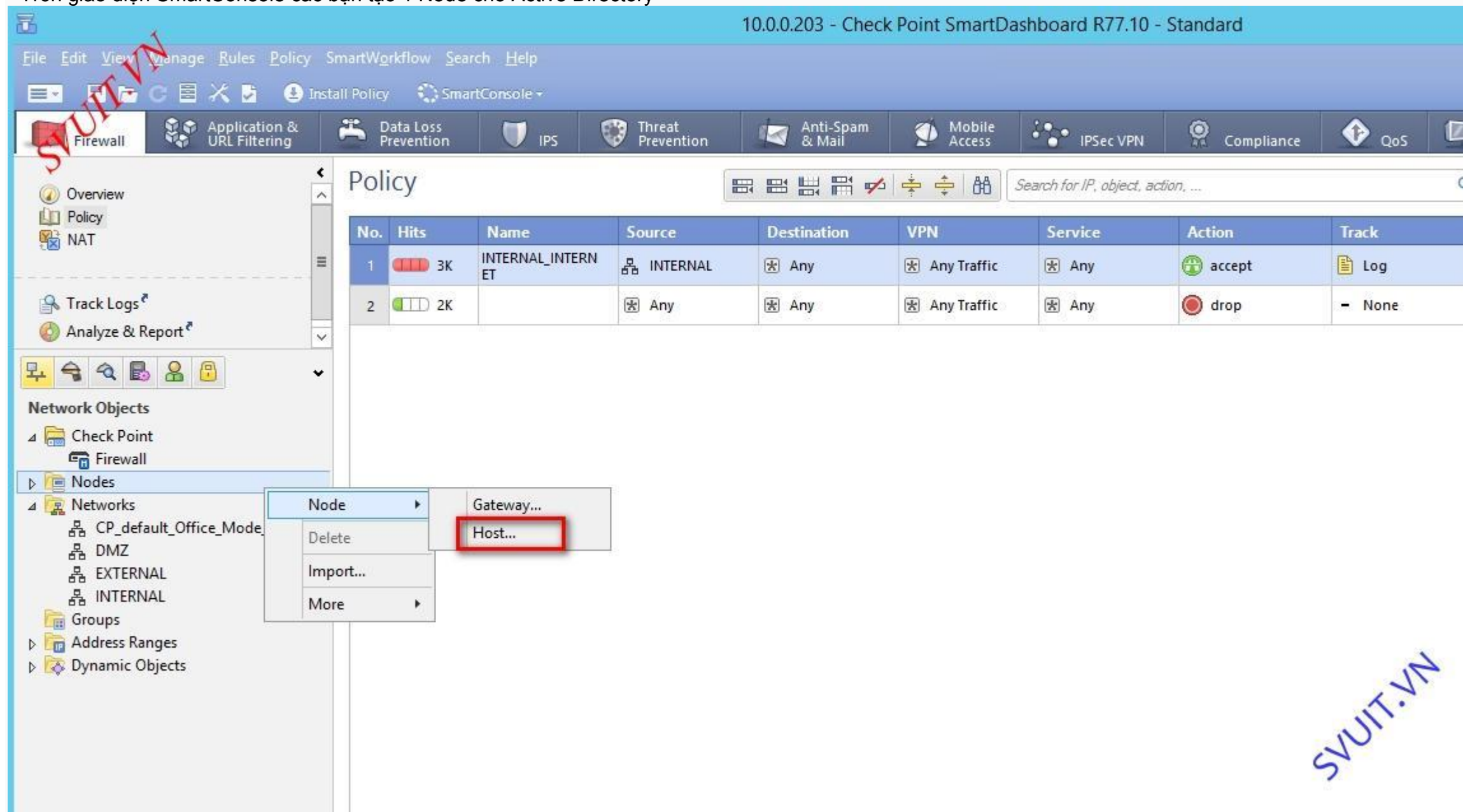


Tích hợp Active Directory 2012R2 với Checkpoint

Tích hợp Active Directory trên windows server 2012R2 với Firewall Checkpoint

- Các bạn tham khảo lại bài viết trước của mình nhé: <http://svuit.vn/checkpoint-122/lab-0...rnet-1019.html>
mình sẽ lấy sơ đồ và mô hình IP của bài trước để làm luôn cho bài viết này

- Trên giao diện SmartConsole các bạn tạo 1 Node cho Active Directory



- Khai báo thông tin name và IP của Active Directory

Host Node - AD01

General Properties
Topology
NAT
Other

Host Node - General Properties

Machine

Name: Color:

IPv4 Address:

IPv6 Address:

Comment:

Products:

OK Cancel

- Qua tab server và tiến hành add LDAP server mà bạn muốn tích hợp

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 Mobile Access IPSec VPN Compliance

Overview Policy NAT Track Logs Analyze & Report

Servers and OPSEC

Servers OPSEC Applications

New Expand Sort

- RADIUS...
- RADIUS Group...
- TACACS...
- LDAP Account Unit...
- CA
- SecuRemote DNS...
- SecurID...
- IF-MAP...

Policy

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

SVUIT.VN

- Điền các thông tin như Profiles, Domain Name... như sau

LDAP Account Unit Properties - SVUIT

General Servers Objects Management Authentication

Name: SVUIT

Comment:

Color: Olive

Profile: Microsoft_AD

Domain: svuit.vn

Account Unit usage

☐ CRL retrieval

☒ User management

☒ Active Directory Query

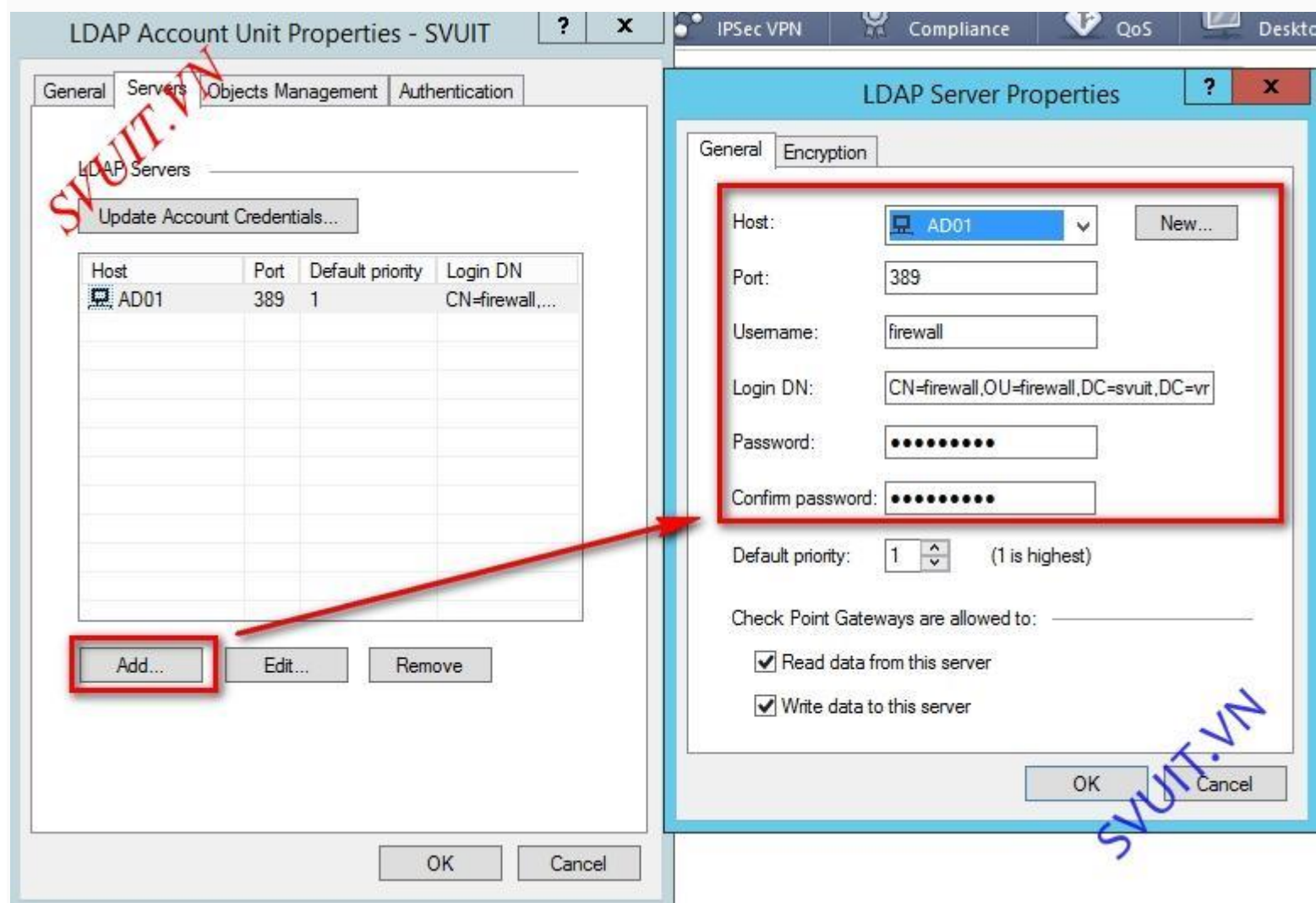
Additional configuration

☒ Enable Unicode support

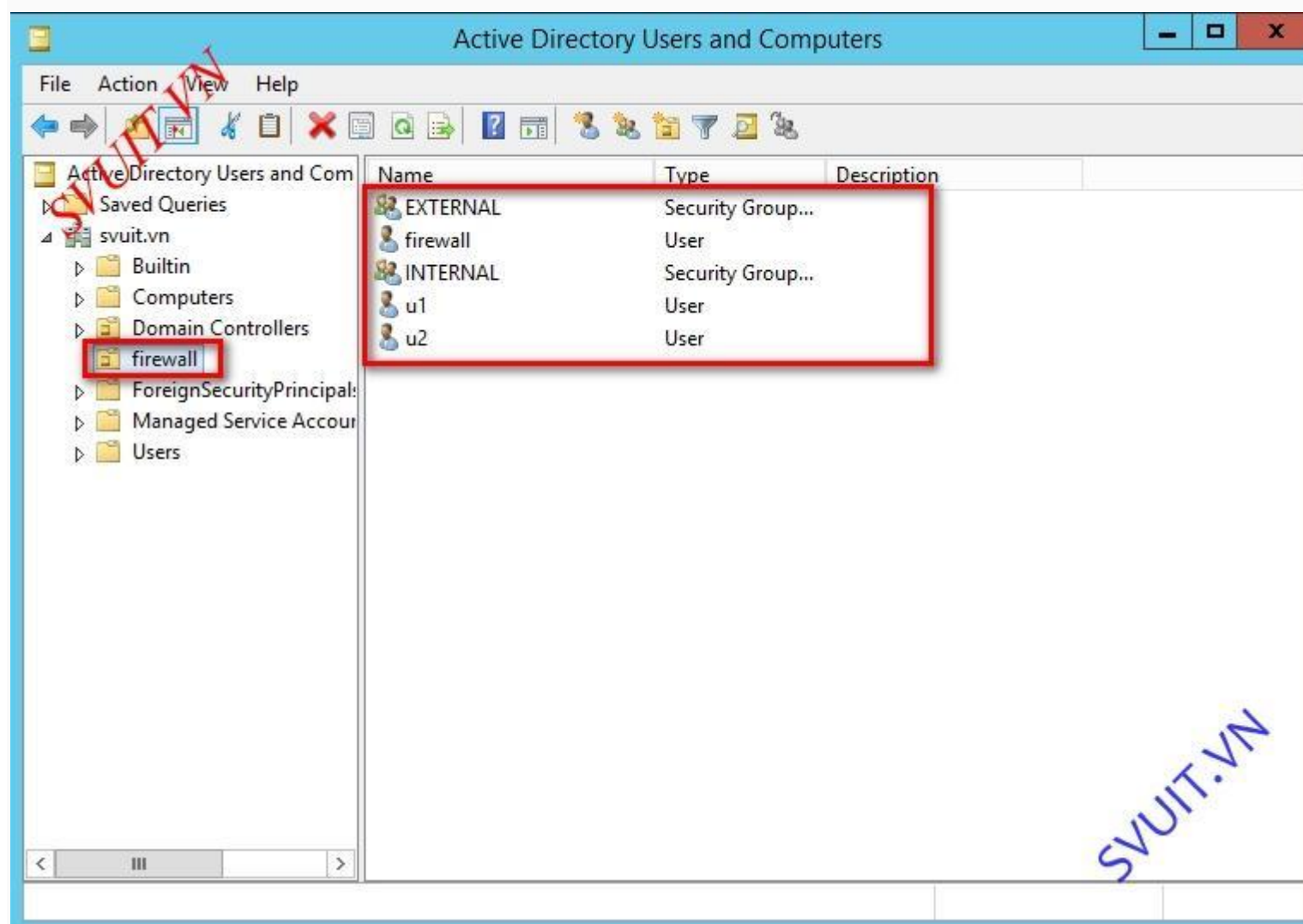
Active Directory SSO configuration

OK Cancel

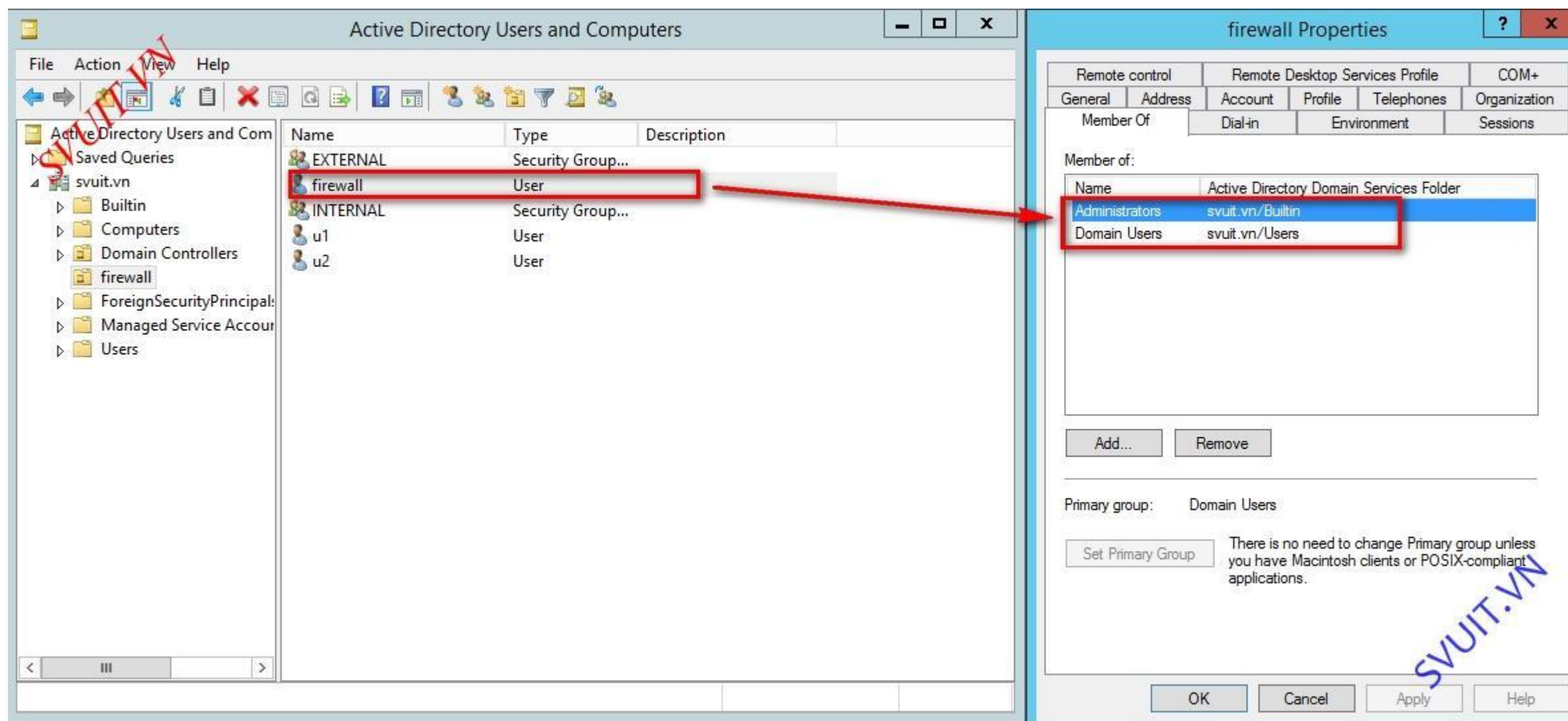
- Điền username và password của user trên AD có quyền cho phép Firewall Checkpoint query user trên AD được



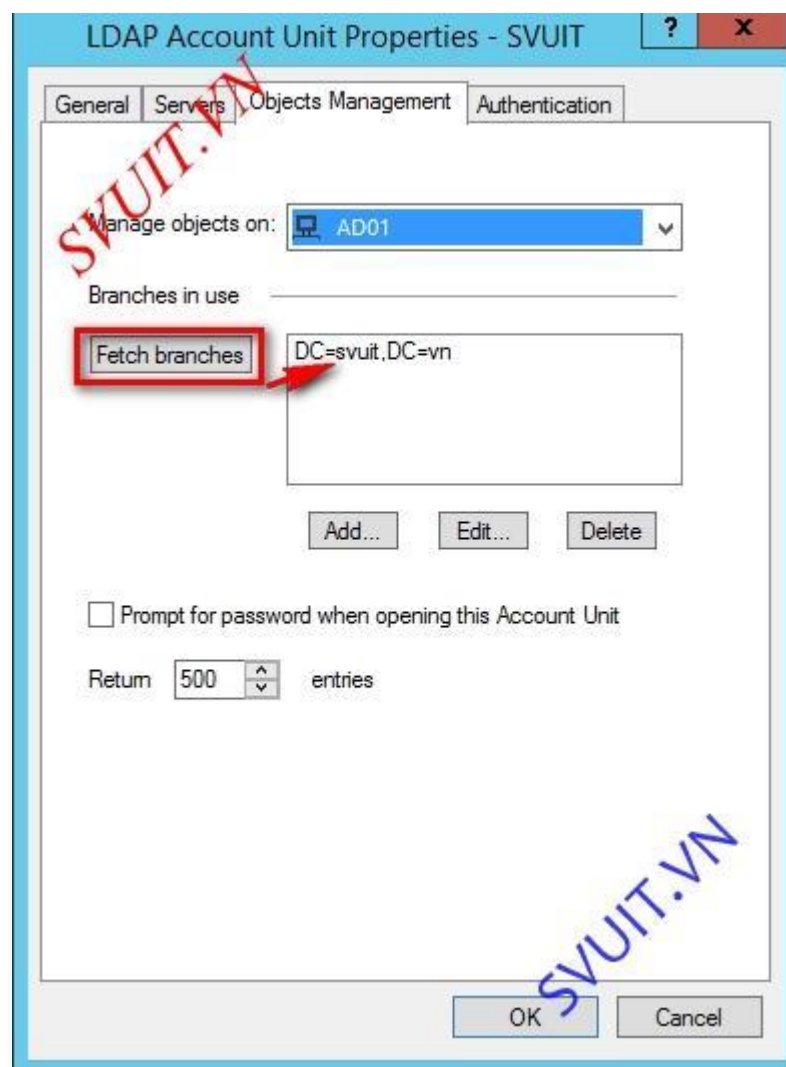
- Trên Active Directory 2012 R2 các bạn cần khai báo OU, Group, User... sử dụng cho Firewall



- Các bạn add user “firewall” trên AD vào group Administrator để có quyền thực hiện Query trên AD



- Tiếp theo quay trở lại giao diện SmartConsole của Checkpoint các bạn nhận “Fetch branches” để nó ra thông tin bên khung bên phải thì các bạn đã cấu hình đúng



- Tab cuối cùng mô tả các cơ chế xác thực

LDAP Account Unit Properties - SVUIT

General Servers Objects Management Authentication

☐ Use common group path for queries

Allowed authentication schemes

☒ Check Point Password ☒ OS Password

☒ SecurID ☒ TACACS

☒ RADIUS

Users' default values

☐ Use user template:

☐ Default authentication scheme:

Login restrictions

☐ Limit login failures

Lock user's account after login failures.

