NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5

Common Criteria Admin Guide

Document Version: **1.0**
Date: **May 15, 2023**

NOKIA INC.
600 March Rd,
Kanata,
ON K2K 2T6
Canada

Document Created by:

intertek acumen security
2400 Research Blvd
Suite 395
Rockville, MD 20850
USA

Table of Contents

1 Introduction 5
1.1 Document References 5
1.2 Common Criteria Certified Models 5
1.3 Common Criteria Evaluated Configuration 6
1.3.1 Product functionality not included in the scope of the evaluation 6
1.3.2 Administering the device 6
2 CC Certified Firmware Installation 7
2.1 Secure Delivery 7
2.2 Physical Security 7
2.3 Device Installation 7
3 Administration using local console and SSH 8
3.1 Accessing the CLI 8
4 FIPS-140-2 Mode of Operation 10
5 Firmware Installation 12
5.1 Performing Manual Software Updates on the Nokia SAR 7705 12
5.2 Updating the Boot Options 12
5.3 Rebooting the device 13
5.4 Verifying the Updated Image Version 13
5.5 Issues that may affect successful boot of device/ firmware 13
6 Authentication 14
6.1 Password Management 14
6.2 Authentication using RADIUS server 17
6.3 Authentication using TACACS server 20
6.4 Configure SSH Public Keys 22
7 Cryptographic Protocols 24
7.1 SSH 24
7.1.1 SSH server cipher algorithm configuration 24
7.1.2 SSH key-exchange configuration for Diffie-Hellman keys 25
7.1.3 Message Authentication Code algorithm configuration for SSHv2 25
7.1.4 Configuring SSH Rekey 27
7.2 IPSec 29
7.2.1 IPSec Security Policy, IKE Policy, and IPSec Transform 29
7.2.2 Internet Key Exchange (IKE) and Transform Commands 29
8 Logging Configuration 39
8.1 Memory Logs 39
8.2 Log Configuration 39
9 Using a Secure Audit Server 41
9.1 Prerequisites 41
9.2 Audit Server Requirements 41
9.3 Configure Nokia SAR 7705 to communicate with an Audit Server 41
9.4 Syslog Commands 42
9.5 Auditable Events 44
9.5.1 Format 44

9.5.2 Audit Events 44
10 X.509 Certificates 55
11 Setting Time 62
12 Acronym Table 63

Revision History

Version	Date	Description
1.0	May 15, 2023	Initial Release

1 Introduction

This document is intended to be an addendum to the other administrative guidance documents for Nokia 7705 SAR Series with SAR OS 21.10R5. The Nokia 7705 SAR Series with SAR OS 21.10R5 conforms to the Common Criteria Network Device Protection Profile v2.2e. The information contained in this document is intended for Administrators who would be responsible for the configuration and management of the Nokia 7705 SAR Series with SAR OS 21.10R5 in the Common Criteria evaluated configuration.

1.1 Document References

The security administrators should refer to the following documents when configuring the certified Nokia 7705 SAR series devices with SAR OS 21.10R5:

- Nokia 7705 SAR Series with SAR OS 21.10R5 Security Target, version 1.2, 16th May 2023.
- 7705 SAR-OS SAR-18/8/X/Ax/Wx/W/H/Hc Data Plane Cryptographic Module (SARDCM), FIPS 140-2 Non-Proprietary Security Policy, version 1.8, December 12, 2022.
- NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R1 Basic System Configuration Guide, Edition 01, October 2021
- NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R1 Interface Configuration Guide, Edition 01, October 2021
- NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R1 Log Events Guide, Edition 01, October 2021
- NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R1 Router Configuration Guide, Edition 01, October 2021
- NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R1 Services Guide, Edition 01, October 2021
- NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R1 System Management Guide, Edition 01, October 2021

Note: The above admin guides for release 21.10R1 are all applicable to the CC certified software version 21.10R5.

1.2 Common Criteria Certified Models

The following models of the Nokia 7705 Service Aggregation Router (SAR) series with SAR OS 21.10R5 are certified:

- Nokia 7705 SAR-18,
- Nokia 7705 SAR-8,
- Nokia 7705 SAR-X,
- Nokia 7705 SAR-H,
- Nokia 7705 SAR-W,
- Nokia 7705 SAR-Wx,
- Nokia 7705 SAR-Hc,
- Nokia 7705 SAR-Ax

Versions of the Nokia 7705 SAR models differ in form factor, networking capacity, and processing capacity.

1.3 Common Criteria Evaluated Configuration

1.3.1 Product functionality not included in the scope of the evaluation

The following product functionality is not included in the CC evaluation:

- FTP and Telnet and are disabled.
- NTP is not used.
- TACACS+ cryptographic protection of the sessions is not covered by the evaluation but the security of TACACS+ relies on IPsec between the Nokia SAR 7705 and the AAA Server.
- MPLS and SNMP are not included in the scope of the evaluation.
- MACsec functionality is not supported.

NOTE:

The CC evaluated configuration does not prevent administrators/users from using the above features that were not evaluated. However, using these features may result in the Nokia SAR 7705 device be not strictly in compliance with the Security Target.

1.3.2 Administering the device

It is expected that the devices that are intended to be used in the CC evaluated configuration are administered only by trusted security hosts/administrators. Instructions on how to configure trusted administrators can be found in the “System Management Guide”.

2 CC Certified Firmware Installation

2.1 Secure Delivery

The Nokia SAR 7705 devices are delivered via commercial carrier (i.e., FedEx, UPS, Expeditors etc.) by Nokia or Nokia commercial partners. The package will contain a packing slip with the serial numbers of all shipped devices. The receiver must verify that the hardware serial numbers match the serial numbers listed in the packing slip. The receiver must examine the external packaging to see if the secure tape sealing is not tampered or damaged. In addition, the receiver must also examine the internal packaging, the unit sealing, and warranty sealing is intact. If any concerns are raised during the integrity verification process of the unit, the supplier should be contacted immediately.

2.2 Physical Security

To comply with the Common Criteria operation requirements, it is expected that the physical Nokia SAR 7705 units are installed in a secure location where the physical access is restricted to authorized operators.

2.3 Device Installation

The administrators are required to refer to the specific model specific hardware guidance supplements and the above referenced administrative guides for installation. These documents provide guidance on physical installation and initial configuration of the unit.

3 Administration using local console and SSH

Before beginning this procedure, ensure that:

1. The Nokia 7705 SAR Series with SAR OS 21.10R5 node has been installed and provisioned with an IP address and gateway for the management network interface. The node must be connected to the management network.
2. A terminal emulator application (for example, PuTTY) has been installed on your PC, and the terminal emulator is running.

3.1 Accessing the CLI

There are two ways to access management of the 7705 SAR:

• Console connection

• SSH connection

To access the CLI and configure the software for the first time, follow these steps:

1. Ensure that the CSM is installed and power to the chassis is turned on. The 7705 SAR software then automatically begins the boot sequence.

2. When the boot loader and BOF image and configuration files are successfully located, establish a router connection (console session).

- Assign a name to the device using the following command:

  ```
  *A:SR-xx# configure system name <system-name>
  ```

- Assign the IP address to the management interface using the following command:

  ```
  *A:SR-xx# bof address <ip-prefix/ip-prefix-length>"active"
  ```

To establish a console connection:

Step 1. Connect the terminal to the Console port on the front panel using the serial cable.

Step 2. Power on the terminal.

Step 3. Establish the connection by pressing the <Enter> key a few times on your terminal keyboard.

Step 4. At the router prompt, enter the login and password.

The default login is admin.

The default password is admin.

To disconnect from a console session, use the following command:

- **logout**

  Syntax: logout

  Context: <global>

  Description: This command logs out of the router session. When the logout command is issued from the console, the login prompt is displayed and any log IDs directed to the console are

discarded. When the console session resumes (regardless of the user), the log output to the console resumes.

SSH Access:

1. Open the terminal emulator on your PC. Specify the IP address of the device that you want to connect. If this is the first time anyone has connected to the device from a terminal using SSH, you are prompted to add the device to your known hosts list.

2. Enter the username of the default user account: `<username>`

3. Enter password of the default user account: `<password>`

To disconnect from an SSH session, use the following commands:

- **logout**

  Syntax: logout

4 FIPS-140-2 Mode of Operation

Once the firmware is installed and the administrators are able to access the device, FIPS mode must be enabled. The 7750 SAR includes a configurable parameter in the bof.cfg file to make the node run in FIPS-140-2 mode.

To support the implementation of FIPS-140-2, the TiMOS software image contains an HMAC-SHA-256 secret key that is verified upon boot-up. When FIPS-140-2 is enabled on the node, an HMAC-SHA-256 integrity check is performed during the loading of the both.tim file to ensure that the calculated HMAC-SHA-256 secret key of the loaded image matches that stored in the hmac-sha256.txt file. This is a signature file that has been added to the TiMOS software image and only applies to FIPS-140-2.

Note: *The hmac-sha256.txt file must be stored in the same directory as the TiMOS image.*

If the image fails the HMAC-SHA-256 check, the node does not boot up, an error message is displayed, and the node tries to reboot the load after a delay of 60 s. The node keeps trying to reboot until the operator cancels the reboot. If the software image is verified by the HMAC-SHA-256 check, the node boots up normally and a message indicating that the software load has passed verification is displayed.

The node performs its normal boot-up sequence, including reading the config.cfg file and loading the configuration. The config.cfg file that is used to boot the node in FIPS-140-2 mode must not contain any configuration that is not supported by the FIPS-140-2 implementation. If such a configuration is present in the config.cfg file when the node boots up, the node loads the config.cfg file until the unsupported configuration is reached and then stops. A failure message is also displayed.

When the node boots in FIPS-140-2 mode, Cryptographic Module Validation Program (CMVP) startup tests are executed on the CSM and applicable data plane. CMVP conditional tests, such as manual key entry tests, pairwise consistency checks, and RNG tests, are executed when required during normal operation.

To enable FIPS-140-2 at the console, follow the steps below:

```
*A:SARX# bof fips-140-2

*A:SARX# bof save
```

To reboot the device, use the following command:

```
*A:SARX# admin reboot now
```

Note*: The Nokia SAR 7705 runs the power-on process and must display "FIPS-140-2 Power-On-Self-Test Passed" after the completion of the reboot.*

After a successful Integrity Check, the Nokia SAR 7705 displays a successful match as shown below:

```
FIPS-140-2 HMAC-SHA256 software load verification passed
```

The FIPS Power on self-test should pass successfully. Upon successful self-test cycle, the Nokia SAR 7705 should display the following result:

```
FIPS-140-2 Power-On Self-Test started

FIPS-140-2 Power-On Self-Test passed

FIPS-140-2 startup selftests passed
```

Note: *If the self-tests fail and the problem remains persistent, please contact Nokia technical assistance.*

Once the FIPS mode is enabled, continue to the firmware installation.

5 Firmware Installation

The Common Criteria validated firmware version is SAR OS 21.10R5.

The Nokia SAR 7705 device is shipped with a software pre-installed on it. The security administrators will have to manually download and install the certified firmware securely. Software updates are available for download from the Nokia website. When software updates are available via the https://www.nokia.com/ website, customers can obtain, manually verify the hash integrity, and install the updates.

The firmware comes with a hmac-sha256 hash file which is used to check the integrity during the firmware update process. If the hash file is missing or corrupted, or do not match, the firmware integrity verification fails, and the update fails.

5.1 Performing Manual Software Updates on the Nokia SAR 7705

To upgrade the firmware, the Administrator first connects to the update server using SFTP and downloads the firmware upgrade to a Compact Flash (CF) device. The upgrade is protected by a HMAC-SHA-256 value which is computed by the developer in the development environment and stored in a separate file.

The Nokia SAR OS uses a Boot Options File (BOF) for indicating to the boot loader the location of the firmware files. Typically, the Administrator stores the firmware upgrade on a CF and modifies the BOF to point to the software on the CF. This does not need to be performed immediately after downloading the software upgrade. The Administrator may time the actual upgrading at a convenient time.

