



连接并防火墙

- 连接防火墙的电缆，第 1 页
- 执行初始配置，第 1 页

连接防火墙的电缆

执行初始配置

使用 Firepower 设备管理器 或 CLI 来执行行初始配置。

初始配置：设备管理器

使用这种方法，在注册防火墙后，除管理接口外还将预先配置以下接口：

- 以太网 1/1 - **outside**，IP 地址来自 DHCP、IPv6 自动配置
- - **inside**，192.168.95.1/24
- 默认路由 - 通过外部接口上的 DHCP 获取
- 其他接口 - 保留 FDM 中的任何接口配置。

不会保留其他设置，如内部的 DHCP 服务器、访问控制策略或安全区域。

过程

步骤 1 将计算机连接到内部接口。

步骤 2 登录FDM。

- a) 转至<https://192.168.95.1>。
- b) 使用用户名 **admin** 和默认密码 **Admin123** 登录。
- c) 系统会提示您阅读并接受“一般条款”并更改管理员密码。

步骤 3 使用设置向导。**注释**

具体的端口配置取决于您的型号。

a) 配置外部接口和管理接口。

图 1: 将防火墙连接到互联网

Connect firewall to Internet

The initial access control policy will enforce the following actions.
You can edit the policy after setup.

<p>Rule 1 Trust Outbound Traffic</p> <p>This rule allows traffic to go from inside to outside, which is needed for the Smart License configuration.</p>	<p>Default Action Block all other traffic</p> <p>The default action blocks all other traffic.</p>
---	---

Outside Interface Address

Connect Ethernet1/1 (Outside) to your ISP/WAN device, for example, your cable modem or router. Then, configure the addresses for the outside interface.

Configure IPv4

Using DHCP ▼

Configure IPv6

Using DHCP ▼

NEXT

Don't have internet connection?
[Skip device setup](#) ⓘ

1. 外部接口地址 - 如果您计划实现高可用性，请使用静态 IP 地址。您不能使用设置向导配置 PPPoE；您可以在完成向导后配置 PPPoE。

2. 管理接口

DNS 服务器 - 系统管理地址的 DNS 服务器。默认值为 OpenDNS 公共 DNS 服务器。

防火墙主机名

b) 配置时间设置 (NTP) (Time Setting [NTP]) 并点击下一步 (Next)。

图 2: 时间设置 (NTP)

Time Setting (NTP)

System Time: 11:56:20AM October 03 2024 -06:00

Time Zone for Scheduling Tasks

(UTC+00:00) UTC

NTP Time Server

Default NTP Servers

Server Name

0.sourcefire.pool.ntp.org

1.sourcefire.pool.ntp.org

2.sourcefire.pool.ntp.org

NEXT

c) 选择启动 90 日评估期而不注册。

Register with Cisco Smart Software Manager

Register with Cisco Smart Software Manager to use the full functionality of this device and to apply subscription licenses.

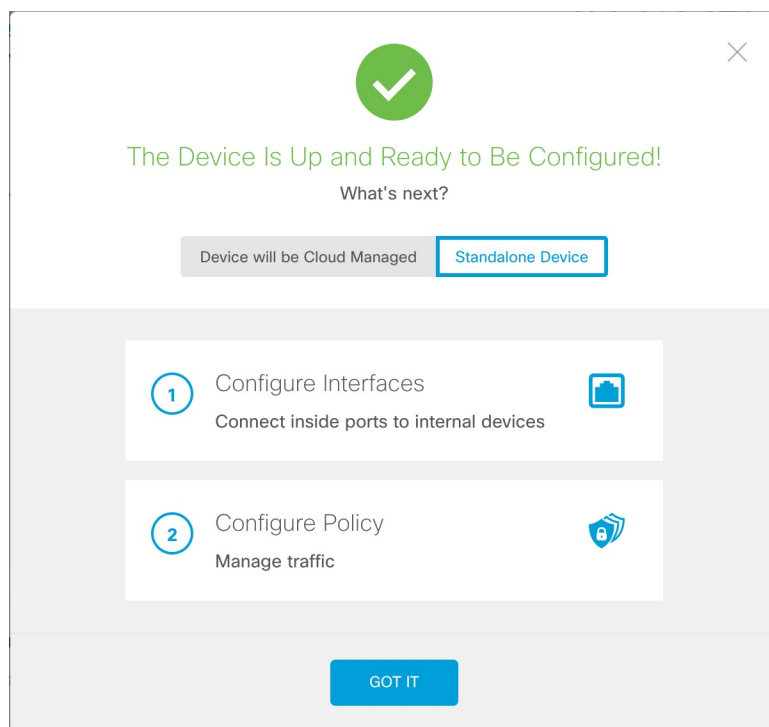
[What is smart license? ↗](#)

☐ **Continue with evaluation period: Start 90-day evaluation period without registration**
Recommended if device will be cloud managed. [Learn More ↗](#)
Please make sure you register with Cisco before the evaluation period ends.
Otherwise you will not be able to make any changes to the device configuration.

不要向智能软件管理器注册 FTD；所有许可均在上执行。

d) 点击完成。

图 3: 后续操作



e) 依次选择独立设备 (**Standalone Device**) 和 明白 (**Got It**)。

步骤 4 如果要配置其他接口，请选择设备 (**Device**)，然后点击接口 (**Interfaces**) 摘要中的链接。

步骤 5 通过选择设备 (**Device**)、> 系统设置 (**System Settings**)、> 集中管理 (**Central Management**) 并点击继续 (**Proceed**)，向注册

配置管理中心/CDO 详细信息。

图 4: 管理中心/CDO 详细信息

Configure Connection to Management Center or CDO

Provide details to register to the management center/CDO.

Management Center/CDO Details

Do you know the Management Center/CDO hostname or IP address?

☒ Yes ☐ No

Threat Defense
10.89.5.16
fe80::6a87:c6ff:fea6:4c00/64


→

Management Center/CDO
10.89.5.35

Management Center/CDO Hostname or IP Address

10.89.5.35

Management Center/CDO Registration Key

●●●● 

NAT ID

Required when the management center/CDO hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/CDO hostname or IP address.

11203

Connectivity Configuration

Threat Defense Hostname

1120-3

DNS Server Group

CustomDNSServerGroup ▼

Management Center/CDO Access Interface

☐ Data Interface

Please select an interface ▼

☒ Management Interface [View details](#)

CANCEL CONNECT

- a) 对于是否知道管理中心/CDO 主机名或 IP 地址，如果您可以使用 IP 地址或主机名访问 FMC，请点击是 (Yes)。

步骤 6 配置连接配置。

- a) 指定威胁防御主机名。

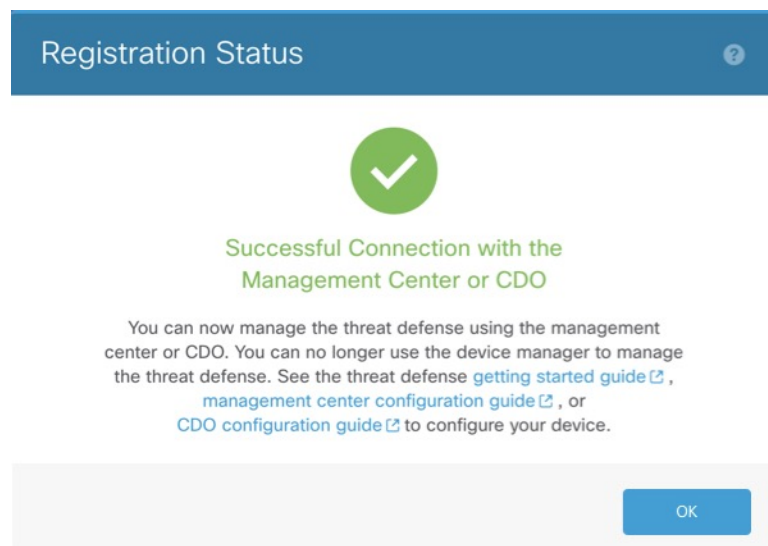
b) 指定 DNS 服务器组。

选择一个现有组，或创建一个新组。默认 DNS 组名为 **CiscoUmbrellaDNSServerGroup**，其中包括 OpenDNS 服务器。

步骤 7 点击连接 (Connect)。

注册状态 (Registration Status) 对话框将显示 注册的当前状态。

图 5: 成功连接



步骤 8 在保存管理中心/CDO 注册设置步骤之后，转到，然后添加防火墙。请参阅。

初始配置: CLI

使用 CLI 设置脚本设置专用管理 IP 地址、网关和其他基本网络设置。

过程

步骤 1 连接控制台端口并访问 FTD CLI。请参阅[访问 CLI](#)。

步骤 2 完成管理界面设置的 CLI 设置脚本。

注释

除非清除配置，否则无法重复 CLI 设置脚本（例如，通过重新建立映像）。但是，可以稍后在 CLI 中使用 **configure network** 命令更改所有这些设置。请参阅 [Cisco Secure Firewall Threat Defense 命令参考](#)。

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
Cisco General Terms
```

[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress. Please stand by.

You must configure the network to continue.

Configure at least one of IPv4 or IPv6 unless managing via data interfaces.

Do you want to configure IPv4? (y/n) [y]:

Do you want to configure IPv6? (y/n) [y]: **n**

指南: 为至少其中一种地址类型输入 **y**。

Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:

Enter an IPv4 address for the management interface [192.168.45.61]: **10.89.5.17**

Enter an IPv4 netmask for the management interface [255.255.255.0]: **255.255.255.192**

Enter a fully qualified hostname for this system [firepower]: **1010-3**

Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220,2620:119:35::35]:

Enter a comma-separated list of search domains or 'none' []: **cisco.com**

If your networking information has changed, you will need to reconnect.

Disabling IPv6 configuration: management0

Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35

Setting DNS domains:cisco.com

Setting hostname as 1010-3

Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0

Updating routing tables, please wait...

All configurations applied to the system. Took 3 Seconds.

Saving a copy of running network configuration to local disk.

For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: **no**

指南: 输入 **no** 以使用 FMC。

Setting hostname as 1010-3

Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0

Updating routing tables, please wait...

All configurations applied to the system. Took 3 Seconds.

Saving a copy of running network configuration to local disk.

For HTTP Proxy configuration, run 'configure network http-proxy'

Configuring firewall mode ...

Device is in OffBox mode - disabling/removing port 443 from iptables.

Update policy deployment information

- add device configuration
- add network discovery
- add system policy

You can register the sensor to a Firepower Management Center and use the Firepower Management Center to manage it. Note that registering the sensor to a Firepower Management Center disables on-sensor Firepower Services management capabilities.

When registering the sensor to a Firepower Management Center, a unique alphanumeric registration key is always required. In most cases, to register a sensor to a Firepower Management Center, you must provide the hostname or the IP address along with the registration key.

'configure manager add [hostname | ip address] [registration key]'

However, if the sensor and the Firepower Management Center are separated by a NAT device, you must enter a unique NAT ID, along with the unique registration

key.

```
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
```

Later, using the web interface on the Firepower Management Center, you must use the same registration key and, if necessary, the same NAT ID when you add this sensor to the Firepower Management Center.

>

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。