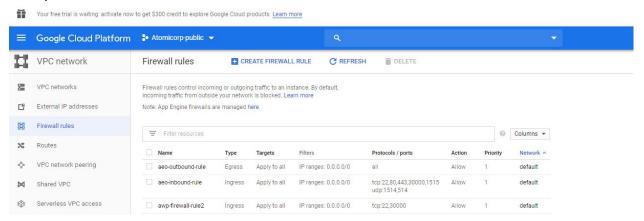
Atomicorp Enterprise Ossec Getting Started

Pre-launch:

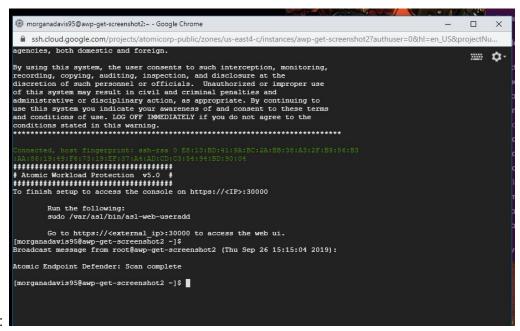
 Ensure that traffic is allowed on ports 22 and 30000 for either this instance or all instances. Go to the GCP VPC network section and then to firewall rules. Select create a firewall rule and create an ingress rule for tcp ports 22, 80, 443, 1515 and 30000 and udp ports 1514 and 514. Also create an egriss rule for the same ports if one doesn't already exist.

Example:



Post-launch:

1. Upon starting the instance, wait approximately 15 minutes for background updates and scans to finish. If you have connected to the instance via ssh, you'll a line that says Atomic Endpoint 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, follow the onscreen instructions. Only run the useradd command once unless you want to add more users. You can run the command asl by itself to see options for the asl command.



Example:

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.