Solution Guide: Respond and recover from a data breach

The **Respond and recover from a data breach** is a portion of the capstone project that puts your cloud cybersecurity skills to the test; the lab is a simulated cloud environment designed for you to respond to a data breach. The lab includes a set of tasks and challenges that you'll complete using the skills you've learned throughout the certificate, focusing on incident response tasks like identifying vulnerabilities, isolating and containing threats, and recovering compromised systems. The lab also requires you to tackle the following challenges to assess your skills on your own: fixing a Compute Engine virtual machine, Cloud Storage bucket, and firewall vulnerabilities related to the data breach.

This solution guide provides the instructions for tasks and challenges in the lab for you to assess against your own work.

Task 1: Analyze the data breach and gather information

To complete this task, navigate to the Security Command Center, access the **Active vulnerabilities** and select **Findings By Resource Type** to filter the active vulnerabilities by resource. There are three cloud resource types with vulnerabilities that you'll remediate: **Cloud storage bucket**, **Compute Instance virtual machine (VM)**, and **firewall**.

Then, navigate to the **Compliance** section to access the details of the **PCI DSS 3.2.1** report. Identify the rules that are non-compliant with PCI DSS. These rules correspond to the vulnerabilities for the bucket, VM, and firewall rules. You will remediate these vulnerabilities in the upcoming tasks and challenges.

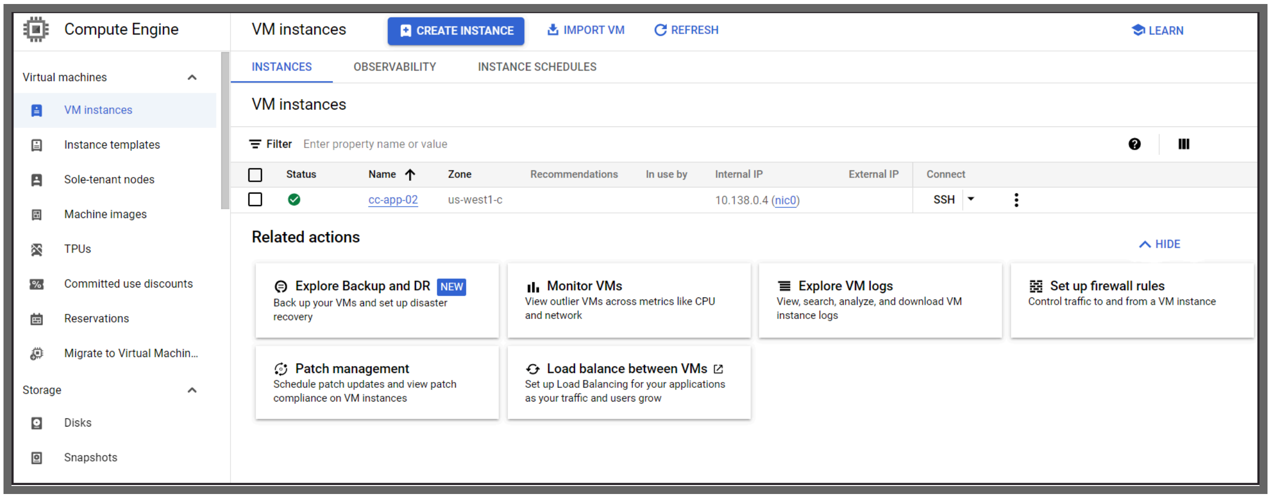
Task 2 challenge: Fix the Compute Engine vulnerabilities

In this task and challenge, you'll remediate the following vulnerabilities related to the vulnerable Compute Engine VM by creating a new VM from a snapshot and deleting the vulnerable VM:

- **Public IP address (VMs should not be assigned public IP addresses)**
- **Compute secure boot disabled**
- **Default service account used**
- **Full API access (Instances should not be configured to use the default service account with full access to all Cloud APIs)**
- **Malware: bad domain**

Before you complete this challenge, you'll need to shut down the vulnerable VM **cc-app-01** by navigating to **Compute Engine** > **VM instances**, and stopping **cc-app-01**. Then, you'll create a new VM **cc-app-02** from a snapshot and configure it with the settings provided in the lab instructions.

To complete this challenge, select the vulnerable VM **cc-app-01** and click **Delete**. After you've deleted the vulnerable VM, **cc-app-02** should be the only VM that's listed.



VM instances

□	Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Connect
□	✓	cc-app-02	us-west1-c			10.138.0.4 (nic0)		SSH

Related actions

Explore Backup and DR NEW
Back up your VMs and set up disaster recovery

Monitor VMs
View outlier VMs across metrics like CPU and network

Explore VM logs
View, search, analyze, and download VM instance logs

Set up firewall rules
Control traffic to and from a VM instance

Patch management
Schedule patch updates and view patch compliance on VM instances

Load balance between VMs
Set up Load Balancing for your applications as your traffic and users grow

Solution

1. On the **VM Instances** page, select the checkbox for the **cc-app-01** VM.
2. Click **Delete**.
3. A pop-up will appear asking you to confirm the instance deletion, click **Delete**.

Task 3 challenge: Fix Cloud Storage bucket permissions

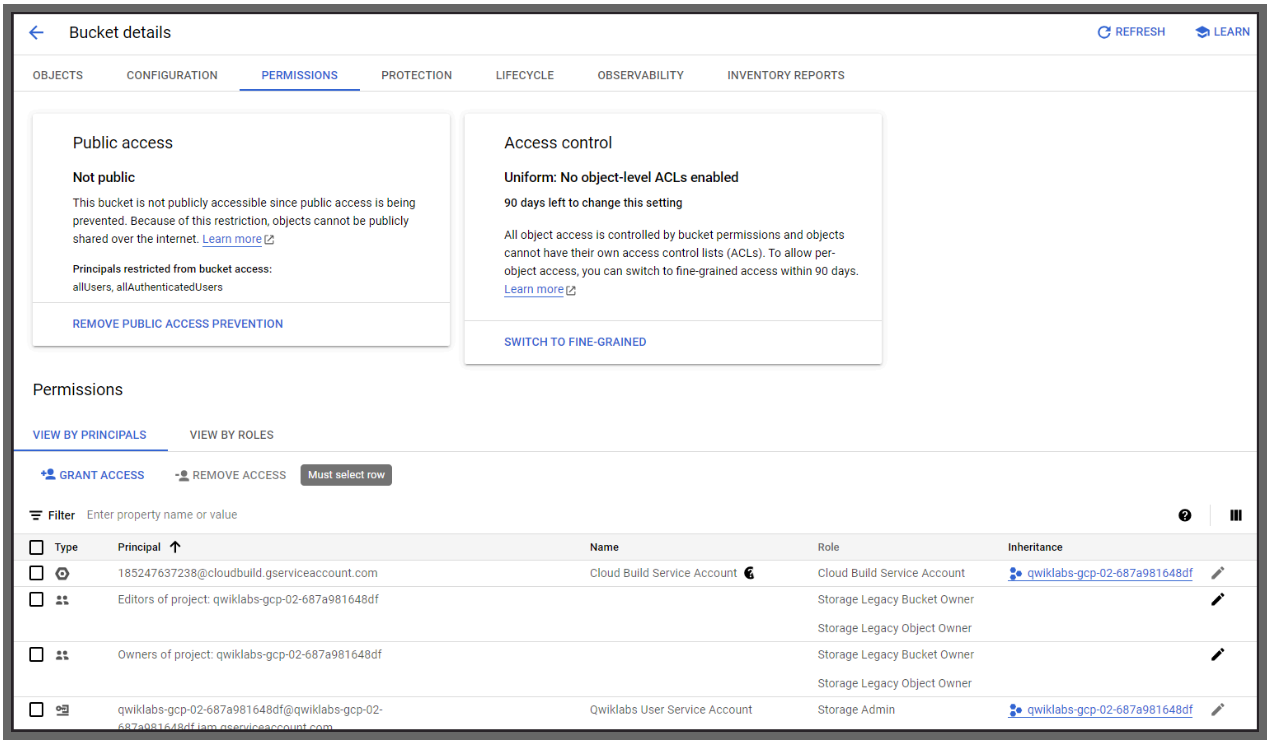
In this task and challenge, you'll remediate the following vulnerabilities related to the Cloud Storage bucket by removing the public access control list, disabling public bucket access, and enabling uniform bucket level access control:

- **Public bucket ACL (Cloud Storage buckets should not be anonymously or publicly accessible)**
- **Bucket policy only disabled**

Please note that while enabling logging for cloud resources is a security best practice, the **Bucket logging disabled** vulnerability will not be remediated in this lab because it requires working with multiple projects. As a result, this vulnerability will still appear in the compliance report after you've completed the remediation tasks and challenges.
To complete this challenge, you'll need to switch the bucket's access control to **uniform** and remove permissions for the **allUsers** principals from the storage bucket. Doing this will enforce a single set of permissions for the bucket and its objects.

First, switch the bucket's access to uniform by navigating to **Cloud Storage** > **Buckets**. Locate and select the vulnerable Cloud Storage bucket, navigate to the bucket's **Permissions** and select **Switch to uniform**. Ensure that you select **Add project role ACLs to the bucket IAM policy** and save the changes.

Lastly, remove permissions for the allUsers principals. In the **Permissions** section, remove access to the **allUsers** principals.



Public access

Not public

This bucket is not publicly accessible since public access is being prevented. Because of this restriction, objects cannot be publicly shared over the internet. Learn more

Principals restricted from bucket access:
allUsers, allAuthenticatedUsers

Access control

Uniform: No object-level ACLs enabled

90 days left to change this setting

All object access is controlled by bucket permissions and objects cannot have their own access control lists (ACLs). To allow per-object access, you can switch to fine-grained access within 90 days. Learn more

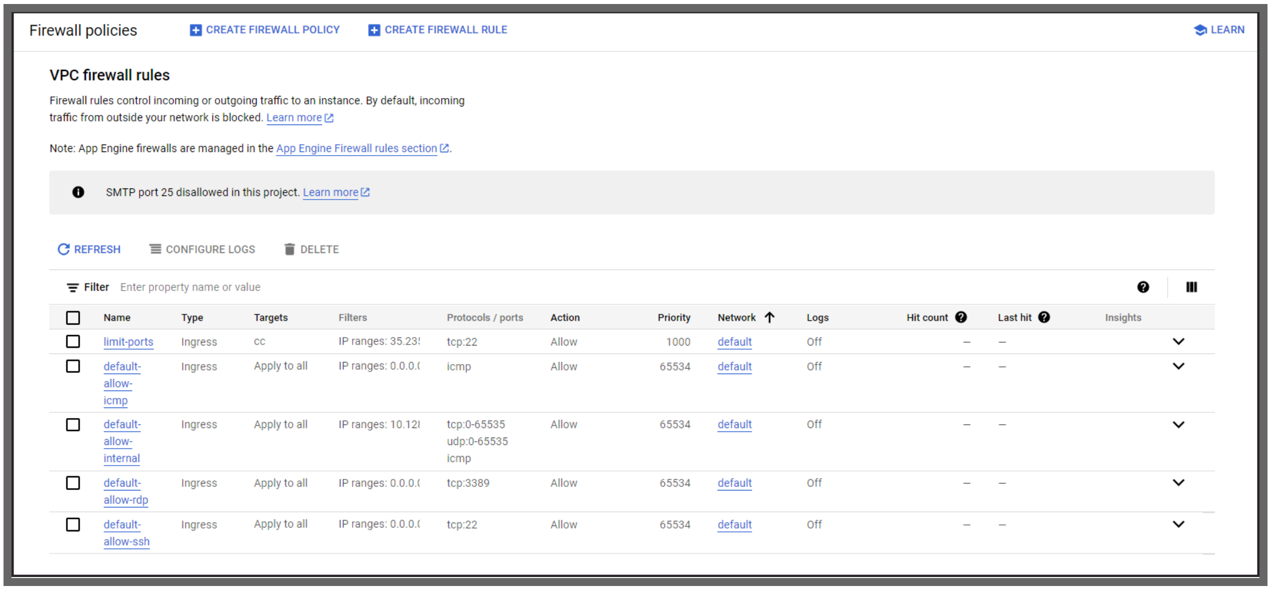
□ Type	Principal ↑	Name	Role	Inheritance
□	185247637238@cloudbuild.gserviceaccount.com	Cloud Build Service Account	Cloud Build Service Account	qwiklabs-gcp-02-687a981648df
□	Editors of project: qwiklabs-gcp-02-687a981648df		Storage Legacy Bucket Owner Storage Legacy Object Owner	
□	Owners of project: qwiklabs-gcp-02-687a981648df		Storage Legacy Bucket Owner Storage Legacy Object Owner	
□	qwiklabs-gcp-02-687a981648df@qwiklabs-gcp-02-687a981648df.iam.gserviceaccount.com	Qwiklabs User Service Account	Storage Admin	qwiklabs-gcp-02-687a981648df

Solution

1. In the **Access control** tile, click **Switch to uniform**.
2. In the **Edit access control** dialog, select **Uniform**.
3. Select the checkbox for **Add project role ACLs to the bucket IAM policy.**
4. Click **Save**.
5. In the **Permissions** section, select the checkbox for **allUsers**.
6. Click **Remove Access**.
7. A pop-up will appear asking you to confirm the removal of **allUsers**, click **Confirm**.

Task 4 challenge: Limit firewall ports access

To complete this challenge, create a new firewall rule named **limit-ports** that restricts SSH (TCP port 22) access to only authorized IP addresses from the source network **35.235.240.0/20** to Compute Engine VM instances with the target tag **cc**.



VPC firewall rules

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. Learn more

Note: App Engine firewalls are managed in the App Engine Firewall rules section.

SMTP port 25 disallowed in this project. Learn more

☐	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network ↑	Logs	Hit count	Last hit	Insights
☐	limit-ports	Ingress	cc	IP ranges: 35.23!	tcp:22	Allow	1000	default	Off	–	–	
☐	default-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.(	icmp	Allow	65534	default	Off	–	–	
☐	default-allow-internal	Ingress	Apply to all	IP ranges: 10.12(	tcp:0-65535 udp:0-65535 icmp	Allow	65534	default	Off	–	–	
☐	default-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.0.(	tcp:3389	Allow	65534	default	Off	–	–	
☐	default-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.0.(	tcp:22	Allow	65534	default	Off	–	–	

Solution

1. In the Google Cloud console, click the **Navigation menu** (☰).
2. Select **VPC Networks > Firewall.** The **Firewall policies** page displays.
3. On the toolbar, click **+ Create Firewall Rule**. The **Create a firewall rule** dialog displays.
4. Specify the following, and leave the remaining settings as their defaults:

Field	Value
Name	limit-ports
Network	default
Targets	Specified target tags
Target tags	cc
Source filter	IPv4 ranges
Source IPv4 ranges	35.235.240.0/20
In the **Protocols and ports** section	● Select **Specified protocols and ports** ● Select the **TCP** checkbox ● In the **Ports** field enter **22**

5. Click **Create**.

Alternatively, you can run the following command in Cloud Shell:

1. Click **Activate Cloud Shell** at the top of the Google Cloud console. You may be asked to click **Continue**.
2. Copy the following commands into the Cloud Shell terminal:

Unset

```
export PROJECT_ID=$(gcloud info
--format='value(config.project)')

gcloud compute --project=$PROJECT_ID firewall-rules create
limit-ports --direction=INGRESS --priority=1000
--network=default --action=ALLOW --rules=tcp:22
--source-ranges=35.235.240.0/20 --target-tags=cc
```

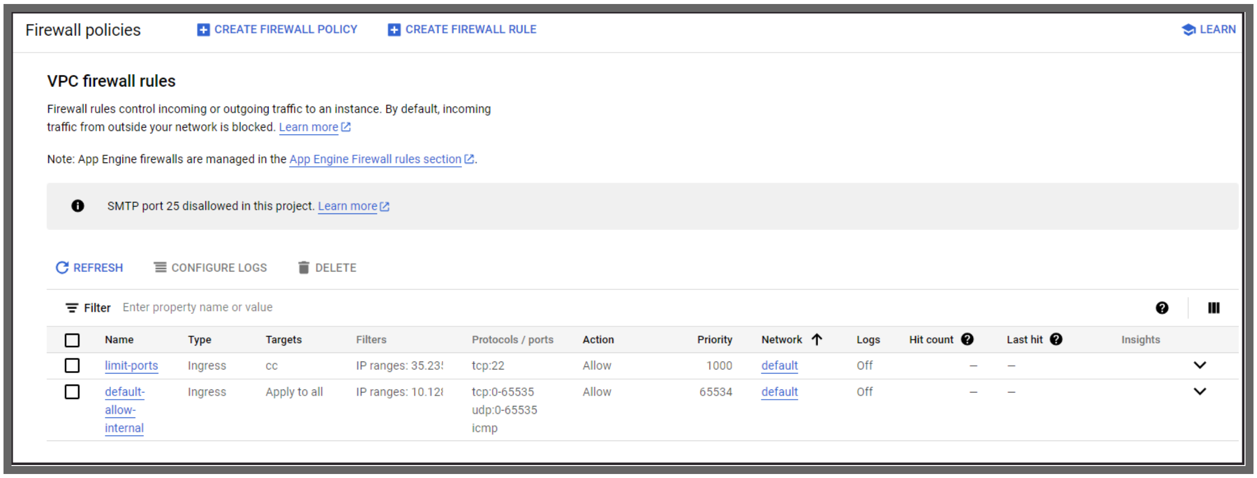
These commands retrieve your current project ID, then create a new firewall rule in that project that allows only SSH traffic from a specific IP range to instances with the target tag **cc**.

3. Press **ENTER**.

Task 5 challenge: Fix the firewall configuration

To complete these challenges, delete the **default-allow-icmp**, **default-allow-rdp**, and **default-allow-ssh** firewall rules and enable logging for the newly created firewall rule **limit-ports** and the existing firewall rule **default-allow-internal**. This will remediate the following firewall vulnerabilities:

- **Open SSH port (Firewall rules should not allow connections from all IP addresses on TCP or SCTP port 22)**
- **Open RDP port (Firewall rules should not allow connections from all IP addresses on TCP or UDP port 3389)**
- **Firewall rule logging disabled (Firewall rule logging should be enabled so you can audit network access)**



Firewall policies

VPC firewall rules

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. Learn more

Note: App Engine firewalls are managed in the App Engine Firewall rules section.

SMTP port 25 disallowed in this project. Learn more

□	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network ↑	Logs	Hit count	Last hit	Insights
□	limit-ports	Ingress	cc	IP ranges: 35.23!	tcp:22	Allow	1000	default	Off	–	–	
□	default-allow-internal	Ingress	Apply to all	IP ranges: 10.12!	tcp:0-65535 udp:0-65535 icmp	Allow	65534	default	Off	–	–	

Solution

1. In the **Navigation menu** (☰), select **Network Security** > **Firewall policies**. The Firewall policies page opens. (You may need to click **More Products** to expand the **Navigation menu** options and locate **Network Security** under **Networking**.)
2. In the **VPC firewall rules** section, select the checkboxes for the following VPC firewall rules:
    - default-allow-icmp
    - default-allow-rdp
    - default-allow-ssh
3. Click **Delete**.
4. A pop-up will appear asking you to confirm the deletion of the 3 firewall rules, click **Delete**.

Enable logging for the remaining firewall rules **limit-ports** (the rule you created in Task 4) and **default-allow-internal**.

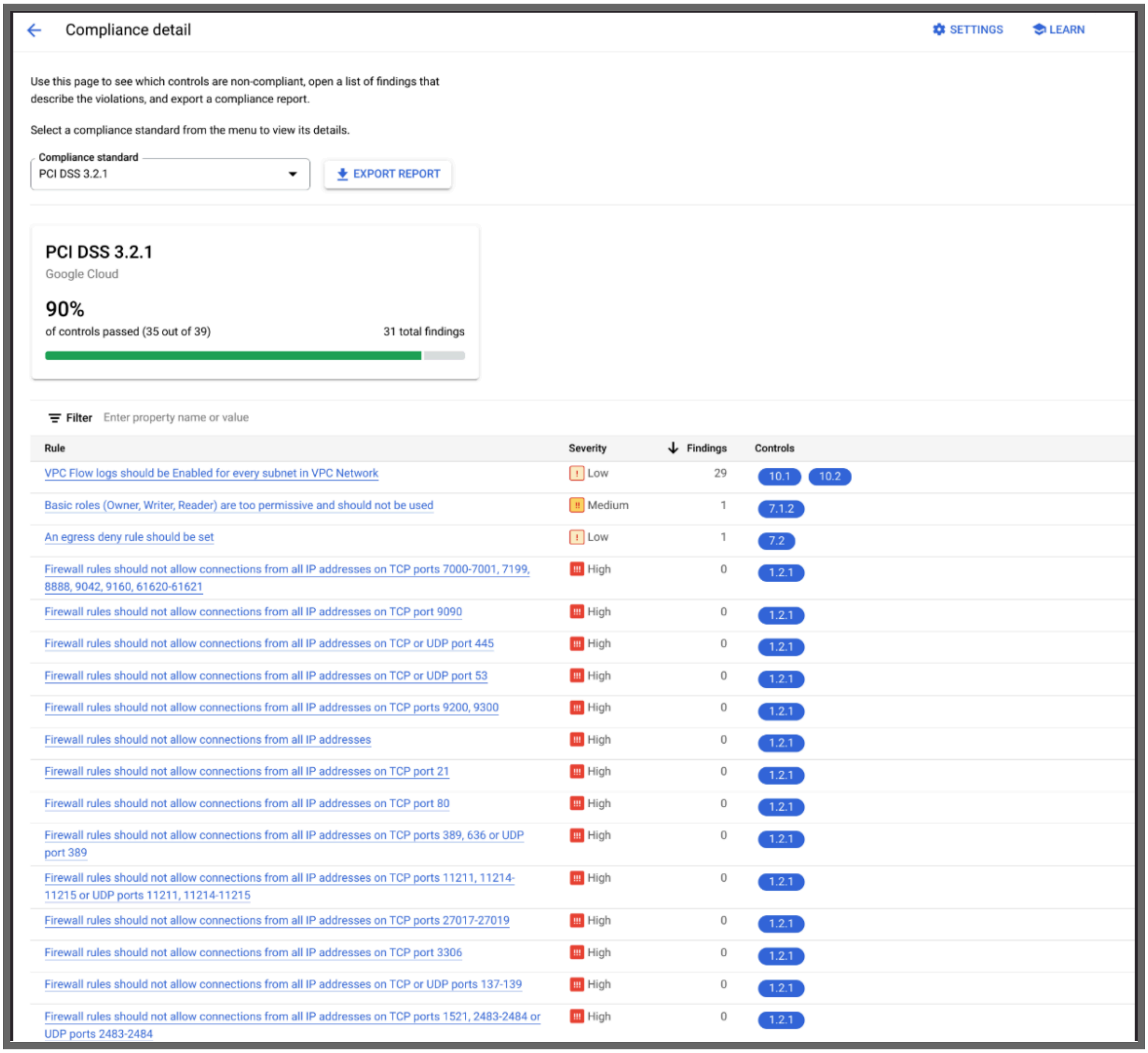
Solution

1. In the **Name** section, click the **limit-ports** firewall rule link. The Firewall rule details page opens.
2. In the action bar, click **Edit**.
3. In the **Logs** section, select **On**.
4. Scroll down to the bottom of the page, and click **Save**.
5. Click the **Back to parent page** button.
6. In the **Name** section, click the **default-allow-internal firewall** rule link. The Firewall rule details page opens.
7. In the action bar, click **Edit**.

8. In the **Logs** section, select **On**.
9. Scroll down to the bottom of the page, and click **Save**.
10. Click the **Back to parent page** button.

Task 6: Verify compliance

To complete this task, navigate to Security Command Center and access the details for the **PCI DSS 3.2.1.** compliance report. Notice that the percentage for **controls passed** has increased, indicating that the vulnerabilities have been sufficiently remediated.



Use this page to see which controls are non-compliant, open a list of findings that describe the violations, and export a compliance report.

Select a compliance standard from the menu to view its details.

Compliance standard: PCI DSS 3.2.1

PCI DSS 3.2.1
Google Cloud

90%
of controls passed (35 out of 39)
31 total findings

Enter property name or value

Rule	Severity	↓ Findings	Controls
VPC Flow logs should be Enabled for every subnet in VPC Network	Low	29	10.1 10.2
Basic roles (Owner, Writer, Reader) are too permissive and should not be used	Medium	1	7.1.2
An egress deny rule should be set	Low	1	7.2
Firewall rules should not allow connections from all IP addresses on TCP ports 7000-7001, 7199, 8888, 9042, 9160, 61620-61621	High	0	1.2.1
Firewall rules should not allow connections from all IP addresses on TCP port 9090	High	0	1.2.1
Firewall rules should not allow connections from all IP addresses on TCP or UDP port 445	High	0	1.2.1
Firewall rules should not allow connections from all IP addresses on TCP or UDP port 53	High	0	1.2.1
Firewall rules should not allow connections from all IP addresses on TCP ports 9200, 9300	High	0	1.2.1
Firewall rules should not allow connections from all IP addresses	High	0	1.2.1
Firewall rules should not allow connections from all IP addresses on TCP port 21	High	0	1.2.1
Firewall rules should not allow connections from all IP addresses on TCP port 80	High	0	1.2.1
Firewall rules should not allow connections from all IP addresses on TCP ports 389, 636 or UDP port 389	High	0	1.2.1
Firewall rules should not allow connections from all IP addresses on TCP ports 11211, 11214-11215 or UDP ports 11211, 11214-11215	High	0	1.2.1
Firewall rules should not allow connections from all IP addresses on TCP ports 27017-27019	High	0	1.2.1
Firewall rules should not allow connections from all IP addresses on TCP port 3306	High	0	1.2.1
Firewall rules should not allow connections from all IP addresses on TCP or UDP ports 137-139	High	0	1.2.1
Firewall rules should not allow connections from all IP addresses on TCP ports 1521, 2483-2484 or UDP ports 2483-2484	High	0	1.2.1

Disregard the following vulnerabilities because they do not relate to the data breach scenario:

- **VPC Flow logs should be Enabled for every subnet VPC Network**
- **Basic roles (Owner, Writer, Reader) are too permissive and should not be used**
- **An egress deny rule should be set**

Resources for more information

Use these readings to help support you as you work through the solution:

- **Guide to Virtual Private Cloud (VPC) reading** available in course 1 module 4
- **Guide to risk assessment and compliance management with Security Command Center reading** available in course 2 module 4
- **Guide to firewall rules reading** available in course 3 module 1
- **Guide to event threat detection reading** in course 4 module 1

As a reminder, the skills and concepts presented in prior labs may also serve as a resource for the capstone project.