CheckPoint.156-315.82.v2026-07-15.q53

Exam Code:	156-315.82
Exam Name:	Check Point Certified Security Expert - R82
Certification Provider:	CheckPoint
Free Question Number:	53
Version:	v2026-07-15
# of views:	102
# of Questions views:	540
https://www.freecram.net/torrent/CheckPoint.156-315.82.v2026-07-15.q53.html	

NEW QUESTION: 1
What is the correct description for the Dynamic Balancing / Spit feature?
A. Dynamic Balancing / Split dynamically distribute the traffic from one network interface to multiple SND's. The interface must support Multi-Queue. It is only available on Quantum Appliances (not on Quantum Spark or Open Server)
B. Dynamic Balancing / Split dynamically change the number of SND's and firewall instances based on the current load. It is only available on Quantum Appliances (not on Quantum Spark or Open Server)
C. Dynamic Balancing / Spit dynamically distribute the traffic from one network interface to multiple SND's. The interface must support Multi-Queue. It is only available on Quantum Appliances and Open Server (not on Quantum Spark)
D. Dynamic Balancing / Split dynamically change the number of SND's and firewall instances based on the current load. It is only available on Quantum Appliances and Open Server (not on Quantum Spark)
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Which statement is WRONG regarding the usage of the Central Deployment in SmartConsole?
A. You can upgrade your cluster without user intervention with the Central Deployment in SmartConsole from R80.40 to R81.20.
B. You can install Hotfixes with the Central Deployment in SmartConsole
C. Only Hotfixes can be installed with the Central Deployment in SmartConsole
D. You can install Jumbo Hotfix accumulators with the Central Deployment in SmartConsole.
Answer: (SHOW ANSWER)

NEW QUESTION: 3
What are SmartEvent Features and Capabilities?

A. 300+ Check Point Security Best Practices, Monitoring in real time policy changes, Regulatory standards Best Practices
B. Full threat visibility, Real-time forensics, Immediate response
C. SmartDashboards, SmartLogs, SmartEvents
D. Compliance Reports, Events Logs and Reports, Best Practices Tests
Answer: (SHOW ANSWER)
SmartEvent provides centralized event correlation and analysis to deliver complete visibility into threats, supports real-time investigation and forensics of security incidents, and enables immediate response through alerts and automated actions.

NEW QUESTION: 4
Which Technology family does ElasticXL belong to?
A. ClusterXL
B. Scalable Platforms
C. SecurePlatform
D. SyncXL
Answer: (SHOW ANSWER)
ElasticXL belongs to the Scalable Platforms family, designed to provide high-performance, scalable, and flexible firewall deployments that can handle large traffic volumes across multiple cluster members.

NEW QUESTION: 5
Under which circumstances are automatic scans performed for Continuous Compliance Monitoring?
A. Every time the CPM and CPD process was restarted.
B. Every time the FWD or CPM service on the gateway was restarted.
C. Daily and SmartConsole changes with the Publish action.
D. Daily and weekly.
Answer: (SHOW ANSWER)
Continuous Compliance Monitoring performs automatic scans on a regular daily schedule and also whenever policy or configuration changes are published in SmartConsole, ensuring compliance checks reflect the latest environment updates.

NEW QUESTION: 6
How many interfaces are required as a minimum on each ElasticXL Cluster member?
A. Five
B. Six
C. At least three
D. At least four
Answer: (SHOW ANSWER)

Each ElasticXL cluster member requires at least four interfaces: one for management, one for internal traffic, one for external traffic, and one dedicated Sync interface for state synchronization.

NEW QUESTION: 7
Which Check Point process provides logging services, such as forwarding logs from Gateway to Log Server, providing Log Export API (LEA) & Event Logging API (ELA) services.
A. CPVIEWD
B. CPD
C. DASSERVICE
D. FWD
Answer: (SHOW ANSWER)

NEW QUESTION: 8
VTI in Site-2-Site VPN stands for_____ .
A. Virtual Tunnel Interface
B. VPN Transfer Interface
C. Virtual Transfer Interface
D. VPN Tunnel Interface
Answer: A (LEAVE A REPLY)
VTI stands for Virtual Tunnel Interface, which is a logical routed interface used in site-to-site VPNs to create route-based VPNs, allowing traffic to be routed through the tunnel like a regular network interface.

