PVLAN 및 VACL을 통한 보안 네트워크

목차

소개

성공적인 네트워크 보안 설계를 구축하기 위한 핵심 요소 중 하나는 적절한 신뢰 모델을 식별하고 적용하는 것입니다. 올바른 신뢰 모델은 교환해야 할 대상 및 트래픽 종류를 정의합니다. 다른 모든 트래픽은 거부해야 합니다. 적절한 신뢰 모델이 식별되면 보안 디자이너가 모델을 적용하는 방법을 결정해야 합니다. 전 세계적으로 더 많은 중요한 리소스가 사용 가능하고 새로운 형태의 네트워크 공격이 발전함에 따라 네트워크 보안 인프라는 더욱 정교해지고 더 많은 제품을 사용할 수 있게 됩니다. 방화벽, 라우터, LAN 스위치, 침입 탐지 시스템, AAA 서버, VPN은 모델을 적용하는 데 도움이 되는 기술 및 제품 중 일부입니다. 물론 이러한 제품 및 기술 각각은 전반적인 보안 구현 내에서 특정 역할을 수행하며 설계자가 이러한 요소를 어떻게 구축할 수 있는지 이해하는 것이 중요합니다.

시작하기 전에

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

사전 요구 사항

이 문서에서는 CatOS를 실행하는 스위치에서만 PVLAN 컨피그레이션에 대해 설명합니다. Cisco IOS 및 CatOS를 실행하는 스위치에서 PVLAN의 side-by-side 컨피그레이션 예는 Catalyst 스위치에서 Configuring Isolated Private VLANs(Isolated Private VLAN 구성) 문서를 참조하십시오.

모든 스위치와 소프트웨어 버전이 PVLAN을 지원하는 것은 아닙니다. 플랫폼 및 소프트웨어 버전이 PVLAN을 지원하는지 여부는 프라이빗 VLAN Catalyst 스위치 지원 매트릭스를 참조하십시오.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

배경 정보

적절한 신뢰 모델을 식별하고 적용하는 것은 매우 기본적인 작업인 것 같지만, 보안 구현을 몇 년 동안 지원하면서 보안 사고가 취약한 보안 설계와 관련이 있는 경우가 많습니다. 일반적으로 이러한 불량한 설계는 적절한 신뢰 모델을 시행하지 않는 직접적인 결과이며, 때로는 필요한 것이 이해되지 않는 경우가 있으며, 다른 경우에는 관련 기술이 완전히 이해되지 않거나 잘못 사용되기 때문입니다.

이 문서에서는 Catalyst 스위치에서 사용할 수 있는 두 가지 기능인 PVLAN(Private VLAN) 및 VACL(VLAN Access Control Lists)이 기업 및 통신 사업자 환경에서 적절한 신뢰 모델을 보장하는 데 어떻게 도움이 되는지 자세히 설명합니다.

올바른 신뢰 모델 구현의 중요성

적절한 신뢰 모델을 시행하지 않아 즉각적인 결과는 전반적인 보안 구현이 악의적인 활동에 대한 면역력을 약화시킨다는 것입니다. DMZ(Demilitarized Zones)는 적절한 정책을 시행하지 않고 일반적으로 구현되므로 잠재적 침입자의 활동을 촉진합니다. 이 섹션에서는 DMZ가 자주 구현되는 방식과 잘못된 설계의 결과를 분석합니다. 나중에 이러한 결과를 완화하는 방법 또는 최상의 경우 피하는 방법에 대해 설명하겠습니다.

일반적으로 DMZ 서버는 인터넷에서 들어오는 요청만 처리하고, 결국 데이터베이스 서버와 같은 내부 또는 기타 DMZ 세그먼트에 있는 일부 백엔드 서버와의 연결을 시작해야 합니다. 동시에 DMZ 서버는 서로 통신하거나 외부 세계와 연결을 시작하지 않아야 합니다. 이는 간단한 신뢰 모델에서 필요한 트래픽 흐름을 명확하게 정의합니다. 그러나 이러한 모델이 적절하게 시행되지 않는 경우가 많습니다.

디자이너는 일반적으로 모든 서버에 대해 공통 세그먼트를 사용하여 DMZ를 구현하는 경향이 있습니다. 이 세그먼트는 서버 간의 트래픽을 제어하지 않습니다. 예를 들어 모든 서버는 공통 VLAN에 있습니다. 어떤 것도 동일한 VLAN 내에서 트래픽을 제어하지 않으므로, 서버 중 하나가 손상된 경우 동일한 서버를 악용하여 동일한 세그먼트에 있는 서버 및 호스트에 공격을 소싱할 수 있습니다. 따라서 포트 리디렉션 또는 애플리케이션 레이어 공격을 수행할 수 있는 잠재적 침입자의 활동이 원활하게 이루어집니다.

일반적으로 방화벽 및 패킷 필터는 수신 연결을 제어하는 데만 사용되지만, DMZ에서 시작된 연결을 제한하는 데에는 일반적으로 아무 작업도 수행되지 않습니다. 얼마 전에는 cgi-bin 스크립트에서 잘 알려진 취약성이 있었는데, 이는 침입자가 HTTP 스트림만 전송하여 X-term 세션을 시작할 수 있게 했습니다. 방화벽에서 허용해야 하는 트래픽입니다. 침입자가 충분히 운이 좋았다면, 그 또는 그녀는 다른 치료를 사용하여 루트 프롬프트를 얻을 수 있는데, 일반적으로 일종의 버퍼 오버플로 공격입니다. 대부분의 경우 적절한 신뢰 모델을 적용하여 이러한 문제를 방지할 수 있습니다. 첫째, 서버는 서로 통신하지 않아야 하며, 두 번째로 이러한 서버에서 외부로 연결되는 연결은 없어야 합니다.

동일한 코멘트는 신뢰할 수 없는 일반 세그먼트에서 애플리케이션 서비스 공급자의 서버 팜까지 이어지는 다른 여러 시나리오에 적용됩니다.

Catalyst 스위치의 PVLAN 및 VACL은 올바른 신뢰 모델을 보장하는 데 도움이 됩니다. PVLAN은 공통 세그먼트에서 호스트 간의 트래픽을 제한함으로써 도움이 되는 반면, VACL은 특정 세그먼트로 향하는 모든 트래픽 흐름을 더욱 세부적으로 제어함으로써 도움이 됩니다. 이러한 기능은 다음 섹션에서 설명합니다.

