File No. NCCS/HQ/COMSEC/2021-22/III-Part-(2)/612

भारत सरकार/ Government of India

संचार मंत्रालय/Ministry of Communications

दूरसंचार विभाग/Department of Telecommunications

राष्ट्रीय संचार सुरक्षा केंद्र / National Centre for Communication Security

बेंगलुरु - 560027/ Bengaluru – 560027

Date: 14.10.2024

Sub: List of Minimum Pre-conditions and Generic Test Cases for IP Router – Document Version 1.0 – Reg.

Reference is invited to the subject cited above.

2. To facilitate the uniformity in approach of test cases in Security Testing and Certification, NCCS has finalised the enclosed document as a reference methodology for creation of the test cases for Security testing of various network products. The test cases provided in the enclosure are generic in nature and has been prepared as a model document for IP-Router Security testing.

3. The document may be customised by TSTLs to create the test cases for other network products, as applicable. Responsibility to prepare conclusive test plans resides with the TSTLs. The document contains clause wise Test objectives and generic test cases for understanding purpose. However, based on the DUT capability, the actual Test cases and Pre-conditions may vary and Test Plan will be created by the TSTL accordingly in liaison with applicants/OEMs of the product. Additionally, based on the DUT Capability, TSTL may add additional Test Cases for conclusive Testing of the DUT.

4. It may be noted that TSTP format earlier shared by NCCS to the TSTLs shall be read in conjunction with these test cases. The relevant details in the prescribed format have to be enclosed accordingly. The other conditions are mentioned in the document.

This issues with approval of the Sr. DDG NCCS.

Encl: As Above

Rama Krishna Majety

Digitally signed by Rama Krishna Majety
Date: 2024.10.14 18:25:42 +05'30'

(Rama Krishna Majety)

Director(SC&HQ), NCCS

To:

(i) Designated TSTLs - through NCCS website

(ii) OEMs for their reference- through NCCS website. OEMs may provide necessary command set and explanatory note to TSTLs to facilitate for creation of test cases.

Copy to:

(I) All officers of NCCS

List of Minimum Pre-conditions and Generic Test Cases for IP Router - Document Version 1.0

Introduction

1. This document is prepared by NCCS as a reference methodology for creation of the test cases for Security testing of various network products. The test cases provided here are generic in nature and has been prepared as an example for IP-Router Security testing. The document may be customised by TSTLs to create the test cases for other network products, as applicable. Responsibility to prepare conclusive test plans resides with the TSTLs.
2. The document contains clause wise Test objectives and generic test cases for understanding purpose. However, based on the DUT capability, the actual Test cases and Pre-conditions may vary and Test Plan will be created by the TSTL accordingly. Additionally, based on the DUT Capability, TSTL may add additional Test Cases for conclusive Testing of the DUT.
3. While submission of Test plan, TSTL need to include the command also which shall be used for testing that clause.
4. It may be noted that TSTP format earlier sent by NCCS to the TSTLs shall remain the same. The relevant details in the prescribed format has to be enclosed accordingly.
5. While submission of Test reports, relevant clear screenshots/Evidences pertaining to the relevant clause testing is to be included

Sr. No.	CSR No	ITSAR Requirement Heading	Test Objective	Minimum Pre-conditions and Test cases required	Any other remarks	OEM documentation
1	1.1.1	Management Protocols Mutual Authentication	Based on the OEM Documentation regarding DUT Supported Management Protocols, checking of mutual authentication for all such protocols is required.	**Pre-conditions:** Review OEM Documentation that lists all of the management protocols and describes the authentication mechanism used for each one. List is to be furnished with the test report. Based on outcome of OEM Documentation 1. Test case to verify DUT Supports authentication attribute (password, certificates, keys, etc.,) of management protocol 1 2. Test case to verify DUT Mutual authentication of Management protocol 1 3. Test case to verify DUT Mutual authentication fails for Management protocol 1 when incorrect authetication attribute in provided. Test 1 to 3 to be completed for Management protocol 2 to N (total Number of supported protocols by DUT) on all interfaces of DUT	Reference to OEM Documentation to be recorded with Test report	List of all the management protocols supported by DUT and the details of authentication mechanism used for each one.
2	1.1.2	Management Traffic Protection	Traffic from Network Product's OAM interface to be protected using Secure cryptographic controls as provided in Cryptogrphic control ITSAR	**Pre-conditions:** Review Network product documentation containing information about supported OAM protocols provided by the vendor. List is to be furnished with the test report. Based on outcome of OEM Documentation 1. Test case to verify OAM Protocol 1 communicates securely using Cryptographic control as provided in Crypto control ITSAR 2. Test case to verify OAM Protocol 1 communication fails when attempting secure communication using lower Cryptographic control compared to the controls provided in Crypto control ITSAR 3. Test case to verify OAM Protocol 1 communication fails when attempting communication without using encyption. Test 1 to 3 to be comepleted for OAM protocol 2 to N (total Number of supported OAM protocols) on all interfaces of DUT	TLS versions are per Annx E of 33.310	Lis of supported OAM protocols in the DUT.
3	1.1.3	Role-Based access control	To verify the DUT Supports creation of Role Based access controls with minimum 3 RBACs.	**Pre-conditions:** Review OEM Documentation for available RBAC Support and list 1. Test case to Create minimum 3 user accounts with different priviledges/RBAC 2. Test case to verify Operations allowed to a particular role is succesful. 3. Test case to verify Operations not allowed to a particular role is not permitted by the DUT 4. Test case to verify a lower priviledged user/RBAC is not able to escalate its priviledge/assign itself a different role.		1. Available RBAC Support and list of such Roles 2. Process/Command to create User account in DUT
4	1.1.4	User Authentication – Local/Remote	The various user and machine accounts on a system shall be protected from misuse.	**Pre-conditions:** 1. OEM Documentation for pre-defined user and machine accounts and list both separately and usage of authentication attributes supported by the DUT 2. OEM Documentation for creation of user and machine accounts and usage of authentication attributes supported by these accounts Based on 1 & 2 above: 3. Test case to verify DUT access login using correct authetication attribute 4. Test case to verify DUT access login using incorrect authetication attribute Testcases 3 & 4 to be repeated for local/remote access for each type of pre-defined/new user and machine accounts as per 1 & 2 above. Test case 5: Test case to verify that authentication based on parameters which can be spoofed and check the response from DUT.		Separate list for pre-defined user and machine accounts and usage of authentication attributes supported by these accounts , as supported by DUT.

