ASDM 6.4: Túnel do VPN de Site-para-Site com exemplo de configuração IKEv2

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Informações de Apoio
Configurar
Diagrama de Rede
Configuração ASDM em HQ-ASA
Verificar
Troubleshooting
Comandos para Troubleshooting
Informações Relacionadas

Introdução

Este documento descreve como configurar um túnel VPN de site a site entre duas Cisco Adaptive Security Appliances (ASAs) que usam Internet Key Exchange (IKE) versão 2. Ele descreve as etapas usadas para configurar o túnel VPN usando um assistente de GUI do Adaptive Security Device Manager (ASDM).

Pré-requisitos

Requisitos

Certifique-se de que Cisco ASA esteve configurado com as configurações básicas.

Componentes Utilizados

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

- Dispositivos de segurança adaptáveis Cisco ASA série 5500 que executa a versão de software 8.4 e mais atrasado
- Versão 6.4 e mais recente do software ASDM de Cisco

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.

Convenções

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

Informações de Apoio

IKEv2, é um realce ao protocolo IKEv1 existente que inclui estes benefícios:

- Menos trocas da mensagem entre pares IKE
- Métodos de autenticação unidirecional
- Suporte embutido para o Dead Peer Detection (DPD) e o NAT-Traversal
- Uso do Extensible Authentication Protocol (EAP) para a autenticação
- Elimina o risco de ataques simples DoS usando Cookie antiobstrução

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

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

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Este documento mostra a configuração do túnel do VPN de Site-para-Site em HQ-ASA. O mesmos podiam ser seguidos que um espelho no BQ-ASA.

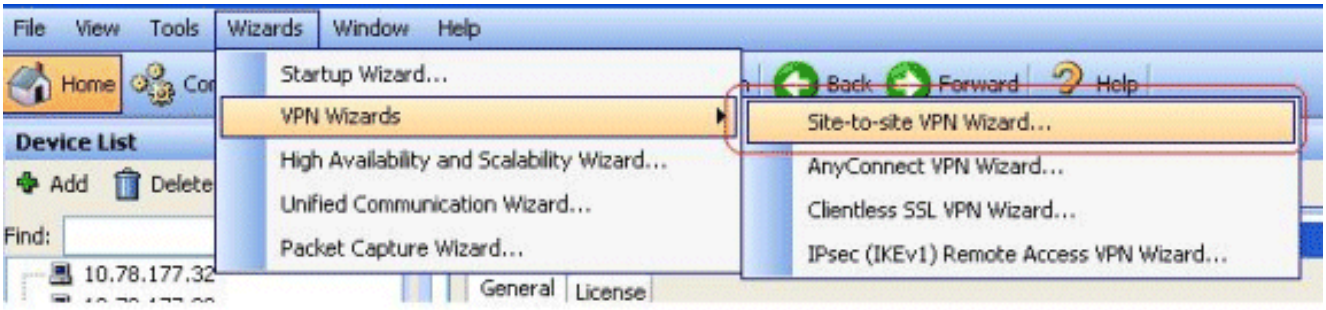
Configuração ASDM em HQ-ASA

Este túnel VPN podia ser configurado usando um assistente fácil de usar GUI.

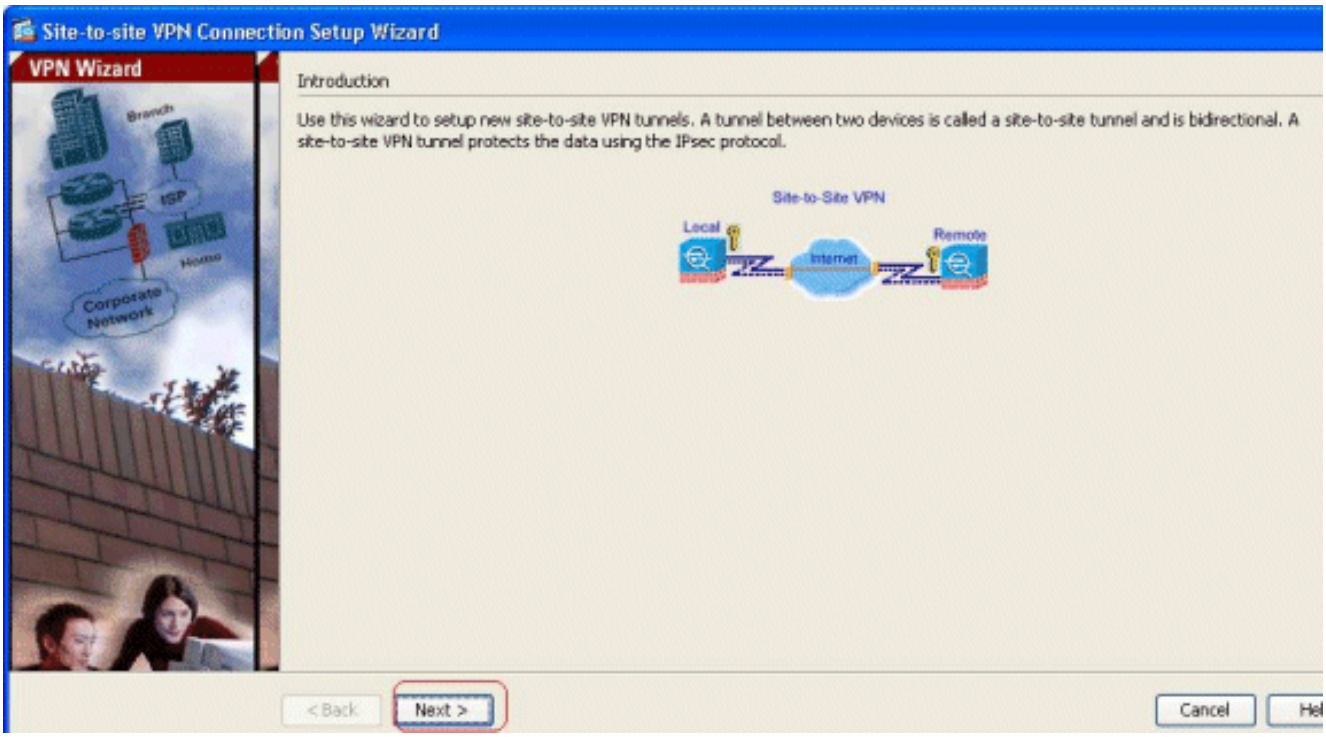
Conclua estes passos:

