



使用命令行界面 (CLI)

以下主题介绍如何使用 Cisco Secure Firewall Threat Defense 设备的命令行界面 (CLI) 以及如何解释命令参考主题。使用 CLI 进行基本系统设置和故障排除。



注释 使用 Cisco Secure Firewall Management Center 或 Secure Firewall 设备管理器部署配置更改时，请勿将 threat defense CLI 用于长时间运行的命令（例如具有大量重复计数或大小的 ping）；这些命令可能会导致部署失败。

- [登录命令行界面 \(CLI\)，第 2 页](#)
- [命令模式，第 3 页](#)
- [语法格式，第 5 页](#)
- [输入命令，第 6 页](#)
- [过滤 show 命令输出，第 7 页](#)
- [命令帮助，第 9 页](#)

登录命令行界面 (CLI)

要登录 CLI，使用 SSH 客户端连接到管理 IP 地址。使用 **admin** 用户名（默认密码为 Admin123）或其他 CLI 用户账号登录。

如果您为 SSH 连接打开某个数据接口，您也可以连接到该接口上的地址。默认情况下，禁用 SSH 数据接口访问。要启用 SSH 访问，请使用设备管理器（管理中心 或 设备管理器）允许与特定数据接口的 SSH 连接。您无法通过 SSH 连接到诊断接口。

您可以使用 **configure user add** 命令创建可登录 CLI 的用户账号。但这些用户只能登录 CLI，他们无法登录设备管理器 Web 接口。CLI 仅支持本地身份验证。您无法使用外部身份验证访问 CLI。

Console Port Access

除 SSH，您还可以直接连接到设备上的控制台端口。使用设备随附的控制台电缆将您的 PC 连接到使用终端仿真器的控制台，终端仿真器的设置为 9600 波特率、8 个数据位、无奇偶校验、1 个停止位、无流量控制。有关控制台电缆的详细信息，请参阅设备的硬件指南。

在控制台端口上访问的初始 CLI 因设备类型而异。

- ASA 硬件平台 - 控制台端口上的 CLI 是常规 threat defense CLI。
- 其他硬件平台 - 控制台端口上的 CLI 是常规 Secure Firewall eXtensible 操作系统 (FXOS)。您可以使用 **connect** 命令进入 threat defense CLI。仅将 FXOS CLI 用于机箱级配置和故障排除。对于 Firepower 2100，您无法在 FXOS CLI 上执行任何配置。使用 threat defense CLI 进行基本配置、监控和正常的系统故障排除。有关 Firepower 4100 和 9300 的 FXOS 命令的信息，请参阅 FXOS 文档。请参阅 FXOS 故障排除指南，了解其他型号的 FXOS 命令的信息。

命令模式

threat defense 设备上的 CLI 具有不同的模式，这些模式实际上是单独的 CLI，而不是单个 CLI 的子模式。您可以通过查看命令提示符来判断您所处的模式。

常规 威胁防御 CLI

使用此 CLI 进行 threat defense 管理配置和故障排除。

>

诊断 CLI

使用此 CLI 可进行高级故障排除。此 CLI 包括附加的显示和其他命令，包括通过 ASA 5506 上的无线接入点进入 CLI 所需的 **session wlan console** 命令。此 CLI 有两种子模式；特权 EXEC 模式下有更多命令可用。

要进入此模式下，请在 threat defense CLI 中使用 **system support diagnostic-cli** 命令。

- 用户 EXEC 模式。提示符反映了运行配置中定义的系统主机名。

```
firepower>
```

- 特权 EXEC 模式。输入 **enable** 命令以进入此模式（当系统提示输入密码时，请按 Enter 键输入密码。）请注意，您无法为此模式设置密码。访问权限仅受登录 threat defense CLI 的账户保护。但是，用户无法在特权 EXEC 模式下进入配置模式，因此不需要额外的密码保护。

```
firepower#
```

专家模式

仅当书面程序指出必须使用或思科技术支持中心要求使用专家模式时，才使用专家模式。要进入此模式下，请在 threat defense CLI 中使用 **expert** 命令。

如果您使用 **admin** 用户登录，则提示符为 **username@hostname**。如果使用其他用户，则仅显示主机名。主机名是为管理接口配置的主机名。例如，

```
admin@firepower:~$
```

FXOS CLI

除 ASA 硬件型号外，FXOS 是控制整个机箱的操作系统。根据型号，您可以使用 FXOS 进行配置和故障排除。在 FXOS 中，您可以使用 **connect** 命令进入 threat defense CLI。

对于所有设备模式型号（Firepower 4100/9300 以外的型号），您可以使用 **connect fxos** 命令从 threat defense CLI 转到 FXOS CLI。

FXOS 命令提示符如下所示，但提示符会根据模式而变化。有关 FXOS CLI 使用的详细信息，请参阅 FXOS 文档。

```
Firepower-module2>  
Firepower-module2#
```

语法格式

命令语法说明使用以下约定：

| 约定 | Description |
|----------------|---|
| command | Command 文本指示按字面显示输入的命令和关键字。 |
| 变量 | 变量 文本指示由您提供值的参数。 |
| [x] | 方括号中包含可选元素（关键字或参数）。 |
| [x y] | 将以竖线分隔的关键字或参数括起来的方括号指示可选选项。 |
| {x y} | 将以竖线分隔的关键字或参数括起来的大括号指示必需选项。 |
| [x {y z}] | 方括号或大括号的嵌套集合指示可选或必需元素中的可选或必需选项。方括号中的大括号和竖线指示可选元素中的必需选项。 |

输入命令

当您通过控制台端口或 SSH 会话登录 CLI 时，系统会显示以下命令提示符：

>

在提示符后键入命令，然后按 **Enter** 键执行命令。其他功能包括：

- 滚动命令历史记录 - 可以使用向上和向下箭头键滚动浏览已输入的命令。您可以重新输入或编辑并重新输入历史记录中的命令。
- 完成命令-要在输入部分字符串后补全命令或关键字，请按空格或 **Tab** 键。部分字符串必须与单个命令或关键字匹配才能完成。
- 缩写命令 - 在常规 CLI 中，不能缩写命令。您必须输入完整的命令字符串。但是，在诊断 CLI 中，您可以将大多数命令缩写为最少的唯一字符；例如，您可以输入 **show ver** instead of **show version**。
- 停止命令输出 - 如果命令产生大量输出，可以按 **q** 键退出。
- 停止长时间运行的命令 - 如果某个命令没有足够快地返回输出，而您想要尝试其他命令，请按 **Ctrl+C**。

过滤 show 命令输出

您可以通过将输出传送给过滤命令来过滤 **show** 命令的输出。管道输出可搭配所有 **show** 命令使用，但搭配产生大量文本的命令使用时最为有用。

要使用过滤功能，请使用以下格式。在这种情况下，显示命令后的竖线 | 是管道字符，属于命令，而不属于语法说明。过滤选项在 | 字符后输入。

show 命令 | {grep | include | exclude | begin} 正则表达式

过滤命令

您可以使用以下过滤命令：

- **grep**- 仅显示匹配该模式的那些行。
- **include**- 仅显示匹配该模式的那些行。
- **exclude**- 排除匹配该模式的所有行并显示所有其他行。
- **begin**- 查找包含模式的第一行，并显示该行和所有后续行。

regular_expression

正则表达式，通常是简单的文本字符串。不要将表达式括在单引号或双引号中，这些引号将被视为表达式的一部分。此外，尾随空格也会包含在表达式中。

以下示例显示如何将 **show access-list** 命令的输出更改为仅显示适用于 **inside1_2** 接口的规则。

```
> show access-list | include inside1_2
access-list NGFW_ONBOX_ACL line 3 advanced trust ip ifc inside1_2 any ifc inside1_3 any
rule-id 268435458
event-log both (hitcnt=0) 0x2c7f5801
access-list NGFW_ONBOX_ACL line 4 advanced trust ip ifc inside1_2 any ifc inside1_4 any
rule-id 268435458
event-log both (hitcnt=0) 0xf170c15b
access-list NGFW_ONBOX_ACL line 5 advanced trust ip ifc inside1_2 any ifc inside1_5 any
rule-id 268435458
event-log both (hitcnt=0) 0xce627c77
access-list NGFW_ONBOX_ACL line 6 advanced trust ip ifc inside1_2 any ifc inside1_6 any
rule-id 268435458
event-log both (hitcnt=0) 0xe37dcdd2
access-list NGFW_ONBOX_ACL line 7 advanced trust ip ifc inside1_2 any ifc inside1_7 any
rule-id 268435458
event-log both (hitcnt=0) 0x65347856
access-list NGFW_ONBOX_ACL line 8 advanced trust ip ifc inside1_2 any ifc inside1_8 any
rule-id 268435458
event-log both (hitcnt=0) 0x6d622775
access-list NGFW_ONBOX_ACL line 9 advanced trust ip ifc inside1_3 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0xc1579ed7
access-list NGFW_ONBOX_ACL line 15 advanced trust ip ifc inside1_4 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0x1d1a8032
access-list NGFW_ONBOX_ACL line 21 advanced trust ip ifc inside1_5 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0xf508bbd8
```

```
access-list NGFW_ONBOX_ACL line 27 advanced trust ip ifc inside1_6 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0xa6be4e58
access-list NGFW_ONBOX_ACL line 33 advanced trust ip ifc inside1_7 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0x699725ea
access-list NGFW_ONBOX_ACL line 39 advanced trust ip ifc inside1_8 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0xd2014e58
access-list NGFW_ONBOX_ACL line 47 advanced trust ip ifc inside1_2 any ifc outside any
rule-id 268435457
event-log both (hitcnt=0) 0xea5bdd6e
```


命令帮助

通过输入以下命令，可从命令行获取帮助信息：

- `?` 查看所有命令的列表。
- `command_name ?` 查看命令的选项。例如，`show ?`。
- `string?` 以显示与该字符串匹配的命令或关键字。例如，`n?` 显示以字母 `n` 开头的所有命令。
- `help command_name` 以查看命令的语法和限制使用信息。输入 `help ?` 以查看哪些命令具有帮助页面。

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。