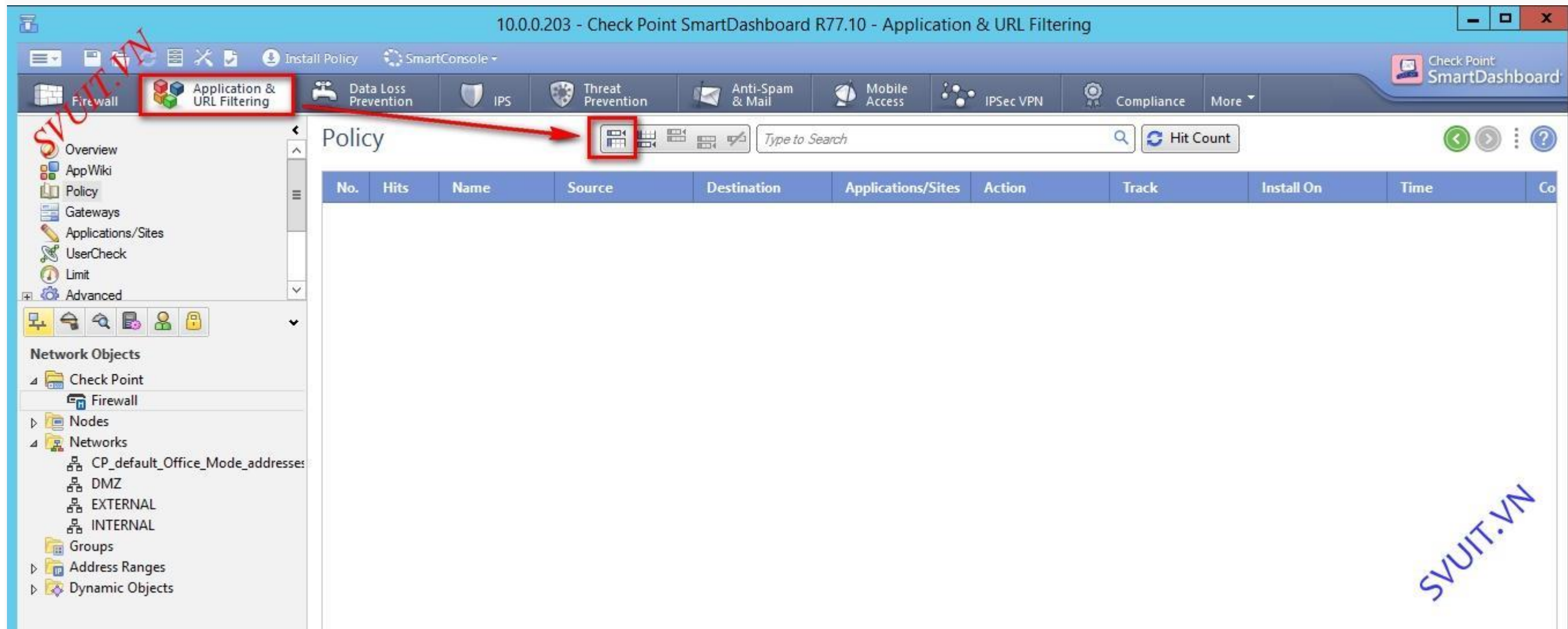


## Application & URL Filtering

### 1. Chặn Facebook

- Sử dụng SmartConsole để login vào Checkpoint.
- Click vào tab “Application & URL filtering” và tiến hành add rule cấm user “u1” truy cập facebook



- Đặt tên cho rule mà chúng ta muốn tạo bằng cách chuột phải vào cột column của Rule 1

Policy

Type to Search

Hit Count

No.	Hit	Name	Source	Destination	Applications/Sites	Action	Track	Install On	Time	Co
1	0	Facebook	Any	Internet	Any Recognized	Block Blocked Message	Log	All	Any	

Edit...

Rule Actions

Policy

Type to Search

Hit Count

No.	Hit	Name	Source	Destination	Applications/Sites	Action	Track	Install On	Time	Co
1	0	Facebook	Any	Internet	Any Recognized	Block Blocked Message	Log	All	Any	

Name

Name: Facebook

OK

Cancel

- Qua tab "Applications/Sites" các bạn click vào dấu "+" và gõ vào ô tìm kiếm từ khóa "facebook" sau đó các bạn check vào các site & ứng dụng facebook mà bạn muốn chặn

10.0.0.203 - Check Point SmartDashboard R77.10 - Application & URL Filtering

Check Point SmartDashboard

Policy

No.	Hits	Name	Source	Destination	Applications/Sites	Action	Track	Install On	Time	Co
1	0	Facebook	Any	Internet	Any Recog...	Block Blocked Message	Log	All	Any	

face

Available (34)

- ☒ Facebook
- ☒ Facebook Apps
- ☒ Facebook Business
- ☒ Facebook Education
- ☒ Facebook Entertainment
- ☒ Facebook File Sharing
- ☒ Facebook Friends & Family

Selected (8)

- Facebook Business
- Facebook Education
- Facebook File Sharing
- Facebook Friends & Family
- Facebook Entertainment

Facebook Entertainment

Facebook widgets related to entertainment, such as books, media, movies, music, etc.

10526 Applications with this category:

Movies, Astrology Badge and Match, Addicted to Scrubs, Addicted to Sex and the City, Addicted to Grey's Anatomy [more...](#)

New... OK Cancel

- Và đây là Rule mà mình tiến hành chặn người dùng truy cập Facebook. Bạn có thể chặn theo giờ ví dụ trong giờ làm việc nhân viên không được truy cập facebook... ở cột Time.



