LanRover VPN Gateway 6.59
FIPS 140-1 Security Policy

Shiva Corporation
900-0949-00
Revision A
April 1999
# Contents

CONTENTS.................................................................................................................................................................................................................. 2

DIFFERENCES BETWEEN 6.5 AND 6.59........................................................................................................................................................................................................ 4

LRVG SECURITY POLICY ...................................................................................................................................................................................................... 10

OVERVIEW .................................................................................................................................................................................................................. 10
FIPS COMPLIANT MODE OF OPERATION ........................................................................................................................................................................ 10
ROLES ...................................................................................................................................................................................................................... 11
LRVG SERVICES ........................................................................................................................................................................................................... 12
LRVG ADMINISTRATOR INTERFACE ........................................................................................................................................................................... 13
DATA ITEMS (OBJECTS) .................................................................................................................................................................................................... 14
AUTHENTICATION METHOD ................................................................................................................................................................................................ 15
IDENTIFICATION AND AUTHENTICATION (I&A) ................................................................................................................................................................. 16
VPN SET UP ........................................................................................................................................................................................................... 16
ACCESS MODES ........................................................................................................................................................................................................ 17
ACCESS CONTROL ......................................................................................................................................................................................................... 17
OBJECT REUSE ........................................................................................................................................................................................................ 17
ZEROIZATION CAPABILITY .................................................................................................................................................................................................. 17
PHYSICAL SECURITY .................................................................................................................................................................................................... 18
CRYPTOGRAPHIC OFFICER USERS .............................................................................................................................................................................. 19
LRVG ERRORS ....................................................................................................................................................................................................... 19
LRVG SESSIONS ...................................................................................................................................................................................................... 21
KEY MANAGEMENT ..................................................................................................................................................................................................... 21
LRVG SELF TESTS ..................................................................................................................................................................................................... 22

CONSOLE ERROR MESSAGES .................................................................................................................................................................................................. 23

SYSLOG MESSAGES ......................................................................................................................................................................................................... 29

[cert] SYSLOG MESSAGES .................................................................................................................................................................................................. 29
[debug] SYSLOG MESSAGES .................................................................................................................................................................................................. 34
[in-proxy] SYSLOG MESSAGES .................................................................................................................................................................................................. 36
[keys] SYSLOG MESSAGES .................................................................................................................................................................................................. 38
[oneway-in] SYSLOG MESSAGES .................................................................................................................................................................................................. 38
[oneway-out] SYSLOG MESSAGES .................................................................................................................................................................................................. 40
[out-proxy] SYSLOG MESSAGES .................................................................................................................................................................................................. 43
[system] SYSLOG MESSAGES .................................................................................................................................................................................................. 45
[tunnel] SYSLOG MESSAGES .................................................................................................................................................................................................. 50

TROUBLESHOOTING TIPS ....................................................................................................................................................................................................... 56

LanRover VPN Gateway FIPS 6.59 Addendum
INTRODUCTION

This document describes the differences between the LanRover VPN Gateway 6.5 and the LanRover VPN Gateway 6.59 FIPS Compliance release.

The LanRover VPN Gateway (LRVG 6.59) satisfies the FIPS 140-1 Level 2 cryptographic module requirements. The LRVG has been subjected to testing at an accredited Lab under the cryptographic module validation program administered by the National Institute of Standards and Technology (NIST) in the USA and the Communications Security Establishment (CSE) in Canada.
Differences between 6.5 and 6.59

Validated Cryptographic Standards
The LRVG contains a validated DES algorithm, a validated secure hash standard (SHA-1), a FIPS approved pseudo-random number generator, and a FIPS approved public key cryptographic system.

Tamper Evident Seals on Rear of Unit
Any attempt to open the unit will break, fracture, or otherwise mutilate the tamper evident seals on the rear of the chassis. Take care not to scratch or damage these tamper resistant labels. Any sign of tampering voids the FIPS certification.

First Time Deployment Of The LRVG
Certain error messages are displayed on the console during the start-up process when the LRVG is deployed following receipt from the manufacturer or following a reset by the Cryptographic Officer. The error messages displayed at this time are part of the normal first time deployment start-up sequence and will be resolved by the normal configuration process.

The Cryptographic Officer must perform the following steps and enter the following commands when prompted:

- Accept the Shiva LRVG license agreement
- Enter an IV and press the “enter” key when prompted
- Enter the default password “shiva” and press the <enter> key
- Enter “write” and press the <enter> key
- Enter “update-fips-fcs” and press the <enter> key
- Enter “reboot” and the <enter> key or switch the power off and then on again

The following error messages are acceptable only upon first time deployment:

- Failed to open the IV file
New and Modified Commands

The new command “update-fips-fcs” is provided to recalculate the flash disk CRC values and update the FIPSFCS file.

The “Show hardware” command has been modified to indicate the Data output interface status.

No Software Encryption

The LanRover VPN Gateway FIPS Version 6.59 will stop operating if the hardware encryption fails as the software encryption is disabled. In the LanRover VPN Gateway Version 6.5, if the hardware encryption board fails, the device automatically switches to software encryption.

SVM Not Compatible With LRVG 6.59

The SVM is not compatible with the FIPS compliant LRVG due to differences at the underlying interface level. The Console is the only permissible administrator interface.

Initialization Vector (IV) Prompt

When you initially set up the LanRover VPN Gateway (or the LRVG was reset) and accept the license agreement, you are then prompted for an Initialization Vector (IV). Please note this extra step when using the Hardware Installation Map and the Manager Installation and Configuration Guide p. 3-36. You may enter an 8-byte IV or press Return for a NULL IV. For compatibility reasons with other LanRover products, we suggest you press Return.

Re-enter Initialization Vector (IV)

To re-enter the IV, the LRVG must be zeroized. This will reset it to the same condition as when it was received from the
manufacturer. Refer to the LRVG security policy for the zeroization procedure.

**No Telnet for Administration**

The Cryptographic Officer must configure the LRVG on initial deployment to set the Telnet sessions to zero (0).

The Console is the only administrator interface permitted for the Cryptographic Officer to administrate the LRVG.

**No TFTP Functionality**

The copy command has been disabled thereby preventing files from being copied to and from the LRVG.

**NO Entrust**

The FIPS LRVG is not compatible with Entrust at this time.

**Only SST with Auth Key Available**

The LRVG may only be used with the Shiva Smart Tunneling (SST) using an authentication key (sometimes referred to as the challenge key). The following authentication methods are NOT available:

1. Certificates;
2. CA Authentication Key;
3. Manager Key;
4. RADIUS keys;
5. IPSec Authentication key
6. PAP and CHAP passwords

**Upgrading LRVG Software Disabled**

Since the copy command has been disabled, the Administrator can not upgrade the LRVG software. The LRVG must be returned to the manufacturer to be upgraded with a FIPS compliant version.

**Packet Keys Eliminated**

When a packet is encrypted, a brand new packet is created. The key (or keys in the case of Triple Pass DES and 3DES) used to
encrypt the original packet in SST (Shiva Smart Tunneling) encapsulation is called a packet key. Packet keys are not used in the FIPS 6.59 version. Take note of this when reading the VPN Concepts Guide, page 26, and anywhere else packet keys are discussed. The session key is used in place of the packet key.

**Field Service Guide Not Applicable**

The Field Service Guide that can be ordered along with the LanRover VPN Gateway is not applicable to the FIPS 6.59 Version of the LanRover VPN Gateway. The chassis is not permitted to be opened. Opening the chassis voids the FIPS certification. You must return the unit to the manufacturer for servicing or upgrading.

**Key Size Requirements**

The LanRover VPN Gateway 6.59 version requires keys (and passwords considered as keys) of exactly 8 alphanumeric characters for a properly formatted 64-bit DES key to maintain the FIPS certification. For robustness, the LRVG will accept passwords that are not 8 characters in length; however, the LRVG is then not operating in an approved FIPS mode.

**Key Entry Procedures**

The LanRover VPN Gateway 6.59 version requires keys to be entered twice for positive verification at the console command line (according to the command syntax).

The LanRover VPN Gateway 6.59 version requires keys to be entered twice for positive verification. When using the Console, the key must be entered twice on the command line according to the command syntax.

The Cryptographic Officer enters the following keys:

- CA Authentication key
- Authentication key
- Manager key (Future capability)
- IPSec Authentication key
- Encrypt key
- Radius primary key
- Radius secondary key
- Radius primary acct key
- Radius secondary acct key

**Manager Password**

The LRVG uses the manager password as a key for SVM sessions (not available in FIPS LRVG 6.59). Therefore, this password must be exactly 8 alphanumeric characters in length for proper security to meet the FIPS operating requirements for keys.

NOTE: This feature is not active for the FIPS LRVG V6.59 and is for future capability to be used with the SVM.

**LRVG Integrity Check**

On power up or reset, the LRVG verifies its operating system and files on the flash disk. If the integrity verification fails, the LRVG will stop processing packets and display the appropriate error message.

The LRVG status and additional error information can be obtained by issuing the “show hardware” command. This command will return, among other information, the status of the data output interfaces. The message “Data Output Interfaces Enabled” or “Data Output Interfaces Disabled” will be displayed on the console indicating the LRVG status.

**Returning The LRVG To Shiva**

The LRVG must be zeroized before returning the LRVG to Shiva. Zeroizing the LRVG ensures the keys and other security critical parameters are not compromised in transit or at Shiva. In addition, the same unit may not be returned.

Refer to the LRVG security policy for the zeroization procedure.

**Reset Command**

The Reset command uses a parameter “RESET” and not a password as incorrectly stated in the LRVG 6.59 documentation. The correct syntax is:
enable <parameter>

where parameter = “RESET”.
LRVG Security Policy

Overview

The LRVG is a multifunction domain isolator separating two or more network domains from each other by providing routing, bridging, firewall, and VPN services. The typical configuration is to use the LRVG to separate a private network from the internet and use tunnels (encrypted sessions) to communicate over a public network to provide confidentiality and integrity services.

The LRVG permits packets matching pre-configured rules (such as valid routing or tunnel entries) to pass from one domain to another. The security policy addresses only the Encryption/decryption (tunnel) and bypass functions (firewall, bridging, filters, and routing services). The details of the bypass functions will not be discussed (they are not security relevant) except for those directly related to the bypass mode. The Cryptographic Officer accesses the LRVG configuration, status, and tunnel services via the control input interface (administrator interface).

The security policy contains policy statements for only those LRVG features usable within the FIPS 140-1 mode of operation.

FIPS Compliant Mode Of Operation

The LRVG is configured by the manufacturer at compile time to be in FIPS 140-1 mode.

The Cryptographic Officer must configure the LRVG on initial deployment to set the Telnet sessions to zero (0) to ensure that only the Console is the administrator interface used for LRVG administration.

The Authentication Key with Diffie-Hellman (using Shiva Proprietary SST method) is the only authentication method to be used within the FIPS 140-1 mode of operation Refer to the Authentication Method section on Page 15.
Roles

Cryptographic Officer - An individual who is authorized to enter keys and other security critical parameters, configure, and monitor the LRVG using the control input interface.

User – This role is implicitly assigned to the Cryptographic Officer role.

Notes:

1. A maintenance role is not defined as there is no maintenance access interface. The LRVG must be returned to the manufacturer for service.

2. There are no other users defined. Source and destination network entities are not considered to be users since they do not have access to the control input interface to configure LRVG services.

Cryptographic Officer Role

The LRVG permits the Cryptographic Officer role access to all services, security critical parameters, and configuration parameters; however, separation of duties may be enforced procedurally. Separation of duties is recommended to be followed as a good security practice as described below.

The Cryptographic Officer role is authorized to perform all functions including but not limited to entering and revising key data and other critical security parameters:

1. Virtual private network (tunnels);
2. Encryption and decryption (tunnels);
3. Bypass mode (firewall functions including proxies, filters, bridging, and routing);
4. Key exchange;
5. Key management;
6. Audit functions; and
7. Cryptographic module management functions.
LRVG Services

The LRVG provides tunnel services only to the authorized Cryptographic Officer configuring the LRVG. The LRVG controls the flow of packets through the LRVG via the pre-configured interface ports and established tunnels. All tunnels provide encryption and are used to implement virtual private networks (VPN).

The following services are available within the cryptographic module:

1. Virtual private networks (tunnels);
2. Encryption and decryption (tunnels);
3. Bypass mode (firewall functions including proxies, filters, bridging, and routing);
4. Key exchange;
5. Key management;
6. Configuration of packet entry and exit via the supported interfaces;
7. Audit functions; and
8. Cryptographic module management functions.

DES Encryption Modes Of Operation

The LRVG provides three DES variation modes of operation. The following table maps the LRVG encryption/decryption functions to the FIPS DES modes of operation. Note that the LRVG Triple DES and 3DES use the same DES mode of operation with different key sizes.

<table>
<thead>
<tr>
<th>LRVG Function</th>
<th>FIPS Mode of Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES</td>
<td>DES with Cipher Block Chaining (56 bit key)</td>
</tr>
<tr>
<td>Triple DES</td>
<td>TDEA Triple Cipher Block Chaining Mode (112 bit key)</td>
</tr>
<tr>
<td>3DES</td>
<td>TDEA Triple Cipher Block Chaining</td>
</tr>
</tbody>
</table>
Encryption/Decryption Service

The Cryptographic Officer must positively select encryption/decryption services by selecting a tunnel service and its associated encryption mode (DES, Triple DES, or 3DES) in the security profile. There can be multiple tunnels each with a different encryption mode. Tunnels are distinct virtual interfaces and may exist within the LRVG at the same time with bypass services that are also distinct interfaces.

A non-encryption service (firewall, filter, etc) may be selected at the same time as a tunnel and still maintain the encryption/decryption service.

Bypass Service

The Cryptographic Officer must positively select a bypass service (firewall, filter, etc) without selecting a tunnel service. Bypass services may exist within the LRVG at the same time as tunnel services.

LRVG Administrator Interface

The LRVG may only be configured via an authorized user using the appropriate administrator interface. The Cryptographic Officer user must enter the “Enable password” for authentication purposes to access the administrator interface. The syntax for the LRVG access password is “enable <password>“.

The available interfaces are:

**Console** - a command line interface using the LRVG console port (COM1);

**Shiva VPN Manager** - a proprietary graphical user interface (GUI) through one of the network interface ports via a network connection.

The LRVG Administrator interface serves as the control input interface and the status output interface.

To use the Shiva VPN Manager, the Cryptographic Officer must configure the control input interface to enable a physical interface and enter the SVM IP address.
Data Items (Objects)

Access Password

The LRVG uses the “Enable password” to authenticate the Cryptographic Officer before granting access to the “Configuration Mode” of the control input interface.

Upon initialization of the LRVG, the Cryptographic Officer must use the default password “shiva” which is set by the manufacturer. The Cryptographic Officer is required to change the default password to a new password consisting of between 6 and 60 alphanumeric characters.

Reset Command

The reset command can only be used once the Cryptographic Officer has been authenticated by the LRVG. Care must be taken when using this command as it will reset specific keys and other security critical parameters.

In Configuration Mode, the enable command functions as the reset command and accepts the “RESET” parameter in place of a Cryptographic Officer password. Note that the Shiva documentation incorrectly refers to the “RESET” parameter as a password.

Link

A communication path between two devices is called a link. A link defines which devices can communicate and how the data packets should be handled to secure the communication. A link definition is comprised of the following:

1. Source IP (LRVG or subnet);
2. Source application port;
3. Destination IP (LRVG or subnet);
4. Destination application port;
5. Communication protocol; and

Security Profile
A security profile defines how data flow should be handled. The data can be encrypted, clear, blocked, or one-way. In addition, a security profile specifies an Authentication Method and a Crypto Period.

1. Profile name
2. Algorithm (DES, 3DES, Triple DES, blocked, one-way, Clear). Note that the parameter “Clear” is for backward compatibility as BYPASS mode is now selected by using the “Filter” command.
3. Authentication method (authentication key “challenge phrase”)
4. Session key crypto period
5. Public key length (512, 1024, 2048)
6. Encryption Key length
7. Encapsulation method (SST\(^1\))

Encapsulation method
1. Encryption key length
2. Initialization Vector (IV) Length; 32 or 64 bits
3. Keep alive
4. Time out - maximum time a tunnel session can exist without receiving a “keep alive”

### Authentication Method

An authentic method defines how a Shiva VPN component validates the identity of the peer tunnel end-point.

The proprietary authentication method “Authentication Key” (using self signed certificates) is the only authentication method to be used within the FIPS 140-1 mode of operation.

The proprietary authentication method is referred to as the authentication key or “Challenge Phrase”. This proprietary method uses authentication-keys to authenticate a peer tunnel end-point.

\(^1\) Shiva Smart Tunneling is a proprietary method (using a challenge phrase for authentication).
**Authentication Key**

Authentication using the authentication key (auth-key) is very similar to authentication using certificates. The difference is that a certificate authority (CA) is not present to create and certify a certificate. Therefore the LRVG must create a certificate for itself. This type of certificate is essentially the same as a certificate generated if a CA existed except the digital signature is encrypted with an authentication key rather than with the CA private key. Therefore, the authentication key for a particular device must be input on both LRVG’s (or compatible devices) to establish a tunnel.

Note that the authentication key is also referred to as the “challenge phrase” in the source code and user documentation.

The self signed digital certificate (based on PKCS5 certificate standard) is a data structure that contains information positively identifying a service.

**Identification And Authentication (I&A)**

The LRVG enforces a role based identity and authentication policy. The user must enter the role to be assumed and the corresponding password. The “Enable Password” may be a minimum of 6 and a maximum of 60 alphanumeric characters. The Cryptographic Officer role is the only authorized role on the LRVG (the user role is implicit).

The Cryptographic Officer password (Enable Password) may be changed at any time by invoking the “password” command or reset to the default enable password “shiva” by resetting the LRVG.

**VPN Set Up**

The LRVG requires a Cryptographic Officer to configure the VPN by using the administrator interface. A VPN is established by configuring two tunnel devices as identical tunnel end-points. Once configured, the tunnel end-points will attempt to establish and complete a tunnel between them.

During the tunnel negotiation, the LRVG uses Diffi-Hellman to perform key negotiation to set up the encrypted tunnel. This key
negotiation also serves to authenticate the remote tunnel end-point by using the authentication key (challenge phrase) to sign packets.

A compatible remote tunnel end-point may be another LRVG, Shiva VPN Client or other Shiva VPN compatible product.

Access Modes

Authorized Cryptographic Officers have the following access rights to the LRVG configuration parameters and data items:

1. Read;
2. Write;
3. Update; and
4. Delete.

Access Control

The LRVG allows read/write access to the visible files by a properly authenticated Cryptographic Officer. System files (e.g. !nvram.!!!, !ace.!!!, !iv.!!!) have their file attributes set to read-only and hidden so that they are not visible to the Cryptographic Officer.

