Unit 3: Securing Networks

Content Area: **Business**
Course(s): **Generic Course**
Time Period: **Semester 1**
Length: **5 weeks**
Status: **Published**

Enduring Understandings

EU 3.1: Structural Communication Vulnerabilities
Every layer of network communication introduces distinct protocols, and each protocol has structural gaps that attackers can exploit. Securing a network requires understanding exactly where data travels (from physical wires to software applications) so that defenders can shrink their attack surface and apply the right security protocols to the right layer.

EU 3.2: Disruption of Identity and Availability
Network protocols often trust data blindly, allowing attackers to fake identities, redirect traffic, or overwhelm services. Without strong verification controls (like cryptographic signatures or automated traffic filtering), core network lookup tools like ARP and DNS can be poisoned to hijack conversations or flood networks until they crash.

EU 3.3: Containment and the Death of the Perimeter
Assuming an internal network is inherently safe creates a massive risk, meaning security must be applied deeply inside the network, not just at the edge. By using VLANs, microsegmentation, and Zero Trust principles, defenders can create internal checkpoints that stop a single compromised device from infecting the rest of the organization.

EU 3.4: Programmatic Traffic Enforcement
Firewalls act as strict, rule-based border guards that must monitor traffic entering and leaving a network to be truly effective. Safe network design requires a default-deny approach—blocking everything unless it is explicitly allowed—and using DMZs to isolate public-facing systems from sensitive internal databases.

EU 3.5: The Trade-off of Inline Monitoring
Catching a network intrusion requires a constant balance between active defense and network speed. Security teams must choose between passively watching traffic to flag threats (IDS) or sitting directly in the traffic flow to block threats instantly (IPS), while continuously fine-tuning their systems to avoid being overwhelmed by false alarms.

Standards

8.1.12.CS.2	Model interactions between application software, system software, and hardware.

8.1.12.CS.3	Compare the functions of application software, system software, and hardware.
8.1.12.NI.1	Evaluate the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing.
8.1.12.NI.2	Evaluate security measures to address various common security threats.
8.1.12.NI.3	Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4	Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.1.12.IC.1	Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.
8.2.12.ED.1	Use research to design and create a product or system that addresses a problem and make modifications based on input from potential consumers.
8.2.12.ED.5	Evaluate the effectiveness of a product or system based on factors that are related to its requirements, specifications, and constraints (e.g., safety, reliability, economic considerations, quality control, environmental concerns, manufacturability, maintenance and repair, ergonomics).
CAEP.9.2.12.C.3	Identify transferable career skills and design alternate career plans.
CAEP.9.2.12.C.7	Examine the professional, legal, and ethical responsibilities for both employers and employees in the global workplace.

Essential Questions

Topic 3.1: Network Vulnerabilities and Attacks

How do the structured layers of network models (OSI and TCP/IP) define both the specific pathways for data transmission and the unique targets available to cyber adversaries?

Topic 3.2: Protecting Networks - Managerial Controls

How do common network exploits—like DDoS, Man-in-the-Middle, ARP poisoning, and DNS spoofing—disrupt communications, and what precise protocols or controls stop them?

Topic 3.3: Protecting Networks - Segmentation

How does moving from a traditional flat network to a segmented, Zero Trust architecture limit an attacker’s ability to move laterally across an organization's infrastructure?

Topic 3.4: Protecting Networks - Firewalls & Packet Filtering

How do modern firewalls use Access Control Lists (ACLs), stateful inspection, and DMZ architectures to strictly enforce default-deny policies for both inbound and outbound traffic?

Topic 3.5: Detecting Network Attacks

What are the architectural and operational trade-offs between passive detection (IDS) and active blocking (IPS) when balancing security alertness against network performance?

Knowledge and Skills

Topic 3.1: Network Vulnerabilities and Attacks

- Name all seven OSI layers in order, describe each layer's function, and identify the primary protocols and attack vectors associated with each layer
- Explain the TCP/IP four-layer model and map its layers to the corresponding OSI layers
- Identify at least 12 critical port numbers, their associated services, and the security risk each poses if left open unnecessarily
- Distinguish between TCP and UDP, explain when each is used, and identify the security implications of each protocol
- Explain encapsulation and describe how headers are added at each OSI layer as data travels from sender to receiver
- Define attack surface in the context of network security and apply attack surface reduction principles to Vantex Financial Group's network
- Identify the OSI layer at which specific attacks and controls operate (e.g., ARP attacks at Layer 2, IP spoofing at Layer 3, TLS at Layer 4–5)
- Recognize the three most common AP exam traps on OSI model and protocol questions

