Welcome to Security Lifecycle: Prevention – Security Architecture.

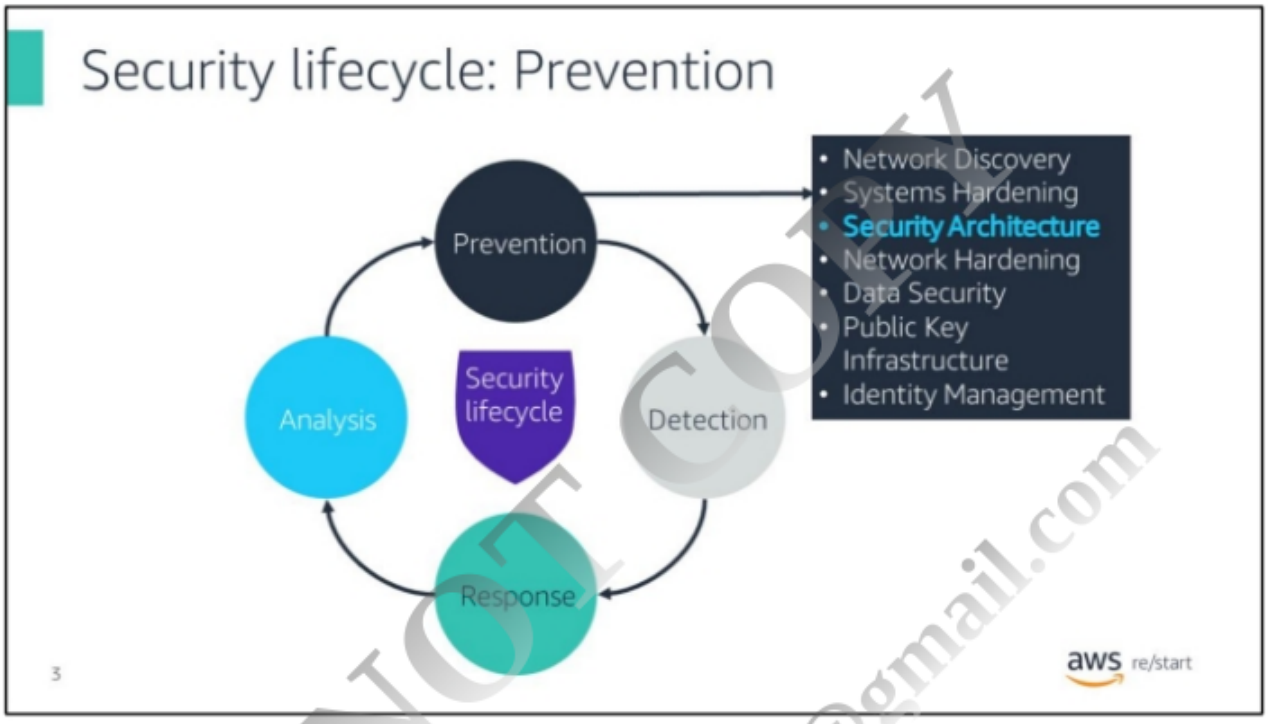
What you will learn

At the core of the lesson

You will learn how to:

- Identify networking devices and their security use
- Describe how network zones work
- Explain the security possibilities at the network level