Object reuse

Object reuse is not implemented within the LRVG.

Zeroization Capability

The Cryptographic Officer can zeroize keys and critical security parameters by invoking LRVG commands manually to invalidate keys and delete files which contain keys, passwords, and other security critical parameters.

The zeroization procedure is required to be done prior to returning the unit to the manufacturer for repair or when shipping to another location (if the shipping method is unsecure).

The Cryptographic Officer must log into the LRVG and manually issue the following command sequence using the console, and power off the LRVG by entering the following command sequence (case sensitive):
1. “enable” <enter-your-new-password>;
2. “delete isbr.cfg”;
3. “delete previous.cfg”;
4. “delete !iv.!!!”;
5. “delete !ace.!!!”;
6. “delete license.txt”;
7. “enable RESET”

**Physical Security**

The LRVG has a removable cover, which is affixed to the base with screws and contains two tamper evident labels. Evidence of tampering by attempts to remove the cover will be visible by observing the label integrity.

The manufacturer applies the required tamper evident labels a minimum of 24 hours prior to shipment. This allows sufficient time for the label adhesive to cure for maximum tamper evidence properties.

The manufacturer affixes 2 tamper evident labels in the prescribed places as shown in Attachment 3 according to the label application procedures supplied by the manufacturer. This ensures that the label is applied correctly and the label integrity is not violated during application.

The tamper evident label has a number of security properties to guard against tampering, and re-application of tampered labels. The label contains the following security properties:

1. A consecutive number is printed to prevent counterfeit labels; and
2. Attempts to remove the label shall cause the label adhesive to “bubble” or fracture thereby leaving visible evidence of tampering, and prevent it from being reused and/or re-applied.

The Cryptographic Officer should visually inspect the cryptographic module periodically for evidence of tampering indicated by the “bubbling” of the label adhesive, and scratch markings around the labels and the perimeter of the cover. If the LRVG or label shows any tamper indications as described
above, the LRVG shall be shut down, and the organization
Security Officer contacted immediately.

**Cryptographic Officer Users**

Only one Cryptographic Officer user (operator) may initiate a console session at any one time. Concurrent Cryptographic Officer sessions and access to the control status interface other than via the console port is not allowed (i.e. Cryptographic Officer sessions via telnet is disabled).

**Passwords**

Passwords per user role are to be kept secret and shall not be shared with other user roles or unauthorized individuals.

Passwords shall be a minimum of 6 and a maximum of 60 alphanumeric characters. The only exception is the default enable password “shiva” which is hard coded by the manufacturer as an encrypted string.

The Cryptographic Officer shall change the default enable password to a suitable secret password following initial deployment, when the file !nvram.!!! is reset, and when the Cryptographic Officer manually resets the LRVG.

**LRVG Errors**

**Error Conditions**

The LRVG can enter one of four error states that can occur within the LRVG depending on the event. Depending on the severity of the error, the cryptographic module may be able to resolve the error automatically or require the Cryptographic Officer to manually resolve the error.

The LRVG requires the Cryptographic Officer to manually reconfigure or reset the LRVG following a fatal error (ERROR-1) except for a corrupt !nvram.!!! file. In this case, the LRVG automatically repairs the file; however, the Cryptographic Officer is still required to switch the power off and on to clear the “DisableInterface” flag to re-enable the data output interface, change the default enable password (it was reset automatically due to the corrupt !nvram.!!!), and reconfigure the keys and security critical parameters. Note that the LRVG will display the
following message if the !nvram.!!! file becomes corrupt: “**
Resetting Secure Storage ...”.

Note that an Encryption Engine Failure causes the LRVG to
transition to an ERROR-1 State. All existing tunnels are
terminated and new tunnels disallowed. Specifically the data
output interface will be disabled.

Tunnel/Bypass errors, ERROR-2, occur when a specific tunnel
or bypass (firewall) link encounters an error. In this case, only
the logical data output interface for that particular tunnel or
bypass link is disabled so that all other tunnels and bypass
remain operational. The Cryptographic Officer is required to
manually resolve these errors by issuing the reset command or
powering the cryptographic module off and on.

Security Relevant Minor errors, ERROR-3, occur when a
Cryptographic Officer command is entered incorrectly, minor
security relevant data transmission errors occur, or a session key
error occurred which the cryptographic module can correct
itself. These errors require the Cryptographic Officer to reenter a
can
ommand or are automatically corrected by the cryptographic
module depending on the event, which preceded this error state.
Error indications are issued via the status output interface for
this error state (some errors are displayed on the console while
others require the Cryptographic Officer to query the syslog).

Minor errors, ERROR-4, occur when non-security relevant
minor data transmission errors occur which the cryptographic
module can correct itself. No error message is issued for these
errors.

Error Resolutions

The Cryptographic Officer is required to investigate all errors as
they occur. and resolve them in a suitable way to mitigate and
prevent further compromise. This requires the Cryptographic
Officer to change the keys and security critical parameters
whenever the LRVG is suspected of compromise.

The Cryptographic Officer is required to manually resolve all
errors by performing one or more of the following resolutions to
recover the LRVG to a secure operational state.

1. Issue a reboot command (if the administration interface is
operational) or move the power switch to the “OFF” position
and then to the “ON” position;
2. Reconfigure the LRVG parameters (if appropriate);
3. Rebuild the FIPSFCS file by using the command “update-fips-fcs”;
4. Zeroize the LRVG, power off, power on, and reconfigure; or
5. Return the LRVG to the manufacturer (if the proceeding steps did not resolve the error).

Fatal errors, ERROR-1, are related to the cryptographic functions or LRVG integrity failing (affecting all tunnels and bypass links) and therefore all LRVG logical data output interfaces are totally disabled to prevent compromised data. The Cryptographic Officer is required to manually resolve these errors by either resetting the cryptographic module (by powering the cryptographic module off and on, reconfiguring the LRVG, or by issuing the reset command sequence) or by returning the cryptographic module to the manufacturer for repair.

LRVG Sessions

Console Session

The console session is active when the Cryptographic Officer logs into the LRVG console interface using the console port on the LRVG. The console serves as the control input interface and status output interface for LRVG administration.

SVM Session

The SVM (not part of this validation) provides a GUI control input interface and status output interface. To activate the SVM, the Cryptographic Officer must first use the console to configure the LRVG to use the SVM.

The SVM communication uses TFTP encapsulated in IP. These sessions are encrypted using DES CBC to protect the packets from unauthorized disclosure and modification.

Key Management

The Cryptographic Officer is the only user permitted to perform key management activities.

Outputting Keys (Electronic Key Distribution)
The does not provide a function to output keys electronically. Electronic key distribution is only performed during session key creation for tunnels using the Diffie-Hellman algorithm (discussed elsewhere in the document).

**Manual Key Entry**

The Cryptographic Officer is the only authorized user to access the LRVG and manually enter a suitable 8 character (56 bits) DES compliant key.

The Cryptographic Officer is required to enter keys twice and visually verify that each key value entered is correct.

**Manual IV Entry**

The IV will be manually entered during the LRVG initial configuration (and upon LRVG reset) when prompted following acceptance of the LRVG license agreement. The Cryptographic Officer shall enter a suitable 8 character (64 bits) IV for use with CBC DES.

Note that an NULL IV will be entered by pressing only the “enter” key and consequently an 8 byte null string will be entered as the IV.

**LRVG Self Tests**

Self tests are initiated by the cryptographic module automatically as part of the Power On Self Test (POST). These tests should be performed periodically according to the organization security policy. If an error is encountered, inform the organization Security Officer immediately.

The Cryptographic Officer can initiate the cryptographic module self tests on demand by turning the power to the LRVG off and then on again or by logging on to the control input interface and issuing the “reboot” command. Note that the reboot command invokes a warm boot which initiates a POST (the RAM does not lose power).

---

2 A properly formatted 56 bit DES key with odd parity becomes a 64 bit key as per FIPS PUB 46-2, December 1993.
Console Error Messages

This module describes the typical LRVG error messages issued to the status output interface.

The Cryptographic Officer is required to investigate all errors as they occur and resolve them in a suitable way to mitigate and prevent further compromise. This requires the Cryptographic Officer to change the keys and security critical parameters periodically and whenever the LRVG is suspected of possible compromise. Refer to the LRVG security policy in the previous section.

Error messages related to encryption, hashing (in support of cryptographic activities), random number generator, or bypass will disable the data output interfaces. Issue the command “show hardware” to verify the data output interface status.

Error Resolutions

The Cryptographic Officer is required to manually resolve all errors by performing one or more of the following resolutions to recover the LRVG to a secure operational state.

The table lists the major errors displayed on the status output interface. This section contains errors that are in addition to any syslog errors.

Some errors may be resolved by simply rebooting and others require the LRVG to be reconfigured. More serious errors may require the Cryptographic Officer to reset the LRVG to the same condition when it arrived from the manufacturer. The best approach is to first attempt the least disruptive error resolution step in case the LRVG experienced a minor glitch. If all of the suggested error resolution procedures (ERP) fail, then the LRVG must be returned to the manufacturer for repair to maintain the FIPS certification (refer to the LRVG security policy for zeroization procedures prior to shipping the LRVG).

