

https://www.skills.google/focuses/46425767?parent=lti_session

Cenário

O Cymbal Bank tem um servidor da Web de demonstração, provisionado em uma rede de nuvem privada virtual (VPC). Chloe, a líder da sua equipe, está preocupada com a segurança do servidor. Ela quer que você analise o tráfego recebido pelo servidor e use regras de firewall para bloquear as conexões com portas desnecessárias. Você precisa analisar as regras de firewall do servidor da Web e testar as conexões dele. Para fazer a tarefa, você vai precisar criar várias regras de firewall, acessar o servidor da Web e analisar os registros das conexões de rede.

Confira como fazer a tarefa: **primeiro**, você vai criar uma regra de firewall que permita a entrada do tráfego de rede no servidor da Web de demonstração. **Segundo**, gerar tráfego HTTP para o servidor e analisar os registros de rede. **Terceiro**, criar e testar uma regra de firewall para negar o tráfego HTTP para o servidor. **Quarto**, analisar os registros do firewall para confirmar se a nova regra está funcionando corretamente.

Observação: este laboratório inclui uma VPC de rede do modo personalizado, **vpc-net**, e uma sub-rede, **vpc-subnet**, configurada com os registros de fluxo de VPC, na região Default region. Também inclui uma instância de VM, **web-server**, com o servidor da Web Apache instalado em **vpc-subnet** e a tag de rede **http-server** na zona Default zone.

Configuração

Antes de clicar em "Começar o laboratório"

Leia as instruções a seguir. Os laboratórios são cronometrados e não podem ser pausados. O timer é iniciado quando você clica em **Começar o laboratório** e mostra por quanto tempo os recursos do Google Cloud vão ficar disponíveis.

Neste laboratório prático, você pode fazer as atividades por conta própria em um ambiente cloud de verdade, não em uma simulação ou demonstração. Você vai receber novas credenciais temporárias para fazer login e acessar o Google Cloud durante o laboratório.

Confira os requisitos para concluir o laboratório:

- Acesso a um navegador de Internet padrão (recomendamos o Chrome).

Observação: para executar este laboratório, use o modo de navegação anônima ou uma janela anônima do navegador. Isso evita conflitos entre sua conta pessoal

e a conta de estudante, o que poderia causar cobranças extras na sua conta pessoal.

- Tempo para concluir o laboratório---não se esqueça: depois de começar, não será possível pausar o laboratório.

Observação: *não use seu projeto ou conta do Google Cloud neste laboratório para evitar cobranças extras na sua conta.*

Como iniciar seu laboratório e fazer login no console do Google Cloud

1. Clique no botão **Começar o laboratório**. No painel **Detalhes do laboratório** à esquerda, você verá o seguinte:

- Tempo restante
- O botão **Abrir console do Google Cloud**
- As credenciais temporárias que você vai usar neste laboratório
- Outras informações, se forem necessárias

Observação: *se for preciso pagar pelo laboratório, um pop-up vai aparecer para você escolher a forma de pagamento.*

2. Se você estiver usando o navegador Chrome, clique em **Abrir console do Google Cloud** (ou clique com o botão direito do mouse e selecione **Abrir link em uma janela anônima**). A página de **login** será aberta em uma nova guia do navegador.

Dica: é possível organizar as guias em janelas separadas, lado a lado, para alternar facilmente entre elas.

Observação: *se a caixa de diálogo **Escolha uma conta** aparecer, clique em **Usar outra conta**.*

3. Se necessário, copie o **Nome de usuário do Google Cloud** abaixo e cole na caixa de diálogo de **login**. Clique em **Próximo**.

"Nome de usuário do Google Cloud"

Copiado.

Você também encontra o **Nome de usuário do Google Cloud** no painel **Detalhes do laboratório**.

4. Copie a **Senha do Google Cloud** abaixo e cole na caixa de diálogo seguinte. Clique em **Próximo**.

"Senha do Google Cloud"

Copiado.

Você também encontra a **Senha do Google Cloud** no painel **Detalhes do laboratório**.

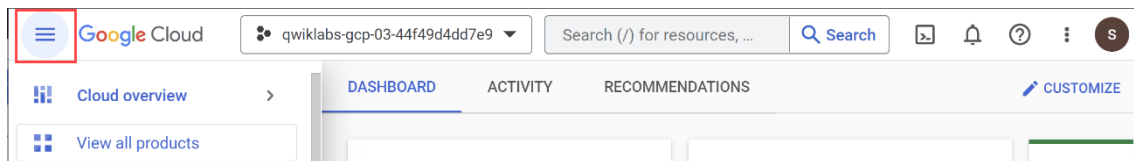
Importante: você precisa usar as credenciais fornecidas no laboratório, e não as da sua conta do Google Cloud. **Observação:** usar sua própria conta do Google Cloud neste laboratório pode gerar cobranças extras.

5. Nas próximas páginas:

- Aceite os Termos e Condições
- Não adicione opções de recuperação nem autenticação de dois fatores nesta conta temporária
- Não se inscreva em testes gratuitos

Depois de alguns instantes, o console será aberto nesta guia.

Observação: para acessar a lista dos produtos e serviços do Google Cloud, clique no **Menu de navegação** no canto superior esquerdo.



Tarefa 1: criar uma regra de firewall

Nesta tarefa, você vai criar uma regra de firewall que permite a conectividade HTTP e SSH. Também vai especificar uma tag de destino para a regra.

No Google Cloud, as regras de firewall precisam ter *destinos*, que definem as instâncias de VM sujeitas às regras. As *tags de destino* são usadas para aplicar uma regra de firewall a determinado grupo de VMs, simplificando o gerenciamento das regras. Você vai usar as tags de destino para ativar a regra de firewall apenas no servidor da Web.

1. No console do Google Cloud, clique no **menu de navegação** (≡).
2. Selecione **Rede VPC > Firewall**. A página **Políticas de firewall** será exibida.

Observação: se aparecer uma mensagem indicando que você não tem as permissões necessárias para conferir as políticas de firewall herdadas pelo projeto, ignore o aviso e continue com as próximas etapas.

3. Na barra de ferramentas, clique em **+ Criar regra de firewall**. A caixa de diálogo **Criar uma regra de firewall** será exibida.

4. Especifique os valores abaixo e não mude as outras configurações padrão:

Campo	Valor
Nome	allow-http-ssh
Registros	Ativado
Rede	vpc-net
Destinos	Tags de destino especificadas
Tags de destino	http-server
Filtro de origem	Intervalos IPv4
Intervalos IPv4 de origem	0.0.0.0/0
Na seção Protocolos e portas	<ul style="list-style-type: none">• Selecione Portas e protocolos especificados• Marque a caixa de seleção TCP• No campo Portas, digite 80, 22

5. Clique em **Criar**.

Observação: aguarde até que apareça a mensagem **A regra de firewall "allow-http-ssh" foi criada**. para continuar.


Clique em **Verificar meu progresso** para confirmar que você concluiu a tarefa corretamente.

Criar uma regra de firewall

Tarefa 2: gerar tráfego de rede HTTP

Nesta tarefa, você vai acessar o endereço IP externo do servidor da Web para gerar tráfego de rede HTTP. O tráfego gerado será registrado, e você vai conferir essas informações na Análise de registros.

Primeiro, é preciso gerar o tráfego de rede.

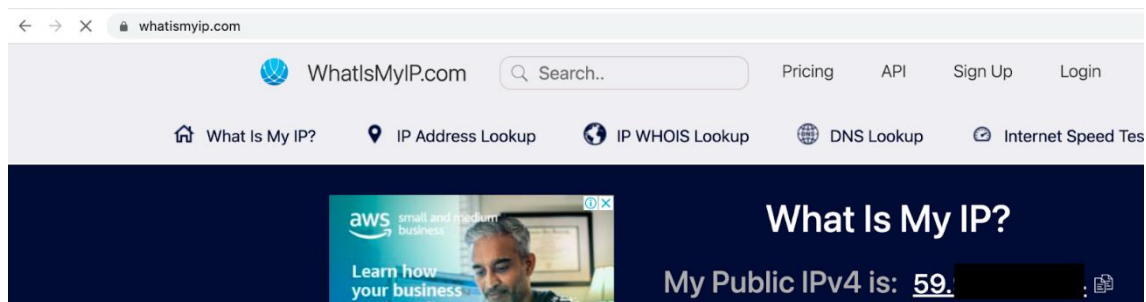
1. No console do Google Cloud, clique no **menu de navegação** ().

2. Selecione **Compute Engine > Instâncias de VM**. A página **Instâncias de VM** será aberta.
3. Em **web-server**, clique no link **IP externo** para acessar o servidor.

Outra opção é adicionar o valor de **IP externo** a **http://EXTERNAL_IP/** em uma nova janela ou guia do navegador. Uma página da Web padrão vai aparecer.

Em seguida, é preciso descobrir qual é o endereço IP do computador que você está usando.

4. Use este link para acessar seu endereço IP: whatismyip.com. Ele vai responder diretamente com o IP.



Observação: o endereço IP precisa conter apenas números (IPv4) e não deve estar no formato hexadecimal (IPv6).

5. Copie o **endereço IP** e salve no bloco de notas. Você vai precisar dele na próxima tarefa.

Clique em **Verificar meu progresso** para confirmar que você concluiu a tarefa corretamente.

Gerar tráfego de rede HTTP

Tarefa 3: analisar os registros de fluxo do servidor da Web

Nesta tarefa, você vai acessar e analisar os registros de fluxo de VPC do servidor da Web usando a Análise de registros.

1. Na barra de título do console do Google Cloud, digite **Análise de registros** no campo **Pesquisar** e clique em **Análise de registros** nos resultados da pesquisa.
2. Clique em **Fixar** ao lado de **Geração de registros de observabilidade**.
3. No lado esquerdo da página **Análise de registros** está o painel **Campos**. As seções **Gravidade** e **Tipo de recurso** estão disponíveis. Na seção **Tipo de recurso**, selecione **Sub-rede**.

Os registros de sub-redes vão aparecer no painel **Resultados da consulta**, à direita do painel **Campos**.

4. No painel **Campos**, na seção **Nome do registro**, selecione **compute.googleapis.com/vpc_flows** para acessar os registros de fluxo de VPC da rede. Se a opção não apareceu, aguarde alguns minutos para que esse tipo de registro seja exibido.

Quando você selecionar a opção, os registros de fluxo de VPC vão aparecer no painel **Resultados da consulta**.

5. No **Criador de consultas** na parte de cima da página, pressione **ENTER** ao final da segunda linha para criar outra linha.
6. Na terceira linha, copie o seguinte:

```
jsonPayload.connection.src_ip=YOUR_IP
```

Copiado.

A consulta vai ficar assim:

```
resource.type="gce_subnetwork"
```

```
log_name="projects/PROJECT_ID/logs/compute.googleapis.com%2Fvpc_flows"
```

```
jsonPayload.connection.src_ip=YOUR_IP
```

7. Substitua YOUR_IP pelo endereço IP que você anotou na Tarefa 2. A consulta vai procurar os registros de tráfego de rede originários do seu endereço IP, que você gerou na tarefa passada.
8. Clique em **Executar consulta**. Os resultados da consulta serão exibidos no painel **Resultados da consulta**.

Observação: se a opção de filtro **vpc_flows** não estiver disponível ou se não houver registros, aguarde alguns minutos e atualize. Se a opção de filtro **vpc_flows** ainda não aparecer depois de alguns minutos, acesse a página do **Compute Engine** e clique algumas vezes no **IP externo** do **servidor da Web** para gerar mais tráfego. Depois confira de novo a opção **vpc_flows**.

9. No painel **Resultados da consulta**, expanda uma das entradas de registro.
10. Na entrada, clique na seta de expansão > para expandir **jsonPayload**. Depois expanda o campo **connection**.

Aqui é possível analisar os detalhes da conexão de rede feita com o servidor da Web:

- **dest_ip:** o endereço IP de destino do servidor da Web.

- **dest_port:** o número da porta de destino do servidor da Web, que é a porta HTTP 80.
- **protocol:** o protocolo é 6, que é o protocolo IANA para tráfego TCP.
- **src_ip:** o endereço IP de origem do seu computador.
- **src_port:** o número da porta de origem atribuído ao seu computador. Segundo as normas da Internet Assigned Numbers Authority (IANA), é geralmente um número de porta aleatório entre 49152 e 65535.

Nos detalhes da entrada de registro, observe que o tráfego de rede gerado (na porta HTTP 80) foi permitido devido à regra de firewall **allow-http-ssh**, que você criou. A regra permite a entrada de tráfego nas portas 80 e 22.

According to the log entries, what is the IP address of the web server?

127.0. 0.1

255.255.255.255

10.1.3.2

0.0.0.0

Tarefa 4: criar uma regra de firewall para negar o tráfego HTTP

Nesta tarefa, você vai criar uma regra de firewall que nega o tráfego da porta 80.

1. No console do Google Cloud, clique no **menu de navegação** (≡).
2. Selecione **Rede VPC > Firewall**. A página de políticas de firewall será exibida.
3. Na barra de ferramentas, clique em **+ Criar regra de firewall**.
4. Na caixa de diálogo **Criar uma regra de firewall**, especifique os valores abaixo, sem mudar as outras configurações:

Campo	Valor
Nome	deny-http
Registros	Ativado
Rede	vpc-net

Ação se houver correspondência	Recusar
Destinos	Tags de destino especificadas
Tags de destino	http-server
Filtro de origem	Intervalos IPv4
Intervalos IPv4 de origem	0.0.0.0/0
Na seção Protocolos e portas	<ul style="list-style-type: none"> • Selecione Portas e protocolos especificados • Marque a caixa de seleção TCP • No campo Portas, digite 80

5. Clique em **Criar**.


Clique em **Verificar meu progresso** para confirmar que você concluiu a tarefa corretamente.

Criar um firewall para negar o tráfego HTTP

Tarefa 5: analisar os registros do firewall

Nesta tarefa, você vai testar a regra de firewall **deny-http**, criada na tarefa passada.

Primeiro, tente acessar o servidor da Web.

1. Clique no **menu de navegação** ()
2. Selecione **Compute Engine > Instâncias de VM**. A página **Instâncias de VM** será aberta.
3. Em **web-server**, clique no link **IP externo** para acessar o servidor.

Esta mensagem de erro vai aparecer na página:



This site can't be reached

34.139.1.60 took too long to respond.

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)

ERR_CONNECTION_TIMED_OUT

O erro ocorreu devido à regra de firewall **deny-http**, que você criou na tarefa passada. Para confirmar isso, acesse a **Análise de registros** e confira os registros de firewall do servidor da Web.

4. No console do Google Cloud, clique no **menu de navegação** (≡).
5. Selecione **Geração de registros > Análise de registros**. A página **Análise de registros** será aberta.
6. Na seção **Tipo de recurso**, selecione **Sub-rede**.
7. No painel **Campos de registro**, na seção **Nome do registro**, selecione **compute.googleapis.com/firewall** para acessar os registros de firewall da rede.
8. No **Criador de consultas** na parte de cima da página, pressione **ENTER** ao final da segunda linha para criar outra linha.
9. Na terceira linha, copie o seguinte:

```
jsonPayload.connection.src_ip=YOUR_IP DENIED
```

Copiado.

Substitua YOUR_IP pelo endereço IP que você anotou na Tarefa 2. A consulta vai procurar registros de firewall que negaram uma conexão do seu endereço IP para o servidor da Web. A consulta vai ficar assim:

```
resource.type="gce_subnetwork"
```

log_name="projects/PROJECT_ID/logs/compute.googleapis.com%2Ffirewall"

jsonPayload.connection.src_ip=YOUR_IP DENIED

10. Clique em **Executar consulta**. Os resultados da consulta serão exibidos no painel Resultados da consulta.
11. No painel **Resultados da consulta**, expanda uma das entradas de registro.
12. Na entrada de registro, clique na seta de expansão > para expandir o campo **jsonPayload**. Depois expanda o campo **connection**. Analise os detalhes da conexão de rede com o servidor da Web para confirmar que a regra de firewall foi acionada:
 - **dest_ip**: o endereço IP de destino do servidor da Web, que é **10.1.3.2**.
 - **dest_port**: o número da porta de destino do servidor da Web, que é a porta HTTP **80**.
 - **protocol**: o protocolo é **6**, que é o protocolo IANA para tráfego TCP.
 - **src_ip**: o endereço IP de origem do seu computador.
 - **src_port**: o número da porta de origem atribuído ao seu computador.
 - **disposition**: este campo indica se a conexão foi permitida ou negada. Aqui aparece **denied**, o que indica que a conexão com o servidor foi negada.
13. Na entrada de registro, clique na seta de expansão > para expandir o campo **rule_details**. Confira os detalhes da regra de firewall. Expanda os campos abaixo da entrada para conferir mais informações:
 - **action**: a ação realizada pela regra, **DENY** neste caso.
 - **direction**: a direção do tráfego da regra pode ser entrada ou saída. Aqui é **INGRESS** (entrada), então a ação será aplicada ao tráfego de entrada.
 - **ip_port_info**: o protocolo e as portas que a regra controla. Os valores de **ip_protocol** e **port_range** indicam **TCP port 80**.
 - **source_range**: as origens de tráfego em que a regra de firewall é aplicada. Aqui é **0.0.0.0/0**.
 - **target_tag**: todas as tags de destino em que a regra de firewall é aplicada. Aqui aparece **http-server**, a tag que você adicionou à regra na tarefa passada.

Analisando os detalhes da entrada de registro do firewall, percebemos que a regra **deny-http** (configurada para negar o tráfego HTTP) foi acionada. A regra negou o tráfego de rede recebido na porta 80.

Clique em **Verificar meu progresso** para confirmar que você concluiu a tarefa corretamente.

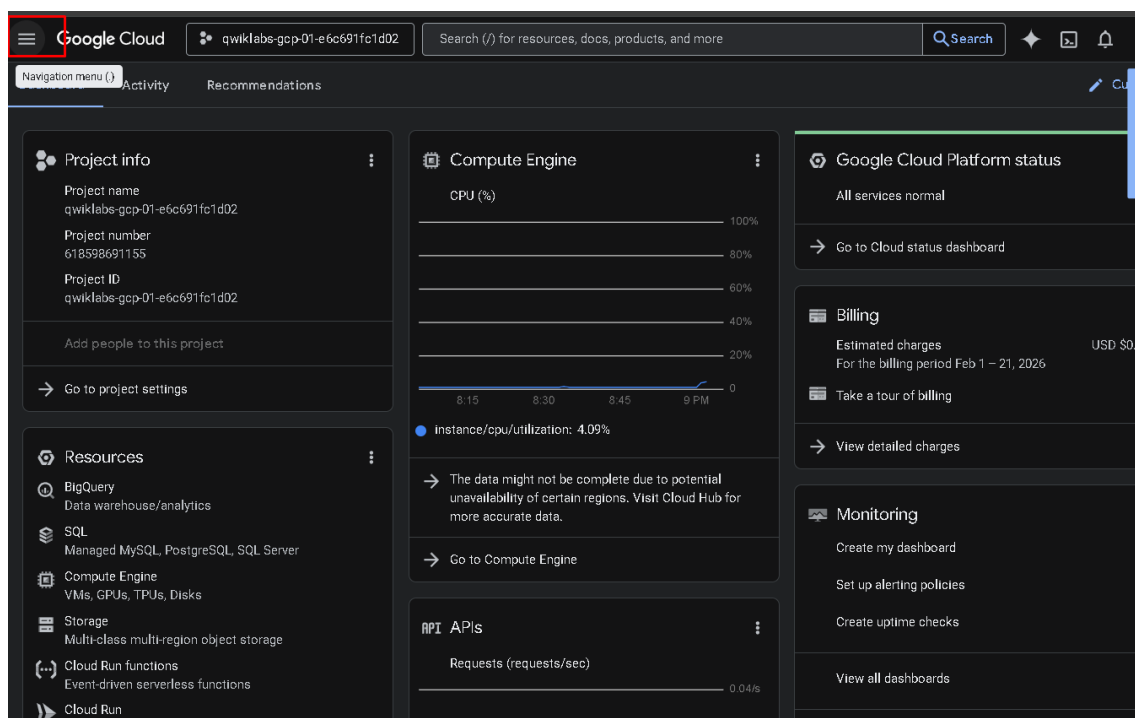
Analisar os registros do firewall

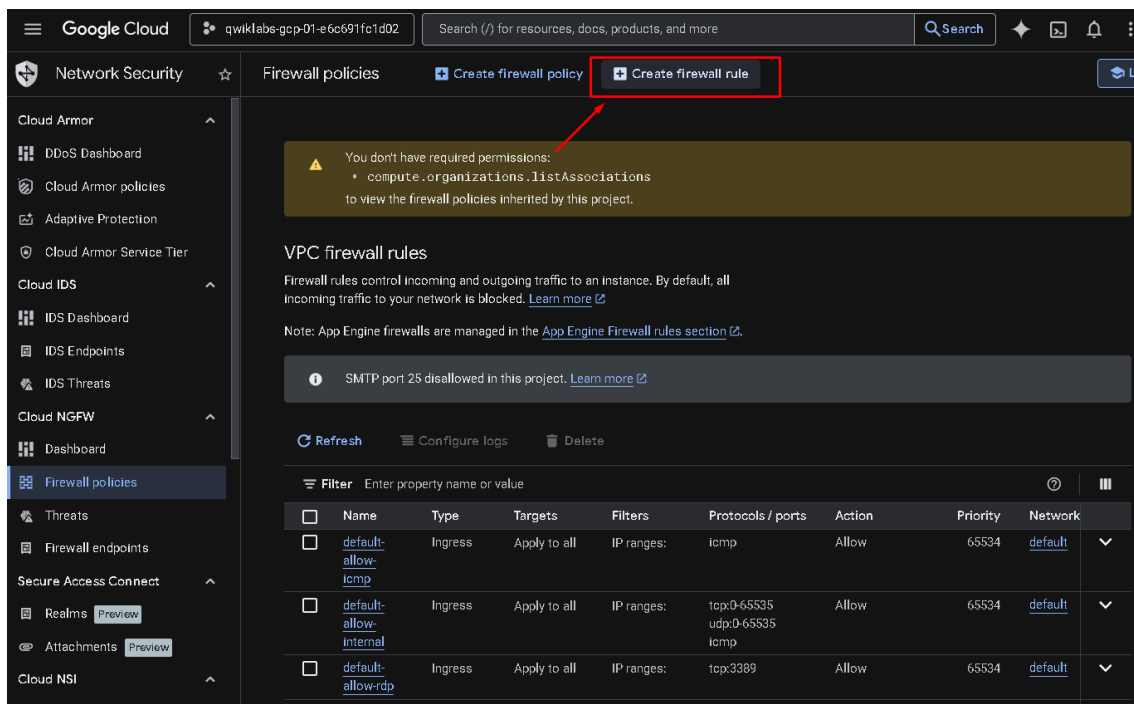
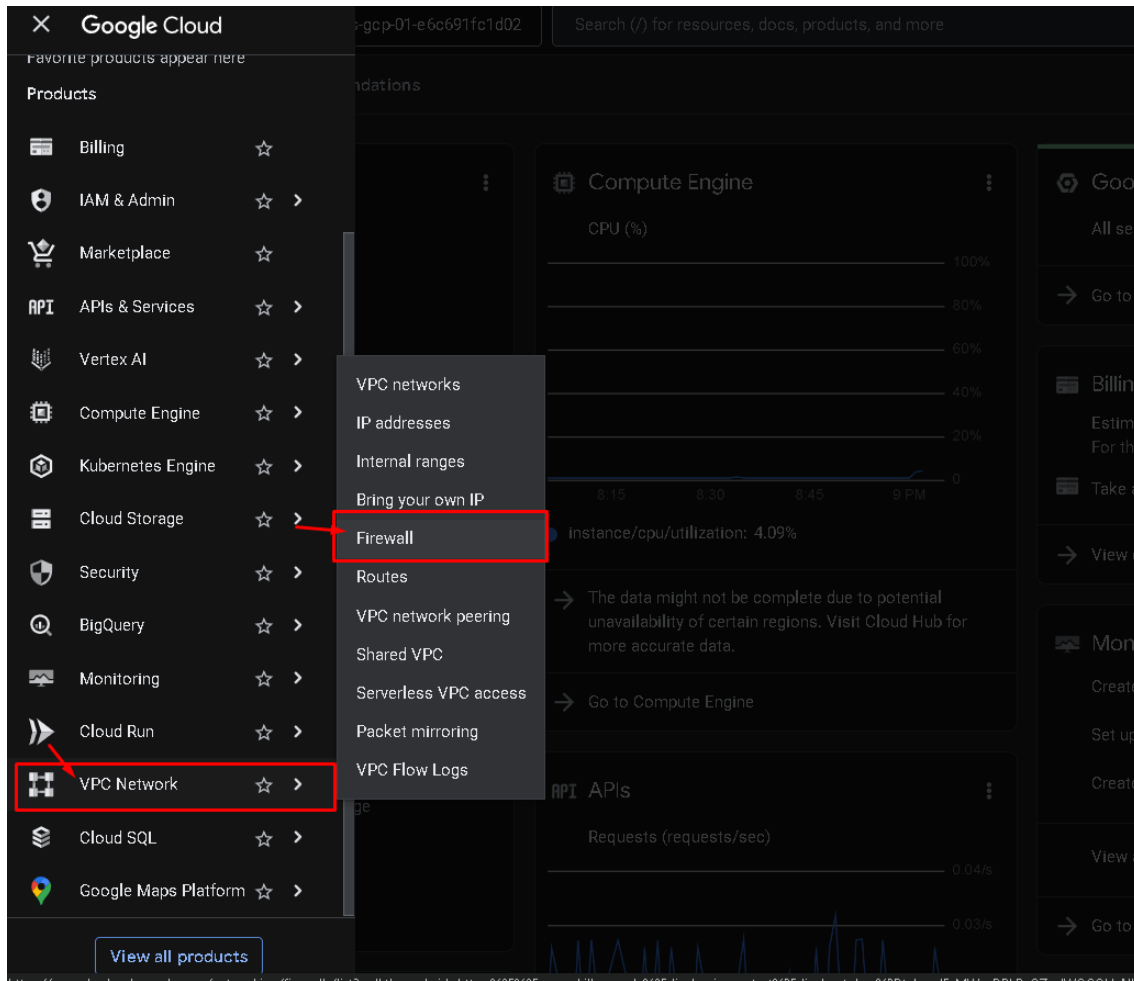
Conclusão

Bom trabalho!

Agora você tem experiência prática em criar e testar regras de firewall para um servidor da Web em um ambiente de nuvem. Ao criar regras de firewall e analisar entradas de registro, você conhece melhor os detalhes da proteção de perímetro. Isso é útil para monitorar e analisar possíveis incidentes de segurança ou ameaças, algo essencial na função de analista de segurança.

Você já pode aprender a modificar regras de firewall para garantir a máxima segurança de rede.





Google Cloud

qwiklabs-gcp-01-e6c691fc1d02

Search (/) for resources, docs, products, and more

Network Security

Cloud Armor

DDoS Dashboard

Cloud Armor policies

Adaptive Protection

Cloud Armor Service Tier

Cloud IDS

IDS Dashboard

IDS Endpoints

IDS Threats

Cloud NGFW

Dashboard

Firewall policies

Threats

Firewall endpoints

Secure Access Connect

Realms

Attachments

Cloud NSI

Deployment groups

Endpoint groups

Secure Web Proxy

Create a firewall rule

Firewall rules control incoming and outgoing traffic to an instance. By default, all incoming traffic to your network is blocked. [Learn more](#)

Name *

allow-http-ssh

Lowercase letters, numbers, hyphens allowed

Description

Permitir conectividade http e ssh

Logs

Turning on firewall logs can generate a large number of logs which can increase costs in Logging. [Learn more](#)

On

Off

Network *

vpc-net

Priority *

1000

Compare

Priority can be 0 - 65535

Direction of traffic

Ingress

Egress

Action on match

Allow

Deny

Targets

Specified target tags

Target tags *

tag

Network Security

Cloud Armor

DDoS Dashboard

Cloud Armor policies

Adaptive Protection

Cloud Armor Service Tier

Cloud IDS

IDS Dashboard

IDS Endpoints

IDS Threats

Cloud NGFW

Dashboard

Firewall policies

Threats

Firewall endpoints

Secure Access Connect

Realms

Attachments

Cloud NSI

Deployment groups

Endpoint groups

Secure Web Proxy

Create a firewall rule

Ingress

Egress

Action on match

Allow

Deny

Targets

Specified target tags

Target tags *

tag

Source filter

IPv4 ranges

Source IPv4 ranges *

0.0.0.0/0

for example, 0.0.0.0/0, 192.168.2.0/24

Second source filter

None

Destination filter

None

Protocols and ports

Allow all

Specified protocols and ports

TCP

Ports

80, 22

E.g. 20, 50-60

UDP

Direction of traffic ?

☒ Ingress

☐ Egress

Action on match ?

☒ Allow

☐ Deny

Targets

Specified target tags

Target tags *

tag

Source filter

IPv4 ranges

Source IPv4 ranges *

Second source filter

None

Destination filter

None

Protocols and ports ?

☐ Allow all

☒ Specified protocols and ports

☒ TCP

Ports

80, 22

E.g. 20, 50-60

Network Security

Firewall policies

Create firewall policy

Create firewall rule

You don't have required permissions:

- compute.organizations.listAssociations

to view the firewall policies inherited by this project.

VPC firewall rules

Firewall rules control incoming and outgoing traffic to an instance. By default, all incoming traffic to 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](#)

Refresh

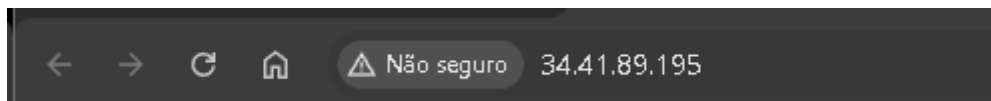
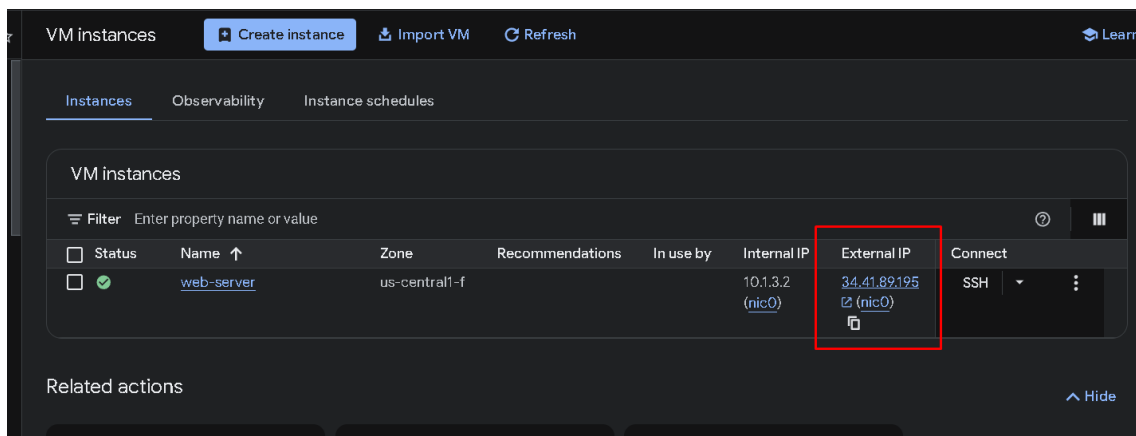
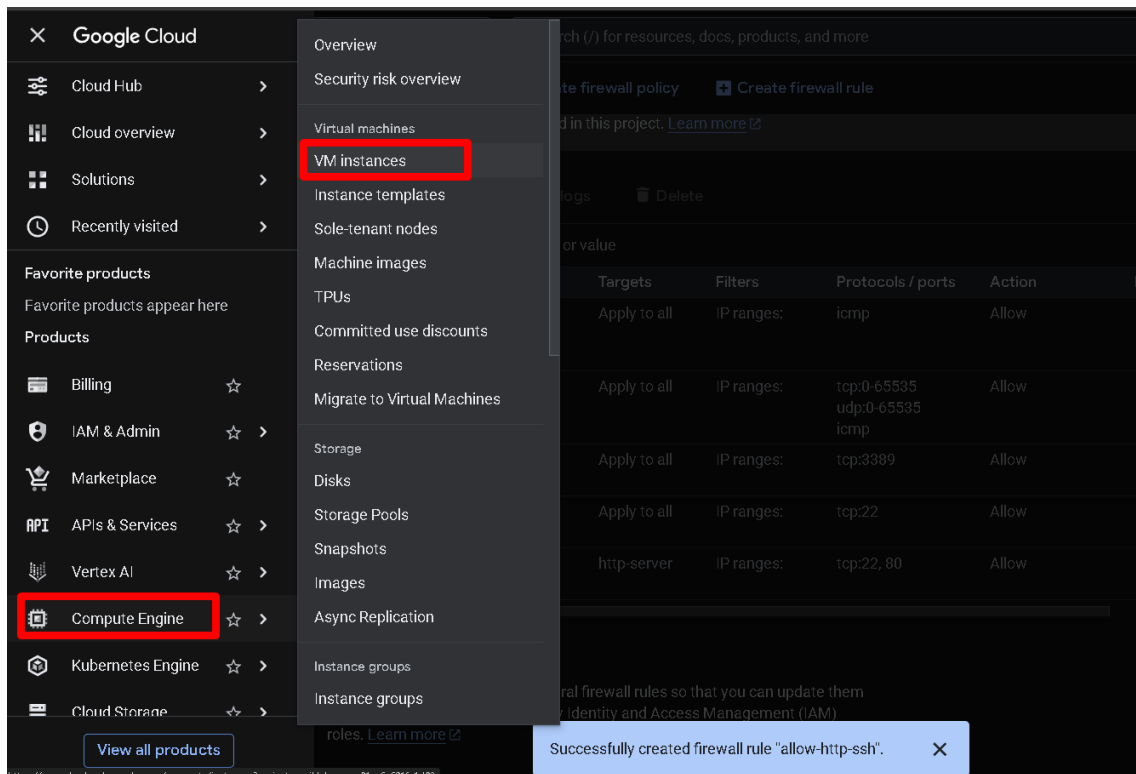
Configure logs

Delete

Filter

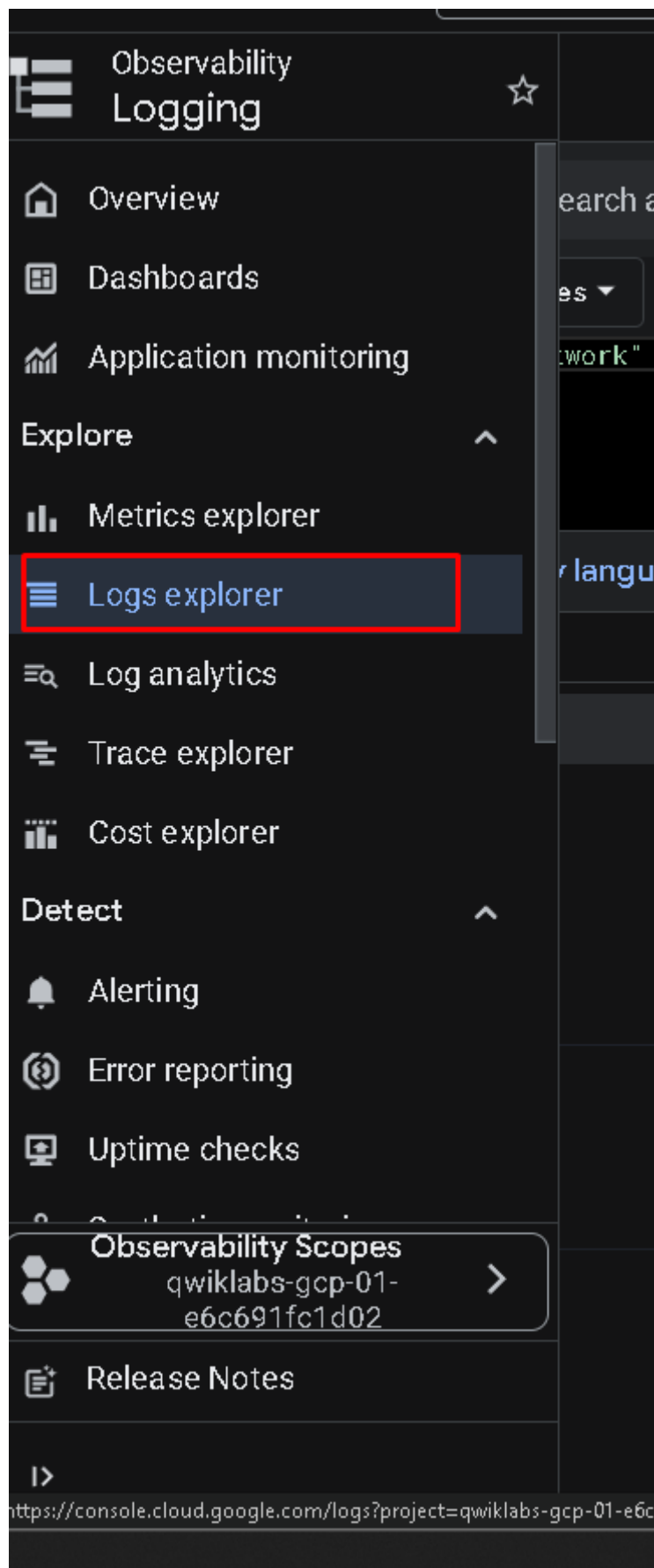
Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network	Logs	Hit count	Last hit
default-allow-icmp	Ingress	Apply to all	IP ranges:	icmp	Allow	65534	default	Off	—	—
default-allow-internal	Ingress	Apply to all	IP ranges:	tcp:0-65535 udp:0-65535 icmp	Allow	65534	default	Off	—	—
default-allow-rdp	Ingress	Apply to all	IP ranges:	tcp:3389	Allow	65534	default	Off	—	—
default-allow-ssh	Ingress	Apply to all	IP ranges:	tcp:22	Allow	65534	default	Off	—	—
allow-http-ssh	Ingress	tag	IP ranges:	tcp:22, 80	Allow	1000	vpc-net	Off	—	—

Successfully created firewall rule "allow-http-ssh".



Cymbal





Project logs

Subnetwork All log names All severities Correlate by

1 resource.type=gce_subnetwork

Example queries Query language guide

Fields

Search fields and values

System Metadata

Severity 4

Showing top 1 of 1 value

Default 4

Resource type 4

Showing top 1 of 1 value

Subnetwork X

Location 4

Log name 4

Project ID 4

Subnetwork ID 4

Timeline

4 results

Showing logs for last 5 minutes from 2/21/26, 9:36 PM to 2/21/26, 9:41 PM. Extend time by: 1 minute Edit time

Showing logs for last 5 minutes from 2/21/26, 9:36 PM to 2/21/26, 9:41 PM. Extend time by: 1 minute Edit time

Logs Explorer

Project logs Search all fields

Subnetwork vpc-flows All severities Correlate by +1 filter

1 resource.type=gce_subnetwork
2 log_name=projects/gcp-01-ec0d1f1c1802/logs/compute.googleapis.com/vpc-flows
3 compute.googleapis.com/vpc-flows

Example queries Query language guide

Fields

Search fields and values

System Metadata

Severity 3

Showing top 1 of 1 value

Default 3

Log name 3

Showing top 1 of 1 value

compute.googleapis.com/vpc-flows X

Resource type 3

Showing top 1 of 1 value

Subnetwork X

Location 3

Project ID 3

Timeline

3 results

This query has been updated. Run it to view matching entries. Run query

Showing logs for last 5 minutes from 2/21/26, 9:43 PM to 2/21/26, 9:48 PM. Extend time by: 1 minute Edit time

Showing logs for last 5 minutes from 2/21/26, 9:43 PM to 2/21/26, 9:48 PM. Extend time by: 1 minute Edit time

Example queries Query language guide

Fields

Search fields and values

System Metadata

Severity 1

Showing top 1 of 1 value

Default 1

Log name 1

Showing top 1 of 1 value

compute.googleapis.com/vpc-flows X

Resource type 1

Showing top 1 of 1 value

Subnetwork X

Timeline

1 result

Investigate log Copy Expand nested fields Hide log summary

{
 insertId: "zj1e3f2nr13j"
 jsonPayload: {
 bytes_sent: "8"
 connection: {
 dest_ip: "10.1.3.2"
 dest_ports: 80
 protocol: 6
 }
 }
}