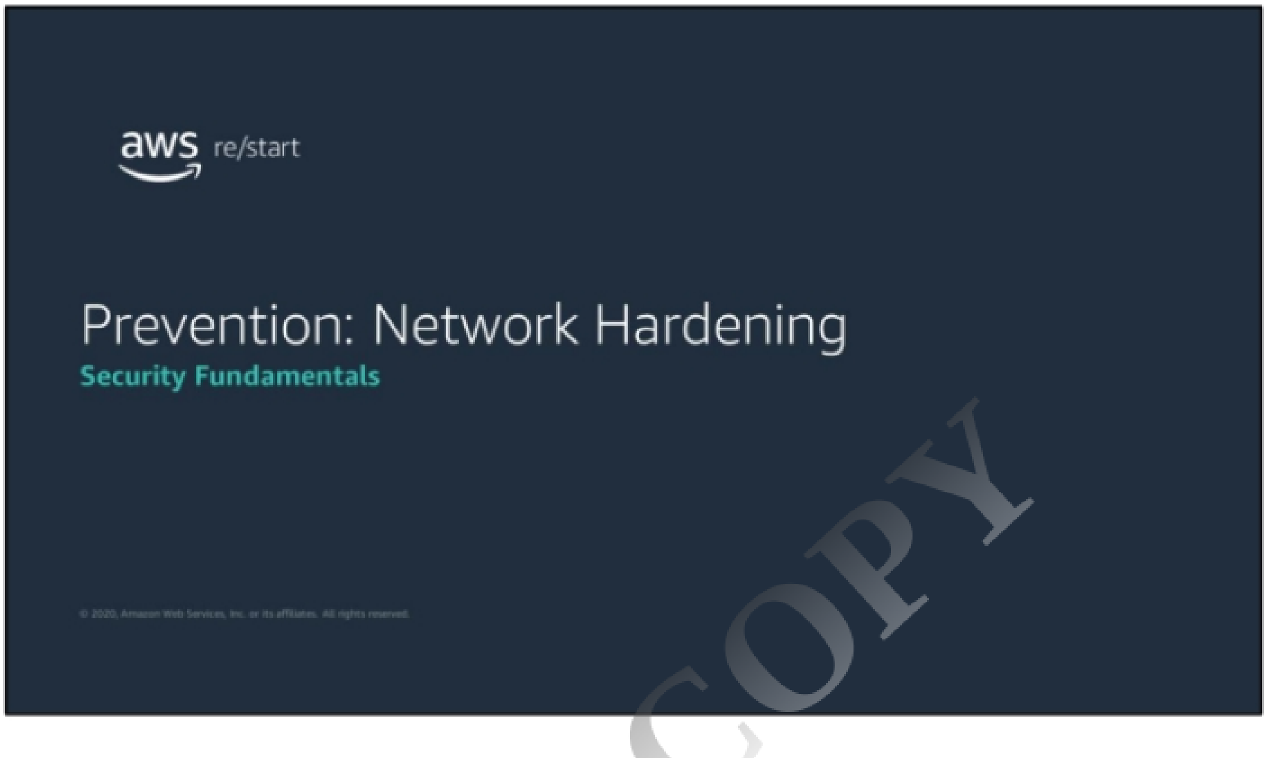
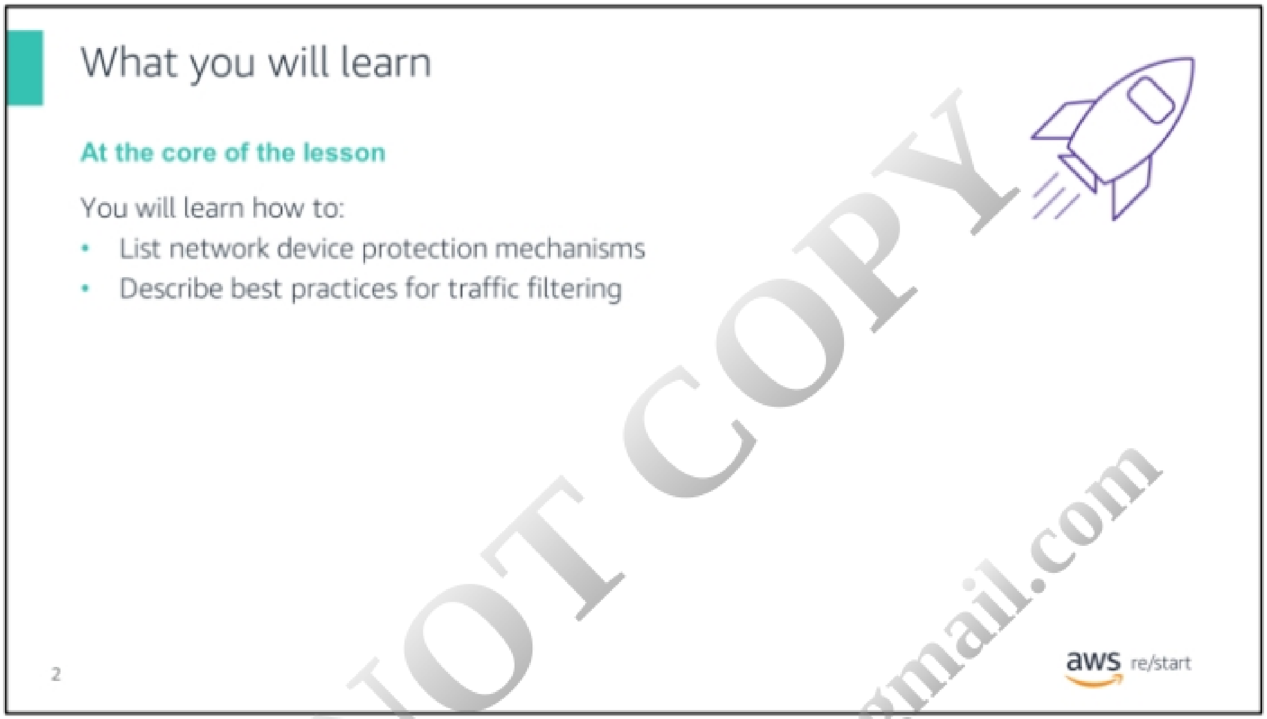


aws re/start

Prevention: Network Hardening

Security Fundamentals

Welcome to Security Lifecycle: Prevention – Network Hardening.