The following error resolution procedures range from procedure #1 being least disruptive. These error resolution procedures are applicable to all LRVG errors regardless if it is listed in the table below or in the SYSLOG messages (in the following section).
1. **Issue** a reboot command (if the administration interface is operational) or move the power switch to the “OFF” position and then to the “ON” position;

2. Reconfigure the LRVG parameters (if appropriate);

3. Rebuild the FIPSFCS file by using the command “update-fips-fcs” (if appropriate);

4. Zeroize the LRVG, power off, power on, and reconfigure; or

5. Return the LRVG to the manufacturer (if the proceeding steps did not resolve the error).

The table below usually only recommends rebooting or resetting the LRVG for brevity. The Cryptographic Officer must take progressively stronger steps (as described above) to resolve the error condition if rebooting or resetting the LRVG fails to resolve the error.

### Partial Error List

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Possible Causes</th>
<th>Suggested Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>ShivICE boot loader file not found</td>
<td>diskkern.bin file does not exist on the flashdisk</td>
<td>Return LRVG to manufacturer for repair</td>
</tr>
<tr>
<td></td>
<td>Note: ShivICE is the name of the LRVG operating system</td>
<td></td>
</tr>
<tr>
<td>ShivICE boot loader file not found</td>
<td>diskkern.bin file does not exist on the flashdisk</td>
<td>Return LRVG to manufacturer for repair</td>
</tr>
<tr>
<td></td>
<td>Note: ShivICE is the name of the LRVG operating system</td>
<td></td>
</tr>
<tr>
<td>Verify ShivICE boot loader Failed</td>
<td>diskkern.bin CRC error</td>
<td>Return LRVG to manufacturer for repair</td>
</tr>
<tr>
<td>UNITTestIsOn = 1</td>
<td>Communication interface board failure or interface configuration (if.cfg) file not present</td>
<td>Reconfigure the L interfaces and rel this fails, return L manufacturer for repair</td>
</tr>
<tr>
<td>Failed to initialize</td>
<td>LRVG secure kernel</td>
<td>Reset the LRVG</td>
</tr>
<tr>
<td>Error Message</td>
<td>Possible Causes</td>
<td>Suggested Solution</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>security kernel</td>
<td>could not be initialized</td>
<td></td>
</tr>
<tr>
<td>Data output interfaces disabled</td>
<td>Transmit queue is disabled</td>
<td>See other error messages to determine what occurred and follow ERP</td>
</tr>
<tr>
<td>Unable to write all data to DiskCache</td>
<td>Insufficient space on flashdisk</td>
<td>Delete flashdisk if required. If this fails, reset the LRVG.</td>
</tr>
<tr>
<td>UNITTestIsOn = 1</td>
<td>GetIFConfig() encountered error looking for file if.cfg</td>
<td>Reconfigure or reset the LRVG. If it can not be resolved, it is most likely a hardware problem. Return the unit to the manufacturer.</td>
</tr>
<tr>
<td>Crypto Bypass for MD5. FIPS function Tests Failed</td>
<td>MD5 self test failed</td>
<td>Reset the LRVG.</td>
</tr>
<tr>
<td>Crypto Bypass for SHA-1 FIPS. function Tests Failed</td>
<td>SHA-1 self test failed</td>
<td>Reset the LRVG.</td>
</tr>
<tr>
<td>Crypto Bypass for RSA. FIPS function Tests Failed</td>
<td>RSA self test failed</td>
<td>Reset the LRVG.</td>
</tr>
<tr>
<td>Invalid Key Set</td>
<td>Loss of Key set (equivalent to secure storage tampered)</td>
<td>LRVG automatically recalculates the !nvram.!!! CRC. If next error message status output interface error resolution decision.</td>
</tr>
<tr>
<td>Secure Storage and Tamper failure</td>
<td>Invalid !nvram.!!! CRC or loss of Key set</td>
<td>The Cryptographic Officer must power off or reboot to resume operation</td>
</tr>
<tr>
<td>Secure Storage failure</td>
<td>Invalid !nvram.!!! CRC</td>
<td></td>
</tr>
<tr>
<td>Secure Storage is tampered</td>
<td>Invalid !nvram.!!! CRC</td>
<td></td>
</tr>
<tr>
<td>Resetting Secure Storage ... OK</td>
<td>Invalid !nvram.!!! CRC regenerated automatically.</td>
<td>The Cryptographic Officer must power off or reboot to resume operation</td>
</tr>
<tr>
<td>Resetting Secure Storage ... Failed</td>
<td>New !nvram.!!! CRC could not be generated</td>
<td>Reset the LRVG</td>
</tr>
<tr>
<td>Random number</td>
<td>The LRVG was unable to generate a random</td>
<td>Turn power off and on again. If problem persists...</td>
</tr>
</tbody>
</table>

LanRover VPN Gateway FIPS 6.59 Addendum
<table>
<thead>
<tr>
<th>Error Message</th>
<th>Possible Causes</th>
<th>Suggested Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>generation failed number</td>
<td></td>
<td>persist, then return LRVG to manuf.</td>
</tr>
<tr>
<td>hardware not found</td>
<td>hardware encryption card not installed or possibly damaged</td>
<td>Return to manuf.</td>
</tr>
<tr>
<td>hardware down</td>
<td>hardware encryption card malfunction</td>
<td>Return to manuf.</td>
</tr>
<tr>
<td>Crypto Bypass FIPS function Tests Failed</td>
<td>The encryption bypass test failed</td>
<td>Return to manuf.</td>
</tr>
<tr>
<td>Crypto FIPS function Tests Failed</td>
<td>The hardware DES encryption test failed</td>
<td>Return to manuf.</td>
</tr>
<tr>
<td>File not found for the FCS calculation</td>
<td>The file (isbr.exe or isbr.cfg) to compute random seed does not exist on flash disk</td>
<td>Reset the LRVG. to manufacturer if error message persists.</td>
</tr>
<tr>
<td>Not enough memory to calculate FCS</td>
<td>Insufficient system memory</td>
<td>Reboot the LRVG.</td>
</tr>
<tr>
<td>Not able to read file to calculate FCS</td>
<td>Not able to read the file (isbr.exe or isbr.cfg) to compute random seed</td>
<td>Reset the LRVG. to manufacturer if error message persists.</td>
</tr>
<tr>
<td>Cannot select local file system</td>
<td>Cannot read the flashdisk</td>
<td>Reboot the LRVG.</td>
</tr>
<tr>
<td>File not found for the FCS calculation</td>
<td>FIPSFCS file does not exist on the flash disk</td>
<td>Reset the LRVG.</td>
</tr>
<tr>
<td>Unable to write to the FCS file</td>
<td>Cannot write the newly computed CRCs to the FIPSFCS file</td>
<td>Reboot or Reset LRVG.</td>
</tr>
<tr>
<td>Unable to read to the FCS file</td>
<td>Cannot read the FIPSFCS file</td>
<td></td>
</tr>
<tr>
<td>Invalid FCS for the isbr.exe file</td>
<td>Invalid CRC for the file</td>
<td></td>
</tr>
<tr>
<td>Invalid FCS for the isbr.cfg file</td>
<td>Invalid CRC for the file</td>
<td></td>
</tr>
<tr>
<td>Invalid FCS for the !ace.!!! file</td>
<td>Invalid CRC for the file</td>
<td>Enter “update-fips-fcs” command to regenerate new CRCs on the flashdisk files</td>
</tr>
<tr>
<td>Error Message</td>
<td>Possible Causes</td>
<td>Suggested Solutions</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Invalid FCS for the dh.dat file</td>
<td>Invalid CRC for the file</td>
<td></td>
</tr>
<tr>
<td>Invalid FCS for the liv.!!! file</td>
<td>Invalid CRC for the file</td>
<td></td>
</tr>
<tr>
<td>Unable to read Authentication Keys</td>
<td>Cannot read authentication keys from isbr.cfg file on flashdisk</td>
<td>Reconfigure the LRVG</td>
</tr>
<tr>
<td>No serial interfaces found</td>
<td>Serial interface board not present or damaged</td>
<td>Return LRVG to manufacturer</td>
</tr>
<tr>
<td>Entry not found</td>
<td>Manager key not valid</td>
<td>Check manager key re-enter. Ask authorized Cryptographic Officer to add new manager key.</td>
</tr>
<tr>
<td>invalid password length valid length is from 6 to 60 bytes</td>
<td>Invalid password length</td>
<td>Re-enter password (if key, enter 8 character key length only)</td>
</tr>
<tr>
<td>Passwords don't match</td>
<td>The two passwords/keys entered do not match</td>
<td>Verify the passwords/keys and re-enter the command</td>
</tr>
<tr>
<td>can't be added, table is full</td>
<td>Maximum limit of manager key reached</td>
<td>Delete manager key entries to make space</td>
</tr>
<tr>
<td>invalid name length valid length is from 1 to 8 bytes</td>
<td>Invalid manager key length entered</td>
<td>Re-enter 8 character manager key</td>
</tr>
<tr>
<td>Error in command</td>
<td>Command entry error</td>
<td>Verify command and re-enter command</td>
</tr>
<tr>
<td>Incomplete Command</td>
<td>Command entry error</td>
<td></td>
</tr>
<tr>
<td>Run and Poker Testing with 20,000 bits...FAILED</td>
<td>LRVG random number generator self-test failed</td>
<td>Reset LRVG</td>
</tr>
<tr>
<td>one runs FAILED</td>
<td>LRVG random number generator self-test failed</td>
<td>Reset LRVG</td>
</tr>
<tr>
<td>MaxRun FAILED</td>
<td>LRVG random number generator self-test failed</td>
<td>Reset LRVG</td>
</tr>
<tr>
<td>key data must be in hex format</td>
<td>Incorrect entry</td>
<td>Re-enter key in hex format</td>
</tr>
<tr>
<td>key data does not match profile key length</td>
<td>Incorrect key entered</td>
<td>Verify key and re-</td>
</tr>
<tr>
<td>Error Message</td>
<td>Possible Causes</td>
<td>Suggested Solu</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>------------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Keys don't match</td>
<td>The duplicate key entries do not match</td>
<td>Re-enter command keys</td>
</tr>
<tr>
<td>esp-auth-key entry is only available for version 2 esp</td>
<td>esp-auth-key not applicable to IPSec version 2</td>
<td>Contact network administration or for more informat</td>
</tr>
<tr>
<td>auth-key length is from 6 to 60 characters</td>
<td>Invalid auth-key length entered</td>
<td>Re-enter 8 character auth-key</td>
</tr>
<tr>
<td>key data does not match required key length (16 bytes)</td>
<td>Invalid IPSec key length entered</td>
<td>Re-enter valid 16 esp-auth-key</td>
</tr>
<tr>
<td>key data does not match required key length (20 bytes)</td>
<td>Invalid IPSec key length entered</td>
<td>Re-enter valid 20 esp-auth-key</td>
</tr>
<tr>
<td>no authentication key entry is required</td>
<td>Invalid IPSec key</td>
<td>An esp-auth-key required</td>
</tr>
<tr>
<td>[System]: Error ** Unable to save Card 0 IRQ Handler **</td>
<td>Hardware encryption card failure</td>
<td>Return to manufacturer</td>
</tr>
<tr>
<td>[System]: Error ** Unable to set Card 0 IRQ Handler **</td>
<td>Hardware encryption card failure</td>
<td>Return to manufacturer</td>
</tr>
<tr>
<td>[System]: Error ** Unable to set Card 1 IRQ Handler **</td>
<td>Hardware encryption card failure</td>
<td>Return to manufacturer</td>
</tr>
</tbody>
</table>
Syslog Messages

