LACNOG-M3 AAWG Conjuntas Mejores prácticas operativas actuales sobre requisitos mínimos de seguridad para la adquisición de equipos de locales del cliente (CPE)

LAC-BCOP-1

Mayo 2019

Este documento está disponible en el sitio web de LACNOG en www.lacnog.net/docs/lac-bcop-1

Este documento está disponible en la M3 Sitio web de AAWG en www.m3aawg.org/CPESecurityBP

Este es un documento conjunto de Mejores Prácticas Operativas Actuales (BCOP) desarrollado por LACNOG[1] (Grupo de Operadores de Red de América Latina y el Caribe) y M3 AAWG[2] (Grupo de trabajo de mensajería, malware y móvil contra el abuso). Es el producto de los borradores originales de LACNOG de sus grupos de trabajo LAC-AAWG[3] (Grupo de trabajo contra el abuso de América Latina y el Caribe) y el Grupo de trabajo BCOP[4], en cooperación con M3 Miembros del AAWG, asesores técnicos superiores y la M3 Comité Técnico AAWG.

Tabla de contenido

1 El Grupo de Operadores de Red de América Latina y el Caribe (LACNOG), https://www.lacnog.net/

2 Grupo de trabajo de mensajería, malware y antiabuso móvil (M3AAWG), https://www.m3aawg.org/

3 Grupo de Trabajo contra el Abuso de América Latina y el Caribe (LAC-AAWG), https://www.lacnog.net/lac-aawg/

4 4 Grupo de trabajo LACNOG BCOP, https://www.lacnog.net/wg-bcops/

Resumen Ejecutivo

"Equipo de la premisa del cliente" (CPE) es el equipo utilizado para conectar a los suscriptores a la red de un proveedor de servicios de Internet (ISP). Ejemplos de CPE incluyen módems (cable, xDSL, fibra) y enrutadores WiFi, entre otros.

Debido a las vulnerabilidades en el software integrado y en las configuraciones predeterminadas, CPE ha sido objeto de una variedad de abusos, que van desde la explotación de servicios mal configurados y las credenciales de autenticación predeterminadas hasta el compromiso total por parte del malware. El propósito de muchos de estos ataques es realizar ataques de denegación de servicio (DoS), minería de criptomonedas no autorizada, propagación de malware, spam, phishing, robo de credenciales y otros abusos. En general, las vulnerabilidades comunes han incluido:

- Credenciales estándar para una gran cantidad de dispositivos.
- Credenciales que no se pueden cambiar (codificadas)
- Uso de protocolos y algoritmos obsoletos e inseguros.
- Accesos no documentados (puertas traseras)
- Falta de mecanismos de actualización automatizados y seguros para abordar problemas de seguridad
- Servicios innecesarios y / o inseguros habilitados por defecto
- Servicios que no pueden ser deshabilitados
- Gestión remota insegura

Este documento tiene como objetivo identificar un conjunto mínimo de requisitos de seguridad que deben especificarse cuando los ISP compran CPE para garantizar que dicho CPE tenga una configuración predeterminada segura y un mecanismo de actualización y administración remota segura. El objetivo es reducir el riesgo de comprometer la red del proveedor y de Internet en su conjunto, y minimizar los costos y el impacto resultante del abuso del equipo por parte de los atacantes, como la degradación o la falta de disponibilidad de servicios, soporte técnico y trabajos de reparación. .

Está fuera del alcance de este documento proporcionar un conjunto completo de características o las especificaciones de hardware y software que CPE debe admitir[5] A los fines de este documento, se supone que los protocolos IPv6 e IPv4 son compatibles, implementados y habilitados.

1. Terminología

Para los propósitos de este documento:

1. Equipo local del cliente (CPE): el equipo utilizado para conectar a los suscriptores a la red del proveedor de servicios de Internet (ISP). Otros pueden usar diferentes nombres para describir este tipo de dispositivos, como el enrutador Customer Edge (CE) y el gateway residencial (RG).

2. Firmware: el software que se ejecuta en el CPE, incluido el sistema operativo, y también puede incluir software de interfaz de red, paquetes y servicios de software y configuraciones.

