Erro Interno do Servidor do Grupo de Túneis de Rede de Acesso Seguro ao Reverter IP de Par Primário

Contents

Problema

Ao tentar modificar o IP do peer remoto em um Network Tunnel Group (NTG) no Cisco Secure Access, os usuários podem encontrar um "Erro interno do servidor" na interface do usuário ao tentar reverter o IP do túnel primário para um valor previamente configurado. O cenário específico envolve:

- Um NTG inicialmente configurado com um IP de túnel primário e um IP secundário, com ambos os túneis sendo estabelecidos com sucesso.
- O IP do túnel primário é alterado para um endereço IP diferente para fins de teste, que é aceito sem problemas.
- Ao tentar reverter o IP do túnel primário de volta ao valor original, o sistema falha ao salvar a configuração e retorna um "Erro interno do servidor" na interface do usuário.
- Esse comportamento é consistentemente reproduzível e aparece ao tentar reutilizar um endereço IP configurado anteriormente.
- O IP original estava funcionando anteriormente e não há conflitos com o IP do túnel secundário.

Ambiente

- Cisco Secure Access (antigo Cisco Umbrella para SSE)
- Configuração do grupo de túneis de rede para acesso privado
- Configuração de túnel duplo com IPs de pares primários e secundários

- Interface de gerenciamento baseada na Web

Resolução

Esse problema é causado por um problema de validação/estado de back-end em que o IP do peer original permanece reservado ou travado no sistema de back-end após as alterações de configuração. As etapas de solução de problemas e resolução explicadas na próxima seção devem ser seguidas:

Passo 1: Coletar informações de diagnóstico

Colete as seguintes informações para validação de back-end:

- ID da Organização de Acesso Seguro
- Nome do grupo de túneis de rede
- ID do túnel primário afetado
- Região/Centro de dados selecionado para o NTG
- Carimbo de data/hora exato de uma tentativa de salvamento com falha, incluindo fuso horário
- Confirmação se o IP original aparece em qualquer outro NTG, atual ou anterior
- Captura HAR do navegador da tentativa de salvamento com falha

Passo 2: Capturar Arquivo HAR do Navegador

Para coletar dados de diagnóstico para a tentativa de salvamento que falhou:

- Abra o navegador Ferramentas de desenvolvedor
- Vá até a guia Rede
- Habilitar log de Preservação

- Reproduzir a falha ao salvar
- Exportar o arquivo HAR e anexá-lo ao caso de suporte


Note: Limpe/remova todos os tokens de sessão ou cookies antes de carregar o arquivo HAR.

Passo 3: Validação e limpeza do back-end

Este problema requer intervenção de back-end e não pode ser resolvido somente a partir da IU. As seguintes ações devem ser executadas pelo Suporte Técnico da Cisco:

- Envolva a equipe de backend de acesso seguro/plataforma SSE
- Validar para reserva peer-IP obsoleta
- Verificar objetos de túnel órfãos
- Identificar chaves de back-end duplicadas ligadas à configuração específica do NTG
- Limpar referência de par de túnel obsoleto para o IP original
- Forçar ressincronização de back-end de objetos NTG, se necessário
- Liberar alocação peer-IP associada ao UUID do NTG

Passo 4: Método alternativo de resolução

Se a limpeza do back-end não estiver disponível imediatamente, tente este procedimento:

- Excluir a configuração primária do Grupo de Túneis de Rede
- Aguarde 5 minutos
- Adicione novamente o NTG com o endereço IP necessário


Caution: Possível. Os detalhes mencionados aqui parecem conter procedimentos ou

---

comandos que poderiam causar um impacto significativo se executados. Verifique se os procedimentos ou comandos acima foram avaliados por um SME ou Unidade de negócios antes de executar ou recomendar.

Passo 5: Solução temporária

Se o NTG estiver em produção e não puder ser removido:

- Continuar usando o túnel secundário para conectividade
- Obtenha um IP público alternativo com seu fornecedor/parceiro
- Atualize o NTG principal para usar o IP alternativo
- Reconhecer a redundância reduzida até que o problema de back-end seja resolvido

Causa

Esse problema é causado por um bug de software no sistema back-end do Cisco Secure Access. Quando um IP de peer primário é alterado e revertido ao seu valor original, o sistema de validação de back-end trata incorretamente o IP original como ainda alocado ou reservado, mesmo que ele deva estar disponível para reutilização. Isso resulta em uma falha de validação de back-end que é mascarada pela interface do usuário como um "Erro interno do servidor" genérico. O sistema back-end não consegue limpar ou liberar corretamente a reserva de IP durante o processo de alteração de configuração, criando um problema de estado persistente que impede que o IP seja reutilizado no mesmo NTG.

Conteúdo relacionado

- Solucionar problemas e coletar informações básicas do Cisco Secure Access
- 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.