

emailmaiTRƯỜNG CAO ĐẲNG CÔNG NGHỆ THỦ ĐỨC

KHOA CÔNG NGHỆ THÔNG TIN



## ĐỒ ÁN MÔN HỌC

### QUẢN TRỊ HỆ THỐNG WINDOWS 2

ĐỀ TÀI:

### SOPHOS FIREWALL

#### Nhóm THEBEST

1. Nguyễn Phước Bình
2. Nguyễn Trung Thành
3. Trần Mạnh Duy
4. Nguyễn Hoàng Tuấn
5. Nguyễn Đình Khả

GVHD: Nguyễn Ngọc Ánh Mỹ

TP. Hồ Chí Minh, 12/2023

## MỤC LỤC

CHƯƠNG 1: GIỚI THIỆU SOPHOS FIREWALL .....	3
1.1    Khái niệm .....	3
1.2    Mô hình thực hiện .....	4
1.3    Phân công công việc.....	5
CHƯƠNG 2: NỘI DUNG ĐỒ ÁN .....	6
2.1    Network Service.....	6
2.1.1    Provide Internet Connection .....	6
2.1.2    DHCP .....	7
2.1.3    DNS.....	8
2.2    Firewall Rule .....	10
2.2.1    Khái niệm.....	10
2.2.2    Cấu hình .....	10
2.3    Web Protection .....	24
2.3.1    Khái niệm.....	24
2.3.2    Cấu hình (chặn user truy cập các web cờ bạc).....	25
2.4    Mail Protection .....	30
2.4.1    Khái niệm.....	30
2.4.2    Cấu hình .....	30
2.5    Antivirus .....	35
2.5.1    Khái niệm.....	35
2.5.2    Cấu hình .....	36
2.6    Server Protection .....	39
2.6.1    Khái niệm.....	39
2.6.2    Cấu hình .....	39
2.7    Sao lưu và phục hồi Sophos .....	48

## Đồ án Quản trị hệ thống Windows 2

2.7.1	Khái niệm.....	48
2.7.2	Cấu hình .....	48
CHƯƠNG 3: TỔNG KẾT .....		56
3.1	Thuận lợi và khó khăn.....	56
3.1.1	Thuận lợi .....	56
3.1.2	Khó khăn .....	56
3.2	Kết luận .....	56
TÀI LIỆU THAM KHẢO .....		57

## CHƯƠNG 1: GIỚI THIỆU SOPHOS FIREWALL

### 1.1 Khái niệm

XG Firewall (còn được gọi là Sophos Firewall) là một giải pháp bảo mật mang hàng đầu, cung cấp các tính năng đa dạng nhằm bảo vệ hệ thống mạng của doanh nghiệp khỏi các mối đe dọa trực tuyến. Được thiết kế để cung cấp một tường lửa mạnh mẽ và toàn diện.

Một số chức năng của Sophos Firewall:

- **Provide Internet Connection**
- **DNS (Domain Name System)**
- **DHCP (Dynamic Host Configuration Protocol)**
- **Firewall Services**

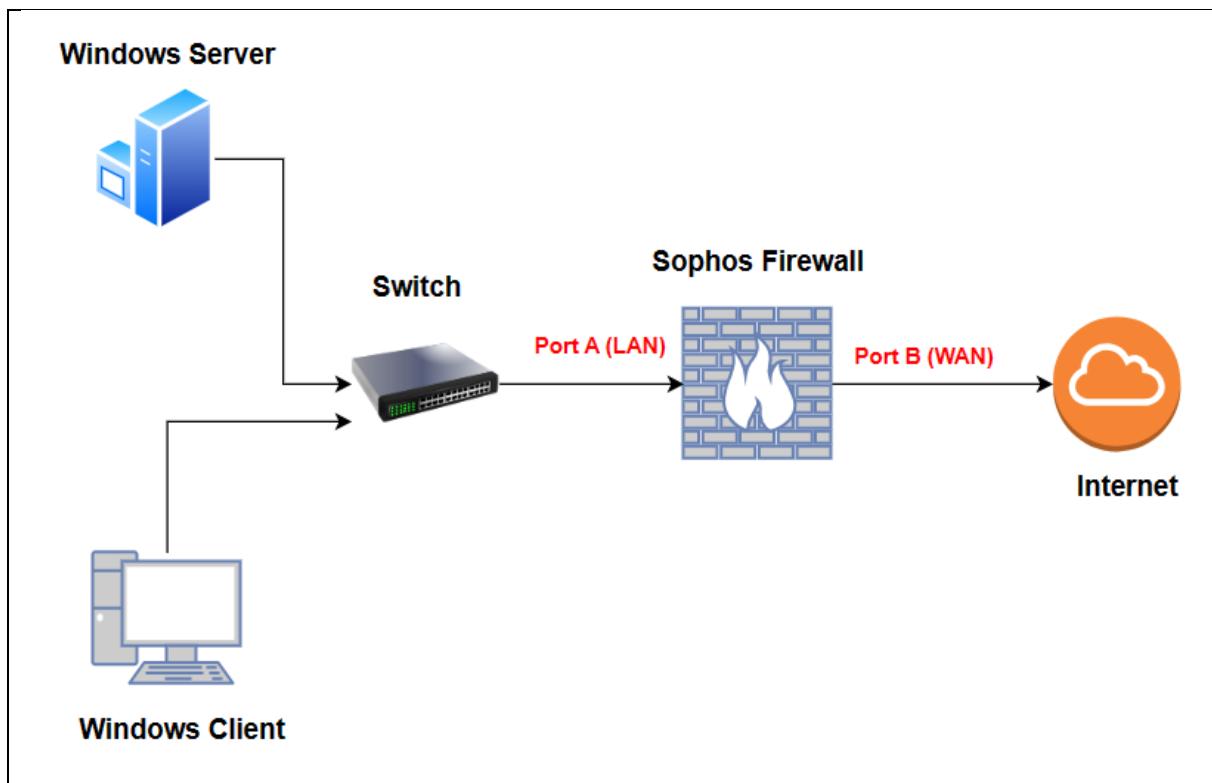
**Ưu điểm của sophos firewall:**

- **Quản lý dễ dàng:** Giao diện người dùng thân thiện và dễ sử dụng giúp người quản trị mạng dễ dàng cấu hình và quản lý hệ thống bảo mật một cách hiệu quả.
- **Phòng ngừa mối đe dọa tốt:** Cung cấp khả năng phòng ngừa và phát hiện mối đe dọa mạng hiệu quả, bao gồm cả phần mềm độc hại, ransomware và các cuộc tấn công zero-day.
- **Bảo Mật và An Toàn:** Các dịch vụ mạng cung cấp các công cụ bảo mật như firewall, VPN để bảo vệ thông tin và dữ liệu trên mạng.

**Nhược điểm:**

- **Rủi ro bảo mật:** Một số dịch vụ mạng có thể trở thành điểm yếu trong hệ thống bảo mật nếu không được cấu hình hoặc quản lý đúng cách.
- **Cần vững kiến thức chuyên ngành mạng máy tính:** Nếu cấu hình không đúng cách, tường lửa sẽ chặn các dịch vụ mà doanh nghiệp đang sử dụng, từ đó khiến toàn bộ hệ thống bị đình trệ.

## 1.2 Mô hình thực hiện



### ❖ Sophos Firewall informations:

<b>Version</b>	SFOS 19.5.3 MR-3-Build652
<b>Port A (LAN)</b>	VMnet 2 (172.16.16.16)
<b>Port B (WAN)</b>	Bridge (DHCP)

### ❖ Windows Server informations:

<b>Version</b>	Windows Server 2019
<b>Software requirement</b>	Sophos Server Protection
<b>Network interface</b>	VMnet 2 – DHCP reservation (172.16.16.254)
<b>Domain Name</b>	thebest.vn

### ❖ Windows Client informations:

<b>Version</b>	Windows 10 x64
<b>Software requirement</b>	Sophos Endpoint Agent
<b>Network interface</b>	VMnet2 – DHCP
<b>Domain Joined</b>	thebest.vn

# Đồ án Quản trị hệ thống Windows 2

## 1.3 Phân công công việc

Nguyễn Phước Bình (nhóm trưởng)	<ul style="list-style-type: none"><li>_ Viết báo cáo: Cơ sở lý thuyết của Firewall Rule, Web Protection, Tổng kết.</li><li>_ Chụp hình các bước thực hiện Firewall Rule và Web Protection.</li></ul>
Nguyễn Trung Thành	<ul style="list-style-type: none"><li>_ Viết báo cáo: Cơ sở lý thuyết của Server Protection.</li><li>_ Chụp hình từng bước thực hiện Server Protection.</li><li>_ Viết BBHN.</li></ul>
Nguyễn Hoàng Tuấn	<ul style="list-style-type: none"><li>_ Viết báo cáo: trình bày ngắn gọn về Sao lưu và phục hồi Sophos.</li><li>_ Hình ảnh các bước thực hiện Sao lưu và phục hồi Sophos.</li><li>_ Làm PowerPoint hoàn chỉnh.</li></ul>
Nguyễn Đình Khả	<ul style="list-style-type: none"><li>_ Viết báo cáo: Cơ sở lý thuyết của Network Service.</li><li>_ Trình bày ngắn gọn về Sophos Firewall</li><li>_ Chụp hình từng bước thực hiện Network Service.</li></ul>
Trần Mạnh Duy	<ul style="list-style-type: none"><li>_ Viết báo cáo: trình bày ngắn gọn về Antivirus và Mail Protection.</li><li>_ Hình ảnh các bước thực hiện Antivirus và Mail Protection.</li></ul>

## CHƯƠNG 2: NỘI DUNG ĐỒ ÁN

### 2.1 Network Service

Trong lĩnh vực mạng máy tính, Network Service là những dịch vụ và chức năng được cung cấp để giúp các thiết bị và hệ thống giao tiếp, chia sẻ thông tin và thực hiện các nhiệm vụ mạng. Đây là những phần quan trọng trong việc xây dựng và duy trì mạng, đồng thời giúp tạo ra môi trường mạng an toàn và hiệu quả.

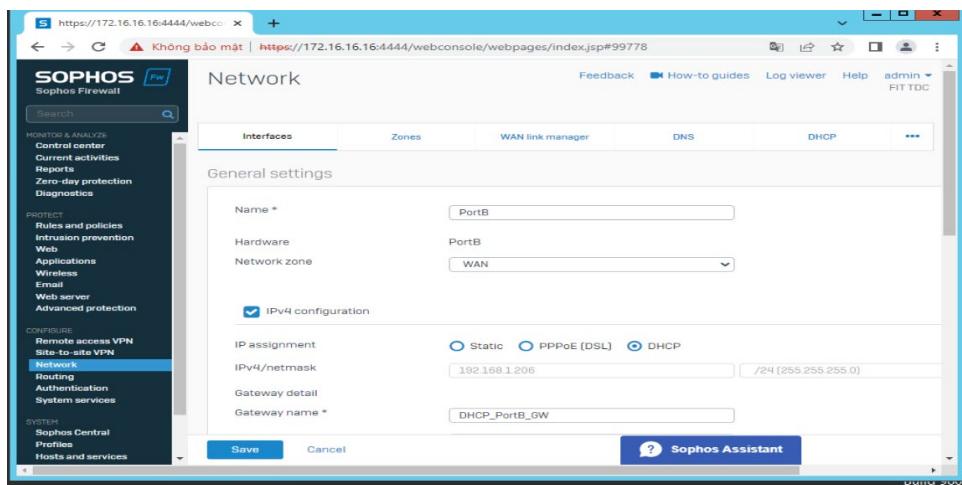
- **Provide Internet Connection:** Network Service đảm bảo rằng mạng LAN truy cập Internet đầy đủ và ổn định. Điều này thường đòi hỏi việc thiết lập một đường truyền Internet thông qua một nhà cung cấp dịch vụ Internet (ISP) hoặc một hệ thống mạng rộng (WAN).
- **DNS (Domain Name System):** Dịch vụ này chuyển đổi các tên miền thành địa chỉ IP để thiết bị có thể hiểu được, giúp người dùng truy cập các trang web dễ dàng hơn.
- **DHCP (Dynamic Host Configuration Protocol):** Cung cấp địa chỉ IP và các thông số cấu hình khác như Default Gateway, máy chủ DNS tự động cho các thiết bị khi chúng kết nối vào mạng.
- **Firewall Services (Dịch vụ Tường Lửa):** Dịch vụ Tường lửa đảm bảo rằng mạng LAN được bảo vệ khỏi các mối đe dọa từ Internet. Nó kiểm soát lưu lượng mạng, ngăn chặn các truy cập không mong muốn và bảo vệ khỏi các cuộc tấn công.

#### 2.1.1 Provide Internet Connection

Để các thiết bị trong mạng nội bộ LAN có thể truy cập internet, ta cần cấu hình một interface WAN cung cấp dịch vụ NAT cho Sophos Firewall để chuyển đổi các IP Private trong mạng nội bộ sang một hoặc một vài IP Public do ISP cung cấp.

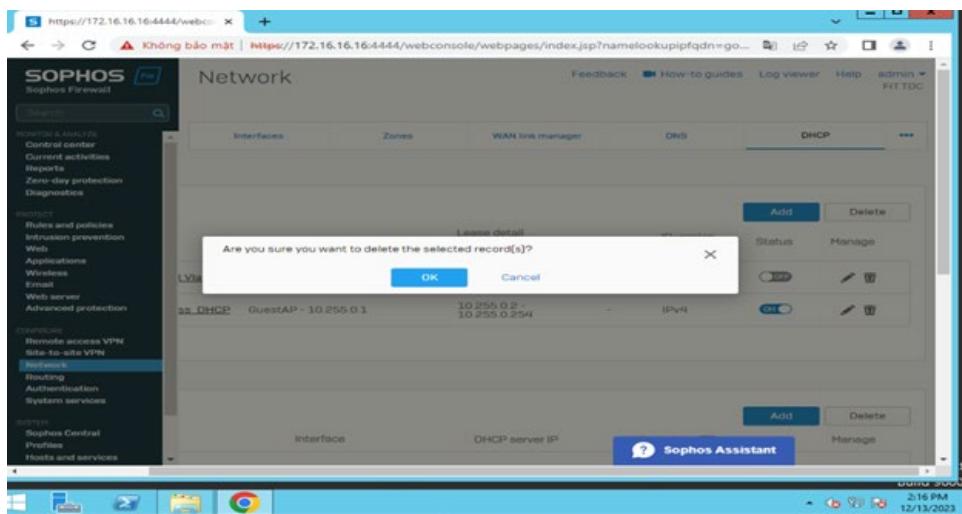
Ta vào phần **Network** → chọn **interfaces** → **Port B (WAN)**:

## Đồ án Quản trị hệ thống Windows 2

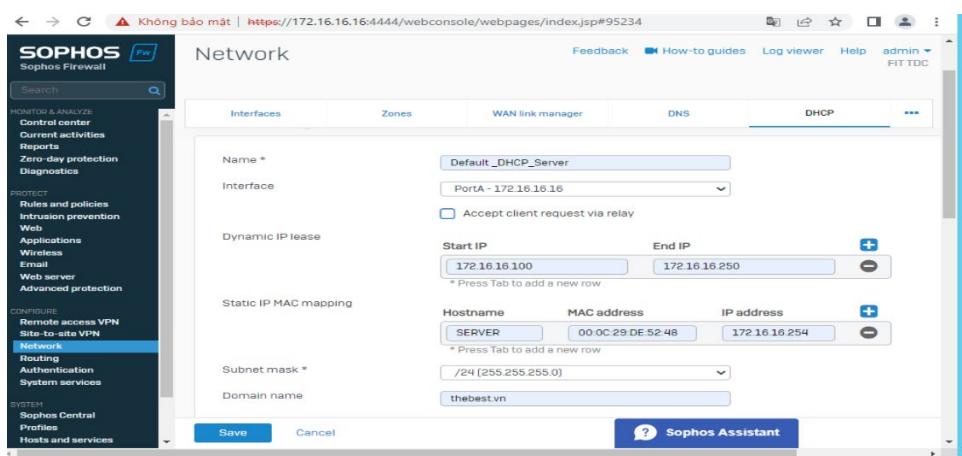


### 2.1.2 DHCP

Bước 1: Ta vào DHCP xóa đi Default range



Bước 2 : Ta sẽ add 1 cái range mới để cấp DHCP và gán cố định một IPv4 cho Server

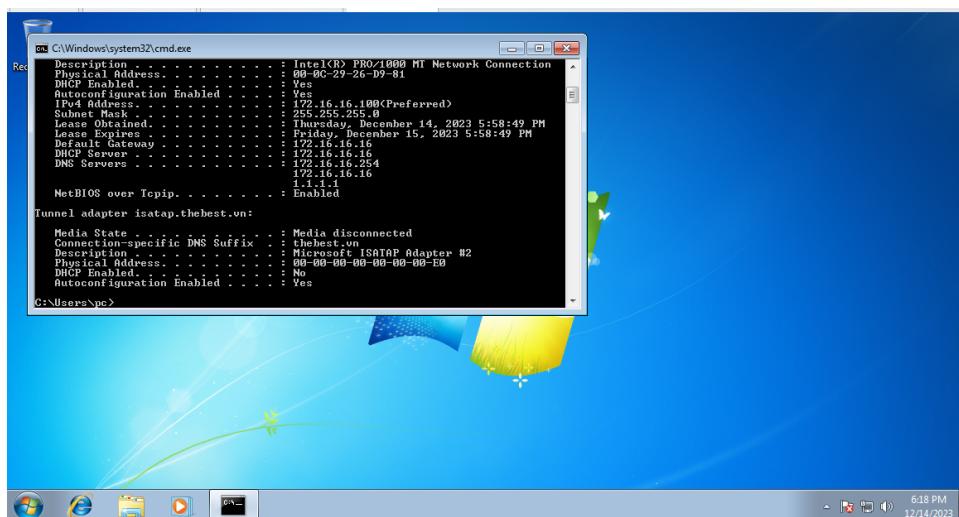


Bước 3: Thay đổi địa chỉ Primary DNS trả về Server, Secondary DNS trả về firewall

## Đồ án Quản trị hệ thống Windows 2

The screenshot shows the Sophos Firewall's Network configuration page. Under the 'DHCP' tab, there are sections for 'DNS server' and 'WINS server'. In the 'DNS server' section, 'Use device's DNS settings' is checked. Below it, 'Primary DNS' is set to 172.16.16.254 and 'Secondary DNS' is set to 172.16.16.16. There is also a 'Boot options' section. At the bottom, there are 'Save' and 'Cancel' buttons, and a 'Sophos Assistant' icon.

Bước 4: Qua máy client test DHCP



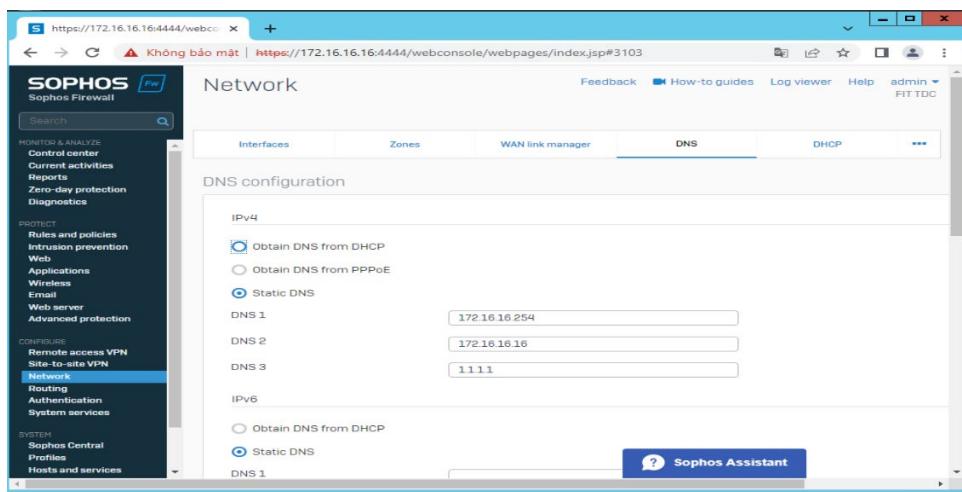
### 2.1.3 DNS

Bước 1: Ta vào Network

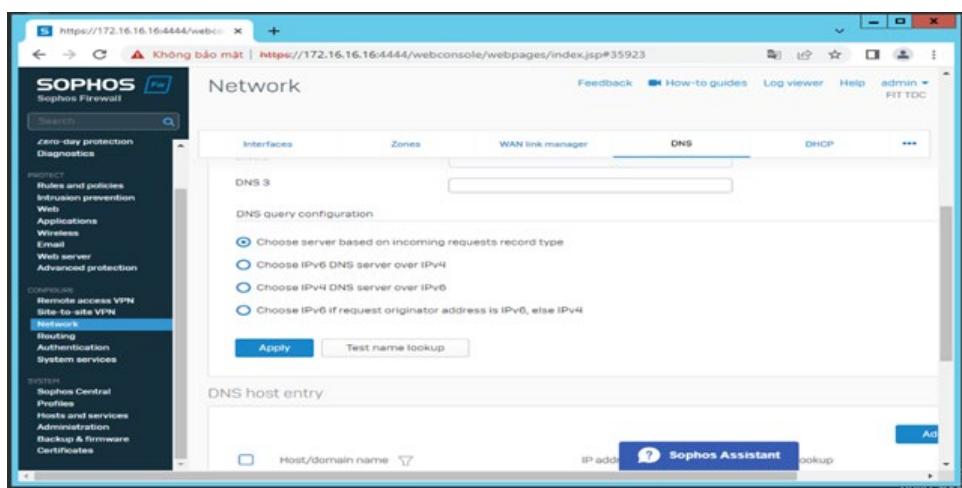
The screenshot shows the Sophos Firewall's Network configuration page under the 'Interfaces' tab. It lists three interfaces: 'GuestAP' (VLAN), 'PortA' (RED), and 'PortB' (RED). 'GuestAP' is unplugged and has a static IP of 10.255.0.1. 'PortA' is connected via Auto-negotiation at 10 Mbps Half Duplex with a static IP of 172.16.16.16. 'PortB' is connected via Auto-negotiation at 10 Mbps Half Duplex with a dynamic IP of 192.168.0.162. The 'Misc' column shows hardware types: 'G' for GuestAP and 'P' for PortA and PortB.

Bước 2: Ta vào phần DNS → chọn Static DNS và cấu hình như sau:

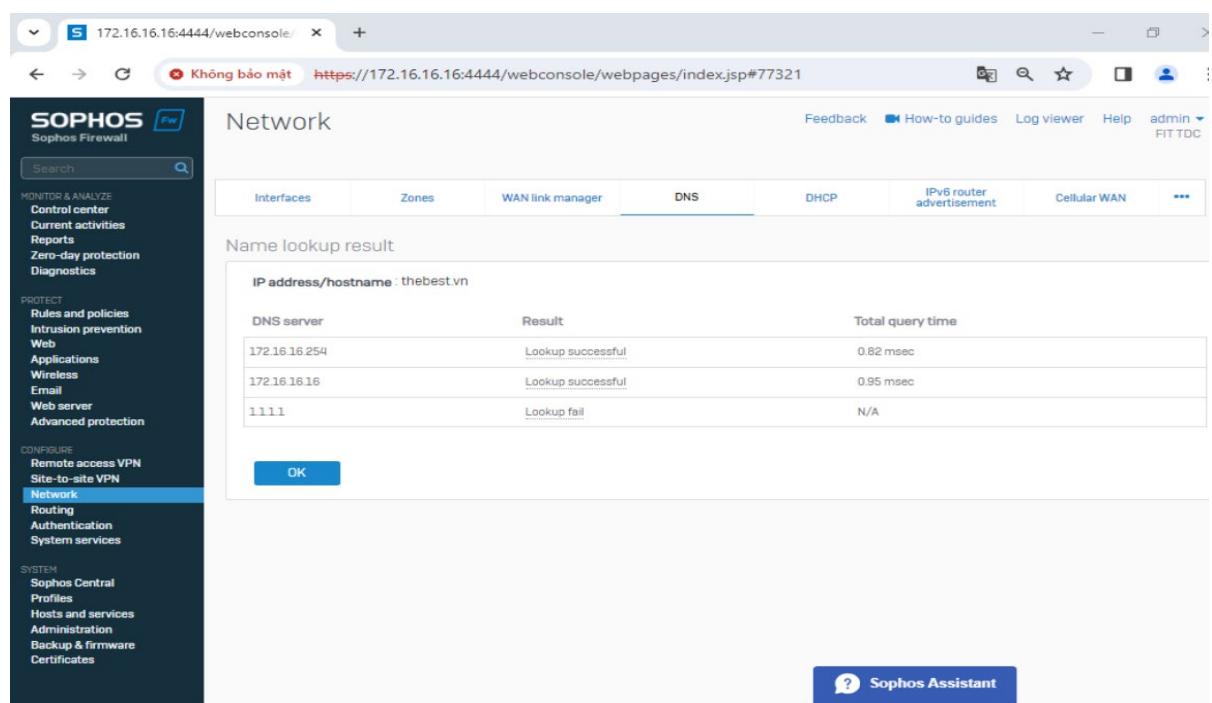
## Đồ án Quản trị hệ thống Windows 2



Bước 3: Kéo xuống chọn Apply



Bước 4: Lúc này mình sẽ vào Test name lookup để test thử DNS



## 2.2 Firewall Rule

### 2.2.1 Khái niệm

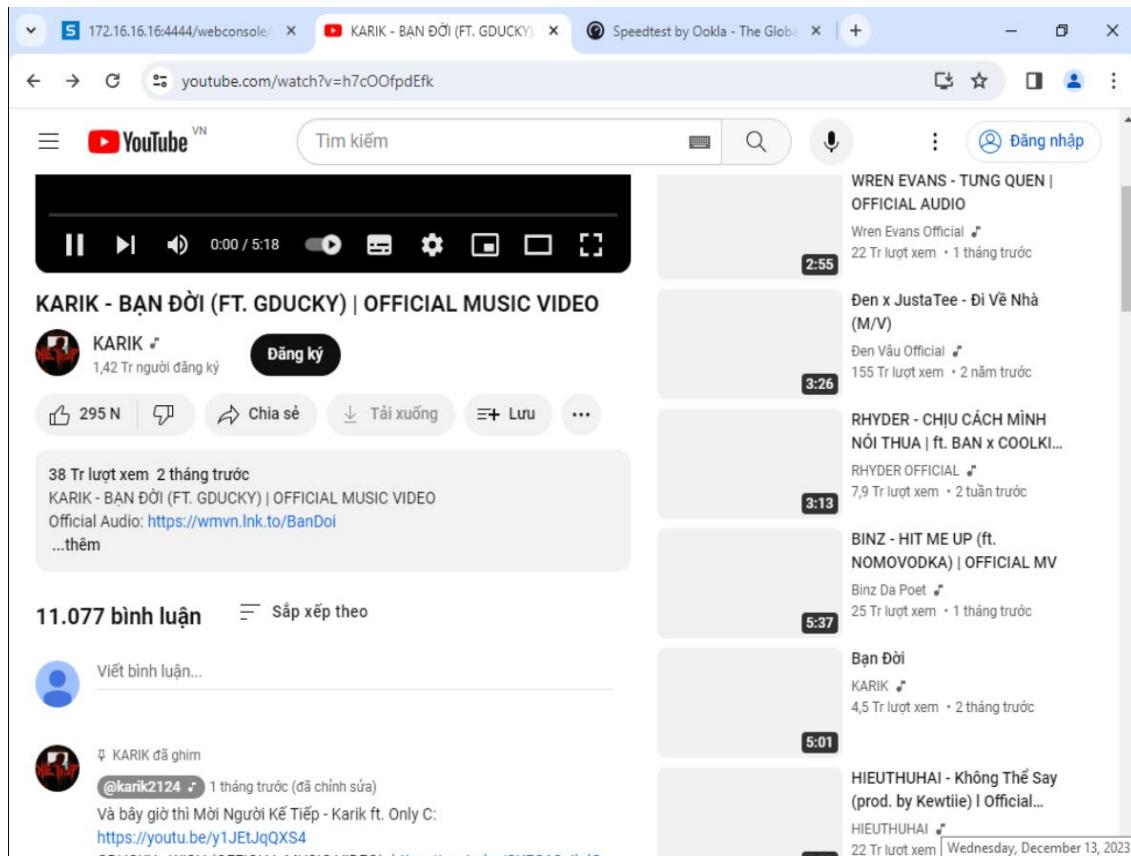
Trong Sophos Firewall, một firewall rule là một quy tắc được đặt ra để kiểm soát lưu lượng mạng. Những quy tắc này quy định cách dữ liệu có thể di chuyển qua firewall và xác định xem nó có được chấp nhận hay bị từ chối.

Mỗi firewall rule thường xác định các thông số như nguồn và đích của dữ liệu, cổng sử dụng, giao thức, và các điều kiện khác. Nếu một gói dữ liệu khớp với một firewall rule cụ thể, quy tắc đó sẽ quyết định liệu gói dữ liệu đó có được chấp nhận hay từ chối. Nếu không có firewall rule nào khớp, có thể áp dụng một quy tắc mặc định để xử lý dữ liệu.

Cấu hình các firewall rule là một phần quan trọng của việc bảo vệ mạng, giúp ngăn chặn các mối đe dọa và tăng cường an ninh hệ thống. Firewall rules cũng có thể được tinh chỉnh để đáp ứng các yêu cầu cụ thể của tổ chức hoặc môi trường mạng.

### 2.2.2 Cấu hình

- Kiểm tra kết nối đến trang web muốn chặn:



## Đồ án Quản trị hệ thống Windows 2

- Truy cập trang web sophos firewall <https://172.16.16.16:4444> → Chọn Rules and policies:

The screenshot shows the Sophos Firewall's web-based management interface. On the left, there's a sidebar with navigation links like 'Monitor & Analyze', 'Control center', 'Current activities', 'Reports', 'Zero-day protection', 'Diagnostics', 'Protect' (selected), 'Rules and policies' (selected), 'Intrusion prevention', 'Web', 'Applications', 'Wireless', 'Email', 'Web server', and 'Advanced protection'. Under 'Configure', there are 'Remote access VPN', 'Site-to-site VPN', 'Network', 'Routing', 'Authentication', and 'System services'. Under 'System', there are 'Sophos Central', 'Profiles', and 'Hosts and services'. The main area is titled 'Rules and policies' and has tabs for 'Firewall rules', 'NAT rules', and 'SSL/TLS inspection rules'. The 'Firewall rules' tab is active, showing a list of rules: 'Traffic to Internal...', 'Traffic to WAN', 'Traffic to DMZ', and 'Auto added firewall...'. A 'New firewall rule' dialog box is overlaid on the page, with the 'Server access assistant [DNAT]' option highlighted. The status bar at the bottom right shows the time as 3:19 PM and the date as 12/13/2023.

- Chọn Add firewall rule → New firewall rule

This screenshot is similar to the previous one, showing the Sophos Firewall's 'Rules and policies' interface. The 'Firewall rules' tab is selected. A 'New firewall rule' dialog box is open, with the 'Server access assistant [DNAT]' option selected. The main table below shows existing rules: 'Traffic to Internal...', 'Traffic to WAN', 'Traffic to DMZ', and 'Auto added firewall...'. The status bar at the bottom right shows the time as 3:19 PM and the date as 12/13/2023.

- Diền Rule name và chọn Action “Reject”

## Đồ án Quản trị hệ thống Windows 2

The screenshot shows the Sophos Firewall web console interface. On the left, a sidebar menu includes sections like PROTECT (Rules and policies, Intrusion prevention, Web, Applications, Wireless, Email, Web server, Advanced protection), CONFIGURE (Remote access VPN, Site-to-site VPN, Network, Routing, Authentication, System services), and SYSTEM (Sophos Central, Profiles, Hosts and services, Administration, Backup & firmware, Certificates). The main content area is titled "Add firewall rule". It has fields for "Rule name" (Chan Youtube), "Description" (Enter Description), "Rule position" (Bottom), and "Rule group" (Automatic). Under "Action", "Reject" is selected. A checked checkbox "Log firewall traffic" is followed by the note: "Logs traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server." A green success message at the bottom states: "Can't add the rule to an existing group based on the selected criteria." Below this is a "Source" section with a table for "Source zones", "Source networks and devices" (set to "Any"), and "During scheduled time" (set to "All the time"). Buttons for "Save" and "Cancel" are at the bottom, along with a "Sophos Assistant" button.

- Ở đây do ta muốn chặn user từ mạng nội bộ truy cập ra youtube (WAN) nên chọn **Source zones** là “LAN” (có thể chọn chặn theo giờ ở mục **During scheduled time**)

This screenshot shows the same Sophos Firewall web console interface as the previous one, but the "Source" configuration is now visible. In the "Source zones" dropdown, the "LAN" option is selected. The "Source networks and devices" field is set to "Any". The "During scheduled time" field is set to "All the time". Other options like "DMZ", "VPN", "WAN", and "WiFi" are also listed in the dropdown. The "Services" section below is partially visible. The "Save" and "Cancel" buttons are at the bottom, along with the "Sophos Assistant" button.

## Đồ án Quản trị hệ thống Windows 2

- Chọn Destination Zones là “WAN” và Destination networks ta “Add FQDN host”

The screenshot shows the Sophos Firewall web interface. On the left, there's a sidebar with sections for PROTECT (Rules and policies, Intrusion prevention, Web, Applications, Wireless, Email, Web server, Advanced protection), CONFIGURE (Remote access VPN, Site-to-site VPN, Network, Routing, Authentication, System services), and SYSTEM (Sophos Central, Profiles, Hosts and services, Administration, Backup & firmware, Certificates). The main area is titled 'Add firewall rule'. It has three main fields: 'Destination zones \*' (set to 'WAN'), 'Destination networks \*' (with a dropdown menu open showing options like 'Any', 'Country group', 'FQDN host', etc.), and 'Services \*' (set to 'Any'). Below these fields are buttons for 'Save' and 'Cancel'. A context menu is open over the 'Destination networks' dropdown, listing various network types. In the bottom right corner, there's a green button labeled 'Apply "Any"' and a 'Sophos Assistant' icon.

- Điền tên miền muốn chặn (“\*.youtube.com”) → Save

This screenshot shows the 'Add FQDN host' dialog box. It has fields for 'Name \*' (filled with 'Social Network') and 'FQDN \*' (filled with '\*youtube.com'). Below the FQDN field, there's a note: 'Use wildcard "\*" as a prefix in FQDN to resolve sub-domains. For example, \*.example.com'. There's also a section for 'FQDN host group' with a 'Save' and 'Cancel' button at the bottom.

- Kiểm tra lại xem đã nhận policy hay chưa

## Đồ án Quản trị hệ thống Windows 2

The screenshot shows the Sophos Firewall webconsole interface. On the left, a sidebar menu includes sections like MONITOR & ANALYZE, PROTECT (selected), CONFIGURE, and SYSTEM. Under PROTECT, 'Rules and policies' is selected. The main content area is titled 'Rules and policies' and shows a table of 'Firewall rules'. The table has columns for Rule type, #, Name, Source, Destination, What, ID, Action, and Feature and serv. There are 8 rules listed:

Rule type	#	Name	Source	Destination	What	ID	Action	Feature and serv
	1	Traffic to Internal...	In 0 B, out 0 B	To LAN, WiFi, VPN, DMZ	Firewall rules with the destination zone as LAN, WiFi, VPN, DMZ would be added to this group on the first match basis if user ...			
	2	Traffic to WAN	In 0 B, out 0 B	Outbound traffic to WAN	Firewall rules with the destination zone as WAN woul...			
	3	(example) Traffic...	In 0 B, out 0 B	Any zone, Any host	WAN, Any host	Any service	#3	Drop
	4	Chan Youtube	In 0 B, out 0 B	LAN, Any host	WAN, Social Network	Any service	#6	Reject
	5	Traffic to DMZ	In 0 B, out 0 B	Inbound traffic to DMZ	Firewall rules with the destination zone as DMZ woul...			
	6							
	7							

At the bottom right of the main content area is a 'Sophos Assistant' button.

– Lúc này ta không thể truy cập youtube được nữa

The screenshot shows a browser window with the URL 'youtube.com'. The page displays an error message: 'Không thể truy cập trang web này' (Cannot access this website). It states that 'youtube.com' has refused the connection. Below the message, there are troubleshooting steps: 'Hãy thử:' (Try this) followed by two bullet points: 'Kiểm tra kết nối' (Check connection) and 'Kiểm tra proxy và tường lửa' (Check proxy and firewall). At the bottom of the error page are buttons for 'Tải lại' (Reload) and 'Chi tiết' (Details).

Wednesday, December 13, 2023

## Đồ án Quản trị hệ thống Windows 2

### ❖ Ta có thể cấu hình chặn theo user trong Domain:

- Chọn Authentication → ở mục Servers nhấn Add

The screenshot shows the Sophos Firewall's web-based management interface. On the left, there's a navigation sidebar with sections like MONITOR & ANALYZE, PROTECT, CONFIGURE, and SYSTEM. Under PROTECT, the 'Authentication' option is highlighted. The main content area is titled 'Authentication' and has tabs for 'Servers', 'Services', 'Groups', 'Users', and 'Multi-factor authentication'. Below these tabs is a table with columns: Name, IP, Port, Type, and Domain/admin. A blue 'Add' button is located at the top right of the table area. The message 'No records found' is displayed below the table. At the bottom right, there's a 'Sophos Assistant' icon.

- Điền các thông số như sau:

<b>Server Type</b>	Active Directory
<b>Server Name</b>	< PC's name của Domain >
<b>Server IP</b>	< địa chỉ IPv4 của Domain >
<b>Connection Security</b>	Plaintext
<b>NetBIOS domain</b>	thebest
<b>AD username &amp; password</b>	< Tài khoản administrator >
<b>Domain name</b>	thebest.vn
<b>Search Queries</b>	dc=thebest, dc=vn

## Đồ án Quản trị hệ thống Windows 2

- Sau khi nhập các thông số như trên ta kiểm tra “Test connection”

The screenshot shows the Sophos Firewall webconsole interface. On the left, there's a sidebar with navigation links like Control center, Reports, and Authentication (which is currently selected). The main area has a form titled "Add external services". It includes fields for Connection security (Plaintext), Port (389), NetBIOS domain (thebest), ADS user name (administrator), Password (redacted), Display name attribute (Enter Display name attribute), Email address attribute (mail), Domain name (thebest.vn), and Search queries (dc=thebest,dc=vn). A green success message at the top right says "Device - AD server connectivity test successful". At the bottom, there are "Test connection", "Save", and "Cancel" buttons, along with a "Sophos Assistant" button.

- Sau khi kết nối thành công ta chọn import ở mục Manage

This screenshot shows the "Import Group Wizard help" page. At the top, there's a table with one row for a server entry. The columns are Name, IP, Port, Type, and Domain/admin, with values 172.16.16.19, 389, Active Directory, and administrator respectively. The "Manage" column has a red box around the edit icon. Below the table, the title "Import group wizard help" is displayed. The page contains two "Overview" sections and a numbered list of steps from 1 to 6. Step 1: "Provide base DN for Groups" and "Step 1. Provide base DN for groups". Step 2: "Select AD groups to Import" and "Step 2. Select AD groups to import". Step 3: "Select common policies for groups" and "Step 3. Select common policies for groups". Step 4: "Select specific policies for groups [if required]" and "Step 4. Select specific policies for groups [if required]". Step 5: "Review selection" and "Step 5: Review selection". Step 6: "View results" and "Once you have performed the above steps, your selected groups will be imported from Active Directory to the device and selected policies will be attached to them". At the bottom right are "Cancel" and "Start" buttons.

## Đồ án Quản trị hệ thống Windows 2

S Import Group Wizard - Google Chrome

Không bảo mật https://172.16.16.16:4444/webconsole/webpages/identity/MigrateGroup.jsp?serverid=...

### Import group wizard help

Overview Step 1: Provide base DN for groups

1 Provide base DN for Groups Currently, authentication is integrated with Active Directory.  
Here, provide base DN for groups

2 Select AD groups to Import Base DN \* dc=thebest,dc=vn

3 Select common policies for groups

4 Select specific policies for groups (if required)

5 Review selection

6 View results

< > Cancel

- Chọn group HCM (chứa user test) và HN (chứa user hn1)

S Import Group Wizard - Google Chrome

Không bảo mật https://172.16.16.16:4444/webconsole/webpages/identity/MigrateGroupToAppliance.jsp... 🌐 🔍

### Import group wizard help

Overview Step 2. Select AD groups to import

1 Provide base DN for Groups Please select the groups from AD server which you want to import into the device. If you import OU, OU will also be imported as a group in the device

2 Select AD groups to Import

3 Select common policies for groups

4 Select specific policies for groups (if required)

5 Review selection

6 View results

Note:  indicates a group/user which already exists in the device or it is a invalid group name

AD groups	Selected groups
<input type="checkbox"/> thebest.vn	<input checked="" type="checkbox"/> HCM
<input type="checkbox"/> Builtin	<input checked="" type="checkbox"/> HN
<input type="checkbox"/> Users	
<input checked="" type="checkbox"/> HCM	
<input checked="" type="checkbox"/> HN	
<input type="checkbox"/> Domain Controllers	

< > Cancel

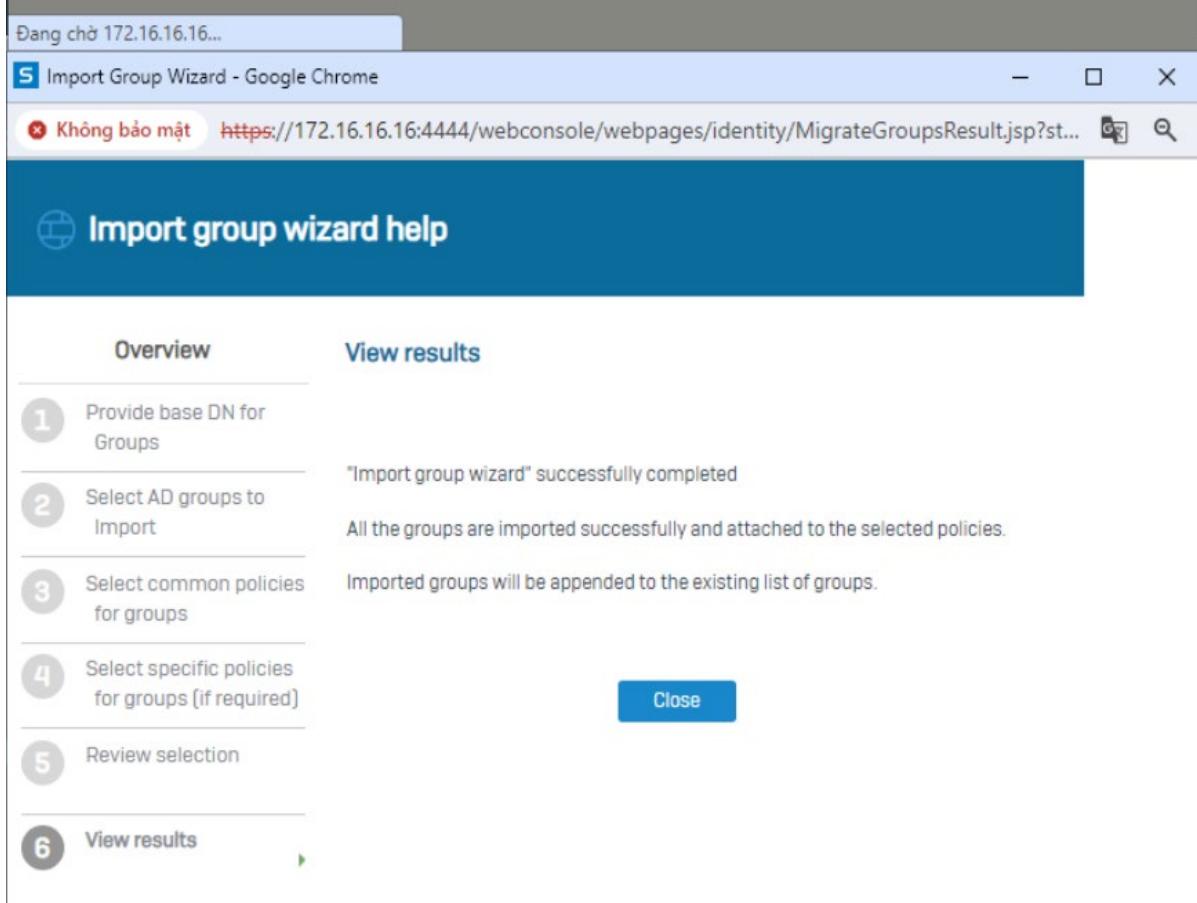
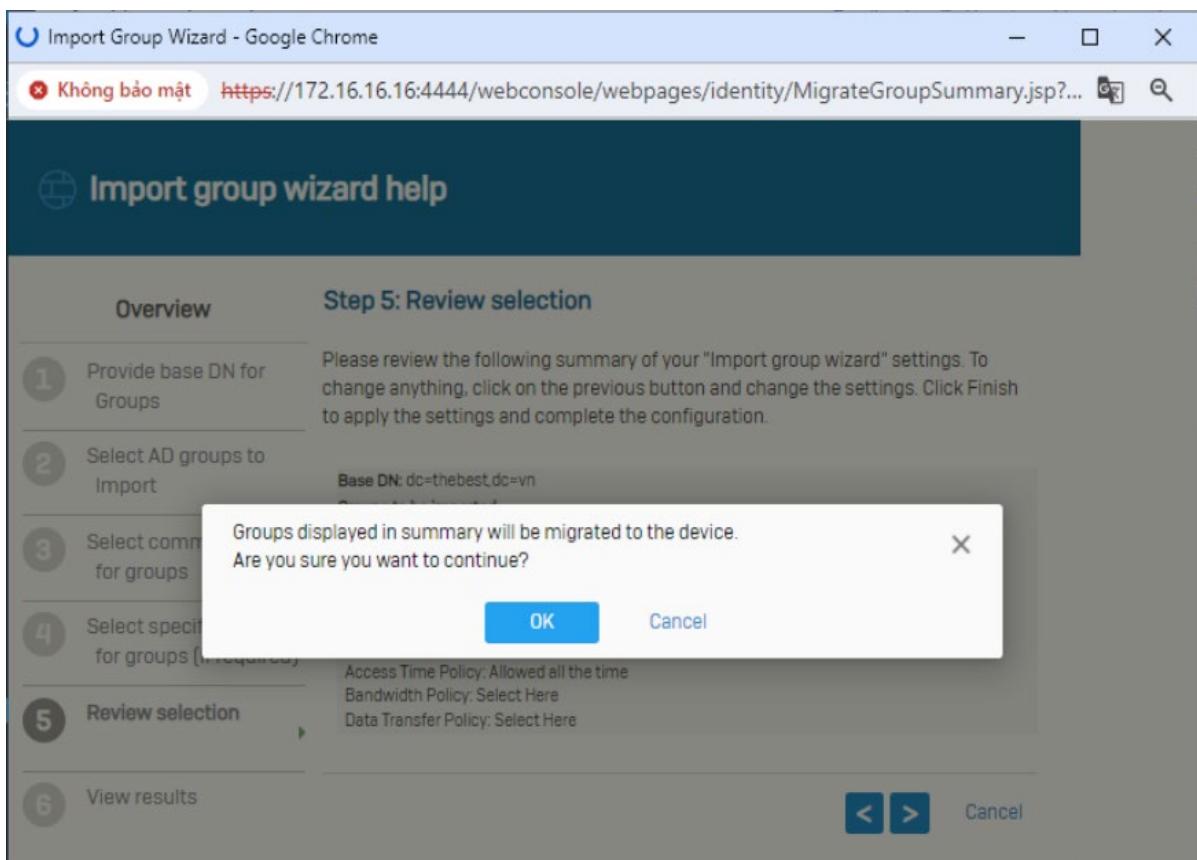
# Đồ án Quản trị hệ thống Windows 2

## – Chọn Next

The screenshot shows the 'Import group wizard help' interface. On the left, a vertical navigation bar lists steps 1 through 6. Step 3, 'Select common policies for groups', is currently selected and expanded, showing four policy options: Surfing quota, Access time, Bandwidth policy, and Network traffic. To the right, a large section titled 'Step 3: Select common policies for groups' contains descriptive text and a checkbox labeled 'Attach to all the groups?'. This checkbox is checked for all four policy options. At the bottom right are navigation buttons for 'Cancel', '<', and '>'.

The screenshot shows the 'Import group wizard help' interface. The navigation bar on the left shows steps 1 through 6, with step 5, 'Review selection', currently selected. The main area is titled 'Step 5: Review selection' and contains a summary of the configuration. It includes sections for 'Base DN', 'Groups to be imported', and 'Common policies for groups'. The 'Base DN' is set to 'dc=thebest,dc=vn'. The 'Groups to be imported' list includes 'HCM' and 'HN'. The 'Common policies for groups' section lists four policies: 'Surfing Quota Policy: Unlimited Internet Access', 'Access Time Policy: Allowed all the time', 'Bandwidth Policy: Select Here', and 'Data Transfer Policy: Select Here'. Navigation buttons for 'Cancel', '<', and '>' are at the bottom right.

## Đồ án Quản trị hệ thống Windows 2



## Đồ án Quản trị hệ thống Windows 2

- Ta quay lại phần **Authentication** → chọn **Service** → tích chọn **Active Directory** mà ta đã thêm vào (Server) để firewall có thể xác thực bằng tài khoản user trong domain

The screenshot shows the Sophos Firewall interface under the 'Authentication' tab. A red box highlights the 'Services' tab. Below it, a red box highlights the 'Selected authentication server' section where 'SERVER' is selected. Another red box highlights the 'Authentication server list' section where 'SERVER' is checked.

- Vào máy Windows Client cài đặt phần mềm **Sophos Endpoint Agent** để tường lửa đồng bộ xác thực user trong domain

The screenshot shows the Sophos Endpoint Agent status window. It displays the following information:

- Your device is protected (green checkmark icon)
- No malware or PUAs (green globe icon)
- Data protection is off (red lock icon): We've let your IT admin know
- Zero Trust Network Access : Not Configured (grey ZT icon)

A blue bar at the bottom shows the Windows taskbar with various icons and system status.

## Đồ án Quản trị hệ thống Windows 2

- Sau khi cài đặt xong ta quay về trang chủ cấu hình Sophos (<https://172.16.16.16:4444>) → vào mục **Current activities** → mục **Live users** kiểm tra xem tường lửa đã đồng bộ xác thực thành công hay chưa (nếu chưa thì ta cần **Sign out** trên Windows Client và tiến hành đăng nhập lại).

The screenshot shows the Sophos Firewall webconsole interface. The left sidebar has sections for MONITOR & ANALYZE, PROTECT, and SYSTEM. The PROTECT section is expanded, showing Rules and policies, Intrusion prevention, Web, Applications, Wireless, Email, Web server, and Advanced protection. The SYSTEM section is also expanded, showing Sophos Central, Profiles, Hosts and services, Administration, Backup & firmware, and Certificates. The main content area is titled "Current activities" and has tabs for "Live users", "Live connections", "Live connections IPv6", "IPsec connections", and "Remote users". The "Live users" tab is selected, showing a table with one row: User ID 9, Username hn1@thebest.vn, Client type Heartbeat, Host IP 172.16.16.100, IP version IPv4, MAC, and Start time 2023-12-16 14:49. A "Disconnect" button is at the top right of the table. A "Sophos Assistant" icon is in the bottom right corner.

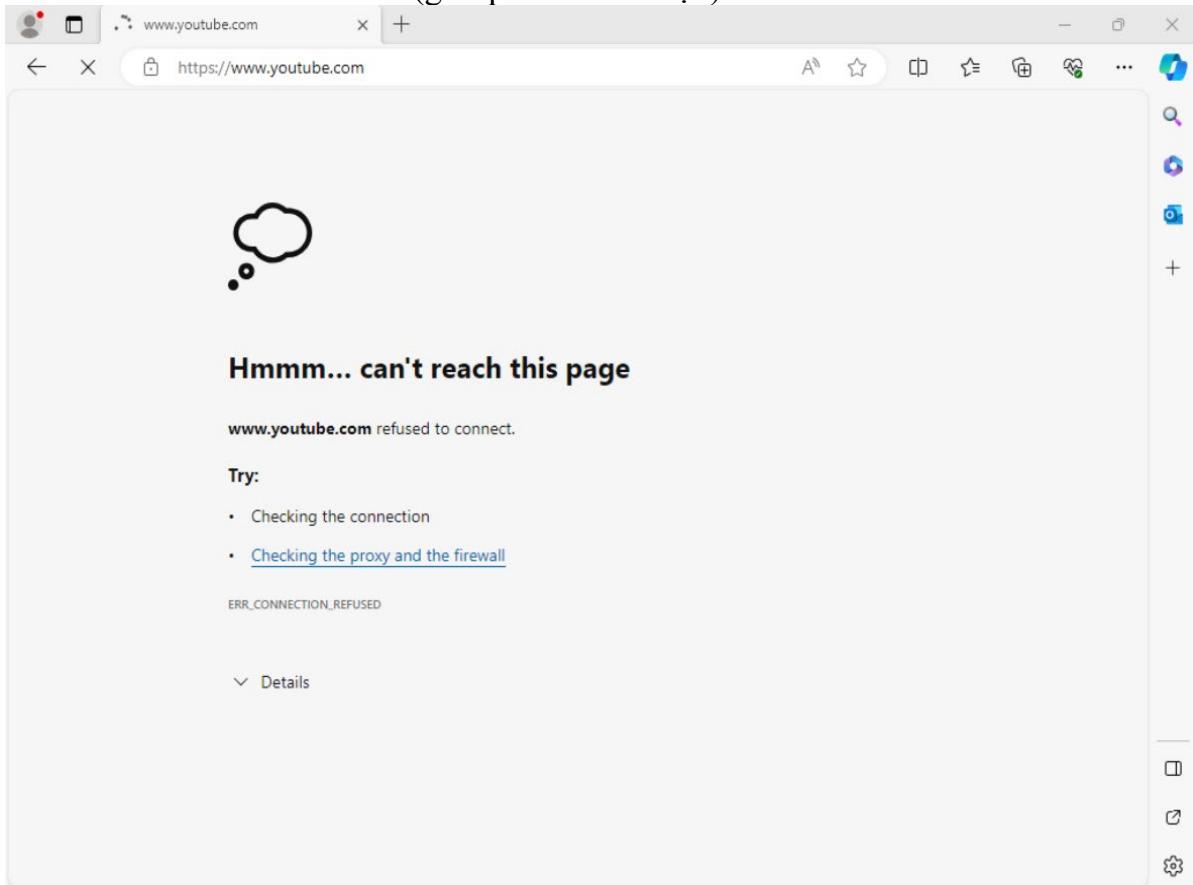
- Sau đó vào mục **Rules and Policies** → **Edit policy “Chan Youtube”** → ở phần **Match known users** thêm vào group **HCM** (chứa user test)

The screenshot shows the Sophos Firewall webconsole interface for editing a firewall rule. The left sidebar is identical to the previous screenshot. The main content area is titled "Edit firewall rule" for policy "Chan Youtube". It shows destination zones (WAN), destination networks (Social Network), and services (Any). Under the "Match known users" section, a checkbox is checked. Under "User or groups", "HCM" is listed. There is also an "Add new item" button. A note says "Services are traffic types based on a combination of protocols and ports." At the bottom, there is an "Add exclusion" section with a help icon.

- Kiểm tra policy vừa Edit

## Đồ án Quản trị hệ thống Windows 2

- Đổi với tài khoản **test** (group HCM → chặn)



- Kiểm tra Log Viewer của tường lửa:

A screenshot of the Sophos Firewall Log Viewer. The interface shows a list of log entries. Each entry includes a red shield icon labeled "Firewall", the date and time (e.g., 2023-12-16 15:09:29), the rule type ("Firewall Rule"), the action ("Denied"), the source IP ("test@thebest.vn"), the port ("6"), the destination ("Chan Youtube"), and two columns for "PortA" and "PortB". There are 10 entries listed, all showing the same pattern of a denied firewall rule from port 6 to Chan Youtube.

- Test Policy tại trình “Log Viewer” của Sophos Firewall:

## Đồ án Quản trị hệ thống Windows 2

Log viewer Policy test

Connection details

URL: youtube.com

User: Authenticated user (checked), test@thebest.vn

Time and day: 15 : 11 Saturday

Test method: Firewall, SSL/TLS, and web

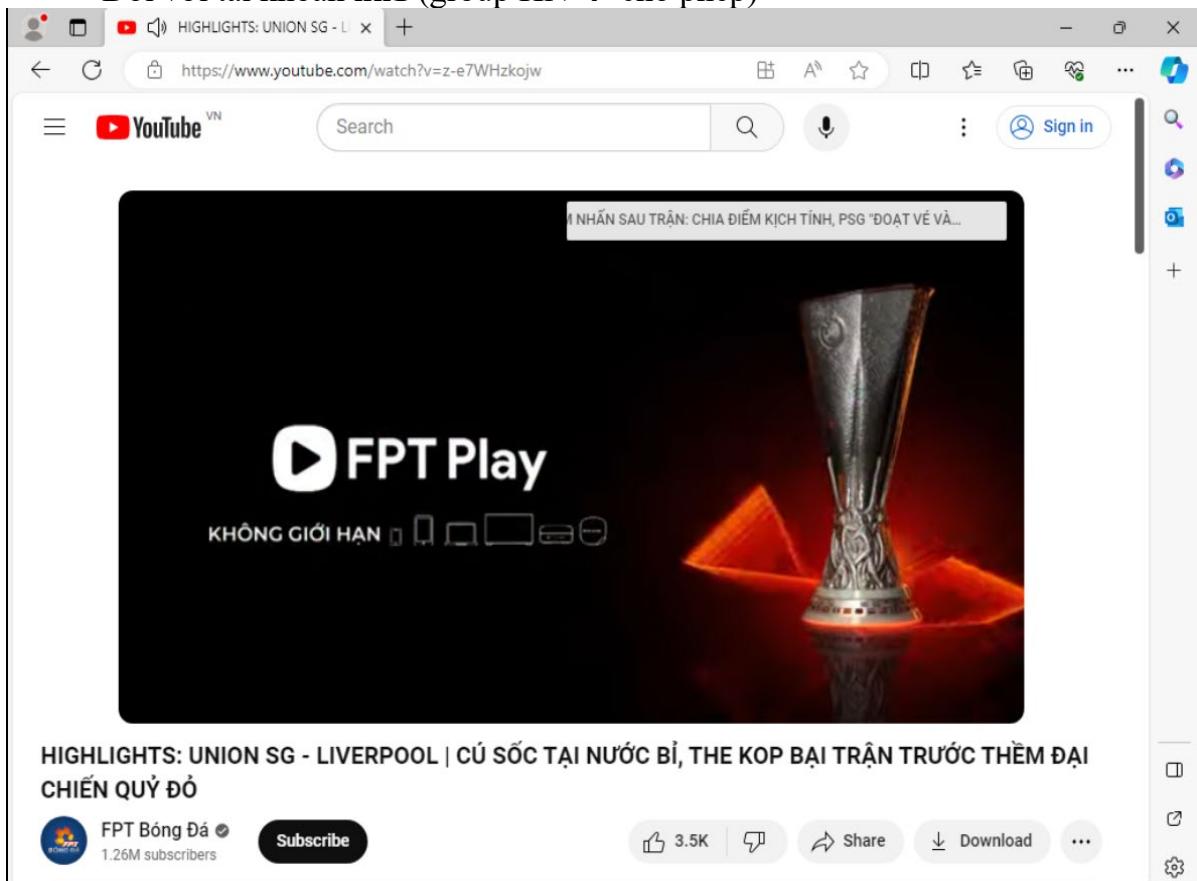
Source IP: 172.16.16.100

Source zone: Auto-detection

Connection: Test time: 15:11:30 Saturday, Destination: http://youtube.com, Destination IP: 142.251.12.91, port 80, TCP, Source IP: 172.16.16.100, Source zone: Auto-detection, User: test@thebest.vn, Firewall rule: Chan Youtube [ID: 6] Reject, Result: Rejected

Clear Test

– Đổi với tài khoản hn1 (group HN → cho phép)



– Test policy trên Log Viewer

## Đồ án Quản trị hệ thống Windows 2

The screenshot shows the Sophos Firewall's Log viewer interface. On the left, the 'Connection details' section displays configuration for a connection to youtube.com. It includes fields for URL, User (Authenticated user), Time and day (15:24 Saturday), Test method (Firewall, SSL/TLS, and web), Source IP (172.16.16.100), and Source zone (Auto-detection). Below these are 'Clear' and 'Test' buttons. On the right, the 'Policy test' results are shown in a table. The 'Connection' row lists the test time (15.24/41 Saturday), destination (http://youtube.com), source IP (172.253.118.93), port (80, TCP), and user (hn1@thebest.vn). The 'Firewall rule' row indicates the rule accepted (#Default\_Network\_Policy [ID: 5] Accept) and that no proxy was used. The 'Result' row shows the connection was allowed. The 'Web protection' row shows the category (Video hosting) and web policy (Default Policy). The 'Matched web rule' section shows a single rule with a green checkmark in the 'Action' column. The table has columns for 'Users', 'Activities', and 'Action'.

## 2.3 Web Protection

### 2.3.1 Khái niệm

Web Protection trên Sophos Firewall là một tính năng an ninh mạng được thiết kế để bảo vệ người dùng và mạng khỏi các mối đe dọa từ Internet khi truy cập các trang web. Đây là một phần của bộ công cụ bảo mật toàn diện của Sophos Firewall, giúp ngăn chặn malware, chống lại các cuộc tấn công trực tuyến, và kiểm soát nội dung truy cập từ các trang web độc hại hoặc không an toàn.

Một số tính năng chính của Web Protection trên Sophos Firewall:

- **Blocking Malicious Websites:** Web Protection giúp chặn truy cập đến các trang web được xác định là độc hại, chứa malware, hoặc liên quan đến các hoạt động tấn công mạng.
- **URL Filtering:** Tính năng này kiểm soát việc truy cập vào các loại trang web cụ thể hoặc các danh mục nội dung nhất định, giúp kiểm soát và quản lý sự xuất hiện của nội dung không mong muốn.
- **HTTPS Scanning:** Sophos Firewall có khả năng kiểm soát và quét nội dung truy cập qua giao thức HTTPS, giúp ngăn chặn các mối đe dọa ẩn danh.

## Đồ án Quản trị hệ thống Windows 2

- **Phishing Protection:** Ngăn chặn trang web giả mạo và các kỹ thuật lừa đảo trực tuyến nhằm đánh cắp thông tin cá nhân.
- **Application Control:** Kiểm soát và quản lý việc sử dụng các ứng dụng web, giúp ngăn chặn việc truy cập vào các dịch vụ không an toàn hoặc không mong muốn.
- **Real-time Threat Intelligence:** Sử dụng thông tin tình báo để dọa thời gian thực để nhận diện và ngăn chặn các mối đe dọa mới và tiến triển.
- **Reporting and Logging:** Cung cấp báo cáo và ghi lại sự kiện liên quan đến hoạt động trên mạng, giúp quản trị viên theo dõi và đánh giá mức độ an toàn của hệ thống.

Tính năng Web Protection của Sophos Firewall là một phần quan trọng của chiến lược bảo mật, giúp bảo vệ người dùng và dữ liệu khỏi các mối đe dọa trực tuyến khi duyệt web.

### 2.3.2 Cấu hình (chặn user truy cập các web cờ bạc)

- Ta vào trang chủ Sophos Firewall → chọn mục **Web** → ở trang **Policies** → chọn **Add Policy**

The screenshot shows the Sophos Firewall interface. On the left sidebar, under the 'PROTECT' section, the 'Web' option is selected and highlighted with a red box, labeled '1.'. In the main content area, the 'Web' tab is active, and the 'Policies' tab is selected, also highlighted with a red box, labeled '2.'. On the right, there is a table titled 'Policy test' listing various policies. A red box highlights the 'Add policy' button at the top right of the table, labeled '3.'.

Name	Description	In use	Manage
Default Policy	A typical starter policy with options suitable for many organizations	1	[Edit]
Default Workplace Policy	Deny access to categories most commonly unwanted in professional environments	0	[Edit]
No Ads or Explicit Content	Deny access to advertisements and sexually explicit sites	0	[Edit]
No Explicit Content	Deny access to sexually explicit sites	0	[Edit]
No Games Ads or Explicit Content	Deny access to games, advertisements, and sexually explicit sites	0	[Edit]
No Online Chat	Deny access to online chat sites	0	[Edit]
No Web Mail	Deny access to web mail sites	0	[Edit]
No Web Mail or Chat	Deny access to web mail and online chat sites	0	[Edit]
No web uploads	Restrict users from uploading content to any site	0	[Edit]
block share file		0	[Edit]

- Đặt tên cho Policy → Add rule

## Đồ án Quản trị hệ thống Windows 2

The screenshot shows the 'Add web policy' interface. At the top, there are fields for 'Name\*' (Chan Web Co Bac) and 'Description'. Below these are tabs for 'Users', 'Activities', 'Action', 'Constraints', 'Manage', and 'Status'. Under the 'Action' tab, a 'Default action' is selected with a green checkmark. A large button labeled 'Add rule' is located at the top right. In the 'Search engine enforcement' section, there are two options: 'Enforce SafeSearch' (unchecked) and 'Enforce YouTube restrictions' (unchecked). Each option has a dropdown menu and a warning message. A 'Sophos Assistant' button is visible at the bottom right.

- Ta chinh các tùy chọn của rule như sau:
  - **Users:** Anybody
  - **Activities:** Game & Gambling
  - **Action:** Block HTTP / HTTPS
  - **Constraint:** All the time
  - **Status:** On

This screenshot shows a more detailed view of the 'Add web policy' interface. It includes the same basic fields and tabs as the previous screenshot. The 'Activities' tab is active, showing 'All web traffic' under 'Content filters'. A dropdown menu for 'User activity' is open, displaying a list of categories. The 'Games and Gambling' category is checked. A green button at the bottom left says 'Apply 1 selected items'. A 'Sophos Assistant' button is at the bottom right.

## Đồ án Quản trị hệ thống Windows 2

The screenshot shows a firewall configuration interface. At the top, there is a form to enter a policy name ('Name\*' field contains 'Chan Web Co Bac') and a description (empty). Below this is a table titled 'Users' with columns: 'Users', 'Activities', 'Action', 'Constraints', 'Manage', and 'Status'. A single row is present: 'Anybody' under 'Users', 'Games and Gambling' under 'Activities', 'Deny' under 'Action', and 'Lock' under 'Constraints'. There are icons for adding (+), deleting (-), and managing (trash bin) rules. A status indicator shows 'ON'. At the bottom, a 'Default action' row has a green checkmark icon.

**Lưu ý:** Default action là sau khi Firewall xem xét traffic qua tất cả các rule bên trên mà không thỏa điều kiện thì nó sẽ thực hiện Default action.

- Sau khi thêm Policy thành công thì lúc này vẫn chưa có hiệu lực, ta cần gán nó vào một Firewall rule nào đó

The screenshot shows the Sophos Firewall web console. The left sidebar has sections like MONITOR & ANALYZE, PROTECT, CONFIGURE, and SYSTEM. Under PROTECT, 'Rules and policies' is selected. The main area shows a table of policies. A green success message at the top says 'Web policy "Chan Web Co Bac" has been created successfully.' A modal dialog box in the center says 'Add this policy to a firewall rule.' It includes a note 'For your policy to take effect, add it to a firewall rule.', a blue button 'Go to firewall rules', and a blue link 'Skip this step'.

- Ta vào Rules and policies → Add firewall rule → New firewall rule:

Lưu ý: Ta phải để phần action là “Accept” thì mới thêm Web policies vào được

## Đồ án Quản trị hệ thống Windows 2

Add firewall rule

Feedback How-to guides Log viewer Help admin FIT TDC

Rule status: On

Rule name \*: Chan web co bac

Description: Enter Description

Action: Accept (highlighted with a red box)

Rule position: Top

Rule group: Traffic to WAN

Log firewall traffic:  Logs traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

**Source**  
Select the source zones, networks, and devices.  
The rule applies to traffic from these sources during the scheduled time period.

Source zones \*: LAN

Source networks and devices \*: Any

During scheduled time: All the time

**Destination and services**  
Select the destination zones, networks, devices, and services.  
The rule applies to traffic to these destinations.

Destination zones \*: WAN

Destination networks \*: Any

Services \*: Any

- Kéo xuống phần **Security features** → mục **Web policy** chọn “**Chan web co bac**”

Match known users

Add exclusion

Create linked NAT rule

**Security features**

Web filtering

Web policy: Chan Web Co Bac (highlighted with a red box)

Apply web category-based traffic shaping:

Block QUIC protocol:

Malware and content scanning

Scan HTTP and decrypted HTTPS:

Use zero-day protection:

Scan FTP for malware:

Filtering common web ports

Use web proxy instead of DPI engine:

DPI engine or web proxy?:

Web proxy options

Decrypt HTTPS during web proxy filtering:

- Cuối cùng save lại và qua máy Client kiểm tra:

## Đồ án Quản trị hệ thống Windows 2

Khi không có Web Protection

Thể Thao Casino Casino Trực Tuyến Thể Thao Ảo Xổ Số Khuyến Mãi Ứng Dụng ĐĂNG NHẬP

CÔNG AN HÀ NỘI VS QUẢNG NAM 15/12/2023 | 19:15  
HỒNG LĨNH HÀ TĨNH VS BÌNH ĐỊNH 16/12/2023 | 17:00  
BÌNH DƯƠNG VS NAM ĐỊNH 16/12/2023 | 18:00  
THÀNH HÓA VS TP. HỒ CHÍ MINH 16/12/2023 | 18:00  
SÔNG LAM NGHỆ AN VS HOÀNG ANH GIA LAI 17/12/2023 | 17:00  
VIETTEL VS HÀ NỘI 17/12/2023 | 19:15  
HẢI PHÒNG VS KHÁNH HÒA 18/12/2023 | 18:00

V-League 2023  
Xem ngay tỷ lệ cược hấp dẫn của Giải Vô Địch Quốc Gia Việt Nam tại 188BET! XEM CUỘC

Casino Trực Tuyến Nổi Bật XEM TẤT CẢ → Bàn Chơi Phổ Biến XEM TẤT CẢ →

Khi có Web Protection

SOPHOS

Stop!  
This website is blocked

The administrator of this network has restricted access to sites categorized as Gambling.

If you think this is incorrect, you may [suggest a different category](#).

[Return to previous page](#)

About this request

Protected by SOPHOS

**Lưu ý:** Khi thay đổi một firewall rule (bật, tắt, thêm, xóa, sửa...) thì rule đó chỉ có hiệu lực khi user login ở lần tiếp theo ( log out → login lại mới được).

## 2.4 Mail Protection

### 2.4.1 Khái niệm

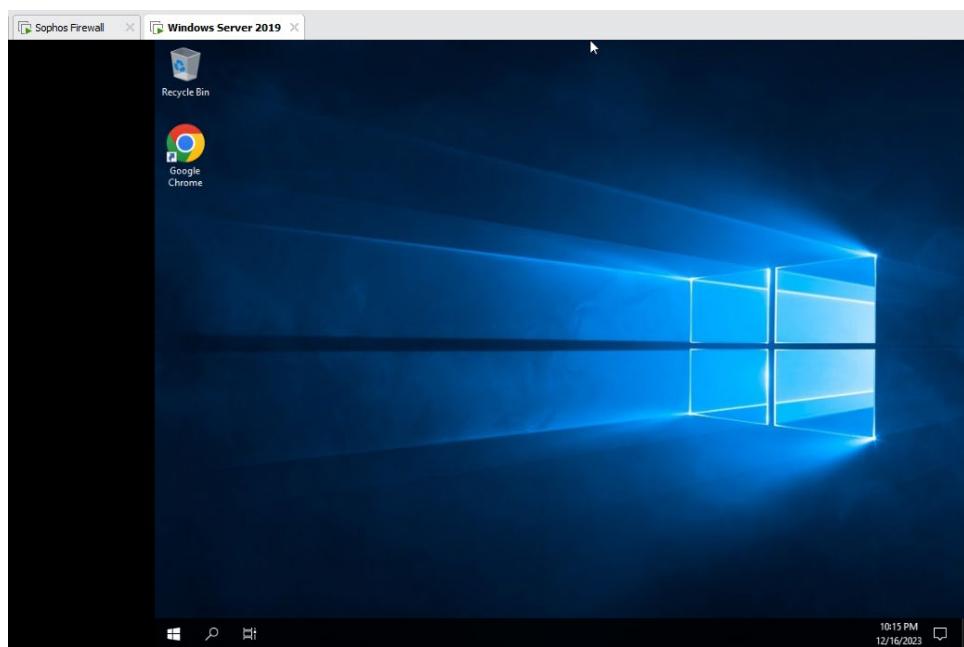
Mail Protection hay còn gọi là Email Security là một trong những ứng dụng của Sophos Firewall giúp bảo vệ những email được gửi và nhận khỏi các mối đe dọa như virus và thư rác. Các tính năng nổi bật của Email Security:

- **Phát hiện những Mailboxes bị xâm nhập:** Các thiết bị bị xâm phạm sử dụng tên tổ chức và hộp thư của bạn để phát tán thư rác và lừa đảo. Sophos Email sẽ kết nối với Sophos Endpoint Protection để tự động phát hiện và ngăn chặn các tin nhắn độc hại này.
  - **Ngăn chặn việc mất dữ liệu:** Tạo ra những chính sách multi-rule DLP cho các nhóm và cá nhân để tăng cường việc bảo vệ các thông tin quan trọng trong tất cả các emails và tệp đính kèm.
  - **Mã hóa và bảo mật:** Mã hóa các thư và thêm chữ ký điện tử để xác minh người gửi bằng S/MIME, hoặc chọn các tùy chọn mã hóa có thể tuỳ chỉnh bao gồm mã hóa TLS, mã hóa tệp đính kèm.
  - **Sức mạnh của AI học chuyên sâu:** Trí thông minh nhân tạo học chuyên sâu của Sophos chặn phần mềm độc hại zero-day và các ứng dụng không mong muốn.
  - **Thông tin về mối đe dọa được chia sẻ:** Tối đa hóa đầu tư bảo mật với thông tin về mối đe dọa được chia sẻ từ người dùng cuối và bảo vệ email trong hồ sơ dữ liệu Sophos XDR. Cho phép bạn xác định các dấu hiệu xâm phạm chưa từng thấy trước đây hoặc xóa các tệp đáng ngờ trong môi trường làm việc. Sau đó, mở rộng khả năng hiển thị trên Microsoft 365, khởi động công việc trên máy chủ đám mây, mạng và hơn thế.
- ❖ **Có 2 chế độ:**
- **Chế độ MTA:** Hành động như là một nhân tố vận chuyển mail, định tuyến và trả lời emails. Hiển thị những mail đang đợi để được gửi đi và mail logs.
  - **Chế độ Legacy:** Hành động như một proxy mail trong suốt để gửi những email.

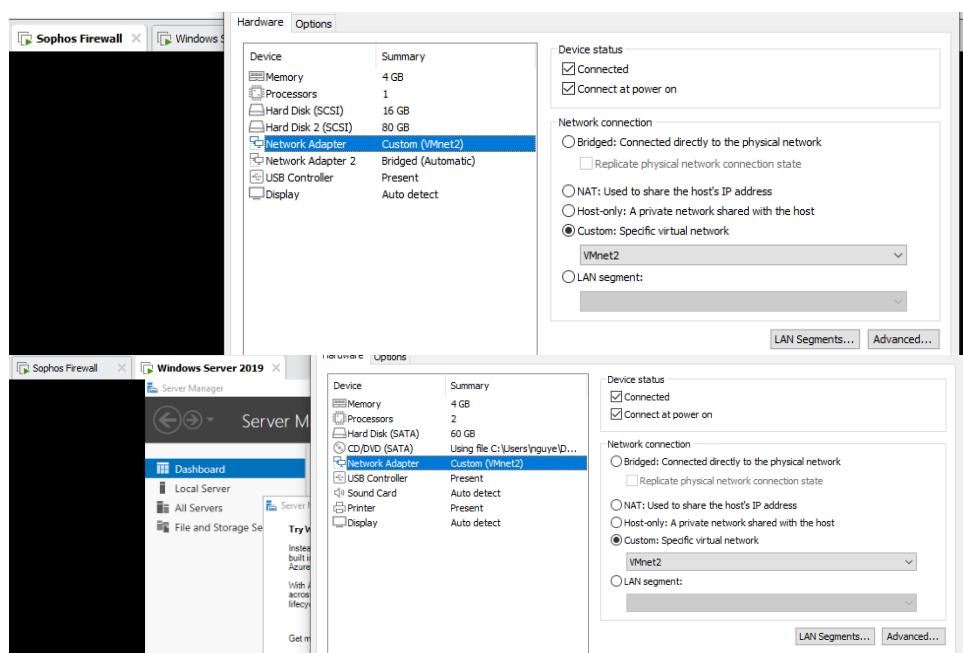
### 2.4.2 Cấu hình

- Đầu tiên ta chuẩn bị 1 máy Window Server và 1 Sophos Firewall

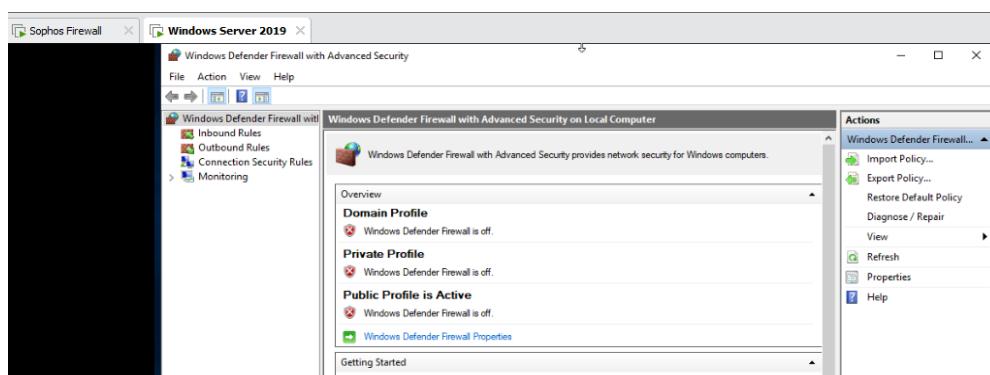
## Đồ án Quản trị hệ thống Windows 2



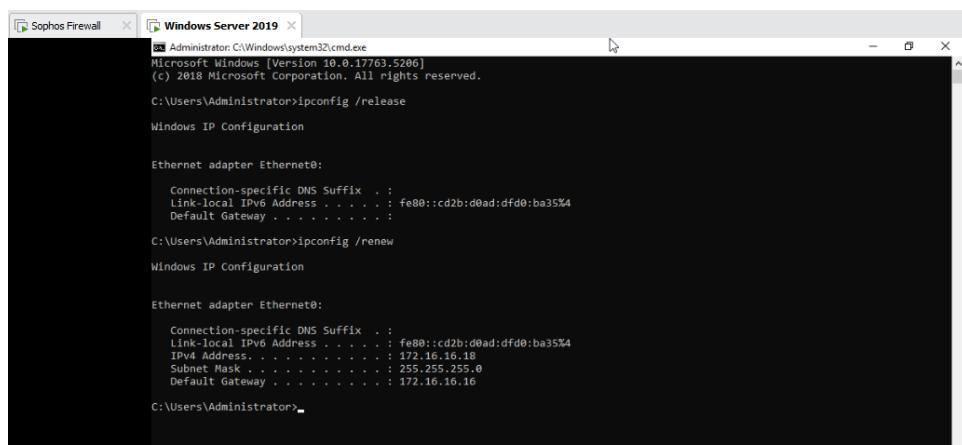
- Sau đó chỉnh card mạng của Server chung với Firewall



- Tắt tường lửa và chạy IP động cho máy Server



## Đồ án Quản trị hệ thống Windows 2



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.5206]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig /release
Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . : fe80::cd2b:d0ad:dfd0:ba35%4
Default Gateway . . . . . :

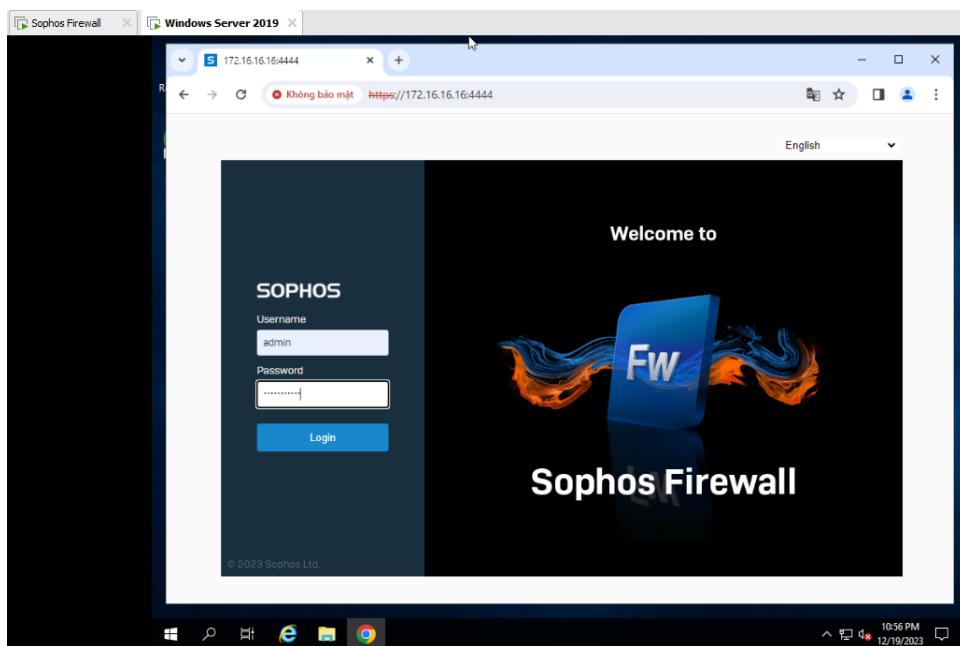
C:\Users\Administrator>ipconfig /renew
Windows IP Configuration

Ethernet adapter Ethernet0:

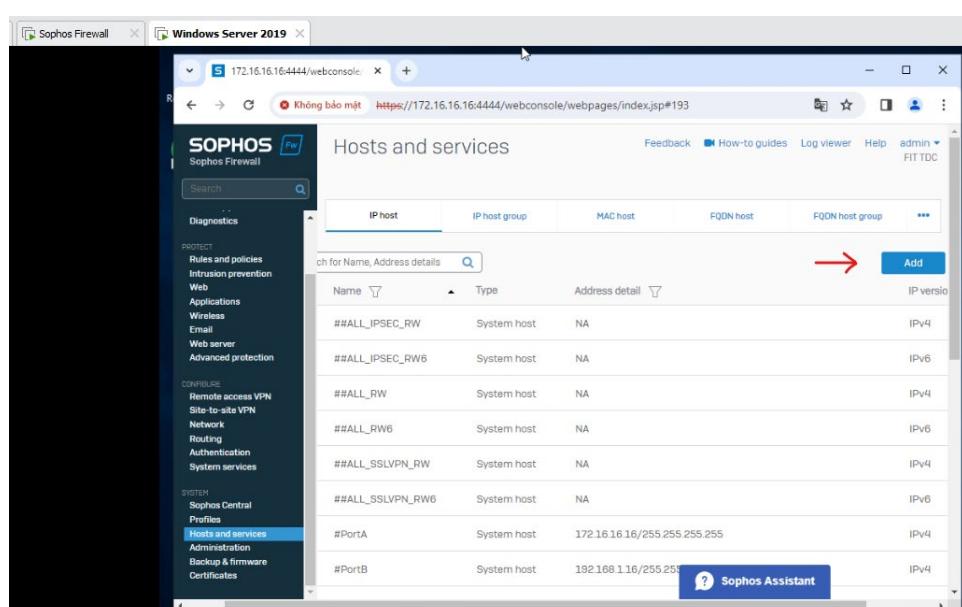
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . : fe80::cd2b:d0ad:dfd0:ba35%4
IPv4 Address . . . . . : 172.16.16.18
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.16.16.16

C:\Users\Administrator>
```

- Ta vào địa chỉ của Firewall để cấu hình policy



- Vào mục Hosts and Services để thêm địa chỉ của mail server

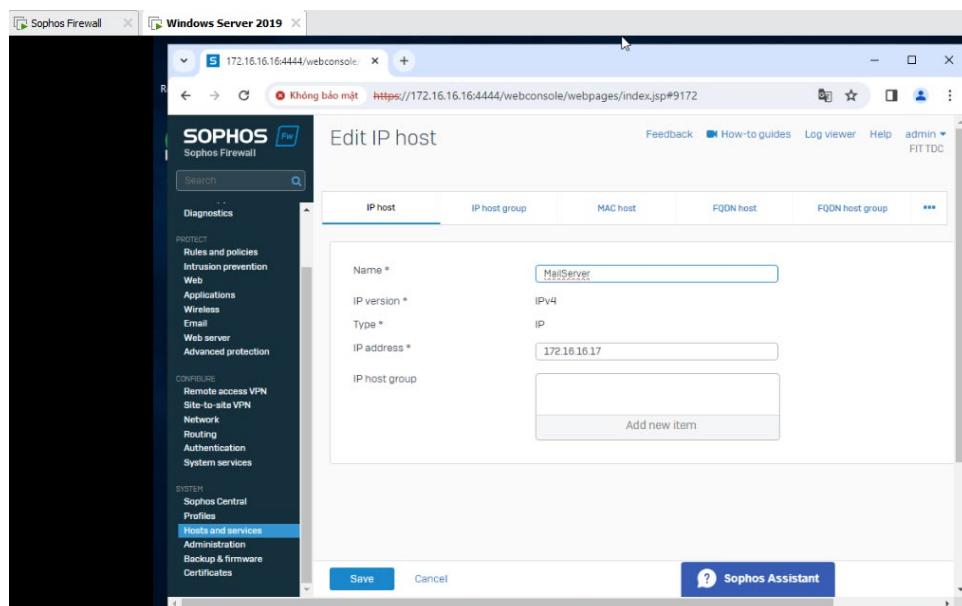


The screenshot shows the "Hosts and services" section of the Sophos Firewall webconsole. On the left, a sidebar lists various categories like "Diagnostics", "Rules and policies", "Intrusion prevention", etc. The "Hosts and services" option is selected. The main area shows a table of hosts:

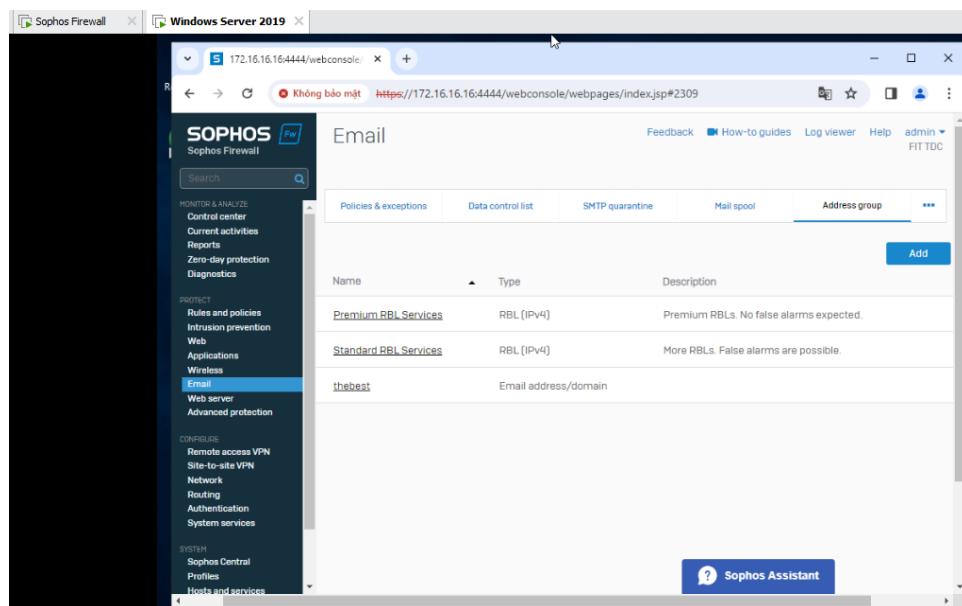
Name	Type	Address detail	IP version
##ALL_IPSEC_RW	System host	NA	IPv4
##ALL_IPSEC_RW6	System host	NA	IPv6
##ALL_RW	System host	NA	IPv4
##ALL_PW6	System host	NA	IPv6
##ALL_SSLVPN_RW	System host	NA	IPv4
##ALL_SSLVPN_RW6	System host	NA	IPv6
#PortA	System host	172.16.16.16/255.255.255.255	IPv4
#PortB	System host	192.168.1.16/255.255.255.255	IPv4

- Thêm địa chỉ của mail server

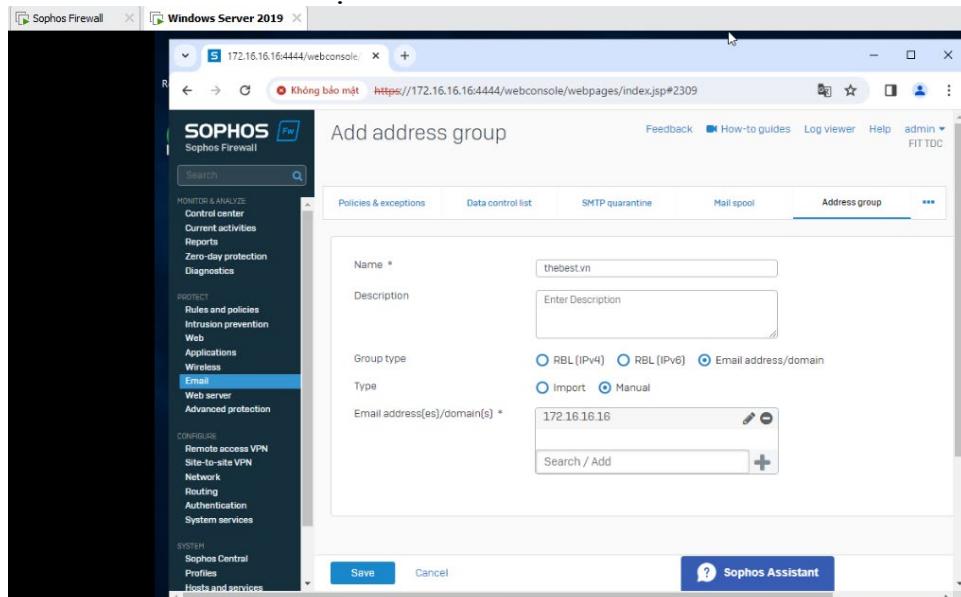
## Đồ án Quản trị hệ thống Windows 2



- Vào phần email tìm Address Group để thêm domain của máy email server

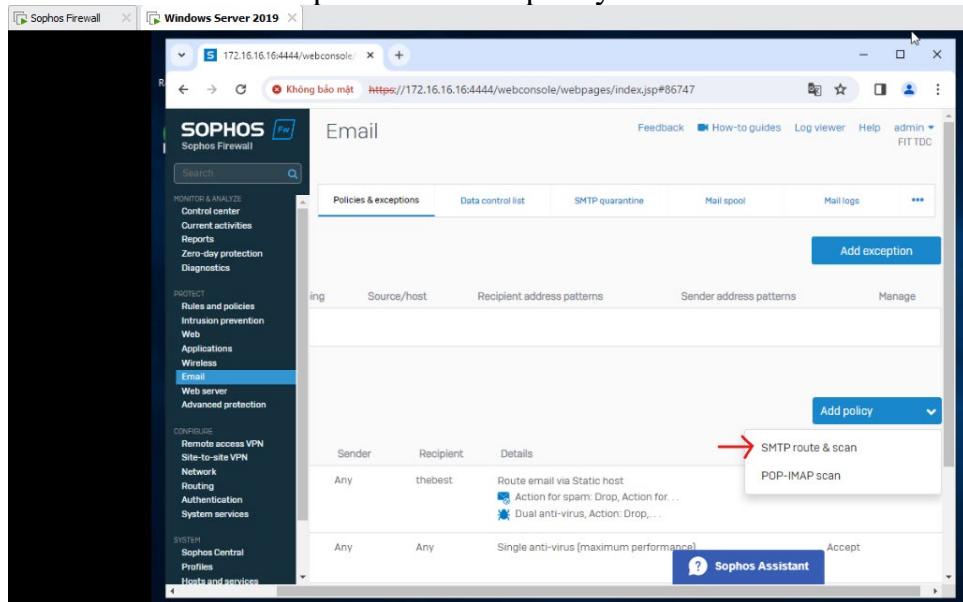


- Thêm tên domain và địa chỉ IP

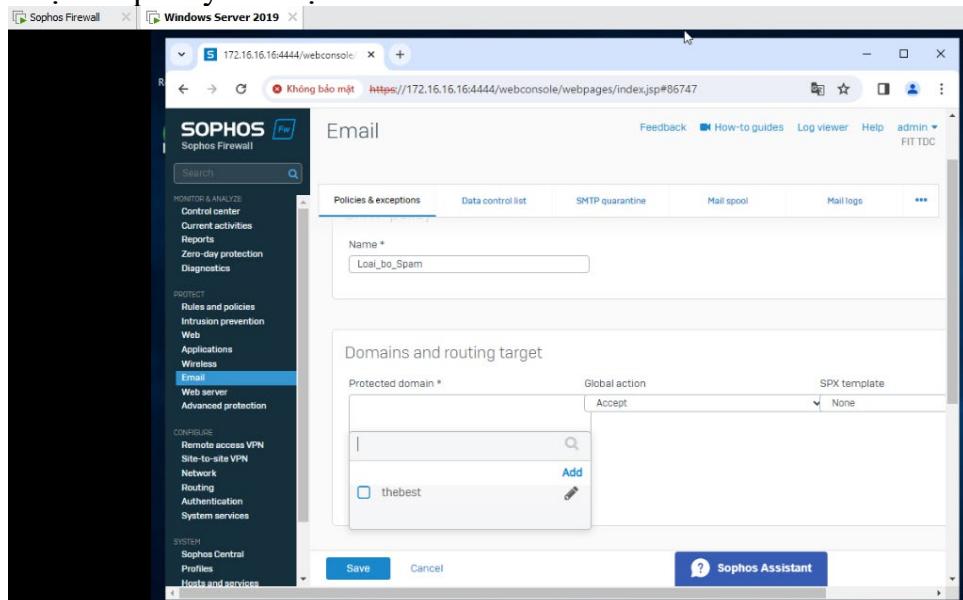


## Đồ án Quản trị hệ thống Windows 2

- Vào Policies & Exceptions để thêm policy mình cần



- Đặt tên policy và chọn domain mà mình đã thêm vào



- Chọn spam protection và mailware protection hoặc theo nhu cầu muốn bảo vệ của doanh nghiệp.

## Đồ án Quản trị hệ thống Windows 2

The screenshot shows two stacked windows of the Sophos Firewall web console. Both windows have the URL <https://172.16.16.16:4444/webconsole/webpages/index.jsp#86747> in the address bar. The top window is titled 'Email' and displays the 'Policies & exceptions' tab. It shows 'Spam protection' is turned on, with 'Check for inbound spam' checked. Under 'Spam', there are sections for 'Action for spam' (Drop, Warn, [SPAM]), 'Action for bulk mail' (Warn, [BULK]), and 'Actions when connection starts' (Use greylisting). The bottom window is also titled 'Email' and displays the 'Policies & exceptions' tab. It shows 'Malware protection' is turned on, with 'Scanning' set to 'Dual anti-virus'. Under 'Selected antivirus action', 'Drop' is selected. Other options include 'Notify sender' (unchecked) and 'Quarantine unscannable content' (checked). There is also a 'Use zero-day protection' checkbox. Below these, a 'File protection' section is shown as 'off'.

## 2.5 Antivirus

### 2.5.1 Khái niệm

Sophos Central phát hiện và dọn dẹp các virus, Trojan, worm, phần mềm gián điệp, phần mềm quảng cáo cũng như các phần mềm không mong muốn khác. Sophos liên tục quét, thông báo về các mối đe doạ và cập nhật phần mềm thường xuyên khi bạn trực tuyến. Các tính năng nổi bật của Sophos về Antivirus:

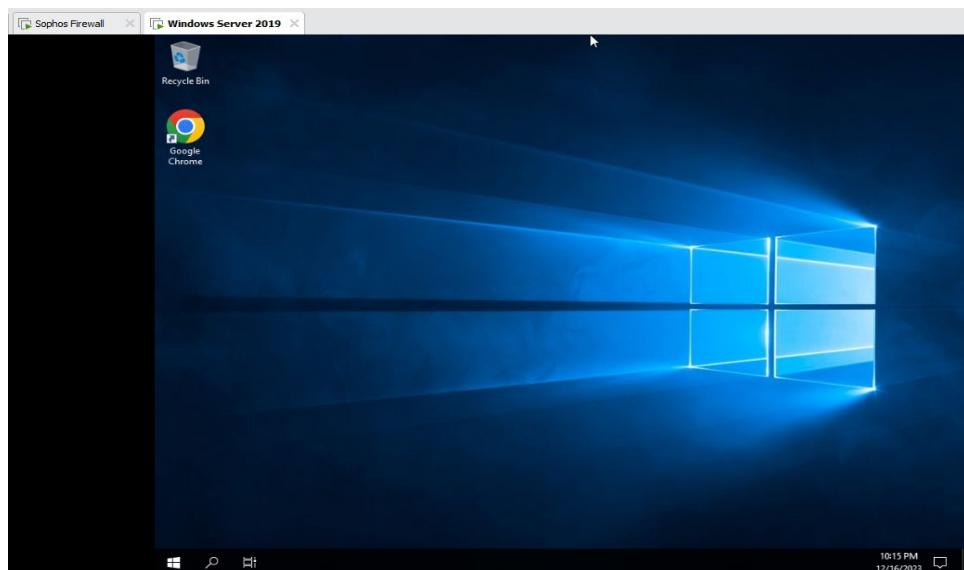
- **Antivirus Scanning:** Sophos Firewall cung cấp tính năng quét antivirus để phát hiện và ngăn chặn virus, malware và các mối đe dọa khác trước khi chúng có thể xâm nhập vào hệ thống.

## Đồ án Quản trị hệ thống Windows 2

- **Sophos Sandstorm:** Sandstorm là một tính năng tiên tiến của Sophos Firewall, giúp chống lại các mối đe dọa mới và không xác định bằng cách phân tích động các tệp và URL. Nếu một tệp hoặc URL không rõ, Sophos Sandstorm sẽ thử nghiệm chúng trong môi trường cô lập an toàn để đảm bảo không có mối đe dọa nào được truyền vào hệ thống.
- **Protection Against Ransomware:** Sophos Firewall có khả năng bảo vệ chống lại ransomware, một loại phần mềm độc hại chặn truy cập vào hệ thống và yêu cầu một khoản tiền chuộc.
- **Live Protection:** Tính năng Live Protection giúp Sophos Firewall tự động cập nhật các chữ ký virus và đặc điểm độc hại để đảm bảo rằng hệ thống luôn được bảo vệ chống lại các mối đe dọa mới và phổ biến.
- **Scheduled Scans:** Sophos Firewall hỗ trợ quét antivirus theo lịch trình được đặt trước để đảm bảo rằng toàn bộ hệ thống đều được kiểm tra định kỳ.
- **Centralized Management:** Tính năng quản lý tập trung của Sophos Firewall cho phép người quản trị quản lý và theo dõi tình trạng bảo mật từ một giao diện duy nhất.
- **Quarantine and Cleanup:** Nếu phần mềm độc hại được phát hiện, Sophos Firewall có khả năng di chuyển nó vào khu karantin và cung cấp các công cụ để làm sạch hệ thống.

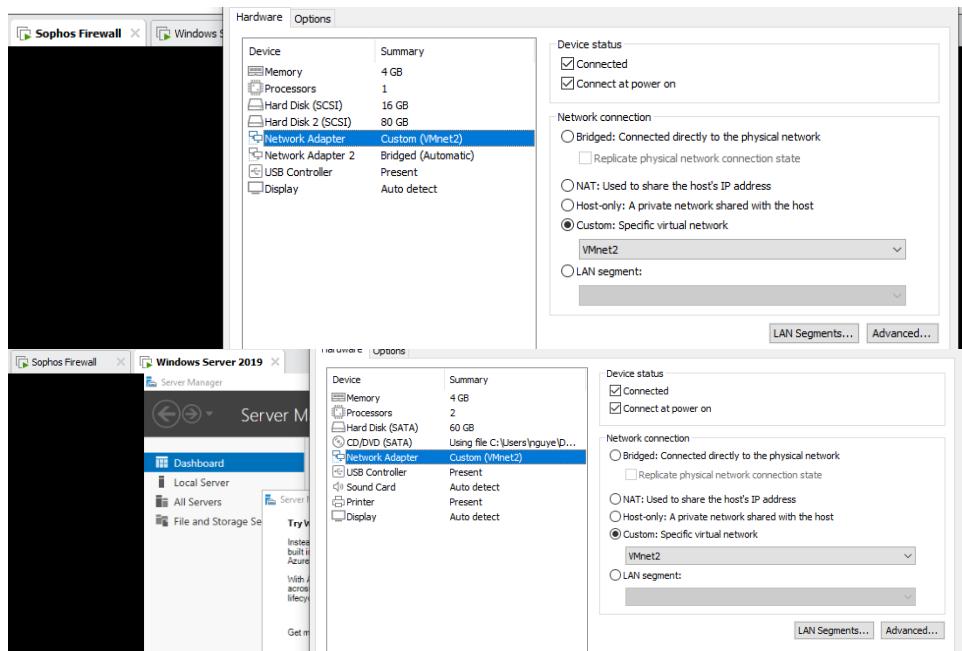
### 2.5.2 Cấu hình

- Đầu tiên ta chuẩn bị 1 máy Window Server 2019 và 1 Sophos Firewall

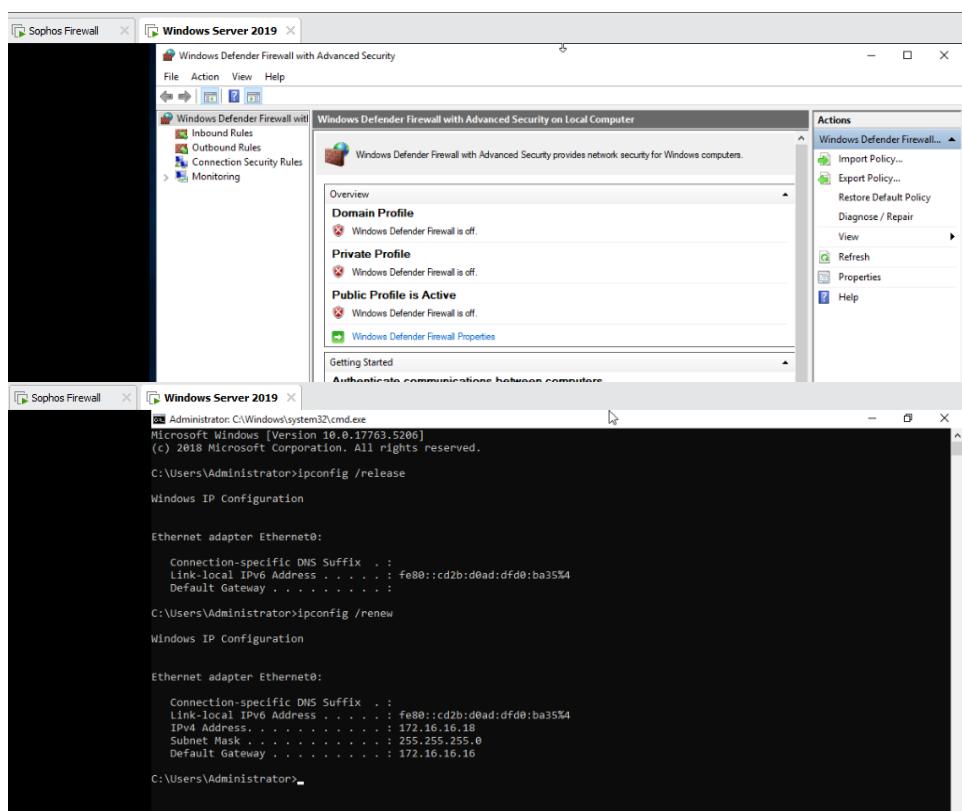


## Đồ án Quản trị hệ thống Windows 2

- Sau đó chỉnh card mạng của Server chung với Firewall

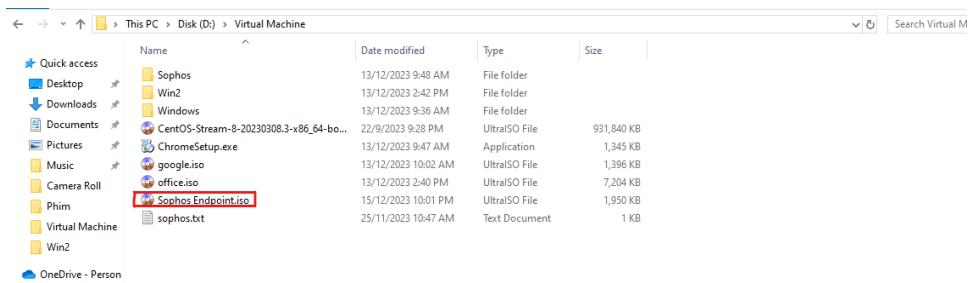


- Tắt tường lửa và chạy IP động cho máy Server

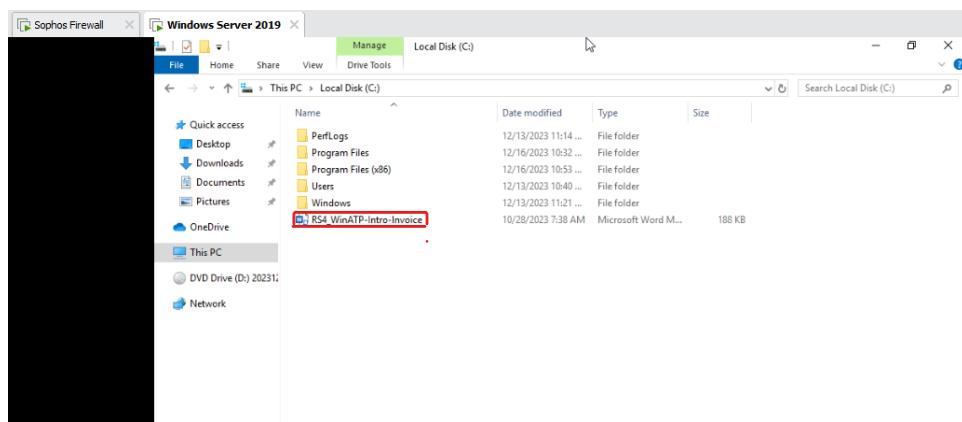


- Ta chạy Sophos Endpoint Agent cho Server

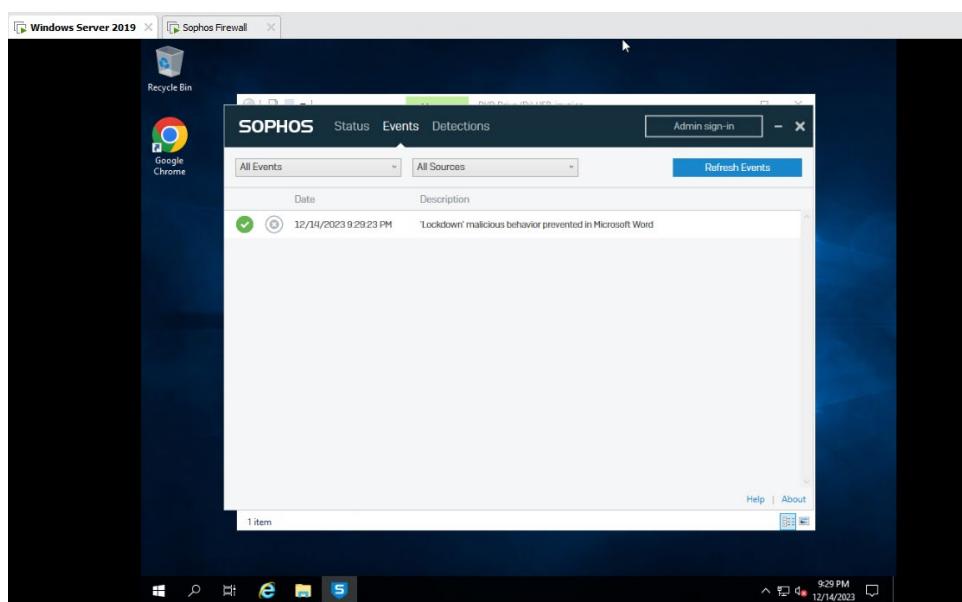
## Đồ án Quản trị hệ thống Windows 2



- Tiếp đó ta chuẩn bị 1 malware (phần mềm độc hại) dưới dạng file word



- Khi ta mở malware đó firewall sẽ chặn việc chạy mã độc



## 2.6 Server Protection

### 2.6.1 Khái niệm

Server Protection trên Sophos Firewall là một tính năng cung cấp bảo vệ an ninh cho các máy chủ trong mạng của bạn. Nó cung cấp các công cụ và chức năng để ngăn chặn các mối đe dọa mạng, bao gồm vi rút, malware, tấn công từ mạng, tấn công từ phía người dùng và các mối đe dọa khác có thể nhắm vào các máy chủ trong hệ thống.

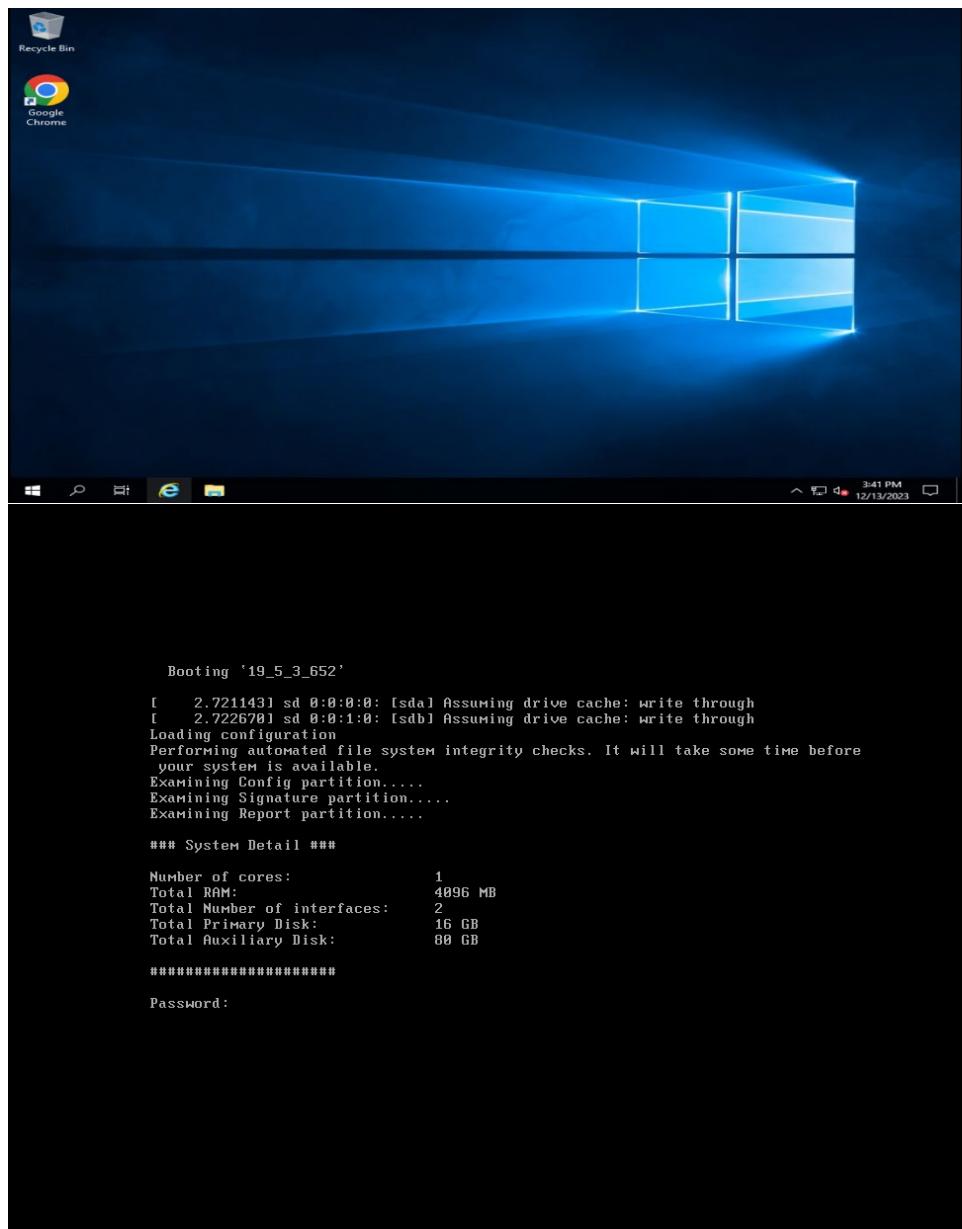
Các tính năng bảo vệ server có thể bao gồm:

- **Firewall Protection:** Sophos Firewall cung cấp bức tường lửa mạnh mẽ để ngăn chặn các tấn công từ bên ngoài và kiểm soát luồng dữ liệu đến và đi từ các máy chủ.
- **Intrusion Prevention System (IPS):** Tính năng này phát hiện và ngăn chặn các loại tấn công nhất định bằng cách kiểm tra các gói tin mạng và hành vi kỹ thuật tấn công thông qua quy tắc đã được cấu hình.
- **Application Control:** Sophos Firewall cho phép quản trị viên xác định và kiểm soát các ứng dụng được chạy trên máy chủ, ngăn chặn việc sử dụng các ứng dụng không an toàn hoặc không được phép.
- **Web Filtering:** Cung cấp khả năng kiểm soát nội dung web để ngăn chặn máy chủ truy cập vào các trang web độc hại hoặc không an toàn.
- **Anti-Malware Protection:** Sophos Firewall có thể được cấu hình để quét và ngăn chặn vi rút, phần mềm độc hại và tác nhân gây hại khác trước khi chúng có thể tấn công các máy chủ.
- **VPN (Virtual Private Network):** Cho phép kết nối an toàn từ xa đến máy chủ thông qua mạng riêng ảo, tăng cường tính bảo mật khi truy cập từ xa.

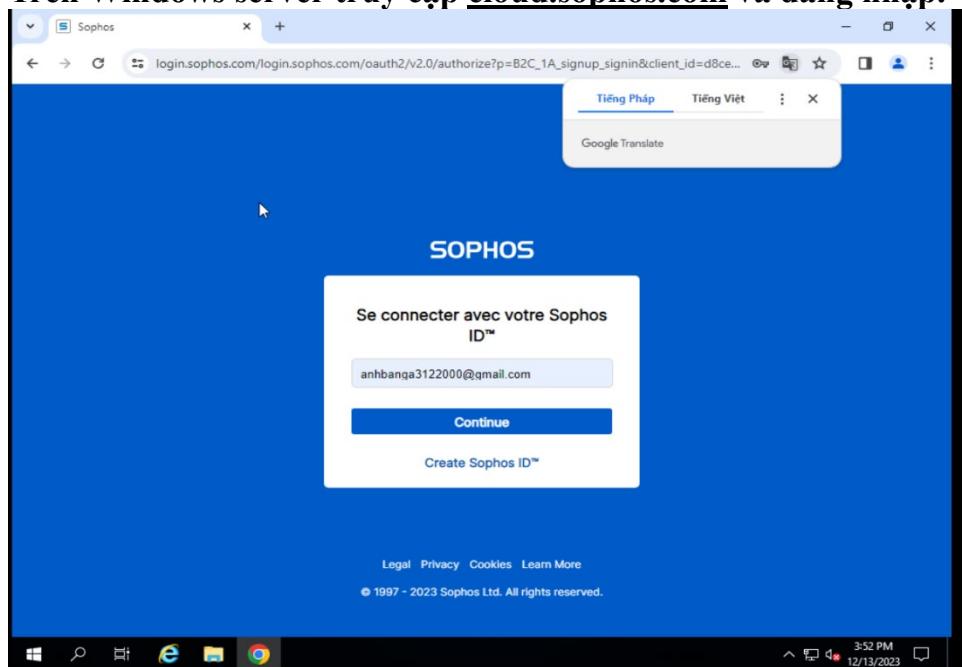
### 2.6.2 Cấu hình

#### Chuẩn bị 1 máy Windows server 2019 và Sophos Firewall

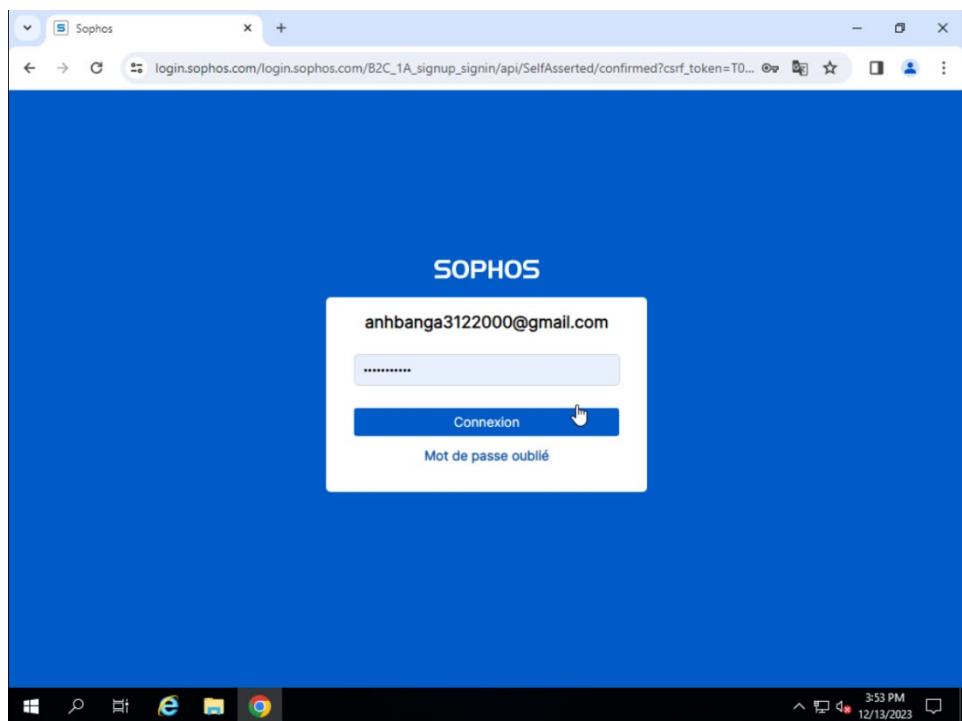
## Đồ án Quản trị hệ thống Windows 2



Trên Windows server truy cập [cloud.sophos.com](https://cloud.sophos.com) và đăng nhập.



## Đồ án Quản trị hệ thống Windows 2



**Chọn My Products → Server → Installers**

SOPHOS Dashboards My Products Threat Analysis Center More

Sophos Central Dashboard See a snapshot of your security protection

5 Total Alerts

Most Recent Alerts

- Dec 13, 2023 11:... A fire...
- Dec 13, 2023 11:... Firewall...
- Dec 13, 2023 11:... A fire...
- Dec 13, 2023 9:5... A fire...
- Dec 11, 2023 7:5... A new firewall has been successfully register...

ENDPOINT PROTECTION

- Endpoint
- Mobile
- Encryption

CLOUD NATIVE SECURITY

- Server
- Cloud Native Security

NETWORK

- Wireless
- Firewall Management
- ZTNA
- Switches

MESSAGING

- Email Protection
- Phish Threat

SERVER

- Dashboard
- Reports
- Servers
- Policies
- Settings
- Installers

1 Low Alerts

View all Alerts

Show full d...

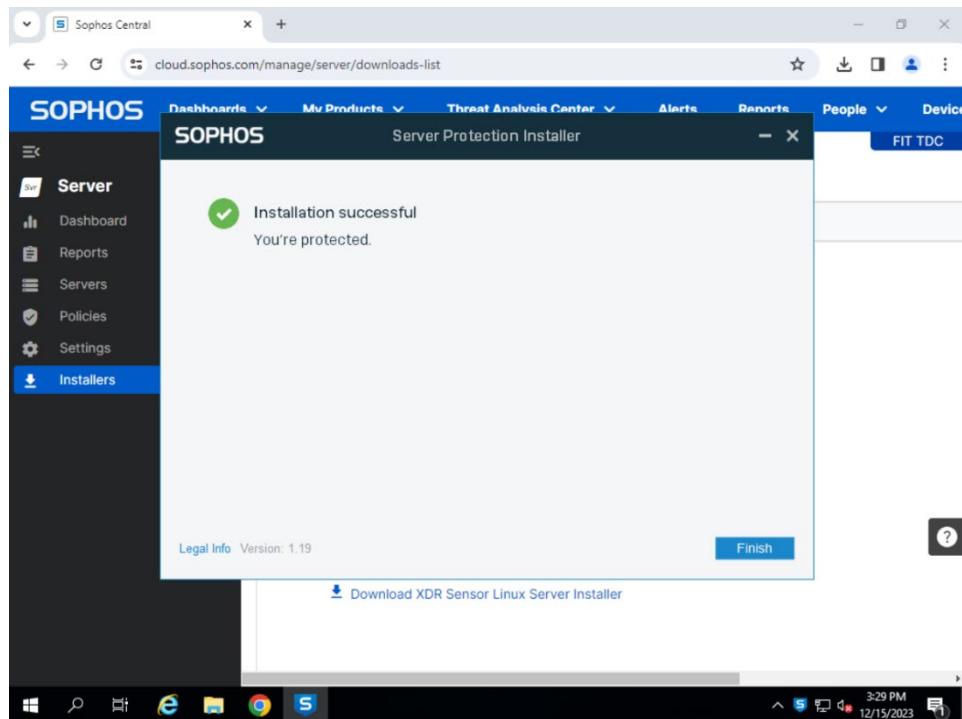
**Tiếp theo các bạn bấm Download Windows Server Installer và Install**

## Đồ án Quản trị hệ thống Windows 2

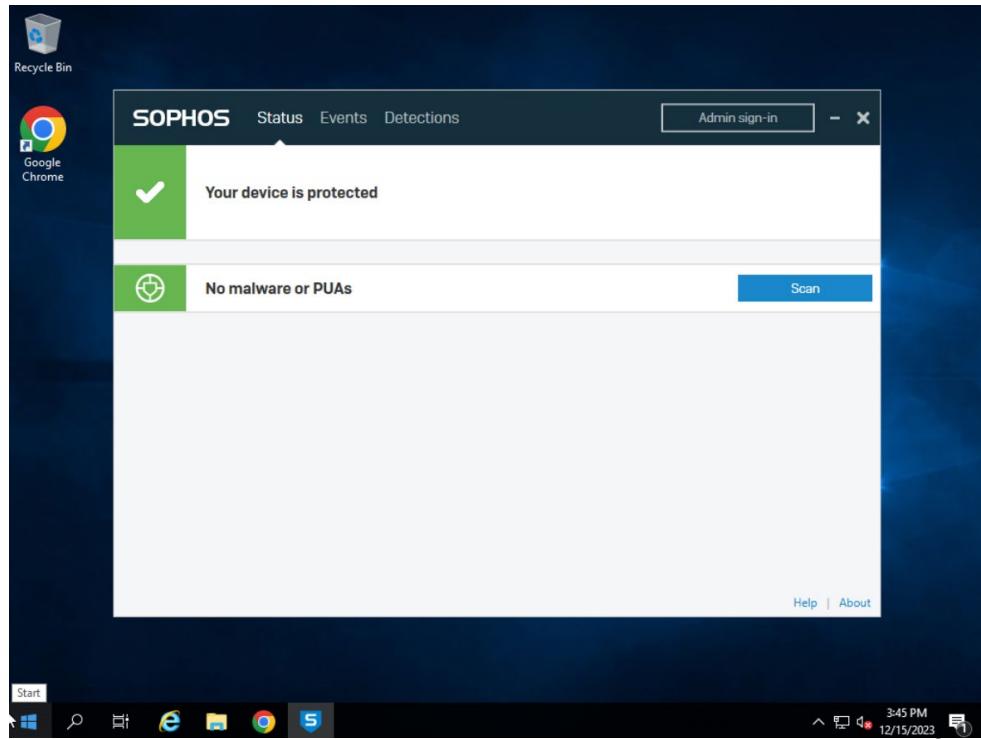
The screenshot displays two windows from the Sophos Central interface. The top window shows the 'Server Protection - Installers' page, which includes sections for 'Server Protection' (with options to download Windows or Linux Server installers) and 'XDR Sensor Installers' (with a note about no Sophos malware protection and options to download XDR Sensor Windows or Linux Server installers). The bottom window shows the 'Server Protection Installer' dialog box, which informs the user they are about to install Intercept X Advanced for Server with XDR, noting it will take about 10 minutes and cannot be cancelled. It also includes a note about removing third-party security software. At the bottom of this dialog is a 'Download XDR Sensor Linux Server Installer' link.

## Đồ án Quản trị hệ thống Windows 2

### Server Protection đã cài đặt xong



Đây là giao diện của ứng dụng



Tiếp theo thì chúng ta sẽ trở lại trang web [cloud.sophos.com](http://cloud.sophos.com) để kiểm tra xem server của mình đã được bảo vệ chưa

## Đồ án Quản trị hệ thống Windows 2

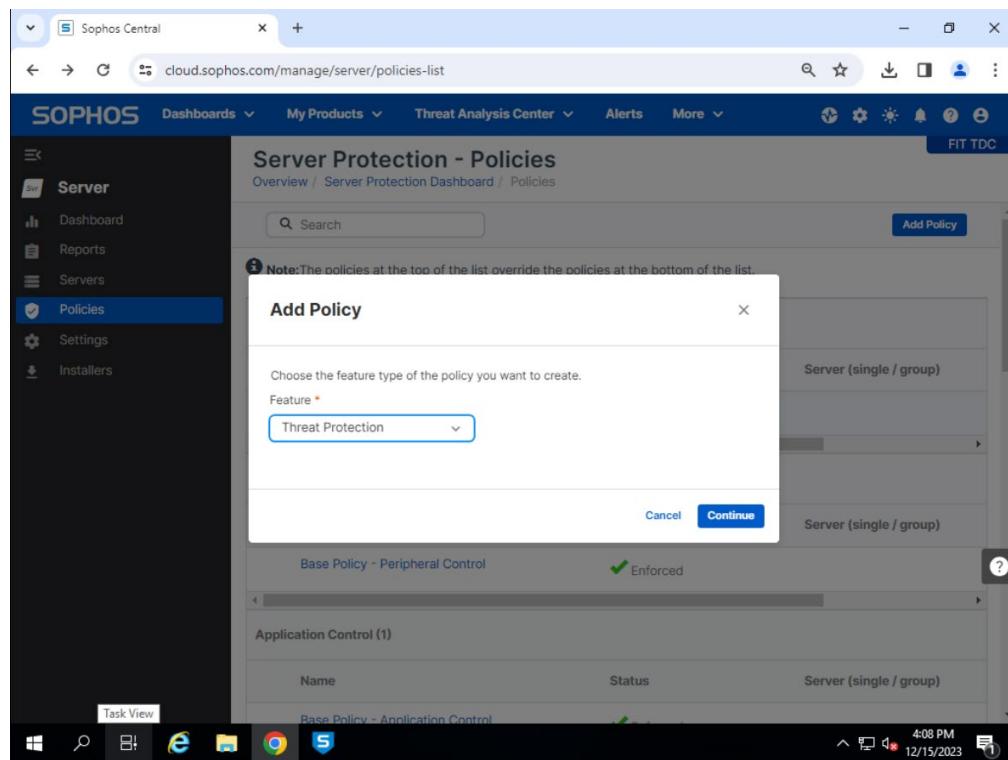
A screenshot of the Sophos Central web interface. The top navigation bar includes links for Dashboards, My Products, Threat Analysis Center, Alerts, Reports, People, and Device. A blue banner at the top right says "FIT TDC". The main content area is titled "Server Protection - Servers" and shows an overview of servers. A sidebar on the left has icons for Srv, Dashboards, Reports, Servers, Policies (which is selected), Settings, and Installers. The central table lists one server: "WIN-DDEMELAE8F50" with IP "172.16.16.17", OS "Windows Server 2019 Standard", and protection status "Intercept X Advanced with XDR". There are buttons for "Manage Endpoint Software", "Add Server", "Turn on tamper protection", "Reset health status", and "Delete". Below the table are filters for "Show all servers", "All Health Status", "Any protection types", and "Recently online". The bottom of the screen shows a taskbar with various icons and the date/time "12/15/2023 3:50 PM".

Kế tiếp ta sẽ cấu hình Policy cho Server Protection.  
Chọn Policies → Add Policy

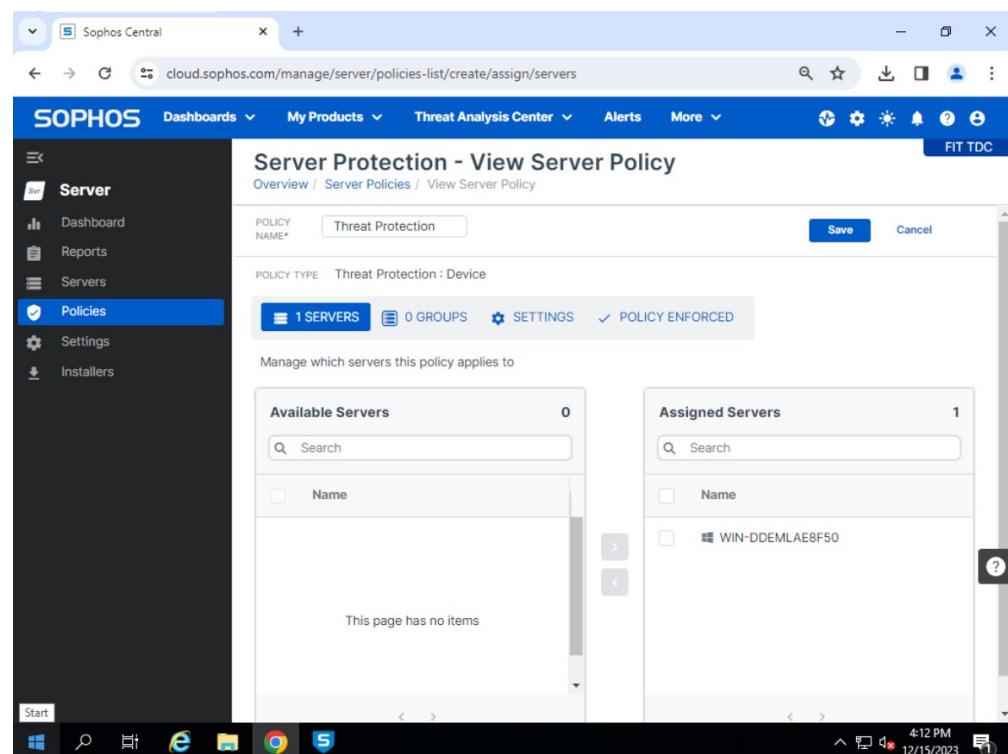
A screenshot of the Sophos Central web interface. The top navigation bar includes links for Dashboards, My Products, Threat Analysis Center, Alerts, More, and FIT TDC. The main content area is titled "Server Protection - Policies" and shows an overview of policies. A sidebar on the left has icons for Srv, Dashboard, Reports, Servers, Policies (selected), Settings, and Installers. A note at the top of the policy list says: "Note: The policies at the top of the list override the policies at the bottom of the list." An "Add Policy" dialog box is open in the center, asking to "Choose the feature type of the policy you want to create." A dropdown menu labeled "Select an option" is shown. Below the dialog, a list of policies is visible, including "Base Policy - Peripheral Control" (status: Enforced) and "Application Control (1)". The bottom of the screen shows a taskbar with various icons and the date/time "12/15/2023 4:04 PM".

Chọn Select an option → Threat Protection → Continue

## Đồ án Quản trị hệ thống Windows 2



Ở đây ta sẽ đặt tên cho Policy và áp dụng với máy Server hiện tại mình đang cấu hình



Ấn vào setting và bật tất cả lên

## Đồ án Quản trị hệ thống Windows 2

The image displays two screenshots of the Sophos Central web interface, both titled "Server Protection - View Server Policy".

**Screenshot 1: Threat Protection Settings**

This screen shows the "Threat Protection" tab selected under "SETTINGS". It indicates "1 SERVERS" and "0 GROUPS" are assigned. A green message box states: "Your policy settings give you the protection we recommend." Below this, the "Live Protection" section is shown, with the "Use Live Protection to check files against the latest malware information from SophosLabs online" toggle switch turned on. Other options include "Use Live Protection during scheduled scans" (checked) and "Enable deep learning" (unchecked). The "Real-time scanning - Local files and network shares" section also has its toggle switch turned on. The "Applies To" column shows green checkmarks for Windows and macOS.

**Screenshot 2: Runtime Protection Settings**

This screen shows the "Runtime Protection" tab selected under "SETTINGS". It lists several protection features: "Protect document files from ransomware (CryptoGuard)" (checked), "Protect from remotely run ransomware" (checked), "Protect from Encrypting File System attacks" (checked), "Mitigate exploits in vulnerable applications" (checked), "Protect processes" (checked), and "Prevent process hollowing attacks" (checked). The "ACTION TO TAKE ON RANSOMWARE DETECTION" dropdown is set to "Terminate Process". A note says: "This setting only applies to servers you add to the New Server Protection Features EAP. Join the EAP now". The "Applies To" column shows green checkmarks for Windows and macOS.

**Sau khi bật xong thì ấn Save để Policy có hiệu lực.  
Và các Policy tiếp theo các bạn cũng thực hiện tương tự như trên**

## Đồ án Quản trị hệ thống Windows 2

Sophos Central - cloud.sophos.com/manage/server/policies-list

**Policies**

Peripheral Control (1)

Name	Status	Server (single / group)	Last modified
Base Policy - Peripheral Control	Enforced		Dec 11, 2023

Application Control (1)

Name	Status	Server (single / group)	Last modified
Base Policy - Application Control	Enforced		Dec 11, 2023

Web Control (1)

Name	Status	Server (single / group)	Last modified
Base Policy - Web Control	Enforced		Dec 15, 2023

Lockdown (1)

Name	Status	Server (single / group)	Last modified
Base Policy - Lockdown	Enforced		Dec 11, 2023

Tiếp theo mình sẽ test bằng cách tải 1 file có chứa virus xem thử con Sophos có cảnh báo gì không.

Sophos Central - Download Anti Malware Testfile

eicar.org/download-anti-malware-testfile/

using the secure, SSL enabled protocol HTTPS

Com-file  
68 Bytes

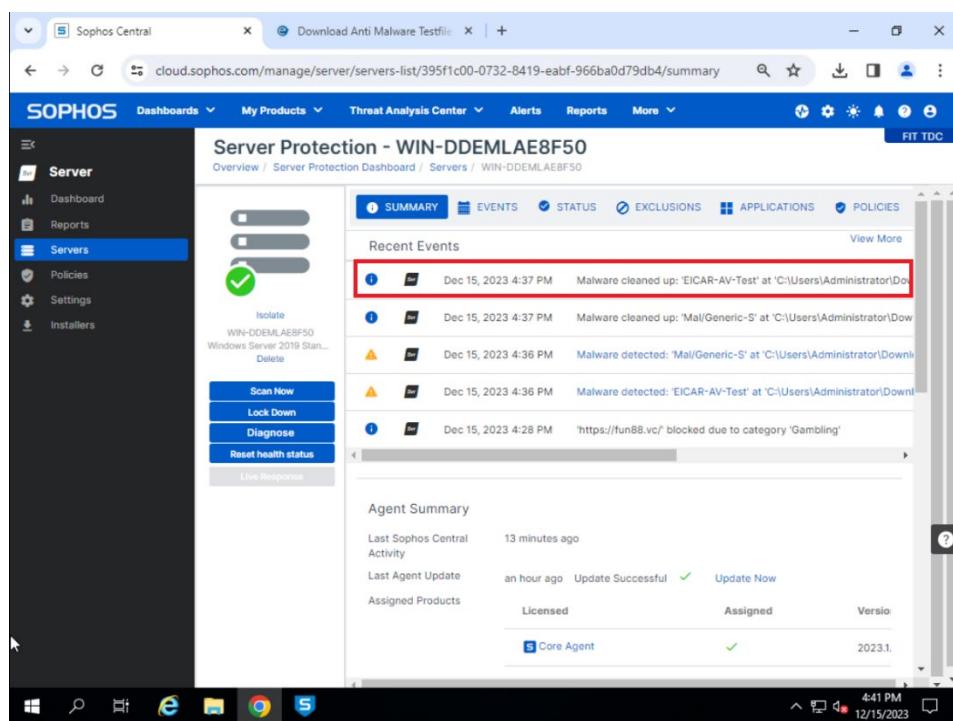
Text-file  
68 Bytes

Zip-file  
184 Bytes

Zip-file  
308 Bytes

Ở đây thì con Sophos đã cảnh báo cho mình là không được download file do chứa virus.

## Đồ án Quản trị hệ thống Windows 2



## 2.7 Sao lưu và phục hồi Sophos

### 2.7.1 Khái niệm

Việc sao lưu và phục hồi trên Sophos Firewall giúp đảm bảo an toàn cho cấu hình và dữ liệu quan trọng của hệ thống mạng, giúp người quản trị có khả năng khôi phục lại trạng thái hoạt động trước đây nhanh chóng khi có xảy ra sự cố.

**Sao lưu (Backup):** Điều này hữu ích khi bạn muốn đảm bảo rằng nếu có sự cố nào đó xảy ra, bạn có thể khôi phục lại hệ thống của mình từ bản sao lưu và tránh mất mát dữ liệu quan trọng.

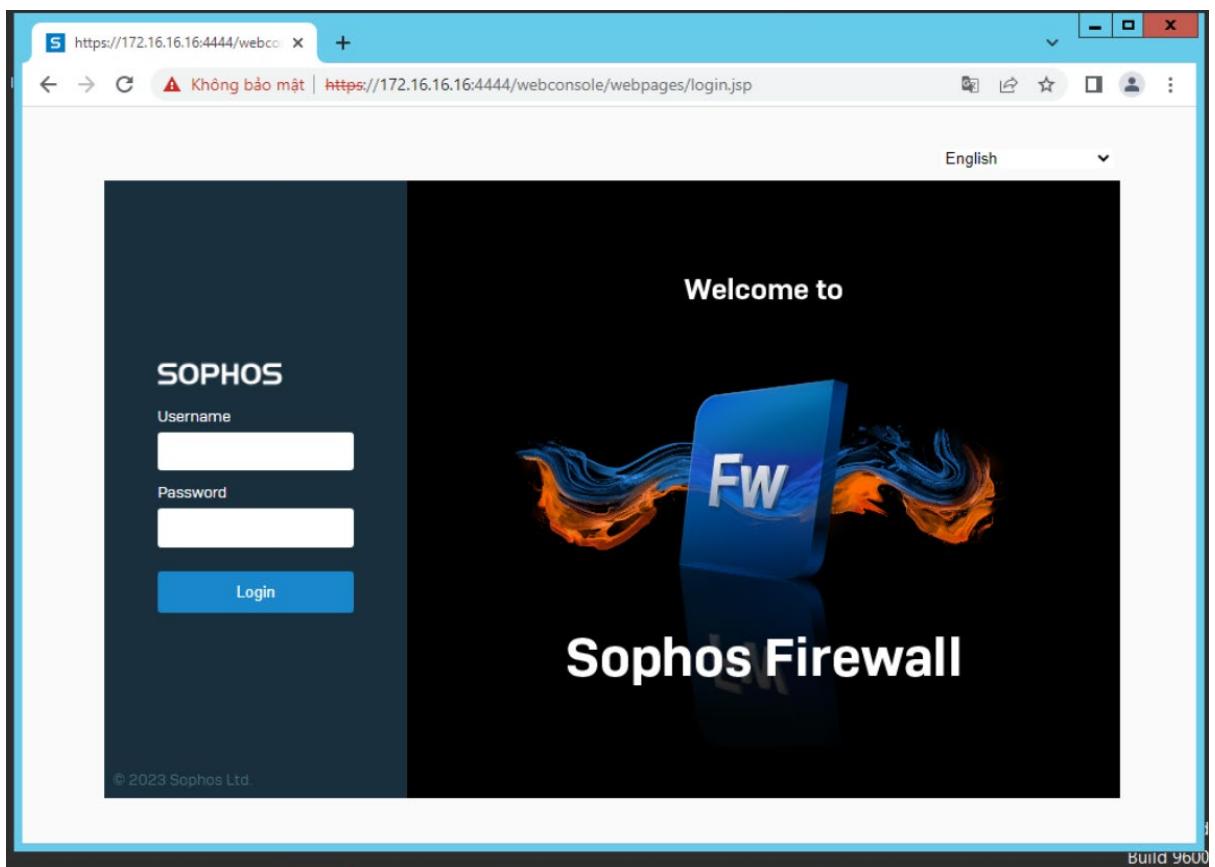
**Phục hồi (Restore):** Quá trình phục hồi thường được sử dụng khi cần khôi phục lại hệ thống từ một trạng thái trước đó đã được sao lưu.

Khi có sự cố như mất dữ liệu, sự cố về tường lửa, hoặc cần di chuyển hệ thống đến một máy chủ mới, quá trình phục hồi từ bản sao lưu là cần thiết.

### 2.7.2 Cấu hình

**Bước 1:** Ta cần chuẩn bị máy windows sever 2019 và sophos firewall

## Đồ án Quản trị hệ thống Windows 2



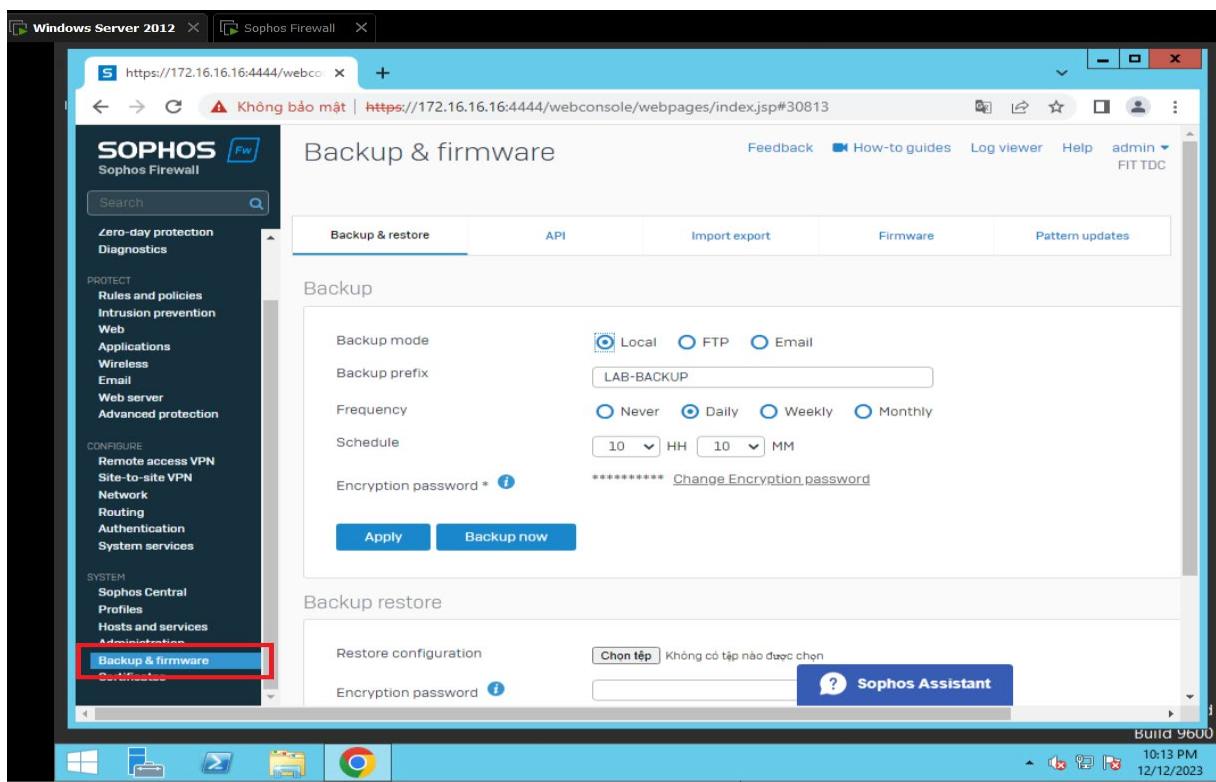
```
Sophos Firewall

Booting '19_5_3_652'

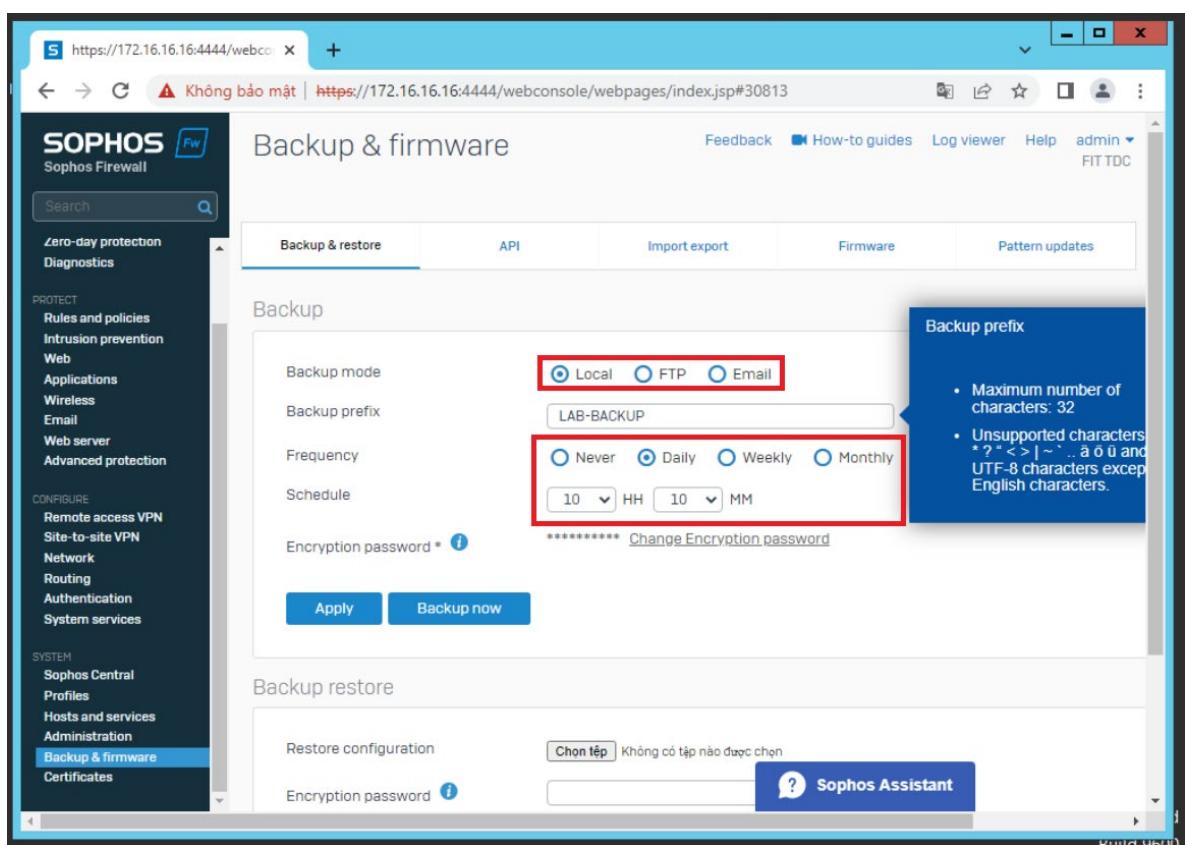
[    2.568927] sd 0:0:0:0: [sda] Assuming drive cache: write through
[    2.570184] sd 0:0:1:0: [sdb] Assuming drive cache: write through
Loading configuration
Performing automated file system integrity checks. It will take some time before your system is available.
Examining Config partition.....
Examining Signature partition.....
Examining Report partition.....
### System Detail ####
Number of cores: 1
Total RAM: 4096 MB
Total Number of interfaces: 2
Total Primary Disk: 16 GB
Total Auxiliary Disk: 80 GB
#####
Password: _
```

Bước 2: Đăng nhập vào firewall sophos và đi đến phần **Backup & firmware**

## Đồ án Quản trị hệ thống Windows 2

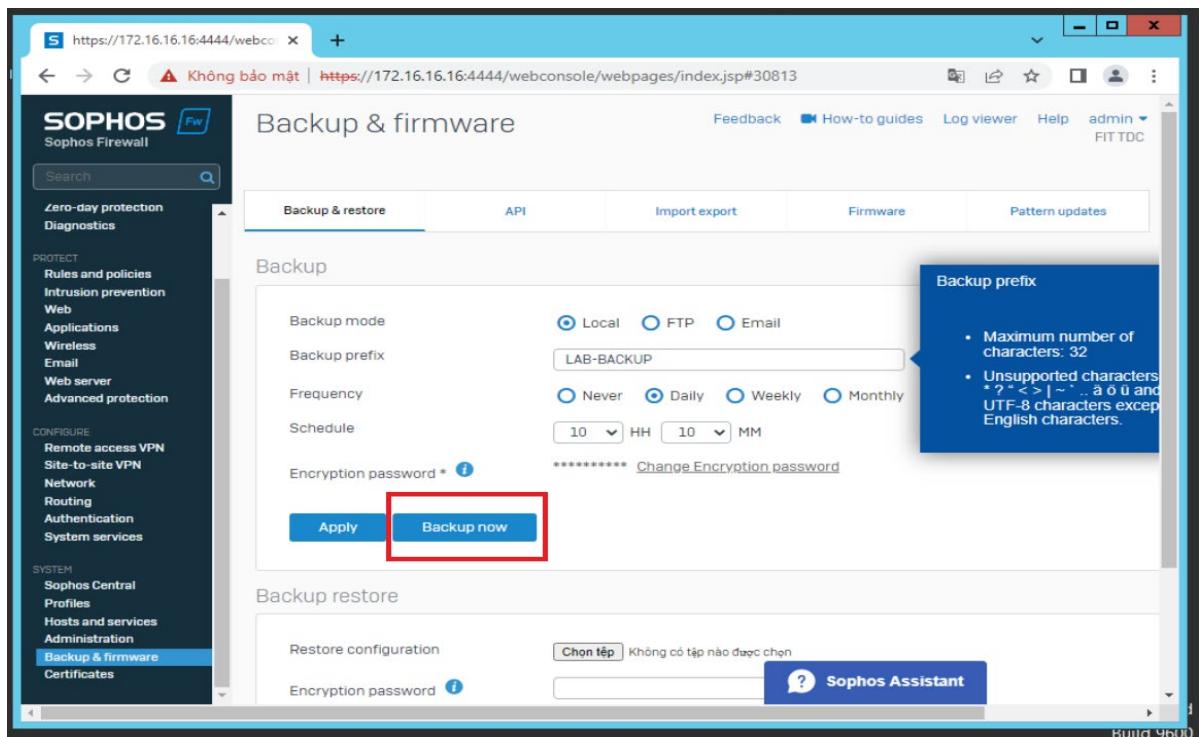


Bước 3: Đặt tên file backup và tùy chọn kiểu , thời gian backup



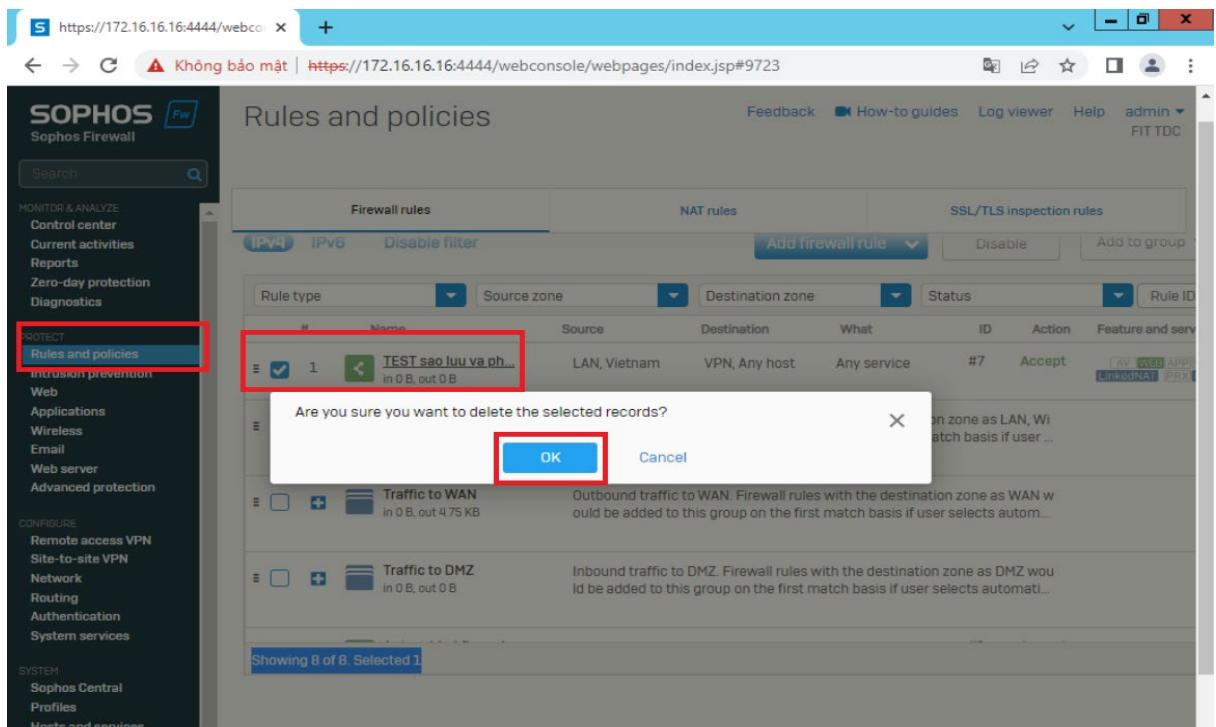
Bước 4: Sau khi tùy chỉnh backup ta sẽ nhấn vào **Backup now** là đã xong bước  
Backup

## Đồ án Quản trị hệ thống Windows 2



Bước 5: Ta sẽ xóa một policy đã được backup trước đó để test restore (phục hồi)

)



Sau khi xóa policy “test”

## Đồ án Quản trị hệ thống Windows 2

SOPHOS FW  
Sophos Firewall

Rules and policies

Feedback How-to guides Log viewer Help admin FIT TDC

MONITOR & ANALYZE  
Control center Current activities Reports Zero-day protection Diagnostics

PROTECT  
Rules and policies Intrusion prevention Web Applications Wireless Email Web server Advanced protection

REMOTE ACCESS  
Remote access VPN Site-to-site VPN Network Routing Authentication System services

SYSTEM  
Sophos Central Profiles Hosts and services Administration Backup & firmware

Firewall rules NAT rules SSL/TLS inspection rules

IPv4 IPv6 Disable filter Add firewall rule Disable

Rule type	Name	Source	Destination	What	ID	Action	Feature and serv
#	Traffic to Internal...	To LAN, WiFi, VPN, DMZ.	in 0 B, out 0 B	Firewall rules with the destination zone as LAN, WiFi, VPN, DMZ. Firewall rules with the destination zone as LAN, WiFi, VPN, DMZ would be added to this group on the first match basis if user ...			
#	Traffic to WAN	Outbound traffic to WAN.	in 0 B, out 4.75 KB	Outbound traffic to WAN. Firewall rules with the destination zone as WAN woul...			
#	Traffic to DMZ	Inbound traffic to DMZ.	in 0 B, out 0 B	Firewall rules with the destination zone as DMZ woul...			
#	Auto added firewall...	Any zone, Any host	Any zone, Any host	SMTP, SMTP(S)	#1	Accept	AV WEB APPS LinkedNAT PRX
#	#Default_Network_P...	LAN, Any host	WAN, Any host	Any service	#5	Accept	AV WEB APPS LinkedNAT PRX

Showing 7 of 7. Selected 0

Sophos Assistant

11:28 PM  
12/12/2023

Bước 6: Đi đến mục backup & firmware kéo xuống phần Backup restore chọn open file

SOPHOS FW  
Sophos Firewall

Feedback How-to guides Log viewer Help admin

MONITOR & ANALYZE  
Control center Current activities Reports Zero-day protection Diagnostics

PROTECT  
Rules and policies Intrusion prevention Web Applications Wireless Email Web server Advanced protection

REMOTE ACCESS  
Remote access VPN Site-to-site VPN Network Routing Authentication System services

SYSTEM  
Sophos Central Profiles Hosts and services Administration **Backup & firmware**

Backup & firmware

Feedback How-to guides Log viewer Help admin

Backup & restore API Import export Firmware Pattern updates

LAB-BACKUP

Frequency: Daily

Schedule: 10 HH 10 MM

Encryption password: \*\*\*\*\* [Change Encryption password](#)

Apply Backup now Last backup taken on Wed 13 Dec 2023 22:35:48 Download

**Backup restore**

Restore configuration: Chọn tệp Không có tệp nào được chọn

Encryption password: [Change](#)

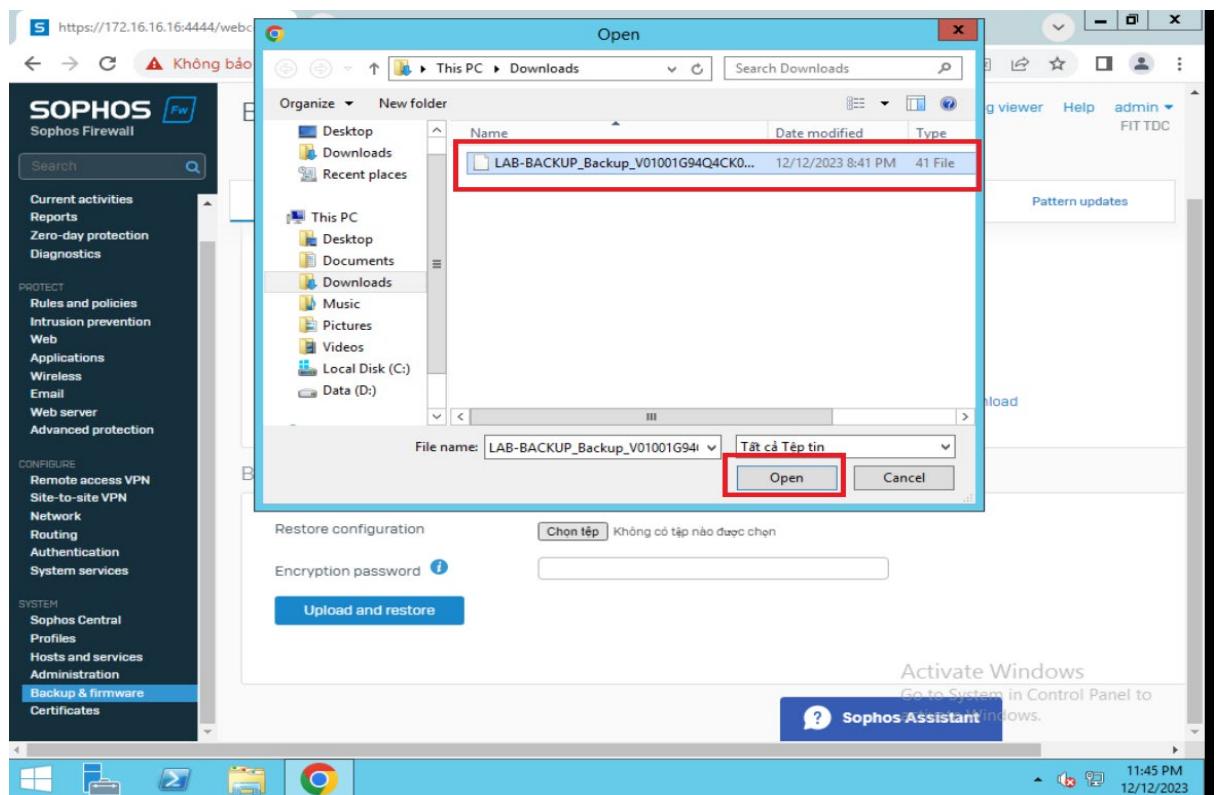
Upload and restore

Sophos Assistant

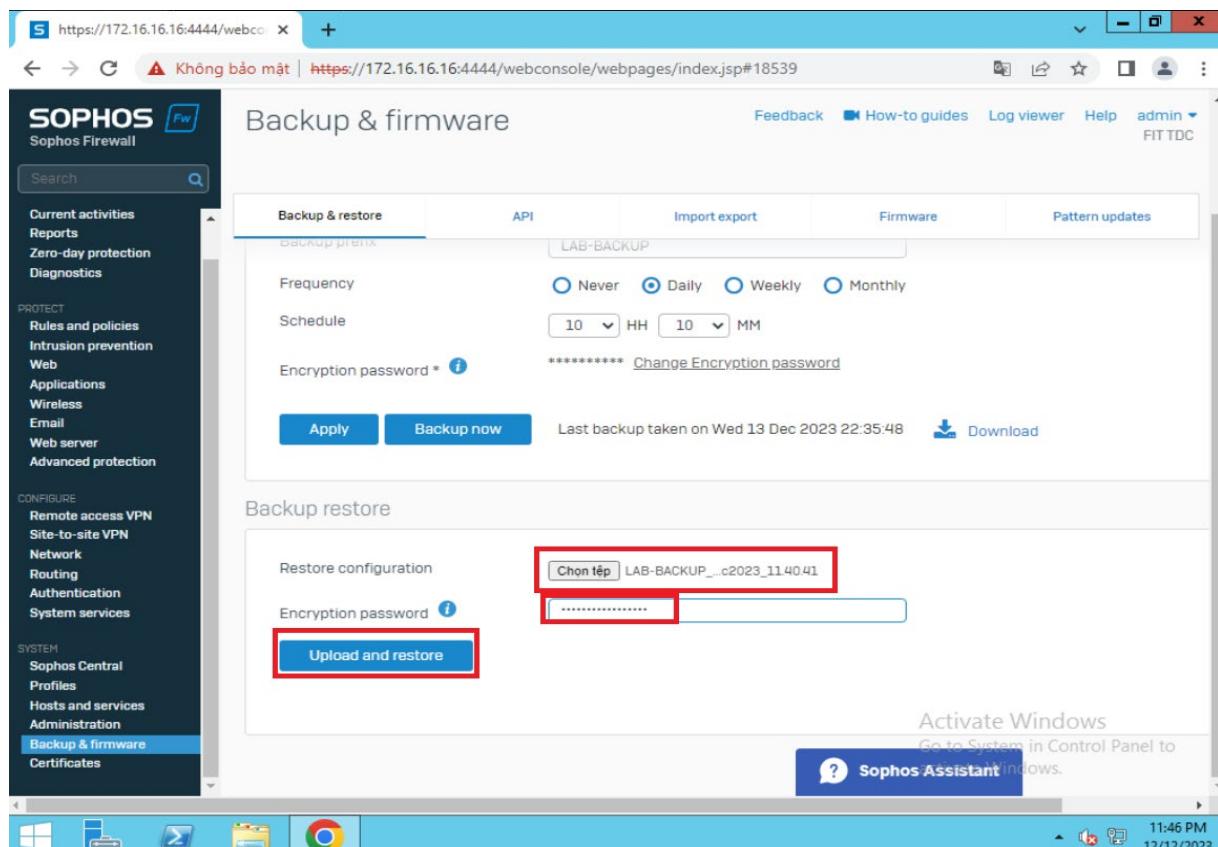
12/12/2023

Bước 7: Chọn file đã backup trước đó và open

## Đồ án Quản trị hệ thống Windows 2

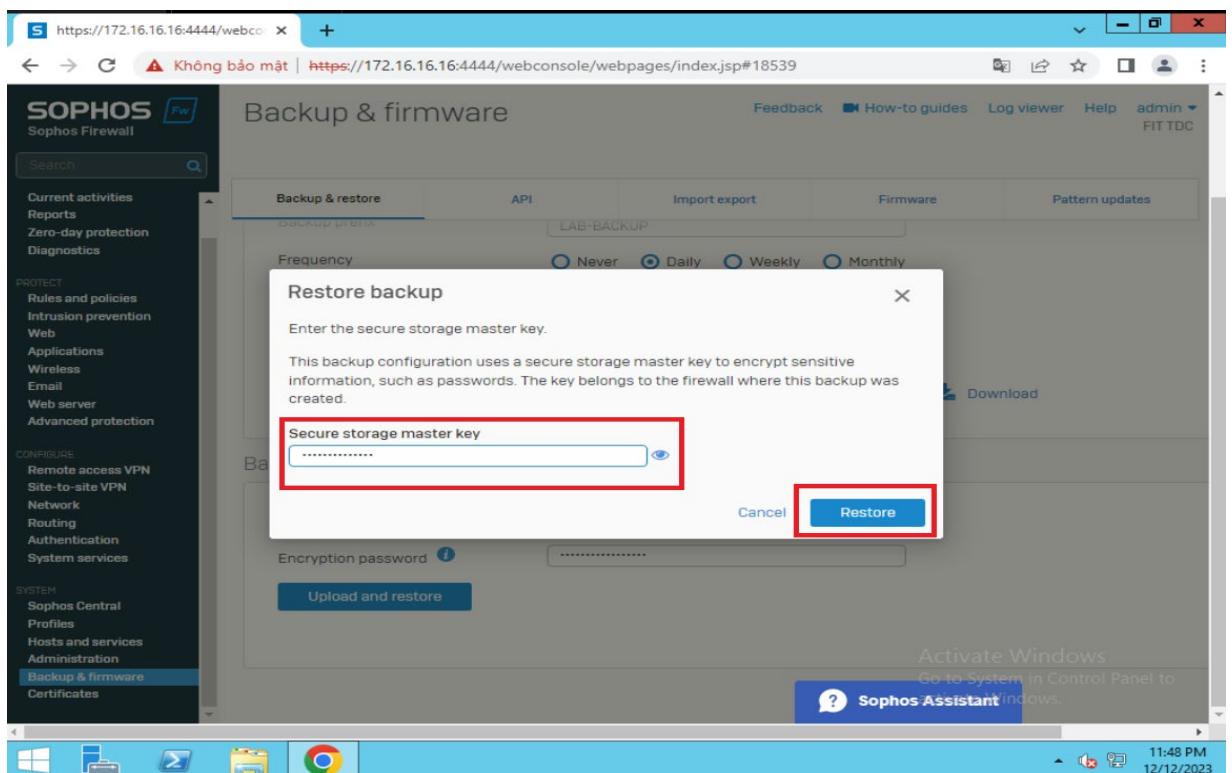


**Bước 8:** Sau khi chọn file backup ta tiến hành nhập **password encryption** (mật khẩu mã hóa) lúc tạo backup và nhấn **Upload and restore**

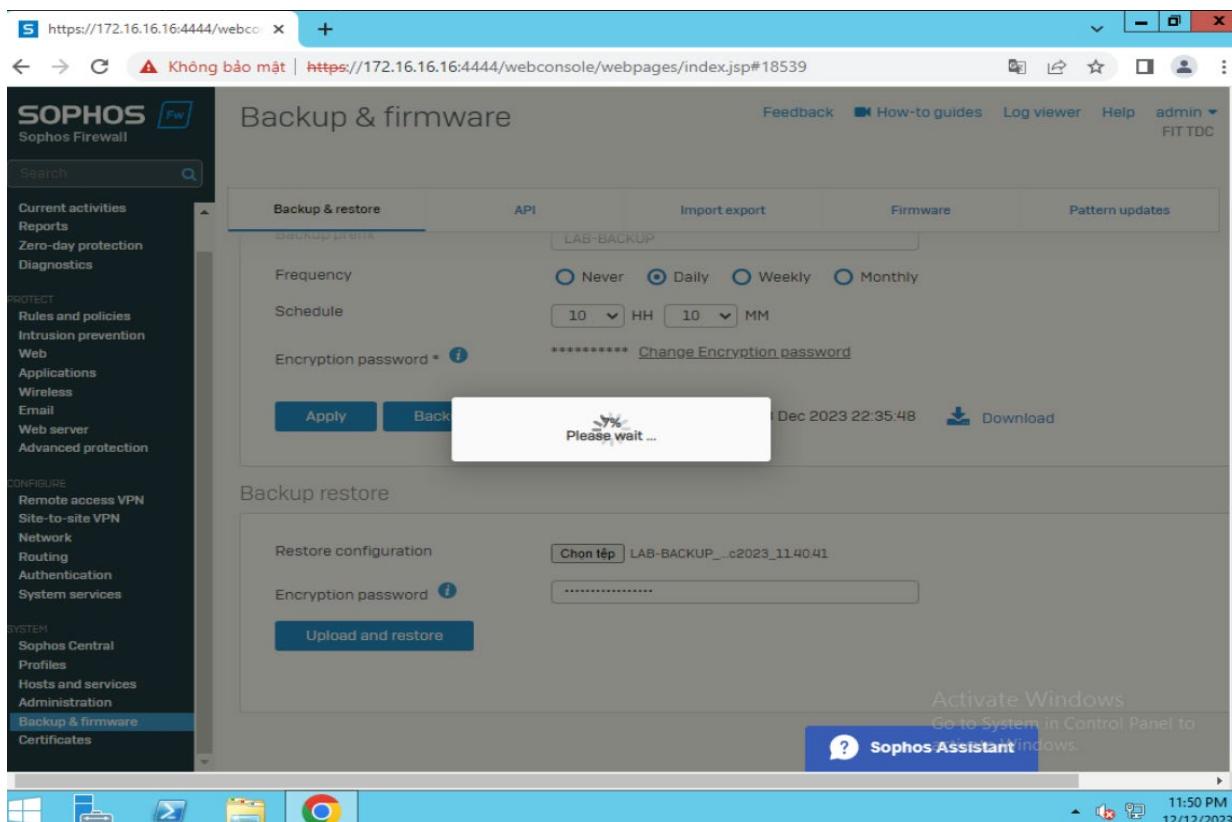


**Bước 9:** Nhập key recovery và tiến hành nhập vào restore (khôi phục) dữ liệu

## Đồ án Quản trị hệ thống Windows 2

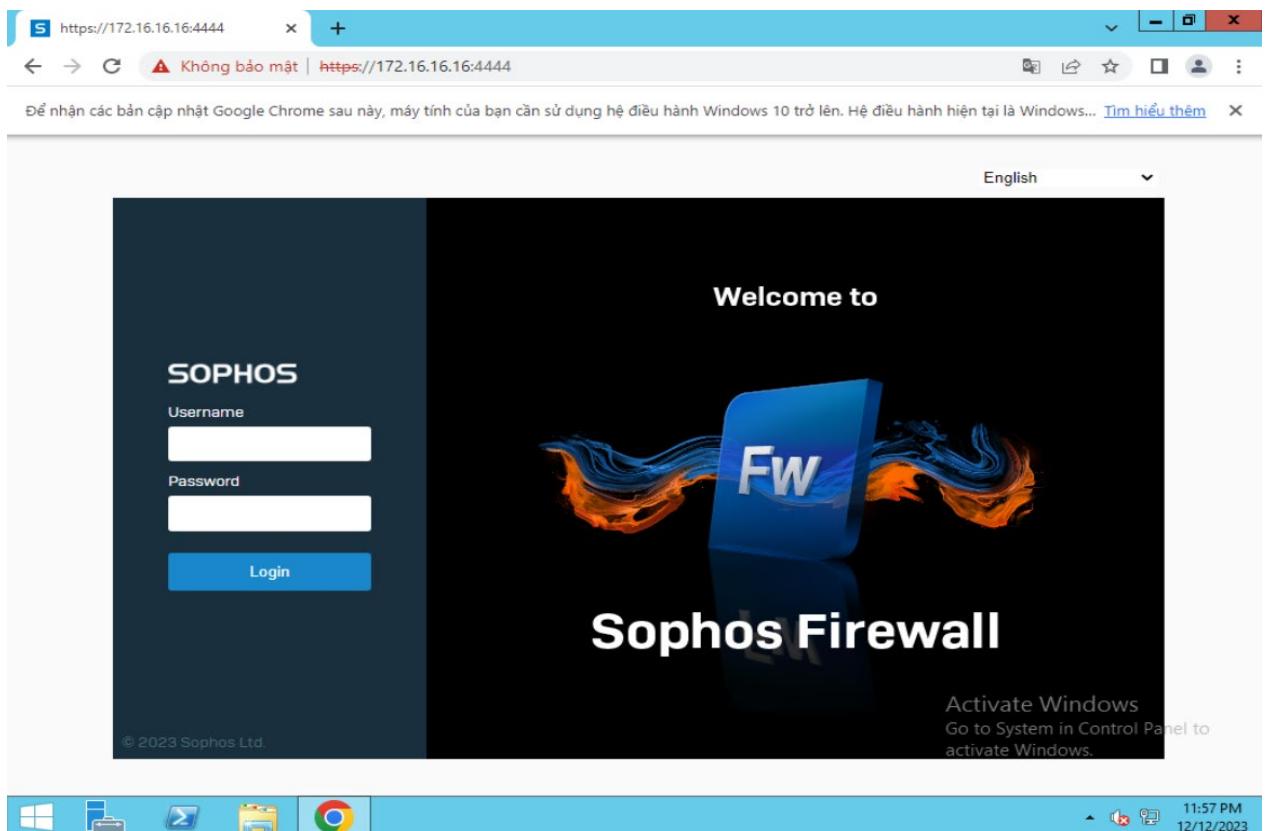


### Đang restore



**Bước 10:** Sau khi load restore (khôi phục) ta tiến hành đăng nhập lại hệ thống firewall sophos

## Đồ án Quản trị hệ thống Windows 2



Bước 11: Lúc này file test đã được khôi phục trở lại sau khi xóa đi

The screenshot shows the 'Rules and policies' section of the Sophos Firewall web console. The left sidebar has 'Rules and policies' selected. The main area displays a table of firewall rules. One rule, 'TEST sao lưu và ph...', is highlighted with a red box. The table columns include '#', 'Name', 'Source', 'Destination', 'What', 'ID', 'Action', and 'Feature and serv'. Other visible rules include 'Traffic to Internal...', 'Traffic to WAN', and 'Traffic to DMZ'. At the bottom, it says 'Showing 8 of 8. Selected 1'.

## CHƯƠNG 3: TỔNG KẾT

### 3.1 Thuận lợi và khó khăn

#### 3.1.1 Thuận lợi

Với nền tảng của môn an ninh mạng nên nhóm chúng em đã dễ dàng triển khai đồ án. Cùng với sự phân công công việc hợp lý và sự chỉ đạo của nhóm trưởng, nhóm chúng em đã vượt qua những khó khăn trong khi làm đồ án.Thêm vào đó, nền tảng của môn Anh Văn chuyên ngành do cô Nguyễn Ngọc Ánh Mỹ dạy đã giúp nhóm chúng em rất nhiều trong việc đọc và tìm hiểu tài liệu tiếng Anh của đồ án.

#### 3.1.2 Khó khăn

Điều kiện cấu hình của máy Server để chạy trong Firewall tối thiểu là Window Server 2019 và máy Client là Windows 10 - 64bit, vì thế việc triển khai mô hình của đồ án là hết sức khó khăn, cùng với những tính năng mới của Firewall.

### 3.2 Kết luận

#### ❖ Ưu điểm:

- Dễ sử dụng, các chính sách có sẵn vì thế những người mới sử dụng có thể thích nghi nhanh chóng.
- Giao diện thân thiện với người dùng, số liệu cập nhật và hiển thị cụ thể.
- Giá cả phải chăng đối với các doanh nghiệp vừa và lớn.

#### ❖ Nhược điểm:

- Cần chuyên môn về tiếng Anh chuyên ngành.
- Phải trả phí.

## **TÀI LIỆU THAM KHẢO**

- [1] [Getting started - Sophos Firewall](#)
- [2] [Rules and policies - Sophos Firewall](#)
- [3] [Network - Sophos Firewall](#)
- [4] [Malware protection - Sophos Firewall](#)
- [5] [Email - Sophos Firewall](#)