IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

College	Department	Course
College of Computer Science and Information Technology	Networks and Communications	CYS502: Network Security

Practical Session Plan

Session Topic/Title	Session No.	Session Duration (Minutes)
Part 1: XG Firewall configuration Part 2: IPsec configuration	No. 8	150

- Download XG Firewall
- Setup XG firewall
- Create an IPsec group and user rule
- Create an IP range rule for IPsec
- Configure the IPsec connection using pre-shared key
- Export the IPsec connection
- Connect the end user to the IPsec service
- Validate IPsec connection
- Capture and filter the traffic using Wireshark
- Identify ESP header

XG Firewall provides a complete portfolio of SD-WAN, cloud, and VPN secure access solutions that integrate distributed networks. Itis the only network security solution that can fully identify the source of an infection on your network and automatically limit access to other network resources in response.

A pre-shared key (PSK) or shared secret is a string of text a VPN (virtual private network) or other service expects to get before it receives any other credentials

1- Session Outcomes

1. Providing an authentication and confidentiality connection to end users through IPsec configuration connection

2- Tool(s)/Software

Tools:

- VMware Player or Workstation
- Wireshark

College	Department	Course
College of Computer Science and Information Technology	Networks and Communications	CYS502: Network Security

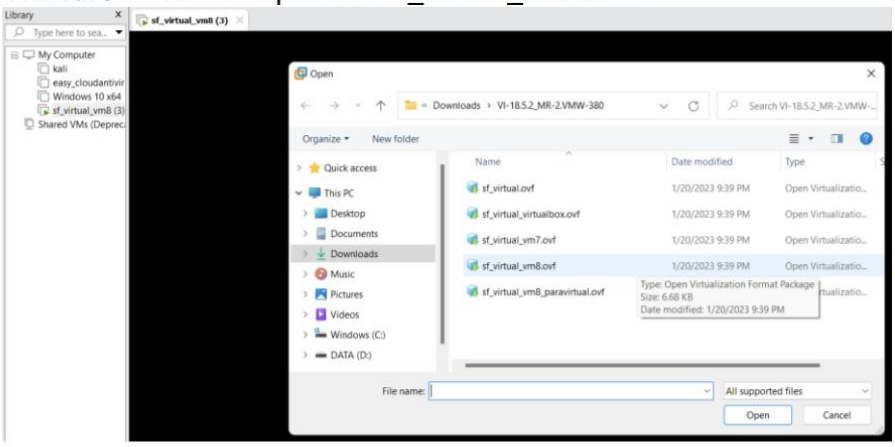
Practical Session Plan

3- Procedural Steps (Tasks)

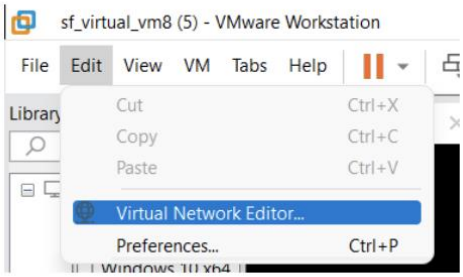
Part1: Downloading and configuring the XG firewall

- Click here to download

VMware >> File >> Open >> "sf_virtual_vm8.ovf"



Edit >> virtual Network Editor >> Change

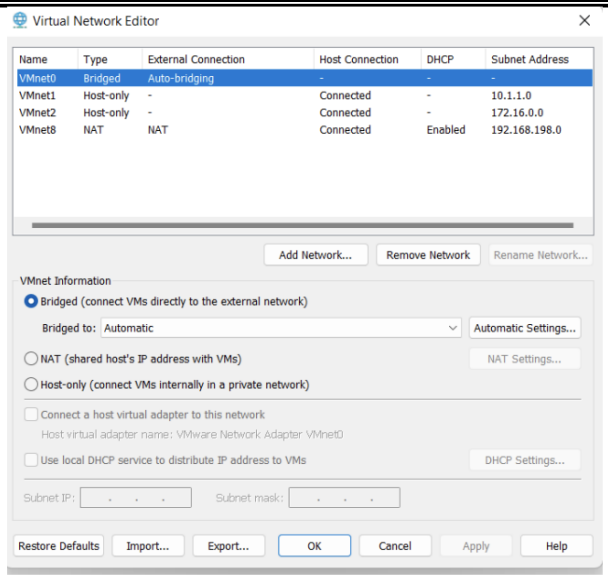


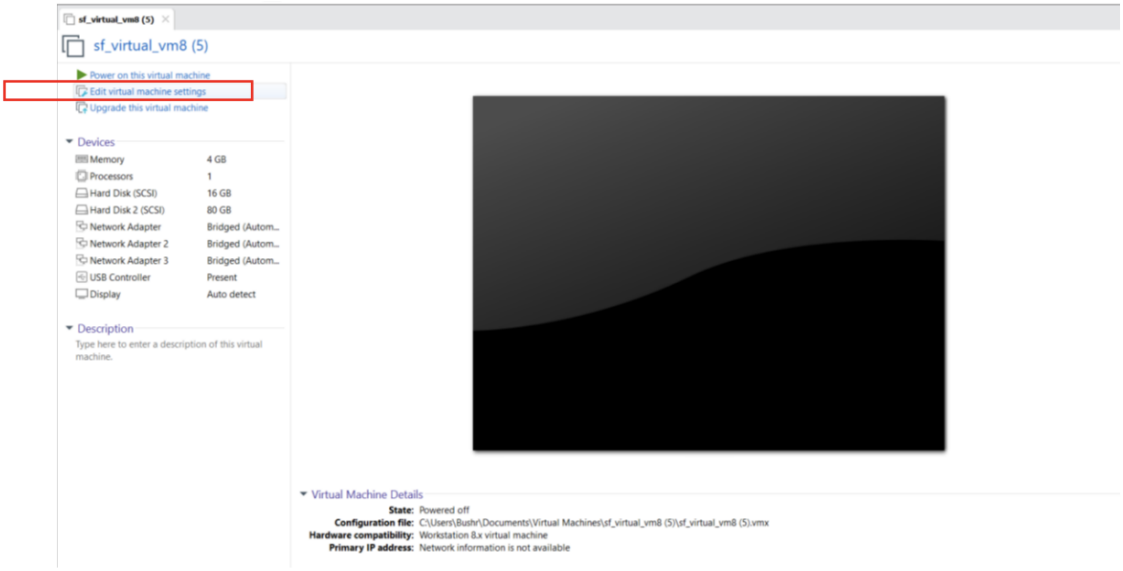
Add Network >> add the following network (VMnet1,2) as its appeare (Name, Type, Subnet Address)

IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

College	Department	Course
College of Computer Science and Information Technology	Networks and Communications	CYS502: Network Security

Practical Session Plan

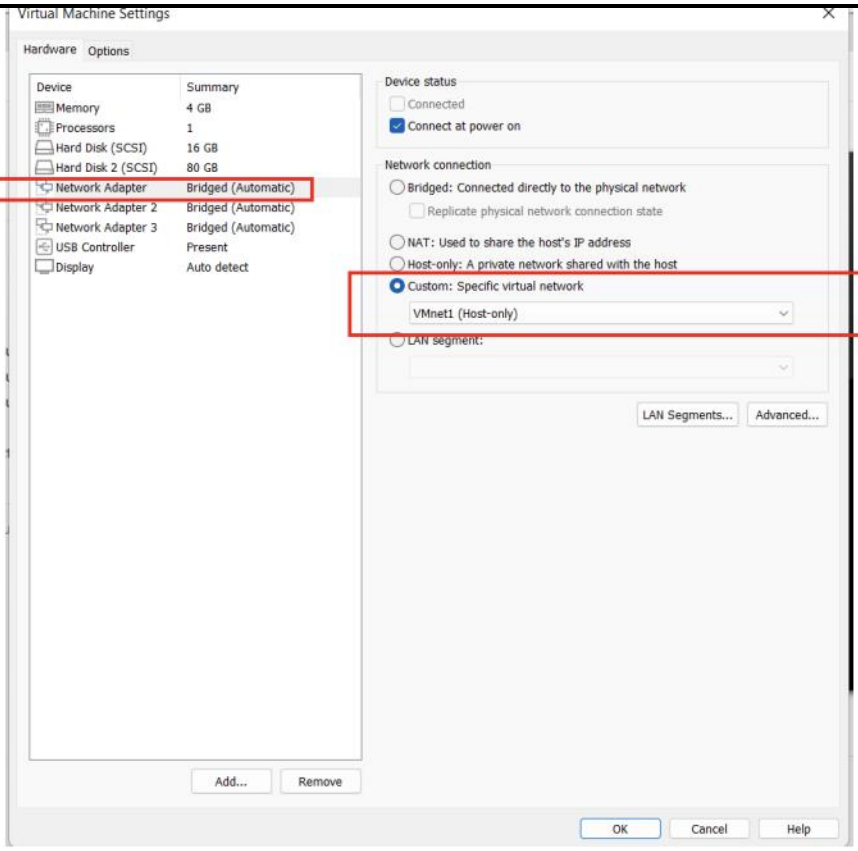


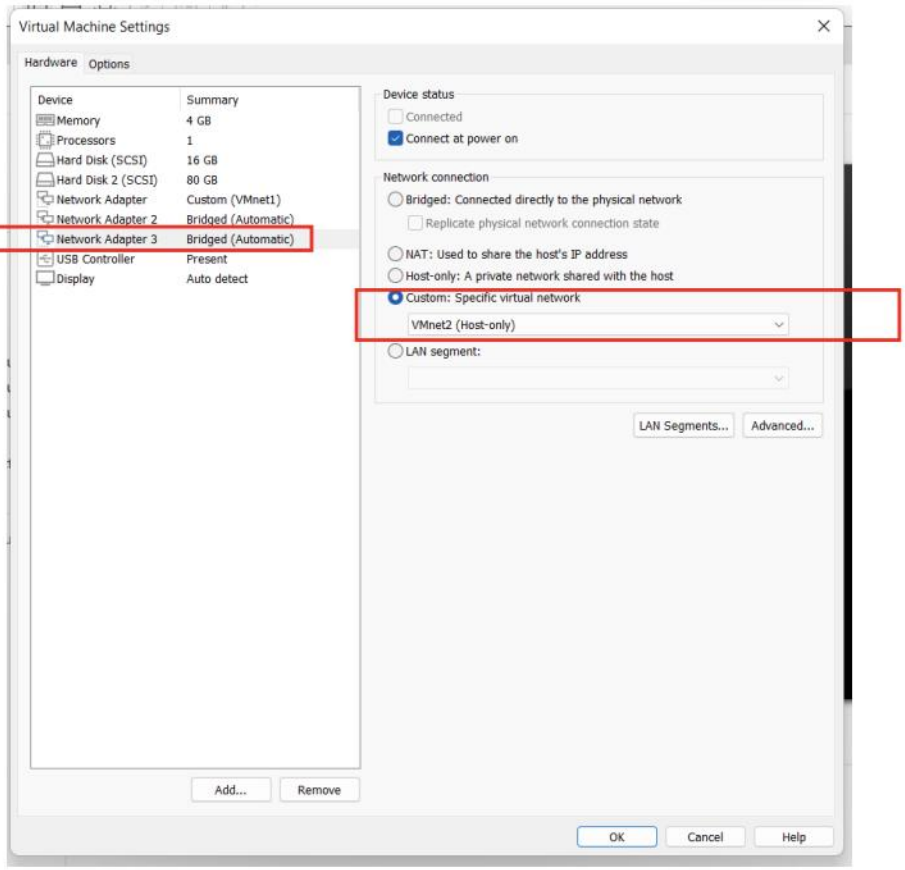


IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

College	Department	Course
College of Computer Science and Information Technology	Networks and Communications	CYS502: Network Security

Practical Session Plan



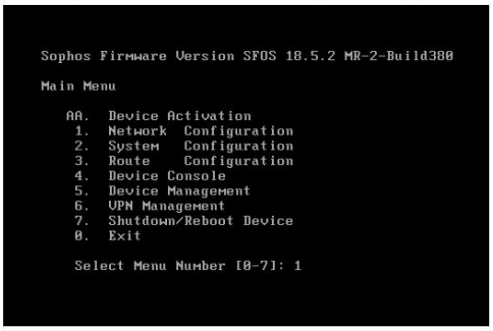


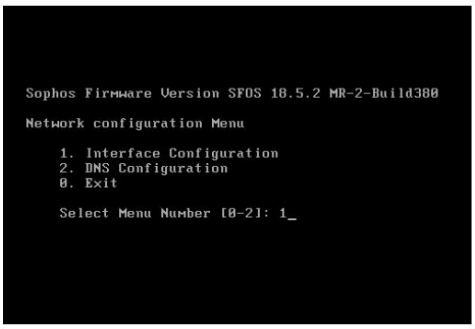
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

College	Department	Course
College of Computer Science and Information Technology	Networks and Communications	CYS502: Network Security

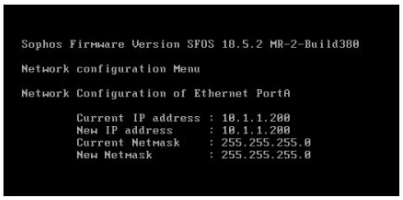
Practical Session Plan

Run the machine >> Default password “admin” >> Tab + “E” >> Enter (For Accept) >>Select 1 in both choices >> then click “Enter” twice

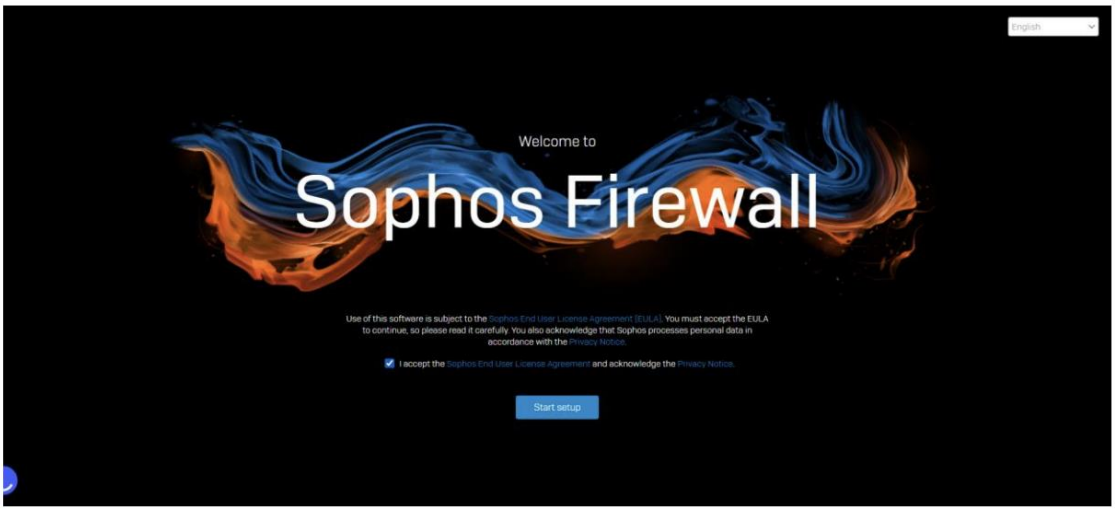








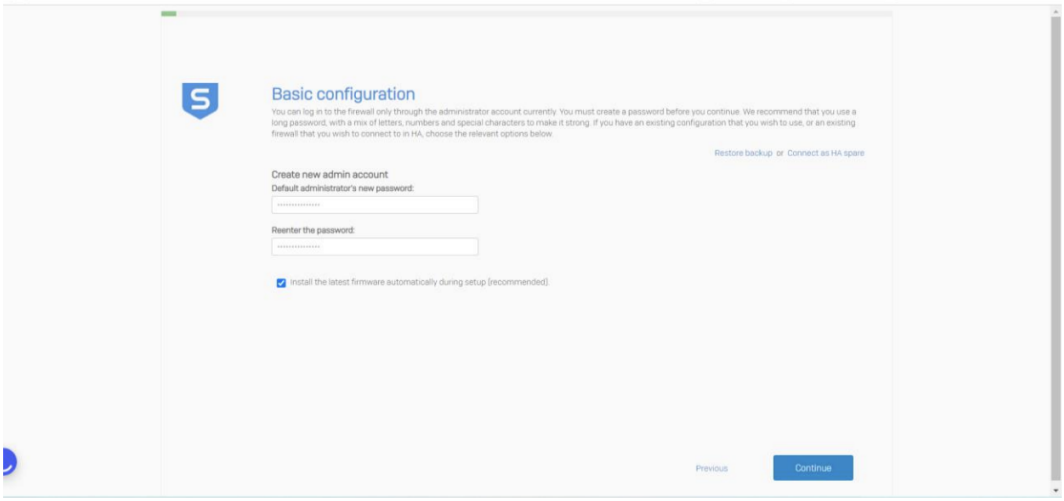
- **Search https://10.1.1.200:4444**

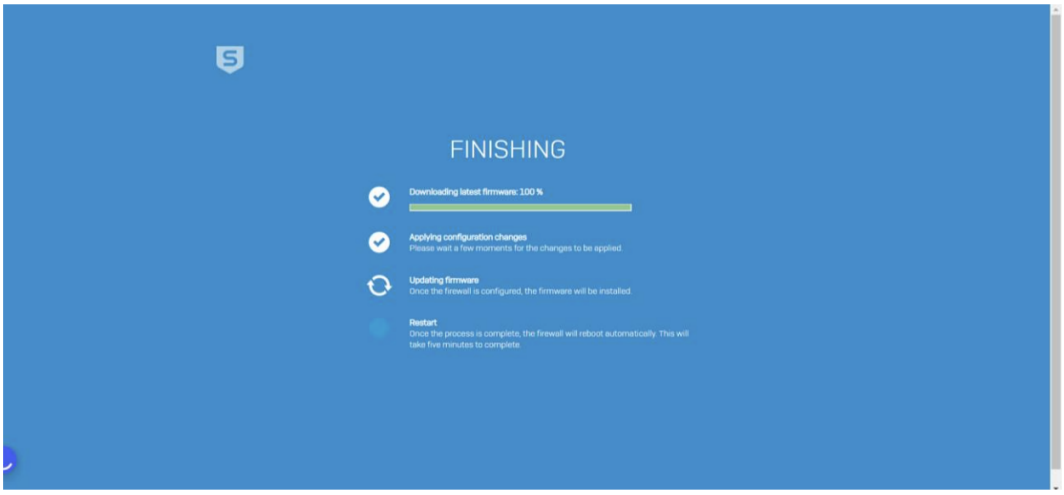


IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

College	Department	Course
College of Computer Science and Information Technology	Networks and Communications	CYS502: Network Security

Practical Session Plan



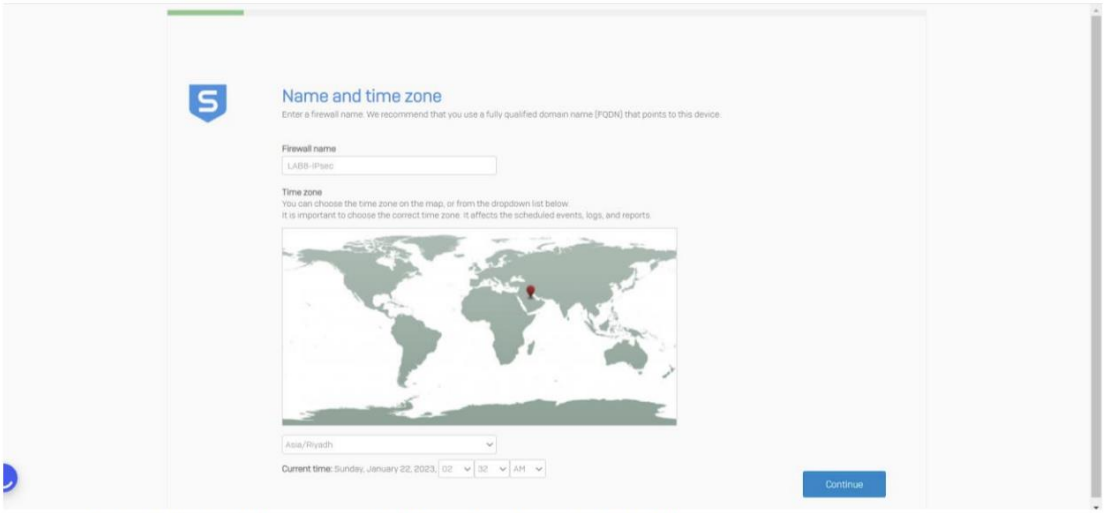


IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

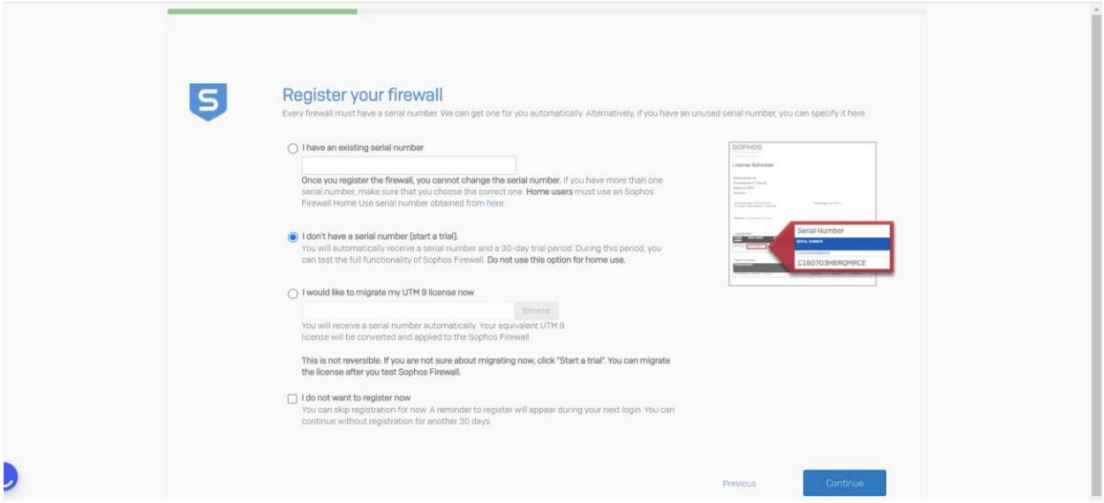
College	Department	Course
College of Computer Science and Information Technology	Networks and Communications	CYS502: Network Security

