Secure-netwerken met PVLAN's en VACL's

Inhoud

[Inleiding](#)
[Voordat u begint](#)
[Conventies](#)
[Voorwaarden](#)
[Gebruikte componenten](#)
[Achtergrondinformatie](#)
[Belangrijk om een goed vertrouwensmodel in te voeren](#)
[Private VLAN's](#)
[VLAN-toegangscontrolelijsten](#)
[Bekende beperkingen van VACL's en PVLAN's](#)
[Voorbeelden van casestudy's](#)
[doorvoer-DMZ](#)
[Externe DMZ](#)
[VPN-Concentrator in parallel met firewall](#)
[Gerelateerde informatie](#)

Inleiding

Een van de belangrijkste factoren om een succesvol netwerk security ontwerp te bouwen is een goed trust model te identificeren en af te dwingen. Het juiste vertrouwensmodel definieert wie met wie moet praten en welk soort verkeer moet worden uitgewisseld; al het andere verkeer moet worden geweigerd . Zodra het juiste trust model is geïdentificeerd, moet de veiligheidsontwerper beslissen hoe het model te handhaven. Aangezien meer cruciale bronnen mondiaal beschikbaar zijn en nieuwe vormen van netwerkaanvallen zich verder ontwikkelen, wordt de infrastructuur van de netwerkveiligheid meestal geavanceerder, en zijn er meer producten beschikbaar. Firewalls, routers, LAN-switches, inbraakdetectiesystemen, AAA-servers en VPN's zijn een aantal technologieën en producten die kunnen helpen om het model af te dwingen. Natuurlijk speelt elk van deze producten en technologieën een specifieke rol in de algehele security implementatie, en het is essentieel voor de ontwerper om te begrijpen hoe deze elementen kunnen worden ingezet.

Voordat u begint

Conventies

Zie de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Voorwaarden

Dit document beschrijft PVLAN-configuraties op switches die alleen CatOS-indeling uitvoeren.

Voor side-by-side configuratievoorbeelden van PVLANs op switches die Cisco IOS en CatOS in werking stellen, verwijs naar het document dat Geïsoleerde Private VLAN's op Catalyst Switches configureren.

Niet alle switches en softwareversies ondersteunen PVLAN's. Raadpleeg de Support Matrix voor Private VLAN-Switch om te bepalen of uw platform- en softwareversie PVLAN's ondersteunt.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Achtergrondinformatie

Het identificeren en handhaven van een goed vertrouwensmodel lijkt een zeer fundamentele taak, maar na verscheidene jaren van het ondersteunen van beveiligingsimplementaties wijst onze ervaring erop dat veiligheidsincidenten vaak te maken hebben met slechte beveiligingsontwerpen. Meestal zijn deze slechte ontwerpen een direct gevolg van het niet afdwingen van een goed trust model, soms omdat wat gewoon nodig is niet wordt begrepen, andere keren alleen omdat de betrokken technologieën niet goed worden begrepen of verkeerd worden gebruikt.

Dit document legt in detail uit hoe twee functies beschikbaar in onze Catalyst-switches, Private VLAN's (PVLAN's) en VLAN Access Control Lists (VACL's) kunnen helpen bij het verzekeren van een geschikt vertrouwensmodel in zowel de ondernemings- als de serviceprovider-omgevingen.

Belangrijk om een goed vertrouwensmodel in te voeren

Een onmiddellijk gevolg van het niet afdwingen van een toereikend vertrouwensmodel is dat de algemene beveiligingsimplementatie minder immuun wordt voor kwaadwillige activiteiten. Gedemilitariseerde zones (DMZ's) worden doorgaans ten uitvoer gelegd zonder het juiste beleid af te dwingen, zodat de activiteit van een potentiële indringer wordt vergemakkelijkt. In dit gedeelte wordt geanalyseerd hoe DMZ's vaak worden geïmplementeerd en wat de gevolgen zijn van een slecht ontwerp. We zullen later uitleggen hoe we deze gevolgen kunnen verzachten, of in het beste geval voorkomen.

Meestal worden DMZ-servers alleen verondersteld binnenkomende verzoeken van het internet te verwerken en uiteindelijk verbindingen te openen naar bepaalde back-end servers in een binnen- of ander DMZ-segment, zoals een database server. Tegelijkertijd zouden DMZ-servers niet met elkaar moeten praten of met de buitenwereld moeten verbinden. Dit definieert de noodzakelijke verkeersstromen duidelijk in een eenvoudig vertrouwensmodel; maar we zien vaak dat dit model niet adequaat wordt gehandhaafd .

Ontwerpers hebben de neiging DMZ's te implementeren met een gemeenschappelijk segment voor alle servers zonder enige controle over het verkeer tussen hen. Bijvoorbeeld, alle servers bevinden zich in een gemeenschappelijk VLAN. Omdat niets het verkeer binnen hetzelfde VLAN controleert, als één van de servers wordt gecompromitteerd, kan de zelfde server worden gebruikt om een aanval op om het even welke servers en hosts in het zelfde segment te ontketenen. Dit vergemakkelijkt duidelijk de activiteit van een potentiële indringer die een poortomleiding of een aanval van de toepassingslaag uitvoert.

Meestal worden firewalls en pakketfilters alleen gebruikt om inkomende verbindingen te controleren, maar er wordt gewoonlijk niets gedaan om verbindingen te beperken die uit de DMZ

afkomstig zijn. Enige tijd geleden was er een bekende kwetsbaarheid in een cgi-bin schrift die een indringer toestaat om een X-termijnsessie te beginnen door alleen een HTTP-stream te sturen; dit is verkeer dat door de firewall moet worden toegestaan . Als de indringer geluk had, kon hij of zij een andere traktatie gebruiken om een wortelvloed te krijgen, typisch een soort bufferoverloop aanval. Meestal kunnen dit soort problemen vermeden worden door een goed trust model in te voeren. In de eerste plaats is het niet de bedoeling dat servers met elkaar praten en in de tweede plaats mogen er geen verbindingen worden gemaakt van deze servers naar de buitenwereld.

De zelfde commentaren zijn van toepassing op vele andere scenario's, die van elk regelmatig onbetrouwbaar segment tot serverboerderijen bij de leveranciers van toepassingsdiensten gaan.

PVLAN’s en VACL’s op Catalyst-switches kunnen u helpen bij het waarborgen van een goed vertrouwensmodel. PVLAN’s zullen helpen door het verkeer tussen hosts in een gemeenschappelijk segment te beperken, terwijl VACL’s ertoe zullen bijdragen dat meer controle wordt uitgeoefend over elke verkeersstroom die is ontstaan of die bestemd is voor een bepaald segment. Deze functies worden in de volgende secties besproken.

