Regra de permissão de DNS não correspondente quando seguida por uma regra Negar qualquer/qualquer

Contents

- Problema
- Ambiente
- Resolução
- Causa
- Conteúdo relacionado

Problema

Quando uma política de acesso à Internet é configurada com uma regra Permitir qualquer/qualquer para permitir o tráfego DNS, seguida por uma regra Negar qualquer/qualquer na parte inferior da política, as solicitações DNS podem não corresponder à regra Permitir. Em vez disso, as solicitações de DNS são avaliadas em relação a regras subsequentes e podem ser bloqueadas pelo bloco global.

Por exemplo, uma política pode ser configurada da seguinte maneira:

1. Permit — Tráfego DNS / Qualquer destino
2. Negar — Qualquer protocolo/qualquer destino

Nessa configuração, o tráfego DNS não corresponde à regra de permissão pretendida e pode ser bloqueado pela regra Deny Any/Any subsequente.

Por que isso pode ser confuso

O Cisco Secure Access permite que os administradores selecionem protocolos de aplicação como:

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

ao configurar uma regra de política de Acesso à Internet.

Isso pode levar à expectativa de que o tráfego DNS sempre possa ser permitido ou negado independentemente usando uma condição de protocolo de aplicativo. No entanto, o tráfego DNS está sujeito a um comportamento de avaliação de política específico, e o protocolo de aplicação ou as condições baseadas em serviço (objeto Serviço) podem não ser avaliados como esperado nesta configuração de regra.

Ambiente

- Esse problema se aplica a ambientes com:
    - Cisco Secure Access (SSE)
    - Políticas de acesso à Internet contendo várias regras
    - Uma combinação de regras baseadas em protocolo/aplicativo e uma regra de Negar Qualquer/Qualquer final
    - Tráfego DNS que deve corresponder a uma regra de permissão anterior, mas que é bloqueado por uma regra subsequente ou pelo bloco global

Resolução

No momento, não há nenhuma configuração com suporte que garanta que uma regra de DNS Permitir Qualquer/Qualquer corresponderá ao tráfego DNS independentemente quando seguida por uma regra Negar Qualquer/Qualquer nesta estrutura de política.

Os clientes devem estar cientes dessa limitação de avaliação de política ao projetar políticas de

acesso à Internet que contenham uma regra de Negar qualquer/qualquer.

Se o tráfego DNS precisar ser permitido, a política deverá ser projetada usando as condições de regra suportadas que são aplicáveis ao tráfego DNS que está sendo avaliado.

Causa

O tráfego DNS não é avaliado em relação às condições baseadas em serviço da mesma maneira que o tráfego de aplicativo geral.

Quando uma regra de política contém condições que não podem ser aplicadas ao tráfego DNS que está sendo avaliado, a regra não corresponde. A avaliação da política continua para a próxima regra aplicável.

Por exemplo:

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

Portanto, colocar uma regra DNS de permissão imediatamente acima de uma regra Deny Any/Any não garante que o tráfego DNS será permitido.

Conteúdo relacionado

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

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.