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

内容
<u>はじめに</u>
前提条件
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
DHCPサーバの設定
<u>DHCPサーバの有効化/DHCPプールの設定</u>
<u>DNS/WINSサーバの設定</u>
高度なパラメータの設定
<u>DHCPリレーの設定</u>
<u>DHCPリレーエージェントの設定</u>
<u>外部DHCPサーバの設定</u>
<u>監視とトラブルシューティング</u>
<u>関連情報</u>

## 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。



### 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。

Devices	Routi	ng	NAT	Interfaces	Inline Sets	DHCP				
+ DHCP	Server			Ping Timeo	ut	50		10 - 10000 ms)		
DHCP F	Relay			Lesse Length		2000		200 - 10 49 575 coc)		
DDNS		Lease Leng	in .	3600		300 - 10,48,575 Sec)				
				Auto-Config	guration	×				
				Interface*		Inside-2	 *			
				Override Au Settings:	uto Configured					
				Domain Na	me					
				Primary DN	IS Server		• 🔾	Primary WINS Server	<b>~</b> O	
				Secondary	DNS Server		- 0	Secondary WINS Server	▼ O	
				Server /	Advanced					
										O Add
				Interface			Addr	ress Pool	Enable DHCP Server	
				Inside			192.1	168.10.3-192.168.10.7	×	a 🖉

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。

Device Management NAT VPN Platform Settings	1					
NGFW						Save Cancel
Cisco Firepower Threat Defense for VMWare						
Devices Routing NAT Interfaces Inline Set	s DHCP					
						Add Interfaces •
Interface	Logical Name	Туре	Security Zone	Mac Address(Active/Standby)	IP Address	
GigabitEthernet0/0	Outside	Physical	Outside		10.83.182.22/24(Static)	1
GigabitEthernet0/1	Inside	Physical	Inside		192.168.10.1/24(Static)	1
GigabitEthernet0/2	Inside-2	Physical	Inside-2			1
Diagnostic0/0	diagnostic	Physical				1
GigabitEthernet0/3	MGMT	Physical	MGMT		192.168.0.1/24(Static)	1
GigabitEthernet0/4		Physical				1

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。

Server Advanced		
		Add
Interface	Address Pool Enable DHCP Server	
	Add Server         ? ×           Interface*         Inside           Address Pool*         192.168.20.10-192.168.2(           Enable DHCP Server         Image: Comparison of the server of	
	OK Cancel	

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。

Ping Timeout	50	(10 - 10000 ms)						
Lease Length	3600	(300 - 10,48,575 sec)						
Auto-Configuration								
Interface*	Outside 💙							
Override Auto Configured Settings:								
Override Auto Configured Set	tings:							
Override Auto Configured Set Domain Name	tings: example.com							
Override Auto Configured Set Domain Name Primary DNS Server	tings: example.com DNS1	Primary WINS Server	SERVER_2008	G				

#### 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

Server Advanced								
		Add						
Option Code	Туре	Data						
	Add Option Code ? × Option Code* 150 Type IP IP Address 1* TFTP-SERVER V 3 IP Address 2 ASCII HEX OK Cancel							

[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。

DHCP Relay Agent DHCP Servers					
				0	Add
Interface	Enable DHCP Rel	lay	Set Route		
	Add DHCP Relay A	Agent Configuration ? ×			
	Interface*	Inside			
	Enable DHCP Relay	0			
	Set Route	0			
		OK Cancel			

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。

DHCP Relay Agent DHCP Servers		
		O Add
Server	Interface	
	Add DHCP Relay Server Configuration ? * Server DHCP_SERVER • • • Interface Inside-2 • OK Cancel	

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

• <u>テクニカル サポートとドキュメント - Cisco Systems</u>

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。