Sicherung von Netzwerken mit privaten VLANs und VLAN-Zugriffskontrolllisten

Inhalt

Einführung

Einer der Schlüsselfaktoren für ein erfolgreiches Netzwerksicherheitsdesign ist die Identifizierung und Durchsetzung eines geeigneten Vertrauensmodells. Das richtige Vertrauensmodell definiert, wer mit wem sprechen muss und welche Art von Datenverkehr ausgetauscht werden muss. der restliche Datenverkehr sollte abgelehnt werden. Nachdem das richtige Vertrauensmodell identifiziert wurde, sollte der Sicherheitsdesigner entscheiden, wie das Modell durchgesetzt werden soll. Da weltweit immer mehr wichtige Ressourcen verfügbar sind und sich neue Formen von Netzwerkangriffen entwickeln, wird die Netzwerksicherheitsinfrastruktur tendenziell komplexer, und es stehen mehr Produkte zur Verfügung. Firewalls, Router, LAN-Switches, Intrusion Detection-Systeme, AAA-Server und VPNs sind einige der Technologien und Produkte, die bei der Durchsetzung dieses Modells helfen können. Natürlich spielt jedes dieser Produkte und Technologien eine besondere Rolle bei der allgemeinen Sicherheitsimplementierung, und es ist wichtig, dass der Designer weiß, wie diese Elemente bereitgestellt werden können.

Vorbereitungen

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Voraussetzungen

Dieses Dokument beschreibt PVLAN-Konfigurationen auf Switches, auf denen CatOS ausgeführt wird. Beispiele für die parallele Konfiguration von PVLANs auf Switches mit Cisco IOS und CatOS finden Sie im Dokument Configuring Isolated Private VLANs on Catalyst Switches.

Nicht alle Switches und Softwareversionen unterstützen PVLANs. In der Private VLAN Catalyst Switch Support Matrix finden Sie Informationen dazu, ob Ihre Plattform- und Softwareversion PVLANs unterstützt.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Hintergrundinformationen

Die Identifizierung und Durchsetzung eines geeigneten Vertrauensmodells scheint eine sehr einfache Aufgabe zu sein, doch nach mehreren Jahren der Unterstützung von Sicherheitsimplementierungen deuten unsere Erfahrungen darauf hin, dass Sicherheitsvorfälle häufig mit schlechten Sicherheitsdesigns zusammenhängen. In der Regel sind diese schlechten Designs eine direkte Folge der Nichtdurchsetzung eines angemessenen Vertrauensmodells, manchmal weil das, was einfach notwendig ist, nicht verstanden wird, in anderen Fällen nur, weil die beteiligten Technologien nicht vollständig verstanden werden oder missbraucht werden.

In diesem Dokument wird ausführlich erläutert, wie zwei in unseren Catalyst Switches verfügbare Funktionen, Private VLANs (PVLANs) und VLAN Access Control Lists (VACLs), dazu beitragen können, ein angemessenes Vertrauensmodell sowohl in Enterprise- als auch in Service Provider-Umgebungen sicherzustellen.

Durchsetzung eines angemessenen Vertrauensmodells

Eine unmittelbare Folge der fehlenden Durchsetzung eines angemessenen Vertrauensmodells besteht darin, dass die Implementierung der Sicherheitsfunktionen insgesamt weniger immun gegen schädliche Aktivitäten wird. Demilitarisierte Zonen (DMZs) werden in der Regel implementiert, ohne die richtigen Richtlinien durchzusetzen, was die Aktivität eines potenziellen Eindringlings erleichtert. In diesem Abschnitt wird analysiert, wie häufig DMZs implementiert werden und welche Folgen ein schlechtes Design hat. Wir werden später erklären, wie diese Folgen gemildert oder im besten Fall vermieden werden können.

In der Regel verarbeiten DMZ-Server nur eingehende Anfragen aus dem Internet und initiieren schließlich Verbindungen zu einigen Back-End-Servern in einem internen oder anderen DMZ-Segment, z. B. einem Datenbankserver. Gleichzeitig sollen DMZ-Server nicht miteinander kommunizieren oder Verbindungen mit der Außenwelt herstellen. Dadurch werden die erforderlichen Datenverkehrsflüsse in einem einfachen Vertrauensmodell klar definiert. Wir sehen jedoch häufig, dass diese Art von Modell nicht ausreichend durchgesetzt wird.

Designer neigen in der Regel dazu, DMZs mithilfe eines gemeinsamen Segments für alle Server zu implementieren, ohne dass die Steuerung des Datenverkehrs zwischen diesen Servern erforderlich ist. Beispielsweise befinden sich alle Server in einem gemeinsamen VLAN. Da der Datenverkehr innerhalb desselben VLAN nicht kontrolliert wird, kann bei einer Beeinträchtigung eines Servers derselbe Server ausgenutzt werden, um einen Angriff auf einen der Server und

Hosts desselben Segments auszulösen. Dies erleichtert die Aktivität potenzieller Eindringlinge, die eine Port-Umleitung oder einen Angriff auf die Anwendungsebene durchführen.

In der Regel werden Firewalls und Paketfilter nur zur Steuerung eingehender Verbindungen verwendet. Verbindungen, die von der DMZ ausgehen, werden jedoch in der Regel nicht eingeschränkt. Vor einiger Zeit gab es eine bekannte Schwachstelle in einem cgi-bin-Skript, die es einem Eindringling ermöglichte, eine X-term-Sitzung durch das Senden eines HTTP-Streams zu starten. Dies ist Datenverkehr, der von der Firewall zugelassen werden sollte. Wenn der Eindringling das Glück hatte, konnte er oder sie einen anderen behandeln, um eine Root-Eingabeaufforderung zu erhalten, in der Regel eine Art Pufferüberlaufangriff. In den meisten Fällen können solche Probleme durch die Durchsetzung eines angemessenen Vertrauensmodells vermieden werden. Erstens sollen Server nicht miteinander kommunizieren, und zweitens sollten keine Verbindungen von diesen Servern zur Außenwelt hergestellt werden.

Dieselben Kommentare gelten für viele andere Szenarien, von jedem normalen nicht vertrauenswürdigen Segment bis hin zu Serverfarmen bei Anwendungs-Service-Providern.

PVLANs und VACLs auf Catalyst-Switches können ein geeignetes Vertrauensmodell gewährleisten. PVLANs helfen, indem sie den Datenverkehr zwischen Hosts in einem gemeinsamen Segment beschränken, während VACLs dazu beitragen, indem sie eine weitere Kontrolle über jeden Datenverkehrsfluss bieten, der von einem bestimmten Segment ausgeht oder für dieses bestimmt ist. Diese Features werden in den folgenden Abschnitten erläutert.

