

Configuración de FMC con Ansible para actualizar la IP de la interfaz FTD

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe los pasos para automatizar Firepower Management Center (FMC) para configurar la IP de interfaz de Firepower Threat Defense (FTD) con Ansible.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Ansible
- Servidor Ubuntu
- Cisco Firepower Management Center (FMC) virtual
- Cisco Firepower Threat Defense (FTD) Virtual

En el contexto de esta situación de laboratorio, Ansible está desplegado en Ubuntu.

Es esencial asegurarse de que Ansible se instale correctamente en cualquier plataforma compatible con Ansible para ejecutar los comandos Ansible a los que se hace referencia en este artículo.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Servidor Ubuntu 22.04
- Ansible 2.10.8
- Python 3.10
- Cisco Firepower Threat Defense Virtual 7.4.1
- Cisco Firepower Management Center Virtual 7.4.1

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

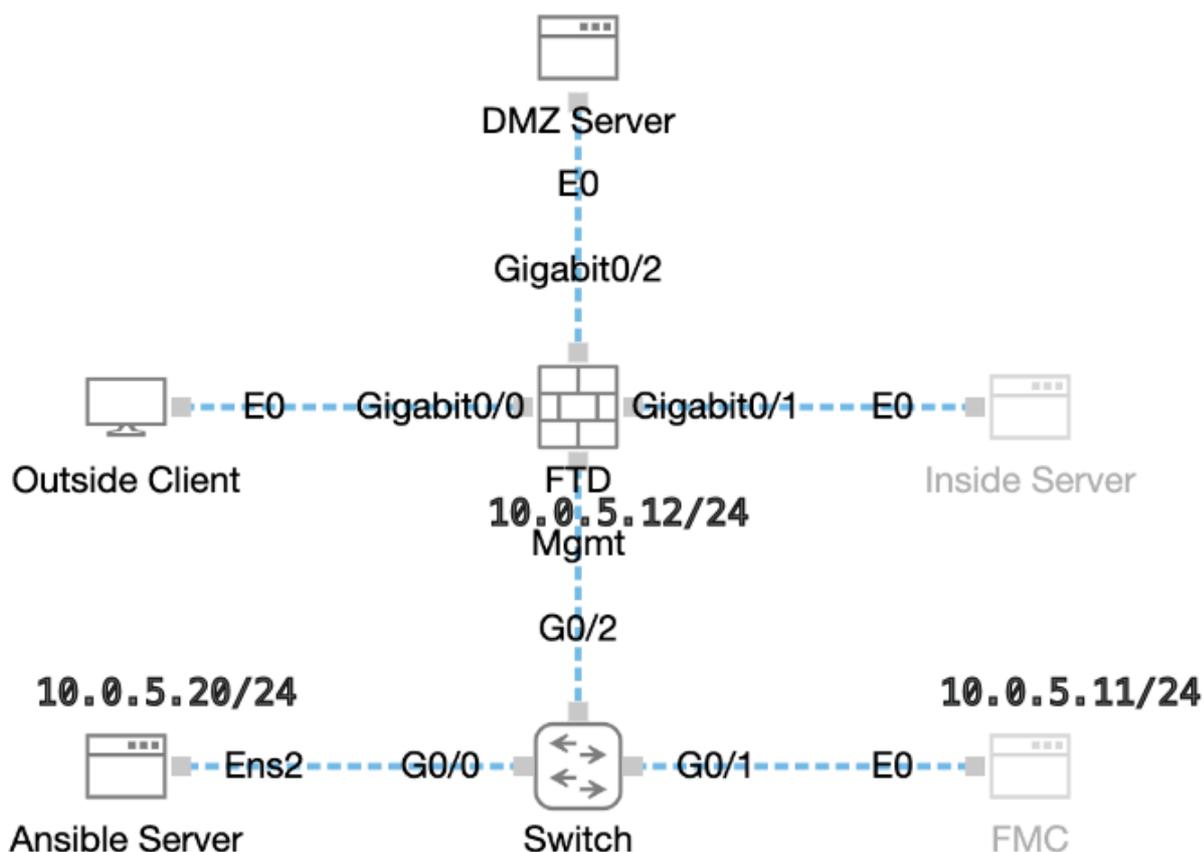
Antecedentes

Ansible es una herramienta muy versátil que demuestra una eficacia significativa en la gestión de dispositivos de red. Se pueden emplear numerosas metodologías para ejecutar tareas automatizadas con Ansible. El método empleado en este artículo sirve de referencia a efectos de ensayo.

En este ejemplo, la dirección IP de la interfaz, la máscara y el nombre de la interfaz se actualizan a FTD después de ejecutar correctamente el ejemplo del cuaderno de campaña.

Configurar

Diagrama de la red



Configuraciones

Como Cisco no admite scripts de ejemplo ni scripts escritos por el cliente, tenemos algunos ejemplos que puede probar según sus necesidades.

Es esencial garantizar que la verificación preliminar se ha completado debidamente.

- El servidor Ansible posee conectividad a Internet.
- El servidor Ansible puede comunicarse correctamente con el puerto GUI de FMC (el puerto predeterminado para la GUI de FMC es 443).
- El FTD se ha registrado correctamente en el FMC.

Paso 1. Conéctese a la CLI del servidor Ansible mediante SSH o la consola.

Paso 2. Ejecute `ansible-galaxy collection install cisco.fmcansible` el comando para instalar la colección Ansible de FMC en su servidor Ansible.

```
<#root>
```

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

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

Paso 3. Ejecute `mkdir /home/cisco/fmc_ansible` el comando para crear una nueva carpeta para almacenar los archivos relacionados. En este ejemplo, el directorio principal es `/home/cisco/`, el nuevo nombre de carpeta es `fmc_ansible`.

```
<#root>
```

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

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

Paso 4. Navegue hasta la carpeta `/home/cisco/fmc_ansible`, crear archivo de inventario. En este ejemplo, el nombre del archivo de inventario es `Inventory.ini`.

```
<#root>
```

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

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

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

```
ls
```

```
inventory.ini
```

Puede duplicar este contenido y pegarlo para su uso, alterando las secciones **resaltadas** con los parámetros precisos.

```
<#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
```

Paso 5. Vaya a la carpeta **/home/cisco/fmc_ansible**, create variable file. En este ejemplo, el nombre de archivo de la variable es **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
```

Puede duplicar este contenido y pegarlo para su utilización, alterando las secciones **resaltadas** con los parámetros precisos.

```
<#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
```

```
'
```

Paso 6. Navegue hasta la carpeta **/home/cisco/fmc_ansible**, cree el archivo del cuaderno. En este ejemplo, el nombre del archivo del cuaderno es `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
```

Puede duplicar este contenido y pegarlo para su uso, alterando las secciones **resaltadas** con los parámetros precisos.

```
<#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

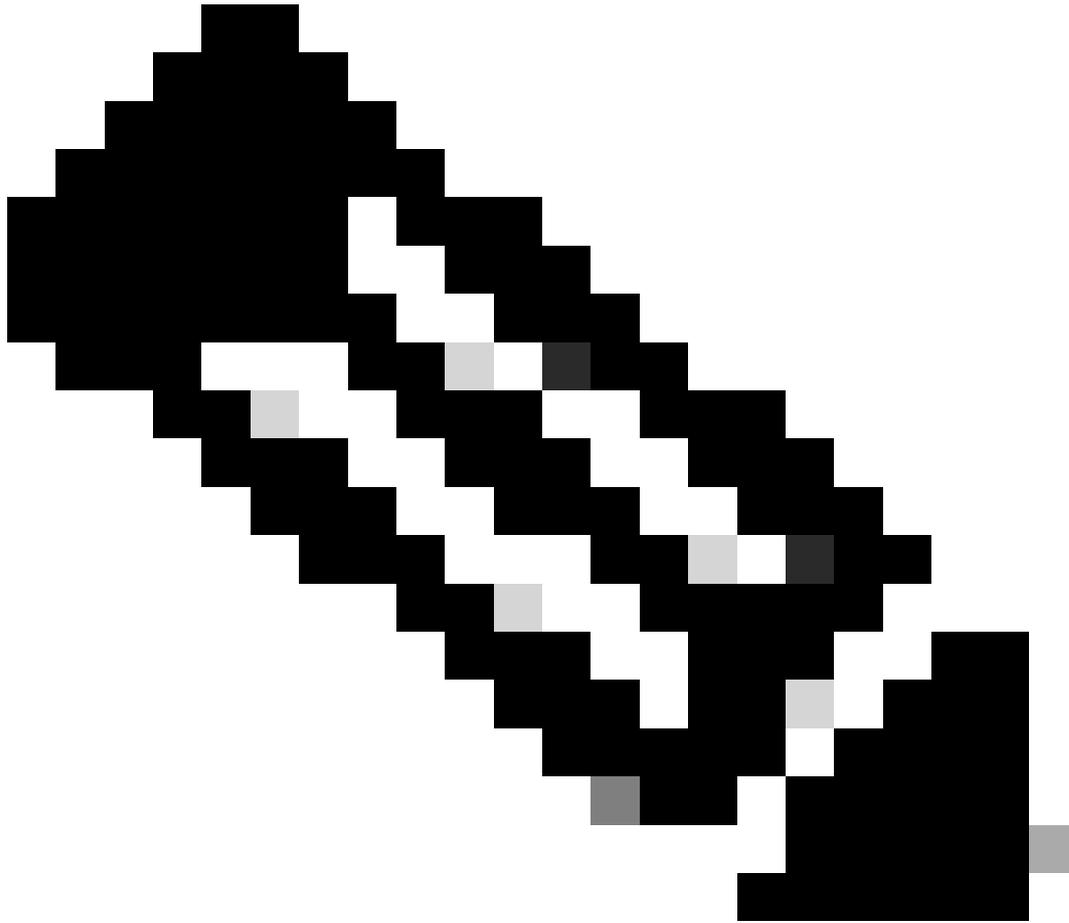
```
) }}" netmask: "{{ DMZ_netmask | default(
```

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: '{{
```



Nota: Los nombres resaltados en este cuaderno de campaña de ejemplo sirven como variables. Los valores correspondientes de estas variables se conservan en el archivo de variables.

Paso 7. Navegue hasta la carpeta **/home/cisco/fmc_ansible**, ejecute el comando `ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yaml"` para reproducir la tarea ansible.

En este ejemplo, el comando es `ansible-playbook -i inventory.ini fmc-configure-interface-playbook.yaml -e@"fmc-configure-interface-vars.yaml"` .

<#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
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Conéctese a la CLI del FTD a través de SSH o de la consola y ejecute los comandos `show interface ip brief` y `show running-config interface GigabitEthernet 0/X`.

El nombre de la interfaz, la dirección IP y la máscara se han configurado correctamente.

```
<#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
```

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Para ver más registros del cuaderno de campaña de Ansible, puede ejecutar el cuaderno de campaña de Ansible con -vv

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

Información Relacionada

[Cisco Devnet FMC Ansible](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).