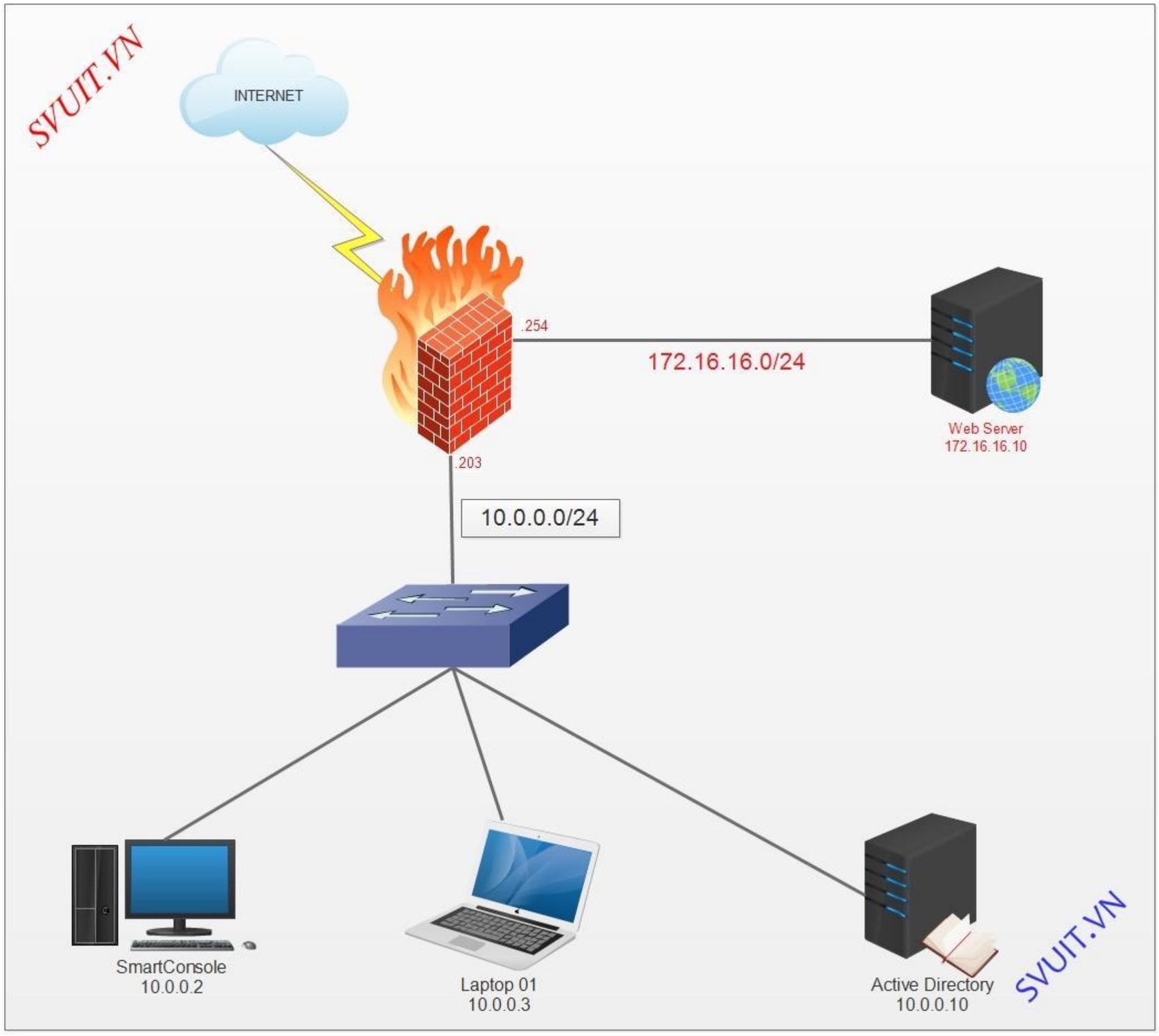
NAT & Rule Internal truy cập Internet

I. Yêu cầu và chuẩn bị

- Sơ đồ đấu nối thiết bị tron bài lab


SVUIT.VN
INTERNET
.254
172.16.16.0/24
Web Server
172.16.16.10
.203
10.0.0.0/24
SmartConsole
10.0.0.2
Laptop 01
10.0.0.3
Active Directory
10.0.0.10
SVUIT.VN

- Sơ đồ IP

Firewall	Eth0	EXTERNAL	172.23.25.243	
Eth1	DMZ	172.16.16.254/24		
Eth2	INTERNAL	10.0.0.203/24		
Active Directory			10.0.0.10/24	10.0.0.203
SmartConsole			10.0.0.2/24	10.0.0.203
Web Server			172.16.16.10/24	172.16.16.254

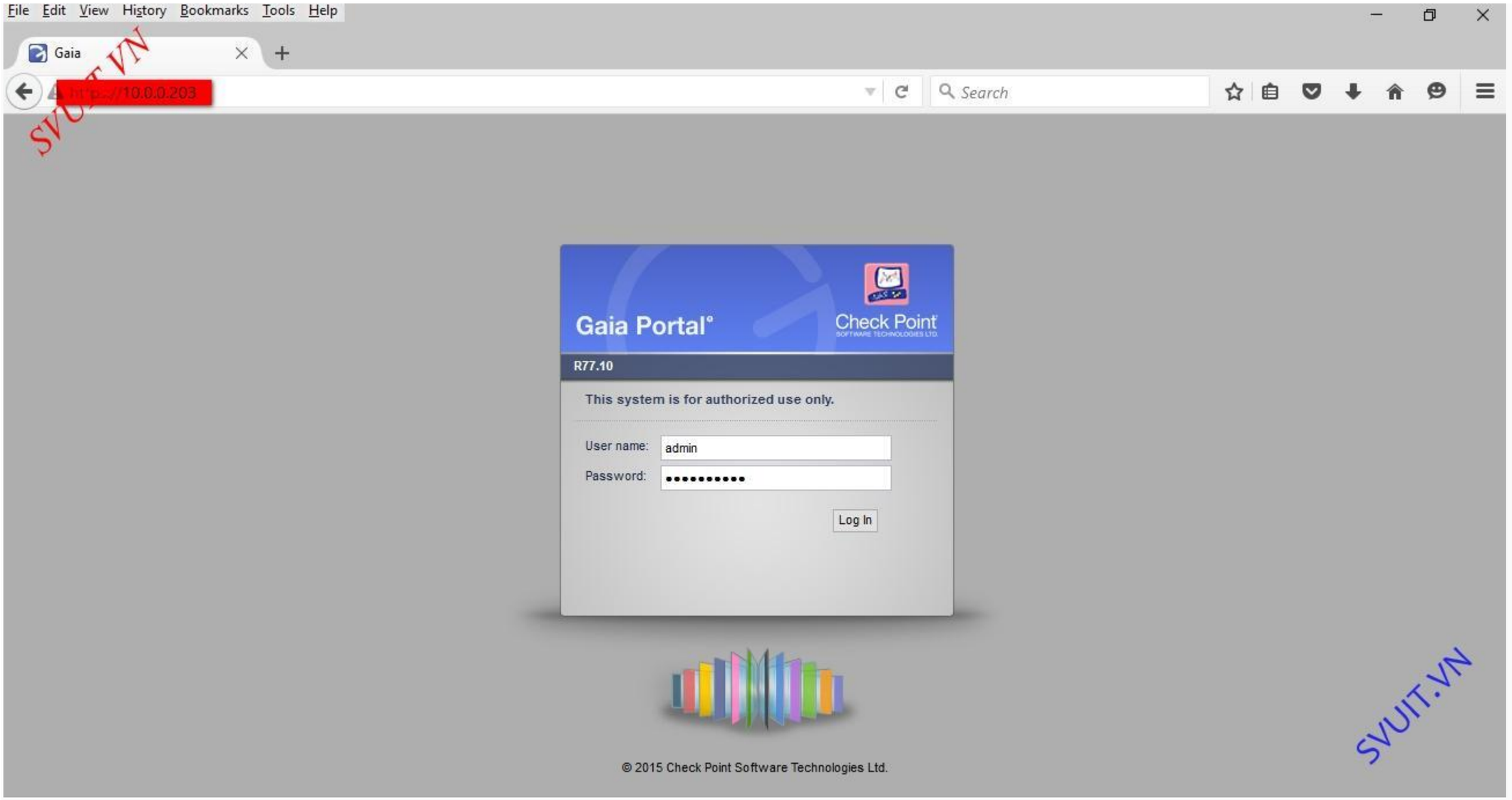
- Yêu cầu:

- Cấu hình để các PC trong Network internal có thể truy cập internet

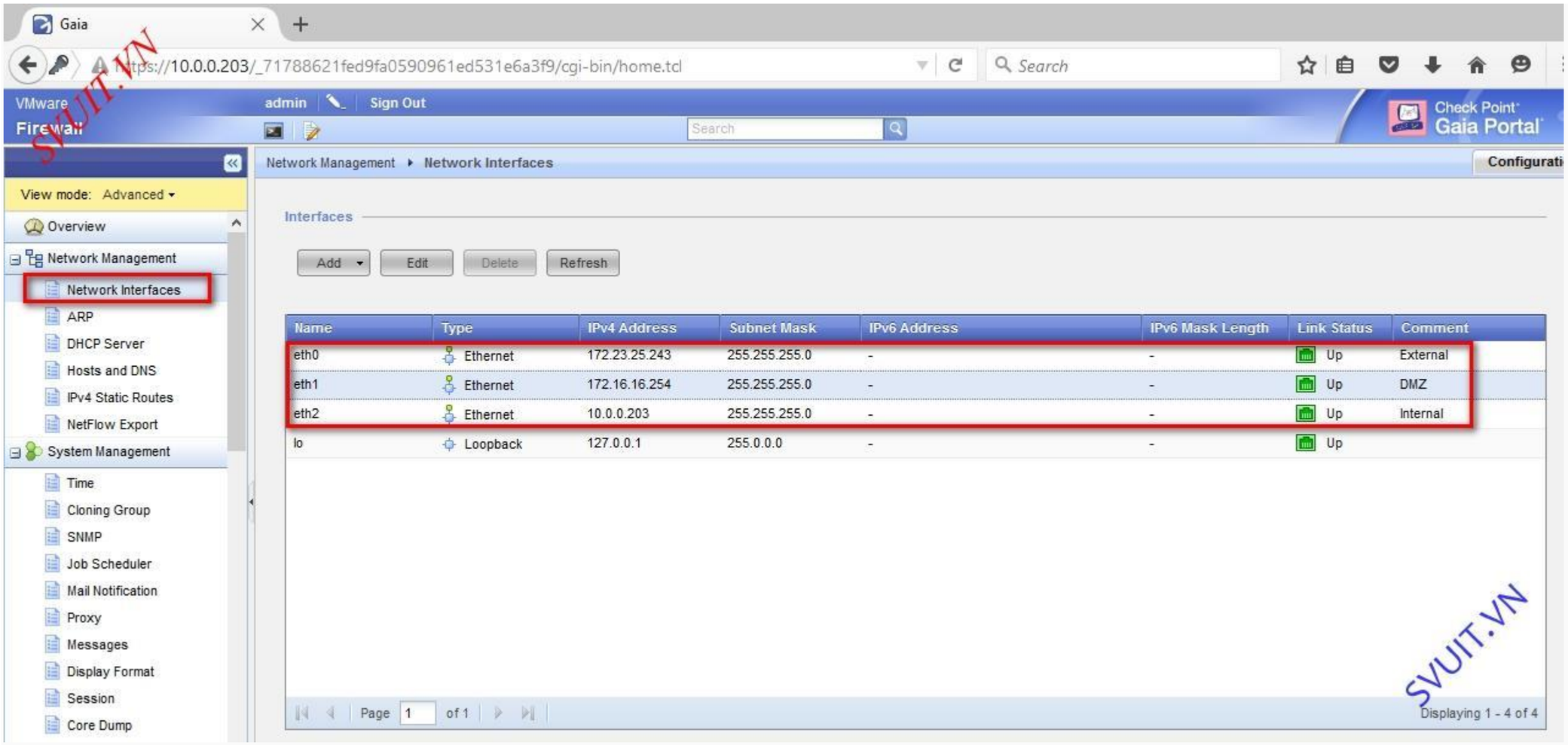
II. Triển khai

2.1. Cấu hình NAT

- Tiến hành NAT trên Firewall Checkpoint để vùng LAN Internal ra internet
- Sử dụng trình duyệt web login vào Firewall Checkpoint thông qua IP của interface Management của Checkpoint



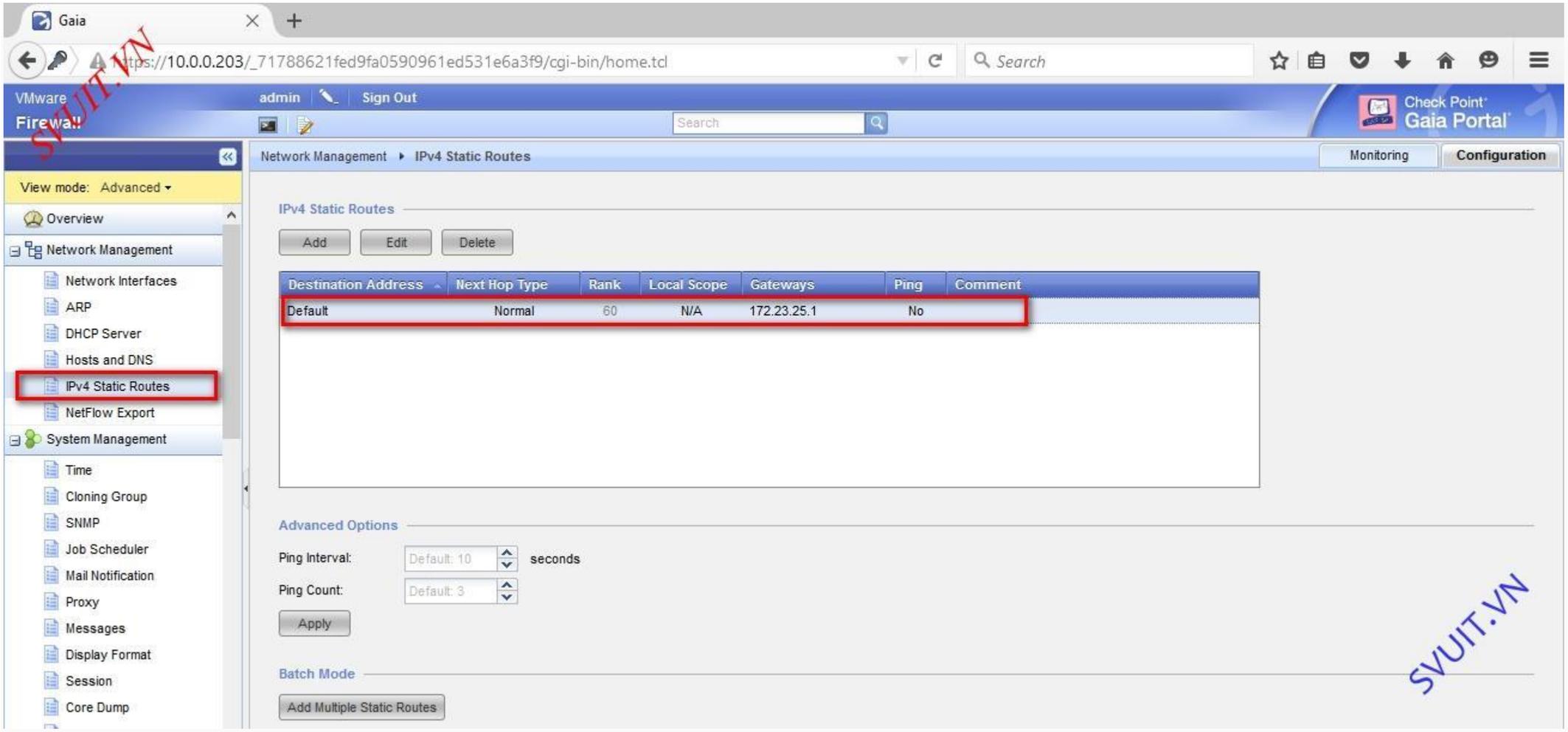
- Thiết lập IP cho các interface của Checkpoint thông qua trình duyệt web



- Hoặc bạn cũng có thể cấu hình IP của các interface Checkpoint thông qua giao diện dòng lệnh của Checkpoint

```
Checkpoint01> set interface eth2 ipv4-address 10.0.0.201 subnet-mask 255.255.255
.0
Checkpoint01> save config
Checkpoint01> _
```

- Tiếp theo chúng cần thực hiện cấu hình default-route cho Checkpoint



- Các bạn qua Checkpoint kiểm tra bảng định tuyến và ping tới 8.8.8.8 thành công

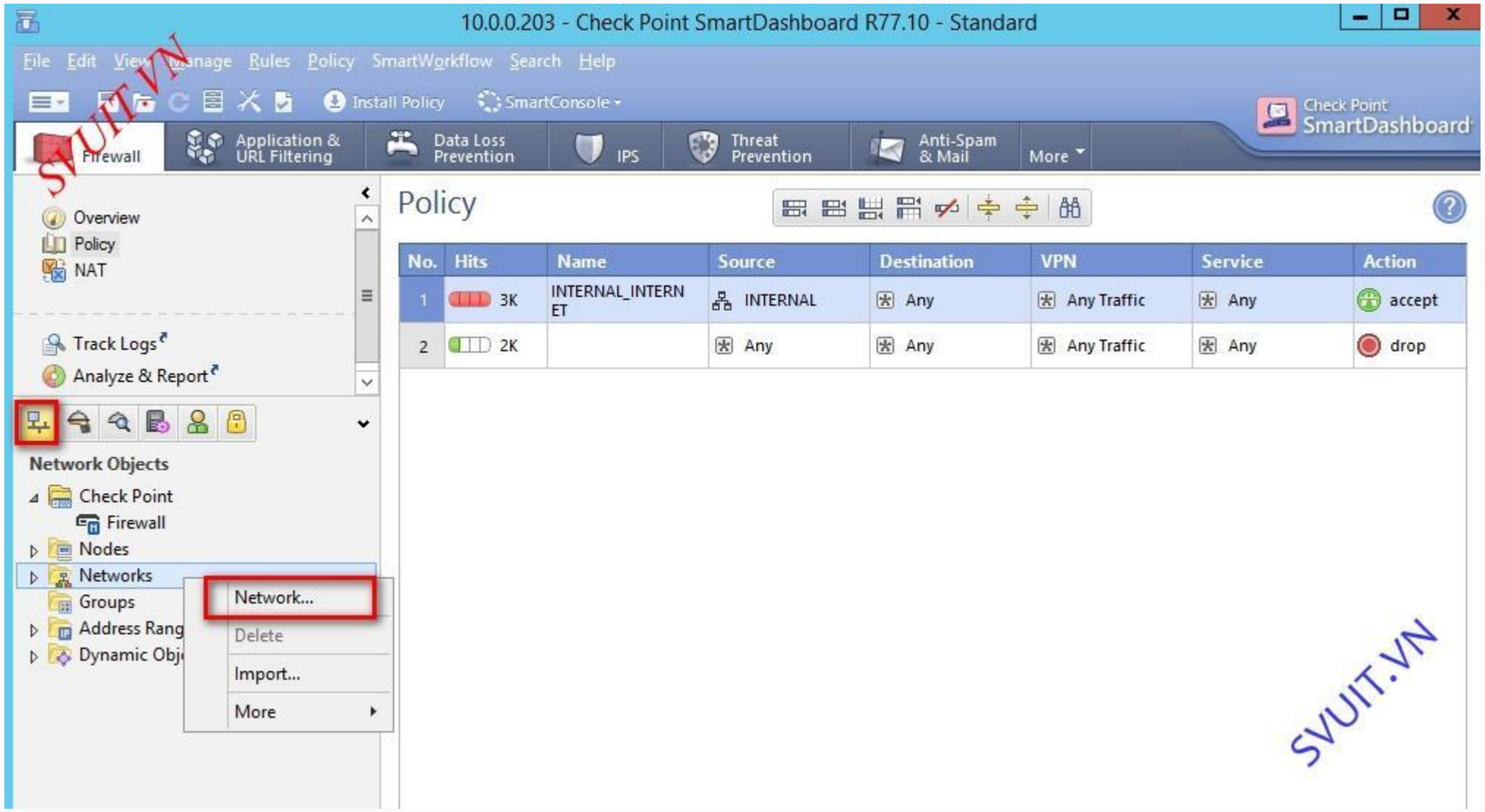
```
Firewall> show route
Codes: C - Connected, S - Static, R - RIP, B - BGP,
       O - OSPF IntraArea (IA - InterArea, E - External, N - NSSA)
       A - Aggregate, K - Kernel Remnant, H - Hidden, P - Suppressed,
       U - Unreachable, i - Inactive

S          0.0.0.0/0           via 172.23.25.1, eth0, cost 0, age 3998
C          10.0.0.0/24         is directly connected, eth2
                                   Internal
C          127.0.0.0/8         is directly connected, lo
C          172.16.16.0/24      is directly connected, eth1
                                   DMZ
C          172.23.25.0/24      is directly connected, eth0
                                   External
Firewall> ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=44 time=61.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=44 time=135 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=44 time=60.8 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3001ms
rtt min/avg/max/mdev = 60.893/85.957/135.767/35.221 ms
^C
```


