SSLVPN com exemplo de configuração dos Telefones IP

Índice

Introdução

Este documento descreve como configurar Telefones IP sobre um secure sockets layer VPN (SSL VPN), igualmente conhecido como um WebVPN. Dois gerentes das comunicações unificadas de Cisco (CallManagers) e três tipos de Certificados são usados com esta solução. Os CallManagers são:

- Gerente das comunicações unificadas de Cisco (CUCM)
- Cisco Unified Communications Manager Express (CME unificado Cisco)

Os tipos do certificado são:

- Certificados auto-assinados
- Os Certificados da terceira, como confiam, Thawte, e GoDaddy
- Certificate Authority (CA) da ferramenta de segurança do Cisco IOS ®/Adaptive (ASA)

O conceito chave a compreender é que, uma vez a configuração no gateway de VPN SSL e o CallManager estão terminados, você deve juntar-se aos Telefones IP localmente. Isto permite os telefones de juntar-se ao CUCM e de usar a informação de VPN e os Certificados corretos. Se os telefones não são juntados localmente, não podem encontrar o gateway de VPN SSL e não têm os Certificados corretos para terminar o aperto de mão SSL VPN.

A maioria de configurações comum são CUCM/Unified CME com certificados auto-assinados ASA e certificados auto-assinados do Cisco IOS. Consequentemente, são o mais fáceis de configurar.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Gerente das comunicações unificadas de Cisco (CUCM) ou Cisco Unified Communications Manager Express (CME unificado Cisco)
- SSL VPN (WebVPN)
- Ferramenta de segurança adaptável de Cisco (ASA)
- O certificado datilografa, como auto-assinado, da terceira, e autoridades de certificação

Componentes Utilizados

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

- Licença do prêmio ASA.
- Licença do telefone de AnyConnect VPN.
  - Para o ASA libere 8.0.x, a licença é AnyConnect para o telefone de Linksys.
  - Para o ASA libere 8.2.x ou mais tarde, a licença é AnyConnect para o telefone de Cisco VPN.
- Gateway de VPN SSL: ASA 8.0 ou mais atrasado (com um AnyConnect para a licença do telefone de Cisco VPN), ou Cisco IOS Software Release 12.4T ou Mais Recente.
  - O Cisco IOS Software Release 12.4T ou Mais Recente não é apoiado formalmente como documentado no guia de configuração de VPN SSL.
  - No Cisco IOS Software Release 15.0(1)M, o gateway de VPN SSL é uma característica Seat-contada licenciar em Cisco 880, em Cisco 890, em Cisco 1900, no Cisco 2900, e no Cisco 3900 Plataformas. Uma licença válida é exigida para uma sessão de VPN bem sucedida SSL.
- CallManager: CUCM 8.0.1 ou mais atrasado, ou CME unificado 8.5 ou mais atrasado.

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.

Configurar

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

A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

Configuração de VPN básica ASA SSL

A configuração de VPN básica ASA SSL é descrita nestes documentos:

- ASA 8.x: O VPN alcança com o cliente VPN de AnyConnect que usa o exemplo de configuração do certificado auto-assinado
- Configurando conexões de cliente de VPN de AnyConnect

Uma vez que esta configuração está completa, um teste remoto PC deve poder conectar ao gateway de VPN SSL, conecta através de AnyConnect, e sibila o CUCM. Assegure-se de que o ASA tenha um AnyConnect para a licença do Cisco IP Phone. (Use o **comando show ver**.) A porta 443 TCP e UDP deve estar aberta entre o gateway e o cliente.

Nota: A função de balanceamento de carga SSL VPN não é apoiada para telefones VPN.

CUCM: ASA SSL VPN com configuração dos certificados auto-assinados

Refira o telefone IP SSL VPN ao ASA usando AnyConnect para mais informação detalhada.

O ASA deve ter uma licença para AnyConnect para o telefone de Cisco VPN. Depois que você configura o SSL VPN, você configura então seu CUCM para o VPN.

