连接设置

本章介绍如何配置通过 ASA 的连接或传至 ASA 的管理连接的连接设置。

什么是连接设置？

连接设置包含与管理流量连接相关的各种功能，例如通过 ASA 的 TCP 流量。某些功能以组件命名，可以配置这些组件，以提供特定服务。

连接设置包括以下内容：

- **Global timeouts for various protocols** - 所有全局超时均具有默认值，因此，只有在遇到过早失去连接的情况下，才需要更改超时值。
- **Connection timeouts per traffic class** - 可以使用服务策略覆盖特定流量类型的全局超时。所有流量类超时均具有默认值，因此，无需设置这些超时。
- **Connection limits and TCP Intercept** - 默认情况下，对于可以通过（或到达）ASA 的连接数量没有限制。可以使用服务策略规则来设置对特定流量类的限制，以保护服务器免受拒绝服务 (DoS) 攻击。具体而言，可以设置对初期连接（未完成 TCP 握手的连接）的限制，防止 SYN 泛洪攻击。当超过初期限制时，TCP 拦截组件会参与代理连接并确保攻击受到限制。
- **Dead Connection Detection (DCD)** - 如果具有有效但经常空闲的持久连接，以至于这些连接因为超出空闲超时设置而关闭，就可以启用失效连接检测，以识别空闲但有效的连接并且（通过重置其空闲计时器）使之保持活动状态。每当超出空闲时间，DCD 便会探测连接的两侧，了解两侧是否均同意连接是有效的。**show service-policy** 命令输出中包含计数器，以显示来自 DCD 的活动量。您可以使用 **show conn detail** 命令获取有关发起方和响应方的信息，以及各自发送探测的频率。
- **TCP 序列随机化** - 每个 TCP 连接都有两个初始序列号 (ISN)：一个由客户端生成，一个由服务器生成。默认情况下，ASA 随机化入站和出站方向的 TCP SYN 的 ISN。随机化可防止攻击者预测新连接的下一个 ISN 而潜在劫持新会话。但是，TCP 序列随机化有效地破坏了 TCP SACK（选

择性确认），因为客户端看到的序列号与服务器看到的序列号不同。可以根据需要按流量类禁用随机化。

- **TCP Normalization** - TCP 规范器可防止异常数据包。可以按流量类配置处理某些数据包异常类型的方式。
- **TCP State Bypass** - 如果在网络中使用非对称路由，可以绕过 TCP 状态检查。
- **SCTP State Bypass** - 如果不希望进行 SCTP 协议验证，可以绕过流控制传输协议 (SCTP) 状态检测。
- **数据流分流** - 可以标识将要分流至超快路径的选定流量，在此路径中，数据流在 NIC 自身进行交换。分流可帮助您提高数据密集型应用（例如大型文件传输）的性能。
- **IPsec 流分流 (IPsec flow offload)** - 在初始设置 IPsec 站点间 VPN 或远程接入 VPN 安全关联 (SA) 后，IPsec 连接将被分流到设备中的现场可编程门阵列 (FPGA)，而这应会提高设备性能。在支持此功能的平台上会默认启用此功能。

配置连接设置

连接限制、超时、TCP 规范化、TCP 序列随机化和减少生存时间 (TTL) 均具有适用于大多数网络的默认值。仅当有特殊要求、网络有特定的配置类型或遇到因过早空闲超时而导致的异常失去连接时，才需要配置这些连接设置。

其他连接相关的功能处于未启用状态。仅可在特定流量类上配置这些服务，并且不能配置为通用服务。这些功能包括以下内容：TCP 拦截、TCP 状态绕行、失效连接检测 (DCD)、SCTP 状态绕行、流量卸载。

以下常规操作步骤介绍所有可能的连接设置配置。请根据自己的需要选择要实施哪些设置。

过程

步骤 1 配置全局超时，第 3 页。这些设置为通过设备的所有流量更改各种协议的默认空闲超时。如果您在因过早超时而重置连接时遇到问题，请先尝试更改全局超时。

步骤 2 保护服务器不受 SYN 洪流 DoS 攻击（TCP 拦截），第 5 页。请使用此操作步骤配置 TCP 拦截。

步骤 3 如果要更改特定流量类的默认 TCP 规范化行为，请自定义异常 TCP 数据包处理（TCP 映射、TCP 规范器），第 7 页。

步骤 4 如果有这种类型的路由环境，请绕过非对称路由的 TCP 状态检查（TCP 状态绕行），第 11 页。

步骤 5 如果默认随机化加扰某些连接的数据，请禁用 TCP 序列随机化，第 14 页。

步骤 6 分流大型数据流，第 16 页（如果需要提升计算密集型数据中心的性能）。

步骤 7 配置特定流量类的连接设置（所有服务），第 23 页。这是连接设置的全部操作步骤。这些设置可以使用服务策略规则覆盖特定流量类的全局默认值。此外，您也可以使用这些规则自定义 TCP 规范器、更改 TCP 序列随机化、减少数据包生存时间和实施其他可选功能。

步骤 8 配置 TCP 选项，第 27 页（如果您需要强制重置或更改其他标准 TCP 行为）。

配置全局超时

可以设置各种协议的连接和转换插槽的全局空闲超时持续时间。如果插槽在指定的空闲时间内未使用，资源将返回到空闲池。

更改全局超时会设置新的默认超时，在某些情况下，可以通过服务策略为特定流量覆盖默认超时。

对于没有特定可配置超时设置的协议（如 GRE），空闲超时为 2 分钟。

过程

使用 **timeout** 命令可设置全局超时。

所有超时值均采用 *hh*:*mm*:*ss* 格式，大多数情况下，最大持续时间为 1193:0:0。使用 **clear configure timeout** 命令将所有超时重置为其默认值。如果只想将一个计时器重置为默认值，请输入 **timeout** 命令，将该设置重置为默认值。

使用 **0** 值以禁用计时器。

可以配置以下全局超时。

- **timeout conn** *hh*:*mm*:*ss* - 连接关闭之前允许的空闲时间，该值介于 0:5:0 到 1193:0:0 之间。默认值为 1 小时 (1:0:0)。
- **timeout half-closed** *hh*:*mm*:*ss* - TCP 半闭连接关闭之前允许的空闲时间。如果同时收到 FIN 和 FIN-ACK，则连接会被认为是半关闭的。如果只看到了 FIN，则常规 **conn** 超时适用。最小值为 30 秒。默认值为 10 分钟。
- **timeout udp** *hh*:*mm*:*ss* - UDP 连接关闭之前允许的空闲时间。此持续时间必须为至少 1 分钟。默认值为 2 分钟。
- **timeout icmp** *hh*:*mm*:*ss* - ICMP 允许的空闲时间，该值介于 0:0:2 到 1193:0:0 之间。默认值为 2 秒 (0:0:2)。
- **timeout icmp-error** *hh*:*mm*:*ss* - ASA 在收到 ICMP 回应应答数据包后删除 ICMP 连接之前允许的空闲时间，该值介于 0:0:0 到 0:1:0 之间；或者为 **timeout icmp** 值，以较低者为准。默认为 0（禁用）。如果禁用此超时并启用 ICMP 检测，ASA 将在收到回应应答后立即删除 ICMP 连接；因此，针对该（现已关闭）连接生成的任何 ICMP 错误都将被丢弃。此超时可延迟删除 ICMP 连接，以便您可以接收重要的 ICMP 错误。
- **timeout sunrpc** *hh*:*mm*:*ss* - 释放 SunRPC 插槽之前允许的空闲时间。此持续时间必须为至少 1 分钟。默认值为 10 分钟。
- **timeout H323***hh*:*mm*:*ss* - H.245 (TCP) 和 H.323 (UDP) 媒体连接关闭之前允许的空闲时间，该值介于 0:0:0 到 1193:0:0 之间。默认值为 5 分钟 (0:5:0)。由于 H.245 和 H.323 媒体连接上设置的连接标志相同，因此 H.245 (TCP) 连接与 H.323（RTP 和 RTCP）媒体连接共享空闲超时。

