액세스 제어 목록 및 IP 프래그먼트

목차

소개

이 백서에서는 서로 다른 종류의 ACL(Access Control List) 항목 및 여러 종류의 패킷에서 이러한 다양한 항목이 발생할 때 발생하는 상황에 대해 설명합니다.ACL은 라우터에서 IP 패킷이 전달되지 않도록 차단하는 데 사용됩니다.

RFC 1858 은 IP 프래그먼트 필터링을 위한 보안 고려 사항을 다루고 TCP 패킷의 IP 프래그먼트, Tiny Fragment Attack 및 Overlapping Fragment Attack과 관련된 호스트에 대한 두 가지 공격을 강조합니다.이러한 공격을 차단하는 것은 호스트를 손상시키거나 내부 리소스를 모두 연결할 수 있기 때문에 바람직합니다.

RFC 1858 은 직접 및 간접이라는 두 가지 공격 방어 방법에 대해서도 설명합니다.직접 방법에서는 최소 길이보다 작은 초기 프래그먼트가 삭제됩니다.간접 메서드에서는 프래그먼트 세트의 두 번째 프래그먼트를 폐기합니다(원래 IP 데이터그램으로 8바이트를 시작하는 경우).자세한 내용은 RFC 1858 을 참조하십시오.

일반적으로 ACL과 같은 패킷 필터는 ACL이 허용 또는 거부 결정을 위해 매칭할 수 있는 레이어 3 및 4 정보를 모두 포함하므로 IP 패킷의 비프래그먼트 및 초기 프래그먼트에 적용됩니다.비초기 프래그먼트는 일반적으로 패킷의 레이어 3 정보를 기반으로 차단할 수 있으므로 ACL을 통해 허용됩니다.그러나 이러한 패킷은 레이어 4 정보를 포함하지 않으므로 ACL 항목의 레이어 4 정보(있는 경우)와 일치하지 않습니다.프래그먼트를 수신하는 호스트가 초기 프래그먼트 없이 원래 IP 데이터그램을 리어셈블할 수 없기 때문에 IP 데이터그램의 비초기 프래그먼트를 허용하는 것이 허용됩니다.

또한 방화벽은 소스 및 대상 IP 주소, 프로토콜, IP ID로 인덱싱된 패킷 프래그먼트 테이블을 유지하여 패킷을 차단하는 데 사용할 수 있습니다.Cisco PIX Firewall과 Cisco IOS® Firewall 모두 이 정보 테이블을 유지하여 특정 플로우의 모든 프래그먼트를 필터링할 수 있지만, 기본 ACL 기능을 위해 라우터에서 필터링하는 것은 너무 비용이 많이 듭니다.방화벽의 기본 작업은 패킷을 차단하는 것이며, 그 보조 역할은 패킷을 라우팅하는 것입니다.라우터의 기본 작업은 패킷을 라우팅하는 것이며, 그 보조 역할은 패킷을 차단하는 것입니다.

Cisco IOS Software 릴리스 12.1(2) 및 12.0(11)에서 TCP 프래그먼트와 관련된 일부 보안 문제를 해결하기 위해 두 가지 변경 사항이 적용되었습니다.RFC 1858 에 설명된 대로 간접 방법은 표준 TCP/IP 입력 패킷 무결성 검사의 일부로 구현되었습니다.또한 초기가 아닌 프래그먼트와 관련하여 ACL 기능을 변경했습니다.

ACL 항목 유형

ACL 라인에는 6가지 유형이 있으며, 패킷이 일치하지 않거나 일치하지 않으면 각각 결과가 발생합니다.다음 목록에서 FO = 0은 TCP 흐름의 비조각이나 초기 조각을 나타내며, FO > 0은 패킷이 비초기 프래그먼트임을, L3은 레이어 3을, L4는 레이어 4를 의미합니다.

참고: ACL 라인에 레이어 3 및 레이어 4 정보가 모두 있고 fragments 키워드가 있는 경우 ACL 작업은 허용 및 거부 작업 모두에 대해 보수적입니다.프래그먼트에는 모든 필터 특성과 일치시킬 수 있는 충분한 정보가 포함되어 있지 않기 때문에 작업의 경우 흐름의 프래그먼트된 부분을 실수로 거부하지 않으려는 것이 좋습니다.거부 사례에서는 초기가 아닌 조각을 거부하는 대신 다음 ACL 항목이 처리됩니다.허용 사례에서는 패킷의 레이어 4 정보(사용 가능한 경우)가 ACL 라인의 레이어 4 정보와 일치하는 것으로 가정합니다.

L3 정보만 포함하는 ACL 라인 허용

1. 패킷의 L3 정보가 ACL 라인의 L3 정보와 일치하면 허용됩니다.
2. 패킷의 L3 정보가 ACL 라인의 L3 정보와 일치하지 않으면 다음 ACL 항목이 처리됩니다.

L3 정보만 포함하는 ACL 라인 거부

1. 패킷의 L3 정보가 ACL 라인의 L3 정보와 일치하면 거부됩니다.
2. 패킷의 L3 정보가 ACL 라인의 L3 정보와 일치하지 않으면 다음 ACL 항목이 처리됩니다.

L3 정보만 포함된 ACL 행 허용, fragments 키워드가 있음

패킷의 L3 정보가 ACL 라인의 L3 정보와 일치하면 패킷의 프래그먼트 오프셋이 선택됩니다.

1. 패킷의 FO가 0보다 크면 패킷이 허용됩니다.
2. 패킷의 FO = 0인 경우 다음 ACL 항목이 처리됩니다.

L3 정보만 포함된 ACL 줄 거부 및 fragments 키워드가 있음

패킷의 L3 정보가 ACL 라인의 L3 정보와 일치하면 패킷의 프래그먼트 오프셋이 선택됩니다.

1. 패킷의 FO가 0보다 크면 패킷이 거부됩니다.
2. 패킷의 FO = 0이면 다음 ACL 행이 처리됩니다.

L3 및 L4 정보로 ACL 라인 허용

1. 패킷의 L3 및 L4 정보가 ACL 라인 및 FO = 0과 일치하면 패킷이 허용됩니다.
2. 패킷의 L3 정보가 ACL 라인 및 FO > 0과 일치하면 패킷이 허용됩니다.

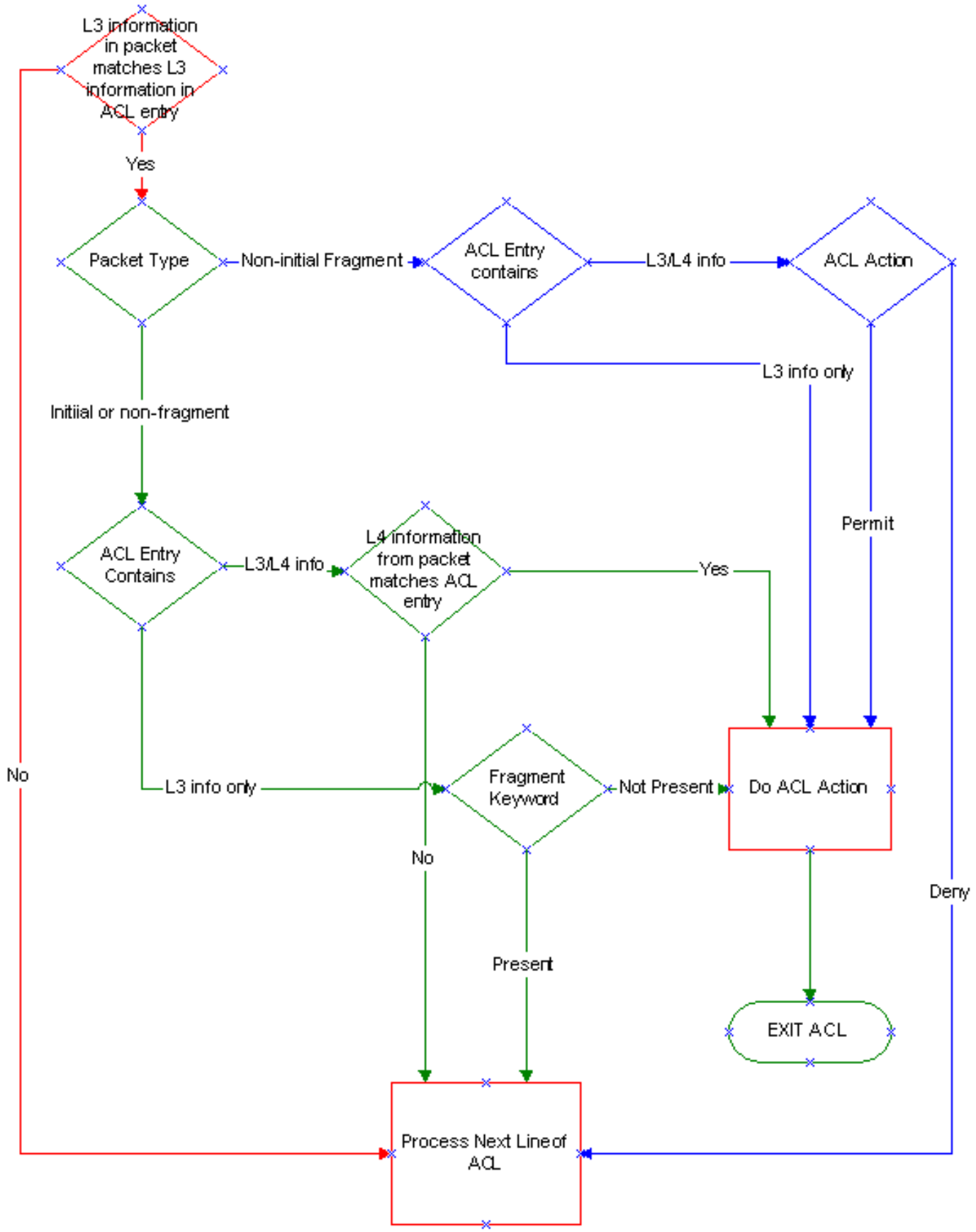
L3 및 L4 정보가 포함된 ACL 라인 거부

1. 패킷의 L3 및 L4 정보가 ACL 항목과 일치하고 FO = 0이면 패킷이 거부됩니다.
2. 패킷의 L3 정보가 ACL 라인 및 FO > 0과 일치하면 다음 ACL 항목이 처리됩니다.

ACL 규칙 순서도

다음 순서도는 ACL에 대해 비프래그먼트, 초기 프래그먼트 및 비초기 프래그먼트가 확인되는 경우 ACL 규칙을 보여줍니다.

참고: 초기가 아닌 프래그먼트는 레이어 3만 포함하지만 레이어 4 정보는 포함하지 않습니다. 단, ACL에는 레이어 3 및 레이어 4 정보가 모두 포함될 수 있습니다.



패킷이 ACL과 일치할 수 있는 방법

예 1

다음 5가지 시나리오는 ACL 100을 접하는 여러 유형의 패킷과 관련이 있습니다. 각 상황에서 발생

하는 사항을 따라 테이블과 순서도를 참조하십시오.웹 서버의 IP 주소는 171.16.23.1입니다.

