Importación de los Certificados SSL al Profiler del NAC

Contenido

Introducción

El sistema UI basado en web del Profiler puede utilizar los Certificados digitales para poder verificar la autenticidad del servidor Web integrado en el servidor del Cisco NAC Profiler por el navegador mientras que conecta para el acceso a la interfaz de usuario del Profiler servida por el HTTPS. El sistema leverages una de la mayoría de las aplicaciones comunes del PKI y de los Certificados digitales donde el buscador Web valida que un servidor Web SSL es auténtico de modo que el usuario sienta seguro que su interacción con el servidor Web, de hecho, está confiada en y sus comunicaciones con ella segura. Éste es el mismo mecanismo que se utiliza hoy para asegurar el comercio electrónico y otras comunicaciones seguras con los sitios web de muchos tipos que utilicen el SSL.

El sistema del Profiler envía con un certificado digital “uno mismo-firmado” que permita el acceso al UI pero sin la verificación del servidor Web a bordo SSL según lo confiado en. Hasta que el certificado predeterminado se substituya por uno creado con los atributos entorno-específicos, tales como Nombre del servidor, y sea firmado por un Certificate Authority (CA), los buscadores Web que acceden la visualización del Profiler UI una advertencia similar a este ejemplo, que indican que el navegador no reconoce CA que publicó el certificado y no puede lo verifican como sitio confiable.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Servidor del NAC

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Tarea principal: Instale el certificado

La mayoría de los navegadores requieren al usuario proporcionar la entrada adicional para continuar la conexión, que puede ser molesta.

Para utilizar completamente la seguridad mayor permitida por el uso de los Certificados digitales para la Seguridad SSL de la interfaz del Profiler, los cambios a la configuración del subsistema SSL de los NP deben ser realizados. Esos cambios requieren el reemplazo de la clave privada y del certificado digital que son utilizados por el sistema por abandono con ésos publicados por un Certificate Authority de confianza y que son específicos a la instalación. Después de este procedimiento, el navegador inicia a las sesiones HTTP con el servidor y lleva al usuario inmediatamente al proceso de ingreso UI para desviar las advertencias del certificado.

Dos opciones

Hay dos alternativas para esto en los sistemas NP:

1. Utilice al residente del juego de herramientas del OpenSSL en el dispositivo para generar un certificado firmado que se pueda instalar en el sistema del servidor NP y los PC usados para manejar el sistema con la red UI.

Esta opción se puede utilizar en los entornos que no tienen CA interno y eligieron actualmente no confiar en los proveedores comerciales de CA que cargan una tarifa para proporcionar un certificado digital firmado que sea reconocido por la mayoría de los navegadores comerciales automáticamente.

2. Utilice el juego de herramientas del OpenSSL para generar un pedido de firma de certificado para el sistema NP que se somete a un servicio comercial interno o externo de CA, que devuelve un certificado digital listo para utilizar, firmado para el uso en el sistema.

Es típicamente una cuestión de la política de seguridad interna de la organización en la cual el sistema del Profiler está instalado para hacer la determinación cuyo opción para utilizar en un entorno específico. Las Instrucciones detalladas para ambas opciones se proporcionan en el recordatorio de este documento.

Opción 1: Utilice el juego de herramientas del OpenSSL en Beacon/NPS para generar la muestra

Antes de comenzar el procedimiento delineado, es importante verificar que el sistema del Profiler está configurado correctamente para utilizar el servicio de Nombre de Enterprise, y que una entrada DNS está hecha tales que el sistema tiene un Nombre de dominio totalmente calificado (FQDN) (FQDN). Para verificar que éste sea el caso, asegúrese de que usted pueda abrir una sesión UI con el sistema del Profiler con el FQDN del sistema (es decir, https://beacon.bspruce.com/beacon) en vez de la dirección IP (o del VIP en el caso de los sistemas HA) en el URL cuando usted hojea al UI.

Este procedimiento se utiliza en los casos cuando no se desea para someter el CSR a un apagado-dispositivo CA para firmar. Este procedimiento permite la creación de un certificado firmado con el juego de herramientas del OpenSSL en el dispositivo exclusivamente - nada necesita ser sometido a otro sistema o anuncio publicitario CA para generar un certificado firmado para el sistema del Profiler.

