


ManySecured CERTIFIED Gateway/Router (GCERT)			
			
ManySecured (https://manysecured.net/)			
Date of Issue:			
			8 August 2022
Version:			
			1.1
Notices, Disclaimer, Terms of Use, Copyright and Trade Marks and Licensing			
Notices:			
Documents published by the IoT Security Foundation (“IoTSEF”) are subject to regular review and may be updated or subject to change at any time. The current status of IoTSEF publications, including this document, can be seen on the public website at: https://iotsecurityfoundation.org/			
Terms of Use:			
The role of IoTSEF in providing this document is to promote contemporary best practices in IoT security for the benefit of society. In providing this document, IoTSEF does not certify, endorse or affirm any third parties based upon using content provided by those third parties and does not verify any declarations made by users.			
In making this document available, no provision of service is constituted or rendered by IoTSEF to any recipient or user of this document or to any third party.			
Disclaimer:			
IoT security (like any aspect of information security) is not absolute and can never be guaranteed. New vulnerabilities are constantly being discovered, which means there is a need to monitor, maintain and review both policy and practice as they relate to specific use cases and operating environments on a regular basis.			

IoTSF is a non-profit organisation which publishes IoT security best practice guidance materials. Materials published by IoTSF include contributions from security practitioners, researchers, industrially experienced staff and other relevant sources from IoTSF's membership and partners. IoTSF has a multi-stage process designed to develop contemporary best practice with a quality assurance peer review prior to publication. While IoTSF provides information in good faith and makes every effort to supply correct, current and high-quality guidance, IoTSF provides all materials (including this document) solely on an 'as is' basis without any express or implied warranties, undertakings or guarantees.

The contents of this document are provided for general information only and do not purport to be comprehensive. No representation, warranty, assurance or undertaking (whether express or implied) is or will be made, and no responsibility or liability to a recipient or user of this document or to any third party is or will be accepted by IoTSF or any of its members (or any of their respective officers, employees or agents), in connection with this document or any use of it, including in relation to the adequacy, accuracy, completeness or timeliness of this document or its contents. Any such responsibility or liability is expressly disclaimed.

Nothing in this document excludes any liability for: (i) death or personal injury caused by negligence; or (ii) fraud or fraudulent misrepresentation.

By accepting or using this document, the recipient or user agrees to be bound by this disclaimer. This disclaimer is governed by English law.

Copyright, Trade Marks and Licensing:

All product names are trade marks, registered trade marks, or service marks of their respective owners.

Copyright © 2022 IoTSF. All rights reserved.

This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license, visit:

[Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

Reqt #	Category	Extracted Reqt																																
1	1 GEN	<p>The vendor must provide release notes for each firmware that comprise a list of software components including their release information and security patch level.</p> <p>The vendor must provide an engineering version of each firmware release that features an access to a root shell via LAN/WLAN interface.</p>																																
2	1 GEN	<p>All services provided by the router MUST be documented by the manufacturer including the port(s) or port ranges used. [A map of network services must be provided to and agreed with the ISP (or user if router is purchased separately).]</p> <p>The router MUST NOT enable services not explicitly advertised as part of the users' service.</p> <p>Any additional functionality that is implemented but not required must be disclosed to and agreed with the ISP.</p>																																
3	1 GEN	<p>In the default configuration (factory/restore setting), only a minimal selection of services SHOULD be available on the LAN and WLAN interface of the router (listed below).</p> <p>[No unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control.]</p> <p>If one of the services offered by the router is deactivated during operation of the router the corresponding port MUST be closed and therefore no longer be available.</p> <table border="1"> <thead> <tr> <th>Service</th> <th>Port</th> <th>Protocol</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>DNS</td> <td>53</td> <td>TCP</td> <td>DNS proxy</td> </tr> <tr> <td>DNS</td> <td>53</td> <td>UDP</td> <td>DNS proxy</td> </tr> <tr> <td>HTTP</td> <td>80</td> <td>TCP</td> <td>Web server (config)</td> </tr> <tr> <td>HTTPS</td> <td>443</td> <td>TCP</td> <td>Web server (config)</td> </tr> <tr> <td>DHCP</td> <td>67</td> <td>UDP</td> <td>DHCP server</td> </tr> <tr> <td>DHCPv6</td> <td>547</td> <td>UDP</td> <td>DHCPv6 server</td> </tr> <tr> <td>ICMPv6</td> <td></td> <td></td> <td>ICMPv6 messages</td> </tr> </tbody> </table>	Service	Port	Protocol	Description	DNS	53	TCP	DNS proxy	DNS	53	UDP	DNS proxy	HTTP	80	TCP	Web server (config)	HTTPS	443	TCP	Web server (config)	DHCP	67	UDP	DHCP server	DHCPv6	547	UDP	DHCPv6 server	ICMPv6			ICMPv6 messages
Service	Port	Protocol	Description																															
DNS	53	TCP	DNS proxy																															
DNS	53	UDP	DNS proxy																															
HTTP	80	TCP	Web server (config)																															
HTTPS	443	TCP	Web server (config)																															
DHCP	67	UDP	DHCP server																															
DHCPv6	547	UDP	DHCPv6 server																															
ICMPv6			ICMPv6 messages																															
4	1 GEN	<p>Functionalities MUST NOT be hidden from the end-user.</p> <p>The user must be able to deactivate unused services and protocols.</p> <p>Functionalities, which are deactivated as a factory setting MUST be made transparent to the end-user IF they become activated during initialization.</p>																																
5	1 GEN	<p>The router MUST run services or applications by applying the principle of least privilege).</p>																																

6	1 GEN	<p>Validation of Data Inputs (all interfaces)</p> <p>Data input to the device via all interfaces shall be validated, to minimally protect the Router from actions such as information leakage, remote code execution and cross-site scripting.</p> <p>Provide input validation at the communication channel layer, including checks of sources, protocols and flows of information.</p> <p>Provide input validation capability at the data interpretation layer, including checks of the commands for IoT applications, their parameters and semantics (to determine possible physical effect).</p> <p>Maintains the integrity and non-repudiation of commands and data at the IoT application layer, including application data encryption, checksum computation and signing, to mitigate threats [T-3],[T-4], [T-5].</p>
7	1 GEN	<p>The operating system of the Home Gateway must be based on (Linux using) a latest stable kernel release with long term support.</p> <p>Protocol stacks available on the device must be implemented robustly.</p>
8	1 GEN	<p>The device (e.g. its bootloader) must allow updating the whole device's firmware.</p> <p>[Firmware updates - To be able to react to newly appearing exploits of soft- or hardware vulnerabilities of the router or any of its components the router MUST have a functionality to update the firmware (operating system and applications) using a firmware package.</p>
9	1 GEN	<p>Vulnerabilities in the software or hardware of the system that have become known must be eliminated or protected against misuse.</p> <p>Vulnerabilities Reporting - a point of contact, e.g., email address and contact number shall be provided to allow the reporting of security vulnerabilities relating to the Residential Gateway.</p>
10	1 GEN	<p>e. Minimum period of the firmware support received by the Router shall be provided upfront to the user.</p>
11	1 GEN	<p>g. Security updates for the Router should be provided in a timely manner. "Timely" in this context varies with the criticality of the identified vulnerability, the availability of a fix and the complexity of fix. The complexity of the fix is dependent on factors, such as constrained devices, involvement of multiple stakeholders, hardware versus software fix, etc.</p>

12	1 GEN	<p>Router firmware and software MUST be updateable via a secure method with minimal user intervention and knowledge/skill. The router MUST allow the end-user to fully control such a firmware update and determine to initiate an online update (router retrieves firmware package from the Internet (WAN interface)) and/ or manually update the firmware through the configuration interface (user provides firmware package).</p> <p>a. The Router shall automatically download the latest security patches. [but MUST be possible for the end-user to deactivate it when using customized settings.]</p> <p>b. The Router shall be updated with the latest security patches automatically. Patching could be carried out through different means and mechanisms, e.g., when Residential Gateway is powered off and on.</p> <p>c. The Router should also provide means for users to manually run and install the downloaded security patches. [The router MUST allow the end-user to fully control such a firmware update and determine to initiate an online update (router retrieves firmware package from the Internet (WAN interface)) and/ or manually update the firmware through the configuration interface (user provides firmware package).]</p> <p>The router SHOULD offer an option to automatically retrieve security relevant firmware updates from a trustworthy source over the Internet (WAN interface). If the router offers this functionality it SHOULD be activated by default, but MUST be possible for the end-user to deactivate it when using customized settings.]</p>
13	1 GEN	<p>The firmware image file must feature a sound integrity protection mechanism and the integrity of the image file must be validated successfully before the image file is installed in the flash memory of the Home Gateway.</p> <p>The firmware update function of the router MUST check the authenticity and integrity of the firmware package (file) before it is installed on the router. This SHOULD [MUST] be done by a Digital Signature that is applied to the firmware package by the manufacturer and checked by the router itself. For this purpose only signature schemes in accordance to [SOG-IS] MUST be used.</p> <p>d. The Router shall verify the patches are digitally signed before installing them. [The firmware image file must feature a sound integrity protection mechanism and the integrity of the image file must be validated successfully before the image file is installed in the flash memory] of the Home Gateway.</p> <p>The router MUST NOT automatically install any unsigned firmware. The router MAY allow the installation of unsigned firmware (i.e. custom firmware) IF a meaningful warning message has been shown to the authenticated end-user and the end-user accepts the installation of the unsigned firmware.</p> <p>Remote upgrade via TFTP MUST be disabled. This feature, if available, would allow the router to listen on the WAN interface for TFTP traffic that could potentially compromise the router firmware.</p>

		<p>f. The device manufacturer should ensure the patches:</p> <ul style="list-style-type: none"> i. do not contain sensitive data such as hardcoded credentials; and ii. are transmitted via secured connection. [firmware MUST support an encryption mechanism.]
14	1 GEN	<p>The device must allow a rollback to the last known good firmware in case that the installation of an update/patch has failed. Security updates cannot be rolled-back, including via a factory reset. [The device must allow a rollback to the last known good firmware in case that the installation of an update/patch has failed.]</p>
15	1 GEN	<p>Data Protection Router uses secure storage for keys, credentials and other sensitive security parameters.</p> <ul style="list-style-type: none"> a. The data elements used by the Router shall be salted and hashed to protect against offline attacks such as brute force or dictionary attacks. Credentials must NOT be stored in cleartext, on any format that can be directly back-calculated or using reversible encryption. b. If the data elements are encrypted, the encrypted key shall be securely stored. Confidential data in the firmware image file must be stored encrypted using the Advanced Encryption Standard (AES) algorithm. c. Encryption algorithms used should be replaceable so that improved encryption algorithms can be adopted without significant change to existing device. <p>The data-encryption-key must be derived at runtime from a key-specific set of certain attributes stored obfuscated within the firmware image file including a random seed. The backup-key must be derived at runtime from a key-specific set of certain attributes including hardware attributes as well as a random seed.</p>