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

access-list 100 deny ip any any
```

패킷은 포트 80에서 서버로 향하는 초기 프래그먼트 또는 비프래그먼트입니다.

ACL의 첫 번째 라인에는 패킷의 레이어 3 및 레이어 4 정보와 일치하는 레이어 3 및 레이어 4 정보가 모두 포함되므로 패킷이 허용됩니다.

패킷은 포트 21에서 서버로 향하는 초기 프래그먼트 또는 비프래그먼트입니다.

1. ACL의 첫 번째 줄에는 레이어 3 및 레이어 4 정보가 모두 포함되지만 ACL의 레이어 4 정보는 패킷과 일치하지 않으므로 다음 ACL 행이 처리됩니다.
2. ACL의 두 번째 행은 모든 패킷을 거부하므로 패킷이 거부됩니다.

패킷은 포트 80 흐름에서 서버에 대한 비초기 프래그먼트입니다.

ACL의 첫 번째 줄에는 레이어 3 및 레이어 4 정보가 포함되며, ACL의 레이어 3 정보는 패킷과 일치하며, ACL 작업은 허용되므로 패킷이 허용됩니다.

패킷은 포트 21 플로우의 서버에 대한 비초기 프래그먼트입니다.

ACL의 첫 번째 줄에는 레이어 3 및 레이어 4 정보가 모두 포함됩니다.ACL의 레이어 3 정보는 패킷과 일치하고, 패킷에는 레이어 4 정보가 없으며, ACL 작업은 허용되므로 패킷이 허용됩니다.

패킷은 서버 서브넷의 다른 호스트에 대한 초기 프래그먼트, 비프래그먼트 또는 비초기 프래그먼트입니다.

1. ACL의 첫 번째 줄에는 패킷의 레이어 3 정보(대상 주소)와 일치하지 않는 레이어 3 정보가 포함되므로 다음 ACL 행이 처리됩니다.
2. ACL의 두 번째 행은 모든 패킷을 거부하므로 패킷이 거부됩니다.

예 2

다음 다섯 가지 가능한 시나리오는 ACL 101을 접하는 여러 유형의 패킷과 관련이 있습니다. 각 상황에서 발생하는 작업을 수행할 때 테이블 및 순서도를 참조하십시오.웹 서버의 IP 주소는 171.16.23.1입니다.