Sr. No.	CSR No	ITSAR Requirement Heading	Test Objective	Minimum Pre-conditions and Test cases required	Any other remarks	OEM documentation
5	1.1.5	Remote login restrictions for privileged users	To verify root user is not able to access DUT Remotely	**Pre-conditions:** OEM Documentation for method to create and access root and highest priviledged user account locally and remotely 1. Test case to verify DUT console login with root and/or highest privileged account. 2. Test case to verify DUT remote login with root account.		Methods to create and access root and highest priviledged user account locally and remotely
6	1.1.6	Authorization Policy	Verification of the authorization policy of the user and their roles	**Pre-conditions:** OEM Documentation detailing authorization policy of the users and their roles Testcases to cover this authorisation policy to be added by TSTL		Authorization policy of the users and their roles in the DUT
7	1.1.7	Unambiguous identification of the user & group accounts removal	Ensure unambigous identification of User accounts and policy on Group accounts	**Pre-conditions:** Test case to verify the kind of unique identifier or user/machine accounts utilised by the DUT from Documentation 1. Test case to verify multiple accounts creation with Same/existing unique identifier is not permitted by the DUT 2. Test case to verify group account policy of the DUT from the documentation. 3. Test case to verify two new users do not belong to same group by default.		Information about the unique identifier or user/machine accounts and group account policy of the DUT
8	1.2.1	Authentication Policy	To Ensure that system functions cannot be accessed without successful authentication and authorization."	Based on the list of access methods available in DUT, proceed with the following: 1: Test case to verify that access to system functions and network services is granted only after successful authentication with a username and at least one attribute (e.g., password, token, certificate). 2: Test case to repeat point 1 for all access methods listed in the OEM documentation . 3: Test case to repeat the point 1 and 2 for remote access methods listed in 1 output. 4: Confirmation to be sought from OEM for requirement of any function for public use.If such available, may be checked by accessing the same without authentication.		List of Access Methods available in DUT
9	1.2.2	Authentication Support – External	When the DUT supports an external authentication server, test whether the communication between the DUT and the AAA server is secure by Test case to verifying if it is encrypted/secured using Crypto controls as defined in ITSAR Crypto controls	Pre-conditions: Review the OEM documentation to identify and list out all the external authentication servers supported by the DUT. 1: Test case to Configure one of the supported AAA servers on the DUT and establish a connection between the DUT and the AAA server. Use a network packet analyzer To verify whether the communication between the DUT and the AAA server is secured (encrypted) using Crypto controls as defined in ITSAR Crypto controls 2: Test case to verify whether the communication between the DUT and the AAA server is possible without encryption. 3: Test case to repeat from OEM documentation for each of the AAA servers supported by the DUT.		List of all the external authentication servers supported by the DUT.
10	1.2.3	Protection against brute force and dictionary attacks	To ensure that the system employs a mechanism with sufficient protection against brute force and dictionary attacks.	1: Test case to verify if the DUT has a timeout delay implemented after multiple incorrect password input 2: Test case to verify if the DUT locks the user account after multiple incorrect password attempts. 3: Test case to verify if CAPTCHA is implemented for authentication during login through the GUI or web application 4: Test case to verify if a vulnerable password blacklist is present in the DUT,this can be done by Test case to verifying password policy, checking for blacklisted passwords, comparing DUTs blacklist with standard vulnerable password list(eg., NIST) 5: Test case to conduct a brute force attack on the DUT (both CLI and GUI). If the attack is successful, the DUT does not meet this requirement. 6: Test case to conduct a dictionary attack on the DUT (both CLI and GUI). If the attack is successful, the DUT does not meet this requirement. Above Test is to be performed for default users, admin, and superuser.	5, 6 and any two test cases from 1 to 4 must pass for the DUT to meet this requirement	
11	1.2.4	Enforce Strong Password	To verify that the password structure meets the password complexity criteria	1: Test case to Create a user with password length less than 8, the DUT should deny it 2: Test case to Configure a password policy with password length greater than 8 and with greater complexity as defined in the ITSAR. 3: Test case to Conduct a positive and Test case Test case to verifying the implementation of the above policy by creating a new user and also while a user changes his password 4: Test case to Check if the password complexity rules are configurable by the admin and also Test case to verify if the absolute minimum length of the password is configurable to a value lesser than 8. 5: Test case to check if central authentication system is supported by DUT, then configure the password policy in the central authentication system and Test case to verify if the password complexity meets this requirement by performing with 1 ,2,3 and 4.		1.Method to Configure Password Policy in DUT 2. Confirmation from OEM whther DU if central authentication system is supported by DUT

Sr. No.	CSR No	ITSAR Requirement Heading	Test Objective	Minimum Pre-conditions and Test cases required	Any other remarks	OEM documentation
12	1.2.5	Inactive Session Timeout	To ensure that an OAM user interactive session is terminated after an inactivity timeout. Additionally, make sure that the inactivity timeout is configurable by the OAM user	1:Test case to log in to an OAM session through both CLI and Web GUI. Check if the inactivity session timeout occurs in both cases. Perform this for both local and remote OAM logins. 2: Test case to verify if the inactivity session timeout period is configurable by the OAM user account. 3: Test case to configure the DUT with a specific inactivity time out period and Test case to verify from the logs if the session log out takes place after inactivity for configured time-out period.		
13	1.2.6	Password Changes	i. To verify that the DUT allows users to change the authentication attribute at any time. ii. Ensure the DUT enforces a password change after the initial login. iii. Confirm that the new password complies with the password management policy and check for a password expiry rule. iv. Ensure the DUT is configuredo to disallow configured number of previously used passwords (Password History). v. To verify that the new password adheres to the password management policy	1: Test case to verify whether the DUT allows the user to change the password/authentication attribute at any time. 2: Test case to verify if the DUT forces the user to change the password/authentication attribute after the initial login. 3: Test case to Check if the DUT enforces a password expiry policy, such as notifying the user to change the password before expiry time as configured. 4: Test case to Check whether the DUT allows configuration of the no.of previously used passwords that are disallowed. And stores atleast last three or more passwords used. DUT should store last 3 passwords by default (before the configuration by operator) 5 : Test case to Check if the DUT allows the last three/configured number of previously used passwords. If it does, the test fails. 6: Test case to Check if the DUT disallows the last three/configured number of previously used passwords. If it does, the test is successful. 7: If any central authentication system is supported by the DUT, Test 1 to 6 are to be performed on all the central authentication systems		
14	1.2.7	Protected Authentication feedback	To verify that password/authentication attribute is not displayed in clear text while entering	1: Test case to enter the password/authentication attribute and Test case to verify that the given password is not visible in clear text. 2: Test case to verify if the password/authentication attribute is displayed is not in clear text during password/authentication attribute change. 1 and 2 must be performed in both CLI and GUI modes		
15	1.2.8	Removal of predefined or default authentication attributes	To check whether DUT forces the user to change default or predefined authentication attributes	**Pre-conditions**:Review the OEM documentation for pre defined users or default authentication attributes (passwords, tokens, cryptographic keys etc.) 1: Test case to perform a factory reset on the DUT. 2: Test case to login with the predefined user credentials, after initial login with the default and pre-defined attributes, Test case to verify whether the DUT forces the user to change the attribute or 3:Test case to verify the OEM documentation for methods to change the pre-defined authentication attributes manually is provided or not. An exception for this is machine accounts		Information about pre defined users or default authentication attributes (passwords, tokens, cryptographic keys etc.)
16	1.3.1	Secure Update	To ensure that DUT perfroming software integrity check before software update/upgrade with proper access control	Precondition : Review OEM documentation for how many modes the DUT can support for software upgrade. Note : Based on the mode of support, perform test on all modes. 1 : Test case to verify that unprivileaged user can not do update/upgrade. 2 : Test case to verify that DUT verifies the hash and signature of image during update/upgrade securely. 3: Test case to verify that DUT does not update/upgrade from corrupted image.		Modes the DUT can support for software update.
17	1.3.2	Secure Upgrade	To ensure that DUT perfroming software integrity check before software upgrade with proper access control	**Precondition :** Review OEM documentation for how many modes the DUT can support for software upgrade. Note : Based on the mode of support, perform test on all modes. 1 : Test case to verify that unprivileaged user can not do update/upgrade. 2 : Test case to verify that DUT verifies the hash and signature of image during update/upgrade securely. 3: Test case to verify that DUT does not update/upgrade from corrupted image.		Modes the DUT can support for software upgrade.
18	1.3.3	Source code security assurance	To ensure that DUT is free from SANS Top 25 and OWASP Top 10 weaknesses.	Precondition : OEM shall submit STD(For source code analysis) of DUT software to the TSTL 1 : Tester has To verify there is no OWASP top 10(latest), SANS top 25(latest) and very high CWE technical impacts(CWSS) related weaknesses in the STD report as per standard SAST/SCA/any other relevant Tools.		STD(For source code analysis) document of DUT software
19	1.3.4	Known Malware Check	To ensure that DUT is free from known malwares.	**Precondition :** OEM shall submit MTD(for malware test document) of DUT software to the TSTL 1: Test case to review of OEM submitted MTD by Tester to ensure that DUT is free from known Malware.		MTD(for malware test document) of DUT software

