Check Point Certified Security Administrator (CCSA)

Exam 156-215.82 Check Point Security Administrator R82 (CCSA)

Demo Questions

CHECK POINT™

CHECK POINT
CCSA
Certified Security Administrator
CERTIFICATION

156.215.82 - Check Point Certified Security Administrator R82 Exam

注意：題目有 ☆ 標記只代表近期出過的題目，☆ 數量越多，代表過去多月出的次數越多，但同學必須溫習“整份”題目才可提升考試合格機會。 (☆=Nov, ☆=Dec, ☆=Jan, ☆=Feb, ☆=Mar)

Q.1 ☆☆☆☆

Which of the following is true about Stateful Inspection?

A. Stateful Inspection looks at both the headers of packets, as well as deeply examining their content.
B. Stateful Inspection requires two rules, one for outgoing traffic and one for incoming traffic.
C. Stateful Inspection requires that a server reply to a request, in order to track a connection's state.
D. Stateful Inspection tracks sate using two tables, one for incoming traffic and one for outgoing traffic.

Answer: A

- **Stateful Inspection** goes beyond simple packet filtering.
- It examines **packet headers** (source/destination IP, ports, protocol) **and tracks the state of the connection** in a state table.
- It can also inspect certain parts of the packet payload to ensure the traffic matches the expected protocol behavior.
- This allows the firewall to make more intelligent decisions, permitting only valid, established connections and blocking suspicious or malformed traffic.

Why the other options are incorrect

- **B. Requires two rules (outgoing/incoming)** → That's packet filtering. Stateful Inspection only needs one rule; return traffic is automatically allowed if it matches the connection state.
- **C. Requires server reply to track state** → Not true; the firewall tracks state as soon as the initial packet is allowed, regardless of whether a reply is received.
- **D. Tracks state using two tables** → It uses a **single state table** to track all connections, not separate tables for incoming/outgoing.

Q.2 ☆☆☆☆

What is NOT an advantage of Stateful Inspection?

A. High Performance
B. No Screening above Network Layer
C. Good Security
D. Transparency

Answer: B

- **Stateful Inspection** is Check Point's core firewall technology. Its advantages include:
  - **High Performance** → Efficiently tracks connections without re-evaluating every packet.
  - **Good Security** → Maintains context of sessions, preventing spoofing and unauthorized traffic.

    - **Transparency** → Operates seamlessly, users don't notice the inspection.
- However, **"No Screening above Network Layer"** is **not an advantage**. In fact, Stateful Inspection goes **beyond the network layer**, inspecting transport and application layer information to make intelligent decisions.

Why the other options are advantages

- **A. High Performance** → Yes, it's efficient compared to pure packet filtering.
- **C. Good Security** → Provides strong session-aware protection.
- **D. Transparency** → Works invisibly to end users.

Q.16 

In SmartConsole, on which tab are Permissions and Administration defined?

A. MANAGE & SETTINGS
B. SECURITY POLICES
C. GATEWAYS & SERVERS
D. LOGS & MONITOR

Answer: A

In **SmartConsole**, the **Permissions and Administration** settings are defined under the **MANAGE & SETTINGS** tab. This is where administrators configure:

- **Administrator accounts and roles**
- **Permissions profiles**
- **Authentication methods**
- **General management settings**

Why the other options are incorrect

- **B. SECURITY POLICIES** → Used for defining firewall, application control, and threat prevention rules, not admin permissions.
- **C. GATEWAYS & SERVERS** → Used to manage gateways, clusters, and servers, not permissions.
- **D. LOGS & MONITOR** → Used for viewing logs, monitoring traffic, and events, not administration.

Q.17 

Which of the following is NOT a valid application navigation tab in SmartConsole?