3. Puerta trasera: cualquier mecanismo insertado en el sistema con el objetivo de permitir el acceso no documentado al sistema o sus datos. Los ejemplos de puertas traseras incluyen un nombre de usuario codificado sin documentar sin contraseña, una contraseña fija o una "contraseña del día" predecible, o servicios no documentados para

[5] [5] No incluir los requisitos relacionados con el soporte e implementación de IPv6 como parte de la especificación de compra de CPE puede resultar en un riesgo comercial para los ISP, ya que es posible que no puedan proporcionar conectividad IPv6 a sus clientes. Esto presenta un riesgo de crecimiento empresarial para el ISP debido al agotamiento de la dirección IPv4.

realizando funciones administrativas sin autenticación, entre otras. Se puede incluir una puerta trasera intencionalmente (diseñada para garantizar el acceso posterior) o accidentalmente (utilizada con fines de desarrollo y luego incluida inadvertidamente en el firmware de disponibilidad general). Las puertas traseras también pueden surgir como consecuencia de malas prácticas de programación.

4. Cifrado / criptografía apropiada: algoritmos / protocolos criptográficos estándar abiertos publicados por Internet Engineering Task Force (IETF) u otras organizaciones de estándares en sus versiones actuales. La implementación debe permitir la selección de conjuntos de cifrado y tamaños de clave actualizados.

5. Credenciales codificadas: credenciales con valores comunes fijados en el código fuente del producto (lo mismo para todas las instalaciones del producto) que no pueden cambiarse o deshabilitarse excepto parcheando el código fuente (y consecuentemente lanzando un nuevo binario / firmware).

6. Servicio (proceso de tipo servidor, o *demonio):* un proceso de servidor que está esperando activamente conexiones en un puerto particular, no el software del cliente que realiza consultas a un servicio, cuando es necesario.

7. PREDETERMINADO: una configuración establecida por el proveedor.

8. Las palabras clave "DEBE", "NO DEBE", "REQUERIDO", "DEBE", "NO DEBE", "DEBE", "NO DEBE", "SE RECOMIENDA", "NO SE RECOMIENDA", "PUEDE", y " OPCIONAL "en este documento debe interpretarse como se describe en BCP 14 RFC 2119 [2] y RFC 8174 [3] cuando, y solo cuando, aparecen en mayúsculas, como se muestra aquí.

2. Requisitos generales (GR)

GR-01: La descripción del dispositivo DEBE incluir la identificación completa de sus componentes principales, en particular:

a. Fabricante, modelo y versiones de chipset

si. Nombre, versión y fecha de lanzamiento del firmware y del sistema operativo base.

GR-02: El proveedor DEBE proporcionar documentación que describa como mínimo:

a. Nombre, versión, fecha de lanzamiento y funcionalidad del firmware o sistema operativo.

si. Nombre, versión, fecha de lanzamiento y estado de arranque de fábrica (por ejemplo, encendido o apagado por defecto) de todas las aplicaciones y servicios instalados en el dispositivo

GR-03: El proveedor DEBE proporcionar la siguiente información para cualquier software de código abierto utilizado:

a. Lista de todas las licencias relevantes para cada software de código abierto utilizado

si. Nombre completo y versión de cada software de código abierto incorporado al sistema CPE

GR-04: Información de contacto para divulgación de vulnerabilidad (VR-03) DEBE incluirse en algún momento (p. Ej., Página, pestaña, etc.) en la interfaz gráfica de usuario (GUI) de CPE.

GR-05: El proveedor DEBE proporcionar información al usuario si el CPE está fuera del período de soporte (ver VR-01 y VR-02) y ya no recibe actualizaciones de firmware (por ejemplo, a través de la interfaz gráfica de usuario).

3. Requisitos de seguridad del software (SSR)

SSR-01: Las credenciales NO DEBEN estar codificadas. Ver también FR-04 y FR-05 .

SSR-02: los datos de credenciales confidenciales (por ejemplo, contraseñas, claves y tokens de seguridad) almacenados en el dispositivo DEBEN ser protegido por algoritmos hash / criptográficos apropiados. Las claves criptográficas DEBEN almacenarse en hardware seguro, si está disponible.

SSR-03: los datos generales que se almacenan en el dispositivo DEBEN estar protegidos mediante un cifrado adecuado. SSR-04: todas las herramientas de software o puertas traseras utilizadas para el desarrollo de firmware o sistema DEBEN eliminarse en La versión de producción en masa.

4. Actualización y requisitos de gestión (MR)

MR-01: El CPE DEBE implementar un mecanismo de gestión remota con, como mínimo, control remoto administración utilizando un protocolo de cifrado apropiado. Mira la tabla en Anexo I para la lista de los protocolos requeridos.

