ASAネットワークアドレス変換(NAT)設定のトラブルシューティング

内容

はじめに

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）プラットフォーム上のネットワーク アドレス変換（NAT）設定をトラブルシュートする方法について説明します。

前提条件

要件

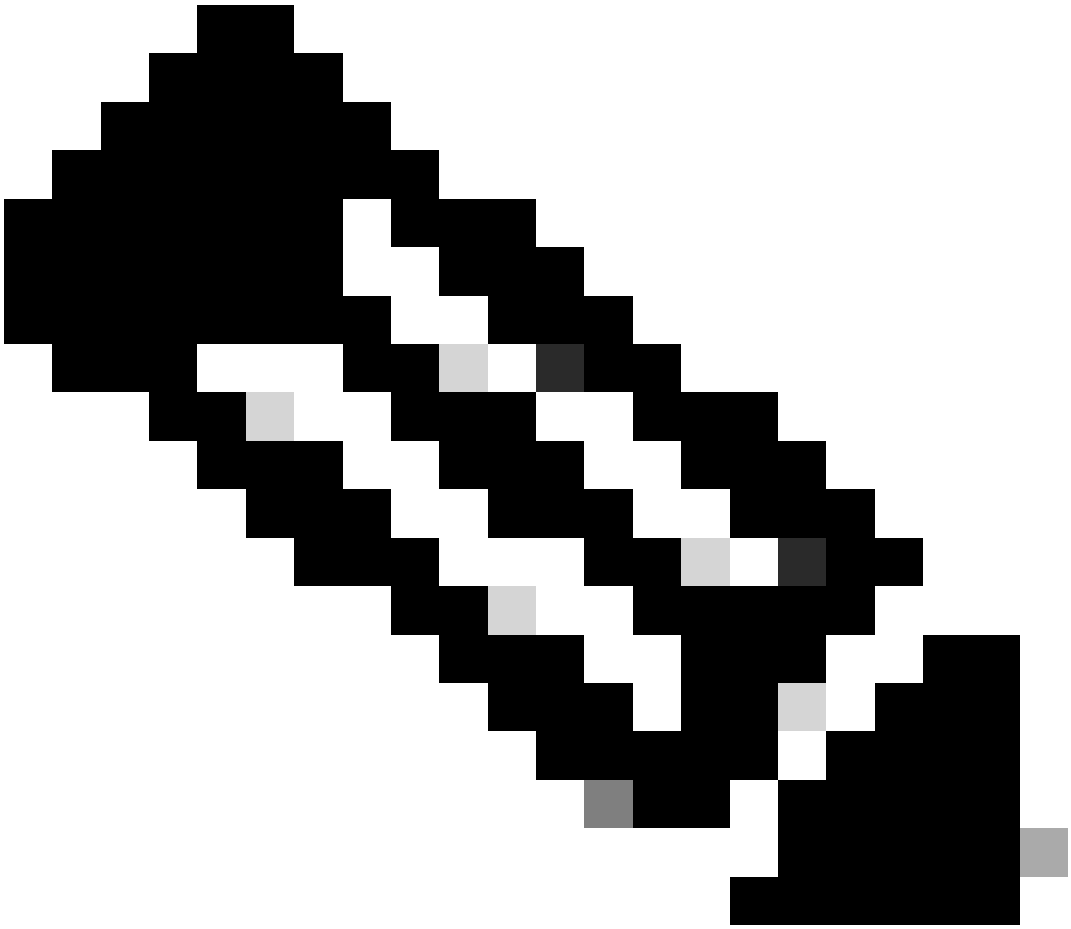
このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、ASAバージョン8.3以降に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ASA の NAT 設定のトラブルシューティング



注：基本的なNAT設定を紹介するビデオを含む、NAT設定の基本的な例については、このドキュメントの最後の「関連情報」のセクションを参照してください。

NAT 設定のトラブルシューティングを行う場合は、NAT ポリシー テーブルを作成するために ASA の NAT 設定がどのように使用されているかを理解する必要があります。

ASA 管理者が直面する NAT の問題の大部分の原因は、次のような設定の誤りです。

- NAT 設定ルールの順序が間違っています。たとえば、手動 NAT ルールが NAT テーブルの最上位に置かれているため、NAT テーブルの下位に置かれている限定性の高いルールがヒットしなくなっています。
- NAT 設定で使用されるネットワーク オブジェクトが広範すぎるため、トラフィックがこれらの NAT ルールに誤って一致し、より限定性の高いルールが無視されています。

パケット トレーサ ユーティリティを使用して、ASA の NAT に関連する大部分の問題を診断でき

ます。NAT 設定を使用して NAT ポリシー テーブルを作成する方法と特定の NAT の問題をトラブルシューティングして解決する方法の詳細については、次のセクションを参照してください。

また、show nat detail コマンドを使用して、新しい接続がどの NAT ルールにヒットするかを把握することができます。

ASA 設定を使用して NAT ポリシー テーブルを作成する方法

ASA によって処理されたすべてのパケットは、NAT テーブルに照らし合わせて評価されます。この評価は、最上位（セクション 1）から始まり NAT ルールに一致するまで下位に移動します。

一般に、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ポリシーはパケットに対してチェックされませんが、次に説明する注意事項があります。

