Regola Consenti DNS non corrispondente quando seguita da una regola Deny Any/Any

Sommario

- Problema
- Ambiente
- Risoluzione
- Causa
- Contenuto correlato

Problema

Quando un criterio di accesso a Internet è configurato con una regola Permit Any/Any per consentire il traffico DNS, seguita da una regola Deny Any/Any in fondo al criterio, le richieste DNS potrebbero non corrispondere alla regola Permit. Al contrario, le richieste DNS vengono valutate rispetto alle regole successive e possono essere bloccate dal blocco globale.

Ad esempio, un criterio può essere configurato come segue:

1. Permit - Traffico DNS / Qualsiasi destinazione
2. Nega: qualsiasi protocollo/destinazione

In questa configurazione, il traffico DNS non corrisponde alla regola di autorizzazione prevista e può essere bloccato dalla successiva regola Deny Any/Any.

Perché questo può confondere

Cisco Secure Access consente agli amministratori di selezionare protocolli applicativi quali:

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

durante la configurazione di una regola di criteri di accesso a Internet.

È quindi possibile prevedere che il traffico DNS possa sempre essere autorizzato o rifiutato in modo indipendente utilizzando una condizione del protocollo dell'applicazione. Il traffico DNS è tuttavia soggetto a un comportamento di valutazione dei criteri specifico e il protocollo dell'applicazione o le condizioni basate sui servizi (oggetto Service) potrebbero non essere valutate come previsto in questa configurazione di regola.

Ambiente

- Questo problema si applica agli ambienti con:
    - SSE (Cisco Secure Access)
    - Criteri di accesso a Internet contenenti più regole
    - Una combinazione di regole basate su protocollo/applicazione e una regola Deny Any/Any finale
    - Traffico DNS che deve corrispondere a una regola di autorizzazione precedente ma che viene invece bloccato da una regola successiva o dal blocco globale

Risoluzione

Non è attualmente disponibile una configurazione supportata che garantisca che una regola DNS Permit Any/Any corrisponda al traffico DNS in modo indipendente quando seguita da una regola Deny Any/Any in questa struttura di criteri.

I clienti devono essere consapevoli di questa limitazione della valutazione dei criteri quando progettano criteri di accesso a Internet che contengono una regola Deny Any/Any finale.

Se è necessario consentire il traffico DNS, i criteri devono essere progettati utilizzando condizioni

delle regole supportate applicabili al traffico DNS in fase di valutazione.

Causa

Il traffico DNS non viene valutato rispetto alle condizioni basate sul servizio allo stesso modo del traffico generale delle applicazioni.

Quando una regola dei criteri contiene condizioni che non possono essere applicate al traffico DNS in fase di valutazione, la regola non corrisponde. La valutazione dei criteri passa quindi alla regola successiva applicabile.

Ad esempio:

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

Pertanto, l'inserimento di una regola Autorizza DNS immediatamente al di sopra di una regola Deny Any/Any non garantisce che il traffico DNS verrà autorizzato.

Contenuto correlato

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).