使用Ansible配置FMC以更新FTD接口IP

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 网络图
- 配置

验证

故障排除

相关信息

简介

本文档介绍自动运行Firepower管理中心(FMC)以使用Ansible配置Firepower威胁防御(FTD)接口IP的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- Ansible
- Ubuntu服务器
- Cisco Firepower管理中心(FMC)虚拟
- Cisco Firepower威胁防御(FTD)虚拟

在这种实验室情况下，Ansible被部署在Ubuntu上。

必须确保Ansible成功安装在Ansible支持的任何平台上，才能运行本文中引用的Ansible命令。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Ubuntu服务器22.04
- Ansible 2.10.8
- Python 3.10
- 思科Firepower威胁防御虚拟7.4.1

- 思科Firepower管理中心虚拟7.4.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

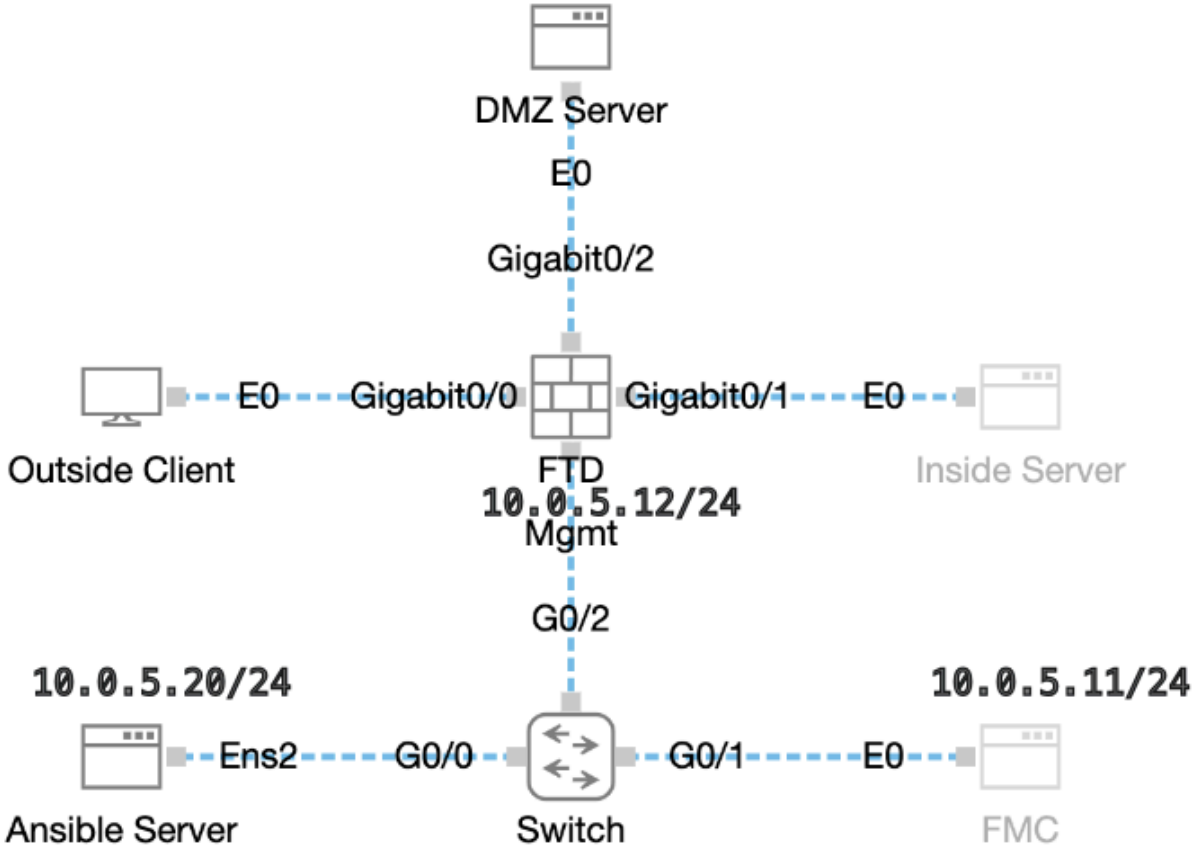
背景信息

Ansible是一个功能非常全面的工具，在管理网络设备时显示了显著的功效。通过Ansible，可以采用多种方法运行自动化任务。本文所采用的方法为试验提供了参考。

在本示例中，成功运行攻略示例后，接口IP地址、掩码和接口名称更新为FTD。

配置

网络图



拓扑

配置

由于思科不支持示例脚本或客户编写的脚本，我们提供了一些您可以根据需要进行测试的示例。

必须确保适当完成初步核查。

- Ansible服务器具有Internet连接。

- Ansible服务器能够与FMC GUI端口成功通信（FMC GUI的默认端口为443）。
- FTD已成功注册到FMC。

步骤1: 通过SSH或控制台连接到Ansible服务器的CLI。

第二步：运行命令ansible-galaxy collection install cisco.fmcansible以在Ansible服务器上安装FMC的Ansible集合。

<#root>

cisco@inserthostname-here:~$

ansible-galaxy collection install cisco.fmcansible

第三步：运行命令mkdir /home/cisco/fmc_ansible以创建一个新文件夹来存储相关文件。在本示例中，主目录为/home/cisco/，新文件夹名称为fmc_ansible。

<#root>

cisco@inserthostname-here:~$

mkdir /home/cisco/fmc_ansible

第四步： 导航到文件夹**/home/cisco/fmc_ansible**，创建资产文件。在本示例中，资产文件名为inventory.ini。

<#root>

cisco@inserthostname-here:~$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible$

ls

inventory.ini

您可以复制此内容并粘贴以供使用，使用准确的参数更改**突出**显示的部分。

<#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
```

第五步： 导航到文件夹**/home/cisco/fmc_ansible**，创建变量文件。在本示例中，变量文件名为fmc-configure-interface-vars.yml。

<#root>

cisco@inserthostname-here:~$

cd /home/cisco/fmc_ansible/

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

ls

fmc-configure-interface-vars.yml

```
inventory.ini
```

您可以复制此内容并粘贴以供使用，从而使用准确的参数更改**突出**显示的部分。

<#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

'

第6步：导航到文件夹**/home/cisco/fmc_ansible**，创建攻略文件。在本示例中，手册文件名为fmc-configure-interface-playbook.yaml。

<#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

您可以复制此内容并粘贴它以供使用，并使用准确参数更改**突出**显示的部分。

<#root>

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

user.domain

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

device_name.ftd1

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

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

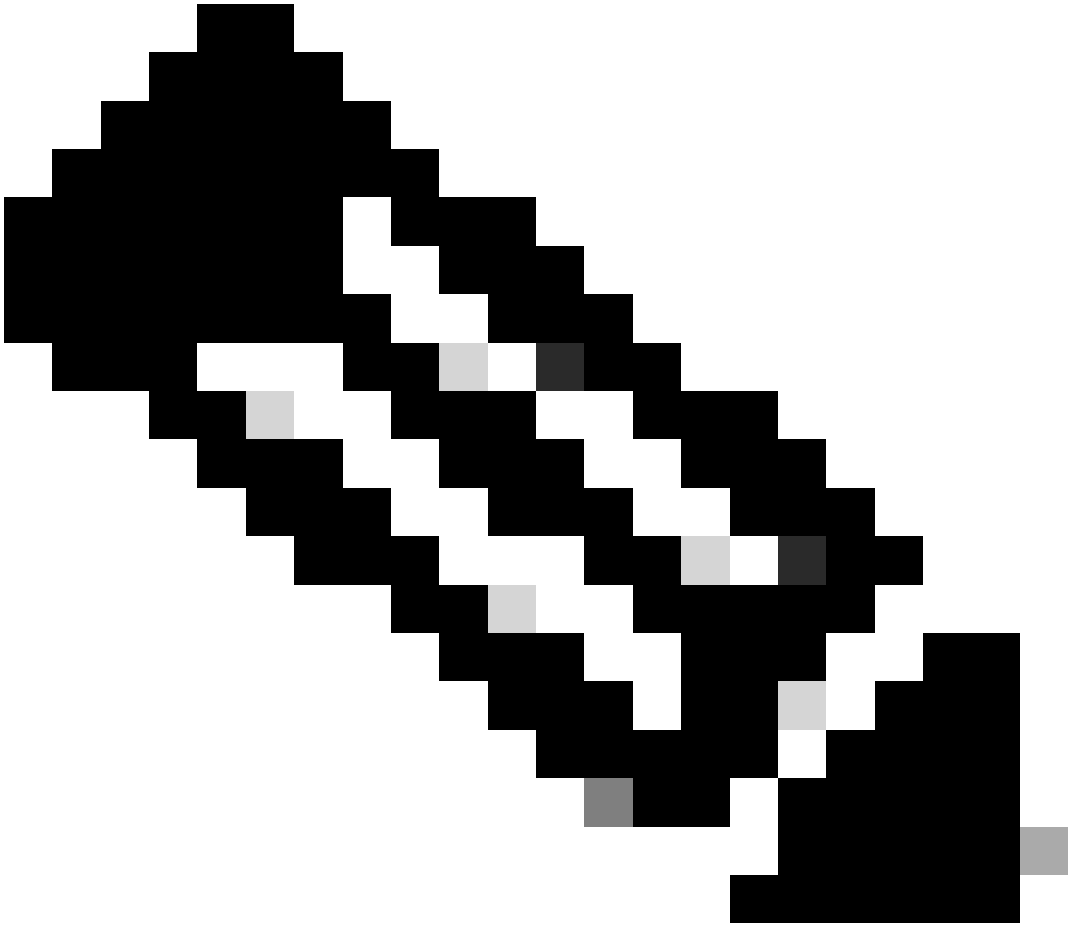
) }}" netmask: "{{ DMZ_netmask | default(

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: '{{



注意：本示例手册中突出显示的名称用作变量。这些变量的对应值保留在变量文件中。

步骤 7. 导航到文件夹**/home/cisco/fmc_ansible**，run commandansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"以播放ansible任务。

在本示例中，该命令是ansible-playbook -i inventory.ini fmc-configure-interface-playbook.yaml -e@"fmc-configure-interface-vars.yml"。

<#root>

cisco@inserthostname-here:~$

cd /home/cisco/fmc_ansible/

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

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

验证

使用本部分可确认配置能否正常运行。

通过SSH或控制台连接到FTD的CLI，并运行命令show interface ip brief和show running-config interface GigabitEthernet 0/X。

接口名称、IP地址和掩码配置成功。

<#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
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

要查看更多ansible攻略日志，您可以使用-vvv运行ansible攻略

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

相关信息

Cisco Devnet FMC Ansible

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。