Release Note for the Cisco Guard and Cisco Traffic Anomaly Detector

June 15, 2004

Note The most current Cisco documentation for released products is also available on Cisco.com. The online documents may contain updates and modifications made after the hardcopy documents were released.

This release note applies to software version 3.0(8.11) for the Cisco Guard and the Cisco Traffic Anomaly Detector.

This release note contains the following sections:

New Features in Software Release 3.0(8.11)

The following new features have been added in software release 3.0(8.11):

- Multiple SNMP Community Strings
- Adding an SNMP Server Community String
- Removing an SNMP Server Community String
- Enhancement to the Riverhead SNMP MIB
- Setting Rebooting Parameters
- Version Installation Process
- Obtaining Debug Information

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Multiple SNMP Community Strings

The configuration of the SNMP service in release 3.0(8) has the functionality to configure multiple SNMP community strings. This functionality allows access to the SNMP agent from clients in different organizational units and with different community strings on each client. The configuration is done using the existing **snmp community** command that enabled you to change the SNMP community string in previous releases.

Adding an SNMP Server Community String

You may now add a new community string. Note that the Guard default community string is ‘riverhead’.

To add a community string, use the following command from the Configuration command group level.

```
admin@GUARD-conf# snmp community <community-string>
```

The *community-string* defines the community string and may be a maximum length of 15 alphanumeric characters excluding spaces.

Removing an SNMP Server Community String

The **no snmp community** command has been added to enable you to remove an SNMP community string. Note that removing all community strings results in losing the ability to retrieve information through the SNMP server.

To remove a community string, enter the following command from the Configuration command group level. Define the *community-string* as the string you want to remove.

```
admin@GUARD-conf# no snmp community <community-string>
```

Enhancement to the Riverhead SNMP MIB

Time OIDs - All time OIDs have been changed from time-ticks type to string type. The string describes the time and date.

New OID - New OID has been added to the Riverhead MIB 'rhZoneLastAttackTime' in the Zone table. This OID indicates the time of the last detected attack on the Zone.

Setting Rebooting Parameters

You may set parameters that relate to the reboot process.

- The Guard default behavior after reboot does not reactivate zones that were active (for example, either in protect or learning modes) prior to the reboot.
- The Detector default behavior after reboot reactivates zones that were active.

You may change these behaviors to either automatic activation of zones that were active prior to the reboot process or to non automatic activation. To change the reboot parameter, enter the following command from the Configuration command group level:

```
admin@GUARD-conf# [no] boot reactivate-zones
```

Version Installation Process

The version installation process involves from this version only one rpm instead of two rpms as it used to (one rpm for base upgrade and another for the main version rpm).

Obtaining Debug Information

In case of an operational problem in the Guard/Detector, Cisco Technical Support may require you to send internal debug information.

To extract the debug information to an FTP server:

1. Enter the following command from the Global command group level:

```
admin@GUARD# copy debug-core <time> ftp <server> <full-file-name> [<login>]
[<password>]
```

The syntax and variables are shown in the following table.

Parameter	Description
time	The time of the event that triggers the need for debug information. The time string uses the format MMDDhhmm[[CC]YY][.ss] • MM - The month in numeric figures. • DD - The day of the month. • hh - The hour in a 24-hour clock. • mm - The minutes. • [[CC]YY] - (Optional) The year. The last two digits may be entered. • .ss - (Optional) The seconds.
server	The FTP server IP address.
full-file-name	The full name of the log file. Note that the server assumes your home directory if you do not specify a path.
login	(Optional) The FTP server login name. Note that the FTP server assumes anonymous login when you do not insert a login name. The server will not prompt you for a password.
password	(Optional) The FTP server password. Note that if you do not enter a password, you will be prompted for one.

For example:

```
admin@GUARD# copy debug-core ftp 10.0.0.191 debug-file user password

Please wait while gathering the required information...
Finished creating file
FTP in progress...
Passive mode off.
Local directory now /Riverhead/ImpExp
admin@GUARD#
```

Software Version 3.0(8.11) Open Caveats

The following caveats are open in software version 3.0(8.11):

- **CSCuk51099**, **CSCuk51368** - The Guard/Detector may, on rare occasions, stop responding during reload if internet/management traffic reaches the Guard over a virtual interface (VLAN or tunnel) while the Guard is in reload. Workaround: Perform power cycle and continue working.
- **CSCrh00789** - All proxy up/down status addresses are directly linked to Giga1 status. If you shut down the Giga1 interface, all proxy addresses are disabled. Workaround: Use Giga1 as the primary interface. Never perform a shutdown for it while the Guard is in action.
- **CSCrh01198** - The Guard erases the default gateway after reloading if the gateway is on the same subnet as one of the Guard's configured VLAN interfaces. Workaround: Use a static route instead of a default gateway.
- **CSCrh01574** - User-filter counters are not cleared after you issue the **renumber** command. This may lead to erroneous filter counter display. Workaround: Disregard rate information for a maximum of 20 seconds after filter re-enumeration.
- **CSCuk51045** - The upgrade procedure from software release 3.05 does not repartition the hard disk. To perform an upgrade from software release 3.05 to software release 3.0(8.11), you must first upgrade to software release 3.07, then upgrade to 3.0(8.11).

Software Version 3.0(8.11) Resolved Caveats

The following caveats were resolved in software version 3.0(8.11):

- **CSCuk50551** - The GRE interface is always shown as down by SNMP.
- **CSCuk50751** - The SSH key exchange between the Guard and the Detector does not always work.
- **CSCuk50788** - When the automatic protection-termination is activated, the report for the terminated attack is badly created or not created at all.
- **CSCuk50870**, **CSCuk51049** - When you turn off self-protection, the total management traffic to the Guard is limited to 10000 bps. This prevents some traffic from reaching the Guard, including ping with large packets, BGP, and SSH to the GIGA interfaces. Workaround: Always keep the self-protection on.
- **CSCuk50891** - CFE is not upgraded automatically during a version upgrade.
- **CSCuk50893** - When upgrading a software version using a combination of the **copy ftp new-version** and **install new-version** commands, the CM indicates that the product had rebooted and not reloaded. The serious direct impact of this is that the Guard does not reactivate zones after a version upgrade.
- **CSCuk50920** - After you change the hostname, SNMP and syslog still use the old hostname.
- **CSCuk50979** - SNMP Trap Level configuration to level X means that only messages that are more severe than X result in a trap, while messages with severity that equals X do not.
- **CSCuk51052** - When entering ssh-dsa keys using the command **key add username ssh-dsa key comment**, the output of the show running-configuration shows the command as **key add username ssh-dss key comment**.
- **CSCuk51056** - SNMP trap definitions are deleted after version upgrade when you use the **install new-version** command.
- **CSCuk51071** - The CLI exits unexpectedly when you attempt to remove dsa keys.

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

This document is to be used in conjunction with the documents listed in the "Obtaining Technical Assistance" section.