# Flexible NetFlow-Filterung mit Performance Monitor

## Inhalt



## Einleitung

In diesem Dokument wird beschrieben, wie bestimmte IPs gefiltert werden, damit sie nicht von NetFlow aufgezeichnet werden.

Unterstützt von Vishal Kothari, Cisco TAC Engineer.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse von Flexible NetFlow verfügen.

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 3650-Switch
- Integrated Service Router (ISR) 4351

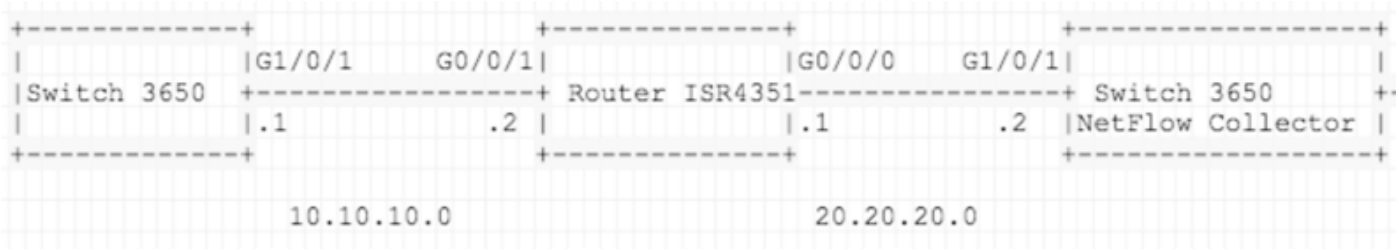
> **Anmerkung:** Um diese erforderliche Filterung unter NetFlow zu erreichen, müssen Sie die AppxK9-Lizenz installieren. Zum Testen können Sie die Lizenz Right-To-Use (RTU) AppxK9 nutzen.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

# Konfigurieren

In diesem Abschnitt müssen Sie die Liste der IPs filtern, die nicht von NetFlow aufgezeichnet werden müssen. Dies bedeutet außerdem, dass der Router keine Details über die Quelle und das Ziel der definierten IP in einer ACL senden sollte. Wie Sie dies mit Flexible NetFlow erreichen, erfahren Sie hier.

## Netzwerkdiagramm




## Konfigurationen

Bereiten Sie eine Liste aller Netzwerke vor, die Sie beim Senden an den NetFlow Collector herausfiltern möchten. In diesem Beispiel wird der Deny/Filter-Telnet-Datenverkehr an einen Collector gesendet und lässt den gesamten anderen Datenverkehr zu.

ISR 4351 Konfiguration:

```
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
```

# Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Wie kann ich überprüfen, ob die Netzwerke beim Senden an NetFlow Collector ausgefiltert wurden?

Um zu beweisen, dass Sie Embedded Packet Capture (EPC) auf dem ISR4351 Gi0/0/0 (Schnittstelle, die auf NetFlow Collector zeigt) verwenden können. Hier die Konfiguration:

```
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
```

Es wurden keine Pakete für Telnet-Datenverkehr unter EPC erfasst, da der Datenverkehr unter Zugriffskontrollliste (ACL) (ACL-Filter) abgelehnt wurde und alles andere erlaubt ist.

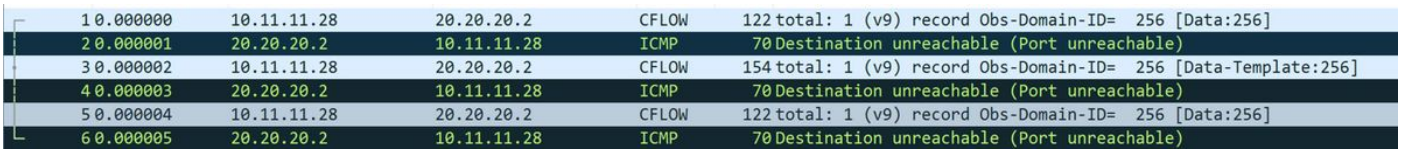
```
show monitor capture CAP buffer brief

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

#   size   timestamp     source             destination   protocol

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

Generieren Sie jetzt in Test 02 Ping-Datenverkehr, um zu überprüfen, ob er unter EPC übereinstimmt:

```
++ 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:

!!!!!
```

ISR 4351:

```
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
```




# Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.