16	1 GEN	<p>The manufacturer of the router MUST provide information on how long firmware updates fixing common vulnerabilities and exposures that have a high severity (i.e. a CVSS combined score higher than 6.0 according to the Common Vulnerability Scoring System assigned to the specific device or a component used by the device) will be made available. This information SHOULD be available on the manufacturer website. Additionally it MAY be made available on the router configuration interface.</p> <p>The manufacturer MUST provide information if the router has reached the End of its Support (EoS) and will not receive firmware updates by the manufacturer anymore. This information (EoS) MUST be made available on the router configuration.</p> <p>The manufacturer MUST provide firmware updates to fix common vulnerabilities and exposures of a high severity without culpable delay (without undue delay) after the manufacturer obtains knowledge.</p>
17	1 GEN	<p>The production version of the firmware release must not implement any kind of shell access or a similar command-line interface at all.</p> <p>OR</p> <p>The router MAY allow access to its command line interface(s) via SSH. SSH access, if supported, MUST NOT be enabled by default. The router MUST NOT allow access to its command line interface(s) via any other protocol.</p>
18	1 GEN	<p>It is RECOMMENDED that the router has a redundant firmware storage in addition to the currently active firmware. In this case the router can start from the redundant firmware storage, if an error occurs during a firmware update process or if the router doesn't start properly after the firmware update.</p>
19	1 GEN	<p>The router MUST use password unique to the unit for default access to its user interface(s).</p> <p>[Router forces both passwords to be changed every 90 days]</p> <p>The MUST prompt the user to change the default password upon first access and any subsequent factory reset.</p> <p>Factory pre-loaded login credentials such as passwords shall be randomised and unique for each Residential Gateway.</p> <p>If pre-loaded login credentials are used and they are not randomised and unique, the Residential Gateways shall be in a disabled state (non-functioning) until the user successfully set new login credentials upon first attempt to access the device's administration login page and the device's configuration settings.</p> <p>[The pre-configured WPA2/WPA3 key (i.e. the WLAN password) must be a random and per device unique value.]</p> <p>IF a preset password is used with factory settings, it MUST NOT contain information that consists of or is derived from data or parts of data that depend on the router itself (e.g. manufacturer, model name, Media Access Control (MAC) address). The preset password used with factory settings MUST NOT be shared by multiple devices of the same manufacturer.</p>

20	1 GEN	<p>The Router shall disable the following system services (on both LAN and WAN interfaces) by default:</p> <ul style="list-style-type: none"> i. WPS ii. HNAP iii. SSH [or should this be allowed for CLI?] 																																
21	2 WAN incl ISP Remote Management	<p>After initialization, only a minimal selection of services MUST be available to the <u>public</u> network - see list below.</p> <p>The services used for Voice over IP (VoIP) telephony (marked with *) MUST only be available IF the router is already configured to use VoIP. The services MUST NOT be available, IF VoIP is deactivated on the router.</p> <p>By default, remote configuration is deactivated on the router; the services used for remote configuration (marked with **) MUST only be available, IF an authenticated user configures the router to use remote configuration. The services MUST NOT be available, IF remote configuration is deactivated on the router.</p> <p>If one of the services offered by the router is deactivated during operation of the router the corresponding port MUST be closed and no longer be available. [The user must be able to deactivate [unused] services and protocols.]</p> <table border="1" data-bbox="544 987 1182 1272"> <thead> <tr> <th>Service</th> <th>Port</th> <th>Protocol</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>CWMP**</td> <td>7547</td> <td>TCP</td> <td>TR-069</td> </tr> <tr> <td>CWMP**</td> <td>7547</td> <td>UDP</td> <td>TR-069</td> </tr> <tr> <td>SIP*</td> <td>5060</td> <td>TCP</td> <td>VoIP</td> </tr> <tr> <td>SIP*</td> <td>5060</td> <td>UDP</td> <td>VoIP</td> </tr> <tr> <td>SIPS*</td> <td>5061</td> <td>TCP</td> <td>VoIP</td> </tr> <tr> <td>SIPS*</td> <td>5061</td> <td>UDP</td> <td>VoIP</td> </tr> <tr> <td>ICMPv6</td> <td></td> <td></td> <td>messages</td> </tr> </tbody> </table>	Service	Port	Protocol	Description	CWMP**	7547	TCP	TR-069	CWMP**	7547	UDP	TR-069	SIP*	5060	TCP	VoIP	SIP*	5060	UDP	VoIP	SIPS*	5061	TCP	VoIP	SIPS*	5061	UDP	VoIP	ICMPv6			messages
Service	Port	Protocol	Description																															
CWMP**	7547	TCP	TR-069																															
CWMP**	7547	UDP	TR-069																															
SIP*	5060	TCP	VoIP																															
SIP*	5060	UDP	VoIP																															
SIPS*	5061	TCP	VoIP																															
SIPS*	5061	UDP	VoIP																															
ICMPv6			messages																															
22	2 WAN incl ISP Remote Management	<p>The Router shall disable the following WAN interfaces by default:</p> <ul style="list-style-type: none"> i. NAT-PMP ii. PCP iii. Remote Administration iv. SNMP v. Telnet vi. UPnP . 																																
23	2 WAN incl ISP Remote Management	<p>The Broadband Forum TR-069 CPE WAN Management Protocol must be implemented for remote device management.</p> <p>The HTTP connection request URL must be unique for each device.</p> <p>The Home Gateway must validate the certificate path of the Auto Configuration Server's TLS sever certificate according to chapter 6 of RFC3280.</p> <p>The TR-069 implementation must not enable the readout of passwords in plain text.</p>																																

24	2 WAN incl ISP Remote Management	Service provider COULD offer security monitoring capability. Provides a monitoring mechanism as a dedicated contract-based service(s), including the isolation of obtained data and the analysis of monitored components, isolation of emergency policy enforcement and an alarm mechanism, isolation and independent execution of the entire monitoring mechanism, facilitating the mitigation of threats.
25	2 WAN incl ISP Remote Management	<p>The router SHOULD allow the end-user to configure a DNS server to be used by entering its IPv4 or IPv6 address.</p> <p>For a higher level of security the router SHOULD implement mechanisms to prevent so called rebind attacks. To prevent DNS spoofing the source ports and Transaction-IDs MUST be selected randomly by the router.</p> <p>The router MUST support forwarding of DNSSEC packets according to [IETF RFC 6781] and DANE packets according to [IETF RFC 6698].</p>
26	2 WAN incl ISP Remote Management	<p>The DNS proxy implementation must be compliant to chapter 3 “Transparency Principle” and chapter 4 “Protocol Conformance” of RFC 5625.</p> <p>The DNS proxy must apply the query matching rules defined in section 9.1 “Query Matching Rules” of RFC 5452.</p> <p>The DNS proxy must implement an unpredictable query ID for outgoing queries, utilizing the full range available (0-65535).</p> <p>The DNS proxy must extend the query ID space by using unpredictable source ports.</p> <p>The DNS proxy must not support DNS queries on any WAN interface.</p> <p>The DNS Proxy must mitigate DNS rebinding attacks.</p>
27	2 WAN incl ISP Remote Management	<p>The router SHOULD implement Internet Protocol version 6 (IPv6) and offer its services accordingly. Due to the importance of the Internet Control Message Protocol (ICMP) when using IPv6 it is RECOMMENDED that the router only supports the types of messages marked with an “X” in Table 7: ICMPv6 message types.</p> <p>The router MUST NOT forward inbound IPv6 traffic IF it does not belong to a known connection.</p>

28	2 WAN incl ISP Remote Management	IF the router offers a VPN feature it SHOULD allow the end-user to configure it as a VPN server. RECOMMENDED protocols are IPsec, L2TP over IPsec and OpenVPN. Suitable cryptographic parameters for IPsec are defined in [TR-02102-3] and SHOULD be used accordingly.
29	2 WAN incl ISP Remote Management	The Router shall disable IPv6 tunnelling mechanisms by default.
30	2 WAN incl ISP Remote Management	DMZ (demilitarized zone), if available, is disabled by default.
31	2 WAN incl ISP Remote Management	Ping response setting is disabled by default.
32	2 WAN incl ISP Remote Management	The router MUST NOT enable FTP by default. The router MAY enable SFTP if it is required for NAS services. The FTPS protocol must be supported in order to enable a secure file transfer over the Internet.
33	2 WAN incl ISP Remote Management	The router MUST NOT ever use the same username or password for remote (WAN) access to its user interface(s) and local (LAN) access to its user interface(s).
34	3 LAN	The router MUST support using DHCP for devices connected on the LAN and WLAN interface. The User should have option to use static IP addresses or define a range of DHCP (Dynamic Host Configuration Protocol) reserved addresses. The router SHOULD provide an option to manually set the DNS server being used by all devices connected to the router via Dynamic Host Configuration Protocol (DHCP). This feature enables the end-user to configure DNSSEC verifying DNS servers manually if the DNS servers of the IAP do not offer DNSSEC verification.

35	3 LAN	<p>The Broadband Forum TR-064 CPE LAN Management Protocol must be implemented for local device management (adds security functions to UPnP IGD).</p> <p>The TR-064 service including the corresponding UPnP SSDP service must only be accessible via LAN and private WLAN interfaces.</p> <p>All TR-064 actions that are modifying the configuration of the Home Gateway and that are reading out confidential data (e.g. usernames, firewall configuration, etc.) must require a HTTP digest authentication by the device password.</p> <p>The TR-064 web service must enforce transport layer security (TLS 1.2) for all actions, which require an authentication and which transport confidential data.</p> <p>The TR-064 web-service implementation must validate each SOAP request so that malformed requests or requests that contain invalid parameters are rejected.</p> <p>The TR-064 actions “AddPortMapping” and “AddForwardingEntry” must only accept IP addresses within the subnet range of the trusted home network (i.e. any LAN and private WLAN interface) for internal clients. But these actions must not accept an IP-address of any LAN / WLAN interface of the Home Gateway itself.</p> <p>The TR-064 implementation must not enable the readout of passwords in plain text.</p>
36	3 LAN	<p>Turn the network off when not in use. It may be impractical to turn devices off and on frequently, but consider this approach during travel or extended periods offline</p> <p>[Drafting note: some ISP/CSPs perform traffic analyses and may 'throttle back' connection speeds if router is switched off].</p> <p>[A user action rather than router function. Auto hibernate may be an alternative based upon internal traffic, but how would a Wi-Fi connected device reactivate the router? Also, some devices 'ping' cloud services frequently, so router would never go into hibernation].</p>
37	4 MGMT	<p>The web GUI must only be accessible via private LAN/WLAN interfaces.</p>
38	4 MGMT	<p>Unprotected access to the Residential Gateway's management webpage shall be prohibited. Access to the Residential Gateway's management webpage shall only via strongly authenticated credentials.</p> <p>Authentication credentials shall be salted and hashed.</p> <p>The router MUST reject attempts to connect to its user interface(s) using incorrect credentials.</p> <p>Secure alternative authentication mechanism or physical factory reset shall be provided to fall-back upon when a login account is blocked.</p> <p>The router MUST NOT be initialized with accounts undocumented to the end-user.</p>