1. Entre ao ASDM, e vá aos **assistentes** > aos **wizard VPN** > ao **assistente do VPN de Site-**

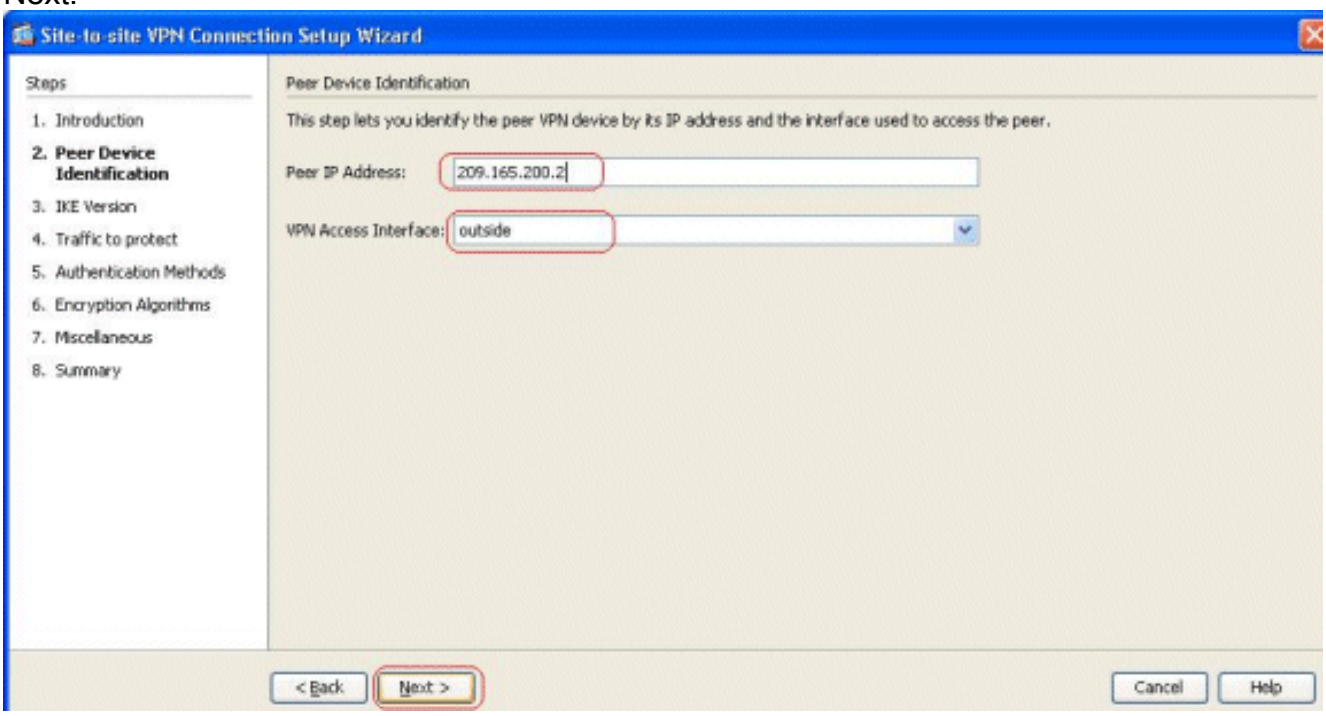
para-
Site.



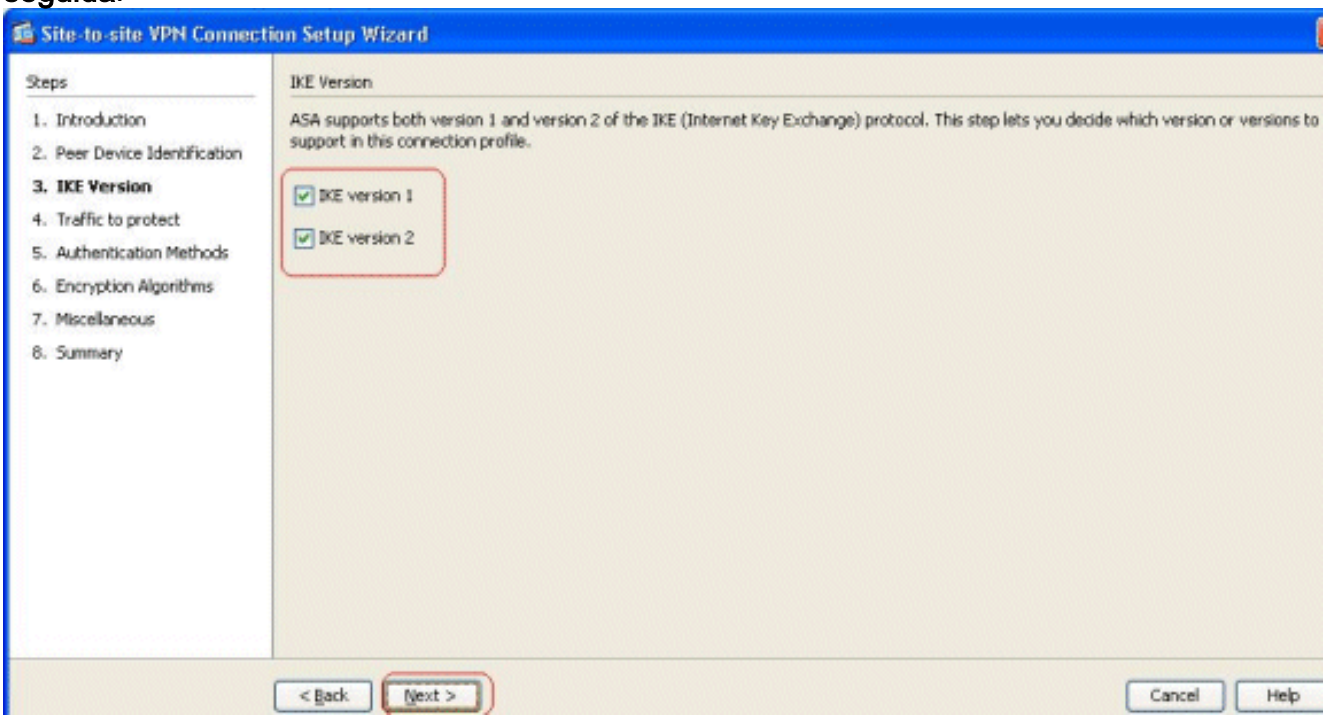
2. Um indicador da instalação de conexão do VPN de Site-para-Site aparece. Clique em Next.



