centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1104

Procedimiento de empleo seguro
Cisco ISE 2.6

Junio 2021

MINISTERIO DE DEFENSA

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
2021.06.21 15:26:38 +02'00'

NIPO: 083-21-119-7

Fecha de Edición: junio de 2021

CISCO y Applus Laboratories han participado en la realización y modificación del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

ÍNDICE

TABLAS

1. INTRODUCCIÓN

1. **Cisco ISE 2.6** es un producto para control de acceso de red unificado que implementa funcionalidades de autenticación, autorización y auditoría. Todas las funcionalidades son configurables mediante la definición de políticas a través de la interfaz web o a través de línea de comandos.

2. El *software* ISE 2.6 funciona sobre el sistema operativo de despliegue de aplicaciones de Cisco (ADE-OS). Se trata de una distribución de Linux propietaria de Cisco basada en *Red Hat Enterprise* (RHEL v7.5).

3. El producto incorpora una instancia del *Enrutador para Servicios Embebidos* (ESR) de Cisco, con IOS 15.5(3)M8. Esta característica dota al producto de la capacidad de establecer conexiones bajo el protocolo seguro *IPsec* entre el producto y la infraestructura de red sobre la que se despliega.

2. OBJETO Y ALCANCE

4. En la presente guía se recoge el **procedimiento de empleo seguro del *software* Cisco ISE 2.6.**

5. En la siguiente tabla se muestran los dispositivos (físicos o virtuales) donde se despliega el producto, siendo estos compatibles y necesarios como parte del entorno de instalación:

Nombre de la distribución	Características *Hardware*
Cisco ISE Appliance 3515 (SNS-3515)	CPU: Intel Xeon E5-2620 v3 (Haswell)
	RAM: 16 GB
	HDD: 1x600 GB (RAID 0)
	I/O: 2xPCIE, 2xRJ45, 4xUSB 3.0, 1xETHERNET, 2xVGA
Cisco ISE Appliance 3595 (SNS-3595)	CPU: Intel Xeon E5- 2640 v3 (Haswell)
	RAM: 64 GB
	HDD: 4x600 GB (RAID 0+1)
	I/O: 2xPCIE, 2xRJ45, 4xUSB 3.0, 1xETHERNET, 2xVGA
Cisco ISE Appliance 3615 (SNS-3615)	CPU: Intel Xeon Silver 4110 (Skylake)
	RAM: 32 GB
	HDD: 1x600 GB
	I/O: 2xPCIE, 2xRJ45, 4xUSB 3.0, 1xETHERNET, 2xVGA
Cisco ISE Appliance 3655 (SNS-3655)	CPU: Intel Xeon Silver 4110 (Skylake)
	RAM: 96 GB
	HDD: 4x600 GB (RAID 1+0)
	I/O: 2xPCIE, 2xRJ45, 4xUSB 3.0, 1xETHERNET, 2xVGA
Cisco ISE Appliance 3695 (SNS-36955)	CPU: Intel Xeon Silver 4110 (Skylake)
	RAM: 256 GB
	HDD: 8x600 GB (RAID 1+0)
	I/O: 2xPCIE, 2xRJ45, 4xUSB 3.0, 1xETHERNET, 2xVGA
Cisco ISE Engine virtualizado (ISE-VM) **(Características asociadas recomendadas)**	CPU: Intel Xeon Silver 4110 (Skylake)
	RAM: 96 GB
	HDD: 4x600 GB (RAID 1+0)
	I/O: 2xPCIE, 2xRJ45, 4xUSB 3.0, 1xETHERNET, 2xVGA
	Hipervisor: ESXi 6.7

Tabla 1. Dispositivos *Hardware* Compatibles

3. ORGANIZACIÓN DEL DOCUMENTO

6. El presente documento se divide en tres (3) partes fundamentales, de acuerdo a distintas fases que componen el ciclo de vida del producto:

   a) **Apartado 4.** En este apartado se recogen los requisitos o recomendaciones asociadas a la fase de **despliegue e instalación física** del producto.

   b) **Apartado 5.** En este apartado se recogen requisitos o recomendaciones asociadas a la fase de **configuración segura** del producto.

   c) **Apartado 6.** En este apartado se recogen requisitos o recomendaciones asociadas a la fase de **operación y mantenimiento**.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

7. Para asegurar una correcta entrega del producto será necesario revisar que no ha sido manipulado de manera alguna durante su transporte. Para ello, se llevarán a cabo los siguientes pasos:

   a) Antes de abrir el paquete, comprobar que el logo y los motivos de *Cisco Systems* están impresos en él. En caso contrario, se debe contactar con el proveedor del producto (*Cisco Systems* o un distribuidor autorizado por Cisco).

   b) Comprobar que el paquete no ha sido abierto y vuelto a sellar. Esto se puede confirmar examinando los sellos de empaquetado. En caso de que parezca que el paquete ha sido sellado más de una vez, contactar con el proveedor del producto (*Cisco System* o un distribuidor autorizado por Cisco).

   c) Comprobar que la caja tiene una etiqueta blanca con un código de barras, el número de producto, número de serie y otra información relacionada con el contenido de la caja. El objetivo de esta etiqueta es evitar la alteración del interior del paquete. Si se observa que la etiqueta está rota o no está, contactar con el proveedor del producto (*Cisco Systems* o un distribuidor autorizado por Cisco).

   d) Tomar nota del número de serie del producto. Este número se encuentra en la etiqueta blanca del exterior. Se debe comprobar que el número de serie que aparece en dicha etiqueta coincide con el número de serie que se envió de manera separada por correo electrónico. Si no coinciden, contactar con el proveedor del producto (*Cisco Systems* o un distribuidor oficial de Cisco).

   e) Compruebe que la caja fue enviada por el proveedor esperado (*Cisco Systems* o un distribuidor autorizado por Cisco). Para ello, contactar con el proveedor para verificar que la caja ha sido enviada por la compañía de transportes que ha entregado la caja y comprobar que el número de serie de los elementos enviados coincide con el número de serie de los elementos recibidos. Este procedimiento debería hacerse a través de otros recursos no presentes en el proceso de entrega (correo electrónico, FAX o alguna herramienta de rastreo del paquete).

   f) Una vez el producto se ha desempaquetado, inspeccionar la unidad. Comprobar que el número de serie que aparece en el propio producto

coincide con el número de serie de la documentación de envío y del correo electrónico recibido. Si no coincide, se debe contactar con el proveedor del producto (*Cisco Systems* o un distribuidor autorizado por Cisco).

g) Comprobar que el producto tiene la identificación externa tal y como se describe en la siguiente tabla:

Nombre del producto	Modelo	Identificación externa
ISE 2.6 - 3500 Series	3515	SNS-3515
	3595	SNS-3595
ISE 2.6 - 3600 Series	3615	SNS-3615
	3655	SNS-3655
	3695	SNS-3695
ISE 2.6 - ISE-VM	ISE Virtual	Cisco UCS C220-M5SX

Tabla 2. Identificación de productos

4.2 INSTALACIÓN SEGURIDA DE CISCO IDENTITY SERVICES ENGINE

4.2.1 ENTORNO DE DESPLIEGUE

8. En la siguiente figura se puede observar el entorno de despliegue del producto. Tanto los servidores de RADIUS como de Syslog son necesarios para el correcto funcionamiento del producto. Los servidores de Directorio Activo y LDAPS son opcionales.

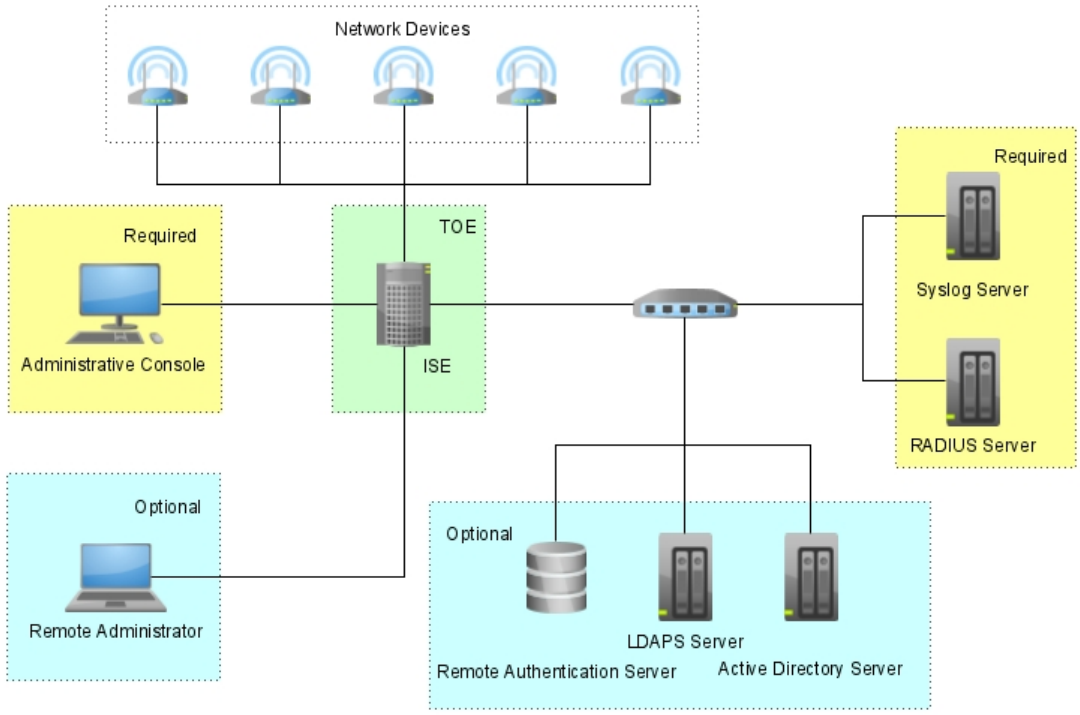

Ilustración 1. Entorno de despliegue

4.2.2 INSTALACIÓN FÍSICA

9. Para llevar a cabo la instalación del dispositivo físico, consultar el documento *Cisco Identity Services Engine Installation Guide, Release 2.6* [**1**], apartado *Install Cisco ISE* bajo la sección *Install Cisco ISE Using CMC*. Es recomendable leer el apartado *SNS 3500/3600 Series Appliances and Virtual Machine Requirements* para comprobar que el entorno de instalación cumple las especificaciones necesarias.

4.2.3 INSTALACIÓN SEGURA

10. Los métodos aprobados para obtener la imagen *software* evaluada *Common Criteria* son los siguientes:

    - Descargar la imagen evaluada *Common Criteria* desde en un ordenador de confianza. Las imágenes *software* se encuentran en la dirección *https://software.cisco.com/download/home/283801620/type/283802505/release/2.6.0*.
    - Seleccionar el fichero llamado *'Cisco ISE Software Version 2.6.0 full installation'*.
    - Comprobar el valor *hash* del *software* descargado con los datos que figuran en la tabla al final del apartado.

11. Los dispositivos se envían con la imagen *software* correcta. Solo será necesario descargar e instalar una nueva imagen en el dispositivo en caso de que la versión obtenida al seguir los pasos marcados en el párrafo 12 no corresponda con la versión evaluada.

