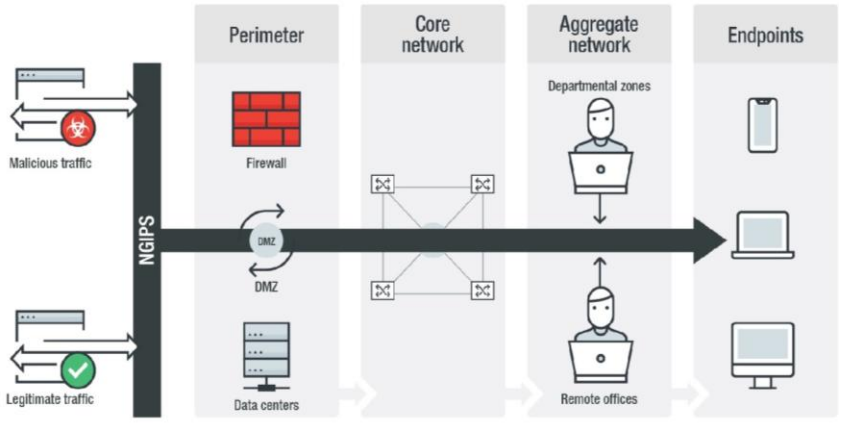
NAIT

Edmonton **Alberta**

CYBR3010

Cybersecurity Foundations

Network Perimeter Defence



CYBR3010

Cybersecurity Foundations

Network Security Lab

Objectives

The major purpose of this lab is to provide the students a realistic experience in securing a network after a merger or acquisition, emphasizing the use of a firewall to protect the internal network and create DMZs for public-facing services. An opportunity to exhibit their knowledge in setting security measures in a computer network, how the network operates, protocols, standards, security considerations, and the prototypes associated with a range of networking technologies.

The assignment will help you check your knowledge for configuring and installation of an integrated, real-time and attack prevention using a virtual firewall appliance.

Prerequisites

- A Virtual Managed Network Switch
- A Virtual Firewall
- Virtual VMs (representing different departments including a server VM with AD DS role installed)

The completion of this assignment will illustrate that the student has been able to:

- Design a secure an efficient networked system.
- Implement and examine advance networking security principles and their protocols.
- Implement and examine networking devices and operations.

There are two parts based on the scenario. You are required to contextualize the task as per the given scenario wherever possible.

Scenario

InnoEng, officially known as Innovative Engineering Ltd, is a prominent global leader specializing in design and engineering solutions. Established in 1985, the company has since amassed a substantial paid-up capital, exceeding 11.36 billion Canadian dollars.

The company's headquarters and corporate offices are situated in Toronto, Ontario, serving as its central hub. InnoEng boasts an extensive network encompassing 140 branches and 135 remote sites, strategically positioned to cater to a diverse clientele.

Notably, InnoEng has recently embarked on an expansion initiative by acquiring Secure Tech Engineering (**STE**), a smaller engineering firm with a strong focus on technology and innovation, situated in Edmonton, Alberta. This acquisition marks InnoEng's foray into the Western Canadian market.

STE's IT services have been overseen by a tech-savvy engineer, leading to an interesting network build that is now part of InnoEng's evolving network infrastructure.

STE has 3 departments with the following responsibilities and infrastructure:

Engineering Department: The Engineering Department is the core of STE business. Engineers and technical staff in this department are responsible for designing, developing, and overseeing various engineering projects. This includes structural engineering, mechanical engineering, electrical engineering, and other specialized engineering fields.

Finance Department: This department is responsible for the financial planning of the company. It comprises of Finance Officer along with other three lower-level officers responsible for the operation of the finance department.

HR Department: This department is responsible for managing and optimizing the workforce of the branch. Hiring, firing, capacity development of working personnel, etc. are some of the main responsibilities of the company. It comprises of an HR Officer allowing with an assistant officer for its operation.

You have been hired as an IT contractor to rebuild and reconfigure network before its given to InnoEng IT staff to support and further maintain. Your major roles and responsibilities are to plan, design, implement, and secure the network system for InnoEng considering ALL security measures, IP addressing, server systems, various other services, Network devices, Security devices, etc.

Network Topology

SecureTech Engineering (Exisiting)

- An unmanaged network switch.
- Staff desktop computers
- A server
- A router

InnoEng Requirements

- ***Segmented Network***
  - Engineering Department (VLAN 10 - InnoEng)
  - Finance Department (VLAN 20 - InnoEng)
  - HR Department (VLAN 30 - InnoEng)
- ***Firewall***
  - Essential configurations including interfaces, IP addressing, DHCP, and routing.
  - Only Active Directory–authenticated “HR” staff accounts are permitted to communicate with Finance department systems; all other inter-departmental communication is blocked.
  - Bandwidth usage for the Engineering Department is capped at a maximum of 3 MB/s.
  - Access to the firewall web console is restricted exclusively to systems within the IT Department.
  - Enable a minimum of two Next-Generation firewall features and demonstrate their impact on network traffic.
  - The SSL inspection certificate is distributed to clients via Group Policy Object (GPO).
  - Logging for firewall events and security incidents is enabled.

  All policies must clearly define network traffic criteria, including IP addresses, address ranges, protocols, applications, and content types, in accordance with organizational information security standards. Configurations should use precise matching conditions to **grant only the necessary access while denying all other traffic.**

- ***Switch:*** Configured with the necessary VLANs to enable local network connectivity, ensuring network segmentation, and implementing suitable layer 2 security measures.
- ***Windows Server:*** Setup with DC with Active Directory services domain environment (Domain named after student’s last name).
- ***Staff Desktops:*** All InnoEng systems are integrated into the domain, using secure Active Directory user logins.

Deliverables#1 – Lab Video (50 Marks):

For this deliverable you will work with your group and turn in a video with a 20 – 30-minute duration**. In your video explain your network, demonstrate live and verify the following:**

- Network overview - Using a network diagram, start the video by providing an overview of the network setup, including the VMs and the firewall configuration.
- Show case security across the 7-layer model by implementing, discussing, and demonstrating at **least 6 security measures in 4 different layers.**
- Complete network connectivity, ensure to highlight and show case security rules, isolations, best practices, and security measures throughout video. (Represent each department with at least 1 VM)
- Justifications for technologies, features and protection applied.
- Perimeter defense
    - Show separation between different departments networks and apply firewall rules according to InnoEng requirements.
    - Demonstrate the before and after states for each firewall rule applied.
    - Verify that the firewall is enforcing the policies by testing network connectivity and traffic flow between the VMs.

Deliverable #2 – Lab Documentation (50 Marks):

For this deliverable your group will create an electronic document that conforms to the CYBR3010 Documentation Standards on the Moodle page. **The document should include the following:**

- An introduction to provide an overview of your report.
- An explanation of networking principles, and devices, including benefits and constraints of networked solutions, the impact of network topology, communication and bandwidth requirements, the effectiveness of security measures, and the firewall rules.
- A Visio diagram of the final network
- A detailed step by step guide that can be used to rebuild the system.
- Answer the following questions:
    - What is meant by “network perimeter defense” in modern enterprise networks? Explain how the traditional concept of a perimeter has evolved with cloud adoption, remote work, and mobile devices.
    - Compare the capabilities of a Next-Generation Firewall (NGFW) with those of a traditional Layer 3/4 firewall. Highlight features such as application awareness, intrusion prevention, SSL inspection, and user-based policies.

- How can NGFWs leverage threat intelligence feeds for proactive defense? Discuss the potential benefits and risks of relying on third-party threat intelligence in firewall policy decisions.
- How can NGFW policies support a Zero Trust security model? Explain how concepts such as micro-segmentation, least privilege, and continuous verification can be applied at the perimeter level.