Indian Telecom Security Assurance Requirements (ITSAR)

भारतीय दूरसंचार सुरक्षा आश्वासन आवश्यकताएँ (भा.दू.सु.आ.आ.)

Network Next Generation Firewall including IDS & IPS

ITSAR Number: ITSAR112062503
ITSAR Name: NCCS/ITSAR/Core Equipment/Security Systems/Network Next Generation Firewall including IDS & IPS

Date of Release: 05.03.2025
Date of Enforcement:

Version: 1.0.0

MTCTE के तहत जारी:
Issued under MTCTE by:

राष्ट्रीय संचार सुरक्षा केंद्र (रा.सं.सु.कें.)
दूरसंचार विभाग, संचार मंत्रालय
भारत सरकार
सिटी दूरभाष केंद्र, एसआर नगर, बैंगलोर-५६००२७, भारत

National Centre for Communication Security (NCCS)
Department of Telecommunications
Ministry of Communications
Government of India
City Telephone Exchange, SR Nagar, Bangalore-560027, India

About NCCS

National Centre for Communication Security (NCCS), with headquarters at Bengaluru was set up in 2018 with the objective to establish and operationalize a framework of security testing and certification within the country. NCCS is mandated to prepare Telecom security requirements/standards called Indian Telecommunication Security Assurance Requirements (ITSAR) that addresses the country specific security needs in telecommunication landscape and notify the same.

Document History

	Title	ITSAR No.	Version	Date of Release	Remark
1.	Network Next Generation Firewall including IDS & IPS	**ITSAR112062503**	1.0.0	05.03.2025	First Release

Table of Contents

A) Outline

The objective of this document is to present comprehensive, country-specific security requirements for the Network Next Generation Firewall including IDS & IPS. These requirements are designed to protect network infrastructure by preventing unauthorized access, detecting and mitigating threats, and ensuring secure communication channels. The Next Generation Firewall supports advanced security features to provide robust protection against unauthorized access and cyber threats while enabling secure communication within the network.

The specifications developed by various regional/international standardization bodies/organizations/associations like NIST, ENISA, 3GPP, Telecommunications Standards Development Society of India (TSDSI) et. al. along with the country-specific security requirements are the basis for this document. The Telecommunication Engineering Centre (TEC)/ TSDSI references made in this document implies that the respective clause has been adopted as it is or with certain modifications.

This document commences with a brief description of the firewalls, types of firewalls followed by a brief about next generation firewalls, its functionalities and then proceeds to address the common and entity specific security requirements of Network Next Generation Firewall including IDS & IPS.

B) Scope

This document targets on the security requirements of the Network Next Generation Firewall including IDS & IPS. Remote Access regulations are governed by the Licensing Wing of the Department of Telecommunications (DoT).

C) Conventions

1. Must or shall or required denotes the absolute requirement of a particular clause of Indian Telecom Security Assurance Requirements (ITSAR).
2. Must not or shall not denote absolute prohibition of a particular clause of ITSAR.
3. Should or recommended denotes that the particular clause of ITSAR may be ignored under justifiable circumstances but after careful examination of its implications.
4. Should not or not recommended denotes the opposite meaning of (3) above.

Chapter 1 – Overview

1.1 Firewall

A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Its primary purpose is to create a barrier between a trusted internal network and untrusted external networks, such as the internet. Traditional firewalls operate by filtering traffic based on IP addresses, port numbers, and protocols. They can block unauthorized access while permitting legitimate communication.

1.2 Types of Firewalls

Firewalls are essential components of network security, designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. There are several types of firewalls, each serving different security needs. Packet-filtering firewalls examine packets at a basic level, checking source and destination addresses, ports, and protocols to allow or block traffic. Stateful inspection firewalls go a step further by tracking the state of active connections and making decisions based on the context of the traffic. Proxy firewalls, also known as application-level gateways, act as intermediaries between users and the internet, filtering traffic at the application layer for enhanced security**.** Next-generation firewalls (NGFWs) combine traditional firewall capabilities with additional features like intrusion prevention systems and deep packet inspection to provide more comprehensive protection. Additionally, firewalls can be categorized by their deployment method, such as hardware firewalls, which are physical devices protecting entire networks, and software firewalls, which are installed on individual devices to safeguard them from threats.

Next-Generation Firewall (NGFW)

With the evolution of cyber threats and the increasing complexity of network environments, traditional firewalls have become insufficient. They were primarily designed to handle straightforward traffic filtering and lacked the capability to inspect deeper into the data packets for more sophisticated threats. This gap led to the development of more advanced solutions, paving the way for Next-Generation Firewalls (NGFWs).
A Next-Generation Firewall (NGFW) is an advanced form of firewall technology that provides comprehensive network security by integrating traditional firewall capabilities with additional features. NGFWs offer a deeper level of inspection and are designed to address the limitations of traditional firewalls. They incorporate a variety of advanced functionalities to better protect modern networks from complex and evolving threats.

1.3 Salient Features

a. Application Awareness: Manages and controls traffic based on specific applications
b. Integrated IPS: Detects and prevents network attacks with intrusion prevention capabilities.
c. Deep Packet Inspection: Analyzes actual content of data packets for accurate threat detection.
d. Advanced Malware Protection: Detects and blocks malware using threat intelligence and sandboxing.
e. SSL/TLS Inspection: Decrypts and inspects encrypted traffic to uncover hidden threats.
f. User Identity Awareness: Applies security policies based on user identities and roles.
g. Threat Intelligence: Integrates global threat intelligence feeds to protect against emerging threats.
h. Multi-function Security: Combines firewall, antivirus, and IPS in one device for simplified management.
i. High Performance: Handles high network throughput and scales with organizational needs.
j. Centralized Management: Provides unified management interfaces and detailed reporting.

1.4 Placement of Firewalls in Network Architecture

Firewalls play a crucial role in network architecture by acting as a gatekeeper between different network segments. Typically, firewalls are strategically placed at key points within a network to control and monitor traffic between trusted internal networks and untrusted external networks, such as the internet. Here are some common placements of firewalls within network architecture:

a. **Perimeter Firewall:** Positioned at the network boundary, it acts as the first line of defense against external threats. It controls traffic entering and leaving the network, ensuring that only legitimate traffic is allowed.

b. **Internal Firewall:** Deployed between internal network segments to control and monitor traffic within the organization. This helps in segmenting the network and protecting sensitive areas from internal threats.

Chapter 2 – Common Security Requirements

Section 2.1: Access and Authorization

2.1.1 Management Protocols Mutual Authentication

Requirement:

Next Generation Firewall shall support mutual authentication of entities on management interfaces, the authentication mechanism can rely on the management protocols used for the interface or other means.

Secure cryptographic controls prescribed in Table 1 of the latest document "Indian Telecom Security Assurance Requirements (ITSAR) for Cryptographic Controls" shall only be used for Next Generation Firewall management and maintenance".

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. Section 4.2.3.4.4.1]

2.1.2 Management Traffic Protection

Requirement:

Next Generation Firewall management traffic (information exchanged during interactions with OAM) shall be protected strictly using secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR For Cryptographic Controls" only.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. Section 4.2.3.2.4]

2.1.3 Role-based access control policy- *Local/Remote*

Requirement:

Next Generation Firewall shall support Role-Based Access Control (RBAC). A role-based access control system uses a set of controls that determines how users interact with domains and resources. The RBAC system controls how users or groups of users are allowed access to the various domains (the domains could be Fault Management, Performance Management, System Admin, etc.) and what type of operation they can perform, i.e. the specific operation command or command group (e.g., View, Modify, Execute). Next Generation Firewall shall

support RBAC with a minimum of 3 user roles, in particular, for OAM privilege management for Next Generation Firewall Management and Maintenance, including authorization of the operation for configuration data and software via the network product console interface.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.2.3.4.6.2]

2.1.4 User Authentication – Local/Remote

Requirement:

The various user and machine accounts on a system shall be protected from misuse. To this end, an authentication attribute is typically used, which, when combined with the username, enables unambiguous authentication and identification of the authorized user.

Authentication attributes include
- Cryptographic keys
- Token
- Passwords

This means that authentication based on a parameter that can be spoofed (e.g., phone numbers, public IP addresses or Virtual Private Network (VPN) membership) is not permitted. Exceptions are attributes that cannot be faked or spoofed by an attacker. Minimum two of the above Authentication attributes shall be mandatorily combined for protecting all the accounts from misuse. An exception to this requirement is local access and machine accounts where at least one authentication attribute shall be supported

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. Section 4.2.3.4.2.1]

2.1.5 Remote login restrictions for privileged users

Requirement:

Direct Login to Next Generation Firewall as root or equivalent highest privileged user shall be limited to the system console only. Root user will not be allowed to login to Next Generation Firewall remotely.

This remote root user access restriction is also applicable to application software's / tools such as TeamViewer, desktop sharing which provides remote access to the Next Generation Firewall.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.3.2.6]

2.1.6 Authorization Policy- *Local/Remote*

Requirement:

The authorizations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform.

Authorizations to a system shall be restricted to a level in which a user can only access data and use functions that he needs in the course of his work. Suitable authorizations shall also be assigned for access to files that are components of the operating system or of applications or that are generated by the same (e.g., configuration and logging files).

Alongside access to data, execution of applications and components shall also take place with rights that are as low as possible. Applications shall not be executed with administrator or system rights.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.2.3.4.6.1]

2.1.7 Unambiguous identification of the user & group accounts removal

Requirement:

Users shall be identified unambiguously by the Next Generation Firewall. Next Generation Firewall shall support the assignment of individual accounts per user, where the user could be a person, or, for Machine Accounts, an application, or a system. Next Generation Firewall shall not enable the use of group accounts or group credentials, or sharing of the same account between several users.

[Ref [3]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.1.2]

Section 2.2: Authentication Attribute Management

2.2.1 Authentication Policy

Requirement:

The usage of a system function without successful authentication on the basis of the user identity and at least two authentication attributes shall be prevented. For machine accounts

and local access one authentication attribute will be sufficient. System functions comprise, for example network services (like Secure Shell (SSH), Secure File Transfer Protocol (SFTP), Web services), local access via a management console, local usage of operating system and applications. This requirement shall also be applied to accounts that are only used for communication between systems.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. Section 4.2.3.4.1.1]

2.2.2 Authentication Support – External

Requirement:

If the Next Generation Firewall supports external authentication mechanism such as AAA server (for authentication, authorization and accounting services), then the communication between Next Generation Firewall and the external authentication entity shall be protected using the authentication and related service protocols built strictly using the Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

2.2.3 Protection against brute force and dictionary attacks

Requirement:

Protection against brute force and dictionary attacks that hinder authentication attribute (i.e., password) guessing shall be implemented in Next Generation Firewall. Brute force and dictionary attacks aim to use automated guessing to ascertain authentication attributes for user and machine accounts.

Various measures or a combination of the following measures can be taken to prevent this: Using the timer delay (this delay could be the same or increased depending on the operator's policy for each attempt) for each newly entered password input following an incorrect entry ("tar pit").

a) Blocking an account following a specified number of incorrect attempts. However, it has to be taken into account that this solution needs a process for unlocking and an attacker can force this to deactivate accounts and make them unusable.
b) Using an authentication attribute blacklist to prevent vulnerable passwords.
c) Using Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) to prevent automated attempts (often used for Web applications). In order to achieve higher security, two or more of the measures indicated above shall be mandatorily supported by Next Generation Firewall. An exception to this requirement is machine accounts

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. Section 4.2.3.4.3.3]

2.2.4 Enforce Strong Password

Requirement:

a) The configuration setting shall be such that Next Generation Firewall shall only accept passwords that comply with the following complexity criteria:
    i) Absolute minimum length of 8 characters (shorter lengths shall be rejected by the Next Generation Firewall). It shall not be possible setting this absolute minimum length to a lower value by configuration.
    ii) Password shall mandatorily comprise all the following four categories of characters:
        1) At least 1 uppercase character (A-Z)
        2) At least 1 lowercase character (a-z)
        3) At least 1 digit (0-9)
        4) At least 1 special character (e.g., @, $., etc.)
b) The minimum length of characters in the passwords and the set of allowable special characters shall be configurable by the operator. The special characters may be categorized in sets according to their Unicode category.
c) If a central system is used for user authentication password policy, then additional assurance shall be provided that the central system enforces the same password complexity rules as laid down for the local system in this sub-clause.
d) If a central system is not used for user authentication, the assurance on password complexity rules shall be performed on the Next Generation Firewall.
e) When a user is changing a password or entering a new password, Next Generation Firewall/central system checks and ensures that it meets the password requirements. Above requirements shall be applicable for all passwords used (e.g., application-level, OS-level, etc.).
f) Passwords shall not be stored in clear text in the system; passwords shall be salted and hashed.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. Section 4.2.3.4.3.1]

2.2.5 Inactive Session timeout

Requirement:

An OAM user interactive session shall be terminated automatically after a specified period of inactivity. It shall be possible to configure an inactivity time-out period. Next Generation Firewall shall monitor inactive sessions of administrative login users and initiate session locking mechanism based on pre-configured timers. Unlocking the session shall be permissible only by user authentication. If the inactivity period further continues for a defined period, session/user ID timeout must occur after this inactivity. Reauthentication of the OAM user shall be repeated following any period of inactivity lasting 15 minutes or longer.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.2.3.5.2]

2.2.6 Password Changes

Requirement:

If a password is used as an authentication attribute, then the system shall offer a function that enables a user to change his password at any time. When an external centralized system for user authentication is used, it shall be possible to implement this function on this system. Password change shall be enforced after initial login (after successful authentication). Next Generation Firewall shall enforce password change based on password management policy. In particular, the system shall enforce password expiry. Next Generation Firewall shall support a configurable period for expiry of passwords.
Previously used passwords shall not be allowed up to a certain number (Password History).

The number of disallowed previously used passwords shall be:

a) Configurable;
b) Greater than 0;
c) And its minimum value shall be 3. This means that the Next Generation Firewall shall store at least the three previously set passwords. The maximum number of passwords that the Next Generation Firewall can store for each user is up to the manufacturer.

When a password is about to expire, a password expiry notification shall be provided to the user. Above requirements shall be applicable for all passwords used (e.g., application-level, OS- level, etc.). An exception to this requirement is machine accounts. Next Generation Firewall to have an in-built mechanism to support this requirement. If a central system is used for user authentication password policy, then additional assurance shall be provided that the central system enforces the same password change policies as laid down for the local system in this subclause. And if a central system is not used for user authentication, the assurance on password changes rules shall be performed on the Next Generation Firewall. The minimum password age shall be set as one day i.e recycling or flipping of passwords to immediate return to favorite password is not possible.

The password shall be changed (need not be automatic) based on key events including, not limited to

- Indication of compromise (IoC)
- Change of user roles
- When a user leaves the organization

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. Section 4.2.3.4.3.2]
[Ref [18]: CIS_Benchmarks_Password_Policy_Guide_v21.12]

2.2.7 Protected Authentication feedback

Requirement:

The Authentication attribute shall not be displayed in such a way that it could be seen and misused by a casual local observer. Typically, the individual characters of the password are replaced by a character such as "*".
This requirement shall be applicable for all passwords used (e.g., application-level, OS-level, etc.). An exception to this requirement is machine accounts.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. Section 4.2.3.4.3.4]

2.2.8 Removal of predefined or default authentication attributes

Requirement:

Predefined or default authentication attributes shall be deleted or disabled. Normally, authentication attributes such as password or cryptographic keys will be preconfigured from producer, Original Equipment Manufacturer (OEM) or developer of a system. Such authentication attributes shall be changed by automatically forcing a user to change it on first time login to the system or the OEM provides instructions on how to manually change it.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. Section 4.2.3.4.2.3]

2.2.9 Logout function

Requirement:

The system shall have a function that allows a signed-in user to logout at any time. All processes under the logged-in user ID shall be terminated on logout. Next Generation Firewall shall be able to continue to operate without interactive sessions.

Only for debugging purposes, processes under a logged-in user ID may be allowed to continue to run after detaching the interactive session.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.2.3.5.1]

2.2.10 Policy regarding consecutive failed login attempts

Requirement:

a. The maximum permissible number of consecutive failed user account login attempts shall be configurable by the operator. The definition of the default value set at manufacturing time for the maximum number of failed user account login attempts shall be less than or equal to 8, typically 5. After the maximum permissible number of consecutive failed user account login attempts is exceeded by a user, there shall be a block delay in allowing the user to attempt login again. This block delay and the capability to set the period of the block delay, e.g., double the delay, or 5 minutes delay, or 10 minutes delay, after each login failure should be configurable by the operator. The default value set at manufacturing time for this delay shall be greater than or equal to 5 sec.

b. If supported, infinite (permanent) locking of an account that has exceeded the maximum permissible number of consecutive failed user account login attempts shall also be possible via configuration, with the exception of administrative accounts, which shall get only temporarily locked.

[Ref [3]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.5]

2.2.11 Suspend accounts on non-use

Requirement:

It shall be possible to configure the system to automatically suspend an account after 'X' days without a valid login.

Note: X may be specified by operator. It can be implemented centrally also.

Ref [18]: CIS_Benchmarks_Password_Policy_Guide_v21.12

Section 2.3: Software Security

2.3.1 Secure Update

Requirement:

1. Software package integrity shall be validated during the software update stage.
2. Next Generation Firewall shall support software package integrity validation via cryptographic means, e.g., digital signature using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only. To this end, the Next Generation Firewall has a list of public keys or certificates of authorized software sources, and uses the keys to verify that the software update originated from only these sources.
3. Tampered software shall not be executed or installed if integrity check fails.
4. A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software update and modify the list mentioned in (2) above.

Note: Code signing (valid and not time expired) is also allowed as an option in (2) above.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. Section 4.2.3.3.5]

2.3.2 Secure Upgrade

Requirement:

1. Software package integrity shall be validated during the software update stage.
2. Next Generation Firewall shall support software package integrity validation via cryptographic means, e.g., digital signature using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only. To this end, the Next Generation Firewall has a list of public keys or certificates of authorized software sources, and uses the keys to verify that the software update originated from only these sources.
3. Tampered software shall not be executed or installed if integrity check fails.
4. A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software update and modify the list mentioned in (2) above.

Note: Code signing (valid and not time expired) is also allowed as an option in (2) above.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. Section 4.2.3.3.5]

2.3.3 Source code security assurance

Requirement:

a) OEM shall follow best security practices including secure coding for software development. Source code shall be made available either at Telecom Security Testing Laboratory (TSTL) premises or at the mutually agreed location for source code

review by the designated TSTL. It may be supported by furnishing the Software Test Document (STD).

b) Also, OEM shall submit the undertaking as below:
   i. Industry standard best practices of secure coding have been followed during the entire software development life cycle of the Next Generation Firewall software which includes OEM developed code, third party software and open-source code libraries used/embedded in the Next Generation Firewall.
   ii. Next Generation Firewall software shall be free from Common Weakness Enumeration (CWE) top 25, Open Worldwide Application Security Project (OWASP) top 10 security vulnerabilities and OWASP top 10 API Security vulnerabilities as on the date of latest release of product or three months prior to the date of offer of product for testing, whichever is latest. For security weaknesses, vulnerabilities identified or discovered during the interim period, OEM shall give mitigation plans.
   iii. The binaries for Next Generation Firewall and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in bullet (ii) above.

