centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1417

Procedimiento de Empleo Seguro de Pulse Connect Secure v9.1

Marzo 2021

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.03.30 17:22:29 +02'00'

NIPO: 083-21-078-4

Fecha de Edición: marzo de 2021
Pulse Secure ha participado en la realización y modificación del presente documento

ÍNDICE

1. INTRODUCCIÓN

1. Pulse Connect Secure (PCS) es la solución de VPN SSL de Pulse Secure que puede proveer tanto servicios a usuarios para conexiones remotas corporativas (VPN SSL) como servicios de iDP a aplicativos cloud a través de SAML 2.0.

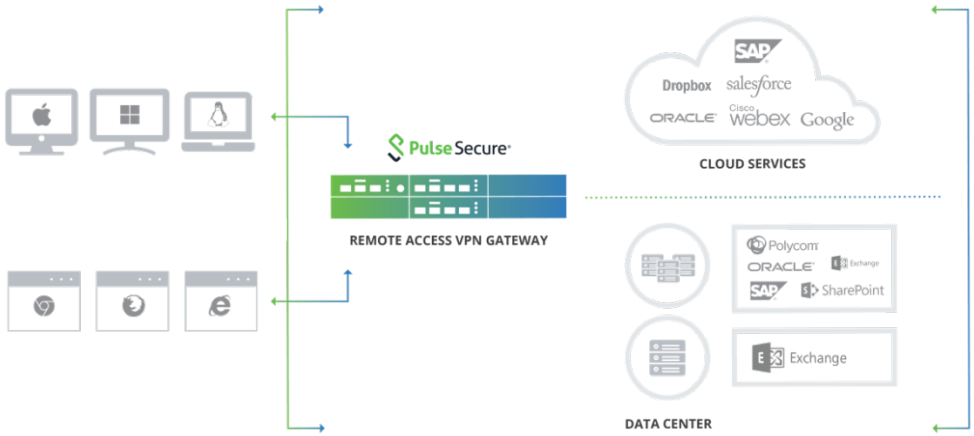

Ilustración 1-1. Esquema estructura PCS.

2. La solución es la evolución de las soluciones SSL VPN comprendidas dentro de los Porfolios de Neoteris (2000), luego Netscreen (2003) y finalmente Juniper (2004). En 2014 se fundó la empresa Pulse Secure (2014) heredando la tecnología y evolucionando la solución al estado actual, y que es el objeto de esta documentación.

2. OBJETO Y ALCANCE

3. El objeto del siguiente documento es servir como guía de buenas prácticas de seguridad en la instalación y configuración de la solución Pulse Connect Secure v9.1R1 de Pulse Secure. No tiene la intención de entrar en detalle en la propia configuración del entorno, pero si en los parámetros de seguridad recomendados.
4. Para más información y detalle en la instalación, despliegue y configuración propiamente dicha se recomienda verificar la documentación online para PCS[1].
5. En la presente guía se hace referencia a la solución PCS en la versión v9.1R1 tanto en las versiones de HW como en las versiones virtuales & Cloud para los entornos VMWare, Hyper-V, KVM.

	Gama 300	Gama 3000	Gama 5000	Gama 7000
Hardware	PSA-300	PSA-3000	PSA-5000	PSA-7000 C/F
Virtual	No aplica	PSA-3000-V	PSA-5000-V	PSA-7000-V
Cloud	No aplica	PSA-3000-V	PSA-5000-V	PSA-7000-V

[1] https://www.pulsesecure.net/

3. ORGANIZACIÓN DEL DOCUMENTO

6. El presente documento se divide en los siguientes apartados que, fundamentalmente, servirá de guía en la configuración segura de la solución de Pulse Secure:

    - Apartado 4. En este apartado se recogen tanto recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto como aspectos relativos a la seguridad del mismo proceso.
    - Apartado 5. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
    - Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de operación del producto, para lograr un funcionamiento en el día a día de forma segura.
    - Apartado 7. En este apartado aparece un Checklist con las tareas a realizar y el estado de cada una de ellas.
    - Apartado 8. Referencias utilizadas en el presente documento.
    - Apartado 9. En el último apartado se hace referencia a las diferentes nomenclaturas utilizadas.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

7. En el siguiente apartado se darán algunas indicaciones tanto para la recepción segura de los dispositivos PSA en formato Hardware como en formato Virtual.

   a) Recepción en formato Hardware:

      a. Información de envío. Es necesario verificar los datos de envío, comprobando si estos concuerdan con los datos corporativos de Pulse Secure. Asimismo, se debe verificar que el número de serie (*Serial Number*) que se encuentra en el exterior de la caja se corresponde con el indicado en la documentación obtenida en el proceso de compra de las soluciones.

      b. Embalaje externo. El embalaje externo será una caja con el logotipo de Pulse Secure y deberá estar debidamente embalada sin tener signos de haber sido manipulado.

      c. Embalaje interno. El *appliance* estará embalado en una "bolsa" de plástico, inmovilizado con protectores adicionales. Se deberán inspeccionar estos elementos para verificar que no ha habido manipulación en los mismos.

      d. Dentro de la caja se encontrarán las instrucciones iniciales para la puesta en marcha de la máquina, así como para la creación inicial de la cuenta de administrador, la cual no existe por defecto y es creada en el inicio del proceso.

      e. La documentación también estará disponible de manera on-line en formato electrónico[2], en el que aparecerá la información específica de cada modelo.

      f. En caso de detectar alguna anomalía o ante cualquier duda, póngase en contacto de inmediato con el equipo de Pulse Secure para verificar los siguientes pasos a seguir.

   b) Recepción en formato Virtual:

      a. En el caso de haber adquirido una subscripción para una máquina virtual es preciso que el usuario cree una cuenta en el portal de soporte[3], para así poder tener acceso y poder proceder a la descarga de los paquetes de software e información correspondientes (ver apartado 4.3-REGISTRO Y LICENCIAS).

      b. Una vez creada la cuenta de usuario, es preciso asociarla a la cuenta corporativa de la organización que haya adquirido el Servidor en versión

[2] https://www-prev.pulsesecure.net/techpubs/pulse-appliances/psa
[3] https://my.pulsesecure.net

Software (VMWare, Hyper-V, KVM, Azure, AWS, Alibaba). Existen detalles adicionales sobre el proceso en el apartado 4.3-REGISTRO Y LICENCIAS de este documento.

c. Se descargará el paquete de software correspondiente desde el portal de soporte en el apartado *"Download"*, siguiendo los pasos incluidos en el siguiente documento:

- KB40028 - [Customer Support Tools] How to download software / firmware for Pulse Secure products using the Licensing & Download Center at my.pulsesecure.net https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40028

d. En la propia área de descarga se pueden extraer las firmas MD5 y SHA2 para su verificación después de la descarga. De esta forma se puede verificar la autenticidad e integridad del fichero descargado.

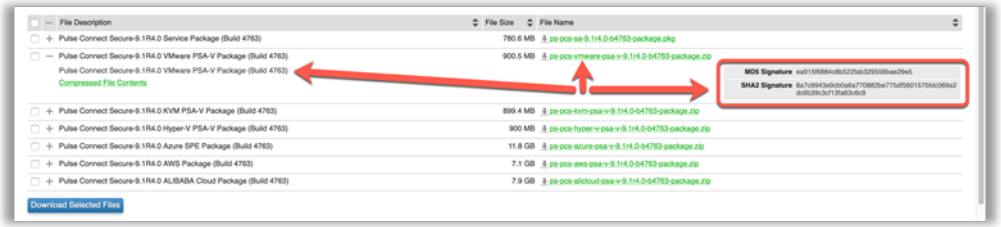

Ilustración 4-1. Hashes de verificación del software.

4.2 ENTORNO DE INSTALACIÓN SEGURO

8. PCS en el lado del servidor actuará a modo de terminador de túneles para los accesos remotos corporativos, se encargará del cumplimiento de las políticas de seguridad para el acceso remoto de los usuarios y verificará el cumplimiento de las normativas de seguridad aplicadas.

9. PCS se debe desplegar en un entorno físico protegido, donde sólo pueda acceder el personal expresamente autorizado por la organización y que disponga de medidas de seguridad adecuadas.

4.3 REGISTRO Y LICENCIAS

10. Desde el portal de Soporte de Pulse Secure es posible tener acceso al inventario para gestionar los productos y las licencias.

11. Se deberá crear una cuenta de usuario, la cual se debe asociar a la cuenta corporativa de la organización que haya adquirido las soluciones de Pulse Secure.

12. Los pasos a seguir para la creación de la cuenta de usuario y su asociación con la cuenta corporativa se pueden consultar en los siguientes documentos:

a) KB40050 – Onboarding FAQ
https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40050

b) KB40031 – [Customer Support Tools] Onboarding my.pulsesecure.net
https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40031

c) KB40565 – What is Right To Use (RTU) and Service Contract certificate
https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40565

13. Una vez creada y vinculada la cuenta de usuario, se procederá a la obtención y aplicación de las licencias de uso. Para la obtención de las licencias del producto, seguir los pasos indicados en el siguiente enlace: Obtención de Licencias.

14. Para aplicar las licencias al producto, seguir los siguientes pasos:

- Ir a la pestaña *System > Configuration > Licensing*.
- En el cuadro *Licensing* introducir la licencia obtenida y hacer clic en *Add*.

4.4 CONSIDERACIONES PREVIAS

4.4.1 ARQUITECTURA

15. Generalmente, los equipos de Pulse Secure (PSA-3000/5000/7000) se despliegan con tres interfaces principales de red:

a) EXTERNO (DMZ)

b) INTERNO

c) GESTIÓN

16. A continuación, se muestra un esquema básico con los principales flujos de comunicación para un despliegue con tres interfaces.

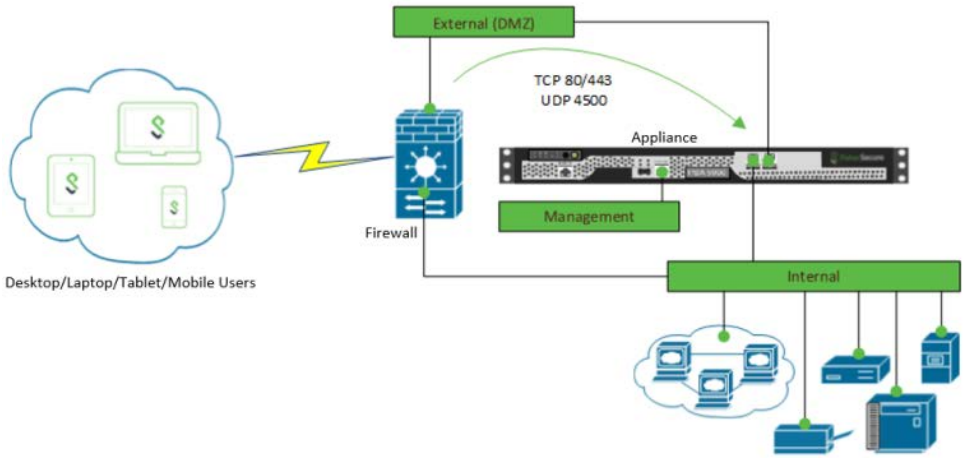

Ilustración 4-2. Esquema flujos de comunicación.

17. En la máquina con denominación PSA-300, dimensionada para pequeñas organizaciones, el despliegue está basado en únicamente 2 interfaces.

a) EXTERNO (DMZ)

b) INTERNO (la gestión se llevará por esta misma interfaz).

18. En el caso de publicar el servicio a internet será preciso que:

a) El dominio público elegido apunte al interfaz externo, como puede se puede ver a modo de ejemplo en: *https://vpn.micompania.es*

b) La comunicación desde el *Firewall* externo al puerto externo del servidor PCS se realizará a través de los siguiente puertos:

   a. (80)/443 TCP

   b. 4500 UDP

4.4.2 DESPLIEGUE EN ALTA DISPONIBILIDAD

19. Management Framework de Pulse Secure ofrece dos posibilidades de despliegue en alta disponibilidad.

    a) Clúster de balanceo de carga, o clúster en Activo / Activo (A/A). Siendo el estándar de dos nodos, pero existiendo la posibilidad de extender hasta 4x nodos en un clúster de máquinas de la gama PSA-7000.

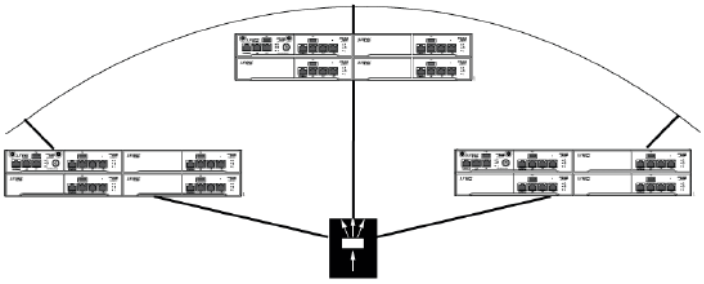

Ilustración 4-3. Clúster de balanceo de carga.

    b) Clúster en modo fail over o clúster Activo / Pasivo (A/P)

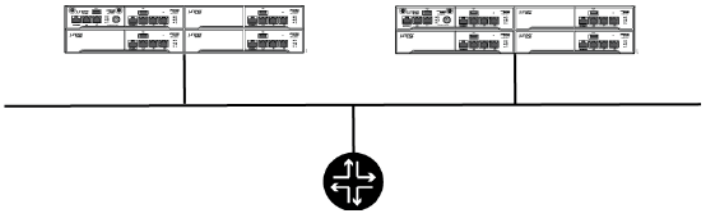

Ilustración 4-4. Clúster en modo Failover.

