使用专用 VLAN 和 VLAN 访问控制列表保护网络安全

目录

简介

建立成功的网络安全设计的一个关键因素是确定和执行正确的信任模式。正确的信任模式定义了需要数据流的双方以及需要交换的数据流类型；所有其他数据流都应被拒绝。一旦确定正确的信任模式，安全设计人员便应决定如何执行此模式。由于更多的重要资源全球可用以及新的网络攻击形式的不断演变，网络安全基础设施势必变得更加复杂并有更多产品可用。防火墙、路由器、LAN 交换机、入侵检测系统、AAA 服务器和 VPN 是可帮助执行该模式的一些技术和产品。当然，其中的每个产品和技术都在整个安全实施中扮演特定的角色，设计人员必须了解如何部署这些元素。

开始使用前

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

先决条件

本文档介绍仅运行 CatOS 的交换机上的 PVLAN 配置。有关运行 Cisco IOS 和 CatOS 的交换机上 PVLAN 的并排配置示例，请参考文档在 Catalyst 交换机上配置隔离的专用 VLAN。

并非所有交换机和软件版本都支持 PVLAN。请参考专用 VLAN Catalyst 交换机支持表，以确定您

的平台和软件版本是否支持 PVLAN。

使用的组件

本文档不限于特定的软件和硬件版本。

背景信息

确定和执行正确的信任模式似乎是一项非常基本的任务，但在支持安全实施几年之后，我们的经验表明安全事件经常与糟糕的安全设计相关。通常，这些糟糕的设计都是未执行正确的信任模式的直接后果，有时候是因为对基本要素不理解，有时候只是因为对涉及的技术没有完全理解或进行了误用。

本文档详细说明我们的 Catalyst 交换机中的两个可用功能（专用 VLAN (PVLAN) 和 VLAN 访问控制列表 (VACL)）如何帮助确保在企业和服务提供商环境中都执行适当的信任模式。

执行正确的信任模式的重要性

未执行适当的信任模式的一个直接后果是整个安全实施对恶意活动的免疫力较低。隔离区 (DMZ) 通常在未执行正确策略（从而使潜在入侵者可以容易地执行其破坏活动）的情况下实施。本部分分析 DMZ 通常的实施方式以及糟糕的设计所带来的后果。我们稍后将说明如何减轻（最好是避免）这些后果。

通常，DMZ 服务器只应处理来自 Internet 的传入请求，并且最终发起到位于内部或其他 DMZ 分段的一些后端服务器（如数据库服务器）的连接。同时，DMZ 服务器之间不应互相通信，也不应发起到外界的任何连接。这清楚地定义了简单信任模式中的必要数据流；但是，我们经常看到未充分执行这种模式的情况。

设计人员通常倾向于使用所有服务器的公共分段实施 DMZ，而不对服务器之间的数据流进行任何控制。例如，所有服务器都位于一个公共 VLAN 中。由于没有对同一 VLAN 中的数据流进行任何控制，因此如果其中一个服务器被攻陷，那么同一服务器可能会被利用，作为源将攻击实施到同一分段中的任何服务器和主机。这显然便于潜在入侵者实施端口重定向或应用程序层攻击。

通常，防火墙和数据包过滤器只用来控制传入连接，但通常不执行任何操作来限制源于 DMZ 的连接。以前在 cgi-bin 脚本中有一个众所周知的漏洞，允许入侵者通过只发送 HTTP 流便开始 X-term 会话；这是防火墙应该允许的数据流。如果入侵者足够幸运，那么他或她可以使用另一种欺骗的手段（通常是某种类型的缓冲区溢出攻击）来获得 root 提示符。多数情况下，这类问题可以通过执行正确的信任模式来避免。首先，服务器之间不应相互通信，其次，不应从这些服务器向外界发起连接。

同样的注释适用于其他许多情况，从任何常规的不受信任分段到应用程序服务提供商处的服务器群。

Catalyst 交换机上的 PVLAN 和 VACL 可帮助确保正确的信任模式。PVLAN 将通过限制公共分段中主机之间的数据流提供帮助，而 VACL 通过对源自或去往某个特定分段的任何数据流提供进一步的控制来提供帮助。这些功能将在以下部分中讨论。

专用 VLAN

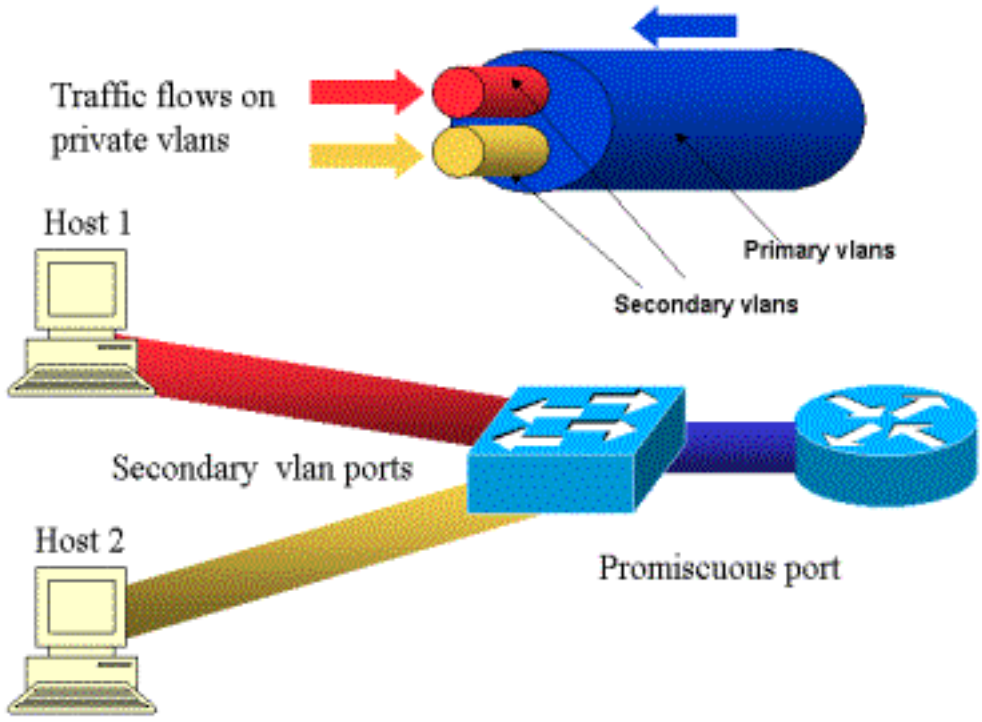
PVLAN 在运行 CatOS 5.4 或更高版本的 Catalyst 6000 以及运行 CatOS 6.2 或更高版本的 Catalyst

4000、2980G、2980G-A、2948G 和 4912G 上可用。

从我们的角度来说，PVLAN是准许分离第二层（L2）数据流、并把广播分段变成非广播多通道分段的一个工具。从混合端口（即，主 VLAN 和辅助 VLAN 均可以转发的端口）传入交换机的数据流可以在属于同一主 VLAN 的所有端口上传出。从映射到辅助 VLAN（可以是隔离 VLAN、社区 VLAN 或双向社区 VLAN）的端口进入交换机的数据流可以转发到混合端口或属于同一社区 VLAN 的端口。映射到同一隔离 VLAN 的多个端口不能交换任何数据流。

下图显示了此概念。

图 1：专用 VLAN



主 VLAN 用蓝色表示；辅助 VLAN 用红色和黄色表示。主机-1 连接到属于红色辅助 VLAN 的交换机端口。Host-2 连接到属于黄色辅助 VLAN 的交换机端口。

当主机进行传输时，数据流被传输到辅助 VLAN 中。例如，当 Host-2 传输时，其数据流流向黄色 VLAN。当这些主机进行接收时，数据流来自蓝色 VLAN，即主 VLAN。

连接路由器和防火墙的端口是混合端口，因为这些端口可以转发来自在映射中定义的每个辅助 VLAN 以及主 VLAN 的数据流。连接到每个主机的端口只能转发来自主 VLAN 和该端口上配置的辅助 VLAN 的数据流。

