centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1214

Procedimiento de empleo seguro
Checkpoint Endpoint Security (SandBlast Agent)

Abril de 2022

MINISTERIO DE DEFENSA

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

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.04.18 11:58:13 +02'00'

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2022
NIPO: 083-22-124-6

Fecha de Edición: abril de 2022

ÍNDICE

1 INTRODUCCIÓN

1. ***CheckPoint Endpoint Security*** es una solución completa de seguridad para puestos finales que ofrece funciones avanzadas de prevención de amenazas en los puestos finales para que puedan navegar de forma segura por el escenario actual de amenazas.
2. Proporciona un sistema integral para prevenir, detectar y corregir de forma proactiva los ataques de *malware* evasivos.
3. Incorpora una gestión integrada disponible en nube o instalación local y sus funcionalidades principales son:
    - Emulación de amenazas (*Sandbox*) y extracción (entrega archivos limpios a usuarios en tiempo real).
    - *Anti-Ransomware* (prevención y reparación) y defensa contra ciberextorsión.
    - *Anti-Bot*.
    - *Anti-Exploit.*
    - *Anti-Malware.*
    - Análisis de comportamientos (detección y bloqueo).

2 OBJETO Y ALCANCE

4. El presente documento tiene como objetivo detallar las configuraciones de seguridad del producto ***Endpoint Security* E82.40 (82.40.1159) con el Servidor de *Harmony Endpoint onpremises* R81 de Checkpoint**, de forma que la protección y funcionamiento del producto se realice de acuerdo a unas garantías mínimas de seguridad.
5. **Este producto ha sido cualificado ENS MEDIO e incluido en las familias de '*Antivirus/EPP*' y '*EDR*' del Catálogo de Productos y Servicios STIC (CPSTIC) del Centro Criptológico Nacional**.

3 ORGANIZACIÓN DEL DOCUMENTO

6. Este documento está organizado en diferentes capítulos, de acuerdo a diferentes fases del ciclo de vida del producto:

   - **Apartado 4**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto.
   - **Apartado 5.** En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
   - **Apartado 6**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.
   - **Apartado 7**. En este apartado aparece un *checklist* con las tareas a realizar y el estado de cada una de ellas.
   - **Apartado 8**. Referencias usadas en este documento.
   - **Apartado 9**. Abreviaturas usadas en este documento.

4 FASE DE DESPLIEGUE E INSTALACIÓN

4.1 CONSIDERACIONES PREVIAS

4.1.1 CONSIDERACIONES PREVIAS SOBRE EL SERVIDOR DE GESTIÓN

7. El dispositivo sobre el que se instalará el servidor de gestión *Endpoint Security Management Server* **debe disponer de, al menos, 10 GB disponibles** en disco en la partición raíz.
8. Los paquetes de clientes y los archivos principales de la versión que se almacenan en la partición raíz son los siguientes:

Espacio requerido	*Descripción*
4 GB	Archivos de instalación del servidor principal.
2 GB o más	Archivos de clientes (cada versión adicional de los paquetes de clientes requiere 1 GB de espacio en el disco).
1 GB	Logs.
1 GB	Apoyo de alta disponibilidad (se puede requerir más en entornos grandes).

Tabla 1: Requisitos de espacio en disco

9. El servidor, en caso de habilitar la indexación de registros, crea y utiliza archivos de índice para un rápido acceso al contenido de los archivos de registro. Los archivos de índice están ubicados de forma predeterminada en *$RTDIR/log_indexes/*. Para asegurar el espacio en disco, el servidor elimina las entradas más antiguas cuando el espacio es inferior al 15% del espacio disponible en disco o a 5000 MB.
10. Se puede configurar el espacio mínimo de disco aplicable siguiendo los siguientes pasos:
    - Desde *SmartConsole*, editar el objeto del *Security Management Server*, el cuál aparecerá en la opción de *Gateways & Servers* con el icono de una corona:

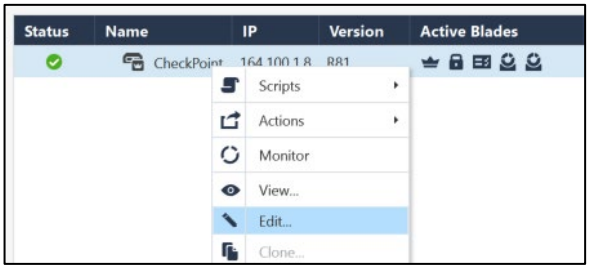

Figura 1: Security Management Server

- En el árbol de navegación de la izquierda, seleccionar *Registros* > *Almacenamiento*.
- Seleccionar *Cuando el espacio de disco esté por debajo de <número> Mbytes, comience a borrar los archivos viejos*. Introducir el valor de espacio deseado.
- Seleccionar *OK*.

11. CheckPoint dispone de un Sistema Operativo propio denominado GAIA. Se recomienda instalar dicho sistema operativo en el dispositivo que vaya a albergar el servidor de gestión.
12. Para instalar un Sistema Operativo GAIA limpio en un dispositivo, están disponibles las siguientes opciones:
    - Reiniciar un dispositivo con el Sistema operativo ya instalado a sus condiciones de fábrica.
    - Realizar una instalación limpia mediante un USB.
    - Realizar una instalación limpia con CPUSE (*Check Point Upgrade Service Engine*).
13. Se puede consultar el detalle de los requisitos Hardware en el documento sobre *Requisitos Hardware – REF5*.

4.1.2 CONSIDERACIONES PREVIAS PARA LOS DISPOSITIVOS FINALES

14. A continuación, se recoge una serie de aspectos a tener en cuenta antes de proceder con la instalación de los agentes en dispositivos finales:
    - **El dispositivo donde se vaya a instalar no debe tener otra solución de seguridad instalada**, si se va a activar el módulo de *Antimalware* de *Harmony Endpoint* (consultar el siguiente enlace).
    - Los Sistemas Operativos compatibles con la versión E82.40 del producto son los siguientes:

Microsoft Windows

Version	Editions	Arch.	SPs or Updates	Supported Features
10 19H2 (version 1909) 10 19H1 (version 1903) 10 LTSC (version 1809) 10 (version 1809) 10 (version 1803) 10 (version 1709) 10 LTSB (version 1607)	Enterprise Pro	32/64-bit		All
8.1	Enterprise Pro	32/64-bit	Update 1	All
7	Enterprise Professional	32/64-bit	SP1 Microsoft update KB3033929	All

Microsoft Windows Server

Version	Editions	Arch.	SPs or Updates	Supported Features
2019	All	64-bit		Compliance, Anti-Malware, Firewall, SandBlast Agent features, Capsule Docs (Standalone Client)
2016 (*)	All	64-bit		Compliance, Anti-Malware, Firewall, SandBlast Agent features, Capsule Docs (Standalone Client)
2012	All	64-bit		Compliance, Anti-Malware, Firewall, SandBlast Agent features, Capsule Docs (Standalone Client)
2012 R2	All	64-bit		Compliance, Anti-Malware, Firewall, SandBlast Agent features, Capsule Docs (Standalone Client)

VMware ESXi

Version	Supported Features
5.1, 5.5, 6.0	All except: Full Disk Encryption and Media Encryption & Port Protection
	Note- If you install a client package with features that are not supported on the server, the installation succeeds but only the supported features are installed.

Figura 2: Sistemas Operativos Compatibles

(*) Para el uso de Endpoint Compliance Rules para Windows Server 2016, ver sk122136.

15. Los dispositivos deben disponer de:
    - 2 GB RAM.
    - 2 GB espacio libre en disco.

16. El producto necesita acceso a internet (directamente o a través de *proxy*). El listado de direcciones a las que debe poder acceder se puede consultar en el siguiente enlace.

4.1.3 INTERFACES DE GESTIÓN

17. El producto dispone de distintas interfaces de gestión que se mencionarán a lo largo del documento. A continuación, se describen brevemente.

    a) ***SmartConsole***: *Software* de gestión que permite operar con los componentes de la arquitectura de *Checkpoint* tales como *Gateways*, servidores *Endpoint*, servidores de *Log*, etc. Se puede descargar directamente desde la web de Check Point. Ver *Understanding SmartConsole*.

    b) ***SmartEndpoint***: Componente que se despliega automáticamente durante la instalación de *SmartConsole*. *SmartEndpoint* permite realizar todas las configuraciones necesarias del servicio de *Harmony Endpoint*, tales como políticas de seguridad, despliegue de agentes, visión de eventos de seguridad, etc. Ver *Harmony Endpoint Security Admin Guide*.

    c) ***Interfaz GUI de Gaia***: El sistema operativo Gaia dispone de una interfaz gráfica (GUI) que permite realizar modificaciones en el sistema operativo de un servidor de seguridad, servidor Endpoint, etc. Dentro de estas modificaciones permitidas se encuentran: direccionamiento de red, servidores de resolución de nombres, SNMP, actualización de versión, etc. Ver *Introduction to Gaia Portal*.

    d) ***Interfaz CLI del servidor de gestión.*** Adicionalmente, el acceso CLI al servidor de gestión, principalmente para habilitar y deshabilitar distintos servicios.

4.1.3.1 ACCESO CONSOLA WEB

18. Adicionalmente, el producto permite activar una consola web, la cual permite realizar alguna de las configuraciones llevadas a cabo desde *SmartEndpoint*.

19. Para poder acceder a la consola web es necesario activar el servicio:

    - Conectarse a la línea de comando del servidor de gestión.
    - Iniciar sesión en el modo experto, para ello ejecutar el comando *expert.*
    - Ejecutar *web_mgmt_start.*
    - Conectarse con un navegador web: *https://<IP Address of Endpoint Security Management Server>/sba/index.html*

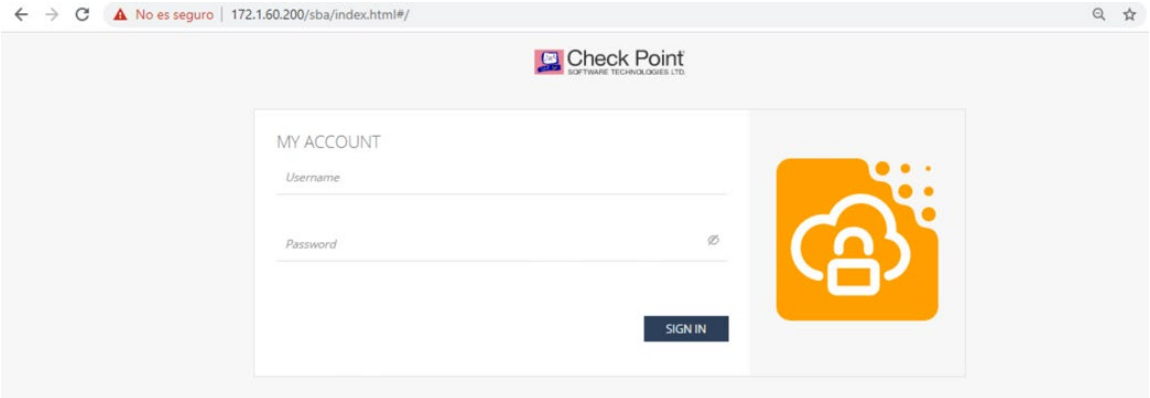

Figura 3: Activación Consola Web

20. La configuración a través de la interfaz Web es muy similar a la realizada por el cliente pesado *SmartEndpoint*.

4.2 DESCARGA SEGURA DEL PRODUCTO

21. La descarga de la última versión de la versión E82.40 del software del producto se puede realizar desde el siguiente enlace. **Se debe verificar que el hash SHA256 del fichero descargado coincide con el que se muestra en la tabla *Details*, antes de realizar la instalación, para verificar su autenticidad e integridad.**

Details

File Name	E82.40_Full_x32.zip
Product	
Version	
Minor Version	E82.40
OS	
Build Number	
MD5	7a55b17ba6edfbae6aa27aaf4576571c
SHA1	0e18dc4d51aee1ea7a38f796808264d5bf642d59
SHA256	64cfd9aa47dda35c156be77c74435c2046cd882561691d79804ffa520cfc0c09
Size	650.56 MB
Date Published	2020-02-16

Ilustración 1. Verificación de la integridad de la descarga.

22. Para la descarga del servidor, versión R81, **se deben seguir los mismos pasos, verificando la integridad del fichero descargado**. Se puede obtener desde el siguiente enlace.

4.3 INSTALACIÓN DEL SERVIDOR DE GESTIÓN

23. Los pasos para realizar la instalación del servidor de gestión en un dispositivo, una vez descargado el *software*, son los siguientes. Este proceso es válido tanto para *appliance* físico como en formato virtuales:

    - Seleccionar I*nstalar el Sistema Operativo Gaia*.

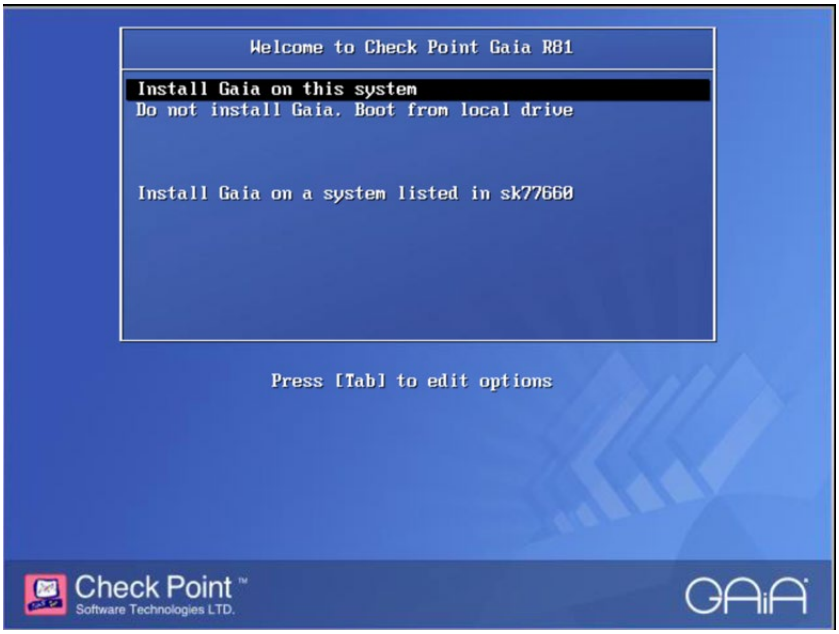

Figura 4: Instalación Gaia

- Seguir las instrucciones del *Wizard* de instalación.

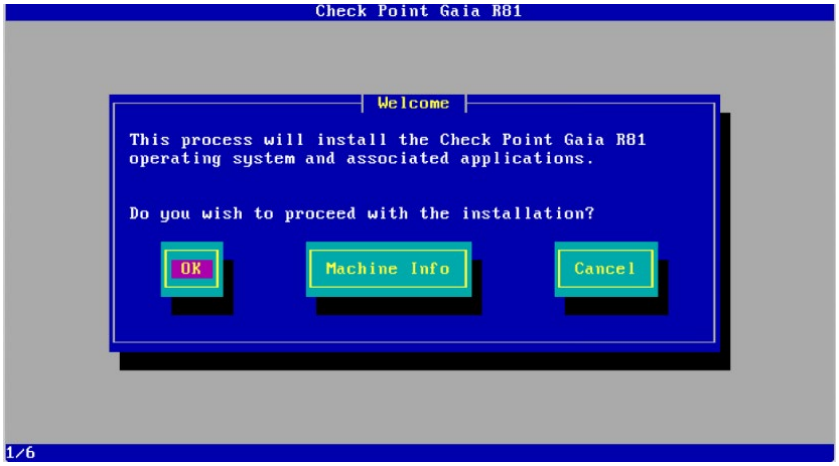

Figura 5: Instalación Gaia

- Realizar la asignación de las particiones del disco, por defecto se muestra una configuración predefinida que puede modificarse según criterios propios.

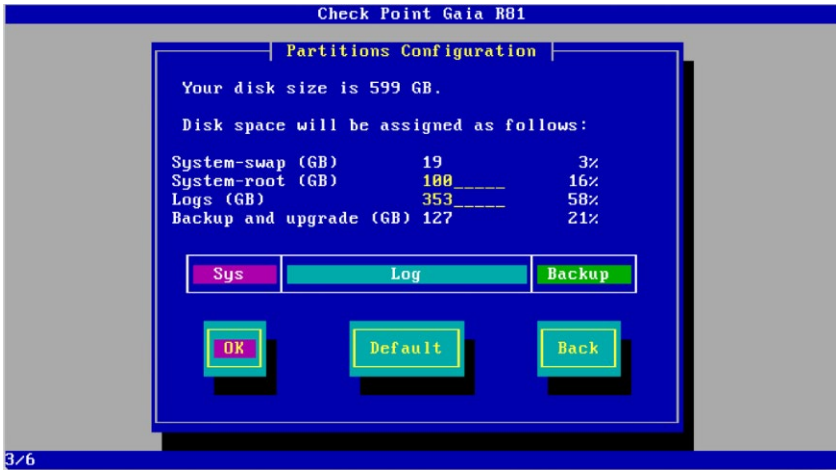

Figura 6: Instalación Gaia

- Configurar la contraseña del usuario *admin.* Se recomienda seguir las indicaciones de la política de contraseñas definida en el apartado 5.3.2 POLÍTICA DE CONTRASEÑAS.

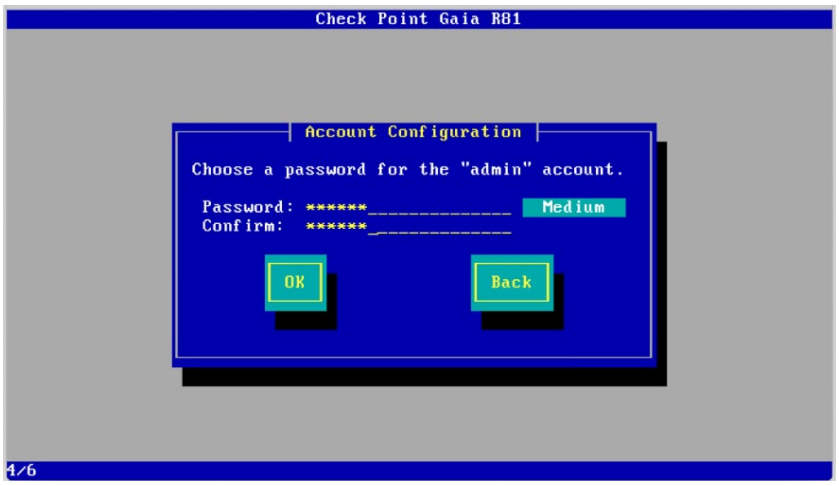

Figura 7: Instalación Gaia

- Configurar la red del interfaz de administración.

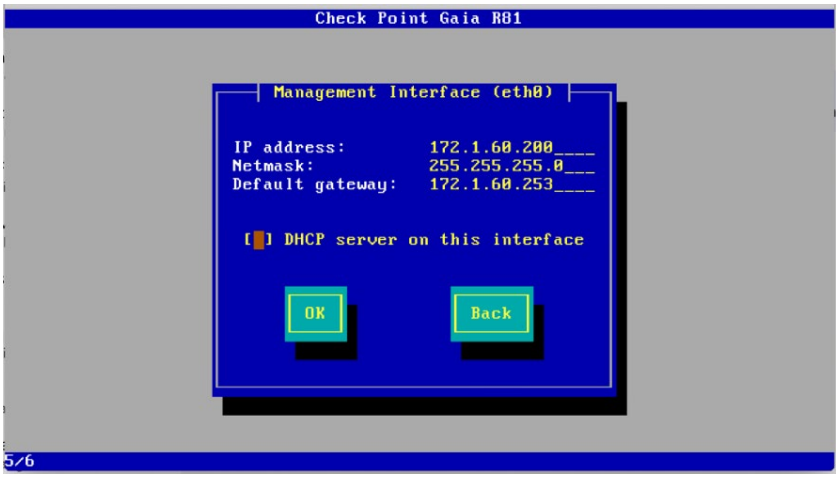

Figura 8: Instalación Gaia

- Una vez finalizada la instalación reiniciar el servidor.

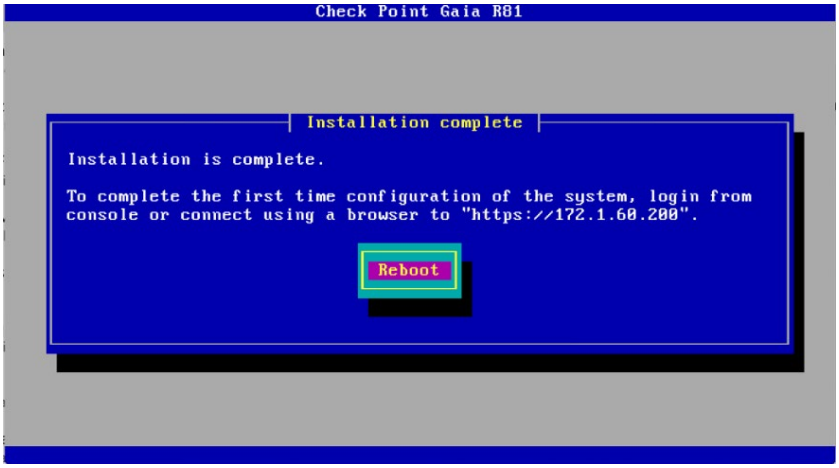

Figura 9: Instalación Gaia

24. Después del reinicio es necesario finalizar la configuración del servidor de gestión y para ello es necesario acceder a través de un navegador a *https://172.1.60.200* y seguir el *Wizard* de configuración.

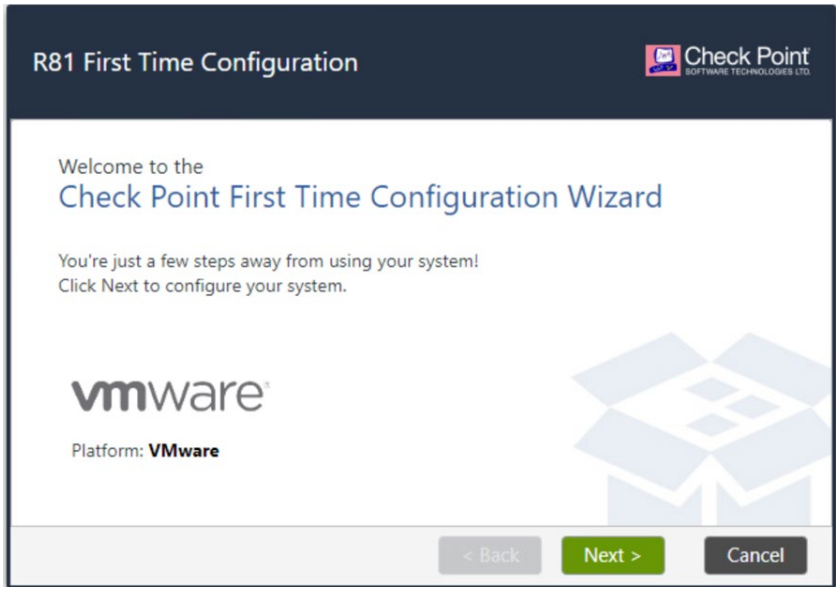

Figura 10: Configuración Gestora

- Seleccionar continuar con la configuración R81.

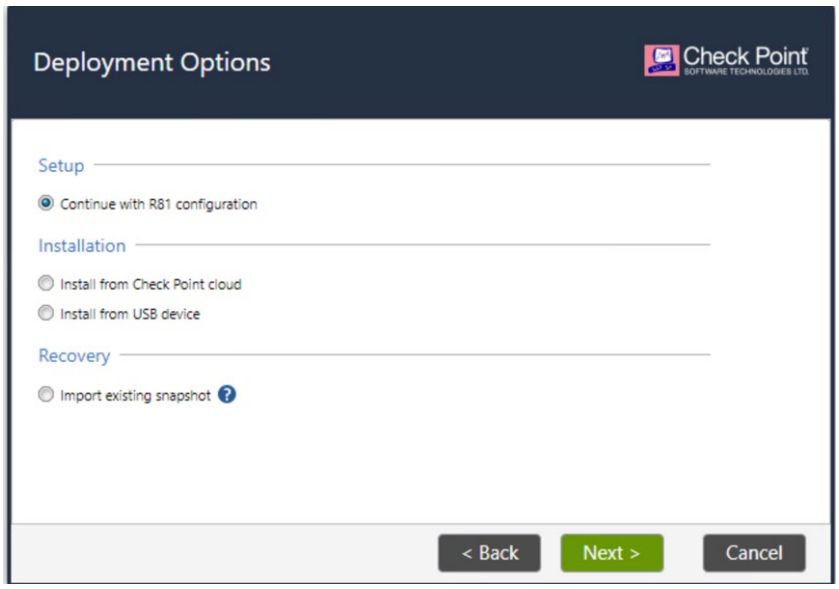

Figura 11: Configuración Gestora

- Revisar la configuración de red del interfaz de administración.

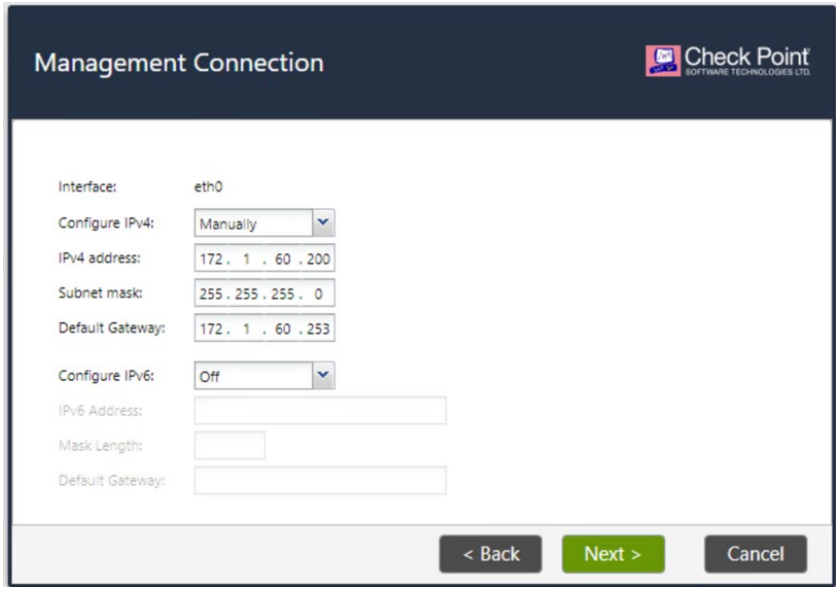

Figura 12: Configuración Gestora

- Asignar un nombre y confirmar los parámetros DNS.

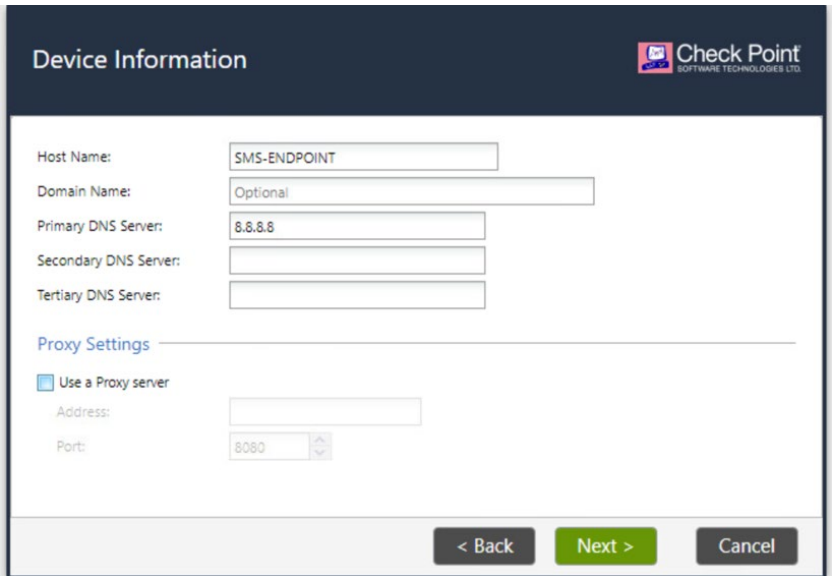

Figura 13: Configuración Gestora

- Configurar los parámetros de hora y fecha. Para su posterior modificación en caso necesario, consultar el apartado 5.6 SINCRONIZACIÓN.

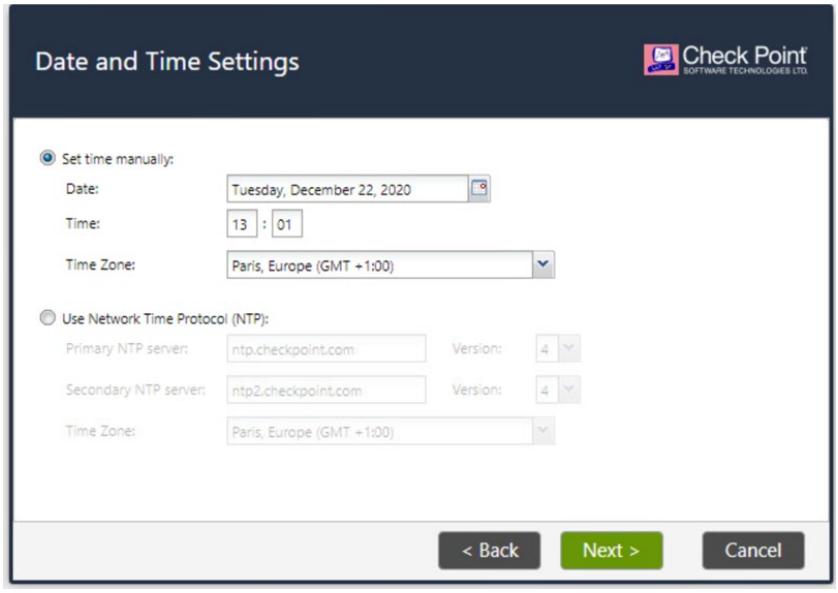

Figura 14: Configuración Gestora

- Seleccionar instalar *Security Gateway and/or Security Management.*

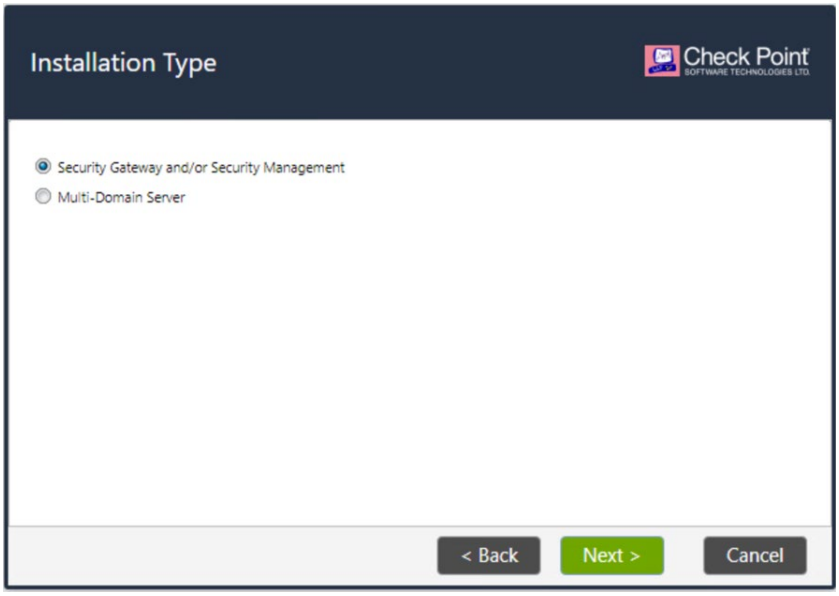

Figura 15: Configuración Gestora

- Marcar la opción de *Security Management* como primaria.

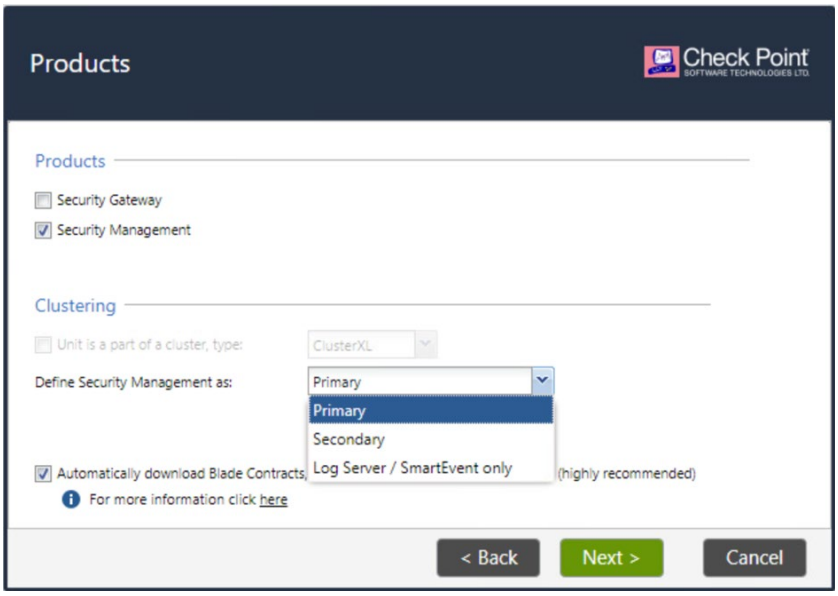

Figura 16: Configuración Gestora

- Seleccionar utilizar el usuario *Admin* del Sistema operativo como usuario Administrador.

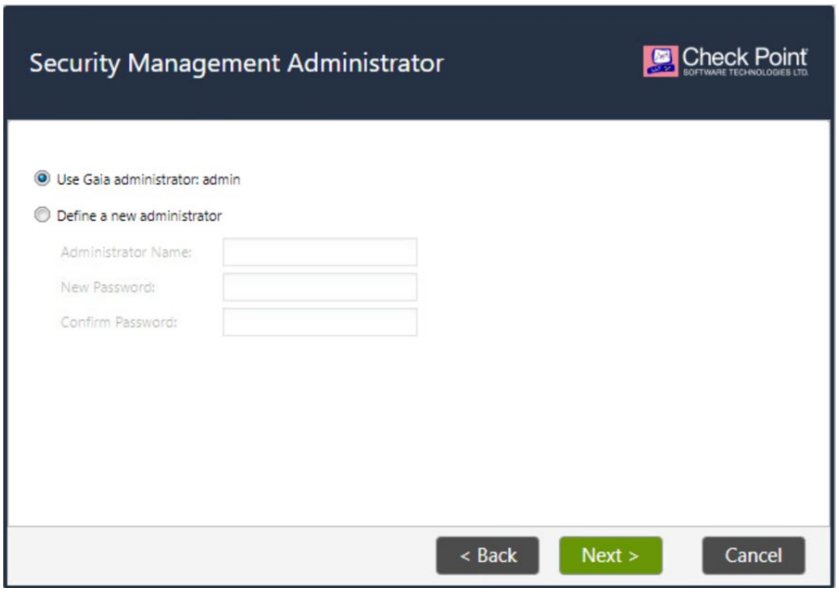

Figura 17: Configuración Gestora

- Definir qué dispositivos podrán acceder a la *Security Management.*

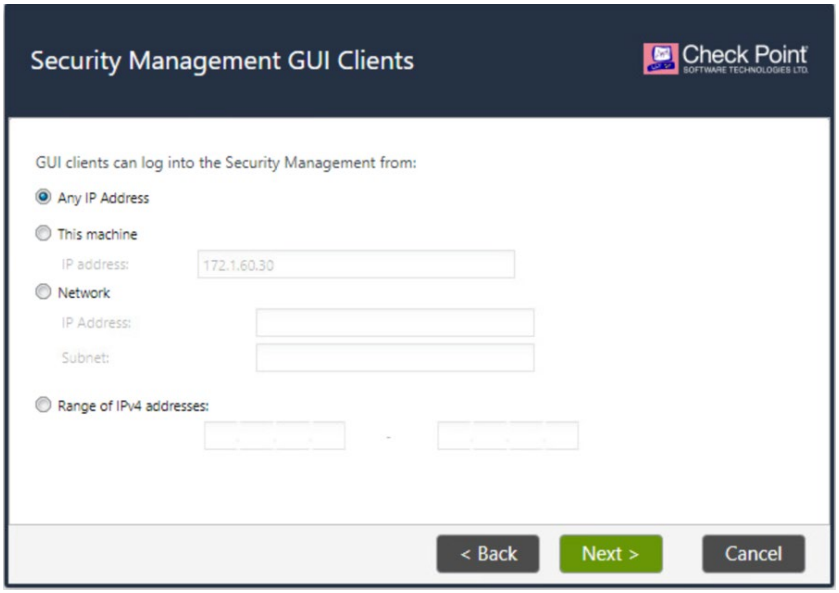

Figura 18: Configuración Gestora

- Finalizar el proceso de configuración.

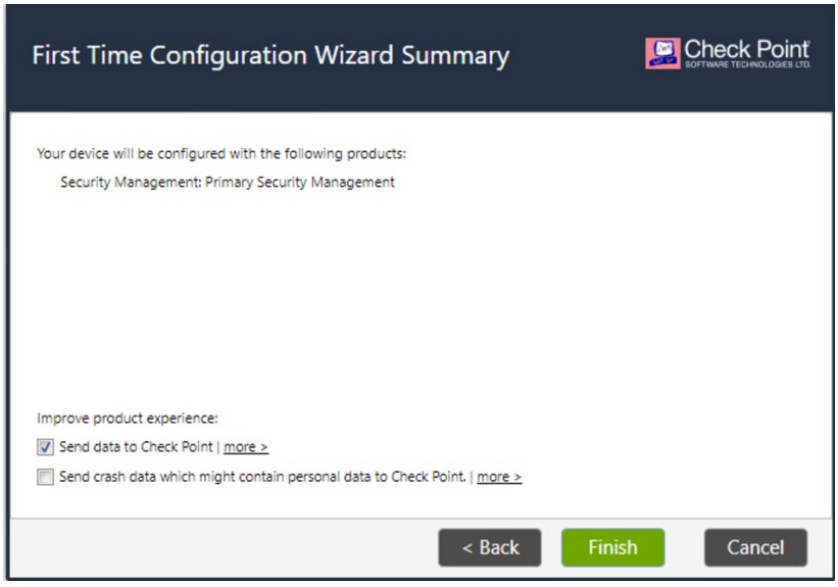

Figura 19: Configuración Gestora

- Una vez finalizado el proceso de configuración, se podrá acceder a la interfaz GUI de GAIA, utilizando el usuario/contraseña configurado.

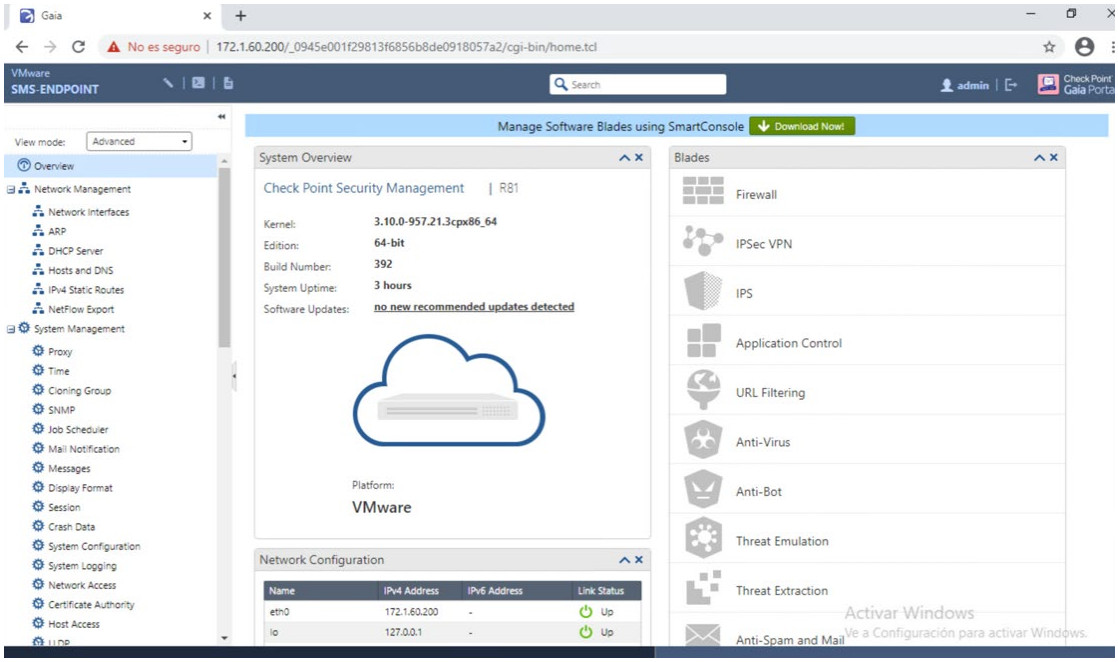

Figura 20: Visión final del Panel De Administración

4.4 INSTALACIÓN DEL AGENTE

25. Para realizar la instalación del agente, primero debe descargarse el cliente inicial desde la *SmartConsole*. Este agente se comunicará con el servidor de gestión para obtener los módulos deseados y las políticas configuradas. Debe distribuirse manualmente exportando el paquete.
26. Para obtener el cliente inicial, desde *SmartConsole*:
    - Ir a *Deployment*. En el apartado *Initial Client*, hacer clic en *Download* y seleccionar la versión deseada (E82.40).
    - Si desea incluir los dispositivos que utilicen el instalador en un grupo virtual, hacer clic en *Select Virtual Group*.
    - Hacer clic en *Download*. Exportar el fichero a los dispositivos finales deseados y ejecutarlo.
27. Posteriormente, desde la consola de gestión del servidor se pueden crear las reglas de despliegue, que permiten crear y distribuir los paquetes de componentes de Endpoint Security. Este paquete incluye los componentes específicos que desea instalarse en el cliente.
28. Para ello se deben seguir los siguientes pasos:
    - En SmartConsole ir a *Deployment > Software Deployment Rules*.
    - Hacer clic en el icono *Create Rule*. Se abrirá una nueva ventana.
    - En *Select Entities*, seleccionar el grupo virtual u ordenadores a los cuales aplicará la regla. Hacer clic en *Next*.

- En *Change Rule Action Settings*, seleccionar la acción, mantener la versión E82.40 del cliente y seleccionar los módulos que desea incluirse. Hacer clic en *Next*.
- Por último, hacer clic en *Save*. Desde la pestaña *Deployment*, seleccionar *Install Policy*, de tal forma que se aplicarán las reglas creadas a los agentes correspondientes.

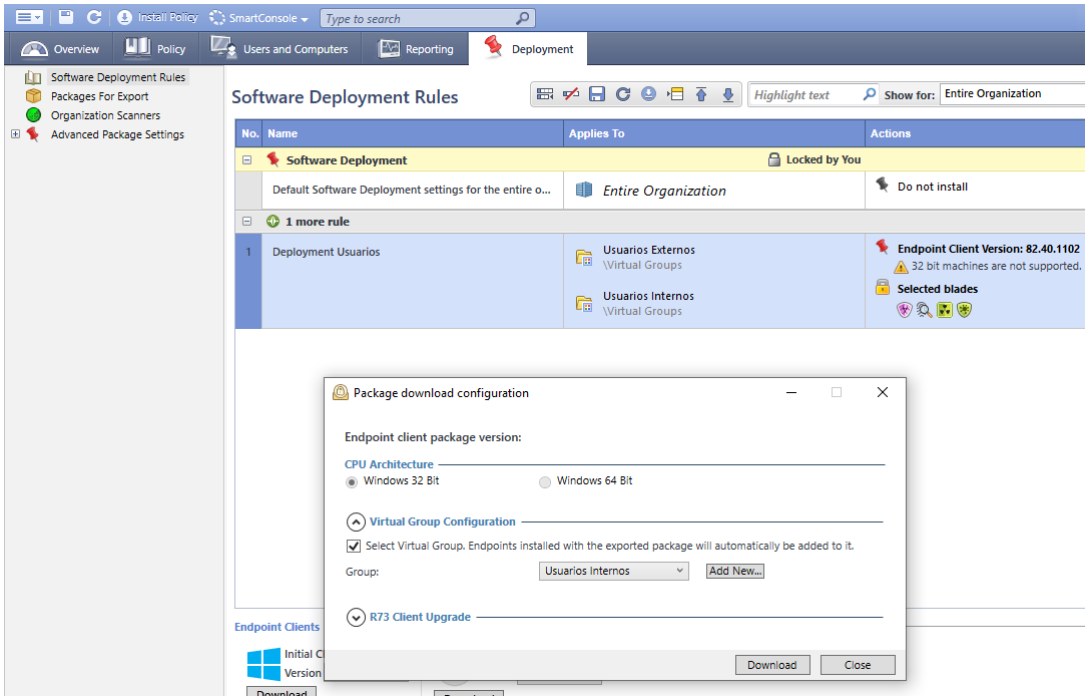

Figura 21: Despliegue de *Initial Client*

4.5 REGISTRO Y LICENCIAS

29. Se requiere disponer de una licencia para:
    - Cada cliente de *Endpoint Security*. La licencia es por dispositivo.
    - El Servidor de Gestión de Seguridad de los Agentes.
30. Las licencias pueden adquirirse como una suscripción, un contrato que se renueva anualmente o una compra única.

