ASA e exemplo nativo da configuração de cliente L2TP-IPSec Android

Índice

Introdução

O protocolo de tunelamento de camada 2 (L2TP) em IPSec fornece a capacidade de distribuir e administrar uma solução de VPN L2TP ao lado do IPSec VPN e serviços de firewall em uma plataforma única. As vantagens principal da configuração do L2TP sobre o IPsec em uma encenação do Acesso remoto são que os usuários remotos podem alcançar um VPN sobre uma rede IP pública sem um gateway ou uma linha dedicada, que permita o Acesso remoto de virtualmente todo o lugar com serviço de telefonia tradicional (POTS). Um benefício adicional é que a única exigência do cliente para o acesso VPN é o uso de Windows com rede de comunicação dial-up de Microsoft (DUN). Nenhum software do cliente adicional, tal como o software Cisco VPN Client, é exigido.

Este documento fornece uma configuração de exemplo para o cliente nativo de Android do L2TP/IPSec. Toma o através de todos os comandos required necessários em uma ferramenta de segurança adaptável de Cisco (ASA), assim como as etapas ser tomado no dispositivo próprio de Android.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações deste documento são baseadas nas seguintes versões de software e de hardware:

- O L2TP/IPSec de Android exige a versão de software 8.2.5 de Cisco ASA ou mais atrasado, a versão 8.3.2.12 ou mais recente, ou a versão 8.4.1 ou mais recente.
- O ASA apoia o apoio da assinatura do certificado do algoritmo de mistura segura 2 (SHA2) para Microsoft Windows 7 e clientes VPN Android-nativos quando o protocolo do L2TP/IPSec é usado.
- Veja o manual de configuração do 5500 Series de Cisco ASA usando o CLI, os 8.4 e os 8.6: Configurando o L2TP sobre o IPsec: Requisitos de licenciamento para o L2TP sobre o IPsec.

As informações apresentadas 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

Esta seção descreve a informação uma precisaria a fim configurar as características descritas neste documento.

Configurar a conexão do L2TP/IPSec em Android

Este procedimento descreve como configurar a conexão do L2TP/IPSec em Android:

1. Abra o menu, e escolha **ajustes**.
2. Escolha **controles do Sem fio e da rede** ou do **Sem fio**. A opção disponível depende de sua versão de Android.
3. Escolha **ajustes VPN**.
4. Escolha **adicionam o VPN**.
5. Escolha **adicionam L2TP/IPsec PSK VPN**.
6. Escolha o **nome VPN**, e dê entrada com um nome descritivo.
7. Escolha **servidor de VPN ajustado**, e dê entrada com um nome descritivo.
8. Escolha **chave pré-compartilhada ajustada do IPsec**.
9. Desmarcar **permitem o segredo L2TP**.
10. O [Optional] ajustou o identificador do IPsec como o nome de grupo de túneis ASA. Nenhum ajuste significa que cairá em DefaultRAGroup no ASA.
11. Abra o menu, e escolha a **salvaguarda**.

Configurar a conexão do L2TP/IPSec no ASA

Estas são a versão exigida 1 do intercâmbio de chave de Internet ASA (IKEv1) ([ISAKMP] do protocolo internet security association and key management) os ajustes da política que permitem

clientes VPN nativos, integrados com o sistema operacional em um valor-limite, para fazer uma conexão de VPN ao ASA quando o L2TP sobre o protocolo IPSec for usado:

- IKEv1 fase 1 - Criptografia do Triple Data Encryption Standard (3DES) com método da mistura SHA1
- Fase de IPSec 2 - Criptografia 3DES ou de Advanced Encryption Standard (AES) com message digest 5 (MD5) ou método da mistura SHA
- Autenticação de PPP - Versão 1 do protocolo password authentication (PAP), do protocolo microsoft challenge handshake authentication (MS-CHAPv1), ou MS-CHAPv2 (preferido)
- Chave pré-compartilhada

  Nota: O ASA apoia somente as autenticações de PPP PAP e MS-CHAP (versões 1 e 2) no base de dados local. O Extensible Authentication Protocol (EAP) e a RACHADURA são executados por server da autenticação de proxy. Consequentemente, se um usuário remoto pertence a um grupo de túneis configurado com o EAP-**proxy da autenticação** ou os **comandos chap da autenticação** e se o ASA está configurado para usar o base de dados local, esse usuário será incapaz de conectar.

  Além disso, Android não apoia o PAP e, porque o Lightweight Directory Access Protocol (LDAP) não apoia o MS-CHAP, o LDAP não é um mecanismo de autenticação viável. A única ação alternativa é usar o RAIO. Veja a identificação de bug Cisco CSCtw58945, "L2TP sobre a falha das conexões IPSec com autorização do ldap e mschapv2," para uns detalhes mais adicionais em edições com MS-CHAP e LDAP.