20. En el apartado 5.10 ALTA DISPONIBILIDAD, de este documento, se detalla el despliegue de Alta disponibilidad del producto.

4.4.3 PREPARACIÓN DE DESPLIEGUE

21. Para la preparación de un despliegue inicial, es importante conocer con antelación los siguientes puntos para desplegar la solución de una forma más eficiente y poder crear las políticas de acceso a recursos ajustadas a las necesidades de la organización:

    a) Que grupo de personas accederán (personal interno/externo, proveedores, etc.).

b) A través de que formas de autenticación (LDAP, AD, RADIUS, etc.).

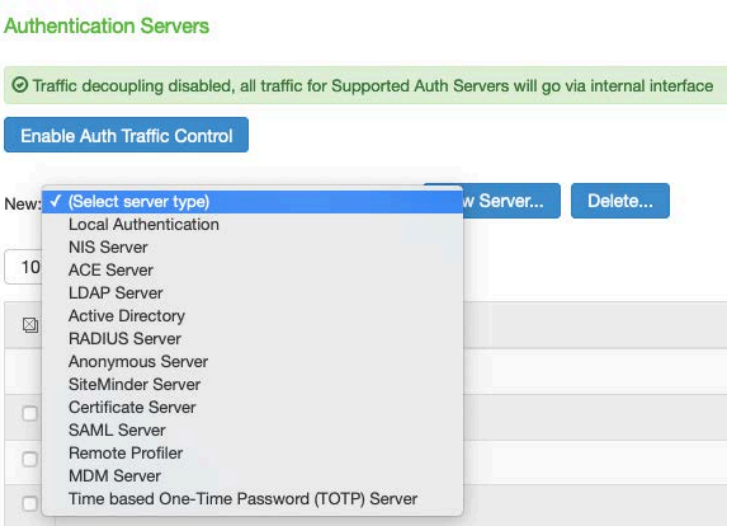

Ilustración 4-5. Servidores de autenticación.

c) A qué recursos:

   a. Conectividad vía capa 3 (L3),

   b. capa 4 (L4),

   c. o a través de un portal Web al estilo quiosco (L7)

4.4.4 CERTIFICADOS

22. Existen varios tipos de Certificados a tener en cuenta para una correcta configuración del entorno:

    a) Certificados de dispositivo: ayudan a proteger el tráfico de red hacia y desde el servicio del cliente Pulse Secure utilizando elementos como el nombre de la empresa, una copia de la clave pública de su empresa, la firma digital de la CA que emitió el certificado, un número de serie y fecha de caducidad. Además, Policy Secure utiliza un certificado de dispositivo para las comunicaciones con ScreenOS Enforcer y Pulse Policy Secure.

    b) CA de cliente de confianza: es un certificado del lado del cliente emitido por una CA. Se pueden usar este tipo de certificados en el ámbito del marco de administración de acceso y configuraciones de roles y requerir certificados con atributos específicos. Por ejemplo, puede especificar que los usuarios deben presentar un certificado válido del lado del cliente con el atributo OU establecido en "yourcompany.com" para iniciar sesión en el dominio de autenticación de Usuarios.

    c) CA de servidor de confianza: es el certificado de un servidor web en el que se confía. Este tipo de certificado se utiliza para validar las credenciales de los sitios web a los que acceden los usuarios a través del servicio de cliente Pulse Secure.

d) Certificados de firma de código solo para Connect Secure: un certificado de firma de código es un tipo de certificado del lado del servidor que vuelve a firmar los *applets* de Java que son intermediados por Connect Secure. Puede usar el certificado de firma de código autofirmado que viene precargado, o puede instalar su propio certificado de firma de código.

e) Certificados de autenticación del cliente solo conexión segura: en este contexto, el certificado de autenticación del cliente se utiliza cuando los servidores SSL en el *Datacenter* requieren que Connect Secure presente un certificado de cliente.

23. En el apartado 5.6 GESTIÓN DE CERTIFICADOS, de este documento, se detalla la configuración de los certificados mencionados.

4.4.5 AUTENTICACIÓN MULTIFACTOR

24. La solución tiene la capacidad de utilizar un segundo factor de autenticación para acceder a los recursos. Los métodos que soporta s son los siguientes:

    a) Time One Time Passwod (TOTP), que permite la integración a gran parte de los tokens software disponibles tanto para Android como para Apple. A modo de ejemplo: Google Authenticator, Microsoft Authenticator, LastPass, DUO, FortiToken, Free TOTP (RedHat), etc.

    b) RADIUS, que permite la integración con soluciones corporativas de terceros como pueden ser: Symantec, SWIVEL, DUO, o desarrollos propios.

    c) SAML, soportada la integración con Microsoft AZURE AD.

25. En el apartado 5.5.4 SEGURIDAD DE AUTENTICACIÓN, de este documento, se detalla la configuración de los métodos de autenticación multi factor disponibles.

4.4.6 SSO PARA EL ACCESO A RECURSOS

26. La solución permite integración de SSO (Single Sign On) hacia los diferentes recursos y soporta los siguientes:

    a) Basic Auth

    b) NTLM

    c) Kerberos

    d) Form Post

    e) Headers/Cookies

    f) SAML

    g) SAML external Apps

27. Es preciso que la organización determine cómo realizar la integración de SSO en el producto.

4.5 INSTALACIÓN

28. La solución se basa en dos componentes:
    - Servidor
    - Cliente (PDC = Pulse Desktop Client, que puede ser tanto cliente para la solución de VPN como de NAC)
29. Previo al despliegue del cliente es recomendable desplegar un programa de ayuda denominado "Pulse Secure Installer Service" para evitar problemas de instalación por derechos de usuario en el momento del despliegue inicial del cliente vía Web. Dicho programa se puede obtener desde la pestaña de *Maintenance > System > Installers*.
30. En el caso del cliente, se recomienda su despliegue a través de medios corporativos (Microsoft SCCM o similares) para, una vez finalizadas las tareas de configuración, que el cliente pueda incluir las configuraciones pertinentes.
31. Para la parte del servidor, existen dos procedimientos a seguir dependiendo de si la plataforma se realiza sobre equipamiento físico (Hardware) o en modo Virtual (VMWare, KVM, Hyper-V, AWS o Azure)

    a) Despliegue en formato físico

        a. Las siguientes guías describen con exactitud los pasos del despliegue inicial del Hardware según el modelo del producto:

            i. Hardware Guide PSA-3000

            ii. Hardware Guide PSA-5000

            iii. Hardware Guide PSA-7000

        b. La configuración inicial deberá realizarse a través de la consola. Tras arrancar un dispositivo no configurado, se inicia el proceso de configuración inicial básico.

        c. Primero deberá introducirse la "personalidad" del dispositivo (características iniciales), mediante consola el dispositivo solicitará elegir el *preset* de "personalidad" del dispositivo, seleccionando entre las distintas opciones disponibles. Se debe seleccionar la opción *Pulse Connect Secure*.

        d. Tras esto, seguir las instrucciones mostradas en la consola para introducir la información básica del dispositivo. Para ello es necesario disponer de los siguientes datos:

            i. IP del puerto INTERNO del dispositivo (el puerto externo se puede configurar a posteriori a través del interfaz de usuario del administrador)

            ii. Mascara de red puerto INTERNO

            iii. Default GW puerto INTERNO

iv. DNS primario / secundario

v. Nombre de usuario Administrador a generar durante el primer Boot

vi. Password para el Administrador principal. A posteriori se podrán generar Administradores adicionales a través de la consola de gestión del Administrador.

vii. Nombre de maquina

viii. Nombre de la organización

b) Despliegue en formato virtual local

   a. Para los detalles del despliegue de la solución en formato virtual se recomienda la lectura de la documentación correspondiente:

      PCS & PPS Virtual Deployment Guide

c) Despliegue en formato Cloud (AZURE / AWS)

   a. Azure. Para los detalles del despliegue de la solución en formato virtual se recomienda la lectura de la documentación correspondiente:

      PCS MS Azure Virtual Deployment Guide.

   b. AWS. Para los detalles del despliegue de la solución en formato virtual se recomienda la lectura de la documentación correspondiente:

      PCS Amazon Web Services Virtual Deployment Guide

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO – FIPS NIVEL 1

32. La solución de PCS de Pulse Secure cumple la normativa de FIPS Nivel 1 como se indica en la documentación del producto, en el siguiente enlace.

33. Se debe habilitar la compatibilidad con FIPS Nivel 1. Una vez habilitada, su navegador estará restringido al cifrado personalizado específico. Se mostrará una lista de cifrados compatibles durante el proceso de habilitación.

34. Durante la configuración del modo de operación seguro, se pueden producir los siguientes eventos en el sistema:

    - SYS30966 cuando el servidor web activa el soporte FIPS nivel 1.
    - ADM30965 cuando el administrador activa o desactiva el soporte de nivel 1 de FIPS.
    - ERR30967 cuando el servidor web no puede activar el soporte FIPS nivel 1.

35. Durante la activación del modo seguro, el servidor web se reinicia y permite solo el uso de los protocolos configurados, tal como se verá a continuación. **Se recomienda exclusivamente el uso de TLSv1.2** o protocolos superiores.

36. Una vez que el soporte FIPS nivel 1 está habilitado, las nuevas sesiones de cliente usarán FIPS si el cliente lo admite. Es posible que las sesiones de cliente existentes no usen FIPS por lo que, para garantizar su uso, todas las sesiones de cliente deben finalizar después de habilitar el modo seguro. Un usuario administrador puede forzar la finalización de las sesiones de cliente desde la página *Sistema > Estado > Usuarios activos*.

37. Para habilitar el modo seguro, seguir los siguientes pasos:

    - Ir a *Sistema > Configuración > Seguridad > Opciones de SSL entrante*.
    - En la opción *Modo FIPS SSL*, seleccionar *Activar modo FIPS.*
    - Una vez activado el soporte FIPS nivel 1, realizar los siguientes cambios:
        - Bajo *SSL permitido y versión TLS*, seleccionar la opción ***Aceptar solo TLS 1.2 o posterior***.
        - En *Fuerza de cifrado permitida*, se establecen los Cifrados de compatibilidad máxima. Se recomienda seleccionar la opción *Perfect Forward Secrecy* o *Ephemeral Diffie Hellman (ECDHE)*.
        - En *Fuerza de cifrado*, se selecciona la opción *No permitir conexiones desde navegadores que solo aceptan cifrados más débiles*. No se puede deshabilitar esta selección.
    - Guardar los cambios.

- Se mostrarán entradas en los registros de eventos y en los registros de acceso de administrador para mostrar que el soporte de nivel 1 de FIPS está habilitado.

38. El detalle de la configuración del soporte FIPS Nivel 1, se puede encontrar en el siguiente enlace.

5.2 AUTENTICACIÓN

5.2.1 AUTENTICACIÓN REMOTA

39. En el framework de administración de acceso de Pulse Secure, la página de inicio de sesión, el *REALM* (forma de autenticación) y las configuraciones de servidor AAA están asociadas. Determinan el acceso del usuario y la función del usuario. Un usuario envía credenciales a través de una página de inicio de sesión, que especifica un *REALM*, que está asociado con un servidor AAA.

40. Si la solicitud de acceso cumple con la política de autenticación del *REALM*, el sistema reenvía las credenciales del usuario al servidor de autenticación asociado. El trabajo del servidor de autenticación es verificar la identidad del usuario. Después de verificar al usuario, el servidor de autenticación envía la aprobación. Si el *REALM* también usa el servidor como un servidor de directorio/atributo, el servidor AAA envía la información del grupo del usuario u otra información de atributo del usuario. El framework de administración de acceso luego evalúa las reglas de asignación de roles del *REALM* para determinar los ROLES de usuario que se aplican a la sesión.

41. Un *REALM* (dominio) de autenticación especifica las condiciones que los usuarios deben cumplir para iniciar sesión en el sistema. Un *REALM* consta de una agrupación de recursos de autenticación, que incluyen:

    a) Un servidor de autenticación: verifica que el usuario sea quien dice ser. El sistema reenvía las credenciales que envía un usuario en una página de inicio de sesión a un servidor de autenticación.

    b) Un servidor de directorio: un servidor LDAP que proporciona información de usuarios y grupos al sistema que el sistema utiliza para asignar usuarios a uno o más roles de usuario.

    c) Una política de autenticación: especifica los requisitos de seguridad del *REALM* que deben cumplirse antes de que el sistema envíe las credenciales de un usuario a un servidor de autenticación para su verificación.

    d) Reglas de asignación de funciones: condiciones que debe cumplir un usuario para que el sistema asigne al usuario una o más funciones de usuario. Estas condiciones se basan en la información del usuario devuelta por el servidor del directorio del *REALM* o en el nombre de usuario del usuario.

42. La configuración de REALMS se puede consultar en los apartados 5.3.2.4 CONFIGURACIÓN DE *REALM* PARA ADMINISTRADORES y 5.3.3.5 CONFIGURACIÓN DE *REALM* de este documento.

