Infinera GX-G42 Optical Network Platform Release 6.2.10

Hardening Guide

Revision V002

January 2025

Infinera continually strives to reduce the adverse environmental effects of its products and services. We invite you to join us in working towards a cleaner, safer environment. Please recycle product packaging and follow the recommendations for power use and proper disposal of our products.

Infinera Corporation. Visit us at www.infinera.com.

Infinera makes no warranties or representations, expressed or implied, of any kind relative to the information or any portion thereof contained in this manual or its adaptation or use, and assumes no responsibility or liability of any kind, including, but not limited to, indirect, special, consequential or incidental damages, (1) for any errors or inaccuracies contained in the information or (2) arising from the adaptation or use of the information or any portion thereof including any application of software referenced or utilized in the manual. The information in this manual is subject to change without notice.

Trademarks

Infinera®, FastSMP™, FlexCoherent®, iWDM®, What the Network Will Be®, and logos that contain Infinera are trademarks or registered trademarks of Infinera Corporation or its subsidiaries, in the United States and other countries.

All other trademarks in this manual are the property of their respective owners.

Infinera Regulatory Compliance for Class A Digital Devices

Federal Communications Commission (FCC) Statement

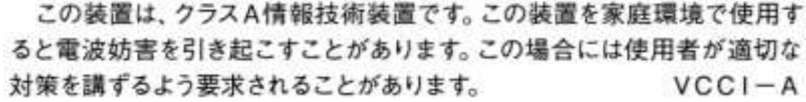
Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Industry Canada Statement

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Japan Voluntary Control Council for Interference (VCCI) Statement



この装置は、クラスA情報技術装置です。この装置を家庭環境で使用す
ると電波妨害を引き起こすことがあります。この場合には使用者が適切な
対策を講ずるよう要求されることがあります。 VCCI－A

Translation:

This is a Class A equipment. Operation of this equipment in a residential environment could cause radio interference. In such a case, the user may be required to take corrective actions. VCCI-A

Warning

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

U.S. Food and Drug Administration (FDA) Regulations for Laser Products

This product complies with the United States Code of Federal Regulations, CFR Title 21, Ch. 1, Sections 1040.10, and 1040.11, except for deviations pursuant to the “Laser Notice No. 50" guidance document, issued on June 24, 2007.

Product Safety

Important Notice on Product Safety

This product may present safety risks due to laser, electricity, heat, and other sources of danger. Only trained and qualified personnel may install, operate, maintain or otherwise handle this product and only after having carefully read the safety information applicable to this product. The safety information is provided in the “Safety Instructions”, part of this document or documentation set.

The same text in German:

Wichtiger Hinweis zur Produktsicherheit

Von diesem Produkt können Gefahren durch Laser, Elektrizität, Hitzeentwicklung oder andere Gefahrenquellen ausgehen. Installation, Betrieb, Wartung und sonstige Handhabung des Produktes darf nur durch geschultes und qualifiziertes Personal unter Beachtung der anwendbaren Sicherheitsanforderungen erfolgen. Die Sicherheitsanforderungen finden Sie unter “Sicherheitshinweise” dieses Dokuments oder dieses Dokumentationssatzes.

Table of Contents

1 Purpose/Scope

Design for Security is the part of Infinera's Create process framework. One mandatory part of DFSEC is the development of a product hardening guide for each system and for each product release.

Product hardening guides provide the recommended configuration changes to maintain system and network security. These guides are based on the risks determined by product security threat and risk analysis. This guide satisfies the Common Criteria requirement for an Assurance Guidance Document for Preparative Procedures (AGD_PRE) and Operational Guidance (AGD_OPE).

The Target of Evaluation (TOE) analyzed in this document is the Infinera GX G42 running C-OS R6.2.10. This revision of the document considers all capabilities of the TOE system currently in the product as of R6.2.10.

1.1 Reference documents

"R6.2.10 Infinera GX G40 CLI Security Command Reference Guide", Revision 002, January 2025

This document contains a list of all the commands that may be executed on the console or an SSH CLI session.

Note that the referenced CLI Guide has not been evaluated and was not used to satisfy any of the NDcPP guidance assurance activities. It is only intended to be used as a supplement, providing additional information beyond the CC evaluated configuration. Furthermore, any commands found in the referenced CLI Guide that have not been explicitly mentioned in this Hardening Guide are outside the scope of this document.

2 Reviewed Subsystems

The following systems were considered when developing these guidelines

Table 1 Reviewed subsystems

#	Category	Assets
1	Network connectivity	Network interfaces, Network configuration
2	User authentication	User account policies, default user configuration
3	System Auditing	Network auditing, User auditing, Time-system auditing

3 Considerations

3.1 FIPS Mode configuration

The TOE must be configured in FIPS mode so that only approved and CAVP certified cryptographic algorithms are available. Other changes to the TOE behavior are summarized below in Table 2.

SSPs (Sensitive Security Parameters) are zeroized when entering and leaving FIPS mode. This means that symmetric keys, asymmetric keys (public and private), secrets and passwords are all erased.
Shell access, console-user, guest containers, third-party applications, TL1 and manual module switchover are not allowed.
Datapath Encryption is always required and cannot be disabled.
Database restoration is limited to other databases that were saved by a device in FIPS mode.
Lockout on invalid login attempts happens with minimum values.
Secure mode, strict-password-check, strict-hostkey-check are always enabled.
Software upgrade always has traffic impact.
Dual controller operation is required, but hitless controller switch over is not available
ZTP may be enabled but uses two passes. ZTP was not included in the NIAP evaluation.

Table 2. FIPS required behaviors

3.2 Unnecessary Network interfaces

Don’t connect/configure interfaces that are not required. This includes the AUX1 and AUX2 interfaces.

The procedure provided in this document will indicate when the NE may be connected to the DCN.

Commands are also provided to disable interfaces that are unnecessary.

3.3 IPSEC requirements

A number of DCN protocols on the TOE do not provide acceptable security, including NTP and RADIUS. Securing these protocols require deployment/configuration of IPSEC.

IPSEC and TLS utilizes X.509 certificates for identity management. A standalone Certificate Authority may be necessary to avoid purchasing X.509 certificates when setting up the network of IPSEC endpoints.

3.4 Limit communications to necessary endpoints

Communications on the TOE should be limited to only those endpoints that are expected. This can be done by entering Security Policy Definitions, allowing traffic received from expected endpoints and discarding traffic from unexpected endpoints.

4 Prerequisite information

Performing the hardening of the TOE requires the following prerequisite information:
NOTE: When Default is blank, there is no default.

Parameter	Description and Range	*Default Value*	*Configured Value*
FIPSMODE	FIPS Mode (Yes / No) and Operation Level (1 / 2)	No	
EXISTINGUSERNAME	Existing User account		
EXISTINGUSERPASSWORD	Existing User password		
FIRSTUSERNAME	Initial SA-user account created on a first boot of a TOE.		
FIRSTUSERPASSWORD	Password for SA-user account created on first boot of a TOE.		
BANNERMSGSTRING	This string will be presented to the user before completing the Login process. It is presented on all interfaces. It may be of 0 to 1440 characters.	*<none>*	
CSPENCRYPTIONKEY	EncryptionKey used for protecting stored Critical Security Parameters (CSPs)		
MXINV	Number of Invalid Login Attempts before account is suspended. [0-9]	3	
DURAL	Duration in seconds for account suspention after exceeding MXINV. [0-300]	60	
MGTETHADDR	IPv4 address for the NE's Management Ethernet interface At least one Management Ethernet or Management Loopback interface must be configured on an NE.	*<none>*	
MGTETHMASK	IPv4 prefix mask for the NE's Management Ethernet interface This is required if the Management Ethernet interface is being configured.	*<none>*	
LOMGMTADDR	IPv4 address for this NE's Management Loopback Interface At least one Management Ethernet or Management Loopback Interface must be configured on an TOE.	*<none>*	
DNSDOMAIN	DNS Domain to be used if a transfer is attempted and a domain name is not included with the hostname.	*<none>*	
DNSSRVRADDR	IP Address of a DNS server	*<none>*	
DNSSRVRADDR2	IP Address of a second DNS server	*<none>*	

DCNNEXTHOP	IP Address of a neighboring IPv4 router to be used as a default router. DO NOT USE IF YOU WILL BE PEERING OSPF WITH THE DCN ROUTER	*<none>*	
INTERFACENAME	Interface Name	*<none>*	

DNSTRING	Distinguished Name ordered string identifiying this TOE NE. The string is a comma separated list consisting of 1 or more of the following Relative Distinguished Names (RDN):
	C=”***<Country>***”
	ST=”***<State or Province>***”
	L=”***<Locality>***”
	O=”***<Organization>***”
	OU=”***<Organizational Unit>***”
	CN=”***<Common Name>***”
	Note: for all RDNs except OU, it is not possible to specify two RDN of the same type in a Distinguished Name. For OU, multiple OUs are allowed, but the order they are specified is important. At least one CN must be specified, all other RDNs are optional.
		<none>	

ROOTCAURL	URL for the root CA X.509v3 to be trusted by this NE. The URL is of the format: [scp/sftp]://<USER>@<SSHSRVRADDR>:/Path/To/CACERT/ca_cert.p7b	*<none>*	
ROOTCANAME	Name to be used to reference the ROOT CA certificate	*<none>*	
ROOTCASFTPSRVRPASSWD	Password used for filetransfer of ROOTCA certificate.	*<none>*	
INTERMEDIATECAURL	URL for an intermediate CA X.509v3 to be trusted by this NE. The URL is of the format: [scp/sftp]://<USER>@<SSHSRVRADDR>:/Path/To/CACERT/intermediate_ca_cert.p7b	*<none>*	
NECERTURL	URL for the NE’s X.509 certificate. The URL is of the format: [scp/sftp]://<USER>@<SSHSRVRADDR>:/Path/To/NECERT/ne_cert.p12	*<none>*	
PASSPHRASETHATPROTECTSPKCS12	Passphrase used to wrap the private key in the NECERT PKCS12 file	*<none>*	
NTPADDR	The IPv4 Address for an NTP server.	*<none>*	
NTPSPDMODE	IPSEC SA Mode: Transport or Tunnel.	*<none>*	
NTPSPDSUITE	Security Suite used for traffic exchanged with the NTP server. The current recommended suite is: DHE2048-AES256CBC-SHA384.	*<none>*	
SYSLOGADDR	The IPv4 Address for a SYSLOG server.	*<none>*	
SYSLOGSPDMODE	IPSEC SA Mode: Transport or Tunnel.	*<none>*	

SYSLOGSPDSUITE	Security Suite used for traffic exchanged with the SYSLOG server. The current recommended suite is: DHE2048-AES256CBC-SHA384.	*<none>*	

5 Hardening Procedures

5.1 Connect the Craft terminal to the TOE and login

Connect the Craft terminal (local console) to the TOE using the console serial interface. Do not establish any other network connections to the TOE or to the Craft PC.

Using the console serial interface, establish a connection to the TOE.

5.1.1 NE with Existing User login

If the first user has already been configured on the TOE, then login as follows:

Login: ***<EXISTINGUSERNAME>***
Password: ***<EXISTINGUSERPASSWORD>***

Once logged in, clear the TOE database using the following command:

```
clear database
```

This will cause the TOE to reboot and clear the system database to an unconfigured state.

5.1.2 First User login

Create the first user as follows:

Login: ***<FIRSTUSERNAME>***
New password: ***<FIRSTUSERPASSWORD>***
Retype new password: ***<FIRSTUSERPASSWORD>***

The <firstUserName> is required to be a string of 1 to 32 characters, containing UpperCaseAlpha, LowerCaseAlpha, Numeric, or LimitedSpecial chacters. These are defined as follows:

LimitedSpecial: -. _
Numeric: 0123456789
UpperCaseAlpha: ABCDEFGHIJKLMNOPQRSTUVWXYZ
LowerCaseAlpha: abcdefghijklmnopqrstuvwxyz

The <firstUserPassword> is required to have basic complexity applied, meaning it can use up to 200(with a minimum of 8 chars) of the following characters (<sp> indicates the space character):

Special: <sp> !“#$%&‘()*+,-./:;<=>?@[\]^_`{|} ~
Numeric: 0123456789
UpperCaseAlpha: ABCDEFGHIJKLMNOPQRSTUVWXYZ
LowerCaseAlpha: abcdefghijklmnopqrstuvwxyz

Note: the <firstUserPassword> will not be echoed to the user – a string of asterisks (*) will be shown in its place.

This login/password pair establishes the default security administrator on the TOE system.

5.1.3 Determine if the system is in ZTP mode

The TOE may be in ZTP mode since the database has been cleared. To find out if it is in ZTP mode, use the following command:

```
show ztp
```

The response will include the attribute ‘ztp-mode’ which will be ‘enabled’ or ‘disabled’. If it is ‘enabled’ disable ztp with the following command:

```
change-ztp-mode disabled
```

5.1.4 Clear Recovery mode

The TOE will be in recovery mode since the database has been cleared. Place the TOE into normal operation mode using the following command:

```
clear recover-mode -f
```

5.2 Place the TOE into FIPS operation mode

On the TOE, NDcPP compliance is dependent on the system being placed into FIPS operational mode. This is necessary as the cryptographic algorithms in Non-FIPS mode have not been CAVP certified as they have been in FIPS mode.

5.2.1 Enable FIPS Mode

Execute the following command to enable FIPS mode:

```
fips mode-enable
```

A confirmation message will be displayed. Answer ‘y’ to proceed.

This will cause the TOE to reboot, delete its database, networking configuration and zeroize all CSPs.

5.2.2 Recreate first user, disable ZTP and recovery-mode changes from §5.1

Recreate the first user and repeat these commands:

```
change-ztp-mode disabled
clear recover-mode -f
```

5.2.3 Determine if TOE is presenting current alarm information

The TOE may be presenting cached alarm information. You can check the alarm-report status using the following command:

```
show alarm-report-ready
```

If the TOE is able to show current alarm information, the TOE will respond with

```
alarm-report-ready    true
```

If the TOE is responding with ‘false’, wait and check again. It must be ‘true’ before you can proceed.

5.2.4 Determine if system has passed FIPS Known Answer Tests (KATs)

If the TOE's encryption subsystem has not passed the Known Answer Tests (KAT) performed at startup, the TOE will be in fips-error state. The following command will retrieve the TOE's fips state:

```
show fips
```

If the TOE has passed all KATs, the returned information should look as follows:

```
fips-mode       enable
fips-state      fips-idle
```

If fips-state is fips-error, the module is currently not operating correctly. Contact Infinera to troubleshoot this failure.

5.2.5 Check NIAP compliance, set expected NIAP compliance mode, retrieve NIAP compliance alarm state and resolve compliance issues

The TOE allows configuration of options that are not NIAP compliant. When this is done, the system administrator must be notified of the non-compliance state. When the TOE is non-compliant, the system administrator must be able to determine what needs to be updated to bring the TOE back into compliance. The expected TOE state and the current issues that need be corrected are set and determined with the following commands:

Determine if TOE is currently NIAP compliant:

```
show system security niap niap-compliance
```

This will return ether 'true' if TOE is compliant or 'false' if non-compliant. The compliance state is also monitored by the system and reported as a alarm, retrievable with the following command:

```
show alarm
```

If the TOE is currently not in the expected NIAP compliance state, the alarm list will include an NIAP-COMPLIANCE-MISMATCH alarm.

If compliance is expected, set the TOE's expected NIAP compliance:

```
set system security niap expected-niap-compliance true
```

To get list of NIAP compliance issues:

```
show system security niap non-compliance-reason
```

When the issues are resolved, the NIAP-COMPLIANCE-MISMATCH alarm will be removed from the TOE.

5.3 Configure TOE security policies

5.3.1 Establish the Pre-login Banner message

All users need awareness of fact that their use of the system will be monitored and can be used as evidence for enforcement. This needs to be done prior to their use of the TOE, so the Banner message must be presented prior to the login process.

To establish the Pre-login Banner message, use the following command:

set system protocols ssh pre-login-message "***<bannerMsgString>***"

The message is a string that may be between 0 and 1440 characters in length. The quotes are necessary since the string may contain spaces. The Banner is displayed on all administrative interfaces, not just SSH.

5.3.2 Set CSP encryption key

The following TOE security policies establish the encryption key used for the storage of Critical Security Parameters (CSP) as well as require the use of secure, encrypted communications for remote access as well as file transfers.

Establish the Encryption key used for Critical Security Parameters

```
set system security security-policies csp-symmetrical-key <cspEncryptionKey>
```

The following network security policies require the use of secure, encrypted communications for all remote accesses as well as file transfers.

Disable the TOE’s use of TELNET, FTP, HTTP and SNMP without encryption:

```
set system security security-policies secure-mode true
```

Configure the TOE’s SSH client to verify SSH server signatures on connection:

```
set system security security-policies ssh-strict-host-key-checking strict
```

5.3.3 Require use of encrypted communications

NOTE: This is done automatically when the TOE is operating in FIPS mode.

Disable the TOE’s use of FTP, HTTP and SNMP without encryption:

```
set system security security-policies secure-mode true
```

5.3.4 Generate host SSH keys

Configure the TOE’s SSH server to support RSA encryption with a key length of 4096 bits:

```
ssh-keygen -b=4096 -t=rsa
```

The ssh-keygen command also supports 2048 or 3072 bit RSA keys by replacing **-b=4096** with **-b=2048** or **-b=3072.** This will also generate an RSA host key.

Configure the TOE’s SSH server to support ECDSA encryption with a key length of 384 bits:

```
ssh-keygen -b=384 -t=ecdsa
```

The ssh-keygen command also supports p256 and p521 ECDSA keys by replacing **-b=384** with **-b=256** or **-b=521.** This will also generate an ECDSA host key.

5.3.5 Modify SSH cipher suite configuration

The SSH subsystem negotiates a number of algorithms at the start of a session. The following sections provide the commands to allow addition/removal of the algorithms supported in the evaluated configuration.

5.3.5.1 Add/remove SSH encryption ciphers available for negotiation

SSH Encryption ciphers offered during negotiation are specified by the *ssh-ciphers* attribute in the system security-policies. To retrieve this attribute from the TOE, use the command:

```
show system security security-policies ssh-ciphers
```

The order of the ciphers specifies preference (i.e. the first cipher in the list has the highest preference). Negotiation will start with the first cipher offered by the client that matches the first cipher supported by the server. This order is independent of cipher strength although we recommend having algorithms with higher strength first.

Modifying this list on the TOE is done with the set command:

```
set system security security-policies ssh-ciphers aes128-ctr,aes256-ctr,aes128-gcm-at-openssh-com,aes256-gcm-at-openssh-com
```

5.3.5.2 Add/remove SSH message authentication codes (MACs) available

SSH message authentication codes (MACs) offered during negotiation are specified by the *ssh-macs* attribute in the system security-policies. To retrieve this attribute from the TOE, use the command:

```
show system security security-policies ssh-macs
```

As with ssh-ciphers, the order of the macs specifies preference.

Modifying this list on the TOE is done with the set command:

```
set system security security-policies ssh-macs hmac-sha2-256,hmac-sha2-512
```

The ssh-macs attribute does not include the implicit algorithm as it is an implicit behavior used when AES-GCM encryption algorithms have been selected. When aes*-gcm@openssh.com is negotiated as the encryption algorithm, the MAC algorithm field is ignored and GCM is implicitly used as the MAC.

5.3.5.3 Add/remove SSH key exchange algorithms

SSH key exchange methods offered during negotiation are specified by the ssh-key-exchange attribute in the system security policies. To retrieve this attribute from the TOE, use the command:

```
show system security security-policies ssh-key-exchange
```

As with ssh-ciphers, the order of the key-exchange specifies preference.

Modifying this list on the TOE is done with the set command:

```
set system security security-policies ssh-key-exchange diffie-hellman-group14- sha256, ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
```

5.3.5.4 Add/remove SSH key-authentication algorithms

SSH key-authentication methods offered during negotiation are specified by the ssh-host-key-algorithms and ssh-public-key-algorithms attributes in the system security policies. Host authentication and client authentication use the same algorithms, but are separately controlled.

