Herencia SCEP con el uso del ejemplo de la configuración CLI

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Configurar](#)
[Aliste el ASA](#)
[Configure un túnel para el uso de la inscripción](#)
[Configure un túnel para la autenticación del Certificado de usuario](#)
[Renueve el Certificado de usuario](#)
[Verificación](#)
[Información Relacionada](#)

Introducción

Este documento describe el uso del protocolo simple certificate enrollment de la herencia (SCEP) en el dispositivo de seguridad adaptante de Cisco (ASA).

> Precaución: A partir del 3.0 de la versión de Cisco AnyConnect, este método no debe ser utilizado. Era previamente necesario porque los dispositivos móviles no tenían el cliente 3.x, pero Android y los iPhones ahora tienen soporte para el proxy SCEP, que se deben utilizar en lugar de otro. Solamente en caso de que no se soporta debido al ASA si usted configura la herencia SCEP. Sin embargo, incluso en estos casos, una actualización ASA es la opción recomendada.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de la herencia SCEP.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

El SCEP es un protocolo que se diseña para hacer la distribución y la revocación de los Certificados digitales tan scalable como sea posible. La idea es de que cualquier usuario de la red estándar pueda pedir un certificado digital electrónicamente con la intervención muy pequeña de los administradores de la red. Para los despliegues de VPN que requieren la autenticación certificada con la empresa, el Certificate Authority (CA), o cualquier CA de tercera persona que soporta el SCEP, los usuarios pueden ahora petición los certificados firmados de las máquinas del cliente sin la implicación de los administradores de la red.

> Nota: Si usted desea de configurar el ASA como el servidor de CA, después el SCEP no es el método del protocolo adecuado. Refiera a la sección local de CA del documento de Cisco de los **Certificados digitales que configura** en lugar de otro.

A partir de la versión 8.3 ASA, hay dos métodos aceptados para el SCEP:

- El más viejo método, llamado Legacy SCEP, se discute en este documento.
- Está el más nuevo el método del proxy SCEP de los dos métodos, donde los proxys ASA la petición de la inscripción del certificado en nombre del cliente. Este proceso es más limpio porque no requiere a un grupo de túnel adicional y es también más seguro. Sin embargo, la desventaja es que los trabajos del proxy SCEP solamente con Cisco AnyConnect liberan 3.x. Esto significa que la versión de cliente actual de AnyConnect para los dispositivos móviles no soporta el proxy SCEP.

Configurar

Esta sección proporciona la información que usted puede utilizar para configurar el método del protocolo SCEP de la herencia.

> Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Aquí están algunas NOTAS IMPORTANTES a tener presente cuando se utiliza la herencia SCEP:

- Después de que el cliente reciba el certificado firmado, el ASA debe reconocer CA que firmó el certificado antes de que pueda autenticar al cliente. Por lo tanto, usted debe asegurarse de que el ASA también aliste con el servidor de CA. El proceso de la inscripción para el ASA debe ser el primer paso porque asegura eso:

CA se configura correctamente y puede publicar los Certificados vía el SCEP si usted utiliza el método de la inscripción URL.

El ASA puede comunicar con CA. Por lo tanto, si no puede el cliente, después hay un problema entre el cliente y el ASA.

- Cuando se hace el primer intento de conexión, no habrá un certificado firmado. Debe haber otra opción que se puede utilizar para autenticar al cliente.

- En el proceso de la inscripción del certificado, el ASA no sirve ningún papel. Sirve solamente como el aggregator VPN de modo que el cliente pueda construir un túnel para obtener con seguridad el certificado firmado. Cuando se establece el túnel, el cliente debe poder alcanzar el servidor de CA. Si no, no es poder alistar.

Aliste el ASA

El proceso de la inscripción ASA es relativamente fácil y no requiere ninguna nueva información. Refiera a alistar Cisco ASA a CA usando el documento SCEP para más información sobre cómo alistar el ASA a CA de tercera persona.

Configure un túnel para el uso de la inscripción

Según lo mencionado previamente, para que el cliente pueda obtenga un certificado, un túnel seguro debe ser construido con el ASA con un método distinto de autenticación. Para hacer esto, usted debe configurar a un grupo de túnel que se utilice solamente para el primer intento de conexión cuando se hace un pedido de certificado. Aquí está una foto de la configuración se utiliza que, que define a este grupo de túnel (las líneas importantes se muestran en las ***negrita cursivas***):

```
rtpvpnoutbound6(config)# show run user
username cisco password ffIRPGpDSOJh9YLq encrypted privilege 0

rtpvpnoutbound6# show run group-policy gp_certenroll
group-policy gp_certenroll internal
group-policy gp_certenroll attributes
wins-server none
dns-server value <dns-server-ip-address>

vpn-tunnel-protocol ikev2 ssl-client ssl-clientless
group-lock value certenroll
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value acl_certenroll
default-domain value cisco.com
webvpn
anyconnect profiles value pro-sceplegacy type user

rtpvpnoutbound6# show run access-l acl_certenroll
access-list acl_certenroll remark to allow access to the CA server
access-list acl_certenroll standard permit host <ca-server-ipaddress>

rtpvpnoutbound6# show run all tun certenroll
tunnel-group certenroll type remote-access
tunnel-group certenroll general-attributes
address-pool ap_fw-policy
```

```
authentication-server-group LOCAL
secondary-authentication-server-group none
default-group-policy gp_certenroll
tunnel-group certenroll webvpn-attributes
authentication aaa
 group-alias certenroll enable
```

Aquí está el perfil del cliente que se puede o pegar en un archivo de la libreta e importar al ASA, o puede ser configurado con el Administrador de dispositivos de seguridad adaptante (ASDM) directamente:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">ReconnectAfterResume
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
 <CertificateEnrollment>
 <AutomaticSCEPHost>rtpvpnoutbound6.cisco.com/certenroll</AutomaticSCEPHost>
 <CAURL PromptForChallengePW="false" >scep_url</CAURL>
 <CertificateImportStore>All</CertificateImportStore>
 <CertificateSCEP>
 <Name_CN>%USER%</Name_CN>
 <KeySize>2048</KeySize>
 <DisplayGetCertButton>true</DisplayGetCertButton>
 </CertificateSCEP>
 </CertificateEnrollment>
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false</RetainVpnOnLogoff>
</ClientInitialization>
 <ServerList>
 <HostEntry>
 <HostName>rtpvpnoutbound6.cisco.com</HostName>
 <HostAddress>rtpvpnoutbound6.cisco.com</HostAddress>
 </HostEntry>
 </ServerList>
</AnyConnectProfile>
```

Nota: Un grupo-URL no se configura para este grupo de túnel. Esto es importante porque la herencia SCEP no trabaja con el URL. Usted debe seleccionar al grupo de túnel con su alias. Esto está debido al Id. de bug Cisco CSCtq74054. Si usted experimenta los problemas debido al grupo-URL, usted puede ser que necesite seguir en este bug.

Configure un túnel para la autenticación del Certificado de usuario

Cuando se recibe el certificado firmado ID, la conexión con la autenticación certificada es posible. Sin embargo, no han configurado al grupo de túnel real que se utiliza para conectar todavía. Esta configuración es similar a la configuración para cualquier otro perfil de la conexión. Este término es sinónimo con el grupo de túnel y no ser confundido con el perfil del cliente, que utiliza la autenticación certificada.

Aquí está una foto de la configuración que se utiliza para este túnel:

```
rtpvpnoutbound6(config)# show run access-l acl_fw-policy

access-list acl_fw-policy standard permit 192.168.1.0 255.255.255.0

rtpvpnoutbound6(config)# show run group-p gp_legacyscep
group-policy gp_legacyscep internal
group-policy gp_legacyscep attributes
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value acl_fw-policy
default-domain value cisco.com
webvpn
anyconnect modules value dart

rtpvpnoutbound6(config)# show run tunnel tg_legacyscep
tunnel-group tg_legacyscep type remote-access
tunnel-group tg_legacyscep general-attributes
address-pool ap_fw-policy
 default-group-policy gp_legacyscep
tunnel-group tg_legacyscep webvpn-attributes
 authentication certificate
group-alias legacyscep enable
group-url https://rtpvpnoutbound6.cisco.com/legacyscep enable
```

Renueve el Certificado de usuario

Cuando el Certificado de usuario expira o se revoca, Cisco AnyConnect falla la autenticación certificada. La única opción es volver a conectar al grupo de túnel de la inscripción del certificado para accionar la inscripción SCEP otra vez.

Verificación

Utilice la información que se proporciona en esta sección para confirmar que su configuración trabaja correctamente.

Nota: Puesto que el método de la herencia SCEP se debe implementar solamente con el uso de los dispositivos móviles, los tratos de esta sección solamente con los clientes

móviles.

Complete estos pasos para verificar su configuración:

1. Cuando usted intenta conectar por primera vez, ingrese el nombre de host o el IP Address ASA.

2. Seleccione el **certenroll**, o al grupo alias que usted configuró en la configuración un túnel para la sección del uso de la inscripción de este documento. Le entonces indican para un nombre de usuario y contraseña, y se visualiza el botón del **certificado del conseguir**.

3. Haga clic el botón del **certificado del conseguir**.

Si usted marca sus registros del cliente, esta salida debe visualizar:

```
[06-22-12 11:23:45:121] <Information> - Contacting https://rtpvpnoutbound6.cisco.com.
[06-22-12 11:23:45:324] <Warning> - No valid certificates available for authentication.
[06-22-12 11:23:51:767] <Information> - Establishing VPN session...
[06-22-12 11:23:51:879] <Information> - Establishing VPN session...
[06-22-12 11:23:51:884] <Information> - Establishing VPN - Initiating connection...
[06-22-12 11:23:52:066] <Information> - Establishing VPN - Examining system...
[06-22-12 11:23:52:069] <Information> - Establishing VPN - Activating VPN adapter...
[06-22-12 11:23:52:594] <Information> - Establishing VPN - Configuring system...
[06-22-12 11:23:52:627] <Information> - Establishing VPN...
[06-22-12 11:23:52:734] <Information> - VPN session established to
https://rtpvpnoutbound6.cisco.com.
[06-22-12 11:23:52:764] <Information> - Certificate Enrollment - Initiating, Please Wait.
[06-22-12 11:23:52:771] <Information> - Certificate Enrollment - Request forwarded.
[06-22-12 11:23:55:642] <Information> - Certificate Enrollment - Storing Certificate
[06-22-12 11:24:02:756] <Error> - Certificate Enrollment - Certificate successfully
imported. Please manually associate the certificate with your profile and reconnect.
```

Aunque el mensaje más reciente muestra el **error**, es informar solamente al usuario que este paso es necesario para que ese cliente sea utilizado para el intento de conexión siguiente, que está en el segundo perfil de la conexión que se configura en la configuración un túnel para la sección de la autenticación del Certificado de usuario de este documento.

Información Relacionada

- CSCtq74054 SCEP no se inicia al usar un URL (ASA-IP/el grupo de túnel alias)
- Soporte técnico y documentación