Firepower Management Center(FMC)でのヘアピンの設定

内容

はじめに

このドキュメントでは、Firepower Threat Defense(FTD)とFirepower Management Center(FMC)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。

- Firepower Management Center（FMC）
- Firepower Threat Defense(FTD)

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。

- Firepower Management Center(FMC)仮想7.2.4
- Firepower Threat Defense(FTD)仮想7.2.4

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。

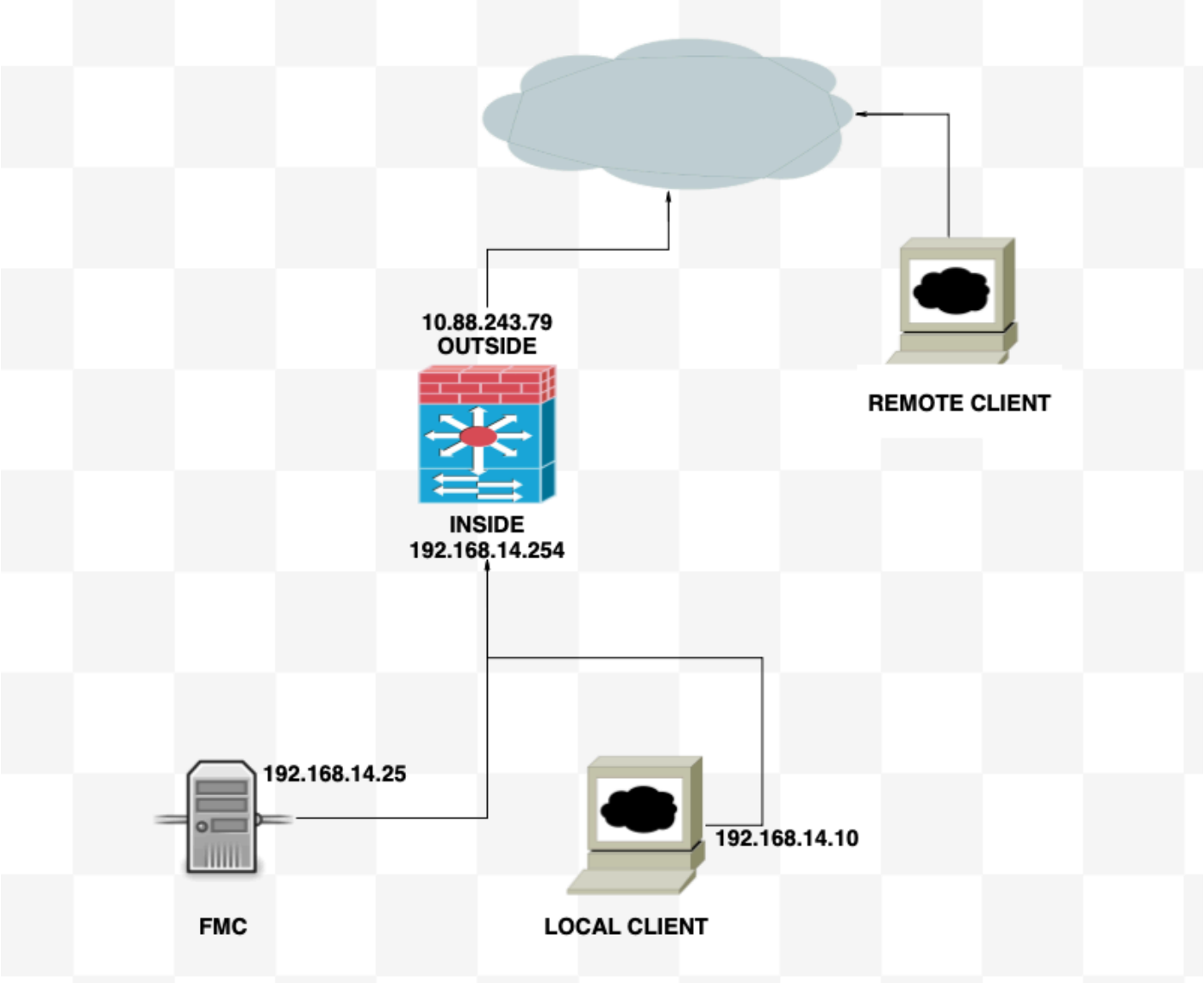
設定

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。

この機能は、ローカルネットワーク内のWebホスティングなどのネットワークサービスに役立ちます。ローカルネットワークのユーザは、外部ユーザが使用するのと同じURLまたはIPアドレスを使用して内部サーバにアクセスする必要があります。ローカルネットワークの内部または外部から要求が発信されたかどうかに関係なく、リソースへの均一なアクセスを保証します。

この例では、FTDの外部インターフェイスのIP経由でFMCにアクセスする必要があります

図

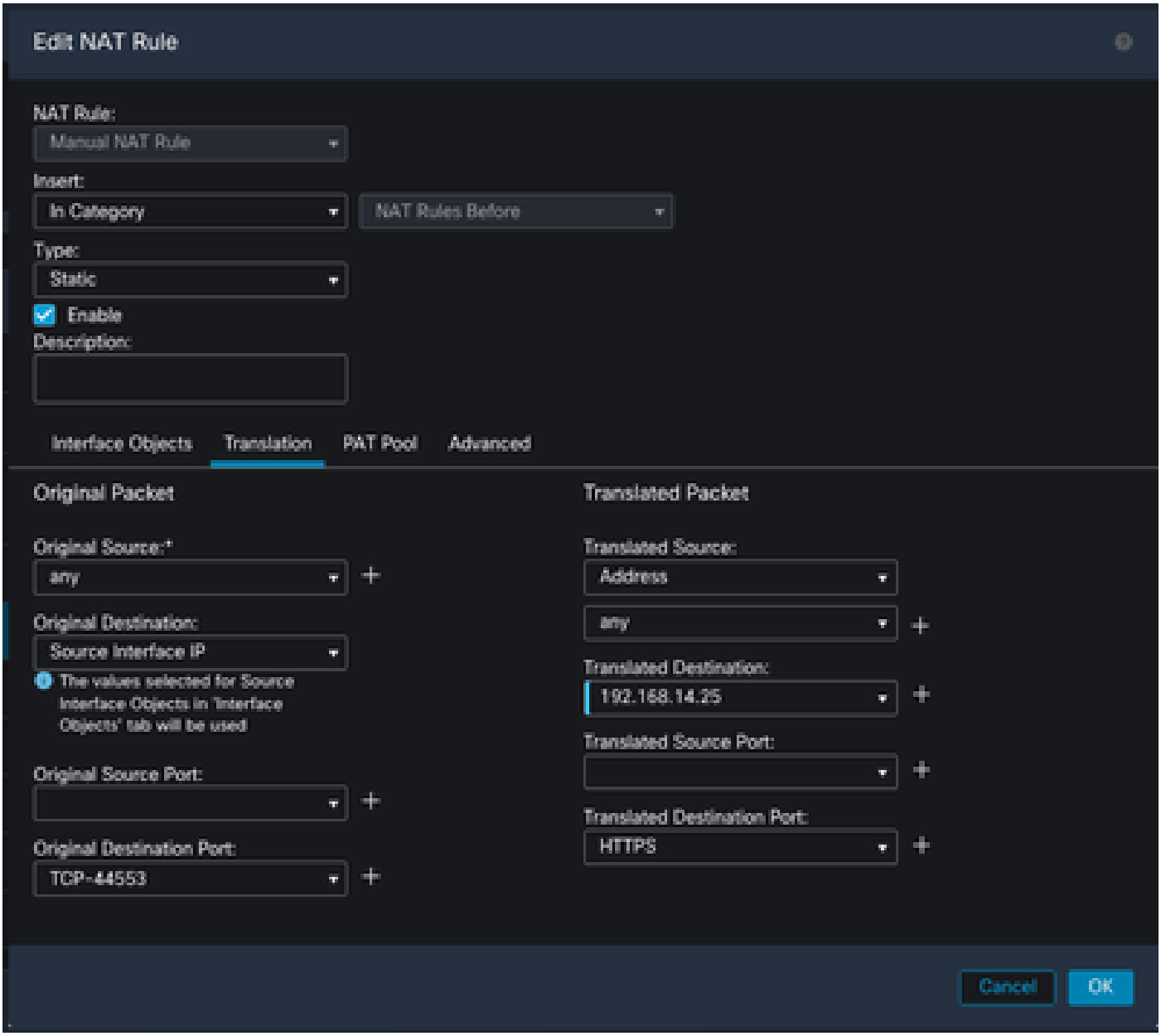


ステップ 1：Outside-Inside Natの設定

最初のステップとして、スタティックNATを設定する必要があります。この例では、宛先IPと宛先ポートが外部インターフェイスのIPを使用して変換され、ポートの宛先は44553です。

FMCで、Device > NATに移動して既存のポリシーを作成または編集してから、Add Ruleボックスをクリックします。

- NATルール：手動Natルール
- 元のソース：任意
- 元の宛先：送信元インターフェイスIP
- 元の宛先ポート：44553
- 変換された宛先:192.168.14.25
- 変換済み宛先ポート：443



ポリシーを設定します。Policies > Access Controlの順に移動して、既存のポリシーを作成または編集してから、Add Ruleボックスをクリックします。

ソースゾーン：外部

宛先ゾーン：内部

送信元ネットワーク：任意

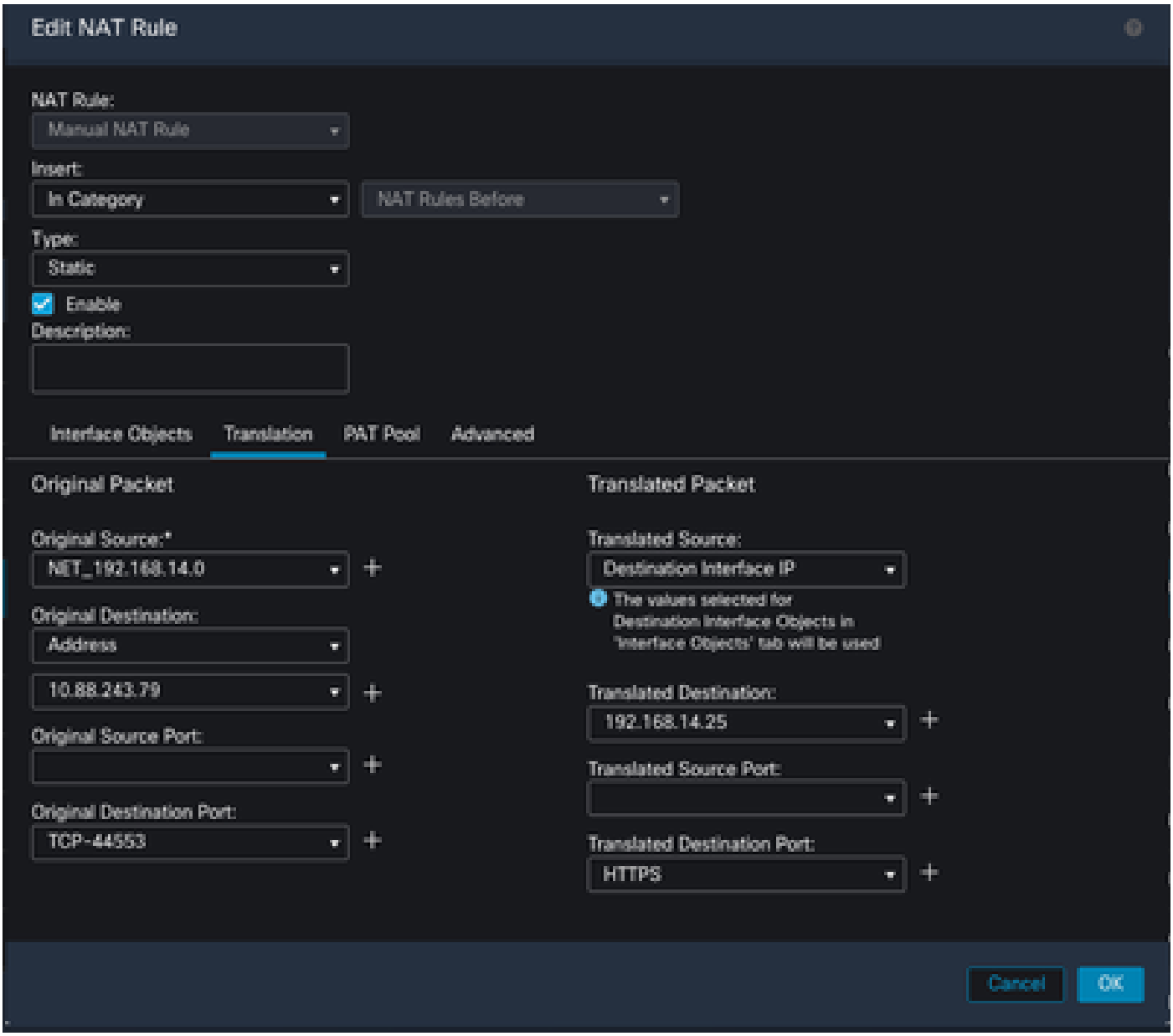
宛先ネットワーク：10.88.243.79

ステップ 2：内部Nat（ヘアピン）の設定

2番目のステップとして、内部から内部へのスタティックNATを設定する必要があります。この例では、宛先IPと宛先ポートが外部インターフェイスのIPを持つオブジェクトを使用して変換され、宛先ポートは44553です。

FMCから、Device > NATに移動して既存のポリシーを編集してから、Add Ruleボックスをクリックします。

- NATルール：手動Natルール
- 出典：192.168.14.0/24
- 元の宛先：アドレス10.88.243.79
- 元の宛先ポート：44553
- 変換済み送信元：宛先インターフェイスIP
- 変換された宛先:192.168.14.25
- 変換済み宛先ポート：443



ポリシーを設定します。Policies > Access Controlの順に移動して既存のポリシーを編集し、Add Ruleボックスをクリックします。

ソースゾーン：任意

宛先ゾーン：任意

送信元ネットワーク：192.168.14.0/24

宛先ネットワーク：10.88.243.79

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks
Mandatory - la primera (1-4)					
1	nat-fmc	OUTSIDE	INSIDE	any	*Any*
2	Hairpin	*Any*	*Any*	NET_192.168.14	10.88.243.79

確認

ローカルクライアントから、宛先IPと宛先ポートを指定してtelnetを実行します。

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

```
┌──(root💀 kali)-[/home/kali]
└─# telnet 10.88.243.79 44553
Trying 10.88.243.79 ...
telnet: Unable to connect to remote host: Connection timed out
```

ただし、Connectedと表示されていれば、設定は成功しています。

```
┌──(root💀 kali)-[/home/kali]
└─# telnet 10.88.243.79 44553
Trying 10.88.243.79 ...
Connected to 10.88.243.79.
Escape character is '^]'.
```

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FMCで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：同じトラフィックに一致する他のルールの先頭にNATルールが配置されていることを確認します。FMC内の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：FMCで利用可能な診断ツールを使用して、デバイスを通過するトラフィックを監視およびデバッグします。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に対する変更が再起動されるまで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。

Linaから：

```
<#root>

firepower#

 clear xlate
```

- 変換の確認：FTD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。

Linaから：

```
<#root>

firepower#

 show nat
```

```
<#root>

firepower#

 show xlate
```

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。