centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1109

Procedimiento de Empleo Seguro
Pulse Policy Secure v9.1R1

Enero de 2022

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

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
2022.01.28 15:36:58 +01'00'

NIPO: 083-22-046-2.

Fecha de Edición: enero de 2022

ÍNDICE

1 INTRODUCCIÓN

1. ***Pulse Policy Secure*** (**PPS**) es una solución de **control de acceso a la red (NAC)** que proporciona acceso a la red exclusivamente a usuarios y dispositivos autorizados. El NAC protege la red, las aplicaciones críticas y los datos confidenciales a través de la administración, la visibilidad y la monitorización integral de las mismas.
2. PPS reduce el coste y la complejidad de implementar un control de acceso granular de identidad, habilitado por roles. También aborda la detección de amenazas internas, permite el control de acceso de invitados y facilita el cumplimiento normativo.
3. La solución PPS gestiona los perfiles de usuario, atributos, roles e identidades de grupo y vincula la información de identidad del usuario al punto final y a la red, utilizando la política resultante para asignar al usuario el rol apropiado durante la sesión de acceso.

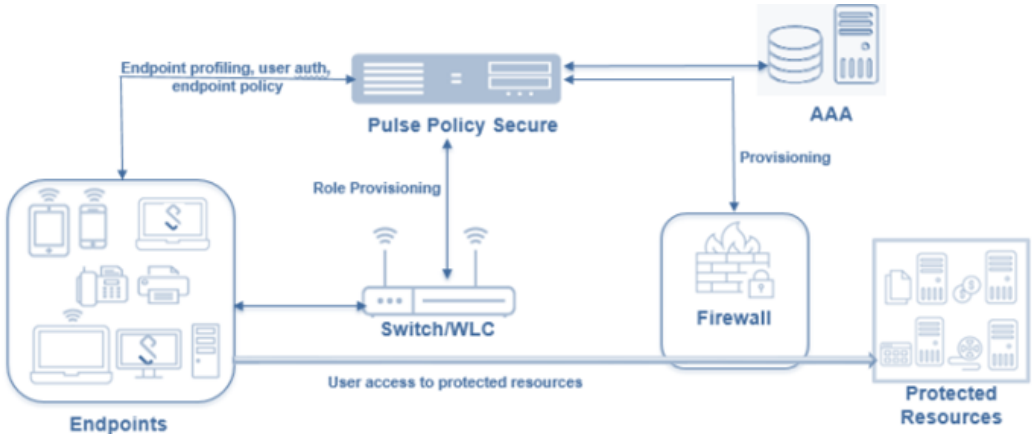

Ilustración 1-1. Esquema estructura PPS

4. La solución PPS utiliza la validación de punto final para dar acceso a los usuarios en grupos de acceso específicos. A dichos grupos se les puede proporcionar acceso a diferentes recursos en función de los mecanismos de control de acceso, tales como LAN virtuales (VLAN), filtros o listas de control de acceso (ACL).
5. Se pueden definir parámetros de QoS adicionales de sesión para la aplicación de políticas basadas en roles, de modo que solo los usuarios autorizados (los que cumplen con las políticas de seguridad definidas) puedan acceder a las aplicaciones y a los datos.
6. PPS también funciona con dispositivos no administrados, como impresoras, teléfonos VoIP y cámaras IP. Es posible configurar *hosts* típicos como el teléfono VoIP, que no está habilitado para 802.1X, el acceso a la red mediante la aplicación SNMP y el generador de perfiles de Pulse Secure.
7. La integración con *Pulse Secure Profiler* permite a PPS construir una base de datos de los dispositivos no administrados en la red, para disponer de un nivel de seguridad de acceso equivalente al de los dispositivos administrados.

8. La solución PPS es extremadamente flexible y ofrece numerosas opciones para su integración en red. Cuando un punto final se conecta a la red, PPS recopila datos de autenticación del usuario, del estado de seguridad del punto final y la ubicación del dispositivo. Esta información es combinada para crear políticas dinámicas, que posteriormente se propagan a los puntos de aplicación. La aplicación puede estar en el borde de la red, antes de otorgar una dirección IP utilizando 802.1X, en el *firewall* o en ambas localizaciones para una mayor granularidad.

2 OBJETO Y ALCANCE

9. El siguiente documento sirve como guía de buenas prácticas de seguridad en la instalación y configuración de la solución PPS de Pulse Secure. No está orientado a construir una guía completa para la instalación y configuración del producto, si no que establece acciones concretas para conseguir un despliegue seguro del producto.

10. Para más información y detalle en el proceso de instalación, despliegue y configuración se puede consultar la documentación online de PPS [REF1].

11. En la presente guía se hace referencia a la solución PPS en la versión v9.1R1 tanto en las versiones de *hardware* como en las versiones virtuales y cloud para los entornos VMWare, Hyper-V, KVM, Azure, y AWS.

	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

12. **Los modelos anteriores son los que han sido cualificados e incluidos en el Catálogo de Productos y Servicios STIC, en las familias '*Control de Acceso a Red*' y '*Servidor de Autenticación*'.**

3 ORGANIZACIÓN DEL DOCUMENTO

13. El presente documento se divide en los siguientes apartados que servirán de guía en la configuración segura de la solución de Pulse Secure PPS:

    - **Apartado 4.** En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue previa a la instalación del producto y aspectos relativos a la seguridad de la misma.
    - **Apartado 5.** En este apartado se recogen las recomendaciones de seguridad a tener en cuenta durante la fase de instalación del producto.
    - **Apartado 6.** En este apartado se recogen las recomendaciones de seguridad a realizar durante la fase de configuración del producto.
    - **Apartado 7.** En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de operación del producto para desempeñar un funcionamiento seguro.
    - **Apartado 8.** En este apartado aparece un *checklist* con las tareas a realizar y el estado de cada una de ellas.
    - **Apartado 9.** Incluye documentación que ha sido referenciada a lo largo del documento.
    - **Apartado 10.** En el último apartado se hace referencia a las diferentes abreviaturas utilizadas a lo largo del documento.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

14. En este apartado se aportan indicaciones para la recepción segura del producto en formato *hardware* y en formato virtual.

Recepción en formato *hardware*:

a) Para garantizar que se reciba el *hardware* de forma correcta, primeramente, debe examinarse el dispositivo para asegurar que no haya sido manipulado durante el proceso de entrega. Antes de desembalar el dispositivo, se debe inspeccionar el embalaje físico en el que se entregó el equipo y comprobar que el embalaje está impreso con el logotipo de Pulse Secure.

b) Verificar que el embalaje no haya sido abierto y comprobar que la cinta sella correctamente el paquete.

c) Verificar que el embalaje incluye una etiqueta blanca codificada para transportes a prueba de manipulaciones. Esta etiqueta incluirá el número de producto, el número de serie y otros datos relacionados con el contenido de la caja.

d) Comprobar que el número de serie del dispositivo que figura en la documentación de envío coincide con el número de serie de la factura recibida.

e) Verificar que el paquete haya sido enviado por el proveedor esperado del equipo (Pulse Secure / distribuidor autorizado por Pulse Secure).

f) Una vez desembalado, inspeccionar la unidad. Verificar que el número de serie que se muestra en la unidad coincide con el que figura en la documentación de envío y la factura. También verificar que la unidad tenga la siguiente identificación externa:

Nombre del Producto	Identificación Externa
Pulse Secure PSA300	Pulse Secure PSA300
Pulse Secure PSA3000	Pulse Secure PSA3000
Pulse Secure PSA5000	Pulse Secure PSA5000
Pulse Secure PSA7000C	Pulse Secure PSA7000C
Pulse Secure PSA7000F	Pulse Secure PSA7000F

g) En el caso de que alguna de las comprobaciones previas no sea satisfactoria, el usuario deberá ponerse en contacto con el proveedor del equipo (Pulse Secure / distribuidor autorizado por Pulse Secure).

Recepción en formato virtual:

a) En el caso de haber adquirido una suscripción en formato virtual, es preciso que el usuario cree una cuenta en el portal de soporte (*https://my.pulsesecure.net*) [REF3], para así poder tener acceso y 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 necesario asociarla a la cuenta corporativa de la organización para la que haya adquirido el servidor en versión *software* (*VMWare, Hyper-V, KVM, Azure, AWS*). Existen detalles adicionales sobre el proceso en el apartado 4.3 REGISTRO Y LICENCIAS de este documento.

c) Una vez vinculada la cuenta se puede descargar el paquete de *software* correspondiente en el área indicada con "*Download*". Se puede consultar el siguiente KB de la página web oficial de Policy Secure [REF2] para obtener ayuda adicional sobre la descarga: *KB40028 - [Customer Support Tools] How to download software / firmware for Pulse Secure products using the Licensing & Download Center at my.pulsesecure.net. [REF 4]*

d) **Se debe comprobar la firma SHA2 para la verificación de integridad tras la descarga del producto**. Se debe obtener el hash SHA-2 y comprobar que coincide con el indicado en el área de descarga.

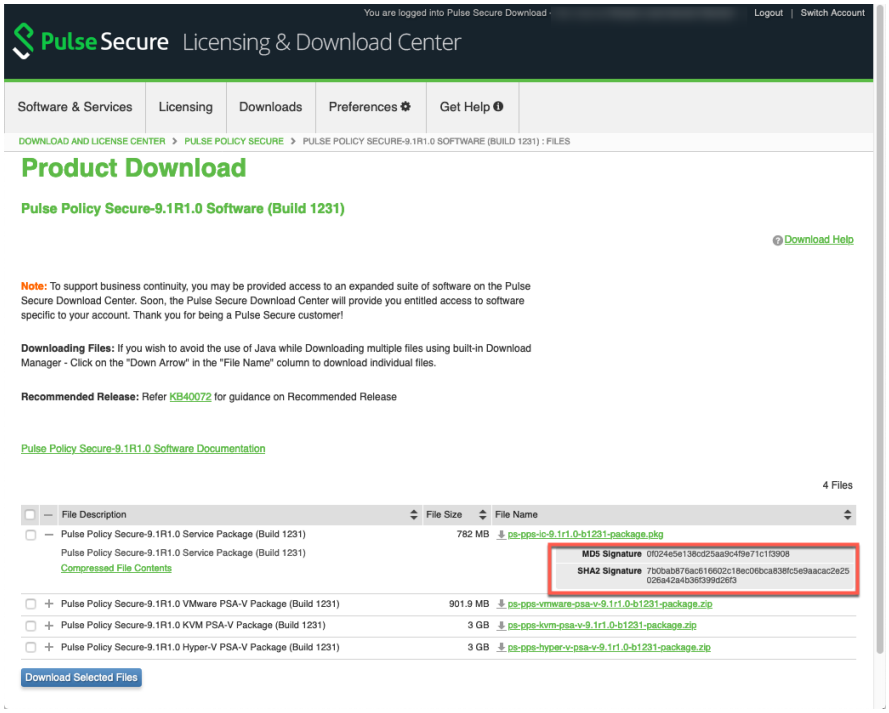

Ilustración 4-1. *Hashes* de verificación del *software*

4.2 ENTORNO DE INSTALACIÓN SEGURO

15. La parte servidora de la solución PPS hará de elemento de seguridad para el acceso remoto a las redes corporativas y se encargará del cumplimiento de las políticas de seguridad para el acceso local de los usuarios y verificando el cumplimiento de las normativas de seguridad aplicadas por los administradores.
16. Consecuentemente, este elemento se desplegará en un centro de proceso de datos en el que se deben tener los controles de acceso adecuados. El acceso físico se debe restringir al personal expresamente autorizado y se deben implantar, tanto los controles de seguridad físicos, como medidas de seguridad de vigilancia correspondientes a este tipo de entornos.

4.3 REGISTRO Y LICENCIAS

17. Para poder tener acceso al inventario de Pulse (*hardware*, licencias, *Auth-Codes*, etc.) es necesario tener acceso al portal de soporte de *Pulse Secure*, al cual se accede a través de la siguiente URL: *https://my.pulsesecure.net.* [REF3]
18. 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.
19. Para mayor detalle en el proceso de alta de usuario y asociación con la cuenta corporativa se pueden consultar los siguientes KBs que describen los pasos del proceso en cuestión:
    a) *KB40050 – Onboarding FAQ*. [REF5]
    b) *KB40031 – [Customer Support Tools] Onboarding at my.pulsesecure.net.* [REF 6]
    c) *KB40565 – What is Right To Use (RTU) and Service Contract certificate.* [REF 7]
20. Una vez creada y vinculada la cuenta de usuario, se procederá a la obtención y aplicación de las licencias de uso.
21. Para obtener las licencias, se deben realizar los siguientes pasos:
    - Acceder a *System > Configuration > Licensing > Download Licenses.*
    - Bajo el apartado "*On demand license downloads*" introducir el código de autenticación ("*authentication code*"). Dicho código debe haber sido proporcionado al administrador a través de un correo asociado al producto en el momento de su adquisición, concretamente en el certificado RTU ("*right to use certificate*").
    - Seleccionar la opción *Download and Install.*
    - Acceder al apartado *License Summary* para comprobar las licencias instaladas.

22. Para más información sobre este procedimiento, consultar la documentación oficial de Pulse: Obtención de Licencias. [REF8]
23. Alternativamente, se puede seguir el siguiente procedimiento:
    - Acceder desde la página web oficial de Pulse Secure al *Pulse Secure Licensing and Software Download Center*. En el apartado *My Assests* buscar el dispositivo a licenciar.
    - Seleccionar *Asset Detail* en el producto y acceder a *Licenses for this Asset* y seleccionar *Generate.*
    - Introducir el código de 16 caracteres "*licensing hardware ID*" disponible en la consola serie o la consola de administración del producto.
    - Introducir el número de serie correspondiente al producto.
    - Introducir el código de autorización asociado al producto.
    - Para finalizar, seleccionar de nuevo *Generate.*
24. Para aplicar la licencia obtenida a través de este último procedimiento, se deben seguir los siguientes pasos:
    - Acceder a la pestaña *System > Configuration > Licensing*.
    - En el cuadro *Licensing* introducir la licencia obtenida y seleccionar *Add*.
25. Para mayor detalle en la obtención de las licencias del producto, se pueden consultar los pasos indicados en el siguiente enlace de la documentación: Obtención de Licencias. [REF9]

4.4 CONSIDERACIONES PREVIAS

4.4.1 NOMENCLATURAS

4.4.1.1 AUTHENTICATION REALM

26. Un *authentication realm* especifica las condiciones que los usuarios deben cumplir para iniciar sesión en el sistema. Un *realm* consiste en 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 el usuario envía desde 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 para la asignación de uno o más roles de usuario.
    c) **Una política de autenticación**: especifica los requisitos de seguridad 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 roles**: condiciones que un usuario debe cumplir para que el sistema le asigne uno o más roles.