2.2. NAT và Access Rules

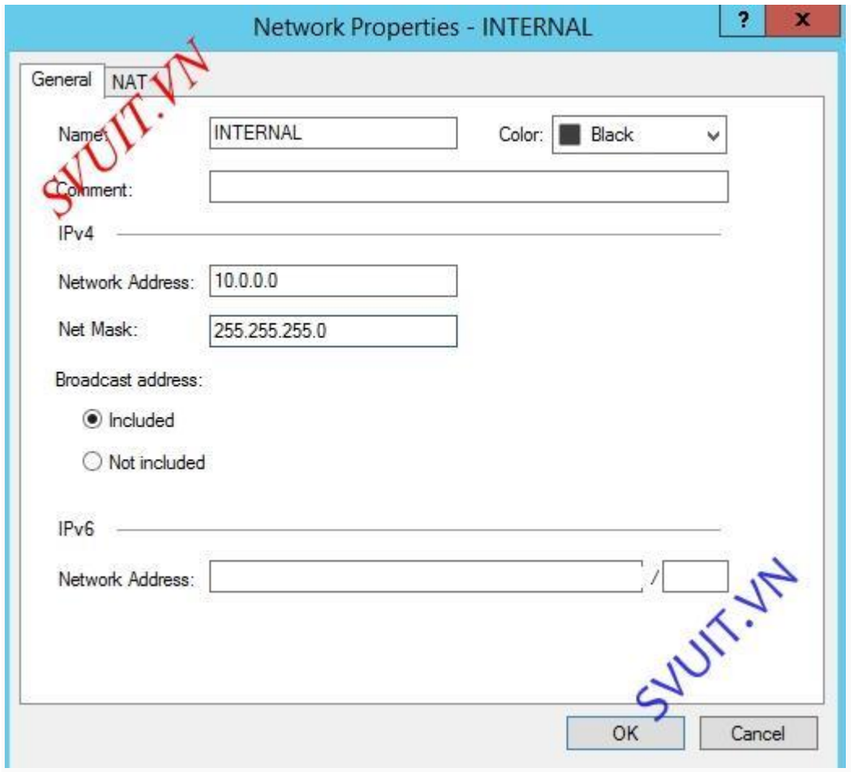
- Các bạn login vào checkpoint thông qua giao diện SmartConsole của Checkpoint để cấu hình NAT và Access Rule cho Checkpoint

- Tiến hành tạo các Network cho các interface của Checkpoint.

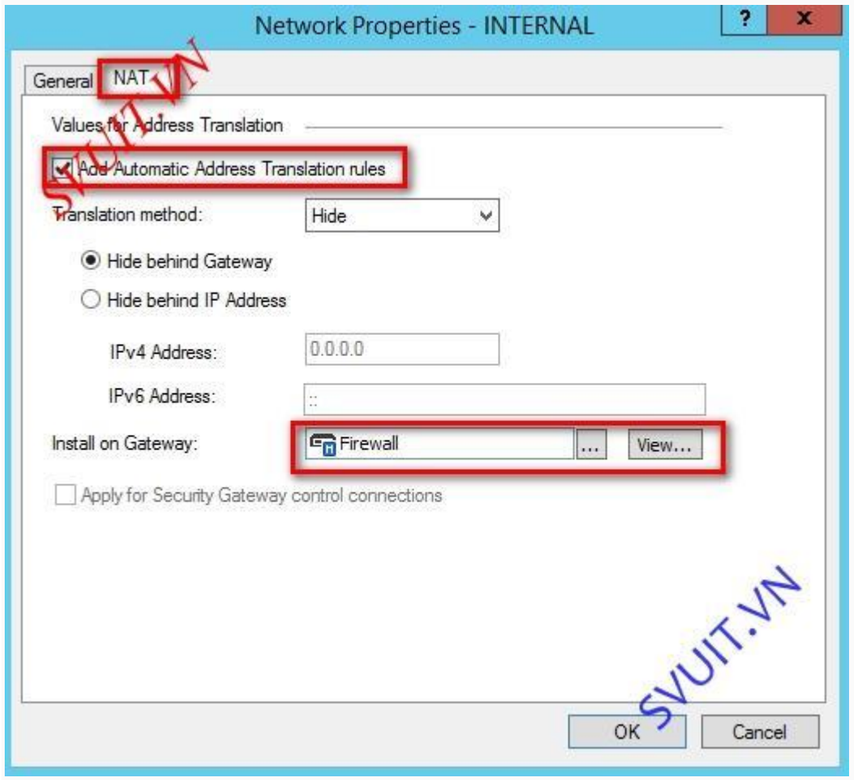
Network Objects -> Network



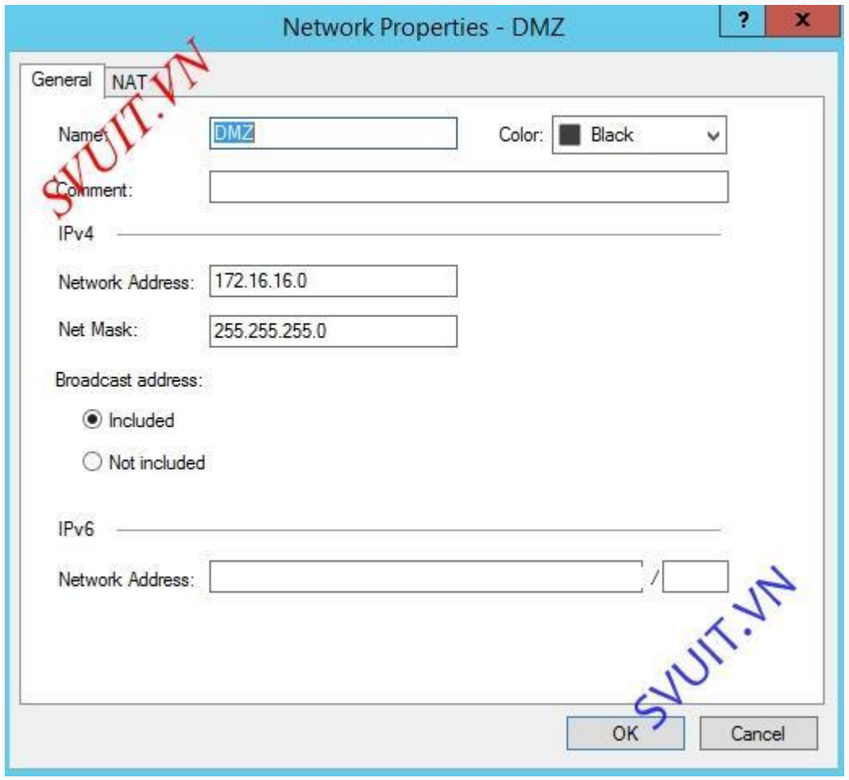
- Khai báo subnet INTERNAL



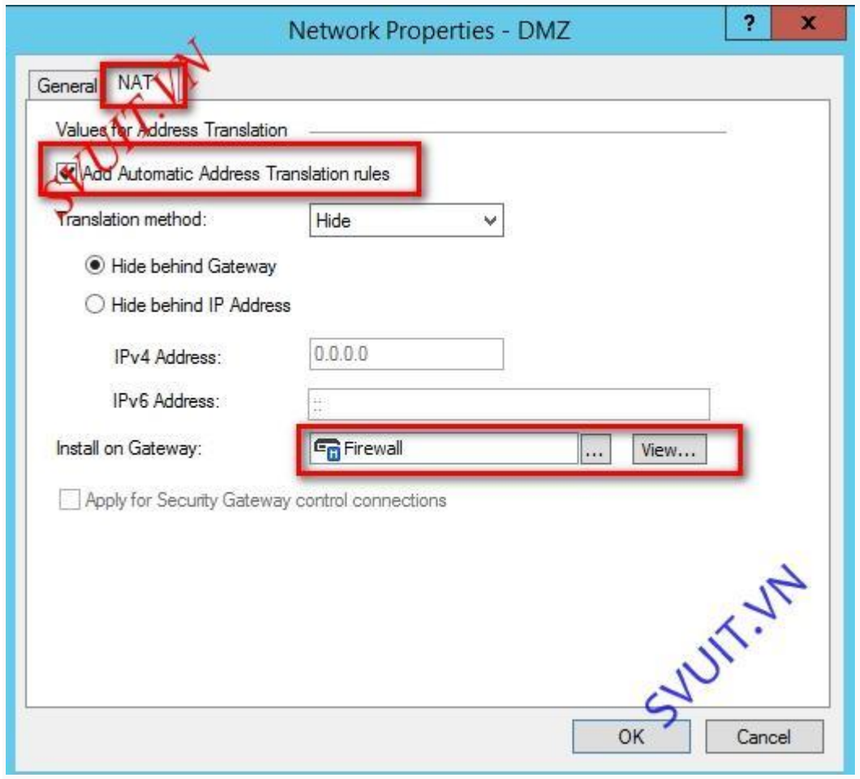
- Tiến hành NAT vùng INTERNAL ra internet thông qua Firewall Checkpoint



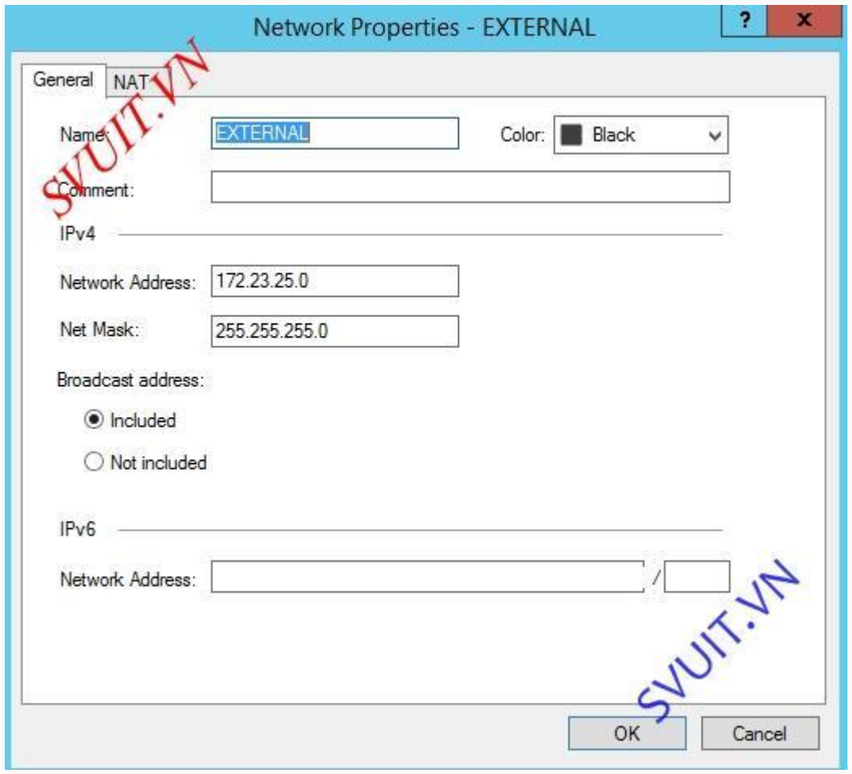
- Chúng ta cấu hình tương tự cho Network DMZ



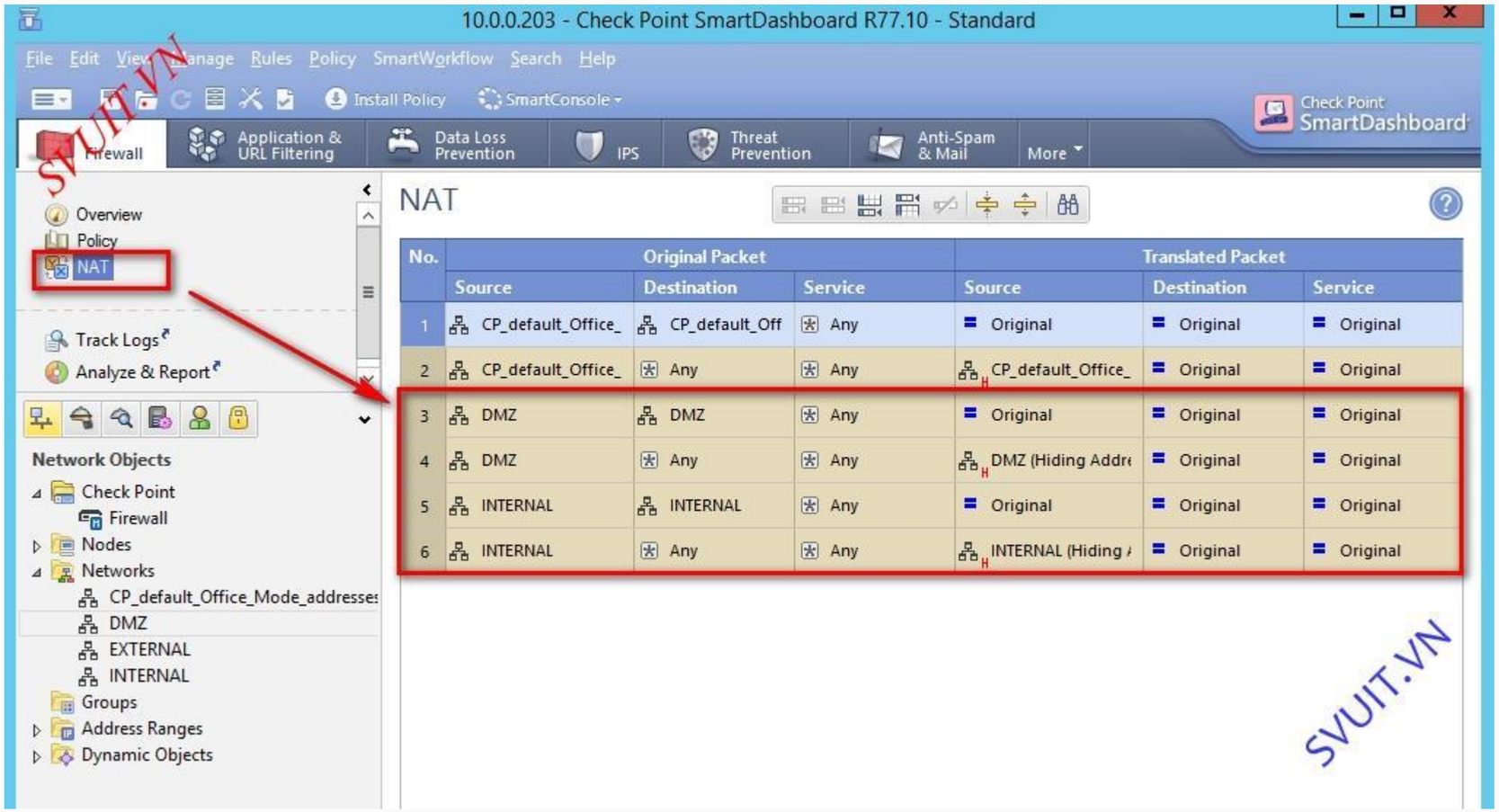
- Và cũng tiến hành NAT vùng DMZ ra internet



- Tạo network cho vùng EXTERNAL

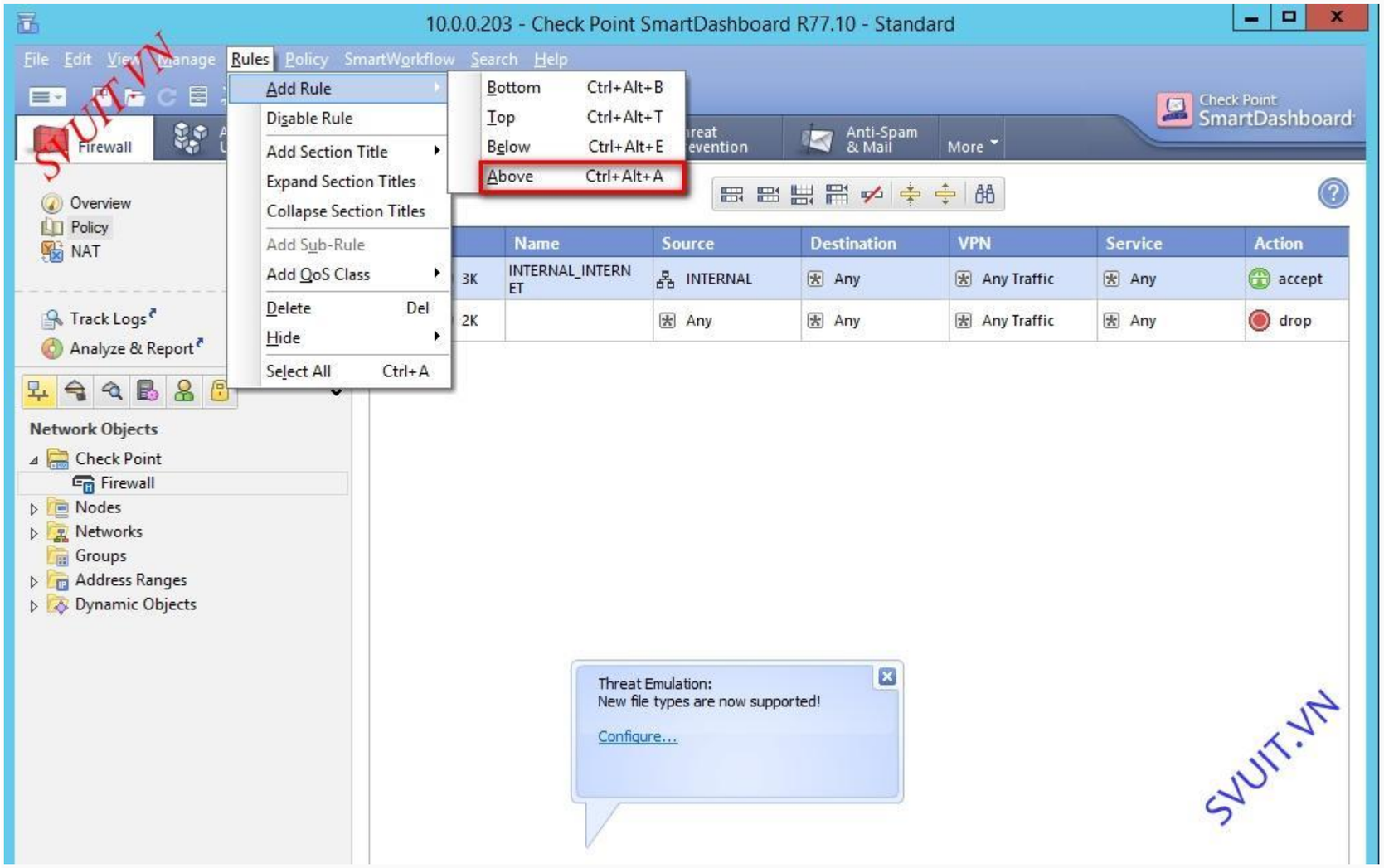


- Các bạn có xem lại bảng NAT mà các bạn đã tạo

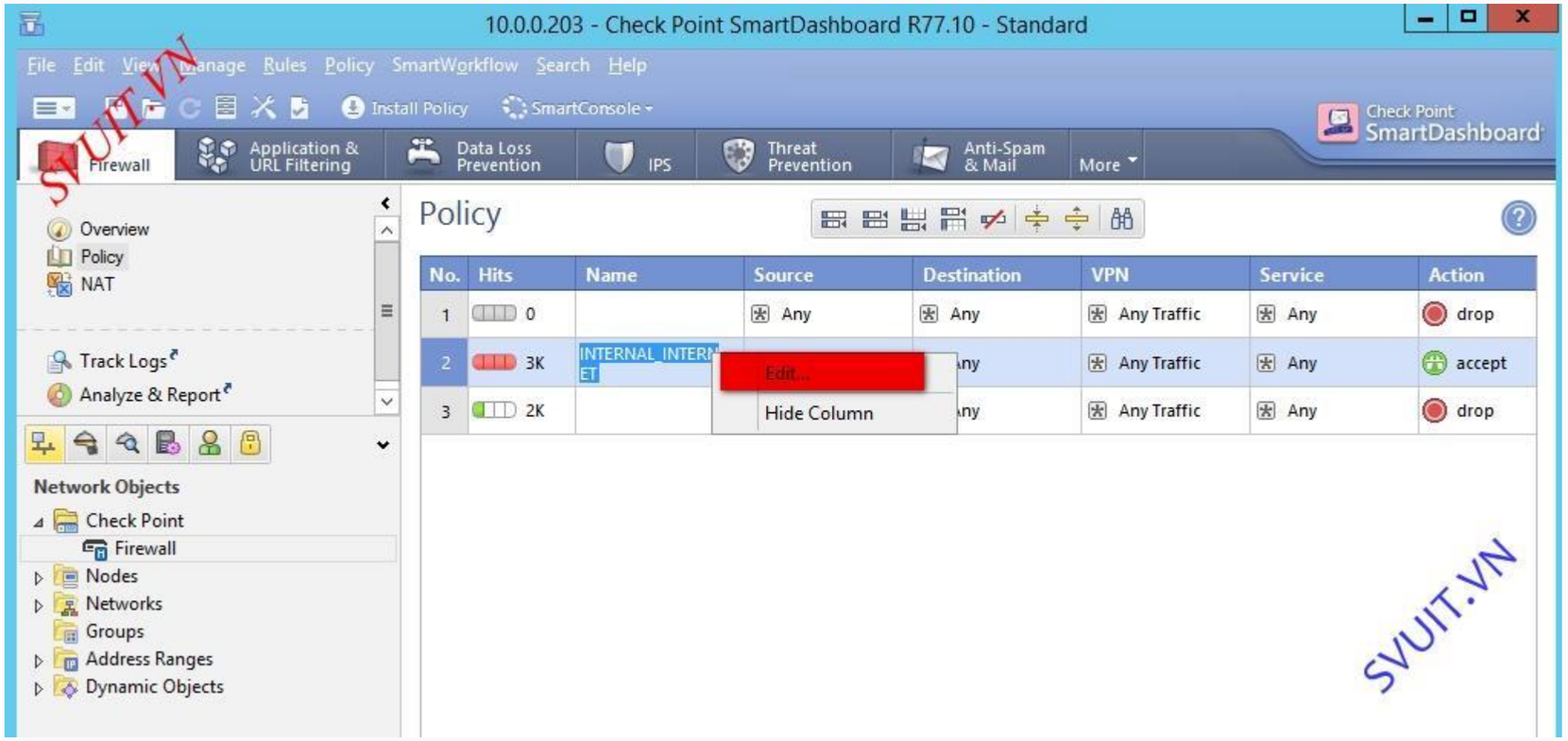


2.3. Access Rule

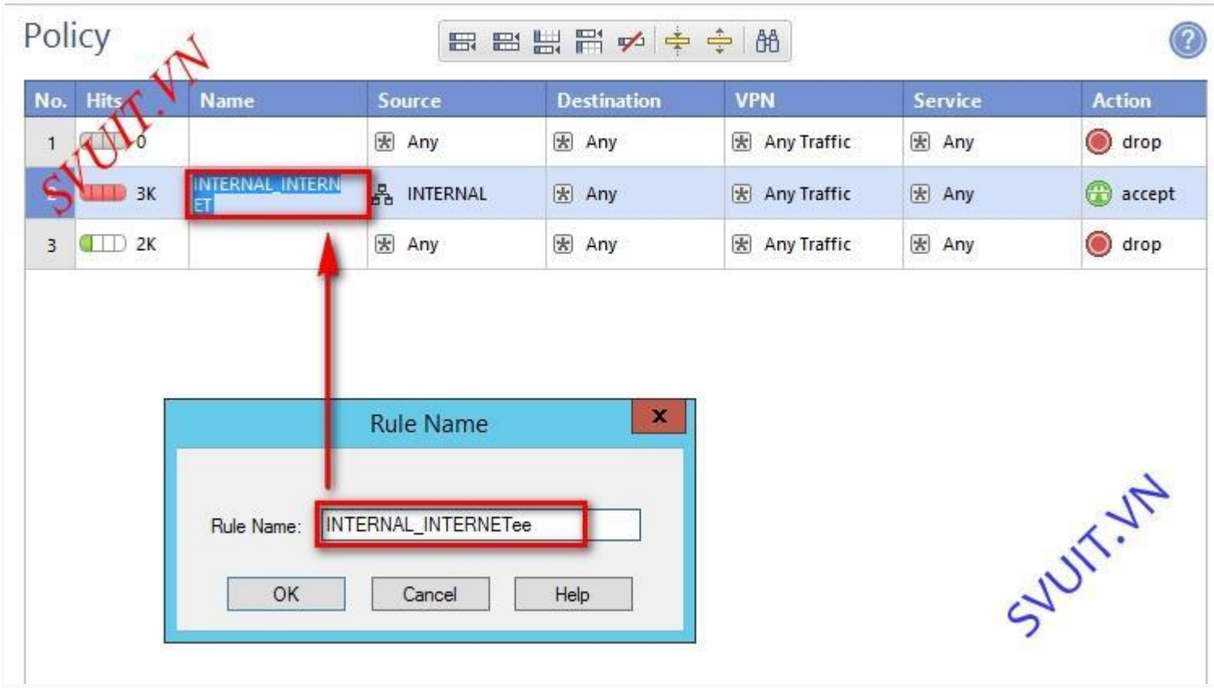
- Tiếp theo chúng ta tiến hành tạo rule cho phép vùng internal được truy cập ra internet. Chúng ta sẽ tạo 1 Rule nằm trên rule default của Firewall



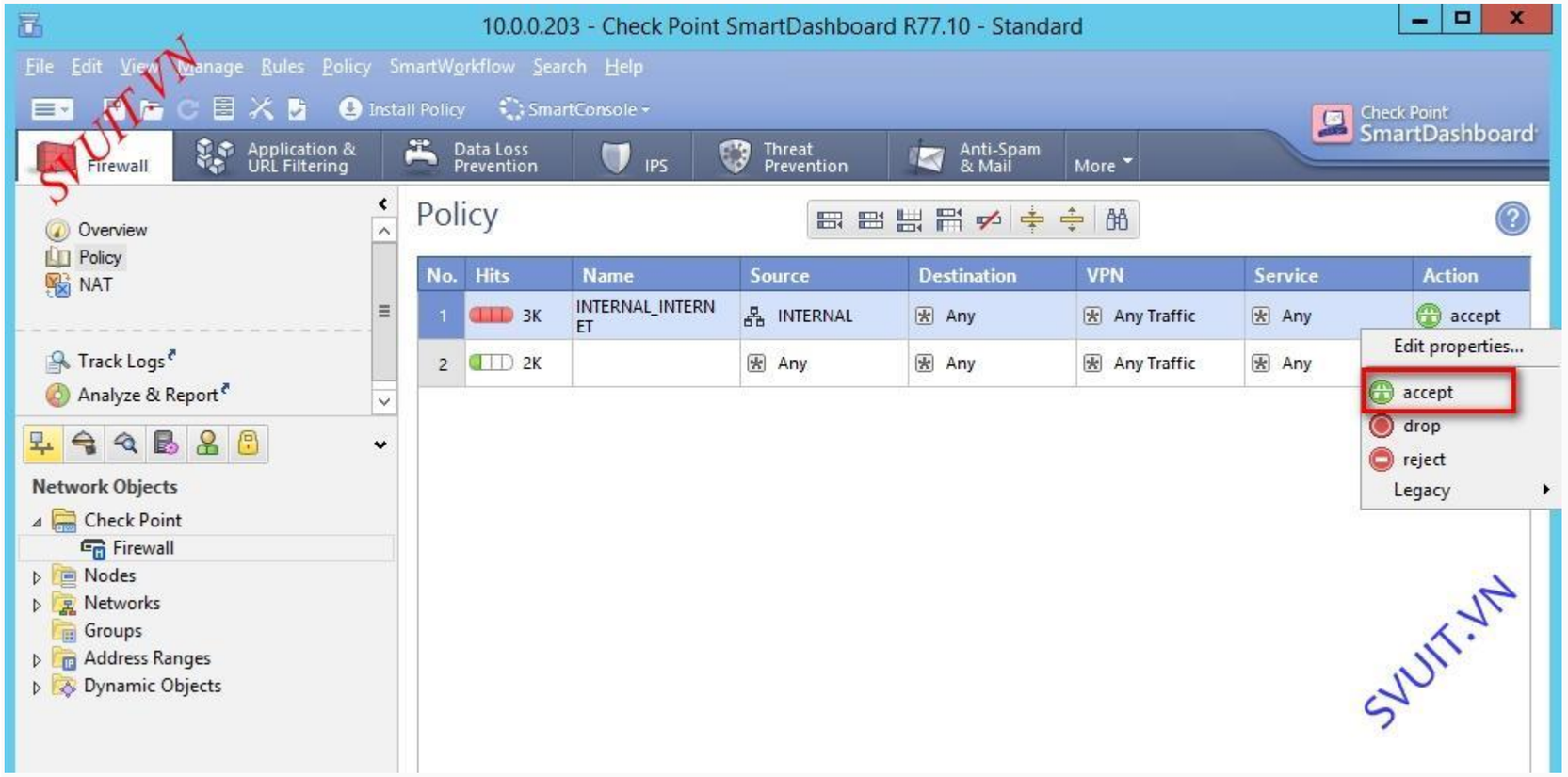
- Sau khi add rule mới các bạn cần edit Rule mới add
- Chuột phải vào vùng Name và chọn edit để đặt tên cho Rule bạn mới tạo



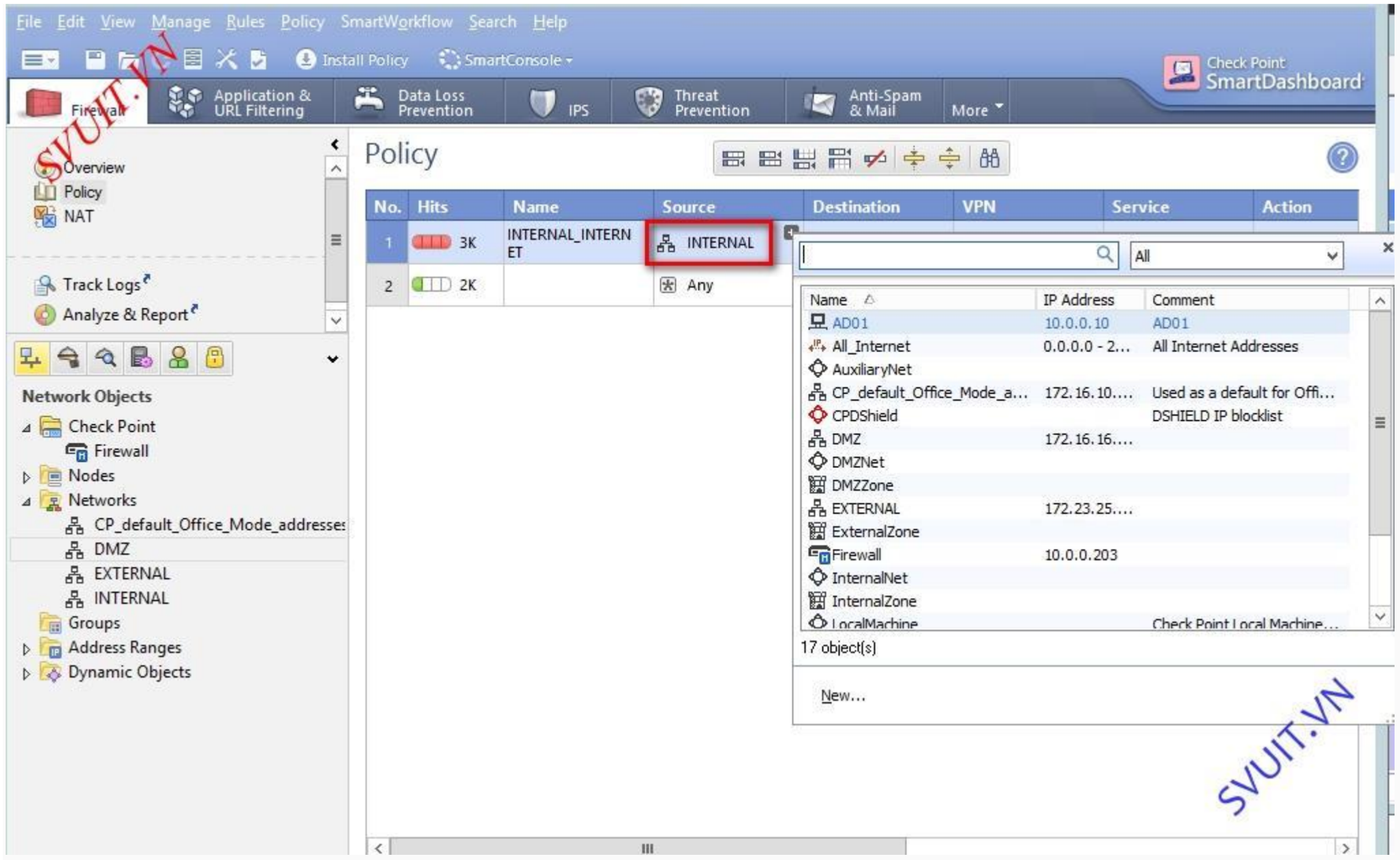
- Đặt tên cho Rule mới tạo



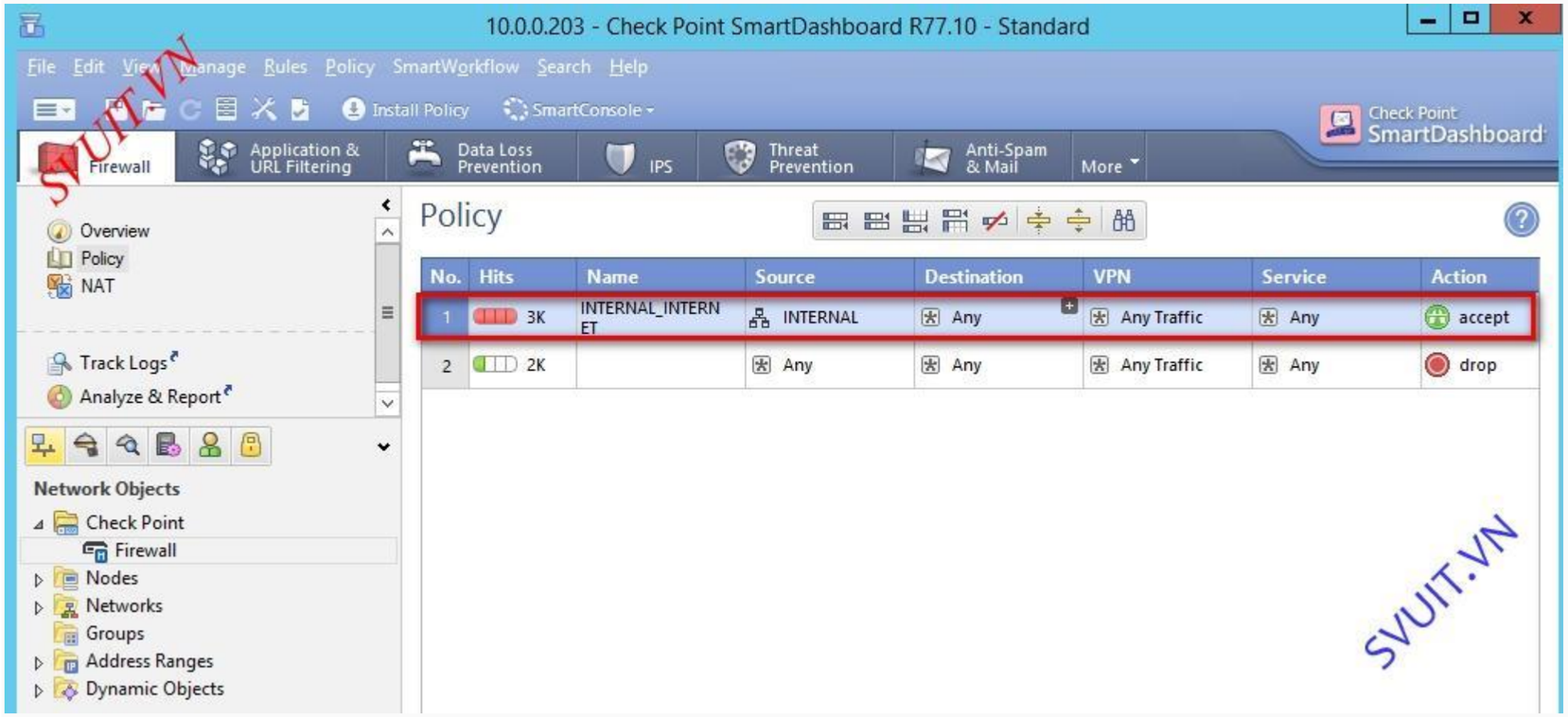
- Chuột phải lên vùng Action để chuyển từ trạng thai Drop sang Accept để cho phép gói tin từ internal đi ra ngoài



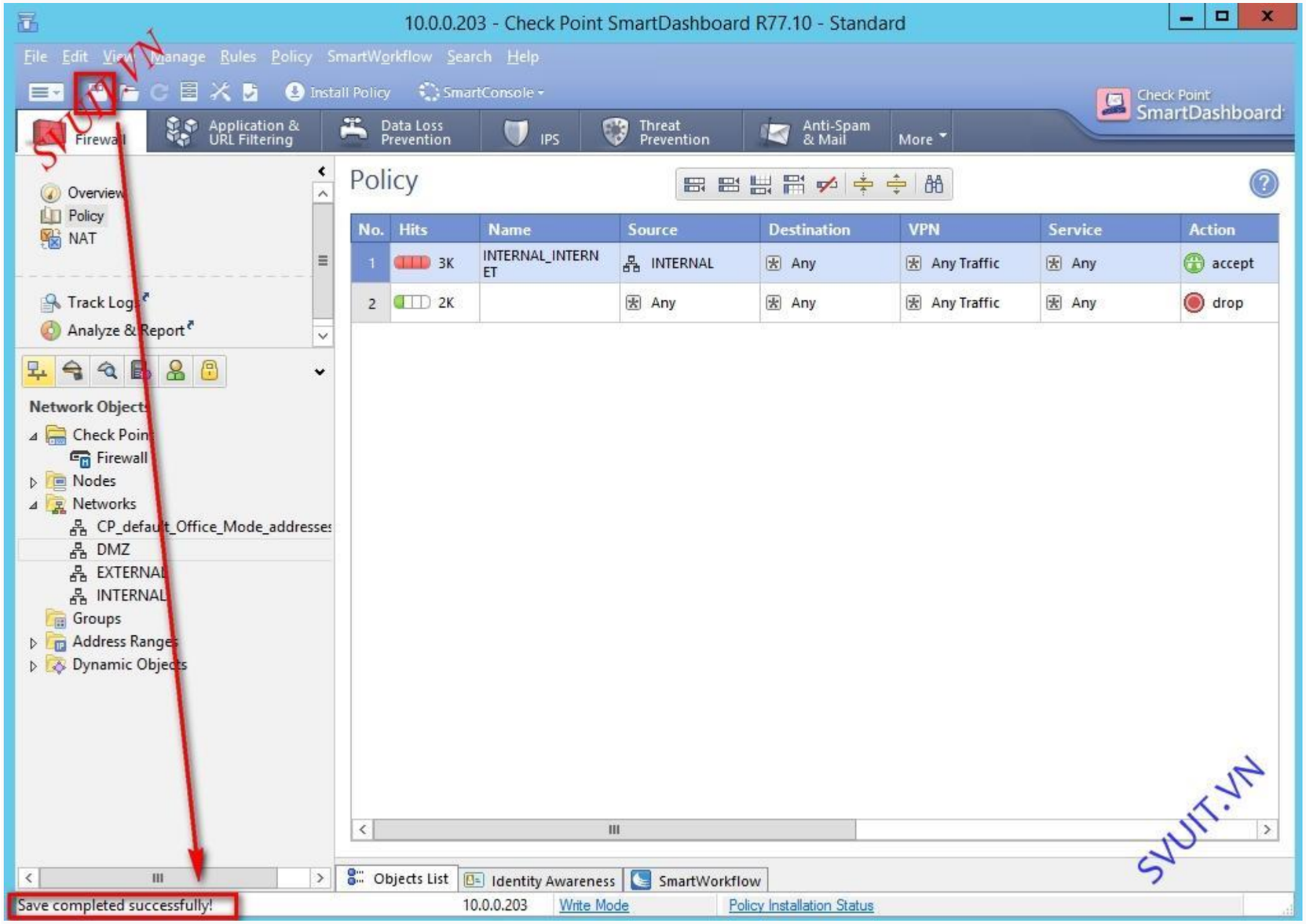
- Source chọn network INTERNAL mà bạn đã tạo, và Destination là any



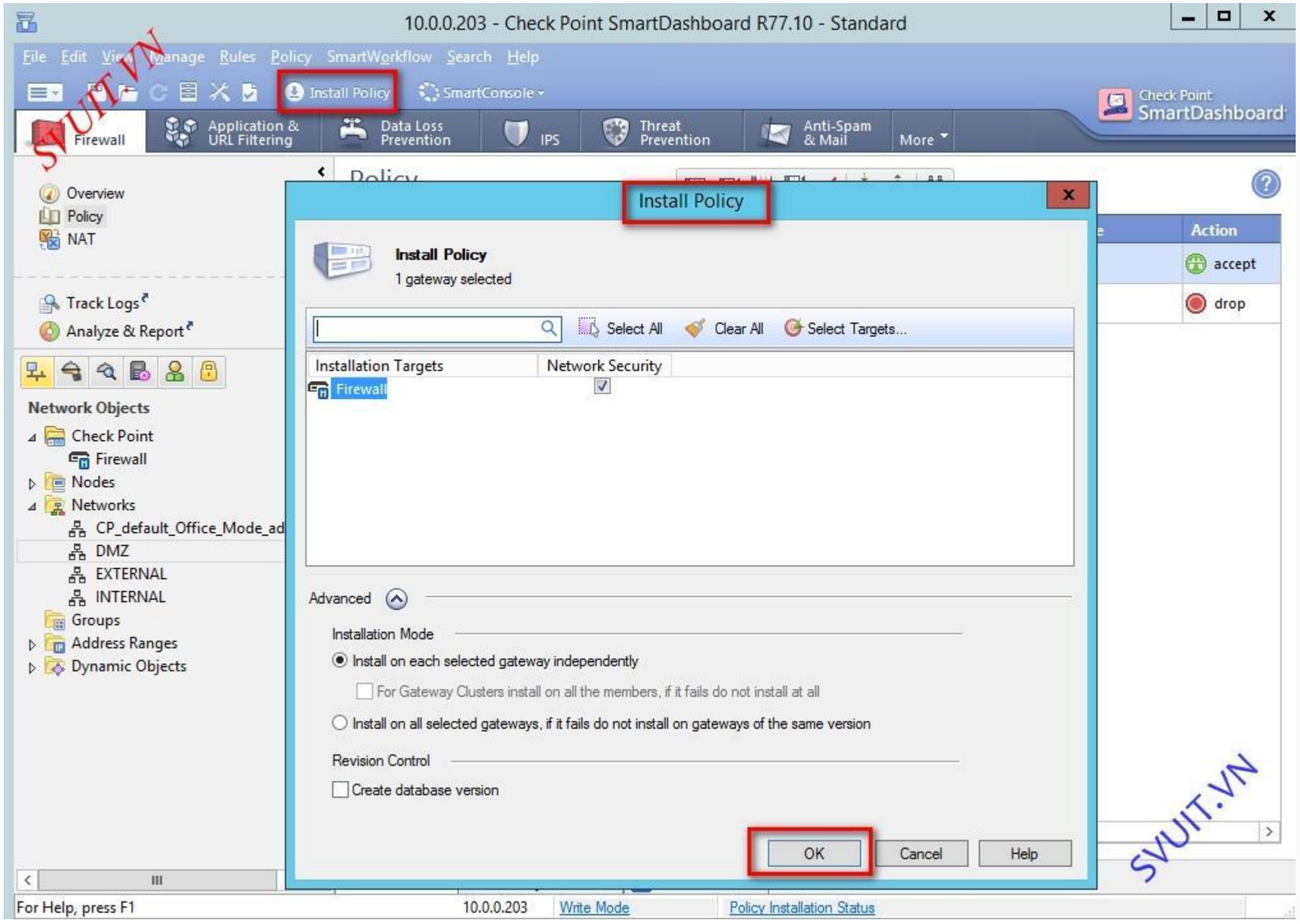
- Chúng ta vừa tạo thành công 1 Rule cho phép INTERNAL truy cập internet

