目录

简介

本文档说明如何配置和升级用于替代已发生故障的防火墙服务模块 (FWSM) 的更换模块。本文档还说明如何配置 Catalyst 6500 系列交换机以最大限度地减少停机时间。这适用于作为故障切换对一部分的 FWSM 以及已进行物理交换的 FWSM（有关详细信息，请参阅硬件安装指南）。

先决条件

要求

在完成本文档中的过程之前：

- 请确保已配置交换机的基本属性。**注意：** 本文档未说明 FWSM 和交换机的初始配置，而是假设在发生硬件故障前，FWSM 和交换机已成功运行。

使用的组件

本文档中的信息基于 Cisco Catalyst 6500 系列防火墙服务模块。

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。

概述

这些步骤在FWSM的配置、升级和更换提示您。这些步骤会在本文档的剩余部分进行进一步详细说明。

1. 在带有更换 FWSM 的交换机上将一个单独 VLAN 定义为防火墙 VLAN（删除旧的防火墙 VLAN 定义）。
2. 将 PC 插入 Catalyst 6000，并将交换机端口分配给刚定义的同一 VLAN。
3. 建立与 FWSM 的会话并启用接口。
4. 使用 PC 作为 TFTP 服务器来下载软件。请确保使用的代码版本与当前活动设备相同。
5. 配置 FWSM 上的基本故障切换设置并恢复旧防火墙 VLAN 和故障切换接口（删除为 TFTP 配置的接口）。此时，会发生配置复制，并且 FWSM 会成为备份。

升级 FWSM 代码

要运行故障切换，两个 FWSM 必须运行同一代码版本。在 RMA'd FWSM 未随附与活动防火墙相同的代码版本的情况下，请完成以下步骤进行升级。

将 FWSM 软件（仅限注册用户）下载到 TFTP 服务器。

启用当前未使用的新交换机 VLAN

完成这些步骤：

1. 将 VLAN 添加到交换机。VLAN 无法成为保留的 VLAN。如果在交换机上运行 Cisco IOS® 软件，请使用 **vlan vlan_number** 命令添加 VLAN。如果在交换机上运行 Catalyst 操作系统软件，请使用 **set vlan vlan_number** 命令添加 VLAN。
2. 将 VLAN 分配给您计划与 PC 连接的交换机端口。使用 Cisco IOS 软件，输入以下命令来将 VLAN 分配到端口：`router(config)#interface type slot/portrouter(config-if)#switchportrouter(config-if)#switchport mode accessrouter(config-if)#switchport access vlan vlan_id`使用 Catalyst 操作系统软件，输入以下命令来将 VLAN 分配到端口：`set vlan vlan_number mod/ports`
3. 将旧防火墙命令复制到记事本以进行备份。接着，替换步骤 1 和 2 中定义的 VLAN，来删除和替换它们。对于 Cisco IOS 软件：`Router(config)#firewall vlan-group firewall_group vlan_rangeRouter(config)#firewall module module_number vlan-group firewall_group`对于 Catalyst 操作系统软件：`Console> (enable) set vlan vlan_list firewall-vlan mod_num`
4. 启用 FWSM 上的接口和 IP 地址：`nameif interface interface_name security_lvlip address interface_name ip_address [mask]interface interface_namefwsm(config-interface) no shutdown`
5. 使用 ping 测试 FWSM 和 PC 之间的连接。确认连接后，使用 theis 命令从 TFTP 服务器下载映像。下载完成后，重新加载 FWSM。`FWSM#copy tftp://server[/path]/filename flash:`例如，输入以下命令：`FWSM#copy tftp://209.165.200.226/cisco/c6svc-fwm-k9.2-1-1.bin flash:`

定义交换机上的防火墙 VLAN

替换在升级 FWSM 代码过程的步骤 1 中删除的命令。

- 对于 Cisco IOS 软件：`Router(config)#firewall vlan-group firewall_group vlan_rangeRouter(config)#firewall module module_number vlan-group firewall_group`
- 对于 Catalyst 操作系统软件：`Console> (enable)set vlan vlan_list firewall-vlan mod_num`

故障切换配置的基本 FWSM

设置一些基本 FWSM 设置以准备将其重新引入对中。然后，重新配置交换机防火墙组/防火墙 VLAN，以将其重新包括到故障切换对中。

1. 删除“启用当前使用的新交换机 VLAN”过程的步骤 4 中定义的旧 nameif 和 IP 地址。
2. 将设备定义为主要设备或辅助设备。`FWSM(config)#`**`fail lan unit {primary|secondary}`**
3. 在系统执行空间中输入以下命令，来配置故障切换 VLAN 接口以用于多个上下文模式：`primary(config)#`**`failover lan interface interface_name vlan vlan`**
4. 输入以下命令，以设置故障切换接口的 IP 地址：`primary(config)#`**`failover interface ip failover_interface ip_address mask standby ip_address`**
5. 启用故障切换：`FWSM(config)#`**`failover`**此输出显示了一个示例：`FWSM(config)#`**`failover lan unit secondary`**`FWSM(config)#`**`failover interface ip fover 10.1.1.10 255.255.255.0 standby 10.1.1.11`**`FWSM(config)#`**`failover LAN Interface fover vlan 50`**`FWSM(config)#`**`failover`**然后将显示此输出：`FWSM(config)#`**`failover lan unit secondary`**`FWSM(config)#`**`failover interface ip fover 10.1.1.10 255.255.255.0 standby 10.1.1.11`**`FWSM(config)#`**`failover LAN Interface fover vlan 50`**`FWSM(config)#`**`failover`**

确认设置和配置

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

发出此 **show** 命令：

```
fwsm(config)#show failoverFailover OnFailover unit PrimaryFailover LAN Interface fover Vlan
150Unit Poll frequency 15 secondsInterface Poll frequency 15 secondsInterface Policy
50%Monitored Interfaces 249 of 250 maximumConfig sync: activeLast Failover at: 10:58:08 Apr 15
2004        This host: Primary - Standby                Active time: 0(sec)
admin Interface inside (10.6.8.91): Normal                admin Interface outside (70.1.1.2):
Normal         Other host: Secondary - Active                Active time: 2232 (sec)
admin Interface inside (10.6.8.100): Normal                admin Interface outside (70.1.1.3):
Normal
```

检查 This host 是否处于备用状态。另请检查是否可以从 FWSM 将设备与接口断开连接。如果想要使新设备成为活动设备，请使用 **no active failover** 命令强制进行故障切换。

在活动模块上输入以下命令，以故障切换到备用模块：

```
primary(config)#no failover active
```

在备用模块上输入以下命令，以强制设备成为活动设备：

```
secondary(config)#failover active
```

有关故障切换配置选项和排除故障的详细信息，请参阅使用故障切换。

相关信息

- Cisco Catalyst 6500 系列防火墙服务模块产品支持
- 技术支持和文档 - Cisco Systems