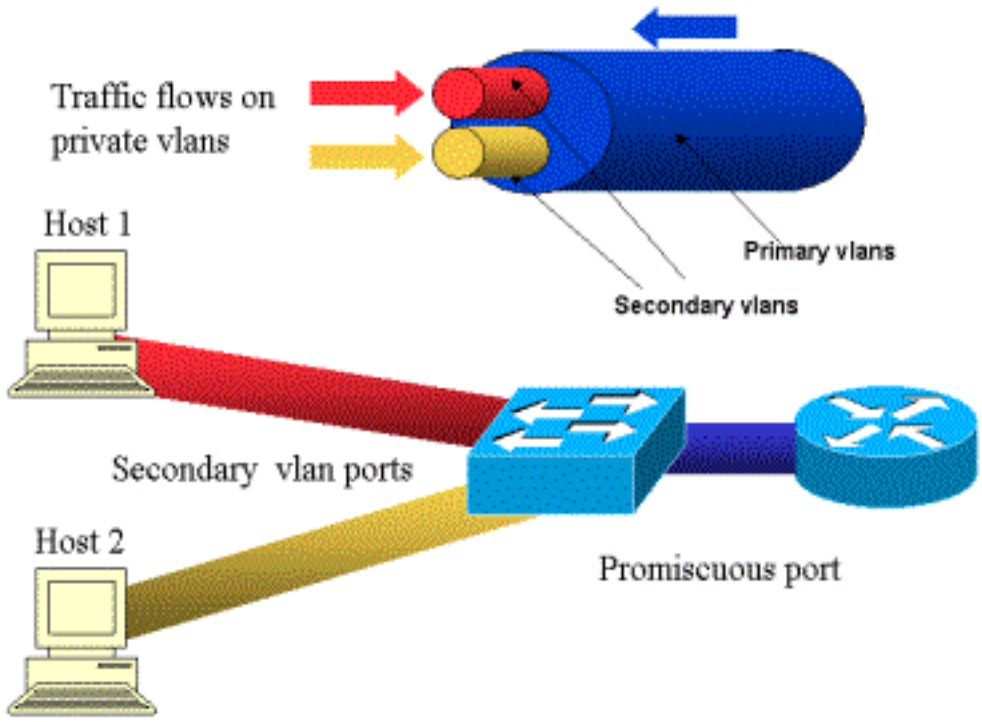
프라이빗 VLAN

PVLAN은 CatOS 5.4 이상을 실행하는 Catalyst 6000, Catalyst 4000, 2980G, 2980G-A, 2948G 및 4912G에서 사용 가능합니다.

우리의 관점에서 PVLAN은 브로드캐스트 세그먼트를 비 브로드캐스트 멀티액세스 세그먼트로 전환하는 레이어 2(L2)에서 트래픽을 분리하는 데 사용할 수 있는 툴입니다. 프로미스큐어스 포트(즉, 기본 VLAN과 보조 VLAN을 모두 포워딩할 수 있는 포트)에서 스위치로 들어오는 트래픽은 동일한 기본 VLAN에 속하는 모든 포트에서 아웃할 수 있습니다. 보조 VLAN에 매핑된 포트에서 스위치로 들어오는 트래픽(격리된 포트, 커뮤니티 또는 양방향 커뮤니티 VLAN일 수 있음)은 프로미스큐어스 포트 또는 동일한 커뮤니티 VLAN에 속하는 포트로 전달할 수 있습니다. 동일한 격리 VLAN에 매핑된 여러 포트가 트래픽을 교환할 수 없습니다.

다음 이미지는 개념을 보여줍니다.

그림 1: 프라이빗 VLAN



기본 VLAN은 파란색으로 표시됩니다. 보조 VLAN은 빨간색과 노란색으로 표시됩니다. 호스트-1은 보조 VLAN 빨간색에 속하는 스위치의 포트에 연결됩니다. 호스트-2는 보조 VLAN 노란색에 속하는 스위치의 포트에 연결됩니다.

호스트가 전송 중일 때 트래픽은 보조 VLAN에서 전달됩니다. 예를 들어, Host-2가 전송되면 해당 트래픽은 VLAN 노란색으로 이동합니다. 이러한 호스트가 수신되면 트래픽은 기본 VLAN인 VLAN 파란색에서 옵니다.

라우터와 방화벽이 연결된 포트는 프로미스큐어스 포트입니다. 이러한 포트는 매핑에 정의된 모든 보조 VLAN과 기본 VLAN에서 오는 트래픽을 전달할 수 있기 때문입니다. 각 호스트에 연결된 포트는 기본 VLAN에서 오는 트래픽과 해당 포트에 구성된 보조 VLAN에서만 전달할 수 있습니다.

드로잉은 프라이빗 VLAN을 라우터와 호스트를 연결하는 서로 다른 파이프로 나타냅니다. 다른 모든 것을 번들링하는 파이프는 기본 VLAN(파란색)이고 VLAN의 트래픽은 라우터에서 호스트로 이동합니다. 기본 VLAN에 내부 파이프는 보조 VLAN이며, 이러한 파이프에서 이동하는 트래픽은 호스트에서 라우터로 이동합니다.

이미지가 표시됨에 따라 기본 VLAN은 하나 이상의 보조 VLAN을 번들로 구성할 수 있습니다.

이 문서의 앞부분에서 PVLAN은 공통 세그먼트 내에서 호스트 분리를 확인함으로써 적절한 신뢰 모델을 적용하는 데 도움이 된다고 밝혔습니다. 프라이빗 VLAN에 대해 자세히 알아보았습니다. 이제 이 기능이 초기 DMZ 시나리오에서 어떻게 구현될 수 있는지 알아보겠습니다. 서버는 서로 통신해서는 안 되지만 여전히 연결된 방화벽이나 라우터와 통신해야 합니다. 이 경우 서버는 격리된 포트에 연결하고 라우터 및 방화벽은 프로미스큐어스 포트에 연결해야 합니다. 이렇게 하면 서버 중 하나가 손상된 경우 침입자는 동일한 서버를 사용하여 동일한 세그먼트 내의 다른 서버에 공격을 소싱할 수 없습니다. 스위치는 성능 저하 없이 유선 속도로 패킷을 삭제합니다.

또 다른 중요한 점은 모든 서버가 동일한 서브넷에 속하므로 이러한 종류의 제어는 L2 디바이스에서만 구현할 수 있다는 것입니다. 서버가 직접 통신을 시도하므로 방화벽이나 라우터가 할 수 있는 일은 없습니다. 또 다른 옵션은 서버당 방화벽 포트를 지정하는 것이지만 이는 너무 비싸고 구현하기 어려우며 확장되지 않습니다.

다음 섹션에서는 이 기능을 사용할 수 있는 기타 일반적인 시나리오에 대해 자세히 설명합니다.

VLAN 액세스 제어 목록

VACL은 CatOS 5.3 이상을 실행하는 Catalyst 6000 시리즈에서 사용할 수 있습니다.

VACL은 라우터가 필요 없이 L2의 Catalyst 6500에서 구성할 수 있습니다(PFC(Policy Feature Card)만 필요). 유선 속도로 적용되므로 Catalyst 6500에서 VACL을 구성할 때 성능 저하 문제가 없습니다. VACL의 조회는 액세스 목록의 크기와 상관없이 하드웨어에서 수행되므로 전달 속도는 변경되지 않습니다.

VACL은 기본 또는 보조 VLAN에 별도로 매핑할 수 있습니다. 보조 VLAN에 VACL을 구성하면 라우터나 방화벽에서 생성된 트래픽을 만지지 않고 호스트가 시작한 트래픽을 필터링할 수 있습니다.

VACL과 프라이빗 VLAN을 결합하면 트래픽 자체의 방향을 기준으로 트래픽을 필터링할 수 있습니다. 예를 들어, 두 라우터가 일부 호스트(예: 서버)와 동일한 세그먼트에 연결되어 있는 경우, 호스트가 생성한 트래픽만 필터링하고 라우터 간에 교환되는 트래픽은 그대로 유지되도록 보조 VLAN에서 VACL을 구성할 수 있습니다.

VACL을 쉽게 구축하여 적절한 신뢰 모델을 적용할 수 있습니다. DMZ 사례를 분석해보겠습니다. DMZ의 서버는 수신 연결만 제공하도록 되어 있으며 외부 세계에 대한 연결을 시작할 것으로 예상되지 않습니다. 이러한 서버에서 나가는 트래픽을 제어하기 위해 VACL을 보조 VLAN에 적용할 수 있습니다. VACL을 사용할 때 트래픽이 하드웨어에서 삭제되므로 라우터의 CPU나 스위치의 CPU에 영향을 미치지 않습니다. 서버 중 하나가 소스로 DDoS(Distributed Denial of Service) 공격에 관련되어 있는 경우에도 스위치는 성능 저하 없이 유선 속도로 모든 불법 트래픽을 삭제합니다. 서버가 연결된 라우터 또는 방화벽에도 유사한 필터를 적용할 수 있지만, 일반적으로 성능에 심각한 영향을 미칩니다.

MAC 기반 ACL은 IP 트래픽에서 제대로 작동하지 않으므로 PVLAN을 모니터링/추적하는 것이 좋습니다.

VACL 및 PVLAN의 알려진 제한 사항

VACL을 사용하여 필터링을 구성할 때 PFC의 프래그먼트 처리 및 하드웨어 사양에 따라 컨피그레이션이 조정되도록 주의해야 합니다.

Catalyst 6500의 Supervisor 1의 PFC의 하드웨어 설계를 고려했을 때 icmp 프래그먼트를 명시적으로 거부하는 것이 좋습니다. 그 이유는 ICMP(Internet Control Message Protocol) 프래그먼트와 에코 응답이 하드웨어에서 동일하게 간주되기 때문이며 기본적으로 하드웨어가 프래그먼트를 명시적으로 허용하도록 프로그래밍됩니다. 따라서 echo-reply 패킷이 서버에서 나가는 것을 중지하려면 회선 **deny icmp any fragment**로 이를 명시적으로 구성해야 합니다. 이 문서의 컨피그레이션을 고려합니다.

PVLAN에 대해 잘 알려진 보안 제한이 있는데, 이는 라우터가 트래픽이 수신된 동일한 서브넷에서 트래픽을 다시 전달할 수 있는 가능성입니다. 라우터는 PVLAN의 목적을 극복하고 격리된 포트 간에 트래픽을 라우팅할 수 있습니다. 이러한 제한은 PVLAN이 레이어 3(L3)이 아니라 L2에서 격리를 제공하는 툴이기 때문입니다.

uRPF(Unicast Reverse Path Forwarding)가 PVLAN 호스트 포트와 제대로 작동하지 않으므로 uRPF를 PVLAN과 함께 사용하면 안 됩니다.

기본 VLAN에 구성된 VACL을 통해 이 문제를 해결할 수 있습니다. 사례 연구에서는 동일한 서브넷에 의해 시작된 트래픽을 삭제하고 동일한 서브넷으로 다시 라우팅하기 위해 기본 VLAN에 구성해야 하는 VACL을 제공합니다.

일부 라인 카드에서 PVLAN 매핑/맵/트렁킹 포트의 컨피그레이션은 여러 PVLAN 매핑이 서로 다른 포트 ASIC(Application-Specific Integrated Circuit)에 속해야 컨피그레이션이 가능합니다. 이러한 제한 사항은 새 포트 ASIC Coil3에서 제거됩니다. 자세한 내용은 소프트웨어 구성에 대한 최신 Catalyst 스위치 설명서를 참조하십시오.

사례 연구

다음 섹션에서는 대부분의 구현을 대표하는 세 가지 사례 연구에 대해 설명하고 PVLAN 및 VACL의 보안 구축과 관련된 세부 정보를 제공합니다.

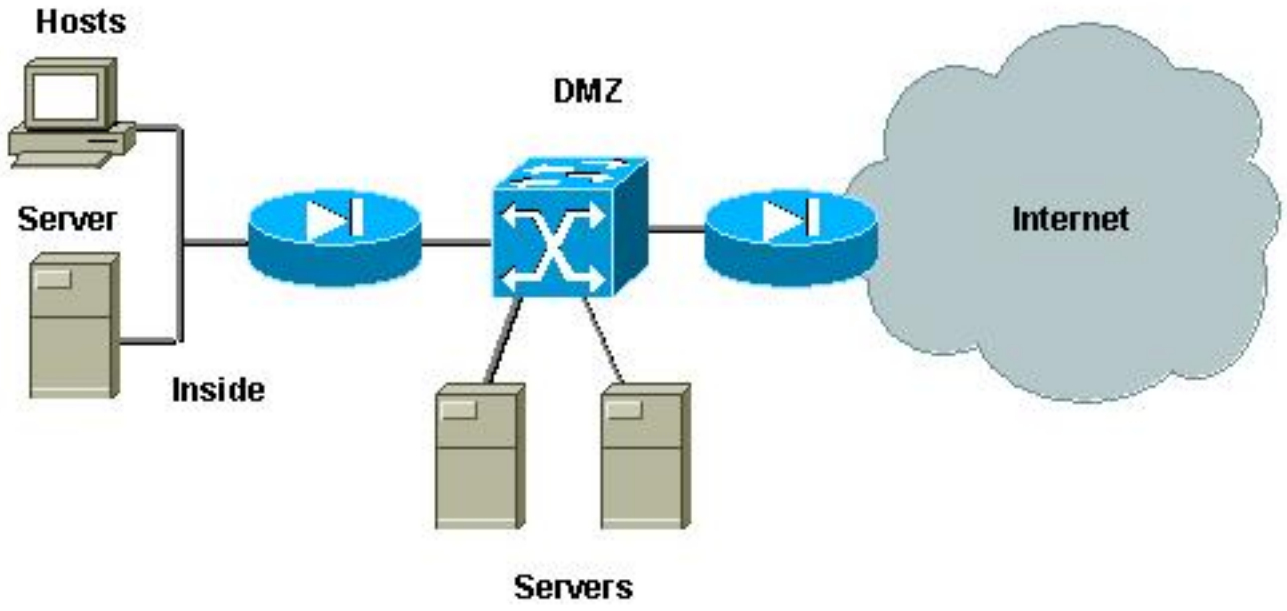
이러한 시나리오는 다음과 같습니다.

- 통과 DMZ
- 외부 DMZ
- 방화벽과 병렬로 작동하는 VPN Concentrator

통과 DMZ

이는 가장 일반적으로 구축된 시나리오 중 하나입니다. 이 예에서 DMZ는 아래 이미지에 표시된 대로 두 방화벽 라우터 간의 전송 영역으로 구현됩니다.

그림 2: 통과 DMZ



이 예에서 DMZ 서버는 외부 및 내부 사용자가 액세스해야 하지만 서로 통신할 필요는 없습니다. 경우에 따라 DMZ 서버는 내부 호스트에 대한 일종의 연결을 열어야 합니다. 동시에 내부 클라이언트는 제한 없이 인터넷에 액세스해야 합니다. 예를 들어 DMZ에 웹 서버가 있고 내부 네트워크에 있는 데이터베이스 서버와 통신해야 하며 내부 클라이언트가 인터넷에 액세스하는 경우가 있습니다.

외부 방화벽은 DMZ에 있는 서버에 대한 수신 연결을 허용하도록 구성되지만, 일반적으로 발신 트래픽, 특히 DMZ에서 시작된 트래픽에 필터 또는 제한이 적용되지 않습니다. 이 문서에서 앞서 설명한 것처럼, 다음과 같은 두 가지 이유로 공격자의 활동을 잠재적으로 용이하게 할 수 있습니다. 첫 번째는 DMZ 호스트 중 하나가 감염되면 다른 모든 DMZ 호스트가 노출됩니다. 두 번째, 공격자는 발신 연결을 쉽게 이용할 수 있습니다.

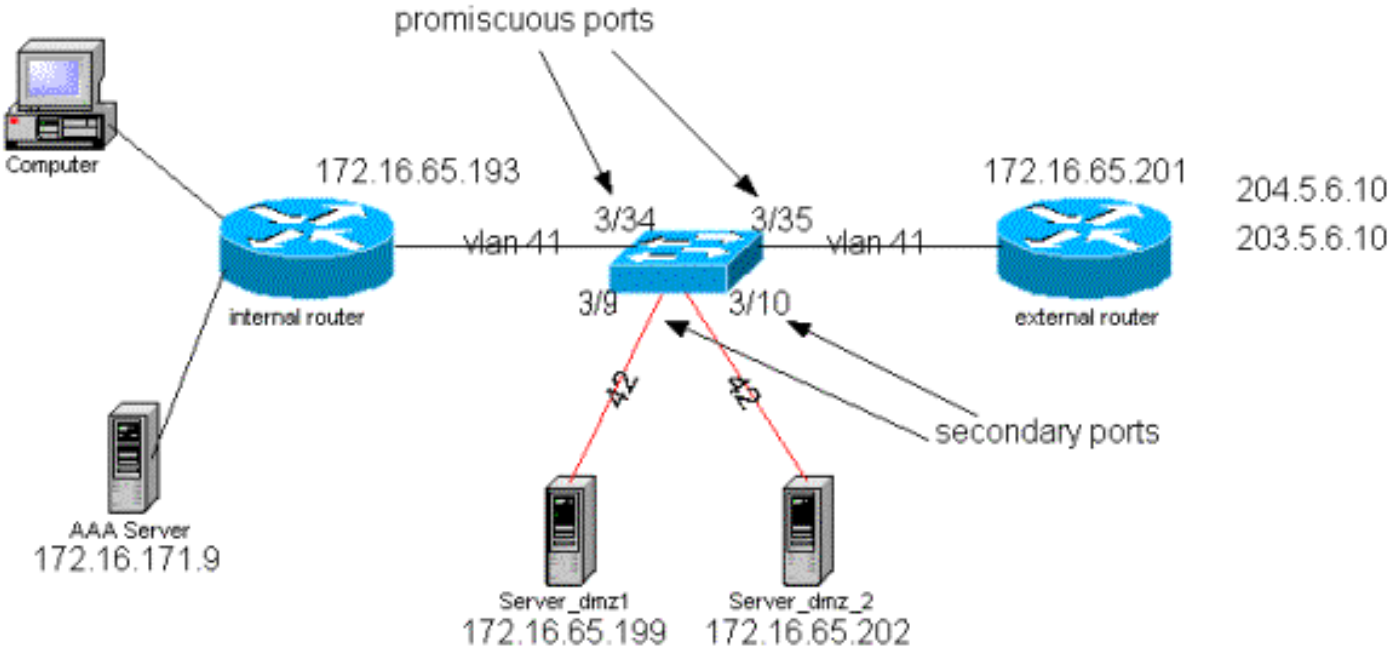
DMZ 서버는 서로 통신할 필요가 없으므로 L2에서 격리되도록 하는 것이 좋습니다. 서버 포트는 PVLAN이 격리된 포트로 정의되고 두 방화벽에 연결된 포트는 프로미스큐어로 정의됩니다. 방화벽에 대한 기본 VLAN과 DMZ 서버에 대한 보조 VLAN을 정의하면 이를 달성할 수 있습니다.

VACL은 DMZ에서 시작된 트래픽을 제어하는 데 사용됩니다. 이렇게 하면 공격자가 불법적인 발신 연결을 열 수 없습니다. DMZ 서버는 클라이언트 세션에 해당하는 트래픽에 응답할 뿐만 아니라 DNS(Domain Name System) 및 MTU(Maximum Transmission Unit) 경로 검색 등의 추가 서비스도 필요하다는 점에 유의해야 합니다. 따라서 ACL은 DMZ 서버에 필요한 모든 서비스를 허용해야 합니다.

통과 DMZ 테스트

테스트 환경에서 server_dmz1 및 server_dmz2 라우터로 구성된 두 개의 라우터가 포함된 DMZ 세그먼트를 구현했습니다. 이러한 서버는 외부 및 내부 클라이언트에서 액세스해야 하며 모든 HTTP 연결은 내부 RADIUS 서버(UNIX용 CiscoSecure ACS)를 사용하여 인증됩니다. 내부 및 외부 라우터는 모두 패킷 필터 방화벽으로 구성됩니다. 다음 그림은 사용된 주소 지정 체계를 포함하여 테스트 환경을 보여줍니다.

그림 3: Pass-Through DMZ 테스트 환경



다음 목록은 PVLAN의 기본 컨피그레이션 단계를 수집합니다. Catalyst 6500은 DMZ에서 L2 스위치로 사용됩니다.

- Server_dmz_1이 포트 3/9에 연결됨
- Server_dmz_2가 포트 3/10에 연결됨
- 내부 라우터가 포트 3/34에 연결됨
- 외부 라우터가 포트 3/35에 연결됨

다음 VLAN을 선택했습니다.

- 41은 기본 VLAN
- 42는 격리된 VLAN

프라이빗 VLAN 컨피그레이션

다음 컨피그레이션은 관련된 포트의 PVLAN을 설정합니다.

```
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
```

기본 VLAN의 VACL 컨피그레이션

이 섹션은 DMZ의 보안을 향상하기 위해 매우 중요합니다. VACL 및 PVLAN의 알려진 제한 사항 섹션에 설명된 대로, 서버가 서로 다른 두 보조 VLAN에 속하거나 동일한 격리 VLAN에 속하더라도 공격자가 서로 통신하기 위해 사용할 수 있는 방법이 있습니다. 서버가 직접 통신을 시도하는 경우 PVLAN 때문에 L2에서 통신할 수 없습니다. 동일한 서브넷에 대한 트래픽이 라우터로 전송되는 방식으로 침입자가 서버를 감염시킨 다음 구성된 경우 이 서버는 트래픽을 동일한 서브넷에 다시 라우팅하여 PVLAN의 목적을 무너뜨립니다.

따라서 기본 VLAN(라우터에서 트래픽을 전달하는 VLAN)에 다음 정책을 사용하여 VACL을 구성해야 합니다.

- 소스 IP가 라우터의 IP인 트래픽을 허용합니다.
- 소스 및 대상 IP가 모두 DMZ 서브넷인 트래픽을 거부합니다.
- 나머지 트래픽 모두 허용

```
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
```

이 ACL은 서버에서 생성된 트래픽에 영향을 주지 않습니다. 이는 라우터가 서버에서 들어오는 트래픽을 동일한 VLAN으로 다시 라우팅하지 못하도록 합니다. 처음 두 명령문은 라우터가 icmp 리디렉션 또는 icmp unreachable과 같은 메시지를 서버로 전송할 수 있도록 합니다.

보조 VLAN의 VACL 컨피그레이션

다음 컨피그레이션 로그는 서버에서 생성된 트래픽을 필터링하기 위해 VACL을 설정하는 방법을 보여 주는 데 사용됩니다. 이 VACL을 구성함으로써 다음을 달성하고자 합니다.

- 서버에서 **ping** 허용(에코 허용)
- 에코 **응답**이 서버에서 나가는 것을 방지
- 외부에서 시작된 HTTP 연결 허용
- RADIUS 인증(UDP 포트 1645) 및 계정 관리(UDP 포트 1646) 트래픽 허용
- DNS 트래픽 허용(UDP 포트 53)

나머지 모든 트래픽을 차단하고자 합니다.

단편화에 관한 한 서버 세그먼트에서 다음을 가정합니다.

- 서버는 조각화된 트래픽을 생성하지 않습니다.
- 서버에서 단편화된 트래픽을 수신할 수 있습니다.

Catalyst 6500의 Supervisor 1에 대한 PFC의 하드웨어 설계에서 ICMP 프래그먼트를 명시적으로 거부하는 것이 좋습니다. 이유는 ICMP 프래그먼트 및 에코 응답이 하드웨어에서 동일하게 간주되며 기본적으로 하드웨어가 프래그먼트를 명시적으로 허용하도록 프로그래밍되기 때문입니다. 따라서 echo-reply 패킷이 서버에서 나가는 것을 중지하려면 회선 **deny icmp any fragment**로 이**를 구성해야 합니다**.

```
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
```

구성 테스트

VACL이 아직 적용되지 않았지만 구성된 PVLAN이 있는 경우 다음 출력이 캡처되었습니다. 이 테스트에서는 외부 라우터에서 사용자가 내부 라우터와 서버를 ping할 수 있음을 보여줍니다.

```
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
```

다음 예에서는 서버에서 기본 게이트웨이인 외부 네트워크로 ping할 수 있지만 동일한 보조 VLAN에 속하는 서버는 ping할 수 없다는 것을 보여줍니다.

```
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)
```

VACL을 매핑한 후 외부 라우터에서 ping은 더 이상 성공하지 않습니다.

```
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)
```

다음 예는 내부 네트워크에서 HTTP GET 요청을 수신하는 서버를 보여줍니다.

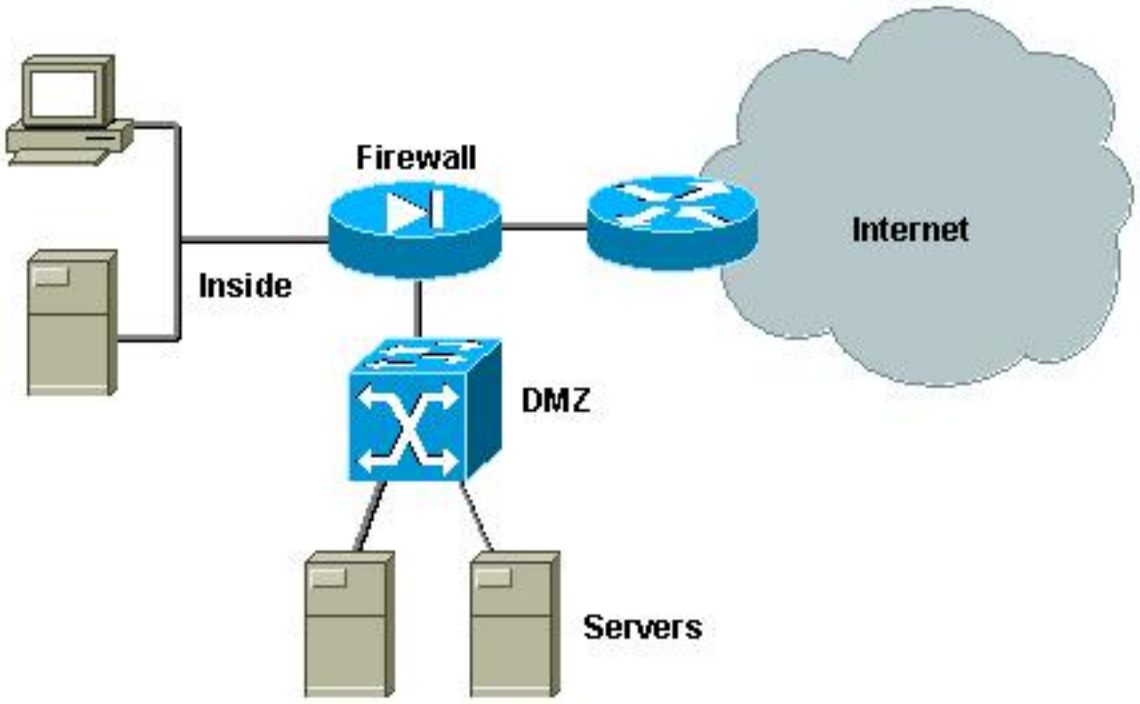
```
server_dmz1#debug ip http url
HTTP URL debugging is on
server_dmz1#debug ip hhtp tran
HTTP transactions debugging is on
server_dmz1#debug ip http auth
HTTP Authentication debugging is on
server_dmz1#
*Mar  7 09:24:03.092 PST: HTTP: parsed uri '/'
*Mar  7 09:24:03.092 PST: HTTP: client version 1.0
*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 ''
```

외부 DMZ

외부 DMZ 시나리오는 아마도 가장 널리 채택되고 구축된 구현일 것입니다. 외부 DMZ는 아래 그림과 같이 하나 이상의 방화벽 인터페이스를 사용하여 구현됩니다.

그림 4: 외부 DMZ



일반적으로 DMZ의 요구 사항은 설계 구현과 상관없이 동일하게 적용됩니다. 이전 사례와 마찬가지로, DMZ 서버는 외부 클라이언트 및 내부 네트워크에서 액세스할 수 있어야 합니다. DMZ 서버는 결국 일부 내부 리소스에 액세스해야 하며 서로 통신해서는 안 됩니다. 이와 동시에 DMZ에서 인터넷으로 향하는 트래픽은 개시되지 않아야 합니다. 이러한 DMZ 서버는 수신 연결에 해당하는 트래픽만 응답해야 합니다.

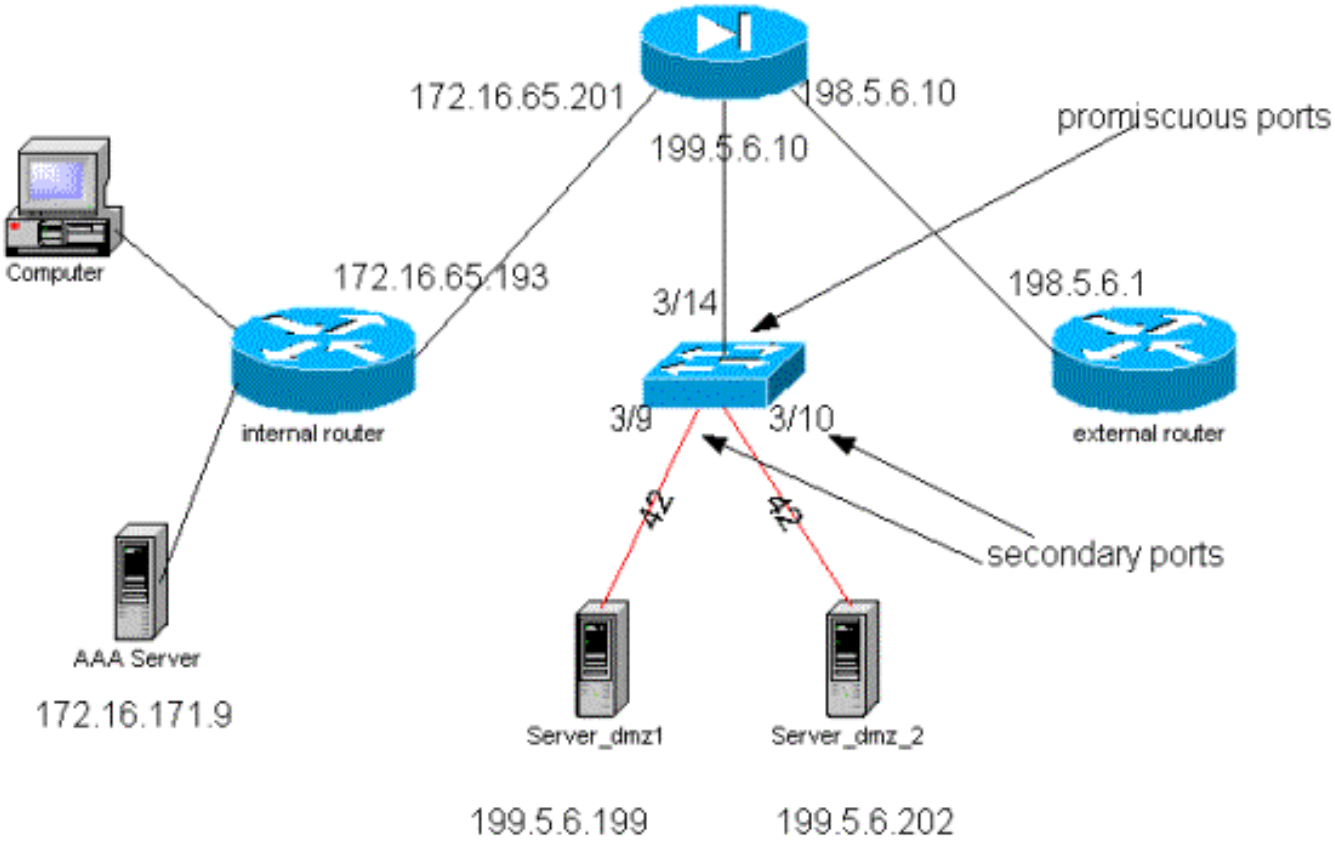
이전 사례 연구에서와 같이 첫 번째 컨피그레이션 단계는 PVLAN을 통해 L2에서 격리를 수행하고 내부 및 외부 호스트가 액세스할 수 있는 동안 DMZ 서버가 서로 통신할 수 없도록 하는 것입니다. 격리 포트를 사용하여 보조 VLAN에서 서버를 설정하여 구현됩니다. 방화벽은 프로미스큐어스 포트를 사용하여 기본 VLAN에 정의되어야 합니다. 방화벽은 이 기본 VLAN 내의 유일한 디바이스입니다.

두 번째 단계는 DMZ에서 시작된 트래픽을 제어하기 위해 ACL을 정의하는 것입니다. 이러한 ACL을 정의할 때는 필요한 트래픽만 허용해야 합니다.

외부 DMZ 테스트

아래 이미지는 이 사례 연구를 위해 구현된 테스트 기반(DMZ에 대해 세 번째 인터페이스가 포함된 PIX 방화벽 사용)입니다. 동일한 라우터 세트가 웹 서버로 사용되고 모든 HTTP 세션이 동일한 RADIUS 서버로 인증됩니다.

그림 5: 외부 DMZ 테스트 환경



이 시나리오에서는 이전 사례 연구에서 PVLAN 및 VACL 컨피그레이션에 대해 자세히 설명했으므로 컨피그레이션 파일에서 더 흥미로운 발췌만 첨부합니다.

PIX 컨피그레이션

```
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 컨피그레이션

NAS 구성

```
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 서버 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 구성

이 컨피그레이션에서는 PIX가 보낸 동일한 인터페이스에서 트래픽을 리디렉션하지 않으므로 기본 VLAN에 VACL을 구성할 필요가 없습니다. 기본 VLAN 섹션의 VACL 컨피그레이션에 설명된

VACL은 이중화됩니다.

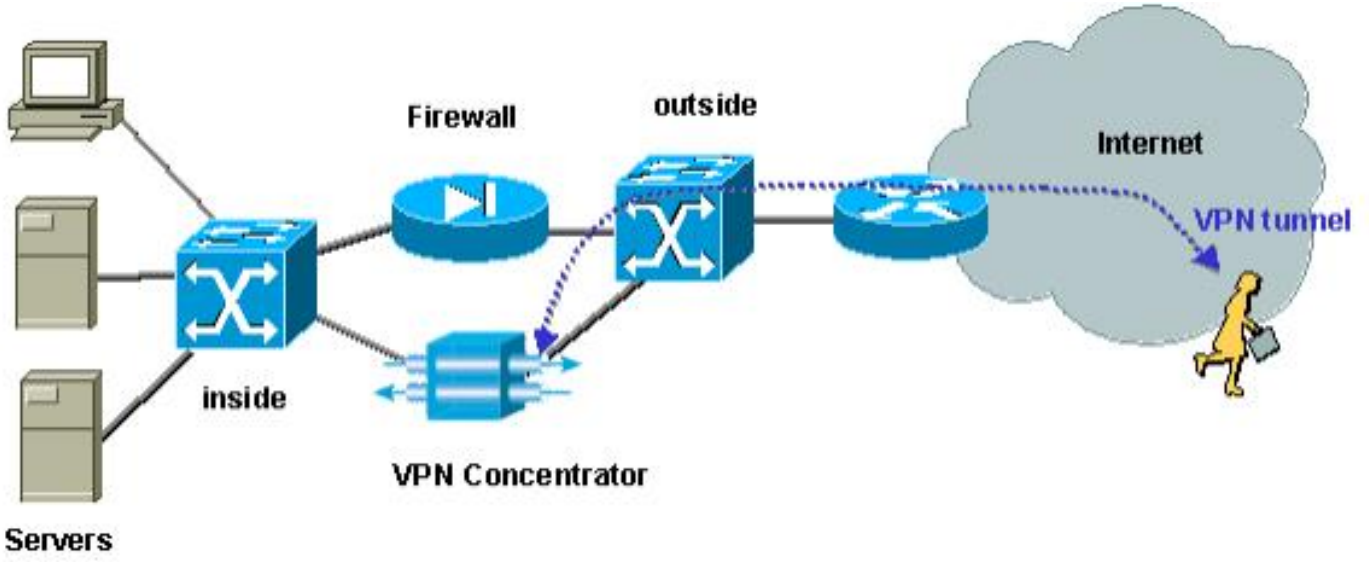
```
set security acl ip dmz_servers_out
---------------------------------------------------
1. deny icmp any any fragment
2. permit icmp host 199.5.6.199 any echo
3. permit icmp host 199.5.6.202 any echo
4. permit tcp host 199.5.6.199 eq 80 any established
5. permit tcp host 199.5.6.202 eq 80 any established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

방화벽과 병렬로 작동하는 VPN Concentrator

Access VPN(Virtual Private Networks)을 구현할 때, 반드시 가장 선호하는 접근 방식 중 하나는 병렬 설계(아래 그림에 나와 있음)입니다. 고객은 기존 인프라에 거의 영향을 미치지 않고 손쉽게 구현할 수 있고 장치 유연성에 따라 상대적으로 쉽게 확장할 수 있기 때문에 일반적으로 이러한 설계 방식을 선호합니다.

병렬 접근 방식에서는 VPN Concentrator가 내부 및 외부 세그먼트에 모두 연결됩니다. 모든 VPN 세션은 방화벽을 거치지 않고 Concentrator에서 종료됩니다. 일반적으로 VPN 클라이언트는 내부 네트워크에 대한 무제한 액세스를 가져야 하지만, 내부 서버(서버 팜) 집합으로 액세스가 제한될 수 있습니다. 바람직한 기능 중 하나는 VPN 트래픽을 일반 인터넷 트래픽과 분리하는 것입니다. 예를 들어 VPN 클라이언트는 회사 방화벽을 통해 인터넷에 액세스할 수 없습니다.

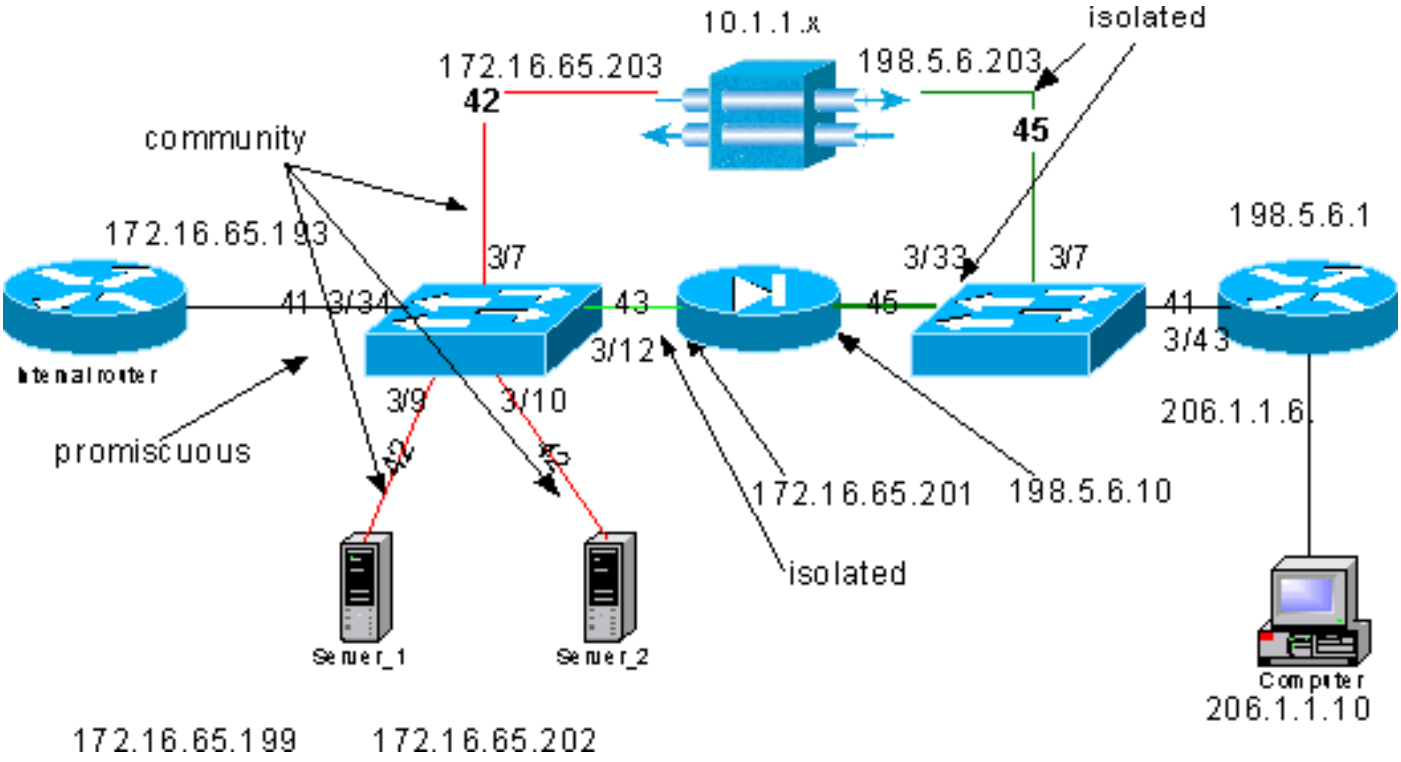
그림 6: 방화벽과 병렬로 작동하는 VPN Concentrator



방화벽과 병렬로 VPN Concentrator 테스트

이 예에서는 PIX 방화벽과 병렬로 설치된 VPN 5000 Concentrator를 사용했습니다. 웹 서버로 구성된 두 라우터는 내부 세그먼트에 내부 서버 팜으로 설치되었습니다. VPN 클라이언트는 서버 팜에 액세스만 가능하며 인터넷 트래픽은 IPSec(VPN traffic)에서 분리되어야 합니다. 아래 그림은 테스트 환경을 보여줍니다.

그림 7: VPN Concentrator를 방화벽 테스트 장비와 병렬로 연결



이 시나리오에서는 두 가지 주요 관심 영역이 있습니다.

- 내부 L2 스위치
- 외부 L2 스위치

내부 L2 스위치에 대한 트래픽 흐름은 다음 문을 기반으로 정의됩니다.

- VPN 클라이언트는 미리 정의된 내부 서버(서버 팜) 집합에 대한 전체 액세스 권한을 가집니다.

- 내부 클라이언트는 서버 팜에 액세스할 수도 있습니다.
- 내부 클라이언트는 인터넷에 무제한 액세스할 수 있습니다.
- VPN Concentrator에서 들어오는 트래픽은 PIX 방화벽에서 격리되어야 합니다.

외부 L2 스위치의 트래픽 흐름은 다음과 같이 정의됩니다.

- 라우터에서 들어오는 트래픽은 VPN Concentrator 또는 PIX로 이동할 수 있어야 합니다.
- PIX에서 들어오는 트래픽은 VPN에서 들어오는 트래픽에서 격리되어야 합니다.

또한 관리자는 내부 네트워크의 트래픽이 VPN 호스트로 이동하는 것을 막고자 할 수 있습니다. 이는 기본 VLAN에 구성된 VACL을 통해 달성할 수 있습니다(VACL은 내부 라우터에서 나가는 트래픽만 필터링하며 다른 트래픽은 영향을 받지 않습니다).

PVLAN 컨피그레이션

이 설계의 주요 목표는 PIX에서 오는 트래픽을 서버 및 VPN Concentrator에서 들어오는 트래픽에서 분리시키는 것입니다. 따라서 서버와 VPN Concentrator가 구성된 PVLAN과 다른 PVLAN에서 PIX를 구성합니다.

내부 네트워크에서 들어오는 트래픽은 서버 팜, VPN Concentrator 및 PIX에 액세스할 수 있어야 합니다. 따라서 내부 네트워크에 연결되는 포트는 프로미스큐어스 포트가 됩니다.

서버와 VPN Concentrator는 서로 통신할 수 있으므로 동일한 보조 VLAN에 속합니다.

외부 L2 스위치의 경우 인터넷에 대한 액세스를 제공하는 라우터(일반적으로 ISP(인터넷 서비스 공급자)가 프로미스큐어스 포트에 연결되고 VPN Concentrator 및 PIX는 동일한 사설 및 격리된 VLAN에 속하므로 트래픽을 교환할 수 없습니다. 이렇게 하면 통신 사업자의 트래픽이 VPN Concentrator로의 경로 또는 PIX의 경로를 사용할 수 있습니다. PIX 및 VPN Concentrator는 격리되므로 더 안전하게 보호됩니다.

내부 L2 스위치의 PVLAN 컨피그레이션

```
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
```

외부 L2 스위치의 PVLAN 컨피그레이션

```
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
```

구성 테스트

이 실험은 내부 라우터가 방화벽을 통과하여 외부 라우터(인터페이스가 198.5.6.1인 외부 방화벽 라우터)에 도달할 수 있음을 보여줍니다.

```
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
```

이 실험에서는 서버 1의 모든 항목을 다음과 같이 보여 줍니다.

- 서버 1은 내부 라우터를 ping할 수 있습니다.
  ```
  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
  ```
- 서버 1은 VPN에 ping할 수 있습니다.
  ```
  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
  ```
- 서버 1에서 PIX 내부 인터페이스를 ping할 수 없습니다.
  ```
  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)
  ```
- 서버 1에서 외부 라우터를 ping할 수 없습니다.
  ```
  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)
  ```

다음 실험에서는 내부 네트워크에서 서버 팜으로 HTTP 세션을 열 수 있음을 보여줍니다.

```
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 ''
```

다음 실험은 VPN 네트워크의 HTTP 트래픽이 서버 팜으로 이동할 수 있음을 보여줍니다(주소 10.1.1.1 주의).

```
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
```

다음은 VPN Concentrator 컨피그레이션입니다.

```
[ 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"
```

다음 명령은 연결된 사용자 목록을 보여줍니다.

```
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
```

서버의 기본 게이트웨이는 내부 라우터 172.16.65.193이며, 이 경우 icmp 리디렉션을 172.16.65.203으로 발급합니다. 이 구현은 호스트가 라우터로 플로우의 첫 번째 패킷을 전송하고 리디렉션을 수신하면 이 트래픽을 처리하는 데 더 적합한 후속 패킷을 게이트웨이로 전송하므로 최적화되지 않은 트래픽 플로우를 발생시킵니다. 또는 10.x.x.x 주소의 VPN을 가리키고 나머지 트래픽의 경우 172.16.65.193을 가리키도록 서버 자체에서 두 개의 다른 경로를 구성할 수 있습니다. 서버에 기본 게이트웨이만 구성된 경우 라우터 인터페이스가 "ip redirect"로 구성되어 있는지 확인해야 합니다.

테스트 중에 알게 된 흥미로운 점은 다음과 같습니다. 서버 또는 VPN에서 198.5.6.1과 같은 외부 주소를 **ping**하려고 시도하면 기본 게이트웨이가 전송하고 icmp 리디렉션을 172.16.65.201으로 전송합니다.

```
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)
```

이 시점에서 서버 또는 VPN은 172.16.65.201에 대한 ARP(Address Resolution Protocol) 요청을 전송하며, 다른 보조 VLAN에 있으므로 201에서 응답을 받지 않습니다. 이것이 PVLAN이 제공하는 것입니다. 실제로 이 문제를 해결할 수 있는 쉬운 방법은 트래픽을 MAC 0.193 및 대상 IP 172.16.65.201으로 보내는 것입니다.

라우터 .193은 트래픽을 동일한 인터페이스로 다시 라우팅하지만, 라우터 인터페이스가 프로미스큐어스 포트이므로 트래픽은 차단하고자 했던 .201에 도달할 것입니다. 이 문제는 VACL 및 PVLAN의 알려진 제한 사항 섹션에서 설명합니다.

VACL 구성

이 섹션은 서버 팜의 보안을 개선하기 위해 중요합니다. VACL 및 PVLAN의 알려진 제한 사항 섹션에 설명된 대로 서버와 PIX가 서로 다른 두 보조 VLAN에 속하더라도 공격자가 서로 통신하도록 하는 데 사용할 수 있는 방법이 있습니다. PVLAN으로 인해 직접 커뮤니케이션을 시도하면 PVLAN으로 인해 통신이 불가능합니다. 동일한 서브넷에 대한 트래픽이 라우터로 전송되는 방식으로 침입자가 서버를 감염시킨 다음 구성된 경우 이 서버는 트래픽을 동일한 서브넷에 다시 라우팅하여 PVLAN의 목적을 무너뜨립니다.

따라서 기본 VLAN(라우터에서 트래픽을 전달하는 VLAN)에 다음 정책을 사용하여 VACL을 구성해야 합니다.

- 소스 IP가 라우터의 IP인 트래픽을 허용합니다.
- 소스 및 대상 IP가 서버 팜의 서브넷이 되는 트래픽을 거부합니다.
- 나머지 트래픽 모두 허용

```
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
```

이 ACL은 서버나 PIX에 의해 생성된 트래픽에 영향을 주지 않습니다. 이는 라우터가 서버에서 들어오는 트래픽을 동일한 VLAN으로 다시 라우팅하지 못하도록 합니다. 처음 두 명령문은 라우터가 icmp 리디렉션 또는 icmp unreachable 등의 메시지를 서버로 전송할 수 있도록 합니다.

관리자가 VACL을 통해 중지하려는 다른 트래픽 흐름을 식별했으며, 이 흐름은 내부 네트워크에서 VPN 호스트로 이동됩니다. 이를 위해 VACL을 기본 VLAN(41)에 매핑하고 이전 VLAN과 결합할 수 있습니다.

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
```

구성 테스트

이제 라우터 .193(zundapp)에서 10.1.1.1 호스트를 ping합니다. VACL을 매핑하기 전에 **ping**이 성공합니다.

```
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
```

VLAN 41에서 VACL을 매핑한 후 동일한 **ping**이 성공하지 못합니다.

```
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)
```

그러나 여전히 외부 라우터를 ping할 수 있습니다.

```
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
```

관련 정보

- 액세스 제어 목록 구성 - Catalyst 6000 설명서
- Technical Support - Cisco Systems