ASU Lab : Security Configuration

Spurthy Mutturaj

Information Technology, Arizona State University

IFT 562: Cloud Security & Operations for IT

Daniel Wells

Nov 12, 2023

Table of Contents

ASU Lab : Security Configuration

AWS Network Firewall:

Position in the Diagram

AWS Network Firewall can be placed at the perimeter of the VPC, between the public and private subnets, acting as a managed firewall service for filtering traffic. Here is how the network traffic would flow: Internet gateway → AWS Network Firewall → Application Load Balancer.

Key Considerations:

- Define Clear Security Objectives: Clearly articulate security goals for AWS Network Firewall, specifying the desired control over inbound and outbound traffic. Identify and prioritize the types of threats or traffic to be allowed or denied.
- Organize Rules into Groups: Structure rules into groups based on specific applications or services, facilitating efficient management. Consider the context of rule groups to tailor security measures according to distinct needs.
- Regularly Update Rules:Establish a routine for monitoring and updating firewall rules to dynamically respond to changing security requirements. Regular updates ensure the adaptability of the AWS Network Firewall to evolving threats and application needs.
- Integrate with AWS Services: Seamlessly integrate AWS Network Firewall with services such as CloudWatch and Security Hub to enable robust monitoring, logging, and compliance checks. This integration enhances the overall security posture and responsiveness of the environment.

Example CLI Commands:

- Create Firewall Policy:

aws network-firewall create-firewall-policy --firewall-policy-name MyFirewallPolicy

- Create Rule Group:

  aws network-firewall create-rule-group --rule-group-name MyRuleGroup --rule-file file://my-rule-file.json

- Create Firewall:

  aws network-firewall create-firewall --firewall-name MyFirewall --firewall-policy-arn arn:aws:network-firewall:region:account-id:firewall-policy/MyFirewallPolicy

- Associate Rule Group with Firewall Policy:

  aws network-firewall associate-firewall-policy --firewall-policy-arn arn:aws:network-firewall:region:account-id:firewall-policy/MyFirewallPolicy --rule-group-arn arn:aws:network-firewall:region:account-id:rule-group/MyRuleGroup

- Create Firewall Status:

  aws network-firewall create-firewall --firewall-name MyFirewall --firewall-policy-arn arn:aws:network-firewall:region:account-id:firewall-policy/MyFirewallPolicy

- Update Route Tables:

  Update the route tables associated with your subnets to direct traffic through the newly created firewall.

AWS Security Groups:

Position in the Diagram:

AWS Security Groups act at the instance level, providing a virtual firewall for controlling inbound and outbound traffic to instances within a VPC. Each instance in the architecture diagram should be associated with one or more security groups.

Key Considerations:

- Define Security Groups for Each Instance Type:

  Tailor security groups based on the role or function of instances. For example, create separate security groups for Bastion, Frontend, and Backend instances, each with rules specific to their needs. This segmentation enhances security and adheres to the principle of least privilege.

- Regularly Review and Update Rules:

  Security requirements evolve. Regularly review and update security group rules to align with changing application needs or security policies. This ensures that access permissions remain accurate and appropriate over time.

Example CLI Commands:

- Create a security group

  aws ec2 create-security-group --group-name MySecurityGroup --description "My security group" --vpc-id vpc-0123456789abcdef0

- Authorize inbound traffic

  aws ec2 authorize-security-group-ingress --group-id sg-0123456789abcdef0 --protocol tcp --port 22 --cidr 0.0.0.0/0

Authorizes inbound traffic to the security group, allowing SSH access (port 22) from any IP address (0.0.0.0/0). Adjust parameters based on your specific requirements.

AWS GuardDuty:

Position in the Diagram:

GuardDuty operates at the AWS account level, analyzing VPC flow logs, CloudTrail event logs, and DNS logs. It doesn't have a specific placement in the diagram but rather spans across the entire AWS environment, monitoring activities at the account level.

Key Considerations:

- Enable GuardDuty: In the AWS Management Console, navigate to GuardDuty and enable it for the AWS account. Configure threat intelligence feeds and set up CloudWatch event rules to automate responses to findings.
- Relevant Data Sources: GuardDuty relies on VPC flow logs, CloudTrail event logs, and DNS logs for threat detection. Ensure these logs are enabled and properly configured in your AWS environment.
- Regular Review of Findings: Regularly review GuardDuty findings in the console or through API calls. Set up CloudWatch Alarms to receive notifications for high-priority findings.
- Automated Responses: Integrate GuardDuty with AWS Lambda to automate responses to specific findings, such as isolating compromised instances or updating security groups.

Example CLI Commands:

- Enable GuardDuty in your AWS account

  aws guardduty create-detector --enable
- List detectors in the account

  aws guardduty list-detectors

- Get findings for a detector

  aws guardduty list-findings --detector-id <detector-id>

GuardDuty, operating at the account level, enhances security by continuously monitoring for malicious activity, unauthorized access, or potential threats across the entire AWS environment. By analyzing VPC flow logs, CloudTrail events, and DNS logs, GuardDuty provides a comprehensive view of potential security issues. Regular reviews of GuardDuty findings empower ASU Inc. to respond promptly to security threats, reducing the risk of unauthorized access or data breaches. The implementation of automated responses using CloudWatch Alarms and AWS Lambda ensures a proactive approach to security incidents, minimizing manual intervention and response time.

Summary

- The combination of AWS Network Firewall, Security Groups, and GuardDuty provides a robust security infrastructure for ASU Inc.'s AWS environment.
- Network Firewall ensures controlled and monitored traffic flow between the public and private subnets.
- Security Groups add an additional layer of security at the instance level, tailored to the specific needs of each type of instance.
- GuardDuty continuously monitors the entire AWS account for potential threats, enhancing overall security posture by providing real-time threat detection and automated response capabilities.

References

Amazon Web Services. (2022). Getting Started with AWS. https://aws.amazon.com/