centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1106

Procedimiento de Empleo Seguro
Forescout CounterACT v8.1

Septiembre 2021

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

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.01.27 13:05:08 +01'00'

NIPO: 083-21-168-0.

Fecha de Edición: septiembre 2021

ÍNDICE

1. INTRODUCCIÓN

1. La plataforma CounterACT de ForeScout es un *appliance* de seguridad sin agente que identifica y evalúa la infraestructura de red, dispositivos y aplicaciones de forma dinámica. En cuanto se conecta a la red, es capaz de establecer y ejecutar las normas de seguridad establecidas en cada organización.

Ilustración 1. *Appliance* físico ForeScout CounterACT.

2. Es una herramienta NAC (*Network Access Policy*) que determina rápidamente quién es el usuario, el propietario y el sistema operativo del dispositivo que se conecta a la red, al igual que su configuración, el *software*, los servicios, el estado de parches y la presencia de agentes de seguridad en los dispositivos. También proporciona corrección, control y supervisión continua de estos dispositivos.

3. La plataforma ForeScout realiza estas acciones en dispositivos de red de la organización y en los dispositivos personales (BYOD), sin que sean necesarios agentes de *software* ni conocimientos previos del dispositivo. Se implementa rápidamente dentro del entorno existente y solo en escasas ocasiones requiere cambios de infraestructura, actualizaciones o reconfiguración de dispositivos.

4. Tradicionalmente, la seguridad de redes se ha enfocado en el bloqueo de los ataques externos con *firewalls* y sistema de prevención de intrusiones. Sin embargo, estas herramientas de seguridad no protegen contra las amenazas internas que causan cada vez más incidentes y problemas de seguridad. Se encuentran entre estas amenazas:

    - Invitados: Los invitados van a las instalaciones y llevan sus propios equipos. Por lo general, necesitan acceso a Internet. Si se otorga acceso ilimitado a estos invitados, se pone en riesgo la red frente a ataques.
    - Usuarios inalámbricos y móviles (BYOD): Los empleados utilizan sus propios teléfonos inteligentes, tabletas y computadoras portátiles. Sin un control adecuado, estos dispositivos pueden infectar la red o causar la pérdida de datos.
    - Dispositivos de Internet de las cosas (IoT): Los dispositivos no tradicionales siguen expandiendo la superficie de ataque porque agregan dispositivos no administrados, tales como proyectores con dirección IP, termostatos, controles de iluminación, cámaras de seguridad y más.
    - Dispositivos no autorizados: Los empleados bienintencionados pueden extender la red con concentradores de cableado de bajo costo, servidores departamentales, enrutadores y puntos de acceso inalámbricos que pueden causar inestabilidad y vulnerabilidad en la red.

- Malware y redes de *bots*: Una vez que la red está en riesgo, los dispositivos conectados a ella pueden ocasionar *pivots attacks*, en los que los terceros pueden examinar la red y exfiltrar datos.

2. OBJETO Y ALCANCE

5. El presente documento tiene como objetivo detallar las configuraciones de seguridad de la **plataforma Forescout, versión 8.1,** de forma que la protección y funcionamiento del producto se realice de acuerdo a unas garantías mínimas de seguridad.

6. El producto se presenta en formato virtual, para su instalación en *appliances* virtuales; y en formato físico, a través de los siguientes *appliances* físicos:

    - ***CT-R, CT-100, CT-1000, CT-2000, CT-4000, CT-10000, CEM-5, CEM-10, CEM-25, CEM-50, CEM-100, CEM150, CEM-200, 5110, 5120, 5140 y 5160.***

7. Los distintos componentes de la plataforma Forescout, permiten ser instalados de forma virtual o física dentro de los centros de datos de la organización o a través de soluciones de cloud en AWS o Azure. Los componentes de la plataforma son:

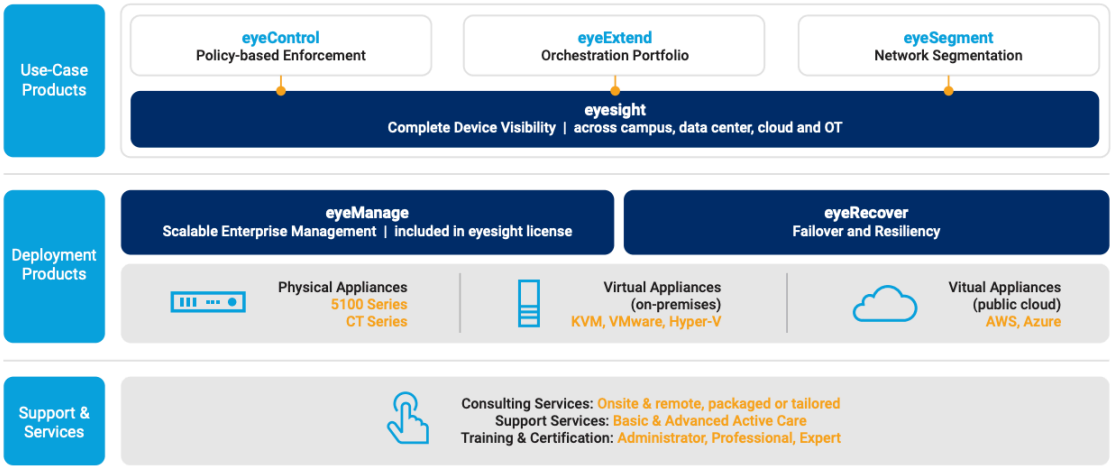

Ilustración 2. Componentes de la plataforma Forescout

3. ORGANIZACIÓN DEL DOCUMENTO

8. El presente documento se estructura de acuerdo con los siguientes capítulos:

   a) **Apartado 4.** En este apartado se recogen tanto recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto como aspectos relativos a la seguridad del mismo proceso.

   b) **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.

   c) **Apartado 6.** En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de operación del producto, para lograr un funcionamiento en el día a día de forma segura.

   d) **Apartado 7.** En este apartado aparece un *checklist* con las tareas a realizar y el estado de cada una de ellas.

   e) **Apartado 8.** Referencias utilizadas en el presente documento.

   f) **Apartado 9.** En el último apartado se hace referencia a las diferentes nomenclaturas utilizadas.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

9. En caso de adquirir el producto *hardware*, este llegará embalado dentro de una caja de cartón de Forescout en la que se encontrarán:
    - Equipo CounterACT.
    - Marco frontal.
    - Rieles (abrazaderas de montaje).
    - Cable(s) de energía.
    - Cable de conexión de la consola DB9 (para conexiones en serie únicamente).
    - Información de seguridad de productos, de medioambiente y regulatoria de ForeScout.
    - Documento de Introducción general (para dispositivos 51xx únicamente).
10. Se debe verificar que la caja no presente indicios de haber sido abierta o manipulada y que incluya todo el contenido descrito. En caso de presentar cualquier problema, se recomienda ponerse en contacto con su contacto de Forescout.
11. En caso de obtener el producto virtualizado, se deberá realizar la descarga del fichero desde la página de soporte de ForeScout. El acceso a dicha página se realizará utilizando el usuario y contraseña obtenidos por correo desde la dirección *license@forescout.com*.
12. La descarga del fichero viene acompañada con un valor de hash para verificar la integridad del fichero descargado. Se recomienda realizar el hash del fichero descargado y compararlo con el presente en la página de descarga, para **verificar su integridad.**

4.2 GESTIÓN DE LICENCIAS

13. La obtención de la licencia de activación se puede llevar a cabo mediante correo electrónico o accediendo a la web de Forescout.
14. En el caso de correo electrónico, se debe contactar con la dirección license@forescout.com y se recibirá un fichero de licencia para que sea instalado manualmente dentro de la consola de administración de Forescout.
15. Se puede consultar el detalle de los tipos de licencia en el siguiente enlace.
16. La gestión de licencias a partir de la versión 8 se puede hacer utilizando dos (2) métodos distintos:
    - FLEXX: Licencia de pago por consumo de activos a monitorizar.

- PALM: Licencia de pago por activos soportados por cada servidor.

17. La licencia predeterminada del dispositivo dependerá del modo de licencia que se utilice en la implementación.
18. Si la implementación de la plataforma ForeScout está funcionando en modo PALM, se puede comenzar a trabajar usando una licencia de demostración, válida por 30 días. Durante este tiempo, se deberá recibir una licencia permanente de ForeScout y ubicarla en una carpeta accesible en su disco o red. En caso de utilizar licenciamiento FLEXX, no se dispone de licencia de prueba.
19. El detalle sobre la activación de las licencias se puede consultar en la guía *Flexx Licensing How-to Guide – REF4*.
20. Tras obtener la licencia del Portal de Soporte de Forescout, se debe subir a la consola de la plataforma. Los pasos a seguir son los siguientes:
    - Seleccionar *Options* desde el menú *Tools*.
    - Seleccionar *Licenses*. Hacer clic en *Activate*, se abrirá la ventana de activación de licencias.
    - Introducir el ID de despliegue (recibido en el email correspondiente a la adquisición de las licencias) y seleccionar *Download License Request.*
    - Ir al portal de soporte de Forescout, en la sección de *License Management*, subir la petición descargada (al seleccionar *Download License Request*) y descargar el fichero de licencia.
    - Ir de nuevo a *Options > Licenses* y seleccionar *Activate*. Hacer clic en *Choose File* y subir el fichero de licencia descargado.
    - Finalmente seleccionar *Close.*

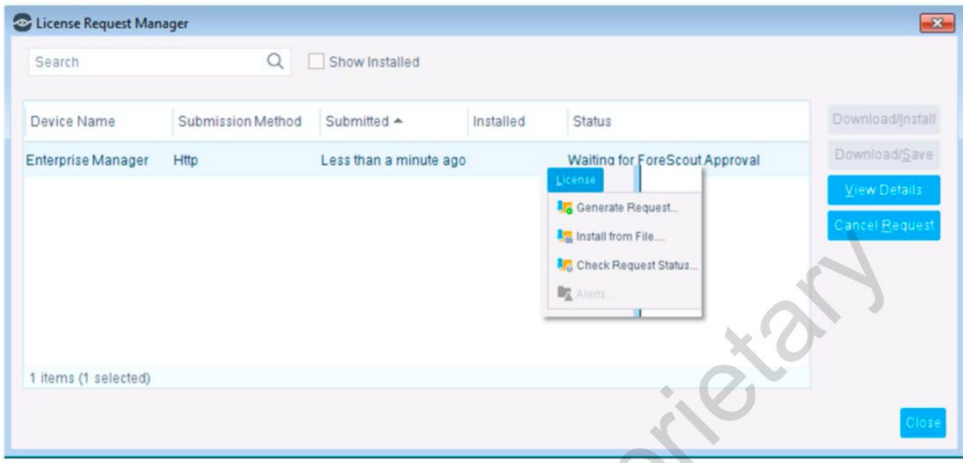

Ilustración 3. Proceso de licenciamiento

21. Es necesario instalar la licencia siguiendo los pasos descritos antes de que expire la licencia de demostración a los 30 días. En caso necesario puede pedirse una extensión de la licencia de prueba. Las licencias de demostración se deben instalar también siguiendo dichos pasos.

22. Se recibirán alertas cuando la licencia de demostración vaya a expirar. Consultar el apartado *License Management* de la Guía *Forescout Administration Guide v8.2.2 – REF2* para más información sobre las alertas de licencia de demostración.

23. Se debe tener también en cuenta:

    - Como mínimo un dispositivo deberá tener acceso a internet. Esta conexión se usa para validar las licencias con el servidor de la Licencia de ForeScout.
    - Las licencias que no pueden ser autenticadas durante un mes serán revocadas. Se enviará un correo electrónico de advertencia una vez al día indicando que existe un error de comunicación con el servidor. Consultar la guía *Forescout Installation Guide v8.2.2 – REF1* para más información.
    - Si la implementación de la plataforma Forescout está funcionando en Modo de licencia centralizado (modo FLEXX), el Administrador recibirá un correo electrónico cuando se habilite la licencia y esté disponible en el Portal del usuario de ForeScout (*support.forescout.com*). Una vez disponible, el administrador de la implementación puede activar la licencia en la consola, siguiendo los pasos indicados anteriormente. Hasta que la licencia esté activada, las características de la plataforma ForeScout no funcionarán correctamente. Por ejemplo, las políticas no serán evaluadas y las acciones no se llevarán a cabo.

4.3 DIMENSIONAMIENTO DEL EQUIPO

24. Para hacer un dimensionamiento correcto del *appliance(s)* a instalar por la organización es necesario conocer una serie de parámetros:

    - Número aproximado de IPs a gestionar por el producto.
    - Electrónica de red de la que se dispone (Fabricante/Modelo y *Firmware*) de los *switches* y de los puntos de acceso *Wireless*.
    - Tipo de directorios a integrar (*Active Directory, Radius, LDAP*).
    - Rangos de redes y VLANs a gestionar.

25. Dependiendo de si el despliegue de los *appliances* es físico o virtualizado, se deben tener en cuenta los requisitos descritos en la guía de acceso público de Forescout, en el siguiente enlace.

4.4 REQUISITOS PARA LA INSTALACIÓN

26. Para la puesta en marcha del *appliance* son necesarios/recomendados los siguientes datos:

    - Dirección IP para la gestión del producto.
    - Una dirección IP disponible por cada VLAN con la que se vaya a integrar en Forescout. También es posible utilizar únicamente IP(s) desde la que alcanzar las diferentes *vlan* o segmentos de red.

