

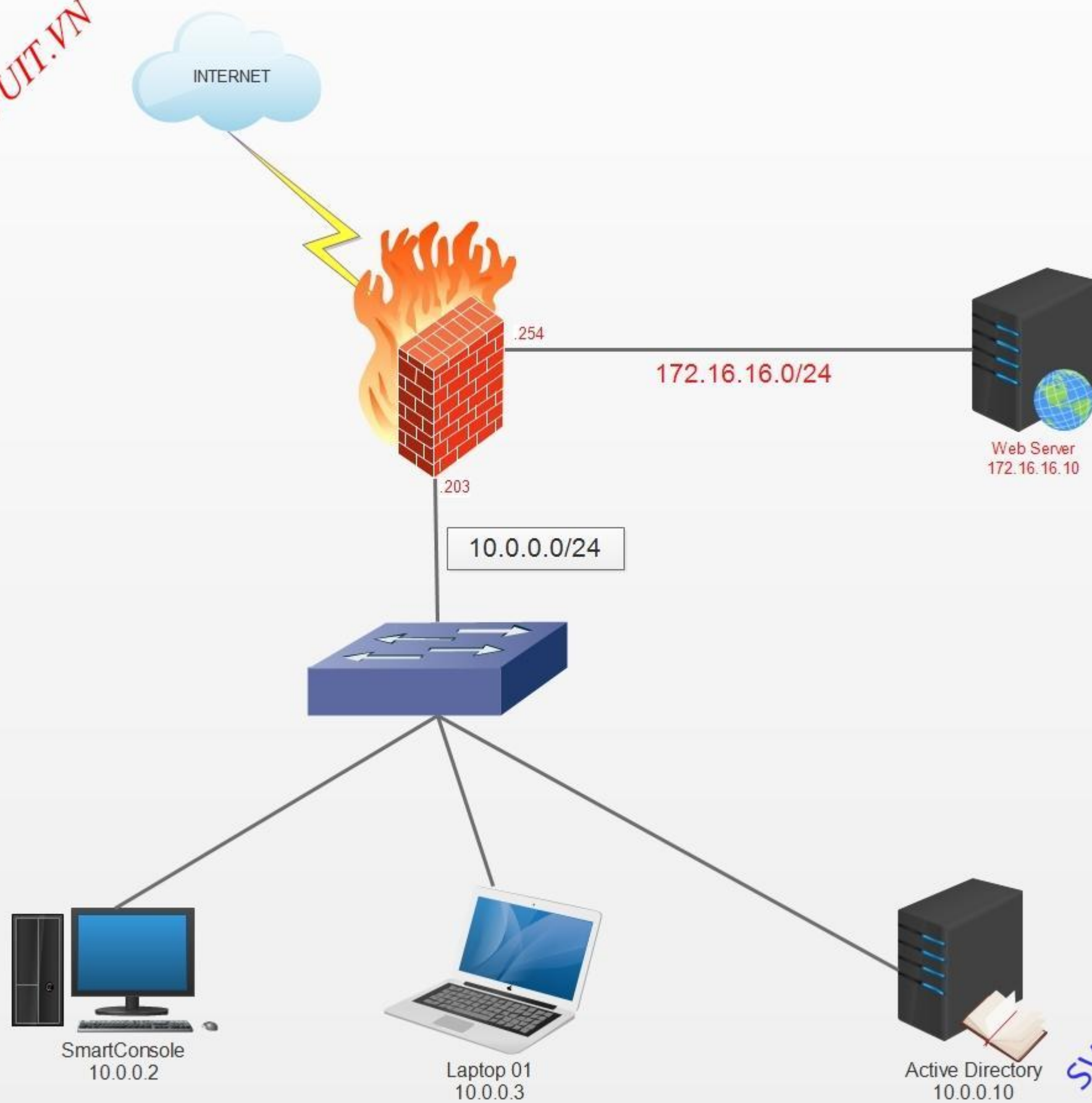
## NAT & Rule Internal truy cập Internet