NEW QUESTION: 9
Alice knows about the Check Point Management HA installation from Bob and needs to know which Check Point Security Management Server is currently in "Active" state. Alice uses the Check Point SmartConsole tool. Which Check Point Console is needed to lookup for the Management High Availability status?
A. SmartView Tracker -> Log Search "Mgmt HA Status"
B. SmartUpdate -> Package Repository -> Management High Availability
C. Gaia Portal -> Overall View -> Management High Availability
D. Check Point SmartConsole -> Applications Menu -> Management High Availability
Answer: (SHOW ANSWER)
The Management High Availability status is viewed directly in SmartConsole through the Applications menu, where the Management High Availability view displays which management server is currently active and which is standby.

NEW QUESTION: 10
What is the oldest software version (on a security gateway) that an R82 Security Management Server is supported to manage?

A. R81

B. There is no backward compatibility and all gateways must be installed with the same version as the SMS.
C. R80.10
D. R77.30
Answer: (SHOW ANSWER)
An R82 Security Management Server can manage gateways running as far back as R77.30, providing backward compatibility for managing legacy gateways while allowing gradual upgrades.

NEW QUESTION: 11
To form a tunnel IKEv2 uses two exchange types - IKE_SA_INIT and IKE_AUTH. How many packets are transferred between the VPN peer gateways during the two exchanges?
A. Each exchange involves two messages, making a total of 4 packets.
B. For a site-to-site VPN on Check Point using IKEv2, the normal exchange is indeed nine packets
C. 9 packets unless legacy peers are included in the VPN community, which uses just 6 packets, 3 per exchange.
D. 6 packets. There are 4 in the SA_INIT exchange because of the Diffie Hellman process.
Answer: (SHOW ANSWER)
IKEv2 uses two exchanges, and each exchange consists of one request and one response message between the peers, resulting in two packets per exchange and four packets total to establish the tunnel.

NEW QUESTION: 12
During the policy installation, the CPM process needs to make a decision for Full Installation Policy or Fast Installation Policy. Depending on the decision the CPM process decides what kind of dump will be used. Which statement is true for the Fast Installation Policy?
A. Modern Dump always combines the Legacy Dump in which the pre-verified and pre-generated code is included
B. Modern Dump files never include the pre-verified and pre-generated code
C. Modern Dump files are sent to the FWM (Firewall) process, which is responsible for code generation and compilation
D. Modern Dump files already include the pre-verified and pre-generated code
Answer: (SHOW ANSWER)
For a Fast Installation Policy, Modern Dump is used and it already contains pre-verified and pre-generated compiled policy code, allowing the gateway to load the policy directly without additional compilation, which significantly speeds up installation.

NEW QUESTION: 13
Internet Key Exchange (IKE) a standard key management protocol that is used to do what exactly?
A. Renew both Phase 1 and Phase 2 IPSec keys when they expire.

B. Renew the Phase 2 key when it expires, after 60 minutes by default.
C. Update the VPN Domain information and renew expired keys when they expire.
D. Create the VPN tunnels by, Authenticating peers, agreeing on keys and methods to be used for encryption.
Answer: (SHOW ANSWER)
Internet Key Exchange is used to establish VPN tunnels by authenticating the peers and negotiating the cryptographic keys and encryption methods that will protect the IPsec communication.

NEW QUESTION: 14
How does SmartEvent determine whether events originated internally or externally?
A. By defining the Internal Network under the Initial Settings in SmartEvent GUI Client
B. Events with a non-routable private source IPs are considered to be originating from internal networks
C. SmartEvent queries Security Gateway topology to determining the direction of events
D. SmartEvent uses AI / ML to determine the direction of events
Answer: C (LEAVE A REPLY)
SmartEvent determines whether events are internal or external by querying the Security Gateway for its topology, including interfaces, network objects, and routing information, to accurately assess the source and destination of traffic.