- Un *port mirror* o *port Span*, en el switch de los puertos a monitorizar o VLANs, en este caso la VLAN de cuarentena.
- Un *trap SNMP* del switch a la IP del producto para verificar cuando se activa o desactiva un puerto (*link up/link down*).
- Una cuenta con privilegios para que pueda escribir los datos de configuración del directorio con el que integrar el producto (IPs, usuario administrador/contraseña, DNS, etc).
- Para el control de los PCs corporativos, sin la instalación de agente, es necesario que esté activado el servicio de "*Registro remoto*" de *Windows* en los dispositivos. Si es necesario, se deberá crear una política administrativa de directiva de grupo en el servidor de Micorsoft[1] (*GPO – Group Policy Object*) para arrancar dicho servicio. También es necesario acceso a los puertos TCP 139 y TCP 445.
- Conectividad necesaria entre la plataforma ForeScout y la infraestructura de la organización.

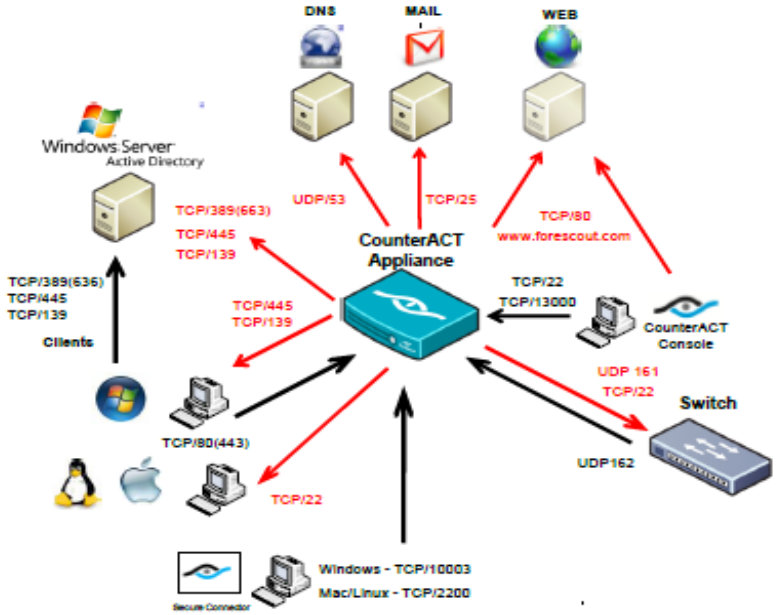

Ilustración 4. Conectividad de la plataforma Forescout

- Flujos de tráfico requeridos para el correcto funcionamiento de la plataforma:

[1] Consultar el enlace para más información sobre la creación y gestión de GPOs: https://docs.microsoft.com/es-es/azure/active-directory-domain-services/manage-group-policy

	Protocol		CounterACT	
22	TCP	SSH	To	Allows endpoints to access the CounterACT command line interface (CLI).
22	TCP	SSH	From	Allows for SSH management of switches, Macintosh, and Linux devices.
25	TCP	SMTP	From	Allows CounterACT access to the enterprise mail relay.
53	UDP	DNS	From	Allows CounterACT access to resolve internal IP addresses.
80	TCP	HTTP	To	Allows HTTP redirection.
80	TCP	HTTP	From	Pulls updates from forescout.com
123	UDP	NTP	From	Allows CounterACT to access time server.
139	TCP	NetBIOS	From	Allows CounterACT to remotely manage windows devices.

Ilustración 5. Flujo de tráfico (I).

161	UDP	SNMP	From	Allows CounterACT to communicate with network switches and routers.
162	UDP	SNMP	To	Allows CounterACT to receive SNMP traps from network switches and routers.
389	TCP	LDAP	From	Query Active Directory information.
443	TCP	HTTPS	To	Allows HTTP redirection using SSL.
445	TCP	MS DS	From	Allows CounterACT to remotely manage windows devices.
514	UDP	syslog	To/From	Sends syslog messages to syslog server. Receives syslog messages supporting advanced capabilities.
636	TCP	LDAP over SSL	From	Query Active Directory information.
1433	TCP	MS SQL	From	Allows CounterACT to query SCCM database.
2200	TCP	SecureConnector	To	Allows a SecureConnector tunnel between Mac/Linux endpoints and the Appliance.
10003	TCP	SecureConnector	To	Allows a SecureConnector tunnel between windows endpoints and the Appliance.
13000	TCP	CounterACT	To	Access appliance from console.
Any	Any	Any	From	Permits scanning and NMAP identification of devices.

Ilustración 6. Flujo de tráfico (II).

- Lo indicado a continuación aplica para soluciones de dispositivos móviles iOS/Android a través del *plugin* de integración MSM (*Mobile Security Module*):
    - Puertos 2195/HTTPS y 2196/HTTPS desde la IP de gestión de ForeScout como tráfico de salida hacia los servidores de Apple
    - Puertos 5223/TCP como tráfico de salida hacia la red 17.0.0.0/8. Los dispositivos iOS utilizan este puerto para comunicarse con los servidores de Apple
    - Puerto 443/HTTPS
- Lo indicado a continuación aplica para la solución MDM (*Mobile Device Management*) a través del *plugin MaaS360*:
    - Puertos 5223/TCP como tráfico de salida hacia la red 17.0.0.0/8. Los dispositivos iOS utilizan este puerto para comunicarse con los servidores de Apple

4.5 INSTALACIÓN

27. A continuación se muestran de forma gráfica las dimensiones de los appliances físicos para su instalación en un rack de 19 ´´. Teniendo en consideración de su peso de 21.9 kg.

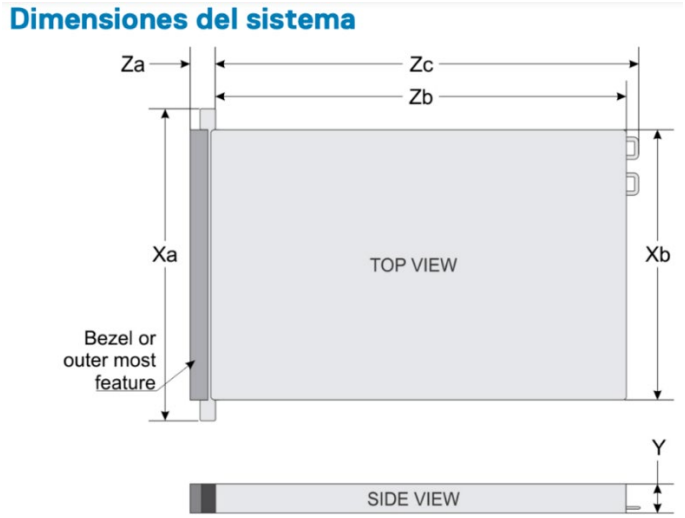

Ilustración 7. Dimensiones appliance físico (I)

Sistema	Xa	Xb	S	Za (con bisel)	Za (sin bisel)	Zb*	Zc
4 x 3,5 pulgadas o 10 x 2,5 pulgadas	482,0 mm (18,97 pulgadas)	434,0 mm (17,08 pulgadas)	42,8 mm (1,68 pulgadas)	35,84 mm (1,41 pulgadas)	22 mm (0,87 pulgadas)	733,82 mm (29,61 pulgadas)	772,67 mm (30,42 pulgadas)
8 x 2,5 pulgadas	482,0 mm (18,97 pulgadas)	434,0 mm (17,08 pulgadas)	42,8 mm (1,68 pulgadas)	35,84 mm (1,41 pulgadas)	22 mm (0,87 pulgadas)	683,05 mm (26,89 pulgadas)	721,91 (28,42 pulgadas)

Ilustración 8. Dimensiones appliance físico (II).

28. Estas instrucciones pueden variar debido a la versión de cada sistema, así como su tipo, virtual o físico.

29. La instalación se puede realizar como *Appliance* o como *Enterprise Manager*:

    - *Appliance*. Dispositivo dedicado que supervisa el tráfico que pasa por la red de la organización. Protege contra actividad maliciosa, realiza protección NAC y gestiona vulnerabilidades. Siempre será necesario disponer de, al menos, un dispositivo configurado como *appliance,* ya que son los encargados de proteger la red.

    - *Enterprise Manager*. Dispositivo de agregación que se comunica con múltiples dispositivos Forescout distribuidos en una organización. Gestiona la actividad y las políticas de los dispositivos y recoge información sobre la actividad maliciosa detectada en cada *appliance*. Permite la visualización de esta información y la elaboración de informes. Solo será necesaria su instalación en caso de disponer de dos o más *appliances* instalados en la red de la organización.

30. A continuación, se detallan los pasos de instalación iniciales de un dispositivo, se trate de un *appliance* virtual o físico, configurado como *appliance*.

    - Si es la primera vez que se enciende el *appliance*, dará opción de instalarlo (si no se selecciona ninguna opción, pasados unos segundos se entrará la opción de instalación, que es la opción marcada por defecto).
    - Si está instalado ya, se iniciará automáticamente y se mostrará el *wizard* de inicio de configuración:

Ilustración 9. Instalación del *appliance* (I)

Ilustración 10. Instalación del *appliance* (II)

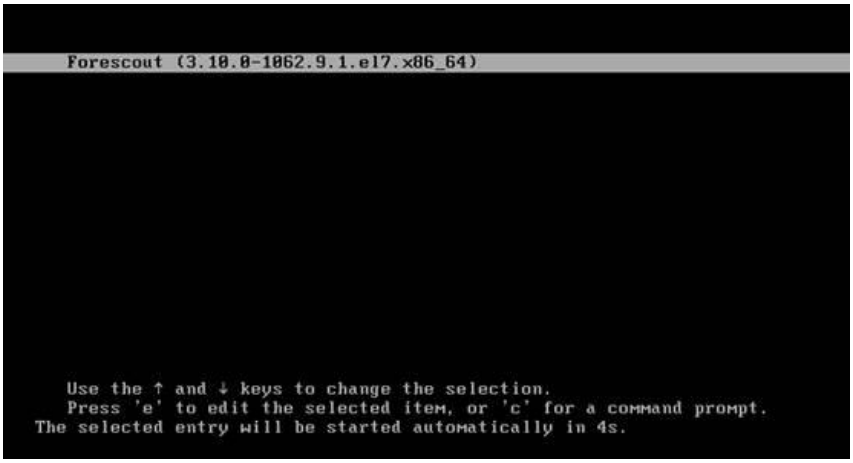

Ilustración 11. Instalación del *appliance* (III)

- A continuación, seleccionar la opción 1, "***Configure Forescout Device***" y después el modo "***Standard Installation***". Para una instalación de alta disponibilidad, consultar el apartado 5.11. Alta disponibilidad.
- El sistema preguntará si se ha seleccionado el modo de configuración deseado. Tras seleccionar *Yes*, se podrán seleccionar dos parámetros:
    - *Certification Compliance Mode*. **Se debe activar esta opción**. Para más información ver apartado 5.1 Modo de operación seguro.
    - *Disk encryption*. Seleccionar esta opción para cifrar el disco. Para más información ver apartado 5.1 Modo de operación seguro.

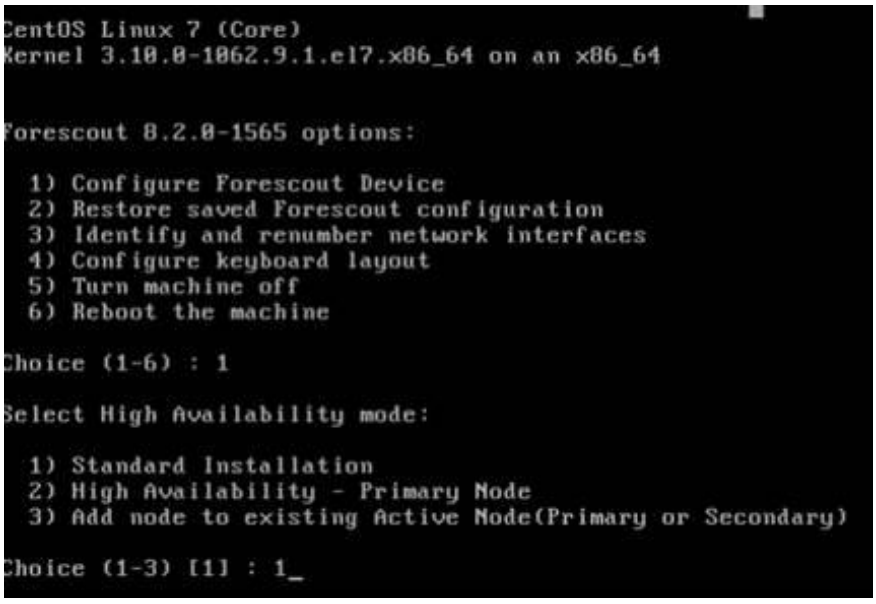

Ilustración 12. Instalación del appliance (IV)

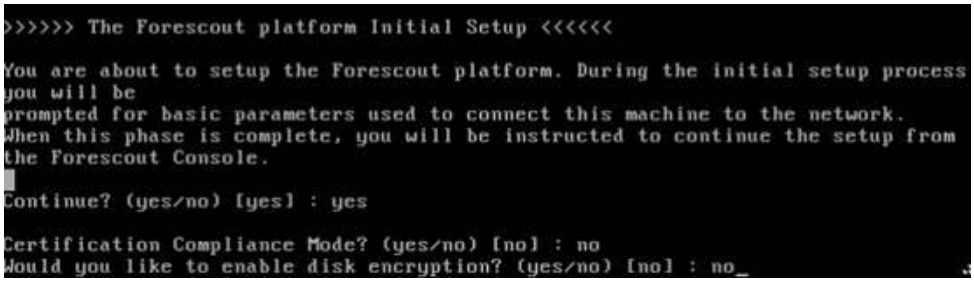

Ilustración 13. Instalación del appliance (V).

- A continuación, seleccionar la opción 1 "***Forescout Appliance***", el modo de licenciamiento correspondiente y una descripción del equipo. En caso de desear realizar la configuración como *Enterprise Manager*, seleccionar dicha opción. Los siguientes pasos son de aplicación para ambos modos.

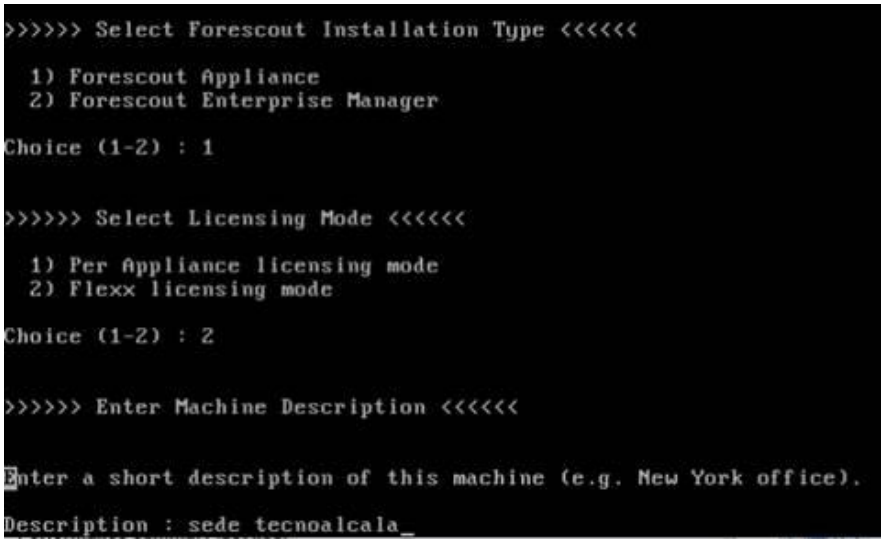

Ilustración 14. Instalación del appliance (VI).

- Se pedirá introducir una contraseña de administración. Esta se utilizará para el usuario de acceso por CLI (*cliadmin*) y para el usuario de acceso a la consola (*admin*). Seguir las recomendaciones indicadas en el apartado 5.3.3 POLÍTICA DE CONTRASEÑAS Y PARÁMETROS DE SESIÓN .Esta contraseña se podrá modificar posteriormente desde *Tools* > *Change Password*.

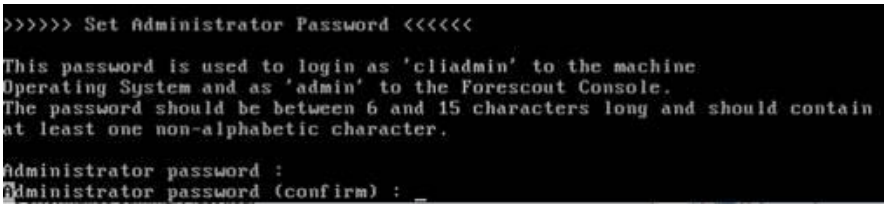

Ilustración 15. Instalación del appliance (VII)

- Añadir el *hostname* del *appliance*.

- Realizar la configuración de la comunicación IP: dirección de gestión, red, *gateway*, dominio y DNS (si no se usa IPv6, indicarlo como "*none*"); se puede hacer un test ("T"), reconfigurarlo ("R") o terminar ("D):

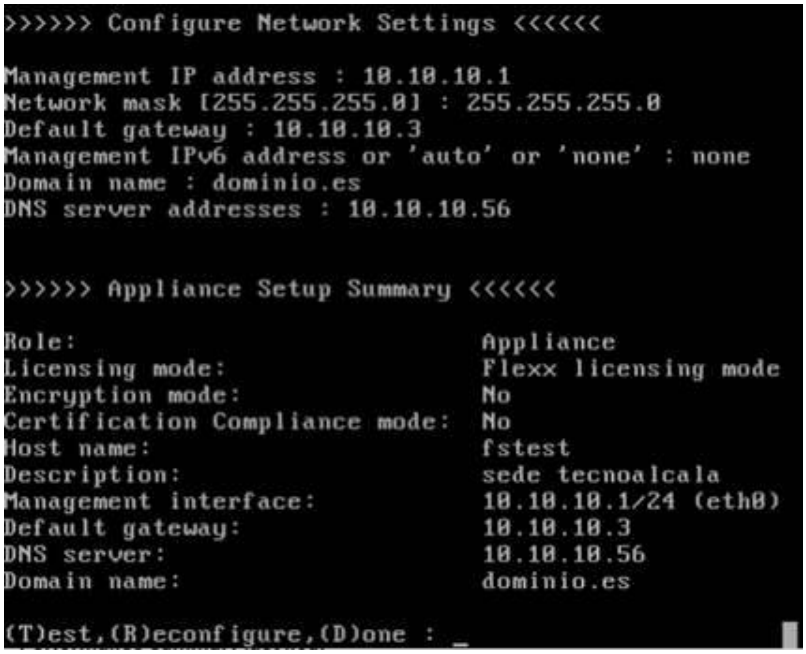

Ilustración 16. Instalación del appliance (VIII)

- El dispositivo tardará unos minutos en aplicar la configuración.
- Finalmente, se puede comprobar la conectividad de red haciendo un *ping* a la IP de gestión asignada al appliance desde la misma red.
- Tras la instalación inicial, se puede descargar la **consola de gestión** desde un navegador en el equipo deseado, que tenga conectividad con el appliance, a través de la URL: https://ipdelappliance/install.
- Esta consola se utilizará para realizar las configuraciones necesarias en el producto. El acceso se realizará con el usuario admin y la contraseña elegida durante la instalación.

31. El detalle del proceso de instalación se puede consultar en la guía *Forescout Installation Guide v8.2.2 – REF1.* En el apartado *Forescout Virtual Systems* se pueden consultar los pasos necesarios para llevar a cabo el despliegue de appliances virtuales, tras lo cual será necesario seguir los pasos indicados en el presente apartado.

4.6 *WIZARD* DE CONFIGURACIÓN INICIAL

32. Tras la instalación del producto, al acceder por primera vez, se lanzará de forma automática el *wizard* de configuración inicial. Se pedirán los datos básicos para el funcionamiento del producto. Entre ellos, se solicitará información sobre los servidores NTP, los servidores externos de autenticación, etc.

33. Se recomienda seguir todos los pasos indicados en el apartado 5. FASE DE CONFIGURACIÓN, para verificar que todas las configuraciones se realicen de forma segura.

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

34. Como se ha visto anteriormente, durante la fase de instalación es posible elegir opciones de operación en modo seguro.

35. Durante el menú de instalación **se debe seleccionar el modo *Certification Compliance Mode*.** El uso de este modo es irreversible. En caso de necesitar desactivarlo, es necesario realizar una reinstalación completa del *appliance*. En este modo **se activa también el modo *FIPS Compliance***. Tras seleccionar el modo *Certification Compliance,* se aplicarán las siguientes restricciones:

    - Se impedirá el uso del *Bash Shell*. Solo se podrá acceder a la CLI mediante FS-CLI, una interfaz de línea de comandos propiedad de Forescout.
    - Se forzará el uso de TLSv1.2. No se permitirá el uso de versiones inferiores.
    - SNMPv3 se establecerá por defecto. En caso de seleccionar otra versión, aparecerá un aviso.
    - NTP con autenticación se establecerá por defecto. En caso de seleccionar NTP sin autenticación (opción no recomendada), aparecerá un aviso.
    - El portal de activos y el portal de informes serán deshabilitados.
    - En los logs de auditoría se registrarán acciones adicionales.

36. Durante la instalación también es posible activar la *Disk encryption*. Esta sirve para cifrar las particiones del appliance. El algoritmo de cifrado usado es AES-128, haciendo uso de SHA-256 como algoritmo de *hash*. Las ubicaciones cifradas son las siguientes:

    - Dirección */fslog* para los logs de la plataforma (también */usr/local/forescout/log*).
    - Dirección */fsdatabase* el cual contiene la información de configuración de los host y endpoint (también */usr/local/forescout/db*).
    - Dirección */usr/local/forescout/etc* el cual contiene la configuración de la plataforma.

37. Por defecto, todas las credenciales utilizadas por el producto son almacenadas cifradas, utilizando el algoritmo AES-128.

5.1.1 PROTECCIÓN DEL *BOOT LOADER*

38. Se recomienda configurar una contraseña para proteger el *boot loader* frente a accesos no autorizados. Para ello seguir los siguientes pasos:

    - Acceder al CLI.
    - Introducir el comando: *fstool grub –setpassword*

- Se solicitará introducir la contraseña deseada y repetirla.
- A partir de este momento, se solicitará la contraseña configurada cuando se traten de editar los ajustes del *boot loader*.

5.1.2 PROTECCIÓN DE LA CONSOLA DE GESTIÓN

39. **Se debe proteger el acceso a la cosola de gestión**, limitando desde qué direcciones IP se puede acceder. Para ello:
    - Ir a *Options* > *Tools*.
    - Seleccionar *Access* > *Console*. Se mostrará desde qué IPs se puede acceder a la consola.
    - Por defecto tendrá el valor *All IP's*. Seleccionar *Add* e introducir el rango de IPs que desde las que desea permitirse el acceso.
    - Hacer clic en *OK*. Por último seleccionar *Apply*.

5.1.3 PROTECCIÓN DE LA CONSOLA CLI

40. **Se debe limitar desde qué direcciones IP se permite el acceso al CLI del producto**. Para ello, aplicar los siguiente comandos:
    - Acceder al equipo mediante CLI.
    - Ejecutar el comando *fstool ssh.* Aparecerá un mensaje mostrando las direcciones IP actuales con acceso mediante SSH.
    - Por ejemplo:

      SSH access list

      192.0.2.1
      192.0.2.2.
      (A)dd,(D)elete,(S)ave,(Q)uit :

    - Seleccionar *A* en línea de comando y presionar *Enter* para configurar nuevas direcciones IP.
    - Escribir las direcciones IP deseadas.
    - Presionar *S* para guardar cambios o *Q* para salir sin guardar los cambios.
    - Para borrar una dirección IP o un rango de direcciones, seleccionar *D* en línea de comando y presionar *Enter*. Escribir la dirección IP que desea eliminarse y pulsar Enter.
    - Presionar *S* para guardar los cambios o *Q* para salir sin guardar los cambios.

5.2 AUTENTICACIÓN

41. El producto permite la autenticación local de usuarios, creando y gestionando usuarios y credenciales localmente (ver apartado 5.3.2 Configuración de usuarios). Permite también la autenticación haciendo uso de servidores externos.

5.2.1 SERVIDORES EXTERNOS DE AUTENTICACIÓN

42. Para realizar la configuración de los servidores externos de autenticación, seguir los siguientes pasos:

    - Ir a *Tools > Options*.
    - Seleccionar *User Directory*.
    - Hacer clic en *Add*.
    - Introducir el nombre deseado para identificar el servidor de autenticación, así como el tipo (por ejemplo: *Active Directory, IBM Lotus Notes, OpenLDAP Server, RADIUS* o *TACACS*).
    - Seleccionar las casillas *Use as directory*, *Use for Authentication* y *Use for CounterACT Login*.
        - *Use as directory.* Indica el uso del servidor como directorio para obtener información de los usuarios.
        - *Use for Authentication.* Indica el uso del servidor para la autenticación de usuarios.
        - *Use for CounterACT Login*. Indica el uso del servidor para la autentiación de usuarios en la consola de Forescout.
    - Si se desea, incluir un comentario en la casilla *Comment*.
    - Hacer clic en *Next*.
    - Introducir los distintos parámetros requeridos según correspondan al tipo de servidor seleccionado. Se recomienda seleccionar la casilla *Use TLS* cuando esté presente.
    - En la pestaña *Advanced Settings*, se puede configurar adicionalmente parámetros de las comunicaciones TLS entre Forescout y los servidores de autenticación:
        - *Present CounterACT client certificate*. Si se activa esta opción, el producto presentará el certificado de cliente al servidor de autenticación. **Se debe activar esta opción.**
        - *Verify user directory server certificate*. Si se activa esta opción, el producto verificará el certificado del servidor. **Se debe activar esta opción.**

- *Check user directory certificate revocation status using*. Permite seleccionar la forma de verificar que el certificado de servidor no esté revocado. Se puede seleccionar CRL o OSCP como método.

- Por último hacer clic en *Finish.*

43. El detalle de configuración de los distintos tipos de servidores de autenticación externa se puede consultar en el siguiente enlace.

5.2.2 USO DE *SMART CARDS*

44. El producto permite a su vez la autenticación mediante *Smart Card*. Para ello es necesario configurar previamente los certificados de la CA y las listas de revocación de certificados (CRL) necesarios para la autenticación (ver apartado 5.6 Gestión de certificados). Para configurar la autenticación mediante *Smart Card*, seguir los siguientes pasos:

    - Ir a *Tools > Options* y seleccionar *CounterACT User Profiles > Smart Card*.
    - Selccionar *Import*. Se abrirá el wizard de Autoridades de Certificación.
    - Seleccionar *Import CA*, seleccionar el fichero deseado y subirlo.
    - Hacer clic en *Next*, seleccionar *Add* y definir la CRL requerida.
    - Finalmente hacer clic en *Finish*.

45. Para que funcione correctamente el acceso mediante *Smart Card* para un usuario ya creado (ver apartado 5.3.2 Configuración de usuarios), se debe verificar que el *Common Name* (CN) de la *Smart Card* y el nombre de usuario definido en el producto son iguales. También debe configurarse el tipo de usuario como *Single – Smart card* (ver apartado 5.3.2 Configuración de usuarios).

