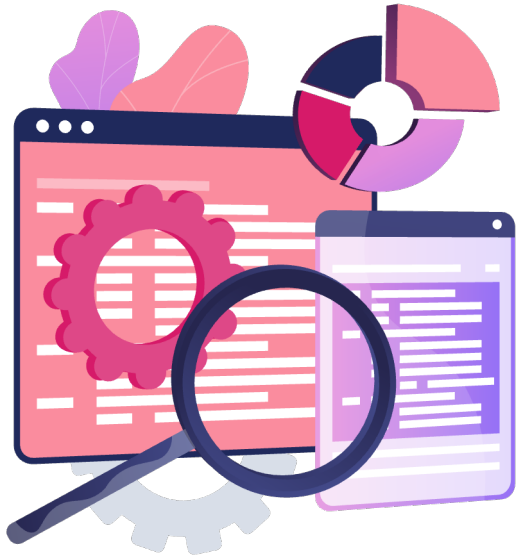
CHAPTER 1

INTRODUCTION TO CHECK POINT QUANTUM SECURITY MANAGEMENT

YOU DESERVE THE BEST SECURITY

Learning Objectives

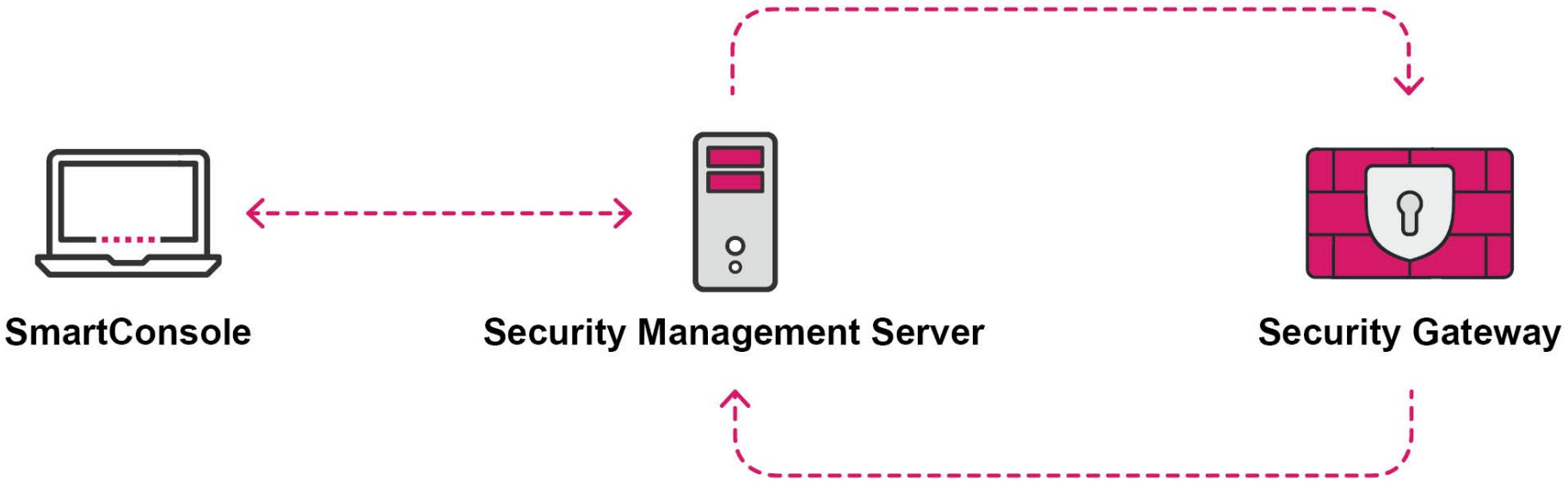
- Describe the primary components of a Check Point Three-Tier Architecture and explain how they work together in the Check Point environment.
- Define and explain the differences between standalone and distributed deployments.
- Explain how communication is secured and how traffic is routed in the Check Point environment.



©2023 Check Point Software Technologies Ltd.

SECURITY MANAGEMENT OVERVIEW

Primary Components of the Three-Tier Architecture



©2023 Check Point Software Technologies Ltd.

SMARTCONSOLE

SmartConsole - Common Uses

Create and Manage

- Security Policies
- User and administrator accounts
- Management Servers, Gateways, and other devices
- Settings for Check Point environment

Monitor

- Logs and events
- Performance
- Regulation compliance

Maintain

- Licenses
- Update products

©2023 Check Point Software Technologies Ltd.

SmartConsole is a tool. It does not store the policy or configuration information.

SmartConsole sends this information to the Security Management Server for storage.

©2023 Check Point Software Technologies Ltd.

Types of SmartConsole Interfaces

Desktop Clients

- SmartConsole Client
- Portable SmartConsole

Clientless, Browser-based Interface

- Web SmartConsole

©2023 Check Point Software Technologies Ltd.

SmartConsole Installation Packages

- SmartConsole Client and Portable SmartConsole are available from:
  - Check Point Quantum R81.20 Home Page (sk173903)
  - Check Point Support Center
  - Gaia Portal
  - Security Management Server
- The installation packages are downloaded as an executable (exe) file.
- Web SmartConsole is accessed from a Web browser. No installation is required

©2023 Check Point Software Technologies Ltd.

SmartConsole Client

- Desktop client is installed on a Windows platform.
  - Does not support the Check Point Gaia operating system.
- To log into SmartConsole, you must have one of the following:
  - Valid credentials (username and password)
  - Valid certificate
- SmartConsole must be able to connect to an operational Security Management Server.

©2023 Check Point Software Technologies Ltd.

Portable SmartConsole

- Deployed without the SmartConsole installer.
- Encapsulates content into directory so it can be moved to a portable device.
- Supported on R81.10 or higher.

©2023 Check Point Software Technologies Ltd.

Portable SmartConsole

- Before installing and using a Portable SmartConsole, you must install the relevant SmartConsole GUI Client on the same computer.
- Administrator credentials are not required to install Portable SmartConsole on the Windows host.

For additional information, refer to sk116158 - Portable SmartConsole for R80.x and R81.x.

©2023 Check Point Software Technologies Ltd.

Web SmartConsole

- Clientless access from a web browser.

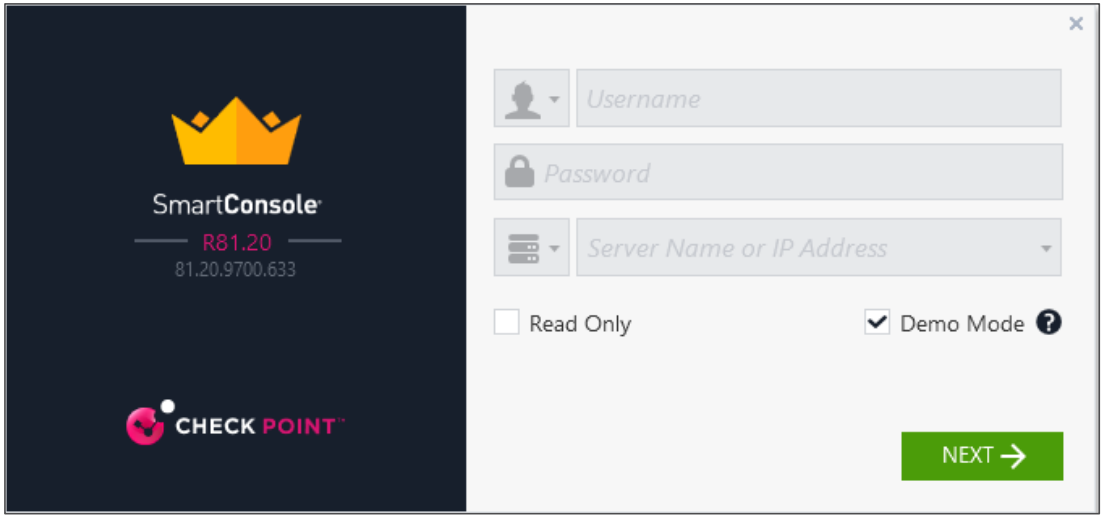
  `https://<management server IP address>/smartconsole`

- Requires R81.10 and R81 Jumbo Hotfix Accumulator Take 10 or higher.
- Google Chrome is recommended browser.
- See sk170314.