When rebooting the device with the modified BOF, the device upgrades the software from the source pointed to by the BOF. When in the FIPS mode, the boot loader searches for the hash file containing the HMAC-SHA-256 value of the firmware in the same location as the software image. When the HMAC file is found, the Nokia SAR 7705 computes a HMAC value of the image and compares it to the value on the HMAC file. If the values match, the device continues with the boot up. If the HMAC file is not found or the comparison fails, the boot loader reboots the system.

Determine the current version by running the following command:

```
*A:SARX# show version
```

Note: *To perform a manual update, administrator must have a console connection to the device. Prior to performing manual software update, confirm all running configuration are saved.*

To save any configuration, run the following the command:

```
*A:SR-xx# /admin save

*A:SR-xx# /bof save
```

5.2 Updating the Boot Options

To update the boot options file (bof) with the new image file, follow the steps below:

```
*A:SR-xx# bof

*A:SR-xx >bof# primary-image cf3:\filename\

*A:SR-xx >bof# save
```

5.3 Rebooting the device

```
*A:SR-xx# /admin reboot now
```

Note: *The BOF must be located on the same compact flash drive as the boot.ldr file.*

Updating the settings during the boot up

To update the settings during the boot sequence, first halt the boot sequence and then follow the steps below:

1. Type "sros" and hit ENTER within 18 seconds to begin changing parameters: sros
2. Press ENTER to begin
3. Update the Software Image URL to cf3:\filename\
4. Enter "no" when prompted to enable auto-discovery
5. Press ENTER to keep the existing Config URL
6. Press ENTER to keep the existing fips-140-2 configuration
7. Enter “yes” to overwrite cf3:/bof.cfg with the new settings
8. Use the **/bof save** command to save the new image file after logging into the device.

Once the new config setting is successfully saved, the new image file from the primary-image location is loaded.

5.4 Verifying the Updated Image Version

After the successful completion of the image update, login as an authorized Security Administrator and check the image version as below:

```
*A:SR-xx# show version
```

5.5 Issues that may affect successful boot of device/ firmware

There may be instances where the device ends up not booting correctly. It can be a result of firmware failure, a POST test failure, or other product software or hardware related issues. The administrators are advised to refer to the available official administrative guidance documents to look for solutions and if the issues are not resolved, contact Nokia support.

6 Authentication

Creating a user account

To create a local user account, use the command:

```
*A:SR-xx# config system security user <user-name>
```

Deleting a user account

To delete a local user account, use the command:

```
*A:SR-xx# config system security no user <user-name>
```

6.1 Password Management

Passwords can be composed of any combination of upper and lower case letters, numbers, and special characters that include: **[“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [".", "_", "+"]**

Minimum password lengths shall be configurable to 6 to 50 characters. The minimum password length is 6 characters. The Nokia SAR 7705 only supports the creation of strong passwords.

- To create a user account and set the password use the following command:

  ```
  *A:SR-xx# configure system security user <username>
  ```

  Note: *The username cannot be more than 32 characters.*

  ```
  *A:SR-xx# configure system security user <username> password <password>
  ```

  Note: *The plaintext password length cannot be more than 56 characters.*

- To set the minimum password length of six (6), use the following command:

  ```
  *A:SR-xx# configure system security password complexity-rules minimum-length 6
  ```

Password Management and Login Control Commands

- **password-options**
  Syntax: password-options
  Context: show>system>security
  Description: This command displays configured password options.

- **password**
  Syntax: password [password]
  Context: config>system>security>user
  Description: This command configures the user password for console access. Passwords must be enclosed in double quotes (" ") at the time of password creation if they contain any special characters (#, $, spaces, etc.). The double quote character (") is not accepted inside a password.

It is interpreted as the start or stop delimiter of a string. The password is stored in an encrypted format in the configuration file when specified.

Parameters: password — the password that must be entered by this user during the login procedure. Passwords can be composed of any combination of upper and lower case letters, numbers, and special characters that include: **[“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [".", "_", "+"]**

The minimum length of the password is determined by the minimum-length command. The maximum length is as follows:
• 56 characters if in unhashed plain text
The unhashed plain text form must meet all the requirements that are defined within the complexity-rules command context.
• 60 characters if hashed with bcrypt
• from 87 to 92 characters if hashed with PBKDF2 SHA-2
• from 131 to 136 characters if hashed with PBKDF2 SHA-3

- **complexity-rules**
  Syntax: complexity-rules
  Context: config>system>security>password
  Description: This command enables the context to configure security password complexity rules.

- **minimum-length**
  Syntax: minimum-length value
  no minimum-length
  Context: config>system>security>password>complexity-rules
  Description: This command configures the minimum number of characters required for passwords. If multiple minimum-length commands are entered, each command overwrites the previously entered command. The no form of the command reverts to the default value.
  Default: 6
  Parameters: value — the minimum number of characters required for a password
  Values: 6 to 50

- **attempts**
  Syntax: attempts *count* [time *minutes1*] [lockout *minutes2*]
  no attempts
  Context: config>system>security>password
  Description: This command configures a threshold value of unsuccessful login attempts allowed in a specified time frame.
  If the threshold is exceeded, the user is locked out for a specified time period.
  If multiple attempts commands are entered, each command overwrites the previously entered command.
  The no attempts command resets all values to the default.
  Default: count: 3
  minutes1: 5
  minutes2: 10
  Parameters: count — the number of unsuccessful login attempts allowed for the specified time. This is a mandatory value that must be explicitly entered.
  Values: 1 to 64

minutes1 — the period of time, in minutes, that a specified number of unsuccessful attempts can be made before the user is locked out
Values: 0 to 60
minutes2 — the lockout period, in minutes, where the user is not allowed to log in
Values: 0 to 1440
When the user exceeds the attempted count times in the specified time, then that user is locked out from any further login attempts for the configured time period.

- **lockout**
  Syntax: lockout all
  lockout user *user-name*
  Context: admin>clear
  Description: This command clears a security lockout for a specific user, or for all users, after they have been locked out for failing too many login attempts.
  Parameters all — clears lockouts for all users
  name — specifies a user name

- **pre-login-message**
  Syntax: pre-login-message *login-text-string* [name]
  no pre-login-message
  Context: config>system>login-control
  Description: This command creates a message displayed prior to console login attempts on the console. Only one message can be configured. If multiple pre-login messages are configured, the last message entered overwrites the previous entry. The system name can be added to an existing message without affecting the current pre-login message.The no form of the command removes the message.
  Default: no pre-login-message
  Parameters: login-text-string — a text string, up to 900 characters. Any printable, 7-bit ASCII characters can be used. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

- **login-banner**

  Syntax: [no] login-banner

  Context: config>system>login-control

  Description: This command enables or disables the display of a login banner. The login banner contains the 7705 SAR copyright and build date information for a console login attempt.

  The no form of the command causes only the configured pre-login-message and a generic login prompt to display.

- **idle-timeout**

  Syntax: idle-timeout {*minutes* | disable}
  no idle-timeout

  Context: config>system>login-control

  Description: This command configures the idle timeout for console and SSH sessions before

the session is terminated by the system. By default, each idle console or SSH session times out after 30 minutes of inactivity. The no form of the command reverts to the default value.

Default: 30

Parameters: minutes — the idle timeout in minutes

Values: 1 to 1440

disable — when the disable option is specified, a session will never time out. To re-enable idle timeout, enter the command without the disable option.

6.2 Authentication using RADIUS server

Using IPSec tunnelling to secure communication between the device and the RADIUS Server.

- The communication between the RADIUS Server and the Nokia SAR devices must be protected by using IPSec tunnels. IPSec tunnel configuration steps can be found in section 7.2 below.
- If the IPsec connections used by the Nokia SAR 7705 device is unintentionally broken, the security administrator needs to restart the connection, or the device will try to re-connect with the authentication server.

Commands

- **radius**

  Syntax: [no] radius

  Context: config>system>security

  Description: This command enables the context to configure RADIUS authentication on the 7705 SAR. For redundancy, multiple server addresses can be configured for each 7705 SAR. The no form of the command removes the RADIUS configuration.

- **accounting**

  Syntax: [no] accounting

  Context: config>system>security>radius

  Description: This command enables RADIUS accounting. The no form of this command disables RADIUS accounting.

  Default: no accounting

- **accounting-port**

  Syntax: accounting-port *port*

  no accounting-port

  Context: config>system>security>radius

  Description: This command specifies a UDP port number on which to contact the RADIUS server for accounting requests.

  Parameters: *port* — specifies the UDP port number

  Values: 1 to 65535

  Default: 1813

- **authorization**

  Syntax: [no] authorization
  Context: config>system>security>radius
  Description: This command configures RADIUS authorization parameters for the system.
  The no form of this command disables RADIUS authorization for the system.
  Default: no authorization

- **port**

  Syntax: port *port*
  no port
  Context: config>system>security>radius
  Description: This command configures the TCP port number to contact the RADIUS server.
  The no form of the command reverts to the default value.
  Default: 1812 (as specified in RFC 2865, Remote Authentication Dial In User Service (RADIUS))
  Parameters: *port* — the TCP port number to contact the RADIUS server
  Values: 1 to 65535

- **retry**

  Syntax: retry *count*
  no retry
  Context: config>system>security>radius
  Description: This command configures the number of times the router attempts to contact the RADIUS server for authentication if there are problems communicating with the server. The no form of the command reverts to the default value.
  Default: 3
  Parameters: *count* — the retry count
  Values: 1 to 10

- **server**

  Syntax: server *server-index* address *ip-address* secret *key* [hash | hash2]
  no server server-index
  Context: config>system>security>radius
  Description: This command adds a RADIUS server and configures the RADIUS server IP address, index, and key values. Up to five RADIUS servers can be configured at any one time. RADIUS servers are accessed in order from lowest to highest index for authentication requests until a response from a server is received. A higher-indexed server is only queried if no response is received from a lower-indexed server (which implies that the server is not available). If a response from a server is received, no other RADIUS servers are queried. It is assumed that there

are multiple identical servers configured as backups and that the servers do not have redundant data. The no form of the command removes the server from the configuration.

Default: no RADIUS servers are configured

Parameters: *index* — the index for the RADIUS server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from lowest to highest index.

Values: 1 to 5

ip-address — the IP address of the RADIUS server. Two RADIUS servers cannot have the same IP address. An error message is generated if the server address is a duplicate.

- **timeout**

Syntax: timeout *seconds*

no timeout

Context: config>system>security>radius

Description This command configures the number of seconds the router waits for a response from a RADIUS server. The no form of the command reverts to the default value.

Default: 3

Parameters: seconds — the number of seconds the router waits for a response from a RADIUS server, expressed as a decimal integer

Values: 1 to 90

- **use-default-template**

Syntax: [no] use-default-template

Context: config>system>security>radius

Description: This command specifies whether the user template defined by this entry is to be actively applied to the RADIUS user.

Default: no use-default-template

- **<u>Example of configuration steps required to have a secure IPsec connection with the RADIUS server:</u>**

A:SARX# configure system security radius
A:SARX>config>system>security>radius$ info detail
---

authorization
accounting
retry 3
timeout 60
port 1812
accounting-port 1813
use-default-template
access-algorithm direct

```
        server 1 address 10.1.12.1 secret "xp95xk5zK1YnUrABq6x0Zg4rTHvXGqjAsW8=" hash2
        no shutdown
-----------------------------------------------
```

Note: *In order to recover from a broken connection, restart the IPSec tunnel.*

6.3 Authentication using TACACS server

Using IPSec tunnelling to secure communication between the device and the TACACS+ Server.

- The communication between the TACACS+ Server and the Nokia SAR devices must be protected by using IPSec tunnels. IPSec tunnel configuration steps can be found in section 7.2 below.
- If the IPsec connections used by the Nokia SAR 7705 device is unintentionally broken, the security administrator needs to restart the connection, or the device will try to re-connect with the authentication server.

Commands

- **tacplus**

  Syntax: [no] tacplus

  Context: config>system>security

  Description: This command enables the context to configure TACACS+ authentication on the 7705 SAR. For redundancy, multiple server addresses can be configured for each 7705 SAR.

  The no form of the command removes the TACACS+ configuration.

- **authorization**

  Syntax: [no] authorization

  Context: config>system>security>tacplus

  Description: This command configures TACACS+ authorization parameters for the system.