Sr. No.	CSR No	ITSAR Requirement Heading	Test Objective	Minimum Pre-conditions and Test cases required	Any other remarks	OEM documentation
20	1.3.5	No unused software	To ensure that there is no unused software or associated components that might be installed in the network product which are not required for its operation or functionality.	**Precondition** : Review OEM document for list of available software in the DUT **1** : Test case to verify the OEM document for list of available software in the DUT and validate.		List of all available software in the DUT
21	1.3.6	Unnecessary Service Removal	To ensure that DUT is running only the necessary servicesand there is no known vulnerabilities on that services	**Precondition :** Review OEM documentation of list of all required network protocols and services containing at least the following information shall be included in the documentation accompanying the Network Product: - protocol handlers and services needed for the operation of network product; - their open ports and associated services; - and a description of their purposes. **1 :** Test case to perform port scanning to find the list of services and Reconcile/cross-check with the OEM list **2 :** Test case to view that unsecure services/protocols as detailed in ITSAR are **initially configured as disabled** in the DUT		List of all required network protocols and services containing at least the following information: - protocol handlers and services needed for the operation of network product; - their open ports and associated services; - and a description of their purposes.
22	1.3.7	Restricting System Boot Source	To verify that the DUT can only boot from memory devices intended for this purpose (e.g. not from external memory like USB key).	**Precondition** :Review OEM documentation for the intented mode of boot of its DUT. 1: Test case to check for booting DUT other than the declared intended mode of boot with highest privilige.		List of Intented mode of boot of DUT.
23	1.3.8	Secure Time Synchronization	To ensure that DUT having reliable time sync in a secure manner	**1 :** Test case to change manual Time settings to be done in DUT and check for audit logs for all changes to time settings. Test cases to be made for both privilged user and unprevilged user. **2:**Test case to change time settings to be done in DUT through NTP Server and check for audit logs for all changes to time settings. Test cases to be made for both privilged user and unprevilged user. 3: DUT should support to configure authentication between itself and external NTP server.		

Sr. No.	CSR No	ITSAR Requirement Heading	Test Objective	Minimum Pre-conditions and Test cases required	Any other remarks	OEM documentation
24	1.3.9	Self Testing	To ensure that Firmware, software,cryptographic modules used in the DUT is not tampered	**Precondition** : Review the OEM documentation to check commnads for self-test and methods implemented by OEM to verify the methods applied for firmware, software,cryptographic modules used in the DUT is not tampered. 1 : Test case to to perform Self Test FOR ALL CRYPTO ALGORITHMS, during boot. 2 : Test case to to perform Self Test FOR ALL CRYPTO ALGORITHMS, when the administrator sends command. 3 : Test case to verify that DUT checks the integrity of firmware/software when the administrator sends command. 4 : Test case to verify that DUT checks the integrity of firmware/software during boot.		List of commnads for self-test and methods implemented by OEM to verify the methods applied for firmware, software,cryptographic modules used in the DUT is not tampered.
25	1.3.10	Restricted reachability of services	To verify that it is possible to restrict to the services only to the interfaces from which they are intended.	Precondition : Review the OEM documentation for the list of available management services supported by DUT. List is to be furnished with the test report. 1: Test case to verify that SSH service is available only on the management interface 2: Test To verify that SSH service is unavailable on non-management interfaces point 1 and 2 to be repeated for all management services.		List of available management services supported by DUT
26	1.3.11	Avoidance of Unspecified Wireless Access	To verify the undertaking to ensure that DUT does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel.	Undertaking as per ITSAR Clause 1.3.11 need to be obtained from OEM.		Undertaking from OEM as per ITSAR Clause 1.3.11
27	1.4.1	No unused functions	To ensure that all active hardware functions or software functions are explicitly required for operation or functionality of the network product.	**Pre-conditions:** Review OEM document for list of available software and hardware function in the DUT. 1: Test case to verify if unused functions of software cannot be deleted or de-installed individually as given under requirement "1.3.5 No unused software" of this document, such functions shall be deactivated in the configuration of the Network product Permanently. 2: Test case to verify hardware functions which are not required for operation or function of the system (e.g.,unused interfaces) shall be permanently deactivated.		List of available software and hardware function in the DUT and their usage in DUT
28	1.4.2	No unsupported components	To ensure that all software and hardware components running in the network product are still supported and have not reached either their end-of-life or end-of-support.	1 : Test case to verify manually to verify for End of Support and EoL for all hardware and proprietary/third party software components. 2: Test case for declaration may be obtained from OEM for open-source components.		
29	1.5.1	Audit trail storage and protection	To check whether security event logs are accessible by only priviledged user and also to check whether these log files are not deletable.	**Pre-conditions:**Review OEM documentation describing where logs are stored and how these logs are accessed and also Tester shall mention the details of the users in the DUT and their assigned privileges. What types of log files are stored in DuT ? 1: Test case to attempt to read the security event log files as a privileged user. 2: Test case to attempt to read and delete the security event log file as a lower privileged user. 3 :- Test case to attempt to delete the security event log file as a privileged user.		List of logs storage location and their access methods.
30	1.5.2	Audit Event Generation	To verify that the DuT correctly logs all required security event types listed in the test clause requirement(atleast mandatory events)	1 :- Test case to sequentially triggers each security event listed in the clause requirement and Test case to verify these events and their options were correctly logged.		