El éxito de este procedimiento es dependiente sobre el siguiente de él según lo especificado. La sintaxis de los comandos es errores largos y propensos. Asegúrese de que usted esté en el directorio correcto como se especifica en las instrucciones antes de que usted ejecute los comandos. La información para los DN generados para el certificado de CA y el pedido de firma de certificado, tal como país, estado, ciudad, Nombre del servidor, etc., se debe ingresar idénticamente (con diferenciación entre mayúsculas y minúsculas), así que esté segura de hacer las notas mientras que usted completa los pasos para asegurarse de que va el proceso suavemente.

1. Inicie SSH o a una sesión de consola al dispositivo NP y elévelos al acceso a raíz. Para los sistemas HA, asegúrese de que usted esté en el sistema primario iniciando SSH al VIP.Antes de usar el OpenSSL por primera vez, un poco de estructura de archivo utilizada por el OpenSSL debe ser inicializada. Complete estos pasos para inicializar el OpenSSL:
2. Cambie el directorio a /etc/pki/CA con este comando:

```
cd /etc/pki/CA/
```

Cree un nuevo directorio llamado los **newcerts**, y publique estos comandos:
`mkdir newcerts touch index.txt`

3. El uso VI de crear un nuevo archivo nombró el **serial**; el separador de millares **01** en el archivo, y confía los cambios. (: wq!)Cambie este directorio:/etc/pki/tls/certs cd
4. Genere una nueva clave privada para el sistema con este comando:
   `openssl genrsa -out profilerFQDN.key 1024`
   (donde el "profilerFQDN" se substituye por el Nombre de dominio totalmente calificado (FQDN) del dispositivo NP cuando independiente desplegada. Para los sistemas HA, el FQDN del VIP se debe utilizar).Si el sistema del Profiler no está en el DNS, la dirección IP del servidor (VIP) se puede utilizar en vez del FQDN, pero del certificado se ata a esta dirección IP, que requiere el uso del IP en el URL (es decir, https://10.10.0.1/profiler) para evitar las advertencias del certificado.
5. Genere un certificado de CA para utilizar para generar el certificado de servidor con este comando, que crea los 3 certificados de CA del año, y la clave generada en el paso #4:
   `openssl req -new -x509 -days 1095 -key profilerFQDN.key -out cacert.pem`
   Le indican para varios atributos que se incorporen en el pedido de certificado y la formación de un Nombre distintivo (DN) para el certificado de CA. Para algo de este se sugieren estos elementos, un valor predeterminado (en el []). Ingrese el valor deseado para cada parámetro del DN o "." Para saltar el elemento, esté seguro de anotar los parámetros DN usados en este paso. Deben ser idénticos a ésos especificados en la generación del pedido de firma de certificado para el certificado de servidor en el paso #7.Mueva el certificado de CA creado en el paso más reciente al directorio requerido:
   `mv cacert.pem /etc/pki/CA`
   Genere un pedido de firma de certificado para el sistema del Profiler con la nueva clave privada:
   `openssl req -new -key profilerFQDN.key -out profilerFQDN.csr`
6. Apenas como en el paso #5, a le indican que complete un DN para el sistema para el servidor CSR. Asegúrese de que usted utilice los mismos valores para el servidor CSR que fueron utilizados para el certificado de CA en el paso #5. Si hay algunas variaciones en los parámetros, el CSR no se crea con éxito. Además, a le indican que cree un passphrase para el certificado. Esté seguro de anotar el passphrase.
7. Genere el certificado de servidor con el CSR y la clave privada generados en los pasos anteriores. La salida de este paso es el certificado firmado que está instalado en el servidor del Profiler (o los servidores, en el caso de los pares HA).
   `openssl ca -in profilerFQDN.csr -out profilerFQDN.crt -keyfile profilerFQDN.key`
   A le indican que firme y confíe el certificado. Ingrese **y** para confirmar la firma y confiar del certificado para completar la generación del certificado de servidor.
8. Mueva el archivo de certificado a la ubicación especificada por la política de seguridad interna (si procede) o utilice las ubicaciones predeterminadas:Los Certificados se deben colocar en /etc/pki/tls/certs/ si no se especifica ninguna ubicación por la política de seguridad interna.
   `mv profilerFQDN.crt /etc/pki/tls/certs/profilerFQDN.crt`
9. Mueva el archivo de clave privado a la ubicación especificada por la política de seguridad interna (si procede) o utilice las ubicaciones predeterminadas:La clave privada se debe poner en /etc/pki/tls/private/ si no se especifica ninguna ubicación por la política de seguridad interna. Use el comando:
   `mv profilerFQDN.key /etc/pki/tls/private/profilerFQDN.key`
10. Edite el **archivo ssl.conf** con un editor por ejemplo VI para realizar los cambios necesarios para forzar al servidor Web del Profiler a utilizar la nuevos clave privada y certificado

