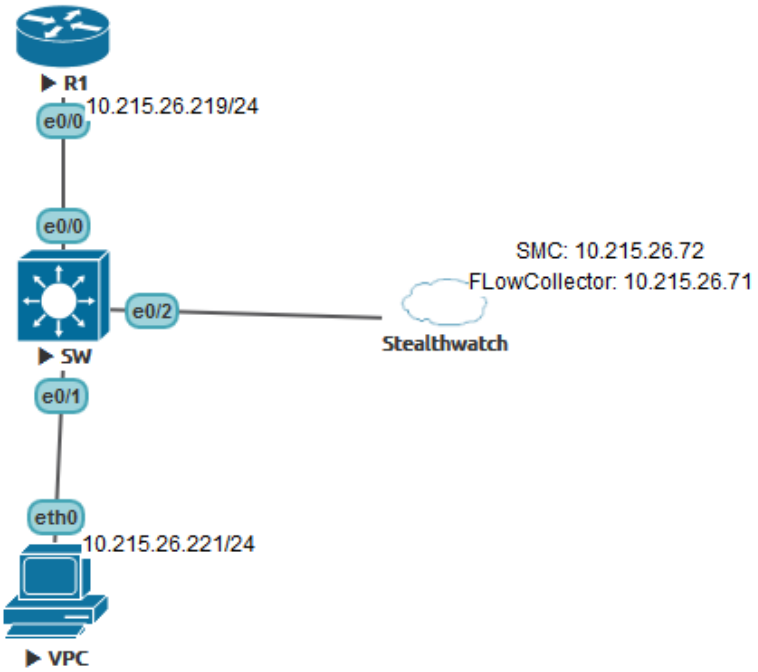
Lab – Steathwatch Basic

Sơ đồ mạng



Mô tả:

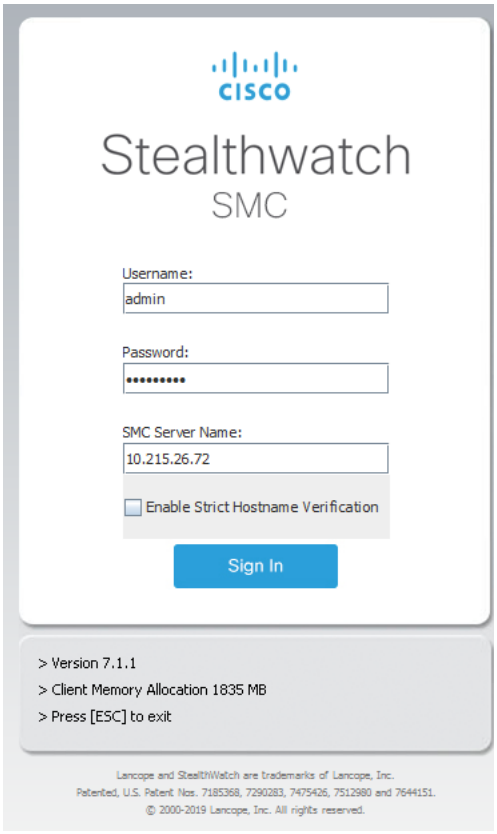
- Bài lab này được thực hiện trên LAB giả lập sử dụng các IOL Switch i86bi_linux_l2-advipservicesk9, IOL Router L3-ADVENTERPRISEK9-M-15.4-2T và PC ảo.
- Cổng e0/0 của R1: địa chỉ ip 10.215.26.219/24
- Trên switch 2 thực hiện cấu hình Netflow.
- Kết nối Switch với đám mây, đám mây này chính là 2 thiết bị stealthwatch cài đặt trên hệ thống ảo hóa Vsphere hoặc Vmware.

Trong mô hình thì Stealthwatch FlowCollector có địa chỉ ip là 10.215.26.71 và trạm quản trị StealthWatch SMC có địa chỉ là 10.215.26.72.

