DNS-Zulassungsregel stimmt nicht überein, wenn auf sie eine Regel zum Verweigern einer beliebigen/einer beliebigen Regel folgt

Inhalt

- Problem
- Umwelt
- Auflösung
- Ursache
- Verwandte Inhalte

Problem

Wenn eine Richtlinie für den Internetzugriff mit einer Any/Any-Regel für die Zulässigkeit von DNS-Datenverkehr konfiguriert wird, gefolgt von einer Any/Any-Regel für die Ablehnung am Ende der Richtlinie, stimmen DNS-Anforderungen möglicherweise nicht mit der Permit-Regel überein. Stattdessen werden die DNS-Anfragen anhand nachfolgender Regeln ausgewertet und können letztendlich durch die globale Sperre blockiert werden.

Eine Richtlinie kann beispielsweise wie folgt konfiguriert werden:

1. Zulassen - DNS-Datenverkehr/Beliebiges Ziel
2. Verweigern - jedes Protokoll/jedes Ziel

In dieser Konfiguration stimmt der DNS-Datenverkehr nicht mit der beabsichtigten Zulässigkeitsregel überein und kann durch die nachfolgende "Any/Any"-Regel verweigern blockiert werden.

Warum kann das verwirrend sein?

Cisco Secure Access ermöglicht Administratoren die Auswahl von Anwendungsprotokollen wie:

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

beim Konfigurieren einer Richtlinie für den Internetzugriff.

Dies kann zu der Erwartung führen, dass DNS-Datenverkehr immer unabhängig zugelassen oder verweigert werden kann, wenn eine Bedingung für das Anwendungsprotokoll verwendet wird. Der DNS-Datenverkehr unterliegt jedoch einem bestimmten Richtlinienbewertungsverhalten, und Anwendungsprotokolle oder dienstbasierte Bedingungen (Service-Objekt) werden in dieser Regelkonfiguration möglicherweise nicht wie erwartet ausgewertet.

Umwelt

- Dieses Problem betrifft Umgebungen mit:
    - Cisco Secure Access (SSE)
    - Richtlinien für den Internetzugriff, die mehrere Regeln enthalten
    - Eine Kombination aus Protokoll-/anwendungsbasierten Regeln und einer abschließenden Deny Any-/Any-Regel
    - DNS-Datenverkehr, der einer vorhergehenden Zulässigkeitsregel entsprechen soll, jedoch durch eine nachfolgende Regel oder den globalen Block blockiert wird

Auflösung

Derzeit gibt es keine unterstützte Konfiguration, die garantiert, dass eine Any/Any DNS-Regel mit dem DNS-Verkehr übereinstimmt, wenn sie von einer Any/Any-Regel in dieser Richtlinienstruktur gefolgt wird.

Kunden sollten diese Einschränkung bei der Richtlinienauswertung beachten, wenn sie Richtlinien für den Internetzugriff entwerfen, die eine abschließende "Any/Any"-Regel für "Verweigern" enthalten.

Wenn DNS-Datenverkehr zugelassen werden muss, sollte die Richtlinie unter Verwendung unterstützter Regelbedingungen konzipiert werden, die für den auszuwertenden DNS-Datenverkehr gelten.

Ursache

DNS-Datenverkehr wird nicht in derselben Weise wie allgemeiner Anwendungsdatenverkehr anhand dienstbasierter Bedingungen ausgewertet.

Wenn eine Richtlinienregel Bedingungen enthält, die nicht auf den auszuwertenden DNS-Datenverkehr angewendet werden können, stimmt die Regel nicht überein. Die Richtlinienauswertung wird dann mit der nächsten zutreffenden Regel fortgesetzt.

Beispiele:

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

Wenn Sie daher eine Permit DNS-Regel direkt über einer Deny Any/Any-Regel platzieren, wird nicht garantiert, dass der DNS-Datenverkehr zugelassen wird.

Verwandte Inhalte

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.