Deny Any/Anyルールに続けてDNS Allow Rule Not Matchingが発生する

内容

- お問い合わせ内容
- 環境
- 解決策
- 原因
- 関連コンテンツ

お問い合わせ内容

インターネットアクセスポリシーが、DNSトラフィックを許可するためのPermit Any/Anyルールで設定され、ポリシーの最後にDeny Any/Anyルールが続いている場合、DNS要求がPermitルールに一致しないことがあります。代わりに、DNS要求は後続のルールに対して評価され、最終的にはグローバルブロックによってブロックされる可能性があります。

たとえば、ポリシーは次のように設定できます。

1. Permit:DNSトラフィック/任意の宛先
2. Deny：任意のプロトコル/任意の宛先

この設定では、DNSトラフィックは目的の許可ルールに一致せず、後続のDeny Any/Anyルールによってブロックされる可能性があります。

混乱の原因

Cisco Secure Accessを使用すると、管理者は次のようなアプリケーションプロトコルを選択できます。

- DNS
- HTTPS経由のDNS(DoH)
- TLS経由のDNS(DoT)

インターネットアクセスポリシールールを設定するとき。

これにより、アプリケーションプロトコル条件を使用して、DNSトラフィックを常に独立して許可または拒否できると期待できます。ただし、DNSトラフィックは特定のポリシー評価動作の対象となり、アプリケーションプロトコルまたはサービスベースの条件（サービスオブジェクト）がこのルール設定で期待どおりに評価されない場合があります。

環境

- この問題は、次の環境に該当します。
  - シスコセキュアアクセス(SSE)
  - 複数のルールを含むインターネットアクセスポリシー
  - プロトコル/アプリケーションベースのルールと最後のDeny Any/Anyルールの組み合わせ
  - 先行するPermitルールに一致することが予想されるが、代わりに後続のルールまたはグローバルブロックによってブロックされるDNSトラフィック

解決策

現在、このポリシー構造でDeny Any/Anyルールに続く場合、Permit Any/Any DNSルールが独立してDNSトラフィックに一致することを保証する設定はサポートされていません。

お客様は、最終的なDeny Any/Anyルールを含むインターネットアクセスポリシーを設計する際に、このポリシー評価の制限を認識する必要があります。

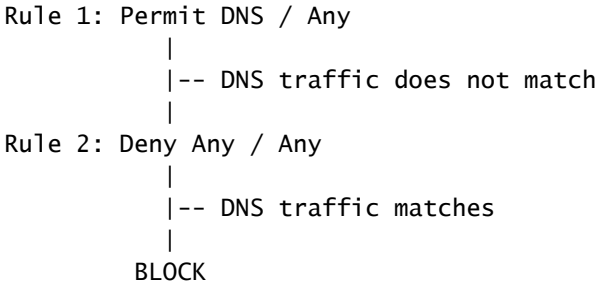
DNSトラフィックを許可する必要がある場合、ポリシーは、評価対象のDNSトラフィックに適用できる、サポートされているルール条件を使用して設計する必要があります。

原因

DNSトラフィックは、一般的なアプリケーショントラフィックと同様に、サービスベースの条件に対して評価されません。

評価対象のDNSトラフィックに適用できない条件がポリシールールに含まれている場合、ルールは一致しません。ポリシーの評価は、次の該当するルールに進みます。

例：



したがって、Deny Any/Anyルールの真上にPermit DNSルールを配置しても、DNSトラフィックが許可されるとは限りません。

関連コンテンツ

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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。