# 服务策略

您可以使用 Firepower Threat Defense 服务策略将服务应用于特定流量类。例如，可以使用服务策略创建特定于某项 TCP 应用而非应用于所有 TCP 应用的超时配置。服务策略由多个应用于某个接口或全局应用的操作或规则组成。



# 有关 Firepower 威胁防御服务策略

您可以使用 Firepower 威胁防御服务策略将服务应用于特定流量类。使用服务策略，您不仅仅可以将相同的服务应用于进入设备或给定接口的所有连接。

流量类是接口和扩展访问控制列表 (ACL) 的组合。ACL“允许”规则确定哪些连接是该类的一部分。ACL 中的任何"被拒绝"流量只是没有应用于其上的服务： 这些连接实际上没有被丢弃。您可以使用 IP 地址和 TCP/UCP 端口根据需要精确识别匹配的连接。

有两种类型的流量类：

- 基于接口的规则 - 如果在服务策略规则中指定安全区域或接口组，则此规则适用于通过作为接口对象一部分的任何接口的 ACL“允许”流量。

  对于指定功能，适用于入口接口的基于接口的规则始终优先于全局规则：如果基于入口接口的规则应用于连接，则忽略任何匹配的全局规则。如果没有适用的入口接口或全局规则，则应用出口接口上的接口服务规则。

- 全局规则 - 这些规则适用于所有接口。如果基于接口的规则不适用于连接，则系统将检查全局规则并将其应用于 ACL“允许”的任何连接。如果没有适用的规则，则连接将继续，而不应用任何服务。

对于指定功能，给定连接只能匹配一个基于接口的流量类或全局流量类。指定接口对象/流量组合最多包含一条规则。

服务策略规则在访问控制规则之后应用。这些服务仅针对您允许的连接进行配置。

# 服务策略如何与 FlexConfig 和其他功能关联

在版本 6.3(0) 之前，您可以使用 TCP_Embryonic_Conn_Limit 和 TCP_Embryonic_Conn_Timeout 预定义 FlexConfig 对象配置连接相关服务规则。您应该使用 Firepower 威胁防御服务策略删除这些对象并重新配置规则。如果已创建任何自定义 FlexConfig 对象以实施任何连接相关功能（即，**set connection** 命令），则还应删除这些对象并通过服务策略实施这些功能。

由于连接相关服务策略功能被视为与其他服务规则实施功能独立的功能组，因此应该不会遇到流量类重叠的问题。但是，进行以下配置请注意：

- 使用服务策略 CLI 实施 QoS 策略规则。这些规则在基于连接的服务策略规则之前应用。但是，QoS 和连接设置都可以应用于相同或重叠的流量类。
- 您可以使用 FlexConfig 策略来实施自定义应用检测和 NetFlow。使用 **show running-config** 命令检查已配置服务规则的 CLI，包括 **policy-map**、**class-map** 和 **service-policy** 命令。Netflow 和应用检测与 QoS 和连接设置兼容，但是您需要在实施 FlexConfig 之前了解现有配置。在应用检测和 Netflow 之前应用连接设置。

**注释** 从 Firepower 威胁防御服务策略创建的流量类名为 **class_map_***ACLname*，其中 *ACLname* 是服务策略规则中使用的扩展 ACL 对象的名称。

# 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 防火墙威胁防御 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。配置 Firepower 威胁防御平台策略中的全局超时。依次选择**设备** > **平台设置**。
- **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）防火墙威胁防御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，防火墙威胁防御 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。您可以使用 FlexConfig 策略配置 TCP 规范化。
- **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。

# 服务策略的要求和前提条件

**型号支持**

威胁防御

**支持的域**

任意

**用户角色**

管理员

访问管理员

网络管理员

# 服务策略准则和限制

- 服务策略仅适用于路由或交换机接口，无论是处于路由模式还是透明模式。这些策略不适用于内联集或被动接口。
- 对于指定接口或全局策略，最多可以有25个流量类。具体而言，这意味着对于指定安全区域或接口组，全局策略的服务策略规则不能超过25条。但是，对于接口而言，由于同一接口可以同时出现在安全区域和接口组中，因此请注意，实际限制基于接口，而不是基于区域/组。因此，根据所在区域/组的成员资格，您可能无法为每个区域/组设置 25 条规则。
- 对于指定接口对象/流量组合，最多只能包含一条规则。

- 当对配置进行服务策略更改后，所有新连接都将使用新的服务策略。现有连接将继续使用在连接建立时配置的策略。如果希望所有连接立即使用新策略，则需要断开当前连接，以便使用新策略重新连接。在 SSH 或控制台 CLI 会话中，输入 **clear conn** 或 **clear local-host** 命令。

# 配置威胁防御服务策略

您可以使用威胁防御服务策略将服务应用于特定流量类。例如，可以使用服务策略创建特定于某项 TCP 应用而非应用于所有 TCP 应用的超时配置。服务策略由多个应用于某个接口或全局应用的操作或规则组成。

### 过程

**步骤 1** 选择 **策略** > **访问控制标题** > **访问控制**，点击要编辑其威胁防御服务策略的访问控制策略的 **编辑** ()。

**步骤 2** 从数据包流末尾的**更多 (More)** 下拉箭头中选择**高级设置 (Advanced Settings)**。

**步骤 3** 点击**威胁防御服务策略 (Threat Defense Service Policy)** 组中的 **编辑** ()。

系统将打开一个对话框，显示现有策略。该策略由有序的规则列表组成，这些规则分为全局规则（适用于所有接口）和基于接口的规则。表格中显示了接口对象和扩展访问控制列表名称（其组合定义规则的流量类）以及所应用的服务。

**步骤 4** 执行以下任一操作：

- 点击**添加规则**以创建新规则。请参阅配置服务策略规则，第 4 页。
- 点击**编辑** ()以编辑现有规则。请参阅配置服务策略规则，第 4 页。
- 点击 **删除** () 以删除规则。
- 点击规则并将其拖动到新位置，以移动规则。您无法在接口和全局列表之间拖动规则，而是必须编辑规则以更改接口/全局设置。列表中与连接匹配的第一条规则将应用于连接。

**步骤 5** 完成策略编辑后，点击**确定** 。

**步骤 6** 在**高级**选项卡窗口中点击**保存**。在您点击保存之前，更改不会被保存。

# 配置服务策略规则

配置服务策略规则，以将服务应用于特定流量类。

### 开始之前

转到**对象** > **对象管理** > **访问列表** > **扩展**并创建扩展访问列表，定义规则适用的流量。此规则适用于与扩展访问列表中的“允许”规则匹配的任何连接。准确定义ACL规则，以便您的服务策略规则仅适用于需要该服务的流量。

如果要创建基于接口的规则，则还必须在已分配的设备上配置接口，并将其添加到安全区域或接口组。

## 过程

**步骤 1** 如果尚未在“威胁防御服务策略”对话框中，请选择 **策略** > **访问控制标题** > **访问控制**，编辑访问控制策略，从数据包流行末尾的**更多**下拉箭头中选择**高级设置**，然后编辑**威胁防御服务策略**。

**步骤 2** 执行以下任一操作：

- 点击**添加规则**以创建新规则。
- 点击**编辑** (✎)以编辑现有规则。

系统将打开服务策略规则向导，逐步指导您完成配置规则的流程。

**步骤 3** 在**接口对象**步骤中，选择用于定义将使用此策略的接口的选项。

- **全局应用** - 选择此选项以创建适用于所有接口的全局规则。
- **选择接口对象** - 选择此选项以创建基于接口的规则。然后，选择包含所需接口的安全区域或接口对象，并点击 > 以将其移到 **下一个** 选定的列表。系统将在所选对象中包含的每个接口上配置此服务策略规则；而不是在区域/组本身配置此规则。

在满足接口条件后点击。

**步骤 4** 在**流量传输 (Traffic Flow)** 步骤中，选择用于定义规则适用的连接的扩展 ACL 对象，然后点击**下一步 (Next)**。

**步骤 5** 在**连接设置**步骤中，配置要应用于此流量类的服务。

- **启用 TCP 状态绕行**（仅适用于 TCP 连接）- 实施 TCP 状态绕行。任何检测引擎都不会检查受 TCP 状态绕行影响的连接，它们会绕过所有 TCP 状态检查和 TCP 规范化。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 7 页。

  **注释**
  在进行故障排除或无法解析非对称路由时使用 TCP 状态绕行。此功能将禁用多项安全功能，如果您没有使用狭义定义的流量类正确实施该功能，则可能会导致大量连接。

- **随机生成 TCP 序列号**（仅适用于 TCP 连接）- 启用还是禁用 TCP 序列号随机化。默认情况下启用随机化。有关详细信息，请参阅禁用 TCP 序列随机化，第 11 页。
- **启用递减 TTL**（仅适用于 TCP 连接）- 减少与类匹配的数据包的生存时间 (TTL)。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（例如 OSPF hello 数据包）发送时 TTL = 1，因此减去生存时间可能会导致意外后果。

