ManageEngine
Log360

Attack proofing your AWS

www.manageengine.com/log360

Introduction

With the adoption of the cloud increasing each year, securing resources on cloud platforms from attacks is something security admins deal with each day. Because many organizations have some or all of their business-critical applications on the cloud, attacks are becoming more common. One of the biggest data breaches in 2019 happened on the Amazon Web Services (AWS) platform. The attacker was able to exploit a misconfigured web application firewall to access the Social Security numbers, credit scores, and credit card transaction data of more than 100 million customers. This data breach is estimated to have cost Capital One over $300 million in damages.

As the Capital One data breach has shown, a misconfiguration of AWS settings could prove disastrous for any organization. In the shared model of responsibility adopted by AWS, security is jointly handled by the customer and AWS. AWS takes responsibility for the security in the cloud such as storage, databases, and the infrastructure. Security of the cloud, which includes IAM, network, and firewall configurations fall under the responsibility of the customer. This underlines the fact that cloud is only as secure as it is configured.

This e-book provides an overview of the configurations and best practices that can help you defend against attacks, and also offers a few key tips on eliminating security loopholes.

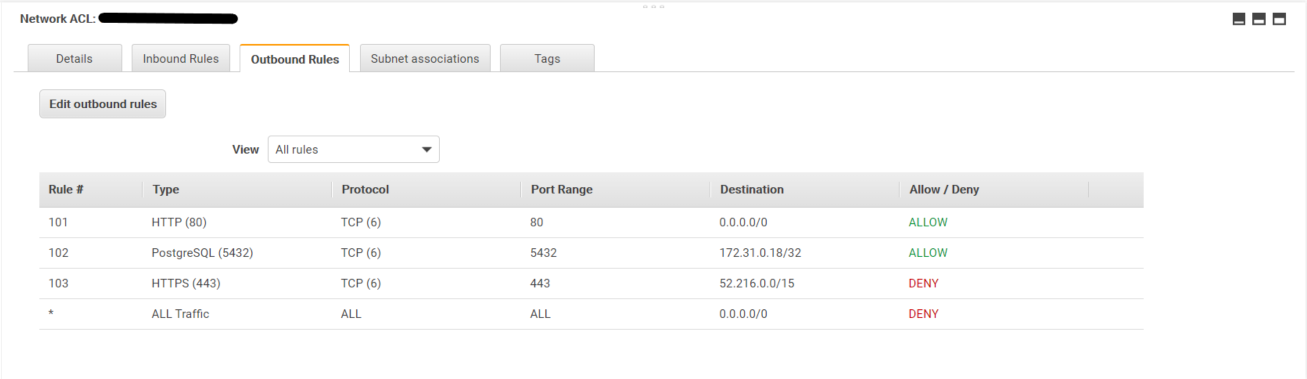
The security architecture of AWS

Understanding the security architecture of AWS is essential for effectively deploying the tools AWS offers to secure the virtual network integrating your on-premises and AWS resources.

Network access control lists

Network access control lists (NACLs) help regulate traffic in and out of each subnet. Having an NACL with a set of granular rules ensures only the authorized traffic flows between subnets. NACLs operate with a list of numbered rules. By default, all custom NACLs deny inbound and outbound traffic. You can add specific rules to allow only the required traffic in and out of the subnet.

The image below shows an example of how configured rules work in NACLs.



Network ACL: [redacted]

View: All rules

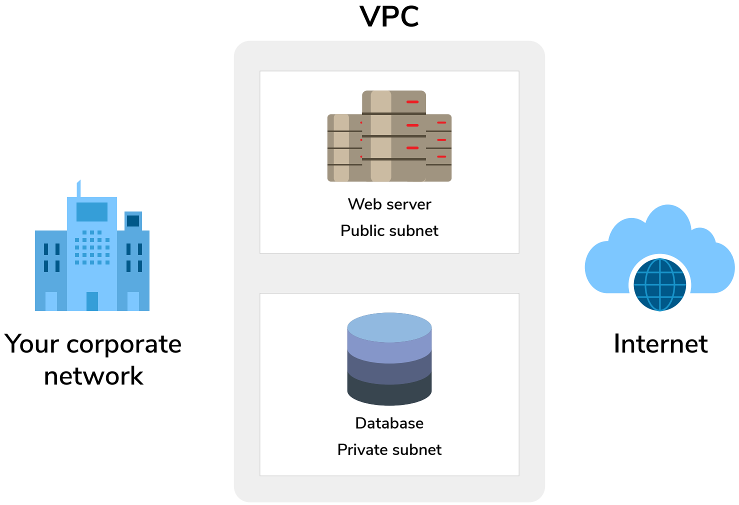
Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
101	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
102	PostgreSQL (5432)	TCP (6)	5432	172.31.0.18/32	ALLOW
103	HTTPS (443)	TCP (6)	443	52.216.0.0/15	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

