정책 라우팅 이해

목차

소개

정책 기반 라우팅은 네트워크 관리자가 정의한 정책을 기반으로 데이터 패킷을 전달 및 라우팅하는 도구를 제공합니다.사실상, 라우팅 프로토콜 결정을 정책 재정의하는 방법입니다.정책 기반 라우팅에는 액세스 목록, 패킷 크기 또는 기타 기준에 따라 정책을 선택적으로 적용할 수 있는 메커니즘이 포함되어 있습니다.수행되는 작업에는 사용자 정의 경로의 라우팅 패킷, 우선 순위 설정, 서비스 비트 유형 등이 포함될 수 있습니다.

이 문서에서는 10.0.0.0/8 개인 주소를 서브넷 172.16.255.0/24에 속하는 인터넷 라우팅 가능 주소로 변환하는 데 방화벽을 사용합니다. 자세한 내용은 아래 다이어그램을 참조하십시오.

자세한 내용은 정책 기반 라우팅을 참조하십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 하드웨어 또는 소프트웨어 버전으로 제한되지 않습니다.

이 문서에 표시된 정보는 아래 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® Software 릴리스 12.3(3)
- Cisco 2500 Series 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.라이브 네트워크에서 작업하는 경우, 사

용하기 전에 모든 명령의 잠재적인 영향을 이해해야 합니다.

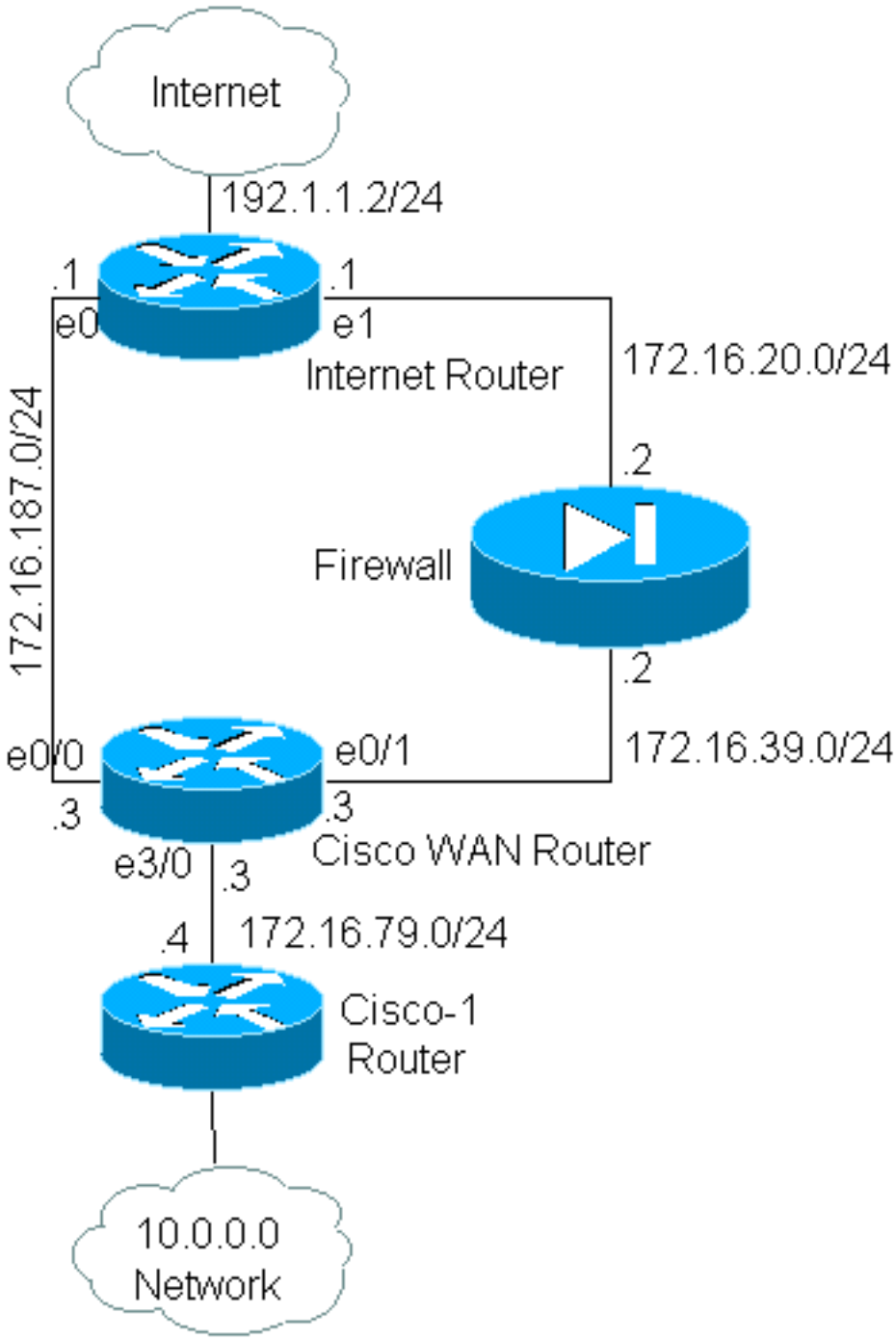
표기 규칙

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

구성

이 예에서는 정상적인 라우팅을 통해 10.0.0.0/8 네트워크에서 인터넷으로 연결되는 모든 패킷이 Cisco WAN 라우터의 인터페이스 이더넷 0/0(172.16.187.0/24 서브넷 사용)을 통해 경로를 취합니다. 이는 메트릭이 가장 적은 최적의 경로입니다.정책 기반 라우팅에서는 이러한 패킷이 방화벽을 통해 인터넷으로 향하는 경로를 따르도록 하려면 정책 라우팅을 구성하여 정상적인 라우팅 동작을 재정의해야 합니다.방화벽은 10.0.0.0/8 네트워크의 모든 패킷을 인터넷으로 변환하지만, 정책 라우팅이 작동하기 위해서는 이러한 패킷이 필요하지 않습니다.

네트워크 다이어그램



방화벽 구성

아래 방화벽 컨피그레이션이 포함되어 완전한 그림을 제공합니다.그러나 이 문서에서 설명한 정책 라우팅 문제의 일부는 아닙니다.이 예에서 방화벽은 PIX 또는 다른 방화벽 디바이스로 쉽게 교체할 수 있습니다.

```
!
ip nat pool net-10 172.16.255.1 172.16.255.254 prefix-length 24
ip nat inside source list 1 pool net-10
!
interface Ethernet0
 ip address 172.16.20.2 255.255.255.0
 ip nat outside
!
interface Ethernet1
```

```
 ip address 172.16.39.2 255.255.255.0
 ip nat inside
!
router eigrp 1
 redistribute static
 network 172.16.0.0
 default-metric 10000 100 255 1 1500
!
ip route 172.16.255.0 255.255.255.0 Null0
access-list 1 permit 10.0.0.0 0.255.255.255
!
end
```

ip nat 관련 명령에 대한 자세한 내용은 IP 주소 지정 및 서비스 명령을 참조하십시오.

이 예에서는 Cisco WAN 라우터가 10.0.0.0/8 네트워크에서 시작된 IP 패킷이 방화벽을 통해 전송되도록 정책 라우팅을 실행하고 있습니다.아래 컨피그레이션에는 10.0.0.0/8 네트워크에서 방화벽으로 보내는 패킷을 전송하는 액세스 목록 문이 포함되어 있습니다.

Cisco_WAN_Router 구성

```
!
interface Ethernet0/0
 ip address 172.16.187.3 255.255.255.0
 no ip directed-broadcast
!
interface Ethernet0/1
 ip address 172.16.39.3 255.255.255.0
 no ip directed-broadcast
!
interface Ethernet3/0
 ip address 172.16.79.3 255.255.255.0
 no ip directed-broadcast
 ip policy route-map net-10
!
router eigrp 1
 network 172.16.0.0
!

access-list 111 permit ip 10.0.0.0 0.255.255.255 any
!
route-map net-10 permit 10
 match ip address 111
 set interface Ethernet0/1
!
route-map net-10 permit 20
!
end
```

route-map 관련 명령에 대한 자세한 내용은 route-map 명령 설명서를 참조하십시오.

참고: access-list 명령의 **log** 키워드는 PBR에서 지원되지 않습니다.**log** 키워드가 구성된 경우 적중 횟수가 표시되지 않습니다.

Cisco-1 라우터에 대한 구성

```
!
version 12.3
```

```
!

interface Ethernet0

!-- Interface connecting to 10.0.0.0 network ip address 10.1.1.1 255.0.0.0 ! interface Ethernet1
!-- Interface connecting to Cisco_Wan_Router ip address 172.16.79.4 255.255.255.0 ! router eigrp
1 network 10.0.0.0 network 172.16.0.0 no auto-summary ! !---Output Suppressed
```

Internet_Router 구성

```
!
version 12.3

!
interface Ethernet1

!-- Interface connecting to Firewall ip address 172.16.20.1 255.255.255.0 interface Serial0 !---
Interface connecting to Internet ip address 192.1.1.2 255.255.255.0 clockrate 64000 no fair-
queue ! interface Ethernet0 !--- Interface connecting to Cisco_Wan_Router ip address
172.16.187.1 255.255.255.0 ! ! router eigrp 1 redistribute static !--- Redistributing the static
default route for other routers to reach Internet network 172.16.0.0 no auto-summary ! ip
classless ip route 0.0.0.0 0.0.0.0 192.1.1.1 !-- Static default route pointing to the router
connected to Internet !---Output Suppressed
```

이 예제를 테스트하면서 Cisco-1 라우터의 10.1.1.1에서 **extended ping** 명령을 사용하여 인터넷의 호스트로 전송된 ping이 있습니다.이 예에서는 192.1.1.1이 대상 주소로 사용되었습니다.인터넷 라우터에서 무슨 일이 일어나고 있는지 확인하기 위해 debug **ip packet 101 detail** 명령을 사용하는 동안 고속 스위칭이 해제되었습니다.

경고: 프로덕션 라우터에서 **debug ip packet detail** 명령을 사용하면 CPU 사용률이 높으므로 성능이 심각하게 저하되거나 네트워크 중단이 발생할 수 있습니다.debug 명령을 사용하기 전에 Ping 및 Traceroute 명령 이해의 Using the Debug Command 섹션을 주의로 읽는 것이 좋습니다.

참고: access-list 101 permit icmp any 문은 **debug ip 패킷** 출력을 필터링하는 데 사용됩니다.이 액세스 목록이 없으면 debug **ip packet** 명령은 콘솔에 너무 많은 출력을 생성하여 라우터가 잠깁니다.PBR을 구성할 때 확장 ACL을 사용합니다.일치 기준을 설정하기 위해 구성된 ACL이 없는 경우 모든 트래픽이 정책 라우팅됩니다.

```
Results of ping from Cisco_1 to 192.1.1.1/internet taken from Internet_Router:
Packet never makes it to Internet_Router

Cisco_1# ping
Protocol [ip]:
Target IP address: 192.1.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
.....
```

```
Success rate is 0 percent (0/5)
```

보시다시피 패킷이 인터넷 라우터에 도달하지 않았습니다.Cisco WAN 라우터에서 가져온 아래의 debug 명령은 이러한 문제가 발생한 이유를 보여줍니다.

```
Debug commands run from Cisco_WAN_Router:
"debug ip policy"
*Mar  1 00:43:08.367: IP: s=10.1.1.1 (Ethernet3/0), d=192.1.1.1, len 100, policy match
*Mar  1 00:43:08.367: IP: route map net-10, item 10, permit
 !--- Packet with source address belonging to 10.0.0.0/8 network !--- is matched by route-map
"net-10" statement 10. *Mar 1 00:43:08.367: IP: s=10.1.1.1 (Ethernet3/0), d=192.1.1.1
(Ethernet0/1), len 100, policy routed *Mar 1 00:43:08.367: Ethernet3/0 to Ethernet0/1 192.1.1.1
!--- matched packets previously are forwarded out of interface !--- ethernet 0/1 by the set
command.
```

패킷이 net-10 정책 맵에서 정책 항목 10과 일치했습니다(예상대로).그러면 왜 패킷이 인터넷 라우터에 도착하지 않았을까요?

```
"debug arp"
*Mar  1 00:06:09.619: IP ARP: creating incomplete entry for IP address: 192.1.1.1 interface
Ethernet0/1
*Mar  1 00:06:09.619: IP ARP: sent req src 172.16.39.3 00b0.64cb.eab1,
                 dst 192.1.1.1 0000.0000.0000 Ethernet0/1
*Mar  1 00:06:09.635: IP ARP rep filtered src 192.1.1.1 0010.7b81.0b19, dst 172.16.39.3
                 00b0.64cb.eab1 wrong cable, interface Ethernet0/1

Cisco_Wan_Router# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.39.3             -   00b0.64cb.eab1  ARPA   Ethernet0/1
Internet  172.16.39.2             3   0010.7b81.0b19  ARPA   Ethernet0/1
Internet  192.1.1.1               0   Incomplete      ARPA
```

디버그 arp 출력에 이 정보가 표시됩니다.Cisco WAN 라우터는 지시된 작업을 시도하고 패킷을 이더넷 0/1 인터페이스에 직접 넣으려고 시도합니다.이렇게 하려면 라우터가 인식하는 192.1.1.1의 대상 주소에 대한 ARP(Address Resolution Protocol) 요청을 전송해야 합니다. 따라서 이 주소에 대한 ARP 항목은 show arp 명령에서 볼 수 있듯이 "Incomplete"입니다.그러면 라우터가 ARP 항목이 없는 와이어에 패킷을 넣을 수 없어 캡슐화 오류가 발생합니다.

방화벽을 next-hop으로 지정하면 이 문제를 방지하고 경로 맵이 예상대로 작동하도록 할 수 있습니다.

```
Config changed on Cisco_WAN_Router:
!
route-map net-10 permit 10
 match ip address 111
 set ip next-hop 172.16.39.2
!
```

이제 인터넷 라우터에서 동일한 debug ip packet 101 detail 명령을 사용하여 패킷이 올바른 경로를 사용하고 있음을 확인할 수 있습니다.또한 패킷이 방화벽에 의해 172.16.255.1으로 변환되었으며 ping되고 있는 시스템 192.1.1.1이 응답했음을 확인할 수 있습니다.

```
Cisco_1# ping
Protocol [ip]:
Target IP address: 192.1.1.1
Repeat count [5]:
```

```
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/70/76 ms

Results of ping from Cisco_1 to 192.1.1.1/internet taken from Internet_Router:
Internet_Router#
*Mar  1 00:06:11.619: IP: s=172.16.255.1 (Ethernet1), d=192.1.1.1 (Serial0), g=192.1.1.1, len
100, forward
*Mar  1 00:06:11.619:     ICMP type=8, code=0
!--- Packets sourced from 10.1.1.1 are getting translated to 172.16.255.1 by !--- the Firewall
before it reaches the Internet_Router. *Mar 1 00:06:11.619: *Mar 1 00:06:11.619: IP: s=192.1.1.1
(Serial0), d=172.16.255.1 (Ethernet1), g=172.16.20.2, len 100, forward *Mar 1 00:06:11.619: ICMP
type=0, code=0 !--- Packets returning from Internet arrive with the destination !--- address
172.16.255.1 before it reaches the Firewall. *Mar 1 00:06:11.619:
```

Cisco WAN 라우터의 **debug ip policy** 명령은 패킷이 방화벽으로 전달되었음을 172.16.39.2:

Cisco_WAN_Router에서 실행되는 디버그 명령

```
"debug ip policy"
*Mar  1 00:06:11.619: s=10.1.1.1 (Ethernet3/0), d=192.1.1.1, len 100, policy match
*Mar  1 00:06:11.619: IP: route map net-10, item 20, permit
*Mar  1 00:06:11.619: s=10.1.1.1 (Ethernet3/0), d=192.1.1.1 (Ethernet0/1), len 100, policy
routed
*Mar  1 00:06:11.619: Ethernet3/0 to Ethernet0/1 172.16.39.2
```

암호화된 트래픽에 대한 정책 기반 라우팅

정책 라우팅을 기반으로 암호화된 트래픽을 라우팅하기 위해 해독된 트래픽을 루프백 인터페이스로 전달한 다음 해당 인터페이스에서 PBR을 수행합니다.암호화된 트래픽이 VPN 터널을 통해 전달되는 경우 인터페이스 `ip cef` vpn 터널을 종료합니다.

관련 정보

- IP 라우팅 지원 페이지
- NAT 지원 페이지
- 기술 지원 툴 및 리소스
- 정책 기반 라우팅
- Cisco IOS 기술
- 기술 지원 및 문서 – Cisco Systems