  Default no authorization.

- **server**

  Syntax: server *index* address *ip-address* secret *key* [hash | hash2] [port *port*]

  no server index

  Context: config>system>security>tacplus

  Description: This command adds a TACACS+ server and configures the TACACS+ server IP address, index, and key values. Up to five TACACS+ servers can be configured at any one time. TACACS+ servers are accessed in order from the lowest index to the highest index for authentication requests. The no form of the command removes the server from the configuration.

  Default: no TACACS+ servers are configured

  Parameters: *index* — the index for the TACACS+ server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from the lowest index to the highest index.

  Values: 1 to 5

ip-address — the IP address of the TACACS+ server. Two TACACS+ servers cannot have the same IP address. An error message is generated if the server address is a duplicate.
port — the port ID
Values: 0 to 65535

- **timeout**

Syntax: timeout *seconds*
no timeout
Context: config>system>security>tacplus
Description: This command configures the number of seconds the router waits for a response from a TACACS+ server.The no form of the command reverts to the default value.
Default: 3
Parameters: *seconds* — the number of seconds the router waits for a response from a TACACS+ server, expressed as a decimal integer
Values: 1 to 90

- **use-default-template**

Syntax: [no] use-default-template
Context: config>system>security>tacplus
Description: This command specifies whether the user template defined by this entry is to be actively applied to the TACACS+ user.

- **Example of configuration steps required to have a secure IPsec connection with the TACACS server:**

```
A:SARX>config>system>security# tacplus
A:SARX>config>system>security>tacplus$ info detail
----------------------------------------------
 no accounting
 authorization
 timeout 90
 use-default-template
 server 1 address 10.1.12.1 secret "we0rmgIAiF4gcGPLccC6hGwNzOSn4H79ZQ==" hash2  port 49
 no shutdown
----------------------------------------------
```

Note: *In order to recover from a broken connection, restart the IPSec tunnel.*

6.4 Configure SSH Public Keys

The Nokia SAR 7705 restricts the ability to manage SSH (session keys) to security administrators via command line. The Security Administrator can modify, generate, and delete the key for SSH.

Use the commands in this section to create a new public key for SSH user authentication. The public key can be used instead of the password to authenticate the remote user.

1. Before SSH can be used with PKI, a public/private key pair must be generated. This is typically supported by the SSH client software. For example, PuTTY supports a utility called PuTTYGen that will generate key pairs. The 7705 SAR currently supports Rivest, Shamir, and Adleman (RSA) and Elliptic Curve Digital Signature Algorithm (ECDSA) user public keys. The RSA public key is supported up to 4096 bits and the ECDSA public key is supported up to NIST P-521.

   Note: *Only the RSA keys are to be used in the CC evaluated configuration because the CC evaluated configuration does not recommend the use of ECDSA keys.*

   If the client is using PuTTY, they first generate a key pair using PuTTYGen. The user sets the key type to SSH-2 RSA and sets the number of bits to be used for the key. The user can also configure a passphrase that is used to store the key locally in encrypted form. If the passphrase is configured, it acts as a password for the private key and the user must enter the passphrase in order to use the private key. If a passphrase is not used, the key is stored in plain text locally.

2. Login as an authorized Security Administrator and import the public key for the user. Follow the steps below to set up the public key for SSH user authentication:
   - The public key must be configured for the user on the 7705 SAR with the command **config>system>security>user *username*>public-keys**. The user can program the public key using the CLI.
   - **public-keys**
     Syntax: public-keys
     Context: config>system>security>user *username*
     Description: This command enables the context to configure public keys for SSH.
   - **rsa**
     Syntax: rsa
     Context: config>system>security>user *username*>public-keys
     Description: This command enables the context to configure RSA public keys.

   - **rsa-key**
     Syntax: rsa-key *key-id* [create]
     no rsa-key *key-id*
     Context: config>system>security>user *username*>public-keys>rsa
     Description This command creates an RSA public key and associates it with the specified user. Multiple public keys can be associated with the user. The key ID is used to identify these keys for the user.
     Parameters: *key-id* — the key identifier
     Values: 1 to 32

create — keyword required when first creating the RSA key. When the key is created, you can navigate into the context without the create keyword.

- **CLI Syntax:**

*A:SR-xx# configure system security user <user-name>

*A: SR-xx >config>system>security>user# public-keys rsa rsa-key <rsa-public-key-id> create

*A: SR-xx >config>system>security>user>public-keys>rsa>rsa-key$ key-value <rsa-public-key-value>

Re-enter key <rsa-public-key-value>

7 Cryptographic Protocols

Enabling CC-NDcPP compliance will ensure that only certified algorithms and key sizes are available for use by the appliance. The Nokia SAR 7705 restricts the ability to manage SSH (session keys), IPsec (session keys), and any configured X.509 certificates (public and private key pairs) to security administrators via command line. The Security Administrator has the ability to configure, modify, generate, and delete the key for SSH.

7.1 SSH

7.1.1 SSH server cipher algorithm configuration

- **cipher**
  Syntax: cipher *index* name *cipher-name*
  no cipher *index*
  Context: config>system>security>ssh>client-cipher-list
  config>system>security>ssh>server-cipher-list
  Description: This command configures the allowed SSH protocol version 1 or version 2 cipher that are available on the SSH client or server. Client cipher and server cipher lists are used to negotiate the best compatible cipher between the SSH client and SSH server. Client ciphers are used when the 7705 SAR node is acting as an SSH client; server ciphers are used when the 7705 SAR node is acting as an SSH server. The no form of this command deletes the specified cipher index.
  Values For SSHv2:
  client ciphers: aes128-ctr, aes192-ctr, aes256-ctr, 3des-cbc, blowfish-cbc, cast128-cbc, arcfour, aes128-cbc, aes192-cbc, aes256-cbc, rijndael-cbc
  server ciphers: aes128-ctr, aes192-ctr, aes256-ctr, 3des-cbc, blowfish-cbc, cast128-cbc, arcfour, aes128-cbc, aes192-cbc, aes256-cbc, rijndael-cbc

  Note:
  - *The blowfish-cbc, cast128-cbc, arcfour, and rijndael-cbc ciphers are not available if the 7705 SAR node is running in FIPS-140-2 mode.*
  - *The cryptographic keys - aes192-ctr and aes192-cbc are not to be used in the CC evaluated configuration because these two algorithms are not allowed for SSH in NDcPP 2.2e.*
  - *The protocol-version 1 is not available under FIPS-140-2 mode.*

- **CLI Syntax:**

```
*A:SR-xx # /config system security ssh server-cipher-list protocol-version 2 cipher 190 name aes256-ctr

*A:SR-xx # config > system > security > ssh# server-cipher-list protocol-version 2 cipher 194 name aes128-ctr

*A:SR-xx # config > system > security > ssh# server-cipher-list protocol-version 2 cipher 200 name aes128-cbc
```

*A:SR-xx # config > system > security > ssh# server-cipher-list protocol-version 2 cipher 230 name aes256-cbc

7.1.2 SSH key-exchange configuration for Diffie-Hellman keys

- **kex**
  Syntax: kex *index* name *kex-name*
  no kex *index*
  Context: config>system>security>ssh>client-kex-list
  config>system>security>ssh>server-kex-list
  Description: This command configures the list of preferred KEX algorithms that are negotiated by the client and server using an SSHv2 phase one handshake.

  Note: *If a 7705 SAR node is running in FIPS-140-2 mode:*
  - *SSHv1 is not supported*
  - *The following KEX algorithm is not available: diffie-hellman-group1-sha1*

  The ***no*** form of this command removes the specified KEX index. Removing all the indexes from a client or server list results in an empty list, and any KEX algorithm the client or server brings to the SSHv2 negotiation will be rejected.

  Default: no kex
  Parameters: index — the index of the KEX algorithm in the list. The list is ordered from highest to lowest.
  Values 1 to 255
  kex-name — the KEX algorithm for computing the shared secret key
  Values: diffie-hellman-group16-sha512, diffie-hellman-group14-sha256, diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1

- **CLI Syntax:**

  *A:SR-xx >config>system>security>ssh>server-kex# kex <index> name diffie-hellman-group14-sha1

  *A:SR-xx >config>system>security>ssh>server-kex# kex <index> name diffie-hellman-group14-sha256

  *A:SR-xx >config>system>security>ssh>server-kex# kex <index> name diffie-hellman-group16-sha512

7.1.3 Message Authentication Code algorithm configuration for SSHv2

- The 7705 SAR supports configurable SSHv2 server MAC and client MAC lists that are used to negotiate the best compatible MAC algorithm between the SSH client and SSH server.

- Each list contains MAC algorithms and their corresponding index values, where a lower index value has a higher preference in the SSHv2 negotiation. The list is ordered by preference from highest to lowest. When the client and server exchange their MAC lists, the first algorithm in the client list that is also supported by the server is the algorithm that is agreed upon.

- In addition, strong HMAC algorithms can be configured at the top of the MAC list (that is, as the lowest index values in the list) in the order to be negotiated first between the client and server. The first algorithm in the list that is supported by both the client and the server is the one that is agreed upon.

  Note: *Configurable MAC lists are only supported for SSHv2.*

- The default list can be changed by manually removing a single index or as many indexes as required using the no mac index command. The default list can also be customized by first removing an index and then redefining it for each algorithm as required (the 7705 SAR does not support customizing an index without first removing it).

- **Configuring SSH MAC Algorithm Lists**

  Use the ssh command to configure SSHv2 client and server MAC algorithm lists. Client MAC algorithm lists are used if the 7705 SAR is acting as an SSH client, and server MAC algorithm lists are used if the 7705 SAR is acting as an SSH server.

  Note: *If a 7705 SAR node is running in FIPS-140-2 mode:*
  - *SSHv1 is not supported*
  - *The following MAC algorithms are not available: hmac-sha1-96, hmac-md5, hmac-ripemd160, hmac-ripemd160-openssh-com, and hmac-mda5-96*

  CLI Syntax:

```
config>system>security
ssh
client-mac-list
mac index name mac-name
server-mac-list
mac index name mac-name
```

- **mac**

  Syntax: mac *index* name *mac-name*
  no mac *index*

  Context: config>system>security>ssh>client-mac-list
  config>system>security>ssh>server-mac-list

  Description: This command configures the list of preferred MAC algorithms that are negotiated by an SSHv2 server or client. Each algorithm in the list has a corresponding index value, where a lower index has a higher preference in the SSH negotiation. The list is ordered by preference from highest to lowest. The no form of this command removes the specified MAC index from the list.

  Default: no mac

  Parameters: *index* — the index of the MAC algorithm in the list

  Values: 1 to 255

  mac-name — the algorithm for calculating the message authentication code

Note: *If a 7705 SAR node is running in FIPS-140-2 mode:*

- *SSHv1 is not supported*
- *for SSHv2, the following MAC algorithms are not available: hmac-sha1-96, hmac-md5, hmac-ripemd160, hmac-ripemd160-openssh-com, and hmac-mda5-96*

- **CLI Syntax:**

```
*A:SR-xx >config>system>security>ssh>server-mac# mac <index> name hmac-sha2-512
*A:SR-xx >config>system>security>ssh>server-mac# mac <index> name hmac-sha2-256
*A:SR-xx >config>system>security>ssh>server-mac# mac <index> name hmac-sha1
```

7.1.4 Configuring SSH Rekey

The Nokia SAR 7705 restricts the ability to manage SSH (session keys) to security administrators via command line. The device is capable of rekeying. It verifies the following thresholds:

- No longer than one hour
- No more than 1 GB of transmitted data

The device continuously checks both conditions. When either of the conditions are met, the device will initiate a rekey.

- **key-re-exchange**

Syntax: key-re-exchange

Context: config>system>security>ssh

Description: This command enables the context to configure key re-exchange parameters for an SSH client or server.

- **mbytes**

Syntax: mbytes {*mbytes* | disable}
no mbytes

Context: config>system>security>ssh>key-re-exchange>client
config>system>security>ssh>key-re-exchange>server

Description: This command configures the maximum number of megabytes that can be transmitted during an SSH session before an SSH client or server initiates the key re-exchange procedure. If both the mbytes and minutes key re-exchange parameters are configured, the key re-exchange will occur at whatever limit is reached first. The no form of this command returns the setting to the default value.

Parameters: *mbytes* — specifies the number of megabytes that can be transmitted during an SSH session before the key re-exchange occurs.

disable — specifies that a session will never time out.

- **minutes**

Syntax: minutes {*minutes* | disable}

no minutes

Context: config>system>security>ssh>key-re-exchange>client

config>system>security>ssh>key-re-exchange>server

Description: This command configures the maximum time that an SSH session can be up before an SSH client or server initiates the key re-exchange procedure. If both the mbytes and minutes key re-exchange parameters are configured, the key re-exchange will occur at whatever limit is reached first. The no form of this command returns the setting to the default value.

Parameters: minutes — specifies the number of minutes before an SSH client or server initiates the key re-exchange.

disable — specifies that a session will never time out.

- **CLI Syntax:**

*A:SR-xx# configure system security ssh key-re-exchange server minutes <minutes> no shutdown

*A:SR-xx# configure system security ssh key-re-exchange server mbytes <mbytes> no shutdown

7.2 IPSec

7.2.1 IPSec Security Policy, IKE Policy, and IPSec Transform

- An IPSec security policy defines the type of traffic allowed to pass in or out of an IPSec tunnel. The policy does this through the configuration of local and remote IP address pairs. The behavior of an IPSec security policy is similar to IP filtering. IPSec security policies are created for a VPRN service context and applied to an IPSec tunnel in that service.

- An IKE policy defines how the 7705 SAR encrypts and authenticates an IPSec tunnel that uses that policy. Its configuration includes specifics on Diffie-Hellman key derivation algorithms, encryption and authentication protocols to be used for establishing phase 1 and phase 2 security associations, and so on.

- An IPSec transform defines the algorithms used for IPSec SA. The transform configuration dictates the algorithms that customer traffic uses for encryption and authentication.

7.2.2 Internet Key Exchange (IKE) and Transform Commands

- **ipsec**
  Syntax: ipsec
  Context: config
  Description: This command enables the context to configure Internet Protocol security (IPSec) parameters. IPSec is a structure of open standards to ensure private, secure communications over Internet Protocol (IP) networks by using cryptographic security services.

- **ike-policy**
  Syntax: ike-policy *ike-policy-id* [create]
  no ike-policy *ike-policy-id*
  Context: config>ipsec
  Description: This command enables provisioning of IKE policy parameters.
  The no form of the command removes the IKE policy.
  Parameters: ike-policy-id — specifies a policy ID value to identify the IKE policy
  Values: 1 to 2048
  create — mandatory keyword required when creating an IKE policy. The create keyword requirement can be enabled/disabled in the environment>create context.

- **auth-algorithm**
  Syntax: auth-algorithm {md5 | sha1 | sha256 | sha384 | sha512}
  no auth-algorithm
  Context: config>ipsec>ike-policy
  Description: This command specifies which hashing algorithm to use for the IKE authentication function.
  The no form of the command returns the parameter to its default value.
  Default: sha1
  Parameters:
  md5 — specifies the hmac-md5 algorithm for authentication

sha1 — specifies the hmac-sha1 algorithm for authentication
sha256 — specifies the sha256 algorithm for authentication
sha384 — specifies the sha384 algorithm for authentication
sha512 — specifies the sha512 algorithm for authentication

Note: *The md5 algorithm is not to be used in the CC evaluated configuration.*

- **dh-group**
  Syntax: dh-group {1 | 2 | 5 | 14 | 15}
  no dh-group
  Context: config>ipsec>ike-policy
  Description: This command specifies which Diffie-Hellman group is used to calculate session keys:
  • Group1: 768 bits
  • Group2: 1024 bits
  • Group5: 1536 bits
  • Group14: 2048 bits
  • Group15: 3072 bits
  More bits provide a higher level of security but require more processing.
  The no form of the command returns the parameter to its default value (Group2).
  Default: no dh-group (Group2)

  Note: *The DH Groups (1, 2, 5) should not be used in the CC evaluated configuration.*

- **dpd**
  Syntax: dpd [interval *interval*] [max-retries *max-retries*] [reply-only]
  no dpd
  Context: config>ipsec>ike-policy
  Description: This command controls the dead peer detection (DPD) mechanism to detect a dead IKE peer. The no form of the command disables DPD and returns the parameters to their default values.
  Default: no dpd
  Parameters: *interval* — specifies the interval that will be used to test connectivity to the tunnel peer. If the peer initiates the connectivity check before the interval timer, it will be reset.
  Values: 10 to 300 s
  Default: 30
  max-retries — specifies the maximum number of retries before the tunnel is removed
  Values: 2 to 5
  Default: 3
  reply-only — specifies to only reply to DPD keepalives. Issuing the command without the reply-only keyword disables the reply-only behavior.

- **encryption-algorithm**
  Syntax: encryption-algorithm {des | 3des | aes128 | aes192 | aes256}
  no encryption-algorithm
  Context: config>ipsec>ike-policy
  Description: This command specifies the encryption algorithm to use for the IKE session.
  The no form of the command returns the algorithm to its default value (aes128).
  Default: aes128

Parameters: des — configures the 56-bit des algorithm for encryption. This is an older algorithm, with relatively weak security. It should only be used when a strong algorithm is not available at both ends at an acceptable performance level.
3des — configures the 3-des algorithm for encryption. This is a modified application of the des algorithm that uses multiple des operations for more security.
aes128 — configures the aes algorithm with a block size of 128 bits. This is the mandatory implementation size for aes.
aes192 — configures the aes algorithm with a block size of 192 bits. This is stronger version of aes.
aes256 — configures the aes algorithm with a block size of 256 bits. This is the strongest available version of aes.

Note: *The aes192, des, and 3des algorithms are not to be used in the CC evaluated configuration.*

- **ike-mode**
  Syntax: ike-mode {main | aggressive}
  no ike-mode
  Context: config>ipsec>ike-policy
  Description: This command specifies the mode of operation for IKEv1 phase 1, either main mode or aggressive mode. The difference between the modes is the number of messages used to establish the session. IKEv1 phase 1 main mode uses three pairs of messages (for a total of six messages) between IPSec peers. IKEv1 phase 1 aggressive mode has only three message exchanges. This command does not apply to IKEv2.
  The no form of the command removes the mode of operation.
  Default: main
  Parameters: main — specifies that IKEv1 phase 1 will operate in main mode.
  aggressive — specifies that IKEv1 phase 1 will operate in aggressive mode.

- **ike-version**
  Syntax: ike-version {1 | 2}
  no ike-version
  Context: config>ipsec>ike-policy
  Description: This command configures the version of the IKE protocol that the IKE policy will use. The no form of the command removes the configured version.
  Default: 2
  Parameters: 1 — specifies that the IKE policy will use IKEv1
  2 — specifies that the IKE policy will use IKEv2

- **ikev2-fragment**
  Syntax: ikev2-fragment mtu *octets* reassembly-timeout *seconds*
  no ikev2-fragment
  Context: config>ipsec>ike-policy
  Description: This command enables IKEv2 protocol-level fragmentation (per RFC 7383). The MTU specified is the maximum size of the IKEv2 packet.
  IKEv2 fragmentation is enabled for a tunnel only if this command is configured and if the peer also announces its support by sending an IKEV2_FRAGMENTATION_SUPPORTED notification.

Default: no ikev2-fragment
Parameters: *octets* — the MTU for IKEv2 messages.
Values: 512 to 9000
seconds — the time allowed for fragment reassembly before the fragments are discarded.
Values: 1 to 5

- **ipsec-lifetime**
  Syntax: ipsec-lifetime *ipsec-lifetime*
  no ipsec-lifetime
  Context: config>ipsec>ike-policy
  Description: This parameter specifies the lifetime of a phase 2 SA.
  The no form of the command returns the ipsec-lifetime value to the default.
  Default: 3600 (1 hr)
  Parameters: *ipsec-lifetime* — specifies the lifetime of the phase 2 IKE key, in seconds
  Values: 1200 to 172800.

- **isakmp-lifetime**
  Syntax: isakmp-lifetime *isakmp-lifetime*
  no isakmp-lifetime
  Context: config>ipsec>ike-policy
  Description: This command specifies the lifetime of a phase 1 SA. ISAKMP stands for Internet Security Association and Key Management Protocol.
  The no form of the command returns the isakmp-lifetime value to the default value.
  Default: 86400
  Parameters: *isakmp-lifetime* — specifies the lifetime of the phase 1 IKE key, in seconds
  Values: 1200 to 172800

- **nat-traversal**
  Syntax: nat-traversal [force] [keep-alive-interval *keep-alive-interval*] [force-keep-alive]
  no nat-traversal
  Context: config>ipsec>ike-policy
  Description: This command specifies whether NAT-T (Network Address Translation Traversal) is enabled, disabled, or in force mode. Enabling NAT-T enables the NAT detection mechanism. If a NAT device is detected in the path between the 7705 SAR and its IPSec peer, then UDP encapsulation is done on the IPSec packet to allow the IPSec traffic to traverse the NAT device.
  When nat-traversal is used without any parameters, NAT-T is enabled and sending keepalive packets is disabled (keep-alive-interval is 0 s).
  When the force keyword is used, the IPSec tunnel always uses a UDP value in its header, regardless of whether a NAT device is detected.
  The force-keep-alive keyword specifies whether keepalive packets are sent only when a NAT device is detected or are always sent (regardless of detection of a NAT device). When force-keep-alive is used, packets are always sent and the “Behind NAT Only” field in the show>ipsec>ike-policy ike-policy-id indicates False. When force-keep-alive is not used, packets are may or may not be sent, depending on the whether NAT-T is enabled or disabled. In this case, the “Behind NAT Only” field indicates True.
  The keep-alive-timer keyword defines the frequency, where “0” means that keepalives are disabled.
  The no form of the command returns the parameters to the default values (NAT-T is disabled, keep-alive-interval is 0 s, and force-keep-alive is True).

Default: no nat-traversal
Parameters: force — when specified, forces NAT-T to be enabled.
keep-alive-interval — specifies the keepalive interval for NAT-T. If the value is 0 s, then keepalive messages are disabled.
Values: 120 to 600 s
Default: 0 s
force-keep-alive — specifies that NAT-T keepalive packets are always sent, regardless of NAT detection results.

- **own-auth-method**
  Syntax: own-auth-method psk
  no own-auth-method
  Context: config>ipsec>ike-policy
  Description: This command specifies the authentication method used by the 7705 SAR to self-authenticate. This command (own-auth-method) applies only to IKEv2.
  The default self-authentication method used by the 7705 SAR is symmetric, which means the self-authentication method is the same as the authentication method used by this IKE policy for the remote peer (that is, the own-auth-method is the same as auth-method).
  The no form of the command returns the parameter to the default value (symmetric).
  Default: no own-auth-method
  Parameters: psk — specifies the use of a pre-shared key to self-authenticate

- **ipsec-transform**
  Syntax: ipsec-transform *transform-id* [create]
  no ipsec-transform transform-id
  Context: config>ipsec
  Description: This command enables the context to create an ipsec-transform policy. IPSec transform policies can be shared between IPSec tunnels by using the transform command.
  IPSec transform policy assignments to a tunnel require the tunnel to be shut down.
  The no form of the command removes the transform ID from the configuration.
  Parameters: *transform-id* — specifies a policy ID value to identify the IPSec transform policy
  Values: 1 to 2048
  create — mandatory keyword required when creating an ipsec-transform policy. The create keyword requirement can be enabled/disabled in the environment>create context.