NEW QUESTION: 15
Which command will allow an administrator to manually load policy files on the gateway?
A. fw fetch
B. fw load
C. fw install
D. fw policy
Answer: (SHOW ANSWER)
The fw fetch command manually retrieves and loads the security policy from the Security Management Server to the gateway, allowing an administrator to install the policy directly on the gateway without using SmartConsole.

NEW QUESTION: 16
What is the CLI command to check the Deployment Agent Built Number?
A. show deployment agent -v
B. show installer version
C. show deployment agent --version
D. show installer status
Answer: C (LEAVE A REPLY)
The command show deployment agent --version is used in CLI to display the build number and version information of the Check Point Deployment Agent installed on the system.

NEW QUESTION: 17
When creating a VPN tunnel with a third party product which object should you create in Smart Console to represent the remote side?
A. Externally Managed VPN Gateway
B. Gateway
C. Host
D. Interoperable Object
Answer: D (LEAVE A REPLY)
For third-party VPN devices, an Interoperable Device object is created to represent the remote peer, allowing configuration of standard IPsec parameters and interoperability without requiring full Check Point gateway management.

NEW QUESTION: 18
The Gateways has to mutually authenticate during the IPSec negotiation phase. There are two methods for this, namely:
A. Pre-shared secret and PKI Certificate
B. Kerberos and LDAP
C. OCSP and Certificate Revocation List
D. RSA SecurID and Dynamic ID
Answer: (SHOW ANSWER)
During IPsec negotiation, gateways authenticate each other using either a shared secret key configured on both peers or digital certificates issued by a trusted PKI to verify identity securely.

NEW QUESTION: 19
How many packets are used in Aggressive Mode for negotiation?
A. 3
B. 4
C. 8
D. 6
Answer: (SHOW ANSWER)

Aggressive Mode completes the Phase 1 negotiation using only three messages between the peers, combining identity, key exchange, and authentication steps to establish the IKE Security Association more quickly than Main Mode.

NEW QUESTION: 20

What is Modern Dump?

A. It's database dump with information stored without pre-generated code that require further verification but does not require compilation before transfer to the Security Gateway

B. It's database dump with information stored with pre-generated code that require further compilation or verification before transfer to the Security Gateway

C. It's database dump with information stored without pre-generated code that does not require further compilation or verification before transfer to the Security Gateway

D. It's database dump with information stored with pre-generated code that does not require further compilation or verification before transfer to the Security Gateway

Answer: (SHOW ANSWER)

Modern Dump stores the database with pre-generated and pre-compiled code on the Management Server, so the Security Gateway can receive and load the policy directly without additional compilation or verification, resulting in faster and more efficient policy installation.

NEW QUESTION: 21

How many Secondary Security Management Servers does Check Point allow a customer to deploy?

A. On premises deployments allow only one Secondary server. Public cloud deployments allow multiple Secondary servers.

B. You can install only one Secondary Security Management Server. The licenses limit the solution to only one Standby server.

C. You can install one or more Secondary Security Management Servers.

D. You can install only one Security Management Server. The Active server can only synchronize to one Standby server.

Answer: (SHOW ANSWER)

Check Point allows the deployment of one or more Secondary Security Management Servers in a Management HA setup, providing redundancy and synchronized backups of the primary management database.

NEW QUESTION: 22

Where does an administrator need to navigate to in the SmartConsole to carry out a Central Deployment upgrade?

A. COMMAND LINE

B. GATEWAYS & SERVERS

C. MANAGE & SETTINGS

D. INFINITY SERVICES

Answer: C (LEAVE A REPLY)
Central Deployment is managed from the Manage & Settings section in SmartConsole, where administrators access the Central Deployment tool to centrally upgrade and manage gateways and servers.

NEW QUESTION: 23
When a solution is configured with Route-based VPN method what interfaces are used?
A. External interface with a secondary IP address
B. Virtual Tunnel Interfaces (VTI)
C. Only the internal interfaces, which are included in a special Route-based Domain (Network Group object).
D. The Gaia Portal Web User Interface (WebUI)
Answer: (SHOW ANSWER)

NEW QUESTION: 24
In Management HA, changes in policy and object are performed through the active server. What happens if the active server fails or is taken offline?
A. One of the standby servers must be promoted to Primary Management Server to make it active
B. The standby server with the highest priority set by the administrator automatically becomes active
C. A changeover can be initiated manually to make a standby server become active
D. The closest standby server will immediately become active within 3 seconds
Answer: C (LEAVE A REPLY)
In Management High Availability, failover is manual by default, so if the active server fails or is taken offline, an administrator must manually initiate a changeover to promote a standby server to become the active server.

NEW QUESTION: 25
What does CPUSE stand for?
A. Check Point Update Security Engine
B. Check Point Upgrade Security Engine
C. Check Point Upgrade Service Engine
D. Check Point Update Service Engine
Answer: (SHOW ANSWER)
CPUSE stands for Check Point Upgrade Service Engine, which is the tool used to manage and perform upgrades of Check Point software components, including gateways and management servers.

NEW QUESTION: 26
What should be upgraded first in Advanced Upgrade Method?

A. Dedicated Log Server
B. Secondary Management Server
C. Primary Management Server
D. Security Gateway
Answer: (SHOW ANSWER)
In the Advanced Upgrade method, the Primary Management Server is upgraded first because it serves as the source for database synchronization and ensures that dependent components like secondary servers and gateways can properly receive policies and updates after the upgrade.

NEW QUESTION: 27
What is the correct statement about requirement of a JSON configuration file when upgrading a Security Management / Log / SmartEvent Server using CPUSE?
A. A JSON configuration file is required to upgrade any Check Point device prior to R80.20 when upgrading to R82 or above release
B. There is no such requirement of a JSON configuration file when using CPUSE. The CPUSE upgrade is completely automatic
C. A JSON configuration file is required only if there is a change of IP address on an of the Security Management / Log / SmartEvent servers
D. A JSON configuration is always required when upgrading a Security Management / Log / SmartEvent server to R82 or above release
Answer: (SHOW ANSWER)
When upgrading a Security Management, Log, or SmartEvent Server to R82 or later using CPUSE, a JSON configuration file is mandatory to define the target deployment parameters and ensure the upgrade process correctly preserves and migrates the server configuration.

NEW QUESTION: 28
Can a VPN Gateway be a member of more than one VPN community?
A. No, it could be used only in one VPN Community.
B. Yes, it is possible, but with correct modifications of vpn_route.conf file on each VPN Gateway
C. Yes, if it doesn't pair with another VPN Gateway in more than one VPN Community.
D. Yes, it could be used in more than one VPN Community, if all VPN Gateways are managed with the same Security Management.
Answer: (SHOW ANSWER)
A VPN Gateway can participate in multiple VPN communities as long as all gateways are managed by the same Security Management Server, which allows the management database to coordinate policies, encryption domains, and tunnel configurations correctly across all communities.

NEW QUESTION: 29
According to the policy installation, the transfer state (CPTA) is invoked by the FWM (Firewall) process which initiates the Transfer/Commit phase. On the Security Gateway side a process

receives them and first stores them into a temporary directory. Which process is true for receiving these files?

A. FWD

B. CPD

C. FWM

D. RAD

Answer: (SHOW ANSWER)

On the Security Gateway, the Firewall Daemon is responsible for receiving the transferred policy files, storing them temporarily, and then loading and enforcing the installed security policy.

NEW QUESTION: 30

How would you import an exported Management Database?

A. $FWDIR/usr/bin/migrate import /<Path>/<ExportFileName>

B. $FWDIR/scripts/migrate_server import -v /<Path>/<ExportFileName>

C. $FWDIR/bin/upgrade_tools/migrate import /<Path>/<ExportFileName>

D. You can only accomplish this task via Gaia Portal.

Answer: (SHOW ANSWER)

To import an exported Management Database, the command $FWDIR/scripts/migrate_server import -v /<Path>/<ExportFileName> is used, which restores the database into the target Security Management Server for the specified version.

NEW QUESTION: 31

Alice & Bob are tasked from their security team lead for deploying Advanced Security Monitoring for all their Check Point Security Gateway(s)/Cluster(s). Which of the features and capabilities of SmartEvent is included?

