Configure Management Access for SSH and HTTPS on FTD via FDM

Contents

Introduction

This document describes the procedure to configure and verify the management access-list for SSH and HTTPS on FTD managed locally or remote.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

- Cisco Secure Firewall Threat Defense running version 7.4.1 managed by FDM.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

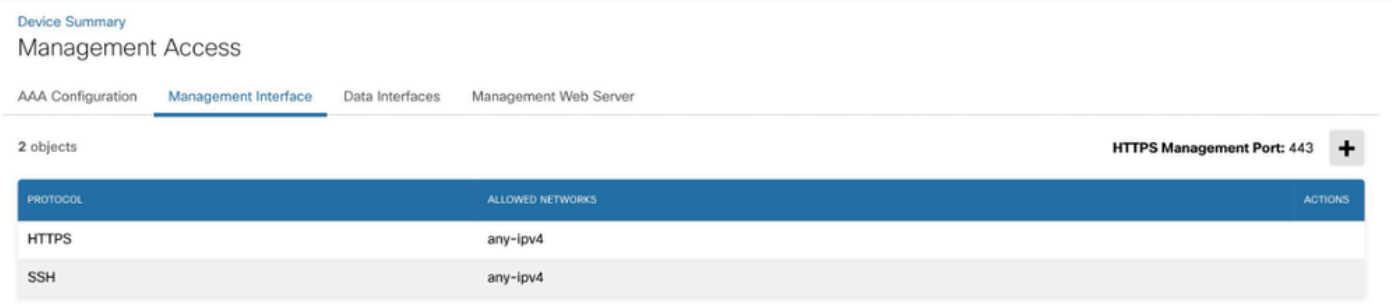
Configure

FTD can be managed locally using FDM or via FMC. In this document, the focus is on management access via FDM and CLI. Using CLI you can make changes for both scenario FDM and FMC.

Caution: Configure SSH or HTTPS access lists one at a time to avoid session lockout. First, update and deploy one protocol, verify access, then proceed with the other.

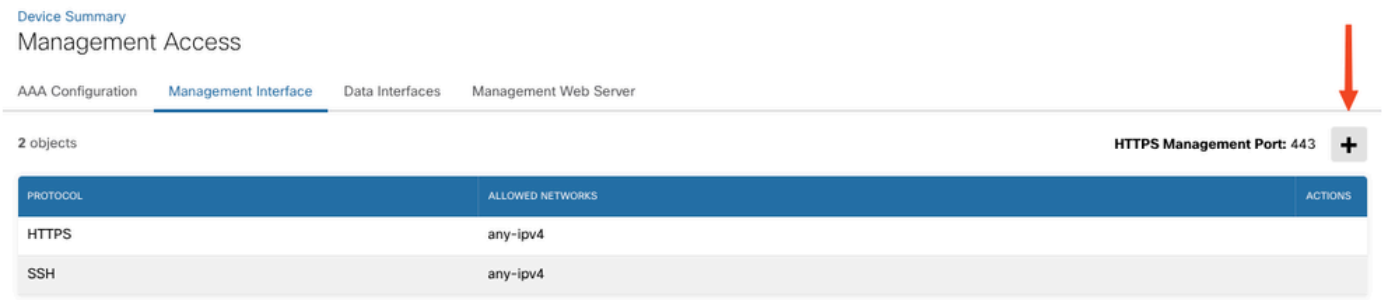
FDM Steps:

Step 1: Log in to the Firepower Device Manager (FDM) and navigate to **System Settings > Management Access > Management Interface** .



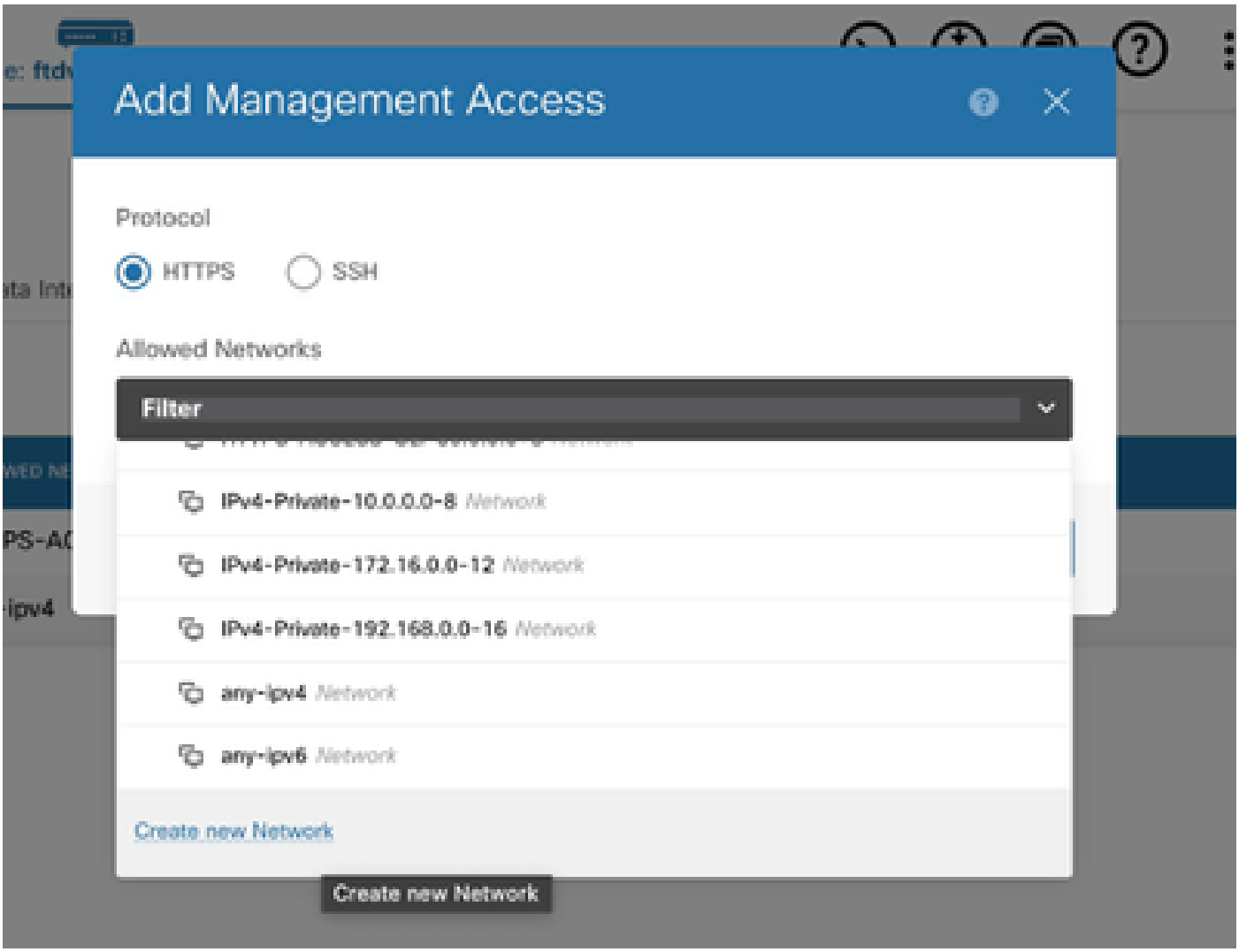
By default, any-ipv4 access is allowed on management port for SSH and HTTPS

Step 2: Click the + icon to open the window for adding the network.



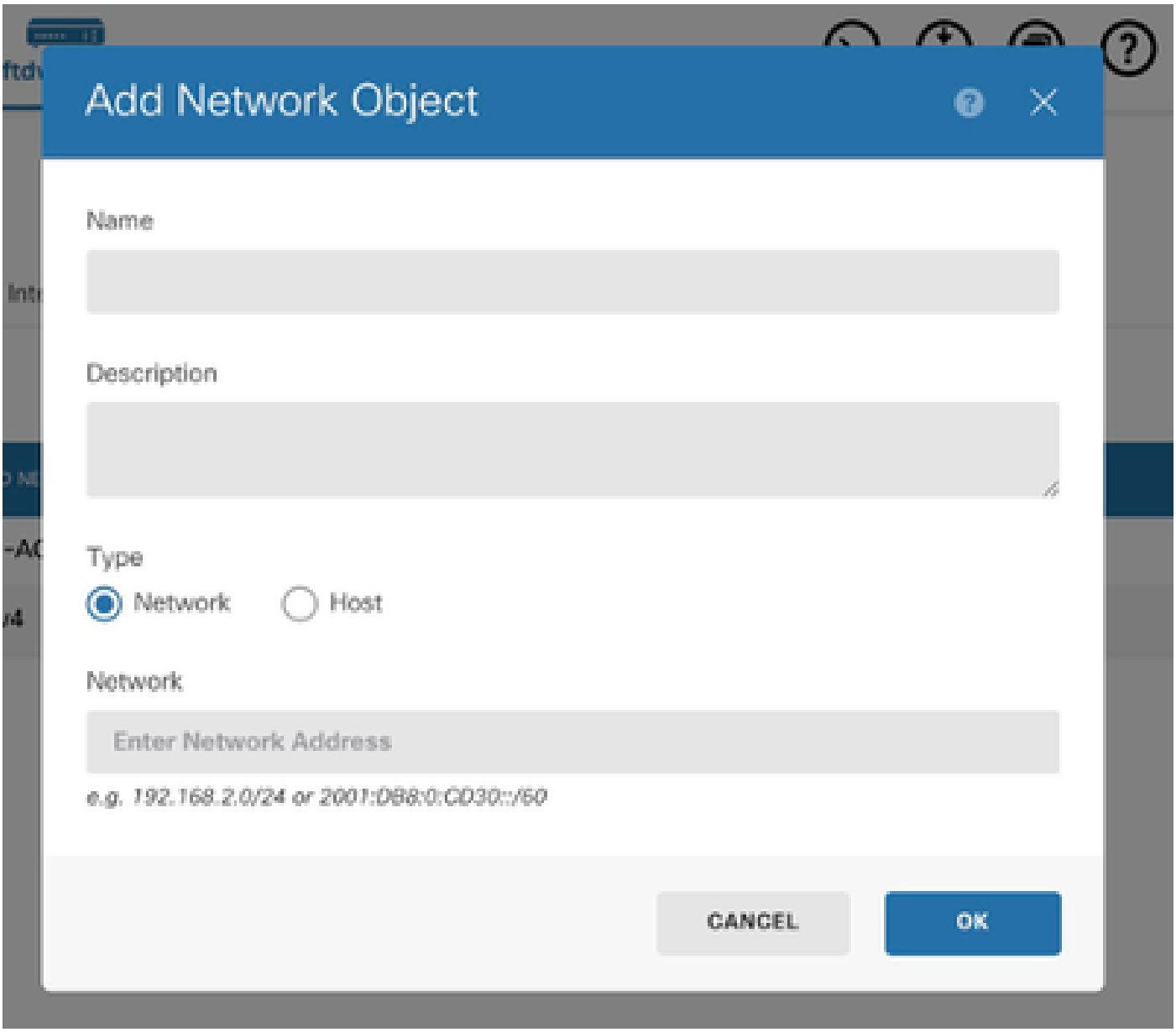
Click the Add button from top right.

Step 3: Add the network object to have SSH or HTTPS access. If you need to create a new network, select the **Create new Network** option. You can add multiple entries for networks or host in the management access.



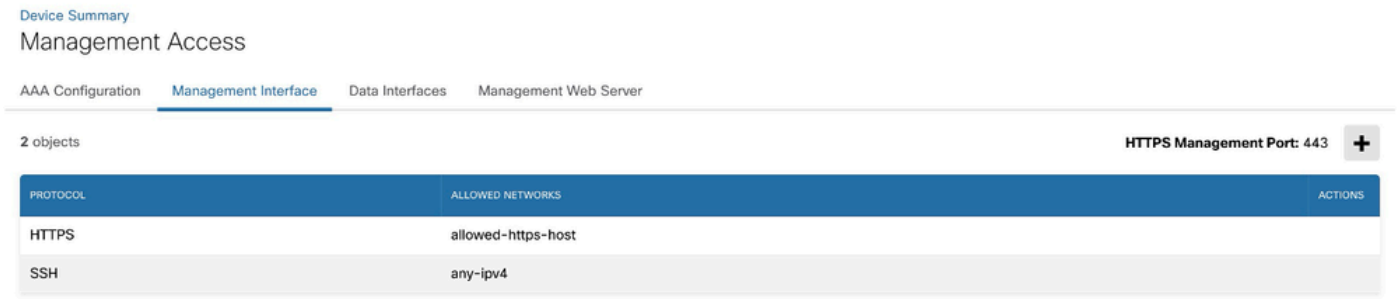
Select the network.

Step 4 (Optional): Create new Network option opens up **Add Network Object** window.

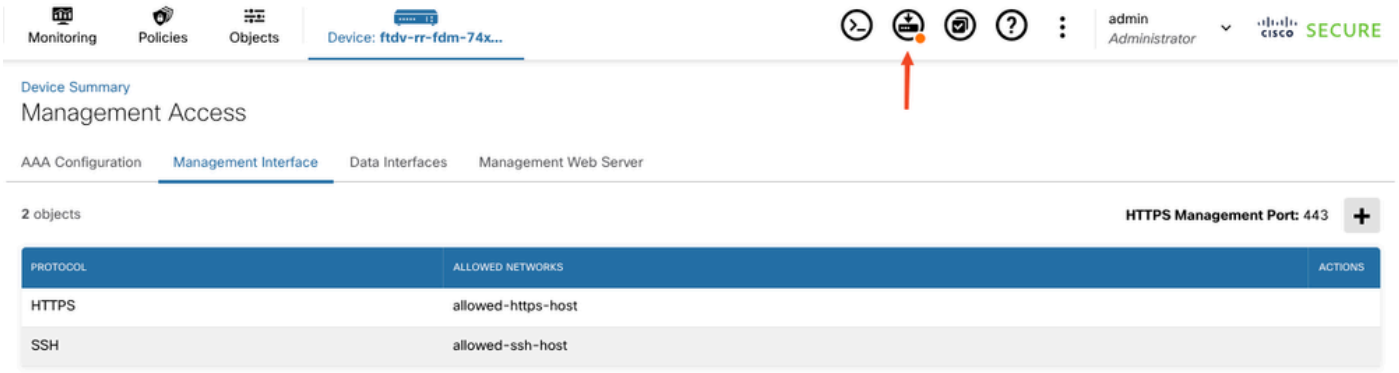


Create a network of host as per your requirement.

Step 5: Verify the changes made and **Deploy**.

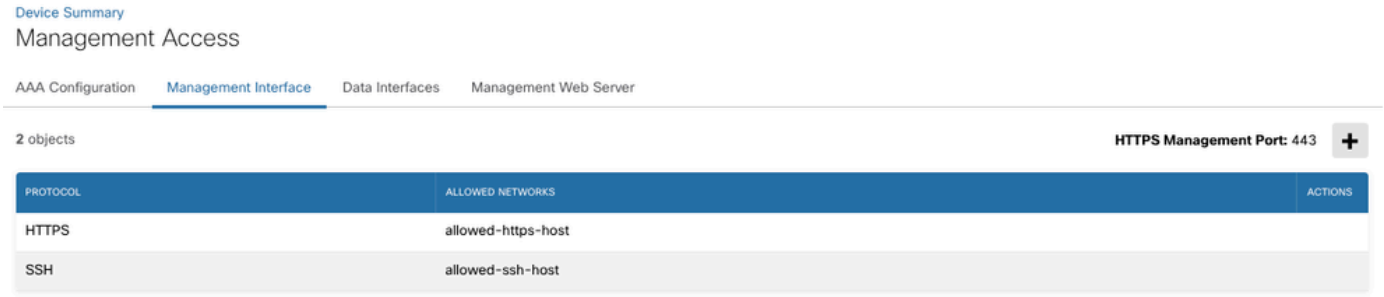


HTTPS management access changed and any-ipv4 is removed.



Deploy on FDM

Step 6 (Optional): Once previous made changes for HTTPS are verified, repeat the same for SSH.



Added network object for SSH and HTTPS.

Step 7 : Finally deploy the changes and verify your access to the FTD from the allowed network and host.

CLISH Steps:

CLI steps can be used in case of both FDM or FMC managed.

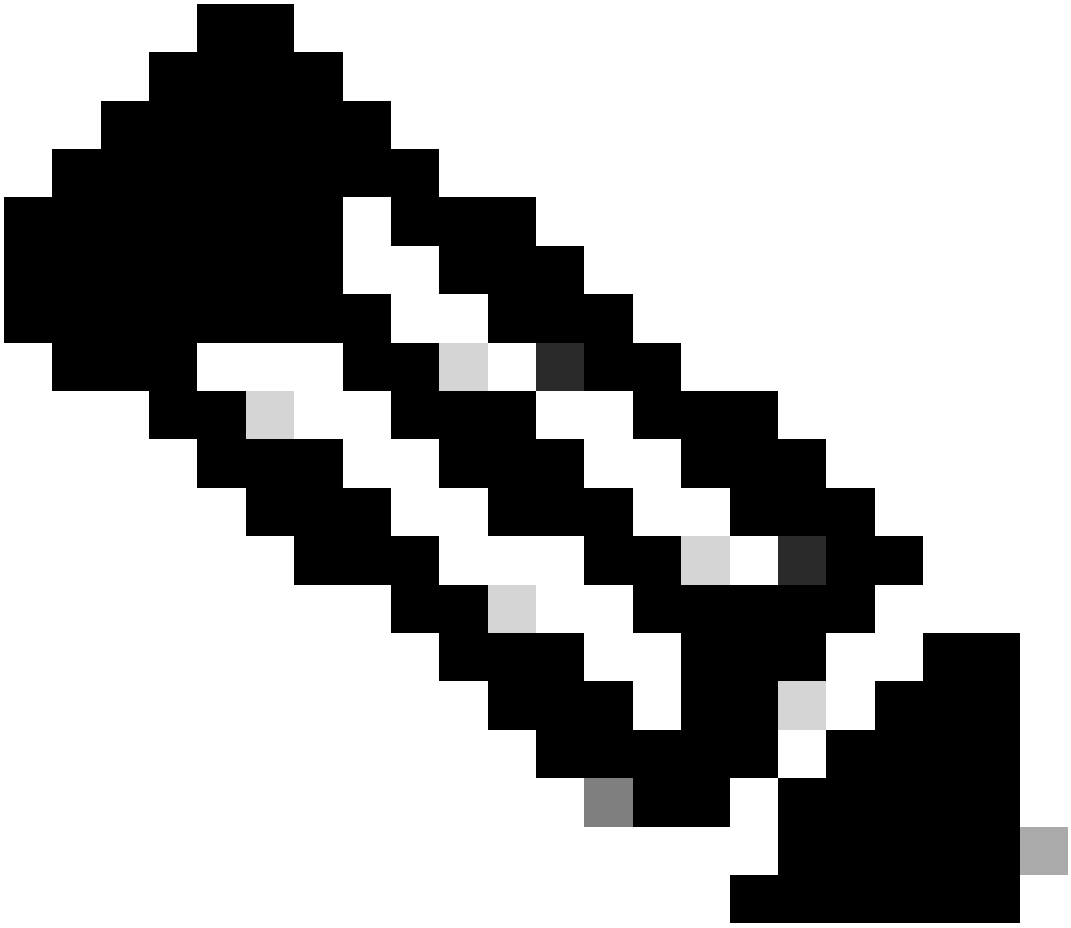
To configure the device to accept HTTPS or SSH connections from specified IP addresses or network, use the`configure https-access-list`or`configure ssh-access-list`command.

- You must include all supported hosts or networks in a single command. Addresses specified in this command overwrite the current contents of the respective access list..
- If the device is a unit in a locally-managed high availability group, your change overwrites the next time the active unit deploys configuration updates. If this is the active unit, the change propagates to the peer during deployment.

```
> configure https-access-list x.x.x.x/x,y.y.y.y/y

The https access list was changed successfully.

> show https-access-list
ACCEPT     tcp  --  x.x.x.x/x            anywhere             state NEW tcp dpt:https
ACCEPT     tcp  --  y.y.y.y/y            anywhere             state NEW tcp dpt:https
```



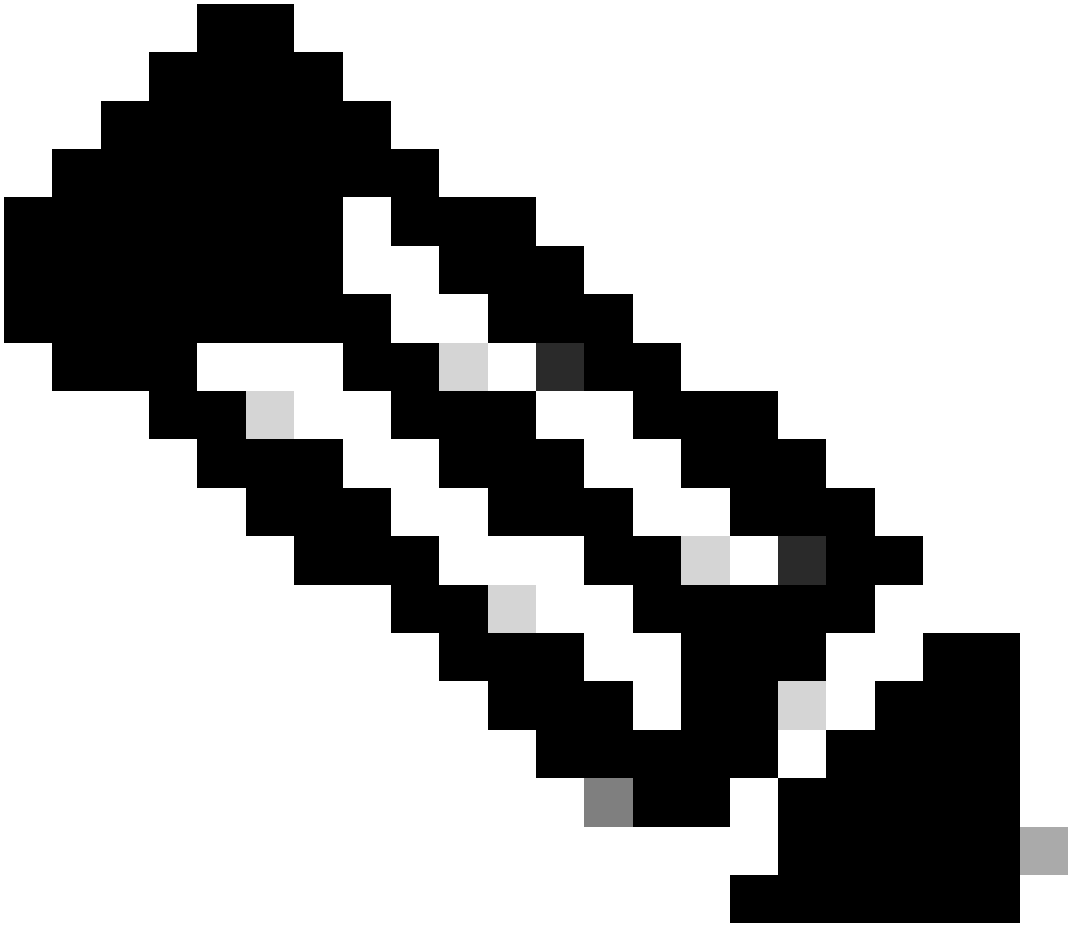
Note: x.x.x.x/x and y.y.y.y/y represents ipv4 address with CIDR notation.

Similarly, for SSH connections use configure ssh-access-listcommand with single or multiple command separated.

```
> configure ssh-access-list x.x.x.x/x

The ssh access list was changed successfully.

> show ssh-access-list
ACCEPT     tcp  --  x.x.x.x/x            anywhere            state NEW tcp dpt:ssh
```



Note: You can use commands **configure disable-https-access** or configure disable-ssh-accessto disable HTTPS or SSH access respectively. Ensure you are aware of these changes as this can lock you out of the session.

Verify

To verify from CLISH you can use commands:

```
> show ssh-access-list
ACCEPT     tcp  --  anywhere            anywhere            state NEW tcp dpt:ssh

> show https-access-list
ACCEPT     tcp  --  anywhere            anywhere            state NEW tcp dpt:https
```

References

Cisco Secure Firewall Threat Defense Command Reference

Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager