Go to the Compute Engine page in the Google Cloud console.

Then, click on the three dots icon right next to your instance, and then click on "View network details". Your instance doesn't need to be running.

M instances	CRE/	ATE INSTANCE		M C REFRE	ESH 🕨	START STOP
= Filter VM instances						
Name ^	Zone	Recommendation	Internal IP	External IP	Connect	
🔮 w4111-instance	us-east1-b		10.142.0.2 (nic0)	35.231.49.215	SSH 🗸	:
						Start Stop Reset Delete New instance group
						View network details View logs

You should see a new screen like the one below. Click on "Firewall Rules"

	VPC network	← Network interface details				
88 13	VPC networks External IP addresses Firewall rules	Network interface details Name Network Subr nic0 default defa	network Primary intern fault 10.142.0.2	al IP Alias IP ranges Ex – 3!	xternal IP 5.231.63.56 (ephem	Network Service 1 neral) Premium
X     Routes       √>     VPC network peering       ⋈     Shared VPC		VM instance details Name Zone w4111-instance us-eas Firewall rules and routes detail Firewall rules Routes	Network tags ist1-b None ails	Service account 648548064486-compute@d	eveloper.gserviceac	:count.com
		Name T default-allow-icmp Ir default-allow-internal Ir	Type Description Ingress Allow ICMP fr Ingress Allow internal	om anywhere traffic on the default network	Targets Apply to all Apply to all	Filters IP ranges: 0.0.0.0/0 IP ranges: 10.128.0.0/9



H	VPC network	Firewall rules	+ CRE	EATE FIREWAL	L RULE C REFRES	H 👕 DELETE
28 C2	VPC networks External IP addresses 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 here.				
**	Routes	<ul> <li>Filter resources</li> <li>Name</li> </ul>	Туре	Targets	Filters	Protocols / ports
M	Shared VPC	default-allow-icmp default-allow-internal	Ingress Ingress	Apply to all Apply to all	IP ranges: 0.0.0.0/0 IP ranges: 10.128.0.0/9	icmp tcp:0-65535 udp:0-65535 icmp
		default-allow-rdp default-allow-ssh	Ingress Ingress	Apply to all Apply to all	IP ranges: 0.0.0.0/0 IP ranges: 0.0.0.0/0	tcp:3389 tcp:22

Follow these instructions. Before submitting, the form should look like the one below:

Name 👩	
flask	Write flask under Name
Description (Optional)	
Logs Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. Learn more On	
• Off	
Network 👩	
default -	
Priority  O Priority can be 0 - 65535 Check priority of other firewall rules	
1000	
Direction of traffic @ Ingress Egress	
Action on match @ Allow Deny	
Targets 😡	Targets:
All instances in the network	Select "All instances in the network"
Source filter 👩	
IP ranges 👻	
Source IP ranges 👩	Source IP ranges:
0.0.0/0 😣	Write 0.0.0.0/0 and hit enter
Second source filter	
None -	
Protocols and ports	Protocols and ports:
<ul> <li>Allow all</li> <li>Specified protocols and ports</li> </ul>	Check tcp and write 8111
✓ tcp: 8111	
udp:	
Other protocols	
protocols, comma separated, e.g. ah, sctp	
X. Dicable rule	
Create Cancel	

Click Create.

You're all set! Now your instance can receive requests on port 8111.