图中将用专用 VLAN 表示为连接路由器和主机的不同管道：将所有其他对象捆绑在一起的管道是主 VLAN（蓝色），蓝色 VLAN 上的数据流从路由器流向主机。主 VLAN 内部的管道是辅助 VLAN，这些管道上传输的数据流从主机流向路由器。

如图所示，主 VLAN 可以捆绑一个或更多辅助 VLAN。

在本文档前面的部分中说过，PVLAN 可以通过在公共分段内确保主机的隔离来帮助执行正确的信任模式。既然我们对专用 VLAN 有了更多了解，让我们来看看如何在我们最初的 DMZ 方案中实施此方案。服务器之间不应相互通信，但是它们仍然需要与它们连接的防火墙或路由器通信。在这种情

况下，服务器应连接到隔离端口，而路由器和防火墙应连接到混合端口。这样，如果其中一个服务器被攻陷，入侵者将不能使用同一服务器作为源将攻击实施到同一分段中的其他服务器。交换机将以线速丢弃任何数据包，而不会对性能产生任何影响。

另一个重要的注意事项是，这种控制只能在第 2 层设备上实施，因为所有服务器都属于同一子网。由于服务器将尝试直接通信，因此防火墙或路由器无法执行任何操作。另一种选择是每个服务器专用一个防火墙端口，但这可能成本太高，很难实现，而且无法扩展。

在后面的部分中，我们将详细介绍可以使用此功能的一些其他典型方案。

VLAN 访问控制列表

VACL 在运行 CatOS 5.3 或更高版本的 Catalyst 6000 系列上可用。

VACL 可以配置在 Catalyst 6500 上的第 2 层（不需要路由器，只需要 Policy Feature Card (PFC)）。它们以线速执行，因此在 Catalyst 6500 上配置 VACL 没有性能影响。由于 VACL 的查找在硬件中执行，因此不管访问列表有多大，转发速率都保持不变。

可以将 VACL 分别映射到主 VLAN 或辅助 VLAN。通过在辅助 VLAN 上配置 VACL，可以在不触及路由器或防火墙生成的数据流的情况下过滤源自主机的数据流。

通过将 VACL 与专用 VLAN 结合，可以根据数据流自身的方向过滤数据流。例如，如果两个路由器连接到与一些主机（例如服务器）相同的分段，可以将 VACL 配置在辅助 VLAN 上，以便只过滤由这些主机生成的数据流，而不触及路由器之间交换的数据流。

可以轻松部署 VACL 来执行正确的信任模式。让我们来分析我们的 DMZ 案例。DMZ 中的服务器应只为传入连接提供服务，它们不应发起与外界的连接。VACL 可以应用到其辅助 VLAN 中，以控制离开这些服务器的数据流。请务必注意，在使用 VACL 时，数据流在硬件中被丢弃，因此不会对路由器或交换机的 CPU 产生影响。即使其中一个服务器作为源被卷入分布式拒绝服务 (DDoS) 攻击，交换机将以线速丢弃所有非法数据流，而不会对性能产生任何负面影响。可以将类似的过滤器应用到服务器连接到的路由器或防火墙中，但这通常对性能有较大影响。

基于 MAC 的 ACL 无法很好地处理 IP 数据流，因此建议使用 VACL 监视/跟踪 PVLAN。

VACL 和 PVLAN 的已知限制

当使用 VACL 配置过滤时，对于 PFC 上的分段处理，应十分小心地进行配置，该配置将根据硬件的规格进行调整。

如果是 Catalyst 6500 的 Supervisor 1 的 PFC 的硬件设计，最好明确地拒绝 icmp 分段。原因是硬件认为 Internet 控制消息协议 (ICMP) 分段和回声应答相同，并且在默认情况下，硬件被编程为明确允许分段。因此，如果希望阻止回声应答数据包离开服务器，必须使用 **deny icmp any any fragment** 一行进行明确配置。本文档中的配置考虑到了这种情况。

PVLAN 有一个众所周知的安全限制，即路由器可能将数据流转发回数据流来自的同一子网。路由器可以在隔离的端口之间路由数据流，从而使 PVLAN 的目的无法实现。此限制是由于 PVLAN 是一种在第 2 层（而不是在第 3 层 (L3)）提供隔离的工具。

单播逆向路径转发 (URPF) 在 PVLAN 主机端口上无法正常工作，因此不能将 uRPF 与 PVLAN 结合使用。

此问题有一个解决方法，可通过在主 VLAN 上配置的 VACL 实现。此案例分析提供了一些 VACL，这些 VACL 需要在主 VLAN 上配置进行配置，以丢弃源自同一子网并路由回同一子网的数据流。

在一些板卡上，PVLAN 映射/中继端口的配置受到一些限制，其中多个 PVLAN 映射必须属于不同的端口专用集成电路 (ASIC) 才能进行配置。这些限制在新端口 ASIC Coil3 上已被去除。有关详细信息，请参考有关软件配置的最新 Catalyst 交换机文档。

示例分析

以下部分介绍三个案例分析，我们认为它们代表了大多数实施并提供了 PVLAN 和 VACL 安全部署的相关详细信息。

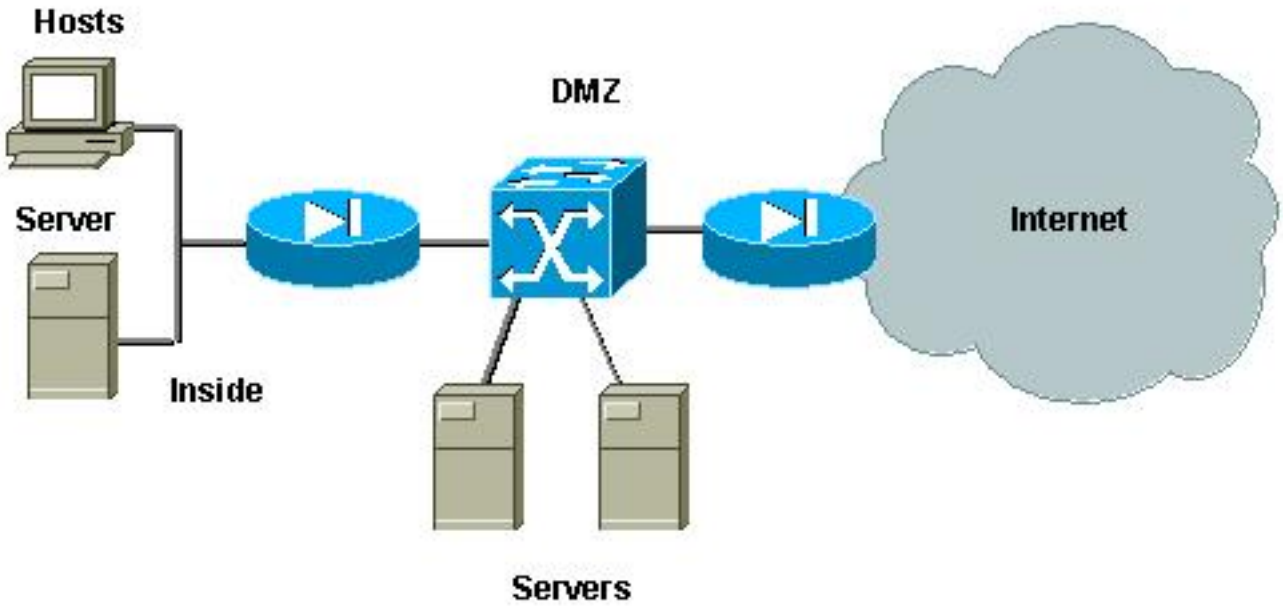
这些方案是：

- Pass-Through DMZ
- 外部 DMZ
- 与防火墙并行的 VPN 集中器

Pass-Through DMZ

这是最常部署的方案之一。在本示例中，DMZ 是作为两个防火墙路由器之间的中转区域实施的（如下图中所示）。

图 2：Pass-Through DMZ



在本示例中，DMZ 服务器应可由外部和内部用户访问，但它们之间不需要相互通信。在某些情况下，DMZ 服务器需要打开与内部主机的某种类型的连接。同时，内部客户端应可以不受限制地访问 Internet。一个好的实例是在DMZ的网络服务器需要与位于内部网络的数据库服务器通信，并使内部客户端访问互联网。