43. Para la creación de un nuevo servidor de autenticación remoto, ir a *Authentication > Auth. Servers* y seleccionar el tipo de servidor deseado. Después hacer clic en *New Server* e introducir la información requerida. El Framework de gestión de acceso Pulse Secure admite los siguientes tipos de servidores AAA:

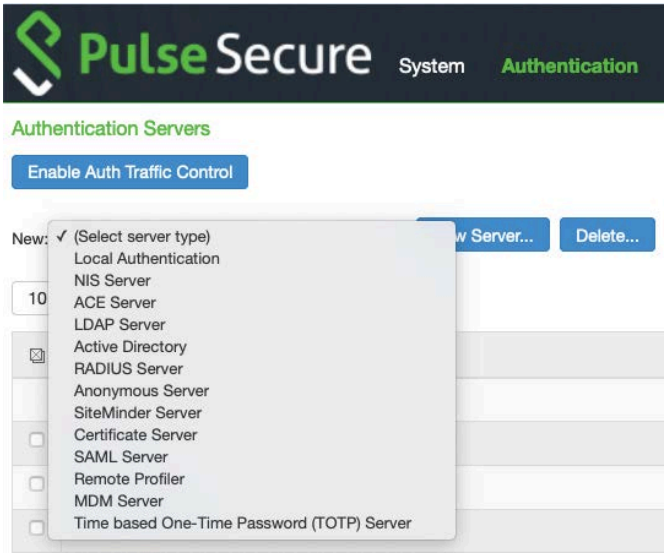

Ilustración 5-1. Servidores de autenticación disponibles.

a) Local: se pueden crear bases de datos locales de propósito especial para crear manualmente cuentas de usuario, administrar el acceso de usuarios invitados, permitir el acceso anónimo o administrar el acceso basado en certificados digitales o direcciones MAC.

b) Externo (basado en estándares): se pueden integrar servidores LDAP y RADIUS basados en estándares con el framework de administración de acceso. Además de usar el servidor de fondo para la autenticación, puede usar el grupo LDAP y la información de atributos RADIUS en las reglas de asignación de roles.

c) Externo (otro): se pueden integrar versiones compatibles de servidores AAA de terceros con el marco de administración de acceso. Además de usar el servidor de fondo para la autenticación, puede usar la información del grupo de Active Directory y los atributos de SiteMinder en las reglas de asignación de roles. Además, puede usar los atributos del dispositivo MDM en las reglas de asignación de roles.

44. La información detallada sobre los diferentes servidores de autenticación disponibles en el producto se puede consultar en el siguiente enlace.

45. Además de utilizar servidores de autenticación para controlar el acceso a Pulse Connect Secure, puede controlar el acceso al PCS y los recursos que gestiona mediante una variedad de comprobaciones adicionales del lado del cliente. Pulse

Connect Secure le permite crear un enfoque multicapa para protegerse a sí mismo y a sus recursos haciendo lo siguiente:

- Como primer paso, realizar verificaciones previas a la autenticación que controle el acceso del usuario a la página de inicio de sesión de PCS. Por ejemplo, se puede configurar el PCS para verificar si el ordenador del usuario ejecuta o no una versión particular de Antivirus. En caso de que no se esté ejecutando, se puede determinar que el dispositivo del usuario no es seguro y deshabilitar el acceso a la página de inicio de sesión de PCS hasta que el usuario haya actualizado el software antivirus de la máquina. Para más detalle en este punto, ver el apartado 5.5.5 SEGURIDAD DEL ENDPOINT de este documento en el que se describen las funcionalidades y configuraciones de Host Checker.
- Una vez que el usuario ha accedido con éxito a la página de inicio de sesión de PCS, se realizan verificaciones a nivel de dominio para determinar si se accede a la página de inicio del usuario final de PCS. La verificación de nivel de dominio más común la realiza un servidor de autenticación. El servidor determina si el usuario ingresa un nombre de usuario y contraseña válidos.
- Si el usuario no supera las comprobaciones de nivel de *REALM* que se especifican, no se le permite iniciar sesión o se muestra una versión "limitada" de la página de inicio. En general, esta versión simplificada contiene una funcionalidad significativamente menor que la que está disponible para sus usuarios estándar porque el usuario no ha pasado todos los criterios de autenticación. El PCS proporciona definiciones de políticas extremadamente flexibles, que le permiten alterar dinámicamente el acceso a los recursos del usuario final en función de las políticas de seguridad corporativas. Ver apartado 5.3.3.5 CONFIGURACIÓN DE *REALM*.
- Después de que PCS asigna con éxito a un usuario a un *REALM*, el dispositivo asigna al usuario a un ROL(E) según sus criterios de selección. Un ROL(E) específica a qué mecanismos de acceso puede acceder un grupo seleccionado de usuarios. También controla las opciones de sesión y UI para ese grupo de usuarios. Puede usar una amplia variedad de criterios para asignar usuarios a roles. Ver apartado 5.3.3.3 CONFIGURACIÓN DE ROLES.

46. En resumen y de forma gráfica las posibilidades de verificaciones de seguridad que puede aplicarse en la solución PCS:

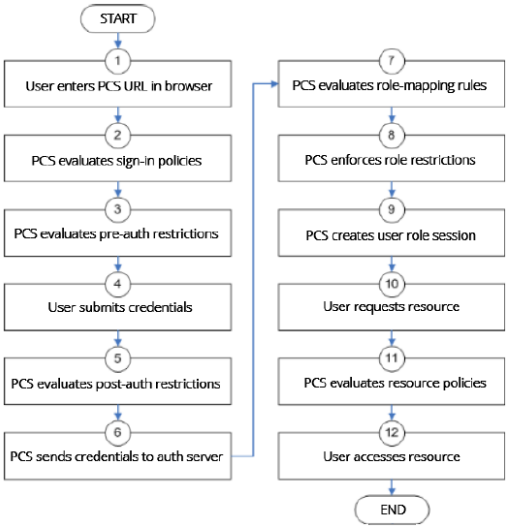

Ilustración 5-2. Verificaciones de seguridad en el acceso.

5.2.2 AUTENTICACIÓN LOCAL

47. Para la autenticación tanto de Administradores como de usuarios comunes, es posible hacer uso del Framework de autenticación de la solución PCS. En el caso de los administradores, la configuración de los mismos está separada para permitir la aplicación de un acceso administrativo granular en formato RBAC (Role Based Access Control). Por otro lado, permite ofrecer la posibilidad de configuración granular de los accesos de administración (Administrador, Operaciones, etc.).

48. La configuración de la autenticación local de usuarios se divide en administradores y usuarios comunes. Los pasos para configurar esta autenticación se describen en los apartados 5.3.2.1 CONFIGURACIÓN DEL SERVIDOR DE AUTENTICACIÓN PARA ADMINISTRADORES LOCALES y 5.3.3.1 CONFIGURACIÓN DEL SERVIDOR DE AUTENTICACIÓN PARA USUARIOS NO ADMINISTRADORES respectivamente.

49. Confianza entre componentes – Certificados. Tal como se ha indicado anteriormente, deben configurarse las CA de confianza en el dispositivo. La descripción detallada tanto de la configuración como de los diferentes elementos, se encuentran en el apartado 5.6 GESTIÓN DE CERTIFICADOS.

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

50. En el momento de la instalación será necesario acceder a la CLI (instalación de HW) o a la consola del entorno virtual para realizar la configuración inicial (ver apartado 4.5 INSTALACIÓN). Para la gestión del día a día ya no se precisa el acceso a la CLI.

51. Una vez realizada la configuración inicial, cualquier cambio de configuración y/o gestión de la solución se hará a través de la consola de administración que es accesible únicamente vía WEB:

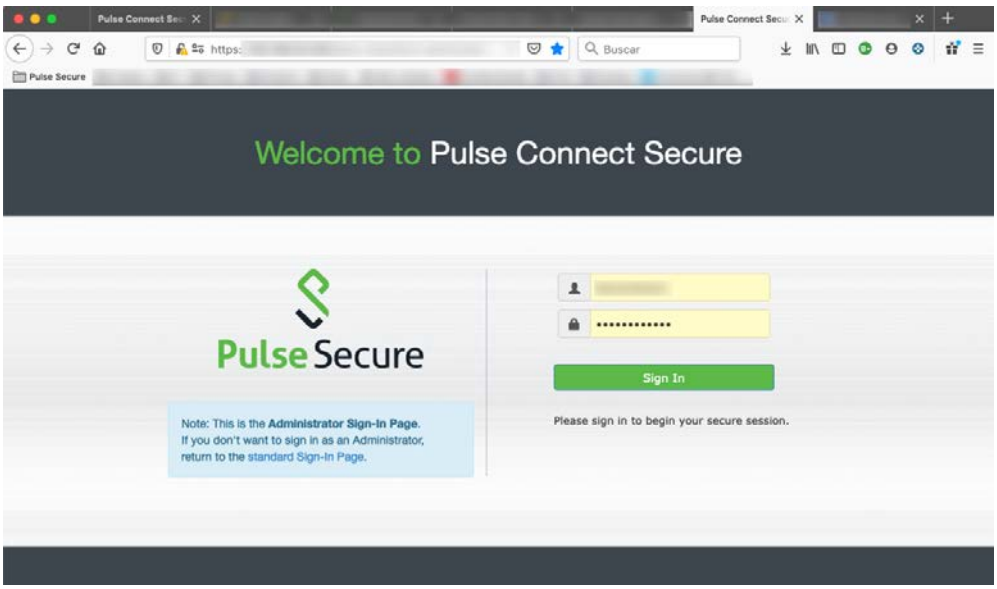

Ilustración 5-3. Consola de gestión Web.

52. Existe la posibilidad de configurar un usuario y password para el CLI (ver apartado 5.5.3 SEGURIDAD DE GESTIÓN DEL DISPOSITIVO), pero es imperativo tener en cuenta que, si se pierde el acceso al CLI y el usuario Administrador inicial, no será posible recuperar los datos dado que:

- Los discos están cifrados.
- La única forma de hacer un reset de la clave del administrador inicial es a través del CLI.
- No se tiene acceso bajo ningún concepto al sistema de ficheros/operativo.

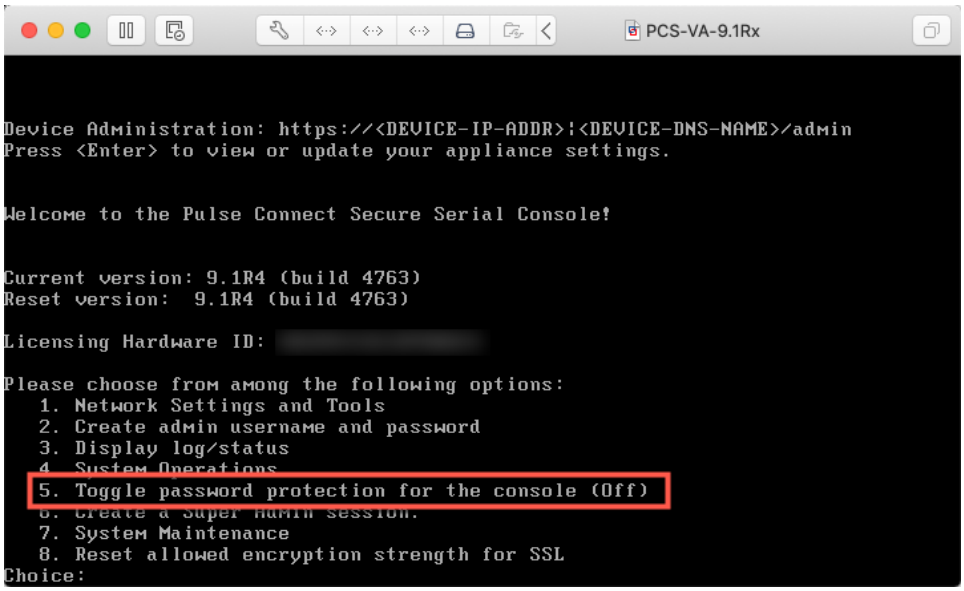

Ilustración 5-4. Configuración de contraseña CLI.

5.3.2 CONFIGURACIÓN DE ADMINISTRADORES

53. El producto tiene la capacidad de permitir tanto a usuarios administradores creados y mantenidos en una base de datos local, como a usuarios corporativos, autenticarse como administrador de la solución a través de alguna solución corporativa como pueden ser: AD, LDAP, RADIUS

5.3.2.1 CONFIGURACIÓN DEL SERVIDOR DE AUTENTICACIÓN PARA ADMINISTRADORES LOCALES

54. Por defecto la solución tiene un servidor de autenticación para administradores locales creado, como los otros elementos explicados en los siguientes puntos, para garantizar el acceso del administrador creado durante la configuración inicial. Aquí es donde se pueden agregar administradores locales adicionales.
55. La configuración del servidor de autenticación local se encuentra bajo siguiente menú dentro de la solución PCS: *Authentication > Auth Servers*.
56. Existe una base de datos de administradores locales que está por defecto y no puede ser borrada. En caso de necesitar crear un servidor de autenticación local adicional, seguir los siguientes pasos:
    - Ir a *Authentication > Auth Servers*, seleccionar *Local Authentication*.
    - Hacer clic en *New Server*.
    - Finalmente completar la información necesaria y guardar la configuración.

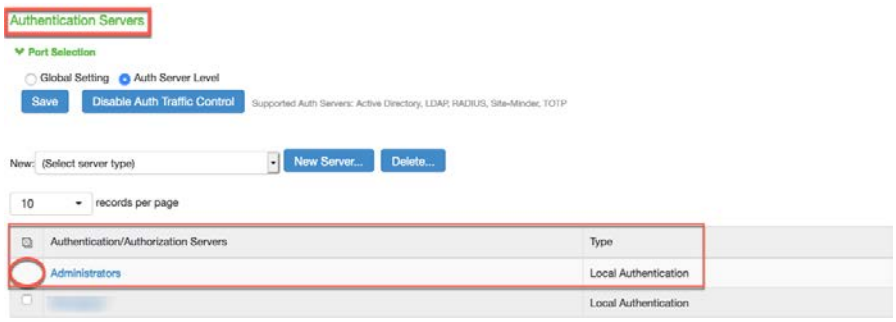

Ilustración 5-5. Servidor de autenticación local pre-configurado.

5.3.2.2 CONFIGURACIÓN DE USUARIOS ADMINISTRADORES

57. Para la creación de usuarios locales en un servidor de autenticación local ya existente, ir a *Authentication > Auth. Server > Servidor de Autenticación local creado > Users.* Hacer clic en *New…* e incluir la información necesaria.

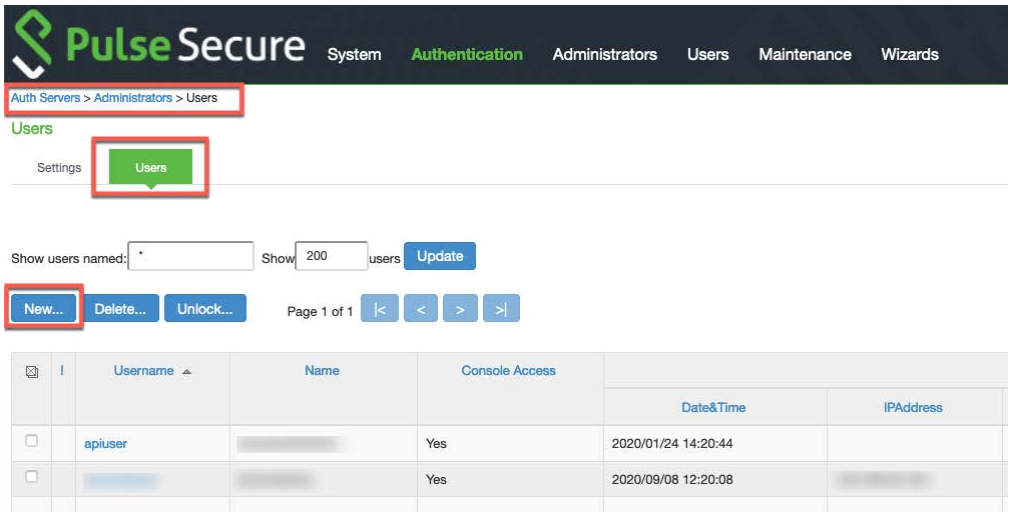

Ilustración 5-6. Creación de usuarios Administradores locales.

58. Para configurar los parámetros de seguridad de las cuentas de usuarios, seguir los siguientes pasos:

- **Complejidad de las contraseñas**. Ir a *Authentication > Auth Server > Administrators > Settings*. Configurar los siguientes parámetros con los valores deseados:
    - Minimum length: longitud mínima de la contraseña, se recomienda configurar al menos 12 caracteres.
    - Minimum digits: número mínimo de dígitos que debe contener. Se recomienda un valor de al menos un dígito.
    - Minimum letters: número mínimo de letras que debe contener. Se recomienda un valor de al menos una letra.
    - Uppercase and lowercase required: Obliga al uso de mayúsculas y minúsculas. Se recomienda activarlo.
    - Different from username: previene el uso del nombre de usuario como parte de la contraseña. Se recomienda activarlo.
    - Different from previous password: previene que la contraseña sea igual a la anterior.
    - Force password change: obliga el cambio de la contraseña tras el número de días configurado. Se recomienda un valor de entre 30 y 90 días.
- Para configurar el bloqueo de cuentas, ir a *Authentication > Auth Server > Administrators > Settings*. Activar "Enable account lockout for users" y configurar "máximum wrong passwords attempts" al valor deseado. Se recomienda un valor de 3 intentos fallidos antes de bloquear la cuenta.
- Se recomienda configurar al menos de un segundo factor (descrita en el apartado 5.5.4 SEGURIDAD DE AUTENTICACIÓN) pudiendo ser estos:

- TOTP (post autenticación del usuario solo).
- RADIUS (pre- y post autenticación del usuario).

59. La configuración de otros parámetros de seguridad de los usuarios se detalla en el apartado 5.5 CONFIGURACIÓN DE SEGURIDAD.

5.3.2.3 CONFIGURACIÓN DE ROLES PARA ADMINISTRADORES

60. En el apartado de ROLES para administradores existen dos ROLES pre-definidos:
    - Administrators: Política general para administradores
    - Read Only Administrators: Política con permisos de solo lectura, sin capacidad de proceder a acometer cambios.

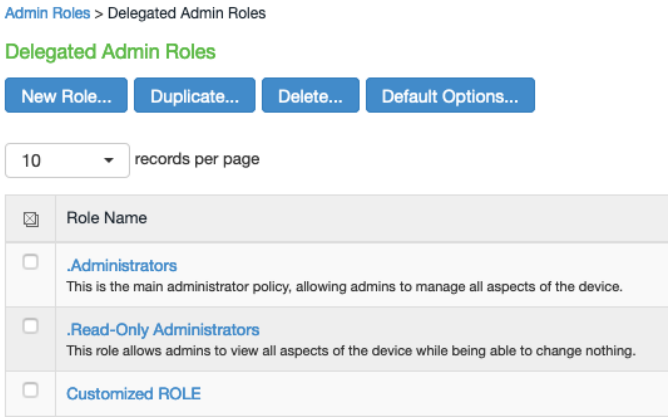

Ilustración 5-7. Roles de administración del producto.

61. Para la creación de ROLES personalizados, seguir los siguientes pasos:
    - Ir a *Administrators > Admin Roles > Delegated Admin Roles*.
    - Hacer clic en *New Role…*
    - Configurar los parámetros deseados y guardar la configuración.
62. Existe también la posibilidad de adaptar los roles existentes modificando sus parámetros, para ello:
    - Ir a *Administrators > Admin Roles > Select Role > System*.
    - Modificar los parámetros deseados:

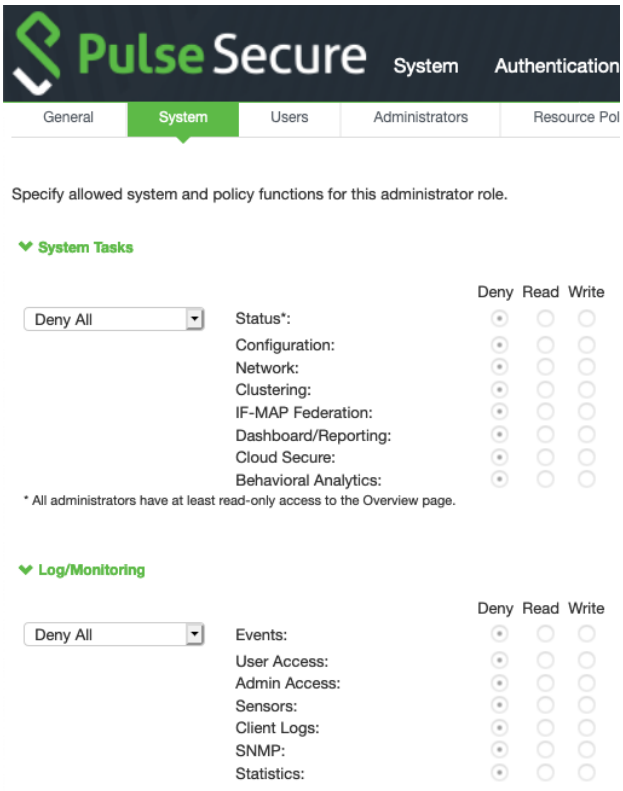

Ilustración 5-8. Modificación de los roles existentes.

5.3.2.4 CONFIGURACIÓN DE *REALM* PARA ADMINISTRADORES

63. En la configuración del *REALM* se configuran tanto las formas de autenticación (local, AD, LDAP, Radius, etc.) como las restricciones de seguridad para el acceso (Pre-autenticación) hacia los recursos, así como el *ROLE mapping*: el mapeo a un ROLE dependiendo de los criterios aplicados. Dichas configuraciones se realizan desde *Administrators > Admin Realm.*

64. Para crear un *REALM*:

    - Ir a *Administrators > Admin Realm* y hacer clic en *New*.
    - Incluir la información solicitada en la página de creación y hacer clic en *Save Changes*.
    - El detalle de la creación de REALMS se puede consultar en el siguiente enlace.

65. Para realizar la configuración del servidor de Autenticación utilizado por el *REALM* de administración, ir a *Administrators > Admin Realm > Admin Users > General* (en la figura de ejemplo se utiliza el servidor pre-configurado). Seleccionar el servidor de autenticación deseado (creado previamente), sea el local o no (RADIUS, LDAP, AD, etc.)

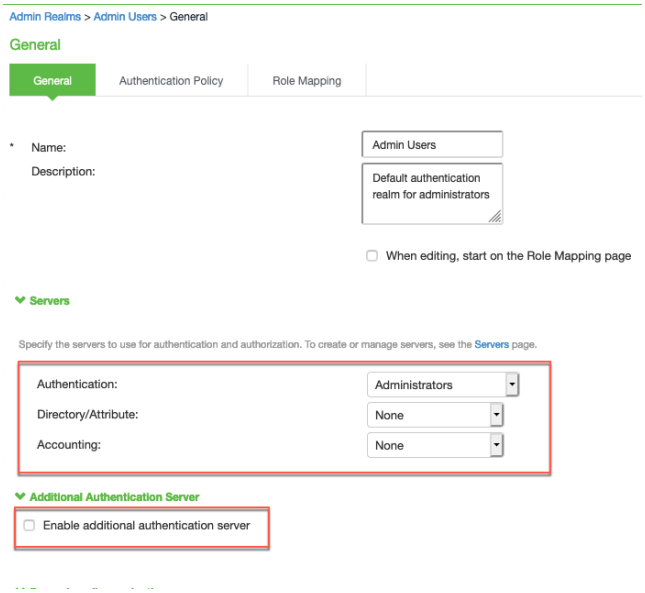

Ilustración 5-9. Configuración del servidor de autenticación.

66. La configuración de los parámetros de seguridad se detalla en el apartado 5.5 CONFIGURACIÓN DE SEGURIDAD.

67. Para configurar las políticas de autenticación de los *REALM*, ir a *Administrators > Admin Realm > Administrators > Authentication Policy*. Configurar los parámetros deseados:

    - *Source IP*: verificación de la IP de origen desde la que se conecta el usuario
    - *Browser*: verificación del navegador web desde el que accede el usuario.
    - *Certificate*: Comprobación de certificado y campos de los mismos
    - *Password:* exigencia de una clave con caracteres mínimos.
    - *HostChecker:* una gran variedad de comprobaciones a nivel de Host para permitir/denegar el acceso
    - *Limit*: limitación de los Admins conectados de forma concurrente.

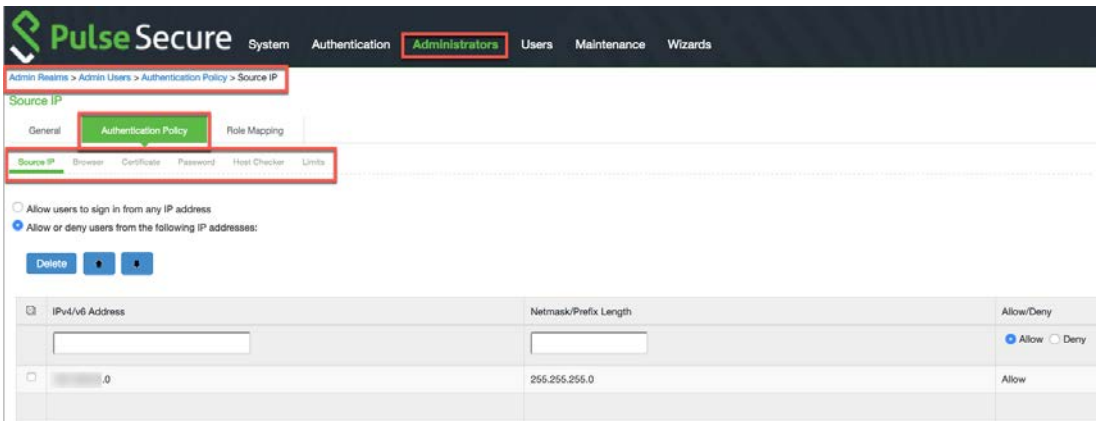

Ilustración 5-10. Creación de Políticas de seguridad.

68. Se puede configurar el Role Mapping, de tal forma que se seleccione el *ROLE* de forma dinámica a través de una extensa cantidad de criterios. Para ello ir a *Administrators > Admin Realms > Admin Users > Role Mapping*. Seleccionar *Role Mapping Rule* y configurar las reglas deseadas.