4.4.1.2 POLÍTICAS DE INICIO DE SESIÓN (*SIGN-IN POLICY*)

27. Las políticas de inicio de sesión definen las URL que los usuarios y administradores utilizan para acceder al dispositivo y las páginas de inicio de sesión que visualizan. El sistema tiene dos (2) tipos de políticas de inicio de sesión: una para usuarios y otra para administradores.

4.4.1.3 ROLES DE USUARIO

28. Un rol de usuario ("*role*") es una entidad que define los parámetros de la sesión del usuario (configuración y opciones de la sesión), la configuración de personalización (personalización de la interfaz de usuario y marcadores) y las funciones de acceso habilitadas: web, archivo, administrador de aplicaciones seguras, tunelización VPN, correo electrónico seguro, integración empresarial SSH, "*terminal services*", reuniones, escritorios virtuales, acceso HTML5 y cliente Pulse Secure.

29. Un rol de usuario no especifica el control de acceso a los recursos ni otras opciones basadas en recursos para una solicitud individual.

4.4.1.4 RESOURCE POLICY (POLITICA DE RECURSO)

30. Una política de recursos (*resource policy*) es una regla del sistema que indica los recursos y acciones asociados a un acceso en particular. Un recurso puede tratarse de un servidor o archivo al que se accede a través del sistema, y una acción puede ser, por ejemplo, "permitir" o "denegar" un determinado recurso.

31. Cada acceso particular tiene uno o más tipos de políticas que determinan la respuesta del sistema a una petición de usuario.

4.4.2 ARQUITECTURA

32. Generalmente, los equipos de Pulse Secure (PSA-3000/5000/7000) se despliegan con tres (3) interfaces de red principales:

    a) **Interna:** para la interconexión con el *hardware* de red ("*switches*") a través de SNMP.

    b) **Externa:** para la interconexión con el *hardware* de red ("*switches*") en modo SPAN/RSPAN, para el portal cautivo, para los procesos de autenticación y para el servicio de RADUIS, en caso de actuar como servidor RADIUS.

    c) **Gestión:** interfaz para la gestión de la solución.

33. En la máquina PSA-300, dimensionada para pequeñas organizaciones, el despliegue está basado en únicamente dos (2) interfaces de red:

    a) **Interna:** para la interconexión con el *hardware* de red ("*switches*") a través de SNMP. Además, la gestión del producto será realizada desde esta interfaz.

b) **Externa:** para la interconexión con el *hardware* de red ("*switches*") en modo SPAN/RSPAN, para el portal cautivo, para los procesos de autenticación y para el servicio de RADIUS, en caso de actuar como servidor RADIUS.

4.4.3 PREREQUISITOS

34. El usuario se debe dar el alta en el Portal de Soporte de Pulse Secure (https://my.pulsesecure.net) [REF3] para obtener acceso a notificaciones de seguridad (*Security Advisories*), parches y nuevas versiones del *software*.
35. Para realizar el alta de forma adecuada, se recomienda seguir los pasos de los KBs referenciados en el apartado 4.3 REGISTRO Y LICENCIAS y, adicionalmente, consultar el siguiente enlace para mayor detalle: *KB40030 - [Customer Support Tools] Pulse Secure Support Services Quick Start Guide*. [REF10]
36. Se debe tener la siguiente información antes de configurar el dispositivo PPS:
    a) Dirección del servidor NTP y otros detalles como la dirección de *gateway*, mascara de red y DNS.
    b) El SKU de licencia o los detalles del servidor de licencias. El dispositivo PPS se agrega al servidor de licencias como un cliente al que adjudica las licencias necesarias desde el propio servidor.
    c) Los servidores de autenticación (AD/LDAP) deben tener grupos definidos para diferentes roles.
    d) La lista de conmutadores junto con su dirección IP y otros parámetros, como la información de VLAN para diferentes grupos de usuarios.
    e) Detalles de la cuenta de administrador de PPS para obtener el servidor de autenticación y los detalles del rol.
    f) Licencia del producto adquirido.
    g) También se dispone de *software* adicional descargable en la sección de Software del portal de Soporte de Pulse Secure (https://my.pulsesecure.net) [REF 3]:
        - **PDC (*Pulse Desktop Client*):** cliente de Pulse Secure para la autenticación vía agente (recomendado para el uso con 802.1x).
        - ***Plugin ESAP (Endpoint Security Assessment Plugin)*:** usar con la funcionalidad de Host Checker para hacer verificaciones varias como pueden ser AV, FW, Registro, Ficheros, Certificados, Servicios, Cifrado, etc.
        - ***Pulse Secure Behaviour Analytics Database***: base de datos que monitoriza el tráfico de usuarios y dispositivos y ayuda a determinar las posibles actividades anómalas.
        - ***Fingerprint Database*:** base de datos de apoyo para la detección y clasificación de dispositivos de red.

- ***Third Party Integration Application*:** usar con la integridad de correladores de eventos como Qradar, Splunk o EPO.

4.4.4 CERTIFICADOS

37. PPS utiliza distintos tipos de certificados digitales para establecer credenciales y transacciones de sesión seguras:

    a) **Certificados de dispositivo:** ayudan a proteger el tráfico de red en el servicio 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, PPS hace uso de un certificado de dispositivo para las comunicaciones con *Infranet Enforcer.*

    b) **CA de cliente de confianza:** es un certificado del lado del cliente emitido por una CA. Puede hacer uso de CA de clientes de confianza en el ámbito del marco de gestión de acceso y configuraciones de roles para requerir certificados o certificados con atributos específicos. Por ejemplo, se puede especificar que los usuarios deben presentar un certificado del lado del cliente que sea válido con el atributo OU establecido en su organización para iniciar sesión en el ámbito de autenticación de usuarios.

    c) **CA de servidor de confianza:** es el certificado de un servidor web de confianza. Puede instalar una CA de servidor de confianza 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 autenticación de cliente:** este certificado se usa cuando los servidores SSL "*backend*" requieren que PPS presente un certificado de cliente.

38. En el apartado 6.6 Gestión de Certificados, se detalla la configuración de los certificados mencionados para un correcto funcionamiento del entorno.

5 INSTALACIÓN

39. La instalación de la solución cuenta con dos (2) procedimientos a seguir en función de si se realiza sobre equipamiento físico (*hardware*) o en modo Virtual (VMWare, KVM, Hyper-V, Azure, AWS).

Despliegue en formato físico:

a) En el caso de dispositivos físicos es preciso conectarse a través de cable de consola al dispositivo, para poder proceder a la configuración inicial.

b) Se adjuntan los enlaces a las guías de *hardware* específicas de los diferentes modelos de dispositivos disponibles:

- *Hardware Guide PSA-300* [REF11]
- *Hardware Guide PSA-3000* [REF12]
- *Hardware Guide PSA-5000* [REF13]
- *Hardware Guide PSA-7000* [REF14]

c) Los pasos a seguir para la creación de la configuración inicial de los dispositivos y poder acceder a la interfaz de administración vía web se encuentran en la sección "*Console and initial configuration*" de dichas guías.

Despliegue en formato virtual:

a) La solución está disponible en diferentes formatos virtuales:

- *VMWare*
- *Hyper-V*
- *KVM*
- *AWS*
- *Azure*

b) Especificaciones recomendadas para los "*appliances*" virtuales:

	PSA-3000-V	PSA-5000-V	PSA-7000-V
RAM	8 GB	8 GB	32 GB
CPU	4 vCPU	4 vCPU	8 vCPU
Disco	40 GB	40 GB	40 B

Las indicaciones detalladas para un despliegue correcto en los diferentes entornos descritos, se encuentra en la siguiente documentación online: 9.1R1 PCS and 9.1R1 PPS Virtual Appliance Deployment Guide. [REF15]

40. El producto permite la instalación de componentes adicionales, indicados previamente en el apartado 4.4.3 PREREQUISITOS:

a) ***Plugin ESAP***: se instala en *Authentication > Endpoint Security > Manage Endpoint Security Assessment Plugin Version*. Documentación relacionada con pasos a seguir: Endpoint Security Assessment Plug-In (ESAP). [REF 16]

b) ***Pulse Secure Behaviour Analytics Database***: se instala en: *System > Behavioral Analytics*. Para ver más documentación relacionada con los pasos a seguir: Behavioral Analytics. [REF17]

c) ***Fingerprint Database:*** se sube a través de la interfaz de administración en: *Authentication > Auth Server > Local Profiler.*

d) ***Third Party Integration Application*:** se sube a través de la interfaz de administración.

41. Para mayor detalle en el proceso de instalación se puede consultar la guía de la documentación: *Installation, Configuration and Start-Up Procedure.* [REF18]

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO – FIPS NIVEL 1

42. La solución de PPS de Pulse Secure cumple la normativa de FIPS Nivel 1 como se indica en la documentación del producto: *FIPS Level 1 Support (Software FIPS)*. [REF19]

43. **Se debe habilitar la compatibilidad con el modo de seguridad 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.

44. 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.

45. 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 *System > Status > Active Users.*

46. Si la plataforma cuenta con aceleración de *hardware*, esta estará deshabilitada para el procesamiento SSL ya que la aceleración de *hardware* no cumple con la validación FIPS.

47. Durante la activación del modo seguro, el servidor web se reinicia y permite solo el uso exclusivo de los protocolos configurados.

48. Para habilitar el modo seguro se deberán seguir los siguientes pasos:

    - Acceder a *System > Configuration > Security > Inbound SSL options*.
    - En la opción *FIPS SSL Mode option*, seleccionar *Turn on FIPS mode*.
    - Una vez activado el soporte FIPS Nivel 1, se deben realizar los siguientes cambios:

      a) En Allowed SSL and TLS version, seleccionar la opción *Accept only TLS 1.2 and later.*

      b) En *Allowed Encryption Strength*, se establecen los cifrados de compatibilidad máxima. Se debe seleccionar la opción *Perfect Forward Secrecy o Ephemeral Diffie Hellman (ECDHE).*

c) En *Encryption Strength*, se selecciona la opción *Do not allow connections from browsers that only accept weaker ciphers.* 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 FIPS Nivel 1 está habilitado.

6.2 AUTENTICACIÓN

6.2.1 AUTENTICACIÓN REMOTA

49. En el "*framework*" de administración de acceso de Pulse Secure, la página de inicio, el "*realm*" (forma de autenticación), y las configuraciones de servidor AAA están asociadas. Estas determinan el acceso y la función del usuario. Un usuario envía credenciales a través de una página de inicio de sesión, que especifica un "realm", que a su vez está asociado a un servidor AAA.
50. 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 verificarlo, el servidor envía la aprobación. Si el "*realm*" también usa el servidor de directorio/atributo, el servidor AAA envía la información del grupo del usuario e información de atributo del usuario. Posteriormente, el "*framework*" de administración de acceso evalúa las reglas de asignación de roles del "*realm*" para determinar los roles de usuario que se aplican a la sesión.
51. Un "*realm*" de autenticación, como se ha indicado en el apartado 4.4.1.1 *AUTHENTICATION REALM*, especifica las condiciones que los usuarios deben cumplir para iniciar la sesión en el sistema. Este consta de un servidor de autenticación, un servidor de directorio, una política de autenticación y unas reglas de asignación de funciones.
52. La configuración de "*realms*" para usuarios y administradores se puede consultar en los apartados 6.3.1.4 CONFIGURACIÓN DE *REALM* PARA ADMINISTRADORES y 6.3.2.4 CONFIGURACIÓN DE *REALM* PARA USUARIOS de este documento.
53. Por otro lado, para la creación de un nuevo servidor remoto, se debe acceder a *Authenticaction > Auth*. Servers y seleccionar el tipo de servidor deseado. Después, se deberá seleccionar *New Server* e introducir la información requerida. El *framework* de gestión de acceso Pulse Secure admite los siguientes tipos de servidores AAA:

    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.

54. La información detallada sobre los diferentes servidores de autenticación disponibles en el producto se puede consultar en el siguiente enlace: AAA Servers. [REF20]

55. Para los accesos de los administradores, **se recomienda hacer uso de un segundo factor** como pueden ser el servidor de TOTP integrado en la solución. Para esto es preciso configurar el mismo en la solución a través de las siguientes indicaciones: *Using a Time-Based One-Time Password (TOTP) Authentication Server* [REF21]

56. Una vez realizada la configuración del segundo factor de autenticación, se configura en el "*realm*" un segundo servidor de autenticación para el acceso de administradores en *Administrators > Admin Realm.*

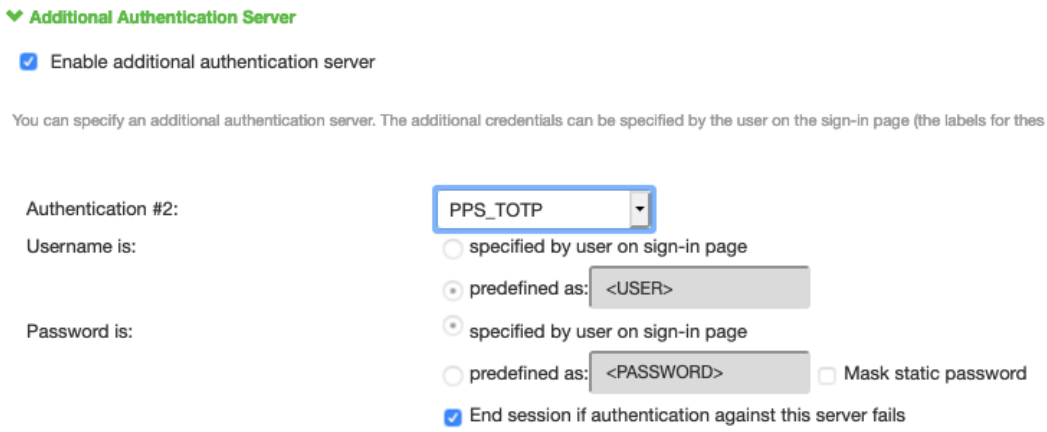

Ilustración 6-1. Configuración servidor de autenticación adicional

57. Esto se explica en mayor detalle en el apartado 6.3.1.2 CONFIGURACIÓN DE USUARIOS ADMINISTRADORES.

6.2.2 AUTENTICACIÓN LOCAL

58. Para la autenticación, tanto de administradores como de usuarios comunes, es posible hacer uso del "*framework*" de autenticación de la solución.

59. En el caso de los administradores, se recomienda mantener en la base de datos local exclusivamente el usuario *Super Admin* generado al inicio de la configuración de la

solución y, posteriormente, proceder a dar acceso administrativo a través de autenticación remota de administradores mediante elementos corporativos como pueden ser los servicios de Directorio Activo o LDAP.

60. La configuración de la autenticación local de usuarios se divide en administradores y usuarios. Los pasos para configurar esta autenticación se describen en los apartados 6.3.1.1 CONFIGURACIÓN DEL SERVIDOR DE AUTENTICACIÓN PARA ADMINISTRADORES LOCALES y 6.3.2.1 CONFIGURACIÓN DE SERVIDOR DE AUTENTICACIÓN PARA USUARIOS NO ADMINISTRADORES.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

61. Una vez realizada la configuración inicial, tanto para el formato virtual como para el físico, a través de la consola CLI se encuentra disponible la consola *Administrator Web Console*. Tras la configuración inicial, no se requiere el uso de la CLI ya que la gestión general de la solución se realizará siempre bajo la consola de administración accesible vía web.

62. Para acceder a la interfaz de administración web se debe acceder a: *https://<FQDN>/admin.*

63. Existe la posibilidad de configurar un usuario y contraseña para el acceso a la CLI (ver apartado 6.5.3 SEGURIDAD DE GESTIÓN DEL DISPOSITIVO), mediante la *opción Toggle Password Protection for the console* a través de la CLI. Sin embargo, es importante tener en cuenta que, si se pierden las credenciales, no se podrá acceder a la CLI y no se podrá resetear la clave del administrador principal.

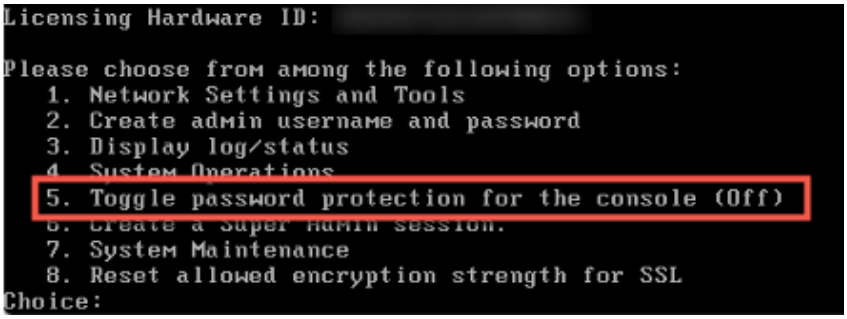

Ilustración 6-2. Configuración de clave de acceso para el CLI

64. Bajo la sección *Administrators > Admin Realms > Realm*, se encuentran medidas de seguridad adicionales para el acceso de los administradores.

65. En la parte *Authentication Policy* (políticas de autenticación), se encuentran elementos de seguridad adicionales para restringir el acceso de administración de la solución, como pueden ser:

    a) ***Source IP*:** direcciones IP desde las que se puede acceder a la solución como administrador

    b) ***Browser*:** configuración de los navegadores permitidos para acceder.

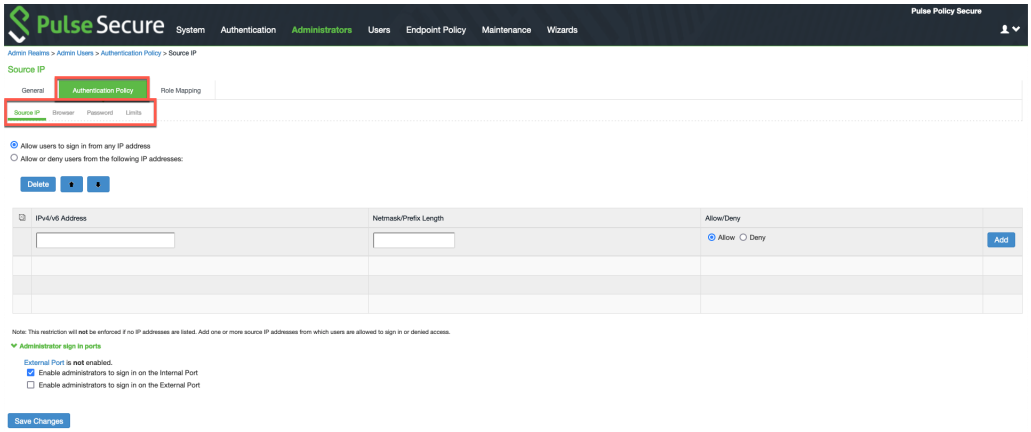

Ilustración 6-3. Apartado de *Source IP* dentro de *Authentication Policy*

66. 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 a través de soluciones corporativas como AD, LDAP o RADIUS.

6.3.1.1 CONFIGURACIÓN DEL SERVIDOR DE AUTENTICACIÓN PARA ADMINISTRADORES LOCALES

67. Por defecto, la solución tiene un servidor de autenticación para administradores locales creado, como los otros elementos explicados en los siguientes apartados, para garantizar el acceso del administrador creado durante la configuración inicial. Aquí es donde se pueden agregar administradores locales adicionales.

68. La configuración del servidor de autenticación local se encuentra bajo la opción: *Authentication > Auth Servers.*

69. Existe una base de datos de administradores locales que se encuentra por defecto y no puede ser borrada. En caso de necesitar crear un servidor de autenticación local adicional, seguir los siguientes pasos:

    - Acceder a *Authentication > Auth Servers* y seleccionar *Local Authentication*.
    - Seleccionar *New Server*.
    - Finalmente, completar la información necesaria y guardar la configuración.

70. Para información más detallada se recomienda acceder a la documentación: *Configuring the Local Authentication Server*. [REF22]

6.3.1.2 CONFIGURACIÓN DE USUARIOS ADMINISTRADORES

71. Para la creación de usuarios administradores en un servidor de autenticación local ya existente, se han de seguir los siguientes pasos:

    - Acceder a *Authentication > Auth Server > <Servidor de Autenticación Local Creado>*.
    - Acceder a *Admin Users* para ver la página de configuración.
    - Especificar un nombre de usuario, seleccionar el *realm* y elegir la opción *Add*.

- Guardar la configuración.

72. Una vez configurado el servidor de autenticación se deberá aumentar la seguridad de las contraseñas *desde Admin Realms > Admin Users > Authentication Policy > Password* realizando los siguientes cambios:

    a) Se debe establecer una longitud mínima de 12 caracteres.

    b) Debe tener al menos 3 dígitos o 3 letras.

    c) La contraseña deberá estar formada por un conjunto de letras en mayúsculas y minúsculas, número y símbolos (“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”).

    d) La contraseña deberá ser diferente del nombre de usuario, y de la anterior contraseña.

    e) Con respecto al almacenamiento de la contraseña, se debe usar *Strong Hash.*

    Nota: Una vez seleccionada esta opción, se deshabilitan los protocolos de autenticación como CHAP, EAP-MD5 y MS-CHAP (v1/v2).

    f) Con respecto a la gestión de contraseñas, se recomienda:

    - Permitir a los usuarios cambiar sus contraseñas.
    - Forzar el cambio de contraseñas cada 60 días.
    - Avisar a los usuarios 7 días antes de la expiración de la contraseña.

    g) Con respecto al bloqueo de cuenta, se deberá configurar el máximo número de intentos fallidos (se recomienda dar un valor de 3) y el tiempo de bloqueo de sesión (se recomiendan 30 minutos).

    h) Se recomienda configurar, al menos, un segundo factor de autenticación (descritos en el apartado 6.5.4 SEGURIDAD DE AUTENTICACIÓN) pudiendo ser este TOTP o RADIUS.

73. La configuración de otros parámetros de seguridad de los usuarios se detalla en el apartado 6.5 Configuración de Seguridad.

6.3.1.3 CONFIGURACIÓN DE ROLES PARA ADMINISTRADORES

74. Dentro de la solución existen dos (2) roles predeterminados para los administradores:

    a) ***Administrators*:** política general para administradores.

    b) ***Read-Only Administrators*:** política con permisos de solo lectura sin capacidad de realizar cambios.

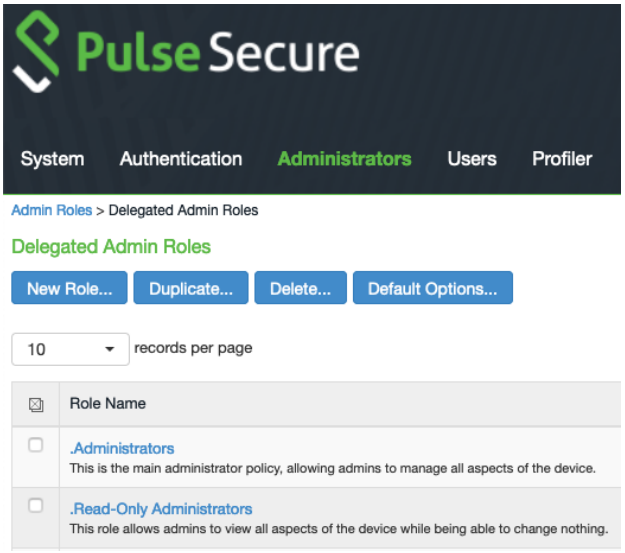

Ilustración 6-4. Configuración de roles para administradores

75. Para la creación de nuevos roles personalizados y adaptados a las necesidades corporativas, se han de seguir los siguientes pasos:
    - Acceder a *Administrators > Admin Roles > Delegated Admin Roles*.
    - Seleccionar *New Role.*
    - Configurar los parámetros deseados y guardar la configuración.
76. También existe la posibilidad de adaptar los roles existentes modificando sus parámetros. Para ello:
    - Acceder a *Administrators > Admin Roles >* <Seleccionar Role> *> General*
    - Modificar los parámetros deseados.

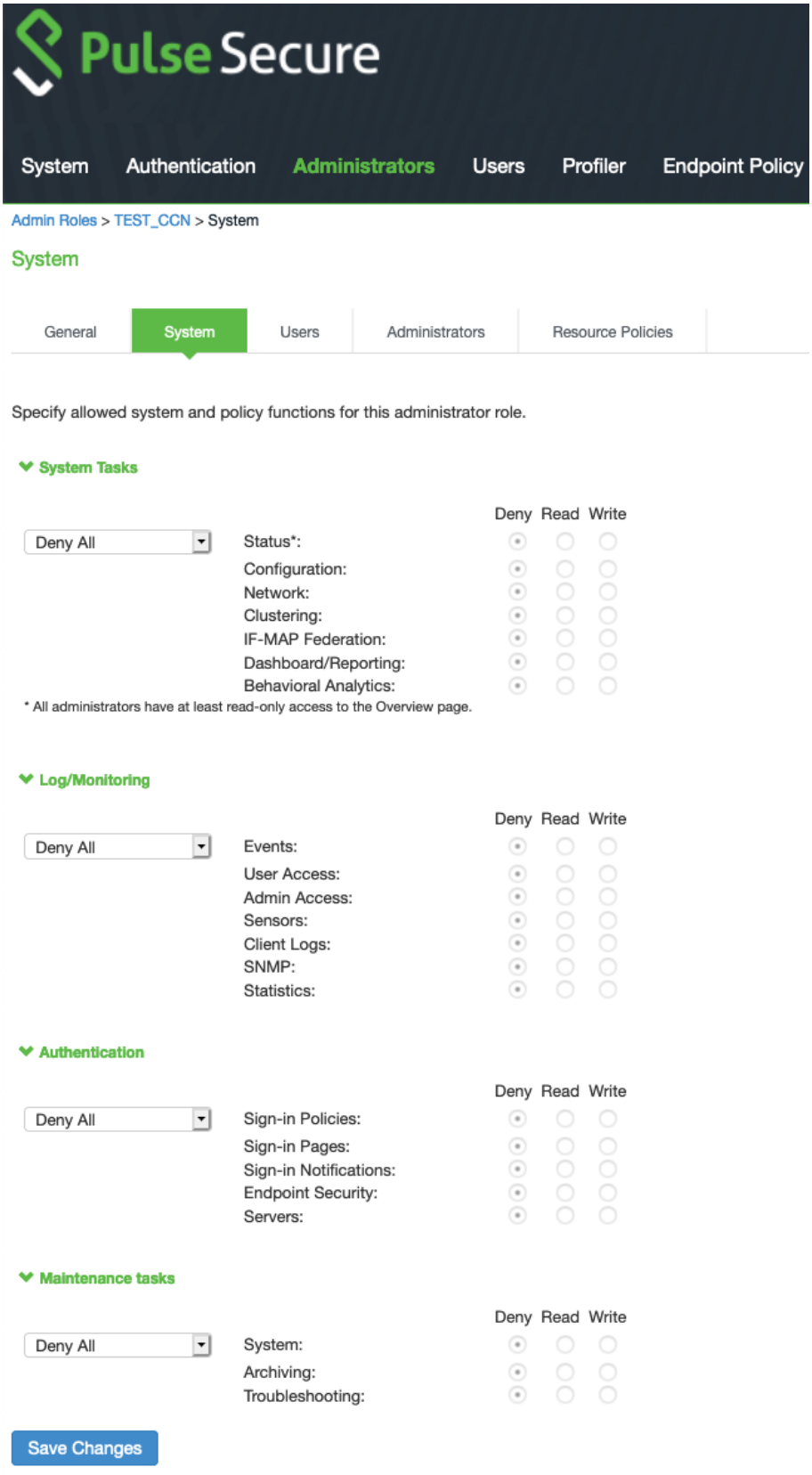

Ilustración 6-5. Modificación de los roles existentes

77. Se recomienda restringir el acceso administrativo estrictamente necesario para el role *Super Admin*, *Operadores*, etc.

