Problemas de coexistência da segurança DNS do Umbrella com o Broadcom WSS no macOS

Contents

Problema

O módulo Umbrella não está interceptando o tráfego DNS no macOS quando coexiste com o Broadcom WSS (Web Security Service). Quando o agente WSS é configurado para interceptar portas da Web específicas, como 80 e 443, a funcionalidade de segurança do DNS do Umbrella não captura todas as consultas DNS. No entanto, quando o WSS é desativado, o Umbrella retoma a interceptação do tráfego DNS como esperado. Somente determinadas consultas DNS estão sendo processadas pelo Umbrella quando o WSS está habilitado, em vez de todo o tráfego DNS ser interceptado.

Ambiente

- Sistema operacional: MacOS
- Módulo de segurança DNS do Cisco Umbrella
- Agente Broadcom WSS (Web Security Service)
- Agente WSS configurado para interceptar as portas da Web 80 e 443

Resolução

Esse problema foi analisado e determinado como uma limitação arquitetônica do macOS, onde a segurança DNS não pode coexistir com o WSS na arquitetura atual do macOS. Essa limitação se aplica às soluções de segurança Infoblox e Cisco Umbrella DNS.

Análise técnica

A causa raiz está relacionada às limitações de proxy DNS do macOS:

- Somente um proxy DNS pode estar ativo no sistema por vez devido às limitações do macOS
- Se os resolvedores DNS estiverem vinculados às interfaces utunX ou aos resolvedores injetados por proxy, o macOS resolverá o DNS dentro do túnel, não via Umbrella
- Quando outro NEDnsProxyProvider estiver ativo no sistema no macOS, o Umbrella não interceptará o tráfego DNS

Comandos de diagnóstico

Para verificar qual resolvedor de DNS está tendo prioridade no macOS, use o seguinte comando:

```
scutil --dns
```

Esse comando mostrará qual resolvedor está marcado como: Com escopo, complementar ou interface: utunX, ajudando a identificar conflitos de proxy DNS.

Opções de solução

Para ambientes macOS, o WSS continuará a interceptar DNS sem qualquer Agente DNS separado. Para avançar com a cobertura de segurança do DNS, uma opção seria implementar o para suportar uma arquitetura de desvio passivo. Com essa abordagem, o provedor ignoraria completamente o fluxo, permitindo que o tráfego fosse processado como se não estivesse ativo.

Causa

O problema é causado por limitações arquitetônicas do macOS, em que apenas um NEDnsProxyProvider pode estar ativo no sistema de cada vez. Quando o Umbrella DNS Security e o Broadcom WSS estão instalados, eles competem pelo controle de proxy DNS, fazendo com que o WSS tenha prioridade e evitando que o Umbrella intercepte o tráfego DNS. Essa é uma limitação fundamental da pilha de rede macOS e afeta todas as soluções de segurança DNS, não apenas o Cisco Umbrella.

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.