(ssl.conf se encuentra en /etc/httpd/conf.d/).En **ssl.conf, la** porción del certificado de servidor comienza por la línea 107. Cambie el elemento de configuración de SSLCertificateFile del valor predeterminado de fábrica (/etc/pki/tls/certs/localhost.cert) para señalar al nuevo archivo de certificado que fue creado en el sistema en el paso #8.En **ssl.conf, la** porción de la clave privada del servidor comienza por la línea 114. Cambie el elemento de configuración de la clave privada del servidor del valor predeterminado de fábrica (etc/pki/tls/soldado/localhost.key) para señalar al nuevo archivo de clave privado puesto en el sistema en el paso #9.

11. Recomience servidor Web Apache encendido el dispositivo con este comando:
    ```
    apachectl -k restart
    ```
    Note: Si el sistema es independiente desplegado, salte para caminar #13.
12. Para los sistemas HA NP solamente, complete estos pasos para instalar la clave privada y el CRT en el otro miembro (secundario actual) de los pares HA. El se asegura de que, sin importar las cuales el dispositivo es primario en los pares, los mecanismos de seguridad SSL para el UI actúen idénticamente.a. Copie la clave privada generada en el dispositivo primario en el paso #3 al dispositivo secundario. La clave privada se debe poner en /etc/pki/tls/private/ si no se especifica ninguna ubicación por la política de seguridad interna. Utilice este comando (del directorio de /etc/pki/tls/private en primario):
    ```
    scp profilerFQDN.key root@[secondary IP]:/etc/pki/tls/private/
    ```
    Copie el CRT firmado que fue vuelto de CA del primario al dispositivo secundario. Los Certificados se deben colocar en /etc/pki/tls/certs/ si no se especifica ninguna ubicación por la política de seguridad interna.
    ```
    scp profilerFQDN.crt root@[secondary IP]:/etc/pki/tls/certs
    ```
    SSH al dispositivo secundario y edita su **archivo ssl.conf** con un editor por ejemplo VI para realizar los cambios necesarios para forzar al servidor Web en el secundario a utilizar la nuevos clave privada y certificado (ssl.conf se encuentra en /etc/httpd/conf.d/)En **ssl.conf, la** porción del certificado de servidor comienza por la línea 107. Cambie el elemento de configuración de SSLCertificateFile del valor predeterminado de fábrica (/etc/pki/tls/certs/localhost.cert) para señalar al nuevo archivo de certificado puesto en el sistema en el paso #11b.En **ssl.conf, la** porción de la clave privada del servidor comienza por la línea 114. Cambie el elemento de configuración de la clave privada del servidor del valor predeterminado de fábrica (etc/pki/tls/soldado/localhost.key) para señalar al nuevo archivo de clave privado puesto en el sistema en el paso #11a.Recomience servidor Web Apache encendido el dispositivo secundario con este comando:
    ```
    apachectl -k restart
    ```
    Porque el certificado de servidor que fue creado con estos pasos utilizó CA privado, los navegadores que acceden el Profiler UI tienen que ser configurados para instalar el certificado en el repositorio del Certificate Authority de la Raíz confiable en Windows PC con IE 7.0. Siga estos pasos:Copie el certificado de servidor creado al directorio de /home/beacon del dispositivo:
    ```
    cp profilerFQDN.crt /home/beacon
    ```
    Utilice WinSCP o un software comparable a SCP el archivo .crt del dispositivo al PC.Haga doble clic el **archivo .crt** para comenzar al Certificate Manager de Windows, y el tecleo **instala el certificado**, que comienza al Asisitente de la importación del certificado.Elija el **botón de radio**. Coloque todos los Certificados en este almacén para activar el **botón Browse**.Elija **hojean**, y hacen clic el almacén de certificados de los **Trusted Root Certification Authority**.Haga Click en OK para validar este certificado.Relance este proceso en los otros PC que se utilizan para manejar el sistema del Profiler.
13. Acceda el Profiler UI y observe que las sesiones HTTP comienzan sin las advertencias del

certificado generadas por el navegador.

