Resolver penalização de DNS no MacOS e problema de acesso com domínios internos

Contents

Introdução

Este documento descreve como resolver um problema com versões mais recentes do MacOS Big Sur que afeta a resolução DNS.

Informações de Apoio

Escopo

- Módulo de segurança de roaming do AnyConnect ou guarda-chuva na rede (como VA ou encaminhamento)
  - Cliente de roaming independente Umbrella não afetado. O ambiente de DNS único está presente onde todo o DNS é substituído por 127.0.0.1).
- Ocorre em ambientes com várias interfaces de rede, mas apenas uma pode resolver endereços internos. Por exemplo:
  - VPN e fora da VPN
  - Várias placas de rede - uma corporativa e uma não corporativa

Sintomas

- Incapacidade (ou capacidade intermitente) de acessar domínios locais enquanto mantém a capacidade de acessar domínios públicos
  - o nslookup não é especificamente afetado e continua a funcionar
    - ping, traceroute, etc. resolve incorretamente ou não localiza o domínio interno

Problema

Esse problema é causado pelo código no MacOS que manipula a forma como as resoluções de

DNS são gerenciadas na presença de vários servidores DNS. Podem ser vários resolvedores em um único adaptador de rede ou vários resolvedores em diferentes adaptadores de rede. Um servidor DNS que responde com REFUSED é "penalizado" por 60 segundos. Quando isso acontece, qualquer consulta de DNS adicional que ocorrer durante esse período é tentada em servidores DNS alternativos que não são penalizados.

Por exemplo, se o DHCP anuncia dois servidores DNS para uma rede, A e B, e A responde com REFUSED, então B é favorecido sobre A por 60 segundos, desde que B não seja penalizado.

Se todos os servidores DNS forem penalizados, o MacOS favorecerá o servidor penalizado menos recentemente. Por exemplo, se B for penalizado enquanto A já estiver penalizado, o MacOS favorecerá A sobre B.

Isso é agravado pela maneira como o MacOS 11 e posterior tenta afirmar DoH (DNS sobre HTTPS). O MacOS é programado para preferir um provedor DoH definido pelo usuário quando possível. Isso contornaria a segurança do DNS do Umbrella, o que significa que retornamos uma resposta REFUSED (conforme RFC) quando o MacOS inicia uma solicitação DoH. Devido à penalização de DNS, isso pode fazer com que domínios internos não sejam resolvidos corretamente. Para obter mais informações sobre esse assunto, consulte este artigo: Seleção de DNS Resolver no iOS 14 e macOS 11.

Solução

Ainda não sabemos se a Apple planeja alterar esse comportamento ou se a Umbrella pode alterar seu comportamento para contornar esse problema. Por enquanto, há duas opções que funcionam como soluções alternativas:

Opção 1

Habilite o split-DNS na política de grupo e adicione especificamente os domínios internos à configuração do split-DNS para que eles possam ser resolvidos somente por túnel. Isso garante que esses domínios só possam ser resolvidos no túnel pelo resolvedor de OS nativo, enquanto outros domínios só podem ser resolvidos fora do túnel.

Opção 2

Habilite tunnel-all-DNS na política de grupo para evitar que qualquer tráfego DNS saia do túnel.

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.