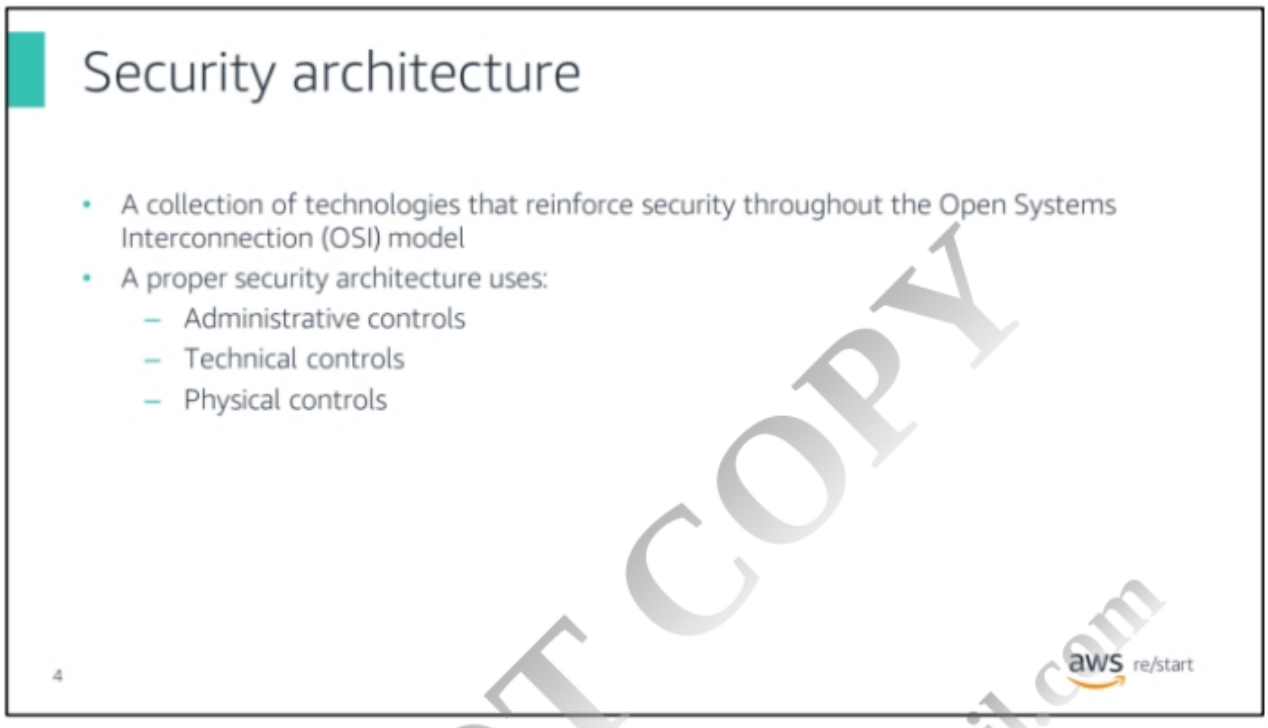
aws re/start



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 upon detection of a security issue.
- **Analysis** – Completes the lifecycle as you implement new preventative measures to prevent the issue from occurring again in the future.

In this lesson, you will learn how *security architecture* decisions help protect your network resources and prevent security threats.

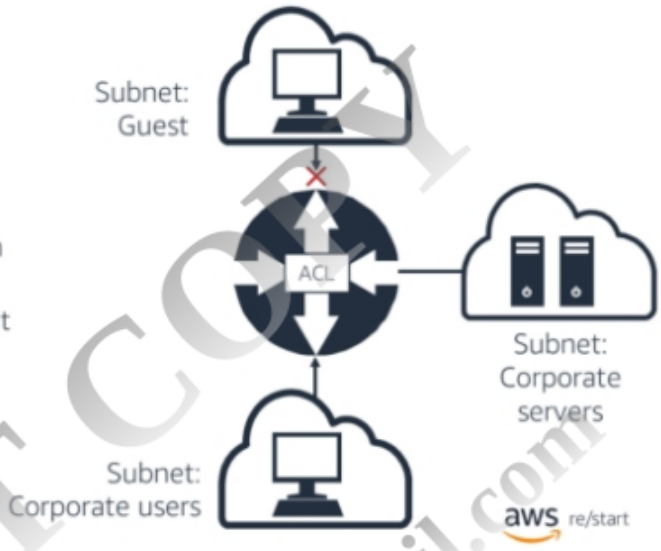


Security architecture refers to a collection of technologies that reinforce security at the network layer. Different solutions accomplish their own parts to keep a network safe so that intrusions are difficult to attempt and traffic flows in the appropriate direction.

The next topics explore tools and techniques that you can use to create a secure network architecture.