10.0.0.203 - Check Point SmartDashboard R77.10 - Application & URL Filtering

SVUIT.VN

Check Point SmartDashboard

Application & URL Filtering

Policy

No.	Hits	Name	Source	Destination	Applications/Sites	Action	Track	Install On	Time	Comment
1	0	Facebook	Any	Internet	<ul style="list-style-type: none"> <li>Facebook</li> <li>Facebook-chat</li> <li>Facebook Apps</li> <li>Facebook Business</li> <li>Facebook Education</li> <li>Facebook File Sharing</li> <li>Facebook Friends &amp; Family</li> <li>Facebook Entertainment</li> </ul>	<ul style="list-style-type: none"> <li>Block</li> <li>Blocked M...</li> </ul>	Log	All	Any	

SVUIT.VN

- Và phần source của rule này chúng ta sẽ tiến hành add user mà chúng ta muốn cấm họ truy cập Facebook

10.0.0.203 - Check Point SmartDashboard R77.10 - Application & URL Filtering

SVUIT.VN

Policy

No.	Hits	Name	Source	Destination	Applications/Sites	Action	Track	Install On	Time	Comment
1	0	Facebook	Any	Internet	Facebook	Block	Log	All	Any	

Context menu for Source:

- Network Object...
- Add User/Access Role...
- Edit...
- Remove
- Last Modified...
- Where Used...
- Negate Cell
- Select All
- Cut
- Copy
- Paste
- Rule Actions

SVUIT.VN

- Ở đây mình sẽ thực hiện cấm user "u1" của domain svuit.vn truy cập facebook

10.0.0.203 - Check Point SmartDashboard R77.10 - Application & URL Filtering

Check Point SmartDashboard

Fire wall Application & URL Filtering Data Loss Prevention IPS Threat Prevention Anti-Spam & Mail Mobile Access IPSec VPN Compliance More

Policy

Access Role

Name: U1 Color: Black

Comment:

Networks Users Machines Authentication

Any user

All identified users

**Specific users/groups:**

Role Preview:

U1

Any network

Users

Specific users

Any machine

Hit Count

No.	Hits	Install On	Time	Comment
1	0	All	Any	

Network Objects

Check Point

Firewall

Nodes

Networks

CP\_default\_Office\_Mode\_addresses

DMZ

EXTERNAL

INTERNAL

Groups

Address Ranges

Dynamic Objects

Name Full Name/Description Distinguished Name

Administrator Built-in account for adminis... CN=Administrator,CN=Use...

firewall firewall CN=firewall,OU=firewall,D...

Guest Built-in account for guest a... CN=Guest,CN=Users,DC=...

krbtgt Key Distribution Center Ser... CN=krbtgt,CN=Users,DC=...

**u1 u1 CN=u1,OU=firewall,DC=s...**

u2 u2 CN=u2,OU=firewall,DC=s...

u3 u3 CN=u3,CN=Users,DC=svu...

u4 u4 CN=u4,OU=firewall,DC=s...

- Sau khi tạo rule cấm facebook xong chúng ta cần tiến hành save & install policy để rule áp phê



10.0.0.203 - Check Point SmartDashboard R77.10 - Application & URL Filtering

Install Policy

SmartConsole

FirewallApplication & URL FilteringData Loss PreventionIPSThreat PreventionAnti-Spam & MailMobile AccessIPSec VPNComplianceMore

OverviewAppWikiPolicyGatewaysApplications/SitesUserCheckLimitAdvanced

Network Objects

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

Policy

Type to Search

Hit Count

No.	Hits	Name	Source	Destination	Applications/Sites	Action	Track	Install On	Time	Comment
1	0	Facebook	u1_URL	Internet	FacebookFacebook-chatFacebook AppsFacebook BusinessFacebook EducationFacebook File SharingFacebook Friends & FamilyFacebook Entertainment	BlockBlocked M...	Log	All	Any	

SVUIT.VN

10.0.0.203 - Check Point SmartDashboard R77.10 - Application & URL Filtering

Install Policy SmartConsole

Firewall Application & URL Filtering Data Loss Prevention IPS Threat Prevention Anti-Spam & Mail Mobile Access IPsec VPN Compliance More

Overview AppWiki Policy Gateways Applications/Sites UserCheck Limit Advanced

Network Objects

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

Policy

No.	Hits
1	0

Hit Count

Track Log Install On All Time Any

Installation Process - Standard

Installation

Installation Targets	Version	Network Security	Threat Prevention	IPS-1 Sensor
Firewall	R77.10	OK		

Progress

Installation completed successfully

Close

- Và bên tab Firewall chúng ta sẽ cho phép user "U1" truy cập internet nhưng không được phép truy cập facebook (vì bị block ở policy mà chúng ta đã tạo ở trên)



10.0.0.203 - Check Point SmartDashboard R77.10 - Standard

Check Point SmartDashboard

Firewall

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

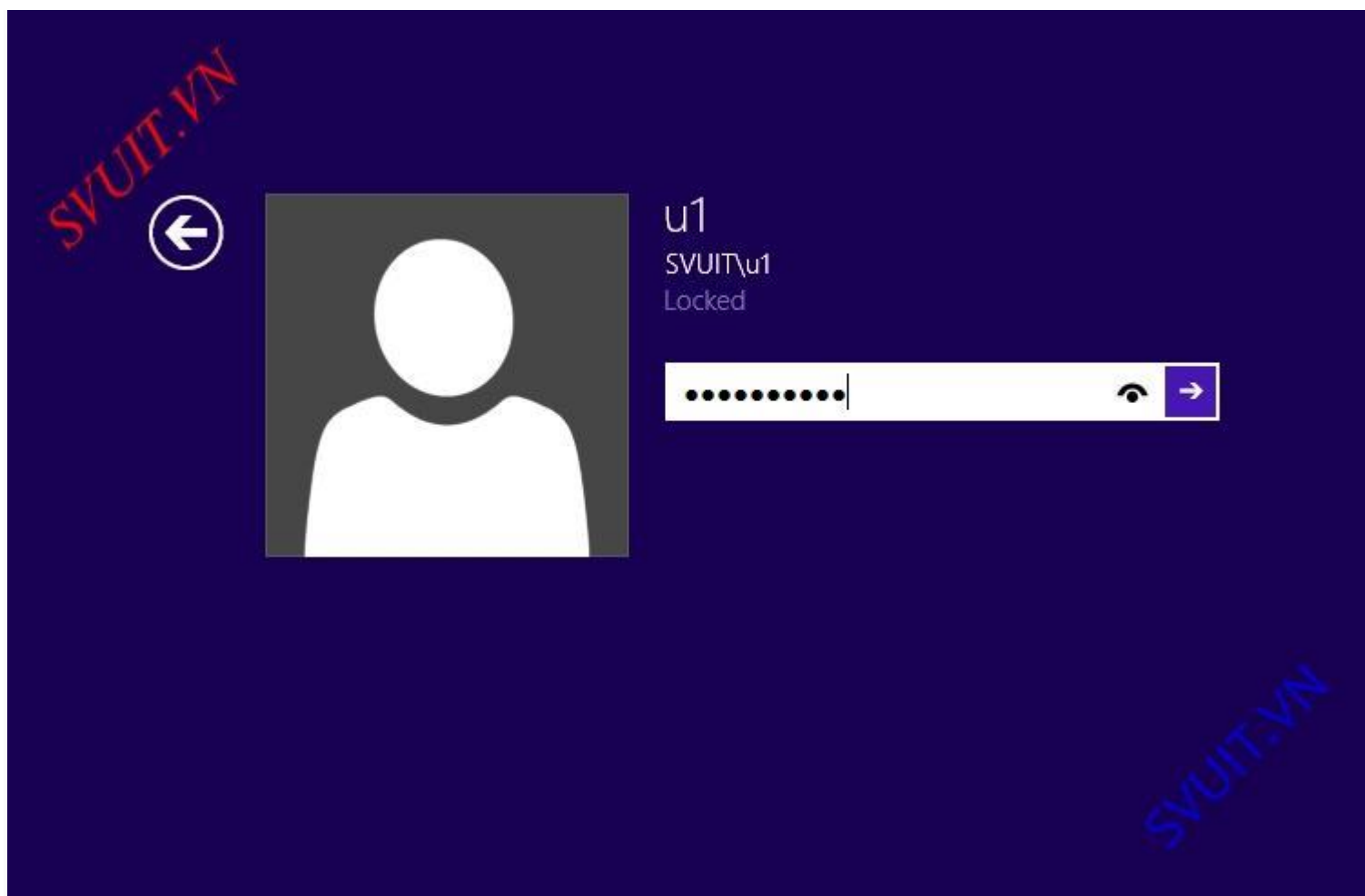
Search for IP, object, action, ...

Query Syntax

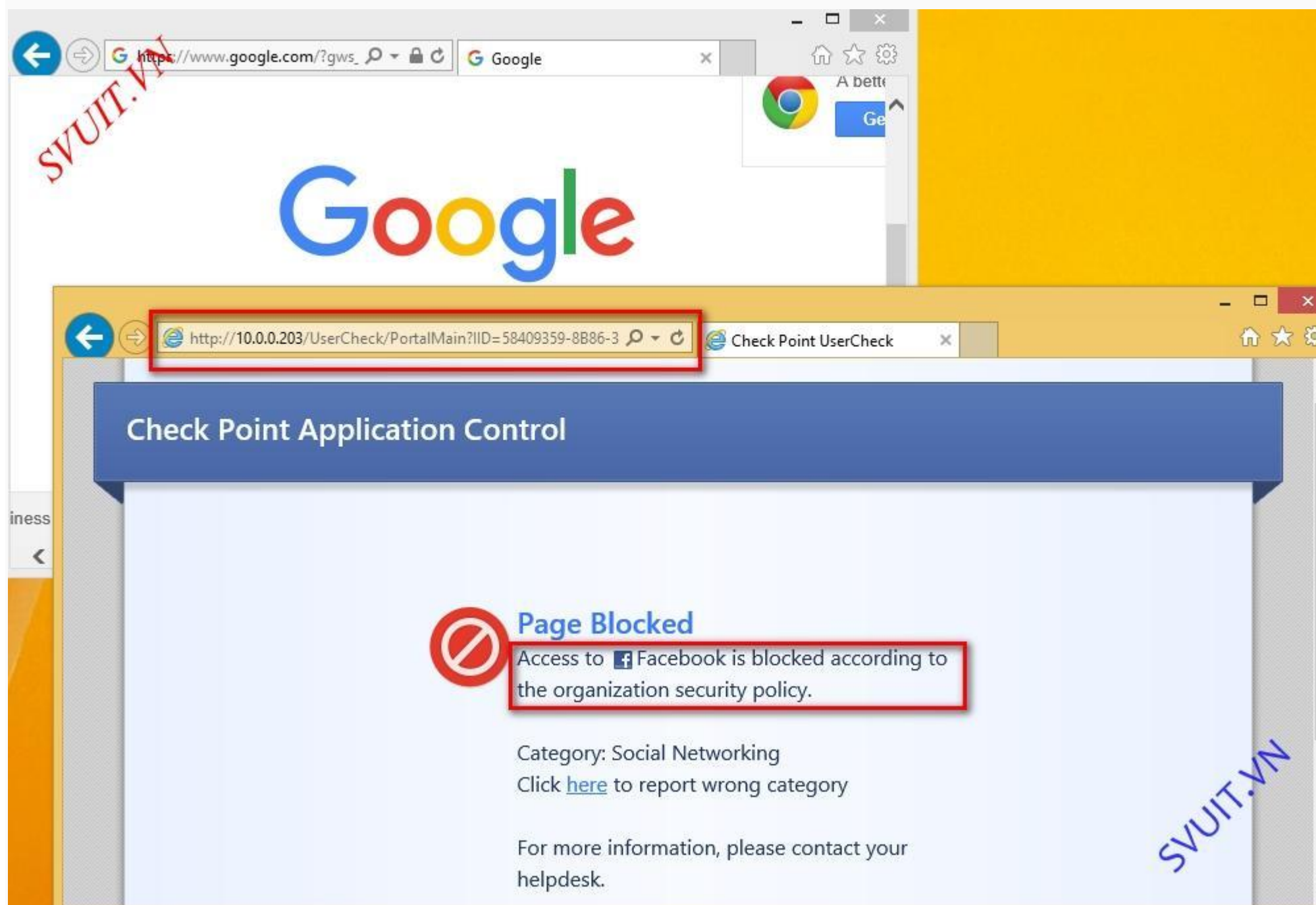
No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time
1	119		AD01	Any	Any Traffic	Any	accept	Log	Policy Targets	Any
2	27		Admin	Any	Any Traffic	Any	accept	Log	Policy Targets	Any
3	130		U1	Any	Any Traffic	Any	accept	Log	Policy Targets	Any
4	0		Any	Any	Any Traffic	Any	drop	None	Policy Targets	Any

SVUIT.VN

- Bây giờ chúng ta login vào PC bằng user “u1” để kiểm tra rule mà chúng ta đã thiết lập trên firewall



- Chúng ta có thể thấy user “u1” được truy cập internet như google... nhưng không lướt facebook được



- Bây giờ chúng ta sẽ thử login vào pc bằng user “administrator” để kiểm tra





- Chúng ta có thể thấy administrator có thể lướt facebook và truy cập web bình thường vì nó không bị ảnh hưởng bởi rule block facebook



- Chúng ta có thể sử dụng giao diện “smartview Tracker” để kiểm tra lại log.
- Các bạn click vào dòng “application and URL filtering -> all” để kiểm tra lại log của firewall. Tại dòng cuối cùng chúng ta có thể thấy user “u1” truy cập đến facebook bị block



10.0.0.203 - Check Point SmartView Tracker - [All\* (fw.log)]

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 Filtering
    - All
    - High Risk
    - More
      - Applications
      - Sites
      - Bandwidth Control
      - Blocked
      - System
      - HTTPS Inspection
      - UserCheck
  - HTTPS Inspection
  - Identity Awareness Blade
  - Mobile Access Blade
  - Anti-Spam & Email Security
  - Data Loss Prevention
  - IPsec VPN Blade
  - Advanced Networking
  - Traditional Anti-Virus
  - More
    - Firewall-1 GX Blade
    - UTM-1 Edge
    - Monitoring Blade

All\* (fw.log)

No.	Date	Time	O...	User	Source	Dst.	Traffic	Dropped	App. / Site	Matched Category
38461	23Oct2015	17:51:42	Firewall	u2 (u2)(+)Administrat...	10.0.0.2	bs.serving-sys...	1935		bs.serving-sys.c...	Business / Economy
38484	23Oct2015	17:51:45	Firewall	u2 (u2)(+)Administrat...	10.0.0.2	ptr.vng.vn	1570		zaloapp.com	Instant Messaging
38498	23Oct2015	17:51:47	Firewall	u2 (u2)(+)Administrat...	10.0.0.2	103.23.159.32	7909		adtimaserver.vn	General
38527	23Oct2015	17:51:50	Firewall	u2 (u2)(+)Administrat...	10.0.0.2	ci76-49.netna...	1153		ants.vn	Computers / Internet
38564	23Oct2015	17:51:56	Firewall	u2 (u2)(+)Administrat...	10.0.0.2	d2.26.5177.ip...	1170		lijit.com	Search Engines / Portals
38569	23Oct2015	17:51:56	Firewall	u2 (u2)(+)Administrat...	10.0.0.2	125.234.54.22...	2039	2	YouTube	Media Sharing
38585	23Oct2015	17:52:00	Firewall	u2 (u2)(+)Administrat...	10.0.0.2	182.161.73.100	1286		criteo.com	Business / Economy
38604	23Oct2015	17:52:03	Firewall	u2 (u2)(+)Administrat...	10.0.0.2	123.30.108.121	13490		anthill.vn	Computers / Internet
38618	23Oct2015	17:52:03	Firewall	u2 (u2)(+)Administrat...	10.0.0.2	ptr.vng.vn	8756		support.brand...	News / Media
38632	23Oct2015	17:52:03	Firewall	u2 (u2)(+)Administrat...	10.0.0.2	edge-star-sh...	23081	2	Facebook	Social Networking
38708	23Oct2015	17:52:12	Firewall	u2 (u2)(+)Administrat...	10.0.0.2	edge-star-sh...		2	Facebook	Social Networking
38713	23Oct2015	17:52:12	Firewall	u2 (u2)(+)Administrat...	10.0.0.2	edge-star-sh...		2	Facebook	Social Networking
38715	23Oct2015	17:52:12	Firewall	u2 (u2)(+)Administrat...	10.0.0.2	edge-star-sh...		2	Facebook	Social Networking
38717	23Oct2015	17:52:12	Firewall	u2 (u2)(+)Administrat...	10.0.0.2	edge-star-sh...		2	Facebook	Social Networking
38723	23Oct2015	17:52:13	Firewall	u2 (u2)(+)Administrat...	10.0.0.2	edge-star-sh...		2	Facebook	Social Networking
38725	23Oct2015	17:52:13	Firewall	u2 (u2)(+)Administrat...	10.0.0.2	edge-star-sh...	489	1	SSL v3	Network Protocols
38823	26Oct2015	10:11:11	Firewall	...						
38982	26Oct2015	10:42:35	Firewall	...	AD01	j.root-servers...	30793	1	DNS Protocol	Network Protocols
39004	26Oct2015	10:42:58	Firewall	Administrator	10.0.0.2	94.245.121.251	452	1	Teredo Protocol	Network Protocols
39430	26Oct2015	11:09:06	Firewall	Administrator	10.0.0.2	hkg08s13-in...	2934	2	Google Search	Search Engines / Portals
39432	26Oct2015	11:09:07	Firewall	Administrator	10.0.0.2	hkg08s13-in...	439505	2	Google Services	Web Services Provider
40301	26Oct2015	14:41:18	Firewall	...						
40638	26Oct2015	16:45:20	Firewall	Administrator	AD01	j.root-servers...	22833	1	DNS Protocol	Network Protocols
40689	26Oct2015	16:45:36	Firewall	Administrator	10.0.0.2	hkg08s13-in...	3459	2	Google Search	Search Engines / Portals
40691	26Oct2015	16:45:36	Firewall	Administrator	10.0.0.2	hkg08s13-in...	9098	2	Google Services	Web Services Provider
40707	26Oct2015	16:45:50	Firewall	Administrator	10.0.0.2	157.56.106.189	452	1	Teredo Protocol	Network Protocols
40752	26Oct2015	16:47:16	Firewall	Administrator	10.0.0.2	hkg08s13-in...	1411	2	Google Search	Search Engines / Portals
40754	26Oct2015	16:47:16	Firewall	Administrator	10.0.0.2	hkg08s13-in...	452657	2	Google Services	Web Services Provider
40776	26Oct2015	16:47:30	Firewall	...	10.0.0.2	edge-star-sh...		2	Facebook	Social Networking
41055	26Oct2015	17:16:29	Firewall	u1 (u1)	10.0.0.4	edge-star-sh...		2	Facebook	Social Networking

- Double click vào dòng cuối cùng của log block facebook của u1 để xem chi tiết hành động của Firewall



Record Details

Previous Next Copy Details

Application Control: Block

**u1 (u1) was blocked access to Facebook from 10.0.0.4 yesterday at 17:16:29**

Details		Policy	
Name	* Facebook (Social Networking)	Action	Block
Matched Category	Social Networking	Rule Name	Facebook
All Categories	Transmits Information, Encrypts communication... >>	Policy Name	Standard
Description	Facebook is a social utility that helps conne... >>	Policy Date	Mon Oct 26 17:14:59 2015
Risk	2 Low	Policy Management	Firewall
URL	<a href="http://facebook.com/">http://facebook.com/</a> <a href="#">Copy</a>		

User Check	
Message to User	Access to Facebook is blocked according to th... >>
Confirmation Scope	For each application
Frequency	1 days

Traffic	
Source	10.0.0.4 u1 (u1) svuit-pc@svuit.vn
Destination	edge-star-shv-01-iad3.facebook.com (31.13.69.197)
Protocol	TCP tcp
Service	http (80)

More	
User Check	1
Client Type	Other: Mozilla/5.0 (Windows NT 6.3; WOW64; Tr... >>
Primary Category	Social Networking
Signature ID	10080872:5
Product Family	Network
Log ID	9999
Origin	Firewall
Number	41055
Type	Log
Information	---
Time	Oct 26, 2015 at 17:16:29
UserCheck ID	58409359-8B86-350C-41F1-E987C86EAB96

## 2. Search Engine

- Tiếp theo chúng ta sẽ tạo rule cấm user “u1” sử dụng các công cụ “Search Engine” như google, bing...
- Tương tự như ở trên chúng ta tạo rule block search engine

Policy

Type to Search

Hit Count

No.	Hits	Name	Source	Destination	Applications/Sites	Action	Track	Install On	Time	Co
1	0		U1_Search_Engine	Internet	Any Recog...	Block Blocked Message	Log	All	Any	
2	1	Facebook	u1_URL	Internet	Facebook Facebook-chat Facebook App...	Block Blocked Message	Log	All	Any	

sea

Categories

Applications/Sites

Custom

Widgets

Any R...

Available (2)

All Categories

Job Search / Careers

☒ Search Engines / Portals

Selected (1)

Search Engines / Portals

A search engine is a commonly used web application designed to let the user search for content based on the terms used.

Examples: <http://www.yahoo.com>, <http://www.google.com>, <http://search.yahoo.com>

45 Applications with this category:

Webcrawler, App Store, HowardForums, Sublight, All of Craigs, AltaVista, playlist.com, Radio-Locator, Google Search [more...](#)

New...

OK

Cancel

- Sau khi tạo xong rule chúng ta save & install policy để rule áp phê

10.0.0.203 - Check Point SmartDashboard R77.10 - Application & URL Filtering

Install Policy

Policy

No.	Hits	Name	Source	Destination	Applications/Sites	Action	Track	Install On	Time	Comment
1	0		U1_Search_Engine	Internet	Search Engines / Portals	Block Blocked M...	Log	All	Any	
2	1	Facebook	u1_URL	Internet	Facebook	Block	Log	All	Any	

Install Policy

1 gateway selected

Installation Targets: Firewall

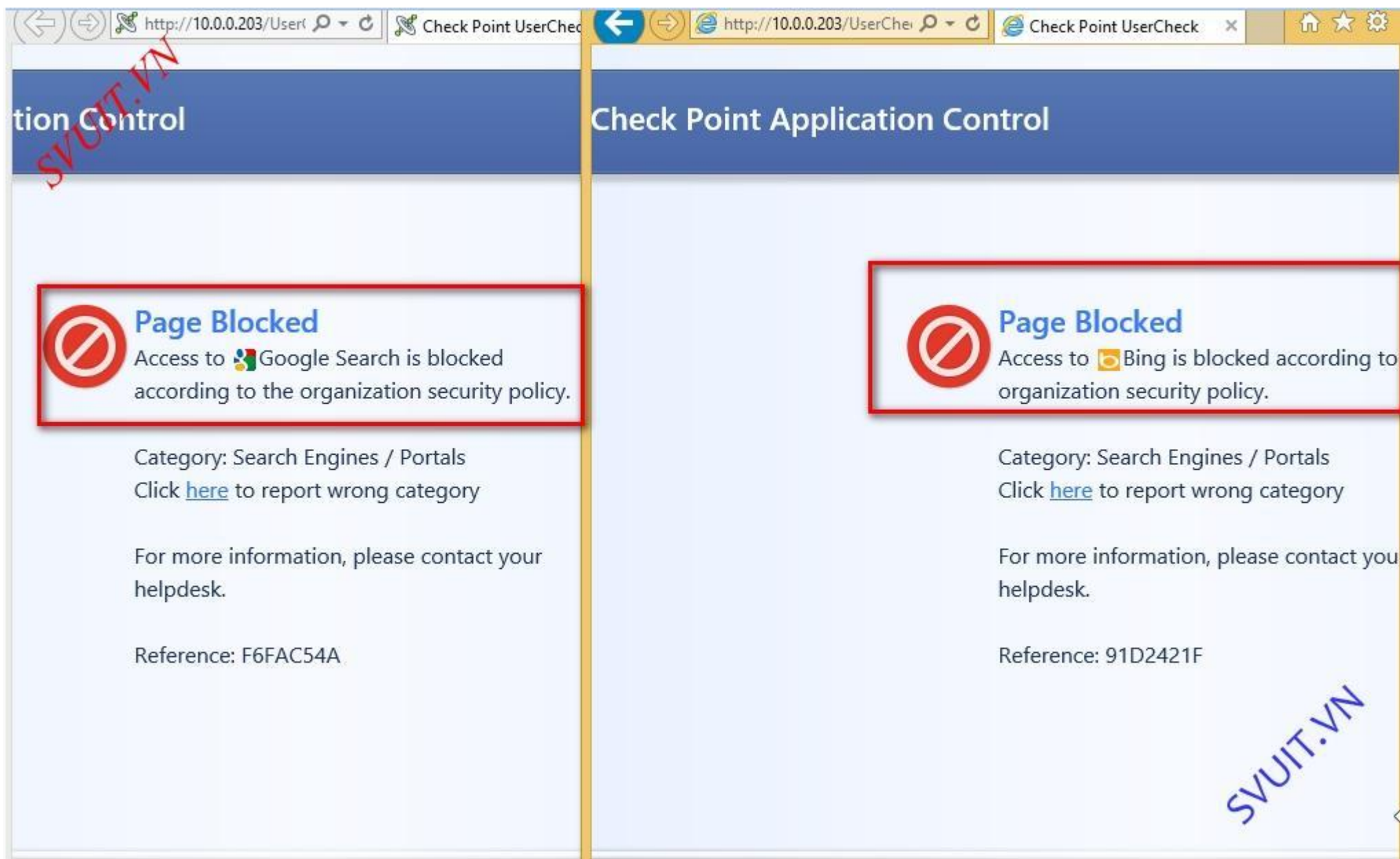
Network Security

OK Cancel Help

SVUIT.VN

- Bây giờ các bạn login vào user "u1" và sử dụng trình duyệt web truy cập thử 2 trang search engine như: google.com, bing.com... thì thấy nó bị block do firewall





- Quay lại firewall chúng ta kiểm tra log của firewall xem các gói tin của u1 vừa bị chặn

Previous Next Copy Details

Application Control: Block

**u1 (u1) was blocked access to Bing from 10.0.0.4 yesterday at 17:33:56**

Details		Policy	
Name	Bing (Search Engines / Portals)	Action	Block
Matched Category	Search Engines / Portals	Rule Name	<a href="#">Go to Policy</a>
All Categories	SSL Protocol, Low Risk, Search Engines / Portals	Policy Name	Standard
Description	Bing is a search engine created by Microsoft ... >>	Policy Date	Mon Oct 26 17:32:58 2015
Risk	Low	Policy Management	Firewall
URL	<a href="http://www.bing.com/">http://www.bing.com/</a> <a href="#">Copy</a>		

User Check	
Message to User	Access to Bing is blocked according to the or... >>
Confirmation Scope	For each application
Frequency	1 days

Traffic	
Source	10.0.0.4 u1 (u1) svuit-pc@svuit.vn
Destination	a-0001.a-msedge.net (204.79.197.200)
Protocol	TCP tcp
Service	http (80)

More	
User Check	1
Client Type	Other: Mozilla/5.0 (Windows NT 6.3; WOW64; Tr... >>
Server Type	Microsoft-IIS
Primary Category	Search Engines / Portals
Signature ID	10091087:3
Product Family	Network
Log ID	9999
Origin	Firewall
Number	41457
Type	Log
Information	---
Time	Oct 26, 2015 at 17:33:56
UserCheck ID	93AFA035-16AD-D06B-2C2F-5CDC91D2421F

### 3. Chặn 1 URL

- Chúng ta có thể chặn bất kì 1 trang web nào đó, không cho người dùng truy cập đến nó. Chẳng hạn như chúng ta sẽ tiến hành chặn trang mp3.zing.vn
- Tương tự như các rule mà chúng ta tạo ở trên bây giờ chúng ta tiến hành tạo 1 rule mới.
- Ở góc bên trái phía cuối cửa sổ chúng ta tiến hành tạo mới 1 site mà chúng ta muốn block "new -> New Application/Site..."

10.0.0.203 - Check Point SmartDashboard R77.10 - Application & URL Filtering

Check Point SmartDashboard

Policy

No.	Hits	Name	Source	Destination	Applications/Sites	Action	Track	Install On	Time	Comment
1	0	mp3.zin.vn	Any	Internet	Any Recognized	Block Blocked M...	Log	All	Any	
2	0	Search_engine	U1_Search_Egine	Internet	Search Engines / Portals	Block Blocked M...	Log	All	Any	
3								All	Any	

Available (171)

- Adds other software
- Alcohol
- Allows remote connect
- Allows remote control
- Anonymizer
- Art / Culture
- Autostarts/Stays Resident
- BitTorrent protocol

Selected

- Any Recognized

48 Applications with this category:

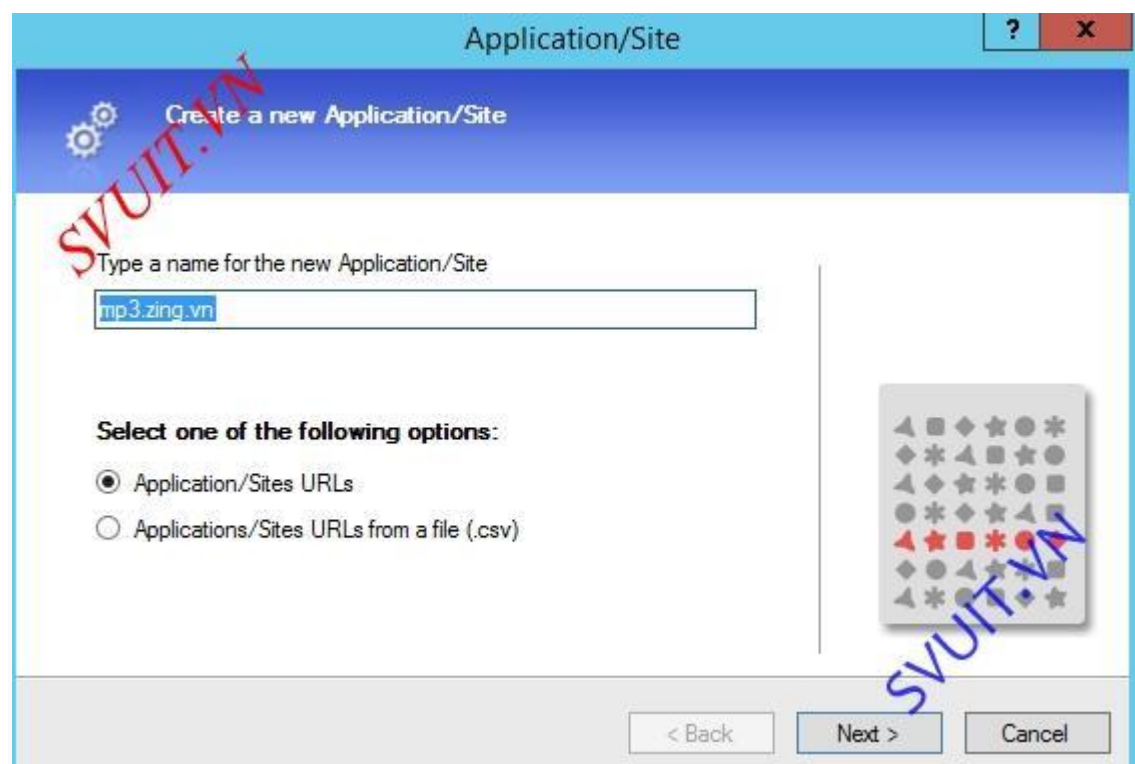
FlashGet, Xolox, Jubster, BearShare, Zilla Mp3 Finder, Kazaa Media Desktop, FreeWire, iMesh, Ask Toolbar [more...](#)

New...

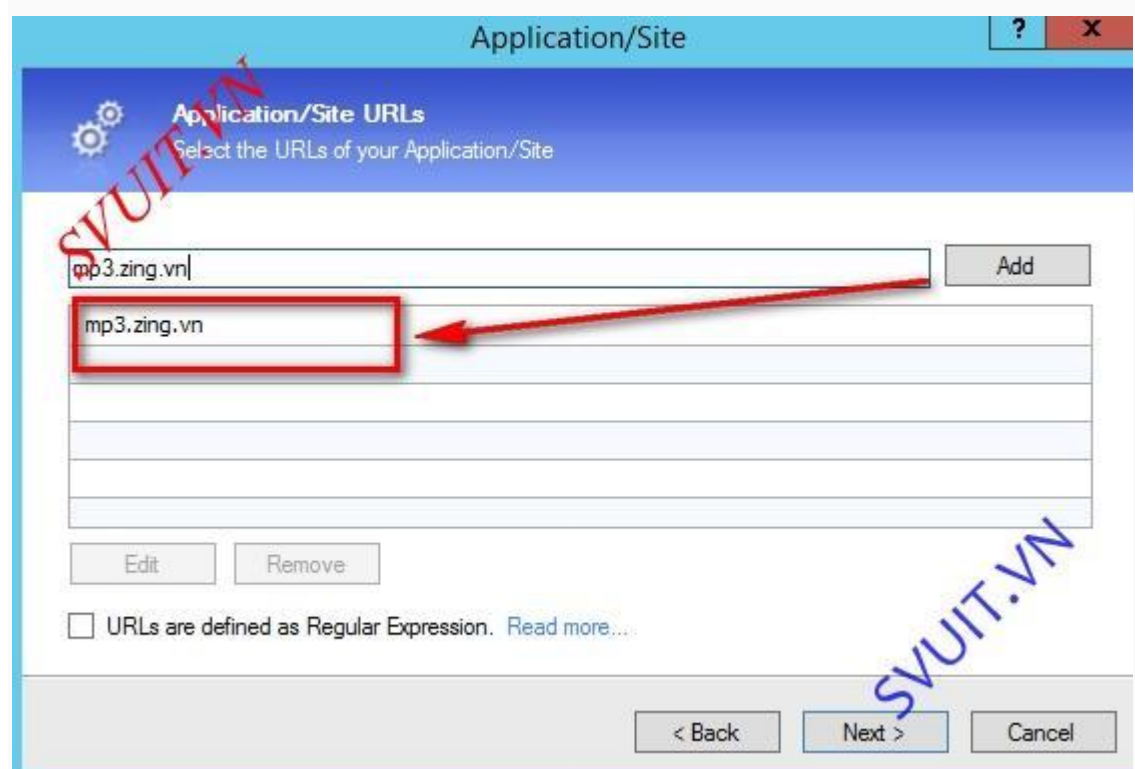
- New Application/Site...
- New Applications/Sites Group...

- Đặt tên cho site mà bạn muốn block

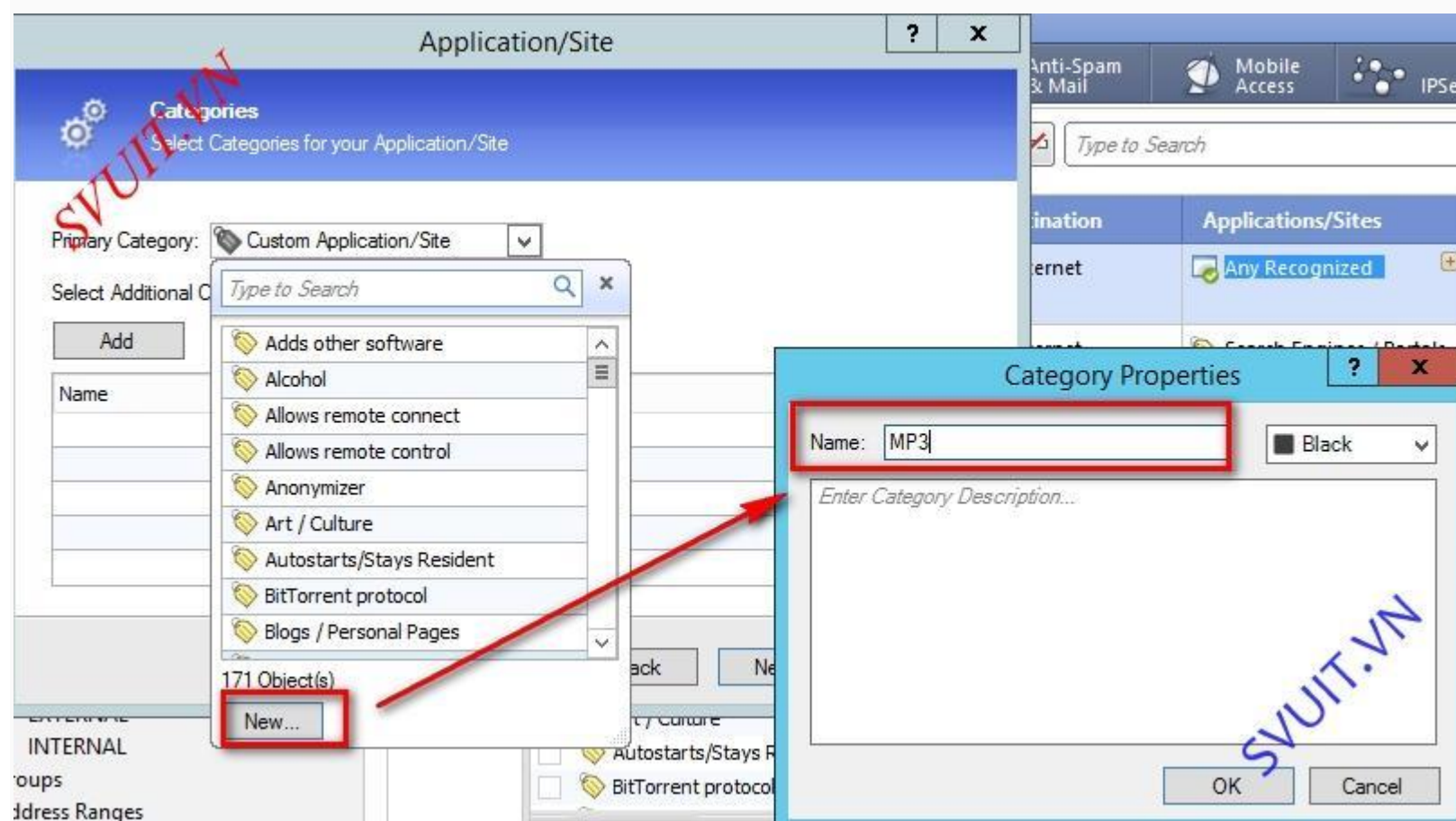




- Nhập URL của site mà bạn muốn cấm người dùng truy cập



- Và chúng ta có thể tạo 1 Object mới để khi cần dùng có thể search trong đồng Object có sẵn



- Như vậy rule block trang mp3.zing.vn chúng ta sẽ lấy trong Category “MP3” mà chúng ta đã tạo ở trên

Application/Site

**Categories**  
Select Categories for your Application/Site

Primary Category:

Select Additional Categories:

Name	Description

< Back   Next >   Cancel

- Hoàn thành việc tạo rule block trang mp3.zing.vn

Application/Site

**Finished**

The Applications/Sites wizard is complete.  
Click finish to have the new Application/Site available for use in the policy.

