Guía de Seguridad de las TIC
CCN-STIC 1431

Procedimiento de Empleo Seguro
ArubaOS 8.10. Controladoras y Puntos de Acceso



Mayo 2025

MINISTERIO DE DEFENSA

cpage.mpr.gob.es

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2025

NIPO: 083-25-191-6
Fecha de Edición: Mayo de 2025

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2026.01.16 07:34:47 +01'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1 INTRODUCCIÓN 4
2 OBJETO Y ALCANCE 5
3 ORGANIZACIÓN DEL DOCUMENTO 6
4 FASE DE DESPLIEGUE E INSTALACIÓN 7
4.1 ENTREGA SEGURA DEL PRODUCTO 7
4.2 ENTORNO DE INSTALACIÓN SEGURO 7
4.3 REGISTRO Y LICENCIAS 8
4.4 INSTALACIÓN 8
4.4.1 DESPLIEGUE DE LOS DISPOSITIVOS DE TIPO MAQUINA VIRTUAL 8
4.4.2 INSTALACION FISICA DE LOS DISPOSITIVOS FISICOS 9
4.4.3 PRIMER ACCESO 9
5 FASE DE CONFIGURACION 11
5.1 MODO DE OPERACIÓN SEGURO 11
5.2 AUTENTICACIÓN 12
5.3 SERVIDORES DE AUTENTICACIÓN 13
5.3.1 PARÁMETROS DE LOS SERVIDORES EXTERNOS 14
5.3.2 BASE DE DATOS INTERNA 14
5.4 ADMINISTRACIÓN DEL PRODUCTO 16
5.4.1 ADMINISTRACIÓN LOCAL Y REMOTA 16
5.4.2 CONFIGURACIÓN DE ADMINISTRADORES 17
5.4.3 DEFINICIÓN DE ADMINISTRADORES LOCALES 17
5.4.4 POLITICA DE CONTRASEÑAS 18
5.4.5 CONFIGURACION DE MENSAJE DE BIENVENIDA (BANNER) 20
5.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 20
5.5.1 INTERFAZ DE GESTIÓN FUERA DE BANDA 21
5.5.2 PROTECCIÓN DEL PUERTO DE CONSOLA DE LOS AP 21
5.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS 21
5.6.1 SNMP 21
5.6.2 TELNET 22
5.6.3 WIFI 22
5.6.4 HTTPS 22
5.6.5 SSH 23
5.6.6 IPSEC 23
5.7 GESTIÓN DE CERTIFICADOS 24
5.8 SINCRONIZACIÓN HORARIA 25
5.9 ACTUALIZACIONES 26
5.10 AUTO-CHEQUEOS 26
5.11 ALTA DISPONIBILIDAD 26
5.12 AUDITORÍA 27
5.13 COPIAS DE SEGURIDAD 27
5.14 SERVICIOS DE SEGURIDAD 28
5.14.1 SEGURIDAD EN EL PLANO DE CONTROL - CPSEC 28
5.14.2 CONFIGURACIÓN DE DEFENSA DEL PLANO DE CONTROL 28
5.14.3 WIRELESS IPS 29
5.14.4 CONTROL DE CONTENIDOS - WEBCC 29
5.14.5 REMOTE ACCESS POINTS 29
5.14.6 MULTIZONA 30

5.14.7 BLOQUEAR TRAFICO DE SYSLOG 30
5.15 VIRTUAL INTRANET ACCESS 31
5.16 CORTAFUEGOS 31
6 FASE DE OPERACIÓN 32
7 CHECKLIST 33
8 REFERENCIAS 35
9 ABREVIATURAS 37

1 INTRODUCCIÓN

1. *ArubaOS* es el sistema operativo de los equipos Aruba de soluciones de comunicaciones inalámbricas, basadas en controladoras y sin controladoras para satisfacer las demandas de las empresas en todo tipo de industrias y es compatible con los estándares actuales y la interoperabilidad de los estándares Wi-Fi.
2. Los equipos que implementan los interfaces inalámbricos son los Puntos de Acceso (APs). Estos pueden trabajar de forma autónoma, o bien mediante unos equipos que centralizan las tareas de operación, configuración y explotación. Estos dispositivos se denominan controladoras de movilidad o simplemente controladoras.
3. En las últimas versiones se ha incorporado una capa adicional de control, donde un elemento denominado *Mobility Conductor* (MCr) centraliza a su vez las tareas de explotación y operación de todas las controladoras de movilidad.
4. *ArubaOS* puede desplegarse como solución inalámbrica para un gran campus, una sucursal de tamaño medio o apoyando a los trabajadores remotos.

2 OBJETO Y ALCANCE

5. El presente documento tiene como objetivo facilitar la instalación y configuración segura de la familia de controladoras y puntos de acceso (APs) de Aruba, con sistema operativo *ArubaOS* 8.10. Esto incluye: Aruba Mobility Controller, Aruba Virtual Mobility Controllers y Puntos de Acceso.
6. Los dispositivos anteriores, con ArubaOS 8.10, han sido cualificados e incluidos en el Catálogo de Productos y Servicios STIC (CPSTIC) para categoría ENS ALTA en la familia "Redes privadas virtuales: IPSec, Cortafuegos, Dispositivos de Red Inalámbricos".
7. Esta guía, por tanto, no reemplaza ni puede compararse con:
   a) La documentación oficial del producto.
   b) Los documentos *Release Notes*.
   c) Formación.
   d) Pruebas de maqueta y preproducción.
8. Se asume que el lector tiene conocimientos de configuración y operación de estos equipos y, por tanto, se apoya en este documento para realizar una configuración segura de los mismos.

3 ORGANIZACIÓN DEL DOCUMENTO

9. El documento se organiza en los siguientes apartados:
   a) Apartado **4**. Fase de despliegue e instalación.
   b) Apartado **5**. Recomendaciones en la fase de configuración y administración.
   c) Apartado **6**. Recomendaciones en la fase de operación.
   d) Apartado **7**. Checklist de las tareas a realizar y el estado de cada una de ellas.
   e) Apartado **8**. Referencias (links de consulta) usadas en este documento.
   f) Apartado **9**. Abreviaturas usadas en este documento.

4 FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

10. Los dispositivos físicos se entregan en cajas, perfectamente identificadas de *Aruba Networks, Hewlett-Packard Enterprise*. Estas cajas se entregan cerradas con un precinto con diversos logos o identificadores. También portan en el lateral una etiqueta identificadora con datos únicos del equipo incluido. En algunos casos hay embalajes multidispositivo, en cuyo caso la etiqueta describe a cada uno de los equipos.
11. **Esos datos deben coincidir con los proporcionados en la orden de compra y/o albarán de entrega**, por lo que debe verificarse que efectivamente los equipos corresponden con los adquiridos. Los datos que se muestran en la etiqueta son, como mínimo, los siguientes:
    a) Identificador de modelo: Texto identificativo.
    b) *HPE Part Number*: Identificador único del modelo. Palabra formada por números y letras.
    c) Número de serie de fabricación (*Serial Number*): Palabra formada por números y letras
    d) Dirección MAC Base (*MAC Address*).
12. Una vez arrancado el producto, se pueden **verificar los datos anteriores mediante comandos en la consola**:
    a) *show inventory*. Proporciona información del equipo grabada de forma permanente en el mismo, para ser consultado vía electrónica.
    b) *show tpm cert-info*. Los equipos físicos también disponen de chip TPM para almacén seguro de certificados. Este trae precargado un certificado de fábrica el cual lleva incluye su *Serial Number* y su dirección MAC base.
13. Los servidores virtuales se ofrecen como una máquina virtual empaquetada que se descarga de forma segura desde la página de soporte de Aruba ([REF1] - https://asp.arubanetworks.com/). Se soporta actualmente versiones para *ESXi VMware, Microsoft Hyper-V* y *Linux KVM*.
14. Para el acceso a la descarga son necesarias credenciales del portal de *Aruba Networks*. En la página de descarga se puede consultar el valor hash del fichero en formato SHA256. **Se debe realizar el hash SHA256 del fichero descargado y verificar que coincide con el mostrado en la página.**

4.2 ENTORNO DE INSTALACIÓN SEGURO

15. **Se debe realizar la instalación física del producto en un local de acceso restringido**, como el Centro de Procesado de Datos (CPD) o *Datacenter*, junto al cortafuegos o elemento de red superior.
16. De esta forma las conexiones de los dispositivos inalámbricos conectados a los SSIDs publicados por los Puntos de Acceso y que terminan en los *Mobility Controllers*, se entregarán de forma centralizada o segura al siguiente nivel de enrutado o al cortafuegos dependiendo de cada caso.

17. Los *Mobility Controllers* por defecto ofrecen que los SSIDs publicados trabajen en modo túnel. En este modo, las conexiones *WPA2/WPA3* no terminan en el punto de acceso, sino que se extienden hasta el *Mobility Controller*. Esto el punto de acceso lo realiza encapsulando el tráfico en un túnel de transporte cuyo fin es el llevar esos tráficos al *Mobility Controller* dado que las tramas 802.11 no llevan en su cabecera información IP para su enrutado (el tráfico que llevan en su interior si lo hace). Como consecuencia de todo ello, la conexión es transportada de forma segura, y confidencial entre el dispositivo y el *Mobility Controller*. Ni el Punto de Acceso ni los *switches/routers* intermedios tienen dato alguno de las comunicaciones.
18. Es importante tener en cuenta que el producto tiene que poder conectarse a los puntos de acceso desplegados. Por lo tanto, se debe dotar de una ubicación física y lógica que pueda establecer dichas conexiones.

4.3 REGISTRO Y LICENCIAS

19. El producto requiere la instalación de licencias para su correcto funcionamiento. Además de la licencia de uso del dispositivo, se deberá adquirir e instalar la licencia *Advanced Cryptography License*, para poder hacer uso de todos los algoritmos criptográficos seguros.
20. El detalle de las distintas licencias disponibles, así como la forma de instalarlas en los dispositivos, se puede consultar en el siguiente enlace – [REF5].