The last rule states that all outbound traffic is denied except for the traffic defined by the rules above. This rule will be present by default when you create an NACL. Rule 103 states that HTTPS traffic is specifically denied for the IPs that fall within the range; 52.216.0.0/15. Rule 102 states that, the port 5432 used to access PostgreSQL is allowed for the IPs falling within the 172.31.0.10/32 range. Similarly, rule 101 states that HTTP access using port 80 is allowed for any IP.

Virtual private cloud and subnets

A virtual private cloud (VPC) protects your Amazon Elastic Cloud Compute (EC2) instances from direct access via the internet. With the VPC, you can set rules to restrict the traffic flowing in and out of your virtual network. By default, when a VPC is first created for your account, it is includes a public subnet which allows inbound and outbound traffic.

It is advisable to change this, and create a public and a private subnet within your VPC. For instance, you would want the web server to be accessible to the internet, but not the databases. One way to achieve this is to place the web server in a public subnet, and the databases in a private subnet within your VPC.

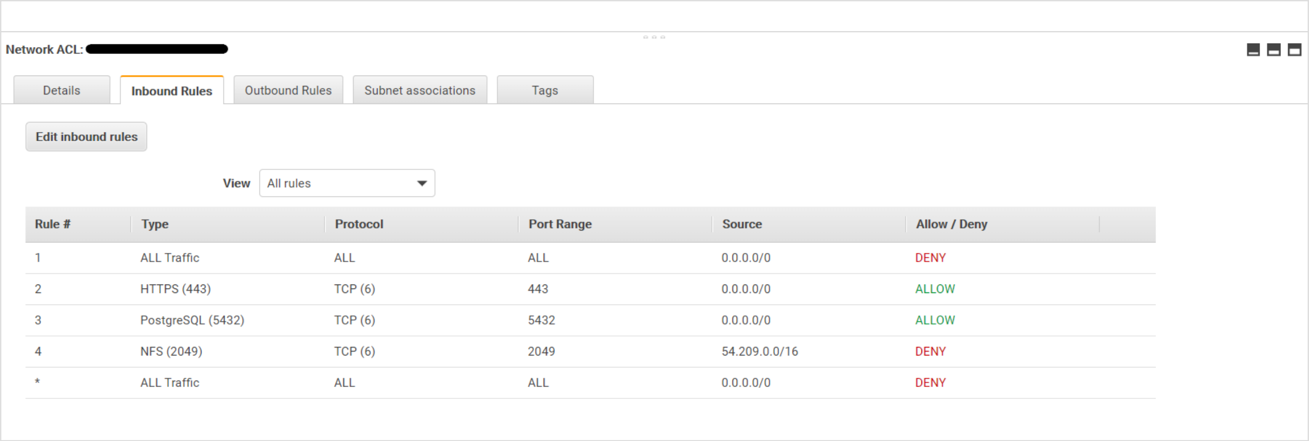


This way, a VPC also enables you to have logical partitions between the different kinds of resources you have in one cloud platform. A single AWS account allows the creation of up to five VPCs. In addition to a web server and a database server, if you want to use AWS for unstructured object storage, like images or word files, you could create another VPC with only a private subnet. This will ensure that the data you store within the VPC stays isolated from the internet and is accessible only to your organization. Partitioning the resources in your AWS account, based on the traffic you would prefer to allow or deny, brings more structure to your cloud operations. This will also ensure that the data that should be accessible via the internet is easily accessible, while the ones that are critical to your operations remain isolated from the internet and private to your organization.

Configurations to secure your AWS environment

Adopting critical security configurations can go a long way in fortifying vital applications in your cloud platforms. Here are some examples:

1. Allow Secure Socket Shell (SSH) and Microsoft's Remote Desktop Protocol (RDP) access to only the administrators of a particular subnet. You could do this by defining the IP range in the source section of the NACL. In addition, you could also deny traffic from a particular source or a port.



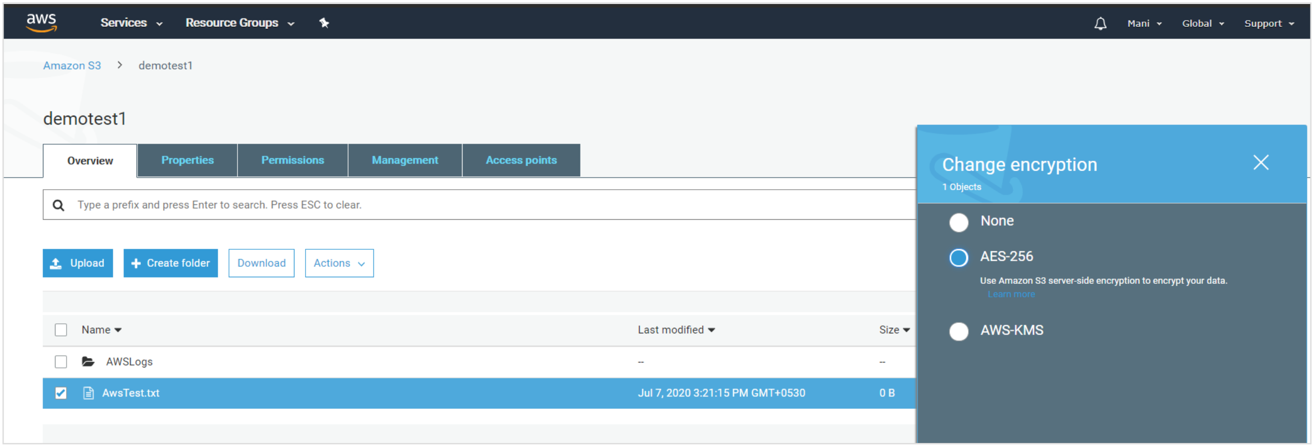
Network ACL: [redacted]

View: All rules

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
1	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY
2	HTTPS (443)	TCP (6)	443	0.0.0.0/0	ALLOW
3	PostgreSQL (5432)	TCP (6)	5432	0.0.0.0/0	ALLOW
4	NFS (2049)	TCP (6)	2049	54.209.0.0/16	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

It could prove disastrous if you accidentally set 0.0.0.0/0 as the source without defining the port range. For instance, consider a rule which states traffic type as "All Traffic", protocol and port range is set as "ALL", and the source is 0.0.0.0/0 and the option is "ALLOW". This means that anyone across the internet can access your critical resources, like a database.

2. Encrypt the objects in your Simple Storage Service (Amazon S3) bucket.
   By selecting the option to encrypt objects in your Amazon S3 bucket, your data will still be protected in case of a breach. Amazon S3 buckets are unencrypted by default. You can change this by selecting the encrypt option.



demotest1

Name	Last modified	Size
□ AWSLogs	--	--
☑ AwsTest.txt	Jul 7, 2020 3:21:15 PM GMT+0530	0 B

Change encryption

1 Objects

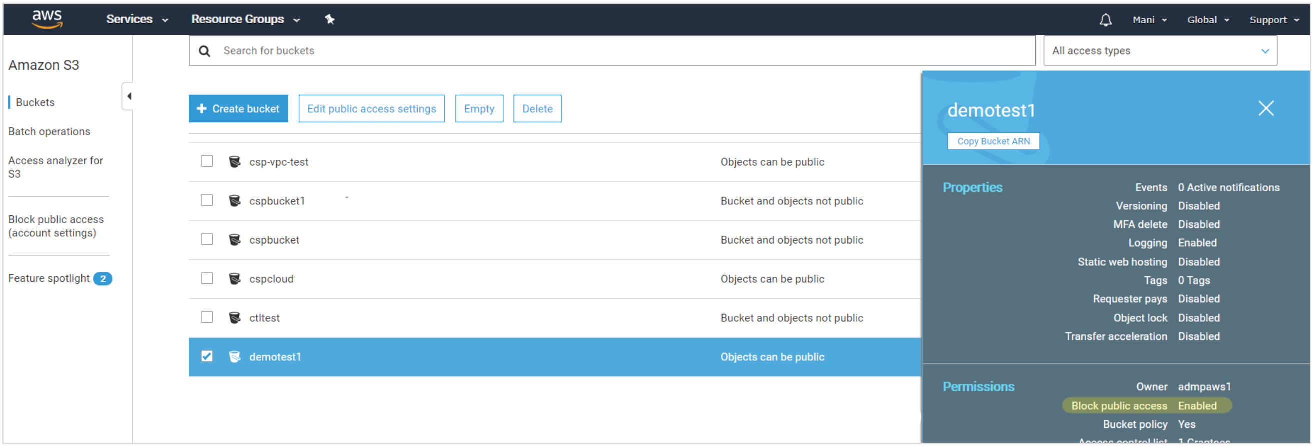
○ None

● AES-256

Use Amazon S3 server-side encryption to encrypt your data. Learn more

○ AWS-KMS

3. Set access to Amazon S3 buckets to private. Not setting the access to private is a common configuration error that results in confidential data being exposed.



☐ csp-vpc-test	Objects can be public
☐ cspbucket1	Bucket and objects not public
☐ cspbucket	Bucket and objects not public
☐ cspcloud	Objects can be public
☐ ctltest	Bucket and objects not public
☑ demotest1	Objects can be public

demotest1

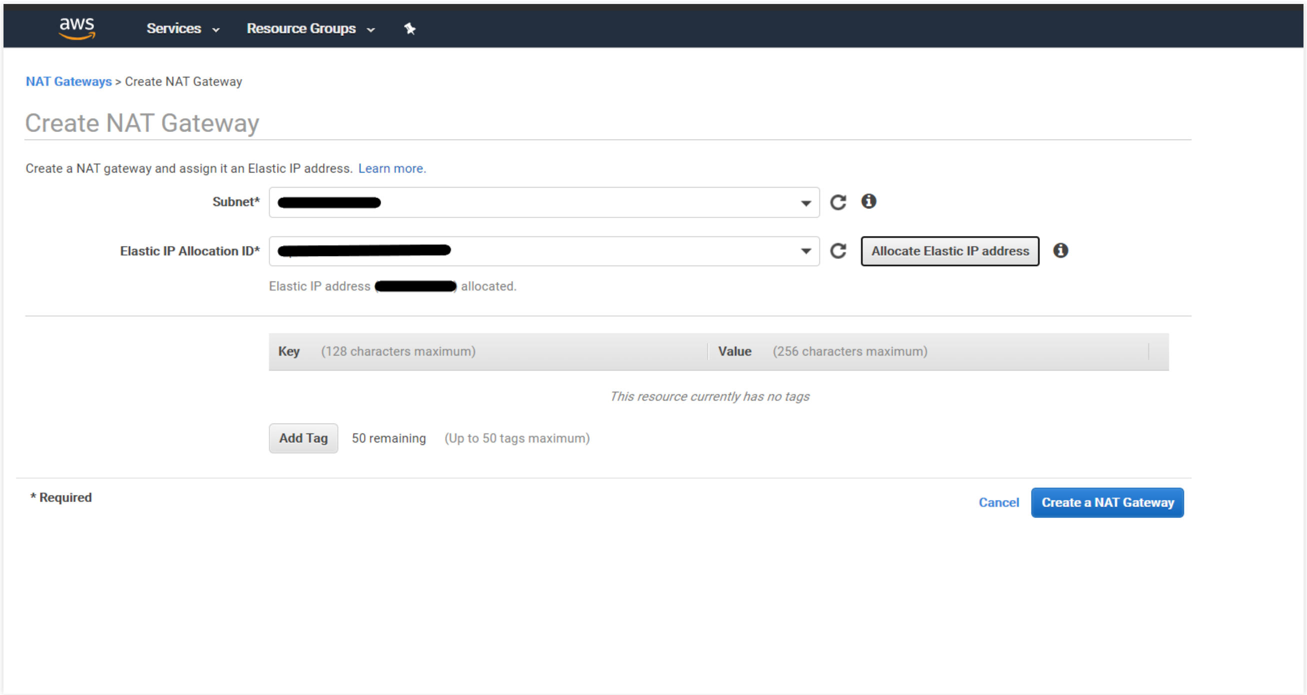
Properties

Events	0 Active notifications
Versioning	Disabled
MFA delete	Disabled
Logging	Enabled
Static web hosting	Disabled
Tags	0 Tags
Requester pays	Disabled
Object lock	Disabled
Transfer acceleration	Disabled

Permissions

Owner	admpaws1
Block public access	Enabled
Bucket policy	Yes
Access control list	1 Grantees

4 Use Network Address Translator (NAT) gateways to provide secure internet access to resources in a private subnet. In case you need internet access to critical resources like Amazon's DynamoDB, configuring a NAT gateway is considered one of the most secure ways to accomplish this.



NAT Gateways > Create NAT Gateway

Create NAT Gateway

Create a NAT gateway and assign it an Elastic IP address. Learn more.

Subnet* [redacted]

Elastic IP Allocation ID* [redacted]

Elastic IP address [redacted] allocated.