78. El parámetro *Session Option*s establece los tiempos y permisos de uso que aplican a cada sesión establecida según el role. Para modificar este parámetro se ha de acceder a *Administrators > Admin Role > <Role específico> > General > Session Options.*

79. **Se recomienda establecer los siguientes valores:**

    a) *Idle Timeout*: 5 minutos.

    b) *Max. Session Length*: 6 min.

80. Adicionalmente, **se debe activar la opción *HTTP Only Device Cookie* y configurar un mensaje de aviso y consentimiento en el inicio de sesión**. Para realizar esto se debe acceder a *Administrators > Admin Role > <Role específico> > General > UI Options*. Para mayor detalle se recomienda consultar el siguiente enlace: *Customizing UI Options*. [REF23]

6.3.1.4 CONFIGURACIÓN DE *REALM* PARA ADMINISTRADORES

81. 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.*

82. Para la creación de un *realm* se han de seguir los siguientes pasos:

    - Acceder a *Administrators > Admin Realm* y seleccionar *New*.
    - Incluir la información solicitada en la página de creación y seleccionar *Save Changes*.
    - El detalle de la creación de *realms* se puede consultar en la documentación: *Creating an Authentication Realm*. [REF24]

83. Para configurar las políticas de autenticación de los *realms*, acceder a *Administrators > Admin Realm > Administrators > Authentication Policy*. Configurar los parámetros deseados:

    - ***Source IP***: Se recomienda especificar las IPs y redes desde las cuales los administradores podrán acceder a la consola web de gestión.
    - ***Browser***: En el caso de usar un navegador específico, se debe configurar este elemento con el *User-Agent* del navegador, para maximizar la seguridad.
    - ***Certificate***: Se recomienda hacer uso de la comprobación del certificado de cliente, permitiendo solo los accesos a la gestión del entorno a conexiones que presente dicho certificado.

- ***Host Checker***. Aplica reglas de *Host Checker* a la conexión. El listado detallado de los puntos que se pueden verificar se encuentra en el siguiente enlace de la documentación: *Configuring Host Checker Rules*. [REF 25]

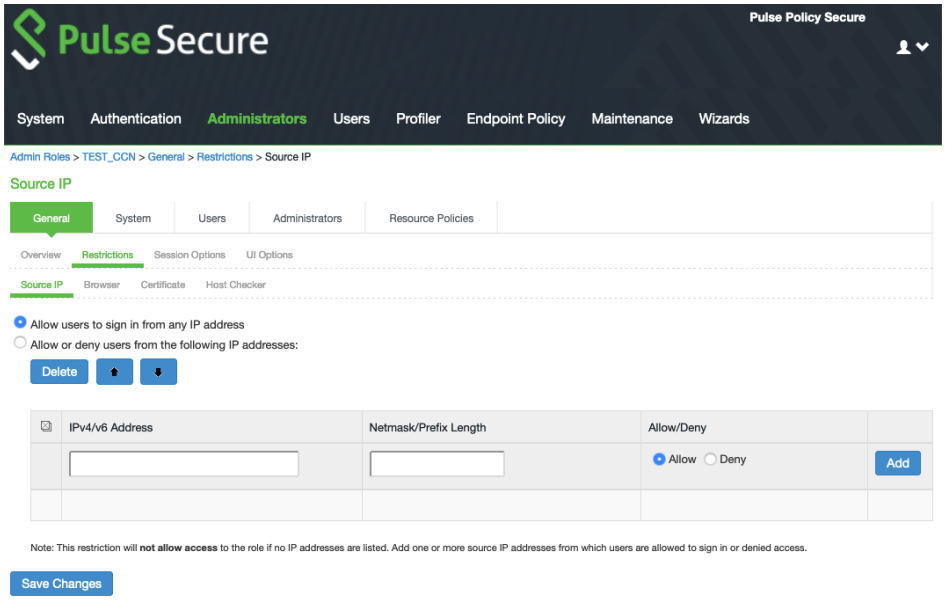

Ilustración 6-6. Restricciones de conexión para IPs de origen

84. También se puede configurar el rol *Mapping* de tal forma que se seleccione el rol de manera dinámica a través de una serie de criterios determinados. Para ello, se debe acceder a *Administrators > Admin Realm > Admin Users > Role Mapping* y configurar o crear las reglas deseadas. Para más detalle de la configuración se recomienda acceder a la documentación: Configuring Role Mapping. [REF26]

6.3.1.5 CONFIGURACIÓN DE *SIGN-IN POLICIES* PARA ADMINISTRADORES

85. La *Sign-in Policy* define tanto la URL a través de la cual se proporcionará el acceso, como la forma de autenticarse del usuario (*realm*). La política por defecto para administradores es */admin*. **Se recomienda el cambio de la URL por defecto a una adaptada y más segura.**

86. Para la creación de una nueva *Sign-in Policy*, se han de seguir los siguientes pasos:

    - Acceder a *Authentication > Signing In > Sign-in Policies*.
    - Seleccionar *New URL*.
    - Seleccionar *Administrators*, para especificar que los usuarios administradores podrán acceder utilizando la URL. Por defecto, se encuentra seleccionado *Users.*
    - Introducir la URL deseada en *Sign-in URL*.
    - En el apartado *Authentication Realm*, seleccionar los *realms* que utilizarán dicha política.
    - Guardar los cambios.

87. Para mayor detalle sobre la creación y configuración de *Sign-in Policy* se puede consultar la documentación: *Configuring Administrator Sign-in Policies*. [REF27]

6.3.2 CONFIGURACIÓN DE USUARIOS

88. Para la autenticación de los usuarios es posible el uso tanto de una base de datos local en la propia solución, como el uso de métodos de autenticación corporativos como pueden ser AD, LDAP y RADIUS.

6.3.2.1 CONFIGURACIÓN DE SERVIDOR DE AUTENTICACIÓN PARA USUARIOS NO ADMINISTRADORES

89. Por defecto, la solución tiene un servidor de autenticación para administradores locales ya creado. Para poder dar acceso a usuarios se requiere habilitar un servidor de autenticación externo soportado para usuarios como pueden ser los servidores AD, LDAP, RADIUS, etc.

90. La configuración del servidor de autenticación local se encuentra bajo la opción: *Authentication > Auth Servers.*

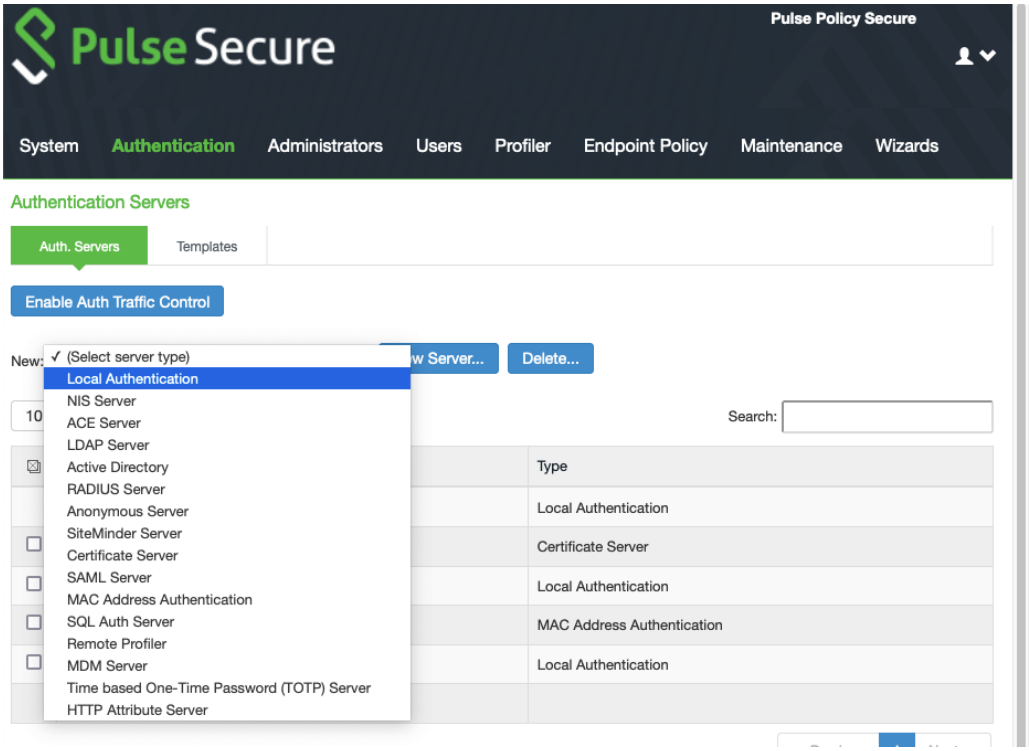

Ilustración 6-7. Configuración del servidor de autenticación

91. Para más información se recomienda acceder a la documentación: AAA Servers. [REF20]

6.3.2.2 CONFIGURACIÓN DE USUARIOS

92. Para el uso de usuarios locales es necesario configurarlos previamente. Para crear nuevos usuarios:

    - Acceder a *Authentication > Auth Server*.

- Seleccionar el servidor en el cual se quieran añadir las cuentas de usuario y seleccionar la pestaña *Users*.
- Seleccionar *New* e introducir la información del usuario.
- Finalmente guardar la información.

93. Una vez configurado el servidor de autenticación se deberá aumentar la seguridad de las contraseñas accediendo desde *Authentication Server > Auth. Server > Servidor de Autenticación local > Authentication Policy > Password* realizando los siguientes cambios de seguridad:

    a) Se debe establecer una longitud mínima de 12 caracteres.

    b) Debe tener al menos 3 dígitos o 3 letras.

    c) La contraseña deberá estar formada por un conjunto de letras en mayúsculas y minúsculas, número y símbolos (“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”).

    d) La contraseña deberá ser diferente del nombre de usuario, y de la anterior contraseña.

    e) Con respecto a la gestión de contraseñas, se recomienda:

        - Permitir a los usuarios cambiar sus contraseñas.
        - Forzar el cambio de contraseñas cada 60 días.
        - Avisar a los usuarios 7 días antes de la expiración de la contraseña.

    f) Con respecto al bloqueo de cuenta, se deberá configurar el máximo número de intentos fallidos (se recomienda dar un valor de 3) y el tiempo de bloqueo de sesión (se recomiendan 30 minutos).

94. La configuración de los parámetros de seguridad de los usuarios se detalla en el apartado 6.5 Configuración de Seguridad.

6.3.2.3 CONFIGURACIÓN DE ROLES PARA USUARIOS

95. Un rol de usuario es una entidad que define los parámetros de sesión del usuario, la configuración de personalización, y las funciones de acceso habilitadas. Dicho rol no especifica el control de acceso a los recursos ni otras opciones basadas en recursos para una solicitud individual. El administrador puede definir múltiples roles de usuario para los usuarios finales. Un ejemplo sería:

    a) **Empleados:** usuarios que requieren acceso a todos los recursos de la empresa.

    b) **Contratistas:** usuarios que trabajan por contrato y requieren acceso a recursos de red específicos.

    c) **Invitados:** usuarios que visitan la empresa y requieren acceso limitado a los recursos de la red.

96. Para la creación de roles de usuario, se han de seguir los siguientes pasos:

- Acceder a *User > User Roles*.
- Seleccionar *New Role* e introducir el nombre del *role* deseado y, opcionalmente, una descripción.

97. Para modificar roles existentes o configurar aquellos recién creados, se deben seguir los siguientes pasos de la documentación: *Configuring User Roles*. [REF28]

6.3.2.4 CONFIGURACIÓN DE *REALM* PARA USUARIOS

98. Un "*realm*" de autenticación especifica las condiciones que los usuarios deben cumplir para iniciar sesión en el sistema.
99. Para crear un "*realm*" para usuarios no administradores, seguir los siguientes pasos:
    - Acceder a *Users > User Realms* y seleccionar *New*.
    - En el apartado *Servers*, seleccionar el tipo de autenticación deseada (Local o mediante Servidor externo).
    - Finalmente guardar con *Save Changes*.
100. El detalle de la creación y configuración de "*realms*" se puede consultar la documentación: *Creating an Authentication Realm*. [REF24]

6.3.2.5 CONFIGURACIÓN DE SIGN IN POLICY PARA USUARIOS

101. 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 usuarios.**
102. Para la creación de una nueva *Sing-in Policy*, seguir los siguientes pasos:
    - Acceder a *Authentication > Signing In > Sign-in Policies*.
    - Seleccionar *New URL*.
    - Seleccionar *Users*, para especificar que los usuarios no administradores podrán acceder utilizando la URL.
    - Introducir la URL deseada en *Sign-in URL*.
    - En el apartado *Authentication Realm* seleccionar qué "realms" utilizarán dicha política.
    - Guardar cambios con la opción *Save Changes*.
103. El detalle de la creación y configuración de *Sign-in Policies* se puede consultar en detalle en la documentación online: *Configuring User Sign-In Policies*. [REF29]

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

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

105. Una vez se tenga acceso a la interfaz de usuario de administrador a través del navegador se recomienda activar/desactivar las configuraciones de IPv4/v6 en la parte de configuración de redes. Esto se puede encontrar en *System > Network.*

106. Posteriormente, toda la configuración adicional, bien sea de interfaces, servicios, etc., se gestionará a través de la interfaz de usuario administrador vía WEB (siempre **HTTPS**).

107. Se indican detalles de cómo configurar las interfaces de red del puerto interno y externo en el apartado 6.5.3 SEGURIDAD DE GESTIÓN DEL DISPOSITIVO.

108. Para más información y detalles sobre la configuración véase por favor el manual en línea la sección de: *Network and Host Administration*. [REF30]

6.5 CONFIGURACIÓN DE SEGURIDAD

6.5.1 SESIÓN DE USUARIOS

109. En los siguientes pasos se especifican parámetros y protocolos para el bastionado de comunicaciones en las sesiones de usuario.

110. **Se debe deshabilitar la sesión de itinerancia (*roaming*) o limitar la subred para los 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 interceptada y reutilizada por un atacante e implicará que un usuario final deba volver a autenticarse cuando se cambie la dirección IP de origen. Para deshabilitar esta opción:

- **Usuarios:** acceder a *Users > User Roles > <nombre del rol> > General > Session Options: Roaming Session* y seleccionar “Disabled”.
- **Administradores:** acceder a *Administrators > Admin Roles > <nombre del rol> > General > Session Options: Roaming Session* y seleccionar “Disabled”.