A. Full threat visibility

B. Medium threat visibility

C. Low threat visibility

D. High threat visibility

Answer: (SHOW ANSWER)

SmartEvent provides full threat visibility by correlating logs and events from multiple gateways, enabling real-time forensics, comprehensive monitoring, and immediate response to security incidents.

NEW QUESTION: 32
When the CPM process does a Modern Dump, what is happening?
A. CPM is using a new version of Postgre SQL to optimize the policy installation, and allow it to happen faster.
B. When doing backups in Gaia CPM uses Modern Dump and is able to export the database faster in R8x version than previous versions.
C. Using pre-generated code does not require further compilation or verification before transfer to the Security Gateway.
D. CPM can bypass FWM and install updated and new rules directly to the Security Gateway.
Answer: (SHOW ANSWER)
During a Modern Dump, the process generates pre-compiled policy code in advance so it can be transferred directly to the Security Gateway without additional compilation or verification, which speeds up policy installation.

NEW QUESTION: 33
Any VPN Gateway that can establish a direct VPN Tunnel with any Peer Gateway is member of which VPN Community
A. Direct Community
B. Any Community
C. Star Community
D. Mesh Community
Answer: (SHOW ANSWER)
In a Mesh Community, every VPN gateway can establish a direct tunnel with every other member, enabling full any-to-any connectivity between all participating gateways.

NEW QUESTION: 34
What is true about the magg1 and Sync interfaces on an ElasticXL Cluster?
A. magg1 is a bonded interface, Sync is also a bonded interface
B. magg1 is a secondary interface of the Mgmt Port, Sync is the Sync port
C. magg1 is a bonded interface, Sync is an individual Sync Port
D. magg1 is only available in Maestro and is a disabled and unused port in ElasticXL. Sync is the Sync Port
Answer: (SHOW ANSWER)
In an ElasticXL Cluster, magg1 functions as a bonded management aggregate interface that combines multiple links for management connectivity and redundancy, while the Sync interface is a dedicated individual port used specifically for state synchronization between cluster members.

NEW QUESTION: 35

Which Components can be upgraded using Central Deployment Tool (CDT) in SmartConsole?
A. Gateways / Cluster members.
B. Multi-Domain Servers, Management Servers and Gateways.
C. Gateways, Clusters, Management Servers.
D. Gateways, Clusters and Standalone Deployments.
Answer: (SHOW ANSWER)
The Central Deployment Tool in SmartConsole can be used to upgrade Check Point Gateways, Cluster members, and Management Servers, providing centralized management for consistent software updates across the deployment.

NEW QUESTION: 36
Where can you see and search records of action done by R80 SmartConsole administrators?
A. In Smartlog, all logs
B. In the Logs & Monitor, logs, select "Audit Log View"
C. In SmartView Tracker, open active log
D. In SmartAudit Log View
Answer: (SHOW ANSWER)

NEW QUESTION: 37
How many packets are used in IKEv1 Phase1 Main Mode exchange?
A. 6
B. 5
C. 8
D. 3
Answer: (SHOW ANSWER)
IKEv1 Phase 1 Main Mode uses three request-response exchanges between peers, resulting in six total packets to negotiate parameters, exchange keys, and authenticate both sides.

NEW QUESTION: 38
When an upgrade is required on 21 Security Gateways managed on a single SMS, the administrator prefers using Central Deployment with SmartConsole. Is this a recommended best practice in such scenarios? Can the administrator choose to upgrade all the Security Gateways together, or must it be done one at a time?
A. Yes, Central Deployment with SmartConsole is a recommended method for upgrading multiple Security Gateways. The administrator can select all the 21 Security Gateways for upgrade in a batch mode, however, only 1 Gateway can run the installation at a time while the others will be queued up.
B. Yes, Central Deployment with SmartConsole is a recommended method for upgrading multiple Security Gateways. The administrator can select only up to 10 Security Gateways for upgrade in a batch mode and these will run simultaneously. Once a batch upgrade is completed, another batch can be selected.

