Change firewall rules using Terraform and Cloud Shell

CLONE THE TERRAFORM REPO

1. In the Google Cloud console, click the **Activate Cloud Shell**
2. Click **Continue**.

It should only take a few moments to provision and connect to the Cloud Shell environment.

3. Copy the following command into the Cloud Shell terminal:

```
cloudshell_open --repo_url "https://github.com/terraform-google-modules/docs-examples.git" --print_file "./motd" --dir "firewall_basic" --page "editor" --tutorial "./tutorial.md" --open_in_editor "main.tf" --force_new_clone
```

Copied!

content_copy

This command clones the Terraform example directory.

4. Press **ENTER**.

This command performs the following actions:

- Clones the `terraform-google-modules`.
- Prints the `motd` file name.
- Switches to the `firewall_basic` directory.
- Checks the cloned files, for example `tutorial.md`.
- Opens `main.tf` in Cloud Shell Editor.

Once the cloning is complete, you'll be at the `~/cloudshell_open/docs-examples/firewall_basic` location in the terminal. Your Cloud Shell prompt should display similar output to the following example:

```
student_01_c2e095df84e2@cloudshell:~/cloudshell_open/docs-examples/firewall_basic (qwiklabs-gcp-04-fde36f013e65)$
```

5. Copy the following command into the Cloud Shell terminal to list the contents of the directory:

```
ls
```

Copied!

content_copy

You should notice that several files in the directory have been downloaded: `backing_file.tf`, `main.tf`, `motd`, and `tutorial.md`.

6. Copy the following command into the Cloud Shell terminal to analyze the configuration of the firewall rule:

```
cat main.tf
```

Copied!

content_copy

7. Press **ENTER**.

DEPLOY THE VPC NETWORK AND FIREWALL

1. Copy the following command into the Cloud Shell terminal.

```
export GOOGLE_CLOUD_PROJECT=qwiklabs-gcp-02-41af73f63289
```

Copied!

content_copy

This command sets the project ID.

2. Press **ENTER**.

3. Copy the following command into the Cloud Shell terminal:

```
terraform init
```

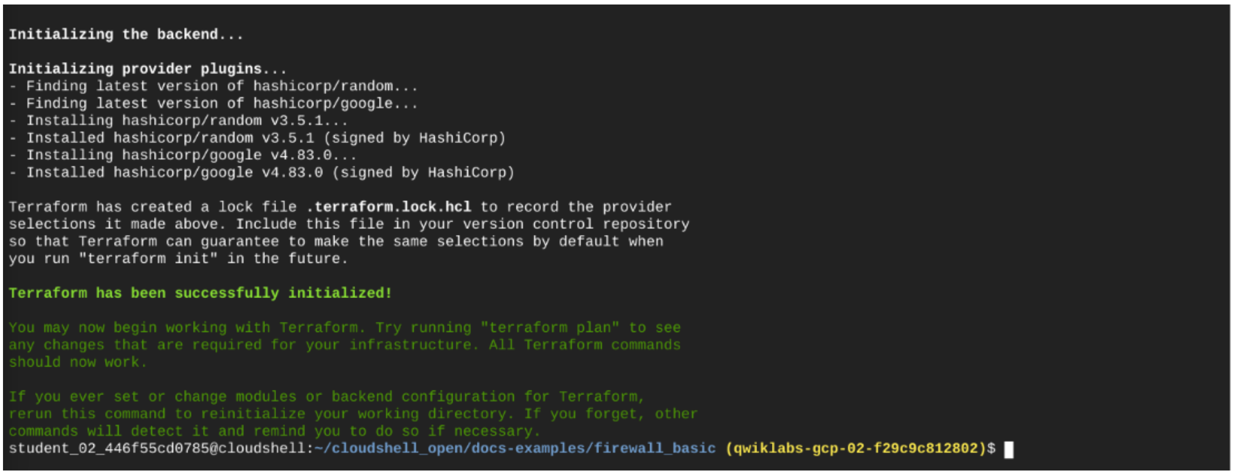
Copied!

content_copy

This command initializes the Terraform script.

4. Press **ENTER**.

The output should return a message stating that the Terraform has been successfully initialized. Take a moment to examine the output. You'll notice that Terraform will create a new firewall and VPC network:



```
Initializing the backend...

Initializing provider plugins...
- Finding latest version of hashicorp/random...
- Finding latest version of hashicorp/google...
- Installing hashicorp/random v3.5.1...
- Installed hashicorp/random v3.5.1 (signed by HashiCorp)
- Installing hashicorp/google v4.83.0...
- Installed hashicorp/google v4.83.0 (signed by HashiCorp)

Terraform has created a lock file .terraform.lock.hcl to record the provider
selections it made above. Include this file in your version control repository
so that Terraform can guarantee to make the same selections by default when
you run "terraform init" in the future.

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
student_02_446f55cd0785@cloudshell:~/cloudshell_open/docs-examples/firewall_basic (qwiklabs-gcp-02-f29c9c812802)$
```

5. Once the initialization is complete, copy the following command into the Cloud Shell terminal:

```
terraform apply
```

Copied!

content_copy

This command applies the changes and deploys the Terraform script.

6. Press **ENTER**.

Note: *If an **Authorize Cloud Shell** dialog box appears, click **Authorize** to grant permission to use your credentials for the gcloud command.*

7. The command prompt will prompt you to **Enter a value**. Type "yes", and press **ENTER**.

This will start creating the VPC network and firewall rules.

Once it’s completed, the output should return the following message:

```
Apply complete! Resources: 3 added, 0 changed, 0 destroyed.
```

VERIFY THE DEPLOYMENT OF THE RESOURCES

1. In the Google Cloud console, from the Navigation menu (☰), select **VPC network > VPC networks**. The VPC networks page opens.
2. You should notice two VPC networks, **default** and the newest one you just created, **test-network**. Click **test-network** to access the VPC network details.
3. Click **Firewalls**. Use the expand arrow to expand **vpc-firewall-rules**.
   Under **Protocols and ports** and **Action** you should notice the firewall rules are the same rules as defined in the configuration file: **Allow** and **tcp:80**, **1000-2000**, **8080** **icmp**.