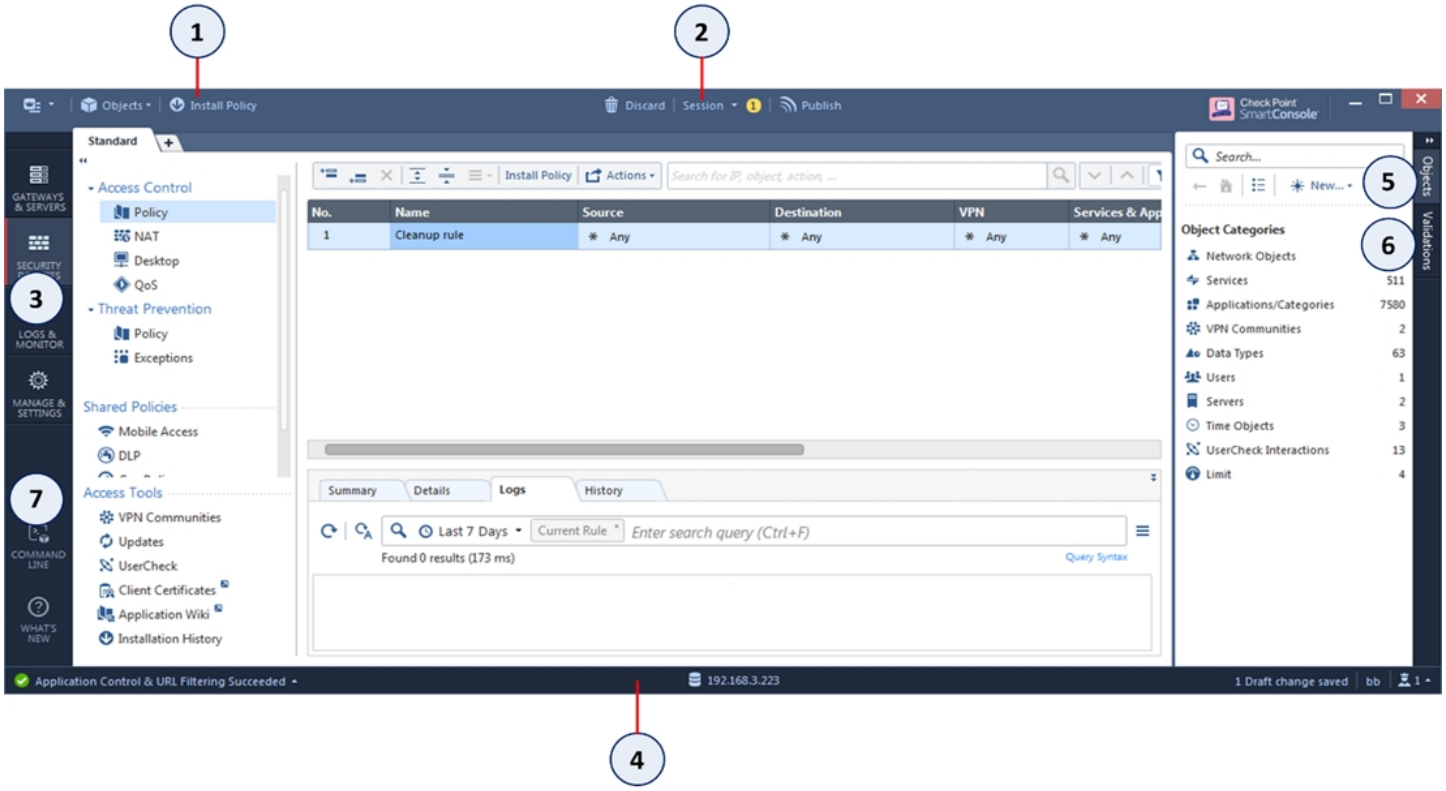
A. WEBUI & COMMAND LINE
B. SECURITY POLICIES
C. GATEWAYS & SERVERS
D. LOGS & MONITOR

Answer: A

In **SmartConsole**, the main navigation tabs include:

- **Security Policies** → where administrators define and manage rule bases.
- **Gateways & Servers** → where gateways, clusters, and servers are managed.
- **Logs & Monitor** → where logs, events, and monitoring dashboards are viewed.
- **WEBUI & COMMAND LINE** is not a SmartConsole navigation tab.

