VPC SECURITY CAPABILITIES

"What network security features are available for VPC?"

Overview

Amazon Web Services (AWS) and AWS Partner Network members offer a comprehensive set of security capabilities for securing AWS network infrastructure; however, information on how to do so is dispersed across whitepapers, service documentation, and presentations. This document consolidates this information to provide a high-level overview of the security considerations and capabilities available when designing secure network infrastructure on AWS. It also provides pointers to related Solution Briefs that describe detailed design patterns for controlling network egress traffic and network security monitoring and management.

The following sections assume basic knowledge of Amazon Virtual Private Cloud (Amazon VPC) and network addressing, subnetting, and routing.

General Best Practices

The following universal security principles apply to any computer network security design[1]:

- Understand the available network security capabilities and how they relate to business objectives.
- Understand the required network-traffic patterns and associated threats and risks. For example, organizations typically implement different security controls for protecting traffic entering their network (ingress traffic) versus outbound traffic originating from within their network (egress traffic).
- Implement multiple controls to provide a layered defense-in-depth approach to security.
- Ensure security controls align with application requirements for scalability, availability, and performance.
- Leverage monitoring and management tools to track and validate changes in network traffic, resources, and configurations and to assess the overall effectiveness of network security controls.
- Know the various methods for implementing secure network connections between a VPC and an outside network or another VPC.

Application on the AWS Platform

The AWS platform has extensive network security capabilities. This section gives a brief overview of these capabilities and how AWS customers leverage them to create highly secure infrastructure that incorporates the following design components:

- **Network Security Management and Monitoring:** Efficient management and monitoring is essential for network security. This includes controlling changes to the network infrastructure and monitoring for traffic irregularities or other anomalous behavior. The VPC Network Management and Monitoring Solution Brief contains additional information about how to control changes and monitor your network traffic.
- **Ingress Traffic Control:** Network traffic originating from outside of the VPC often includes a variety of authorized and unauthorized users, especially for publicly facing applications. Network controls used to control inbound traffic need to reduce your application's attack surface, distinguish between legitimate and illegitimate traffic, and allow you to mitigate external threats to your network.
- **Egress Traffic Control:** Network traffic leaving a VPC could be doing so for authorized or unauthorized reasons. Network controls used to control outbound traffic need to be able to distinguish between legitimate and illegitimate traffic and allow you to mitigate external threats like allowing compromised internal servers to communicate with command and control systems or to steal sensitive data. The Controlling VPC Egress Traffic Solution Brief contains additional information about how to control network traffic exiting a VPC.

For additional information about the following service features, see the *Overview of Security Processes* and *AWS Security Best Practices* whitepapers or individual service documentation.

[1] See the *Resources* section for related Solution Briefs that provide detailed guidance on implementing these network design best practices.

Network Traffic Control

Network Address Spoofing

Network MAC addresses are dynamically assigned to Amazon Elastic Compute Cloud (Amazon EC2) instances by the AWS network infrastructure. IP addresses are either dynamically assigned by the AWS network infrastructure or statically assigned by an EC2 administrator through authenticated API requests. The AWS network only allows EC2 instances to send traffic from IP and MAC addresses specifically assigned to them, or the traffic will be dropped.

By default, AWS also protects EC2 instances by treating an instance as a standalone network host, not a router or network gateway, and drops any traffic not specifically addressed to the instance. Customers who need EC2 network appliances to run network address translation, routing, or firewall services can change this default behavior by disabling the Source/Destination Check attribute and configuring VPC route tables to send outbound traffic through the network appliance.

Packet Sniffing

It is not possible for a virtual instance running in promiscuous mode to receive or *sniff* traffic that is intended for a different virtual instance. While customers can elect to place their interfaces into promiscuous mode, the hypervisor will not deliver any traffic to an instance that is not addressed to it. Even two virtual instances that are owned by the same customer located on the same physical host cannot listen to each other's traffic. Additionally, attacks such as ARP cache poisoning do not work within Amazon EC2 and Amazon VPC. While Amazon EC2 does provide ample data protection between customers by default, as a standard practice it is best to always encrypt sensitive traffic.

Subnets and Network Routing

Amazon VPC allows customers to create virtual networks and divide them into subnets. VPC subnets are mapped to specific Availability Zones (AZs) and, therefore, subnet placement is one mechanism to ensure EC2 instances are properly distributed across multiple locations. AWS automatically routes network traffic between a VPC's subnets and allows customers to specify outbound routes on a subnet-by-subnet basis. The following sections describe how to control traffic between subnets with security groups and network ACLs, and between a VPC and external networks with routing rules and in-line network appliances (if desired) in addition to security groups and network ACLs.

Network Routing Control

Customers can create routing rules to control which VPC subnets are able to communicate directly with external networks, whether these external networks are other VPCs, private customer networks, or the Internet. VPC route tables allow customers to configure which subnets are allowed to route external traffic over backend VPN or Direct Connect connections, VPC peering connections, Internet connections, or even specific EC2 instances. Therefore, customers can leverage multiple subnets to create hierarchical routing rules where Internet-facing, public subnets control traffic to private subnets that may or may not have the ability to route traffic over VPN, Direct Connect, or VPC peering connections.

Network ACL

A network access control list (ACL) is an optional layer of security that provides a stateless firewall for controlling traffic in and out of a subnet. Network ACLs support up to 20 IP CIDR-based allow or deny rules for both inbound and outbound traffic. AWS customers typically leverage security groups as their primary method of network packet filtering since they are more versatile than network ACLs due to their ability to perform stateful packet filtering and utilize rules that reference other security groups. However, network ACLs can be effective as a secondary control for denying a specific subset of traffic or providing high-level guard rails for a subnet. By implementing both network ACLs and security groups as a defense-in-depth means of controlling traffic, a mistake in the configuration of one of these controls will not expose the host to unwanted traffic

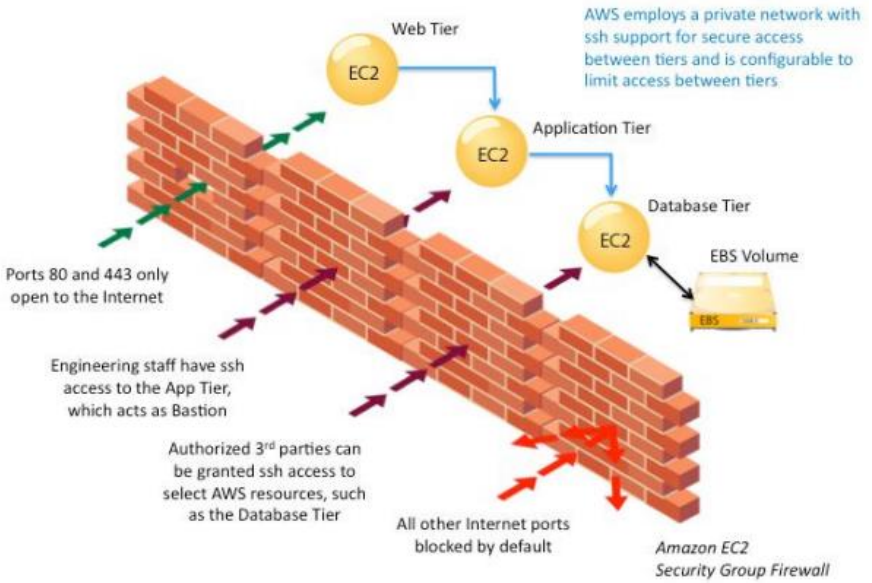
Network Firewall Options

Security Groups

A security group acts as a virtual stateful firewall that controls the traffic for one or more instances. This mandatory firewall is configured in a default deny-all mode and customers must explicitly open the ports needed to allow inbound traffic. Traffic can be restricted by protocol, by service port, and also by source IP address (individual IP or CIDR block) or security group.

Security groups can be configured to set different rules for different classes of instances. Consider, for example, the case of a traditional three-tiered web application. The group for the web servers would have port 80 (HTTP) and/or port 443 (HTTPS) open to the Internet. The group for the application servers would have port 8000 (application specific) accessible only to the web server group. The group for the database servers would have port 3306 (MySQL) open only to the application server group. All three groups would permit administrative access on port 22 (SSH), but only from the customer's corporate network. This mechanism enables the deployment of highly secure applications.

Although enforced at the hypervisor, security groups have capabilities similar to traditional network firewall appliances, such as stateful packet inspection, centralized configuration, and out-of-band rule administration independent from guest OS configuration. Security groups operate not only between subnets but also on each instance interface, providing interface-level network rule granularity as opposed to the subnet-level granularity of traditional network firewall appliances.



Firewall Logging

VPC Flow Logs capture network flow information for a VPC, subnet, or network interface and stores it in Amazon CloudWatch Logs. Flow log data can help customers troubleshoot network issues; for example, to diagnose why specific traffic is not reaching an instance, which might be a result of overly restrictive security group rules. Customers can also use flow logs as a security tool to monitor the traffic that reaches their instances, to profile network traffic, and to look for abnormal traffic behaviors.

AWS WAF

AWS WAF is a web application firewall that helps protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. Using AWS WAF, customers can define customizable web security rules that control which traffic accesses their web applications. Web security rules that target specific application request patterns can be very effective for minimizing the effect of application-level attacks. For example, VPC security groups can be used to limit permitted traffic to a webserver to port 80 or 443; and the AWS WAF can be configured to inspect the traffic that is permitted to reach port 80 or 443.

Host-Based Firewall

In addition to security groups at the hypervisor level, customers can also enable operating system firewalls. These include built-in OS capabilities such as *iptables* and Windows Firewall, or third-party software that provides additional functionality such as deep packet inspection, IPS/IDS, or network threat protection. Host-based security software works well with highly distributed and scalable application architectures because network packet inspection is distributed across the entire software fleet.

In-Line Firewall

Multiple AWS Partner Network members offer virtual firewall appliances that can be deployed as an in-line gateway for inbound or outbound network traffic. Firewall appliances provide additional application-level filtering, deep packet inspection, IPS/IDS, and network threat protection features. Note that due to the in-line nature of this option, the firewall/gateway can become a throughput bottleneck or single point of failure. Therefore, customers must take extra care when selecting this approach over host-based options to ensure that an in-line network appliance is architected and engineered to be highly available and scalable.

DDoS Attack Mitigation

AWS provides several capabilities to help customers mitigate network-based denial of service threats. These include providing global DNS and content delivery network services with high-bandwidth network connectivity, as well as web application firewall and load balancing services. Please see the Denial of Service Attack Mitigation on AWS Solution Brief for additional information about these capabilities.

Resources

AWS Security Best Practices	https://d0.awsstatic.com/whitepapers/aws-security-best-practices.pdf
Amazon Web Services: Overview of Security Processes	https://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf
VPC Network Management and Monitoring	https://d0.awsstatic.com/aws-answers/VPC_Network_Management_and_Monitoring.pdf AWS Solution Brief on network security management and monitoring tools
Controlling VPC Egress Traffic	https://d0.awsstatic.com/aws-answers/Controlling_VPC_Egress_Traffic.pdf AWS Solution Brief on approaches to control network traffic out of a VPC
Single Data Center HA Network Connectivity	https://d0.awsstatic.com/aws-answers/AWS_Single_Data_Center_HA_Network_Connectivity.pdf AWS Solution Brief describing options for creating highly available connections from a single data center to AWS
Multiple Data Center HA Network Connectivity	https://d0.awsstatic.com/aws-answers/AWS_Multiple_Data_Center_HA_Network_Connectivity.pdf AWS Solution Brief describing options for creating highly available connections from multiple data centers to AWS
Multiple-VPC VPN Connection Sharing	https://d0.awsstatic.com/aws-answers/AWS_Multiple_VPC_VPN_Connection_Sharing.pdf AWS Solution Brief on leveraging a single VPN connection across multiple VPCs
Single Region Multi-VPC Connectivity	https://d0.awsstatic.com/aws-answers/AWS_Single_Region_Multi_VPC_Connectivity.pdf AWS Solution Brief on connecting VPCs within a single region
Denial of Service Attack Mitigation on AWS	https://d0.awsstatic.com/aws-answers/AWS_DDoS_Attack_Mitigation.pdf AWS Solution Brief of services and features to help mitigate DDoS attacks