firepower Management Center(FMC)を使用したFTDでのDHCPサーバ/リレーの設定

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

背景説明

DHCPサーバの設定

- DHCPサーバの有効化/DHCPプールの設定
- DNS/WINSサーバの設定
- 高度なパラメータの設定

DHCPリレーの設定

- DHCPリレーエージェントの設定
- 外部DHCPサーバの設定

監視とトラブルシューティング

関連情報

はじめに

このドキュメントでは、FMCを介したFirepower Threat Defense(FTD)でのDHCPサーバおよびDHCPリレーサービスの設定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 の知識
- 適応型セキュリティ アプライアンス（ASA）の基礎知識
- Dynamic Host Control Protocol(DHCP)サーバ/DHCPリレーに関する知識

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。

- ソフトウェアバージョン6.0.1以降を実行するASA(5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)用のASAFirepower脅威対策イメージ。
- firepowerバージョン6.0.1以降を実行するASA(5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X)用ASA Software Threat Defense Image。
- FMCバージョン6.0.1以降。

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。

注:FTDアプライアンスはFMCに登録できます。Register a Device with a FireSIGHT Management Centerをクリックして、FTDをFMCに登録します。

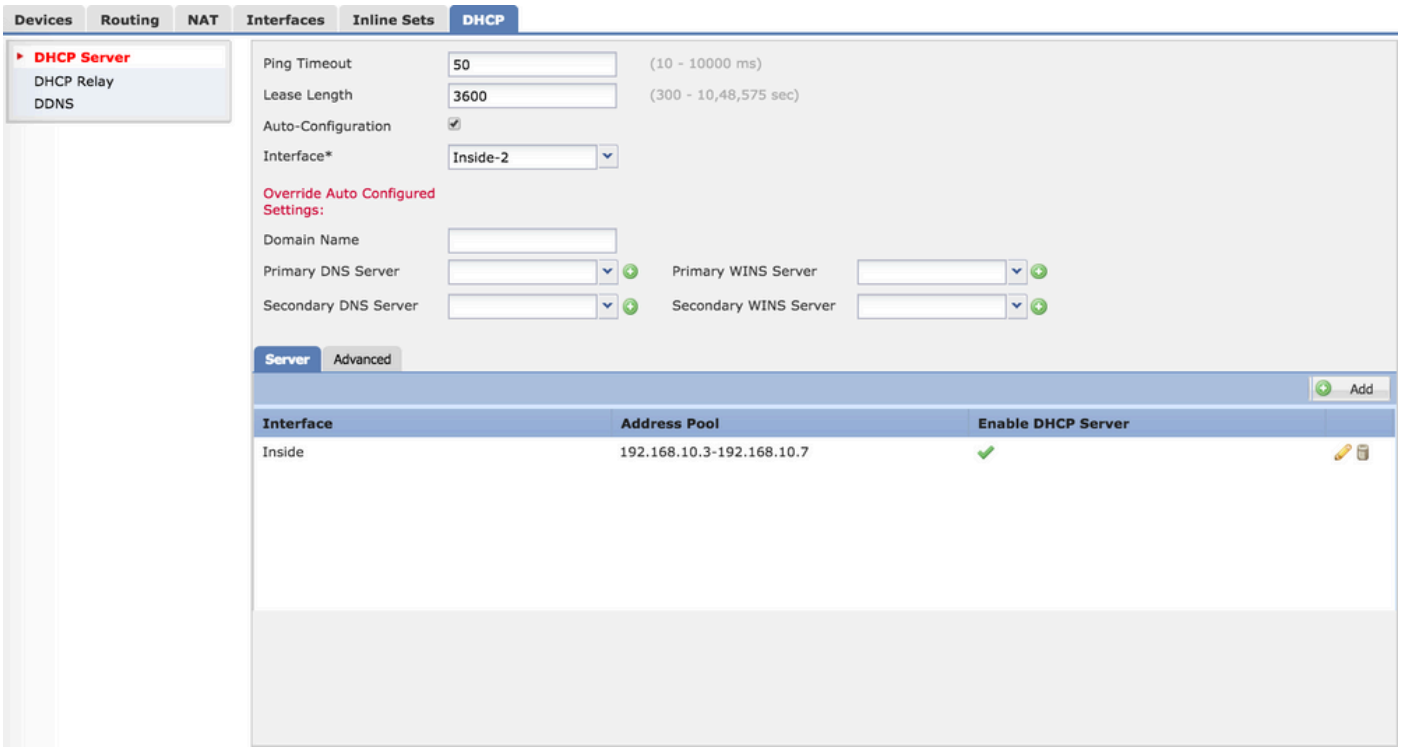
背景説明

DHCPは、IPアドレス、DNSサーバの詳細、その他のパラメータなどのネットワーク設定パラメータをDHCPクライアントに自動的に提供します。FTDルーテッドインターフェイスは、DHCPサーバとして動作し、クライアントにIPアドレスを提供できます。

FTDは内部クライアントにDHCPリレーサービスを提供します。クライアントはFTDのインターフェイスの1つに接続され、外部DHCPサーバはもう1つに接続されています。 リレーサービスの動作は、クライアントに対して透過的に行われます。

DHCPサーバの設定

DHCPサーバを設定するには、FMC GUIにログインし、Devices > Device Managementの順に選択します。 FTDアプライアンスのeditボタンをクリックします。DHCPタブに移動し、DHCP Serverタブをクリックします。



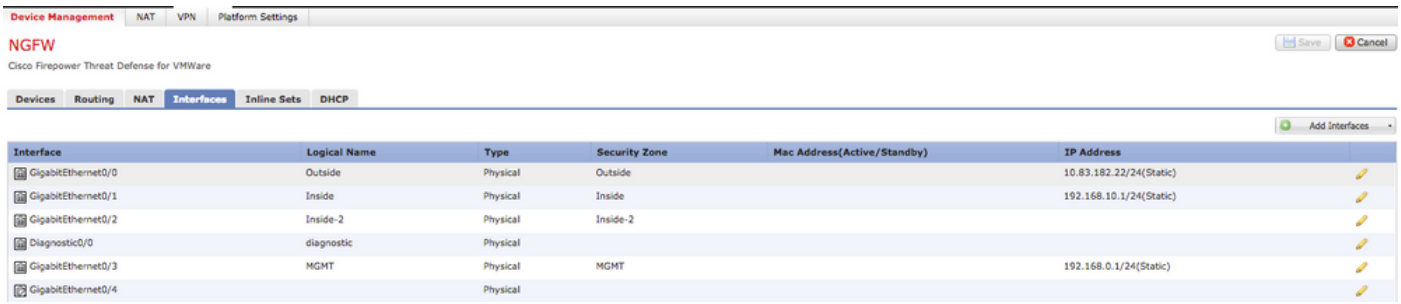
DHCPサーバを設定するには、次の3つの手順を実行します。

ステップ 1：DHCPサーバの有効化/DHCPプールの設定

ステップ 2：高度なパラメータを設定します。

ステップ 3：DNS/WINSサーバを設定します。

注:DHCP設定を開始する前に、インターフェイスにIPアドレスと論理名を設定する必要があります。



DHCPサーバの有効化/DHCPプールの設定

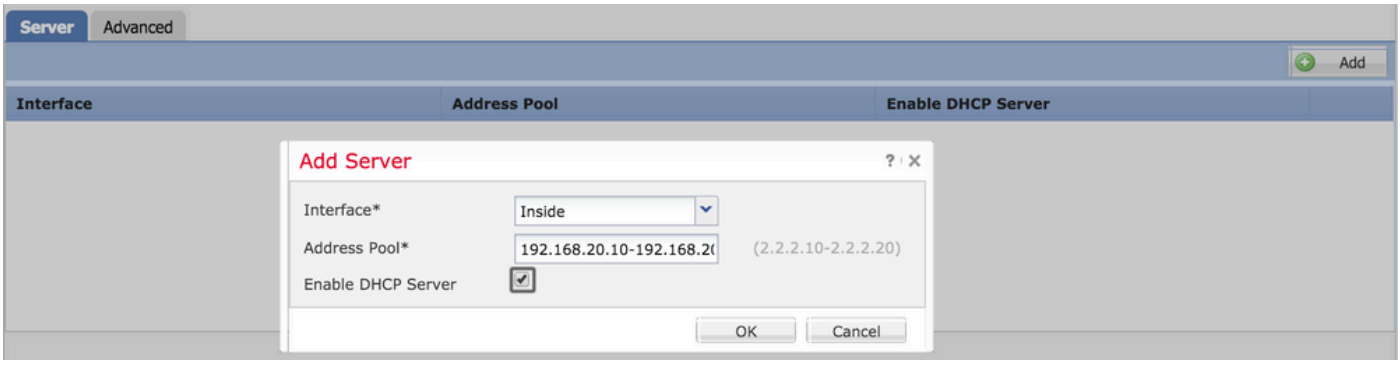
ルーティングされたインターフェイスはDHCPサーバとして使用でき、インターフェイスのIPアドレスはエンドクライアントのゲートウェイとして機能します。したがって、IPアドレス範囲を定義するだけで済みます。

任意のインターフェイスでDHCPサーバを有効にするには、Serverタブで**Add**ボタンをクリックします。

Interface：ドロップダウンリストから、DHCPサーバを有効にするインターフェイスを指定します。

アドレスプール：IPアドレスの範囲を指定します。

DHCPサーバを有効にする：このインターフェイスでDHCPサーバを有効にするには、チェックボックスをオンにします。



OKをクリックして、DHCP設定を保存します。

DNS/WINSサーバの設定

DHCPサーバは、エンドクライアントにIPアドレスの詳細とともにDNS/WINS/ドメイン名パラメータを提供します。これらのパラメータは、名前解決に役立ちます。したがって、これらのパラメータを正しく設定することが重要です。

これを設定するには、次の2つのオプションがあります。

まず、FTDのいずれかのインターフェイスがDHCPクライアントとして設定されている場合は、Auto-Configurationオプションを選択できます。 この方法では、DHCPサーバからDNS/WINS/ドメイン名情報の設定を取得し、同じ情報をDHCPクライアントに提供します。

2つ目は、独自のDNS/WINSドメイン名パラメータを設定する方法です。このパラメータはエンドクライアントに提供されます。

これを設定するには、DHCPタブに移動します。

- pingタイムアウト：アドレスの競合を回避するために、FTDはアドレスに2つのICMP pingパケットを送信してから、そのアドレスをDHCPクライアントに割り当てます。このコマンドは、これらのパケットのタイムアウト値を指定します

- Lease Length：このリースは、クライアントが割り当てられたIPアドレスをリースの期限が切れるまでに使用できる時間（秒単位）と同じです
- 自動構成：DNS/WINS/ドメイン名の自動構成を構成するには、このチェックボックスをオンにします
- Interface:DHCPクライアントとして機能するインターフェイスを指定します

Override Auto Configured Setting：独自のDNS/WINS/ドメイン名をエンドクライアントに割り当てる場合は、このオプションを設定します。

ドメイン名：ドメイン名を指定します。

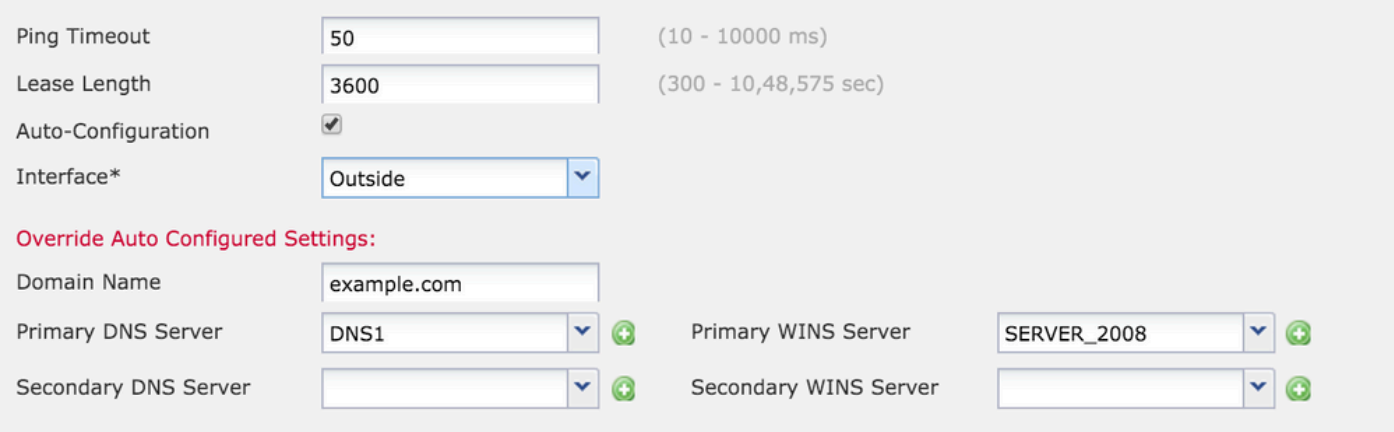
プライマリDNSサーバ：プライマリDNSサーバを指定します。ドロップダウンリストからネット

ワークオブジェクトを選択するか、プラス(+)アイコンをクリックして、プライマリDNSサーバのネットワークオブジェクトを作成します。

セカンダリDNSサーバ：セカンダリDNSサーバを指定します。ドロップダウンリストからネットワークオブジェクトを選択するか、プラス(+)アイコンをクリックして、セカンダリDNSサーバのネットワークオブジェクトを作成します。

プライマリWINSサーバ：セカンダリDNSサーバを指定します。ドロップダウンリストからネットワークオブジェクトを選択するか、プラス(+)アイコンをクリックして、セカンダリDNSサーバのネットワークオブジェクトを作成します。

セカンダリWINSサーバー：セカンダリDNSサーバーを指定します。ドロップダウンリストからネットワークオブジェクトを選択するか、プラス(+)アイコンをクリックして、セカンダリDNSサーバのネットワークオブジェクトを作成します。

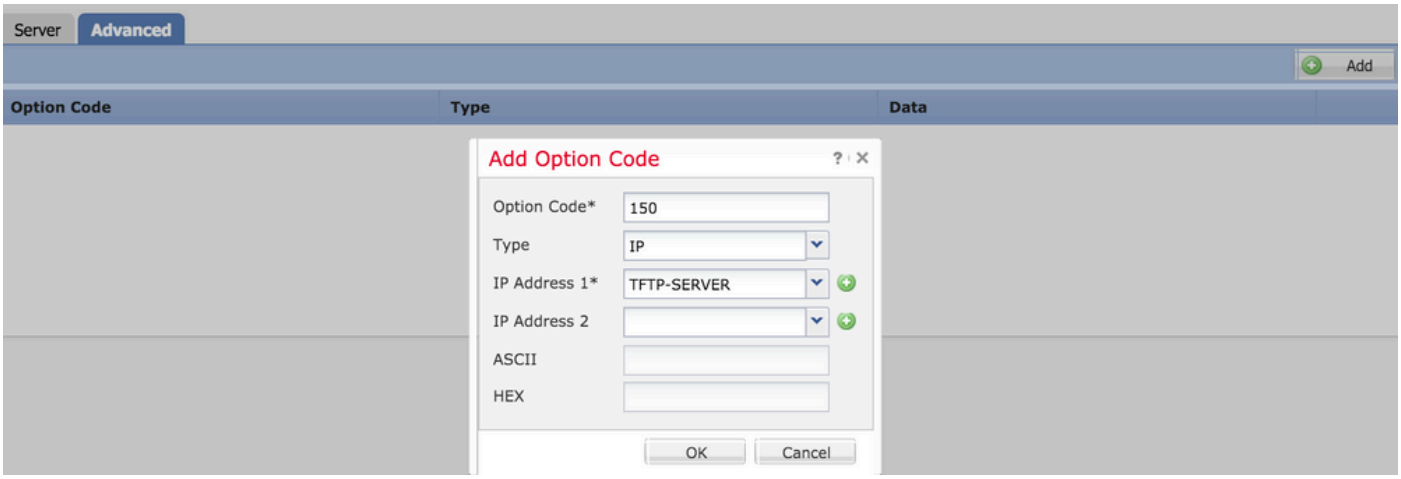


高度なパラメータの設定

FTDインターフェイスのDHCPサーバには、DHCPコードとオプションを含める機能があります。たとえば、Cisco IP Phoneは、DHCPサーバにオプション(150/ 66)を指定して要求を送信し、TFTPサーバのIPアドレスを取得して、電話機がTFTPサーバからファームウェアをダウンロードできるようにします。

これを設定するには、DHCP> Advancedオプションに移動して、Addをクリックします。

- オプションコード：RFC 2132、RFC 2562、RFC 5510に記載されているオプションコードを指定します
- タイプ：ドロップダウンからタイプを指定します
- IPアドレス1：タイプオプションとしてIPを選択した場合は、最初のTFTPサーバのIPアドレスを指定します。
- IPアドレス2：タイプオプションとしてIPを選択した場合は、最初のTFTPサーバのIPアドレスを指定します。
- ASCII：タイプオプションとしてASCIIを選択した場合は、ASCII値を指定します。
- HEX：タイプオプションとしてHEXを選択した場合は、HEX値を指定します



[OK] をクリックして、設定を保存します。

Saveボタンをクリックして、プラットフォーム設定を保存します。 Deployオプションに移動し、変更を適用するFTDアプライアンスを選択し、Deployボタンをクリックしてプラットフォーム設定の導入を開始します。

Saveボタンをクリックして、プラットフォーム設定を保存します。 Deployオプションに移動し、変更を適用するFTDアプライアンスを選択し、Deployボタンをクリックしてプラットフォーム設定の導入を開始します。

DHCPリレーの設定

FTDインターフェイスは、クライアントと外部DHCPサーバ間のDHCPリレーエージェントとして動作します。インターフェイスはクライアント要求をリッスンし、クライアントのアドレスを割り当てるためにDHCPサーバが必要とするクライアントのリンク情報などの重要な設定データを追加します。DHCPサーバが応答すると、インターフェイスは応答パケットをDHCPクライアントに転送します。

DHCPリレーの設定には、主に2つの設定手順があります。

ステップ 1：DHCPリレーエージェントを設定します。

ステップ 2：外部DHCPサーバを設定します。

DHCPリレーエージェントの設定

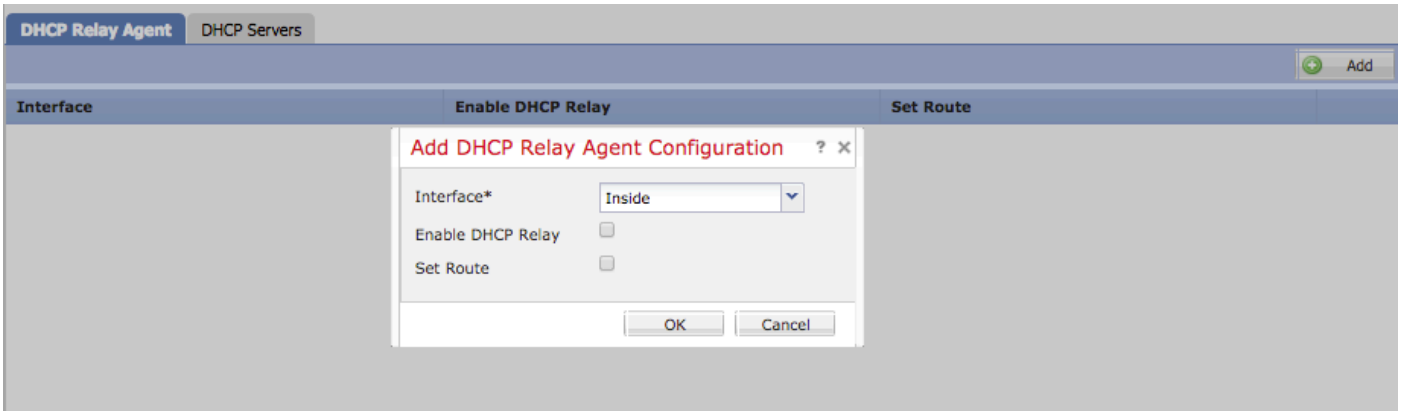
Devices > Device Managementに移動します。FTDアプライアンスのeditボタンをクリックします。DHCP > DHCP Relayオプションの順に移動します。 Addボタンをクリックします。

Interface：インターフェイスがクライアント要求をリッスンするインターフェイスをドロップダウンリストから指定します。DHCPクライアントは、IPアドレス要求のためにこのインターフェイスに直接接続できます。

DHCPリレーの有効化：チェックボックスをオンにして、DHCPリレーサービスを有効にします

。

Set Route：インターフェイスのIPアドレスをデフォルトゲートウェイとして設定するには、このチェックボックスをオンにします。



OKボタンをクリックして、DHCPリレーエージェントの設定を保存します。

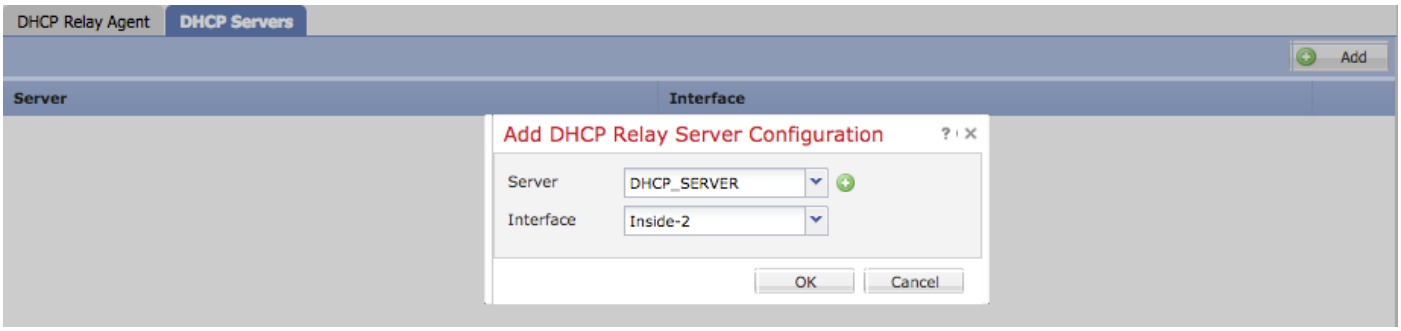
外部DHCPサーバの設定

クライアント要求が転送される外部DHCPサーバのIPアドレスを指定する必要があります。

DHCPサーバを指定するには、DHCP Serverに移動し、Addをクリックします。

Server:DHCPサーバのIPアドレスを指定します。 ドロップダウンリストからネットワークオブジェクトを選択するか、プラス(+)アイコンをクリックしてDHCPサーバのネットワークオブジェクトを作成します。

Interface:DHCPサーバが接続するインターフェイスを指定します。



[OK] をクリックして、設定を保存します。

Saveボタンをクリックして、プラットフォーム設定を保存します。 Deployオプションに移動し、変更を適用するFTDアプライアンスを選択し、Deployボタンをクリックしてプラットフォーム設定の導入を開始します。

監視とトラブルシューティング

- DHCPサーバ/リレーの設定を開始する前に、FTDがFMCに登録されていることを確認します。
- DHCPリレー設定でDHCPサーバへの接続を確認します。

```
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

><Press Enter>
firepower# ping <DHCP_SERVER_IP>
```

- FTD CLIでDHCP関連の設定を確認します。FTD CLIに管理インターフェイスにログインして、コマンドを実行できます

```
firepower# show running-config dhcpd.
dhcpd auto_config Inside-2
!
dhcpd address 192.168.10.3-192.168.10.7 Inside
!
```

- ポリシーの展開が正常に適用されていることを確認します。
- 自動設定または手動設定によって、正しいDNS/WINSサーバエントリを設定していることを確認します。
- IPアドレスプールは、インターフェイスIPアドレスと同じサブネットに含めることができます。
- IPアドレスと論理名がインターフェイスで設定できることを確認します。
- クライアントがIPアドレスを取得しないという問題をトラブルシューティングするために、FTDルーテッドインターフェイスでパケットキャプチャを取得できます。パケットキャプチャでは、DHCPサーバのDORAプロセスを確認できます。CLIおよびASDMでのASAパケットキャプチャの設定例を使用して、パケットキャプチャを取得できます。
- コマンドラインからDHCPの統計情報を確認します。

```
firepower# show dhcpd statistics
```

- CLIからDHCPバインディング情報を確認します。

```
 firepower# show dhcpd binding
```

- Devices > Platform Settings > FTD Policy > System loggingで適切なロギングを有効にし、プラットフォーム設定をFTDに展開します。FTD CLIにログインし、コマンドを実行してSyslogメッセージを確認します。

```
 Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower# show logging
```

関連情報

- テクニカル サポートとドキュメント - Cisco Systems

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。