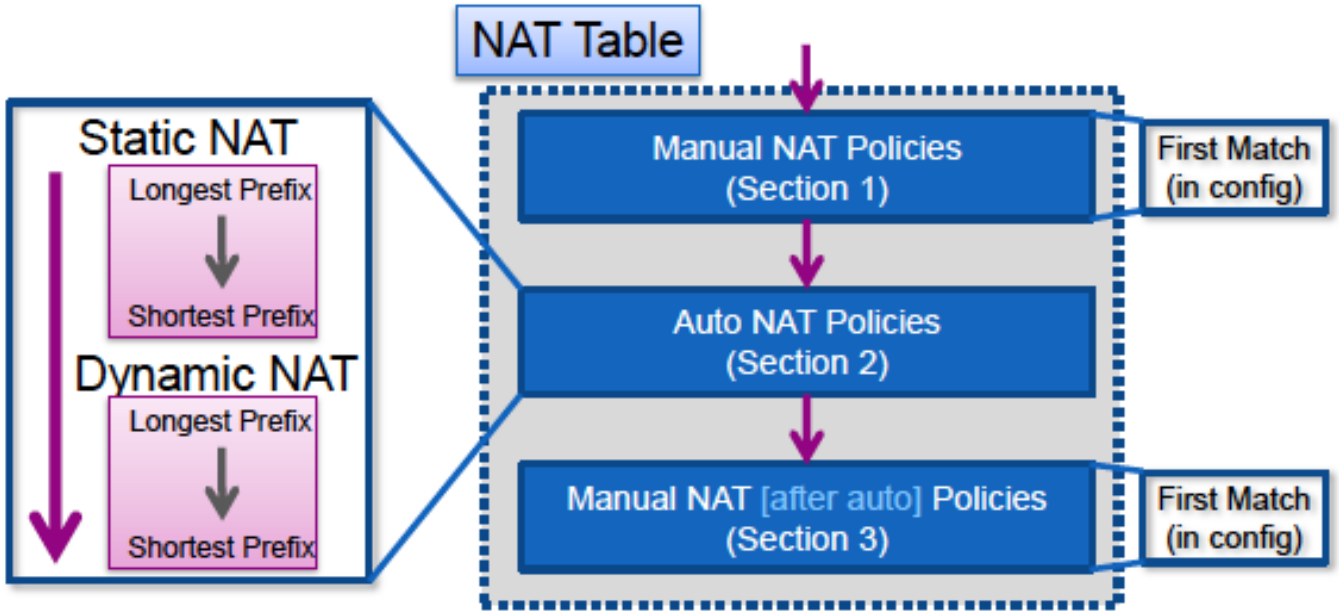
NATポリシーテーブル

ASA の NAT ポリシーは NAT 設定から作成されます。

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 これらのポリシーは、設定に表示される順に従って処理されます。
セクション 2	自動 NAT ポリシー これらのポリシーは 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ス（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	自動後の手動 NAT ポリシー これらのポリシーは、設定に表示される順に従って処理されます。

次の図は、3 つの NAT セクションとそれらの順序を示しています。



NATルールの一致

セクション 1

- フローは、最初のルールで始まるNATテーブルのセクション1に対して最初に評価されます。
  - パケットの送信元IPと宛先IPが手動NATルールのパラメータと一致する場合、変換が適用されてプロセスが停止し、どのセクションのNATルールも評価されなくなります。
  - 一致するNATルールがない場合、フローはNATテーブルのセクション2に対して評価されます。

