SCEP legado com o uso do exemplo de configuração da CLI

Contents

Introduction

Este documento descreve o uso do SCEP (Simple Certificate Enrollment Protocol) legado no Cisco Adaptive Security Appliance (ASA).

> **Caution**: A partir do Cisco AnyConnect versão 3.0, esse método não deve ser usado. Antes era necessário porque os dispositivos móveis não tinham o cliente 3.x, mas tanto o Android quanto os iPhones agora têm suporte para proxy SCEP, que deve ser usado. Somente nos casos em que não há suporte devido ao ASA, você deve configurar o SCEP legado. No entanto, mesmo nesses casos, uma atualização do ASA é a opção recomendada.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do SCEP legado.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Informações de Apoio

O SCEP é um protocolo projetado para tornar a distribuição e a revogação de certificados digitais o mais escalável possível. A ideia é que qualquer usuário de rede padrão possa solicitar um certificado digital eletronicamente com pouca intervenção dos administradores de rede. Para implantações de VPN que exigem autenticação de certificado com a empresa, Autoridade de Certificação (CA) ou qualquer CA de terceiros que ofereça suporte ao SCEP, os usuários agora podem solicitar certificados assinados das máquinas cliente sem o envolvimento dos administradores de rede.

> **Note**: Se você deseja configurar o ASA como o servidor CA, o SCEP não é o método de protocolo apropriado. Consulte a seção CA local do documento **Configuring Digital Certificates** Cisco.

A partir do ASA versão 8.3, há dois métodos suportados para o SCEP:

- O método mais antigo, chamado de SCEP legado, é discutido neste documento.
- O método de proxy SCEP é o mais novo dos dois métodos, em que o ASA faz o proxy da solicitação de inscrição de certificado em nome do cliente. Esse processo é mais limpo porque não requer um grupo de túnel extra e também é mais seguro. No entanto, a desvantagem é que o proxy SCEP só funciona com o Cisco AnyConnect versão 3.x. Isso significa que a versão atual do cliente AnyConnect para dispositivos móveis não suporta proxy SCEP.

Configurar

Esta seção fornece informações que você pode usar para configurar o método do protocolo SCEP legado.

> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Aqui estão algumas notas importantes a serem lembradas quando o SCEP legado é usado:

- Depois que o cliente recebe o certificado assinado, o ASA deve reconhecer a CA que assinou o certificado antes de poder autenticar o cliente. Portanto, você deve garantir que o ASA também se inscreva no servidor CA. O processo de inscrição do ASA deve ser a primeira etapa, pois garante que:

  A CA está configurada corretamente e pode emitir certificados através do SCEP se você usar o método de inscrição de URL.

O ASA pode se comunicar com a CA. Portanto, se o cliente não puder, há um problema entre o cliente e o ASA.

- Quando a primeira tentativa de conexão for feita, não haverá um certificado assinado. Deve haver outra opção que possa ser usada para autenticar o cliente.

- No processo de inscrição de certificado, o ASA não tem nenhuma função. Ele serve apenas como o agregador de VPN para que o cliente possa criar um túnel para obter com segurança o certificado assinado. Quando o túnel é estabelecido, o cliente deve conseguir acessar o servidor CA. Caso contrário, ele não poderá se inscrever.

Inscreva o ASA

O processo de inscrição no ASA é relativamente fácil e não exige nenhuma informação nova. Consulte o documento Como inscrever o Cisco ASA em uma CA usando o SCEP para obter mais informações sobre como inscrever o ASA em uma CA de terceiros.

Configurar um túnel para uso da inscrição

Como mencionado anteriormente, para que o cliente possa obter um certificado, um túnel seguro deve ser criado com o ASA por meio de um método diferente de autenticação. Para fazer isso, você deve configurar um grupo de túneis que é usado somente para a primeira tentativa de conexão quando uma solicitação de certificado é feita. Aqui está um instantâneo da configuração usada, que define este grupo de túneis (as linhas importantes são mostradas em ***negrito-itálico***):

```
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
```

Aqui está o perfil do cliente que pode ser colado em um arquivo do Bloco de Notas e importado para o ASA ou pode ser configurado diretamente com o Adaptive Security Device Manager (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>
```

> **Note**: Um group-url não está configurado para este grupo de túneis. Isso é importante porque o SCEP legado não funciona com o URL. Você deve selecionar o grupo de túneis com seu alias. Isso ocorre devido à ID de bug da Cisco CSCtq74054. Se você tiver problemas devido ao group-url, talvez seja necessário dar seguimento a esse bug.

Configurar um túnel para a autenticação do certificado do usuário

Quando o certificado de ID assinado é recebido, a conexão com a autenticação do certificado é possível. No entanto, o grupo de túneis real que é usado para conectar ainda não foi configurado. Essa configuração é semelhante à configuração para qualquer outro perfil de conexão. Esse termo é sinônimo de tunnel-group e não deve ser confundido com o perfil do cliente, que usa autenticação de certificado.

Aqui está um instantâneo da configuração usada 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
```

Renove o certificado do usuário

Quando o certificado do usuário expira ou é revogado, o Cisco AnyConnect falha na autenticação do certificado. A única opção é reconectar ao grupo de túneis de inscrição de certificado para disparar a inscrição do SCEP novamente.

Verificar

Use as informações fornecidas nesta seção para confirmar se sua configuração funciona corretamente.

> **Note**: Como o método SCEP legado deve ser implementado somente com o uso de dispositivos móveis, esta seção trata somente de clientes móveis.

Conclua estes passos para verificar sua configuração:

1. Ao tentar se conectar pela primeira vez, insira o nome do host ASA ou o endereço IP.
2. Selecione **certenroll** ou o alias de grupo que você configurou na seção Configurar um túnel para uso de inscrição deste documento. Em seguida, é solicitado um nome de usuário e uma senha, e o botão **obter certificado** é exibido.
3. Clique no botão **obter certificado**.

Se você verificar os logs do cliente, essa saída deverá exibir:

```
[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]
```

Embora a última mensagem mostre **erro**, é somente para informar ao usuário que essa etapa é necessária para que esse cliente seja usado na próxima tentativa de conexão, que está no segundo perfil de conexão configurado na seção Configurar um túnel para autenticação de certificado do usuário deste documento.

Informações Relacionadas

- O CSCtq74054 SCEP não é iniciado ao usar um URL (asa-IP/tunnel-group alias)
- Suporte técnico e documentação