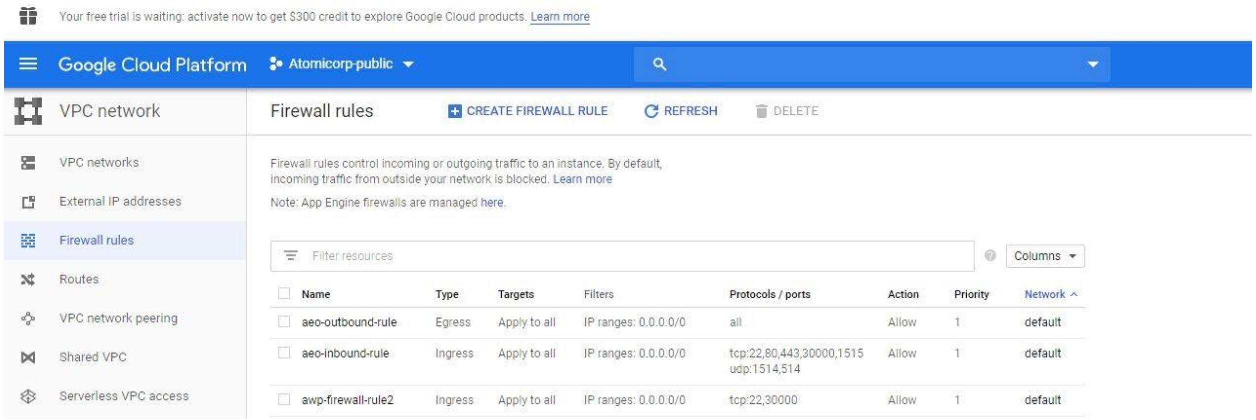
Atomicorp Enterprise Ossec Getting Started

Pre-launch:

1. Ensure that traffic is allowed on ports 22 and 30001 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 rule for tcp ports 22, 80, 443, 1515 and 30001 and udp ports 1514 and 514. Also create an egriss rule for the same ports if one doesn't already exist.

Example:



Your free trial is waiting: activate now to get $300 credit to explore Google Cloud products. Learn more

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

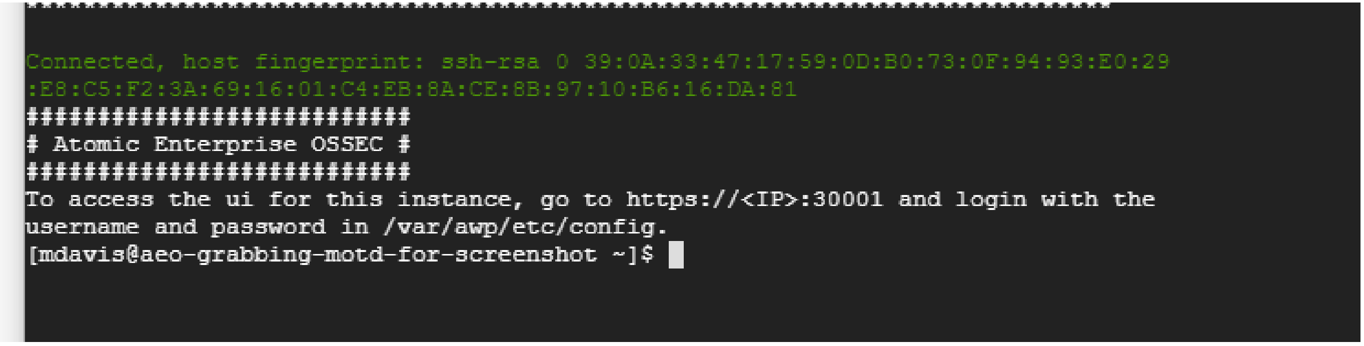
Note: App Engine firewalls are managed here.

□	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network ^
□	aeo-outbound-rule	Egress	Apply to all	IP ranges: 0.0.0.0/0	all	Allow	1	default
□	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
□	awp-firewall-rule2	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22,30000	Allow	1	default

Post-launch:

1. Upon starting the instance, wait approximately 30 minutes for background updates and scans to finish. If you have connected to the instance via ssh, you'll a line that says Atomic Eterprise OSSEC Defender: Scan complete when it is finished. You may not see this if you wait till the scan is finished before connecting. Once this is done, note the onscreen instructions.

Example:



```
Connected, host fingerprint: ssh-rsa 0 39:0A:33:47:17:59:0D:B0:73:0F:94:93:E0:29
:E8:C5:F2:3A:69:16:01:C4:EB:8A:CE:8B:97:10:B6:16:DA:81
###########################
# Atomic Enterprise OSSEC #
###########################
To access the ui for this instance, go to https://<IP>:30001 and login with the
username and password in /var/awp/etc/config.
[mdavis@aeo-grabbing-motd-for-screenshot ~]$
```

2. In order to connect an agent to the hub, run: wget http://ip_of_hub/installers/ossec-installer.sh replacing ip_of_hub with the external ip of your instance to download the agent installer. From there, run bash ossec-installer ip_of_hub replacing it as before. This should connect your agent to the hub at the specified ip.