  **注释**
  如果希望 威胁防御设备显示在跟踪路由中，必须配置递减 TTL 选项并在平台设置策略中设置 ICMP 不可达速率限制。请参阅使 威胁防御 设备显示在跟踪路由上，第 15 页。

- **连接** - 整个类允许的连接数限制。您可以配置以下选项：
  - **最大 TCP 和 UDP 数**（仅适用于 TCP/UDP 连接）- 整个类允许的最大同步 TCP 或 UDP 连接数，该值介于 0 到 2000000 之间。对于 TCP，这仅适用于已建立的连接。默认值为 0，允许无限制连接。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。设置每个客户端的限制，以缓解这一问题。
  - **最大初期连接数**（仅适用于 TCP 连接）- 允许的最大同步初期 TCP 连接数（未完成 TCP 握手的连接数），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。有关详细信息，请参阅保护服务器不受 SYN 洪流 DoS 攻击（TCP 拦截），第 12 页。
- **每个客户端连接数** - 指定客户端（源 IP 地址）的连接数限制。您可以配置以下选项：
  - **最大 TCP 和 UDP 数**（仅适用于 TCP/UDP 连接）- 每个客户端允许的最大同步连接数，该值介于 0 到 2000000 之间。对于 TCP 连接，这包括现有、半开和半闭连接。默认值为 0，允许无限制连接。此选项限制与类匹配的每台主机所允许的最大同步连接数。
  - **最大初期连接数**（仅适用于 TCP 连接）- 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。有关详细信息，请参阅保护服务器不受 SYN 洪流 DoS 攻击（TCP 拦截），第 12 页。
- **连接同步 Cookie MSS (Connections Syn Cookie MSS)** - 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。仅当您为连接和/或每个客户端配置了**最多初期连接次数 (Maximum Embryonic)** 时，此设置才有意义。
- **连接超时** - 要应用于流量类的超时设置。这些超时设置会覆盖平台设置策略中定义的全局超时设置。您可以配置以下内容：
  - **初期连接数**（仅适用于 TCP 连接）- 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。
  - **半闭**（仅适用于 TCP 连接）- 半闭连接关闭之前经过的空闲超时时间，该值介于 0:0:30 到 1193:0:0 之间。默认值为 0:10:0。半闭连接不受失效连接检测 (DCD) 影响。此外，如果取消半闭连接，系统将不发送重置消息。
  - **空闲**（仅适用于 TCP、UDP、ICMP、IP 连接）- 任何协议的已建立连接关闭之前经过的空闲超时时间，该值介于 0:0:1 到 1193:0:0 之间。除非您选择“TCP 状态绕行”选项（其中默认值为 0:2:0），否则默认值为 1:0:0。
  - **超时后重置连接**（仅适用于 TCP 连接）- 是否在空闲连接删除后将 TCP RST 数据包发送到两个终端系统。
- **失效连接检测 (DCD)** - 是否启用失效连接检测 (DCD)。在空闲连接失效前，系统会探测终端主机以确定连接是否有效。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。您无法在也已分流的连接上配置DCD，因此请勿在预过滤器策略中的快速路径连接上配置 DCD。在 CLI 中使用 **show conn detail** 命令跟踪发起方和响应方发送的 DCD 探测数量。

配置以下选项：

- **检测超时** - 每个 DCD 探测器无响应之后发送另一个探测器之前的等待时间（采用 hh:mm:ss 格式），该值介于 0:0:1 到 24:0:0 之间。默认值为 0:0:15。

  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。

- **检测重试次数** - DCD 在宣称连接为失效连接之前可连续失败重试的次数，该值介于 1 到 255 之间。默认值为 5。

**步骤 6** 点击**完成**以保存所做的更改。

此规则将添加到相应列表的底部，即接口或全局。全局规则以自上而下的顺序匹配。接口列表中的规则按自上而下的顺序匹配每个接口对象。请将狭义定义的流量类的规则置于更广泛的规则之上，以确保应用正确的服务。您可以通过拖放操作在每个列表中移动规则。您无法在列表之间移动规则。

