# Toegangscontrolelijsten en IP-fragmentaties

## Inhoud



## Inleiding

Dit Witboek verklaart de verschillende soorten van de ingangen van de Toegangscontrolelijst (ACL) en wat er gebeurt wanneer verschillende soorten pakketten deze verschillende ingangen tegenkomen. ACL's worden gebruikt om IP-pakketten te blokkeren nadat deze door een router zijn verzonden.

RFC 1858 bespreekt beveiligingsoverwegingen voor IP-fragment-filtering en benadrukt twee aanvallen op hosts die IP-fragmenten van TCP-pakketten omvatten, de kleine fragmentatie-aanval en de overlappende fragmentatie-aanval. Het blokkeren van deze aanvallen is wenselijk omdat ze een gastheer kunnen aantasten of al zijn interne middelen kunnen vastbinden.

RFC 1858 beschrijft ook twee methoden om tegen deze aanvallen te verdedigen: de directe en de indirecte. In de directe methode worden initiële fragmenten die kleiner zijn dan een minimumlengte, weggegooid. De indirecte methode is het wegwerpen van het tweede fragment van een fragment-set, als deze 8 bytes in het oorspronkelijke IP-datagram start. Zie RFC 1858 voor meer informatie.

Traditioneel worden pakketfilters als ACL's toegepast op de niet-fragmenten en het eerste fragment van een IP-pakket omdat ze zowel Layer 3 als 4-informatie bevatten waartegen de ACL's kunnen matchen voor een licentie of beslissingen weigeren. Niet-initiële fragmenten zijn traditioneel toegestaan door de ACL omdat ze geblokkeerd kunnen worden op basis van Layer 3-informatie in de pakketten; Maar omdat deze pakketten geen informatie van Layer 4 bevatten, komen ze niet overeen met Layer 4 informatie in de ACL-ingang, als deze bestaat. Het toestaan van de niet-initiële fragmenten van een IP-datagram is aanvaardbaar omdat de host die de fragmenten ontvangt, niet in staat is het oorspronkelijke IP-datagram opnieuw te assembleren zonder het eerste fragment.

Firewalls kunnen ook worden gebruikt om pakketten te blokkeren door een tabel met pakketfragmenten te onderhouden, die is geïndexeerd aan de bron en het bestemming van IP-

adres, protocol en IP-ID. Zowel de Cisco PIX-firewall als de Cisco IOS® Firewall kunnen alle fragmenten van een bepaalde stroom filteren door deze informatietabel te behouden, maar het is te duur om dit op een router te doen voor basis-ACL-functies. De primaire taak van een firewall is om pakketten te blokkeren, en zijn secundaire rol is om pakketten te verzenden; de primaire taak van een router is pakketten te routeren , en zijn secundaire rol is deze te blokkeren .

Er zijn twee wijzigingen aangebracht in Cisco IOS-softwarereleases 12.1(2) en 12.0(11) om bepaalde security problemen rond TCP-fragmenten aan te pakken. De indirecte methode, zoals beschreven in RFC 1858 , werd geïmplementeerd als onderdeel van de standaard TCP/IP-pakketanalysecontrole. Er werden ook wijzigingen aangebracht in de ACL-functionaliteit met betrekking tot niet-initiële fragmenten.

## Typen ACL-vermeldingen

Er zijn zes verschillende typen ACL-lijnen, en elk heeft een gevolg als een pakket wel of niet overeenkomt. In de volgende lijst geeft FO = 0 een non-fragment of een initieel fragment in een TCP-stroom aan, met FO > 0 dat het pakket een niet-initieel fragment is, met L3 Layer 3 en met L4 Layer 4.

**Opmerking:** Wanneer er zowel Layer 3 als Layer 4 informatie in de ACL-lijn is en het sleutelwoord van **fragmenten** aanwezig is, is de ACL-actie conservatief voor zowel de licentie- als ontkenningsacties. De handelingen zijn conservatief omdat u niet per ongeluk een gefragmenteerd deel van een stroom wilt ontkennen omdat de fragmenten niet voldoende informatie bevatten om alle filtereigenschappen aan te passen. In het ontkenningsgeval, in plaats van een niet-eerste fragment te ontkennen, wordt de volgende ACL-ingang verwerkt. In het vergunningsgeval, wordt verondersteld dat de informatie van Layer 4 in het pakket, indien beschikbaar, de informatie van Layer 4 in de ACL lijn aanpast.

### Alleen ACL-lijn met L3-informatie toestaan

1. Als de L3-informatie van een pakket overeenkomt met de L3-informatie in de ACL-lijn, is deze toegestaan.
2. Als de L3-informatie van een pakket niet overeenkomt met de L3-informatie in de ACL-lijn, wordt de volgende ACL-ingang verwerkt.

### Dense ACL-lijn met alleen L3-informatie

1. Als de L3-informatie van een pakket overeenkomt met de L3-informatie in de ACL-lijn, wordt de informatie ontkend.
2. Als de L3-informatie van een pakket niet overeenkomt met de L3-informatie in de ACL-lijn, wordt de volgende ACL-ingang verwerkt.

### Toestaan ACL-lijn met alleen L3-informatie en het sleutelwoord fragmenten is aanwezig

Als de L3-informatie van een pakje overeenkomt met de L3-informatie in de ACL-lijn, wordt de offset van het pakket geselecteerd.

1. Als de inhoud van een pakje > 0 is, is het pakje toegestaan.
2. Als een pakket FO = 0 is, wordt de volgende ACL-ingang verwerkt.

### Ontken ACL-lijn met alleen L3-informatie en het sleutelwoord fragmenten is aanwezig

Als de L3-informatie van een pakje wel overeenkomt met de L3-informatie in de ACL-lijn, wordt de offset van het pakket geselecteerd.

1. Als een pakje van > 0 is, wordt het pakje ontkend.
2. Als een pakje FO = 0 is, wordt de volgende ACL-lijn verwerkt.

### Toegangscontrolelijn voor ACL's met L3- en L4-informatie

1. Als de L3- en L4-informatie van een pakket overeenkomen met de ACL-lijn en FO = 0, is het pakket toegestaan.
2. Als de L3-informatie van een pakket overeenkomt met de ACL-lijn en FO > 0, is het pakket toegestaan.