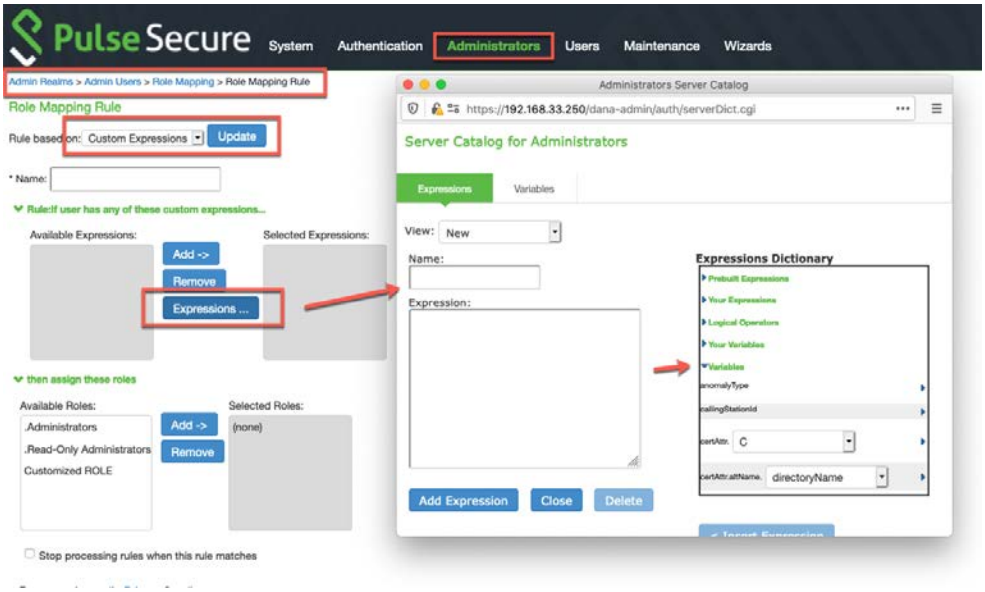

Ilustración 5-11. Reglas de "Role Mapping"

5.3.2.5 CONFIGURACIÓN DE SIGN IN POLICY PARA ADMINISTRADORES

69. La *sign in Policy* define tanto la "URL" a través de la que se dará el acceso, como la forma de autenticarse del usuario (*REALM*). La política por defecto para Administradores es la de: /admin en la sección de Administrator URL's. Se recomienda el cambio de la URL por defecto a una adaptada y más segura para el acceso de los administradores.

70. Para la creación de una nueva *Sing in Policy*:

- Ir a *Authentication > Signing In > Sign-in Policies.*
- Hacer clic en *New URL*.
- Seleccionar *Administrators*, para especificar que los usuarios administradores podrán acceder utilizando la URL.
- Introducir la URL deseada y en el apartado *Authentication Realm* seleccionar qué REALMs utilizarán dicha política.
- Por último, guardar los cambios.

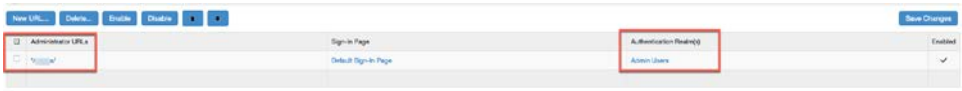

Ilustración 5-12. URL de acceso de los Administradores.

71. El detalle de la creación y configuración de *Sign in Policies* se puede consultar en la documentación online, en el siguiente enlace.

5.3.3 CONFIGURACIÓN DE USUARIOS

72. Para la autenticación de usuarios es posible el uso tanto de una base de datos local en la propia solución como de una gran variedad de métodos de autenticación corporativos como pueden ser AD, LDAP, RADIUS, etc.

73. En el siguiente esquema se muestra la forma lógica de los elementos involucrados durante un acceso por parte de un usuario.

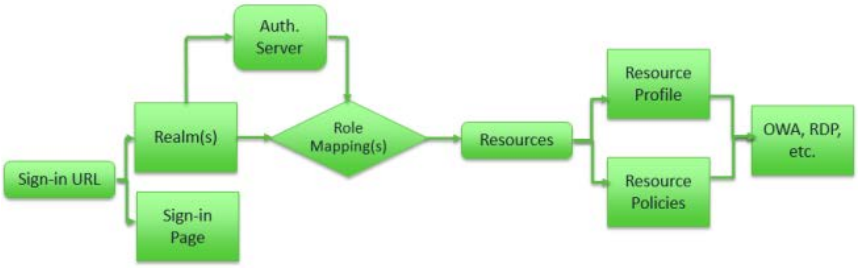

Ilustración 5-13. Esquema de acceso de usuarios

5.3.3.1 CONFIGURACIÓN DEL SERVIDOR DE AUTENTICACIÓN PARA USUARIOS NO ADMINISTRADORES

74. Para configurar el servidor de autenticación para los usuarios no administradores, ir a *Authentication > Auth. Servers*. Seleccionar el método de autenticación deseado (local/corporativo)

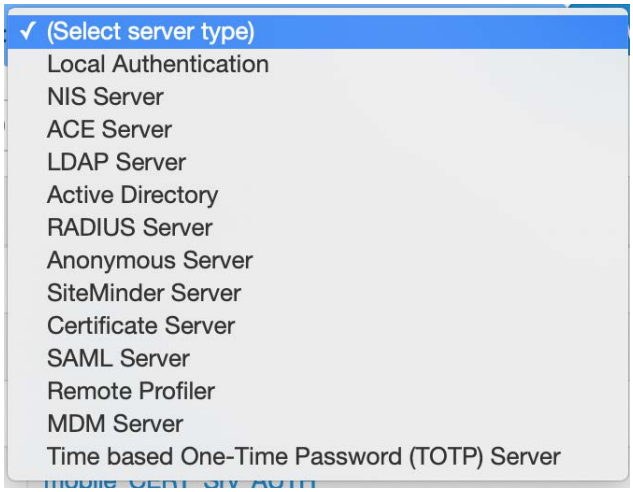

Ilustración 5-14. Métodos de autenticación disponibles.

75. En caso de hacer uso de autenticación remota, se puede consultar la configuración detallada de los distintos tipos de servidor en el siguiente enlace.

76. En caso de querer hacer uso de la autenticación local es preciso crear un "Local Authentication Server", para así poder hacer uso de este. Para ello:

    - Ir a *Authentication > Auth. Servers.*
    - Seleccionar *Local Authentication* y hacer clic en *New Server*.
    - Finalmente completar la información del servidor y guardar.

77. Una vez creado es preciso, en la configuración del *Authentication server*, la creación de los usuarios y los parámetros en relación a estos, tal como se verá en los siguientes apartados.

78. El detalle de la configuración de los servidores de autenticación para usuarios no administradores se puede encontrar en el siguiente enlace: Authentication and Directory Servers.

5.3.3.2 CONFIGURACIÓN DE USUARIOS

79. En el caso de directorios corporativos no es preciso la configuración de usuarios dado que estos mismos se obtienen del servidor corporativo.

80. En el caso de usuarios locales es preciso configurarlos en el producto. Para crear nuevos usuarios:

    - Ir a *Authentication > Auth. Server*.
    - Seleccionar el servidor en el cual se quieren añadir las cuentas de usuario y hacer clic en la pestaña *Users*.
    - Ir a *New* e introducir la información del usuario.
    - Finalmente guardar la configuración.

81. Para configurar la complejidad de las contraseñas de los usuarios, ir a *Authentication > Auth Server > Local Auth Server* y configurar los siguientes parámetros:

    - Minimum length: longitud mínima de la contraseña, se recomienda configurar al menos 12 caracteres
    - Minimum digits: número mínimo de dígitos que debe contener. Se recomienda un valor de al menos un dígito.
    - Minimum letters: número mínimo de letras que debe contener. Se recomienda un valor de al menos una letra.
    - Uppercase and lowercase required: Obliga al uso de mayúsculas y minúsculas. Se recomienda activarlo.
    - Different from username: previene el uso del nombre de usuario como parte de la contraseña. Se recomienda activarlo.
    - Different from previous password: previene que la contraseña sea igual a la anterior.
    - Force password change: obliga el cambio de la contraseña tras el número de días configurado. Se recomienda un valor de entre 30 y 90 días.

82. La configuración de los parámetros de seguridad de los usuarios se detallan en el apartado 5.5 CONFIGURACIÓN DE SEGURIDAD.

5.3.3.3 CONFIGURACIÓN DE ROLES

83. Un *ROLE* de usuario es una entidad que define los parámetros de sesión del usuario (configuración y opciones de sesión), la configuración de personalización (personalización de la interfaz de usuario y marcadores) y las funciones de acceso habilitadas (Web, archivo, aplicación, Telnet / SSH, Terminal Services, red, reunión, y acceso al correo electrónico).
84. Un *ROLE* de usuario no especifica el control de acceso a los recursos ni otras opciones basadas en recursos para una solicitud individual.
85. Por ejemplo, un *ROLE* de usuario puede definir si un usuario puede o no realizar la navegación web. Sin embargo, los recursos web individuales a los que puede acceder un usuario están definidos por las políticas de recursos (ver apartado 5.3.3.7 CONFIGURACIÓN DE RESOURCE POLICIES (ACL)) web que configura por separado.
86. Para la creación de ROLES de usuario, seguir los siguientes pasos:
    - Ir a *User > User Roles*.
    - Hacer clic en *New Role* e introducir el nombre de *ROLE* deseado y, opcionalmente, una descripción.
87. Para modificar *ROLES* existentes, o configurar aquellos recién creados, seguir los siguientes pasos:
    - Ir a *User > User Roles > Role Name > General > Overview*.
    - En el apartado *Role-Specific*, seleccionar en qué páginas será de aplicación.
    - En el apartado *Access Features*, seleccionar los parámetros específicos de acceso del *ROLE*.
    - Ir a *User > User Roles > Role Name > General > Restrictions*, para configurar las restricciones de dirección IP, Navegador Web o Certificado deseadas.
88. El detalle de la configuración de *ROLES* puede consultarse en el siguiente enlace del manual de administración: User Roles
89. Si se quiere proveer accesos a recursos por diferentes *ROLES* se recomienda el uso de *resource profiles*, explicado a continuación.

5.3.3.4 CONFIGURACIÓN DE RESOURCE PROFILES

90. Un perfil de recurso (*Resource Profile*) contiene todas las políticas de recursos, asignaciones de funciones y marcadores de usuario final necesarios para proporcionar acceso a un recurso individual. Los perfiles de recursos simplifican la configuración de recursos al consolidar la configuración relevante para un recurso individual en una sola página dentro de la consola de administración.
91. Para crear un perfil de recurso, seguir los siguientes pasos:
    - Ir a *User > Resource Profiles > Web*.

- Hacer clic en *New Profile*.
- Incluir la información requerida, como el nombre del perfil, el recurso a proteger o las acciones que se llevarán a cabo.
- Hacer clic en *Save* y luego en *Continue*, yendo así a la página de configuración del perfil recién creado.
- Hacer clic en la pestaña *Roles*, seleccionar el *ROLE* al que aplicará el perfil de recurso y hacer clic en *Add*.
- Por ultimo hacer clic en *Save Changes*.

92. El detalle de la creación y configuración de *Resource Profiles*, puede consultarse en: Resource Profiles.

5.3.3.5 CONFIGURACIÓN DE *REALM*

93. Un *REALM* de autenticación especifica las condiciones que los usuarios deben cumplir para iniciar sesión en el sistema.
94. Para crear un *REALM*, seguir los siguientes pasos:
    - Ir a *Users* > *User Realm* y hacer clic en *New*.
    - En el apartado *Servers*, seleccionar el tipo de autenticación deseada (Local o mediante Servidor externo).
    - Finalmente, hacer clic en *Save Changes*.
95. El detalle de la creación y configuración de *REALM* se puede consultar en el siguiente enlace.

5.3.3.6 CONFIGURACIÓN DE SIGN IN POLICY

96. La *sign in Policy* define tanto la "URL" a través de la que se dará el acceso, como la forma de autenticarse del usuario (*REALM*). Se recomienda el cambio de la URL por defecto a uno adaptado y más seguro para el acceso de los administradores.
97. Para la creación de una nueva *Sing in Policy*, seguir los siguientes pasos:
    - Ir a *Authentication* > *Signing In* > *Sign-in Policies*.
    - Hacer clic en *New URL*.
    - Seleccionar *Users*, para especificar que los usuarios no administradores podrán acceder utilizando la URL.
    - Introducir la URL deseada y en el apartado *Authentication Realm* seleccionar qué REALMs utilizarán dicha política.
    - Por último, hacer clic en *Save Changes*.
98. El detalle de la creación y configuración de *Sign in Policies* se puede consultar en la documentación online, en el siguiente enlace.

5.3.3.7 CONFIGURACIÓN DE RESOURCE POLICIES (ACL)

99. Una *Resource Policy* es una regla del sistema que especifica recursos y acciones para una característica de acceso en particular. Un recurso es un servidor o un archivo al que se puede acceder a través del sistema, y una acción es "permitir" o "denegar" el acceso o realizar o no realizar una función.

100. Cada función de acceso tiene uno o más tipos de políticas, que determinan la respuesta del sistema a una solicitud de usuario o cómo habilitar una función de acceso.