- **esp-auth-algorithm**
  Syntax: esp-auth-algorithm {null | md5 | sha1 | sha256 | sha384 | sha512}
  no esp-auth-algorithm
  Context: config>ipsec>transform
  Description: This command specifies which hashing algorithm should be used for the authentication function Encapsulating Security Payload (ESP). Both ends of a tunnel must share the same configuration parameters in order for the IPSec tunnel to enter the operational state. The null keyword in this command and the null keyword in the esp-encryption-algorithm command are mutually exclusive.
  The no form of the command returns the parameter to its default value.
  Default: sha1

Parameters: null — a very fast algorithm specified in RFC 2410, which provides no authentication
md5 — configures ESP to use the hmac-md5 algorithm for authentication
sha1 — configures ESP to use the hmac-sha1 algorithm for authentication
sha256 — configures ESP to use the sha256 algorithm for authentication
sha384 — configures ESP to use the sha384 algorithm for authentication
sha512 — configures ESP to use the sha512 algorithm for authentication

Note: *The null, md5 and sha1 algorithms are not to be used in the CC evaluated configuration.*

- **esp-encryption-algorithm**
  Syntax: esp-encryption-algorithm {null | des | 3des | aes128 | aes192 | aes256}
  no esp-encryption-algorithm
  Context: config>ipsec>transform
  Description: This command specifies the encryption algorithm to use for the IPSec session.
  Encryption only applies to Encapsulating Security Payload (ESP) configurations.
  For IPSec tunnels to come up, both ends of the IPSec tunnel (both private-side endpoints) must be configured with the same encryption algorithm. That is, the configuration for vprn>if>sap> ipsec-tunnel transform must match at both nodes.
  The null keyword in this command and the null keyword in the esp-auth-algorithm command are mutually exclusive. The no form of the command returns the parameter to its default value.
  Default: aes128
  Parameters: null — configures the high-speed null algorithm, which does nothing. This is the same as not having encryption turned on.
  des — configures the 56-bit des algorithm for encryption. This is an older algorithm, with relatively weak security. Although slightly better than no encryption, it should only be used when a strong algorithm is not available at both ends at an acceptable performance level.
  3des — configures the 3-des algorithm for encryption. This is a modified application of the des algorithm that uses multiple des operations to make things more secure.
  aes128 — configures the aes algorithm with a block size of 128 bits. This is the mandatory implementation size for aes. This is a very strong algorithm choice.
  aes192 — configures the aes algorithm with a block size of 192 bits. This is a stronger version of aes.
  aes256 — configures the aes algorithm with a block size of 256 bits. This is the strongest available version of aes.

  Note: *The null, des, and 3des algorithms are not to be used in the CC evaluated configuration.*

1. PBR

PBR (policy-based routing) is a part of the ingress ACL (access control list) configuration on the 7705 SAR. PBR configuration can be applied in two places for an IPSec service. The first place is for VPRN and applies to all incoming access traffic into a private VPRN. In this case, PBR can be used to direct the customer traffic into uplink IPSec tunnels by means of ACL matching criteria. The filtering action of forwarding to an indirect next hop can be used to direct customer traffic into the appropriate IPSec tunnel. The security policy works only on the original (customer packet) IP header; that is, the

PBR next hop is not used in making the security policy decision. The second place is for IPSec traffic entering the 7705 SAR from the public domain. A PBR filter can be placed on the network interface, the VPRN interface, or the IES interface to direct the IPSec packet based on the matching/forwarding criteria. In this case, IPSec packets are processed by the PBR filter in the same way as any other IP packet.

Note:

• All routing decisions are made based on the PBR configuration; therefore, it is possible that even if the packet is destined for the local node security gateway (SeGW), the PBR filter might redirect the packet to another interface.

• Alternatively, for IPSec packets that are not destined for the local node SeGW, PBR can force the packets into the local node SeGW. In this case, the encapsulating security payload (ESP) index of the IPSec packet will not match the SeGW ESP configuration and the packet will be dropped. Thus, it is the responsibility of the network administrator to ensure that the PBR configuration is correct and meets the network needs.

2. NGE and ACL Interactions

When NGE is enabled on a router interface, the ACL function is applied as follows:

• on ingress — Normal ACLs are applied to traffic received on the interface that could be either NGE-encrypted or clear text. For NGE-encrypted packets, this implies that only the source, destination, and IP options are available to filter on ingress, as the protocol is ESP and the packet is encrypted. If an IP exception ACL is also configured on the interface, the IP exception ACL is applied first to allow any clear text packets to ingress as needed. After the IP exception ACL is applied and if another filter or ACL is configured on the interface, the other filter will process the remaining packet stream (NGE-encrypted and IP exception ACL packets), and other ACL functions such as PBR or Layer 4 information filtering could be applied to any clear text packets that passed the exception ACL.

• on egress — ACLs are applied to packets before they are NGE-encrypted as per normal operation without NGE enabled.

3. Interface SAP Commands

- **egress**
  Syntax: egress
  Context: config>service>vprn>if>sap
  Description: This command enables the context to configure egress SAP QoS policies and filter policies. If no sap-egress QoS policy is defined, the system default sap-egress QoS policy is used for egress processing. If no egress filter policy is defined, no filtering is performed.

- **ingress**
  Syntax: ingress
  Context: config>service>vprn>if>sap
  Description: This command enables the context to configure ingress SAP QoS policies and filter policies. If no sap-ingress QoS policy is defined, the system default sap-ingress QoS policy is used for

ingress processing. If no ingress filter policy is defined, no filtering is performed.

- **filter**
  Syntax: filter ip *ip-filter-id*
  no filter ip [*ip-filter-id*]
  Context: config>service>vprn>if>sap>egress
  config>service>vprn>if>sap>ingress
  Description: This command associates an IPv4 filter policy with an ingress or egress SAP or IP interface. Filter policies control the forwarding and dropping of packets based on IP matching criteria.
  The filter command is used to associate a filter policy with a specified ip-filter-id with an ingress or egress SAP. The ip-filter-id must already be defined before the filter command is executed. If the filter policy does not exist, the operation will fail and an error message will be returned.
  In general, filters applied to SAPs apply to all packets on the SAP. One exception is that IP match criteria are not applied to non-IP packets, in which case the default action in the filter policy applies to these packets.
  The no form of this command removes any configured filter ID association with the SAP or IP interface. The filter ID is not removed from the system unless the scope of the created filter is set to local. To avoid deletion of the filter ID and only break the association with the service object, use the scope command within the filter definition to change the scope to local or global. The default scope of a filter is local.
  Parameters: *ip-filter-id* — the IPv4 filter policy. The filter ID or filter name must already exist within the
  created IPv4 filters.
  Values: 1 to 65535 or filter-name (up to 64 characters)

4. Configuring IPSec and IPSec Tunnels in Services

- IPSec is configured under VPRN services. The device operates only in tunnel mode by default and no separate configuration is required. For the private-side IPSec tunnel interface and SAP, under the VPRN service context, configure IPSec security policies, and create tunnel interfaces, private tunnel SAPs, IPSec tunnels, and IPSec tunnel parameters. The tunnel keyword must be used when creating an interface for a private tunnel SAP.
- For a public-side IPSec tunnel interface and SAP, under VPRN service context, create an interface and public tunnel SAP. The tunnel keyword is not used when creating an interface for a public tunnel SAP.
- Private-side and public-side tunnels function in pairs, where a pair is defined by the service ID and the interface subnet.
- The local gateway address and delivery service configured using the VPRN ipsec-tunnel>local-gateway-address command correspond to the VPRN interface address and service ID where the public-side tunnel interface is defined. In the example below, the local-gateway-address is 10.1.5.28 and the delivery-service is 3.

- **The following example demonstrate the configuration steps and output when configuring IPSec for a private-side and a public-side VPRN service:**

  i. Configure the ISA tunnel as follows:
  *A:SARX# configure isa tunnel-group 1
  *A:SARX>config>isa>tunnel-grp# info

```
        description "IPSec-Test-on-SARX"
        no shutdown
```

ii. IKE policy configuration:

```
*A:SARX# configure ipsec ike-policy 1
*A: SARX>config>ipsec>ike-policy# info
        description "ike-policy_1"
        own-auth-method psk
        ipsec-lifetime 86400
        isakmp-lifetime 21600
         pfs dh-group 5
        dpd
```

iii. ESP authentication and encryption algorithm:

```
*A:SARX# configure ipsec ipsec-transform 1
*A: SARX>config>ipsec>transform# info detail
        esp-auth-algorithm sha1
        esp-encryption-algorithm aes128
```

iv. Public service configuration:

```
*A:SARX# configure service vprn 3
*A:SARX>config>service>vprn# info
          route-distinguisher 1.1.1.1:3
          interface "TO_VM-02" create
              address 10.1.8.253/30
              sap 1/2/1 create
              exit
        exit
        interface "TO_STRONGSWAN_IPSEC_TUNNEL" create
            address 10.1.5.254/24
              sap tunnel-1.public:3 create
              exit
            exit
              interface "STRONGSWAN-INTERCONNECT" tunnel create
              exit
              static-route-entry 10.1.11.0/24
                 next-hop 10.1.8.254
                     no shutdown
                   exit
              exit
             service-name "PUBLIC_NETWORK'S_SECURE_GATEWAY"
               no shutdown
```

v. Private service configuration:

```
*A:SARX# configure service vprn 4
*A:SARX>config>service>vprn# info
      ipsec
        security-policy 1 create
          entry 1 create
            local-ip 10.1.100.0/24
            remote-ip 10.1.12.0/24
          exit
        exit
```

```
exit
route-distinguisher 1.1.1.1:4
interface "STRONGSWAN-INTERCONNECT" tunnel create
   sap tunnel-1.private:1 create
      ipsec-tunnel "STRONGSWAN-INTERCONNECT" create
         security-policy 1
         local-gateway-address 10.1.5.28 peer 10.1.11.1 delivery-service 3
         dynamic-keying
            ike-policy 1
            pre-shared-key"xp95xk5zK1YnUrABq6x0ZqnQu1v5eUCZtX4=" hash2
            transform 1
         exit
         no shutdown
      exit
   exit
exit
interface "PRIVATE-CLIENT-1" create
   address 10.1.100.1/32
   loopback
exit
static-route-entry 10.1.12.0/24
      ipsec-tunnel "STRONGSWAN-INTERCONNECT"
         no shutdown
   exit
exit
service-name "PRIVATE-DOMAIN-SECURITYGW"
no shutdown
```

5. Configuring Reference Identifiers

- The Nokia SAR 7705 device supports the following reference identifiers:
  - SAN: IP address
  - SAN: FullyQualifiedDomainName (FQDN)
  - SAN: user FQDN

- The following configuration is used to configure reference identifiers on the device:

  remote-id type <ipv4, fqdn, email> value *value*

6. Deleting an IPSec Tunnel

IPSec tunnels are created under the VPRN service. Although an IPSec tunnel is created on the private side of the tunnel in the CLI, the configuration itself is general and can apply to either the public or private side of the tunnel. To delete an IPSec tunnel:

CLI Syntax:

config>service>vprn>if>sap# no ipsec-tunnel *ipsec tunnel-name*

Example: config>service>vprn>if>sap# no ipsec-tunnel ies_tunnelPublicSide_1

8 Logging Configuration

8.1 Memory Logs

A memory log is a circular buffer. When the log is full, the oldest entry in the log is replaced with the new entry. When a memory log is created, the specific number of entries it can hold can be specified; otherwise, it will assume a default size. An event log can send entries to a memory log destination.

8.2 Log Configuration

The most basic log configuration must have the following:

- a log ID or an accounting policy ID
- a log source
- a log destination

Use the following CLI syntax to configure a log file:

CLI Syntax:

```
config>log
log-id log-id
description description-string
filter filter-id
from {[main] [security] [change] [debug-trace]}
to console
to memory [size]
to syslog syslog-id
time-format {local | utc}
no shutdown
```

The following displays an example of the event log file configuration command syntax:

Example:

```
config# log
config>log# log-id 2
config>log>log-id# description "This is a test log file."
config>log>log-id# filter 1
config>log>log-id# from main security
config>log>log-id# to file 1
config>log>log-id# no shutdown
config>log>log-id# exit
```

The following are the steps required to configure logging:

1. **Configure a log ID**
   CLI Syntax:
   config>log
   log-id *log-id*

description description-string

2. **Configure the Logging Source**
   CLI Syntax:
   config>log
   log-id *log-id*
   from {[main] [security] [change] [debug-trace]}

3. **Configure the Logging Destination**

- **to memory**
  Syntax: to memory [size]
  Context: config>log>log-id
  Description: This command instructs the events selected for the log ID to be directed to a memory file. A memory file is a circular buffer. Once the file is full, each new entry replaces the oldest entry in the log.
  Parameters: size — indicates the number of events that can be stored in the memory log
  Values: 50 to 3000
  Default: 100

- **to syslog**
  Syntax: to syslog *syslog-id*
  Context: config>log>log-id
  Description: This command instructs the alarms and traps to be directed to a specified syslog. To remain consistent with the standards governing syslog, messages to syslog are truncated to 1 Kbyte.
  Parameters: syslog-id — instructs the events selected for the log ID to be directed to the syslog-id. The characteristics of the syslog-id referenced here must have been defined in the **config>log>syslog** *syslog-id* context.
  Values: 1 to 10

- **to console**
  Syntax: to console
  Context: config>log>log-id
  Description: This command instructs the events selected for the log ID to be directed to the console. If the console is not connected, all entries are dropped.