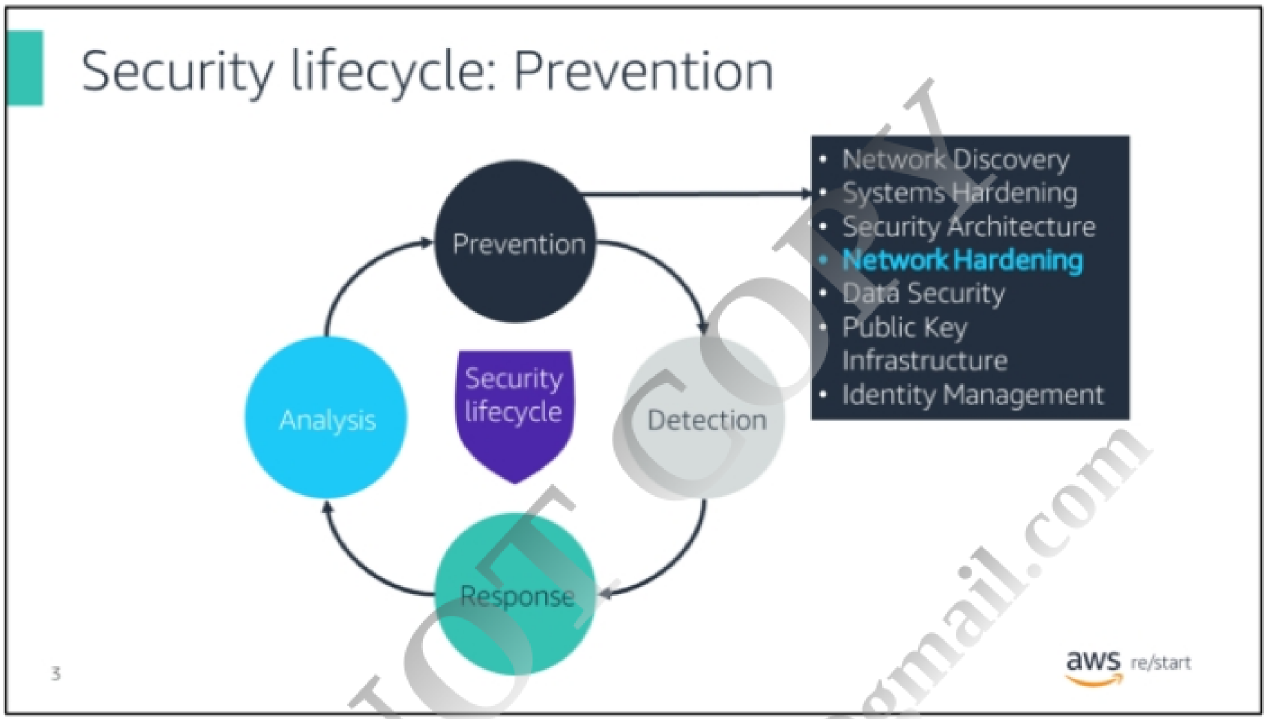


What you will learn

At the core of the lesson

You will learn how to:

- List network device protection mechanisms
- Describe best practices for traffic filtering



Security lifecycle: Prevention

Prevention

Detection

Response

Analysis

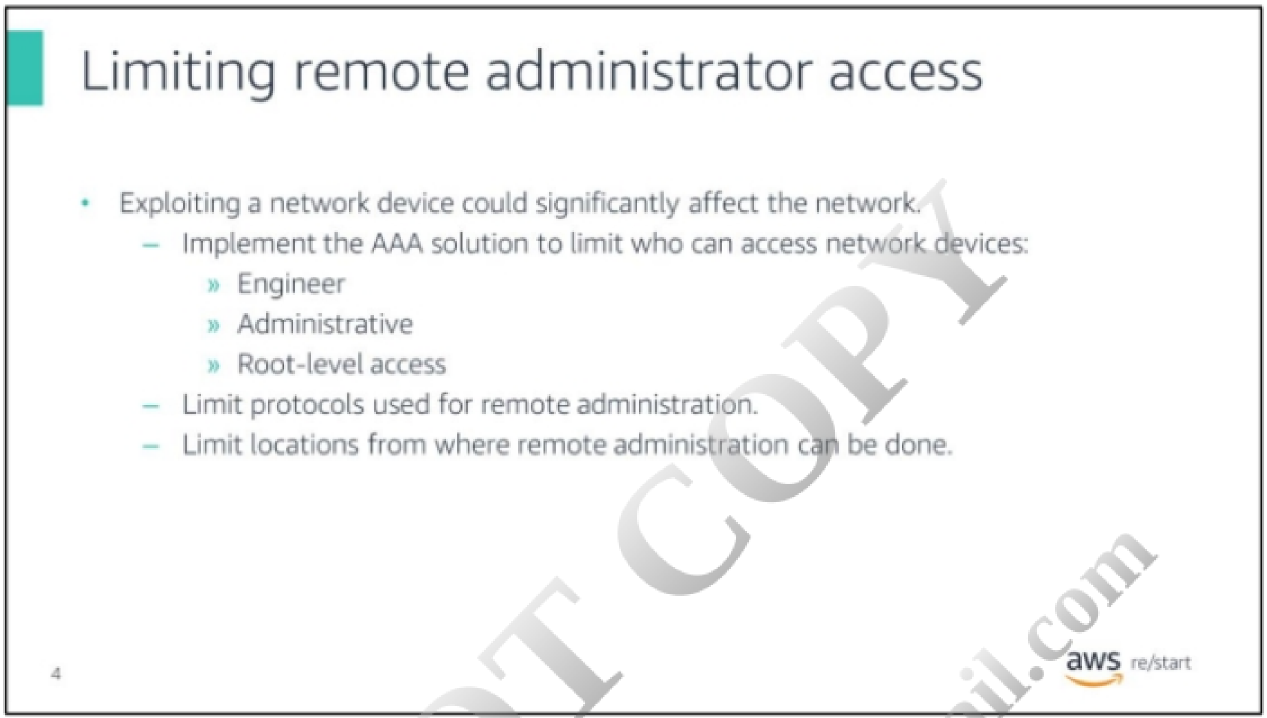
Security lifecycle

- Network Discovery
- Systems Hardening
- Security Architecture
- **Network Hardening**
- Data Security
- Public Key Infrastructure
- Identity Management

As a review, the phases of the security lifecycle consist of:

- **Prevention** – The first line of defense.
- **Detection** – Occurs when prevention fails.
- **Response** – Describes what you do when a security threat is detected.
- **Analysis** – Completes the cycle as you implement new measures to prevent the issue from occurring again in the future.

In this lesson, you will learn *network hardening* techniques that you can use in the Prevention phase.



Limiting remote administrator access

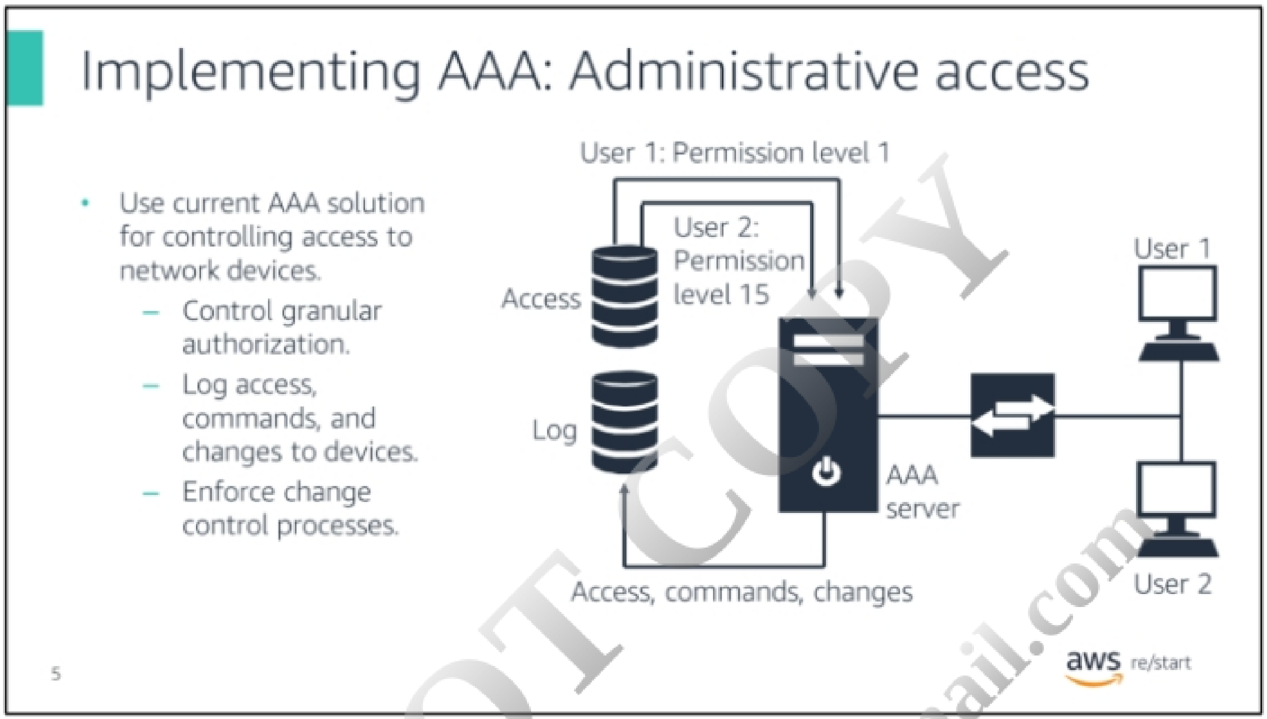
- Exploiting a network device could significantly affect the network.
  - Implement the AAA solution to limit who can access network devices:
    - Engineer
    - Administrative
    - Root-level access
  - Limit protocols used for remote administration.
  - Limit locations from where remote administration can be done.

4

Exploiting or disabling a network device can affect a significant portion of the network. Therefore, you must implement a well-designed authentication, authorization, and accounting (AAA) solution for all engineer, administrative, and root-level access to network devices. This AAA solution is especially necessary for the remote administration of network devices.

Ways to limit access:

- Limit *who* is allowed administrative access.
- Limit *how* the devices are accessed (for example, which protocols can be used).
- Limit *where* the devices are accessed (for example, remote administration from the internet is strictly prohibited).



