ASA 8.x/ASDM 6.x: Adicionar a informação de peer nova VPN em um VPN de Site-para-Site existente usando o ASDM

Índice

Introdução

Este documento fornece a informação sobre as mudanças configurational para fazer quando um par novo VPN é adicionado à configuração existente do VPN de Site-para-Site usando o Security Device Manager adaptável (ASDM). Isto é exigido nestas encenações:

- O provedor de serviço do Internet (ISP) foi mudado e um grupo novo de escala pública IP é usado.
- Um re-projeto completo da rede em um local.
- O dispositivo usado como o gateway de VPN em um local é migrado a um dispositivo novo com um endereço IP público diferente.

Este documento supõe que o VPN de Site-para-Site está configurado já corretamente e trabalha muito bem. Este documento fornece as etapas para seguir a fim mudar uma informação de peer VPN na configuração de VPN L2L.

Pré-requisitos

Requisitos

A Cisco recomenda ter conhecimento deste tópico:

- Exemplo de configuração do VPN de Site-para-Site ASA

Componentes Utilizados

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

- 5500 Series da ferramenta de segurança de Cisco Adapative com versão de software 8.2 e mais atrasado
- Security Device Manager de Cisco Adapative com versão de software 6.3 e mais atrasado

Convenções

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

Informação de Backround

O VPN de Site-para-Site está trabalhando muito bem entre o HQASA e o BQASA. Supõe que o BQASA tem um re-projeto completo da rede e o esquema IP esteve alterado a nível ISP, mas todos os detalhes internos da sub-rede permanecem os mesmos.

Esta configuração de exemplo usa estes endereços IP de Um ou Mais Servidores Cisco ICM NT:

- Endereço IP externo existente BQASA - 200.200.200.200
- Endereço IP externo novo BQASA - 209.165.201.2

Nota: Aqui, somente a informação de peer será alterada. Porque não há nenhuma outra mudança na sub-rede interna, as listas de acesso criptos permanecem as mesmas.

Configuração ASDM

Esta seção fornece a informação sobre os métodos possíveis usados para mudar a informação de peer VPN em HQASA usando o ASDM.

Crie um perfil da nova conexão

Este pode ser o método mais fácil porque não perturba a configuração de VPN existente e pode criar um perfil da nova conexão com a informação relacionada nova do par VPN.

1. Vá à *configuração > ao VPN de Site-para-Site > aos perfis de conexão* e o clique *adiciona* sob a área dos perfis de conexão.O indicador *de site para site do perfil de conexão do IPsec adicionar* abre.
2. Sob a aba básica, forneça os detalhes para o *endereço IP do peer*, a *chave pré-compartilhada*, e as *redes protegidas*. Use todos os mesmos parâmetros que o VPN existente, exceto a informação de peer. Clique em OK.
3. Sob o menu avançado, clique a *entrada do crypto map*. Refira a aba da *prioridade*. Esta prioridade é igual ao número de sequência em sua configuração de CLI equivalente. Quando pouco número do que a entrada existente do crypto map é atribuído, este perfil

novo está executado primeiramente. Mais alto o número de prioridade, o menos o valor. Isto é usado para mudar a ordem de sequência que um crypto map específico será executado. Clique a *APROVAÇÃO* para terminar a criação do perfil da nova conexão.

Isto cria automaticamente um grupo de túneis novo junto com um crypto map associado. Certifique-se que você pode alcançar o BQASA com o endereço IP de Um ou Mais Servidores Cisco ICM NT novo antes que você use este perfil da nova conexão.

Edite a configuração de VPN existente

Uma outra maneira de adicionar um par novo é alterar a configuração existente. O perfil da conexão existente não pode ser editado para a informação de peer nova porque é limitado a um par específico. A fim editar a configuração existente, você precisa de executar estas etapas:

1. Crie um grupo de túneis novo
2. Edite o crypto map existente

Crie um grupo de túneis novo

Vão à *configuração > ao VPN de Site-para-Site > avançaram > os grupos de túneis* e o clique *adiciona* para criar um grupo de túneis novo que contenha a informação de peer nova VPN. Especifique os campos do *nome* e de *chave pré-compartilhada*, a seguir clique a *APROVAÇÃO*.

Nota: Certifique-se que a chave pré-compartilhada combina a outra extremidade do VPN.

Nota: No campo de nome, somente o endereço IP de Um ou Mais Servidores Cisco ICM NT do peer remoto deve ser incorporado quando o modo de autenticação é chaves pré-compartilhada. Todo o nome pode ser usado somente quando o método de autenticação é através dos Certificados. Este erro aparece quando um nome está adicionado no campo de nome e o método de autenticação PRE-está compartilhado:

Edite o crypto map existente

O crypto map existente pode ser editado a fim associar a informação de peer nova.

Conclua estes passos:

1. Vão à *configuração > ao VPN de Site-para-Site > avançaram > os crypto map*, a seguir selecionam o crypto map exigido e o clique *edita*.O indicador da *regra do IPsec da edição* aparece.
2. Sob a aba (básica) da política do túnel, na área dos ajustes do par, especifique o par novo no endereço IP de Um ou Mais Servidores Cisco ICM NT do par para ser campo adicionado. Então, o clique *adiciona*.
3. Selecione o endereço IP do peer existente e o clique *remove* para reter a informação de peer nova somente. Clique em OK.**Nota:** Depois que você altera a informação de peer no crypto map atual, o perfil de conexão associado com este crypto map está suprimido imediatamente no indicador ASDM.
4. Os detalhes das redes cifradas permanecem os mesmos. Se você precisa de alterar estes, vá à aba da *seleção do tráfego*.
5. Vai à *configuração > ao VPN de Site-para-Site > avançou > a* placa dos *crypto map* a fim ver

o crypto map alterado. Contudo, estas mudanças não ocorrem até que você clique *se aplique*. Depois que você clique *se aplica*, vai à *configuração > ao VPN de Site-para-Site > avançou > o* menu dos *grupos de túneis* a fim verificar se um grupo de túneis associado esta presente ou não. Se sim, um *perfil de conexão* associado será criado então.

Verificar

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

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- Use este comando ver os parâmetros da associação de segurança específicos a um único par:**mostre o endereço IP de Um ou Mais Servidores Cisco ICM NT cripto do <Peer do par IPsec sa >**

Troubleshooting

Use esta seção para resolver problemas de configuração.

Iniciador IKE incapaz de encontrar a política: Test_ext de Intf, Src: 172.16.1.103, Dst: 10.1.4.251

Este erro é indicado nos mensagens de registro ao tentar mudar o VPN espreita de um concentrador VPN ao ASA.

Solução:

Este pode ser um resultado das etapas da configuração imprópria seguidas durante a migração. Assegure-se de que o emperramento cripto à relação esteja removido antes que você adicione um par novo. Também, certifique-se de que você usou o endereço IP de Um ou Mais Servidores Cisco ICM NT do par no grupo de túneis, mas não o nome.

Informações Relacionadas

- **Local para situar (L2L) o VPN com ASA**
- **A maioria de problemas comuns VPN**
- **Página de suporte técnico ASA**
- **Suporte Técnico e Documentação - Cisco Systems**