Configurar o telefone de AnyConnect VPN com certificado de autenticação em um ASA

Índice

Introdução

Este documento fornece uma configuração de exemplo que mostra como configurar a ferramenta de segurança adaptável (ASA) e dispositivos do CallManager para fornecer o certificado de autenticação para os clientes de AnyConnect que são executado em Telefones IP de Cisco. Depois que esta configuração está completa, os Telefones IP de Cisco podem estabelecer as conexões de VPN ao ASA que utilizam Certificados a fim fixar a comunicação.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Licença superior de AnyConnect SSL
- AnyConnect para a licença do telefone de Cisco VPN

Dependente em cima da versão ASA, você verá “AnyConnect para o telefone de Linksys” para a liberação 8.0.x ASA ou “AnyConnect para o telefone de Cisco VPN” para a liberação 8.2.x ASA ou mais tarde.

Componentes Utilizados

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

- ASA - Liberação 8.0(4) ou mais atrasado
- Modelos do telefone IP - 7942/7962/7945/7965/7975
- Telefones - 8961/9951/9971 com firmware da liberação 9.1(1)
- Telefone - Liberação 9.0(2)SR1S - Skinny Call Control Protocol (SCCP) ou mais tarde
- Gerente das comunicações unificadas de Cisco (CUCM) - Liberação 8.0.1.100000-4 ou mais atrasado

As liberações usadas neste exemplo de configuração incluem:

- ASA - Liberação 9.1(1)
- Versão do CallManager 8.5.1.10000-26

Para uma lista completa de telefones apoiados em sua versão CUCM, termine estas etapas:

1. Abra esta URL: *IP de servidor Address>:8443/cucreports/systemReports.do de* https:// *<CUCM*
2. Escolha a **lista unificada dos recursos de telefone CM > gerenciem um relatório > uma característica novos: Virtual Private Network**.

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.

Telefone a tipos do certificado

Cisco usa que estes o certificado datilografa dentro telefones:

- Certificado instalado fabricante (MIC) - Os MIC são incluídos em todos os 7941, 7961, e Telefones IP de Cisco de um modelo mais novo. Os MIC são os Certificados 2048-bit chaves que são assinados pelo Certificate Authority (CA) de Cisco. Quando um MIC esta presente, não é necessário instalar localmente o certificado significativo a - (LSC). Para que o CUCM confie o certificado MIC, utiliza os certificados de CA instalados CAP-RTP-001, CAP-RTP-002, e Cisco_Manufacturing_CA em sua loja da confiança do certificado.
- LSC - O LSC fixa a conexão entre CUCM e o telefone depois que você configura o modo da segurança do dispositivo para a autenticação ou a criptografia.O LSC possui a chave pública para o Cisco IP Phone, que é assinada pela chave privada da função do proxy do Certificate Authority CUCM (CAPF). Este é o método preferido (ao contrário do uso dos MIC) porque somente os Telefones IP de Cisco que é manualmente fornecida por um administrador são permitidos transferir e verificar o arquivo CTL.**Note**: Devido ao risco de segurança aumentada, Cisco recomenda o uso dos MIC unicamente para a instalação LSC e não para o uso continuado. Os clientes que configuram Telefones IP de Cisco para usar MIC para a

autenticação do Transport Layer Security (TLS) ou para toda a outra finalidade fazem tão por sua conta e risco.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

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

Configurações

Este documento descreve estas configurações:

- Configuração ASA
- Configuração do CallManager
- Configuração de VPN no CallManager
- Instalação certificada em Telefones IP

Configuração ASA

A configuração do ASA é quase a mesma que quando você conecta um computador de cliente de AnyConnect ao ASA. Contudo, estas limitações aplicam-se:

- O grupo de túneis deve ter uma grupo-URL. Esta URL será configurada no CM sob o gateway de VPN URL.
- A política do grupo não deve conter um túnel em divisão.