外部防火墙配置为允许到位于 DMZ 的服务器的传入连接，但是，通常未对传出数据流（特别是对

源自 DMZ 的数据流）应用任何过滤器或限制。如我们在本文档前面部分所讨论，这可能潜在地方便了攻击者的活动，原因有以下两个：第一个，当其中一台 DMZ 主机被攻陷时，其他所有 DMZ 主机将立即暴露；第二个，攻击者可以轻松利用传出连接。

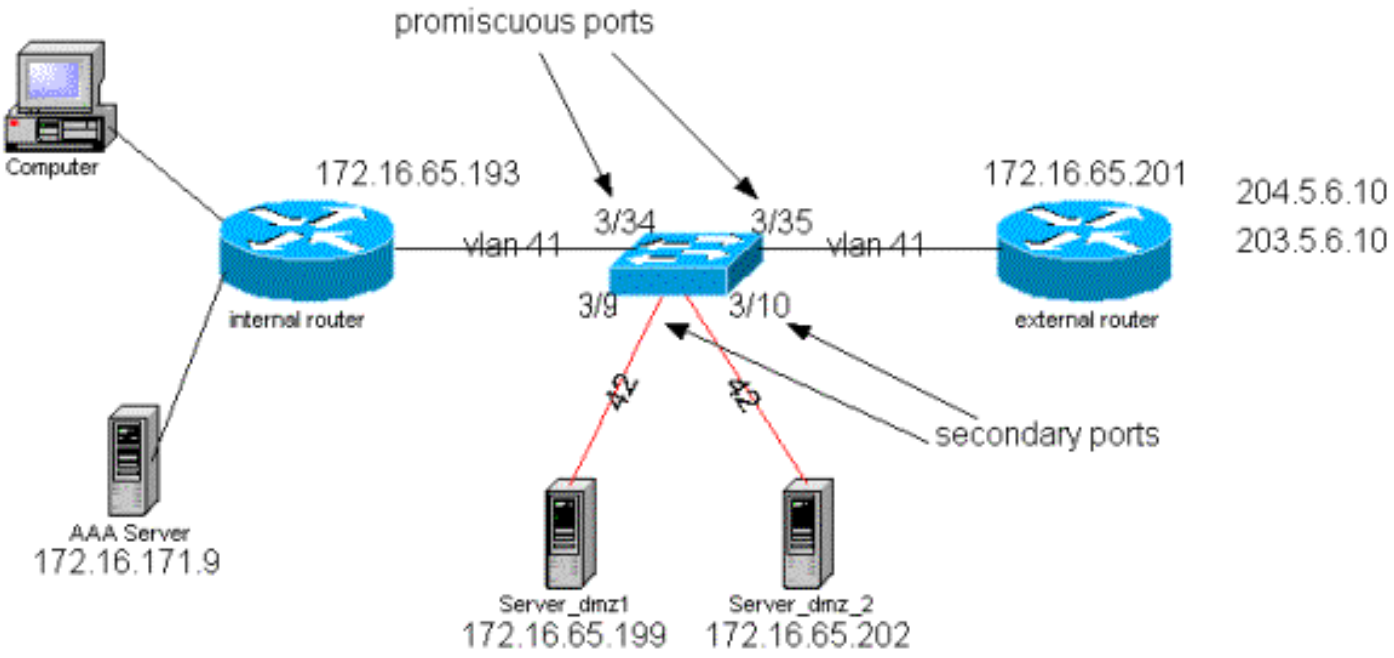
由于 DMZ 服务器之间不需要相互通信，因此建议确保将它们在第 2 层相互隔离。服务器端口将被定义为 PVLAN 隔离端口，而连接到两个防火墙的端口将被定义为混合端口。可以通过为防火墙定义主 VLAN 并为 DMZ 服务器定义辅助 VLAN 来实现此目的。

VACL 将用于控制源自 DMZ 的数据流。这将防止攻击者打开非法的传出连接。需要记住的是，DMZ 服务器不仅需要使用与客户端会话对应的数据流进行回复，还需要一些其他服务，如域名系统 (DNS) 和最大传输单元 (MTU) 路径发现。因此，ACL 应该允许 DMZ 服务器需要的所有服务。

测试 Pass-Through DMZ

在我们的试验床上，我们实施一个DMZ分段，将2个路由器配置为床服务器，分别为server_dmz1和server_dmz。这些服务器应该可由外部和内部客户端访问，并且所有 HTTP 连接都使用内部 RADIUS 服务器 (CiscoSecure ACS for UNIX) 进行验证。内部和外部路由器都被配置为数据包过滤器防火墙。下图说明试验床，包括使用的编址方案。

图 3：Pass-Through DMZ 试验床



以下列表收集了 PVLAN 的基本配置步骤。Catalyst 6500 被用作 DMZ 中的第 2 层交换机。

- Server_dmz_1 被连接到端口 3/9
- Server_dmz_2 被连接到端口 3/10
- 内部路由器被连接到端口 3/34
- 外部路由器被连接到端口 3/35

我们选择了以下 VLAN：

- 41 是主 VLAN
- 42 是隔离 VLAN

专用 VLAN 配置

以下配置在涉及的端口上设置 PVLAN。

```
ecomm-6500-2 (enable) set vlan 41 pvlan primary
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 41 configuration successful

ecomm-6500-2 (enable) sh pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
41      -         -
ecomm-6500-2 (enable) set vlan 42 pvlan isolated
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 42 configuration successful
ecomm-6500-2 (enable) set pvlan 41 42 3/9-10
Successfully set the following ports to Private Vlan 41,42:
3/9-10

ecomm-6500-2 (enable) set pvlan mapping 41 42 3/35
Successfully set mapping between 41 and 42 on 3/35
ecomm-6500-2 (enable) set pvlan mapping 41 42 3/34
Successfully set mapping between 41 and 42 on 3/34

Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/9  server_dmz1        connected  41,42      a-half  a-10 10/100BaseTX
 3/10 server_dmz2        connected  41,42      a-half  a-10 10/100BaseTX

 3/34 to_6500_1          connected   41        auto  auto 10/100BaseTX
 3/35 external_router_dm connected  41        a-half  a-10 10/100BaseTX
```

主 VLAN 上的 VACL 配置

本部分对于提升 DMZ 上的安全性至关重要。如 VACL 和 PVLAN 的已知限制部分中所述，即使服务器属于两个不同的辅助 VLAN 或属于同一个隔离 VLAN，攻击者仍有方法使它们相互通信。如果服务器尝试直接通信，它们将由于 PVLAN 而无法在第 2 层上直接通信。如果入侵者攻陷这些服务器，并且然后将这些服务器配置为将同一子网的数据流发送到路由器，该路由器会将数据流路由回同一子网，从而使 PVLAN 的目的无法实现。

因此，需要使用以下策略在主 VLAN（传输来自路由器的数据流的 VLAN）上配置 VACL：

- 允许源 IP 为路由器 IP 的数据流
- 拒绝源和目标 IP 都属于该 DMZ 子网的数据流
- 允许所有其余数据流ecomm-6500-2 (enable) **sh sec acl info protect_pvlan**
  set security acl ip protect_pvlan
  ----
  1. permit ip host 172.16.65.193 any
  2. permit ip host 172.16.65.201 any
  3. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
  4. permit ip any any

  ecomm-6500-2 (enable) **sh sec acl**
  ACL   Type VLANS
  ---------- ---- -----
  protect_pvlan   IP   41

此 ACL 不会影响由服务器生成的数据流；它将只防止路由器路由来自服务器的数据流回到同一个 VLAN。前两个语句允许路由器将 icmp 重定向或 icmp 不可到达等消息发送给服务器。

辅助 VLAN 上的 VACL 配置

以下配置日志用于显示如何设置 VACL 以过滤由服务器生成的数据流。我们希望通过配置此 VACL 实现以下目的：

- 允许从服务器 ping（允许回声）
- 防止 echo replies 从服务器上发出
- 允许源自外部的 HTTP 连接
- 允许 RADIUS 验证（UDP 端口 1645）和记账（UDP 端口 1646）数据流
- 允许 DNS 数据流（UDP 端口 53）