Các bước cấu hình

Chúng ta login vào giao diện web của flow SMC và quan sát góc trên bên trái có biểu tượng Desktop Client, chúng ta sẽ click vào biểu tượng đó. Máy tính sẽ tiến hành download một Java App gọi là Stealthwatch Management Console vào Windows (chỉ chạy trên windows 64 bit). Java App này sẽ giúp người dùng thao tác thuận tiện hơn.

Sau khi download thành công, double click vào biểu tượng App SMC để chạy ứng dụng. Cần nhập username và password của SMC và trỏ SMC server name là địa chỉ ip của SMC.



Bước tiếp theo chúng ta sẽ tiến hành cài đặt giao thức Netflow trên thiết bị mạng, cụ thể là R1 và Switch 2. R1 và Switch2 sẽ gửi các thông tin lưu lượng IP về Flow Collector.

TRÊN R1:

Đặt ip cho cổng e0/0

```
R1(config)#interface Ethernet0/0
R1(config-if)#ip address 10.215.26.219 255.255.255.0
R1(config-if)#no shut
```

Tiếp tục cấu hình Netflow cho R1. Đầu tiên chúng ta cấu hình *Flow record.*

```
R1(config)#flow record FLOW-RECORD
R1(config-flow-record)#description stealthwatch
R1(config-flow-record)#match datalink mac source address input
R1(config-flow-record)#match datalink mac destination address input
R1(config-flow-record)#match ipv4 tos
R1(config-flow-record)#match ipv4 ttl
R1(config-flow-record)#match ipv4 protocol
```

```
R1(config-flow-record)#match transport source-port
R1(config-flow-record)#match transport destination-port
R1(config-flow-record)#match interface input
R1(config-flow-record)#match interface output
R1(config-flow-record)#collect transport tcp flags
R1(config-flow-record)#collect counter bytes long
R1(config-flow-record)#collect counter packets long
```

Tiếp đến chúng ta sẽ cấu hình *Flow Exporter*.

```
R1(config)#flow exporter FLOW-EXPORTER
R1(config-flow-exporter)#destination 10.215.26.71    //Trong destination cần
trỏ về stealthwatch FlowCollector
R1(config-flow-exporter)#source Ethernet0/0     //source trong exporter sẽ
chọn cổng e0/0 trên R1 cần gửi thông tin về stealthwatch
R1(config-flow-exporter)#transport udp 2055
```

Flow monitor sẽ là bước cấu hình tiếp theo.

```
R1(config)#flow monitor FLOW-MON
R1(config-flow-monitor)#exporter FLOW-EXPORTER
R1(config-flow-monitor)#cache timeout inactive 60
R1(config-flow-monitor)#cache timeout active 15
R1(config-flow-monitor)#record FLOW-RECORD
```

Gán flow monitor vào cổng và cấu hình bắt luồng ingress và egress trên cổng này.

```
R1(config)#interface Ethernet0/0
R1(config-if)#ip flow monitor FLOW-MON input
R1(config-if)#ip flow monitor FLOW-MON output
R1(config-if)#ip flow ingress
R1(config-if)#ip flow egress
R1(config)#ip flow-export destination 10.215.26.71 2055
```

TRÊN SWITCH 2:

Tương tự R1 thì chúng ta cũng cấu hình Netflow trên Switch 2.

```
SW2(config)#flow record FLOW-RECORD
SW2(config-flow-record)#description stealthwatch
SW2(config-flow-record)#match datalink mac source address input
SW2(config-flow-record)#match datalink mac destination address input
SW2(config-flow-record)#match ipv4 tos
SW2(config-flow-record)#match ipv4 ttl
SW2(config-flow-record)#match ipv4 protocol
SW2(config-flow-record)#match transport source-port
SW2(config-flow-record)#match transport destination-port
SW2(config-flow-record)#match interface input
```

```
SW2(config-flow-record)#match interface output
SW2(config-flow-record)#collect transport tcp flags
SW2(config-flow-record)#collect counter bytes long
SW2(config-flow-record)#collect counter packets long
```

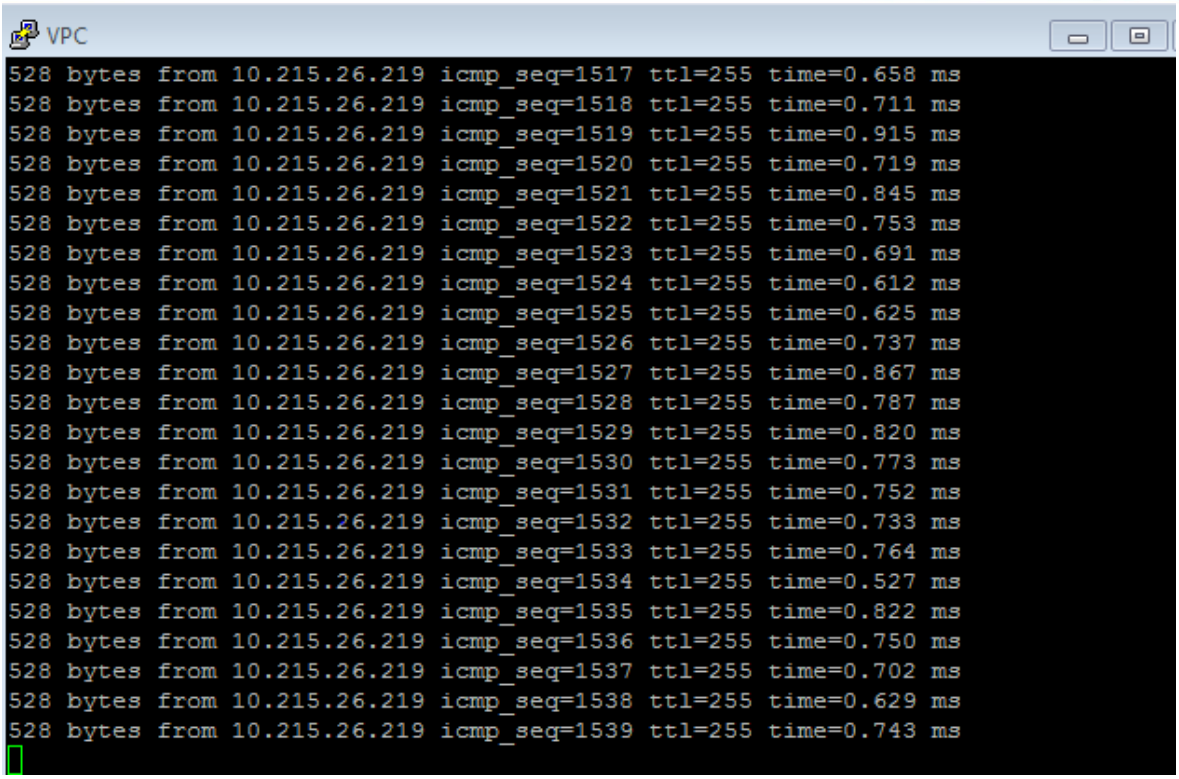
```
SW2(config)#flow exporter FLOW-EXPORTER
SW2(config-flow-exporter)#destination 10.215.26.71   //Destination sẽ trỏ về
stealthwatch FlowCollector.
SW2(config-flow-exporter)#transport udp 2055
```

```
SW2(config)#flow monitor FLOW-MON
SW2(config-flow-monitor)#exporter FLOW-EXPORTER
SW2(config-flow-monitor)#cache timeout inactive 60
SW2(config)#ip flow-exporter destination 10.215.26.71 2055
```

Sau khi cấu hình Netflow, chúng ta sẽ gán flow monitor và cấu hình bắt luồng ingress-egress trên các cổng.

```
SW2(config)#interface Ethernet0/0-2
SW2(config-if-range)# ip flow ingress
SW2(config-if-range)#  ip flow egress
SW2(config-if-range)# ip flow monitor FLOW-MON input
```

Tiến hành dùng vPC để ping đến địa chỉ 10.215.26.219 của R1.(vPC có địa chỉ ip tĩnh là 10.215.26.221 và đặt gateway là 10.215.26.219)



Dùng lệnh **show ip cache flow** để xem luồng dữ liệu chạy qua R1.

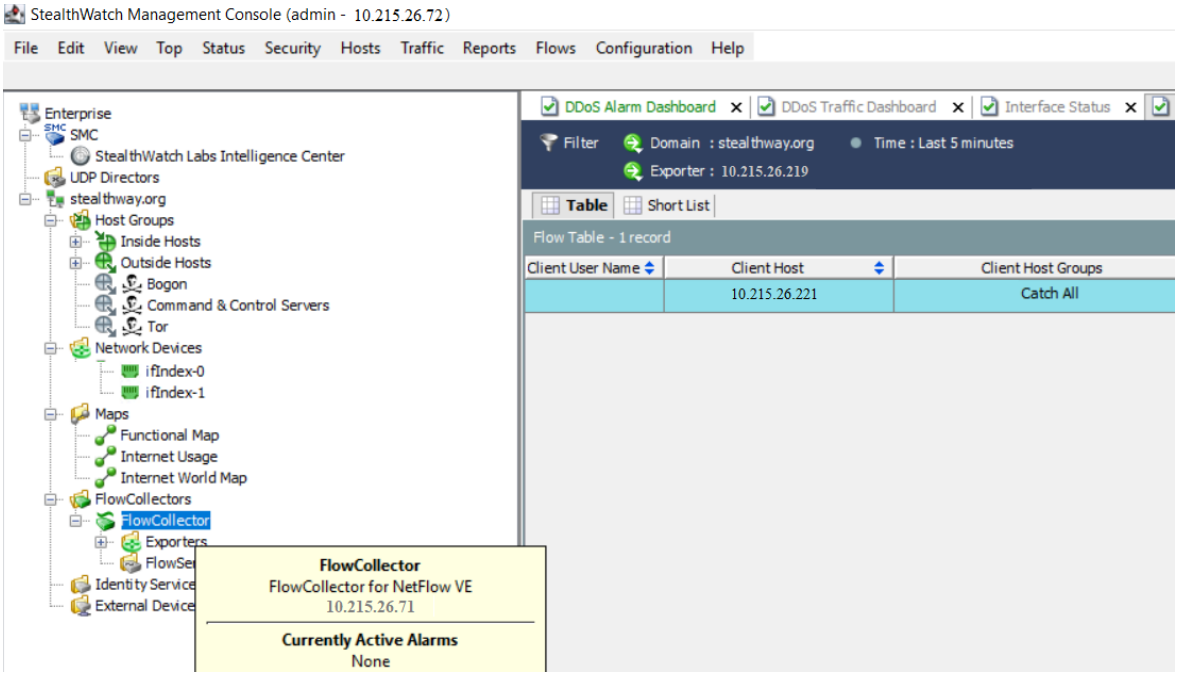
```
R1#show ip cache flow
IP packet size distribution (165 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448
480
   .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
.000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  1 active, 4095 inactive, 1 added
  167 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec)
Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
```

```
SrcIf           SrcIPaddress     DstIf           DstIPaddress     Pr SrcP DstP
Pkts
Et0/0           10.215.26.221    Local           10.215.26.219    01 0000 0800
165
```

