具有PVLAN和VACL的安全網路

目錄

簡介

成功構建網路安全設計的一個關鍵因素是確定並實施適當的信任模型。適當的信任模型定義了需要與誰對話以及需要交換的流量型別；應拒絕所有其他流量。一旦確定了正確的信任模型，安全設計人員就應該決定如何實施該模型。隨著更多關鍵資源在全球範圍內可用，以及新型網路攻擊不斷演化，網路安全基礎架構會變得越來越複雜，而且可用的產品也越來越多。防火牆、路由器、LAN交換機、入侵檢測系統、AAA伺服器和VPN是有助於實施該模型的技術和產品。當然，這些產品和技術中的每一種都在整體安全實施中發揮著特定的作用，設計師必須瞭解如何部署這些元素。

開始之前

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

必要條件

本檔案介紹僅執行CatOS的交換器上的PVLAN組態。有關運行Cisco IOS和CatOS的交換機上的PVLAN並行配置示例，請參閱在Catalyst交換機上配置隔離專用VLAN文檔。

並非所有交換機和軟體版本都支援PVLAN。請參閱專用VLAN Catalyst交換機支援清單，以確定您的平台和軟體版本是否支援PVLAN。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

背景資訊

確定並實施適當的信任模型似乎是一個非常基本的任務，但在支援安全實施幾年之後，我們的經驗表明，安全事件往往與糟糕的安全設計有關。通常這些糟糕的設計是不執行恰當的信任模型的直接後果，有時是因為根本就需要的東西得不到理解，而有時僅僅是因為所涉及的技術沒有被完全理解或誤用。

本檔案將詳細介紹Catalyst交換器中的兩個可用功能(私人VLAN(PVLAN)和VLAN存取控制清單(VACL))如何協助確保在企業和服務供應商環境中都建立適當的信任模式。

實施適當的信任模型的重要性

不執行適當的信任模型的一個直接後果是，總體安全實施對惡意活動的免疫力降低了。通常實施非軍事區(DMZ)時未執行正確的策略，因此便於潛在的入侵者進行活動。本節分析如何經常實施DMZ以及設計不良的後果。我們稍後將解釋如何減輕這些後果，或者在最好的情況下避免這些後果。

通常，DMZ伺服器只應處理來自Internet的傳入請求，並最終啟動與位於內部或其他DMZ網段的一些後端伺服器的連線，例如資料庫伺服器。同時，DMZ伺服器不應相互通訊或啟動與外部世界的連線。這在一個簡單的信任模型中明確定義了必要的通訊流；然而，我們經常看到這種模式沒有得到充分的執行。

設計人員通常傾向於對所有伺服器使用公共段來實施DMZ，而對其之間的流量沒有任何控制。例如，所有伺服器都位於一個通用VLAN中。由於相同VLAN中的流量不受任何控制，因此如果其中一個伺服器受到危害，那麼可以利用同一台伺服器向同一網段中的任何伺服器和主機發起攻擊。這顯然有利於潛在的入侵者進行埠重定向或應用層攻擊。

通常，防火牆和資料包過濾器僅用於控制傳入連線，但通常不執行任何操作來限制源自DMZ的連線。一段時間前，cgi-bin指令碼中存在一個眾所周知的漏洞，使得入侵者能夠僅通過傳送HTTP流來開始X-term會話；這是防火牆應允許的流量。如果入侵者足夠幸運，他或她可以使用其他方法獲得根提示，通常是某種緩衝區溢位攻擊。大多數情況下，這類問題可以通過實施適當的信任模型來避免。首先，伺服器不應相互通訊，其次，不應從這些伺服器與外部世界建立連線。

同樣的註釋也適用於許多其他場景，從任何常規不可信任的分段到應用程式服務提供商的伺服器群。

Catalyst交換器上的PVLAN和VACL有助於確保適當的信任模式。PVLAN通過限制公共網段中主機之間的流量而提供幫助，而VACL則通過對發往或發往特定網段的任何流量提供進一步控制。這些功能將在以下部分討論。

專用VLAN

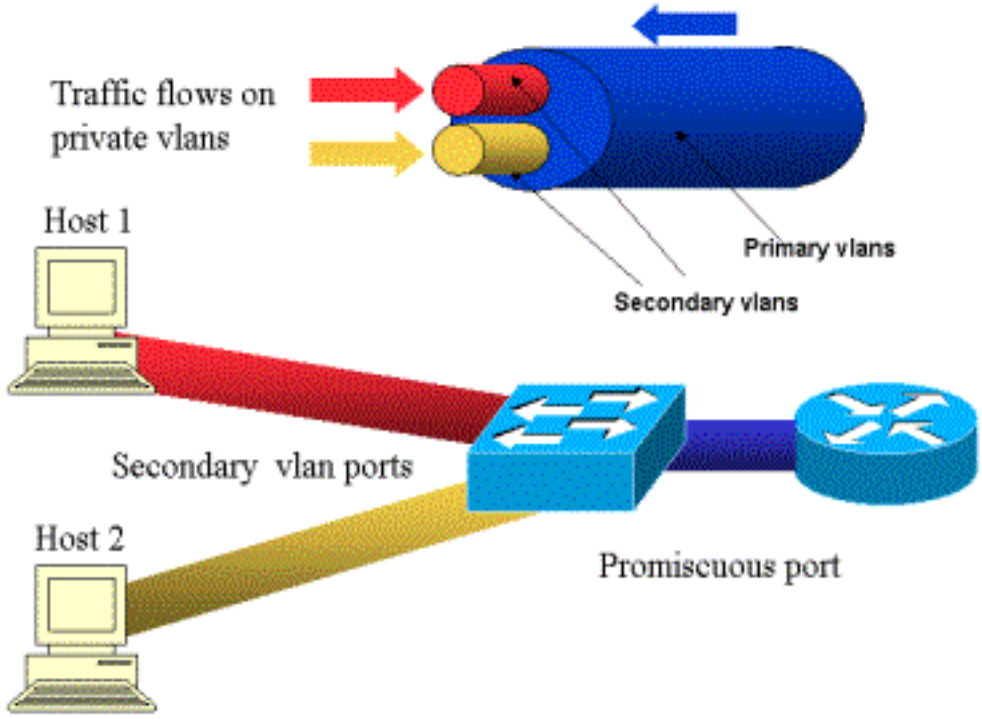
PVLAN在運行CatOS 5.4或更高版本的Catalyst 6000、2980G、2980G-A、2948G和4912G（運行CatOS 6.2或更高版本）上可用。

從我們的角度來看，PVLAN是一種工具，它允許在第2層(L2)隔離流量，將廣播網段轉換為類似於

非廣播多路訪問網段。從混合連線埠（即能夠轉送主要和輔助VLAN的連線埠）進入交換器的流量可以在屬於相同主要VLAN的所有連線埠上出去。從對映到輔助VLAN（可以是隔離、社群或雙向社群VLAN）的埠傳到交換機的流量可以轉發到混雜埠或屬於同一社群VLAN的埠。對映到同一個隔離VLAN的多個埠無法交換任何流量。

下圖顯示了此概念。

圖1:專用VLAN



主要VLAN以藍色表示；輔助VLAN以紅色和黃色表示。Host-1連線到屬於輔助VLAN紅色的交換機埠。Host-2連線到屬於輔助VLAN黃色埠的交換機埠。

當主機傳輸時，流量在輔助VLAN中傳輸。例如，主機2傳輸時，其流量會進入VLAN黃色狀態。當這些主機接收時，流量來自VLAN藍色，即主要VLAN。

路由器和防火牆連線的埠是混雜埠，因為這些埠可以轉發來自對映中定義的每個輔助VLAN以及主要VLAN的流量。連線到每台主機的埠只能轉發來自該埠上配置的主VLAN和輔助VLAN的流量。

該圖將專用VLAN表示為連線路由器和主機的不同管道：捆綁所有其他裝置的管道是主VLAN（藍色），VLAN藍色上的流量從路由器流向主機。主要VLAN的內部管道是輔助VLAN，在這些管道上傳輸的流量是從主機到路由器。

如圖所示，主VLAN可以捆綁一個或多個輔助VLAN。

在本文檔的前面部分，我們說PVLAN只需確保在一個公共網段中隔離主機，即可幫助實施適當的信任模型。現在我們對專用VLAN有了更多瞭解，接下來我們來看一下如何在我們最初的DMZ場景中實施該功能。伺服器不應相互通訊，但它們仍需要與所連線的防火牆或路由器通訊。在這種情況下，伺服器應連線到隔離埠，而路由器和防火牆應連線到混雜埠。這樣，如果其中一個伺服器受到危害，入侵者將無法使用同一伺服器向同一網段中的另一伺服器發起攻擊。交換器將以線速捨棄任何封包，而且不會減損效能。

另一個重要注意事項是，此類控制只能在第2層裝置上實施，因為所有伺服器都屬於同一子網。防火牆或路由器無法執行任何操作，因為伺服器會嘗試直接通訊。另一種選擇是每台伺服器專用一個防火牆埠，但這可能成本太高，難以實施，而且無法擴展。

在後面的部分中，我們將詳細介紹可以使用此功能的一些其他典型方案。

VLAN存取控制清單

VACL可在執行CatOS 5.3或更新版本的Catalyst 6000系列上使用。

無需路由器(您只需要策略功能卡(PFC))，即可在L2的Catalyst 6500上配置VACL。 它們以線速執行，因此在Catalyst 6500上設定VACL時不會產生效能下降。由於查詢硬體中的VACL而不管訪問清單的大小如何，因此轉發速率保持不變。

VACL可以分別對映到主或輔助VLAN。通過在輔助VLAN上配置VACL，可以過濾主機發起的流量，而無需接觸路由器或防火牆生成的流量。

通過合併VACL和專用VLAN，可以根據流量本身的方向過濾流量。例如，如果兩台路由器與某些主機（例如伺服器）連線到同一個網段，則可以在輔助VLAN上配置VACL，以便在路由器之間交換的流量未受到影響時，僅過濾主機生成的流量。

VACL可以輕鬆部署以實施適當的信任模型。我們來分析下非軍事區案例。DMZ上的伺服器應該只為傳入連線提供服務，並且不期望它們啟動與外部世界的連線。可以將VACL應用於其輔助VLAN，以便控制離開這些伺服器的流量。必須注意的是，使用VACL時，流量會在硬體中丟棄，因此不會對路由器的CPU或交換機產生影響。即使其中一台伺服器作為來源捲入分散式拒絕服務(DDoS)攻擊，交換器也會以線速捨棄所有非法流量，而且不會降低效能。類似的過濾器可以應用於伺服器所連線的路由器或防火牆，但通常會對效能造成嚴重影響。

基於MAC的ACL不能很好地處理IP流量，因此建議使用VACL來監控/跟蹤PVLAN。

VACL和PVLAN的已知限制

使用VACL配置過濾時，對於PFC上的片段處理，您應該小心，並且配置會根據硬體的規格進行調整。

鑑於Catalyst 6500的Supervisor 1的PFC的硬體設計，最好明確拒絕icmp片段。原因在於，硬體認為網際網路控制訊息通訊協定(ICMP)片段和回應回覆相同，且預設會對硬體進行程式設計以明確允許片段。因此，如果要停止回應回覆封包離開伺服器，必須明確使用**deny icmp any any fragment**行進行設定。本檔案中的組態已考慮這一點。

PVLAN有一個眾所周知的安全限制，即路由器可能將流量從它來自的同一子網轉回。路由器可以通過隔離埠路由流量，這有悖於PVLAN的用途。此限制是由於PVLAN是一種在L2提供隔離的工具，而不是在第3層(L3)提供隔離的工具。