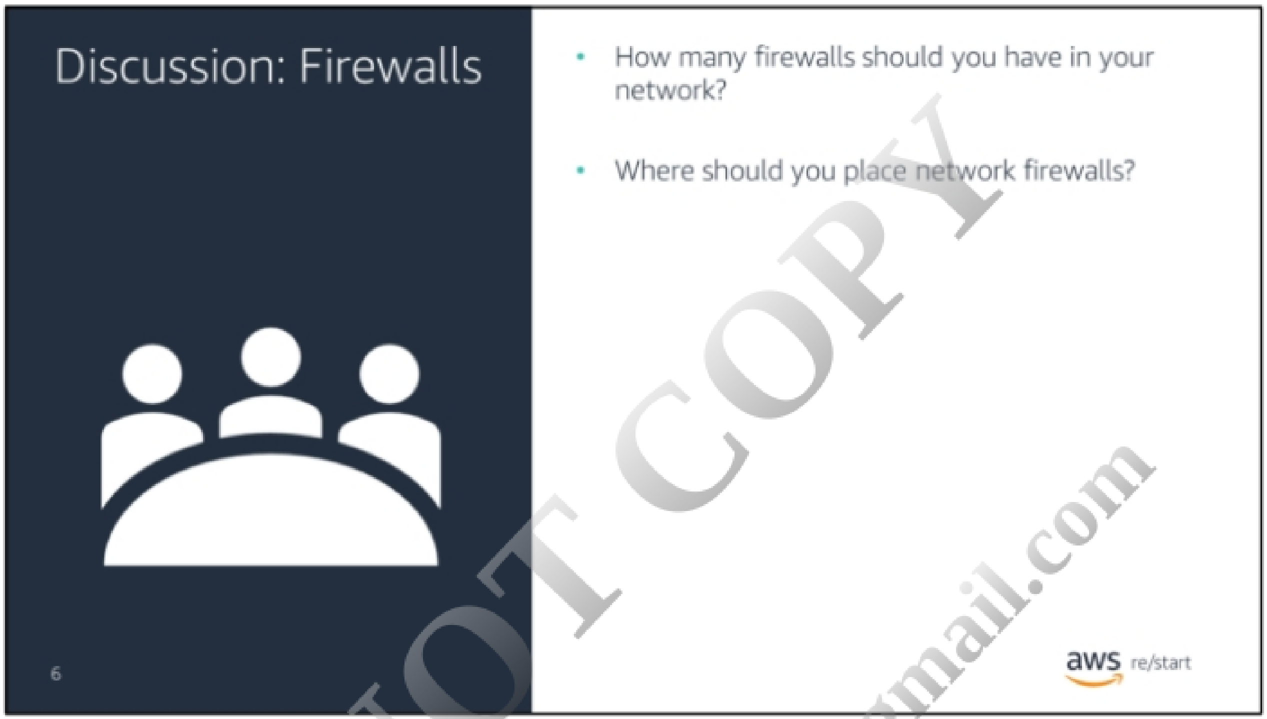
Implementing AAA: Administrative access

- Use current AAA solution for controlling access to network devices.
  - Control granular authorization.
  - Log access, commands, and changes to devices.
  - Enforce change control processes.

User 1: Permission level 1
User 2: Permission level 15
Access
Log
AAA server
User 1
User 2
Access, commands, changes

Use an AAA solution for controlling access to network devices. An AAA solution should do the following:

- Log access, commands, and changes to the network devices.
- Enforce the processes for managing change requests (change control).



Discussion: Firewalls

- How many firewalls should you have in your network?
- Where should you place network firewalls?

6

aws re/start

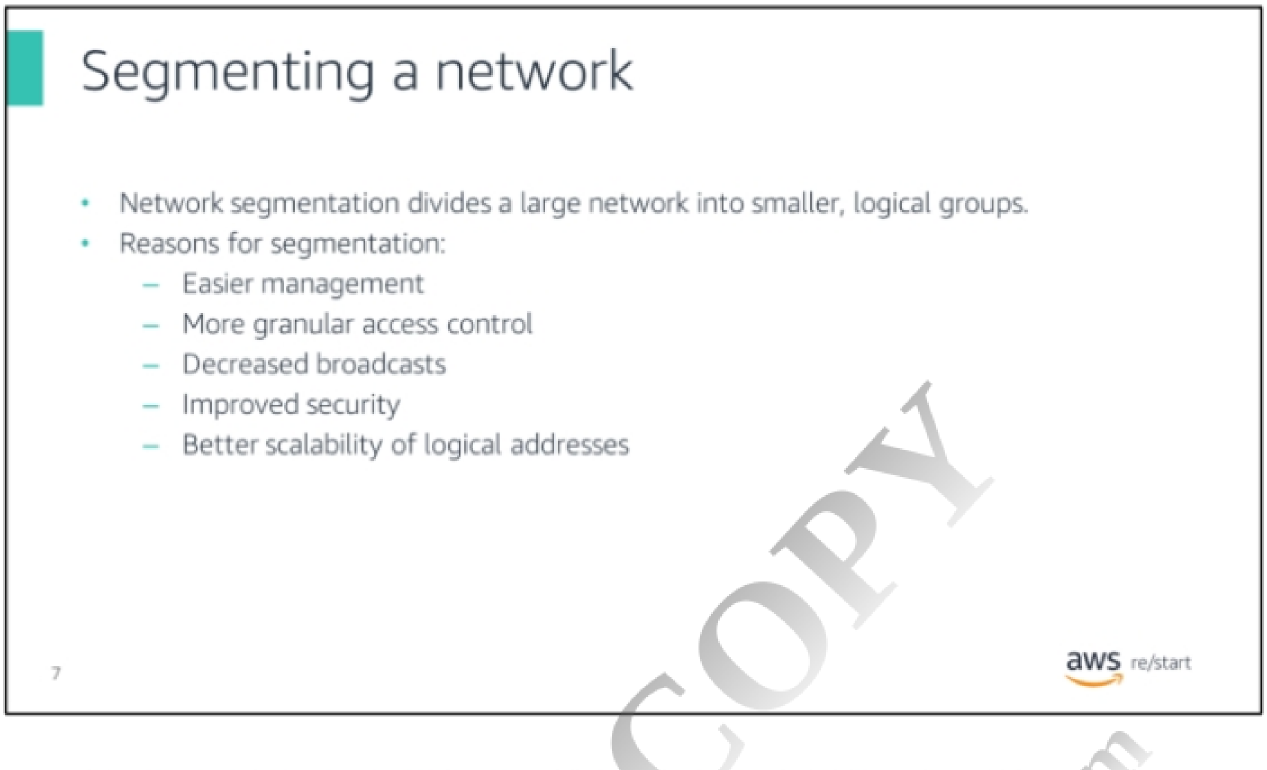
Recall the purpose of a firewall and how you can use firewalls to harden network security.

Try to answer the following questions:

1. How many firewalls should you have in your network?
2. Where should you place network firewalls?

Answers

1. The blanket response is: As many as make sense. More specifically, the answer will depend on your network topology and security requirements. It will be influenced by such factors as the number of devices, type of devices, access requirements, and vulnerability risk.
2. Position firewalls at the junction points of the network as close to the source as possible to identify bad traffic, stop bad traffic, or do both.

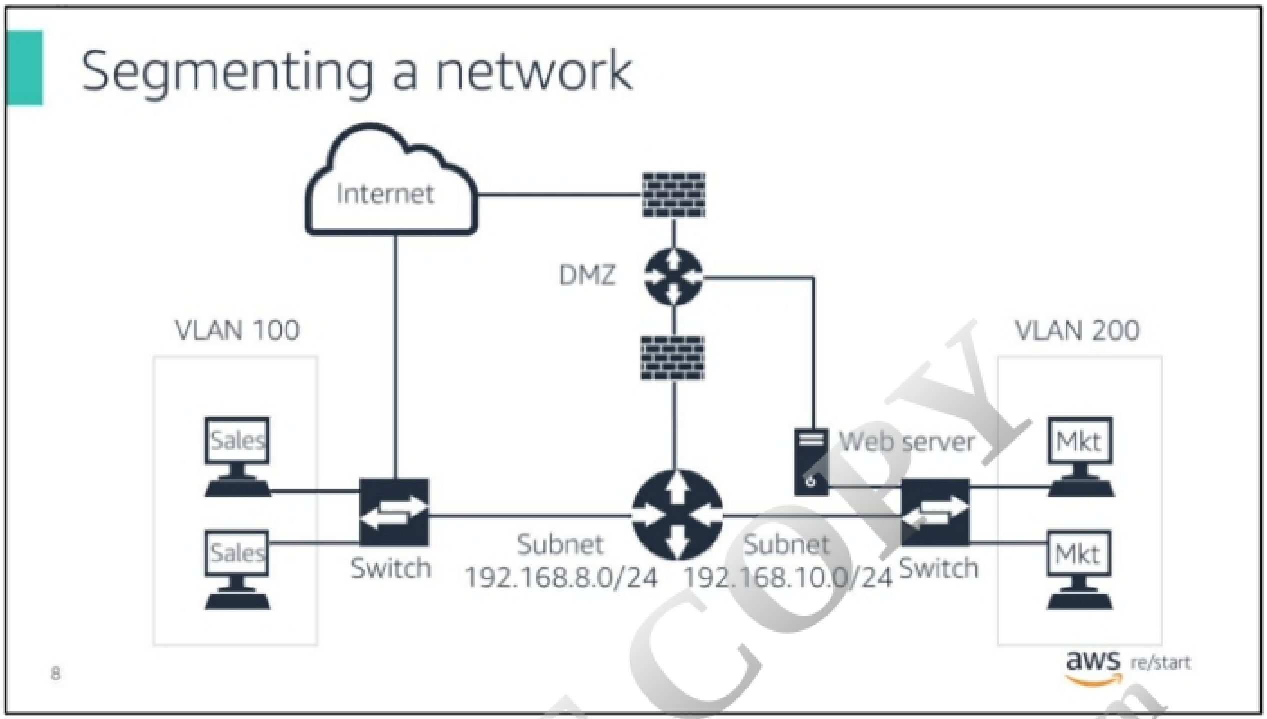


Segmenting a network

- Network segmentation divides a large network into smaller, logical groups.
- Reasons for segmentation:
  - Easier management
  - More granular access control
  - Decreased broadcasts
  - Improved security
  - Better scalability of logical addresses

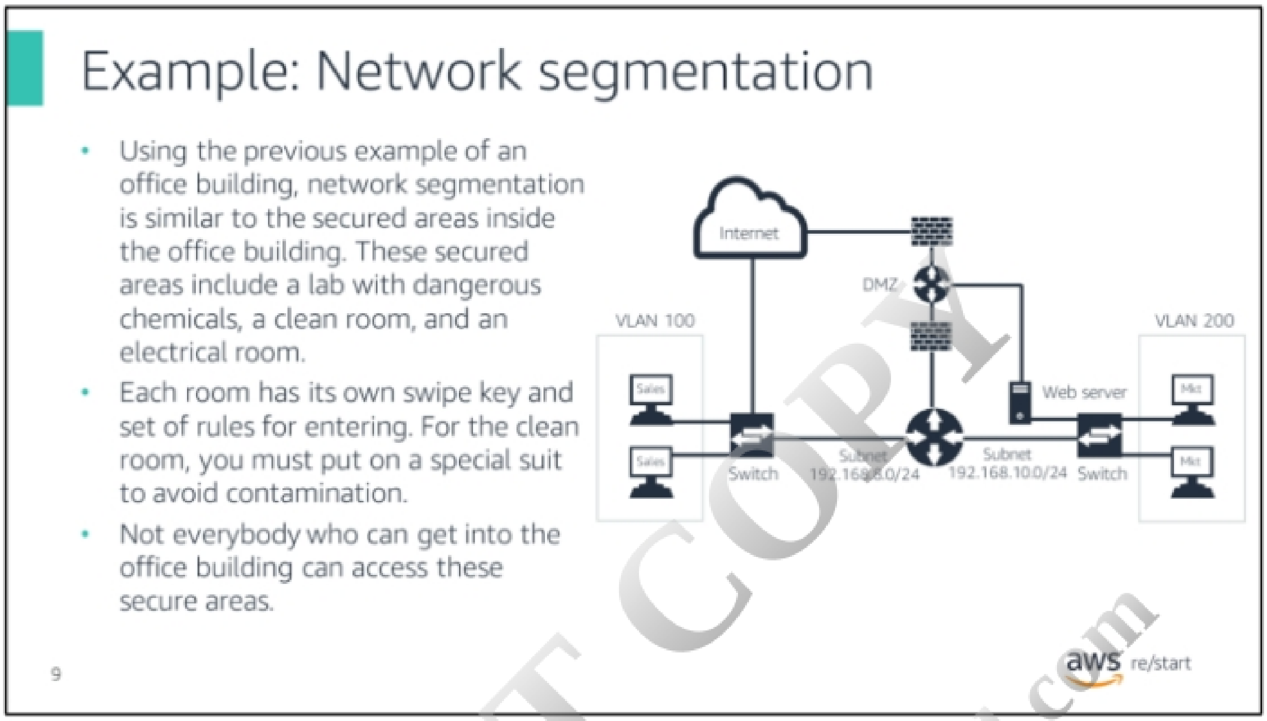
aws re/start

Network segmentation is another technique for enhancing the security of a network. Different resources are hosted on different networks depending on the types of services they provide. The collection of smaller networks results in better security and scalability, and easier management.



Segmenting a network

Network segmentation is another technique for enhancing the security of a network. Different resources are hosted on different networks depending on the types of services they provide. The collection of smaller networks results in better security and scalability, and easier management.

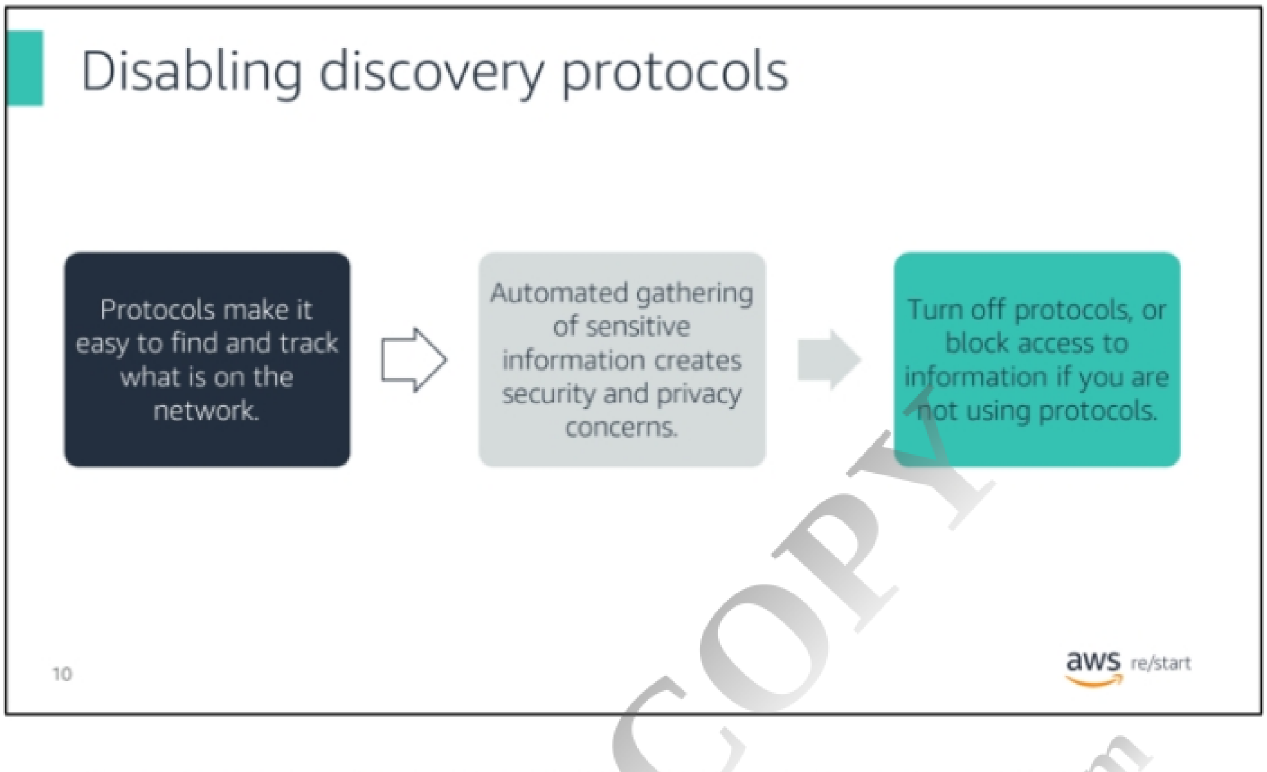


Example: Network segmentation

- Using the previous example of an office building, network segmentation is similar to the secured areas inside the office building. These secured areas include a lab with dangerous chemicals, a clean room, and an electrical room.
- Each room has its own swipe key and set of rules for entering. For the clean room, you must put on a special suit to avoid contamination.
- Not everybody who can get into the office building can access these secure areas.

Using the example of the office building described in an earlier lesson, network segmentation is similar to having secured areas inside the office building. These secured areas include a lab with dangerous chemicals, a clean room, and an electrical room.

Each room has its own swipe key and set of rules for entering. For the clean room, you must put on a special suit to avoid contamination. Not everyone who can get into the office building can access these secure areas.



Disabling discovery protocols

Protocols make it easy to find and track what is on the network.

Automated gathering of sensitive information creates security and privacy concerns.

Turn off protocols, or block access to information if you are not using protocols.

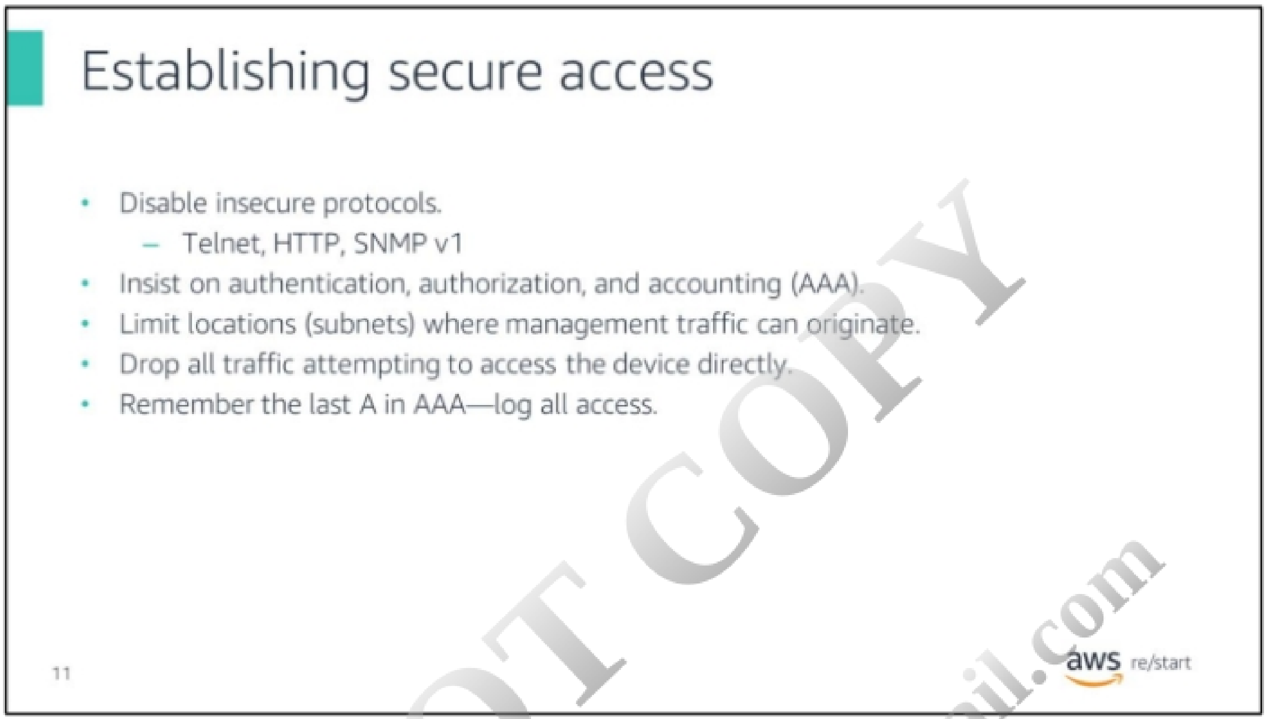
10

Another technique that you can use to harden network security is to disable discovery protocols. This technique is especially useful if the protocols are not closely monitored and controlled.

Disabling discovery protocols prevents outside parties from using those protocols to get crucial information about your network.

Examples of discovery protocols include:

- Cisco Discovery Protocol (CDP)
- Link Layer Discovery Protocol (LLDP)



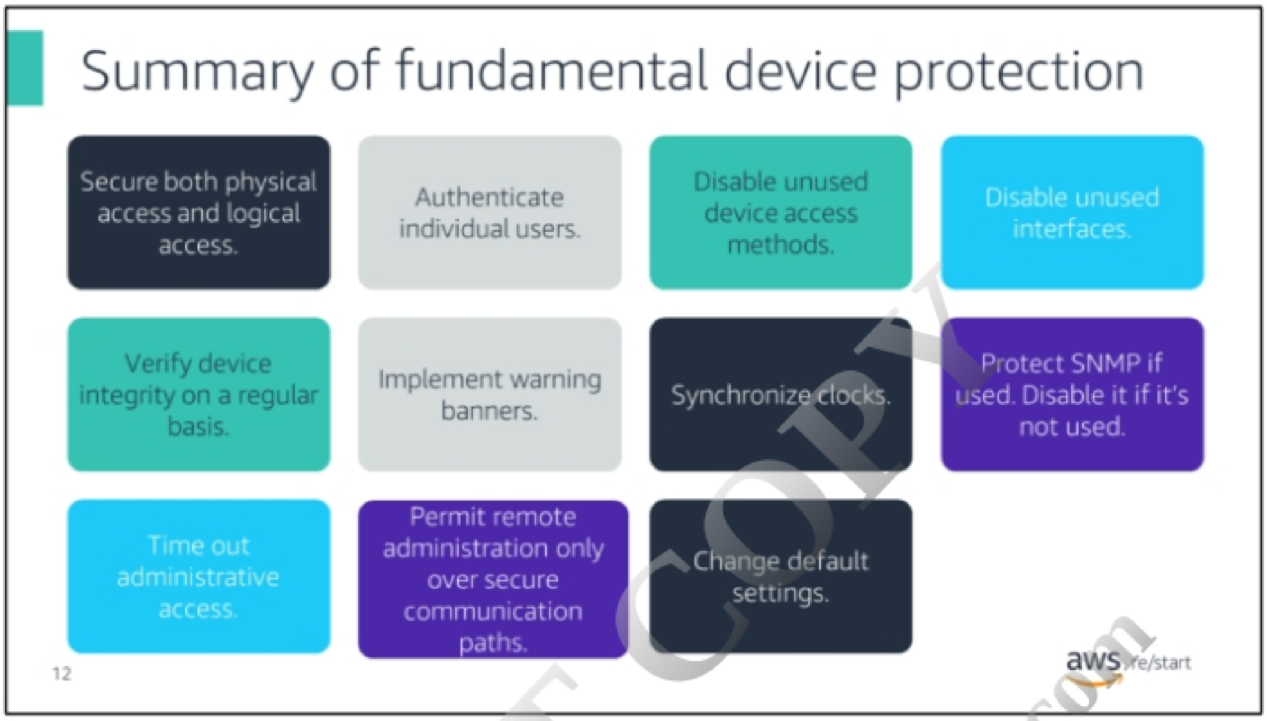
Establishing secure access

- Disable insecure protocols.
  - Telnet, HTTP, SNMP v1
- Insist on authentication, authorization, and accounting (AAA).
- Limit locations (subnets) where management traffic can originate.
- Drop all traffic attempting to access the device directly.
- Remember the last A in AAA—log all access.

This list is an overview of the network hardening techniques described so far.

Acronyms

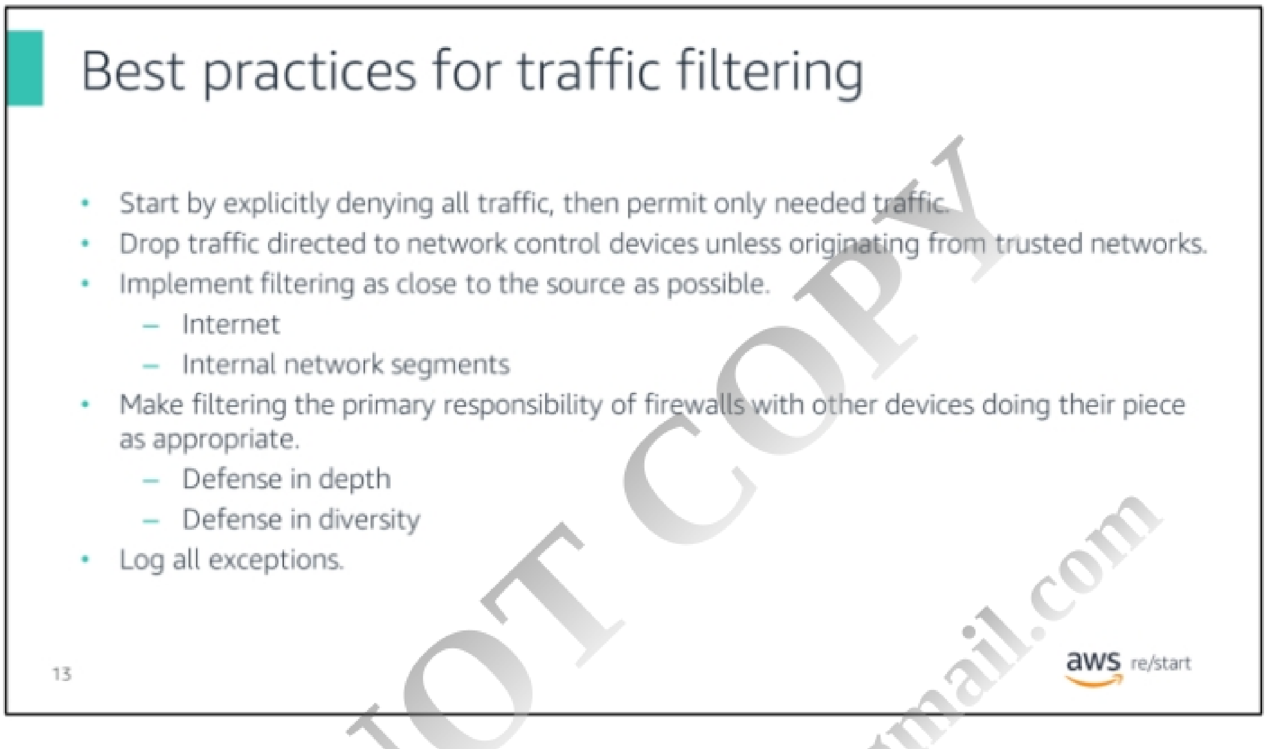
- Simple Network Management Protocol (SNMP)



Summary of fundamental device protection

Secure both physical access and logical access.	Authenticate individual users.	Disable unused device access methods.	Disable unused interfaces.
Verify device integrity on a regular basis.	Implement warning banners.	Synchronize clocks.	Protect SNMP if used. Disable it if it's not used.
Time out administrative access.	Permit remote administration only over secure communication paths.	Change default settings.	

This summary lists measures for fundamental network device protection.



Best practices for traffic filtering

- Start by explicitly denying all traffic, then permit only needed traffic.
- Drop traffic directed to network control devices unless originating from trusted networks.
- Implement filtering as close to the source as possible.
  - Internet
  - Internal network segments
- Make filtering the primary responsibility of firewalls with other devices doing their piece as appropriate.
  - Defense in depth
  - Defense in diversity
- Log all exceptions.

This list shows best practices for network traffic filtering.

Key takeaways

- Network hardening techniques include:
  - Limiting remote administrative access
  - Implementing an authentication, authorization, and accounting (AAA) solution
  - Using firewalls to filter traffic closest to the source
  - Disabling unused or vulnerable protocols
  - Segmenting a network into subnets
- Secure both physical access and logical access to devices.

The following are some key takeaways from this lesson:

- Network hardening techniques include:
  - Limiting remote administrative access
  - Implementing an authentication, authorization, and accounting (AAA) solution
  - Using firewalls to filter traffic closest to the source
  - Disabling unused or vulnerable protocols
  - Segmenting a network into subnets

- Secure both physical access and logical access to devices.