MR-02: El CPE DEBE implementar un mecanismo para la actualización remota segura. Mira la tabla en Anexo I para la lista de los protocolos requeridos.

MR-03: La gestión y administración remotas, y los mecanismos de actualización remota DEBEN soportar:

a. Autenticación segura y

si. Conexiones encriptadas, y

C. Restricciones de acceso para limitar las conexiones a fuentes específicas (por ejemplo, segmentos de red seleccionados, un URL específica, etc.), y

re. La capacidad de elegir el puerto de conexión (es decir, admite cambiar el número de puerto del POR DEFECTO / puerto asignado para el servicio [17])

MR-04: En el caso de actualizaciones automatizadas y seguras, DEBE implementarse un mecanismo para autenticar y validar el repositorio de origen.

MR-05: El CPE DEBE implementar un mecanismo para verificar, antes de continuar con la actualización real (normalmente en la memoria flash): la integridad y la autoridad del archivo descargado y si está destinado a ese dispositivo (por ejemplo, está destinado a la arquitectura, modelo, versión, etc. del dispositivo). MR-06: El proceso de actualización DEBE preservar la configuración existente. Un vendedor PUEDE cambiar un existente establecer si dicho cambio mejora la seguridad del dispositivo. Tal cambio DEBE estar claramente documentado.

MR-07: Con respecto a la búsqueda de actualizaciones, CPE:

a. DEBE tener la capacidad de ejecutar comprobaciones periódicas para obtener actualizaciones de forma automática y programada base;

si. DEBE permitir que el usuario inicie la búsqueda de actualizaciones.

C. DEBE admitir las actualizaciones automáticas solicitadas por el ISP a pedido. MR-08: CPE DEBE implementar mecanismos para evitar que se vuelvan inútiles como resultado del firmware error de actualización (ladrillo). Los procedimientos de recuperación DEBEN estar claramente documentados y NO DEBEN requerir el acceso a partes internas del hardware.

5. Requisitos funcionales (FR)

Este documento asume que el soporte de IPv6 de acuerdo con RFC 7084 [8] forma parte del documento de requisitos generales de compra.

Estas características deben ser compatibles o eliminadas del CPE:

FR-01: CPE NO DEBE habilitarse en los servicios WAN BY DEFAULT que permiten la divulgación de información confidencial o se puede abusar para realizar ataques de amplificación (por ejemplo, Telnet, FTP, SOCKS, CHARGEN, SNMP, etc.)

FR-02: CPE DEBE implementar actualizaciones remotas y funcionalidades de administración remota como se describe en el Actualización y requisitos de gestión (MR) sesión de este documento. FR-03: Cualquier comunicación de gestión del usuario final desde la LAN / WLAN al CPE DEBE ser autenticado[66] y DEBE estar encriptado.

FR-04: Cualquier información de autenticación (por ejemplo, contraseñas) DEBE ser modificable, incluido el maestro contraseña de administración (raíz) Los identificadores de usuario (por ejemplo, nombres de usuario) DEBEN ser modificables.

FR-05: Con respecto a la contraseña para acceder a las interfaces administrativas:

a. La contraseña inicial DEBE ser única para cada dispositivo y NO DEBE derivarse de la información que se puede obtener a través de la captura de paquetes o métodos similares de observación (por ejemplo, dirección MAC);

si. En cualquier momento cuando se cambia o restablece una contraseña, la contraseña NO DEBE ser nula (es decir, vacía, en blanco) ni la misma que el nombre de usuario, y DEBEN seguirse las mejores prácticas relevantes para la complejidad de la contraseña.

FR-06: El firmware de producción NO DEBE tener ningún mecanismo no documentado para acceder al sistema o sus datos.

FR-07: El dispositivo NO DEBE tener mecanismos de comunicación no documentados para enviar datos al vendedor o terceros. Cualquier comunicación y datos enviados al vendedor o terceros DEBEN ser documentados explícitamente[77]

FR-08: Un usuario final autenticado DEBE poder, a través de la interfaz gráfica de usuario:

a. Para cambiar la configuración específica del usuario según corresponda (por ejemplo, nombre de red WiFi, firewall / reglas de reenvío, etc.), y

si. Para deshabilitar cualquier servicio que no sea esencial para la operación o administración del dispositivo.

