Stingray™ Virtual Appliance: Compliance with the Security Technical Implementation Guidelines (STIG)

Version 9.9

January 2015

riverbed®

Riverbed Technology
680 Folsom St.
San Francisco, CA 94107

Phone: 415-247-8800
Fax: 415-247-8801
Web: http://www.riverbed.com

Part Number
712-00164-01

Contents

CHAPTER 1 About This Guide

Introduction

This document describes the set-up procedure necessary to place the Stingray Virtual Appliance into a special *locked-down* state ready for compliance with the Security Technical Implementation Guidelines (STIG). This process is two-fold:

1. Run the built-in lock-down script in order to secure the virtual appliance;
2. Configure the virtual appliance to comply with the STIG requirements.

The first chapter covers the lock-down procedure. The second discusses the configuration key settings required, with a brief description of their use.

This is followed by an introduction to the Maintenance CLI, an alternative control method to the Admin UI. Additional features pertaining to a STIG-compliant Virtual Appliance are included at the end of this document.

Where applicable, the relevant STIG-IDs are provided for reference. These are described in the following documents, available from:

http://iase.disa.mil/stigs/index.html

- UNIX Security Technical Implementation Guide (version 5, release 1)
- Web Server STIG (version 7, release 1)
- Application Security and Development STIG (version 3, release 2)

Pre-requisites

You will require the following:

- The OVF edition of the Stingray Virtual Appliance
- A valid customer account number
- An IP address for the Virtual Appliance
- A valid licence key serial number
- Ensure a suitable server is within network reach of the Virtual Appliance to allow connections via SCP/SFTP

CHAPTER 2 Lock-down Procedure

The following procedure will result in a *locked-down* virtual appliance:

1. Import the OVF version of the Stingray Virtual Appliance into VMware VSphere (or other compatible virtualization platform);

2. Log in to the newly created virtual appliance via **ssh** using the credentials:

   Username: `admin`

   Passsword: `admin`

3. Run the following commands at the prompt:

   ```
   /usr/lib/zeus-customisations/z-lock-down
   ```

4. Follow any instructions given to you by the `z-lock-down` script. This will create a maintenance user **ssh** key-pair, disable password-based **ssh** access, and store the key-pair and other information in a *maintenance details* temporary directory along with a tarball archive of the contents. The location and name of this tarball will be displayed at the prompt.

   Important: The credentials stored within the tarball are the only means to gain root level access to the virtual appliance once you've logged out of the shell you are in. **Do not log off without first copying the tarball off the appliance (covered in the next step)**, or you will need to re-install it from scratch.

   A signature key known as the *Maintenance ID* is generated by the lock-down script. This consists of a series of hexadecimal values separated by colons, and is the alpha-numeric string appended to the name of the maintenance tarball (minus the colons).

   For example, where the Maintenance ID is:

   ```
   aa:bb:cc:dd:ee:ff:00:11:22:33:44:55:66:77:88:99
   ```

   The tarball archive name will be:

   ```
   Stingray-Support-aabbccddeeff00112233445566778899.tar.gz
   ```

   This ID is displayed on the **Diagnose > Technical Support** page of the Admin UI and the login banner of the Maintenance CLI. It can also be found in the TSR (Technical Support Report), and is required by your support provider in order to identify the correct maintenance credentials tarball created through this procedure.

5. Using the command **scp**, copy the tarball to a **secure** location outside of the virtual appliance;

6. Type `reboot` at the prompt to restart your virtual appliance. This will ensure that any remaining temporary files are removed.

Provided that you have completed the procedure set out in this guide, and have procured the necessary maintenance tarball archive, your virtual appliance should now be in a locked-down state ready for the STIG compliance operations (covered in the next chapter).

Informing Your Support Provider

It is imperative that upon completing the lock-down procedure you inform your support provider. This can be achieved by opening a new Support case indicating that you have created a locked-down virtual appliance and gained the necessary maintenance details tarball.

Important: Do not send the maintenance tarball unless instructed to do so by a designated and verifiable support engineer.

You will need to indicate if your local security policy allows transfer of the maintenance tarball off-site. Depending on the answer to this question, one of two procedures will apply:

Your Security Policy Allows Transfer of the Maintenance Tarball

In this case, your support provider will respond to the newly opened support case with an email providing instructions on how to perform a secure file transfer for the tarball.

Please follow this procedure and wait for acknowledgement that your tarball has been successfully received. It is very important that you do not delete your copy of the tarball without first gaining this acknowledgement.

Your Security Policy Forbids Transfer of the Maintenance Tarball

If you are prohibited from providing the tarball to your support provider, you should instead store it in a secure and reliable location of your choosing. It is conceivable that this tarball may be held for a long period of time without being required, so it is recommended that you be satisfied with the long-term retrieval and backup processes in place.

Please then inform your support provider of its existence, including as much detail as possible. Ideally, the specific location, full file path, and the contact details of the person/role responsible for the server or service holding the tarball. This will assist your support provider in locating the maintenance details should the person originally responsible for configuring the Z100 no longer be available at that point in time.

If you have questions about any aspect of the procedures discussed in this chapter, please contact your support provider for assistance.

CHAPTER 3 Configuring Stingray Virtual Appliance for STIG Compliance

Logon Banners

These settings are configured in the **Login and Security** section of the **System > Global Settings** page.

`login_banner`	Sets the desired login banner (shown before login). (GEN000400, GEN000420)
`banner_accept`	Set to yes if users should explicitly accept the terms of the login banner before logging in.
`post_login_banner`	Sets the desired `post_login_banner` (shown after a successful login).
`uipage_banner`	Set a banner that will be displayed on all pages of the UI. (V-6146 APP3270)

Login Security

These settings are configured in the **Login and Security** section of the **System > Global Settings** page.

`max_login_attempts`	The number of sequential failed login attempts that will cause a user account to be suspended. Setting this to 0 disables this feature. Default: 0 STIG: Set to: 3 (GEN000460)
`max_login_external`	Whether or not usernames blocked due to the `max_login_attempts` limit should also be blocked from authentication against external services (such as LDAP and RADIUS). Default: No STIG: Set this to Yes unless the external service implements its own login suspension for failed passwords.
`max_login_suspension_t`	The number of minutes for which users who have

ime	exceeded the `max_login_attempts` limit should be suspended. Default: 15 STIG: set to 15 (default) (GEN000460)
`login_delay`	The delay, in seconds, after a failed login before another login attempt can be made. Default: 0 STIG: set to 4 (GEN000480)
`bootloader_password`	Enable or disable bootloader password protection. Note on a Stingray Virtual Appliance, this only sets the bootloader password used for choosing between different versions of the Stingray software. Even if this is unset, a vendor-only password prevents access to the recovery shell. STIG: Enable and set password (LNX00140)

Password Restrictions

These settings are configured in the **Password Security Settings** section of the **System > Users > Local Users > Password Policy** page.

`password_security`	Sets various password security settings. For STIG compliance, set to "default", which sets settings as follows: min_password_length: 8 (GEN000580) min_alpha_chars: 2 (GEN000600) min_uppercase_chars: 1 (GEN000600) min_numeric_chars: 1 (GEN000620) min_special_chars: 1 (GEN000640) allow_consecutive_chars: No (GEN000680)

	(Or choose "custom" to set individual values for these items.)
`password_reuse_after`	Sets the number of times passwords must be changed before the same password can be set again. STIG: set to 10 (GEN000800)
`password_changes_per_day`	Sets the maximum number of password changes per day. STIG: set to 1 (GEN000540)

The password expiry time is set by permission group, from:

System > Users > Groups > {admin, Demo, Guest, Monitoring}

`password_expire_time`	Sets the number of days after which members of a group must change their passwords. If set to 0 (default), members are never required to change their passwords. STIG: set to 90 for all four default groups, and any new groups (GEN000720)

CHAPTER 4 The Maintenance CLI (Command Line Interface)

You will normally administer the Stingray Virtual Appliance through the web-based Admin UI. However, you can also access the appliance through the maintenance CLI to access the command sub-system and perform various system maintenance operations. To do this, you can log in to the appliance using an SSH client.

