防火墙服务模块(FWSM)常见问题

目录

简介
支持的功能
许可授权
VLAN问题
Ping问题
故障切换问题
其他
相关信息

简介

本文档包含有关 Catalyst 6500 系列防火墙服务模块 (FWSM) 的常见问题 (FAQ)。

注意： 有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

支持的功能

Q. 要支持 FWSM、入侵检测系统模块 2 (IDSM2) 和 VPN 服务模块 (VPNSM)，需要运行的最低代码版本是多少？

A. 相应的代码版本取决于 6500 或 7600 机箱中的 Supervisor 模块类型，以及所运行的软件类型（CatOS [混合] 或 Cisco IOS [本地]）。有关模块和 Multilayer Switch Feature Card (MSFC) 的特定代码版本，请参阅此表格。

	Sup1（带有 MSFC）		Sup2（带有 MSFC）		Sup720	
模块	**Cisco IOS**	**CatOS**	**Cisco IOS**	**CatOS**	**Cisco IOS**	**CatOS**
FWSM	12.1(13)E	7.5(1)	12.1(13)E	7.5(1)	12.2(14)SX1	8.2(1)
IDSM2	不支持	7.6(1)	12.1(19)E	7.6(1)	12.2(14)SX1	8.2(1)
VPNSM	不支持	不支持	12.2(14)SY	不支持	12.2(17a)SX10	不支持*

*我们计划将提供支持。

注意： 有关 CatOS（混合）与 Cisco IOS（本地）之间的差别，请参阅用于 Cisco Catalyst 6500 系列交换机的 Cisco Catalyst 和 Cisco IOS 操作系统的比较。

Q. 能否在同一机箱中运行 FWSM、入侵检测系统模块 2 (IDSM2) 和 VPN 服务模块 (VPNSM)？

A. 可以，如果交换机运行的是 Cisco IOS 软件版本 12.2(14)SY (Sup2) 或 12.2(17a)SX10 (Sup720) 及更高版本的集成 Cisco IOS 软件，则可以在同一机箱中运行这些模块。目前的 CatOS 版本均不支持在同一个 6500 或 7600 机箱中运行这些服务模块。

Q. FWSM 有哪些配置和管理选项？

A. 配置和管理选项如下。

选项	version	说明
防火墙管理中心	1.1.1 及更高版本*	这是一个基于 Web 的界面，可用于配置和管理多个防火墙。 **注意：** 对象分组内对服务组的支持是有限的。服务组被成功解析，但会立即被抹平。这会影响包含 **icmp-type**、protocol 和 service 关键字的命令。1.3 及更早版本存在该限制。
安全监控中心	1.2 及更高版本*	这是基于 Web 的界面，用于监控 Cisco 安全设备。该软件集中多个 Cisco 安全设备的 Syslog 管理功能，提供灵活的报告和警报选项。
性能监控中心	2.0 及更高版本*	这是基于 Web 的界面，用于监控与网络安全相关服务的运行状况和性能并对其进行故障排除。所用的底层协议为简单网络管理协议 (SNMP)。
PDM	版本 2.1	这是基于 Web 的界面，用于配置、管理和监控单个防火墙。PIX 设备管理器 (PDM) 必须安装在本地 PIX 防火墙上。
Telnet	不适用	Telnet 允许通过远程命令行界面 (CLI) 对防火墙进行访问。 **注意：** 为允许通过 Telnet 对最底层的安全接口（通常称为外部接口）进行访问，需要配置 IPsec 以进行管理。
Secure Shell (ssh)	不适用	SSH 允许通过远程 CLI 对防火墙进行安全访问。
SNMP	不适用	SNMP 提供了一种 FWSM 监控方法。 **注意：** SNMP 在 FWSM 上是只读的。
Syslog	不适	Syslog 提供了一种 FWSM 监控方法。

	用	

*此软件是 CiscoWorks VPN/安全管理解决方案 (VMS) 捆绑件的一部分。此软件提供了一种集成式管理方法，即通过基于浏览器的企业网络界面管理 Cisco 安全设备。

Q. 什么是 SVI？能否配置多个 SVI？

A. SVI 代表交换机虚拟接口。它代表交换机上第 3 层逻辑接口。对低于 7.6(1) 的 CatOS 版本和低于 12.2(14)SY 的 Cisco IOS 软件版本而言，仅允许一个 SVI 作为防火墙 VLAN 的一部分。换句话说，在 FWSM 和 Multilayer Switch Feature Card (MSFC) 之间只能配置一个第 3 层接口。若试图配置多个 SVI，命令行界面 (CLI) 将会产生错误消息。

对于 CatOS 7.6(1) 及更高版本和 Cisco IOS 软件版本 12.2(14)SY 及更高版本，FWSM 支持多个 SVI。默认情况下，仅支持一个 SVI。使用下列命令之一可在交换机上启用对多个 SVI 的支持。

- 对于 CatOS，键入 set firewall multiple-vlan-interfaces enable。对于 Cisco IOS，键入 firewall multiple-vlan-interfaces。

如果为交换机配置 FWSM VLAN 后收到错误消息，消息表明存在多个 SVI，请查看交换机和/或 MSFC 配置，确保只有一个第 3 层接口（或 VLAN 接口）作为防火墙 VLAN 的一部分存在。

注意： 仅使用一个 SVI。这样可以避免包含策略路由的复杂配置。

Q. FWSM 是否支持 SNMPv3？

A. 不能。

Q. FWSM 支持多少个 VLAN？

A. FWSM 版本 1.1 支持 100 个 VLAN，FWSM 版本 2.1 支持 250 个 VLAN。

Q. FWSM 是否支持 access-list compiled 命令？

A. CLI 处于非活动状态 10 秒钟后，FWSM 会自动将访问列表编译到硬件中，因此无需 Turbo 访问列表。FWSM 版本 2.1 还提供了其他功能，能够指定访问列表的编译时间。

Q. FWSM 是否支持 IOS 开放最短路径优先 (OSPF) auto-cost reference-bandwidth 命令？

A. 不能。FWSM 无法识别与之连接的物理端口。必须使用 ospf cost 命令为每个接口手动配置 OSPF 开销。

Q. 能否在 FWSM 的两个不同接口与同一网络相连的拓扑中运行开放最短路径优先 (OSPF) 协议？

A. 可以。2.1 及更高版本支持此功能。

Q. FWSM 支持哪些路由协议？

A. 开放最短路径优先 (OSPF) 和路由信息协议 (RIP) 均为受支持的路由协议。关于FWSM的更多信

息，参考在Cisco Catalyst 6500系列防火墙服务模块页的文档联机。

Q. FWSM 是否支持多播（Internet 组管理协议 [IGMP] v2 和残域多播路由）？

A. 可以。FWSM 2.1 及更高版本支持此功能。如果您运行的是版本 1.1，可以使用通用路由封装 (GRE) 隧道作为解决办法。

Q. FWSM 是否支持 URL 过滤？

A. 可以。1.1 及更高版本支持 Websense，2.1 版中还增加了对 N2H2 的支持。

Q. FWSM 为什么会丢弃分段的数据包？

A. 默认情况下，分段的数据包不能通过 FWSM 进行传输。可以使用 fragment 命令配置此功能。该行为与 PIX 防火墙有所不同。使用分段数据包的常见协议是开放最短路径优先 (OSPF) 和网络文件系统 (NFS)。

Q. 能否终止 FWSM 上的 VPN 连接？

A. FWSM 不支持 VPN 功能。VPN 连接的终止由交换机和/或 VPN 服务模块控制。3DES 许可仅用于管理目的，例如通过 Telnet、Secure Shell (SSH) 和安全 HTTP (HTTPS) 连接到安全级别低的接口。

Q. FWSM 是否支持基于 RADIUS 或 TACACS+ 的身份验证、授权和记账 (AAA) 功能？

A. AAA 对于 FWSM 管理和通过 FWSM 的数据流均支持。有关其他详细信息，请参阅防火墙服务模块文档。

FWSM 提供与 PIX 防火墙相似的功能，除此之外，还提供可下载的访问列表和 VPN。因此，您可以使用下列 PIX 防火墙文档作为 FWSM 配置指南。

- 如何在 Cisco 安全 PIX 防火墙（5.2 到 6.2）中执行并启用身份验证
- 在 PIX 5.2 及更高版本中执行用户身份验证、授权和记账

Q. 如何对 FWSM 执行口令恢复？

A. 有关口令恢复的信息，请参阅下列文档。

- 对于版本1.1(1)，参考关于更改和恢复密码的FWSM配置说明1.1(1)。
- 对于版本1.1(2)和1.1(3)，参考关于更改和恢复密码的FWSM配置说明1.1(2)。

Q. FWSM 是否支持超巨型帧？

A. 是，FWSM 可以支持超巨型帧。

Q. 当收到数据包和其源地址一起作为环回地址， FWSM如何响应？

A. 它对待数据包作为无效并且丢弃数据包。默认情况下， FWSM丢弃数据包和一无效源地址一起例如环回地址、广播地址和目的地主机地址。如此示例所显示的日志消息生成。

```
%FWSM-2-106016: Deny IP spoof from (IP_address) to
 IP_address on interface interface_name.
```

Q. FWSM 是否支持 PVLAN？

A. 从软件版本 3.1 起开始支持 PVLAN。如果运行的软件为 3.1 之前的版本，则唯一可能的解决办法是使用交叉电缆将 PVLAN 的混合端口连接到普通的接入端口，然后为该接入端口的 VLAN 建立防火墙。

Q. FWSM 是否支持访问列表行编号？

A. 仅 3.1 及更高版本的软件支持此功能。

Q. 能否限制用户在 FWSM 上可以拥有的连接数？

A. 能，您可以借助模块化策略框架限制连接。要限制连接数，请完成以下步骤：

1. 创建一个类映射以匹配数据流。
2. 将类映射放置到策略映射中，并在策略映射中使用连接限制。
3. 使用服务策略应用策略映射。

有关更多信息和详细的步骤，请参阅配置连接限制和超时。

Q. 在 FWSM 中实施多播是否有任何限制？

A. 可以。FWSM 不支持将 232.x.x.x 子网作为组名称，因为已将其保留用于安全服务模块 (SSM)。

Q. 是否允许定向广播通过 FWSM？

A. 不能。和路由器不同，FWSM 不允许定向广播通过其接口。一个较类似的解决办法是使用内建的 DHCP 中继功能将广播从一个接口转发到另一个接口。

Q. HTTP 检测引擎能否检测到 HTTP 会话中的非 HTTP 数据流或非标准数据流？

A. 可以。带有高级 HTTP 检测的应用层防火墙可以检测和控制这些数据流。有关详细信息，请参阅应用检测引擎概述。

Q. ASA 和 FWSM 中的标准化功能是否互相兼容？

A. 在 FWSM 中，TCP 标准化仅适用于满足 TCP 协议组的数据流。正常的数据层面（快速路径）数据流不受影响。这与 ASA 不同，因为所有的 ASA 数据流均受规范器的控制。

在 FWSM 上，如果禁用规范器，模块将返回到 2.3 的行为。但如果禁用 **control-point tcp-normalizer**，将会在 FWSM 中阻止对控制层面上收到的、用于检查第 7 层的 TCP 数据包进行严格的 TCP 检查（例如检测无序分段和监控 TCP 选项），而且该检查将不会被执行。因此，我们不建议将其禁用。FWSM 不允许调整默认的 tcp-map 参数。

Q. 是否需要启用/禁用 TCP 规范器？

A. 由于无法将某些连接的特定信息从 NP 传递到控制层面，因此 TCP 规范器可能在 FWSM 中始终不能正常运行。另外，也无法识别与连接相关联的唯一 tcp-map。因此，FWSM 依赖于默认的 tcp-map，而默认的 tcp-map 可能不会对所有连接都正常运行。由于这些限制，有必要在控制层面中启用/禁用 TCP 规范器，以使数据流通过防火墙。FWSM 不允许调整默认的 tcp-map 参数。

Q. FWSM 最多可支持多少个 mfib 条目？

A. 最多支持 5000 个条目。

Q. 如何在 FWSM 中捕获数据包？

A. 可以在 FWSM 中捕获数据包。ASDM 不支持使用 CLI 捕获数据包，而且也不支持 **capture** 命令。有关详细信息，请参阅忽略的和仅限查看的命令。有关 FWSM 中数据包捕获配置的详细信息，请参阅捕获数据包。有关数据包捕获配置示例的详细信息，请参阅 ASA/PIX/FWSM：使用 CLI 和 ASDM 进行数据包捕获的配置示例。

Q. FWSM 支持哪个版本的 ASDM？

A. 有关 FWSM 和 ASDM 发行版本兼容性的详细信息，请参阅 FWSM 和 ASDM 发行版本兼容性。

许可授权

Q. 我拥有在多上下文模式下运行 FWSM 的许可证。我能否获得备用 FWSM 许可证，以备出现硬件故障时使用？

A. 您可以获取备用 FWSM 许可证。但和普通许可证一样，您需要订购备用 FWSM 许可证。出现硬件故障时，请联系 Cisco 技术支持部门，确认故障并获取备用 FWSM 许可证。有关许可信息，请参阅 Cisco 防火墙模块软件版本 2.2(1)。

Q. FWSM 是否支持多个共享接口？

A. FWSM 不支持多个共享接口，但可以在多上下文中有一个 VLAN。有关详细信息，请参阅在上下文之间共享资源和接口。

VLAN问题

Q. 如何在 FWSM 后放置额外的 VLAN？

A. 要将 vlan 200 添加到配置中，请使用 **nameif** 命令。安全等级应在 0 和 100 之间。完整的命令语法是 **nameif vlan200 <接口名称> <安全级别>**。

Q. 使用单上下文路由模式可在 FWSM 后放置多少 VLAN？

A. 使用单上下文路由模式可在 FWSM 后放置 1000 个 VLAN。

Ping问题

Q. 为什么我无法在直接连接的接口上对 FWSM 执行 ping 操作？

A. 默认情况下，每个接口都会拒绝 Internet 控制消息协议 (ICMP)。请使用 **icmp** 命令允许该数据流发往接口。该行为与 PIX 有所不同。

注意： 当发往接口的 ICMP 被 **icmp** 命令拒绝时，您仍会在地址解析协议 (ARP) 表中看到正确的 MAC 地址。如果看不到 MAC 地址，请参阅下一个问题。

Q. 我无法对直接连接的接口上的 FWSM 执行 ping 操作，而且看不到对应该接口的地址解析协议 (ARP) 条目。我在交换机上运行的是 CatOS（或混合）软件。我该怎么办？

A. 如果在交换机上（CatOS 的监控模块上）配置接口之前，先在 FWSM 配置中（使用 nameif 命令）或在 Multilayer Switch Feature Card (MSFC) 上 [使用 interface vlan 命令] 配置接口，可能会使接口看起来似乎根本未响应，没有 ARP 条目，或者没有 Internet 控制消息协议 (ICMP) 响应。

如果在配置交换机之前已在属于防火墙 VLAN 的 FWSM 或 MSFC 上配置了一个接口，请删除 FWSM 或 MSFC 条目，重新加载模块，然后重新添加条目。

Q. 为什么我无法执行 ping 操作或使任何数据流通过 FWSM？

A. 要使数据流通过 FWSM 从安全级别较高的接口（内部接口）流向安全级别较低的接口（外部接口），必须使用 nat 0、nat/global 或 static 命令配置网络地址转换 (NAT)。

您还必须使用 **access-list** 命令实施允许数据流通过 FWSM 的访问列表。默认情况下，访问列表会拒绝所有接口上的所有数据流 (**deny ip any any**)。该行为不同于 PIX 的默认配置，该默认配置允许数据流从安全级别较高的接口流向安全级别较低的接口，拒绝数据流从安全级别较低的接口流向安全级别较高的接口。使用 **permit ip any any** 配置访问列表并将其应用于安全级别高的接口，使 FWSM 的行为和 PIX 一样。

Q. 我可以对直接连接到我的网络的 FWSM 接口执行 ping 操作，但无法对其他接口执行 ping 操作。这是否正常？

A. 可以。这是一种内建安全机制，也存在于 PIX 防火墙中。

故障切换问题

Q. 能否在两个运行不同版本代码的 FWSM 之间配置故障切换？

A. 不能。故障切换要求两个 FWSM 运行相同版本的代码。故障切换功能中的机制将验证对等版本，如果代码版本不同，将阻止故障切换。因此，您必须同时升级两个 FWSM。

Q. 能否在不同机箱中的两个 FWSM 之间配置故障切换？

A. 可以。但所有接口上的 FWSM 都必须通过第 2 层相连。换句话说，所有接口必须能够彼此互相交换第 2 层广播数据包 [地址解析协议 (ARP) 等]。不可以在第 3 层上路由故障切换协议数据包。

Q. 我已经在两个 FWSM 之间设置故障切换，但是它们不同步。可能是什么原因？

A. 要成功实施故障切换，请确保您的配置满足下列要求。

- 两个 FWSM 必须运行相同版本的代码。
- 两个 FWSM 必须拥有相同数量的 VLAN。
- 第 2 层连接必须存在于 FWSM 上的所有 VLAN 之间。如果 FWSM 位于不同机箱中且机箱之间配置有中继，请确保所有 VLAN 均存在且中继上允许所有 VLAN。

Q. 能否为分布于不同交换机机箱上的三个或更多 FWSM 单元配置故障切换？

A. **不能。**故障切换设置仅支持一对 FWSM，例如两个单元。这两个单元可以在同一个交换机中，也可以在两台独立的交换机中。如果将辅助 FWSM 与主要 FWSM 安装在同一交换机中，则可防止模块出现故障。为了防止模块和交换机发生故障，可将辅助 FWSM 安装在单独的交换机中。FWSM 不会直接通过交换机协调故障切换，而是与交换机故障切换操作协同运行。有关详细信息，请参阅机箱内部和机箱之间的模块放置。

其他

Q. FWSM 上有个标签说明："当状态指示灯为绿色时请勿将卡拆除，否则可能损坏磁盘。"这是什么意思？

A. 拆除防火墙模块之前必须使用以下方法之一关闭电源。（以下方法无优劣之分。）

- 请使用交换机的命令行界面 (CLI) 发出以下任意一条命令。CatOS - set module power down modCisco IOS® 软件 - no power enable module slot
- 按下刀片上的**关闭**按钮。
- 关闭机箱电源。

当状态指示灯不显示绿色时，可将该模块安全拆除。

Q. 使用了 show module 命令后，我的 FWSM 状态为 faulty/other。我该怎么办？

A. 请参阅以下核对表，对状态为 faulty/other 的 FWSM 进行故障排除。

- 确保交换机上运行的代码版本是受支持的。
- 确保 FWSM 可以与同一机箱中的其他刀片共存。有关详细信息，请参阅 Catalyst 6500 发行版本注释和/或 Software Advisor（仅限注册用户）。
- 如果要在交换机上运行 CatOS/混合代码，请重置 FWSM 模块占用的插槽配置。请使用下列命令执行此操作。键入 set module power down mod，关闭 FWSM 的电源。键入 **clear config mod**，清除与该插槽相关联的交换机的配置，并打开模块的电源。

有关详细信息，请参阅本文档。

- 运行 CatOS 的 Catalyst 4000、5000 和 6000 系列交换机的硬件故障清单
- 对运行集成 Cisco IOS（本地模式）的 Catalyst 6000 系列交换机硬件和常见问题进行故障排除

如果仍然出现问题，请联系 Cisco 技术支持以进行进一步的故障排除。

Q. 在哪里可以找到 FWSM 文档？

A. 有关 FWSM 的发行版本注释，请参阅 Catalyst 6500 系列发行版本注释。欲知更多信息，参考在 Cisco Catalyst 6500系列防火墙服务模块页的文档联机。

Q. 在哪里可以找到有关 FWSM 所示错误消息的信息？

A. 错误消息解码器（仅限注册用户）提供了许多 FWSM 错误消息的详细信息。另外，关于系统消息的产品文档也包含许多有用的信息。如果需要进一步协助，请与 Cisco 技术支持部门联系。

Q. 在哪里可以找到关于 FWSM 上现有 Bug 的信息？

A. 有关现有 Bug 的详细信息，请参阅 Bug 工具包（仅限注册用户）。

Q. PIX 防火墙和防火墙服务模块有何区别？

A. PIX 和 FWSM 基于相似的代码。但两者有着根本性的区别。PIX（提供支持）提供 VPN 和 IDS 功能。FWSM 不提供 VPN 和 IDS 功能，因为其他板卡已提供了这些功能。有关 Catalyst 6500 系列入侵检测系统 (IDSM-2) 服务模块的详细信息，请参阅 Catalyst 6500 系列入侵检测系统 (IDSM-2) 服务模块数据表。有关 Catalyst 6500 IPsec VPN 服务模块的详细信息，请参阅 Catalyst 6500 IPsec VPN 服务模块产品数据表。

有关 PIX 与 FWSM 之间的细微差别，请参阅以下文档：

- PIX 技术文档
- PIX 发行版本注释
- PIX 命令参考
- FWSM 技术文档
- FWSM 发行版本注释
- FWSM 命令参考

Q. 我无法在 FWSM 上对每个接口发出多个 access-group 命令。FWSM 似乎对每个接口只接受一个访问组。为什么？

A. 在 FWSM 中发出这些命令时，只有最后一个 **access-group** 命令会显示：

```
access-group allow_icmp in interface outside
access-group allow_caltech in interface outside
```

这是因为 FWSM 对每个方向的每个接口只允许一个访问列表。

Q. FWSM 的 xlate 条目中存储有哪些信息？

A. Xlate 条目会存储以下信息：

1. **源接口** — 这是接收数据包的接口，例如 outside。
2. **源 IP 地址** — 这是数据包的源 IP 地址。
3. **转换后的 IP 地址** — 假如没有 NAT 语句，则转换后的 IP 地址和源 IP 地址相同。
4. **目标接口** — 根据路由表中对数据包目标 IP 地址的查询结果，数据包离开的接口。

Q. 在 FWSM 上使用 show perfmon 命令输出的值和统计数据表示什么？

A. 使用 **show perfmon** 命令可获取有关 FWSM 性能的信息。

```
FWSM#show perfmon FWSM#show console-output Context: my_context PERFMON STATS: Current Average
```

```
Xlates 0/s 0/s Connections 0/s 0/s TCP Conns 0/s 0/s UDP Conns 0/s 0/s URL Access 0/s 0/s URL
Server Req 0/s 0/s WebSns Req 0/s 0/s TCP Fixup 0/s 0/s TCP Intercept 0/s 0/s HTTP Fixup 0/s 0/s
FTP Fixup 0/s 0/s AAA Authen 0/s 0/s AAA Author 0/s 0/s AAA Account 0/s 0/s
```

Current 列按照当前间隔时间显示统计数据，而最后一列 Average 显示自上次清除统计数据起的累计平均值。它以 /s 表示，因为它是速率，而非绝对值。

默认情况下，命令输出中显示的统计数据每隔 120 秒更新一次。间隔时间可通过 **perfmon interval** 命令进行更改。

```
FWSM#perfmon interval 20
```

这意味着每 20 秒计算一次 Current 列中报告的统计速率。另外，每当输入 **show perfmon** 命令时，速率都会按那个时间点的统计数据进行计算。

FWSM 不包括串行控制台端口，但某些消息（包括 **show perfmon** 和 perfmon 命令的输出）只显示在控制台端口上。使用 **show output-console** 命令可查看控制台缓冲区，其中包括 show perfmon 命令的输出。

Q. 在 FWSM 上使用 no monitor session servicemodule 命令是否会影响性能？

A. 由于用于数据流复制的 ASIC 硬件限制，因此需要在 FWSM 上使用 span 会话。FWSM 需要 ASIC 进行数据包复制，然后会利用 span 会话传递数据包。受该命令影响的数据流有分布式 EtherChannel、多播和 GRE。我们建议配置生成会话，而不要将其删除。

如果出于某种原因需要将其删除，请确保您没有复制原始数据流，例如分布式 EtherChannel；有关可能受到的影响，请参阅 Field Notice：FN - 61935 - Catalyst 6500 系列和 7600 系列服务模块与分布式 EtherChannel 和数据包再循环的互不兼容性。

Q. 能否通过增加内存存储更多访问控制列表 (ACL)？

A. FWSM 中分配给 ACL 的内存是有限的。有关 FWSM 资源分配的详细信息，请参阅规范 - 规则限制。

当为ACL分配的内存在上下文被超出时，您可以收到这些错误消息中的任一：

- `ERROR: access-list`
- `ERROR:`
-

某些访问列表使用的内存比其他访问列表多。这取决于访问列表的类型，系统可支持的实际限制低于最大值。规则和内存分配之间的映射不是一对一的映射。这实际上取决于规则及其在硬件中编程的方式。

以下两个选项可优化 ACE 内存使用率：

- 汇总并简化 ACE 条目 — 为此，可执行以下建议的步骤：请尽可能使用连续的主机地址。将 ACE/对象组中的主机语句聚合到网络中。请尽可能使用 any 代替网络，使用网络代替主机。尝试简化对象组。这样做可在 ACL 扩展时节省数百个 ACE。例如，将单个的端口语句分组到一个范围内。
- 对每个分区上分配给 ACE 的内存进行重新划分。这需要重新启动 FWSM 模块。FWSM 将分配给 ACE 的内存基本划分成 12 个分区，并为每个分区分配相应的内存。该过程是自动完成的。在 2.3(2) 及更高版本中，可以使用资源管理器根据所拥有的上下文数量重新分配内存。发出 **show context count** 命令可检查所拥有的上下文数量。然后可通过配置对其验证。然后找出使用 **show resource acl-partition** 命令的分区数量。如果您拥有的分区数量超过所定义的上下文

，则可以使用 **resource acl-partition number-of-partitions** 命令使分区数量与上下文数量相匹配。之后，您需要保存配置并重新启动 FWSM。上述命令可以为 ACE 分配更多的内存，而内存是否足够取决于向上下文中添加的 ACE。**警告：** 上述重新映射的缺点在于，如果要添加其他上下文，则必须再次重新分配内存映射。这将导致每个上下文获得的内存减少，从而违背当前的 ACE 定义。FWSM 上所分配的内存是有限的，它将以预定方式或如以上所述通过手动资源分配对其进行划分。

从版本4.0向前， FWSM介绍呼叫“为存储多ACL条目高效地利用内存资源的ACL优化的”功能。这处理在任何可能的情况下自动地聚集ACL条目，无需未命中所有一ACL条目效力的一种内置的算法。此算法一起加入用不同的ACL条目是指的连续子网到单个语句，并且检测在端口范围的交叠。此功能启用通过使用命令，在优化执行后，完整ACL配置查找与上一个(原始) ACL配置不同。此顺序的ACL配置可能在验证以后保留，并且优化可能禁用保存CPU计算超载。关于此功能的更多信息，参考与其配置细节一起描述ACL优化功能的访问列表组优化部分。

版本4.0也介绍呼叫“Increasaed访问列表产能的”另一个功能。使用此功能，用户当前有能力存储在单一上下文模式的130,000 ACL条目和150,000个条目在multicontext模式。关于此功能的更多信息，参考在Cisco防火墙服务模块软件版本4.0公告版的“增加的访问列表产能”部分。

Q. 为什么捕获命令应用于 FWSM 时会停止运行，且当接口上应用了其他捕获命令后无法捕获数据流？

A. 在已应用捕获“x”的同一接口上配置捕获“z”时，捕获“z”将会取代捕获“x”。最后一个连接到特定接口的捕获为活动捕获。

唯一的例外情况是当捕获“x”的访问列表与捕获“z”的访问列表相互重叠时。这种情况下，这两个捕获将继续捕获访问列表相互重叠的数据流。

Q. 如何能解决在FWSM的NPPCcmplx错误？

A. 重新加载FWSM模块为了解决此错误。

Q. 如何能配置FWSM使用TCP拦截防止SYN溢出特定类型？

A. 您能配置FWSM使用TCP拦截防止SYN溢出特定类型。参考的FWSM TCP拦截和欲知更多信息解释的SYN Cookie。

Q. 有没有处理IPv6数据包的任何性能问题？

A. 可以。您能看到性能问题，当发送IPv6流量，作为数据包时需要由CPU处理。由于在处理IPv4流量和IPv6流量的差异由CPU， IPv6数据包处理将导致与FWSM的某些性能问题。

Q. 如何可以防止FWSM应答到有其自己的MAC地址的遥远的服务器？

A. 您需要禁用在指定的接口的代理活动记录程序功能用此命令：

```
"sysopt noproxyarp <interface>"
```

关于代理活动记录程序功能的更多信息，参考FWSM命令参考指南。

Q. 如何可以通过FWSM防止呼叫丢弃？

A. 为了解决此问题、禁用检查H323的和H225 ：

```
policy-map global_policy
class inspection_default
no inspect h323 h225
no inspect h323 ras
```

Q. 如何能解决NAT在FWSM的转换问题？

A. 为了解决此问题，请使用xlate**旁路**命令。默认情况下， FWSM创建所有连接的NAT会话，即使您不使用NAT。您能未翻译的流量的禁用NAT会话，呼叫xlate旁路，为了避免最大数量NAT会话限制。**xlate旁路**命令可以配置如显示：

```
hostname(config)#xlate-bypass
```

参考配置Xlate旁路关于如何的更多信息对xlate旁路的配置。

相关信息

- **FWSM 基本配置示例**
- **防火墙服务模块文档**
- **防火墙服务模块产品支持页**
- **技术支持和文档 - Cisco Systems**