Sr. No.	CSR No	ITSAR Requirement Heading	Test Objective	Minimum Pre-conditions and Test cases required	Any other remarks	OEM documentation
31	1.5.3	Secure Log Export	To verify that i. DuT supports securely uploading/forwarding of the security event logging data to an external centralized location . ii. In absence of external system, DuT should have the capability to drop / overwrite old audit data based on defined criteria in case of its own log buffer full. iii. Network product shall alert administrator when its log buffer reaches configured threshold limit.	1 : Test case to verify configuration of external system so that DuT can forward the security event logs to it. 2 : Test case to verify whether the used transport protocol to export logs from DUT to external system is secure protocol as per Cryptographic controls ITSAR. 3 : Test case to verify that the DuT can handle log buffer overflow by dropping or overwriting logs based on defined criteria. 4 : Test case to verify that the DuT alerts the administrator when the log buffer reaches the configured threshold.		
32	1.6.1	Cryptographic Based Secure Communication	To verify the secure communication between the DUT and connected entities	**Pre-conditions:**Review Network product OEM documentation containing information about supported OAM protocols and control plane routing protocols provided by the vendor. List is to be furnished with the test report. Based on outcome of OEM documentation 1 : Test case to verify OAM Protocol 1/Control Plane Routing Protocol 1 communicates securely using Cryptographic control as provided in Crypto control ITSAR 2: Test case to verify OAM Protocol 1 /Control Plane Routing Protocol 1 communication fails when attempting secure communication using lower Cryptographic control compared to the controls provided in Crypto control ITSAR 3 : Test case to verify OAM Protocol 1/Control Plane Routing Protocol 1 communication fails when attempting communication without using encyption. Test 1 to 3 to be comepleted for OAM protocol/Control Plane Routing Protocol 2 to N (total Number of supported OAM protocols) on all interfaces of DUT 4 : Test case to verfiy the secure communication between the DUT and its peer and check if all the cryptographic services are using secure ciphers.		Supported OAM protocols and control plane routing protocols provided by the vendor.
33	1.6.2	Cryptographic Module Security Assurance	To verify the the OEM undertaking given on the security services and the FIPS compliance provided by Cryptographic module embedded inside the Network product	1: Test case to verify the OEM undertaking		OEM underaking
34	1.6.3	Cryptographic Algorithms implementation Security Assurance	To verify the OEM undertaking given w.r.t to the crytographic algorithms in crypto module of DUT	1: Test case to verify the OEM unndertaking		OEM underaking
35	1.6.4	Protecting data and information – Confidential System Internal Data	To verify that no confidentail system internal data is revealed in clear text in any system function	Pre-conditions:Review the OEM documentation To verify the operational and the maintainence mode supported in the DUT and its manual access. 1:Test case to verify no clear password is visible in local console/remote access or in GUI(test case covered in 1.2.7) 2:Test case to verify error logs,trace files and alarms/monitor for reveal of any confidentail system internal data. 3:Test case to verify the configuration file export for any reveal of confidential system internal data 4:Test case to verify the access to maintainence mode by an authorized user		Details of Operational and the maintenance modes supported in the DUT.
36	1.6.5	Protecting data and information in storage	To verify sensitive data are strored in secure manner	**Pre-conditions**:Review the OEM documentation about the sensitive data/files present in the DUT based on the OEM declaration (eg : startup-config , cryptokeys, dB) 1:Test case to verify the access rights of the sensitive files are available only to authorized users. 2:Test case to verify unauthorized manipulation of sensitive system files is not possible. 3: Test case to verify if the sensitive information is stored in hashed or encrypted format.		List of the sensitive data/files present in the DUT (eg : startup-config , cryptokeys, dB) along with list of authorized users with their previlige rights may access this infiormatiom.

Sr. No.	CSR No	ITSAR Requirement Heading	Test Objective	Minimum Pre-conditions and Test cases required	Any other remarks	OEM documentation
37	1.6.6	Protection against Copy of Data	To verify the protection of copy of data in use/in transit	1:Test case to verify the system functions used for copying have been disabled(eg: "cp" , "mv") or available only to priviledged users. 2: Test case to verfiy the data in transit is encrypted		
38	1.6.7	Protection against Data Exfiltration - Overt Channel	To verify only authorized use of outbound overt channels for data exfltration	**Pre-conditions:**Review the OEM documentation to identify the outbound channels supported by the DUT. 1:Test case to verify if unauthorized user can perform outbound data export from the overt channels and check if they are logged. 2:Test case to verify if authorized user can perform outbound data export from the overt channels and check if they are logged.		List of outbound channels supported by the DUT
39	1.7.1	Traffic Filtering – Network Level	i. To verify if DUT hase a mechanism to filter incoming IP packets on any IP interface at network layer and transport layer. ii. To verify if the DUT has ACL policy configurable by the user	1: Test case to Configure any of the IP interface of the DUT with a rule to accept the packet of any network layer protocol (eg: icmp) and check if the DUT accepts the packets from incoming traffic 2: Test case to Configure any of the IP interface of the DUT with a rule to deny the packet of any network layerprotocol (eg: icmp) and check if the DUT accepts the packets from incoming traffic. If the DUT accepts this, then the test fails 3: Test case to repeat 1 and 2 for any of the transport layer protocol (eg: TCP or UDP) 4: Test case to create a specific filtering rule to accept the IP packets and check if the DUT accepts the packets matching the filtering rule. Also Test case to verify the counter for accounting the accepted packets 5: Test case to create a specific filtering rule to deny the IP packets and check whether the DUT denies the packets matching the filtering rule, if it does not then this test case fails 6: Test case to create a specific filtering rule to discard/drop the IP packets and check if the DUT discards/drops the packets matching the filtering rule. Also Test case to verify the counter for accounting the dropped packets 7: Test case to create a specific filtering rule to discard/drop the IP packets and check whether the DUT discards/drops the packets matching the filtering rule, if it does not then this test case fails. 8: Test case to Check if the counter reset mechanism is present 9: Test case to check whether logging of dropped packets can be enabled and disabled. 10: Test case to Configure protocol header specific filtering rule in the DUT and Test case to verify if the DUT is able to filter the packets on the basis of protocol header value received from the IP packets. 11: Test case to Check if the DUT has a mechanism to configure enable or disable defined rules individually.		
40	1.7.2	Traffic Separation	To verify the if there is physical and logical seperation of OAM and control plane traffic	1: Test case to verify the DUT to determine separate interfaces for control plane and management traffic 2: Test case to Configure external tester machines one (PC1) on the management interface and another(PC2) on the control interface. Ping the management interface from PC1 and check if the packets are accepted 3: Test case to verify with the configuration as in 2, Ping the control interface from PC1 and check if the packets are dropped. If this fails, then the test case is failed. 4:Test case to check with the configuration as in 2, Ping the control interface from PC2 and check if the packets are accepted. 5:Test case to check with the configuration as in 2,Ping the management interface from PC2 and check if the IP packets are dropped. If this fails, then the test case is failed.	Illustrative example for 2: Configure two ACL rules (ACL1 and ACL2) (i) ACL1 is to allow packets received from O&M traffic and to deny control plane traffic IF1 (ii) ACL2 is to allow packets received from control plane traffic and to deny O&M traffic on IF2. Enable both the ACLs and check for positive and negative cases. Case2a: Send multiple traffic packets combining O&M packets and control plane packets and check if the counter of the corresponding interface is incremented correctly. Case2b: Send multiple traffic packets combining O&M packets and control plane packets and check if the counter	
41	1.7.3	Traffic Protection –Anti-Spoofing	To verify that DUT shall not process IP packets received from the sources which are unreachable from the incoming IP interface.	1: Test case to make a test setup of DUT and a test machine such that the test machine is reachable from the incoming IP interface. Then test if the packets from the test machine are received by the DUT. 2: Test case to make a test setup of DUT and a test machine such that the test machine is un- reachable from the incoming IP interface. Then test if the packets from the test machine are dropped by the DUT. If this fails ,then the test case is failed.	Test setup can make use of subnetting or loop back or physical disconnection of the test machine	
42	1.8.1	Network Level and application-level DDoS	To verify security measures for network level and application level DDOS prevention to deal with overload situations which may occur as a result of DOS attack/increased traffic.	**Pre-conditions**:Review OEM documentation for the list of security measures available in the DUT from OEM to handle overload situation. 1: Test case to verify each of these available measures on applications like SSH, HTTPS and others using any appropriate tool. 2: Test case to verify each of these available measures for network level on DUT and check the overload condition of traffic through DUT.		List of security measures available in the DUT to handle overload situation.