FR-09: Al habilitar la operación de servicios para usuarios en las interfaces LAN / WLAN del CPE, tales Los servicios NO DEBEN ser accesibles desde la WAN / Internet, en particular servicios como DNS, NTP, SSDP, UPnP o cualquier otro protocolo que pueda usarse en ataques de amplificación.

[66] CPE puede admitir mecanismos de autenticación alternativos para ofrecer un mayor nivel de seguridad que simplemente el nombre de usuario / contraseña.

[77] Las legislaciones de protección de datos en muchos países / regiones pueden imponer requisitos especiales en el procesamiento de datos personales, requiriendo que sean detallados y documentados explícitamente.

FR-10: para utilizar un servicio / agente de supervisión y / o gestión:

a. La configuración de un mecanismo de autenticación apropiado para establecer valores y / o para DEBE requerirse la recuperación de información / datos confidenciales;

si. El acceso desde las interfaces WAN DEBE usar autenticación y DEBE estar restringido a fuente (s) específica (p. ej. a un segmento de red o dirección seleccionados).

FR-11: El dispositivo DEBE implementar métodos criptográficos basados en estándares abiertos en su actual versiones que permiten la selección de parámetros seguros con respecto al conjunto de cifrado y los tamaños de clave. FR-12: Servicios o aplicaciones criptográficas que implican la generación de claves y / o certificados digitales. para la autenticación del dispositivo DEBE generar las claves para cada dispositivo; es decir, una clave privada NO DEBE ser compartida entre diferentes dispositivos.

FR-13: El CPE DEBE soportar la sincronización horaria a través de un protocolo de tiempo centralizado, como el Protocolo de tiempo de red (NTP). Solo se requiere el software de cliente NTP. El CPE NO DEBE tener una configuración codificada para servidores NTP y NO DEBE usar servidores POR DEFECTO que el proveedor no tenga permiso para usar.

FR-14: El CPE DEBE soportar RFC 6092 "Capacidades de seguridad simples recomendadas en Equipo de instalaciones del cliente (CPE) para proporcionar servicio residencial de Internet IPv6 "[6 6] En caso de conflicto entre RFC 6092 y este documento, prevalecerá el requisito de este documento.

FR-15: El CPE DEBE soportar el filtrado anti-spoofing de acuerdo con BCP 38 RFC 2827 [12] para tanto IPv4 como IPv6. DEBE ser una opción seleccionable habilitada POR DEFECTO. Está fuera del alcance de este documento determinar la técnica que se utilizará para la validación de la dirección IP de origen. FR-16: El CPE DEBE admitir el filtrado de paquetes para direcciones IP de propósito especial. Direcciones considerado FALSO "FALSO" y "Reenviable" FALSO "Globalmente Alcanzable", de acuerdo con RFC 6890 [13] y RFC 8190 [14], DEBE ser ~~filtr~~ado. En este caso, el C~~PE~~ DEBE ser capaz de configurarse para incluir direcciones IPv4 e IPv6 de acuerdo con los registros mantenidos por IANA (Autoridad de Números Asignados de Internet) como se describe en el "Registro de Direcciones de Propósito Especial IvA IPv4" [15] y "Registro de direcciones de propósito especial IANA IPv6" [dieciséis] FR-17: CPE NO DEBE actuar como un solucionador abierto. En cuanto a los servicios de DNS:

a. Las consultas DNS recibidas en el puerto WAN y destinadas al CPE en sí NO DEBEN permitirse ni responderse de ninguna manera.

si. PUEDEN permitirse las consultas DNS recibidas en el puerto WAN y destinadas a reenviarse al puerto LAN siempre que exista una regla explícita para esto en la configuración de CPE (por ejemplo, regla de reenvío, regla de firewall, etc.) [8]

C. Si el CPE ejecuta un servidor DNS local, DEBE establecer consultas DNS salientes para realizar la validación DNSSEC.

re. Si el CPE no ejecuta un servidor DNS local y reenvía consultas DNS a otro servidor, NO DEBE eliminar las marcas de validación DNSSEC de las consultas DNS si existen.

[8] El CPE no debe evitar que el usuario aloje un servidor DNS en la LAN. Vale la pena mencionar que una regla de reenvío / firewall en este caso solo tiene sentido si se ejecuta un servidor DNS autorizado en la LAN.

FR-18: cuando se proporciona WiFi, CPE:

a. DEBE implementar mecanismos de seguridad con la criptografía adecuada.

si. DEBE admitir la última versión de la especificación de características de seguridad de Acceso protegido a Wi-Fi (WPA) ®.

FR-19: Las contraseñas NO DEBEN ser visibles en texto claro POR DEFECTO en ninguna interfaz de administración.
Las contraseñas PUEDEN hacerse visibles cuando lo solicite el usuario.

FR-20: DEBE haber un método para descargar la configuración del dispositivo en un formato de texto claro (ASCII
o UTF-8), siempre que cualquier información confidencial (por ejemplo, contraseñas, cadenas de comunidad, etc.) se elimine de la salida.

6. Requisitos de configuración inicial (IR)

Los dispositivos DEBEN tener la siguiente configuración predeterminada de fábrica:

IR-01: CPE DEBE configurarse de forma restrictiva en lugar de configurarse permisivamente. Todos los servicios
(es decir, procesos de tipo servidor) que no son estrictamente necesarios para el proceso de configuración inicial (bootstrapping) DEBEN deshabilitarse, especialmente (si está implementado) SSDP, SNMP, UPnP, SOCKS, SMB, Prueba de ancho de banda (ergo iperf incrustado y otros). Además, los servicios que están habilitados o se pueden activar DEBEN operar en un modo predeterminado restrictivo y / o seguro. IR-02: los parámetros relacionados con las direcciones del servidor DNS (direcciones de resolución) DEBEN estar sin configurar y el

La opción de retransmisión de DNS (si está implementada) DEBE estar deshabilitada.

IR-03: el reenvío de puertos o la opción de host DMZ, si está disponible, DEBEN deshabilitarse POR DEFECTO. IR-04: la contraseña inicial para

acceder a las interfaces administrativas, tanto gráficas como de línea de comandos,
DEBE ser único para cada dispositivo y DEBE ser posible identificarlo visualmente en la etiqueta del dispositivo. IR-05: cuando se

proporciona WiFi, las redes WiFi DEBEN tener una contraseña inicial única, NO igual
al SSID de WiFi, y DEBE ser posible identificar visualmente las contraseñas iniciales en la etiqueta del dispositivo. La (s) contraseña (s) DEBERÍA ser diferente de la contraseña predeterminada del administrador. IR-06: cuando se proporciona WiFi, los valores predeterminados de los identificadores (SSID) del conjunto de servicios WiFi DEBEN
NO debe estar relacionado con el nombre del proveedor ni el modelo del producto y DEBE ser personalizable. Mira la tabla en Anexo I para valores predeterminados personalizados de ISP[9]

IR-07: En el caso del servicio SSH, el par de claves del servidor NO DEBE generarse previamente en la fábrica. La clave DEBE generarse después de la primera inicialización / arranque del servicio y cualquier restablecimiento de fábrica del dispositivo hará que se genere una nueva clave. El par de claves generado proporcionará suficientes bits de seguridad para considerarse seguro en el momento del despliegue. IR-08: Filtrado antifalsificación [FR-15] DEBE estar habilitado POR DEFECTO. IR-09:

Los mecanismos de transición IPv6, túneles, VPN y servicios similares DEBEN estar deshabilitados POR DEFECTO.

[9] En caso de que el ISP quiera elegir cómo se nombrarán los SSID POR DEFECTO (por ejemplo, un solo nombre para todos los dispositivos o nombres únicos por dispositivo), el ISP deberá describir cómo se DEBEN nombrar los SSID. De lo contrario, el proveedor puede elegir el PREDETERMINADO.

7. Requisitos del vendedor (VR)

El vendedor:

VR-01: DEBE tener una política clara de soporte del producto, especialmente con respecto a la disponibilidad de soluciones para vulnerabilidades de seguridad, incluido el período posterior a la fecha de finalización de la venta.

VR-02: DEBE proporcionar soluciones para las vulnerabilidades de seguridad como mínimo mientras el dispositivo esté a la venta. los El proveedor DEBE continuar proporcionando soluciones de seguridad durante 3 (tres) años a partir de la fecha de finalización de la venta.

VR-03: DEBE tener una capacidad coordinada de divulgación de vulnerabilidades, incluida una comunicación canal / punto de contacto que permite a los clientes de ISP, usuarios finales y terceros (como investigadores) informar vulnerabilidades de seguridad descubiertas en los productos. Idealmente, DEBERÍA tener un Equipo de Respuesta a Incidentes de Seguridad del Producto (PSIRT).

