Ejemplo de Configuración de SCEP Heredada con Uso de CLI

Contenido

Introducción

Este documento describe el uso del protocolo SCEP (del inglés Legacy Simple Certificate Enrollment Protocol, protocolo simple de inscripción de certificados heredados) en Cisco Adaptive Security Appliance (ASA).

> **Precaución:** A partir de Cisco AnyConnect versión 3.0, no se debe utilizar este método. Anteriormente era necesario porque los dispositivos móviles no tenían el cliente 3.x, pero tanto Android como iPhones ahora son compatibles con el proxy SCEP, que se debe utilizar en su lugar. Sólo en los casos en que no se admita debido al ASA debe configurar el SCEP heredado. Sin embargo, incluso en estos casos, la opción recomendada es una actualización de ASA.

Prerequisites

Requirements

Cisco recomienda que conozca SCEP heredado.

Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

El SCEP es un protocolo diseñado para hacer que la distribución y revocación de certificados digitales sea lo más escalable posible. La idea es que cualquier usuario de red estándar pueda solicitar un certificado digital electrónicamente con muy poca intervención de los administradores de red. En el caso de implementaciones de VPN que requieren autenticación de certificados con la empresa, la Autoridad de Certificación (CA) o cualquier CA de terceros que admita SCEP, los usuarios ahora pueden solicitar certificados firmados de los equipos cliente sin la participación de los administradores de red.

> **Nota:** Si desea configurar el ASA como servidor de CA, SCEP no es el método de protocolo adecuado. En su lugar, consulte la sección CA local del **documento Configuración de certificados digitales** de Cisco.

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

- El método más antiguo, denominado SCEP heredado, se describe en este documento.
- El método proxy SCEP es el más reciente de los dos métodos, donde ASA envía la solicitud de inscripción de certificados en nombre del cliente. Este proceso es más limpio porque no requiere un grupo de túnel adicional y también es más seguro. Sin embargo, el inconveniente es que el proxy SCEP sólo funciona con Cisco AnyConnect versión 3.x. Esto significa que la versión actual del cliente AnyConnect para dispositivos móviles no admite proxy SCEP.

Configurar

Esta sección proporciona información que puede utilizar para configurar el método de protocolo SCEP heredado.

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

Estas son algunas notas importantes que deben tenerse en cuenta cuando se utiliza Legacy SCEP:

- Después de que el cliente recibe el certificado firmado, el ASA debe reconocer la CA que firmó el certificado antes de poder autenticar al cliente. Por lo tanto, debe asegurarse de que ASA también se inscriba en el servidor de la CA. El proceso de inscripción para el ASA debe ser el primer paso, ya que garantiza que:

La CA está configurada correctamente y puede emitir certificados a través de SCEP si utiliza el método de inscripción de URL.

ASA puede comunicarse con la CA. Por lo tanto, si el cliente no puede, entonces hay un problema entre el cliente y el ASA.

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

- En el proceso de inscripción de certificados, el ASA no cumple ninguna función. Sólo funciona como el agregador VPN para que el cliente pueda construir un túnel para obtener de forma segura el certificado firmado. Cuando se establece el túnel, el cliente debe poder alcanzar el servidor de la CA. De lo contrario, no podrá inscribirse.

Inscriba el ASA

El proceso de inscripción en ASA es relativamente fácil y no requiere ninguna información nueva. Refiérase al documento Registro de Cisco ASA en una CA Usando SCEP para obtener más información sobre cómo inscribir el ASA en una CA de terceros.

Configuración de un Túnel para Uso de Inscripción

Como se mencionó anteriormente, para que el cliente pueda obtener un certificado, se debe construir un túnel seguro con el ASA a través de un método de autenticación diferente. Para hacerlo, debe configurar un grupo de túnel que sólo se utiliza para el primer intento de conexión cuando se realiza una solicitud de certificado. Aquí hay una instantánea de la configuración que se utiliza, que define este grupo de túnel (las líneas importantes se muestran en ***negrita y cursiva***):

```
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
```

```
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
```

Este es el perfil del cliente que se puede pegar en un archivo de Bloc de notas e importarlo al ASA, o se puede configurar directamente con el Administrador adaptable de dispositivos de seguridad (ASDM):

```
<?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>
```

```
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false</RetainVpnOnLogoff>
</ClientInitialization>
```

```
</AnyConnectProfile>
```

> **Nota:** No se ha configurado una url de grupo para este grupo de túnel. Esto es importante porque Legacy SCEP no funciona con la URL. Debe seleccionar el grupo de túnel con su alias. Esto es debido al Id. de bug Cisco CSCtq74054. Si experimenta problemas debido a la url del grupo, es posible que deba realizar un seguimiento de este error.

Configuración de un Túnel para la Autenticación de Certificado de Usuario

Cuando se recibe el certificado de ID firmado, es posible la conexión con la autenticación de certificado. Sin embargo, el grupo de túnel real que se utiliza para conectarse todavía no se ha configurado. Esta configuración es similar a la configuración para cualquier otro perfil de

conexión. Este término es sinónimo de tunnel-group y no debe confundirse con el perfil del cliente, que utiliza la autenticación de certificados.

Esta es una instantánea 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
```

Renovación del certificado de usuario

Cuando el certificado de usuario caduca o se revoca, Cisco AnyConnect falla la autenticación del certificado. La única opción es volver a conectarse al grupo de túnel de inscripción de certificados para activar la inscripción SCEP de nuevo.

Verificación

Utilice la información proporcionada en esta sección para confirmar que su configuración funciona correctamente.

> **Nota:** Dado que el método SCEP heredado solo se debe implementar con el uso de dispositivos móviles, esta sección solo se ocupa de los clientes móviles.

Complete estos pasos para verificar su configuración:

1. Cuando intente conectarse por primera vez, introduzca el nombre de host o la dirección IP de ASA.

2. Seleccione **certenroll** o el alias de grupo que configuró en la sección Configure un Túnel para Uso de Inscripción de este documento. A continuación, se le solicitará un nombre de usuario y una contraseña, y se muestra el botón **obtener certificado**.

3. Haga clic en el botón **Obtener certificado**.

Si marca los registros de su cliente, se mostrará este resultado:

```
[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]



[06-22-12 11:23:52:764]



[06-22-12 11:23:52:771]



[06-22-12 11:23:55:642]



[06-22-12 11:24:02:756]
```

Aunque el último mensaje muestra **error**, es solamente para informar al usuario que este paso es necesario para que ese cliente sea usado para el siguiente intento de conexión, que está en el segundo perfil de conexión que está configurado en la sección Configurar un Túnel para Autenticación de Certificado de Usuario de este documento.

Información Relacionada

- CSCtq74054 SCEP no se inicia cuando se utiliza una URL (asa-IP/tunnel-group alias)
- Asistencia técnica y documentación