12. Para verificar los archivos de actualización de *software* o *firmware*, antes de que sean usados para cualquier actualización, se usan mecanismos de firma digital. Las actualizaciones se pueden descargar desde *software.cisco.com*. Las imágenes están digitalmente firmadas por lo que su integridad puede comprobarse durante la propia actualización. Una imagen cuya comprobación de integridad falla, no será cargada. Los certificados digitales que usan los mecanismos de verificación están dentro del propio producto. Si la firma digital falla, se debe contactar con el Centro de Asistencia Técnica de Cisco.

13. Se debe instalar (si corresponde) la imagen correcta y verificada en el producto. Para ello, arrancar el producto como se indica en *Cisco Identity Services Engine Installation Guide, Release 2.6* [**1**] en el apartado *Install Cisco ISE* bajo la sección *Install Cisco ISE Using CIMC*. Se debe verificar que se carga la imagen correctamente, que completa las auto-comprobaciones internas y que muestra un aviso de exportación criptográfica en la consola.

14. El usuario debe confirmar que, una vez el producto se ha iniciado, la versión cargada es la evaluada. Para ello, se debe ejecutar la sentencia '*show application version ise*' para mostrar la versión del *software* que se está ejecutando en ese momento.

15. A continuación, se encuentra una tabla con las versiones del *software* evaluadas:

Versión	Nombre de la imagen	Función resumen
ISE v2.6.0Cisco Identity	*ise-2.6.0.156.SPA.x86_64.iso*	***SHA512:****9b656990e93397d4e932921af4d563018688fff17677e093d3f70033c85a2773a2c26a933d317d5e1a9191f2e416437f2c0efdd4dcebа0667414ff6e078818f5*
Services Engine Software Patch Version 2.6.0.156-Patch3-19110111	*ise-patchbundle-2.6.0.156-Patch3-19110111.SPA.x86_64.tar.gz*	***SHA512:****3b284436736b93f31ec60fc9f9c8c44f03714c5089143cdfb2ecfdf40ddf7b99e42c6218aa4958f72709629fc53f584b61ec2b06a4738643c2aa8cc32f853489*

Tabla 3. Versiones de *software*

5. FASE DE CONFIGURACIÓN

5.1 CONFIGURACIÓN BÁSICA DEL PRODUCTO

16. El producto requiere de una configuración básica a través de la consola antes de ser conectado a cualquier red.

5.1.1 PARÁMETROS DE CONFIGURACIÓN INICIALES DEL PRODUCTO

17. Al comenzar la configuración del ISE vía CLI, es necesario establecer unos parámetros determinados. Se recomienda consultar el documento *Cisco Identity Services Engine Installation Guide, Release 2.6* [1], apartado *Install Cisco ISE* bajo la sección *Run the Set Up Program.*

18. Es necesario tener en cuenta criterios de complejidad y robustez a la hora de crear la contraseña de administrador. Para ello, se debe consultar la sección del presente documento *Recomendaciones para el entorno de seguridad* [6.1].

19. Del mismo modo, la configuración inicial a través de la GUI HTTPS en lo relativo a contraseñas se realizará de la siguiente manera:

    - Administration > System > Admin Access > Authentication.
    - Hacer *click* en la pestaña *Password Policy*.
    - Cambiar el campo *Minimum Length* a 12.
    - Consultar la sección *Recomendaciones para el entorno de seguridad* [**6.1**] del presente documento y analizar si las necesidades de su organización requieren de políticas adicionales y/o más restrictivas que las aquí presentes.

5.1.2 GUARDADO DE LA CONFIGURACIÓN

20. El producto utiliza dos (2) configuraciones al usar CLI: la configuración de arranque y la configuración en ejecución. Los cambios de configuración afectan a la segunda, por lo que es necesario copiarla y sustituirla por la primera para que tome efecto en un nuevo arranque del sistema. Este propósito puede conseguirse ejecutando las sentencias *write memory* o *copy running-config startup-config*. Estos comandos deben utilizarse frecuentemente al realizar cambios en la configuración del producto. De no ser así, la configuración en tiempo de ejecución se perderá en el reinicio del producto. Al trabajar con la GUI, la configuración queda guardada automáticamente cuando se utiliza el botón *Save*.

5.1.3 HABILITAR EL MODO FIPS

21. **El modo FIPS debe ser activado** para que el producto funcione con la configuración evaluada con Common Criteria. Es decir, para que el producto funcione de acuerdo a unas mínimas garantías de seguridad.

22. Para obtener información adicional sobre el proceso de configuración del modo FIPS, se puede consultar *Configure FIPS Mode on ISE [4]*. A continuación, se muestran los pasos detallados para configurar el producto en modo de operación FIPS:

- Para añadir protocolos permitidos, ir a *Policy > Policy Elements > Results > Authentication > Allowed Protocol"* y hacer *click* sobre el botón *Add*:

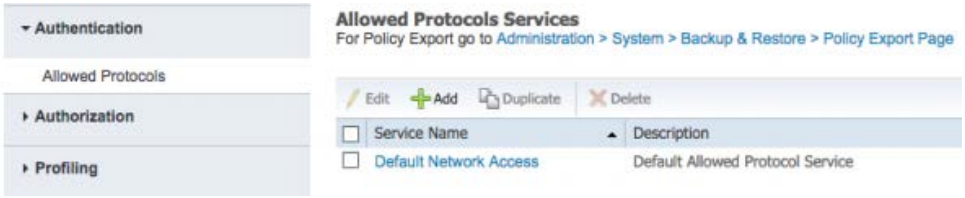

Ilustración 2. Acceso a los protocolos permitidos

- Añadir nombre, descripción y marcar las casillas *Allow EAP-TLS* y *Require Message-Authenticator for all RADIUS Requests* y desmarcar todas las demás:

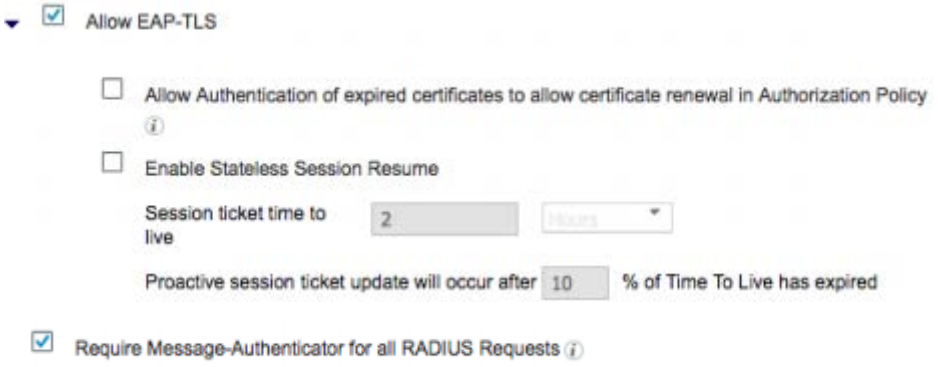

Ilustración 3. Habilitar EAP-TLS

- Hacer click en el botón *Submit* para guardar los cambios. El nuevo servicio de protocolo permitido se mostrará como aparece a continuación:

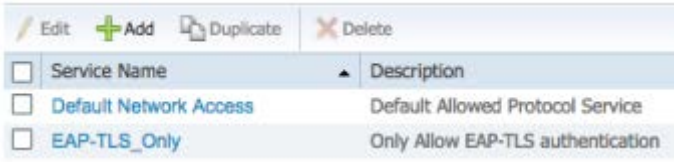

Ilustración 4. Comprobación del nuevo protocolo permitido

- Ir a *Policy > Policy Sets* para modificar la política de autenticación por defecto y permitir los ajustes configurados en lo pasos anteriores. Localizar la política por defecto que tendrá el aspecto mostrado a continuación:

Ilustración 5. Modificación del conjunto de políticas por defecto

- En la columna *Allowed Protocols/Server Sequence*, hacer click en el menú desplegable y la opción creada con anterioridad. En nuestro ejemplo *EAP-TLS_Only y termine haciendo click en el botón* Save:

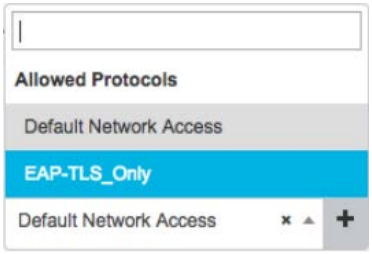

Ilustración 6. Selección de la política de configuración EAP-TLS

- Para eliminar la configuración por defecto que contiene valores inseguros, acceder a *Policy > Policy Elements > Results > Authentication > Allowed Protocols*, seleccionar la casilla *Default Network Access*, hacer click en el botón *Delete* y aceptar el aviso de confirmación haciendo *click* en el botón *Ok*:

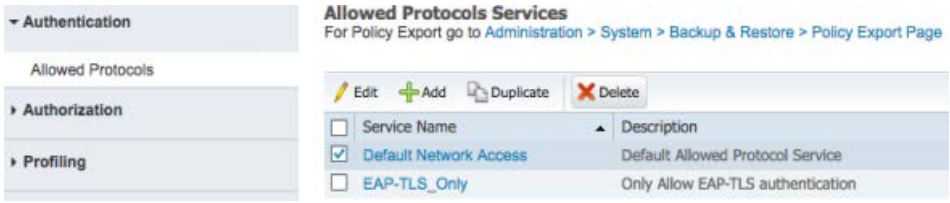

Ilustración 7. Eliminación de los protocolos permitidos por defecto

- Para configurar el producto en modo de operación FIPS, ir a *Administration > System > Settings > FIPS Mode*, en el menú desplegable seleccionar *Enabled*, aceptar el mensaje de confirmación que avisa del reinicio de todos los servicios para aplicar la configuración haciendo *click* en el botón *Ok* y hacer *click* en el botón *Save*:

Ilustración 8. Activación del modo FIPS

- Finalmente, se avisará de que la sesión de usuario terminará y el usuario es devuelto a la interfaz de inicio de sesión. Sin embargo, es necesario esperar a que todos los servicios se reinicien para poder acceder nuevamente. En el nuevo arranque del producto, estará funcionando en el modo de operación seguro FIPS.

23. Una vez activado el modo de operación, el administrador debe verificar que el icono de funcionamiento en modo FIPS aparece a la izquierda del nombre del nodo ISE en la esquina superior derecha de la pantalla dentro de la GUI. A continuación, se muestra la configuración adicional necesaria para llevar a cabo la configuración segura del producto:

    - Ir a *Administration > System > Settings > Security Settings*.
    - Desmarcar las casillas *Allow TLS 1.0, Allow TLS 1.1, Allow legacy unsafe TLS renegotiation for ISE as a client and accept certificates without validation purpose.*

5.1.4 CONFIGURACIÓN DE RADIUS

24. El proceso a seguir para la configuración del protocolo RADIUS utilizando la GUI es el siguiente:

    - Ir a *Administration > System > Settings > Protocols > RADIUS.*
    - Rellenar los campos pertinentes requeridos para llevar a cabo la configuración.

25. Para conectar el producto a un servidor RADIUS externo se puede seguir el siguiente proceso:

    - Ir a *Administration > External RADIUS Servers*
    - Seleccionar '*New*' y especificar nombre, dirección IP, secreto compartido, puerto de autenticación, puerto de datos, tiempo de espera e intentos de conexión.
    - Guardar los cambios haciendo *click* en Enviar.

5.1.5 FIN DE LA SESIÓN

26. La sesión del administrador debe cerrarse si lleva un tiempo inactiva. Para configurar los tiempos de fin de sesión:

    - A través de la GUI, ir a *Administration > System > Admin Access > Settings > Session.* En esta sección se puede configurar el tiempo de inactividad máximo permitido en minutos.
    - Para CLI, la sentencia a ejecutar es terminal *session-timeout <minutos>.*

27. En ambos casos, cuando el tiempo de inactividad máximo permitido es superado, la sesión se cierra y el administrador debe autenticarse nuevamente. El valor seguro que se recomienda para el *timeout* son 15 minutos.

28. El administrador podrá reanudar una sesión cerrada por inactividad tras autenticarse nuevamente. A continuación, se muestra la opción que permite reanudar la sesión:

Ilustración 9. Reanudar una sesión anterior

29. Esta configuración está reservada a los grupos de roles Administrador de CLI, Súper Administrador y Administrador del Sistema. Cualquier administrador del producto puede finalizar su sesión utilizando el botón *Log Out* de la GUI o ejecutando las sentencias *exit* o *forceout <nombre de usuario>* vía CLI.

5.2 CONFIGURACIÓN DE PROTOCOLOS DE RED Y CRIPTOGRAFÍA

5.2.1 PROTOCOLOS DE ADMINISTRACIÓN REMOTA

30. Existen dos (2) alternativas para administrar el producto de forma remota: SSH y/o HTTPS.

31. La única versión de SSH permitida en la configuración segura es la v2. A continuación se encuentra la configuración segura básica del protocolo y su puesta en marcha:

    - El cliente de SSH debe trabajar únicamente con los algoritmos AES-CBC 128 y AES-CBC 256 para cifrado y con SHA-256 para el control de

integridad. La configuración de estos parámetros se realiza ejecutando la siguiente sentencia:

ssh -2 –c [aes128-cbc | aes256-cbc] –m hmac-sha2-256

Nota: El cliente SSH es una entidad externa al producto.

- Para habilitar SSH, el Administrador de CLI deberá ejecutar la siguiente sentencia desde el modo de configuración:

  service sshd enable

- Para asegurar que se utiliza el intercambio de claves con el método adecuado, ejecute la siguiente sentencia desde el modo de configuración de CLI:

  service sshd key-exchange-algorithm ecdh-sha2-nistp256

32. **Debe utilizarse siempre HTTPS para las conexiones con la GUI**. Aunque ambos puertos HTTP (80) y HTTPS (443) se encuentren en estado de escucha, todo el tráfico cuyo destinatario sea el puerto 80 será redirigido al puerto 443. Esta configuración no puede cambiarse.

    Nota: para obtener más información sobre los puertos e interfaces disponibles en el producto, consultar la guía *Cisco Identity Services Engine Installation Guide, Release 2.* [**1**] en la sección *Cisco ISE Administrator Node Port*s.

5.2.2 CONFIGURACIÓN SSL/TLS

33. La configuración segura evaluada y cualificada requiere que las conexiones TLS 1.2 establecidas con el producto utilicen alguno de los siguientes algoritmos:

    - *TLS_RSA_WITH_AES_128_CBC_SHA256* definido en RFC 5246.
    - *TLS_RSA_WITH_AES_256_CBC_SHA256* definido en RFC 5246.
    - *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256* definido en RFC 5289.
    - *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256* definido en RFC 5289.
    - *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384* definido en RFC 5289.
    - *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384* definido en RFC 5289.
    - *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256* definido en RFC 5289.
    - *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384* definido en RFC 5289.
    - *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256* definido en RFC 5289.
    - *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384* definido en RFC 5289.

5.2.2.1 CERTIFICATE SIGNING REQUEST

34. Las instrucciones detalladas para hacer peticiones de firma de certificados a una CA se encuentran en Cisco *Identity Services Engine Administrator Guide, Release*

*2.6 [**2**] bajo Basic Setup > Federal Information Processing Standard Mode Support > Enable Federal Information Processing Standard Mode Support > Create a Certificate Signing Request and Submit it to a Certificate Authority.*

35. El menú para acceder a esta característica está en *Administration > System > Certificates > Certificate Signing Requests.*

5.2.2.2 CONFIGURACIÓN DE CERTIFICADOS DE CLIENTE PARA TLS

36. Los certificados del servidor TLS de la CA para la aplicación administrativa del producto, el servidor LDAPS y el servidor seguro de auditoría *Syslog* se deben importar en el contenedor *Trusted Certificates*. Al realizar esta tarea, se debe aplicar la siguiente configuración:

    - Ir a *Administration > System > Certificates* y seleccionar la opción pertinente entre System Certificates y Trusted Certificates.
    - Marcar la opción *Validate Certificate Extensions*.
    - Los campos con la cabecera *Trusted For* se configuran teniendo en cuenta lo siguiente:

        a) Se debe marcar la opción *Trust for client authentication and Syslog* cuando el producto actúe como cliente seguro *Syslog* de un servidor seguro *Syslog* y el certificado confiable de la CA sea para el servidor.

        b) Cuando el certificado HTTPS del cliente se utiliza para autenticar al producto utilizando autenticación cliente-certificado, el certificado de la CA debe tener también marcada la opción *Trust for client authentication and Syslog*.

        c) Se debe marcar la opción *Trust for authentication within ISE* cuando el certificado de la CA sea para el servidor LDAPS que no pertenece al producto.

37. El certificado del servidor configurado para el uso de autenticación con EAP debe contener, al menos, un identificador de referencia definido en el RFC 6125 como los configurados para el servidor/es LDAPS y servidor/es seguros de auditoría *Syslog*. Para obtener información sobre los identificadores de referencia, se puede consultar la sección "*5.2.12 Configuración del identificador de referencia para la validación de certificados en TLS*" del presente documento.

38. Cuando el producto actúa como servidor TLS, no tiene conocimiento previo del nombre de dominio ni de las direcciones IP de los clientes que se conectan. Los métodos de verificación descritos en el RFC 6125, RFC 2818 y otros, están

diseñados para la verificación de clientes del servidor a través de indicadores de referencia para evitar ataques del tipo *Man-in-The-Middle*.

39. En modo de operación FIPS, el producto no permitirá importar certificados con un tamaño de clave RSA de 1024 bits. El hecho de configurar el producto en este modo de operación también establece un tamaño de 2048 bits en el parámetro de *Diffie-Hellman* para configuraciones de servidor TLS para la administración del producto.

5.2.2.3 REVOCACIÓN DE CERTIFICADOS X.509

40. Cuando el producto actúa como cliente de servidores de auditoría seguros *Syslog* se debe configurar la lista de revocación de certificados (CRL) para cada CA raíz o intermedia. No se utiliza la información de la CRL contenida en los *X.509 CRL Distribution Points.* La revocación de certificados a través del protocolo OCSP tampoco está soportado.

41. Cuando el producto actúa como cliente TLS ante servidores LDAPS, el administrador puede configurar comprobaciones de a través de OCSP y/o CRLs. En el caso de OCSP, el administrador puede configurar la información del respondedor o la información del respondedor contenida en la extensión *Authority Information Access (AIA)* del certificado. Para CRL, los servidores deben configurarse para cada una de las CA raíz o intermedias.

5.2.2.3.1 CONFIGURACIÓN DE REVOCACIÓN DE CERTIFICADOS UTILIZANDO CRLs

42. Para configurar la revocación de certificados X.509 utilizando CRLs se debe seguir el proceso descrito a continuación:

    - Ir a *Administration > System > Certificates > Certificate Management > Trusted Certificates.*
    - Marcar la opción *Download CRL*.
    - Desmarcar las opciones *Bypass CRL Verification if CRL is not Received y Ignore that CRL is not yet valid or expired.*
    - Hacer click en el botón *Save*.

    Nota: esta configuración debe repetirse para cada certificado de una CA raíz o intermedia.

5.2.2.3.2 CONFIGURACIÓN DE LA REVOCACIÓN DE CERTIFICADOS MEDIANTE OCSP

43. Para configurar el revocado de certificados mediante respondedores OCSP, se debe seguir el siguiente proceso:

- Para configurar el respondedor OCSP, ir *a Administration > System > Certificates > Certificate Management > OCSP Client Profile.*
- Para usar la información contenida en la extensión AIA, marcar la casilla *Use OCSP URLs specified in Authority Information Access (AIA)*.
- Marcar la opción *Enable Nonce Extension Support* si el respondedor utiliza *nonces*.
- Marcar la opción *Validate Response* Signakture.
- Para terminar y guardar, hacer *click* en el botón *Submit*.

Nota: si se desea sobrescribir la información del respondedor OCSP contenida en la extensión AIA, se debe desmarcar la opción *Use OCSP URLs specified in Authority Information Access (AIA)* e introducir manualmente la URL del respondedor.

Nota: en caso de querer configurar un segundo respondedor OCSP por si el primero no puede consultarse, se debe marcar la opción *Enable Secondary Server* y repetir la configuración del apartado.

44. Para configurar el respondedor OCSP para todas las CA raíz o intermedias, se debe seguir el proceso definido a continuación:
    - Ir a *Administration > System > Certificates > Certificate Management > Trusted Certificates.*
    - Para cada una de las CA, importar el certificado, marcar la opción *Validate against OCSP Server*, seleccionar el nombre del cliente OSCP creado en el apartado anterior y marcar las opciones *Reject the request if OCSP returns UNKNOWN status* y *Request if OCSP Responder is unreachable*.

5.3 CONFIGURACIÓN DE LOS REGISTROS DE AUDITORÍA

45. El producto incorpora capacidades de registro de las tareas administrativas relevantes como, por ejemplo, la identificación y autenticación de usuarios administrativos. Estos eventos quedan registrados independientemente de si ocurren a través de CLI o de GUI. A continuación, se muestra cómo configurar el producto para que registre todos los eventos relevantes:
    - A través de la GUI, ir a *Administrator > System > Logging > Debug Log Configuration.*
    - Hacer click en el botón *ise* y después en *Edit*.
    - Hacer *click* en el botón *admin-infra* y después en *Edit*.

- Cambiar el valor de *Log Level* a *DEBUG*.
- Hacer *click* en el botón *Save*.
- Hacer *click* en el botón *Infrastructure* y después en *Edit*.
- Cambiar el valor de *Log Level* a *DEBUG*.

5.4 AUTENTICACIÓN DE CLAVE PÚBLICA MEDIANTE SSH

46. Para configurar la autenticación de clave pública en SSH para la conexión CLI, se debe realizar el siguiente proceso, para cada nodo ISE:

- Iniciar sesión vía CLI con privilegios de administrador y acceder al modo de configuración global para crear un usuario CLI ejecutando las siguientes sentencias:

  hostname/userid #configure terminal

  hostname/userid (config)#username <nombre de usuario> password plain <contraseña> role admin

  hostname/userid (config)#end

  hostname/userid #copy running-config startup-config

- Generar un par de claves RSA SSH para el usuario creado en el paso anterior ejecutando las siguientes sentencias en un equipo externo confiable para el usuario de ejemplo *foobar*:

  #/usr/bin/ssh-keygen -v -b 4096

  Nota: la ejecución de este comando genera dos ficheros, uno terminado en "*.key*" y otro en "*.key.pub*", necesarios para el siguiente paso.

