ASA 8.X: Exemplo de configuração do registro SCEP de AnyConnect

Índice

Introdução

A funcionalidade do registro SCEP foi introduzida no cliente independente 2.4 do AnyConnect. Neste processo, você altera o perfil de AnyConnect XML para incluir uma configuração SCEP-relacionada e para criar uma política e um perfil de conexão específicos do grupo para o certificado de registro. Quando um usuário de AnyConnect conecta a este grupo específico, AnyConnect envia um pedido do certificado de registro ao server de CA, e o server de CA automaticamente aceita ou nega o pedido.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Dispositivos de segurança adaptáveis Cisco ASA série 5500 essa versão de software 8.x da corrida
- Versão de VPN 2.4 de Cisco AnyConnect

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.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

O objetivo do registro SCEP automático para AnyConnect é emitir um certificado ao cliente em uma maneira segura e escalável. Por exemplo, os usuários não precisam de pedir um certificado de um server de CA. Esta funcionalidade é integrada no cliente de AnyConnect. Os Certificados são emitidos aos clientes baseados nos parâmetros do certificado mencionados no arquivo de perfil XML.

Vista geral das mudanças exigidas

A característica do registro SCEP de AnyConnect exige determinados parâmetros do certificado ser definida no perfil XML. Uma política e um perfil de conexão do grupo são criados no ASA para o certificado de registro, e o perfil XML é associado com essa política. O cliente de AnyConnect conecta ao perfil de conexão que usa esta política específica e envia um pedido para um certificado com os parâmetros que são definidos no arquivo XML. O Certificate Authority (CA) automaticamente aceita ou nega o pedido. O cliente de AnyConnect recupera Certificados com o protocolo scep se o elemento do <CertificateSCEP> é definido em um perfil do cliente.

A autenticação do certificado de cliente deve falhar antes que as tentativas de AnyConnect para recuperar automaticamente os Certificados novos, assim que se você já tenham um certificado válido instalado, o registro não ocorre.

Quando os usuários entram ao grupo específico, estão registrados automaticamente. Há igualmente um método manual disponível para a recuperação de certificado em que os usuários são presentado com um botão do **certificado da obtenção**. Isto trabalha somente quando o cliente tem de acesso direto ao server de CA, não através do túnel.

Refira o guia do administrador do Cisco AnyConnect VPN Client, libere 2.4 para mais informação.

Ajustes XML para permitir a característica de Anyconnect SCEP

Estes são os elementos importantes que precisam de ser definidos no arquivo de AnyConnect XML. Refira o guia do administrador do Cisco AnyConnect VPN Client, libere 2.4 para mais informação.

- <AutomaticSCEPHost> — Especifica o nome de host ASA e o perfil de conexão (grupo de túneis) para que a recuperação de certificado SCEP é configurada. O valor precisa de estar no formato do nome de domínio totalmente qualificado do nome ASA \ perfil de conexão ou do endereço IP de Um ou Mais Servidores Cisco ICM NT do nome ASA \ perfil de conexão.

- <CAURL> — Identifica o server SCEP CA.
- <CertificateSCEP> — Define como os índices do certificado são pedidos.
- <DisplayGetCertButton> — Determina se o AnyConnect GUI indica o botão do certificado da obtenção. Permite usuários de pedir manualmente a renovação ou o abastecimento do certificado.

