ASA ネットワーク アドレス変換構成のトラブルシューティング

目次

概要

このドキュメントでは、Cisco 適応型セキュリティ アプライアンス (ASA) プラットフォームでのネットワーク アドレス変換 (NAT) 設定をトラブルシュートする方法を説明します。 このドキュメントは、ASA バージョン 8.3 以降に適用されます。

> **注:** 基本的な NAT 設定を紹介するビデオなどの基本的な NAT 設定の一部の例は、このドキュメントの最後の「関連情報」を参照してください。

ASA での NAT 設定のトラブルシュート

NAT の設定をトラブルシュートする場合、ASA での NAT 設定が NAT ポリシー テーブルを構築するためにどのように使用されているかを理解することが重要です。

以下の設定の誤りが、ASA 管理者が直面する NAT の問題の大部分の原因です。

- NAT 設定ルールが正常に動作していません。 たとえば、手動の NAT ルールは NAT テーブルの最上位に置かれ、これが NAT テーブルのずっと下の方にあるより特殊なルールがまったく

一致しない原因になります。
- NAT 設定で使用されるネットワーク オブジェクトが幅広過ぎるため、これが誤ってこれらの NAT ルールと一致するためにトラフィックを発生させ、より特殊な NAT ルールを見逃す原因になります。

パケット トレーサ ユーティリティは、ASA のほとんどの NAT 関連の問題を診断するのに使用できます。 NAT 設定を NAT ポリシー テーブルの構築に使用する方法、および特定の NAT の問題をトラブルシュートし解決する方法の詳細については、次の項を参照してください。

また、**show nat detail コマンド**は、新しい接続によってどの NAT ルールが一致するのかを理解するために使用できます。

ASA 設定を NAT ポリシー テーブルの構築に使用する方法

ASA によって処理されたすべてのパケットは NAT テーブルに対して評価されます。 この評価は、最上位（セクション 1）から始まり NAT ルールが一致するまで下位に移動します。 NAT ルールが一致すると、その NAT ルールが接続に適用され、それ以上の NAT ポリシーは、そのパケットに対して検査されません。

ASA の NAT ポリシーは NAT 設定から構築されます。

ASA NAT テーブルの 3 つのセクションは次のとおりです。

セクション 1	**手動 NAT ポリシー** これらは、このポリシー内で設定に表示される順序で処理されます。
セクション 2	**オート NAT ポリシー** これらは NAT のタイプ（スタティックまたはダイナミック）とオブジェクトのプレフィック（サブネット マスク）長に基づいて処理されます。
セクション 3	**オート後手動 NAT ポリシー** これらは、このポリシー内で設定に表示される順序で処理されます。

次の図は異なる NAT セクションおよびそれらがどのように命令されるかを示します。

この例は、2 ルール（1 個の手動 NAT 文と 1 個のオート NAT 設定）の ASA の NAT 設定が NAT テーブルでどのように表されるかを示しています。

NAT 問題をトラブルシュートする方法

パケット トレーサ ユーティリティを使用

NAT の設定の問題をトラブルシュートするには、パケットが NAT ポリシーに一致することを確認するために**パケット トレーサ** ユーティリティを使用します。 パケット トレーサでは ASA に入るサンプル パケットを指定でき、ASA はそのパケットに適用する設定およびそれが許可されるかどうかを指定します。

次の例では、内部インターフェイスに入りインターネット上のホストに着信するサンプル TCP パケットが示されています。 パケット トレーサ ユーティリティは、ダイナミック NAT ルールに一致し **172.16.123.4** の外部 IP アドレスに変換されたパケットを表示します。

```
ASA# packet-tracer input inside tcp 10.10.10.123 12345 209.165.200.123 80

...(output omitted)...

Phase: 2
Type: NAT
Subtype:
Result: ALLOW
Config:
object network 10.10.10.0-net
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 10.10.10.123/12345 to 172.16.123.4/12345

...(output omitted)...

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow

ASA#
```

NAT ルールを選択し、Cisco Adaptive Security Device Manager（ASDM）からのパケット トレーサを有効化するために [Packet Trace] をクリックします。 これは、パケット トレーサ ツールの入力として NAT ルールで指定された IP アドレスを使用します。

show nat コマンドの出力の表示

show nat detail コマンドの出力は NAT ポリシー テーブルを確認するために使用できます。 具体的には、**translate_hits** と **untranslate_hits** のカウンタが、どの NAT エントリが ASA で使用されているかを判断するために使用できます。 新しい NAT のルールに **translate_hits** か **untranslate_hits** がないことがわかった場合、これはトラフィックが ASA に到達しないか、あるいは NAT テーブルで優先度のより高い別のルールがそのトラフィックと一致しているかのどちらかを意味します。

異なる ASA 設定からの NAT 設定と NAT ポリシー テーブルを次に示します。

前記の例では、この ASA で設定された 6 つの NAT ルールがあります。 **show nat** の出力は、各ルールの **translate_hits** と **untranslate_hits** の数だけでなく、これらのルールが NAT ポリシー テーブルの構築にどのように使われるかを示します。 これらの一致カウンタは接続のたびに 1 度だけ増加します。 接続が ASA 経由で構築された後、この現在の接続と一致する後続のパケットは NAT 行を増やしません（ASA 上で動作するアクセス リストの一致カウントの方法と非常に似ています）。

Translate_hits： 順方向で NAT ルールに一致する新しい接続の数。

「順方向」は、接続が NAT ルールで指定されたインターフェイスの方向で ASA を通過して構築されたことを意味します。 NAT ルールで内部サーバが外部インターフェイスに変換されると指定されている場合、NAT ルールでのインターフェイスの順序は「nat (inside,outside)...」となり、そのサーバで外部のホストへの新しい接続が開始する場合、**translate_hit** カウンタが増加します。

Untranslate_hits： 逆方向で NAT のルールに一致する新しい接続の数。

NAT ルールで内部サーバが外部インターフェイスに変換されると指定されている場合、NAT ルールでのインターフェイスの順序は「nat (inside,outside)...」となり、 ASA の外部クライアントが内部のサーバへの新しい接続を開始しタ場合、untranslate_hit カウンタが増加します。

再度の説明になりますが、新しい NAT のルールに translate_hits か untranslate_hits がないことがわかった場合、これはトラフィックが ASA に到達しないか、あるいは NAT テーブルで優先度のより高い別のルールがそのトラフィックと一致しているかのどちらかを意味します。

NAT 問題のトラブルシューティング方法論

サンプル パケットが ASA の適切な NAT 設定ルールに一致することを確認するにはパケット トレーサを使用します。 どの NAT ポリシー ルールが一致したのかを理解するために show nat detail コマンドを使用します。 接続が予定と異なる NAT 設定に一致している場合、次の質問を使ってトラブルシュートしてください。

- トラフィックを一致させようとした NAT ルールに優先する別の NAT ルールがありますか。
- このトラフィックが誤ったルールと一致する原因となる、幅広過ぎるオブジェクト定義（サブネット マスクが 255.0.0.0 のように短過ぎる）を含む別の NAT ルールがありますか。
- パケットが間違ったルールに一致する原因になる、手動 NAT ポリシーの規則違反はないですか。
- NAT ルールが正しく設定されてなくて、それがトラフィックがルールに一致しない原因になっていませんか。

問題の例とその解決策については、次の項を参照してください。

NAT 設定の一般的な問題

ASA で NAT を設定するときに発生する一般的な問題を次に示します。

問題： NAT Reverse Path Failure（RPF）のエラーが原因のトラフィックの失敗：非対称 NAT ルールが、順方向および逆方向のフローと一致

NAT RPF チェックは、順方向の ASA によって変換された TCP 同期（SYN）のような接続が、TCP SYN/ACK などの逆方向の同じ NAT ルールによって変換されるかを確認します。

多くの場合、この問題は NAT 文の宛先がローカル（未変換）アドレスの着信接続が原因となります。 基本的なレベルで、NAT RPF はサーバからクライアントへのリバース接続が同じ NAT ルールと一致することを確認します。 そうでない場合は、NAT RPF チェックが失敗します。

例：

209.165.200.225 の外部ホストが 10.2.3.2 のローカル（未変換）の IP アドレスに着信するパケットを直接転送する場合、ASA はパケットを廃棄しこれを syslog に口グします。

```
ASA# packet-tracer input inside tcp 10.10.10.123 12345 209.165.200.123 80
```

```
...(output omitted)...

Phase: 2
Type: NAT
Subtype:
Result: ALLOW
Config:
object network 10.10.10.0-net
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 10.10.10.123/12345 to 172.16.123.4/12345

...(output omitted)...

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow

ASA#
```

解決策：

最初に、ホストが適切なグローバル NAT アドレスにデータを送信することを確認します。 ホストが正しいアドレスに着信するパケットを送った場合、その接続に一致した NAT ルールを検査します。 NAT のルールが正しく定義されていること、および NAT のルールで参照されるオブジェクトが正しいことを確認します。 また、NAT ルールの順序が適切であることを確認します。

拒否されたパケットの詳細を指定するために、パケット トレーサ ユーティリティを使用します。 パケット トレーサは RPF チェックの失敗により廃棄されたパケットを示します。 次に、NAT フェーズおよび NAT-RPF フェーズでどの NAT ルールが一致したのかを確認するために、パケット トレーサの出力を参照します。

パケットが、NAT RPF チェック フェーズで NAT ルールに一致し、これが逆フローが NAT 変換に一致することを示し、しかし NAT フェーズのルールに一致せず、これが順フローが NAT ルールに一致しないことを示す場合は、パケットが廃棄されます。

この出力は、外部ホストが間違ってグローバル (変換された) IP アドレスではなくサーバのローカル IP アドレスにトラフィックを送信した前の図に示すシナリオと一致します。

```
ASA# packet-tracer input outside tcp 209.165.200.225 1234 10.2.3.2 80

.....

Phase: 8
Type: NAT
Subtype: rpf-check
Result: DROP
Config:
object network inside-server
nat (inside,outside) static 172.18.22.1
Additional Information:
...
ASA(config)#
```

パケットが 172.18.22.1 の正しいマッピング IP アドレスに着信する場合、パケットは順方向で

UN-NAT フェーズの正しい NAT ルールおよびおよび NAT RPF チェック フェーズでの同じルールに一致します。

```
ASA(config)# packet-tracer input outside tcp 209.165.200.225 1234 172.18.22.1 80
...
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network inside-server
nat (inside,outside) static 172.18.22.1
Additional Information:
NAT divert to egress interface inside
Untranslate 172.18.22.1/80 to 10.2.3.2/80
...
Phase: 8
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network inside-server
nat (inside,outside) static 172.18.22.1
Additional Information:
...

ASA(config)#
```

問題： 手動 NAT ルールは規則違反で、これが不正なパケットの一致の原因

手動 NAT ルールは、設定の発生に基づいて処理されます。 非常に広範な NAT ルールが設定に最初にリストされている場合は、これが NAT テーブルで下の方にあるより特別なルールに優先する可能性があります。 どの NAT ルールにトラフィックが一致するのかを確認するためにパケットトレーサを使用します。 別の順序に手動 NAT エントリを再割り当てする必要がある場合があります。

解決策：

ASDM で NAT ルールの順序を変更します。

解決策：

NAT のルールは、ルールを削除して特定の行番号に再挿入する場合は、CLI で並べ替えできます。 特定の行に新しいルールを挿入するには、インターフェイスに指定された後に行番号を入力します。

例：

```
ASA(config)# nat (inside,outside) 1 source static 10.10.10.0-net
10.10.10.0-net destination static 192.168.1.0-net 192.168.1.0-net
```

問題： NAT のルールは非常に広範囲で、一部のトラフィックに誤って一致する

非常に広範囲オブジェクトを使用して NAT ルールが作成されることがあります。 これらのルールが NAT テーブルの最上位近く（たとえば、セクション 1 の最上位）にある場合、意図されている以上のトラフィックに一致し、テーブルのかなり下の NAT ルールがまったく一致しない原因になる場合があります。

解決策：

トラフィックが範囲が広すぎるオブジェクト定義のルールと一致するかどうかを判断するには、パケット トレーサを使用します。 これに当たる場合、そのオブジェクトの範囲を減らすか、または NAT テーブルのずっと下にルールを移動するか、または NAT テーブルのオート後（セクション 3）に移動します。

問題： NAT ルールが誤ったインターフェイスにトラフィックを転送

NAT ルールは、どのインターフェイスがパケットを ASA に出力するかを決定する際にルーティング テーブルに優先できます。 受信パケットが NAT 文で変換された IP アドレスに一致する場合、出力インターフェイスを決定するために NAT ルールが使用されます。

NAT 転送チェック（ルーティング テーブルを上書きできるもの）は、インターフェイス上で受信される受信パケットの宛先アドレスの変換を指定する NAT ルールがあるかどうかを確認するためにチェックを行います。 そのパケットの宛先 IP アドレスを変換する方法を明示的に指定するルールがない場合、出力インターフェイスを決定するためにグローバル ルーティング テーブルが参照されます。 そのパケットの宛先 IP アドレスを変換する方法を明示的に指定するルールがある場合、NAT ルールはパケットを変換でほかのインターフェイスに「取得」し、グローバル ルーティング テーブルが効果的にバイパスされます。

この問題は、外部インターフェイスに到達する着信トラフィックで非常によく見られ、通常は意図しないインターフェイスにトラフィックを転送する規則違反の NAT ルールが原因です。

例：

解決策：

この問題は、次のいずれかで解決することができます。

- より特別なエントリが最初にリストされるように NAT テーブルを並び替えます。
- NAT 文でオーバーラップしないグローバル IP アドレスの範囲を使用します。

NAT ルールが同一のルールの場合（これは IP アドレスがルールによって変更されないことを意味します）、**route-lookup** キーワードが使用できます（このキーワードは、NAT のルールが同一のルールではないため上記の例に適用できるわけではありません）。 **route-lookup キーワードは**、NAT ルールに一致する場合に ASA が追加チェックを実行する原因になります。 このチェックでは、ASA のルーティング テーブルがこの NAT 設定でパケットを転送する先の同じ出力インターフェイスにパケットを転送していることを検査します。 ルーティング テーブルの出力インターフェイスが NAT 転送インターフェイスと一致しなければ、NAT ルールは一致せず（ルールはとばされます）、パケットはその後の NAT ルールで処理されるために NAT テーブルの参照を下方向に続けます。

ルート検索オプションは、NAT のルールが「同一」の NAT ルールである場合、つまり IP アドレスがルールによって変更されない場合にのみ使用できます。 ルート検索オプションは、NAT 行の最後に **route-lookup** を追加するか、または ASDM の NAT ルール設定で [Lookup route table to locate egress interface] チェックボックスをチェックする場合に NAT ルールごとに有効にできま

す。

問題： NAT ルールは、マッピング インターフェイスのトラフィック用の Proxy Address Resolution Protocol (ARP) に対する ASA の原因になります。

グローバル IP アドレスの ASA プロキシ ARP は、グローバル インターフェイスでの NAT 文の範囲です。 このプロキシ ARP 機能は、NAT 文に **no-proxy-arp** キーワードを追加する場合 NAT ルール単位で無効にできます。

またこの問題は、間違ってグローバル アドレス サブネットが意図するよりも極端に大きく作成された場合も発生します。

解決策：

可能なら、NAT 行に **no-proxy-arp** キーワードを追加します。

例：

```
ASA(config)# object network inside-server
ASA(config-network-object)# nat (inside,outside) static 172.18.22.1 no-proxy-arp
ASA(config-network-object)# end
ASA#
ASA# show run nat
object network inside-server
nat (inside,outside) static 172.18.22.1 no-proxy-arp
ASA#
```

これは、ASDM を使用しても実行できます。 NAT ルールで、[Disable Proxy ARP on egress interface] チェックボックスをチェックします。

関連情報

- ビデオ： DMZ サーバ アクセス (バージョン 8.3 および 8.4) の ASA ポート転送
- 基本的な ASA NAT コンフィギュレーション： ASA バージョン 8.3 以降の DMZ の Web サーバ
- ブック 2： Cisco ASA シリーズ ファイアウォール CLI コンフィギュレーション ガイド、9.1
- テクニカル サポートとドキュメント – Cisco Systems