1. Use este comando a fim exportar o certificado auto-assinado do ASA:

   `ciscoasa(config)# crypto ca export trustpoint name identity-certificate`Este comando indica um certificado de identidade PEM-codificado ao terminal.
2. A cópia e cola o certificado a um editor de texto, e salvar o como um arquivo do .pem. Seja certo incluir o CERTIFICADO do COMEÇO e TERMINAR linhas do CERTIFICADO, ou o certificado não importará corretamente. Não altere o formato do certificado porque isto causará problemas quando o telefone tenta autenticar ao ASA.
3. Navegue a **Cisco unificou o > gerenciamento de certificado do > segurança da administração do sistema operacional > o certificado/certificate chain da transferência de arquivo pela rede** a fim carregar o arquivo certificado à seção de gerenciamento de certificado do CUCM.
4. Transfira os Certificados CallManager.pem, CAPF.pem, e Cisco_Manufacturing_CA.pem da mesma área usada para carregar os certificados auto-assinados do ASA (veja etapa 1), e salvar os a seu desktop.
   1. Por exemplo, a fim importar o CallManager.pem ao ASA, use estes comandos:

      ```
      ciscoasa(config)# crypto ca trustpoint certificate-name
      ciscoasa(config-ca-trustpoint)# enrollment terminal
      ciscoasa(config)# crypto ca authenticate certificate-name
      ```
   2. Quando você é alertado copiar e colar o certificado correspondente para o ponto confiável, abra o arquivo que você salvar do CUCM, a seguir da cópia e cole o certificado Base64-encoded. Seja certo incluir o CERTIFICADO do COMEÇO e TERMINAR linhas

do CERTIFICADO (com hífens).
3. Datilografe a **extremidade**, a seguir pressione o **retorno**.
4. Quando alertado para aceitar **sim o** certificado, o tipo, pressiona então **entra**.
5. Repita etapas 1 4 para outros dois Certificados (CAPF.pem, Cisco_Manufacturing_CA.pem) do CUCM.

5. Configurar o CUCM para as configurações de VPN corretas, como descrito em CUCM IPphone VPN config.pdf.

   Nota: O gateway de VPN configurado no CUCM deve combinar a URL que é configurada no gateway de VPN. Se o gateway e a URL não combinam, o telefone não pode resolver o endereço, e você não verá que algum debuga no gateway de VPN.

- No CUCM: O gateway de VPN URL é https://192.168.1.1/VPNPhone
- No ASA, use estes comandos:

```
ciscoasa# configure terminal
ciscoasa(config)# tunnel-group VPNPhones webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url https://192.168.1.1/VPNPhone
enable
ciscoasa(config-tunnel-webvpn)# exit
```

- Você pode usar estes comandos no Security Device Manager adaptável (ASDM) ou sob o perfil de conexão.

CUCM: ASA SSL VPN com configuração da terceira dos Certificados

Esta configuração é muito similar à configuração descrita em CUCM: O ASA SSLVPN com seção de configuração dos certificados auto-assinados, salvo que você estão usando Certificados da terceira. Configurar SSL VPN no ASA com os Certificados da terceira como descrito em ASA 8.x instalam manualmente Certificados do vendedor da 3ª parte para o uso com exemplo de configuração WebVPN.

Nota: Você deve copiar o certificate chain completo do ASA ao CUCM e incluir todo o intermediário e certificados de raiz. Se o CUCM não inclui a corrente completa, os telefones não têm os Certificados necessários a autenticar e falharão o aperto de mão SSL VPN.

Configuração de VPN básica IO SSL

Nota: Os Telefones IP são designados como não apoiado em IO SSL VPN; as configurações estão no melhor esforço somente.

