



## VPN 监控和故障排除

本章介绍 Firepower 威胁防御 VPN 监视工具、参数和统计信息以及故障排除。

- [VPN 摘要控制面板，第 1 页](#)
- [VPN 会话和用户信息，第 2 页](#)
- [VPN 运行状况事件，第 2 页](#)
- [VPN 故障排除，第 3 页](#)

### VPN 摘要控制面板

系统控制面板为您提供当前系统状态的概览视图，包括有关系统收集和生成的事件的数据。您可以使用 VPN 控制面板查看有关 VPN 用户的整合信息，包括用户当前状态、设备类型、客户端应用、用户地理位置信息和连接持续时间。您可以查看已配置的 VPN 拓扑的详细信息，例如 VPN 接口、隧道状态等。

对于所有 VPN 拓扑，您可以通过编辑和删除按钮来编辑或删除拓扑。

### 查看 VPN 摘要控制面板

远程接入 VPN 为远程用户（如移动用户或远程工作者）提供安全连接。监控这些连接可以让连接和用户会话性能的重要指标变得一目了然。

您必须是枝叶域中的管理员用户才能执行此任务。

#### 过程

**步骤 1** 选择概述 > 控制板 > 访问受控用户统计信息 > VPN。

**步骤 2** 查看远程接入 VPN 信息构件：

- 按持续时间划分的当前 VPN 用户。
- 按客户端应用划分的当前 VPN 用户。
- 按设备划分的当前 VPN 用户。
- 按传输的数据划分的 VPN 用户。

- 按持续时间划分的 VPN 用户。
- 按客户端应用划分的 VPN 用户。
- 按客户端所在国家/地区划分的 VPN 用户。

## VPN 会话和用户信息

系统生成在网络上传达用户活动详细信息的事件，包括与 VPN 相关的活动。系统监视功能使您能够快速确定远程接入 VPN 问题是否存在及其存在的位置。然后，您可以应用这些知识并使用网络管理工具来减少或消除网络和用户问题。或者，您可以根据需要注销远程接入 VPN 用户。

### 查看远程接入 VPN 活动会话

分析 > 用户 > 活动会话

使您可以使用支持信息（如用户名、登录持续时间、身份验证类型、分配的/公用 IP 地址、设备详细信息、客户端版本、终端消息、吞吐量、占用带宽的组策略、隧道组等）在任何给定的时间点查看当前登录的 VPN 用户。系统允许您过滤当前用户信息、注销用户以及从摘要列表中删除用户。



**注释** 如果在高可用性部署中配置了 VPN，则针对活动 VPN 会话显示的设备名称可以是识别用户会话的主要或辅助设备。

### 查看远程接入 VPN 用户活动

分析 > 用户 > 用户活动

用于查看网络上用户活动的详细信息。系统记录历史事件，包括与 VPN 相关的信息，如连接配置文件信息、IP 地址、地理位置信息、连接持续时间、吞吐量和设备信息。

## VPN 运行状况事件

通过“运行状况事件”页面，您可以查看由运行状况监控器在管理中心记录的 VPN 运行状况事件。当设备之间的一个或多个 VPN 隧道关闭时，运行状况监控器会跟踪以下事件：

- 适用于 Cisco Secure Firewall Threat Defense 的站点间 VPN
- 适用于 Cisco Secure Firewall Threat Defense 的远程接入 VPN

## 查看 VPN 运行状况事件

当您在 Cisco Secure Firewall Management Center 中从“运行状况事件”页面访问运行状况事件时，可以检索所有受管设备的所有运行状况事件。可以通过指定生成要查看的运行状况事件的模块来缩小事件范围。

您必须是管理员、维护用户或安全分析师才能执行此任务。

### 过程

**步骤 1** 选择系统 > 运行状况 > 事件。

**步骤 2** 在模块名称列下选择 **VPN 状态**。

## VPN 故障排除

本部分介绍 VPN 故障排除工具和调试信息。

## 系统消息

邮件中心是开始进行故障排除的地方。通过此功能，可以查看持续生成的有关系统活动和状态的消息。要打开消息中心，请点击位于主菜单中部署 (Deploy) 按钮正右侧的**系统状态 (System Status)**。

## VPN 系统日志

您可以为威胁防御设备启用系统日志记录（系统日志）。日志记录信息可以帮助您发现并隔离网络或设备配置问题。启用 VPN 日志记录时，这些系统日志将从威胁防御设备发送到 Cisco Secure Firewall Management Center 进行分析和存档。

所有出现的 VPN 系统日志都具有默认严重性级别“错误” (ERROR) 或更高（除非已更改）。您可以通过威胁防御平台设置来管理 VPN 日志记录。您可以通过编辑目标设备的威胁防御平台设置策略中的 **VPN 日志记录设置** 来调整消息严重性级别（**平台设置 > 系统日志 > 日志记录设置**）。有关启用 VPN 日志记录、配置系统日志服务器以及查看系统日志的详细信息，请参阅[系统日志](#)。



**注释** 只要您配置了具有站点间或远程访问 VPN 的设备，它就会默认自动启用将 VPN 系统日志发送至管理中心。

## 查看 VPN 系统日志

系统捕获事件信息，以帮助您收集有关 VPN 问题源的其他信息。显示的任何 VPN 系统日志都具有默认严重性级别“ERROR”或更高（除非已更改）。默认情况下，行按时间列排序。

您必须是枝叶域中的管理员用户才能执行此任务。

### 开始之前

通过选中 威胁防御平台设备中的使记录至 FMC 复选框，启用 VPN 日志记录（设备 > 平台设置 > 系统日志 > 日志记录设置）。有关启用 VPN 日志记录、配置系统日志服务器以及查看系统性记录的详细信息，请参阅[系统日志](#)。

### 过程

**步骤 1** 选择设备 > VPN > 故障排除。

**步骤 2** 您有以下选择：

- 搜索 - 要过滤当前消息信息，请点击 [编辑搜索](#)。
- 查看 - 要查看与视图中所选消息关联的 VPN 详细信息，请点击 [查看](#)。
- 查看全部 - 要查看视图中所有消息的事件详细信息，请点击 [查看全部](#)。
- 删除 - 要从数据库中删除选定的消息，请点击 [删除](#) 或点击 [全部删除](#) 以删除所有消息。

## 调试命令

本节介绍如何使用调试命令来帮助您诊断和解决与 VPN 相关的问题。此处介绍的命令并非详尽无遗，本节将根据命令的作用来帮助您诊断 VPN 相关问题。

### 使用指南

由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。为此，应仅在对特定问题进行故障排除或与思科 Technical Assistance Center (TAC) 进行故障排除会话时使用 **debug** 命令。此外，最好在网络流量较低和用户较少时使用 **debug** 命令。在这些时段进行调试会减少因 **debug** 命令处理开销增加而影响系统使用的可能性。

您只能在 CLI 会话中查看调试输出。在连接到控制台端口的情况下，或者在诊断 CLI 中，您可以直接查看输出结果（输入 **system support diagnostic-cli**）。此外，您也可以在常规 Firepower Threat Defense CLI 中使用 **show console-output** 命令查看输出结果。

要显示给定功能的调试消息，请使用 **debug** 命令。要禁用调试消息的显示，请使用此命令的 **no** 形式。使用 **no debug all** 关闭所有调试命令。

**debug feature** [*subfeature*] [*level*]

**no debug feature** [*subfeature*]

### Syntax Description

<i>feature</i>	指定要为其启用调试的功能。若要查看可用功能，请使用 <b>debug ?</b> 命令获取 CLI 帮助。
<i>subfeature</i>	（可选）根据功能，您可以为一项或多项子功能启用调试消息。使用 ? 查看可用的子功能。
<i>level</i>	（可选）指定调试级别。使用 ? 可查看可用的级别。

**Command Default**

默认调试级别为 1。

**示例**

在远程接入 VPN 上运行多个会话时，由于日志的大小，可能会很难进行故障排除。可以使用 **debug webvpn condition** 命令设置过滤器，以便更精确地定位调试进程。

```
debug webvpn condition { group name | p-ipaddress ip_address [{ subnet subnet_mask | prefix length]} | reset | user name}
```

其中：

- **group name** 对组策略进行过滤，而不是隧道组或连接配置文件。
- **p-ipaddress ip\_address** [{**subnet subnet\_mask** | **prefix length**}] 对客户端的公共 IP 地址进行过滤。子网掩码（用于 IPv4）或前缀（用于 IPv6）是可选的。
- **reset** 重置所有过滤器。可以使用 **no debug webvpn condition** 命令关闭特定的过滤器。
- **user Name** 按用户名过滤。

如果配置多个条件，则条件是合并的 (AND)，因此只有满足所有条件时才显示调试。

设置条件过滤器后，使用基本 **debug webvpn** 命令打开调试。只设置条件不会启用调试。使用 **show debug** 和 **show webvpn debug-condition** 命令查看调试的当前状态。

下文是在用户 jdoe 上启用条件调试的示例。

```
firepower# debug webvpn condition user jdoe

firepower# show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe

firepower# debug webvpn
INFO: debug webvpn enabled at level 1.

firepower# show debug
debug webvpn enabled at level 1
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

**Related Commands**

命令	说明
<b>show debug</b>	显示当前活动的调试设置。
<b>undebug</b>	禁用功能调试。此命令与 <b>no debug</b> 的效果相同。

## 调试 aaa

请参阅以下命令以调试配置或身份验证、授权和记帐 (AAA) 设置。

**debug aaa** [*accounting* | *authentication* | *authorization* | *common* | *internal* | *shim* | *url-redirect*]

Syntax Description	aaa	启用对 AAA 的调试。使用 ? 查看可用的子功能。
	<i>accounting</i>	(可选) 启用 AAA 记帐调试。
	<i>authentication</i>	(可选) 启用 AAA 身份验证调试。
	<i>authorization</i>	(可选) 启用 AAA 授权调试。
	<i>common</i>	(可选) 指定 AAA 通用调试级别。使用 ? 查看可用的级别。
	<i>internal</i>	(可选) 启用 AAA 内部调试。
	<i>shim</i>	(可选) 指定 AAA shim 调试级别。使用 ? 查看可用的级别。
	<i>url-redirect</i>	(可选) 启用 AAA url-redirect 调试。

**Command Default** 默认调试级别为 1。

Related Commands	命令	说明
	<b>show debug aaa</b>	显示 AAA 当前的活动调试设置。
	<b>undebug aaa</b>	禁用 AAA 的调试。此命令与 <b>no debug aaa</b> 的效果相同。

## debug crypto

请参阅以下用于调试与 crypto 相关联的配置或设置的命令。

**debug crypto** [*ca* | *condition* | *engine* | *ike-common* | *ikev1* | *ikev2* | *ipsec* | *ss-apic*]

Syntax Description	crypto	启用对 crypto 的调试。使用 ? 查看可用的子功能。
	<i>ca</i>	(可选) 指定 PKI 调试级别。可以使用 ? 查看可用子功能。
	<i>condition</i>	(可选) 指定 IPsec/ISAKMP 调试过滤器。可以使用 ? 查看可用过滤器。
	<i>engine</i>	(可选) 指定 crypto 引擎调试级别。可以使用 ? 查看可用级别。
	<i>ike-common</i>	(可选) 指定 IKE 常用调试级别。可以使用 ? 查看可用级别。
	<i>ikev1</i>	(可选) 指定 IKE 版本 1 调试级别。可以使用 ? 查看可用级别。
	<i>ikev2</i>	(可选) 指定 IKE 版本 2 调试级别。可以使用 ? 查看可用级别。

<i>ipsec</i>	(可选) 指定 IPsec 调试级别。使用 ? 可查看可用的级别。
<i>condition</i>	(可选) 指定 Crypto 安全套接字 API 调试级别。可以使用 ? 查看可用级别。
<i>vpnclient</i>	(可选) 指定 EasyVPN 客户端调试级别。使用 ? 可查看可用的级别。

**Command Default** 默认调试级别为 1。

命令	说明
<b>show debug crypto</b>	显示当前处于活动状态的适用于 crypto 的调试设置。
<b>undebug crypto</b>	禁用对 crypto 的调试。此命令与 <b>no debug crypto</b> 的效果相同。

## debug crypto ca

请参阅以下用于调试与 crypto ca 相关联的配置或设置的命令。

**debug crypto ca** [*cluster* | *messages* | *periodic-authentication* | *scep-proxy* | *transactions* | *trustpool*] [*1-255*]

Syntax Description	说明
<i>crypto ca</i>	启用对 <i>crypto ca</i> 的调试。使用 ? 查看可用的子功能。
<i>cluster</i>	(可选) 指定 PKI 集群调试级别。可以使用 ? 查看可用级别。
<i>cmp</i>	(可选) 指定 CMP 交易调试级别。可以使用 ? 查看可用级别。
<i>messages</i>	(可选) 指定 PKI 输入/输出消息调试级别。可以使用 ? 查看可用级别。
<i>periodic-authentication</i>	(可选) 指定 PKI 周期性身份验证调试级别。可以使用 ? 查看可用级别。
<i>scep-proxy</i>	(可选) 指定 SCEP 代理调试级别。可以使用 ? 查看可用级别。
<i>server</i>	(可选) 指定本地 CA 服务器调试级别。可以使用 ? 查看可用级别。
<i>transactions</i>	(可选) 指定 PKI 交易调试级别。可以使用 ? 查看可用级别。
<i>trustpool</i>	(可选) 指定信任池调试级别。使用 ? 查看可用的级别。
<i>1-255</i>	(可选) 指定调试级别。

**Command Default** 默认调试级别为 1。

命令	说明
<b>show debug crypto ca</b>	显示当前处于活动状态的适用于 crypto ca 的调试设置。
<b>undebug</b>	禁用对 crypto ca 的调试。此命令与 <b>no debug crypto ca</b> 的效果相同。

## debug crypto ikev1

## debug crypto ikev1

有关与 Internet 密钥交换版本 1 (IKEv1) 相关联的调试配置或设置，请参阅以下命令。

```
debug crypto ikev1 [timers] [1-255]
```

## Syntax Description

<i>ikev1</i>	启用 <i>ikev1</i> 调试。使用 ? 查看可用的子功能。
<i>timers</i>	(可选) 启用 IKEv1 计时器调试。
<i>1-255</i>	(可选) 指定调试级别。

## Command Default

默认调试级别为 1。

## Related Commands

命令	说明
<b>show debug crypto ikev1</b>	显示 IKEv1 的当前活动调试设置。
<b>undebug crypto ikev1</b>	禁用 IKEv1 调试。此命令与 <b>no debug crypto ikev1</b> 的效果相同。

## debug crypto ikev2

有关与 Internet 密钥交换版本 2 (IKEv2) 相关联的调试配置或设置，请参见以下命令。

```
debug crypto ikev2 [ha | platform | protocol | timers]
```

## Syntax Description

<i>ikev2</i>	启用调试 <i>ikev2</i> 。使用 ? 查看可用的子功能。
<i>ha</i>	(可选) 指定 IKEv2 HA 调试级别。使用 ? 查看可用的级别。
<i>platform</i>	(可选) 指定 IKEv2 平台调试级别。使用 ? 查看可用的级别。
<i>protocol</i>	(可选) 指定 IKEv2 协议调试级别。使用 ? 查看可用的级别。
<i>timers</i>	(可选) 启用针对 IKEv2 计时器的调试。

## Command Default

默认调试级别为 1。

## Related Commands

命令	说明
<b>show debug crypto ikev2</b>	显示 IKEv2 的当前活动调试设置。
<b>undebugcrypto ikev2</b>	禁用针对 IKEv2 的调试。此命令与 <b>no debug crypto ikev2</b> 的效果相同。

## debug crypto ipsec

有关调试与 IPsec 关联的配置或设置的信息，请参阅以下命令。

```
debug crypto ipsec [1-255]
```



<b>Syntax Description</b>	<i>ipsec</i>	启用对 <i>ipsec</i> 的调试要使用？请查看可用的子功能。
	<i>1-255</i>	(可选) 指定调试级别。

**Command Default** 默认调试级别为 1。

<b>Related Commands</b>	命令	说明
	<b>show debug crypto ipsec</b>	显示 IPsec 的当前活动调试设置。
	<b>undebugcrypto ipsec</b>	禁用对 IPsec 的调试。此命令与 <b>no debug crypto ipsec</b> 的效果相同。

## debug ldap

有关调试与 LDAP 关联的配置或设置的信息（轻量级目录访问协议），请参阅以下命令。

**debug ldap** [*1-255*]

<b>Syntax Description</b>	<i>ldap</i>	启用对 LDAP 的调试。要使用？请查看可用的子功能。
	<i>1-255</i>	(可选) 指定调试级别。

**Command Default** 默认调试级别为 1。

<b>Related Commands</b>	命令	说明
	<b>show debug ldap</b>	显示 LDAP 的当前活动调试设置。
	<b>undebugldap</b>	禁用对 LDAP 的调试。此命令与 <b>no debug ldap</b> 的效果相同。

## 调试 ssl

请参阅调试与 SSL 会话关联的配置或设置的以下命令。

**debug ssl** [*cipher | device*] [*1-255*]

<b>Syntax Description</b>	<i>ssl</i>	启用对 SSL 的调试。使用？查看可用的子功能。
	<i>cipher</i>	(可选) 指定 SSL 密码调试级别。使用？查看可用的级别。
	<i>device</i>	(可选) 指定 SSL 设备调试级别。使用？查看可用的级别。
	<i>1-255</i>	(可选) 指定调试级别。

**Command Default** 默认调试级别为 1。

Related Commands	命令	说明
	<b>show debug ssl</b>	显示 SSL 当前的活动调试设置。
	<b>undebug ssl</b>	禁用对 SSL 的调试。此命令与 <b>no debug ssl</b> 的效果相同。

## debug webvpn

请参阅以下调试与 WebVPN 关联的配置或设置的命令。

**debug webvpn** [*anyconnect* | *chunk* | *cifs* | *citrix* | *compression* | *condition* | *cstp-auth* | *customization* | *failover* | *html* | *javascript* | *kcd* | *listener* | *mus* | *nfs* | *request* | *response* | *saml* | *session* | *task* | *transformation* | *url* | *util* | *xml*]

Syntax Description	webvpn	启用 WebVPN 的调试。使用 ? 可查看可用的子功能。
	<i>anyconnect</i>	(可选) 指定 WebVPN AnyConnect 调试级别。使用 ? 可查看可用的级别。
	<i>chunk</i>	(可选) 指定 WebVPN 分块调试级别。使用 ? 可查看可用的级别。
	<i>cifs</i>	(可选) 指定 WebVPN CIFS 调试级别。使用 ? 可查看可用的级别。
	<i>citrix</i>	(可选) 指定 WebVPN Citrix 调试级别。使用 ? 可查看可用的级别。
	<i>compression</i>	(可选) 指定 WebVPN 压缩调试级别。使用 ? 可查看可用的级别。
	<i>condition</i>	(可选) 指定 WebVPN 过滤条件调试级别。使用 ? 可查看可用的级别。
	<i>cstp-auth</i>	(可选) 指定 WebVPN CSTP 身份验证调试级别。使用 ? 可查看可用的级别。
	<i>customization</i>	(可选) 指定 WebVPN 自定义调试级别。使用 ? 可查看可用的级别。
	<i>failover</i>	(可选) 指定 WebVPN 故障切换调试级别。使用 ? 可查看可用的级别。
	<i>html</i>	(可选) 指定 WebVPN HTML 调试级别。使用 ? 可查看可用的级别。
	<i>javascript</i>	(可选) 指定 WebVPN Javascript 调试级别。使用 ? 可查看可用的级别。
	<i>kcd</i>	(可选) 指定 WebVPN KCD 调试级别。使用 ? 可查看可用的级别。
	<i>listener</i>	(可选) 指定 WebVPN 侦听程序调试级别。使用 ? 可查看可用的级别。
	<i>mus</i>	(可选) 指定 WebVPN MUS 调试级别。使用 ? 可查看可用的级别。
	<i>nfs</i>	(可选) 指定 WebVPN NFS 调试级别。使用 ? 可查看可用的级别。
	<i>request</i>	(可选) 指定 WebVPN 请求调试级别。使用 ? 可查看可用的级别。
	<i>response</i>	(可选) 指定 WebVPN 响应调试级别。使用 ? 可查看可用的级别。

<i>saml</i>	(可选) 指定 WebVPN SAML 调试级别。使用 ? 可查看可用的级别。
<i>session</i>	(可选) 指定 WebVPN 会话调试级别。使用 ? 可查看可用的级别。
<i>task</i>	(可选) 指定 WebVPN 任务调试级别。使用 ? 可查看可用的级别。
<i>transformation</i>	(可选) 指定 WebVPN 转换调试级别。使用 ? 可查看可用的级别。
<i>url</i>	(可选) 指定 WebVPN URL 调试级别。使用 ? 可查看可用的级别。
<i>util</i>	(可选) 指定 WebVPN 实用程序调试级别。使用 ? 可查看可用的级别。
<i>xml</i>	(可选) 指定 WebVPN XML 调试级别。使用 ? 可查看可用的级别。

**Command Default**

默认调试级别为 1。

**Related Commands**

命令	说明
<b>show debug webvpn</b>	显示 WebVPN 的当前活动调试设置。
<b>undebug webvpn</b>	禁用 WebVPN 的调试。此命令与 <b>no debug webvpn</b> 的效果相同。



## 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。