  Nota: aunque se trate de un ejemplo, en la sentencia anterior se utilizará para el parámetro "-b" (longitud de clave) y "-t" (tipo de claves) el valor mínimo de 3072 y RSA para cumplir con los estándares definidos en **[6]**.

- Copiar el valor de la clave pública a un servidor que el nodo ISE pueda alcanzar ejecutando la siguiente sentencia:

  #cd /home/foobar

  # scp foobar_ise-administration-node.key.pub

  sftpuser@sftp-server:/home/sftpuser/pub/

- Usar un navegador web, iniciar sesión en el nodo ISE primario como Súper Administrador y configurar un repositorio ISE para permitir al producto obtener el archivo de clave pública del servidor SFTP:

a) Ir a *Administration > System > Maintenance > Repository.*

b) Hacer *click* en el botón *Add.*

c) Rellenar el nombre del repositorio, seleccionar el protocolo SFTP, introducir el nombre del servidor y la ruta e introducir las credenciales.

d) Terminar la configuración haciendo *click* en el botón *Submit*.

- Añadir la clave de host del servidor SFTP iniciando sesión vía CLI en el nodo ISE de administración donde fue creado el usuario del primer apartado de la sección y ejecute las siguientes sentencias:

  hostname/userid #crypto host_key add host [FQDN | dirección IPv4]

  Nota: la dirección IPv4 o el FQDN deben coincidir con el valor del campo configurado en el repositorio *SFTP Server Name*.

- Para autorizar el uso de clave pública para el usuario creado en el primer apartado, ejecutar las siguientes sentencias iniciando sesión vía CLI con este mismo usuario:

  hostname/userid #crypto host_key add host [FQDN | IPv4 address]

  Nota: la dirección IPv4 o el FQDN deben coincidir con el valor del campo configurado en el repositorio *SFTP Server Name*.

  hostname/userid #show repository sftp | include foobar

  Nota: el resultado de la ejecución de la sentencia anterior debería ser semejante a *foobar_ise-administration-node.key.pub*, indicando así que el fichero está presente en el servidor SFTP y que el cliente SFTP de ISE es capaz de encontrarlo.

  hostname/foobar #crypto key import foobar_ise-administration-node.key.pub repository sftp

  Nota*:* los campos *foobar_ise-administration-node.key.pub* y *sftp* se corresponden con los nombres de la clave pública y del repositorio respectivamente.

  hostname/foobar #show crypto authorized_keys

  Nota: comprobar que el resultado de la ejecución de la sentencia anterior muestra la clave pública asociada al usuario creado en el ejemplo.

5.5 PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

47. Si se desean realizar copias de seguridad de los registros de auditoría de las instancias del producto o enviarlos a otras entidades de la infraestructura IT, se debe garantizar la seguridad en las comunicaciones. Para ello, se necesita inhabilitar la utilización del protocolo UDP para la gestión de registros de auditoría en virtud de una configuración segura con TLS.

48. Para configurar la seguridad de los canales de comunicación del producto con entidades externas de auditoría:

    - Ir a Administration > System > Logging > Remote Logging Targets.
    - Hacer *click* en el botón *Add* e introducir los campos de información requeridos para identificar al recibidor seguro *Syslog* incluyendo nombre, dirección IP o *Full Qualified Hostname*.

      Nota: introducir solo el *Full Qualified Hostname* cuando el certificado X.509 del servidor seguro Syslog contenga una extensión subjectAltName del tipo *dNSName* o cuando el *Subject Common Name* contenga el *Fully Qualified Domain Name* del servidor seguro *Syslog*.
    - Introducir la dirección IPv4 cuando el certificado X.509 del servidor seguro *Syslog* contenga una extensión *subjectAltName* del tipo *iPAddress*.
    - Escoger la opción *Secure Syslog* dentro del menú desplegable *Target Type*.
    - Confirmar que el puerto elegido se corresponde con el establecido en el servidor de Syslog.
    - Elegir LOCAL5 en el desplegable de *Facility Code*.
    - Marcar las opciones Buffer Messages When Server Down y Enable Server Identity Check.
    - Escoger el certificado de la CA para el servidor seguro *Syslog* dentro del menú desplegable *Select CA Certificate*.
    - Asegurarse de dejar el resto de ajustes en sus valores por defecto y de desmarcar la opción *Include Alarms for this Target*.
    - Guardar los cambios en la configuración haciendo *click* en el botón *Submit*.

49. Después de completar la configuración, aparecerá el nuevo nodo en la tabla con el rótulo *"Remote Logging Targets"*. Sin embargo, todavía se debe especificar qué tipo de registros de auditoría se mandarán al nodo recién configurado:

- En la GUI, ir a *Administration > System > Logging > Logging Categories*.
- Para cada opción disponible, hacer *click* en el botón *Edit* y seleccionar el nombre del nodo configurado con anterioridad mediante el menú *Targets > Available*. Hacer *click* en el botón *">"* para añadirlo en la caja de seleccionados.
- Guardar la configuración haciendo *click* en el botón *Save*.

50. Finalmente, configurar los nodos ISE configurados para recibir registros de auditoría:

- En la GUI, ir a *Administration > System > Logging > Remote Logging Targets.*
- Desactivar la opción *Log Collector* y hacer click en el botón *Edit*. En el menú desplegable *Status*, seleccionar *Disabled*. Se recomienda asegurarse que no existen más *Log Collector* en la lista con el mismo nombre puesto que utilizan el puerto UDP y son inseguros. En caso de existir, repetir este paso para eliminarlos. Hacer click en *Save* para guardar los cambios.
- Para activar el *Secure Log Collector*, seleccionar la opción *TCPLogCollector*, hacer click en *Edit*, seleccionar del desplegable *Status* la opción *Enabled* y finalizar la configuración haciendo click en *Save*.

5.6 BLOQUEO DE USUARIO

51. Para configurar los intentos de inicio de sesión que tiene un usuario antes de que sea bloqueada su cuenta, se seguirá el siguiente procedimiento:

- Acceder al menú Administration > System > Admin Access > Authentication > Lock/Suspend Settings.
- Marcar la opción Suspend or Lock Account with Incorrect Login Attempts.
- Especificar el número de intentos fallidos disponibles (en un rango de 3 a 20 intentos) por el usuario antes de que su cuenta sea bloqueada. No se recomienda utilizar más de 5 intentos.
- Seleccionar la opción *Lock Account*.
- De manera opcional, se podrá mostrar un mensaje cuando la cuenta sea bloqueada mediante la opción *Configure Lockout Message*.

52. Para asegurar que la cuenta de administrador no queda bloqueada y sin acceso a causa de esta política, se deberá configurar una cuenta de emergencia administrativa local.

5.7 GESTIÓN DEL RELOJ DEL SISTEMA

53. Para establecer manualmente el reloj *hardware* local del sistema se utilizará el comando *clock*. A continuación, se encuentra un ejemplo de su sintaxis básica:

clock [set {mes | día | hh:min:ss | año}]

54. Para más información, consultar el comando clock en Cisco Identity Services Engine CLI Reference Guide, Release 2.6 [**3**], bajo la sección Cisco ISE CLI Commands in EXEC Mode.

5.8 IDENTIFICACIÓN Y AUTENTICACIÓN

55. La configuración de identificación y autenticación está reservada para los grupos administrativos siguientes: Administrador de CLI, Administrador de Identidades, Súper Administrador y Administrador del Sistema.

56. Cisco ISE 2.6 funciona con los siguientes métodos de autenticación:

- Autenticación remota (Directorio Activo y LDAP) requiriendo al usuario de una combinación de usuario y contraseña correcta. Esta configuración es opcional.
- Autenticación local mediante contraseña administrativa. Es la configuración por defecto y no es necesario realizar ninguna configuración adicional para habilitarla.

5.9 REDES PRIVADAS VIRTUALES (VPN)

57. Para acceder a los recursos protegidos de la organización, el NAS (*Network Access Server*), los dispositivos de red se comunican con el producto para verificar la identidad de los usuarios antes de permitir su acceso. Para llevar a cabo esta tarea, el tráfico entre los dos agentes debe estar protegido. En esta sección se explican los parámetros de configuración para utilizar IPsec e IKE con el objetivo de establecer un túnel seguro.

58. Mediante el uso de *IPsec*, los administradores privilegiados pueden definir el tipo de tráfico que debe ser protegido entre dos puertos *IPsec*, a través de la configuración de listas de acceso y su aplicación a las interfaces utilizando conjuntos de mapas criptográficos. Por ejemplo, el tráfico a proteger se puede seleccionar en base a la dirección de destino y al origen del flujo de información.

59. Adicionalmente, un conjunto de mapas criptográficos con múltiples entradas funciona de tal manera que el enrutador intenta comprobar si cierto paquete se ajusta a la lista de acceso de alguna de dichas entradas.

60. Este filtrado puede activar la ejecución de *IPsec* utilizando IKE para establecer una conexión segura entre los dos puertos. De este modo, se utiliza un conjunto de transformaciones compuesto por protocolos de seguridad, algoritmos y otros ajustes que se aplican al tráfico protegido por *IPsec*. Durante la negociación de la conexión con IKE, se acuerda utilizar un mismo conjunto de transformaciones.

61. Los ajustes específicos de *IKE* e *IPsec* deben configurarse manualmente puesto que los valores por defecto no cumplen con los estándares mínimos para considerarse seguros, según las guías *CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad* [**6**] y *CCN-STIC 836 Seguridad en VPN* [**7**].

62. Para configurar los túneles *IPSec,* es necesario asignar una dirección IP a la interfaz por la que se va a establecer el túnel. Para ello, hay que seguir los siguientes pasos:

    configure terminal

    interface GigabitEthernet <número de la interfaz>

    ip address <ip para asignar> <máscara de red>

    no shutdown

63. Se debe llevar a cabo el siguiente procedimiento para habilitar la utilización de IPsec en un nodo ISE con una interfaz específica:

    - Ir a *Administration > Settings > Protocols > IPSec.*
    - Seleccionar el nodo ISE deseado.
    - Marcar el valor *Enabled* para la opción *Enable/Disable IPSec for selected nodes.*
    - En la opción *IPSec interface for selected nodes*, elegir la interfaz de red deseada.
    - En la opción *Authenticated for selected nodes,* elegir la opción *Pre-shared key* e introduzca el valor secreto compartido para establecer el túnel IPSec.
    - Hacer *click* en *Save* para guardar los cambios y aceptar el mensaje de alerta que le indicará el reinicio del producto para aplicar la configuración definida anteriormente.

5.9.1 CONJUNTOS DE TRANSFORMACIÓN IKEv2

64. Una proposición IKEv2 es un conjunto de transformaciones utilizado en la negociación de una conexión segura. Esta proposición se da por concluida cuando se negocia al menos un algoritmo criptográfico, un algoritmo de integridad y un grupo *Diffie-Hellman (DH).*

65. Para configurar los conjuntos de transformación *IKEv2*, se debe seguir el siguiente procedimiento:

TOE-common-criteria#conf t

TOE-common-criteria (config)#crypto ikev2 proposal sample

TOE-common-criteria (config-ikev2-proposal)#integrity sha256

TOE-common-criteria (config-ikev2-proposal)#encryption aes-gcm-256

Nota: adicionalmente, pueden elegirse los algoritmos 'encryption aes-cbc-128', aes-cbc-256' y 'aes-gcm-128'.

