تصفية مرنة ل NetFlow مع مراقبة الأداء

المحتويات

المقدمة

يوضح هذا المستند كيفية تصفية بعض عناوين IP حتى لا يتم تسجيلها بواسطة NetFlow.

تمت المساهمة بواسطة فيشال كوثاري، مهندس TAC من Cisco.

المتطلبات الأساسية

المتطلبات

توصي cisco أن يتلقى أنت معرفة من NetFlow مرن.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- المحول 3650
- موجه الخدمة المتكاملة (ISR) 4351

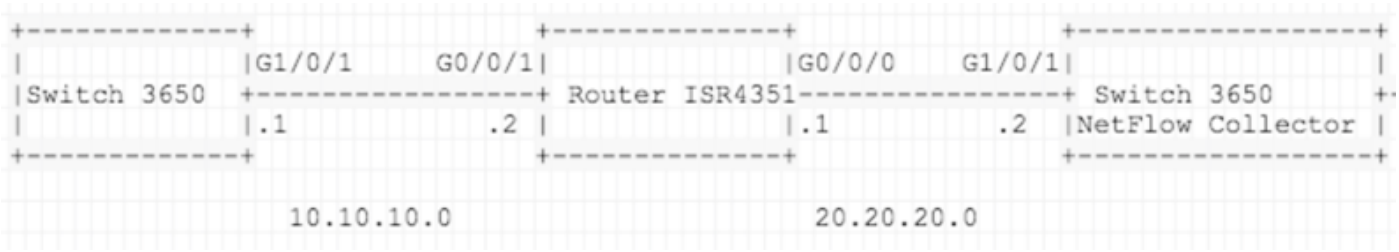
> **ملاحظة**: لتحقيق هذه التصفية المطلوبة تحت NetFlow، ستحتاج إلى تثبيت ترخيص AppxK9. للاختبار، يمكنك الاستفادة من ترخيص APPXk9 الموجود ضمن حق الاستخدام (RTU).

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

في اذه الqسم، يجب عليك تصفية قائمة برووتوكولات IP التي ال يلزم تسجيلها بواسطة NetFlow، وهو ما يعني أيضا أن المهوجه يجب ألا يرسل تفاصيل حول مصدر IP والوجهة المحددين في قائمة التحكم في الوصول (ACL). كيف يمكنك تحقيق ذلك من خالل تقنية NetFlow المرنة، ستجد هنا.

الرسم التخطيطي للشبكة



التكوينات

قم بإعداد قائمة بجميع هذه الشبكات التي تريد تصفيتها أثناء إرسالها إلى مجمع NetFlow. في اذه المثال، يتم إرسال حركة مرور رفض/تصفية Telnet إلى مجمع ويسمح لجميع حركة المرور الأخرى.

تكوين ISR4351:

```
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
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

كيف يمكنك تأكيد ما إذا كان قد تمت تصفية الشبكات عند إرسالها إلى مجمع NetFlow؟

إثبات أنه يمكنك أخذ التقاط الحزم المضمن (EPC) على ISR4351 Gi0/0/0 (واجهة تشير إلى مجمع NetFlow). هنا التكوين:

```
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
```

لم يتم التقاط أي حزم لحركة مرور Telnet ضمن EPC، وسبب ذلك أن حركة المرور تم رفضها بواسطة قائمة التحكم في الوصول (ACL) (تصفية قائمة التحكم في الوصول) وتم السماح بكل شيء للراحة.

```
show monitor capture CAP buffer brief

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

#   size   timestamp     source             destination   protocol
```

الآن في الاختبار 02، قم بإنشاء حركة مرور أزيز in order to رأيت إن يتم مطابقتها تحت EPC:

```
++ 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)

استكشاف الأخطاء وإصلاحها

لا تتوفر حالياً معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).