A configuração de VPN básica do Cisco IOS SSL é descrita nestes documentos:

- **Exemplo de Configuração de Cliente VPN SSL (SVC) no IOS com SDM**
- O cliente VPN de AnyConnect no IOS Router com zona IO baseou o exemplo da configuração de firewall da política

Uma vez que esta configuração está completa, um teste remoto PC deve poder conectar ao gateway de VPN SSL, conecta através de AnyConnect, e sibila o CUCM. No Cisco IOS 15.0 e mais atrasado, você deve ter uma licença válida SSL VPN terminar esta tarefa. A porta 443 TCP

e UDP deve estar aberta entre o gateway e o cliente.

CUCM: IO SSL VPN com configuração dos certificados auto-assinados

Esta configuração é similar à configuração descrita em CUCM: ASA SSLVPN com configuração da terceira dos Certificados e CUCM: ASA SSLVPN com seções de configuração dos certificados auto-assinados. As diferenças são:

1. Use este comando a fim exportar o certificado auto-assinado do roteador:

```
R1(config)# crypto pki export trustpoint-name pem terminal
```

2. Use estes comandos a fim importar os Certificados CUCM:

```
R1(config)# crypto pki trustpoint certificate-name
R1(config-ca-trustpoint)# enrollment terminal
R1(config)# crypto ca authenticate certificate-name
```

A configuração do contexto WebVPN deve mostrar este texto:

```
R1(config)# crypto pki trustpoint certificate-name
R1(config-ca-trustpoint)# enrollment terminal
R1(config)# crypto ca authenticate certificate-name
```

Configurar o CUCM como descrito em CUCM: ASA SSLVPN com seção de configuração dos certificados auto-assinados.

CUCM: IO SSL VPN com configuração da terceira dos Certificados

Esta configuração é similar à configuração descrita em CUCM: ASA SSLVPN com seção de configuração dos certificados auto-assinados. Configurar seu WebVPN com um certificado da terceira.

> Nota: Você deve copiar o certificate chain completo WebVPN ao CUCM e incluir todo o intermediário e certificados de raiz. Se o CUCM não inclui a corrente completa, os telefones não têm os Certificados necessários a autenticar e falharão o aperto de mão SSL VPN.

CME unificado: ASA/Router SSL VPN com certificados auto-assinados/configuração da terceira dos Certificados

A configuração para o CME unificado é similar às configurações do CUCM; por exemplo, as configurações do valor-limite WebVPN são as mesmas. A única diferença significativa é as configurações do agente unificado do atendimento CME. Configurar o grupo de VPN e a política de VPN para o CME unificado como descrito em configurar o cliente VPN SSL para Telefones IP SCCP.

> Nota: O CME unificado apoia somente o Skinny Call Control Protocol (SCCP) e não apoia o Session Initiation Protocol (SIP) para telefones VPN.

> Nota: Não há nenhuma necessidade de exportar os Certificados do CME unificado para o

ASA ou o roteador. Você precisa somente de exportar os Certificados do ASA ou o gateway do roteador WebVPN para o CME unificado.

A fim exportar os Certificados do gateway WebVPN, refira a seção ASA/router. Se você está usando um certificado da terceira, você deve incluir o certificate chain completo. A fim importar os Certificados ao CME unificado, use o mesmo método que usado aos certificados de importação em um roteador:

```
CME(config)# crypto pki trustpoint certificate-name
CME(config-ca-trustpoint)# enrollment terminal
CME(config)# crypto ca authenticate certificate-name
```

Telefones IP UC 520 com configuração de VPN SSL

O telefone IP modelo UC 520 do 500 Series das comunicações unificadas de Cisco é bastante diferente das configurações CUCM e CME.

- Desde que o telefone IP UC 520 é o CallManager e o gateway WebVPN, não há nenhuma necessidade de configurar Certificados entre os dois.
- Configurar o WebVPN em um roteador como você normalmente com certificados auto-assinados ou os Certificados da terceira.
- O telefone IP UC 520 tem construído no cliente WebVPN, e você pode configurar-lo apenas porque você um PC normal conectaria ao WebVPN. Entre no gateway, então a combinação de nome de usuário/senha.
- O telefone IP UC 520 é compatível com os telefones dos TERMAS 525G do telefone IP da empresa de pequeno porte de Cisco.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

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