TOE-common-criteria (config-ikev2-proposal)#group 19

Nota: adicionalmente, pueden elegirse los grupos, 20 (384-bit ECP aleatorio), 24 (2048-bit MODP con 256-bit POS) y 16 (4096-bit MODP).

TOE-common-criteria (config)#crypto ikev2 keyring keyring-1

TOE-common-criteria (config-ikev2-keyring)#peer peer1

TOE-common-criteria (config-ikev2-keyring-peer)#address 0.0.0.0 0.0.0.0

TOE-common-criteria (config-ikev2-keyring-peer)#pre-shared-key <clave>

Nota: en la generación de una PSK (*pre-shared key*) se deben observar y respetar las mismas indicaciones que para la generación de contraseñas personales. Consultar la sección 5.5 Contraseñas del presente documento para obtener más información al respecto.

Nota: al generar la PSK, puede elegirse un tamaño de clave de hasta 128 bytes. A mayor longitud, mayor seguridad del criptosistema a costa de un tiempo de procesamiento mayor.

TOE-common-criteria (config)#crypto logging ikev2

Nota: la configuración para IKEv2 anterior es solo un extracto de los parámetros seguros que deben introducirse, pero no está completa. Para obtener información sobre la configuración completa consulte *"Configuring Internet Key Exchange Version 2 (IKEv2)"* [**8**].

5.9.2 TRANSFORMACIONES IPSEC Y TIEMPOS DE ESPERA

66. Con el objetivo de configurar correctamente las transformaciones *IPsec* para el cifrado ESP y los tiempos de espera *IPsec,* se deben ejecutar las siguientes sentencias:

TOE-common-criteria (config)#crypto ipsec transform-set example esp-gcm 256 esp-sha256-hmac

Nota: este comando configura ESP de IPsec para trabajar con HMCA-SHA-256 y AES-CBC-256. Para establecer otras configuraciones válidas, se pueden utilizar los siguientes valores:

Algoritmo de cifrado	Comando
AES-CBC-256	*esp-aes 256*
AES-GCM-128	*esp-gcm 128*
AES-GCM-256	*esp-gcm 256*

Tabla 4. Configuraciones IPSec

Nota: el tamaño de la clave seleccionada debe ser igual o menor que la seleccionada en los ajustes de cifrado para IKE. Por ejemplo, si el cifrado de IKE se configuró para trabajar con aes-cbc-128, **únicamente** podría seleccionarse aquí *aes-cbc-128* o *aes-gcm-128*.

TOE-common-criteria (config)#mode tunnel (la alternative es transport)

Nota: el modo túnel de IPsec es el valor por defecto de la configuración. Sin embargo, si se especifica explícitamente, el enrutador solicitará el modo túnel y este será el que únicamente se acepte.

TOE-common-criteria (config)#crypto ipsec security-association lifetime seconds 14400

Nota: el valor por defecto para este ajuste es de 1 hora. Sin embargo, para ceñirse a la configuración segura admitida en las guías *CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad* [**6**] y *CCN-STIC 836 Seguridad en VPN* [**7**], este tiempo no debería ser superior a 4 horas.

Nota: el valor por defecto para este ajuste es de 2560 KB (el mínimo configurable). Sin embargo, el valor recomendado para asociaciones de seguridad es de 100 MB de tráfico.

Nota: toda la configuración relativa a este apartado está reservada al administrador privilegiado.

5.9.3 NAT TRAVERSAL

67. Para que pueda aplicarse correctamente *NAT traversal* en un dispositivo *NAT* con *IOS-XE* para establecer una comunicación *IPsec* entre dos puertos *IOS-XE*, se debe realizar la siguiente configuración:

- Para un dispositivo *IOS NAT* (enrutador entre dos pares *IPsec*):

  config terminal

  ip nat service list <número de la CAL> ESP spi-match

  access-list <número de la CAL> permit <protocolo> <rango local> <rango remoto>

  end

- Para cada dispositivo *IOS* (dispositivos finales conectados al enrutador *IPsec*):

  config terminal

  crypto ipsec nat-transparency spi-matching

  end

5.9.4 CERTIFICADOS X.509

68. **Se deben utilizar certificados X.509**. Hasta ahora el producto se ha configurado con *pre-shared-key,* por lo tanto, estos pasos sólo deberán seguirse para configurar el uso de certificados. La configuración del producto soporta la utilización de certificados *X.509v3* para autenticar pares *IPsec*. El proceso de creación y carga de certificados al producto está cubierto por los puntos siguientes.

5.9.4.1 CREACIÓN DE CSRs

69. La petición de firma de certificado se creará utilizando el par de claves RSA y el nombre de dominio configurados en el producto con anterioridad. Para generar esta petición, el producto debe configurarse con un nombre de *host* y un punto confiable (*trustpoint*) como se muestra a continuación:

Device #configure terminal

Device (config)#hostname <nombre de host>

Decive (ca-trustpoint)#crypto pki trustpoint <nombre del trustpoint>

Decive (ca-trustpoint)#enrollment <terminal> <url> (ejemplo: enrollment url http://192.168.2.137:80)

Decive (ca-trustpoint)#subject-name CN=<hostname.domain.com>, OU=<OU>

Decive (ca-trustpoint)#revocation-check crl

Decive (ca-trustpoint)#exit

Device (config)#crypto pki enroll <nombre del endpoint>

5.9.4.2 CONEXIÓN SEGURA A UNA AUTORIDAD DE CERTIFICACIÓN (CA) PARA LA FIRMA DEL CERTIFICADO

70. El producto se conectará con la CA para la firma del certificado utilizando *IPsec*. El siguiente ejemplo configurará el dispositivo para trabajar con un túnel *IPsec* con cifrado AES, con la dirección 10.10.10.102 en el extremo *IPsec* de la CA y con la dirección 10.10.10.110 en el extremo de un dispositivo local:

Device #configure terminal

Device (config)#crypto ikev2 policy <nombre de la política>

Device (config-ikev2)#encryption aes

Device (config-ikev2)#authentication [local | remote] ecdsa-sig

Device (config-ikev2)#group 19

Device (config-ikev2)#lifetime seconds 86400

Device (config)#crypto ikev2 enable outside

Device (config)#crypto ipsec ikev2 ipsec-proposal ikev2-proposal

Device (config)#protocol esp encryption aes

Device (config)#protocol esp integrity sha256

Device (config)#access-list ikev2-list extended permit ip 10.10.10.0 0.255.255.255 10.10.10.0 0.255.255.255

Device (config-tunnel-ipsec)#tunnel-group 10.10.10.102 type ipsec-l2l

Device (config-tunnel-ipsec)#tunnel-group 10.10.10.102 ipsec-attributes

Device (config)#ikev2 local-authentication certificate

Device (config)#ikev2 remote-authentication certificate CA

Device (config)#crypto ikev2-map 1 match address ikev2-list

Device (config)#crypto map ikev2-map 1 set peer 10.10.10.102

Device (config)#crypto map ikev2-map 1 set ikev2 ipsec-proposal ikev2-proposal

Device (config)#crypto map ikev2-map interface outside

5.9.4.3 AUTENTICACIÓN DE LA AUTORIDAD DE CERTIFICACIÓN (CA)

71. El producto realiza la autenticación de la CA comprobando que sus atributos coinciden con la huella digital de acceso público. El administrador del producto cotejará manualmente los resultados del siguiente proceso con los datos figurantes en la página web de la CA:

    Device (config)#crypto ca authenticate <nombre del trustpoint>

    Nota: después de la ejecución de esta sentencia se devolverá un resultado con la huella digital de la CA del estilo:

    "Fingerprint XXX: YYYY…"

    "Do you accept this certificate? [yes/no]: yes" (elegir la opción adecuada en función de la comparación de los datos explicada con anterioridad).

    "Trustpoint CA certificate accepted".

5.9.4.4 GUARDADO DE LOS CERTIFICADOS EN EL ALMACENAMIENTO LOCAL

72. Por defecto, los certificados se almacenan en *NVRAM*. Sin embargo, algunos enrutadores no disponen de la cantidad de *NVRAM* necesaria para almacenar certificados. Todas las plataformas Cisco permiten el almacenaje local y en *NVRAM*.

73. Dependiendo de la plataforma, el administrador autorizado podrá disponer de otros dispositivos de almacenaje soportados como *bootflash, slot*, *disco*, *flash USB* o *token USB*. El administrador autorizado puede decidir en tiempo de ejecución qué método de almacenamiento local desea utilizar. Para más información, consultar [**9**].

74. El siguiente ejemplo muestra cómo se configura el dispositivo para guardar certificados en el almacenamiento local:

    Device #configure terminal

    Device (config)#crypto pki certificate storage <identificador de almacenaje> (por ejemplo: flash:/certs)

    Device (config)#exit

    Device #copy system:running-config nvram:startup-config

    Device #show crypto pki certificates storage

    Nota: un ejemplo de respuesta tras ejecutar la sentencia:
    *"**show crypto pki certificates storage**" podría ser el siguiente:*
    "Certificates will be stored in flash:/certs/"

5.9.4.5 CONFIGURACIÓN DE VERIFICACIÓN DEL ESTADO DE LOS CERTIFICADOS

75. La siguiente tarea permite configurar mecanismos de revocación de certificados basados en *CRL* (esta es la configuración recomendada) u *OCSP*. **Se debe comprobar el estado de revocación de los certificados.**

76. Se debe utilizar el comando *revocation-check* para seleccionar, dentro de lo posible *CRL* u *OCSP* en su defecto. También es posible especificar uno y después el otro para que, de esta manera, primero se utilice *CRL* y, si resultase algún error, *OCSP*.

77. En la situación en la que el producto no sea capaz de obtener una *CRL* y/o el servidor *OCSP* retorne un error, el producto rechazará el certificado del extremo.

78. Al utilizar *OCSP* se utilizan valores únicos en las comunicaciones de seguridad (*nonces*) que proporcionan una seguridad mayor al canal de comunicación. Sin embargo, si el servidor *OCSP* no acepta estos datos, el administrador podrá desactivar esta característica.

5.9.4.6 CONFIGURACIÓN OSCP

79. Los administradores pueden invalidar los ajustes del servidor *OCSP* que figuran en el campo *Authority Information Access (AIA)* del certificado, ejecutando la sentencia *ocsp url.*

80. Pueden especificarse varios servidores *OCSP*; por certificado del cliente o por grupo de certificados utilizando el comando *match certificate override ocsp*. Esta sentencia hace que los datos del campo AIA del certificado del cliente o la configuración establecida con *ocsp url* no tengan validez si el certificado de un cliente coincide correctamente con un mapa de certificado durante la comprobación de la revocación.

5.9.4.7 CONFIGURACIÓN DE LA VALIDACIÓN DE LA CADENA DE CERTIFICADOS

81. A continuación, se indica la configuración necesaria para determinar el nivel de profundidad de validación de la ruta de certificación. Se deberá tener en cuenta que el dispositivo en cuestión debe estar inscrito en una jerarquía de PKI y que debe estar asociado con el certificado el par correcto de claves.