Routers

- Routers:
  - Perform basic routing and filtering functions
  - Use access control lists (ACLs) to filter traffic
  - Support network segmentation through subnets
  - Process information quickly, but do not use advanced filtering techniques



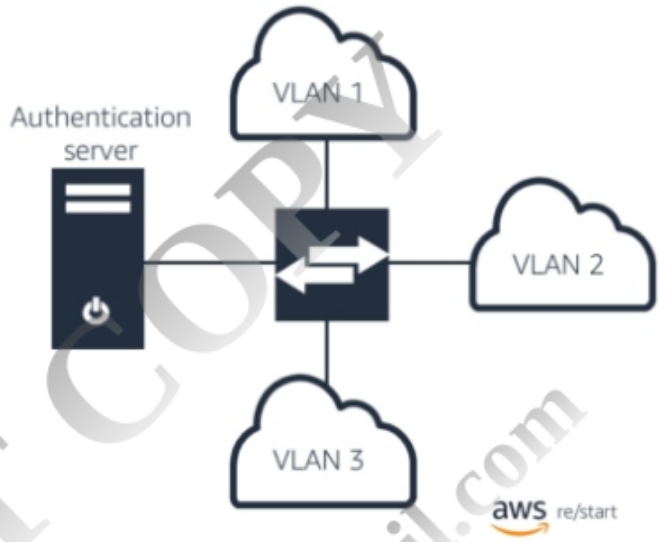
5

To secure a network, use the basic filtering functions of routers. You can use an access control list (ACL) to restrict the traffic allowed in the network. Specifically, an ACL defines rules that grant or deny access to the network.

Subnets are identifiable portions of your network. By segmenting the network into individual subnets, you can design an architecture that isolates part of the network. With this architecture, you can assign the subnets different security access levels.

Switches

- Switches:
  - Segment and control physical access to a network
  - Group computers to create virtual large area networks (VLANs)
  - Support device authentication.
  - Protect against network flooding
- Layer 3 (the network layer) switches perform both routing and switching functions.



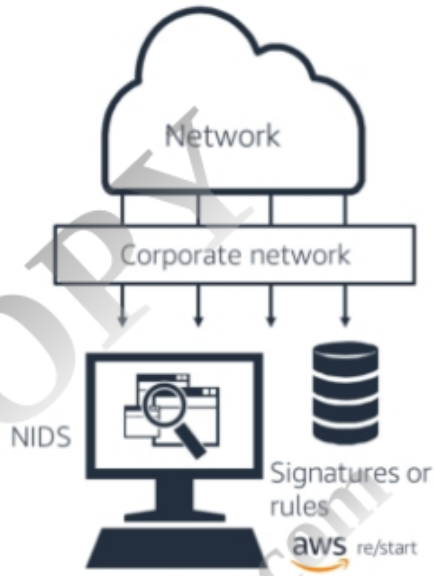
6

aws re/start

Similar to routers, you can use switches to segment a network and create virtual large area networks (VLANs). A VLAN enables devices that are connected to the same physical network to appear as if they are on separate networks. Using this capability, you can design a network architecture that protects different parts of the network based on different access requirements.

Network-based intrusion detection system

- Also known as NIDS
- A NIDS:
  - Monitors network activity
  - Uses signatures and rules to detect malicious patterns
  - Uses a local database to identify live events
  - Must be configured to minimize false alerts.
  - Can be installed as a network appliance or as an application



7

A network-based intrusion detection system (NIDS) scans live network traffic to identify traffic and protocol anomalies and report them. It uses a combination of *signature-based* detection and *behavior-based* detection.

Signature-based detection compares network traffic against a database of known malicious patterns and notifies you when it detects a match. Its weakness is that it is ineffective against unknown events.

For protection against unknown events, you can use *behavior-based* detection, also known as *anomaly-based* detection. This type of detection uses a set of *rules* or a known baseline to detect anomalies or anything that is considered to be outside the norm.

