FWSM 基本配置示例

目录

简介

本文档介绍如何配置安装在 Cisco 6500 系列交换机或 Cisco 7600 系列路由器中的防火墙服务模块 (FWSM) 的基本配置。包括配置 IP 地址、默认路由、静态和动态 NATing、用于允许所需数据流或阻止不需要的数据流的访问控制列表 (ACL) 语句、应用程序服务器（如用于检查来自内部网络的 Internet 数据流的 Websense）以及针对 Internet 用户的 Web 服务器。

注意： 在 FWSM 高可用性 (HA) 方案中，仅当模块之间的许可证密钥完全相同时，故障切换才可成功同步。因此，无法在使用不同许可证的 FWSM 之间进行故障切换。

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以下软件和硬件版本：

- 运行软件版本 3.1 及更高版本的防火墙服务模块
- 带有如下所示的必需组件的 Catalyst 6500 系列交换机：有Cisco IOS软件，叫作Supervisor Cisco IOS，或者Catalyst操作系统的(OS) Supervisor引擎。有关所支持的 Supervisor 引擎和软件版本的信息，请参阅表。装有 Cisco IOS 软件的 Multilayer Switch Feature Card (MSFC) 2。有关所支持的 Cisco IOS 软件版本的信息，请参阅表。

[1] FWSM不支持Supervisor 1或1A。

您使用在Supervisor的Catalyst OS的[2]When，您能使用其中每一个在MSFC的支持的Cisco IOS软件版本。在 Supervisor 上使用 Cisco IOS 软件时，需在 MSFC 上使用相同的版本。

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。

相关产品

此配置也可用于带有如下所示的必需组件的 Cisco 7600 系列路由器：

- 装有 Cisco IOS 软件的 Supervisor 引擎。有关所支持的 Supervisor 引擎和 Cisco IOS 软件版本的信息，请参阅表。
- 装有 Cisco IOS 软件的 MSFC 2。有关所支持的 Cisco IOS 软件版本的信息，请参阅表。

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

FWSM 是安装在 Catalyst 6500 系列交换机和 Cisco 7600 系列路由器上的性能较高、占用空间较少且有状态的防火墙模块。

防火墙可保护内部网络，阻止外部网络的用户对其进行未经授权的访问。防火墙还可在内部网络之间提供保护（例如，如果将人力资源网络与用户网络分开，可采用防火墙保护）。如果某些网络资源（如 Web 或 FTP 服务器）需要供外部用户访问，则可将这些资源置于防火墙之后的一个独立网络（称为隔离区 (DMZ)）上。防火墙允许对 DMZ 的有限访问权限，但是由于 DMZ 仅包括公共服务器，因此，此处的攻击仅影响这些服务器，而不会影响其他内部网络。当内部用户访问外部网络（例如访问 Internet）时，也可进行控制，可以仅允许访问某些外部地址、要求进行身份验证或授权，或者配合使用外部 URL 过滤服务器。

FWSM 包括许多高级功能，如类似于虚拟防火墙的多个安全上下文、透明（第 2 层）防火墙或路由（第 3 层）防火墙操作、数百个接口，以及许多其他功能。

连接到防火墙的网络具有以下特点：外部网络位于防火墙之前，内部网络位于防火墙之后且受到保护，而位于防火墙之后的 DMZ 则允许外部用户进行有限访问。由于 FWSM 可使您使用多种安全策略配置许多接口，其中包括许多内部接口、许多 DMZ，甚至是许多外部接口（如果需要），所以这些术语仅用于泛指。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

配置

本文档使用以下配置：

- Catalyst 6500 系列交换机配置
- FWSM 配置

Catalyst 6500 系列交换机配置

1. 可在 Catalyst 6500 系列交换机或 Cisco 7600 系列路由器上安装 FWSM。这两个系列的配置是相同的，在本文档中，这两个系列通称为**交换机**。**注意：** 在配置 FWSM 之前，首先需要正确配置交换机。
2. **将 VLAN 分配到防火墙服务模块** - 此部分描述如何将 VLAN 分配到 FWSM。FWSM 不包括任何外部物理接口。相反，它使用的是 VLAN 接口。将 VLAN 分配到 FWSM 与将 VLAN 分配到交换机端口类似；FWSM 包括到交换矩阵模块（如果存在）或共享总线的内部接口。**注意：** 有关如何创建 VLAN 以及将其分配到交换机端口的详细信息，请参阅 Catalyst 6500 交换机软件配置指南的配置 VLAN 部分。**VLAN 指南：**可对 FWSM 使用专用 VLAN。将主 VLAN 分配到 FWSM；FWSM 可自动处理辅助 VLAN 数据流。不能使用保留的 VLAN。不能使用 VLAN 1。如果在同一交换机机箱中使用 FWSM 故障切换，请勿将为故障切换和有状态通信保留的 VLAN 分配到交换机端口。但是，如果在机箱之间使用故障切换，则必须将 VLAN 包括在机箱之间的中继端口中。如果将 VLAN 分配到 FWSM 之前未将其添加到交换机，则 VLAN 会存储在 Supervisor 引擎数据库中，这些 VLAN 会在添加到交换机时被发送到 FWSM。将 VLAN 分配到 MSFC 之前，请首先将其分配到 FWSM。不满足此条件的 VLAN 将不会包括在您尝试在 FWSM 上分配的 VLAN 范围内。**在 Cisco IOS 软件中将 VLAN 分配到 FWSM：**在 Cisco IOS 软件中创建最多 16 个防火墙 VLAN 组，然后将这些组分配到 FWSM。例如，可以将所有 VLAN 分配到某一个组，或者可以创建一个内部组和一个外部组，也可以为每位用户创建一个组。每个组可以包含无限多个 VLAN。不可将同一个 VLAN 分配到多个防火墙组；但是，可以将多个防火墙组分配到某个 FWSM，并且可以将单个防火墙组分配到多个 FWSM。例如，要分配到多个 FWSM 的 VLAN 可位于一个单独的组中，该组独立于每个 FWSM 所独有的 VLAN。完成以下步骤，将 VLAN 分配到 FWSM：`Router(config)#`**`firewall vlan-group firewall_group vlan_range`** vlan_range 可以为一个或多个 VLAN（例如 2 到 1000，以及 1025 到 4094），其可以为单个数字 (n)（如 5、10、15）或某个范围 (n-x)（如 5-10、10-20）。**注意：** 路由端口和 WAN 端口会消耗内部 VLAN，因此在 1020-1100 范围内的 VLAN 很可能已被使用。**示例：**

firewall vlan-group 1 10,15,20,25 完成以下步骤，将防火墙组分配到 FWSM。
Router(config)#**firewall module module_number vlan-group firewall_group** firewall_group 为一个或多个组编号，可以是单个数字 (n)（如 5）或某个范围（如 5-10）。**示例：**
firewall module 1 vlan-group 1 **在 Catalyst 操作系统软件中将 VLAN 分配到 FWSM** - 在 Catalyst OS 软件中，可将一列 VLAN 分配到 FWSM。如果需要，可将同一个 VLAN 分配到多个 FWSM。列表可以包含无限多个 VLAN。完成以下步骤，将 VLAN 分配到 FWSM。
Console> (enable)**set vlan vlan_list firewall-vlan mod_num** vlan_list 可以是一个或多个 VLAN（例如 2 到 1000，以及 1025 到 4094），其可以为单个数字 (n)（如 5、10、15）或某个范围 (n-x)（如 5-10、10-20）。

3. **将交换虚拟接口添加到 MSFC** - 在 MSFC 上定义的 VLAN 称为交换虚拟接口。如果将用于 SVI 的 VLAN 分配到 FWSM，则 MSFC 将会在 FWSM 和其他第 3 层 VLAN 之间路由。由于安全原因，默认情况下，在 MSFC 和 FWSM 之间仅可存在一个 SVI。例如，如果错误地为系统配置了多个 SVI，则为 MSFC 分配了内部和外部 VLAN 时，可能会意外允许数据流绕过 FWSM。完成以下步骤，配置 SVIRouter(config)#**interface vlan vlan_number** Router(config-if)#**ip address address mask** **示例：**
interface vlan 20 ip address 192.168.1.1 255.255.255.0

Catalyst 6500 系列交换机配置
!--- Output Suppressed firewall vlan-group 1 10,15,20,25 firewall module 1 vlan-group 1 interface vlan 20 ip address 192.168.1.1 255.255.255.0 *!--- Output Suppressed*

注意： 使用适用于交换机操作系统的命令从交换机建立到 FWSM 的会话：

- Cisco IOS 软件：Router#**session slot <number> processor 1**
- Catalyst OS 软件：Console> (enable) **session module_number**

（可选）与其他服务模块共享 VLAN - 如果交换机具有其他服务模块（例如应用程序控制引擎 (ACE)），则可能必须要与这些服务模块共享某些 VLAN。有关与其他此类模块一起使用时，如何优化 FWSM 配置的详细信息，请参阅包含 ACE 和 FWSM 的服务模块设计。

FWSM 配置

1. **为 FWSM 配置接口** - 需要配置接口名称和 IP 地址才可允许数据流通过 FWSM。还应该更改默认为 0 的安全等级。如果将接口命名为 inside，并且未明确设置安全等级，则 FWSM 会将安全等级设置为 100。**注意：** 每个接口必须具有从 0（最低）到 100（最高）的安全等级。例如，应该将最安全的网络（如内部主机网络）分配为 100 级，而连接到 Internet 的外部网络可以为 0 级。其他网络（如 DMZ）可以在二者之间。可将任一 VLAN ID 添加到配置，但是仅有那些由交换机分配到 FWSM 的 VLAN（例如 10、15、20 和 25）才可传输数据流。使用 **show vlan** 命令可查看所有分配到 FWSM 的 VLAN。
interface vlan 20 nameif outside security-level 0 ip address 192.168.1.2 255.255.255.0
interface vlan 10 nameif inside security-level 100 ip address 10.1.1.1 255.255.255.0
interface vlan 15 nameif dmz1 security-level 60 ip address 192.168.2.1 255.255.255.224
interface vlan 25 nameif dmz2 security-level 50 ip address 192.168.3.1 255.255.255.224 **提示**：在 **nameif <name>** 命令中，*name* 是最多为 48 个字符的文本字符串，且不区分大小写。使用新值重新输入此命令可更改名称。请勿输入 no 形式，因为该命令将会导致删除所有引用此名称的命令。
2. **配置默认路由：**
route outside 0.0.0.0 0.0.0.0 192.168.1.1 默认路由用于标识网关 IP 地址 (192.168.1.1)，FWSM 会将没有其获知路由或静态路由的所有 IP 数据包发送到此网关地址。

默认路由仅仅是目标 IP 地址为 0.0.0.0/0 的静态路由。标识特定目标的路由优先于默认路由。

3. **动态 NAT** 可将一组实际地址 (10.1.1.0/24) 转换成可在目标网络上路由的映射地址 (192.168.1.20-192.168.1.50) 池。映射池包括的地址可以比实际组少。当要转换的主机访问目标网络时，FWSM 会从映射池中为其分配一个 IP 地址。仅当实际主机启动连接时才会添加转换。转换仅在连接期间开启，转换超时之后，不会为特定用户保留相同的 IP 地址。
   nat (inside) 1 10.1.1.0 255.255.255.0 global (outside) 1 192.168.1.20-192.168.1.50 netmask 255.255.255.0 access-list Internet extended deny ip any 192.168.2.0 255.255.255.0 access-list Internet extended permit ip any any access-group Internet in interface inside 需要创建 ACL 以拒绝来自内部网络 10.1.1.0/24 的数据流进入 DMZ1 网络 (192.168.2.0)，并通过将 ACL *Internet* 应用到作为传入数据流进入方向的内部接口以允许其他类型的数据流传输到 Internet。
4. **静态 NAT** 可创建从实际地址到映射地址的固定转换。使用动态 NAT 和 PAT 时，每台主机在每次后续转换时均使用不同的地址或端口。因为使用静态 NAT 时每个连续连接的映射地址是相同的，并且存在持久性的转换规则，因此，静态 NAT 可允许目标网络上的主机发起流向已转换主机的数据流，但前提是存在允许该行为的访问列表。动态 NAT 和静态 NAT 地址范围之间的主要区别是：如果存在允许相应行为的访问列表，静态 NAT 可允许远程主机发起与已转换主机的连接，而动态 NAT 却不允许这样做。对于静态 NAT，映射地址的数量需与实际地址相同。
   static (dmz1,outside) 192.168.1.6 192.168.2.2 netmask 255.255.255.255 static (dmz2,outside) 192.168.1.10 192.168.3.2 netmask 255.255.255.255 access-list outside extended permit tcp any host 192.168.1.10 eq http access-list outside extended permit tcp host 192.168.1.30 host 192.168.1.6 eq pcanywhere-data access-list outside extended permit udp host 192.168.1.30 host 192.168.1.6 eq pcanywhere-status access-list inbound extended permit udp any host 216.70.55.69 range 8766 30000 access-group outside in interface outside 以上显示了两个静态 NAT 语句。第一个语句用于将内部接口上的实际 IP 192.168.2.2 转换为外部子网上的映射 IP 192.168.1.6，前提是 ACL 允许来自源 192.168.1.30 的数据流传输到映射 IP 192.168.1.6 以便访问 DMZ1 网络中的 Websense 服务器。同样地，在ACL允许从互联网的流量到被映射的IP 192.168.1.10为了访问在DMZ2网络的网络服务器和有udp端口号在8766到30000范围内条件下，第二个静态NAT语句含义翻译在内部接口的实时IP 192.168.3.2到在外部子网的被映射的IP 192.168.1.10。
5. **url-server** 命令可指定运行 Websense URL 过滤应用程序的服务器。相关的限制是单上下文模式下最多 16 个 URL 服务器，多模式下最多 4 个 URL 服务器，但是每次仅可使用一个应用程序（N2H2 或 Websense）。此外，更改安全设备上的配置后，应用程序服务器上的配置并不会更新。需按照供应商的相关说明分别进行配置更改。在发出针对 HTTPS 和 FTP 的 filter 命令之前必须先配置 **url-server** 命令。如果从服务器列表中删除了所有 URL 服务器，则也会删除与 URL 过滤相关的所有 filter 命令。指定服务器之后，请使用 **filter url** 命令启用 URL 过滤服务。
   url-server (dmz1) vendor websense host 192.168.2.2 timeout 30 protocol TCP version 1 connections 5 **filter url** 命令允许阻止来自您使用 Websense 过滤应用程序指定的 World Wide Web URL 的出站用户的访问。
   filter url http 10.1.1.0 255.255.255.0 0 0

FWSM 配置

```
!--- Output Suppressed interface vlan 20 nameif outside
security-level 0 ip address 192.168.1.2 255.255.255.0
interface vlan 10 nameif inside security-level 100 ip
address 10.1.1.1 255.255.255.0 interface vlan 15 nameif
dmz1 security-level 60 ip address 192.168.2.1
255.255.255.224 interface vlan 25 nameif dmz2 security-
level 50 ip address 192.168.3.1 255.255.255.224 passwd
fl0wer enable password treeh0u$e route outside 0 0
```

```
192.168.1.1 1 url-server (dmz1) vendor websense host
192.168.2.2 timeout 30 protocol TCP version 1
connections 5 url-cache dst 128 filter url http 10.1.1.0
255.255.255.0 0 0 !--- When inside users access an HTTP
server, FWSM consults with a !--- Websense server in
order to determine if the traffic is allowed. nat
(inside) 1 10.1.1.0 255.255.255.0 global (outside) 1
192.168.1.20-192.168.1.50 netmask 255.255.255.0 !---
Dynamic NAT for inside users that access the Internet
static (dmz1,outside) 192.168.1.6 192.168.2.2 netmask
255.255.255.255 !--- A host on the subnet 192.168.1.0/24
requires access to the Websense !--- server for
management that use pcAnywhere, so the Websense server
!--- uses a static translation for its private address.
static (dmz2,outside) 192.168.1.10 192.168.3.2 netmask
255.255.255.255 !--- A host on the Internet requires
access to the Webserver, so the Webserver !--- uses a
static translation for its private address. access-list
Internet extended deny ip any 192.168.2.0 255.255.255.0
access-list Internet extended permit ip any any access-
group Internet in interface inside !--- Allows all
inside hosts to access the outside for any IP traffic,
!--- but denies them access to the dmz1 access-list
outside extended permit tcp any host 192.168.1.10 eq
http !--- Allows the traffic from the internet with the
destination IP address !--- 192.168.1.10 and destination
port 80 access-list outside extended permit tcp host
192.168.1.30 host 192.168.1.6 eq pcanywhere-data access-
list outside extended permit udp host 192.168.1.30 host
192.168.1.6 eq pcanywhere-status !--- Allows the
management host 192.168.1.30 to use !--- pcAnywhere on
the Websense server access-list inbound extended permit
udp any host 216.70.55.69 range 8766 30000 !--- Allows
udp port number in the range of 8766 to 30000. access-
group outside in interface outside access-list WEBSENSE
extended permit tcp host 192.168.2.2 any eq http access-
group WEBSENSE in interface dmz1 !--- The Websense
server needs to access the Websense !--- updater server
on the outside. !--- Output Suppressed
```

验证

使用本部分可确认配置能否正常运行。

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。

1. 根据操作系统查看模块信息，以验证交换机是否已确认 FWSM 并将其联机：Cisco IOS 软件：`Router#show module Mod Ports Card Type Model Serial No. --- ----- ---------- ---------- ----------- 1 2 Catalyst 6000 supervisor 2 (Active) WS-X6K-SUP2-2GE SAD0444099Y 2 48 48 port 10/100 mb RJ-45 ethernet WS-X6248-RJ-45 SAD03475619 3 2 Intrusion Detection System WS-X6381-IDS SAD04250KV5 4 6 Firewall Module WS-SVC-FWM-1 SAD062302U4` Catalyst OS 软件：`Console>show module [mod-num] The following is sample output from the show module command: Console> show module Mod Slot Ports Module-Type Model Sub Status --- ---- ----- ---------- ---------- --- ------ 1 1 2 1000BaseX Supervisor WS-X6K-SUP1A-2GE yes ok 15 1 1 Multilayer Switch Feature WS-F6K-MSFC no ok 4 4 2 Intrusion Detection Syste WS-X6381-IDS no ok 5 5 6 Firewall Module WS-SVC-FWM-1 no ok 6 6 8 1000BaseX Ethernet WS-X6408-GBIC no ok`**注意：** **show module** 命令用于显示 FWSM 的 6 个端口。这些端口是组合为 EtherChannel 的内部端口。

2. `Router#show firewall vlan-group Group vlans ----- ------ 1 10,15,20 51 70-85 52 100`
3. `Router#show firewall module Module Vlan-groups 5 1,51 8 1,52`
4. 输入适用于操作系统的命令，以查看当前引导分区：Cisco IOS 软件：`Router#show boot device [mod_num]` **示例：**`Router#show boot device [mod:1 ]: [mod:2 ]: [mod:3 ]: [mod:4 ]: cf:4 [mod:5 ]: cf:4 [mod:6 ]: [mod:7 ]: cf:4 [mod:8 ]: [mod:9 ]:`Catalyst OS 软件：`Console> (enable) show boot device mod_num` **示例：**`Console> (enable) show boot device 6 Device BOOT variable = cf:5`

故障排除

本部分提供了可用于对配置进行故障排除的信息。

1. **设置默认引导分区** - 默认情况下，FWSM 从 cf:4 应用程序分区中引导。但是，您可以选择从 **cf:5** 应用程序分区中引导或从 cf:1 维护分区引导。要更改默认引导分区，请输入适用于操作系统的命令：Cisco IOS 软件：`Router(config)#boot device module mod_num cf:n` 其中的 n 为 1（维护）、4（应用程序）或 5（应用程序）。Catalyst OS 软件：`Console> (enable) set boot device cf:n mod_num` 其中的 n 为 1（维护）、4（应用程序）或 5（应用程序）。
2. **在 Cisco IOS 软件中重置 FWSM** - 要重置 FWSM，请输入如下所示的命令：`Router#hw-module module mod_num reset [cf:n] [mem-test-full]` cf:**n** 参数为分区，可以是 1（维护）、4（应用程序）或 5（应用程序）。如果未指定分区，则使用默认分区，通常为 **cf:4**。**mem-test-full** 选项用于运行完整内存测试，完成该测试大约需要 6 分钟。**示例：**`Router#hw-mod module 9 reset Proceed with reload of module? [confirm] y % reset issued for module 9 Router# 00:26:55:%SNMP-5-MODULETRAP:Module 9 [Down] Trap 00:26:55:SP:The PC in slot 8 is shutting down. Please wait ...` **Catalyst OS 软件**：`Console> (enable) reset mod_num [cf:n]` 其中的 **cf:n** 为分区，可以是 1（维护）、4（应用程序）或 5（应用程序）。如果未指定分区，则使用默认分区，通常为 **cf:4**。

注意： 无法在 FWSM 上配置 NTP，因为 NTP 是在交换机中进行设置的。

问题：无法将 VLAN 数据流从 FWSM 传输到 IPS Sensor 4270

无法将数据流从 FWSM 传输到 IPS Sensor。

解决方案

使数据流通过 IPS 的方法是创建辅助 VLAN，以便有效地将当前 VLAN 分为两部分，然后将其桥接在一起。使用 VLAN 401 和 501 检查此示例，以便进一步了解以下内容：

- 如果要扫描主 **VLAN 401** 上的数据流，请创建另一个 vlan VLAN 501（辅助 VLAN）。然后禁用 VLAN 接口 401，401 中的主机当前正将其用作默认网关。
- 然后使用之前在 VLAN 401 接口上禁用的*同*一地址启用 VLAN 501 接口。
- 将 IPS 接口中的一个置于 VLAN 401 中，另一个置于 VLAN 501 中。

只需将 VLAN 401 的默认网关移到 VLAN 501 上。如果存在 VLAN，则需要对 VLAN 做类似的更改。请注意，VLAN 本质上与 LAN 网段类似。默认网关可在与使用该网关的主机不同的线路上。

FWSM 中的无序数据包问题

如何解决 FWSM 中的无序数据包问题？

解决方案

在全局配置模式下发出 sysopt np completion-unit 命令可解决 FWSM 中的无序数据包问题。在 FWSM 版本 3.2(5) 中引入了此命令，用于确保数据包的转发顺序和接收顺序相同。

问题：无法将非对称路由数据包传输通过防火墙

无法将非对称路由数据包传输通过防火墙。

解决方案

在类配置模式下发出 set connection advanced-options tcp-state-bypass 命令可将非对称路由数据包传输通过防火墙。在 FWSM 版本 3.2(1) 中引入了此命令。

FWSM 中的 Netflow 支持

FWSM 是否支持 Netflow？

解决方案

FWSM 不支持 Netflow。

相关信息

- Cisco Catalyst 6500 系列防火墙服务模块支持页
- Cisco Catalyst 6500 系列交换机支持页
- Cisco 7600 系列路由器支持页
- FWSM TCP拦截和解释的SYN Cookie
- 技术支持和文档 - Cisco Systems