101. La creación de *Resource Policies* se puede llevar a cabo desde *Users > Resource Policies*.

102. El detalle de creación y configuración de las políticas de recursos se puede consultar en: Resource Policies

103. Las configuraciones para este punto se hacen a través de siguiente menú: Users > Resource Policies.

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

104. La configuración inicial del *appliance* tanto en formato físico como virtual, se realiza tanto a través de cable (Serial) como a través de consola (en el despliegue virtual).

105. Posteriormente toda la configuración adicional, bien sea de interfaces, servicios, etc… Se gestionará a través del interfaz de usuario de administrador vía WEB (HTTPS).

106. Durante el primer BOOT se generará un Certificado autofirmado aconsejándose la creación de un certificado específico para el *appliance* a través de una CA de confianza. Se puede crear un CSR en la parte correspondiente: *SYSTEM > Configuration > Certificate > Device Certificate*. Y es preciso que la CA esté presente en la parte: Trusted Client CA's.

107. En el apartado 5.6 GESTIÓN DE CERTIFICADOS, de este documento, se detallan los pasos para crear un CSR y añadir una CA de confianza.

5.5 CONFIGURACIÓN DE SEGURIDAD

5.5.1 SESIÓN DE USUARIOS

108. En los siguientes pasos se especifican parámetros para la securización de los Protocolos de Comunicaciones aportando mejoras en seguridad para las sesiones de usuarios.

109. Activar *Server Certificate Trust Enforcement* para que, en dispositivos móviles, solo se acepten conexiones a servidores PCS con certificados válidos. Para ello:

- Ir a *System > Configuration > Mobile*.

- Seleccionar "Enabled" en *Server certificate trust enforcement.*

110. Activar en los ROLES correspondientes la funcionalidad de *HTTP Only Device Cookie*, para mejorar la protección contra ataques XSS y Cookie stealing. Para ello:
    - Ir a *Users > User Roles > Select Role > Session*.
    - Marcar la opción como "Enabled" en *HTTP Only Device Cookie.*
111. Deshabilitar la sesión de itinerancia o límite a la subred para roles de usuario que no sean de itinerancia: esta característica garantiza que, en el caso de robo de una cookie de sesión, esta no pueda ser reutilizada por una dirección IP diferente a la del usuario que inició sesión por primera vez. Esto reduce la posibilidad de que una sesión sea robada y reutilizada por un atacante. Esto implicará que un usuario final vuelva a autenticarse cuando se cambie la dirección IP de origen.
    - Usuarios: Ir a *Users > User Roles > <role name> > General > Session Options: Roaming Session* y seleccionar "Disabled".
    - Administradores: Ir a *Administrators > Admin Roles > <role name> > General > Session Options: Roaming Session* y seleccionar "Disabled"
112. Desactivar las sesiones persistentes:
    - Ir a *Users > User Roles > <role name> > General > Session Options: Persistent Session.*
    - Seleccionar "Disabled".
113. Activar el borrado de la Cookie de sesión del Navegador:
    - Ir a *Users > User Roles > <role name> > General > Session Options: Remove Browser Session Cookie*.
    - Seleccionar "Enabled".
114. Deshabilitar el Split Tunnel: esto ayudará a garantizar que todo el tráfico se envíe a través de la conexión VPN y que el cliente no pueda aceptar conexiones o comunicarse con otros hosts en su subred local. Esto reduce la posibilidad de que un sistema cliente se convierta en una puerta de enlace o proxy en el túnel seguro. Para ello:
    - Ir a *Users > User Roles > <role name> > VPN Tunneling > Options > Split Tunneling Options*.
    - Seleccionar "Disable".
115. Configurar los límites de sesión: asegura que las sesiones de usuario estén limitadas a una duración establecida. Si se roba una sesión, solo estará activa hasta que la sesión se agote. Se recomienda configurar un valor bajo para el límite de sesión, por ejemplo 24 horas.
    - *Ir a Users > User Roles > <role name> > General > Session Options: Session lifetime lengths.*

- Configurar el valor deseado. Se recomienda configurar un valor bajo.

116. Usar la opción de bloqueo de IP para bloquear los ataques de contraseña de fuerza bruta. Advertencia: si los usuarios acceden al dispositivo Pulse Secure a través de un balanceador o proxy, esto no será viable ya que puede parecer que provienen de la misma dirección IP. La configuración se realiza desde *Configuration > Security > Miscellaneous: Lockout Options.*

117. Se recomienda elevar el cifrado para la conexión con el protocolo ESP a 256 bit. Por defecto está configurado en 128 bit.

    - Ir a *Users > Resource Policies > VPN Tunneling > Connection Profiles > <profile name> > Connection Settings: Encryption*.
    - Seleccionar "AES256/SHA256".

118. Configuración de web ACL: se recomienda eliminar o cambiar a DENY para la "Política inicial de recursos locales". Se puede modificar desde *Users > Resource Policies > Web ACL*.

119. Reescritura selectiva (*web rewriting ROLE*): se recomienda eliminar la "Política de web rewriting inicial" desde *Users > Resource Policy > Web Rewriting Policies > Rewriting*.

120. Control de acceso de túnel VPN: se recomienda eliminar o cambiar a DENY para la "Política de túnel VPN inicial" desde *Users > Resource Policy > VPN Tunneling > Access Control.*

121. Deshabilitar "Allow saving logon information " y "Dynamic certificate trust " para la Configuración de conexiones en Pulse Secure Client, desde *Users > Pulse Secure Client > Connection > Options.* De esta forma será necesario realizar la autenticación e introducir las credenciales cada vez que se trate de acceder al producto.

122. Habilitar Server Certificate Trust Enforcement desde *System > Configuration > Mobile* seleccionando “Enabled" bajo Server certificate trust enforcement.

5.5.2 SEGURIDAD SERVIDOR PCS

123. Logueo: habilitar el registro en un servidor syslog. Esto debe hacerse para cada uno de los siguientes casos:

    - Eventos.
    - Acceso de usuario.
    - Registros de acceso de administrador.

124. En el apartado 5.11.3 ALMACENAMIENTO REMOTO, de este documento, se detallan los pasos para configurar un servidor syslog desde *System > Log/Monitoring > "Events" / "User Access / "Admin Access" > Settings: Syslog Servers*

125. Deshabilitar el soporte de renegociación SSL legacy:

- Ir a *Security > Configuration > Security > SSL Options.*
- Quitar la marca en "SSL Legacy Renegotiation Support option".

126. Deshabilitar clientes que solo admiten cifrados débiles:
    - Ir a *System > Configuration > Security > SSL Options > Encryption Strength Option*.
    - Activar el checkbox para “Do not allow connections from browsers that only accept weaker ciphers”.
127. Deshabilitar 3DES en las conexiones SSL:
    - Ir a *System > Configuration > Security > SSL Options > Inbount SSL Options*.
    - En el apartado *Allowed Encryption Strength* desmarcar las casillas con cifrados 3DES.
128. Configurar los ajustes SSL entrantes para "Aceptar solo TLS 1.2 y versiones posteriores". Ver apartado 5.1 MODO DE OPERACIÓN SEGURO – FIPS Nivel 1.
129. Habilitar *Perfect Forward Secrecy* o configurar Ephemeral Diffie Hellman (ECDHE) en la parte superior de la lista de suites de cifrado. Para ello:
    - Ir a *Configuration > Security > Inbound SSL Options*.
    - Seleccionar el botón para “Perfect Forward Secrecy” o “ECDHE”.
130. Configurar las Cabeceras Personalizadas. Para ello:
    - Ir a *System > Configuration > Security > Advanced*.
    - Introducir las cabeceras deseadas.
    - Las cabeceras recomendadas se pueden consultar en el siguiente enlace.
131. Con las notificaciones de inicio de sesión, puede crear y configurar mensajes de notificación detallados que aparecen para los clientes Pulse y para los puntos finales de acceso sin agente cuando el usuario intenta iniciar sesión (**Banner de acceso**). Por ejemplo, puede configurar un mensaje de notificación que explique los términos de uso, específicos de la empresa políticas, una página de bienvenida, un contrato de licencia de usuario final (EULA) o un mensaje del día (MOTD).
    - Para un inicio de sesión basado en navegador (sin agente), el mensaje de notificación aparece en una página separada antes (pre-autenticación) o después (post-autenticación) de la autenticación del usuario durante el proceso de inicio de sesión.
    - Para el inicio de sesión de un cliente de Pulse, los mensajes de notificación aparecen en un cuadro de mensaje de Pulse. Se espera que el usuario lea el contenido del mensaje de notificación de inicio de sesión y lo reconozca haciendo clic en el botón Continuar. El usuario puede indicar su desacuerdo haciendo clic en el botón Rechazar, que finaliza el intento de inicio de sesión.

132. Para configurar el banner de acceso seguir los siguientes pasos:

- Ir a *Authentication > Signing In > Sign-in Notifications.* Hacer clic en *New Notification*.
- Introducir el texto que desea mostrarse y hacer clic en *Save Changes*.
- Ir a *Authentication > Signing In > Sign-in Notifications*.
- En la pestaña de *Configure Sign-in Notifications*, seleccionar ***Pre-Auth Sign-in Notification*** y ***Post-Auth Sign-in Notification.***
- Finalmente hacer clic en *Save Changes*.

5.5.3 SEGURIDAD DE GESTIÓN DEL DISPOSITIVO

133. Permitir el acceso administrativo solo a las interfaces internas o de administración y Bloquear el resto. Para ello:

- Deshabilitar el acceso de administrador desde el puerto externo, que aparece como configuración predeterminada.
- Ir a *Administrators > Admin Realms > <realm name> > Authentication Policy > Source IP.*
- Asegurar que "Enable administrators to sign in on the External Port" no está activado.

134. Bloquear el acceso a la consola serie con una contraseña. Esto deberá hacerse desde la interfaz de línea de comando a través del puerto de consola. Importante: no perder esta clave, ya que se perdería el acceso a la interfaz de línea de comandos. Se puede consultar la configuración de la contraseña en el siguiente enlace: KB40686 - Enable password protection when accessing through the serial console

135. Si el dispositivo está usando una configuración de un interfaz de red (solo puerto interno) y SNMP está habilitado, asegurar de que el puerto UDP 161 esté bloqueado de accesos externos.

5.5.4 SEGURIDAD DE AUTENTICACIÓN

136. Autenticación de dos factores (2FA): se recomienda el uso de la autenticación de dos factores. Una contraseña de un solo uso (OTP) o la autenticación con un certificado de cliente, son dos buenas opciones disponibles, así como el uso de soluciones de terceros u propias que utilicen RADIUS.

- La configuración de la integración de un segundo factor vía TOTP se puede consultar en detalle en el siguiente enlace: Configuring Authentication with a TOTP Authentication Server.
- La configuración de la integración de un segundo factor a nivel de RADIUS, se realiza configurando un servidor de autenticación RADIUS, tal como se ha visto en apartados anteriores y, posteriormente se debe añadir en la

parte de *REALM* (*Users > User Realm*) como segundo factor de autenticación.

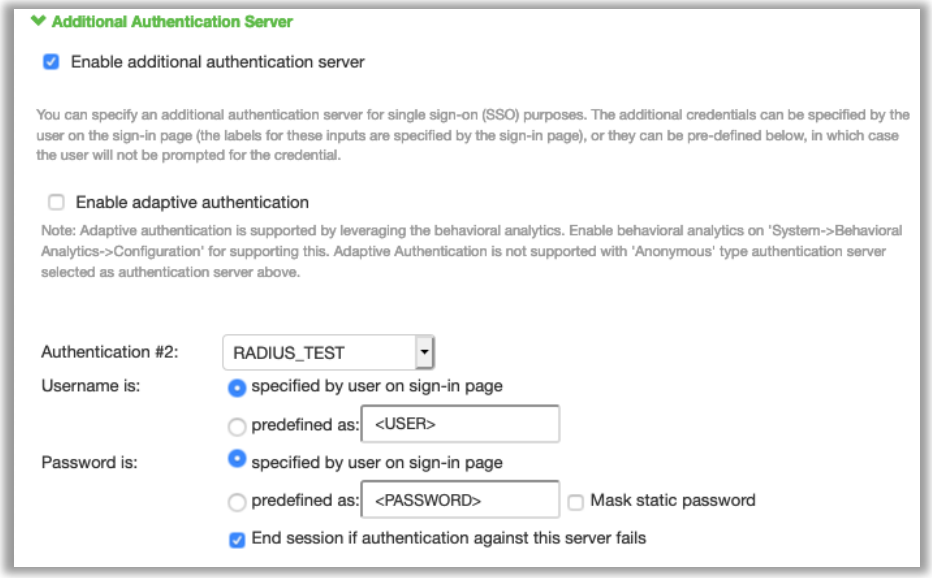

Ilustración 5-15. Servidor RADIUS como segundo factor.

137. En el caso de uso de LDAP, se recomienda habilitar el uso de LDAPS o Iniciar TL. El detalle de dicha configuración se puede consultar en el siguiente enlace: Configuring Authentication with LDAP Server.

138. En el caso de uso de Active Directory, se recomienda el uso del modo estándar de Active Directory. El detalle de dicha configuración se puede consultar en el siguiente enlace: KB40251 - Pulse Connect Secure recommended Active Directory authentication server mode.