111. **Se deben configurar los tiempos máximos de sesión**: Esta opción asegura que las sesiones de usuarios estén limitadas a una duración establecida y, si se roba una sesión, solo estará activa hasta que se agote el tiempo de espera de la sesión.

- Acceder a *Users > User Roles > <role name> > General > Session Options: Session lifetime lengths*.
- Configurar el valor deseado. Se recomienda configurar un valor bajo, por ejemplo 24 hordas.

112. Se recomienda usar la opción de bloqueo de IP para bloquear ataques de contraseña por fuerza bruta. Se debe tener en cuenta que si los usuarios acceden al dispositivo Pulse Secure a través de un balanceador de carga o proxy, este no será viable ya que indicará que provienen de la misma dirección IP. La configuración se realiza desde *Security > Configuration > Security > Miscellaneous: Lockout Options.*

113. **Se ha de deshabilitar la opción *"Allowing saving logon information"* y *"Dynamic Certificate Trust"*** para la configuración de conexiones en *Pulse Secure Client* desde *Users > Pulse Secure Client > Connections > <connection> > Options*. De esta forma será necesario realizar la autenticación e introducir las credenciales cada vez que se trate de acceder al producto.

6.5.2 SEGURIDAD DE SERVIDOR

114. **Se debe deshabilitar 3DES en las conexiones SSL:**

- Acceder a *System > Configuration > Security > SSL Options > Inbount SSL Options*.
- En el apartado *Allowed Encryption Strength* desmarcar las casillas con cifrados 3DES.

115. Para mayor información, se puede consultar el siguiente artículo donde se indica cómo desactivar los conjuntos de cifrado 3DES: *KB40706 - Disable 3DES cipher suites for Pulse Connect Secure or Pulse Policy Secure.* [REF31]

116. Además, se deben configurar los ajustes SSL entrantes para **aceptar solo TLS 1.2 y versiones posteriores**. Ver apartado 6.1 Modo de operación seguro – FIPS Nivel 1.

117. **Se debe habilitar *Perfect Forward Secrecy* o configurar *Ephemeral Diffie-Hellman (ECDHE)* en la parte superior de la lista de suites de cifrado**. Para ello:

- Acceder a *Configuration > Security > Inbound SSL Options*.
- Seleccionar el botón para *Perfect Forward Secrecy*.

118. **Se debe deshabilitar todos los cifrados TLS_RSA para evitar la amenaza "*Return Of Bleichenbacher's Oracle Threat" (ROBOT).***

6.5.3 SEGURIDAD DE GESTIÓN DEL DISPOSITIVO

119. Se deberá limitar el acceso administrativo solo a las interfaces internas o de administración. Para ello:

- Deshabilitar el acceso de administrador desde el puerto externo que aparece como configuración predeterminada.
- Acceder a *Administrators > Admin Realms > <realm name> > Authentication Policy > Source IP*.
- Asegurarse de que la opción "*Enable administrators to sign in on the External Port*" no se encuentre activada.

120. Se debe bloquear el acceso a la consola serie con una contraseña. Esto se realiza desde la interfaz de línea de comandos a través del puerto de la consola. No se debe 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.* [REF32]

121. Se deben agregar restricciones de nivel de *realm* para roles y dominios de administración, añadiendo así protección adicional. Estas opciones se encuentran en: *Administrators > Admin Realms > Authentication Policy.*

122. Además, se recomienda el cifrado de las exportaciones de configuración de *backup* y se deberán almacenar de forma segura. Esto se realiza desde: *Maintenance > Import/Export.*

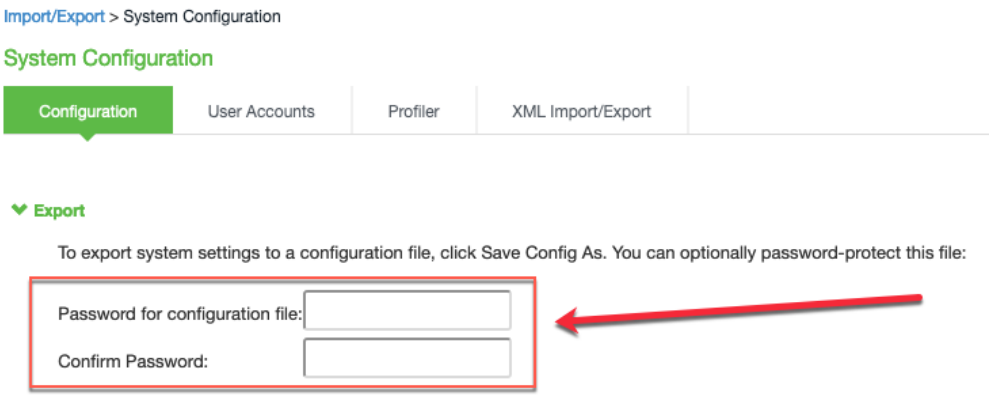

Ilustración 6-8.Campos de contraseña para la exportación de configuración

123. No se deberán usar nombres de inicio de sesión o contraseñas de administradores populares, como pueden ser "*admin*" o "*administrador*". **Se debe elegir un nombre de usuario administrador adecuado y contraseña acorde a criterios ya descritos en apartados anteriores.**

124. Además**, se deberá cambiar el nombre de la URL de inicio de sesión predeterminada** para el administrador de /admin a un nombre no estándar. Para realizar esto se debe acceder a *Authentication > Signing in > Sign-in Policies.*

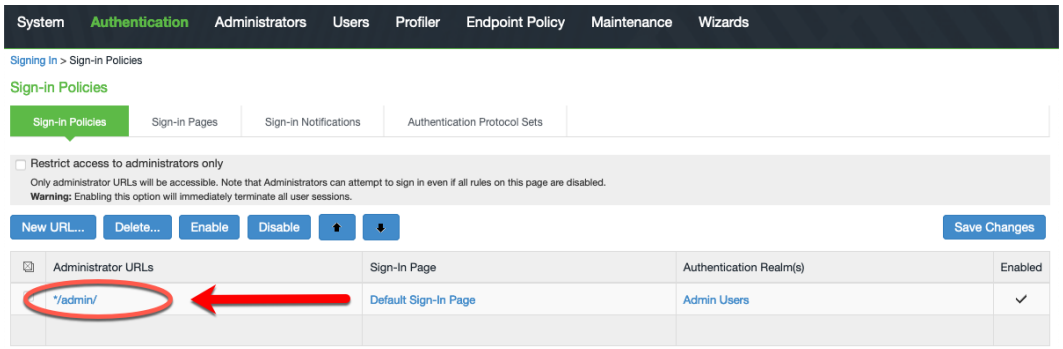

Ilustración 6-9. Configuración de *Sign-In* URL para administradores

125. Se recomienda que, siempre que sea posible, se haga uso de la configuración de dos (2) interfaces de red (puerto externo e interno).

a) La configuración del puerto interno se realiza desde *System > Network Internal Port > Settings.*

b) La configuración del puerto externo se realiza desde *System > Network > External Port > Settings.*

126. Por último, si el dispositivo está usando una configuración de una interfaz de red (solo puerto interno) y SNMP está habilitado, se debe verificar que el puerto UDP 161 esté bloqueado para el acceso externo.

6.5.4 SEGURIDAD DE AUTENTICACIÓN

127. **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 de certificado de cliente son recomendaciones disponibles, así como el uso de soluciones de terceros o propias que utilice 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*. [REF33]
    - La integración de un segundo factor en RADIUS se realiza configurando un servidor de autenticación RADIUS, tal como se ha visto en el apartado *6.3.1.1 CONFIGURACIÓN DEL SERVIDOR DE AUTENTICACIÓN PARA ADMINISTRADORES LOCALES* y *6.3.2.1 CONFIGURACIÓN DE SERVIDOR DE AUTENTICACIÓN PARA USUARIOS NO ADMINISTRADORES*. Posteriormente se debe añadir dicho servidor en el apartado *realm* (*Users* > *User Realm*) como segundo factor de autenticación. Para mayor información, se recomienda acceder al siguiente enlace de la documentación: *Configuring Authentication with a RADIUS Server*. [REF34]

128. En el caso de usar LDAP, se recomienda habilitar el uso de LDAPS o Start TLS. El detalle de dicha configuración se puede consultar en el siguiente enlace: *Configuring Authentication with a LDAP Server*. [REF35]

129. Para activar esta opción se ha de acceder a *Authentication* > *Auth Server* > *LDAP Server* y seleccionar *LDAPS* o *Start TLS*.

Ilustración 6-10. Configuración LDAPS y *Start TLS* para las comunicaciones LDAP

130. Con respecto al uso de directorio activo, el modo permitido por el producto es el estándar, el cual es el recomendado. Para mayor detalle se puede consultar el siguiente enlace de la documentación: *Configuring Authentication and Authorization with Active Directory Service (Standard Mode)*. [REF36]

6.5.5 SEGURIDAD DEL ENDPOINT

131. Se recomienda usar la solución de *Host Checker* (herramienta de verificación y obligación de cumplimiento) para garantizar que los clientes están ejecutando el software de seguridad corporativo requerido como el antivirus (verificando que el

mismo esté actualizado) o el *firewall* (verificando que este habilitado, parcheado, etc.)

132. El detalle de la configuración de las funcionalidades y la puesta en marcha se puede consultar en el siguiente enlace de la documentación: *Host Checker*. [REF37]

6.5.6 ACTUALIZACIONES Y NOTIFICACIONES DE SEGURIDAD

133. **Se recomienda suscribirse a las alertas de Pulse Secure para obtener avisos de seguridad y mantenerse al día sobre las actualizaciones de *software***. Los detalles 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.* [REF38]

134. Las actualizaciones de *software* deben realizarse por parte de un usuario administrador de forma manual. Ver el apartado 6.9 ACTUALIZACIONES.

6.6 GESTIÓN DE CERTIFICADOS

135. PPS utiliza la infraestructura de clave pública (PKI) para proteger los datos enviados a los clientes a través de la red. El producto hace uso de los distintos certificados indicados en el apartado 4.4.4 CERTIFICADOS para la correcta protección de sus comunicaciones.

136. La importación, creación y visualización de los certificados debe realizarse desde: *System > Configuration > Certificates > Device Certificates > Certificates*, tal como se ilustra en la siguiente imagen.

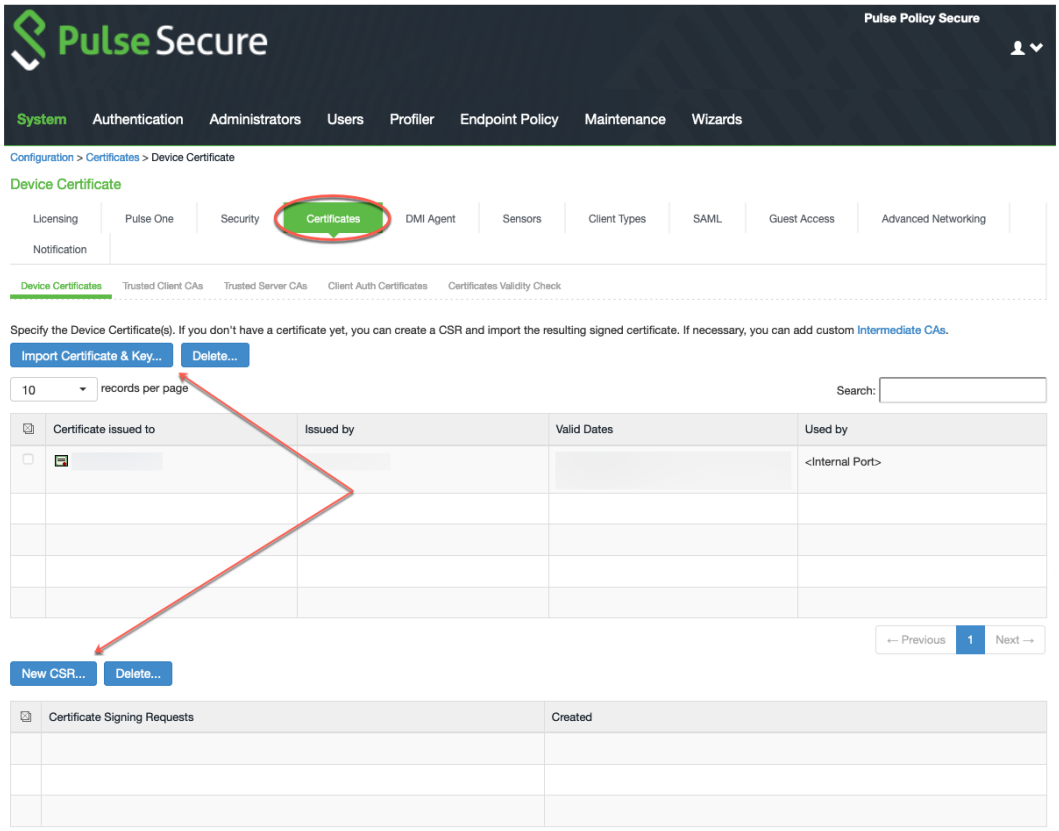

Ilustración 6-11. Gestión de Certificado

137. Una vez instalado el certificado, seleccionándolo se tiene la posibilidad de usar CRLs (*Certification Revocation Lists*) para el mismo.

