

Traffic Anomaly Detector and Guard (Riverhead Networks) FAQ

Document ID: 63559

Questions

Introduction

What is the default password for the Cisco Traffic Anomaly Detector and Guard?
I changed the date information from 08062004 to a future date of 12012004 using the "date 12012004" CLI command. I then tested the date change to a zone via the SNMP OID rhZoneLastChangeTime. This worked well except when the date is changed to a date earlier than the last changed date. Next, I changed the date back to 08062004 on the CLI. However, the SNMP OID response to query for rhZoneLastChangeTime remained 12012004 (the old date). After a reload, the OID response showed the correct (last) date change. Is this a bug?

What is the difference between TCP Reset and TCP Safe-Reset?

After an upgrade I receive the "Can't connect to management module; SYSTEM IS NOT FULLY OPERATIONAL: Connection refused Can't write to socket" error message. How do I fix this?

When I configure a Zone using the default template, I am unable to find the HTTP policy template under the zone when I issue the "show policies" command. I see every other policy template except for HTTP. How can I find it?

How do I perform root user password recovery?

Can I import custom SSL certificates to Cisco Anomaly Guard?

I received this error message. How can I resolve the issue?

```
RHWatchdog: RHWatchdog: Hardware Monitoring card reports HW errors.
```

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document addresses the most frequently asked questions (FAQs) related to the Cisco Traffic Anomaly Detector and Guard (Riverhead Networks).

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Q. What is the default password for the Cisco Traffic Anomaly Detector and Guard?

A. The default password for the Cisco Traffic Anomaly Detector and Guard is **admin/rhadmin**.

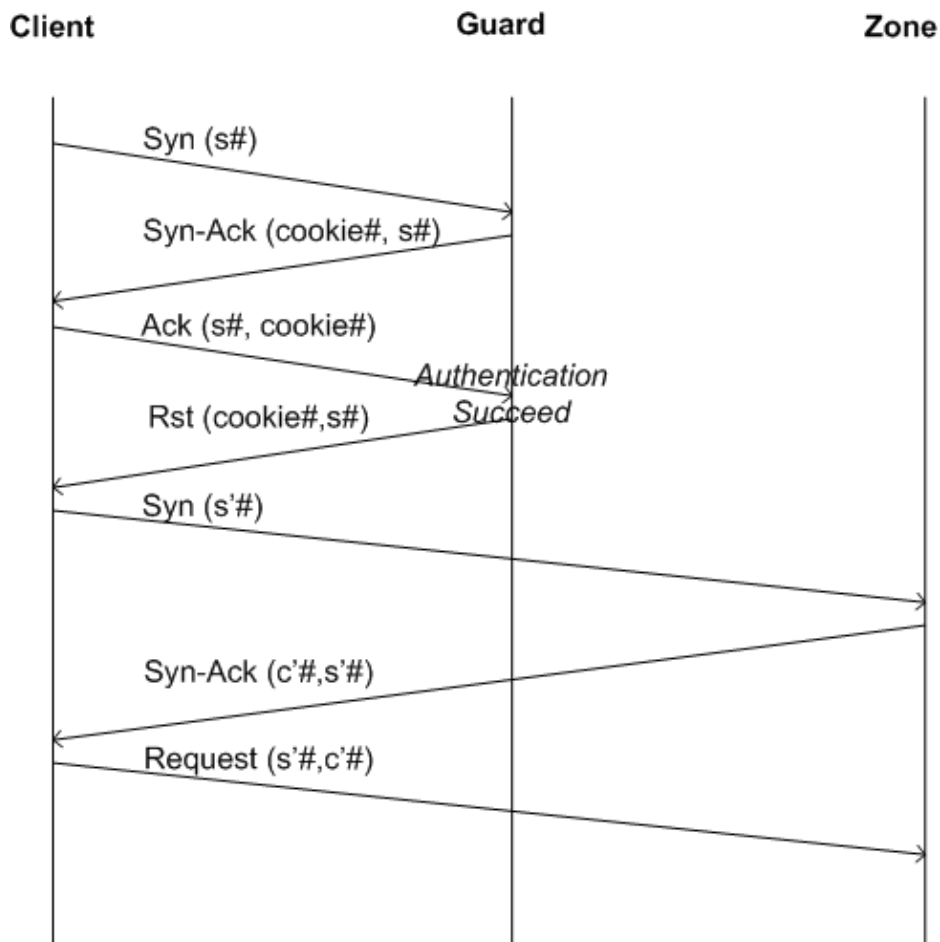
Q. I changed the date information from 08062004 to a future date of 12012004 using the "date 12012004" CLI command. I then tested the date change to a zone via the SNMP OID rhZoneLastChangeTime. This worked well except when the date is changed to a date earlier than the last changed date. Next, I changed the date back to 08062004 on the CLI. However, the SNMP OID response to query for rhZoneLastChangeTime remained 12012004 (the old date). After a reload, the OID response showed the correct (last) date change. Is this a bug?