©2023 Check Point Software Technologies Ltd.

SmartConsole Demo Mode

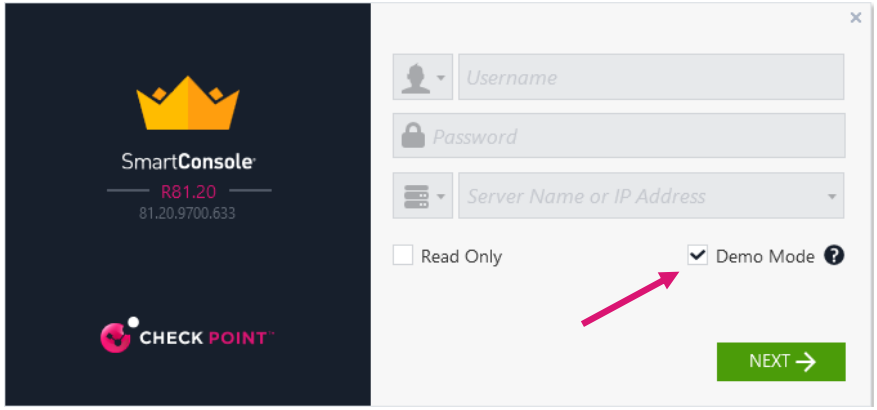
- Desktop client version provides a Demo Mode.
- Become familiar with SmartConsole in non-production environment.

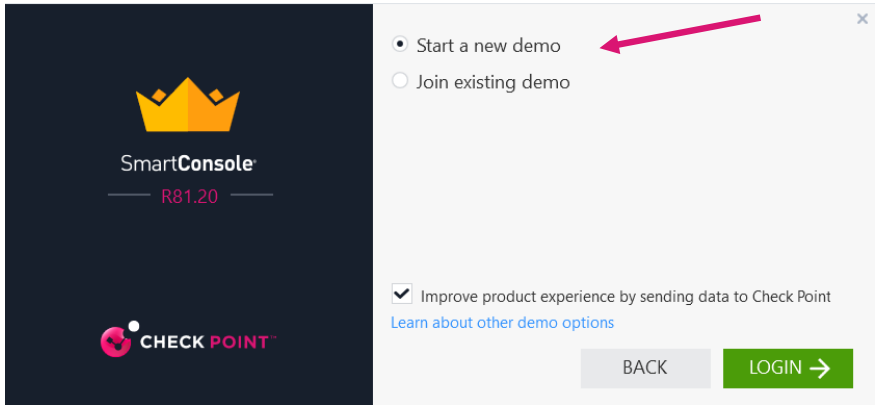


You can install SmartConsole, but you cannot manage your actual Check Point environment without a connection to an operational Security Management Server.

©2023 Check Point Software Technologies Ltd.

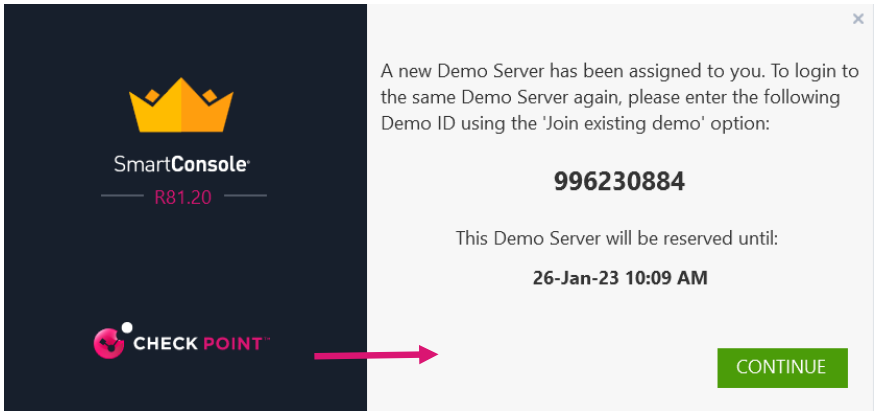
Running SmartConsole in Demo Mode





The same login window displays when you connect to an operational System Management Server.

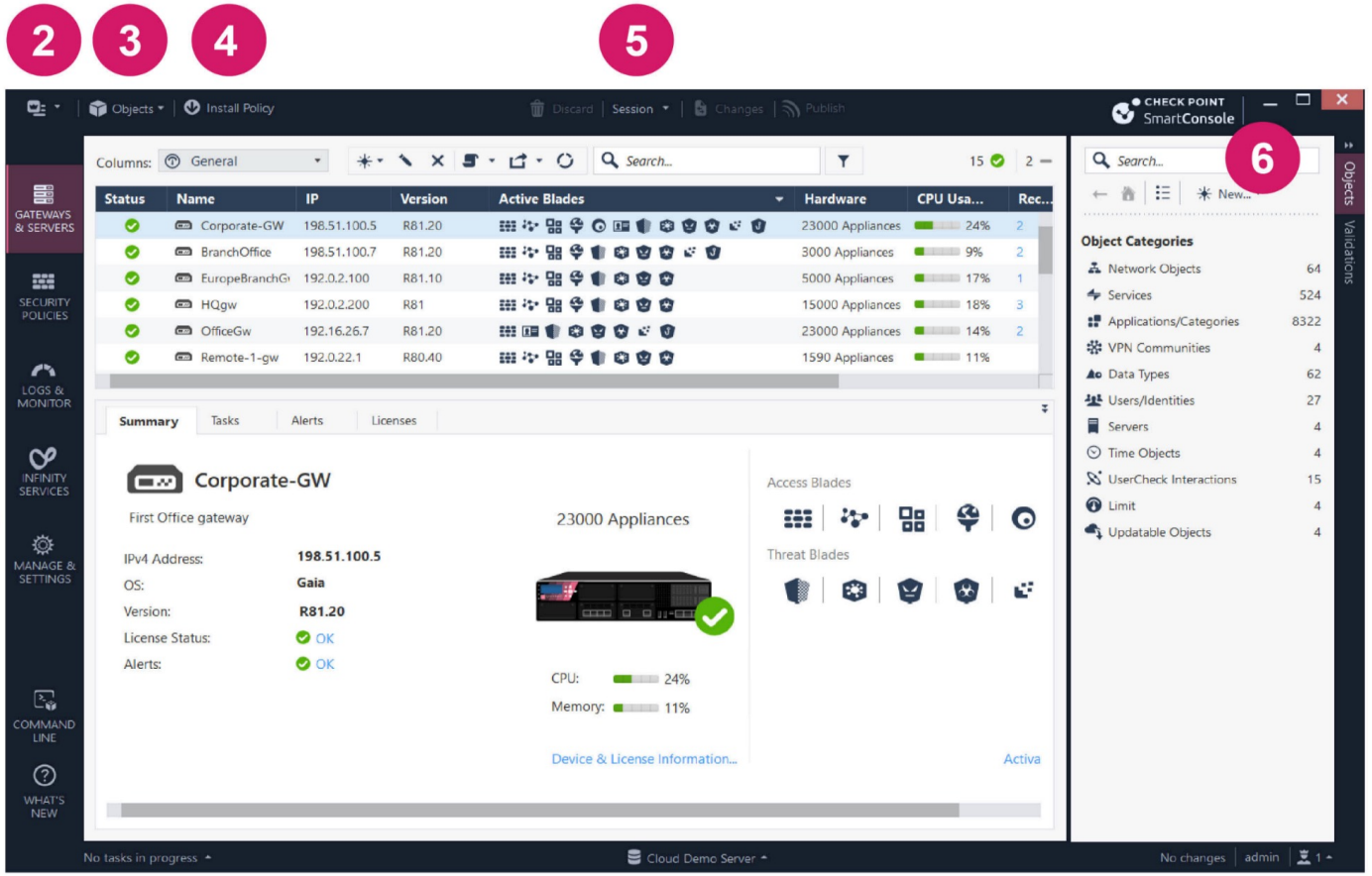
Supply valid SmartConsole credentials.



©2023 Check Point Software Technologies Ltd.

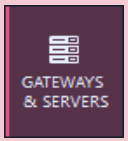
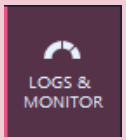
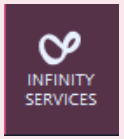
SmartConsole Main Window

1. Navigation toolbar
2. Application menu
3. Objects menu
4. Install policy button
5. Session management controls
6. Search box
7. Validations pane



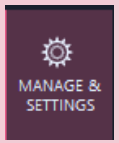
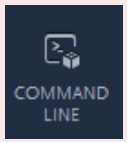
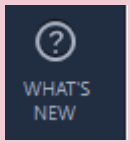
©2023 Check Point Software Technologies Ltd.

SmartConsole Navigation Toolbar

Item	Description
	Create and manage Gateways and Security Gateways. **Note**: In this class, you deploy a Security Management Server and a Security Gateway.
	Create and manage security policies and related settings. **Note**: Security policies are discussed in Chapters 5 and 6.
	View security events, logs, audit logs, and regulation compliance. **Note**: This is discussed in Chapter 10.
	Connect to the cloud-based Infinity Portal. **Note**: Beyond scope of this course. For details, refer to the *Infinity Portal Administration Guide*.

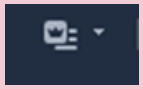
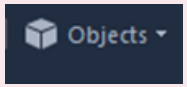
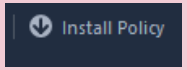
©2023 Check Point Software Technologies Ltd.

SmartConsole Navigation Toolbar

Item	Description
	Create and manage administrators and system settings. **Note**: Introduced in Chapter 3.
	Open the API command line to run commands and scripts. **Note**: Discussed in CCSE. For details, refer to the *Management API Reference*.
	Displays changes and enhancements for the release. This view also links to the online Release Notes.

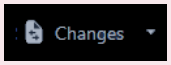
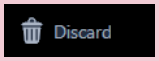
©2023 Check Point Software Technologies Ltd.

SmartConsole Menus and Buttons

Item	Description
	Applications menu. Used to initiate selected tasks, access other tools, and view online Help. Unavailable actions are dimmed.
	Objects menu. View and manage objects, such as Host, Network Group, or Cloud. Also accesses Object Explorer. **Note**: Discussed in Chapters 3 and 5.
	Install Policy. Install a configured policy on one or more Gateways. You can also press **Ctrl + Shift + Enter**.

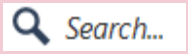
©2023 Check Point Software Technologies Ltd.

SmartConsole Session Management Controls

Icon	Description
	Session Name. Identify a SmartConsole session.
	Session Changes. SmartConsole tracks the changes you make. You can review the changes for a session before saving them to the database.
	Discard changes.
	Publish changes. You must publish before you can install policies.

©2023 Check Point Software Technologies Ltd.

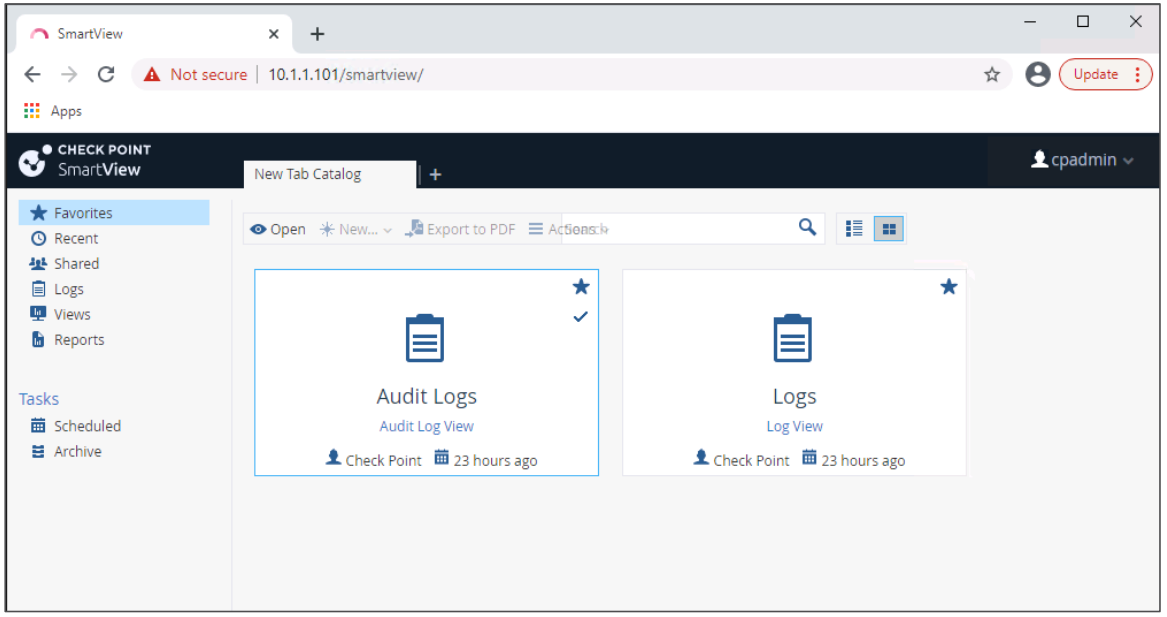
SmartConsole Boxes, Objects, and Bars

Icon	Description
	Search for information relevant to a view.
	Toggle the Objects and Validation panes on and off. **Objects Pane** The Objects pane is used to manage security and network objects. **Validations Pane** The Validation pane is used to view validation errors.

©2023 Check Point Software Technologies Ltd.

SmartView

- Provides clientless access to logs and reports.
- Use SmartConsole credentials.

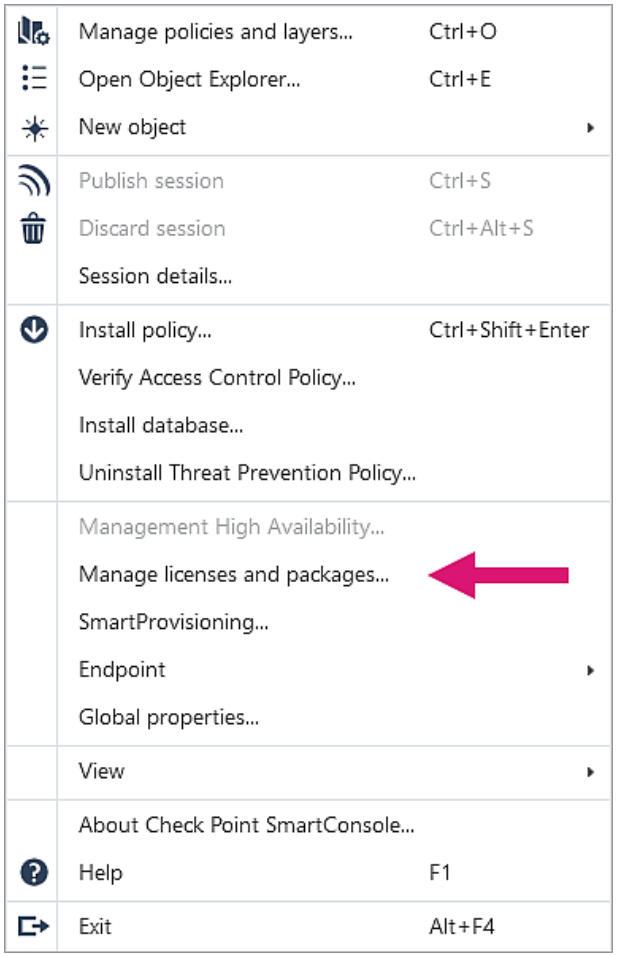


https://<management Server IP>/smartview

©2023 Check Point Software Technologies Ltd.

SmartUpdate

- Legacy tool to manage licenses and contracts.



©2023 Check Point Software Technologies Ltd.

SECURITY MANAGEMENT SERVER

Security Management Server

Quantum

Security Gateway

Management

Edge

IoT Protect

SMB Security Suite

QUANTUM

Secure The Network

©2023 Check Point Software Technologies Ltd.

Management Server

- Database
- Internal Certificate Authority
- Log Server
- Licenses and Contracts Repository
- Monitoring
- Security Automation

©2023 Check Point Software Technologies Ltd.

Management Server

Database

- Hosts a centralized PostgreSLQ database.
- Securely stores managed data and makes data available upon request.

©2023 Check Point Software Technologies Ltd.

Management Server

Internal Certificate Authority

- Created on the Management Server during initial configuration.
- Issues certificates for:
  - Secure Internal Communication (SIC)
  - VPN certificates for Gateways
  - Users

©2023 Check Point Software Technologies Ltd.

- There are situations when an organization might use an external CA. Examples include:
- Establish a VPN with a Security Gateway managed by a different Security Management Server.
- Use a third-party CA already functioning within the organization.

This is discussed in the CCSE course.

©2023 Check Point Software Technologies Ltd.

Management Server

Log Server

- Hosts Check Point product log files collected from Security Gateways and third-party devices.
- Can be installed on a separate server.

©2023 Check Point Software Technologies Ltd.

Management Server

Licenses and Contracts Repository

- Central repository for licenses and contracts.

©2023 Check Point Software Technologies Ltd.

Management Server

Monitoring

- Display real time information about:
  - CPU
  - Disk and memory usage
  - Traffic statistics

©2023 Check Point Software Technologies Ltd.

Management Server

Security Automation

- Used to develop Check Point APIs.
- Allows script creation and Security Policy changes using the command line and web services.

©2023 Check Point Software Technologies Ltd.

Security Management Server Options

Quantum Smart-1 Appliances

Open Servers

Quantum Smart-1 Cloud

©2023 Check Point Software Technologies Ltd.

Quantum Smart-1 Appliances

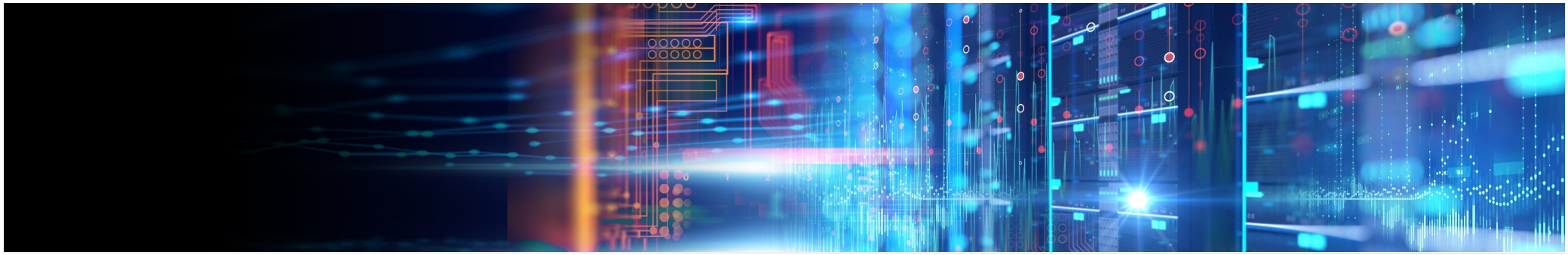
- Check Point proprietary hardware
- Run the Check Point Gaia operating system.
- Optimized for performance, hardened for security.

Ultra High End	High End
Smart-1 6000-XL 200/400 managed Gateways	Smart-1 600-M - 25/50 managed Gateway
Smart-1 6000-L - 75/150 managed Gateways	Smart-1 600-S - 5/10 managed Gateway

©2023 Check Point Software Technologies Ltd.

Open Servers

- Hardware offered by third-party vendors.
- Run the Check Point Gaia operating system.
- Must be on the Hardware Compatibility List, which ranks open servers by:
  - Certified for use with Gaia
  - Certified with remarks (exceptions)
  - Not certified (not supported)



©2023 Check Point Software Technologies Ltd.

Security Management Server Software Blades (Features)

- The R81.20 Management Server Software Blades include:

©2023 Check Point Software Technologies Ltd.

Software Blades (Features)

Feature	Description
Network Policy Management	Centralized Policy Management
Endpoint Policy Management	Unifies Endpoint Security capabilities in a single console.
User Directory	Obtains user identification and security information from LDAP servers.
Provisioning	Centralized administration and provisioning of devices.
Compliance	Fully automated security and compliance monitoring solution.
SmartEvent Server	Reads and analyzes logs.
SmartEvent Correlation	Analyzes logs and identifies events.

©2023 Check Point Software Technologies Ltd.


SECURITY
GATEWAY

Security Gateway

Quantum

- Security Gateway
- Management
- Edge
- IoT Protect
- SMB Security Suite

©2023 Check Point Software Technologies Ltd.

Quantum Security Gateways

Proprietary appliances that combine:

- The translation capabilities of network gateways
- The security functions of next-generation firewalls (NGFWs)
- Threat prevention

©2023 Check Point Software Technologies Ltd.

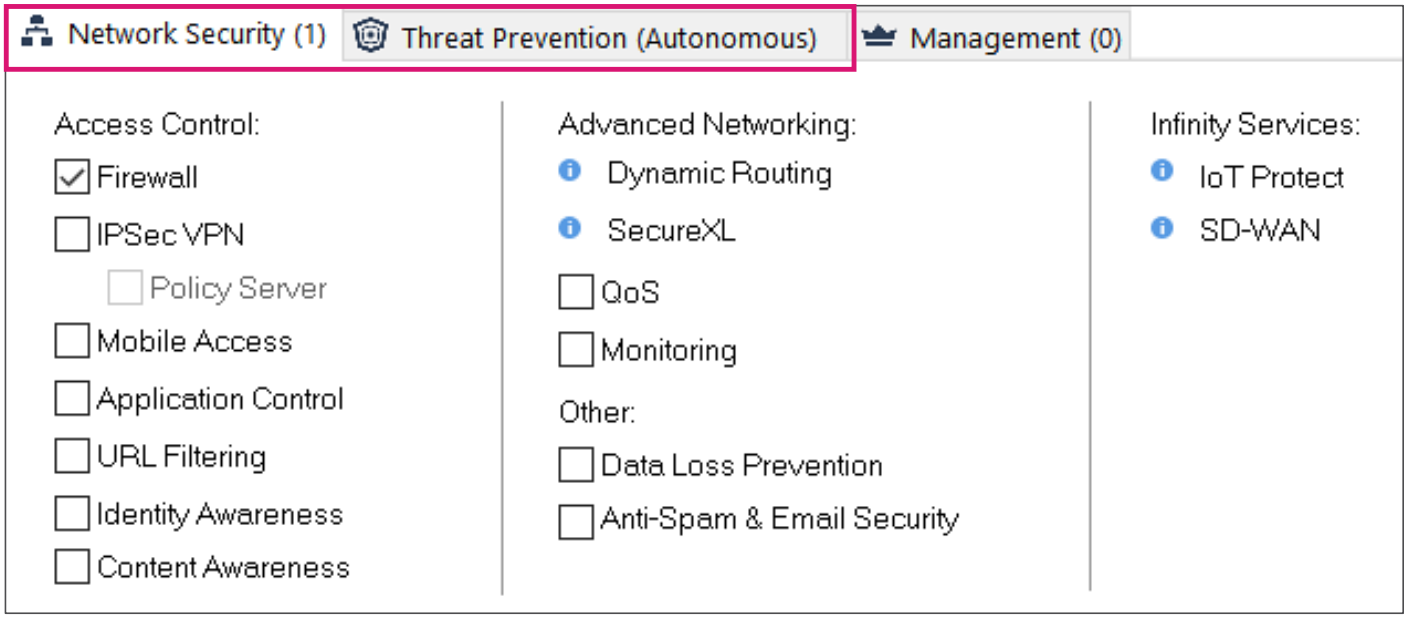
Quantum Security Gateway Models

Category	Model
Hyperscale Network Security	Quantum Maestro
Data Center	Quantum Lightspeed Firewall QLS800, QLS650, QLS450, QLS250
High End Enterprise	Quantum Spark 26000, 28000, 28600
Large Enterprise	Quantum Spark: 6900-7000, 16200
Midsize Enterprise	Quantum Spark 6200, 6400 6600, 6900
Branch Office	Quantum Spark 1530-1550, 1570-1590, 3600-3800
Small Business	Quantum Spark1530-1550, 1570-1590, 1600, 1800
Industrial Appliances	Quantum Rugged 1570R

©2023 Check Point Software Technologies Ltd.

Security Gateway Software Blades or Features

- Two main types:
  - Network Security
  - Threat Prevention



©2023 Check Point Software Technologies Ltd.

Feature Summary – Access Control

Feature	Description
Firewall	Integrated into the architecture and included automatically when you purchase a Security Gateway product.
IPsec VPN	Encrypts and decrypts traffic between Security Gateways/clients in Site-to-Site and Remote Access VPNs.
Mobile Access	Extends Remote Access to include clients and deployments.
Application Control	Detects/blocks traffic.
URL Filtering	Controls access to web sites and applications based on categorization.
Identity Awareness	Enforces Access Control policy rules and audit data based on identity.
Content Awareness	Provides data visibility and enforcement in the Access Control policy.

©2023 Check Point Software Technologies Ltd.

Feature Summary - Advanced Networking

Feature	Description
Dynamic Routing	Determines the best path for traffic to travel through the network.
SecureXL	Software-based cluster solution for Security Gateway redundancy and load sharing.
QoS	Optimizes the performance of an organization's network.
Monitoring	Monitors system counters, traffic connections, and traffic throughput in real-time.

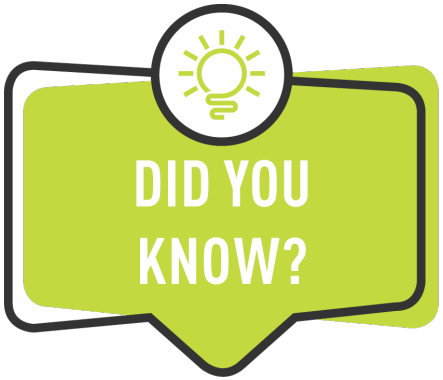
©2023 Check Point Software Technologies Ltd.

Feature Summary – Other and Infinity Services

Feature	Description
Data Loss Prevention	Identifies, monitors, and protects data movement through deep content inspection and analysis of transaction parameters.
Anti-Spam & Email Security	Blocks spam and malware at the connection level.

Feature	Description
IoT Protection (R81.20+)	Instantly discovers and protects Internet of Things (IoT) assets.
SD-WAN (R81.20+)	Applies software-defined networking (SDN) concepts to distribute network traffic throughout a WAN.

©2023 Check Point Software Technologies Ltd.



The Internet of Things, or IoT, is the network of devices connected to the Internet that communicate with one another.

IoT technology is present in a wide variety of sectors stretching from the medical field to the agriculture industry.

For additional information, refer to:

https://www.checkpoint.com/cyber-hub/network-security/what-is-iot

©2023 Check Point Software Technologies Ltd.

Threat Prevention Features for Gateways

- SandBlast Threat Emulation, Threat Extraction, and Zero Phishing
- IPS
- Anti-Bot
- Anti-Virus

©2023 Check Point Software Technologies Ltd.

Autonomous Threat Prevention and Custom Threat Prevention are available.

Autonomous Threat Prevention provides out-of-the-box protection that eliminates the need for manual administration of Threat Prevention Policies. Autonomous Threat Prevention is the focus of Chapter 8 of this course.

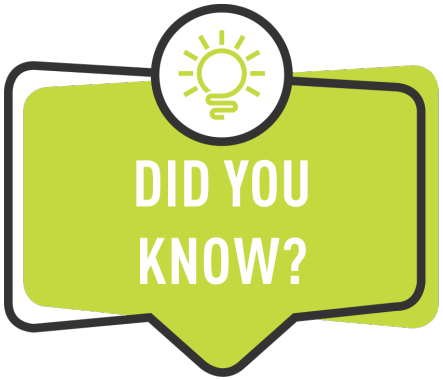
Custom Threat Prevention lets you plan your policy independently based on the needs of your organization. It is the focus of CCSE.

©2023 Check Point Software Technologies Ltd.

Feature Summary - Threat Prevention

Feature	Description
SandBlast Threat Emulation	Uses Internet-connected sandboxes to prevent multi-stage attacks at the earliest stage.
SandBlast Threat Extraction	Eliminates threats from Microsoft Office and PDFs by removing exploitable content such as macros, embedded objects and files, and external links.
SandBlast Zero Phishing	Prevents unknown zero-day and known phishing attacks on websites in real-time.
IPS	Delivers complete and proactive intrusion prevention including thousands of signatures and behavioral and preemptive protections.
Anti-Bot	Discovers infections by correlating multiple detection methods.
Anti-Virus	Performs pre-infection detection and blocking of malware at the Security Gateway.

©2023 Check Point Software Technologies Ltd.



Firewalls deny or permit traffic based on rules defined in the Security Policy. Some industry-standard technologies used to deny or permit network traffic include Packet Filtering, Stateful Inspection, and Application Layer Firewall.

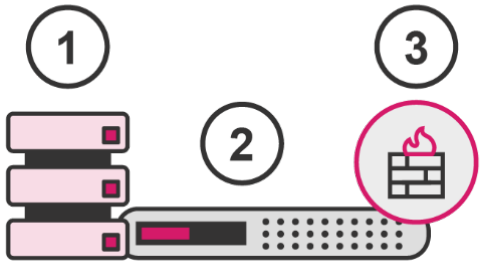
For additional information about how these technologies work, see the Appendix for this course.

©2023 Check Point Software Technologies Ltd.

COMMON DEPLOYMENT SCENARIOS

Standalone Deployment

- Security Management Server and Security Gateway are installed on the same computer or appliance.
- Not recommended except for small businesses.

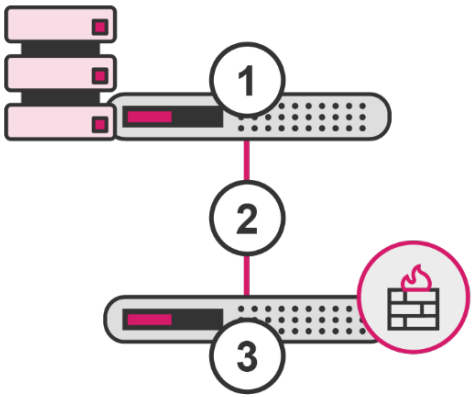


ITEM	DESCRIPTION
1	Security Management Server
2	Standalone Server
3	Security Gateway Component

©2023 Check Point Software Technologies Ltd.

Distributed Deployment

Security Gateway and the Security Management Server are installed on different computers or appliances.



ITEM	DESCRIPTION
1	Security Management Server
2	Network Connection
3	Security Gateway

©2023 Check Point Software Technologies Ltd.

A Security Management Server is required even if the deployment system has only a single Security Gateway.

A single Security Management Gateway can manage multiple Gateways.

©2023 Check Point Software Technologies Ltd.

BRINGING IT ALL TOGETHER

Secure Communications

- Authentication using SIC (Secure Internal Communication).
- SIC uses the SSL protocol to encrypt data.
- Management Server acts as an ICA (Internal Certificate Authority) for the environment.

©2023 Check Point Software Technologies Ltd.

Basic Workflow: Create, Store, Enforce

SmartConsole

- **Create** and manage security policies, user accounts, devices, and settings.
- Send to Security Management Server.

Create

Security Management Server

- **Store** security policies in a PostgreSQL database.
- Compile policy information into inspect code.
- Send policy information to Security Gateway.

Store

Security Gateway

- **Enforce** security policies using inspect code.

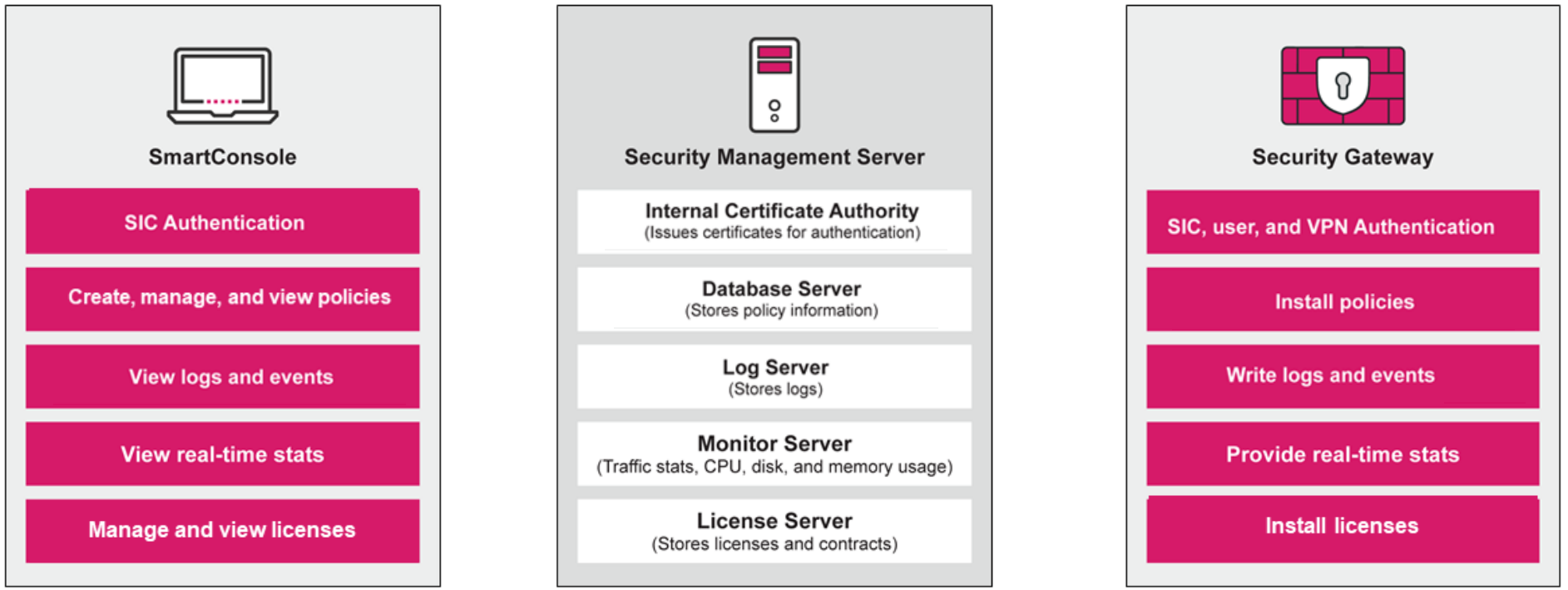
For example:
- ✓ If source = x
- ✓ And destination = y
- ✓ And Port = z

Action = Accept or Drop
Else = Go to next rule

Enforce

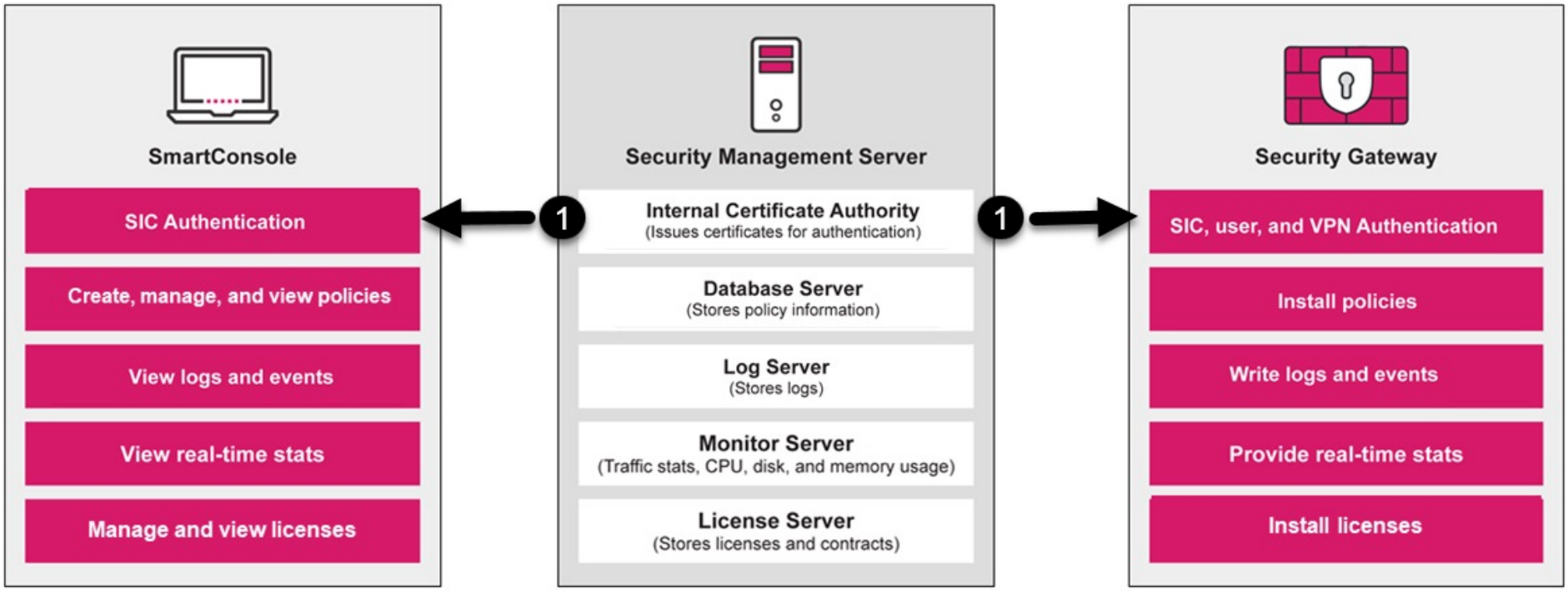
©2023 Check Point Software Technologies Ltd.

