Conectividade site a site com sub-redes sobrepostas no Cisco Secure Access

Contents

Introdução

Este documento descreve a solução de sub-rede sobreposta do Cisco Secure Access.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Administração do Cisco Secure Access.
- Administração de firewall/roteador.

A Cisco recomenda que você:

- Acesso administrativo ao Cisco Secure Access.
- Acesso administrativo ao dispositivo IPSec Headend (firewall ou roteador)

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Antes de Começar

Neste exemplo, há dois sites de filial diferentes com a mesma sub-rede IP 192.168.200.0/24, nos quais eles estão conectados ao Cisco Secure Access através de dois túneis IPSec separados.

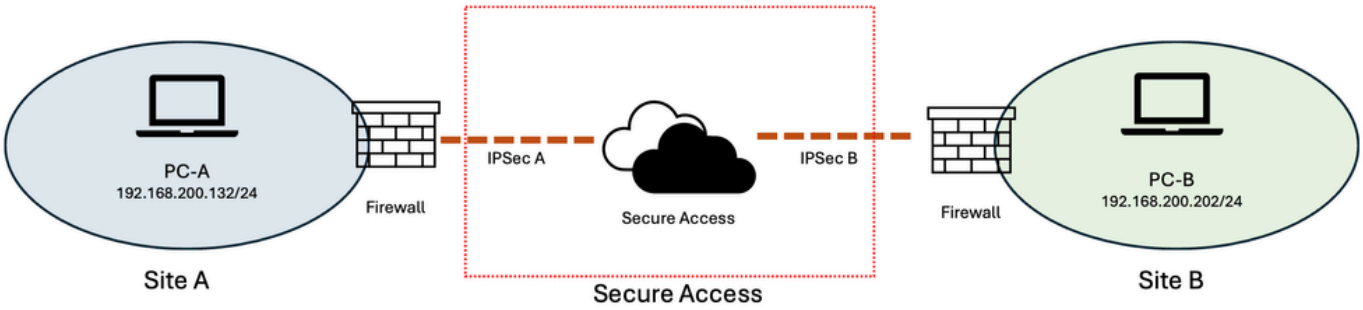


Imagem - Diagrama de rede

O objetivo é que os usuários do "Site A" possam acessar os recursos do "Site B" e vice-versa.

Preparação e Planejamento

Como ambos os sites usam a mesma sub-rede IP (`192.168.200.0/24`), o espaço de endereço sobreposto impede a comunicação direta entre os dois sites. Para resolver essa sobreposição, duas sub-redes virtuais sem sobreposição são atribuídas para representar os recursos em cada site.

Neste exemplo:

- Local A: `10.30.30.0/24`

- Local B: `10.40.40.0/24`
- Sub-rede real em ambos os locais: `192.168.200.0/24`

As sub-redes virtuais fornecem espaços de endereços exclusivos para cada site, enquanto os recursos reais continuam a usar seus endereços `192.168.200.0/24` existentes.

Quando um usuário no Site A acessa um recurso localizado no Site B, o usuário acessa o recurso através da sub-rede virtual do Site B (10.40.40.0/24) em vez de usar diretamente o espaço de endereço de sobreposição 192.168.200.0/24.

O Cisco Secure Access fornece um recurso de NAT de destino um a um (D-NAT) que pode converter os endereços virtuais para os endereços reais correspondentes. O intervalo de endereços D-NAT tem o mesmo tamanho da sub-rede original. Neste exemplo, as redes virtual e real são sub-redes `/24`, fornecendo um mapeamento um para um entre os endereços IP virtual e real.

Por exemplo:

`10.40.40.202` → `192.168.200.202`

Portanto, uma solicitação do Site A destinada a `10.40.40.202` é convertida pelo D-NAT para `192.168.200.202`, permitindo que a solicitação alcance o recurso correspondente no Site B, apesar de ambos os sites usarem a mesma sub-rede IP subjacente.

Essa abordagem cria efetivamente um espaço de endereço virtual sem sobreposição para cada site, preservando o endereçamento IP existente dos recursos. Ele também fornece uma relação consistente de um para um entre os endereços virtual e real, facilitando a compreensão, o gerenciamento e a solução de problemas da configuração.

Configuration Steps

Devido ao design atual e às limitações do Cisco Secure Access, atingir esse cenário requer configuração nos dispositivos headend por trás dos túneis IPsec e no Cisco Secure Access.

O dispositivo headend é o firewall ou roteador que estabelece o túnel IPsec para o Cisco Secure Access. Além de configurar o D-NAT no Cisco Secure Access, o firewall do headend também deve executar o NAT de origem (S-NAT) para o tráfego de retorno.

Portanto, a configuração consiste em duas seções:

1. Configurando o NAT de destino (D-NAT) no Cisco Secure Access para cada túnel de rede separadamente.
2. Configurando o NAT de origem (S-NAT) nos firewalls para garantir que o tráfego de retorno seja convertido de volta para o espaço de endereço virtual.

Configurando o Cisco Secure Access

Passo 1: No portal de gerenciamento do Cisco Secure Access, navegue para Connect > Network Connections e selecione a guia Network Tunnel Groups.

Passo 2: Edite o Grupo de Túneis de Rede associado ao túnel IPsec para o site que usa a sub-rede sobreposta.

Neste exemplo:

- IPSec-A = Network Tunnel Group para o site A
- IPSec-B = Network Tunnel Group para o Site B

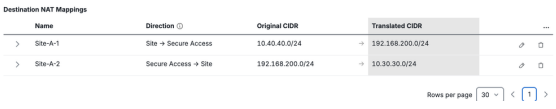
Passo 3: Clique no menu de três pontos ao lado do Network Tunnel Group necessário e selecione Edit.

Passo 4: No menu à esquerda, selecione a guia Routing e habilite Network Address Translation (NAT) se ela ainda não estiver habilitada.

Passo 5: Em Mapeamentos NAT de destino, clique em Adicionar mapeamentos.

Passo 6: Use esta tabela para configurar os mapeamentos de D-NAT para cada grupo de túnel de rede:

	Site A - Túnel IPSec	Local B - Túnel IPSec
NAT-1 de destino	Site → acesso seguro CIDR original: 10.40.40.0/24 CIDR traduzido: 192.168.200.0/24	Site → acesso seguro CIDR original: 10.30.30.0/24 CIDR traduzido: 192.168.200.0/24

NAT-2 de destino	Acesso seguro → site CIDR original: 192.168.200.0/24 CIDR traduzido: 10.30.30.0/24	Acesso seguro → site CIDR original: 192.168.200.0/24 CIDR traduzido: 10.40.40.0/24
	 IPsec Tunnel Site A - Configuração de D-NAT	 IPsec Tunnel Site B - Configuração de D-NAT

Note: Depois de definir as configurações para cada grupo de túnel de rede, clique em Save. Quando a janela de confirmação for exibida, digite UPDATE para confirmar a alteração. Repita o mesmo procedimento para o outro Network Tunnel Group

Configurando o firewall

A configuração do firewall é necessária devido a uma limitação atual no tratamento de sub-redes IP sobrepostas atrás de Grupos de Túnel de Rede.

Quando o Cisco Secure Access executa o D-NAT em um pacote recebido, o endereço destino convertido é usado para entregar o pacote ao recurso destino. No entanto, a conversão reversa correspondente não é executada automaticamente para o tráfego de retorno nesse cenário de sub-rede sobreposta.

Como resultado, o tráfego de retorno precisa ser manualmente NAT de origem no firewall.

O principal requisito é que o servidor de destino veja o tráfego de retorno usando o endereço IP virtual que o cliente acessou originalmente, em vez do endereço IP real do servidor.

Exemplo

Considere o seguinte:

- Cliente do site A: `192.168.200.132`
- Servidor Web do Site B: `192.168.200.202`
- Sub-rede virtual do local B: `10.40.40.0/24`
- Endereço virtual do servidor Web: `10.40.40.202`

O cliente no Site A acessa o servidor Web do Site B usando https://10.40.40.202

O Cisco Secure Access executa o D-NAT `10.40.40.202 → 192.168.200.202`

O pacote então alcança o Servidor web em `192.168.200.202`.

O problema ocorre com o tráfego de retorno. Sem NAT adicional no firewall, o servidor Web gera a resposta com Source: `192.168.200.202`

No entanto, o cliente iniciou a conexão com o Destino: `10.40.40.202`

Portanto, o tráfego de retorno precisa ser convertido para que o endereço de origem apresentado ao cliente corresponda ao endereço virtual `192.168.200.202 → 10.40.40.202`

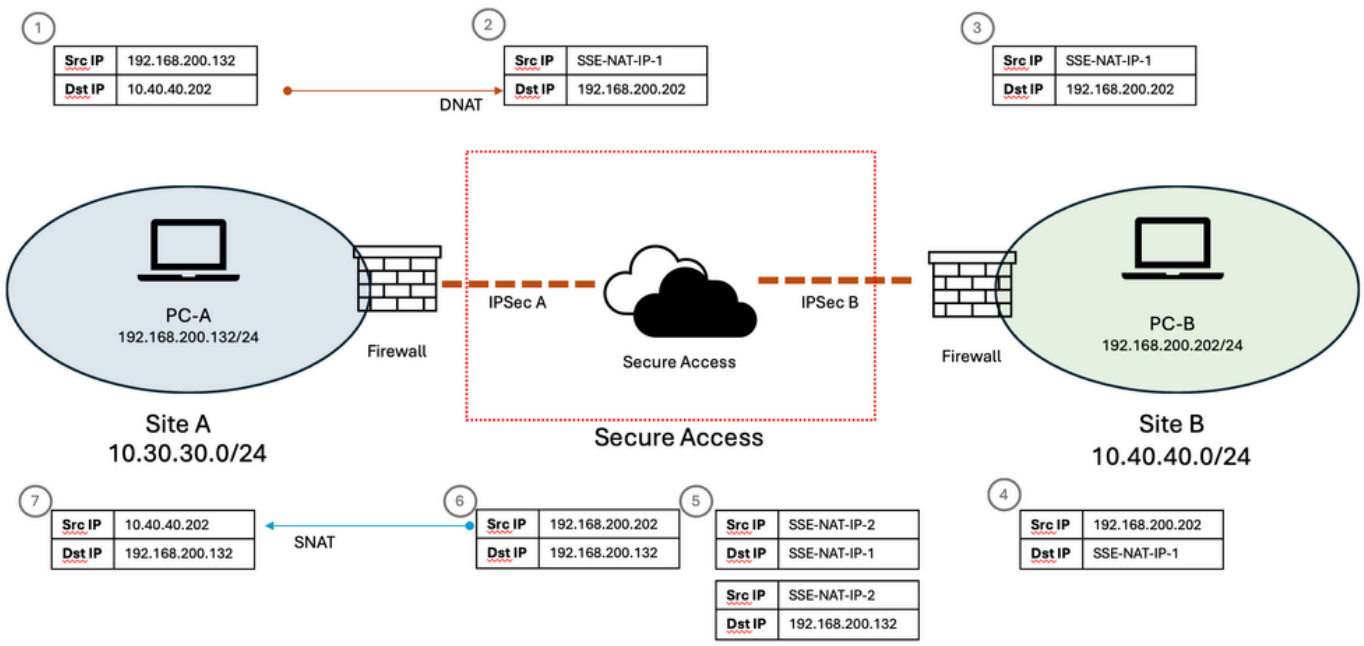


Imagem - Fluxo de rede

Para conseguir isso, o firewall executa o NAT de origem no tráfego que sai em direção ao grupo de túnel de rede.

Para este exemplo, o mapeamento necessário é`192.168.200.0/24 → 10.40.40.0/24`

Isso cria uma relação um a um inversa entre os endereços reais e seus endereços virtuais correspondentes.

SNAT um para um

Se o firewall suportar NAT de origem um para um para toda a sub-rede, uma única regra NAT pode representar o intervalo de endereços completo `/24`.

Por exemplo:

Fonte real	Fonte traduzida
`192.168.200.0/24`	`10.40.40.0/24`

Isso resulta em mapeamentos como `192.168.200.202 → 10.40.40.202` e `192.168.200.203 → 10.40.40.203`

A mesma relação um-para-um se aplica a toda a sub-rede.

Firewalls sem SNAT um para um

Se o firewall não suportar NAT de origem um para um para toda a sub-rede, cada mapeamento necessário deverá ser configurado individualmente.

Por exemplo, para o servidor Web:

- IP de origem: `192.168.200.202`
- Interface de origem: Grupo de Túneis de Rede
- Direção de tráfego: Entrada
- IP de Origem Convertido: `10.40.40.202`

A conversão resultante é`192.168.200.202 → 10.40.40.202`

A mesma abordagem pode ser aplicada a cada recurso que requer acesso por meio da sub-rede virtual.

Isso garante que ambas as direções da comunicação mantenham o esquema de endereçamento virtual e que o cliente receba a resposta do mesmo endereço IP virtual que usou ao estabelecer a conexão.

Informações Relacionadas

Mapeamento de NAT do Cisco Secure Access / configuração do grupo de túnel de rede : https://securitydocs.cisco.com/docs/csa/olh/168842.dita

Referência de configuração e roteamento do Cisco Secure Access Network Tunnel Group: https://securitydocs.cisco.com/docs/csa/olh/118900.dita

Solução de problemas do Cisco Secure Access e guia básico de coleta de dados: https://www.cisco.com/c/en/us/support/docs/security/secure-access/221240-troubleshoot-and-collect-basic-informati.html

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.