cisco.



Cisco Firepower Threat Defense Virtual スタートアップガイド (**Oracle** クラウドインフラストラクチャ向け)

初版:2020年10月22日 最終更新:2020年11月18日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー http://www.cisco.com/jp お問い合わせ先:シスココンタクトセンター 0120-092-255 (フリーコール、携帯・PHS含む) 電話受付時間:平日 10:00~12:00、13:00~17:00 http://www.cisco.com/jp/go/contactcenter/



Firepower Threat Defense 仮想 と Oracle Cloud Infrastructure の使用開始

Firepower Threat Defense 仮想(FTDv)は、シスコの Firepower 次世代ファイアウォール機能を 仮想化環境にもたらし、一貫性のあるセキュリティポリシーを実現して、物理、仮想、クラウ ドの各環境にわたって、またクラウド間で、ワークロードを把握します。

この章では、Oracle Cloud Infrastructure (OCI) 環境内における Firepower Threat Defense 仮想の 機能について解説し、機能のサポート、システム要件、ガイドライン、制限事項などを説明し ます。また、この章では FTDv を管理するためのオプションについても説明します。

展開を開始する前に、管理オプションを理解しておくことが重要です。FTDvの管理と監視には Firepower Management Center を使用できます。

- OCI への FTDv の展開について (1ページ)
- FTDv と OCI の前提条件 (2 ページ)
- FTDv と OCI のガイドラインおよび制限事項 (3ページ)
- OCI 上の FTDv のネットワークトポロジの例 (3ページ)

OCI への FTDv の展開について

Cisco Firepower Threat Defense 仮想(FTDv)は、物理的な Cisco FTD と同じソフトウェアを実行して、仮想フォームファクタにおいて実証済みのセキュリティ機能を提供します。FTDvは、 パブリック OCIで展開できます。その後設定を行うことで、時間の経過とともにロケーション を展開、契約、またはシフトする仮想および物理データセンターのワークロードを保護できま す。

OCI のコンピューティングシェイプ

シェイプは、インスタンスに割り当てられる CPU の数、メモリの量、およびその他のリソー スを決定するテンプレートです。FTDv は、次の OCI のシェイプタイプをサポートします。 表 1: でサポートされるコンピューティングシェイプ FTDv

OCI シェイプ	属性		インターフェイス
	oCPU	RAM (GB)	
VM.Standard2.4	4	60 GB	最小4、最大4
VM.Standard2.8	8	120 GB	最小4、最大8

• OCI では、1 つの oCPU は 2 つの vCPU に相当します。

•FTDvには、少なくとも4つのインターフェイスが必要です。

ユーザは、OCI でアカウントを作成し、Oracle Cloud Marketplace の Cisco Firepower NGFW 仮想 ファイアウォール (NGFWv) 製品を使用してコンピューティングインスタンスを起動し、OCI のシェイプを選択します。

FTDv と OCI の前提条件

- https://www.oracle.com/cloud/ で、OCI アカウントを作成します。
- Cisco スマートアカウント。Cisco Software Central (https://software.cisco.com/) で作成できます。
- Firepower Threat Defense 仮想 へのライセンス付与。
 - Firepower Management Center からセキュリティ サービスのすべてのライセンス資格を 設定します。
 - ライセンスを管理する方法の詳細については、『Firepower Management Center Configuration Guide』の「Licensing the Firepower System」を参照してください。
- •インターフェイスの要件:
 - 管理インターフェイス(2):1 つは Firepower Threat Defense 仮想 を Firepower Management Center に接続するために使用されます。もう1つは診断目的に使用され、 通過トラフィックには使用できません。
 - トラフィックインターフェイス(2): Firepower Threat Defense 仮想 を内部のホスト およびパブリックネットワークに接続するために使用されます。
- 通信パス:

• Firepower Threat Defense 仮想 にアクセスするためのパブリック IP。

• FTDv のシステム要件については、『Cisco Firepower Compatibility Guide』を参照してください。

FTDvと OCI のガイドラインおよび制限事項

サポートされる機能

- OCI 仮想クラウドネットワーク (VCN) での展開
- •ルーテッドモード (デフォルト)
- ・ライセンス:BYOLのみをサポート
- Firepower Management Center サポートのみ。

サポートされない機能

- Firepower Device Manager を介したローカル管理サポート。
- IPv6
- FTDv ネイティブ HA
- ・自動スケール
- ・トランスペアレント/インライン/パッシブモード
- DHCP を使用したデータインターフェイス設定

OCI上の FTDv のネットワークトポロジの例

次の図は、FTDv用に4つのサブネット(管理、診断、内部、外部)がOCI内に設定された ルーテッドファイアウォールモードのFTDvの推奨トポロジを示しています。

図 **1 : 0CI**上の FTDvの展開例





Firepower Threat Defense Virtual の OCI への 展開

FTDv は、Oracle Cloud Infrastructure (OCI) に展開できます。OCI は、オラクルが提供するパブリック クラウド コンピューティング サービスで、高可用性のホステッド環境でアプリケー ションを実行できます。

次の手順では、OCI環境を準備し、FTDv インスタンスを起動する方法について説明します。 OCIポータルにログインし、OCI Marketplace で Cisco Firepower NGFW virtual firewall (NGFWv) 製品を検索し、コンピューティングインスタンスを起動します。FTDv の起動後に、トラフィッ クの送信元と接続先に応じて、トラフィックをファイアウォールに転送するようにルートテー ブルを設定する必要があります。

- ・仮想クラウドネットワーク (VCN) の設定 (5ページ)
- OCI 上の FTDv インスタンスの作成 (9ページ)
- •インターフェイスの接続(10ページ)
- ・接続された VNIC のルートルールの追加 (11ページ)

仮想クラウドネットワーク(VCN)の設定

FTDv 展開用の仮想クラウドネットワーク (VCN) を設定します。少なくとも、FTDv の各インターフェイスに1つずつ、合計4つの VCN が必要です。

次の手順に進み、管理 VCN を完了できます。次に、[ネットワーキング (Networking)]に戻り、診断、内部、および外部の各インターフェイスの VCN を作成します。

始める前に



(注) ナビゲーションメニューからサービスを選択すると、左側のメニューにコンパートメントリストが表示されます。コンパートメントはリソースの整理に役立ち、リソースへのアクセスを制御しやすくなります。ルートコンパートメントは、テナントがプロビジョニングされるときにOracleによって作成されます。管理者は、ルートコンパートメントにさらに多くのコンパートメントを作成し、アクセスルールを追加して、どのユーザがそれらのコンパートメントを表示してアクションを実行できるかを制御できます。詳細については、Oracleのドキュメント『コンパートメントの管理(Managing Compartments)』を参照してください。

手順

ステップ1 OCI にログインし、地域を選択します。

OCI は互いに分かれた複数の地域に分割されています。地域は、画面の右上隅に表示されま す。ある地域内のリソースは、別の地域には表示されません。目的の地域内に存在しているこ とを定期的に確認してください。