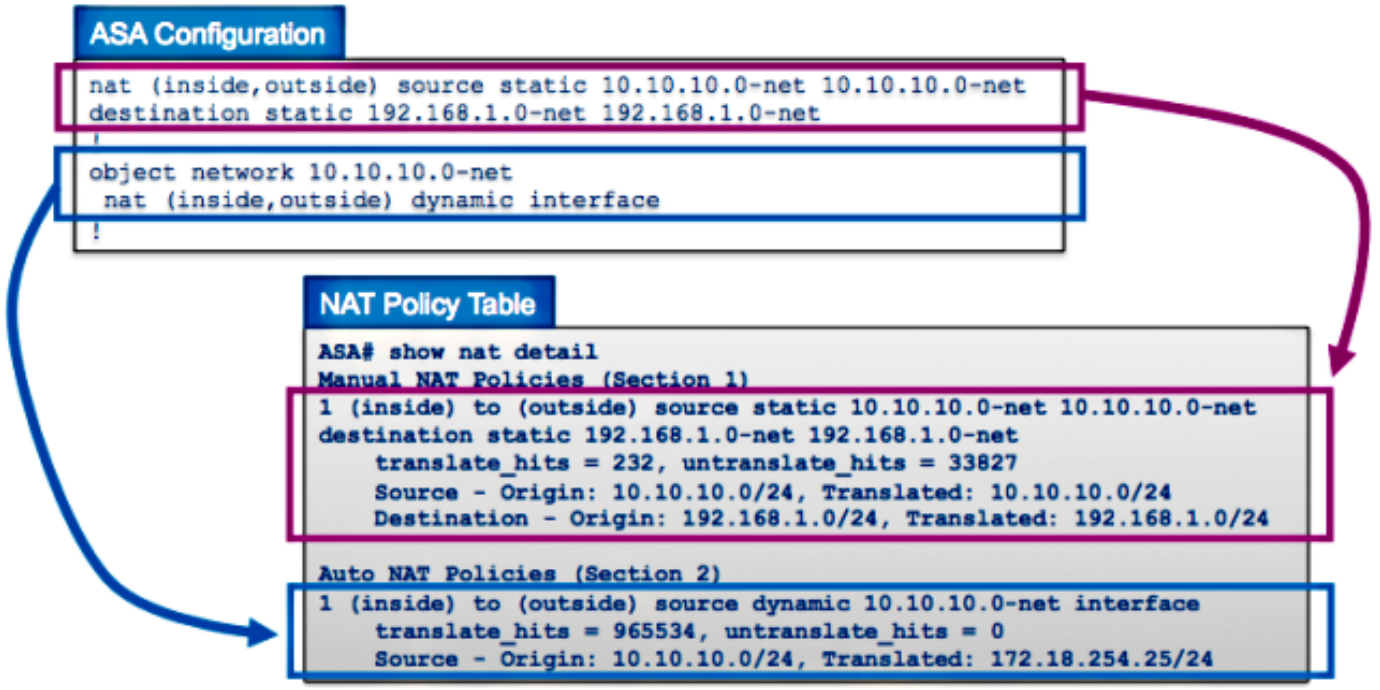
セクション 2

- フローは、セクション2のNATルールに対して、先にスタティックNATルール、次にダイナミックNATルールの順に評価されます。
  - 変換ルールがフローの送信元IPまたは宛先IPのいずれかに一致する場合、変換を適用し、残りのルールを引き続き評価して、フロー内の他のIPに一致するかどうかを確認できます。たとえば、ある自動NATルールで送信元IPを変換し、別の自動NATルールで宛先を変換することができます。
  - フローが自動NATルールに一致する場合、セクション2の終わりに達するとNATルックアップが停止し、セクション3のルールは評価されません。
  - セクション2のNATルールがフローと照合されない場合、ルックアップはセクション3に進みます

セクション 3

- セクション3のプロセスは、セクション1と基本的に同じです。 パケットの送信元IPと宛先IPが手動NATルールのパラメータと一致する場合、変換が適用されてプロセスが停止し、どのセクションのNATルールも評価されなくなります。

次の例は、2つのルール（1つの手動NATステートメントと1つの自動NAT設定）を含むASA 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 の問題をトラブルシューティングする方法

パケット トレーサ ユーティリティの使用

NAT 設定の問題をトラブルシューティングするには、パケット トレーサ ユーティリティを使用して、パケットが NAT ポリシーにヒットしていることを確認します。パケット トレーサを使用すると、ASA に入るサンプル パケットを指定できます。ASA では、そのパケットに適用される設定と、パケットが許可または拒否されるかどうかを示すことができます。

次の例では、内部インターフェイスに着信し、インターネット上のホストを宛先とするサンプルの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、パケットがダイナミック 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ることを示しています。

<#root>

ASA#

packet-tracer input inside tcp 10.10.10.123 12345 192.168.200.123 80

...(output omitted)...

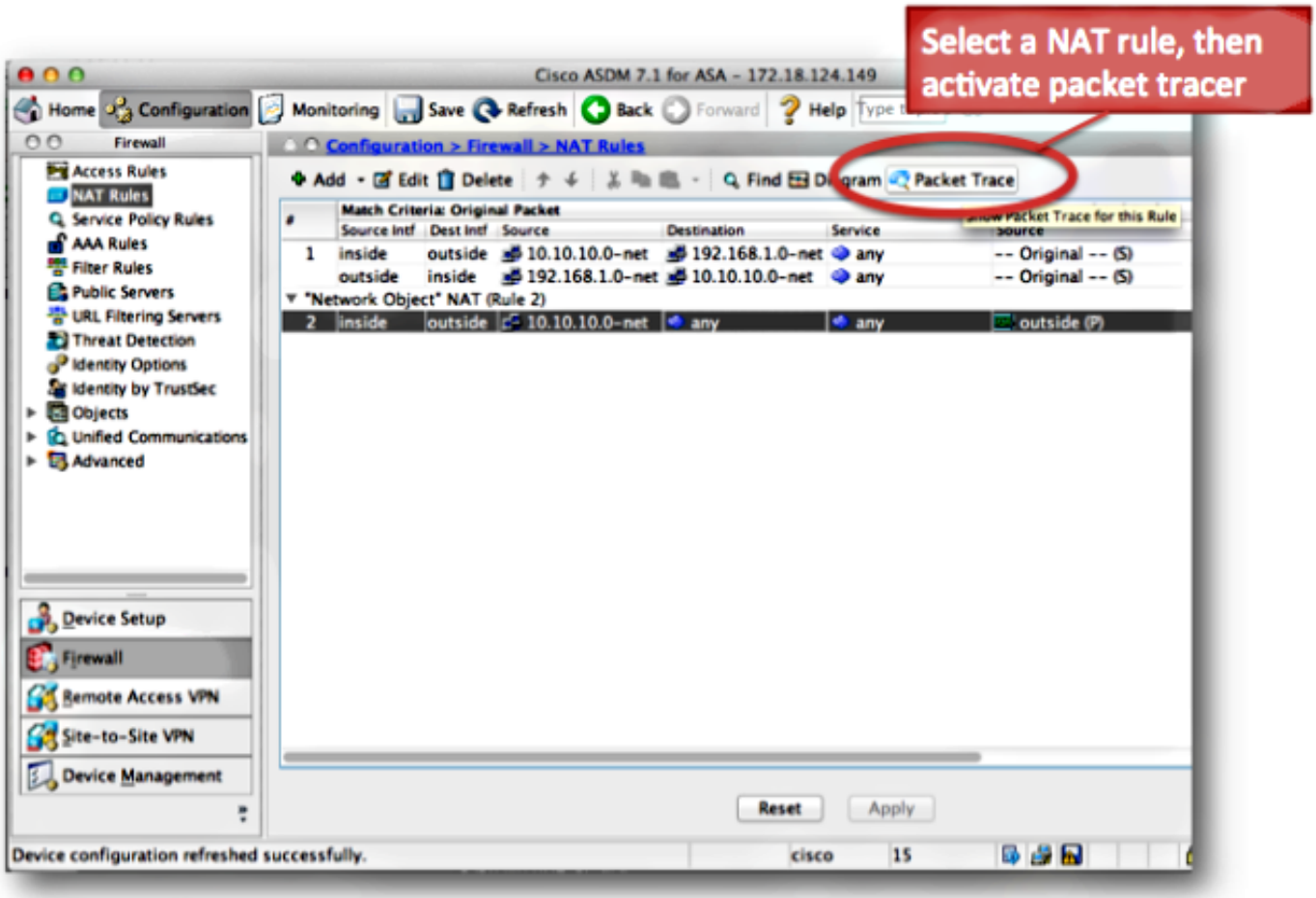
Phase: 2
Type: NAT
Subtype:
Result: ALLOW
Config:

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#
```

Cisco Adaptive Security Device Manager（ASDM）で、[NAT rule] を選択して、[Packet Trace] をクリックし、パケット トレーサをアクティブにします。ここでは、NAT ルールで指定された IP アドレスをパケット トレーサ ツールの入力として使用しています。



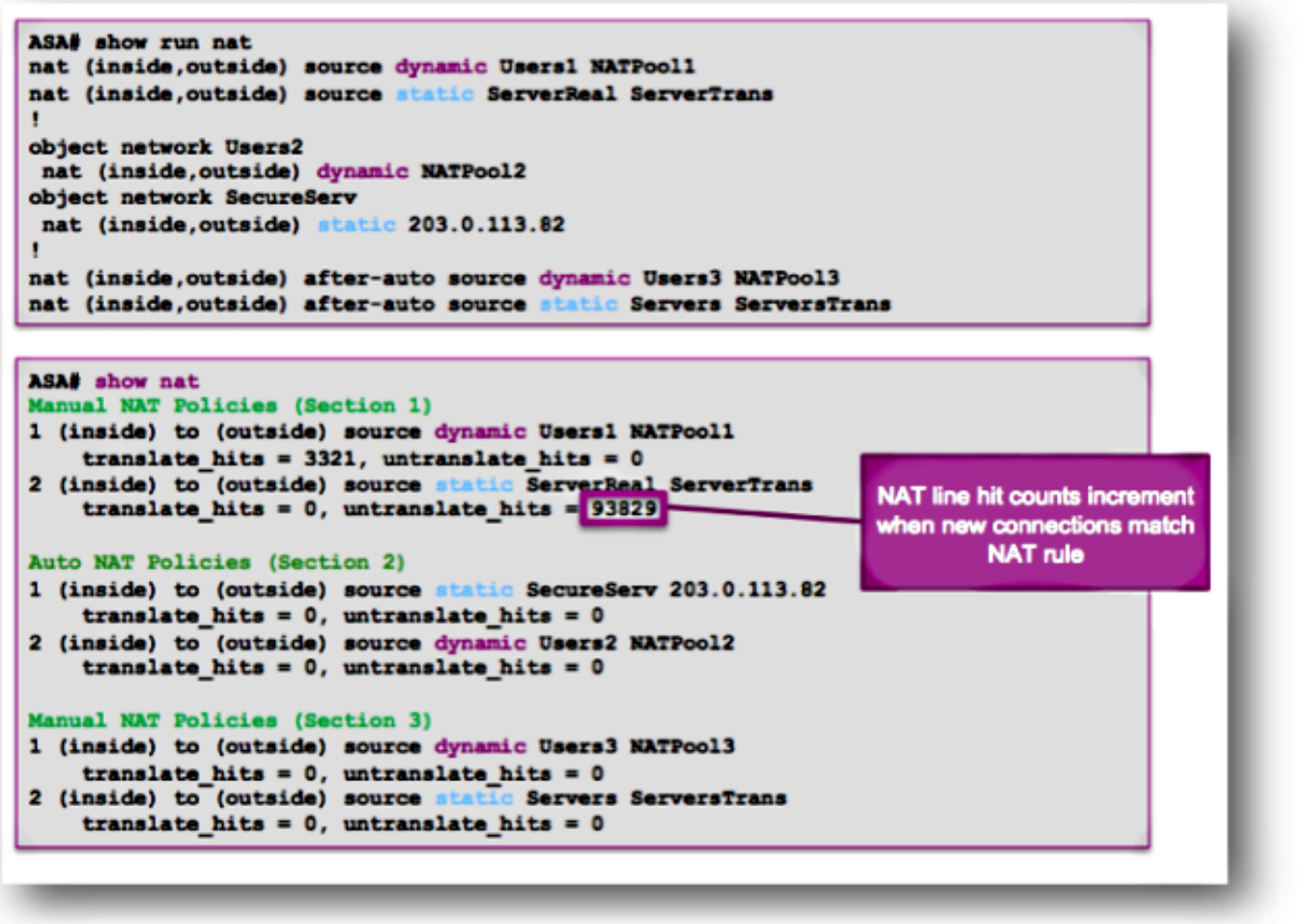
show nat コマンドの出力の表示

show nat detail コマンドの出力を使用して、NAT ポリシー テーブルを確認できます。具体的には、translate_hits と untranslate_hits のカウンタを使用して、ASA で使用されている NAT エントリ

を判別できます。

新しい NAT ルールに translate_hits または untranslate_hits がない場合は、トラフィックが ASA に到達していないか、NAT テーブルにある優先度のより高い別のルールがトラフィックと一致している可能性があります。

別の ASA 設定の NAT 設定と NAT ポリシー テーブルを次に示します。



上記の例では、この ASA には 6 つの NAT ルールが設定されています。show nat の出力は、各ルールの translate_hits と untranslate_hits の数だけでなく、これらのルールを使用して NAT ポリシー テーブルを作成する方法を示しています。

これらのヒット カウンタは接続のたびに 1 度だけ増分します。ASA を介して接続が確立された後、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 access-list ヒット カウンタが動作する方法と非常に似ています）。

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

「順方向」とは、NAT ルールで指定されたインターフェイスの方向で ASA を介して接続が確立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)...」になります。そのサーバが外部のホス

トへの新しい接続を開始すると、translate_hitカウンタが増分します。

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

InsideサーバがOutsideインターフェイスに変換されるとNATルールで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)...」になります。ASAのOutsideのクライアントがInsideのサーバへの新しい接続を開始すると、untranslate_hitカウンタが増分します。

繰り返しますが、新しい NAT ルールに translate_hits または untranslate_hits がない場合は、トラフィックが ASA に到達していないか、NAT テーブルにある優先度のより高い別のルールがトラフィックと一致している可能性があります。

NAT の問題をトラブルシューティングする際の方法論

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 ルールにヒットしたかを把握するには、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は、次の質問を参照してトラブルシューティングしてください。

- トラフィックをヒットさせようとした NAT ルールよりも優先度の高い別の NAT ルールがありますか。
- 広範すぎるオブジェクト定義（サブネット マスクが 255.0.0.0 のように短すぎる）を含む別の NAT ルールがあるため、トラフィックが間違ったルールに一致していませんか。
- 手動 NAT ポリシーの順序が間違っているため、パケットが間違ったルールに一致していませんか。
- NAT ルールが正しく設定されていないため、ルールがトラフィックに一致しなくなっていませんか。

問題の例とその解決策については、次のセクションを参照してください。

NAT 設定の一般的な問題

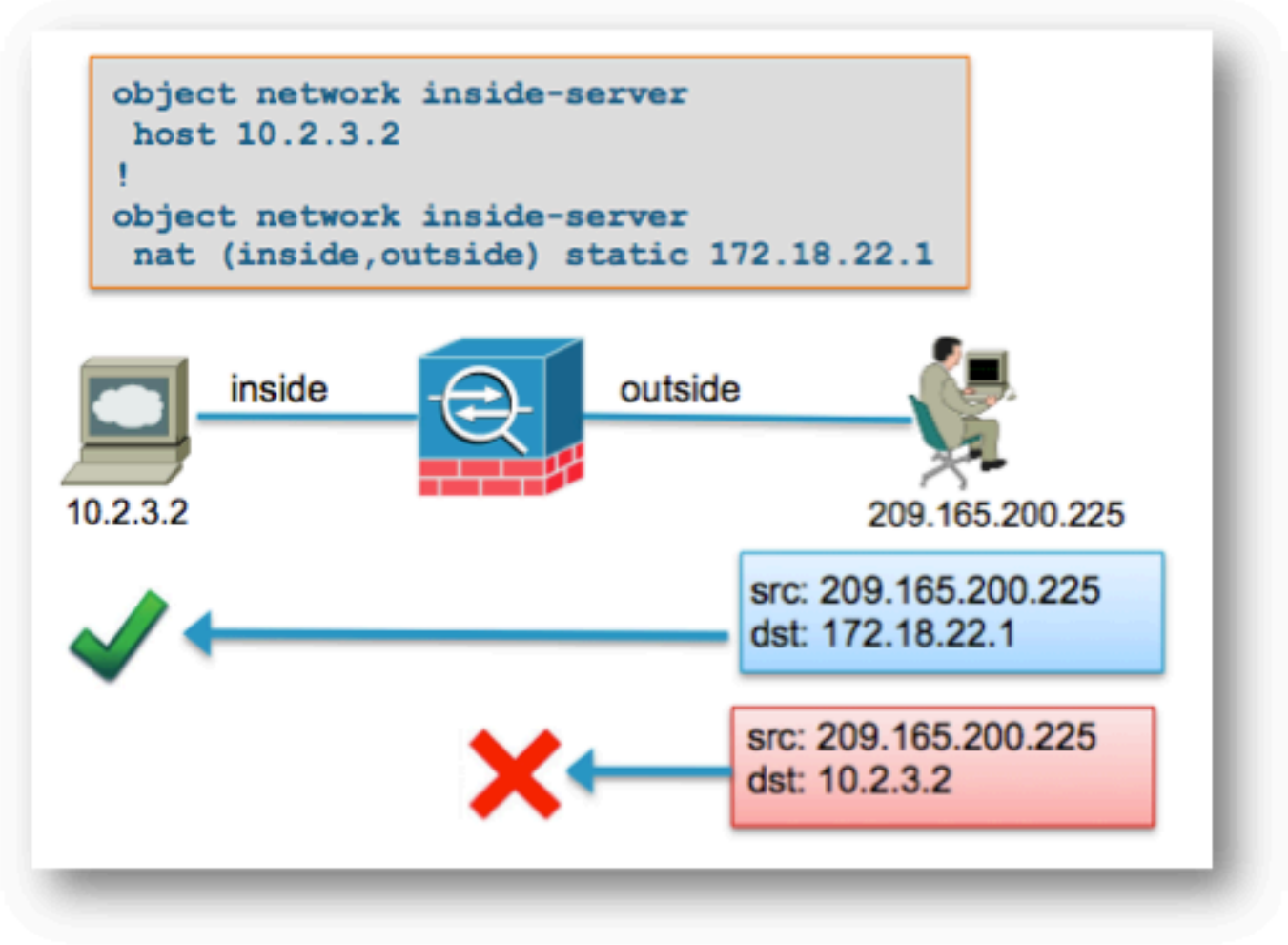
ASA で NAT を設定するときに発生する一般的な問題を次に示します。

問題：NAT Reverse Path Failure(RPF)エラーが原因でトラフィックが失敗する：非対称NATルールが順方向および逆方向のフローで一致する

NAT RPF チェックでは、TCP 同期（SYN）などで、ASA によって順方向で変換された接続が、TCP SYN/acknowledge（ACK）の場合などのように、同じ NAT ルールによって逆方向で変換されることを確認します。

多くの場合、この問題は、NAT ステートメントのローカル（未変換）アドレス宛ての着信接続が原因で発生します。基本的なレベルでは、NAT RPFはサーバからクライアントへの逆接続が同じNATルールに一致していることを確認します。一致していない場合、NAT RPFチェックは失敗します。

例： 209.165.200.225



外部ホスト 192.168.200.225 がローカル（未変換）IP アドレス 10.2.3.2 にパケットを直接送信すると、ASA はこのパケットを破棄して、この syslog にログを記録します。

```
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows;
Connection for icmp src outside:192.168.200.225 dst inside:10.2.3.2 (type 8, code 0)
denied due to NAT reverse path failure
```

ソリューション：

最初にホストが正しいグローバル 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宛てのパケットを送信する場合は、この接続にヒットする NAT ルールをチェックします。

NAT ルールが正しく定義されていて、NAT 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。

パケット トレーサ ユーティリティを使用して、拒否されるパケットの詳細を指定します。パケットトレーサは、RPFチェックの失敗によってドロップされたパケットを表示する必要があります

。

次に、パケット トレーサの出力を調べて、NAT フェーズと NAT-RPF フェーズでどの NAT ルールにヒットしたかを確認します。

NAT RPF チェック フェーズでパケットが NAT ルールに一致する場合（逆方向のフローが NAT 変換にヒットするが、NAT フェーズのルールには一致しないことに加えて、順方向のフローが NAT ルールにヒットすることを示す）、パケットが破棄されます。

この出力は、前の図に示したシナリオに一致します。このシナリオでは、外部ホストが、グローバル（変換済み）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クを誤って送信しています。

<#root>

ASA#

packet-tracer input outside tcp 192.168.200.225 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 のマッピングされた正しい IP アドレスを宛先にしている場合、パケットは順方向の UN-NAT フェーズで正しい NAT ルールに一致し、NAT RPF チェック フェーズで同じルールに一致します。

<#root>

ASA(config)#

packet-tracer input outside tcp 192.168.200.225 1234 172.18.22.1 80

...
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:

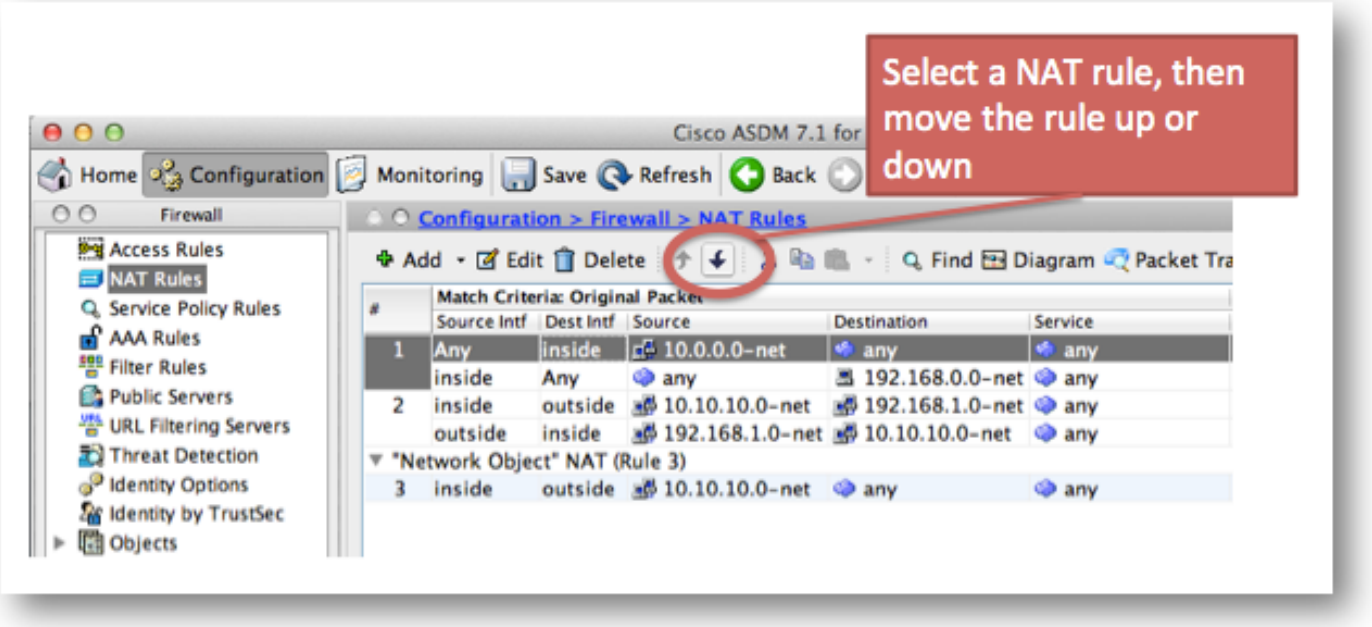
```
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
NAT divert to egress interface inside
Untranslate 172.18.22.1/80 to 10.2.3.2/80
...
Phase: 8
Type: NAT
Subtype: rpf-check
Result:

ALLOW


Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
...

ASA(config)#
```

問題：手動NATルールの順序が間違っているため、不正なパケット一致が発生する

手動 NAT ルールは、設定での表示に基づいて処理されます。非常に広範なNATルールが設定の最初にリストされている場合は、NATテーブルの下位にあるより具体的な別のルールを上書きできます。トラフィックがどのNATルールにヒットするかを確認するには、パケットトレーサを使用します。手動NATエントリを別の順序に並べ替える必要がある場合があります。

ソリューション：

ASDM で NAT ルールの順序を変更します。



ソリューション：

NAT ルールを削除して、そのルールを特定の行番号で再度挿入する場合は、CLI で NAT ルールの順序を変更できます。特定の行に新しいルールを挿入するには、インターフェイスを指定した直後に行番号を入力します。

以下に例を挙げます。

<#root>

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 ルールが広範すぎるため一部のトラフィックに誤って一致する. 広範すぎるオブジェクトを使用する NAT ルールが作成される場合があります。これらのルールがNATテーブルの上部付近（セクション1の上部など）に配置されている場合は、意図したよりも多くのトラフィックに一致することがあり、テーブルのより下のNATルールがヒットしなくなります。

解決方法

広範すぎるオブジェクト定義があるルールにトラフィックが一致するかどうかを確認するには、パケット トレーサを使用します。このような場合は、これらのオブジェクトのスコープを縮小するか、ルールをNATテーブルの下位またはNATテーブルの自動チェック後のセクション（セクション3）に移動する必要があります。

問題

NAT ルールにより、誤ったインターフェイスにトラフィックが転送される. NATルールは、パケットがASAから出力されるインターフェイスを決定する際に、ルーティングテーブルよりも優先されます。着信パケットが NAT ステートメントの変換済み IP アドレスに一致する場合は、NAT ルールを使用して、出力インターフェイスが決定されます。

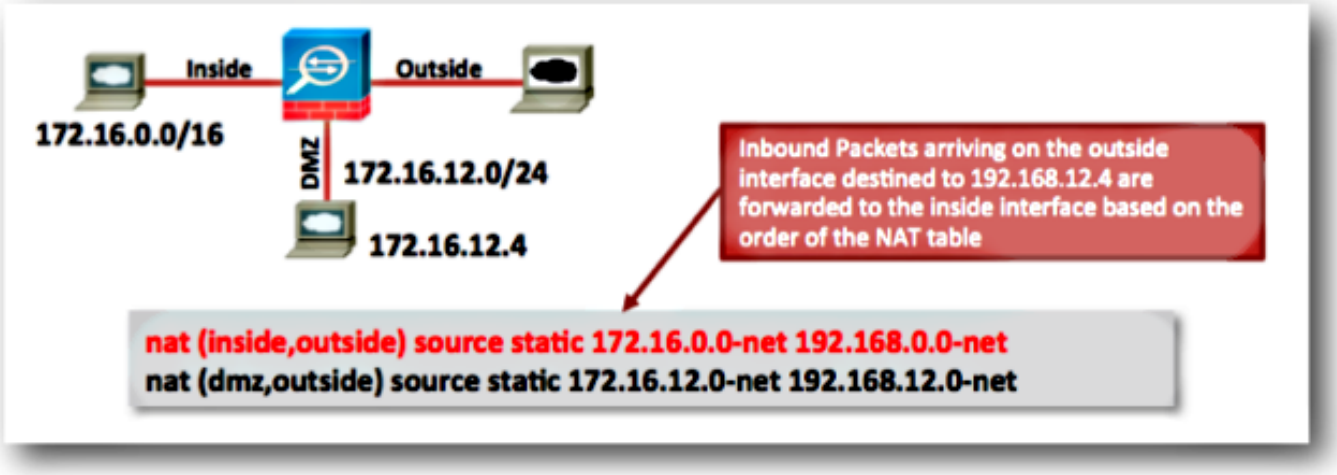
NAT 転送チェック（ルーティング テーブルをオーバーライドできる）では、インターフェイスに着信する着信パケットの宛先アドレス変換を指定する NAT ルールがあるかどうかを確認します。

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。

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内の他のインターフェイスにプルし、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着信する着信トラフィックで最も多く発生し、通常、NAT ルールの順序が間違っているためにトラフィックが意図しないインターフェイスに転送されることが原因です。

以下に例を挙げます。



解決策：

この問題は、次のいずれかの操作で解決できます。

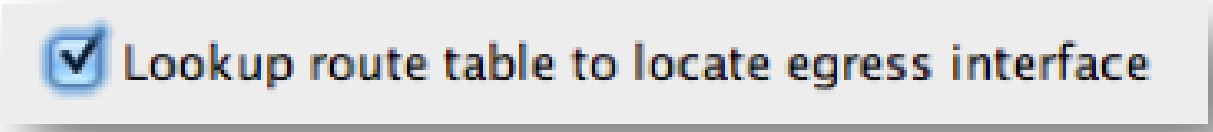
- NAT テーブルの順序を変更して、より限定性の高いエントリが上位にリストされるようにします。
- NAT ステートメントで、重複しないグローバル IP アドレスの範囲を使用します。

NATルールがIDルールの場合（つまり、IPアドレスがルールによって変更されない場合）、route-lookupキーワードを使用できることに注意してください（このキーワードは、NATルールがIDルールではないため前の例には適用されません）。

route-lookup キーワードを使用すると、ASA では、NAT ルールに一致するときに追加のチェックが実行されます。このチェックでは、ASA のルーティング テーブルによってこの NAT 設定のパケット転送先となる同じ出力インターフェイスにパケットが転送されることを確認します。

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い場合は、NAT ルールが一致せず（ルールがスキップされる）、パケットは NAT テーブルの下位に移動して、後のルールによって処理されます。

route-lookupオプションは、NATルールがアイデンティティ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。route-lookup を NAT 行の最後に追加するか、ASDM で NAT ルール設定の [Lookup route table to locate egress interface] チェックボックスをオンにしている場合、NAT ルールごとに route-lookup オプションを有効にできます。



問題：NATルールにより、ASAはマッピングされたインターフェイスでトラフィックのプロキシAddress Resolution Protocol(ARP)を実行する

グローバル IP アドレスの ASA プロキシ ARP は、グローバル インターフェイスの NAT ステートメントの範囲にあります。NAT ステートメントに no-proxy-arp キーワードを追加している場合、このプロキシ ARP 機能は NAT ルールごとに無効にできます。

この問題は、グローバル アドレス サブネットが当初の意図よりも大幅に大きくなるように誤って作成された場合にも発生します。

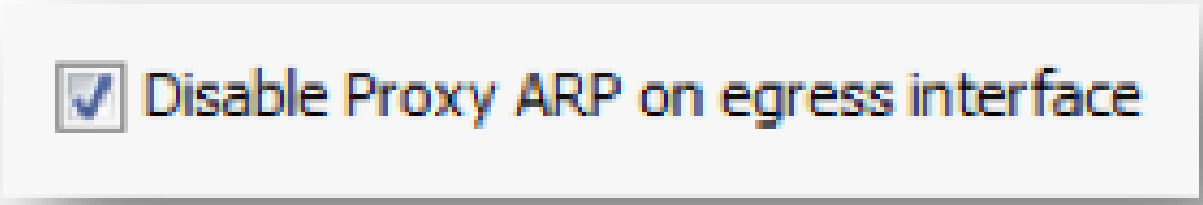
解決方法

可能であれば、NAT ステートメントに no-proxy-arp キーワードを追加します。

以下に例を挙げます。

```
<#root>
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を使用して実行することもできます。NAT ルール内で、[Disable Proxy ARP on egress interface] チェックボックスをオンにします。



.

関連情報

- ビデオ：DMZサーバアクセスのためのASAポート転送（バージョン8.3および8.4）
- 基本的なASA NAT設定：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
- シスコのテクニカルサポートとダウンロード

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。