- **timeout h225** *hh*:*mm*:*ss* - H.225 信令连接关闭之前允许的空闲时间。H.225 默认超时为 1 小时 (1:0:0)。要在所有呼叫清除之后立即关闭连接，建议将该值设置为 1 秒 (0:0:1)。
- **timeout mgcp** *hh*:*mm*:*ss* - 删除 MGCP 媒体连接之前允许的空闲时间，该值介于 0:0:0 到 1193:0:0 之间。默认值为 5 分钟 (0:5:0)
- **timeout mgcp-pat** *hh*:*mm*:*ss* - 删除 MGCP PAT 转换之前允许的绝对间隔，该值介于 0:0:0 到 1193:0:0 之间。默认值为 5 分钟 (0:5:0)。最短时间为 30 秒。
- **timeout sctp** *hh*:*mm*:*ss* - 流控制传输协议 (SCTP) 连接关闭之前允许的空闲时间，该值介于 0:1:0 到 1193:0:0 之间。默认值为 2 分钟 (0:2:0)。
- **timeout sip***hh*:*mm*:*ss* - SIP 信令端口连接关闭之前允许的空闲时间，该值介于 0:5:0 到 1193:0:0 之间。默认值为 30 分钟 (0:30:0)。
- **timeout sip_media***hh*:*mm*:*ss* - SIP 媒体端口连接关闭之前允许的空闲时间。此持续时间必须为至少 1 分钟。默认值为 2 分钟。SIP 媒体计时器用于具有 SIP UDP 媒体数据包的 SIP RTP/RTCP，而不是 UDP 非活动超时。
- **timeout sip-provisional-media***hh*:*mm*:*ss* - SIP 临时媒体连接的超时值，该值介于 0:1:0 到 0:30:0 之间。默认值为 2 分钟。
- **timeout sip-invite***hh*:*mm*:*ss* - 关闭 PROVISIONAL 响应和媒体转换的针孔之前允许的空闲时间，该值介于 0:1:0 到 00:30:0 之间。默认值为 3 分钟 (0:3:0)。
- **timeout sip-disconnect***hh*:*mm*:*ss* - 在 CANCEL 或 BYE 消息未收到 200 OK 的情况下，删除 SIP 会话之前允许的空闲时间，该值介于 0:0:1 到 0:10:0 之间。默认值为 2 分钟 (0:2:0)。
- **timeout uath** *hh*:*mm*:*ss* {**absolute** | **inactivity**} - 身份验证和授权缓存超时并且用户必须对下一连接重新进行身份验证之前经过的持续时间，该值介于 0:0:0 到 1193:0:0 之间。默认值为 5 分钟 (0:5:0)。默认计时器为 **absolute**；可以通过输入 **inactivity** 关键字设置在非活动状态持续了特定时间后发生超时。未经授权的持续时间必须比转换持续时间短。设置为 0 表示禁用缓存。如果连接使用被动 FTP 或使用虚拟 http 命令进行 Web 身份验证，请勿使用 0。
- **timeout xlate***hh*:*mm*:*ss* - 释放转换插槽之前允许的空闲时间。此持续时间必须为至少 1 分钟。默认值为 3 小时。
- **timeout pat-xlate***hh*:*mm*:*ss* - 释放 PAT 转换插槽之前允许的空闲时间，该值介于 0:0:30 到 0:5:0 之间。默认值为 30 秒。如果上游路由器拒绝使用释放的 PAT 端口的新连接，您可能会想要增加超时，因为以前的连接在上游设备中可能仍处于开放状态。
- **timeout tcp-proxy-reassembly***hh*:*mm*:*ss* - 丢弃等待重组的缓冲数据包之前允许的空闲超时，该值介于 0:0:10 到 1193:0:0 之间。默认值为 1 分钟 (0:1:0)。
- **timeout floating-conn***hh*:*mm*:*ss* - 当多个具有不同指标的路由共存于一个网络时，ASA 在创建连接时使用指标最好的路由。如果有更好的路由变得可用，则此超时可让连接关闭，以便使用更好的路由重新建立连接。默认值为 0（连接永不超时）。为了可以使用更好的路由，请将超时设置为 0:0:30 至 1193:0:0 之间的值。
- **timeout conn-holddown***hh*:*mm*:*ss* - 系统应在该连接使用的路由不再存在或处于非活动状态时维持连接的时间长度。如果在此等待期间内路由未处于活动状态，系统将释放该连接。配置连接

等待计时器的目的是为了降低路由摆动的影响，其中路由可能会快速显示和断开。您可以减小等待计时器，以便更快地进行路由融合。默认值为 15 秒，范围介于 00:00:00 到 00:00:15 秒之间。

- **timeout igp stale-route***hh*:*mm*:*ss* - 从路由器信息库中删除过时路由之前允许保留的时间长度。这些路由供内部网关协议（例如 OSPF）使用。默认值为 70 秒 (00:01:10)，范围介于 00:00:10 到 00:01:40 之间。

保护服务器不受 SYN 洪流 DoS 攻击（TCP 拦截）

当攻击者将一系列 SYN 数据包发送到主机时，即表示发生 SYN 泛洪拒绝服务 (DoS) 攻击。这些数据包通常来自虚假 IP 地址。SYN 数据包的持续泛洪将使服务器 SYN 队列始终处于充满状态，而无法处理来自合法用户的连接请求。

可以限制初期连接的数量，这样有助于防止SYN泛洪攻击。半开连接是源与目标之间尚未完成必要握手的连接请求。

当超过连接的初期连接阈值时， ASA 将充当服务器代理，使用 SYN cookie 方法向客户端 SYN 请求生成 SYN-ACK 响应，使该连接不加入到目标主机的 SYN 队列中。SYN Cookie 是在 SYN-ACK 中返回的初始序列号，它由 MSS、时间戳和其他项目的数学散列构成，用于创建密钥。如果在有效的时间窗口内 ASA 收到来自客户端的具有正确序列号的 ACK，可以对实际客户端的真实性进行身份验证，并且允许连接到服务器。执行代理的组件称为 TCP 拦截。

保护服务器免受 SYN 泛洪攻击的端到端流程包括设置连接限制，启用 TCP 拦截统计信息，然后监控结果。

开始之前

- 请确保设置的初期连接限制低于要保护的服务器上的 TCP SYN 积压工作队列。否则，在 SYN 攻击期间，有效客户端将无法访问服务器。为了确定初期限制的合理值，请仔细分析服务器容量、网络和服务器使用情况。
- 根据 ASA 型号中的 CPU 核心数，由于每个核心管理连接的方式不同，最大并发和初始连接数可超出配置的数量。在最坏的情形下，ASA 允许最多 *n*-1 个额外连接和初始连接，其中 *n* 为核心数。例如，如果设备型号有 4 个核心，而配置了 6 个并发连接和 4 个初期连接，那么每个类型可能有 3 个额外连接。要确定型号的核心数量，请输入 **show cpu core** 命令。

过程

步骤 1 创建 L3/L4 类映射以确定要保护的服务器。使用访问列表匹配。

```
class-map name
match parameter
```

示例：

```
hostname(config)# access-list servers extended permit tcp any host 10.1.1.5 eq http
hostname(config)# access-list servers extended permit tcp any host 10.1.1.6 eq http
hostname(config)# class-map protected-servers
hostname(config-cmap)# match access-list servers
```

步骤 2 添加或编辑用于设置要对类映射流量执行的操作的策略映射，并确定类映射。

policy-map *name*
class *name*

示例：

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class protected-servers
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。对于类映射，请指定在本程序前面部分中创建的类。

步骤 3 设置初期连接限制。

- **set connection embryonic-conn-max** *n* - 允许的最大同时初期 TCP 连接数，该值介于 0 到 2000000 之间。默认值为 0，允许无限制连接。
- **set connection per-client-embryonic-max** *n* - 每个客户端允许的最大同步初期 TCP 连接数，该值介于 0 到 2000000 之间。默认值为 0，允许无限制连接。
- **set connection syn-cookie-mss** *n* - 在达到初期连接限制时为初期连接的 SYN-Cookie 设置服务器最大分段大小 (MSS)，范围为 48 到 65535。默认值为 1380。仅当配置 **set connection embryonic-conn-max** 或 **per-client-embryonic-max** 时，此设置才有意义。

示例：

```
hostname(config-pmap-c)# set connection embryonic-conn-max 1000
hostname(config-pmap-c)# set connection per-client-embryonic-max 50
```

步骤 4 如果编辑的是现有服务策略（例如，名为 global_policy 的默认全局策略），您即可跳过此步骤。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

Global 关键字指示将策略映射应用于所有接口，而 **interface** 指示仅将策略应用于一个接口。仅允许存在一个全局策略。可以通过向接口应用服务策略来覆盖该接口上的全局策略。每个接口只能应用一个策略映射。

步骤 5 配置 TCP 拦截所拦截攻击的威胁检测统计信息。

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

其中：

- **rate-interval** *minutes* 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** *attacks_per_sec* 设置生成系统日志消息的阈值，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** *attacks_per_sec* 设置生成系统日志消息的平均速率阈值，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。

示例：

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

步骤 6 可以使用以下命令监控结果：

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**] - 查看遭受攻击的前 10 名受保护服务器。**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。
- **clear threat-detection statistics tcp-intercept** - 清除 TCP 拦截统计信息。

