Detecting AWS network ACL activity

Applicability

- Product: Splunk Cloud Platform or Splunk Enterprise
- Feature: Monitoring
- Technology: Splunk App for AWS and Splunk Add-on for AWS
- Data: Amazon Web Services: CloudTrail and CloudWatch
- Data: Amazon Web Services: VPC Flow Logs

Scenario

You are an Amazon Web Services (AWS) admin who manages access to AWS resources and services across your organization. AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational/risk auditing of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Part of your role involves monitoring events and actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs to ensure that your servers are not vulnerable to attacks.

These searches help you to monitor your AWS network infrastructure, using CloudTrail logs from AWS to check for bad configurations and malicious activity in your AWS network access controls.

- Some commands, parameters, and field names in the searches below may need to be adjusted to match your environment. In addition, to optimize the searches shown below, you should specify an index and a time range when appropriate.
- To run these searches, install the AWS App for Splunk (version 5.1.0 or later) and Splunk Add-on for AWS (version 4.4.0 or later), and configure your CloudTrail inputs. Some of these searches also require configuration of VPC flow logs.

Support searches

► Baseline of blocked outbound traffic from AWS

In order to run this search, you need to configure your VPC flow logs.

This search establishes, on a per-hour basis, the average and the standard deviation of the number of outbound connections blocked in your VPC flow logs by each source IP address (IP address of your EC2 instances). The number of data points for each source IP is also recorded. This table outputs to a lookup file to allow the detection search to operate quickly.
Baseline of network ACL activity by ARN

In order to run this search, you need to configure your VPC flow logs.

This search establishes, on a per-hour basis, the average and the standard deviation of the number of API calls that were related to network access control lists (ACLs) made by each user. The number of data points for each user is also recorded. This table is then outputted to a lookup file to allow the detection search to operate quickly.

Detection searches

AWS network access control list created with all open ports

A network access control list (ACL) is a layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. Network ACLs with all open ports have a larger attack surface. This search looks for CloudTrail events to detect if any network ACLs were created with all the ports open to a specified CIDR, in this example ports ranging from 1024 to 65525. The search creates a table comprised of AWS account id, src, user, and all parameters of the request made by the user and the server response.

False positives could occur from this search as it's possible that an admin has created this ACL with all ports open for some legitimate purpose. However, this type of ACL should not be allowed in a production environment.
Enforcing network-access controls is one of the defensive mechanisms used by cloud administrators to restrict access to a cloud instance. After the attacker has gained control of the AWS console by compromising an admin account, they can delete a network ACL and gain access to the instance from anywhere.

This search queries the CloudTrail logs to detect users deleting network ACLs. The search then looks for CloudTrail events to detect whether any network ACLs have been deleted and gives you values of error messages and error codes (if any), user details, user source IP, the user who initiated this request, and the name of the event.

False positives could occur from this search as it's possible that a user has legitimately deleted a network ACL.

### AWS network access control list deleted

```splunk
| search requestParameters.portRange.from=1024 requestParameters.portRange.to=65525 requestParameters.ruleAction=allow
| rename userIdentity.arn AS arn
| rename requestParameters.networkAclId AS networkAclid
| table _time aws_account_id src userName arn networkAclid requestParameters.* responseElements.*
```

### Contextual searches

#### AWS network ACL details from ID

In order to run this search, you need to configure your AWS description inputs.

This search queries AWS description logs and returns all the information about a specific network ACL via network ACL ID.

```splunk
| search sourcetype=aws:description id={networkAclid}
| table id account_id vpc_id network_acl_entries{}.*
```

#### AWS network interface details via resourceId

In order to run this search, you need to configure your AWS configuration inputs.

This search queries AWS configuration logs and returns the information about a specific network interface via network interface ID. The information includes the ARN of the network interface, its relationships with other AWS resources, and the public and the private IPs associated with the network interface.
Investigative searches

AWS investigate user activities by ARN

This search lists all the logged CloudTrail activities by a specific user ARN and will create a table containing the source of the user, the region of the activity, the name and type of the event, the action taken, and all of the user's identity information.

| search sourcetype=aws:cloudtrail userIdentity.arn={arn} | table _time userIdentity.type userIdentity.userName userIdentity.arn aws_account_id src awsRegion eventName eventType |

AWS network ACL details from ID

This search queries AWS description logs and returns all the information about a specific network ACL via network ACL ID.

| search sourcetype=aws:description | rename id AS networkAclId | search networkAclId=$networkAclId$ | table id account_id vpc_id network_acl_entries{}.* |

AWS network interface details via resourceId

This search queries AWS configuration logs and returns the information about a specific network interface via network interface ID. The information will include the ARN of the network interface, its relationships with other AWS resources, the public and the private IP associated with the network interface.

| search sourcetype=aws:config resourceId=$resourceId$ | table _time ARN relationships{}.resourceType relationships{}.name relationships{}.resourceId configuration. privateIpAddresses{}.privateIpAddress configuration.privateIpAddresses{}.association.publicIp |

Get all AWS activity from IP address

This search retrieves all the activity from a specific IP address and will create a table containing the time, ARN, username, the type of user, the IP address, the AWS region the activity was in, the API called, and whether or not the API call was successful.

| search sourcetype=aws:cloudtrail | iplocation sourceIPAddress | search src_ip=$src_ip$ |
Get DNS server history for a host

While investigating any detections it is important to understand which and how many DNS servers a host has connected to in the past. This search uses data that is tagged as DNS and gives you a count and list of DNS servers that a particular host has connected to the previous 24 hours.

```
| search tag=dns src_ip=$src_ip$ dest_port=53
| streamstats time_window=1d count values(dest_ip) AS dcip BY src_ip
| table date_mday src_ip dcip count
| sort -count
```

Get DNS traffic ratio

To successfully implement this search you need to be populating the Network Traffic data model. Content developed by the Splunk Security Research team requires the use of consistent, normalized data provided by the Common Information Model (CIM). For information on installing and using the CIM, see the Common Information Model documentation.

This search calculates the ratio of DNS traffic originating and coming from a host to a list of DNS servers over the last 24 hours. A high value of this ratio could be very useful to quickly understand if a src_ip (host) is sending a high volume of data out via port 53, which could be an indicator of data exfiltration via DNS.

```
| tstats allow_old_summaries=true sum("All_Traffic.bytes_out") AS bytes_out, sum("All_Traffic.bytes_in") as bytes_in FROM datamodel=Network_Traffic WHERE (nodename=All_Traffic "All_Traffic.dest_port"=53) BY "All_Traffic.src", "All_Traffic.dest"
| rename "All_Traffic.*" AS *
| search (dest=$dest_ip src=$src_ip$)
| eval ratio=(bytes_out / bytes_in)
| table ratio
```

Get process info

To successfully implement this search you need to be populating the Endpoint data model. Content developed by the Splunk Security Research team requires the use of consistent, normalized data provided by the Common Information Model (CIM). For information on installing and using the CIM, see the Common Information Model documentation.

This search queries the Endpoint data model to give you details about the process running on a host which is under investigation. To gather the process info, enter the values for the process name in question and the destination IP address.

```
| tstats summariesonly=true allow_old_summaries=true count, values("Processes.process") AS process,
```
min(_time) AS firstTime, max(_time) AS lastTime FROM datamodel=Endpoint.Processes BY "Processes.user", "Processes.parent_process_name", "Processes.process_name", "Processes.dest" | rename "Processes.*" AS "*" | search (dest=$dest$ process_name=$process_name$) | convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime) | convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime)

**Additional resources**

This use case is included within Splunk Enterprise Security, a Splunk app that provides prebuilt content and searches to help answer root-cause questions in real-time about malicious and anomalous events in your IT infrastructure. In addition, Splunk Enterprise Security provides a number of other searches to help reinforce your Cloud Security posture, including:

- Detecting AWS cross-account activity
- Detecting AWS suspicious provisioning activities
- Detect suspicious new instances in your EC2 environment
- Monitoring user activity spikes in AWS
- Monitoring AWS and AWS EC2 for suspicious login activities
- Monitoring AWS EC2 for suspicious login activities
- Monitoring AWS S3 for suspicious activities
- Monitoring AWS for suspicious traffic
- Monitoring AWS EC2 for unusual modifications

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.