5.5.5 SEGURIDAD DEL ENDPOINT

139. Se recomienda usar la solución de Host Checker (herramienta de verificación y obligación de cumplimiento) para garantizar que los clientes estén ejecutando el software de seguridad corporativo requerido, como puede ser el antivirus, verificando que el mismo esté actualizado, firewall, parcheado, etc.

140. El detalle de la configuración de las funcionalidades y la puesta en marcha se puede consultar en el siguiente enlace.

5.5.6 UPDATES DE SEGURIDAD Y ACTUALIZACIONES

141. Se recomienda suscribirse a las alertas de Pulse Secure para obtener avisos de seguridad y mantenerse al día sobre las actualizaciones de software. El detalle sobre cómo suscribirse a dichas alertas se puede consultar en el siguiente enlace: KB40243 - Subscribe to Security Advisory notification emails and Software Release notification emails.

142. Actualizaciones de software: las actualizaciones de software deben realizarse por parte de un usuario administrador de forma manual. Ver el apartado 5.8 ACTUALIZACIONES.

5.5.7 PROTECCIÓN DEL PROCESO DE BOOT

143. La solución integra una autoprotección del entorno para el caso de que durante al proceso de arranque del sistema, exista alguna divergencia en las verificaciones de los ficheros de sistema y el fichero de manifest. Una vez activada esta opción solo se podrá:

- O revertir a la versión anterior en el caso de que las verificaciones sean positivas
- O revertir a la versión de fabrica

144. Para activar esta opción es preciso ir a *System* > *Configuration* > *Security* > *Miscellaneous* y activar *Host Manifest Integrity Validation***.** Por último, guardar la configuración.

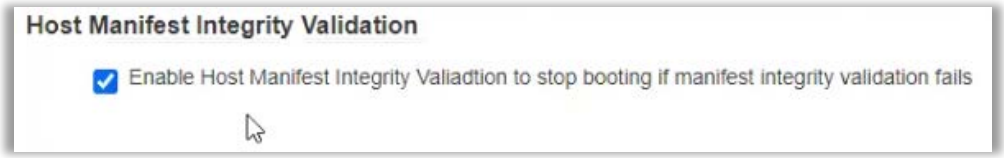

Ilustración 5-16. Comprobación de integridad del Manifest.

5.6 GESTIÓN DE CERTIFICADOS

145. Pulse Connect Secure (PCS) utiliza la infraestructura de clave pública (PKI) para proteger los datos enviados a los clientes a través de Internet. PKI es un método de seguridad que utiliza claves públicas y privadas para cifrar y descifrar información. Estas claves se habilitan y almacenan mediante certificados digitales. Un certificado digital es un archivo electrónico encriptado emitido por una autoridad de certificación (CA) que establece las credenciales para las transacciones cliente / servidor.

146. El producto utiliza los distintos certificados vistos en el apartado 4.4.4 CERTIFICADOS para la correcta protección de sus comunicaciones. Para el detalle de configuración de los certificados del producto, consultar el siguiente enlace.

147. A continuación, se describen las configuraciones más relevantes.

5.6.1 CERTIFICADOS DE DISPOSITIVO

148. Para la creación de un certificado de dispositivo, utilizado por el producto para asegurar sus comunicaciones, se puede crear una solicitud de firma de certificado (CSR). Durante la creación de la solicitud, se recomienda utilizar longitudes de clave de 3072b en caso de usar RSA o 256b en caso de utilizar ECDSA. Seguir los siguientes pasos:

- Ir a *System > Configuration > Certificates > Device Certificates.*
- Hacer clic en *New CSR* para abrir la página de configuración.
- Completar la información requerida y hacer clic en *Create CSR*.
- Seguir las instrucciones en pantalla, que explican qué información enviar a la CA y cómo enviarla.

149. Una vez se reciba el certificado firmado de la CA, debe importarse en el dispositivo. Seguir los siguientes pasos:

- Ir a *System > Configuration > Certificates > Device Certificates.*
- En el apartado *Certificate Signing Requists*, hacer clic en *Pending CSR*.
- Ir a *Import signed certificate* y seleccionar el certificado. Finalmente hacer clic en *Import*.

150. Para importar un certificado de CAs intermedias, en caso de ser necesario, seguir los siguientes pasos:

- Ir a *System > Configuration > Certificates > Device Certificates.*
- Hacer clic en *Intermediate Device CAs* para abrir la página de configuración.
- Hacer clic en *Import CA certificate* y buscar el certificado deseado.
- Finalmente hacer clic en *Import Certificate*.

5.6.2 CERTIFICADOS DE AUTORIDADES DE CERTIFICACIÓN

151. Para la configuración de un CA de cliente de confianza, utilizado, por ejemplo, para la autenticación de los certificados de usuarios. Seguir los siguientes pasos:

- Ir a *System > Configuration > Certificates > Trusted Client CAs.*
- Hacer clic en *Import CA Certificate*.
- Seleccionar el certificado deseado y hacer clic sobre *Import Certificate*.

152. Para la configuración de un CA de servidor de confianza, utilizado, por ejemplo, para validar los sitios web a los que acceden los usuarios. Seguir los siguientes pasos:

- Ir a *System > Configuration > Certificates > Trusted Server CAs.*
- Hacer clic en *Import Trusted Server CA*.
- Seleccionar el certificado deseado y hacer clic sobre *Import Certificate*.

5.6.3 CERTIFICADOS DE CLIENTE

153. En caso de ser necesario el uso de un certificado de cliente, de tal forma que el producto pueda autenticarse ante otros servidores, seguir los siguientes pasos:

- Ir a *System > Configuration > Certificates > Client Auth Certificates.*

- Hacer clic en *Import Certificate & Key* para abrir la página de configuración.
- Completar la información requerida y hacer clic sobre *Import*.

5.7 SINCRONIZACIÓN HORARIA

154. Para configurar el servicio NTP (Network Time) seguir los siguientes pasos:

- Ir a *System > Status > Overview > "System Date & Time".*
- Hacer clic en *Edit*. En el apartado *Time Source*, seleccionar *Use NTP Server.*
- Rellenar los datos de NTP.

5.8 ACTUALIZACIONES

155. Las actualizaciones precisan ser instaladas manualmente por un usuario administrador de la solución. La descarga de la actualización debe realizarse de acuerdo a lo indicado en el apartado 4.1 ENTREGA SEGURA DEL PRODUCTO, para la comprobación de la autenticidad e integridad de la descarga mediante la verificación del hash.

156. Para realizar una actualización:

- Ir a *Maintentance > System Maintenance > Install Service Package > Upgrade/Downgrade.*
- En el apartado *Install Service Package*, seleccionar la opción deseada y seleccionar el fichero de actualización descargado previamente.
- Finalmente, hacer clic en *Install.*

5.9 SNMP

157. La solución de Pulse Secure PCS ofrece la posibilidad del uso de SNMP para controlar el estado del sistema. Se recomienda el uso solo de SNMP v3.

158. Para configurar el agente SNMP:

- Ir a *System > Log / Monitoring*.
- Hacer clic en la pestaña SNMP para mostrar la página de configuración de SNMP.
- Completar la configuración. En el apartado ***SNMP Version*, seleccionar v3**.
- Guardar la configuración

159. El detalle de la configuración de SNMP se puede consultar en el siguiente enlace: Configuring SNMP.

5.10 ALTA DISPONIBILIDAD

160. En el marco de administración de acceso seguro Pulse Secure Connect admite dos tipos de clústeres:

- Clúster en modo Load Balancing o grupos en modo activo/activo
- Clúster en modo failover por error o clústeres activo/pasivo

161. Clústeres en modo Load Balancing o A/A: los clústeres en modo activo/activo proporcionan escalabilidad y aumentan la disponibilidad de servicios basados en la Web. La Figura siguiente muestra un ejemplo de una implementación activa/activa. Un usuario puede implementar un clúster de 4 nodos en PSA-7000. Todos los demás modelos de plataforma solo admiten clústeres de 2 nodos. Un PSA-7000 puede admitir hasta 4 nodos.

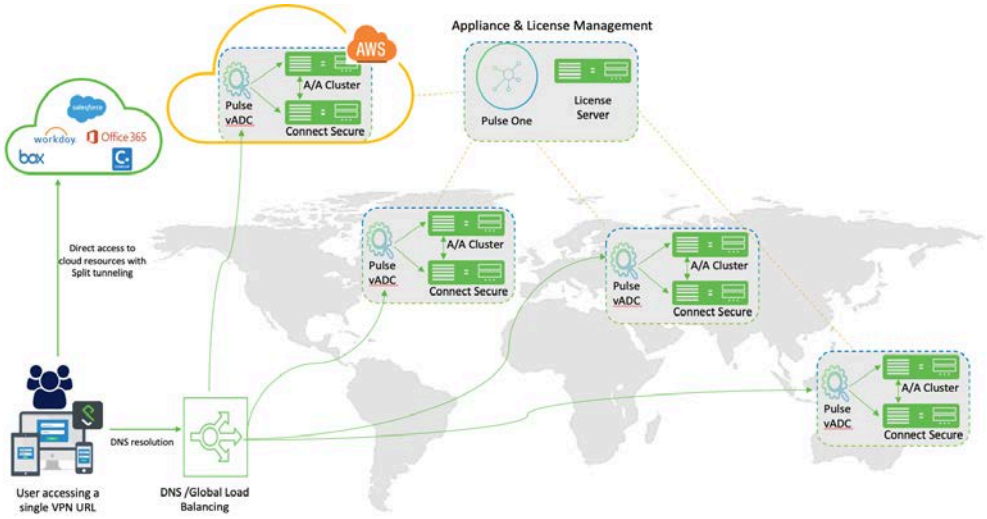

Ilustración 5-17. Clústeres en modo A/A

162. Clústeres de conmutación por error o clústeres activo/pasivo: los clústeres de conmutación por error proporcionan alta disponibilidad (HA). El objetivo principal de los clústeres HA es proporcionar acceso ininterrumpido a los datos, incluso si un servidor pierde conectividad de red o almacenamiento, o falla por completo, o si falla la aplicación que se ejecuta en el servidor. La Figura siguiente muestra un ejemplo de una implementación activo/pasivo. El clúster activo/pasivo solo admite clústeres de 2 nodos en todos los tipos de plataformas, excepto VA.

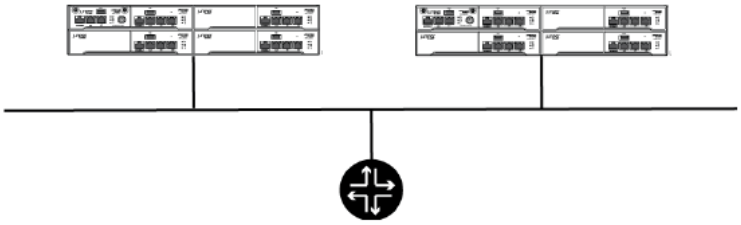

Ilustración 5-18. Clústeres en modo A/P

163. El detalle de la instalación y configuración de los distintos tipos de clúster se puede consultar en el siguiente enlace: Clustering.

164. El despliegue recomendado es un clúster en modo activo/activo o en modo single node – nodos independientes – con sincronización a través de:

- Replicación de configuración (ver el enlace: Push Configuration Feature).
- Uso de la solución de Pulse One (Solución de Gestión Global de Pulse Secure).

165. Las recomendaciones de seguridad son las mismas que para los nodos independientes vistas en los apartados previos.

5.11 AUDITORÍA

166. El sistema genera registros de eventos relacionados con el rendimiento del sistema, acciones del administrador, comunicaciones de red, resultados del marco de administración de acceso, sesiones de usuarios, etc. El sistema admite los siguientes métodos de recopilación de registros:

- Recolector y visor de registros local.
- Reportando a servidores de syslog externos.
- Reportando a servidores SNMP.

167. La siguiente tabla describe el nivel de severidad de los logs de la solución

Nivel de Severidad	Descripción
Crítico (nivel 10)	El sistema no puede atender solicitudes de usuarios y administradores o pierde funcionalidad a la mayoría de los subsistemas.
Mayor (niveles 8-9)	El sistema pierde funcionalidad en uno o más subsistemas, pero los usuarios aún pueden acceder al sistema para otros mecanismos de acceso.
Menor (niveles 5-7)	El sistema encuentra un error que no corresponde a una falla mayor en un subsistema. Los eventos menores generalmente corresponden a fallas de solicitudes individuales.
Información (niveles 1-4)	El sistema escribe un evento informativo en el registro cuando un usuario realiza una solicitud o cuando un administrador realiza una modificación.

5.11.1 REGISTRO DE EVENTOS

168. El registro de eventos se puede configurar de la siguiente manera:

- Ir a *System > Log/Monitoring*.
- Hacer clic en la pestaña de *Settings* para abrir la página de configuración.
- Seleccionar los registros que se desea monitorizar y hacer clic en *Save Changes*.

169. El detalle de la configuración del registro de eventos se puede consultar en el siguiente enlace: Configuring Events to Log.

5.11.2 ALMACENAMIENTO LOCAL

170. El valor predeterminado del tamaño de los logs locales es de 200 MB. El máximo es de 500 MB. El valor predeterminado es una buena opción para los registros con formato Estándar. Si utiliza un formato más detallado, como WELF, se recomienda especificar un valor mayor. La modificación del tamaño de los logs locales se puede realizar desde *System > Log/Monitoring > Events / User Access / Admin Access > Settings*.