These are typical syslog messages and their workarounds.

[cert] Syslog Messages

This module describes the status and syslog messages that appear under the [cert] heading in the System Log:

[cert]: 'noname' certificate not yet valid
[cert]: All certificates have been cleared
[cert]: CACERT packet decapsulation failed for certname
[cert]: Certificate from CAname failed signature verification
[cert]: Certificate issued by `CAname1 ', should be `CAname2', discarded
[cert]: certname certificate is revoked
[cert]: Expiring my certificate - certname
[cert]: Purging all certsize certificates
[cert]: Received CA's certsize certificate
[cert]: Received CERTREQREJECT packet for certname
[cert]: Received my certsize certificate
[cert]: Sent CA certificate request - certname
[cert]: Sent my certificate request - certname

[cert]: 'noname' certificate not yet valid

The device is unable to negotiate a tunnel because its own certificate is not yet valid according to the clock on the device.

Severity: Notice

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The start time and date defined for the certificate is later than the current time and date.</td>
<td>If a sooner start time and date desired, this certificate should I revoked and a new certificate c in the Certificate Authority.</td>
</tr>
</tbody>
</table>
The clock on the device is set incorrectly.

Check the time and date on the device using the Show clock menu option on the Manager. To change the clock on the device, use the Set Clock menu option on the Manager.

[cert]: All certificates have been cleared

All certificates have been cleared on the device. Note that the status of the certificates on the Certificate Authority are not affected.

Severity: Informational

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Certificate Authority name has been changed on the device.</td>
<td>Define new certificates for the device on the desired Certificate Authority.</td>
</tr>
</tbody>
</table>

[cert]: CACERT packet decapsulation failed for certname

The device has received its certificate with the name certname from the Certificate Authority but was unable to read it or determined it to be bad.

Severity: Notice

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The device could not read the certificate.</td>
<td>Ensure that the challenge phrase entered in the Challenge Phrase field of the Configure Device window in the Manager matches the challenge phrase entered for the certificate on the Certificate Authority.</td>
</tr>
</tbody>
</table>

[cert]: Certificate from CAname failed signature verification

The device was unable to verify the certificate it received from the Certificate Authority CAname because the time and date on the device was different enough from the time and date on the
Certificate Authority that the device was using the wrong public key to attempt to verify the certificate.

**Severity:** Notice

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The clock on the device is not synchronized with the clock on the Certificate Authority.</td>
<td>Check the time and date on the device using the Show Clock menu option on the Manager. Check the time and date on the Certificate Authority. Ensure that the two are the same. To change the clock on the device, use the Set Clock menu option on the manager. You may also need to clear the certificates on the device using Clear command.</td>
</tr>
</tbody>
</table>

**[cert]: Certificate issued by 'CAname1', should be 'CAname2', discarded**

Upon receiving its certificate, the device decapsulated the certificate and found that the Certificate Authority that issued the certificate (CAname1) does not match the Certificate Authority name entered in the device for the certificate (CAname2).

**Severity:** Notice

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The certificate was found to be bad after decapsulation because the Certificate Authority name did not match the expected Certificate Authority name.</td>
<td>Ensure that the Certificate Authority name entered in the Name field Configure Device dialog of the Manager matches the Certificate Authority Name entered on the Certificate Authority.</td>
</tr>
</tbody>
</table>

**[cert]: certname certificate is revoked**

The device was unable to negotiate a tunnel with the opposing device because the opposing device's certificate certname has been revoked.

**Severity:** Notice
The opposing device's certificate has been revoked.

If the opposing device's certificate was revoked so that it no longer communicates with any of the other devices in the network, delete the tunnel using the Delete Tunnel button on the Tunnels Tab of the Manager. If the opposing device's certificate was revoked by mistake, create a new certificate for the opposing device in the Certificate Authority.

[cert]: Expiring my certificate - certname

The device has determined its certificate certname to have expired by comparing the expiry date with the clock on the device.

Severity: Informational

The certificate has expired, either normally or because the clock on the device has been changed.

Check the clock on the device. If it is correct and you want the device to have a certificate, issue a new certificate on the Certificate Authority.

[cert]: Purging all certsize certificates

All certificates of size certsize on the device were cleared because Delete was selected in the Configure Device dialog of the Manager. The cleared certificates can be any or all of the Certificate Authority's certsize certificate, the device's current certsize certificate, and the device's next certsize certificate.

Severity: Informational

[cert]: Received CA's certsize certificate

The device has received the Certificate Authority's own certificate of size certsize, where certsize is one of 512, 1024, or 2048 bytes.

Severity: Informational
[cert]: Received CERTREQREJECT packet for certname

The Certificate Authority rejected the device's request for the certificate with name certname.

Severity: Debug

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>No such certificate is defined on the Certificate Authority.</td>
<td>Ensure that this certificate was on the Certificate Authority.</td>
</tr>
<tr>
<td></td>
<td>Ensure that the certificate name was entered correctly in the Certificate Name field of the Configure Device window in the Manager.</td>
</tr>
<tr>
<td></td>
<td>Ensure that the correct certificate size was selected for the certificate in the Key Length field of the Configure Device window in the Manager.</td>
</tr>
</tbody>
</table>

[cert]: Received my certsize certificate

The device has received the certificate of size certsize, where certsize is one of 512, 1024, or 2048 bytes.

Severity: Informational

[cert]: Sent CA certificate request - certname

The device has sent a request to the Certificate Authority for a copy of the Certificate Authority's certificate of the same size as certificate certname. The device needs the Certificate Authority's certificate in order to negotiate with the Certificate Authority for the device's own certificate with the name certname.

Severity: Debug

[cert]: Sent my certificate request - certname

The device is requesting a certificate with the name certname from the Certificate Authority. If this message appears repeatedly and the message Received my certsize certificate
does not appear, the device is making repeated requests for the certificate but the certificate is not being fulfilled.

**Severity:** Debug

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The device is unable to communicate with the Certificate Authority.</td>
<td>Ensure that the packets from the device are reaching the Certificate Authority and vice versa.</td>
</tr>
<tr>
<td>The Certificate Authority is rejecting the request.</td>
<td>Ensure that the certificate has not been revoked or already fulfilled, in which case the certificate will have to be reissued on the Certificate Authority. Ensure that the certificate size selected in the Key Length field of the Configure Device window matches the size defined for the certificate in the Configure Device window.</td>
</tr>
</tbody>
</table>

[debug] Syslog Messages

**VERSION:** VPN660-1298

This module describes the status and syslog messages that appear under the [debug] heading in the System Log:

[debug] Connecting to ip
[debug]: Connection request from [ ip ]
[debug]: Negotiating with ip
[debug]: Received key agreement reply from ip
[debug]: Received negotiation reply from ip
[debug]: Requesting key agreement with ip

**[debug] Connecting to ip**

The device is attempting to establish a tunnel with another VPN Gateway device of IP address ip. If this message appears repeatedly and the message [tunnel]: Secure tunnel established with name [ip] does not appear, the device is making repeated
attempts to connect to the opposing device, but is unable to establish a tunnel.

**Severity:** Debug

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The device is unable to communicate with the opposing device.</td>
<td>Ensure that the packets from the device are reaching the opposing device and vice versa.</td>
</tr>
<tr>
<td>The link may be defined incorrectly.</td>
<td>Look at the other messages appearing on the Syslog for more information as to what is wrong with this link.</td>
</tr>
</tbody>
</table>

**[debug]: Connection request from [ ip ]**

The opposing device of IP address ip has requested to establish a tunnel with the device. If this message appears repeatedly and the message [tunnel]: Secure tunnel established with name [ip] does not appear, the opposing device is making repeated attempts to connect to the device, but is unable to establish a tunnel.

