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, Security Management Server 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 Management Server:

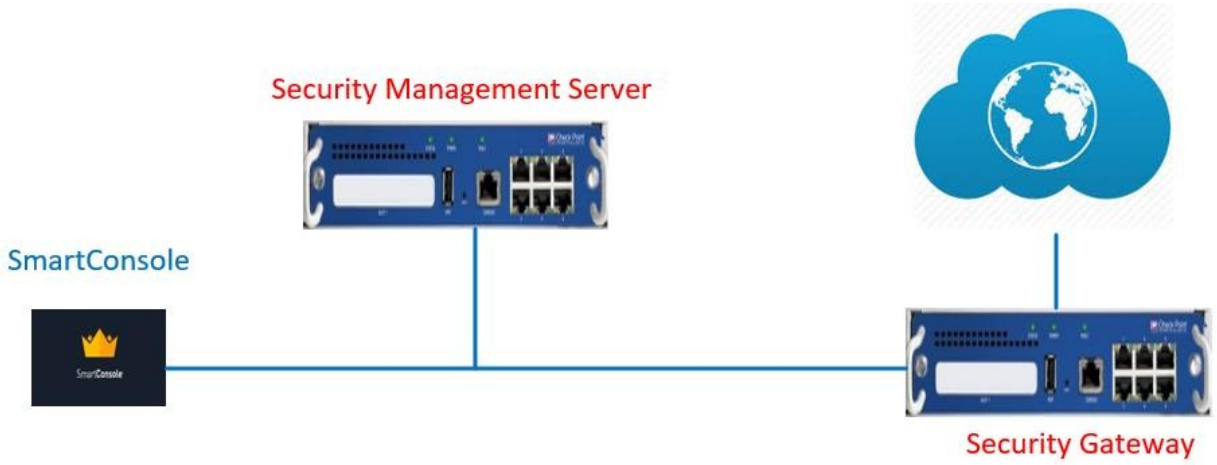
The server used by the system administrator to manage the security policy. The organization's databases and security policies are stored on the Security Management server and downloaded to the gateway. All the actual policies and configurations would be stored in the management server. When you open 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.

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.

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:

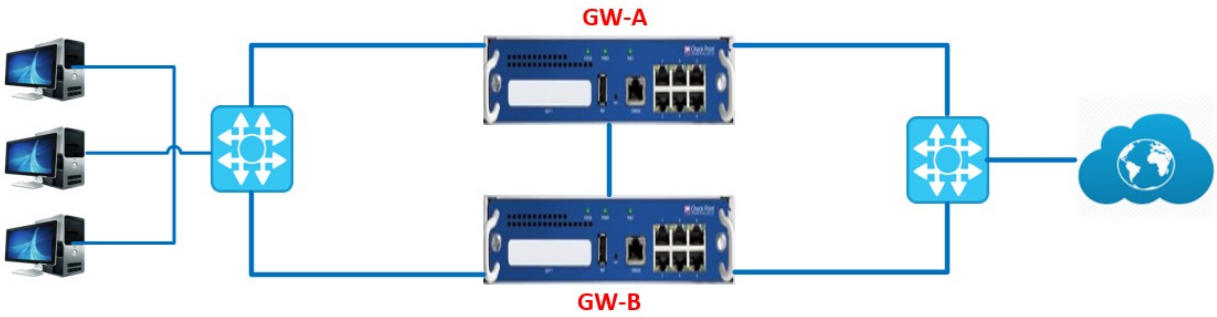
Routed Mode is the most common. In this case, Security Gateway performs L3 routing when forwarding traffic allowed by Security Policy. This is a regular and standard method used to deploy Security Gateways. You usually use this mode when you deploy the Security Gateway at the perimeter. In this case, 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.



Software Blades:

Software Blades Check Point is using this term for specific features of its products. Security Gateways and Management Servers have collections of related Software Blades that one can enable or disable when required, depending on licensing.