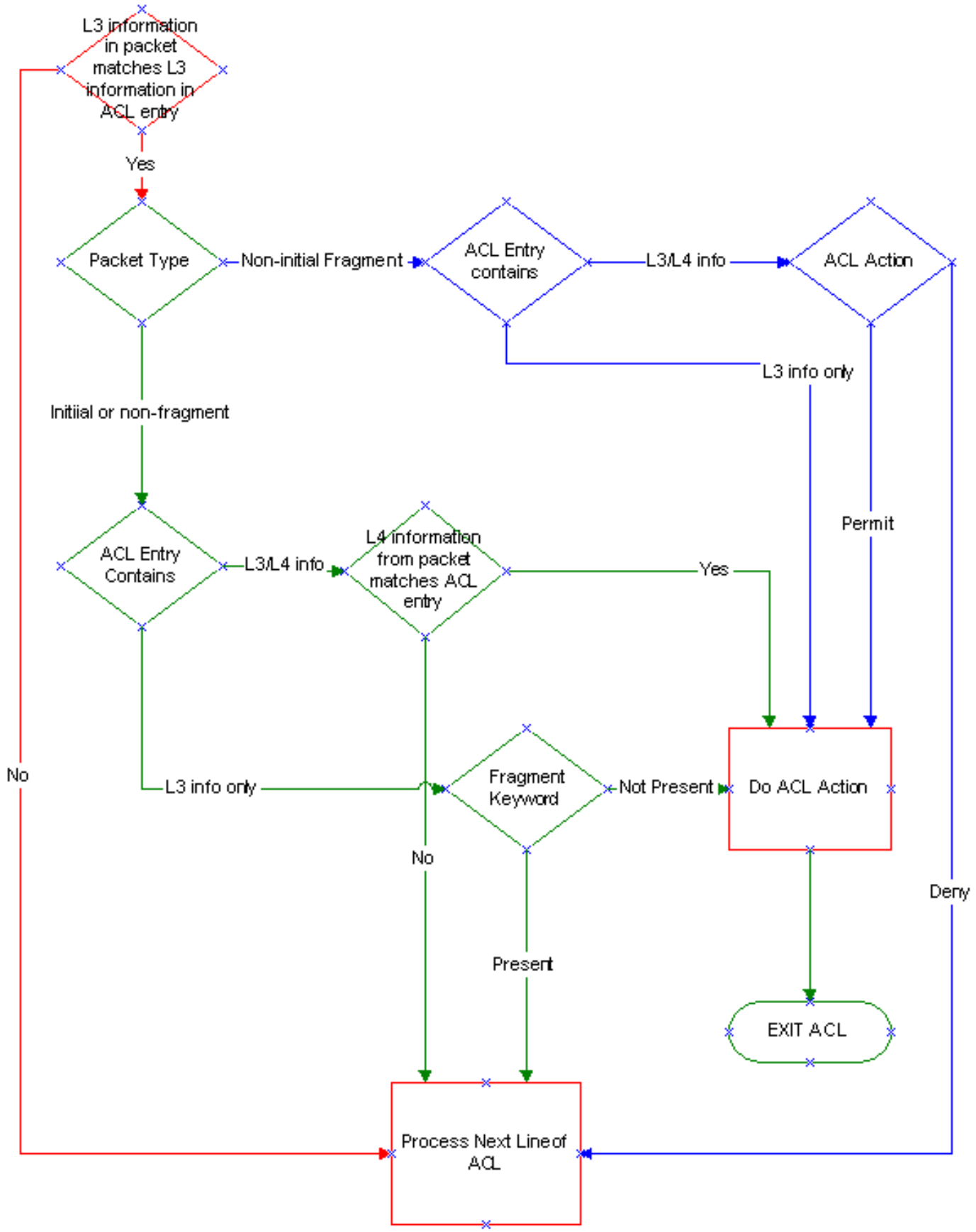
### Dense ACL-lijn met L3- en L4-informatie

1. Als de L3- en L4-informatie van een pakje met de ACL-ingang en FO = 0 overeenkomt, wordt het pakje geweigerd.
2. Als de L3-informatie van een pakket overeenkomt met de ACL-lijn en FO > 0, wordt de volgende ACL-ingang verwerkt.

## ACL-lijnkaart

Het volgende stroomschema illustreert de ACL-regels wanneer niet-fragmenten, initiële fragmenten en niet-initiële fragmenten tegen de ACL worden gecontroleerd.

**Opmerking:** De niet-initiële fragmenten zelf bevatten alleen Layer 3, nooit Layer 4 informatie, hoewel ACL zowel Layer 3 als Layer 4 informatie kan bevatten.




# Hoe pakketten overeenkomen met een ACL

## Voorbeeld 1

De volgende vijf mogelijke scenario's omvatten verschillende types van pakketten die ACL 100

tegenkomen. Raadpleeg de tabel en het stroomschema zoals u volgt wat in elke situatie gebeurt. Het IP-adres van de webserver is 171.16.23.1.

```
access-list 100 permit tcp any host 171.16.23.1 eq 80

access-list 100 deny ip any any
```

### Het pakket is een eerste fragment of een niet-fragment dat voor de server op poort 80 is bestemd:

De eerste lijn van ACL bevat zowel Layer 3 als Layer 4-informatie, die overeenkomt met Layer 3 en Layer 4 informatie in het pakket, zodat het pakket is toegestaan.

### Het pakket is een eerste fragment of een niet-fragment dat voor de server op poort 21 is bestemd:

1. De eerste lijn van ACL bevat zowel Layer 3 als Layer 4-informatie, maar de informatie op Layer 4 in ACL komt niet overeen met het pakket, zodat de volgende ACL-lijn wordt verwerkt.
2. De tweede lijn van ACL ontkent alle pakketten, zodat het pakket wordt ontkend.

### Het pakket is een niet-eerste fragment naar de server in een poort 80-flow:

De eerste lijn van ACL bevat Layer 3 en Layer 4 informatie, de informatie van Layer 3 in de ACL komt overeen met het pakket en de actie ACL is om toe te staan, zodat het pakket is toegestaan.

### Het pakket is een niet-eerste fragment naar de server in een poort 21-flow:

De eerste lijn van ACL bevat zowel Layer 3 als Layer 4-informatie. Layer 3 informatie in de ACL komt overeen met het pakket, er is geen Layer 4-informatie in het pakket en de ACL-actie is vereist om toe te staan, zodat het pakket is toegestaan.

### Het pakket is een eerste fragment, niet-fragment of niet-initieel fragment naar een andere host op de server-subversie:

1. De eerste lijn van ACL bevat Layer 3-informatie die niet overeenkomt met Layer 3-informatie in het pakket (het doeladres), zodat de volgende ACL-lijn wordt verwerkt.
2. De tweede lijn van ACL ontkent alle pakketten, zodat het pakket wordt ontkend.

## Voorbeeld 2

De volgende vijf mogelijke scenario's omvatten verschillende types van pakketten die ACL 101 tegenkomen. Nogmaals, raadpleeg de tabel en het stroomschema zoals u volgt wat in elke situatie gebeurt. Het IP-adres van de webserver is 171.16.23.1.

```
access-list 101 deny ip any host 171.16.23.1 fragments

access-list 101 permit tcp any host 171.16.23.1 eq 80
```

```
access-list 101 deny ip any any
```

### Het pakje is een eerste fragment of een niet-fragment dat voor de server is bestemd op poort 80:

1. De eerste regel van ACL bevat Layer 3-informatie die overeenkomt met Layer 3-informatie in het pakket. De ACL-actie moet worden ontkend, maar omdat het sleutelwoord **fragmenten** aanwezig is, wordt de volgende ACL-ingang verwerkt.
2. De tweede lijn van ACL bevat Layer 3 en Layer 4 informatie, die overeenkomt met het pakket, zodat het pakket is toegestaan.

### Het pakket is een eerste fragment of een niet-fragment dat voor de server op poort 21 is bestemd:

1. De eerste lijn van ACL bevat Layer 3 informatie, die het pakket aanpast, maar de ACL-ingang heeft ook het sleutelwoord van **fragmenten**, dat niet overeenkomt met het pakket omdat FO = 0, zodat de volgende ACL-ingang wordt verwerkt.
2. De tweede lijn van ACL bevat Layer 3 en Layer 4 informatie. In dit geval komt de informatie van Layer 4 niet overeen, zodat de volgende ACL-ingang wordt verwerkt.
3. De derde lijn van ACL ontkent alle pakketten, zodat het pakket wordt ontkend

### Het pakket is een niet-eerste fragment naar de server in een poort 80-flow:

De eerste regel van ACL bevat Layer 3-informatie die overeenkomt met Layer 3-informatie in het pakket. Vergeet niet dat, ook al is dit deel van een poort 80 flow, er geen Layer 4 informatie in het niet-initiële fragment is. Het pakket wordt ontkend omdat Layer 3-informatie overeenkomt.

### Het pakket is een niet-eerste fragment naar de server in een poort 21-flow:

De eerste lijn van ACL bevat slechts informatie van Layer 3 en het past het pakket aan, zodat het pakket wordt ontkend.

