防火墙服务模块透明防火墙配置示例

目录

简介

通常，防火墙是一个路由跃点，充当连接到其屏蔽子网之一的主机的默认网关。另一方面，透明防火墙是第 2 层防火墙，作用类似于*线路插件* 或“隐藏防火墙”，并不视为到连接设备的路由器跃点。防火墙服务模块 (FWSM) 在其内部和外部接口上连接相同的网络。由于这种防火墙不是路由跃点，因此您可以很容易将透明防火墙引入到现有网络中。而无需重新分配 IP 地址。

由于没有复杂的路由模式进行故障排除，且无需配置 NAT，因此便于维护。

尽管可以使用透明模式充当网桥，但除非您使用扩展访问列表明确允许，否则第 3 层流量（例如 IP 流量）无法通过 FWSM。无需访问列表即允许通过透明防火墙的唯一流量是 ARP 流量。ARP 流量可以由 ARP 检查功能控制。

在路由模式下，即使在访问列表中允许，一些流量类型也不能穿过 FWSM。透明防火墙也可以使用

扩展访问列表（用于 IP 流量）或 Ethertype 访问列表（用于非 IP 流量）允许任何流量通过。

例如，可以通过透明防火墙建立路由协议邻接。您可以根据扩展访问列表，允许 VPN (IPSec)、OSPF、RIP、EIGRP 或者 BGP 流量通过。同样，HSRP 或 VRRP 等协议可以穿过 FWSM。

可以使用 Ethertype 访问列表，配置非 IP 流量（例如，AppleTalk、IPX、BPDU 和 MPLS）通过。

对于透明防火墙上没有直接支持的功能，您可以允许流量通过，以便上游路由器和下游路由器能够支持该功能。例如，可以使用扩展访问列表，允许 DHCP 流量（而非不受支持的 DHCP 中继功能）或多播流量（如 IP/TV 创建的流量）通过。

当 FWSM 运行在透明模式下时，数据包的出站接口将通过 MAC 地址查找确定，而非路由查找。您仍然可以配置路由语句，但它们仅适用于 FWSM 发出的数据流。例如，如果您的系统日志服务器位于远程网络，您必须使用静态路由，这样 FWSM 才能访问该子网。

此规则的例外是，当您使用语音检查并且端点距离 FWSM 至少一次跳跃时。例如，如果在 CCM 和 H.323 网关之间使用透明防火墙，并且在透明防火墙和 H.323 网关之间存在路由器，那么您需要在 FWSM 中添加 H.323 网关的静态路由才能成功完成呼叫。

注意： 透明模式 FWSM 不会传递 CDP 数据包，也不会传递不具有大于或等于 0x600 的有效 Ethertype 的任何数据包。例如，您不能传递 IS-IS 数据包。但 BPDU 例外，它是受支持的。

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 3.x 版的 FWSM。

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。

透明防火墙

网桥组

如果不想要安全上下文的开销，或者要最大限度使用安全上下文，则可以配置最多 8 个接口对，这些接口对称为网桥组。每个网桥组都连接到单独的网络。网桥组数据流与其他网桥组相互独立。数据流不会被路由到 FWSM 中的另一个网桥组，并且在外部路由器将数据流路由回 FWSM 中的另一个网桥组之前，数据流必须退出 FWSM。虽然每个网桥组都具有独立的桥接功能，但许多其他功能则是所有网桥组共有的。例如，所有网桥组共享系统日志服务器或 AAA 服务器配置。要完全隔离安全策略，请按照每个上下文对应一个网桥组的方式使用安全上下文。

由于这种防火墙不是路由跃点，因此您可以很容易将透明防火墙引入到现有网络中。而无需重新分配 IP 地址。由于没有复杂的路由模式进行故障排除，且无需配置 NAT，因此便于维护。

注意： 每个网桥组需要一个管理 IP 地址。FWSM 将使用此 IP 地址作为从该网桥组发出的数据包的源地址。管理 IP 地址与连接的网络必须位于相同的子网。

指南

规划透明防火墙网络时，请遵循以下指南：

- 每个网桥组都需要一个管理 IP 地址。在路由模式下，每个接口都需要一个 IP 地址，而与路由模式不同的是，透明防火墙为整个网桥组分配一个 IP 地址。FWSM 将使用此 IP 地址作为从该 FWSM 发出的数据包的源地址，例如系统消息或 AAA 通信数据包。管理 IP 地址与连接的网络必须位于相同的子网。您不能将该子网设置为主机子网 (255.255.255.255)。FWSM 不支持辅助网络上的数据流；仅支持与管理 IP 地址位于相同网络的数据流。有关管理 IP 子网的详细信息，请参阅为网桥组分配 IP 地址。
- 每个网桥组仅使用一个内部接口和一个外部接口。
- 每个直接连接的网络必须位于相同的子网。
- 请勿将网桥组管理 IP 地址指定为连接设备的默认网关。设备需要将位于 FWSM 另一端的路由器指定为默认网关。
- 透明防火墙的默认路由仅应用于来自网桥组网络的管理数据流，它是为管理数据流提供返回路径所必需的。这是因为默认路由在网桥组中指定了接口，同时在网桥组网络中指定了路由器 IP 地址，因此您只能定义一个默认路由。如果您具有来自多个网桥组网络的管理数据流，则需要指定静态路由以识别要接收管理数据流的网络。
- 对于多上下文模式，每个上下文必须使用不同的接口。您无法在上下文之间共享接口。
- 对于多上下文模式，每个上下文通常使用不同的子网。您可以使用重叠子网，但是从路由角度来看，网络拓扑需要具有路由器和 NAT 配置才能使之成为可能。您必须使用扩展访问列表来允许第 3 层流量（例如 IP 流量）通过 FWSM。此外，还可以选择性地使用 Ethertype 访问列表来允许非 IP 流量通过。

允许的 MAC 地址

以下目标 MAC 地址允许通过透明防火墙。不在此列表上的所有 MAC 地址将被丢弃。

- 等于 FFFF.FFFF.FFFF 的 TRUE 广播目标 MAC 地址
- 范围从 0100.5E00.0000 到 0100.5EFE.FFFF 的 IPv4 多播 MAC 地址
- 范围从 3333.0000.0000 到 3333.FFFF.FFFF 的 IPv6 多播 MAC 地址
- 等于 0100.0CCC.CCCD 的 BPDU 多播地址
- 范围从 0900.0700.0000 到 0900.07FF.FFFF 的 AppleTalk 组播 MAC 地址

不支持的功能

在透明模式下不支持以下功能：

- NAT/PATNAT 是在上游路由器上执行的。**注意：** FWSM版本3.2和以上版本的透明防火墙支持NAT/PAT。
- 动态路由协议（例如 RIP、EIGRP、OSPF）您可以对 FWSM 发出的数据流添加静态路由。您还可以使用扩展访问列表允许动态路由协议通过 FWSM。

- 用于网桥组 IP 地址的 IPv6。然而，您可以使用 EtherType 访问列表传递 IPv6 EtherType。
- DHCP 中继透明防火墙可以作为 DHCP 服务器，但它不支持 DHCP 中继命令。由于您可以使用扩展访问列表来允许 DHCP 流量通过，因此不需要 DHCP 中继。
- 服务质量 (QoS)
- 组播如果您在扩展访问列表中允许多播流量，则可允许其通过 FWSM。有关详细信息，请参阅穿过流量部分。
- 通过流量的 VPN 终止透明防火墙支持仅用于管理连接的站点到站点的 VPN 隧道。它不会终止通过 FWSM 的流量的 VPN 连接。您可以使用扩展访问列表允许 VPN 流量通过 FWSM，但它不会终止非管理连接。
- 交换机上的 LoopGuard如果 FWSM 处于透明模式下，请勿在交换机上启用全局 LoopGuard。LoopGuard 自动应用于交换机和 FWSM 之间的内部 EtherChannel，因此在故障切换和故障回复以后，LoopGuard 将导致辅助单元被断开，因为 EtherChannel 进入了 err-disable 状态。

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

网络图显示了一个典型的透明防火墙网络，其中外部设备与内部设备位于相同的子网。内部路由器和主机显示为直接连接到外部路由器。

配置

您可以设置要在路由防火墙模式（默认）或透明防火墙模式下运行的每种上下文。

当您更改模式时，FWSM 将清除配置，因为有很多命令不为这两种模式同时支持。如果您已预先填好了配置，请务必在更改模式之前备份此配置。在创建新配置时，可以使用此备份作为参考。

如果您将文本配置下载到 FWSM 中，并使用 firewall transparent 命令更改模式，请务必将此命令置于配置顶部。FWSM 将会在读取此命令时更改模式，然后继续读取您下载的配置。如果此命令不是位于配置顶部，则 FWSM 将清除位于此配置之前的所有配置行。

要将模式设置为透明，请在每种上下文中输入以下命令：

```
hostname(config)#firewall transparent
```

要将模式设置为路由，请在每种上下文中输入以下命令：

```
hostname(config)#no firewall transparent
```

数据在不同的情况下通过透明防火墙

内部用户访问外部电子邮件服务器

内部网络上的用户访问置于 Internet（外部）中的电子邮件服务器。FWSM 将会收到数据包，并将源 MAC 地址添加到 MAC 地址表中（如有需要）。由于它是新会话，因此会根据安全策略（访问列表、过滤器或 AAA）的条款来验证是否允许数据包。

注意： 对于多上下文模式，FWSM 将首先根据唯一的接口对数据包进行分类。

FWSM 会记录已建立的会话。如果目标 MAC 地址在其表中，FWSM 会将数据包转发到外部接口外面。目标 MAC 地址是上游路由器 192.168.1.2 的地址。如果目标 MAC 地址不在 FWSM 表中，FWSM 会在发送 ARP 请求和 ping 时尝试发现 MAC 地址。第一个数据包将被丢弃。

电子邮件服务器将响应请求。由于已建立会话，因此数据包将绕过与新连接相关联的许多查找。FWSM 会将数据包转发给内部用户。

内部的用户访问有NAT的电子邮件服务器

如果在 Internet 路由器中启用 NAT，则通过 Internet 路由器的数据包流会稍有变化。

内部网络上的用户访问置于 Internet（外部）中的电子邮件服务器。FWSM 将会收到数据包，并将源 MAC 地址添加到 MAC 地址表中（如有需要）。由于它是新会话，因此会根据安全策略（访问列表、过滤器或 AAA）的条款来验证是否允许数据包。

注意： 对于多上下文模式，FWSM 将首先根据唯一的接口对数据包进行分类。

Internet 路由器会将主机 A (192.168.1.5) 的实际地址转换为 Internet 路由器 (172.16.1.1) 的映射地址。由于映射地址与外部接口位于不同网络，请确保上游路由器具有到指向 FWSM 的映射网络的静态路由。

FWSM 将记录已建立的会话并转发来自外部接口的数据包。如果目标 MAC 地址在其表中，FWSM 会将数据包转发到外部接口外面。目标 MAC 地址是上游路由器 172.16.1.1 的地址。如果目标 MAC 地址不在 FWSM 表中，FWSM 会在发送 ARP 请求和 ping 时尝试发现 MAC 地址。第一个数据包将被丢弃。

电子邮件服务器将响应请求。由于已建立会话，因此数据包将绕过与新连接相关联的许多查找。在将映射地址转换为实际地址 192.168.1.5 时，FWSM 将执行 NAT。

内部用户访问内部 Web 服务器

如果主机A设法访问内部WEB服务器(10.1.1.1)，主机A (192.168.1.5)发送请求包到互联网路由器(因为它是默认网关)通过从里面的FWSM到外部。然后数据包重定向到Web服务器(10.1.1.1)通过FWSM (从外部对里面)和内部路由器。

注意： 只有当FWSM有允许一的访问列表流量从自里面的外面请求包回到Web服务器。

为了解决此问题，请将主机 A (10.1.1.1) 的默认网关更改为内部路由器 (192.168.1.3)，而不要使用 Internet 路由器 (192.168.1.2)。这样可避免将任何不必要的流量发送到外部网关，以及可重定向外部路由器（Internet 路由器）上出现的流量。它也会反向解析，亦即，当 Web 服务器或内部路由器中存在的任何主机 (10.1.1.0/24) 尝试访问主机 A (192.168.1.5) 时。

外部用户访问内部网络上的 Web 服务器

以下步骤描述了数据如何通过 FWSM：

1. 外部网络中的用户向内部 Web 服务器请求一个网页。FWSM 将会收到数据包，并将源 MAC 地址添加到 MAC 地址表中（如有需要）。由于它是新会话，因此会根据安全策略（访问列表、过滤器或 AAA）的条款来验证是否允许数据包。**注意：** 对于多上下文模式，FWSM 将首先

根据唯一的接口对数据包进行分类。
2. 仅当外部用户具有内部 Web 服务器的有效访问权限时，FWSM 才会记录已建立的会话。必须将访问列表配置为允许外部用户访问 Web 服务器。
3. 如果目标 MAC 地址在其表中，FWSM 会将数据包转发到内部接口外面。目标 MAC 地址是下游路由器 192.168.1.3 的地址。
4. 如果目标 MAC 地址不在 FWSM 表中，FWSM 会在发送 ARP 请求和 ping 时尝试发现 MAC 地址。第一个数据包将被丢弃。
5. Web 服务器将响应请求。由于已建立会话，因此数据包将绕过与新连接相关联的许多查找。FWSM 会将数据包转发给外部用户。

外部用户尝试访问内部主机

外部网络中的用户尝试访问内部主机。FWSM 将会收到数据包，并将源 MAC 地址添加到 MAC 地址表中（如有需要）。由于它是新会话，因此会根据安全策略（访问列表、过滤器或 AAA）的条款来验证是否允许数据包。

注意： 对于多上下文模式，FWSM 将首先根据唯一的接口对数据包进行分类。

由于外部用户不具有访问内部主机的权限，因此数据包将被拒绝，并且 FWSM 会丢弃数据包。如果外部用户试图攻击内部网络，FWSM 将采用多种技术来确定数据包对已建立的会话是否有效。

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。

```
cisco(config)#show firewall Firewall mode: Transparent
```

故障排除

穿过流量

在透明防火墙中，需要从高到低以及从低到高访问列表允许多播数据流通过。在普通防火墙中，则不需要从高到低允许其通过。

注意： 多播地址 (224.0.0.9) 不可能是回程数据流的源地址，因此它将无法返回，这也是为什么我们需要在 ACL 中允许其数据流双向通过的原因。

例如，为了允许 Rip 数据流通过，透明防火墙的访问列表应类似如下所示：

RIP

外部 ACL（从外到内）：

```
access-list outside permit udp host (outside source router) host 224.0.0.9 eq 520
access-group outside in interface outside
```

内部 ACL（从内到外）：

```
access-list inside permit udp host (inside source router) host 224.0.0.9 eq 520
access-group inside in interface inside
```

要运行的 EIGRP：

```
access-list inside permit eigrp host (inside source) host 224.0.0.10
 access-group inside in interface inside
access-list outside permit eigrp host (outside source) host 224.0.0.10
access-group outside in interface outside
```

对于 OSPF：

```
access-list inside permit ospf host ( inside source ) host 224.0.0.5
( this access-list is for hello packets )
access-list inside permit ospf host ( inside source ) host 224.0.0.6
( dr send update on this port )
access-list inside permit ospf host ( inside source ) host ( outside source )
access-group inside in interface inside
 access-list outside permit ospf host ( outside source ) host 224.0.0.5
access-list outside permit ospf host ( outside source ) host 224.0.0.6
access-list outside permit ospf host ( outside sourec ) host ( inside source )
access-group outside in interafce outside
```

MSFC VLAN 与 FWSM VLAN

在透明模式下，不必在 MSFC 接口和 FWSM 中具有相同 VLAN，因为它属于桥接类型。

相关信息

- Cisco PIX 防火墙软件
- 请求注解 (RFC)
- 安全产品 Field Notices（包括 PIX）
- Cisco Secure PIX 防火墙命令参考
- PIX/ASA：透明防火墙配置示例
- 技术支持和文档 - Cisco Systems