



监控 VPN

- [监控 VPN 连接图，第 1 页](#)
- [监控 VPN 统计信息，第 1 页](#)

监控 VPN 连接图

有关以图形或表格形式为 ASA 显示 VPN 连接数据，请参阅以下屏幕。

Monitor IPsec Tunnels

Monitoring> VPN> VPN Connection Graphs> IPsec Tunnels

用于指定要查看或预备导出或打印的 IPsec 隧道类型的图形和表格。

Monitor Sessions

Monitoring> VPN> VPN Connection Graphs> Sessions

用于指定要查看或预备导出或打印的 VPN 会话类型的图形和表格。

监控 VPN 统计信息

有关显示特定远程访问或 LAN 到 LAN 会话的详细参数和统计信息，请参阅以下屏幕。参数和统计信息因会话协议而异。统计信息表的内容取决于您选择的连接类型。详细信息表显示每个会话的所有相关参数。

Monitor Session Window

Monitoring> VPN> VPN Statistics> Sessions

用于查看 ASA 的 VPN 会话统计信息。此窗格中的第二个表的内容取决于 Filter By 列表中的选择。



注释 管理员可跟踪处于非活动状态的用户数量，也可以查看统计信息。处于非活动状态时间最长的会话会被标记为空闲（并自动注销），这样就不会达到许可证容量限制，而且新用户也可以登录。您还可以使用 **show vpn-sessiondb** CLI 命令访问这些统计信息（请参阅相应版本的《思科 ASA 命令参考指南》）。

- **All Remote Access**

指示此表中的值与远程访问（IPSec 软件和硬件客户端）流量相关。

- **Username/Connection Profile** - 显示用户名或登录名以及会话的连接配置文件（隧道组）会话。

如果客户端使用数字证书进行身份验证，此字段显示此证书的主题 CN 或主题 OU。

- **Group Policy Connection Profile** - 显示会话的隧道组策略连接配置文件。

- **Assigned IP Address/Public IP Address** - 显示分配给此会话远程客户端的专用（“已分配”）IP 地址。这也称为“内部”或“虚拟”IP 地址，它允许客户端在专用网络上显示为主机。同样显示的还有此远程访问会话的客户端的公用 IP 地址。这也称为“外部”IP 地址。它通常由 ISP 分配给客户端，并且允许客户端在公用网络上充当主机。

- **Ping** - 发送 ICMP Ping（数据包互联网探测器）数据包测试网络连接。具体而言，ASA 将 ICMP 回应请求消息发送到选定主机。如果主机可以访问，它会返回回应应答消息，且 ASA 会显示一条带被测主机名称的成功消息，以及请求发送和收到响应之间经过的时间。如果系统由于任何原因无法访问（例如，主机故障、ICMP 未在主机上运行、路由未配置、中间路由器故障或者网络故障或堵塞），ASA 会显示一个带被测主机名称的错误屏幕。

- **Logout By** - 选择用于过滤要被注销的会话的条件。如果您选择除 --All Sessions-- 外的任意选项，位于 Logout By 列表右侧的框会变为活动状态。如果您为 Logout By 选择值 Protocol，此框会变为一个列表，您可以从中选择用作注销过滤器的协议类型。此列表的默认值是 IPsec。对于 Protocol 以外的所有选项，您必须在此列中提供适当的值。

监控主用 VPN 会话

监控 > VPN > VPN 统计信息 > 会话

用于查看按用户名、IP 地址、地址类型或公用地址排序的 Secure Client 会话。

Monitor VPN Session Details

Monitoring > VPN > VPN Statistics > Sessions > Details

用于查看关于选定会话的配置设置、统计和状态信息。

- **NAC Result and Posture Token**

仅当您已在 ASA 上配置网络准入控制时，ASDM 才会在此列中显示值。

- **Accepted** - ACS 已成功验证远程主机的终端安全评估。
- **Rejected** - ACS 未能成功验证远程主机的终端安全评估。

- “豁免” - 根据 ASA 上配置的“终端安全评估验证豁免”列表，远程主机被豁免终端安全评估验证。
- Non-Responsive - 远程主机没有响应 EAPoUDP Hello 消息。
- Hold-off - ASA 在终端安全评估验证成功后丢失与远程主机的 EAPoUDP 通信。
- N/A - 根据 VPN NAC 组策略，已为远程主机禁用 NAC。
- Unknown - 终端安全评估验证正在进行中。

终端安全评估标记是可在访问控制服务器上配置的信息文本字符串。ACS 将终端安全评估标记下载至 ASA，以实现协助系统监控、报告、调试和记录的参考用途。在 NAC 结果之后出现的典型终端安全评估标记如下：Healthy、Checkup、Quarantine、Infected 或 Unknown。

Session Details 窗格中的 Details 选项卡会显示以下列：

- ID - 动态分配给会话的唯一 ID。ID 用作此会话的 ASA 索引。它使用此索引维护和显示会话的相关信息。
- Type - 会话类型：IKE、IPSec 或 NAC。
- Local Addr.、Subnet Mask、Protocol、Port、Remote Addr.、Subnet Mask、Protocol 和 Port - 分配给实际（本地）对等体的地址和端口，以及出于外部路由用途分配给此对等体的地址和端口。
- Encryption - 此会话正在使用的数据加密算法（如果有）。
- Assigned IP Address and Public IP Address - 显示分配给此会话远程对等体的专用 IP 地址。也称为内部或虚拟 IP 地址，分配的 IP 地址允许远程对等体似乎位于专用网络上。第二个字段显示此会话的远程计算机的公用 IP 地址。公用 IP 地址也称为外部 IP 地址，通常由 ISP 分配给远程计算机。它允许远程计算机在公用网络上充当主机。
- Other - 与此会话关联的其他属性。

以下属性应用于 IKE 会话、IPsec 会话和 NAC 会话：

- Revalidation Time Interval - 每次成功的终端安全评估验证之间所需的间隔，以秒为单位。
- Time Until Next Revalidation - 如果上次终端安全评估验证尝试未成功，则为 0。否则，为重新验证时间间隔与上次成功终端安全评估验证以来的秒数之间的差值。
- Status Query Time Interval - 每次成功的终端安全评估验证或状态查询响应和下次状态查询响应之间允许的时间，以秒为单位。状态查询是 ASA 向远程主机发出的请求，指示主机在上次终端安全评估验证后是否有任何终端安全评估更改。
- EAPoUDP Session Age - 自上次成功的终端安全评估验证起经过的秒数。
- Hold-Off Time Remaining - 如果上次终端安全评估验证成功，则为 0 秒。否则，为下一终端安全评估验证尝试之前剩余的秒数。
- Posture Token - 访问控制服务器上可配置的信息文本字符串。ACS 将终端安全评估标记下载至 ASA，以实现协助系统监控、报告、调试和记录的参考用途。典型的终端安全评估标记为 Healthy、Checkup、Quarantine、Infected 或 Unknown。

- Redirect URL- 终端安全评估验证或无客户端身份验证之后，ACS 会将此会话的访问策略下载到 ASA。Redirect URL 是访问策略负载的可选部分。ASA 将此远程主机的所有 HTTP（端口 80）和 HTTPS（端口 443）请求重定向至“重定向 URL”（如果有）。如果访问策略不包含“重定向 URL”，ASA 不会重定向来自远程主机的 HTTP 和 HTTPS 请求。

重定向 URL 保持有效，直到 IPsec 会话结束或直到终端安全评估重新验证为止，对此，ACS 下载新的访问策略，其中可以包含其他重新定向 URL 或不包含重定向 URL。

More - 按此按钮可重新验证或初始化此会话或隧道组。

ACL 选项卡显示包含与此会话匹配的 ACE 的 ACL。

Monitor Cluster Loads

Monitoring > VPN > VPN Statistics > Cluster Loads

用于查看 VPN 负载均衡集群中的服务器之间的当前流量负载分布。如果服务器不是集群的一部分，您将收到一条表示此服务器不参与 VPN 负载均衡集群的信息消息。

Monitor Crypto Statistics

Monitoring > VPN > VPN Statistics > Crypto Statistics

用于查看 ASA 上当前活动用户和管理员会话的加密统计信息。表中每一行表示一则加密统计信息。

Monitor Compression Statistics

Monitoring > VPN > VPN Statistics > Compression Statistics

用于查看 ASA 上当前活动用户和管理员会话的压缩统计信息。表中每一行表示一则压缩统计信息。

Monitor Encryption Statistics

Monitoring > VPN > VPN Statistics > Encryption Statistics

用于查看 ASA 上当前活动用户和管理员会话使用的数据加密算法。表中每一行表示一个加密算法类型。

Monitor Global IKE/IPsec Statistics

Monitoring > VPN > VPN Statistics > Global IKE/IPSec Statistics

用于查看 ASA 上当前活动用户和管理员会话的全局 IKE/IPsec 统计信息。表中每一行表示一则全局统计信息。

Monitor NAC Session Summary

用于查看活动和积累的网络准入控制会话。

- Active NAC Sessions - 有关要进行终端安全评估验证的远程对等体的常规统计信息。
- Cumulative NAC Sessions - 有关要进行或已经进行终端安全评估验证的远程对等体的常规统计信息。
- Accepted - 传递终端安全评估验证并由访问控制服务器授予访问策略的对等体的数量。

- **Rejectd** - 终端安全评估验证失败或访问控制服务器未授予访问策略的对等体的数量。
- **Exempted** - 由于与 ASA 上配置的“终端安全评估验证豁免”列表中的条目匹配而不进行终端安全评估验证的对等体数量。
- **Non-responsive** - 未响应终端安全评估验证的经由 UDP 的可扩展身份验证协议 (EAP) 请求的对等体的数量。未在其中运行 CTA 的对等体不响应这些请求。如果 ASA 配置支持无客户端主机，访问控制服务器会为这些对等体将与无客户端主机关联的访问策略下载至 ASA。否则，ASA 将分配 NAC 默认策略。
- **Hand-off** - 终端安全评估验证成功后，ASA 丢失 EAPoUDP 通信的对等体的数量。NAC Hold Timer 属性 (Configuration > VPN > NAC) 可确定此事件类型和下次终端安全评估验证尝试之间的延迟。
- **N/A** - 根据 VPN NAC 组策略禁用 NAC 的对等体的数量。
- **Revalidate All** - 如果对等体的终端安全评估状态或分配的访问策略（即下载的 ACL）已发生变化，请点击此按钮。点击此按钮可对 ASA 管理的所有 NAC 会话发起新的无条件终端安全评估验证。在您点击此按钮之前，有效的终端安全评估验证和分配的访问策略仍然有效，直到新的终端安全评估验证成功或失败。点击此按钮不会影响已豁免终端安全评估验证的会话。
- **Initializa All** - 如果对等体的终端安全评估状态或分配的访问策略（即下载的 ACL）已发生变化，而且您想要清除分配给会话的资源，可以点击此按钮。点击此按钮可清除 EAPoUDP 关联和用于 ASA 管理的所有 NAC 会话的终端安全评估验证的已分配访问策略，并发起新的无条件终端安全评估验证。NAC 默认 ACL 在重新验证期间是有效的，因此，会话初始化可能会中断用户流量。点击此按钮不会影响已豁免终端安全评估验证的会话。

Monitor Protocol Statistics

Monitoring > VPN > VPN Statistics > Protocol Statistics

用于查看 ASA 上当前活动用户和管理员会话使用的协议。表中每一行表示一种协议类型。

Monitor VLAN Mapping Sessions

用于查看分配至出口 VLAN 的会话的数量，这取决于每个所用组策略的 Restrict Access to VLAN 参数的值。ASA 会将所有流量转发至指定的 VLAN。

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。