含效能監控器的Flexible NetFlow篩選

目錄

簡介

本文檔介紹如何過濾某些IP以便不被NetFlow記錄。

作者：思科TAC工程師Vishal Kothari。

必要條件

需求

思科建議您瞭解Flexible NetFlow。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 3650交換器
- 整合式服務路由器(ISR)4351路由器

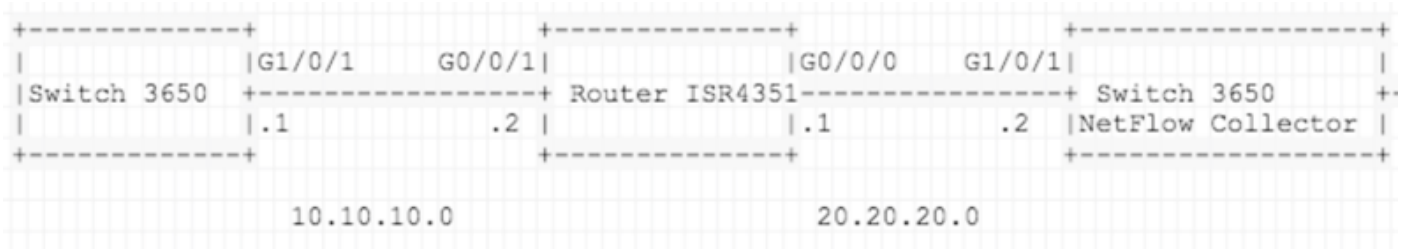
> **附註**：為了在NetFlow下實現所需的過濾，您需要安裝AppxK9許可證。對於測試，您可以使用使用權(RTU)AppxK9許可證。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

在本節中，您需要過濾掉NetFlow不需要記錄的IP清單，這進一步表示，路由器不應在ACL中傳送有關已定義IP的來源和目的地的詳細資訊。如何通過靈活的NetFlow實現這一目標，請點選此處。

網路圖表



組態

準備要過濾掉的所有網路的清單，同時將其傳送到NetFlow收集器。在此範例中，拒絕/過濾Telnet流量會傳送到收集器，且允許所有其他流量。

ISR4351配置：

```
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
```

驗證

使用本節內容，確認您的組態是否正常運作。

在將網路傳送到NetFlow收集器時，如何確認是否已過濾出網路？

為了證明您能夠在ISR4351 Gi0/0/0（指向NetFlow收集器的介面）上採用嵌入式資料包捕獲(EPC)。 以下是組態：

```
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
```

未在EPC下擷取Telnet流量的封包，原因是流量在存取控制清單(ACL)(ACL-filter)下遭到拒絕，且其餘所有內容都允許通過。

```
show monitor capture CAP buffer brief

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

#   size   timestamp     source             destination   protocol

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

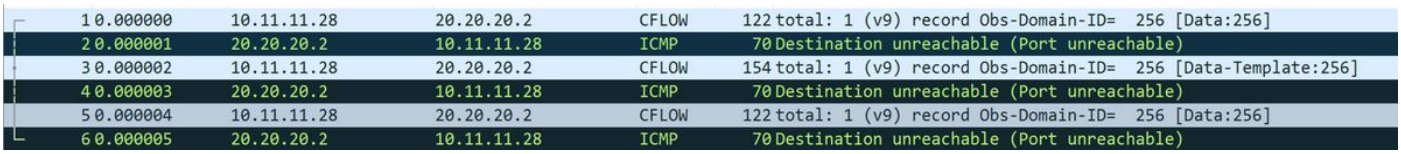
現在，在測試02中，生成ping流量，以檢視它是否在EPC下匹配：

```
++ 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)

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。