5 FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

31. El producto no dispone de un modo de operación seguro. Sin embargo, se dispone de unas **configuraciones iniciales consideradas seguras que constituyen un punto de partida para el uso del producto**.

32. Estas configuraciones seguras iniciales se recogen bajo las *Best Practice*. Se puede consultar en el siguiente enlace. Se recomienda seguir inicialmente los pasos de configuración iniciales indicados en dicho documento de *Best Practice – REF4*, para asegurar un punto de partida seguro.

33. Posteriormente la organización podrá modificar estas configuraciones como desee, según sus necesidades.

5.2 AUTENTICACIÓN

34. El producto dispone de autenticación para el acceso al servidor de gestión. Esta autenticación puede llevarse a cabo de las siguientes formas:

    - Autenticación local. Mediante base de datos local en el sistema operativo GAIA. Para la creación de usuarios locales, ver apartado 5.3.1 CONFIGURACION DE USUARIOS DEL SERVIDOR DE GESTIÓN.
    - Autenticación mediante servidores externos. Permite el uso de RADIUS y TACACS+. Ver apartado 5.2.1 SERVIDORES DE AUTENTICACIÓN EXTERNOS EN GAIA.

35. Cuando un agente conecta con el servidor de gestión, un proceso de autenticación identifica el usuario y agente que realiza la conexión. Por defecto, el producto no realiza ninguna verificación en este proceso. **Se debe activar el modo *Strong Authentication*, de tal forma que se autentique mediante Directorio Activo** (ver apartado 5.2.2 CONFIGURACIÓN DE DIRECTORIO ACTIVO).

36. La autenticación en el acceso al agente no es llevada a cabo por el producto, si no que será el usuario con acceso al dispositivo en el cual se encuentre instalado el agente quien utilizará este mismo.

5.2.1 SERVIDORES DE AUTENTICACIÓN EXTERNOS EN GAIA

37. El sistema operativo GAIA permite la autenticación de usuarios a través de servidores externos de autenticación. Se puede consultar el detalle de configuración de servidores de autenticación en el apartado *Authentication Servers* de la guía *Gaia R81 Administration Guide – REF2*.

5.2.2 CONFIGURACIÓN DE DIRECTORIO ACTIVO

38. El Directorio Activo se utiliza para autenticar las comunicaciones entre los agentes y el servidor de gestión. Se debe configurar para fortalecer la seguridad de dichas comunicaciones.
39. El detalle de configuración de Directorio Activo se puede consultar en el apartado *Configuring Active Directory Authentication* de la guía *Harmony Endpoint Server R81 Administration Guide – REF6*.

5.3 ADMINISTRACIÓN DEL PRODUCTO

40. La administración del producto se divide a su vez en dos (2) partes: la administración local del agente y la administración a través del servidor de gestión.
41. La administración local del agente es llevada a cabo por el usuario con acceso al dispositivo en el cual se encuentra instalado el agente. En este caso las acciones que se pueden llevar a cabo son muy limitadas, como, por ejemplo:
    - Forzar de forma manual la actualización de la configuración.
    - Escaneo manual del sistema.
    - Ver el estado de las distintas funcionalidades.
    - Llevar a cabo una actualización manual del módulo *anti-malware*.
    - Ver los detalles de las políticas configuradas, pero no editarlas.
    - En menú Avanzado, hay disponibles varios submenús que permiten realizar algunas acciones.

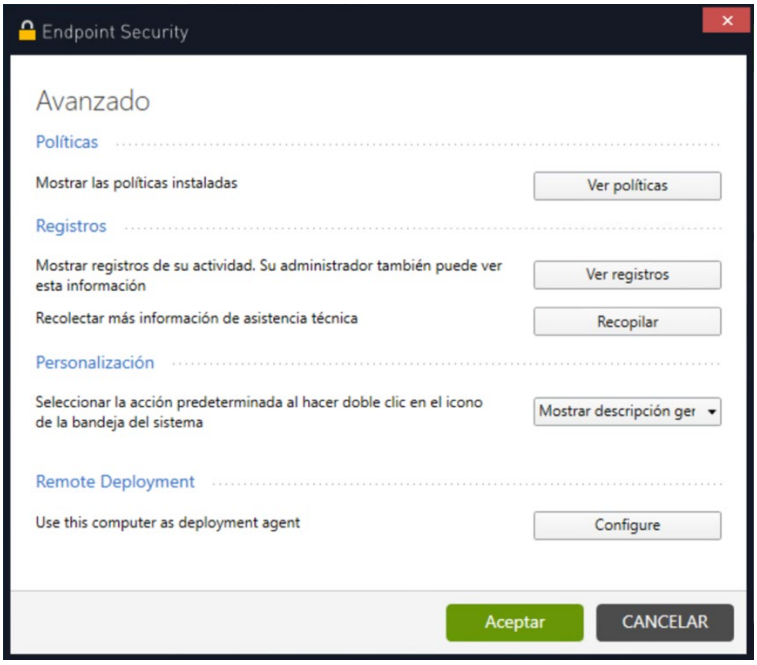

Figura 22: Interfaz de Usuario

42. Por otra parte, desde el servidor de gestión, se pueden llevar a cabo todas las acciones disponibles. Es desde este servidor desde donde **se deben configurar las políticas de seguridad que serán de aplicación a los distintos dispositivos** (ver apartado 5.9 CONFIGURACION DE POLITICAS DE SEGURIDAD PARA LOS DISPOSITIVOS FINALES).

43. La gestión a través del servidor se puede realizar mediante las siguientes interfaces:

    - Portal SmartConsole. Interfaz GUI de configuración.
    - Portal GAIA. Interfaz GUI de configuración.
    - Acceso local o mediante SSH CLI a GAIA.

5.3.1 CONFIGURACION DE USUARIOS DEL SERVIDOR DE GESTIÓN

44. La configuración de los usuarios del servidor de gestión se lleva a cabo en el sistema operativo GAIA. Para la creación de nuevos usuarios:

    - En la interfaz GUI de Gaia, ir a *User Management* > *Users*.
    - Hacer clic en *Add*.
    - Introducir el nombre y contraseña deseados. Seleccionar la casilla *User must change password at next logon*, para forzar el cambio de la contraseña por parte del usuario.
    - Seleccionar el tipo de acceso, *Web* o *Clish Access* (para el acceso CLI).
    - Seleccionar el rol deseado y hacer clic en *OK*.

45. Por defecto el producto dispone de los roles *adminRole* y *monitorRole*, que proporcionan permisos de escritura/lectura y solo lectura a todas las características disponibles respectivamente.
46. Para crear nuevos roles, se pueden seguir los siguientes pasos:
    - En la interfaz GUI de Gaia ir a *User Management > Roles*.
    - Hacer clic en *Add*.
    - Introducir el nombre y en el apartado *Features*, seleccionar los permisos deseados.
    - Hacer clic en *OK*.
47. El listado completo de permisos disponibles se puede consultar en el apartado *List of Available Features in Roles* de la guía *Gaia R81 Administration Guide – REF2*.

5.3.2 POLÍTICA DE CONTRASEÑAS

48. Para hacer uso de contraseñas seguras, el producto **permite la creación de una política de contraseñas**:
    - En la interfaz GUI de Gaia ir a *User Management > Password Policy*.
    - En *Password Strenght*, configurar los siguientes parámetros:
        - *Minimum Password lenght*. **Se debe configurar un valor de, al menos, 12 caracteres.**
        - *Disallow Palindromes*. Impide el uso de cadenas que se lean igual en ambas direcciones.
        - *Password Complexity*. **Se debe configurar un valor de 4,** para exigir el uso de cuatro tipos de caracteres (minúsculas, mayúsculas, números, caracteres especiales).
    - En *Password History*, configurar los siguientes parámetros:
        - *Check for password reuse*. Se debe **habilitar esta opción** para evitar la repetición de contraseñas antiguas.
        - *History lenght*. Indica la **antigüedad de contraseñas** que se verifica. Se debe configurar un valor de, **al menos, 5** contraseñas.
    - En *Mandatory Password change*, configurar los siguientes parámetros:
        - *Password expiration.* El número de días tras el cual una contraseña es inválida. **Se debe configurar un valor máximo de 60 días**.
        - *Warn users before password expiration.* Especifica el número de días previo a la expiración en el que se manda un recordatorio al usuario. **Por defecto el valor es de 7 días**.
        - *Lockout users after password expiration.* Bloquea a los usuarios en caso de no cambiar su contraseña antes de expirar. **Se recomienda**

configurar un valor de 1 día, de tal forma que, si la contraseña expira, se bloquea el usuario. Un administrador puede desbloquear los usuarios desde *Management > Users*.

- *Force users to change password at first login after password was changed from Users page.* **Se debe configurar este parámetro ya que obliga al cambio de contraseña a los usuarios tras acceder por primera vez al sistema.**

- En *Deny Access to unused accouts*, configurar los siguientes parámetros:
  - *Deny Access to unused accounts.* Si no se accede a la cuenta en un periodo determinado de tiempo, se bloquea.
  - *Days of non-use before lock-out*. Establece el número de días, por defecto tiene un valor de 365 días. **Se debe reducir a un valor lo más bajo posible**, acorde a las características de la organización.
- En *Deny Access after failed login attempts*, configurar los siguientes parámetros:
  - *Deny Access after failed login attempts.* Activa **el bloqueo de usuarios** tras el número configurado de fallos. **Se debe habilitar**.
  - *Block admin user.* Activa el bloqueo también para usuarios administradores. **Se debe habilitar**.
  - *Maximum number of failed attemts allowed*. Número de fallos permitido, **se debe configurar un valor de 3 intentos.**
  - *Allow access again after time*. Tiempo tras el cual se podrá volver a acceder a la cuenta. El valor por defecto es de 1200 segundos (20 minutos). **No se recomiendan valores inferiores a 5 minutos**.
- Hacer clic en *Apply*.

5.3.3 CONFIGURACIÓN DEL BANNER DE ACCESO

49. **Se debe configurar un *banner* de acceso** que informe al usuario de la sensibilidad de la información a la que va a acceder. Se puede configurar un mensaje de aviso en el *login* al sistema GAIA. Para ello:
    - En la interfaz GUI de Gaia ir a *System Management > Messages*.
    - En *Banner Message*, configurar el mensaje deseado para mostrar previo al acceso al sistema.
    - En *Message of the day*, configurar el mensaje deseado para mostrar una vez permitido el acceso.
    - Hacer clic en *apply*.

5.4 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

50. El producto utiliza los siguientes protocolos seguros en sus comunicaciones:
    - HTTPS. En las comunicaciones de los usuarios con la interfaz GUI de Gaia y con SmartConsole. Se hace uso de HTTPS por defecto y no requiere configuración.
    - SSHv2. En el acceso CLI al sistema operativo GAIA. Dicho protocolo no es configurable.
    - TLS. En las comunicaciones entre el servidor de gestión y los agentes. Por defecto, se permite el uso de las versiones TLSv1.2 y TLSv1. **Se debe hacer uso únicamente de TLSv1.2.**
51. **Para forzar el uso de TLSv1.2, seguir los siguientes pasos**:
    - En el servidor, mediante CLI, ejecutar el siguiente comando *cpstop.*
    - Editar el fichero *$UEPMDIR/apache/conf/ssl.conf*, cambiando el valor *SSLProtocol* a ***SSLProtocol TLSv1.2.***
    - Salvar los cambios en el fichero y ejecutar *cpstart*.
52. **Se debe deshabilitar el protocolo Telnet en el sistema operativo**. Para ello, en la interfaz GUI de Gaia, ir a *System Management > Network Access* y verificar que la casilla *Enable Telnet* se encuentra desactivada.