Detailed Workflow: Create, Store, and Enforce



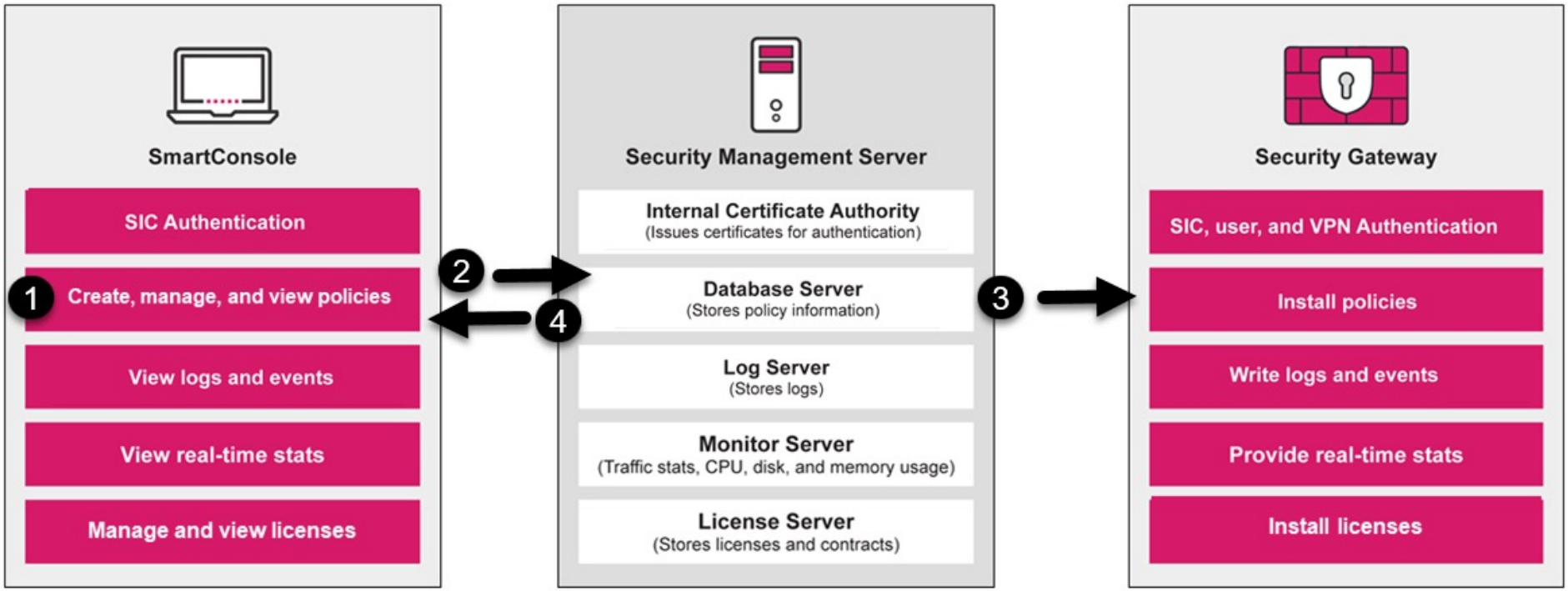
©2023 Check Point Software Technologies Ltd.

Authentication



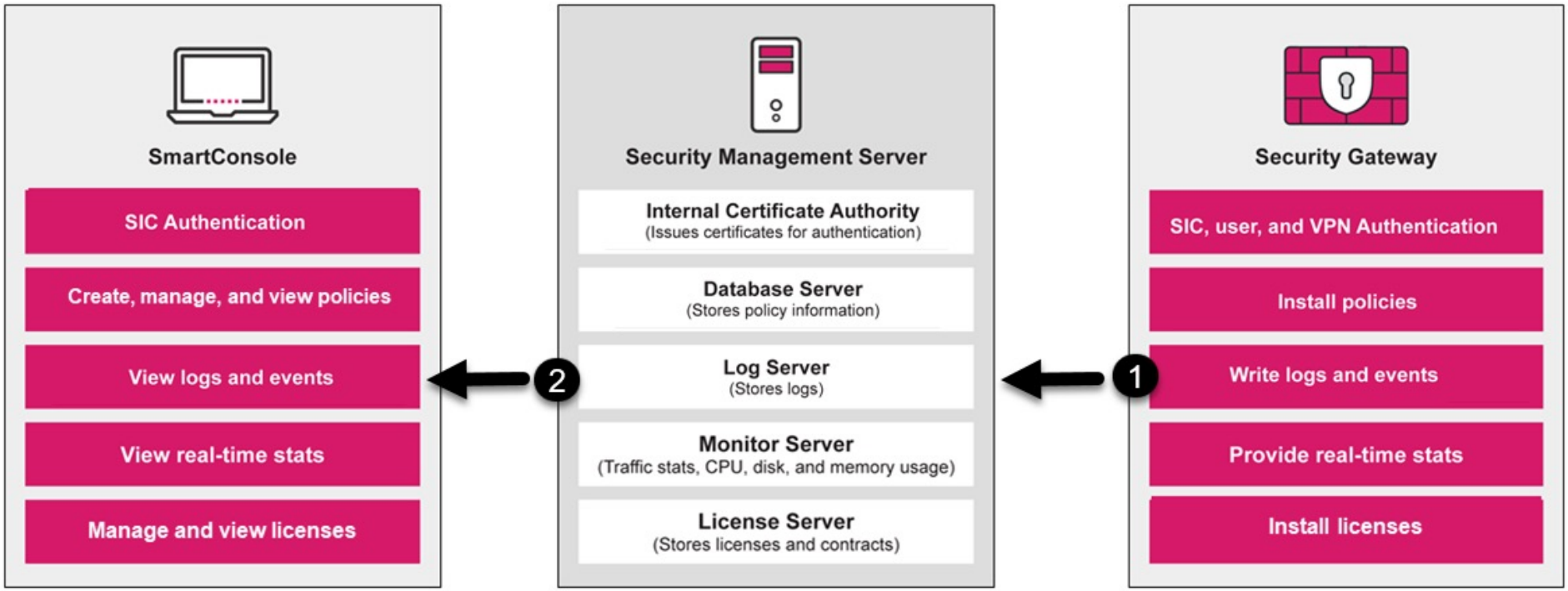
©2023 Check Point Software Technologies Ltd.

Policies



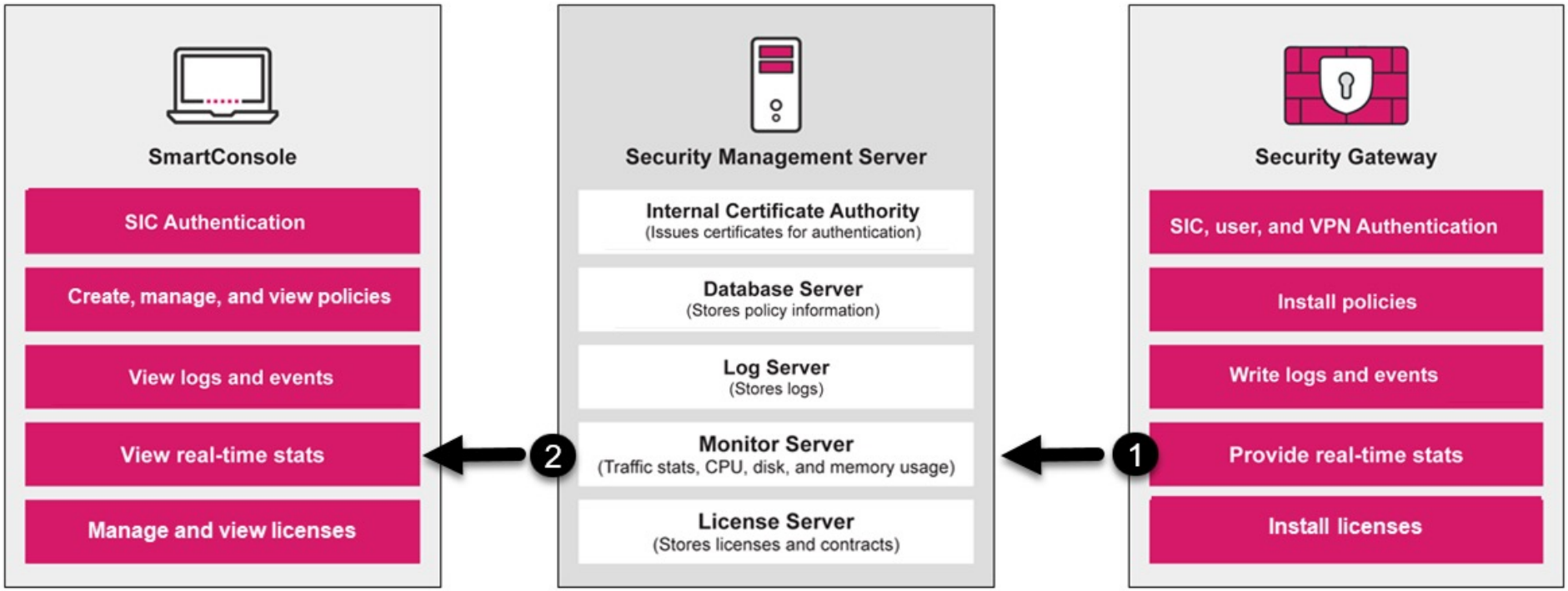
©2023 Check Point Software Technologies Ltd.

Logs



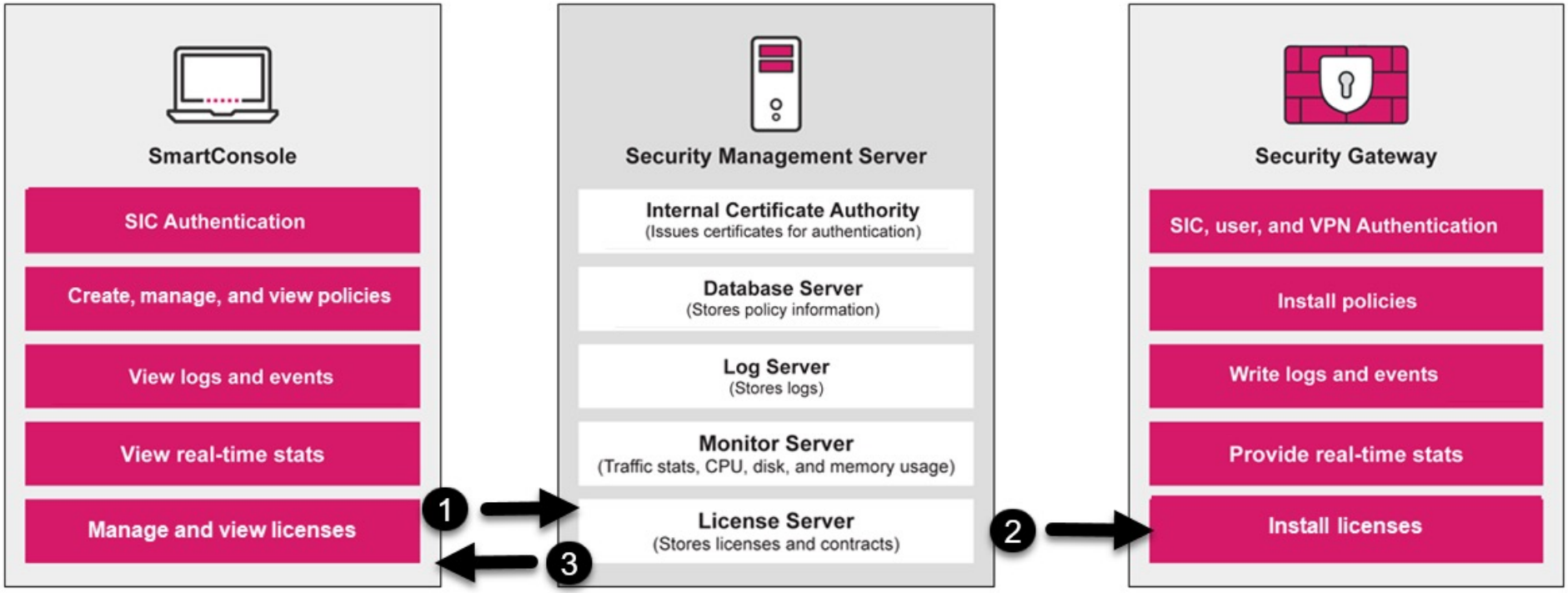
©2023 Check Point Software Technologies Ltd.

Statistics



©2023 Check Point Software Technologies Ltd.

Licenses



©2023 Check Point Software Technologies Ltd.

Resource – Information Flow

SmartConsole	Information Flow	Management Server	Information Flow	Security Gateway
SIC authentication		Issues certificates for authentication		SIC, user, and VPN authentication
Create, manage, and view policies		Store policy information in database		Install and enforce policies
View logs and events		Store logs		Send logs and events
View real time stats		Store traffic, CPU, disk, and memory status		Send real time stats
Manage and view licenses and contracts		Store licenses and contracts		Install licenses

©2023 Check Point Software Technologies Ltd.

Further Learning - Advanced Deployments

Deployment	Resources
Management High Availability	• Documentation: *Quantum Security Management Administration Guide* • Training: Check Point Certified Security Expert (CCSE)
Clustering for Security Gateway redundancy and Load Sharing	• Documentation: *Quantum Security Management Administration Guide* • Training: Check Point Certified Security Expert (CCSE)
Multi-domain security for largescale, distributed environments	• Documentation: *Multi-Domain Security Management Administration Guide* • Training: Check Point Certified Multi-Domain Security Management Specialist (CCMS)

©2023 Check Point Software Technologies Ltd.

Advanced Deployments (Continued)

Deployment	Resources
Virtual System eXtension solution that runs multiple virtual firewalls on the same hardware	• Documentation: *VSX Administration Guide* • Training: Check Point Virtual System eXtension (VSX) Specialist (CCVS)
Scalable Network Security	• Documentation: *Quantum Maestro Administration Guide* • Training: Check Point Certified Maestro Expert

For information about training, go to https://trainingcertifications.checkpoint.com.

For documentation, go to the Check Point Quantum 81.20 Home page (sk173903).

©2023 Check Point Software Technologies Ltd.

Review Questions

1. What are the three main components of the Check Point Three-Tier Architecture?
2. What is the main purpose of SmartConsole?
3. What is the main purpose of a Security Management Server?
4. What is the main purpose of a Security Gateway?

©2023 Check Point Software Technologies Ltd.

Lab 1A

Deploying SmartConsole

©2023 Check Point Software Technologies Ltd.