Règle d'autorisation DNS ne correspondant pas lorsqu'elle est suivie d'une règle Refuser tout/tout

Table des matières

- Problème
- Environnement
- Résolution
- Motif
- Autres informations utiles

Problème

Lorsqu'une stratégie d'accès à Internet est configurée avec une règle Autoriser tout/Tout destinée à autoriser le trafic DNS, suivie d'une règle Refuser tout/Tout au bas de la stratégie, les requêtes DNS peuvent ne pas correspondre à la règle Autoriser. Au lieu de cela, les requêtes DNS sont évaluées par rapport aux règles suivantes et peuvent finalement être bloquées par le bloc global.

Par exemple, une stratégie peut être configurée comme suit :

1. Autoriser — Trafic DNS / Toute destination
2. Refuser : tout protocole / toute destination

Dans cette configuration, le trafic DNS ne correspond pas à la règle d'autorisation prévue et peut être bloqué par la règle Deny Any/Any suivante.

Pourquoi cela peut être déroutant

Cisco Secure Access permet aux administrateurs de sélectionner des protocoles d'application tels que :

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

lors de la configuration d'une règle de stratégie d'accès Internet.

Cela peut conduire à penser que le trafic DNS peut toujours être autorisé ou refusé indépendamment à l’aide d’une condition de protocole d’application. Cependant, le trafic DNS est soumis à un comportement d'évaluation de stratégie spécifique, et le protocole d'application ou les conditions basées sur le service (objet Service) peuvent ne pas être évalués comme prévu dans cette configuration de règle.

Environnement

- Ce problème s'applique aux environnements avec :
    - Accès sécurisé Cisco (SSE)
    - Politiques d'accès Internet contenant plusieurs règles
    - Combinaison de règles basées sur le protocole/l'application et d'une règle finale Refuser tout/tout
    - Trafic DNS qui est censé correspondre à une règle d'autorisation précédente, mais qui est bloqué par une règle suivante ou par le blocage global

Résolution

Aucune configuration actuellement prise en charge ne garantit qu'une règle d'autorisation Any/Any DNS correspondra au trafic DNS indépendamment lorsqu'elle est suivie d'une règle d'interdiction Any/Any dans cette structure de stratégie.

Les clients doivent tenir compte de cette limite d'évaluation des politiques lorsqu'ils conçoivent des politiques d'accès à Internet qui contiennent une règle finale Refuser tout/tout.

Si le trafic DNS doit être autorisé, la stratégie doit être conçue en utilisant les conditions de règle

prises en charge qui sont applicables au trafic DNS évalué.

Motif

Le trafic DNS n'est pas évalué par rapport aux conditions basées sur les services de la même manière que le trafic d'application général.

Lorsqu'une règle de stratégie contient des conditions qui ne peuvent pas être appliquées au trafic DNS évalué, la règle ne correspond pas. L'évaluation de la stratégie passe ensuite à la règle applicable suivante.

Exemple :

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

Par conséquent, le fait de placer une règle Autoriser DNS immédiatement au-dessus d'une règle Refuser tout/tout ne garantit pas que le trafic DNS sera autorisé.

Autres informations utiles

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.