4.4 INSTALACIÓN

21. Los equipos físicos se entregan con una versión precargada de *software*, en cada una de las dos (2) particiones. Los equipos virtuales llevan intrínsecamente asociados una versión de sistema operativo, en cada una de las dos particiones.
22. Existen tres (3) tipos distintos de versiones *software*:
    a) Versión con asistencia larga (LSR, Long Supported Release). Se trata de versiones de larga duración en las que Aruba introduce nuevas características y hardware además de disponer de mantenimiento y servicio técnico durante 5 años. **Se recomienda el uso de la última versión conservadora de ArubaOS 8.10**.
    b) Versión con asistencia breve (SSR, Short Supported Release). Se trata de versiones de corta duración en las que Aruba introduce nuevas características y hardware centrándose en los requisitos de mercado en evolución, permitiendo atender a demandas específicas.
    c) Versión Personalizada (C-build). Versiones poco comunes, creadas para atender de forma rápida una necesidad específica de un cliente.

4.4.1 DESPLIEGUE DE LOS DISPOSITIVOS DE TIPO MAQUINA VIRTUAL

23. El detalle sobre cómo realizar el despliegue e instalación de los dispositivos virtuales se puede consultar en la guía *ArubaOS 8.10.0.0 Virtual Appliance Installation Guide* - [REF2].
24. Se debe tener en cuenta que los puertos de red de los dispositivos virtuales requieren capacidades de puerto promiscuo en sus tarjetas de red. Debido a esto, **se recomienda**

que los puertos físicos del dispositivo donde se instale la máquina virtual sean dedicados para el producto.

25. El acceso a la consola de gestión se puede realizar mediante tres (3) métodos:
    a) A través de la propia consola que ofrece la plataforma de virtualización. Este método es más simple, pero requiere que el administrador del producto disponga también de credenciales de acceso al dispositivo sobre el que se instala.
    b) Crear un puerto de consola. En la guía *ArubaOS 8.10.0.0 Virtual Appliance Installation Guide* – [REF2] se detalla cómo realizarlo para cada plataforma de virtualización soportada. **Se recomienda hacer uso de este método**.
    c) Interfaz de gestión fuera de banda. Consultar apartado 5.5.1 INTERFAZ DE GESTIÓN FUERA DE BANDA.

4.4.2 INSTALACION FISICA DE LOS DISPOSITIVOS FISICOS

26. En el caso de los dispositivos físicos se recomienda seguir el manual de instalación en función del modelo del equipo.
27. En función del modelo (tanto de *Mobility Controller* como de *Punto* de Acceso), localizar la correspondiente guía de instalación en el siguiente enlace.

4.4.3 PRIMER ACCESO

28. Tras la instalación física se puede proceder a la configuración inicial del equipo. En la guía *Getting Started Guide* – [REF6], se encuentra el detalle sobre cómo llevar a cabo la configuración inicial de los dispositivos tras el primer acceso.
29. Existen dos (2) formas de llevar a cabo dicha configuración:
    a) Automática o desatendida. Este tipo de instalación está pensada para facilitar las tareas de administración. Existen varios tipos y modalidades. El equipo obtiene diversa información vía DHCP o se le proporciona resolución DNS de algunos FQDN predefinidos en la controladora.
    b) Manual. En esta modalidad, los datos básicos se introducen a manualmente en un *script* inicial de configuración vía consola.
30. **Se recomienda hacer uso de la provisión manual de los dispositivos**. A continuación, se indican los pasos más importantes a seguir en una instalación manual.
31. Es necesario conectarse al puerto de consola del equipo. **Se recomienda no tener ningún puerto de red conectado**, para evitar el inicio no deseado de la configuración automática. Al finalizar el proceso de arranque, seleccionar la opción *full-setup* y confirmar la selección.
32. Los equipos *Mobility Controllers* pueden ejecutar las siguientes funciones:
    a) *Stand-Alone*: Controladoras inalámbricas autónomas, con o sin redundancia. **Se deberá seleccionar esta opción**.
    b) MD: *Managed Device*. Rol de *Mobility Controller* (Controladora inalámbrica) administrada y explotada desde equipos *Mobility Conductors*.
    c) VPNC: Concentrador VPN para *Mobility Controller* remotas.

33. La selección se hace en el paso Enter Switch Role (standalone|md).
34. Se deben rellenar los datos correspondientes de la organización, como la dirección IP deseada. Se deberá introducir también la contraseña correspondiente al usuario *admin*, utilizado posteriormente para llevar a cabo la configuración del dispositivo. Seguir las recomendaciones indicadas en el apartado 5.4.4 POLITICA DE CONTRASEÑAS.
35. Una vez finalizada la configuración inicial, se reiniciará el dispositivo.

5 FASE DE CONFIGURACION

5.1 MODO DE OPERACIÓN SEGURO

36. Dentro de las diferentes familias de controladoras, y para casi todos los modelos, existe una variante de fabricación denominada FIPS/TAA. Estos modelos implementan las normativas FIPS y TAA.

37. La diferencia entre modelos estándar y FIPS/TAA son principalmente:

Modelo *standard*	Modelo FIPS/TAA
Soporta Criptografía de 56bits (DES), <64bits (MD5) y de >=112bits de robustez.	Soporta Criptografía de 112 bits como mínimo (como regula FIPS 140-2), permitiendo la configuración de una seguridad equivalente a 128 bits.
Pueden ejecutar versiones de *software* FIPS y *standard*	Implementa medidas *hardware* para dificultar el acceso a componentes internos
	Proporciona etiquetas de sellado para puertos (según normativa FIPS)
	Dispositivo y/o componentes fabricados en países según norma TAA
	Sólo pueden ejecutar versiones de *software* FIPS.

Tabla 1. Diferencias entre Modelo standard y FIPS/TAA

38. Un dispositivo que ejecute versiones FIPS tendrá por tanto limitadas las funciones criptográficas a aquellas consideradas seguras. En dispositivos estándar, se puede realizar la configuración necesaria (manualmente) para deshabilitar los protocolos y algoritmos criptográficos no seguros.

39. **Se deberán adquirir modelos FIPS/TAA siempre que sea posible**, de tal forma que se dispondrá de la seguridad por defecto, no siendo necesario llevar a cabo configuraciones adicionales.

40. **En caso de adquirir un dispositivo sin modelo FIPS/TAA, se deberá realizar la descarga del *software* de tipo FIPS desde la página de soporte de Aruba**. Tras su descarga **deberá verificarse la integridad del fichero descargado**, comprobando que el hash SHA256 de dicho fichero coincide con el presente en la página de descarga. Adicionalmente el *software* es firmado por Aruba y el dispositivo verifica automáticamente el certificado.

41. En los modelos FIPS/TAA, **se deberá activar el modo seguro** para deshabilitar el empleo de protocolos y algoritmos inseguros. Para ello **utilizar el comando *fips enable*** en la interfaz CLI. Se puede verificar el modo seguro mediante el comando *show fips*.

42. En caso de haber adquirido otro tipo de modelo, se deberá llevar a cabo la configuración manual de cada protocolo para asegurar el nivel de seguridad requerido. Para ello, en el apartado 5.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS, se describen los pasos

necesarios para la securización de los distintos protocolos utilizados por el producto, indicando en aquellos casos donde sea necesario, qué configuraciones es necesario llevar a cabo.

5.2 AUTENTICACIÓN

43. El producto requiere la autenticación de los usuarios para el acceso a las funcionalidades y configuración. De aquí en adelante, se hará referencia a los usuarios con capacidades de gestión del producto como "administradores" y a los usuarios que únicamente dispongan de acceso para hacer uso de las funcionalidades del producto como "clientes".

44. Los mecanismos de autenticación utilizados para dicho propósito son:

    a) Credenciales locales, mediante usuario y contraseña. En el caso de SSH se puede hacer uso de clave pública. En la sección 5.4.2 CONFIGURACIÓN DE ADMINISTRADORES se detalla el proceso de definición de administradores locales. La sección 5.3.2 BASE DE DATOS INTERNA detalla la configuración local de clientes.

    b) Servidor de autenticación externo. Mediante la integración con distintos servidores de autenticación. Para la configuración y gestión de dichos servidores, ver apartado 5.3 SERVIDORES DE AUTENTICACIÓN.

45. Los equipos no ofrecen la posibilidad de cambio de contraseña a los usuarios de forma dinámica. Es decir, el cambio de la contraseña de un usuario local requiere la modificación de la configuración. Estas tareas se pueden simplificar mediante servidores externos de autenticación si se deben cambiar las contraseñas con cierta frecuencia. Por lo tanto, **se recomienda el uso de servidores externos de autenticación para la creación y gestión de usuarios del producto, ya que permitirá la rotación dinámica de contraseñas por parte de los usuarios**.

46. El producto permite también dar servicio a conexiones inalámbricas, conexiones cableadas que recibe por los interfaces ethernet que tienen y a conexiones VPN; ya que son dispositivos que también proporcionan este tipo de servicios. El detalle de configuración de la autenticación de clientes para estos propósitos se puede consultar en los capítulos *802.1X Authentication* y *Authentication Servers* de la guía *ArubaOS 8.10.0.0 User Guide* – [REF7].

47. Para la autenticación de tipo 802.1X, **se recomienda emplear siempre que sea posible EAP-TLS, para una mayor seguridad**.

48. Adicionalmente, el producto dispone de un portal cautivo para la detección y aprovisionamiento de nuevos clientes. **No se recomienda su uso, pero en caso de ser necesario, se debe verificar que emplea únicamente HTTPS para las comunicaciones**. Este es el comportamiento por defecto. Se puede consultar en detalle en el apartado *Captive Portal Authentication* de la guía *ArubaOS 8.10.0.0 User Guide* – [REF7].

49. El producto es compatible tanto con WPA2, como con WPA3. **Se deberá hacer uso de WPA3** siempre que sea posible, ya que proporciona un mayor nivel de seguridad. En caso de requerir el uso de WPA2, se recomienda que la red trabaje únicamente en este modo. Esto se debe a que, si se utiliza el modo de transición, que permite trabajar con clientes WPA2 y WPA3, los clientes en modo WPA3 se pueden ver forzados a una degradación de protocolo a WPA2. En la guía *WAP3* - [REF12] se proporcionan enlaces a la documentación detallada del producto, así como a un documento que describe los pormenores de WPA3.

50. Es posible también configurar los puntos de acceso para que se autentiquen en la red cableada. Esto hace que los puertos de red destinados a dar conectividad a los puntos de acceso no puedan ser usados por usuarios maliciosos, desconectando un punto de acceso y conectando en su lugar otro dispositivo. Esto se logra mediante la creación de un *ap provisioning-profile*. Lo cual hace que todos los APs de un determinado grupo utilicen esa configuración. **Se recomienda hacer uso de EAP-TLS**.