Está aqui um perfil do exemplo:

```
<?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">true</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AutoConnectOnStart UserControllable="true">true</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">
     ReconnectAfterResume
   </AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">
    Automatic
  </RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Automatic
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<CertificateEnrollment>
<AutomaticSCEPHost>asa2.cisco.com/certenroll</AutomaticSCEPHost>
<CAURL PromptForChallengePW="false">
     http://10.11.11.1/certsrv/mscep/mscep.dll
   </CAURL>
<CertificateSCEP>
<Name_CN>cisco</Name_CN>
<Company_O>Cisco</Company_O>
<DisplayGetCertButton>true</DisplayGetCertButton>
</CertificateSCEP>
</CertificateEnrollment>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>asa2.cisco.com</HostName>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

Configurar o ASA para apoiar o protocolo scep para AnyConnect

A fim fornecer o acesso a um registration authority (RA autoridade de registro) privado, o administrador ASA deve criar um pseudônimo que tenha um ACL que restrinja a conectividade de

rede lateral privada ao RA desejado. A fim recuperar automaticamente um certificado, os usuários conectam e autenticam ao este aliás.

Conclua estes passos:

1. Crie um pseudônimo no ASA para apontar ao grupo configurado específico.
2. Especifique o pseudônimo no elemento do <AutomaticSCEPHost> no perfil do cliente do usuário.
3. Anexe o perfil do cliente que contém a seção do <CertificateEnrollment> ao grupo configurado específico.
4. Ajuste um ACL para que o grupo configurado específico restrinja o tráfego ao lado privado RA.

Conclua estes passos:

1. Transfira arquivos pela rede o perfil XML ao ASA.Escolha o **acesso do acesso remoto VPN > da rede (cliente) > avançou > SSL VPN > ajustes do cliente**.Sob perfis do cliente VPN SSL, o clique **adiciona**.O clique **consulta arquivos locais** a fim selecionar o arquivo de perfil, e o clique **consulta o flash** a fim especificar o nome de arquivo instantâneo.**Arquivo da transferência de arquivo pela rede do** clique.
2. Estabelecer uma política do grupo do **certenroll** para o certificado de registro.Escolha o **acesso do acesso remoto VPN > de cliente de rede > a política do grupo**, e o clique **adiciona**.Adicionar um túnel em divisão para o server de CA.Expanda **avançado**, e selecione então o **Split Tunneling**.Escolha a **lista da rede de túnel abaixo do** menu da política, e o clique **controla** a fim adicionar o Access Control List.Selecione o **cliente VPN SSL**, e escolha o perfil para o certenroll do **perfil do cliente transferir o** menu.
3. Crie um outro grupo chamado **certauth** para o certificado de autenticação.
4. Crie um perfil de conexão do certenroll.Escolha o **acesso do acesso remoto VPN > de cliente de rede > os perfis de conexão de AnyConnect**, e o clique **adiciona**.Incorpore o grupo do **certenroll ao** campo dos pseudônimos.**Nota:** O nome de pseudônimo deve combinar o valor usado no perfil de AnyConnect sob AutomaticSCEPHost.
5. Faça um outro perfil de conexão chamado **certauth** com certificado de autenticação. Este é o perfil de conexão real que é usado após o registro.
6. A fim certificar-se do uso do pseudônimo é permitida, verificação **permite que o usuário selecione o perfil de conexão, identificado por seu pseudônimo, na página de login. Se não, DefaultWebVPNGroup é o perfil de conexão.**

Teste AnyConnect SCEP

Use esta seção para confirmar se a sua configuração funciona corretamente.

1. Lance o cliente de AnyConnect, e conecte-o ao perfil do certenroll.AnyConnect passa o pedido do registro ao server de CA com o SCEP.AnyConnect passa o pedido do registro diretamente e não atravessa o túnel, se o botão do **certificado da obtenção** é usado.
2. Este aviso aparece. Clique **sim** para instalar o usuário e o certificado de raiz do uso
3. Uma vez que o certificado é registrado, conecte ao perfil do **certauth**.

Certificate o armazenamento em Microsoft Windows depois que

pedido SCEP

Conclua estes passos:

1. Clique o **Iniciar > Executar > o mmc**.
2. O clique **adiciona/remove a pressão dentro**.
3. Clique **adicionam**, e escolhem **Certificados**.
4. Adicionar **meus** Certificados da **conta de usuário** e da **conta do computador**.Esta imagem mostra o certificado de usuário instalado na loja do certificado de Windows:Esta imagem mostra o certificado de CA instalado na loja do certificado de Windows:

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

- Trabalhos do registro SCEP de AnyConnect somente quando o certificado de autenticação falhar. Se não se está registrando, verifique a loja do certificado. Se os Certificados são instalados já, suprima d e teste-os outra vez.
- O registro SCEP não trabalha a menos que o comando da **porta de saída 443 da relação do certificado de autenticação SSL** for usado.Refira estes ao Bug da Cisco ID para mais informação:Identificação de bug Cisco CSCtf06778 (clientes registrados somente) — AnyConnect SCEP registra-se não trabalha com pelo AUTH 2 CERT do grupoIdentificação de bug Cisco CSCtf06844 (clientes registrados somente) — Registro SCEP de AnyConnect que não trabalha com o ASA pelo AUTH CERT do grupo
- Se o server de CA está na parte externa do ASA, certifique-se permitir o Hair-Pinning com o **comando intra-interface da licença do same-security-traffic**. Igualmente adicionar a parte externa e os comandos access-list nat segundo as indicações deste exemplo:`nat (outside) 1 access-list natoutside extended permit ip 172.16.1.0 255.255.255.0 host 171.69.89.87`Onde 172.16.1.0 está o pool e 171.69.89.87 de AnyConnect são o endereço IP do servidor de CA.
- Se o server de CA está no interior, certifique-se inclui-lo na lista de acessos do túnel em divisão para a política do grupo do **certenroll**. Neste documento, supõe-se que o server de CA está no interior.
```
group-policy certenroll attributes
split-tunnel-policy tunnelspecified
 split-tunnel-network-list value scep

access-list scep standard permit 171.69.89.0 255.255.255.0
```

Informações Relacionadas

- Guia do administrador do Cisco AnyConnect VPN Client, liberação 2.4
- Suporte Técnico e Documentação - Cisco Systems