# 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 防火墙威胁防御 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。

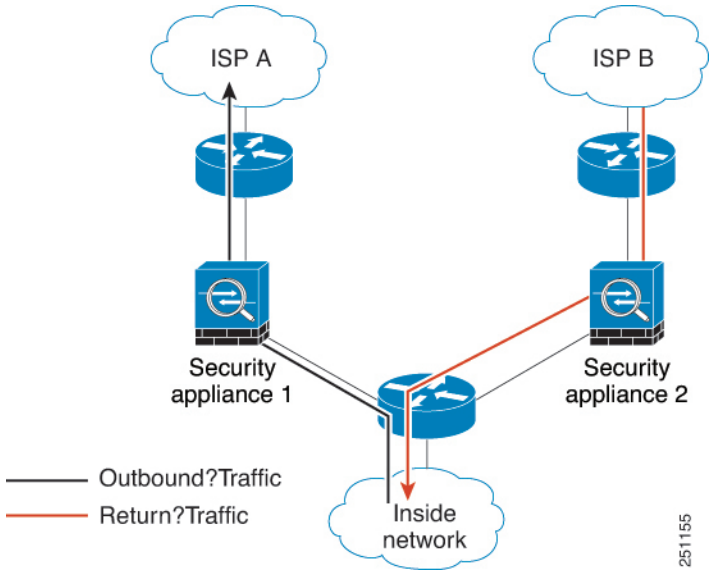
## 非对称路由问题

默认情况下，所有经过防火墙威胁防御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。防火墙威胁防御 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 防火墙威胁防御。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 防火墙威胁防御 。

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 防火墙威胁防御：

图 *1:* 非对称路由




如果在上游路由器中配置了不对称路由，且流量在两个防火墙威胁防御之间交替，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 防火墙威胁防御 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 防火墙威胁防御，因此不会对 TCP 状态绕行流量应用检测。
- Snort 检测 - 检测要求入站和出站流量通过同一设备。但是，对于 TCP 状态绕行流量，不会自动绕过 Snort 检测。还必须针对您配置 TCP 状态绕行的相同流量类配置预过滤器快速路径规则。否则，数据包可能会被意外丢弃，因为 TCP 规范器也未启用。
- TCP 拦截、最大初期连接限制、TCP 序列号随机化 - 防火墙威胁防御 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。
- 在内联或内联分流接口上使用 TCP 状态绕行时，无法使用 TLS 服务器身份发现。

### TCP 状态绕行 NAT 准则

由于转换会话是为每个 防火墙威胁防御 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。您还必须为相同的流量配置相应的预过滤器快速路径策略，以确保此流量也绕过检查。

由于绕行会降低网络安全性，请尽可能限制网络应用。

### 过程

**步骤 1** 创建定义流量类的扩展 ACL。

例如，要为从 10.1.1.1 到 10.2.2.2 的 TCP 流量定义流量类，请执行以下操作：

a) 选择**对象 (Object)** > **对象管理 (Object Management)**。
b) 从目录中选择**访问列表** > **扩展**。
c) 点击**添加扩展访问列表**。
d) 为对象输入一个**名称**，例如 bypass。
e) 点击**添加**以添加规则。
f) 保持**允许**操作。
g) 在**源**列表下方输入 10.1.1.1 并点击**添加 (Add)**，然后在**目标**列表下方输入 10.2.2.2 并点击**添加 (Add)**。
h) 点击**端口 (Port)**，选择**选定源端口 (Selected Source Ports)** 列表下方的 **TCP (6)**，然后点击**添加 (Add)**。不要输入端口号，只需添加 TCP 作为协议，这将覆盖所有端口。
i) 在“扩展访问列表条目”对话框中点击**添加**，以将规则添加到 ACL。
j) 点击“扩展访问列表对象”对话框中的**保存**，以保存 ACL 对象。