82. Seguir el proceso a continuación para llevar a cabo dicha configuración:

    TOE-common-criteria #configure terminal

    TOE-common-criteria (config)#crypto pki trustpoint <nombre del trustpoint de la PKI>

TOE-common-criteria (ca-trustpoint)#chain-validation [stop | continue] <nombre del trustpoint padre>

Nota: la palabra clave *stop* indica que el certificado ya está validado, mientras que la palabra clave *continue* indica que debe verificarse el certificado subordinado de la CA asociado con el *trustpoint*.

83. El argumento *<nombre del trustpoint padre>* indica el nombre del *trustpoint* de nivel superior contra el que debe verificarse el certificado.

TOE-common-criteria#exit

5.9.4.8 VALIDACIÓN DE CERTIFICADOS

84. El producto valida por defecto los certificados del extremo *IPsec*. Opcionalmente, el administrador puede añadir restricciones al nombre del sujeto en el *truspoint* de CA. A continuación, se muestra una configuración de ejemplo para este proceso:

TOE-common-criteria (config)#crypto pki certificate map <nombre del mapa de certificado> 1 subject-name co example

TOE-common-criteria (config)#crypto pki trustpoint <nombre del trustpoint de la CA>

TOE-common-criteria (ca-trustpoint)#enrollment terminal

TOE-common-criteria (ca-trustpoint)#match certificate <nombre del mapa de certificado>

TOE-common-criteria (ca-trustpoint)#end

TOE-common-criteria (config)#crypto pki trustpoint CA sub

TOE-common-criteria (ca-trustpoint)#enrollment terminal

TOE-common-criteria (ca-trustpoint)#subject-name CN=<common name>,OU=<organizational unit>,O=<organization>

TOE-common-criteria (ca-trustpoint)#match certificate

TOE-common-criteria (ca-trustpoint)#end

85. Para obtener más información relacionada con la configuración de certificados, consulte el capítulo *Configuring Certificate Enrollment for a PKI* de [**10**].

Nota: el administrador será notificado con un mensaje de error diciendo que la cadena de verificación del certificado ha fallado cuando algún certificado no concuerde con los criterios configurados.

5.9.4.9 CONFIGURACIÓN DE X.509 PARA IKEv2

86. Para utilizar certificados *X.509* junto con *IKEv2*, realice la siguiente configuración:

TOE-common-criteria (config)#crypto ikev2 profile simple

TOE-common-criteria (config-ikev2-profile)#authentication [remote | local] [rsa-sig | ecdsa-sig]

Nota: si se carga un certificado inválido la autenticación no funcionará.

5.9.4.10 BORRADO DE CERTIFICADOS

87. El producto almacena los certificados propios y el certificado de la CA. Por este motivo, cabe la posibilidad de necesitar borrar algún certificado.

88. Para borrar un certificado del producto, se debe seguir el siguiente proceso:

Device #show crypto ca certificates

Device (config)#crypto ca certificate chain name

Device (config-cert-cha)#no certificate certificate-serial-number

89. Para borrar el certificado de una CA, debe eliminarse completamente la identidad de la CA. Este proceso también elimina todos los certificados asociados a la CA (el certificado del producto y el de la CA). Para realizar esta tarea, seguir el siguiente proceso:

Device (config)#no crypto ca identity name

5.9.5 CONFIGURACIÓN DE EAP-TLS

90. Para iniciar la configuración de EAP-TLS será necesario continuar la configuración que se empezó habilitando el modo FIPS en el párrafo 21.

91. Para la creación de una regla de política de autenticación para *EAP-TLS,* se deben seguir los siguientes pasos:

- Ir a *Policy > Policy Sets*, en la fila con la descripción *Default Policy Set*. Hacer *click* en el botón > y se desplegarán las políticas de autenticación y las reglas de políticas de autorización.

Ilustración 10. Acceso a las reglas y políticas de autorización

- Hacer *click* en *Authentication Policy* para mostrar dichas reglas y, en la nombrada como *Dot1X*, hacer *click* en el icono del engranaje ⚙ en el extremo derecho de la regla y seleccionar *Insert* New *Row Above*. Se

mostrará la nueva regla creada con el nombre *Authentication Rule 1* encima de la regla nombrada como *Dot1X*.

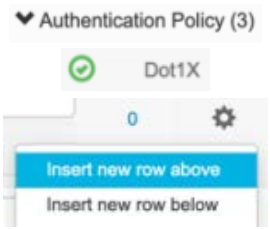

Ilustración 11. Adición de una política de autenticación

- Modificar el nombre de la nueva regla creada identificada como *Authentication Rule 1* por uno más descriptivo haciendo click sobre el texto. Por ejemplo, *EAP_TLS_Dot1X*.

Ilustración 12. Creación de una política de autenticación

- Añadir una condición en la nueva regla creada. Para ello, hacer *click* en el botón  de la columna *Conditions*. Observar que se abre el menú llamado *Conditions Studio*.
- Arrastrar el ítem *EAP-TLS* de la lista de librerías de la parte izquierda hacia el Editor para que se aplique la regla. Finalmente, hacer *click* en el botón *Use* para guardar los cambios en la regla.

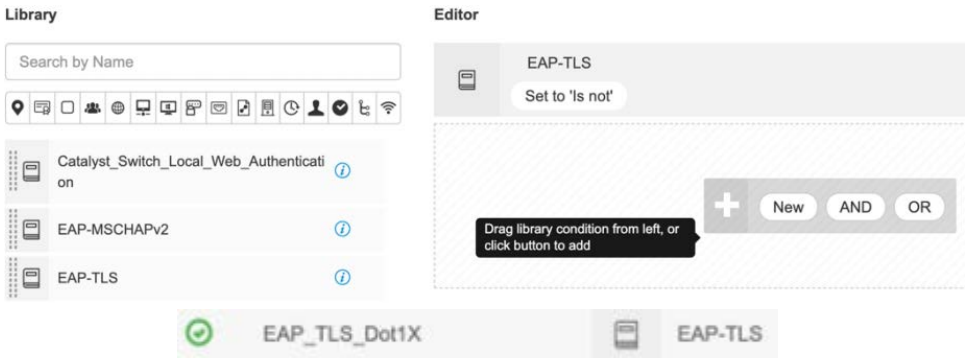

Ilustración 13. Añadir la nueva condición de EAP-TLS a la política de autenticación

- En la columna *Use* que se corresponde con la regla, hacer *click* en el icono  del valor *Internal Users* y seleccionar la opción del *Certificate Authentication Profile* creado con anterioridad. Hacer *click* en el botón *Save* para guardar los cambios.

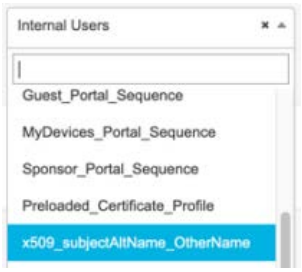

Ilustración 14. Elección del campo del certificado para la autenticación

- Añadir un dispositivo de acceso a la red. Ir a Administration > Network Resources > Network Devices.

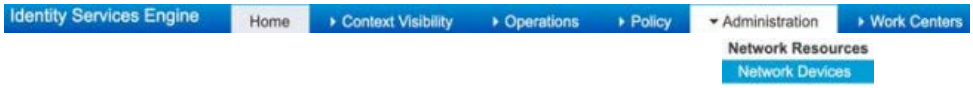

Ilustración 15. Acceso a la opción *Network Devices*

- Hacer *click* en el botón *Add* para agregar un dispositivo de acceso a la red.

Ilustración 16. Adición de un dispositivo de red

- Rellenar los campos de datos relativos a *RADIUS*: nombre, dirección/es IP del dispositivo de red, marcar la opción RADIUS *Authentication Settings*, rellenar el secreto compartido para *RADIUS* y hacer *click* en el botón *Submit* para guardar los cambios.

92. La configuración segura del producto para trabajar exclusivamente con TLS 1.2 y suites de cifrado seguras, se realiza a través de la barra superior, ir a *Administration > System > Settings.*

Ilustración 17. Acceso a los ajustes del sistema

- En la barra de navegación situada en el lateral izquierdo, seleccionar *Security Settings*.

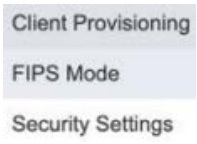

Ilustración 18. Acceso a los ajustes de seguridad

- Desmarcar todas las casillas de configuración por defecto y marcar las siguientes: *Allow ECDHE-RSA ciphers y Disclose invalid usernames* con la opción *Always show invalid usernames*. Hacer *click* en *Save* y aceptar el aviso de reinicio del producto para que los cambios tomen efecto.
- Para comprobar el estado del servicio y asegurarse de que se ha completado el reinicio correctamente, autentíquese mediante CLI con un usuario administrativo y ejecute la sentencia *show application status ise.* Si el estado es *initializing*, esperar entre 5-10 minutos, repetir la ejecución de la sentencia y observar que el estado del servicio es *running*.

```
ISE PROCESS NAME                       STATE            PROCESS ID
------------------------------------------------------------------
Database Listener                      running          1945
Database Server                        running          73 PROCESSES
Application Server                     initializing

ISE PROCESS NAME                       STATE            PROCESS ID
------------------------------------------------------------------
Database Listener                      running          1945
Database Server                        running          94 PROCESSES
Application Server                     running          2525
```

Ilustración 19. Comprobación del estado de los servicios

93. Importar los certificados de CA para la verificación de los certificados de cliente *EAP-TLS* en el almacén de certificados del producto:

- A través de la barra superior, ir a Administration > System > Certificates.

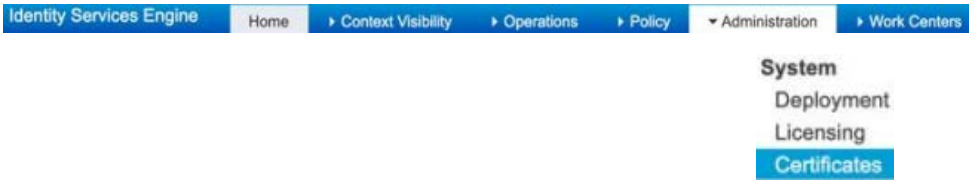

Ilustración 20. Acceso a los ajustes de certificados

- En la barra de navegación situada en el lateral izquierdo, seleccionar *Certificate Management > Trusted Certificates.*

Ilustración 21. Acceso al almacén de certificados confiables

- Hacer *click* en el botón *Import* para añadir el certificado de la CA en formato PEM o DER.

Ilustración 22. Importado del certificado de la CA

- Marcar las siguientes casillas para completar la configuración: *Trust for authentication within ISE* y la opción *Trust for client authentication and syslog*, *Validate Certificate Extensions*. Puede añadir, opcionalmente, un nombre y una descripción. Para finalizar, hacer *click* en el botón *Submit*.

