ASA 8.4(4)：許可されていない特定のアイデンティティ NAT 設定

内容

概要

8.4(4) 以降を実行している適応型セキュリティ アプライアンス（ASA）が、特定の NAT コンフィギュレーションを拒否して、次のようなエラー メッセージを表示する場合があります。

```
ERROR: <mapped address range> overlaps with <interface> standby interface
   address
ERROR: NAT Policy is not downloaded
```

この問題は、ASA を以前のリリースから 8.4(4) 以降にアップグレードした場合にも発生する可能性があります。一部の NAT コマンドが ASA の running-config から削除されています。次の例で、出力されたコンソール メッセージを調査して、上記形式のメッセージが存在するかどうかを確認する必要があります。

生じる可能性があるもう 1 つの影響として、ASA の背後の特定のサブネットのトラフィックが、ASA で終端するバーチャル プライベート ネットワーク（VPN）トンネルを通過しなくなることがあります。このドキュメントでは、これらの問題を解決する方法について説明します。

はじめに

要件

この問題に対処するためには、次の条件を満たす必要があります。

- ASA がバージョン 8.4(4) 以降を実行している、または、以前のリリースからバージョン 8.4(4) 以降にアップグレードされている。
- 1 つ以上のインターフェイスで ASA にスタンバイ IP アドレスが設定されている。
- NAT が上記インターフェイスを使用してマッピング先のインターフェイスとして設定されている。

使用するコンポーネント

このドキュメント内の情報は、次のハードウェアとソフトウェアのバージョンに基づいています。

- 8.4(4) 以降を実行している ASA

表記法

ドキュメントの表記法の詳細は、「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。

問題

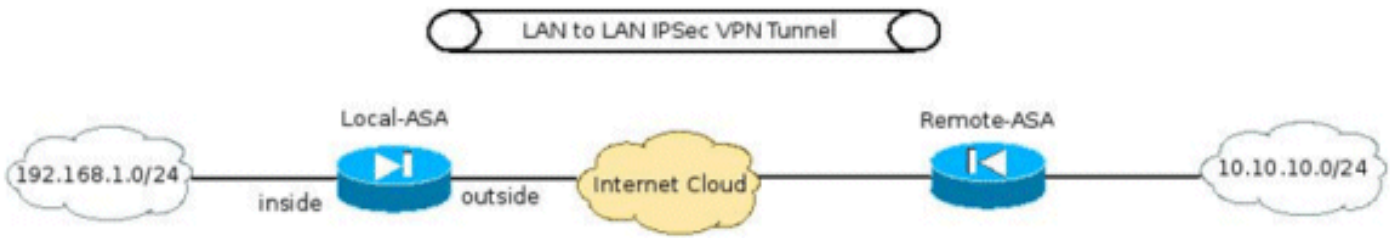
エラー メッセージからわかるように、スタティック NAT ステートメント内のマッピング先のアドレス範囲にマッピング先のインターフェイスに割り当てられた「スタンバイ」IP アドレスが含まれている場合は、NAT コマンドが拒否されます。この動作は、スタティック ポート リダイレクションで必ず発生しますが、Cisco Bug ID CSCtw82147（登録ユーザ専用）の修正としてのバージョン 8.4(4) を使用したスタティック 1 対 1 NAT ステートメントでも発生します。

このバグは、8.4(4) より前の ASA では、ユーザがスタティック NAT コンフィギュレーション内のマッピング先のアドレスをマッピング先のインターフェイスに割り当てられたスタンバイ IP アドレスと一致するように設定できるという理由で報告されたものです。たとえば、ASA からの次のコンフィギュレーションの断片を見てください。

```
ciscoasa(config)# show run int e0/0
!
interface Ethernet0/0
 nameif vm
 security-level 0
 ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
ciscoasa(config)# show run nat
!
object network obj-10.76.76.160
 nat (tftp,vm) static 192.168.1.2
```

コマンドが受け入れられても、この NAT コンフィギュレーションは設計どおりに機能しません。そのため、8.4(4) 以降の ASA では、最初の段階で、このような NAT ルールの設定が許可されません。

これが別の予期せぬ問題につながります。たとえば、ASA 上で VPN トンネルが終端されており、"inside" サブネットとリモート VPN サブネットが対話できるようにするシナリオを考えてみましょう。



VPN トンネルの設定に必要な他のコマンドの中で、より重要なコンフィギュレーションの 1 つが VPN サブネット間のトラフィックが NAT されないように保証することです。これは、次の形式

の Manual/Twice NAT コマンドを使用した 8.3 以降で実装されます。

```
interface Ethernet0/0
 nameif inside
 security-level 0
 ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
!
object network obj-192.168.1.0
 description Inside subnet
 subnet 192.168.1.0 255.255.255.0
object network obj-10.10.10.0
 description Remote VPN subnet
 subnet 10.10.10.0 255.255.255.0
!
nat (inside,any) source static obj-192.168.1.0 obj-192.168.1.0 destination
   static obj-10.10.10.0 obj-10.10.10.0
!
object network obj-192.168.1.0
 nat (inside,outside) dynamic interface
```

この ASA を 8.4(4) 以降にアップグレードすると、この NAT コマンドが ASA の running-config から削除され、次のエラーが ASA のコンソールに出力されます。

```
ERROR: 192.168.1.0-192.168.1.255 overlaps with inside standby interface
   address
ERROR: NAT Policy is not downloaded
```

その結果、サブネットの 192.168.1.0/24 と 10.10.10.0/24 間のトラフィックが VPN トンネルを通過しなくなります。

解決方法

この状況に対して使用可能な回避策が 2 つあります。

- 8.4(4) にアップグレードする前に、マッピング先のインターフェイスが「任意」でなくなるように、NAT コマンドをできるだけ具体的にします。 たとえば、上記の NAT コマンドはリモート VPN サブネットが到達可能なインターフェイス (上記シナリオでは "outside" という名前) に変更できます。

  ```
  nat (inside,outside) source static obj-192.168.1.0 obj-192.168.1.0 destination
     static obj-10.10.10.0 obj-10.10.10.0
  ```

- 上記回避策が使用できない場合は、次の手順を実行します。ASA が 8.4(4) 以降を実行している場合は、インターフェイスに割り当てられたスタンバイ IP アドレスを削除します。NAT コマンドを適用します。インターフェイスに対してスタンバイ IP アドレスを再適用します。以下に、いくつかの例を示します。

  ```
  ciscoasa(config)# interface Ethernet0/0
  ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
  ciscoasa(config-if)# exit
  ciscoasa(config)# nat (inside,any) 1 source static obj-192.168.1.0
     obj-192.168.1.0 destination static obj-10.10.10.0 obj-10.10.10.0
  ciscoasa(config)# interface Ethernet0/0
  ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
  ```

関連情報

- テクニカル サポートとドキュメント – Cisco Systems