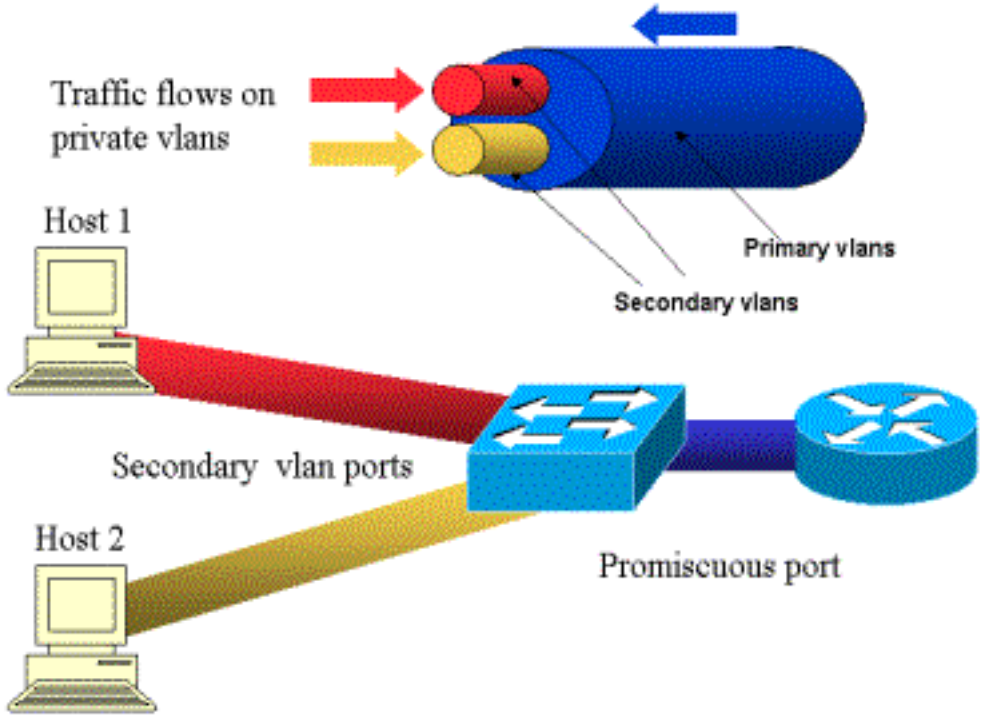
Private VLANs

PVLANs sind auf dem Catalyst 6000 mit CatOS 5.4 oder höher, auf den Catalyst Switches 4000, 2980G, 2980G-A, 2948G und 4912G mit CatOS 6.2 oder höher verfügbar.

Aus unserer Sicht sind PVLANs ein Tool, das die Trennung des Datenverkehrs auf Layer 2 (L2) ermöglicht, das ein Broadcast-Segment in ein nicht-Broadcast-Segment mit mehreren Access-Zugangspunkten verwandelt. Der Datenverkehr, der von einem Promiscuous-Port zu einem Switch gelangt (d. h. ein Port, der sowohl primäre als auch sekundäre VLANs weiterleiten kann), kann an allen Ports ausgeführt werden, die demselben primären VLAN angehören. Datenverkehr, der von einem einem einem sekundären VLAN zugeordneten Port zu einem Switch gelangt (entweder ein isoliertes, ein Community- oder ein bidirektionales Community-VLAN), kann an einen Promiscuous-Port oder an einen Port weitergeleitet werden, der zum selben Community-VLAN gehört. Mehrere Ports, die demselben isolierten VLAN zugeordnet sind, können keinen Datenverkehr austauschen.

Das folgende Bild zeigt das Konzept.

Abbildung 1: Private VLANs



Das primäre VLAN wird blau dargestellt. die sekundären VLANs sind rot und gelb dargestellt. Host 1 ist mit einem Port des Switches verbunden, der zum roten sekundären VLAN gehört. Host 2 ist mit einem Switch-Port verbunden, der zum gelben sekundären VLAN gehört.

Wenn ein Host überträgt, wird der Datenverkehr im sekundären VLAN übertragen. Wenn z. B. Host-2 überträgt, wird der Datenverkehr gelb im VLAN übertragen. Wenn diese Hosts empfangen, kommt der Datenverkehr vom blauen VLAN, dem primären VLAN.

Die Ports, mit denen Router und Firewalls verbunden sind, sind Promiscuous-Ports, da diese Ports Datenverkehr weiterleiten können, der von jedem in der Zuordnung definierten sekundären VLAN sowie vom primären VLAN eingeht. Die mit den einzelnen Hosts verbundenen Ports können nur den Datenverkehr weiterleiten, der vom primären VLAN und dem sekundären VLAN stammt, das für diesen Port konfiguriert wurde.

Die Zeichnung stellt die privaten VLANs als verschiedene Leitungen dar, die Router und Hosts verbinden: Die Leitung, die alle anderen Pakete bündelt, ist das primäre VLAN (blau), und der Datenverkehr im VLAN ist blau und fließt von den Routern zu den Hosts. Die internen Pipes für das primäre VLAN sind die sekundären VLANs, und der Datenverkehr, der über diese Pipes fließt, verläuft von den Hosts zum Router.

Wie das Bild zeigt, kann ein primäres VLAN ein oder mehrere sekundäre VLANs bündeln.

In diesem Dokument haben wir bereits darauf hingewiesen, dass PVLANs dazu beitragen, das richtige Vertrauensmodell durchzusetzen, indem sie einfach die Trennung von Hosts innerhalb eines gemeinsamen Segments sicherstellen. Nachdem wir nun mehr über Private VLANs wissen, möchten wir uns ansehen, wie dies in unserem ursprünglichen DMZ-Szenario implementiert werden kann. Server sollen nicht miteinander kommunizieren, aber sie müssen trotzdem mit der Firewall oder dem Router kommunizieren, mit der sie verbunden sind. In diesem Fall sollten Server mit isolierten Ports verbunden werden, während Router und Firewalls mit Promiscuous-Ports verbunden werden sollten. Wenn einer der Server kompromittiert wird, kann der Eindringling nicht denselben Server verwenden, um einen Angriff auf einen anderen Server innerhalb

desselben Segments auszulösen. Der Switch verwirft jedes Paket mit Leitungsgeschwindigkeit ohne Leistungseinbußen.

Ein weiterer wichtiger Hinweis ist, dass diese Art von Steuerung nur auf dem L2-Gerät implementiert werden kann, da alle Server demselben Subnetz angehören. Eine Firewall oder ein Router kann nichts tun, da Server versuchen, direkt zu kommunizieren. Eine weitere Option besteht darin, einen Firewall-Port pro Server zu reservieren. Dies ist jedoch wahrscheinlich zu teuer, schwierig zu implementieren und nicht skalierbar.

In einem späteren Abschnitt werden einige andere typische Szenarien beschrieben, in denen Sie diese Funktion verwenden können.

VLAN-Zugriffskontrolllisten

VACLs sind auf der Catalyst 6000-Serie mit CatOS 5.3 oder höher verfügbar.

VACLs können auf einem Catalyst 6500 mit L2 ohne Router konfiguriert werden (Sie benötigen nur eine Policy Feature Card (PFC)). Sie werden mit Leitungsgeschwindigkeit durchgesetzt, sodass bei der Konfiguration von VACLs auf einem Catalyst 6500 keine Leistungseinbußen entstehen. Da die Suche nach VACLs in der Hardware erfolgt, bleibt die Weiterleitungsrate unabhängig von der Größe der Zugriffsliste unverändert.

VACLs können Primär- oder Sekundär-VLANs separat zugeordnet werden. Wenn eine VACL auf einem sekundären VLAN konfiguriert ist, kann der von Hosts generierte Datenverkehr gefiltert werden, ohne den von Routern oder Firewalls generierten Datenverkehr zu berühren.

Durch die Kombination von VACLs und privaten VLANs ist es möglich, Datenverkehr basierend auf der Richtung des Datenverkehrs selbst zu filtern. Wenn beispielsweise zwei Router mit demselben Segment wie einige Hosts (z. B. Server) verbunden sind, können VACLs in sekundären VLANs konfiguriert werden, sodass nur der von den Hosts generierte Datenverkehr gefiltert wird, während der zwischen den Routern ausgetauschte Datenverkehr unberührt bleibt.

VACLs können problemlos bereitgestellt werden, um das richtige Vertrauensmodell durchzusetzen. Lassen Sie uns den Fall DMZ analysieren. Server in der DMZ sollen nur eingehende Verbindungen versorgen, und es wird nicht erwartet, dass sie Verbindungen zur Außenwelt initiieren. Eine VACL kann auf das sekundäre VLAN angewendet werden, um den Datenverkehr zu steuern, der von diesen Servern ausgeht. Bei Verwendung von VACLs ist unbedingt zu beachten, dass der Datenverkehr in der Hardware verworfen wird, sodass weder die CPU des Routers noch der Switch betroffen sind. Selbst wenn einer der Server an einem DDoS-Angriff (Distributed Denial of Service) beteiligt ist, verwirft der Switch den gesamten unzulässigen Datenverkehr mit Leitungsgeschwindigkeit, ohne Leistungseinbußen. Ähnliche Filter können im Router oder in der Firewall angewendet werden, mit dem Server verbunden sind. Dies hat jedoch in der Regel schwerwiegende Auswirkungen auf die Leistung.

MAC-basierte ACLs funktionieren nicht gut mit IP-Datenverkehr, daher werden VACLs zur Überwachung/Verfolgung von PVLANs empfohlen.

Bekannte Einschränkungen von VACLs und PVLANs

Beim Konfigurieren der Filterung mit VACLs sollten Sie sorgfältig auf die Fragment-Verarbeitung auf der PFC achten und die Konfiguration entsprechend der Hardware-Spezifikation anpassen.

Angesichts des Hardwaredesigns der PFC von Supervisor 1 des Catalyst 6500 ist es besser, die ICMP-Fragmente explizit abzulehnen. Der Grund hierfür ist, dass die Hardware die ICMP-Fragmente (Internet Control Message Protocol) und die Echo-Antwort (Echo-Response) als identisch betrachtet und die Hardware standardmäßig so programmiert ist, dass sie Fragmente explizit zulassen. Wenn Sie also verhindern möchten, dass Echo-Antwort-Pakete die Server verlassen, müssen Sie dies explizit mit der Zeile **deny icmp any fragment** konfigurieren. Dies wird bei den Konfigurationen in diesem Dokument berücksichtigt.

Es gibt eine bekannte Sicherheitsbeschränkung für PVLANs. Hierbei handelt es sich um die Möglichkeit, dass ein Router Datenverkehr aus demselben Subnetz weiterleitet, aus dem er stammt. Ein Router kann den Datenverkehr über isolierte Ports weiterleiten, die den Zweck von PVLANs nicht erfüllen. Diese Einschränkung ist darauf zurückzuführen, dass PVLANs ein Tool sind, das Isolierung auf L2 und nicht auf Layer 3 (L3) ermöglicht.

Unicast Reverse Path Forwarding (uRPF) funktioniert nicht gut mit PVLAN-Host-Ports, daher darf uRPF nicht in Kombination mit PVLAN verwendet werden.

Dieses Problem lässt sich beheben, indem die auf den primären VLANs konfigurierten VACLs verwendet werden. Die Fallstudie enthält die VACLs, die im primären VLAN konfiguriert werden müssen, um den Datenverkehr vom gleichen Subnetz zu verwerfen, der an dasselbe Subnetz zurückgeleitet wird.

Auf einigen Linecards unterliegt die Konfiguration von PVLAN-Zuordnungen/Karten/Trunking-Ports bestimmten Einschränkungen, bei denen mehrere PVLAN-Zuordnungen zu unterschiedlichen Port Application-Specific Integrated Circuits (ASICs) gehören müssen, um konfiguriert zu werden. Diese Einschränkungen werden auf dem neuen Port ASIC Coil3 entfernt. Weitere Informationen zur Softwarekonfiguration finden Sie in der aktuellen Dokumentation zu Catalyst-Switches.

Fallstudien

Im folgenden Abschnitt werden drei Fallstudien beschrieben, die unserer Meinung nach für die meisten Implementierungen repräsentativ sind. Außerdem werden die Details zur Bereitstellung von PVLANs und VACLs für die Sicherheit erläutert.

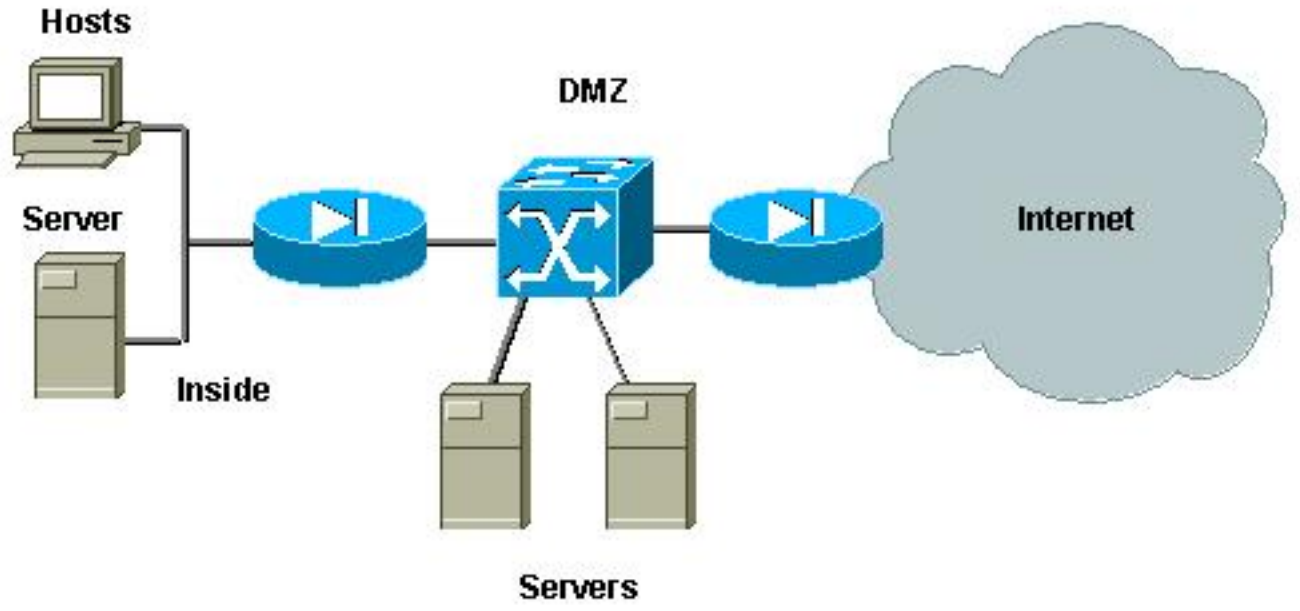
Folgende Szenarien sind möglich:

- Passthrough-DMZ
- Externe DMZ
- Paralleler VPN-Concentrator zur Firewall

Passthrough-DMZ

Dies ist eines der am häufigsten verwendeten Szenarien. In diesem Beispiel wird die DMZ als Transit-Bereich zwischen zwei Firewall-Routern implementiert, wie in der Abbildung unten gezeigt.

Abbildung 2: Passthrough-DMZ



In diesem Beispiel sollen sowohl externe als auch interne Benutzer auf DMZ-Server zugreifen, aber sie müssen nicht miteinander kommunizieren. In einigen Fällen müssen DMZ-Server eine Verbindung zu einem internen Host herstellen. Gleichzeitig sollen interne Clients ohne Einschränkungen auf das Internet zugreifen können. Ein gutes Beispiel hierfür sind Webserver in der DMZ, die mit einem Datenbankserver im internen Netzwerk kommunizieren müssen und interne Clients auf das Internet zugreifen.

Die externe Firewall ist so konfiguriert, dass eingehende Verbindungen zu den Servern in der DMZ zugelassen werden. In der Regel werden jedoch keine Filter oder Einschränkungen auf den ausgehenden Datenverkehr angewendet, insbesondere auf den Datenverkehr, der von der DMZ ausgeht. Wie bereits in diesem Dokument erläutert, kann dies die Aktivität eines Angreifers aus zwei Gründen vereinfachen: Beim ersten werden alle anderen DMZ-Hosts verfügbar gemacht, sobald einer der DMZ-Hosts kompromittiert ist. Zweitens kann ein Angreifer eine ausgehende Verbindung leicht ausnutzen.

Da DMZ-Server nicht miteinander kommunizieren müssen, wird empfohlen, sicherzustellen, dass sie bei L2 isoliert sind. Die Server-Ports werden als isolierte PVLANs-Ports definiert, während die Ports, die mit den beiden Firewalls verbunden sind, als "Promiscuous" definiert werden. Durch das Definieren eines primären VLAN für die Firewalls und eines sekundären VLAN für die DMZ-Server wird dies erreicht.

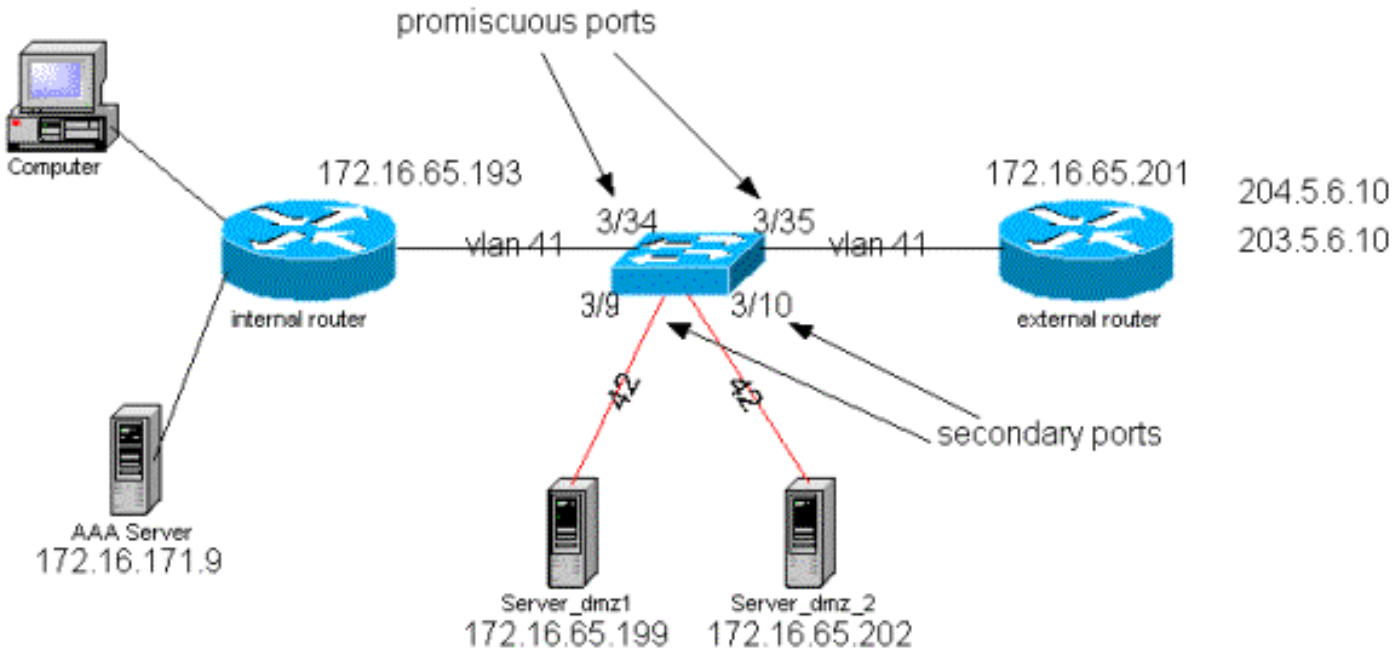
VACLs dienen zur Steuerung des von der DMZ stammenden Datenverkehrs. Dies verhindert, dass ein Angreifer eine unberechtigte ausgehende Verbindung öffnen kann. Es ist wichtig, zu beachten, dass DMZ-Server nicht nur mit dem Datenverkehr antworten müssen, der den Client-Sitzungen entspricht, sondern auch einige zusätzliche Services benötigen, wie Domain Name System (DNS) und Maximum Transmission Unit (MTU) Path Discovery. Daher sollte die ACL alle Services zulassen, die von den DMZ-Servern benötigt werden.

Testen der Passthrough-DMZ

In unserer Testumgebung wurde ein DMZ-Segment implementiert, in dem zwei Router als Bettserver konfiguriert wurden: server_dmz1 und server_dmz2. Der Zugriff auf diese Server soll sowohl von außen als auch von internen Clients erfolgen, und alle HTTP-Verbindungen werden

über einen internen RADIUS-Server (CiscoSecure ACS für UNIX) authentifiziert. Sowohl interne als auch externe Router werden als Paketfilter-Firewalls konfiguriert. Die folgende Abbildung zeigt die Testumgebung mit dem verwendeten Adressierungsschema.

Abbildung 3: Test-Bed: Passthrough-DMZ



In der folgenden Liste sind die grundlegenden Konfigurationsschritte für PVLANs aufgeführt. Der Catalyst 6500 wird als L2-Switch in der DMZ verwendet.

- Server_dmz_1 ist mit Port 3/9 verbunden
- Server_dmz_2 ist an Port 3/10 angeschlossen
- Der interne Router ist an Port 3/34 angeschlossen.
- Der externe Router ist mit Port 3/35 verbunden.

Wir haben die folgenden VLANs ausgewählt:

- 41 ist das primäre VLAN.
- 42 ist das isolierte VLAN.

Private VLAN-Konfiguration

Die folgende Konfiguration legt die PVLANs für die betreffenden Ports fest.

```
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
```

VACL-Konfiguration im primären VLAN

Dieser Abschnitt ist zur Verbesserung der Sicherheit der DMZ von entscheidender Bedeutung. Wie im Abschnitt "Bekannte Grenzen von VACLs und PVLANs" beschrieben, besteht selbst wenn Server zu zwei verschiedenen sekundären VLANs oder zu demselben isolierten VLAN gehören, ein Angreifer immer noch die Möglichkeit, sie miteinander zu kommunizieren. Wenn die Server versuchen, direkt zu kommunizieren, können sie dies aufgrund der PVLANs nicht mit L2 tun. Wenn die Server kompromittiert und dann von einem Eindringling so konfiguriert werden, dass der Datenverkehr für dasselbe Subnetz an den Router gesendet wird, leitet dieser den Datenverkehr zurück in das gleiche Subnetz und besiegelt damit den Zweck der PVLANs.

Daher muss eine VACL im primären VLAN (dem VLAN, das den Datenverkehr von den Routern überträgt) mit den folgenden Richtlinien konfiguriert werden:

- Zulassen des Datenverkehrs, dessen Quell-IP die IP des Routers ist
- Verweigern des Datenverkehrs, wobei Quell- und Ziel-IPs das DMZ-Subnetz sind
- Zulassen des gesamten restlichen Datenverkehrs

```
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
```

Diese ACL hat keine Auswirkungen auf den von den Servern generierten Datenverkehr. wird nur verhindert, dass die Router den Datenverkehr von den Servern zurück zum selben VLAN leiten. Die ersten beiden Anweisungen ermöglichen es den Routern, Meldungen wie icmp redirect oder icmp unreachable an die Server zu senden.

VACL-Konfiguration im sekundären VLAN

Die folgenden Konfigurationsprotokolle zeigen, wie eine VACL eingerichtet wird, um den von den Servern generierten Datenverkehr zu filtern. Durch die Konfiguration dieser VACL soll Folgendes erreicht werden:

- **Ping** von Servern zulassen (**echo** zulassen)
- Verhindern, dass **Echo**-Antworten die Server verlassen
- HTTP-Verbindungen von außen zulassen
- Zulassen von RADIUS-Authentifizierung (UDP-Port 1645) und Abrechnung (UDP-Port 1646)
- DNS-Datenverkehr zulassen (UDP-Port 53)

Wir wollen den gesamten restlichen Verkehr verhindern.

Was die Fragmentierung angeht, so gehen wir im Serversegment von folgenden Aussagen aus:

- Die Server generieren keinen fragmentierten Datenverkehr.
- Die Server empfangen möglicherweise fragmentierten Datenverkehr.

Angesichts des Hardwaredesigns der PFC von Supervisor 1 des Catalyst 6500 ist es besser, die icmp-Fragmente explizit abzulehnen. Der Grund dafür ist, dass ICMP-Fragmente und Echo-Antworten von der Hardware als identisch betrachtet werden. Die Hardware ist standardmäßig so programmiert, dass sie Fragmente explizit zulassen. Wenn Sie also verhindern möchten, dass Echo-Antwort-Pakete die Server verlassen, müssen Sie dies explizit mit der Zeile **deny icmp any fragment** konfigurieren.

```
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
```

Testen der Konfiguration

Die folgende Ausgabe wurde erfasst, wenn PVLANs konfiguriert wurden, aber noch keine VACL angewendet wurden. Dieser Test zeigt, dass der Benutzer vom externen Router aus **Ping** an den internen Router und die Server senden kann.

```
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
```

Das folgende Beispiel zeigt, dass wir **Ping** von den Servern an das externe Netzwerk, das Standard-Gateway, aber nicht an die Server senden können, die zum selben sekundären VLAN gehören.

```
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)
```

Nach der Zuordnung der VACLs ist der **Ping** vom externen Router nicht mehr erfolgreich:

```
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)
```

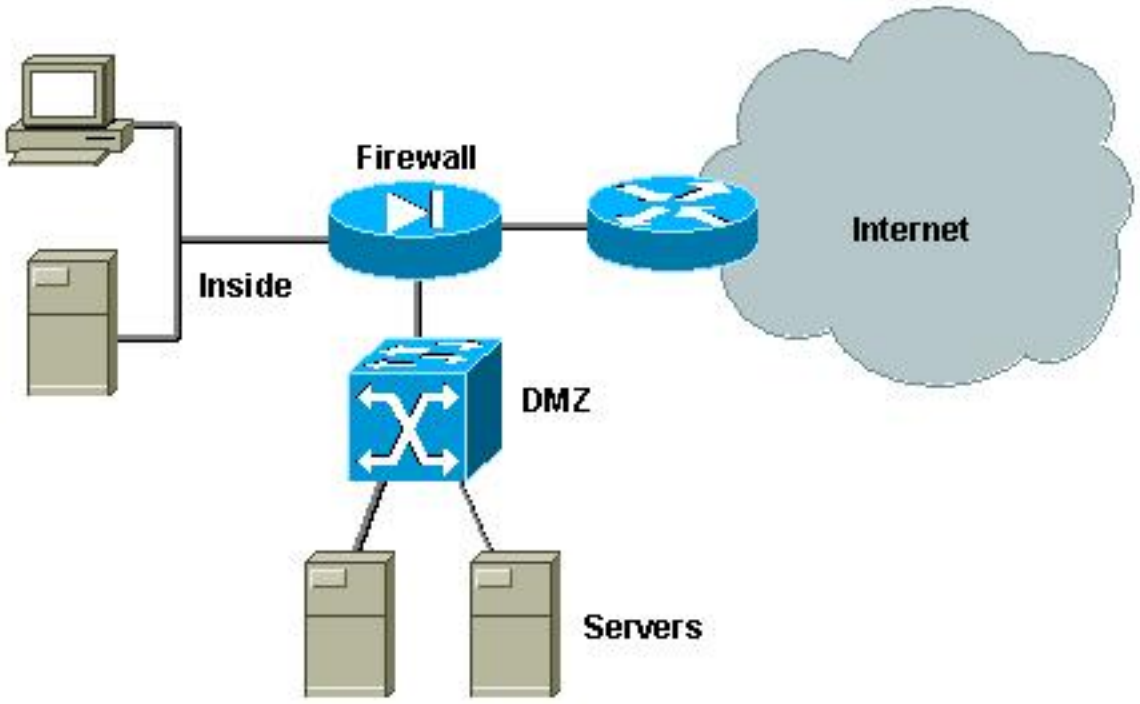
Das folgende Beispiel zeigt den Server, der HTTP GET-Anfragen vom internen Netzwerk empfängt:

```
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 ''
```

Externe DMZ

Das externe DMZ-Szenario ist wahrscheinlich die am weitesten verbreitete Implementierung. Eine externe DMZ wird mithilfe einer oder mehrerer Schnittstellen einer Firewall implementiert, wie in der folgenden Abbildung dargestellt.

Abbildung 4: Externe DMZ



In der Regel sind die Anforderungen für DMZs unabhängig von der Designimplementierung identisch. Wie im vorherigen Fall soll der Zugriff auf DMZ-Server sowohl von externen als auch vom internen Netzwerk aus möglich sein. DMZ-Server benötigen irgendwann Zugriff auf einige interne Ressourcen und sollten nicht miteinander kommunizieren. Gleichzeitig sollte kein Datenverkehr von der DMZ zum Internet initiiert werden. Diese DMZ-Server sollten nur mit Datenverkehr antworten, der eingehenden Verbindungen entspricht.

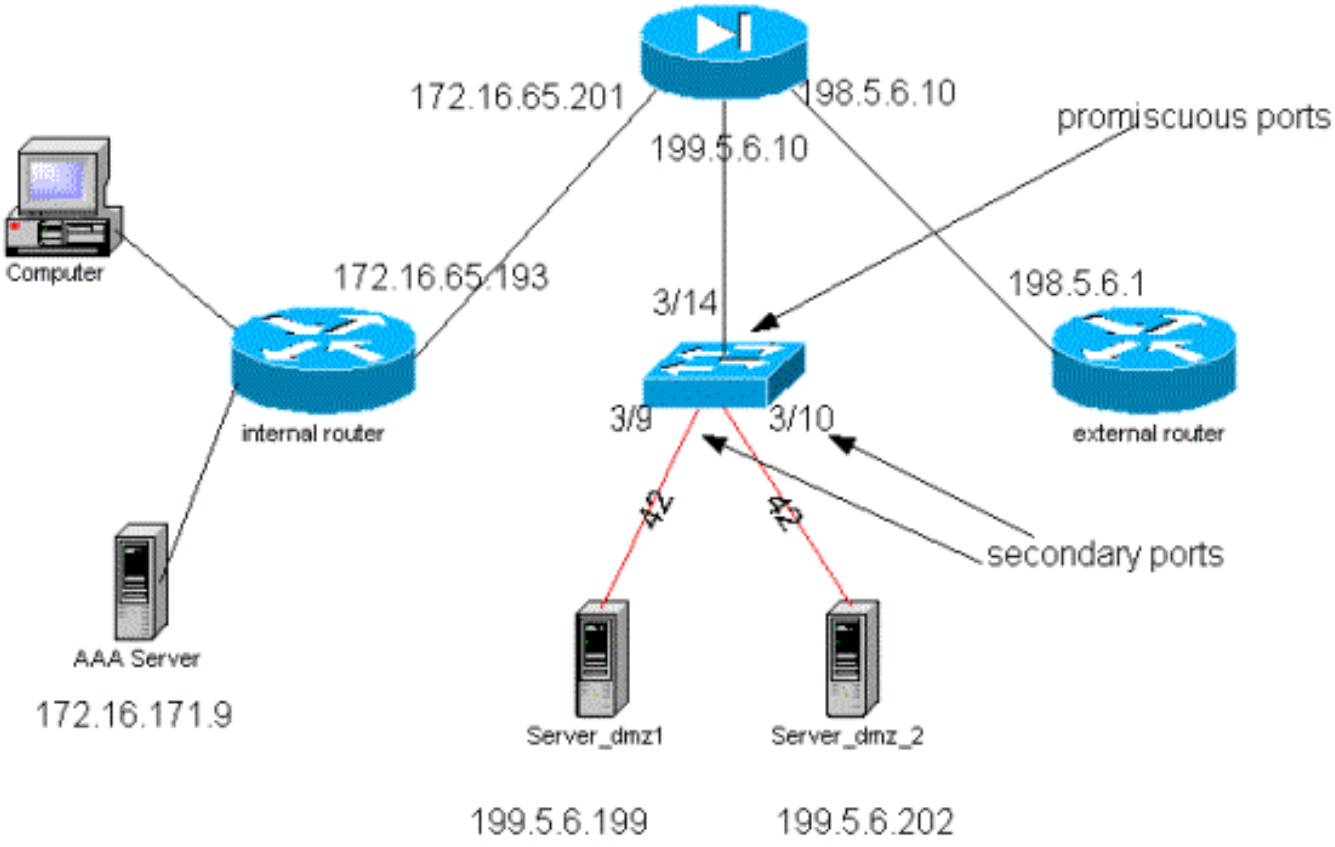
Wie in der vorherigen Fallstudie besteht der erste Konfigurationsschritt darin, mithilfe von PVLANs die Isolierung bei L2 zu erreichen und sicherzustellen, dass die DMZ-Server nicht miteinander kommunizieren können, während interne und externe Hosts darauf zugreifen können. Dies wird implementiert, indem die Server in einem sekundären VLAN mit isolierten Ports eingerichtet werden. Die Firewall sollte in einem primären VLAN mit einem Promiscuous-Port definiert werden. Die Firewall ist das einzige Gerät in diesem primären VLAN.

Im zweiten Schritt werden ACLs definiert, um den von der DMZ ausgehenden Datenverkehr zu steuern. Beim Definieren dieser ACLs müssen wir sicherstellen, dass nur der erforderliche Datenverkehr zugelassen wird.

Testen der externen DMZ

Die folgende Abbildung zeigt die für diese Fallstudie implementierte Testumgebung, in der eine PIX-Firewall mit einer dritten Schnittstelle für die DMZ verwendet wurde. Die gleichen Router werden wie Webserver verwendet, und alle HTTP-Sitzungen werden mit demselben RADIUS-Server authentifiziert.

Abbildung 5: Externe DMZ-Testumgebung



In diesem Szenario werden nur die interessanteren Auszüge aus den Konfigurationsdateien hinzugefügt, da die PVLANs- und VACL-Konfigurationen im vorherigen Anwenderbericht ausführlich erläutert wurden.

PIX-Konfiguration

```
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-Konfiguration

NAS-Konfiguration

```
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-Server-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-Konfiguration

Es ist zu beachten, dass in dieser Konfiguration keine VACL für das primäre VLAN konfiguriert

werden muss, da der PIX den Datenverkehr nicht über dieselbe Schnittstelle umleitet, von der er stammt. Eine VACL, wie in der VACL-Konfiguration im primären VLAN-Abschnitt beschrieben, ist redundant.

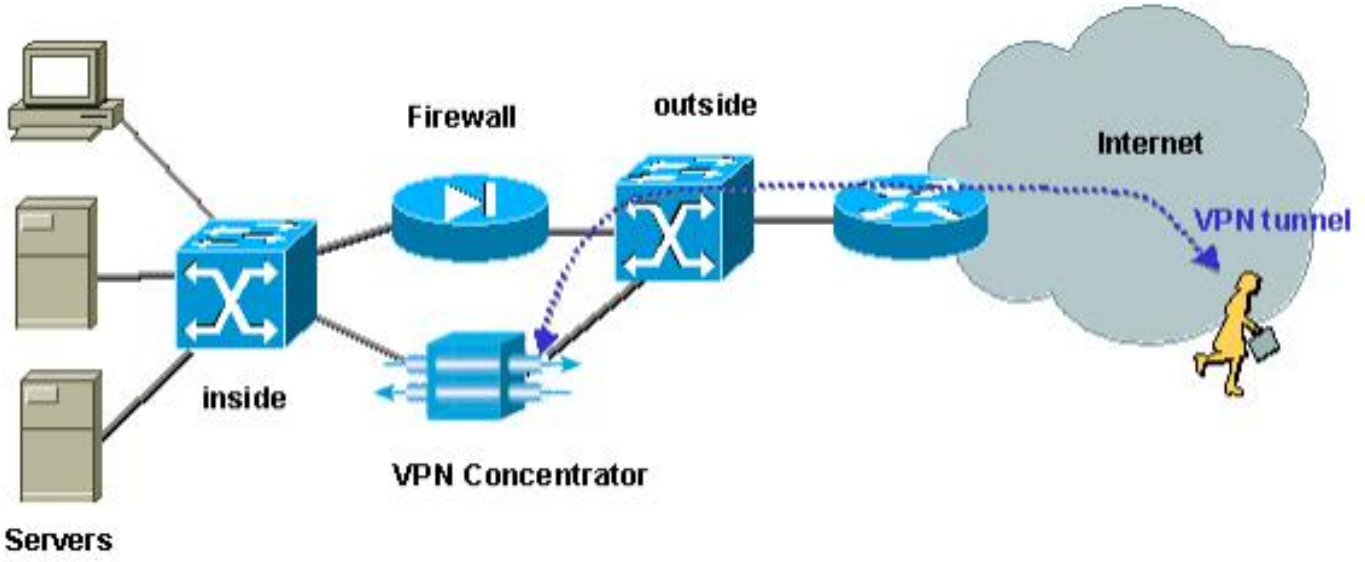
```
set security acl ip dmz_servers_out
------------------------------------------------
1. deny icmp any any fragment
2. permit icmp host 199.5.6.199 any echo
3. permit icmp host 199.5.6.202 any echo
4. permit tcp host 199.5.6.199 eq 80 any established
5. permit tcp host 199.5.6.202 eq 80 any established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

Paralleler VPN-Concentrator zur Firewall

Bei der Implementierung von Access Virtual Private Networks (VPNs) ist zweifellos einer der bevorzugten Ansätze das parallele Design (wie in der Abbildung unten gezeigt). Kunden bevorzugen diesen Designansatz in der Regel, da er einfach zu implementieren ist, sich kaum auf die bestehende Infrastruktur auswirkt und sich relativ einfach auf die Geräteflexibilität auswirkt.

Im parallelen Ansatz wird der VPN-Konzentrator sowohl mit Innen- als auch mit Außensegmenten verbunden. Alle VPN-Sitzungen enden am Konzentrator, ohne die Firewall zu durchlaufen. In der Regel wird von VPN-Clients erwartet, dass sie uneingeschränkten Zugriff auf das interne Netzwerk haben, aber manchmal kann ihr Zugriff auf eine Reihe von internen Servern (Serverfarm) beschränkt werden. Eine der wünschenswerten Funktionen besteht darin, den VPN-Datenverkehr vom regulären Internetdatenverkehr zu trennen, sodass z. B. VPN-Clients nicht über die Firewall des Unternehmens auf das Internet zugreifen dürfen.

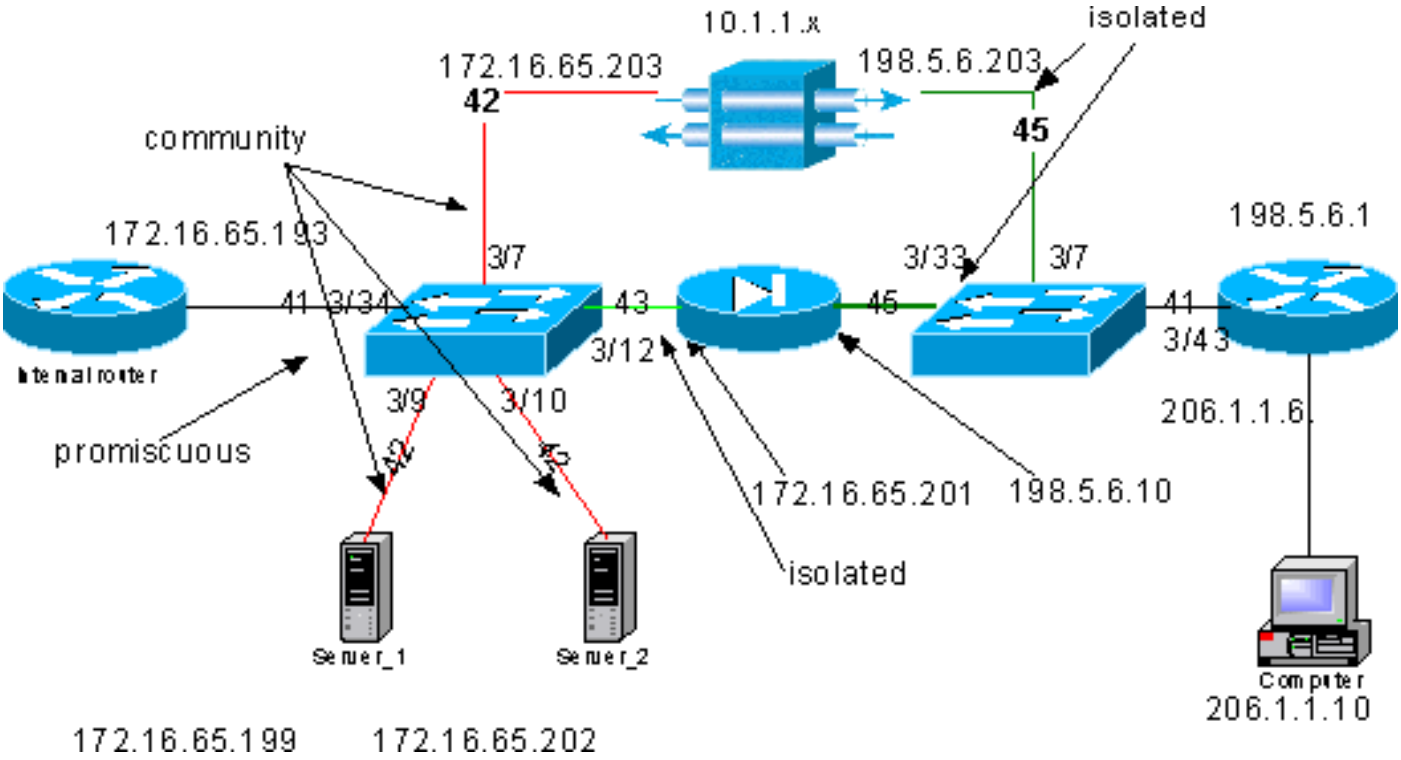
Abbildung 6: Paralleler VPN-Concentrator zur Firewall



Paralleles Testen des VPN-Concentrators mit der Firewall

In diesem Beispiel wurde ein VPN 500-Konzentrator verwendet, der parallel zu einer PIX-Firewall installiert wurde. Die beiden als Webserver konfigurierten Router wurden im internen Segment als interne Serverfarm installiert. VPN-Clients dürfen nur auf die Serverfarm zugreifen, und der Internetdatenverkehr sollte vom VPN-Datenverkehr (IPSec) getrennt werden. Die folgende Abbildung zeigt die Testumgebung.

Abbildung 7: VPN-Konzentrator parallel zur Firewall-Testumgebung



In diesem Szenario gibt es zwei Hauptbereiche:

- Interner L2-Switch
- Externer L2-Switch

Die Datenverkehrsflüsse für den internen L2-Switch werden anhand der folgenden Anweisungen definiert:

- VPN-Clients haben vollen Zugriff auf eine vordefinierte Gruppe interner Server (Serverfarm)
- Interne Clients können auch auf die Serverfarm zugreifen
- Interne Clients haben uneingeschränkten Zugriff auf das Internet
- Datenverkehr vom VPN-Konzentrator muss von der PIX-Firewall isoliert werden

Die Datenverkehrsflüsse für den externen L2-Switch werden wie folgt definiert:

- Datenverkehr vom Router muss entweder zum VPN-Konzentrator oder zum PIX-System geleitet werden können.
- Datenverkehr vom PIX muss vom VPN-Datenverkehr isoliert werden.

Außerdem kann der Administrator verhindern, dass Datenverkehr aus dem internen Netzwerk zu den VPN-Hosts gelangt. Dies kann mithilfe von VACLs erreicht werden, die im primären VLAN konfiguriert sind (die VACL filtert nur den Datenverkehr, der vom internen Router zurückgeht, kein anderer Datenverkehr wird davon betroffen).

PVLAN-Konfiguration

Da das Hauptziel dieses Designs darin besteht, den Datenverkehr des PIX vom Datenverkehr der Server und des VPN-Konzentrators getrennt zu halten, konfigurieren wir das PIX auf einem anderen PVLAN als dem PVLAN, auf dem die Server und der VPN-Konzentrator konfiguriert sind.

Der Datenverkehr aus dem internen Netzwerk muss auf die Serverfarm sowie den VPN-Konzentrator und den PIX zugreifen können. Folglich wird der Port, der mit dem internen Netzwerk verbunden ist, ein Promiscuous-Port sein.

Die Server und der VPN-Konzentrator gehören demselben sekundären VLAN an, da sie miteinander kommunizieren können.

Was den externen L2-Switch angeht, so ist der Router, der Zugriff auf das Internet gewährt (was normalerweise einem Internet Service Provider (ISP) angehört), mit einem Promiscuous-Port verbunden, während der VPN-Konzentrator und der PIX zu denselben privaten und isolierten VLANs gehören (sodass kein Datenverkehr ausgetauscht werden kann). Auf diese Weise kann der vom Service Provider stammende Datenverkehr entweder den Pfad zum VPN-Konzentrator oder den Pfad zum PIX nehmen. Der PIX- und VPN-Konzentrator sind besser geschützt, da sie isoliert sind.

PVLAN-Konfiguration des internen L2-Switches

