配置在5500系列的ASA的TCP状态旁路功能

目录

简介

本文描述如何配置TCP状态旁路功能，允许出站和入站数据流流经分开的Cisco ASA 5500系列自适应安全设备(ASA)。

先决条件

要求

思科ASA必须有安装的至少基础许可证，在您能继续进行在本文描述的配置前。

使用的组件

运行软件版本9.x的本文档中的信息根据5500系列Cisco的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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

此部分提供TCP状态旁路功能和相关支持信息的概述。

TCP状态旁路功能概述

默认情况下，穿过ASA的所有流量通过自适应安全算法被检查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，证实它是否是新连接或建立的连接)并且分配它到任一会话管理路径(新连接同步(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)。

在快速路径匹配当前连接的TCP信息包能穿过ASA，不用安全策略的每个方面复校。此功能最大化性能。然而，使用为了在快速路径(建立会话使用SYN数据包)的方法，并且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。如果在此连接的后续信息包通过*ASA 1*，数据包在快速路径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状态旁路功能。TCP状态旁路功能改变方式会话在快速路径建立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：当匹配指定的网络时的非SYN数据包输入ASA和那里是没有快速路径条目，然后数据包通过会话管理路径为了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5500系列Cisco的ASA禁用。另外，如果没有适当地实现， TCP状态旁路配置能导致连接大量。

支持信息

此部分描述TCP状态旁路功能的支持信息。

- **上下文模式**âÂ TCP状态旁路功能单个和多个上下文模式支持 Â 。
- **防火墙模式**âÂ TCP状态旁路功能已路由和透明模式支持 Â 。
- **故障切换**âÂ Â TCP状态旁路功能支持故障切换。

这些功能，当您使用TCP状态旁路功能时，不支持：

- **应用检查**âÂ Â 应用检查要求入站和出站通流量通过同样ASA的两个，因此应用检查不支持与TCP状态旁路功能。
- **验证、授权和统计(AAA)认证的会话**âÂ Â ，当用户验证与一个ASA，回归通过另一个ASA拒绝的流量，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**âÂ Â ASA不连接的状态的跟踪，因此这些功能没有应用。
- **TCP标准化**âÂ Â TCP规整器禁用。
- **安全服务模块(SSM)和安全服务卡德(SSC)功能**âÂ Â 您不能以在SSM或SSC运行，例如IPS或内容安全的任何应用程序使用TCP状态旁路功能(CSC)。

  注意：由于转换会话为每个ASA分开建立，请保证您配置静态网络地址转换(NAT)在两个TCP状态旁路流量的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ASA的TCP状态旁路功能5500系列在两个不同的方案。

注意：请使用命令查找工具(仅限注册用户)为了得到关于在此部分使用的命令的更多信息。

场景 1

这是使用第一个方案的拓扑：

注意：您必须运用在对两个的此部分描述ASA的配置。

完成这些步骤为了配置TCP状态旁路功能：

1. 输入**类映射class_map_name**命令为了创建*类映射*。类映射用于为了识别您要禁用状态防火墙检查的流量。**注意**：在本例中使用的类映射是**tcp_bypass**。`ASA(config)#class-map tcp_bypass`
2. 输入**匹配参数**命令为了指定流量在类映射内的利益。当您使用模块化政策架构时，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您要运用操作流量的识别。这是此配置示例：

   ```
   ASA(config)#class-map tcp_bypass
   ASA(config-cmap)#match access-list tcp_bypass
   ```

   注意：**tcp_bypass**是用于此示例的名称access-list。*参考Cisco ASA 5500系列配置指南的*识别的流量(3/4层类映射)*使用CLI*，部分， *8.2*关于如何指定流量的更多信息利益。
3. 输入**name命令的策略映射**为了添加策略映射或编辑已经存在)分配操作关于指定类地图流量被采取的策略映射(。当您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. 输入**class命令**在*policy-map配置*模式为了分配已创建类映射(*tcp_bypass*)到策略映射(*tcp_bypass_policy*)，以便您能分配操作到类映射流量。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. 输入**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. 输入**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**。输入**service-policy命令**为了启用一套在接口的策略。**全局**关键字应用策略映射对所有接口，并且**接口**关键字只应用策略映射对一个接口。仅允许有一个全局策略。为了改写在接口的全局策略，您能运用服务策略到该接口。您只能应用一个策略映射到每个接口。示例如下：

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

这是TCP状态旁路功能的一配置示例在*ASA1* ：

```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.

ASA1(config)#access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.0
172.16.1.0 255.255.255.0

!--- Configure the class map and specify the match parameter for the
!--- class map to match the interesting traffic.

ASA1(config)#class-map tcp_bypass
ASA1(config-cmap)#description "TCP traffic that bypasses stateful firewall"
ASA1(config-cmap)#match access-list tcp_bypass

!--- Configure the policy map and specify the class map
!--- inside this policy map for the class map.

ASA1(config-cmap)#policy-map tcp_bypass_policy
ASA1(config-pmap)#class tcp_bypass

!--- Use the set connection advanced-options tcp-state-bypass
!--- command in order to enable TCP state bypass feature.

ASA1(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.

ASA1(config-pmap-c)#service-policy tcp_bypass_policy outside

!--- NAT configuration

ASA1(config)#object network obj-10.1.1.0
ASA1(config-network-object)#subnet 10.1.1.0 255.255.255.0
ASA1(config-network-object)#nat(inside,outside) static 192.168.1.0
```

这是TCP状态旁路功能的一配置示例在*ASA2* ：

```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.

ASA2(config)#access-list tcp_bypass extended permit tcp 172.16.1.0 255.255.255.0
10.1.1.0 255.255.255.0

!--- Configure the class map and specify the match parameter for the
!--- class map to match the interesting traffic.

ASA2(config)#class-map tcp_bypass
ASA2(config-cmap)#description "TCP traffic that bypasses stateful firewall"
ASA2(config-cmap)#match access-list tcp_bypass

!--- Configure the policy map and specify the class map
!--- inside this policy map for the class map.

ASA2(config-cmap)#policy-map tcp_bypass_policy
ASA2(config-pmap)#class tcp_bypass

!--- Use the set connection advanced-options tcp-state-bypass
!--- command in order to enable TCP state bypass feature.

ASA2(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.

ASA2(config-pmap-c)#service-policy tcp_bypass_policy outside

!--- NAT configuration

ASA2(config)#object network obj-10.1.1.0
ASA2(config-network-object)#subnet 10.1.1.0 255.255.255.0
ASA1(config-network-object)#nat(inside,outside) static 192.168.1.0
```

场景 2

此部分描述如何配置在ASA的TCP状态旁路功能使用不对称路由，流量输入并且离开从同样接口的方案的(u*启用*)的ASA。

这是在此方案使用的拓扑：

完成这些步骤为了配置TCP状态旁路功能：

1. 创建*access-list*为了匹配应该绕过TCP检查的流量：
   ```
   ASA(config)#access-list tcp_bypass extended permit tcp 192.168.2.0 255.255.255.0
   192.168.1.0 255.255.255.0
   ```
2. 输入**类映射**class_map_name命令为了创建*类映射*。类映射用于为了识别您要禁用状态防火墙检查的流量。**注意**：在本例中使用的类映射是tcp_bypass。`ASA(config)#class-map tcp_bypass`
3. 输入**匹配参数**命令为了指定兴趣流量在类映射上。当您使用模块化政策架构时，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您要运用操作流量的识别。这是此配置示例：
   ```
   ASA(config)#class-map tcp_bypass
   ASA(config-cmap)#match access-list tcp_bypass
   ```
   注意：tcp_bypass是用于此示例的名称access-list。*参考*识别*Cisco ASA 5500系列配置指南的*流量(3/4层类映射)部分*使用CLI， 8.2*关于如何

指定流量的更多信息利益。

4. 输入**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(设置操作关于指定类地图流量被采取。当您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
   ```
5. 输入**class命令**在*policy-map配置*模式为了分配已创建类映射(*tcp_bypass*)到策略映射(*tcp_bypass_policy*)，以便您能分配操作到类映射流量。在本例中，类映射是**tcp_bypass** ：
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ASA(config-pmap)#class tcp_bypass
   ```
6. 输入**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
   ```
7. 输入**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**。输入**service-policy命令**为了启用一套在接口的策略。**全局**关键字应用策略映射对所有接口，并且**接口**关键字只运用策略对一个接口。仅允许有一个全局策略。为了改写在接口的全局策略，您能运用服务策略到该接口。您只能应用一个策略映射到每个接口。示例如下：
   ```
   ASA(config-pmap-c)#service-policy tcp_bypass_policy inside
   ```
8. 允许流量的同一个安全等级在ASA ：
   ```
   ASA(config)#same-security-traffic permit intra-interface
   ```

这是TCP状态旁路功能的一配置示例在ASA ：

```
!--- Configure the access list to specify the TCP traffic
!--- that needs to bypass inspection to improve the performance.

ASA(config)#access-list tcp_bypass extended permit tcp 192.168.2.0 255.255.255.0
192.168.1.0 255.255.255.0

!--- 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 inside

!--- Permit same security level traffic on the ASA to support U-turning
```

```
ASA(config)#same-security-traffic permit intra-interface
```

验证

输入show conn命令为了查看激活TCP编号和UDP连接和信息关于多种类型的连接。为了显示指定连接类型的连接状态，请输入show conn命令在*特权EXEC模式*。

> **注意**：此命令支持 IPv4 和 IPv6 地址。为连接显示使用TCP状态旁路功能的输出包括标志**b**。

下面是示例输出：

```
ASA(config)show conn
1 in use, 3 most used
TCP tcp 10.1.1.1:49525 tcp 172.16.1.1:21, idle 0:01:10, bytes 230, flags b
```

故障排除

没有此功能的特定故障排除信息。参考这些文档一般连接故障排除信息：

- 有CLI和ASDM配置示例的ASA数据包捕获
- ASA 8.2 ：数据包流经思科ASA防火墙

> **注意**：TCP状态旁路连接没有复制对在故障切换对的备用装置。

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
```

互联网控制消息协议(ICMP)数据包由ASA丢弃由于由有状态的ICMP功能添加的安全性检查。这些通常是与任何TCP，UDP没有涉及的ICMP echo应答没有在ASA间已经通过的一个有效*ECHO请求*或者ICMP错误信息，或者在ASA当前建立的ICMP会话。

ASA显示此日志，即使TCP状态旁路功能启用，因为此功能的不合格(即在连接表里检查ICMP*返回*条目Type3)不是可能的。然而， TCP状态旁路功能正确地运作。

输入此命令为了防止这些消息外观：

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

相关信息

- Cisco 自适应安全设备管理器
- 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