# ASA： 8.4(3) へのアップグレード後に NAT アドレスへのインバウンド アクセスが失敗する

## 目次



## 概要

このドキュメントでは、バージョン 8.4(3) に適応型セキュリティ アプライアンス（ASA）をアップグレードした後に失敗する NAT アドレスに関する情報を提供します。 また、この問題の解決策についても説明します。

## 前提条件

### 要件

このドキュメントの読者は次のトピックについて理解している必要があります。

- アドレス解決プロトコル（ARP）およびプロキシ ARP の概念に関する基本的な知識

### 使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づくものです。

- 任意の Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- 適応型セキュリティ アプライアンス バージョン 8.4(3) 以降

### 表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

# 症状

ASA バージョン 8.4(3) 以降、ASA は、IP アドレスがインターフェイスの IP サブネットの一部でない場合、そのインターフェイスで受信した ARP 要求に応答しません。 8.4(3) よりも前のバージョンでは、ASA は、ASA のインターフェイス IP サブネットの一部でない ARP 要求にも応答しました。

この変化は、ASA をバージョン 8.4(3) にアップグレードするとすぐに発生します。 場合によっては、インターネット ユーザは、ASA を介して変換されたサーバのグローバル アドレスに接続できません。

この状況が発生すると、次のメッセージが表示され、ASA の CLI で「debug arp」が有効になります。

```
arp-in: Arp packet received from 192.168.10.1 which is in different subnet
than the connected interface 192.168.11.1/255.255.255.0
```

この問題の原因はバグではありません。 可能性のある原因および解決策の詳細については、以下を参照してください。

# 状況および環境

この問題を発生させるには、ASA は、設定された NAT 変換のグローバル アドレスと一致する IP アドレスの ARP 要求を受け取る必要があります。 グローバル IP アドレスは、ASA のインターフェイスで設定されている IP サブネットとは別の IP サブネットに常駐する必要があります。

# 原因/問題の説明

この問題が与えるすべての影響を理解するには、この問題の原因およびこの問題を軽減するための最良の方法を十分に理解しておく必要があります。

次に、この問題が発生する状況をいくつか示します。

**アップストリーム デバイスの IP ルートのネクスト ホップ IP アドレスが設定されていない**

この問題の一般的な原因です。 これは、アップストリーム デバイスの構成が最適ではないことが原因です。 IP ルートのネクスト ホップが、インターフェイスのアドレスと同じサブネットの IP アドレスとなるように、IP ルートを設定することお勧めします。

```
ip route 10.1.2.0 255.255.255.0 192.168.1.2
```

ただし、ネットワーク管理者によって、ネクスト ホップとして、IP アドレスではなく、インターフェイスが設定されている場合もあります。

```
ip route 10.1.2.0 255.255.255.0 FastEthernet0/1
```

この場合、ルータは、10.1.2.0/24 ネットワークを宛先とするトラフィックを FastEthernet0/1 インターフェイスにルーティングし、IP パケットの宛先 IP アドレスの ARP 要求を送信します。 一部のデバイスが ARP 要求に応答してから、ルータが ARP プロセスにより解決された MAC アドレスにパケットを転送することを前提としています。 このような設定のメリットは、設定と管理が非常に簡単になるということです。 管理者は、ルートのネクスト ホップ IP アドレスを明示的に設定する必要はなく、隣接デバイスでプロキシ ARP が有効にされ、パケットを宛先 IP アドレスにルーティングできる場合は ARP 要求に応答することを前提としています。

ただし、このような IP ルート設定には重大な問題があります。

- ARP 要求を送信して IP トラフィックのネクスト ホップを判別することで、ルータは、その ARP 要求に正しく応答しない他のデバイスにより生じる問題の影響を受けます。 この結果、トラフィックは、正しくないデバイスに送信されるとブラックホールに入ります。
- このルート設定では、デバイスは、ルートに一致するパケットのすべての固有な宛先アドレスの ARP 要求を送信します。 これにより、サブネットに大量の ARP トラフィックが発生し、大量の ARP エントリの保持に必要なパフォーマンスおよびメモリ使用に悪影響を及ぼします。
- ARP テーブル スペースはメモリ バウンド リソースであるため、大量のエントリにより、ルータのパフォーマンスおよび安定性に悪影響を及ぼします。

そのため、最良の方法は、すべてのルータに明示的な IP ネクスト ホップ アドレスを設定し、発信インターフェイスの識別のためにインターフェイスの名前を使用するルートを使用しないことです。 フェールオーバーの出力インターフェイスへのルートにインターフェイスを接続する必要がある場合、出力インターフェイス名とスタティック ルートのネクスト ホップの両方を入力します。

一部のシスコのお客様には、管理のために新しく安全な動作を設定できるように、機能拡張の要求がオープンにされています。 Cisco バグ ID CSCty95468 （登録ユーザのみ）（ENH: 非接続サブネットからの ARP キャッシュ エントリを許可するコマンドの追加）

### 隣接デバイスの不一致 IP サブネット マスク

ASA のインターフェイスと隣接デバイスのインターフェイスで設定されている IP サブネット マスクが一致しないと、同様の問題が発生します。 隣接デバイスのサブネット マスクが、ASA のインターフェイス IP サブネット マスク（255.255.255.0）のスーパーネット（255.255.240.0）である場合、隣接デバイスは、ASA のインターフェイス IP サブネットにない IP アドレスの ARP を要求します。 サブネット マスクが正しいことを確認します。

### トランスペアレント モードについて

この変化により、トランスペアレント モードの非直接接続サブネットから MAC アドレスを学習できないという問題もあります。 これは、次の状況の通信に影響します。

- トランスペアレント ASA で、管理 IP アドレスが設定されていない、または設定が正しくない。
- トランスペアレント ASA が同じセグメントのセカンダリ サブネットを使用している。

ダウングレードする以外、トランスペアレント モードでのこの問題の回避策はありません。 ただし、この拡張機能の要求は、ASA がトランスペアレント モードでセカンダリ サブネットと相互運用できるようにオープンにされています。 Cisco バグ ID CSCty49855 （登録ユーザのみ）（ENH: MAC Discovery Mechanism での非直接接続ホストのサポート）

## 解決策

この問題（問題の IP アドレスが ASA のインターフェイス IP と同じレイヤ 3 サブネットにない場合）の解決策は、デバイスで IP アドレスの代わりにプロキシ ARP を使用せずに、ASA に隣接するデバイスが、ネクスト ホップ デバイスとして ASA のインターフェイス IP アドレスにトラフィックを直接ルーティングできるように、必要な変更を行うことです。

## 関連情報

- テクニカルサポートとドキュメント - Cisco Systems