我们希望阻止所有其余数据流。

就分段而言，我们在服务器分段上作如下假设：

- 服务器不会生成分段的数据流
- 服务器可能收到分段的数据流

如果是 Catalyst 6500 的 Supervisor 1 的 PFC 硬件设计，最好明确拒绝 icmp 分段。原因是硬件认为 ICMP 分段和回声应答相同，且硬件在默认情况下被编程为明确允许分段。因此，如果希望阻止回声应答数据包离开服务器，您必须使用 deny icmp any any fragment 一行进行明确配置。

```
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out deny icmp any any fragment
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit icmp host 172.16.65.199 any echo
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit icmp host 172.16.65.202 any echo
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit tcp host 172.16.65.199 eq 80 any
established
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit tcp host 172.16.65.202 eq 80 any
established
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.199
eq 1645 host 172.16.171.9 eq 1645
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.202
eq 1645 host 172.16.171.9 eq 1645
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.199
eq 1646 host 172.16.171.9 eq 1646
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.202
eq 1646 host 172.16.171.9 eq 1646
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.199 any eq 53
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.202 any eq 53

ecomm-6500-2 (enable) Commit sec acl all

ecomm-6500-2 (enable) Set sec acl map dmz_servers_out 42

ecomm-6500-2 (enable) sh sec acl
ACL                              Type VLANS
-------------------------------  ---- -----
protect_pvlan                    IP   41
dmz_servers_out                  IP   42

ecomm-6500-2 (enable) sh sec acl info dmz_servers_out
set security acl ip dmz_servers_out
---------------------------------------------------
1. deny icmp any any fragment
2. permit icmp host 172.16.65.199 any echo
3. permit icmp host 172.16.65.202 any echo
4. permit tcp host 172.16.65.199 eq 80 any established
5. permit tcp host 172.16.65.202 eq 80 any established
6. permit udp host 172.16.65.199 eq 1645 host 172.16.171.9 eq 1645
7. permit udp host 172.16.65.202 eq 1645 host 172.16.171.9 eq 1645
```

```
8. permit udp host 172.16.65.199 eq 1646 host 172.16.171.9 eq 1646
9. permit udp host 172.16.65.202 eq 1646 host 172.16.171.9 eq 1646
10. permit udp host 172.16.65.199 any eq 53
11. permit udp host 172.16.65.202 any eq 53
```

测试配置

在已经配置 PVLAN 但尚未应用 VACL 时，将捕获到以下输出。此试验显示，用户可以从外部路由器 ping 内部路由器和服务器。

```
external_router#ping 172.16.65.193
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.193, timeout is 2 seconds:
!!!!

external_router#ping 172.16.65.202
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.202, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
external_router#ping 172.16.65.199
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.199, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

以下示例显示，我们可以从服务器 ping 到外部网络和默认网关，但不能 ping 到属于同一辅助 VLAN 的服务器。

```
server_dmz1#ping 203.5.6.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.5.6.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.193, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

server_dmz1#ping 172.16.65.202
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.202, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

在映射 VACL 后，来自外部路由器的 ping 将再也不能成功：

```
external_router#ping 172.16.65.199
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.199, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

以下示例显示收到来自内部网络的 HTTP GET 请求的服务器：

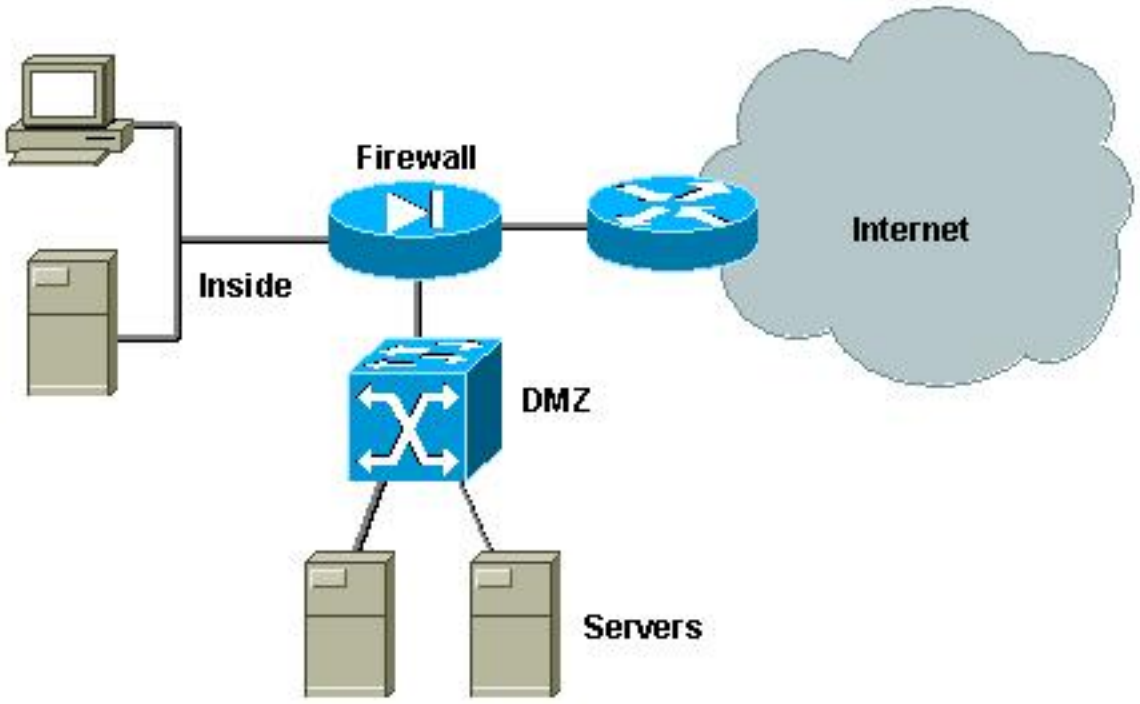
```
server_dmz1#debug ip http url
HTTP URL debugging is on
server_dmz1#debug ip hhtp tran
HTTP transactions debugging is on
server_dmz1#debug ip http auth
HTTP Authentication debugging is on
server_dmz1#
```

