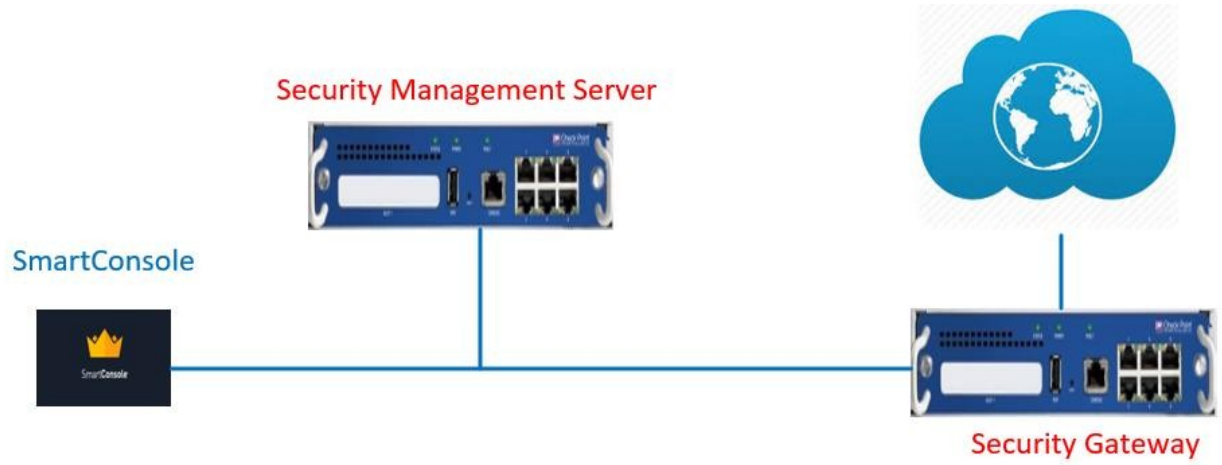
Deployment Options:

There are different deployment scenarios for Check Point software products. Distributed Deployment, Standalone Deployment, Routed Mode, Transparent mode, ClusterXL Mode, Standalone Full HA and Management High Availability HA.

Distributed Deployment:

Gateway and the Security Management server are installed on separate machines. In Distributed deployment, the communication between Gateway and Management servers happens via Secure Internal Communication or SIC. if Security Management Server and Security Gateways are installed in different virtual machines or deployed as different appliances, then it is referred as Distributed mode of installation.



Standalone Deployment:

The Security Management server and the gateway are installed on the same machine. With small environments, it’s possible to have the Management Server and Gateway on the same hardware. This is called Standalone deployment. If Security Management Server and Security Gateway are installed together, then it's called as a Standalone Mode of Installation.

Routed Mode:

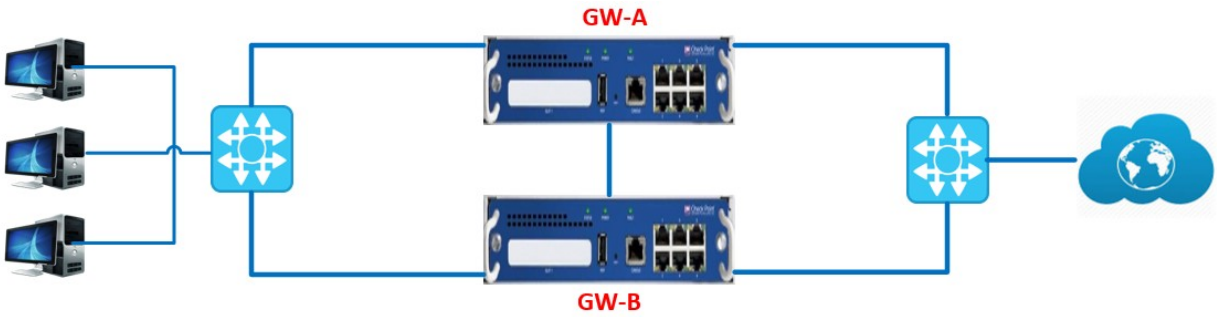
Routed Mode is the most common. In this case, Security Gateway performs L3 routing when forwarding traffic allowed by Security Policy. This is a regular and standard method used to deploy Security Gateways. You usually use this mode when you deploy the Security Gateway at the perimeter. In this case, the Security Gateway behaves as an IP router that inspects and forwards traffic from the internal interface to the external interface and vice versa. Both interfaces should be located and configured using different network subnets and ranges.

Bridge Mode:

Bridge Mode or Transparent mode can be deployed without changing network topology, to control traffic on Layer 2. Some functionality is limited in this mode. This deployment method lets you install the Security Gateway as a Layer 2 device, rather than an IP router. The benefit of this method is that it does not require any changes in the network infrastructure. It lets you deploy the Security Gateway inline in the same subnet. This deployment option is mostly suitable when you must deploy a Security Gateway for network segregation and Data Center protection purposes.

ClusterXL Mode:

A ClusterXL cluster is a group of identical Check Point Security Gateways connected in such a way that if one fails, another immediately takes its place. ClusterXL is a software-based Load Sharing and High Availability solution that distributes network traffic between clusters of redundant Security Gateways and provides transparent failover between machines in a cluster. ClusterXL also handles state synchronization to maintain connections in case of a failover.



Management HA:

A Primary and Secondary Security Management server are configured. The databases of the Security Management servers are synchronized, either manually or on a schedule, so they can back up one another. The administrator makes one Security Management Server Active and the other Standby. If the Active Security Management server is down, the administrator can make the Standby Server Active. In Management High Availability, the Active Security Management server always has one, or more, backup Standby Security Management servers that are ready to take over from the Active Security Management server, in case of failure. This must all be of the same OS and version. The database of objects and users, policy information and ICA files are stored on both the Standby Security Management server, as well as on the Active Security Management server. These are synchronized, so that data is maintained and ready to be used. If the Active Security Management server is down, a Standby Security Management server needs to become active, in order to be able to edit and install the Security Policy.