單點傳送反向路徑轉送(uRPF)在PVLAN主機連線埠上無法正常運作，因此uRPF不得與PVLAN結合使用。

此問題可通過在主VLAN上配置的VACL得到解決。本案例研究提供了需要在主VLAN上配置的VACL，以丟棄源自同一子網並路由回同一子網的流量。

在某些線卡上，PVLAN對映/對映/中繼埠的配置受一些限制，其中多個PVLAN對映必須屬於不同的

埠特定應用積體電路(ASIC)才能進行配置。新埠ASIC Coil3上刪除了這些限制。有關詳細資訊，請參閱有關軟體配置的最新Catalyst交換機文檔。

案例分析

下一節將介紹三個案例分析，我們認為它們代表了大多數實施，並提供了與PVLAN和VACL的安全部署相關的詳細資訊。

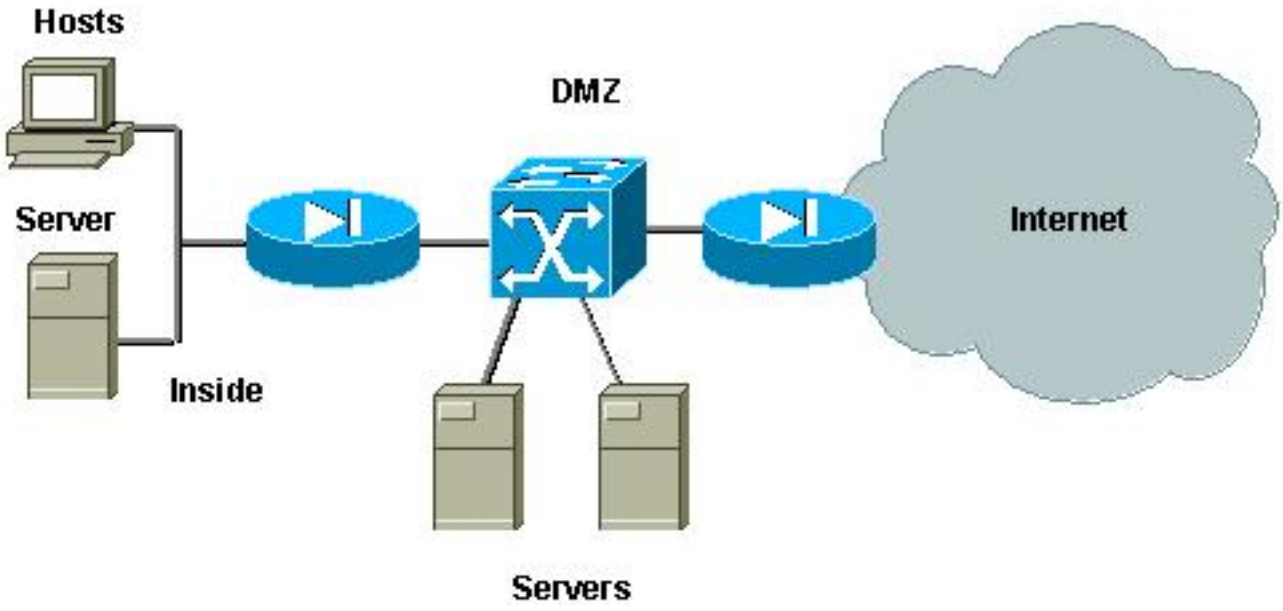
這些場景是：

- 直通DMZ
- 外部DMZ
- 與防火牆並行的VPN集中器

直通DMZ

這是最常見的部署情況之一。在此範例中，DMZ實作兩個防火牆路由器之間的傳輸區域，如下圖所示。

圖2:直通DMZ



在本示例中，DMZ伺服器應該由外部和內部使用者訪問，但是它們不需要彼此通訊。在某些情況下，DMZ伺服器需要開啟與內部主機的某種連線。同時，內部客戶端應該不受限制地訪問Internet。DMZ中包含Web伺服器的伺服器就是一個很好的示例，這些伺服器需要與位於內部網路中的資料庫伺服器進行通訊，並讓內部客戶端訪問Internet。

外部防火牆設定為允許傳入連線到位於DMZ的伺服器，但通常不對傳出流量（尤其是源自DMZ的流量）應用過濾或限制。正如我們在本文檔前面所討論的，這可能使攻擊者更容易活動，原因有二：第一，一旦其中一個DMZ主機受到危害，所有其他DMZ主機都會被暴露出來；第二種，攻擊者可以輕鬆利用傳出連線。

由於DMZ伺服器不需要相互通訊，因此建議確保它們在第2層隔離。伺服器埠將定義為PVLAN隔離

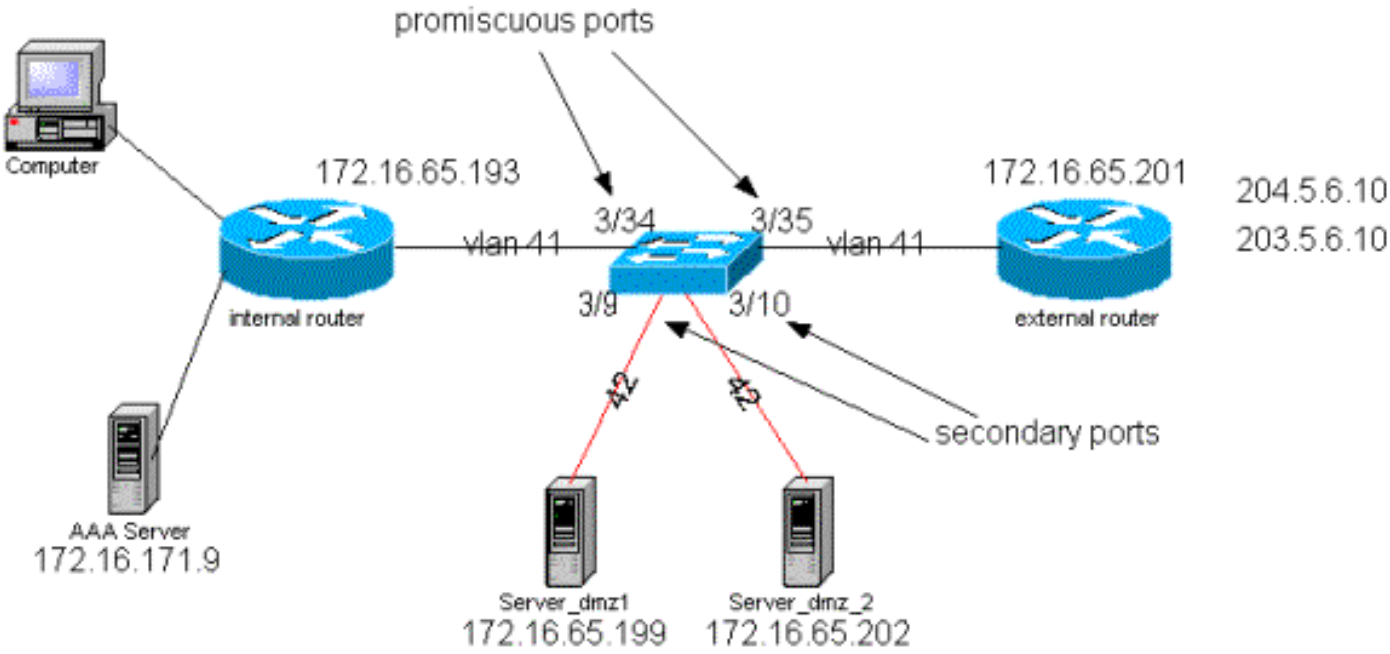
埠，而連線到兩個防火牆的埠將定義為「混雜」。為防火牆定義主VLAN，為DMZ伺服器定義輔助VLAN即可實現此目的。

VACL將用於控制源自DMZ的流量。這將防止攻擊者開啟非法的傳出連線。請務必記住，DMZ伺服器不僅需要回覆與客戶端會話對應的流量，而且還需要一些額外的服務，例如域名系統(DNS)和最大傳輸單元(MTU)路徑發現。因此，ACL應允許DMZ伺服器所需的所有服務。

測試直通DMZ

在我們的測試台中，我們實施了一個DMZ網段，其中兩台路由器配置為台伺服器：server_dmz1和server_dmz2。這些伺服器應該由外部和內部客戶端訪問，並且所有HTTP連線都通過使用內部RADIUS伺服器(CiscoSecure ACS for UNIX)進行身份驗證。 內部和外部路由器均配置為資料包過濾防火牆。下圖說明了測試平台，包括使用的編址方案。

圖3:直通DMZ試驗檯



以下清單收集PVLAN的基本配置步驟。Catalyst 6500用作DMZ中的L2交換器。

- Server_dmz_1連線到埠3/9
- Server_dmz_2連線到埠3/10
- 內部路由器連線到埠3/34
- 外部路由器連線到埠3/35

我們選擇了以下VLAN:

- 41是主要VLAN
- 42是隔離VLAN

專用VLAN配置

以下配置設定相關埠上的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

本節對於提高DMZ的安全性至關重要。如VACL和PVLAN的已知限制一節所述，即使伺服器屬於兩個不同的輔助VLAN或屬於同一個隔離VLAN，攻擊者仍然可以使用某種方法來使其相互通訊。如果伺服器嘗試直接通訊，由於PVLAN的原因，它們將無法在L2進行通訊。如果伺服器受到攻擊，然後被入侵者以相同子網的流量傳送到路由器的方式配置，該入侵者會將流量路由回同一子網，從而破壞PVLAN的用途。

因此，需要使用以下策略在主VLAN（傳送來自路由器的流量的VLAN）上配置VACL:

- 允許來源IP為路由器IP的流量
- 拒絕源IP和目標IP都是DMZ子網的流量
- 允許所有其餘流量

```
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不會影響伺服器生成的流量；這只會防止路由器將來自伺服器的流量路由回同一個VLAN。前兩條語句允許路由器向伺服器傳送消息，例如icmp重定向或icmp無法訪問。

輔助VLAN上的VACL配置

以下配置日誌用於顯示如何設定VACL以過濾伺服器生成的流量。通過配置此VACL，我們希望實現以下目標：

- 允許從伺服器ping(允許echo)
- 防止echo應答離開伺服器
- 允許源自外部的HTTP連線
- 允許RADIUS驗證（UDP埠1645）和記帳（UDP埠1646）流量
- 允許DNS流量（UDP埠53）

我們想阻止其餘的交通。

就分段而言，我們假設在伺服器段上有以下情況：

- 伺服器不會生成碎片流量
- 伺服器可能收到分段流量

鑑於Catalyst 6500的Supervisor 1的PFC的硬體設計，最好明確拒絕icmp片段。原因是硬體認為ICMP片段和回應回覆相同，預設情況下，硬體會設定為明確允許片段。因此，如果要阻止回應回覆封包離開伺服器，您必須明確使用deny icmp any fragment行進行設定。

```
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
```

測試配置

當已配置但未應用VACL的PVLAN時，捕獲以下輸出。此測試顯示使用者能夠從外部路由器ping內部路由器和伺服器。

```
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
```

以下範例顯示，我們可以從伺服器ping外部網路、預設閘道，但不能對屬於同一個輔助VLAN的伺服器執行ping。

```
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)
```

對映VACL後，來自外部路由器的ping將不再成功：

```
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)
```

以下示例顯示從內部網路接收HTTP GET請求的伺服器：

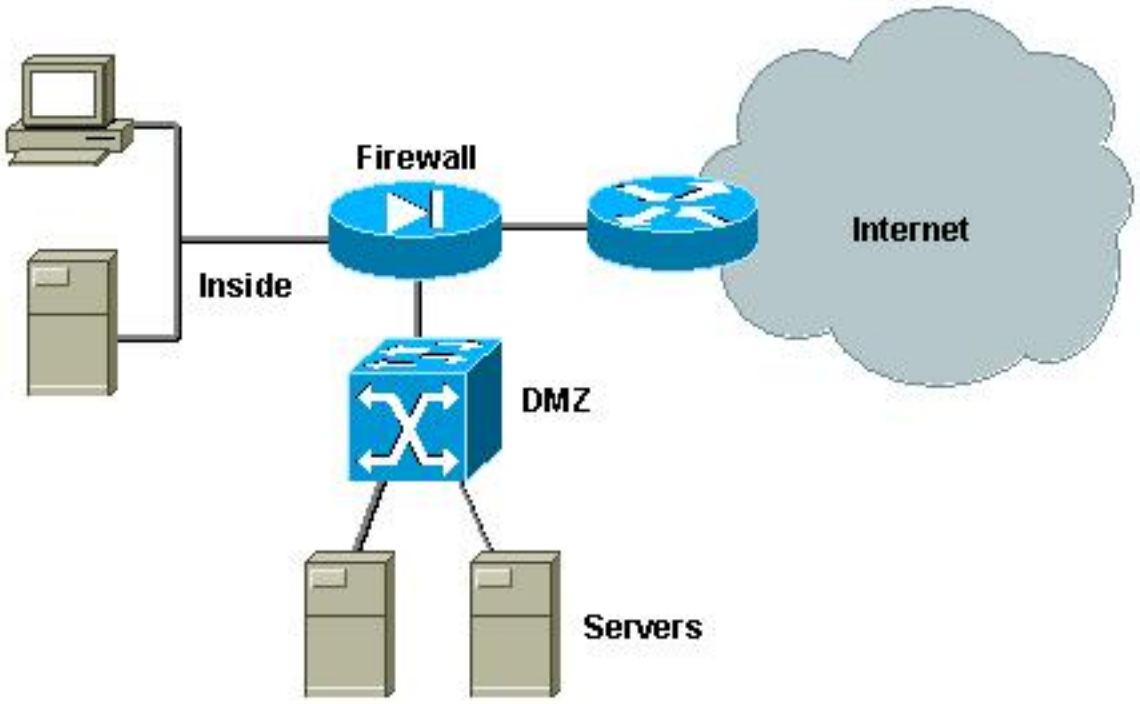
```
server_dmz1#debug ip http url
HTTP URL debugging is on
server_dmz1#debug ip hhtp tran
```

```
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方案可能是最被接受且部署最廣泛的實施方案。外部DMZ通過使用防火牆的一個或多個介面來實現，如下圖所示。