**步骤 2** 配置 TCP 状态绕行服务策略规则。

例如，要为此流量类全局配置 TCP 状态绕行，请执行以下操作：

a) 选择**策略** > **访问控制标题** > **访问控制**，然后编辑分配给需要此服务的设备的策略。
b) 点击数据包流行末尾的**更多 (More)** 下拉箭头中的**高级设置 (Advanced Settings)**，然后点击**威胁防御服务策略 (Threat Defense Service Policy)** 的 **编辑** (✎)。
c) 点击**添加规则**。
d) 选择**全局应用 (Apply Globally)** > **下一步 (Next)**。
e) 选择为此规则创建的扩展 ACL 对象，然后点击**下一步 (Next)**。
f) 选择**启用 TCP 状态绕行**。
g) （可选。）调整绕行连接的**空闲**超时。默认值为 2 分钟。
h) 点击**完成**以添加规则。如有必要，将规则拖放到服务策略中的所需位置。

i) 点击**确定 (OK)** 以保存对服务策略所做的更改。
j) 点击**高级**中的**保存**，以保存对访问控制策略所做的更改。

**步骤 3** 配置流量类的预过滤器快速路径规则。

不能在预过滤器规则中使用ACL对象，因此您需要直接在预过滤器规则中重新创建流量类，或者通过首先创建定义类的网络对象来创建流量类。

以下程序假定您已经在访问控制策略中附加了预过滤器策略。如果尚未创建预过滤器策略，请转至**策略 (Policies)** > **预过滤器 (Prefilter)**，然后首先创建策略。然后，您可以按照此程序将其附加到访问控制策略并创建规则。

在我们的示例中，此程序为 10.1.1.1 到 10.2.2.2 的 TCP 流量创建快速路径规则。

a) 选择**策略** > **访问控制标题** > **访问控制**，然后编辑包含 TCP 绕行服务策略规则的策略。
b) 点击**预过滤器策略**链接，该策略位于策略说明的左下方。
c) 在“预过滤器策略”对话框中，选择要分配给设备的策略（如果尚未选择正确的策略）。不要点击“确定”。

由于您无法将规则添加到默认预过滤器策略，因此必须选择自定义策略。

d) 在“预过滤器策略”对话框中，点击**编辑**(✎)。此操作将打开一个新的浏览器窗口，您可以在其中编辑策略。
e) 点击**添加预过滤器规则**并配置包含以下属性的规则。

- **名称** - 您觉得有意义的任何名称均可，例如 TCPBypass。
- **操作** - 选择**快速路径**。
- **接口对象 (Interface Objects)** - 如果已将 TCP 状态绕行配置为全局规则，则为源和目标接口保留默认值“any”。如果已创建基于接口的规则，则在**源接口对象**列表中选择用于规则的相同接口对象，并将“any”作为目标接口。
- **网络 (Networks)** - 将 10.1.1.1 添加到**源网络 (Source Networks)** 列表中，并将 10.2.2.2 添加到**目标网络 (Destination Networks)** 列表中。您可以使用网络对象或手动添加地址。
- **端口 (Ports)** - 在**选定源端口 (Selected Source Ports)** 下, 选择 TCP(6)，**不要输入端口**，然后点击**添加 (Add)**。这会将规则应用于所有（且仅限）TCP 流量（不考虑 TCP 端口号）。

f) 点击**添加**以将规则添加到预过滤器策略中。
g) 点击**保存**以保存对预过滤器策略所做的更改。

现在您可以关闭预过滤器编辑窗口并返回访问控制策略编辑窗口。

h) 在访问控制策略编辑窗口中，“预过滤器策略”对话框仍处于打开状态。点击**确定 (OK)** 以保存对预过滤器策略分配所做的更改。
i) 如果您做出了更改，则点击访问控制策略上的**保存**以保存已更改的预过滤器策略分配。

现在您可以将更改部署到受影响的设备。

# 禁用 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。威胁防御设备会为通过入站和出站两个方向的 TCP SYN 随机生成 ISN。

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。以下是您可能希望禁用随机化的一些情况：

- 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。
- 如果通过此设备使用 eBGP 多跳，并且 eBGP 对等设备在使用 MD5。随机化会中断 MD5 校验和。
- 如果使用要求 威胁防御设备不为连接随机生成序列号的 WAAS 设备。
- 如果为 ISA 3000 启用硬件旁路，当 ISA 3000 不再是数据路径时的一部分时，TCP 连接将被丢弃。

## 过程

**步骤 1** 创建定义流量类的扩展 ACL。

例如，要从任何主机到 10.2.2.2 的 TCP 流量定义流量类，请执行以下操作：

a) 选择**对象 (Object)** > **对象管理 (Object Management)**。
b) 从目录中选择**访问列表** > **扩展**。
c) 点击**添加扩展访问列表**。
d) 为对象输入一个**名称**，例如 preserve-sq-no。
e) 点击**添加**以添加规则。
f) 保持**允许**操作。
g) 将**源 (Source)** 列表留空，在**目标 (Destination)** 列表下方输入 10.2.2.2，然后点击**添加 (Add)**。
h) 点击**端口 (Port)**，选择**选定源端口 (Selected Source Ports)** 列表下方的 **TCP (6)**，然后点击**添加 (Add)**。不要输入端口号，只需添加 TCP 作为协议，这将覆盖所有端口。
i) 在“扩展访问列表条目”对话框中点击**添加**，以将规则添加到 ACL。
j) 点击“扩展访问列表对象”对话框中的**保存**，以保存 ACL 对象。

**步骤 2** 配置将禁用 TCP 序列号随机化的服务策略规则。

例如，要为此流量类全局禁用随机化，请执行以下操作：

a) 选择**策略** > **访问控制标题** > **访问控制**，然后编辑分配给需要此服务的设备的策略。
b) 点击数据包流行末尾的**更多 (More)** 下拉箭头中的**高级设置 (Advanced Settings)**，然后点击**威胁防御服务策略 (Threat Defense Service Policy)** 的 **编辑** (✎)。

c) 点击**添加规则**。
d) 选择**全局应用 (Apply Globally)** > **下一步 (Next)**。
e) 选择为此规则创建的扩展 ACL 对象，然后点击**下一步 (Next)**。
f) 取消选择**随机生成 TCP 序列号**。
g) （可选。）根据需要调整其他连接选项。
h) 点击**完成**以添加规则。如有必要，将规则拖放到服务策略中的所需位置。
i) 点击**确定 (OK)** 以保存对服务策略所做的更改。
j) 点击**高级**中的**保存**，以保存对访问控制策略所做的更改。

现在您可以将更改部署到受影响的设备。

# 服务策略规则示例

以下主题提供服务策略规则示例。

## 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， 威胁防御 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 威胁防御 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。

设置连接限制可以保护服务器免受 SYN 泛洪攻击。或者，您可以选择启用 TCP 拦截统计信息并监控策略的结果。以下程序介绍端到端流程。

### 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 Cisco Secure Firewall Threat Defense型号中 CPU 内核数量，由于每个内核管理连接的方式不同，最大并发和正在建立的连接可能超出配置的数量。在最糟糕的情况下，此设备最多允许 n-1 个额外连接和初期连接，其中 n 是内核数量。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。要确定型号的内核数量，请在设备 CLI 中输入 **show cpu core** 命令。

过程

**步骤 1** 创建定义流量类的扩展 ACL，该列表是要保护的服务器列表。

例如，要定义流量类以使用 IP 地址 10.1.1.5 和 10.1.1.6 保护 Web 服务器，请执行以下操作：

a) 选择**对象 (Object)** > **对象管理 (Object Management)**。
b) 从目录中选择**访问列表** > **扩展**。
c) 点击**添加扩展访问列表**。
d) 为对象输入一个**名称**，例如，protected-servers。
e) 点击**添加**以添加规则。
f) 保持**允许**操作。
g) 将**源 (Source)** 列表留空，在**目标 (Destination)** 列表下方输入 10.1.1.5，然后点击**添加 (Add)**。
h) 此外，在**目标 (Destination)** 列表下方输入 10.1.1.6，然后点击**添加 (Add)**。
i) 点击**端口 (Port)**，从可用端口列表中选择 **FMC_CONNECTION**，然后点击**添加到目标 (Add to Destination)**。如果您的服务器还支持 HTTPS 连接，还需添加此端口。
j) 在“扩展访问列表条目”对话框中点击**添加**，以将规则添加到 ACL。
k) 点击“扩展访问列表对象”对话框中的**保存**，以保存 ACL 对象。

**步骤 2** 配置用于设置初期连接限制的服务策略规则。

例如，要将总并发初期连接限制设置为 1000 个并将每客户端的连接限制设置为 50 个，请执行以下操作：

a) 选择**策略** > **访问控制标题** > **访问控制**，然后编辑分配给需要此服务的设备的策略。
b) 点击数据包流行末尾的**更多 (More)** 下拉箭头中的**高级设置 (Advanced Settings)**，然后点击**威胁防御服务策略 (Threat Defense Service Policy)** 的 **编辑** ()。
c) 点击**添加规则**。
d) 选择**全局应用 (Apply Globally)** > **下一步 (Next)**。
e) 选择为此规则创建的扩展 ACL 对象，然后点击**下一步 (Next)**。
f) 为**连接** > **最大初期连接数**输入 1000。
g) 为**每个客户端的连接数** > **最大初期连接数**输入 50。
h) （可选。）根据需要调整其他连接选项。
i) 点击**完成**以添加规则。如有必要，将规则拖放到服务策略中的所需位置。
j) 点击**确定 (OK)** 以保存对服务策略所做的更改。
k) 点击**高级**中的**保存**，以保存对访问控制策略所做的更改。