Este procedimento descreve como configurar a conexão do L2TP/IPSec no ASA:

1. Defina um pool do endereço local ou use um DHCP-server para a ferramenta de segurança adaptável a fim atribuir endereços IP de Um ou Mais Servidores Cisco ICM NT aos clientes para a política do grupo.
2. Crie uma grupo-política interna. Defina o protocolo de túnel para ser l2tp-ipsec.Configurar um Domain Name Server (DNS) a ser usado pelos clientes.
3. Crie um grupo de túneis novo ou altere os atributos do DefaultRAGroup existente. (O grupo de túneis novo A pode ser usado se o identificador do IPsec é ajustado como o nome do grupo no telefone; veja a etapa 10 para a configuração telefônica.)
4. Defina os atributos gerais do grupo de túneis que são usados. Trace a política do grupo definido a este grupo de túneis.Trace o conjunto de endereços definido a ser usado por este grupo de túneis.Altere o grupo de Authentication Server se você quer usar algo a não ser o LOCAL.
5. Defina a chave pré-compartilhada sob os atributos do IPsec do grupo de túneis a ser usado.
6. Altere os atributos PPP do grupo de túneis que são usados de modo que somente a rachadura, ms-chap-v1 e ms-chap-v2 sejam usados.
7. Crie uma transformação ajustada com um tipo de criptografia e um tipo do autenticação específicos do Encapsulating Security Payload (ESP).
8. Instrua o IPsec para usar o modo de transporte um pouco do que o modo de túnel.
9. Defina uma política ISAKMP/IKEv1 usando a criptografia 3DES com método da mistura SHA1.
10. Crie um mapa cripto dinâmico, e trace-o a um crypto map.
11. Aplique o crypto map a uma relação.
12. Permita o ISAKMP nessa relação.

Comandos do arquivo de configuração para a compatibilidade ASA

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

Este exemplo mostra os comandos do arquivo de configuração que asseguram a compatibilidade ASA com um cliente VPN nativo em todo o sistema operacional.

ASA 8.2.5 ou exemplo de configuração mais atrasado

```
Username <name> password <passwd> mschap
ip local pool l2tp-ipsec_address 192.168.1.1-192.168.1.10
group-policy l2tp-ipsec_policy internal
group-policy l2tp-ipsec_policy attributes
           dns-server value <dns_server>
           vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
           default-group-policy l2tp-ipsec_policy
           address-pool l2tp-ipsec_address
tunnel-group DefaultRAGroup ipsec-attributes
           pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
           no authentication pap
           authentication chap
           authentication ms-chap-v1
           authentication ms-chap-v2
crypto ipsec transform-set trans esp-3des esp-sha-hmac
crypto ipsec transform-set trans mode transport
crypto dynamic-map dyno 10 set transform-set set trans
crypto map vpn 65535 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto isakmp enable outside
crypto isakmp policy 10
           authentication pre-share
           encryption 3des
           hash sha
           group 2
           lifetime 86400
```

ASA 8.3.2.12 ou exemplo de configuração mais atrasado

```
Username <name> password <passwd> mschap
ip local pool l2tp-ipsec_address 192.168.1.1-192.168.1.10
group-policy l2tp-ipsec_policy internal
group-policy l2tp-ipsec_policy attributes
           dns-server value <dns_server>
           vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
           default-group-policy l2tp-ipsec_policy
           address-pool l2tp-ipsec_addresses
tunnel-group DefaultRAGroup ipsec-attributes
           pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
           no authentication pap
           authentication chap
           authentication ms-chap-v1
           authentication ms-chap-v2
```

```
crypto ipsec ikev1 transform-set my-transform-set-ikev1 esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport
crypto dynamic-map dyno 10 set ikev1 transform-set my-transform-set-ikev1
crypto map vpn 20 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto ikev1 enable outside
crypto ikev1 policy 10
          authentication pre-share
          encryption 3des
          hash sha
          group 2
          lifetime 86400
```

Verificar

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

Este procedimento descreve como estabelecer a conexão:

1. Abra o menu, e escolha **ajustes**.
2. Selecione **controles do Sem fio e da rede** ou do **Sem fio**. (A opção disponível depende de sua versão de Android.)
3. Selecione a configuração de VPN da lista.
4. Insira seu nome de usuário e senha.
5. Seleto **recorde o username**.
6. Seleto **conecte**.

Este procedimento descreve como desligar:

1. Abra o menu, e escolha **ajustes**.
2. Selecione **controles do Sem fio e da rede** ou do **Sem fio**. (A opção disponível depende de sua versão de Android.)
3. Selecione a configuração de VPN da lista.
4. Selecione a **disconexão**.

Use estes comandos a fim confirmar que sua conexão trabalha corretamente.

- **mostre o isakmp cripto da corrida** - Para a versão ASA 8.2.5
- **mostre a corrida ikev1 cripto** - Para versão ASA 8.3.2.12 ou mais tarde
- **mostre VPN-sessiondb ra-ikev1-ipsec -** Para versão ASA 8.3.2.12 ou mais tarde
- **mostre o telecontrole VPN-sessiondb -** Para a versão ASA 8.2.5

  Nota: 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.

Caveats conhecidos

- Identificação de bug Cisco CSCtq21535, “retorno de monitoramento ASA ao conectar com o cliente de Android L2TP/IPsec”
- A identificação de bug Cisco CSCtj57256, conexão "L2TP/IPSec de Android não estabelece

ao ASA55xx"
- A identificação de bug Cisco CSCtw58945, "L2TP sobre conexões IPSec falha com autorização e mschapv2" do ldap

Informações Relacionadas

- Manual de configuração do 5500 Series de Cisco ASA usando o CLI, os 8.4 e os 8.6: Configurando o L2TP sobre o IPsec
- Release Note para o 5500 Series de Cisco ASA, versão 8.4(x)
- Manual de configuração do 5500 Series de Cisco ASA usando o CLI, 8.3: Informação sobre o NAT
- ASA Pre-8.3 a 8.3 exemplos da configuração de NAT
- Suporte Técnico e Documentação - Cisco Systems