威胁检测

以下主题介绍如何配置威胁检测统计信息和扫描威胁检测。

检测威胁

ASA 上的威胁检测是抵御攻击的第一道防线。威胁检测在第 3 层和第 4 层上工作，为设备上的流量制定基准，基于流量模式分析丢包统计信息，并累计“前面的”报告。相比之下，提供 IPS 或下一代 IPS 服务的模块可在 ASA 允许的流量中识别和减轻高达第 7 层的攻击媒介，但不能查看已被 ASA 丢弃的流量。因此，威胁检测和 IPS 能够协同工作，以提供更加全面的威胁防御。

威胁检测由以下要素组成：

- 为各种威胁收集的不同级别统计信息。

  威胁检测统计信息可帮助您管理ASA面临的威胁，例如，如果启用扫描威胁检测，则查看统计信息可帮助您分析威胁。可以配置两种类型的威胁检测统计信息：

  - 基本威胁检测统计信息 - 包括有关针对整个系统的攻击活动的信息。默认情况下启用基本威胁检测统计信息，并且不会对性能产生影响。请参阅基本威胁检测统计信息， 第 2 页。
  - 高级威胁检测统计信息 - 在对象级别跟踪活动，以便 ASA 可报告单个主机、端口、协议或 ACL 的活动。高级威胁检测统计信息会对性能产生重要影响，具体情况视收集的统计信息而定，因此，在默认情况下，仅启用 ACL 统计信息。请参阅高级威胁检测统计信息， 第 2 页。

- 扫描威胁检测，其确定主机何时执行扫描。或者，可以避开任何被确定为扫描威胁的主机。请参阅扫描威胁检测， 第 3 页。

- VPN 服务的威胁检测，可用于防止来自 IPv4 地址的以下类型的 VPN 攻击：
  - 远程访问 VPN 验证尝试失败过多，例如用户名/密码暴力扫描。
  - 客户端启动攻击，即攻击者从一台主机发起但未完成与远程访问 VPN 头端的重复连接尝试。
  - 尝试访问无效的 VPN 服务，即仅供内部使用的服务。

这些攻击即使未能成功获取访问权，也会消耗计算资源，有时甚至会导致拒绝服务。请参阅为 VPN 服务配置威胁检测，第 9 页。

基本威胁检测统计信息

使用基本威胁检测统计信息，ASA 可监控由于以下原因被丢弃的数据包和安全事件的比率：

- 被 ACL 拒绝。
- 数据包格式错误（例如，invalid-ip-header 或 invalid-tcp-hdr-length）。
- 超出连接限制（系统范围的资源限制和在配置中设定的限制）。
- 检测到 DoS 攻击（例如，无效 SPI、状态防火墙检查故障）。
- 基本防火墙检查失败。此选项是一个组合比率，包含此列表中所有与防火墙有关的丢包。它不包括非防火墙相关丢弃，如接口过载、使应用检查失败的数据包以及检测到的扫描攻击。
- 检测到可疑的 ICMP 数据包。
- 数据包未通过应用检查。
- 接口过载。
- 检测到扫描攻击。此选项监控扫描攻击；例如，第一个 TCP 数据包并非 SYN 数据包，或者 TCP 连接未通过三方握手。例如，完整扫描威胁检测采用此扫描攻击频率信息，通过将主机分类为攻击者并自动避开这些主机，从而根据此信息采取行动。
- 不完整会话检测，例如检测到 TCP SYN 攻击或检测到无返回数据的 UDP 会话攻击。

当 ASA 检测到威胁时，会立即发送系统日志消息 (733100)。ASA 会跟踪两种速率类型：一段间隔的平均事件速率和较短突发间隔的突发事件速率。突发速率间隔为平均速率间隔的 1/30 或 10 秒，以较大者为准。对于收到的每个事件，ASA 会检查平均速率限制和突发速率限制；如果两种速率均超出限制，则 ASA 会发送两条单独的系统消息，对于每个突发期间的每种速率类型最多发送一条消息。

基本威胁检测仅当有丢包或潜在威胁时影响性能；即使在这种情况下，对性能的影响仍然可以忽略。

高级威胁检测统计信息

高级威胁检测统计信息显示单个对象（例如，主机、端口、协议或 ACL）允许和丢弃的流量速率。

注意 启用高级统计信息可能会影响ASA性能，具体取决于启用的统计信息类型。启用主机统计信息会严重影响性能；如果是高流量负载，可能要考虑临时启用这种统计信息类型。不过，端口统计信息造成的影响较小。

扫描威胁检测

典型的扫描攻击包含测试子网中每个IP地址可达性（通过扫描子网中的多台主机或扫描主机或子网中的多个端口）的主机。扫描威胁检测功能确定主机何时执行扫描。ASA 威胁检测扫描与基于流量签名的 IPS 扫描检测不同，前者维护着广泛的数据库，其中包含可用来分析扫描活动的主机统计信息。

主机数据库跟踪可疑的活动（例如没有返回活动的连接、访问关闭的服务端口、如非随机IPID等易受攻击的 TCP 行为以及更多行为）。

如果超出扫描威胁速率，ASA会发送系统日志消息(733101)并会选择性地避开攻击者。ASA会跟踪两种速率类型：一段间隔的平均事件速率和较短突发间隔的突发事件速率。突发事件率为平均速率间隔的 1/30 或 10 秒，以较高者为准。对于检测到的被视为属于扫描攻击的每个事件，ASA 会检查平均速率限制和突发速率限制。如果从主机发送的流量超出任一速率，则该主机被视为攻击者。如果主机接收的流量超出任一速率，则该主机被视为目标。

下表列出扫描威胁检测的默认速率限制。

表 *1:* 扫描威胁检测的默认速率限制

平均速率	突发速率
在过去 600 秒内 5 个丢包/秒。	在过去 20 秒内 10 个丢包/秒。
在过去 3600 秒内 5 个丢包/秒。	在过去 120 秒内 10 个丢包/秒。

注意 扫描威胁检测功能可能会严重影响ASA的性能和内存，同时会创建和收集基于主机和子网的数据结构及信息。

威胁检测准则

安全情景准则

除了高级威胁统计信息和 VPN 服务，仅支持单一模式的威胁检测。在多模式下，仅支持 TCP 拦截统计信息。

监控的流量类型

- 统计时，只监控通过设备的流量，不监控传入流量。

- ACL 拒绝的流量不会触发扫描威胁检测；只有允许通过 ASA 和创建数据流的流量才会受扫描威胁检测影响。
- 对于 VPN 服务，只监控来自 IPv4 地址的设备流量。

威胁检测的默认设置

默认情况下，启用基本威胁检测统计信息。

下表列出了默认的设置。可以使用 中的 **show running-config all threat-detection** 命令查看所有这些默认设置。

对于高级统计信息，默认情况下，启用 ACL 统计信息。

对于 VPN 服务威胁检测，默认情况下禁用所有服务。

表 *2:* 基本的威胁检测默认设置

	触发器设置	
丢包原因	平均速率	突发速率
• 检测到 DoS 攻击 • 数据包格式错误 • 超出连接限制 • 检测到可疑的 ICMP 数据包	在过去 600 秒内 100 个丢包/秒。	在过去 20 秒内 400 个丢包/秒。
	在过去 3600 秒内 80 个丢包/秒。	在过去 120 秒内 320 个丢包/秒。
检测到扫描攻击	在过去 600 秒内 5 个丢包/秒。	在过去 20 秒内 10 个丢包/秒。
	在过去 3600 秒内 4 个丢包/秒。	在过去 120 秒内 8 个丢包/秒。
检测不完整会话，例如检测到 TCP SYN 攻击或检测到无返回数据的 UDP 会话攻击（组合）	在过去 600 秒内 100 个丢包/秒。	在过去 20 秒内 200 个丢包/秒。
	在过去 3600 秒内 80 个丢包/秒。	在过去 120 秒内 160 个丢包/秒。
被 ACL 拒绝	在过去 600 秒内 400 个丢包/秒。	在过去 20 秒内 800 个丢包/秒。
	在过去 3600 秒内 320 个丢包/秒。	在过去 120 秒内 640 个丢包/秒。

丢包原因	触发器设置	
	平均速率	突发速率
• 基本防火墙检查失败 • 数据包未通过应用检查	在过去 600 秒内 400 个丢包/秒。	在过去 20 秒内 1600 个丢包/秒。
	在过去 3600 秒内 320 个丢包/秒。	在过去 120 秒内 1280 个丢包/秒。
接口过载	在过去 600 秒内 2000 个丢包/秒。	在过去 20 秒内 8000 个丢包/秒。
	在过去 3600 秒内 1600 个丢包/秒。	在过去 120 秒内 6400 个丢包/秒。

配置威胁检测

默认情况下，启用基本威胁检测统计信息，而且您可能只需要威胁检测服务。如果要实施其他威胁检测服务，请使用以下操作步骤。

过程

步骤 1 配置基本威胁检测统计信息，第 5 页。

基本威胁检测统计信息包括可能与攻击（例如，DoS 攻击）有关的活动。

步骤 2 配置高级威胁检测统计信息，第 6 页。

步骤 3 配置扫描威胁检测，第 8 页。

步骤 4 为 VPN 服务配置威胁检测，第 9 页。

配置基本威胁检测统计信息

默认情况下，启用基本威胁检测统计信息。可以禁用此功能，或者，如果已禁用，可以再次启用。

过程

步骤 1 启用基本威胁检测统计信息（如果以前已禁用）。

threat-detection basic-threat

示例：

```
hostname(config)# threat-detection basic-threat
```

默认情况下，启用基本威胁检测。使用 **no threat-detection basic-threat** 禁用此功能。

步骤 2 （可选）更改一种或多种事件类型的默认设置。

threat-detection rate {**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**} **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

有关每种事件类型的说明，请参阅第 8-1 页的“基本威胁检测统计信息”。

当您将此命令与 **scanning-threat** 关键字配合使用时，还可以在扫描威胁检测中使用此命令。如果不配置基本威胁检测，依然可以将此命令与 **scanning-threat** 关键字配合使用，以配置扫描威胁检测的速率限制。

可以为每种事件类型配置最多三个不同的速率间隔。

示例：

```
hostname(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60 burst-rate
 100
```

配置高级威胁检测统计信息

您可以将 ASA 配置为收集各种统计信息。默认情况下，启用 ACL 统计信息。要启用其他统计信息，请执行以下步骤。

过程

步骤 1 （可选）启用全部统计信息。

threat-detection statistics

要仅启用某些统计信息，请为每个统计信息类型输入此命令（如此操作步骤后面所示），但不要输入不带任何选项的命令。可以输入 **threat-detection statistics**（不带任何选项），然后通过输入具有统计信息特定选项（例如，**threat-detection statistics host number-of-rate 2**）的命令自定义某些统计信息。如果输入 **threat-detection statistics**（不带任何选项），然后输入特定统计信息的命令，但不带任何统计信息特定选项，则该命令没有任何影响，因为命令已启用。

如果输入此命令的 **no** 形式，它会删除所有 **threat-detection statistics** 命令，包括默认情况下已启用的 **threat-detection statistics access-list** 命令。

示例：

```
hostname(config)# threat-detection statistics
```

步骤 2 （可选）启用 ACL 统计信息（如果以前被禁用）。

threat-detection statistics access-list

默认情况下，启用 ACL 统计信息。ACL 统计信息只能使用 **show threat-detection top access-list** 命令禁用。

示例：

```
hostname(config)# threat-detection statistics access-list
```

步骤 3 （可选）为主机（**host** 关键字）、TCP 和 UDP 端口（**port** 关键字）或者非 TCP/UDP IP 协议（**protocol** 关键字）配置统计信息。

threat-detection statistics {**host** | **port** | **protocol**} [**number-of-rate** {**1** | **2** | **3**}]

number-of-rate 关键字设置为统计信息维护的速率间隔数量。默认速率间隔数为 **1**，该值将保持较低的内存利用率。要查看更多速率间隔，请将该值设置为 **2** 或 **3**。例如，如果将该值设置为 **3**，则查看过去 1 小时、8 小时和 24 小时的数据。如果将此关键字设置为 **1**（默认值），则仅维护最短速率间隔的统计信息。如果将该值设置为 **2**，则维护最短的两个间隔。

只要主机处于活动状态并且位于扫描威胁主机数据库中，即可累积主机统计信息。处于非活动状态 10 分钟后，将从数据库中删除主机（并清除统计信息）。

示例：

```
hostname(config)# threat-detection statistics host number-of-rate 2
hostname(config)# threat-detection statistics port number-of-rate 2
hostname(config)# threat-detection statistics protocol number-of-rate 3
```

步骤 4 （可选）配置 TCP 拦截所拦截的攻击的统计信息。

threat-detection statistics tcp-intercept [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]

其中：

- **rate-interval** 设置历史监控窗口的大小，该值介于 1 到 1440 分钟之间。默认值为 30 分钟。在此间隔内，ASA 将对攻击数量抽样 30 次。
- **Burst-rate** 为系统日志消息生成设置阈值，该值介于 25 到 2147483647 之间。默认值为每秒 400 条消息。超出突发速率时，将生成系统日志消息 733104。
- **Average-rate** 为系统日志消息生成设置平均速率阈值，该值介于 25 到 2147483647 之间。默认值为每秒 200 条消息。超出平均速率时，将生成系统日志消息 733105。

要启用 TCP 拦截，请参阅保护服务器不受 SYN 洪流 DoS 攻击（TCP 拦截）。

注释
此命令在多情景模式下可用，不同于其他威胁检测命令。

示例：

```
hostname(config)# threat-detection statistics tcp-intercept rate-interval 60
burst-rate 800 average-rate 600
```

配置扫描威胁检测

可以配置扫描威胁检测，以识别攻击者，或者避开攻击者。

您可以将ASA配置为发送有关攻击者的系统日志消息，也可以自动避开主机。默认情况下，主机被标识为攻击者后，将生成系统日志消息 730101。当您预期主机会发送大量信息时，请确保将地址从规避中删除。例如，如果启用了 PIM 组播，则 PIM 路由器或 PIM 信息将被放弃。

过程

步骤 1 启用扫描威胁检测。

threat-detection scanning-threat [**shun** [**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*}]]

默认情况下，主机被标识为攻击者后，将生成系统日志消息 733101。多次输入此命令以标识无需回避的多个 IP 地址或网络对象组。

示例：

```
hostname(config)# threat-detection scanning-threat shun except
ip-address 10.1.1.0 255.255.255.0
```

步骤 2 （可选）为攻击主机设置避开持续时间。

threat-detection scanning-threat shun duration *seconds*

示例：

```
hostname(config)# threat-detection scanning-threat shun duration 2000
```

步骤 3 （可选）更改 ASA 将主机标识为攻击者或目标时的默认事件限制。

threat-detection rate scanning-threat rate-interval *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

如果在基本威胁检测配置过程中已配置了此命令，则那些设置将与扫描威胁检测功能共享；不能为基本和扫描威胁检测配置独立速率。如果不使用此命令设置速率，则将默认值用于扫描威胁检测功能和基本威胁检测功能。通过输入不同的命令，最多可配置三个不同的速率间隔。

示例：

```
hostname(config)# threat-detection rate scanning-threat rate-interval 1200
average-rate 10 burst-rate 20

hostname(config)# threat-detection rate scanning-threat rate-interval 2400
```

```
average-rate 10 burst-rate 20
```

为 VPN 服务配置威胁检测

您可以启用 VPN 服务威胁检测，以帮助防止来自 IPv4 地址的拒绝服务 (DoS) 攻击。针对以下类型的攻击，可提供单独的服务：

- 远程访问 VPN 登录身份验证。通过在密码泄露攻击中反复开始登录尝试，攻击者可以消耗用于身份验证尝试的资源，从而阻止真实用户登录 VPN。
- 客户端启动攻击，即攻击者从一台主机发起但未完成与远程访问 VPN 头端的重复连接尝试。与密码泄露攻击类似，这种攻击也会消耗资源，并阻止有效用户连接到 VPN。
- 尝试连接到无效的 VPN 服务，即服务仅供内部使用。尝试这种连接的 IP 地址会立即被避开。

启用这些服务后，系统会自动避开超过阈值的主机，以防止进一步的尝试。您可以使用地址的 **no shun** 命令来手动删除回避。

要手动将服务的计数器重置为 0，请使用 **clear threat-detection service** 命令。

开始之前

在决定适当的抑制值和阈值时，请考虑在您的环境中使用 NAT。如果使用 PAT，使许多请求来自同一 IP 地址，则应考虑提高身份验证失败和客户端启动服务的值，以确保有效用户有足够的时间完成连接。例如，在一家酒店，许多客户可能会在很短的时间内尝试连接。

过程

步骤 1 启用远程访问 VPN 身份验证失败的威胁检测。

threat-detection service remote-access-authentication hold-down *minutes* **threshold** *count*

其中：

- **hold-down** *minutes* 定义了从最后一次失败算起的抑制时间。攻击者的 IPv4 地址必须在前一次失败的抑制期内达到连续失败的阈值次数，才能触发回避。例如，如果抑制时间为 10 分钟，阈值为 20，并且来自单个 IPv4 地址的连续 20 次身份验证失败，且任何两次连续失败之间的时间间隔不超过 10 分钟，则将避开该源 IPv4 地址。可以指定介于 1 和 1440 分钟之间的时间。
- **threshold** *count* 定义在抑制期间必须发生的、会触发回避的失败尝试次数。可以指定 1 到 100 之间的阈值。

要禁用该服务，请使用以下命令：

no threat-detection service remote-access-authentication

示例：

下面的示例设置的指标是 20 分钟内发生 10 次故障。

```
ciscoasa(config)# threat-detection service remote-access-authentication
hold-down 10 threshold 20
```

步骤 2 启用远程访问 VPN 客户端启动时的威胁检测。

threat-detection service remote-access-client-initiations hold-down *minutes* **threshold** *count*

其中：

- **hold-down** *minutes* 定义了从最后一次启动算起的抑制时间。必须在上一次启动的抑制期内达到连续启动的阈值次数，才能触发对客户端 IPv4 地址的回避。例如，如果抑制时间为 10 分钟，阈值为 20，并且来自单个 IPv4 地址的连续启动次数为 20 次，且任何两次连续启动之间的时间间隔不超过 10 分钟，则将避开该源 IPv4 地址。可以指定介于 1 和 1440 分钟之间的时间。
- **threshold** *count* 定义在抑制期间必须发生的发起次数才能触发规避。可以指定 5 到 100 之间的阈值。

要禁用该服务，请使用以下命令：

no threat-detection service remote-access-client-initiations

示例：

下面的示例设置的指标是 20 分钟内启动 10 次。

```
ciscoasa(config)# threat-detection service remote-access-client-initiations
hold-down 10 threshold 20
```

步骤 3 对尝试连接无效 VPN 服务的行为启用威胁检测。

threat-detection service invalid-vpn-access

要禁用该服务，请使用以下命令：

no threat-detection service invalid-vpn-access

示例：

下面的示例启用了无效 VPN 访问服务。

```
ciscoasa(config)# threat-detection service invalid-vpn-access
```

监控威胁检测

以下主题介绍如何监控威胁检测和查看流量统计信息。

监控基本威胁检测统计信息

要显示基本威胁检测统计信息，请使用以下命令：

show threat-detection rate [**min-display-rate** *min_display_rate*] [**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**]

min-display-rate *min_display_rate* 参数将显示内容限制为超出每秒最低事件显示速率的统计信息。可以将 *min_display_rate* 设置在 0 到 2147483647 之间。

其他参数可以让您将显示内容限制为特定类别。有关每种事件类型的说明，请参阅基本威胁检测统计信息，第 2 页。

输出显示两个固定时间段中的平均速率（单位：事件数/秒）：最后 10 分钟和最后 1 小时。它还显示：最后完成的突发间隔（平均速率间隔的 1/30 或 10 秒，以较大者为准）内当前突发速率（单位：事件数/秒）；超出（被触发）速率的次数；以及时间段中的事件总数。

对于完成的总共 30 个突发间隔，ASA 在每个突发期间的末尾存储计数。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率间隔为 20 分钟，则突发间隔为 20 秒。如果上一个突发间隔为 3:00:00 至 3:00:20，并且您在 3:00:25 使用 **show** 命令，则最后 5 秒不会包含在输出中。

此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。这种情况下，ASA 会计算过去 29 个完成间隔的总事件数再加上未完成突发间隔到目前的事件数。此例外可让您实时监控事件的大幅增加。

可以使用 **clear threat-detection rate** 命令清除统计信息。

以下是 **show threat-detection rate** 命令的输出示例：

```
hostname# show threat-detection rate

                        Average(eps)    Current(eps) Trigger         Total events
  10-min ACL  drop:                0               0       0                   16
  1-hour ACL  drop:                0               0       0                  112
  1-hour SYN attck:                5               0       2                21438
  10-min  Scanning:                0               0      29                  193
  1-hour  Scanning:              106               0      10               384776
  1-hour Bad  pkts:               76               0       2               274690
  10-min  Firewall:                0               0       3                   22
  1-hour  Firewall:               76               0       2               274844
  10-min DoS attck:                0               0       0                    6
  1-hour DoS attck:                0               0       0                   42
  10-min Interface:                0               0       0                  204
  1-hour Interface:               88               0       0               318225
```

监控高级威胁检测统计信息

要监控高级威胁检测统计信息，请使用下表中显示的命令。显示内容输出显示以下内容：

- 固定时间段内的平均速率（单位：事件数/秒）。
- 上一个完整突发间隔（平均速率间隔的 1/30 或 10 秒，两者中取较大的一个）内的当前突发速率（单位：事件数/秒）

- 超过速率的次数（仅适用于丢弃流量统计信息）
- 固定时间段内的事件总数。

对于完成的总共 30 个突发间隔，ASA 在每个突发期间的末尾存储计数。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率间隔为 20 分钟，则突发间隔为 20 秒。如果上一个突发间隔为 3:00:00 至 3:00:20，并且您在 3:00:25 使用 **show** 命令，则最后 5 秒不会包含在输出中。

此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。这种情况下，ASA 会计算过去 29 个完成间隔的总事件数再加上未完成突发间隔到目前的事件数。此例外可让您实时监控事件的大幅增加。

命令	目的
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top** [[**access-list** | **host** | **port-protocol**] [**rate-1** | **rate-2** | **rate-3**] | **tcp-intercept** [**all**] **detail**]]	显示前 10 条统计信息。如果不输入任何选项，将显示所有类别的前 10 条统计信息。 **min-display-rate** *min_display_rate* 参数将显示内容限制为超出每秒最低事件显示速率的统计信息。可以将 *min_display_rate* 设置在 0 到 2147483647 之间。 以下行将解释可选关键字。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top access-list** [**rate-1** | **rate-2** | **rate-3**]	要查看匹配数据包的前 10 个 ACE（包括允许和拒绝 ACE），请使用 **access-list** 关键字。允许和拒绝的流量在此显示内容中没有区别。如果使用 **threat-detection basic-threat** 命令启用基本威胁检测，则可以使用 **show threat-detection rate acl-drop** 命令跟踪 ACL 拒绝。 **rate-1** 关键字显示在显示内容中提供的最小固定速率间隔的统计信息；**rate-2** 显示第二大的速率间隔；如果定义了三个间隔，则 **rate-3** 显示最大的速率间隔。例如，显示内容显示最后 1 小时、8 小时和 24 小时的统计信息。如果设置为 **rate-1** 关键字，则 ASA 仅显示 1 小时的时间间隔。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top host** [**rate-1** | **rate-2** | **rate-3**]	要仅查看主机统计信息，请使用 **host** 关键字。**注意**：由于威胁检测算法，用作组合故障转移和状态链路的接口会在前 10 个主机中显示；这是预期行为，而且您可以在显示内容中忽略此 IP 地址。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top port-protocol** [**rate-1** | **rate-2** | **rate-3**]	要查看端口和协议统计信息，请使用 **port-protocol** 关键字。**port-protocol** 关键字显示端口和协议统计信息（必须为显示内容启用两者），并且显示 TCP/UDP 端口和 IP 协议类型的组合统计信息。TCP（协议 6）和 UDP（协议 17）未包含在 IP 协议的显示内容中；但是，TCP 和 UDP 端口包含在端口的显示内容中。如果仅启用这些类型中一个类型（端口或协议）的统计信息，则只能查看启用的统计信息。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top tcp-intercept** [**all**] **detail**]]	要查看 TCP 拦截统计信息，请使用 **tcp-intercept** 关键字。显示内容包含受到攻击的前 10 台受保护服务器。**all** 关键字显示所有被跟踪服务器的历史数据。**detail** 关键字显示历史记录采样数据。在该速率间隔内，ASA 会对攻击数量抽样 30 次，所以对于默认的 30 分钟期间，统计信息每 60 秒收集一次。

命令	目的
show threat-detection statistics [**min-display-rate** *min_display_rate*] **host** [*ip_address* [*mask*]]	显示所有主机或特定主机或子网的统计信息。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **port** [*start_port*[-*end_port*]]	显示所有端口或特定端口或端口范围的统计信息。
show threat-detection statistics [**min-display-rate** *min_display_rate*] **protocol** [*protocol_number* | *protocol*]	显示所有 IP 协议或特定协议的统计信息。 *protocol_number* 参数是介于 0 到 255 之间的整数。*protocol* 参数可以是 **ah**、**eigrp**、**esp**、**gre**、**icmp**、**icmp6**、**igmp**、**igrp**、**ip**、**ipinip**、**ipsec**、**nos**、**ospf**、**pcp**、**pim**、**pptp**、**snp**、**tcp**、**udp** 中的一个。

评估主机威胁检测统计信息

以下是 **show threat-detection statistics host** 命令的输出示例：

```
hostname# show threat-detection statistics host

                        Average(eps)    Current(eps) Trigger         Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0
  1-hour Sent byte:             2938              0       0             10580308
  8-hour Sent byte:              367              0       0             10580308
 24-hour Sent byte:              122              0       0             10580308
  1-hour Sent pkts:               28              0       0               104043
  8-hour Sent pkts:                3              0       0               104043
 24-hour Sent pkts:                1              0       0               104043
  20-min Sent drop:                9              0       1                10851
  1-hour Sent drop:                3              0       1                10851
  1-hour Recv byte:             2697              0       0              9712670
  8-hour Recv byte:              337              0       0              9712670
 24-hour Recv byte:              112              0       0              9712670
  1-hour Recv pkts:               29              0       0               104846
  8-hour Recv pkts:                3              0       0               104846
 24-hour Recv pkts:                1              0       0               104846
  20-min Recv drop:               42              0       3                50567
  1-hour Recv drop:               14              0       1                50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                0              0       0                  614
  8-hour Sent byte:                0              0       0                  614
 24-hour Sent byte:                0              0       0                  614
  1-hour Sent pkts:                0              0       0                    6
  8-hour Sent pkts:                0              0       0                    6
 24-hour Sent pkts:                0              0       0                    6
  20-min Sent drop:                0              0       0                    4
  1-hour Sent drop:                0              0       0                    4
  1-hour Recv byte:                0              0       0                  706
  8-hour Recv byte:                0              0       0                  706
 24-hour Recv byte:                0              0       0                  706
  1-hour Recv pkts:                0              0       0                    7
```

下表对输出进行了解释。

表 *3: show threat-detection statistics host*

字段	说明
Host	主机 IP 地址。
tot-ses	自主机添加到数据库后的该主机会话总数。
act-ses	主机当前参与的活动会话总数。
fw-drop	防火墙丢包数量。防火墙丢包是一个组合速率，其中包括在基本威胁检测中跟踪的与防火墙有关的所有丢包，包括 ACL 拒绝的数据包、错误数据包、超出连接限制的数据包、DoS 攻击数据包、可疑 ICMP 数据包、TCP SYN 攻击数据包以及无返回数据 UDP 会话攻击数据包。它不包括非防火墙相关丢弃，如接口过载、使应用检查失败的数据包以及检测到的扫描攻击。
insp-drop	因为数据包未通过应用检查而被丢弃的数据包的数量。
null-ses	空会话数量，空会话是指在 3 秒超时内未完成的 TCP SYN 会话，以及在会话开始后 3 秒内没有其服务器发送的任何数据的 UDP 会话。
bad-acc	对处于关闭状态的主机端口的不良访问尝试次数。当确定端口处于空会话中（请参阅 null-ses 字段说明）时，主机的端口状态被设为 HOST_PORT_CLOSE。任何访问该主机端口的客户端都会被立即分类为错误访问，无需等待超时。
Average(eps)	每个时间段内的平均速率（单位：事件数/秒）。 对于完成的总共 30 个突发间隔，ASA 在每个突发期间的末尾存储计数。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率间隔为 20 分钟，则突发间隔为 20 秒。如果上一个突发间隔为 3:00:00 至 3:00:20，并且您在 3:00:25 使用 **show** 命令，则最后 5 秒不会包含在输出中。 此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。这种情况下，ASA 会计算过去 29 个完成间隔的总事件数再加上未完成突发间隔到目前的事件数。此例外可让您实时监控事件的大幅增加。
Current(eps)	上一个完整突发间隔（平均速率间隔的 1/30 或 10 秒，两者中取较大的一个）内的当前突发速率（单位：事件数/秒）。对于 Average(eps) 说明中指定的示例，当前速率为 3:19:30 至 3:20:00 的速率
触发器	超出丢包速率限制的次数。对于发送和接收的字节和数据包行中标识的有效流量，此值始终为 0，因为对触发有效流量没有速率限制。
Total events	每个速率间隔内的事件总数。当前进行的未完成突发间隔不包括在事件总数中。此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。这种情况下，ASA 会计算过去29个完成间隔的总事件数再加上未完成突发间隔到目前的事件数。此例外可让您实时监控事件的大幅增加。

字段	说明
20-min, 1-hour, 8-hour, and 24-hour	这些固定速率间隔的统计信息。对于每个间隔： • Sent byte - 从主机成功发送的字节数。 • Sent pkts - 从主机成功发送的数据包数。 • Sent drop - 已从主机发送但因为是扫描攻击的一部分而被丢弃的数据包数。 • Recv byte - 主机成功接收的字节数。 • Recv pkts - 主机成功接收的数据包数。 • Recv drop - 主机已接收但因为是扫描攻击的一部分而被丢弃的数据包数。

监控被避开的主机、攻击者和攻击目标

要监控和管理回避的主机和攻击者以及扫描威胁检测目标，请使用以下命令。这些命令仅用于扫描威胁检测，不适用于其他服务。

- **show threat-detection shun**

  显示当前避开的主机。例如：

```
hostname# show threat-detection shun

Shunned Host List:
(outside) src-ip=10.0.0.13 255.255.255.255
(inside) src-ip=10.0.0.13 255.255.255.255
```

- **clear threat-detection shun** [*ip_address* [*mask*]]

  释放回避的主机。如果不指定 IP 地址，所有主机都将从避开列表清除。

  例如，要释放位于 10.1.1.6 的主机，请输入以下命令：

```
hostname# clear threat-detection shun 10.1.1.6
```

- **show threat-detection scanning-threat** [**attacker** | **target**]

  显示ASA确定为攻击者的主机（包括避开列表中的主机），并显示成为攻击目标的主机。如果不输入选项，将显示攻击者和攻击目标主机。例如：

```
hostname# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0 (l2l)
    192.168.1.249 (l2l)
Latest Attacker Host & Subnet List:
    192.168.10.234 (outside)
```

```
192.168.10.0 (outside)
192.168.10.2 (outside)
192.168.10.3 (outside)
192.168.10.4 (outside)
192.168.10.5 (outside)
192.168.10.6 (outside)
192.168.10.7 (outside)
192.168.10.8 (outside)
192.168.10.9 (outside)
```

监控 VPN 服务的威胁检测

您可以使用 syslog 和 show 命令监控 VPN 服务的威胁检测，具体说明见以下主题。

威胁检测 VPN 服务的系统日志监控

您可能会看到以下与这些服务相关的系统日志消息：

- %ASA-6-733200：威胁检测信息：消息

  此消息报告用于威胁检测的一般信息事件。

- %ASA-4-733201:威胁检测：服务[服务]对等体[对等体]：已超过阈值阈的阈值。正在将回避添加到接口 *interface*。额外消息

  此消息显示，由于指定服务的可疑活动，威胁检测服务规避了某个 IP 地址。该消息可能包含其他信息。例如，对于 RA VPN 客户端发起尝试，附加信息可能是“SSL（或 IKEv2）：RA 客户端发起请求过多”。

  您可以使用 **show shun** 命令来查看规避的主机列表。如果知道 IP 地址不是攻击者，则可以使用 **no shun** 命令移除回避。

显示 VPN 服务威胁检测的监控命令

要显示威胁检测 VPN 服务的统计数据，请使用以下命令：

show threat-detection service［*service*］［**entries**｜ **details**］

您可以选择将视图限制为特定服务（**remote-access-authentication**、**remote-access-client-initiations** 或 **invalid-vpn-access**）。您可以通过添加这些参数来进一步限制视图：

- **entries** - 仅显示正在跟踪的条目。例如，身份验证尝试失败的 IP 地址。
- **details** - 显示服务详细信息和服务条目。

根据所选选项，显示输出如下：

- 服务名称
- 服务状态：启用或禁用
- 服务抑制设置

- 服务阈值设置
- 服务操作统计信息
  - 失败 - 处理报告的事件时发生故障。
  - 阻止 - 报告的事件发生在抑制时间段内并且达到或超过阈值。因此，服务会自动安装回避以阻止恶意对等体。
  - 记录 - 报告的事件在抑制时间段之外，或者达到或超过阈值。因此，服务将记录发生的情况。
  - 不支持 - 报告的事件当前不支持自动避开。
  - 禁用 — 已报告事件；请参阅但服务已禁用。

示例

以下示例显示所有服务都已启用，远程访问身份验证服务正在跟踪潜在攻击者。

```
ciscoasa# show threat-detection service
Service: invalid-vpn-access
    State     : Enabled
    Hold-down : 1 minutes
    Threshold : 1
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
    Total entries: 3
Name: remote-access-client-initiations
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
```

以下是 **show threat-detection service entries** 命令的示例。

```
ciscoasa# show threat-detection service remote-access-authentication entries
```

```
Service: remote-access-authentication
    Total entries: 2

Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1         721           0
  2 192.168.100.102/ 32              outside              2         486         114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

以下是 **show threat-detection service details** 命令的示例。

```
ciscoasa# show threat-detection service remote-access-authentication details
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
     Total entries: 2

Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1         721           0
  2 192.168.100.102/ 32              outside              2         486         114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

删除对 VPN 服务违规应用的规避次数

您可以使用以下命令监控为 VPN 服务申请的分区，并删除分区。请注意，威胁检测对 VPN 服务应用的规避不会显示在 **show threat-detection shun** 命令中，该命令仅适用于扫描威胁检测。

- **show shun** [*ip_address*]

  显示规避的主机，包括通过 VPN 服务的威胁检测自动规避的主机，或使用 **shun** 命令手动规避的主机。您可以选择将视图限制到指定的 IP 地址。

- **no shun** *ip_address* [**interface** *if_name*]

  仅从指定的 IP 地址删除回避。如果某个地址在多个接口上被避开，并且您想在某些接口上保留 shun，则可以选择性地为回避指定接口名称。

- **clear shun**

  从所有 IP 地址中删除回避。

威胁检测示例

以下示例配置基本威胁检测统计信息，并且更改 DoS 攻击速率设置。启用所有高级威胁检测统计信息，速率间隔的主机统计信息数量低至 2。还自定义 TCP 拦截速率间隔。启用扫描威胁检测，自动避开除了 10.1.1.0/24 以外的所有地址。自定义扫描威胁速率间隔。

```
threat-detection basic-threat
threat-detection rate dos-drop rate-interval 600 average-rate 60 burst-rate 100
threat-detection statistics
threat-detection statistics host number-of-rate 2
threat-detection statistics tcp-intercept rate-interval 60 burst-rate 800 average-rate 600
threat-detection scanning-threat shun except ip-address 10.1.1.0 255.255.255.0
threat-detection rate scanning-threat rate-interval 1200 average-rate 10 burst-rate 20
threat-detection rate scanning-threat rate-interval 2400 average-rate 10 burst-rate 20
```

威胁检测的历史记录

功能名称	平台版本	说明
基本和高级威胁检测统计信息、扫描威胁检测	8.0(2)	引入了基本和高级威胁检测统计信息、扫描威胁检测。 引入了以下命令：**threat-detection basic-threat**、**threat-detection rate**、**show threat-detection rate**、**clear threat-detection rate, threat-detection statistics**、**show threat-detection statistics**、**threat-detection scanning-threat**、**threat-detection rate scanning-threat**、**show threat-detection scanning-threat**、**show threat-detection shun**、**clear threat-detection shun**。
避开持续时间	8.0(4)/8.1(2)	现在可以设置避开持续时间。 引入了以下命令：**threat-detection scanning-threat shun duration**。
TCP 拦截统计信息	8.0(4)/8.1(2)	引入了 TCP 拦截统计信息。 引入或修改了以下命令：**threat-detection statistics tcp-intercept**、**show threat-detection statistics top tcp-intercept**、**clear threat-detection statistics**。
自定义主机统计信息速率间隔	8.1(2)	现在，可以自定义收集统计信息的速率间隔数。默认速率数已从 3 更改为 1。 修改了以下命令：**threat-detection statistics host number-of-rates**。

功能名称	平台版本	说明
突发速率间隔已更改为平均速率的 1/30。	8.2(1)	在早期版本中，突发速率间隔为平均速率的1/60。为最大限度利用内存，采样间隔已在平均速率中减少到 30 次。
自定义端口和协议统计信息速率间隔	8.3(1)	现在，可以自定义收集统计信息的速率间隔数。默认速率数已从 3 更改为 1。 修改了以下命令：**threat-detection statistics port number-of-rates**、**threat-detection statistics protocol number-of-rates**。
提高了内存使用率	8.3(1)	提高了威胁检测的内存使用率。 引入了以下命令：**show threat-detection memory**。
适用于 VPN 服务的威胁检测	9.20(3)	您可以为 VPN 服务配置威胁检测，以防止来自 IPv4 地址的以下类型的 VPN 攻击： • 远程访问 VPN 验证尝试失败过多，例如用户名/密码暴力扫描。 • 客户端启动攻击，即攻击者从一台主机发起但未完成与远程访问 VPN 头端的重复连接尝试。 • 尝试访问无效的VPN服务，即仅供内部使用的服务。 这些攻击即使未能成功获取访问权，也会消耗计算资源，有时甚至会导致拒绝服务。 引入或更改了以下命令：**clear threat-detection service**、**show threat-detection service**、**shun**、**threat-detection service**。

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。