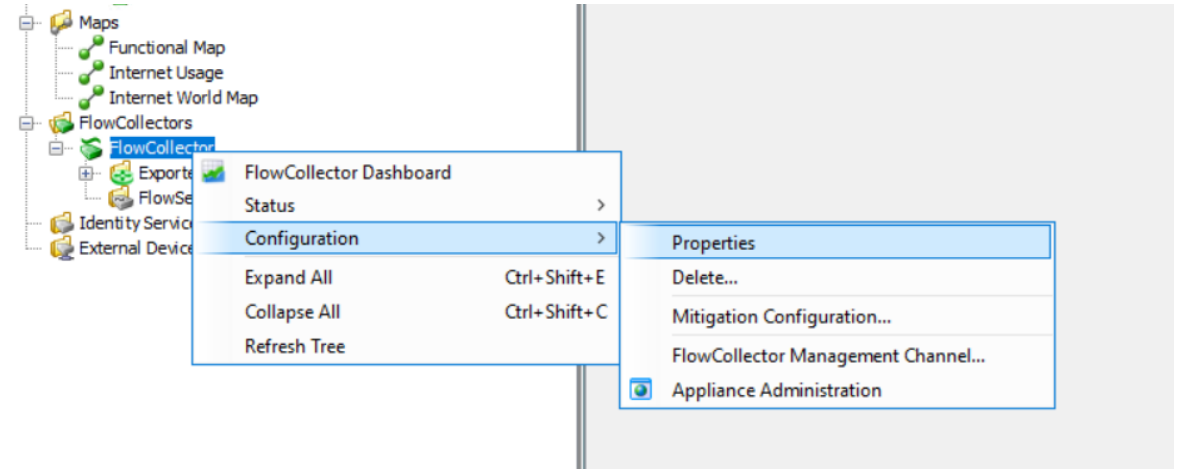
Chuyển sang Stealthwatch để giám sát lưu lượng traffic.

Đầu tiên thay đổi monitor port của flow collector trong desktop client SMC

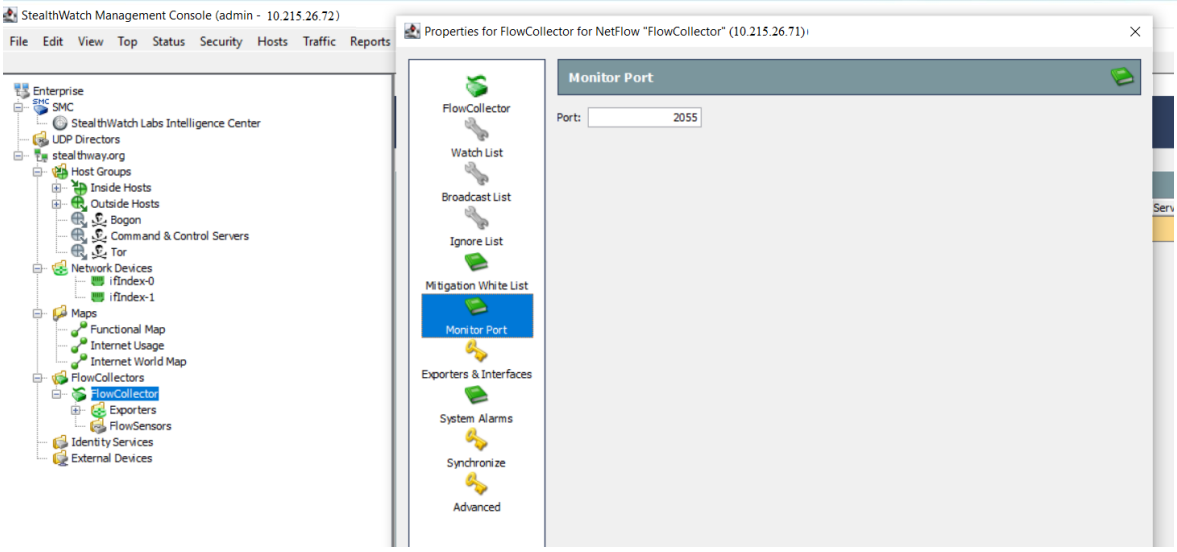
Mở rộng domain của SMC, ở phần FlowCollectors, rê chuột đến FlowCollector để xem thông tin và chọn đúng FlowCollector cần chỉnh sửa (Trong trường hợp này là 10.215.26.71.