To retrieve these attributes from the TOE, use these commands:

```
show system security security-policies ssh-host-key-algorithms
```

```
show system security security-policies ssh-public-key-algorithms
```

As with ssh-ciphers, the order of the key-algorithm specifies preference.

Modifying this list on the TOE is done with these set commands:

```
set system security security-policies ssh-host-key-algorithms rsa-sha2-256,rsa-sha2-512,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521
```

```
set system security security-policies ssh-public-key-algorithms rsa-sha2-256,rsa-sha2-512,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521
```

5.3.5.5 SSH Client Public Key Authentication

It is possible for a user to connect to the TOE using an SSH Public Key. To do this, the TOE user account needs to have the SSH Public Key loaded into it. This is done using the following commands:

```
add ssh-authorized-key-<username>/1 public-key <base64publicKey>
set security-policies ssh-authentication-method public-key
```

NOTE: When the second statement is entered, the TOE will require SSH public keys for all users.

5.4 Configure user security policies

NOTE: This settings in this section are done automatically if the TOE is operating in FIPS mode

The following user security policies limit the possibility of unauthorized system access.

Configure the TOE’s user authentication subsystem to require complex passwords, and prevent the user from reusing previously used passwords when changing their password:

```
set system security security-policies strict-password-check true
set system security security-policies enforce-password-history-check true
```

Configure the TOE’s user authentication subsystem to suspend user accounts that have too many invalid login attempts, set the threshold that triggers account suspension, and set the duration of account suspension:

```
set system security disable-user-lockout false
set system security user-<firstUserName> max-invalid-login <MXINV>
set system security user-<firstUserName> suspension-time <DURAL>
```

where ***<MXINV>*** and ***<DURAL>*** have the ranges 1..255 count and 0..1440 minutes.

Local serial console port access to the CLI is not subject to the lockout and ensures that administrator access is always available.

5.5 Establish System SSH Identities

5.5.1 Retrieve TOE’s SSH host public keys

The TOE’s SSH host public keys should be retrieved and placed in a repository so it may be used by SSH clients to validate it is speaking to the correct TOE when establishing a connection. The following command will retrieve all the SSH public keys from the TOE:

```
show system protocols ssh ssh-host-key-ssh-rsa4096 public-key
show system protocols ssh ssh-host-key-ecdsa-sha2-nistp384 public-key
```

The host SSH public key is within the quoted *public-key* attribute returned by the NE.

5.6 Configure the IPv4 DCN

Note that IPv6 addresses were not configured or tested in the evaluated configuration.

5.6.1 Configure TOE's IPv4 Management Ethernet interface(s)

The Management Ethernet Interface is a physical interface located on the TOE front panel. In cases where the TOE is managed via GCC or OSC channels, this interface may not be required. See section 0 regarding configuration of unnecessary interfaces.

```
set -f interface-DCN ipv4-address-assignment-method static
```

```
add ipv4-address-DCN/<MGTETHADDR> netmask <MGTETHMASK>
```

5.6.2 Configure TOE's IPv4 Management Loopback Interface

The Management Loopback Interface is a logical interface. If a Management Ethernet Interface has been configured and this NE will not support management via Comm Channels, this interface may be omitted.

```
add ipv4-address-LO-MGMT/<LOMGMTADDR> netmask 255.255.255.255
```

```
add system networking routing ospf-instance router-id <OSPFROUTERID>
  ospf-area-<OSPFAREAID> ospf-interface-<LOMGMTADDR>
```

5.6.3 Configure TOE's IPv4 Comm Channel Interface(s)

Configure each Comm Channel Interface on the TOE supporting DCN communications. Note: Configuring one or more Comm Channel requires the configuration of the Management Loopback interface.

Each Comm Channel interface will use the following command, with an interface named by the card and port used:

```
add ipv4-address-<OSCAID>/0.0.0.0 ipv4-enabled true
```

```
set system networking routing ospf-instance ospf-area-<OSPFAREAID>
  ospf-interface-<OSCAID>
```

5.6.4 Disable unnecessary DCN interfaces

Interfaces that are not necessary on the TOE are disabled in order to reduce the system's attack surface. For each interface on the TOE that is unnecessary, disable the interface using the following command:

```
set equipment <card> <port> admin-state lock
```

Respond affirmatively (i.e. 'y') to the warnings regarding NE unreachability.

This should be done for all TOE interfaces not in use, including:

```
card-1-1 port-AUX-1
card-1-1 port-AUX-2
```

The admin-state of a port can be retrieved using the following command:

```
show equipment <card> <port> admin-state
```

5.6.5 Disenable ARP Proxy

The TOE supports ARP Proxy to enable non-local systems to appear local (i.e. connected to the DCN Ethernet) if they are reachable from the TOE. This is a potential security attack point as it places unnecessary equipment in the network path to reach a destination. Such equipment can host “Man-In-The-Middle” attacks and may cause neighboring equipment to become suspicious of “ARP Spoofing”. For this reason we do not recommend enabling ARP Proxy on the TOE.

The status of ARP Proxy on a TOE interface can be determined using the following command:

show networking ***<interface>*** proxy-arp-enabled

5.6.6 Configure IPv4 Application details

The TOE supports IPv4 applications similar to normal Unix or Windows computers. This section has the commands to configure the DNS server.

5.6.6.1 Configure IPv4 DNS domain search path and server

This command enables the TOE to resolve names using DNS and configures the domain search path:

set dns enabled true search ***<DNSDOMAIN>***

This command configures a DNS domain server:

add dns-server-***<DNSSRVRADDR>***

Multiple DNS domain servers may be specified by repeating the command with additional IP addresses:

add dns-server-***<DNSSRVRADDR2>***

5.6.6.2 Configure TOE IPv4 Source Interface

The local IP address used in communications is the Management Loopback interface. Unlike classic Coriant equipment, the ASINTF does not need to be specified.

5.6.7 Configure Access Control Lists (ACL)

Access Control Lists are used to filter packets that arrive on a TOE interface as they are making their way to their destination. ACLs are configured in two steps: 1) Setting admin-state/avail-state of an ACL rule on an interface and 2) configuring rule chains or Access Control Entries (ACEs).

5.6.7.1 Creating an Access Control List (ACL)

Creating an ACL is done by the following command:

add acl-***<name>*** type ***<ipv4|ipv6>*** interface ***<1-AUX-1|1-AUX-2|DCN>*** [admin-state ***<lock|maintenance|unlock>***]

5.6.7.2 Creating an Access Control Entry (ACE)

Creating an ACE is done by the following command:

add ace-<name/sequence-id> [action ***<drop|accept>***] [direction ***<input>***] [interface ***<1-AUX-1|1-AUX-2|DCN>***] source-ip-address ***<ipv4 or ipv6 address>*** destination-ip-address ***<ipv4 or ipv6 address>*** source-lower-port ***<port number>*** source-upper-port ***<port number>*** destination-lower-port ***<port number>*** destination-upper-port ***<port number>*** [label ***<label>***] protocol ***<protocol>*** [logging-action ***<true|false>***] ttl ***<hop limit>***

We recommend creating Access Control Entries for IPv4 addresses that should never be possible on an interface (i.e. martian addresses)

5.6.8 Configure IPv4 DCN routes

The DCN network deployed may be extremely simple (e.g. a single TOE acting as a host), or it may be extremely complex (e.g. a TOE acting as an OSPF router). The following two sections provide example commands to configure IPv4 routes

5.6.8.1 Configure IPv4 DCN Static routes

If not using OSPF routing, add a static default route using the following command:

```
add ipv4-static-route-0.0.0.0/0/MGMT next-hop-address <DCNNextHop>
```

5.6.8.2 Configure IPv4 DCN routing protocol

If OSPF routing will be used to learn the network topology and compute routes, the following commands are appropriate:

Create an OSPF instance and OSPF area instance. The management vrf (vrf-MGMT) is created automatically. The following commands create the rest of these entities:

Create the OSPF instance and area:

```
add ospf-instance-<ospfName>
add ospf-area-<ospfName>/<ospfAreaID>
```

Enable OSPF on the DCN, Loopback and optical interfaces:

```
add ospf-interface-<ospfName>/<ospfAreaID>/DCN
add ospf-interface-<ospfName>/<ospfAreaID>/LO-MGMT
```

Configure OSPF Authentication for each interface using these commands:

```
set ospf-interface-<ospfName>/<ospfAreaID>/<interfaceName>
  ospf-if-routing active ospf-auth-enable true
add ospfv3-ipsec-security-association-<ospfName>/<ospfAreaID>/<interfaceName>/<spi> integrity-algorithm <integrityValue>
add auth-key-<ospfName>/<ospfAreaID>/<if>/<spi> key <keyValue>
```

5.6.9 Connect TOE's DCN interface

You may now connect the TOE's DCN interface to the network.

5.7 Configure System X.509 Certificates

5.7.1 Load the ROOT CA Certificates recognized by the TOE

ROOT CA certificates are loaded on the TOE using the following command:

```
download trusted_certificate source=<ROOTCAURL> certificate-name=<ROOTCANAME> password=<ROOTCASFTPSRVRPASSWD>
```

Example that imports an PKCS#7 public certificate file:

```
download trusted_certificate source=sftp://tom@1.2.3.4/rootca_cert.p7b certificate-name=rootca-1 password='my_sftp_password'
```

5.7.2 Load an Intermediate CA Certificate for the TOE

Intermediate CA certificates is loaded using the following command:

download trusted_certificate source=***<INTERMEDIATECAURL>*** certificate-name=***<INTERMEDIATECANAME>*** password=**<INTERMEDIATECASFTPSRVRPASSWD>**

Example that imports an PKCS#7 public certificate file:

download trusted_certificate source=**sftp://tom@1.2.3.4/intermediateca_cert.p7b** certificate-name=**intermediateca-1** password=**'my_sftp_password'**

5.7.3 Establish the TOE's Identity Certificate

The TOE's identity for TLS and IPSEC is contained in an X.509 certificate. The certificate establishes a binding between the TOE's stated identity and its Asymmetric key pair. The certificate is installed on the TOE either by 1) generating an asymmetric key pair (consisting of a Public Key and Private Key), issuing a CSR containing the Public key and receiving a P7 file containing a signed certificate from a CA, or 2) receiving a P12 file containing a signed certificate and Private Key file.

The certificate is only valid for the entity that has access to the Private Key, so it is very important to keep this key safely stored. For this reason, the preference is to use CSRs instead of loading P12 files. The following sub-sections provide the commands to create a key pair, issue a CSR

5.7.3.1 Generate TOE Asymmetric Key Pair & issue Certificate Signing Request (CSR)

Capture the output returned to the Console TTY for the follow command:

csr-gen certificate-name=***common-leaf-1*** key-algorithm=***rsa4096*** subject=***'/C=US/ST=CA/L=San Jose/OU=InfineraR&D/CN=test'***

NOTE: The key-algorithm can be ***rsa2048***, ***rsa3084***, ***rsa4096***, ***eccp256***, ***eccp384*** or ***eccp521***.

This should return a CSR block, bracketed by '-----BEGIN CERTIFICATE REQUEST-----' and '-----END CERTIFICATE REQUEST-----'. Capture this CSR block including the BEGIN and END lines and send it to your Certificate Authority (CA) for processing. The CA should return a PKCS7 file containing a signed certificate.

5.7.3.2 Load the Signed Certificate for the TOE

Signed TOE certificates are loaded using the following command:

download local-certificate source=***<NECERTURL>*** certificate-name=***<LEAFCERTNAME>*** password=**<LEAFCERTSFTPSRVRPASSWD>**

Example that imports an PKCS#7 public certificate file:

download local-certificate source=**sftp://tom@1.2.3.4/leaf_cert.p7b** certificate-name=**common-leaf-1** password=**'my_sftp_password'**

The source URL above accesses the file 'leaf_cert.p7b' on the host 1.2.3.4 using the user 'tom'.

The same name must be used for the csr-gen command and for the download local-certificate command. This is so the TOE may associate the Asymmetric Key Pair with the received certificate.

5.7.3.3 Alternative: Install signed X.509 Certificate and Private Key for this TOE

The following command will import an PCKS#12 file containing a signed X.509 Certificate and its password-wrapped Private Key into the TOE:

```
download local-certificate source=<NECERTURL> certificate-name=common-leaf-1
  password='my_sftp_password'
  passphrase='<PASSPHRASETHATPROTECTSPKCS12>'
```

NOTE: Self-signed certificates are NOT accepted by the TOE.

NOTE: The passphrase has basic complexity rules applied, meaning it can use up to 200 characters(with a minimum of 8 chars) of the following characters:

<table>
<tr><td>Special:</td><td>&lt;sp&gt; !“#$%&amp;‘()*+,-./:;<=&gt;?@[\]^_`{|} ~</td></tr>
<tr><td>Numeric:</td><td>0123456789</td></tr>
<tr><td>UpperCaseAlpha:</td><td>ABCDEFGHIJKLMNOPQRSTUVWXYZ</td></tr>
<tr><td>LowerCaseAlpha:</td><td>abcdefghijklmnopqrstuvwxyz</td></tr>
</table>

5.7.4 CRL, CDP and OCSP configuration.

Certificate Revocation Lists (CRL), CRL Distribution Points (CDP) and Online Certificate Status Protocol (OCSP) are supported by the TOE. Configuration of CRLs, CDPs and OCSP servers is discussed in Section 6.0.

5.8 Configure TLS based applications

The system supports a number of TLS applications and provides its identity using X.509 certificates. This section is to set TLS configuration parameters and system identity.

5.8.1 Configure TLS version

The TOE supports TLS1.2. The system default configuration is for TLS1.2-only, but this can be changed using the following command:

```
set system security security-policies supported-tls-version <TLS version>
```

The values allowed are *1.2-only*, *1.3-only* and *1.3-with-fallback-to-1.2*. No value other than ***1.2-only*** has been tested and will cause the system to go into alarm as it cannot comply with the *expected-niap-compliance* state.

5.8.2 Configure TLS version cipher precedence

The order of cipher preference is specified using this command:

```
set system security security-policies tls-1.2-cipher-suites <TLS 1.2 ciphers ordered list>
```

The list of supported TLS 1.2 ciphers can be retrieved by replacing ***set*** with ***show***. The listed ciphers are:

```
DHE-RSA-AES128-SHA256
DHE-RSA-AES256-SHA256
DHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES128-SHA256
ECDHE-RSA-AES256-SHA384
ECDHE-ECDSA-AES128-SHA256
ECDHE-ECDSA-AES256-SHA384
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES256-GCM-SHA384
```

Ciphers that appear earlier in the list have preference over ciphers that appear later in the list. The list entries are separated by commas. The default cipher preference is based on the security strength of the ciphers as described in Table 2 of NIST SP800-57, with ECDHE preferred over DHE, ECDSA certificate authentication preferred over RSA certificate authentication and AES GCM preferred over AES CBC. Not all ciphers need to be included in the list. Some supported ciphers (e.g. TLS_RSA_WITH_AES_256_GCM_SHA384) may not be in the default list.

The TOE performs key establishment using Diffie-Hellman groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 or ECDHE curves: secp256r1, secp384r1, secp521r1 depending on the chosen cipher suite. The key agreement parameters of the server key exchange message are specified in the RFC 5246 (section 7.4.3) for TLSv1.2.

5.8.3 Configure TLS application identity

Associate the TOE local X.509 certificate to be used as an identity by existing TOE TLS applications.
In general, the following command will be repeated for each local application in use:

```
set secure-application-<appname> active-certificate-id common-leaf-cert-1
```

5.8.3.1 WebGUI

Now associate the TOE WebGUI application with the common X.509 leaf certificate using the following command:

```
set secure-application-WebGUI active-certificate-id common-leaf-cert-1
```

5.9 Configure IPSEC

Configuring IPSEC may be done using X.509 certificates or pre-shared keys. If Pre-shared keys are in use, these first two steps may be omitted. If X.509 certificates are being used, these steps MUST be done.

5.9.1 Optional: Install Trusted CA Certificate

It is assumed the same Root CA and Intermediate CAs for TLS are being used on the TOE for IPSEC. If different CAs are being used, repeat the steps in Section 5.7 to install additional CA certificates.

5.9.2 Optional: Install signed X.509 Certificate and Private Key for this TOE

The commands in Section 5.7.3 imports signed X.509 Certificates and (optionally) key-wrapped Private Key into the NE. If a separate end certificate is being used for IKE (IPSEC Key Exchange), load it now using the same command, but with a different certificate-name.

For P7 certificates generated in response to a Certificate Signing Request (CSR), use the command:

```
download local-certificate source=<NECERTURL> certificate-name=<LEAFCERTNAME>
password=<LEAFCERTSFTPSRVRPASSWD>
```

For P12 certificates, use the command:

```
download pkcs12 <NECERTURL> certificate-name=ike-leaf-2
  password=<LEAFCERTSFTPSRVRPASSWD>
  passphrase='<PASSPHRASETHATPROTECTSPKCS12>'
```

NOTE: Self-signed certificates are NOT accepted by the NE. See the Annex (section 8) for information for how to setup a Certificate Authority (CA).

Now associate the end certificate with the IPSEC application:

```
set local-certificate ike-leaf-2
```

5.9.3 Configure IPSEC Instance and Peer association

The specific command used to create an Encryption context for IPSEC is dependent the DCN interface used to cary the IPSEC traffic. Typically a Loopback Interface is used for this purpose. It was created in section 5.6.2 above and is used in this command:

```
set networking use-as-source LO-MGMT
```

5.9.3.1 IPSEC peer using X.509 certificate authentication

Now specify the IPSEC peer entity

```
add ikev2-peer-ipsec/<peer> destination <peerIPaddress>
  authentication-scheme x.509-certificate
  local-identity <localIdentity> local-identity-type <identityType>
  peer-identity <peerIdentity> peer-identity-type <identityType>
```

The local-identity-type and peer-identity-type may be ***ipv4-address***, ***ipv6-address***, ***fqdn***, or ***dnx509***. For IPv4 address, the related identity is an IPv4 addresses. For IPv6 address, the related identity is an IPv6 address. For fqdn, the related identity is a DNS address. For dnx509, the related identity is a X.509 Distinguished Name

5.9.3.2 Alternate: IPSEC peer using pre-shared key authentication

It is possible to have an IKEv2 peer use pre-shared-keys instead of X.509 certificates. For this, the peer entity configuration changes the authentication-scheme attribute and adds pre-shared-key-type and psk-***<type>*** attributes as follows:

```
add ikev2-peer-ipsec/<peer> destination <peerIPaddress>
  authentication-scheme pre-shared-key
  local-identity <localDNSName> local-identity-type <identityType>
  peer-identity <peerDNSName> peer-identity-type <identityType>
  pre-shared-key-type <keyType> psk-<type> <preSharedKey>
```

where: ***<keyType>*** is ascii, hex or hash, psk-***<type>*** is psk-ascii, psk-hex or psk-hash, and ***<preSharedKey>*** is a string that is 8 to 128 characters (ascii) or 8 to 128 bytes (hex) in length

5.9.3.3 Configure encryption proposal

Now provide an encryption proposal for IKE communications with the peer:

```
add ike-sa-proposal-ipsec/<peer>/<proposalNum> dh-group <dheGroup>
  prf <saPrf> integrity-algorithm <integrityAlg>
```

```
add encryption-algorithm-ipsec/<peer>/<proposalNum>/<encryAlg>/<keylen>
```

where: ***<dheGroup>*** can be ***dhe-2048, dhe-3072, dhe-4096, dhe-6144, dhe-8192, ecp-256, ecp-384,*** or ***ecp-521***

<saPrf> can be ***hmac-sha2-256, hmac-sha2-384,*** or ***hmac-sha2-512, hmac-sha1***

<integrityAlg> can be ***hmac-sha2-256-128, hmac-sha2-384-192, hmac-sha2-512-256,*** or ***hmac-sha1-160***

<encryAlg> can be ***null, aes-gcm-8, aes-gcm-12, or aes-gcm-16***

<keylen> can be ***key-length-0*** (for null)***, key-length-128, key-length-192, key-length-256***

This proposal covers encryption used for IKE communications between the local system and the peer.