Esta configuração usa um certificado previamente configurado e instalado ASA (auto-assinado ou terceira parte) no ponto confiável do Secure Socket Layer (SSL) do dispositivo ASA. Para mais informação, refira estes documentos:

- Configurando Certificados digitais
- O ASA 8.x instala manualmente Certificados do vendedor da 3ª parte para o uso com exemplo de configuração WebVPN
- ASA 8.x: O VPN alcança com o cliente VPN de AnyConnect que usa o exemplo de configuração do certificado auto-assinado

A configuração relevante do ASA é:

```
ip local pool SSL_Pool 10.10.10.1-10.10.10.254 mask 255.255.255.0
group-policy GroupPolicy_SSL internal
group-policy GroupPolicy_SSL attributes
split-tunnel-policy tunnelall
vpn-tunnel-protocol ssl-client

tunnel-group SSL type remote-access
tunnel-group SSL general-attributes
address-pool SSL_Pool
default-group-policy GroupPolicy_SSL
tunnel-group SSL webvpn-attributes
```

```
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable

webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.0.3054-k9.pkg
anyconnect enable

ssl trust-point SSL outside
```

Configuração do CallManager

A fim exportar o certificado do ASA e importar o certificado no CallManager como um certificado da Telefone-VPN-confiança, termine estas etapas:

1. Registrar o certificado gerado com CUCM.
2. Verifique o certificado usado para o SSL.
   ```
   ASA(config)#show run ssl
   ssl trust-point SSL outside
   ```
3. Exporte o certificado.
   ```
   ASA(config)#crypto ca export SSL identity-certificate
   ```
   O certificado de identidade codificado do Privacy Enhanced Mail (PEM) segue:
   ```
   ASA(config)#crypto ca export SSL identity-certificate
   ```
4. Copie o texto do terminal e salvar o como um arquivo do .pem.
5. Entre ao CallManager e escolha o **> gerenciamento de certificado do > segurança da administração do OS > o certificado unificados da transferência de arquivo pela rede > Telefone-VPN-confiança seleta** a fim transferir arquivos pela rede o arquivo certificado salvar na etapa precedente.

Configuração de VPN no CallManager

1. Navegue a Cisco unificou a administração CM.
2. Da barra de menus, escolha **recursos avançados > VPN > gateway de VPN**.
3. Na janela de configuração do gateway de VPN, termine estas etapas:No campo de nome do gateway de VPN, dê entrada com um nome. Este pode ser todo o nome.No campo de descrição do gateway de VPN, incorpore uma descrição (opcional).No campo URL do gateway de VPN, incorpore a grupo-URL definido no ASA.Nos Certificados VPN neste campo do lugar, selecione o certificado que foi transferido arquivos pela rede ao CallManager previamente para o mover do truststore para este lugar.
4. Da barra de menus, escolha **recursos avançados > VPN > grupo de VPN**.
5. Em todos os gateways de VPN disponíveis coloque, selecione o gateway de VPN definido previamente. Clique a seta para baixo a fim mover o gateway selecionado para os gateways de VPN selecionados neste campo do grupo de VPN.
6. Da barra de menus, escolha **recursos avançados > perfil VPN > VPN**.
7. A fim configurar o perfil VPN, termine todos os campos que são identificados por meio de um asterisco (*).**Permita a auto rede detectam:** Se permitido, o telefone VPN sibila-ao servidor TFTP e se nenhuma resposta é recebida, auto-novatos uma conexão de VPN.**Permita a verificação do ID do host:** Se permitido, o telefone VPN compara o FQDN do gateway de VPN URL contra o CN/SAN do certificado. O cliente não conecta se não combinam ou se um certificado do convite com um asterisco (*) está usado.**Permita a persistência da senha:** Isto permite que o telefone VPN ponha em esconderijo o username e o passsword para a tentativa seguinte VPN.
8. No indicador comum da configuração de perfil do telefone, o clique **aplica a configuração** a

fim aplicar a configuração de VPN nova. Você pode usar do “o perfil comum do telefone padrão” ou criar um perfil novo.
9. Se você criou um perfil novo para telefones/usuários específicos, vá ao indicador da configuração telefônica. No campo comum do perfil do telefone, escolha o **perfil comum do telefone do padrão**.
10. Registrar o telefone ao CallManager outra vez a fim transferir a configuração nova.

Configuração do certificado de autenticação

A fim configurar o certificado de autenticação, termine estas etapas no CallManager e no ASA:

1. Da barra de menus, escolha **recursos avançados > perfil VPN > VPN**.
2. Confirme o campo do método de authenticação do cliente é ajustado **para certificate.**
3. Entre ao CallManager. Da barra de menus, escolha o **> gerenciamento de certificado > o achado unificados do > segurança da administração do OS**.
4. Exporte os certificados corretos para o método de certificado de autenticação selecionado:MIC: Cisco_Manufacturing_CA - Autentique Telefones IP com um MICLSC: A função do proxy do Certificate Authority de Cisco (CAPF) - autentique Telefones IP com um LSC
5. Encontre o certificado, Cisco_Manufacturing_CA ou CAPF. Transfira o arquivo do .pem e salvar como um arquivo de .txt
6. Crie um ponto confiável novo no ASA e autentique o ponto confiável com o certificado salvar precedente. Quando você é alertado para o certificado de CA codificado base-64, seleto e cole o texto no arquivo transferido do .pem junto com o COMEÇO e as linhas final. Um exemplo é mostrado:

```
ASA (config)#crypto ca trustpoint CM-Manufacturing
ASA(config-ca-trustpoint)#enrollment terminal
ASA(config-ca-trustpoint)#exit
ASA(config)#crypto ca authenticate CM-Manufacturing
ASA(config)#

<base-64 encoded CA certificate>

quit
```

7. Confirme a autenticação no grupo de túneis é ajustado ao certificado de autenticação.

```
tunnel-group SSL webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable
```

Instalação certificada em Telefones IP

Os Telefones IP podem trabalhar com os MIC ou os LSC, mas o processo de configuração é diferente para cada certificado.

A instalação MIC

Àrevelia, todos os telefones que apoiam o VPN PRE-são carregados com os MIC. Os 7960 e 7940 telefones não vêm com um MIC, e exigem um procedimento de instalação especial para que o LSC registre-se firmemente.

Note: Cisco recomenda que você usa MIC para a instalação LSC somente. Cisco apoia LSC para autenticar a conexão TLS com CUCM. Porque os certificados de raiz MIC podem ser comprometidos, os clientes que configuram telefones para usar MIC para a autenticação TLS ou para toda a outra finalidade fazem tão por sua conta e risco. Cisco não supõe nenhuma

responsabilidade se os MIC são comprometidos.

A instalação LSC

1. Permita o serviço CAPF em CUCM.
2. Depois que o serviço CAPF é ativado, atribua as instruções do telefone para gerar um LSC em CUCM. Entre a Cisco unificou a administração CM e escolhem o **dispositivo > o telefone**. Selecione o telefone que você configurou.
3. Na seção de informação da função do proxy do Certificate Authority (CAPF), assegure-se de que todos os ajustes estejam corretos e a operação esteja ajustada a uma data futura.
4. Se o modo de autenticação é ajustado à corda nula ou ao certificado existente, nenhuma ação mais adicional está exigida.
5. Se o modo de autenticação é ajustado a uma corda, selecione manualmente a **configuração do > segurança dos ajustes > ** # > LSC > atualização no** console do telefone.

Verificar

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

Verificação ASA

```
ASA5520-C(config)#show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : CP-7962G-SEPXXXXXXXXXXXX
Index : 57
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium, AnyConnect for Cisco VPN Phone
Encryption : AnyConnect-Parent: (1)AES128 SSL-Tunnel: (1)AES128
DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)SHA1 SSL-Tunnel: (1)SHA1
DTLS-Tunnel: (1)SHA1Bytes Tx : 305849
Bytes Rx : 270069Pkts Tx : 5645
Pkts Rx : 5650Pkts Tx Drop : 0
Pkts Rx Drop : 0Group Policy :
GroupPolicy_SSL Tunnel Group : SSL
Login Time : 01:40:44 UTC Tue Feb 5 2013
Duration : 23h:00m:28s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 57.1
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : AnyConnect Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
```

```
Bytes Tx : 1759 Bytes Rx : 799
Pkts Tx : 2 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 57.2
Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 50529
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 835 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 57.3
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 51096
UDP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : DTLS VPN Client
Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 303255 Bytes Rx : 269270
Pkts Tx : 5642 Pkts Rx : 5649
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

Verificação CUCM

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Erros relacionados

- A identificação de bug Cisco CSCtf09529, adiciona o apoio para a característica VPN em CUCM para 8961, 9951, 9971 telefones
- A identificação de bug Cisco CSCuc71462, Failover do telefone IP VPN toma 8 minutos
- Identificação de bug Cisco CSCtz42052, apoio do telefone IP SSL VPN para não números de porta padrão
- A identificação de bug Cisco CSCth96551, não todos os caracteres ASCII é apoiada durante o usuário do telefone VPN + o início de uma sessão da senha.
- Identificação de bug Cisco CSCuj71475, entrada TFTP manual necessária para o telefone IP VPN
- Atendimentos faltados, colocados, ou recebidos do registro da identificação de bug Cisco CSCum10683, dos Telefones IP

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems