

Filtro NetFlow flessibile con Performance Monitor

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

Questo documento illustra come filtrare alcuni indirizzi IP in modo che non vengano registrati da NetFlow.

Contributo di Vishal Kothari, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di Flexible NetFlow.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Nota: Per ottenere il filtro richiesto in NetFlow, è necessario installare la licenza AppxK9. Per il test, è possibile utilizzare la licenza RTU (Right-To-Use) AppxK9.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione


```
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
```

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Come verificare se le reti sono state escluse quando le si invia a NetFlow Collector?

Per dimostrare che è possibile usare Embedded Packet Capture (EPC) su ISR4351 Gi0/0/0 (interfaccia verso NetFlow Collector). La configurazione è la seguente:

```
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
```

Nessun pacchetto acquisito per il traffico Telnet in EPC. Il motivo è che il traffico è stato rifiutato in Access Control List (ACL) (ACL-filtro) e il resto è stato autorizzato.

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

```
-----  
#   size  timestamp      source          destination    protocol  
-----
```

Nel test 02, generare il traffico ping per verificare se corrisponde ai valori 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
```

10.000000	10.11.11.28	20.20.20.2	CFLOW	122 total: 1 (v9) record Obs-Domain-ID= 256 [Data:256]
20.000001	20.20.20.2	10.11.11.28	ICMP	70 Destination unreachable (Port unreachable)
30.000002	10.11.11.28	20.20.20.2	CFLOW	154 total: 1 (v9) record Obs-Domain-ID= 256 [Data-Template:256]
40.000003	20.20.20.2	10.11.11.28	ICMP	70 Destination unreachable (Port unreachable)
50.000004	10.11.11.28	20.20.20.2	CFLOW	122 total: 1 (v9) record Obs-Domain-ID= 256 [Data:256]
60.000005	20.20.20.2	10.11.11.28	ICMP	70 Destination unreachable (Port unreachable)

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).