圖4:外部DMZ



無論設計實施如何，DMZ的要求通常都是相同的。與前面的情況一樣，DMZ伺服器應該可從外部客戶端和內部網路訪問。DMZ伺服器最終需要訪問一些內部資源，並且它們不應該相互通訊。同時，不應啟動從DMZ到Internet的流量；這些DMZ伺服器應僅回覆與傳入連線對應的流量。

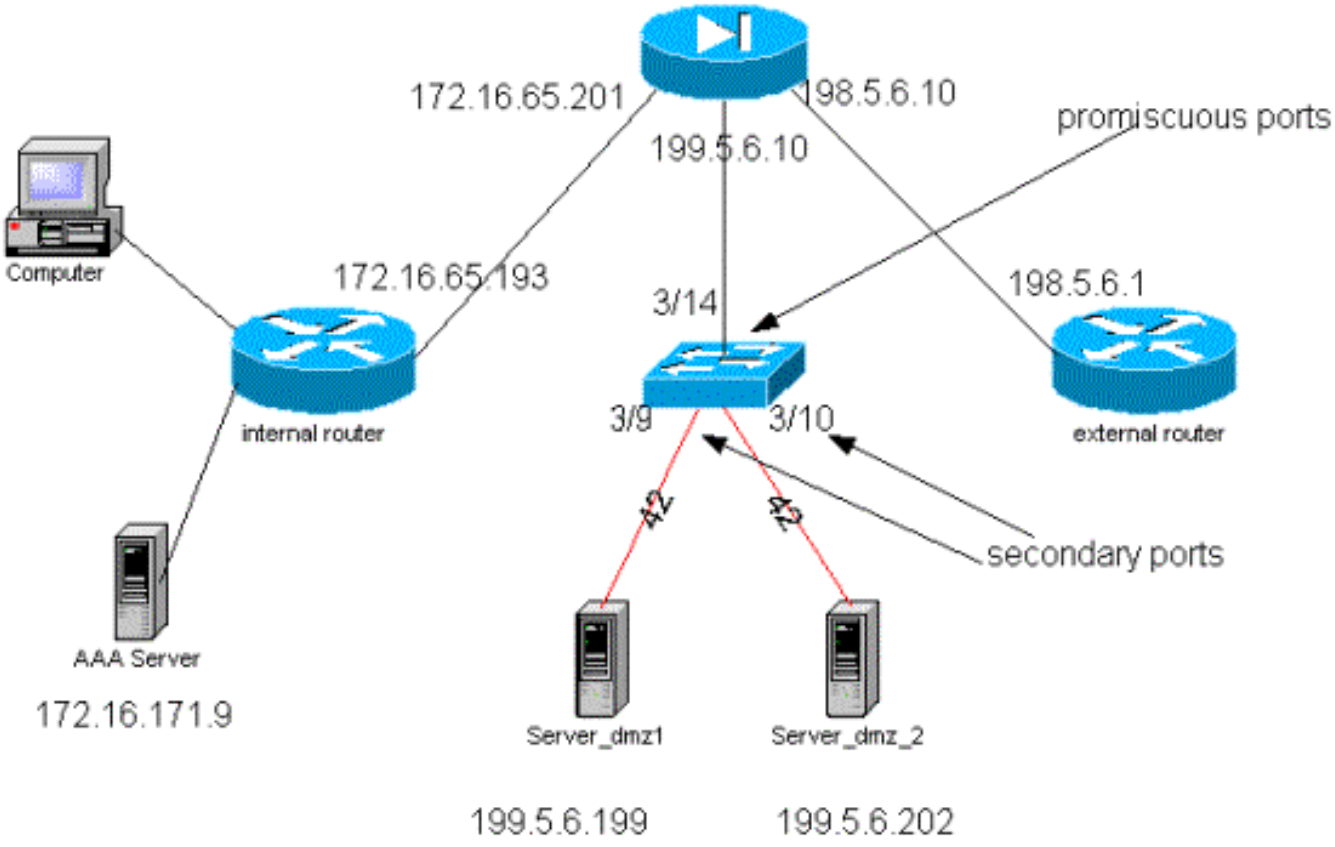
與先前的案例研究一樣，第一個配置步驟是通過PVLAN在L2實現隔離，並確保DMZ伺服器無法相互通訊，而內部和外部主機可以訪問它們。這可以通過將伺服器設定為具有隔離埠的輔助VLAN來實現。防火牆應在具有混雜連線埠的主VLAN中定義。防火牆將是此主要VLAN中的唯一裝置。

第二步是定義ACL以控制源自DMZ的流量。定義這些ACL時，我們需要確保只允許必要的流量。

測試外部DMZ

下圖顯示了為此案例研究實現的測試平台，其中我們使用了一個具有第三個介面的PIX防火牆來用於DMZ。使用同一組路由器作為Web伺服器，並且所有HTTP會話都使用同一個RADIUS伺服器進行身份驗證。

圖5:外部DMZ測試平台



在此案例中，我們只附上配置檔案中更有趣的摘錄，因為已在先前的個案研究中詳細解釋了PVLAN和VACL組態。

PIX配置

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
ip address outside 198.5.6.10 255.255.255.0
ip address inside 172.16.65.201 255.255.255.240
ip address dmz 199.5.6.10 255.255.255.0
global (outside) 1 198.5.6.11
global (dmz) 1 199.5.6.11
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (dmz,outside) 199.5.6.199 199.5.6.199 netmask 255.255.255.255 0 0
static (dmz,outside) 199.5.6.202 199.5.6.202 netmask 255.255.255.255 0 0
static (inside,dmz) 172.16.171.9 172.16.171.9 netmask 255.255.255.255 0 0
static (inside,dmz) 171.68.10.70 171.68.10.70 netmask 255.255.255.255 0 0
static (inside,dmz) 171.69.0.0 171.69.0.0 netmask 255.255.0.0 0 0
conduit permit tcp host 199.5.6.199 eq www any
conduit permit tcp host 199.5.6.202 eq www any
conduit permit udp any eq domain any
conduit permit icmp any any echo-reply
conduit permit icmp any any unreachable
conduit permit udp host 172.16.171.9 eq 1645 host 199.5.6.199
conduit permit udp host 172.16.171.9 eq 1646 host 199.5.6.199
conduit permit udp host 172.16.171.9 eq 1646 host 199.5.6.202
conduit permit udp host 172.16.171.9 eq 1645 host 199.5.6.202
conduit permit icmp any host 199.5.6.199 echo
conduit permit icmp any host 199.5.6.202 echo
route outside 0.0.0.0 0.0.0.0 198.5.6.1 1
route inside 171.69.0.0 255.255.0.0 172.16.65.193 1
route inside 171.68.0.0 255.255.0.0 172.16.65.193 1
```