示例：

```
hostname(config)# show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
------------------------------------------------------------------------------
1    10.1.1.5:80 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    10.1.1.6:80 inside 10 10 6080 10.0.0.200 (0 secs ago)
```

自定义异常 TCP 数据包处理（TCP 映射、TCP 规范器）

TCP 规范器标识被检测到时可由 ASA 处理的异常数据包；例如，ASA 可允许、丢弃或清除这些数据包。TCP 规范化有助于防止 ASA 遭受攻击。TCP 规范化始终启用，但是，可以自定义某些功能的行为方式。

默认配置包括以下设置：

```
no check-retransmission
no checksum-verification
exceed-mss allow
queue-limit 0 timeout 4
```

```
reserved-bits allow
syn-data allow
synack-data drop
invalid-ack drop
seq-past-window drop
tcp-options range 6 7 clear
tcp-options range 9 18 clear
tcp-options range 20 255 clear
tcp-options md5 allow
tcp-options mss allow
tcp-options selective-ack allow
tcp-options timestamp allow
tcp-options window-scale allow
ttl-evasion-protection
urgent-flag clear
window-variation allow-connection
```

要自定义TCP规范器，请首先使用TCP映射定义设置。然后，可以使用服务策略将映射应用到所选的流量类。

过程

步骤 1 创建 TCP 映射，以指定要查找的 TCP 规范化条件：**tcp-map** *tcp-map-name*

步骤 2 通过输入下列一个或多个命令配置 TCP 映射条件。系统对您未输入的所有命令使用默认设置。使用命令的 **no** 形式可禁用该设置。

- **check-retransmission** - 防止 TCP 重新传输出现不一致。此命令默认禁用。
- **checksum-verification** - 验证 TCP 校验和，丢弃验证失败的数据包。此命令默认禁用。
- **exceed-mss** {**allow** | **drop**} - 允许或丢弃数据长度超出 TCP 最大分段大小的数据包。默认为允许数据包。
- **invalid-ack** {**allow** | **drop**} - 允许或丢弃具有无效 ACK 的数据包。默认丢弃该类数据包，但 WAAS 连接除外，因为系统允许 WAAS 连接。可能会在以下实例中看到无效 ACK：
  - 在 TCP 连接 SYN-ACK 已接收状态下，如果已接收的 TCP 数据包的 ACK 号与正在发送的下一个 TCP 数据包的序列号不完全相同，则是无效 ACK。
  - 如果已收到TCP数据包的ACK号大于发送的下一个TCP数据包的序列号，则为无效ACK。
- **queue-limit** *pkt_num* [**timeout** *seconds*] - 设置 TCP 连接可缓冲并可按顺序排列的最大无序数据包数量，该值介于 1 到 250 个数据包之间。默认值为 0，表示禁用此设置，而且使用的默认系统队列限制取决于流量类型：
  - 对于用于应用检查（**inspect** 命令）、 和 TCP 检查重传（TCP 映射 **check-retransmission** 命令）的连接，队列限制为 3 个数据包。如果 ASA 收到具有不同窗口大小的 TCP 数据包，则队列限制会动态变化以符合传送的设置。
  - 对于其他 TCP 连接，无序数据包会按原样通过。

如果将 **queue-limit** 命令设置为 1 或以上，则允许用于所有 TCP 流量的无序数据包的数量与此设置匹配。例如，对于应用检查 和 TCP 检查重发流量，来自 TCP 数据包的所有通告设置将被忽略，以支持 **queue-limit** 设置。对于其他 TCP 流量，现在会缓冲无序数据包并将其按顺序排列，而不是按原样通过。

timeout *seconds* 参数设置无序数据包可停留在缓冲区的最长时间，介于 1 至 20 秒之间；如果这些数据包在超时期间内未按顺序排列并通过，则将被丢弃。默认值为 4 秒。如果 *pkt_num* 参数设置为 0，则不能更改任何流量的超时；需要将该限制设置为 1 或更大的值，**timeout** 关键字才会生效。

- **reserved-bits** {**allow** | **clear** | **drop**} - 为 TCP 报头保留位设置操作。可以 **allow** 数据包（不更改保留位），**clear** 保留位并允许数据包，或者 **drop** 数据包。
- **seq-past-window** {**allow** | **drop**} - 为具有超出窗口序列号的数据包设置操作，即已收到 TCP 数据包的序列号超出 TCP 接收窗口的右边。仅当 **queue-limit** 命令设置为 0（禁用）时，才可以 **allow** 数据包。默认为丢弃数据包。
- **synack-data** {**allow** | **drop**} - 允许或丢弃含有数据的 TCP SYNACK 数据包。默认为丢弃数据包。
- **syn-data** {**allow** | **drop**} - 允许或丢弃含有数据的 SYN 数据包。默认为允许数据包。
- **tcp-options** {**md5** | **mss** | **selective-ack** | **timestamp** | **window-scale** | **range** *lower upper*} *action* - 设置包含 TCP 选项的数据包的操作。这些选项被命名为：**md5**、**mss**、**selective-ack**（选择性确认机制）、**timestamp** 和 **window-scale**（窗口缩放机制）。对于其他选项，可按 **range** 关键字中的编号指定它们，其中的范围限制为 6-7、9-18 和 20-255。要按编号定位单一选项，请对范围下限和上限输入相同的编号。可以在映射中多次输入命令来定义完整的策略。请注意，如果 TCP 连接已检测，则不论您的配置如何，都会清除除 MSS 和选择性确认 (SACK) 选项以外的所有选项。可能的操作如下：
  - **allow** [**multiple**] - 允许包含单一此类型选项的数据包。这是所有已命名选项的默认设置。如果要允许数据包，即便其中包含该选项的多个实例亦不例外，请添加 **multiple** 关键字。（**multiple** 关键字不适用于 **range**。）
  - **maximum** *limit* - 仅适用于 **mss**。将最大分段大小设置为所示的限制，范围为 68-65535。默认 TCP MSS 在 **sysopt connection tcpmss** 命令中定义。
  - **clear**- 从报头中删除此类型的选项并允许该数据包。这是所有已编号选项的默认设置。请注意，清除时间戳选项将禁用 PAWS 和 RTT。
  - **drop**- 丢弃包含此选项的数据包。此操作仅适用于 **md5** 和 **range**。
- **ttl-evasion-protection** - 为连接设置最大 TTL 数，由初始数据包中的 TTL 确定。后续数据包的 TTL 可以减少，但不能增加。系统会将 TTL 重置为该连接之前看到过的最低 TTL。这样有助于防御 TTL 回避攻击。默认启用 TTL 逃逸防护，因此只需要输入此命令的 **no** 形式。

  例如，攻击者可能发送一个使用极短 TTL 通过策略的数据包。当 TTL 变为零时，ASA 与终端之间的路由器将丢弃该数据包。攻击者可能在此时发送包含长 TTL 的恶意数据包，在 ASA 看来则像是重新传输数据包并进行传送。但到达终端主机时，它是攻击者收到的第一个数据包。在这种情况下，攻击者可以成功绕过防范攻击的安全措施。

- **urgent-flag** {**allow** | **clear**} - 为具有 URG 标志的数据包设置操作。可以 **allow** 数据包，或者 **clear** 标志并允许数据包。默认为清除标志。

  URG 标志用于指示数据包包含优先级高于流内其他数据的信息。TCP RFC 对 URG 标记的确切解释比较模糊，因此终端系统以不同的方式处理紧急偏移，这可能使终端系统容易受到攻击。

- **window-variation** {**allow** | **drop**} - 允许或丢弃意外更改其窗口大小的连接。默认为允许连接。

  窗口大小机制允许 TCP 通告一个大窗口，随后通告一个不接受过多数据的较小窗口。根据 TCP 规范，强烈反对“缩小窗口”。检测到这种情况时，连接可能会断开。

步骤 3 使用服务策略将 TCP 映射应用到流量类。

a) 使用 L3/L4 类映射定义流量类，并将该映射添加到策略映射中。

```
class-map name
match parameter
policy-map name
class name
```

示例：

```
hostname(config)# class-map normalization
hostname(config-cmap)# match any
hostname(config)# policy-map global_policy
hostname(config-pmap)# class normalization
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。有关类映射匹配语句的信息，请参阅为通过流量创建第 3/4 层类映射。

b) 应用 TCP 映射：**set connection advanced-options** *tcp-map-name*

示例：