### Het pakket is een eerste fragment, niet-fragment of niet-initieel fragment naar een andere host op de server-subversie:

1. De eerste regel van ACL bevat slechts informatie van Layer 3 en het komt niet overeen met het pakket, zodat de volgende ACL-lijn wordt verwerkt.
2. De tweede lijn van ACL bevat Layer 3 en Layer 4 informatie. Layer 4 en Layer 3 informatie in het pakket komen niet overeen met die van ACL, zodat de volgende ACL-lijn wordt verwerkt.
3. De derde lijn van ACL ontkent dit pakket

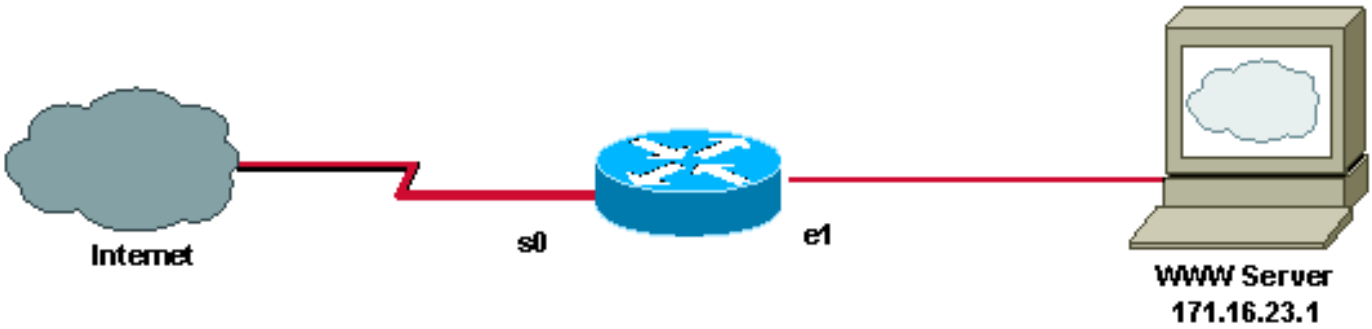
## fragmenten-sleutelwoordscenario's

### Scenario 1

Router B verbindt zich met een webserver en de netwerkbeheerder wil geen fragmenten toestaan om de server te bereiken. Dit scenario toont wat gebeurt als de netwerkbeheerder ACL 100 tegen ACL 101 implementeert. ACL wordt binnenkomend toegepast op de routers Seriële0 (s0) interface en zou alleen niet-gefragmenteerde pakketten om de webserver te bereiken moeten toestaan. Zie

het ACL-schema van regels en de Hoe pakketten bij een ACL-gedeelte kunnen worden afgestemd op het scenario.

## Gevolgen van het gebruik van het fragment




Het volgende is ACL 100:

```
access-list 100 permit tcp any host 171.16.23.1 eq 80

access-list 100 deny ip any any
```

De eerste lijn van ACL 100 staat slechts HTTP aan de server toe, maar het maakt ook niet-initiële fragmenten aan om het even welke TCP poort op de server mogelijk. Het staat deze pakketten toe omdat de niet-aanvankelijke fragmenten geen informatie van Layer 4 bevatten, en de ACL logica veronderstelt dat als de informatie van Layer 3 aan elkaar past, de informatie van Layer 4 ook zou aanpassen, als het beschikbaar was. De tweede lijn is impliciet en ontkent al het andere verkeer.

Het is belangrijk om op te merken dat, vanaf Cisco IOS-softwarereleases 12.1(2) en 12.0(11), de nieuwe ACL-code fragmenten laat vallen die niet overeenkomen met een andere lijn in de ACL. Eerdere releases staan niet-initiële fragmenten door toe als ze niet overeenkomen met een andere lijn van de ACL.

Het volgende is ACL 101:

```
access-list 101 deny ip any host 171.16.23.1 fragments

access-list 101 permit tcp any host 171.16.23.1 eq 80

access-list 101 deny ip any any
```

ACL 101 staat niet-initiële fragmenten door aan de server toe vanwege de eerste regel. Een niet-eerste fragment naar de server wordt ontkend wanneer de eerste ACL-lijn wordt tegengekomen omdat Layer 3-informatie in het pakket overeenkomt met Layer 3-informatie in de ACL-lijn.

Initiële of niet-fragmenten om 80 op de server te plaatsen komen ook overeen met de eerste lijn van ACL voor Layer 3-informatie, maar omdat het sleutelwoord van fragmenten aanwezig is, wordt de volgende ACL-ingang (de tweede lijn) verwerkt. De tweede lijn van ACL maakt de eerste of niet-fragmenten mogelijk omdat deze overeenkomen met de ACL-lijn voor Layer 3 en Layer 4-informatie.

Niet-initiële fragmenten die bestemd zijn voor de TCP-poorten van andere hosts op het 171.16.23.0-netwerk worden geblokkeerd door deze ACL. Layer 3 informatie in deze pakketten komt niet overeen met Layer 3 informatie in de eerste ACL-lijn, zodat de volgende ACL-lijn wordt verwerkt. Layer 3 informatie in deze pakketten komt niet overeen met de informatie van Layer 3 in de tweede ACL-lijn, zodat de derde ACL-lijn wordt verwerkt. De derde regel is impliciet en ontkent al het verkeer.

De netwerkbeheerder in dit scenario beslist ACL 101 uit te voeren omdat het slechts niet-gefragmenteerde HTTP stromen naar de server toestaat.

## Scenario 2

Een klant heeft internetconnectiviteit op twee verschillende plaatsen, en er is ook een achterdeurverbinding tussen de twee plaatsen. Het beleid van de netwerkbeheerder is om Groep A in Site 1 toegang te geven tot de HTTP server op Site 2. De routers op beide sites gebruiken privé-adressen (RFC 1918 ) en Network Address Translation (NAT) om pakketten te vertalen die via internet worden Routed.

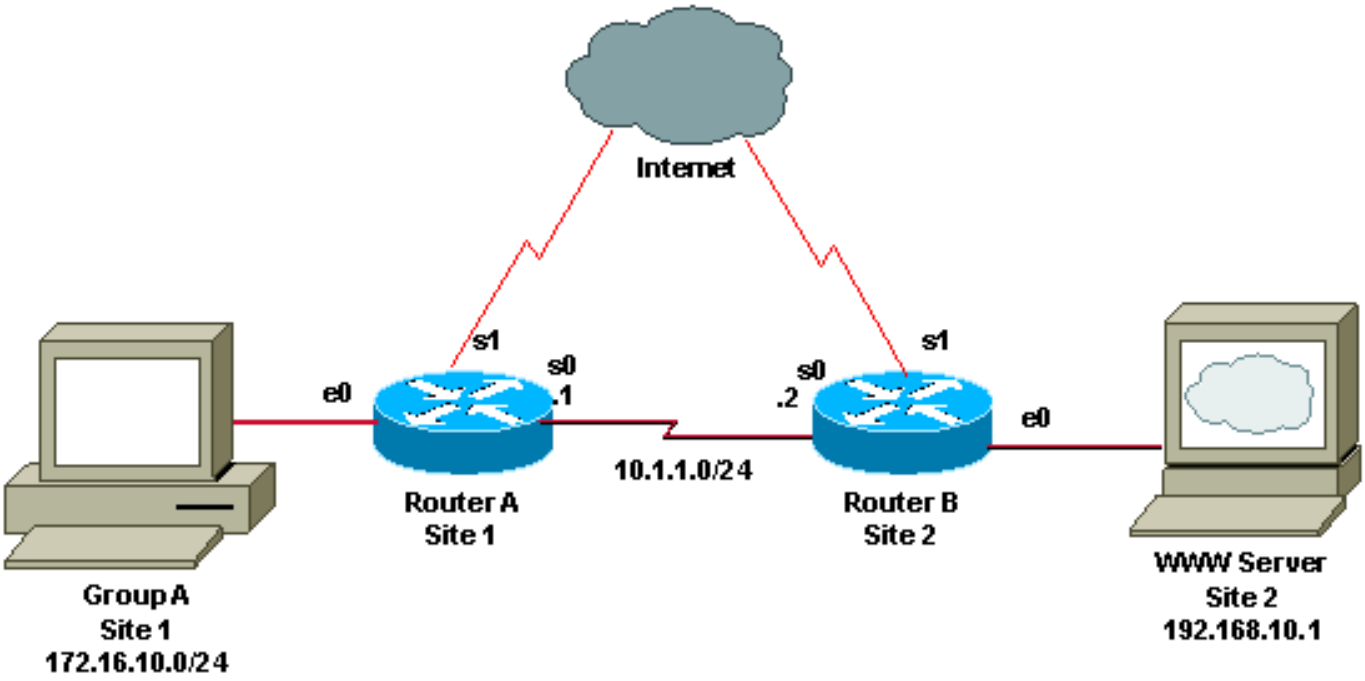
De netwerkbeheerder op Site 1 is beleid-routing de privé adressen toegewezen aan Groep A, zodat zij de achterdeur door de Seriële0 van de router A gebruiken bij toegang tot de HTTP server op Site 2. De router op Site 2 heeft een statische route naar 172.16.10.0, zodat het retourverkeer naar Groep A ook door de achterdeur wordt geleid. Al het andere verkeer wordt verwerkt door NAT en via het internet verstuurd. De netwerkbeheerder in dit scenario moet besluiten welke toepassing of stroom zal werken als de pakketten worden gefragmenteerd. Het is niet mogelijk om zowel de HTTP- als File Transfer Protocol (FTP)-stromen tegelijkertijd te laten werken, omdat een of de andere einden kapot zijn.

