ASA VPN负载均衡导向器选举过程

目录

简介

本文档介绍Cisco 5500-X系列自适应安全设备(ASA)在VPN负载均衡场景中的指挥交换机选举过程。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于运行软件版本9.2的Cisco ASA 5500-X。

> **注意**：本文档也适用于所有软件版本，因为该功能是第一次在7.0(1)版中引入的。

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。

背景信息

VPN负载均衡是一种机制，用于在虚拟集群中的设备之间公平分配网络流量。负载均衡基于简单分配；它不考虑吞吐量利用率或其他因素。负载均衡集群由两台或多台设备、一台指挥交换机和一台或多台辅助设备组成，这些设备无需进行相同配置。

负载均衡算法

以下是负载均衡算法的概述：

- 指挥交换机设备按内部IP地址的升序维护辅助集群成员的排序列表。
- 负载计算为每个辅助集群成员提供的整数百分比（活动/最大会话数）。
- 指挥交换机设备将IPSec/安全套接字层(SSL)VPN隧道重定向到负载最低的设备，直到其比其他设备高1%。
- 仅当所有辅助集群成员都比指挥交换机设备高1%时，指挥交换机设备才会重定向到自身。

以下是一个包含一个指挥交换机和两个辅助集群成员的示例：

- 所有节点以零百分比负载开始，所有百分比均四舍五入到最接近的半%。
- 如果所有成员的负载都比指挥交换机设备高1%，则指挥交换机设备将进行连接。
- 如果指挥交换机设备未进行连接，则会话由当前负载百分比最小的备份设备进行。
- 如果所有成员的负载百分比相同，则会话数最少的备份设备会使用会话。
- 如果所有成员具有相同的负载百分比和相同的会话数，则具有最少IP地址的备份设备将会话。

董事选举过程

在群集外部网络上执行VPN负载平衡指挥交换机选举过程。在外部网络上交换的数据有两种类型：

- 交换用于指挥交换机发现的集群IP地址的地址解析协议(ARP)数据包。为发现指挥交换机而为集群IP地址发送的ARP数据包的最大数量为：

  （10 — 优先级）+ 1

  在此，*优先级*配置为**vpn load-balancing** CLI命令的**priority** 子命令。

- 外部上用于Hello请求/响应消息的UDP数据包会交换。端口号在cluster port load-balancing子**命令**中指定，默认为**9023**。

例如，如果负载均衡设备的*优先级*为5，则它会尝试发送最多6个ARP数据包，以查看是否有指挥交换机设备拥有集群IP地址。如果检测到指挥交换机设备，ASA不会再发送任何ARP消息，并等待15秒后再发送UDP Hello请求。然后，指挥交换机设备以UDP Hello响应进行响应。

重新启动场景警告

在负载均衡集群中有两个ASA的重新启动情况下：

- ASA-1或ASA-2在重新启动前是指挥交换机。
- ASA-1重新启动。

- 如果ASA-2之前不是指挥交换机，则它将成为指挥交换机。
- ASA-1只需在重新启动后作为成员加入集群。

负载均衡算法可能会受到交换机配置的影响，其中集群设备的外部接口也连接在交换机上。例如，当连接到交换机的设备重新启动时，生成树算法可能会导致连接延迟。

> **提示**：spanning-tree port fast命令有助于加快进程。

在某些情况下，启用了负载均衡的新重新启动的ASA可能会尝试成为指挥交换机设备（即使已存在指挥交换机设备），因为交换机中的连接延迟导致它无法到达当前指挥交换机设备。当检测到因ARP冲突而发生董事冲突时，具有低媒体访问控制(MAC)地址的ASA会获胜，而具有高MAC地址的ASA会放弃指挥交换机设备角色。

董事连任流程

有两种情况会导致导向器设备重新选举。

从集群中删除的指挥交换机设备

在ASA上禁用该功能时，会向所有集群成员发送广播消息以通知更改，并执行之前描述的选举过程。

指挥交换机设备不响应集群成员Hello消息

如果指挥交换机设备未响应集群成员Hello消息，则ASA集群成员需要大约20秒才能检测到指挥交换机不再存在。Hello消息每五秒发送一次（不可配置）。 如果集群成员在四个Hello消息后未收到来自指挥交换机设备的响应，则会触发选举过程。

故障排除

> **注意**：在使用debug命令之前，请参阅Cisco的“Importent Information on Debug Commands”一文。

以下debug命令对于尝试排除系统故障非常有用：

- **debug fsm 255** — 使用此命令激活常规有限状态机调试。输入no debug **all命令**以停用。
- **debug menu vpnlb 3** — 使用此命令以激活VPN负载平衡调试跟踪。再次输入**debug menu vpnlb 3**命令以停用。
- **debug menu vpnlb 4** — 使用此命令以激活VPN负载平衡功能跟踪。再次输入**debug menu vpnlb 4**命令以停用。

相关信息

- 了解负载均衡
- 技术支持和文档 - Cisco Systems