3. Especifique o endereço IP do peer e a interface de acesso VPN. Clique em Next.

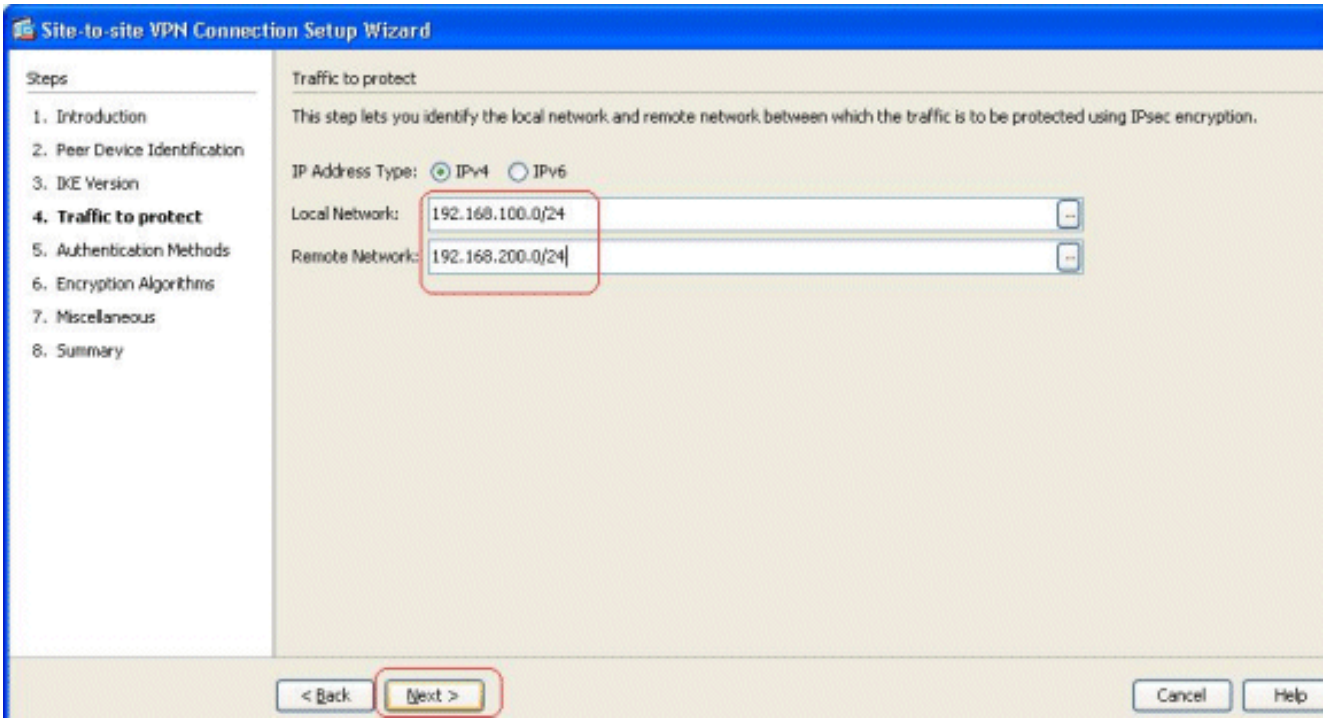


4. Selecione ambas as versões IKE, e clique-as **em seguida**.

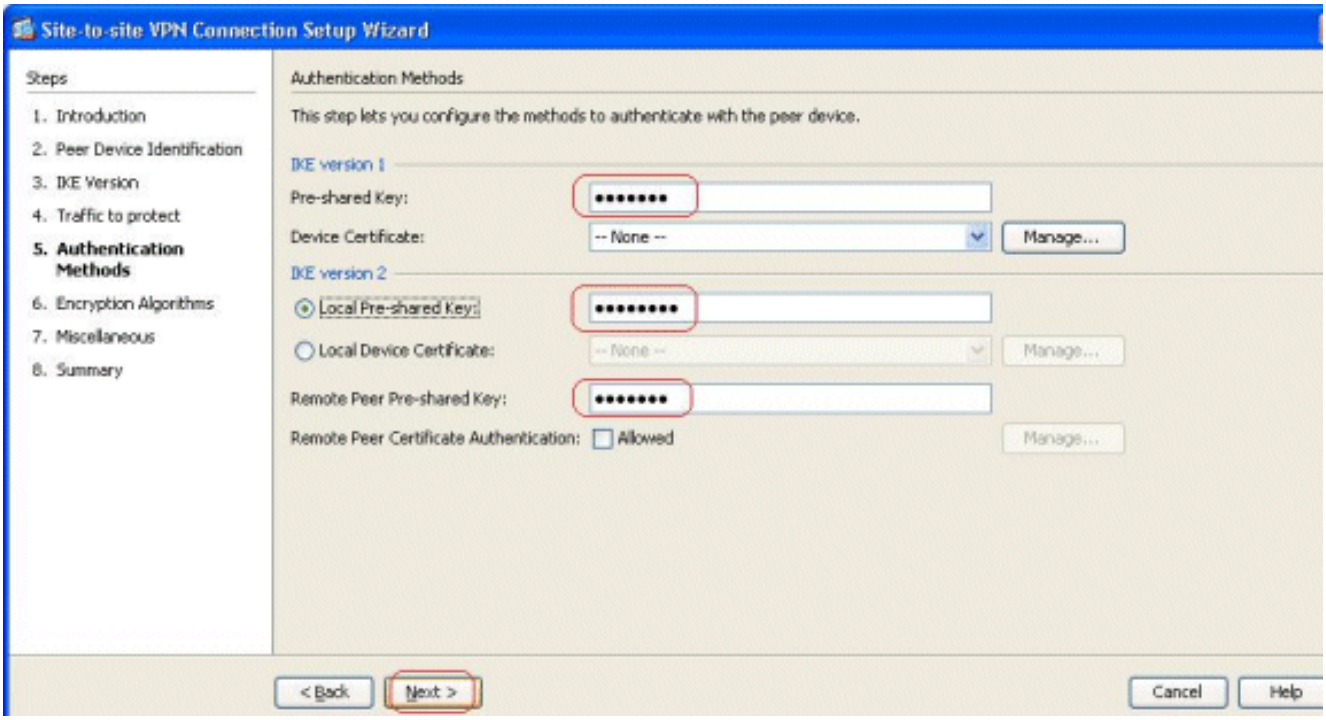


Nota: Ambas as versões do IKE são configuradas aqui porque o iniciador poderia ter um backup de IKEv2 a IKEv1 quando IKEv2 falha.

5. Especifique a rede local e a rede remota de modo que o tráfego entre estas redes seja cifrado e passado através do túnel VPN. Clique em Next.

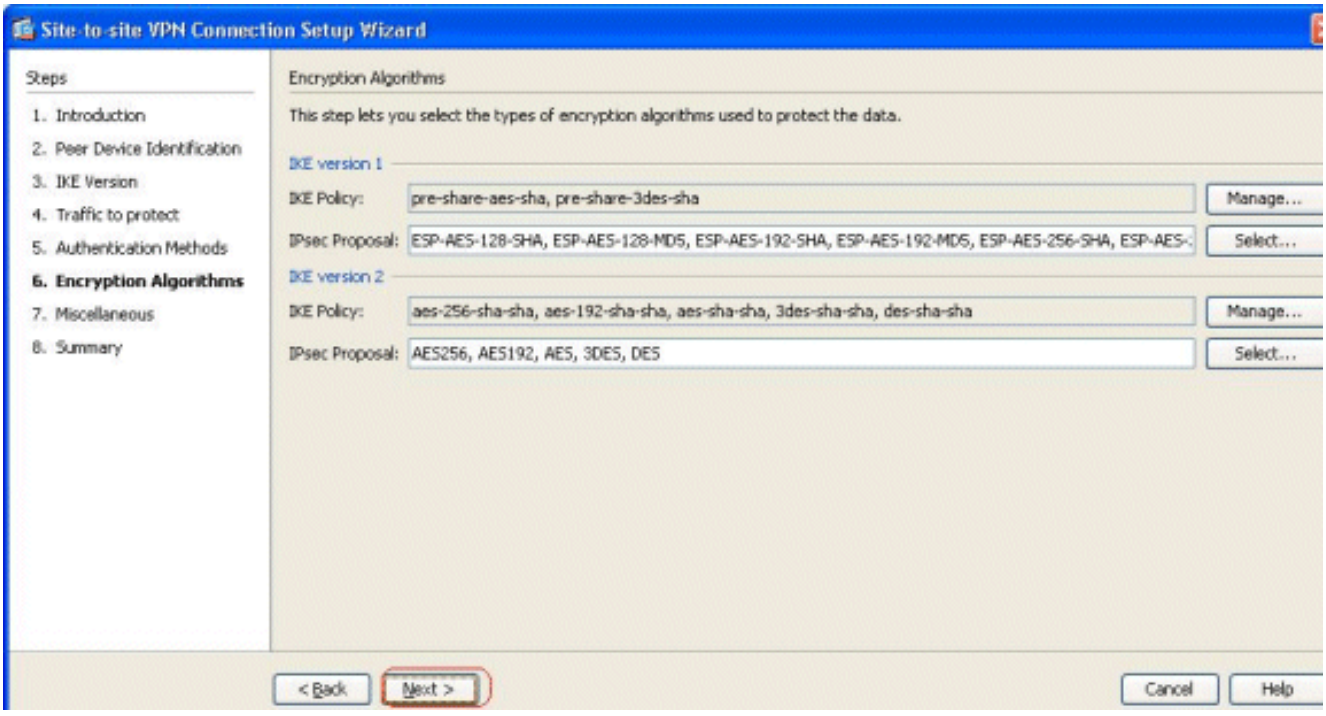


6. Especifique as chaves pré-compartilhada para ambas as versões do IKE.



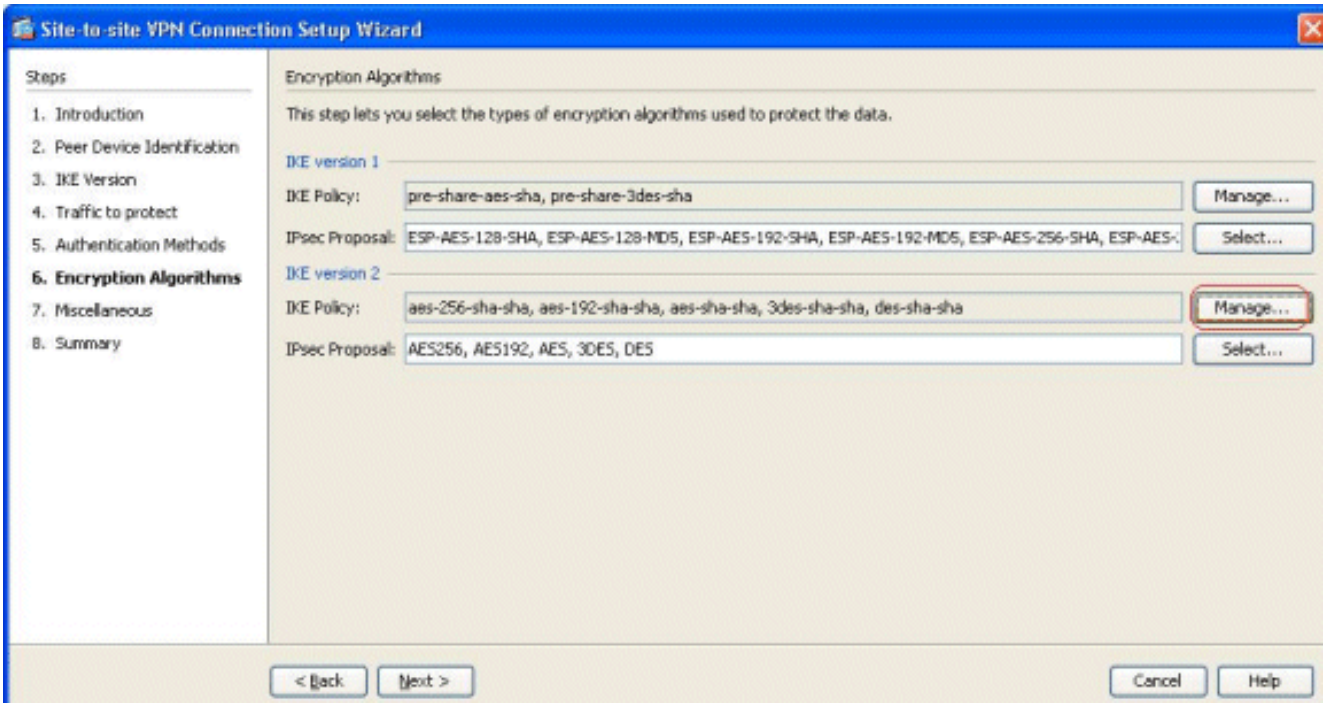
A diferença principal entre versões 1 e 2 IKE encontra-se em termos do método de autenticação que permitem. IKEv1 permite somente um tipo de autenticação em ambas as extremidades VPN (isto é, chave pré-compartilhada ou certificado). Contudo, IKEv2 permite que os métodos de autenticação assimétricos sejam configurados (isto é, autenticação da chave pré-compartilhada para o autor, mas certificado de autenticação para o que responde) usando o local separado e a autenticação remota CLI.Mais, você pode ter chaves pré-compartilhada diferentes no ambas as extremidades. A chave pré-compartilhada local na extremidade HQ-ASA transforma-se a chave pré-compartilhada remota na extremidade BQ-ASA. Igualmente, a chave pré-compartilhada remota na extremidade HQ-ASA transforma-se a chave pré-compartilhada local na extremidade BQ-ASA.

7. Especifique os algoritmos de criptografia para ambas as versões 1 e 2 IKE. Aqui, os valores padrão são
aceitados:



8. O clique **controla…** a fim alterar a política de

IKE.

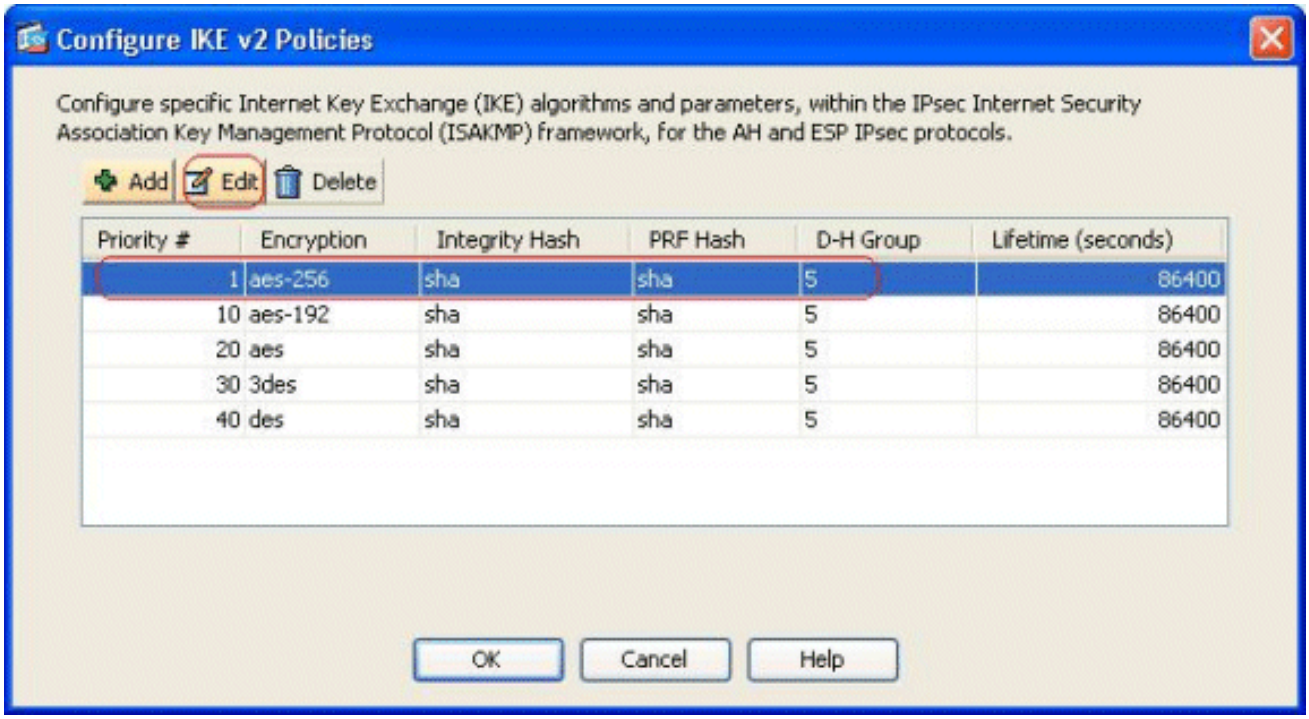


Nota: A política de IKE em IKEv2 é sinônima à **política de ISAKMP em** IKEv1.**A proposta do IPsec em** IKEv2 é sinônima à **transformação ajustada em** IKEv1.

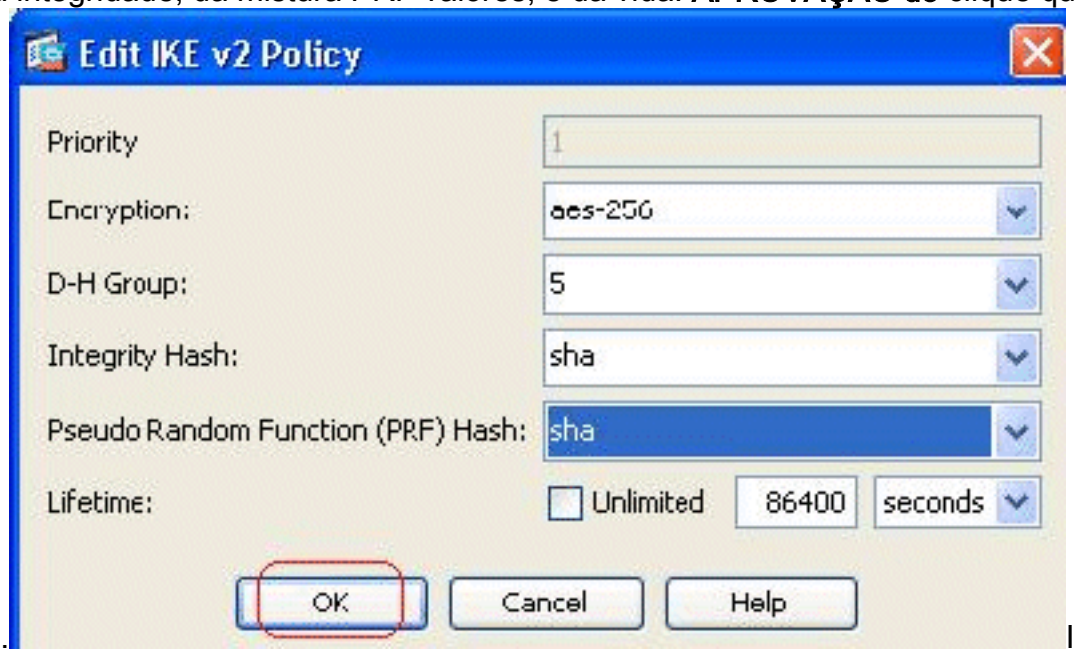
9. Esta mensagem aparece quando você tenta alterar a política existente:

APROVAÇÃO do clique a fim continuar.

10. Selecione a política de IKE especificada, e o clique **edita**.

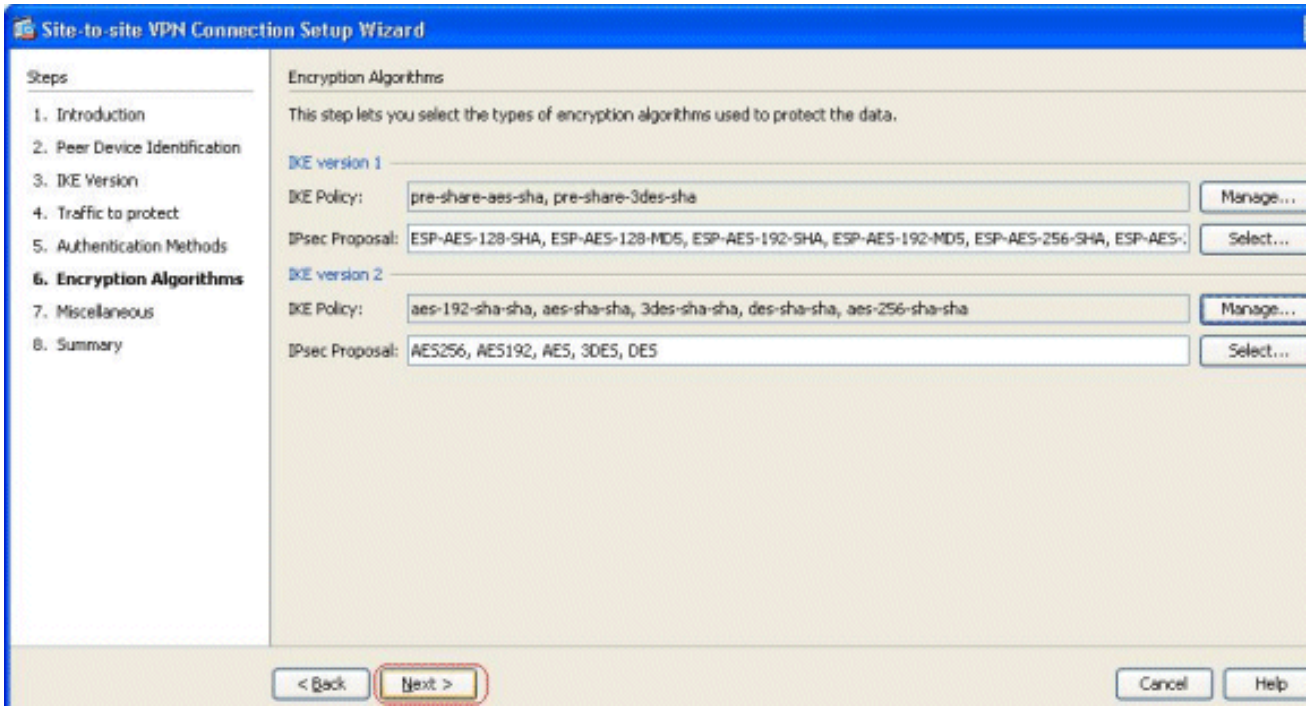


11. Você pode alterar os parâmetros tais como a prioridade, a criptografia, o grupo do D-H, a mistura da integridade, da mistura PRF valores, e da vida. **APROVAÇÃO do** clique quando terminado.



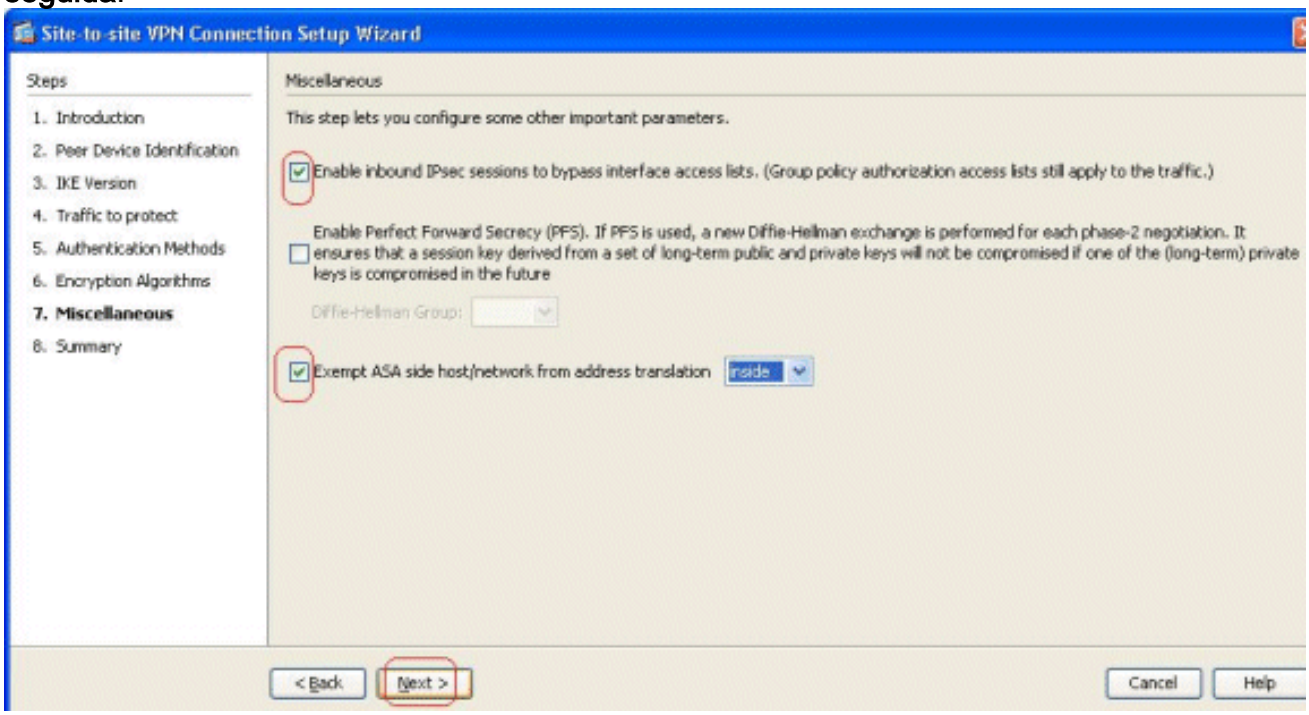
IKEv2 permite o algoritmo da integridade ser negociado separadamente do algoritmo aleatório pseudo- da função (PRF). Isto podia ser configurado na política de IKE com as opções disponíveis atuais que são SHA-1 ou MD5.Você não pode alterar os parâmetros da proposta do IPsec que são definidos à revelia. Clique **seleto** ao lado do campo da proposta do IPsec a fim adicionar parâmetros novos. A diferença principal entre IKEv1 e IKEv2, em termos das propostas do IPsec, é que IKEv1 aceita a transformação ajustada em termos das combinações de criptografia e de algoritmos de autenticação. IKEv2 aceita os parâmetros da criptografia e da integridade individualmente, e faz finalmente todo o possível OU combinações destes. Você poderia ver estes na extremidade deste assistente, na corrediça sumária.

12. Clique em Next.

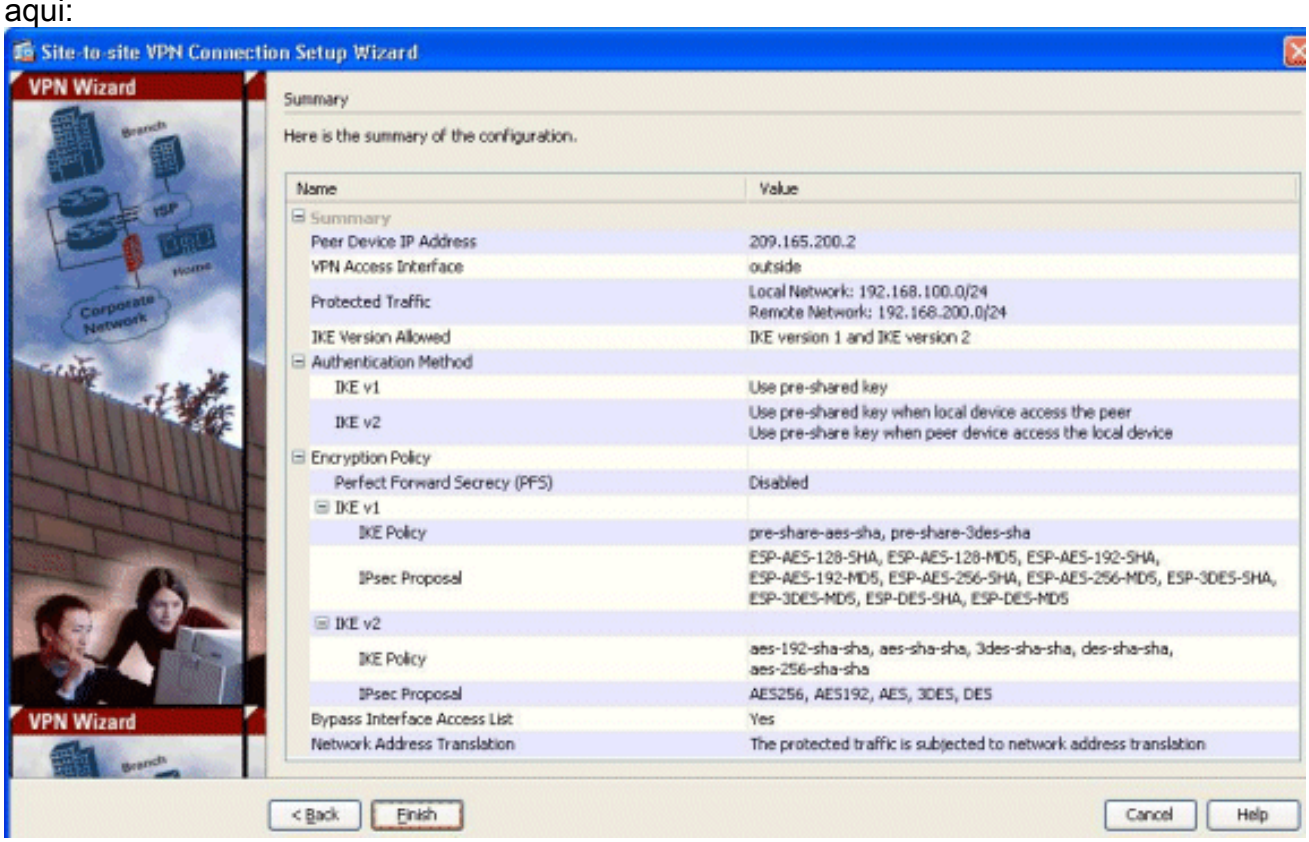


13. Especifique os detalhes, tais como a isenção de NAT, o PFS, e contornear da relação ACL. Escolha **em**

seguida.



14. Um sumário da configuração pode ser considerado aqui:



Revestimento do clique a fim terminar o assistente do túnel do VPN de Site-para-Site. Um perfil da nova conexão é criado com os parâmetros configurados.

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.

- mostre ikev2 criptos sa - Indica IKEv2 o base de dados tempo de execução SA.
- mostre VPN-sessiondb o detalhe l2l - Indica a informação sobre sessões do VPN de Site-para-Site.

Troubleshooting

Comandos para Troubleshooting

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.

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

- debug crypto ikev2 - As mostras **debugam** mensagens para IKEv2.

Informações Relacionadas

- Suporte técnico dos dispositivos do 5500 Series de Cisco ASA
- Suporte Técnico e Documentação - Cisco Systems