Zie het ACL-schema van regels en de Hoe pakketten bij een ACL-gedeelte kunnen worden afgestemd op het scenario.

### Uitleg van de opties van de netwerkbeheerder

In het volgende voorbeeld, de routekaart die FOO op router A wordt genoemd stuurt pakketten die ACL 100 over router B door s0 aanpassen. Alle pakketten die niet overeenkomen worden door NAT verwerkt en de standaardroute door het internet nemen.

**Opmerking:** Als een pakje van de onderkant van de ACL valt of door deze wordt ontkend, dan is het niet politiek verstuurd.




Het volgende is een gedeeltelijke configuratie van router A, die aantoont dat een beleidsroute-kaart die FOO wordt genoemd wordt toegepast op interface e0, waar het verkeer van Groep A de router ingaat:

```
hostname Router_A
int e0
ip policy route-map FOO
route-map FOO permit 10
match ip address 100
set ip next-hop 10.1.1.2

access-list 100 permit tcp 172.16.10.0 0.0.0.255 host 192.168.10.1 eq 80
access-list 100 deny ip any any
```

ACL 100 staat beleidsrouting toe op zowel initiële, niet-fragmenten en niet-initiële fragmenten van HTTP-stromen naar de server. Initiële en niet-fragmenten van HTTP-stromen naar de server zijn toegestaan door ACL's en routed beleid omdat ze overeenkomen met Layer 3 en Layer 4-informatie in de eerste ACL-lijn. Niet-initiële fragmenten zijn toegestaan door de ACL en het routed beleid, omdat Layer 3-informatie in het pakket ook overeenkomt met de eerste ACL-lijn; de ACL-logica veronderstelt dat de informatie op Layer 4 in het pakket ook overeenkomt als deze beschikbaar is.

**Opmerking:** ACL 100 breekt andere typen gefragmenteerde TCP-stromen tussen Groep A en de server omdat de initiële en niet-initiële fragmenten de server via verschillende paden bereiken; de oorspronkelijke fragmenten worden door NAT verwerkt en via het internet verstuurd, maar de niet-initiële fragmenten van dezelfde stroom zijn beleidsroutinematig.