**Severity:** Debug

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The device is unable to communicate with the opposing device.</td>
<td>Ensure that the packets from the device are reaching the opposing device.</td>
</tr>
<tr>
<td>The link may be defined incorrectly.</td>
<td>Look at the other messages appearing on the Syslog as well as on the opposing device for more information as to what is wrong with this link.</td>
</tr>
</tbody>
</table>

**[debug]: Negotiating with ip**

The device is attempting to authenticate the opposing device of IP address ip.

**Severity:** Debug

**[debug]: Received key agreement reply from ip**
The device has successfully performed the Session Key Exchange with the opposing device of IP address ip.

Severity: Debug

[debug]: Received negotiation reply from ip

The device has successfully authenticated the opposing device of IP address ip.

Severity: Debug

[debug]: Requesting key agreement with ip

The device is attempting to perform the Session Key Exchange with the opposing device of IP address ip.

Severity: Debug

[in-proxy] Syslog Messages

This module describes the status and syslog messages that appear under the [in-proxy] heading in the System Log:

[in-proxy]: tcp from sourceip - sourceport to destip - destport established

[in-proxy]: tcp from sourceip - sourceport to destip - destport terminated with numbytes bytes

[in-proxy]: tcp from sourceip - sourceport to destip - destport timeout with numbytes bytes

[in-proxy]: udp from sourceip - sourceport to destip - destport established

[in-proxy]: tcp from sourceip - sourceport to destip - destport established

A TCP connection has been established through an in-proxy firewall rule (that is, an inbound, stateful connection with NAT) from source IP address sourceip and source port sourceport to destination IP address destip and destination port destport.

Severity: Informational
[in-proxy]: tcp from sourceip - sourceport to destip - destport terminated with numbytes bytes

A TCP connection through an in-proxy firewall rule (that is, an inbound, stateful connection with NAT) from source IP address sourceip and source port sourceport to destination IP address destip and destination port destport has been terminated normally with numbytes bytes transferred.

Severity: Informational

[in-proxy]: tcp from sourceip - sourceport to destip - destport timeout with numbytes bytes

A TCP connection from source IP address sourceip and source port sourceport to destination IP address destip and destination port destport through an in-proxy firewall rule (that is, an inbound, stateful connection with NAT) has been terminated due to a timeout condition.

Severity: Informational

### Possible Causes

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The amount of idle time elapsed (that is, with no packets transferred) has exceeded the maximum allowable set in the Enable Proxy Timeout (minutes) field of the Configure Device window in the Manager.</td>
<td>Increase the maximum proxy timeout interval in the Enable Proxy Timeout (minutes) field of the Configure Device window in the Manager, or ensure that the amount of idle time does not exceed the maximum by maintaining frequent communication between the two devices.</td>
</tr>
<tr>
<td>All of the available proxy sessions (maximum 1024) are in use and another session has been requested by some device. In this situation, the device that has the most idle time elapsed (that is, with no packets transferred) will have its session terminated. However, a session will terminate only if the idle time elapsed exceeds the minimum set in the Enable Proxy Timeout (minutes) field.</td>
<td>To increase the amount of idle time available to any session before allowing it to be terminated, increase the minimum idle time set in the Enable Proxy Timeout (minutes) field of the Configure Device window in the Manager.</td>
</tr>
</tbody>
</table>
[in-proxy]: udp from sourceip - sourceport to destip - destport established

A UDP connection has been established through an in-proxy firewall rule (that is, an inbound, stateful connection with NAT) from source IP address sourceip and source port sourceport to destination IP address destip and destination port destport.

Severity: Informational

[keys] Syslog Messages

This module describes the status and syslog messages that appear under the [keys] heading in the System Log:

[keys]: Generated size-bit queued DHValue

[keys]: Generated size-bit queued DHValue

The Enterprise has done the mathematical operations required to create the DHValue of size bits for the Diffie-Hellman Session Key Exchange.

Severity: Debug

[oneway-in] Syslog Messages

This module describes the status and syslog messages that appear under the [oneway-in] heading in the System Log:

[oneway-in]: tcp from sourceip - sourceport to destip - destport established

[oneway-in]: tcp from sourceip - sourceport to destip - destport terminated with numbytes bytes

[oneway-in]: tcp from sourceip - sourceport to destip - destport timeout with numbytes bytes

[oneway-in]: udp from sourceip - sourceport to destip - destport established
[oneway-in]: tcp from sourceip - sourceport to destip - destport established

A TCP connection has been established through a oneway-in firewall rule (that is, an inbound, stateful connection without NAT) from source IP address sourceip and source port sourceport to destination IP address destip and destination port destport.

**Severity:** Informational

[oneway-in]: tcp from sourceip - sourceport to destip - destport terminated with numbytes bytes

A TCP connection through a oneway-in firewall rule (that is, an inbound, stateful connection without NAT) from source IP address sourceip and source port sourceport to destination IP address destip and destination port destport has been terminated normally with numbytes bytes transferred.

**Severity:** Informational

[oneway-in]: tcp from sourceip - sourceport to destip - destport timeout with numbytes bytes

A TCP connection from source IP address sourceip and source port sourceport to destination IP address destip and destination port destport through a oneway-in firewall rule (that is, an inbound, stateful connection without NAT) has been terminated due to a timeout condition.

**Severity:** Informational

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The amount of idle time elapsed (that is, with no packets transferred) has exceeded the maximum allowable set in the Enable Proxy Timeout (minutes) field of the Configure Device window in the Manager.</td>
<td>Increase the maximum proxy timeout interval in the Enable Proxy Timeout (minutes) field of the Configure Device window in the Manager, or ensure that the amount of idle time does not exceed the maximum by maintaining frequent communication between two devices.</td>
</tr>
</tbody>
</table>
All of the available proxy sessions (maximum 1024) are in use and another session has been requested by some device. In this situation, the device that has the most idle time elapsed (that is, with no packets transferred) will have its session terminated. However, a session will terminate only if the idle time elapsed exceeds the minimum set in the Enable Proxy Timeout (minutes) field of the Configure Device window in the Manager.

To increase the amount of idle available to any session before allowing it to be terminated, increase the minimum idle time set in the Enable Proxy Timeout (minutes) field of the Configure Device window in the Manager.

[oeway-in]: udp from sourceip - sourceport to destip - destport established

A UDP connection has been established through a oneway-in firewall rule (that is, an inbound, stateful connection without NAT) from source IP address sourceip and source port sourceport to destination IP address destip and destination port destport.

Severity: Informational

[oeway-out] Syslog Messages

This module describes the status and syslog messages that appear under the [oneway-out] heading in the System Log:

[oeway-out]: icmp echo from sourceip -0 to destip -0 established

[oeway-out]: icmp echo-reply from sourceip -0 to destip -0 terminated with 0 bytes transferred

[oeway-out]: tcp from sourceip - sourceport to destip - destport established

[oeway-out]: tcp from sourceip - sourceport to destip - destport terminated with numbytes bytes

[oeway-out]: tcp from sourceip - sourceport to destip - destport timeout with numbytes bytes

[oeway-out]: udp from sourceip - sourceport to destip - destport established
[oneway-out]: icmp echo from sourceip -0 to destip -0 established

A ping packet was successfully sent from IP address sourceip on port 0 (designated port for ping packets) to destination IP address destip on port 0 through a oneway-out firewall rule (that is, an outbound, stateful connection without NAT).

Severity: Informational

[oneway-out]: icmp echo-reply from sourceip -0 to destip -0 terminated with 0 bytes transferred

A response to a ping packet was sent from source IP address sourceip on port 0 (designated port for ping packets) to destination IP address destip on port 0 through a oneway-out firewall rule (that is, an outbound, stateful connection without NAT).

Severity: Informational

[oneway-out]: tcp from sourceip -sourceport to destip -destport established

A TCP connection has been established through a oneway-out firewall rule (that is, an outbound, stateful connection without NAT) from source IP address sourceip and source port sourceport to destination IP address destip and destination port destport.

Severity: Informational

[oneway-out]: tcp from sourceip -sourceport to destip -destport terminated with numbytes bytes

A TCP connection through a oneway-out firewall rule (that is, an outbound, stateful connection without NAT) from source IP address sourceip and source port sourceport to destination IP address destip and destination port destport has been terminated normally with numbytes bytes transferred.

Severity: Informational
A TCP connection from source IP address sourceip and source port sourceport to destination IP address destip and destination port destport through a oneway-out firewall rule (that is, an outbound, stateful connection without NAT) has been terminated due to a timeout condition.