```
*Mar  7 09:24:03.092 PST: HTTP: parsed uri '/'
*Mar  7 09:24:03.092 PST: HTTP: client version 1.0
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Connection
*Mar  7 09:24:03.092 PST: HTTP: parsed line  Keep-Alive
*Mar  7 09:24:03.092 PST: HTTP: parsed extension User-Agent
*Mar  7 09:24:03.092 PST: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Host
*Mar  7 09:24:03.092 PST: HTTP: parsed line  172.16.65.199
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept
*Mar  7 09:24:03.092 PST: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept-Encoding
*Mar  7 09:24:03.092 PST: HTTP: parsed line  gzip
*Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Language
*Mar  7 09:24:03.096 PST: HTTP: parsed line  en
*Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Charset
*Mar  7 09:24:03.096 PST: HTTP: parsed line  iso-8859-1,*,utf-8
*Mar  7 09:24:03.096 PST: HTTP: Authentication for url '/' '/' level 15  privless '/'
*Mar  7 09:24:03.096 PST: HTTP: authentication required, no authentication information was
provided
*Mar  7 09:24:03.096 PST: HTTP: authorization rejected
*Mar  7 09:24:22.528 PST: HTTP: parsed uri '/'
*Mar  7 09:24:22.532 PST: HTTP: client version 1.0
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Connection
*Mar  7 09:24:22.532 PST: HTTP: parsed line  Keep-Alive
*Mar  7 09:24:22.532 PST: HTTP: parsed extension User-Agent
*Mar  7 09:24:22.532 PST: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Host
*Mar  7 09:24:22.532 PST: HTTP: parsed line  172.16.65.199
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept
*Mar  7 09:24:22.532 PST: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Encoding
*Mar  7 09:24:22.532 PST: HTTP: parsed line  gzip
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Language
*Mar  7 09:24:22.532 PST: HTTP: parsed line  en
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Charset
*Mar  7 09:24:22.532 PST: HTTP: parsed line  iso-8859-1,*,utf-8
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Authorization
*Mar  7 09:24:22.532 PST: HTTP: parsed authorization type Basic
*Mar  7 09:24:22.532 PST: HTTP: Authentication for url '/' '/' level 15  privless '/'
*Mar  7 09:24:22.532 PST: HTTP: Authentication username = 'martin' priv-level = 15 auth-type =
aaa
*Mar  7 09:24:22.904 PST: HTTP: received GET ''
```

外部 DMZ

外部 DMZ 方案可能是最被认可和最广泛部署的实施。外部 DMZ 是通过使用防火墙的一个或多个接口实施的，如下图所示。

图 4：外部 DMZ



通常，不管设计实施如何，DMZ 的要求往往是相同的。与以前的案例中一样，DMZ 服务器应该可以从外部客户端和内部网络访问。DMZ 服务器最终将需要访问一些内部资源，并且它们之间不应相互通信。同时，不应从 DMZ 发起到 Internet 的任何数据流；这些 DMZ 服务器只应使用与传入连接对应的数据流进行回复。

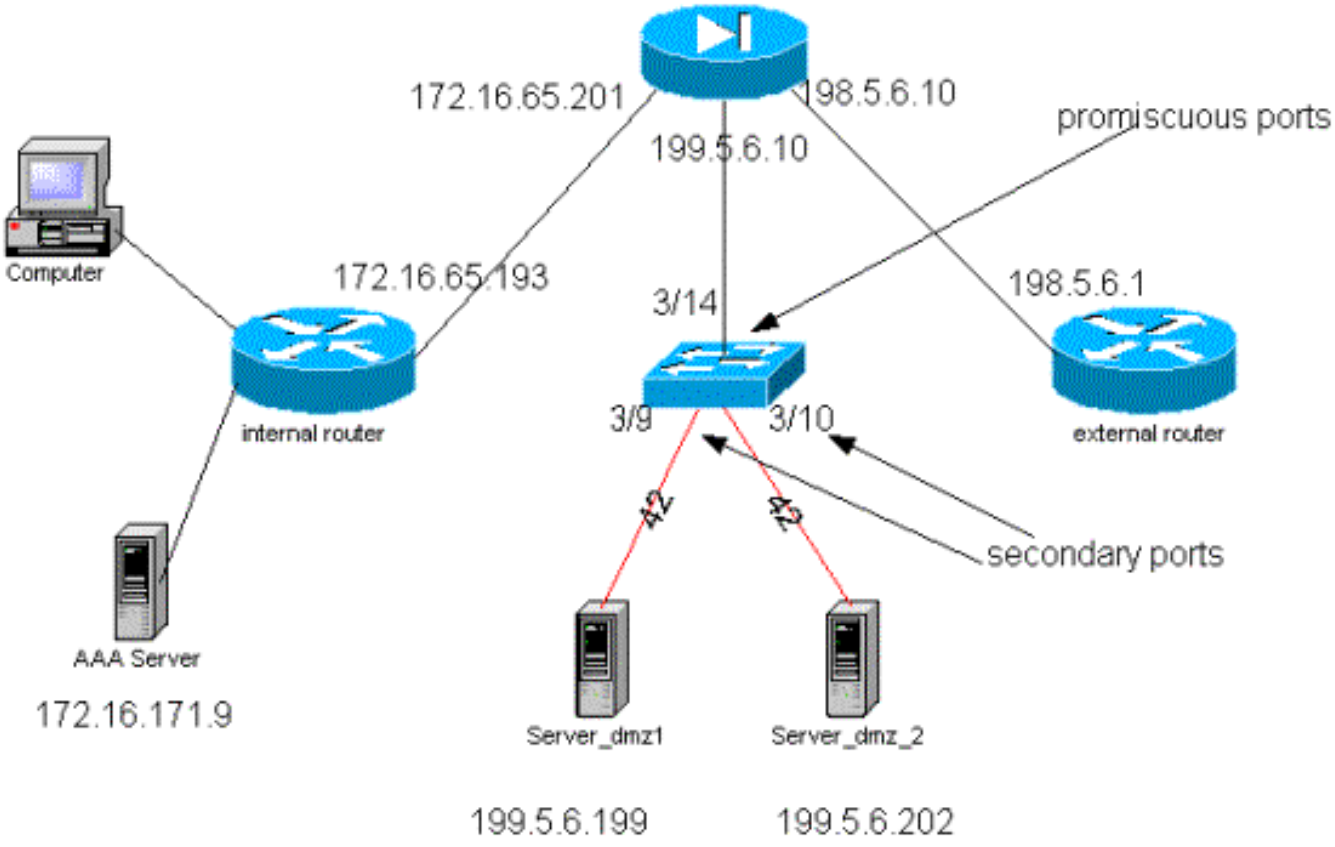
与前一个案例分析中一样，第一个配置步骤包括通过 PVLAN 在第 2 层实现隔离，并且确保 DMZ 服务器之间不能相互通信，而内部和外部主机可以访问它们。这是通过在具有隔离端口的辅助 VLAN 中设置服务器实施的。防火墙应在具有混合端口的主 VLAN 中定义。防火墙将是此主 VLAN 内的唯一设备。

第二步是定义 ACL 以控制源自 DMZ 的数据流。在定义这些 ACL 时，我们需要确保只允许必要的数据流。

测试外部 DMZ

下图显示此案例分析中使用的试验床，在这个案例中，我们使用了带第三个接口的PIX防火墙 DMZ。使用同一组路由器作为 Web 服务器，并且所有 HTTP 会话都使用同一个 RADIUS 服务器进行验证。

图 5：外部 DMZ 试验床



由于前一案例分析中已对 PVLAN 和 VACL 配置进行了详细说明，在此方案中我们只从配置文件中选取了更引人注意的部分。

PIX 配置

```
server_dmz1#debug ip http url
HTTP URL debugging is on
server_dmz1#debug ip hhtp tran
HTTP transactions debugging is on
server_dmz1#debug ip http auth
HTTP Authentication debugging is on
server_dmz1#
*Mar  7 09:24:03.092 PST: HTTP: parsed uri '/'
*Mar  7 09:24:03.092 PST: HTTP: client version 1.0
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Connection
*Mar  7 09:24:03.092 PST: HTTP: parsed line  Keep-Alive
*Mar  7 09:24:03.092 PST: HTTP: parsed extension User-Agent
*Mar  7 09:24:03.092 PST: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Host
*Mar  7 09:24:03.092 PST: HTTP: parsed line  172.16.65.199
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept
*Mar  7 09:24:03.092 PST: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept-Encoding
*Mar  7 09:24:03.092 PST: HTTP: parsed line  gzip
*Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Language
*Mar  7 09:24:03.096 PST: HTTP: parsed line  en
*Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Charset
*Mar  7 09:24:03.096 PST: HTTP: parsed line  iso-8859-1,*,utf-8
*Mar  7 09:24:03.096 PST: HTTP: Authentication for url '/' '/' level 15  privless '/'
*Mar  7 09:24:03.096 PST: HTTP: authentication required, no authentication information was
provided
*Mar  7 09:24:03.096 PST: HTTP: authorization rejected
*Mar  7 09:24:22.528 PST: HTTP: parsed uri '/'
*Mar  7 09:24:22.532 PST: HTTP: client version 1.0
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Connection
```

```
*Mar  7 09:24:22.532 PST: HTTP: parsed line  Keep-Alive
*Mar  7 09:24:22.532 PST: HTTP: parsed extension User-Agent
*Mar  7 09:24:22.532 PST: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Host
*Mar  7 09:24:22.532 PST: HTTP: parsed line  172.16.65.199
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept
*Mar  7 09:24:22.532 PST: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Encoding
*Mar  7 09:24:22.532 PST: HTTP: parsed line  gzip
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Language
*Mar  7 09:24:22.532 PST: HTTP: parsed line  en
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Charset
*Mar  7 09:24:22.532 PST: HTTP: parsed line  iso-8859-1,*,utf-8
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Authorization
*Mar  7 09:24:22.532 PST: HTTP: parsed authorization type Basic
*Mar  7 09:24:22.532 PST: HTTP: Authentication for url '/' '/' level 15  privless '/'
*Mar  7 09:24:22.532 PST: HTTP: Authentication username = 'martin' priv-level = 15 auth-type =
aaa
*Mar  7 09:24:22.904 PST: HTTP: received GET ''
```

RADIUS 配置

NAS 配置

```
server_dmz1#debug ip http url
HTTP URL debugging is on
server_dmz1#debug ip hhtp tran
HTTP transactions debugging is on
server_dmz1#debug ip http auth
HTTP Authentication debugging is on
server_dmz1#
*Mar  7 09:24:03.092 PST: HTTP: parsed uri '/'
*Mar  7 09:24:03.092 PST: HTTP: client version 1.0
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Connection
*Mar  7 09:24:03.092 PST: HTTP: parsed line  Keep-Alive
*Mar  7 09:24:03.092 PST: HTTP: parsed extension User-Agent
*Mar  7 09:24:03.092 PST: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Host
*Mar  7 09:24:03.092 PST: HTTP: parsed line  172.16.65.199
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept
*Mar  7 09:24:03.092 PST: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept-Encoding
*Mar  7 09:24:03.092 PST: HTTP: parsed line  gzip
*Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Language
*Mar  7 09:24:03.096 PST: HTTP: parsed line  en
*Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Charset
*Mar  7 09:24:03.096 PST: HTTP: parsed line  iso-8859-1,*,utf-8
*Mar  7 09:24:03.096 PST: HTTP: Authentication for url '/' '/' level 15  privless '/'
*Mar  7 09:24:03.096 PST: HTTP: authentication required, no authentication information was
provided
*Mar  7 09:24:03.096 PST: HTTP: authorization rejected
*Mar  7 09:24:22.528 PST: HTTP: parsed uri '/'
*Mar  7 09:24:22.532 PST: HTTP: client version 1.0
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Connection
*Mar  7 09:24:22.532 PST: HTTP: parsed line  Keep-Alive
*Mar  7 09:24:22.532 PST: HTTP: parsed extension User-Agent
*Mar  7 09:24:22.532 PST: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Host
*Mar  7 09:24:22.532 PST: HTTP: parsed line  172.16.65.199
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept
*Mar  7 09:24:22.532 PST: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Encoding
*Mar  7 09:24:22.532 PST: HTTP: parsed line  gzip
```

```
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Language
*Mar  7 09:24:22.532 PST: HTTP: parsed line  en
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Charset
*Mar  7 09:24:22.532 PST: HTTP: parsed line  iso-8859-1,*,utf-8
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Authorization
*Mar  7 09:24:22.532 PST: HTTP: parsed authorization type Basic
*Mar  7 09:24:22.532 PST: HTTP: Authentication for url '/' '/' level 15  privless '/'
*Mar  7 09:24:22.532 PST: HTTP: Authentication username = 'martin' priv-level = 15 auth-type =
aaa
*Mar  7 09:24:22.904 PST: HTTP: received GET ''
```

RADIUS 服务器 CSUX

```
server_dmz1#debug ip http url
HTTP URL debugging is on
server_dmz1#debug ip hhtp tran
HTTP transactions debugging is on
server_dmz1#debug ip http auth
HTTP Authentication debugging is on
server_dmz1#
*Mar  7 09:24:03.092 PST: HTTP: parsed uri '/'
*Mar  7 09:24:03.092 PST: HTTP: client version 1.0
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Connection
*Mar  7 09:24:03.092 PST: HTTP: parsed line  Keep-Alive
*Mar  7 09:24:03.092 PST: HTTP: parsed extension User-Agent
*Mar  7 09:24:03.092 PST: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Host
*Mar  7 09:24:03.092 PST: HTTP: parsed line  172.16.65.199
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept
*Mar  7 09:24:03.092 PST: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept-Encoding
*Mar  7 09:24:03.092 PST: HTTP: parsed line  gzip
*Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Language
*Mar  7 09:24:03.096 PST: HTTP: parsed line  en
*Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Charset
*Mar  7 09:24:03.096 PST: HTTP: parsed line  iso-8859-1,*,utf-8
*Mar  7 09:24:03.096 PST: HTTP: Authentication for url '/' '/' level 15  privless '/'
*Mar  7 09:24:03.096 PST: HTTP: authentication required, no authentication information was
provided
*Mar  7 09:24:03.096 PST: HTTP: authorization rejected
*Mar  7 09:24:22.528 PST: HTTP: parsed uri '/'
*Mar  7 09:24:22.532 PST: HTTP: client version 1.0
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Connection
*Mar  7 09:24:22.532 PST: HTTP: parsed line  Keep-Alive
*Mar  7 09:24:22.532 PST: HTTP: parsed extension User-Agent
*Mar  7 09:24:22.532 PST: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Host
*Mar  7 09:24:22.532 PST: HTTP: parsed line  172.16.65.199
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept
*Mar  7 09:24:22.532 PST: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Encoding
*Mar  7 09:24:22.532 PST: HTTP: parsed line  gzip
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Language
*Mar  7 09:24:22.532 PST: HTTP: parsed line  en
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Charset
*Mar  7 09:24:22.532 PST: HTTP: parsed line  iso-8859-1,*,utf-8
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Authorization
*Mar  7 09:24:22.532 PST: HTTP: parsed authorization type Basic
*Mar  7 09:24:22.532 PST: HTTP: Authentication for url '/' '/' level 15  privless '/'
*Mar  7 09:24:22.532 PST: HTTP: Authentication username = 'martin' priv-level = 15 auth-type =
aaa
*Mar  7 09:24:22.904 PST: HTTP: received GET ''
```

Catalyst 配置

应该注意在此配置中，不需要在主VLAN上配置VACL，因为PIX不重定向来自同一接口的数据流。如主 VLAN 上的 VACL 配置部分中所述的 VACL 将是多余的。

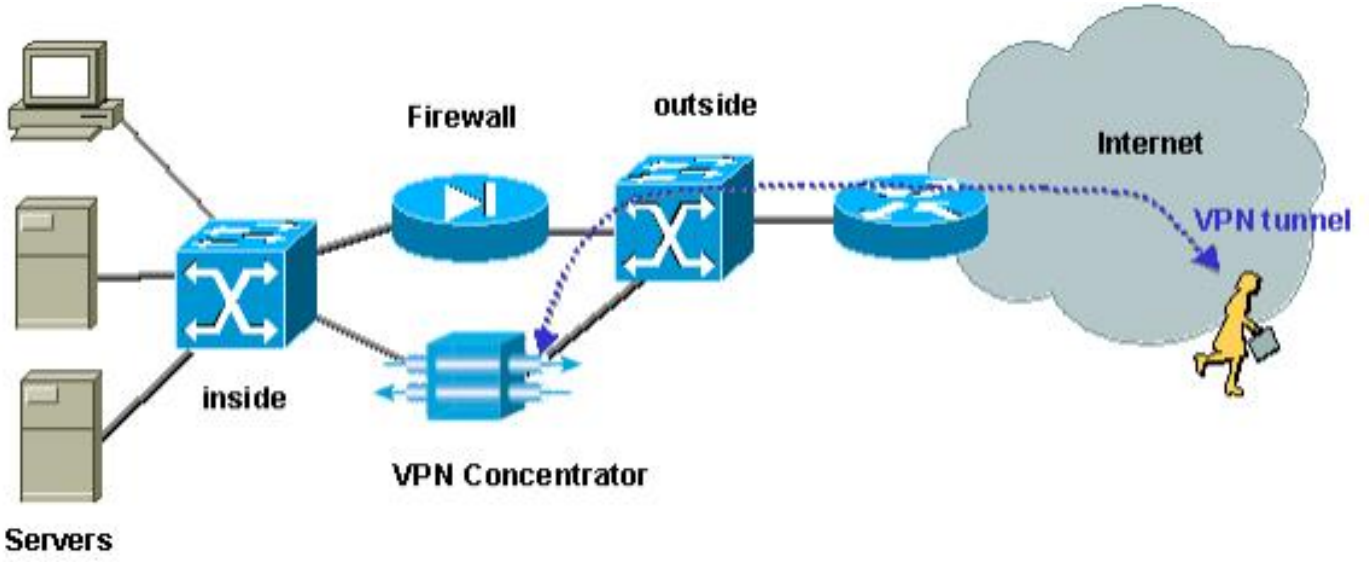
```
set security acl ip dmz_servers_out
------------------------------------------------
1. deny icmp any any fragment
2. permit icmp host 199.5.6.199 any echo
3. permit icmp host 199.5.6.202 any echo
4. permit tcp host 199.5.6.199 eq 80 any established
5. permit tcp host 199.5.6.202 eq 80 any established
6. permit udp host 199.5.6.199 eq 1645 host 172.16.171.9 eq 1645
7. permit udp host 199.5.6.202 eq 1645 host 172.16.171.9 eq 1645
8. permit udp host 199.5.6.199 eq 1646 host 172.16.171.9 eq 1646
9. permit udp host 199.5.6.202 eq 1646 host 172.16.171.9 eq 1646
10. permit udp host 199.5.6.199 any eq 53
11. permit udp host 199.5.6.202 any eq 53
ecomm-6500-2 (enable) sh pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
41      42        isolated         3/9-10

ecomm-6500-2 (enable) sh pvlan mapping
Port Primary Secondary
---- ------- ---------
 3/14 41      42
 3/34 41      42
 3/35 41      42
ecomm-6500-2 (enable) sh port
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/9  server_dmz1        connected  41,42      a-half  a-10 10/100BaseTX
 3/10 server_dmz2        connected  41,42      a-half  a-10 10/100BaseTX
 3/14 to_pix_port_2      connected  41           full   100 10/100BaseTX
 3/35 external_router_dm notconnect 41           auto  auto 10/100BaseTX
```

与防火墙并行的 VPN 集中器

实施访问虚拟专用网络 (VPN) 时，最常用的方法之一无疑是并行设计（如下图中所示）。用户通常更喜欢此设计方法，因为该方法容易实施，对现有基础设施几乎没有影响，并且它可以相对容易地根据设备灵活性进行扩展。

在并行方法中，VPN 集中器同时连接到内部和外部分段。所有 VPN 会话都将在集中器处终止，而不会通过防火墙。通常，VPN Client 应可以不受限制地访问内部网络，但有时它们可能被限制为访问一组内部服务器（服务器群）。其中一个很好的功能是从常规 Internet 数据流中分离出 VPN 数据流，因此（例如）不允许 VPN Client 通过公司防火墙访问 Internet。

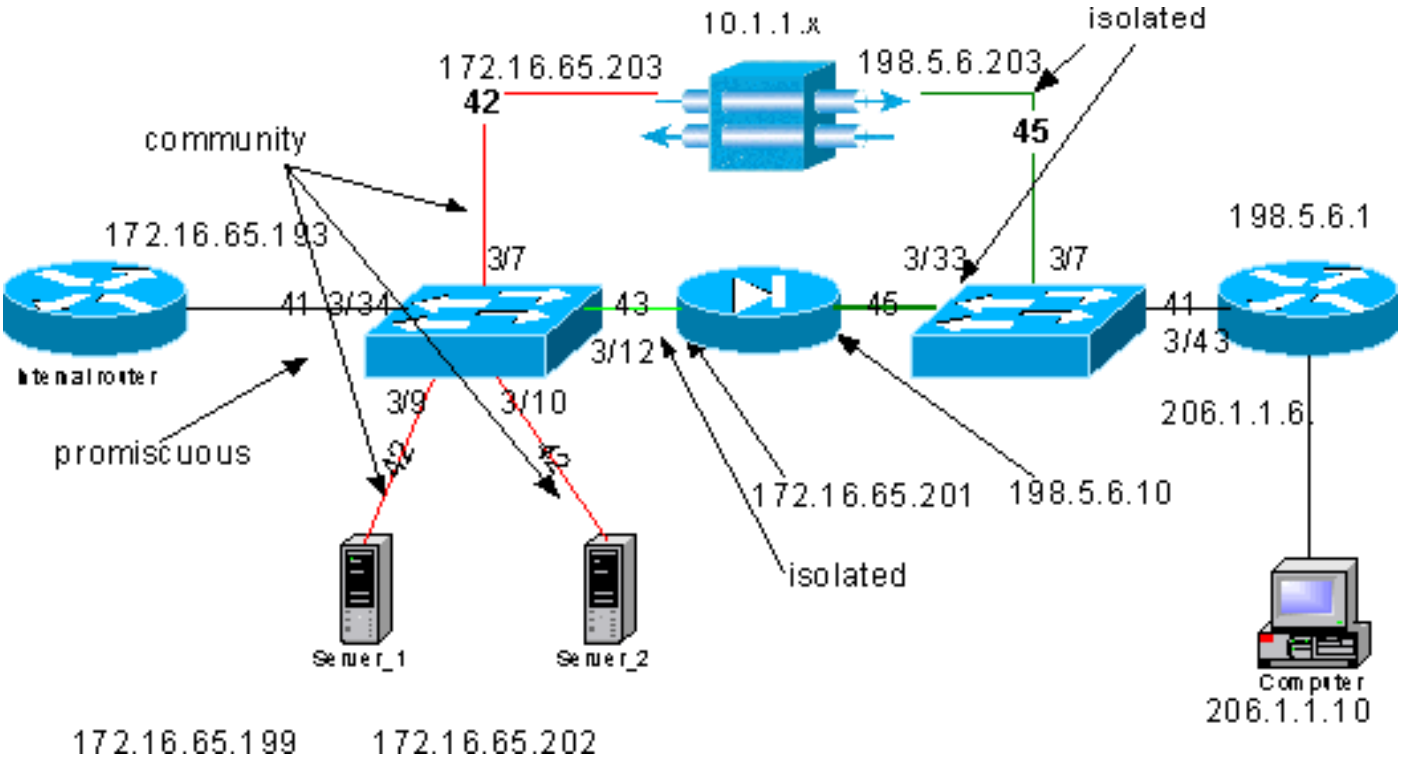
图 6：与防火墙并行的 VPN 集中器



测试与防火墙并行的 VPN 集中器

在本示例中，我们使用了一台 VPN 5000 集中器，它是与 PIX 防火墙平行安装的。配置为 Web 服务器的两个路由器已作为内部服务器群安装在内部分段中。VPN Client 仅允许访问服务器群，并且应该从 VPN 数据流 (IPSec) 中分离出 Internet 数据流。下图显示试验床。

图 7：与防火墙并行的 VPN 集中器试验床



在此方案中我们有两个感兴趣的主要区域：

- 内部第 2 层交换机
- 外部第 2 层交换机

内部第 2 层交换机的数据流根据下面的语句来定义：

- VPN Client 具有对预定义的一组内部服务器（服务器群）的完全访问权限
- 内部客户端也可以访问服务器群

- 内部客户端可以不受限制地访问 Internet
- 必须将来自 VPN 集中器的数据流从 PIX 防火墙隔离

外部第 2 层交换机的数据流按如下所示进行定义：

- 来自路由器的数据流必须能够流向 VPN 集中器或 PIX
- 来自 PIX 的数据流必须与来自 VPN 的数据流隔离

此外，管理员可能希望防止来自内部网络的数据流流向 VPN 主机，这可以通过在主 VLAN 上配置的 VACL 来实现（VACL 将只过滤来自内部路由器的数据流，任何其他数据流都不会受到影响）。

PVLAN 配置

由于此设计的主要目标是保持来自 PIX 的数据流与来自服务器和 VPN 集中器的数据流隔离，因此我们在配置服务器和 VPN 集中器的 PVLAN 以外的 PVLAN 上配置 PIX。

来自内部网络的数据流必须能够访问服务器群、VPN 集中器和 PIX。因此，连接到内部网络的端口将是混合端口。

服务器和 VPN 集中器属于同一个辅助 VLAN，因为它们将能够相互通信。

至于外部第 2 层交换机，允许访问 Internet 的路由器（通常属于 Internet 服务提供商 (ISP)）连接到混合端口，而 VPN 集中器和 PIX 属于同一专用隔离 VLAN（因此它们不能交换任何数据流）。通过执行此操作，来自服务提供商的数据流可以采用通向 VPN 集中器的路径或到 PIX 的路径。PIX 和 VPN 集中器受到了更好的保护，因为它们相互隔离。

内部第 2 层交换机的 PVLAN 配置

