Performance MonitorによるFlexible NetFlowフィルタリング

内容

概要

このドキュメントでは、NetFlowによって記録されないように特定のIPをフィルタリングする方法について説明します。

著者：Cisco TACエンジニア、Vishal Kothari

前提条件

要件

Flexible NetFlowに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 3650 スイッチ
- サービス統合型ルータ(ISR)4351ルータ

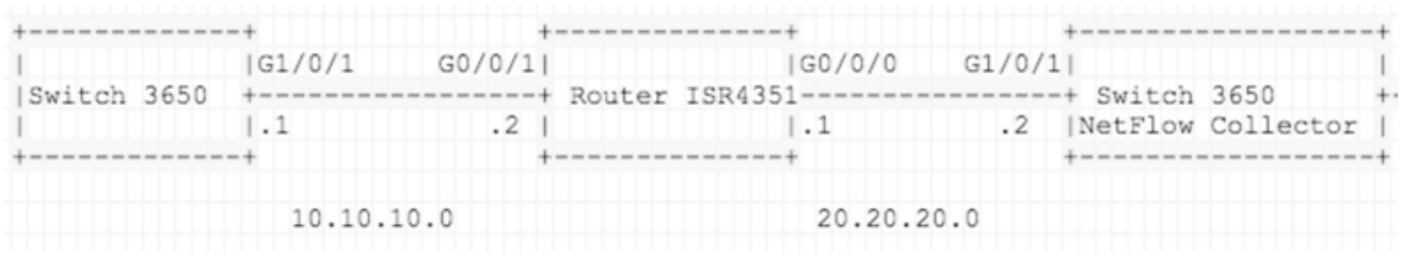
> **注：**NetFlowでこの必要なフィルタリングを行うには、AppxK9ライセンスをインストールする必要があります。テストには、Right-To-Use(RTU) AppxK9ライセンスを使用できます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

このセクションでは、NetFlowで記録する必要がないIPのリストをフィルタリングする必要があります。つまり、定義されたIPの送信元と宛先に関する詳細をACLでルータが送信してはなりません。Flexible NetFlowを通じてこれを実現する方法については、こちらをご覧ください。

ネットワーク図



設定

NetFlow Collectorへの送信時に除外するすべてのネットワークのリストを準備します。この例では、Telnetトラフィックの拒否/フィルタ処理がコレクタに送信され、他のすべてのトラフィックが許可されます。

ISR4351の設定：

```
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
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

NetFlow Collectorにネットワークを送信するときに、ネットワークがフィルタで除外されたかどうかを確認する方法

ISR4351 Gi0/0/0（NetFlowコレクタを指すインターフェイス）でEmbedded Packet Capture(EPC)を実行できることを証明するため。 次に設定を示します。

```
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
```

EPC下のTelnetトラフィックに対してパケットがキャプチャされませんでした。これは、トラフィックがアクセスコントロールリスト(ACL)(ACL-filter)下で拒否され、残りはすべて許可されているためです。

```
show monitor capture CAP buffer brief
```

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

#   size   timestamp     source             destination   protocol

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

次にテスト02で、EPCで一致するかどうかを確認するためにpingトラフィックを生成します。

```
++ 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)

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。