```
route inside 172.16.0.0 255.255.0.0 172.16.65.193 1
```

RADIUS組態

NAS配置

```
aaa new-model
aaa authentication login default radius local
aaa authentication login consoleauth none
aaa authorization exec default radius local
aaa authorization exec consoleautho none
aaa accounting exec default start-stop radius
aaa accounting exec consoleacct none
radius-server host 172.16.171.9 auth-port 1645 acct-port 1646
radius-server key cisco123
!
line con 0
 exec-timeout 0 0
 password ww
 authorization exec consoleautho
 accounting exec consoleacct
 login authentication consoleauth
 transport input none
line aux 0
line vty 0 4
 password ww
!
end
```

RADIUS伺服器CSUX

```
User Profile Information
user = martin{
profile_id = 151
profile_cycle = 5
radius=Cisco {
check_items= {
2=cisco
}
reply_attributes= {
6=6
}
}

}

User Profile Information
user = NAS.172.16.65.199{
profile_id = 83
profile_cycle = 2
NASName="172.16.65.199"
SharedSecret="cisco123"
RadiusVendor="Cisco"
Dictionary="DICTIONARY.Cisco"

}
```

Catalyst組態

應該注意的是，在此配置中，不需要在主VLAN上配置VACL，因為PIX不會將流量重定向出它來自的同一介面。主VLAN上的VACL配置一節中所述的VACL將是冗餘的。

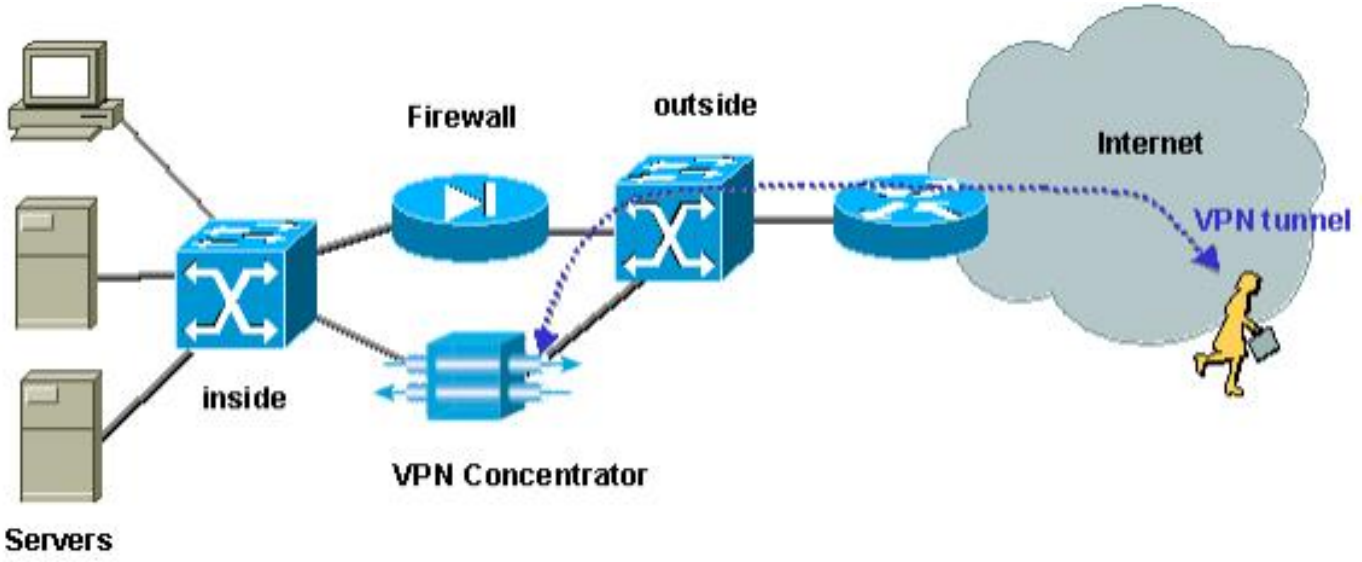
```
set security acl ip dmz_servers_out
------------------------------------------------
1. deny icmp any any fragment
2. permit icmp host 199.5.6.199 any echo
3. permit icmp host 199.5.6.202 any echo
4. permit tcp host 199.5.6.199 eq 80 any established
5. permit tcp host 199.5.6.202 eq 80 any established
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
```

與防火牆並行的VPN集中器

在實施接入虛擬專用網路(VPN)時，並行設計無疑是首選方法之一（如下圖所示）。 客戶通常更喜歡這種設計方法，因為它易於實施，對現有基礎架構幾乎沒有影響，而且基於裝置靈活性進行擴展相對容易。

在並行方式中，VPN集中器連線到內部網段和外部網段。所有VPN會話在集中器處終止，無需通過防火牆。通常VPN客戶端應具有對內部網路的無限制訪問許可權，但有時其訪問許可權可限製為一組內部伺服器（伺服器群）。 一個理想的功能是將VPN流量與常規網際網路流量隔離，例如，不允許VPN客戶端通過公司防火牆訪問網際網路。

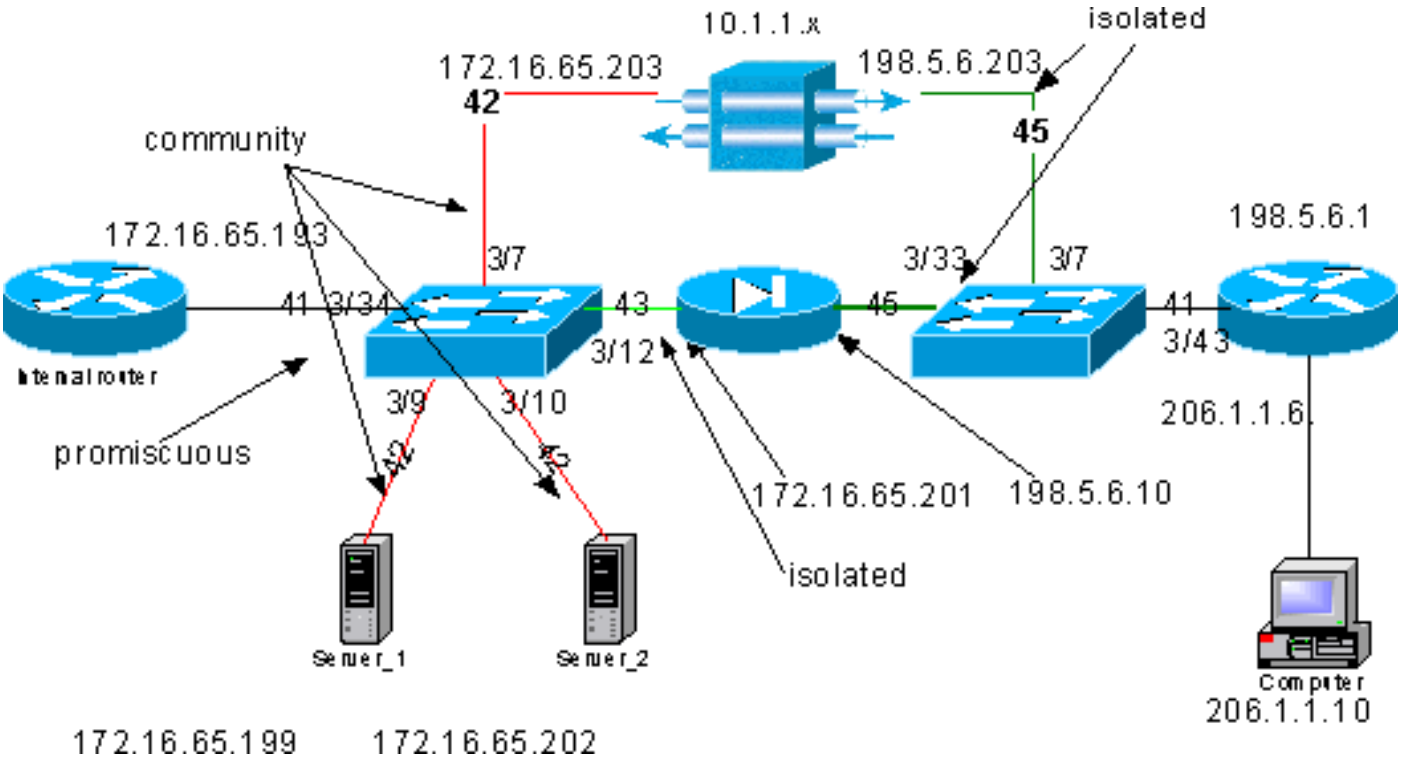
圖6:與防火牆並行的VPN集中器



並行測試防火牆中的VPN集中器

在本例中，我們使用VPN 5000集中器，該集中器與PIX防火牆並行安裝。配置為Web伺服器的兩台路由器安裝在內部網段作為內部伺服器群。僅允許VPN客戶端訪問伺服器群，並且應該將網際網路流量與VPN流量(IPSec)隔離。 下圖顯示了測試台。

圖7:並行防火牆測試平台上的VPN集中器



在此案例中，我們主要關注兩個方面：

- 內部L2交換機
- 外部L2交換器

內部L2交換機的流量根據以下語句定義：

- VPN客戶端擁有對一組預定義內部伺服器（伺服器群）的完全訪問許可權
- 還允許內部客戶端訪問伺服器群

- 內部客戶端可以不受限制地訪問Internet
- 來自VPN集中器的流量必須與PIX防火牆隔離

外部L2交換器的流量流定義如下：

- 來自路由器的流量必須能夠到達VPN集中器或PIX
- 來自PIX的流量必須與VPN的流量隔離

此外，管理員可能希望阻止來自內部網路的流量通往VPN主機，這可以通過在主VLAN上配置的VACL來實現（VACL僅過濾從內部路由器離開的流量，其他流量不會受到影響）。

PVLAN配置

由於本設計的主要目標是將來自PIX的流量與來自伺服器和VPN集中器的流量隔離，因此我們將PIX配置在不同於配置伺服器和VPN集中器的PVLAN的PVLAN上。

來自內部網路的流量必須能夠訪問伺服器群以及VPN集中器和PIX。因此，連線到內部網路的埠將成為混雜埠。

伺服器和VPN集中器屬於同一個輔助VLAN，因為它們可以彼此通訊。

對於外部L2交換機，允許訪問Internet(通常屬於網際網路服務提供商(ISP))的路由器連線到混雜埠，而VPN集中器和PIX屬於相同的專用和隔離VLAN（因此它們不能交換任何流量）。 這樣，來自服務提供商的流量可以採用通往VPN集中器的路徑或通往PIX的路徑。PIX和VPN集中器被隔離，因此受到更好的保護。

內部L2交換機的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L2交換機的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
```

測試配置

此實驗顯示內部路由器可以透過防火牆到達外部路由器（介面為198.5.6.1的外部防火牆路由器）。

```
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
```

本實驗顯示了以下內容（全部來自伺服器1）：

- 伺服器1可以ping通內部路由器：

```
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
```

- 伺服器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
```

- 伺服器1無法ping通PIX內部介面：

```
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)
```

- 伺服器1無法ping通外部路由器：

```
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)
```

以下實驗顯示，可以從內部網路到伺服器群開啟HTTP會話。

```
server_2#
1w1d: HTTP: parsed uri '/'
1w1d: HTTP: processing URL '/' from host 171.68.173.3
1w1d: HTTP: client version 1.0
1w1d: HTTP: parsed extension Connection
1w1d: HTTP: parsed line  Keep-Alive
1w1d: HTTP: parsed extension User-Agent
1w1d: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
1w1d: HTTP: parsed extension Host
1w1d: HTTP: parsed line  172.16.65.202
1w1d: HTTP: parsed extension Accept
1w1d: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
1w1d: HTTP: parsed extension Accept-Encoding
1w1d: HTTP: parsed line  gzip
1w1d: HTTP: parsed extension Accept-Language
1w1d: HTTP: parsed line  en
1w1d: HTTP: parsed extension Accept-Charset
1w1d: HTTP: parsed line  iso-8859-1,*,utf-8
1w1d: HTTP: Authentication for url '/' '/' level 15  privless '/'
1w1d: HTTP: authentication required, no authentication information was provided
1w1d: HTTP: authorization rejected
1w1d: HTTP: parsed uri '/'
1w1d: HTTP: processing URL '/' from host 171.68.173.3
1w1d: HTTP: client version 1.0
1w1d: HTTP: parsed extension Connection
1w1d: HTTP: parsed line  Keep-Alive
1w1d: HTTP: parsed extension User-Agent
1w1d: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
1w1d: HTTP: parsed extension Host
1w1d: HTTP: parsed line  172.16.65.202
1w1d: HTTP: parsed extension Accept
1w1d: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
```

```
1w1d: HTTP: parsed extension Accept-Encoding
1w1d: HTTP: parsed line  gzip
1w1d: HTTP: parsed extension Accept-Language
1w1d: HTTP: parsed line  en
1w1d: HTTP: parsed extension Accept-Charset
1w1d: HTTP: parsed line  iso-8859-1,*,utf-8
1w1d: HTTP: parsed extension Authorization
1w1d: HTTP: parsed authorization type Basic
1w1d: HTTP: Authentication for url '/' '/' level 15  privless '/'
1w1d: HTTP: Authentication username = 'maurizio' priv-level = 15 auth-type = aaa
1w1d: HTTP: received GET ''
```

以下實驗顯示，來自VPN網路的HTTP流量可以到達伺服器群（注意地址10.1.1.1）。

```
1w1d: HTTP: parsed uri '/'
1w1d: HTTP: processing URL '/' from host 10.1.1.1
1w1d: HTTP: client version 1.0
1w1d: HTTP: parsed extension Connection
1w1d: HTTP: parsed line  Keep-Alive
1w1d: HTTP: parsed extension User-Agent
1w1d: HTTP: parsed line  Mozilla/4.76 [en] (Windows NT 5.0; U)
1w1d: HTTP: parsed extension Host
1w1d: HTTP: parsed line  172.16.65.202
1w1d: HTTP: parsed extension Accept\
1w1d: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
1w1d: HTTP: parsed extension Accept-Encoding
1w1d: HTTP: parsed line  gzip
1w1d: HTTP: parsed extension Accept-Language
1w1d: HTTP: parsed line  en
1w1d: HTTP: parsed extension Accept-Charset
1w1d: HTTP: parsed line  iso-8859-1,*,utf-8
1w1d: HTTP: Authentication for url '/' '/' level 15  privless '/'
1w1d: HTTP: authentication required, no authentication information was provided
```

以下是VPN集中器的配置：

```
[ IP Ethernet 0:0 ]
ipbroadcast = 172.16.65.255
mode = routedSubnetMask = 255.255.255.240
IPAddress               = 172.16.65.203

[ General ]
IPsecGateway = 198.5.6.1
DeviceName              = "VPN5008"
EnablePassword          = "ww"
Password                = "ww"
EthernetAddress         = 00:30:85:14:5c:40
DeviceType              = VPN 5002/8
ConcentratorConfiguredOn            = Timeserver not configured
ConfiguredFrom          = Command Line, from 171.68.173.3

[ IP Static ]
206.1.1.0 255.255.255.0
198.5.6.1 10.0.0.0
0.0.0.0 172.16.65.193 1

[ IP Ethernet 1:0 ]
ipbroadcast = 172.16.65.255
mode = routedSubnetMask              = 255.255.255.0
IPAddress               = 198.5.6.203

[ IKE Policy ]
```

```
Protecction = MD5_DES_G1

[ VPN Group "RemoteUsers" ]
maxconnections = 10IPNet                    = 172.16.65.0/24
LocalIPNet              = 10.1.1.0/24
Transform = esp(des,md5)

[ VPN Users ]
martin Config="RemoteUsers"
SharedKey="mysecretkey"
maurizio Config="RemoteUsers"
SharedKey="mysecretkey"
```

以下命令顯示連線的使用者清單：

```
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
```

請注意，伺服器上的預設閘道是內部路由器172.16.65.193，其會發出一個icmp重新導向到172.16.65.203。此實作會導致非最佳流量流，因為主機會將流量的第一個封包傳送到路由器，並在收到重新導向時，會將後續封包傳送到更適合處理此流量的閘道。或者，您也可以在伺服器自身配置兩個不同的路由，以便為10.x.x.x地址指向VPN，為其餘流量指向172.16.65.193。如果伺服器上只設定了預設閘道，則需要確保路由器介面已設定為「ip redirect」。

我們在測試期間注意到的一個有趣點是以下一點。如果嘗試從伺服器或VPN對外部位址（例如198.5.6.1）執行**ping**，則預設閘道會傳送並icmp重新導向至172.16.65.201。

```
Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds:
1w1d: ICMP: redirect rcvd from 172.16.65.193 -- for 198.5.6.1 use gw 172.16.65.201.
1w1d: ICMP: redirect rcvd from 172.16.65.193 -- for 198.5.6.1 use gw 172.16.65.201.
1w1d: ICMP: redirect rcvd from 172.16.65.193 -- for 198.5.6.1 use gw 172.16.65.201.
1w1d: ICMP: redirect rcvd from 172.16.65.193 -- for 198.5.6.1 use gw 172.16.65.201.
1w1d: ICMP: redirect rcvd from 172.16.65.193 -- for 198.5.6.1 use gw 172.16.65.201.
Success rate is 0 percent (0/5)
```

此時，伺服器或VPN將傳送對172.16.65.201的地址解析協定(ARP)請求，並且不會從201獲得任何響應，因為它位於另一個輔助VLAN上；這就是PVLAN為我們提供的功能。實際上，有一個簡單的方法可以繞過它，那就是將流量傳送到MAC .193，目的IP為172.16.65.201。

路由器。193會將流量路由回同一個介面，但由於路由器介面是一個混雜埠，因此流量將到達。201，這是我們希望阻止的。此問題已在VACL和PVLAN的已知限制一節中說明。

VACL配置

本節對於提高伺服器群的安全性至關重要。如已知的VACL和PVLAN限制一節所述，即使伺服器和PIX屬於兩個不同的輔助VLAN，仍然可以使用一種方法來讓它們相互通訊。如果他們嘗試直接通訊，則由於PVLAN而無法進行通訊。如果伺服器受到攻擊，然後被入侵者以相同子網的流量傳送到路由器的方式配置，該入侵者會將流量路由回同一子網，從而破壞PVLAN的用途。

因此，需要使用以下策略在主VLAN（傳送來自路由器的流量的VLAN）上配置VACL:

- 允許來源IP為路由器IP的流量
- 拒絕源IP和目標IP均為伺服器群子網的資料流

- 允許所有其餘流量

```
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不會影響伺服器和PIX生成的流量；這只會防止路由器將來自伺服器的流量路由回同一個VLAN。前兩條語句允許路由器向伺服器傳送icmp重定向或icmp無法到達等消息。

我們確定了管理員可能希望通過VACL停止的另一個流量，而且此流量是從內部網路到VPN主機。為此，可以將VACL對映到主VLAN(41)，並與前一個VLAN組合：

```
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
```

測試配置

現在，我們正從路由器。193(zundapp)對10.1.1.1主機執行ping操作。 對映VACL之前，ping操作是成功的。

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

在VLAN 41上對映VACL後，同一ping不會成功：

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

但是我們仍可以ping外部路由器：

```
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 = 100/171/192 ms
```

相關資訊

- 配置訪問控制清單 — Catalyst 6000文檔
- 技術支援 - Cisco Systems