46. Siempre que sea posible, se recomienda la **utilización de doble factor de autenticación (2MFA).**

5.2.3 CONFIGURACIÓN DE SSO

47. El producto permite el uso de *Single Sign On (SSO)* mediante la configuración de un proveedor de identidad (IDP). Se encuentran disponibles OKTA o Ping Identity, así como aquellos compatibles con SAML 2.0.

48. Para configurar un IDP, seguir los siguientes pasos:

    - Ir a *Tools > Options* y seleccionar *CounterACT User Profiles*.
    - Seleccionar *External Identity Provider*. Se abrirá una ventana nueva.
    - Seleccionar *Enable External Identity Provider*. Hacer clic en *Apply.* Esto iniciará el servicio SSO del producto.
    - Repetir los pasos anteriores y verificar que la casilla *Enable External Identity Provider* está marcada en esta ocasión.

- Desde el menú *External Identity Provide*, seleccionar el proveedor deseado. Completar los datos requeridos.
- Por último hacer clic en *Apply*. Se reiniciará el servidor. A partir de este momento, el botón *Log in with SSO*, se encontrará disponible en la pantalla de inicio de sesión.

5.2.4 AUTENTICACIÓN ENTRE COMPONENTES

49. El producto realiza la autenticación de sus componentes cuando existen comunicaciones internas haciendo uso de los siguientes protocolos:
    - Las comunicaciones entre los appliances se realizan haciendo uso de TLS. El producto permite el uso de TLSv1.1 y TLSv1.2. **Se debe usar solo de TLSv1.2**. Para ello, mediante línea de comandos, ejecutar el siguiente comando: ***fstool set_property fs.supported.tls.protocols= TLSv1.2***
    - Las sesiones entre el agente *SecureConnector* (ver apartado 5.14.3 AGENTE *SECURECONNECT*) y los nodos/*appliances* de Forescout, utilizan también TLSv1.1 y TLSv1.2. De igual manera, **se debe utilizar solo TLSv1.2**. Para ello, ejecutar: ***fstool set_property fs.supported.tls.protocols= TLSv1.2***

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

50. La administración del producto se puede llevar a cabo utilizando cualquiera de los siguientes tres (3) métodos:
    - Conexión física local al dispositivo.
    - Acceso mediante CLI: utilizando el protocolo SSH con/sin clave pública. Para su configuración ver el apartado 5.5.2 Configuración de SSH.
    - Acceso mediante GUI: se debe descargar y utilizar la consola de gestión, tal como se ha visto durante la instalación. Ver apartado 4.5 Instalación. Se utiliza HTTPS sobre el protocolo TLSv1.2 para el acceso mediante la consola de gestión.

5.3.2 CONFIGURACIÓN DE USUARIOS

51. Forescout permite la creación de perfiles de usuarios locales personalizados, gestionando también los distintos permisos que estos usuarios tienen individualmente. El producto no dispone de roles de usuario, si no que los permisos se asignan individualmente a cada usuario o grupo.
52. Se pueden utilizar los Grupos de Usuarios para simplificar la creación de usuarios. Forescout permite la definición de grupos basados en RADIUS o en directorios de usuario. Todos los usuarios asociados a un grupo tendrán los mismos permisos.

53. Para la creación de grupos de usuarios se pueden seguir dos (2) métodos:
    - Asociar los grupos de usuarios con un atributo y valor concreto de RADIUS.
    - Asociar los grupos de usuarios con la pertenencia a un grupo del directorio de usuarios específico.
54. De esta forma, se pueden gestionar los permisos para un grupo de usuarios perteneciente a un servidor externo. Sin embargo, para los usuarios locales no se pueden definir grupos, siendo necesario configurar sus permisos individualmente.
55. Seguir los siguientes pasos para crear grupos de usuarios:
    - Ir a *Tools > Options > CounterACT User Profiles.*
    - Seleccionar *Add*. Se abrirá una nueva ventana.
    - En *User Type*, seleccionar:
        - *Group – External User Directory* o *Group – SSO with User Directory*, según se desee, para asociar el grupo a la pertenencia a un directorio concreto. Tras seleccionar una de estas dos opciones, seleccionar el nombre del servidor.
        - *Group – External RADIUS*, para asociar el grupo a un atributo y valor concreto. Tras seleccionar la opción, introducir el atributo y valor concreto que definirán la pertenencia al grupo.
    - Hacer clic en *Next* y seleccionar los permisos (de escritura y lectura) que tendrá dicho grupo.
    - Hacer clic en *Next*. Seleccionar los segmentos de red sobre los que tendrá visibilidad el grupo.
    - Por último hacer clic en *Finish*.
56. El detalle sobre la configuración de Grupos de usuarios se puede consultar en el apartado *Creating Users and User Groups*, de la guía *Forescout Administration Guide v8.2.2 – REF2*.
57. Para acceder a la configuración de usuarios seguir los siguientes pasos. Se configurarán tanto las credenciales de los usuarios, como sus permisos:
    - Ir a *Tools > Options > CounterACT User Profiles.*
    - Seleccionar *Add*. Se abrirá una nueva ventana.
    - En *User Type*, seleccionar:
        - *Single – Password*. Usuarios locales que se autentican mediante usuario/contraseña.
        - *Single – SSO (web Only)*. Usuarios que se autentican mediante SSO.
        - *Single – External User Directory*. Usuarios que se autentican mediante un servidor externo configurado previamente (ver apartado 5.2.1 Servidores externos de autenticación).

- *Single – Smart Card*. Usuarios que se autentican mediante Smart Card, configurado previamente (ver apartado 5.2.2 Uso de Smart Cards).

- Introducir el nombre de usuario y contraseña. En el siguiente apartado, se muestra cómo requerir que los usuarios modifiquen la contraseña tras el primer acceso. **Esta opción debe ser activada**.
- Hacer clic en *Next* y seleccionar los permisos (de escritura y lectura) que tendrá dicho usuario.
- Hacer clic en *Next*. Seleccionar los segmentos de red sobre los que tendrá visibilidad el usuario.
- Por último hacer clic en *Finish*.

58. Tras la creación de los usuarios, estos pueden cambiar sus contraseñas manualmente cuando accedan desde *Tools > Change Password*.
59. Se recuerda que la gestión de usuarios debe realizarse de acuerdo al **principio de mínimo privilegio**.

5.3.3 POLÍTICA DE CONTRASEÑAS Y PARÁMETROS DE SESIÓN

60. **Se debe crear una política de contraseñas** que establezca unos parámetros mínimos de complejidad. Esta política será de aplicación para los usuarios locales. En el caso de los usuarios de servidores de directorio, se seguirán los requisitos impuestos en dicho servidor, por lo que se recomienda configurar unas restricciones similares a las indicadas en el presente apartado. Para ello, seguir los siguientes pasos:
    - Ir a *Tools > Options > CounterACT User Profiles > Passwords and Sessions*.
    - Seleccionar la pestaña *Password*.
    - Definir, según se desee, los siguientes requisitos:
        - *Minimum lenght*. Define el número mínimo de caracteres que deben tener las contraseñas. **Se debe configurar un valor de, al menos, doce (12) caracteres.**
        - *Password must contain at least {x} upper-case alphabetic characters*. Define el número mínimo de letras en mayúscula que deben tener las contraseñas. **Se recomienda un valor de al menos uno (1).**
        - *Password must contain at least {x} lower-case alphabetic characters*. Define el número mínimo de letras en minúscula que deben tener las contraseñas. **Se recomienda un valor de al menos uno (1).**

- *Password must contain at least {x} digits*. Define el número mínimo de dígitos que deben tener las contraseñas. **Se recomienda un valor de al menos uno (1).**
- *Password must contain at least {x} special characters*. Define el número caracteres especiales en minúscula que deben tener las contraseñas. **Se recomienda un valor de al menos uno (1).**
- *Password must not contain {x} repeated characters or digits*. Define el número máximo de caracteres repetidos que puede tener una contraseña.
- *Password must differ from previous password by at least {x} characters*. Define el número mínimo de caracteres en los que deben diferir las nuevas contraseñas configuradas respecto a las anteriores.
- *Password must not contain user name*. Define si la contraseña puede o no contener el nombre de usuario. Se recomienda activar esta opción (*Enabled*) para impedir que las contraseñas puedan estar formadas por nombres de usuario. **Se recomienda activar esta opción.**
- *Password must not contain commonly used weak passwords*. En caso de estar activada (*Enabled*), las contraseñas no podrán estar formadas por ciertas combinaciones usualmente utilizadas. **Se debe activar esta opción.** Por ejemplo, *abcd1234*, no sería permitido.
- *Last {x} passwords cannot be reused*. Define el número de contraseñas pasadas que recuerda el dispositivo, forzando a que las nuevas contraseñas sean distintas a las previas. **Se recomienda un valor de, al menos, cuatro (4).**
- *Password expires after {x} {days/weeks}*. Define el número de días tras los cuales expirará la contraseña y se exigirá un cambio. **Se recomienda un valor entre sesenta (60) y noventa (90) días.**
- *Lock user account after {x} failed logins for {x} {minutes/hours}*. Define el número máximo de intentos de inicio de session fallidos antes de bloquear al usuario y el tiempo que estará bloqueado en minutos y horas. **Se recomienda configurar un valor de tres (3) intentos fallidos y, al menos, quince (15) minutos.**
- *Limit password change to once every {x} {hours/days}*. Define el tiempo mínimo que debe pasar desde un cambio de contraseña, antes de poder modificarla de nuevo.
- *User must change password at next login if changed by admin user*. En caso de ser activada (*Enabled*), exige el cambio de

contraseña a un usuario al iniciar sesion si un administrador la cambió previamente. Exige también el cambio de contraseña en el primer acceso tras la creación de dicho usuario. **Se debe activar esta opción.**

- Por último hacer clic en *Apply*.

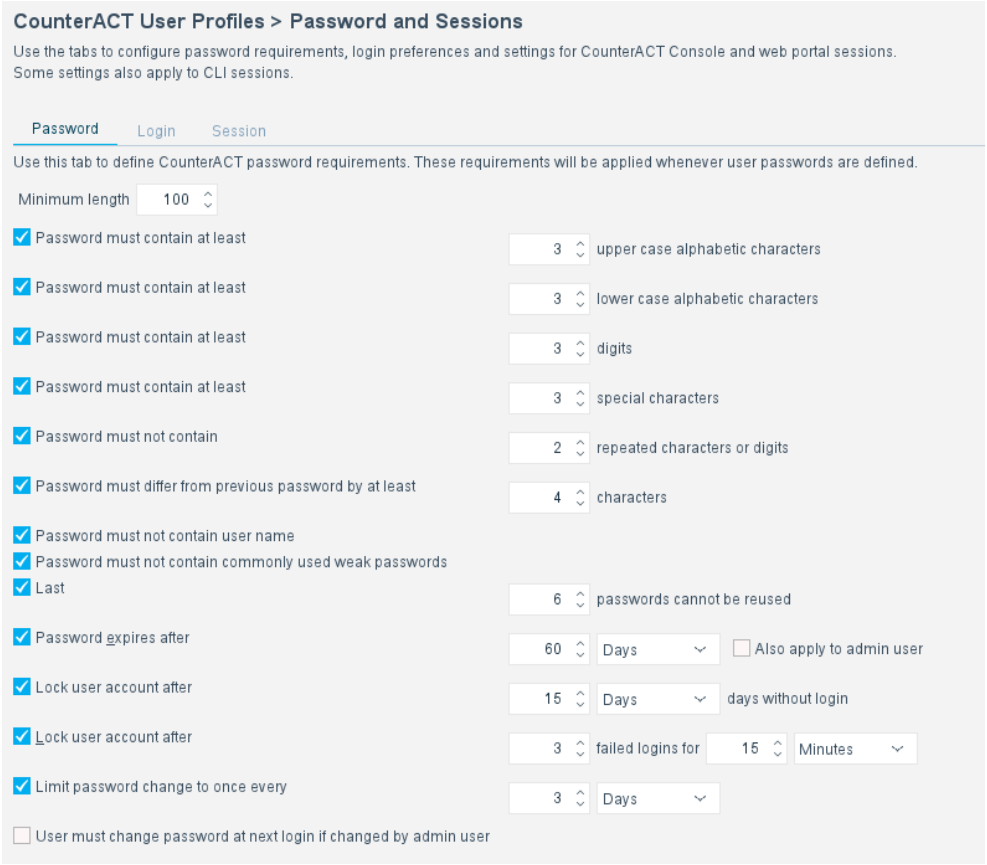

Ilustración 17. Configuración de la política de contraseñas, pestaña Password

61. El producto permite configurar también distintos parámetros para proteger las sesiones de usuarios. Se describen a continuación:

    - Ir a *Tools > Options > CounterACT User Profiles > Passwords and Sessions*.
    - Seleccionar la pestaña *Session*.
    - La opción *Allow only one sesión per user*, permite limitar el número de sesiones concurrentes de un usuario. Se recomienda activar esta opción, marcando la casilla, para evitar que un usuario pueda abrir dos sesiones de forma simultánea.
        - *Terminate existing sesión upon new login*. En caso de tratar de iniciar una sesión, cuando existe otra abierta, se finalizará la sesión existente, iniciando una nueva.
        - *Reject additional login attemts*. En caso de tratar de iniciar una sesión, cuando existe otra abierta, se denegará el acceso.

- La opción *Terminate each session after*, define el tiempo en minutos u horas tras el cual finalizará una sesión. Se recomienda configurar este parámetro, por ejemplo, en una (1) hora.
- La opción *Terminate inactive sessions after*, define el tiempo en minutos u horas tras el cual finalizará una sesión inactiva de usuario. Se recomienda configurar este parámetro, por ejemplo, en diez (10) minutos.
- La opción *Attempt to automatically restore dropped options*, permite al producto tratar de restaurar sesiones. Se recomienda deshabilitar esta opción.
- Por último hacer clic en *Apply*.

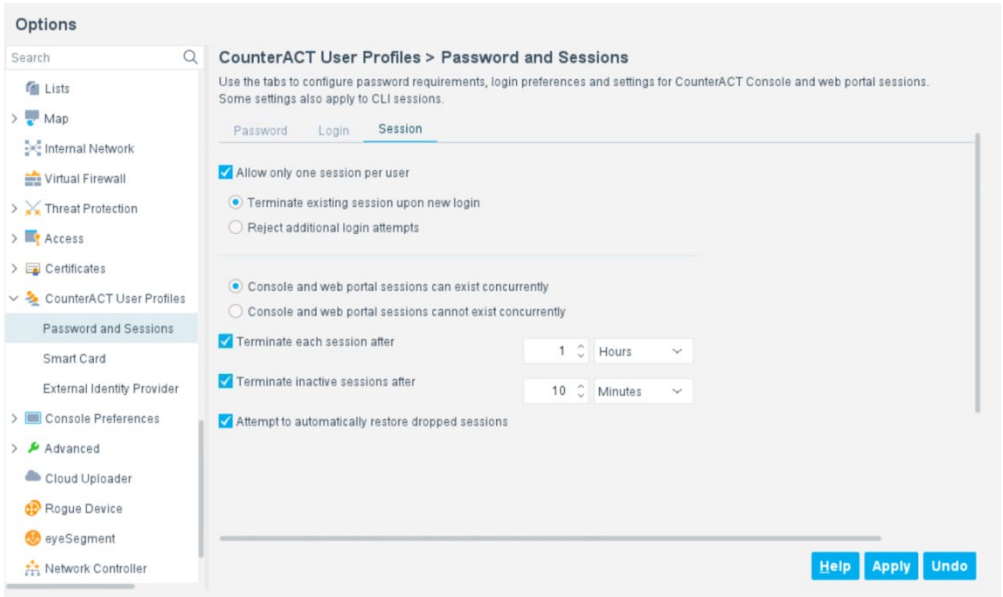

Ilustración 18. Configuración de la política de contraseñas, pestaña *session*

62. **Se debe configurar un banner de acceso**. Para configurarlo, ir a *Tools > Options > CounterACT User Profiles > Passwords and Sessions*. Ir a la pestaña *Login* y activar las casillas *Before login, prompt user to accept these Terms and Conditions* y *After login, prompt user to accept these Terms and Conditions*, según se desee mostrar el mensaje antes o después de realizar el inicio de sesión. En el cuadro de texto bajo la casilla, introducir el mensaje que se desea mostrar.
63. **Se debe activar** también la casilla *After login, show the login summary dialog*. De esta forma, tras iniciar sesión, se mostrará **un diálogo con los inicios de sesión recientes del usuario.**
64. El detalle de configuración de la pestaña *Login*, se puede consultar en el siguiente enlace.

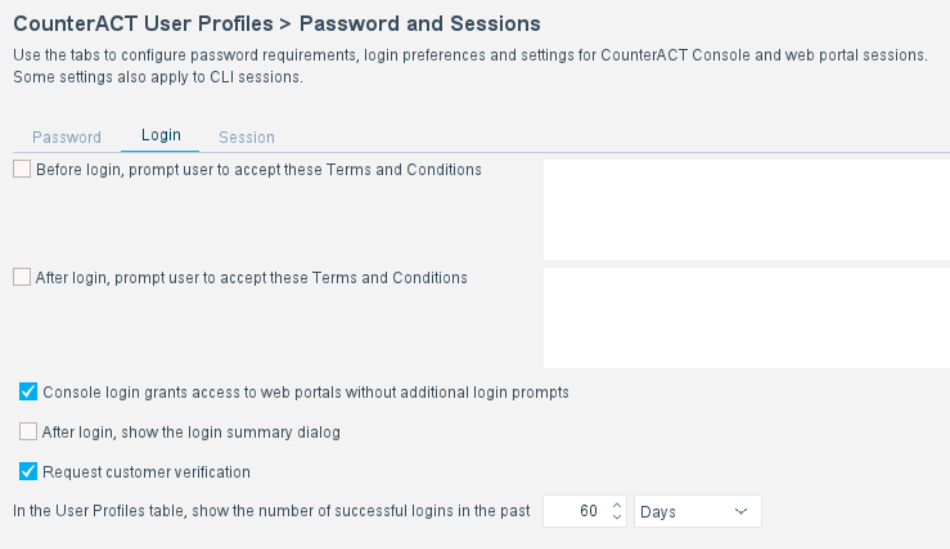

Ilustración 19. Configuración de la política de contraseñas, pestaña *login*

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

65. A continuación y de forma gráfica se muestran las interfaces del equipo de forescout:

Muestra del panel trasero — Dispositivo CounterACT

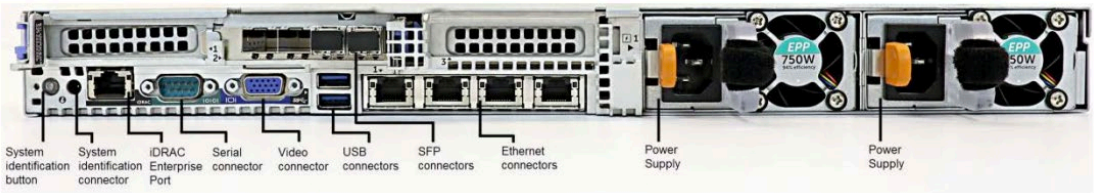

Ilustración 20. Interfaces físicas del producto

66. **Todos aquellos puertos que no se utilicen deben ser deshabilitados**.

5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

67. El producto hace uso de los protocolos HTTPS y SSH para la gestión e interconectividad con aplicaciones y controles externos. Tal como se ha visto en el apartado 5.1 MODO DE OPERACIÓN SEGURO, al activar dicho modo se exige el uso de TLSv1.2.

68. Por defecto, la comunicación interna de *appliance* con *appliance* utiliza SSHv2 vía puerto TCP 22 y TLSv1.2 vía puerto TCP 13000. Estos protocolos son los únicos permitidos por el producto en caso de activar el modo seguro (ver apartado 5.1 MODO DE OPERACIÓN SEGURO).

5.5.1 CONFIGURACIÓN DE TLS

69. Se utiliza HTTPS sobre TLS para la gestión de los módulos de *dashboard* y *reporting*, accesibles mediante GUI desde *Dashboard*. Por defecto utiliza el puerto TCP 443. Se utiliza TLSv1.2 (en caso de estar activado el modo seguro, ver 5.1 MODO DE OPERACIÓN SEGURO) en las comunicaciones entre el producto y la consola de gestión.
70. Por defecto, los certificados generados por Forescout son utilizados en la configuración inicial HTTPS. **Se debe instalar un nuevo certificado interno en Forescout**, ver apartado 5.6 Gestión de certificados.
71. La integración con directorios de usuarios (ver apartado 5.2.1 SERVIDORES EXTERNOS DE AUTENTICACIÓN), que usan TLS, utilizará el método que LDAP presente. **Por lo tanto, se debe configurar el servidor LDAP para hacer uso solo de TLSv1.2.**
72. Para las comunicaciones entre los distintos componentes del producto, se deben seguir las indicaciones del apartado 5.2.4 Autenticación entre componentes, para permitir sólo el uso de TLS1.2.
73. Para *SecureConnector* (el agente de Forescout, ver apartado 5.14.1 Agente SecureConnect) se puede configurar la versión de TLS a utilizar en el menú desplegable. **Se debe seleccionar TLSv1.2** como el método más seguro. Para ello:
    - Ir a *Options > HPS Inspection Engine.*
    - Navegar hasta la pestaña *SecureConnector*.
    - En la casilla *Minimum supported TLS version*, seleccionar la opción *TLS version 1.2*.

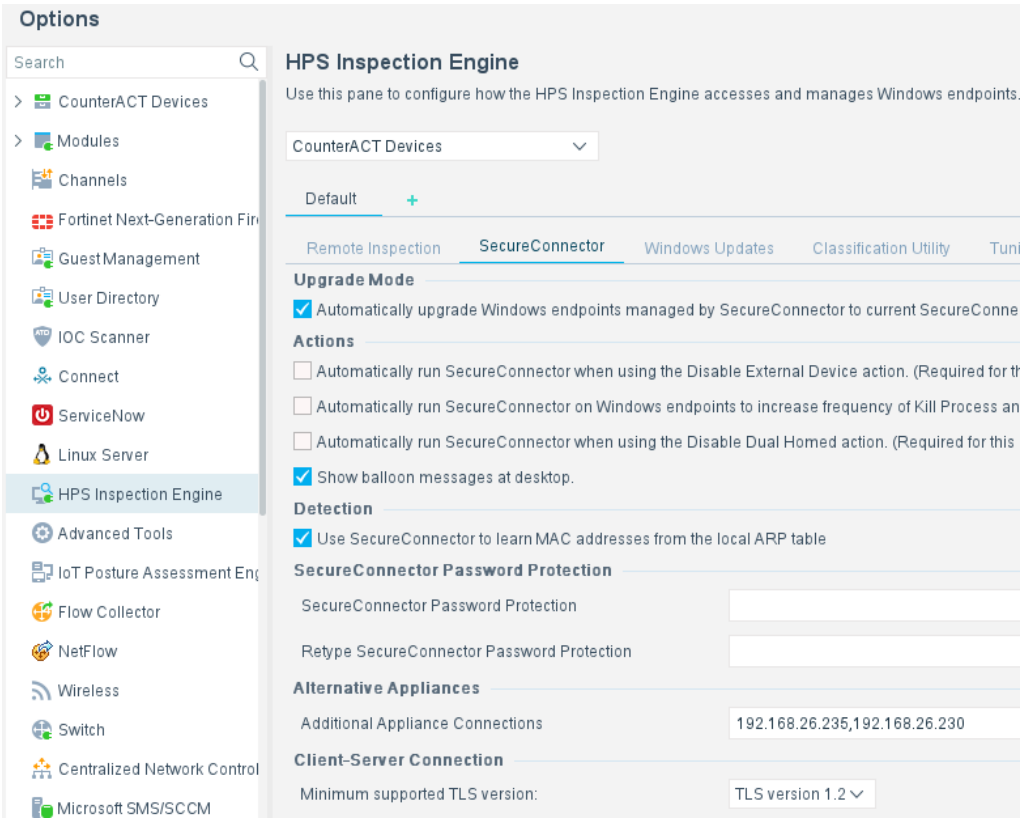

Ilustración 21. Configuración TLS en el SecureConnect

5.5.2 CONFIGURACIÓN DE SSH

74. SSH se utiliza en el acceso por línea de comandos a los *appliances* de Forescout.

75. El producto utiliza FS-CLI. Se trata de una interfaz de comandos propiedad de ForeScout. Viene activada y configurada por defecto y permite ejecutar comandos especiales a través de la CLI, sin permitir el acceso al sistema operativo. Los comandos especiales (del tipo *fstool*) disponibles se pueden consultar en el siguiente enlace.

76. Se puede desactivar el acceso mediante contraseña para SSH, permitiendo solo el acceso mediante claves. Para ello:

    - Acceder al CLI y ejecutar el comando *user ssh-passwd disable*.
    - Generar un nuevo par de claves RSA con el comando *ssh-keygen –b lenght*, sustituyendo *length,* por el valor deseado. **Se deben utilizar claves de 3072 bits o superiores.**
    - Utilizar el comando *user auth setkey username* (sustituyendo *username* por el usuario para el cual se desea generar dichas claves) e introducir la clave creada.

77. El protocolo *Elliptic Curve 25519* es el método primario de uso de claves de los *appliances* de Forescout. Los métodos de cifrado utilizados son los siguientes:

- AES128-CTR
- AES192-CTR

5.6 GESTIÓN DE CERTIFICADOS

78. La configuración completa de los distintos certificados utilizados y necesarios para el empleo del producto se pueden consultar en el siguiente enlace.

79. Desde la página principal de gestión de certificados (*Options* > *Certificates*) se pueden configurar los siguientes parámetros:

    - *Email Notice for Certificate Expiration*. Permite configurar a qué usuario o dirección de correo se enviarán los avisos de expiración de los certificados, cuándo se empezarán a enviar dichos avisos y con qué frecuencia.
    - *Auto-download CRLs of trusted and system certificates.* Esta casilla permite activar la descarga automática de las listas de revocación de certificados (CRL), así como la periodicidad con la que se realizarán estas descargas.
    - *Ongoing TLS sessions.* Si se activa esta casilla, se verificarán los certificados utilizados en las conexiones TLS abiertas, con una periodicidad determinada, elegida por el administrador.

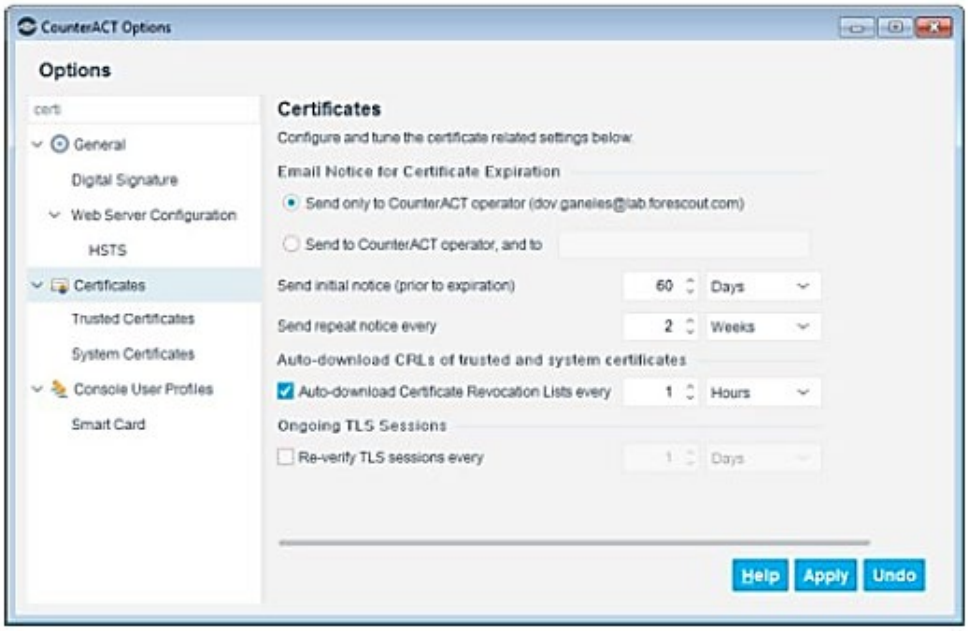

Ilustración 22. Configuración de certificados

5.6.1 CREACIÓN DE CSR

80. Para realizar la configuración de los certificados utilizados por el producto en las comunicaciones seguras con los distintos componentes y entidades autorizadas, se pueden crear peticiones de firma de certificados (CSR) a autoridades de

certificación o importar los certificados directamente. A continuación, se mostrarán los pasos a seguir para generar una CSR:

- Ir a *Options > Certificates > System Certificates*.
- Crear la petición con los datos deseados. **Se debe utilizar una longitud de clave de 3072 bits o superior.**
- Seleccionar los usos del certificado (*Key Usage*), así como la validez (*Validity*).

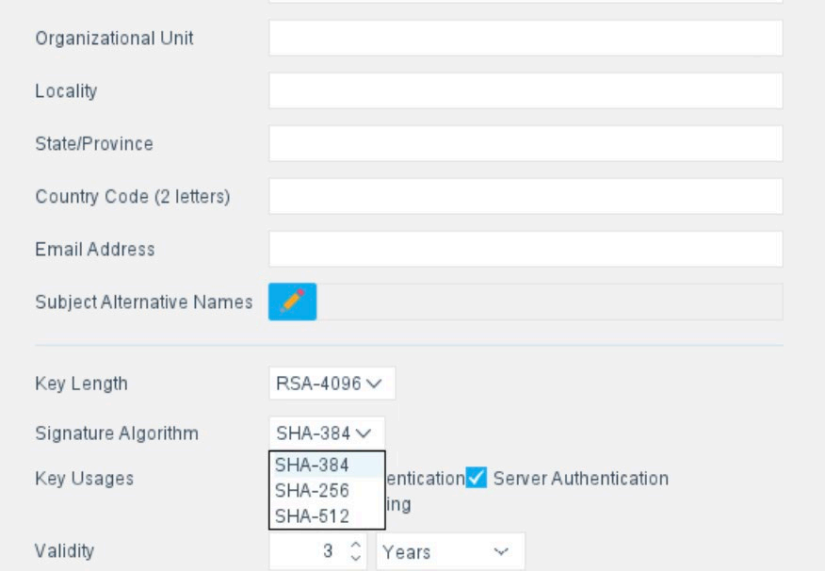

Ilustración 23. Selección del algoritmo de firma

Ilustración 24. Selección de la longitud de clave

- Hacer clic en *Next* y copiar el texto de CSR para enviarlo a la CA correspondiente.
- A continuación, seleccionar *Import certificates later*. Una vez creado el certificado por la CA, seleccionar el certificado en el producto, hacer clic en *Edit* e importar el fichero obtenido.
- Configurar la cadena de confianza del certificado, hacer clic en *Next*.
- Configurar el alcance (*Scope*) del certificado, en el campo *Used for Subsystem*, seleccionando los subsistemas del producto que presentarán dicho certificado al comunicarse con otros componentes. Seleccionar *All* si desea utilizarse en todos los casos.
- Repetir el paso anterior, en esta ocasión con los dispositivos en los cuales se utilizará el certificado (*Used for devices*).
- Finalmente hacer clic en *Next*, introducir el nombre identificativo deseado para el certificado y hacer clic en *Finish*.
- Para aplicar los cambios seleccionar *Apply*.

5.6.2 IMPORTAR CERTIFICADOS DEL SISTEMA

81. **Se deben importar y utilizar solo certificados cuya clave sea de 3072 bits o superior**. Para importar certificados, se deben seguir los siguientes pasos:
    - Ir a *Options > Certificates > System Certificates.* Se abrirá una nueva ventana.
    - Seleccionar *Add from PKCS#12*, para importar un certificado.
    - Buscar el certificado correspondiente para importar y hacer clic en *Apply*.
    - Hacer clic en *Next*, introducir la contraseña de la clave privada del certificado y hacer clic en *OK*.
    - Revisar la información del certificado y hacer clic en *Next*. Configurar la cadena de confianza y seleccionar *Next*.
    - Configurar el alcance (*Scope*) del certificado, en el campo *Used for Subsystem*, seleccionando los subsistemas del producto que presentarán dicho certificado al comunicarse con otros componentes. Seleccionar *All* si desea utilizarse en todos los casos.
    - Repetir el paso anterior, en esta ocasión con los dispositivos deseados (*Used for devices*).
    - Finalmente hacer clic en *Next*, introducir el nombre identificativo deseado para el certificado y hacer clic en *Finish*.
    - Para aplicar los cambios seleccionar *Apply*.

5.6.3 CERTIFICADOS DE AUTORIDADES DE CERTIFICACIÓN

82. Para el correcto funcionamiento del producto, se deben importar los certificados de las CA correspondientes al certificado utilizado para las comunicaciones HTTPS, así como las CA de los certificados empleados en las comunicaciones con componentes de confianza (por ejemplo, servidores de auditoría externos o servidores de autenticación externos).

83. Para importar un certificado raíz (*Root certificate*) de una autoridad de certificación (CA) seguir los siguientes pasos:

    - Ir a *Options* > *Certificates* > *Trusted Certificates*.
    - Hacer clic en *Add.* Se abrirá una nueva ventana.

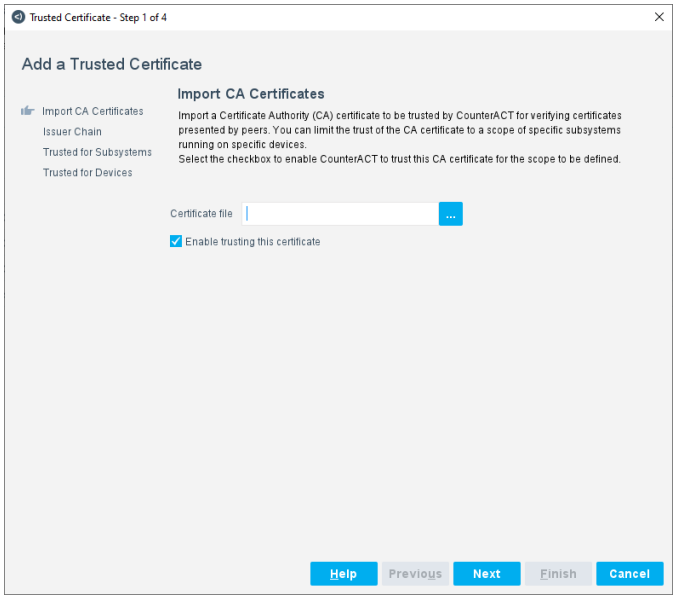

Ilustración 25. Importar certificado de CA (I)

- Seleccionar el certificado deseado y hacer clic en *Next*. Verificar la información del certificado importado (utilizando el botón *Details* se puede consultar la información detallada), si todo es correcto, hacer clic en *Next.*

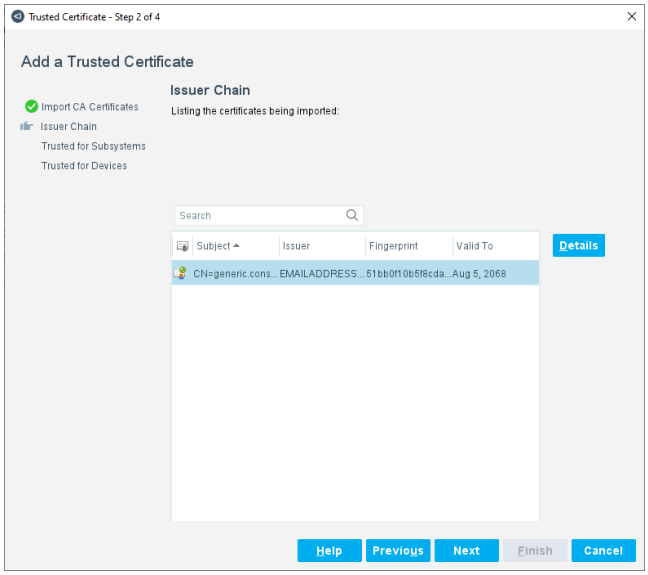

Ilustración 26. Importar certificado de CA (II)

- Una vez verificado, seleccionar para qué subsistemas será de confianza el certificado o seleccionar todos los sistemas

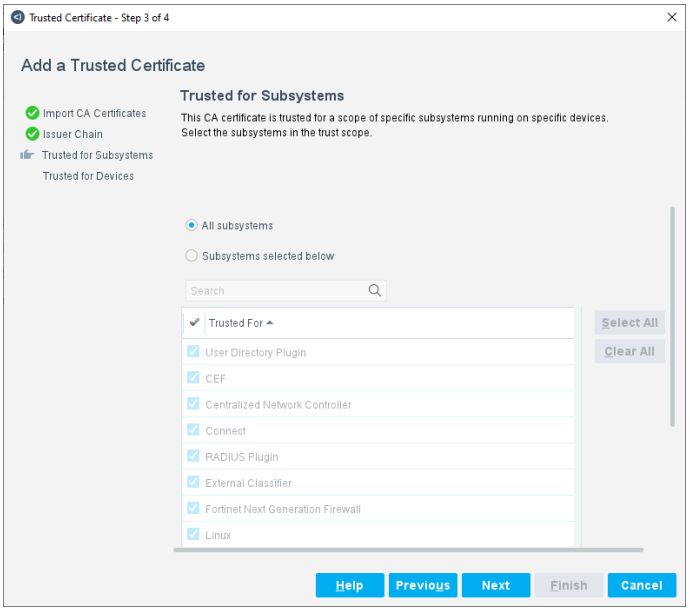

Ilustración 27. Importar certificado de CA (III)

- Hacer clic en *Next* y seleccionar los appliances de Forescout que confiarán en el certificado, o todos y hacer clic en *Finish*.
- Por último, hacer clic en *apply*, verificar la información incluída y seleccionar *OK*.

5.7 SINCRONIZACIÓN HORARIA

84. El producto permite la configuración de servidores NTP para la sincronización de los relojes. Para ello, por defecto, se realiza una conexión mediante el puerto UDP 123.

85. Para llevar a cabo la configuración de servidores NTP, seguir los siguientes pasos:

    - Ir a *Options* > *General* > *Time*.
    - Seleccionar la casilla *Enable sync with NTP server*. De esta forma se activa la sincronización con un servidor NTP.
    - En el cuadro *NTP Server*, introducir la dirección IP, o el nombre de dominio completo (FQDN), del servidor NTP deseado.
    - En el cuadro *Key*, introducir la clave de autenticación. **Se debe hacer uso de claves de autenticación.**
    - Hacer clic en *Apply* para guardar la configuración. Se puede utilizar el botón *Test* para verificar la correcta conexión con el servidor NTP.

86. El detalle sobre la configuración de servidores NTP se puede consultar en el apartado *Configure System Clock Synchronization with NTP Servers* de la guía *Forescout Administration Guide – REF2.*

5.8 AUTOCHEQUEOS

87. El producto permite configurar una serie de autochequeos, que se ejecutarán durante el arranque del dispositivo, impidiendo el uso en caso de errores.

88. **Se debe configuración la ejecución de dichos chequeos.** Para que se lleven a cabo estos chequeos, es necesario seguir los siguientes pasos:

    - Acceder vía CLI.
    - Ejecutar el siguiente comando: *get_property fs.selftest.enable*
    - Si devuelve por pantalla *"fs.selftest.enable="*, ejecutar el siguiente comando: *set_property fs.selftest.enable true.*

89. A partir de este momento, cuando se arranque el dispositivo se ejecutarán distintos chequeos a la integridad del *software* y los módulos criptográficos. En caso de error en alguna de las comprobaciones, el dispositivo no arrancará.

5.9 ACTUALIZACIONES

90. Las actualizaciones se realizan desde la máquina que corre la consola de gestión de la herramienta. Este dispositivo tiene que tener acceso a internet donde residen los servidores de actualización de Forescout.

91. Si existe un proxy, este debe configurarse en la máquina donde corre la consola. Si el proxy está haciendo filtrado de URLs, se debe dejar pasar las conexiones hacia *updates.forescout.com*.