51. El detalle de configuración de la autenticación de los Puntos de Acceso se puede consultar en el capítulo *Before Deploying an AP > AP Provisioning* de la guía *ArubaOS 8.10.0.0 User Guide* – [REF7].

52. Se soportan los siguientes tipos de autenticación de usuarios finales:

    a) IEEE 802.1X (EAP, LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, EAP-POTP, EAP-GTC, EAP-TLV, EAP-AKA, EAP-Experimental, EAP-MD5).

    b) RFC 2548 Microsoft vendor-specific RADIUS attributes.

    c) RFC 2716 PPP EAP-TLS.

    d) RFC 2865 RADIUS authentication.

    e) RFC 3579 RADIUS support for EAP.

    f) RFC 3580 IEEE 802.1X RADIUS guidelines.

    g) RFC 3748 extensible authentication protocol.

    h) MAC address authentication.

    i) Web-based captive portal authentication.

5.3 SERVIDORES DE AUTENTICACIÓN

53. El producto soporta cuatro (4) tipos de servidores externos de autenticación: RADIUS, LDAP, TACACS+ y Windows (autenticación NTLM *stateful*). Además, dispone de una base de datos interna para autenticar a los clientes a través de la creación de entradas para cada usuario.

54. El producto permite la creación también de *Server Group*. Se trata de grupos de servidores para tipos específicos de autenticación. Por ejemplo, puede especificar uno o más servidores RADIUS que se utilizarán para la autenticación 802.1X. La lista de servidores en un grupo de servidores es una lista ordenada. Esto significa que el primer servidor de la lista se utiliza siempre, a menos que no esté disponible, en cuyo caso se utiliza el siguiente servidor de la lista. Se pueden configurar servidores de diferentes tipos en un mismo grupo. Un servidor puede pertenecer a varios grupos.

55. La funcionalidad de grupos de servidores permite activar el parámetro *Load-Balance* que permite repartir la carga entre diferentes servidores en caso necesario. Permite también el uso de *Server Group Match Rules* para determinar qué servidor atenderá la petición en función a las características del cliente o la conexión.

56. El alta de un servidor externo en el producto, con independencia del tipo que sea, se realiza desde la consola GUI en el menú *Configuration > Authentication > Auth Servers*. En el cuadro inferior, se puede añadir nuevo servidor pulsando *[+]*. A continuación, se debe seleccionar el tipo de servidor e insertar las opciones de *IP/hostname* y Nombre. Una vez

añadido el servidor se deben particularizar las opciones en función de cada tipo de servidor.

57. El detalle de configuración de servidores de autenticación se puede consultar en el apartado *Authentication Servers* de la guía *ArubaOS 8.10.0.0 User Guide* –[REF7].

5.3.1 PARÁMETROS DE LOS SERVIDORES EXTERNOS

58. En caso de utilizar RADIUS, se debe elegir una de las siguientes opciones para asegurar el tráfico:

    a) Emplear un túnel IPSEC para asegurar el canal. Se puede emplear el producto para ello y crear un túnel desde *Configuration > VPN > Site to Site*.

    b) Hacer uso de RADSEC (*RADIUS over TLS*). Para ello, después de crear el servidor RADIUS, se deberán emplear los siguientes comandos CLI:

```
(host) [mynode] (config) #aaa authentication-server radius <rad_server_name>
enable-radsec
radsec-client-cert-name <name>
radsec-port <radsec-port>
radsec-trusted-cacert-name <radsec-trusted-ca>
radsec-trusted-servercert-name <name>
```

59. En caso de utilizar TACACS+, se debe elegir una de las siguientes opciones para asegurar el tráfico:

    a) Emplear un túnel IPSEC para asegurar el canal. Se puede emplear el producto para ello, creando un túnel desde *Configuration > VPN > Site to Site*.

    b) Añadir las rutas IP necesarias para completar la configuración, en los dos extremos.

60. En caso de utilizar LADP, se deben configurar los siguientes parámetros:

    a) *Admin-dn*. Usuario del directorio para efectuar las consultas. Se recomienda que sea un usuario que sólo pueda hacer esta función.

    b) *Admin-password.* Contraseña del usuario.

    c) *Allow-clear-text*. Se debe deshabilitar para no usar comunicaciones en claro.

    d) *Base-dn*: Rama del directorio donde se buscarán los usuarios.

    e) *Preferred connection type.* Se recomienda *ldap-s* o *start-tls*. En caso de no funcionar uno, se probará con los otros. *Clear-text* no funcionará si se ha desactivado el campo anterior *Allow-clear-text*.

5.3.2 BASE DE DATOS INTERNA

61. Se dispone de una base de datos interna para autenticar a los clientes de la red inalámbrica. La base de datos interna contiene una lista de clientes, junto con la

contraseña y el rol por defecto de cada cliente. Dichos roles indicarán cómo se pueden conectar los clientes y bajo qué condiciones.

62. Esta base de datos interna es la que está configurada por defecto.

63. Para gestionar los clientes de la base de datos interna de usuarios, ir a Configuration > Authentication > Auth Servers > All Servers Configuration > Authentication > Auth Servers > All Servers y seleccionar Internal.

64. Los campos más relevantes cuando se da de alta un usuario son:

    a) *User name*. Se dispone de generación automática

    b) *Password*. Se dispone de generación automática.

    c) *Role*. Nombre del rol de cliente que se le asocia. Estos roles deben crearse previamente. El detalle de configuración de los roles de usuarios locales se puede consultar en la guía *Creating a user role* – [REF13].

    d) *Enabled*. Si el usuario está activado o desactivado.

    e) *Expiration*. Opciones de expiración de la cuenta de usuario en tiempo restante o por fecha y hora determinadas.

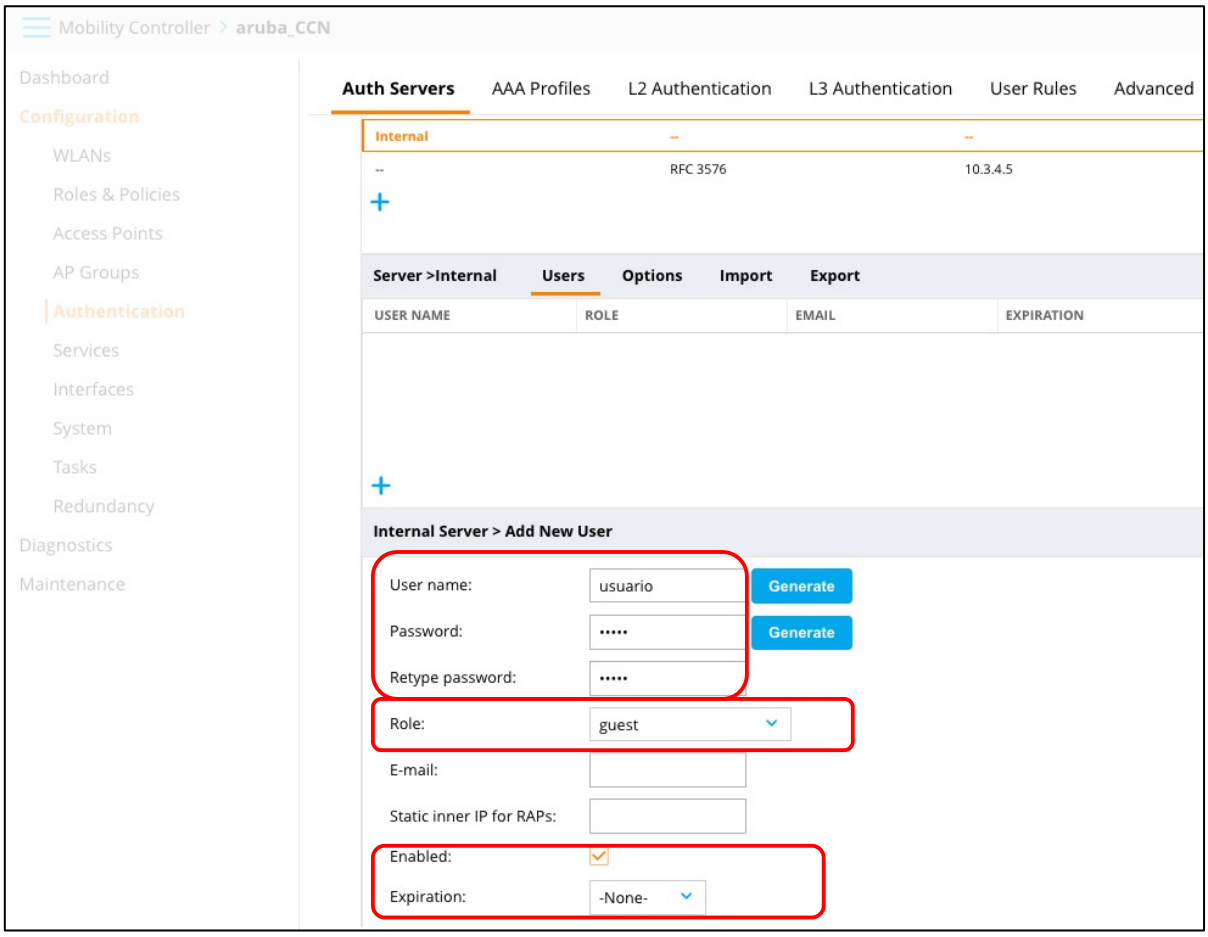


Ilustración 1. Creación de Usuarios en la Base de Datos Interna

65. También es posible realizar esta configuración vía CLI. Para eso se hace uso del comando *local-userdb*. Es importante destacar que este comando no se ejecuta en modo configuración sino desde el acceso privilegiado.

(aruba_CCN) [mynode] #Local-userdb add {generate-username|username <name>}{generate-password|password <password>}

5.4 ADMINISTRACIÓN DEL PRODUCTO

5.4.1 ADMINISTRACIÓN LOCAL Y REMOTA

66. El producto dispone de las siguientes interfaces para su administración:
    a) Administración local por consola, a través del puerto físico dedicado.
    b) Administración local de tipo CLI mediante SSH.
    c) Administración remota mediante interfaz gráfica, a través de HTTPS o API JSON.

67. La configuración de los protocolos utilizados para la administración del producto se puede consultar en el apartado 5.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS.