The maintenance CLI is presented as a limited shell, with a number of useful commands. Typing '`help`' at the prompt provides a list of the available commands. Specific help for each command can be displayed by typing '`help <command>`'. The current appliance you are connected to is indicated by the hostname appearing at the prompt (`stm1` in the example below):

```
Last login: Tue Jan 25 08:43:48 2011 from 10.100.1.86
------------------------------------------------------------
Stingray Traffic Manager Maintenance CLI

Type 'help' for information on available commands.
------------------------------------------------------------
Maintenance ID: aa:bb:cc:dd:ee:ff:11:22:33:44:55:66:77:88:99:00
------------------------------------------------------------
stm1 >
```

The CLI commands broadly fall into two categories. Firstly, commands to gather support information, such as traces, tcpdumps and networking information. Or secondly, commands to restore access to the web-based Admin UI on a machine, such as when you break the networking configuration.

Below is a list of the current CLI commands:

<table>
<tr>
<td><code>delete-file</code></td>
<td>
Usage:

<code>delete-file <filename></code>

Arguments:

<table>
<tr><td><code>filename</code></td><td>The support file or log to delete.</td></tr>
</table>

Delete a support file or log from disk. Use the 'list-files' command to see all files that can be deleted. Deleting 'errors' will clear the event log, this action must be confirmed. Audit log files cannot be deleted. Wildcard characters can be used to delete multiple files.

Aliases:

<code>rm</code>
</td>
</tr>
</table>

`exit`	Logs you out of the CLI and terminates your session. Aliases: `Logout, quit`
`firewall-clear`	Clears all internal firewall rules on the traffic manager. This should only be used if the system's firewall settings have caused the virtual appliance to become un-contactable. To see the current firewall rules, run command '`info firewall`' (as shown below).
`info`	Available with the following sub-commands: `arp, disk, firewall, interfaces, maintenance-id, memory, nat, net-devices, net-stats, ports, processes, routes, sockets, version` Displays various different types of system information.
`install-package`	Usage: `install-package <package>` Install a package uploaded to the 'uploads' directory. The command displays information about the package and requests confirmation before installing. Use '`help scp`' for more information on uploading files. Arguments: `package` — The package to install. It must be under the 'uploads/' directory.
`list-files`	Usage: `list-files` Lists files that can be accessed by the maintenance CLI and the sizes of the files. These files can be viewed (using the '`view-file`' command), deleted (using the '`delete-file`' command) and

<table>
<tr>
<td></td>
<td>
downloaded with <code>scp</code> (use '<code>help scp</code>' for further details).

The files available are:

<table>
<tr><td><code>errors</code></td><td>Event log</td></tr>
<tr><td><code>audit</code></td><td>Audit log</td></tr>
<tr><td><code>tmp/*</code></td><td>Temporary files</td></tr>
<tr><td><code>statd/*</code></td><td>Historical activity logs</td></tr>
<tr><td><code>vservers/*</code></td><td>Virtual server request logs</td></tr>
<tr><td><code>maintenance/*</code></td><td>Files created by the maintenance CLI</td></tr>
<tr><td><code>uploads/*</code></td><td>Files uploaded using <code>scp</code></td></tr>
<tr><td><code>discoveryagent/*</code></td><td>Steelhead discovery agent support data</td></tr>
</table>

Aliases:

<code>ls</code>
</td>
</tr>
<tr>
<td><code>network-configure</code></td>
<td>
Usage:

<code>network-configure <ip> <netmask> [<interface>] [<gateway>]</code>

Arguments:

<table>
<tr><td><code>ip</code></td><td>The IP address to use.</td></tr>
<tr><td><code>netmask</code></td><td>The netmask to use.</td></tr>
<tr><td><code>interface</code></td><td>The interface to setup. If omitted the interface is assumed to be your primary network interface,</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td></td><td>usually <code>eth0</code>. (optional)</td></tr>
<tr><td><code>gateway</code></td><td>The IP address for default gateway of the interface. (optional)</td></tr>
</table>
Sets up the IP address and netmask of the primary ethernet interface. You can optionally specify an alternative network interface (rather than the default primary) or gateway IP. It will wipe any existing setup for the interface, and should only be used if the networking settings have caused the appliance to become un-contactable.
NOTE: If using the CLI over SSH, this command may terminate your session.
</td></tr>
<tr><td><code>reboot</code></td><td>Reboots the Stingray Virtual Appliance. This will also log you out of the Admin UI.</td></tr>
<tr><td><code>reset-to-factory-defaults</code></td><td>Resets all configuration and settings to the factory defaults. All system and traffic management configuration will be lost by running this command and the system will be rebooted. You will be asked to confirm this action.</td></tr>
<tr><td><code>restart</code></td><td>
Usage:
<code>restart [<component>]</code>
Arguments:
<table>
<tr><td><code>component</code></td><td>The component to restart. (optional - if not set, <code>all</code> is assumed)

Can be one of: <code>all, traffic_manager, ui, rest_api, hardserver.</code>

Note that <code>all</code> does not include <code>hardserver</code>.</td></tr>
</table>
Restarts the component specified, or all components by default (excluding the hardserver). This will be the traffic management service, the admin UI and the REST API service. You can specific a component of <code>traffic_manager</code>, <code>ui</code> or <code>rest_api</code> to restart these
</td></tr>
</table>

<table>
<tr><td></td><td>components individually.

The ‘hardserver’ is a background process that handles communications with an nShield HSM device. It should not normally be necessary to restart this process unless communications have been disrupted for some reason, or if instructed to do so by your support provider. Please refer to your nCipher documentation for more details.</td></tr>
<tr><td><code>rollback-delete</code></td><td>Usage:

<code>rollback-delete <revision></code>

Arguments:

<table><tr><td><code>revision</code></td><td>The previously installed revision to delete.</td></tr></table>
Completely removes an archived minor revision of the traffic manager software. Note that you will not be able to retrieve the revision once you have performed this action.

This command facilitates removal of minor revisions of the presently installed full version only. For example, if this appliance is running version 8.0, you will only be able to remove minor ‘r’ revisions installed for this version.

If you wish to remove ‘r’ revisions for other versions, you would first need to perform a full version rollback through the appliance ‘grub menu’ (see the Stingray Virtual Appliance Getting Started Guide for full details).</td></tr>
<tr><td><code>rollback-list</code></td><td>Usage:

<code>rollback-list</code>

Lists all previously installed revisions of the current traffic manager software version.</td></tr>
<tr><td><code>rollback-to</code></td><td>Usage:

<code>rollback-to <revision></code></td></tr>
</table>

<table>
<tr><td></td><td>Arguments:
<table><tr><td>revision</td><td>The previously installed revision to delete.</td></tr></table>
Performs a roll-back to the desired revision of the traffic manager software.

This command facilitates rolling back to a minor revision of the presently installed full version only. For example, if this appliance is running version 8.0, you will be able to roll back to minor ‘r’ revisions installed for this version.

If you wish to roll back to ‘r’ revisions for other versions, you would first need to perform a full version rollback through the appliance ‘grub menu’ (see the Stingray Virtual Appliance Getting Started Guide for full details).</td></tr>
<tr><td>shutdown</td><td>Shut down the Stingray Virtual Appliance. This will also log you out of the Admin UI.</td></tr>
<tr><td>start</td><td>Usage:

start [<component>]

Arguments:
<table><tr><td>component</td><td>The component to start. (optional - if not set, all is assumed)

Can be one of: all, traffic_manager, ui, rest_api, hardserver.

Note that all does not include hardserver.</td></tr></table>
Starts the component specified (if stopped), or all components by default (excluding the hardserver). This will be the traffic management service, the admin UI and the REST API service. You can specific a component of traffic_manager, ui or rest_api to start these components individually.

The ‘hardserver’ is a background process that handles communications with an nShield HSM device. It should not</td></tr>
</table>

<table>
<tr><td></td><td>normally be necessary to send commands to this process unless instructed to do so by your support provider. Please refer to your nCipher documentation for more details.</td></tr>
<tr><td>stop</td><td>Usage:

stop [<component>]

Arguments:

<table><tr><td>component</td><td>The component to stop. (optional - if not set, all is assumed)

Can be one of: all, traffic_manager, ui, rest_api, hardserver.

Note that all does not include hardserver.</td></tr></table>
Stops the component specified, or all components by default (excluding the hardserver). This will be the traffic management service, the admin UI and the REST API service. You can specific a component of traffic_manager, ui or rest_api to stop these components individually.

The ‘hardserver’ is a background process that handles communications with an nShield HSM device. It should not normally be necessary to send commands to this process unless instructed to do so by your support provider. Please refer to your nCipher documentation for more details.</td></tr>
<tr><td>support-report</td><td>Generates a support report tarball (.tgz) and places it in the support files directory. It can then be downloaded via the Support Files page in the Admin UI or using the scp tool from a remote client (use 'help scp' for further details).</td></tr>
<tr><td>tcpdump</td><td>Usage:

tcpdump <interface> <mode> <additional>

Arguments:

<table><tr><td>interface</td><td>The interface to listen on, or 'any' to listen on</td></tr></table></td></tr>
</table>

	<table><tr><td></td><td>all interfaces. Must be one of: <code>any, eth0, lo.</code></td></tr><tr><td><code>mode</code></td><td>Determine the type of output to produce. '<code>text</code>' prints text information on the packet and '<code>raw</code>' prints out raw binary data. Must be one of: <code>text, raw</code>.</td></tr><tr><td><code>additional</code></td><td>Additional parameters and filters. Specified in the same format as the command-line arguments to <code>tcpdump</code>.</td></tr></table> Captures packet information passing through the traffic manager appliance. Running this command outputs the packet capture to *stdout* and to disk. The file on disk can be accessed via the **Diagnose > Support Files** page of the Admin UI. To stop the packet capture, type **Ctrl+C**.
`trace`	Usage: `trace <process> <additional>` Arguments: <table><tr><td><code>process</code></td><td>The type of process to trace, as requested by your support provider. Must be one of: <code>children, child, parent, eventd, flipper, admin, monitor, sysd.</code></td></tr><tr><td><code>additional</code></td><td>Additional flags to use when tracing. Specified in the same format as the command-line arguments to <code>trace</code>.</td></tr></table> Trace a traffic manager process. This should only be done if requested by your support provider. Running this command outputs the trace to the standard out and to disk. The file on disk

<table>
<tr><td></td><td>can be accessed via the Diagnose > Support Files page of the Admin UI (discussed below).

To stop the trace, type Ctrl+C.</td></tr>
<tr><td><code>view-file</code></td><td>Usage:

<code>view-file <filename> [lines]</code>

View a support file or log from disk. Use the '<code>list-files</code>' command to see all available files. Can only view text files.

Arguments:

<table><tr><td><code>filename</code></td><td>The support file or log to view.</td></tr><tr><td><code>lines</code></td><td>The number of lines from the file to display. (Optional)</td></tr></table>
Aliases:

<code>cat</code></td></tr>
</table>

CHAPTER 5 Additional Features

The Audit User

STIG-compliant Stingray Virtual Appliances provide a dedicated 'audit' user and group. This user cannot be modified or removed, has specific access to only view Audit/Event log pages, and is solely authorized to remove qualifying audit log archive files (files that are older than the pre-set minimum retention age of five years). Archived audit logs are maintained on the **Diagnose > Audit Log > Audit Archive** page of the Admin UI. Please refer to the *Stingray Traffic Manager User Manual* for details on Audit logging, including rotation, archiving and deletion.

No other user account has the ability to remove audit logs in order to maintain a more secure audit trail, including members of the admin group. Additionally, only the audit user can change his or her own password. The audit *group* provides the pre-configured set of access privileges necessary for this sole audit user. It too cannot be modified or removed, and no other users can be added into it.