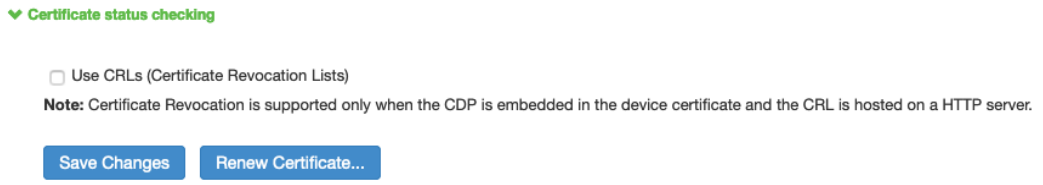

Ilustración 6-12. Configuración de CRLs (*Certificate Revocation Lists*)

138. Para el detalle de la configuración de los certificados del producto, se debe consultar el siguiente enlace de la documentación: *Certificate Security Administration* [REF39]. **Se debe hacer uso de RSA con claves de, al menos, 3072 bits de longitud, ECDSA con curvas P-256 o superior, y funciones hash SHA-256 o superior, en línea con las indicaciones de la guía CCN-STIC-807 Criptología en el ENS.**

139. A continuación, se describen las configuraciones de los certificados más relevantes.

6.6.1 CERTIFICADOS DE DISPOSITIVO

140. 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, al menos,

longitudes de clave de 3072b en caso de usar RSA o 256b en caso de utilizar ECDSA. Se han de seguir los siguientes pasos:

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

141. Una vez se reciba el certificado firmado de la CA, debe importarse en el dispositivo. Se han de seguir los siguientes pasos:

- Acceder a *System > Configuration > Certificates > Device Certificates.*
- En el apartado *Certificate Signing Requests*, seleccionar *Pending CSR*.
- Acceder a *Import signed certificate* y elegir el certificado.
- Finalmente seleccionar la opción *Import*.

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

- Acceder a *System > Configuration > Certificates > Device Certificates.*
- Seleccionar *Intermediate Device CAs* para acceder a la página de configuración.
- Seleccionar *Import CA certificate* y buscar el certificado deseado.
- Finalmente seleccionar *Import Certificate*.

6.6.2 CERTIFICADOS DE AUTORIDADES DE CERTIFICACIÓN

143. 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:

- Acceder a *System > Configuration > Certificates > Trusted Client CAs.*
- Seleccionar *Import CA Certificate*.
- Seleccionar el certificado deseado y elegir la opción *Import Certificate*.

144. 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:

- Acceder a *System > Configuration > Certificates > Trusted Server CAs.*
- Seleccionar *Import Trusted Server CA*.
- Seleccionar el certificado deseado y elegir la opción *Import Certificate*.

6.6.3 CERTIFICADOS DE CLIENTE

145. 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:

- Acceder a *System > Configuration > Certificates > Client Auth Certificates.*
- Seleccionar *Import Certificate & Key* para abrir la página de configuración.
- Completar la información requerida y elegir la opción *Import*.

6.7 SERVIDORES DE AUTENTICACIÓN

146. La solución de PPS puede interactuar y comunicarse con diferentes métodos y servidores de autenticación como los listados en la siguiente ilustración:

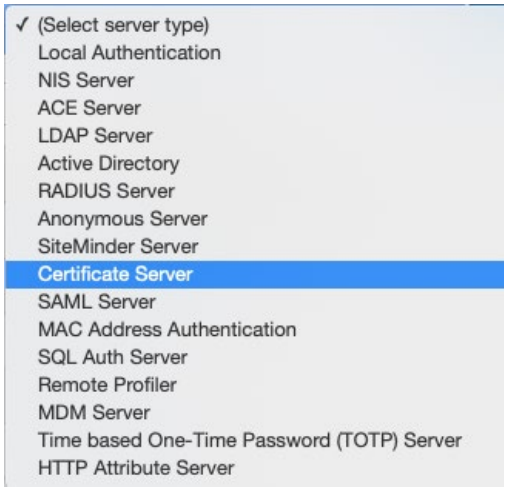

Ilustración 6-13. Servidores de Autenticación

147. La configuración de los diferentes servidores de autenticación se encuentra en: *Authentication > Auth Servers.*

148. Para información adicional sobre los servidores de autenticación, se puede acceder al siguiente enlace de la documentación: AAA Servers [REF20].

149. Algunas recomendaciones a seguir en los diferentes servidores de autenticación son:

Servidor de autenticación local:

a) Se debe establecer una longitud mínima de 12 caracteres.

b) Se deben activar las siguientes opciones:

- *Password must have at least 3 digits.*
- *Password must have at least 3 letters.*
- *Password must have mix of uppercase and lowercase letters.*
- *Password must be different from username.*
- *New password must be different from previous password.*
- *Password Storage type: Strong Hash*
- *Allow users to change their password.*

- *Force password change after 60 days.*
- *Prompt user to change their password 14 days before current password expire.*

c) Con respecto al bloqueo de la cuenta, se recomienda activar:

- *Maximum password attemps: 3*
- *Account Lockout period: 10*

Servidor LDAP:

a) Para el valor del parámetro *Connection*, se recomienda hacer uso de una de las siguientes dos opciones:

- LDAPS.
- Start TLS.

b) No se debe hacer uso de *Unencrypted*.

c) *Active Directory*. Se recomienda hacer uso de Kerberos o NTLM v2.

150. Además de las recomendaciones indicadas, en el apartado *6.5 CONFIGURACIÓN DE SEGURIDAD* se indica el uso del doble factor de autenticación y otros métodos recomendados para hacer uso del mismo.

6.8 SINCRONIZACIÓN

151. **La sincronización horaria** es esencial en los entornos virtuales y cloud, por lo que debe estar **configurada correctamente**.

152. Para configurar el servicio NTP, seguir los siguientes pasos:

- Acceder a *System > Status > Overview > System Date & Time.*
- Seleccionar *Edit*. En el apartado *Time Source* seleccionar *Use NTP Server.*
- Rellenar los datos de NTP.

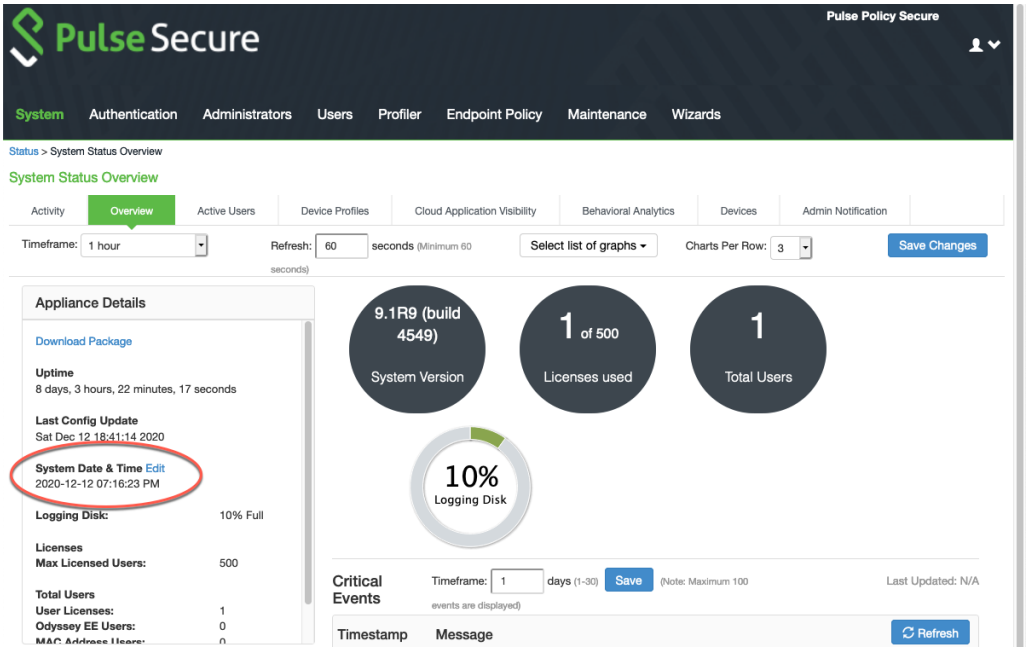

Ilustración 6-14. *"System Date & Time"* en el apartado "*System Status Overview*"

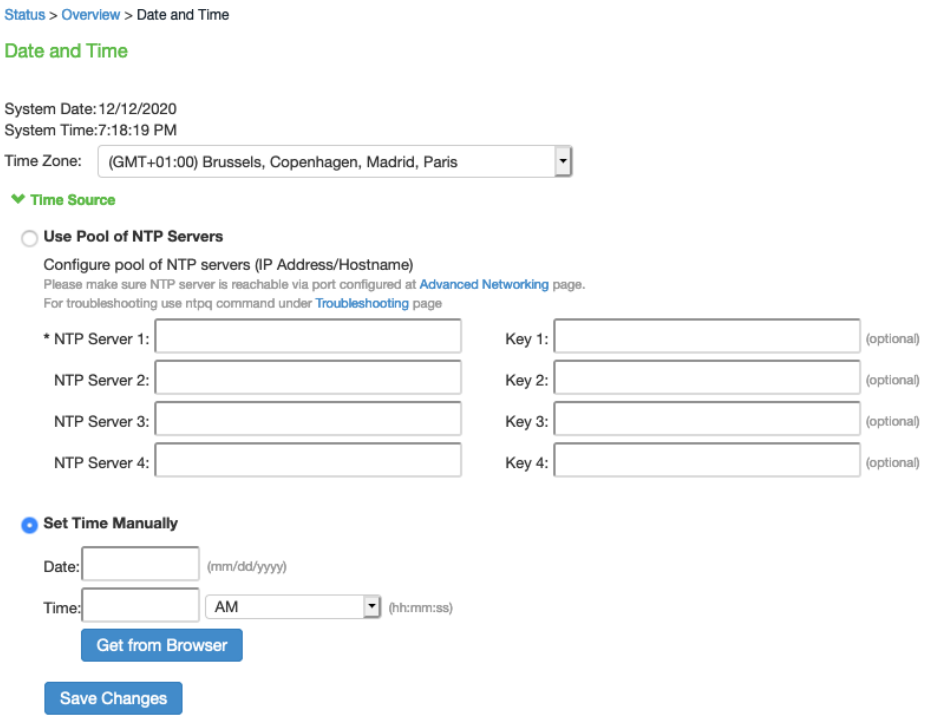

Ilustración 6-15. Configuración NTP

6.9 ACTUALIZACIONES

153. El dispositivo se envía con la imagen de *software* instalada. Sin embargo, esta puede no ser la recomendada y debe ser actualizada. Para actualizar el dispositivo a la imagen del *software* certificada, se deben seguir las instrucciones en la

documentación: *Downloading Pulse Policy Secure Software and License* [REF40] y, posteriormente, actualizar el dispositivo a la imagen del *software* obtenida. A través del portal de soporte (*https://my.pulsesecure.net*) [REF3] se pueden hacer las configuraciones pertinentes para recibir las notificaciones sobre disponibilidad de nuevas versiones y parcheados.

154. Las actualizaciones deben ser instaladas manualmente por un usuario administrador de la solución. La descarga del producto debe realizarse de acuerdo con 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.

155. Teniendo ya instalada la solución, se puede realizar una actualización del *firmware* para obtener la versión recomendada accediendo al portal de soporte de Pulse Secure con el usuario dado de alta en el mismo. Seguidamente se siguen los pasos indicados:

    a) Descargar el paquete de *software* recomendado en formato **.pkg* para su posterior instalación.

    b) Verificar su integridad con el SHA-2 mostrado en la propia página de descarga.

    c) Una vez descargado se procede a abrir la consola de administración en: *Maintenance > System > Upgrade / Downgrade.*

    d) En la opción de *Install Service Package,* se selecciona la opción de *File* para añadir el paquete que se ha descargado. Seleccionar la opción *Install*.

    e) En el siguiente enlace de la documentación se desarrolla con mayor detalle la actualización del *firmware*: *Installing the Service Package*. [REF41]

156. Para realizar la actualización del paquete de *software* se han de seguir los siguientes pasos:

    a) Se deberá descargar la versión a actualizar a través de la página *https://my.pulsesecure.net* [REF3], y se verificará su integridad con el hash SHA-2 de los mostrados en la misma página.

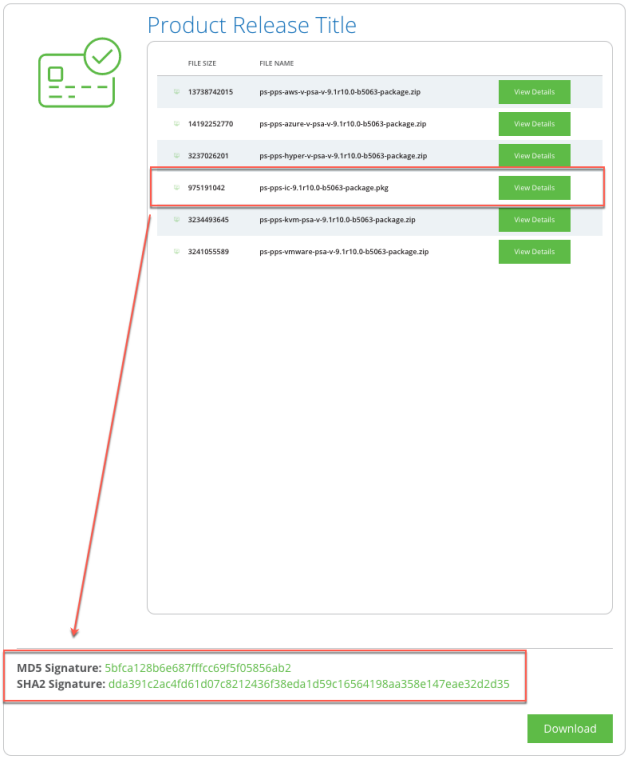

Ilustración 6-16. Pantalla de descarga de actualizaciones

b) A continuación, en el producto PPS se deberá acceder a *Maintenance > System Maintenace > Install Service Package > Upgrade/Downgrade.*

c) En el apartado *Install Service Package*, se deberá seleccionar la opción deseada y el fichero de actualización descargado previamente.

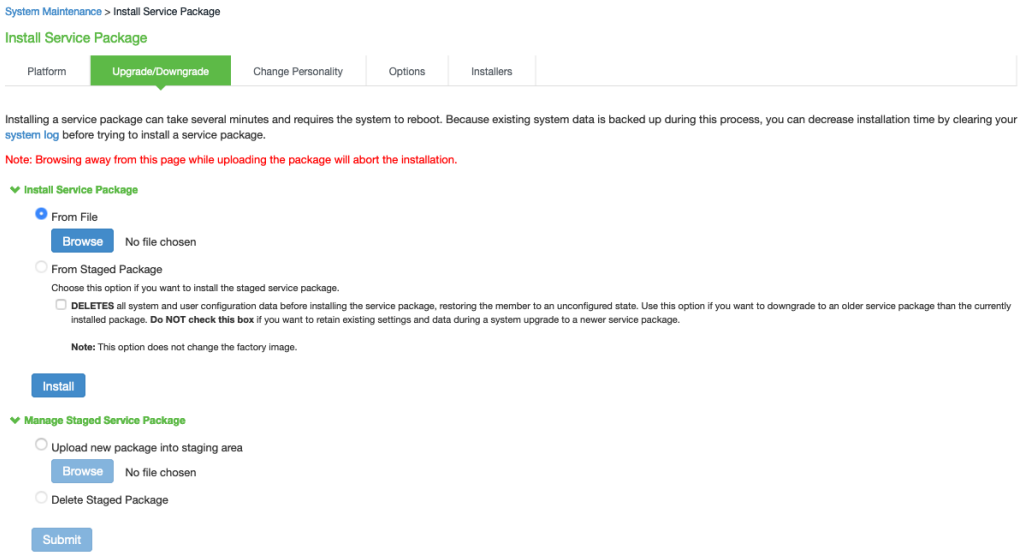

Ilustración 6-17. Instalación de paquetes de actualización

d) Finalmente, seleccionar *Install*.

