

Endereços Destino de Acesso Seguro para Configuração de Roteamento Dividido

Contents

Problema

Ao implantar o Cisco Secure Access (CSA) com o Cisco Secure Client (CSC) em endpoints do Windows em uma arquitetura de rede Hub-Spoke, as organizações provavelmente precisarão configurar o roteamento dividido para permitir que o tráfego do site Spoke se conecte diretamente ao CSA através do circuito de Internet Spoke local em vez de fazer hairpinning através do Hub. Essa configuração exige conhecimento de todos os endereços de destino da Cisco usados ao estabelecer o túnel CSA para que as exceções de roteamento (roteamento de breakout/divisão) possam ser definidas em dispositivos de rede, como firewalls Fortigate.

O requisito específico é identificar todas as informações de destino (endereços IP ou URLs) para os endpoints CSA usados pelo CSC ao estabelecer túneis TLS/DTLS, permitindo a configuração adequada de políticas de roteamento que ignoram o túnel VPN Hub-Spoke para o tráfego CSA.

Ambiente

- Implantação do Cisco Secure Access (CSA)
- Cisco Secure Client (CSC) em endpoints Windows
- Topologia de rede hub-spoke com firewalls Fortigate
- Conectividade de túnel TLS/DTLS para CSA

Resolução

Para configurar o roteamento dividido para conexões Cisco Secure Access, as informações de

destino descritas nas próximas seções devem ser configuradas no dispositivo Fortigate para permitir a conectividade direta com os pontos finais CSA.

Domínio e portas de destino CSA

Domínio Primário

`*.vpn.sse.cisco.com`

Portas e protocolos necessários

- TCP/UDP 443 Usado para estabelecimento de túnel TLS/DTLS
- UDP 500/4500: Usado para estabelecimento de túnel IPsec
- TCP 80: Usado para verificações de revogação de certificados VPN

Fortifique a abordagem de configuração

Configure as políticas de roteamento no dispositivo Fortigate para direcionar o tráfego destinado para o domínio CSA (`*.vpn.sse.cisco.com`) e as portas especificadas através do circuito de Internet Spoke local em vez de através do túnel VPN Hub-Spoke. Isso ativa o fluxo de tráfego descrito nos próximos códigos.

Fluxo de tráfego desejado

Spoke Site → CSA Tunnel Connection → CSA-mediated Internet Communication

Em vez de fluxo de tráfego através do local do hub

Spoke Site → Hub Site → CSA Tunnel Connection → CSA-mediated Internet Communication

Considerações importantes

Os destinos de conexão CSA são determinados dinamicamente durante o tempo de execução, o que significa que endereços IP específicos não podem ser predeterminados para a configuração de roteamento estático. A abordagem baseada em domínio usando *.vpn.sse.cisco.com fornece o método mais confiável para configurar políticas de roteamento dividido.

Consulte a documentação oficial do Cisco Secure Access para obter os requisitos mais atuais de destino e porta, pois eles provavelmente serão atualizados com novas versões de software.

Causa

Nas topologias de rede Hub-Spoke, todo o tráfego vinculado à Internet dos sites Spoke normalmente roteia através do site Hub por padrão. Ao implementar o CSA com o CSC, esse comportamento de roteamento padrão faz com que o tráfego de túnel CSA percorra o local do hub antes de alcançar os endpoints CSA, potencialmente introduzindo ineficiências de latência e largura de banda. A natureza dinâmica da seleção de endpoint CSA requer políticas de roteamento baseadas em domínio em vez de regras baseadas em IP estático para garantir a funcionalidade de roteamento dividido adequada.

Conteúdo relacionado

- [Documentação do Cisco Secure Access - Requisitos de conexão](#)
- [Documentação do Cisco Secure Access - Configuração de rede](#)
- [Suporte técnico e downloads da Cisco](#)

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.