Key (128 characters maximum)	Value (256 characters maximum)

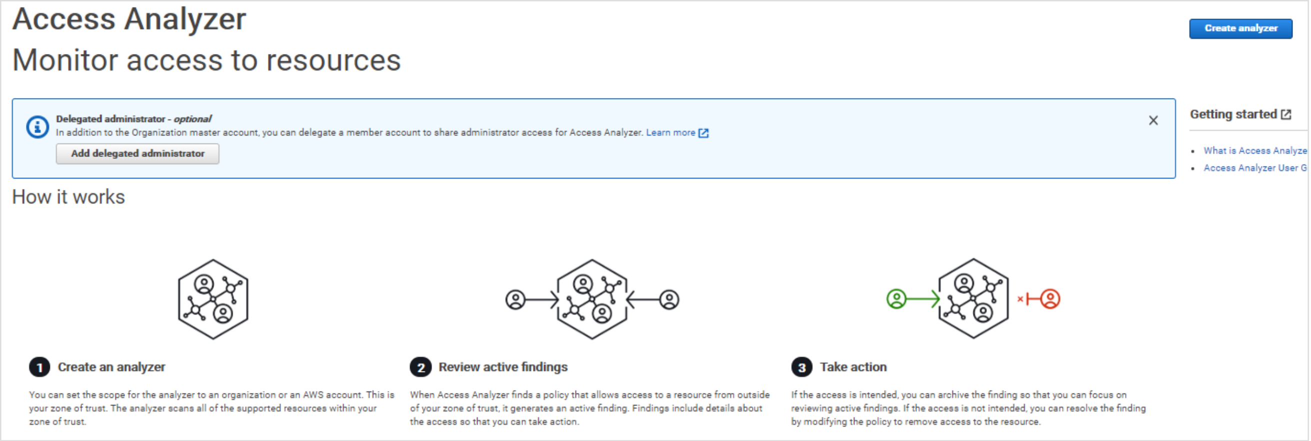
This resource currently has no tags

50 remaining (Up to 50 tags maximum)

* Required

5 In case you are using AWS for the development and testing of applications, ensure that you use separate VPCs for development, staging, and production.

6 Ensure that the principle of least privilege is utilized for identity and access management (IAM) roles. Excessive privileges for a user is a vulnerability. In the IAM console, you can check what actions a user could perform with their level of access. This can be a great tool to analyze and tweak permissions.



Access Analyzer

Monitor access to resources

Delegated administrator - *optional*

In addition to the Organization master account, you can delegate a member account to share administrator access for Access Analyzer. Learn more

How it works

1 **Create an analyzer**

You can set the scope for the analyzer to an organization or an AWS account. This is your zone of trust. The analyzer scans all of the supported resources within your zone of trust.

2 **Review active findings**

When Access Analyzer finds a policy that allows access to a resource from outside of your zone of trust, it generates an active finding. Findings include details about the access so that you can take action.

3 **Take action**

If the access is intended, you can archive the finding so that you can focus on reviewing active findings. If the access is not intended, you can resolve the finding by modifying the policy to remove access to the resource.

7 Ensure that CloudTrail, that allows AWS customers to record application program interface (API) calls and log files to Amazon S3 buckets for storage, is enabled. You could also integrate CloudTrail with Amazon CloudWatch to monitor events, resources and customer applications in your AWS.

8 A root user is a role created when your AWS account is established. It is advisable to create administrator roles for everyday tasks, rather than using the root user account. This is because the root user account comes with complete privileges. Restricting the use of this account can help protect it from misuse.

How a SIEM solution like Log360 can help in securing your cloud

ManageEngine Log360, an integrated security information and event management (SIEM) solution, can help you control your side of the cloud better. It collects log data from CloudTrail, aggregates this information, and presents this to you in the form of actionable reports, including graphs and charts. Log360's machine learning algorithms can also alert you of events that do not follow regular and established patterns.

Is it usual for a user to log in at 5am and make changes to an EC2 instance? If so, this event will be logged as an anomaly with a risk score assigned. A high risk score indicates that the series of events that lead to it are deviations from the norm. This preemptive approach to security can help security admins to narrow down focus to areas that really need attention.

Here are some areas Log360 can help you monitor:

- Amazon S3 log management
- Amazon S3 bucket logging
- AWS IAM activity reporting
- Auto-configuration of AWS
- AWS ELB traffic analysis
- AWS security group change auditing
- Amazon RDS activity reporting
- Forensic analysis using CloudTrail logs

ManageEngine
Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats.

Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

$ Get Quote   ⤓ Download