```
sh pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- -----------
41      42        community        3/7,3/9-10
41      43        isolated         3/12

ecomm-6500-2 (enable) sh pvlan map
Port Primary Secondary
---- ------- ---------
 3/34 41      42-43

ecomm-6500-2 (enable) sh port 3/7
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/7  to_vpn_conc        connected  41,42      a-half  a-10 10/100BaseTX

ecomm-6500-2 (enable) sh port 3/9
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/9  server_1           connected  41,42      a-half  a-10 10/100BaseTX


ecomm-6500-2 (enable) sh port 3/10
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/10 server_2           connected  41,42      a-half  a-10 10/100BaseTX

ecomm-6500-2 (enable) sh port 3/12
Port  Name               Status     Vlan       Duplex Speed Type
```

```
----- ----------------- ---------- ---------- ------ ----- ------------
 3/12 to_pix_intf1       connected  41,43      a-full a-100 10/100BaseTX


ecomm-6500-2 (enable) sh pvlan map
Port Primary Secondary
---- ------- ---------
 3/34 41      42-43

ecomm-6500-2 (enable) sh port 3/34
Port  Name               Status     Vlan       Duplex Speed Type
----- ----------------- ---------- ---------- ------ ----- ------------
 3/34 to_int_router      connected  41         a-full a-100 10/100BaseTX
```

外部第 2 层交换机的 PVLAN 配置

```
sh pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
41      45        isolated         3/7,3/33

ecomm-6500-1 (enable) sh pvlan mapping
Port Primary Secondary
---- ------- ---------
 3/43 41      45

ecomm-6500-1 (enable) sh port 3/7
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/7  from_vpn           connected  41,45      a-half  a-10 10/100BaseTX

ecomm-6500-1 (enable) sh port 3/33
Port  Name               Status     Vlan       Duplex Speed Type
----- ----------------- ---------- ---------- ------ ----- ------------
 3/33 to_pix_intf0       connected  41,45      a-full a-100 10/100BaseTX

ecomm-6500-1 (enable) sh pvlan map
Port Primary Secondary
---- ------- ---------
 3/43 41      45
ecomm-6500-1 (enable) sh port 3/43
Port  Name               Status     Vlan       Duplex Speed Type
----- ----------------- ---------- ---------- ------ ----- ------------
 3/43 to_external_router connected  41         a-half  a-10 10/100BaseTX
```

测试配置

此实验显示，内部路由器可以通过防火墙到达外部路由器（接口为 198.5.6.1 的外部防火墙路由器）。

```
ping 198.5.6.1
Type escape sequence to abort
Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

此实验显示以下信息，这些信息都来自服务器 1：

- 服务器 1 可以 ping 内部路由器：`server_1#ping 172.16.65.193`

  ```
  Type escape sequence to abort.
  ```

```
Sending 5, 100-byte ICMP Echos to 172.16.65.193, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

- 服务器 1 可以 ping VPN：`server_1#`**`ping 172.16.65.203`**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.203, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

- 服务器 1 不能 ping PIX 内部接口：`server_1#`**`ping 172.16.65.201`**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.201, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

- 服务器 1 不能 ping 外部路由器：`server_1#`**`ping 198.5.6.1`**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

以下实验显示，可以打开从内部网络到服务器群的 HTTP 会话。

```
server_1#ping 198.5.6.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

以下实验显示，来自 VPN 网络的 HTTP 数据流可以流向服务器群（请注意地址 10.1.1.1）。

```
server_1#ping 198.5.6.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

下面是 VPN 集中器的配置：

```
server_1#ping 198.5.6.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

以下命令显示连接用户的列表：

```
sh VPN user
Port        User            Group           Client          Local           ConnectNumber
                                            Address         Address         Time
-------------------------------------------------------------------------------------
VPN 0:1     martin          RemoteUsers     206.1.1.10      10.1.1.1        00:00:11:40
```

应注意，服务器上的默认网关是内部路由器 172.16.65.193，它将向 172.16.65.203 发出 icmp 重定向消息。此实施将导致非最优数据流，因为主机会将数据流的第一个数据包发送到路由器，并在收到重定向时，将后续数据包发送到更适合处理此数据流的网关。或者，用户可以自己在服务器上配置两个不同的路由，以便将 10.x.x.x 地址指向 VPN，将其余的数据流指向 172.16.65.193。如果只在服务器上配置默认网关，那么我们需要确保路由器接口使用“ip 重定向”进行配置。

下面是我们在测试期间注意到一个引人关注的现象。如果我们尝试从服务器或从 VPN ping 像 198.5.6.1 一样的外部地址，默认网关将发送重定向包告知本路由器应将 icmp 重定向至 172.16.65.201。

```
sh VPN user
Port        User            Group           Client          Local           ConnectNumber
                                            Address         Address         Time
--------------------------------------------------------------------------------
VPN 0:1     martin          RemoteUsers     206.1.1.10      10.1.1.1        00:00:11:40
```

此时服务器或 VPN 将发送 172.16.65.201 的地址解析协议 (ARP) 请求，并且不会从 201 那里获得任何响应，因为它位于另一个辅助 VLAN 上；这是 PVLAN 带来的问题。实际上，有一个简单的方法可以解决这个问题，即向 .193 的 MAC 发送数据流并使用目标 IP 172.16.65.201。

路由器 .193 会将数据流路由回同一接口，但由于路由器接口是混合端口，数据流将到达 .201，这是我们希望阻止的。此问题在 VACL 和 PVLAN 的已知限制部分中说明。

VACL 配置

本部分对于提升服务器群上的安全性至关重要。如 VACL 和 PVLAN 的已知限制部分中所述，即使服务器和 PIX 属于两个不同的辅助 VLAN，攻击者仍然有方法使它们相互通信。如果它们尝试直接通信，由于 PVLAN 的缘故，它们将无法成功。如果入侵者攻陷这些服务器，并且然后将这些服务器配置为将同一子网的数据流发送到路由器，该路由器会将数据流路由回同一子网，从而使 PVLAN 的目的无法实现。

因此，需要使用以下策略在主 VLAN（传输来自路由器的数据流的 VLAN）上配置 VACL：

- 允许源 IP 为路由器 IP 的数据流
- 拒绝源和目标 IP 都属于服务器群子网的数据流
- 允许所有其余数据流

```
ecomm-6500-2 (enable) sh sec acl info protect_pvlan
set security acl ip protect_pvlan
------------------------------------------------
1. permit ip host 172.16.65.193 any
2. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
3. permit ip any any

ecomm-6500-2 (enable) sh sec acl
ACL                              Type VLANS
-------------------------------  ---- -----
protect_pvlan                    IP   41
```

此 ACL 不会影响由服务器或 PIX 生成的数据流；它将只防止路由器路由来自服务器的数据流回到同一个VLAN。前两个语句允许路由器将 icmp 重定向或 icmp 不可到达等消息发送给服务器。

我们已确定了管理员可能希望通过 VACL 阻止的另一个数据流，此数据流从内部网络流向 VPN 主机。为了实现此目的，可以将 VACL 映射到主 VLAN (41) 并将其与前一个 VACL 结合：

```
show sec acl info all

set security acl ip protect_pvlan

1. deny ip any 10.1.1.0 0.0.0.255
2. permit ip host 172.16.65.193 any
3. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
```

```
4. permit ip any any
```

测试配置

现在我们从路由器 .193 (zundapp) ping 10.1.1.1 主机。在映射 VACL 之前，ping 是成功的。

```
show sec acl info all

set security acl ip protect_pvlan

1. deny ip any 10.1.1.0 0.0.0.255
2. permit ip host 172.16.65.193 any
3. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
4. permit ip any any
```

在 VLAN 41 上映射 VACL 以后，同一 ping 将不会成功；

```
show sec acl info all

set security acl ip protect_pvlan

1. deny ip any 10.1.1.0 0.0.0.255
2. permit ip host 172.16.65.193 any
3. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
4. permit ip any any
```

但是，我们仍然可以 ping 外部路由器：

```
show sec acl info all

set security acl ip protect_pvlan

1. deny ip any 10.1.1.0 0.0.0.255
2. permit ip host 172.16.65.193 any
3. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
4. permit ip any any
```

相关信息

- 配置访问控制列表 - Catalyst 6000 文档
- 技术支持 - Cisco Systems