ASA 8.2.X TCP状态旁路功能配置示例

目录

简介

本文档介绍如何配置TCP状态绕行功能。此功能允许通过单独的Cisco ASA 5500系列自适应安全设备的出站和入站流量。

先决条件

许可证要求

Cisco ASA 5500系列自适应安全设备应至少具有基本许可证。

使用的组件

本文档中的信息基于8.2(1)及更高版本的思科自适应安全设备(ASA)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

关于文件规则的信息，请参见Cisco技术提示规则。

TCP状态绕行

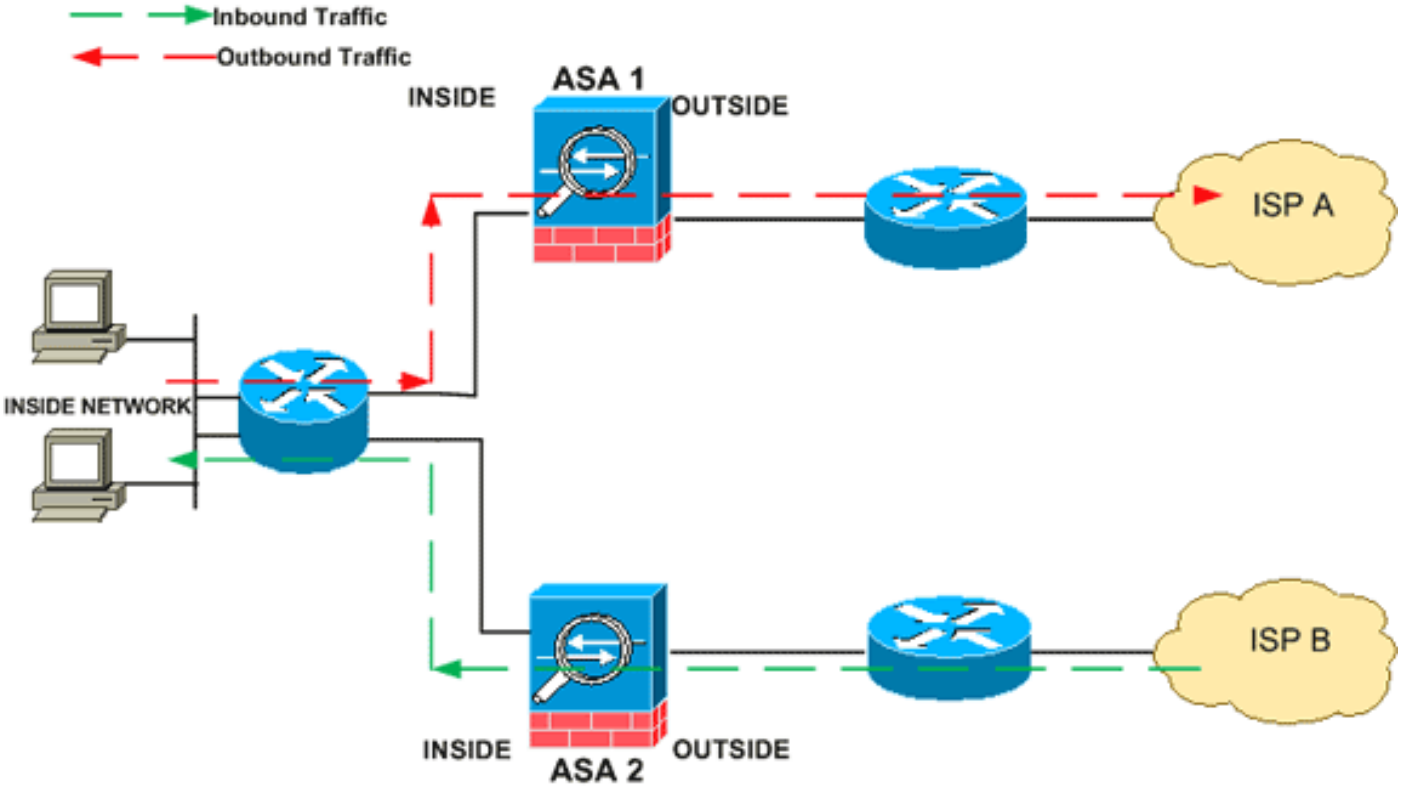
默认情况下，通过思科自适应安全设备(ASA)的所有流量都使用自适应安全算法进行检查，并根据安全策略允许或丢弃。为了最大限度地提高防火墙性能，ASA检查每个数据包的状态（例如，这是新连接还是已建立连接？），并将其分配给会话管理路径（新连接SYN数据包）、快速路径（已建立连接）或控制平面路径（高级检查）。

匹配快速路径中现有连接的TCP数据包可以通过自适应安全设备，而无需重新检查安全策略的每个方面。此功能可最大限度地提高性能。但是，用于在快速路径（使用SYN数据包）中建立会话的方法和在快速路径（如TCP序列号）中发生的检查可能会阻碍非对称路由解决方案：连接的出站和入站流量必须通过同一ASA。

例如，新连接将转到*ASA 1*。SYN数据包将通过会话管理路径，并且连接的条目将添加到快速路径表中。如果此连接的后续数据包通过*ASA 1*，则数据包将与快速路径中的条目匹配并通过。如果后续数据包转到*ASA 2*，且没有SYN数据包通过会话管理路径，则快速路径中没有用于连接的条目，并且数据包将被丢弃。

如果在上游路由器上配置了非对称路由，并且流量在两个ASA之间交替，则可以为特定流量配置TCP状态绕行。TCP状态绕行会改变在快速路径中建立会话的方式，并禁用快速路径检查。此功能处理TCP流量的方式与处理UDP连接的方式相同：当与指定网络匹配的非SYN数据包进入ASA，且没有快速路径条目时，该数据包将通过会话管理路径在快速路径中建立连接。进入快速路径后，流量会绕过快速路径检查。

此映像提供非对称路由示例，其中出站流量通过与入站流量不同的ASA:



注意：Cisco ASA 5500系列自适应安全设备默认禁用TCP状态旁路功能。

支持信息

本节提供TCP状态绕行功能的支持信息。

- 情景模式 — 在单情景和多情景模式中受支持。
- 防火墙模式 — 在路由和透明模式下受支持。

- 故障转移 — 支持故障转移。

使用TCP状态绕行时不支持以下功能：

- 应用检测 — 应用检测要求入站和出站流量都通过同一ASA，因此TCP状态绕行不支持应用检测。
- AAA身份验证会话 — 当用户使用一个ASA进行身份验证时，通过另一个ASA返回的流量将被拒绝，因为用户未使用该ASA进行身份验证。
- TCP拦截，最大初期连接限制，TCP序列号随机化 — ASA不跟踪连接状态，因此不应用这些功能。
- TCP规范化 — TCP规范器已禁用。
- SSM和SSC功能 — 不能使用TCP状态旁路和SSM或SSC上运行的任何应用，如IPS或CSC。

NAT准则:由于转换会话是为每个ASA单独建立的，因此请务*必*在两个ASA上为TCP状态绕行流量配置静态NAT;如果使用动态NAT，则为ASA 1上的会话选择*的地*址将与为ASA 2上的会话选择的*地址不同*。

配置

本节介绍如何在Cisco ASA 5500系列自适应安全设备(ASA)上配置TCP状态旁路功能。

TCP状态旁路功能配置

要在Cisco ASA 5500系列自适应安全设备上配置TCP状态旁路功能，请完成以下步骤：

1. 使用class-map class_map_name命令可创建类*映射*。类映射用于标识要禁用状态防火墙检测的流量。本示例中使用的类映射是*tcp_bypass*。
   ```
   ASA(config)#class-map tcp_bypass
   ```

2. 使用match参数命令以在类映射中指定相关流量。使用模块化策略框架时，请在类映射配置模式下使用**match access-list**命令，以便使用访问列表识别要应用操作的流量。以下是此配置的示例：
   ```
   ASA(config)#class-map tcp_bypass
   ASA(config-cmap)#match access-list tcp_bypass
   ```

   *tcp_bypass*是本示例中使用的访问列表的名称。有关指定相关流量的详细信息，请参阅识别流量（第3/4层类映射）。
3. 使用policy-map name命令可添加策略映射或编辑策略映射（已存在），该策略映射设置对已指定的类映射流量执行的操作。在使用模块化策略框架时，请在全局配置模式下使用**policy-map**命令（不带type关键字），以便将操作分配给您使用第3/4层类映射（class-map或class-map type management命令）标识的流量。 在本示例中，策略映射为*tcp_bypass_policy*:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ```

4. 在策略映射配置模式下使用class命令，以将已创建的类映射(*tcp_bypass*)分配到策略映射(*tcp_bypass_policy*)，在该策略映射中可以为类映射流量分配操作。在本例中，类映射为*tcp_bypass*:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ASA(config-pmap)#class tcp_bypass
   ```

5. 在类配置模式下使用set connection advanced-options tcp-state-bypass命令以启用TCP状态旁路功能。此命令在8.2(1)版中引入。 可从策略映射配置模式访问类配置模式，如下例所示：

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

6. 使用service-policy policymap_name [global | interface *intf*] 命令，以便在所有接口或目标接口上全局激活策略映射。要禁用服务策略，请使用此命令的no形式。使用service-policy命令在接口上启用一组策略。global将策略映射应用于所有接口，而interface将策略应用于一个接口。仅允许有一个全局策略。您可以通过对接口应用服务策略以覆盖此接口的全局策略。您只能将一个策略映射应用到每个接口。
   ```
   ASA(config-pmap-c)#service-policy tcp_bypass_policy outside
   ```

以下是TCP状态绕行的示例配置：

```
!--- Configure the access list to specify the TCP traffic !--- that needs to by-pass inspection
to improve the performance. ASA(config)#access-list tcp_bypass extended permit tcp 10.1.1.0
255.255.255.224 any

!--- Configure the class map and specify the match parameter for the !--- class map to match the
interesting traffic. ASA(config)#class-map tcp_bypass
ASA(config-cmap)#description "TCP traffic that bypasses stateful firewall"
ASA(config-cmap)#match access-list tcp_bypass

!--- Configure the policy map and specify the class map !--- inside this policy map for the
class map. ASA(config-cmap)#policy-map tcp_bypass_policy
ASA(config-pmap)#class tcp_bypass
!--- Use the set connection advanced-options tcp-state-bypass !--- command in order to enable
TCP state bypass feature.

ASA(config-pmap-c)#set connection advanced-options tcp-state-bypass
!--- Use the service-policy policymap_name [ global | interface intf ] !--- command in global
configuration mode in order to activate a policy map !--- globally on all interfaces or on a
targeted interface.

ASA(config-pmap-c)#service-policy tcp_bypass_policy outside

ASA(config-pmap-c)#static (inside,outside) 192.168.1.224 10.1.1.0 netmask
255.255.255.224
```

验证

show conn命令显示活动TCP和UDP连接的数量，并提供各种类型连接的相关信息。要显示指定连接类型的连接状态，请在特权EXEC模式下使用show conn命令。此命令支持 IPv4 和 IPv6 地址。使用TCP状态旁路的连接的**输出显示**包括标记**b**。

故障排除

错误消息

ASA在启用TCP状态绕行功能后显示此错误消息。

```
%PIX|ASA-4-313004:Denied ICMP type=icmp_type, from source_address oninterface
interface_name to dest_address:no matching session
```

安全设备丢弃了ICMP数据包，因为状态ICMP功能添加的安全检查通常是ICMP回应应答，没有在安全设备上传递有效回应请求，或与安全设备中已建立的任何TCP、UDP或ICMP会话无关的ICMP错误消息。

即使TCP状态旁路已启用，ASA也会显示此日志，因为无法禁用此功能（即，检查连接表中第3类的ICMP返回条目）。但TCP状态绕行功能工作正常。

使用此命令可防止出现以下消息：

```
hostname(config)#no logging message 313004
```

相关信息

- Cisco ASA 5500 系列自适应安全设备
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems