Acesso Seguro Falha de Acesso a Recurso Privado ZTNA RDP para Um Recurso Específico

Contents

Problema

Os usuários não puderam acessar um recurso privado RDP específico por meio do Cisco Secure Access Zero Trust Network Access (ZTNA). Ao tentar se conectar, os usuários receberam uma mensagem de "erro interno". O problema afetou vários usuários, incluindo usuários recém-adicionados, e impediu que usuários de trabalho em casa acessassem os recursos de desktop necessários. Outros recursos RDP e recursos privados não RDP permaneceram acessíveis, indicando que o problema era específico a essa configuração de recurso específica.

Ambiente

- Cisco Secure Access - Acesso à rede com confiança zero (ZTNA)
- Configuração de recurso privado com protocolo RDP
- Políticas de acesso baseadas em grupo do Ative Diretory (AD)
- Várias configurações de recursos privados com endereços IP sobrepostos
- Inscrição com base no cliente e avaliação de postura

Resolução

O problema foi resolvido identificando e corrigindo conflitos de configuração na configuração de recursos privados. As etapas descritas nas próximas seções foram executadas para resolver o problema.

Identificar conflitos de configuração

A investigação revelou que o recurso RDP específico foi configurado em vários recursos privados: Faça login no CSA Dashboard > Connect > End User connectivity > Under Zero Trust Access > Add a ZTA profile > Give it a Name e procure um destino específico.

Remover Atribuições de Endereço IP Conflitantes

O endereço IP 172.26.106.136 foi removido de recursos privados conflitantes.

O endereço IP foi deixado somente sob o recurso apropriado que correspondeu às associações de grupo do Ative Diretory dos usuários e aos requisitos da política de acesso.

Verificar Associação do Grupo de Usuários

Confirmação feita de que os usuários recém-adicionados que estavam com problemas de acesso não eram membros do grupo correto do Ative Diretory (AD) necessário para acesso de acordo com a política de acesso configurada.

Além disso, verifique se o grupo ou usuário do AD correto está associado ao perfil de acesso de confiança zero.

Testar o acesso após as alterações de configuração

Depois que as alterações de configuração foram implementadas, os usuários puderam acessar com êxito o recurso RDP conforme necessário. Confirmou-se que o problema foi resolvido e os usuários puderam se conectar sem receber a mensagem de "erro interno ocorrido".

Causa

A causa principal do problema foi um conflito de configuração em que o recurso específico foi atribuído a vários recursos privados com políticas de acesso diferentes. Isso criou uma situação em que os usuários estavam sendo avaliados em relação às políticas para as quais eles não tinham a associação de grupo apropriada do Ative Diretory, resultando em recusas de acesso e na mensagem de "erro interno ocorrido". Os usuários recém-adicionados não eram membros dos grupos corretos do AD necessários para as políticas conflitantes, o que os impedia de acessar o recurso mesmo que tivessem acesso por meio da política apropriada.

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.