

SHP RaQ 4

User Guide

Version 1.5
February 25, 2002



take it to the nth

Copyright © 1997-2002 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, California 94303-4900 U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and other countries.

This document and the product to which it pertains are distributed under licenses restricting their use, copying, distribution and decompilation. No part of the product or of this document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, JavaScript, JDK, Sun Cobalt, Sun Cobalt RaQ, Sun Cobalt CacheRaQ, Sun Cobalt Qube and the Sun Cobalt logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Netscape and Netscape Navigator are trademarks or registered trademarks of Netscape Communication Corporation in the United States and other countries.

Legato NetWorker is a registered trademark of Legato Systems, Inc. Linux is a trademark of Linus Torvalds.

Federal Acquisitions: Commercial Software -- Government Users Subject to Standard License Terms and Conditions.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright © 1997-2002 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, California 94303-4900 États-Unis. Tous droits réservés.

Sun Microsystems, Inc. détient des droits de propriété intellectuelle sur la technologie réunie dans le produit qui est décrit par ce document. Ces droits de propriété intellectuelle peuvent s'appliquer en particulier, sans toutefois s'y limiter, à un ou plusieurs des brevets américains répertoriés à l'adresse <http://www.sun.com/patents> et à un ou plusieurs brevets supplémentaires ou brevets en instance aux États-Unis et dans d'autres pays.

Ce produit ou document est distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a.

Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux États-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, JavaScript, JDK, Sun Cobalt, Sun Cobalt RaQ, Sun Cobalt CacheRaQ, Sun Cobalt Qube et le logo Sun Cobalt sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Netscape et Netscape Navigator sont des marques de fabrique ou des marques déposées de Netscape Communication Corporation aux Etats-Unis et dans d'autres pays.

Legato NetWorker est une marque déposée de Legato Systems, Inc. Linux est une marque de fabrique de Linus Torvalds.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU AL'ABSENCE DE CONTREFAÇON.

Part Number / Numéro de pièce : 816-3754-01

Date : 02-2002

Contents

Introduction	1
Installation Note	1
Security Functions	1
Port Scan Detection	1
Buffer Overflow Protection	2
Root Privilege Control	3
Configuring Security Functions	4
Configuring Scan Detection	5
Buffer Overflow Alerts	8

Introduction

This document describes the security functions and their features provided by the Security Hardening Product (SHP) added to RaQ 4 and accessed through the User Interface (UI). These functions have been added to the existing RaQ 4 UI; please refer to the RaQ 4 UI documentation for descriptions of other UI features and functions.

This document presents an overview of these security functions, then details how they are accessed and configured.

Installation Note

Before installing the RaQ 4 SHP, you must first update the OS and the kernel. Install OS Update 2 and the latest kernel package, RaQ4-All-Kernel-4.0.1-2.2.16C32III-4.pkg.

Security Functions

Security Functions include:

- Scan detection, logging, and lockout
- Buffer overflow protection
- Root privilege control

Port Scan Detection

Port scanning is a well-used and established hacker technique for gaining access to a system. Your RaQ 4 implementation likely uses typical ports for access, and may have ports defined that are not currently in use or necessary for operation by installed web servers. Up to 65,535 ports can be defined in a Linux system, and while some such as Telnet, SMTP, IMAP, POP3, etc. are commonly used, others that are unused also present opportunities for hackers to gain entry into the system. Port scans check to see what ports are open (have a running application associated), then the hacker selects a port to contact using TCP. Particular ports have known vulnerabilities and have widely-known techniques for exploitation (Netbios port 137, for example, is famous for that). Once TCP communication is established, the hacker can access directories in the target system and load viruses, Trojan Horses, or other executables, associated with “stack smashing”.

Another technique is to scan for open ports, then Telnet (which can be configured to connect via TCP to any port) to an open port and access the system. Even if a port is not open, it may be accessible using TCP.

:
SHP protection against port scanners includes scan detection and logging, plus user-settable threshold settings to record and take action based on the number of ports scanned (from the same IP address) in a settable time interval. Scanners falling within these user-determined parameters are logged and automatically locked out for a fixed time interval.

Scan detection does not monitor legitimate port accesses; that is, to ports used for functions that are running and necessary for installed web server(s). This prevents legitimate users from being locked out due to multiple accesses.

Scan Detection and Access Protocols

While TCP port scanning is probably most common, UDP scanning is also used. UDP scanners typically send empty datagrams to ports. If a port is closed, it will send back an ICMP port unreachable message.

SHP's port scan detection works for both TCP and UDP scans. It works by detecting TCP RST and ICMP type 3 packets sent out by the IP stack in response to probes, allowing the mechanism to work automatically without requiring a list of port numbers. The Linux kernel limits the number of ICMP error packets sent every second, therefore UDP scan detection is slower than TCP scan detection.

Buffer Overflow Protection

A common, dangerous hacking technique is known as "stack smashing". This technique takes advantage of vulnerability created when execution of a called function results in "buffer overflow".

The buffer overflow occurs when the executing function reads external information such as a character string and there is no checking, so the size of the string could exceed the buffer capacity. The buffer allocated at run-time is placed on the stack, which keeps the information for executing functions such as local variables, argument variables, and the return address. The overflowing string overflows the buffer and (for example) overwrites ("smashes") the return address. When the function returns, the return address is the new data instead of the legitimate return address. This data could be an address intentionally placed there by a hacker that returns the program counter to the address of a program (also placed in the system by the hacker through a TCP port access) that then gives the hacker control of the machine.

The functions supplied with the SHP update are installed when SHP is installed, and have been compiled using a modified C compiler. The modified compiler generates code that verifies a function stack has not been smashed before allowing program control to return from the function. If the code detects that the stack has been smashed, the program is terminated and an alert sent (if alerting is enabled).

Buffer overflow protection is always active; alerting is toggled on/off by the user.

Root Privilege Control

If hackers gain access to your system as “Administrator” they may be able to gain root access to other applications. This happens due to “Excessive Root Permissions” vulnerability and is a common “back door” into control of a system.

Excessive Root Permissions vulnerability means that the Administrator of non-essential server applications is given root access permission. By gaining Administrator access on one application, a hacker can gain root access to all the applications on a server. The SHP Security Functions have redesigned the “set UID” permissions on the RaQ 4 to “sandbox” frequently vulnerable applications. Sandboxing an application ensures that if a hacker gains administrative access on one application, they will not receive administrative level permission within any other application.

Root Privilege Control is automatic, and its operation is transparent.

Configuring Security Functions

Security Functions are accessible from a window displayed by clicking on the Control Panel button in the list along the left side of the basic RaQ 4 *Server Management* UI screen (Figure 1). Figure 2 shows the Control Panel screen.