157. Adicionalmente, se recomiendan los siguientes artículos relacionados con este aspecto:

    a) *KB40028 - [Customer Support Tools] How to download software / firmware for Pulse Secure products using the Licensing & Download Center at my.pulsesecure.net* [REF42]

    b) *KB12940 - Recommended procedure for upgrading PPS firmware* [REF43]

6.10 AUTO-CHEQUEOS

158. La solución PPS incluye funcionalidades de autoprotección para prevenir situaciones críticas y para recuperarse de ciertos eventos críticos.

159. Se deben activar las siguientes opciones:

- Acceder *a Maintenance > System > Options*.
- Activar la opción *Enable Kernel Watch Dog*. Esta opción reinicia automáticamente el sistema cuando el *kernel* se queda sin recursos clave o cuando se encuentra en punto muerto.
- Activar la opción *Prevent System Overload*. Dicha opción permite que PPS mitigue la carga bloqueando temporalmente los inicios de sesión y el acceso a algunos recursos una vez que la máquina llega a un nivel crítico en el uso de recursos.

6.11 SNMP

160. La solución de Pulse Secure PPS ofrece la posibilidad del uso de SNMP para controlar el estado del sistema. **Solo se debe usar de SNMPv3.**

161. Para configurar el agente SNMP se deben seguir los siguientes pasos:

    a) Acceder a *System > Log / Monitoring*

    b) Seleccionar la pestaña SNMP para mostrar la página de configuración de SNMP.

    c) Completar la configuración. En el apartado SNMP Versión, seleccionar v3**.**

    d) Guardar la configuración.

162. El detalle de la configuración de SNMP se puede consultar en el siguiente enlace de la documentación: *Monitoring using SNMP* [REF44].

6.12 ALTA DISPONIBILIDAD

163. La solución ofrece una forma fácil y ágil para la configuración del entorno en modo clúster. El producto admite dos (2) tipos de clústeres:

    a) **Clúster en modo Activo/Activo**: este tipo de clúster proporciona funcionalidades de balanceador de carga, junto con alta disponibilidad.

Además, el clúster Activo/Activo proporciona un mayor rendimiento y un balanceo de carga entre los nodos, en el caso de que un nodo se desconecte o no se encuentre disponible.

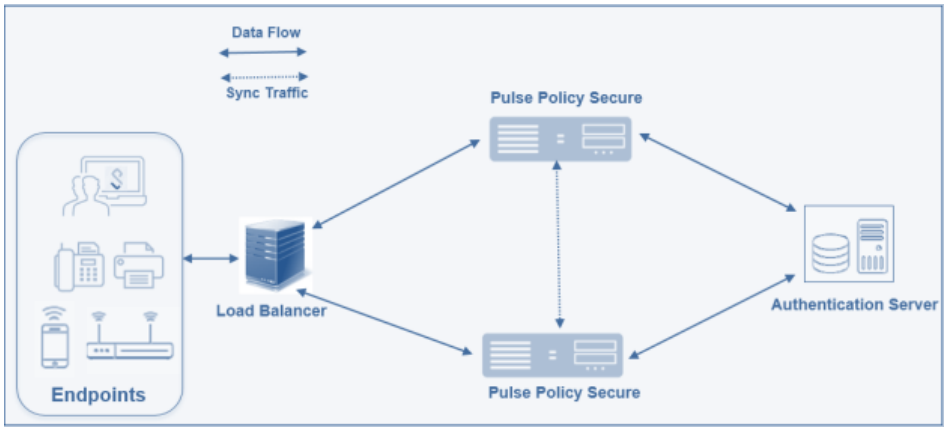

Ilustración 6-18. Esquema básico modo Activo / Activo

b) **Clúster en modo Activo/Pasivo**: estos clústeres proporcionan alta disponibilidad. Su objetivo principal es proporcionar acceso ininterrumpido a los datos, incluso si un servidor pierde conectividad de red o almacenamiento, falla por completo o falla la aplicación que se ejecuta en el servidor.

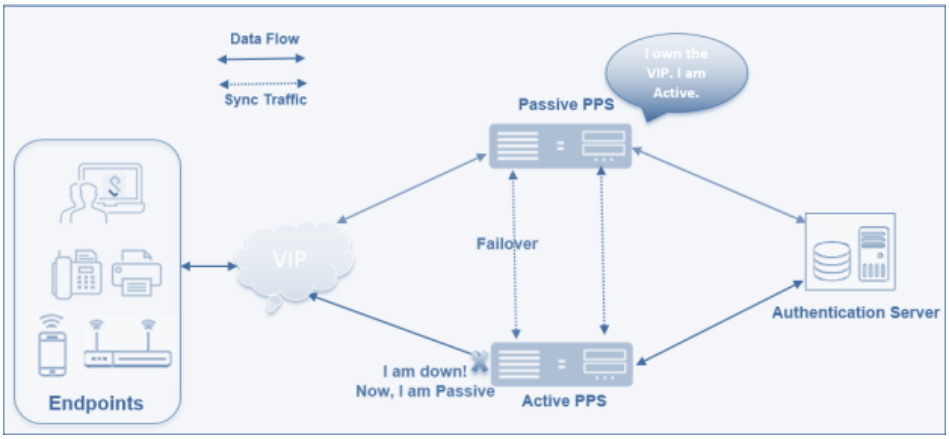

Ilustración 6-19. Esquema básico modo Activo / Pasivo

164. El detalle de la instalación y configuración de los distintos tipos de clústeres se puede consultar en el siguiente enlace de la documentación: *Clustering*. [REF45]

6.13 AUDITORÍA

165. El sistema genera registros de eventos relacionados con el rendimiento del sistema, acciones del administrador, comunicaciones de red, resultados del "*framework*" de acceso, sesiones de usuario, etc.

166. El sistema admite los siguientes métodos de recopilación de registros:

a) Recopilador de registros y visor de registros locales.

b) Reportando a los servidores de *syslog*.

c) Reportando a los servidores SNMP.

167.La siguiente tabla describe el nivel de severidad de los diferentes logs:

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

6.13.1 REGISTRO DE EVENTOS

168.Los diferentes registros disponibles incluyen:

a) **Registro de eventos**: contiene eventos del sistema, como tiempos de espera de sesión, errores y advertencias del sistema, notificaciones de reinicio del servidor y solicitudes de conectividad.

b) **Registro de acceso de usuario**: contiene información sobre el acceso del usuario al dispositivo, la hora, el número de usuarios simultáneos y, los inicios y cierres de sesión de los usuarios.

c) **Registro de acceso de administrador**: contiene información de administración, entre la que se incluyen los cambios del administrador en la configuración del usuario, el sistema y la red, cambios en los tiempos de espera de las sesiones, cambios de licencia, etc.

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

- Acceder a *System > Log/Monitoring*.
- Seleccionar la pestaña de *Settings* para abrir la página de configuración.
- Seleccionar los registros que se desean monitorizar y elegir la opción *Save Changes*.

170.**Se debe usar únicamente TLS 1.2 para la comunicación**. Las configuraciones para el cifrado se han descrito en el apartado 6.13.3 ALMACENAMIENTO REMOTO.

171. El detalle de la monitorización y la configuración del registro de eventos se puede consultar en el siguiente enlace de la documentación: *Logging and Monitoring*. [REF46]

6.13.2 ALMACENAMIENTO LOCAL

172. PPS tiene la posibilidad y capacidad de almacenar los registros de eventos de forma local. El valor predeterminado del tamaño de los logs es de 200MB, permitiendo un máximo de 500MB. El valor predeterminado es aceptable para los registros con formato estándar. Si se utiliza un formato más detallado como WELF, se recomienda especificar un valor mayor.

173. La modificación del tamaño de los logs locales se puede realizar desde *System > Log/Monitoring > Events > Log Settings > Events > Settings.*

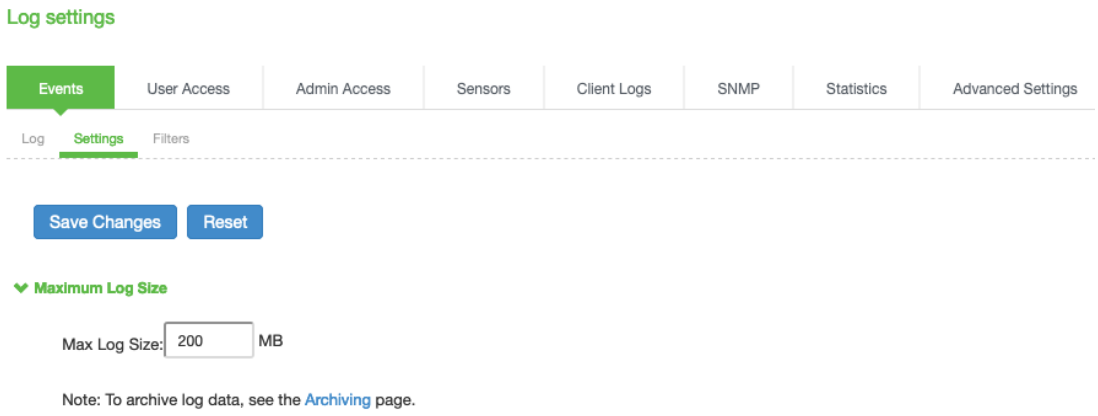

Ilustración 6-20. Configuración del tamaño de *logs*

174. 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 nuevos de registro posteriores. El visor de registros muestra los 5000 mensajes de registro más recientes (límite de visualización). En caso de que el archivo de registro actual contenga menos de 5000 mensajes de registro, se podrán mostrar mensajes de registros anteriores del archivo de respaldo hasta alcanzar el límite. Esto provoca que los archivos de registro aparezcan con los demás a pesar de que se almacenan por separado.

175. En caso de alcanzar el 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 como pueden ser los servidores syslog/SIEM corporativos.

6.13.3 ALMACENAMIENTO REMOTO

176. Además del almacenamiento local, PPS permite enviar los datos de registro a un servidor externo syslog.

177. Para la configuración del envío de logs al servidor syslog, se han de seguir los siguientes pasos:

- Acceder a *System > Log/Monitoring*.

- Seleccionar la pestaña *Settings*.
- Especificar el tamaño máximo de registro y seleccionar los eventos que se van a registrar.
- Introducir la información relativa al servidor que se desea configurar. Se pueden especificar varios servidores syslog.
- Por último, **seleccionar el protocolo TLS para hacer uso único de TLS 1.2** o posteriores y elegir la opción *Save Changes*.

178. Para mayor detalle, se recomienda consultar el siguiente enlace de la documentación: *Configuring an External Syslog Server*. [REF47]

6.14 BACKUP

179. El sistema admite múltiples funciones de administrador relacionadas con la gestión de archivos de configuración. Estas funciones se pueden encontrar en las diferentes páginas accesibles desde *Maintenance*. A continuación, se describe el propósito de las diferentes utilidades:

a) **Archivado (Archiving):** programa de copias de seguridad periódicas en un servidor de "*backup*" remoto. Debe programar la salvaguarda tanto para el archivo binario de configuración del sistema (*system.cfg*) como para el archivo binario de configuración de usuario (*user.cfg*). Si es necesario, se puede importar una configuración archivada utilizando la función de importación/exportación de archivos binarios de configuración.

b) **Copia de seguridad local y restauración (*backup and restore*):** crea copias de seguridad en el sistema local como precaución cuando se realicen cambios significativos en la configuración. Con esta utilidad se puede restaurar rápidamente a una configuración anterior.

c) **Importación/exportación de archivos de configuración binarios (binary configuration file import/export):** exportación de archivos de configuración binarios a un host local. Sirve como alternativa al servidor de archivo remoto y al proceso de archivo que se ejecuta de forma programada. Se puede crear si no se utiliza o no se tiene acceso a un servidor de archivado o si se desea utilizar una configuración que aún no se encuentra archivada. Puede exportar el archivo de configuración del sistema binario (system.cfg), y el archivo de configuración del usuario binario (user.cfg). Además, se puede usar la función de importación/exportación de archivos binarios para clonar una configuración que se desea implementar de manera más amplia, como implementar un dispositivo de respaldo o un grupo de dispositivos. Se pueden 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.

d) **Importación/exportación de archivos de configuración XML (XML configuration file import/export):** importación o exportación de la configuración para las características y configuraciones seleccionadas. Esto permite adoptar un enfoque más granular para la gestión de la configuración masiva que la función de importación/exportación de archivos binarios. La función de importación/exportación de archivos XML es útil para la administración de un solo nodo. Por ejemplo, es posible que se desee agregar muchos usuarios nuevos al servidor de autenticación local, pudiendo ser más rápida la edición del XML que la utilización de la interfaz de usuario.

e) **Configuración push (*push configuration*):** permite desplegar, de forma completa o parcial, 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.