Sr. No.	CSR No	ITSAR Requirement Heading	Test Objective	Minimum Pre-conditions and Test cases required	Any other remarks	OEM documentation
43	1.8.2	Excessive Overload Protection	To verify that the DUT is behaving in the way it is designed by the OEM for protecting excessive overload in a predictable way. Details of controlled mechanism available in DUT in such extreme cases is to be verified.	**Pre-conditions**:Review OEM documentation for the details of available features in DUT to protect against excessive overload . 1: Test case to verify overload DUT Interface with excessive traffic and assess the performance of DUT whether operating in a predictable way even in excessive overload condition. 2: Test case to verify that under extreme cases test the DUT's performance whether controlled system shut down or any other phenomenon happens which match with the OEM documentation.		List of available features in DUT to protect against excessive overload .
44	1.8.3	Filtering IP Options	To verify that the DUT can filte IP options where IP packets with unnecessary options or extension headers shall not processed.	**Pre-conditions**:Review OEM documentation for the details on Filtering IP options as listed: o The support of filtering capability for IP packets with unnecessary options or extensions headers. – o The actions performed by the network product when an IP packet with unnecessary options or extensions headers is received. o Guidelines on how to enable and configure this filtering capability. 1: Test case to Configures the filtering rule(ACL) on DUT to drop any packets with IP options/extension headers that are enabled and apply the rule to the appropriate interfaces to ensure that the DUT is denying all IP options enabled packets. 2: Test case to send an IPv4/IPV6 packets from the tester machine with an appropriate destination interfaces without setting any IP Options/extension headers the tester verifies that the IP packet is received by the DUT and tester verifies that the corresponding ACK message is sent back. 3: Test case to send IPv4/IPV6 packets from the tester machine an with an appropriate destination interfaces with setting any IP Options/extension headers the tester verifies that the IP packet is received by the DUT and tester verifies that the corresponding ACK message is not sent back. 4: Test case to Configure and apply ACL for handling exceptional requirment of allowing IP options and extension headers.		Details on Filtering IP options for the following is present in DUT or not: a) The support of filtering capability for IP packets with unnecessary options or extensions headers. – b) The actions performed by the network product when an IP packet with unnecessary options or extensions headers is received. cc) Guidelines on how to enable and configure this filtering capability.
45	1.9.1	Fuzzing – Network and Application Level	Test case to verify that externally reachable services are reasonably robust when receiving unexpected input	**Pre-condition:**Review the OEM documentation containing list of protocols supported by the DUT **1: (Curernt configuration for illustration purpose is only for Fuzzer tool Defensics of M/s Synopsis . In case, any other tool is utlised , the underlying principle of testing all protocols remains same):** Tester to fuzz all the available protocols on the DUT. i.Tester shall attach the screenshots of the test-suites/groups interoperability & message sequence selection for validation purpose. ii. Tester shall fuzz all the protocols in full mode with balanced mode execution. However, in case protocol takes more time, validator may decide and testing shall happen as per validator decision on the selection of mode and no of test cases. iii.Instrumentation frequency -1. iv. Timeout for the protocol shall be OEM dependent or as per RFC.		List of protocols supported by the DUT
46	1.9.2	Port Scanning	Test case to verify that on all network interfaces, only documented ports on the transport layer respond to requests from outside the system.	**Pre-conditions:Review OEM documentation for the list of documented ports on transport layer and associated services** **1:**Test case to verify the list the available network services on the documented ports which are necessary for the operation of the DUT. **2:** Test case to perform port scanning to identify open ports and check with the list of documented ports In case of any unknown port is open the same may be recorded.		List of documented ports on Transport layer and associated services
47	1.9.3	Vulnerability Scanning	To perform automated vulnerability scanning on the DUT to check vulnerabilities present in the DUT.	Pre-condition:Vulnerability database of the testing tool should be up-to-date. 1: Test case to conduct a credential based vulnerability scan using a suitable Vulnerability assessment/scanning tool against IP interfaces of the Network Product To verify that there are no known vulnerabilities in the system. 2: Test case to Repeat 1 for web server also Tester shall evaluate the test results based on their severity score. This is required only for vulnerabilities related to cross site scripting and command injection.	Applicable for other network products.If any vulnerabilities are discovered in the DUT, OEM shall provide remediation plan.	

Sr. No.	CSR No	ITSAR Requirement Heading	Test Objective	Minimum Pre-conditions and Test cases required	Any other remarks	OEM documentation
48	1.10.1	Growing Content Handling	To verify that the growing or dynamic content (e.g., log files, uploads) does not influence system functions.	**Pre-condition:** Review the OEM documentation for the storage sources that are susceptible to being exhausted and measures to prevent by the OEM such as **a) Usage of dedicated file systems or quotas for dynamic or growing contents b) File system monitoring.** 1. Test case to enable monitoring of the system operation by configuring syslog server(external or internal). Note: Prority may be given to the internal logging buffer. 2. Test case to initiates the generation of random logs files and monitors the system behaviour on the syslog server until the log file either reaches its quota or until file system is exhausted. While executing this step, flood traffic on available interfaces to check the stability of the device for growing content handling. 3. Test case to check for separation of file systems for main system functions and other functions. 4. Test case to be conducted by uploading a file exceeding the predefined quota. While executing this step, flood traffic on available interfaces to check the stability of the device.		List of storage sources that are susceptible to being exhausted and measures to prevent by the OEM such as a) Usage of dedicated file systems or quotas for dynamic or growing contents b) File system monitoring.
49	1.10.2	Handling of ICMP	To verify that processing of ICMPv4 and ICMPv6 packets which are not required for operation are disabled on the Network product.	**Pre-condition:** Review OEM documentation for ICMP message types which are allowed in addition to permitted ICMP types as per ITSAR. 1.Test case to check for OEM declaration regarding those ICMP message types that are leading to response from DUT or causing configuration changes apart from these- a)Redirect b) Timestamp c) Timestamp reply d) Router solicitation e) Router advertisement . 2. Test case to verify ICMP packet types marked as optional as per the table(1) of ITSAR clause are disabled by default. 3. Test case to verify that ICMP packets types marked as NOT Permitted as per the table (2) of ITSAR clause are blocked.		1.List of ICMP message types which are allowed in addition to permitted ICMP types as per ITSAR. 2. OEM declaration regarding expected DUT behaviour for those ICMP message types that are leading to response from DUT or causing configuration changes
50	1.10.3	Authenticated Privilege Escalation only	To verify that privilege escalation does not take place without authentication.	Pre-conditions:Review OEM documentation for verifying user accounts and their privileges. 1. Test case to login to lower privilege on CLI and GUI of the DUT and try escalating privilege , it should ask for authentication. 2.Test case to exceute commands that require higher privileges from a lower privileged account, it should fail.		List of commands for User accounts and their privileges.
51	1.10.4	System account identification	To verify that each system account has unique identification.	Pre-conditions: Review OEM documentation for verifying user accounts present in the device. 1. Test case to Check that each account has unique identifier. 2. Test case to Create a user account, it should be created with a unique identifier 3. Test case to Create a duplicate user account, the DUT should not permit or it should overwrite the existing credentials.		List of commands for verifying User accounts present in DUT
52	1.10.5	OS Hardening - Kernel Security	To verify that the OS is sufficiently hardened and Kernel based applications / functions not needed for the operation of the Network product are deactivated.	**Pre-conditions:** Review Declaration from the OEM that OS is sufficiently hardened, and Kernel based applications / functions not needed for the operation of the Network product are deactivated. 1.Test case to Check the OEM documentation for kernel based applications/functions needed for operation . Also, review OEM dcumentation for procedure to identify kernel based applications/functions. 2. Test case to List all necessary kernel based applications/functions running in the DUT and Test case to verify it with OEM documentation. 3. Test case toReset the DUT and then Test case to verify that the runninng system processes do not contain by default applications/functions such as a) IP packet forwarding b)Proxy ARP c)Directed broadcast d)IPv4 Multicast handling and e)Gratuitous ARP messages by carrying out test i.ro. each of these from the test machine. 4. Test case if In case any of the features at (3) is running by default, check for OEM declaration supporting their necessity for the operation of the DUT.		1.Declaration from the OEM that OS is sufficiently hardened, and Kernel based applications / functions not needed for the operation of the Network product are deactivated. 2.List of kernel based applications/functions needed for operation. 3.procedure to identify kernel based applications/functions
53	1.10.6	No automatic launch of removable media	To verify automatic launch from removable media is disabled.	**Preconditions:** Review OEM documentation for removable media ports. 1.Test case to Connect removable media to port and Test case to verify that it is not mounted on its own. 2. Test case to Connect removable media to ports and Test case to verify that no application is launched . 3. Test case Either of 1 or 2 shall suffice. 4. Test case to Activation/Deactivation of auto mounting removable media shall be verified.		List of removable media ports
54	1.10.7	External file system mount restrictions	If normal users/non admin are allowed to mount external file systems, OS-level restrictions shall be set properly in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.	**Pre conditions**: Create a normal user in the DUT and mounting privilge may be allowed for that user. 1.Test case to verify if file mounting is applicable for any user, then check that the mounted file system objetcs have inherited same access policies/privileges as that of the user mounting the file systems.		

