Manuseio de Pacotes ICMP Fragmentados do Cisco Secure Access

Contents

Problema

As solicitações de eco ICMP maiores que a MTU não estão recebendo respostas quando enviadas com o bit DF (Don't Fragment) desativado. Esse comportamento ocorre em dois cenários específicos:

- De pontos finais RAVPN sobre a interface VPN ao enviar pacotes ICMP que excedem o tamanho de MTU da interface VPN com o bit DF limpo
- De pontos finais no local em um túnel IPsec entre um roteador local e o Cisco Secure Access (CSA) ao enviar pacotes ICMP que excedem o tamanho de MTU da interface do túnel IPsec com o bit DF limpo

Em ambos os casos, nenhuma resposta ICMP é recebida, levando a dúvidas sobre se o CSA descarta pacotes fragmentados com o bit DF desativado.

Ambiente

- Acesso seguro da Cisco (CSA)
- Pontos de extremidade RAVPN (Remote Access VPN)
- Túneis IPsec entre roteadores de site e CSA
- Tráfego ICMP excedendo os tamanhos de MTU da interface
- Cenários de pacotes fragmentados com remoção de bit DF

Resolução

O Cisco Secure Access descarta pacotes fragmentados nos cenários de sobreposição e de

sobreposição. Esse comportamento é documentado na documentação da Ajuda do Cisco Secure Access, que declara explicitamente: "Os pacotes fragmentados na subjacência ou na sobreposição são descartados."

Comportamento esperado

O Cisco Secure Access foi projetado para descartar pacotes fragmentados, independentemente de ocorrerem na rede subjacente ou de sobreposição. Aplicável a:

- Pacotes ICMP enviados de pontos finais RAVPN que excedem o MTU da interface VPN com o bit DF limpo
- Pacotes ICMP enviados de endpoints locais por túneis IPsec que excedem a interface de túnel MTU com bit DF limpo

Esse comportamento é consistente em todos os cenários que envolvem pacotes fragmentados na infraestrutura do Cisco Secure Access.

A solicitação de recurso CSE-I-5739 foi criada para isso.

Causa

O Cisco Secure Access foi projetado para descartar pacotes fragmentados como uma decisão de projeto de segurança e desempenho. Esse comportamento é implementado para evitar possíveis vulnerabilidades de segurança e a sobrecarga de processamento associada à remontagem de pacotes nos cenários de rede subjacente e de sobreposição.

Conteúdo relacionado

- Documentação da Ajuda do Cisco Secure Access - Manipulação de pacotes fragmentada
- 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.