The audit user password is first set during the Initial Configuration Wizard. Step 6 of the wizard is modified to allow you to set the password for both the **admin** and **audit** users as shown below:

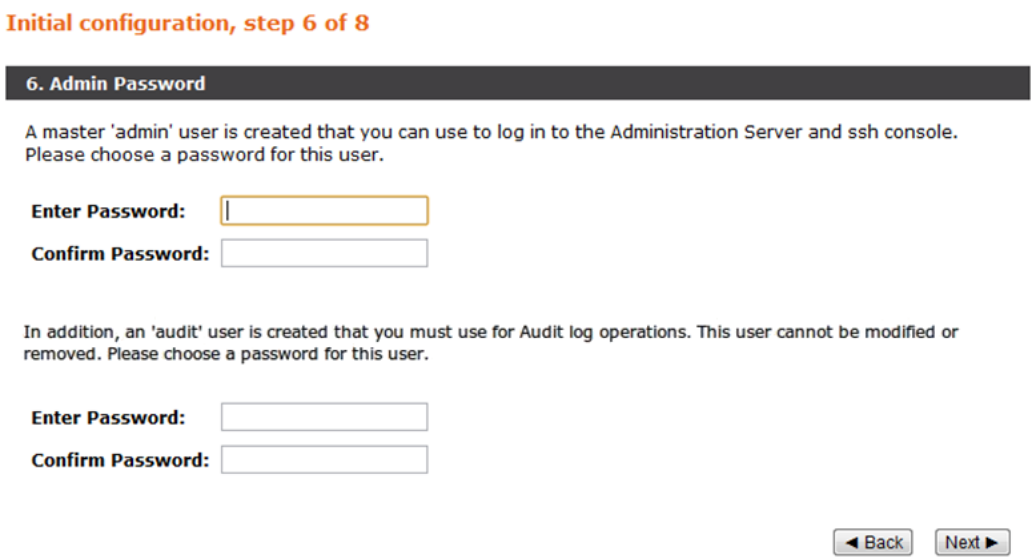

Fig. 1. Entering the Admin and Audit passwords

The Support Files Page

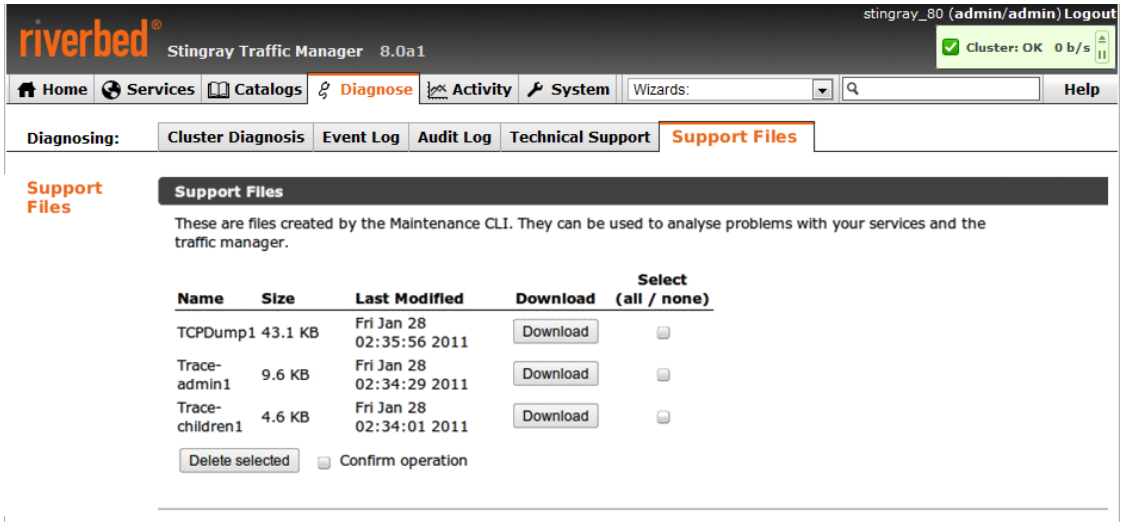

Fig. 2. The Support Files page

In the event that you encounter issues or problems that compromise the normal performance of your system, your support provider can often diagnose the cause by analyzing various system logs and parameters gathered in the *Technical Support Report* generated from the **Diagnose > Technical Support** page.

In addition to this, you can generate system traces and TCP dumps through the Maintenance CLI that can help provide detailed process data to your support provider of the state of the appliance during the period of inoperability. Such output is captured in files that are available to download from the **Diagnose > Support Files** page of the Admin UI. Please refer to *The Maintenance CLI (Command Line Interface)* section above for detailed instructions on the Maintenance CLI.