THOMAS MORE | UNIVERSITY OF APPLIED SCIENCES

THOMAS MORE | University of Applied Sciences

Computing Fundamentals

Planning

Session	Subject	Test – Hand-in
1	Network Models	
2	Internet Protocol Suite	
3	Network segmentation	
4	Network protocols	
5	Operating systems	
6	Command Line	
-- 30/10 – 5/11 --	Autumn break – HERFSTVAKANTIE	
7	Command Line	
8	Mid-term test	**Test**
9	**Scripting**	
10	Virtualization - Cloud computing	

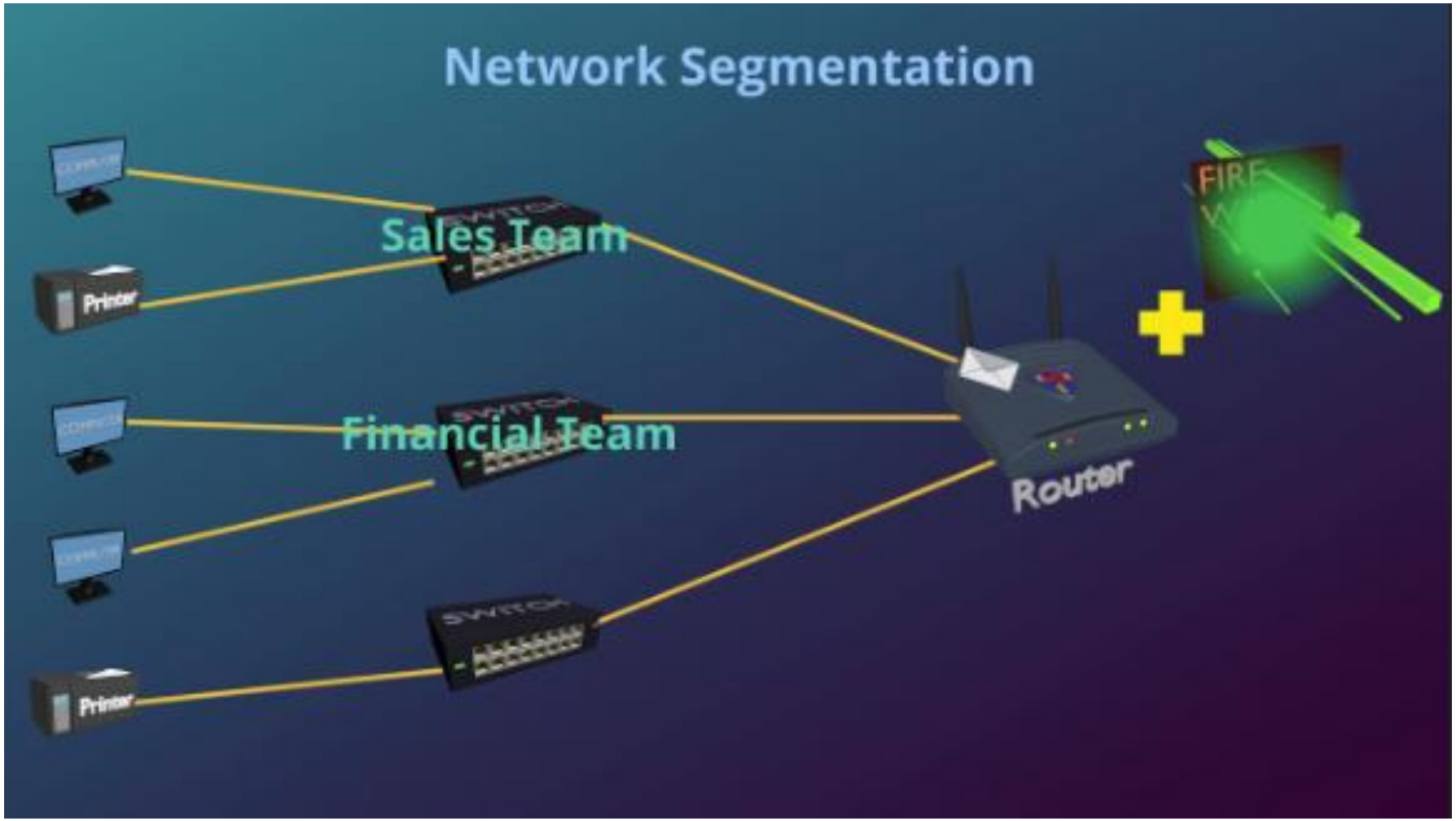
Computing Fundamentals

Network segmentation

- Network segmentation is the practice of subdividing a network into functional domains and limiting the communications between those domains.

- For example, an enterprise might create separate segments for accounting, HR, product development, manufacturing, customer service, marketing, sales and building automation. No part of the network is exempt. Segmentation works for cloud computing, as well as SaaS applications.

Computing Fundamentals



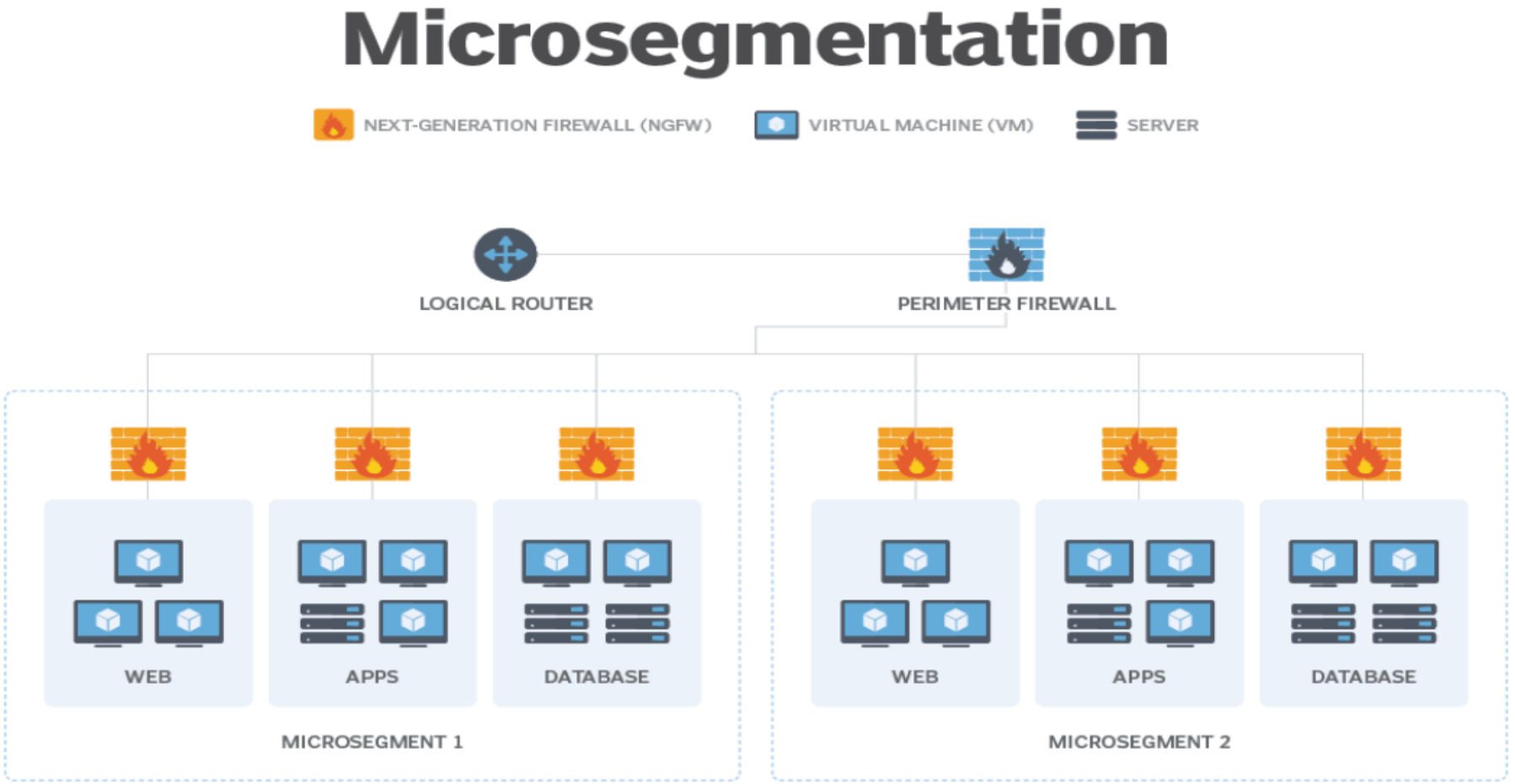
The benefits of network segmentation

- The primary benefit is that network segmentation limits the cybersecurity **attack surface**, resulting in minimization of the damage.
- On the **monitoring** front, security systems can provide alerts when an unauthorized endpoint tries to access the system, **identifying bad actors** who are attempting lateral spread.
- Segmentation can also **reduce the scope of regulatory compliance**, like the Payment Card Industry Data Security Standard. Audits only need to involve the part of the network that processes and stores payment card information. Of course, such audits should validate proper segmentation practices.

Network segmentation vs. microsegmentation

- Network segmentation divides a network into smaller sections, to which different security controls and policies are applied.
- Microsegmentation, by contrast, is a subset of network segmentation that allows even more granular controls to be applied to individual workloads.

Computing Fundamentals



Computing Fundamentals

Network segmentation in multi-layer defense mechanisms

- Network segmentation is the core of multi-layer defense in depth for modern services. Segmentation slow down an attacker if he cannot implement attacks such as:

- SQL-injections;
- compromise of workstations of employees with elevated privileges;
- compromise of another server in the perimeter of the organization;
- compromise of the target service through the compromise of the LDAP directory, DNS server, and other corporate services and sites published on the Internet.

- From owasp.org

Network segmentation best practices

- **Create security policies and identify resources**
  To implement network segmentation, network designers should start by creating security policies for each type of data and asset they need to protect. The policies should identify each resource, the users and systems that access it, and the type of access that should be provided.
- **Use allowlist ACLs**
  Next, network designers should implement allowlist access control lists. This practice significantly improves network security. Designers need to identify the application data flows for each application to make this work. While this process can take a significant amount of work, it is well worth the time and effort when compared with the cost of a cybersecurity event.

Network segmentation best practices

- **Technologies to implement network segmentation**
  Network segmentation can be based on physical separation, logical separation or both, depending on the specific instance. Firewalls, access control lists (ACLs) and virtual LANs (VLANs) provide the basic segmentation functionality.
  The next step adds virtual routing and forwarding (VRF) to segment routing information. An advanced implementation would implement a full multi-tenant system based on software-defined technologies that combine firewalls, ACLs, VLANs and VRF.

