

FTDインターフェイスIPを更新するためにFMCをAnsibleで設定します。

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](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[確認](#)

[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、Ansibleを使用してFirepower Threat Defense(FTD)インターフェイスIPを設定するために、Firepower Management Center(FMC)を自動化する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。

- アンサブル
- Ubuntuサーバ
- Cisco Firepower Management Center(FMC)仮想
- Cisco Firepower Threat Defense(FTD)仮想

このラボ環境では、AnsibleはUbuntuに導入されています。

この記事で参照されているAnsibleコマンドを実行するために、AnsibleがサポートするすべてのプラットフォームにAnsibleが正常にインストールされていることを確認する必要があります。

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。

- Ubuntuサーバ22.04

- Ansible 2.10.8
- Python 3.10
- Cisco Firepower Threat Defense(FTD)仮想7.4.1
- Cisco Firepower Management Center(FMC)仮想7.4.1

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。

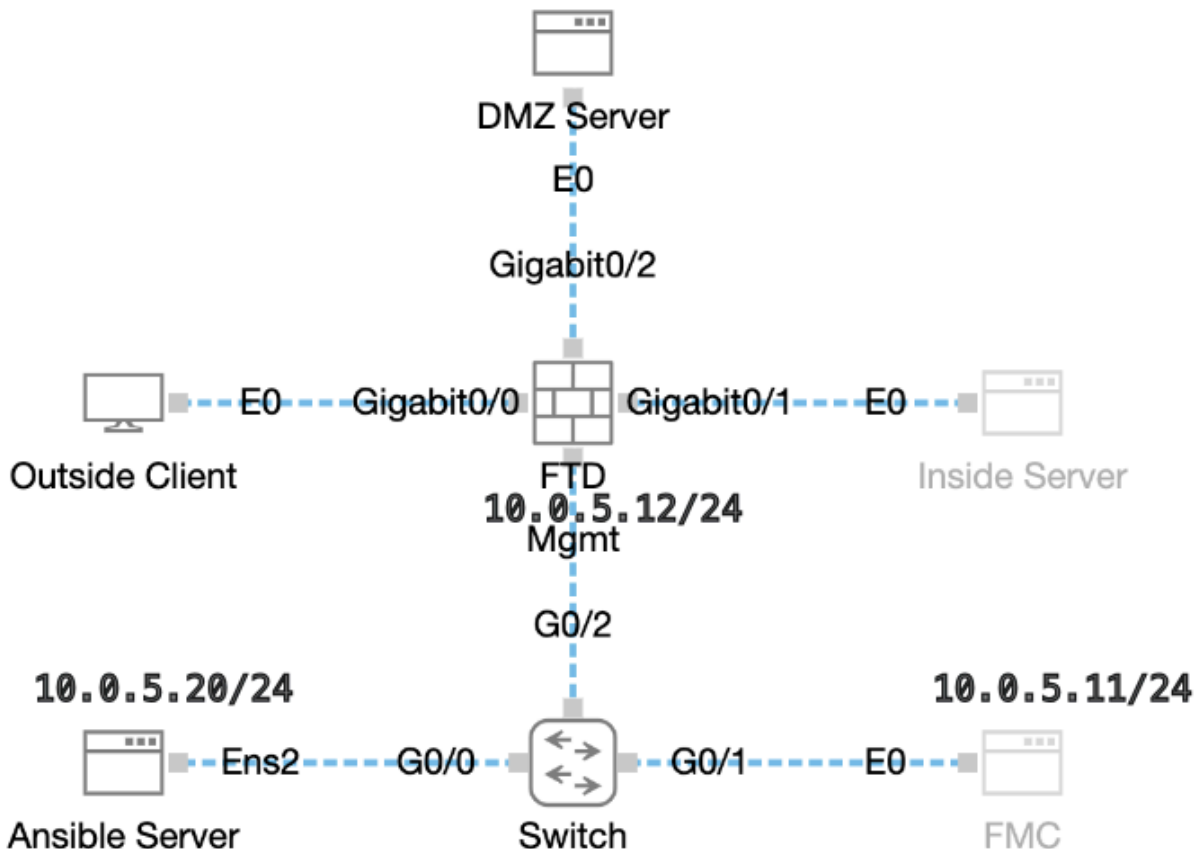
背景説明

Ansibleは汎用性の高いツールで、ネットワークデバイスの管理において大きな効果を発揮します。Ansibleを使用して自動化されたタスクを実行するには、さまざまな方法を使用できます。この文書で使用されている方法は、テスト目的の参照用として使用できます。

この例では、プレイブックの例が正常に実行された後、インターフェイスのIPアドレス、マスク、およびインターフェイス名がFTDに更新されます。

設定

ネットワーク図



コンフィギュレーション

シスコはサンプルスクリプトまたはお客様が作成したスクリプトをサポートしていないため、お客様のニーズに応じてテストできる例がいくつかあります。

予備検証が正常に完了したことを確認することが不可欠です。

- Ansibleサーバはインターネット接続を備えています。
- Ansibleサーバは、FMC GUIポート (FMC GUIのデフォルトポートは443) と正常に通信できます。
- FTDがFMCに正常に登録されます。