68. **Se debe deshabilitar el puerto consola**. Esto evitará que el procedimiento de recuperación de contraseña esté disponible. Si el dispositivo se reinicia, se puede seguir accediendo a la ROM de arranque a través del puerto de consola, lo que puede utilizarse para arrancar archivos de configuración alternativos, arrancar imágenes de *software* alternativas o borrar datos de la memoria *flash*. Para deshabilitar el acceso al puerto de consola desde *ArubaOS*:

    (aruba_CCN) [mynode] (config) # mgmt-user console-block

69. En caso de hacer uso de la interfaz gráfica, los cambios realizados en la configuración deberán ejecutarse. En la esquina superior derecha se notifica que hay cambios pendientes de realizar, mediante la notificación en la pantalla como *Pending Changes*. Se deberá hacer clic sobre dicha notificación, revisar los cambios realizados y hacer clic sobre *Deploy Changes*.

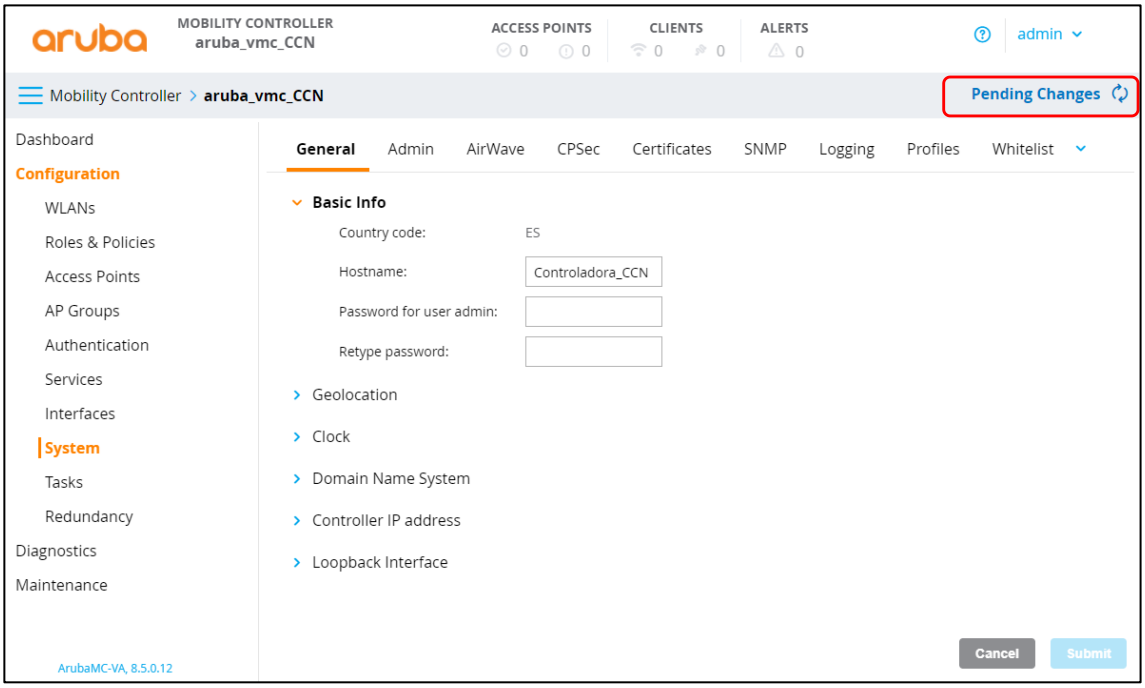


Ilustración 2. Ejemplo cambio de *hostname*. Cambio ejecutado, pendiente de despliegue.

70. De igual manera, en caso de hacer uso de la interfaz CLI, los comandos introducidos en este modo no se aplican hasta que se guarden los cambios mediante el comando *write memory*. Cuando existen comandos pendientes de ser aplicados, el *propmt* lo indica con el carácter ´^´.

```
(host) ^[mynode] #
```

71. Los comandos no aplicados pueden consultarse con el comando *show configuration pending*. En caso de desear cancelar los comandos introducidos, hacer uso del comando *configuration purge-pending-config*.

5.4.2 CONFIGURACIÓN DE ADMINISTRADORES

72. Dentro de la plataforma existen diferentes roles predefinidos de administrador. No se permite la creación de roles de administrador adicionales. El detalle de los permisos de los roles predefinidos de administrador se puede consultar en el siguiente enlace.

73. De forma general, la selección del servidor de autenticación (externo/interno) mediante la consola GUI se realiza desde *Configuration > System > Admin > Admin Authentication Options*. Esta selección aplicará a todos los administradores del producto. El producto tratará de autenticar el administrador contra el primer servidor configurado y, en caso de no recibir respuesta, probará contra el siguiente en la lista. Si un servidor deniega la autenticación, no se prueba más.

74. Para la creación de administradores se deben tener en cuenta los siguientes aspectos:

    a) Definición del usuario. Local en el equipo o en un servidor externo.

    b) Permisos del usuario. Un rol de administración

    c) Tipo de credenciales. Contraseña o certificados.

5.4.3 DEFINICIÓN DE ADMINISTRADORES LOCALES

75. La creación de administradores con contraseña se puede hacer mediante el interfaz gráfico o línea de comandos. Mediante el interfaz gráfico se debe ir a *Managed Network > Configuration > System > Admin > Management Users*. Hacer clic en *+.* Introducir el nombre de usuario deseado, la contraseña que tendrá dicho usuario y hacer clic en *Submit*.

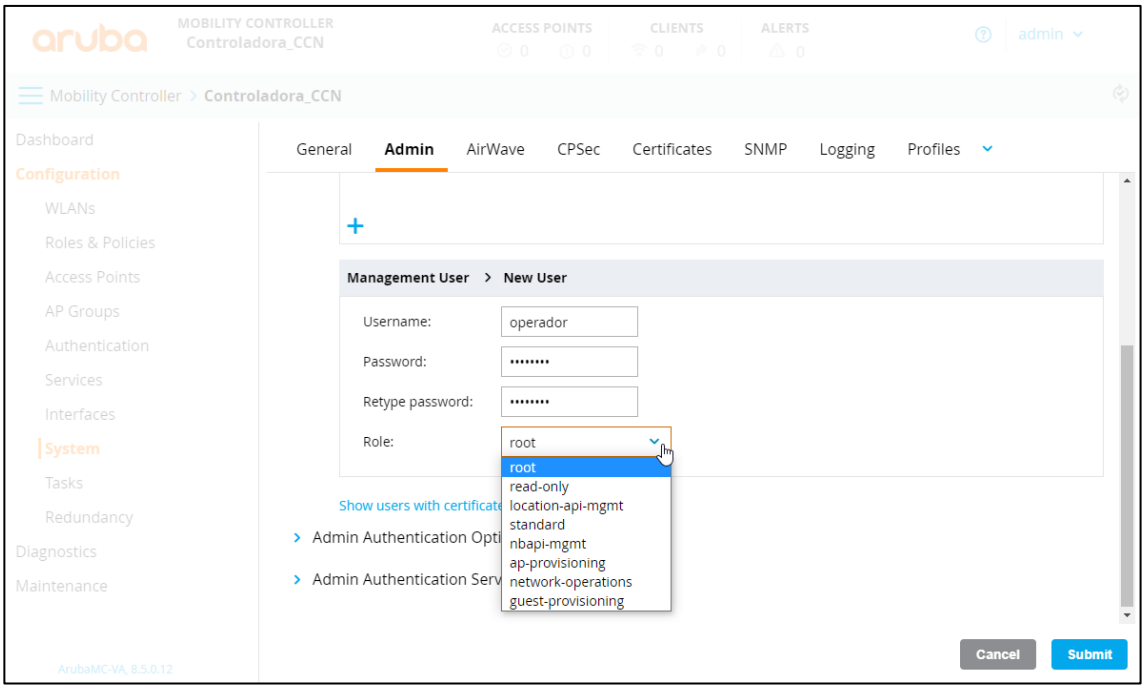


Ilustración 3 Creación de un usuario local con contraseña

76. Por CLI la definición de usuario se hace mediante el comando *mgmt-user*. Con este comando, además del perfil y del nombre de usuario, se define el número máximo de sesiones que este usuario puede abrir.

```
mgmt-user <username> <rolename> max-concurrent-sessions
<num_sesiones>
```

77. Una vez creados los usuarios, se puede configurar el uso de la autenticación mediante certificados para los usuarios en el acceso a la interfaz GUI. Para ello, se deben seguir los pasos indicados en el capítulo *Configuring Certificate Authentication for WebUI Access* de la guía *ArubaOS 8.10.0.0 User Guide* – [REF7].

78. De igual forma, el producto permite el uso de autenticación de clave pública en el acceso a la interfaz CLI. Para ello, seguir los pasos indicados en el capítulo *Secure Shell > Enabling Public Key Authentication* de la guía *ArubaOS 8.10.0.0 User Guide* – [REF7].

79. Para el detalle de configuración de los certificados, consultar el apartado 5.7 GESTIÓN DE CERTIFICADOS.

5.4.4 POLITICA DE CONTRASEÑAS

80. Es posible configurar una política de contraseñas para todas aquellas almacenadas en el producto. Para ello, **se debe configurar el perfil de gestión de contraseñas** (*Management Password Policy Profile*) desde *Managed Network > Configuration > System > Profiles > Other Profiles > Mgmt Password Policy*.