```
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
```

패킷은 포트 80에서 서버로 향하는 초기 프래그먼트 또는 비프래그먼트입니다.

1. ACL의 첫 번째 줄에는 패킷의 레이어 3 정보와 일치하는 레이어 3 정보가 포함됩니다.ACL 작업은 거부하지만 fragments 키워드가 **있으므로** 다음 ACL 항목이 처리됩니다.
2. ACL의 두 번째 줄에는 패킷과 일치하는 레이어 3 및 레이어 4 정보가 포함되므로 패킷이 허용됩니다.

패킷은 포트 21에서 서버로 향하는 초기 프래그먼트 또는 비프래그먼트입니다.

1. ACL의 첫 번째 줄에는 패킷과 일치하는 레이어 3 정보가 포함되지만, ACL 항목에는 **fragments** 키워드도 포함되는데, 이는 FO = 0 때문에 패킷과 일치하지 않으므로 다음 ACL 항목이 처리됩니다.
2. ACL의 두 번째 줄에는 레이어 3 및 레이어 4 정보가 포함됩니다.이 경우 레이어 4 정보가 일치하지 않으므로 다음 ACL 항목이 처리됩니다.
3. ACL의 세 번째 행은 모든 패킷을 거부하므로 패킷이 거부됩니다

패킷은 포트 80 흐름에서 서버에 대한 비초기 프래그먼트입니다.

ACL의 첫 번째 줄에는 패킷의 레이어 3 정보와 일치하는 레이어 3 정보가 포함됩니다.포트 80 흐름의 일부이지만, 초기 이외 프래그먼트에는 레이어 4 정보가 없습니다.레이어 3 정보가 일치하므로 패킷이 거부됩니다.

패킷은 포트 21 플로우의 서버에 대한 비초기 프래그먼트입니다.

ACL의 첫 번째 행은 레이어 3 정보만 포함하며 패킷과 일치하므로 패킷이 거부됩니다.

패킷은 서버 서브넷의 다른 호스트에 대한 초기 프래그먼트, 비프래그먼트 또는 비초기 프래그먼트입니다.

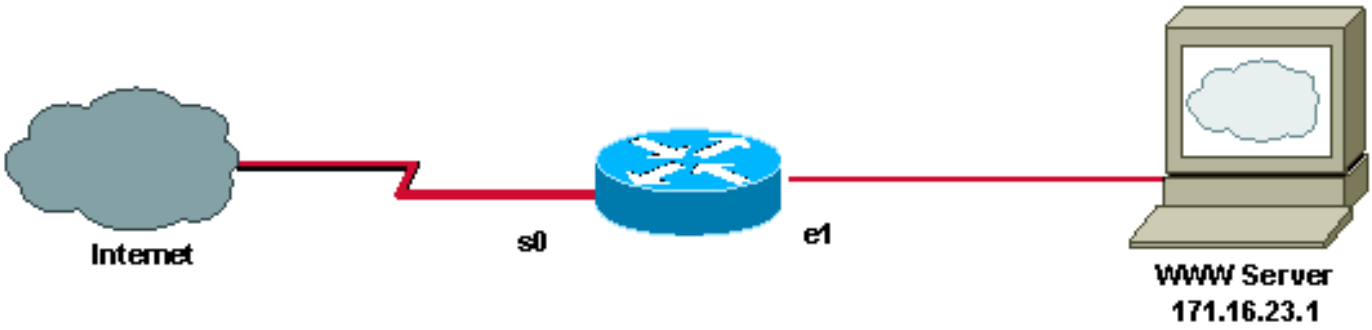
1. ACL의 첫 번째 행은 레이어 3 정보만 포함하며 패킷과 일치하지 않으므로 다음 ACL 행이 처리됩니다.
2. ACL의 두 번째 줄에는 레이어 3 및 레이어 4 정보가 포함됩니다.패킷의 레이어 4 및 레이어 3 정보가 ACL의 정보와 일치하지 않으므로 다음 ACL 행이 처리됩니다.
3. ACL의 세 번째 행은 이 패킷을 거부합니다.

fragments 키워드 시나리오

시나리오 1

라우터 B는 웹 서버에 연결되며 네트워크 관리자는 프래그먼트가 서버에 도달하는 것을 허용하지 않습니다.이 시나리오에서는 네트워크 관리자가 ACL 100과 ACL 101을 함께 구현하는 경우 어떤 일이 발생하는지 보여줍니다. ACL은 라우터 Serial0(s0) 인터페이스에 인바운드에 적용되며 조각화되지 않은 패킷만 웹 서버에 연결하도록 허용해야 합니다.시나리오를 따라 ACL 규칙 순서도 및 패킷이 ACL과 매칭하는 방법 섹션을 참조하십시오.

fragments 키워드 사용의 결과



다음은 ACL 100입니다.

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

access-list 100 deny ip any any
```

ACL 100의 첫 번째 행은 서버에 대한 HTTP만 허용하지만 서버의 모든 TCP 포트에 대한 초기가 아닌 프래그먼트도 허용합니다.초기가 아닌 프래그먼트에는 레이어 4 정보가 포함되지 않으며 ACL 로직에서는 레이어 3 정보가 일치하는 경우 레이어 4 정보가 사용 가능한 경우 일치하는 것으로 간주하므로 이러한 패킷을 허용합니다.두 번째 줄은 암시적이며 다른 모든 트래픽을 거부합니다.

Cisco IOS Software Release 12.1(2) 및 12.0(11)부터 새로운 ACL 코드는 ACL의 다른 줄과 일치하지 않는 프래그먼트를 삭제합니다.이전 릴리스에서는 ACL의 다른 줄과 일치하지 않는 경우 초기가 아닌 프래그먼트를 통과하도록 허용합니다.

다음은 ACL 101입니다.

```
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 101은 첫 번째 줄 때문에 서버에 대한 비초기 프래그먼트를 허용하지 않습니다.패킷의 Layer 3 정보가 ACL 라인의 Layer 3 정보와 일치하기 때문에 첫 번째 ACL 선이 발견되면 서버에 대한 비초기 프래그먼트가 거부됩니다.

서버의 포트 80에 대한 초기 또는 비프래그먼트는 레이어 3 정보에 대한 ACL의 첫 번째 줄과도 일치하지만 fragments 키워드가 있기 때문에 다음 ACL 항목(두 번째 줄)이 처리됩니다.ACL의 두 번째 줄은 레이어 3 및 레이어 4 정보에 대한 ACL 라인과 일치하므로 초기 또는 비프래그먼트를 허용합니다.

171.16.23.0 네트워크에 있는 다른 호스트의 TCP 포트로 향하는 비초기 프래그먼트는 이 ACL에 의해 차단됩니다.이러한 패킷의 레이어 3 정보는 첫 번째 ACL 라인의 레이어 3 정보와 일치하지 않으므로 다음 ACL 행이 처리됩니다.이러한 패킷의 레이어 3 정보는 두 번째 ACL 라인의 레이어 3 정보와 일치하지 않으므로 세 번째 ACL 라인이 처리됩니다.세 번째 줄은 암시적이며 모든 트래픽을 거부합니다.

이 시나리오의 네트워크 관리자는 서버에 단편화되지 않은 HTTP 플로우만 허용하기 때문에 ACL 101을 구현하기로 합니다.

시나리오 2

고객은 서로 다른 두 사이트에서 인터넷에 연결되어 있으며, 두 사이트 간에는 백도어 연결이 있습니다.네트워크 관리자의 정책은 사이트 1의 그룹 A가 사이트 2의 HTTP 서버에 액세스할 수 있도록 하는 것입니다. 두 사이트의 라우터는 사설 주소(RFC 1918) 및 NAT(Network Address Translation)를 사용하여 인터넷을 통해 라우팅된 패킷을 변환합니다.