VR-04: DEBE tener un canal de soporte público disponible que no requiera preinscripción o un cuenta, como mínimo, a través de un sitio web en inglés para:

a. Informar sobre vulnerabilidades existentes, medidas de mitigación y arreglos de seguridad asociados con sus productos;

si. Proporcionar correcciones de seguridad y / o nuevas versiones de firmware o software para sus productos;

C. Proporcionar manuales y otros materiales relacionados con la configuración, actualización y seguridad del dispositivo.

8. Lista de acrónimos

BCOP: Mejores prácticas operativas actuales BBF:

Foro de banda ancha CE:

Cliente Edge Router CPE:

Equipo de instalaciones del cliente

CWMP: CPE WAN (Wide Area Network) Protocolo de gestión IANA:

ISP de la Autoridad de Números Asignados de Internet:

Proveedor de servicios de Internet

PSIRT: Equipo de respuesta a incidentes de seguridad del producto RG:

SSID de puerta de enlace

residencial: Identificador de conjunto de servicios

WLAN: LAN inalámbrica (red de área local)

9. Agradecimientos

Muchas personas contribuyeron al desarrollo de este documento, desde su iniciación en el Grupo de Trabajo contra el Abuso de América Latina y el Caribe (LAC-AAWG) hasta su publicación.

Los autores agradecen a todos los contribuyentes por sus muchas sugerencias útiles, en algunos casos proporcionando una revisión detallada. Los contribuyentes (en orden alfabético) incluyen: Nicolas Antoniello, John Brown, Dennis Dayman, Carmen Denis, Yuri Ferreira, Alexandre Giovaneli, Steve Goeringer, Cristine Hoepers, Markus Lintula, Jason Livingood, Art Manion, Jordi Palet Martínez, Roney Medeiros, Luciano Minuchin , Eduardo Barasal Morales, Massimiliano Pala, Ricardo Patara, Nathalia Sautchuk Patrício, Fernando Quintero, Marcelo Batista Sarmento, Joe St Sauver, Klaus Steding-Jessen, Italo Valcy, Severin Walker, Ariel Weher, Gilberto Zorello y Jan Žorž.

Un agradecimiento especial a:

- Lucimara Desiderá, co-presidente fundador de LAC-AAWG, autor / editor
- Christian O'Flaherty, copresidente fundador de LAC-AAWG
- La comunidad del Grupo de Trabajo LACNOG BCOP y el Presidente por apoyar el proceso de desarrollo y revisión de documentos
- El WARP LACNIC (Aviso de advertencia y punto de notificación) del Registro de direcciones de Internet de América Latina y el Caribe (LACNIC) para proporcionar infraestructura para las reuniones cara a cara
- El grupo de trabajo de mensajería, malware y móvil contra el abuso (M$_3$ AAWG) por apoyar la iniciativa LAC-AAWG y aceptar este documento para revisión técnica

10. Referencias informativas

[1] Abuso del equipo de las instalaciones del cliente y acciones recomendadas
https://resources.sei.cmu.edu/asset_files/WhitePaper/2014_019_001_312679.pdf

[2] Palabras clave para usar en RFC para indicar niveles de requisitos, BCP 14, RFC 2119
http://www.rfc-editor.org/info/rfc2119

[3] Ambigüedad de mayúsculas vs minúsculas en RFC 2119 palabras clave, RFC 8174
https://tools.ietf.org/html/rfc8174

[4] Glosario de seguridad de Internet, versión 2, RFC 4949
https://tools.ietf.org/html/rfc4949

[5] Requisitos de seguridad comunes para CPE proporcionado por MSO basado en IP - Versión I01
https://apps.cablelabs.com/specification/common-security-requirements-for-ip-based-mso- proporcionado-cpe

[6] Capacidades de seguridad simples recomendadas en equipos locales del cliente (CPE) para proporcionar servicio residencial de Internet IPv6, RFC 6092
https://tools.ietf.org/html/rfc6092

[7] Especificaciones de interfaz de servicio de datos por cable DOCSIS® 3.1, Especificación de seguridad, CM-SP-SECv3.1-I07-170111
https://apps.cablelabs.com/specification/CM-SP-SECv3.1

[8] Requisitos básicos para enrutadores periféricos de cliente IPv6, RFC 7084
https://tools.ietf.org/html/rfc7084

