Local dinâmico para situar um túnel IKEv2 VPN entre um exemplo de configuração dois ASA

Índice

Introdução

Este documento descreve como configurar um túnel de site para site da versão 2 do intercâmbio de chave de Internet (IKEv2) VPN entre duas ferramentas de segurança adaptáveis (ASA) onde um ASA tem um endereço IP dinâmico e o outro tem um endereço IP estático.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Versão ASA 5505
- Versão ASA 9.1(5)

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

Há duas maneiras que esta configuração pode se estabelecer:

- Com o grupo de túneis DefaultL2LGroup
- Com um grupo de túneis Nomeado

A diferença de configuração a mais grande entre as duas encenações é o Internet Security Association and Key Management Protocol (ISAKMP) ID usado pelo ASA remoto. Quando o DefaultL2LGroup é usado no ASA estático, o ISAKMP ID do par tem que ser o endereço. Contudo se um grupo de túneis Nomeado é usado, o ISAKMP ID do par tem que ser o mesmo o nome de grupo de túneis usando este comando:

```
crypto isakmp identity key-id <tunnel-group_name>
```

A vantagem de usar grupos de túneis Nomeados no ASA estático é que quando o DefaultL2LGroup é usado, a configuração nos ASA dinâmicos remotos, que inclui as chaves pré-compartilhada, tem que ser idêntica e não permite muita granularidade com a instalação das políticas.

Diagrama de Rede

Configurar

Esta seção descreve a configuração em cada ASA segundo que solução você decide usar.

Solução 1 - Uso do DefaultL2LGroup

Esta é a maneira a mais simples de configurar um túnel do LAN para LAN (L2L) entre dois ASA quando um ASA obtém seu endereço dinamicamente. O grupo DefaultL2L é grupo de túneis preconfigured no ASA e todas as conexões que não combinam explicitamente nenhuma queda do grupo do túnel específico nesta conexão. Desde que o ASA dinâmico não tem uma constante predeterminou o endereço IP de Um ou Mais Servidores Cisco ICM NT, ele significa que o admin não pode configurar o Statis ASA a fim permitir a conexão em um grupo de túneis específico. Nesta situação, o grupo DefaultL2L pode ser usado a fim permitir as conexões dinâmica.

> Dica: Com este método, o downside é que todos os pares terão a mesma chave pré-compartilhada desde que somente uma chave pré-compartilhada pode ser definida pelo grupo de túneis e todos os pares conectarão ao mesmo grupo de túneis DefaultL2LGroup.

Configuração estática ASA

```
crypto isakmp identity key-id <tunnel-group_name>
```

No Security Device Manager adaptável (ASDM), você pode configurar o DefaultL2LGroup como mostrado aqui:

ASA dinâmico

```
crypto isakmp identity key-id <tunnel-group_name>
```

No ASDM, você pode usar o assistente padrão a fim estabelecer o perfil de conexão apropriado ou você pode simplesmente adicionar uma nova conexão e seguir o procedimento padrão.

Solução 2 - Crie um grupo de túneis definido pelo utilizador

Este método exige slighly mais configuração, mas permite mais granularidade. Cada par pode ter suas próprias política separada e chave pré-compartilhada. De qualquer modo aqui é importante mudar o ISAKMP ID no par dinâmico de modo que use um nome em vez de um endereço IP de Um ou Mais Servidores Cisco ICM NT. Isto permite que o ASA estático combine o pedido entrante da iniciação ISAKMP ao grupo de túneis adequado e use as políticas direitas.

Configuração estática ASA

```
crypto isakmp identity key-id <tunnel-group_name>
```

No ASDM, o nome do perfil de conexão é um endereço IP de Um ou Mais Servidores Cisco ICM NT à revelia. Assim quando você o cria, você deve mudá-lo a fim dar-lhe aqui um nome segundo as indicações do tiro de tela:

Configuração dinâmica ASA

O ASA dinâmico é configurado quase a mesma maneira em ambas as soluções com a adição de um comando como mostrado aqui:

```
crypto isakmp identity key-id DynamicSite2Site1
```

Como descrito previamente, à revelia o ASA usa o endereço IP de Um ou Mais Servidores Cisco ICM NT da relação que o túnel VPN é traçado como ao ISAKMP CHAVE-ID. De qualquer modo neste caso, o chave-ID no ASA dinâmico é o mesmo que o nome do grupo de túneis no ASA estático. Assim em cada par dinâmico, a chave-identificação será diferente e um grupo de túneis correspondente deve ser criado no ASA estático com o nome direito.

No ASDM, isto pode ser configurado segundo as indicações deste tiro de tela:

Verificar

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

No ASA estático

Está aqui o resultado do comando **cripto do det IKEv2 sa da mostra**:

```
crypto isakmp identity key-id DynamicSite2Site1
```

Está aqui o resultado do **comando show crypto ipsec sa**:

```
crypto isakmp identity key-id DynamicSite2Site1
```

No ASA dinâmico

Está aqui o resultado do **comando detail cripto IKEv2 sa da mostra**:

```
crypto isakmp identity key-id DynamicSite2Site1
```

Está aqui o resultado do **comando show crypto ipsec sa**:

```
crypto isakmp identity key-id DynamicSite2Site1
```

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.

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

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.

> Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **pacote IKEv2 cripto deb**
- **deb IKEv2 cripto interno**