with EnGarde Secure Linux you can check out the Quick Setup Guide (http://www.engardelinux.org/doc/guides/engarde-quick-setup-guide-3.0/engarde-quick-setup-guide-3.0/index.shtml) or the Quick Start Guide (http://www.engardelinux.org/doc/guides/engarde-quick-start-guide-3.0/engarde-quick-start-guide-3.0/index.shtml). Want to write a WebTool module? Check the WebTool API Guide (http://www.engardelinux.org/doc/guides/webtool-api-guide/webtool-api-guide/).

- **EnGarde Secure Linux Wiki** (http://wiki.engardelinux.org/)

  The wiki is a great place to contribute or look for answers to your questions before you ask them on the EnGarde Secure Linux Community forum.

- **EnGarde Secure Linux Community Forum** (http://www.engardelinux.org/forums/)

  Have a question? Ask the EnGarde Secure Linux community. Our forums are constantly monitored by Guardian Digital staff and community volunteers so you should get an answer to your question quickly.

- **Secure By Design: How Guardian Digital Secures EnGarde Secure Linux** (http://www.engardelinux.org/doc/other/wmes/wmes.html)

  Linux and open source systems have long been renowned for their stability, versatility and scalability. EnGarde Secure Linux adds the feature crucial to providing services on the modern Internet -- security. This document outlines in great detail how Guardian Digital builds security into every element of EnGarde by selecting the best available open source tools and services available and configuring them with security as the top priority.

- **LinuxSecurity.com** (http://www.linuxsecurity.com/)

  LinuxSecurity.com was first launched in 1996 by a handful of Open Source enthusiasts and security experts who recognized a void in the availability of accurate and insightful news relating to open source security issues. Headquartered in Guardian Digital's offices, LinuxSecurity.com's editorial and web development staff creates feature articles, commentaries and surveys designed to keep readers informed of the latest Linux advancements and to promote the general growth of Linux around the world.