ASA 8.2.X TCP状态旁路功能配置示例

目录

简介

本文描述如何配置TCP状态旁路功能。此功能允许出站，并且入站流经分开的Cisco ASA 5500系列自适应安全设备。

先决条件

许可证要求

Cisco ASA 5500系列自适应安全设备应该有至少基础许可证。

使用的组件

本文档中的信息根据Cisco可适应安全工具(ASA)有版本8.2(1)和以上的。

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状态旁路

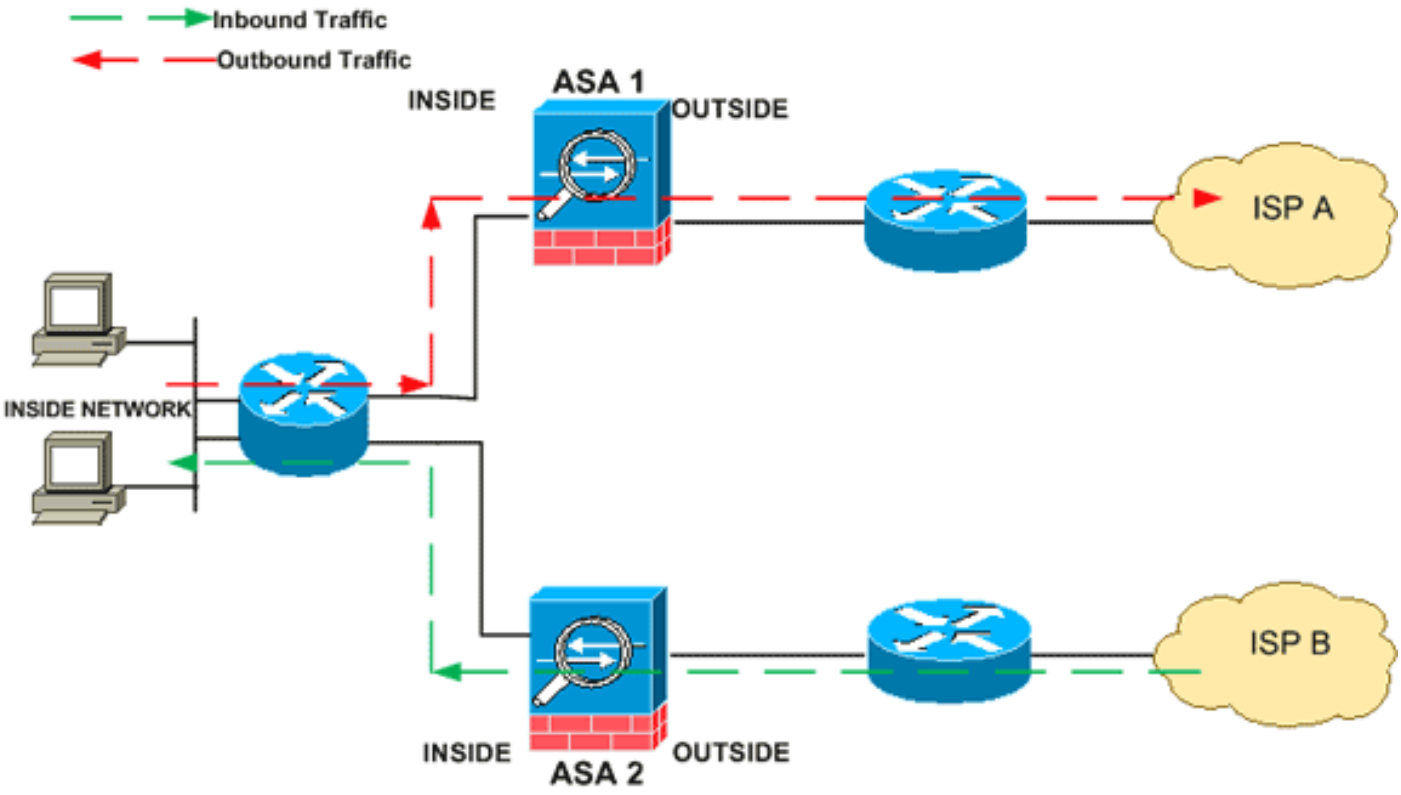
默认情况下，穿过思科可适应安全工具的所有流量(ASA)被检查使用自适应安全算法和通过允许或丢弃基于安全策略。为了最大化防火墙性能， ASA检查每数据包的状态(例如，是这新连接或建立的连接？)并且分配它到会话管理路径(新连接SYN数据包)，快速路径(建立的连接)，或者控制层面路径(先进的检查)。

在快速路径匹配现有连接的TCP信息包能穿过可适应安全工具，无需复校安全策略的每个方面。此功能最大化性能。然而，使用的方法建立会话在使用SYN数据包)的快速路径(和在快速路径发生的检查(例如TCP序列号)能阻碍不对称的路由解决方案：连接的出站和入站流必须穿过同样ASA。

例如，新连接去*ASA 1*。SYN数据包穿过会话管理路径，并且连接的一个条目被添加到快速路径表。如果后续信息包此连接通过*ASA 1*，数据包在快速路径将匹配条目和通过通过。如果后续信息包去*ASA 2*，其中没有通过会话管理路径的SYN数据包，则没有条目在连接的快速路径，并且数据包丢弃。

如果有在上游路由器配置的不对称路由，并且流量交替在两ASA之间，则您能配置特定的流量的TCP状态旁路。TCP状态旁路改变会话在快速路径建立的方式并且禁用快速路径检查。当对待UDP连接，此功能对待TCP数据流：当匹配指定的网络的非SYN数据包输入ASA时，并且没有快速路径条目，然后数据包通过会话管理路径在快速路径建立连接。一旦在快速路径，流量绕过快速路径检查。

此镜像提供不对称路由示例，出站流量比入站数据流通过不同的ASA ：



注意： 默认情况下TCP状态旁路功能在Cisco ASA 5500系列自适应安全设备禁用。

支持信息

此部分为TCP状态旁路功能提供支持信息。

- 上下文模式—支持在单个和多个上下文模式。
- 防火墙模式—支持在已路由和透明模式。
- 故障切换—支持故障切换。

这些功能，当您使用TCP状态旁路时，不支持：

- 应用检查—应用检查要求两穿过的入站和出站通流量同样ASA，因此应用检查不用TCP状态旁路支持。
- AAA认证的会话—当用户验证与一个ASA，返回通过另一个ASA的流量将拒绝，因为用户没有验证与该ASA。
- TCP拦截，最大初期连接限制， TCP序列号随机化— ASA不记录连接的状态，因此这些功能没有应用。
- TCP标准化— TCP规整器禁用。
- SSM和SSC功能—您不能使用TCP状态旁路和任何应用程序运行在SSM或SSC，例如IPS或CSC。

NAT指南：由于转换会话为每个ASA分开建立，请务必配置静态NAT在TCP状态旁路流量的两ASA;如果使用动态NAT，为*ASA的1*会话选择的地址与为*ASA的2*.会话选择的地址将有所不同。

配置

此部分描述如何配置在Cisco ASA 5500系列可适应安全工具(ASA)的TCP状态旁路功能。

TCP状态旁路功能配置

完成这些步骤为了配置TCP状态在Cisco ASA 5500系列可适应安全工具的旁路功能：

1. 请使用**类映射class_map_name**命令为了创建*类映射*。类映射用于识别您要禁用状态防火墙检查的流量。用于此示例的类映射是*tcp_bypass*。`ASA(config)#class-map tcp_bypass`
2. 请使用**匹配参数**命令为了指定在类映射的关注数据流。当曾经模块化政策架构时，请使用**匹配访问列表命令**在等级映射配置模式为了使用访问列表识别您要运用操作的流量。这是此配置示例：`ASA(config)#class-map tcp_bypass ASA(config-cmap)#match access-list tcp_bypass` *tcp_bypass*是用于此示例access-list的名称。参考识别流量(3/4层类映射)关于指定关注数据流的更多信息。
3. 请使用**name命令的策略映射**为了添加策略映射或编辑已经存在)该的策略映射(设置操作采取与已经指定的类映射流量。当使用模块化政策架构时，请使用**policy-map命令**(没有类型关键字)在全局配置模式为了分配操作到您识别与3/4层类映射的流量(类映射或类映射类型管理命令)。在本例中，策略映射是*tcp_bypass_policy* ：`ASA(config-cmap)#policy-map tcp_bypass_policy`
4. 请使用**class命令**在policy-map配置模式为了分配(*tcp_bypass*)已经创建的类映射到策略映射(*tcp_bypass_policy*)您能分配操作到类映射流量的地方。在本例中，类映射是*tcp_bypass* ：`ASA(config-cmap)#policy-map tcp_bypass_policy ASA(config-pmap)#class tcp_bypass`
5. 请使用**集合connection advanced-options TCP状态旁路**in命令等级配置模式为了启用TCP状态旁路功能。此命令在版本8.2(1)介绍。等级配置模式从policy-map配置模式是可访问如此示例所显示：`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. 请使用**服务策略policymap_name [全局|建立接口*intf*]** in命令全局配置模式为了激活一个策略映射全局在所有接口或在一个目标接口。为了禁用服务策略，请使用此命令**no表示**。请使用**service-policy命令**启用一套在interface.global的策略应用策略映射对所有接口，并且**接口**运用策略对一个接口。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。您只能应用一个策略映射到每个接口。`ASA(config-pmap-c)#service-policy tcp_bypass_policy outside`

这是TCP状态旁路的一配置示例：

```
!--- 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命令显示激活TCP和UDP连接数量并且提供关于多种类型的连接的信息。为了显示指定连接类型的连接状态，请使用show conn命令在特权EXEC模式。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志**b。**

故障排除

错误消息

在TCP状态旁路功能启用以后， ASA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
```

ICMP数据包由安全工具丢弃由于通常是ICMP echo应答没有一个有效ECHO请求已经通过在安全工具间或ICMP错误信息没涉及与所有TCP，UDP有状态的ICMP功能，或者ICMP会话添加的安全性检查已经建立在安全工具。

ASA显示此日志，即使TCP状态旁路启用，因为禁用此功能(即检查ICMP返回条目Type3在连接表里)不是可能的。但是TCP状态旁路功能正确地运作。

请使用此命令为了防止这些消息出现：

```
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