< Back   Finish   Cancel

- Save và install policy mà chúng ta đã tạo ở trên



10.0.0.203 - Check Point SmartDashboard R77.10 - Application & URL Filtering

Check Point SmartDashboard

Application & URL Filtering

Policy

No.	Hits	Name	Source	Destination	Applications/Sites	Action	Track	Install On	Time	Comment
1	0	mp3.zin.vn	Any	Internet	mp3.zing.vn	Block Blocked M...	Log	All	Any	
2	0	Search_engine	U1_Search_Egine	Internet	Search Engines / Portals	Block Blocked M...	Log	All	Any	
3	1	Facebook						All	Any	

Installation Process - Standard

Installation

Installation Targets	Version	Network Security	Threat Prevention	IPS-1 Sensor
Firewall	R77.10	OK		

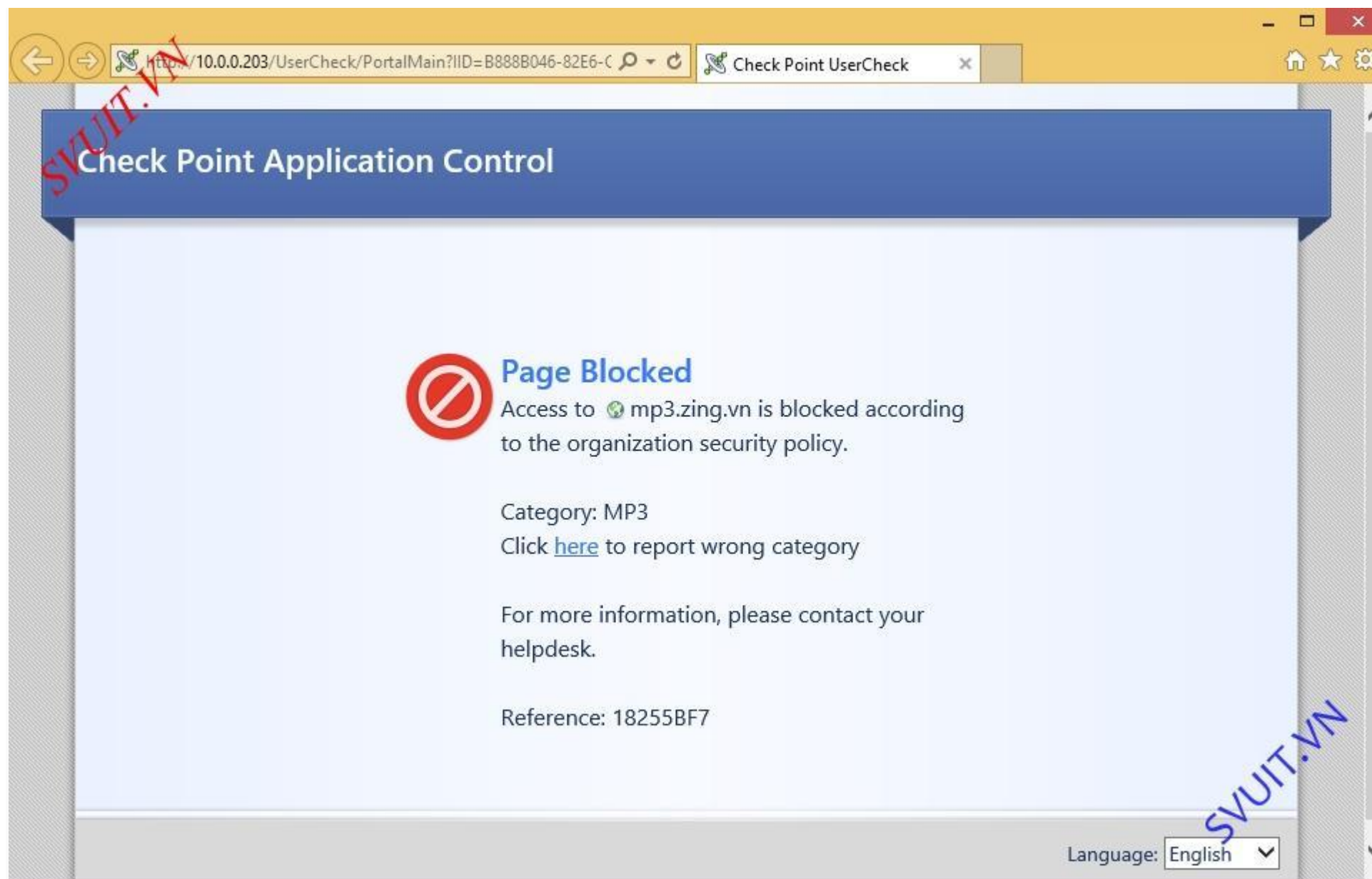
Progress

✓ Installation completed successfully

Close

SVUIT.VN

- Bây giờ người dùng thử truy cập vào trang mp3.zing.vn sẽ bao page Block do bị chặn bởi firewall



- Các bạn có thể xem rõ lại hành động của firewall trên Smartview tracker

Previous Next Copy Details

URL Filtering: Block

u1 (u1) was blocked access to mp3.zing.vn from 10.0.0.4 yesterday at 17:40:43

Details	
Name	* mp3.zing.vn (MP3)
Matched Category	MP3
All Categories	MP3
Risk	Unknown
URL	<a href="http://mp3.zing.vn/">http://mp3.zing.vn/</a> <a href="#">Copy</a>

User Check	
Message to User	Access to mp3.zing.vn is blocked according to... >>
Confirmation Scope	For each application
Frequency	1 days

Traffic	
Source	10.0.0.4 u1 (u1) svuit-pc@svuit.vn
Destination	120.138.69.80
Protocol	TCP tcp
Service	http (80)

Policy	
Action	Block
Rule Name	mp3.zin.vn
Policy Name	Standard
Policy Date	Mon Oct 26 17:39:31 2015
Policy Management	Firewall

More	
User Check	1
Client Type	Other: Mozilla/5.0 (Windows NT 6.3; WOW64; Tr... >>
Primary Category	MP3
Signature ID	20000003:1
Product Family	Network
Log ID	9999
Origin	Firewall
Number	41519
Type	Log
Information	---
Time	Oct 26, 2015 at 17:40:43
UserCheck ID	B888B046-82E6-C388-48E8-789818255BF7