5.5 GESTIÓN DE CERTIFICADOS

53. Por defecto, las comunicaciones del producto utilizan certificados firmados por la CA interna del producto. **Se recomienda sustituir estos certificados por aquellos firmados por una CA válida y reconocida por el organismo**.
54. Los certificados utilizados deberán ser de tipo ECDSA. En caso de utilizar certificados RSA, **la longitud de la clave deberá ser igual o superior a 3072 bits.**
55. El producto hace uso de los siguientes certificados:
    - Certificado de la entidad de certificación. Se debe instalar tanto en el servidor como en los agentes.
    - Certificado de servidor utilizado para las comunicaciones entre los usuarios y la interfaz GUI.
    - Certificado de cliente para las conexiones *Syslog* sobre TLS.
56. Para importar un certificado (de CA, de servidor o de cliente) en el servidor, seguir los siguientes pasos:
    - Desde SmartEndpoint, ir a *Manage > Certificate Management.*
    - Hacer clic en *Import*.

- Seleccionar el tipo de certificado (.p12, .pem o .crt) y seleccionar el certificado que desea importarse.
- Hacer clic en *Next*. En caso de faltar la clave privada, se abrirá una nueva ventana para importarla.
- Hacer clic en *Finish* y, por último, en *Close*.

57. Una vez importados los certificados de servidor y de la CA, deberán instalarse. Para instalar el certificado de servidor, seguir los siguientes pasos:
    - Desde SmartEndpoint, ir a *Manage > Endpoint Server*.
    - Seleccionar el servidor y hacer clic en *Edit*.
    - Hacer clic en *Next > Manage*, seleccionar el certificado importado correspondiente y hacer clic en *Assign*.
    - Hacer clic en *Next > Finish*.
58. Para instalar el certificado de CA en los agentes, seguir los siguientes pasos:
    - Desde SmartEndpoint, ir a *Users and Computers > Global Actions.*
    - Hacer clic en *Push Operation*.
    - Seleccionar *Client Settings > Push CA Certificate*.
    - Hacer clic en *Next > Manage*. Seleccionar el certificado correspondiente.
    - Hacer clic en *Next* y en *Finish*.
    - El servidor enviará el certificado a los agentes.

5.6 SINCRONIZACIÓN

59. **La hora de los componentes de un sistema debe estar sincronizada**. Se puede configurar el tiempo del sistema manualmente en la interfaz de gestión de GAIA desde *System Management > Time*.
60. **Se recomienda configurar un servidor de tiempo mediante el protocolo NTP**. Para ello seguir los siguientes pasos:
    - Desde la interfaz de gestión de Gaia, ir a *System Management > Time*.
    - Hacer clic en *Set Time and Date*. Seleccionar *Set time and date automatically using Network Time Protocol (NTP).*
    - Introducir los datos del servidor NTP correspondiente. Seleccionar la versión de NTP. **Se recomienda hacer uso de la versión 4 de NTP.**
    - Hacer clic en *Apply*.

5.7 ALTA DISPONIBILIDAD

61. El producto permite dos (2) tipos de despliegue que proporcionan alta disponibilidad:

    - Gestión en alta disponibilidad. Se despliega un servidor principal, que tendrá conexión de forma directa o indirecta con un servidor secundario. Las bases de datos de ambos servidores se sincronizan, de forma manual o programada, para mantener la disponibilidad de los datos. En caso de caída del servidor principal, un administrador puede activar el servidor secundario.
    - Alta disponibilidad total. El funcionamiento es similar a la "gestión en alta disponibilidad", pero en esta ocasión la conexión es directa y se realiza a nivel de dispositivo, de tal forma que ambos dispositivos forman un cluster, manteniéndose sincronizados continuamente.

62. En el apartado *Installing a Security Management Server* de la guía *Installation and upgrade guide – REF7*, se pueden consultar los pasos necesarios para el despliegue de tipo "gestión en alta disponibilidad".

63. En el apartado *Installing a Standalone* de la guía *Installation and upgrade guide – REF7*, se pueden consultar los pasos necesarios para el despliegue de tipo "alta disponibilidad total". Durante el *wizard* de configuración inicial, se deberá configurar un servidor como primario y otro como secundario en el apartado *Clustering*.

5.8 AUDITORÍA

5.8.1 LOGS DE AUDITORÍA DE LOS AGENTES

64. Los agentes generan y almacenan logs de auditoría de forma automática. Estos se pueden consultar en el propio agente desde *Endpoint Security Main Page > Advanced > View Logs*.

65. En caso necesario, se pueden exportar a un fichero local dichos logs, desde *Endpoint Security Main Page > Advanced > View Logs*, haciendo clic en *Export > Edit > Export to file*.

66. Los logs almacenados en los agentes incluyen:

    - Tráfico *anti-malware* y VPN.
    - Comunicaciones del agente.
    - Eventos de las distintas funcionalidades.

67. Estos logs se envían de forma automática (no configurable) al servidor de gestión. En este, se almacenan en *C:\Documents and Settings\All Users\Application Data\CheckPoint\Endpoint\Security\Logs*. Cuando el fichero de log alcanza cierto tamaño, se genera uno nuevo.

68. El servidor solo almacena 10 ficheros de logs, tras lo cual elimina el más antiguo para continuar almacenando logs. Por esto, **se recomienda realizar el envío de los logs de los agentes a un servidor externo.**

69. Para ello se debe configurar la herramienta *Log exporter* del servidor de gestión:

    - Desde *SmartConsole*, ir a *Objects > More object types > Server > Log Exporter/SIEM.* En esta página se creará un nuevo objeto de *log exporter*.
    - Introducir los datos del servidor de auditoría externo al que se desea hacer el envío y hacer clic en *OK*. **Bajo el parámetro *Protocol*, se deberá seleccionar *TCP* para realizar el envío mediante TLSv1.2.**
    - Configurar el servidor para hacer uso de dicho objeto. Ir a *Gateways & Servers*, hacer clic sobre el servidor de gestión e ir a *logs > export*.
    - Hacer clic en *[+]* y seleccionar el objeto creado.
    - Por último, ir a *Menu > Install databese* y seleccionar *Install*.

70. Para permitir la conexión con el servidor de auditoría mediante TLS, una vez configurado el *Log exporter*, **se deberán importar los certificados necesarios** para la conexión, siguiendo los pasos indicados en el apartado 5.5 GESTIÓN DE CERTIFICADOS:

    - Certificado de la CA del servidor de auditoría.
    - Certificado de cliente del producto.

71. Por último, se debe configurar el producto para hacer uso de estos certificados:

    - Acceder mediante CLI. Ir al directorio del *Log exporter*:

      cd $EXPORTERDIR/targets/<Name of Log Exporter Configuration>
    - Crear un nuevo directorio para los certificados:

      mkdir -v certificates

      cd certificates
    - Transferir los certificados indicados anteriormente a dicho directorio.
    - Dar permisos a los certificados:

      chmod -v +r CertificadoCA

      chmod -v +r CertificadoCliente
    - Volver al directorio del *Log Exporter*:

      cd $EXPORTERDIR/targets/<Name of Log Exporter Configuration>
    - Modificar el fichero de configuración para hacer uso de los certificados. En el fichero *targetConfiguration.xml* incluir la dirección completa al ceriticado de cliente.

72. El detalle completo sobre la configuración del envío de logs mediante *Log exporter* se puede consultar en el apartado *Log Exporter* de la guía *Logging and Monitoring R81 Administration Guide – REF13*.

5.8.2 LOGS DE AUDITORÍA DEL SERVIDOR DE GESTIÓN

73. El servidor de gestión, a su vez, genera logs de auditoría propios, correspondientes a los cambios realizados tanto en el servidor como en el sistema operativo GAIA. Estos logs se almacenan localmente y se pueden enviar a un servidor externo.
74. El envío de los logs de auditoría del servidor de gestión solo se puede realizar mediante Syslog. Para ello:
    - En la interfaz de gestión de Gaia, ir a *System Management > System Logging*.
    - En la sección *Remote System Logging*, hacer clic en *Add*.
    - En el campo *IPv4 Address* introducir la dirección del servidor remoto al que se desean enviar los logs.
    - En el campo *Priority*, seleccionar *All* para realizar el envío de todos los logs al servidor remoto. Hacer clic en *OK*.
75. **Se recomienda el envío a un servidor remoto para una gestión centralizada y duradera de los registros de auditoría.**

5.9 CONFIGURACION DE POLITICAS DE SEGURIDAD PARA LOS DISPOSITIVOS FINALES

76. Para gestionar las políticas de seguridad de aplicación para los dispositivos finales, se debe utilizar la pestaña *Policy* de la consola *SmartEndpoint.*

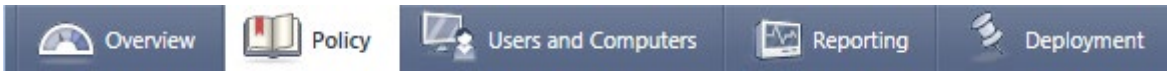

Figura 23: Menú SmartEndpoint

77. En dicha pestaña, desde *Policy rule base*, se pueden consultar las distintas políticas para cada módulo de seguridad. Estas políticas definen las protecciones para los agentes.
78. Cada política se compone de reglas. A continuación, se muestra un ejemplo de reglas en la pestaña *Policy*:

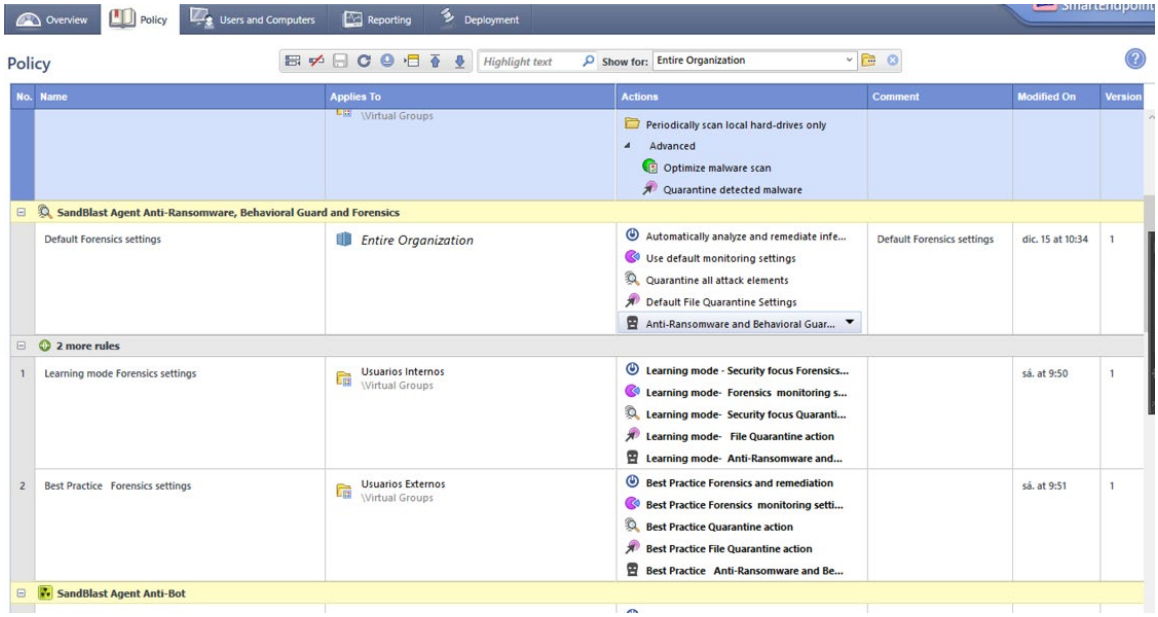

Figura 24: Conjunto de políticas

79. Cada regla se aplica a un módulo específico y a una parte concreta de la organización.

80. La política para cada componente tiene una regla predeterminada que se aplica a toda la organización. Se pueden cambiar las acciones de una regla predeterminada, pero no se puede hacer que la regla predeterminada se aplique a una parte específica de la organización. No se puede eliminar la regla predeterminada.

81. Se recomienda no modificar las reglas por defecto, si no clonarlas y modificar estas nuevas en su lugar. Para ello, en *SmartEndpoint*, hacer *click* derecho sobre la regla por defecto y seleccionar *Clone Rule*. Sobre esta nueva regla, la cual puede ser nombrada con cualquier texto descriptivo, es dónde se recomienda hacer todas las modificaciones pertinentes.

5.9.1 CONFIGURACION PREVIA

82. Es necesario organizar las políticas en grupos organizativos. Estos grupos pueden ser de *Active Directory* o grupos locales creados en el servidor de gestión.

83. Se pueden utilizar los siguientes grupos:

- Grupo de Directorio Activo - Estos se sincronizan automáticamente desde el Directorio Activo usando la integración con *Active Directory*. No se puede modificar un grupo de *Active Directory*. Ver *Active Directory Integration* para conocer más detalles sobre esta integración.
- Grupo virtual – Se pueden crear los grupos deseados o utilizar uno de los grupos virtuales predefinidos. Hay dos (2) tipos de grupo virtual:
  - Grupo virtual - Puede contener usuarios y computadoras.

- Grupo Dispositivos  - Sólo puede contener computadoras.

84. Los grupos virtuales funcionan como los grupos del Directorio Activo. Permiten:
    - Crear grupos y luego agregar usuarios y computadoras a los grupos de forma automática o manual.
    - Asignar políticas a grupos o usuarios virtuales.
    - Poner a los usuarios y a las computadoras en más de un grupo.
    - Seleccionar qué políticas tienen prioridad para los dispositivos finales que pertenecen a más de un grupo virtual.
85. Se pueden usar Grupos Virtuales con Directorio Activo para mayor flexibilidad o como alternativa al Directorio Activo. Los miembros de las unidades o grupos del Directorio Activo también pueden ser miembros de los Grupos Virtuales.
86. Para cada componente de seguridad de los puntos finales, solo se puede asignar una regla a un usuario o a un ordenador. Por lo tanto, si un usuario pertenece a más de un grupo, con diferentes reglas asignadas a cada grupo, el servidor de administración de seguridad de *endpoints* aplica la primera regla que coincida con los usuarios o el equipo.
87. Para crear grupos virtuales, seguir los siguientes pasos:
    - Desde SmartEndpoint, ir a *Users and Computers* > *Global Actions* > *New Virtual Group*.
    - Introducir el nombre deseado para el grupo y seleccionar el tipo (grupo virtual o de dispositivos).
    - Hacer clic en *Next* y seleccionar los miembros del grupo. Se pueden añadir más miembros posteriormente.
    - Hacer clic en *Finish*.
88. Para añadir usuarios de Directorio Activo a un grupo virtual, seguir los siguientes pasos:
    - Desde SmartEndpoint, ir a *Users and Computers* y hacer clic derecho en una unidad organizativa en *Directories*.
    - Seleccionar *Add content to a Virtual Group*.
    - Seleccionar el grupo y hacer clic en *OK*. Todos los usuarios de dicha unidad organizativa pertenecerán al grupo virtual.

5.10 COPIAS DE SEGURIDAD

89. El producto dispone de varios métodos para realizar una copia de seguridad del servidor de gestión y sus datos de configuración. Se diferencian por el tamaño, el tiempo de creación y el contenido.
90. Los procedimientos de respaldo disponibles son los siguientes:

- Gestión de Snapshots.
- Respaldo del sistema (y restauración del sistema).
- Guardar/Mostrar configuración (y Cargar configuración).

91. Todos los métodos son específicos para cada dispositivo y sólo pueden ser restaurados en el mismo modelo de dispositivo. En caso de utilizar un servidor virtual, las copias de seguridad realizadas se podrán recuperar en otro servidor virtual si es necesario.

92. **Se recomienda hacer uso del respaldo del sistema como método principal para realizar las copias de seguridad. Este método realiza una copia de seguridad de la configuración actual del sistema.**

93. Para ello, desde la interfaz GUI de Gaia, ir a *Maintenance > System Backup*. Desde esta página se pueden realizar copias de seguridad manualmente o pueden programarse.

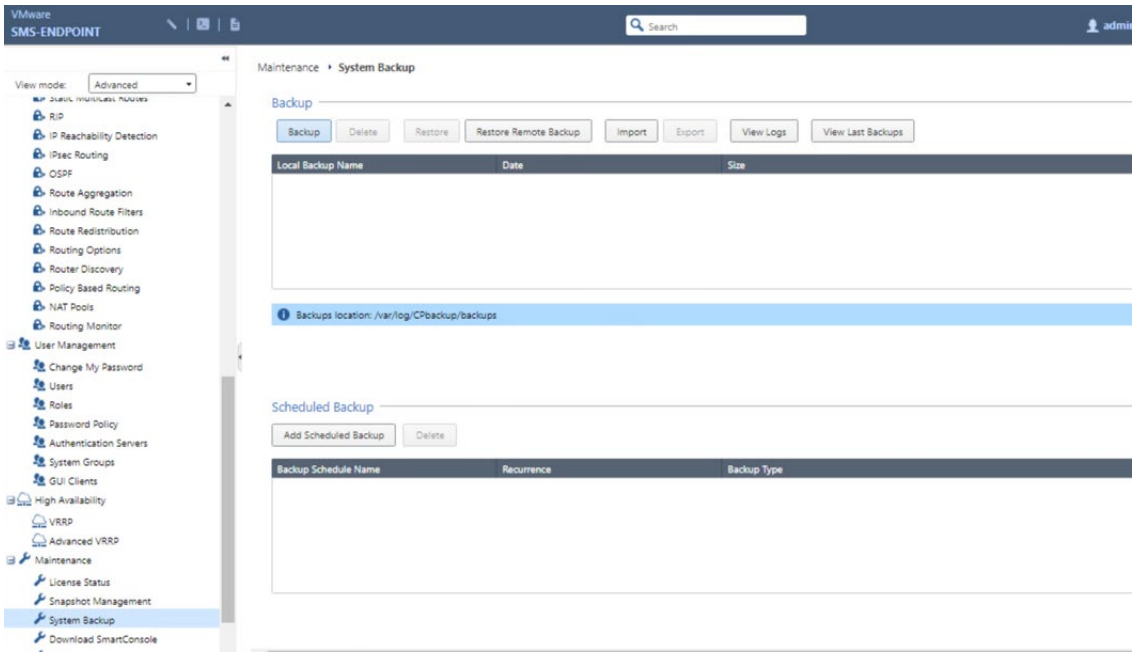

Figura 25: Generar Copia de Seguridad

94. Para programar la realización de una copia de seguridad de forma periódica y realizar su envío a un servidor externo, hacer clic sobre *Add Scheduled Backup*, rellenar los datos del servidor al que se desea hacer el envío. **Se debe seleccionar la opción *SCP Server*, de tal forma que el envío de la copia de seguridad se realice utilizando un protocolo seguro.** Por último, introducir la periodicidad y la hora con las que se desea realizar las copias y hacer clic en *Add*.

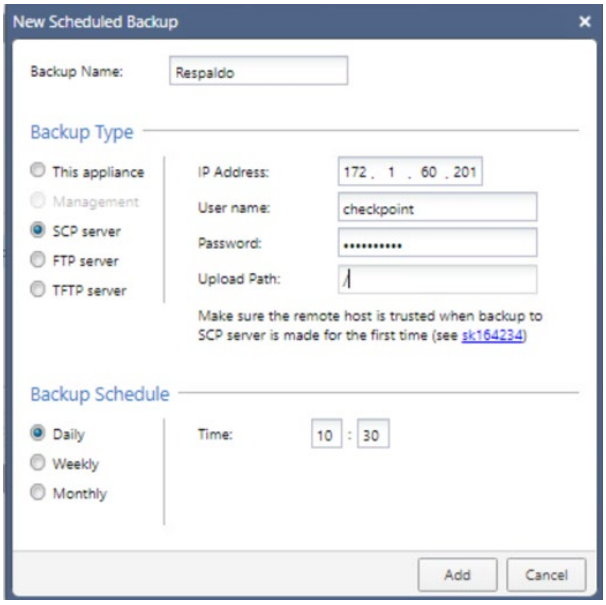

Figura 26: Generar Copia de Seguridad

95. El detalle de la configuración de los distintos métodos de copia de seguridad se puede consultar en el siguiente enlace:

    https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108902

5.11 ACTUALIZACIONES

96. **Los agentes deben estar actualizados, de acuerdo con las nuevas distribuciones publicadas por el fabricante.** Esta sección incluye el procedimiento para actualizar los agentes desplegados en los dispositivos finales:

    - Se deberá actualizar el cliente inicial y el paquete de componentes de seguridad del punto final al mismo tiempo. No se puede actualizar el Cliente inicial por sí mismo.
    - Durante la actualización no puede eliminar el componente de Cifrado de disco completo.
    - Se podrá cambiar todos los demás componentes y todos los ajustes de configuración de los componentes.

97. El proceso para actualizar los agentes de forma manual es el mismo que para el despliegue inicial, eligiendo la versión deseada. Para ello ver el apartado 4.4 INSTALACIÓN DEL AGENTE.

5.11.1 ACTUALIZACIÓN CON REGLAS DE DESPLIEGUE

98. Otra opción disponible es el despliegue de las actualizaciones mediante reglas. La política de configuración de clientes controla si los usuarios pueden posponer una instalación de actualización o si la actualización se instala en los clientes

inmediatamente. Puede configurar los ajustes en la Política de configuración de clientes.

99. Para actualizar los clientes con las asignaciones de despliegue:

    - En *SmartConsole*, en la pestaña *Despliegue*, seleccionar una regla y cambiar su Versión del cliente del punto final en la columna Versión del cliente.
    - Todos los equipos asignados a esa regla de la política se actualizarán.
    - Opcional: Cambiar a quién se aplica la regla en la columna *Aplica a*.
    - Seleccionar *Archivo > Guardar* o hacer clic en el icono *Guardar*.
    - Seleccionar *Archivo > Instalar políticas* o hacer clic en el icono *Instalar políticas*.
    - El agente en cada cliente asignado descargará el nuevo paquete. La instalación del cliente se inicia según la configuración de la regla de la política de configuración del cliente. Se puede configurar:
        - Si la política de configuración del cliente obliga a la instalación y se reinicia automáticamente sin notificación al usuario.
        - Si el Agente Final envía un mensaje al usuario de que una instalación está lista y le da la oportunidad de posponer la instalación o guardar el trabajo e instalarla inmediatamente.
    - Si el usuario no hace clic en *Instalar ahora*, la instalación se inicia automáticamente después de un tiempo de espera.
    - Después de la instalación, el agente del punto final puede reiniciar el ordenador.

5.11.2 ACTUALIZACIÓN CON UN PAQUETE EXPORTADO

100. Otra alternativa es actualizar un cliente a un nuevo paquete que incluya los mismos componentes que tiene ahora. Para actualizar los clientes con un paquete exportado:

    - En *SmartConsole*, en la pestaña de *Despliegue*, ir a *Paquetes de Exportación*.
    - Seleccionar un paquete y hacer clic en *Actualizar perfil.*
    - Se abre un mensaje que muestra si hay una actualización disponible.
    - Hacer clic en *Sí* para confirmar que desea actualizar el perfil.
    - En la ventana del Paquete de Exportación:
        - Para los paquetes dinámicos, se selecciona cualquier CPU. Para los paquetes MSI, se seleccionan las plataformas (32-Bit y/o 64 bit) a exportar para portátiles y ordenadores de sobremesa.
    - Introducir o buscar una carpeta de destino.

- Seleccionar *OK*.

101. Los archivos del paquete se descargan en la ruta especificada. Se crea automáticamente una carpeta diferente para cada opción seleccionada en el paso 4. Cuando se utiliza el Paquete Dinámico, el paquete exportado es un ejecutable autoextraíble (*.EXE). De forma predeterminada, el nombre del archivo es EPS.exe. Para otros tipos de paquete, el nombre del paquete es EPS.msi y/o PreUpgrade.exe.

102. Enviar los archivos del paquete a los usuarios finales. Los usuarios de los puntos finales instalan manualmente los paquetes. Deben utilizar los privilegios de administrador.

103. También se puede utilizar un *software* de implementación de terceros, una ruta de red compartida, correo electrónico o algún otro método.

5.12 FUNCIONES DE SEGURIDAD

5.12.1 ANTIMALWARE

104. Check Point *Anti-Malware* protege su red de todo tipo de amenazas de *malware*, desde gusanos y troyanos hasta *adware* y registradores de pulsaciones de teclas. Utilice *Anti-Malware* para gestionar de forma centralizada la detección y el tratamiento de *malware* en sus ordenadores de punto final.

105. El *Endpoint Security Management* Server actualiza regularmente las definiciones de *Anti-Malware* desde un servidor de actualización de Check Point. Las principales funciones son:

- Escaneo de todos los archivos.

  Por defecto, todos los archivos son escaneados cuando se abren o se usan.

  Se pueden configurar los procesos de confianza como excepciones. Cuando un proceso de confianza accede a un archivo, este no se analiza. **Se debe excluir un proceso solo si confía plenamente en él y si se está seguro de que no es *malware*.**

- Comprobación de existencia de actualizaciones de firmas de *malware*.

  Anti-Malware recibe actualizaciones de firmas de *malware* a intervalos regulares para asegurarse de que puede escanear en busca de las amenazas más recientes.

- Escaneo periódico anti-malware.

  El *Anti-Malware* escanea los *endpoints* en busca de *malware* a intervalos regulares para asegurarse de que los archivos sospechosos son tratados, puestos en cuarentena o eliminados.

- Escaneo periódico de los discos duros locales.

  El escaneo programado explora áreas críticas del sistema, por ejemplo: el sistema operativo, los procesos y la memoria.

- Optimización del análisis de malware.

  Las opciones de optimización del análisis permiten realizar análisis de *malware* rápidamente y con menos impacto en el rendimiento y los recursos del sistema.

- Detección de *malware* en cuarentena.

106. En el apartado *Anti-Malware* de la guía *Harmony Endpoint Server R81 Administration Guide – REF6*, se puede consultar el detalle de configuración.

5.12.2 ANTI-RANSONWARE, BEHAVIORAL GUARD AND FORENSICS

107. El componente 'Forense' y '*Anti-Ransomware*' del Agente *Harmony Endpoint* monitoriza las operaciones de los archivos, los procesos y la actividad de la red para detectar comportamientos sospechosos. También analiza los ataques detectados por otros componentes del cliente o por la puerta de enlace de seguridad de puntos de control. Aplica la reparación a los archivos maliciosos.

108. El *Anti-Ransomware* monitorea constantemente los archivos y procesos para detectar actividades inusuales. Antes de que un ataque de *Ransomware* pueda cifrar los archivos, el *Anti-Ransomware* hace una copia de seguridad de los archivos en una ubicación segura. Una vez detenido el ataque, elimina los archivos implicados en el mismo y restaura los archivos originales de la ubicación de la copia de seguridad.

109. Todos los detalles de los ataques se organizan en el Informe de análisis forense. También puede configurar el componente Forense para analizar los incidentes que son detectados por una solución *Anti-Malware* de terceros.

110. Si los servidores de *Endpoint Security* no tienen conectividad a Internet, la información forense se almacena y se envía para su evaluación inmediatamente cuando un servidor se conecta a Internet.

111. En la configuración de la cuarentena predeterminada de archivos, los archivos se mantienen en cuarentena durante 90 días y los usuarios pueden eliminar permanentemente elementos de la cuarentena.

112. En el apartado *SandBlast Agent Anti-Ransomware* de la guía *Harmony Endpoint Server R81 Administration Guide – REF6*, se puede consultar el detalle de configuración.

5.12.3 ANTI-BOT

113. El componente *Harmony Endpoint Anti-Bot* monitoriza los *endpoints* para identificar comunicaciones relacionada con bots y alerta a los administradores sobre los dispositivos afectados por su actividad. El comportamiento predeterminado es que el anti-bot solo bloquea la actividad cuando es casi seguro que la actividad es maliciosa.

114. Se pueden configurar entidades de confianza, que no serán inspeccionadas por el componente Anti-Bot. Estas se llaman *Exclusiones de Detección*.

115. En el apartado *Sandblast Agent Anti-Bot* de la guía *Harmony Endpoint Server R81 Administration Guide – REF6*, se puede consultar el detalle de configuración.

5.12.4 THREAT EXTRACTION, EMULATION AND ANTI-EXPLOIT

116. La emulación de amenazas detecta ataques de día cero. Los archivos del *endpoint* se envían a una *sandbox* para su emulación y así detectar ataques evasivos de día cero.

117. *Threat Extraction* protege proactivamente a los usuarios frente a contenido malicioso. Entrega rápidamente archivos seguros mientras se inspeccionan los archivos originales en busca de posibles amenazas.

118. Como parte de la solución de extracción y emulación de amenazas, cuando se instala el agente *Harmony Endpoint* en un equipo cliente, la extensión del navegador del agente *Harmony Endpoint* también se instala en el navegador de Google Chrome. La Extensión del navegador del agente *Harmony Endpoint* protege contra los archivos maliciosos que provienen de fuentes de Internet.

119. El componente de prevención de *phishing* comprueba las diferentes características de un sitio web para asegurarse de que no pretende ser un sitio diferente y utiliza la información personal de forma maliciosa. Previene los intentos de explotación de aplicaciones legítimas, analiza los archivos estáticos y bloquea los archivos maliciosos.

120. En el apartado *SandBlast Agent Threat Extraction and Threat Emulation* de la guía *Harmony Endpoint Server R81 Administration Guide – REF6*, se puede consultar el detalle de configuración.

6 FASE DE OPERACIÓN

121. Desde *SmartEndpoint* se pueden consultar informes sobre el estado de las conexiones con los agentes Endpoint Security y el cumplimiento de las políticas de seguridad y otros eventos de seguridad. Se pueden consultar los logs de auditoría desde las pestañas *Logs* y *Monitor*.

122. **Se debe verificar periódicamente esta información para evitar y prevenir cualquier problema que pudiese surgir.**

123. Se recomienda también:

- **Realizar copias de seguridad periódicas y almacenarlas en un servidor externo.**
- **Llevar a cabo comprobaciones del *hardware* y *software*** para asegurar que no se han introducido componentes no autorizados.
- **Aplicar regularmente los parches de seguridad disponibles**.

7 CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Descarga y verificación del software	☐	☐	
Instalación y despliegue del Agente	☐	☐	
Aplicación de licencias	☐	☐	
CONFIGURACIÓN			
AUTENTICACIÓN			
Configuración del servidor RADIUS externo	☐	☐	
Configuración del Directorio Activo	☐	☐	
ADMINISTRACIÓN DEL PRODUCTO			
Creación de usuarios y roles	☐	☐	
Configuración de la política de contraseñas	☐	☐	
Configuración del banner de acceso	☐	☐	
CONFIGURACIÓN DE PROTOCOLOS SEGUROS			
Habilitar el uso de TLSv1.2 únicamente	☐	☐	
GESTIÓN DE CERTIFICADOS			
Importar certificado de servidor y de CA	☐	☐	
SINCRONIZACIÓN			
Configuración de NTP	☐	☐	
AUDITORÍA			
Envío de registros por syslog	☐	☐	
CONFIGURACIÓN DE POLÍTICAS DE SEGURIDAD			
Creación de las políticas de seguridad	☐	☐	
COPIAS DE SEGURIDAD			
Configuración de las copias de seguridad periódicas	☐	☐	

8 REFERENCIAS

REF1 Quantum Security Management R81 Administration Guide
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Welcome.htm

REF2 Gaia R81 Administration Guide
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Gaia_AdminGuide/Topics-GAG/Gaia-Overview.htm

REF3 R81 CLI Reference Guide
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_CLI_ReferenceGuide/Topics-CLIG/Introduction.htm

REF4 Best Practice Configuration
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk154052

REF5 Requisitos Hardware
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_RN/Topics-RN/Hardware-Requirements.htm?TocPath=Open%20Server%20Hardware%20Requirements%7C_____2

REF6 Harmony Endpoint Server R81 Administration Guide
https://sc1.checkpoint.com/documents/R81/SmartEndpoint_OLH/EN/Front-Matter/Front-Matter-How-to-Search-in-this-Book.htm?tocpath=_____1

REF7 Installation and upgrade guide R81
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/Topics-IUG/Installing-Security-Management-Server.htm?tocpath=Installing%20a%20Security%20Management%20Server%7C_____0

REF8 R81 Fresh Install
https://supportcenter.checkpoint.com/supportcenter/portal/user/anon/page/default.psml/media-type/html?action=portlets.DCFileAction&eventSubmit_doGetdcdetails=&fileid=109064

REF9 Check Point R81
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk166715

REF10 Asignar Contratos de Licencia
https://sc1.checkpoint.com/documents/R81/SmartEndpoint_OLH/EN/Topics-EPSG/Endpoint-Security-Licenses.htm?tocpath=Endpoint%20Security%20Licenses%7C_____0#Getting

REF11 Backup Gaia
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108902

REF12 Learning Mode
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk153714

REF13 Logging and Monitoring R81 Administration Guide
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGuide/Topics-LMG/Log-Exporter.htm?tocpath=Log%20Exporter%7C_____0

9 ABREVIATURAS

AD	*Active Directory* (Directorio Activo)
CLI	*Command Line Interface*
CPUSE	*Check Point Upgrade Service Engine*
DNS	Domain Name System
ENS	Esquema Nacional de Seguridad.
GUI	*Graphical User Interface* (Interfaz Gráfica de Usuario)
HEP	*Harmony Endpoint*
NTP	*Network Time Protocol* (Protocolo de Tiempo de Red)
SBA	*SandBlast Agent*
SNMP	*Simple Network Management Protocol*
VPN	*Virtual Private Network* (Red Privada Virtual)

PUBLICACIONES DE DEFENSA

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