---

### I. Yêu cầu và chuẩn bị

- Sơ đồ đầu nối thiết bị tron bài lab

SVUIT.VN



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

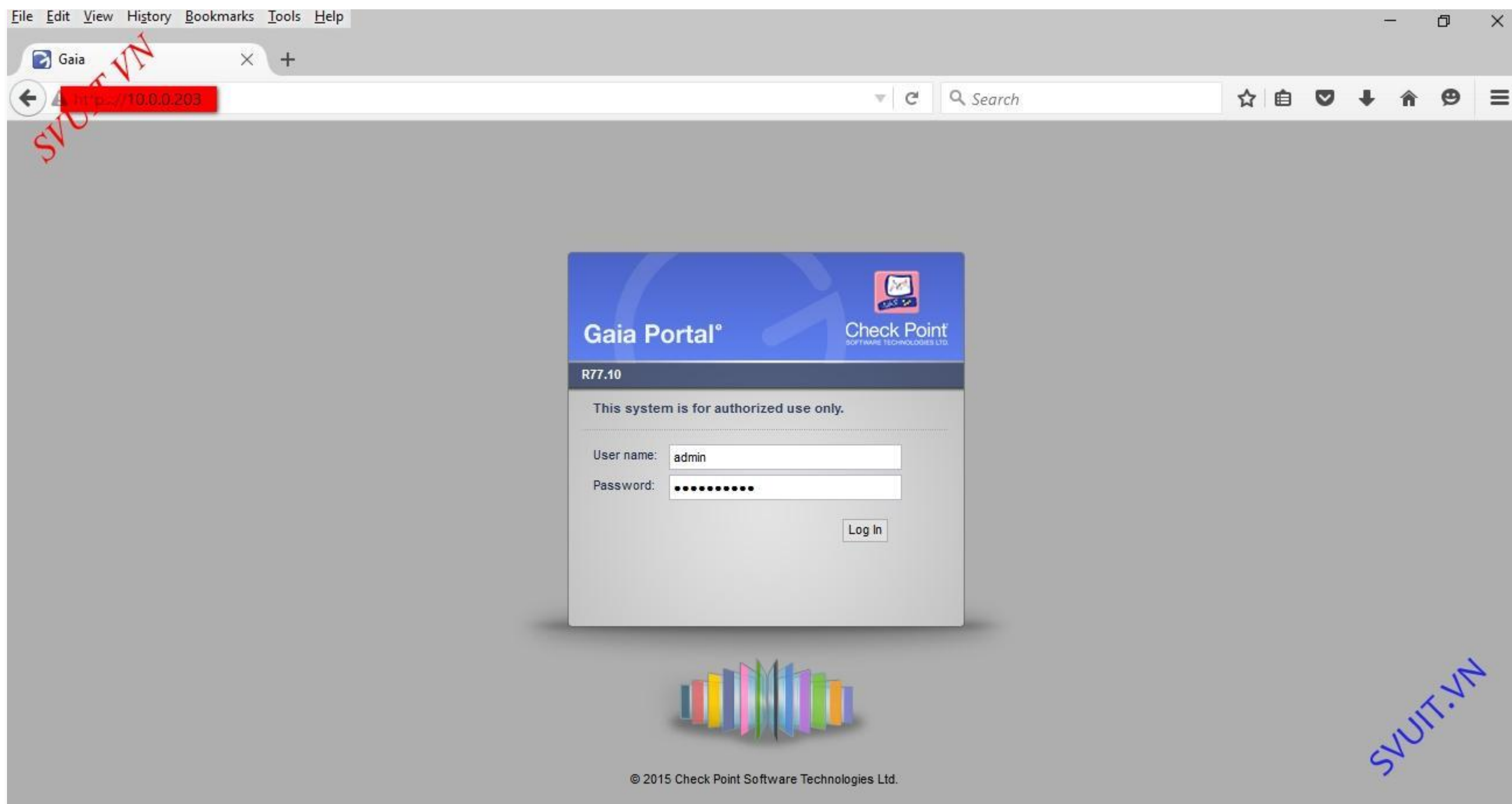
- Yêu cầu:

- 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

VMware Firewall

admin | Sign Out

Check Point® Gaia Portal

Network Management > Network Interfaces

View mode: Advanced

Overview

Network Management

Network Interfaces

ARP

DHCP Server

Hosts and DNS

IPv4 Static Routes

NetFlow Export

System Management

Time

Cloning Group

SNMP

Job Scheduler

Mail Notification

Proxy

Messages

Display Format

Session

Core Dump

Interfaces

Add Edit Delete Refresh

Name	Type	IPv4 Address	Subnet Mask	IPv6 Address	IPv6 Mask Length	Link Status	Comment
eth0	Ethernet	172.23.25.243	255.255.255.0	-	-	Up	External
eth1	Ethernet	172.16.16.254	255.255.255.0	-	-	Up	DMZ
eth2	Ethernet	10.0.0.203	255.255.255.0	-	-	Up	Internal
lo	Loopback	127.0.0.1	255.0.0.0	-	-	Up	

Page 1 of 1

Displaying 1 - 4 of 4

- 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

Gaia

admin Sign Out

Check Point Gaia Portal

Network Management IPv4 Static Routes

View mode: Advanced

Overview

Network Management

- Network Interfaces
- ARP
- DHCP Server
- Hosts and DNS
- IPv4 Static Routes
- NetFlow Export

System Management

- Time
- Cloning Group
- SNMP
- Job Scheduler
- Mail Notification
- Proxy
- Messages
- Display Format
- Session
- Core Dump

IPv4 Static Routes

Add Edit Delete

Destination Address	Next Hop Type	Rank	Local Scope	Gateways	Ping	Comment
Default	Normal	60	N/A	172.23.25.1	No	

Advanced Options

Ping Interval: Default: 10 seconds

Ping Count: Default: 3

Apply

Batch Mode

Add Multiple Static Routes

- 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

The screenshot shows the Check Point SmartDashboard R77.10 interface. The top menu bar includes File, Edit, View, Manage, Rules, Policy, SmartWorkflow, Search, and Help. The left sidebar contains a tree view with categories like Overview, Policy, NAT, Track Logs, and Analyze & Report. Under Network Objects, the 'Networks' folder is expanded, and a context menu is open with options: Network..., Delete, Import..., and More. The main area displays a table titled 'Policy' with the following data:

No.	Hits	Name	Source	Destination	VPN	Service	Action
1	3K	INTERNAL_INTERNET	INTERNAL	Any	Any Traffic	Any	accept
2	2K		Any	Any	Any Traffic	Any	drop

SVUIT.VN

- Khai báo subnet INTERNAL



Network Properties - INTERNAL

General NAT

Name: INTERNAL Color: Black

Comment:

IPv4

Network Address: 10.0.0.0

Net Mask: 255.255.255.0

Broadcast address:

☒ Included

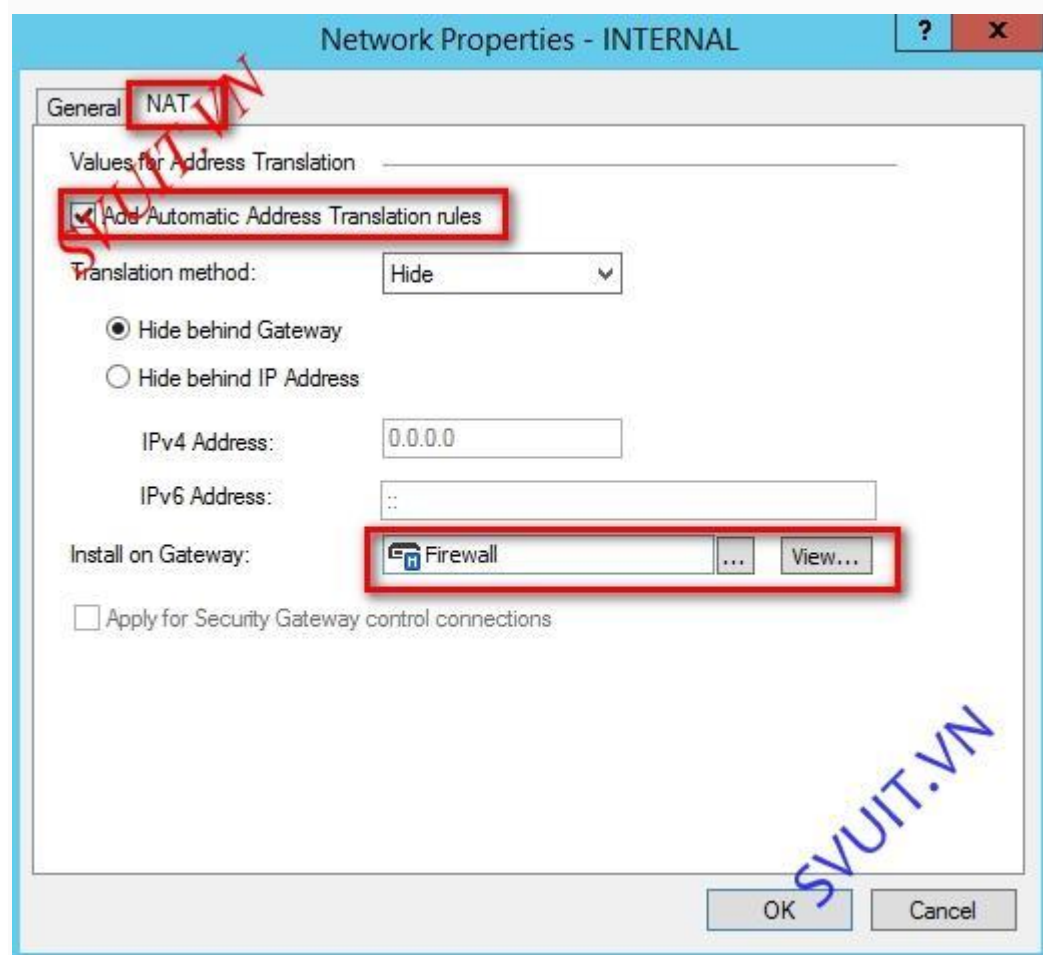
☐ Not included

IPv6

Network Address: /

OK Cancel

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



- Chúng ta cấu hình tương tự cho Network DMZ

Network Properties - DMZ

General NAT

Name:  Color: Black

Comment:

IPv4

Network Address:

Net Mask:

Broadcast address:

☒ Included

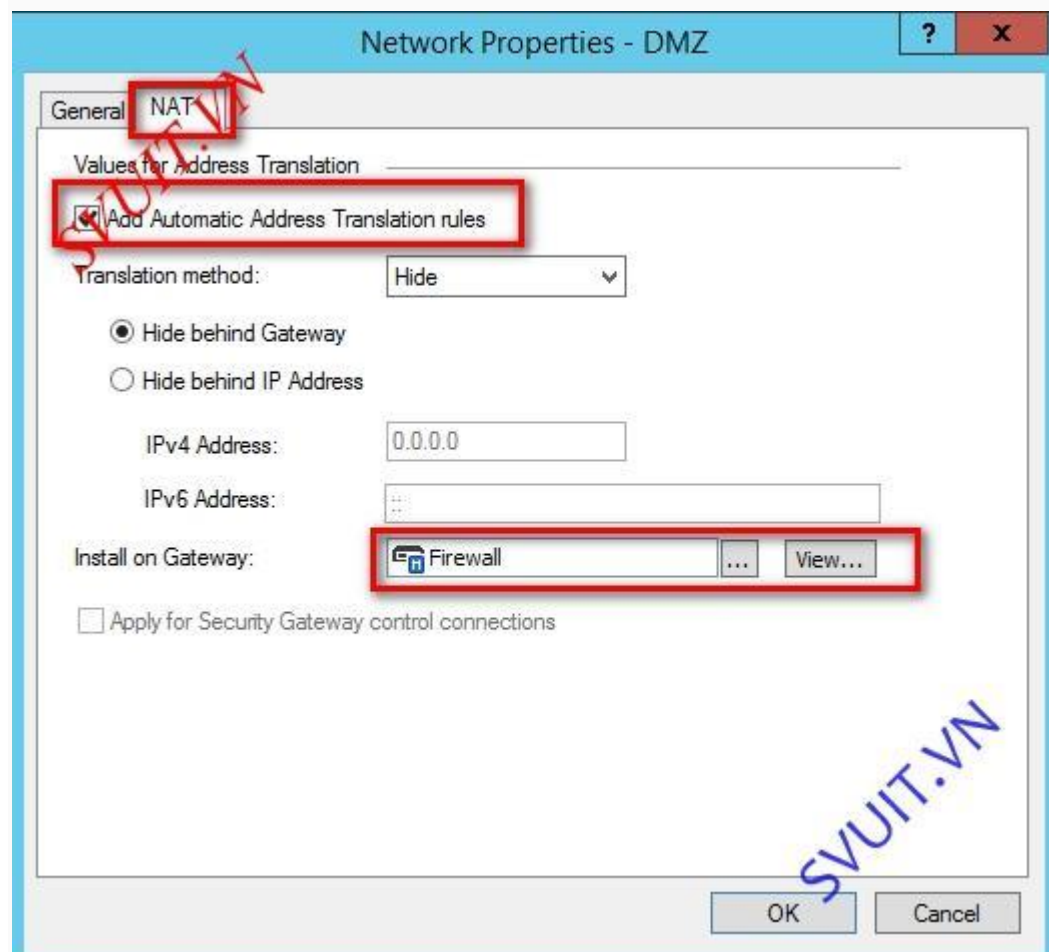
☐ Not included

IPv6

Network Address:  /

OK Cancel

- Và cũng tiến hành NAT vùng DMZ ra internet



- Tạo network cho vùng EXTERNAL

Network Properties - EXTERNAL

General NAT

Name: EXTERNAL Color: Black

Comment:

IPv4

Network Address: 172.23.25.0

Net Mask: 255.255.255.0

Broadcast address:

☒ Included

☐ Not included

IPv6

Network Address: /

OK Cancel

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



10.0.0.203 - Check Point SmartDashboard R77.10 - Standard

File Edit View Manage Rules Policy SmartWorkflow Search Help

Install Policy SmartConsole

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\_addresses
  - DMZ
  - EXTERNAL
  - INTERNAL
- Groups
- Address Ranges
- Dynamic Objects

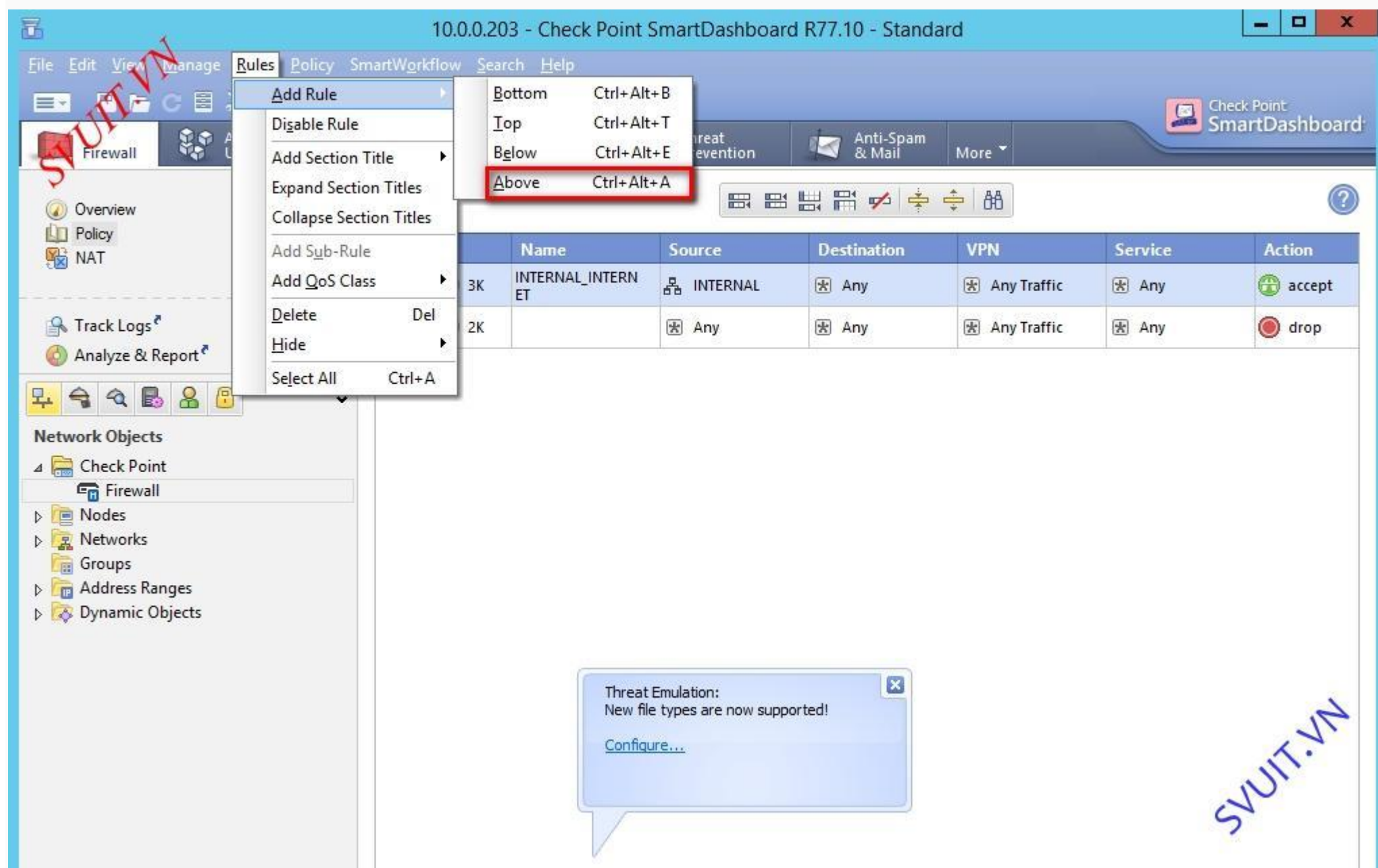
NAT

No.	Original Packet			Translated Packet		
	Source	Destination	Service	Source	Destination	Service
1	CP_default_Office_	CP_default_Off	Any	Original	Original	Original
2	CP_default_Office_	Any	Any	CP_default_Office_	Original	Original
3	DMZ	DMZ	Any	Original	Original	Original
4	DMZ	Any	Any	DMZ (Hiding Addr	Original	Original
5	INTERNAL	INTERNAL	Any	Original	Original	Original
6	INTERNAL	Any	Any	INTERNAL (Hiding /	Original	Original

SVUIT.VN

## 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

10.0.0.203 - Check Point SmartDashboard R77.10 - Standard

File Edit View Manage Rules Policy SmartWorkflow Search Help

Install Policy SmartConsole

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
    - Groups
    - Address Ranges
    - Dynamic Objects

### Policy

No.	Hits	Name	Source	Destination	VPN	Service	Action
1	0		Any	Any	Any Traffic	Any	drop
2	3K	INTERNAL INTERNET		any	Any Traffic	Any	accept
3	2K		Hide Column	any	Any Traffic	Any	drop

SVUIT.VN

- Đặt tên cho Rule mới tạo

SVUIT.VN

Policy

No.	Hits	Name	Source	Destination	VPN	Service	Action
1	0		Any	Any	Any Traffic	Any	drop
2	3K	INTERNAL_INTERNET	INTERNAL	Any	Any Traffic	Any	accept
3	2K		Any	Any	Any Traffic	Any	drop

Rule Name

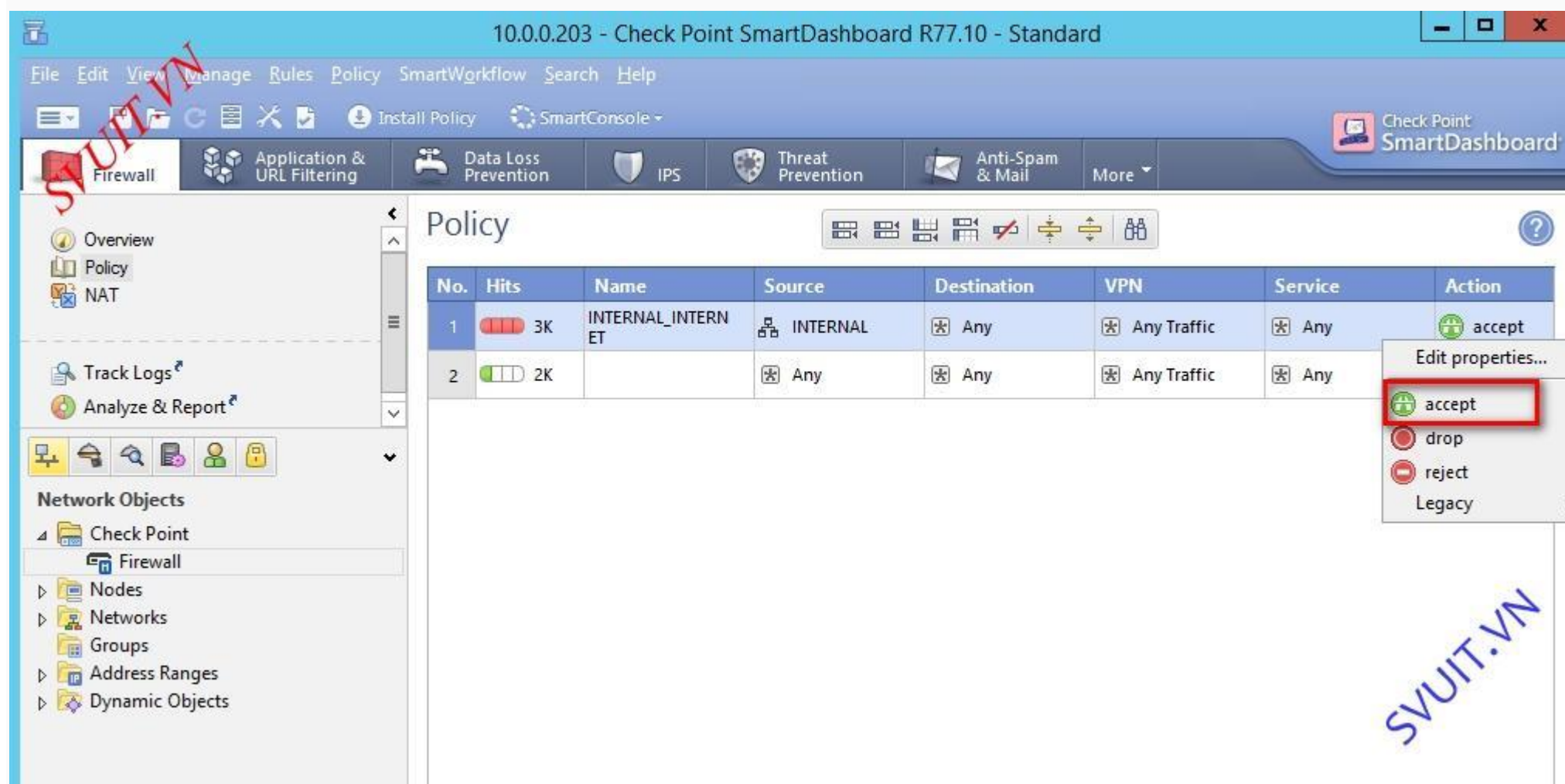
Rule Name: INTERNAL\_INTERNET

OK Cancel Help

SVUIT.VN

- Chuột phải lên vùng Action để chuyển từ trạng thái 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



SVUIT.VN

File Edit View Manage Rules Policy SmartWorkflow Search Help

Install Policy SmartConsole

Firewall Application & URL Filtering Data Loss Prevention IPS Threat Prevention Anti-Spam & Mail More

Check Point SmartDashboard

Overview Policy NAT

Track Logs Analyze & Report

Network Objects

- Check Point
- Firewall
- Nodes
- Networks
  - CP\_default\_Office\_Mode\_addresses
  - DMZ
  - EXTERNAL
  - INTERNAL
- Groups
- Address Ranges
- Dynamic Objects

### Policy

No.	Hits	Name	Source	Destination	VPN	Service	Action
1	3K	INTERNAL_INTERNET	INTERNAL			All	
2	2K		Any				

AD01 10.0.0.10 AD01

All\_Internet 0.0.0.0 - 2... All Internet Addresses

AuxiliaryNet

CP\_default\_Office\_Mode\_a... 172.16.10... Used as a default for Off...