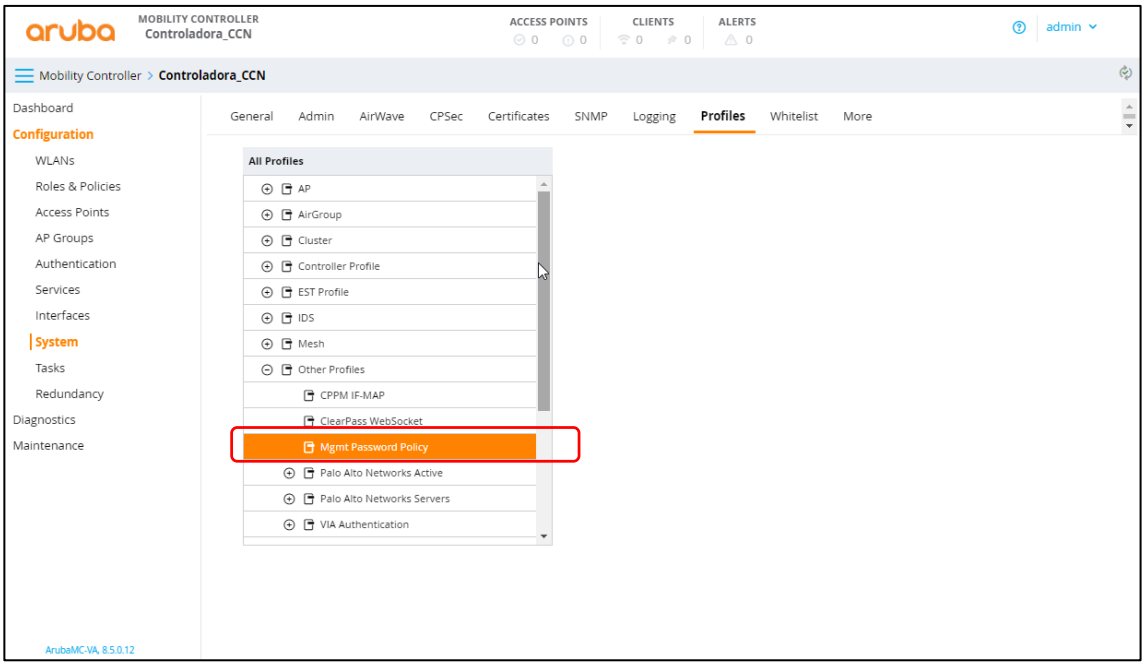


Ilustración 4. Configuración del perfil de la política de contraseñas

81. Las opciones disponibles son:

    a) *Minimum password length required*: define el número mínimo de caracteres de la contraseña, se recomienda un valor de, al menos, 12 caracteres.

    b) *Minimum number of Upper Case Characters*: define el número mínimo de letras minúsculas que deben formar la contraseña. **Se recomienda, al menos, uno.**

    c) *Minimum number of Lower Case Characters*: define el número mínimo de letras mayúsculas que deben formar la contraseña. **Se recomienda, al menos, uno.**

    d) *Minimum number of Digits*: define el número mínimo de números que deben formar la contraseña. **Se recomienda, al menos, un valor de uno.**

    e) *Minimum number of differing characters between* passwords: define el número mínimo de caracteres en los que debe diferenciarse una contraseña respecto a la anterior.

    f) *Minimum number of special characters*: define el número mínimo de caracteres especiales que deben formar la contraseña. **Se recomienda, al menos, un valor de uno.**

    g) *Username or Reverse Username NOT in password*: **se recomienda activar** esta opción para prevenir que el nombre de usuario forme parte de la contraseña.

    h) *Maximum consecutive characters repeats*: define el número de caracteres iguales que se pueden repetir de forma consecutiva.

    i) *Maximum Number of failed attempts in 3 minute window to lockout user*: define el número de intentos de inicio de sesión fallidos tras el cual se bloqueará la cuenta durante un periodo de tiempo definido. **Se recomienda configurar un valor bajo, por ejemplo, de 3 intentos.**

j) *Time duration to lock out the user upon crossing the "lock-out" threshold*: define la duración del bloqueo de las cuentas de usuario en minutos. **Se recomienda un valor de 5 minutos.**

82. Adicionalmente, de manera procedural en la organización:

    a) No se podrán reutilizar las últimas 5 contraseñas.

    b) Se deberán modificar las contraseñas tras un periodo de 60 días.

    c) No se podrá modificar una contraseña nueva hasta pasados 7 días.

83. En el caso de los administradores definidos en servidores de autenticación externos, la política de contraseñas de aplicación será la implementada en dicho servidor. Por lo tanto, **se deberá utilizar una política de contraseñas igual o equivalente en los servidores de autenticación externos**.

5.4.5 CONFIGURACION DE MENSAJE DE BIENVENIDA (BANNER)

84. **Se debe configurar un mensaje de bienvenida o banner de acceso al sistema**. Este se mostrará en las conexiones CLI y GUI.

85. Desde el CLI se configura con el comando *banner motd*. Con el comando *banner enforce-accept* se fuerza que el banner deba ser aceptado antes de poder acceder al equipo.

```
(Controladora_CCN) [mynode] (config) #banner motd $
Enter TEXT message [maximum of 4095 characters].
End with the character '$'.
=========================================================
Este dispositivo ha sido configurado para la elaboracion de este procedimiento.
Desconectese puesto que este dispositivo ya no existe.
Cualquier inquietud dirigase atentamente.
Madrid 2021
=========================================================
$
(Controladora_CCN) ^[mynode] (config) # banner enforce-accept
(Controladora_CCN) ^[mynode] (config) #
```

86. Tras aceptar el mensaje, se procede al acceso regular mediante usuario y contraseña.

87. La misma configuración se puede realizar desde el interfaz gráfico, en el menú *Configuration > system > Admin*. Se debe configurar el texto que se desea presentar, así como la casilla *Banner has to be accepted*.

5.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

88. Todos los puertos del producto pueden configurarse en modo acceso o modo troncal. Un puerto está en modo de acceso activado por defecto y transporta tráfico sólo para la VLAN a la que está asignado. En modo troncal, un puerto puede transportar tráfico para múltiples VLANs.

89. El tráfico en los interfaces *ethernet* puede ser clasificado en modo confiable (*trusted*) o no confiable (*untrusted*). En modo no confiable el dispositivo dispararía mecanismos de autenticación análogos a los que existen para Wireless.
90. Si el tráfico se clasifica como no fiable, entonces el tráfico es susceptible de ser autenticado. Para eso, dentro de la VLAN es necesario determinar un perfil de autenticación.
91. El detalle de configuración de las interfaces se puede consultar en el apartado *Network Configuration Parameters* de la guía *ArubaOS 8.10.0.0 User Guide* – [REF7].

5.5.1 INTERFAZ DE GESTIÓN FUERA DE BANDA

92. Algunos modelos disponen de puerto fuera de banda.
93. El puerto de *Management* en los dispositivos *ArubaOS* no es un puerto de gestión fuera de banda (OOB) totalmente funcional. Este puerto es de "mantenimiento" y solo debe utilizarse para ello. El puerto no puede enrutar paquetes y solo puede alcanzar direcciones IP de la misma subred en la que la interfaz está configurada. Por lo tanto, **se recomienda no hacer uso de la interfaz de gestión fuera de banda**.
94. **Es necesario deshabilitar este puerto,** para ello hacer uso del siguiente comando:

```
interface mgmt shutdown
```

5.5.2 PROTECCIÓN DEL PUERTO DE CONSOLA DE LOS AP

95. Los puntos de acceso disponen de puerto de consola propio. El producto realiza una protección de dichos puertos mediante la configuración del perfil de propiedades de sistema AP (*Profile AP-System*). Para ello ir a *Configuration > System > Profiles > AP system*.
96. **Se recomienda seleccionar la opción de configurar una contraseña para poder hacer uso de dichos puertos o deshabilitarlos**. **Es necesario asegurarse que la casilla *Telnet* se encuentra desmarcada** para no permitir el acceso mediante dicho protocolo.

5.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

97. Tal como se ha visto anteriormente, en caso de obtener un modelo estándar de controladora, es necesario llevar a cabo la configuración de los protocolos para **asegurar una seguridad mínima equivalente a 128 bits en los servicios criptográficos.**
98. En caso de obtener un modelo FIPS/TAA con el modo seguro activado, se pueden consultar los siguientes apartados para verificar que todas las configuraciones son activadas en el dispositivo son correctas.

5.6.1 SNMP

99. En caso de requerir el uso de SNMP, **se debe hacer uso de SNMPv3 ya que soporta cifrado**. Para configurar SNMPv3, primero se debe crear un usuario SNMPv3. Esto se hace desde *Configurations > System > SNMP > Users SNMPv3*.
100. Se recomienda el uso de SHA como protocolo de autenticación y AES128 de cifrado.

101. A continuación, se debe dar alta el servidor que usará SNMPv3. Desde *Configurations > System > SNMP > SNMP Trap Receivers* se procede a añadir el servidor, seleccionando la versión y el usuario antes creado. Se debe seleccionar SNMPv3 en el apartado *Version*.
102. Para realizar dicha configuración desde la interfaz CLI, utilizar los siguientes comandos:

```
(Controladora_CCN) #configure terminal

(Controladora_CCN) (config) #snmp-server user "usuario_snmpv3" auth-prot
SHA "clave_prot" priv-prot AES "clave_encript"

(Controladora_CCN)  (config) #snmp-server host "10.3.3.3" version 3 " us
uario_snmpv3"
```

5.6.2 TELNET

103. En versiones estándar el servidor telnet está deshabilitado. En versiones FIPS no es posible activarlo. En caso de habilitarlo (configuración insegura) y requerir deshabilitarlo posteriormente, se deben usar los siguientes comandos:

```
no telnet cli
no telnet soe
```

104. Para verificar el estado del servicio ejecutar el comando *show telnet*.
105. Desde el interfaz gráfico, se puede configurar y verificar el estado actual, desde *Managed Networks* ir a *Configuración > System > Admin > Admin Autentication Options* y deseleccionar *Management telnet Access*.

5.6.3 WIFI

106. **Se recomienda evitar el uso de cifrados de tipo TKIP en las configuraciones de los SSID**. Este tipo de cifrados contienen debilidades conocidas.
107. La configuración de los SSID se lleva a cabo desde *Configuration > System > Profiles tab*, seleccionando *Wireless LAN > SSID*.

5.6.4 HTTPS

108. El producto hace uso de HTTPS por defecto para el acceso a la interfaz GUI, en caso de operar en modo seguro. Se debe configurar el perfil de cifrados “alto”, el cual especifica la **seguridad de longitudes de claves de 128 bits o equivalente**.
109. Este perfil se encuentra configurado por defecto y es el único disponible en modo seguro.

```
(Controladora_CCN) [mynode] (config) #web-server profile ciphers high
```

110. Las suites de cifrado disponibles serán las siguientes:
    a) TLS_RSA_WITH_AES_128_CBC_SHA
    b) TLS_RSA_WITH_AES_256_CBC_SHA
    c) TLS_DHE_RSA_WITH_AES_128_CBC_SHA
    d) TLS_DHE_RSA_WITH_AES_256_CBC_SHA
    e) TLS_RSA_WITH_AES_128_CBC_SHA256
    f) TLS_RSA_WITH_AES_256_CBC_SHA256

g) TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

h) TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

i) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

j) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

k) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

l) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

111. Para el correcto uso de HTTPS se deberán configurar previamente los certificados de servidor que utilizará el producto en sus comunicaciones. Ver apartado 5.7 GESTIÓN DE CERTIFICADOS.

112. **Se debe utilizar solo TLS v1.2 o versiones superiores. Para ello, TLS 1.0 y TLS 1.1 deben ser deshabilitados**. Para habilitar solo el soporte de TLS 1.2, configurar *web-server profile ssl-protocol tlsv1.2*.

```
(Controladora_CCN) [mynode] (config) #web-server profile ciphers high

(Controladora_CCN) [mynode] (config) #web-server profile ssl-protocol tl
sv1.2
```

113. En el interfaz gráfico estas opciones se configuran desde Configuration > System > Profiles > Other Profiles > Web Server Configuration.

114. **Se debe configurar también el límite de tiempo de las sesiones GUI**. Para ello, desde el interfaz gráfico, ir a Configuration > System > Profiles > Other Profiles > Web Server Configuration, parámetro User absolute session timeout, con el valor en segundos tras el cual finalizarán las sesiones, **se recomienda un valor de 5 minutos** (300 segundos).

5.6.5 SSH

115. El producto hace uso de SSH para el acceso remoto a la interfaz CLI. La única versión disponible es SSHv2.

116. Para llevar a cabo la configuración de SSH, desde la interfaz gráfica, ir a *Managed Networks* y luego a *Configuración > System > Admin > Admin Autentication Options*. **Se debe utilizar AES-CTR como mecanismo de cifrado recomendado y HMAC-SHA1-96 como algoritmo de autenticación**. Se recomienda también configurar el parámetro *Idle session timeout*, con el tiempo tras el cual se cerrarán las sesiones inactivas, **se recomienda un valor bajo, por ejemplo, 5 minutos.**

5.6.6 IPSEC

117. El producto hace uso de IPsec para la creación de VPNs y túneles punto a punto.

118. Para el uso de IPSEC con CPsec (ver apartado 5.14.1 SEGURIDAD EN EL PLANO DE CONTROL - CPSec) y terminación de Puntos de Acceso Remotos (RAP), la configuración se realiza automáticamente por parte del equipo. No se requiere intervención del administrador. Esto securiza la comunicación entre *Mobility Controller* y Punto de Acceso.

119. La creación o modificación de políticas puede hacerse usando el CLI o bien el interfaz gráfico GUI. Mediante CLI se hace utilizando los *comandos crypto isakmp policy* y *crypto dynamic-map*. Desde GUI se debe ir a *Configuración > Servicios > VPN*. Para eliminar una

política IKE, seleccionar una política existente y hacer clic en el icono de la papelera para eliminar la política.

120. A continuación, se indican, dentro de los distintos parámetros disponibles, cuales se recomienda utilizar. **Se deberán eliminar las políticas predefinidas que utilicen algoritmos no listados a continuación y crear políticas nuevas acorde a la seguridad especificada**.

    - Algoritmos de cifrado.
        - AES128
        - AES192
        - AES256 (Para la conexión con el AP)
    - Algoritmos hash.
        - sha2-256-128 (Para la conexión con el AP).
        - sha2-384-192.
    - Autenticación.
        - rsa-sig. En caso de usarse, deberán emplearse longitudes de clave de, al menos, 3072 bits.
        - ecdsa-256.
        - ecdsa-384.
    - Intercambio de claves.
        - Grupo 14 (Para la conexión con el AP).
        - Grupo 19.
        - Grupo 20.
    - Función HMAC.
        - PRF-HMAC-SHA2-256 (Para la conexión con el AP)., longitud de claves >=125.
        - PRF-HMAC-SHA2-384, longitud de claves >=125.

121. En caso de hacer uso de la funcionalidad de mapas dinámicos, **se debe activar la función de *Perfect Forward Secrecy***, el cual asegura que la clave utilizada no ha sido derivada de ninguna otra, aportando mayor seguridad.

122. El detalle de configuración de IPsec se puede consultar en el apartado *Virtual Private Networks* de la guía *ArubaOS 8.10.0.0 User Guide* – [REF7].

5.7 GESTIÓN DE CERTIFICADOS

123. El detalle de configuración de los certificados se puede consultar en el apartado *Managing Certificates* de la guía *ArubaOS 8.10.0.0 User Guide* – [REF7].

124. Se deberán seguir los siguientes pasos generales:

    - Crear un CSR (*Certificate Signing Request*). **Se deberá utilizar uno de los siguientes parámetros para la creación del certificado**:

- Tipo de clave ECDSA, con un tamaño de 256 o 384 bits.
- Tipo de clave RSA, con una longitud de clave de 4096 bits.

- Importar los siguientes certificados:
  - Certificado de servidor del producto (creado mediante CSR en el paso anterior). Si se desea, se pueden importar distintos certificados de servidor para los distintos servicios que los utilizan.
  - Certificado de la CA utilizada para generar el certificado de servidor.
  - Certificados de CA necesarios para validar los certificados de los dispositivos o usuarios con los que interactuará el producto. Por ejemplo, CA de los certificados de usuarios administradores o CA del servidor RADIUS (RADSEC).
  - Certificados de claves públicas de cliente, utilizados para el acceso por parte de los usuarios (en caso de configurarse dicho comportamiento). El certificado se utilizará para el acceso GUI y la clave para SSH. **Se recomienda emplear claves RSA de, al menos, 3072 bits o claves de tipo ECDSA de, al menos, 256 bits**.

125. El producto permite verificar la validez de los certificados mediante listas CLR. Adicionalmente, se puede configurar el producto como cliente OSCP para realizar dicha verificación mediante consultas a servidores OSCP remotos. El detalle de configuración de la verificación de validez de los certificados se puede consultar en el apartado *Certificate Revocation* de la guía *ArubaOS 8.10.0.0 User Guide* – [REF7].

5.8 SINCRONIZACIÓN HORARIA

126. **Se recomienda que todos los sistemas utilizados por la organización se encuentren sincronizados** para permitir una alta fiabilidad en los sistemas de auditoría y *logging*.

127. El producto permite sincronizar los registros de auditoría mediante el uso de NTP. Para un mayor grado de seguridad, **deberá utilizarse autenticación NTP**, para evitar la posible intercepción de comunicaciones NTP y su modificación.

128. Para activar la autenticación NTP, desde *Configuration > System > General > Clock* crear una clave de autenticación. **Se debe usar SHA**, en vez de la opción MD5.

129. Una vez creada la clave de autenticación, se debe configurar el servidor NTP que hará uso de dicha clave, introducir los datos del servidor NTP y seleccionar la casilla *Use NTP authentication*.

130. Para realizar la configuración desde la interfaz CLI, se deben emplear los siguientes comandos:

```
(Controladora_CCN) #configure terminal
(Controladora_CCN) (config) #ntp authentication-key 1 sha1 secreto
(Controladora_CCN) (config) #ntp trusted-key 1
(Controladora_CCN) (config) #ntp server 10.9.8.7 key 1
(Controladora_CCN) (config) #ntp authenticate
```

5.9 ACTUALIZACIONES

131. De forma previa a la actualización del sistema, deberá descargarse el *software* desde la página de soporte de Aruba. Tras su descarga **deberá verificarse la integridad del fichero descargado, comprobando que el hash SHA256 de dicho fichero coincide** con el presente en la página de descarga. Adicionalmente, el *software* es firmado por Aruba y el dispositivo verifica automáticamente el certificado.

132. Es posible actualizar el sistema operativo del dispositivo a través de la WebUI o de la CLI. Se pueden utilizar los siguientes métodos para actualizar el sistema operativo del controlador:

    a) TFTP. **No se debe emplear este método.**

    b) FTP. **No se debe emplear este método.**

    c) SCP. **Se recomienda el uso de este método para llevar a cabo las actualizaciones.**

    d) Archivo local (Esta opción está disponible cuando se actualiza a través de WebUI).

    e) USB (en los dispositivos físicos que los soportan).

133. De forma previa a una actualización del sistema, se recomienda llevar a cabo una copia de seguridad. Ver apartado 5.13 COPIAS DE SEGURIDAD.

134. Para actualizar el sistema, ir a *Maintenance > Software Management > Upgrade*. Una vez lanzado el proceso, se debe determinar si se desea reiniciar el dispositivo después de la actualización.

135. Mediante la interfaz CLI se puede realizar la actualización haciendo uso del siguiente comando:

```
(aruba_CCN) [mynode] (config)# copy scp: 10.1.2.3 usuario fichero_fimware system: partition 0

Password:*******
```

5.10 AUTO-CHEQUEOS

136. El equipo verifica en el arranque la integridad del software. Se verifica tanto el *bootloader* como la imagen de *firmware*. Se utiliza para ello un hash SHA-256 en base a información de certificados instalados en el TPM. También se verifica en el arranque el sistema de archivos, así como el resto de componentes.

137. En caso de fallo, el equipo considera la imagen dañada e intenta la otra partición. Esta acción se refleja en los logs del equipo. Cuando el equipo arranca el sistema operativo envía el correspondiente mensaje de *logging* a la consola. El equipo por tanto no arranca y una o las dos imágenes inválidas deben ser reemplazadas.

5.11 ALTA DISPONIBILIDAD

138. El producto dispone de varios mecanismos para la implementación de Alta Disponibilidad:

    a) Uso de *Mobility Conductors*. Opción recomendada si se busca lograr facilidades de administración y continuidad de servicio. Permite la implementación de clústeres que aportan mecanismos de alta disponibilidad de cara a los puntos de acceso y dispositivos conectados.

b) *Mobility Conductors* en un diseño Activo/Pasivo. Cada punto de acceso establece un túnel activo y otro en espera con la otra controladora, lo cual permite una rápida conmutación de una a otra con mínima pérdida de servicio.

c) Uso de VRRP (*Virtual Router Redundancy Protocol*). Se emplea VRRP entre las controladoras, estas configuran a los puntos de acceso para el establecimiento del túnel. Está limitado a dos controladoras. En caso de caída de una controladora, un punto de acceso se resetea para registrarse de nuevo con la controladora.

139. El detalle de los distintos tipos de Alta Disponibilidad disponibles y de cómo llevar a cabo su configuración se puede consultar en la guía *ArubaOS 8.10 - AP and User Redundancy Methods* – [REF8].

5.12 AUDITORÍA

140. El detalle de configuración de los mensajes de auditoría del producto se puede consultar en la guía *Syslog Message Guide* – [REF9].

