|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Security Category | Measurement Criteria | Scoring Scale (0-10 or Yes/No) | Source/Justification | Notes |
| Default Credentials | Are default credentials required to be changed upon initial setup? |  | Source: **Cable Labs.** (2021). *Gateway device security best common practices 5* (CL-GL-GDS-BCP-V01-211007, Version 01-211007). Cable Labs. <https://account.cablelabs.com/server/alfresco/1209eea3-bd81-40cb-9a18-21bd6cfcd80d>  <https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/ict-standards/telecommunication-standards/radio-comms/imda-ts-rg-sec.pdf>  Justification: Easy to test & check to see if present | REQ OOB-006  4.1.1 - IMDA |
| Optional Network Services | Are optional network services disabled by default? |  | Source: **Cable Labs.** (2021). *Gateway device security best common practices 5* (CL-GL-GDS-BCP-V01-211007, Version 01-211007). Cable Labs. <https://account.cablelabs.com/server/alfresco/1209eea3-bd81-40cb-9a18-21bd6cfcd80d>  <https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/ict-standards/telecommunication-standards/radio-comms/imda-ts-rg-sec.pdf>  Justification: Easy to test & check to see if present | REQ OOB-005  4.2.1 – IMDA  a. The Residential Gateway shall disable the following system services (on both LAN and WAN interfaces) by default: i. WPS ii. HNAP iii. SSH b. The Residential Gateway shall disable the following Residential Gateway WAN interfaces by default: i. NAT-PMP ii. PCP iii. Remote Administration iv. SNMP v. Telnet vi. UPnP |
| Firewall Enabled by Default – NAT Support | Is the firewall enabled by default and is NAT supported to prevent internal systems from being accessed directly from the internet? |  | <https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/ict-standards/telecommunication-standards/radio-comms/imda-ts-rg-sec.pdf> | 4.2.d - IMDA |
| Factory Rest | Can the device be factory reset erasing all customer and configuration data? |  | Source: **Cable Labs.** (2021). *Gateway device security best common practices 5* (CL-GL-GDS-BCP-V01-211007, Version 01-211007). Cable Labs. <https://account.cablelabs.com/server/alfresco/1209eea3-bd81-40cb-9a18-21bd6cfcd80d>  Justification: Easy to test & check to see if present | REQ OOB-009 |
| Remote Access | Is remote access to the admin interface disabled until the password has been changed by the user or it has a device-unique password? |  | Source: **Cable Labs.** (2021). *Gateway device security best common practices 5* (CL-GL-GDS-BCP-V01-211007, Version 01-211007). Cable Labs. <https://account.cablelabs.com/server/alfresco/1209eea3-bd81-40cb-9a18-21bd6cfcd80d>  Justification: Easy to test & check to see if present | REQ OOB-008  Device-unique is a different id per same device. No two devices have the same password. |
| Password Strength | Are weak passwords allowed to be set? |  | Source: **Cable Labs.** (2021). *Gateway device security best common practices 5* (CL-GL-GDS-BCP-V01-211007, Version 01-211007). Cable Labs. <https://account.cablelabs.com/server/alfresco/1209eea3-bd81-40cb-9a18-21bd6cfcd80d>  Justification: Easy to test & check to see if present | REQ OOB-012  4.1.2 – IMDA Password Strength |
| Encryption at Rest | Is all confidential or sensitive data in flash memory encrypted at rest? |  | Source: **Cable Labs.** (2021). *Gateway device security best common practices 5* (CL-GL-GDS-BCP-V01-211007, Version 01-211007). Cable Labs. <https://account.cablelabs.com/server/alfresco/1209eea3-bd81-40cb-9a18-21bd6cfcd80d>  Justification: Privacy of data needs to be encrypted. Will have to define “confidential” and link that to a standard as well as encryption levels. | REQ DRP-001  Encryption at rest best practices NIST. Definition of confidential or sensitive data? Maybe rate on level of encryption |
| TLS | Only approved TLS connections used? |  | Source: **Cable Labs.** (2021). *Gateway device security best common practices 5* (CL-GL-GDS-BCP-V01-211007, Version 01-211007). Cable Labs. <https://account.cablelabs.com/server/alfresco/1209eea3-bd81-40cb-9a18-21bd6cfcd80d>  Justification: Privacy of data needs to be encrypted. Will have to define “confidential” and link that to a standard as well as encryption levels. | REQ DE-002  Link to NIST standard on TLS encryption standards: NIST Special Publication (SP) 800-52 Rev. 2. TLS 1.2 and above. TLS 1.3 preferred (more points for this?) TLS 1.2 acceptable |
