

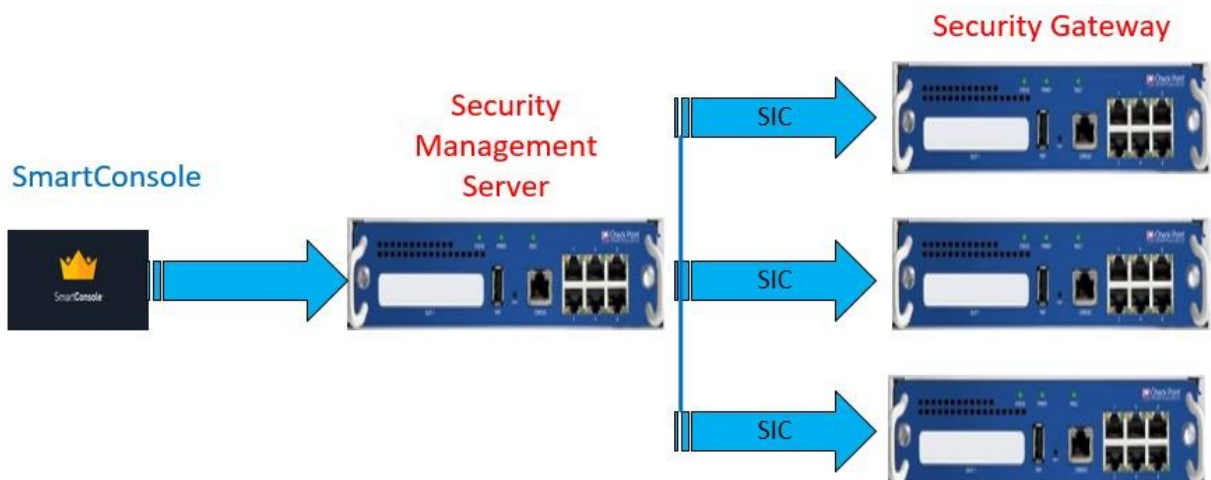
Three Tier Architecture:

The main product of Check Point is the network security solution – Next Generation Firewall (NGFW). When working with it, you will encounter three main components: Security Gateway (SG), Security Management Server (SMS) and SmartConsole. Three-Tier Architecture defines how checkpoint components are inter-related and how these components work in like a concert. Each Component is responsible for its defined set of tasks.



Security Gateway:

The software component that enforces the organization's security policy and acts as a security enforcement point. Security Gateway is the firewall where firewall software is installed and do State Full Inspection. The security gateway enforces the organization's security policy and acts as a security enforcement. Security Gateway is responsible for performing Access Control and Threat Prevention. Security Gateway (SG) is usually deployed on the perimeter to control and secure traffic with Firewall and Threat Prevention capabilities. Security Gateway intercepts and inspects all inbound and outbound packets on a Gateway. Security Gateway is responsible to protect the network. Firewall is based on Stateful inspection.



Security Management Server:

The server used by the system administrator to manage the security policy. The organization's databases and security policies are stored on the Security Management server and downloaded to the gateway. All the actual policies and configurations would be stored in the management server. When you open the smart console, you access the checkpoint management appliance with it. In the PaloAlto Firewall, you may know that you can manage all the firewalls using the Panorama device. In Checkpoint, we use the same method but here it is called Checkpoint Management Server. Security Management Server stores and distribute security policies to multiple security gateways. Security Management Server acts like a CA Server and Log Server. Stores Users, Groups and Permission database. You can create Certificates for users and administrator for authentication purpose. As a database it stores network-object definitions, user definitions, security polices and log files for firewalled gateways.

SmartConsole:

GUI applications that are used to manage various aspects of security policy enforcement. For example, SmartView Tracker is a SmartConsole application that manages logs. It's a GUI application with the help of GUI client an administrator can configure security policy for all entire organization. SmartConsole is a GUI administration tool to connect to SMS. Through this tool, a security administrator is able to prepare and apply security policies to the Security Gateways. Security Administrator opens SmartConsole and connects to the Security Management Server.

