La regla de permiso de DNS no coincide cuando va seguida de una regla de denegación de cualquiera/cualquiera

Contenido

- Problema
- Entorno
- Resolución
- Causa
- Contenido relacionado

Problema

Cuando una directiva de acceso a Internet se configura con una regla Permitir cualquiera/Cualquiera diseñada para permitir el tráfico DNS, seguida de una regla Denegar cualquiera/Cualquiera en la parte inferior de la directiva, es posible que las solicitudes DNS no coincidan con la regla Permitir. En su lugar, las solicitudes DNS se evalúan según las reglas subsiguientes y, en última instancia, el bloque global puede bloquearlas.

Por ejemplo, una política se puede configurar de la siguiente manera:

1. Permitir: tráfico DNS/cualquier destino
2. Denegar: cualquier protocolo/cualquier destino

En esta configuración, el tráfico DNS no coincide con la regla de permiso deseada y puede ser bloqueado por la regla de denegación Any/Any subsiguiente.

Por qué esto puede ser confuso

Cisco Secure Access permite a los administradores seleccionar protocolos de aplicación como:

- DNS
- DNS sobre HTTPS (DoH)
- DNS sobre TLS (DoT)

al configurar una regla de directiva de acceso a Internet.

Esto puede dar lugar a la expectativa de que el tráfico DNS siempre se puede permitir o denegar de forma independiente mediante una condición de protocolo de aplicación. Sin embargo, el tráfico DNS está sujeto a un comportamiento de evaluación de políticas específico y es posible que el protocolo de aplicación o las condiciones basadas en servicios (objeto de servicio) no se evalúen como se esperaba en esta configuración de regla.

Entorno

- Este problema se aplica a entornos con:
    - Cisco Secure Access (SSE)
    - Políticas de acceso a Internet que contienen varias reglas
    - Una combinación de reglas basadas en protocolo/aplicación y una regla final Denegar cualquiera/cualquiera
    - Tráfico DNS que se espera que coincida con una regla de permiso anterior, pero que en su lugar está bloqueado por una regla posterior o el bloque global

Resolución

Actualmente no hay ninguna configuración admitida que garantice que una regla de permiso de cualquiera/cualquiera de DNS coincidirá con el tráfico DNS de forma independiente cuando vaya seguida de una regla de denegación de cualquiera/cualquiera en esta estructura de políticas.

Los clientes deben tener en cuenta esta limitación de evaluación de políticas al diseñar políticas de acceso a Internet que contengan una regla final Denegar cualquiera/cualquiera.

Si se debe permitir el tráfico DNS, la política debe diseñarse utilizando condiciones de regla admitidas que sean aplicables al tráfico DNS que se está evaluando.

Causa

El tráfico DNS no se evalúa en función de condiciones basadas en servicios de la misma manera que el tráfico de aplicaciones general.

Cuando una regla de directiva contiene condiciones que no se pueden aplicar al tráfico DNS que se está evaluando, la regla no coincide. La evaluación de la política continúa con la siguiente regla aplicable.

Por ejemplo:

```
Rule 1: Permit DNS / Any
            |
            |-- DNS traffic does not match
            |
Rule 2: Deny Any / Any
            |
            |-- DNS traffic matches
            |
          BLOCK
```

Por lo tanto, la colocación de una regla Permitir DNS inmediatamente por encima de una regla Denegar cualquiera/Cualquiera no garantiza que se permita el tráfico DNS.

Contenido relacionado

https://securitydocs.cisco.com/docs/csa/olh/121998.dita

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).