39	4 MGMT	<p>Access to the configuration MUST at least be secured by a password in the initialized and customized state.</p> <p>The router MAY offer a higher level of security by providing alternative authentication mechanisms that offer a higher level of security like requiring the usage of One Time Passwords (OTP), hardware token or similar techniques to realize 2-Factor-Authentication. [Login to the router's user interface(s) SHOULD use a 2-pass challenge mechanism. If used, it MUST NOT be dependent on connections to WAN resources.]</p> <p>A challenge handshake authentication protocol implementing mechanisms comparable to CHAP defined in RFC1994 must be implemented to verify the device password.</p> <p>If a password is used as part of the authentication then:</p> <ol style="list-style-type: none"> a. The minimum length of a password shall be 12, and shall meet at least 3 out of the following 4 complexity rules: <ol style="list-style-type: none"> i. Minimally 1 uppercase character (A-Z) ii. Minimally 1 lowercase character (a-z) iii. Minimally 1 digit (0-9) iv. Minimally 1 special character (punctuation and/or space) b. The password shall not have consecutive identical characters. c. Values used in the login ID and password shall not be the same. <p>An authenticated administrator MUST be able to change the password after entering the previous password.</p> <p>Router SHOULD provide a mechanism to indicate the password strength based on the entropy of the password entered by the user.</p>
40	4 MGMT	<p>Change the default login username and password every 30 to 90 days. A strong password (14 letters/numbers or more) is recommended.</p> <p>Change the pre-set passphrase on your router</p>
41	4 MGMT	<p>The Router management interface MUST be protected against brute force and/or other abusive login attempts to the administration page/settings [ENISA GP-TM-25]:</p> <p>The router MUST use exponential rate limiting of login attempts upon failed login attempts (e.g. tarpit).</p> <p>The login account shall be blocked after a fixed number of unsuccessful login attempts.</p>
42	4 MGMT	<p>The Home Gateway web GUI application must only accept one active authenticated session at any time.</p> <p>The Home Gateway web GUI application must provide a logout functionality that enables the user to terminate the current web GUI session.</p>

43	4 MGMT	<p>After authentication the session of the authenticated end-user MUST be protected against session hijacking attacks. Minimal requirements for such a protection are a session time out and the use of a CSRF token.</p> <p>[For every request to the web GUI application that causes data to be read or modified, an additional security attribute ("anti-CSRF token") must be incorporated as a hidden field, transmitted and successfully validated by the web application before the requested action is executed.]</p> <p>A session identifier (session cookie) must be not guessable, that means:</p> <ul style="list-style-type: none"> • The session identifier must be unique for each session. • The entropy of the session identifier must be at least 64 bit, which means > 20 digits [0...9] or > 10 characters [A-Z, a-z, 0-9]. • Session identifiers must be generated randomly each time a session starts.
44	4 MGMT	<p>Device Management Interface.</p> <p>The router MUST use HTTPS over TLS 1.2 or later for access to its graphical user interface (GUI).</p> <p>[the Device management interface to the Router shall be protected via international standardised secure communication protocol such as HTTPS to prevent the communication channel from being sniffed by unauthorised actors with malicious intent. Signed certificates from a Certification Authority ("CA") and self-signed certificates can be considered for this purpose.]</p> <p>[The Home Gateway must provide a device specific self-signed sever certificate for TLS.]</p> <p>A reset to the factory-default state of the Home Gateway must trigger the generation of a new self-signed TLS server certificate.</p>
45	4 MGMT	<p>Credentials Handling - the Router shall ensure that the credentials are properly managed to avoid them being compromised when they are used:</p> <ol style="list-style-type: none"> a. Password fields shall prevent its contents from being copied. b. Password shall not be displayed by default on a user's screen and shall be masked with the asterisk character, or another benign glyph. Router may have an option to unmask passwords at user's own discretion. c. Password recovery or reset mechanism shall be protected and does not supply an attacker with any form of information indicating a valid account [ENISA GP-TM-26] d. Network management credentials, e.g., remote login credentials specified in Broadband Forum's Technical Report 069 ("TR-069"), shall not be displayed on the Router's management web page. <p>Confidential data in the firmware image file must be stored encrypted using the Advanced Encryption Standard (AES) algorithm.</p>
46	4 MGMT	<p>The web GUI must prevent the browser from storing the content of any password in form fields (AutoComplete makes it easier for malware to gain unauthorised access).</p> <p>Any response of the web GUI application must not contain confidential data that are not absolutely necessary for any use case.</p>

		Any input data sent by a client must be validated by the web GUI application.
47	4 MGMT	Initial Setup Handling - First attempt to access to the Router's administration page/settings SHOULD be conducted through a wired connection. If a wireless connection is used, the wireless communication SHOULD leverage on at least AES encryption, with at least WPA2 CCMP protection.
48	4 MGMT	Administrator workstations used to manage the router should be locally connected or on a trusted segment of the network to mitigate outsiders sniffing the management data and collecting information about your network.
49	4 MGMT	Access to the configuration over the WAN interface must be deactivated in the factory setting. IF the router offers remote configuration the status of this functionality (active/ inactive) MUST be made available to the end-user. If the router allows access the configuration over the WAN interface (e.g. Webserver, App) as a customization feature this communication MUST be encrypted using TLS version 1.2 or newer. The end-user SHOULD be able to configure the port to be used for access to the configuration via the WAN interface.
50	4 MGMT	The router MAY offer an option to save the current configuration of the router to a file. This backup can be used to easily restore a previously running configuration on the same router model. To export and/ or import the router settings the end-user MUST be successfully authenticated at the device. The configuration file SHOULD only be exported in an encrypted way and SHOULD be protected by a user selected password. The end-user SHOULD be assisted upon setting the password by a mechanism indicating the strength of the password. Confidential configuration data must be stored encrypted using the Advanced Encryption Standard (AES).

