Legado SCEP com o uso do exemplo da configuração de CLI

Índice

Introdução

Este documento descreve o uso do protocolo simple certificate enrollment do legado (SCEP) na ferramenta de segurança adaptável de Cisco (ASA).

> Cuidado: Até à data do 3.0 da liberação de Cisco AnyConnect, este método não deve ser usado. Era previamente necessário porque os dispositivos móveis não tiveram o cliente 3.x, mas Android e os iPhones têm agora o apoio para o proxy SCEP, que devem ser usados pelo contrário. Somente nos casos onde não se apoia devido ao ASA deve você configurar o legado SCEP. Contudo, mesmo nesses casos, uma elevação ASA é a opção recomendada.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do legado SCEP.

Componentes Utilizados

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

O SCEP é um protocolo que seja projetado a fim fazer a distribuição e a revogação dos Certificados digitais tão escaláveis como possível. A ideia é que todo o usuário da rede padrão deve poder pedir eletronicamente um certificado digital com intervenção muito pequena dos administradores de rede. Para as distribuições VPN que exigem o certificado de autenticação com a empresa, o Certificate Authority (CA), ou todo o CA da terceira que apoia o SCEP, os usuários podem agora pedir para certificados assinados das máquinas cliente sem a participação dos administradores de rede.

> Nota: Se você deseja configurar o ASA como o server de CA, a seguir o SCEP não é o método do protocolo apropriado. Refira a seção local de CA do documento Cisco **configurando dos Certificados digitais** pelo contrário.

Até à data do ASA libere 8.3, lá são dois métodos suportados para o SCEP:

- O método mais velho, chamado Legado SCEP, é discutido neste documento.
- O método do proxy SCEP é o mais novo dos dois métodos, onde os proxys ASA o pedido do certificado de registro em nome do cliente. Este processo está mais limpo porque não exige um grupo de túneis extra e é igualmente mais seguro. Contudo, o inconveniente é que os trabalhos do proxy SCEP somente com Cisco AnyConnect liberam 3.x. Isto significa que a versão de cliente atual de AnyConnect para dispositivos móveis não apoia o proxy SCEP.

Configurar

Esta seção fornece a informação que você pode usar a fim configurar o método do protocolo scep do legado.

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

Estão aqui algumas observações importantes a manter-se na mente quando o legado SCEP é usado:

- Depois que o cliente recebe o certificado assinado, o ASA deve reconhecer CA que assinou o certificado antes que possa autenticar o cliente. Consequentemente, você deve assegurar-se de que o ASA igualmente se registre com o server de CA. O processo do registro para o ASA deve ser a primeira etapa porque assegura aquele:

CA está configurado corretamente e pode emitir Certificados através do SCEP se você usa o método do registro URL.

O ASA pode comunicar-se com CA. Consequentemente, se o cliente não pode, a seguir há uma edição entre o cliente e o ASA.

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

- No processo do certificado de registro, o ASA não serve nenhum papel. Serve somente como o agregador VPN de modo que o cliente possa construir um túnel a fim obter firmemente o certificado assinado. Quando o túnel é estabelecido, o cliente deve poder alcançar o server de CA. Se não, não é poder registrar-se.

Registre o ASA

O processo do registro ASA é relativamente fácil e não exige nenhuma informação nova. Refira registrar Cisco ASA a CA usando o documento SCEP para obter mais informações sobre de como registrar o ASA a CA da terceira.

Configurar um túnel para o uso do registro

Como mencionado previamente, para que o cliente possa obtenha um certificado, um túnel seguro deve ser construído com o ASA com um método diferente da autenticação. A fim fazer isto, você deve configurar um grupo de túneis que está usado somente para a primeira tentativa de conexão quando um pedido do certificado é feito. Está aqui um instantâneo da configuração que é usada, que define este grupo de túneis (as linhas importantes são mostradas nos ***itálicos e negrito***):

```
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
```

Está aqui o perfil do cliente que pode ou ser colado em um arquivo do bloco de notas e ser importado ao ASA, ou pode ser configurado com o Security Device Manager adaptável (ASDM) diretamente:

```
<?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: Uma grupo-URL não é configurada para este grupo de túneis. Isto é importante porque o legado SCEP não trabalha com a URL. Você deve selecionar o grupo de túneis com seu aliás. Isto é devido à identificação de bug Cisco CSCtq74054. Se você experimenta edições devido à grupo-URL, você pôde precisar de continuar neste erro.

Configurar um túnel para a autenticação do certificado de usuário

Quando o certificado assinado ID é recebido, a conexão com o certificado de autenticação é possível. Contudo, o grupo de túneis real que é usado a fim conectar não foi configurado ainda. Esta configuração é similar à configuração para todo o outro perfil de conexão. Este termo é sinônimo com grupo de túneis e para não ser confundido com o perfil do cliente, que usa o certificado de autenticação.

Está aqui um instantâneo da configuração que é 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 de usuário

Quando o certificado de usuário expira ou é revogado, Cisco AnyConnect falha o certificado de autenticação. A única opção é reconectar ao grupo de túneis do certificado de registro a fim provocar outra vez o registro SCEP.

Verificar

Use a informação que é fornecida nesta seção a fim confirmar que sua configuração trabalha corretamente.

Nota: Desde que o método do legado SCEP deve somente ser executado com o uso dos dispositivos móveis, negócios desta seção somente com clientes móveis.

Termine estas etapas a fim verificar sua configuração:

1. Quando você tenta conectar pela primeira vez, incorpore o hostname ou o endereço IP de Um ou Mais Servidores Cisco ICM NT ASA.

2. Selecione o **certenroll**, ou o grupo aliás que você configurou configurar um túnel para a seção do uso do registro deste documento. Você é alertado então para um nome de usuário e senha, e o botão do **certificado da obtenção** é indicado.

3. Clique o botão do **certificado da obtenção**.

Se você verifica seus logs do cliente, esta saída deve indicar:

```
[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.
```

Mesmo que a última mensagem mostre o **erro**, é informar somente o usuário que esta etapa é necessária para que esse cliente esteja usado para a tentativa de conexão seguinte, que está no segundo perfil de conexão que é configurado configurar um túnel para a seção da autenticação do certificado de usuário deste documento.

Informações Relacionadas

- CSCtq74054 SCEP não é iniciado ao usar uma URL (ASA-IP/grupo de túneis aliás)
- Suporte técnico & documentação