성능 모니터를 통한 유연한 NetFlow 필터링

목차

소개

이 문서에서는 NetFlow에 기록되지 않도록 특정 IP를 필터링하는 방법에 대해 설명합니다.

기고자: Vishal Kothari, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

Flexible NetFlow에 대한 지식이 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 3650 스위치
- ISR(Integrated Service Router) 4351 라우터

> **참고:** NetFlow에서 이 필수 필터링을 수행하려면 AppxK9 라이센스를 설치해야 합니다. 테스트를 위해 RTU(Right-To-Use) AppxK9 라이센스를 사용할 수 있습니다.

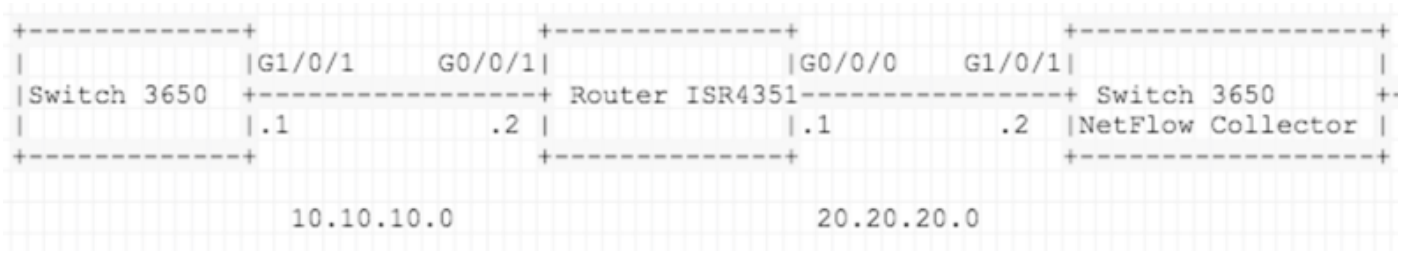
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

이 섹션에서는 NetFlow에서 기록할 필요가 없는 IP 목록을 필터링해야 합니다. 즉, 라우터가 ACL에서 정의된 IP의 소스 및 대상에 대한 세부 정보를 전송하지 않아야 합니다. 유연한 NetFlow를 통해

이를 실현하는 방법은 다음과 같습니다.

네트워크 다이어그램



설정

NetFlow 컬렉터로 전송하는 동안 필터링할 모든 네트워크의 목록을 준비합니다. 이 예에서는 텔넷 트래픽을 컬렉터로 전송하고 다른 모든 트래픽을 허용합니다.

ISR4351 구성:

```
IP access-list extended acl-filter

deny   tcp host 10.10.10.1 host 10.10.10.2 eq telnet

deny   tcp host 10.10.10.2 eq telnet host 10.10.10.1

permit ip any any



flow record type performance-monitor NET-FLOW

match ipv4 tos

match ipv4 protocol

match ipv4 source address

match ipv4 destination address

match transport source-port

match transport destination-port

match interface output

match flow direction

match flow sampler

match application name

collect routing source as

collect routing destination as

collect routing next-hop address ipv4
```

```
collect ipv4 source mask
collect ipv4 destination mask
collect transport tcp flags
collect interface input
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
!
!
flow exporter NET-FLOW
description NET-FLOW
destination 20.20.20.2
source Loopback28
transport udp 2055
!
!
flow monitor type performance-monitor NET-FLOW
record NET-FLOW
exporter NET-FLOW

class-map match-any class-filter
match access-group name acl-filter
!
policy-map type performance-monitor policy-filter
class class-filter
  flow monitor NET-FLOW



interface Loopback28
ip address 10.11.11.28 255.255.255.255
```

```
interface GigabitEthernet0/0/1

 ip address 10.10.10.2 255.255.255.0

negotiation auto

service-policy type performance-monitor input policy-filter
```

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

NetFlow Collector로 네트워크를 전송할 때 네트워크가 필터링되었는지 확인하는 방법

ISR4351 Gi0/0/0(NetFlow Collector를 가리키는 인터페이스)에서 EPC(Embedded Packet Capture)를 사용할 수 있음을 입증하기 위해 구성은 다음과 같습니다.

```
ip access-list extended CAP-FILTER

permit ip host 10.11.11.28 host 20.20.20.2

permit ip host 20.20.20.2 host 10.11.11.28
```

```
monitor capture CAP access-list CAP-FILTER buffer size 10 interface GigabitEthernet 0/0/0 both

monitor capture CAP start
```

```
++  TEST I

3650: -
```

```
telnet 10.10.10.2

Trying 10.10.10.2 ... Open
```

EPC에서 텔넷 트래픽에 대해 패킷이 캡처되지 않았습니다. 그 이유는 트래픽이 ACL(Access Control List)(ACL-filter)에서 거부되었고 나머지 모든 것이 허용되었기 때문입니다.

```
show monitor capture CAP buffer brief

------------------------------------------------------------

#   size   timestamp     source             destination   protocol

------------------------------------------------------------
```

이제 테스트 02에서 EPC에 따라 일치하는지 확인하기 위해 ping 트래픽을 생성합니다.

++ **TEST II**

3650: -

```
ping 10.10.10.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:

!!!!!
```

ISR4351:

```
show monitor capture CAP buffer brief

------------------------------------------------------------

#   size   timestamp     source             destination   protocol

------------------------------------------------------------

   0  122    0.000000   10.11.11.28      ->  20.20.20.2       UDP

   1   70    0.001998   20.20.20.2       ->  10.11.11.28      ICMP
```

1	0.000000	10.11.11.28	20.20.20.2	CFLOW	122	total: 1 (v9) record Obs-Domain-ID= 256 [Data:256]
2	0.000001	20.20.20.2	10.11.11.28	ICMP	70	Destination unreachable (Port unreachable)
3	0.000002	10.11.11.28	20.20.20.2	CFLOW	154	total: 1 (v9) record Obs-Domain-ID= 256 [Data-Template:256]
4	0.000003	20.20.20.2	10.11.11.28	ICMP	70	Destination unreachable (Port unreachable)
5	0.000004	10.11.11.28	20.20.20.2	CFLOW	122	total: 1 (v9) record Obs-Domain-ID= 256 [Data:256]
6	0.000005	20.20.20.2	10.11.11.28	ICMP	70	Destination unreachable (Port unreachable)

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.