Opción 2: Genere/someta el CSR a CA interno y externo

Antes de que usted comience el procedimiento delineado después, es importante verificar que el sistema del Profiler está configurado correctamente para utilizar el servicio de Nombre de Enterprise, y que una entrada DNS está hecha tales que el sistema tiene un Nombre de dominio totalmente calificado (FQDN) (FQDN). Para verificar que éste sea el caso, asegúrese de que usted pueda abrir una sesión UI con el sistema del Profiler con el FQDN del sistema (es decir, https://beacon.bspruce.com/beacon) en vez de la dirección IP o del VIP en el caso de los sistemas HA.

Complete estos pasos para generar una nueva clave privada para el sistema, genere un CSR a presentar a CA interno o externo, y después coloque el certificado firmado válido en los NP:

1. Inicie SSH o a una sesión de consola al dispositivo NP, y elévela al acceso a raíz. Para los sistemas HA, inicie SSH al VIP para asegurarse de que usted está en el sistema primario.
2. Vaya al directorio del valor por defecto PKI para los NP:
   `cd /etc/pki/tls`
3. Utilice este comando de generar un nuevo archivo de clave privado para el sistema:
   `openssl genrsa ?des3 ?out profilerFQDN.key 1024`
   Donde el “profilerFQDN” se substituye por el Nombre de dominio totalmente calificado (FQDN) del dispositivo NP cuando independiente desplegada. Para los sistemas HA, el FQDN del VIP se debe utilizar). A le indican que ingrese y confirme un passphrase para completar la generación de la clave privada. Este passphrase se requiere para las operaciones futuras usando la clave privada. Esté seguro de anotar el passphrase usado para la generación de clave privada.
4. Con la clave privada generada en el paso más reciente, genere un pedido de firma de certificado (CSR) que está enviado al Certificate Authority (CA) para la generación del certificado (CRT) para este sistema.

   Utilice este comando de generar el CSR
   `openssl req ?new ?key profilerFQDN.key ?out profilerFQDN.csr`
   (Substituya el Nombre de dominio totalmente calificado (FQDN) del sistema para el “profilerFQDN”.)Le indican para el passphrase para la clave privada cuando usted crea el CSR para el sistema; ingreselo para proceder.Le entonces indican para varios atributos que se incorporen en el pedido de certificado y la formación de un Nombre distintivo (DN). Para algo de este se sugieren estos elementos, un valor predeterminado (en el []). Ingrese el valor deseado para cada parámetro del DN o “.” para saltar el elemento.
5. Verifique el contenido del CSR con este comando:
   `openssl req -noout -text -in profilerFQDN.csr`
   (Substituya el Nombre de dominio totalmente calificado (FQDN) del sistema para el “profilerFQDN”.) Esto devuelve la información sobre el CSR y el DN que fueron ingresados en el paso más reciente. Si alguna información en el CSR necesita ser cambiada, relance el paso #4 en su totalidad
6. Someta el CSR al Certificate Authority (CA) elegido de acuerdo con las directivas internas. Si la petición es acertada, CA devuelve un certificado de identidad que se ha firmado digitalmente con la clave privada de CA. Cuando este nuevo CRT firmado por su CA elegido se utiliza para substituir el valor predeterminado de fábrica CRT en el sistema del Profiler, cualquier navegador que acceda el Profiler UI puede verificar la identidad del sitio, y los

mensajes de advertencia en el navegador considerado sobre la conexión al servidor Web en los NP que el servidor se visualiza no más antes de la autenticación de usuario para mientras el CRT siga siendo válido. (Esto asume que el navegador ha tenido CA agregado a sus autoridades de certificación de la Raíz confiable.)