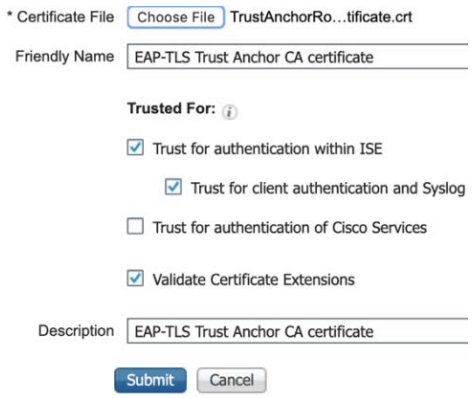

Ilustración 23. Configuración del certificado de la CA

94. Los pasos finales serían instalar los certificados EAP-TLS cliente en los dispositivos 802.1X y su configuración para utilizar el producto como servidor RADIUS. Consultar la documentación del fabricante para más información.

5.10 REGISTROS DE AUDITORÍA

95. El producto genera registros de auditoría conteniendo los siguientes campos: fecha, hora, tipo de evento, identidad del sujeto, dirección IP (opcional), número de puerto (opcional), resultado e información adicional.

5.10.1 BORRADO DE LOS REGISTROS DE AUDITORÍA

96. Un usuario Súper Administrador o Administrador del Sistema puede gestionar y eliminar los registros de auditoría locales a través del menú *Administration > System > Logging > Local Log Settings*. Por ejemplo, puede establecer el periodo de almacenaje de los registros en días y eliminar el registro actual haciendo uso de la opción *Delete Local Logs Now*.

97. Una vez que cumple el periodo de almacenaje de los registros, todos los registros de eventos que excedan esta marca de tiempo se eliminarán.

98. Un administrador privilegiado puede también configurar y eliminar los registros de auditoría de una plataforma externa. Para llevar a cabo esta tarea, seguir el proceso a continuación:

    - Debe autenticarse en el nodo ISE de monitorización encargado de los registros de auditoría.
    - Ejecutar la sentencia *application* configure *ise*.
    - Seleccionar la opción 9 Purgue M&T Operational Data.
    - Introducir el número de días (entre 1 y 90) que desea conservar los registros de auditoría y confirme la selección introduciendo el carácter y.

99. Los registros de auditoría posteriores a la marca de tiempo configurada serán eliminados.

5.11 PROCEDIMIENTOS DE CONFIGURACIÓN OPCIONALES

5.11.1 MODOS DE AUTENTICACIÓN

100. El producto utiliza almacenes de credenciales locales para la autenticación e identificación del administrador. La configuración de recursos externos para la autenticación se trata en el documento *Cisco Identity Services Engine Administrator Guide, Release 2."* [**2**] en la sección *Overview > Cisco ISE Administrators > Force CLI Administrator to Use External Identity Store*. La configuración evaluada solo contempla autenticación local, mediante Directorio Activo o mediante LDAP. Esta última configuración es totalmente opcional, solo se debe configurar en caso de querer usar un Directorio Activo o LDAPS.

5.11.2 CONFIGURACIÓN DEL IDENTIFICADOR DE REFERENCIA PARA LA VALIDACIÓN DE CERTIFICADOS TLS

101. Cuando el producto actúa como cliente TLS con servidores LDAPS, se obtienen los identificadores de referencia del valor configurado por el administrador en el campo LDAP *Identity Source Hostname/IP*. La configuración de este campo se realiza accediendo desde *Administration > Identity Management > External Identity Sources > LDAP > IP/Host Address*.

102. Cuando el producto actúa como cliente para servidores *Syslog* con TLS, se obtienen los identificadores de referencia del valor configurado por el administrador en los campos *Remote Logging Targets IP/Host Address*. La configuración de este campo se realiza accediendo desde *Administration > System > Logging > Remote Logging Targets > IP/Host Address*.

103. El producto soporta los siguientes tipos de identificador:

- Entrada *subjectAltName* del tipo *dNSName* (DNS-ID en el RFC 6125).
- Entrada CN-ID como se define en el RFC 6125 distinguiendo entre mayúsculas y minúsculas (no se permiten *wildcards*).
- Entrada *subjectAltName* del tipo *iPAddress*.

104. El producto no soporta *certificate pinning*.

5.11.3 SINCRONIZACIÓN DE LA CONFIGURACIÓN ENTRE INSTANCIAS DE ISE

105. El producto puede configurarse como un entorno distribuido con múltiples instancias de nodos ISE que comparten registros de auditoría y datos de configuración. En este supuesto, se utiliza TLS por defecto para establecer conexiones seguras con la excepción de las transferencias de los registros de auditoría. Para cambiar esto, seguir las instrucciones de la sección a continuación.

    Nota: para llevar a cabo la configuración del producto en un entorno distribuido, consultar en *Cisco Identity Services Engine Administrator Guide, Release 2.6* [**2**] bajo la sección *Deploy Cisco ISE Nodes -> Set Up Cisco ISE in a Distributed Environment.*

5.11.4 *BANNER* DE INICIO DE SESIÓN

106. El producto puede ser configurado para mostrar banners de inicio de sesión vía CLI y GUI que se mostrarán antes de que se solicite el usuario y la contraseña. Para configurar esta funcionalidad, ir *a Administration > System > Admin Access > Settings > Access Page* y hacer lo siguiente:

    - En el menú izquierdo, hacer doble *click* en *Settings* y repita la operación para *Access*.
    - Bajo la sección GUI *Sessions*, marcar la opción *Pre-login banner*.
    - Rellenar el campo de texto que desea mostrar en el banner con un máximo de 1520 caracteres.
    - Repetir la misma operación para la sección *CLI Sessions*.
    - Finalizar el proceso seleccionando *Save*.

107. El banner de CLI puede configurarse por parte de un Administrador de CLI utilizando los comandos:

    #banner install pre-login <nombre de fichero> repository <nombre del repositorio>

En el comando. *'nombre de fichero'* hace referencia al fichero que contiene el *banner* y '*nombre del repositorio'* hace referencia a la ubicación de dicho fichero.

108. Adicionalmente, puede eliminarse el *banner* ejecutando la siguiente sentencia:

#banner remove pre-login

6. FASE DE OPERACIÓN Y MANTENIMIENTO

6.1 RECOMENDACIONES PARA LA FASE DE OPERACIÓN

109. El correcto funcionamiento del producto requiere de características que deben estar presentes en el entorno. Es la responsabilidad del administrador autorizado asegurar que el entorno operacional cumple con los requisitos enumerados a continuación:

    a) El producto estará instalado y será mantenido en un entorno físico seguro. Esto incluye un edificio seguro con control de acceso o un entorno móvil controlado por el administrador.

    b) El producto no contendrá ninguna aplicación de uso general como compiladores o aplicaciones de usuario.

    c) Los administradores deben asegurar con otras medidas de seguridad complementarias el tráfico que atraviesa el producto, puesto que este no presenta ese tipo de funcionalidad.

    d) Los administradores deben estar correctamente entrenados en el uso y la correcta operación del producto, así como en las características del entorno seguro en que está presente. Al mismo tiempo, los administradores seguirán las guías e indicaciones presentes.

    e) Los administradores se asegurarán de que el producto cuenta con las últimas actualizaciones de *firmware* y *software* para preservar al mismo de amenazas y vulnerabilidades conocidas.

    f) Los administradores mantendrán sus credenciales de acceso al producto seguras y protegidas.

    g) Los administradores deben eliminar toda la información residual sensible que pudiera quedar resultante de operar con el producto después de terminar la vida útil de este.

    h) Los administradores deben asegurar que las peticiones de autenticación se encuentran centralizadas antes de ser transmitidas al producto.

110. Con el fin de prevenir que los administradores escojan contraseñas inseguras, estas deben de cumplir con los siguientes requisitos:

    - Deberán observarse y tenerse en cuenta las recomendaciones expuestas en la guía *CCN-STIC 821, Apéndice V: Normas de Creación y Uso de Contraseñas NP40* [**5**].

- Las contraseñas deben de tener una longitud recomendada de 12 caracteres.
- Deben de estar compuestas por una combinación de caracteres pertenecientes, al menos, a 3 o 4 de los siguientes grupos de caracteres: letras en minúscula, letras en mayúscula, números y los caracteres especiales: *"!", "@", "#", "$", "%", "^", "&", "*", "(", ")"*.
- Cuando se cambia la contraseña, esta tendrá que diferir de la anterior en, al menos, las 5 contraseñas anteriores.
- El cambio de contraseña debe realizarse cada cierto tiempo, máximo de 60 días para los administradores.
- Desde el cambio de contraseña, esta no puede ser cambiada en un mínimo de 4 días.
- Algunas buenas prácticas en la selección de la contraseña, son: evitar palabras de diccionario, secuencias numéricas, secuencias de caracteres seguidos en el teclado, evitar añadir números al final de la palabra o números al final de la contraseña anterior, caracteres repetidos, información personal, etc.

111. Destacar, que la política de contraseñas en términos de longitud y conjuntos de caracteres, así como otras políticas adicionales pueden configurarse en el menú *Administration > System > Admin Access > Authentication*. Esta configuración está reservada para los roles de grupo de Súper Administrador y Administrador del Sistema.

6.2 MONITORIZACIÓN Y MANTENIMIENTO DE LOS REGISTROS DE AUDITORÍA

112. Los administradores deben realizar un correcto seguimiento y mantenimiento de los registros de auditoría, asegurando que no son borrados, modificados ni accedidos por agentes no autorizados. Del mismo modo, procesarán la información que contienen con el fin de agilizar el proceso de respuesta y/o mitigación de potenciales problemas de seguridad.

113. Entre los registros de mayor importancia se encuentran los relacionados con acciones administrativas, cambios de configuración, fallo de las funciones de seguridad y acceso al producto por cualquiera de sus vías.

114. Para consultar los registros de auditoría (con los permisos administrativos pertinentes) a través de CLI, ejecutar la siguiente sentencia:

show logging application <ruta de almacenamiento de los registros/nombre del fichero de registro> tail

115. Para consultar los registros de auditoría como Súper Administrador a través de la GUI, seguir los pasos a continuación:

- Ir al menú *Operations* > *Download Logs*.
- En la barra izquierda, seleccionar el nodo ISE donde se generó el registro de auditoría de interés.
- Seleccionar *Logs* de Depuración.
- Moverse por la ventana principal hasta encontrar el fichero con la extensión "*.log*" de interés que podrá ser descargado y visualizado por un programa externo.

Nota: recordar que el tiempo de vida de los registros de auditoría es configurado a la hora de adecuar y aplicar la política de supervisión del producto.

6.3 COPIA DE SEGURIDAD

116. Se deben realizar copias de seguridad periódicas de forma automatizada y centralizada de la configuración actual del producto y de la información sensible que pueda contener para garantizar, en la medida de lo posible, la respuesta a incidentes de disponibilidad y pérdida de información.

6.4 COMPROBACIÓN DE LA INTEGRIDAD Y ACTUALIZACIONES

117. Se debe comprobar periódicamente la integridad del *hardware* y del *software* que compone el producto con el fin de detectar y/o mitigar posibles problemas de seguridad derivados de la presencia de malware y/o técnicas de *tampering*.

118. Los administradores se encargarán de la actualización regular del *firmware* y el *software* que compone el producto con el fin de solventar los problemas de seguridad presentes y potenciales conocidos. De la misma manera que el propio producto, las actualizaciones serán verificadas y siempre obtenidas por vías aceptadas y reconocidas por el fabricante.