51	4 MGMT	<p>The application must provide a system log that informs the user about security relevant events. Router logging is enabled by default. Logs store a minimum of 90 days of events. To maintain a secure operation of the router the device MUST provide the necessary security relevant information to the authenticated end-user. [Security-relevant logging must be forwarded to a separate log server immediately after it has been generated]. The information does not have to be permanently saved on the router and made available by the router after reboot. The information on the state of the various functionalities of the router SHOULD be made available at a central source of information (e.g. on a specific site on the configuration interface). Each event SHOULD include the time and date, the IP address and the MAC address of the device generating the event. An event SHOULD be generated for a change in any of the following:</p> <ul style="list-style-type: none"> • Firmware Status • Firewall Status • Remote Configuration • Login Attempt(s)/ Log • Running Services • Connected Devices • System Status/ Log • Intrusions, probes, attacks, etc
52	4 MGMT	Log messages must not disclose any confidential data like cryptographic keys and passwords.
53	4 MGMT	The Router shall disable feature(s) that collects and sends the device's network statistics data back to manufacturer by default.
54	4 MGMT	Running Services - The router MUST display a summary page for the currently active services on all interfaces (LAN, WLAN(s) and WAN). This especially refers to those services optionally provided by the router. The router SHOULD display exact details on the services running (e.g. service and port(s) being used). Detail of running services to include those offered to the private network and the public network by the router.
55	4 MGMT	Connected Devices - The router SHOULD display information of the devices that are currently connected to the router and the interface (LAN, WLAN(s) or WAN) being used for this connection. This information MUST include the devices IP address, MAC address and SHOULD contain information on the duration of the connection.
56	4 MGMT	Firewall Status - The router MUST allow the end-user to display the current state (active/ inactive) of the firewall. The router MUST display the rule set currently set up by the enduser (e.g. port forwarding configuration).

57	4 MGMT	<p>Firmware Status - The router MUST allow the end-user to display the version number of the firmware currently installed on the router.</p> <p>The router MAY additionally show an estimate date of the firmware such as the release date, compilation date or the date of the installation of the firmware on the router.</p> <p>If the router has obtained knowledge that the firmware installed on it is currently out-of-date the router MUST inform the end-user about this with a meaningful message (e.g. display Pop-Up after Log-In).</p> <p>As soon as a decision is made by the manufacturer to not support (release firmware updates) for the router anymore the same mechanism MUST be used by the manufacturer to inform the end-user about the End of Service (EoS) of the router.</p>
58	4 MGMT	<p>The router SHOULD provide a functionality to send (push) notifications of security relevant events (e.g. changes to the configuration, protocols of observed attacks on the firewall, firmware updates) to the enduser additionally to providing the information on request.</p> <p>The device must provide a means to notify users of available updates.</p> <p>The functionality to send (push) notifications MUST only be activated upon the enduser's request.</p> <p>This functionality MUST always be encrypted (TLS version 1.2 or stronger) and MAY be provided through eMail, an App or similar techniques.</p>
59	4 MGMT	<p>The router MUST allow an authenticated end-user to reset the router back to factory settings from an initialized or end-user customized state by deleting the personal data and settings of the end-user from the router.</p> <p>A reset to the factory-default state of the Home Gateway must trigger the generation of a new self-signed TLS server certificate, since a user might import this certificate into their devices/browser.</p>
60	4 MGMT	<p>The router MAY offer remote configuration of the device either by the ISP or the manufacturer. For retail devices that are not pre-configured with end-user specific settings remote configuration MUST NOT be active before initialization.</p> <p>Remote configuration MUST only be allowed with an encrypted and (server-) authenticated connection. The router MUST reject attempts to connect to its user interface(s) using incorrect credentials.</p> <p>It MUST be visible to the end-user if remote configuration is currently activated.</p>
61	4 MGMT	<p>By default:</p> <p>Disable USB, console and other local connection sockets [user should enable sockets through admin interface].</p> <p>Anti-tamper seals/tape should be placed on at least two locations that are necessary to be opened to enable access to the router internals.</p>

62	4 MGMT	Security integration security capability. Provides the ability to integrate different rules and policies for input validation at different layers if diverse technologies are employed by these layers, facilitating the mitigation of threats.
63	4 MGMT	Router automatically logs out the administrator account within 20 minutes of inactivity. The Home Gateway web GUI application must invalidate the authenticated session after a time of inactivity that is not longer than 20 minutes.
64	4 MGMT	The embedded HTTP server on the Home Gateway must be installed in an absolutely minimum configuration. The web server document root directory must be separated from any Linux system directory and it must not include any files containing confidential information. The CGI directory must not contain executables which can be used for attacks, e.g. interpreters and shells.
65	5 IF incl Wi-Fi	The router Wi-Fi access MUST be protected by strong authentication by default [no open access, unless configured by Administrator]. If a password is used as part of the authentication then: <ul style="list-style-type: none"> • The pre-configured key (i.e. the WLAN password) must be a random and per device unique value. Passphrase MUST NOT contain information that consists of or is derived from data or parts of data that depend on the router itself (e.g. manufacturer, model name, Media Access Control (MAC) address). The passphrase configured in factory settings SHOULD have a length of at least 20 digits consisting of the numbers 0-9 (and uppercase letters A-Z without I or O).] <ul style="list-style-type: none"> • OR Router forces the administrator to enter a new Wi-Fi password upon initial configuration and any subsequent factory reset. • The router MUST allow an authenticated end-user to set the passphrase to a different value. It must not be possible to set a WLAN password that is shorter than 8 characters. • Router SHOULD provide a mechanism to indicate the password strength based on the entropy of the password entered by the user. [Router checks that the minimum length of password is 14 letters/numbers.] • Password based authentication MUST be protected against brute force attacks. • [Router forces both passwords to be changed every 90 days]
66	5 IF incl Wi-Fi	Encryption MUST be enabled by default [for user data and in some cases signalling, control and management plane data]. The wireless LAN interface must support WPA2 and WPA3. By default the wireless LAN must be encrypted using at least WPA2 and the CCMP protocol. Only WPA3 or WPA2-AES CCMP is used. If weaker security protection such as WPA is chosen by users, warning(s) of the higher security risk to use these encryption algorithms shall be displayed.

		WEP and WPA-Personal (or WPA-PSK) should be avoided, and only used with a 128-bit key option.
67	5 IF incl Wi-Fi	Limit WLAN coverage by: Enabling user to adjust Wi-Fi signal strength. [Use directional antenna(s) to direct WLAN coverage]
68	5 IF incl Wi-Fi	WPS SHOULD be disabled by default. Wi-Fi Protected Setup - The router MAY implement Wi-Fi Simple Configuration (WSC) version 2.0.2 or above, according to [WSC2] to provide an easier way of registering user devices at the router. The user must be able to permanently deactivate the WSC (WPS) protocol. The activation of the WSC registration protocol must require a user interaction at the Home Gateway. Push Button Configuration (PBC) and USB Flash Drive (UFD) MAY be offered. Personal Identification Number (PIN) based WPS MAY only be used, IF the feature is deactivated in the initialized state and a new PIN is generated for each newly registered device. [The WLAN access point must always generate a fresh, random device PIN each time before the WSC registration protocol with the external registrar PIN method is activated.] Performing WPS based on Near Field Communication (NFC) SHOULD be deactivated in the initialized state. The WLAN access point of the home gateway must limit the activation time of the registration protocol.
69	5 IF incl Wi-Fi	If the Router provides a secondary (guest) network then: - It SHOULD be disabled by default - MUST NOT allow communication with the private WLAN or LAN network (and devices connected to those networks). - MUST NOT allow access to the Router configuration settings. - MUST be issued with a separate access password.
70	5 IF incl Wi-Fi	In factory settings the Extended Service Set Identifier (ESSID) SHOULD NOT contain information that consists of or is derived from data or parts of data that depend on the router model itself (e.g. model name). This requirement does not apply to the Basic Service Set Identifier (BSSID) used by the router. An authenticated user SHOULD be able to hide the broadcast of the SSID. Default SSID: • Minimum length is greater than eight characters long. • Uses combination of alphanumeric and symbols. • Does NOT readily identify manufacturer or model of router. The router MUST allow an authenticated end-user to change the ESSID: • Enforce minimum length to be greater than eight characters long.

		<ul style="list-style-type: none"> •Enforce use alphanumeric and symbols in the SSID. •[Enforce change of the SSID on a reoccurring basis].
71	5 IF incl Wi-Fi	<p>The UPnP A/V server must only be accessible via the home network (i.e. via LAN and private WLAN interfaces).</p> <p>The UPnP A/V server must limit the file system access to the file system of an attached USB storage.</p>
72	5 IF incl Wi-Fi	<p>The FTP(S) server must rely on the identity management of the NAS server.</p> <p>If WAN access is required for FTP(S) then the identity management must support to enable / disable FTP(S) WAN access for each NAS user individually.</p> <p>The FTP(S) Server must limit the file system access to the file system of an attached USB storage</p>
73	5 IF incl Wi-Fi	<p>The NAS server must only be accessible via the home network (i.e. via LAN and private WLAN interfaces).</p> <p>The NAS server must limit the file system access to the file system of an attached USB storage.</p> <p>The NAS server must support users with different access rights to the file system of the attached storage.</p> <p>If NAS user passwords are set the Home Gateway must enforce the following policy:</p> <ul style="list-style-type: none"> • The password has a length of 8 - 32 characters. • The password can consist of the following classes of characters: numbers, lowercase/uppercase letters and special characters (e.g. “! ” \$ % & / () = + * # ; , . “”). • The password must at least consist of two different character classes.
74	5 IF incl Wi-Fi	<p>The USB device class support of the embedded Linux operating system of the Home Gateway must be limited to the required ones.</p> <p>The Home Gateway must not execute any code that is stored on USB mass storage devices.</p>

75	5 IF incl Wi-Fi	<p>A router MAY support the use of Voice over IP (VoIP) for IP based communication. If the router provides this kind of functionality it SHOULD be implemented in a way that the end-user can turn off the functionality completely and certain phone numbers can be blocked in a dedicated blocked list (denied list).</p> <p>The RTP protocol implementation must not disclose any confidential information about the source of the data stream.</p> <p>The SIP user agent must only accept and process SIP requests from the call control it is registered to.</p> <p>The router MUST NOT respond to SIP requests to unknown communication partners on the WAN interface.</p> <p>The WAN interface does not have extensions that do not require an authentication (noauth).</p> <p>The services providing VoIP functionalities MUST only be running as long as IP based communication is activated.</p>
76	5 IF incl Wi-Fi	<p>The DECT/CAT-iq base station implemented in the Home Gateway must enforce a mutual authentication between a handset and the base station (DSSA2 with a minimum 32-bit authentication vector).</p> <p>The DECT/CAT-iq base station in the Home Gateway must enforce an encrypted transmission of voice and signalling data to the handset.</p> <p>The DECT base station in the Home Gateway must implement a cryptographic strong random number generator so that strong encryption keys are generated.</p>
77	6 SEC incl Firewall	<p>The router MUST contain firewall functionalities that include the basic monitoring and controlling of how IP packets between the private network of the end-user (WLAN and LAN interface) on the one side and the public network i.e. Internet (WAN interface) on the other side are exchanged.</p> <p>Router firewall is enabled by default. The firewall functionalities of the router MUST be enabled after initialization.</p> <p>The firewall must implement a stateful packet filter.</p> <p>After initialization the firewall SHOULD allow all outgoing communication from the private network and deny all not requested incoming communication from the public network. By default, all incoming connections on any WAN interface must be denied.</p> <p>The firewall MUST NOT contain any port forwarding rules configured initially.</p>
78	6 SEC incl Firewall	<p>The router MUST allow the end-user to define rules for incoming network traffic (public to private network) as well as outgoing (private to public network) network traffic. To support an easier configuration a list of ports used by common Internet services MAY be provided by the router configuration.</p> <p>Forwarding rules to any IP address of the LAN/WLAN interface of the Home Gateway must not be accepted by any device configuration</p>

		<p>option accessible to the user.</p> <p>User should be able to (easily) configure Allowed/Disallowed lists, if available.</p>
79	6 SEC incl Firewall	<p>The firewall/network subsystem must implement a strong end system model according to section 3.3.4.2 multihoming requirements of RFC1122.</p> <p>The Router shall support NAT to prevent its internal systems from being accessed directly from the Internet.</p> <p>If the device has firewall functionality, an IPv4 stack and NAT functionality, the firewall must implement "port-restricted cone" NAT (RFC3489).</p> <p>The IPv6 firewall must enforce a similar network security model than the IPv4 NAT firewall.</p> <p>Disable bridging.</p> <p>Maintains the integrity and authenticity of commands and data at the communication channel layer, including protocol data encryption.</p>
80	6 SEC incl Firewall	<p>Router provides attack detection capability, including detection of probing, infrastructure attacks, remote attacks, insider attacks and system misuse, to mitigate threats [T-1], [T-3].</p> <p>User can apply a firewall or MAC filtering rule on the router to prevent devices from using the network. [Explicit allowed list alternative?].</p> <p>Router provides the ability to monitor the load on equipment and communication channels, including the detection of both unintentional overload and denial of service attacks, to mitigate threats [T-1], [T-2], [T-5].</p> <p>Router provides a reliable communication capability, including resistance to channel overflow and denial of service attacks, to mitigate threats [T-1], [T-2], [T-5].</p> <p>Router provides the ability to detect attacks on recovery and response capabilities to mitigate threats [T-1], [T-2], [T-5].</p> <p>The router COULD provide an intrusion detection system (IDS)/intrusion prevention system (IPS) [Note: typically found on high-spec equipment].</p>

81	6 SEC incl Firewall	<p>Protection mechanisms against Denial of Service (DoS) attacks is also required, at least for the following list:</p> <ul style="list-style-type: none"> • Tear Drop • Ping of Death • Smurf • Fraggel • UDP Flood • SYN-ACK <p>ICMP flooding LAND attack IP fragmentation attacks</p> <p>The IPv6 firewall must mitigate the Neighbour Discovery Protocol table exhaustion attack.</p>
82	6 SEC incl Firewall	<p>Data Protection</p> <p>Router uses secure storage for keys, credentials and other sensitive security parameters.</p> <p>a. The data elements used by the Router shall be salted and hashed. b. If the data elements are encrypted, the encrypted key shall be securely stored. c. Encryption algorithms used should be replaceable so that improved encryption algorithms can be adopted without significant change to existing device.</p>
83	6 SEC incl Firewall	<p>The Firewall MUST NOT reveal closed ports during a port scan.</p>
84	8 TBC	<p>Segment, packet and frame PDU filters in any physical or logical interface, and in the incoming and/or outgoing directions simultaneously with fine-grained – per subscriber - granularity. Filters will be able to take into account any combination of the following arguments:</p> <ul style="list-style-type: none"> • source/destination IP address •source/destination port •protocol •source/destination •MAC address •VLAN •TCP flags •fragmentation flags •ICMP type •packet size <p>There must be counters available for each rule in the filter, increasing with each matching packet, and available for consultation via SNMP.</p>
85	8 TBC	<p>Mgt Ops support:</p> <ul style="list-style-type: none"> • TACACS+ for authentication and authorization of the CLI features. • Logging of all the commands executed by all the operators, for audit purposes. • SSH sessions with 3DES encryption – and not preclude options to use more advanced encryption methods e.g. AES-128 or AES-256.

		<ul style="list-style-type: none"> • Restriction of the management access only to a defined subset of IP addresses.
86	8 TBC	In the data plane, the platform must support Unicast Reverse Path Forwarding (URPF), (RFC3704). Further, for PPP Termination and Aggregation (PTA) sessions, uRPF must be applied per subscriber. It must also be capable of limiting the maximum number of MAC addresses and limiting the BUM (broadcast, unknown unicast and multicast) traffic per physical or logical interface.
87	8 TBC	Mechanisms to moderate control protocol (e.g. LCP) traffic load per subscriber(requests rate, filters, etc.) shall be implemented.
88	8 TBC	Architecture must ensure the maximum possible isolation between the control and management planes, and the data plane.