Falha de Conexão do Cliente VPN do Azure com o Secure Access Web Security Habilitado

Contents

Problema

Após a migração do Umbrella para o SSE e a habilitação do Web Security com uma licença SIA recém-atribuída, as conexões do Azure VPN Client não são estabelecidas para usuários quando o Web Security está habilitado. O problema de conectividade do cliente VPN do Azure afeta todos os clientes, impedindo-os de se conectarem à VPN. Quando o Cisco Secure Access Client é desinstalado das máquinas cliente, a conectividade VPN é restaurada, indicando que o cliente Secure Access está bloqueando a conexão com os serviços de VPN do Azure.

Desabilitar o Web Security ou desinstalar o Cisco Secure Access Client restaura a conectividade VPN, mas isso afeta o acesso do usuário aos recursos sobre o Azure VPN quando a proteção do Web Security é necessária.

Ambiente

- Cisco Secure Access (anteriormente SIA) com Web Security ativado
- Cliente de VPN do Azure
- Migração do Umbrella para o SSE concluída
- Licença SIA atribuída recentemente

Resolução

A resolução envolve adicionar o endereço IP público do gateway de VPN do Azure à lista de exceções SSE/SWG para evitar a interceptação de tráfego que bloqueia conexões VPN.

Passo 1: Identificar o Endereço IP do Gateway VPN do Azure

Determine o endereço IP público do gateway VPN do Azure.

Passo 2: Adicionar exceção baseada em IP ao SSE/SWG

1.- Adicione o endereço IP público do gateway virtual do Azure à lista de exceções do SSE/SWG no ambiente do Cisco Secure Access.

2.- Faça login no Cisco Secure Access Dashboard - Clique em Conectar - Conectividade do usuário final - Segurança da Internet - Adicionar exceção. Isso evita que o Secure Web Gateway intercepte e inspecione o tráfego destinado ao gateway de VPN do Azure.

Passo 3: Testar a conectividade VPN

Após aplicar a exceção baseada em IP, teste a conexão VPN do Azure para verificar se os clientes podem estabelecer conexões VPN com êxito com o Web Security habilitado.

Passo 4: Expandir teste

Estenda o teste da exceção baseada em IP para usuários adicionais em todo o ambiente para garantir a funcionalidade consistente antes de considerar a resolução completa.

Causa

O problema ocorre porque o mecanismo de exceção do Secure Web Gateway (SWG) requer uma pesquisa de DNS em um domínio para criar uma entrada de cache de domínio para IP. Quando o cliente VPN do Azure se conecta diretamente ao endereço IP sem executar uma consulta DNS para a URL VPN, o módulo SWG não pode mapear o domínio para o endereço IP. Como resultado, o SWG continua a inspecionar e interceptar o tráfego para o endereço IP, impedindo o

estabelecimento da conexão VPN.

A análise de captura de pacotes não mostrou consultas de DNS para a URL da VPN e nenhum tráfego de interceptação de SWG visível para o IP de gateway do Azure, confirmando que o SWG estava bloqueando a conexão devido à falta de mapeamento de domínio para IP apropriado em seu cache.

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.