171. Cuando el registro local alcanza el tamaño máximo de registro, los datos actuales se transfieren a un archivo de registro de respaldo automáticamente. Después se crea un nuevo archivo vacío para todos los mensajes de registro posteriores (nuevos). El visor de registros muestra los 5000 mensajes de registro más recientes (el límite de visualización). Si el archivo de registro actual contiene menos de 5000 mensajes de registro, se pueden mostrar mensajes de registro anteriores del archivo de registro de respaldo, hasta un total de 5000 mensajes de registro. Esto hace que los archivos de registro aparezcan como uno, a pesar de que se almacenan por separado.

172. La visualización de los logs almacenados localmente se puede realizar desde la página *System Logs*.

173. En caso de llegar al límite de almacenamiento local de logs, se sobrescriben las entradas más antiguas de forma automática. Por esto, se recomienda el uso de sistemas externos de almacenamiento de logs.

5.11.3 ALMACENAMIENTO REMOTO

174. Para la configuración del envío de logs a un servidor externo Syslog, seguir los siguientes pasos:

- Ir a *System > Log/monitoring*.
- Hacer clic en *Settigns*.
- En el apartado *Syslog Servers*, introducir la información relativa al servidor que desea configurarse.
- Por último, seleccionar el protocolo TLS para hacer uso solo de TLS 1.2 o posteriores y hacer clic en *Save changes.*

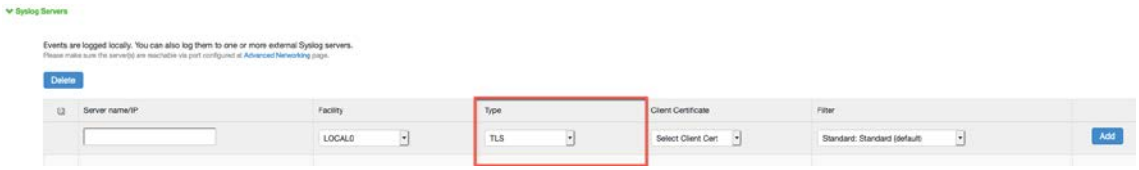

Ilustración 5-19. Configuración de TLS en servidor Syslog

5.12 BACKUP

175. El sistema admite múltiples utilidades de administrador relacionadas con la gestión de archivos de configuración. Estas utilidades se pueden encontrar en las diferentes páginas accesibles desde *Maintenance*. La siguiente Tabla describe el propósito de las diferentes utilidades.

Utilidad	**Uso Recomendado**
Archivado *Archiving*	Programa copias de seguridad periódicas en un servidor de copia de seguridad remoto. Debe programar la salvaguarda tanto para el archivo binario de configuración del sistema (system.cfg) como para el archivo binario de configuración del usuario (user.cfg). Si es necesario, puede importar una configuración archivada utilizando la función de importación / exportación de archivos binarios de configuración.
Copia de seguridad local y restauración *Backup and restore*	Crea copias de seguridad en el sistema local como precaución cuando realice cambios significativos en la configuración. Con esta utilidad, puede restaurar rápidamente a una configuración anterior.
Importación / exportación de archivos de configuración binarios *Import/Export Feature for Binary System Configuration Files*	Exporte archivos de configuración binarios a un host local (una alternativa al servidor de archivo remoto y al proceso de archivo que se ejecuta como un trabajo programado). Puede hacerlo si no utiliza o no tiene acceso a un servidor de archivado, o si desea utilizar una configuración que aún no se ha archivado. Puede exportar el archivo de configuración del sistema binario (system.cfg) y el archivo de configuración del usuario binario (user.cfg). Puede usar la función de importación / exportación de archivos binarios para clonar una configuración que desea implementar de manera más amplia, como implementar un dispositivo de respaldo o un grupo de dispositivos. Puede usar las opciones de "importación selectiva" para excluir identificadores de red únicos (como la dirección IP) que causarían problemas si la configuración se importara y activara por completo.
Importación / exportación de archivos de configuración XML *Import/Export Feature for XML*	Importe o exporte la configuración solo para las características y configuraciones que seleccione. Esto le permite adoptar un enfoque más granular para la gestión de la configuración masiva que la función de importación / exportación de archivos binarios. Por ejemplo, es posible que desee desplegar una configuración de servidor de autenticación en una gran cantidad de nodos. Puede exportar solo ese elemento de configuración, y cuando lo importe en los otros nodos a través del XML, no sobrescribirá una gran

Configuration Files	cantidad de elementos de configuración adicionales, que si se realizaría en el caso de haber importado el archivo user.cfg. También puede encontrar útil la función de importación / exportación de archivos XML al administrar un solo nodo. Por ejemplo, es posible que desee agregar muchos usuarios nuevos al servidor de autenticación local, pudiendo ser más rápido la edición del XML que la utilización de la interfaz de usuario. O quizás desee realizar cambios globales en las convenciones o descripciones de denominación de objetos de configuración como parte de una iniciativa de "limpieza". Esto también podría lograrse editando el XML de una manera más rápida que haciendo clic en la interfaz de usuario.
Configuración "push" *Push Configuration*	Permite desplegar, completa o parcialmente, la configuración de un sistema en producción en otro sistema o sistemas destino. Es una buena opción para el despliegue de configuraciones en dispositivos que actualmente están dando servicio.

176. La opción recomendada para la **gestión de copias de seguridad local** es el uso de *Backup and restore*, mediante la creación de *Local Backups.* Se puede usar para guardar y restaurar hasta 5 copias de la configuración actual del sistema, de las cuentas de usuario o de la base de datos. Se recomienda realizar una copia de seguridad antes de aplicar nuevas configuraciones u otros cambios en el entorno, es decir, antes de cualquier gestión de cambio que se le aplicará al sistema. Las Copias de seguridad locales se realizan desde la página *Maintenance > Archiving > Local Backups*.

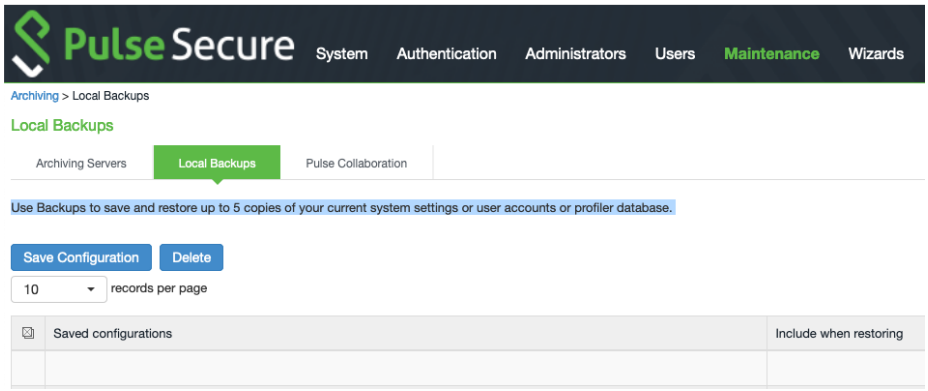

Ilustración 5-20. Creación de una copia de seguridad local

177. La opción recomendada para la **gestión de copias de seguridad remota** es el uso de *Archiving*. Se puede utilizar para programar el envío de copias periódicas de los archivos de configuración y logs del sistema a un servidor remoto configurado. Para configurar esta opción, seguir los siguientes pasos:

- Ir a *Maintenance > Archiving > Archiving Servers*.

- Completar la información del servidor, como la dirección IP, el directorio en el que se desea guardar la copia y las credenciales de acceso al servidor.
- Se recomienda utilizar el protocolo SCP (opción por defecto), en el apartado *Method*.
- En el apartado *Archive Schedule*, configurar la periodicidad de las copias.
- Finalmente, hacer clic en *Save Changes*.

178. El detalle de la configuración de las distintas utilidades vistas en el presente apartado puede consultarse en el siguiente enlace.

6. FASE DE OPERACIÓN

179. Para la fase operativa es recomendable de forma periódica valorar la implementación las nuevas versiones de paquetes de Software, dado que estas suelen incluir tanto parches para problemas conocidos, mejoras de seguridad y estabilidad, así como soporte para sistemas operativos actualizados de terceros como pueden ser Microsoft, Windows, Linux, etc.

    a) Página de documentación general

    b) Página de documentación v9.1R Servidor

    c) Página de documentación v9.1R Cliente

    d) Página de documentación Cliente (Android/iOS)

    e) Página de documentación para ESAP

180. Se recomienda realizar copias de seguridad periódicas, así como configurar el envío de copias a un servidor externo con una periodicidad definida.

181. Se recomienda auditar o tener alarmas para los elementos CRÍTICOS recogidos en los logs de eventos para poder hacer seguimiento de posibles problemas.

182. Se recomienda verificar periódicamente el uso de memoria y CPU dado que valores elevados de uso pueden generar problemas.

183. Se recomienda configurar el envío de logs a un servidor Sylog, para evitar la pérdida de información al producirse la sobrescritura de los logs almacenados localmente al alcanzar el límite de espacio definido.

184. Se recomienda gestionar correctamente los certificados utilizados por el producto, cambiando estos cuando sea necesario. Por ejemplo, al expirar los certificados configurados.

7. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Registro y aplicación de las licencias	☐	☐	
Actualización de Firmware al último parcheado disponible	☐	☐	
Configuración Servidor NTP	☐	☐	
Configuración Servidor SYSLOG para registros	☐	☐	
Configuración de BACKUP & ARCHIVADO periódico	☐	☐	
Configuración de los Certificados de cliente, maquina, CA's de confianza, etc.	☐	☐	
Configuración de puntos de seguridad a nivel global plasmados en esta guía	☐	☐	KB Configuration Best Practice
Creación de Servidor de Autenticación (LDAP, AD, RADIUS, TOTP, etc.)	☐	☐	
Creación de ROLES / RESOURCE PROFILES	☐	☐	
Creación de *REALM*	☐	☐	
Creación de las configuraciones de Endpoint Protection (Host Checker)	☐	☐	
Configuración de las Authentication Policies (*REALM* & *ROLE*)	☐	☐	
Creación de Sign-in URL	☐	☐	
Configuración de Cloud Secure para aplicaciones Cloud (O365, Google Apps, Dropbox, etc. ..)	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Modo de Operación seguro activado (FIPS-CC)	☐	☐	FIPS Level 1 Support (Software FIPS)

8. REFERENCIAS

Doc. Global Página de Documentación Global de Pulse Secure https://www-prev.pulsesecure.net/techpubs/

Doc. PCS Página Global de documentación para la parte servidor https://www-prev.pulsesecure.net/techpubs/pulse-connect-secure/pcs/9.1Rx

Doc. ESAP Página Global de documentación para la parte de ESAP usada en HC (Host Checker) https://www-prev.pulsesecure.net/techpubs/pulse-connect-secure/esap

Doc. PDC Página Global de documentación para la parte de Cliente https://www-prev.pulsesecure.net/techpubs/pulse-client/pulse-secure-client-desktop/9.1Rx

KB Base de conocimientos técnica de Pulse Secure https://kb.pulsesecure.net/

SA Security Advisories, base de conocimiento técnica para los avisos de seguridad relacionados con las soluciones de Pulse Secure https://kb.pulsesecure.net/?atype=sa

KB29805 Pulse Connect Secure: Buenas Practicas de configuración de Seguridad https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB29805/

KB40028 How to download software / firmware for Pulse Secure products using the Licensing & Download Center at my.pulsesecure.net https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40028

KB40031 Onboarding at my.pulsesecure.net https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40031

KB40030 Pulse Secure Support Services Quick Start Guide https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40030

KB40050 Onboarding FAQ https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40050

KB40499 Support Process for Enhancement Request (ER). https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40499

KB40565 What is Right To Use (RTU) and Service Contract certificate https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40565

Doc. Cloud Secure Guía de Administración de Cloud Secure (PDF)

Doc. Cloud Secure Guía de Administración Cloud Secure fromato WEB

9. ABREVIATURAS

AAA	Autenticación, Autorización, contabilización (Accounting)
ACL	Access Control List
AWS	Amazon Web Services
CA	Autoridad de Certificación
DMZ	Zona demilitarizada (DeMilitarized Zone)
ECDHE	Ephemeral Diffie Hellman
EULA	End-User License Agreement
FTP	File Transfer Protocol
FIPS	Federal Information Processing Standard
LDAP	Lightweight Directory Access Protocol
MOTD	Message Of The Day
PCS	Pulse Connect Secure, solución de VPN SSL de Pulse Secure
PDC	Pulse Desktop Client
PPS	Pulse Policy Secure, solución de NAC de Pulse Secure
RADIUS	Remote Authentication Dial-In User Service
SAML	Security Assertion Markup Language
SCP	Secure Copy Protocol
SHA	Secure Hash Algorithm
SSH	Secure Shell Protocol
SSO	Single Sign On
TCP	Transmission Control Protocol
TLS	Transport Layer Security Protocol
TOTP	Time One Time Passwod
UDP	User Datagram Protocol
URL	Uniform Resource Locator
vADC	Solución de balanceo de Pulse Secure que incluye optimizaciones para PCS & PPS
VPN	Virtual Private Network