- ステップ2 [ネットワーキング(Networking)]>[仮想クラウドネットワーク(Virtual Cloud Networks)] を選択し、[VCN の作成(Create VCN)]をクリックします。
- ステップ3 [名前(Name)] に、VCN のわかりやすい名前を入力します(例: FTDv-Management)。
- ステップ4 VCNの CIDR ブロックを入力します。
- ステップ5 [VCN の作成 (Create VCN)]をクリックします。

次のタスク

次の手順に進み、管理VCNを完了します。管理VCNを完了したら、診断、内部、および外部 の各インターフェイスの VCN を作成します。

ネットワーク セキュリティ グループの作成

ネットワーク セキュリティ グループは、一連の vNIC と、vNIC に適用される一連のセキュリ ティルールで構成されます。

手順

ステップ1 [ネットワーキング(Networking)]>[仮想クラウドネットワーク(Virtual Cloud Networks)]> [仮想クラウドネットワークの詳細(Virtual Cloud Network Details)]>[ネットワーク セキュ リティ グループ(Network Security Groups)]を選択し、[ネットワーク セキュリティ グルー プの作成(Create Network Security Group)] をクリックします。

- **ステップ2**[名前(Name)]に、ネットワーク セキュリティ グループのわかりやすい名前を入力します (例:FTDv-Mgmt-Allow-22-8305)。
- ステップ3 [Next] をクリックします。
- ステップ4 セキュリティルールを追加します。
 - a) SSH アクセスに TCP ポート 22 を許可するルールを追加します。
 - b) HTTPS アクセスに TCP ポート 443 を許可するルールを追加します。

FTDvはFirepower Management Center を介して管理できます。これには、HTTPS 接続用に ポート 8305 を開く必要があります。

(注) これらのセキュリティルールを管理インターフェイス/VCN に適用します。

ステップ5 [作成 (Create)]をクリックします。

インターネットゲートウェイの作成

管理サブネットを公的にアクセス可能にするには、インターネットゲートウェイが必要です。

手順

- ステップ1 [ネットワーキング(Networking)]>[仮想クラウドネットワーク(Virtual Cloud Networks)]> [仮想クラウドネットワークの詳細(Virtual Cloud Network Details)]>[インターネットゲート ウェイ(Internet Gateways)]を選択し、[インターネットゲートウェイの作成(Create Internet Gateway)] をクリックします。
- **ステップ2** [名前 (Name)] にインターネットゲートウェイのわかりやすい名前を入力します(例: *FTDv-IG*)。
- ステップ3 [インターネットゲートウェイの作成 (Create Internet Gateway) をクリックします。
- **ステップ4** インターネットゲートウェイへのルートを追加します。
 - a) [ネットワーキング (Networking)]>[仮想クラウドネットワーク (Virtual Cloud Networks)]>[仮想クラウドネットワークの詳細 (Virtual Cloud Network Details)]>[ルー トテーブル (Route Tables)]を選択します。
 - b) ルートルールを追加するには、デフォルトのルートテーブルのリンクをクリックします。
 - c) [ルートルールの追加(Add Route Rules)]をクリックします。
 - d) [ターゲットタイプ(Target Type)] ドロップダウンから、[インターネットゲートウェイ (Internet Gateway)]を選択します。
 - e) 宛先 CIDR のブロックを入力します(例: 0.0.0/0)。
 - f) [ターゲット インターネット ゲートウェイ(Target Internet Gateway)] ドロップダウンか ら、作成したゲートウェイを選択します。
 - g) [ルートルールの追加(Add Route Rules)]をクリックします。

サブネットの作成

各 VCN には、少なくとも1つのサブネットがあります。管理 VCN の管理サブネットを作成し ます。また、診断 VCN の診断サブネット、内部 VCN の内部サブネット、および外部 VCN の 外部サブネットも必要です。

手順

- ステップ1 [ネットワーキング(Networking)]>[仮想クラウドネットワーク(Virtual Cloud Networks)]> [仮想クラウドネットワークの詳細(Virtual Cloud Network Details)]>[サブネット(Subnets)] を選択し、[サブネットの作成(Create Subnet)]をクリックします。
- ステップ2 サブネットのわかりやすい名前を入力します(例: Management)。
- ステップ3 [サブネットタイプ (Subnet Type)]を選択します(推奨されるデフォルトの[地域 (Regional)] のままにします)。
- **ステップ4 CIDR ブロック**を入力します(例:10.10.0.0/24)。サブネットの内部(非公開)IP アドレス は、この CIDR ブロックから取得されます。
- ステップ5 [ルートテーブル (Route Table)]ドロップダウンから、以前に作成したルートテーブルのいず れかを選択します。
- ステップ6 サブネットの[サブネットアクセス (Subnet Access)]を選択します。

管理サブネットの場合、これはパブリックサブネットである必要があります。

- ステップ7 [DHCPオプション(DHCP Option)]を選択します。
- ステップ8 以前作成した [セキュリティリスト (Security List)]を選択します。
- ステップ9 [サブネットの作成 (Create Subnet)]をクリックします。

次のタスク

VCN(管理、診断、内部、外部)を設定すると、FTDvを起動する準備が整います。FTDvVCN 構成の例については、次の図を参照してください。

図 2: FTDv 仮想クラウドネットワーク

Virtual Cloud Networks in ftdv Compartment

Virtual Cloud Networks are virtual, private networks that you set up in Oracle data centers. It closely resembles a traditional network, with firewall rules and specific types of communication gateways that you can choose to use.

Name	State	CIDR Block	Default Route Table	DNS Domain Name	Created •	
FTDy-Outside	Available	10.10.3.0/24	Default Route Table for FTDV-Outside	fidvoutside.oraclevcn.com	Mon, Jul 6, 2020, 14:32:07 UTC	ł
ETDy-Inside	 Available 	10.10.2.0/24	Default Route Table for FTDV-Inside	fidvinside.oraclevcn.com	Mon, Jul 6, 2020, 14:31:38 UTC	:
ETDy-Diagnostic	 Available 	10.10.1.0/24	Default Route Table for FTDv-Diagnostic	ftdvdiagnostic.oraclevcn.com	Mon, Jul 6, 2020, 14:30:46 UTC	:
ETDy-Management	Available	10.10.0/24	Default Route Table for FTDv-Management	fidvmanagement oraclevon.com	Mon, Jul 6, 2020, 14:29:16 UTC	:

OCI 上の FTDv インスタンスの作成

Oracle Cloud Marketplace の Cisco Firepower NGFW 仮想ファイアウォール (NGFWv) 製品を使用して、コンピューティングインスタンスを介して OCI に FTDv を展開します。CPU の数、メモリの量、ネットワークリソースなどの特性に基づいて、最適なマシンシェイプを選択します。