| Hash default | Is the default configuration a hash function of a security strength similar to SHA2 or higher? |  | Source: **Cable Labs.** (2021). *Gateway device security best common practices 5* (CL-GL-GDS-BCP-V01-211007, Version 01-211007). Cable Labs. <https://account.cablelabs.com/server/alfresco/1209eea3-bd81-40cb-9a18-21bd6cfcd80d> | REQ DE-006  SHA 1 and MD5 are deprecated |
| Disabling Cipher Suite | Is disabling a cipher suite allowed? |  | Source: **Cable Labs.** (2021). *Gateway device security best common practices 5* (CL-GL-GDS-BCP-V01-211007, Version 01-211007). Cable Labs. <https://account.cablelabs.com/server/alfresco/1209eea3-bd81-40cb-9a18-21bd6cfcd80d>  Justification: Allowing the disabling of less secure cipher suites enforces the use of more secure cipher suites. | REQ DE-007 |
| Ports | Are all physical and/or local communications ports that are not required for normal operations disabled by default? |  | Source: **Cable Labs.** (2021). *Gateway device security best common practices 5* (CL-GL-GDS-BCP-V01-211007, Version 01-211007). Cable Labs. <https://account.cablelabs.com/server/alfresco/1209eea3-bd81-40cb-9a18-21bd6cfcd80d> | REQ MI-003 |
| MFA | Does the device support MFA for admin access? |  | Source: **Cable Labs.** (2021). *Gateway device security best common practices 5* (CL-GL-GDS-BCP-V01-211007, Version 01-211007). Cable Labs. <https://account.cablelabs.com/server/alfresco/1209eea3-bd81-40cb-9a18-21bd6cfcd80d> | REQ MI-004 |
| Reauthentication | Is reauthentication required after a configurable period of inactivity?? |  | Source: **Cable Labs.** (2021). *Gateway device security best common practices 5* (CL-GL-GDS-BCP-V01-211007, Version 01-211007). Cable Labs. <https://account.cablelabs.com/server/alfresco/1209eea3-bd81-40cb-9a18-21bd6cfcd80d> | REQ MI-009  NIST 800-63B for reauthentication and timeout periods  30 min per MI-010 |
| Input Validation | Are all inputs validated to prevent improper resource use? |  | Source: **Cable Labs.** (2021). *Gateway device security best common practices 5* (CL-GL-GDS-BCP-V01-211007, Version 01-211007). Cable Labs. <https://account.cablelabs.com/server/alfresco/1209eea3-bd81-40cb-9a18-21bd6cfcd80d>  Justification: This is important but t]his may be hard to prove | REQ MI-012  OWASP PC C4 and C5 sections |
| Updates | Does the manufacturer upgrade any software component/library with known applicable security vulnerabilities in a timely manner? |  |  | REQ SBOM-010 |
| Web GUI HTTPS | Does the Web GUI use HTTPS? |  |  | REQ NETS-001 |
| Telnet of FTP | Is Telnet and FTP not allowed to be enabled? |  |  | REQ NETS-005 |
| Necessary Protocols | Does the firewall on the device only permit required protocols and services by default? |  |  | REQ NETS-007 |
| Wi-Fi Security | Is WPA2 or higher enabled by default? |  |  | REQ NETA-002 |
| Wi-Fi WPA | If WPA is selected by end user, is a security warning messaged displayed? |  | <https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/ict-standards/telecommunication-standards/radio-comms/imda-ts-rg-sec.pdf> | 4.4.b IMDA |
| Firmware Updates | Are the latest patches automatically downloaded and applied in a timely manner? |  | <https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/ict-standards/telecommunication-standards/radio-comms/imda-ts-rg-sec.pdf> | 4.3.a & 4.3.g IMDA |

Usability note: 4.1.2 GEN.OPS – Device Operation

<https://rg-device-requirements.broadband-forum.org/index.pdf>

GEN.OPS.4 – The life expectancy of the residential gateway device should be at least 7 years.

GEN.OPS.10 - The RG SHOULD be self­installable by an end user in under 20 minutes assuming the default configuration and mode of operation. This is the time from when the box is opened to when the user is using the service including any driver installation (assuming no network complications and excluding micro­filter installation and customer ordering/ registration).