92. El producto, por defecto, verifica automáticamente si existen actualizaciones disponibles. En caso afirmativo, aparecerá un icono en la barra de estado (icono *Check for updates*) de la consola indicando que existen nuevas actualizaciones. Se puede configurar la periodicidad de estas comprobaciones:

    - Ir a *Options > General > Check for Updates*.
    - Verificar que la casilla *Enable Check for Updates* se encuentra marcada. En caso de no estar marcada, no se verificará de forma automática la existencia de actualizaciones.
    - En el cuadro *Check for Updates every*, seleccionar la periodicidad deseada.
    - Por último hacer clic en *Apply*.

93. También puede verificarse de forma manual la existencia de nuevas actualizaciones o parches, desde *Tools > Check for Updates*:

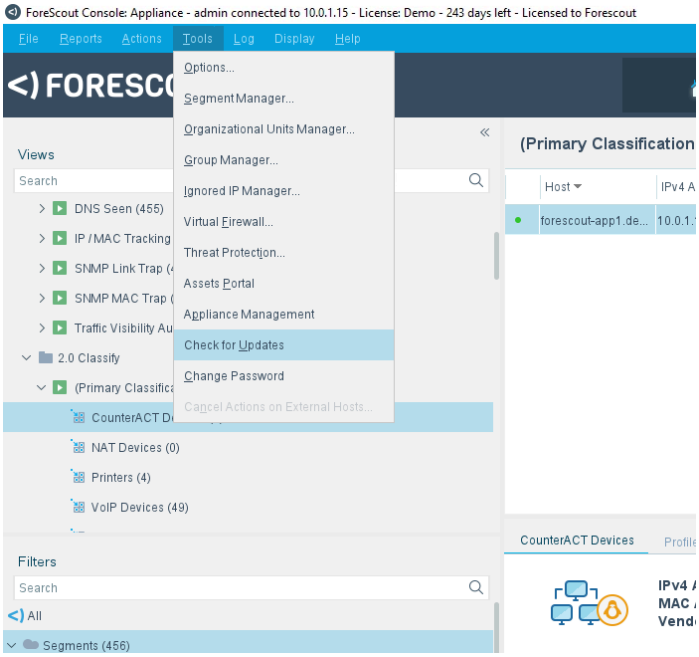

Ilustración 28. Verificación manual de actualizaciones

94. Una vez que se detecten actualizaciones disponibles, el proceso de actualización debe iniciarlo manualmente uno de los administradores de la herramienta, nunca es iniciado de manera automática por el sistema.

95. Para llevar a cabo la actualización del producto, seguir los siguientes pasos:

    - Cuando aparezca el icono *Check for updates*, hacer doble clic. Se abrirá el dialogo de actualización de software. Este mostrará la versión actual y la nueva de software, enlaces a las *Release Notes* y otra información relativa a la actualización.

- Seleccionar las versiones o parches que desean instalarse y hacer clic sobre *Install*. Se abrirá una nueva ventana.
- Seleccionar *I agree to the License Agreement* y hacer clic sobre *Install*.

96. El detalle sobre la configuración de las actualizaciones del sistema se puede consultar en el apartado *Check for Updates*, de la guía *Forescout Administration Guide – REF2.*
97. Se recuerda que el **producto debe estar actualizado** para minimizar la posibilidad de que presente vulnerabilidades de seguridad.

5.10 SNMP

98. El equipo de Forescout utiliza SNMP en todas sus versiones para comunicarse con los diferentes componentes activos de la red. También dispone de un servidor SNMP para que sistemas de monitorización pregunten por su estado.
99. La configuración de SNMP se lleva a cabo mediante los siguientes pasos:
    - Ir a *Tools > Options > General > SNMP Settings*.

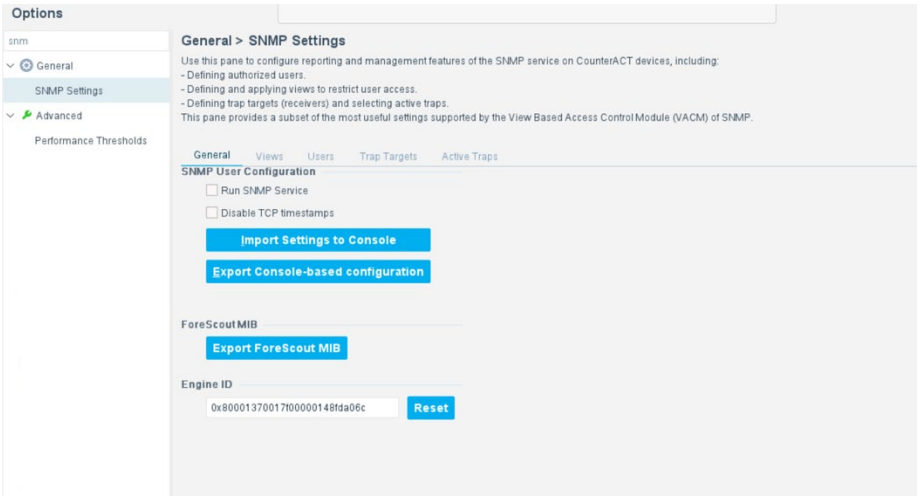

Ilustración 29. Configuración de SNMP (I).

- La casilla *Run SNMP Service*, permite activar/desactivar el servicio SNMP, en función de si se encuentra marcada/desmarcada.
- La casilla *Disable TCP timestams*, permite desactivar las marcas de tiempo TCP para los mensajes SNMP.
- Desde la pestaña *Users*, se pueden definir los usuarios que podrán acceder a los MIB (modelos de información utilziados por SNMP) de Forescout. Para ello, hacer clic en *Add* e introducir los datos deseados**. Se recomienda marcar la casilla *SNMP v3*,** para hacer uso de dicha versión.

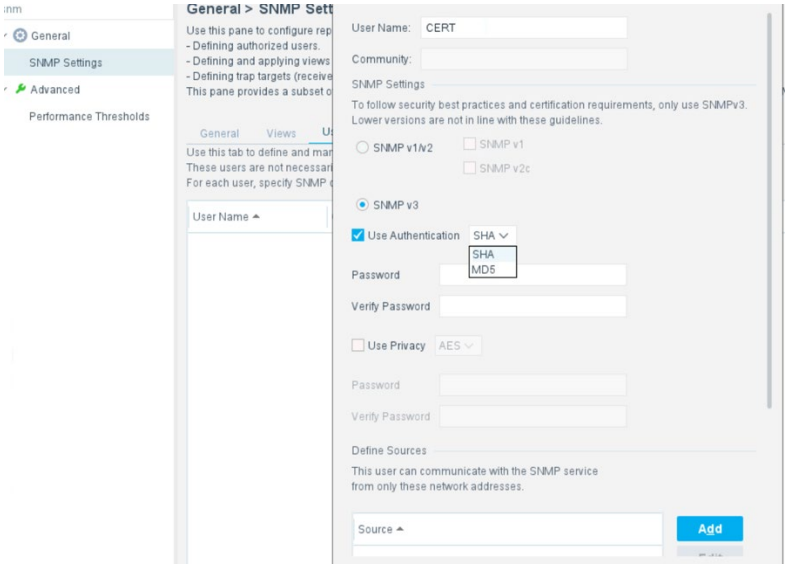

Ilustración 30. Configuración de SNMP (II)

100. El detalle de configuración de SNMP se puede consultar en el apartado *Appendix E* de la guía *Forescout Administration Guide – REF2*.

5.11 ALTA DISPONIBILIDAD

101. El producto presenta dos (2) soluciones para Alta Disponibilidad:

- *Failover Clustering.* La redundancia se obtiene definiendo *clusters* de *appliances*, los cuales toman el control de forma automática en caso de fallo en uno o varios *appliances* dentro del *cluster*. La carga de trabajo se balancea entre los dispositivos del cluster siempre, incluso cuando no hay error.
- *High Availability Pairing.* Se implementa en parejas de dispositivos, de tal forma que la redundancia se obtiene configurando un dispositivo como "Activo" y otro "En espera". El dispositivo en espera toma el control automáticamente en caso de error en el activo.

102. La configuración recomendada es la llamada *Failover Clustering*, al ser la más rápida en la conmutación de la gestión de los dispositivos a controlar entre *appliances* y poder ser configurada en despliegues híbridos.

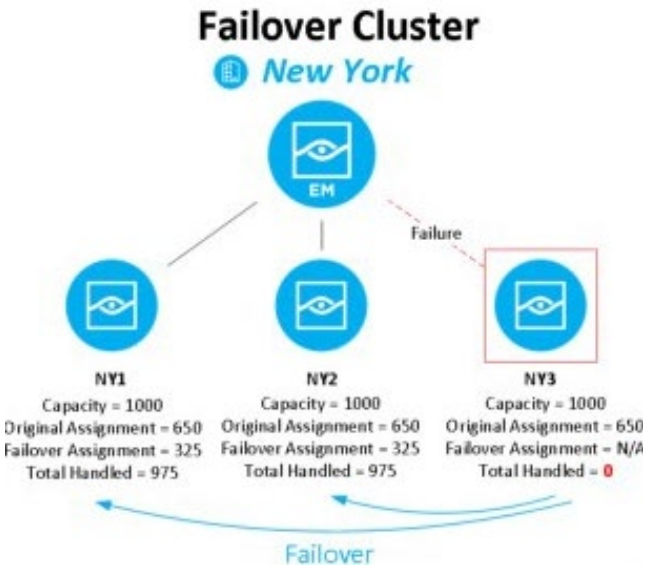

Ilustración 31. Despliegue de Alta Disponibilidad recomendado

103. El detalle sobre los distintos tipos de despliegue de Alta Disponibilidad, así como la configuración de los mismos, se puede consultar en la guía *Forescout Resiliency and Recovery Solutions User Guide – REF3*:

5.12 AUDITORÍA

5.12.1 REGISTRO DE EVENTOS

104. El sistema crea un log con la auditoria de **todas las acciones** realizadas por los administradores/operadores de la herramienta y guarda los eventos de las operaciones (modificaciones/adiciones o borrado) de los usuarios sobre:

- Políticas.
- Arrancar/parar la plataforma de Forescout.
- Claves de usuarios.
- *Plugins* y modulos.

105. Para ver los logs de auditoría, ir a *Log > Audit Trails* y seleccionar el periodo de tiempo deseado. Los detalles de cada log se pueden ver haciendo doble clic sobre el mismo.

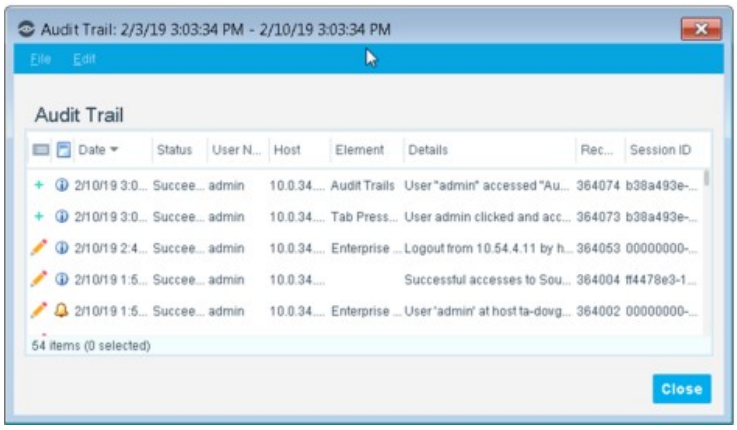

Ilustración 32. Consulta de logs de auditoría

106. El acceso a esta información se puede hacer vía de GUI (tal como se ha visto) o vía ficheros del sistema desde */usr/local/forescout/logs/* con derechos de administrador.

5.12.2 ALMACENAMIENTO LOCAL

107. El almacenamiento local de los logs de auditoría es automático y van rotando. Es decir, los registros más antiguos se borran al llenarse dicho almacenamiento. El tamaño de almacenamiento local viene determinado por el *hardware* y no es configurable, por lo que es **recomendable enviar esos *logs* de forma automática y segura a servidores externos**.

108. Para exportar los logs, desde *Log* > *Audit Trails*, seleccionar *Export* y la ubicación a la que desea exportarse el fichero de logs. El dispositivo permite guardar el fichero en formato TXT o XLS.

5.12.3 ALMACENAMIENTO REMOTO

109. La información de auditoría contenida en la plataforma ForeScout se puede enviar a un servidor de syslog **mediante TLS v1.2.**

110. Para llevar a cabo la configuración de un servidor *syslog* externo y realizar el envío de los logs de auditoría, seguir los siguientes pasos:

- Ir a *Tools* > *Options* > *Modules* > *Core Extensions* > *Syslog*, seleccionar la pestaña *Appliances* y seleccionar el dispositivo que se desee configurar. En caso de despliegues con un solo *appliance*, solo se listará dicho *appliance*. Hacer clic en *Configure*.
- Ir a la pestaña *Send Events To* y hacer clic en *Add*.
- Introducir la información del servidor Syslog externo al cual se desean envíar los logs de auditoría. **Se debe marcar la casilla *Use TLS***, para hacer uso de dicho protocolo en las comunicaciones con el servidor. Por último hacer clic en *Ok*.

- En la pestaña *Syslog Triggers*, seleccionar la casilla *Include timestamp and CounterACT device identifier in all messages*, para incluir toda la información en los logs de auditoría. Seleccionar los tipos de mensajes que se desea enviar al servidor. Verificar que como mínimo se encuentran marcados los de tipo *System Logs and Events*.

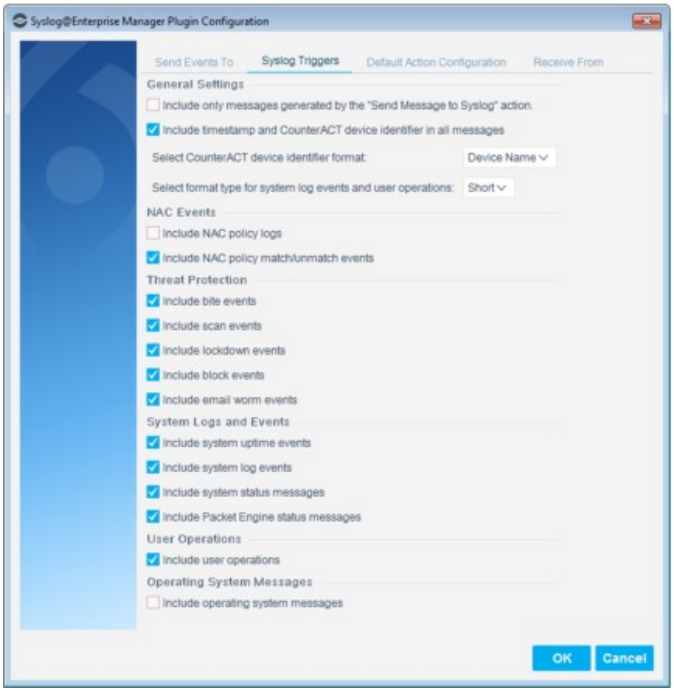

Ilustración 33. Configuración de mensajes enviados al servidor Syslog.

111. Para el correcto funcionamiento utilizando TLS, es necesario configurar los certificados utilizados. Se debe configurar el certificado de sistema (o generar uno nuevo si se desea que sean distintos), para el uso por el *Plugin Syslog*, siguiendo los pasos del apartado 5.6.1 CREACIÓN DE CSR.

112. El detalle de configuración de los servidores Syslog externos se puede consular en el siguiente enlace.

5.13 *BACKUP*

113. El producto permite realizar copias de seguridad de forma manual o automática. La información sobre la que realizar el *backup* es propia de cada dispositivo, por lo que con más de un dispositivo se deben realizar copias de seguridad por cada dispositivo. Un ejemplo de este escenario sería un despliegue con varios *appliances* y un Enterprise Manager.

114. Cada *backup* contiene la configuración de *appliance* y la configuración de la consola. Esta información contiene diferentes categorías:

- Configuración.
- Licencia.
- Configuración del sistema operativo.

- *Plugins*/Módulos.

115. El fichero de *backup* del sistema y sus componentes se cifra utilizando AES-256 para proteger la información sensible que contiene. Para configurar dicha contraseña ir a *Options* > *Advanced* > *Backup* y en la pestaña *Encrypted Password* introducir la contraseña deseada. **Se recomienda el cifrado de la información de *backup*.**

116. Los pasos a seguir para realizar una copia de seguridad manual son los siguientes:

- Ir a *Options* > *Tools*.
- Seleccionar *CounterACT Devices* y después seleccionar el *appliance* deseado.
- Hacer clic en *Backup*. Seleccionar la ubicación en la que se quiere guardar el fichero y hacer clic en *Save*.

117. Los pasos a seguir para programar las copias de seguridad automáticas son los siguientes:

- Ir a *Options* > *Backup*.
- En la pestaña *Backup Server*, introducir los datos del servidor externo al que se desean enviar las copias de seguridad programadas. Se recomienda seleccionar el protocolo *SFTP* para mayor seguridad.
- Las copias de seguridad son cifradas con AES-256. En la pestaña *Encrypted password*, introducir la contraseña de cifrado deseada. Será necesaria posteriormente para acceder a las copias de seguridad.
- Por último, en la pestaña *System Backup, s*eleccionar en *Backup Schedule* la periodicidad con la que se desea realizar las copias y la hora del día deseada.

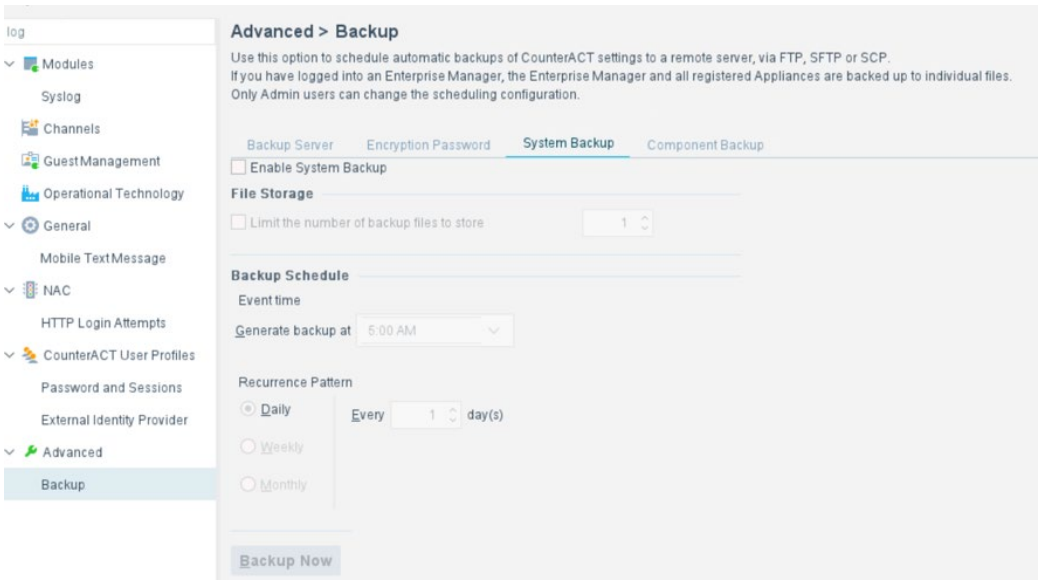

Ilustración 34. Programación de copias de seguridad

118. El detalle de configuración de copias de seguridad, así como su restauración, se puede consultar en el apartado *Backup and Restore Procedures* de la guía *Forescout Upgrade Guide – REF5*.

5.14 SERVICIOS DE SEGURIDAD

5.14.1 CONFIGURACIÓN DE POLÍTICAS

119. Las políticas permiten automatizar y simplificar las tareas necesarias para la securización de la red, por ejemplo:

- Poner en cuarentena dispositivos sin antivirus o con parches desactualizados.
- Limitar el acceso a la red para invitados.
- Habilitar la detección automática de dispositivos.
- Creación de políticas de admisión que determinen quién puede acceder a la red y bajo qué requisitos.

120. El producto contiene políticas predefinidas que pueden utilizarse. Si se desea crear políticas personalizadas, se deben seguir los siguientes pasos:

- Ir a la pestaña *Policy*.
- Seleccionar *Add* en el apartado *Policy Manager*.
- Se abrirá una nueva ventana. Seleccionar *Custom* y luego *Next*.
- Introducir las características deseadas para la política y hacer clic en *Finish*.

121. El detalle sobre las políticas y su utilización se puede consultar en el apartado *Policy Management*, de la guía *Forescout Administration Guide – REF2*.

5.14.2 CONFIGURACIÓN DE ACCIONES

122. Las acciones son medidas tomadas en los dispositivos finales, notificaciones, avisos o restricciones que puede llevar a cabo el producto. Las acciones se pueden incorporar a las políticas y llevarse a cabo cuando ocurren determinadas situaciones.

123. La configuración de las acciones se lleva a cabo desde *Tools > Options > Actions*.

124. El detalle sobre las Acciones se puede consultar en el apartado *Working with Actions*, de la guía *Forescout Administration Guide – REF2*.

5.14.3 AGENTE *SECURECONNECT*

125. El producto permite la instalación del agente *SecureConnect*. Dicho agente permite configurar y gestionar ciertos dispositivos finales desde el producto, realizar ciertas acciones de optimización (como la asignación a VLANs) y el uso del *Compliance Center* (para más información consultar el siguiente enlace).

126. El detalle sobre la configuración y uso del agente se puede consultar en el apartado *Start SecureConnector/Stop SecureConnector* de la guía *Forescout Administrarion Guide – REF2.*

6. FASE DE OPERACIÓN

127. En esta sección se describe la operativa del día a día de la solución y los procesos de mantenimiento para que se dé una utilización segura de la plataforma.

- Comprobaciones periódicas del *hardware* y *software*. **Se deben monitorizar** todas las partes involucradas en la solución. Para llevar a cabo esta monitorización, se recomienda incluir en los sistemas de monitorización de la organización los dispositivos desplegados por Forescout. La herramienta es capaz de mandar eventos del estado de sus sistemas vía *syslog* (cifrado sobre TLS) y recibir *queries* vía SNMPv3 para obtener información del estado del sistema.
- La consola de Forescout, cuando tiene acceso a Internet, comprueba cada cierto tiempo si existen actualizaciones disponibles. Algunas de estas actualizaciones son críticas ya que aplican parches de seguridad sobre la herramienta. Se debe incluir **la aplicación de estas actualizaciones de seguridad** en los procesos de mantenimiento regulares de la organización para tener el sistema en un estado óptimo.
- Así mismo, el producto mantiene registros de auditoria con las actividades que realizan los diferentes administradores de la herramienta y es capaz de mandar de forma segura este tipo de información a un dispositivo externo (SIEM, servidor de *syslog*) para su almacenamiento de forma segura y por el tiempo requerido por la normativa de seguridad de aplicación. **Los registros de auditoría deben ser analizados** con el objetivo de detectar comportamientos anómalos.

6.1 MONITORIZACIÓN DEL ENTORNO

128. El producto recopilará la información de la red y se verificará por el personal de la organización que esta es correcta y que el alcance de recogida de información es el adecuado y deseado.

129. Se crearán la dos (2) políticas básicas:

- Clasificación de dispositivos por tipo (Windows, Linux, impresoras, dispositivos red, etc...).
- Clasificación de dispositivos corporativos y no corporativos, por ejemplo según su pertenecía o no al AD.

6.2 CREACIÓN DE POLÍTICAS

130. **Se deben crear las políticas de control de acceso** (ver apartado 5.14.1 CONFIGURACIÓN DE POLÍTICAS) que se adecuen a las exigencias de seguridad de la organización y verificar la correcta categorización de los dispositivos en cada una de las políticas, aplicando las excepciones que se consideren necesarias antes de aplicar cualquier tipo de acceso de remediación o restricción de acceso.

7. CHECKLIST

131. En este apartado se recoge el *checklist* que recoge las medidas de seguridad definidas a lo largo del documento:

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Registro de los equipos	☐	☐	
Registro de las licencias	☐	☐	
Actualización de firmware	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Modo de Operación seguro activado (FIPS-CC)	☐	☐	
Configuración de servidores externos de autenticación	☐	☐	
Configuración de parámetros de autenticación	☐	☐	
Configuración de usuarios	☐	☐	
Configuración de protocolos seguros	☐	☐	
Creación de certificado de sistema	☐	☐	
Importar certificados de CA de confianza	☐	☐	
Sincronización de hora	☐	☐	
Realización de autochequeos	☐	☐	
Gestión de actualizaciones	☐	☐	
Configuración de SNMP	☐	☐	
Despliegue de Alta Disponibilidad	☐	☐	
Configuración de auditoría	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Creación de servidor externo *Syslog*	☐	☐	
Realización de *backups* periódicos a través de canales seguros	☐	☐	
Configuración de Políticas de Control de Acceso	☐	☐	
Configuración de Acciones	☐	☐	
Instalación de *SecureConnect*	☐	☐	

8. REFERENCIAS

132. El portal de documentación de Forescout donde hace referencia todos los links de este documento se encuentra en: https://docs.forescout.com/

REF1 Forescout Installation Guide v8.2.2
https://docs.forescout.com/bundle/install-guide-8-2/page/install-guide-8-2.Installation-Overview.html

REF2 Forescout Administration Guide v8.2.2
https://docs.forescout.com/bundle/admin-guide-8-2-2/page/admin-guide-8-2-2.Welcome-to-Forescout.html

REF3 Forescout Resiliency and Recovery Solutions User Guide
https://docs.forescout.com/bundle/resiliency-8-2-ug/page/resiliency-8-2-ug.About-Forescout-Resiliency-and-Recovery-Solution.html

REF4 Flexx Licensing How-to Guide
https://docs.forescout.com/bundle/flexx-8-2-htg/page/flexx-8-2-htg.Activate-a-New-License-File.html#pID0E0OE0HA

REF5 Forescout Upgrade Guide
https://docs.forescout.com/bundle/upgrade-guide-8-2-1/page/upgrade-guide-8-2-1.Backup-and-Restore-Procedures.html

9. ABREVIATURAS

AAA	*Authentication, Authorization and Accounting*
AD	*Acrive Directory*
API	*Application Programming Interface*
BYOD	*Bring Your Own Device*
CA	*Certification Authority*
CLI	*Command Line Interface*
CRL	*Certificate Revocation List*
DNS	*Domain Name System*
ENS	*Esquema Nacional de Seguridad*
FTP	*File Transfer Protocol*
GPO	*Group Policy Object*
HTTP	*Hyper Text Transfer Protocol*
HTTPS	*Hyper Text Transfer Protocol Secure*
ICMP	*Internet Control Message Protocol*
IoT	*Internet of Things*
IP	*Internet Protocol*
LAN	*Local Area Network*
NAC	Network Access Policy
NTP	*Network Time Protocol*
OCSP	*Online Certificate Status Protocol*
RADIUS	*Remote Authentication Dial-in User Service*
SFTP	*Secure FTP*
SNMP	*Simple Network Management Protocol*
SSH	*Secure Sehll*
SSL	*Secure Sockets Layer*
SSO	*Single Sign On*
TACACS	*Terminal Access Controller Access Control System*
TCP	*Transmision Control Protocol*
TLS	*Transport Layer Security*
VLAN	*Virtual Local Area Network*

PUBLICACIONES DE DEFENSA

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