Figure 1. Accessing the Control Panel

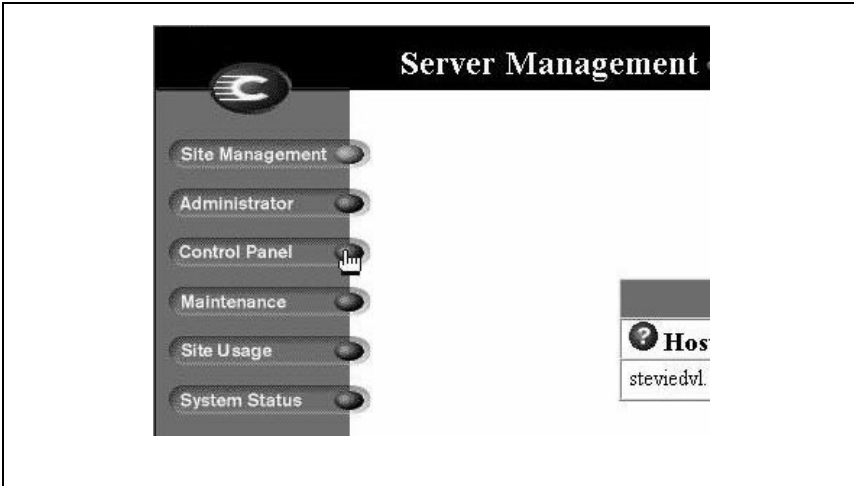
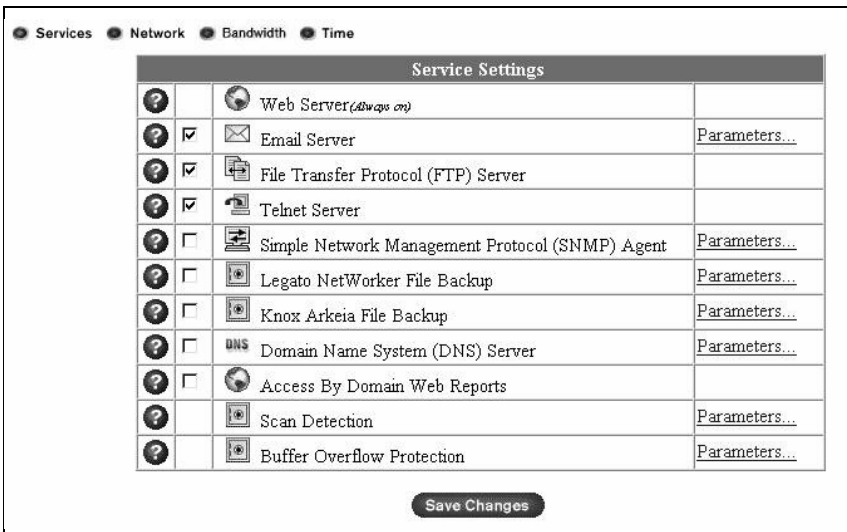


Figure 2. Control Panel Screen



Note the *Scan Detection* and *Buffer Overflow Protection* items at the bottom of the list in Figure 2. You can move the cursor over any of the colored circles with question marks to see explanation text displayed in the along the bottom of your browser window.

Configuring Scan Detection

Click on the blue, underlined, [Parameters](#) link to the right of the Scan Detection item in the Control Panel screen. This brings up the *Scan Detection Settings* screen (Figure 3).

Figure 3. Scan Detection Settings Screen

Scan Detection Settings		
View Log	View Dynamically Blocked IP addresses	Test Email Alerts
?	Action Against Detected Scans	Log only
?	Time Between Scans (In Seconds)	300 (60-600)
?	Number of Ports Scanned	5 (3-8)
?	Enable Email Alerts	<input type="checkbox"/>
?	Email Address for Alerts	
?	IP Addresses Always Blocked	
?	IP Addresses Never Blocked	
		Save Changes Cancel

Starting at the top of the screen as shown in Figure 3, select whether you want to log and block IP addresses from which port scans originate, log only, or neither (do nothing). The decision whether to block a scanning IP address will be made according to the settings you select in the next two fields, *Time Between Scans*, and *Number of Ports Scanned*.

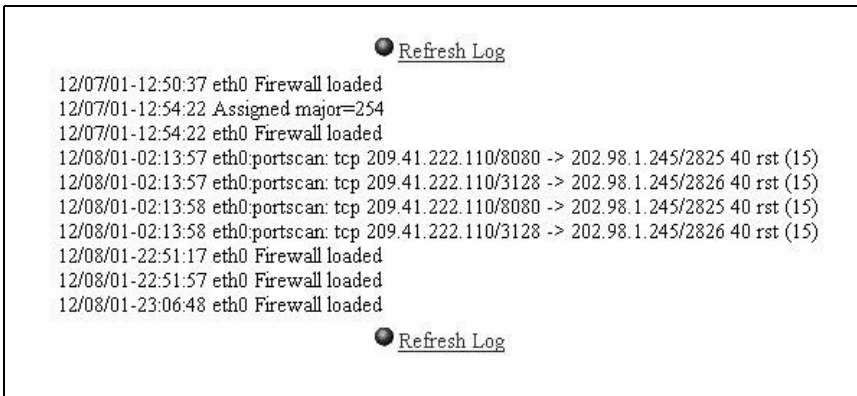
:
For example, with the settings shown in Figure 3, if a port scanner scans 5 different ports in a time interval of not less than 300 seconds between each scan, the IP address of the scanner will be logged, the IP address of the scanner locked out automatically, an email alert sent to the admin user specified for this unit (always), and to the email address specified in the *Email Address for Alerts* field if the *Enable Email Alerts* box is checked. The lockout lasts for five minutes, at which time the lock is reset. If the scanning occurs again, the IP address will again be logged and locked out, email alert sent, and so on. The email alert is always sent to the admin user regardless of whether the *Enable Email Alerts* box is checked

The next (large) field is a place for you to add any known IP addresses that you want blocked regardless of the parameter settings (numbers of ports scanned and time interval). If you keep getting alerts about scanning from a particular IP address, you may want to enter that IP address so that it is permanently blocked and you do not keep getting the alerts. Conversely, the next field is supplied for you to add IP addresses you never want blocked. This allows you to specify known addresses that might have legitimate business with RaQ 4, but would otherwise get blocked due to multiple port accesses falling within the time and port number parameters you have selected. If you mistakenly add the same IP address to both fields, you will get an error message.

- **Note:Do not enter leading zeros in any numeric field. Omit them.**
- Note:You must click the *Save Changes* button for any changes you make to take effect, even while the screen is displayed. For example, if you enter an email address for Alerts, then click the *Test Email Alerts* line, it will not work unless you have saved the changes.

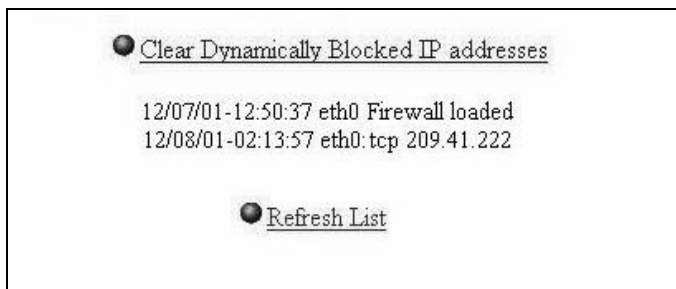
Click on the [View Log](#) or [View Dynamically Blocked Addresses](#) links to see the log of scan attempts (plus other system events), and the list of blocked IP addresses, respectively (Figure 4 and Figure 5).

Figure 4. Scan Attempt Log



The log of port scan attempts logs the most recent 10 events only. While the log is open, new logged attempts can be viewed by clicking on the “Refresh Log” line.

Figure 5. Blocked IP Address Log



The Blocked IP Address Log logs all Dynamically Blocked IP addresses. It does not list blocked IP addresses that have been manually entered into the *IP Addresses Always Blocked* box in the *Scan Detection Settings* window. At some point if the list becomes too long you can click on the *Clear Blocked IP addresses* line to clear the list.

While the log is open, new logged attempts can be viewed by clicking on the *Refresh Log* line.

Buffer Overflow Alerts

In the Control Panel screen, click on the [Parameters](#) link to the right of the Buffer Overflow Protection. This brings up the *Buffer Overflow Protection Settings* screen (Figure 6).

Figure 6. Buffer Overflow Protection Settings Screen



[Test Email Alerts](#)

Buffer Overflow Protection settings	
<input type="checkbox"/> Enable Buffer Overflow Protection alerts	<input checked="" type="checkbox"/>
<input type="checkbox"/> Email Address for Alerts	<input type="text" value="user@anywhere.net"/>

To control email alerts, check/uncheck the box as appropriate, and enter an email address for the alerts.

Note: You must click the *Save Changes* button for any changes you make to take effect, even while the screen is displayed. For example, if you enter an email address for Alerts, then click the *Test Email Alerts* line, it will not work unless you have saved the changes.

The email alert message will include the name of the binary function that overflowed.