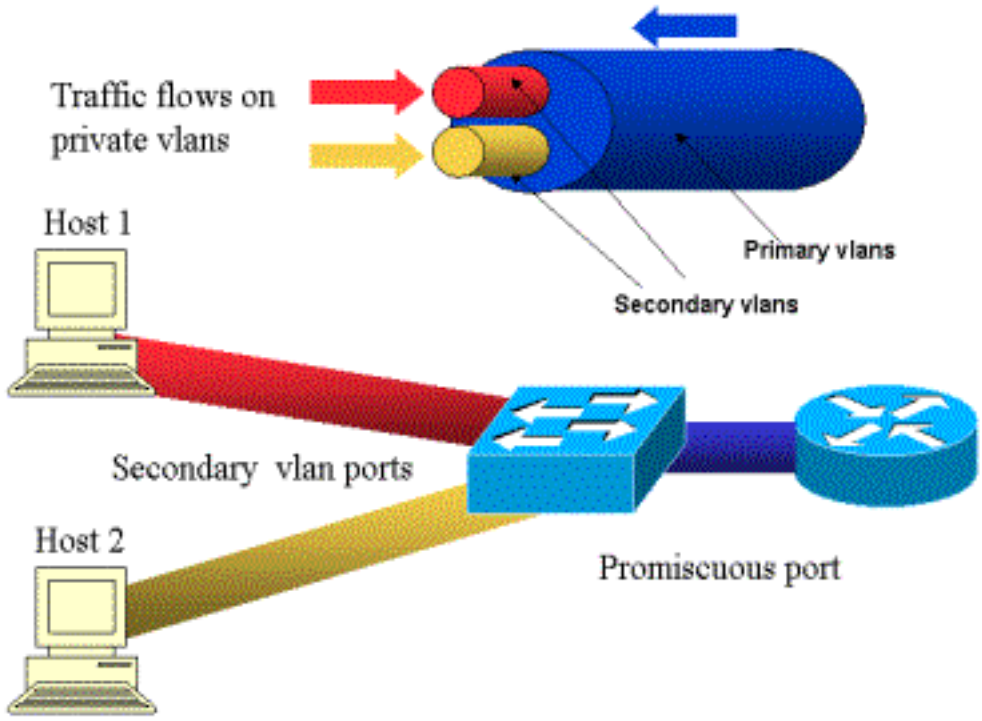
Private VLAN’s

PVLAN’s zijn beschikbaar op Catalyst 6000 met CatOS 5.4 of hoger, op Catalyst 4000, 2980G, 2980G-A, 2948G en 4912G met CatOS 6.2 of hoger.

Vanuit ons perspectief zijn PVLAN’s een gereedschap dat het segregerend verkeer op Layer 2 (L2) mogelijk maakt door een uitzending-segment in een niet-uitzending multi-access-achtig segment te draaien. Het verkeer dat aan een switch van een veelbelovende haven komt (dat wil zeggen, een haven die zowel primaire als secundaire VLAN's kan verzenden) kan op alle havens uitgaan die tot het zelfde primaire VLAN behoren. Het verkeer dat aan een switch van een haven komt die aan een secundair VLAN in kaart wordt gebracht (het kan of een geïsoleerd, een gemeenschap, of een tweerichtingsgemeenschap VLAN zijn) kan aan een veelbelovende haven of een haven die aan het zelfde communautaire VLAN toebehoren worden doorgestuurd. Meerdere poorten die aan hetzelfde geïsoleerde VLAN zijn gekoppeld, kunnen geen verkeer uitwisselen.

De volgende afbeelding toont het concept.

Afbeelding 1: Private VLAN’s



Het primaire VLAN wordt in blauw weergegeven; de secundaire VLAN's worden in rood en geel weergegeven. Host-1 wordt aangesloten op een poort van de switch die in het rood van het secundaire VLAN voorkomt. Host-2 wordt aangesloten op een poort van de switch die aan het secundaire geel VLAN behoort.

Wanneer een gastheer overbrengt, wordt het verkeer gedragen in het secundaire VLAN. Bijvoorbeeld, wanneer Host-2 uitzendt, gaat zijn verkeer op VLAN geel. Wanneer die gastheren ontvangen, komt het verkeer uit het blauwe VLAN, dat het primaire VLAN is.

De poorten waar routers en firewalls worden aangesloten zijn veelbelovende poorten omdat die poorten verkeer kunnen doorsturen vanuit elk secundair VLAN dat in de mapping is gedefinieerd, evenals het primaire VLAN. De poorten die op elke host worden aangesloten kunnen alleen het verkeer doorsturen dat afkomstig is van het primaire VLAN en het secundaire VLAN dat op die poort is geconfigureerd.

De tekening vertegenwoordigt de privé VLAN's als verschillende pijpen die routers en hosts met elkaar verbinden: De buis die alle anderen bundelt is het primaire VLAN (blauw), en het verkeer op VLAN blauw stroomt van de routers naar de hosts. De leidingen intern aan het primaire VLAN zijn de secundaire VLAN's, en het verkeer dat op deze buizen rijdt is van de hosts naar de router.

Zoals de afbeelding toont, kan een primair VLAN één of meer secundaire VLAN's bundelen.

Eerder in dit document zeiden we dat PVLAN's helpen het juiste vertrouwensmodel te handhaven door simpelweg de segregatie van hosts binnen een gemeenschappelijk segment te verzekeren. Nu we meer over Private VLAN's weten, laten we zien hoe dit in ons eerste DMZ-scenario kan worden geïmplementeerd. De servers moeten niet met elkaar praten, maar moeten nog met de firewall of router praten waarmee ze verbonden zijn. In dit geval moeten servers worden aangesloten op geïsoleerde poorten en moeten routers en firewalls worden aangesloten op veelbelovende poorten. Als een van de servers gecompromitteerd is, kan de indringer niet dezelfde server gebruiken om een aanval naar een andere server binnen hetzelfde segment te brengen. De switch laat elk pakje met draadsnelheid vallen zonder dat er een prestatietriem is.

Een andere belangrijke opmerking is dat dit soort controle alleen bij het L2 apparaat kan worden uitgevoerd omdat alle servers tot hetzelfde net behoren. Er is niets wat een firewall of router kan doen aangezien servers direct zullen proberen te communiceren. Een andere optie is om een firewallpoort per server te oormerken, maar deze is waarschijnlijk te duur, moeilijk te implementeren en niet schaalbaar.

In een later gedeelte beschrijven we in detail enkele andere typische scenario's waarin u deze functie kunt gebruiken.

VLAN-toegangscontrolelijsten

VACL's zijn beschikbaar in Catalyst 6000 Series die CatOS 5.3 of hoger uitvoeren.

VACL's kunnen op een Catalyst 6500 bij L2 worden ingesteld zonder dat u een router nodig hebt (u hebt alleen een beleidsfunctiekaart (PFC) nodig. Ze worden afgedwongen bij draadsnelheid zodat er geen prestatiemethode is voor het configureren van VACL's op een Catalyst 6500. Aangezien de raadpleging van VACL's in hardware wordt uitgevoerd, ongeacht de grootte van de toegangslijst, blijft het verzendingspercentage ongewijzigd.

VACL's kunnen afzonderlijk aan primaire of secundaire VLAN's worden toegewezen. Met een VACL op een secundair VLAN kunt u het verkeer filteren dat door hosts is gegenereerd zonder het verkeer aan te raken dat door routers of firewalls is gegenereerd.