ステップ 1 : SSHまたはコンソールを使用してAnsibleサーバのCLIに接続します。

ステップ 2 : コマンド `ansible-galaxy collection install cisco.fmcansible` を実行して、AnsibleサーバにFMCのAnsibleコレクションをインストールします。

```
<#root>
```

```
cisco@inserthostname-here:~$
```

```
ansible-galaxy collection install cisco.fmcansible
```

ステップ 3 : `mkdir /home/cisco/fmc_ansible` コマンドを実行して、関連ファイルを保存する新しいフォルダを作成します。この例では、ホームディレクトリは `/home/cisco/` で、新しいフォルダ名は `fmc_ansible` です。

```
<#root>
```

```
cisco@inserthostname-here:~$
```

```
mkdir /home/cisco/fmc_ansible
```

ステップ 4 : `/home/cisco/fmc_ansible` フォルダに移動し、インベントリファイルを作成します。この例では、インベントリファイルの名前は `inventory.ini` です。

```
<#root>
```

```
cisco@inserthostname-here:~$
```

```
cd /home/cisco/fmc_ansible/
```

```
ccisco@inserthostname-here:~/fmc_ansible$
```

```
ls
```

```
inventory.ini
```

このコンテンツを複製して使用目的で貼り付け、正確なパラメータを使用して強調表示されたセクションを変更できます。

```
<#root>
```

```
[fmc]
```

```
10.0.5.11
```

```
[fmc:vars]
```

```
ansible_user=
```

```
cisco
```

```
ansible_password=
```

```
cisco
```

```
ansible_httpapi_port=443
```

```
ansible_httpapi_use_ssl=True
```

```
ansible_httpapi_validate_certs=False
```

```
network_type=HOST
```

```
ansible_network_os=cisco.fmcansible.fmc
```

ステップ 5 : /home/cisco/fmc_ansibleフォルダに移動し、変数ファイルを作成します。この例では、変数のファイル名はfmc-configure-interface-vars.ymlです。

```
<#root>
```

```
cisco@inserthostname-here:~$
```

```
cd /home/cisco/fmc_ansible/
```

```
ccisco@inserthostname-here:~/fmc_ansible$
```

```
ls
```

```
fmc-configure-interface-vars.yml
```

```
inventory.ini
```

この内容を複製して利用できるように貼り付け、正確なパラメータで強調表示されたセクションを変更できます。

```
<#root>
```

```
user: domain: 'Global' onboard: acp_name: 'TEMPACP' device_name: ftd1: 'FTDA' ftd_data: outside_name: '
```

```
Outside
```

```
' inside_name: '  
Inside  
' dmz_name: '  
DMZ  
' outside_ip: '  
10.1.1.1  
' inside_ip: '  
10.1.2.1  
' dmz_ip: '  
10.1.3.1  
' mask24: '  
255.255.255.0  
,
```

ステップ6:/home/cisco/fmc_ansibleフォルダに移動し、プレイブックファイルを作成します。この例では、プレイブックのファイル名はfmc-configure-interface-playbook.yamlです。

<#root>

```
cisco@inserthostname-here:~$
```

```
cd /home/cisco/fmc_ansible/
```

```
ccisco@inserthostname-here:~/fmc_ansible$
```

```
ls
```

```
fmc-configure-interface-playbook.yaml
```

```
fmc-configure-interface-vars.yml inventory.ini
```

このコンテンツを複製して使用目的で貼り付け、正確なパラメータを使用して強調表示されたセクションを変更できます。

<#root>

```
--- - name: Update FTD Interface IP Address hosts: fmc connection: httpapi tasks: - name: Task01 - Get User Domain cisco.fmcansible.fmc_configuration
```

```
user.domain
```

```
}}" register_as: domain - name: Task02 - Get Devices cisco.fmcansible.fmc_configuration: operation: get
```

```
device_name.ftd1
```

```
}}" register_as: device_list - name: Task03 - Get Physical Interfaces cisco.fmcansible.fmc_configuration
```

ftd_data.outside_name

}}" ipv4: static: address: "{{ Outside_ip | default(

ftd_data.outside_ip

) }}" netmask: "{{ Outside_netmask | default(

ftd_data.mask24

) }}" MTU: 1500 enabled: True mode: NONE type: physicalinterface name:

GigabitEthernet0/0

path_params: domainUUID: '{{ domain[0].uuid }}' containerUUID: '{{ device_list[0].id }}' objectId: '{{

ftd_data.inside_name

}}" ipv4: static: address: "{{ Inside_ip | default(

ftd_data.inside_ip

}}" netmask: "{{ Inside_netmask | default(

ftd_data.mask24

) }}" MTU: 1500 enabled: True mode: NONE type: physicalinterface name:

GigabitEthernet0/1

path_params: domainUUID: '{{ domain[0].uuid }}' containerUUID: '{{ device_list[0].id }}' objectId: '{{

ftd_data.dmz_name

}}" ipv4: static: address: "{{ DMZ_ip | default(

ftd_data.dmz_ip

) }}" netmask: "{{ DMZ_netmask | default(

ftd_data.mask24

) }}" MTU: 1500 enabled: True mode: NONE type: physicalinterface name:

GigabitEthernet0/2

path_params: domainUUID: '{{ domain[0].uuid }}' containerUUID: '{{ device_list[0].id }}' objectId: '{{

注：このプレイブック例で強調表示されている名前は、変数として機能します。これらの変数に対応する値は、変数ファイル内に保存されます。

手順 7： `/home/cisco/fmc_ansible` フォルダに移動し、ansibleタスクを再生する `ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yaml"` ためにコマンドを実行します。

この例では、コマンドは `ansible-playbook -i inventory.ini fmc-configure-interface-playbook.yaml -e@"fmc-configure-interface-vars.yaml"` です。

<#root>

cisco@inserthostname-here:~\$

```
cd /home/cisco/fmc_ansible/
```

```
cisco@inserthostname-here:~/fmc_ansible$
```

```
ls
```

```
fmc-configure-interface-playbook.yaml fmc-configure-interface-vars.yaml inventory.ini
```

```
cisco@inserthostname-here:~/fmc_ansible$
```

```
ansible-playbook -i inventory.ini fmc-configure-interface-playbook.yaml -e@"fmc-configure-interface-vars"
```

```
PLAY [Update FTD Interface IP Address] *****
```

```
TASK [Gathering Facts] *****  
ok: [10.0.5.11]
```

```
TASK [Task01 - Get User Domain] *****  
ok: [10.0.5.11]
```

```
TASK [Task02 - Get Devices] *****  
ok: [10.0.5.11]
```

```
TASK [Task03 - Get Physical Interfaces] *****  
ok: [10.0.5.11]
```

```
TASK [Task04 - Setup Outside Interface with static IP] *****  
changed: [10.0.5.11]
```

```
TASK [Task05 - Setup Inside Interface with static IP] *****  
changed: [10.0.5.11]
```

```
TASK [Task06 - Setup DMZ Interface with static] *****  
changed: [10.0.5.11]
```

```
TASK [Task07 - Get Deployable Devices] *****  
ok: [10.0.5.11]
```

```
TASK [Task08 - Start Deployment] *****  
changed: [10.0.5.11]
```

```
TASK [Wait for Deployment Complete] *****  
ok: [10.0.5.11]
```

```
TASK [Task09 - Poll Deployment Status Until Deployment Successful] *****  
ok: [10.0.5.11]
```

```
TASK [Task10 - Stop The Playbook If The Deployment Failed] *****  
skipping: [10.0.5.11]
```

```
PLAY RECAP *****  
10.0.5.11 : ok=11 changed=4 unreachable=0 failed=0 skipped=1 rescued=0 ignored=0
```

確認

このセクションでは、設定が正常に動作していることを確認します。

SSHまたはコンソールを使用してFTDのCLIに接続し、show interface ip briefコマンドとshow running-config interface GigabitEthernet 0/Xコマンドを実行します。

インターフェイス名、IPアドレス、およびマスクが正常に設定されました。

```
<#root>
```

```
> show interface ip brief
```

```
Interface IP-Address OK? Method Status Protocol
```

```
GigabitEthernet0/0 10.1.1.1
```

```
YES manual
```

```
up up
```

```
GigabitEthernet0/1 10.1.2.1
```

```
YES manual
```

```
up up
```

```
GigabitEthernet0/2 10.1.3.1
```

```
YES manual
```

```
up up
```

```
>
```

```
show running-config interface GigabitEthernet 0/0
```

```
!  
interface GigabitEthernet0/0  
nameif
```

```
Outside
```

```
cts manual  
propagate sgt preserve-untag  
policy static sgt disabled trusted  
security-level 0
```

```
ip address 10.1.1.1 255.255.255.0
```

```
>
```

```
show running-config interface GigabitEthernet 0/1
```

```
!
```

```
interface GigabitEthernet0/1
nameif

Inside

cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0

ip address 10.1.2.1 255.255.255.0
```

>

```
show running-config interface GigabitEthernet 0/2
```

```
!
interface GigabitEthernet0/2
nameif

DMZ
```

```
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0

ip address 10.1.3.1 255.255.255.0
```

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。

Ansible Playbookのログをさらに表示するには、`-vvv`を使用してAnsible Playbookを実行します

```
cisco@inserthostname-here:~/fmc_ansible$ ansible-playbook -i inventory.ini fmc-configure-interface-playbook.yaml -e@"fmc-configure-interface-vars.yml"
```

関連情報

[Cisco Devnet FMCアンサブル](#)

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。