Topic 3.2: Protecting Networks - Managerial Controls

- Classify network attacks by their goal (Availability, Confidentiality, or Integrity violation) and the OSI layer at which they primarily operate
- Distinguish between DoS and DDoS attacks, explain the mechanism of SYN floods, UDP floods, and volumetric attacks, and identify the defenses for each
- Explain how a man-in-the-middle attack works, describe the two phases (interception and optional modification), and identify the attacks that enable MitM positioning
- Describe ARP poisoning in detail — how it works, what it enables, which OSI layer it operates at, and how Dynamic ARP Inspection prevents it
- Explain DNS spoofing and DNS cache poisoning, describe how they redirect traffic, and identify DNSSEC as the primary mitigation
- Define replay attacks, explain why they require timestamping or nonces to prevent, and distinguish them from real-time interception attacks
- Apply network attack knowledge to Vantex Financial Group scenarios in exercises and labs throughout Unit 3
- Recognize and avoid the four most common AP exam traps on network attack questions

Topic 3.3: Protecting Networks - Segmentation

- Explain what a flat network is, describe the lateral movement risk it creates, and contrast it with a segmented network architecture
- Define a VLAN, explain how switches use VLAN tags (802.1Q) to separate traffic on shared physical infrastructure, and describe the difference between access ports and trunk ports
- Explain why inter-VLAN routing must go through a Layer 3 device (router or Layer 3 switch), and how this creates a firewall enforcement point between segments
- Describe Vantex Financial Group's VLAN architecture and explain the security purpose of each segment
- Explain the Zero Trust principle of "never trust, always verify," describe how it differs from perimeter-based security, and identify its key implementation components
- Define microsegmentation and explain how it applies Zero Trust principles at the workload level
- Apply segmentation concepts to identify lateral movement paths in described network architectures
- Recognize the three most common AP exam traps on network segmentation questions

Topic 3.4: Protecting Networks - Firewalls & Packet Filtering

- Explain what a firewall does at the network level and describe the fundamental difference between packet filtering and stateful inspection
- Distinguish between stateless, stateful, and next-generation firewall types — identify which OSI layers each inspects, and determine when each type is appropriate
- Read and interpret ACL rules: given a rule set, determine whether a specific packet is permitted or denied, and explain why each rule is evaluated in order
- Apply the default-deny (implicit deny all) principle, explain why it is superior to default-allow, and identify what happens to traffic that matches no explicit rule
- Describe DMZ architecture, explain the purpose of having two firewalls, and identify which server types belong in a DMZ vs. the internal network
- Explain egress filtering and explain why outbound traffic rules are as important as inbound rules
- Analyze Vantex Financial Group's firewall rule sets for gaps, misconfigurations, and opportunities for improvement
- Recognize the three most common AP exam traps on firewall and ACL questions

Topic 3.5: Detecting Network Attacks

- Distinguish between an IDS (passive detection and alerting) and an IPS (active inline blocking), explain why the deployment position differs for each, and identify the tradeoff each creates
- Compare signature-based and anomaly-based detection methods: explain how each works, what attacks each excels and fails at detecting, and when each is appropriate
- Define false positive, false negative, true positive, and true negative in the context of intrusion detection, and explain the security impact of each error type
- Explain the tuning challenge: describe how decreasing false positives often increases false negatives and vice versa, and why proper tuning is a continuous operational process
- Describe what a SIEM does: log collection, normalization, correlation, alerting, and dashboarding — and explain how correlation across multiple log sources detects attacks that individual logs would miss
- Explain what a SOC (Security Operations Center) does and describe how analysts use SIEM data to investigate and respond to security incidents
- Apply IDS/IPS/SIEM knowledge to Vantex Financial Group's detection architecture and identify gaps in coverage

- Recognize the four most common AP exam traps on IDS, IPS, and SIEM questions

Transfer Goals

Students will be able to visualize how data moves across different layers of technology, allowing them to better troubleshoot technical issues and understand where their digital footprint is vulnerable.

Students will be able to identify when the underlying systems they rely on—like web addresses or internet traffic—are being tampered with, helping them avoid compromised websites and network-level scams.

Students will be able to organize their digital lives (like home Wi-Fi networks or smart devices) into separate, secure zones so that a compromise of one device does not grant access to everything they own.

Students will be able to establish strict "default-deny" rules for what data, traffic, or applications are allowed into their personal devices and networks, drastically reducing their exposure to outside threats.

Students will be able to interpret security alerts and system warnings critically, knowing how to fine-tune notifications to avoid the "alert fatigue" that leads people to ignore real danger signs.

Resources

AP Cybersecurity Course and Exam Description, Effective Fall 2026, College Board

AP Cybersecurity Course Framework, Effective 2026-2027 School Year, College Board

AP Cybersecurity Curriculum, by APCSExamPrep.com

Cybersecurity Curriculum Materials, by Cyber.org

Cyber Range, provided by Cyber.org