Door VACL's en Private VLAN's te combineren is het mogelijk om verkeer te filteren op basis van de richting van het verkeer zelf. Als twee routers bijvoorbeeld op hetzelfde segment worden aangesloten als sommige hosts (servers bijvoorbeeld), kunnen VACL's op secundaire VLAN's worden geconfigureerd, zodat alleen het verkeer dat door de hosts wordt gegenereerd wordt gefilterd terwijl het verkeer dat tussen de routers wordt uitgewisseld, onaangeroerd is.

VACL's kunnen eenvoudig worden uitgevoerd om het juiste trust-model af te dwingen. Laten we onze DMZ-zaak analyseren. De servers bij de DMZ zouden alleen inkomende verbindingen moeten dienen, en van hen wordt niet verwacht dat ze verbindingen naar de buitenwereld gaan. Een VACL kan op hun secundaire VLAN worden toegepast om het verkeer te controleren dat deze servers verlaat. Het is van cruciaal belang om op te merken dat wanneer u VACL's gebruikt, het verkeer op hardware is gevallen zodat er geen impact is op de CPU van de router of de switch. Zelfs in het geval dat een van de servers betrokken is bij een aanval van de Distributed Denial of Service (DDoS) als bron, zal de switch al het illegale verkeer via de bedradingssnelheid laten vallen zonder enige prestatieboete. Gelijkaardige filters kunnen worden toegepast in de router of de firewall waar servers op worden aangesloten, maar dit heeft meestal ernstige implicaties voor de prestaties.

MAC-gebaseerde ACL's werken niet goed met IP-verkeer, zodat VACL's worden aanbevolen om PVLAN's te controleren/volgen.

Bekende beperkingen van VACL's en PVLAN's

Bij het configureren van filter met VACL's dient u voorzichtig te zijn met betrekking tot de fragmentatieverwerking op de PFC en moet de configuratie worden aangepast volgens de specificaties van de hardware.

Gegeven het hardwareontwerp van de PFC van supervisor 1 van Catalyst 6500, is het beter om

de fragmenten van icmp expliciet te ontkennen. De reden is dat de fragmenten en het echo-antwoord van Internet Control Message Protocol (ICMP) door de hardware hetzelfde worden geacht en dat de hardware standaard is geprogrammeerd om fragmenten expliciet toe te staan. Dus als u wilt voorkomen dat de echo-antwoordpakketten de servers verlaten, moet u dit expliciet configureren met de lijn **om elk fragment te ontkennen**. De configuraties in dit document houden hiermee rekening.

Er is een bekende veiligheidsbeperking aan PVLANs, wat de mogelijkheid is dat een router verkeer terug uit zelfde voorwerp terugstuurt waarvan het kwam. Een router kan verkeer over geïsoleerde havens leiden die het doel van PVLANs verslaan. Deze beperking is toe te schrijven aan het feit dat PVLAN's een gereedschap zijn dat isolatie biedt bij L2, niet bij Layer 3 (L3).

Unicast omgekeerd pad doorsturen (uRPF) werkt niet goed met PVLAN-host poorten, dus uRPF moet niet in combinatie met PVLAN worden gebruikt.

Er is een oplossing voor dit probleem, dat wordt bereikt door middel van VACL's die op de primaire VLAN's zijn geconfigureerd. De casestudy's zijn VACL's die op het primaire VLAN moeten worden geconfigureerd om het verkeer te laten vallen dat door hetzelfde subnetwerk gegenereerd is en naar hetzelfde subtype routed is.

Op sommige lijnkaarten is de configuratie van PVLAN-mappings / maps / trunking-poorten onderworpen aan enige beperkingen waar de meerdere PVLAN-mappings moeten behoren tot verschillende Port Application-Specific Geïntegreerde Circuits (ASIC's) om zo te worden geconfigureerd. Deze beperkingen worden op de nieuwe poort van ASIC Coil3 verwijderd. Raadpleeg de nieuwste Catalyst switch documentatie over de softwareconfiguratie voor deze details.

Voorbeelden van casestudy's

In het volgende gedeelte worden drie casestudy's beschreven, die naar onze mening representatief zijn voor de meeste implementaties en die de details geven met betrekking tot de beveiligingsimplementatie van PVLAN's en VACL's.

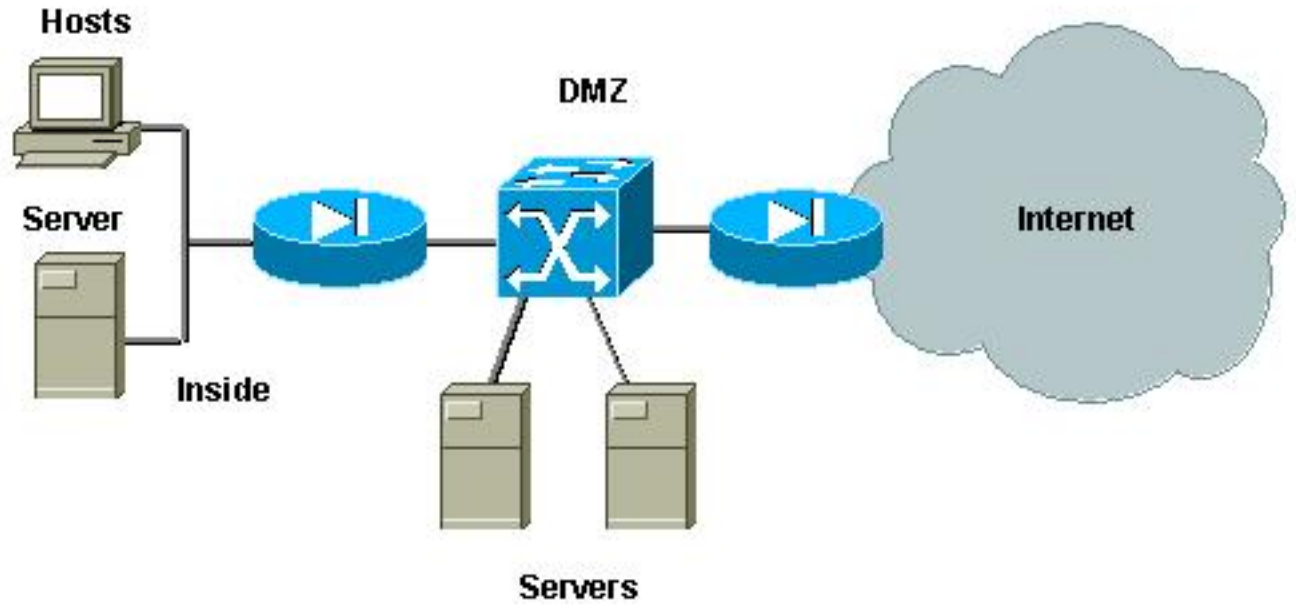
Deze scenario's zijn:

- doorvoer-DMZ
- Externe DMZ
- VPN-Concentrator in parallel met firewall

doorvoer-DMZ

Dit is één van de meest gebruikte scenario's. In dit voorbeeld wordt de DMZ uitgevoerd als een transitgebied tussen twee firewallrouters zoals weergegeven in de afbeelding hieronder.

Afbeelding 2: doorvoer-DMZ



In dit voorbeeld, zouden de servers van DMZ door zowel externe als interne gebruikers moeten worden benaderd, maar zij hoeven niet met elkaar te communiceren. In sommige gevallen moeten DMZ-servers een soort verbinding naar een interne host openen. Tegelijkertijd moeten interne klanten het internet zonder beperkingen benaderen. Een goed voorbeeld zal zijn met Web servers bij de DMZ, die moeten communiceren met een database server in het binnennetwerk en die binnen klanten toegang hebben tot het internet.

De externe firewall is ingesteld om inkomende verbindingen naar de servers in de DMZ mogelijk te maken, maar meestal worden er geen filter of beperkingen toegepast op het uitgaande verkeer, vooral het verkeer dat afkomstig is van de DMZ. Zoals we eerder in dit document hebben besproken, kan dit de activiteit van een aanvaller mogelijk vergemakkelijken om twee redenen: de eerste, zodra een van de DMZ-hosts gecompromitteerd is, worden alle andere DMZ-hosts blootgesteld; de tweede , een aanvaller kan gemakkelijk een uitgaande verbinding exploiteren .

Aangezien DMZ-servers niet met elkaar hoeven te praten, is de aanbeveling ervoor te zorgen dat ze op L2 zijn geïsoleerd. De serverpoorten worden gedefinieerd als PVLAN's geïsoleerde poorten, terwijl de poorten die op de twee firewalls aansluiten, worden gedefinieerd als veelbelovend. Het definiëren van een primair VLAN voor de firewalls en een secundair VLAN voor de DMZ-servers zal dit bereiken.

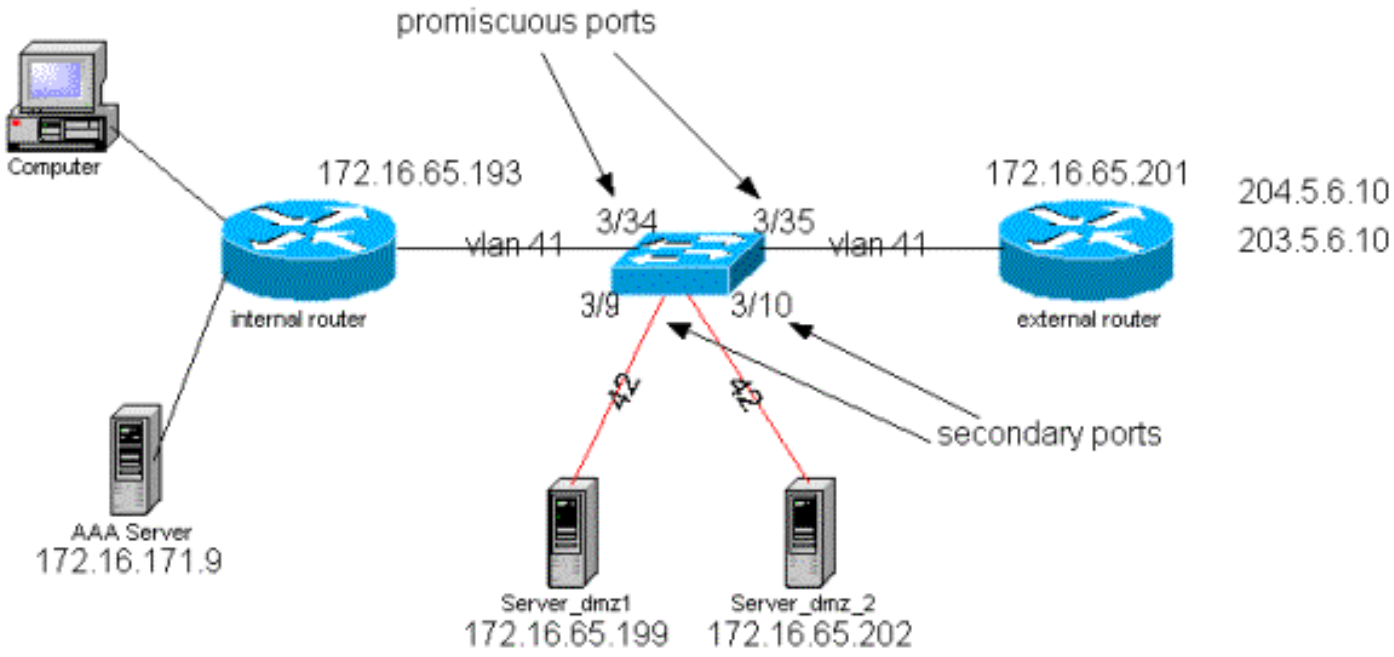
VACL’s worden gebruikt om het verkeer dat afkomstig is van de DMZ te controleren. Dit zal voorkomen dat een aanvaller een onrechtmatige uitgaande verbinding kan openen. Het is belangrijk om in gedachten te houden dat DMZ-servers niet alleen moeten reageren met het verkeer dat overeenkomt met sessies van klanten, maar ze zullen ook bepaalde extra services nodig hebben, zoals Domain Name System (DNS) en maximum transmission unit (MTU) door het vinden van een pad. De ACL moet dus alle diensten mogelijk maken die nodig zijn voor de DMZ-servers.

Doorvoersnelheid voor DMZ testen

In onze testbank hebben we een DMZ-segment geïmplementeerd met twee routers die zijn geconfigureerd als bed-servers, server_dmz1 en server_dmz2. Deze servers zouden zowel door buiten als binnen clients moeten worden benaderd, en alle HTTP-verbindingen zijn

geauthentiseerd door gebruik te maken van een interne RADIUS-server (Cisco Secure ACS voor UNIX). Zowel interne als externe routers worden geconfigureerd als firewalls voor pakketfilter. Het volgende plaatje illustreert het testbed, inclusief het gebruikte adresseringsschema.

Afbeelding 3: Doorvoersnelheid voor DMZ, testgebaseerd



De volgende lijst verzamelt de fundamentele configuratiestappen van PVLANs. Catalyst 6500 wordt gebruikt als L2-switch in de DMZ.