Sr. No.	CSR No	ITSAR Requirement Heading	Test Objective	Minimum Pre-conditions and Test cases required	Any other remarks	OEM documentation
55	1.11.1	HTTPS	Ensure secure communication between the web client and web server by implementing the specified cryptographic controls from ITSAR and prohibiting null encryption.	1 :Test case to verify that the cryptographic algorithms used in communication between the web client and web server comply with the Cryptographic Controls specified in ITSAR. 2 :Test case to verify whether the web server does not allow NULL encryption. 3 :Test case to verify that the HTTPS protocol is not vulnerable to known attacks, such as the Lucky 13, Breach, sweet 32 vulnerability.		
56	1.11.2	Webserver logging	Test case to verify that all accesses to the webserver are logged with the required information.	**Pre-conditions:**Review OEM documentation which contains information on log file location and procedure to access it 1.Test case to Perform a successful authentication attempt on the web page using correct credentials and Test case to verify that the appropriate logs with clause requirement (Access timestamp,Source (IP address),Account (if known),Attempted login name ,Relevant fields in http request,Status code of web server response) are generated. 2 Test case to Perform an unsuccessful authentication attempt on the web page using incorrect credentials and Test case to verify that the appropriate logs with clause requirement (Access timestamp,Source (IP address),Account (if known),Attempted login name ,Relevant fields in http request,Status code of web server response) are generated.		Information on log file location and procedure to access it
57	1.11.3	HTTP User sessions	Test case to verify that the above 12 session ID and session cookie requirements have been met.	**Pre-conditions:**Review OEM documentation that describes how a session is maintained, where the session ID is stored, how it is communicated, the expiration duration of sessions, and algorithm used to generate the session ID. 1 Test case to verify that each session is assigned a unique session ID that distinguishes it from other active sessions. 2 Test case to verify that the session IDs are unpredictable and cannot be easily guessed. Note: Minimum entropy size =64(As per OWASP current reference) 3 Test case to verify that session ID doesn't contain the sensitive information in clear text. 4 Test case to verify that sessions are automatically terminated after the configured maximum session lifetime.(default set to 8 hours) 5 Test case to verify that Every new login, the new session ID is regenerated. 6 Test case to verify that the network product uses only session cookies and does not use persistent cookies to manage sessions. 7 Test case to verify that the session cookie has secure attributes like HttpOnly, path, and domain set correctly. 8 Test case to verify that session IDs are not passed through GET or POST variables and are only accepted via web server-generated session IDs. 9 Test case to verify that session ID shall not be reused or renewed in subsequent sessions.		1.Procedure for how a session is maintained, where the session ID is stored, how it is communicated, the expiration duration of sessions, algorithm used to generate the session ID.
58	1.11.4	HTTP input validation	Test case to verify DUT shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks	1 Test case to verify identify and list all input fields within the web application.(Example - all forms, search boxes, text inputs, and other interactive fields). 2 Test case to verify that all the input fields in the WEB Application is free from XSS attack. 3 Test case to verify that all the input fields in the WEB Application is free from Command Injection attack. Note: 2 and 3 to be tested with manuall attempt as well as VA Tool with these specific plugins.		
59	1.11.5	No system privileges	Test case to verify that the Web server is not run under system privileges.	**Pre-conditions:** Review OEM documentation confirming that no web server processes run with system-level privileges (e.g., root or administrator). Additionally, the documentation should include commands and procedures to identify the same. 1.Test case to ensure that the web server process is not running under root or system-level privileges by checking the user account under which the web server is operating.		1.List of web server processes run with system-level privileges (e.g., root or administrator). 2. List of user account and its previlige under which the web server is operating
60	1.11.6	No unused HTTP methods	Test case to verify that the Web server has deactivated all HTTP methods that are not required.	**Pre-conditions**: Review OEM documentation for the list of HTTP methods that are required for the web server's operation. 1 Test case to verify that only GET, HEAD, and POST methods are allowed on the web server unless other methods are explicitly required. 2: Test case to verify if additional HTTP methods (besides GET, HEAD, and POST) are required, Test case to verify that they do not introduce security vulnerabilitie		List of HTTP methods that are required for the web server's operation.

Sr. No.	CSR No	ITSAR Requirement Heading	Test Objective	Minimum Pre-conditions and Test cases required	Any other remarks	OEM documentation
61	1.11.7	No unused add-ons	To verify that the Web server has deactivated unneeded add-ons and unneeded scripting components.	**Pre-conditions:** Review OEM documentation for the list of add-ons or scripting tools for Web server components needed for system operation, and that therefore need to be exempted from the test investigation. Additionally, the OEM should provide the path of the configuration file. 1: Test case to verify that any optional components (e.g., scripting modules like PHP, Python, CGI, WebDAV,SSI, plugins) are disabled unless documented as necessary by the OEM.		1.List of add-ons or scripting tools for Web server components needed for system operation, 2. The path of the configuration file of web server
62	1.11.8	No compiler, interpreter, or shell via CGI or other server- side scripting	To verify that there are no compilers, interpreters or shell accessible via CGI or other scripting components.	**Pre-conditions:** Review OEM documentation for the supported scripting technology or CGI used in web server and paths to the directories offered for these CGI or scripting technology used/supported. Additionally OEM provide the path of the installed compiler/interpriter 1 Test case to verify that no compilers or interpreters (e.g., PERL interpreter, PHP interpreter/compiler, Tcl interpreter/compiler, or operating system shells) are present in the CGI or scripting directory.		1. List of Supported scripting technology or CGI used in web server and paths to the directories offered for these CGI or scripting technology used/supported. 2. path of the installed compiler/interpreter
63	1.11.9	No CGI or other scripting for uploads	To test whether the upload directory is equal to the CGI/Scripting directory	**Pre-conditions:** Review OEM documentation for thepaths to the Upload directory, CGI, and scripting directories. 1 Test case to upload a file to the specified Upload directory and verifies that the file is successfully uploaded in the directory provided by the OEM. 2 Test case to verify that the Upload directory is configured to be separate from the CGI/scripting directory, ensuring that uploads do not occur in the CGI/scripting directory. 3 Test case to verify that the web server does not have write permissions for the CGI/scripting directory to prevent unauthorized uploads.		Paths to the Upload directory, CGI, and scripting directories.
64	1.11.10	No execution of system commands with SSI	To test whether it is possible to use the exec directive and if so, whether it can be used for system commands.	**Pre-conditions:** Review OEM documentation indicating the web server configuration settings for SSI if available. 1 Test case to actually attempt to use the exec directive in an SSI file with and without system commands.		Web server configuration settings for SSI if available.
65	1.11.11	Access rights for web server configuration	To verify that the access rights for Web server configuration files are correctly set	**Pre-conditions**: Review OEM documentation about the path to the web server configuration file. 1 Test case to verify Access Rights for Web Server Configuration Files is not available to unprivilage user.		Path to the web server's configuration file.
66	1.11.12	No default content	To verify that there is no default content on the web server, that is not needed for web server operation, since such default content can be useful for an attacker.	**Pre-conditions:** Review OEM documentation about the path to the root directory and all accessible directories of the web server. 1 Test case to verify that the root directory and all accessible directories do not contain any default content.		Path to the root directory and all accessible directories of the web server.
67	1.11.13	No directory listings	To verify that Directory listings / Directory browsing has been deactivated in all Web server components.	**Pre-conditions:** Review OEM documentation about the path to the web server's configuration file, path to the root directory. 1 Test case to verify Directory Browsing is Disabled in configration 2 Test case to verify directory Browsing not possible through web server.		Path to the web server's configuration file, path to the root directory.
68	1.11.14	Web server information in HTTP headers	To verify that HTTP headers do not include information on the version of the web server and the modules/add-ons used.	**Pre-conditions:** Review OEM documentation about the path to the web server's configuration file. 1 Test case to verify that the web server is configured to suppress version information and modules/add-ons information in response headers. 2 Test case to send HTTP requests using all HTTP methods (GET, POST, PUT, DELETE, etc.) and Test case to verify that the response headers do not disclose the web server version. 3 Additionally, use a web server scanner, Ex: Nikto, which is capable of identifying HTTP header misconfigurations.		Path to the web server's configuration file.
69	1.11.15	Web server information in error pages	To verify that error pages and error messages do not include information about the web server.	**Pre-conditions:** Review OEM documentation about the path to the web server's configuration file 1: Test case to verify that default error pages are available in DUT and not disclose version information or internal information. 2: Test case to trigger an error on the web server and confirms that user-defined error pages and error messages do not disclose version information or internal information.		Path to the web server's configuration file.
70	1.11.16	Minimized file type mappings	To verify that file type- or script-mappings that are not required have been deleted	**Pre-conditions:** Review OEM documentation about the path to the web server's MIME configuration file and a list of file types required for the operation of the web server and web applications. 1: Test case to verify that unused mappings, based on the provided list of file types, should be deleted.		Path to the web server's MIME configuration file and a list of file types required for the operation of the web server and web applications.

Sr. No.	CSR No	ITSAR Requirement Heading	Test Objective	Minimum Pre-conditions and Test cases required	Any other remarks	OEM documentation
71	1.11.17	Restricted file access	To test whether the restrictive access rights are assigned to all files which are directly or indirectly in the web server's document directory and To verify whether path traversal is made improbable.	**Pre-conditions:** Review OEM documentation about the path to the web server's configuration file and the web server's document directory. 1: Test case to verify that default access rights for files in the web server's document directory are restrictive. 2: Test case to verify that any new files added to the document directory automatically receive restrictive access rights. 3: Test case to attempt to access files outside the document directory through path traversal		Path to the web server's configuration file and the web server's document directory.
72	1.11.18	Execute rights exclusive for CGI/Scripting directory	To test whether the web server only has execute permissions on the CGI/Scripting directory.	**Pre-conditions:** Review OEM documentation about the path to the web server's configuration file and the web server's document directory. 1 Test case to verify Execute Rights for the CGI/Scripting Directory 2 Test case to verify Non-Execute Rights for Other Content Directories		Path to the web server's configuration file and the web server's document directory.
73	1.12.1	Remote Diagnostic Procedure – Verification	To verify only authorised user are allowed to access DUT remotely for troubleshooting purposes/alarm maintenance and logging of all such activities	**Pre-conditions:** Review OEM documentation to find methodology of remote troubleshooting/alarm maintenance of the DUT 1.Test case to verify remote access of the DUT bu authorised/unauthorised user and Test case to verify DUT records all login attempts and remote configuration changes on the DUT and logs at least following entries like user id, timestamp, interface type, event level , result (if applicable as per troubleshooting guide/alarm maintenance of the DUT)		Methodology of remote troubleshooting/alarm maintenance of the DUT
74	1.12.2	No Password Recovery	In the event of system password reset, the entire configuration of the Network product shall be irretrievably deleted. No provision should exist for password recovery	1. Test case to verify if the DUT configuration is irretrievably deleted in the successful system password reset 2. Test case to verify if the DUT does not support password recovery for system passwords		
75	1.12.3	Secure System Software Revocation	Only authorised user can initiate Rollback of DUT software to previous versions	**Pre-conditions**:Review OEM documentation regarding controlled network software rollback mechanisms deployed in the DUT. 2 Test case to verify that a privileged user can modify the DUT's software image 3 Test case to verify that an unprivileged user cannot modify the DUT's software image		Controlled network software rollback mechanisms deployed in the DUT.
76	1.12.4	Software Integrity Check – Installation	Network product shall install or execute only the software package which are not tampered	1:Test case to verify that the DUT verifies the hash and the signature of image during installation process. 2: Test case to verify that the DUT does not install a tampered image.		
77	1.12.5	Software Integrity Check – Boot	The Network product shall support the possibility To verify software image integrity at boot time	1: Test case to verify that the DUT verifies the hash and the signature of image during boot process. 2:Test case to verify that the DUT does not boot from a tampered image and/or unauthorised software image updates.		
78	1.12.6	Unused Physical Interfaces Disabling	Physically accessible Interfaces which are not under use shall be disabled by configuration that they remain inactive even in the event of a reboot.	Pre-conditions: Review OEM documentation regarding List of the default used Physical Interfaces/Ports shall be given by the vendor 1: Test case to verify the list as per Test 1 that Physical Interfaces/Ports that are necessary for the operation of the Network product are only used by the DUT 2: Test case to verify that the DUT has the ability To verify the physical status of the interfaces 3: Test case to verify that unused interfaces can be shut down by the administrator. 4: Test case to verify physical status of the interfaces remains as configured after a reboot		List of the default used Physical Interfaces/Ports.
79	1.12.7	No Default Profile	Predefined or default user accounts shall be deleted or disabled	1: Test case to verify all Predefined or default user accounts are deleted or disabled		
80	1.12.8	Security Algorithm Modification	protection against a downgrade attack/bidding down attack	1: Test case to verify all DUT denies establishment of remote session requesting communication with weaker ciphers compared to the stronger ciphers which are configured in the DUT for communication		
81	1.12.9	Control Plane Traffic Protection	Control plane traffic shall be protected in the Network product using standard cryptographic mechanisms	**Pre-conditions:** Review OEM documentation regarding List of the control plane traffic protocols supported by the DUT 1. Test case to verify DUT control plane traffic uses secure protocols as per crypto controls detailed in CRYPTO controls ITSAR 2. Test case to verify Control plane traffic flow fails when weak ciphers or null ciphers are used.		List of the control plane traffic protocols supported by the DUT

Sr. No.	CSR No	ITSAR Requirement Heading	Test Objective	Minimum Pre-conditions and Test cases required	Any other remarks	OEM documentation
82	2.1	Audit event generation	The logs shall be generated and verified for the following events: ACL Violation, Attempts to initiate manual/initiate/Complete software updation, All authentication and identification mechanisms	1.Test case to Configure ACL, apply ACL on respective Interfaces and Test case to verify the logs. Generate traffic which will be affected by this ACL and Test case to verify the logs. 2. Test case for the following shall be designed to perform and identify the logs generated. a. manual/Initiate/Complete the software update b. Available methods of Identification and Authentication mechanisms Test case to verify logs for these events both positive and negative cases.	Each test case shall comprise: 1. Configuration of ACL 2. Event creation for generating logs. 3. Checking the logs and counters. Identify all types of Identification/Authentication mechanisms and similar test cases shall be conducted for each of them for Successful and Unsuccessful authentication.	
83	2.2	Audit data protection	Log files shall be protected only for privileged users and shall not be deletable. Even by the Administrator.	1. Test case for privileged user accessing the log 2. Test case for Privileged user attempting the deletion of logs 3. Test case for Unprivileged user attempting to access the logs. 4. Test case for Administrator attempting the deletion of logs	For each case, screenshot of successful login and log details is allowed to view has to be captured. Log screenshot for the successful/unsuccessful attempts of deleting the log files.	
84	2.3	Control Plane Traffic Protection	Control plane traffic (Routing Tables, forwarding tables, MAC tables, Crypto Algorithm/Key Negotiation) shall be secured and DUT shall be capable of sharing this traffic on selective interfaces	Control Plane Traffic security shall be checked for the following cases: 1. Test case to configure Key authentication for DUT and peer router and Check the successful updation of Routing Table from logs. 2. Test case to Configure changed key in Peer router and check the rejection of routing table from logs. 3. Test case to Configure selected interface as passive and check routing table is shared through this interface or not 4. Repeat above *three* cases for RIP, OSPF, BGP, etc. 5. Test cases for prefix-lists for filtering the control plane traffic shall be tested for RIP, BGP and OSPF, etc.	List of Dynamic protocols DUT supports may be obtained from OEM. Screen shots of logs also shall be taken. Screenshots of failure cases also to be included.	List of Dynamic protocols supported by DUT
85	2.4	Traffic Filtering – Network Level	Filtering the traffic based on network attribute like Source IP/Port and Dest IP/Port, Header Flags etc. Filtering based on Access type like Telnet, SSH.	Test case to verify the Network level Traffic Filtering shall be tested by: 1. Port/IP/Header filtering for IPv4 and Ipv6. 2. Access type SSH, HTTP/S, Telnet shall be filtered on an interface	ACLs can be configured for each test case. All available access types shall be checked with screenshots of negative and postive results.	
86	2.5	Traffic Filtering – Applications and Services	Permitting/restricting the application services on configured interfaces: HTTP, OSPF, PING, BGP, RIP, SSH, TELNET etc.	1.Test case to verify the Configure DUT's interface for restricting each service and check the service is available from this interface or not. Simultaneously the service shall be permitted from other interfaces. Test cases shall be designed to include each of all available services.	Screenshots of failure and success service accesses can be captured.	
87	2.6	Data Plane Traffic Protection	DUT shall have the capability of filtering the Data plane traffic. ACL for URPF, prevent IP Spoofing, Blocking ICMP traffic, Filter packets with IP Options, Disable With IP Source routing option. etc. to be checked.	1. Test case to configure ACL for each operation listed below. 2. Test case to verify the filtering shall be conducted and screenshots shall be captured. The following cases shall be tested: a. Header manipulation b. Traffic filtering with IP Options c. Low TTL Blocking d. IP Spoofing Blind and No-blind and discard them. e. Traffic filtering and identifying services like Windows IIS, Https, ssh, telnet, ICMP etc. f. Preventing the URPF traffic. g. IP Source routing.	Configure ACL for blocking each case on respective Interfaces. Check the logs and packet counts. Tools like Scapy can be used to design script for modifying the Port, Header etc.	
88	2.7	NAT (Network Address Translation) services support	To check NAT capability is available in DUT. If NAT is available necessary protection mechanism against the NAT traversal attack and Pin Hole attack is available in the DUT.	**Pre-condition:** Review OEM documentation whether DUT has NAT Capability and if yes, details of the protection mechanism against NAT Traversal attacks and pin hole attack shall be informed. 1: Test case to check availability of NAT in the DUT. NAT shall be configured in DUT if available and test the traffic. 2: Test case to verify the protection of the DUT from NAT Traversal attack and Pin Hole attack shall be checked.	Test can be done simulating NAT traversal attack and Pin Hole Attack	Declaration for the Availability of NAT Capability in DUT

Sr. No.	CSR No	ITSAR Requirement Heading	Test Objective	Minimum Pre-conditions and Test cases required	Any other remarks	OEM documentation
89	2.8	IP Sec VPN support	To Check ISAKMP/IKEv2 and IP Sec VPN support available in DUT. Site to site VPN only shall be available. Remote access VPN as a server and many clients shall not be available.	**Pre-condition**: Review OEM documentation for the availability of ISAKMP/IKEv2 and IP Sec VPN support in DUT 1.. Test case to configure ISAKMP, IPSec VPN shall be configured for two hosts connected through the DUT or optionally through another peer router and perform the test whether the host to host has encrypted VPN service or not.	Tester can inspect the packets before configuring VPN and after configuring VPN. Relevant screenshots shall be captured.	Declaration for the Availability of ISAKMP/IKEv2 and IP Sec VPN support in DUT.
90	2.9	Access Banners	To Check access banner is available in the DUT where a warning for unauthorised usage can be displayed, before the starting of session.	1.Test case to initiate a user session and check the availability of Banner and whether this banner is configurable for an advisory warning about the legitimate usage of the DUT		
91	2.10	Inter-VLAN Routing support	Inter-VLAN routing functionality by default is not permitted, only permitted configuration by administrator.	VLANs shall be configured and routed through the DUT. 1: Tester shall check the routing between these VLANS and check the reachability. 2: Tester shall login as administrator and configure routing between these VLANs and check the reachability. 3: Tester shall login as a user without sufficient privileges and repeat the 2 for negative case.		
92	2.11	Router updates security	DUT shall have the capability to accept or reject the Inter AS route update for preventing the Routing Table Poisoning. This privilege shall be available with only privileged user.	1.Test case to verify if a facility of Inter AS Route update in BGP is available with only privileged user. 2: Test case to verify is it possible to accept and reject the Inter AS Route update with privileged access rights. 3: Test case to verify a negative case of Inter AS route update by logging in as an unprivileged user.		