7. El dependiente sobre CA se utiliza que, de la información adicional las necesidades posiblemente de ser sometido junto con el CSR, tal como otras credenciales o pruebas de la identidad requeridas por el Certificate Authority, y el Certificate Authority pueden entrar en contacto al candidato para más información.Una vez que el CRT firmado digitalmente se vuelve de CA, proceda con el siguiente paso a substituir la clave privada y el certificado de la fábrica por ésos creados en los pasos arriba. Para los sistemas HA, el mismo procedimiento se utiliza para instalar la clave privada y el certificado en el dispositivo secundario en los pares, también.
8. Mueva el certificado y el archivo de clave privado a la ubicación especificada por la política de seguridad interna, si procede, o utilice las ubicaciones predeterminadas:La clave privada se debe poner en /etc/pki/tls/private/ si no se especifica ninguna ubicación por la política de seguridad interna. Utilice este comando:
   ```
   mv profilerFQDN.key /etc/pki/tls/private/profilerFQDN.key
   ```
   Los Certificados se deben colocar en /etc/pki/tls/certs/ si no se especifica ninguna ubicación por la política de seguridad interna.
   ```
   mv profilerFQDN.crt /etc/pki/tls/certs/profilerFQDN.crt
   ```
9. Edite el **archivo ssl.conf** con un editor tal como Vito realizan los cambios necesarios para forzar al servidor Web a utilizar la nuevos clave privada y certificado (ssl.conf se encuentra en /etc/httpd/conf.d/).En **ssl.conf, la** porción del certificado de servidor comienza por la línea 107. Cambie el elemento de configuración de SSLCertificateFile del valor predeterminado de fábrica (/etc/pki/tls/certs/localhost.cert) para señalar al nuevo archivo de certificado puesto en el sistema en el paso #8.b.En **ssl.conf, la** porción de la clave privada del servidor comienza por la línea 114. Cambie el elemento de configuración de la clave privada del servidor del valor predeterminado de fábrica (etc/pki/tls/soldado/localhost.key) para señalar al nuevo archivo de clave privado puesto en el sistema en el paso #8.a.
10. Recomience servidor Web Apache encendido el dispositivo con este comando:
    ```
    apachectl -k restart
    ```
    Note: Si el sistema es independiente desplegado, salte para caminar #12.
11. Para los sistemas HA NP solamente, complete estos pasos para instalar la clave privada y el CRT en el otro miembro (secundario actual) de los pares HA. El se asegura de que, sin importar las cuales el dispositivo es primario en los pares, los mecanismos de seguridad SSL para el UI actúen idénticamente.Copie la clave privada generada en el dispositivo primario en el paso #3 al dispositivo secundario. La clave privada se debe poner en /etc/pki/tls/private/ si no se especifica ninguna ubicación por la política de seguridad interna. Utilice este comando (del directorio de /etc/pki/tls/private en primario):
    ```
    scp profilerFQDN.key root@[secondary IP]:/etc/pki/tls/private/
    ```
    . Copie el CRT firmado vuelto de CA del primario al dispositivo secundario. Los Certificados se deben colocar en /etc/pki/tls/certs/ si no se especifica ninguna ubicación por la política de seguridad interna.
    ```
    scp profilerFQDN.crt root@[secondary IP]:/etc/pki/tls/certs
    ```
    SSH al dispositivo secundario y edita su archivo ssl.conf con un editor por ejemplo VI para realizar los cambios necesarios para forzar al servidor Web en el secundario a utilizar la nuevos clave privada y certificado (ssl.conf se encuentra en /etc/httpd/conf.d/).En **ssl.conf, la** porción del certificado de servidor comienza por la línea 107. Cambie el elemento de configuración de SSLCertificateFile del valor predeterminado de fábrica

(/etc/pki/tls/certs/localhost.cert) para señalar al nuevo archivo de certificado puesto en el sistema en el paso #11.b.En **ssl.conf, la** porción de la clave privada del servidor comienza por la línea 114. Cambie el elemento de configuración de la clave privada del servidor del valor predeterminado de fábrica (etc/pki/tls/soldado/localhost.key) para señalar al nuevo archivo de clave privado puesto en el sistema en el paso #11.a.Recomience servidor Web Apache encendido el dispositivo secundario con este comando:

```
apachectl -k restart
```

12. Acceda el Profiler UI y observe que las sesiones HTTP comienzan sin las advertencias del certificado generadas por el navegador. Si persiste la advertencia, verifique que el navegador usado tenga CA de publicación agregado a sus autoridades de certificación de la Raíz confiable.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Página de productos del Cisco NAC Appliance (Clean Access)
- Soporte Técnico y Documentación - Cisco Systems