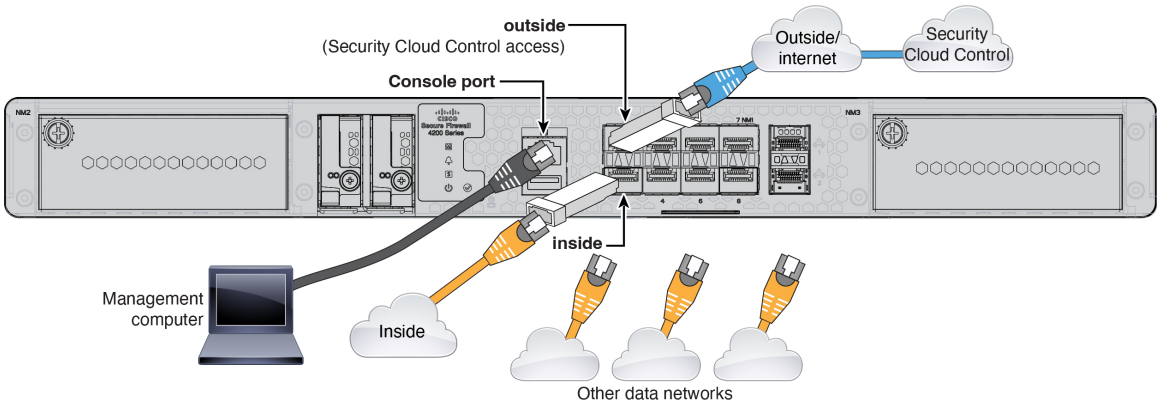
连接并载入防火墙

连接防火墙并载入到安全云控制。

连接防火墙的电缆

- 获取控制台电缆 - 默认情况下，防火墙不随附控制台电缆，因此您需要购买第三方 USB 转 RJ-45 串行电缆。
- 将 SFP 安装到数据接口端口 - 内置端口是需要 1/10/25-Gb SFP28 模块的 1/10/25-Gb SFP28 端口。
- 有关详细信息，请参阅硬件安装指南。



通过手动调配载入防火墙

使用 CLI 注册密钥载入防火墙。

过程

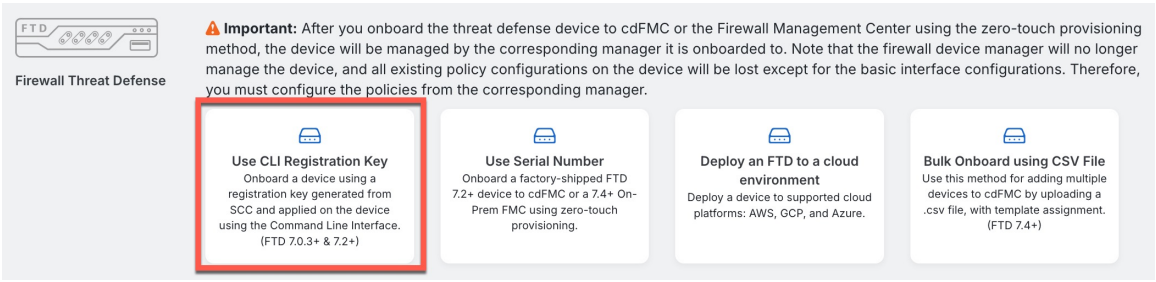
步骤 1 在 安全云控制 导航窗格中，点击 **安全设备 (Security Devices)**，然后点击蓝色加号按钮（  ）以便**载入**设备。

步骤 2 点击 **FTD** 磁贴。

步骤 3 在 **管理模式**下，确保选择 **FTD** 。

步骤 4 选择**使用 CLI 注册密钥 (Use CLI Registration Key)** 作为激活方法。

图 *1:* 使用 *CLI* 注册密钥

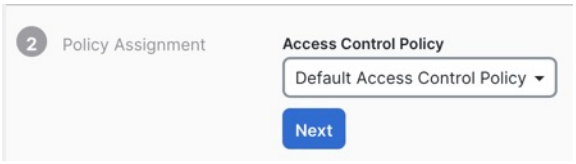


步骤 5 输入**设备名称 (Device Name)**，然后点击**下一步 (Next)**。

图 *2:* 设备名称

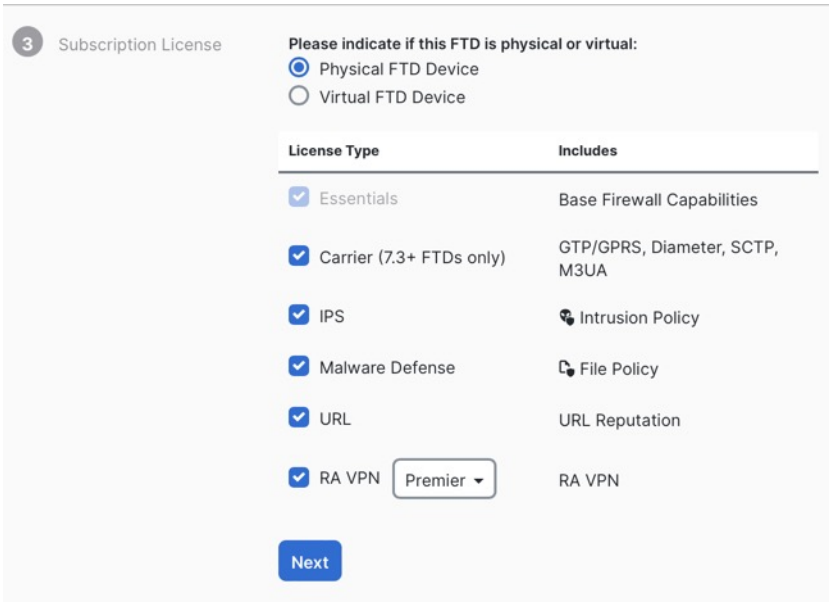
步骤 6 对于**策略分配 (Policy Assignment)**，请使用下拉菜单为设备选择访问控制策略。如果未配置策略，请选择**默认访问控制策略 (Default Access Control Policy)**。

图 *3:* 访问控制策略



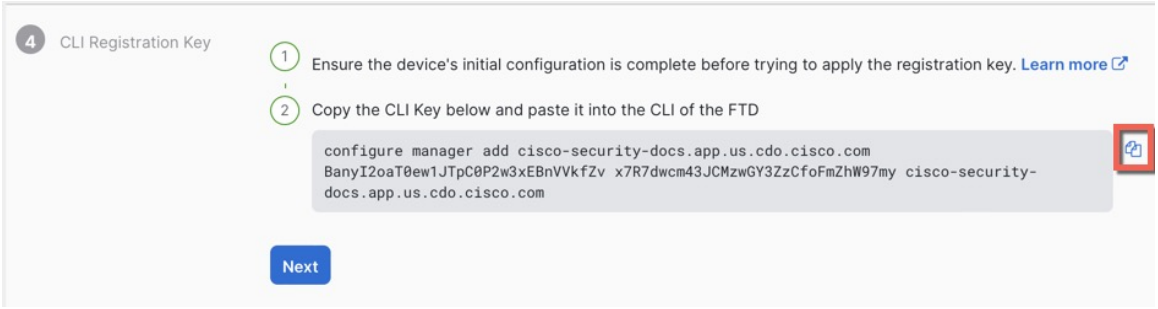
步骤 7 对于**订用许可证 (Subscription License)**，请点击**物理 FTD 设备 (Physical FTD Device)** 单选按钮，然后选中要启用的每个功能许可证。点击**下一步**。

图 *4:* 订用许可证



步骤 8 对于 **CLI 注册密钥**，安全云控制 会使用注册密钥和其他参数来生成命令。您必须复制此命令并在威胁防御的初始配置中使用它。

图 *5: CLI* 注册密钥



configure manager add 安全云控制*_hostname registration_key nat_id display_name*

完成启动脚本后，在 威胁防御 CLI 中复制此命令。请参阅初始配置：CLI，第 4 页。

示例：

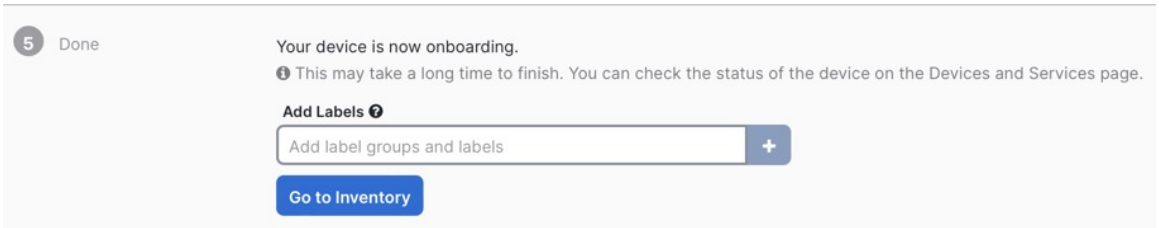
CLI 设置的命令示例：

```
configure manager add account1.app.us.scc.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.scc.cisco.com
```

步骤 9 在激活向导中点击**下一步 (Next)**，以便开始注册设备。

步骤 10 （可选） 向设备添加标签，以帮助对**安全设备 (Security Devices)** 页面进行排序和过滤。输入标签，然后选择蓝色加号按钮（ ）。标签会在设备载入 安全云控制后应用到设备。

图 *6:* 完成



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 威胁防御 CLI。请参阅访问威胁防御 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**。虽然您不打算使用管理接口，但必须设置 IP 地址，例如专用地址。

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

指南：选择**手动**。使用外部接口访问管理器时，不支持DHCP。确保此接口与管理器访问接口位于不同的子网上，以防止出现路由问题。

```
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 the IPv4 default gateway for the management interface [data-interfaces]:
```

指南：将网关设置为 **data-interfaces**。此设置可将管理流量转发到背板上，以便通过外部接口进行路由。

```
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
```

指南：设置管理接口 DNS 服务器。这些服务器很可能与您稍后设置的外部接口 DNS 服务器一致，因为它们都是从外部接口访问的。

```
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'
```

```
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'
```

指南：输入 **routed**。只有路由防火墙模式支持外部管理器访问。

```
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.
>
```

步骤 3 配置用于管理器访问的外部接口。

configure network management-data-interface

然后，系统会提示您为外部接口配置基本网络设置。

手动 IP 地址

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
```

指南：要在注册后保留外部 DNS 服务器，您需要在 管理中心 中重新配置 DNS 平台设置。

```
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to change the manager
 access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

DHCP 的 IP 地址

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://dwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to change the manager
 access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

步骤 4 使用 安全云控制 生成的 **configure manager add** 命令确定将管理此 威胁防御 的 安全云控制。请参阅通过手动调配载入防火墙，第 1 页以生成命令。

示例：

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
```

步骤 5 关闭 威胁防御，以便将设备发送到远程分支机构。

正确关闭系统非常重要。仅拔掉电源或按下电源开关可能会导致文件系统严重损坏。请记住，有许多进程一直在后台运行，拔掉或关闭电源不能正常关闭系统。

a) 输入 **shutdown** 命令。
b) 观察电源 LED 和状态 LED 以验证机箱是否已断电（不亮）。

c) 在机箱成功关闭电源后，您可以在必要时拔下电源插头以物理方式断开机箱的电源。

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。