- Server_dmz_1 is aangesloten op poort 3/9
- Server_dmz_2 is aangesloten op poort 3/10
- De interne router is aangesloten op poort 3/34
- De externe router is aangesloten op poort 3/35

We kozen de volgende VLAN's:

- 41 is het primaire VLAN
- 42 is het geïsoleerde VLAN

Private VLAN-configuratie

De volgende configuratie stelt de PVLAN's in op de betrokken poorten.

```
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-configuratie op Primair VLAN

Deze sectie is van cruciaal belang om de beveiliging van de DMZ te verbeteren. Zoals beschreven in de gekende Beperkingen van VACL's en PVLAN's, zelfs als servers behoren tot twee verschillende secundaire VLAN's of tot hetzelfde geïsoleerde VLAN, is er nog steeds een manier waarop een aanvaller kan gebruiken om ze met elkaar te laten communiceren. Als de servers proberen direct te communiceren, zullen ze het niet kunnen doen bij L2 vanwege de PVLAN's. Als de servers gecompromitteerd en dan gevormd worden door een indringer op dusdanige wijze dat het verkeer voor het zelfde voorwerp naar de router wordt verzonden, zal deze het verkeer op zelfde vorm terugleiden, en zo het doel van PVLANs verslaan.

Daarom moet een VACL op het primaire VLAN (het VLAN dat het verkeer van de routers) met het volgende beleid worden geconfigureerd:

- staan het verkeer toe waarvan bron IP het IP van de router is
- Ontken het verkeer met zowel bron- als doelIPs die het DMZ-subsysteem zijn
- Alle rest van het verkeer toestaan

```
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
```

Deze ACL heeft geen invloed op het door de servers gegenereerde verkeer; het zal alleen verhinderen dat de routers het verkeer routeren dat van de servers naar hetzelfde VLAN komt. De eerste twee verklaringen staan de routers toe om berichten zoals icmp om te leiden of icmp onbereikbaar naar de servers te verzenden.

VACL-configuratie op secundair VLAN

De volgende configuratielogbestanden worden gebruikt om te laten zien hoe we een VACL instellen om het verkeer te filteren dat door de servers gegenereerd is. Door deze VACL te configureren willen we het volgende bereiken:

- Sta **ping** van servers toe (**sta echo toe**)
- Beletten dat **echo-**antwoorden de servers verlaten
- HTTP-verbindingen van buitenaf toestaan
- Toestaan van RADIUS-verificatie (UDP-poort 1645) en accounting (UDP-poort 1646) verkeer
- DNS-verkeer toestaan (UDP poort 5.3)

We willen alle rest van het verkeer voorkomen.

Wat de fragmentatie betreft, gaan we uit van het volgende op het serversegment:

- De servers zullen geen gefragmenteerd verkeer genereren
- De servers zouden gefragmenteerd verkeer kunnen ontvangen

Gezien het hardwareontwerp van de PFC van supervisor 1 van Catalyst 6500, is het beter om de fragmenten van ICMP expliciet te ontkennen De reden is dat de fragmenten en het echo-antwoord door de hardware als hetzelfde worden beschouwd en dat de hardware standaard geprogrammeerd is om fragmenten expliciet toe te staan. Dus als u wilt voorkomen dat de echo-antwoordpakketten de servers verlaten, moet u dit expliciet configureren met de lijn **en elk fragment** van **een fragment ontkennen**.

```
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
```

De configuratie testen

De volgende uitvoer werd opgenomen wanneer PVLAN's zijn geconfigureerd maar er nog geen VACL is toegepast. Deze test toont aan dat de gebruiker vanaf de externe router zowel de interne router als de servers **kan pingelen**.

```
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
```

Het volgende voorbeeld laat zien dat we van de servers naar het externe netwerk kunnen **pingelen**, de standaardpoort, maar niet de servers die tot hetzelfde secundaire VLAN behoren.

```
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)
```

Na het in kaart brengen van VACL's gaat het **pingelen** van de externe router niet meer slagen:

```
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)
```

Het volgende voorbeeld toont de server die HTTP GET verzoeken van het interne netwerk ontvangt:

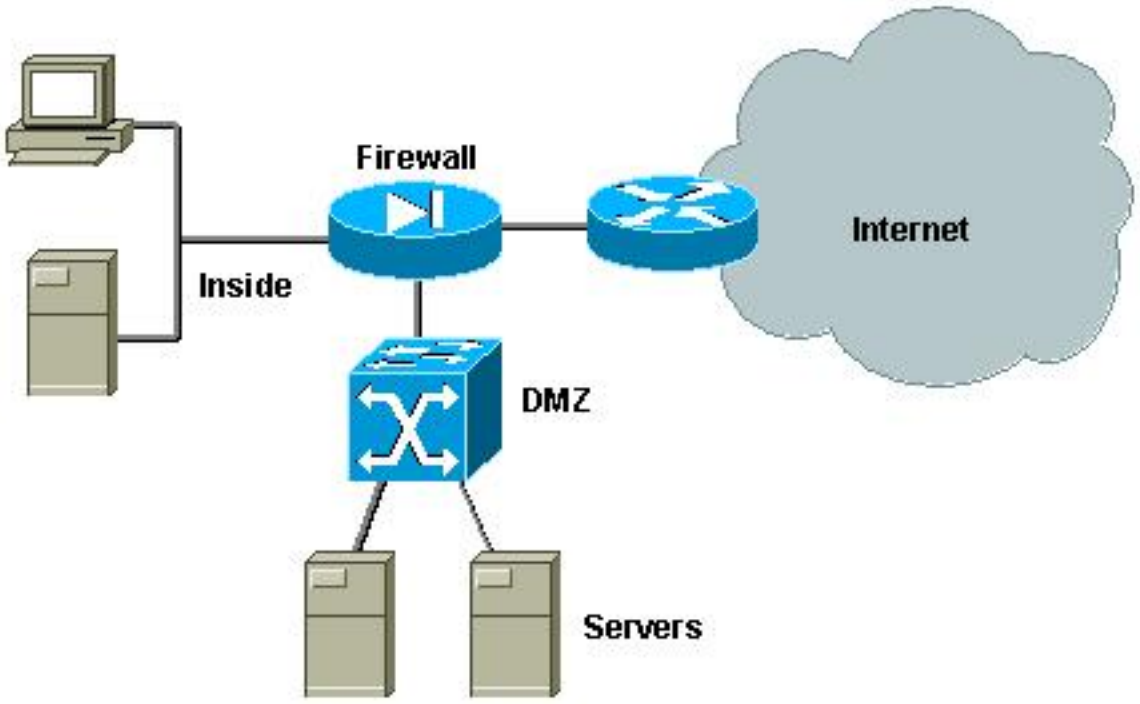
```
server_dmz1#debug ip http url
```

```
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

Het externe DMZ-scenario is waarschijnlijk de meest geaccepteerde en veelgebruikte implementatie. Een externe DMZ wordt uitgevoerd door gebruik te maken van een of meer interfaces van een firewall, zoals de onderstaande afbeelding.

Afbeelding 4: Externe DMZ



Normaal gesproken zijn de eisen voor DMZ's hetzelfde, ongeacht de ontwerpimplementatie. Zoals in het vorige geval, moeten de DMZ-servers zowel van externe klanten als van het interne netwerk toegankelijk zijn. DMZ-servers zullen uiteindelijk toegang nodig hebben tot een aantal interne bronnen, en ze worden niet verondersteld met elkaar te praten. Tegelijkertijd dient er geen verkeer te worden geïnitieerd van de DMZ naar het internet; deze DMZ-servers mogen alleen antwoorden met verkeer dat overeenkomt met inkomende verbindingen.

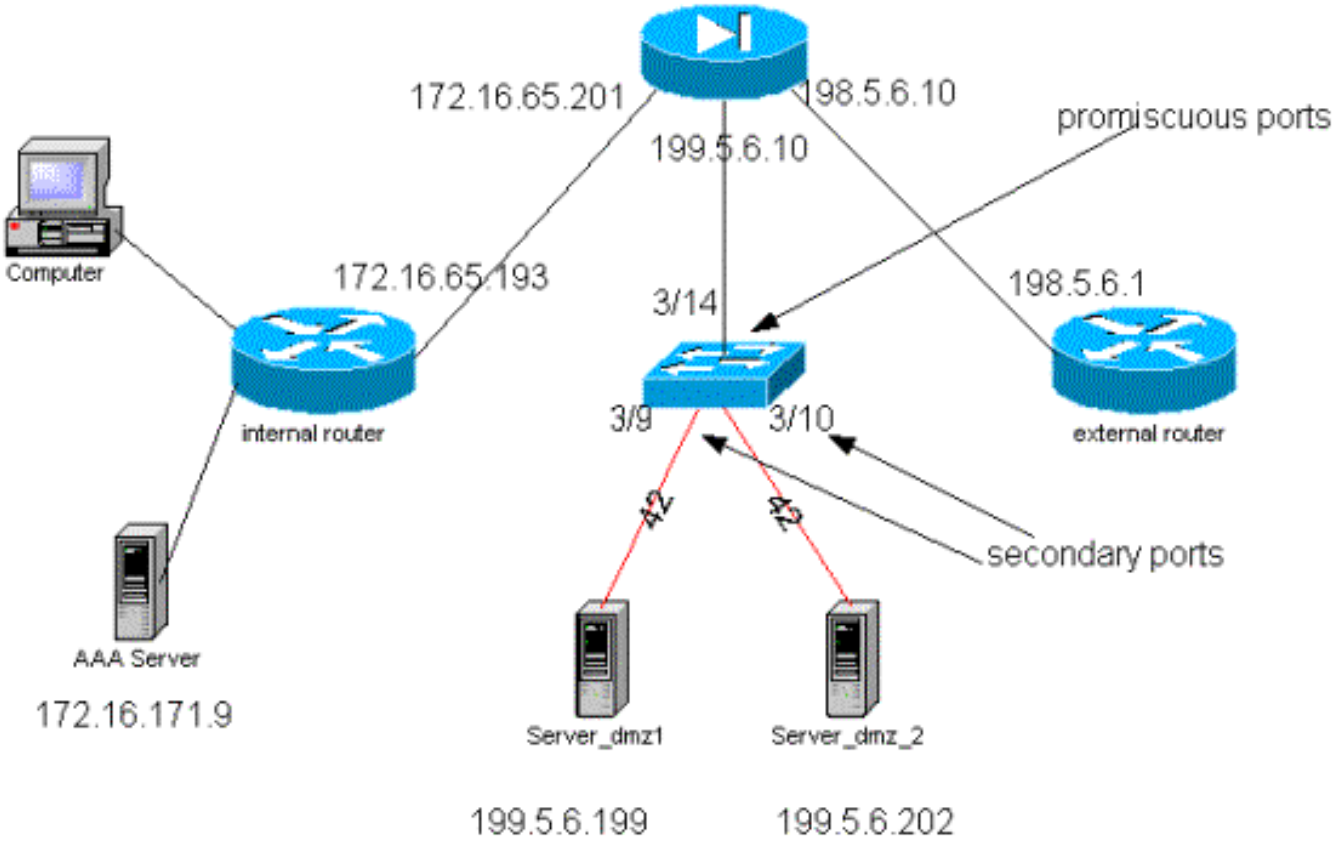
Zoals in de vorige casestudy, bestaat de eerste configuratiestap in het bereiken van isolatie bij L2 door middel van PVLAN's, en om ervoor te zorgen dat de DMZ-servers niet met elkaar kunnen praten terwijl interne en externe hosts toegang hebben tot deze servers. Dit wordt geïmplementeerd door de servers in een secundair VLAN in te stellen met geïsoleerde poorten. De firewall zou in een primair VLAN met een veelbelovende poort moeten worden gedefinieerd. De firewall zal het enige apparaat binnen dit primaire VLAN zijn.

De tweede stap is het definiëren van ACL's om het verkeer te controleren dat uit de DMZ voortkomt. Bij het definiëren van deze ACL's moeten we ervoor zorgen dat alleen het gewenste verkeer is toegestaan.

Externe DMZ testen

Het onderstaande beeld toont de testbank die voor deze casestudy is geïmplementeerd, waarbij we een PIX-firewall met een derde interface voor DMZ hebben gebruikt. Dezelfde set routers wordt gebruikt als webservers, en alle HTTP-sessies zijn geauthentiseerd met dezelfde RADIUS-server.

Afbeelding 5: Externe DMZ testbank



Voor dit scenario voegen we alleen de interessantere fragmenten uit de configuratiebestanden toe, aangezien de PVLAN's en VACL-configuraties in de vorige casestudy in detail zijn uitgelegd.

PIX-configuratie

```
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-configuratie

NAS-configuratie

```
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-serverCSUX

```
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-configuratie

Het moet worden opgemerkt dat in deze configuratie er geen behoefte is om een VACL op het primaire VLAN te configureren omdat de PIX geen verkeer vanuit dezelfde interface richt als waar

het vandaan kwam. Een VACL zoals die in de VACL-configuratie op de sectie Primair VLAN wordt beschreven, is overbodig.

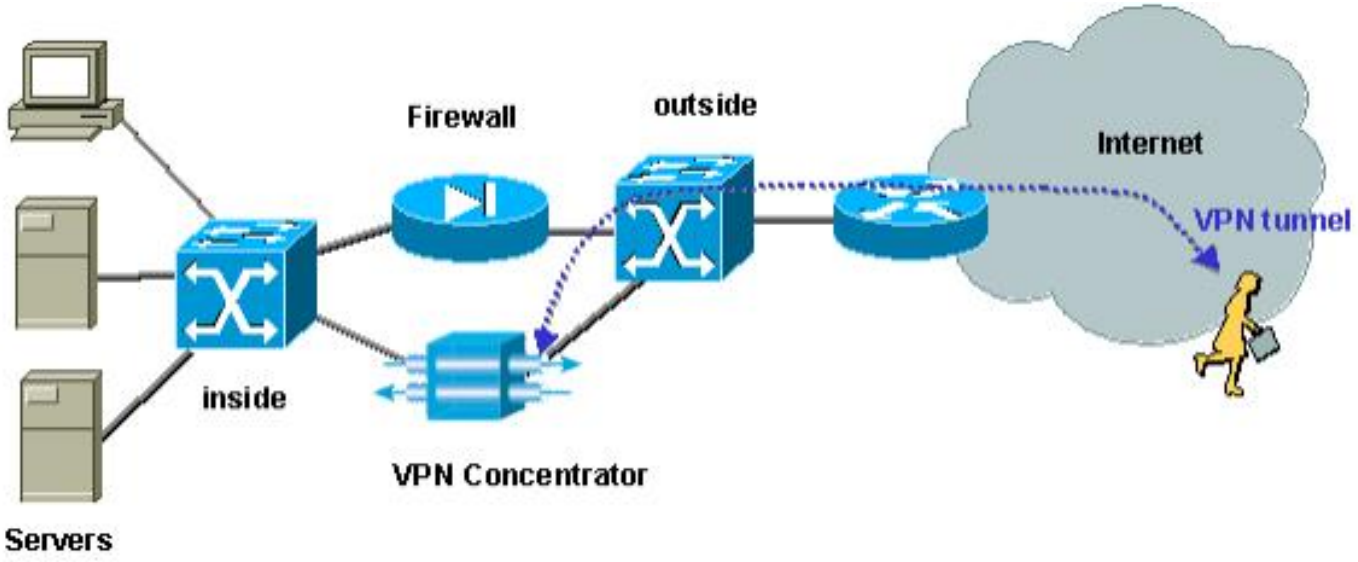
```
set security acl ip dmz_servers_out
------------------------------------------------
1. deny icmp any any fragment
2. permit icmp host 199.5.6.199 any echo
3. permit icmp host 199.5.6.202 any echo
4. permit tcp host 199.5.6.199 eq 80 any established
5. permit tcp host 199.5.6.202 eq 80 any established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

