Resolver penalización de DNS en MacOS y problemas de acceso con dominios internos

Contenido

Introducción

Este documento describe cómo resolver un problema con las versiones más recientes de MacOS Big Sur que afecta la resolución DNS.

Antecedentes

Alcance

- AnyConnect Roaming Security Module o Umbrella en la red (como AV o reenvío)
  - Cliente de roaming independiente de Umbrella no afectado. El entorno de DNS único está presente cuando todos los DNS se sobrescriben con 127.0.0.1).
- Se produce en entornos con varias interfaces de red, pero sólo una puede resolver direcciones internas. Por ejemplo:
  - VPN y fuera de VPN
  - NIC múltiple: una corporativa y una no corporativa

Síntomas

- Incapacidad (o capacidad intermitente) para acceder a dominios locales sin perder la capacidad de acceder a dominios públicos
  - nslookup no se ve afectado específicamente y continúa funcionando
    - ping, traceroute, etc. se resuelven incorrectamente o no encuentran el dominio interno

Problema

Este problema es causado por el código en MacOS que maneja la forma en que se administran

las resoluciones DNS en presencia de varios servidores DNS. Pueden ser varias resoluciones en un único adaptador de red o varias resoluciones en diferentes adaptadores de red. Un servidor DNS que responda con RECHAZADO será "penalizado" durante 60 segundos. Cuando esto sucede, cualquier consulta DNS adicional que ocurra durante este período de tiempo se prueba en servidores DNS alternativos que no están penalizados.

Por ejemplo, si DHCP anuncia dos servidores DNS para una red, A y B, y A responde con RECHAZADO, entonces B es favorecido sobre A durante 60 segundos mientras B no sea penalizado.

Si todos los servidores DNS están penalizados, MacOS favorece al servidor penalizado menos recientemente. Por ejemplo, si B se penaliza mientras que A ya estaba penalizado, MacOS favorece A sobre B.

Esto se ve agravado por la forma en que MacOS 11 y versiones posteriores intentan imponer el DoH (DNS sobre HTTPS). MacOS está programado para preferir un proveedor DoH configurado por el usuario cuando sea posible. Esto eludiría la seguridad de Umbrella DNS, lo que significa que devolvemos una respuesta REFUSED (según RFC) cuando MacOS inicia una solicitud DoH. Debido a la penalización de DNS, esto puede dar lugar a que los dominios internos no se resuelvan correctamente. Para obtener más información sobre este tema, consulte este artículo: Selección de resolución de DNS en iOS 14 y macOS 11.

Solución

Todavía no sabemos si Apple planea cambiar este comportamiento o si Umbrella es capaz de cambiar su comportamiento para solucionar este problema. Por el momento, existen dos opciones que sirven como soluciones alternativas:

Opción 1

Habilite split-DNS en la política de grupo y agregue específicamente los dominios internos a la configuración split-DNS para que sólo se puedan resolver a través del túnel. Esto garantiza que esos dominios sólo se puedan resolver a través del túnel mediante la resolución de SO nativa, mientras que cualquier otro dominio sólo se puede resolver fuera del túnel.

Opción 2

Habilite tunnel-all-DNS en la política de grupo para evitar que el tráfico DNS salga del túnel.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).