Host-based intrusion detection system

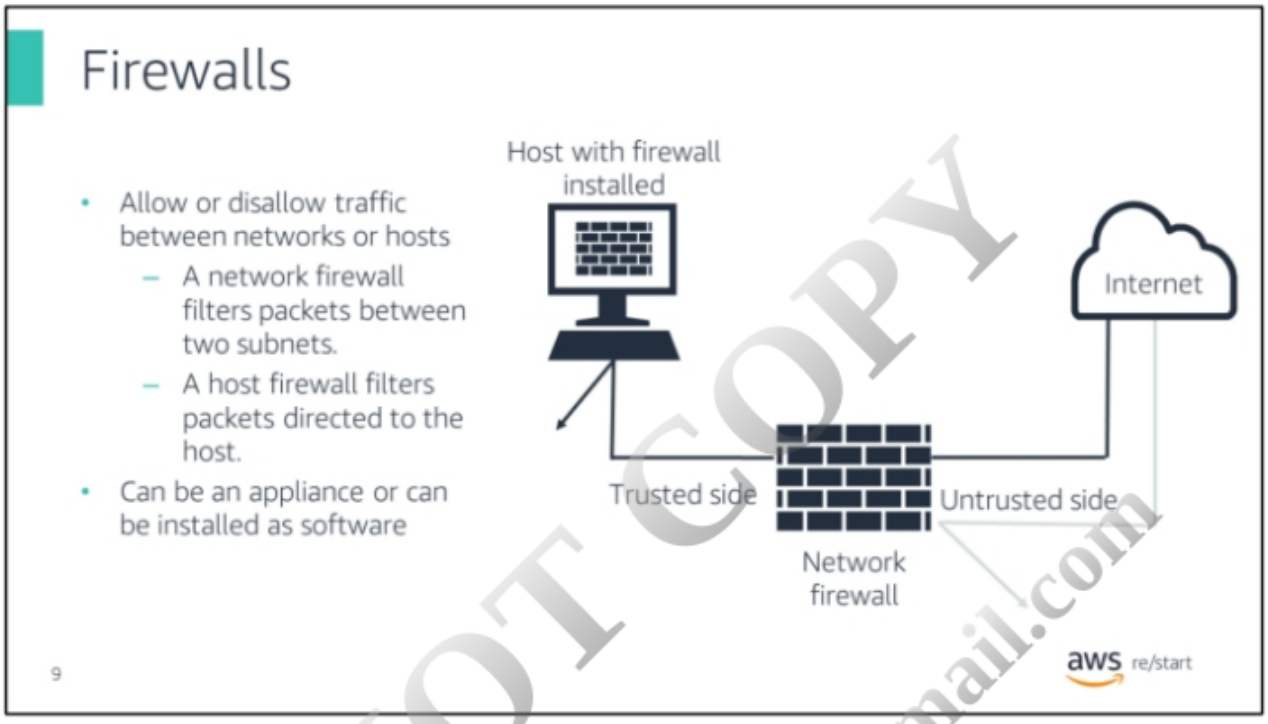
- Protects critical files
- Prevents behavior changes due to corrupt computer state
- Identifies rogue software
- Complements antivirus software

8

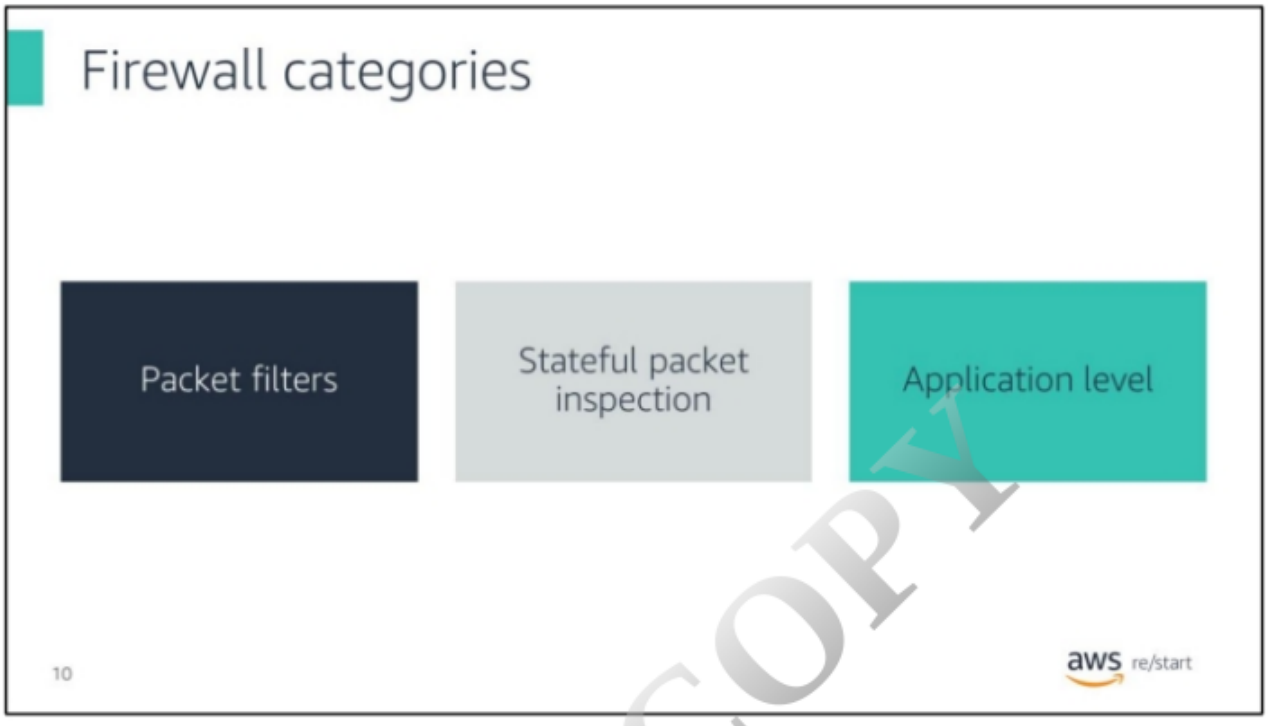
aws re/start

A host-based intrusion detection system complements an antivirus solution. It does this by performing additional scans of critical system files to detect specialized threats, such as:

- Backdoor threat: A vulnerability that allows an attacker to bypass normal security checks and access a system.
- Rootkit threat: A vulnerability that allows an attacker to access a system as a privileged (root) user in an undetected fashion.



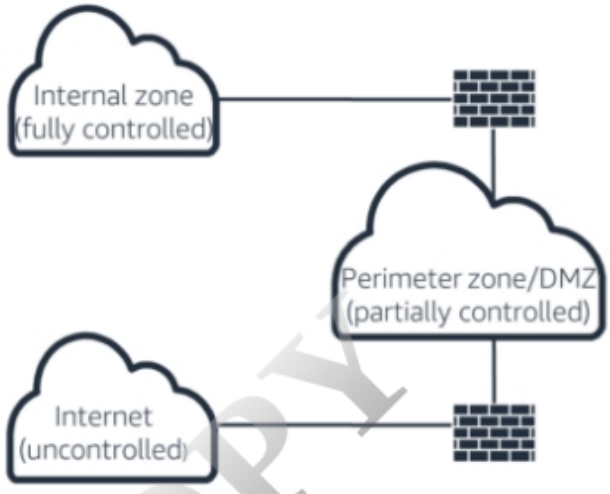
Firewalls are essential elements of a security architecture. They allow you to create rules and exceptions that help control network traffic. Make sure to have them in place at the appropriate locations in your architecture, and make sure that they are enabled.



Different categories of firewalls are shown. Packet filters work faster. By contrast, stateful packet inspection is slowest, but it detects more sophisticated events.

Network zones

- A network zone is a designated area with common security properties. A zone can be:
  - Fully controlled
  - Partially controlled
  - Uncontrolled



11

aws re/start

The *intranet* is an example of a *fully controlled* zone.

A *perimeter zone*, also known as a *demilitarized zone (DMZ)* is an example of a *partially controlled* zone.

The *internet* is an example of an *uncontrolled* zone.

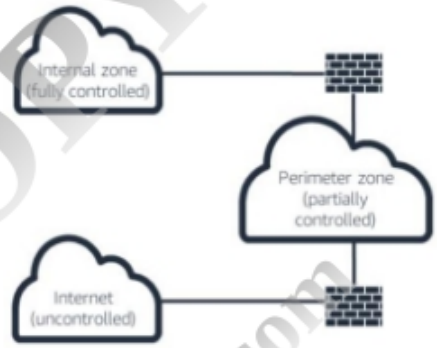
Example: Network zone

Consider an office building. The internet is like the street outside the building. It is public land that is accessible to anyone, and the company inside the building has no control over what happens here.

The perimeter zone is like the parking lot and reception area. The public might have access to some of the resources here. For example, they can park in a visitor parking spot or enter the reception area to use the restroom or drinking fountain.

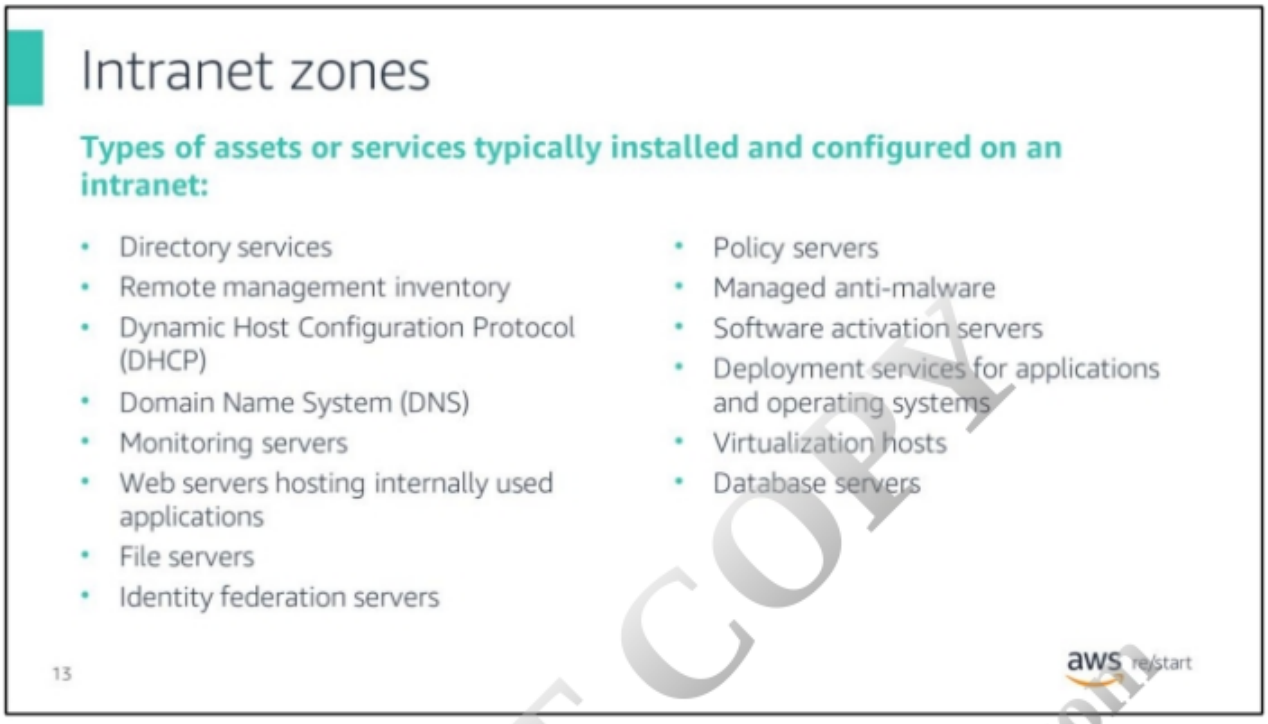
However, a visitor is limited in what they can do, and the business still has authority to remove them from the premises.

The main building past the reception area is the intranet. This space is fully controlled. Only authorized personnel are allowed here. Personnel must have a badge to enter.



12

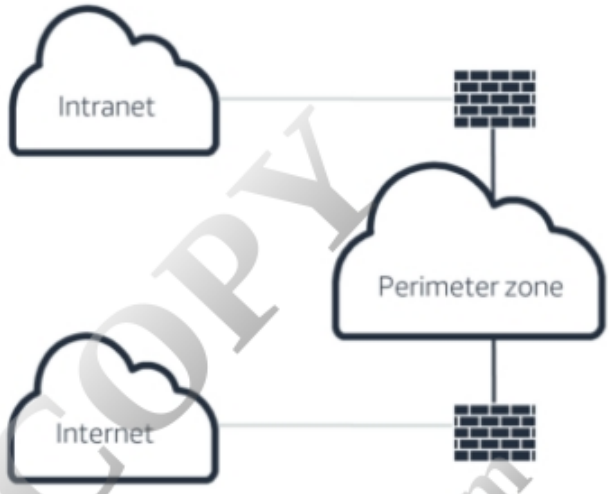
aws re/start



For an organization with on-premises resources (versus cloud), most of your infrastructure is on the intranet side.

Perimeter zone

- A perimeter zone serves as a buffer between two zones with different trust levels.
- Types of configurations for perimeter zones:
  - Back-to-back
  - Three-leg

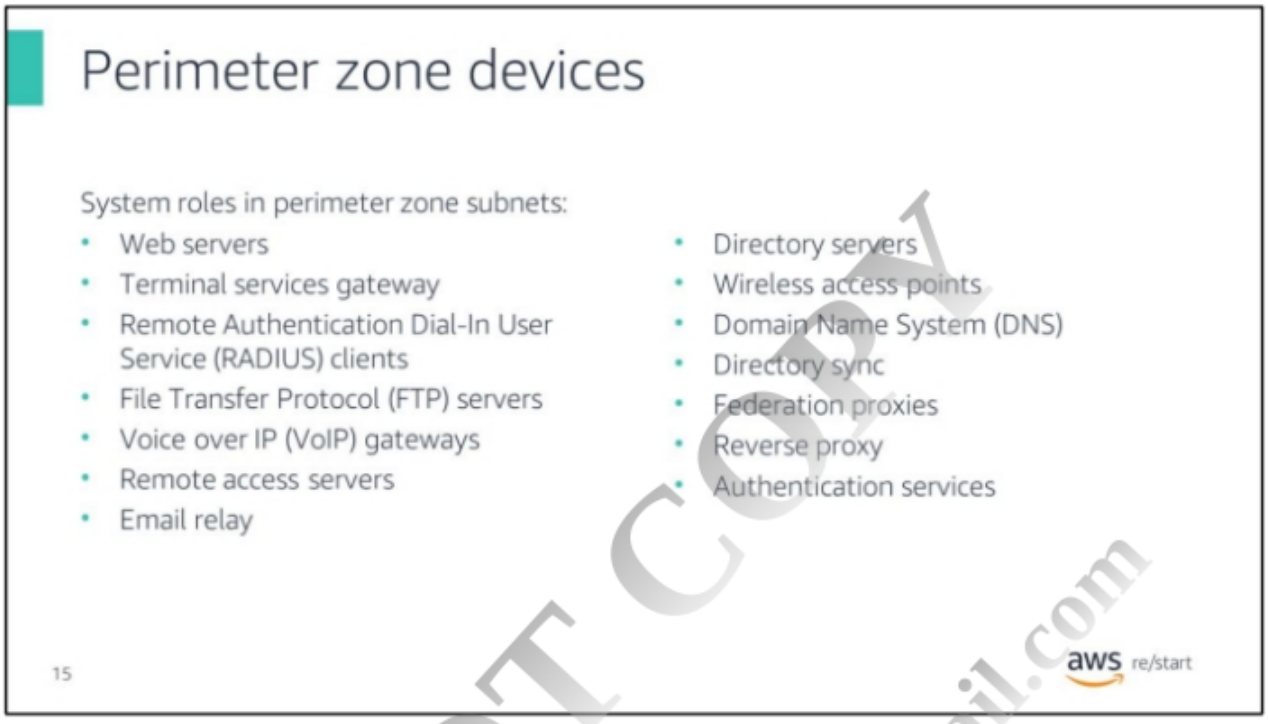


14

aws re/start

Common configuration types for a perimeter zone:

- **Back-to-back** – The perimeter zone is placed between two firewalls. The illustration shows an external firewall and an internal firewall.
- **Three-leg** – The perimeter zone is behind the same firewall that protects the internal network.



This list includes typical devices that are in a perimeter zone.

Network address translation

- NAT translates private addresses to public addresses.
- NAT is primarily performed by a networking device.
- PAT associates multiple private addresses with one public address.
- Several limitations exist with NAT; (not probably used in IPv6).

16

aws re/start

When a network is segmented into public and private subnets, network address translation (NAT) is necessary. NAT internally translates public IP addresses to private IP addresses, and vice versa.

Acronyms:
- Port address translation (PAT)

One of the important elements of a good network security architecture is to provide a network access control list (network ACL) solution. A network ACL system checks for compliance of network resources. The network ACL automatically quarantines noncompliant devices or keeps insecure nodes from infecting the network.

Key takeaways from this lesson include:

- Architectural design affects the security posture of your network and it can be used to prevent threats.
- Use the filtering and access control capabilities of routers and switches to implement network security.
- Firewalls and network segmentation are effective means for protecting a network.