ASA 8.x/ASDM 6.x: Adicione novas informações de peer de VPN em uma VPN site a site existente usando o ASDM

Contents

Introduction
Prerequisites
Requirements
Componentes Utilizados
Conventions
Informações de fundo
Configuração do ASDM
Criar um novo perfil de conexão
Edite a Configuração de VPN Existente
Verificar
Troubleshoot
Iniciador IKE incapaz de encontrar a política: Intf test_ext, Src: 172.16.1.103, Data: 10.1.4.251
Informações Relacionadas

Introduction

Este documento fornece informações sobre as alterações de configuração a serem feitas quando um novo peer VPN é adicionado à configuração de VPN site a site existente usando o Adaptive Security Device Manager (ASDM). Isso é necessário nestes cenários:

- O provedor de serviços de Internet (ISP) foi alterado e um novo conjunto de intervalo de IP público é usado.
- Um novo projeto completo da rede em um local.
- O dispositivo usado como gateway VPN em um local é migrado para um novo dispositivo com um endereço IP público diferente.

Este documento pressupõe que a VPN site a site já está configurada corretamente e funciona bem. Este documento fornece as etapas a serem seguidas para alterar as informações de um peer de VPN na configuração da VPN L2L.

Prerequisites

Requirements

A Cisco recomenda ter conhecimento deste tópico:

- Exemplo de configuração de VPN site a site ASA

Componentes Utilizados

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

- Cisco Adapative Security Appliance série 5500 com versão de software 8.2 e posterior
- Cisco Adaptive Security Device Manager com software versão 6.3 e posterior

Conventions

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

Informações de fundo

A VPN site a site está funcionando bem entre o HQASA e o BQASA. Suponha que o BQASA tenha um novo projeto de rede completo e que o esquema IP tenha sido modificado no nível do ISP, mas todos os detalhes da sub-rede interna permaneçam os mesmos.

Este exemplo de configuração usa estes endereços IP:

- Endereço IP externo BQASA existente - 200.200.200.200
- Novo endereço IP externo BQASA - 209.165.201.2

Observação: aqui, somente as informações do peer serão modificadas. Como não há outra alteração na sub-rede interna, as listas de acesso criptografadas permanecem as mesmas.

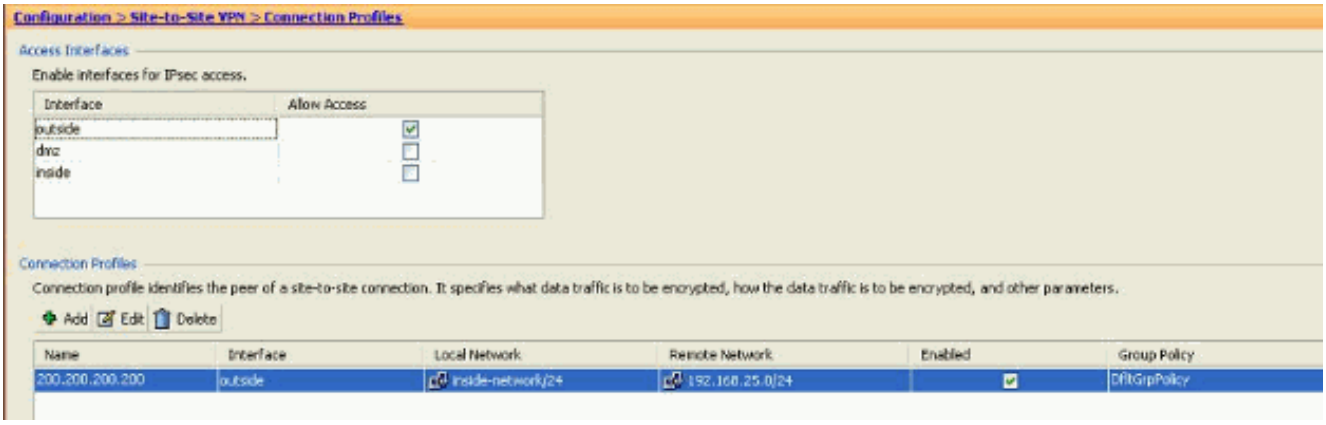
Configuração do ASDM

Esta seção fornece informações sobre os possíveis métodos usados para alterar as informações de peer da VPN no HQASA usando o ASDM.

Criar um novo perfil de conexão

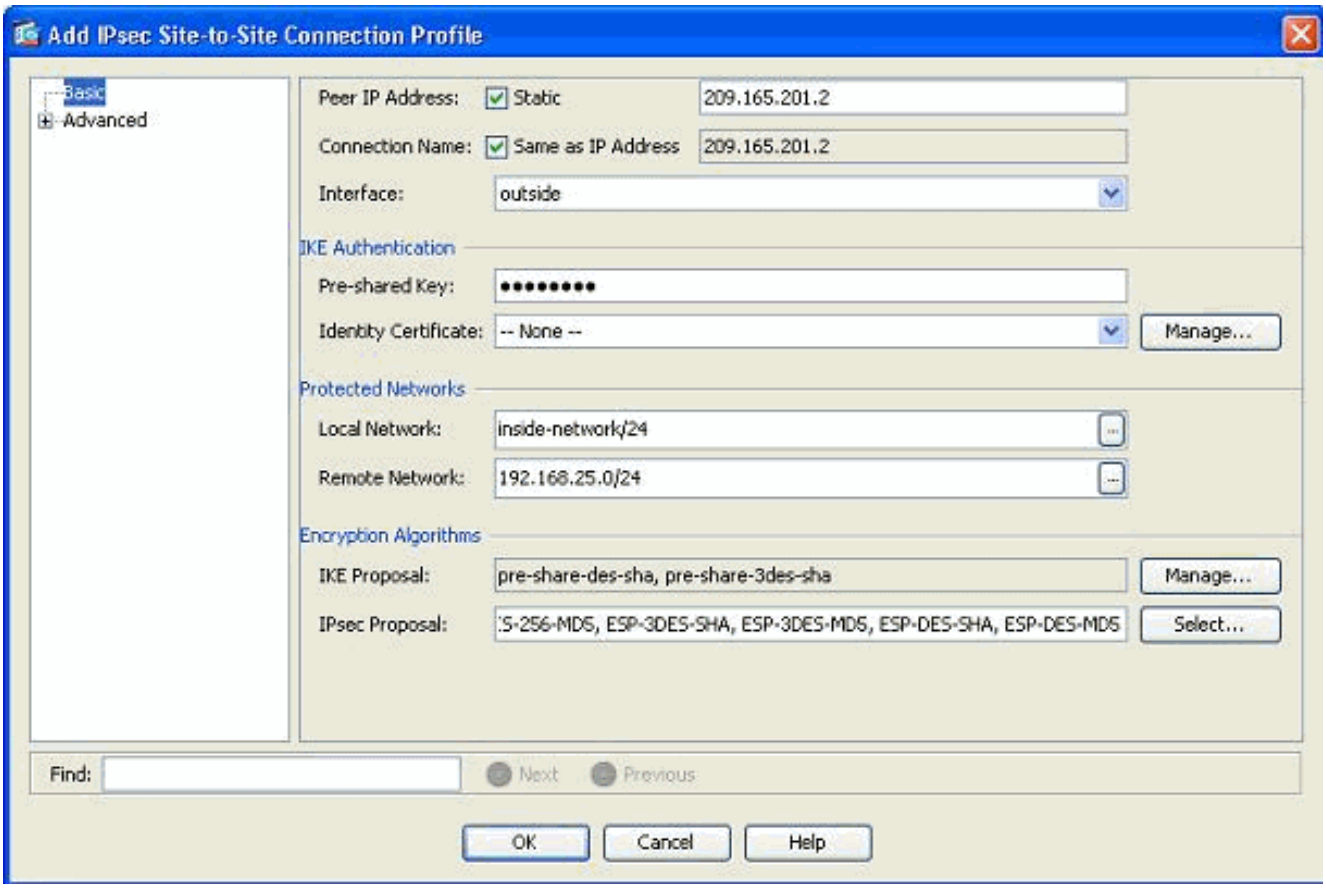
Esse pode ser o método mais fácil, pois não perturba a configuração de VPN existente e pode criar um novo perfil de conexão com as novas informações relacionadas ao ponto VPN.

1. Vá para *Configuration > Site-to-Site VPN > Connection Profiles* e clique em *Add* na área Connection
   Profiles.

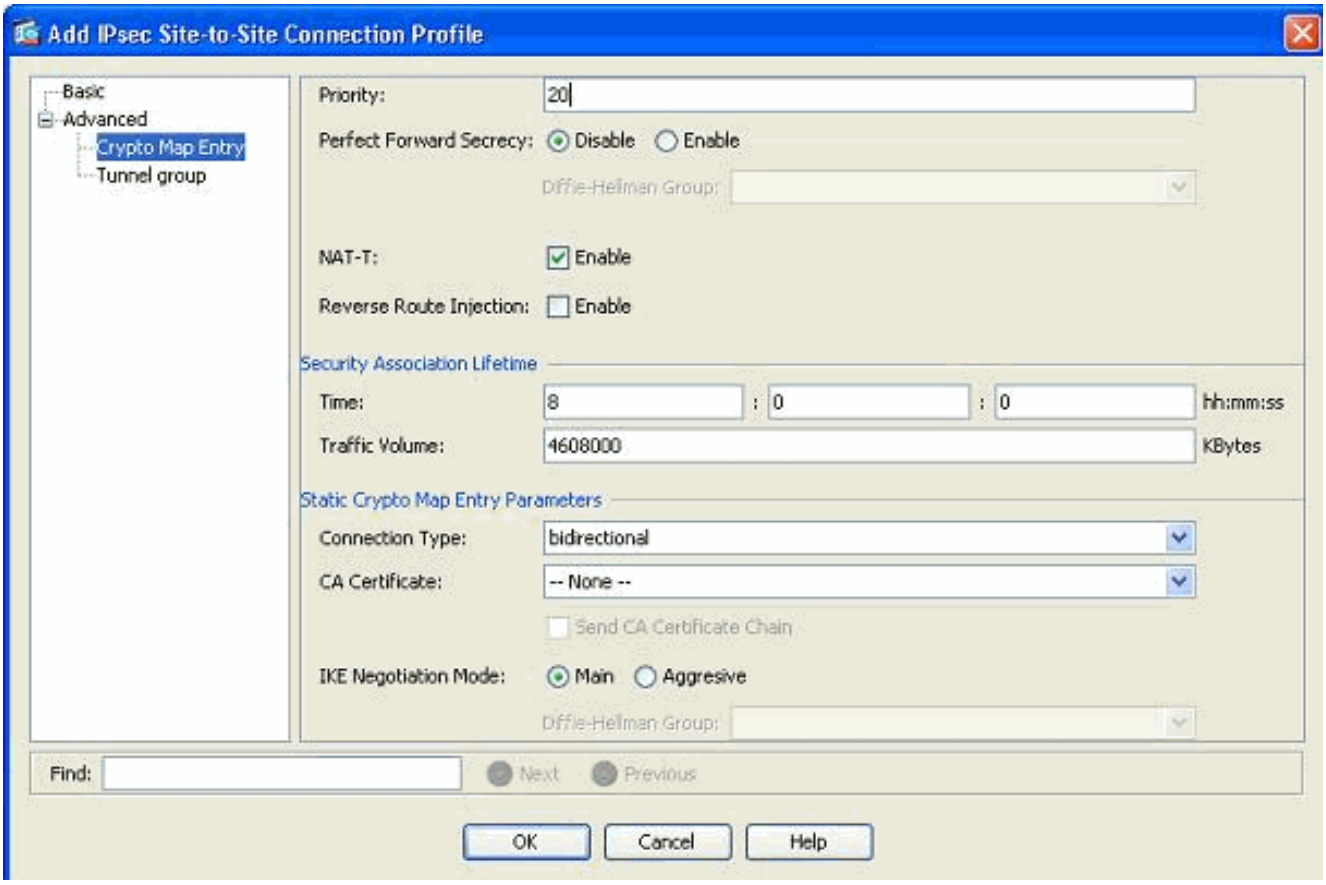


A janela *Add IPSec Site-to-Site Connection Profile* é aberta.

2. Na guia Basic, forneça os detalhes de *Peer IP Address*, *Pre-shared Key* e *Protected Networks*. Use todos os mesmos parâmetros da VPN existente, exceto as informações do peer. Click
OK.



3. No menu Avançado, clique em *Crypto Map Entry*. Consulte a guia *Prioridade*. Essa prioridade é igual ao número de sequência em sua configuração de CLI equivalente. Quando um número menor do que a entrada existente do mapa de criptografia é atribuída, esse novo perfil é executado primeiro. Quanto maior o número de prioridade, menor o valor. Isso é usado para alterar a ordem da sequência em que um mapa de criptografia específico será executado. Clique em *OK* para concluir a criação do novo perfil de conexão.



Isso cria automaticamente um novo grupo de túneis junto com um mapa de criptografia associado. Certifique-se de poder acessar o BQASA com o novo endereço IP antes de usar esse novo perfil de conexão.

Edite a Configuração de VPN Existente

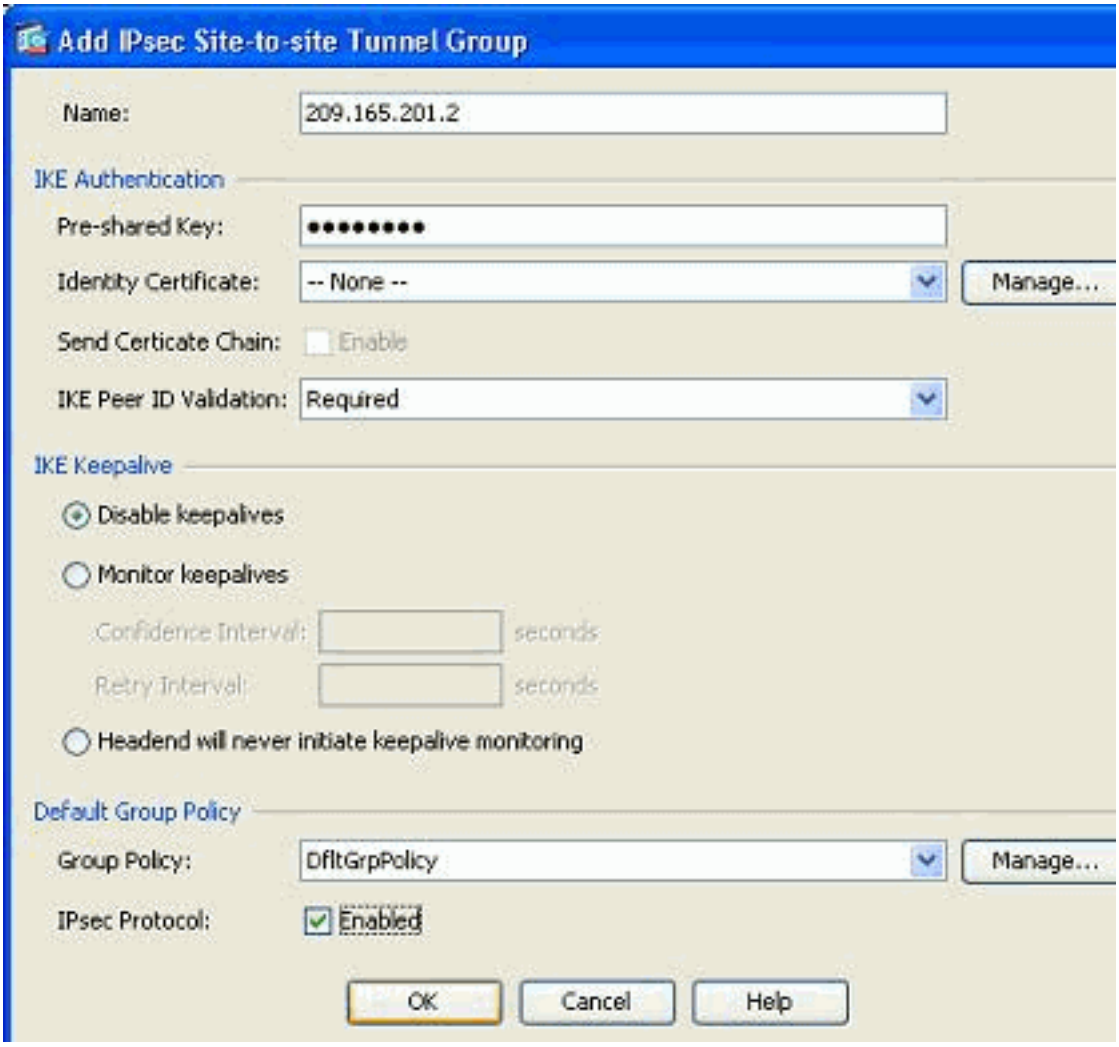
Outra maneira de adicionar um novo peer é modificar a configuração existente. O perfil de conexão existente não pode ser editado para as informações do novo peer porque está vinculado a um peer específico. Para editar a configuração existente, você precisa executar estas etapas:

1. Criar um novo grupo de túneis
2. Edite o Mapa de Criptografia Existente

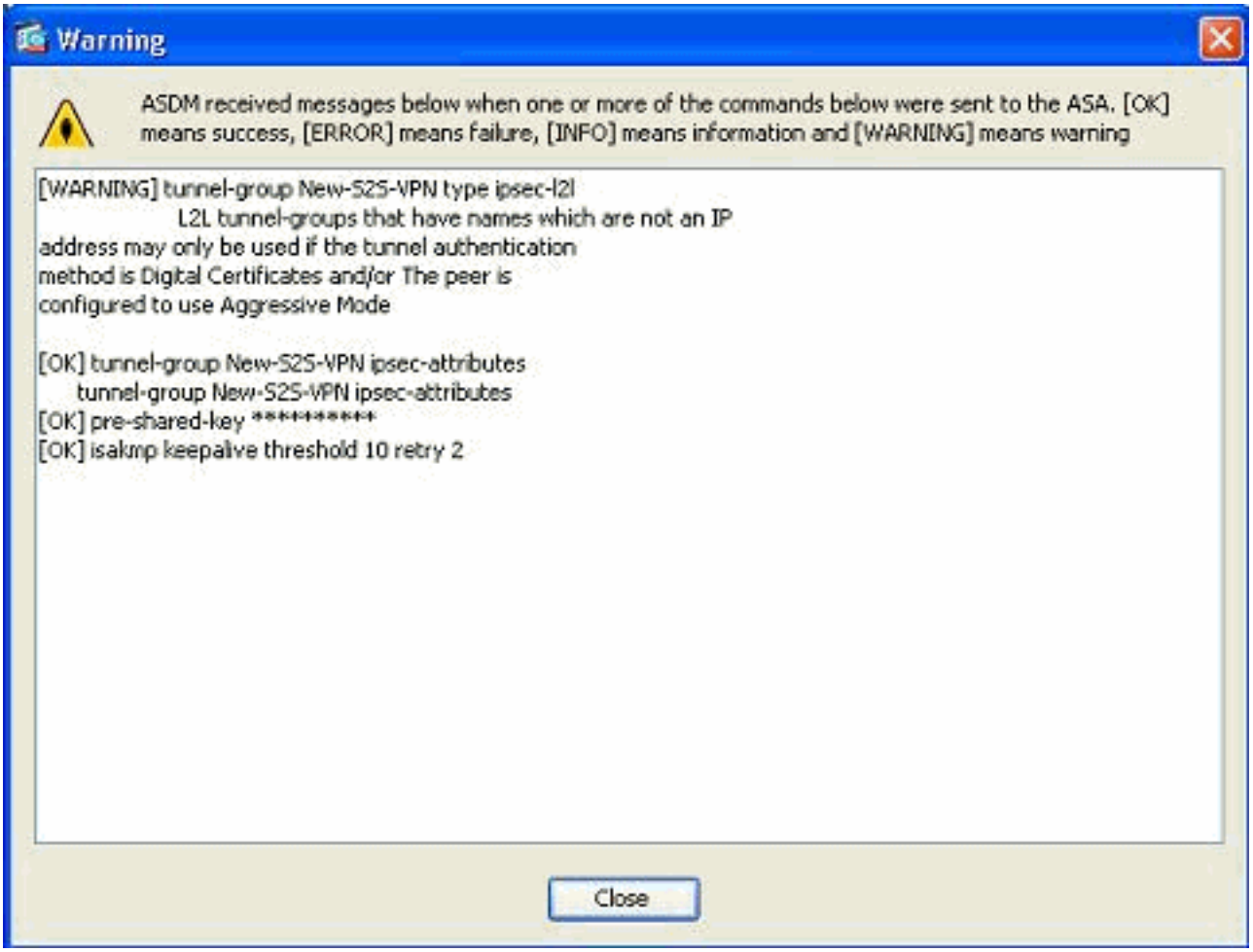
Criar um novo grupo de túneis

Vá para *Configuration > Site-to-Site VPN > Advanced > Tunnel groups* e clique em *Add* para criar um novo grupo de túneis que contenha as novas informações de pares de VPN. Especifique os campos *Nome* e *Chave pré-compartilhada* e clique em *OK*.

Observação: verifique se a chave pré-compartilhada corresponde à outra extremidade da VPN.



Observação: no campo Nome, somente o endereço IP do peer remoto deve ser inserido quando o modo de autenticação for chaves pré-compartilhadas. Qualquer nome pode ser usado somente quando o método de autenticação é por meio de certificados. Este erro aparece quando um nome é adicionado no campo Nome e o método de autenticação é pré-compartilhado:

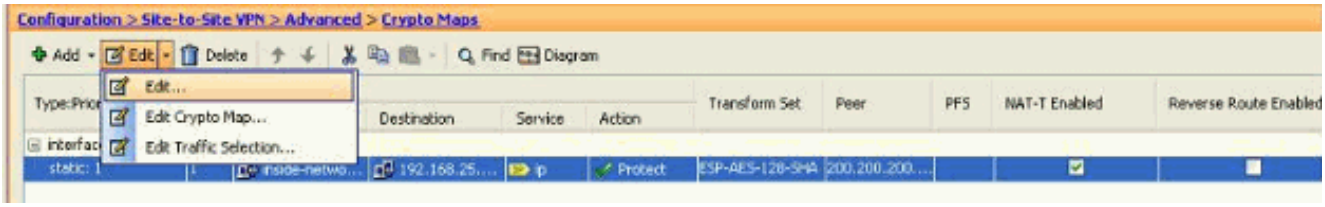


Edite o Mapa de Criptografia Existente

O mapa de criptografia existente pode ser editado para associar as novas informações de peer.

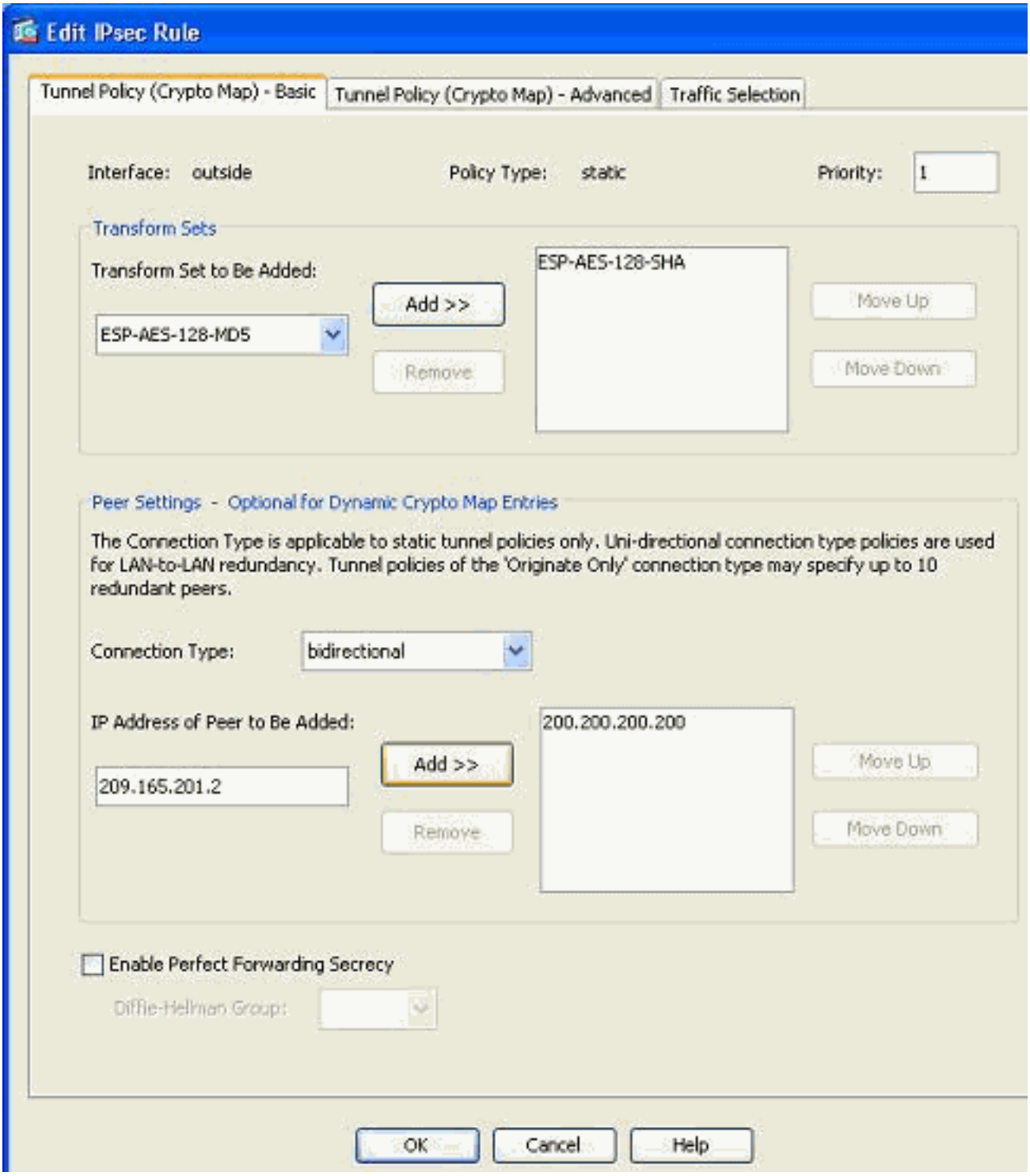
Conclua estes passos:

1. Vá para *Configuration > Site-to-Site VPN > Advanced > Crypto Maps*, selecione o mapa de criptografia necessário e clique em *Edit*.

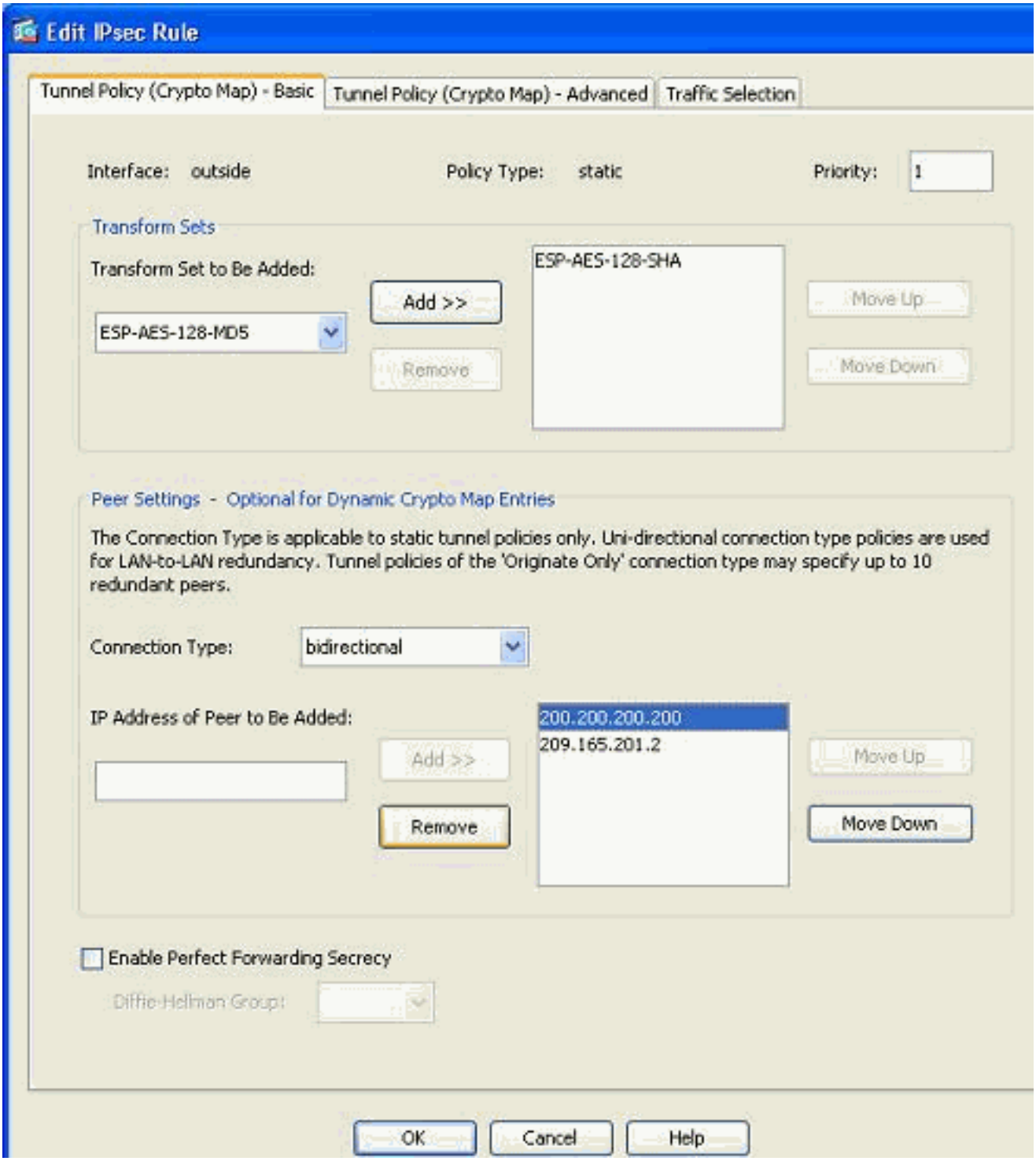


A janela *Editar regra de IPSec* é exibida.

2. Na guia Política de túnel (Básica), na área Configurações do peer, especifique o novo peer no campo Endereço IP do peer a ser adicionado. Em seguida, clique em *Adicionar*.

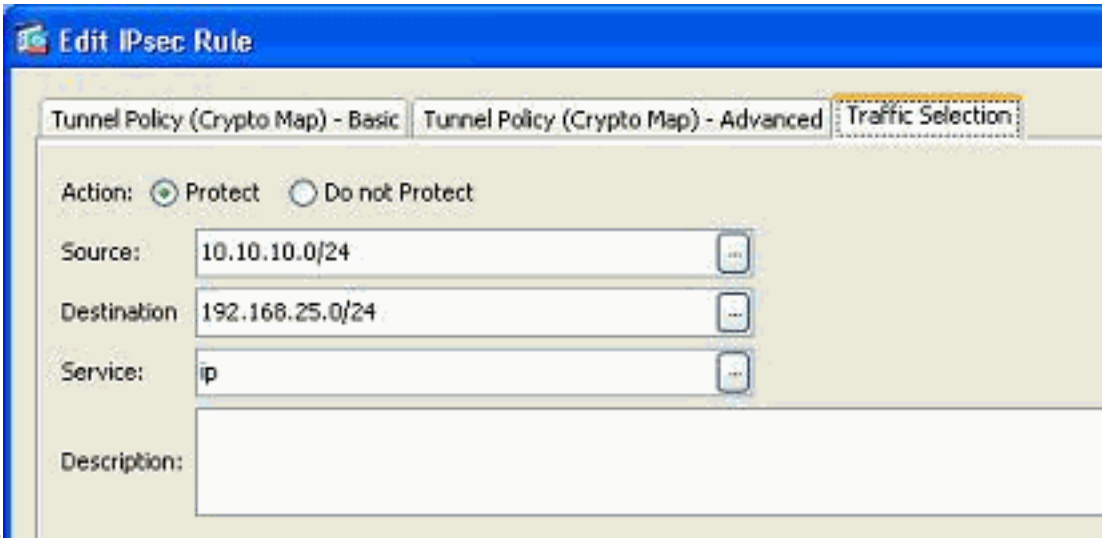


3. Selecione o endereço IP do peer existente e clique em *Remover* para manter as informações do novo peer somente. Click *OK*.



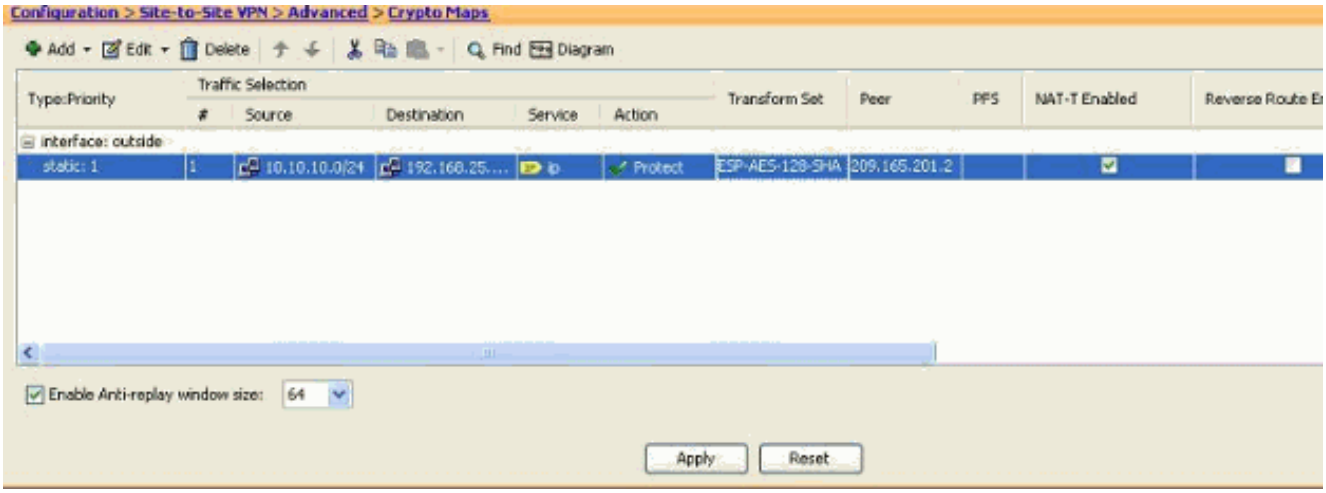
Observação: depois de modificar as informações do peer no mapa de criptografia atual, o perfil de conexão associado a esse mapa de criptografia é excluído instantaneamente na janela do ASDM.

4. Os detalhes das redes criptografadas permanecem os mesmos. Se precisar modificá-los, vá para a guia *Seleção de*



tráfego.

5. Vá para o painel *Configuração > VPN Site a Site > Avançado > Mapas de Criptografia* para exibir o mapa de criptografia modificado. No entanto, essas alterações não ocorrerão até você clicar em *Aplicar*. Depois de clicar em *Apply*, vá para o *menu Configuration > Site-to-Site VPN > Advanced > Tunnel groups* para verificar se um grupo de túneis associado está presente ou não. Se sim, um *perfil de conexão* associado será criado.



Verificar

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

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

- Use este comando para exibir os parâmetros de associação de segurança específicos para um único peer:show crypto ipsec sa peer <endereço IP do peer>

Troubleshoot

Use esta seção para resolver problemas de configuração.

Iniciador IKE incapaz de encontrar a política: Intf test_ext, Src: 172.16.1.103, Data: 10.1.4.251

Esse erro é exibido nas mensagens de log ao tentar alterar o peer VPN de um VPN Concentrator para o ASA.

Solução:

Isso pode ser resultado de etapas de configuração inadequadas seguidas durante a migração. Certifique-se de que a ligação de criptografia à interface seja removida antes de adicionar um novo peer. Além disso, certifique-se de usar o endereço IP do peer no grupo de túneis, mas não o nome.

Informações Relacionadas

- VPN site a site (L2L) com ASA
- Problemas mais comuns de VPN
- Página de suporte técnico do ASA
- Suporte Técnico e Documentação - Cisco Systems