180. **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, ya sea 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 fuera a aplicar al sistema. Las Copias de seguridad locales se realizan desde la página *Maintenance > Archiving > Local Backups.*

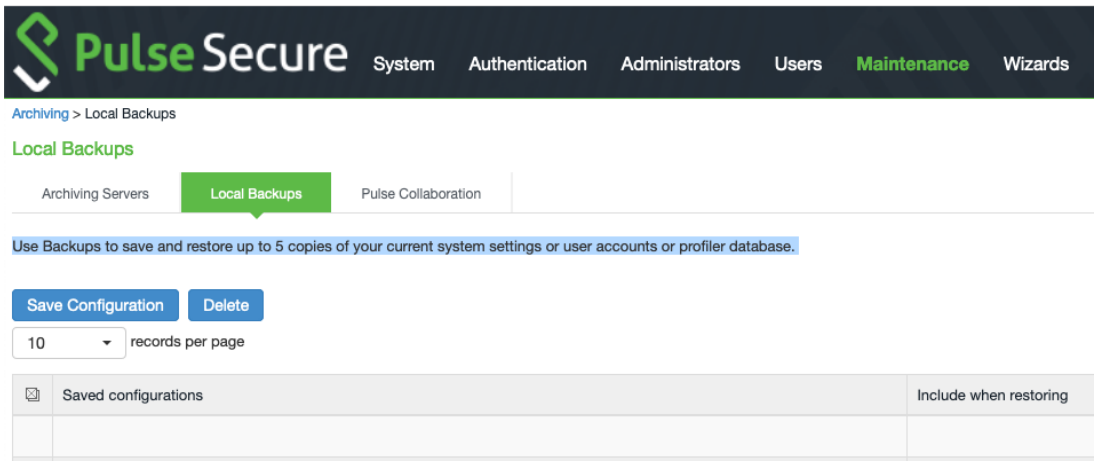

Ilustración 6-21. *Backups* locales

181. **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 se han de seguir los siguientes pasos:

- Acceder 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 el uso del protocolo SCP (opción por defecto) en el apartado *Method*.
- En el apartado *Archive Schedule* configurar la periodicidad de las copias.
- Finalmente, seleccionar la opción *Save Changes*.

182. El detalle de la configuración de las distintas utilidades vistas en el presente apartado puede consultarse en el siguiente enlace de la documentación: *Configuration*. [REF48]

7 FASE DE OPERACIÓN

183. Durante la fase de operación, se deben realizar las siguientes actividades:

a) Implementar 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.

b) Realizar copias de seguridad periódicas, así como configurar el envío de copias a un servidor externo con una periodicidad definida.

c) Revisar tanto las exportaciones de la configuración periódica como el funcionamiento de esta y verificar su integridad, en caso de que sea necesario utilizarla en caso de emergencia.

d) Auditar y revisar las alarmas asociadas a los elementos críticos recogidos en los logs de eventos para poder hacer seguimiento de posibles incidencias.

e) Verificar periódicamente el uso de memoria y CPU, dado que valores elevados de uso pueden generar problemas.

f) Configurar el envío de logs a un servidor syslog para evitar la pérdida de información al producirse la sobrescritura de los logs almacenados localmente, al alcanzar el límite de espacio definido.

g) Gestionar correctamente los certificados utilizados por el producto, cambiándolos cuando sea necesario. Por ejemplo, en su expiración.

8 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 y archivado	☐	☐	
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 [REF49]
Creación de Servidor de Autenticación (LDAP, AD, RADIUS, TOTP, etc.)	☐	☐	
Creación de roles	☐	☐	
Creación de "*Realms*"	☐	☐	
Creación de *Sign-in Policies*	☐	☐	
Creación de las configuraciones de *Endpoint Protection (Host Checker)*	☐	☐	
Creación de *Sign-in URL*	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Activación modo seguro FIPS-CC	☐	☐	FIPS Level 1 Support (Software FIPS) [REF19]
OPERACIÓN			

ACCIONES	SÍ	NO	OBSERVACIONES
Actualización del *software* y parches de seguridad	☐	☐	
Realización de copias de seguridad	☐	☐	
Exportar y verificar la integridad de la configuración	☐	☐	
Auditoría de eventos	☐	☐	
Verificar el uso de memoria y CPU	☐	☐	
Envío seguro de logs a una entidad externa	☐	☐	
Gestión y actualización de certificados	☐	☐	

9 REFERENCIAS

REF1 Documentación Global de Pulse Secure.
https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm

REF2 *Knowledge Articles* de Pulse Secure.
https://kb.pulsesecure.net/

REF3 Página oficial de Pulse Secure.
https://my.pulsesecure.net/

REF4 *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

REF5 *KB40050 - Onboarding FAQ*
https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40050

REF6 *KB40031 – [Customer Support Tools] Onboarding at my.pulsesecure.net.*
https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40031

REF7 *KB40565 – What is Right To Use (RTU) and Service Contract certificate.*
https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40565

REF8 *Pulse Secure: Obtaining License Keys*
https://docs.pulsesecure.net/WebHelp/License_Management/Home.htm#pcs-pps-licensemgmt_9.0_r1/Obtaining_License_Keys.htm

REF9 *Pulse Secure: Obtain Licenses*
https://docs.pulsesecure.net/WebHelp/PCS/9.1R1/AG/Home.htm#ps-pcs-gettingstartedguide-9.1R1/Obtain_Licenses.htm

REF10 *KB40030 - [Customer Support Tools] Pulse Secure Support Services Quick Start Guide.*
https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40030

REF11 *Pulse Appliances: Hardware Guide PSA-300*
https://docs.pulsesecure.net/WebHelp/PSA_Hardware/Content/ps-psa300-hardware-guide/ps-psa300-hardware-guide.htm

REF12 *Pulse Appliances: Hardware Guide PSA-3000*
https://docs.pulsesecure.net/WebHelp/PSA_Hardware/Content/ps-psa3000-hardware-guide/ps-psa3000-hardware-guide.htm

REF13 *Pulse Appliances: Hardware Guide PSA-5000*
https://docs.pulsesecure.net/WebHelp/PSA_Hardware/Content/ps-psa5000-hardware-guide/ps-psa5000-hardware-guide.htm

REF14 *Pulse Appliances: Hardware Guide PSA-7000*
https://docs.pulsesecure.net/WebHelp/PSA_Hardware/Content/ps-psa7000-hardware-guide/ps-psa7000-hardware-guide.htm

REF15 *9.1R1 PCS and 9.1R1 PPS Virtual Appliance Deployment Guide*
https://help.ivanti.com/ps/legacy/pps/9.1rx/9.1r1/ps-pcs-pps-9.1r1-virtual-appliance-deployment-guide.pdf?psredirect

REF16 *Endpoint Compliance: Endpoint Security Assessment Plug-In (ESAP)*
https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/Endpoint_Security_Assessment.htm

REF17 *Pulse Policy Secure Administration: Behavioral Analytics*
https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/Contents.htm%3FTocPath%3DPulse%2520Policy%2520Secure%7CPulse%2520Policy%2520Secure%2520Administration%7CBehavioral%2520Analytics%7C_____0

REF18 *Getting Started: Installation, Configuration and Start-Up Procedure.*
https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS-gettingstartedguide/Installation__Config_and_Start-Up.htm%3FTocPath%3DPulse%2520Policy%2520Secure%7CGetting%2520Started%7CInstallation%252C%2520Configuration%2520and%2520Start-Up%2520Procedure%7C_____0

REF19 *System Management: FIPS Level 1 Support (Software FIPS)*
https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/CHAPTER_27_FIPS_Level_1_Support.htm

REF20 *Pulse Policy Secure Administration: AAA Servers*
https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/CHAPTER_20_AAA_Servers.htm%3FTocPath%3DPulse%2520Policy%2520Secure%7CPulse%2520Policy%2520Secure%2520Administration%7CAAA%2520Servers%7C_____0

REF21 *Pulse Policy Secure Administration: Using a Time-Based One-Time Password (TOTP) Authentication Server*
https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#TOTP_Server/Using_a_Time_Based_One_Time.htm%3FTocPath%3DPulse%2520Policy%2520Secure%7CPulse%2520Policy%2520Secure%2520Administration%7CAAA%2520Servers%7CUsing%2520a%2520Time-Based%2520One-Time%2520Password%2520(TOTP)%2520Authentication%2520Server%7C_____0

REF22 *Pulse Policy Secure Administration: Configuring the Local Authentication Server.*

https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/Configuring_the_Local_Authentication.htm

REF23 *Pulse Policy Secure Administration: Customizing UI Options.*

https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/Customizing_UI_Options.htm%3FTocPath%3DPulse%2520Policy%2520Secure%7CPulse%2520Policy%2520Secure%2520Administration%7CIntroduction%7CRoles%252C%2520Realms%252C%2520and%2520Sign-In%2520Policy%7CConfiguring%2520User%2520Roles%7C_____3

REF24 *Pulse Policy Secure Administration: Creating an Authentication Realm.*

https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/Creating_an_Authentication.htm

REF25 *Pulse Policy Secure Administration: Configuring Host Checker Rules.*

https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/Configuring_HC_Rules.htm%3FTocPath%3DPulse%2520Policy%2520Secure%7CPulse%2520Policy%2520Secure%2520Administration%7CEndpoint%2520Compliance%7CHost%2520Checker%7CConfiguring%2520Host%2520Checker%2520Rules%7C_____0

REF26 *Pulse Policy Secure Administration: Configuring Role Mapping.*

https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/Configuring_Role_Mapping.htm%3FTocPath%3DPulse%2520Policy%2520Secure%7CPulse%2520Policy%2520Secure%2520Administration%7CIntroduction%7CRoles%252C%2520Realms%252C%2520and%2520Sign-In%2520Policy%7CConfiguring%2520Authentication%2520Realm%7C_

REF27 *Pulse Policy Secure Administration: Configuring Administrator Sign-in Policies.*

https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/Configuring_Administrator.htm%3FTocPath%3DPulse%2520Policy%2520Secure%7CPulse%2520Policy%2520Secure%2520Administration%7CIntroduction%7CRoles%252C%2520Realms%252C%2520and%2520Sign-In%2520Policy%7CConfiguring%2520Sign-in%2520Policies%7C____

REF28 *Pulse Policy Secure Administration: Configuring User Roles.*

https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/Configuring_User_Roles.htm

REF29 *Pulse Policy Secure Administration: Configuring User Sign-In Policies.*
https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/Configuring_User_Sign_In_Policies.htm

REF30 *Pulse Policy Secure Administration: Network and Host Administration.*
https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/CHAPTER_25_Network_and_Host.htm

REF31 *KB40706 - Disable 3DES cipher suites for Pulse Connect Secure or Pulse Policy Secure*
https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40706

REF32 *KB40686 - Enable password protection when accessing through the serial console.*
https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40686/

REF33 *Pulse Policy Secure Administration: Configuring Authentication with a TOTP Authentication Server.*
https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#TOTP_Server/Configuring_Authentication.htm

REF34 *Pulse Policy Secure Administration: Configuring Authentication with a RADIUS Server.*
https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/Configuring_Authentication_7.htm

REF35 *Pulse Policy Secure Administration: Configuring Authentication with a LDAP Server.*
https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/Configuring_Authentication_5.htm

REF36 *Pulse Policy Secure Administration: Configuring Authentication and Authorization with Active Directory Service (Standard Mode).*
https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/Configuring_Authentication_1.htm

REF37 *Pulse Policy Secure Administration: Host Checker.*
https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/CHAPTER_18_Host_Checker.htm

REF38 *KB40243 - Subscribe to Security Advisory notification emails and Software Release notification emails*
https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40243/?kA1j0000000fySj

REF39 *Pulse Policy Secure Administration: Certificate Security Administration*
https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/CHAPTER_26_Certificate_Security.htm

REF40 *Installation, Configuration and Start-Up Procedure: Downloading Pulse Policy Secure Software and License.*

https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS-gettingstartedguide/Step_3_Downloading_Pulse_Policy.htm%3FTocPath%3DPulse%2520Policy%2520Secure%7CGetting%2520Started%7CInstallation%252C%2520Configuration%2520and%2520Start-Up%2520Procedure%7C_____3

REF41 *Pulse Policy Secure Administration: Installing the Service Package.*

https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/Installing_the_Service_Package.htm

REF42 *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/?kA1j0000000Fnaj

REF43 *KB12940 - Recommended procedure for upgrading PPS firmware.*

https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB12940/?kA1j0000000FjZe

REF44 *Pulse Policy Secure Administration: Monitoring using SNMP.*

https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/Monitoring_using_SNMP.htm

REF45 *Pulse Policy Secure Administration: Clustering.*

https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/CHAPTER_24_Clustering.htm%3FTocPath%3DPulse%2520Policy%2520Secure%7CPulse%2520Policy%2520Secure%2520Administration%7CClustering%7C_____0

REF46 *Pulse Policy Secure Administration: Logging and Monitoring.*

https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/CHAPTER_31_Logging_and_Monitoring.htm

REF47 *Pulse Policy Secure Administration: Configuring an External Syslog Server.*

https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/Configuring_an_External_Syslog.htm

REF48 *Pulse Policy Secure Administration: Configuration.*

https://docs.pulsesecure.net/WebHelp/PPS/9.1R1/Home.htm#PPS_Admin_Guide/Configuration.htm

REF49 *KB44152 - Pulse Policy Secure: Security configuration best practices*

https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44152

10 ABREVIATURAS

AAA	*Authentication, Authocrization and Accounting.*
ACL	*Access Control List.*
AD	*Active Directory.*
AWS	*Amazon Web Services.*
ENS	Esquema Nacional de Seguridad.
FIPS	*Federal Information Processing Standard.*
FIPS	*Federal Information Processing Standard.*
FQDN	*Fully Qualified Domain Name.*
GW	*Gateway.*
IP	*Internet Protocol.*
KB	*Knowledge Base.*
KVM	*Kernel-based Virtual Machine.*
LDAP	*Lightweight Directory Access Protocol.*
NDcPP	*Network Device Collaborative Protection Profile.*
NTP	*Network Time Protocol*
OGS	*Optimal Gateway Selection.*
OU	*Organization Unit.*
PCS	*Pulse Connect Secure.*
PDC	*Pulse Desktop Client.*
PPS	*Pulse Policy Secure.*
RADIUS	*Remote Access Dial in User Service.*
SCP	*Secure Copy Protocol.*
SHA	*Secure Hash Algoritm.*
SSH	*Secure Shell Protocol.*
TCP	*Transmission Control Protocol.*
TLS	*Transport Layer Security Protocol.*
UDP	*User Datagram Protocol.*
vADC	*Virtual Application Delivery Controller.*
VLAN	*Virtual Local Area Network.*
VPN	*Virtual Private Network.*
WLC	Wireless Lan Controller.

PUBLICACIONES DE DEFENSA

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