Configuração da lista de exceção e do comportamento de direcionamento do tráfego de acesso seguro

Contents

Problema

Os usuários precisam de esclarecimentos sobre o comportamento do Cisco Secure Access Traffic Steering ao usar a configuração Use ZTA para proteger todos os destinos da Internet com configurações de exceção padrão. Colocam-se questões específicas relativas:

- Decisões de direcionamento de tráfego baseadas em endereços IP de destino de resolução pós-DNS.
- Como o tráfego DNS em si é tratado no processo de direção.
- Se entradas de domínio local adicionais precisam ser configuradas além da entrada de domínio .local padrão na lista Exceção.

A configuração em questão está localizada em: Connect > End User Connectivity > Zero Trust Access > (Zero Trust Access Profiles) > Secure Internet Access > Traffic Steering > Use ZTA para proteger todos os destinos da Internet

A lista de exceções padrão inclui intervalos de endereços IP privados (Classe A, B e C) e o domínio .local, e os usuários precisam entender o comportamento operacional dessas configurações.

Ambiente

- Acesso seguro da Cisco
- Configuração do Zero Trust Access (ZTA)

- Recurso Traffic Steering habilitado
- Lista de exceções padrão contendo intervalos de IP privados e domínio .local

Resolução

O comportamento Cisco Secure Access Traffic Steering opera da seguinte forma:

Processo de decisão de direcionamento de tráfego

As decisões de orientação de tráfego são tomadas com base no endereço IP de destino após a resolução DNS. O sistema avalia o IP de destino real que resulta da resolução de nomes DNS para determinar se o tráfego deve ser direcionado pela pilha de segurança Zero Trust Access.

Manipulação de tráfego DNS

As consultas DNS em si não estão sujeitas ao direcionamento de tráfego. Quando os pontos de extremidade recebem atribuições de servidor DNS via DHCP que apontam para servidores DNS internos (geralmente usando endereços IP privados), essas comunicações DNS ignoram o mecanismo de controle de tráfego e são tratadas localmente.

Configuração da Lista de Exceções

A lista de exceções padrão inclui:

- Intervalos de endereços IP privados (Classe A: 10.0.0.0/8, Classe B: 172.16.0.0/12, Classe C: 192.168.0.0/16)
- O domínio .local

Para organizações que usam domínios locais personalizados (nomes de domínio internos), entradas de domínio adicionais devem ser adicionadas à lista Exceção para garantir que o tráfego

interno não seja desnecessariamente direcionado pela pilha de segurança. A entrada padrão .local cobre os protocolos de descoberta de rede local padrão, mas possivelmente não abrange todos os domínios internos da organização.

Verificação de configuração

Para verificar a configuração apropriada:

Navegue para Connect > End User Connectivity > Zero Trust Access > Secure Internet Access > Traffic Steering.

Revise a lista Exceção para garantir que ela inclua todos os intervalos de IP privados necessários e nomes de domínio locais específicos para a infraestrutura interna de sua organização.

Causa

Esta é uma solicitação informativa sobre o comportamento operacional dos recursos do Cisco Secure Access Traffic Steering. A necessidade de esclarecimento surge da complexidade da lógica de direcionamento de tráfego e da interação entre a resolução DNS, decisões de roteamento baseadas em IP e mecanismos de tratamento de exceções.

Conteúdo relacionado

- 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.