[Ref [4]: https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html]
[Ref [5]: https://owasp.org/www-project-top-ten/]
[Ref [6]: https://owasp.org/www-project-api-security/]

2.3.4 Known Malware and backdoor Check

Requirement:
OEM shall submit an undertaking stating that Next Generation Firewall is free from all known malware and backdoors as on the date of offer of Next Generation Firewall to designated TSTL for testing and shall submit their internal Malware Test Document (MTD) of the Next Generation Firewall to the designated TSTL.

2.3.5 No unused software

Requirement:

Software components or parts of software which are not needed for operation or functionality of the Next Generation Firewall shall not be present/configured. Orphaned software components /packages shall not be present in Next Generation Firewall. OEM shall provide the list of software that are necessary for Next Generation Firewall 's operation. In addition, OEM shall furnish an undertaking as "Next Generation Firewall does not contain software that is not used in the functionality of Next Generation Firewall."

[Ref [3]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.3]

2.3.6 Unnecessary Services Removal

Requirement:

Next Generation Firewall shall only run protocol handlers and services which are needed for its operation, and which do not have any known security vulnerabilities. In particular, by default the following services shall be initially configured to be disabled on Next Generation Firewall by the vendor except if services are needed during deployment. In that case those services shall be disabled according to vendor's instructions after deployment is done. Disabled protocols may still need to be enabled for other reasons by the operators, e.g., remote diagnostics.

a) File Transfer Protocol (FTP)
b) Trivial File Transfer Protocol (TFTP)
c) Telnet
d) rlogin, Rate Control Protocol (RCP), Remote Shell Protocol (RSH)
e) HTTP
f) Simple Network Management Protocol (SNMP) v1 and v2
g) SSHv1
h) Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) Small Servers (Echo, Chargen, Discard and Daytime)
i) Finger
j) Bootstrap Protocol (BOOTP) server
k) Discovery protocols (Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP))
l) IP Identification Service (Identd)
m) Packet Assembler/Disassembler (PAD)
n) Maintenance Operations Protocol (MOP)

Any other protocols, services that are vulnerable are also to be permanently disabled. Full documentation of required protocols and services (communication matrix) of the Next Generation Firewall and their purpose needs to be provided by the OEM as a prerequisite for the test case.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.3.2.1]

2.3.7 Restricting System Boot Source

Requirement:

The Next Generation Firewall can boot only from the memory devices intended for this purpose.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. Section - 4.2.3.3.2]

2.3.8 Secure Time Synchronization

Requirement:

Next Generation Firewall shall establish a secure communication channel through standard interface with the Network Time Protocol (NTP) / Precision Time Protocol (PTP) server as per appropriate TEC ER (Essential Requirement) document.

Next Generation Firewall shall establish a secure communication channel strictly using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" with NTP/PTP server.

Next Generation Firewall shall generate audit logs for all changes to time settings.

Note: RFC 8915 which proposes Network Time Security (NTS) as an extension field for the NTP version 4 is also permitted.

[Ref [7]: RFC 8915 - Network Time Security for the Network Time Protocol (NTP).]

2.3.9 Restricted reachability of services

Requirement:

Next Generation Firewall shall restrict the reachability of services so that they can only be reached on interfaces meant for the purpose. On interfaces where services are active, the reachability should be limited to legitimate communication peers. This limitation shall be realized on the Next Generation Firewall itself (without measures (e.g., firewall) at network side) according to the requirement detailed in section 2.7.1 Traffic Filtering. Administrative services (e.g., SSH, Hyper Text Transfer Protocol Secure (HTTPS), Remote Desktop Protocol (RDP)) shall be restricted to interfaces in the management plane to support separation of management traffic from user traffic.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.3.2.2]

2.3.10 Self-Testing

Requirement:

Next Generation Firewall's cryptographic module shall perform power-up self-tests and conditional self-tests to ensure that the module is functioning properly. Power-up self-tests shall be performed when the cryptographic module is powered up during system bootup/restart. Conditional self-tests shall be performed when an applicable security function or operation is invoked (i.e., security functions for which self-tests are required). If a cryptographic module fails a self-test, the module shall enter an error state and output an error indicator via the status output interface. The cryptographic module shall not perform any cryptographic operations while in an error state.

Section 2.4: System Secure Execution Environment

2.4.1 No unused functions

Requirement:

Unused functions i.e., the software and hardware functions which are not needed for operation or functionality of the Next Generation Firewall shall be permanently deactivated. Permanently means that they shall not be reactivated again after the Next Generation Firewall system's reboot. If unused functions of software cannot be deleted or uninstalled individually as required in clause "2.3.5 No unused software" of the present document, such functions shall be deactivated in the configuration of Next Generation Firewall permanently.

The list of hardware and software functions installed in the system shall match with the ones that have been mentioned and deemed necessary for the operation of the Next Generation Firewall.

EXAMPLE: A debugging function in software which can be used for troubleshooting shall not be activated during normal operation of the Next Generation Firewall.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.3.2.4]

2.4.2 No unsupported components

Requirement:
OEM to ensure that the Next Generation Firewall shall not contain software and hardware components that are no longer supported by them or their 3rd Parties (e.g., vendor, producer, or developer) including the open-source communities, such as components that have reached end-of-life or end-of-support. An undertaking in this regard shall be provided by OEM.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.3.2.5]

2.4.3 Avoidance of Unspecified mode of Access

Requirement:

Next Generation Firewall shall not contain any access mechanism which is unspecified or not declared. An undertaking shall be given by the OEM as follows:
The Next Generation Firewall does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel.

Section 2.5: User Audit

2.5.1 Audit trail storage and protection

Requirement:

The security event log shall be access-controlled (file access rights) such only privileged users have access to the log files.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.2.3.6.3]

2.5.2 Audit Event Generation

Requirement:

Next Generation Firewall shall log all important Security events with unique System Reference details as given in the table below.

Next Generation Firewall shall record within each audit record at least information pertaining to date and time of the event, type of event, subject identity, protocol, service or program used for access, source and destination IP addresses & ports and the outcome (success or failure) of the event.

Additional audit record information, depending on the audit event, shall also be provided as given in the Table below:

Sr. No.	Event Types (Mandatory or Optional)	Description	Event data to be logged
1.	Incorrect login attempts		Username

	(Mandatory)	Records any user's incorrect login attempts to the NGFW system	Source (IP address) if remote access
			Outcome of event (Success or failure)
			Timestamp
2.	Administrator access (Mandatory)	Records any access attempts to accounts that have system privileges.	Username
			Timestamp
			Length of session
			Outcome of event (Success or failure)
			Source (IP address) if remote access
3.	Account administration (Mandatory)	Records all account administration activity, i.e. configure, delete, copy, enable, and disable.	Administrator username
			Administered account
			Activity performed (configure, delete, enable and disable)
			Outcome of event (Success or failure)
			Timestamp
4.	Resource Usage (Mandatory)	Records events that have been triggered when system parameter values such as disk space, CPU load over a longer period	Value exceeded
			Value reached
			(Here suitable threshold values shall be defined depending on the individual system.)

		have exceeded their defined thresholds.	Outcome of event (Success or failure)
			Timestamp
5.	Configuration change (Mandatory)	Changes to configuration of the NGFW system	Change made
			Timestamp
			Outcome of event (Success or failure)
			Username
6.	Reboot/shutdown/ crash (Mandatory)	This event records any action on the network device/NGFW system that forces a reboot or shutdown OR where the network device/NGFW system has crashed.	Action performed (boot, reboot, shutdown, etc.)
			Username (for intentional actions)
			Outcome of event (Success or failure)
			Timestamp
7.	Interface status change (Mandatory)	Change to the status of interfaces on the NGFW system (e.g., shutdown)	Interface name and type
			Status (shutdown, down, missing link, etc.)
			Outcome of event (Success or failure)
			Timestamp
8.	Change of group membership or accounts (Mandatory)	Any change of group membership for accounts	Administrator username
			Administered account
			Activity performed (group added or removed)

			Outcome of event (Success or failure)
			Timestamp
9.	Resetting Passwords (Mandatory)	Resetting of user account passwords by the Administrator	Administrator username
			Administered account
			Activity performed (configure, delete, enable and disable)
			Outcome of event (Success or failure)
			Timestamp
10.	Services (Mandatory)	Starting and Stopping of Services (if applicable)	Service Identity
			Activity performed (start, stop, etc.)
			Timestamp
			Outcome of event (Success or failure)
11.	X.509 Certificate Validation (Optional)	Unsuccessful attempt to validate a certificate	Timestamp
			Reason for failure
			Subject identity
			Type of event
12.	Secure update (Mandatory)	Attempt to initiate manual update, initiation of update, completion of update	User identity
			Timestamp
			Outcome of event (Success or failure)

			Activity performed
13.	Time change (Mandatory)	Change in time settings	Old value of time
			New value of time
			Timestamp
			Origin of attempt to change time (e.g., IP address)
			Subject identity
			Outcome of event (Success or failure)
			User identity
14.	Session unlocking /termination (Optional)	Any attempts at unlocking of an interactive session, termination of a remote session by the session locking mechanism, termination of an interactive session	User identity (wherever applicable)
			Timestamp
			Outcome of event (Success or failure)
			Subject identity
			Activity performed
			Type of event
15.	Trusted Communication paths with IT entities such as Authentication Server, Audit Server, NTP Server, etc. and	Initiation, Termination and Failure of trusted Communication paths	Timestamp
			Initiator identity (as applicable)
			Target identity (as applicable)

	for authorized remote administrators (Optional)		User identity (in case of Remote administrator access)
			Type of event
			Outcome of event (Success or failure, as applicable)
16.	Audit data changes (Mandatory)	Changes to audit data including deletion of audit data	Timestamp
			Type of event (audit data deletion, audit data modification)
			Outcome of event (Success or failure)
			Subject identity
			User identity
			Origin of attempt to change time (e.g., IP address)
			Details of data deleted or modified
17.	User Login (Mandatory)	All use of Identification and authentication mechanisms.	User identity
			Origin of attempt (IP address)
			Outcome of event (Success or failure)
			Timestamp

Note: The security events generated by IdAM/IAM are also acceptable.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.2.3.6.1]

2.5.3 Secure Log Export

Requirement:

a) Next Generation Firewall shall support (near real time) forwarding of security event logging data to an external system available in redundant configuration by push or pull mechanism through diverse links.
b) Log functions should support secure uploading of log files to a central location or to a system external for the Next Generation Firewall.
c) Next Generation Firewall shall be able to store the generated audit data locally. The memory for this purpose shall be dimensioned to cater for the continuous storage of two days of audit data. OEM shall submit justification document for sufficiency of local storage requirement.
d) Secure Log export shall comply with the secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.2.3.6.2]

2.5.4 Logging access to personal data

Requirement:

In some cases, access to personal data in clear text might be required. If such access is required, access to this data shall be logged, and the log shall contain who accessed what data without revealing personal data in clear text. When for practical purposes, such logging is not available, a coarser grain logging is allowed.

In some cases, the personal data stored in the log files may allow the direct identification of a subscriber. In such cases, the revealed personal information may not expose the subscriber to any kind of privacy violation.

[Ref [3]: TSDSI STD T1.33.117-17.1.0 V1.1.0. Section 4.2.3.2.5]

2.5.5 Security audit log:

Requirement:

The security audit log must not contain

1) Authentication credentials, even if encrypted (e.g password)
2) Access Tokens-To be masked when outputting
3) Proprietary or sensitive personal information

[Ref [17]: GSMA NG 133 Cloud Infrastructure Reference Architecture Ver 2.0 6.3.7.3]

2.5.6 Audit Logs

Requirement:

1) All security logging mechanisms must be active from system initialization
2) Logs must be time synchronized
3) Security audit logs must be protected in transit and at rest
4) The following systems events must be logged (apart from those listed in 2.5.2)
   a) Successful and unsuccessful changes to privilege level
   b) Successful and unsuccessful security policy changes
   c) Starting and stopping of security logging
   d) Starting and stopping of processes including attempts to start unauthorized processes
   e) All command line activity performed by innate OS programs known to otherwise leave no evidence upon command completion including Power shell on windows system.

[Ref [17]: GSMA NG 133 Cloud Infrastructure Reference Architecture version 2.0 6.3.7.1 and 6.3.7.2]

2.5.7 Centralized log Auditing

Requirement:

Next Generation Firewall must be able to submit security events (e.g. authentication, authorization and accounting, login attempts, administration functions and configurations) to a centralized platform, which shall monitor and analyze in real time the messages for possible attempts at intrusion.

Note: This clause requires external system for testing. The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfilment of this clause.

[Ref [14]: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T17]

Section 2.6: Data Protection

2.6.1 Cryptographic Based Secure Communication

Requirements:

Next Generation Firewall shall communicate with the connected entities strictly using the secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

OEM shall submit to TSTL, the list of the connected entities with Next Generation Firewall and the method of secure communication with each entity with details of interface, protocol stack implemented, configuration, detailed procedure of establishing communication with each entity and any other details required for verifying this requirement.

2.6.2 Cryptographic Module Security Assurance

Requirement:

Cryptographic module embedded inside the Next Generation Firewall (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 or later as prescribed by NIST standards.

Till further instructions, this clause will be considered 'complied' by submission of an undertaking by the OEM in specified format along with self-certified test reports. An undertaking is to be submitted by the OEM mentioning that "Cryptographic module embedded inside the Next Generation Firewall (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 or later as prescribed by NIST standards."

[Ref [16]: ENISA Recommendation "Standardization in support of the cybersecurity certification", Dec 2019.]
[Ref [8]: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf]

2.6.3 Cryptographic Algorithms implementation Security Assurance

Requirement:

Cryptographic algorithm implemented inside the crypto module of Next Generation Firewall shall be in compliance with the respective latest FIPS standards (for the specific crypto algorithm). Till further instructions, this clause will be considered 'complied' by submission of an undertaken by the OEM in specified format along with self-certified test reports.

An undertaking is to be submitted by the OEM mentioning that "Cryptographic algorithms implemented inside the Crypto module of Next Generation Firewall is in compliance with the

respective latest FIPS standards (for the specific crypto algorithm embedded inside the Next Generation Firewall)."

2.6.4 Protecting data and information – Confidential System Internal Data

Requirement:

a) When the next generation firewall is in normal operational mode (i.e., not in maintenance mode) there shall be no system function that reveals confidential system internal data in the clear text to users and administrators.
   Such functions could be, for example, local or remote OAM CLI or GUI, logging messages, alarms, configuration file exports etc. Confidential system internal data contains authentication data (i.e., PINs, cryptographic keys, passwords, cookies) as well as system internal data that is not required for systems administration.
b) Access to maintenance mode shall be restricted only to authorized privileged user.

[Ref [3]: TSDSI STD T1.33.117-17.1.0 V1.1.0. Section 4.2.3.2.2.]

2.6.5 Protecting data and information in storage

Requirement:

1. For sensitive data (persistent or temporary) in storage, read access rights shall be restricted. Sensitive files of Next Generation Firewall system that are needed for the functionality shall be protected against manipulation strictly using the Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" with appropriate non-repudiation controls.
2. In addition, the following rules apply for:
   a. Systems that need access to identification and authentication data in the clear/readable form e.g., in order to perform an activity/operation. Such systems shall not store this data in the clear/readable form, but scramble or encrypt it by implementation-specific means.
   b. Systems that do not need access to sensitive data (e.g., user passwords) in the clear. Such systems shall hash this sensitive data strictly using the cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.
   c. Stored files in the Next Generation Firewall shall be protected against manipulation strictly using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. Section 4.2.3.2.3]

2.6.6 Protection against Copy of Data

Requirement:

a) Without authentication& authorization and except for specified purposes, Next Generation Firewall shall not create a copy of data in use or data in transit.
b) Protective measures shall exist against use of available system functions / software residing in system to create copy of data for illegal transmission.

2.6.7 Protection against Data Exfiltration - Overt Channel

Requirement**:**

a) Next Generation Firewall shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit. (Within its boundary).
b) Establishment of outbound overt channels such as, HTTPS, Instant Messaging (IM), Peer-to-Peer (P2P), e-mail etc. are to be forbidden if they are auto-initiated by / auto-originated from the firewall.
c) Session logs shall be generated for establishment of any session initiated by either user or system.

2.6.8 Protection against Data Exfiltration - Covert Channel

Requirement:

a) Next Generation Firewall shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit (within its boundary).
b) Establishment of outbound covert channels and tunnels such as Domain Name System (DNS) Tunnel, HTTPS Tunnel, Internet Control Message Protocol (ICMP) Tunnel, Transport Layer Security (TLS), Secure Sockets Layer (SSL), SSH, Internet Protocol Security (IPSec), Virtual Private Network (VPN), Real-time Transfer Protocol (RTP) Encapsulation etc. are to be forbidden if they are auto-initiated by / auto-originated from the firewall.
c) Session logs shall be generated for establishment of any session initiated by either user or system.

2.6.9 System Robustness Against Unexpected Input

Requirement:

During the processing of incoming data, all inputs to the Next Generation Firewall shall be validated before processing them further. This includes all data sent to the system, such as user inputs and protocol data. The following typical implementation errors shall be avoided:

1. No validation on the lengths of transferred data.
2. Incorrect assumptions about data formats.
3. No validation that received data complies with the specification.
4. Insufficient handling of protocol errors in received data.
5. Insufficient restriction on recursion when parsing complex data formats.
6. Whitelisting or escaping for inputs outside the expected value ranges.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. section 4.2.3.3.4]

2.6.10 Security of backup data

Requirement:

Next Generation Firewall shall support secure mechanisms for taking backup of sensitive data, configuration, and log files. An effective backup strategy shall be in place and documented.

[Ref [15]: "Security Guidance for 5G Cloud Infrastructure Part III: Data Protection" by NSA CISA]

2.6.11 Secure deletion of sensitive data

Requirement:

Next Generation Firewall shall support secure deletion of sensitive data by authorized user in such a manner that it cannot be recovered through any forensic means.

Section 2.7: Network Services

2.7.1 Traffic Filtering – Network Level

Requirement:

Next Generation Firewall shall provide a mechanism to filter incoming IP packets on any interface (Refer to RFC 3871) In particular, the Next Generation Firewall shall provide a mechanism:

a) To filter incoming IP packets on any IP interface at Network Layer and Transport Layer of the stack ISO/Open Systems Interconnection (OSI).
b) To allow specified actions to be taken when a filter rule matches. In particular at least the following actions should be supported:
    i) Discard/Drop: the matching message is discarded; no subsequent rules are applied and no answer is sent back.
    ii) Accept: the matching message is accepted.
    iii) Account: the matching message is accounted for i.e., a counter for the rule is incremented. This action can be combined with the previous ones. This feature is useful to monitor traffic before its blocking.
c) To enable/disable for each rule the logging for Dropped packets, i.e., details on messages matching the rule for troubleshooting.
d) To filter on the basis of the value(s) of source IP, destination IP and port addresses of the protocol header
e) To reset the accounting.
f) Next Generation Firewall shall provide a mechanism to disable/enable each defined rule.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.2.6.2.1]
[Ref [11]: RFC 3871 – Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure]

2.7.2 Traffic Separation

Requirement:

The Next Generation Firewall shall support the physical or logical separation of traffic belonging to different network domains. For example, OAM traffic and control plane traffic belong to different network domains. Refer to RFC 3871 for further information.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.5.1]
[Ref [11]: RFC 3871 – Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure]

2.7.3 Traffic Protection –Anti-Spoofing

Requirement:

Next Generation Firewall shall not process IP packets if their source address is not reachable via the incoming interface. Implementation example: Use of “Reverse Path Filter” (RPF) provides this function.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.3.1.1]

Section 2.8: Attack Prevention Mechanisms

2.8.1 Network Level and application-level DDoS

Requirement:

The Next Generation Firewall shall have protection mechanisms against Network level and Application-level Distributed Denial of Service (DDoS) attacks.

The NG firewall shall provide security measures to deal with overload situations which may occur as a result of a denial-of-service attack or during periods of increased traffic. In particular, partial or complete impairment of system availability shall be avoided.
Potential protective measures may include:

a) Restricting available RAM per application
b) Restricting maximum sessions for a Web application
c) Defining the maximum size of a dataset
d) Restricting Central Processing Unit (CPU) resources per process
e) Prioritizing processes
f) Limiting amount or size of transactions of a user or from an IP address in a specific time range
g) Limiting amount or size of transactions to an IP address/Port Address in a specific time range

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. Section 4.2.3.3.1

2.8.2 Excessive Overload Protection

Requirement:

Next Generation Firewall shall act in a predictable way if an overload situation cannot be prevented. Next generation shall be built in such a way that it can react to an overload situation in a controlled way.
However, it is possible that a situation happens where the security measures are no longer sufficient. In such a case it shall be ensured that Next Generation Firewall cannot reach an undefined and thus potentially insecure, state. In an extreme case this means that a controlled system shutdown is preferable to uncontrolled failure of the security functions and thus loss of system protection.

OEM shall provide a technical description of the Next Generation Firewall' s over load control mechanisms.

[Ref [3]: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.3]

2.8.3 Interface robustness requirements

Requirement:

The Next Generation Firewall shall be not be affected in its availability or robustness by incoming packets, from other network elements, that are manipulated or differing the norm. This means that appropriate packets shall be detected as invalid and be discarded. The process shall not be affecting the performance of the Next Generation Firewall. This robustness shall be just as effective for a great mass of invalid packets as for individual or a small number of packets.

a) Mass-produced TCP packets with a set SYN flag to produce half-open TCP connections (SYN flooding attack).
b) Packets with the same IP sender address and IP recipient address (Land attack).
c) Mass-produced ICMP packets with the broadcast address of a network as target address (Smurf attack).
d) Fragmented IP packets with overlapping offset fields (Teardrop attack).
e) ICMP packets that are larger than the maximum permitted size (65,535 Bytes) of IPv4 packets (Ping-of-death attack).
f) Uncorrelated reply packets (i.e. packets which cannot be correlated to any request).

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.2.6.2.2]

Section 2.9: Vulnerability Testing Requirements

2.9.1. Fuzzing – Network and Application Level

Requirement:

It shall be ensured that externally reachable services of Next Generation Firewall are reasonably robust when receiving unexpected input.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. section 4.4.4]

2.9.2. Port Scanning

Requirement:

It shall be ensured that on all network interfaces of Next Generation Firewall, only documented ports on the transport layer respond to requests from outside the system.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.4.2]

2.9.3. Vulnerability Scanning

Requirement:

The purpose of vulnerability scanning is to ensure that there are no known vulnerabilities (or that relevant vulnerabilities are identified and remediation plans in place to mitigate them) on the Next Generation Firewall, both in the OS and in the applications installed, that can be detected by means of automatic testing tools via the Internet Protocol enabled network interfaces.
The vulnerabilities found during the Vulnerability Scanning/Assessment process shall be remediated as below. For other than critical vulnerabilities, OEM shall provide a remediation plan.

Sl No	CVSS Score	Severity	Remediation
1	9.0-10.0	Critical	To be patched immediately
2	7.0-8.9	High	To be patched within a month
3	4.0-6.9	Medium	To be patched within three months
4	0.1-3.9	Low	To be patched within an year

Zero-day vulnerabilities shall be remediated immediately or as soon as possible.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.4.3]
[Ref [9]: https://nvd.nist.gov/vuln-metrics/cvss]
[Ref [19]: Cloud Infrastructure Reference Architecture managed by Open Stack]

Section 2.10: Operating System

2.10.1. Growing Content Handling

Requirement:

a) Growing or dynamic content shall not influence system functions.
b) A file system that reaches its maximum capacity shall lead to an event getting logged with appropriate message parameters and shall not stop Next Generation Firewall from operating properly.
Therefore, countermeasures shall be taken to ensure that this scenario is avoided. The Countermeasures are usage of dedicated filesystems, separated from main system functions, or quotas, or at least a file system monitoring.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.2.4.1.1.1]

2.10.2. Handling of ICMP

Requirement:

Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the Next Generation Firewall. In particular, there are certain types of ICMPv4 and ICMPv6 that are not used in most networks, but represent a risk. ICMP message types which on receipt lead to responses or to configuration changes are not mentioned in this requirement, but they may be necessary to support relevant and specified networking features. Those must be documented.

Certain ICMP types are generally permitted and do not need to be specifically documented. Those are marked as "Permitted" in the table below.
The Next Generation Firewall shall not send certain ICMP types by default but it may support the option to enable utilization of these types (e.g., for debugging) which are marked as "Optional" in below table:

Type (IPv4)	Type (IPv6)	Description	Send	Respond to
0	128	Echo Reply	Optional (i.e. as automatic reply to "Echo Request")	N/A
3	1	Destination Unreachable	Permitted	N/A
8	129	Echo Request	Permitted	Optional
11	3	Time Exceeded	Optional	N/A
12	4	Parameter Problem	Permitted	N/A
N/A	2	Packet too Big	Permitted	N/A

N/A	135	Neighbor Solicitation	Permitted	Permitted
N/A	136	Neighbor Advertisement	Permitted	N/A

The Next Generation Firewall shall not respond to, or process (i.e., do changes to configuration) under any circumstances certain ICMP message types as marked in the below table.

Type (IPv4)	Type (IPv6)	Description	Send	Respond to	Process (i.e., do changes to configuration)
5	137	Redirect	N/A	N/A	Not Permitted
13	N/A	Timestamp	N/A	Not Permitted	N/A
14	N/A	Timestamp Reply	Not Permitted (i.e. as automatic reply to "Timestamp")	N/A	N/A
N/A	133	Router Solicitation	N/A	Not Permitted	Not Permitted
N/A	134	Router Advertisement	N/A	N/A	Not Permitted

N/A: Not Applicable

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.2.4.1.1.2.]

2.10.3. Authenticated Privilege Escalation only

Requirement:

The Next Generation Firewall shall not support a privilege escalation method in interactive sessions (both CLI and GUI) which allows a user to gain administrator/root privileges from another user account without re-authentication.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.2.4.1.2.1]

2.10.4. System account identification

Requirement:

Each system user account in Next Generation Firewall shall have a unique User ID (UID) with appropriate non-repudiation controls.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section 4.2.4.2.2]

2.10.5. OS Hardening - Minimized kernel network functions

Requirement:

Kernel based network functions not needed for the operation of the Next Generation Firewall shall be deactivated.
In particular the following ones shall be disabled by default:

1. IP Packet Forwarding between different interfaces of the network product.
2. Proxy Address Resolution Protocol (ARP) (to prevent resource exhaustion attack and man-in-the-middle attacks)
3. Directed broadcast (to prevent attacks like Smurf, Denial of Service etc.,)
4. IPv4 Multicast handling. In particular all packets with IP source or destination address belonging to the multicast IP ranges (224.0.0.0 through 239.255.255.255) shall be discarded by default and multicast route caching and forwarding shall be disabled to prevent smurf and fraggle attacks. A configuration option shall be available to enable the IPv4 multicast handling if required.
5. Gratuitous ARP messages (to prevent ARP Cache Poisoning attacks)

[Ref [3]: TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section – 4.3.3.1.2]

2.10.6. No automatic launch of removable media

Requirement:

The Next Generation Firewall shall not automatically launch any application when a removable media device such as Compact Disk (CD), Digital Versatile Disk (DVD), Universal Serial Bus (USB)-Sticks or USB-Storage drive is connected. If the operating system supports an automatic launch, it shall be deactivated unless it is required to support availability requirements.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section – 4.3.3.1.3]

2.10.7. Protection from buffer overflows

Requirement:

The Next Generation Firewall shall support mechanisms for buffer overflow protection. Documentation which describes these buffer overflow mechanisms and also how to check that they have been enabled and/or implemented shall be provided by OEM.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section – 4.3.3.1.5]

2.10.8. External file system mount restrictions

Requirement:

If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in the Next Generation Firewall in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems. OS-level restrictions shall apply to normal users against mount / use of removable media devices (e.g., USB drive, CD ROM etc.) for data transfer.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section – 4.3.3.1.6]

2.10.9. File-system Authorization privileges

Requirement:

The Next Generation Firewall shall be designed to ensure that only users that are authorized to modify files, data, directories or file systems have the necessary privileges to do so.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section - 4.3.2.7]

2.10.10. SYN Flood Prevention

Requirement:

Next Generation Firewall shall support a mechanism to prevent Syn Flood attacks. This feature shall be enabled by default.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section - 4.3.3.1.4]

2.10.11. Handling of IP options and extensions

Requirement:

IP packets with unnecessary options or extension headers shall not be processed. IP options and extension headers (e.g., source routing) are only required in exceptional cases. So, all packets with enabled IP options or extension headers shall be filtered.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. Section - 4.2.4.1.1.3]

2.10.12. Restrictions on running Scripts / Batch-processes

Requirement:

Scheduled tasks for carrying out the activities such as taking the backups, monitoring disk space and system maintenance activities shall be executed by the privileged user such as administrator only. Similarly, the Next Generation Firewall shall have feature to restrict Scripts / Batch-processes / Macros usage among various users. It shall be possible to administratively configure scheduled tasks usage i.e., Cron-Job usage (permit / deny) among various users like Normal users, privileged users.

2.10.13. Restrictions on Soft-Restart

Requirement:

Next Generation Firewall shall restrict software-based system restart options usage among various users. The software reset/restart either through command or use of key-combinations like CTRL+ALT+DEL is not available to normal users for prevention of unintended / malicious trigger of system reset/restart.

Section 2.11: Web Servers

This entire section of the security requirements is applicable if the Next Generation Firewall supports **web management interface.**

2.11.1. HTTPS

Requirement:

The communication between Next Generation Firewall Web client and Web server shall be protected strictly using the Secure cryptographic controls prescribed in Table1 of the latest

document “Cryptographic Controls for Indian Telecom Security Assurance Requirement ITSAR” only

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.2.5.1]

2.11.2. Webserver logging

Requirement:

Access to the webserver (for both successful as well as failed attempts) shall be logged by Next Generation Firewall. The web server log shall contain the following information:

1. Access timestamp
2. Source (IP address)
3. Account (if known)
4. Attempted login name (if the associated account does not exist)
5. Relevant fields in http request. The URL shall be included whenever possible.
6. Status code of web server response

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.2.5.2]

2.11.3. HTTPS input validation

Requirement:

The Next Generation Firewall shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks. The Next Generation Firewall shall validate, filter, escape, and encode user-controllable input before it is placed in output that is used as a web page that is served to other users.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.2.5.4]

2.11.4. No system privileges

Requirement:

No Next Generation Firewall web server processes shall run with system privileges. If a process is started by a user with system privileges, execution shall be transferred to a different user without system privileges after the start.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.2]

2.11.5. No unused HTTPS methods

Requirement:

HTTPS methods that are not required for system operation shall be deactivated.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.3]

2.11.6. No unused add-ons

Requirement:

All optional add-ons and components of the web server shall be deactivated if they are not required for Next Generation Firewall operation.
In particular, Common Gateway Interface (CGI) or other scripting components, Server Side Includes (SSI), and Web based Distributed Authoring and Versioning (WebDAV) shall be deactivated if they are not required.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.4]

2.11.7. No compiler, interpreter, or shell via CGI or other server-side scripting

Requirement:

If CGI (Common Gateway Interface) or other scripting technology is used, the CGI directory or other corresponding scripting directory shall not include compilers or interpreters.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.5]

2.11.8. No CGI or other scripting for uploads

Requirement:
If CGI or other scripting technology is used, the associated CGI/script directory shall not be used for uploads.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.6]

2.11.9. No execution of system commands with SSI

Requirement:

If Server Side Includes (SSI) is active, the execution of system commands shall be deactivated.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.7]

2.11.10. Access rights for web server configuration

Requirement:

Access rights for Next Generation Firewall web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges. Implementation example: Delete "read" and "write" access rights for "others." Only grant "write" access to the user who configures the web server.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.8]

2.11.11. No default content

Requirement:

Default content (examples, help files, documentation, aliases) that is provided with the standard installation of the Next Generation Firewall web server shall be removed.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.9]

2.11.12. No directory listings

Requirement:

Directory listings (indexing) / "Directory browsing" shall be deactivated.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.10]

2.11.13. Web server information in HTTPS headers

Requirement:

The HTTPS header shall not include information on the version of the Next Generation Firewall web server and the modules/add-ons used.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.11]

2.11.14. Web server information in error pages

Requirement:

User-defined error pages and Error messages shall not include version information and other internal information about the Next Generation Firewall web server and the modules/add-ons used. Error messages shall not include internal information such as internal server names, error codes, etc. Default error pages of the Next Generation Firewall web server shall be replaced by error pages defined by the OEM.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.11]

2.11.15. Minimized file type mappings

Requirement:

File type or script-mappings that are not required for NGFW operation shall be deleted e.g., php, phtml, js, sh, csh, bin, exe, pl, vbe, vbs.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.13]

2.11.16. Restricted file access

Requirement:

Restrictive access rights shall be assigned to all files which are directly or indirectly (e.g., via links or in virtual directories) reside in the Next Generation Firewall web server's document directory. In particular, the Next Generation Firewall web server shall not be able to access files which are not meant to be delivered.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.3.4.14]

2.11.17. HTTP User session

Requirement:

To protect user sessions, Next Generation Firewall shall support the following session ID and session cookie requirements:

a) The session ID shall uniquely identify the user and distinguish the session from all other active sessions.
b) The session ID shall be unpredictable.
c) The session ID shall not contain sensitive information in clear text (e.g., account number, social security, etc.).

d) In addition to the Session Idle Timeout, Next Generation Firewall shall automatically terminate sessions after a configurable maximum lifetime. This maximum lifetime defines the maximum session span. When the maximum lifetime expires, the session shall be closed, the session ID shall be deleted and the user shall be forced to (re)authenticate in the web application and to establish a new session. The default value for this maximum lifetime shall be set to 8 hours.
e) Session IDs shall be regenerated for each new session (e.g., each time a user is logged in).
f) The session ID shall not be reused or renewed in subsequent sessions.
g) The Next Generation Firewall shall not use persistent cookies to manage sessions but only session cookies. This means that neither the "expire" nor the "max-age" attribute shall be set in the cookies.
h) Where session cookies are used the attribute 'HttpOnly' shall be set to true.
i) Where session cookies are used the 'domain' attribute shall be set to ensure that the cookie can only be sent to the specified domain.
j) Where session cookies are used the 'path' attribute shall be set to ensure that the cookie can only be sent to the specified directory or sub-directory.
k) The NGFW shall not accept session identifiers from GET/POST variables.
l) The NGFW shall be configured to only accept server generated session ID.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.1.0. section 4.2.5.3

Section 2.12: Other Security requirements

2.12.1. Remote Diagnostic Procedure – Verification

Requirement:

If the firewall is providing Remote access for troubleshooting purposes/alarm maintenance then it shall be allowed only for authorized users, other than the root user. All activities performed by the remote user are to be logged with the following parameters:

a) User id
b) Time stamp
c) Interface type
d) Event level (e.g. CRITICAL, MAJOR, MINOR)
e) Command/activity performed and
f) Result type (e.g. SUCCESS, FAILURE).
g) IP Address of remote machine

[Ref [23]: GSMA 133: GSM Association Non-confidential Official Document NG.133 - Cloud Infrastructure Reference Architecture managed by OpenStack, section:2.2.7.7]

2.12.2. No System Password Recovery

Requirement:

No provision shall exist for firewall System / Root password recovery in Next Generation Firewall.

2.12.3. Secure System Software Revocation

Requirement:

Once the Next Generation Firewall software image is legally updated/upgraded with new software image, it shall not be possible to roll back to a previous software image.

In case roll back is essential, it shall be done only by the administrator with appropriate non-repudiation controls. Next Generation Firewall shall support a well-established control mechanism for rolling back to previous software image.

2.12.4. Software Integrity Check –Installation

Requirement:

Next Generation Firewall shall validate the software package integrity before the installation/upgrade stage strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only. Tampered software shall not be executed or installed if integrity check fails.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V.1.0.0. Section 4.2.3.3.5]

2.12.5. Software Integrity Check – Boot

Requirement:

The Next Generation Firewall shall verify the integrity of a software component by comparing the result of a measurement of the component, typically a standard cryptographic hash generated strictly using the Secure cryptographic controls prescribed in Table1 of the

latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" to the expected reference value.

2.12.6. Unused Physical and Logical Interfaces Disabling

Requirement:

Next Generation Firewall shall support the mechanism to verify both the physical and logical interfaces exist in the product.
Physical and logical accessible interfaces (except console interface) which are not under use shall be disabled so that they remain inactive even in the event of reboot.

2.12.7. Predefined accounts shall be deleted or disabled

Requirement:

Predefined or default user accounts (other than Admin/Root) in Next Generation Firewall shall be deleted or disabled.

[Ref [3]: TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0. Section 4.2.3.4.2.2]

2.12.8. Control Plane Traffic Protection

Requirement:

Control plane traffic shall be protected in the Next General Firewall using standard cryptographic mechanisms i.e., by using the industry standard cryptographic secure protocols such as TLS, IPSec, etc.

Chapter 3 Specific Security Requirements

3.1 Audit Event Generation

Requirement:

The Next Generation Firewall shall generate audit events for security-relevant activities, including but not limited to the following:

a. Port scans detected
b. Vulnerability scans detected
c. Intrusion attempts detected
d. Denial-of-Service (DoS) attacks detected
e. Changes to firewall rules and policies

[Ref [1]: NIST 800-41 - Guidelines on Firewalls and Firewall Policy]
[Ref [13]: WaTech Firewall Standard]

3.2 Traffic Filtering

The Next Generation Firewall shall provide robust traffic filtering capabilities to control network traffic based on predefined security policies. This includes implementing stateful inspection for all inbound and outbound traffic to ensure comprehensive security measures. The firewall shall support the creation, modification, and deletion of filtering rules based on various criteria, including but not limited to,

1. **IP Addresses**: Support filtering rules for IP whitelisting and blacklisting, allowing traffic only from trusted IP addresses and blocking traffic from malicious or untrusted IP addresses.
2. **Ports**: Control traffic on specific ports or port ranges, enabling precise management of allowed and blocked ports.
3. **Protocols**: Manage traffic based on specific protocols (e.g., TCP, UDP, ICMP), allowing or blocking protocol-based traffic as needed.