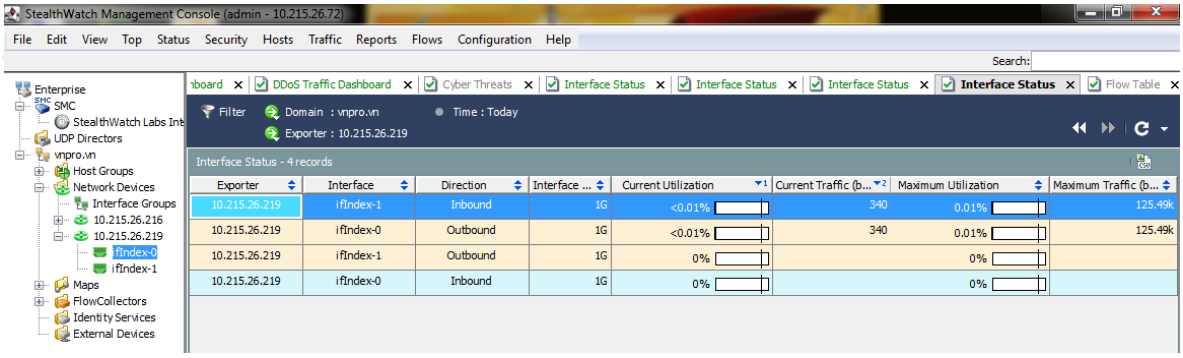
Click chuột phải vào FlowCollector cần chỉnh và chọn Configuration → Properties



Vào phần monitor port và chỉnh sửa lại 2055 như số port khi cấu hình

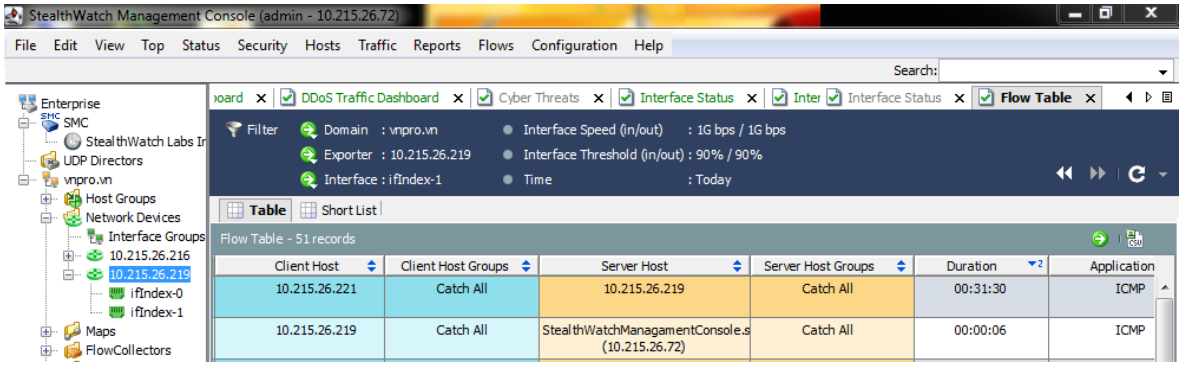


Bên góc trái màn hình, có thể thấy Stealthwatch đã nhận các địa chỉ từ các thiết bị cấu hình Netflow về.(địa chỉ 10.215.26.219 của R1).



Trong hình trên, có thể thấy Stealthwatch đã bắt được luồng traffic từ vPC gửi đến R1. Để quan sát và theo dõi kỹ hơn source và destination ip cũng như dạng application là gì chúng ta thực hiện **trỏ chuột vào hàng ip cần theo dõi → flow→ flow table**(hoặc nếu bạn đang xem ở dạng biểu đồ,thì thực hiện trỏ chuột vào biểu đồ cần xem → flow→ flow table).

Kết quả trong hình dưới đây cho thấy source và destination ip của gói ICMP cần theo dõi cũng như lưu lượng của nó là bao nhiêu.



icmp (Echo Request)	4k	922.36k	1,889	Nov 16, 2019 3:50:14 PM (53 minutes 40s ago)	922.36k	100%		

Như vậy chúng ta đã có thể thực hiện việc theo dõi traffic cơ bản bằng giao thức Netflow với sự hỗ trợ của Stealthwatch.