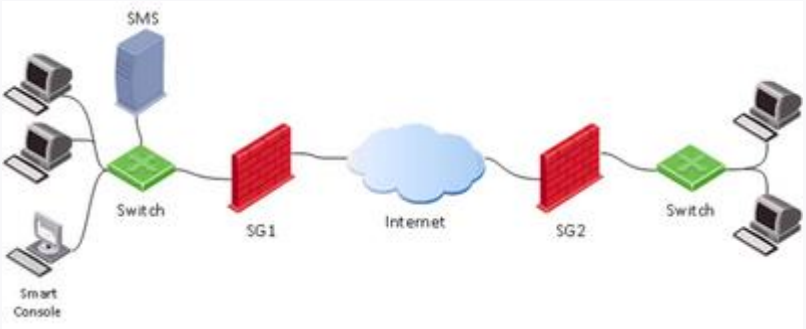
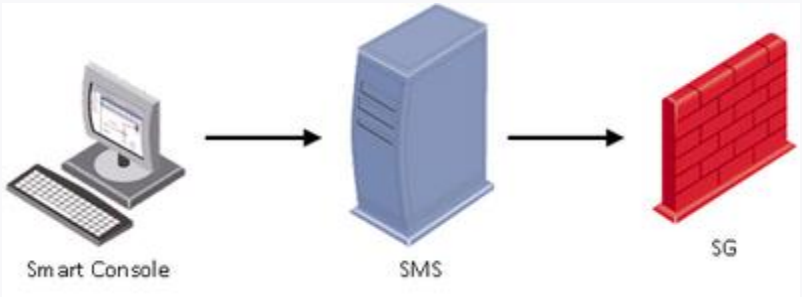
# Network Defense. Three Tier Architecture components

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.




1. Security Gateway (SG) is usually deployed on the perimeter to control and secure traffic with Firewall and Threat Prevention capabilities.
2. Security Management Server (SMS) defines and controls security policies on the Gateways. It can also be used to as a log server with built-in system of log indexing (SmartLog) and event correlation (SmartEvent – a SIEM-like solution for Check Point products). Usually, SMS is the main element of central management with multiple Security Gateways in operation. Nevertheless, you need an SMS even if your security system has a single gateway only.
3. 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.

Administration process includes the following steps:



1. Security Administrator opens SmartConsole and connects to the Security Management Server.
2. Security Administrator changes the existing (or defines a new) security policy and applies the changing by pressing Install Policy button.
3. Security Management Server verifies policy for consistency to avoid logical errors, compiles it and send the result policy package to a Security Gateway.
4. Security Gateway receives the compiled policy and applies it to the network traffic crossing the gateway.

# Operating Systems

Historically, Check Point Software Technologies was oriented to different OSs: SUN, AIX, HP-OS, various flavors of Linux and Windows, IPSO, Secure Platform (SPLAT) and others. Today three component of Check Point are using the following Operating Systems:

1. Windows – for SmartConsole only. SG and SMS cannot be deployed on Windows.
2. Gaia – Check Point own OS based on hardened RH Enterprise Linux. Gaia will be the focus of some further materials, as it is the main option when deploying both SMS and SG on open server platform and Check Point appliances.

Note: Check Point SMB appliances based on ARM processors are using Gaia Embedded OS, which is a stripped and optimized version of Gaia.

# Software Versions

At this moment Check Point supports three main software versions of its products:

- R77.30
- R80.10
- R80.20

R77.30 is planned to go out of support in May 2019. R80.20 was released at the end of September 2018.

# Deployment option

There are different deployment options for a Network Security System based on Check Point products:

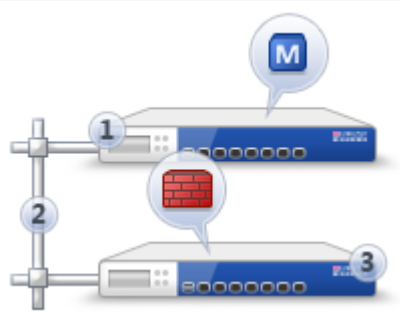
1. **Check Point Security Appliance**. This option includes both hardware and software required to run Check Point Network Security System.

2. **Open Server**. Gaia OS can be deployed on specific certified servers from a Hardware Compatibility List available on Check Point web site.
3. **A Virtual Machine**. Gaia supports VMware ESX and the most popular public cloud platforms: AWS, Azure, Google Cloud, Alibaba, and Oracle.

# Standalone and Distributed Deployment

Security Gateway and Security Management Server components can be deployed on the same hardware of VM (Standalone):


or as different entities (Distributed Deployment).