6.5 RECUPERACIONES ANTE FALLOS EN LAS CONEXIONES SEGURAS

119. Existen diversos escenarios en los cuales puede ocurrir un fallo en el establecimiento o mantenimiento de las conexiones seguras con el resto de elementos que interactúan con el producto. A continuación, se detallan estos escenarios:

a) De nodo ISE a nodo ISE solicitando información de auditoría y configuración – la conexión entre ambos nodos ISE será reestablecida automáticamente cuando el servicio vuelva a estar nuevamente disponible. Sin embargo, el administrador debe de comprobar que la configuración de conexión es correcta y no ha sido alterada.

b) De nodo ISE a LDAP (también Directorio Activo) – la conexión entre ambos agentes será reestablecida automáticamente cuando el servicio vuelva a estar nuevamente disponible. Sin embargo, el administrador debe de comprobar que la configuración de conexión es correcta y no ha sido alterada.

c) De nodo ISE a servidor *syslog* – si el campo opcional de la configuración del Punto de Registro Remoto ISE llamado "almacenar mensajes cuando el servidor esté caído", los datos de auditoría no se pierden, sino que son almacenados y transmitidos una vez que se reestablece el canal seguro de comunicaciones. Si esta opción no está activada, es posible perder registros de auditoría en el tiempo en el que el canal seguro de comunicaciones no está operativo.

6.6 GESTIÓN DE LOS MECANISMOS DE CONTROL DE ACCESO

120. En esta sección se describen en detalle los procedimientos para configurar y aplicar políticas de control de acceso por parte del Administrador.

6.6.1 POLÍTICAS DE ACCESO BASADAS EN INTERVALOS DE TIEMPO

121. Para definir condiciones de control de acceso basadas en intervalos de tiempo, se debe seguir el siguiente proceso:

- Ir a *Policy > Policy Elements > Conditions > Common > Time and Date.*
- Hacer click en el botón *Add* para agregar una condición del tipo *Time and Date*.
- Introducir un nombre y una descripción para la nueva condición.
- Bajo la sección *Standard Settings*, definir el intervalo de tiempo y/o las fechas en las que se denegará el acceso. Para hacer esto, se deben seleccionar las opciones *Specific Date Range*, *Specific Date*, *Specific Hours*, *Specific Days* y combinarlas como se desee.
- Opcionalmente, configurar la sección *Exceptions* para añadir excepciones a las normas previamente definidas.

122. A continuación, crear una *Authorization Policy Rule* que aplique las condiciones definidas con anterioridad:

- Ir a Policy > Authorization.
- En la fila *Applicable*, seleccionar dentro del menú desplegable *Edit* la opción *Insert New Row Above* o *Insert New Row Below*.
- Opcionalmente, seleccionar a qué grupos de identidad aplica la regla o deje el valor por defecto *All* para que se aplique a todos los usuarios.
- Bajo la sección *Condition(s)*, hacer click en el icono *+* y seleccionar la opción *Select Existing Condition from Library*.
- En el menú desplegable *Select Condition*, elegir la opción *Time and Date Conditions* y seleccionar las condiciones creadas en el párrafo anterior.
- Para aplicar varias condiciones, utilizar los modificadores de condición *AND* y *OR*.
- Hacer click en el botón *Save* para guardar los cambios.

123. **Nota:** puede concatenar condiciones de diversas categorías para crear políticas de control de acceso complejas en función de las necesidades de la organización. Por ejemplo, puede crear una política que aplique condiciones de restricción de acceso horaria a un determinado grupo de usuarios.

6.6.2 POLÍTICAS DE RESTRICCIÓN DE ACCESO CONCURRENTE

124. Para configurar el número máximo de sesiones por usuario, se debe seguir el siguiente proceso:

- Ir a Administration > System > Settings > Max Sessions.
- Desactivar la opción Unlimited session per user.
- En el campo *Maximum per user Sessions*, elegir el valor máximo de sesiones por usuario permitidas. Por ejemplo, 2.

Nota: para comprobar las sesiones activas de un usuario, ir a *Operations > Radius > Live Sessions.*

125. Para configurar el número máximo de sesiones por grupo, seguir el siguiente proceso:

- Ir a *Administration > System > Settings > Max Sessions > Group.*
- Identificar el grupo objetivo con los datos de la columna *Name* y configure las sesiones del grupo con el valor de la columna *Max Sessions for Group*.

Nota: si un usuario tiene activas las restricciones de sesiones activas por grupo y por usuario, las restricciones por usuario toman precedencia.

126. Para configurar el tiempo de borrado de sesiones activas, seguir el siguiente proceso:

- Ir a *Administration > System > Settings > Max Sessions > Counter Time Limit.*
- Modificar el campo *Deleting sessions after* para especificar el tiempo de vida de las sesiones guardadas en caché.
- Desmarcar la opción *Unlimited – no time limit.*

6.6.3 POLÍTICAS DE ACCESO BASADAS EN RESTRICCIONES DE IPv4 Y MAC

127. Seguir el proceso mostrado a continuación para definir condiciones de control de acceso basadas en direcciones IPv4 y MAC:

- Ir a *Policy > Policy Elements > Conditions > Network Conditions > Endstation Network Connections.*
- Hacer *click* en el botón *Add* y en la lista *IP Addresses* seleccionar las direcciones IPv4 y subredes cuyo acceso desea restringir.
- Bajo la lista *MAC Addresses,* seleccionar las direcciones MAC cuyo acceso desea restringir.

128. A continuación, crear una *Authorization Policy Rule* que aplique las condiciones definidas con anterioridad:

- Ir a *Policy > Authentication.*
- Insertar una nueva fila dentro de *Dot1X* o *MAB*.
- Rellenar la condición y seleccionar *Create New Condition*.
- Seleccionar dentro de *Network Condition* el valor de las condiciones creadas en el párrafo anterior y seleccionar en el campo *Equals* el valor *True*.
- Seleccionar *Internal Users* y elegir la opción *Deny Access*.
- Hacer *click* en el botón *Save* para guardar los cambios.

7. REFERENCIAS

[1] Cisco, *"Cisco Identity Service Engine Installation Guide, Release 2.6"* [En línea]: https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/install_guide/b_ise_InstallationGuide26.html

[2] Cisco, "*Cisco ISE Release 2.6 Administrator Guide*" [En línea]:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ISE_26_admin_guide.html

[3] Cisco, "*Cisco Identity Services Engine CLI Reference Guide, Release 2.6"* [En línea]:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/cli_guide/b_ise_CLIReferenceGuide_26.html

[4] Cisco, "*FIPS Mode on ISE*" [En línea]:

http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200535-FIPS-Mode-on-ISE.html

[5] CCN, "CCN-STIC 821, Apéndice V: Normas de Creación y Uso de Contraseñas NP40", 2018

[6] CCN, "CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad", 2017

[7] CCN, "CCN-STIC 836 Seguridad en VPN", 2017

[8] Cisco, "*Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Site-to-Site"* [En línea]:

https://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-cfg-ikev2-flex.html

[9] Cisco, *"Public Key Infrastucture Configuration Guide, Cisco IOS XE Release 3S"* [E línea]:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-3s/sec-pki-xe-3s-book.pdf.

[10] Cisco, "*Public Key Infrastructure Configuration Guide, Cisco IOS Release 15 MT"* [En línea]:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mt-book/sec-cert-enroll-pki.html

8. ABREVIATURAS

CA	Certificate Authority
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de productos de Seguridad TIC
CRL	*Certificate Revocation List*
DH	*Diffie – Hellman Algorithm*
DHCP	*Dynamic Host Configuratio Protocol*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
ENS	Esquema Nacional de Seguridad
FIPS-CC	*Federal Information Processing Standard – Common Criteria*
FTP	*File Transport Protocol*
ICMP	*Internet Control Message Protocol*
IPsec	*Internet Protocol security*
RSA	*Rivest, Shamir y Adleman Algorithm*
SCP	*Secure Copy Protocol*
SHA	*Secure Hash Algorithm*
SSH	*Secure Shell Protocol*
SSL	*Secure Sockets Layer Protocol*
STIC	Seguridad de Tecnologías de Información y Comunciación
TCP	*Transmission Control Protocol*
TFTP	*Trivial File Transport Protocol*
TLS	*Transport Layer Security*
TLS	*Transport Layer Security Protocol*
UDP	*User Datagram Protocol*
VPN	*Virtual Private Network*

ANEXO A. ROLES DE USUARIO

129. La utilización del rol de usuario Súper Administrador (con acceso a toda la funcionalidad del producto) **debe limitarse** tras el despliegue y la instalación del producto. Se debe tener el configurar el nivel de privilegio mínimo necesario para llevar a cabo las tareas.

130. A continuación, se muestra una lista de la funcionalidad accesible a los usuarios de la interfaz gráfica autenticados:

- Capacidad para aceptar las alarmas y desactivarlas para otros usuarios administrativos (teniendo en cuenta que todo cambio en la configuración queda registrado en el fichero de auditoría pertinente a la configuración).
- Consultar la ventana emergente que indica si el ISE es una copia de evaluación.
- Consultar el *banner* que aparece en la interfaz después de iniciar sesión.
- Consultar el estado de cada uno de los nodos ISE, CPU, memoria y latencia.
- Consultar las alarmas, incluyendo la información relativa a las mismas. Por ejemplo, acceder a los detalles de cambios en la configuración si la alarma está relacionada con este tipo de evento.
- Consultar el número de intentos de autenticación fallidos y exitosos por parte de usuarios finales y dispositivos.
- Consultar el número de dispositivos y usuarios finales con un perfil específico.

131. En esta sección se encuentra la relación de grupos administrativos con el acceso específico a los menús de la interfaz gráfica que poseen:

Nombre del menú	Grupo RBCA	Ítems del menú
Menú del Súper Administrador	Súper Administrador	*Operations > all menu items* *Policy > all menu items* *Administration > all menu items*
Menú del Administrador de Políticas	Administrador de Políticas	*Operations > all menu items* *Policy > all menu items* *Administration > Identity Management > all menu items*

Nombre del menú	Grupo RBCA	Ítems del menú
		System > Settings
Menú del Administrador de Servicio Técnico (Helpdesk)	Administrador de Servicio Técnico (Helpdesk)	*Operations > all menu items*
Menú del Administrador de Identidades	Administrador de Identidades	*Operations > all menu items* *Administration >* *Identity Management > all menu items*
Menú del Administrador de la Red	Administrador de la Red	*Operations > all menu items* *Administration >* *Network Resources > all menu items*
Menú del Administrador del Sistema	Administrador del Sistema	*Operations > Authentication, Alarms, Reports and Troubleshoot* *Administration >* *System > all menu items*
Menú del Administrador RBCA	Administrador RBCA	*Operations > all menu items* *Administration >* *Admin Access > all menu Access*
Menú del Administrador MnT	Administrador MnT	*Operations > all menu items*

Tabla 5. Usuarios

Nota: para obtener detalles adicionales acerca de los comandos disponibles, los roles asociados y los niveles de privilegio en CLI, *consulte Cisco Identity Services Engine Administrator Guide, Release 2.6* [**2**] en el apartado Cisco ISE Administrator Groups.

PUBLICACIONES DE DEFENSA

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