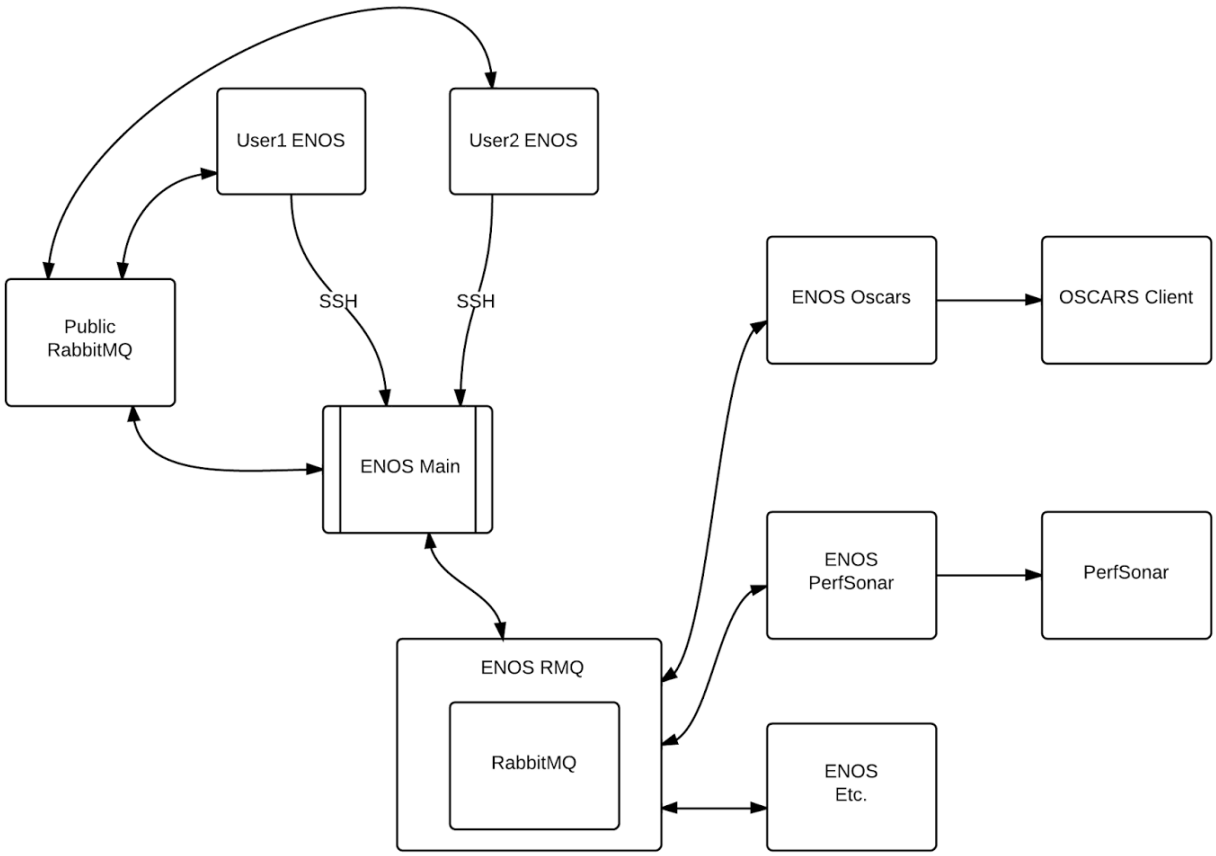
Distributed ENOS Security Model

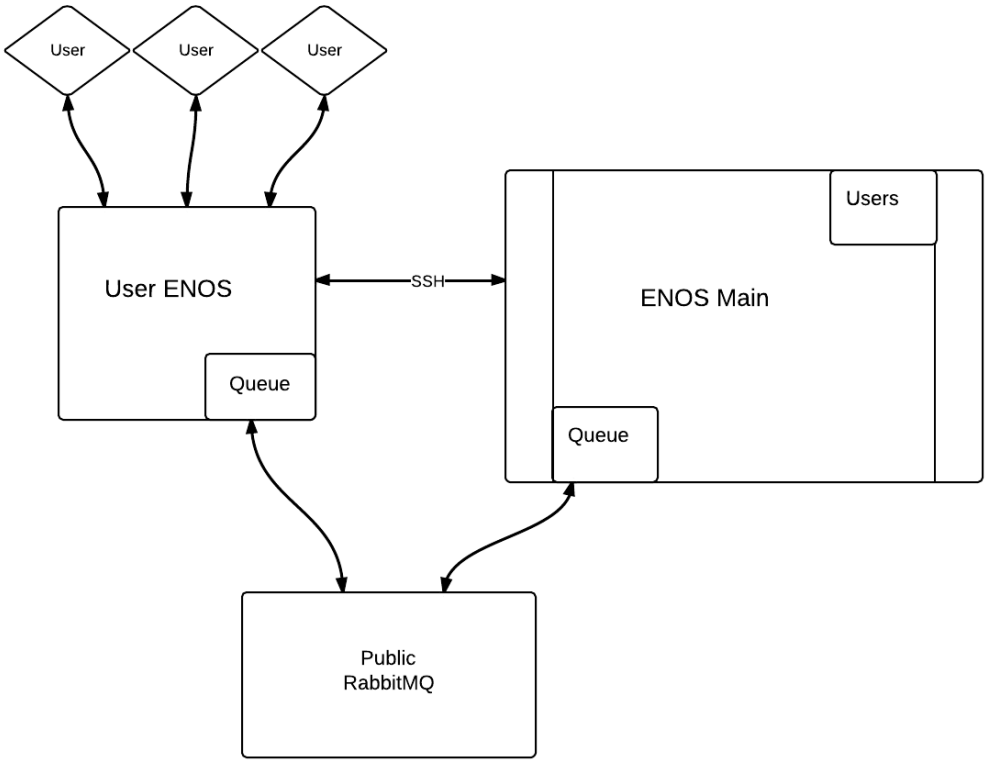


This document describes the various techniques to be implemented in ENOS to ensure the security of a distributed ENOS system and the network.

Link to this document:
https://docs.google.com/a/lbl.gov/document/d/1a90lVV1DBpzwKoCR3466_381wgVDtoTQcxckpm79H6g/edit?usp=sharing

Scaling Issues

ENOS applications are often times CPU and memory intensive. In order to better facilitate the scaling of ENOS, we can separate applications that do not involve operations on the network to run only on a user-side ENOS instance ("User ENOS"). This way, a central ENOS instance ("ENOS Main") can pass over the topology and other information to a User Enos instance, where the actual computation will occur. The user ENOS instance would first need to authenticate itself to the ENOS Main instance through SSH (perhaps eliminating this step in the future), passing along information about its local queue. Upon successful authentication, ENOS Main would create a queue for this User ENOS instance, so communication can then occur between ENOS Main and User ENOS through a Public RabbitMQ server (?Wouldn't Public RMQ server still need to be secured?). Actual users of the User ENOS Instance would then be able to run their applications on the topology without taking up CPU time on ENOS Main.



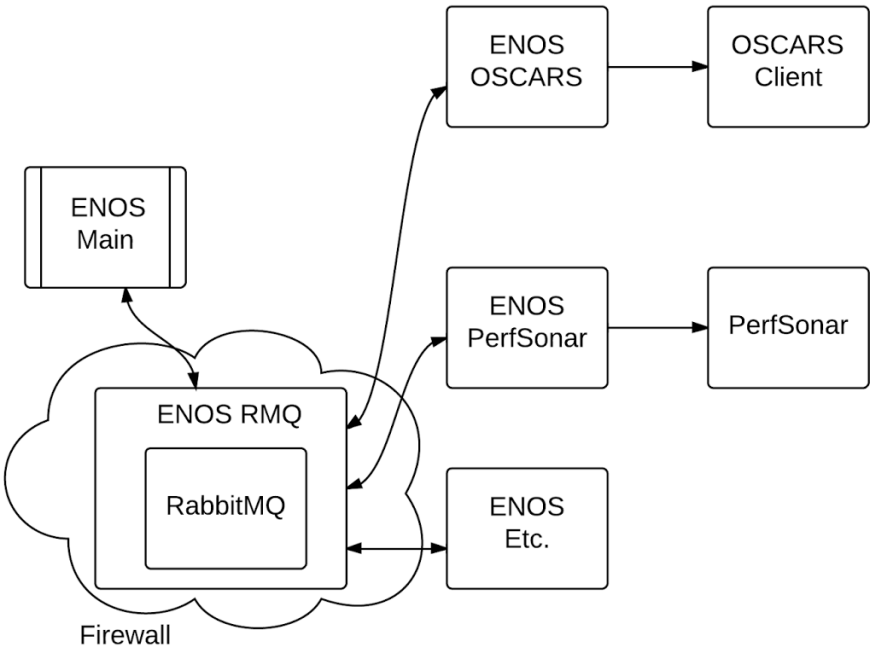
Network-altering operations

For any application that have to use a network service (i.e. OSCARS Reservations), the user in an User ENOS instance will send a request to ENOS Main. After confirming the User ENOS' privileges to perform network-altering operations, ENOS Main will then communicate to a network-altering client (such as an ENOS OSCARS instance) through RabbitMQ (RMQ).

Since the RMQ server has the ability to communicate to these network-altering clients, we must protect the RMQ server to prevent malicious activity.

This can be done by:

A. Embedding RMQ in an ENOS instance ("ENOS RMQ") where messages from ENOS Main will be routed to ENOS RMQ, which will then check whether the message should be forwarded to the RMQ server. This way, any user must go through this security layer before actually sending messages.
B. Having nothing else on the VM where the RMQ server will be located
C. Having a firewall that restricts network traffic to the RMQ server



ENOS Main Connection to Client ENOS Instances

Once a User ENOS instance is authorized to use a network-altering application, the ENOS Main instance must then send the request to the proper Client Application. In order for this to occur, a map that links Java class names to RMQ Queue names is utilized. ENOS Main queries this table to determine which queue a message should be sent through in order to reach the correct client application. Only privileged users may add entries to this table, preventing messages from being misrouted maliciously.