Unlock user's account after seconds.

Encryption

IKE pre-shared secret encryption key:

OK Cancel

- Bây giờ bạn qua tab “Users” trên giao diện Smartconsole của Firewall các bạn có thể tiến hành query user trên Active Directory

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 Mobile Access IPsec VPN Compliance QoS Desktop

Overview Policy NAT

Track Logs Analyze & Report

Users and Administrators

- Access Roles
- Administrator Groups
- Administrators
 - cpconfig_administrators
- External User Profiles
- LDAP Groups
- Templates
- User Groups
- Users
- SVUIT
 - vn
 - svuit
 - Computers
 - ForeignSecurityPrincipals
 - Managed Service Accounts
 - Program Data
 - System
 - Users
 - Domain Controllers
 - firewall

Policy

Search for IP, object, action, ... Query Syntax

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time	Com
1	3K	INTERNAL_INTERN ET	INTERNAL	Any	Any Traffic	Any	accept	Log	Policy Targets	Any	
2	2K		Any	Any	Any Traffic	Any	drop	None	Policy Targets	Any	

Objects List Identity Awareness SmartWorkflow

Search is Unavailable Users and Administrators SVUIT\vn\svuit Action...

Full Name	Login Name	DN (Distinguished Name)
INTERNAL		CN=INTERNAL,OU=firewall,DC=svuit,DC=vn
EXTERNAL		CN=EXTERNAL,OU=firewall,DC=svuit,DC=vn
u1	u1	CN=u1,OU=firewall,DC=svuit,DC=vn
u2	u2	CN=u2,OU=firewall,DC=svuit,DC=vn
firewall	firewall	CN=firewall,OU=firewall,DC=svuit,DC=vn

Total 0 items in list

10.0.0.203 Write Mode Policy Installation Status

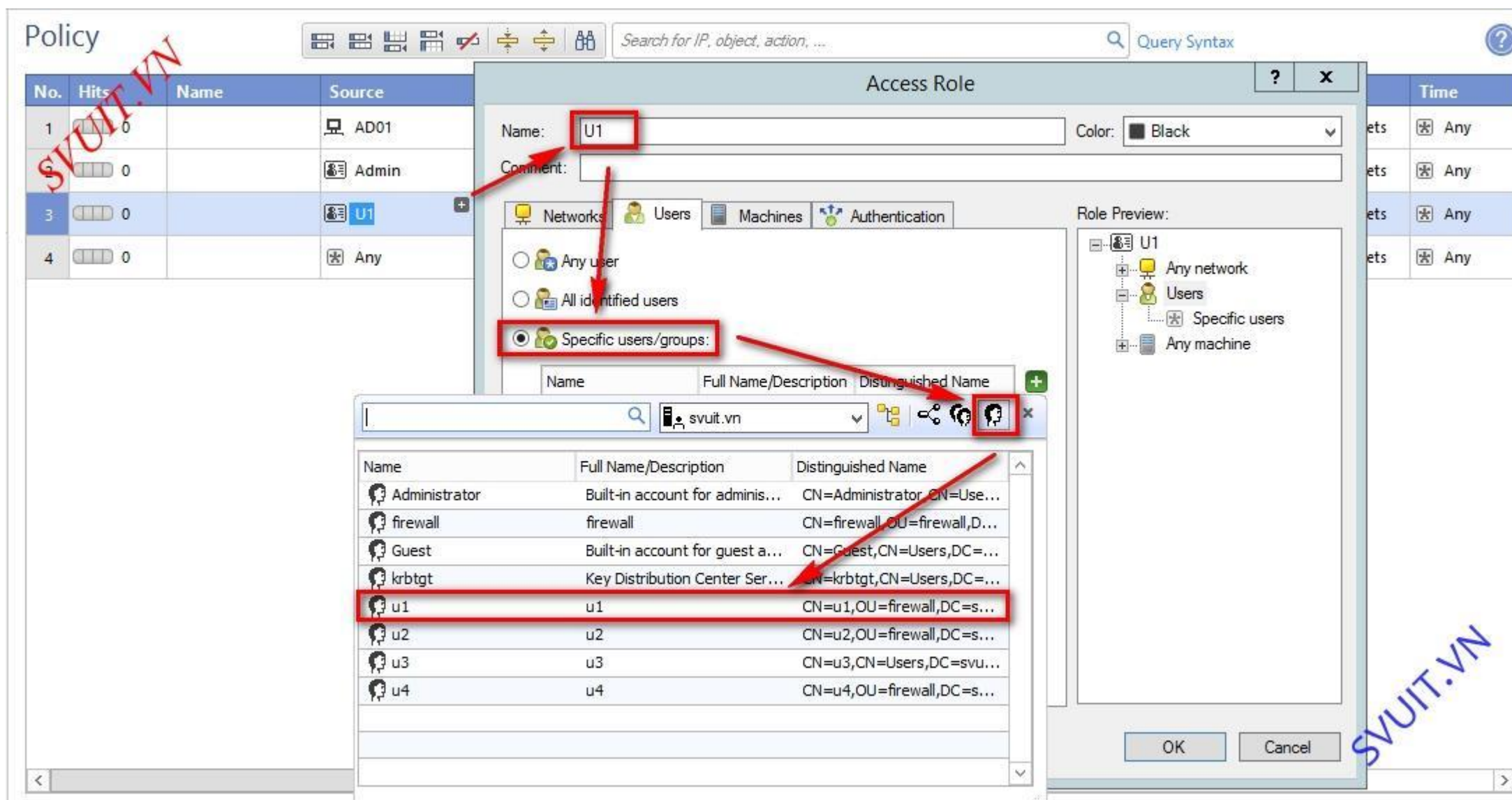
Tiến hành tạo các Rule với mục đích như sau:

- Rule 1:** Cho phép máy Active Directory được đi ra internet (mục đích là mở port DNS cho phép AD phân giải Domain của client truy cập ra internet)
- Rule 2:** Cho phép user "administrator" trong domain svuit.vn được đi internet
- Rule 3:** Cấm user "u1" đi internet
- Rule 4:** Cấm toàn bộ traffic khi gói tin không thỏa các Rule ở trên

The screenshot shows the Check Point SmartDashboard interface. The top navigation bar includes various security modules like Firewall, Application & URL Filtering, Data Loss Prevention, IPS, Threat Prevention, Anti-Spam & Mail, Mobile Access, IPSec VPN, and Compliance. The left sidebar contains navigation options: Overview, Policy (highlighted with a red box and arrow), NAT, Track Logs, and Analyze & Report. Below these are Network Objects (Check Point, Firewall, Nodes, Networks, Groups, Address Ranges, Dynamic Objects). The main area displays the 'Policy' configuration table.