Firewall


Mobile Access


Identify Awareness


Application Control

URL Filtering

DLP


IPS


Anti-Bot


Anti-Virus


Anti-Spam


Sandblast Threat Emulation

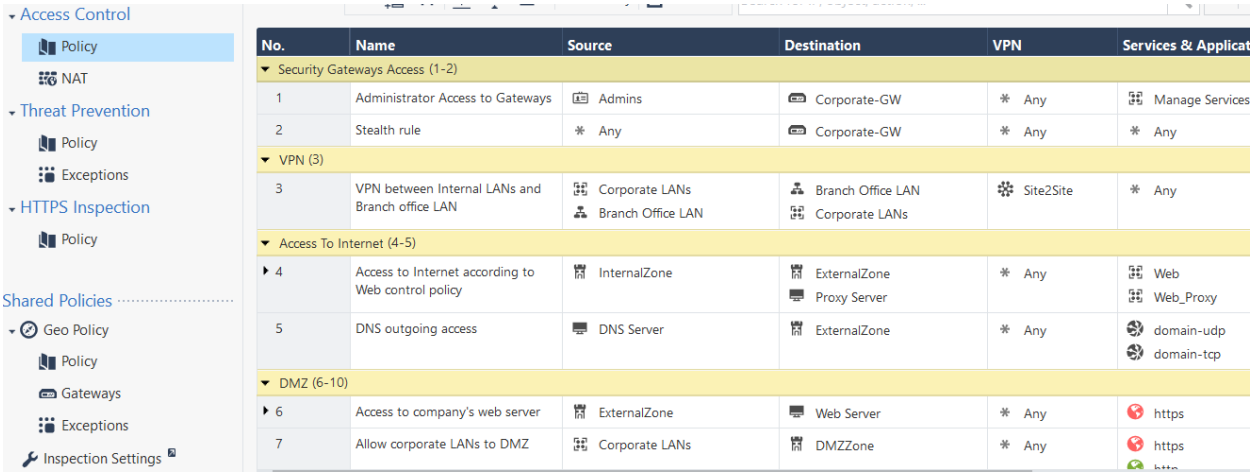

Sandblast Threat Extraction

Secure Internal Communication SIC:

It stands for Secure Internal Communication and it is a Checkpoint propertiory Protocol.
It is a where a secured tunnel is created with enforcement module and management server and from management server to management console. The protocol used between Checkpoint security gateway and the management server communication is called Secure Internal Communication (SIC) protocol. Secure Internal Communication (SIC) let's Check Point platforms and products authenticate with each other. The SIC procedure creates a trusted status between gateways, management servers and other Check Point components.

Security Policy:

The policy created by the system administrator that regulates the flow of incoming and outgoing communication. The security gateway is the checkpoint firewall, and all the firewalls are again connected to the management server. And when you open the management server via smart console, you should be able to see all the security gateways and the management servers inside it.



Gaia:

IPSO was the initial version, based on BSD (Nokia's IPSO). Check Point IPSO is the operating system for the 'Check Point firewall' appliance and other security devices, based on FreeBSD, with numerous hardening features applied. In 2009, Check Point acquired the Nokia security appliance business, including IPSO, from Nokia. Check Point IPSO is no longer maintained by Check Point. Afterward, SecurePlatform (SPLAT), based on RedHat.

Gaia is the latest version of Checkpoint which is a combination of SPLAT and IPSO. Gaia is the Check Point next generation operating system for security applications. In Greek mythology, Gaia is the mother of all. The Gaia Operating System supports the full portfolio of Check Point Software Blades, Gateway and Security Management products. Gaia is a unified security Operating System that combines the best of Check Point original operating systems, and IPSO, the operating system from appliance security products. Gaia is available for all Check Point Security Appliances and Open Servers.

Here are some benefits of Gaia as compare to SPLAT/IPSO.

1. Web-Based user interface with Search Navigation
2. Full Software Blade support
3. High connection capacity
4. Role-Based administrative Access
5. Intelligent Software updates
6. Native IPv4 and IPv6 Support
7. ClusterXL or VRRP Clusters
8. Manageable Dynamic Routing Suite
9. Full Compatibility with IPSO and SecurePlatform.

Firewall	OS
Check Point Firewall	IPSO and Gaia (Linux-based)
FortiGate Firewall	FortiOS, Based on the Linux kernel
Palo Alto Firewall	PAN-OS, Based on the Linux kernel
Juniper SRX	Junos