```
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
```

PVLAN-Konfiguration des externen L2-Switches

```
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
```

Testen der Konfiguration

Dieses Experiment zeigt, dass der interne Router die Firewall passieren und den externen Router (den externen Firewall-Router, dessen Schnittstelle 198.5.6.1 ist) erreichen kann.

```
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
```

Dieses Experiment zeigt Folgendes, alles von Server 1:

- Server 1 kann einen Ping an den internen Router senden:
  ```
  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
  ```
- Server 1 kann VPN pingen:
  ```
  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
  ```
- Server 1 kann PIX-interne Schnittstelle nicht pingen:
  ```
  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)
  ```
- Server 1 kann keinen Ping an den externen Router senden:
  ```
  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)
  ```

Das folgende Experiment zeigt, dass HTTP-Sitzungen vom internen Netzwerk zur Serverfarm geöffnet werden können.

```
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 ''
```

Das folgende Experiment zeigt, dass der HTTP-Datenverkehr aus dem VPN-Netzwerk den Weg zur Serverfarm finden kann (beachten Sie die Adresse 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
```

Der VPN-Konzentrator wird wie folgt konfiguriert:

```
[ 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"
```

Der folgende Befehl zeigt die Liste der verbundenen Benutzer an:

```
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
```

Beachten Sie, dass das Standard-Gateway auf den Servern der interne Router 172.16.65.193 ist, der eine ICMP-Umleitung zu 172.16.65.203 ausgibt. Diese Implementierung führt zu nicht optimalen Datenverkehrsflüssen, da der Host das erste Paket eines Datenflusses an den Router sendet und beim Empfang der Umleitung die nachfolgenden Pakete an das Gateway sendet, das für diesen Datenverkehr besser geeignet ist. Alternativ kann man zwei verschiedene Routen auf den Servern selbst konfigurieren, um auf das VPN für die 10.x.x.x-Adressen und auf 172.16.65.193 für den restlichen Datenverkehr zu verweisen. Wenn auf den Servern nur das Standard-Gateway konfiguriert ist, müssen wir sicherstellen, dass die Router-Schnittstelle mit "ip redirect" konfiguriert ist.

Ein interessanter Punkt, den wir während des Tests bemerkten, ist der folgende. Wenn wir versuchen, eine externe Adresse wie 198.5.6.1 von den Servern oder vom VPN zu pingen, sendet das Standardgateway und icmp umgeleitet zu 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)
```

Die Server oder das VPN senden zu diesem Zeitpunkt eine ARP-Anfrage (Address Resolution Protocol) für 172.16.65.201 und erhalten keine Antwort ab 201, da es sich in einem anderen sekundären VLAN befindet. Das bietet uns das PVLAN. In Wirklichkeit gibt es eine einfache Möglichkeit, um diesen Vorgang zu umgehen, nämlich Datenverkehr an die MAC-Adresse von .193 und die Ziel-IP-Adresse von 172.16.65.201 zu senden.

Der Router 193 leitet den Datenverkehr zurück an die gleiche Schnittstelle. Da es sich bei der Router-Schnittstelle jedoch um einen Promiscuous-Port handelt, wird der Datenverkehr auf 0,201 ansteigen, was verhindert werden sollte. Dieses Problem wurde im Abschnitt "Bekannte Grenzen von VACLs und PVLANs" erläutert.

VACL-Konfiguration

Dieser Abschnitt ist für die Verbesserung der Sicherheit auf der Serverfarm von entscheidender Bedeutung. Wie im Abschnitt "Bekannte Grenzen von VACLs und PVLANs" beschrieben, gibt es, selbst wenn Server und PIX zu zwei verschiedenen sekundären VLANs gehören, noch eine Methode, mit der ein Angreifer sie miteinander kommunizieren lassen kann. Wenn sie versuchen, direkt zu kommunizieren, können sie dies aufgrund der PVLANs nicht tun. Wenn die Server kompromittiert und dann von einem Eindringling so konfiguriert werden, dass der Datenverkehr für dasselbe Subnetz an den Router gesendet wird, leitet dieser den Datenverkehr zurück in das gleiche Subnetz und besiegelt damit den Zweck der PVLANs.

Daher muss eine VACL im primären VLAN (dem VLAN, das den Datenverkehr von den Routern überträgt) mit den folgenden Richtlinien konfiguriert werden:

- Zulassen des Datenverkehrs, dessen Quell-IP die IP des Routers ist
- Den Datenverkehr verweigern, wobei Quell- und Ziel-IPs das Subnetz der Serverfarm darstellen
- Zulassen des gesamten restlichen Datenverkehrs

```
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
```

Diese ACL hat keine Auswirkungen auf den von den Servern oder vom PIX generierten Datenverkehr. wird nur verhindert, dass die Router den Datenverkehr von den Servern zurück zum selben VLAN leiten. Die ersten beiden Anweisungen ermöglichen es den Routern, Meldungen wie icmp redirect oder icmp unreachable an die Server zu senden.

Wir haben einen weiteren Datenverkehrsfluss identifiziert, den der Administrator mithilfe von VACLs stoppen möchte. Dieser Datenfluss verläuft vom internen Netzwerk zu den VPN-Hosts. Dazu kann eine VACL dem primären VLAN (41) zugeordnet und mit dem vorherigen VLAN kombiniert werden:

```
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
```

Testen der Konfiguration

Wir pingen jetzt den Host 10.1.1.1 vom Router 193 (zundapp). Bevor wir die VACL zuordnen, ist der **Ping** erfolgreich.

```
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
```

Nach der Zuordnung der VACL in VLAN 41 ist dasselbe **Ping** nicht erfolgreich:

```
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)
```

Dennoch können wir den externen Router **pingen**:

```
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
```

Zugehörige Informationen

- Konfigurieren von Zugriffskontrolllisten - Dokumentation für Catalyst 6000
- Technischer Support – Cisco Systems