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time
1	0		AD01	Any	Any Traffic	Any	accept	Log	Policy Targets	Any
2	0		Admin	Any	Any Traffic	Any	accept	Log	Policy Targets	Any
3	0		U1	Any	Any Traffic	Any	drop	Log	Policy Targets	Any
4	0		Any	Any	Any Traffic	Any	drop	Log	Policy Targets	Any

- **Rule 3:** Tạo rule số 3 để cấm user u1 truy cập ra bên ngoài.
 - Source của Rule 3 thực hiện chọn user “u1” của domain svuit.vn



- **Action:** drop. Gởi tin khi thỏa điều kiện
- **Track:** log. Có lưu log lại khi firewall xử lý gói tin thuộc rule này

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time
1	0		AD01	Any	Any Traffic	Any	accept	Log	Policy Targets	Any
2	0		Admin	Any	Any Traffic	Any	accept	Log	Policy Targets	Any
3	0		U1	Any	Any Traffic	Any	drop	Log	Policy Targets	Any
4	0		Any	Any	Any Traffic	Any	drop	Log	Policy Targets	Any

Access Role

Name: U1
Color: Black

Comment:

Networks
Users
Machines
Authentication

Any user
All identified users
Specific users/groups:

Name	Full Name/Description	Distinguished Name
u1	u1	CN=u1,OU=firew...

Role Preview:

U1
Any network
Users
u1
Any machine

- Tương tự Rule 2 cho user “Administrator” chúng ta select đến user “administrator” thuộc domain svuit.vn và action “accept” cho phép traffic của Administrator đi ra bên ngoài.

SVUIT.VN

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time
1	0		AD01	Any	Any Traffic	Any	accept	Log	Policy Targets	Any
2	0	Admin		Any	Any Traffic	Any	accept	Log	Policy Targets	Any
3	0								Policy Targets	Any
4	0								Policy Targets	Any

Access Role

Name: Color:

Comment:

☒ Networks
 ☐ Users
 ☐ Machines
 ☐ Authentication

☐ Any user
☐ All identified users
☒ Specific users/groups:

Name	Full Name/Description	Distinguished Name
Administrator		CN=Administrator,...

Role Preview:

- Admin
 - Any network
 - Users
 - Administrator
 - Any machine

SVUIT.VN

- Rule 1:** Rule này là để máy DNS có thể truy cập ra bên ngoài internet. Điều này giúp các client có DNS server trở về DNS server (nằm trên AD) có thể truy cập ra bên ngoài nhờ sự phân giải tên miền của DNS server.

Policy

Search for IP, object, action, ... Query Syntax

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time
1	0		AD01	Any	Any Traffic	Any	accept	Log	Policy Targets	Any
3									Policy Targets	Any
4									Policy Targets	Any

Host Node - AD01

General Properties

Machine

Name: AD01

IPv4 Address: 10.0.0.10

IPv6 Address:

Comment: AD01

Products:

Configure Servers...

SVUIT.VN

- Sau khi chúng ta tạo các Rule xong chúng ta cần save cấu hình lại và cần nhấn "install policy" để áp phê cho các rule mới mà chúng ta đã tạo

Check Point SmartDashboard

Install Policy

Policy

Search for IP, object, action, ...

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time
1	0		AD01	Any	Any Traffic	Any	accept	Log	Policy Targets	Any
2	0		Admin	Any	Any Traffic	Any	accept	Log	Policy Targets	Any
3	0		U1	Any	Any Traffic	Any	drop	Log	Policy Targets	Any
4	0		Any	Any	Any Traffic	Any	drop	Log	Policy Targets	Any

