9.5.5 Cloud Security Solutions Facts

Cloud security is a responsibility of the cloud service provider, but ultimately, it’s the IT security professional’s responsibility to ensure that the organization does all it can to keep its data safe.

This lesson covers the following topics:

- Cloud security solutions
- Cloud native controls vs. third-party solutions

Cloud Security Solutions

Be familiar with the following security solutions:

Solution	Description
Cloud access security broker (CASB)	*Cloud access security broker* is an on-premises cloud-based software tool or service that sits between an organization and a cloud service provider. CASBs: ▪ Monitor communication for compliance with an organization's security policies and procedures. ▪ Can offer malware protection and encryption. ▪ Can give more specific protection and monitoring capabilities than secure web gateways (SWGs) and enterprise firewalls.
Application Security	Cloud computing has become the norm for many organizations today. It has become common to add applications and tools to the cloud environment. It’s critical to use security best practices when adding each new application or tool. Each additional has the potential to create a network vulnerability. Application security best practices include: ▪ Verify the application is correctly configured. ▪ Secure APIs and interfaces through encryption and multifactor authentication with limited authorization.
Cloud-based firewalls	A *cloud-based firewall* is a software network device that is deployed in the cloud. It protects against unwanted access to a private network. When making a decision about a cloud-based firewall, consider the following. ▪ Cost ▪ Liability and damage to your cloud applications and services. ▪ The cost of a misconfigured firewall. Misconfiguration includes ports left open and other security holes exposed. ▪ There are cloud-based firewalls available whose fees are based on usage to help lower the cost. The cost of damages and liability may be far higher than the cost of a firewall. ▪ Segmentation ▪ Implement internal segmented firewalls (ISFWs) and access control lists to control access to each segment.

    - Use segmentation to partition networks into trust zones to limit access.
    - Become familiar with networking methods and network segmentation tools provided by your cloud provider to optimize the cloud-based firewall for your organization.
    - Use segmentation tools such as firewall rule sets and load balancers to regulate the IP addresses that can access network segments.
- OSI layers
    - Application layer firewalls work on the Layer 7 of the OSI model. They are considered to be third-generation firewalls.
        - Third generation firewalls work by inspecting inbound and outbound packets and blocking packets that don't meet the rule requirements.
        - The application layer firewall protects the stack of layers below it.
    - Transport layer (Layer 4) firewalls are considered to be stateful firewalls. They are referred to as second-generation firewalls. These firewalls:
        - Log all connections and sort by new connections and existing connections. If traffic is not part of any connection, it's inspected against the firewall rules.
        - Block connections that fail to meet the rule requirements.
    - Network layer firewalls work on Layer 3. They are considered to be first-generation firewalls. First-generation firewalls:
        - Check the network packet's source and destination address, protocol, and destination ports.
        - Protect against packets coming from certain IP addresses.
- Secure Web Gateways
    - SWGs and firewalls both detect malicious traffic. Firewalls work at the packet level, while SWGs work at the application level in the cloud.
    - SWGs are a network security service which filters malware from user-side internet connections. SWGs use URL filtering, application control, data loss prevention, https inspections, and antivirus protection.
    - SWGs are proxies between the organization and the internet. They receive requests from clients before deciding if the session is legitimate.
    - SWGs can monitor and log all on-premises traffic, as well as traffic in public and private clouds. This helps you understand where your vulnerabilities are, which allows you to implement security and use policies intentionally.

Cloud Native Controls vs. Third-party Solutions

There are a few thing to consider in choosing to implement the security controls native to the cloud service provider or to add a third-party security solution to meet your security needs and requirements. To help with this decision:

- List all requirements and check those against what your native controls offer and what the cloud service provider offers.
- Look at how each option can meet your security and compliance requirements.
- Look for third-party solutions for any unmet requirements at the native level.
- Be sure that the third-party options utilize the cloud provider's APIs.