ASAでのヘアピンの設定

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

設定

- ネットワーク図

コンフィギュレーション

- ステップ 1：オブジェクトの作成
- ステップ 2：NATの作成

確認

トラブルシュート

- ステップ1:NATルール設定の確認
- ステップ2：アクセスコントロールルール(ACL)の検証
- ステップ3：追加の診断

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)でヘアピンを正常に設定するために必要な手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ASAでのNATの設定
- ASAでのACLの設定

使用するコンポーネント

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

- Cisco適応型セキュリティアプライアンスソフトウェアバージョン9.18(4)22

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。

設定

ヘアピンネットワークアドレス変換(NAT)は、NATループバックまたはNATリフレクションとも呼ばれ、プライベートネットワーク上のデバイスがパブリックIPアドレスを介して同じプライベートネットワーク上の別のデバイスにアクセスできるネットワークルーティングで使用される技術です。

これは、サーバがルータの背後でホストされている場合に、外部デバイスと同様に、パブリックIPアドレス(インターネットサービスプロバイダー(ISP)によってルータに割り当てられたアドレス)を使用して、サーバと同じローカルネットワーク上のデバイスがサーバにアクセスできるようにする場合に使用されます。

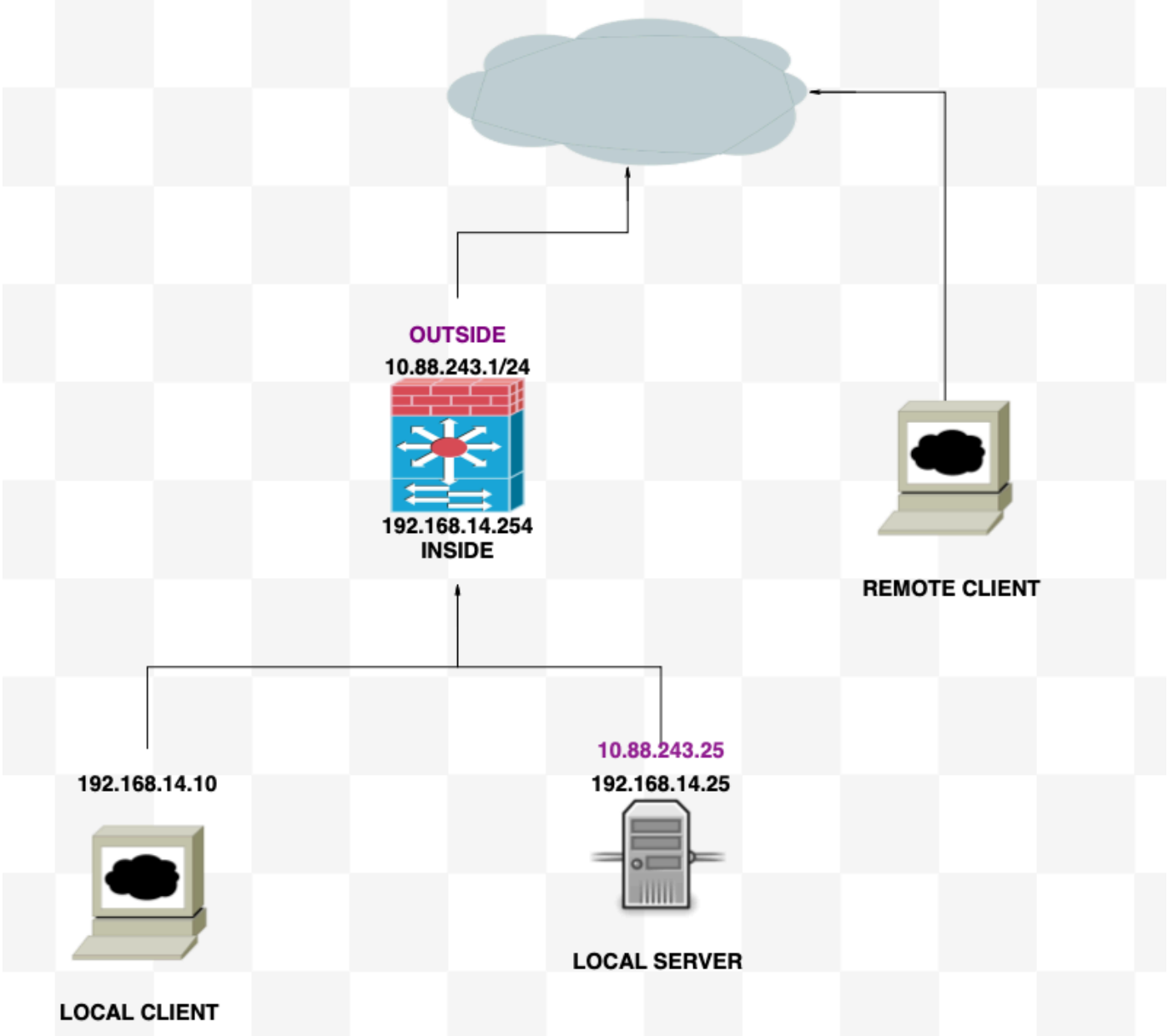
ヘアピンという用語が使用されるのは、クライアントからのトラフィックがルータ（またはNATを実装するファイアウォール）に到達し、変換後に内部ネットワークにヘアピンのように戻されて、サーバのプライベートIPアドレスにアクセスするためです。

たとえば、ローカルネットワーク上にプライベートIPアドレスを持つWebサーバがあるとします。同じローカルネットワーク上にある場合でも、パブリックIPアドレスまたはパブリックIPアドレスに解決されるドメイン名を使用してこのサーバーにアクセスする。

ヘアピンNATを使用しないと、ルータはこの要求を理解できません。パブリックIPアドレスの要求がネットワークの外部から来ることを想定しているためです。

ヘアピンNATを使用すると、要求はパブリックIPに対して行われていますが、ローカルネットワーク上のデバイスにルーティングする必要があることをルータが認識できるようになるため、この問題は解決します。

ネットワーク図



コンフィギュレーション

ステップ 1：オブジェクトの作成

- 内部ネットワーク：192.168.14.10
- Webサーバ：192.168.14.25
- パブリックWebサーバ：10.88.243.25
- ポート：80

<#root>

```
ciscoasa(config)#
 object network Local_Client
ciscoasa(config-network-object)#
 host 192.168.14.10
```

```
ciscoasa(config)#
 object network Web_Server
ciscoasa(config-network-object)#
 host 192.168.14.25
ciscoasa(config)#
 object network P_Web_Server
ciscoasa(config-network-object)#
 host 10.88.243.25
ciscoasa(config)#
 object service HTTP
ciscoasa(config-service-object)#
 service tcp destination eq 80
```

ステップ 2：NATの作成

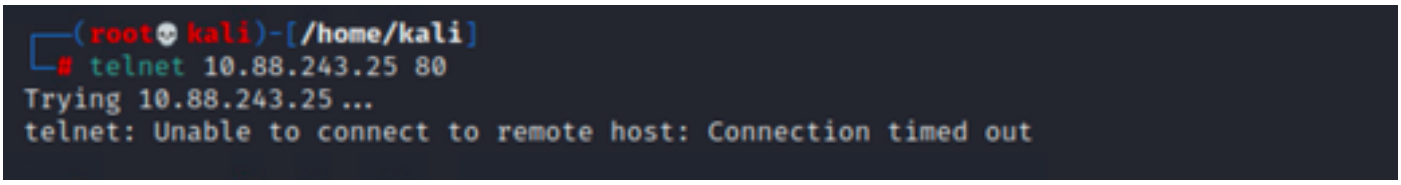
<#root>

```
ciscoasa
(config-service-object)# nat (Inside,Inside) source dynamic Local_Client interface destination static P_
```

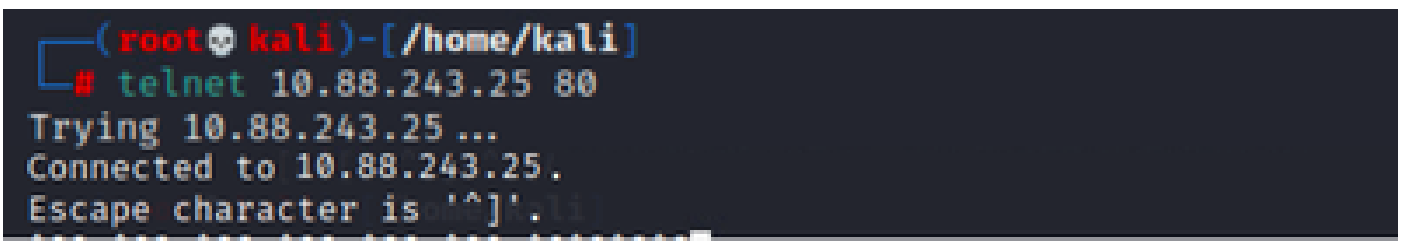
確認

ローカルクライアントから、デスティネーションポートを使用してtelnetの宛先IPを実行します。

「telnet unable to connect to remote host: Connection timed out」というメッセージが表示された場合、設定中に何らかの問題が発生しています。



Connectedと表示されていれば機能します。



トラブルシュート

ネットワークアドレス変換(NAT)に関する問題が発生した場合は、このステップバイステップガイドを使用して、一般的な問題のトラブルシューティングと解決を行ってください。

ステップ1:NATルール設定の確認

- NATルールの確認：すべてのNATルールが正しく設定されていることを確認します。送信元と宛先のIPアドレスおよびポートが正確であることを確認します。
- インターフェイス割り当て：送信元インターフェイスと宛先インターフェイスの両方がNATルールに正しく割り当てられていることを確認します。マッピングが正しくないと、トラフィックが正しく変換またはルーティングされない可能性があります。
- NAT Rule Priority:NATルールに、同じトラフィックに一致する可能性のあるその他のルールよりも高い優先順位が付けられていることを確認します。ルールは順番に処理されるため、上位に配置されたルールが優先されます。

ステップ2：アクセスコントロールルール(ACL)の検証

- ACLの確認：アクセスコントロールリストをチェックして、NATトラフィックを許可するのに適切であることを確認します。変換されたIPアドレスを認識するようにACLを設定する必要があります。
- ルールの順序：アクセスコントロールリストが正しい順序であることを確認します。NATルールと同様に、ACLは上から下へ処理され、トラフィックに一致する最初のルールが適用されます。
- トラフィック許可：内部ネットワークから変換済み宛先へのトラフィックを許可する適切なアクセスコントロールリストが存在することを確認します。ルールが見つからないか、誤って設定されている場合、目的のトラフィックがブロックされる可能性があります。

ステップ3：追加の診断

- 診断ツールの使用：デバイスを通過するトラフィックの監視とデバッグに使用できる診断ツールを利用します。これには、リアルタイムログと接続イベントの表示が含まれます。
- 接続の再起動：既存の接続では、NATルールまたはACLを再起動するまで変更が認識されない場合があります。既存の接続をクリアして、新しい規則を強制的に適用することを検討してください。

<#root>

ciscoasa(config)#

 clear xlate

- 変換の確認：ASAデバイスを使用してNAT変換が期待どおりに実行されていることを確認する場合は、コマンドラインでshow xlateやshow natなどのコマンドを使用します。

<#root>

ciscoasa(config)#

 show xlate

<#root>

ciscoasa(config)#

 show nat

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。