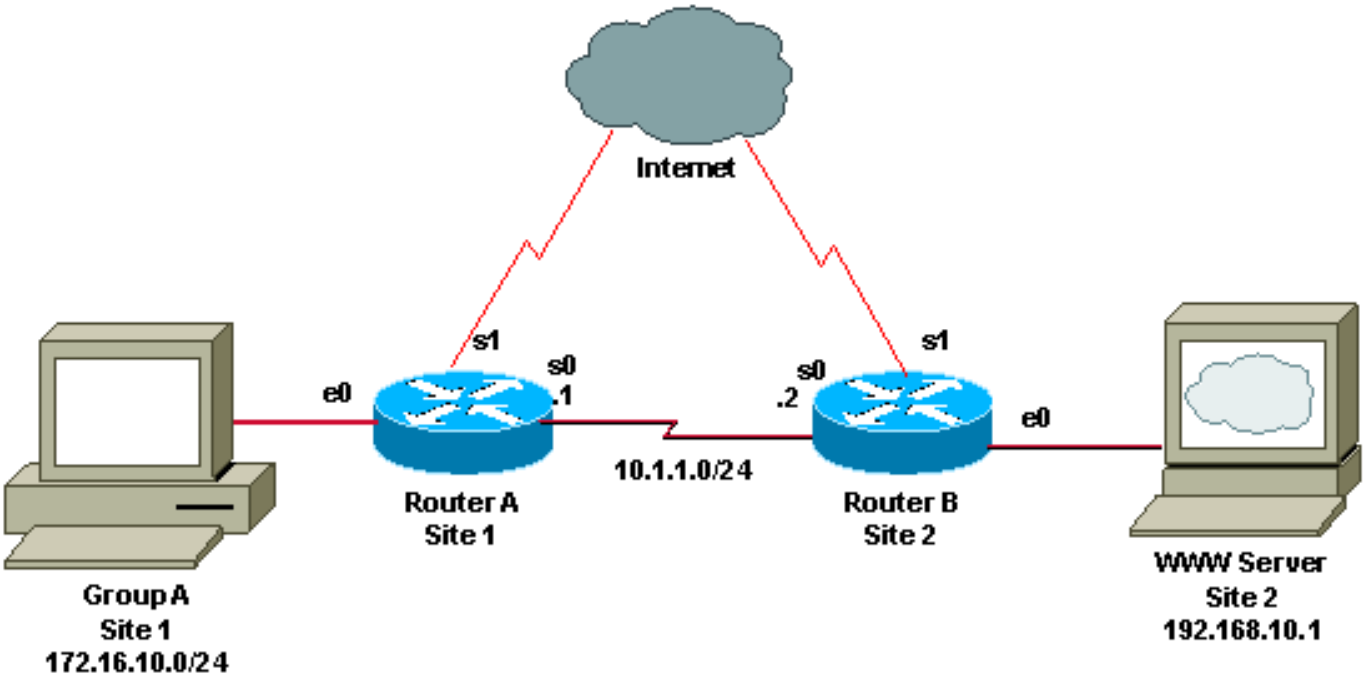
사이트 1의 네트워크 관리자는 그룹 A에 할당된 개인 주소를 정책 라우팅하므로 사이트 2의 HTTP 서버에 액세스할 때 라우터 A의 일련 번호0(s0)을 통해 백도어를 사용합니다. 사이트 2의 라우터에는 172.16.10.0에 대한 고정 경로가 있으므로 그룹 A에 대한 반환 트래픽도 백도어를 통해 라우팅됩니다.다른 모든 트래픽은 NAT에서 처리되고 인터넷을 통해 라우팅됩니다.이 시나리오의 네트워크 관리자는 패킷이 프래그먼트화될 경우 어떤 애플리케이션 또는 플로우가 작동하는지 결정해야 합니다.HTTP 및 FTP(File Transfer Protocol) 플로우를 둘 다 동시에 작동시킬 수는 없습니다. 둘 중 하나가 중단되기 때문입니다.

시나리오를 따라 ACL 규칙 순서도 및 패킷이 ACL과 매칭하는 방법 섹션을 참조하십시오.

네트워크 관리자 옵션 설명

다음 예에서 라우터 A의 FOO라는 경로 맵은 라우터 B에서 s0까지 ACL 100과 일치하는 패킷을 전송합니다. 일치하지 않는 모든 패킷은 NAT에서 처리되며 인터넷을 통해 기본 경로를 사용합니다.

참고: 패킷이 ACL의 하단에서 떨어지거나, 패킷에 의해 거부된 경우 정책 라우팅이 되지 않습니다.



다음은 라우터 A의 부분 컨피그레이션으로, 그룹 A의 트래픽이 라우터로 들어가는 인터페이스 e0에 FOO라는 정책 경로 맵이 적용되었음을 보여줍니다.

```
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 100은 서버에 대한 HTTP 흐름의 초기, 비프래그먼트 및 비초기 프래그먼트에서 정책 라우팅을 허용합니다.서버에 대한 HTTP 흐름의 초기 및 비프래그먼트는 첫 번째 ACL 라인의 레이어 3 및 레이어 4 정보와 일치하기 때문에 라우팅된 ACL 및 정책에 의해 허용됩니다.패킷의 레이어 3 정보도 첫 번째 ACL 라인과 일치하므로 ACL 및 라우팅된 정책에 의해 초기가 아닌 프래그먼트가 허용됩니다.ACL 로직에서는 패킷의 레이어 4 정보가 사용 가능한 경우에도 일치한다고 가정합니다.

참고: 초기 프래그먼트와 비초기 프래그먼트가 서로 다른 경로를 통해 서버에 도달하기 때문에 ACL 100은 그룹 A와 서버 간에 프래그먼트된 다른 유형의 TCP 흐름을 중단합니다.초기 프래그먼트는 NAT에 의해 처리되고 인터넷을 통해 라우팅되지만, 동일한 플로우의 초기 프래그먼트가 아닌 프래그먼트는 정책 라우팅입니다.

단편화된 FTP 흐름은 이 시나리오의 문제를 설명하는 데 도움이 됩니다.FTP 흐름의 초기 프래그먼트는 첫 번째 ACL 라인의 레이어 4 정보가 아니라 레이어 3 정보와 일치하며, 그 다음에는 두 번째 줄에 의해 거부됩니다.이러한 패킷은 NAT에서 처리되고 인터넷을 통해 라우팅됩니다.

FTP 흐름의 비초기 프래그먼트는 첫 번째 ACL 라인의 레이어 3 정보와 일치하며, ACL 로직에서는 레이어 4 정보에 대해 긍정적인 매칭을 가정합니다.이러한 패킷은 정책이 라우팅되며, 호스트에서 이러한 패킷을 리어셈블하는 경우 초기 프래그먼트의 소스 주소를 변경했기 때문에 NAT가 정책 라우팅이 아닌 초기 프래그먼트와 동일한 플로우의 일부로 초기 프래그먼트를 인식하지 못합니다.

아래 컨피그레이션의 ACL 100은 FTP 문제를 해결합니다.ACL 100의 첫 번째 행은 그룹 A에서 서버로의 초기 및 비초기 FTP 프래그먼트를 모두 거부합니다.

```
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
```

초기 프래그먼트는 첫 번째 ACL 라인의 레이어 3 정보에 일치하지만, fragments 키워드가 있으면 다음 ACL 라인이 처리됩니다.초기 프래그먼트는 레이어 4 정보에 대한 두 번째 ACL 라인과 일치하지 않으므로 ACL의 다음 암시적 선이 처리되며, 이는 패킷을 거부합니다.초기가 아닌 프래그먼트는 ACL의 첫 번째 행에 있는 레이어 3 정보와 일치하므로 거부됩니다.초기 프래그먼트와 비초기 프래그먼트는 모두 NAT에 의해 처리되고 인터넷을 통해 라우팅되므로 서버는 리어셈블에 문제가 없습니다.

초기 HTTP 프래그먼트가 이제 정책으로 라우팅되었지만, 초기가 아닌 프래그먼트는 NAT에 의해 처리되고 인터넷을 통해 라우팅되기 때문에 FTP 플로우를 수정하면 프래그먼트된 HTTP 플로우가 중단됩니다.

그룹 A에서 서버로 향하는 HTTP 흐름의 초기 프래그먼트가 ACL의 첫 번째 줄을 발견하면 ACL의 레이어 3 정보와 일치하지만 fragments 키워드 때문에 ACL의 다음 행이 처리됩니다.ACL의 두 번째

줄은 패킷을 서버에 라우팅합니다.

Group A에서 서버로 향하는 초기가 아닌 HTTP 프래그먼트가 ACL의 첫 번째 행을 발견하면 패킷의 레이어 3 정보가 ACL 라인과 일치하고 패킷이 거부됩니다.이러한 패킷은 NAT를 통해 처리되며 서버에 연결하기 위해 인터넷을 통과합니다.

이 시나리오의 첫 번째 ACL은 프래그먼트된 HTTP 플로우를 허용하고 프래그먼트된 FTP 플로우를 중단시킵니다.두 번째 ACL은 프래그먼트된 FTP 흐름을 허용하고 조각화된 HTTP 흐름을 중단시킵니다.초기 프래그먼트와 비초기 프래그먼트는 서버에 대해 서로 다른 경로를 사용하기 때문에 TCP 플로우는 각 경우에 중단됩니다.NAT가 비초기 프래그먼트의 소스 주소를 변경했기 때문에 리어셈블할 수 없습니다.

서로 다른 종류의 서버 흐름을 모두 허용하는 ACL을 구성할 수는 없으므로 네트워크 관리자가 원하는 흐름을 선택해야 합니다.

관련 정보

- IP 라우팅 지원 페이지
- 기술 지원 및 문서 – Cisco Systems