The Gaia Portal (WebUI) and CLI (Clish/Bash) are separate configuration interfaces for Gaia OS, not part of SmartConsole's navigation.



Item	Description
1	Global Toolbar
2	Session Management Toolbar
3	Navigation Toolbar
4	System Information Area

Item	Description
5	Objects Bar (F11)
6	Validations pane
7	Command line interface button

Q.18

Which SmartConsole tab shows logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?

A. LOGS & MONITOR
B. SECURITY POLICIES
C. GATEWAY & SERVERS
D. MANAGE & SETTINGS

Answer: A

- The **Logs & Monitor tab** is the central location in SmartConsole for:
  - Viewing **traffic logs** from all gateways.
  - Detecting **security threats** and suspicious activity.
  - Correlating events to identify **attack patterns** across the network.
- It provides administrators with a **real-time and historical view** of what's happening, making it the go-to tab for monitoring and threat detection.

Why the other options are incorrect

- **B. Security Policies** → Used to configure and manage rules/policies, not to monitor logs or threats.
- **C. Gateway & Servers** → Used to manage gateway and server objects, not for centralized log viewing.
- **D. Manage & Settings** → Used for global configuration and settings, not for monitoring.

Q.19 

Which part of SmartConsole allows administrators to add, edit, delete, and clone objects?

A. Object Explorer
B. Object Navigator
C. Object Editor
D. Object Browser

Answer: A

- In **SmartConsole**, the **Object Explorer** is the central window for managing network objects (hosts, networks, services, tags, etc.).
- It provides the full set of operations: **Add, Edit, Delete, Clone**.
- This makes it the administrator's main interface for object lifecycle management.

Why the other options are incorrect

- **B. Object Navigator** → Not a valid SmartConsole component.
- **C. Object Editor** → Used for editing the details of a single object, but not for adding, deleting, or cloning across the repository.
- **D. Object Browser** → Not an official SmartConsole tab; sometimes confused with Explorer, but the correct term is **Object Explorer**.

Q.20 

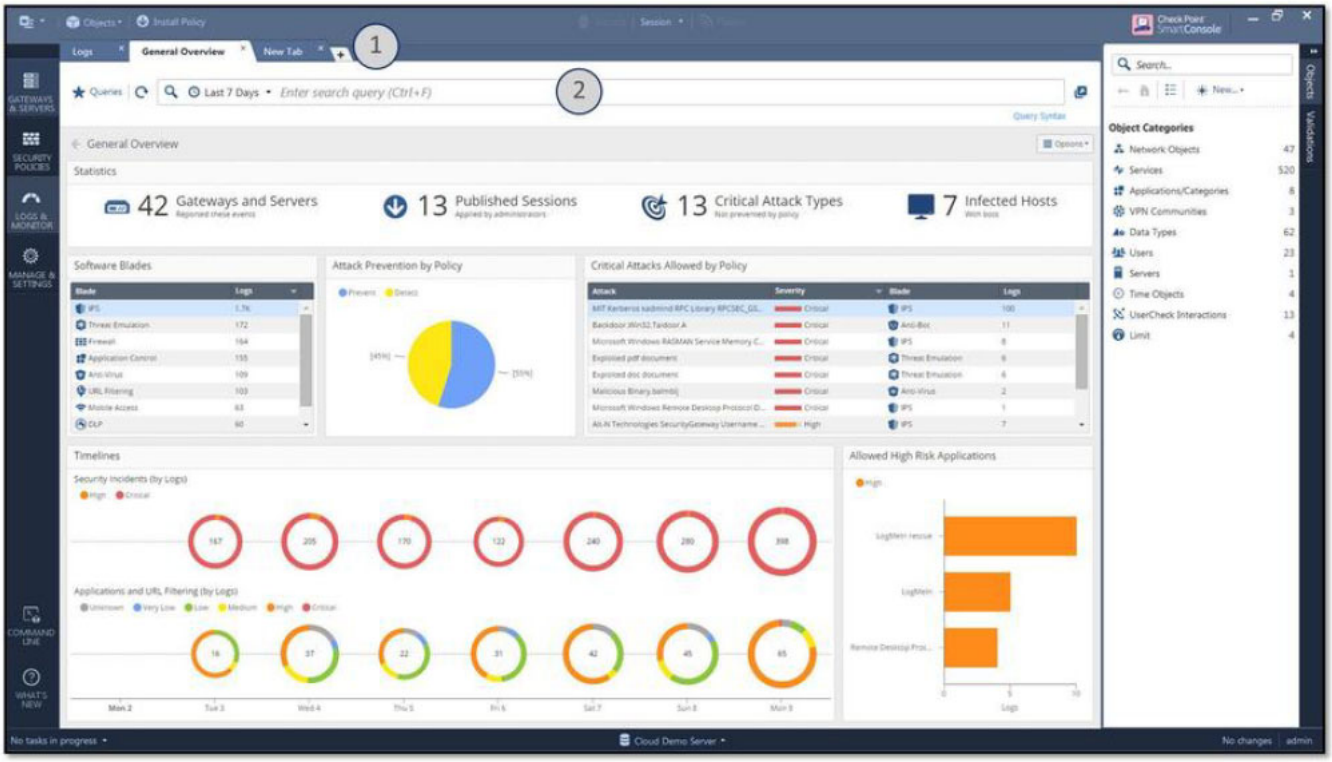
Which SmartConsole tab is used to monitor network and security performance?

A. Logs & Monitor
B. Manage & Settings
C. Security Policies
D. Gateway & Servers

Answer: A

The Logs & Monitor tab allows you to view graphs and pivot tables in an organized dashboard, search through logs, schedule customizable reports, and monitor gateways.

- The **Logs & Monitor tab** in SmartConsole is specifically designed for **monitoring network traffic, security events, and performance metrics**.
- It provides:
  - Real-time and historical logs.
  - Security event analysis.
  - Monitoring dashboards for gateways and blades.
- This is the tab administrators use to **track performance and security posture**.



Why the other options are incorrect

- **B. Manage & Settings** → Used for managing global settings, administrators, and configuration, not monitoring.
- **C. Security Policies** → Used to define and edit rules/policies, not to monitor performance.
- **D. Gateway & Servers** → Used to manage gateways/servers objects, not for monitoring.

Q.21 

In order for changes made to policy to be enforced by a Security Gateway, what action must an administrator perform?

A. Install policy
B. Publish changes
C. Install database
D. Save changes

Answer: A

- In **Check Point SmartConsole**, administrators make changes to the security policy.
- These changes must be **published** to the management database so they are visible to other administrators.
- However, publishing alone does **not** enforce the changes on the Security Gateway.
- To actually apply the new rules, the administrator must **install the policy** onto the gateway.
- **Install Policy = push compiled rules from the management server to the gateway → enforcement begins.**

Why the other options are incorrect

- **B. Publish changes** → Saves changes to the management database, but does not enforce them on the gateway.
- **C. Install database** → Not a valid action in SmartConsole.
- **D. Save changes** → Saves locally but does not push to the gateway.

Q.22 

What is a role of Publishing?

A. The Publish operation sends the modifications made via SmartConsole in the private session and makes them public.
B. The Security Management Server Installs the updated policy and the entire database on Security Gateways.
C. The Security Management Server installs the updated session and the entire Rule Base on Security Gateways.
D. Modifies network objects, such as servers, users, services, or IPS profiles, but not the Rule Base.

Answer: A

In Check Point's **Management workflow**, administrators work in **sessions** within SmartConsole:

- **Private Session** → Changes made by an administrator are visible only to them until published.
- **Publish** → This operation **commits the changes** from the private session into the **main database**, making them visible to all administrators.
- **Install Policy** → After publishing, the updated policy can be installed on Security Gateways.

So, **Publishing** is about **sharing and committing changes** into the management database, not about installing them on gateways.

Why the other options are incorrect

- **B. The Security Management Server installs the updated policy and the entire database on Security Gateways** → That's the role of **Policy Installation**, not Publishing.
- **C. The Security Management Server installs the updated session and the entire Rule Base on Security Gateways** → Again, that's **Policy Installation**, not Publishing.

- **D. Modifies network objects, such as servers, users, services, or IPS profiles, but not the Rule Base**
  → Publishing applies to **all changes** (objects, rules, profiles) in the session.

Q.23 

Which one of the following is TRUE?

A. One policy can be either inline or ordered, but not both.

B. Inline layer can be defined as a rule action.

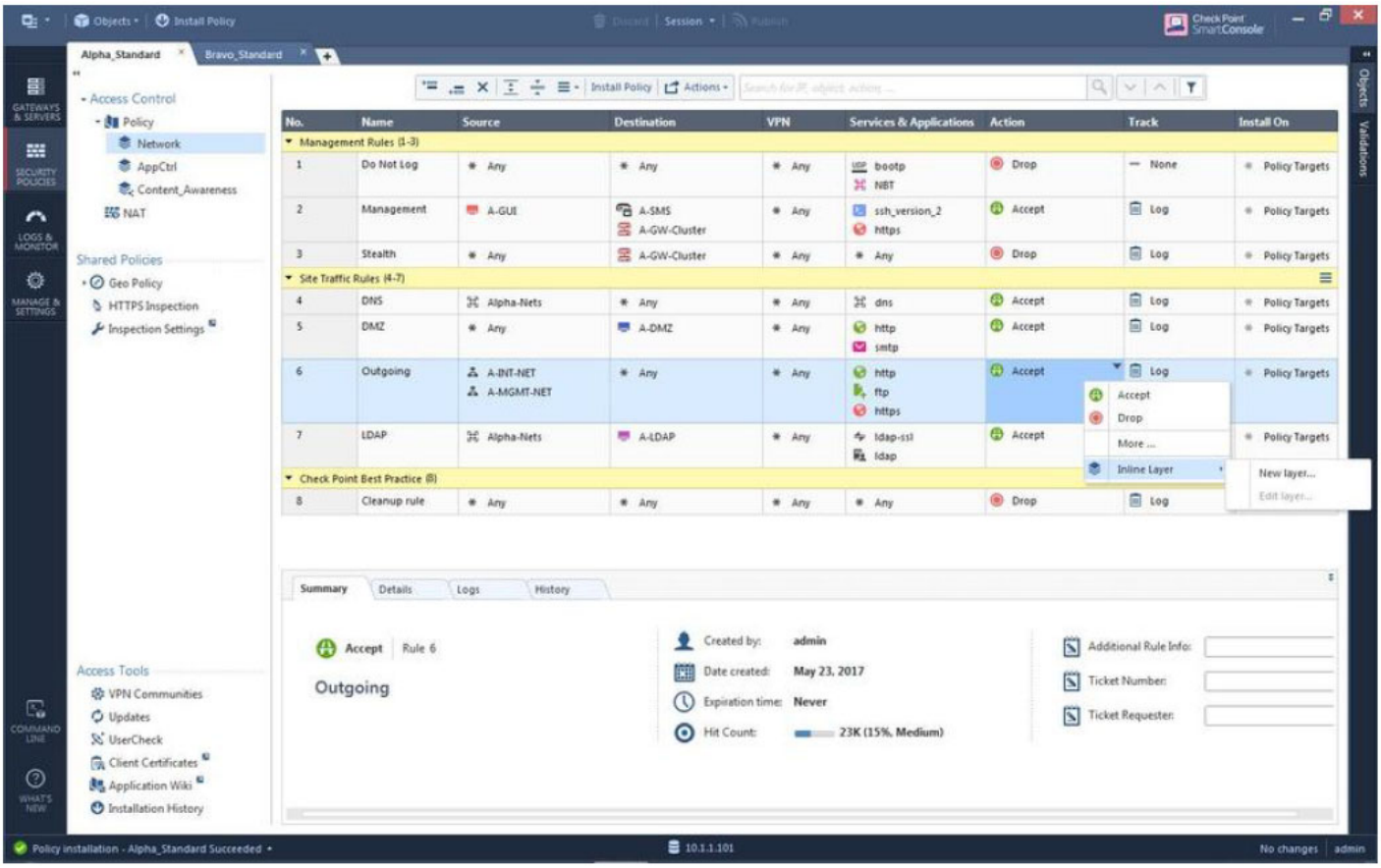
C. Ordered policy is a sub-policy within another policy.

D. Pre-R80 Gateways do not support ordered layers.

Answer: B

Define an in-line Application & URL Filtering layer that appears in the Network Layer for Alpha.

1. In the Alpha_Standard Security Policy, view the Network layer.
2. In the Rule Base, select the Outgoing rule.
3. Right-click the **Action** column and select **Inline Layer**:



- In **R80 and later**, Check Point introduced the concept of **policy layers**:
  - **Ordered layers** → Applied sequentially, one after another.
  - **Inline layers** → Defined as a **rule action** inside the policy, allowing deeper inspection when traffic matches that rule.
- Inline layers essentially act like a "sub-policy" triggered by a specific rule, but they are defined **as the rule's action**, not as a separate ordered policy.

Why the other options are incorrect

- **A. One policy can be either inline or ordered, but not both** → Wrong; a policy can contain both ordered and inline layers.
- **C. Ordered policy is a sub-policy within another policy** → Misleading; ordered layers are sequential, not embedded sub-policies.
- **D. Pre-R80 Gateways do not support ordered layers** → Incorrect; ordered layers are supported, but the new unified policy model was introduced in R80.

Q.24 

When dealing with rule base layers, what two layer types can be utilized?

A. Inbound Layers and Outbound Layers
B. Ordered Layers and Inline Layers
C. Structured Layers and Overlap Layers
D. R81.X does not support Layers

Answer: B

In Check Point R81.x and later, the **rule base** can be structured using two types of layers:

- **Ordered Layers**
  - Evaluated **sequentially**, one after another.
  - Each layer must match before traffic is passed to the next.
  - Commonly used for separating **network security rules** from **application control rules**.
- **Inline Layers**
  - Placed **inside a rule** as a sub-policy.
  - Allow more granular control by creating a mini rule base within a single rule.
  - Useful for scenarios like applying different rules to specific groups of users or applications.

Why the other options are incorrect

- **A. Inbound Layers and Outbound Layers** → Not valid Check Point terminology.
- **C. Structured Layers and Overlap Layers** → Not recognized types in Check Point.
- **D. R81.X does not support Layers** → Incorrect; R81.x fully supports Ordered and Inline Layers.

Q.25 

Where is the "Hit Count" feature enabled or disabled in SmartConsole?

A. In Global Properties
B. On each Security Gateway
C. On the Policy layer
D. On the Policy Package

Answer: A

- The **Hit Count feature** shows how many times each rule in the Security Policy has matched traffic.
- It helps administrators identify unused rules, optimize policies, and improve performance.
- This feature is **enabled or disabled globally** in **Global Properties**, not per gateway or per policy.

Why the other options are incorrect

- **B. On each Security Gateway** → Hit Count is not configured per gateway; it's a global setting.
- **C. On the Policy layer** → Policy layers define rule sets, but Hit Count is not enabled/disabled here.
- **D. On the Policy Package** → Policy packages are collections of rules, but Hit Count is controlled globally.

Q.26 

In which deployment is the security management server and Security Gateway installed on the same appliance?

A. Switch
B. Standalone
C. Distributed
D. Remote

Answer: B

In Check Point's **Security Management Architecture**:

- **Standalone Deployment**
  - The **Security Management Server** and the **Security Gateway** are installed on the **same appliance**.
  - This is common in smaller environments or labs where simplicity is preferred.
- **Distributed Deployment**
  - The **Security Management Server** and the **Security Gateway** are installed on **separate appliances**.
  - This is the standard design for larger or production environments.
- **Switch** → Not a Check Point deployment type.
- **Remote** → Not a valid deployment type in this context.

Q.27 

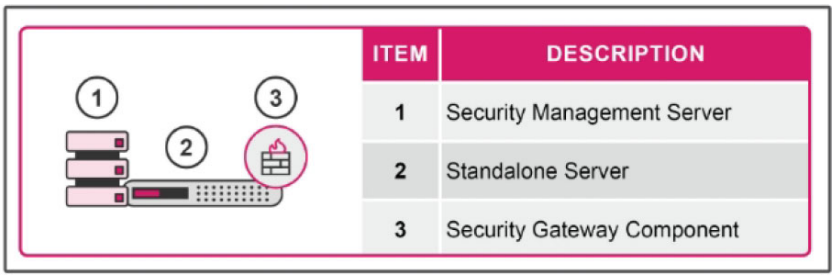
What are the two deployment options available for a security gateway?

A. Bridge and Switch
B. Local and Remote
C. Cloud and Router
D. Standalone, Distributed

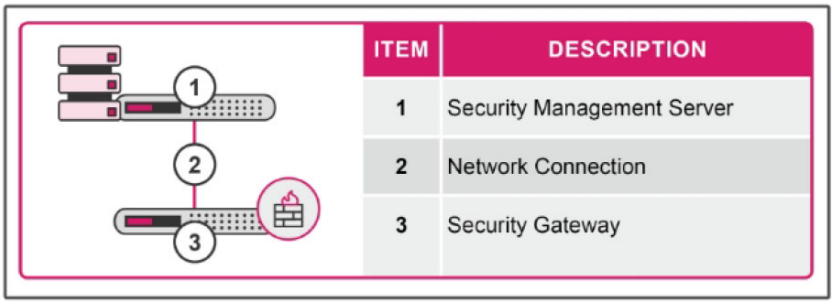
Answer: D

In Check Point deployments, a **Security Gateway** can be installed in two main ways:

1. **Standalone Deployment**
   - The **Security Gateway** and the **Security Management Server** are installed on the **same appliance**.
   - Common in smaller environments, labs, or testing setups where simplicity is preferred.



2. **Distributed Deployment**
   - The **Security Gateway** and the **Security Management Server** are installed on **separate appliances**.
   - Standard in larger or production environments for scalability, performance, and separation of duties.



Why the other options are incorrect

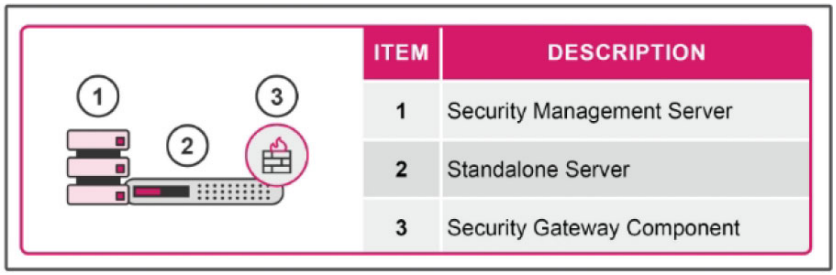
- **A. Bridge and Switch** → These are networking modes, not Check Point deployment options.
- **B. Local and Remote** → Not valid Check Point terminology for gateway deployment.
- **C. Cloud and Router** → Incorrect; while gateways can run in cloud environments, "Cloud" and "Router" are not the official deployment types.
- **D. Standalone, Distributed** → Correct. These are the two recognized deployment options.

Q.28 
Which of the following is a valid deployment option?

A. CloudSec deployment
B. Disliked deployment
C. Router only deployment
D. Standalone deployment

Answer: D

- In Check Point terminology, **Standalone deployment** means the **Security Gateway and Security Management Server are installed on the same machine**.



- This is a valid and supported deployment option, often used in smaller environments or labs where simplicity is preferred.
- Other valid deployment options include **Distributed deployment** (Gateway and Management on separate machines) and **Multi-Domain deployment** (for large enterprises).

Why the other options are incorrect

- **A. CloudSec deployment** → Not a recognized Check Point deployment type.
- **B. Disliked deployment** → Clearly invalid; no such option exists.
- **C. Router only deployment** → Check Point gateways are firewalls/security appliances, not simple routers.

Q.29 

In a Distributed deployment, the Security Gateway and the Security Management software are installed on what platforms?

A. The installation can be done on virtual machines only, but not on appliances and not in mixed environments.
B. The installation is done on different computers or appliances.
C. The installation is done on the same computer or appliance.
D. The installation is allowed in Azure only but not in AWS cloud environments.

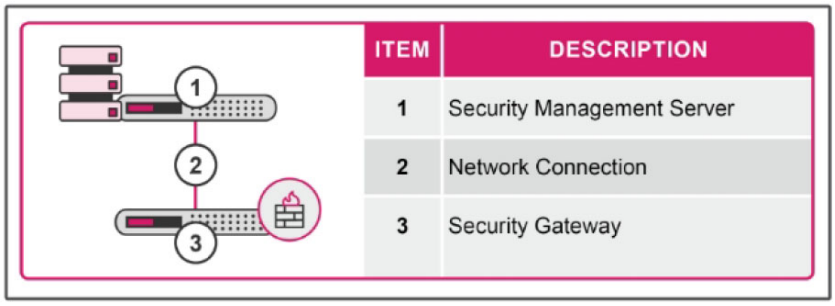
Answer: B

In a distributed deployment, the Security Gateway and the Security Management Server are installed on different computers or appliances.

• The Security Management Server generally runs in a single management domain. Multi-Domain environments are supported but are beyond the scope of this course.

• The Security Gateway is usually deployed at the perimeter to control and secure traffic.

• SmartConsole is installed on a Windows host that connects to the Security Management Server.



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

Why the other options are incorrect

- **A. Virtual machines only** → Not true; deployments can be on physical appliances, virtual machines, or mixed environments.
- **C. Same computer/appliance** → That describes a **Standalone deployment**, not Distributed.
- **D. Azure only, not AWS** → Check Point supports multiple cloud environments (Azure, AWS, GCP, etc.), so this is incorrect.

Q.30 ☆☆☆

When a Security Gateways communicates about its status to an IP address other than its own, which deployment option was chosen?

A. Targeted
B. Bridge Mode
C. Distributed
D. Standalone

Answer: C

- In a **Distributed deployment**, the **Security Gateway** and the **Security Management Server** are installed on **different machines/appliances**.
- Because of this separation, the gateway reports its status to the **management server's IP address**, which is different from its own.
- This allows centralized monitoring and management of multiple gateways in larger environments.

Why the other options are incorrect

- **A. Targeted** → Not a valid Check Point deployment option.
- **B. Bridge Mode** → Refers to transparent firewalling at Layer 2, not management communication.
- **D. Standalone** → In standalone, gateway and management are on the same machine, so communication is local (same IP).