VPN-Concentrator in parallel met firewall

Bij het implementeren van Access Virtual Private Networks (VPN's) is ongetwijfeld een van de favoriete benaderingen het parallelle ontwerp (geïllustreerd in de onderstaande afbeelding). Klanten geven doorgaans de voorkeur aan deze ontwerpbenadering omdat deze makkelijk te implementeren is, zonder impact op de bestaande infrastructuur, en omdat het relatief gemakkelijk te opschalen is op basis van de flexibiliteit van het apparaat.

In de parallelle benadering sluit de VPN-concentrator zich aan op zowel binnen- als buitenkant. Alle VPN-sessies eindigen bij de concentrator zonder de firewall uit te voeren. Gewoonlijk wordt van VPN-klanten verwacht dat ze onbeperkte toegang tot het interne netwerk hebben, maar soms kan hun toegang worden beperkt tot een reeks binnenservers (serverboerderij). Een van de gewenste functies is het VPN-verkeer te scheiden van het normale internetverkeer. VPN-clients zijn bijvoorbeeld niet toegestaan om via de firewall van het bedrijf toegang te krijgen tot internet.

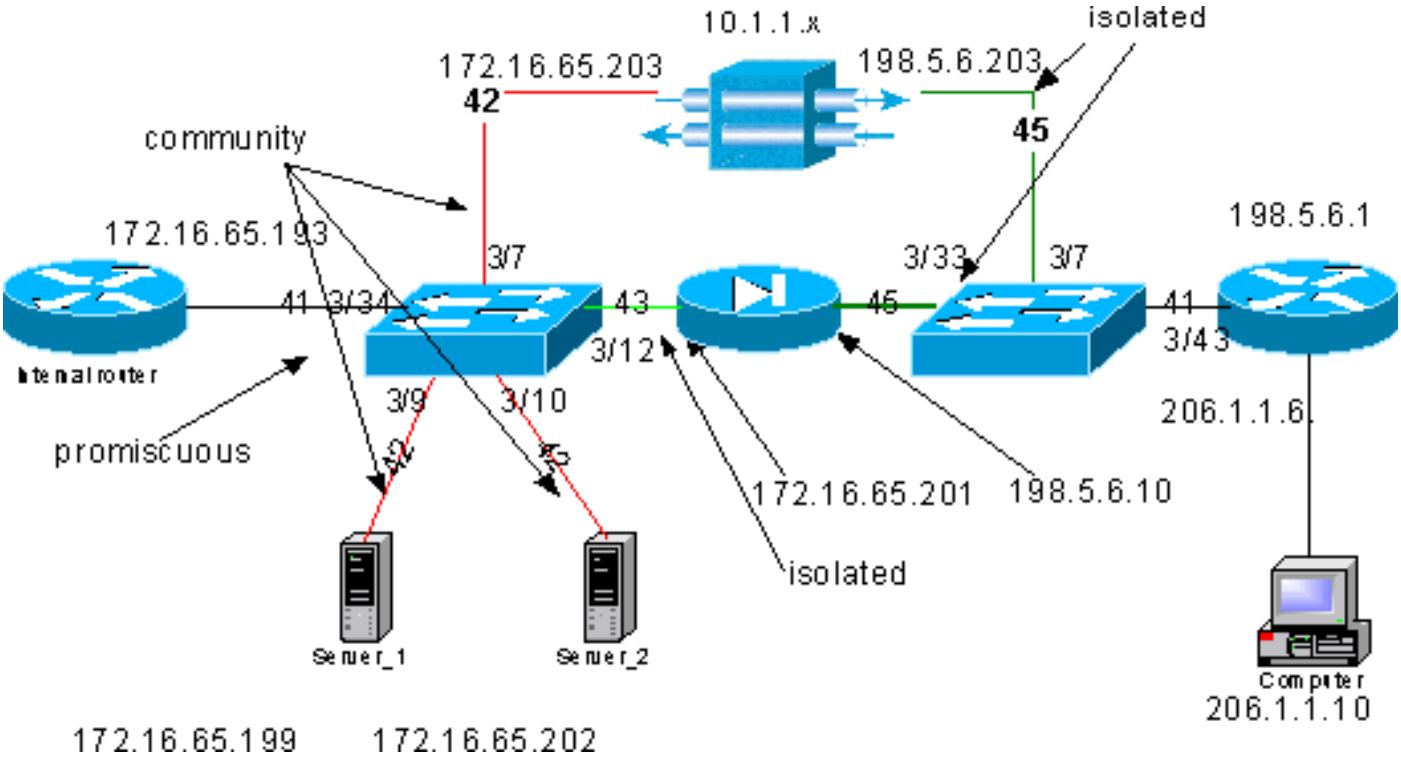
Afbeelding 6: VPN-Concentrator in parallel met firewall



[VPN-concentratie tegelijkertijd testen met firewall]

In dit voorbeeld gebruikten we een VPN 5000 Concentrator, die parallel met een PIX-firewall was geïnstalleerd. De twee routers die als Webservers waren geconfigureerd werden in het binnensegment geïnstalleerd als een interne serverboerderij. VPN-clients hebben alleen toegang tot de serverboerderij en internetverkeer moet van VPN-verkeer (IPSec) worden gescheiden. In onderstaande afbeelding is de testopslag te zien.

