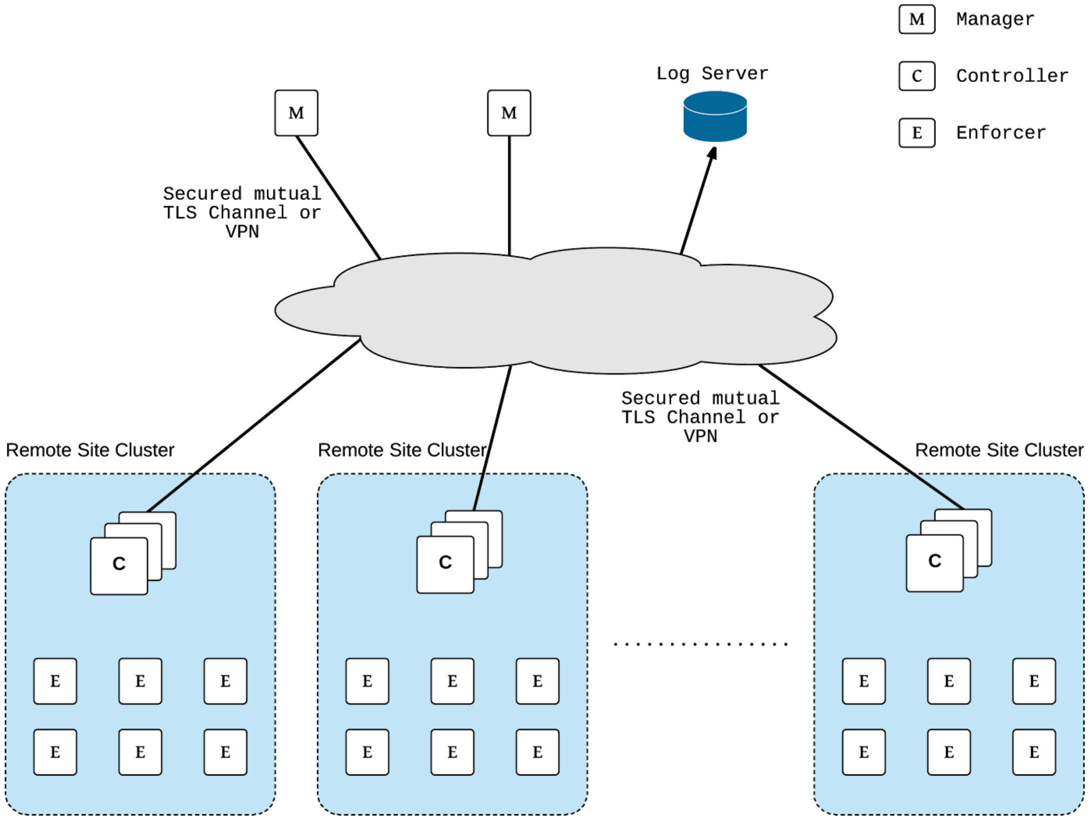
Multi-site Container Security Proposal

Multi-site container security architecture is designed for the following use case.

1. There are large number of remote sites. Each site has a container deployment;
2. Communication between applications of these sites are rare;
3. Upstream network connection of each site has limited bandwidth.

The following diagram captures the proposed architecture.



Each blue box in the diagram represents a remote site cluster. There are multiple container hosts running in each cluster. Each host has one NeuVector enforcer deployed.

Multiple NeuVector controllers are deployed in each cluster to support High Availability, so services are not interrupted and security is not compromised when container hosts fail or when controller upgrade is needed.

NeuVector managers can be created on demand to manage controllers running in the remote cluster.

There are several advantages about this architecture,

1. High scalability - controllers only manage the local container cluster of each site. Large number of remote clusters are supported.
2. Minimal overhead added to the remote cluster's upstream network connection, because only the management messages and filtered log reports use the connection.
3. High availability in each remote cluster.
4. Controllers expose REST APIs. They can be used by the manager or other software to manage remote sites' security policies.
5. Communications between managers and the remote sites are secured.
6. Managers can be created on demand to reduce attack surfaces.