- **filter**
  Syntax: filter *filter-id*
  no filter
  Context: config>log>log-id
  Description: This command associates an event filter policy with the log destination.
  The filter command is optional. If no event filter is configured, all events, alarms and traps generated by the source stream will be forwarded to the destination. Only one filter-id can be configured per log destination. The *no* form of the command removes the specified event filter from the log-id.
  Default: no filter
  Parameters: *filter-id* — the event filter policy ID that is used to associate the filter with the log-id configuration. The event filter policy ID must already be defined in the

config>log>filter filter-id context. Log ID 100 is preconfigured by the system as a Severe Event Log that is associated with filter policy 1001 by default.
Values: 1 to 1001

- **time-format**
  Syntax: time-format {local | utc}
  Context config>log>log-id
  Description: This command specifies whether the time should be displayed in local or Coordinated Universal Time (UTC) format.
  Default: utc
  Parameters: local — specifies that timestamps are written in the system's local time
  utc — specifies that timestamps are written using the UTC value.

9 Using a Secure Audit Server

Use the following procedure to configure a secure audit server.

9.1 Prerequisites

Configure an audit server on external IT environment.

9.2 Audit Server Requirements

4.2.1 Syslog

An event log can be configured to send events to one syslog destination. Syslog destinations have the following properties:

• syslog server IP address
• the UDP port used to send the syslog message
• the Syslog Facility Code
• the Syslog Severity Threshold (0 to 7) (events exceeding the configured level will be sent)

9.3 Configure Nokia SAR 7705 to communicate with an Audit Server

To use an audit server using trusted channel, follow the steps below:

1. **Use the following CLI syntax to configure a syslog file:**

   CLI Syntax:
   config>log
   syslog *syslog-id*
   address *ip-address*
   description *description-string*
   facility *syslog-facility* level {emergency | alert | critical | error | warning | notice | info | debug}
   log-prefix *log-prefix-string*
   port *port*

   Example:

```
config# log
config>log# syslog 1
config>log>syslog# description "This is a syslog file."
config>log>syslog# address 10.10.10.104
config>log>syslog# facility user
config>log>syslog# level warning
```

2. **Configure a log-id for the syslog server and set the destination directed to the syslog server.**

CLI Syntax:

```
config>log
log-id log-id
description description-string
from {[main] [security] [change] [debug-trace]}
to syslog syslog-id
```

Example:

```
A:SARX>config>log>log-id# info
----------------------------------------------
        no shutdown
        description "This is a test log file."
        from main security change debug-trace
        to syslog 1
```

---

3. **Using IPSec tunnelling to secure communication between the device and the Audit Server.**
   - If an authorized administrator wants to back up logs to a syslog server, then protection must be provided for the syslog server communications which can be done with a syslog server operating as an IPsec peer of the Nokia SAR 7705 and the log records being tunneled over that connection.
   - If the IPsec connections used by the device is unintentionally broken, the security administrator needs to restart the connection, or the device will try to re-connect with the audit server.
   - When a Syslog server is configured on the device, the generated audit events are simultaneously sent to the external server and the local logging buffer.

9.4 Syslog Commands

- **syslog**
  Syntax: [no] syslog *syslog-id*
  Context: config>log
  Description: This command enables the context to configure a syslog target host that is capable of receiving selected syslog messages from the 7705 SAR.
  A valid syslog-id must have the target syslog host address configured.
  A maximum of 10 syslog IDs can be configured.
  No log events are sent to a syslog target address until the syslog-id has been configured as the log destination (to) in the log-id node.
  Default: No syslog IDs are defined.

Parameters: syslog-id — the syslog ID number for the syslog destination, expressed as a decimal integer
Values: 1 to 10

- **address**
  Syntax: address *ip-address*
  no address
  Context: config>log>syslog
  Description: This command associates the syslog target host IP address with the syslog ID. This parameter is mandatory. If no address is configured, syslog data cannot be forwarded to the syslog target host.
  Only one address can be associated with a syslog-id. If multiple addresses are entered, the last address entered overwrites the previous address.
  The same syslog target host can be used by multiple log IDs.
  The no form of the command removes the syslog target host IP address.
  Default: no address
  Parameters: *ip-address* — the IP address of the syslog target host
  Values: *ipv4-address* a.b.c.d

- **facility**
  Syntax: facility *syslog-facility*
  no facility
  Context: config>log>syslog
  Description: This command configures the facility code for messages sent to the syslog target host.
  Multiple syslog IDs can be created with the same target host but each syslog ID can only have one facility code. If multiple facility codes are entered, the last facility code entered overwrites the previous facility code.
  If multiple facilities need to be generated for a single syslog target host, then multiple log-id entries must be created, each with its own filter criteria to select the events to be sent to the syslog target host with a given facility code.
  The no form of the command reverts to the default value.
  Parameters: syslog-facility — the syslog facility name for the event type being sent to the syslog target host.

- **level**
  Syntax: level syslog-level
  no level
  Context: config>log>syslog
  Description: This command configures the syslog message severity level threshold. All messages with a severity level equal to or higher than the threshold are sent to the syslog target host.
  Only a single threshold level can be specified. If multiple level commands are entered, the last command will overwrite the previous command.
  The no form of the command reverts to the default value.
  Default: info
  Parameters: syslog-level — the threshold severity level value
  Values: emergency, alert, critical, error, warning, notice, info, or debug

- **log-prefix**
  Syntax: log-prefix *log-prefix-string*
  no log-prefix
  Context: config>log>syslog
  Description: This command adds the string prepended to every syslog message sent to the syslog host.
  The no form of the command removes the log prefix string.
  Default: no log-prefix
  Parameters: *log-prefix-string* — an alphanumeric string of up to 32 characters. Spaces and colons (:) cannot be used in the string

- **port**
  Syntax: port *value*
  no port
  Context: config>log>syslog
  Description: This command configures the UDP port that will be used to send syslog messages to the syslog target host.
  The port configuration is needed if the syslog target host uses a port other than the standard UDP syslog port 514.
  Only one port can be configured. If multiple port commands are entered, the last entered port overwrites the previously entered ports.
  The no form of the command reverts to default value.
  Default: no port
  Parameters: *value* — the configured UDP port number used when sending syslog messages
  Values: 0 to 65535

9.5 Auditable Events

9.5.1 Format

The Nokia SAR 7705 generates a comprehensive set of audit logs that identify specific device operations whenever an auditable event occurs. Each audit record contains the date and time of event, type of event, subject identity, and the outcome (success or failure) of the event.

All configuration changes are recorded with subject identity as the user request is made through the command line interface (CLI) with either local or remote connection.

9.5.2 Audit Events

Table 4. Log Event Element Descriptions

Label	Description
nnnn	The log entry sequence number
YYYY/MM/DD	The UTC or local date stamp for the log entry *YYYY* — year *MM* — month *DD* — day

HH:MM:SS.SS	The UTC timestamp for the event *HH* — hours (24-hour format) *MM* — minutes *SS.SS* — seconds
TZONE	The timezone (for example, UTC, EDT) as configured by configure log log-id *log-id* time-format
<severity>	The severity level of the event CRITICAL MAJOR MINOR WARNING INFO CLEARED
<application>	The name of the application generating the log message
<event_id>	The application event ID number for the event
<router>	The router name representing the VRF ID that generated the event
<subject>	The subject/affected object for the event
<message>	A text description of the event

Table 5. NDcPP Audit Events

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit
FAU_GEN.1	None.	None.	None.
FAU_GEN.2	None.	None.	None.
FAU_STG_EXT.1	None.	None.	None.
FCS_CKM.1	None.	None.	None.
FCS_CKM.2	None.	None.	None.
FCS_CKM.4	None.	None.	None.
FCS_COP.1/DataEncryption	None.	None.	None.
FCS_COP.1/SigGen	None.	None.	None.
FCS_COP.1/Hash	None.	None.	None.
FCS_COP.1/KeyedHash	None.	None.	None.

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure	**Below listed logs show the failure of IPsec connection.** 862 2022/09/12 07:38:14.82 UTC MINOR: IPSEC 82014 vprn3 IPsec tunnel failure "Tunnel STRONGSWAN-INTERCONNECT failed: invalid_exchange_type." 861 2022/09/12 07:37:51.49 UTC MINOR: IPSEC 2014 vprn3 IPsec tunnel failure "Tunnel STRONGSWAN-INTERCONNECT failed: invalid_exchange_type." 860 2022/09/12 07:37:38.53 UTC MINOR: IPSEC 2014 vprn3 IPsec tunnel failure "Tunnel STRONGSWAN-INTERCONNECT failed: invalid_exchange_type."
FCS_RBG_EXT.1	None.	None.	None.
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure	**Below listed log shows the SSH session failed due to hmacMismatch.** 39 2022/06/16 10:23:56.97 UTC MINOR: SECURITY #2240 Base SSH session failed "SSH session failed from client 10.1.2.250, reason 'hmacMismatch"
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded	Origin of the attempt (e.g., IP address)	**Below listed log represents the failed authentication.** 36 2022/06/07 14:28:19.35 UTC MINOR: SECURITY #2011 Base sarx "User sarx from 10.1.2.250 failed authentication" 35 2022/06/07 14:27:16.81 UTC MINOR: SECURITY #2012 Base sarx "User sarx from 10.1.2.250 attempted more than 3 times to log in, user locked out for 3 min" 34 2022/06/07 14:27:16.81 UTC MINOR: SECURITY #2011 Base sarx "User sarx from 18.1.2.250 failed authentication" 33 2022/06/07 14:26:20.31 UTC MINOR: SECURITY #2011 Base sarx "User sarx from 10.1.2.250 failed authentication" 32 2022/06/07 14:26:18.64 UTC MINOR: SECURITY #2011 Base sarx "User sarx from 18.1.2.250 failed authentication"
FIA_PMG_EXT.1	None.	None.	None.

FIA_UIA_EXT.1	All use of identification and authentication mechanism	Origin of the attempt (e.g., IP address)	**Below listed logs represent all identification and authentication mechanism.** **While logging in using password-based authentication:** 305 2022/06/28 14:15:19.13 UTC MINOR: SECURITY #2011 Base admin "User admin from 10.1.2.250 failed authentication" **While logging in using public key:** 303 2022/06/28 14:00:34.42 UTC MINOR: SECURITY #2009 Base admin "User admin from 10.1.2.250 logged in" **While logging in using RADIUS server:** 965 2022/09/05 08:36:09.17 UTC MINOR: USER #2003 Base test "User from 10.1.2.250 failed authentication" 964 2022/09/05 08:36:09.17 UTC MINOR: SECURITY # 2011 Base test "User test from 10.1.2.250 failed authentication" 963 2022/09/05 08:36:06.13 UTC MINOR: USER #2003 Base test "User from 10.1.2.250 failed authentication" 962 2022/09/05 08:36:06.13 UTC MINOR: SECURITY # 2011 Base test "User test from 10.1.2.250 failed authentication" 961 2022/09/05 08:36:01.18 UTC MINOR: USER #2003 Base test "User from 10.1.2.250 failed authentication" 960 2022/09/05 08:36:01.18 UTC MINOR: SECURITY #2011 Base test "User test from 10.1.2.250 failed authentication" **While logging in using TACACS server:** 502 2022/09/19 14:40:18.40 UTC MINOR: USER #2004 Base user176 "User from 10.1.2.250 attempted more than 3 times to log in, user is locked out" 501 2022/09/19 14:40:18.40 UTC MINOR: SECURITY #2012 Base user176 "User user176 from 10.1.2.250 attempted more than 3 times to log in, user locked out for 3 min” 500 2822/09/19 14:40:18.39 UTC MINOR: USER #2003 Base user176

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit
			"User from 10.1.2.250 failed authentication" 499 2822/09/19 14:40:18.39 UTC MINOR: SECURITY #2011 Base user176 "User user176 from 10.1.2.250 failed authentication" 498 2022/09/19 14:40:17.52 UTC MINOR: USER #2003 Base user176 "User from 10.1.2.250 failed authentication" 497 2022/09/19 14:40:17.52 UTC MINOR: SECURITY #2011 Base user176 "User user176 from 10.1.2.250 failed authentication" 496 2822/09/19 14:40:16.59 UTC MINOR: USER #2003 Base user176 "User from 10.1.2.250 failed authentication" 495 2022/09/19 14:40:16.59 UTC MINOR: SECURITY #2011 Base user176 "User user176 from 10.1.2.250 failed authentication"

FIA_UAU_EXT.2	All use of identification and authentication mechanism	Origin of the attempt (e.g., IP address)	**Below listed logs represent all identification and authentication mechanism.** **While logging in using password-based authentication:** 305 2022/06/28 14:15:19.13 UTC MINOR: SECURITY #2011 Base admin "User admin from 10.1.2.250 failed authentication" **While logging in using public key:** 303 2022/06/28 14:00:34.42 UTC MINOR: SECURITY #2009 Base admin "User admin from 10.1.2.250 logged in" **While logging in using RADIUS server:** 965 2022/09/05 08:36:09.17 UTC MINOR: USER #2003 Base test "User from 10.1.2.250 failed authentication" 964 2022/09/05 08:36:09.17 UTC MINOR: SECURITY # 2011 Base test "User test from 10.1.2.250 failed authentication" 963 2022/09/05 08:36:06.13 UTC MINOR: USER #2003 Base test "User from 10.1.2.250 failed authentication" 962 2022/09/05 08:36:06.13 UTC MINOR: SECURITY # 2011 Base test "User test from 10.1.2.250 failed authentication" 961 2022/09/05 08:36:01.18 UTC MINOR: USER #2003 Base test "User from 10.1.2.250 failed authentication" 960 2022/09/05 08:36:01.18 UTC MINOR: SECURITY #2011 Base test "User test from 10.1.2.250 failed authentication" **While logging in using TACACS server:** 502 2022/09/19 14:40:18.40 UTC MINOR: USER #2004 Base user176 "User from 10.1.2.250 attempted more than 3 times to log in, user is locked out" 501 2022/09/19 14:40:18.40 UTC MINOR: SECURITY #2012 Base user176 "User user176 from 10.1.2.250 attempted more than 3 times to log in, user locked out for 3 min"

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit
			500 2822/09/19 14:40:18.39 UTC MINOR: USER #2003 Base user176 "User from 10.1.2.250 failed authentication" 499 2822/09/19 14:40:18.39 UTC MINOR: SECURITY #2011 Base user176 "User user176 from 10.1.2.250 failed authentication" 498 2022/09/19 14:40:17.52 UTC MINOR: USER #2003 Base user176 "User from 10.1.2.250 failed authentication" 497 2022/09/19 14:40:17.52 UTC MINOR: SECURITY #2011 Base user176 "User user176 from 10.1.2.250 failed authentication" 496 2822/09/19 14:40:16.59 UTC MINOR: USER #2003 Base user176 "User from 10.1.2.250 failed authentication" 495 2022/09/19 14:40:16.59 UTC MINOR: SECURITY #2011 Base user176 "User user176 from 10.1.2.250 failed authentication"
FIA_UAU.7	None.	None.	None.
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the device's trust store	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the device's trust store	**Below mentioned log shows the verification failure.** 1377 2922/08/10 13:87:21.36 UTC MINOR: IPSEC #2814 vprn3 IPsec tunnel failure "Tunnel STRONGSWAN-INTERCONNECT failed: authentication failed." 1376 2022/08/10 13:07:21.36 UTC MINOR: SECURITY #2844 Base Cert Verification "IPsec Tunnel STRONGSWAN-INTERCONNECT: Certificate /C=US/D=Acumen/OU=CC/CN=Strongswan verification failed due to certificate revoked at certificate:/C=US/D=A cumen/OU=CC/CN=Strongswan
FIA_X509_EXT.2	None.	None.	None.
FIA_X509_EXT.3	None.	None.	None.
FMT_MOF.1/Functions	None.	None.	None.

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.	**Below listed log shows the attempt to initiate a manual update without admin privilege.** *A:SARX# admin reboot MINOR: CLI Command not allowed for this user.
FMT_MOF.1/Services	None.	None.	**Below listed log shows the attempt to use a service without admin privilege.** *A:SARX# configure system security user "test1" MINOR: CLI Command not allowed for this user.
FMT_MTD.1/CoreData	None.	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.	None.
FMT_SMF.1	All management activities of TSF data	None.	None.
FMT_SMR.2	None.	None.	None.
FPT_SKP_EXT.1	None.	None.	None.
FPT_APW_EXT.1	None.	None.	None.
FPT_TST_EXT.1	None.	None.	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	**The following logs show that the time has been changed on the device.** 526 2022/07/06 08:08:50.00 UTC WARNING: SYSTEM # 2001 Base System date/time "Date and time on the system is 2022/07/06 08:08:50" 525 2022/07/06 08:08:50.00 UTC WARNING: SYSTEM #2081 Base System date/time "Date and time on the system is changing from 2022/07/05 07:13:27"
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.	

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit
FTA_SSL.3	The termination of a remote session by the session locking mechanism	None.	**Below listed log shows the termination of remote session.** 494 2022/07/04 12:25:44.40 UTC MINOR: SECURITY #2010 Base sarx "User sarx from 10.1.2.250 logged out"
FTA_SSL.4	The termination of an interactive session	None.	**Below listed log shows the termination of an interactive session.** 347 2022/06/29 10:24:04.46 UTC MINOR: SECURITY #2002 Base admin "User admin from CONSOLE logged out"
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism	None.	**Below listed log show the termination of a local interactive session by the session locking mechanism.** 317 2022/10/14 11:57:14.57 UTC MINOR: SECURITY #2002 Base admin "User admin from CONSOLE logged out"
FTA_TAB.1	None.	None.	None.

FTP_ITC.1	Initiation of the trusted channel Termination of the trusted channel Failure of the trusted channel functions	Identification of the initiator and target of failed trusted channels establishment attempt	**Below listed logs shows the Initiation of the trusted channel.** 829 2022/07/08 07:17:55.02 UTC MINOR: IPSEC #2011 vpre4 IPSEC "Operational state change for IPsec Tunnel STRONGMAN-INTERCONNECT on service 4 and SAP tunnel-1.private:1, admin state: inService, oper state: inService" 828 2022/07/08 07:17:55.02 UTC WARNING: SYSTEM #2009 vprn4 IPSEC "Status of IPsec tunnel STRONGSWAN-INTERCONNECT changed administrative state: inService, operational state: inService" **Below listed logs shows the Termination of the trusted channel.** 2037 2622/18/06 21:07:30.23 UTC MINOR: IPSEC #2911 vprn4 IPSEC "Operational state change for IPsec Tunnel STRONGSWAN-INTERCONNECT on service 4 and SAP tunnel-1.private:1, admin state: inService, oper state: outOfService" 2036 2622/10/06 21:07:30.23 UTC WARNING: SYSTEM #2609 vprn4 IPSEC "Status of IPsec tunnel STRONGSWAN-INTERCONNECT changed administrative state: inService, operational state: outofService **Below listed logs shows the Failure of trusted channel.** 387 2022/07/13 17:40:10.93 UTC WARNING: SYSTEM #2008 Base OAM "Test name "CliIcmpPing-15", owner name "TiMOS CLI", ping managed object deleted" 386 2022/07/13 17:40:07.07 UTC MINOR: IPSEC #2014 vprn3 IPsec tunnel failure "Tunnel STRONGSWAN-INTERCONNECT failed: malformed_message." 385 2022/07/13 17:40:05.86 UTC MINOR: IPSEC # 2014 vprn3 IPsec tunnel failure "Tunnel STRONGSWAN-INTERCONNECT failed: malformed_message."

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit
			384 2022/07/13 17:40:04.75 UTC MINOR: IPSEC #2014 vprn3 IPsec tunnel failure "Tunnel STRONGSWAN-INTERCONNECT failed: malformed_message." 383 2022/07/13 17:40:03.04 UTC MINOR: IPSEC #2014 vprn3 IPsec tunnel failure "Tunnel STRONGSWAN-INTERCONNECT failed: malformed_message." 382 2022/07/13 17:40:01.91 UTC WARNING: SYSTEM #2007 Base OAM "Test name "CliIcmpPing-15", owner name "TIMOS CLI", ping managed object created" 381 2022/07/13 17:39:47.44 UTC MINOR: IPSEC #2014 vprn3 IPsec tunnel failure "Tunnel STRONGSWAN-INTERCONNECT failed: transform_mismatch." 380 2022/07/13 17:39:26.92 UTC MINOR: IPSEC #2014 vprn3 IPsec tunnel failure "Tunnel STRONGSWAN-INTERCONNECT failed: transform_mismatch." 379 2022/07/13 17:38:56.31 UTC WARNING: SYSTEM #2006 vprn4 IPSEC "IPsec tunnel STRONGSWAN-INTERCONNECT configuration modified"
FTP_TRP.1/Admin	Initiation of the trusted path Termination of the trusted path. Failure of the trusted path functions.	None.	**Below listed logs show Initiation of the trusted path.** 336 2022/10/14 12:34:35.00 UTC MINOR: SECURITY #2009 Base sarw "User sarw from 10.1.2.200 logged in" **Below listed logs show Termination of the trusted path.** 308 2022/10/14 08:59:47.69 UTC MINOR: SECURITY #2010 Base sarw "User sarw from 10.1.2.200 logged out" **Below listed logs show failure of the trusted path.** 237 2022/10/12 14:56:12.20 UTC MINOR: SECURITY #2011 Base admin "User admin from 10.1.2.200 failed authentication"

10 X.509 Certificates

1. X.509 and Certificate Commands

- **gen-keypair**

  Syntax: gen-keypair *url-string* [size {512 | 1024 | 2048}] [type {rsa | dsa}]

  Context: admin>certificate

  Description: This command generates an RSA or DSA private key/public key pair and stores it in a local file in the cf3:\system-pki\key directory.

  Parameters: *url-string* — the name of the key file

  Values: *url-string*: local-url, 99 characters maximum

  local-url: cflash-id/file-path

  cflash-id: cf1:, cf2:, cf3:

  size — the key size in bits

  Values 512, 1024, or 2048

  Default 2048

  type — the type of key

  Values: rsa, dsa

  Default: rsa

  Note: *The key sizes 512 and 1024 are not supported in FIPS mode. The DSA key pairs should not be configured in the CC evaluated configuration. The minimum key size is 2048 bits in FIPS mode.*

  CLI Syntax:

  ```
  *A:SR-xx# /admin certificate gen-keypair <url-string> size 2048 type rsa
  ```

- **gen-local-cert-req**

  Syntax: gen-local-cert-req keypair *url-string* subject-dn *subject-dn* [domain-name domain-name] [ip-addr {*ip-address*}] file *url-string* [hash-alg *hash-algorithm*] [use-printable]

  Context: admin>certificate

  Description: This command generates a PKCS# 10 formatted certificate request by using a local existing key pair file.

  Default: n/a

  Parameters: *url-string* — the name of the key file in cf3:\system-pki\key that is used to generate a certificate request

  Values: url-string : local-url, 99 characters maximum

  local-url : cflash-id/file-path

  cflash-id : cf1:, cf2:, cf3:

subject-dn — the distinguishing name that is used as the subject in a certificate request, including:

- C – Country
- ST – State
- O – Organization name
- OU – Organization Unit name
- CN – common name

This parameter is formatted as a text string including any of the above attributes. The attribute and its value are linked by using "=", and "," is used to separate different attributes.