5.9.4 Configure Security Policy Definitions

Security Policy Definitions identify the traffic to be placed in a security association, and the encryption suite to be used. The encryption suite used for an SPD must be of the same strength or stronger than the suite used for the IPSEC Peer.

The Security Policy Definitions (SPD) priority is configurable for each SPD rule. The SPD is used if the traffic selector matches the traffic, and the priority is the lowest (ie. 1 has priority over 9999) in the system. On ingress traffic, interface ACLs are processed prior to IPsec. On egress traffic, interface ACLs are processed after IPsec.

All SPDs have traffic selector statements. These statements provide targets to match the network protocol as well as local and remote endpoints for the network addresses and ports.

All SPDs entries follow the pattern of the following three sections:

5.9.4.1 Create SPD Entry

Create an SPD, provide it an evaluation priority order, specify its behavior and traffic mode:

```
add ipsec-spd-entry-ipsec/<peer>/<spdName> priority 1 action <action> mode
  <trafMode>
```

where: ***<peer>*** is a local identifier for the peer. A ***<peer>*** name of ‘global’ is reserved for use by SPDs that don’t require a named peer (e.g. rules where action is ***discard*** or ***bypass***)

<spdName> is the local name for the SPD

<action> is either ***protect***, ***bypass*** or ***drop***

<trafMode> is ***tunnel*** or ***transport***. (default is tunnel)

5.9.4.2 Add Traffic Selectors

Add traffic selectors to the SPD to identify traffic to send in the Security Association (SA):

add ipsec-traffic-selector-ipsec/***<peer>***/***<spdName>***/***<trafSel>*** next-layer-protocol ***<protoNo>***

add local-subnet-ipsec/**<peer>**/***<spdName>***/***<trafSel>***/***<ipv4Subnet>***/***<ipv4Len>***

add remote-subnet-ipsec/**<peer>**/***<spdName>***/***<trafSel>***/***<ipv4Subnet>***/***<ipv4Len>***

add local-ports-ipsec/***<peer>***/***<spdName>***/***<trafSel>***/***<startPort>***/***<stopPort>***

add remote-ports-ipsec/***<peer>***/***<spdName>***/***<trafSel>***/***<startPort>***/***<stopPort>***

where: ***<peer>*** is a local identifier for the peer. A ***<peer>*** name of 'global' is reserved for use by SPDs that don't require a named peer (e.g. rules where action is ***discard*** or ***bypass***)

<spdName> is the local name for the SPD

<trafSel> is the local name for the traffic selector

<ipv4Subnet> is the subnet prefix for traffic to match

<ipv4Len> is the effective number of bits in the subnet prefix

<startPort> is the starting port for a range of TCP or UDP ports

<stopPort> is the ending port for a range of TCP or UDP ports

NOTE: ***<startPort>***/***<stopPort>*** can be replaced by 'all' to match all TCP or UDP ports

5.9.4.3 Provide an encryption proposal for the SA

After the traffic for a Security Association is identified, the traffic needs to be encrypted in a way so it can be decrypted. This is done consistent with the encryption proposal negotiated between the endpoints. These commands specify the encryption used:

add ipsec-sa-proposal-ipsec/***<peer>***/***<trafSel>***/***<proposalNum>*** dh-group ***<dheGroup>*** integrity-algorithm ***<integrityAlg>***

add encryption-algorithm-ipsec/***<peer>***/***<trafSel>***/***<proposalNum>***/***<encryAlg>***/***<keylen>***

where: ***<dheGroup>*** can be ***dhe-2048, dhe-3072, dhe-4096, dhe-6144, dhe-8192, ecp-256, ecp-384,*** or ***ecp-521***

<integrityAlg> can be ***hmac-sha2-256-128, hmac-sha2-384-192, hmac-sha2-512-256,*** or ***hmac-sha1-160***

<encryAlg> can be ***null, aes-gcm-8, aes-gcm-12, or aes-gcm-16***

<keylen> can be ***key-length-0*** (for null)***, key-length-128, key-length-192, key-length-256***

This proposal covers the encryption used for the IPSEC SA. A proposal is not needed for bypass or discard SPDs.

5.9.5 Configure IPSEC Bypass Security Policy Definitions for TLS and SSH-based protocols

TLS and SSH communications are inherently secured and therefore do not need processing by IPSEC. So TLS and SSH need SPDs to bypass IPSEC processing.

5.9.5.1 Configure bypass of HTTPS

The first set of commands configure bypass on the TOE for inbound HTTPS traffic:

```
add ipsec-spd-entry-ipsec/global/https priority 1 action bypass
add ipsec-traffic-selector-ipsec/global/https/ts1 next-layer-protocol 6
add local-subnet-ipsec/global/https/ts1/<LOMGMTADDR>/32
add remote-subnet-ipsec/global/https/ts1/0.0.0.0/0
add remote-ports-ipsec/global/https/ts1/all
add local-ports-ipsec/global/https/ts1/443/443
```

NOTE: Since this SPD is for bypass, the peer is ‘global’ and no encryption proposal is required.

5.9.5.2 Configure bypass of RESTCONF

The next set of commands configure bypass on the TOE for inbound RESTCONF traffic:

```
add ipsec-spd-entry-ipsec/global/restconf priority 1 action bypass
add ipsec-traffic-selector-ipsec/global/restconf/ts1 next-layer-protocol 6
add local-subnet-ipsec/global/restconf/ts1/<LOMGMTADDR>/32
add remote-subnet-ipsec/global/restconf/ts1/0.0.0.0/0
add remote-ports-ipsec/global/restconf/ts1/all
add local-ports-ipsec/global/restconf/ts1/8181/8181
```

NOTE: Since this SPD is for bypass, the peer is ‘global’ and no encryption proposal is required.

5.9.5.3 Configure bypass of SSH connections

The next set of commands configure bypass on the TOE for inbound SSH traffic:

```
add ipsec-spd-entry-ipsec/global/ssh priority 1 action bypass
add ipsec-traffic-selector-ipsec/global/ssh/ts1 next-layer-protocol 6
add local-subnet-ipsec/global/ssh/ts1/<LOMGMTADDR>/32
add remote-subnet-ipsec/global/ssh/ts1/0.0.0.0/0
add remote-ports-ipsec/global/ssh/ts1/all
add local-ports-ipsec/global/ssh/ts1/22/22
```

NOTE: Since this SPD is for bypass, the peer is ‘global’ and no encryption proposal is required.

5.9.5.4 Configure bypass of NETCONF

The next set of commands configure bypass on the TOE for inbound NETCONF traffic:

```
add ipsec-spd-entry-ipsec/global/netconf priority 1 action bypass
add ipsec-traffic-selector-ipsec/global/netconf/ts1 next-layer-protocol 6
add local-subnet-ipsec/global/ssh/ts1/<LOMGMTADDR>/32
add remote-subnet-ipsec/global/ssh/ts1/0.0.0.0/0
add remote-ports-ipsec/global/ssh/ts1/all
add local-ports-ipsec/global/ssh/ts1/830/830
```

NOTE: Since this SPD is for bypass, the peer is 'global' and no encryption proposal is required.

5.9.5.5 Configure default Security Policy Definition

Traffic that is not encrypted, either by IPSEC or by the application itself, should not be exchanged by the TOE with other systems on the DCN. This SPD will prevent this traffic:

```
add ipsec-spd-entry-ipsec/global/default priority 99 discard
add ipsec-traffic-selector-ipsec/global/default/ts1 next-layer-protocol all
add local-subnet-ipsec/global/default/ts1/0.0.0.0/0
add remote-subnet-ipsec/global/default/ts1/0.0.0.0/0
add remote-ports-ipsec/global/default/ts1/all
add local-ports-ipsec/global/default/ts1/all
```

NOTE: Since this SPD is for discard, the peer is 'global' and no encryption proposal is required.

5.10 Configure Time

The command used to examine the system time is:

```
show clock
```

which will display the current system time. The command used to set the system time is:

```
set-time <yearMoDayThhmmssZ>
```

where ***<yearMoDayThhmmssZ>*** is the system time as represented by ISO 8601. An example is:

```
set-time 2024-12-17T07:08:03Z
```

which sets the system time immediately to 07:08:03Z on 2024-12-17.

5.11 Configure NTPv4 Synchronization

Synchronized Time is important to correlating events in Audit logs and for enforcing certificate expiration. Configuring NTP synchronizes the clock on the NE with other systems, yielding synchronized timestamps in audit logs.

The GX G42 TOE only supports directed NTPv4 sessions. It will not react to receiving a broadcast NTP or multicast NTP packet. No configuration is needed for this behavior.

Use this command to configure NTP:

```
set system ntp ntp-enabled true ntp-server-<NTPADDR> admin-state unlock
```

The following SPD should be entered to pass the NTP communications over an IPSEC SA:

```
add ipsec-spd-entry-ipsec/<peer>/ntp1 priority 1 action protect
add ipsec-traffic-selector-ipsec/<peer>/ntp1/ts1 next-layer-protocol all
add local-subnet-ipsec/<peer>/ntp1/ts1/<LOMGMTADDR>/32
add remote-subnet-ipsec/<peer>/ntp1/ts1/<NTP1IPADDR>/32
add remote-ports-ipsec/<peer>/ntp1/ts1/all
add local-ports-ipsec/<peer>/ntp1/ts1/all
add ipsec-sa-proposal-ipsec/<peer>/ntp1/1 dh-group <dheGroup> integrity-algorithm <integrityAlg>
add encryption-algorithm-ipsec/<peer>/ntp1/1/<encryAlg>/<keylen>
```

For High Availability purposes, it is desirable for the TOE to have access to three or more NTP servers. Additional SPD entries will be needed. Use the following commands, replacing ***<NTP2IPADDR>*** and ***<NTP3IPADDR>*** with the second and third NTP server's IP address:

```
add ipsec-spd-entry-ipsec/<peer2>/ntp1 priority 1 action protect
add ipsec-traffic-selector-ipsec/<peer2>/ntp1/ts2 next-layer-protocol all
add local-subnet-ipsec/<peer2>/ntp1/ts2/<LOMGMTADDR>/32
add remote-subnet-ipsec/<peer2>/ntp1/ts2/<NTP1IPADDR>/32
add remote-ports-ipsec/<peer2>/ntp1/ts2/all
add local-ports-ipsec/<peer2>/ntp1/ts2/all
add ipsec-sa-proposal-ipsec/<peer2>/ntp1/1 dh-group <dheGroup> integrity-algorithm <integrityAlg>
add encryption-algorithm-ipsec/<peer2>/ntp1/1/<encryAlg>/<keylen>

add ipsec-spd-entry-ipsec/<peer3>/ntp1 priority 1 action protect
add ipsec-traffic-selector-ipsec/<peer3>/ntp1/ts3 next-layer-protocol all
add local-subnet-ipsec/<peer3>/ntp1/ts3/<LOMGMTADDR>/32
add remote-subnet-ipsec/<peer3>/ntp1/ts3/<NTP1IPADDR>/32
add remote-ports-ipsec/<peer3>/ntp1/ts3/all
add local-ports-ipsec/<peer3>/ntp1/ts3/all
add ipsec-sa-proposal-ipsec/<peer3>/ntp1/1 dh-group <dheGroup> integrity-algorithm <integrityAlg>
add encryption-algorithm-ipsec/<peer3>/ntp1/1/<encryAlg>/<keylen>
```

5.12 Configure RADIUS/TACACS+ servers

Centralized account management is provided by RADIUS or TACACS+ servers. At this time, the TOE does not support TLS variations of these protocols (i.e. RADSEC or TACACS+ over TLS). As a consequence, IPSEC must be used to secure these protocols. Two steps are required to establish RADIUS or TACACS+ over IPSEC: 1) configure the NE to carry RADIUS or TACACS+ over IPSEC using an SPD, and 2) configure the NE use a RADIUS or TACACS+ to Authenticate/Authorize users. Use the following commands:

The following sections describe how to configure RADIUS and TACACS+ servers on the TOE.

5.12.1 Configure the use of a RADIUS or TACACS+ server

5.12.1.1 Configure RADIUS server

To configure the TOE to use RADIUS for Authentication, use the following commands:

```
add aaa-server-<NAME> protocol-supported RADIUS role-supported authentication
  server-priority 1 server-address <RADIUSADDR> shared-secret <RADIUSSECRET>
  server-port-authentication <RADSRVRPORT> server-priority <RADSRVRPRIO>
```

where the parameters are:

<RADSRVRNAME> is the name of the RADIUS server

<RADSRVRADDR> is the IPv4 address of the RADIUS server

<RADSRVRSECRET> is the Shared Secret used for communication between this GX and the RADIUS server

<RADSRVRPORT> is the RADIUS authentication port number

<RADSRVRPRIO> is the priority order of this RADIUS server in the list of RADIUS and TACACS+ authentication servers configured in the node. Lowest Priority Server is tried first.

NOTE: RADIUS does not support Authorization checking separate from Authentication.

Set the authentication method/policy for the ordering of local and remote servers with the following command:

```
set security-policies aaa-authentication-method remote-first-then-local
```

5.12.1.2 Configure TACACS+ server

To configure the TOE to use TACACS+ for Authentication, use the following command:

```
add aaa-server-<TACACSSRVRNAME> protocol-supported TACACSPLUS
  role-supported authentication server-priority 1
  server-address <TACACSSRVRADDR> shared-secret <TACACSSRVRSECRET>
  server-port-authentication <TACACSSVRPORT> server-priority <TACACSSRVRPRIO>
```

To configure the TOE to use TACACS+ for Authorization (e.g. when the system is using MFA), use the following command instead:

```
add aaa-server-<TACACSSRVRNAME> protocol-supported TACACSPLUS
  role-supported authorization server-priority 1
  server-address <TACACSSRVRADDR> shared-secret <TACACSSRVRSECRET>
  server-port-authentication <TACACSSVRPORT> server-priority <TACACSSRVRPRIO>
```

where the parameters are:

<TACACSSRVRNAME> is the name of the TACACS+ server

<TACACSSRVRADDR> is the IPv4 address of the TACACS+ server

<TACACSSRVRSECRET> is the Shared Secret used for communication between the TOE and the TACACS+ server

<TACACSSRVRPORT> is the TACACS+ port number

<TACACSSRVRPRIO> is the priorty order of this TACACS+ server in the list of RADIUS and TACACS+ authentication servers configured in the node. Lowest Priority Server is tried first.

5.12.2 Configure SPDs so that RADIUS/TACACS+ traffic is carried by IPSEC

5.12.2.1 Configure an SPD for RADIUS to be carried by IPSEC

The following SPD should be entered to pass the RADIUS communications over an IPSEC SA:

```
add ipsec-spd-entry-ipsec/<peer>/radius priority 10 action protect
add ipsec-traffic-selector-ipsec/<peer>/radius/ts1 next-layer-protocol 17
add local-subnet-ipsec/<peer>/radius/ts1/<LOMGMTADDR>/32
add remote-subnet-ipsec/<peer>/radius/ts1/<RADIUSSRVRADDR>/32
add remote-ports-ipsec/<peer>/radius/ts1/all
add local-ports-ipsec/<peer>/radius/ts1/1812/1812
add ipsec-sa-proposal-ipsec/<peer>/radius1/1 dh-group <dheGroup> integrity-algorithm
  <integrityAlg>
add encryption-algorithm-ipsec/<peer>/radius1/1/<encryAlg>/<keylen>
```

5.12.2.2 Configure an SPD for TACACS+ to be carried by IPSEC

The following SPD should be entered to pass the TACACS+ communications over an IPSEC SA:

```
add ipsec-spd-entry-ipsec/<peer>/tacacsplus priority 10 action protect
add ipsec-traffic-selector-ipsec/<peer>/tacacsplus/ts1 next-layer-protocol 6
add local-subnet-ipsec/<peer>/tacacsplus/ts1/<LOMGMTADDR>/32
add remote-subnet-ipsec/<peer>/tacacsplus/ts1/<TACACSSRVRADDR>/32
add remote-ports-ipsec/<peer>/tacacsplus/ts1/all
add local-ports-ipsec/<peer>/tacacsplus/ts1/49
add ipsec-sa-proposal-ipsec/<peer>/tacacsplus/1 dh-group <dheGroup> integrity-
  algorithm <integrityAlg>
add encryption-algorithm-ipsec/<peer>/tacacsplus/1/<encryAlg>/<keylen>
```

5.13 Configure Remote Audit Logging

Remote Audit logs enable centralized event dashboards and event/action processing. The TOE supports remote SYSLOG feeds over TCP/UDP and should be configured in the NE using this command:

```
add syslog log-server <SYSLOGSRVR> address <SYSLOGADDR> transport tcp port 514
enabled true message-coalescence true
```

The following SPD should be entered to pass the syslog communications over an IPSEC SA:

```
add ipsec-spd-entry-ipsec/<peer>/syslog1 priority 1 action protect
add ipsec-traffic-selector-ipsec/<peer>/syslog1/ts1
  next-layer-protocol all
add local-subnet-ipsec/<peer>/syslog1/ts1/<LOMGMTADDR>/32
add remote-subnet-ipsec/<peer>/syslog1/ts1/<SYSLOGADDR>/32
add remote-ports-ipsec/<peer>/syslog1/ts1/all
add local-ports-ipsec/<peer>/syslog1/ts1/all
```

add ipsec-sa-proposal-ipsec/***<peer>***/syslog1/1 dh-group ***<dheGroup>*** integrity-algorithm ***<integrityAlg>***

add encryption-algorithm-ipsec/***<peer>***/syslog1/1/***<encryAlg>***/***<keylen>***

Again, for High Availability purposes, it is desirable for the TOE to have access to two or more SYSLOG servers. The second server would be configured using the same command, updating the traffic selector name and using the additional SYSLOG server's IP address for ***<SYSLOGADDR>***.

6 Certificate Revocation

This section provides the steps Security Administrator should follow if the connection cannot be established during the validity check of a certificate used in establishing a trusted channel

The TOE checks the validity of the certificates it receives from its peers (such as the certificate's extended key usage, expiration, revocation, basic constraints, and reference identifiers) as part of the authentication step of the IPsec. The TOE performs these checks on the peer's certificate before moving up the chain to check each intermediate CA. This is done because any certificate in the chain must be checked for revocation and basic constraints. The TOE will not authenticate using only a leaf certificate - full path resolution is always required. If a partial path is provided by the peer, the system will ask the peer for the missing certificates to resolve the path to a known root. If the peer does not provide them then the connection will be aborted. If the certificate is invalid, the TOE also rejects the connection attempt.

The TOE supports the following Certificate revocation methods: Certificate Revocation List, CRL Distribution Point (CDP) and Online Certificate Status Protocol (OCSP). OCSP and CRL revocation methods can be simultaneously enabled. If both methods are configured, then OCSP is used by default to query the Certificate revocation status. CRL will be used if a definite revocation status is not determined by the OCSP method. The TOE checks the IPsec peer's certificate revocation during the authentication step of a connection. The TOE checks each level of the certificate chain sent by the peer. If any certificate in the chain is revoked, the TOE will reject the connection attempt.

If the TOE cannot establish communications with the external server for OCSP revocation checks, then the TOE will not accept the certificate and will terminate the connection attempt with the peer and there will be no fall back to CRL-based revocation checking. If only CRL revocation checking is enabled and the TOE cannot establish communications with the external server, the TOE will not accept the certificate and will terminate the connection attempt. In this case, the Administrator should troubleshoot and resolve the issue before proceeding.

The TOE will perform Certificate verification when it receives a certificate from a peer or when a Certificate is installed. The TOE performs certificate revocation checking by communicating with an external server specified in the certificate’s AIA extension for OSCP or CDP extension for CRL.

6.1 Dealing with revoked certificates

The Security Administrator should review all certificates, starting at the leaf and progressing to the root certificate. Each certificate should be checked (for CA certificates) for a set Basic Constraints CAFlag and (for leaf certificates) applicableExtended Key Usage. Each certificate should be checked for signature validity. The system will log why a certificate was not accepted. The Security Administrator will need to work with the peer system’s Security Administrator to resolve any issues.

6.2 Certificate Revocation List (CRL)

CRL checking is not enabled by default. To enable CRL checking on the TOE, use the following command:

```
set security-policies crl-based-revocation true
```

CRLs contain the CA issuer and Serial Numbers for certificates that should be considered invalid.

The contents of the CRL will take effect immediately and matching certificates will not be recognized as valid.

6.3 Online Certificate Status Protocol (OCSP)

OCSP is a remote procedure protocol (RPC) used for obtaining the révocation status of an X.509 digital certificate. It must be enabled to avoid attempts to access unreachable OCSP servers when an AIA extension is received in a certificate. OCSP servers may be provided by a peer when it sends an X.509 certificate (using the AIA extension).

6.3.1 Enabling OCSP

To enable OCSP on the TOE,use the following command:

```
set security-policies ocsp-based-revocation true
```

7 Annex: Glossary

Masquerade – an attempt to gain unauthorized access to, or greater privilege to a system, by posing as an authorized user (e.g., using stolen logon ids and passwords). This may be done by replaying data or inserting false data that appears genuine into a communications path. System software and data may be deleted, disclosed, or corrupted. An example is the re-programming of NE software to insert malicious code to steal passwords.

Disclosure of information – data disclosed without authorization, either by deliberate action or by accident.

Message stream or data modification – data altered in some meaningful way by reordering, deleting or modifying it.

Denial of service – actions that prevent the NE from functioning in accordance with its intended purpose. A piece of equipment or entity may be rendered inoperable or forced to operate in a degraded state; operations that depend on timeliness maybe delayed.

Traffic analysis – a form of passive attack in which an intruder observes information being transmitted and makes inferences based on the volume of the traffic, end points of the traffic etc.

8 Annex: Assurance requirements

This section provides information to satisfy the assurance requirements in the named section.

8.1 AGD_OPE.1

The GX G42 TOE provides security functionality as required by NIAP NDcPP as well as additional functionality that is not in the NDcPP. This section lists the additional functionality that has not been tested for NDcPP compliance. This includes:

- The use of FTP, HTTP and SNMP
- The use of RADIUS, TACACS+, NTP and SYSLOG without configuring an IPSEC tunnel.
- The use of TLS1.3 cryptography.
- The use of IPv6
- The use of dial out server functionality
- The use of optical network communication
- The use of dial-out server

The system does not have any default passwords. The initial system password (stored and authenticated locally) is provided when the system is first powered on, either by the user connected to the console or from the DCHP Server Autoconfiguration function.

The cryptographic modules and functions performed in the testing of the TOE are:

- Intel OpenSSL, Strongswan and SNMP Crypto Libraries (Openssl with libSNMP and libIKE) Version 6.2 firmware. This OpenSSL library is used for IKEv2 key generation and negotiation as well as SSH and TLS cryptographic services including secret negotiation, authentication, key exchange, encryption/decryption, message authentication, hashing and DRBG.
- Intel Kernel IPsec Crypto Library Version 4.19.274 firmware. This Kernel IPsec library is used for IPsec encryption/decryption, message authentication and hashing.

WARNING: No other cryptographic modules were used in the testing of the TOE.

8.2 FAU_GEN.1

The GX G42 TOE provides auditing for all operations performed on the system, regardless of the interface used. This means that the auditing is done for commands entered at the serial interface, on SSH interactive sessions, SSH Netconf sessions, RESTCONF sessions and GRPC sessions.

The audit information is independent of the interface as the request is mediated from the interface form into the internal system YANG models.

See Annex 9 for audit logs generated by the system.

8.3 FAU_STG_EXT.1

The GX G42 TOE maintains an internal log as well as connects to an external system for log reporting. The interface to external systems is described in section **5.13** of the in this document. Log messages are generated by system functions and sent to all log recording points (local as well as remote) simultaneously. Each log message has timestamp and a message ID. If a connection to a remote log server is not available (e.g. due to lack of configuration, or a network issue), only an authorized administrator can view the local audit records and there are no interfaces via which the administrator can clear/delete or otherwise modify the contents of the local audit logs.

When the local audit storage is full, the TOE will overwrite the oldest audit records first using a FIFO (First in, First out) replacement mode performed via rotation of log files. The TOE retains 10 log files which are rotated when they exceed 30 MB. The log files are stored in a filesystem of 8.4GB with typically 3.0GB of available space. The TOE will issue a warning message when there is only 10% storage space remaining. The TOE will not allow configuration of a smaller rotation size or lower the number of log files to be retained.

8.4 FCS_CKM.4

The GX G42 TOE provides management facilities to request, create, validate, use and destroy keys. These facilities operate on:

- storage of the system database (AES-CBC 512bit keys)
- X.509 certificates (using 2048-, 3072- or 4096-bit RSA, p256, p384, p521 ECDSA keys)
- TLS session keys (AES-CTR (128, 192, 256 bit) and AES-GCM (128, 192, 256 bit) keys)
- SSH authentication (2048-, 3072- or 4096-bit RSA and p256, p384 or p521 bit ECDSA)
- SSH session keys (AES-CTR (128, 192, 256bit) and AES-GCM (128, 192, 256bit) session keys)
- shared keys (ASCII keys for RADIUS and TACACS sessions).

The destruction of individual keys as well as system zeroization is supported. The destruction process invokes internal operations that guarantee the destruction request has completed before the operation response is provided.

Zeroization is done by invoking the command:

```
fips zeroize
```

Zeroization affects all of the keys listed above, zeroing the keys. It also reboots the system.

8.5 FCS_RBG_EXT.1

When running in FIPS mode, only approved algorithms that have been CAVP tested are used, including the TOE's CAVP AES-256-CTR DRBG. There is no further configuration required for configuring RNG functionality.

ENTROPY-LOW Alarm

The G42 system is designed to identify the entropy low condition in the system that arises due to a dip in the entropy level below a pre-defined threshold (low amount of available Entropy bits). That is, when the amount of unused entropy bits in the entropy buffer is at or below threshold.

Following this condition, the ENTROPY-LOW alarm is reported on the system.

This condition is reported as a non-service affecting, major alarm, categorized as a security alarm on the specific card (line card or controller card) where the condition is seen.

To clear this alarm, wait for more entropy bits to be collected such that the amount of unused entropy bits in the entropy buffer is above the threshold. Ideally, the alarm must be cleared by the system in a couple of minutes after it is reported. If the alarm persists beyond a minute or two, contact Infinera Technical Assistance Center for further analysis and investigations.

Tip: Generation of entropy bits happens all the time in the system. However, they are consumed by applications that use random numbers. This includes key generation and establishing TLS sessions. Hold off on doing these operations to minimize the amount of entropy bits being consumed.

8.6 FTA_SSL.3

Automatic logout is performed based on inactivity of a remote session. For sessions that do not have long standing serial or network connections (such as RESTCONF), the session life is started with the start session action. The amount of inactivity time to trigger automatic logout is configured for each user.

To set the timeout for a user, use the following command:

```
set user-<user> timeout <minutes>
```

where ***<user>*** is the username and ***<minutes>*** has the range 0..1440 minutes.

8.7 FTA_SSL.4

The GX G42 TOE supports administrator shutdown of their own interactive sessions. They can log out of both local and remote CLI administrative sessions by issuing the ‘exit’ command and from the Web UI via the “logout” icon.

8.8 FTA_SSL_EXT.1

Local interactive sessions have inactivity timeouts. When an inactivity timeout has been exhausted, the session is disconnected. The timeout for a session is set using the command:

```
set system security user-<name> timeout <minutes>
```

Where <*name*> is the user name and <*minutes*> is the timeout value in minutes.

8.9 FTA_TAB.1

The GX G42 TOE supports an administrative banner that is displayed to users prior to completing login authentication. The banner is set using the command:

```
set system protocols ssh pre-login-message “<bannerMsgString>”
```

8.10 FCS_SSHS_EXT.1.8

The GX G42 TOE supports SSH re-keying, but does not support configuration of the re-keying thresholds. The thresholds are statically defined at 1hr and 1Gb of traffic exchanged. Re-keying will occur when either of these events are satisfied, and the timers/counters will be reset to 0 with the use of the new key.

8.11 FIA_UAU.7

The GX G42 TOE suppresses output when prompting a user to enter a password as a part of user authentication. This is the case as soon as the system is placed into FIPS mode. As a part of entering FIPS mode, the system configuration is zeroized and all password information needs to be re-entered.

When in FIPS mode, passwords are entered at the CLI for configuration, (e.g. as a part of adding users, as a part of transferring files to other systems). In these cases, the passwords are echoed as they are entered, but will be replaced with a string of three asterisks when the command is sent for execution (i.e. after enteing carriage-return).

8.12 FMT_MOF.1/ManualUpdate, FPT_TUD_EXT.1 and AGD_OPE.1

The GX G42 TOE supports administrator requested upgrade. A software release consists of a manifest file as well as a .tar.gz file. The manifest file and the .tar.gz file must have the same prefix and must be in the same directory. Only the manifest filename is used in the download command.

To determine the current version of software on the system use this command command:

```
swversion
```

This will return the running version on the active controller and on the backup controller.

The software update file is downloaded from the Infinera Customer Support Portal (https://support.infinera.com). Signature verification is performed when the image is uploaded to the TOE for both full software package upgrades and delta/patch upgrades. The file's digital signature is verified before it is saved to the TOE's flash. The TOE checks the update image integrity using ECDSA P-521 with SHA2-512. If the integrity verification fails, the TOE does not save the uploaded image to flash and the installation fails.

Once the file is verified successfully and saved to the flash, the administrator issues commands or performs actions via the Web UI to install and activate the image. The TOE will then reboot and will come up following the reboot with the newly installed version of the software.

To upgrade the software version, use this command:

download swimage source=***<url>*** password=***<password>***

where the ***<url>*** can use https, sftp or scp protocol uri and references the manifest file. URLs may contain login information and may look like:

```
scp://user@10.220.224.136:/home/user/FullPackage/ThanOS-F1.0-Main-2020.02.19_12_56pm.manifest
```

or

```
sftp://user@10.220.224.136:/home/user/FullPackage/ThanOS-F1.0-Main-2020.02.19_12_56pm.manifest
```

or

```
https://10.220.224.136:/home/user/FullPackage/ThanOS-F1.0-Main-2020.02.19_12_56pm.manifest
```

The ***<password>*** provided will be used if required by the file transfer protocol (i.e. for SFTP, SCP). This command will download the manifest and .tar.gz file to the GX G42 TOE. It will be verified but no further processing will be performed.

The download operation can be verified by the command:

```
show downloads
```

If the download was not successful, the manifest will not be visible.

After this command is executed, the next command to execute is:

prepare-upgrade apply manifest=***<manifest file name>***

This will cause the manifest file and .tar.gz to be extracted. If an error occurs, it will be noted on the manifest file, visible using the command:

```
show sw-management
```

The final command to be executed is:

activate swimage db-action=***<db-action>***

The <*db-action*> can be: empty-db, upgrade-db, rollback-db or auto. Normally, the db-action would be upgrade-db.

8.13 FMT_SMR.2

A new user is added using the following command:

add user-***<username>*** password ***<password> <user-attributes>***

where <user-attributes> defines a number of different attributes for the new user. These attributes include “user-groups” which associate a user with one or more “roles”. The Administrator account is broken into three roles in non-FIPS operations: Encryption Administrator, System Administrator and Network Administrator. In FIPS operation, which is required by NIAP operation, an administrator must have all three roles (i.e. must be in all three user-groups). This is done using the user-group attribute. Here is an example command setting that attribute:

add user-newuser password ***<password>*** user-group EA,NA,SA

The TOE allows administrators to configure a minimum password length for users that is between 8 and 200 characters. Along with upper and lower case letters and numbers, the TOE allows the following special characters: [*'!', '@', '#', '$', '%', '^', '&', '*', '(', ')'* ***[and additional special characters: <sp>*** ~ _ - + = ` | { } " [ ] : ; < > , . ? / ' \ ***]***]. The TOE provides obscured feedback to the administrative user while the authentication is in progress at the local console. The TOE can be configured with either a local database or a remote RADIUS or TACACS+ database for authenticating users.

To configure the TOE to require a minimum password length, use this command:

set system security security-policies minimum-password-length ***<minCharLength>***

where ***<minCharLength>*** would be in the recommended range of 15 and 200 with passwords having no less than a minimum of 15 characters in length.

To change a password, use the command:

set user-***<Login>*** password ***<password>***

As stated above, the password must conform with the composition requirements stated above.

8.14 FPT_TST_EXT.1

The GX G42 TOE performs self-tests at system startup. These tests include **pair-wise consistency tests, KDF tests and software integrity test** and Cryptographic known answer tests. These tests are all performed as a part of the boot process and failures of any test are noted by an alarm being raised. To view TOE alarms, use this command:

show alarm

If the TOE is in FIPS error, the TOE will reboot and will not re-establish its network connection. In this case, the only way to query TOE alarms or view logs is via the serial console using a locally authenticated account.

To attempt clearing the fips-error condition, the SA needs to manually attempt a self-test. This is done using the TOE command:

fips self-test

This will cause the TOE to reset and execute the self-test. When it is complete, the TOE will either be out of fips-error (and operational) or will be in fips-error again. If it persists in fips-error, the TOE will need to be RMAed.

8.15 FTP_ITC.1.3

The GX G42 TOE supports the use of IPSEC for inter-TSF trusted channel communications. The operations to establish a channel are:

1. If X.509 is being used for certificate based authentication, load the X.509 certificate for local identity and the remote certificate's trust chain (see example in Section 5.10.2)
2. Establish the IPSEC Peer relationship (i.e. IPSEC SA) (see example in Section 5.10.3)
3. Establish the SPD and traffic filter for the IPSEC Child SA (see example in Section 5.12.2.1)

If an IPSEC connection fails, the status can be found by reviewing the SYSLOG for IPSEC. This is done with the following command:

```
show log security
```

To attempt a reconnect of an IPSEC session, use the following pair of commands:

```
set ikev2-peer-<ipsecPeer>/<ikev2peername> admin-state lock
set ikev2-peer-<ipsecPeer>/<ikev2peername> admin-state unlock
```

If a SYSLOG session fails, the syslog connection should be reattempted. This is done by disabling and re-enabling syslog using the following commands:

```
set log-server-<name> enabled false
set log-server-<name> enabled true
```

If a TACACS+ or RADIUS server session fails, the TACACS+ or RADIUS adjacency will need to be re-established using the following commands:

```
set aaa-server-<servername> enabled false
set aaa-server-<servername> enabled true
```

8.16 FTP_TRP.1.3/Admin and FIA_UIA_EXT.1

For a serial terminal, connect to the serial interface a terminal operating at 15200 bps, 8bits, no parity, 1 stop bit.

For SSH, establish an SSH session to the GX G42 TOE's IP address, TCP port 22. For NETCONF, establish an SSH session to the GX G42 TOE's IP address, TCP port 830. For RESTCONF, establish a HTTPS session to the GX G42 TOE's IP address, TCP port 8181.

The SSH and NETCONF sessions will negotiate the cryptographic algorithms used for their session from the algorithms configured on the client and the GX G42 TOE. For RESTCONF, the negotiation is done based on the TLS1.2 algorithms configured on the client and the GX G42 TOE.

The Pre-login banner is conveyed on the serial terminal and SSH sessions prior to performing authentication.

All remote administration of the TOE takes place over a secure communication path between the remote administrator and the TOE using either an SSHv2 client or a web browser.

SSH Client – The remote administrator uses an SSH client to access the CLI and the NETCONF API over a secure, encrypted SSHv2 session.

Web browser – The remote administrator uses a web browser to access the Web UI and the RESTCONF API over a secure HTTPS/TLS connection.

8.17 FCS_SSHS_EXT.1

The GX G42 TOE supports SSH session key aging. The session key is aged based on the amount of elapsed time or amount of data exchanged. The session limits are static and occur when 1) 24 hours of time or 2) 1Gb of data has been exchanged.

8.18 FCS_IPSEC_EXT.1.13

The GX G42 TOE supports IPSEC authenticated by Pre-Shared Keys as well as X.509 certificates. All of the examples provided so far have been using X.509 certificates. This section provides information for Pre-Shared Keys.

The IPSEC objects are shared for X.509 authentication and for Pre-shared-key authentication. As a result many of the objects will be familiar. The main different is in the configuration of the peer. All object operations are included in this description.

1. Create IPSEC peer association with the following command:

   ```
   add ikev2-peer-ipsec/<peer> destination <ipAddress> authentication-scheme pre-shared-key pre-shared-key-type ascii psk-ascii <pskString> local-identity ‘<localSystemName>’ local-identity-type fqdn peer-identity ‘<peerSystemName>’ peer-identity-type fqdn
   ```

2. Create IPSEC SA proposal with the following commands:

   ```
   add ike-sa-proposal-ipsec/<peer>/<proposalID> dh-group dhe-2048 integrity-algorithm hmac-sha2-384-912

   add encryption-algorithm-ipsec/<peer>/<proposalID>/<encryptAlg>/<keyLength>
   ```

3. Create traffic SPD with the following commands:

   ```
   add ipsec-spd-entry-ipsec/<peer>/<spdID> priority <priority> action protect
   ```

4. Associate Traffic Selectors with SPD

   ```
   add ipsec-traffic-selector-ipsec/<peer>/<spdID>/<traffSelID> next-layer-protocol <protocolNum>

   add local-subnet-ipsec/<peer>/<spdID>/<traffSelID>/<ipv4addr>/<ipv4addrLen>

   add remote-subnet-ipsec/<peer>/<spdID>/<traffSelID>/<ipv4addr>/<ipv4addrLen>

   add local-ports-ipsec/<peer>/<spdID>/<traffSelID>/all

   add remote-ports-ipsec/<peer>/<spdID>/<traffSelID>/<startPort>/<stopPort>
   ```

5. Create IPSEC SA proposals and encryption

   ```
   add ipsec-sa-proposal-ipsec/<peer>/<spdID>/<proposalID> dh-group dhe-3072 integrity algorithm hmac-sha2-384-192

   add encryption-algorithm-ipsec/<peer>/<spdID>/<proposalID>/<encryptAlg>/keyLength>
   ```

8.19 FCS_IPSEC_EXT.1.7

The GX G42 TOE supports automatic IKE re-keying based on the amount of time the session has been operating. The specific limits that trigger re-keying may be lower in reality so the re-keying process can be completed in-time. For example, the IKE re-keying time limit may need to be set to 23hr45 minutes so it is completed within 24 hours.

Setting the rekeying thresholds for an existing IKE peer is done with the following command:

```
set ikev2-peer-ipsec/<peer> re-key-frequency <seconds>
```

8.20 FCS_IPSEC_EXT.1.8

The GX G42 TOE supports automatic IPSEC Child SA re-keying based on 1) the amount of time, and 2) the amount of data. As with the IPSEC SA rekeying, the specific limits that trigger re-keying may be lower in reality so the re-keying process can be completed in time.

Setting the rekeying thresholds on an SPD based on time and bytes is done with the following commands:

add ipsec-sa-re-key-ipsec/***<peer>***/***<trafficSelector>*** frequency ***<seconds>***

add ipsec-sa-re-key-ipsec/***<peer>***/***<trafficSelector>*** bytes ***<integer>***

Note: The SA re-key time must be less than the supporting IKE peer re-key time.

8.21 FCS_IPSEC_EXT.1.14

The GX G42 TOE supports a number of types of identifiers for IPSEC authentication. The supported identifier types are: ipv4 address, fqdn, and X.509 DN. This is configured per peer, in the peer-identity-type attribute.

When X.509 certificate authentication is used, certificates may be presented with and without SAN extensions. When SAN extensions are used, it is expected the SAN contain an identifier consistent with the configured identifier. This may be an ipv4 address, ipv6 address or a DNS name. For a DNS name, it is expected that it is resolvable to the IP address sending the certificate. When SAN extensions are not used, the NE will fall back to verifying the certificate’s Subject field contains the Distinguished Name expected from the peer.

9 Annex: Audit Generation

The following file contains evidences of Audit log entries issued by the GX G42 for different events:

FAU_GEN1.xlsx