

## OSSEC Open-Source Getting Started

### Pre-launch:

1. Ensure that traffic is allowed on ports tcp22, udp514, udp1514, tcp1515 for either this instance or all instances. Go to the GCP VPC network section and then to firewall rules. Select create a firewall rule and create an ingress/allow rule for the aforementioned ports.

### Example:

Your free trial is waiting; activate now to get \$300 credit to explore Google Cloud products. [Learn more](#)

Google Cloud Platform Atomicorp-public

VPC network Firewall rules [CREATE FIREWALL RULE](#) [REFRESH](#) [DELETE](#)

VPC networks  
External IP addresses  
**Firewall rules**  
Routes  
VPC network peering  
Shared VPC  
Serverless VPC access

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](#).

Filter resources

<input type="checkbox"/>	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network
<input type="checkbox"/>	aeo-outbound-rule	Egress	Apply to all	IP ranges: 0.0.0.0/0	all	Allow	1	default
<input type="checkbox"/>	aeo-inbound-rule	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22,80,443,30000,1515 udp:1514,514	Allow	1	default
<input type="checkbox"/>	awp-firewall-rule2	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22,30000	Allow	1	default

Post-launch: NA