Problemas de direcionamento de tráfego ZTNA com cliente seguro

Contents

Problema

O Zero Trust Network Access (ZTNA) baseado em cliente não fornece acesso a aplicativos internos quando acessado por FQDN ou endereço IP direto, enquanto os mesmos aplicativos permanecem acessíveis por conexão VPN.

Os sintomas específicos observados incluem:

- O Cliente Seguro ZTNA não pode acessar aplicativos internos por FQDN ou IP direto quando a VPN está desconectada.
- O acesso ZTNA baseado em navegador funciona corretamente para os mesmos aplicativos.
- Nenhum evento ZTNA aparece nos logs de atividade quando a VPN está inativa, indicando que o tráfego do cliente não está sendo roteado pelo caminho ZTNA.
- As definições de aplicativos privados foram verificadas para corresponder recursos roteáveis por VPN com configurações IP/porta/FQDN corretas.
- As políticas ZTNA foram confirmadas para corresponder às atribuições do usuário de teste e do grupo.

O problema isola especificamente o mecanismo de direcionamento ou aplicação de tráfego Secure Client ZTNA, já que a ZTNA baseada em navegador valida que a publicação e aplicação de backend estejam funcionando corretamente.

Ambiente

- Tecnologia: Acesso seguro - ZTNA (Zero Trust Network Access)

- Componentes: ZTNA baseado em cliente, postura, inscrição, acesso a recursos privados
- Cliente seguro com perfis VPN coexistentes
- Aplicativos privados acessíveis via FQDN e endereçamento IP direto
- Funcionalidade ZTNA baseada em navegador confirmada em funcionamento
- Imposição de política configurada no Modo de Imposição de Correspondência Mais Específico

Resolução

A resolução envolveu ajustes de configuração no perfil ZTA e validação de política. As etapas descritas nas próximas seções foram realizadas para restaurar a funcionalidade ZTNA baseada em cliente.

Passo 1: Adicionar recursos privados ao perfil ZTA

Recursos privados foram adicionados à configuração do perfil ZTA. Após essa alteração, os eventos bloqueados começaram a aparecer nos logs de atividade e capturas de tela, indicando que o tráfego do cliente agora estava sendo roteado corretamente pelo caminho ZTNA.

Passo 2: Verificação e teste de políticas

Uma regra temporária "permit any" foi adicionada para validar o fluxo de tráfego. Enquanto essa regra estava ativa, o acesso ZTNA baseado em cliente funcionou corretamente, confirmando que o mecanismo de direcionamento de tráfego estava funcionando, mas a aplicação da política precisava de ajuste.

Passo 3: Refinamento de política

A regra temporária permit-any foi removida e as políticas de acesso específicas foram validadas. O recurso privado foi confirmado como acessível sob a política de acesso chamada Private

Resources_Cyril usando o Modo de Execução de Correspondência Mais Específica da plataforma.

Passo 4: Validação da configuração

O usuário confirmou que o acesso ZTNA baseado em cliente começou a funcionar consistentemente após as alterações de configuração. O problema foi resolvido sem a necessidade de modificações adicionais na política ou no sistema.

Causa

A causa raiz foi uma configuração de recurso privado incompleta no perfil ZTA. Sem os recursos privados adequados definidos no perfil ZTA, o tráfego do cliente não estava sendo direcionado pelo caminho de aplicação ZTNA, fazendo com que voltasse para os mecanismos de roteamento locais. Isso fez com que o tráfego ignorasse totalmente as políticas da ZTNA, o que explicou por que nenhum evento da ZTNA apareceu nos logs de atividade quando a VPN foi desconectada.

O problema era específico da configuração de direcionamento de tráfego ZTNA baseada em cliente, enquanto a ZTNA baseada em navegador continuou a funcionar porque usa um mecanismo de tratamento de tráfego diferente que foi configurado corretamente.

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.