

Cài đặt Check Point Gateway Security R77.20

Tổng quan:

Chuẩn bị 1 server (RAM: 2G; HDD: 20G; Network Interface: 3 Card), nếu ko có server thì cài lên Vmware cũng ok

Các bạn có thể tham khảo thêm:

Giới thiệu về CheckPoint:

<http://svuit.vn/showthread.php?686-Chapter-4-Gi%E1%BB%9Bi-thi%E1%BB%87u-Checkpoint>

Hướng dẫn cài CheckPoint Gateway Security R75

<http://svuit.vn/showthread.php?685-Lab-4-1-C%C3%A0i-%C4%91%E1%BA%B7t-Checkpoint-Gateway-R77>

Link download cho anh em nào muốn cài thử:

<https://drive.google.com/uc?id=0Byd5pXHPHDOYIJOdIB1bVNRMTg&export=download>

Link này rất khó tìm, bạn nào có tài khoản VIP hoặc là đối tác của CheckPoint mới có để download từ website của CheckPoint 😊

Quá trình cài đặt:

Quá trình cài đặt cũng rất đơn giản, các bạn chỉ cần làm theo các bước chỉ dẫn trên hình là ok 😊

Welcome to Check Point Gaia R77.20

Install Gaia on this system

Do not install Gaia. Boot from local drive

Install Gaia on a system listed in sk77660

svuit.com

Press [Tab] to edit options



Check Point™
Software Technologies LTD.

GAiA

Starting Installation
Please wait while installation starts...

svuit.com

Check Point Gaia R77.20

Welcome
This process will install the Check Point Gaia R77.20
operating system and associated applications.

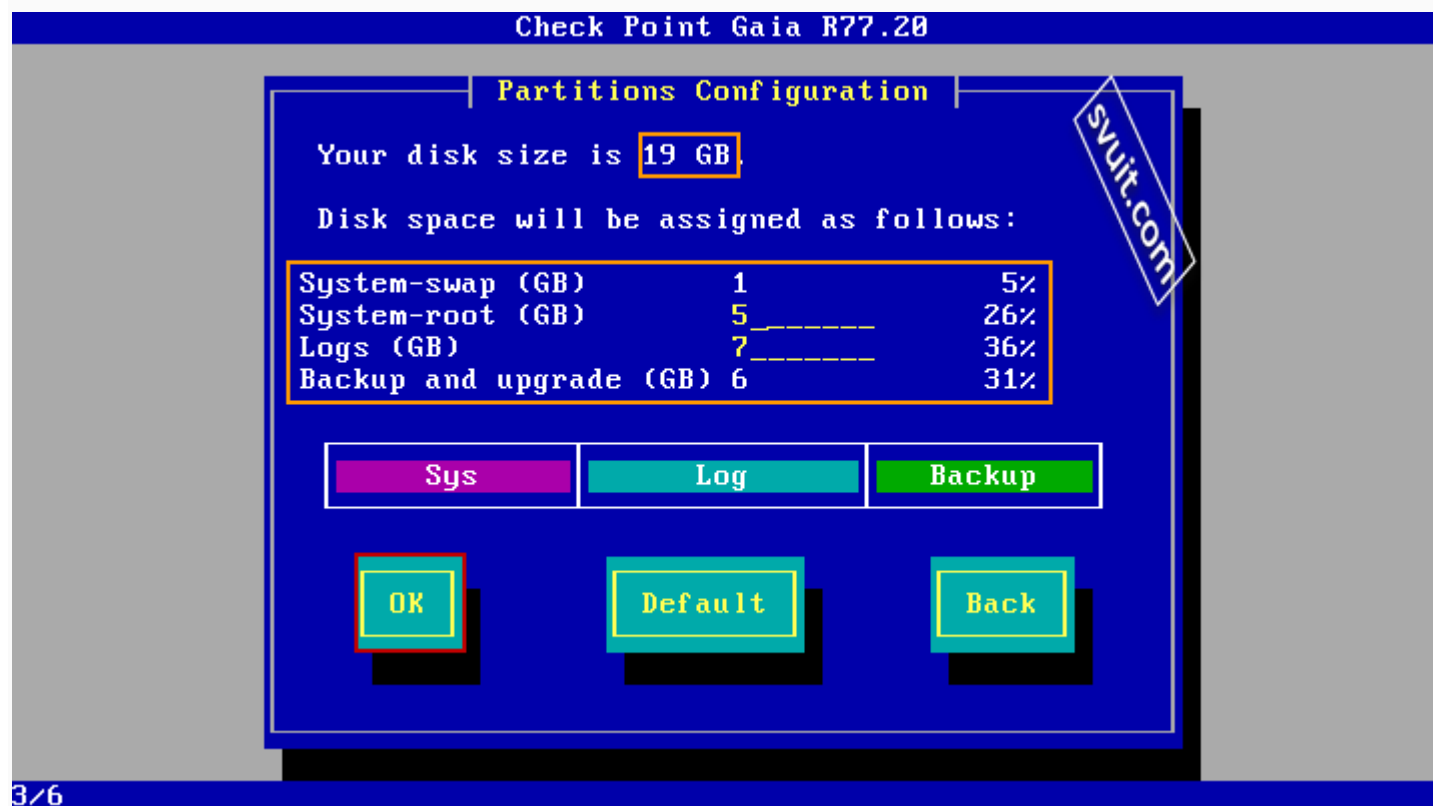
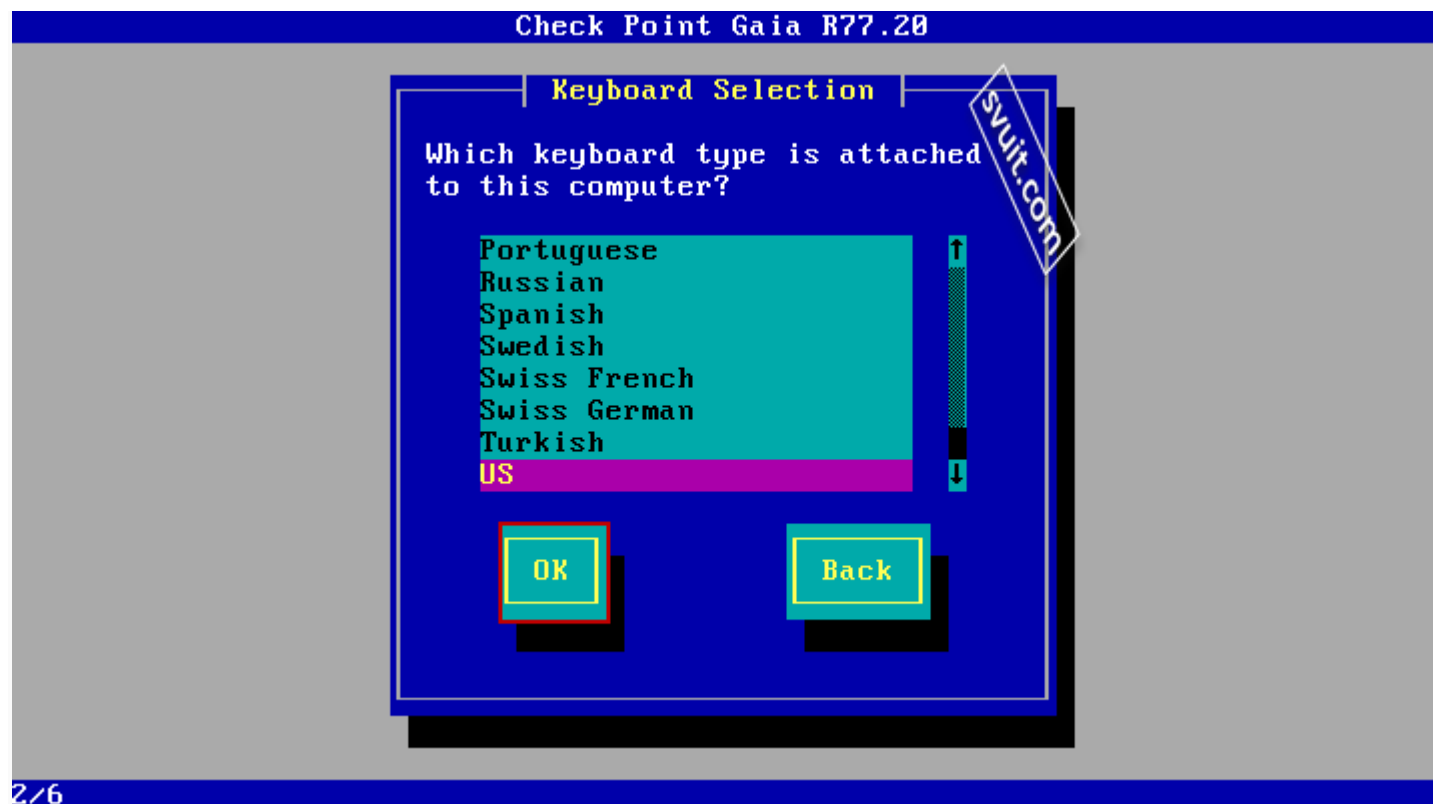
Do you wish to proceed with the installation?

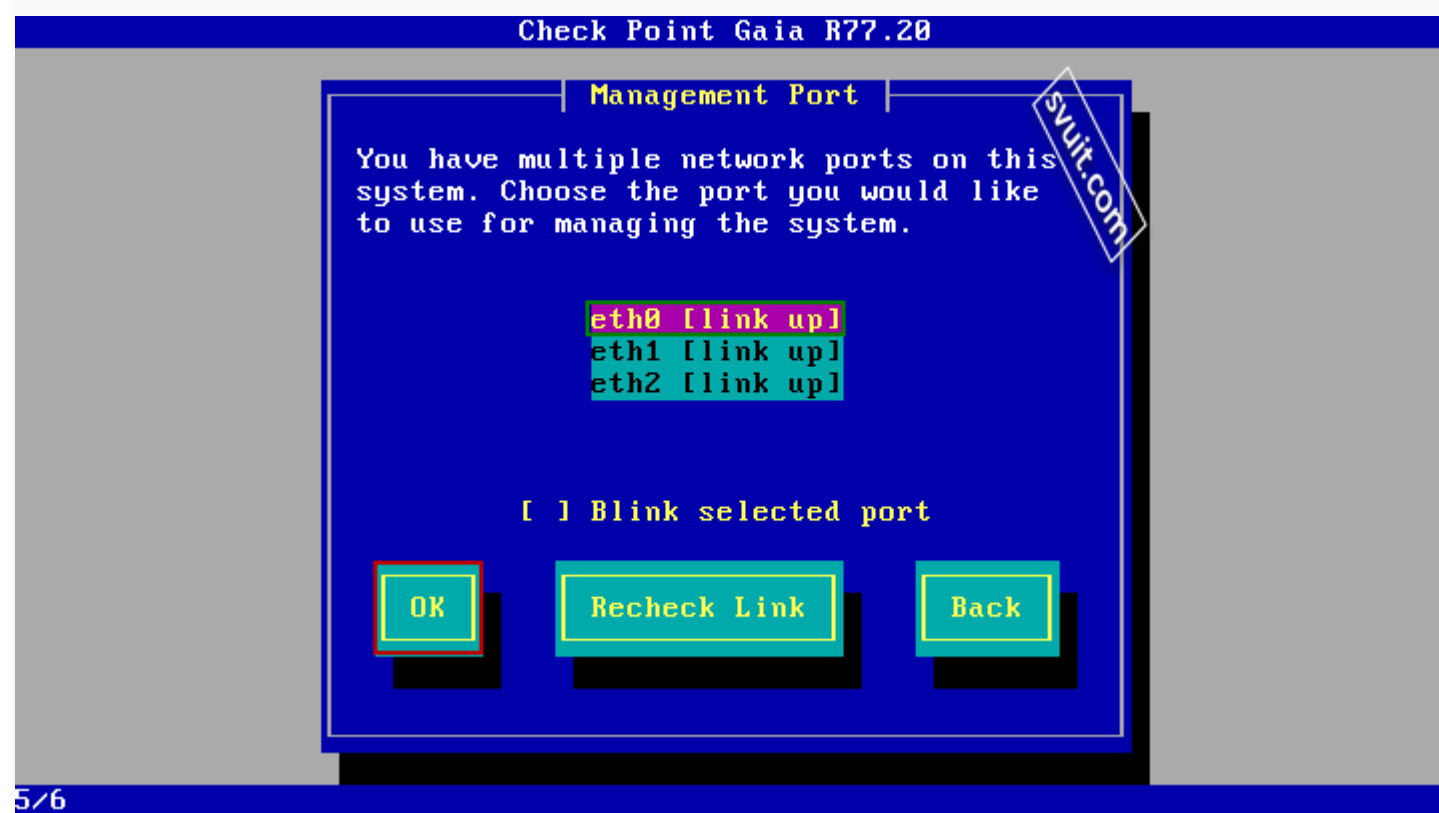
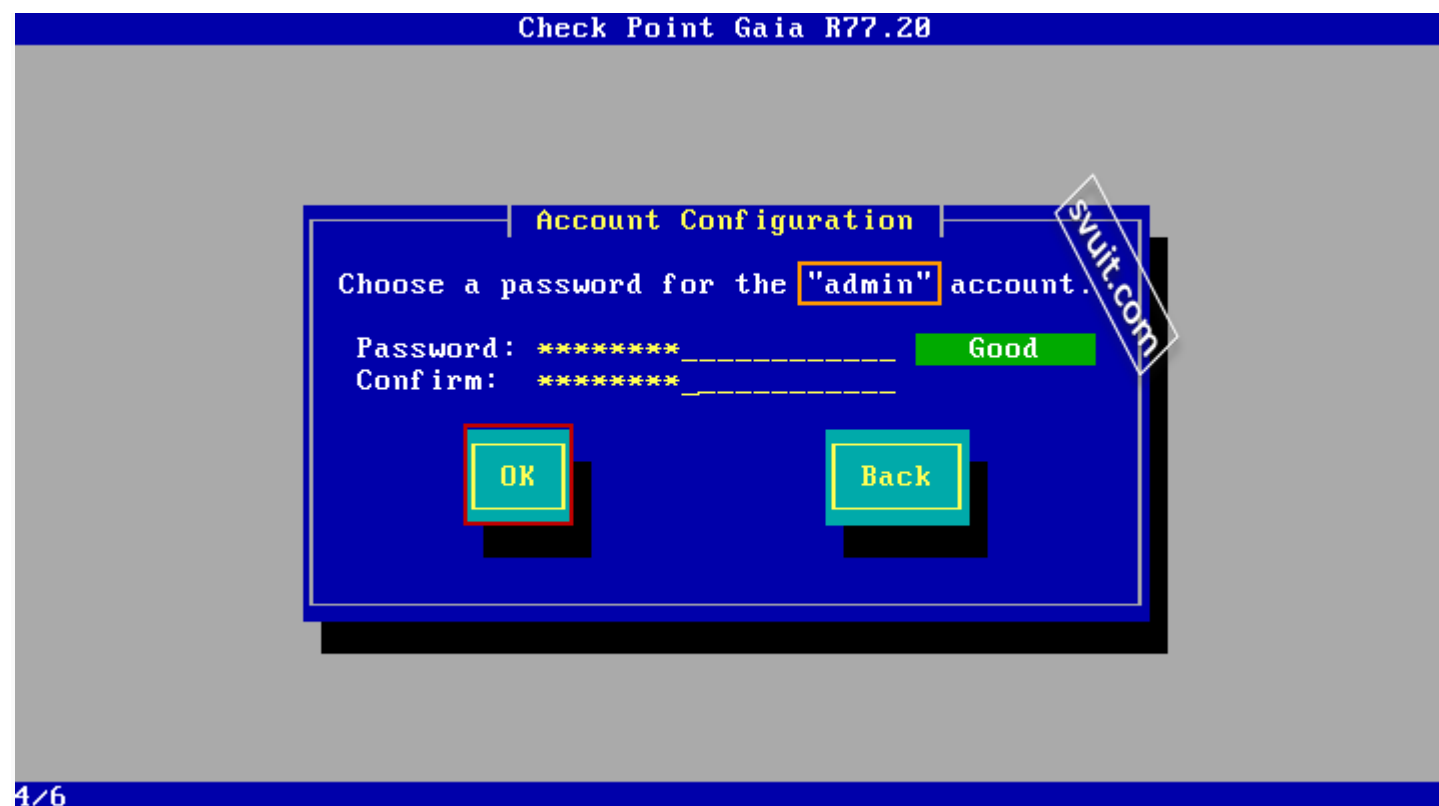
OK

Machine Info

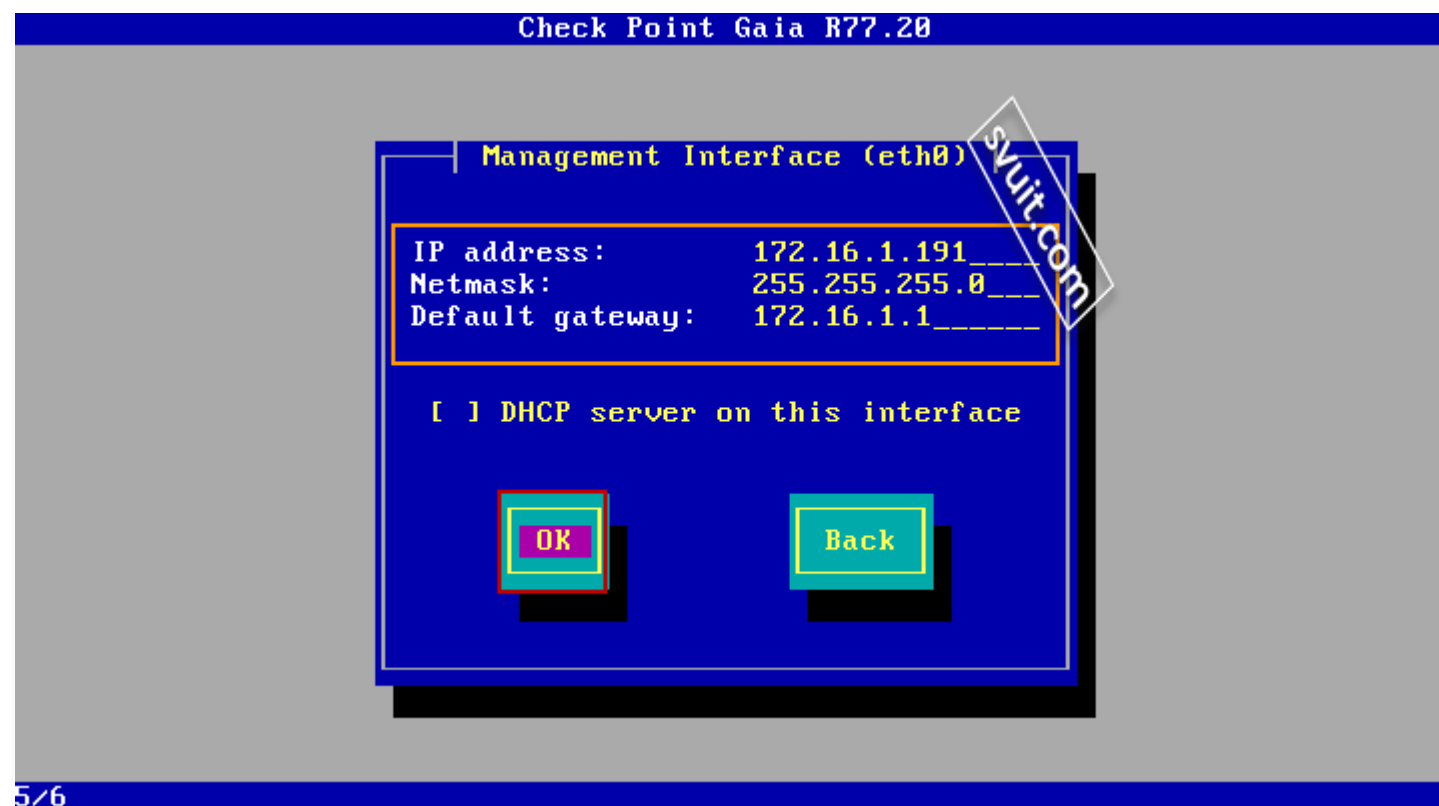
Cancel

svuit.com

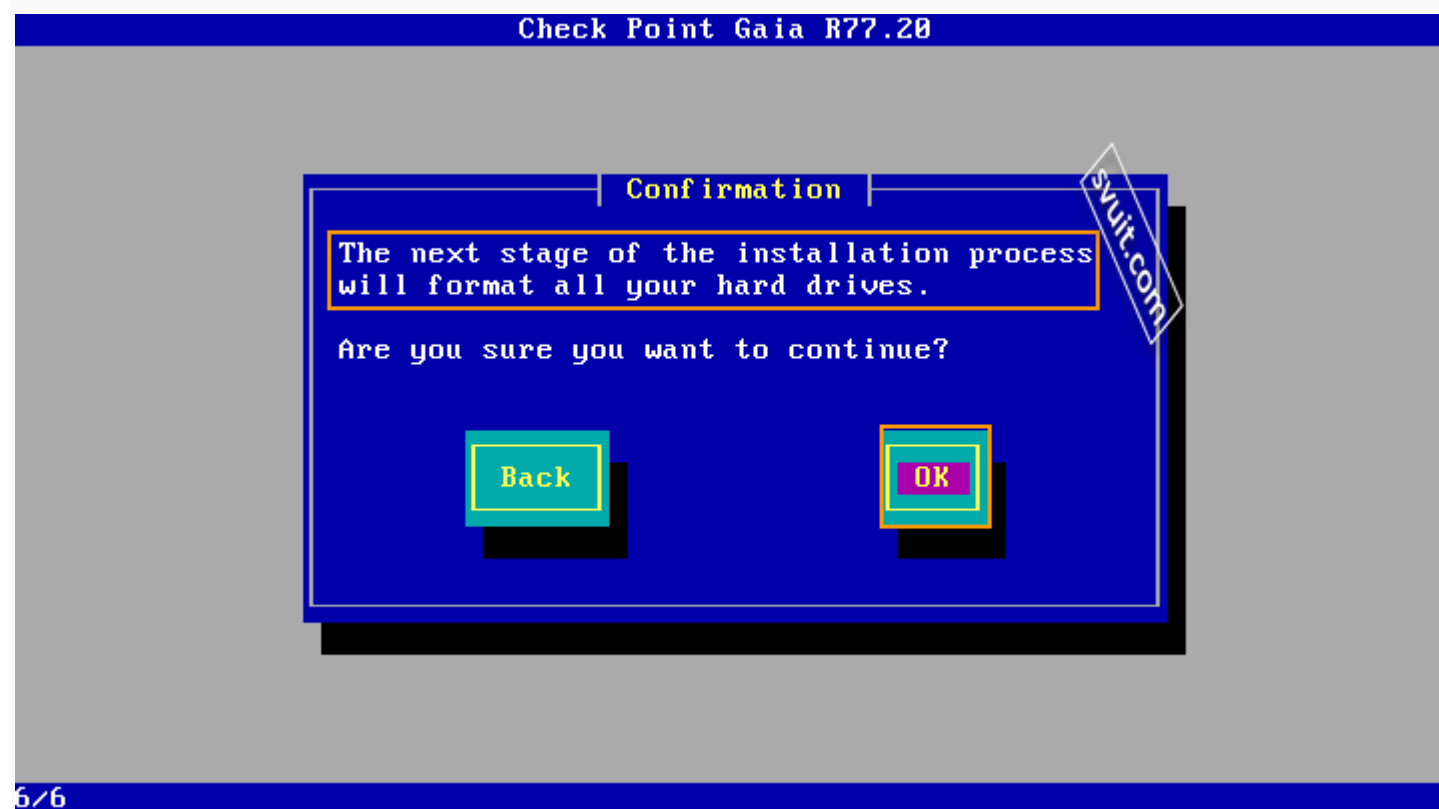




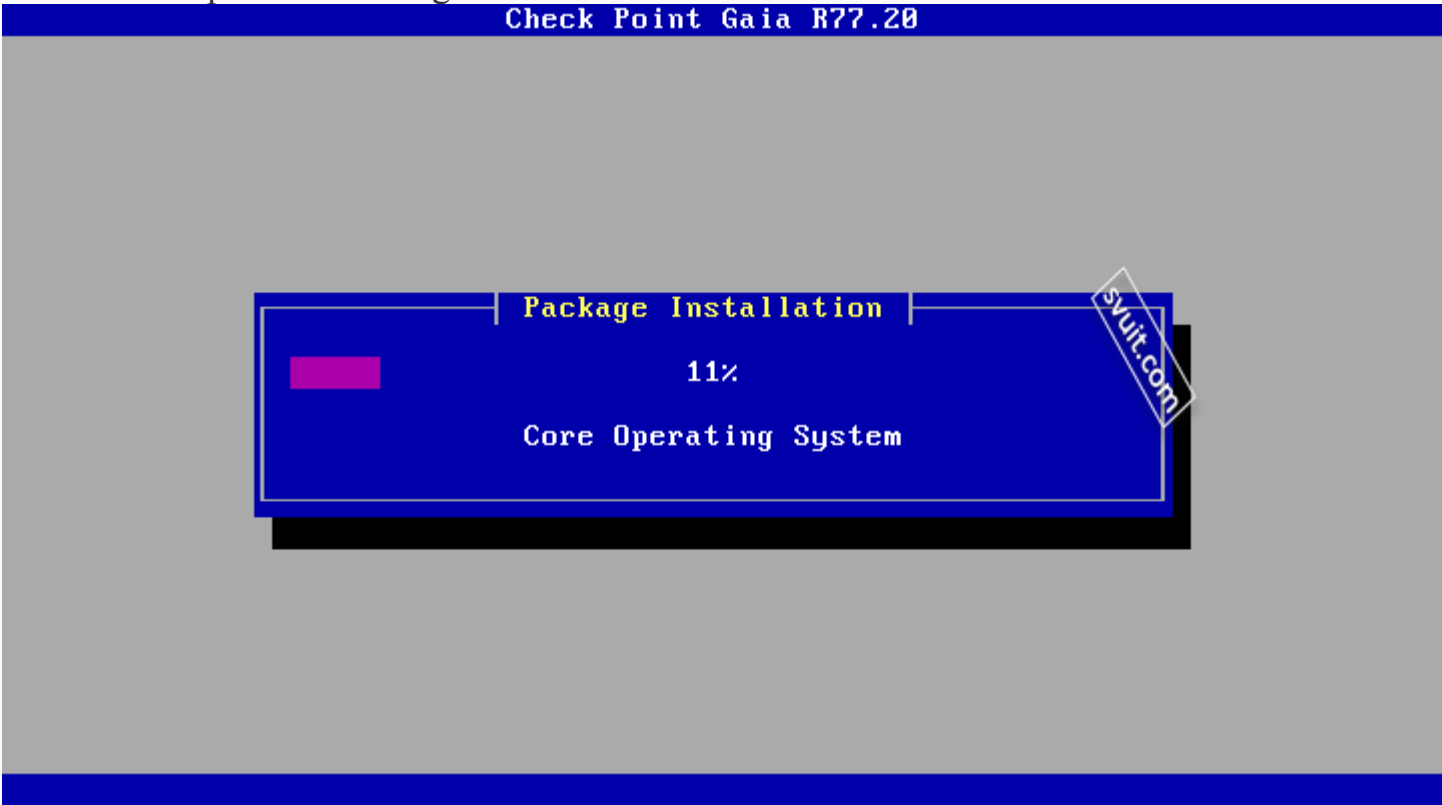
Cấu hình địa chỉ IP cho Management Interface (eth0)



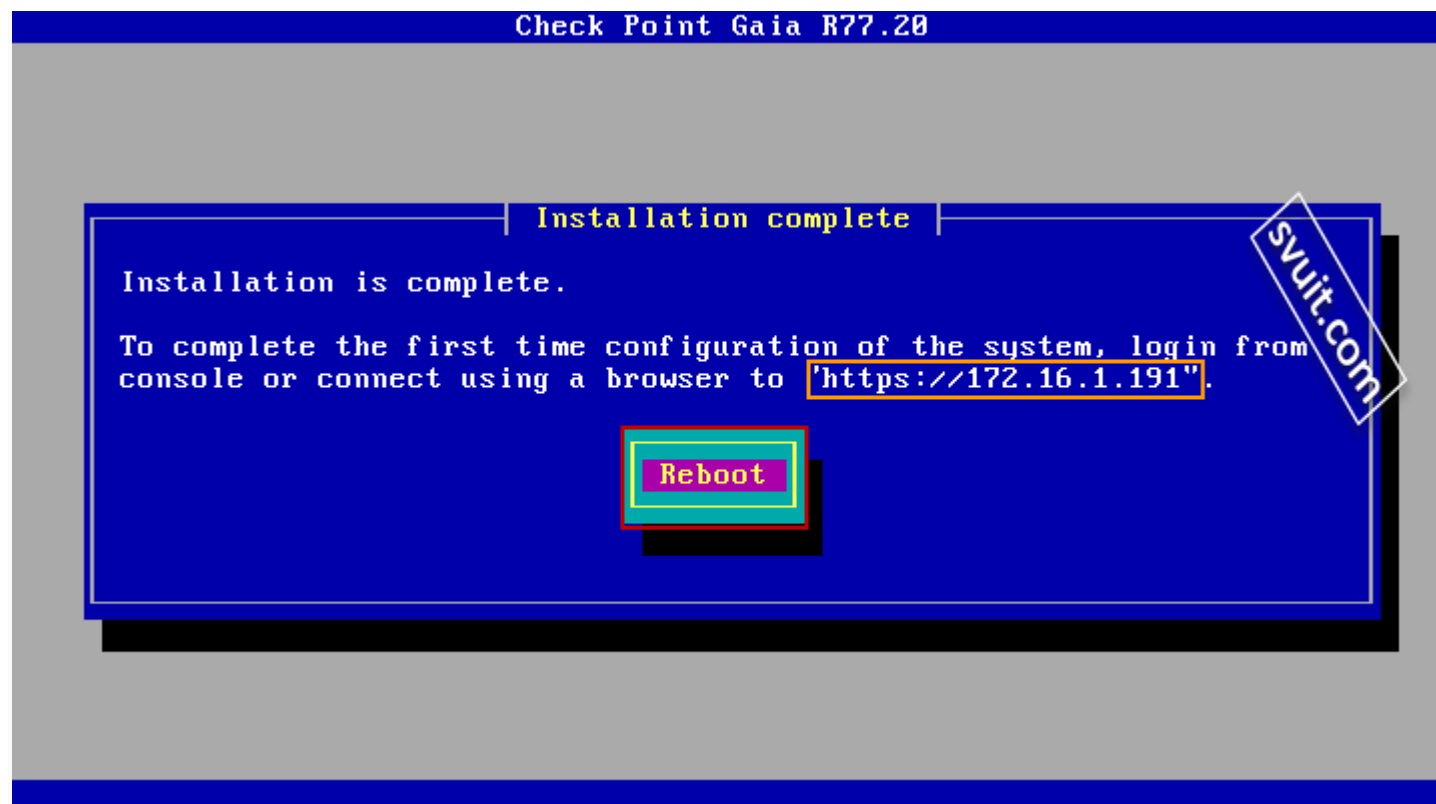
Cảnh báo sẽ format ổ đĩa cứng cứng, nếu ổ cứng còn trống thì bạn ko cần phải lo ngại, cứ ok là xong 🙄



Bây giờ quá trình cài đặt sẽ bắt đầu...
Khoản 15-30 phút sẽ cài xong...

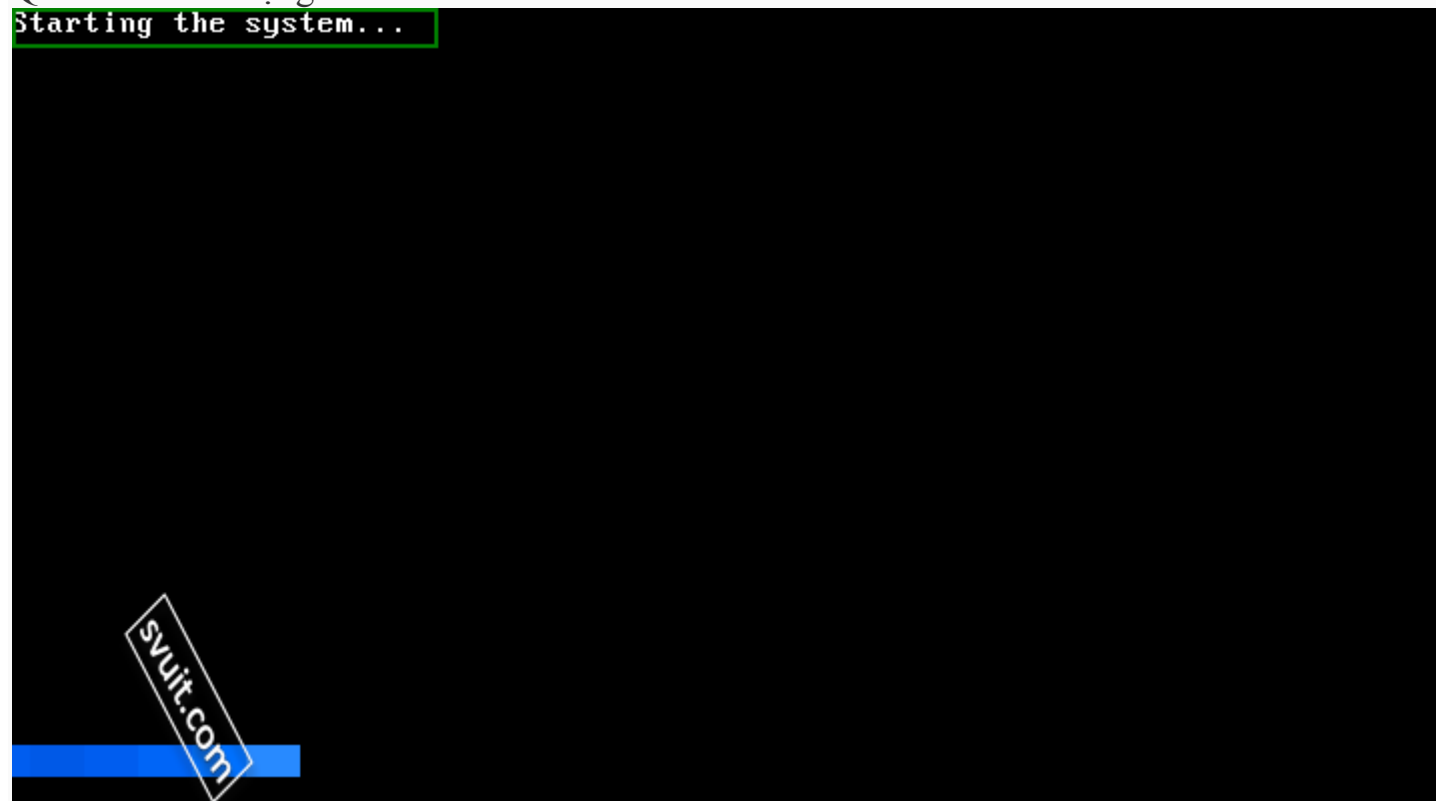


Sau khi cài xong bạn sẽ nhận được một màn hình thông báo, yêu cầu Reboot lại hệ thống, bạn để ý sẽ thấy đường dẫn để truy cập vào giao diện web để quản trị: <https://172.16.1.191>

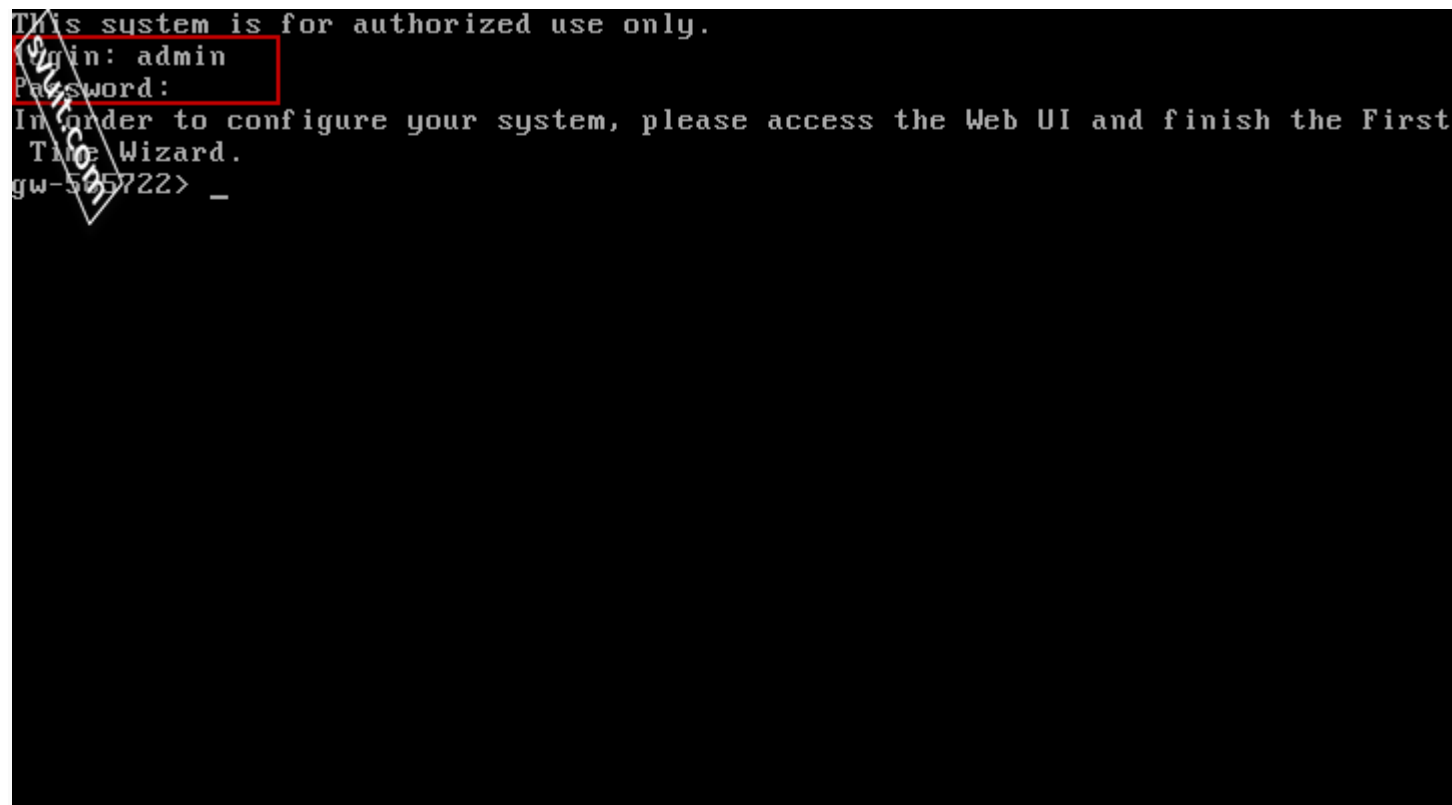


Quá trình khởi động server

Starting the system...



Khi khởi động bạn đăng nhập bằng tài khoản admin vào hệ thống, đây là giao diện console cho phép quản trị bằng dòng lệnh...

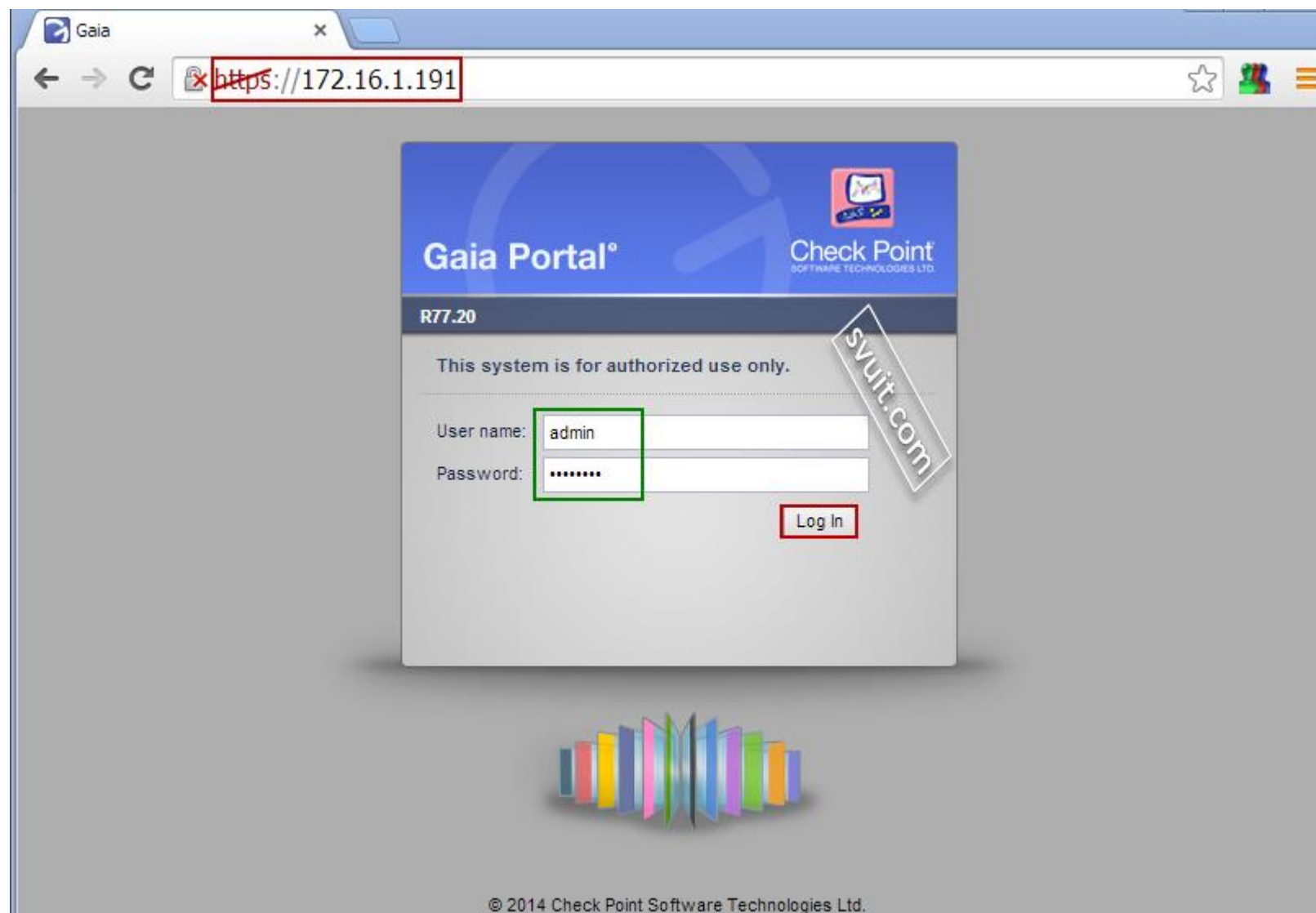


OK vậy là bạn đã cài xong 1 em Check Point Gateway Security R77.22 (phiên bản mới nhất).
Bạn được dùng thử miễn phí, full tính năng trong vòng 15 ngày...

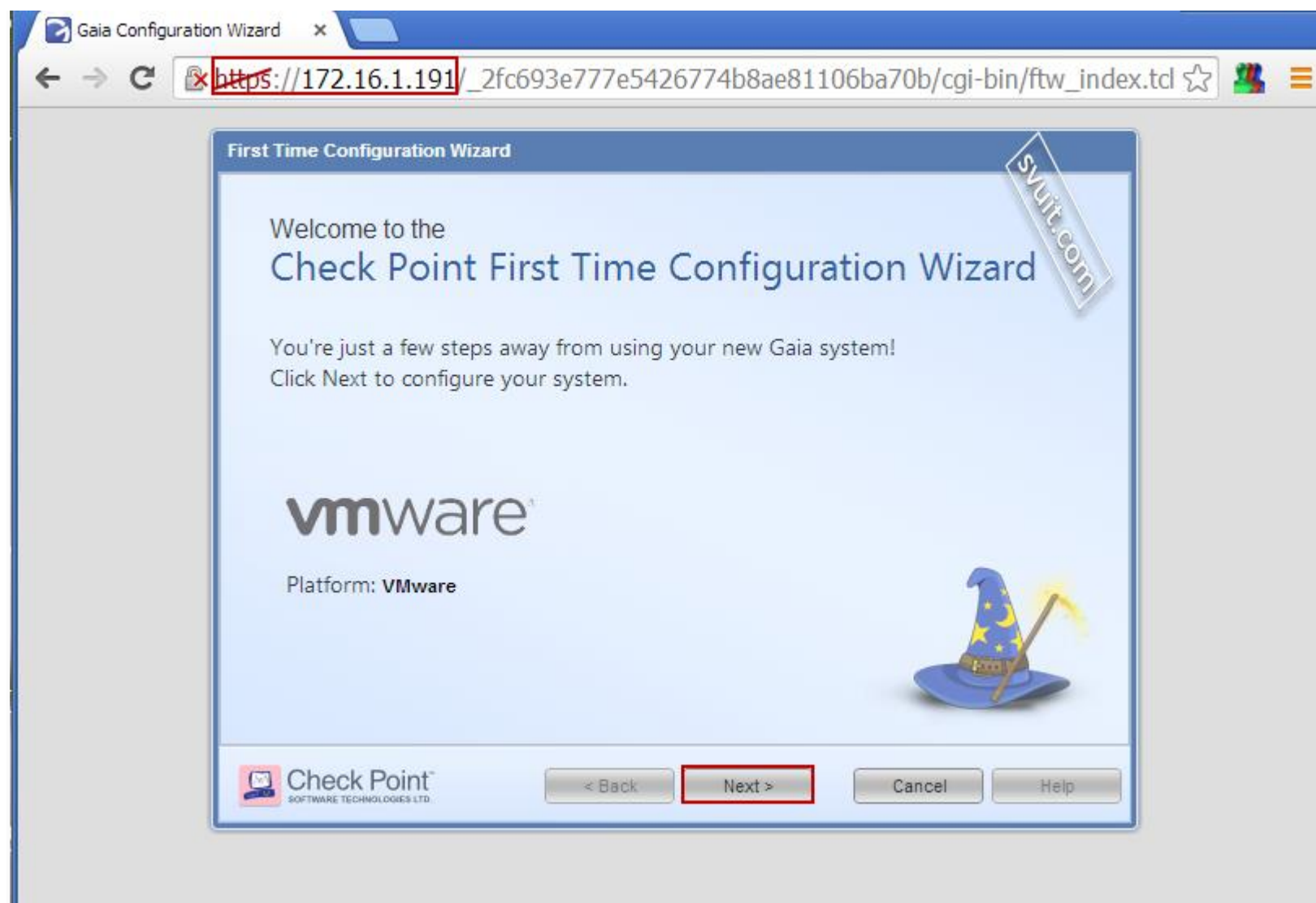
Cài đặt cấu hình ban đầu cho Check Point Gateway Security R755.22

Dùng trình duyệt (chrome, firefox, ie) truy cập web vào link <https://172.16.1.191> để bắt đầu quá trình cài đặt cấu hình ban đầu...

Đăng nhập bằng tài khoản admin:



Quá trình cài đặt cấu hình ban đầu cũng khá đơn giản, chỉ việc next,... là xong 😊



First Time Configuration Wizard

Deployment Options



Clean Install

- ☒ Continue with Gaia R77.20 configuration
- ☐ Install a version from Check Point Cloud
- ☐ Install from USB device

Recovery

- ☐ Import existing snapshot ?



< Back

Next >

Cancel

Help

First Time Configuration Wizard

Management Connection



Interface:

eth0

Configure IPv4:

Manually

IPv4 address:

172 . 16 . 1 . 191

Subnet mask:

255 . 255 . 255 . 0

Default Gateway:

172 . 16 . 1 . 1

Configure IPv6:

Off

IPv6 Address:

Subnet:

Default Gateway:



< Back

Next >

Cancel

Help

First Time Configuration Wizard

Connection to UserCenter

Configure the interface to connect to Check Point UserCenter (optional) ?

Interface:

Configure IPv4:

IPv4 address:


Subnet mask:

Configure IPv6:

IPv6 Address:

Subnet:

UserCenter connection is required for license activation

 Check Point™
SOFTWARE TECHNOLOGIES LTD.

< Back **Next >** Cancel Help

Cấu hình Host Name, DNS Server, Domain Name.

First Time Configuration Wizard

Device Information



Host Name:

svuit-hcm-gw

Domain Name:

svuit.com

Primary DNS Server:

8.8.8.8

Secondary DNS Server:

8.8.4.4

Tertiary DNS Server:

Proxy Settings

☐ Use a Proxy server

Address:

Port:

8080



< Back

Next >

Cancel

Help

First Time Configuration Wizard

Date and Time Settings



☒ Set time manually:

Date:

Thursday, October 02, 2014

Time:

20 : 08

Time Zone:

Bangkok, Asia (GMT +7:00)

☐ Use Network Time Protocol (NTP):

Primary NTP server:

Example: pool.ntp.org

Version:

1

Secondary NTP server:

Version:

1

Time Zone:

Bangkok, Asia (GMT +7:00)

< Back

Next >

Cancel

Help

First Time Configuration Wizard

Installation Type



☒ Security Gateway or Security Management

☐ Multi-Domain Server

< Back

Next >

Cancel

Help

First Time Configuration Wizard

Products

Check Point
SOFTWARE TECHNOLOGIES LTD.

Products

☒ Security Gateway
☒ Security Management

Clustering

☐ Unit is a part of a cluster, type: ClusterXL
Define Security Management as: Primary

☒ Automatically download Blade Contracts and other important data (highly recommended)
For more information click [here](#)

< Back Next > Cancel Help

Bạn lưu ý, đây là bước tạo user Administrator cho **Security Management**, user này sẽ được dùng để login vào **Smart Console** để quản trị, user "**admin**" ko login vào được **Smart Console**

First Time Configuration Wizard

Security Management Administrator

Check Point
SOFTWARE TECHNOLOGIES LTD.

Administrator Name: svuit

New Password:

Confirm Password:

Good

< Back Next > Cancel Help

Chọn giới hạn cho phép địa chỉ IP, hoặc Network nào được phép login vào **Sercurity Management**,

First Time Configuration Wizard

Security Management GUI Clients

GUI clients can log into the Security Management from:

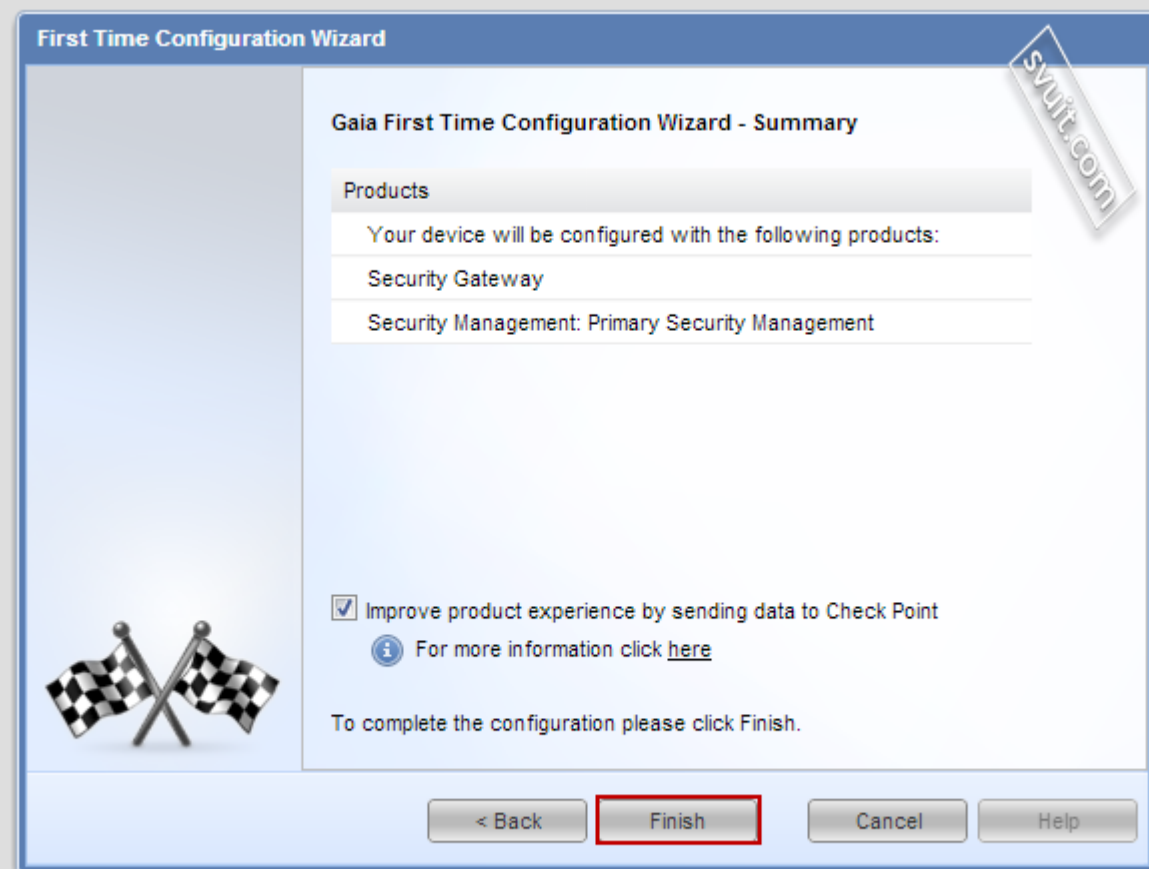
☒ Any IP Address

☐ This machine
IP address: 172.16.1.120

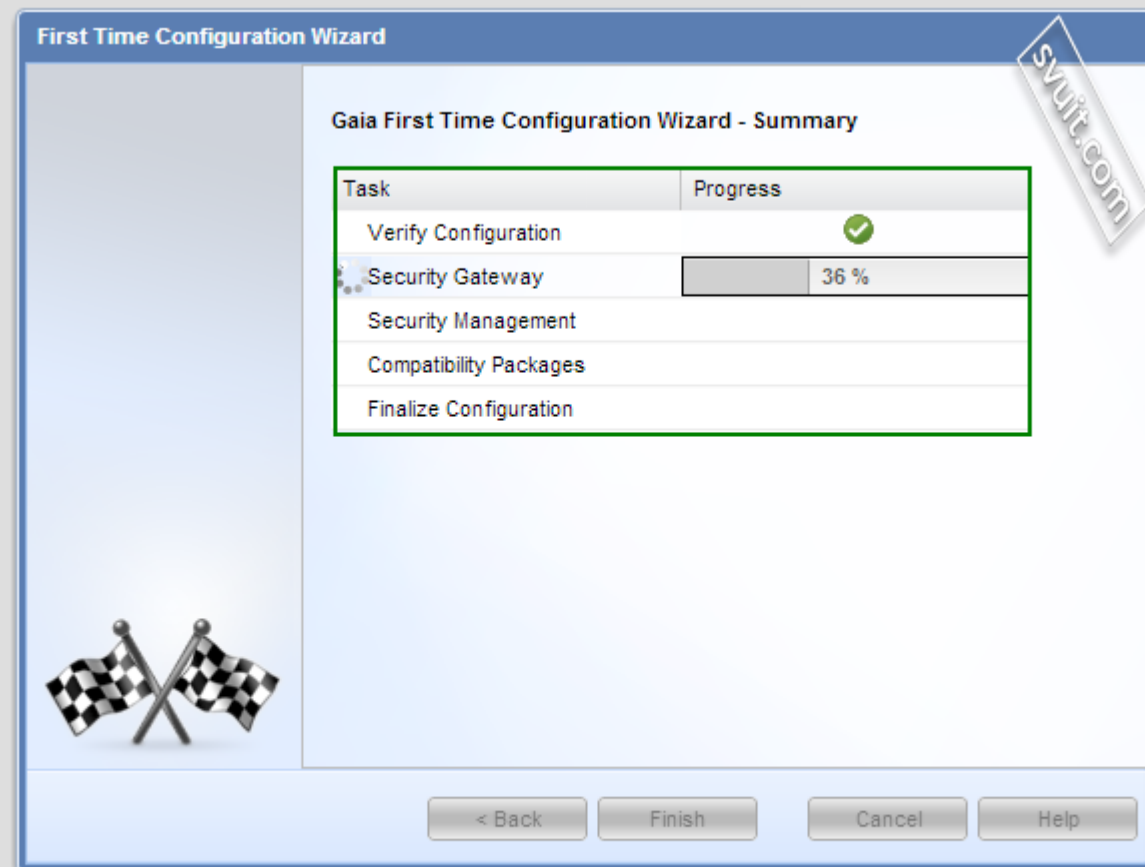
☐ Network
IP Address:
Subnet:

☐ Range of IPv4 addresses:
 -

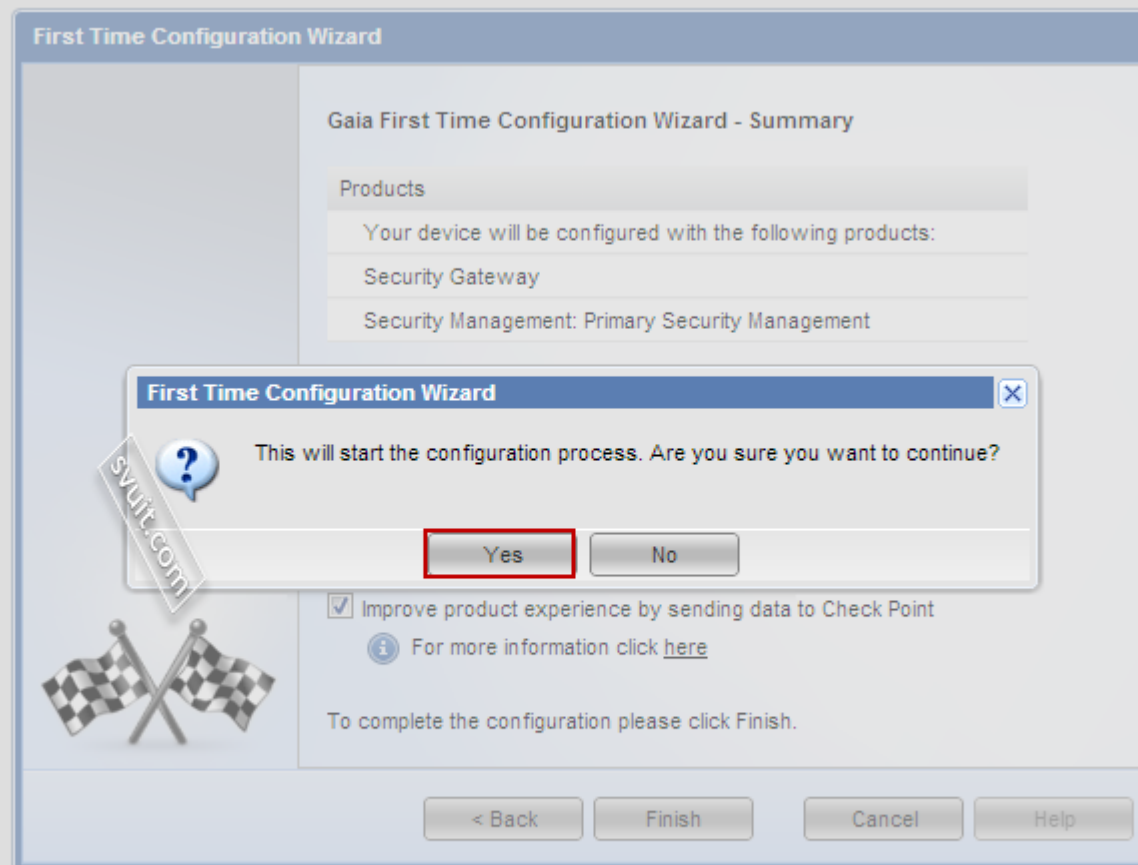
< Back Next > Cancel Help



Bây giờ là lúc cài đặt và lưu cấu hình, bạn đợi khoản 5-10 phút là xong...



Sau khi cài xong sẽ khởi động lại server
Chọn "yes" để khởi động lại...



Starting the system..._

svuit.com

Bạn đăng nhập lại...



Bạn sẽ vào được màn hình quản trị của Check Point..

Gaia

admin Sign Out

svuit-hcm-gw

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
- System Configuration
- System Logging
- Network Access
- Certificate Authority

Manage Software Blades using SmartConsole

Download Now!

System Overview

Check Point Security Gateway | R77.20

Kernel: 2.6.18-92cp

Edition: 32-bit

Build Number: 124

System Uptime: 3 minutes

Platform: VMware

Network Configuration

Name	IPv4 Address	IPv6 Address	Link Status
eth0	172.16.1.191	-	Up
eth1	-	-	Down
eth2	-	-	Down
lo	127.0.0.1	-	Up

Blades

- Firewall
- IPS
- IPSec VPN
- URL Filtering
- Anti-Spam and Mail

Cài đặt Smart Console và xem qua giao diện quản trị **Security Management**

Download Source cài đặt:

Gaia

admin Sign Out

svuit-hcm-gw

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
- System Configuration
- System Logging

Manage Software Blades using SmartConsole **Download Now!**

System Overview

Check Point Security Gateway | R77.20

Kernel: 2.6.18-92cp
Edition: 32-bit
Build Number: 124
System Uptime: 23 minutes

Platform: VMware

Network Configuration

Name	IPv4 Address	IPv6 Address	Link Status
eth0	172.16.1.191	-	Up
eth1	-	-	Down
eth2	-	-	Down
lo	127.0.0.1	-	Up

Blades

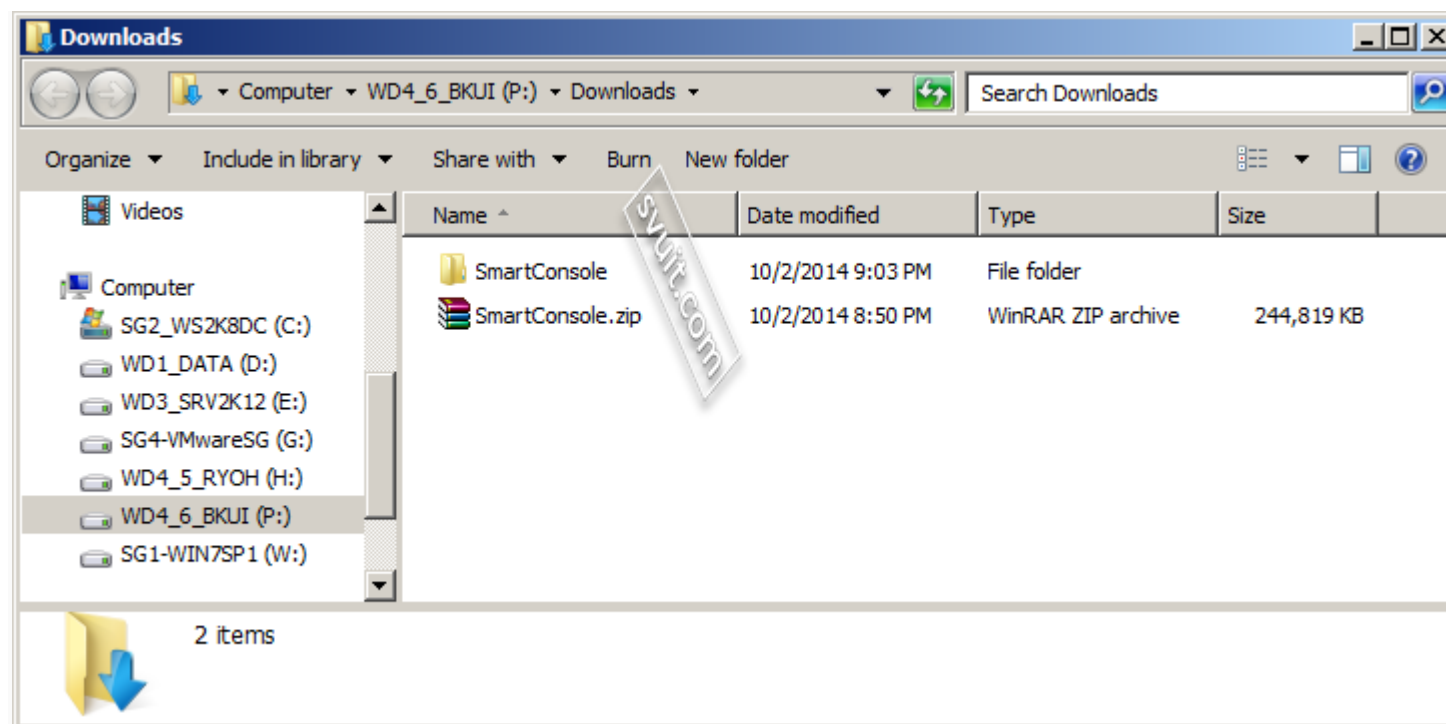
- Firewall
- IPS
- IPSec VPN
- URL Filtering
- Anti-Spam and Mail

172.16.1.191/.../home.tcl

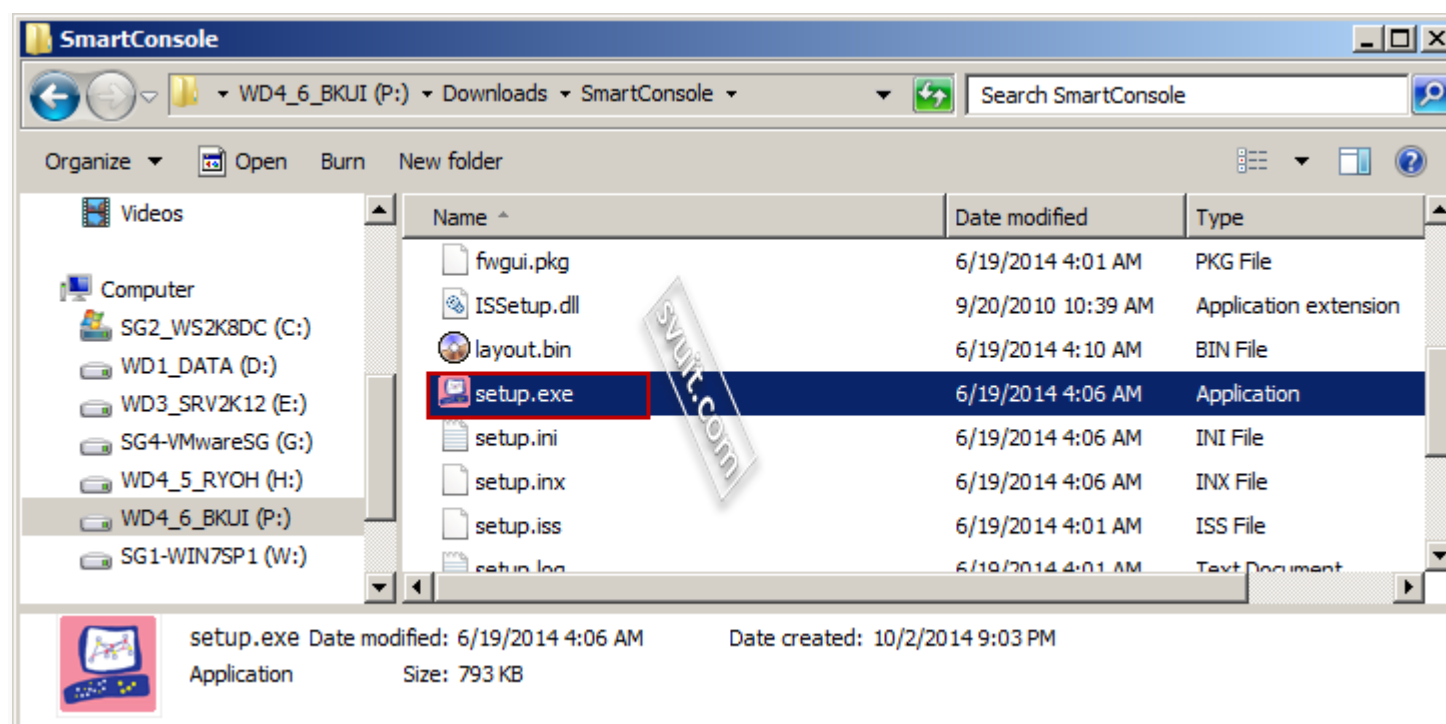
SmartConsole.zip

Show all downloads...

Unzip...

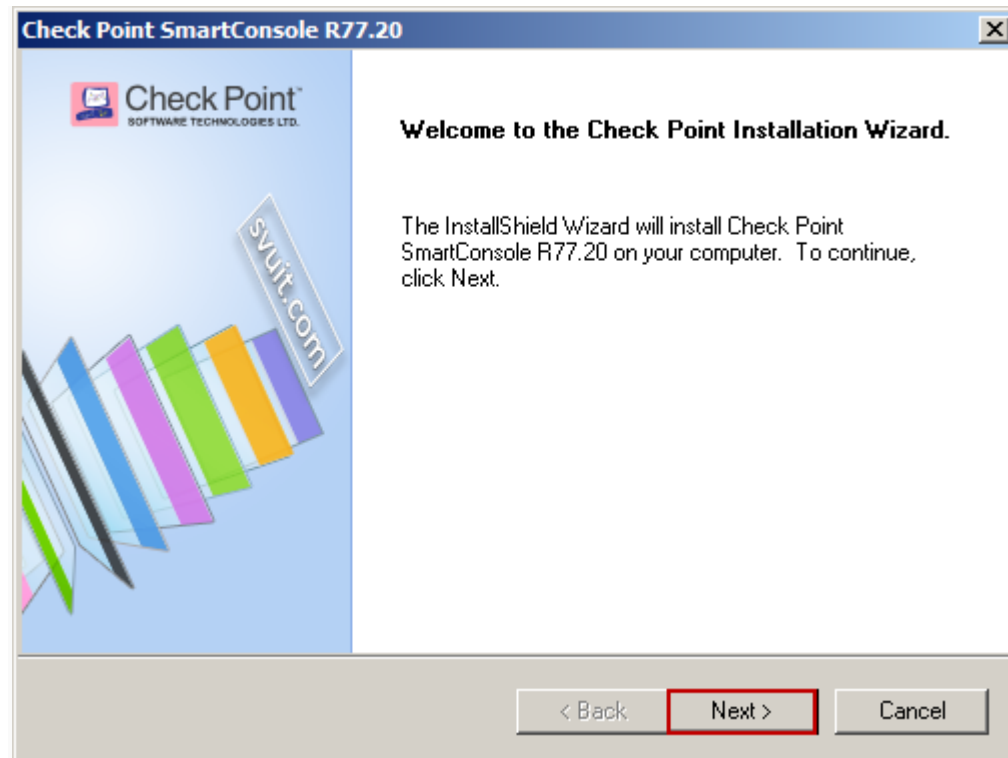
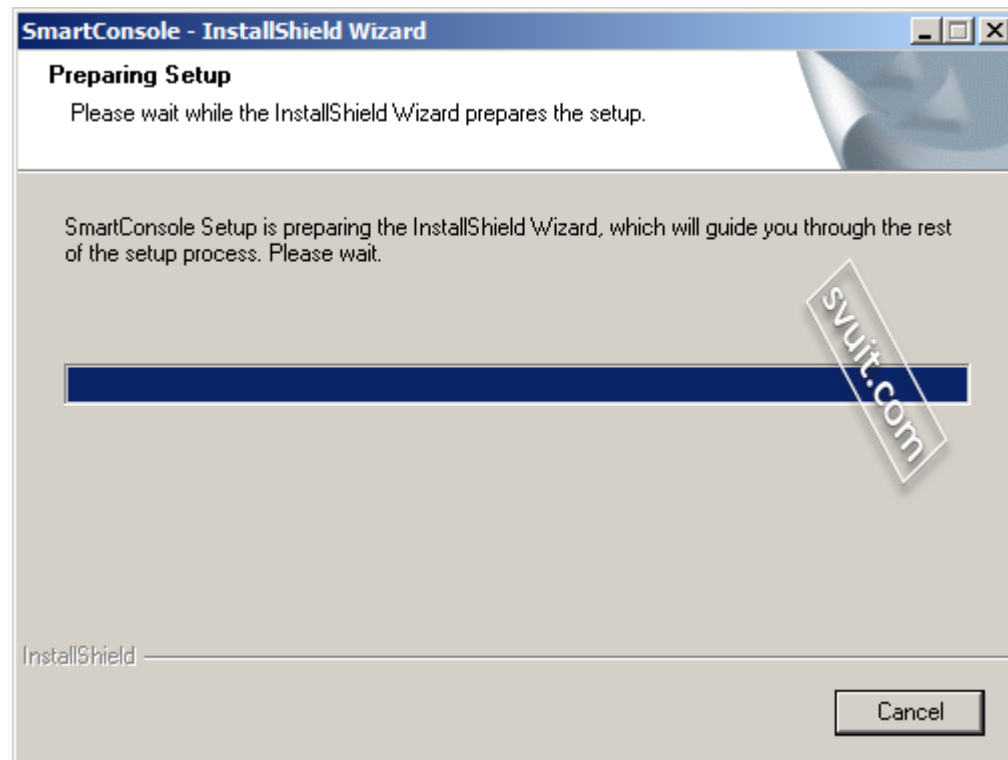


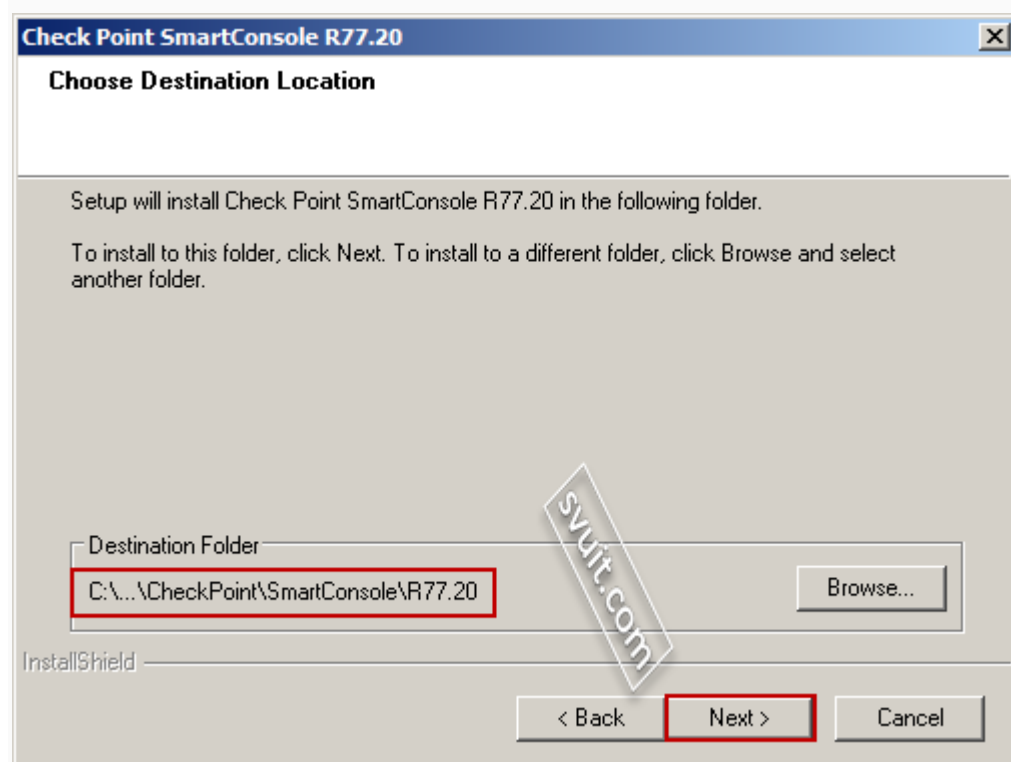
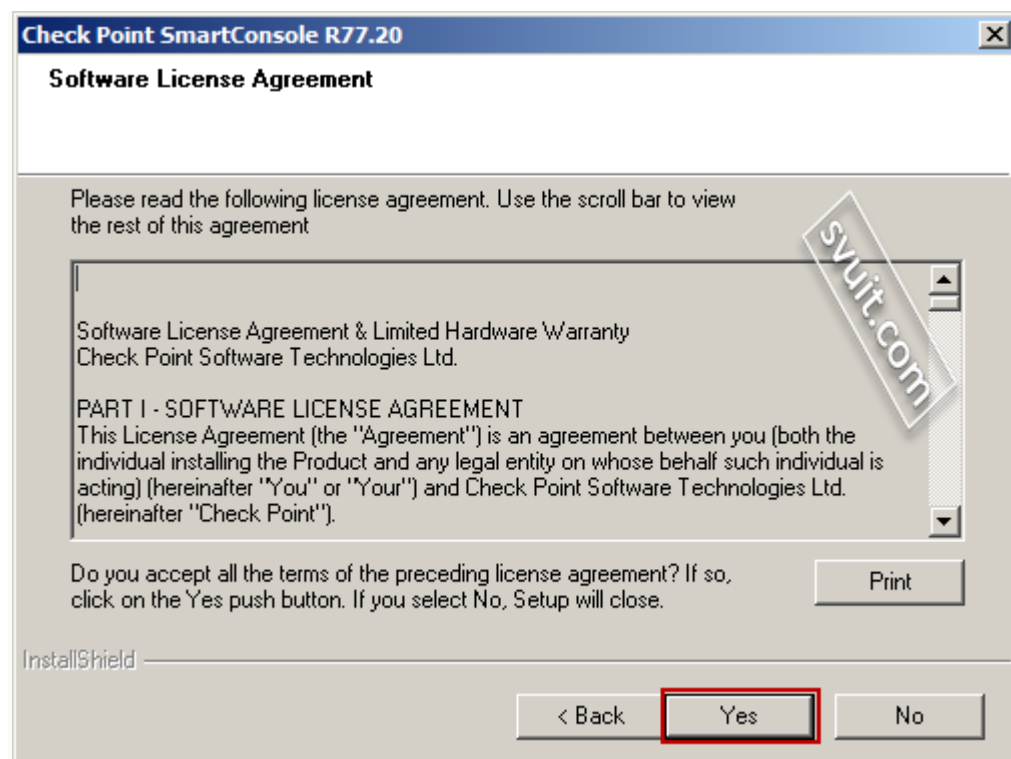
Chạy file cài đặt "setup.exe"

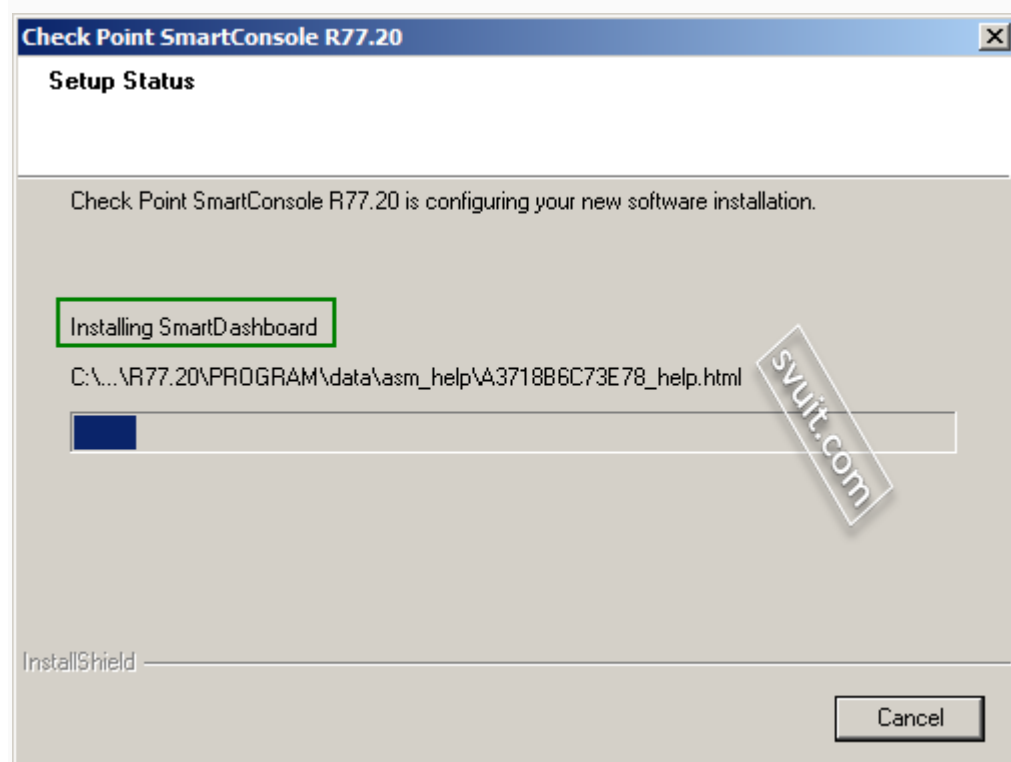
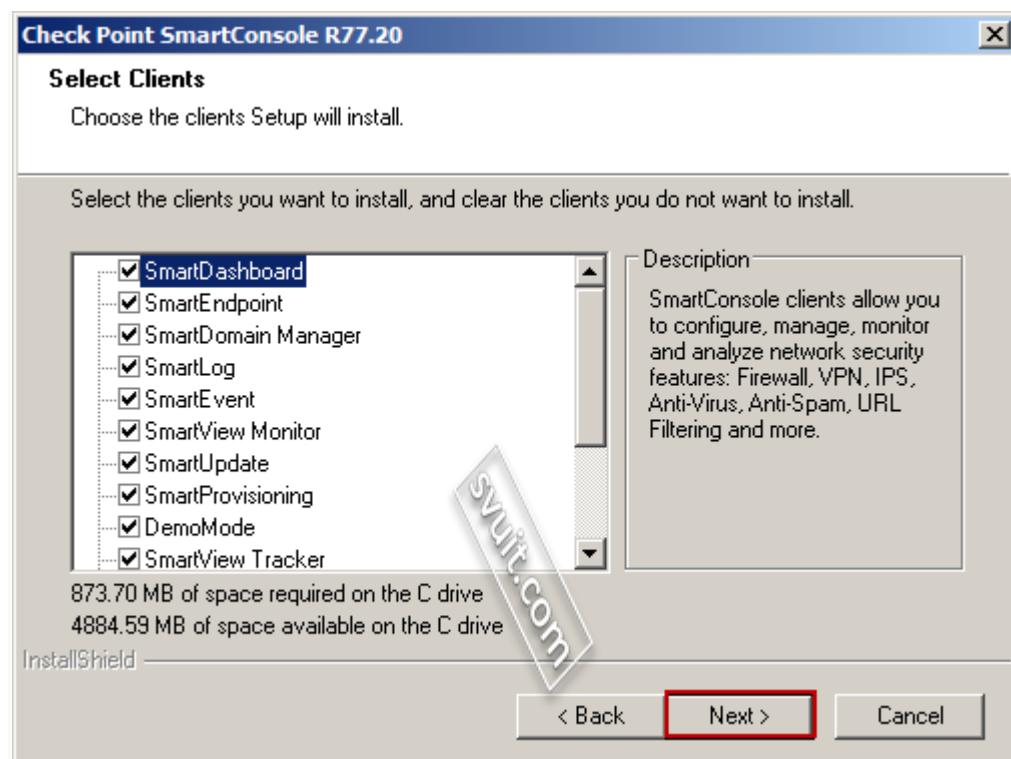


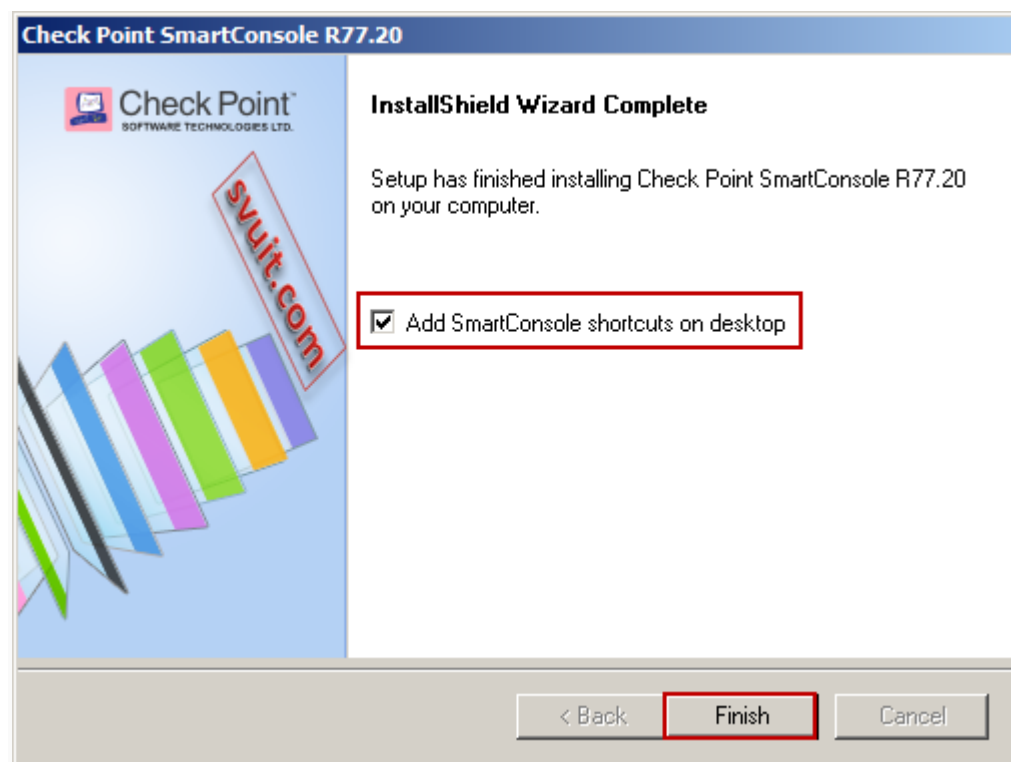
Quá trình cài sẽ bắt đầu...

Cài đặt Smart Console cũng rất là đơn giản, Bạn chỉ cần nhấn Next, ...là OK 😊

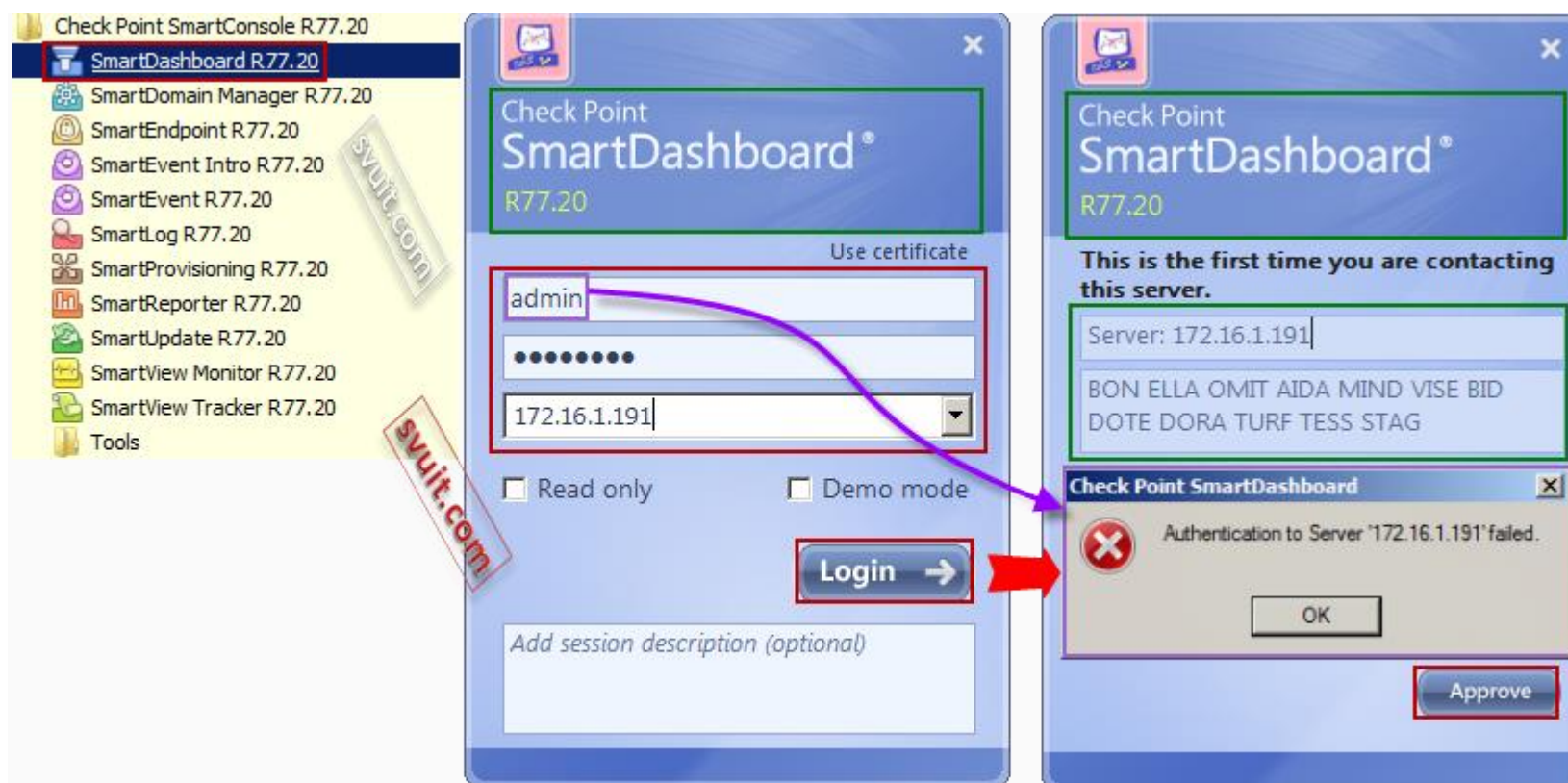




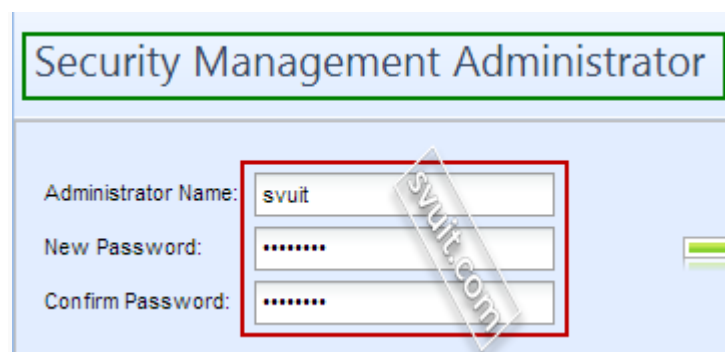




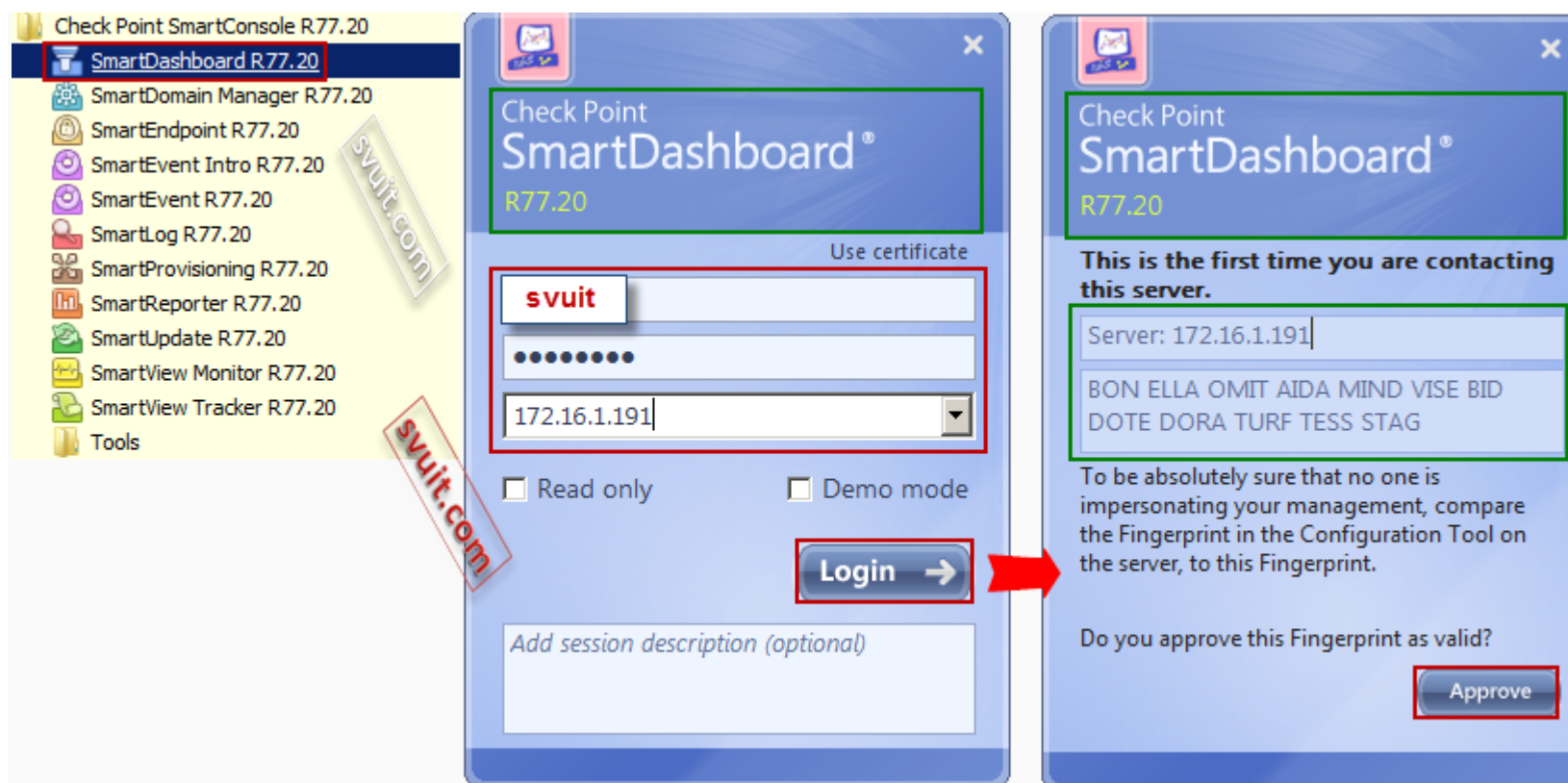
Sau khi cài xong bạn login vào Management Security
Đầu tiên bạn thử dùng tài khoản "**admin**" để login....
Bạn sẽ nhận được thông báo lỗi 🙄



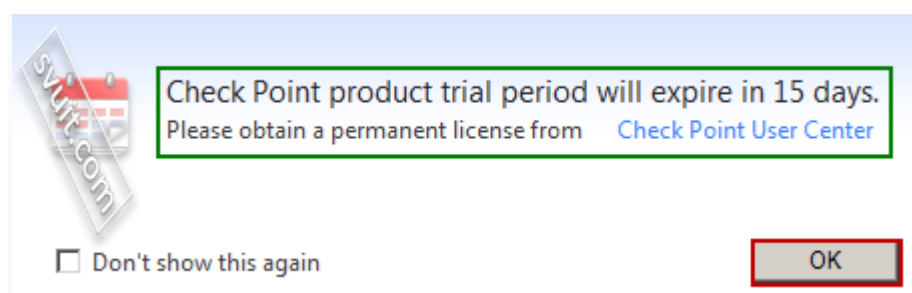
Bạn nhớ lại trong phần cài đặt cấu hình ban đầu có một bước tạo user cho Security Management.
User này sẽ được dùng để login vào vào giao diện Smart Console...



Login bằng tài khoản "**svuit**"
Login thành công...



Trong quá trình login bạn nhận được thông báo, cho biết thời hạn dùng thử của CheckPoint là 15 ngày...



Vậy là xong, bạn đã vào được giao diện quản trị Smart Console

Sau đây là một số hình ảnh của giao diện quản trị Smart Console:

172.16.1.191 - Check Point SmartDashboard R77.20 - Standard

Firewall

Application & URL Filtering

Data Loss Prevention

IPS

Threat Prevention

Anti-Spam & Mail

Mobile Access

IPSec VPN

More

Overview

Policy

NAT

Track Logs

Analyze & Report

svuit.com

Overview

World's most proven Firewall solution, featuring the most adaptive and intelligent inspection technology.

My Organization

1 Security Gateway

	IP Address	Version	Policy Package
svuit-hcm-gw	172.16.1.191	R77.20	Not Install

Top Gateways

Display by: Concurrent Connections

Network Objects

Check Point

Nodes

Networks

Groups

Address Ranges

Dynamic Objects

Objects List

Identity Awareness

SmartWorkflow

Type to Search

Network Objects

Action...

Name	IPv4	IPv6	NAT Properties	Version	Net Mask	Comment
svuit-hcm-gw	172.16.1.191	N/A	None	R77.20	N/A	
CP_default_Office_Mode_addre...	172.16.10.0	N/A	Hide behind: All	N/A	255.255.25...	Used as a default for Office Mode. If deleted,...
All_Internet	0.0.0.0 - 255.2...	N/A	None	N/A	N/A	All Internet Addresses
LocalMachine_Loopback	127.0.0.1 - 127...	N/A	None	N/A	N/A	Local machine loopback address range
AuxiliaryNet	N/A	N/A	N/A	N/A	N/A	
CPDShield	N/A	N/A	N/A	N/A	N/A	DSHIELD IP blocklist
DMZNet	N/A	N/A	N/A	N/A	N/A	
InternalNet	N/A	N/A	N/A	N/A	N/A	
LocalMachine	N/A	N/A	N/A	N/A	N/A	Check Point Local Machine (Dynamic Interfaces)
LocalMachine_All_Interfaces	N/A	N/A	N/A	N/A	N/A	Check Point Local Machine (All Interfaces)

172.16.1.191 Write Mode NUM

172.16.1.191 - Check Point SmartDashboard R77.20 - Standard

Firewall

Application & URL Filtering

Data Loss Prevention

IPS

Threat Prevention

Anti-Spam & Mail

Mobile Access

IPSec VPN

More

Overview

Policy

NAT

Track Logs

Analyze & Report

svuit.com

Overview

Network Activity

Policy Information

Services

Objects List

Identity Awareness

SmartWorkflow

172.16.1.191

Write Mode

NUM

Select Gateway: svuit-hcm-gw

Packets/Sec

60

50

40

30

20

10

0

21:35:00

Accepted

Dropped

0 rules in policy

0 rules are expired

0 rules are disabled

0 rules have zero hits

0 Accept Rules

0 Drop Rules

0 Reject Rules

Type to Search

Services

Action...

Name	Port	Protocol	Match for Any	Session Timeout (seconds)	Comment
TCP wais	210	N/A	Yes	Default (3600)	Wide Area Information Servers
TCP ssh_version_2	22	N/A	No	Default (3600)	Secure Shell, version 1.x block
TCP rtsp	554	N/A	Yes	Default (3600)	Real Time Streaming Protocol
UDP RIPng	521	N/A	Yes	Default (40)	Routing Information Protocol for IPv6
? sip_dynamic_ports	N/A	-1	No	Default (60)	Supported from version R55W, it allows sip connectio
TCP nfsd-tcp	2049	N/A	Yes	Default (3600)	Network File System Daemon over TCP
? AH	N/A	51	Yes	600	IPSEC Authentication Header Protocol
MSExchange-RemoteAdmin	N/A	N/A	N/A	N/A	Microsoft Exchange Remote Administration
UDP MSSQL_resolver	1434	N/A	No	Default (40)	MS SQL Sapphire /SQL Slammer Worm
NBT	N/A	N/A	N/A	N/A	NetBios Services

172.16.1.191 - Check Point SmartDashboard R77.20 - Application & URL Filtering

Firewall

Application & URL Filtering

Data Loss Prevention

IPS

Threat Prevention

Anti-Spam & Mail

Mobile Access

IPSec VPN

More

Overview

AppWiki

Policy

Gateways

Applications/Sites

UserCheck

Limit

Advanced

Legacy URL Filtering

Track Logs

Analyze & Report

Network Objects

Check Point

Nodes

Networks

Groups

Address Ranges

Dynamic Objects

Overview

Application Control & URL Filtering helps you control applications and websites access in your organization.

My Organization

No Security Gateways are enforcing Application Control & URL Filtering. Add...

IP AddressApplication ControlURL FilteringIdentity Aware

2 Rules in policy | 1 Allow rule | 1 Block rule

Detected in My Organization

Top CategoriesTop ApplicationsTop Sites

Logs...Graphs...

Traffic by Bandwidth in the last Hour

Application and URL Filtering blades are not enabled on any Security Gateways.

Messages and Actions

The Management server is up to date with the latest application database (9/28/2014).

Enter Application/Site URL

Top Users

Bandwidth in last Hour

Application and URL Filtering blades are not enabled on any Security Gateways.

Objects ListIdentity AwarenessSmartWorkflow

172.16.1.191Write ModeNUM

172.16.1.191 - Check Point SmartDashboard R77.20 - Data Loss Prevention

Firewall

Application & URL Filtering

Data Loss Prevention

IPS

Threat Prevention

Anti-Spam & Mail

Mobile Access

IPSec VPN

More

Install Policy

SmartConsole

Check Point SmartDashboard

Overview

Policy

Whitelist Policy

Data Types

Repositories

My Organization

Gateways

UserCheck

Additional Settings

Track Logs

Analyze & Report

Network Objects

Check Point

Nodes

Networks

Groups

Address Ranges

Dynamic Objects

Overview

DLP protects your organization from potential data loss

Refresh

My Organization

No Security Gateways are enforcing DLP

Add Gateway...

No Exchange Agents are enforcing DLP.

IP Address

Status

Comments

Statistics

Number of DLP incidents during the last:

Hour

24 Hours

Week

Month

0%

Percentage of internal incidents to all emails sent: No Mail Incidents.

Critical

High

Medium

Low

Prevented

Ask User

Inform User

Detected

Average

Statistics not collected yet

0

1

2

3

4

5

6

7

8

9

10

Last updated on Thursday, Oct 02, 2014 21:57:11

Messages and Action items

13 pre-defined items can be customized to improve accuracy:

11 Data Types

2 Rules

No items are flagged for Follow Up.

'Learn user actions' is applied on Web. [Change](#)

Track Logs

Open SmartEvent

Featured Data Types

Compliance

17 Data Types in this category. 4 activated.

Featured Data Types

PCI - Cardholder Data

HIPAA - Protected Health Information

GLBA - Personal Financial Information

U.S. State Laws - Personally Identifia...

EU Data Protection Directive

View rule

Add to policy

Add to policy

Add to policy

Add to policy

Objects List

Identity Awareness

SmartWorkflow

172.16.1.191 [Write Mode](#) NUM

172.16.1.191 - Check Point SmartDashboard R77.20 - IPS

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

OverviewGatewaysProfilesProtectionsGeo ProtectionNetwork ExceptionsDownload UpdatesFollow UpAdditional SettingsTrack LogsAnalyze & Report

Network ObjectsCheck PointNodesNetworksGroupsAddress RangesDynamic Objects

Overview

IPS provides protection from network, application and web attacks.

IPS in My Organization

0 Security Gateways are enforcing IPS
2 profiles are configured

Profile	IPS Mode	Activation	Gateways
Default_Protection	Prevent	IPS Poli...	0 GWs
Recommended_Pr...	Prevent	IPS Poli...	0 GWs

Messages and Action Items

New update package (v.634146563) is available. [Update](#)

Need help managing IPS? [Click here](#)

[View Events](#) [Manage Events](#) [View Reports](#)

Security Status

Number of events handled by IPS during the last: ☐ Hour ☒ 24 Hours ☐ Week ☐ Mo

CriticalHighMediumLow

Statistics not collected yet

DetectedPreventedAverage in My Organization

Security Center

[Open](#)
Sun, 31 Aug 2014 Critical
Adobe Flash Player Use After Free Code Execution (APSB14-18; CVE-2014-0538)
[Open](#)
Sun, 31 Aug 2014 High
Jenkins Groovy Script Console Remote Code Execution
[Open](#)
Sun, 31 Aug 2014 High
WordPress MailPoet Newsletters Unauthenticated File Upload

Objects ListIdentity AwarenessSmartWorkflow

172.16.1.191Write ModeNUM

172.16.1.191 - Check Point SmartDashboard R77.20 - Threat Prevention

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

OverviewThreat WikiPolicyException GroupsGatewaysProtectionsProfilesSitesUserCheckAdvancedTraditional Anti-VirusTrack LogsAnalyze & Report

Network ObjectsCheck PointNodesNetworksGroupsAddress RangesDynamic Objects

Check Point SmartDashboard

Overview

Threat Prevention helps you detect and prevent malware in your organization

My Organization

No Security Gateways are enforcing Anti-Bot, Anti-Virus or Threat Emulation. Add...

IP Address	Anti-Bot	Anti-Virus	Threat Emulation
------------	----------	------------	------------------

Statistics

No Security Gateways Are Enforcing Anti-Bot, Anti-Virus or Threat Emulation.


Messages and Actions

Threat Emulation supports additional file types. Enable

Enter malware name to get details (e.g. Troja)

Latest Malware Activity

No attack sources were found in your network.



Vin32.ZacomTrojan-Downloader.Win32.ChoxyTrojan-Downloader.Win32.SeccivTrojan-Downloader.Win32.Ldmon

Objects ListIdentity AwarenessSmartWorkflow

172.16.1.191Write ModeNUM

172.16.1.191 - Check Point SmartDashboard R77.20 - Anti-Spam & Mail

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

OverviewAnti-SpamTraditional Anti-VirusAdvanced

Network Objects

- Check Point
- Nodes
- Networks
- Groups
- Address Ranges
- Dynamic Objects

svuit.com

Overview







Enforcing Gateways

Traditional Anti-Virus0/1 GatewaysAnti-Spam0/1 GatewaysConfigureAutomatic updates are not configured

Database Updates

ConfigureAutomatic updates are not configured

Some Anti-Spam Mail features involve communication with an external server. For more information, refer to our [privacy policy](#).

 <div><div>Content based Anti-Spam</div><div>Filter spam based on content fingerprint</div><div>SettingsView Logs</div><div>High protection</div></div>	<div><div>Filter spam</div><div>Filter suspected spam</div></div> <div><div>Protects against all types of spam</div><div>Filters more than 97% of spam</div><div>A false positive rate of 1 in a 100,000</div><div>Up to thousands of messages/sec</div></div>
 <div><div>IP Reputation Anti-Spam</div><div>Filter spam from known spammers</div><div>SettingsView Logs</div><div>High protection</div></div>	<div><div>Filter spam</div><div>Filter suspected spam</div></div> <div><div>Blocks the majority of malicious mail</div><div>Filters more than 70% of spam</div><div>Saves bandwidth, Improves performance</div></div>
 <div><div>Block List Anti-Spam</div><div>User defined IPs and addresses blocking</div><div>SettingsView Logs</div><div>Block</div></div>	<div><div>Block senders by IP</div><div>Block senders by address</div></div> <div><div>0 IPs will be blocked</div><div>0 Senders/Domains will be blocked</div></div>
 <div><div>Mail Anti-Virus</div><div>Scan and filter mail for malware</div><div>SettingsView Logs</div><div>Block</div></div>	<div><div>Block</div><div>To enable on UTM-1 Edge go to Anti-Virus Settings</div></div> <div><div>Up to thousands of messages/sec</div></div>
 <div><div>Zero hour malware protection</div><div>Filter mail using rapid response signatures</div><div>SettingsView Logs</div><div>Off</div></div>	<div><div>Immediate proactive malware protection</div><div>Up to thousands of messages/sec</div></div>
 <div><div>IPS</div><div>Email IPS protections</div><div>SettingsView Logs</div></div>	<div><div>Go to IPS Tab to manage</div><div>IPS profiles</div><div>IPS mail</div></div> <div><div>0 POP3 servers defined</div><div>0 SMTP servers defined</div><div>0 IMAP servers defined</div></div>

Objects ListIdentity AwarenessSmartWorkflow

172.16.1.191Write ModeNUM

172.16.1.191 - Check Point SmartDashboard R77.20 - Mobile Access

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

OverviewPolicyGatewaysApplicationsAuthenticationClient CertificatesPortal SettingsIPSEndpoint Security On DemandMobile SettingsAdditional Settings

Network Objects

- Check Point
- Nodes
- Networks
- Groups
- Address Ranges
- Dynamic Objects

Objects ListIdentity AwarenessSmartWorkflow

172.16.1.191Write ModeNUM

Overview

Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web browser.

My Organization

No Security Gateways are allowing Mobile Access [Add Gateway...](#)

IP Address	Web	Mobile	Desktop	Compliance
------------	-----	--------	---------	------------

Messages and Actions

- Endpoint Compliance automatic updates are not configured
- All Portals have valid certificates

[Open SmartView Tracker](#) [Open SmartEvent](#)

Users and Policy

Active Sessions on Gateway/s: All Gateways

No Security Gateways are enabling Mobile Access...

Applications

No Applications are configured.

0Web Application

0Mobile Application

0Files Application

0Mail Application

0Citrix Application

0Native Application

172.16.1.191 - Check Point SmartDashboard R77.20 - IPSec VPN

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

OverviewCommunitiesGateways

Network Objects

- Check Point
- Nodes
- Networks
- Groups
- Address Ranges
- Dynamic Objects

Overview

Secure connectivity for offices and end users via sophisticated but easy to manage Site-to-Site VPN and flexible remote access.

My Organization

2 VPN Communities are configured New...

	Topology	Encryption Suite	Comments
MyIntranet	Meshed	Custom	
RemoteAccess	Remote Access	Custom	

Messages and Actions

There are no messages and actions

Encrypted Throughput

Top 5CustomSelect...

No Security Gateways are enabling VPN

Number of Tunnels

Top 5CustomSelect...

No Security Gateways are enabling VPN

Objects ListIdentity AwarenessSmartWorkflow

172.16.1.191Write ModeNUM

172.16.1.191 - Check Point SmartDashboard R77.20 - Compliance

FirewallApplication & URL FilteringData Loss PreventionIPSThreat PreventionAnti-Spam & MailMobile AccessComplianceMore

OverviewSecurity Best PracticesGatewaysRegulationsMessages and Action ItemsReportsAdvanced

Network Objects

- Check Point
- Nodes
- Networks
- Groups
- Address Ranges
- Dynamic Objects

Overview

Compliance blade helps you optimize your security settings and compliance with regulatory requirements.

Security Best Practices Compliance

0

Security Best Practices monitored across

0

Gateways and

0

Blades

Security Status

Secure0%

High0%

Medium0%

Low0%

More Details

Gateways

Security Status by Gateway

Top 5

Bottom 5

Favorites

See all Gateways

Blades

Security Status By Blade

More

Regulatory Compliance

0

Regulatory Requirements are being monitored

Action Items and Messages

0

Action Items are pending

Overdue0 items

Upcoming0 items

Future0 items

Unscheduled0 items

Objects ListIdentity AwarenessSmartWorkflow

172.16.1.191Write ModeNUM

172.16.1.191 - Check Point SmartDashboard R77.20 - Standard

Firewall

Application & URL Filtering

Data Loss Prevention

IPS

Threat Prevention

Anti-Spam & Mail

Mobile Access

QoS

More

Check Point SmartDashboard

Network Objects

Check Point

Nodes

Networks

Groups

Address Ranges

Dynamic Objects

Policy

Standard

Default

Name	Source	Destination	Service	Action	Track	Install On	Time
Default	Any	Any	Any	Weight 10	None	All	Any

Objects List

Identity Awareness

SmartWorkflow

172.16.1.191

Write Mode

NUM

svuit.com

172.16.1.191 - Check Point SmartDashboard R77.20 - Standard

Firewall

Application & URL Filtering

Data Loss Prevention

IPS

Threat Prevention

Anti-Spam & Mail

Mobile Access

Desktop

More

Check Point SmartDashboard

Network Objects

Check Point

svuit-hcm-gw

Nodes

Networks

CP_default_Office_Mode_addr

Groups

Address Ranges

All_Internet

LocalMachine_Loopback

Dynamic Objects

AuxiliaryNet

CPDShield

DMZNet

InternalNet

LocalMachine

LocalMachine_All_Interfaces

Policy

Inbound Rules

No.	Source	Desktop	Service	Action	Track	Comment
-----	--------	---------	---------	--------	-------	---------

Outbound Rules

No.	Desktop	Destination	Service	Action	Track	Comment
-----	---------	-------------	---------	--------	-------	---------

Objects List

Identity Awareness

SmartWorkflow

172.16.1.191

Write Mode

NUM

svuit.com

172.16.1.191 - Check Point SmartDashboard R77.20 - Standard

Install PolicySmartConsole

FirewallApplication & URL FilteringData Loss PreventionIPSThreat PreventionAnti-Spam & MailMobile AccessDesktopMore

Services

+

 TCP

+

 Compound TCP

+

 Citrix TCP

+

 UDP

+

 RPC

+

 ICMP

+

 DCE-RPC

+

 Other

+

 Group

- AOL_Messenger
- Authenticated
- CIFS
- Citrix_metaFrame
- DAIP_Control_services
- daytime
- Direct_Connect
- discard
- dns
- echo
- eDonkey
- Entrust-CA
- FreeTel-outgoing
- FW1_dntauth
- GNUTella
- Hotline
- icmp-requests
- Integrity_Server
- IPSEC
- IPv6_group
- irc
- kerberos

Policy

Inbound Rules

No.	Source	Desktop	Service	Action	Track	Comment
-----	--------	---------	---------	--------	-------	---------

Objects ListIdentity AwarenessSmartWorkflow

Type to SearchServicesGroupAction...

Name	Port	Protocol	Match for Any	Session Timeout (seconds)	Comment
AOL_Messenger	N/A	N/A	N/A	N/A	AOL Instant Messenger. Also used by: ICQ & Ap
Authenticated	N/A	N/A	N/A	N/A	Authenticated group
CIFS	N/A	N/A	N/A	N/A	Common Internet File System Services
Citrix_metaFrame	N/A	N/A	N/A	N/A	group for citrix communication
DAIP_Control_services	N/A	N/A	N/A	N/A	
daytime	N/A	N/A	N/A	N/A	Daytime Protocol group (TCP/UDP)
Direct_Connect	N/A	N/A	N/A	N/A	Direct Connect P2P application. Used also by oth
discard	N/A	N/A	N/A	N/A	Discard Protocol group (TCP/UDP)
dns	N/A	N/A	N/A	N/A	Domain Name System (TCP/UDP)
echo	N/A	N/A	N/A	N/A	Echo Protocol group (TCP/UDP)

172.16.1.191Write ModeNUM

172.16.1.191 - Check Point SmartView Tracker - [All Records (fw.log)]

Network & Endpoint

Active

Management

Check Point SmartView Tracker

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	Source User Name	Destination	Rule
1	20Oct2014	20:27:59	svuit-hcm-gw	??	172.16.1.1		all-systems.mcast.net	
2	20Oct2014	20:27:59	svuit-hcm-gw					
3	20Oct2014	20:27:59	svuit-hcm-gw					
4	20Oct2014	20:28:27	svuit-hcm-gw					
5	20Oct2014	20:28:31	svuit-hcm-gw					
6	20Oct2014	20:28:33	svuit-hcm-gw					
7	20Oct2014	20:28:33	svuit-hcm-gw					
8	20Oct2014	20:28:35	svuit-hcm-gw					
9	20Oct2014	20:28:35	svuit-hcm-gw					
10	20Oct2014	20:28:38	svuit-hcm-gw					
11	20Oct2014	20:28:38	svuit-hcm-gw					
12	20Oct2014	20:30:03	svuit-hcm-gw	??	172.16.1.1		all-systems.mcast.net	
13	20Oct2014	20:32:08	svuit-hcm-gw	??	172.16.1.1		all-systems.mcast.net	
14	20Oct2014	20:32:50	svuit-hcm-gw					
15	20Oct2014	20:32:50	svuit-hcm-gw					
16	20Oct2014	20:34:13	svuit-hcm-gw	??	172.16.1.1		all-systems.mcast.net	
17	20Oct2014	20:36:18	svuit-hcm-gw	??	172.16.1.1		all-systems.mcast.net	
18	20Oct2014	20:38:23	svuit-hcm-gw	??	172.16.1.1		all-systems.mcast.net	
19	20Oct2014	20:40:28	svuit-hcm-gw	??	172.16.1.1		all-systems.mcast.net	
20	20Oct2014	20:42:33	svuit-hcm-gw	??	172.16.1.1		all-systems.mcast.net	
21	20Oct2014	20:44:38	svuit-hcm-gw	??	172.16.1.1		all-systems.mcast.net	
22	20Oct2014	20:46:43	svuit-hcm-gw	??	172.16.1.1		all-systems.mcast.net	
23	20Oct2014	20:48:48	svuit-hcm-gw	??	172.16.1.1		all-systems.mcast.net	
24	20Oct2014	20:50:53	svuit-hcm-gw	??	172.16.1.1		all-systems.mcast.net	
25	20Oct2014	20:52:59	svuit-hcm-gw	??	172.16.1.1		all-systems.mcast.net	
26	20Oct2014	20:55:04	svuit-hcm-gw	??	172.16.1.1		all-systems.mcast.net	
27	20Oct2014	20:57:09	svuit-hcm-gw	??	172.16.1.1		all-systems.mcast.net	
28	20Oct2014	20:59:14	svuit-hcm-gw	??	172.16.1.1		all-systems.mcast.net	
29	20Oct2014	21:01:19	svuit-hcm-gw	??	172.16.1.1		all-systems.mcast.net	
30	20Oct2014	21:03:24	svuit-hcm-gw	??	172.16.1.1		all-systems.mcast.net	

Ready

Ready

Total records in file: 67

Track Logs: Read/Write NUM

172.16.1.191 - Check Point SmartView Tracker - [All Records (fw.adtlog)]

Network & Endpoint Active **Management**

Management Queries
 Predefined
 Records with Session
 All Records
 Custom

All Records (fw.adtlog)

No.	Date	Time	Application	Subject	Operation	Object Type	Performed On	Changes
3	2Oct2014	20:30:45	Security Manag...	Database Updat...	Downloaded a datab...			
4	2Oct2014	20:30:45	Security Manag...	Database Updat...	Downloaded a datab...			
5	2Oct2014	20:30:45	cpmidu_update...	Object Manipul...	Modify Object	asm_audit_ctrl	ASMAuditCtrl	allow_audit: chan
6	2Oct2014	21:28:43	SmartDashboard	Administrator Lo...	Log In			
7	2Oct2014	21:29:09	SmartDashboard	Administrator Lo...	Log In			
8	2Oct2014	21:30:46	SmartDashboard	Administrator Lo...	Log In			
9	2Oct2014	21:31:01	SmartDashboard	Administrator Lo...	Log In			
10	2Oct2014	21:31:12	SmartDashboard	File Operation	File Retrieved			
11	2Oct2014	21:40:41	SmartDashboard	Object Manipul...	Create Object	policies_collection	Standard	
12	2Oct2014	21:40:41	SmartDashboard	Object Manipul...	Create Object	firewall_policy	Standard	
13	2Oct2014	21:40:41	SmartDashboard	Object Manipul...	Create Object	floodgate_policy	Standard	
14	2Oct2014	21:40:41	SmartDashboard	Object Manipul...	Create Object	securelan_policy	Standard	
15	2Oct2014	21:40:41	SmartDashboard	Object Manipul...	Create Object	appfw_policy	Standard	
16	2Oct2014	21:40:41	SmartDashboard	Object Manipul...	Create Object	anti_malware_rule...	A_8BCB2721-E40E...	
17	2Oct2014	21:40:41	SmartDashboard	Object Manipul...	Create Object	anti_malware_rule...	A_0D745736-D991...	
18	2Oct2014	21:40:41	SmartDashboard	Object Manipul...	Create Object	entity_local_instance	A_92F6495D-4B1F...	
19	2Oct2014	21:40:41	SmartDashboard	Object Manipul...	Modify Object	anti_malware_rule...	A_0D745736-D991...	num_rules_this_se
20	2Oct2014	21:40:41	SmartDashboard	Object Manipul...	Create Object	anti_malware_rule...	A_1E234C71-CDA4...	
21	2Oct2014	21:40:41	SmartDashboard	Object Manipul...	Create Object	entity_local_instance	A_21248493-BE1E-...	
22	2Oct2014	21:40:41	SmartDashboard	Object Manipul...	Create Object	antimalware_policy	Standard	
23	2Oct2014	21:40:41	SmartDashboard	Object Manipul...	Modify Object	firewall_properties	firewall_properties	Is this the first log
24	2Oct2014	21:40:41	SmartDashboard	Object Manipul...	Modify Object	floodgate_policy	Standard	Rule 1: added 'bai
25	2Oct2014	21:40:47	SmartDashboard	Administrator Lo...	Log Out			
26	2Oct2014	21:41:00	SmartDashboard	Administrator Lo...	Log In			
27	2Oct2014	21:53:05	SmartDashboard	Administrator Lo...	Log In			
28	2Oct2014	21:53:12	SmartDashboard	Administrator Lo...	Log In			
29	2Oct2014	21:58:47	SmartDashboard	File Operation	File Retrieved			
30	2Oct2014	22:16:35	SmartView Trac...	Administrator Lo...	Log In			
31	2Oct2014	22:16:39	SmartView Trac...	File Operation	File Retrieved			
32	2Oct2014	22:19:04	SmartView Trac...	Object Manipul...	Create Object	tracker_leaf	A0DF21A42A6493A...	

Ready

Ready

Total records in file: 35

Audit Logs: Read/Write NUM

OK, Vậy là xong! Có quá nhiều tính năng đang chờ bạn tìm hiểu...