CPDShield DSHIELD IP blocklist

DMZ 172.16.16...

DMZNet

DMZZone

EXTERNAL 172.23.25...

ExternalZone

Firewall 10.0.0.203

InternalNet

InternalZone

LocalMachine Check Point Local Machine...

17 object(s)

New...

SVUIT.VN

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

10.0.0.203 - Check Point SmartDashboard R77.10 - Standard

File Edit View Manage Rules Policy SmartWorkflow Search Help

Install Policy SmartConsole

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
    - Groups
    - Address Ranges
    - Dynamic Objects

### Policy

No.	Hits	Name	Source	Destination	VPN	Service	Action
1	3K	INTERNAL_INTERNET	INTERNAL	Any	Any Traffic	Any	accept
2	2K		Any	Any	Any Traffic	Any	drop

SVUIT.VN

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

10.0.0.203 - Check Point SmartDashboard R77.10 - Standard

File Edit View Manage Rules Policy SmartWorkflow Search Help

Install Policy SmartConsole

Firewall Application & URL Filtering Data Loss Prevention IPS Threat Prevention Anti-Spam & Mail More

Overview Policy NAT

Track Log Analyze & Report

Network Objects

- Check Point
- Firewall
- Nodes
- Networks
  - CP\_default\_Office\_Mode\_addresses
  - DMZ
  - EXTERNAL
  - INTERNAL
- Groups
- Address Ranges
- Dynamic Objects

### Policy

No.	Hits	Name	Source	Destination	VPN	Service	Action
1	3K	INTERNAL_INTERN ET	INTERNAL	Any	Any Traffic	Any	accept
2	2K		Any	Any	Any Traffic	Any	drop

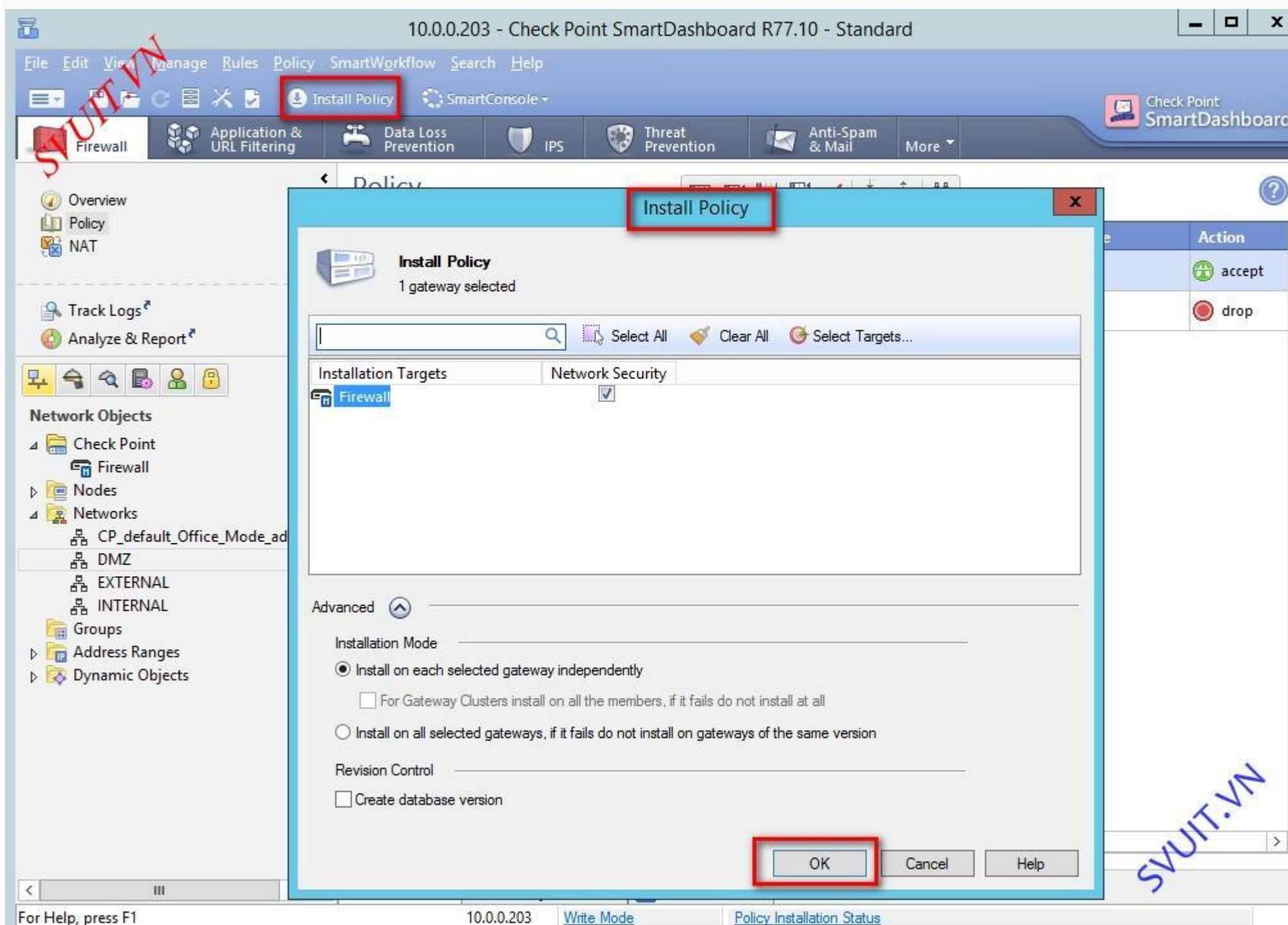
Save completed successfully!

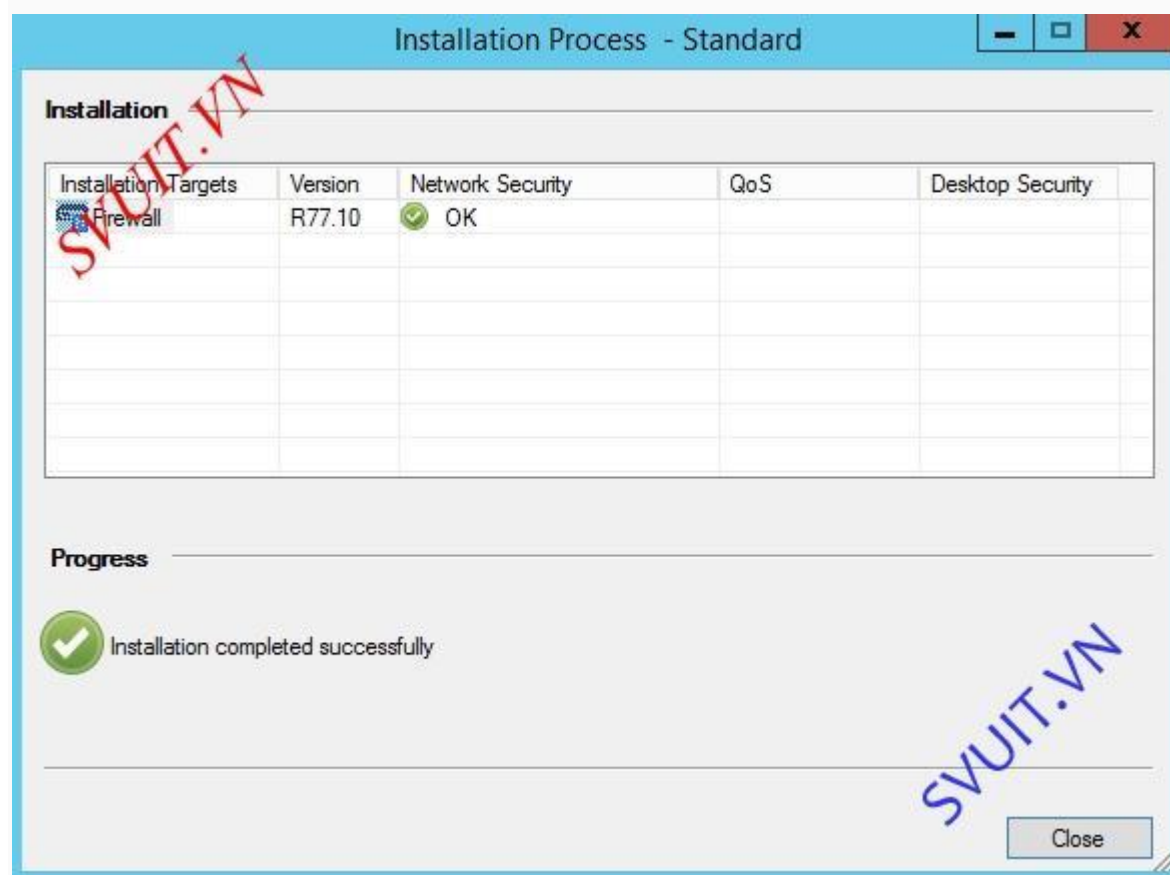
10.0.0.203 Write Mode Policy Installation Status

SVUIT.VN

- Và tiến hành install rule đó







### 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



```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : smartconsole
Primary Dns Suffix . . . . . : svuit.vn
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : svuit.vn

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-26-9A-C9
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::48b1:5d22:ee24:a3d5%12(Preferred)
IPv4 Address. . . . . : 10.0.0.2(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.0.203
DHCPv6 IAID . . . . . : 301793001
DHCPv6 Client DUID. . . . . : 00-01-00-01-1D-95-45-AE-00-0C-29-26-9A-C9

DNS Servers . . . . . : 8.8.8.8
                        8.8.4.4
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter Teredo Tunneling Pseudo-Interface:

Connection-specific DNS Suffix . : 
Description . . . . . : Teredo Tunneling Pseudo-Interface
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:0:9d38:6abd:3817:2234:f5ff:fffd(Pref
erred)
Link-local IPv6 Address . . . . . : fe80::3817:2234:f5ff:fffd%14(Preferred)
Default Gateway . . . . . : 
DHCPv6 IAID . . . . . : 385875968
DHCPv6 Client DUID. . . . . : 00-01-00-01-1D-95-45-AE-00-0C-29-26-9A-C9

NetBIOS over Tcpip. . . . . : Disabled

Tunnel adapter isatap.{4986B480-9F3D-4EC1-B1CE-AA189354960F}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Microsoft ISATAP Adapter #2
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

C:\Users\Administrator>
```



- 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
- ...

10.0.0.203 - Check Point SmartView Tracker

Network & Endpoint Active Management

Network & Endpoint Queries

Predefined

- All Records
- Network Security Blades
  - Firewall Blade
  - IPS Blade
  - DDoS Protector
  - Threat Prevention
  - Application and URL Filter
  - HTTPS Inspection
  - Identity Awareness Blade
  - Mobile Access Blade
  - Anti-Spam & Email Security
  - Data Loss Prevention Blade
  - IPsec VPN Blade
  - Advanced Networking Blade
  - Traditional Anti-Virus Blade
  - More
- Firewall-1 GX Blade
- UTM-1 Edge
- Monitoring Blade
- Endpoint Security Blades
  - All
  - Media Encryption & Port
  - Firewall
  - Endpoint Compliance
  - Application Control
  - Full Disk Encryption
  - Anti-Malware
  - WebCheck
  - Client Events
- Custom

All Records (fw.log)

No.	Date	Time	Origin	Service	Source User Name	Destination	Rule	Curr. Rule ...	Rule Name	Source Port	User
6360	20Oct2015	11:48:12	Firewall	UDP	domain-udp	10.0.0.2	125.212.219.19	1	1-Standard	INTERNAL_INTERNET	59120
6361	20Oct2015	11:48:23	Firewall	TCP	135	Firewall	AD01	1	1-Standard	INTERNAL_INTERNET	64415
6362	20Oct2015	11:48:23	Firewall	TCP	135	Firewall	AD01	1	1-Standard	INTERNAL_INTERNET	64416
6363	20Oct2015	11:48:32	Firewall	UDP	domain-udp	10.0.0.2	google-public-dns...	1	1-Standard	INTERNAL_INTERNET	51079
6364	20Oct2015	11:48:32	Firewall	UDP	nbname	10.0.0.2	10.0.0.255	1	1-Standard	INTERNAL_INTERNET	nbname
6365	20Oct2015	11:48:33	Firewall	UDP	nbname	10.0.0.2	10.0.0.255			INTERNAL_INTERNET	nbname
6366	20Oct2015	11:48:33	Firewall	UDP	nbname	10.0.0.2	10.0.0.255			INTERNAL_INTERNET	nbname
6367	20Oct2015	11:49:26	Firewall	TCP	135	Firewall	AD01	1	1-Standard	INTERNAL_INTERNET	64417
6368	20Oct2015	11:49:26	Firewall	TCP	135	Firewall	AD01	1	1-Standard	INTERNAL_INTERNET	64418
6369	20Oct2015	11:49:45	Firewall	ICMP		10.0.0.2	192.168.144.129	1	1-Standard	INTERNAL_INTERNET	
6370	20Oct2015	11:50:29	Firewall	TCP	135	Firewall	AD01	1	1-Standard	INTERNAL_INTERNET	64419
6371	20Oct2015	11:50:29	Firewall	TCP	135	Firewall	AD01	1	1-Standard	INTERNAL_INTERNET	64420
6372	20Oct2015	11:51:32	Firewall	TCP	135	Firewall	AD01	1	1-Standard	INTERNAL_INTERNET	64421
6373	20Oct2015	11:51:32	Firewall	TCP	135	Firewall	AD01	1	1-Standard	INTERNAL_INTERNET	64422
6374	20Oct2015	11:52:35	Firewall	TCP	135	Firewall	AD01	1	1-Standard	INTERNAL_INTERNET	64423
6375	20Oct2015	11:52:35	Firewall	TCP	135	Firewall	AD01	1	1-Standard	INTERNAL_INTERNET	64424
6376	20Oct2015	11:52:56	Firewall	UDP	nbname	10.0.0.30	10.0.0.255	1	1-Standard	INTERNAL_INTERNET	nbname
6377	20Oct2015	11:52:57	Firewall	UDP	nbname	10.0.0.30	10.0.0.255			INTERNAL_INTERNET	nbname
6378	20Oct2015	11:52:57	Firewall	UDP	nbname	10.0.0.30	10.0.0.255			INTERNAL_INTERNET	nbname
6379	20Oct2015	11:53:28	Firewall	UDP	nbdatalogram	10.0.0.2	10.0.0.255	1	1-Standard	INTERNAL_INTERNET	nbdatalogram
6380	20Oct2015	11:53:38	Firewall	TCP	135	Firewall	AD01	1	1-Standard	INTERNAL_INTERNET	64425
6381	20Oct2015	11:53:38	Firewall	TCP	135	Firewall	AD01	1	1-Standard	INTERNAL_INTERNET	64426
6382	20Oct2015	11:54:33	Firewall	UDP	domain-udp	10.0.0.2	google-public-dns...	1	1-Standard	INTERNAL_INTERNET	58172
6383	20Oct2015	11:54:34	Firewall	UDP	domain-udp	10.0.0.2	google-public-dns...	1	1-Standard	INTERNAL_INTERNET	58172
6384	20Oct2015	11:54:34	Firewall	UDP	nbname	10.0.0.2	10.0.0.255	1	1-Standard	INTERNAL_INTERNET	nbname
6385	20Oct2015	11:54:34	Firewall	UDP	nbname	10.0.0.2	10.0.0.255			INTERNAL_INTERNET	nbname
6386	20Oct2015	11:54:35	Firewall	UDP	nbname	10.0.0.2	10.0.0.255			INTERNAL_INTERNET	nbname
6387	20Oct2015	11:54:41	Firewall	TCP	135	Firewall	AD01	1	1-Standard	INTERNAL_INTERNET	64427
6388	20Oct2015	11:54:41	Firewall	TCP	135	Firewall	AD01	1	1-Standard	INTERNAL_INTERNET	64428
6389	20Oct2015	11:54:46	Firewall	ICMP		10.0.0.2	192.168.144.129	1	1-Standard	INTERNAL_INTERNET	

Ready

Ready

Total records in file: 6391

Track Logs: Read/Write

- 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