141. Para cada categoría o subcategoría, **se recomienda configurar al menos un nivel de registro *debug***, para registrar todos los eventos del sistema. Para ello ir a *Configuration > System > Logging > Logging Levels*.

142. El producto dispone de un espacio de almacenamiento local limitado para los registros de auditoría. Tras alcanzar el límite de almacenamiento, comenzará a eliminar registros antiguos para poder almacenar los nuevos.

143. Debido a esto, para asegurar la disponibilidad de los registros a largo plazo, **se recomienda configurar el envío de registros a un servidor *Syslog* externo**. Para ello ir a *Configuration > System > Logging > Syslog Servers* y configurar los parámetros deseados.

144. La comunicación entre el producto y el servidor *Syslog* se produce en claro, por lo que **deberá protegerse mediante un túnel IPsec**. Esto se puede hacer desde *Configuration > VPN > Site to Site*, creando un túnel que apunte al servidor *Syslog*.

145. La auditoría relacionada con los certificados en IPSEc no está activada por defecto, por lo que se deberá activar mediante SSH con los siguientes comandos:

```
configure terminal
logging security subcat est level debugging
write memory
```

146. Por último, se puede hacer uso del comando CLI *tar logs* para crear un archivo con todos los registros locales y, a continuación, utilice el comando CLI *copy* (**empleando siempre el protocolo SCP**) para copiar el archivo en un servidor externo.

5.13 COPIAS DE SEGURIDAD

147. **Se recomienda realizar copias de seguridad periódicas de la configuración del producto** para, en caso de ser necesario, poder recuperar el estado. Para ello es posible crear copias de seguridad locales o exportarlas a una ubicación externa.

148. Dichas copias de seguridad pueden contener todo el sistema de archivos flash del dispositivo o únicamente la configuración del producto.

149. Para realizar una copia de seguridad ir a *Maintenance > Configuration Management > Backup*. Se debe seleccionar si se desea salvar el sistema de ficheros o la configuración.

150. Una vez generado, se puede copiar el archivo comprimido en un servidor externo, para ello pulsar sobre *Copy Backup*. Llevará a la página de gestión de ficheros que se encuentra en *Diagnostics > Technical Support > Copy Files*. **Se debe configurar un servidor de tipo SCP para realizar el envío de las copias de seguridad**.

5.14 SERVICIOS DE SEGURIDAD

5.14.1 SEGURIDAD EN EL PLANO DE CONTROL - CPSEC

151. La función de seguridad en el plano de control entre *Mobility Controllers* y APs (CPSec) tiene dos (2) funciones principales:

    a) Asegurar el canal de control entre los *Mobility Controllers* y sus APs conectados.

    b) Impedir que los APs no autorizados se unan a la red WLAN de la organización.

152. **Activar y usar CPSEC**. Esta funcionalidad se encuentra habilitada por defecto. Para mayor seguridad, se recomienda también deshabilitar el auto-aprovisionamiento de certificados para los AP. Para ello seleccionar *Mobility Controller* e ir a *Configuration > System > CPsec,* y deshabilitar la opción ***Enable auto cert provisioning***.

153. El producto dispone de dos (2) listas separadas de APs permitidas, una para los AP campus (pertenecientes a la red LAN) y otra para los AP remotos (pertenecientes a una red remota). Se recomienda hacer uso de estas listas para añadir los AP válidos y revocar el acceso a aquellos que no vayan a utilizarse o sean sospechosos.

154. El detalle de configuración de CPSEC se puede consultar en el apartado *Control Plane Security Overview* de la guía *ArubaOS 8.10.0.0 User Guide* – [REF7].

5.14.2 CONFIGURACIÓN DE DEFENSA DEL PLANO DE CONTROL

155. El producto proporciona mecanismos de protección del plano de control del equipo. Existen tres (3) áreas principales de la configuración de estos parámetros.

    a) Parámetros Globales (Global Settings).

    b) ACLs de sistema permitidas (ACL White List).

    c) Contratos de Ancho de Banda. Adicionalmente, pueden configurarse direcciones MAC a modo de excepciones (BW Contracts Exception List).

156. El detalle del funcionamiento y configuración de los parámetros generales se puede consultar en la guía *Understanding Global Firewall Parameters* – [REF3]. Entre estos se encuentran protecciones contra ataques conocidos y monitorización de las sesiones.

157. Se deberá analizar qué parámetros utilizar para proteger la red de la organización en base a las posibles amenazas de esta. Sin embargo, se recomienda hacer uso de, al menos, los siguientes parámetros:

    a) *Deny inter user bridging y Deny inter user traffic*. Limita la comunicación entre usuarios. Si el producto va a dar servicios donde los usuarios no deben tener visibilidad entre sí se recomienda hacer uso de estos parámetros.

b) *Prohibit ARP-spoofing*. Bloquea que un cliente inalámbrico envíe respuestas o mensajes ARP para una combinación IP/MAC que no sea la suya.

c) *Prohibit IP Spoofing*. Un ataque de suplantación de IP se produce cuando un usuario inalámbrico configura estáticamente un dispositivo con una dirección IP que pertenece a otro dispositivo de la red. Este parámetro bloquea una dirección IP concreta con una dirección MAC determinada.

158. El detalle del funcionamiento y configuración de las listas de acceso y los controles de Ancho de Banda se puede consultar en la guía *Firewall Policies* – [REF10]. Entre estos se encuentran protecciones contra ataques conocidos y monitorización de las sesiones.

159. Adicionalmente, desde *Configuration > System > Profiles > Wireless LAN > Virtual AP > <ssid> > AAA*, se puede activar *Enforce DHCP*. Este parámetro obliga el uso de DHCP e impide las asignaciones estáticas de IPs.

5.14.3 WIRELESS IPS

160. El producto incluye la funcionalidad de detección de APs falsos y otras capacidades más avanzadas si se adquiere la licencia *RFProtect*. En caso de utilizarse, se recomienda utilizar el nivel Medio, ya que aporta un buen nivel de seguridad y evita crear demasiados falsos positivos.

161. El detalle de las funcionalidades y configuración de la funcionalidad WIPS se puede consultar en la guía *Wireless Intrusion Prevention* – [REF4].

5.14.4 CONTROL DE CONTENIDOS - WEBCC

162. El uso de la funcionalidad de Control de Contenidos requiere la licencia *WebCC*. Esta funcionalidad permite clasificar todo el tráfico web y permite que el dispositivo gestionado aplique políticas de cortafuegos basadas en la categoría y la reputación del contenido web. Requiere acceso a internet.

163. El detalle de configuración de la funcionalidad de Control de Contenidos se puede consultar en la guía *Web Content* – [REF11].

5.14.5 REMOTE ACCESS POINTS

164. El servicio de Punto de Acceso Remoto Seguro permite conectar un Punto de Acceso en ubicaciones remotas, conectarse a un *Mobility Controller* a través de Internet o en general a través de una red ajena. El tráfico entre el *Mobility Controller* y el AP será cifrado mediante IPSec.

165. En el caso de que la red a través de la cual se trate de conectar sea Internet, será necesario que el *Mobility Controller* disponga de una IP Pública a la cual tratará de conectarse el Punto de Acceso Remoto.

166. A través del túnel IPSec, se envía tanto el tráfico de control como de los usuarios. En el caso de que se vaya a hacer uso de esta funcionalidad, se recomienda que el *Mobility Controller* se ubique en una DMZ protegido por un cortafuegos. En organizaciones de mayor tamaño es conveniente dedicar un *Mobility Controller* ubicado en DMZ a los Puntos de Acceso Remoto, y otro *Mobility Controller* en la zona interna para el servicio normal.

167. El detalle de configuración de los Puntos de Acceso Remotos se puede consultar en el apartado *Remote Access Points* de la guía *ArubaOS 8.10.0.0 User Guide* – [REF7].

5.14.6 MULTIZONA

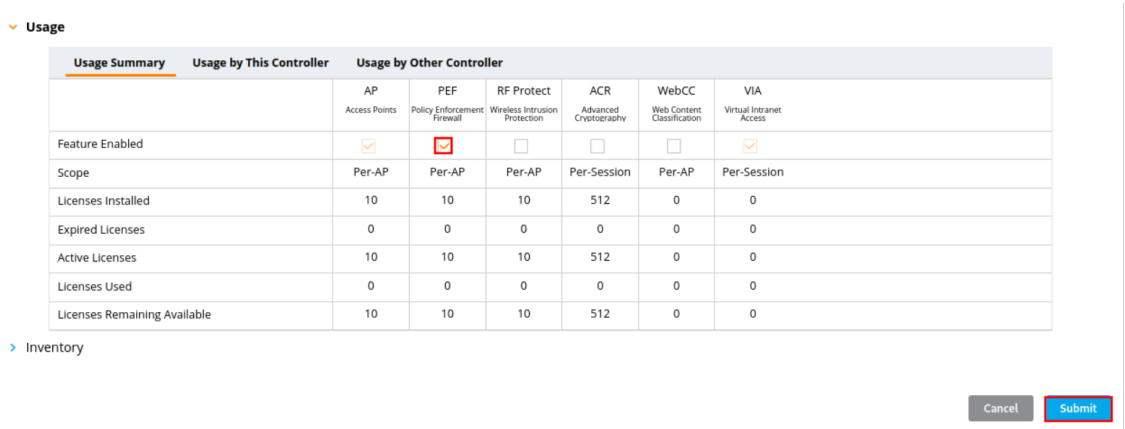
168. El servicio de MultiZona permite administrar redes distintas haciendo uso de un mismo AP. Permite así que el tráfico de las distintas redes no se mezcle, a pesar de emplear el mismo AP.

169. En caso de hacer uso de MultiZona, se recomienda emplearlo en conjunto con la funcionalidad CPsec.

170. El detalle de configuración de MultiZona se puede consultar en el apartado Multizone de la guía *ArubaOS 8.10.0.0 User Guide* – [REF7].

5.14.7 BLOQUEAR TRAFICO DE SYSLOG

171. Es necesario bloquear el tráfico de Syslog de todas las interfaces para permitirlo únicamente a través de CPsec. Para activar el cortafuegos, ve hacia *Configuration > License > Usage*, activa *Policy Enforcement Firewall (PEF)* y guarda los cambios.



172. Ahora entra a través de SSH, crea una regla para bloquear el tráfico Syslog y aplícalo a todas las interfaces.

```
configure terminal
ip access-list session denegar-syslog
any any svc-syslog deny
any any any permit
interface gigabitethernet 0/0/0
ip access-group in denegar-syslog
exit
interface gigabitethernet 0/0/1
ip access-group in denegar-syslog
exit
(así para todas las interfaces disponibles)
write memory
```

5.15 VIRTUAL INTRANET ACCESS

173. La solución Aruba VIA está diseñada para proporcionar un acceso corporativo seguro a los ordenadores y teléfonos inteligentes de los empleados desde cualquier lugar. El cliente Aruba VIA es un servicio VPN seguro para los usuarios que necesitan conectividad corporativa en casa, en sitios temporales o mientras están en movimiento.

174. Se trata de un cliente VPN híbrido IPsec/SSL. El cliente se puede descargar directamente desde un controlador.

175. Los tres (3) elementos más relevantes de la configuración de Aruba VIA son:

    a) Perfil VIA de Autenticación Web (*Web Authentication Profile*). Regula quién y cómo se puede descargar los perfiles VPN de los usuarios, así como descargar el cliente del Mobility Controller.

    b) Perfil VIA de Autenticación (*VIA Authentication Profile*). Regula cómo autenticar a los usuarios VPN. Se debe configurar para hacer uso de IKEv2. **Se recomienda seleccionar como protocolo de autenticación MSCHAPv2**.

    c) Perfil VIA de Conexión (*VIA Connection Profile*). Regula cómo se conectan y comportan los usuarios VPN. Se debe configurar para hacer uso de IKEv2.

176. El detalle de configuración de *Virtual Intranet Access* se puede consultar en el apartado Virtual Intranet Access de la guía ArubaOS 8.10.0.0 User Guide – [REF7] y en la guía *Aruba VIA 3.0.0 for Mobility Master* – [REF14].

5.16 CORTAFUEGOS

177. El producto dispone también de la funcionalidad de cortafuegos. Para ello se puede hacer uso de las políticas de cortafuegos o listas de acceso (ACL). Las políticas de cortafuegos permiten tomar distintas acciones para el mismo tipo de tráfico en función del usuario, son bidireccionales, dinámicas y son de tipo *stateful*.

178. Se recomienda crear una ACL de tipo *Service ACL* para permitir el acceso administrativo al producto solo desde redes y direcciones IP autorizadas.

179. **Se recomienda, en todos los casos, denegar implícitamente todo el tráfico, creando las reglas específicas para permitir el tráfico admitido.**

180. El detalle de configuración de la funcionalidad de Cortafuegos se puede consultar en el apartado *Firewall Policies* de la guía *ArubaOS 8.10.0.0 User Guide* – [REF7].

6 FASE DE OPERACIÓN

181. El correcto funcionamiento del producto requiere de unas características que deben estar presentes en el entorno operacional:

a) El producto **debe contar con las últimas actualizaciones de seguridad** para preservar al mismo de amenazas y vulnerabilidades conocidas. En el portal de soporte de Aruba, *Aruba Support Portal (https://asp.arubanetworks.com/)* se dispone la sección de *Software & Downloads* que permite la descarga de las versiones de *software*, parches y documentación. También es relevante la sección de *Notifications* donde se recogen todas las vulnerabilidades y notificaciones. Se recomienda la subscripción activa para recibir notificaciones vía correo electrónico.

b) Se deben **mantener y analizar los registros de auditoría**. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.

c) Se deben **gestionar correctamente los certificados** utilizados, actualizándolos cuando sea necesario, por ejemplo, al expirar.

d) Se deben realizar **copias periódicas de seguridad de los logs y de las configuraciones de los dispositivos.**

7 CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la integridad del paquete	☐	☐	
Registro de licencias	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Activación del modo seguro	☐	☐	
SERVIDORES DE AUTENTICACIÓN			
Configuración de servidores de autenticación	☐	☐	
ADMINISTRACIÓN DEL PRODUCTO			
Configuración de la política de contraseñas	☐	☐	
Configuración del mensaje de acceso	☐	☐	
Configuración de los parámetros de sesión	☐	☐	
Creación de usuarios y configuración de los administradores	☐	☐	
CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS			
Configuración de la protección del Puerto de Consola	☐	☐	
CONFIGURACIÓN DE PROTOCOLOS SEGUROS			
Configuración/Verificación de los parámetros de cada protocolo	☐	☐	
GESTIÓN DE CERTIFICADOS			
Importar CA, crear CSR e importar el certificado de servidor	☐	☐	
SINCRONIZACIÓN HORARIA			
Configuración de la sincronización de la hora de los sistemas	☐	☐	
SINCORNIZACIÓN			
Configuración de un servidor de hora NTP	☐	☐	
COPIAS DE SEGURIDAD			

ACCIONES	SÍ	NO	OBSERVACIONES
Creación de los backups	☐	☐	
AUDITORÍA			
Configuración del envío de los logs a un servidor *Syslog*	☐	☐	
OPERACIÓN			
Actualización del producto	☐	☐	
mantener y analizar los registros de auditoría	☐	☐	
Gestión de los certificados	☐	☐	
Realización de copias de seguridad de logs y de la configuración	☐	☐	

8 REFERENCIAS

[REF1] *Aruba Support Portal*
https://asp.arubanetworks.com

[REF2] *ArubaOS 8.10.0.0 Virtual Appliance Installation Guide*
https://www.arubanetworks.com/techdocs/ArubaOS-8.x-Books/810/ArubaOS-8.10.0.0-Virtual-Appliance-Installation-Guide.pdf

[REF3] Understanding Global Firewall Parameters
https://www.arubanetworks.com/techdocs/ArubaOS_8.10.0_Web_Help/Content/arubaos-solutions/roles-policies/glob-fire-para.htm

[REF4] Wireless Intrusion Prevention
https://www.arubanetworks.com/techdocs/ArubaOS_8.10.0_Web_Help/Content/arubaos-solutions/wireless-intrus-prev/wip.htm

[REF5] *Mobility Master Software Licenses*
https://www.arubanetworks.com/techdocs/ArubaOS_8.10.0_Web_Help/Content/licenseguide/gs-aoslc1.htm

[REF6] *Getting Started Guide*
https://www.arubanetworks.com/techdocs/ArubaOS_8.10.0_Web_Help/Content/gsg/install-mm-md.htm

[REF7] *ArubaOS 8.10.0.0 User Guide*
https://www.arubanetworks.com/techdocs/ArubaOS-8.x-Books/810/ArubaOS-8.10.0.0-User-Guide.pdf

[REF8] *ArubaOS 8. 10 - AP and User Redundancy Methods*
https://www.arubanetworks.com/techdocs/ArubaOS_8.10.0_Web_Help/Content/arubaos-solutions/vrrp/ap-user-redu-meth.htm

[REF9] *Syslog Message Guide*
https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-c05321932

[REF10] *Firewall Policies*
https://www.arubanetworks.com/techdocs/ArubaOS_8.10.0_Web_Help/Content/arubaos-solutions/roles-policies/conf-fire-poli.htm

[REF11] *Web Content*
https://www.arubanetworks.com/techdocs/ArubaOS_8.10.0_Web_Help/Content/arubaos-solutions/dashboard-monitoring/webc.htm

[REF12] *WPA3*
https://www.arubanetworks.com/assets/wp/WP_WPA3-Enhanced-Open.pdf
https://www.arubanetworks.com/techdocs/ArubaOS_8.10.0_Web_Help/Content/arubaos-solutions/802-1x/wpa3-supp.htm

[REF13] *Creating a user role*
https://www.arubanetworks.com/techdocs/ArubaOS_8.10.0_Web_Help/Content/arubaos-solutions/roles-policies/user-role.htm

[REF14] *Aruba VIA 3.0.0 for Mobility Master*
https://support.hpe.com/hpesc/public/docDisplay?docId=a00107894en_us

9 ABREVIATURAS

AES *Advanced Encryption Standard*

AP Punto de Acceso

CBC *Cipher Block Chaining*

CLI Interfaz de Linea de comandos (*Command Line Interface*)

CPD Centro de Procesado de Datos

CTR *Counter Mode*

DHCP *Dynamic Host Configuration Protocol*

DHE *Diffie-Hellman*

DMZ *Demilitarized Zone*

DNS *Domain Name System*

EAP *Extensible Authentication Protocol*

ECDHE *Elliptic Curve Diffie-Hellman Ephemeral*

ECDSA *Elliptic Curve Digital Signature Algorithm*

ENS Esquema Nacional de Seguridad

FIPS *Federal Information Processing Standard*

FQDN *Fully Qualified Domain Name*

FTP *File Transfer Protocol*

GCM *Galois/Counter Mode*

GUI Interfaz gráfico de usuario (*Graphic User Interface*)

HMAC *Hash-based Message Authentication Code*

HTTPS *HyperText Transfer Protocol Secure*

IKE *Internet Key Exchange*

IPsec *IP Security*

LAN *Local Area Network*

LDAP *Lightweight Directory Access Protocol*

MAC *Media Access Control*

MC *Mobility Controller*

MCr *Mobility Conductor*

MD *Managed Device*

MM *Mobility Master*

NTLM *Windows New Technology LAN Manager*

NTP *Network Time Protocol*

OOB *Out Of Band*

PRF *Pseudo Random Functions*

RADIUS *Remote Authentication Dial-In User Service*

RAP *Remote Access Point*

RFC *Request for Comments*

ROM *Read-Only Memory*

RSA *Rivest–Shamir–Adleman*

SCP *Secure Copy Protocol*

SHA *Secure Hash Algorithm*

SNMP *Simple Network Management Protocol*

SSH *Secure SHell*

SSID *Service Set Identifier*

TACACS *Terminal Access Controller Access-Control System*

TFTP *Trivial File Transfer Protocol*

TKIP *Temporal Key Integrity Protocol*

TLS *Transport Layer Security*

TPM *Trusted Platform Module*

USB *Universal Serial Bus*

VIA *Virtual Intranet Access*

VLAN	*Virtual Local Area Network*
VPN	*Virtual Private Network*
VPNC	*VPN Concentrator*
VRRP	*Virtual Router Redundancy Protocol*
WIDS	*Wireless Intrussion Detection System*
WIP	*Wireless Intrussion Protection*
WIPS	*Wireless Intrussion Protection System*
WPA	*Wi-Fi Protected Access*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL