

Week 7 Tutorial: Security Technologies- Firewalls and VPNs

Group Discussion and Analysis (60 minutes)

Groups discussion continues using the same scenarios and groups allocation as previous weeks.

Scenario topics:

1. An online holiday booking system.
2. A medium size school timetabling and attendance system
3. An estate agent web application
4. A restaurant self-service digital ordering system

Risk management work phase (1 hour)

Each group must:

a) Choose Suitable Firewall Types

1. Evaluate different Firewall types (e.g., Packet-Filtering Firewalls, Stateful Inspection Firewalls, Proxy Firewalls, Next-Generation Firewalls (NGFWs)).
2. Determine the most appropriate firewall type(s) for your system, considering factors such as:
 - Sensitivity of data being processed
 - Threat landscape and risk exposure
 - System architecture (e.g., cloud-based, on-premises, hybrid)
 - Compliance requirements
3. Justify why the chosen firewall is best suited for your system.
4. Research a specific firewall product that meets the type you identified. Consider factors such as:
 - Vendor reputation and support
 - Features and functionalities
 - Cost and scalability
 - Integration with existing security infrastructure

b) Choose Suitable VPN Types

1. Assess different VPN types (e.g., Site-to-Site VPN, Remote Access VPN, SSL VPN, IPSec VPN).

2. Determine the most appropriate VPN solution for your system, considering:
 - Who needs remote access (e.g., employees, contractors, customers)
 - Level of encryption and security required
 - System integration with existing security infrastructure
 - Compliance and data privacy regulations
 3. Justify why the selected VPN type is the best fit for your system.
- c) Implement Network Security Best Practices
1. Firewall Configuration: Define how firewall rules and policies will be set up (e.g., whitelisting, blacklisting, deep packet inspection).
 2. VPN Implementation: Explain how VPN authentication and encryption will be handled.
 3. Monitoring and Maintenance: Identify how firewall logs and VPN access logs will be monitored and reviewed for security compliance.

Presentation (10 minutes each)

Each group will briefly present their findings, explaining:

- Key network security requirements based on last week's risk assessment.
- Chosen firewall type and justification.
- Researched firewall product and why it meets the needs.
- Chosen VPN type and justification.
- Implementation of firewall rules, VPN policies, and monitoring mechanisms.

Class Discussion (30 minutes)

The remaining of the session is focused on the assignment and how you should align this week activity with the assignment tasks.