Practical Session Plan

- **Fill the name and the time zone**



- **Select "I don't have a serial Number (start a trial)"**

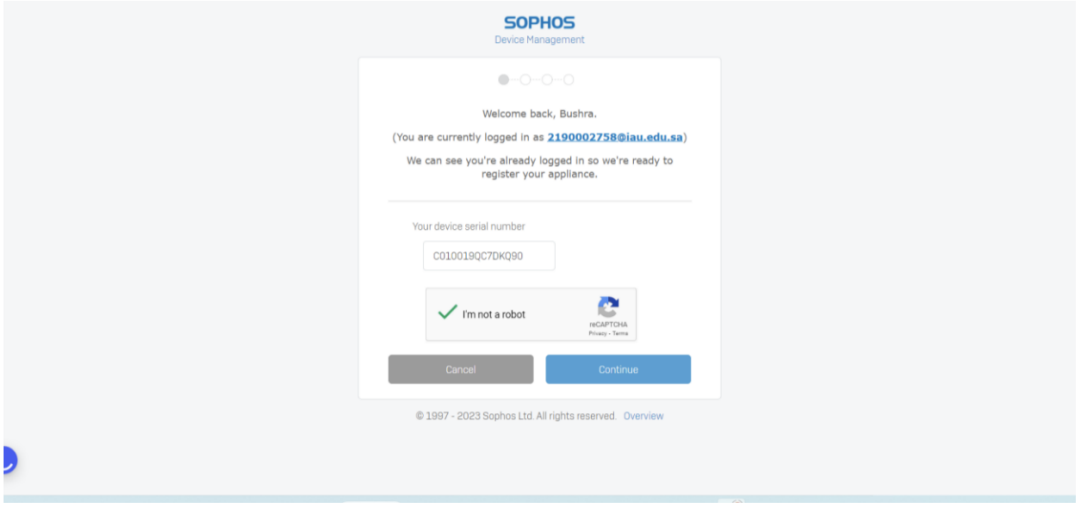


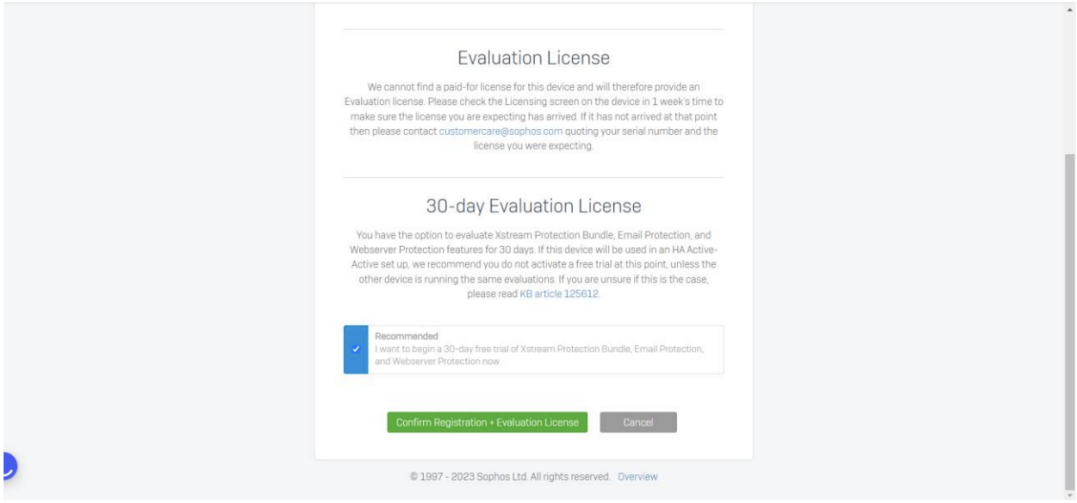
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

College	Department	Course
College of Computer Science and Information Technology	Networks and Communications	CYS502: Network Security

Practical Session Plan

- **Create Sophos ID >> Sign in >> "Confirm regestration + Evaluation License"**

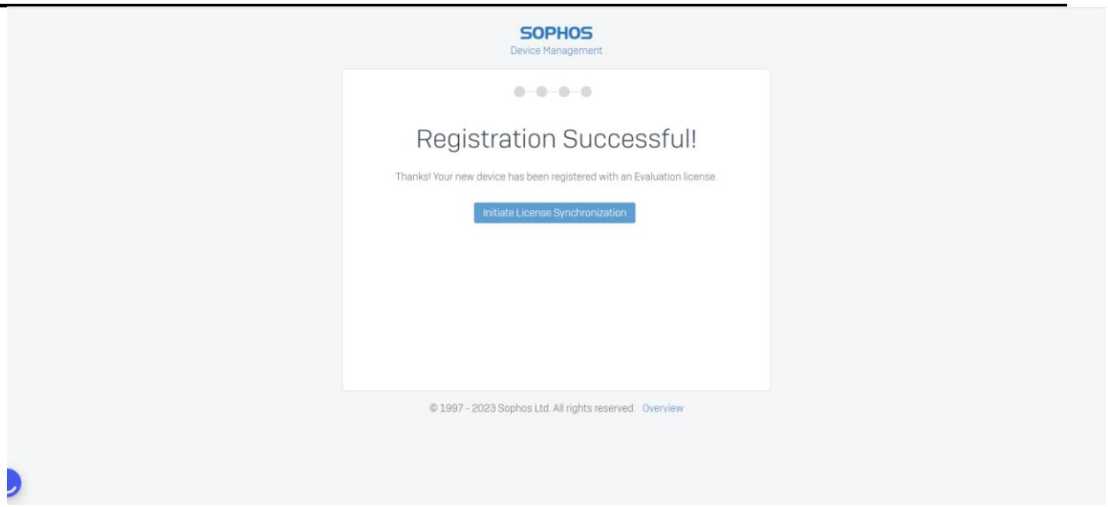


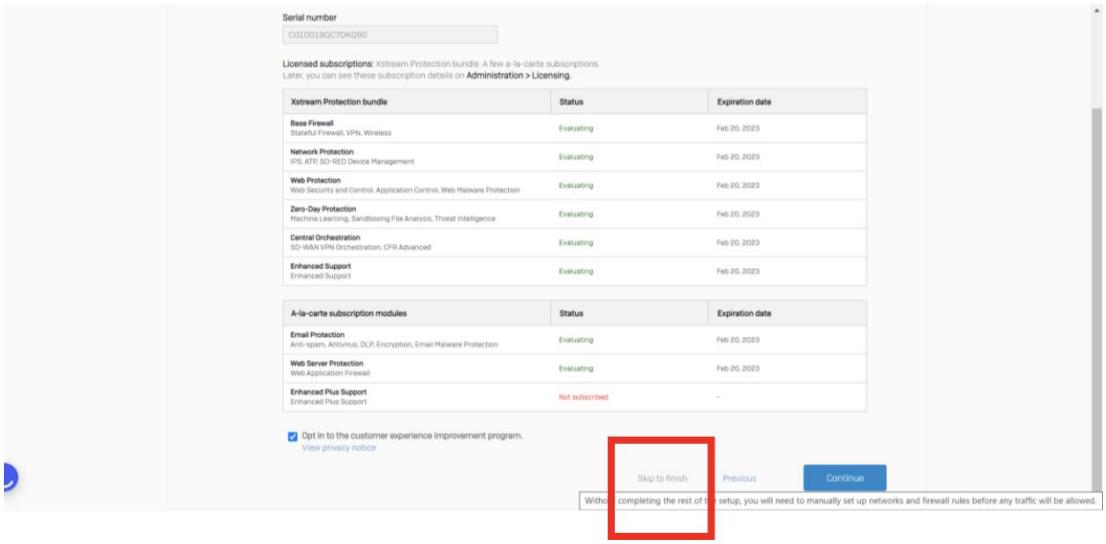


IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

College	Department	Course
College of Computer Science and Information Technology	Networks and Communications	CYS502: Network Security

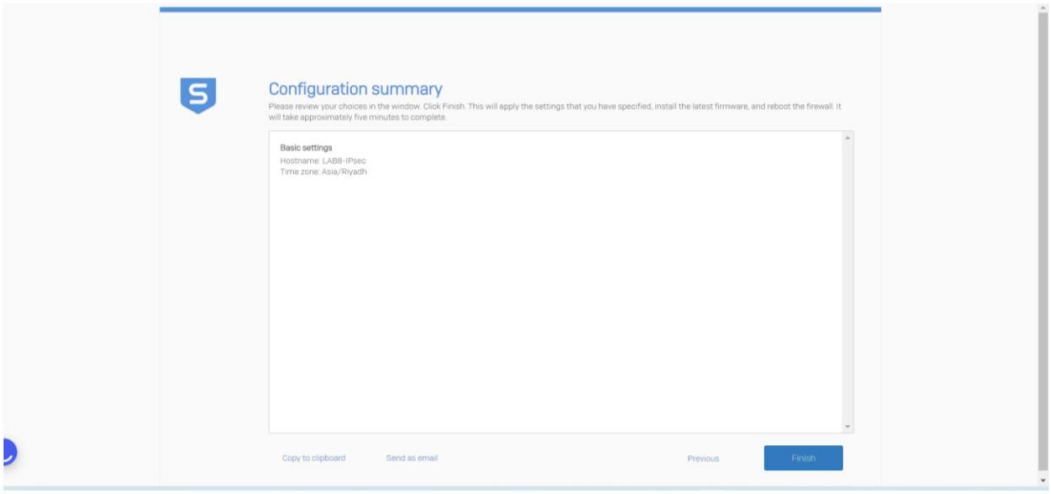
Practical Session Plan



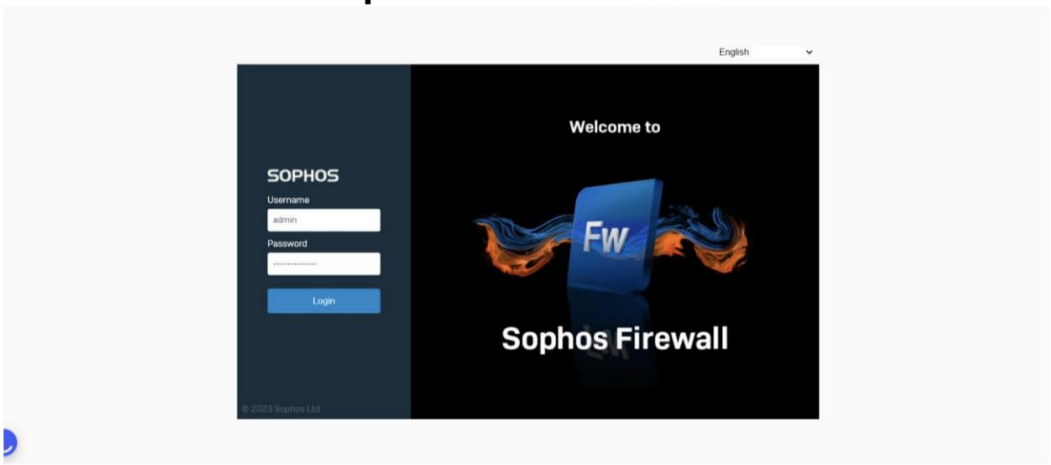


College	Department	Course
College of Computer Science and Information Technology	Networks and Communications	CYS502: Network Security

Practical Session Plan



- **The username and password are "Admin**

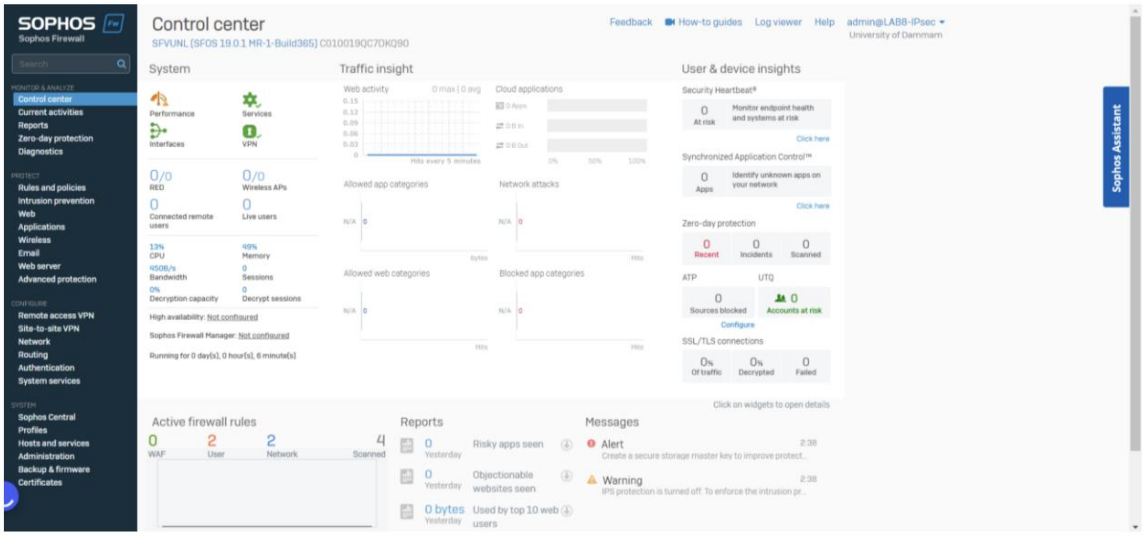


IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

College	Department	Course
College of Computer Science and Information Technology	Networks and Communications	CYS502: Network Security

Practical Session Plan

- **It works! Now you can start with part 2** 😊



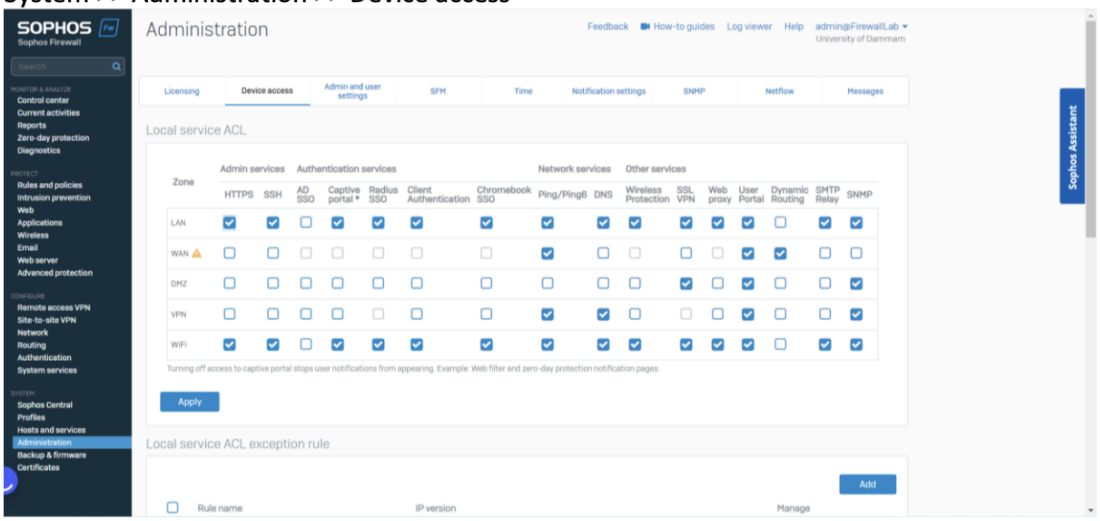
Part2: IPsec configuration

Setup requestions

- **Modify on ACL to enable ping and User Portal**

Note: Ping allow for diagnosis for troubleshooting, while User Portal allow users to connect the VPN

System >> Administration >> Device access



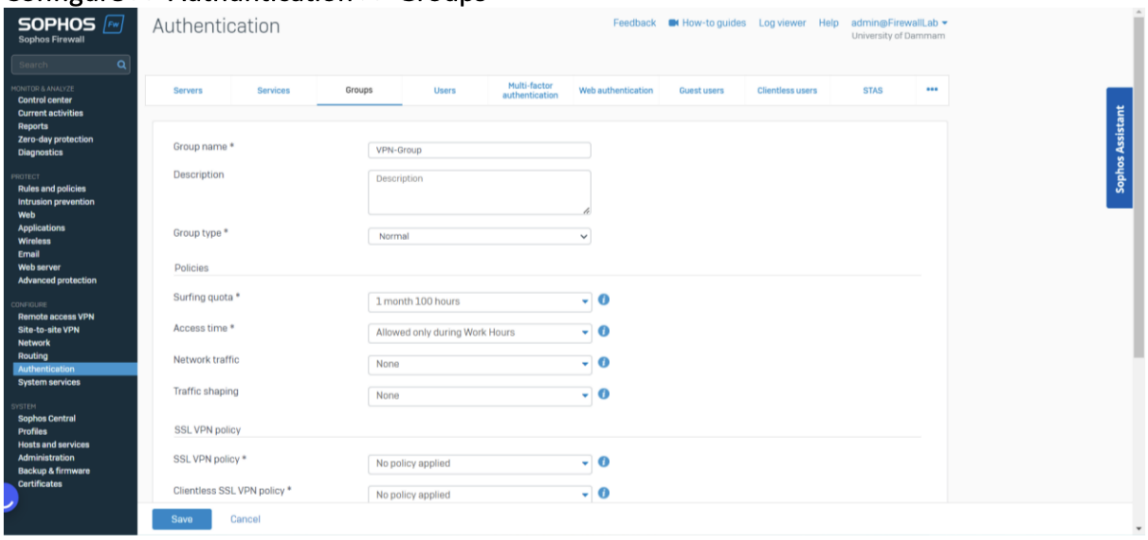
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

College	Department	Course
College of Computer Science and Information Technology	Networks and Communications	CYS502: Network Security

Practical Session Plan

- **Create a new group and allow accessing time only during working hours and 100 hours of surfing for one month**

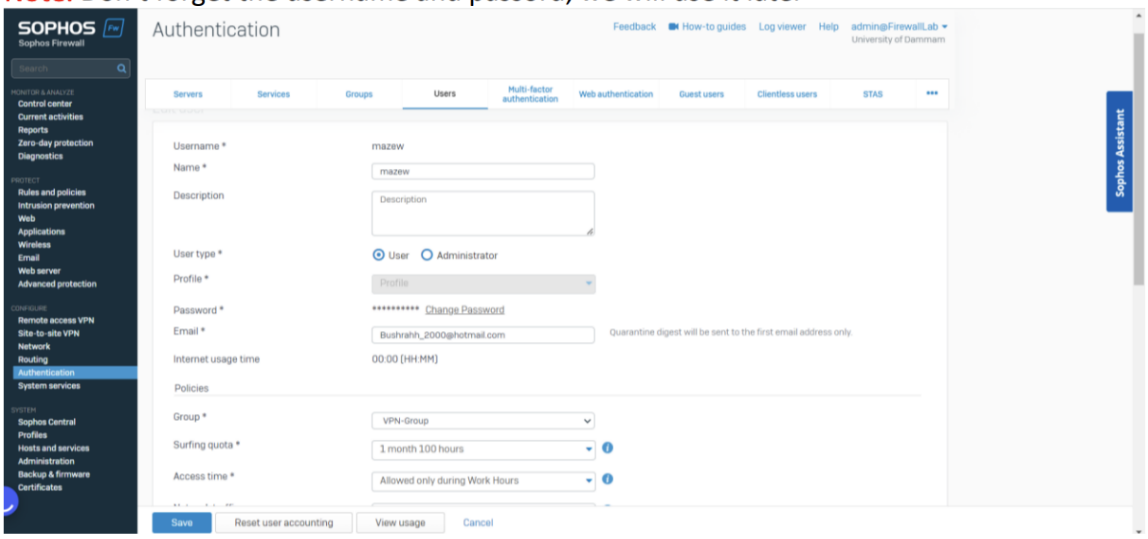
Configure >> Authuntication >> Groups



- **Create a new user and assign it to the VPN-Group**

Configure >> Authuntication >> Users

Note: Don't forget the username and passord, we will use it later



IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

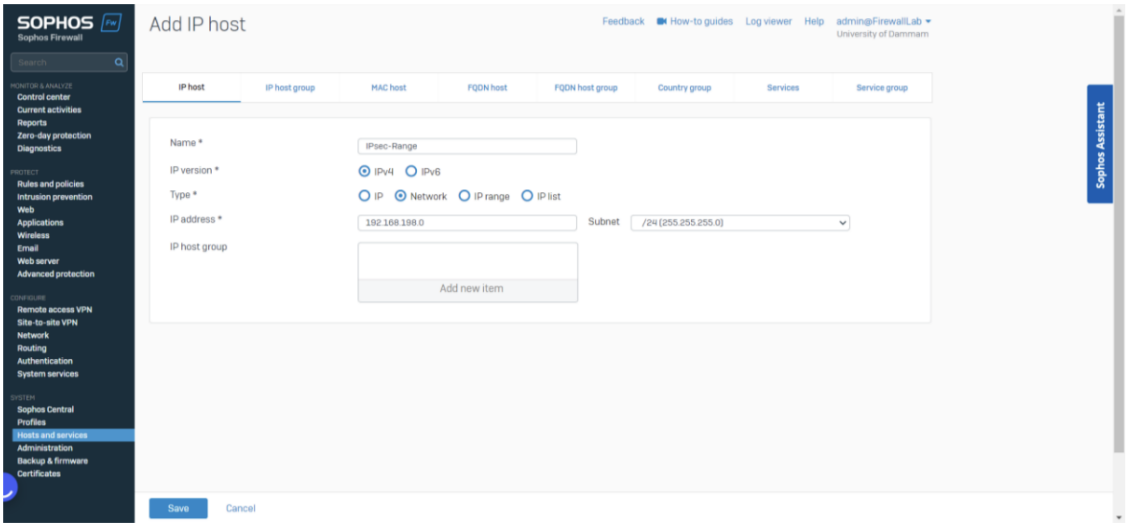
College	Department	Course
College of Computer Science and Information Technology	Networks and Communications	CYS502: Network Security

Practical Session Plan

- **Create a rule that covers the IP range which will use IPsec**

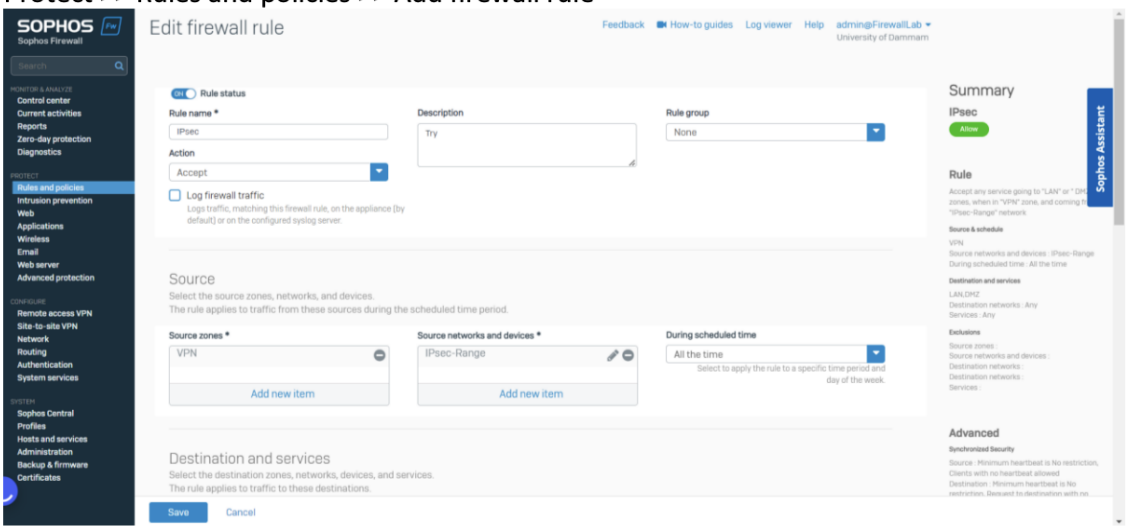
Note: Use your local IP range

System >> Host and services >> IP host



- **Setup the firewall rule for IPsec connection**

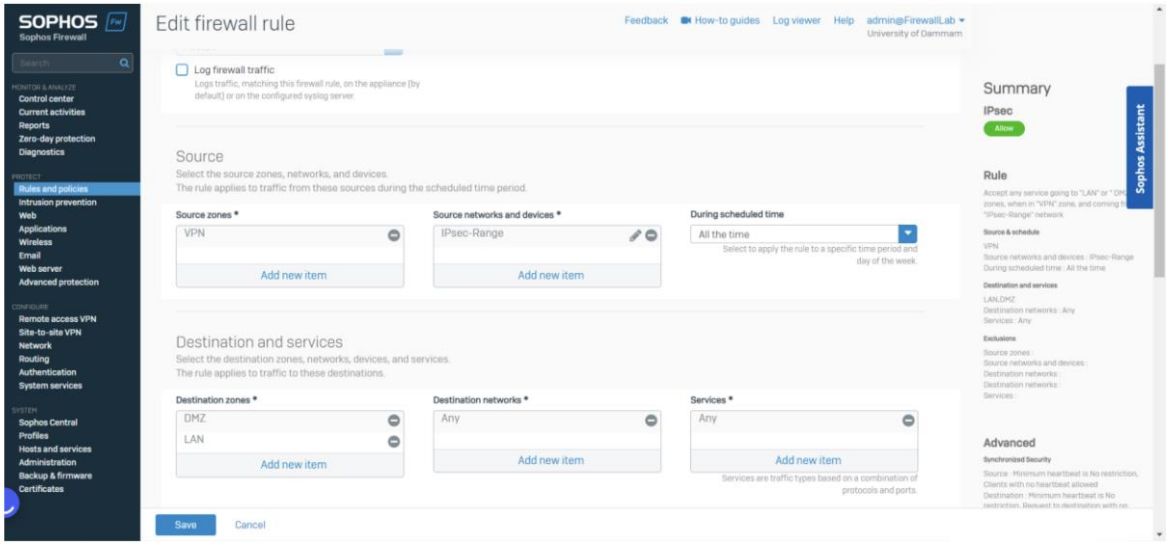
Protect >> Rules and policies >> Add firewall rule



IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

College	Department	Course
College of Computer Science and Information Technology	Networks and Communications	CYS502: Network Security

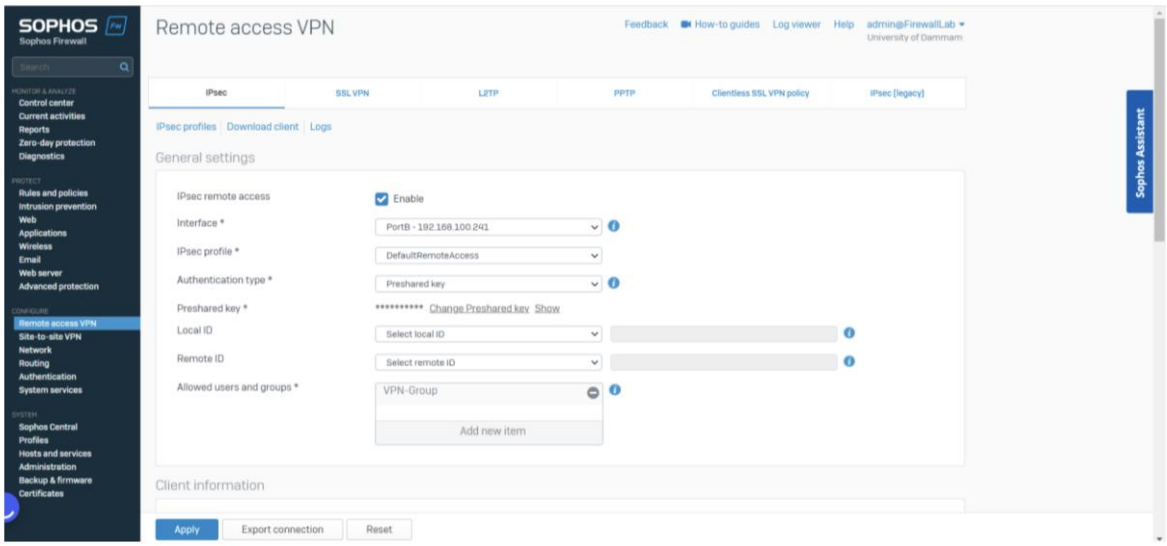
Practical Session Plan



IPsec configuration

- **Create the configuration for IPsec connection and export the connection**

Note: **Interface** It is the connection that which XG firewall expecting to come from
Note: **Authentication type** select the *"pre shared"* key and fill a password from your own choose

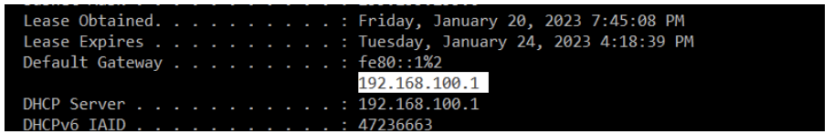


IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

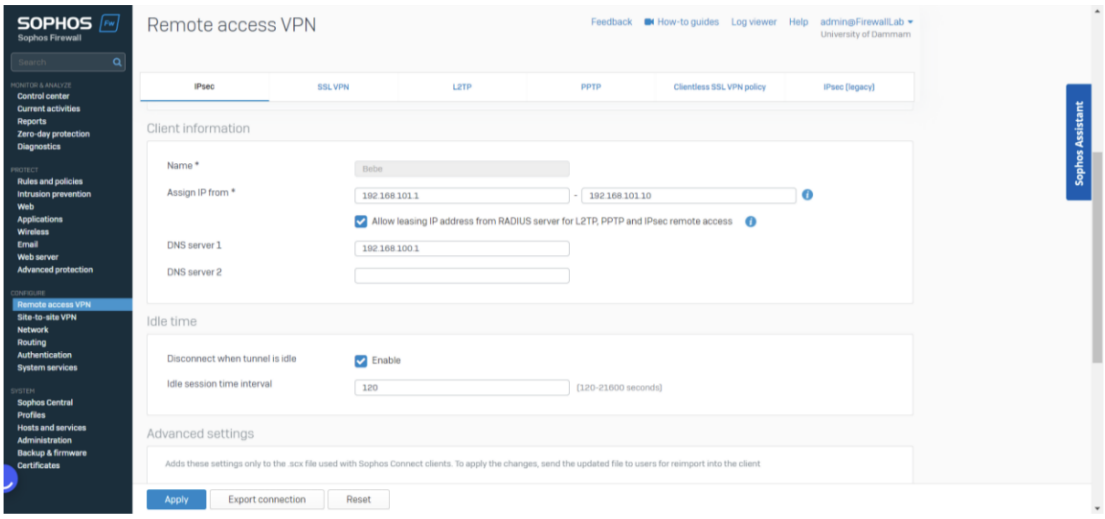
College	Department	Course
College of Computer Science and Information Technology	Networks and Communications	CYS502: Network Security

Practical Session Plan

Note: To find the DNS server, CMD >> ipconfig /all



Note: **Assigning IP form** It is the IP address which will assigned to the user of IPsec connect (You can choose whatever you want, but make sure this range not overlap with any other network)



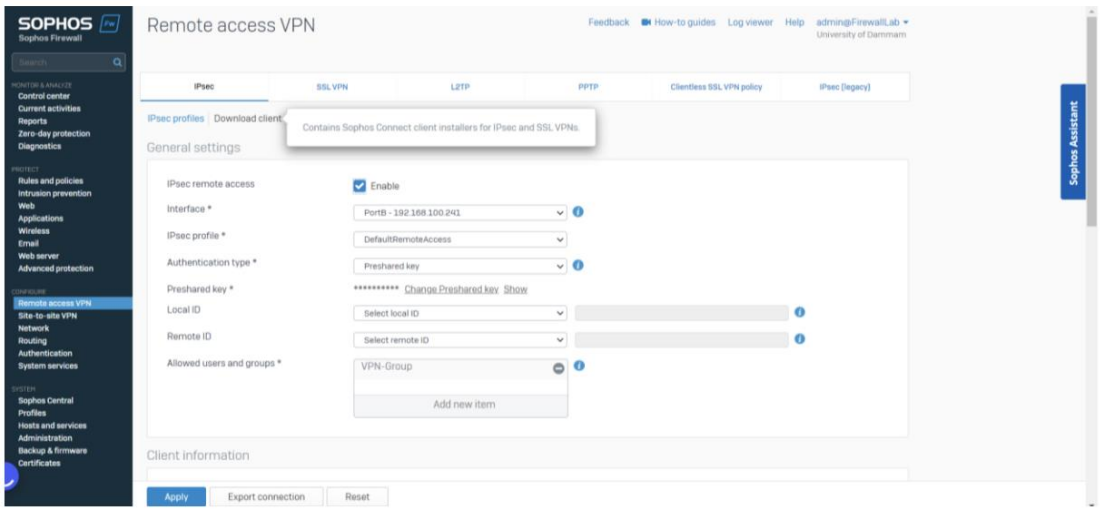
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

College	Department	Course
College of Computer Science and Information Technology	Networks and Communications	CYS502: Network Security

Practical Session Plan

Connect To IPsec

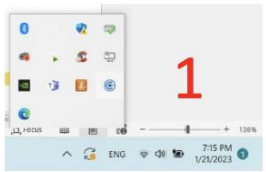
- **Download the client and run the "SophosConnect_2.2.75_(IPsec_and_SSLVPN).msi"**

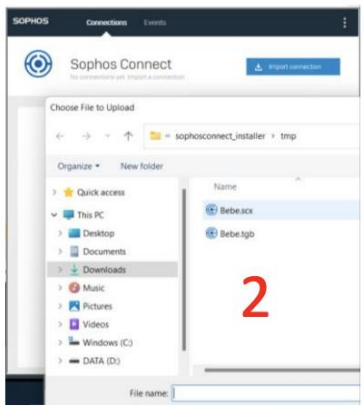


- **Export the connection and extract it**



- **Import the connection on "Sophos connect"**

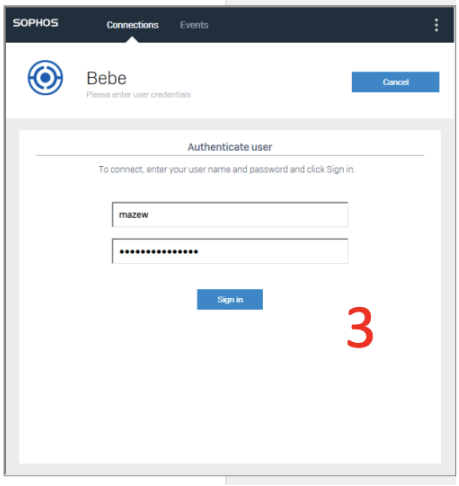




IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

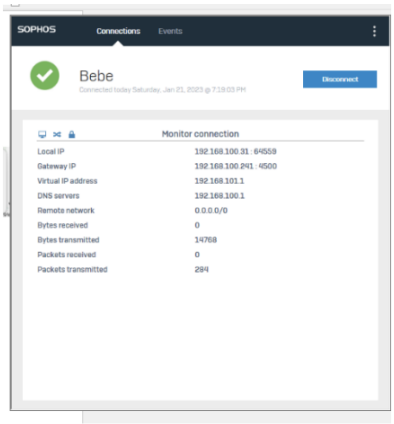
College	Department	Course
College of Computer Science and Information Technology	Networks and Communications	CYS502: Network Security

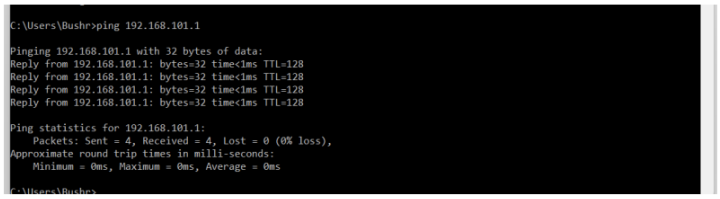
Practical Session Plan





Validate the IPsec Connection





And try to search on the browser, it works!

4- Assessment

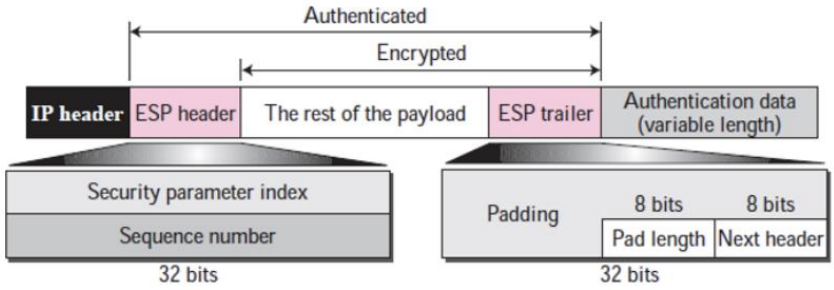
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

College	Department	Course
College of Computer Science and Information Technology	Networks and Communications	CYS502: Network Security

Practical Session Plan

Tasks:

1- Download and configure the XG firewall
2- Create your own IPsec and name it with your nickname
3- Connect to the IPsec and verify the connection (provide screenshots)
4- Capture the traffic and figure out the ESP headers (provide screenshots)



5- Resources

- https://www.youtube.com/watch?v=_Bsxv8gT7tU
- https://techvids.sophos.com/watch/wtqMJE1La6TkFjAiaT2d3H
- https://docs.sophos.com/nsg/sophos-firewall/18.5/Help/enus/webhelp/onlinehelp/AdministratorHelp/VPN/RemoteAccessVPN/VPNIPsecSophosCo nnectClient/index.html