[9] Requisitos funcionales para dispositivos de puerta de enlace residencial de banda ancha, TR-124, edición 5
https://www.broadband-forum.org/technical/download/TR-124_Issue-5.pdf

[10] Protocolo de gestión CPE WAN, TR-069, edición 1, enmienda 6
https://www.broadband-forum.org/technical/download/TR-069.pdf

[11] Especificación de eRouter IPv4 e IPv6 CM-SP-eRouter-I19-160923
https://apps.cablelabs.com/specification/ipv4-and-ipv6-erouter-specification/

[12] Filtrado de entrada de red: Derrota de ataques de denegación de servicio que emplean dirección de origen IP Suplantación de identidad, BCP 38, RFC 2827
https://tools.ietf.org/html/rfc2827

[13] Registros de direcciones IP para fines especiales, BCP 153, RFC 6890
https://tools.ietf.org/html/rfc6890

[14] Actualizaciones a los registros de direcciones IP para fines especiales, BCP 153, RFC 8190
https://tools.ietf.org/html/rfc8190

[15] Registro de direcciones de propósito especial IANA IPv4
https://www.iana.org/assignments/iana-ipv4-special-registry

[dieciséis]Registro de direcciones de propósito especial IANA IPv6
https://www.iana.org/assignments/iana-ipv6-special-registry

[17] Nombre del servicio y protocolo de transporte Número de puerto Registro
https://www.iana.org/assignments/service-names-port-numbers/service-names-port- numbers.xhtml

[18] Abordar el desafío de la suplantación de propiedad intelectual
https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-AntiSpoofing-20150909-en-2.pdf

[19] ISO / IEC 29147: 2014 Tecnología de la información - Técnicas de seguridad - Divulgación de vulnerabilidad
https://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip

[20] BSI TR-03148:Enrutador de banda ancha seguro
Requisitos para una versión segura de enrutador de banda ancha: 1.0
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03148/TR03148.pdf?__blob=publicationFile&v=2

Anexo 1 - Tabla de requisitos

La siguiente tabla resume el conjunto de requisitos presentados en este documento y está destinado a ayudar a las organizaciones (por ejemplo, ISP) a preparar RFP o especificar los requisitos que desean de los proveedores. Algunos campos ya están rellenados con la selección recomendada, especialmente cuando el requisito es obligatorio, pero una buena parte de los requisitos requieren que la organización decida si quiere una configuración determinada o no y que defina su configuración POR DEFECTO.

Vale la pena señalar que los elementos enumerados en este documento son un conjunto mínimo de requisitos de seguridad y se recomienda encarecidamente que las opciones no se reduzcan a un nivel inferior (por ejemplo, de implementación obligatoria a recomendada u opcional). Siempre que sea posible, se deben mover a la opción más estricta.

Requisitos generales (GR)		
Requisito M obligatorio	**R Recomendado O Opcional**	**Configuración por defecto**
GR-01	METRO	
GR-02	METRO	
GR-03	METRO	
GR-04	R	Información de contacto para divulgación de vulnerabilidad disponible en la interfaz gráfica de usuario
GR-05	R	Estado actual de actualizaciones
Requisito de requisitos de seguridad de software		
(SR) M obligatorio	**R Recomendado O Opcional**	**Configuración por defecto**
SSR-01	METRO	
SSR-02	METRO	Datos sensibles protegidos
SSR-03	R	
SSR-04	METRO	Herramientas de desarrollo de software y / o puertas traseras eliminadas

Requisito de actualización y requisitos de gestión (MR) M		
obligatorio	**R Recomendado O Opcional**	**Configuración por defecto**
MR-01	**M (una)**	**(una)**
MR-02	**M (si)**	**(si)**
MR-03	a. METRO si. METRO C. METRO re. METRO	**(C)**
MR-04	METRO	
MR-05	METRO	
MR-06	METRO	
MR-07	a. METRO si. METRO C. R	
MR-08	METRO	
Requisito de requisitos funcionales		
(FR) M obligatorio	**R Recomendado O Opcional**	**Configuración por defecto**
FR-01	METRO	Telnet, FTP, SOCKS, CHARGEN, SNMP deshabilitado
FR-02	METRO	**(C)**
FR-03	DEBE autenticarse y se RECOMIENDA cifrar.	
FR-04	METRO	
FR-05	a. METRO si. METRO	Contraseña inicial única por dispositivo
FR-06	METRO	
FR-07	METRO	
FR-08	a. METRO si. METRO	