手順

- ステップ1 OCI ポータルにログインします。 地域は、画面の右上隅に表示されます。目的の地域内に存在していることを確認してください。
- ステップ2 [マーケットプレイス (Marketplace)]>[アプリケーション (Applications)]を選択します。
- **ステップ3** マーケットプレイスで「Cisco Firepower NGFW virtual firewall (NGFWv)」を検索して、製品を 選択します。
- **ステップ4** 契約条件を確認し、[Oracle の利用規約とパートナーの契約条件を確認して同意します。(I have reviewed and accept the Oracle Terms of Use and the Partner terms and conditions.)] チェック ボックスをオンにします。
- ステップ5 [インスタンスの起動(Launch Instance)]をクリックします。
- ステップ6 [名前 (Name)] に、インスタンスのわかりやすい名前を入力します(例: FTDv-6-7)。
- ステップ7 [シェイプの変更(Change Shape)]をクリックし、FTDv に必要な CPU の数、RAM の量、お よびインターフェイスの数が指定されたシェイプ(VM.Standard2.4 など)を選択します(OCI への FTDv の展開について(1ページ)を参照)。
- **ステップ8** [仮想クラウドネットワーク(Virtual Cloud Network)] ドロップダウンから、[管理 VCN (Management VCN)]を選択します。
- **ステップ9** 自動入力されていない場合は、**[サブネット(Subnet)]** ドロップダウンから [管理サブネット (Management subnet)]を選択します。
- ステップ10 [ネットワークセキュリティグループを使用してトラフィックを制御する(Use Network Security Groups to Control Traffic)]にチェックを入れ、管理 VCN に設定したセキュリティグループ を選択します。
- **ステップ11** [パブリック IP アドレスの割り当て(Assign a Public Ip Address)] オプションボタンをクリッ クします。
- **ステップ12** [SSH キーの追加(Add SSH keys)]の下で、[公開キーの貼り付け(Paste Public Keys)]オプ ションボタンをクリックして、SSH キーを貼り付けます。

Linux ベースのインスタンスは、パスワードの代わりにSSH キーペアを使用してリモートユー ザを認証します。キーペアは、秘密キーと公開キーで構成されます。インスタンスを作成する ときに、秘密キーをコンピュータに保持し、公開キーを提供します。ガイドラインについて は、『Linux インスタンスでのキーペアの管理(Managing Key Pairs on Linux Instances)』 https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/Tasks/managingkeypairs.htmを参照してください。

- **ステップ13** [詳細オプションの表示 (Show Advanced Options)] リンクをクリックして、オプションを展開します。
- ステップ14 [初期化スクリプト(Initialization Script)]の下で、[クラウド初期化スクリプトの貼り付け(Paste Cloud-Init Script)]オプションボタンをクリックして、FTDvのday0構成を指定します。day0構成は、FTDvの初回起動時に適用されます。

次に、[クラウド初期化スクリプト(Cloud-Init Script)]フィールドにコピーして貼り付ける ことができる day0 構成の例を示します。

```
{
"Hostname": "ftdv-oci",
"AdminPassword": "myPassword@123456",
"FirewallMode": "routed",
"IPv4Mode": "dhcp",
"ManageLocally": "No",
"FmcIp": "1.2.3.4",
"FmcRegKey": "ciscol23reg",
"FmcNatId": "ciscol23nat"
}
```

- FmcRegKey:これは、デバイスを Firepower Management Center に登録するために使用される1回限りの登録キーです。登録キーは、ユーザ定義の最大 37 文字の英数字値です。
- FmcNatId:これは1回限り使用される一意の文字列です(ユーザが定義)。ただし、センサーと Defense Center が NAT デバイスにより分離されている場合は、この一意の登録 キーと同時に一意の NAT ID を入力する必要があります。

ステップ15 [作成 (Create)]をクリックします。

次のタスク

[作成(Create)]ボタンをクリックした後、状態が[プロビジョニング(Provisioning)]として 表示される FTDv インスタンスをモニタします。



重要 ステータスをモニタすることが重要です。FTDv インスタンスの状態が [プロビジョニング (Provisioning)]から [実行中(Running)]に移行したら、FTDv ブートが完了する前に必要に 応じて VNIC を接続する必要があります。

インターフェイスの接続

FTDv は、1 つの VNIC が接続された状態で実行状態になります([コンピューティング (Compute)]>[インスタンス(Instances)]>[インスタンスの詳細(Instance Details)]>[接 続された VNIC (Attached VNICs)]を参照)。これはプライマリ VNIC と呼ばれ、管理 VCN にマッピングされます。FTDvが最初のブートを完了する前に、VNICがFTDvで正しく検出されるように、以前に作成した他のVCNサブネット(診断、内部、外部)のVNICを接続する 必要があります。

手順

- **ステップ1**新しく起動した FTDv インスタンスを選択します。
- ステップ2 [接続された VNIC (Attached VNICs)]>[VNIC の作成(Create VNIC)]の順に選択します。
- ステップ3 [名前 (Name)] に、VNIC のわかりやすい名前を入力します(例: Inside)。
- ステップ4 [仮想クラウドネットワーク(Virtual Cloud Network)]ドロップダウンから VCN を選択しま す。
- **ステップ5** [サブネット (Subnet)]ドロップダウンからサブネットを選択します。
- **ステップ6** [ネットワークセキュリティグループを使用してトラフィックを制御する(Use Network Security Groups to Control Traffic)] をオンにして、選択した VCN 用に設定したセキュリティグループを選択します。
- **ステップ7** [送信元と宛先のチェックをスキップ (Skip Source Destination Check)]をオンにします。
- ステップ8 (オプション)[プライベートIPアドレス (Private IP Address)]を指定します。これは、VNIC に対して特定の IP を選択する場合にのみ必要です。

IP を指定しない場合、OCI はサブネットに割り当てられた CIDR ブロックから IP アドレスを 割り当てます。

- ステップ9 [変更の保存 (Save Changes)] をクリックし、VNIC を作成します。
- ステップ10 展開で必要となる各 VNIC について、この手順を繰り返します。

接続された VNIC のルートルールの追加

診断、内部、および外部の各ルートテーブルにルートテーブルルールを追加します。

手順

- ステップ1 [ネットワーキング(Networking)]>[仮想クラウドネットワーク(Virtual Cloud Networks)] を選択し、VCNに関連付けられているデフォルトルートテーブル(内部または外部)をクリッ クします。
- ステップ2 [ルートルールの追加(Add Route Rules)]をクリックします。
- ステップ3 [ターゲットタイプ (Target Type)]ドロップダウンから、[プライベート IP (Private IP)]を選択します。
- **ステップ4** [宛先タイプ (Destination Type)] ドロップダウンから、[CIDR ブロック (CIDR Block)] を選 択します。

ステップ5 [宛先 CIDR ブロック (Destination CIDR Block)]を入力します (例: 0.0.0.0/0)。

ステップ6 [ターゲット選択(Target Selection)] フィールドに VNIC のプライベート IP アドレスを入力します。

VNICにIPアドレスを明示的に割り当てていない場合は、VNICの詳細([コンピューティング (Compute)]>[インスタンス(Instances)]>[インスタンスの詳細(Instance Details)]>[接 続された VNIC(Attached VNICs)])で自動割り当てされた IP アドレスを確認できます。

- ステップ7 [ルートルールの追加(Add Route Rules)]をクリックします。
- ステップ8 展開で必要となる各 VNIC について、この手順を繰り返します。



OCI 上の FTDv インスタンスへのアクセス

セキュアシェル(SSH)接続を使用して、実行中のインスタンスに接続できます。

- ほとんどの UNIX スタイルのシステムには、デフォルトで SSH クライアントが含まれています。
- Windows 10 および Windows Server 2019 システムには、OpenSSH クライアントが含まれている必要があります。Oracle Cloud Infrastructure によって生成された SSH キーを使用してインスタンスを作成した場合に必要になります。
- その他の Windows バージョンの場合は、http://www.putty.org から無償の SSH クライアン トである PuTTY をダウンロードできます。

前提条件

インスタンスに接続するには、次の情報が必要です。

- インスタンスのパブリック IP アドレス。アドレスは、コンソールの[インスタンスの詳細 (Instance Details)]ページから取得できます。ナビゲーションメニューを開きます。[コ アインフラストラクチャ(Core Infrastructure)]の下で、[コンピューティング(Compute)] に移動し、[インスタンス(Instances)]をクリックします。次に、インスタンスを選択し ます。あるいは、コアサービス APIの ListVnicAttachments および GetVnic 操作を使用でき ます。
- インスタンスのユーザ名とパスワード、またはインスタンスを起動したときに使用した SSHキーペアの秘密キー部分へのフルパス、またはその両方。



(注)

Day0構成を追加しない場合は、デフォルトのログイン情報(admin/Admin123)を使用して FTDv インスタンスにログインできます。

最初のログイン試行時にパスワードを設定するように求められます。

- SSH を使用した FTDv インスタンスへの接続 (14 ページ)
- OpenSSH を使用した FTDv インスタンスへの接続 (14ページ)
- PuTTY を使用した FTDv インスタンスへの接続 (15ページ)

SSH を使用した FTDv インスタンスへの接続

UNIX スタイルのシステムから FTDv インスタンスに接続するには、SSH を使用してインスタンスにログインします。

手順

ステップ1 次のコマンドを使用して、ファイルの権限を設定し、自分だけがファイルを読み取れるように します。

\$ chmod 400 <private key>

ここで、

<private_key>は、アクセスするインスタンスに関連付けられた秘密キーを含むファイルの フルパスと名前です。

ステップ2 インスタンスにアクセスするには、次の SSH コマンドを使用します。

\$ ssh -i <private_key> <username>@<public-ip-address>

ここで、

<private_key>は、アクセスするインスタンスに関連付けられた秘密キーを含むファイルの フルパスと名前です。

<username>は、FTDv インスタンスのユーザ名です。

<public-ip-address>は、コンソールから取得したインスタンスの IP アドレスです。

OpenSSHを使用した FTDv インスタンスへの接続

Windows システムから FTDv インスタンスに接続するには、OpenSSHを使用してインスタンス にログインします。

手順

ステップ1 このキーペアを初めて使用する場合は、自分だけがファイルを読み取れるようにファイルの権限を設定する必要があります。

次の手順を実行します。

- a) Windows Explorer で、秘密キーファイルに移動し、ファイルを右クリックして[プロパティ (**Properties**)]をクリックします。
- b) [セキュリティ (Security)] タブで、[詳細設定 (Advanced)] をクリックします。

- c) [オーナー (Owner)] が自分のユーザアカウントであることを確認します。
- d) [継承の無効化(Disable Inheritance)] をクリックし、[継承された権限をこのオブジェクトの明示的な権限に変換する(Convert inherited permissions into explicit permissions on this object)] を選択します。
- e) 自分のユーザアカウントではない各権限エントリを選択し、[削除(Remove)]をクリック します。
- f) 自分のユーザアカウントのアクセス権限が [フルコントロール (Full Control)] であるこ とを確認します。
- g) 変更を保存します。

ステップ2 インスタンスに接続するには、Windows PowerShell を開き、次のコマンドを実行します。

\$ ssh -i <private_key> <username>@<public-ip-address>

ここで、

<private_key>は、アクセスするインスタンスに関連付けられた秘密キーを含むファイルの フルパスと名前です。

<username>は、FTDv インスタンスのユーザ名です。

vpublic-ip-address>は、コンソールから取得したインスタンスのIPアドレスです。

PuTTYを使用した FTDv インスタンスへの接続

PuTTY を使用して Windows システムから FTDv インスタンスに接続するには、次の手順を実行します。

手順

- ステップ1 PuTTYを開きます。
- **ステップ2 [カテゴリ(Category)]** ペインで、**[セッション(Session)]** を選択し、次の内容を入力しま す。
 - •ホスト名または IP アドレス:
 - <username>@<public-ip-address>

ここで、

<username>は、FTDv インスタンスのユーザ名です。

<public-ip-address>は、コンソールから取得したインスタンスのパブリックIPアド レスです。

- ポート: 22
- 接続タイプ:SSH

ステップ3 [カテゴリ (Category)]ペインで、[Window]を展開し、[変換 (Translation)]を選択します。 ステップ4 [リモート文字セット (Remote character set)]ドロップダウンリストで、[UTF-8]を選択しま す。

> Linux ベースのインスタンスでデフォルトのロケール設定はUTF-8 です。これにより、PuTTY は同じロケールを使用するように設定されます。

- **ステップ5** [カテゴリ(Category)]ペインで、[接続(Connection)]、[SSH]の順に展開し、[認証(Auth)] をクリックします。
- ステップ6 [参照 (Browse)] をクリックして、秘密キーを選択します。
- ステップ7 [開く (Open)]をクリックして、セッションを開始します。

インスタンスに初めて接続する場合は、「サーバのホストキーがレジストリにキャッシュされ ていない(the server's host key is not cached in the registry)」というメッセージが表示されるこ とがあります。[はい(Yes)]をクリックして、接続を続行します。



Firepower Management Center を使用した Firepower Threat Defense Virtual の管理

この章では、FMCを使用して管理されるスタンドアロンのFTDvデバイスを展開する方法について説明します。

(注)

本書では、最新の FTDv バージョンの機能を取り上げています。機能の変更の詳細について は、「Firepower Management を使用した Firepower Threat Defense Virtual の管理の履歴 (34 ページ)」を参照してください。古いバージョンのソフトウェアを使用している場合は、お使 いのバージョンの FMC 設定ガイドの手順を参照してください。

- Firepower Management Center を使用した Firepower Threat Defense Virtual について (17 ページ)
- Firepower Management Center へのデバイスの登録 (18 ページ)
- ・基本的なセキュリティポリシーの設定 (21ページ)
- Firepower Threat Defense CLI へのアクセス $(33 \, \stackrel{\sim}{\sim} \stackrel{\scriptstyle \checkmark}{\scriptstyle \checkmark})$
- Firepower Management を使用した Firepower Threat Defense Virtual の管理の履歴 (34 ページ)

Firepower Management Center を使用した Firepower Threat Defense Virtual について

Firepower Threat Defense 仮想 (FTDv) は、Cisco NGFW ソリューションの仮想化コンポーネン トです。FTDv は、ステートフル ファイアウォール、ルーティング、VPN、Next-Generation Intrusion Prevention System (NGIPS) 、Application Visibility and Control (AVC) 、URL フィル タリング、高度なマルウェア防御 (AMP) などの次世代ファイアウォールサービスを提供しま す。 FTDv を管理するには、別のサーバ上で実行されるフル機能のマルチデバイスマネージャである Firepower Management Center (FMC)を使用します。FMC のインストールの詳細については、『FMCgetting started guide』を参照してください。

FTDvは、FTDv仮想マシンに割り当てた管理インターフェイス上のFMCを登録して通信します。

トラブルシューティングの目的で、管理インターフェイス上の SSH を使用して FTD CLI にア クセスすることも、Firepower CLI から FTD に接続することもできます。

Firepower Management Center へのログイン

FMC を使用して、FTD を設定および監視します。

始める前に

サポートされているブラウザの詳細については、使用するバージョンのリリースノート (https://www.cisco.com/go/firepower-notes)を参照してください。

手順

ステップ1 サポートされているブラウザを使用して、次の URL を入力します。

https://fmc_ip_address

fmc_ip_address は、FMC の IP アドレスまたはホスト名を指定します。

ステップ2 ユーザ名とパスワードを入力します。

ステップ3 [ログイン (Log In)]をクリックします。

Firepower Management Center へのデバイスの登録

始める前に

FTDv 仮想マシンが、正常に展開されていて、電源がオンになっており、最初のブート手順を 実行済みであることを確認してください。



(注) この手順では、day0/bootstrap スクリプトを使用して、FMC の登録情報が指定されていることを前提としています。ただし、これらの設定すべては、後から CLI で configure network コマンドを使用して変更できます。FTD のコマンドリファレンスを参照してください。

手順

- ステップ1 [デバイス(Devices)]>[デバイス管理(Device Management)]を選択します。
- ステップ2 [追加(Add)]ドロップダウンリストから、[デバイスの追加(Add Device)]を選択し、次の パラメータを入力します。

dd Device		?
Host:*	ftd-1.cisco.com	
Display Name:	ftd-1.cisco.com	
Registration Key:*	•••••	
Group:	None	*
Access Control Policy:*	Initial Policy	*
Smart Licensing		
Malware		
Threat		
URL Filtering	2	
Advanced		
Unique NAT ID:†	cisco123nat	
Transfer Packets		
	Register	Cancel

- [ホスト(Host)]: 追加するデバイスの IP アドレスを入力します。
- [表示名(Display Name)]: FMC に表示するデバイスの名前を入力します。
- •[登録キー(Registration key)]: FTDv ブートストラップ設定で指定したものと同じ登録 キーを入力します。
- •[ドメイン (Domain)]:マルチドメイン環境を使用している場合は、デバイスをリーフド メインに割り当てます。
- •[グループ(Group)]: グループを使用している場合は、デバイスグループに割り当てま す。
- 「アクセスコントロールポリシー(Access Control Policy)]:初期ポリシーを選択します。
 使用する必要があることがわかっているカスタマイズ済みのポリシーがすでにある場合を
 除いて、[新しいポリシーの作成(Create new policy)]を選択し、[すべてのトラフィック
 をブロック(Block all traffic)]を選択します。後でこれを変更してトラフィックを許可す
 ることができます。「アクセス制御の設定(31ページ)」を参照してください。

Name:	ftd_ac_policy		
Description:			
Select Base Policy:	None	v	
Default Action:	• Block all traffic O Intrusion Pre	evention O Network Discovery	

- [スマートライセンス (Smart Licensing)]:展開する機能に必要なスマートライセンスとして、[マルウェア (Malware)](AMP マルウェアインスペクションを使用する予定の場合)、[脅威 (Threat)](侵入防御を使用する予定の場合)、および[URL](カテゴリベースの URL フィルタリングを実装する予定の場合)を割り当てます。
- •[一意の NAT ID (Unique NAT ID)]: FTDv ブートストラップ設定で指定した NAT ID を 指定します。
- 「パケットの転送(Transfer Packets)]: デバイスから FMC へのパケット転送を許可します。このオプションを有効にして IPS や Snort などのイベントがトリガーされた場合は、 デバイスが検査用としてイベントメタデータ情報とパケットデータを FMCに送信します。 このオプションを無効にした場合は、イベント情報だけが FMCに送信され、パケットデー タは送信されません。
- ステップ3 [登録(Register)]をクリックし、正常に登録されたことを確認します。

登録が成功すると、デバイスがリストに追加されます。失敗した場合は、エラーメッセージが 表示されます。FTDv が登録に失敗した場合は、次の項目を確認してください。

ping: FTD CLI(「Firepower Threat Defense CLIへのアクセス (33ページ)」)にアクセスし、次のコマンドを使用して FMC IP アドレスへの ping を実行します。

ping system ip_address

ping が成功しない場合は、show network コマンドを使用してネットワーク設定を確認しま す。FTD IP アドレスを変更する必要がある場合は、configure network {ipv4 | ipv6} manual コマンドを実行します。

- NTP:NTPサーバが[システム (System)]>[設定 (Configuration)]>[時刻の同期 (Time Synchronization)] ページの FMC サーバセットと一致することを確認します。
- ・登録キー、NAT ID、および FMC IP アドレス:両方のデバイスで同じ登録キーを使用していることを確認し、使用している場合は NAT ID を使用していることを確認します。
 configure manager add コマンドを使用して、FTDv で登録キーと NAT ID を設定することができます。また、このコマンドで FMC IP アドレスを変更することもできます。

基本的なセキュリティポリシーの設定

ここでは、次の設定を使用して基本的なセキュリティポリシーを設定する方法について説明します。

- 内部インターフェイスと外部インターフェイス:内部インターフェイスにスタティックIP アドレスを割り当て、外部インターフェイスに DHCP を使用します。
- DHCP サーバ: クライアントの内部インターフェイスで DHCP サーバを使用します。
- ・デフォルトルート:外部インターフェイスを介してデフォルトルートを追加します。
- •NAT:外部インターフェイスでインターフェイス PAT を使用します。
- •アクセスコントロール:内部から外部へのトラフィックを許可します。

手順

ステップ1 インターフェイスの設定 (21ページ)

- ステップ2 DHCP サーバの設定 (25 ページ)
- ステップ3 デフォルトルートの追加 (26ページ)
- ステップ4 NAT の設定 (28 ページ)
- ステップ5 アクセス制御の設定(31ページ)
- ステップ6 設定の展開 (32ページ)

インターフェイスの設定

FTDv インターフェイスを有効にし、それらをセキュリティゾーンに割り当て、IP アドレスを 設定します。通常は、システムで意味のあるトラフィックを通過させるように、少なくとも2 つのインターフェイスを設定する必要があります。通常は、アップストリームルータまたはイ ンターネットに面した外部インターフェイスと、組織のネットワークの1つ以上の内部イン ターフェイスを使用します。これらのインターフェイスの一部は、Webサーバなどのパブリッ クアクセスが可能なアセットを配置する「緩衝地帯」(DMZ)となる場合があります。

一般的なエッジルーティングの状況は、内部インターフェイスでスタティックアドレスを定義 すると同時に、ISP から DHCP を介して外部インターフェイスアドレスを取得することです。

次の例では、DHCPによるスタティックアドレスとルーテッドモードの外部インターフェイス を使用して、ルーテッドモードの内部インターフェイスを設定します。

手順

- **ステップ1 [デバイス (Devices)**]>**[デバイス管理 (Device Management)**]を選択し、デバイスの をク リックします。
- ステップ2 [インターフェイス (Interfaces)]をクリックします。

Overview Analysis Policies	Devices Objects	AMP Inte	dligence			e, o	eploy System I	Help + admin +
Device Management NAT	VPN VQoS Platfo	rm Settings	FlexConfig C	ertificates				
FTD Virtual							8	Cancel
Cisco Firepower Threat Defense for VMIII	iare (
Device Routing Interface	Inline Sets DH	CP						
						Search by name	Sync Device	Add Interfaces •
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address		Virtual Router	-
Disprostict/0	diagnostic	Physical					Global	1
GipabitEthemet0/0		Physical						1
GipabitEthernet0/1		Physical						1
GigabitEthernet0/2		Physical						1
Gipsbittthemett/3		Physical						1
GipabitEthernet0/4		Physical						1
Gipsbittthemet0/5		Physical						1
GigabitEthemetD/6		Physical						1
GipabitEthernet0/7		Physical						1

ステップ3 「内部」に使用するインターフェイスの をクリックします。

[全般(General)]タブが表示されます。

	Edit Physical Interfac	e					? ×
	General IPv4 IPv6	Advanced Hare	dware Configuration				
	Name:	inside			Enabled	🗌 Manager	nent Only
	Description:						
	Mode:	None		*			
	Security Zone:	inside_zone		*			
	Interface ID:	GigabitEthernet0/0					
	MTU:	1500	(64 - 9000)				
					0	K Ca	ancel
a) 48 文字までの [名育	〕(Name)] を入:	力します。				
			•) , > / / / /	6.0			

- たとえば、インターフェイスに inside という名前を付けます。
- b) [有効(Enabled)]チェックボックスをオンにします。
- c) [モード (Mode)]は[なし (None)]に設定したままにします。

d) [セキュリティゾーン (Security Zone)]ドロップダウンリストから既存の内部セキュリティ ゾーンを選択するか、[新規 (New)]をクリックして新しいセキュリティゾーンを追加し ます。

たとえば、inside_zoneという名前のゾーンを追加します。各インターフェイスは、セキュ リティゾーンおよびインターフェイスグループに割り当てる必要があります。インター フェイスは、1つのセキュリティゾーンにのみ属することも、複数のインターフェイスグ ループに属することもできます。ゾーンまたはグループに基づいてセキュリティポリシー を適用します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インター フェイスを外部ゾーンに割り当てることができます。この場合、トラフィックが内部から 外部に移動できるようにアクセスコントロールポリシーを設定することはできますが、 外部から内部に向けては設定できません。ほとんどのポリシーはセキュリティゾーンのみ サポートしています。NAT ポリシー、プレフィルタ ポリシー、および QoS ポリシーで、 ゾーンまたはインターフェイスグループを使用できます。

- e) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。
 - •[IPv4]:ドロップダウンリストから[スタティックIPを使用する(Use Static IP)]を選択し、IPアドレスとサブネットマスクをスラッシュ表記で入力します。

たとえば、192.168.1.1/24 などと入力します。

Edit Physical Interface	e	
General IPv4 IPv6	Advanced	Hardware Configuration
IP Type:	Use Static IP	×
IP Address:	192.168.1.1/24	eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

•[IPv6]:ステートレス自動設定の場合は[自動設定(Autoconfiguration)]チェックボッ クスをオンにします。

f) [OK] をクリックします。

ステップ4 「外部」に使用するインターフェイスの をクリックします。

[全般(General)]タブが表示されます。

Edit Physical Inte	erface						? >
General IPv4	IPv6	Advanced	Hardware	Configuration			
Name:		outside			🗹 En	abled	Management Only
Description:							
Mode:		None			*		
Security Zone:		outside_zone			~		
Interface ID:		GigabitEtherne	et0/0				
MTU:		1500		(64 - 9000)			
					(Ok	Cancel

a) 48 文字までの [名前 (Name)] を入力します。

たとえば、インターフェイスに「outside」という名前を付けます。

- b) [有効(Enabled)]チェックボックスをオンにします。
- c) [モード (Mode)]は[なし (None)]に設定したままにします。
- d) [セキュリティゾーン (Security Zone)]ドロップダウンリストから既存の外部セキュリティ ゾーンを選択するか、[新規 (New)]をクリックして新しいセキュリティゾーンを追加し ます。

たとえば、「outside zone」という名前のゾーンを追加します。

- e) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。
 - •[IPv4]: [DHCPの使用(Use DHCP)]を選択し、次のオプションのパラメータを設定 します。
 - [DHCP を使用してデフォルトルートを取得(Obtain default route using DHCP)]:
 DHCP サーバからデフォルトルートを取得します。
 - [DHCPルートメトリック(DHCP route metric)]:アドミニストレーティブディス タンスを学習したルートに割り当てます(1~255)。学習したルートのデフォ ルトのアドミニストレーティブディスタンスは1です。

Edit Phys	sical Int	terface			
General	IPv4	IPv6	Advanced	Hardware	e Configuration
IP Type:		L	Jse DHCP	~	
Obtain def DHCP:	ault route	using 🧧	3		
DHCP rout	e metric:	1	L		(1 - 255)

•[IPv6]:ステートレス自動設定の場合は[自動設定(Autoconfiguration)]チェックボックスをオンにします。

f) [OK] をクリックします。

ステップ5 [保存 (Save)] をクリックします。

DHCP サーバの設定

(注) AWS、Azure、GCP、OCIなどのパブリッククラウド環境に展開する場合は、この手順をスキッ プします。

クライアントでDHCPを使用してFTDvからIPアドレスを取得するようにする場合は、DHCP サーバを有効にします。

手順

- ステップ1 [デバイス (Devices)]>[デバイス管理 (Device Management)]を選択し、デバイスの をク リックします。
- ステップ2 [DHCP] > [DHCPサーバ(DHCP Server)]を選択します。
- ステップ3 [サーバ (Server)]ページで、[追加 (Add)]をクリックして、次のオプションを設定します。

Add Server			? ×
Interface*	inside	~	
Address Pool*	10.9.7.9-10.9.7.25		(2.2.2.10-2.2.2.20)
Enable DHCP Server			
			OK Cancel

•[インターフェイス (Interface)]:ドロップダウンリストからインターフェイスを選択します。

- [アドレスプール(Address Pool)]: DHCP サーバが使用する IP アドレスの最下位から最 上位の間の範囲を設定します。IP アドレスの範囲は、選択したインターフェイスと同じサ ブネット上に存在する必要があり、インターフェイス自身の IP アドレスを含めることは できません。
- •[DHCPサーバを有効にする(Enable DHCP Server)]: 選択したインターフェイスの DHCP サーバを有効にします。

ステップ4 [OK] をクリックします。

ステップ5 [保存 (Save)]をクリックします。

デフォルトルートの追加

デフォルトルートは通常、外部インターフェイスから到達可能なアップストリームルータを指 し示します。外部インターフェイスにDHCPを使用する場合は、デバイスがすでにデフォルト ルートを受信している可能性があります。手動でルートを追加する必要がある場合は、次の手 順を実行します。DHCPサーバからデフォルトルートを受信した場合は、[デバイス (Devices)]> [デバイス管理 (Device Management)]>[ルーティング (Routing)]>[スタティックルート (Static Route)]ページの [IPv4ルート (IPv4 Routes)] または [IPv6ルート (IPv6 Routes)] テーブルに表示されます。

手順

- **ステップ1** [デバイス (Devices)]>[デバイス管理 (Device Management)]を選択し、デバイスの をク リックします。
- **ステップ2** [ルーティング (Routing)]>[スタティックルート (Static route)]を選択し、[ルートを追加 (Add route)]をクリックして、次のように設定します。

Type:	◉ IPv4 ○ IPv6		
Interface*	outside	~	
Available Net	work C 🔘	Selected Network	
🔍 Search		any-ipv4	1
any-ipv4			
💂 IPv4-Ben	chmark-Tests		
📄 IPv4-Link	c-Local		
📄 IPv4-Mult	ticast	dd	
📰 IPv4-Priv	ate-10.0.0.0-8		
IPv4-Priv	ate-172.16.0.0		
IPv4-Priv	ate-192.168.0.		
E IPv4-Priv	ate-All-RFC191		
IPV6-t0-1	PV4-Relay-Any		
Gateway*	default-gateway	▼ ②	
Metric:	1	(1 - 254)	
Tunneled:	Used only for default Rou	te)	
Route Tracking:		v ()	

- •[タイプ (Type)]: 追加するスタティックルートのタイプに応じて、[IPv4] または [IPv6] オプションボタンをクリックします。
- •[インターフェイス (Interface)]:出力インターフェイスを選択します。通常は外部イン ターフェイスです。
- [使用可能なネットワーク (Available Network)]: IPv4 デフォルト ルートの場合は [any-ipv4]、IPv6 デフォルトルートの場合は [any-ipv6] を選択します。
- [ゲートウェイ(Gateway)]または[IPv6ゲートウェイ(IPv6 Gateway)]:このルートのネ クストホップであるゲートウェイルータを入力または選択します。IPアドレスまたはネッ トワーク/ホストオブジェクトを指定できます。
- •[メトリック(Metric)]: 宛先ネットワークへのホップの数を入力します。有効値の範囲 は1~255で、デフォルト値は1です。

ステップ3 [OK] をクリックします。

ルートがスタティックルートテーブルに追加されます。

Overview Analysis Policies	Devices Obj	ects AMP Int	elligence		Deploy	04 System	Help 🔻 ad
Device Management NAT	VPN VOS	Platform Settings	FlexConfig	Certificates			
10.89.5.20 Cisco Firepower 9000 Series SM-24 Thre	eat Defense				You have unsav	ved changes	Save
Device Routing Interface	es Inline Sets	DHCP					
OSPF							Add Route
OSPFv3	Network	Interface	Gateway	Tunneled	Metric	Tracked	
D 💋 BGP	▼ IPv4 Routes						
Static Route	any-ipv4	outside	10.99.10.1	false	1		a 🖓
Multicast Routing	▼ IPv6 Routes						

ステップ4 [保存 (Save)] をクリックします。

NAT の設定

一般的な NAT ルールでは、内部アドレスを外部インターフェイスの IP アドレスのポートに変換します。このタイプの NAT ルールのことをインターフェイス ポート アドレス変換 (PAT) と呼びます。

手順

- ステップ1 [デバイス (Devices)]>[NAT] をクリックし、[新しいポリシー (New Policy)]>[Threat Defense NAT] をクリックします。
- **ステップ2** ポリシーに名前を付け、ポリシーを使用するデバイスを選択し、[保存 (Save)]をクリックします。

Description: Targeted Devices Select devices to which you want to apply this p Available Devices Search by name or value	olicy Selected Devices	
Targeted Devices Select devices to which you want to apply this p Available Devices Search by name or value	olicy Selected Devices	
Select devices to which you want to apply this p Available Devices Search by name or value	olicy Selected Devices	
Search by name or value	Selected Devices	
	192.168.0.16	6)
192,168,0,16	-	
Add to Policy		
	-	
		Control

ポリシーが FMC に追加されます。引き続き、ポリシーにルールを追加する必要があります。

ステップ3 [ルールの追加(Add Rule)]をクリックします。

[NATルールの追加(Add NAT Rule)]ダイアログボックスが表示されます。

ステップ4 基本ルールのオプションを設定します。

Add NAT Rule			
NAT Rule:	Auto NAT Rule	~	
Type:	Dynamic	¥	I Enable
Interface Objects	Translation	PAT Pool	Advanced

- [NATルール (NAT Rule)]: [自動NATルール (Auto NAT Rule)]を選択します。
- •[タイプ(Type)]:[ダイナミック(Dynamic)]を選択します。
- **ステップ5** [インターフェイスオブジェクト (Interface objects)]ページで、[使用可能なインターフェイス オブジェクト (Available Interface Objects)]領域から[宛先インターフェイスオブジェクト (Destination Interface Objects)]領域に外部ゾーンを追加します。

NAT Rule: Auto NAT Rule Type: Dynamic Dynamic Enable	Add NAT Rule						?
Type: Dynamic Constraints PAT Pool Advance Available Interface Objects C Source Interface Objects (0) Destination Interface Objects (1) Search by name Source Interface Objects (0) Destination Interface Objects (1) any Add to Source 2 Add to Destination 2 Add to	NAT Rule:	Auto NAT Rule	~				
Interface Objects Translation PAT Pool Advanced Available Interface Objects C Source Interface Objects (0) Destination Interface Objects (1) Search by name any 3 outside_zone Image: Control of Co	Type:	Dynamic	×	✓ Enable			
Available Interface Objects C Source Interface Objects (0) Destination Interface Objects (1)	Interface Objects	Translation	PAT Pool	Advanced	L		
Search by name any 3▲ outside_zone Add to Source 2 Add to Destination	Available Interface O	bjects 🖒		S	ource Interface Objects (0)	Destination Interface Objects (1)	
	inside_zone		A Sr 2 A Dest	dd to purce dd to ination	1179	3 🔊 outside_zone	

ステップ6 [変換 (Translation)]ページで、次のオプションを設定します。

Add NAT Rule				?
NAT Rule:	Auto NAT Rule	•		
Type:	Dynamic	▼		
Interface Objects	Translation PAT Poe	Advanced		
Original Packet			Translated Packet	
Original Source:*	all-ipv4		Translated Source:	Destination Interface IP
Original Port:	ТСР 💙			
			Translated Port:	

•[元の送信元 (Original Source)]:をクリックして、すべてのIPv4トラフィック (0.0.0.0/0) のネットワークオブジェクトを追加します。

Name	all-ipv4			
Description				
Network	O Host	O Range	Network	○ FQDN
Allow Override	s			

(注) 自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義のany-ipv4オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

- [変換済みの送信元 (Translated Source)]: [宛先インターフェイスIP (Destination Interface IP)]を選択します。
- ステップ1 [保存 (Save)] をクリックしてルールを追加します。

ルールが [ルール (Rules)] テーブルに保存されます。

Overview An	alysis Pol	icies Devices O	bjects AMP Int	elligence					(Deploy 04 S	ystem Help 🕯	admin v
Device Manager	ient NAT	VPN VOS	Platform Settings	FlexConfig Ce	rtificates							
interface_	PAT								You	have unsaved change	s 📄 Save	🙁 Cancel
Enter Description												
											Policy i	Assignments
Rules												
Hilter by Device											0	Add Rule
					Original Pa	cket			Translated Packet		1	
# Direction	Туре	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinatio	Origin ns Servic	al es	Translated Sources	Translated Destinations	Translated Services	Options	
 NAT Rules Before 	re											
 Auto NAT Rules 												
# +	Dynamic	🥞 any	outside_zone	all-ipv4				🍓 Interface			🍓 Dns:faise	0
▼ NAT Rules Afte	r											

ステップ8 NAT ページで [保存 (Save)]をクリックして変更を保存します。

アクセス制御の設定

FTDvをFMCに登録したときに、基本の[すべてのトラフィックをブロック(Block all traffic)] アクセスコントロールポリシーを作成した場合は、デバイスを通過するトラフィックを許可 するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部 ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切な ネットワークへのトラフィックを許可するルールを追加してください。

より高度なセキュリティ設定とルールを設定する場合は、FMCの設定ガイドを参照してください。

手順

- ステップ1 [ポリシー(Policy)]>[アクセスポリシー(Access Policy)]>[アクセスポリシー(Access Policy)]を選択し、FTD に割り当てられているアクセス コントロール ポリシーの をクリック します。
- ステップ2 [ルールを追加(Add Rule)]をクリックし、次のパラメータを設定します。

Add Rule												? ×
Name inside	e_to_outside				🗹 Enal	oled	Insert	into Manda	tory			~
Action 🖌 A	llow			▼ ∪ D ,@ t	60							
Zones	Networks	VLAN Tags	🛆 Users	Applications	Ports	URLs	SGT/ISE Attributes	5		Inspection	Logging	Comments
Available Zor	nes 🖒				Source	Zones (1	L)		Destina	tion Zones (1)		
Search by	name				👬 🛦 i	nside_zon	e	6	<u></u>	utside_zone		6
📩 📐 inside_	zone											
📩 📐 outside	e_zone											
				Add to Source								
				Add to Destination								

- •[名前(Name)]: このルールに名前を付けます(たとえば、inside_to_outside)。
- [送信元ゾーン (Source Zones)]: [使用可能なゾーン (Available Zones)]から内部ゾーン を選択し、[送信元に追加 (Add to Source)]をクリックします。
- 「宛先ゾーン(Destination Zones)]: [使用可能なゾーン(Available Zones)] から外部ゾーンを選択し、[宛先に追加(Add to Destination)] をクリックします。

他の設定はそのままにしておきます。

ステップ3 [追加 (Add)]をクリックします。

ルールが [ルール (Rules)] テーブルに追加されます。

Over	view Analysis P	olicies Dev	ices Objects	AMP Int	elligence							Dep	oloy 🏮	System Help 🔻	
Acce	s Control + Access	Control Ne	twork Discovery	Application	n Detectors	Correlation	Actions v								
ftd_ Enter I	ftd_ac_policy You have unsaved changes Analyze Hit Counts E Save Save														
Prefilt	Prefiter Policy: Default Prefiter Policy: None Identity Policy: None														
												Te	Inheritance	Settings 👖 Policy Assignm	nents (1)
Rule	Rules Security Intelligence HTTP Responses Logging Advanced														
台F	Iter by Device								Show Rul	e Conflicts 😡	Add Categor	y 🕓 Add Ru	le Search F	tules	×
#	Name	Source Zo	Dest Zones	Source Ne	Dest Netw	VLAN Tags	Users	Applications	Source Po	Dest Ports	URLs	ISE/SGT A	Action	U 🗅 🧏 🕁 🔳 🛡	*
- M	▼ Mandatory - ftd_sc_policy (1-1)														
1	🔌 inside_to_outside	🚓 inside_zone	🚓 outside_zone	Any	Any	Any	Any	Any	Any	Any	Any	Any	🖋 Allow	002000	a 🖉
✓ Default - ftd_ac_policy (-)															
There are no rules in this section. Add Rule or Add Category															
Defa	alt Action										Access Cor	trol: Block All Tr	affic		× _ i

ステップ4 [保存 (Save)] をクリックします。

設定の展開

設定の変更をFTDvに展開します。変更を展開するまでは、デバイス上でどの変更もアクティブになりません。

手順

ステップ1 右上の [展開 (Deploy)] をクリックします。



ステップ2 [ポリシーの展開(Deploy Policies)]ダイアログボックスでデバイスを選択し、[展開(Deploy)] をクリックします。

Dep	ploy Policies Version:2019-03-05 03:17 PM					? ×
	Device	Inspect Interruption	Туре	Group	Current Version	(j)
	■ 192.168.0.16	No	FTD		2019-02-28 07:11 AM	

ステップ3 展開が成功したことを確認します。展開のステータスを表示するには、メニューバーの[展開 (Deploy)]ボタンの右側にあるアイコンをクリックします。



Firepower Threat Defense CLI へのアクセス

FTDv CLIを使用して、管理インターフェイスパラメータを変更したり、トラブルシューティングを行ったりできます。CLIにアクセスするには、管理インターフェイスへのSSHを使用するか、VMware コンソールから接続します。

手順

ステップ1 (オプション1) FTDv 管理インターフェイスの IP アドレスに直接 SSH 接続します。

管理 IP アドレスは、仮想マシンを展開したときに設定したものです。初期展開時に設定した「admin」アカウントとパスワードを使用して FTDv にログインします。

ステップ2 (オプション2) VMware コンソールを開き、初期展開時に設定したデフォルトのユーザ名 「admin」アカウントとパスワードを使用して ログインします。

Firepower Management を使用した Firepower Threat Defense Virtual の管理の履歴

機能名	プラット フォームリ リース	機能情報
FMC 管理	6.0	初期サポート。

I

【注意】シスコ製品をご使用になる前に、安全上の注意(www.cisco.com/jp/go/safety_warning/)をご確認ください。本書は、米国シスコ発行ド キュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更され ている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照くだ さい。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.