Een gefragmenteerde FTP-stroming helpt het probleem in dit scenario te illustreren. De aanvankelijke fragmenten van een FTP-stroming komen overeen met Layer 3-informatie, maar niet met Layer 4-informatie van de eerste ACL-lijn, en worden vervolgens ontkend door de tweede lijn. Deze pakketten worden verwerkt door NAT en via het internet verzonden.

De niet-initiële fragmenten van een FTP-stroming passen de informatie van Layer 3 in de eerste

ACL-lijn aan, en de logica van ACL veronderstelt een positieve match op Layer 4-informatie. Deze pakketten zijn beleid routed, en het herassembleren van de gastheer deze pakketten herkent de aanvankelijke fragmenten niet als deel van de zelfde stroom zoals de beleid-routed niet aanvankelijke fragmenten omdat NAT het bronadres van de aanvankelijke fragmenten heeft veranderd.

ACL 100 in de onderstaande configuratie stelt het FTP-probleem vast. De eerste lijn van ACL 100 ontkent zowel aanvankelijke als niet-initiële FTP fragmenten van Groep A aan de server.

```
hostname Router_A

int e0
ip policy route-map FOO
route-map FOO permit 10
match ip address 100
set ip next-hop 10.1.1.2

access-list 100 deny tcp 172.16.10.0 0.0.0.255 host 192.168.10.1 fragments
access-list 100 permit tcp 172.16.10.0 0.0.0.255 host 192.168.10.1 eq 80
access-list 100 deny ip any any
```

Initiële fragmenten komen overeen op Layer 3 informatie in de eerste ACL-lijn, maar de aanwezigheid van het fragment veroorzaakt dat de volgende ACL-lijn wordt verwerkt. Het eerste fragment komt niet overeen met de tweede ACL-lijn voor Layer 4-informatie en dus wordt de volgende impliciete lijn van ACL verwerkt, die het pakket ontkent. Niet-initiële fragmenten komen overeen met Layer 3 informatie in de eerste lijn van ACL, zodat ze worden ontkend. Zowel eerste als niet-eerste fragmenten worden door NAT verwerkt en door het internet verzonden, zodat de server geen probleem heeft met reassembleren.

Het repareren van FTP-stromen breekt gefragmenteerde HTTP-stromen omdat de initiële HTTP-fragmenten nu worden routeerd, maar de niet-initiële fragmenten worden door NAT verwerkt en via het internet verzonden.

Wanneer een eerste fragment van een HTTP-stroom van groep A naar de server de eerste regel van ACL tegenkomt, komt deze overeen op Layer 3-informatie in de ACL, maar vanwege het fragmenten-trefwoord wordt de volgende regel van ACL verwerkt. De tweede lijn van de ACL vergunningen en beleid leidt het pakket naar de server.

Wanneer niet-initiële HTTP-fragmenten die van Groep A naar de server zijn bestemd, de eerste lijn van de ACL ontmoeten, komt de informatie op Layer 3 in het pakket overeen met de ACL-lijn en wordt het pakket ontkend. Deze pakketten worden verwerkt door NAT en dwars door Internet om naar de server te gaan.

De eerste ACL in dit scenario maakt gefragmenteerde HTTP-stromen mogelijk en breekt gefragmenteerde FTP-stromen. tweede ACL maakt gefragmenteerde FTP-stromen mogelijk en breekt gefragmenteerde HTTP-stromen. De TCP stromen breken in elk geval omdat de eerste en niet-initiële fragmenten verschillende paden naar de server brengen. Hermontage is niet mogelijk omdat NAT het bronadres van de niet-initiële fragmenten heeft gewijzigd.

Het is niet mogelijk om ACL te bouwen dat beide soorten gefragmenteerde stromen naar de server toelaat, zodat de netwerkbeheerder moet kiezen welke stroom hij wil werken.

## Gerelateerde informatie

- Ondersteuningspagina voor IP-routing
- Technische ondersteuning en documentatie – Cisco Systems