Problemas de coexistencia de seguridad de Umbrella DNS con Broadcom WSS en macOS

Contenido

Problema

El módulo Umbrella no intercepta el tráfico DNS en macOS cuando coexiste con Broadcom WSS (servicio de seguridad web). Cuando el agente WSS está configurado para interceptar puertos web específicos como 80 y 443, la funcionalidad de seguridad de Umbrella DNS no puede capturar todas las consultas DNS. Sin embargo, cuando WSS está deshabilitado, Umbrella reanuda la interceptación del tráfico DNS como se esperaba. Umbrella sólo procesa determinadas consultas DNS cuando se habilita WSS, en lugar de interceptar todo el tráfico DNS.

Entorno

- Sistema operativo: macOS
- Módulo de seguridad de DNS de Cisco Umbrella
- Agente Broadcom WSS (servicio de seguridad web)
- Agente WSS configurado para interceptar los puertos web 80 y 443

Resolución

Este problema se ha analizado y se ha determinado que es una limitación arquitectónica de macOS donde la seguridad de DNS no puede coexistir con WSS en la arquitectura de macOS actual. Esta limitación se aplica a las soluciones de seguridad de DNS Infoblox y Cisco Umbrella.

Análisis técnico

La causa raíz está relacionada con las limitaciones del proxy DNS de macOS:

- Debido a las limitaciones de macOS, solo puede estar activo un proxy DNS en el sistema a la vez
- Si los resolvers DNS están enlazados a interfaces utunX o a resolvers inyectados por proxy, macOS resuelve DNS dentro del túnel, no a través de Umbrella
- Cuando otro NEDnsProxyProvider está activo en el sistema en macOS, Umbrella no interceptará el tráfico DNS

Comandos de diagnóstico

Para verificar qué resolución de DNS está tomando prioridad en macOS, utilice el siguiente comando:

```
scutil --dns
```

Este comando mostrará qué resolución está marcada como: Alcance, suplementario o interfaz: utunX, ayudando a identificar conflictos de proxy DNS.

Opciones de solución

Para entornos macOS, WSS continuará interceptando DNS sin ningún agente DNS independiente. Para avanzar con la cobertura de seguridad de DNS, una opción sería implementar para admitir una arquitectura de omisión pasiva. Con este enfoque, el proveedor omitiría por completo el flujo, permitiendo que el tráfico se procese como si el proveedor no estuviera activo.

Causa

El problema se debe a las limitaciones de la arquitectura de macOS, en la que solo puede haber un NEDnsProxyProvider activo en el sistema a la vez. Cuando se instalan Umbrella DNS Security y Broadcom WSS, compiten por el control de proxy DNS, lo que hace que WSS tenga prioridad y evite que Umbrella intercepte el tráfico DNS. Esta es una limitación fundamental de la pila de redes de macOS y afecta a todas las soluciones de seguridad DNS, no solo a Cisco Umbrella.

Contenido relacionado

- Soporte técnico y descargas de Cisco

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).