Network segmentation best practices

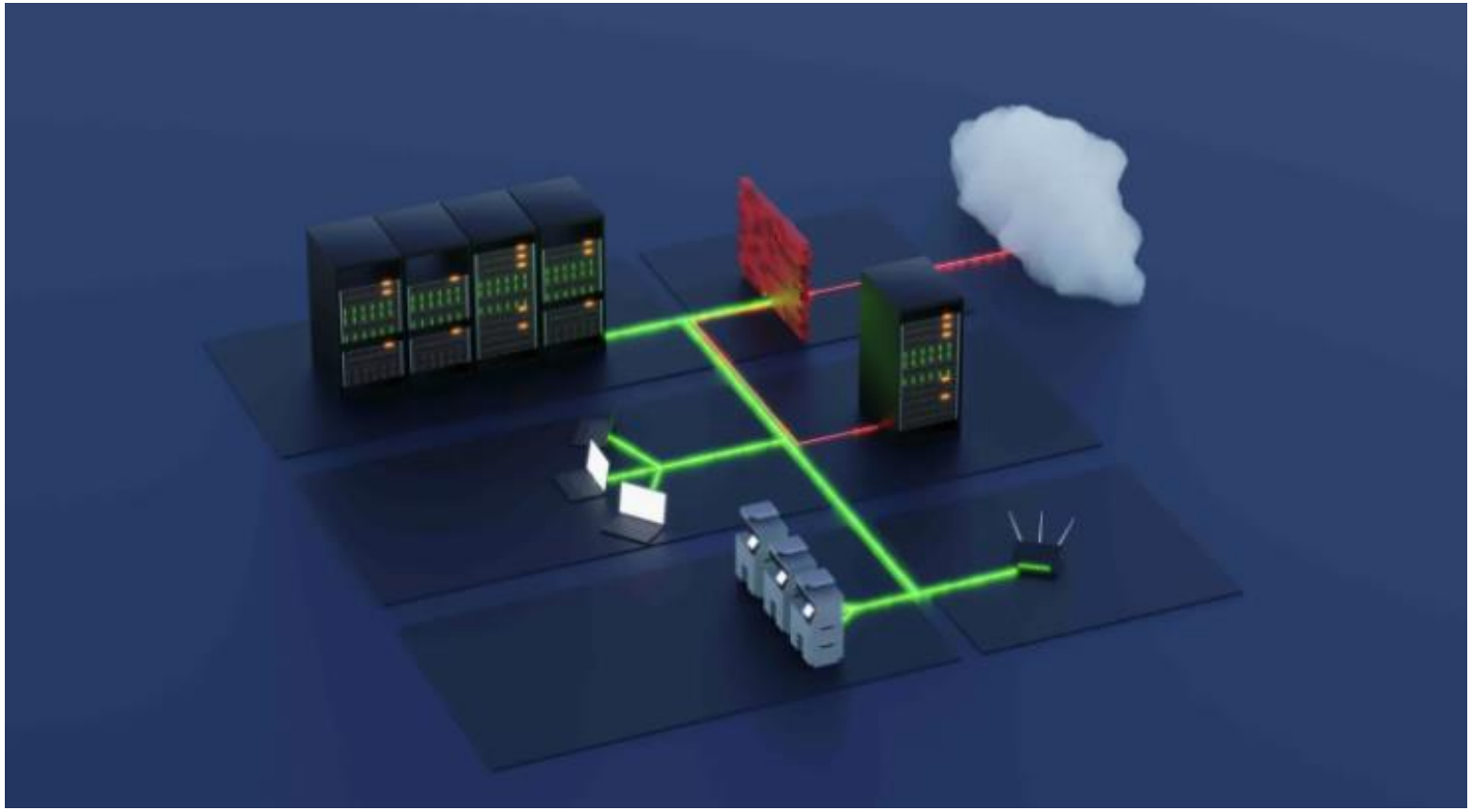
- **Software-defined access**
  Software-defined access (SD-access) identifies endpoints and assigns them to the proper network segments, regardless of where they physically connect into the network. SD-access tags packets to identify the segment to which they belong. Tagging makes it efficient for the network to apply the proper policy to network flows.
- **Physical separation**
  Network teams should use physical separation, such as separate firewalls, when they need to reduce the complexity of firewall rules. Mixing the firewall rules for a large number of applications in one firewall can become impossible to maintain.

Network segmentation best practices

- **Automation**

  Finally, network teams can use automation to help maintain network security. Many of the security audit steps can and should be automated to ensure they are consistently applied. Tools based on software-defined technology can aid in automation.

Computing Fundamentals



How does network segmentation work?

- **Complete blocking**
  The most restrictive policy completely blocks any connectivity between certain segments. For example, you may want to completely isolate payment card data to comply with PCI regulations. This would cut off lateral pathways for threats to spread as well.
- **Selective filtering**
  Instead of completely cutting connectivity, you can use selective filtering to limit what kind of traffic can flow between zones. For example, you may allow DNS and NTP but block other traffic types. Or restrict based on source IP, destination port, app fingerprints, and more.

How does network segmentation work?

- **Application-layer inspection**
  Modern environments require granular application-level controls instead of relying only on IP addresses and ports. Segmentation can integrate **next-gen firewalls** to inspect flows and explicitly allow or deny access requests based on user identity, device posture, and other contextual signals. The criteria and mechanisms may differ, but segmentation always works by enabling and securing lateral communications between isolated zones rather than just erecting perimeter boundaries. This **zero-trust** approach provides layered internal defenses to limit an attacker's progression.