Standalone option is economical but also limited, especially when talking about performance.

Distributed is the most popular and deployment option for Check Point customers. For some specific functions, such as SmartEvent, distributed deployment is a requirement.

# Gateway Deployment

Security Gateway is deployed in a **Routed Mode** or a **Bridge Mode**.

**Routed Mode** is the most common. In this case, Security Gateway performs L3 routing when forwarding traffic allowed by Security Policy.

**Bridge Mode** can be deployed without changing network topology, to control traffic on Layer 2. Some functionality is limited in this mode.

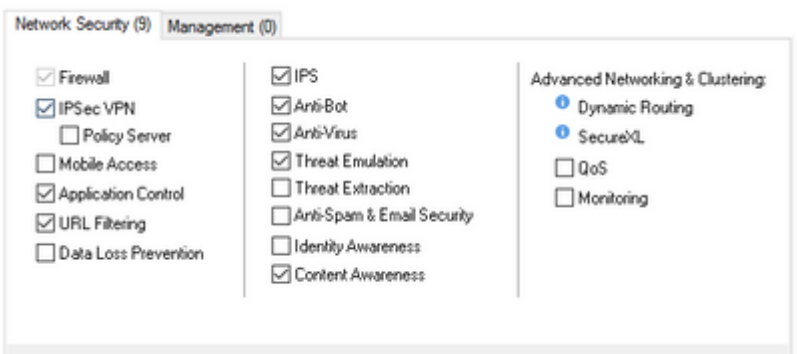
# Check Point Software Blades

One of the most frequent questions beginners have is about the term “Software Blades”. In plain words, 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. Combination of those defines specific flavor of Check Point products.

We will be addressing most of the Software Blades and their functions in the further CP4B materials. However, it worth listing all Software Blades available for Management and Gateways here.

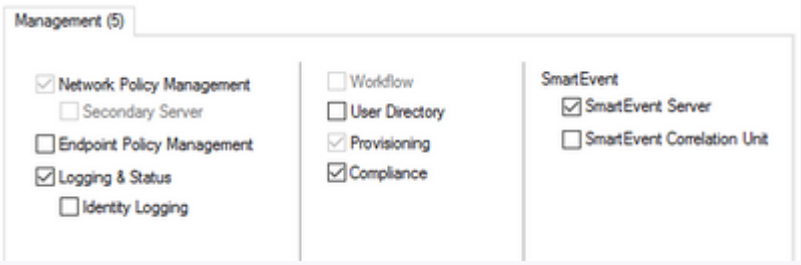
## Security Gateway Software Blades




- **Firewall** – Basic security filtering functionality
- **IPSec VPN** – functionality for creating IPSec-based Site to Site Virtual Private Networks
- **Mobile Access** – SSL and IPSec Endpoint VPN solution
- **Application Control & URL Filtering** – Advanced Security solution to control Web URL and Application traffic through the gateway
- **Data Loss Prevention** – Pre-emptively prevent sensitive information from leaving the organization, educate users on proper data handling procedures, and allow remediation in real-time
- **IPS** – Intrusion Prevention System

- **Anti-Bot** – blade to detect and prevent Advanced Persistent Threats (APT) activity within the protected network
- **Anti-Virus** – AVI scanning on the fly for downloads and uploads crossing Security Gateways
- **Threat Emulation** – Sandboxing solution for downloads and email attachments
- **Threat Extraction** – Unique technique to remove active content from downloads and attachments to prevent incidental malware infections and APT
- **AntiSpam & Email Security** – email protection blade
- **Identity Awareness** – Provides visibility to the identities of end users and the specific Active Directory host they are connecting from. This allows security policies to be enforced based on any combination of user, specific machine, or network.
- **Content Awareness** – Control over specific types of content data files crossing Security Gateways
- **QoS** – Quality of Service, traffic shaping and prioritization functionality
- **Monitoring** – Real Time Monitoring of performance and traffic indicators for Security Gateways

# Security Management Server Software Blades




- **Network Policy Management** — to create and manage SG security policies
- **Endpoint Policy Management** — to create and manage Endpoint Security Policies
- **Logging & Status** – central logging and log consolidation functionality
- **Workflow** — Change Management Cycle functionality with ability to audit and approve certain policy management operations
- **User Directory** — User management and integration with external authentication solutions
- **Provisioning** — Centralized maintenance tool
- **Compliance** — Automated compliance tool for security and best practices audits
- **SmartEvent** — Log correlation and Security Events management tool