Problemas de conectividade do FQDN hospedado no Azure via Acesso Seguro com Integração com Meraki

Contents

Problema

FQDNs específicos hospedados no Azure se tornam inalcançáveis quando o tráfego do usuário é roteado através da Meraki para o Cisco Secure Access, apesar dos logs do Secure Access mostrarem o tráfego como "permitido". O problema afeta principalmente a conectividade RDP usando portas não padrão para esses FQDNs.

Ao pesquisar logs por FQDN no portal de Acesso Seguro, somente os logs de Segurança DNS são exibidos com o status "permitido". No entanto, a conectividade RDP para os mesmos destinos em portas fora do padrão falha. Quando o FQDN é resolvido para um endereço IP e a pesquisa de atividades usa o IP de destino, os logs do Cloud Firewall que estavam bloqueando o tráfego são revelados.

Ambiente

- Cisco Secure Access (SSE) com integração com Meraki
- Painel Meraki com recurso de breakout local
- Recursos de desenvolvimento hospedados no Azure que exigem acesso RDP em portas não padrão
- Roteamento de tráfego através do túnel Meraki para acesso seguro

Resolução

Solução imediata

Adicione os FQDNs afetados às regras de breakout local da Meraki para ignorar o Secure Access para os destinos específicos detalhados nas próximas seções.

Passo 1: Acesse o painel da Meraki

Navegue até o painel da Meraki e localize a seção de configuração da reunião à parte local.

Passo 2: Configurar Regras de Reunião à Parte Local

Adicione os FQDNs problemáticos às regras de breakout locais para ignorar o roteamento de Acesso Seguro. Essa alteração de configuração restaura imediatamente o acesso dos usuários afetados roteando o tráfego diretamente da Meraki para a Internet, ignorando o túnel de acesso seguro.

Solução de problemas e análise

Passo 1: Análise de Log por FQDN

Pesquise logs de Atividade de Acesso Seguro usando o FQDN. Isso mostra principalmente logs de segurança DNS e pode exibir o status "permitido" para o tráfego da Web na porta 443.

Passo 2: Análise de log por IP de destino

Resolva o FQDN para seu endereço IP e pesquise os logs de atividade usando o IP de destino em vez do FQDN. Isso revela logs do Cloud Firewall que mostram o tráfego bloqueado, fornecendo a disposição real do tráfego.

Passo 3: Verificar o fluxo de tráfego

Confirme se o problema ocorre somente quando o tráfego segue o caminho: O usuário → Meraki → Tunnel → acesso seguro → Internet. Teste se o desvio via breakout local resolve o problema de conectividade.

Resolução de longo prazo

O comportamento observado foi identificado como funcionalidade esperada na implementação atual do Secure Access. Uma solicitação de recurso (FR CSE-I-5543) foi aberta para abordar a visibilidade e as preocupações funcionais relacionadas a:

- Discrepância entre pesquisas de log baseadas em FQDN e baseadas em IP
- Relatório de disposição de tráfego inconsistente entre os logs de segurança DNS e firewall de nuvem
- Visibilidade aprimorada do tráfego RDP em portas fora do padrão

Causa

O problema deriva de uma discrepância em como o Secure Access processa e relata o tráfego para FQDNs hospedados no Azure quando acessados via RDP em portas não padrão. Ao pesquisar logs por FQDN, o sistema exibe principalmente logs de Segurança DNS que mostram o status "permitido" para o tráfego da Web (geralmente a porta 443). No entanto, o tráfego RDP real em portas não padrão está sendo processado pelas regras do Cloud Firewall, que são visíveis apenas quando se pesquisa pelo endereço IP destino resolvido, em vez do FQDN.

Isso cria uma lacuna de visibilidade onde os administradores veem o tráfego "permitido" em pesquisas baseadas em FQDN, enquanto as conexões RDP reais são bloqueadas por políticas de firewall que são apenas aparentes em pesquisas de registro baseadas em IP. O comportamento é atualmente considerado funcionalidade esperada, mas uma solicitação de recurso foi enviada para melhorar a visibilidade e a consistência dos relatórios de tráfego em diferentes métodos de pesquisa.

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.