FR-09	METRO	DNS, NTP, SSDP, UPnP no accesibles desde la WAN
FR-10	a. METRO si. METRO	(re)
FR-11	METRO	
FR-12	METRO	
FR-13	METRO	Cliente NTP solamente. Sin configuración codificada.
FR-14	R	
FR-15	METRO	Filtrado antifalsificación habilitado
FR-16	R	Sin configurar (mi) _
FR-17	a. METRO si. R C. R re. METRO	si. Ninguna regla de reenvío habilitada
FR-18	a. METRO si. R	Cifrado apropiado habilitado
FR-19	METRO	
FR-20	R	

Requisitos de configuración inicial (IR) Requisito

M obligatorio	**R Recomendado O Opcional**	**Configuración por defecto**
IR-01	METRO	SSDP, SNMP, UPnP, SOCKS, SMB, Prueba de ancho de banda deshabilitada
IR-02	METRO	No hay direcciones DNS predefinidas y el relé DNS deshabilitado
IR-03	METRO	Discapacitado
IR-04	METRO	(F)
IR-05	METRO	(F)
IR-06	METRO	(gramo)
IR-07	METRO	Sin clave SSH pregenerada
IR-08	METRO	Habilitado
IR-09	METRO	Mecanismos de transición, túneles, VPN deshabilitada

Requisitos del proveedor (VR)		
Requisito	**M obligatorio R Recomendado O Opcional**	**Configuración por defecto**
VR-01	METRO	
VR-02	METRO	
VR-03	METRO	
VR-04	METRO	

(a) El ISP debe tener la capacidad de administrar los dispositivos de forma remota (por ejemplo, para la configuración). Dependiendo de
La tecnología utilizada por el proveedor (cable, fibra, xDSL), la industria correspondiente puede haber especificado protocolos. En este elemento, el ISP debe elegir los protocolos que el dispositivo debe admitir de acuerdo con su tecnología (por ejemplo, BBF TR-069 CWMP para banda ancha), si debe habilitarse POR DEFECTO y la configuración predeterminada requerida. Si se debe admitir más de un protocolo, la organización debe incluirlos a todos.

(b) El ISP debe tener la capacidad de actualizar el dispositivo de forma remota (principalmente el firmware). Dependiendo de
tecnología utilizada por el proveedor (cable, fibra, xDSL), la industria correspondiente puede tener protocolos ya especificados. En este elemento, la organización necesita elegir los protocolos que el dispositivo debe admitir de acuerdo con su tecnología (por ejemplo, BBF TR-069 CWMP para banda ancha), si debe habilitarse POR DEFECTO y la configuración predeterminada requerida. Si se debe admitir más de un protocolo, la organización debe incluirlos a todos.

(c) No utilizar mecanismos mínimos para el control de acceso, la confidencialidad y la verificación de integridad en el
Las transacciones entre los CPE y los servidores de administración / actualización a menudo pueden comprometer la infraestructura del proveedor. Se recomienda encarecidamente utilizar una conexión encriptada (por ejemplo, TLS / HTTPS) para todos los accesos; usar la autenticación no basada en un único nombre de usuario / contraseña predefinido para todos los dispositivos; y restringir el acceso a fuentes específicas (por ejemplo, a un segmento de red seleccionado, URL específica, etc.).

(d) Si el ISP quiere un servicio / agente de monitoreo y / o administración habilitado POR DEFECTO, tiene que
Proporcionar los parámetros apropiados para la autenticación y la restricción de acceso a la red. (e) Si el ISP desea implementar el filtrado

para direcciones IP de propósito especial directamente en el CPE, puede
proporcione la lista de prefijos que pueden filtrarse POR DEFECTO. De lo contrario, la configuración PREDETERMINADA es "no configurada" y el CPE no aplica ningún filtro para dichos prefijos. (f) Si el ISP desea personalizar cómo se configurará la contraseña inicial, el ISP debe informar al
proveedor en el proceso de selección de contraseña. De lo contrario, el proveedor puede establecer valores únicos aleatorios como DEFAULT.

(g) Si el ISP desea personalizar los nombres de la red WiFi, debe informar cómo los identificadores WiFi
(SSID) debe configurarse. De lo contrario, el proveedor puede elegir los valores predeterminados.