SVUIT.VN

Install Policy

1 gateway selected

Installation Targets

Network Security

Firewall

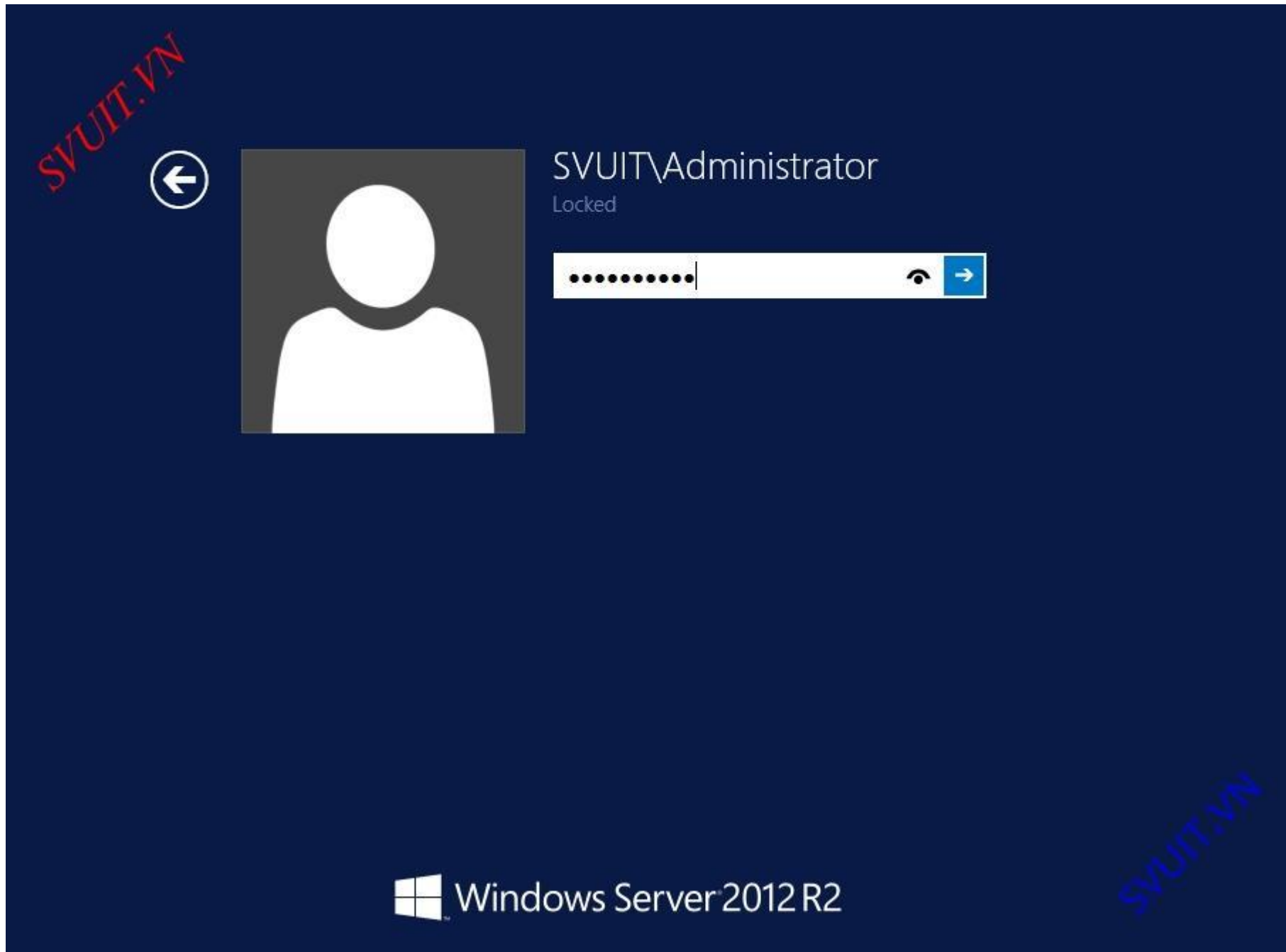
Advanced

OK Cancel Help

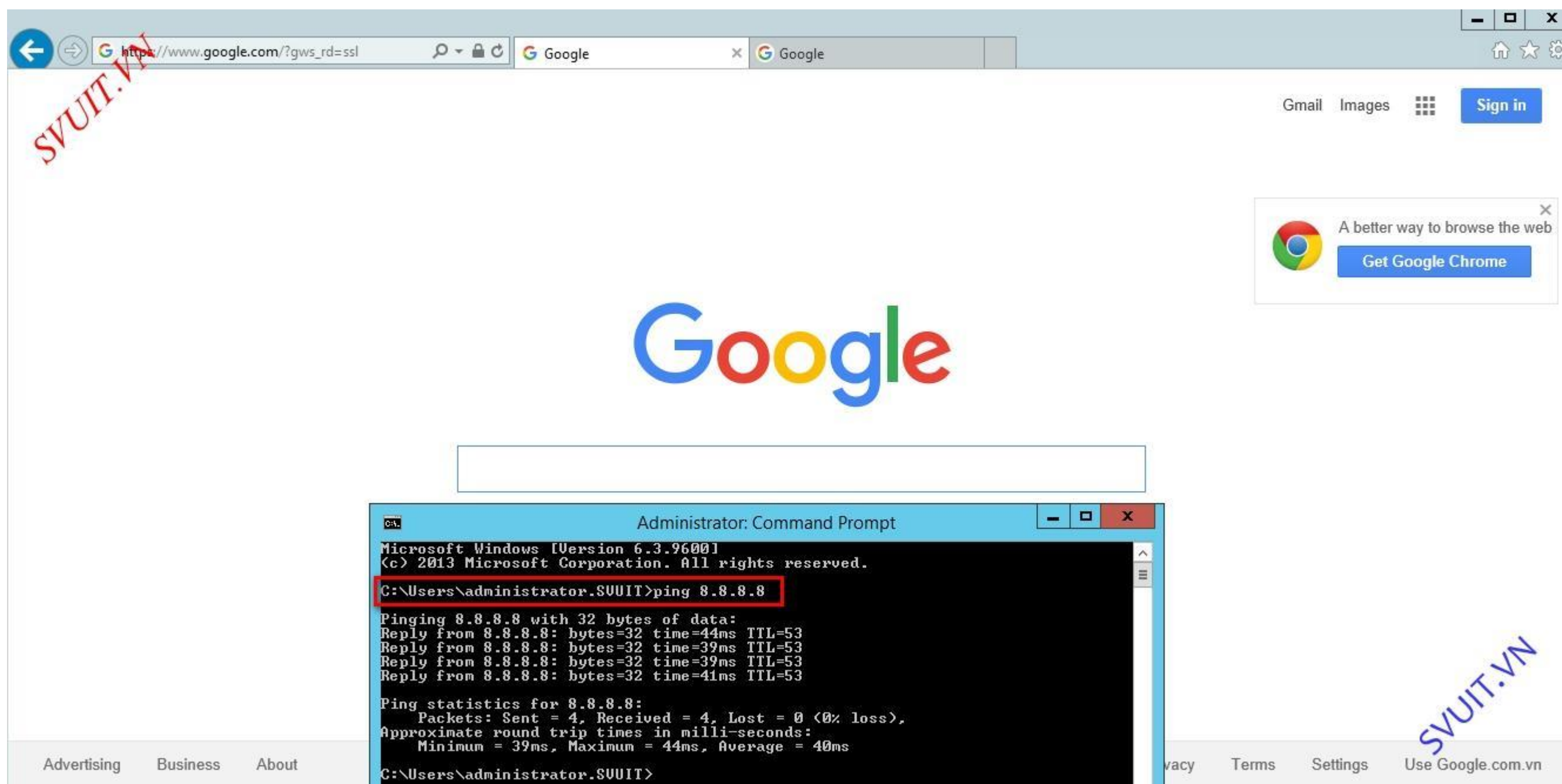
SVUIT.VN

Test

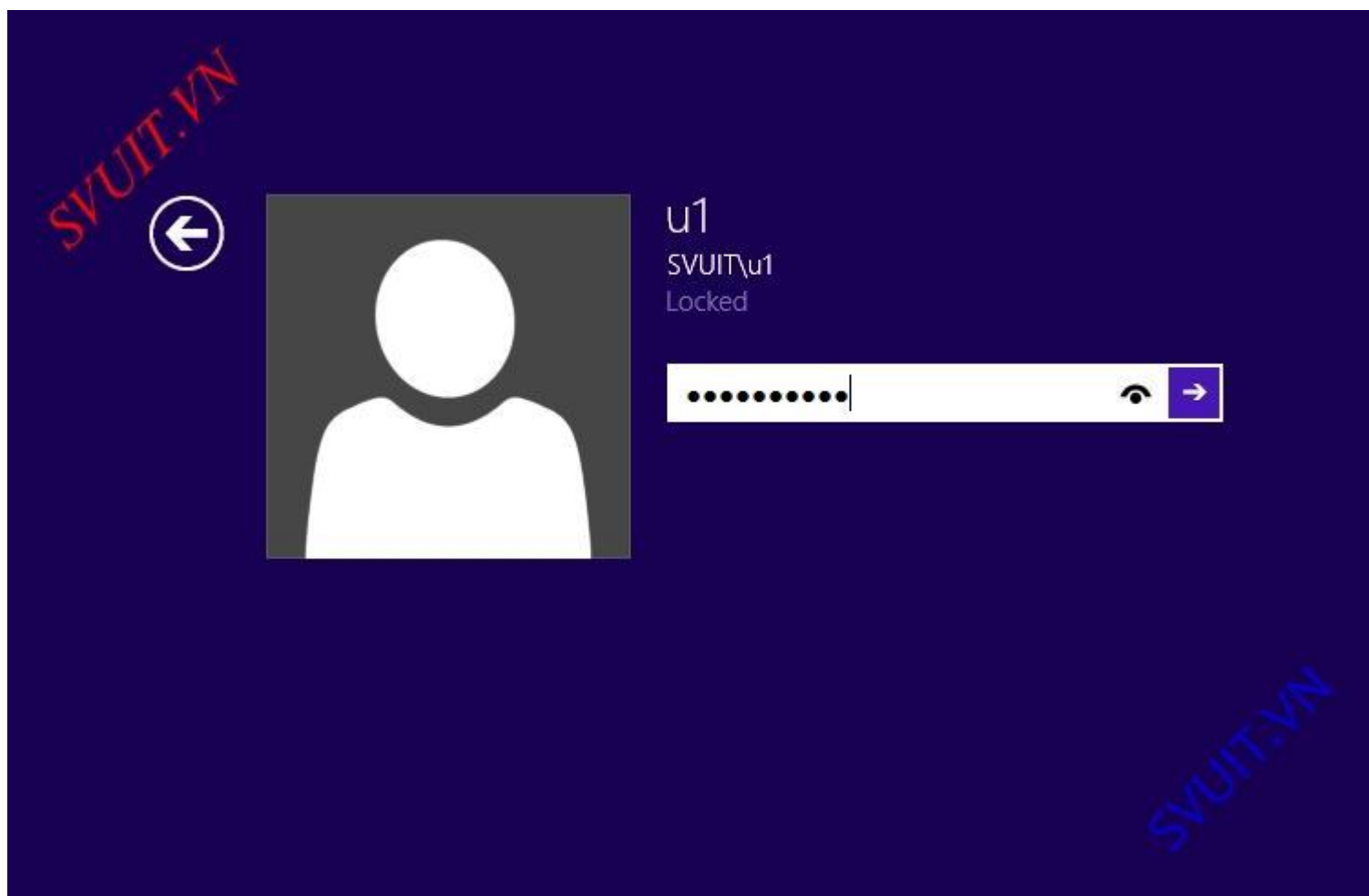
- Bây giờ chúng ta sử dụng 1 máy tính đã join domain và login vào với user “administrator” để kiểm tra kết quả các rule chúng ta đã tạo



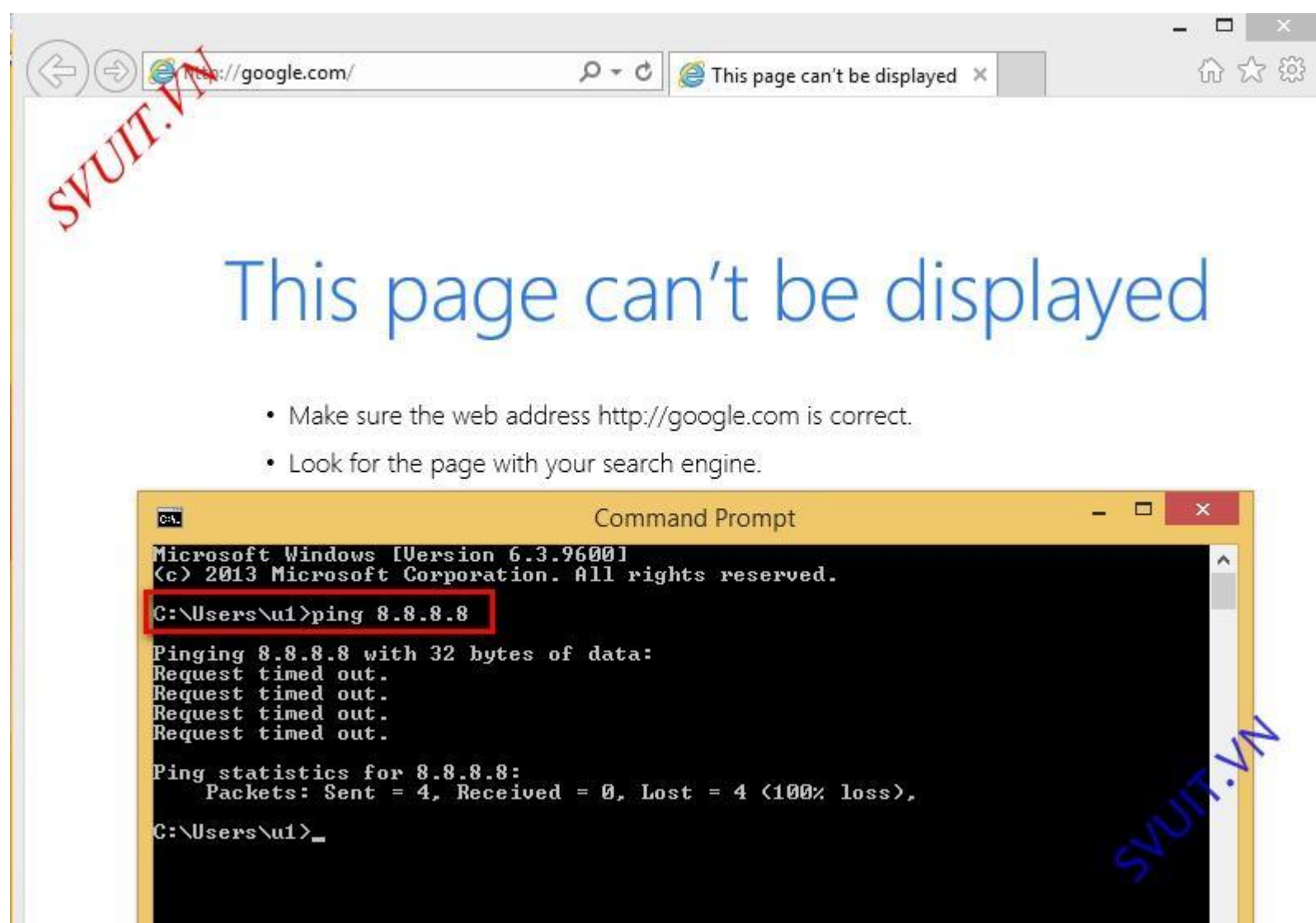
- Chúng ta có thể thấy với user “administrator” có thể ping ra ngoài internet và truy cập web thành công



- Tương tự bây giờ dùng 1 máy tính đã join domain khác và login vào với user "u1" để kiểm tra



- Ở đây trên máy tính user “u1” không thể ping ra ngoài internet và không thể truy cập web ra bên ngoài



- Bây giờ chúng ta quay lại giao diện “smart Console” để kiểm tra lại log mà firewall đã ghi về các hành động mà chúng ta đã test ở trên nhé

The screenshot shows the Check Point SmartDashboard interface. The 'SmartConsole' menu is open, listing various tools. The 'SmartView Tracker' option is highlighted with a red box. Below the menu, a table displays policy rules. The table has columns: No., H, Destination, VPN, Service, Action, Track, Install On, and Time. The first two rules show 'accept' actions, while the third and fourth show 'drop' actions. A watermark 'SVUIT.VN' is visible in the bottom right corner.

No.	H	Destination	VPN	Service	Action	Track	Install On	Time
1		Any	Any Traffic	Any	accept	Log	Policy Targets	Any
2		Any	Any Traffic	Any	accept	Log	Policy Targets	Any
3	0	Any	Any Traffic	Any	drop	Log	Policy Targets	Any
4	0	Any	Any Traffic	Any	drop	Log	Policy Targets	Any

- Ở đây chúng ta có thể thấy gói ping (ICMP) của user “administrator” có màu xanh được phép đi, còn gói ICMP của user “u1” thì bị drop có màu đỏ

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

All Records* (fw.log)

abc

- Các bạn double click lên dòng log ICMP của user “administrator” chúng ta có thể thấy. Với user “administrator” các gói tin sẽ chịu ảnh hưởng bởi Rule số 2 và action của nó là “accept”

Record Details

Previous

Next

Copy Details

Security Gateway/Management

Log Info

Product	Security Gateway/Management
Date	26Oct2015
Time	11:26:33
Number	39573
Type	Log
Origin	Firewall

Traffic

Source	10.0.0.2
	Administrator
	smartconsole@svuit.vn
Destination	google-public-dns-a.google.com (8.8.8.8)
Service	---
Protocol	icmp
Interface	eth2
Source Port	---

Policy

Policy Name	Standard
Policy Date	Mon Oct 26 10:49:21 2015
Policy Management	Firewall

Rule


Action	Accept
Rule	2
Current Rule Number	2-Standard
Rule Name	---
User	Administrator

More

Rule UID	{F245DAD8-FF2C-41D8-B8A8-5C9982DC4F01}
NAT rule number	6
NAT additional rule number	1
XlateSrc	192.168.40.19
Session ID	5e055440
Product Family	Network
Information	service_id: icmp-proto ICMP: Echo Request ICMP Type: 8 ICMP Code: 0

- Ngược lại với gói tin của user “u1” bị chặn bởi rule số 3

Previous Next Copy Details

 Security Gateway/Management

Log Info	
Product	Security Gateway/Management
Date	26Oct2015
Time	11:26:42
Number	39574
Type	Log
Origin	Firewall

Traffic	
Source	10.0.0.4
	u1 (u1)
	svuit-pc@svuit.vn
Destination	google-public-dns-a.google.com (8.8.8.8)
Service	---
Protocol	icmp
Interface	eth2
Source Port	---

Policy	
Policy Name	Standard
Policy Date	Mon Oct 26 10:49:21 2015
Policy Management	Firewall

Rule	
Action	Drop
Rule	3
Current Rule Number	3-Standard
Rule Name	---
User	u1 (u1)

More	
Rule UID	{484930FA-E538-4359-BD79-4ADDD7281ECA}
Session ID	204c8e55
Product Family	Network
Information	ICMP: Echo Request ICMP Type: 8 ICMP Code: 0

SVUIT.VN

- Tương tự với các dòng log khi sử dụng giao thức http, https...

10.0.0.203 - Check Point SmartView Tracker

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

All Records* (fw.log)

No.	Date	Time	Origin	Service	Src.	Src. User ...	Destination	Rule	Curr. Rule ...	R	Source Port
39590	26Oct2015	11:29:48	Firewall	UDP	17500	Z	255.255.255.255	4	4-Standard		17500
39591	26Oct2015	11:29:48	Firewall	UDP	17500	Z	192.168.40.255	4	4-Standard		17500
39592	26Oct2015	11:30:08	Firewall	UDP	nbdatalogram		192.168.40.255	4	4-Standard		nbdatalogram
39593	26Oct2015	11:30:12	Firewall	UDP	nbdatalogram		192.168.40.255	4	4-Standard		nbdatalogram
39594	26Oct2015	11:30:15	Firewall	UDP	17500		255.255.255.255	4	4-Standard		17500
39595	26Oct2015	11:30:16	Firewall	UDP	nbname		192.168.40.255	4	4-Standard		nbname
39596	26Oct2015	11:30:16	Firewall	UDP	nbname	Z	192.168.40.255	4	4-Standard		nbname
39597	26Oct2015	11:31:15	Firewall	UDP	17500		192.168.40.255	4	4-Standard		17500
39598	26Oct2015	11:31:18	Firewall	UDP	17500	Z	255.255.255.255	4	4-Standard		17500
39599	26Oct2015	11:31:18	Firewall	UDP	17500	Z	192.168.40.255	4	4-Standard		17500
39600	26Oct2015	11:31:45	Firewall	UDP	17500		255.255.255.255	4	4-Standard		17500
39601	26Oct2015	11:32:26	Firewall	UDP	nbname	10.0.0.2 Administrator	10.0.0.255	2	2-Standard		nbname
39602	26Oct2015	11:32:27	Firewall	UDP	nbname	10.0.0.2 Administrator	10.0.0.255				nbname
39603	26Oct2015	11:32:28	Firewall	UDP	nbname	10.0.0.2 Administrator	10.0.0.255				nbname
39604	26Oct2015	11:32:41	Firewall	TCP	https	10.0.0.2 Administrator	hkg08s13-in-f4.1e1...	2	2-Standard		49248
39605	26Oct2015	11:32:41	Firewall	TCP	https	10.0.0.2 Administrator	125.234.54.29.hcm....	2	2-Standard		49249
39606	26Oct2015	11:32:41	Firewall	TCP	https	10.0.0.2 Administrator	125.234.53.88.hcm....	2	2-Standard		49250
39607	26Oct2015	11:32:41	Firewall	UDP	domain-udp	AD01	172.16.1.10	1	1-Standard		58633
39608	26Oct2015	11:32:44	Firewall	UDP	domain-udp	AD01	ns2.google.com	1	1-Standard		57901
39609	26Oct2015	11:32:44	Firewall	TCP	https	10.0.0.2 Administrator	125.234.53.20.hcm....	2	2-Standard		49251
39610	26Oct2015	11:32:45	Firewall	UDP	17500		192.168.40.255	4	4-Standard		17500
39611	26Oct2015	11:32:48	Firewall	UDP	17500	Z	255.255.255.255	4	4-Standard		17500
39612	26Oct2015	11:32:48	Firewall	UDP	17500	Z	192.168.40.255	4	4-Standard		17500
39613	26Oct2015	11:32:48	Firewall	TCP	http	10.0.0.4 u1 (u1)	hkg08s13-in-f4.1e1...	3	3-Standard		49230
39614	26Oct2015	11:32:49	Firewall	TCP	http	10.0.0.4 u1 (u1)	hkg08s13-in-f4.1e1...	3	3-Standard		49229
39615	26Oct2015	11:32:55	Firewall	TCP	http	10.0.0.4 u1 (u1)	hkg08s13-in-f4.1e1...	3	3-Standard		49231
39616	26Oct2015	11:32:58	Firewall	UDP	nbname		192.168.40.255	4	4-Standard		nbname
39617	26Oct2015	11:32:58	Firewall	UDP	nbname	10.0.0.30	10.0.0.255	4	4-Standard		nbname
39618	26Oct2015	11:32:58	Firewall	UDP	nbname	admins-...	192.168.40.255	4	4-Standard		nbname
39619	26Oct2015	11:32:58	Firewall	UDP	nbname	Jessies-...	192.168.40.255	4	4-Standard		nbname