Exclusão de Perfil de Acesso de Confiança Zero Causando Perda de Acesso do Usuário

Contents

Problema

Depois de excluir um perfil ZTA (Zero Trust Access) que se acreditava não ser usado, todos os usuários com o módulo ZTNA experimentaram perda completa de acesso a recursos privados e à navegação na Internet. A exclusão desse perfil resultou em interrupção imediata do serviço para todos os usuários da ZTNA, impedindo-os de acessar qualquer recurso através da infraestrutura Zero Trust Network Access.

Os usuários afetados não conseguiram estabelecer conexões com:

- Recursos internos privados
- Navegação na Internet através do módulo ZTNA

Ambiente

- Acesso seguro (acesso à rede com confiança zero)
- Módulo ZTNA implantado com vários perfis de usuário
- Política padrão configurada com controle ZTNA
- Vários perfis ZTA configurados para gerenciamento de acesso do usuário

Resolução

Compreender a lógica de correspondência de perfil ZTA

Os perfis Zero Trust Access são aplicados com base em uma ordem e lógica de correspondência específica:

- Ordem de Correspondência de Perfil: Os perfis ZTA são avaliados em ordem com base nos critérios de correspondência de usuário e destino
- Comportamento do perfil padrão: Quando nenhum perfil específico corresponde aos critérios de usuário ou destino, o sistema retorna ao perfil padrão
- Dependências de perfil: Excluir um perfil que serve como o padrão efetivo pode causar a interrupção do serviço, mesmo que ele pareça não utilizado

O perfil excluído provavelmente estava funcionando como o perfil padrão efetivo para correspondência de usuário, apesar de parecer não utilizado na interface de configuração. Quando esse perfil foi removido, os usuários perderam seu caminho de acesso principal por meio da infraestrutura da ZTNA.

Etapas de validação

Para evitar problemas semelhantes no futuro, esta abordagem de validação deve ser implementada:

1.- Revise todos os perfis ZTA configurados e seus critérios de correspondência antes da exclusão.

2.- Identifique qual perfil serve como o valor-padrão efetivo para o acesso do usuário.

3.- Verifique o mapeamento de usuário para perfil por meio de capturas de tela de configuração e revisão de políticas.

4.- Teste as alterações de perfil de maneira controlada antes de aplicar à produção.

Causa

A causa raiz foi a exclusão de um perfil ZTA que estava funcionando como o perfil padrão efetivo para acesso de usuário ZTNA, apesar de parecer não utilizado na interface de configuração. Quando esse perfil foi removido, o sistema perdeu os critérios de correspondência primários para o acesso do usuário, fazendo com que todos os usuários da ZTNA perdessem a conectividade com recursos privados e navegação na Internet. A lógica de correspondência de perfil depende de ter um perfil padrão válido disponível para fallback quando critérios específicos de usuário ou destino não são atendidos por outros perfis configurados.

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.