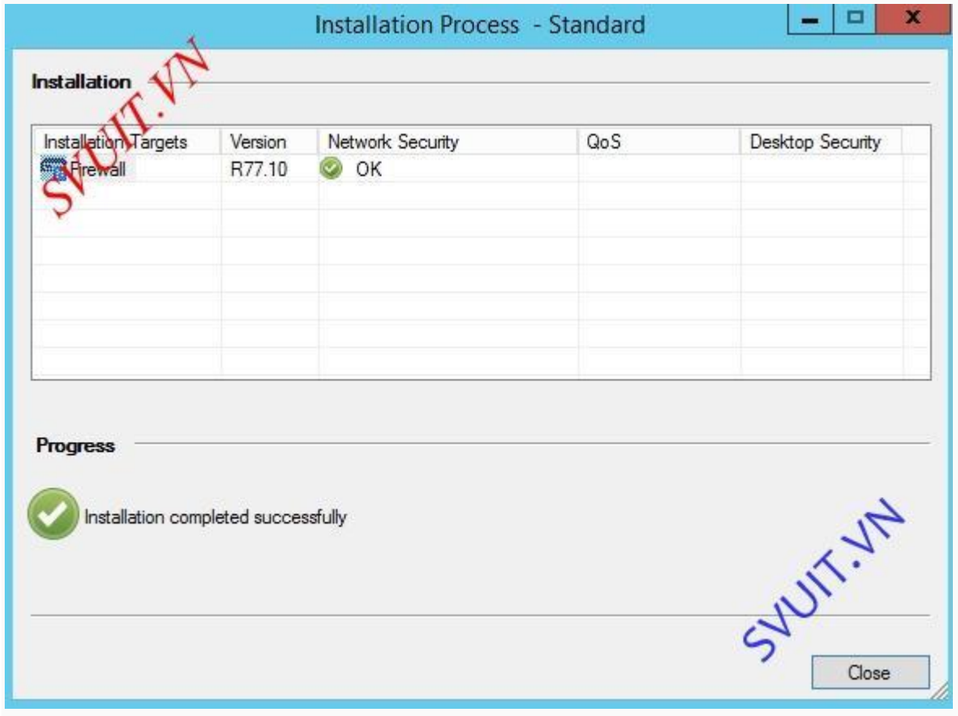


- Sau khi tạo rule xong chúng ta cần save lại rule vừa cấu hình



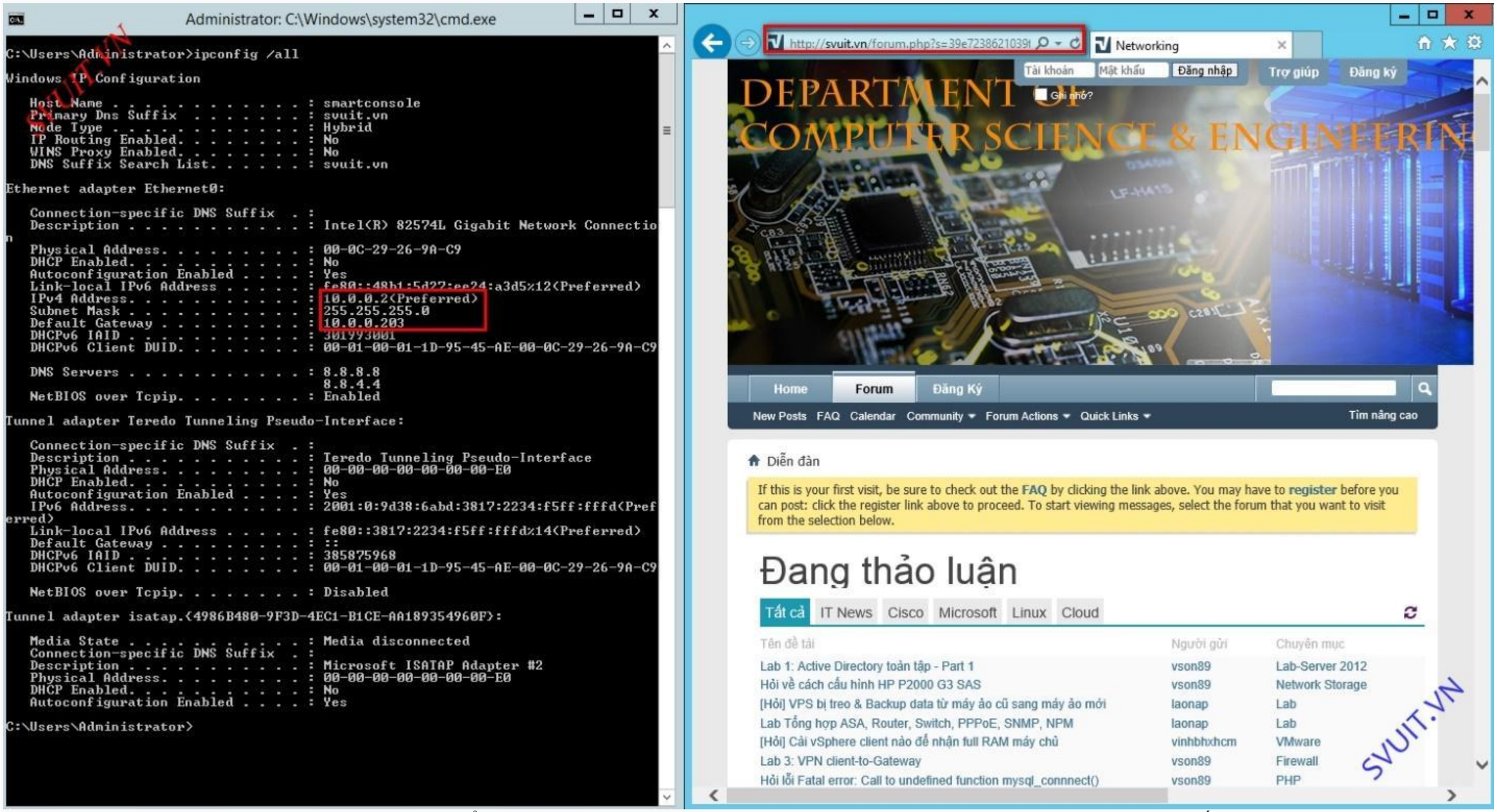
- Và tiến hành install rule đó


10.0.0.203 - Check Point SmartDashboard R77.10 - Standard
File Edit View Manage Rules Policy SmartWorkflow Search Help
Install Policy
SmartConsole
Check Point SmartDashboard
Firewall
Application & URL Filtering
Data Loss Prevention
IPS
Threat Prevention
Anti-Spam & Mail
More
Overview
Policy
NAT
Track Logs
Analyze & Report
Network Objects
Check Point
Firewall
Nodes
Networks
CP_default_Office_Mode_ad
DMZ
EXTERNAL
INTERNAL
Groups
Address Ranges
Dynamic Objects
Action
accept
drop
Install Policy
Install Policy
1 gateway selected
Select All
Clear All
Select Targets...
Installation Targets
Network Security
Firewall
Advanced
Installation Mode
Install on each selected gateway independently
For Gateway Clusters install on all the members, if it fails do not install at all
Install on all selected gateways, if it fails do not install on gateways of the same version
Revision Control
Create database version
OK
Cancel
Help
For Help, press F1
10.0.0.203
Write Mode
Policy Installation Status
SVUIT.VN



III. Kiểm tra

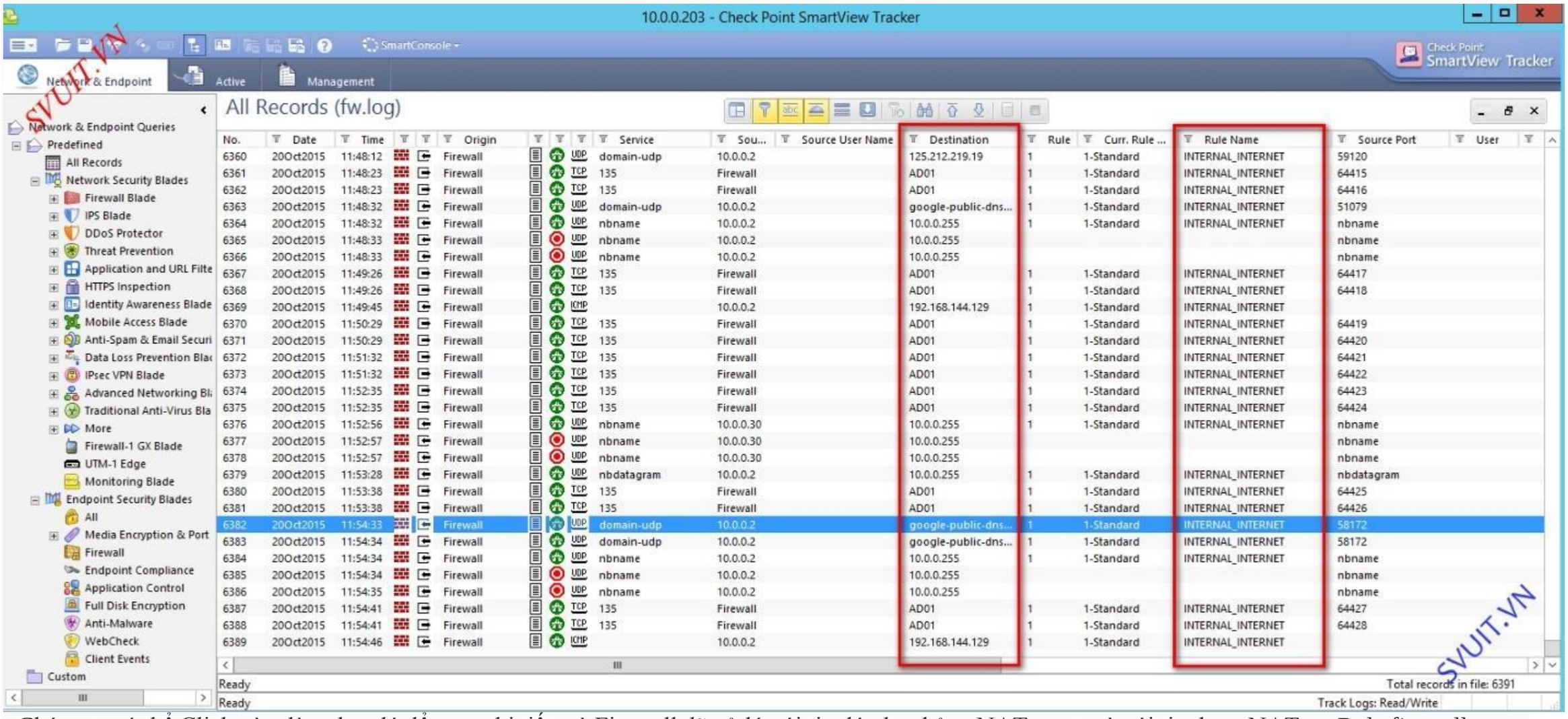
- Bây giờ các bạn vào 1 máy client và truy cập web ra internet thành công vì Firewall đã cho client NAT và rule cho client truy cập ra internet



- Bây giờ trên giao diện SmartConsole các bạn thể xem lại gói tin mà client đã gửi đi ngang qua Firewall. Nó sẽ cho các bạn biết

- Gói tin thuộc giao thức nào

- Port mà firewall mở để gói tin đó đi qua
- Rule mà gói tin đó được apply
- …



- Chúng ta có thể Click vào dòng log đó để xem chi tiết mà Firewall đã xử lý gói tin đó như: bảng NAT, port mà gói tin được NAT ra, Rule firewall apply lên cho client…

Record Details

Previous | Next | Copy Details

Security Gateway/Management

Log Info	
Product	Security Gateway/Management
Date	20Oct2015
Time	11:54:33
Number	6382
Type	Log
Origin	Firewall

Traffic	
Source	10.0.0.2
Destination	google-public-dns-a.google.com (8.8.8.8)
Service	domain-udp (53)
Protocol	udp
Interface	eth2
Source Port	58172

Policy	
Policy Name	Standard
Policy Date	Tue Oct 20 10:25:07 2015
Policy Management	Firewall

Rule	
Action	Accept
Rule	1
Current Rule Number	1-Standard
Rule Name	INTERNAL_INTERNET
User	---

More	
Rule UID	{941779C8-83DB-4471-AF7E-0F4D1B4461A3}
NAT rule number	6
NAT additional rule number	1
XlateSrc	Firewall (172.23.25.243)
XlateSPort	28300
Product Family	Network
Information	service_id: domain-udp