**步骤 3** （可选。）配置 TCP 拦截统计信息的速率。

TCP 拦截使用以下选项来确定收集统计信息的速率。所有选项都具有默认值，因此如果这些速率符合您的需求，您可以跳过此步骤。

- 速率间隔 - 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。在此间隔期间，系统会进行 30 次攻击数量采样。

- 突发速率 - 系统日志消息生成的阈值，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，设备将生成系统日志消息 733104。
- 平均速率 - 系统日志消息生成的平均速率阈值，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，设备将生成系统日志消息 733105。

如果要调整这些选项，请执行以下操作：

a) 选择**对象 (Object)** > **对象管理 (Object Management)**。
b) 选择 **FlexConfig** > **文本对象**。
c) 点击 threat_defense_statistics 系统定义对象的 **编辑** ()。
d) 虽然您可以直接更改值，但建议的方法是打开**覆盖**部分，然后点击**添加**以创建设备覆盖。
e) 选择要为其分配服务策略的设备（通过访问控制策略分配），然后点击**添加**以将其移动到所选列表中。
f) 点击**覆盖 (Override)**。
g) 此对象必须有 3 个条目，因此请根据需要点击**计数 (Count)**，直至获得 3 个条目。
h) 按照 1-3 的顺序输入所需的值作为速率间隔、突发速率和平均速率。请参阅对象说明以验证您是否按正确的顺序输入值。
i) 在“对象覆盖”对话框中点击**添加 (Add)**。
j) 在“编辑文本对象”对话框中点击**保存**。

**步骤 4** 启用 TCP 拦截统计信息。

您必须配置 FlexConfig 策略以启用 TCP 拦截统计信息。

a) 选择**设备** > **FlexConfig**。
b) 如果已为设备分配策略，请对其进行编辑。否则，请创建新策略并将其分配给受影响的设备。
c) 选择**可用 FlexConfig** 列表中的 **Threat_Detection_Configure** 对象，然后点击 **>>**。此对象将添加到**所选附加 Flexconfig** 列表中。
d) 点击**保存**。
e) （可选。）您可以通过点击**预览配置**并选择其中一个设备来验证是否具有正确的设置。

系统会生成将在下次部署期间写入设备的 CLI 命令。这些命令将包括服务策略所需的命令以及威胁检测统计信息所需的命令。滚动到预览的底部以查看附加的CLI。如果使用默认值，TCP拦截统计信息命令应如下所示（为清晰起见已添加换行符）：

```
###Flex-config Appended CLI ###

threat-detection statistics tcp-intercept rate-interval 30
       burst-rate 400 average-rate 200
```

**步骤 5** 现在您可以将更改部署到受影响的设备。

**步骤 6** 使用以下命令从设备 CLI 监控 TCP 拦截统计信息：

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**] - 查看遭受攻击的前 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** 关键字显示历史采样数据。在速率间隔内，系统会进行 30 次攻击次数采样，因此，在默认的 30 分钟内，每 60 秒收集一次统计信息。

注释
您可以使用 **shun** 命令阻止攻击主机 IP 地址。要删除阻止列表，请使用 **no shun** 命令。

- **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)
```

# 使 威胁防御 设备显示在跟踪路由上

默认情况下，威胁防御不会在跟踪路由上显示为跃点。要使其显示，您需要递减通过设备的数据包上的生存时间，并增加对 ICMP 不可达消息的速率限制。要实现此目的，必须配置服务策略规则并调整 ICMP 平台设置策略。

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（例如 OSPF hello 数据包）发送时 TTL = 1，因此减去生存时间可能会导致意外后果。定义流量类时，请注意这些事项。

过程

**步骤 1** 创建扩展 ACL，以定义要为其启用跟踪路由报告的流量类。

例如，要为所有地址（但不包括 OSPF 流量）定义流量类，请执行以下操作：

a) 选择**对象 (Object)** > **对象管理 (Object Management)**。
b) 从目录中选择**访问列表** > **扩展**。
c) 点击**添加扩展访问列表**。
d) 为对象输入一个**名称**，例如，traceroute-enabled。
e) 点击**添加**以添加规则，从而排除 OSPF。
f) 将操作更改为**阻止 (Block)**，点击**端口 (Port)** 选项卡，选择 **OSPFIGP (89)** 作为**目标端口 (Destination Ports)** 列表下方的协议，然后点击**添加 (Add)** 将此协议添加到所选列表。
g) 在“扩展访问列表条目”对话框中点击**添加**，以将 OSPF 规则添加到 ACL。
h) 点击**添加**以添加规则，从而包含所有其他连接。
i) 保持**允许**操作，并将“源”和“目标”列表留空。

j) 在“扩展访问列表条目”对话框中点击**添加**，以将规则添加到 ACL。

确保 OSPF 拒绝规则优先于“允许所有”规则。如有必要，拖放以移动规则。

k) 点击“扩展访问列表对象”对话框中的**保存**，以保存 ACL 对象。

**步骤 2** 配置用于递减生存时间值的服务策略规则。

例如，要全局递减生存时间，请执行以下操作：

a) 选择**策略** > **访问控制标题** > **访问控制**，然后编辑分配给需要此服务的设备的策略。
b) 点击数据包流行末尾的**更多 (More)** 下拉箭头中的**高级设置 (Advanced Settings)**，然后点击**威胁防御服务策略 (Threat Defense Service Policy)** 的 **编辑** (✎)。
c) 点击**添加规则**。
d) 选择**全局应用 (Apply Globally)**，然后点击**下一步 (Next)**。
e) 选择为此规则创建的扩展 ACL 对象，然后点击**下一步 (Next)**。
f) 选择**启用递减 TTL**。
g) （可选。）根据需要调整其他连接选项。
h) 点击**完成**以添加规则。如有必要，将规则拖放到服务策略中的所需位置。
i) 点击**确定 (OK)** 以保存对服务策略所做的更改。
j) 点击**高级**中的**保存**，以保存对访问控制策略所做的更改。

现在您可以将更改部署到受影响的设备。

**步骤 3** 增加 ICMP 不可达消息的速度限制。

a) 选择**设备** > **平台设置**。
b) 如果已为设备分配策略，请对其进行编辑。否则，请创建新的威胁防御平台设置策略并将其分配给受影响的设备。
c) 从目录中选择 **ICMP**。
d) 增加**速率限制**，例如，增加至 50。您可能还希望将 **突发大小** 增加到 10，以确保在速率限制内生成足够的响应。

您可以将 ICMP 规则表留空，它与此任务无关。

e) 点击**保存**。

**步骤 4** 现在您可以将更改部署到受影响的设备。

# 监控服务策略

您可以使用设备 CLI 监控服务策略相关信息。以下是一些有用的命令。

- **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 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。在速率间隔内，系统会进行 30 次攻击次数采样，因此，在默认的 30 分钟内，每 60 秒收集一次统计信息。

# 威胁防御服务策略的历史记录

| 功能 | 防火墙管理中心最低版本 | 最低版本 | 说明 |
|---|---|---|---|
| 威胁防御服务策略。 | 6.3 | 任意 | 现在您可以将威胁防御服务策略配置为访问控制策略高级选项的一部分。您可以使用威胁防御服务策略将服务应用于特定流量类。支持的功能包括 TCP 状态绕行、随机生成 TCP 序列号、递减数据包的生存时间 (TTL) 值、失效连接检测、设置每个流量类和每个客户端的最大连接数和初期连接数限制以及初期、半闭和空闲连接的超时时间。<br>新屏幕： **策略** > **访问控制** > **访问控制**、 **高级** 选项卡， **威胁防御服务策略**。<br>支持的平台： Cisco Secure Firewall Threat Defense |
| 集群中的“死连接检测”(DCD) 支持的发起方和响应方信息。 | 6.5 | 任意 | 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。<br>新增/修改的命令：**show conn**（仅输出）<br>支持的平台： Cisco Secure Firewall Threat Defense |

| 功能 | 防火墙管理中心最低版本 | 最低版本 | 说明 |
| --- | --- | --- | --- |
| 配置初期连接的最大分段大小 (MSS)。 | 7.1 | 任意 | 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。<br>新增或更改的屏幕：添加/编辑服务策略向导中的**连接设置**。 |

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。