VPN 监控和故障排除

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

站点间 VPN 摘要页面

您可以使用站点间VPN摘要页面来查看有关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。对于SASE拓扑VPN，您可以选择部署、编辑和删除任何拓扑。

远程访问 VPN 控制面板

远程访问虚拟专用网络 (RA VPN) 允许远程用户安全地连接到您的网络。通过 RA VPN 控制面板，您可以监控设备上活动 RA VPN 会话的实时数据。您可以快速确定与用户会话相关的问题，同时缓解网络和用户的问题。

RA VPN 控制面板（**概述 > 控制面板 > 远程访问 VPN**）提供 管理中心管理的威胁防御设备上的活动 RA VPN 会话快照。

控制面板具有以下构件：

- 活动会话（表格视图）
- 活动会话（地图视图）
- 会话

- 设备身份证书

活动会话（表格视图）

此构件提供已连接的活动 RA VPN 用户的表格视图。您可以查看活动 RA VPN 会话的详细信息，例如用户名、分配的IP、公共IP、登录时间、VPN网关（威胁防御设备）、客户端应用、客户端操作系统、连接配置文件和组策略。您可以使用过滤器根据不同的条件来缩小搜索范围。您还可以对各个会话执行以下操作：

- 终止特定用户的会话。
- 终止连接到特定 VPN 网关的特定用户的所有会话。
- 终止连接到特定 VPN 网关的所有会话。

如果客户端设备支持双地址栈，并且 威胁防御 设备上的 RA VPN 配置允许 IPv4 和 IPv6 地址池，那么当客户端与头端设备建立 RA VPN 会话时，它会为客户端的隧道接口分配一个 IPv4 和一个 IPv6 地址。RA VPN 会话有两个 IP 地址，即威胁防御设备上的 IPv4 和 IPv6 地址。管理中心 显示同一用户的两个会话，一个使用 IPv4 地址，另一个使用 IPv6 地址，会话计数为 2。

因此，即使根据设备上的 **show vpn-sessiondb l2l filter ipaddress** 命令，用户只有一个RA VPN会话，管理中心 也会显示两个不同的会话。

活动会话（地图视图）

该构件会显示交互式热度地图，以便直观地显示通过 RA VPN 会话连接到设备上的用户的位置。

- 具有用户会话的国家/地区会显示为蓝色阴影。
- 地图图例提供了一个比例，表示某个国家/地区的会话数与其蓝色阴影之间的相关性。
- 将鼠标指针悬停在地图上即可查看国家/地区名称和活动用户会话总数。
- 提供放大、缩小和重置选项。

会话

此构件允许您监控设备上活动RA VPN会话的实时数据。您可以根据以下条件来过滤和查看活动RA VPN 会话的分布情况：

- 设备：显示每台设备的会话数。
- 加密类型：显示 Secure Client SSL 或 IPsec 会话的数量。
- Secure Client 版本：显示每个 Secure Client 版本的会话。
- 操作系统：显示每个操作系统的会话。例如，Windows、Linux、Mac、Mobile OS 等。
- 连接配置文件：显示每个连接配置文件的会话。

设备身份证书

此构件提供有关RA VPN网关身份证书到期的信息。您可以查看过期的证书和一个月内到期的证书。点击**查看详细信息 (View Details)**，在**设备 (Device) > 证书 (Certificates)** 页面中查看证书。

Cisco SD-WAN 摘要控制面板

SD-WAN 摘要控制面板（**概述 > 控制面板 > SD-WAN 摘要**）提供 WAN 设备及其接口的快照。此控制面板可帮助您：

- 确定底层网络和重叠网络 (VPN) 拓扑的问题。
- 使用现有的 **运行状况监控**、 **设备管理**和 **站点间监控** 页面解决 VPN 问题。
- 监控 WAN 接口的应用性能指标。威胁防御系统会根据这些指标引导应用流量。

WAN 设备必须满足以下条件之一：

- 设备必须是一个 VPN 对等体。
- 设备必须有 WAN 接口。

WAN 接口必须满足以下条件之一：

- 接口已启用基于 IP 地址的路径监控。
- 接口具有策略型路由 (PBR) PBR 策略，并配置了至少一个应用来对其进行监控。

有关 PBR 策略和路径监控的详细信息，请参阅 策略型路由。

点击 **上行链路决策** 以查看 **VPN 故障排除** 页面。您可以查看 ID 为 880001 的系统日志。这些系统日志显示威胁防御接口，它通过这些接口根据配置的 PBR 策略引导流量。

要查看上述系统日志并查看此控制面板上的数据，请确保查看使用 SD-WAN 摘要控制面板的前提条件，第 3 页。

对于集群，此控制面板仅显示控制节点的应用性能指标，而不显示数据节点的应用性能指标。

使用 SD-WAN 摘要控制面板的前提条件

- 您必须是管理员、安全分析师或运维用户才能查看控制面板。
- 威胁防御设备必须为 7.2 或更高版本。
- 在 WAN 接口上启用基于 IP 的路径监控和基于 HTTP 的应用监控。
  1. 选择**设备 > 设备管理**。
  2. 点击要编辑的设备旁边的编辑图标。
  3. 点击要编辑的接口旁边的编辑图标。

4. 点击 **路径监控 (Path Monitoring)** 选项卡。
5. 选中**启用基于 IP 的监控 (Enable IP based Monitoring)** 复选框。
6. 选中**启用基于 HTTP 的应用监控 (Enable HTTP based Application Monitoring)** 复选框。
7. 点击**确定 (OK)**。

- 配置 PBR 策略，其中至少有一个应用配置为对其进行监控：
  1. 选择**设备 > 设备管理**。
  2. 点击要编辑的设备旁边的编辑图标。
  3. 点击**路由**。
  4. 在左侧窗格，点击 **策略型路由**。
  5. 点击**添加 (Add)**。
  6. 从 **入口接口** 下拉列表中，选择接口。
  7. 点击 **添加** 以配置转发操作。
  8. 配置相关参数。
  9. 点击**保存 (Save)**。
- 要查看 WAN 的应用性能指标，您必须：
  - 威胁防御设备必须是版本 7.4.1。
  - 在运行状况策略中启用 SD-WAN 模块的数据收集。
    1. 选择**系统 (System) > 策略 (Policy)**。
    2. 点击**编辑运行状况策略 (Edit health policy)** 图标。
    3. 在 **运行状况模块** 选项卡，在 **SD-WAN**下，点击 **SD-WAN 监控** 切换按钮。
  - 为 PBR 策略配置应用。
    1. 选择**对象 (Objects) > 对象管理 (Object Management) > 访问列表 (Access List) > 扩展 (Extended)**。
    2. 点击访问列表旁边的编辑图标，然后为 PBR 策略添加应用。
  - 使用四种应用指标之一为策略配置转发操作。
    1. 选择**设备 > 设备管理**。
    2. 点击要编辑的设备旁边的编辑图标。
    3. 点击**路由**。
    4. 在左侧窗格，点击 **策略型路由**。

5. 点击要编辑的策略旁边的编辑图标。
6. 在 **编辑基于策略的路由** 对话框中，点击相应 ACL 旁边的编辑图标。
7. 在 **编辑转发操作** 对话框中，从 **接口排序** 下拉列表中选择以下选项之一：
   - **最小抖动**
   - **最大平均意见得分**
   - **最短往返时间**
   - **最小丢包率**

   如果选择 **接口优先级** 或 **顺序**，则不会在接口上启用应用监控。

- 在 WAN 接口上配置 ECMP：
  1. 选择**设备 > 设备管理**。
  2. 点击要编辑的设备旁边的编辑图标。
  3. 点击**路由**。
  4. 在左侧窗格中，点击 **ECMP**。
  5. 点击 **添加** 并指定 ECMP 区域的名称。
  6. 点击 **添加** ，将接口从 **可用接口** 移至 **所选接口**。
  7. 点击**确定 (OK)**。
- 确保流量通过接口。
- 在每个 WAN 设备上启用 DNS 检查，以便威胁防御设备可以执行 DNS 监听，并配置受信任的 DNS 服务器：
  1. 选择 **设备 > 平台设置**。
  2. 点击要编辑的威胁策略旁边的编辑图标。
  3. 在左侧窗格中，点击 **DNS**。
  4. 点击 **DNS 设置** 选项卡。
  5. 选择 **启用按设备 DNS 域名解析** 复选框。
  6. 点击 **受信任的 DNS 服务器** 选项卡。
  7. 执行以下操作之一：
     - 点击 **Trust Any DNS 服务器** 切换按钮。
     - 请在 **指定 DNS 服务器**下，点击 **编辑**来添加受信任的 DNS 服务器。

- 要在点击**上行链路决策 (Uplink Decisions)** 时查看系统日志，必须执行以下操作：
  - 选择**设备 (Devices)** > **平台设置 (Platform Settings)** 并创建或编辑威胁防御策略。
  - 在左侧窗格中，点击**系统日志 (Syslog)**。
  - 点击**日志记录设置 (Logging Setup)** 选项卡。
  - 选中**启动日志记录 (Enable Logging)** 复选框为威胁防御设备开启数据平面系统日志记录。
  - 点击**所有日志 (All Logs)** 单选按钮以启用对所有故障排除系统日志消息的日志记录。

    或者

    点击 **VPN 日志记录 (VPN Logs)** 单选按钮以启用仅记录 VPN 故障排除消息。
  - 点击**保存 (Save)**。

使用 SD-WAN 摘要控制面板监控 WAN 设备和接口

SD-WAN 摘要控制面板在 **概述选项卡** 上具有以下 构件：

- 排名靠前的应用，第 6 页
- WAN 连接，第 6 页
- VPN 拓扑，第 7 页
- 接口吞吐量，第 7 页
- 设备清单，第 7 页
- WAN 设备运行状况，第 7 页

排名靠前的应用

此构件显示根据吞吐量排名的前 10 个应用。

从 **显示最后时间** 下拉列表，选择构件数据的时间范围。范围为 15 分钟到两周。

WAN 连接

此构件提供 WAN 接口的状态摘要。它显示处于 **在线**、 **离线** 或 **无数据** 状态的 WAN 接口的数量。请注意，您无法使用此构件监控子接口。

点击 **查看所有接口**，以在“运行状况监控器”页面中查看有关接口的更多详细信息。

如果 WAN 接口处于 **离线** 或 **无数据** 状态，您可以从运行状况监控页面进行故障排除：

1. 在 **监控** 窗格中，展开 **设备**。
2. 点击相应的 WAN 设备可查看设备特定的运行状况详细信息。
3. 点击 **接口** 选项卡可查看特定时间的接口状态和汇聚流量统计信息。

或者，您可以点击 **查看系统和故障排除详细信息**。系统将显示运行状况监控页面，其中包含所有必要的详细信息。

VPN 拓扑

此构件提供站点间 VPN 隧道状态的摘要。它显示 **活动**、 **非活动**和 **无活动数据** VPN 隧道的数量。

点击 **查看所有连接** ，在 **站点间 VPN 监控** 控制面板中查看 VPN 隧道详细信息。

如果隧道处于 **非活动** 或 **无活动数据** 状态，您可以使用 **站点间 VPN 监控控制** 面板进行故障排除。在**隧道状态 (Tunnel Status)** 构件中，将光标悬停在拓扑上，点击 **视图 (** **)** 并执行以下操作之一：

- 点击 **CLI 详细信息** 选项卡以查看 VPN 隧道的详细信息。
- 点击 **数据包跟踪器** 选项卡，为拓扑使用数据包跟踪器工具。

接口吞吐量

此构件会监控所选时间段内 WAN 接口的平均吞吐量。

接口吞吐量分为四个频段。这些详细信息有助于成本规划和资源配置。从 **显示最后时间** 下拉列表，选择构件数据的时间范围。范围是从 15 分钟到两周。

点击 **查看运行状况监控** ，以在“运行状况监控”页面中查看有关接口的更多详细信息。

设备清单

此构件根据型号列出所有托管设备并对其进行分组。

点击 **查看设备管理** ，在 **设备管理** 页面中查看有关设备的更多详细信息。

WAN 设备运行状况

此构件根据 WAN 设备的运行状况显示设备计数。您可以查看出现错误、警告或处于 **禁用** 状态的设备数量。

点击 **查看运行状况监控** ，查看警报并快速识别、隔离和解决问题。

如果设备的运行状况受到影响，您可以从运行状况监控页面进行故障排除。

1. 在 **监控** 窗格中，展开 **设备**。
2. 点击相应的 WAN 设备可查看设备特定的运行状况详细信息。
3. 点击 **查看系统和故障排除详细信息**。系统将显示运行状况监控页面，其中包含所有必要的详细信息。

设备可能由于多种原因而处于 **禁用** 状态，包括以下原因：

- 禁用管理接口。
- 设备已关闭。
- 设备正在升级。

使用 SD-WAN 摘要控制面板监控 WAN 接口的应用性能指标

在 **应用监控** 选项卡中，您可以选择 WAN 设备并查看相应 WAN 接口的应用性能指标。这些指标包括抖动、往返时间 (RTT)、平均意见得分 (MOS) 和丢包。

默认情况下，指标数据每 5 分钟刷新一次。您可以更改刷新时间；范围为 5 到 30 分钟。您可以以表格和图形格式查看指标。对于每个 WAN 接口，表中列出了指标的最新值。对于图形数据，您可以选择最多 24 小时的时间间隔来查看相应 WAN 接口的指标数据。

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。

站点间 VPN 连接事件监控

通过站点间 VPN 连接事件，您可以了解 VPN 是否加密连接，并帮助您解决连接问题，尤其是在多跳 VPN 部署中。 管理中心 的事件控制面板显示加密或解密流量的 VPN 对等体的 IP 地址（对等体的 IKE 地址），并显示 VPN 操作，如下所示：

- 如果连接由 VPN 解密，则**解密对等体 (Decrypt Peer)** 列会显示接收流量的对等体地址 IP 地址，并将**解密 (Decrypt)** 显示为 VPN 操作。

- 如果连接由 VPN 加密，则**加密对等体 (Encrypt Peer)** 列会显示流量发送到的 VPN 对等体的 IP 地址，并将**加密 (Encrypt)** 显示为 VPN 操作。
- 如果VPN服务器级联连接，它将在一个隧道上解密，并在另一个隧道上重新加密。在这种情况下，事件中会同时显示 **加密对等体** 和 **解密对等体** IP 地址。 **VPN 操作** 列显示 **VPN 路由** 作为指示连接通过 VPN 服务器传输的操作。

如果启用绕过已解密流量的访问控制策略选项，则系统会绕过访问控制策略，并且不会记录已解密流量的事件。默认情况下，此选项处于禁用状态，VPN 隧道中的所有已解密流量都会经过 ACL 检查。

查看站点间 VPN 连接事件

访问 管理中心 的连接事件查看器，了解 VPN 是否加密连接流量，并检索 VPN 对等体详细信息。

开始之前

确保在访问控制规则中启用连接开始时和连接结束时的连接事件日志记录。

过程

步骤 1 选择**分析** > **连接** > **事件**。

步骤 2 转到 **连接事件的表视图** 选项卡。

步骤 3 事件表视图中的多个字段在默认情况下处于隐藏状态。要更改显示的字段，请点击任何列名称中的 **x** 图标以显示字段选择器。

步骤 4 选择以下列：

- 解密对等体
- 加密对等体
- VPN 操作

步骤 5 点击**应用 (Apply)**。

有关连接事件的详细信息，请参阅《Cisco Secure Firewall Management Center 管理指南》中的连接和安全相关的连接事件。

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 VPN 故障排除系统日志的日志记录。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 管理中心。

所有出现的 VPN 系统日志都具有默认严重性级别 **错误** 或更高严重性（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。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，请参阅配置 FTD 设备的系统日志日志记录。

从故障排除日志表（**设备 > 故障排除日志**）中，您可以查看和分析 VPN 系统日志消息，以识别和隔离网络和设备配置问题。

建议将 VPN 日志的记录级别设置为 3 （错误）。将 VPN 日志级别设置为 4 或更高的严重性（“警告”、“通知”、“信息”或“调试”）可能会导致 管理中心过载。

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。

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

feature	指定要为其启用调试的功能。若要查看可用功能，请使用 **debug ?** 命令获取 CLI 帮助。
subfeature	（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。
level	（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
show debug	显示当前活动的调试设置。
undebug	禁用功能调试。此命令与 **no debug** 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。
accounting	（可选）启用 AAA 记帐调试。
authentication	（可选）启用 AAA 身份验证调试。
authorization	（可选）启用 AAA 授权调试。
common	（可选）指定 AAA 通用调试级别。使用 ? 查看可用的级别。
internal	（可选）启用 AAA 内部调试。
shim	（可选）指定 AAA shim 调试级别。使用 ? 查看可用的级别。
url-redirect	（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
show debug aaa	显示 AAA 当前的活动调试设置。
undebug aaa	禁用 AAA 的调试。此命令与 **no debug aaa** 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。
ca	（可选）指定 PKI 调试级别。可以使用 ? 查看可用子功能。
condition	（可选）指定 IPsec/ISAKMP 调试过滤器。可以使用 ? 查看可用过滤器。

engine	（可选）指定 crypto 引擎调试级别。可以使用 ? 查看可用级别。
ike-common	（可选）指定 IKE 常用调试级别。可以使用 ? 查看可用级别。
ikev1	（可选）指定 IKE 版本 1 调试级别。可以使用 ? 查看可用级别。
ikev2	（可选）指定 IKE 版本 2 调试级别。可以使用 ? 查看可用级别。
ipsec	（可选）指定 IPsec 调试级别。使用 ? 可查看可用的级别。
condition	（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。
vpnclient	（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。

Related Commands

命令	说明
show debug crypto	显示当前处于活动状态的适用于 crypto 的调试设置。
undebug crypto	禁用对 crypto 的调试。此命令与 **no debug crypto** 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

crypto ca	启用对 *crypto ca* 的调试。使用 ? 查看可用的子功能。
cluster	（可选）指定 PKI 集群调试级别。可以使用 ? 查看可用级别。
cmp	（可选）指定 CMP 交易调试级别。可以使用 ? 查看可用级别。
messages	（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。
periodic-authentication	（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。
scep-proxy	（可选）指定 SCEP 代理调试级别。可以使用 ? 查看可用级别。
server	（可选）指定本地 CA 服务器调试级别。可以使用 ? 查看可用级别。
transactions	（可选）指定 PKI 交易调试级别。可以使用 ? 查看可用级别。
trustpool	（可选）指定信任池调试级别。使用 ? 查看可用的级别。
1-255	（可选）指定调试级别。

Command Default 默认调试级别为 1。

Related Commands

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

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

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

Command Default 默认调试级别为 1。

Related Commands

命令	说明
show debug crypto ikev1	显示 IKEv1 的当前活动调试设置。
undebug crypto ikev1	禁用 IKEv1 调试。此命令与 **no debug crypto ikev1** 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

ikev2	启用调试 *ikev2*。使用 ? 查看可用的子功能。
ha	（可选）指定 IKEv2 HA 调试级别。使用 ? 查看可用的级别。
platform	（可选）指定 IKEv2 平台调试级别。使用 ? 查看可用的级别。
protocol	（可选）指定 IKEv2 协议调试级别。使用 ? 查看可用的级别。
timers	（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
show debug crypto ikev2	显示 IKEv2 的当前活动调试设置。
undebugcrypto ikev2	禁用针对 IKEv2 的调试。此命令与 **no debug crypto ikev2** 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*］

Syntax Description

ipsec	启用对 *ipsec* 的调试要使用？请查看可用的子功能。
1-255	（可选）指定调试级别。

Command Default 默认调试级别为 1。

Related Commands

命令	说明
show debug crypto ipsec	显示 IPsec 的当前活动调试设置。
undebugcrypto ipsec	禁用对 IPsec 的调试。此命令与 **no debug crypto ipsec** 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*］

Syntax Description

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

Command Default 默认调试级别为 1。

Related Commands

命令	说明
show debug ldap	显示 LDAP 的当前活动调试设置。
undebugldap	禁用对 LDAP 的调试。此命令与 **no debug ldap** 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*］

Syntax Description

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

Command Default

默认调试级别为 1。

Related Commands

命令	说明
show debug ssl	显示 SSL 当前的活动调试设置。
undebug ssl	禁用对 SSL 的调试。此命令与 **no debug ssl** 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。
anyconnect	（可选）指定 WebVPN 安全客户端 调试级别。使用 ? 可查看可用的级别。
chunk	（可选）指定 WebVPN 分块调试级别。使用 ? 可查看可用的级别。
cifs	（可选）指定 WebVPN CIFS 调试级别。使用 ? 可查看可用的级别。
citrix	（可选）指定 WebVPN Citrix 调试级别。使用 ? 可查看可用的级别。
compression	（可选）指定 WebVPN 压缩调试级别。使用 ? 可查看可用的级别。
condition	（可选）指定 WebVPN 过滤条件调试级别。使用 ? 可查看可用的级别。
cstp-auth	（可选）指定 WebVPN CSTP 身份验证调试级别。使用 ? 可查看可用的级别。
customization	（可选）指定 WebVPN 自定义调试级别。使用 ? 可查看可用的级别。
failover	（可选）指定 WebVPN 故障切换调试级别。使用 ? 可查看可用的级别。
html	（可选）指定 WebVPN HTML 调试级别。使用 ? 可查看可用的级别。
javascript	（可选）指定 WebVPN Javascript 调试级别。使用 ? 可查看可用的级别。
kcd	（可选）指定 WebVPN KCD 调试级别。使用 ? 可查看可用的级别。

listener	（可选）指定 WebVPN 侦听程序调试级别。使用 ? 可查看可用的级别。
mus	（可选）指定 WebVPN MUS 调试级别。使用 ? 可查看可用的级别。
nfs	（可选）指定 WebVPN NFS 调试级别。使用 ? 可查看可用的级别。
request	（可选）指定 WebVPN 请求调试级别。使用 ? 可查看可用的级别。
response	（可选）指定 WebVPN 响应调试级别。使用 ? 可查看可用的级别。
saml	（可选）指定 WebVPN SAML 调试级别。使用 ? 可查看可用的级别。
session	（可选）指定 WebVPN 会话调试级别。使用 ? 可查看可用的级别。
task	（可选）指定 WebVPN 任务调试级别。使用 ? 可查看可用的级别。
transformation	（可选）指定 WebVPN 转换调试级别。使用 ? 可查看可用的级别。
url	（可选）指定 WebVPN URL 调试级别。使用 ? 可查看可用的级别。
util	（可选）指定 WebVPN 实用程序调试级别。使用 ? 可查看可用的级别。
xml	（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
show debug webvpn	显示 WebVPN 的当前活动调试设置。
undebug webvpn	禁用 WebVPN 的调试。此命令与 **no debug webvpn** 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。