Afbeelding 7: VPN-Concentrator parallel met firewall-testbank



In dit scenario hebben we twee belangrijke gebieden:

- De interne L2-switch
- De externe L2-switch

De verkeersstromen voor de interne L2-switch worden gedefinieerd op basis van de volgende verklaringen:

- VPN-klanten hebben volledige toegang tot een vooraf bepaalde reeks interne servers (serverboerderij)
- Interne klanten mogen ook toegang krijgen tot de serverboerderij
- Interne klanten hebben onbeperkte toegang tot internet
- Verkeer dat u vanuit de VPN-concentrator komt, moet worden geïsoleerd uit de PIX-firewall

De verkeersstromen voor de externe L2-switch worden als volgt gedefinieerd:

- Het verkeer dat van de router komt moet in staat zijn om naar de VPN-concentrator of de PIX te gaan
- Het verkeer dat uit de PIX komt moet worden geïsoleerd van het verkeer dat uit VPN komt

Bovendien is het mogelijk dat de beheerder verkeer van het interne netwerk wil verhinderen om zijn weg naar de hosts te maken, dit kan worden bereikt door middel van VACL's die zijn geconfigureerd op het primaire VLAN (VACL zal alleen het verkeer filteren dat van de interne router vertrekt, geen ander verkeer zal worden beïnvloed).

PVLAN-configuratie

Aangezien het belangrijkste doel in dit ontwerp is om het verkeer dat van PIX komt gescheiden te houden van het verkeer dat van de servers en van de VPN-concentrator komt, vormen we de PIX op een ander PVLAN dan PVLAN waarop de servers en de VPN-concentrator zijn geconfigureerd.

Het verkeer dat van het interne netwerk komt moet toegang hebben tot de serverboerderij zowel als de VPN concentrator en de PIX. Als gevolg daarvan zal de poort die zich verbindt met het interne netwerk een veelbelovende haven zijn.

De servers en de VPN concentrator behoren tot hetzelfde secundaire VLAN omdat ze met elkaar zullen kunnen communiceren.

Wat de externe L2-switch betreft, wordt de router die toegang tot internet geeft (wat normaal tot een Internet Service Provider (ISP) behoort) aangesloten op een veelbelovende poort terwijl de VPN-concentrator en de PIX behoren tot dezelfde privé en geïsoleerde VLAN's (zodat ze geen verkeer kunnen uitwisselen). Door dit te doen, kan het verkeer van de dienstverlener of het pad naar de VPN concentrator of het pad naar de PIX nemen. De PIX- en VPN-concentrator worden beter beschermd omdat ze geïsoleerd zijn.

PVLAN-configuratie van de interne L2-Switch

```
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-configuratie van de externe L2-Switch

```
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
```

De configuratie testen

Dit experiment toont aan dat de interne router door de firewall kan gaan en de externe router (de externe firewallrouter waarvan de interface 198.5.6.1 is) kan bereiken.

```
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
```

Dit experiment toont het volgende, allemaal van server 1:

- Server 1 kan de interne router pingelen:

```
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 kan VPN pingelen:

```
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 kan PIX-interne interface niet pingelen:

```
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 kan de externe router niet pingelen:

```
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)
```

Het volgende experiment toont aan dat HTTP sessies kunnen worden geopend van het interne netwerk naar de serverboerderij.

```
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 ''
```

Het volgende experiment toont aan dat het HTTP-verkeer van het VPN-netwerk zijn weg kan maken naar de serverboerderij (merk het adres 10.1.1.1 op.)

```
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
```

Het volgende is de configuratie van de VPN-concentrator:

```
[ 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"
```

De volgende opdracht toont de lijst met aangesloten gebruikers:

```
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
```

Het moet opgemerkt worden dat de standaardgateway op de servers de interne router 172.16.65.193 is, die een icmp-omleiding naar 172.16.65.203 geeft. Deze implementatie veroorzaakt niet-optimale verkeersstromen, omdat de host het eerste pakket van een stroom naar de router zou sturen, en na ontvangst van de router, zal ze het redirect sturen volgende pakketten naar de gateway die meer geschikt is om dit verkeer af te handelen. U kunt ook twee verschillende routes op de servers zelf configureren om naar VPN te wijzen voor de 10.x.x.x-adressen en naar 172.16.65.193 voor de rest van het verkeer. Als alleen de standaardgateway op de servers is ingesteld, moeten we ervoor zorgen dat de router-interface is ingesteld met "ip redirect".

Een interessant punt dat we tijdens de test zagen is de volgende. Als we proberen een extern adres als 198.5.6.1 te pingelen van de servers of van VPN, zal de standaardgateway naar 172.16.65.201 sturen en icmp omleiden naar 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)
```

De servers of VPN zullen op dit punt een verzoek om een adresresolutie Protocol (ARP) voor

172.16.65.201 verzenden en geen antwoord van 201 krijgen omdat het op een ander secundair VLAN is; Dit is wat PVLAN ons biedt. In werkelijkheid is er een makkelijke manier om dit te bereiken, namelijk om het verkeer naar de MAC van 2.193 en met de bestemming IP van 172.16.65.201 te sturen.

De router .193 zal het verkeer terug naar de zelfde interface leiden, maar aangezien de router interface een veelbelovende haven is, zal het verkeer 0.201 bereiken, wat wij wilden verhinderen. Dit probleem werd uitgelegd in de sectie Bekende beperkingen van VACL's en PVLAN's.

VACL-configuratie

Deze sectie is van cruciaal belang om de beveiliging op de serverboerderij te verbeteren. Zoals beschreven in de gekende Beperkingen van VACL's en PVLAN's, zelfs als servers en de PIX behoren tot twee verschillende secundaire VLAN's, is er nog een methode die een aanvaller kan gebruiken om ze aan elkaar te laten communiceren. Als ze direct proberen te communiceren, zullen ze het niet kunnen doen vanwege de PVLAN's. Als de servers gecompromitteerd en dan gevormd worden door een indringer op dusdanige wijze dat het verkeer voor het zelfde voorwerp naar de router wordt verzonden, zal deze het verkeer op zelfde vorm terugleiden, en zo het doel van PVLANs verslaan.

Daarom moet een VACL op het primaire VLAN (het VLAN dat het verkeer van de routers) met het volgende beleid worden geconfigureerd:

- staan het verkeer toe waarvan bron IP het IP van de router is
- Ontken het verkeer met zowel bron als bestemming IPs die van de serverkwekerij zijn voorzien
- Alle rest van het verkeer toestaan

```
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
```

Deze ACL heeft geen invloed op het verkeer dat door de servers of door de PIX wordt gegenereerd; het zal alleen verhinderen dat de routers het verkeer routeren dat van de servers naar hetzelfde VLAN komt. De eerste twee verklaringen staan de routers toe om berichten als icmp om te leiden of icmp onbereikbaar naar de servers te verzenden.

We identificeerden een andere verkeersstroom die de beheerder met behulp van VACL's zou willen stoppen, en deze stroom is van het interne netwerk naar de VPN hosts. Om dit te doen, kan een VACL aan het primaire VLAN (41) in kaart worden gebracht en gecombineerd met het vorige:

```
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
```

De configuratie testen

We pompen nu de 10.1.1.1 host uit de router .193 (zundapp). Voordat we de VACL in kaart brengen, is **ping** geslaagd.

```
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
```

Na het in kaart brengen van VACL op VLAN 41, zal zelfde **ping** niet slagen:

```
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)
```

U kunt de externe router echter nog steeds **pingelen**:

```
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
```

Gerelateerde informatie

- Configuratie van toegangscontrolelijsten - Catalyst 6000 documentatie
- Technische ondersteuning - Cisco-systemen