CLI Syntax:

```
*A:SR-xx# /admin certificate gen-local-cert-req keypair <url-string> subject-dn
CN=<a.b.c.d>,C=<country>,O=<organization name>,OU=<organizational unit> file <url-
string>
```

2. PKI Commands

- **auth-method**
  Syntax: auth-method {psk | cert-auth}
  no auth-method
  Context: config>ipsec>ike-policy
  Description: This command specifies the authentication method used with this IKE policy. The no form of the command removes the parameter from the configuration.
  Default: no auth-method

- **own-auth-method**
  Syntax: own-auth-method {psk | cert}
  no own-auth-method
  Context: config>ipsec>ike-policy
  Description: This command configures the authentication method used with this IKE policy on its own side.

- **trust-anchor-profile**
  Syntax: trust-anchor-profile *name* [create]
  no trust-anchor-profile *name*
  Context: config>ipsec
  Description: This command specifies the trust-anchor-profile for the IPSec tunnel. This command will override the trust-anchor-profile configuration in the config>service>vprn>if>sap>ipsec-tunnel>cert context.
  Default: no trust-anchor-profile
  Parameters: *profile-name* — the trust-anchor-profile name

- **cert-profile**

Syntax: cert-profile *profile-name* [create]
no cert-profile *profile-name*

Context: config>ipsec

Description: This command creates a new certificate profile or enters the configuration context of an existing certificate profile.

The no form of the command removes the profile name from the cert-profile configuration.

Default: n/a

Parameters: *profile-name* — the name of the certificate profile, up to 32 characters in length

- **send-chain**
  Syntax: [no] send-chain
  Context: config>ipsec>cert-profile>entry
  Description: This command enters the configuration context of send-chain in the cert-profile entry.
  This command is optional. By default, the system sends the certificate specified by the cert command in the selected entry to the peer. This command allows the system to send additional CA certificates to the peer. These additional CA certificates must be in the certificate chain of the certificate specified by the cert command in the same entry.

3. Configuring X.509v3 Certificate Parameters

The Nokia SAR 7705 can be configured by the privileged administrators to use X.509v3 certificates to authenticate IPsec peers. RSA certificates are supported.

Perform the following steps to configure certificate enrollment:

Step 1. Generate a key:
admin certificate gen-keypair cf3:/key_plain_rsa2048 size 2048 type rsa

Step 2. Generate a certificate request:
admin certificate gen-local-cert-req keypair cf3:/key_plain_rsa2048 subject-dn "C=US, OU=CC, CN=7705" ip-addr 10.1.5.28 file 7705_req.csr

Step 3. Send the certificate request to CA-1 to sign and get the signed certificate.

Step 4. Import the key:
admin certificate import type key input cf3:/key_plain_rsa2048 output key1_rsa2048 format der

Step 5. Import the signed certificate:
admin certificate import type cert input cf3:/7705_cert.pem output 7705cert format pem

Perform the following steps to import the CA certificate and CRL:

Step 1. Import the CA certificate:
admin certificate import type cert input cf3:/CA_1_cert.pem output ca_cert format pem

Step 2. Import the CA's CRL:
admin certificate import type crl input cf3:/CA_1_crl.pem output ca_crl format pem

Perform the following steps to create CA profiles:

Step 1. Create the CA profile:
configure system security pki ca-profile "CA" create

Step 2. Add the certificate and crl file:
cert-file "ca_cert"
crl-file "ca_crl"

Following example displays certificate-based authentication configuration for IPSec tunnel:

```
config>system>security>pki# info
----------------------------------------------
ca-profile "CA" create
cert-file "ca_cert"
crl-file "ca_crl"
no shutdown
exit

----------------------------------------------
config>ipsec# info
----------------------------------------------
ike-policy 1 create
        description "ike-policy_1"
        auth-method cert-auth
        ipsec-lifetime 86345
        isakmp-lifetime 21600
        dpd
        ikev2-fragment mtu 1280 reassembly-timeout 5
    exit
    ipsec-transform 1 create
    exit
    cert-profile "CertProfile" create
        entry 1 create
            cert 10.1.5.129
            key NOKIA_KEY
            send-chain
                ca-profile "ICA"
            exit
        exit
        no shutdown
    exit
    trust-anchor-profile "RootCA" create
        trust-anchor "CA"
    exit

----------------------------------------------
```

```
config>service>vprn>if>sap
----------------------------------------------
ipsec-tunnel "Strongswan-Interconnect" create
      security-policy 1
      local-gateway-address 10.1.5.129 peer 10.1.11.2 delivery-service 3
      dynamic-keying
        ike-policy 1
        transform 1
        cert
          trust-anchor-profile "RootCA"
          cert-profile "CertProfile"
        exit
      exit
      no shutdown
    exit
  exit
exit
```

4. Certificate Revocation Check

- A revocation check is a process that checks whether a certificate has been revoked by the issuer CA. The 7705 SAR supports revocation check using CRL (as specified in RFC 5280 Section 6.3).
- The CRL can be used for both EE and CA certificate checks. By default, the system uses the CRL to check the revocation status of a certificate, whether it is an end entity certificate or a CA certificate. This makes the CRL a mandatory configuration in the ca-profile.
- In CC mode, the audo-crl-update must be enabled (ie. Periodic queries to a remote CRL server should be made by the Nokia SAR 7705 that is in the CC evaluated configuration).
- If the CRL server is unreachable, the device will not accept the certificates.
- If the issuer is not present, or if the issuer certificate does not have the CA:true flag in the basicConstraints section, the validation fails. The device verifies the validity of the signature. If the signature is not valid, the validation fails. It then confirms that the current date and time is within the valid time period specified in the certificate.

Note:

The 7705 SAR supports CRLs and OCSP for certificate revocation checking. However, in the FIPS-140-2 mode, in the CC evaluated configuration, only CRL server to be used for certificate revocation checks.

5. CRL Configuration

Use a web server (Example Apache 2) to host the CRL files on the CRL server which the Nokia SAR 7705 can then retrieve via HTTP.

Automatic CRL Update Commands

- **crl-update**
  Syntax: crl-update ca *ca-profile-name*
  Context: admin>certificate
  Description: This command manually initiates a CRL update for the specified CA profile.

Automatic CRL update must be shutdown before this command can be issued.
Default: n/a
Parameters: *ca-profile-name* — the name of the CA profile

- **file-transmission-profile**
  Syntax: file-transmission-profile *name* [create]
  no file-transmission-profile name
  Context: config>system
  Description: This command creates a new file transmission profile. The profile can be configured with transport parameters for protocols such as HTTP and additional file transmission options.
  Default: n/a
  Parameters *name* — the file transmission profile name, up to 32 characters
  create — keyword required when first creating the configuration context. When the context is created, you can navigate into the context without the create keyword.

- **auto-crl-update**
  Syntax: auto-crl-update [create]
  no auto-crl-update
  Context: config>system>security>pki>ca-profile
  Description: This command creates the context to configure automatic CRL update parameters. When automatic CRL update is configured and enabled with the no shutdown command, the system downloads a CRL file from a list of configured HTTP URLs, either periodically or before an existing CRL expires. If the downloaded CRL is a valid CRL signed by the CA and is more recent than the existing CRL, the existing CRL is replaced.The no form of this command deletes the automatic CRL update context and any configurations inside it.
  Default: n/a
  Parameters: create — keyword required when first creating the configuration context. When the context is created, you can navigate into the context without the create keyword.

- **crl-urls**
  Syntax: crl-urls
  Context: config>system>security>pki>ca-prof>auto-crl-update
  Description: This command enables the context to configure CRL URL parameters. Up to eight URL entries can be configured under each CA profile. The configured URLs must point to a DER-encoded CRL file. When a CRL update is initiated, the system accesses each URL in order, and the first successfully downloaded and qualified CRL is used to update the existing CRL. If the download fails or the downloaded CRL is not qualified, the system moves to the next URL in the list. If no CRL file is successfully downloaded or qualified, the system attempts to contact each URL again at the next scheduled update time (when the schedule type is configured as periodic) or after the time configured with the retry-interval command (when the schedule type is configured as next-update-based). The CRL download can be manually interrupted by issuing the shutdown command in the auto-crl-update context.
  Default: n/a

- **url-entry**
  Syntax: url-entry *entry-id* [create]

no url-entry *entry-id*

Context: config>system>security>pki>ca-prof>auto-crl-update>crl-urls

Description: This command creates a new CRL URL entry or enters an existing URL entry configuration context.

The no form of this command removes the specified entry.

Default: n/a

Parameters: *entry-id* — the URL entry identifier

Values: 1 to 8

create — keyword required when first creating the URL entry. When the URL entry is created, you can navigate into the context without the create keyword.

- **file-transmission-profile**

  Syntax: file-transmission-profile *profile-name*

  no file-transmission-profile

  Context: config>system>security>pki>ca-prof>auto-crl-update>crl-urls>url-entry

  Description: This command specifies an existing file transmission profile to use when the system downloads a CRL from the configured URL in this URL entry. The profile must already be configured with the config>system>file-transmission-profile command.

  Automatic CRL update supports base, management, or VPRN routing instances. If VPRN is used, the HTTP server port can only be 80 or 8080. The no form of this command removes the file transmission profile name from the URL entry.

  Default: no file-transmission-profile

  Parameters: *profile-name* — the name of the file transmission profile to be used

Example to configure the remote CRL on the device:

- **Configure CRL in the ca-profile:**

```
*A:SARW# configure system security pki
*A:SARW>config>system>security>pki# ca-profile "CA" *A:SARW>config>system>security>pki>ca-profile# info
                    cert-file "CA"
                    crl-file "CA_crl"
                    auto-crl-update create
                        crl-urls
                            url-entry 1 create
                                file-transmission-profile "CA_CRL"
                                url "http://10.1.2.200:80/CA_crl.pem"
                            exit
                        exit
                        no shutdown
                    exit
                    no shutdown
```

11 Setting Time

For CC-NDcPP compliance, time can be manually set. Ensure that NTP client has been disabled. To set the date and time, use the following commands,

Set the system time:

```
*A:SR-xx# admin set-time <YYYY/MM/DD>
```

Example:

```
admin# set-time 2010/09/24 14:10:00
```

Confirm the system time and date:

```
*A:SR-xx# show time
```

Save the provisioned setting to the configuration file:

```
*A:SR-xx# /admin save
```

12 Acronym Table

Table 6 – Acronyms

Acronym	Definition
AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
BOF	Boot Options File
CA	Certification Authority
CBC	Cipher Block Chaining
CC	Common Criteria
CF	Compact Flash
CLI	Command Line Interface
CMAC	Cipher MAC
cPP	collaborative PP
CPU	Central Processing Unit
CRL	Certificate Revocation List
CTR	Counter Mode
DH	Diffie-Hellman
RDBG	Deterministic Random Bit Generator
EP	Extension Package
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
FD	Flexible Data-Rate
FTP	File Transfer Protocol
gRPC	gRPC Remote Procedure Calls
Gb	Giga-bit
GCM	Galois Counter Mode
HMAC	Hash Message Authentication Code
HTTP	Hyper Text Transfer Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP Security
KAT	Known Answer Test
MAC	Message Authentication Code
MACsec	MAC Security
Mb	Mega-bit
MPLS	Multiprotocol Layer Switching
NDcPP	Network Device cPP
NIAP	National Information Assurance Partnership
NTP	Network Time Protocol

Acronym	Definition
OCSP	Online Certificate Status Protocol
OSP	Organizational Security Policy
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PoE	Power Over Ethernet
PoE+	PoE Plus
PP	Protection Profile
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RFC	Request For Comments
RSA	Rivest Shamir Adleman
SAR	Security Assurance Requirement or Service Aggregation Router
SFP	Small Form-Factor Pluggable
SFP+	SFP Plus
SFR	Security Functional Requirements
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SRAM	Static RAM
SAR OS	Service Router Operating System
SSH	Secure Shell
TACACS+	Terminal Access Controller Access-Control System Plus
TCP	Transport Control Protocol
TD	Technical Decision
TOE	Target of Evaluation
TRNG	True Random Number Generator
TSF	TOE Security Function
TSS	TOE Summary Specification