A. This is Cisco bug ID CSCuk52710 (registered customers only) . It is generally not recommended to change the time of the device backwards. This can result in the overlap of some history data. A workaround for this problem is to restart the snmp-server whenever the time is set backwards:

```
admin@Guard-conf#no service snmp-server
admin@Guard-conf#service snmp-server
```

This clears the SNMP cache and brings the updated data to the requester.

Q. What is the difference between TCP Reset and TCP Safe-Reset?



◆ **Reset:** Suitable for all TCP applications that retry to connect when a RST packet is received (or enable the user to reconnect). The connection is closed with a RST

packet and no tag is sent. See figure for the packet flow of the Reset algorithm.

- ◆ **Safe-Reset:** While the above method requires application-level awareness, safe-reset requires only TCP stack RFC compliance, but adds a 3 second delay to the first connection setup time. It is suitable for most automatic TCP protocols (such as mail). As a reply to the client SYN, the Guard sends an ACK with a bad acknowledgment number which holds a cookie. If the client is compliant with RFC 793, it answers with a RST packet which contains the bad acknowledgment number and retransmits the original SYN after a 3-second timeout. When the Guard receives the RST packet with the bad acknowledgment number, it authenticates the connection and does not interfere with the next connection. The main caveat in this solution is that some firewalls silently drop the badly-numbered ACK even though this is not RFC compliant. In order to provide a solution in such cases, if the Guard receives a second SYN packet from the same source within 4 seconds of the first, with no RST in between, the second SYN is treated in the same way as it is treated in the Reset method.

Q. After an upgrade I receive the "Can't connect to management module; SYSTEM IS NOT FULLY OPERATIONAL: Connection refused Can't write to socket" error message. How do I fix this?

A. In addition to the Can't connect to management module; SYSTEM IS NOT FULLY OPERATIONAL: Connection refused Can't write to socket error message, this error is generated when you reboot:

```
myguard@GUARDUS#reboot
Are you sure? Type 'yes' to reboot
yes
sh: /sbin/reboot: Input/output error
myguard@GUARDUS#

myguard@GUARDUS#show diagnostic-info
Can't connect to managment module; SYSTEM IS NOT FULLY OPERATIONAL:
Connection refused
Can't write to socket
Management module is busy. Please try again in 10 seconds
Failed to get counters
myguard@GUARDUS#

myguard@GUARDUS#
Message from syslogd@GUARDUS at Sun Sep 19 17:38:51 2004 ...
GUARD-US RHWatcdog: RHWatcdog: subsystem failure - CM
```

This looks like a file system error on the guard. In order to solve the FS errors, reboot the guard and watch the **fsck** process closely. If you get into single user mode, issue the **fsck -y /** command to request a manual run of **fsck**.

Q. When I configure a Zone using the default template, I am unable to find the HTTP policy template under the zone when I issue the "show policies" command. I see every other policy template except for HTTP. How can I find it?

A. The default policy is available when you issue the **wr t |** command and include HTTP. This shows you something similar to **policy-template http -1 10.0 enabled**. The Cisco Traffic Anomaly Detector and Guard then looks at traffic that is based on the threshold form

that the HTTP policy is based on.

Q. How do I perform root user password recovery?

A. Refer to Cisco Guard and Traffic Anomaly Detector Password Recovery for instructions on **root** user password recovery.

Q. Can I import custom SSL certificates to Cisco Anomaly Guard?

A. No, Cisco Anomaly Guard only supports the self-signed SSL certificate.

Q. I received this error message. How can I resolve the issue?

RHWatchdog: RHWatchdog: Hardware Monitoring card reports HW errors.

A. Reseat the power supply to resolve the issue.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [Cisco Guard and Mitigation Appliances Technical Documentation](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 10, 2008

Document ID: 63559