```
hostname(config-pmap-c)# set connection advanced-options tcp_map1
```

c) 如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

Global 关键字指示将策略映射应用于所有接口，而 **interface** 指示仅将策略应用于一个接口。仅允许存在一个全局策略。可以通过向接口应用服务策略来覆盖该接口上的全局策略。每个接口只能应用一个策略映射。

示例

例如，要允许所有流量的紧急标志和紧急偏移数据包发送到众所周知的 FTP 数据端口与 Telnet 端口之间的 TCP 端口范围，请输入以下命令：

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow
hostname(config-tcp-map)# class-map urg-class
hostname(config-cmap)# match port tcp range ftp-data telnet
hostname(config-cmap)# policy-map pmap
hostname(config-pmap)# class urg-class
hostname(config-pmap-c)# set connection advanced-options tmap
hostname(config-pmap-c)# service-policy pmap global
```

绕过非对称路由的 TCP 状态检查（TCP 状态绕行）

如果网络中有非对称路由环境，其中，给定连接的出站和入站流量可以通过两个不同的ASA设备，则需要在受影响的流量上实施 TCP 状态绕行。

但是，TCP 状态绕行会削弱网络安全性，因此应在非常具体的有限流量类上应用绕行。

以下主题详细介绍该问题和解决方案。

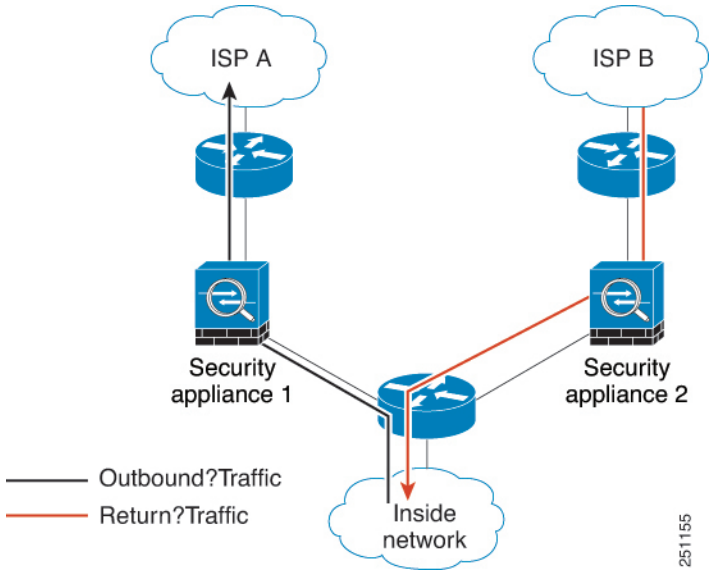
非对称路由问题

默认情况下，所有经过ASA的流量都会使用自适应安全算法检查，并根据安全策略允许通过或予以丢弃。ASA 通过检查每个数据包的状态（新连接还是现有连接）并将其分配到会话管理路径（新连接SYN数据包）、快速路径（现有连接）或控制平面路径（高级检测），最大程度地提高防火墙性能。

匹配快速路径中现有连接的TCP数据包，不重新检查安全策略的每个方面即可通过ASA。此功能可最大程度地提高性能。但是，使用SYN数据包在快速路径中建立会话的方法，以及在快速路径中进行的检查（例如 TCP 序列号），可能会阻碍非对称路由解决方案：出站和入站连接流必须通过同一 ASA 。

例如，有一个新连接传入安全设备 1。SYN 数据包通过会话管理路径，而且连接的条目添加到快速路径表中。如果此连接的后续数据包通过安全设备 1，则这些数据包与快速路径中的该条目匹配，可以通过。但是，如果后续数据包传入安全设备 2，其中没有经过会话管理路径的 SYN 数据包，则快速路径中没有该连接的条目，数据包将被丢弃。下图显示一个不对称路由示例，其中，出站流量通过一个与入站流量不同的 ASA：

图 *1:* 非对称路由



如果在上游路由器中配置了不对称路由，且流量在两个 ASA 之间交替，则可以为特定流量配置 TCP 状态绕行。TCP 状态绕行将改变会话在快速路径中建立的方式，并且禁用快速路径检查。此功能按处理 UDP 连接的大致方式来处理 TCP 流量：当匹配指定网络的非 SYN 数据包进入 ASA 时，其中没有快速路径条目，该数据包将通过会话管理路径在快速路径中建立该连接。流量到达快速路径后，将绕过快速路径检查。

有关 TCP 状态绕行的准则和限制

TCP 状态绕行不支持的功能

使用 TCP 状态绕行时不支持以下功能：

- 应用检测 - 检测要求入站和出站流量通过同一 ASA，因此不会对 TCP 状态绕行流量应用检测。
- 通过 AAA 身份验证的会话 - 如果用户通过一个 ASA 的身份验证，那么通过另一个 ASA 返回的流量将被拒绝，因为该用户未通过该 ASA 的身份验证。
- TCP 拦截、最大初期连接限制、TCP 序列号随机化 - ASA 不跟踪连接的状态，因此不会应用这些功能。
- TCP 标准化 - 禁用 TCP 规范器。
- 状态故障转移。

TCP 状态绕行 NAT 准则

由于转换会话是为每个 ASA 单独建立，请务必在两个设备上均为 TCP 状态绕行流量配置静态 NAT。如果使用动态 NAT，则在设备 1 上为会话选择的地址将与在设备 2 上为会话选择的地址不同。

配置 TCP 状态绕行

要在非对称路由环境中绕过 TCP 状态检查，请仔细定义适用于受影响主机或仅适用于网络的流量类，然后使用服务策略在流量类上启用 TCP 状态绕行。由于绕行会降低网络安全性，请尽可能限制网络应用。

开始之前

如果指定的连接上在 2 分钟内没有流量，则连接超时。您可以覆盖此默认值，将 **set connection timeout idle** 命令用于 TCP 状态绕行流量类。一般的 TCP 连接超时默认为 60 分钟后。

过程

步骤 1 创建 L3/L4 类映射以确定需要 TCP 状态绕行的主机。使用 access-list match 确定源主机和目标主机。

```
class-map name
match parameter
```

示例：

```
hostname(config)# access-list bypass extended permit tcp host 10.1.1.1 host 10.2.2.2
hostname(config)# class-map bypass-class
hostname(config-cmap)# match access-list bypass
```

步骤 2 添加或编辑用于设置要对类映射流量执行的操作的策略映射，并确定类映射。

```
policy-map name
class name
```

示例：

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class bypass-class
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。对于类映射，请指定在本程序前面部分中创建的类。

步骤 3 在该类上启用 TCP 状态绕行：**set connection advanced-options tcp-state-bypass**

步骤 4 如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

Global 关键字指示将策略映射应用于所有接口，而 **interface** 指示仅将策略应用于一个接口。仅允许存在一个全局策略。可以通过向接口应用服务策略来覆盖该接口上的全局策略。每个接口只能应用一个策略映射。

示例

以下是 TCP 状态绕行的示例配置：

```
hostname(config)# access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.224 any

hostname(config)# class-map tcp_bypass
hostname(config-cmap)# description "TCP traffic that bypasses stateful firewall"
hostname(config-cmap)# match access-list tcp_bypass

hostname(config-cmap)# policy-map tcp_bypass_policy
hostname(config-pmap)# class tcp_bypass
hostname(config-pmap-c)# set connection advanced-options tcp-state-bypass

hostname(config-pmap-c)# service-policy tcp_bypass_policy interface outside
```

禁用 TCP 序列随机化

每个 TCP 连接都有两个 ISN：一个由客户端生成，一个由服务器生成。ASA 会将入站和出站方向传送的 TCP SYN 的 ISN 随机化。

随机化受保护主机的 ISN 可防止攻击者预测新连接的下一个 ISN 而潜在劫持新会话。但是，TCP 序列随机化有效地破坏了 TCP SACK（选择性确认），因为客户端看到的序列号与服务器看到的序列号不同。

可以根据需要禁用 TCP 初始序列号随机化，例如，由于数据混乱。例如：

- 如果另一个在线防火墙也随机化初始序列号，则即使此操作不影响流量，两个防火墙也无需执行此操作。
- 如果通过 ASA 使用 eBGP 多跳，则 eBGP 对等体使用 MD5。随机化会中断 MD5 校验和。
- 使用要求 ASA 不对连接的序列号随机化的 WAAS 设备。
- 如果为 ISA 3000 启用硬件绕行，当 ISA 3000 不再是数据路径时的一部分时，TCP 连接将被丢弃。

注释 不建议您在使用集群时禁用 TCP 序列随机化。由于 SYN/ACK 数据包可能会被丢弃，因此少数情况下可能无法建立某些 TCP 会话。

过程

步骤 1 创建 L3/L4 类映射以确定不应随机化 TCP 序列号的流量。应对 TCP 流量应用类匹配；可以识别特定的主机（使用 ACL）、执行 TCP 端口匹配或简单地匹配任何流量。

```
class-map name
match parameter
```

示例：

```
hostname(config)# access-list preserve-sq-no extended permit tcp any host 10.2.2.2
hostname(config)# class-map no-tcp-random
hostname(config-cmap)# match access-list preserve-sq-no
```

步骤 2 添加或编辑用于设置要对类映射流量执行的操作的策略映射，并确定类映射。

```
policy-map name
class name
```

示例：

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class no-tcp-random
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。对于类映射，请指定在本程序前面部分中创建的类。

步骤 3 禁用类上的 TCP 序列号随机化：

set connection random-sequence-number disable

如果以后确定要重新打开它，请将“disable”替换为 **enable**。

步骤 4 如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

Global 关键字指示将策略映射应用于所有接口，而 **interface** 指示仅将策略应用于一个接口。仅允许存在一个全局策略。可以通过向接口应用服务策略来覆盖该接口上的全局策略。每个接口只能应用一个策略映射。

分流大型数据流

如果在数据中心支持的设备上部署 ASA，就可以将选定的流量卸载到超快速路径上，在该路径上，流量在网卡本身进行切换。分流可帮助您提高数据密集型应用（例如大型文件传输）的性能。

- 高性能计算 (HPC) 研究站点，其中 ASA 部署在存储设施与高性能计算站之间。当一个研究站使用 NFS 上的 FTP 文件传输或文件同步备份时，庞大的数据流量会影响 ASA 上的所有情景。对 NFS 上的 FTP 文件传输或文件同步分流可降低对其他流量的影响。
- 高频交易 (HFT)，其中 ASA 部署在工作站与交易所之间，主要是出于合规目的。通常无需担心安全问题，但延迟是一个重大问题。

在分流之前，ASA 首先应用建立连接期间的正常安全处理，例如访问规则和检测。此外，ASA 还会终止会话。但建立连接后，如果流量符合分流的条件，则会在 NIC（而不是 ASA）中执行进一步的处理。

已分流的数据流会继续接受具有限制性的状态检测，例如基本 TCP 标记和选项检查以及校验和验证（如果已配置）。如有必要，系统可以有选择地将数据包上报至防火墙系统以进行进一步处理。

为了识别可分流的数据流，可以创建一项应用数据流分流服务的服务策略规则。如果数据流满足以下条件，则可进行分流：

- 仅有 IPv4 地址。
- 仅有 TCP、UDP 和 GRE。
- 仅有标准或 802.1Q 标记的以太网帧。
- （仅有透明模式。）包含两个且仅包含两个接口的桥接组的组播数据流。

已分流数据流的逆向数据流也会被分流。

数据流分流限制

并非所有数据流都可分流。即使在分流后，在某些情况下可取消对数据流的分流。以下是一些限制条件：

设备限制

以下设备支持此功能：

- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200
- Firepower 4100/9300

无法分流的数据流

以下数据流类型无法分流。

- 任何不使用 IPv4 寻址的流，例如 IPv6 寻址。
- 除 TCP、UDP 和 GRE 之外的任意协议的数据流。

注释 无法分流 PPTP GRE 连接。

- 需要由 检查的数据流。在某些情况下（例如 FTP），虽然无法分流控制通道，但可以分流次要数据通道。
- 在设备上终止的 IPsec 和 TLS/DTLS VPN 连接。
- 路由模式下的组播数据流。
- 具备三个或更多接口的网桥组在透明模式下的组播数据流。
- TCP 拦截数据流。
- TCP 状态绕过流。不能在同一流量上配置数据流分流和 TCP 状态绕行。
- AAA 直通代理流。
- Vpath、VXLAN 相关数据流。
- 使用安全组标记的数据流。
- 从不同集群节点转发来的逆向数据流（在集群中数据流不对称的情况下）。
- 集群中的集中数据流（如果数据流的所有者不是控制设备）。

其他限制

- 流分流与死连接检测 (DCD) 不兼容。不要在可分流的连接上配置 DCD。
- 如果多个与数据流分流条件匹配的数据流排队等待同时分流到硬件上的同一位置，则只会分流第一个数据流。其他数据流则会照常处理。这称为冲突。在CLI中使用**show flow-offload flow** 命令显示此情况的统计信息。
- 虽然分流的数据流通过FXOS接口，但这些数据流的统计信息不会显示在逻辑设备接口上。因此，逻辑设备接口计数器和数据包速率不会反映分流流量。

逆向分流的条件

对数据流分流后，如果数据流中的数据包符合以下条件，则将被返回到ASA接受进一步处理：

- 数据包包含时间戳以外的 TCP 选项。
- 数据包经过分段。
- 它们会进行等价多路径 (ECMP) 路由，并且入口数据包会从一个接口移至另一个接口。

配置数据流分流

要配置数据流分流，必须首先启用该服务，再创建服务策略来识别符合分流条件的流量。 对于Firepower 4100/9300：初次启用该服务时，必须重新启动。。

过程

步骤 1 启用数据流分流服务。

flow-offload enable

对于 Firepower 4100/9300：初次启用该服务时，必须重新启动。

如果需要重新加载，则需要对集群或故障转移对进行特殊考虑，以实现无中断更改：

- 集群 - 首先在控制节点上输入命令，但不要立即重启控制节点。相反，首先重新启动该集群的每个节点，再返回控制节点并对其重新启动。然后，即可在控制节点上配置分流服务策略。
- 故障转移 - 首先在主用设备上输入该命令，但不立即重新启动。相反，首先重新启动备用设备，再重新启动主用设备。然后，即可在主用设备上配置分流服务策略。

在多情景模式下，启用或禁用数据流分流将致使在所有情景下都启用或禁用它。每个情景无法进行不同设置。

示例：

```
ciscoasa(config)# flow-offload enable

WARNING: This command will take effect after the running-config is
saved and the system has been rebooted.

ciscoasa(config)# write memory
ciscoasa(config)# reload
```

步骤 2 创建用于识别符合分流条件的流量的服务策略规则。

a) 创建一个 L3/L4 类映射，以识别符合数据流分流条件的流量。最常用的选项是按访问列表或端口匹配。

```
class-map name
match parameter
```

示例：

```
hostname(config)# access-list offload permit tcp 10.1.1.0 255.255.255.224 any
hostname(config)# class-map flow_offload
hostname(config-cmap)# match access-list offload
```

b) 添加或编辑用于设置要对类映射流量执行的操作的策略映射，并确定类映射。

```
policy-map name
class name
```

示例：

```
hostname(config)# policy-map offload_policy
```

```
hostname(config-pmap)# class flow_offload
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。对于类映射，请指定在本程序前面部分中创建的类。

c) 对于类启用数据流分流： **set connection advanced-options flow-offload**

d) 如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy offload_policy interface outside
```

Global 关键字指示将策略映射应用于所有接口，而 **interface** 指示仅将策略应用于一个接口。仅允许存在一个全局策略。可以通过向接口应用服务策略来覆盖该接口上的全局策略。每个接口只能应用一个策略映射。

示例

以下示例将来自 10.1.1.0 255.255.255.224 子网的所有 TCP 流量归为符合分流条件，并将该策略附加到外部接口。

```
hostname(config)# access-list offload permit tcp 10.1.1.0 255.255.255.224 any
hostname(config)# class-map flow_offload
hostname(config-cmap)# match access-list offload
hostname(config)# policy-map offload_policy
hostname(config-pmap)# class flow_offload
hostname(config-pmap-c)# set connection advanced-options flow-offload
hostname(config)# service-policy offload_policy interface outside
```

IPsec 流分流

您可以将支持的设备型号配置为使用 IPsec 数据流分流。初始设置 IPsec 站点间 VPN 或远程访问 VPN 安全关联 (SA) 后，IPsec 连接将被分流到设备中的现场可编程门阵列 (FPGA)，这应该会提高设备性能。 在 Secure Firewall 1200 系列上，IPsec 连接被分流到Marvell 加密加速器 (CPT)，以提高设备性能。

分流操作特别涉及入口上的预解密和解密处理，以及出口上的预加密和加密处理。系统软件处理内部流以应用安全策略。

默认情况下启用 IPsec 数据流分流，并应用于以下设备类型：

- Cisco Secure Firewall 1200
- Cisco Secure Firewall 3100

- Cisco Secure Firewall 4200

启用设备的 VTI 环回接口时，也会使用 IPsec 数据流分流。

IPsec 流分流的限制

不分流以下 IPsec 流：

- IKEv1 隧道。仅 IKEv2 隧道将被分流。IKEv2 支持更强的密码。
- 配置了基于卷的密钥更新的流。
- 已配置压缩的流。
- 传输模式流。仅会分流隧道模式流。
- AH 格式。仅支持 ESP/NAT-T 格式。
- 已配置后分段的流。
- 防重放窗口大小不是 64 位且防重放的流不会被禁用。
- 已启用防火墙过滤器的流。
- 多情景模式。

配置 IPsec 数据流分流

默认情况下，在支持该功能的硬件平台上启用IPsec数据流分流。但是，默认情况下并不启用出口优化功能，因此如果需要该功能，需要对其进行配置。

开始之前

IPsec 流分流是全局配置的。无法为选定流量进行配置。

要禁用这些功能，请使用这些命令的 **no** 形式。

要显示当前配置状态，请使用 **show flow-offload ipsec info** 命令。

过程

步骤 1 启用 IPsec 流分流。

flow-offload-ipsec

步骤 2 启用出口优化以优化数据路径，从而提高单个隧道流的性能。

flow-offload-ipsec egress-optimization

出口优化配置与流分流是分开的。但即使已启用，也只有在同时启用 IPsec 流分流的情况下才会有效。默认情况下不启用出口优化。

DTLS 加密加速

ASA在 FPGA 和 Nitrox V 加密加速器的帮助下支持 DTLS 加密加速。

- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200

此功能可提高 DTLS 加密和 DTLS 解密流量的吞吐量。支持 IPv4 和 IPv6 流量。

ASA还会对出口加密数据包执行优化，以改善延迟。数据路径经过优化，可增强单个隧道流的性能。

默认情况下，这两项功能均已启用，并且仅适用于 DTLS 1.2。

配置 DTLS 加密加速

默认情况下，启用 DTLS 加密加速。如果需要，您可以禁用它。

在以下情况下，ASA 不会执行 DTLS 加密加速：

- 流使用 DTLS 1.0 或数据包压缩。
- 重新生成 DTLS 密钥。
- 集群或多情景模式。

过程

步骤 1 在设备上禁用 DTLS 加密加速。

no flow-offload-dtls

示例：

```
ciscoasa(config)# no flow-offload-dtls
```

要重新启用它，请使用 **flow-offload-dtls** 命令。

步骤 2 禁用出口加密数据包优化并改善延迟。

no flow-offload-dtls egress-optimization

示例：

```
ciscoasa(config)# flow-offload-dtls egress-optimization
```

要重新启用它，请使用 **flow-offload-dtls egress-optimization** 命令。

监控 DTLS 加密加速

在威胁防御设备上使用以下 CLI 命令验证并监控出口加密数据包的 DTLS 加密加速和优化。

- 要验证 DTLS 加密加速和出口加密数据包优化的状态，请使用以下命令：

```
ciscoasa# show flow-offload-dtls info
  DTLS offload : Enabled
  Egress Optimization: Enabled
```

- 要查看 DTLS 加密加速统计信息，请使用以下命令：

```
ciscoasa# show flow-offload-dtls statistics
  Packet stats of Pipe 0
  ----------------------
  Rx Packet count : 975638666
  Tx Packet count : 975638666
  Error Packet count : 0
  Drop Packet count : 0

  CAM stats of Pipe 0
  ----------------------
  Option ID Table CAM Hit Count : 1145314723
  Option ID Table CAM Miss Count : 0
  Tunnel Table CAM Hit Count : 0
  Tunnel Table CAM Miss Count : 0
  6-Tuple CAM Hit Count : 975638666
  6-Tuple CAM Miss Count : 169676057
   NOTE: The counters displayed are cumulative counters
   for all offload applications and indicates the total packets
  offloaded
```

- 要查看设备的 Nitrox V 加密加速器统计信息，请使用以下命令：

```
ciscoasa# show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
<snip>
[Offloaded SSL Input statistics, Pipe 0]
      Input packets: 290593023
      Input bytes: 147049729714
      Decrypted packets: 290593023
      Decrypted bytes: 147049729714
   [Offloaded SSL Output statistics, Pipe 0]
      Output packets: 254271808
      Output bytes: 136352952720
      Encrypted packets: 254271808
      Encrypted bytes: 136352952720
.
.
.
```

配置特定流量类的连接设置（所有服务）

可以使用服务策略配置特定流量类的不同连接设置。使用服务策略进行以下操作：

- 自定义用于防御 DoS 和 SYN 泛洪攻击的连接限制和超时。
- 实施失效连接检测，以便让有效但空闲的连接保持活动状态。
- 在不需要 TCP 序列号随机化的情况下将其禁用。
- 自定义 TCP 规范器如何防止异常 TCP 数据包。
- 为受不对称路由限制的流量实施 TCP 状态绕行。绕行流量不受检查限制。
- 实施流控制传输协议 (SCTP) 状态绕行，以便关闭 SCTP 状态检测。
- 实施流量卸载，以提高受支持的硬件平台上的性能。
- 减少数据包的生存时间 (TTL)，以便 ASA 显示在跟踪路由输出中。

注释 如果减少生存时间，系统会丢弃 TTL 为 1 的数据包，但会为会话打开一个连接，前提是假设该连接可能包含具有更大 TTL 的数据包。请注意，某些数据包（如 OSPF hello 数据包）的发送 TTL = 1，因此递减生存时间可能会给透明模式 ASA 设备带来意想不到的后果。当 ASA 以路由模式运行时，递减生存时间设置不会影响 OSPF 进程。

可以为给定流量类配置这些设置的任意组合，但 TCP 状态绕行与 TCP 规范器自定义除外，因为这两者互相排斥。

提示 此过程显示用于通过 ASA 的流量的服务策略。还可以为管理（通过设备）流量配置最大连接数量和最大初期连接数量。

开始之前

如果要自定义 TCP 规范器，请先创建所需的 TCP 映射，再继续操作。

下文将单独介绍各个参数的 **set connection** 命令（用于连接限制和序列标准化）和 **set connection timeout** 命令。但是，可以在一行中输入这两个命令，如果您分别输入，这些命令会在配置中显示为一个命令。

过程

步骤 1 创建 L3/L4 类映射，以确定要为其自定义连接设置的流量。

```
class-map name
```

```
match parameter
```

示例：

```
hostname(config)# class-map CONNS
hostname(config-cmap)# match any
```

有关匹配语句的信息，请参阅为通过流量创建第 3/4 层类映射。

步骤 2 添加或编辑用于设置要对类映射流量执行的操作的策略映射，并确定类映射。

```
policy-map name
class name
```

示例：

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class CONNS
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。对于类映射，请指定在本程序前面部分中创建的类。

步骤 3 设置连接限制和 TCP 系列号随机化。（TCP 拦截。）

默认情况下，没有连接限制。如果实施了限制，系统就必须开始跟踪它们，这可能会增加CPU和内存的使用量，导致系统（尤其是集群中的系统）在负载较重的情况下出现运行问题。

- **set connection conn-max** *n* -（TCP、UDP、SCTP。）整个类允许的最大同时连接数，该值介于 0 到 2000000 之间。默认值为 0，允许无限制连接。对于 TCP 连接，这仅适用于已建立的连接。
  - 如果有两台服务器被配置为允许同时连接，则连接限制单独适用于每个配置的服务器。
  - 由于限制适用于一个类，一台攻击主机可占用所有连接而且使其余所有主机无法与该类匹配。
- **set connection per-client-max** *n* -（TCP、UDP、SCTP。）每个客户端允许的最大同时连接数，该值介于 0 到 2000000 之间。默认值为 0，允许无限制连接。此参数限制与类匹配的每台主机所允许的最大同步连接数。对于 TCP 连接，这包括已建立、半开和半闭的连接。
- **set connection embryonic-conn-max** *n* - 允许的最大同时初期 TCP 连接数，该值介于 0 到 2000000 之间。默认值为 0，允许无限制连接。通过设置非零限制启用 TCP 拦截，从而防止内部系统受到 DoS 攻击（这种攻击使用 TCP SYN 数据包对接口发起泛洪攻击）。另外，请设置每客户端选项，以防止 SYN 泛洪。
- **set connection per-client-embryonic-max** *n* - 每个客户端允许的最大同时初期 TCP 连接数，该值介于 0 到 2000000 之间。默认值为 0，允许无限制连接。
- **set connection syn-cookie-mss** *n* - 在达到初期连接限制时为初期连接的 SYN-Cookie 设置服务器最大分段大小 (MSS)，范围为 48 到 65535。默认值为 1380。仅当配置 **set connection embryonic-conn-max** 或 **per-client-embryonic-max** 时，此设置才有意义。

- **set connection random-sequence-number** {**enable** | **disable**} - 启用还是禁用 TCP 序列号随机化。默认情况下启用随机化。

示例：

```
hostname(config-pmap-c)# set connection conn-max 256 random-sequence-number disable
```

步骤 4 设置连接超时和失效连接检测 (DCD)。

下述默认值假设未使用 **timeout** 命令更改这些行为的全局默认值；全局默认值覆盖此处所述的值。输入 **0** 禁用计时器，以便连接永不超时。

- **set connection timeout embryonic** *hh*:*mm*:*ss* - TCP 初期（半开）连接关闭之前的超时时间，该值介于 0:0:5 到 1193:00:00 之间。默认值为 0:0:30。
- **set connection timeout idle** *hh*:*mm*:*ss* [**reset**] - 空闲超时期间，该期间过后建立的任何协议连接均将关闭，该值介于 0:0:1 到 1193:0:0 之间。默认值为 1:0:0。对于 TCP 流量，在连接超时情况下，**reset** 关键字会向 TCP 终端发送重置消息。

  默认 **udp** 空闲超时为 2 分钟。默认 **icmp** 空闲超时为 2 秒。默认 **esp** 和 **ha** 空闲超时为 30 秒。对于所有其他协议，默认空闲超时为 2 分钟。
- **set connection timeout half-closed** *hh*:*mm*:*ss* - - 半闭连接关闭前的空闲超时期间，该值介于 0:5:0（适用于 9.1(1) 和更早版本）或 0:0:30（适用于 9.1(2) 和更高版本）到 1193:0:0 之间。默认值为 0:10:0。半闭连接不受 DCD 影响。另外，当半闭连接断开时，ASA 不会发送重置。
- **set connection timeout dcd** [*retry-interval* [*max_retries*]] - 启用失效连接检测 (DCD)。在空闲连接过期前，ASA 会探测终端主机来确定连接是否有效。如果两台主机均响应，系统会保留连接，否则会释放连接。在透明防火墙模式下运行，必须为终端配置静态路由。不能在同时分流的连接上配置 DCD，因此要确保 DCD 和流量分流流量类别不重叠。使用 **show conn detail** 命令跟踪发起方和响应方发送的 DCD 探测数量。

  retry-interval 以 ***hh*:*mm*:*ss*** 格式设置每个未响应的 DCD 探测在发送另一个探测之前等待的时间段，该值介于 0:0:1 到 24:0:0 之间。默认值为 0:0:15。max-retries 设置 DCD 在宣称连接为失效连接之前可连续失败重试的次数。最小值为 1，最大值为 255。默认值为 5。

  对于在集群或高可用性配置中运行的系统，我们建议您不要将间隔设置为小于一分钟 (0:1:0)。如果需要在系统之间移动连接，则所需的更改需要花费超过 30 秒，并且连接可能会在完成更改之前被删除。

示例：

```
hostname(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0
half-closed 0:20:0 dcd
```

步骤 5 减少与类匹配的数据包的生存时间 (TTL)：**set connection decrement-ttl**

要允许跟踪路由通过 ASA（作为其中一跳显示 ASA），需要使用此命令连同 **icmp unreachable** 命令。

示例：

```
hostname(config)# class-map global-policy
hostname(config-cmap)# match any
hostname(config-cmap)# exit
hostname(config)# policy-map global_policy
hostname(config-pmap)# class global-policy
hostname(config-pmap-c)# set connection decrement-ttl
hostname(config-pmap-c)# exit
hostname(config)# icmp unreachable rate-limit 50 burst-size 6
```

步骤 6 设置高级连接选项。

高级选项指在正常情况下无需使用的专用配置。使用 **set connection advanced-options** 命令进行配置。

- **set connection advanced-options** *tcp_map_name* - 通过应用 TCP 映射自定义 TCP 规范器行为。有关详细信息，请参阅自定义异常 TCP 数据包处理（TCP 映射、TCP 规范器），第 7 页。
- **set connection advanced-options tcp-state-bypass**- 实施 TCP 状态绕行。有关详细信息，请参阅绕过非对称路由的 TCP 状态检查（TCP 状态绕行），第 11 页。
- **set connection advanced-options sctp-state-bypass**- 实施 SCTP 状态绕行，以便关闭 SCTP 状态检测。有关详细信息，请参阅SCTP 状态检测。
- **set connection advanced-options flow-offload** -（仅限 FXOS 1.1.3 或更高版本 Firepower 4100/9300 机箱 中的 ASA。）实施流量卸载。将符合条件的流量卸载到使用 NIC 本身交换流量的超快路径。此外，还必须输入 **flow-offload enable** 命令，该命令不属于服务策略。

示例：

```
hostname(config-pmap-c)# set connection advanced-options tcp_map1
```

步骤 7 如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

Global 关键字指示将策略映射应用于所有接口，而 **interface** 指示仅将策略应用于一个接口。仅允许存在一个全局策略。可以通过向接口应用服务策略来覆盖该接口上的全局策略。每个接口只能应用一个策略映射。

示例

以下示例设置所有流量的连接限制和超时：

```
hostname(config)# class-map CONNS
```

```
hostname(config-cmap)# match any
hostname(config-cmap)# policy-map CONNS
hostname(config-pmap)# class CONNS
hostname(config-pmap-c)# set connection conn-max 1000 embryonic-conn-max 3000
hostname(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0
half-closed 0:20:0 dcd
hostname(config-pmap-c)# service-policy CONNS interface outside
```

可以输入带多个参数的 **set connection** 命令，也可以作为单独命令输入每个参数。在运行配置中，ASA 会将这些命令组合成一行。例如，如果在类配置模式下输入了以下两个命令：

```
hostname(config-pmap-c)# set connection conn-max 600
hostname(config-pmap-c)# set connection embryonic-conn-max 50
```

show running-config policy-map 命令的输出将在单一组合命令中显示两个命令的结果：

```
set connection conn-max 600 embryonic-conn-max 50
```

配置 TCP 选项

您可以配置选项，以控制 TCP 行为的某些方面。这些设置的默认值适合大多数网络。

过程

步骤 1 (CLI)。配置 TCP 重置行为。

service { **resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside** }

- **resetinbound**。为所有试图通过 ASA 并被 ASA 根据访问列表或 AAA 设置拒绝的入站 TCP 会话发送 TCP 重置。ASA 还会对访问列表或 AAA 允许但不属于现有连接且被状态防火墙拒绝的数据包发送重置。相同安全级别接口之间的流量也会受到影响。不启用此选项时，ASA 会静默地丢弃被拒绝的数据包。如果未指定接口，则此设置适用于所有接口。
- **resetoutbound**。为所有试图通过 ASA 并被 ASA 根据访问列表或 AAA 设置拒绝的出站 TCP 会话发送 TCP 重置。ASA 还会对访问列表或 AAA 允许但不属于现有连接且被状态防火墙拒绝的数据包发送重置。相同安全级别接口之间的流量也会受到影响。不启用此选项时，ASA 会静默地丢弃被拒绝的数据包。默认情况下，此选项已启用。例如，您可能希望禁用出站重置，以减少流量风暴期间的 CPU 负载。
- **resetoutside**。对终止于安全性最低的接口且被 ASA 根据访问列表或 AAA 设置拒绝的 TCP 数据包启用重置。ASA 还会对访问列表或 AAA 允许但不属于现有连接且被状态防火墙拒绝的数据包发送重置。不启用此选项时，ASA 会静默地丢弃被拒绝的数据包。

  建议您将此选项与接口 PAT 配合使用。此选项允许 ASA 终止来自外部 SMTP 或 FTP 服务器的 IDENT。主动重置这些连接可避免 30 秒的超时延迟。

步骤 2 设置 TCP MSS 可确保直通流量的最大 TCP 分段大小不超过您设置的值，且最大值不小于指定大小。

sysopt connection tcpmss [**minimum**] *bytes*

不带 **minimum** 关键字。以字节为单位设置 TCP 最大分片大小，范围在 48 和任何最大值之间。默认值为 1380 字节。您可以禁用此功能，只需将字节数设置为 0。

minimum。覆盖最大段大小，使其不小于指定字节，介于 48 和 65535 字节之间。默认情况下，此功能已禁用（设置为 0）。

步骤 3 设置 TCP 连接等待时间。

sysopt connection timewait

使用此命令可强制每个 TCP 连接在最后一个正常 TCP 关闭序列后处于缩短的 TIME_WAIT 状态（至少 15 秒）。如果终端主机应用默认的 TCP 终止序列是同时关闭，则可能需要使用此功能。

步骤 4 设置 TCP 未处理分段的最大数量。

sysopt connection tcp-max-unprocessed-seg 数据段

设置 TCP 未处理网段的最大数量，从 6 到 24 不等。默认值为 6。如果您发现 SIP 电话未连接到呼叫管理器，您可以尝试增加未处理的 TCP 分段的最大数量。

监控连接

可以使用以下命令监控连接：

- **show conn** [**detail**]

  显示连接信息。详细信息使用标志来表示特殊连接特性。例如，“b”标志表示会对流量应用 TCP 状态绕行。

  使用 **detail** 关键字时，您可以查看有关失效连接检测 (DCD) 探测的信息，这会显示发起方和响应方探测连接的频率。例如，对于启用 DCD 的连接，其连接详细信息如下所示：

```
TCP dmz: 10.5.4.11/5555 inside: 10.5.4.10/40299,
    flags UO , idle 1s, uptime 32m10s, timeout 1m0s, bytes 11828,
cluster sent/rcvd bytes 0/0, owners (0,255)
  Traffic received at interface dmz
        Locally received: 0 (0 byte/s)
  Traffic received at interface inside
        Locally received: 11828 (6 byte/s)
  Initiator: 10.5.4.10, Responder: 10.5.4.11
  DCD probes sent: Initiator 5, Responder 5
```

- **show flow-offload** {**info** [**detail**] | **cpu** | **flow** [**count** | **detail**] | **statistics**}

  显示有关数据流分流的信息，包括常规状态信息、用于分流的 CPU 使用量、已分流的数据流数和详细信息，以及已分流的数据流统计信息。

- **show service-policy**

  显示服务策略统计信息，包括失效连接检测 (DCD) 统计信息。

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**]

  查看遭受攻击的前 10 名受保护服务器。**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。

注释 在ASA配置中，初期连接（尚未完成三次握手过程的连接请求）会快速关闭，并且不会在主用设备和备用设备之间同步。此设计可确保高可用性系统的效率和安全性。因此，两台ASA设备上的连接数可能存在差异，这是预期行为。

连接设置的历史记录

功能名称	平台版本	说明
TCP 状态绕行	8.2(1)	引入了此功能。引入了以下命令：**set connection advanced-options tcp-state-bypass**。
所有协议的连接超时	8.2(2)	空闲超时已被更改为应用于所有协议，而不仅是 TCP 协议。 修改了以下命令：**set connection timeout**
使用备份静态路由的连接超时	8.2(5)/8.4(2)	当多个静态路由以不同的指标共存于一个网络时，ASA 将使用创建连接时指标最好的路由。如果有更好的路由变得可用，则此超时可让连接关闭，以便使用更好的路由重新建立连接。默认值为 0（连接永不超时）。要利用此功能，请将超时更改为新值。 修改了以下命令：**timeout floating-conn**。
可配置 PAT 转换超时	8.4(3)	如果 PAT 转换超时（默认为 30 秒后）且 ASA 使用该端口执行新的转换，因为以前的连接在上游设备中可能仍处于打开状态，有些上游路由器可能会拒绝该新连接。PAT转换超时现在可配置为一个介于 30 秒到 5 分钟之间的值。 引入了以下命令：**timeout pat-xlate**。 此功能在 *8.5(1)* 或 *8.6(1)* 中不可用。
服务策略规则增加的最大连接数限制	9.0(1)	服务策略规则的最大连接数从 65535 增加至 2000000。 修改了以下命令：**set connection conn-max**、**set connection embryonic-conn-max**、**set connection per-client-embryonic-max**、**set connection per-client-max**。

功能名称	平台版本	说明
半闭超时最小值减小至 30 秒	9.1(2)	全局超时和连接超时的半闭超时最小值从 5 分钟缩短至 30 秒，以提供更好的 DoS 保护。 修改了以下命令：**set connection timeout half-closed**、**timeout half-closed**。
路由融合的连接等待超时。	9.4(3) 9.6(2)	现在，您可以配置在连接使用的路由不再存在或不活动时，系统应保持连接的时间。如果路由在此抑制期间未变为活动状态，连接将被释放。您可以减小抑制计时器，使路由汇聚更快速地进行。但是，默认值 15 秒适合大多数网络，可以防止路由摆动。 添加了以下命令：**timeout conn-holddown**。
SCTP 空闲超时和 SCTP 状态绕行	9.5(2)	您可以为 SCTP 连接设置空闲超时。另外，您还可以启用 SCTP 状态绕行，关闭某一类流量的 SCTP 状态检测。 添加或修改了以下命令：**timeout sctp**、**set connection advanced-options sctp-state-bypass**。
Firepower 9300 上 ASA 的数据流分流。	9.5(2.1)	您可以标识应从 ASA 中分流并直接在 NIC（在 Firepower 9300 上）中切换的流量。此功能可提升数据中心中的大数据流性能。 此功能要求具有 FXOS 1.1.3 版本。 添加或修改了以下命令：**clear flow-offload**、**flow-offload enable**、**set-connection advanced-options flow-offload**、**show conn detail** 和 **show flow-offload**。
Firepower 4100 系列 上 ASA 的数据流分流支持。	9.6(1)	您可以标识应从 ASA 中分流并直接在 Firepower 4100 系列 的 NIC 中切换的流量。 此功能需要 FXOS 1.1.4。 此功能没有新的命令或 ASDM 屏幕。
透明模式下组播连接的数据流分流支持。	9.6(2)	现在，您可以卸载将在透明模式 Firepower 4100 和 9300 系列设备的网络接口卡中直接切换的组播连接。组播卸载仅适用于有且只有两个接口的网桥组。 对于此功能，没有新的命令或 ASDM 菜单项。

功能名称	平台版本	说明
TCP 选项处理方式的变化。	9.6(2)	现在，当配置 TCP 映射时，您可以在数据包的 TCP 报头中为 TCP MSS 和 MD5 选项指定操作。此外，对 MSS、timestamp、window-size 和 selective-ack 选项的默认处理已更改。以前，允许这些选项，即使报头中具有指定类型的多个选项也是如此。现在，默认情况下会丢弃包含指定类型的多个选项的数据包。例如，以前允许具有 2 个 timestamp 选项的数据包，而现在将丢弃该数据包。 您可以配置 TCP 映射，以针对 MD5、MSS、selective-ack、timestamp 和 window-size 允许同一类型的多个选项。对于 MD5 选项，以前的默认设置为清除该选项，而现在的默认设置是允许它。您还可以丢弃包含 MD5 选项的数据包。对于 MSS 选项，您可以在 TCP 映射中设置最大分段大小（每个流量类）。所有其他 TCP 选项的默认设置均保持不变：被清除。 修改了以下命令：**timeout igp stale-route**。
内部网关协议的过时路由超时	9.7(1)	现在您可以配置超时，用于删除内部网关协议（如 OSPF）的陈旧路由。 添加了以下命令：**timeout igp stale-route**。
ICMP 全局超时错误	9.8(1)	现在可以设置 ASA 在 接收 ICMP echo-reply 数据包后后、删除 ICMP 连接之前的空闲时间。如果禁用了此超时（默认），并且启用了 ICMP 检查，则 ASA 将在接收 echo-reply 后立即删除 ICMP 连接；因此将丢弃为该连接（现已关闭）生成的任何 ICMP 错误。此超时可以延迟删除 ICMP 连接，使您能够接收重要的 ICMP 错误。 添加了以下命令：**timeout icmp-error**
TCP 状态绕行的默认空闲超时	9.10(1)	TCP 状态绕行连接的默认空闲超时现在为 2 分钟，而不是 1 小时。
集群中的“死连接检测”(DCD) 支持的发起方和响应方信息。	9.13(1)	如果启用死连接检测(DCD)，则可以使用该 **show conn detail** 命令获取有关发起人和响应方的信息。通过死连接检测，您可以保持非活动连接，并且 **show conn** 输出会告诉您终端的探测频率。此外，在集群中现在还支持 DCD。 新增/修改的命令：**show conn**（仅输出）
配置初期连接的最大分段大小 (MSS)。	9.16（1）	您可以配置服务策略，以在达到初期连接限制时为初期连接的 SYN-Cookie 设置服务器最大分段大小 (MSS)。这对于还设置初期连接最大值的服务策略非常重要。 新增的或更改的命令：**set connection syn-cookie-mss**。

功能名称	平台版本	说明
IPsec 流分流。	9.18(1)	在 Cisco Secure Firewall 3100上，默认情况下会分流 IPsec 流。初始设置 IPsec 站点间 VPN 或远程访问 VPN 安全关联 (SA) 后，IPsec 连接将被分流到设备中的现场可编程门阵列 (FPGA)，这应该会提高设备性能。 添加了以下命令：**clear flow-offload-ipsec**、**flow-offload-ipsec**、**show flow-offload-ipsec**
DTLS 加密加速	9.22(1)	Cisco Secure Firewall 4200 和 3100 系列支持 DTLS 加密加速。硬件执行 DTLS 加密和解密，并提高 DTLS 加密和 DTLS 解密流量的吞吐量。硬件还会对出口加密数据包执行优化，以改善延迟。 新增/修改的命令： **flow-offload-dtls**、**flow-offload-dtls egress-optimization**

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。