[Ref [1]: NIST 800-41 - Guidelines on Firewalls and Firewall Policy]
[Ref [10]: Next Generation Firewall Test Methodology v9.95 RFC DRAFT]

3.3 Stateful Packet Inspection (SPI)

Requirement:

The Next Generation Firewall shall implement Stateful Packet Inspection (SPI) to maintain a record of the state of active connections. SPI shall analyze packet headers and state information, including IP addresses, port numbers, sequence numbers, and protocol flags. The firewall shall support SPI for TCP, UDP, and ICMP protocols, with inspection of application-layer protocols such as but not limited to HTTP and FTP. The firewall shall maintain a state table which should store information such as but not limited to, sequence number, source and destination IP, port numbers, connection state and perform inspection to ensure that only valid, stateful packets are allowed through.

[Ref [1]: NIST 800-41 - Guidelines on Firewalls and Firewall Policy]

3.4 Intrusion Detection and Prevention System (IDPS)

Requirement:

The Next Generation Firewall must incorporate an Intrusion Detection and Prevention System (IDPS) that includes detection methodologies that includes but not limited to signature-based detection anomaly-based detection, and Stateful Protocol Analysis. The system must support real-time threat mitigation, including automatically blocking or limiting malicious activity, and generating alerts when anomalies are detected.

[Ref [1]: NIST 800-41 - Guidelines on Firewalls and Firewall Policy]
[Ref [2]: Security Standard-Firewall Security (SS-013)]
[Ref [10]: Next Generation Firewall Test Methodology v9.95 RFC DRAFT]
[Ref [12]:NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)]

3.5 Application Layer Filtering

Requirement:

The Next Generation Firewall shall provide application layer filtering at Layer 7, capable of identifying and controlling traffic based on specific applications, independent of port or protocol. It shall support inspection of inbound traffic. The firewall must act as a man-in-the-middle proxy between the external client and the internal server and must generate a new session key for each secure session. The firewall must create a secure session between the

client and the firewall and another secure session between the firewall and the server to decrypt and inspect the traffic. This functionality includes the analysis of application-specific protocols such as HTTP, FTP, SMTP, DNS, and HTTPS.
Ref [1]: NIST 800-41 - Guidelines on Firewalls and Firewall Policy]
[Ref [2]: Security Standard-Firewall Security (SS-013)]

3.6 Virtual Private Network (VPN) Support

Requirement:

The Next Generation Firewall shall provide robust VPN support to secure remote connections and ensure data confidentiality and integrity. This includes support for protocols such as IPsec, SSL/TLS (TLS 1.2 and above), L2TP over IPsec, or any other tunneling protocol. The firewall may support either site-to-site or both site-to-site and remote access VPN configurations. All protocols used for VPN shall comply with the secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

[Ref [1]: NIST 800-41 - Guidelines on Firewalls and Firewall Policy]
[Ref [10]: Next Generation Firewall Test Methodology v9.95 RFC DRAFT]

3.7 Failover Protection

Requirement:

In case of failure, the Next Generation Firewall must block all incoming traffic instead of allowing all traffic to pass.

[Ref [2]: Security Standard-Firewall Security (SS-013)]
[Ref [10]: Next Generation Firewall Test Methodology v9.95 RFC DRAFT]

3.8 NAT (Network Address Translation) Services Support

Requirement:

The Next Generation Firewall shall support NAT configuration including but not limited to specifying source zones to mitigate attacks like IP spoofing and source translating untrusted traffic. If NAT is used, it must report the private address in the logs instead of the translated public address,

[Ref [1]: NIST 800-41 - Guidelines on Firewalls and Firewall Policy]
[Ref [2]: Security Standard-Firewall Security (SS-013)]

3.9 Access Banners

Requirement:

The Next Generation Firewall shall be configured to display pre-login access banners when a user tries to log into the firewall device, this informs users about the organization's legal and security policies. These banners serve as a warning message to ensure that users acknowledge and comply with regulatory requirements regarding system access.

[Ref [2]: Security Standard-Firewall Security (SS-013)]

3.10 Threat Intelligence Integration

Requirement:

The Next Generation Firewall shall update its threat database periodically with the period not more than two weeks.

3.11 Deep Packet Inspection (DPI)

Requirement:

The Next Generation Firewall shall support Deep Packet Inspection (DPI) of payload data and packet headers. It shall be capable of decrypting both inbound and outbound traffic, allowing thorough inspection of encrypted content.

[Ref [1]: NIST 800-41 - Guidelines on Firewalls and Firewall Policy]
[Ref [2]: Security Standard-Firewall Security (SS-013)]
[Ref [10]: Next Generation Firewall Test Methodology v9.95 RFC DRAFT]

3.12 Network Segmentation

Requirement:

The Next Generation Firewall shall provide capabilities for creating a Demilitarized Zone (DMZ) to isolate public-facing services from the internal network.

[Ref [1]: NIST 800-41 - Guidelines on Firewalls and Firewall Policy]

3.13 Malware and Antivirus Protection

Requirement:

The Next Generation Firewall must include anti-malware scanning capabilities to inspect network traffic for malware and viruses. It may support sandboxing to securely isolate and analyze suspicious files in a controlled environment. The Next Generation Firewall shall be able to intercept and decrypt network traffic and submit suspicious files to the sandbox for behavioral analysis.

[Ref [1]: NIST 800-41 - Guidelines on Firewalls and Firewall Policy]
[Ref [2]: Security Standard-Firewall Security (SS-013)]

3.14 IPv6 Support

Requirement:
The Next Generation Firewall shall support the IPv6 capabilities including but not limited to:

- NGFW must support inbound and outbound IPv4 and IPv6 traffic.
- The NGFW should be able to use IPv6 addresses in all filtering rules that use IPv4 addresses.
- The administrative interface should allow administrators to clone IPv4 rules to IPv6 addresses to make administration easier.
- The NGFW needs to be able to filter ICMPv6, as specified in RFC 4890,
- The NGFW should be able to block IPv6-related protocols such as 6-to-4 and 4-to-6 tunnelling, Teredo, and Intra-site Automatic Tunnel Addressing Protocol (ISATAP) if they are not required.
- Many sites tunnel IPv6 packets in IPv4 packets. This is particularly common for sites experimenting with IPv6, because it is currently easier to obtain IPv6 transit from a tunnel broker through a v6-to-v4 tunnel than to get native IPv6 transit from an Internet service provider (ISP). If the NGFW is able to inspect the contents of IPv4 packets, it needs to know how to inspect traffic for any tunnelling method used by the organization. A corollary to this is that if an organization is using a NGFW to prohibit IPv6 coming into or going out of its network, that NGFW needs to recognize and block all forms of v6-to-v4 tunnelling. NGFW shall be also be able block all unanalysed tunnelled packets.
- Next Generation Firewall must discard all traffic from and to reserved IPv6 address space. Firewalls should also filter packets with illegal IPv6 Header chains. The firewall shall drop all traffic from the internal network that does not use a legitimate internal address range as its source address.

[Ref [1]: NIST 800-41 - Guidelines on Firewalls and Firewall Policy
Ref [13]: WaTech Firewall Standard
Ref [22]: NIST IPv6 Profile]

3.15 WAF Support

Requirement:

Next Generation Firewall should have Web Application Firewall (WAF) capabilities to block web-based attacks, including but not limited to Cross-Site Scripting (XSS), SQL Injection, Cross-Site Request Forgery (CSRF), Remote File Inclusion (RFI), Directory Traversal, Command Injection, File Upload vulnerabilities, and Sensitive Data Exposure.

[Ref [1]: NIST 800-41 - Guidelines on Firewalls and Firewall Policy]
[Ref [2]: Security Standard-Firewall Security (SS-013)]

3.16 Traceroute

Requirement:

The Next Generation Firewall shall be configurable to block responses to traceroute requests, preventing attackers from mapping the network path to the firewall.

3.17 Geo-Fencing

Requirement:

The Next Generation Firewall shall be configured to block traffic from/to IP addresses associated with specific geographic regions based on threat intelligence data.

[Ref [2]: Security Standard-Firewall Security (SS-013)]

3.18 URL Filtering

Requirement:

Next Generation Firewall shall support URL filtering capability to block access to URL, based on the firewall's threat intelligence and as per the defined policies.

[Ref [1]: NIST 800-41 - Guidelines on Firewalls and Firewall Policy]
[Ref [2]: Security Standard-Firewall Security (SS-013)]

3.19 Policy Creation and Management

Requirement:

Next Generation Firewall shall enable administrators to create, manage, and enforce a wide range of security policies which can control access, define acceptable use, and specify actions to be taken for various types of network traffic. The firewall shall support granular policy definitions based on factors including but not limited to IP addresses, ports, protocols, the application, the user, and the service.

[Ref [1]: NIST 800-41 - Guidelines on Firewalls and Firewall Policy]
[Ref [2]: Security Standard-Firewall Security (SS-013)]
[Ref [10]: Next Generation Firewall Test Methodology v9.95 RFC DRAFT]

3.20 Proxy Configuration

Requirement:

The next Generation Firewall shall support proxy configurations to control and secure internet access for network clients. This feature allows administrators to direct traffic through proxy servers, enabling content filtering, access control, and enhanced privacy. The firewall shall support latest version of common proxy protocols, including but not limited to HTTP/HTTPS (Hypertext Transfer Protocol/Hypertext Transfer Protocol Secure), SOCKS (SOCKet Secure) versions 5.

[Ref [21]: RFC 1928 - SOCKS Protocol Version 5]

3.21 Simple Network Management Protocol (SNMP)

Requirement:

The Next Generation Firewall shall support latest version of Simple Network Management Protocol (SNMP).

[Ref [10]: Next Generation Firewall Test Methodology v9.95 RFC DRAFT]

3.22 Link Layer Discovery Protocol (LLDP):

Requirement:

The Next Generation Firewall shall support latest version of Link Layer Discovery Protocol. It shall properly handle all the fields of an LLDP frame to prevent an attacker to cause the LLDP service to crash and stop running. Additionally, Next Generation Firewall should provide configurable options for enabling or disabling LLDP on individual interfaces.

[Ref [20]: IEEE Standard for Local and Metropolitan Area Networks-- Station and Media Access Control Connectivity Discovery]

3.23 Mail Notifications

Requirement:

The Next Generation Firewall shall support mail notifications using Simple Mail Transfer Protocol (SMTP) over SSL/TLS.

3.24 Certificate Authority Management

Requirement:

NGFW must ensure that all CA certificates adhere to the X.509 standard. Use of revoked certificates shall be prevented by the firewall using methods including but not limited to the Online Certificate Status Protocol (OCSP), Certificate Revocation Lists (CRL), with immediate alerts for any revocation detection. For confidentiality and authentication, the firewall must support TLS 1.2 and above. Additionally, the Next Generation Firewall must be able to generate new certificates as per cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls"

[Ref [1]: NIST 800-41 - Guidelines on Firewalls and Firewall Policy]

3.25 IP Address Filtering

Requirement:

- Traffic with invalid source or destination addresses should always be blocked, regardless of the firewall location. Examples of relatively common invalid IPv4 addresses are 127.0.0.0 to1 27.255.255.255 (also known as the localhost addresses) and 0.0.0.0 (interpreted by some operating systems as a localhost or a broadcast address). These have no legitimate use on a network. Also, traffic using link-local addresses (169.254.0.0 to 169.254.255.255) should be blocked.

- Traffic with an invalid source address for incoming traffic or destination address for outgoing traffic (an invalid "external" address) should be blocked at the network perimeter. This traffic is often caused by malware, spoofing, denial of service attacks, or misconfigured equipment. The most common type of invalid external addresses is an IPv4 address within the ranges in RFC 1918, Address Allocation for Private Internets, that are reserved for private networks. These ranges are 10.0.0.0 to 10.255.255.255 (10.0.0.0/8 in Classless Inter-Domain Routing [CIDR] notation), 172.16.0.0 to 172.31.255.255 (172.16.0.0/12), and 192.168.0.0 to 192.168.255.255 (192.168.0.0/16).
- Traffic with a private destination address for incoming traffic or source address for outgoing traffic (an "internal" address) should be blocked at the network perimeter. Perimeter devices can perform address translation services to permit internal hosts with private addresses to communicate through the perimeter, but private addresses should not be passed through the network perimeter.
- Outbound traffic with invalid source addresses should be blocked (this is often called egress filtering). Systems that have been compromised by attackers can be used to attack other systems on the Internet; using invalid source addresses makes these kinds of attacks more difficult to stop. Blocking this type of traffic at an organization's firewall helps reduce the effectiveness of these attacks.
- Incoming traffic with a destination address of the firewall itself should be blocked unless the firewall is offering services for incoming traffic that require direct connections—for example, if the firewall is acting as an application proxy.

[Ref [1]: NIST 800-41 - Guidelines on Firewalls and Firewall Policy]

Annexure-I

Definitions

1. **DDoS**: DDoS is a distributed denial-of-service attack that renders the victim un-usable by the external environment.
2. **Kernel:** The kernel serves as the central component of an operating system, responsible for handling essential tasks such as managing hardware resources, facilitating communication between hardware and software, and ensuring the smooth execution of processes. If you strip away all the UI and frontend of all operating systems, what is left is the kernel
3. **Machine Accounts:** These will be used for authentication and authorization from system to system or between applications on a system and cannot be assigned to a single person or a group of persons. [3]
4. **Medium Access Control**: A sub-layer of radio interface layer 2 providing unacknowledged data transfer service on logical channels and access to transport channels.
5. **Network Function:** A 3GPP adopted or 3GPP defined processing function in a network, which has defined functional behavior and 3GPP defined interfaces. NOTE 1: A network function can be implemented either as a network element on a dedicated hardware, as a software instance running on a dedicated hardware, or as a virtualized function instantiated on an appropriate platform, e.g., on a cloud infrastructure. [1]
6. **Protocol:** A formal set of procedures that are adopted to ensure communication between two or more functions within the same layer of a hierarchy of functions (source: ITU-T I.112). [3]
7. **Secure state:** A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with an organizational security policy.
8. **Sensitive data:** data that may be used for authentication or may help to identify the user, such as user names, passwords, PINs, cryptographic keys, IMSIs, IMEIs, MSISDNs, or IP addresses of the UE, as well as files of a system that are needed for the functionality such as firmware images, patches, drivers or kernel modules. [3]
9. **Personal data:** Any information relating to an identified or identifiable natural person ('data subject').[3]

Annexure-II

Acronyms

3GPP	-	Third Generation Partnership Project
AAA	-	Authentication, Authorization and Accounting
API	-	Application Programming Interfaces
ARP	-	Address Resolution Protocol
BOOTP	-	Bootstrap Protocol
CAPTCHA	-	Completely Automated Public Turing test to tell Computers and Humans Apart
CD	-	Compact Disk
CDP	-	Cisco Discovery Protocol
CPU		Central Processing Unit
CGI	-	Common Gateway Interface
CWE	-	Common Weakness Enumeration
DDoS	-	Distributed Denial of Service
DoT	-	Department of Telecommunications
DNS	-	Domain Name System
DVD	-	Digital Versatile Disk
FTP	-	File Transfer Protocol
GUI	-	Graphical User Interface
HTTP	-	Hypertext Transfer Protocol
HTTPS	-	HyperText Transfer Protocol Secure
ICMP	-	Internet Control Message Protocol
ICMPv4	-	ICMP version 4
ICMPv6	-	ICMP version 6
IP	-	Internet Protocol
IPv4	-	IP version 4
IPv6	-	IP version 6
IPSEC	-	Internet Protocol Security
ISO	-	International Organization for Standardization
ITSAR	-	Indian Telecom Security Assurance Requirements
ITU-T	-	ITU - Telecommunications Standardization Sector
LLDP	-	Link Layer Discovery Protocol
MAC		Medium Access Control
NF	-	Network Function

NGFW	-	Next Generation Firewall
NTP	-	Network Time Protocol
OAM	-	Operations, Administration and Management
OCSP	-	Online Certificate Status Protocol
OEM	-	Original Equipment Manufacturer
OS	-	Operating System
OSI	-	Open Systems Interconnection
OWASP	-	Open Worldwide Application Security Project
P2P	-	Peer-to-peer
PAD	-	Packet Assembler/Disassembler
PFD	-	Packet Flow Description
PTP	-	Precision Time Protocol
RAN	-	Radio Access Network
RBAC	-	Role-Based Access Control
RCP	-	Rate Control Protocol
RDP	-	Remote Desktop Protocol
REST	-	Representational State Transfer
RPF	-	Reverse Path Filter
RSP	-	Remote Shell Protocol
RTP	-	Real-time Transfer Protocol
SDN	-	Software Defined Networking
SFTP	-	Secure File Transfer Protocol
SMS	-	Short Message Service
SNMP	-	Simple Network Management Protocol
SOCKS	-	SOCKet Secure
SSH	-	Secure Shell
SSI	-	Server Side Includes
SSL	-	Secure Sockets Layer
SYN	-	Synchronize
TCP	-	Transmission Control Protocol
TEC	-	Telecommunication Engineering Centre
TFTP	-	Trivial File Transfer Protocol
TLS	-	Transport Layer Security
TSDSI	-	Telecommunications Standards Development Society India
TSTL	-	Telecom Security Testing Laboratory
UDP	-	User Datagram Protocol

URL	-	Uniform Resource Locator
USB	-	Universal Serial Bus
USIM	-	Universal Subscriber Identity Module
VPN	-	Virtual Private Network

Annexure-III

List of Submissions

List of Undertaking to be furnished by the OEM for Network Next Generation Firewall including IDS & IPS Security Testing Submissions.

1. Source Code Security Assurances (against test case 2.3.3)
2. Know Malware and backdoor check (against test case 2.3.4)
3. No unused software (against test case 2.3.5)
4. No unsupported Components (against test case 2.4.2)
5. Avoidance of unspecified mode of access (against test-case 2.4.3)
6. Cryptographic module Security Assurance (against test case 2.6.2)
7. Cryptographic Algorithms Implementation Security Assurance (against test case 2.6.3

Annexure-IV

References

1. NIST 800-41 - Guidelines on Firewalls and Firewall Policy
2. Security Standard-Firewall Security (SS-013)
3. TSDSI STD T1.3GPP 33.117-17.1.0 V1.1.0 “Catalogue of general security assurance Requirements”
4. https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html
5. https://owasp.org/www-project-top-ten/
6. https://owasp.org/www-project-api-security/
7. RFC 8915 - Network Time Security for the Network Time Protocol (NTP)
8. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
9. https://nvd.nist.gov/vuln-metrics/cvss
10. Next Generation Firewall Test Methodology v9.95 RFC DRAFT
11. RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure.
12. NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)
13. WaTech Firewall Standard
14. ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022)
15. “Security Guidance for 5G Cloud Infrastructure Part III: Data Protection” by NSA &CISAhttps://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_III_508_Compliant.pdf
16. ENISA Recommendation “Standardization in support of the cybersecurity certification”, Dec 2019
17. GSMA NG 133 Cloud Infrastructure Reference Architecture ver 2.0 6.3.7.1 and 6.3.7.2 RFC 6749 - The OAuth 2.0 Authorization Framework
18. CIS_Benchmarks_Password_Policy_Guide_v21.12
19. Cloud Infrastructure Reference Architecture managed by OpenStack
20. IEEE Standard for Local and Metropolitan Area Networks-- Station and Media Access Control Connectivity Discovery
21. RFC 1928 - SOCKS Protocol Version 5
22. NIST IPv6 Profile