**Severity:** Informational

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The amount of idle time elapsed (that is, with no packets transferred) has exceeded the maximum allowable set in the Enable Proxy Timeout (minutes) field of the Configure Device window in the Manager.</td>
<td>Increase the maximum proxy timeout interval in the Enable Proxy Timeout (minutes) field of the Configure Device window in the Manager, or ensure that the amount of idle time does not exceed the maximum by maintaining frequent communication between two devices.</td>
</tr>
<tr>
<td>All of the available proxy sessions (maximum 1024) are in use and another session has been requested by some device. In this situation, the device that has the most idle time elapsed (that is, with no packets transferred) will have its session terminated. However, a session will terminate only if the idle time elapsed exceeds the minimum set in the Enable Proxy Timeout (minutes) field of the Configure Device window in the Manager.</td>
<td>To increase the amount of idle time available to any session before allowing it to be terminated, increase the minimum idle time set in the Enable Proxy Timeout (minutes) field of the Configure Device window in the Manager.</td>
</tr>
</tbody>
</table>

A UDP connection has been established through a oneway-out firewall rule (that is, an outbound, stateful connection without NAT) from source IP address sourceip and source port sourceport to destination IP address destip and destination port destport.
Severity: Informational

[out-proxy] Syslog Messages

This module describes the status and syslog messages that appear under the [out-proxy] heading in the System Log:

[out-proxy]: icmp echo from sourceip -0 to destip -0 established
[out-proxy]: icmp echo-reply from sourceip -0 to destip -0 terminated with 0 bytes transferred
[out-proxy]: tcp from sourceip - sourceport to destip - destport established
[out-proxy]: tcp from sourceip - sourceport to destip - destport terminated with numbytes bytes
[out-proxy]: tcp from sourceip - sourceport to destip - destport timeout with numbytes bytes
[out-proxy]: udp from sourceip - sourceport to destip - destport established

[out-proxy]: icmp echo from sourceip -0 to destip -0 established

A ping packet was successfully sent from IP address sourceip on port 0 (designated port for ping packets) to destination IP address destip on port 0 through an out-proxy firewall rule (that is, an outbound, stateful connection with NAT).

Severity: Informational

[out-proxy]: icmp echo-reply from sourceip -0 to destip -0 terminated with 0 bytes transferred

A response to a ping packet was sent from source IP address sourceip on port 0 (designated port for ping packets) to destination IP address destip on port 0 through an out-proxy firewall rule (that is, an outbound, stateful connection with NAT).

Severity: Informational
[out-proxy]: tcp from sourceip - sourceport to destip - destport established

A TCP connection has been established through an out-proxy firewall (that is, an outbound, stateful connection with NAT) from source IP address sourceip and source port sourceport to destination IP address destip and destination port destport.

Severity: Informational

[out-proxy]: tcp from sourceip - sourceport to destip - destport terminated with numbytes bytes

A TCP connection through an out-proxy firewall rule (that is, an outbound, stateful connection with NAT) from source IP address sourceip and source port sourceport to destination IP address destip and destination port destport has been terminated normally with numbytes bytes transferred.

Severity: Informational

[out-proxy]: tcp from sourceip - sourceport to destip - destport timeout with numbytes bytes

A TCP connection from source IP address sourceip and source port sourceport to destination IP address destip and destination port destport through an out-proxy firewall rule (that is, an outbound, stateful connection with NAT) has been terminated due to a timeout condition.

Severity: Informational

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The amount of idle time elapsed (that is, with no packets transferred) has exceeded the maximum allowable set in the Enable Proxy Timeout (minutes) field of the Configure Device window in the Manager.</td>
<td>Increase the maximum proxy timeout interval in the Enable Proxy Timeout (minutes) field of the Configure Device window in the Manager, or ensure that the amount of idle time does not exceed the maximum by maintaining frequent communication between the two devices.</td>
</tr>
<tr>
<td>All of the available proxy sessions</td>
<td>To increase the amount of idle time elapsed by maintaining frequent communication between the devices.</td>
</tr>
</tbody>
</table>
(maximum 1024) are in use and another session has been requested by some device. In this situation, the device that has the most idle time elapsed (that is, with no packets transferred) will have its session terminated. However, a session will terminate only if the idle time elapsed exceeds the minimum set in the Enable Proxy Timeout (minutes) field of the Configure Device window in the Manager.

Available to any session before allowing it to be terminated, increase the minimum idle time set in the Enable Proxy Timeout (minutes) field of the Configure Device window in the Manager.

[out-proxy]: udp from sourceip - sourceport to destip - destport established

A UDP connection has been established through an out-proxy firewall rule (that is, an outbound, stateful connection with NAT) from source IP address sourceip and source port sourceport to destination IP address destip and destination port destport.

Severity: Informational

[system] Syslog Messages

This module describes the status and syslog messages that appear under the [system] heading in the System Log:

[system]: Attempt to erase DISKKERN.BIN file called from ph-ide.c line 1188

[system]: fclose() called from program .c line linenum

[system]: fgets() failed. program .c line linenum

[system]: fgets() ok. program .c line linenum

[system]: fopen() ok. program .c line linenum

[system]: fwrite() ok. program .c line linenum

[system]: request for unserviced tcp: destip - destport from sourceip - sourceport denied

[system]: tcp from sourceip - sourceport to destip - destport no rule matched

[system]: udp from sourceip - sourceport to destip - destport no rule matched
[system]: Attempt to erase DISKKERN.BIN file called from ph-ide.c line 1188

An attempt was made by C program ph-ide at line number 1188 of the program to erase the operating system file DISKKERN.BIN from the flash ROM. This message is a warning rather than an error only because the device has not allowed the file to be deleted. Without this file the device could not function.

Severity: Warning

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The user instructed the device to delete the file DISKKERN.BIN.</td>
<td>Do not attempt to delete this file. Attempt will be unsuccessful as device cannot function without</td>
</tr>
<tr>
<td>The software on the device attempted to delete the file DISKKERN.BIN.</td>
<td>If this seems to be the only explanation for the appearance of the message, note the circumstances under which this message appeared and contact your Shiva support representative.</td>
</tr>
</tbody>
</table>

[system]: ffclose() called from program .c line linenum

The C program program .c closed a file on the flash ROM from line linenum of program .c. This is not an error.

Severity: Debug

[system]: ffgets() failed. program .c line linenum

The C program program .c was unable to read data from a file on the flash ROM from line linenum of program .c. This message is not necessarily an error in that this situation occurs whenever the end of the file on the flash ROM is reached because there is no more data in the file to get. In this case the failed message will occur after a series of [system]: ffgets() ok. program.c line linenum messages.

Severity: Debug
[system]: ffgets() ok. program .c line linenum

The C program program .c successfully read part of a file on the flash ROM from line linenum of program .c. This is not an error.

Severity: Debug

[system]: ffopen() ok. program .c line linenum

The C program program .c successfully opened a file on the flash ROM from line linenum of program .c. This is not an error.

Severity: Debug

[system]: fwrite() ok. program .c line linenum

The C program program .c successfully wrote (saved) a file on the flash ROM from line linenum of program .c. This is not an error.

Severity: Debug

[system]: request for unserviced tcp: destip - destport from sourceip - sourceport denied

The device blocked a TCP packet from source IP address sourceip and source port sourceport going to destination IP address destip and destination port destport because the device has a firewall rule defined to block the packet from crossing from either the black to the red or the red to the black side of the device (that is, "denied" was selected from the Action menu of the Configure Device window on the Manager). Note that this message is only a warning (and not an error) because you may actually want to be blocking the packet with the firewall rules set up on the device.

Severity: Warning

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is a firewall rule defined to block the packet.</td>
<td>To allow this traffic through the either remove the blocking firev</td>
</tr>
</tbody>
</table>
or, if possible, define a more specific firewall rule to allow this traffic using the Firewall Tab of the Configure Device window of the Manager.

**[system]: tcp from sourceip - sourceport to destip - destport no rule matched**

The device blocked a TCP packet from source IP address sourceip and source port sourceport going to destination IP address destip and destination port destport because the device has no firewall rule defined to allow the packet either from the red to the black or from the black to the red side of the device. Note that this message is only a warning (not an error) because you may actually want to be blocking the packet with the firewall rules set up on the device.

**Severity:** Warning

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the packet did not come out of a tunnel, then there is no firewall rule defined to allow the packet through.</td>
<td>To allow this traffic through the device, define the appropriate firewall rule in the Firewall Tab of the Configure Device window of the Manager. Consider installing the Client on the opposing device to allow you to set up a tunnel from the opposing device directly to the red side of the device.</td>
</tr>
<tr>
<td>If the packet did come out of a tunnel, then the destination IP address is found on the other side of the firewall and there is no rule to allow the packet through.</td>
<td>Remember that tunnels terminate either the red or the black side of the device. If the tunnel terminates on the black and the destination IP is on the red, then you must define an appropriate firewall rule to let the packet through (use the Firewall Tab). If the tunnel terminates on the red and the destination is on the black, then define a firewall rule or change the color of the tunnel to black.</td>
</tr>
<tr>
<td>If the packet was expected to come out of a tunnel but arrived in the clear, the tunnel may not have been set up</td>
<td>Check the tunnel configuration on the opposing device (usually a VPN Gateway device).</td>
</tr>
</tbody>
</table>
The device blocked a UDP packet from source IP address sourceip and source port sourceport going to destination IP address destip and destination port destport because the VPN Gateway has no firewall rule defined to allow the packet either from the red to the black or from the black to the red side of the device. Note that this message is only a warning because you may actually want to be blocking the packet with the firewall rules set up on the device.

**Severity:** Warning

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the packet did not come out of a tunnel, then there is no firewall rule defined to allow the packet through.</td>
<td>To allow this traffic through the define the appropriate firewall rule on the Firewall Tab of the Configure Device window of the Manager. Consider installing the Client on the opposing device to allow you to set up a tunnel from the opposing device directly to the red side of the device.</td>
</tr>
<tr>
<td>If the packet did come out of a tunnel, then the destination IP address is found on the other side of the firewall and there is no rule to allow the packet through.</td>
<td>Remember that tunnels terminate on either the red or the black side device. If the tunnel terminates on the black and the destination IP is on the red, then you must define an appropriate firewall rule to let the packet through (use the Firewall Tab) or you must change the termination color of the tunnel to red (use the Tunnel Tab). If the tunnel terminates on the red and the destination is on the black, then define a firewall rule and change the color of the tunnel.</td>
</tr>
<tr>
<td>If the packet was expected to come out of a tunnel but arrived in the clear, the tunnel may not have been set up properly (or at all) on the opposing device.</td>
<td>Check the tunnel configuration on the opposing device (usually a VPN Gateway device).</td>
</tr>
</tbody>
</table>
[tunnel] Syslog Messages

This module describes the status and syslog messages that appear under the [tunnel] heading in the System Log:

[tunnel]: Authentication key invalid name [ip]
[tunnel]: Connection to name [ip] timed out
[tunnel]: Local Public key invalid or not ready name [ip]
[tunnel]: Public key has expired name [ip]
[tunnel]: Req ignored, link does not exist [ip]
[tunnel]: Req ignored, public profile mismatch IP: ip
[tunnel]: Req ignored, session profile mismatch IP: ip
[tunnel]: Secure tunnel established with name [ip]
[tunnel]: Session failure, cert does not exist name [ip]
[tunnel]: Session failure, invalid certificate certname [ip]

[tunnel]: Authentication key invalid name [ip]

The device was unable to negotiate a tunnel with opposing device name and IP address ip because the challenge phrase entered on the device does not match the challenge phrase entered on the opposing device.

Severity: Warning

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The challenge phrase entered on the device does not match the challenge phrase entered on the opposing device.</td>
<td>Ensure that the challenge phrase entered in the Key field of the Configure Device window of the Manager matches the challenge phrase entered on the opposing device.</td>
</tr>
</tbody>
</table>
[tunnel]: Connection to name [ip] timed out

The secure tunnel with the opposing device of name name and IP address ip has been terminated because the VPN Gateway has been configured to reconnect if no keepalive packet is received within a specified interval and the interval has elapsed without any keepalive packet being received.

Severity: Informational

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>No keepalive packet was received from the opposing device within the specified interval.</td>
<td>Ensure that connectivity with the opposing device has not been lost. Ensure that the opposing device is configured to send keepalive packets. Ensure that the timeout interval selected for the device in the Enable Timeout field of the Configure Device window is equal to or greater than the frequency with which the opposing device sends out its keepalive packets.</td>
</tr>
</tbody>
</table>

[tunnel]: Local Public key invalid or not ready name [ip]

The VPN Gateway was unable to negotiate a tunnel with an opposing device name and IP address ip because the VPN Gateway's public key does not exist.

Severity: Warning

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the authentication method being used is Challenge Phrase, no challenge phrase has been entered for the VPN Gateway.</td>
<td>Enter a challenge phrase in the Key field of the Configure Device window of the Manager.</td>
</tr>
<tr>
<td>If the authentication method being used is certificates, the VPN Gateway has no certificate of the size selected for the tunnel.</td>
<td>Create a certificate for the VPN Gateway on the Certificate Authority using the Certificate Name and Key Length fields of the Configure Device window of the Manager.</td>
</tr>
</tbody>
</table>
[tunnel]: Public key has expired name [ip]

The VPN Gateway is unable to negotiate a tunnel with the device of peername name and IP address ip because the public keys being presented by the opposing device are either not yet valid or have already expired according to the clock on the VPN Gateway. Note that this message refers to the public keys used to negotiate a link when authentication is being done using challenge phrase.

Severity: Warning

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The clock on the VPN Gateway is not synchronized with the clock on the opposing device. The times on the two clocks are set far enough apart that what appears to be a valid set of public keys on the opposing device does not appear to be valid on the VPN Gateway.</td>
<td>Check the time and date on the Gateway using the Show Clock option on the Manager. Check and date on the opposing device. Ensure that the two are the same. To change the clock on the VPN Gateway, use the Set Clock command on the Manager.</td>
</tr>
</tbody>
</table>
[tunnel]: Req ignored, public profile mismatch IP: ip

The VPN Gateway was unable to establish a secure tunnel with the opposing device of IP address ip due to a public profile mismatch.

Severity: Warning

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>One or more of the parameters of the link definition on the VPN Gateway does not match the associated parameters as defined on the opposing device.</td>
<td>Ensure that the authentication selected in the Method field and public key length selected in the Key Length field of the Link Entry window match those on the opposing device.</td>
</tr>
</tbody>
</table>

[tunnel]: Req ignored, session profile mismatch IP: ip

The VPN Gateway was unable to establish a secure tunnel with the opposing device of IP address ip due to a session profile mismatch.

Severity: Warning

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>One or more of the parameters of the link definition on the VPN Gateway does not match the associated parameters as defined on the opposing device.</td>
<td>Ensure that the crypto period entered in the Session Key Crypto Period Length field, the algorithm selected from the Algorithm field, and the encapsulation method selected in the Encapsulation field of the Configure Device window of the Manager match those on the opposing device.</td>
</tr>
</tbody>
</table>

[tunnel]: Secure tunnel established with name [ ip ]

The VPN Gateway has successfully negotiated a secure tunnel with the opposing device of peername name and IP address ip.

Severity: Informational
[tunnel]: Session failure, cert does not exist name [ip]

An active tunnel between the VPN Gateway and the opposing device of name name and IP address ip has been closed because the certificate used to establish the tunnel no longer exists. Note that this message will appear only once as the tunnel closes.

Severity: Warning

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The certificate has expired either normally or because the clock on the VPN Gateway has been changed.</td>
<td>Check the clock on the VPN Gateway. If it is correct and you want the Gateway to have a certificate, issue a new certificate on the Certificate Authority.</td>
</tr>
</tbody>
</table>

[tunnel]: Session failure, invalid certificate certname [ip]

The VPN Gateway was unable to negotiate a tunnel with the device with IP address ip because the device's certificate certname has been determined by the VPN Gateway to be invalid.

Severity: Warning

<table>
<thead>
<tr>
<th>Possible Causes</th>
<th>Suggested Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The clock on the VPN Gateway is not synchronized with the clock on the opposing device.</td>
<td>Check the time and date on the Gateway using the Show Clock option on the Manager. Check and date on the opposing device. Ensure that the two are the same. To change the clock on the VPN Gateway, use the Set Clock command on the Manager.</td>
</tr>
<tr>
<td>The opposing device's certificate has been revoked.</td>
<td>If the opposing device's certificate was revoked so that it can no longe communicate with any of the other devices in the network, delete the tunnel using the Delete Tunnel on the Tunnels Tab of the Manager. If the opposing device's certificate was revoked so that it can no longe communicate with any of the other devices in the network, delete the tunnel using the Delete Tunnel on the Tunnels Tab of the Manager.</td>
</tr>
<tr>
<td>The opposing device’s host name is different from the one contained in the certificate.</td>
<td>The host name was probably entered into the Certificate Authority incorrectly when the certificate was defined. Revoke and reissue the certificate in the Certificate Authority.</td>
</tr>
</tbody>
</table>
Troubleshooting Tips

Use the following tips to ensure a smoother implementation and maintenance of your VPN environment.

The following list summarizes the tips in this document:

- Error! Unknown switch argument.
- Error! Unknown switch argument.
- Error! Unknown switch argument.
- Error! Unknown switch argument.
- Error! Unknown switch argument.
- Error! Unknown switch argument.
- Error! Unknown switch argument.
- Error! Unknown switch argument.
- Error! Unknown switch argument.
- Error! Unknown switch argument.

**Remember your Passwords**

Record the default passwords that are preset with your hardware and software, as well as the new passwords you assign. There are default passwords included with your:

- LanRover VPN Gateway
- Shiva VPN Manager software
- Shiva Certificate Authority (Server and Client)
- Shiva VPN Client

**Use the Site Planning Guide to Help with Initial Setup**

The initial setup of the LanRover VPN Gateway requires knowledge of the IP addresses used for the Ethernet interfaces, the default gateway IP address, passwords for the device and VPN Manager, in addition to date and time information. Use the Site Planning Guide included with your LanRover VPN Gateway to help you gather the information before you perform the initial setup.
Enabling the Ethernet Interfaces

Once you complete the initial setup and assign IP addresses to the Ethernet interfaces, the interfaces are, by default, shut down. Though they appear to be configured correctly, you need to expressly enable them.

Use the `shutdown delete` command to enable the interfaces. To check the status of the interfaces, use the `show interface` command.

Ensure the System Time is Consistent

The system time on the workstation running the VPN Manager must be set within 10 minutes of the other LanRover VPN Gateway devices on the network. If the variance is more than 10 minutes, timing and security issues can occur.

This holds true for the VPN Client, the Certificate Authority Server, and the Certificate Authority Client.

Configuring a Remote Link to a LanRover VPN Gateway

Since Internet Service Providers (ISPs) often assign IP addresses from an address pool, make sure you choose User Name rather than IP address from the configuration dialog box.

Because a user most likely disconnects from the network for periods of time, the LanRover VPN Gateway does not attempt to connect with a remote link without the remote user initiating the connection.

Configuring a Remote Link to a Client

Ensure that the properties of the VPN Secure profile matches that of the Client's. Alternatively, enable the Accept Peer Proposal option in the Client.

Using the Command Shell

There is a root level and three levels of commands.

Entering a root command takes you to the next level of commands.

Typing the `exit` command moves you up one level of commands.
Typing the `end` command always places you in the root level.

**Proxies and Links**

If you have an existing firewall, the firewall should have a pre-defined proxy to allow encrypted packets to pass through the firewall to the LanRover VPN Gateway.

With inbound proxies, incoming packets know the address of the gateway, but not the specific destination address. With inbound links, incoming packets know the specific destination address.

Likewise, outbound proxies have a gateway address the destination knows as the source address. Outbound links have the specific address the destination knows as the source address.