C. No, Central Deployment is not a recommended method when there are more than 5 Security Gateways to be upgraded. The administrator must use Gaia Portal to upgrade the Security Gateways.
D. Yes, Central Deployment with SmartConsole is a recommended method for upgrading multiple Security Gateways. The administrator can select all the 21 Security Gateways for upgrade in a batch mode, however, only up to 10 Gateways can run the installation at the same time while the others will be queued up.
Answer: (SHOW ANSWER)
Central Deployment with SmartConsole is the recommended method for upgrading multiple Security Gateways. Administrators can select all gateways in a batch, but the system allows only up to 10 concurrent installations at a time, with remaining gateways queued for sequential upgrade.

NEW QUESTION: 39
What is the command to get the state information of the interfaces of a cluster node?
A. get cluster elastic interfaces
B. show interfaces -a
C. show cluster info interfaces
D. ifconfig -a -clx
Answer: (SHOW ANSWER)
The command show cluster info interfaces is used on a cluster member to display the state and status of all interfaces, providing detailed information about connectivity, sync, and operational status within the cluster.

NEW QUESTION: 40
Which daemon makes the decision if Modern Dump or Legacy Dump should be used during Policy Installation?

A. FWM (Firewall Management)
B. CPTA (Check Point Transfer Agent)
C. CPD (Check Point Daemon)
D. CPM (Check Point Management)
Answer: (SHOW ANSWER)
The Check Point Management process controls policy installation logic and determines whether to use Modern Dump or Legacy Dump based on the type of installation, handling the preparation of the appropriate dump format before transfer to the gateway.

NEW QUESTION: 41
Which of the following is a trigger for synchronization between Active and Standby Management Servers?
A. Publishing a session in SmartConsole
B. Making a change in a network object and clicking on OK

C. Running the Save operation from the SmartConsole toolbar or Menu
D. After 10 seconds of inactivity in SmartConsole
Answer: (SHOW ANSWER)
Synchronization between active and standby Management Servers is triggered when a session is published, because publishing commits the changes to the management database and initiates the synchronization of those updates to the standby server.

NEW QUESTION: 42
Alice wants to upgrade the current security management machine to R82 and she wants to check the Deployment Agent status over the GAIA CLISH. Which of the following GAIA CLISH commands is correct?
A. show agent status
B. show installer packages
C. show uninstaller status
D. show installer status
Answer: (SHOW ANSWER)
The show installer status command in GAIA CLISH displays the current status of the Check Point Deployment Agent, including any ongoing or pending installation or upgrade tasks on the system.

NEW QUESTION: 43
What is correct regarding the target device for deploying SmartEvent components?
A. SmartEvent is just a blade on Security Management Server and can be activated on a Primary or Secondary SMS only
B. SmartEvent works by correlating logs, hence it has to be deployed on each log server. If any log server does not include SmartEvent components then its logs will not be correlated
C. SmartEvent is always a dedicated Standalone exclusive device
D. SmartEvent can be integrated with the Security Management Server, or deployed on a dedicated Log or SmartEvent Server
Answer: (SHOW ANSWER)
SmartEvent components can be deployed on the Security Management Server, on a dedicated Log Server, or on a dedicated SmartEvent Server, allowing flexible architecture depending on performance and scalability requirements.

NEW QUESTION: 44
In SmartEvent Settings & Policy App, Severity contains which options?
A. Informational, Warning, Low, Medium, High
B. Low, Medium, High
C. Low, Medium, High, Critical
D. Informational, Low, Medium, High, Critical
Answer: (SHOW ANSWER)

SmartEvent severity levels classify events by impact and include Informational, Low, Medium, High, and Critical, allowing administrators to prioritize alerts and responses based on risk level.

NEW QUESTION: 45
What are the main stages of a policy installation?
A. Verification, Compilation, Transfer and Commit
B. Verification, Commit, Installation
C. Initiation, Conversion and FWD REXEC
D. Initiation, Conversion and Save
Answer: (SHOW ANSWER)

NEW QUESTION: 46
What can be upgraded using Central Deployment?
A. Security Management Servers, Gateways, Cluster Members
B. Security Management Servers, Dedicated Log Servers, Gateways, Cluster Members
C. Gateways, Cluster Members
D. Only Gateways (no Clusters)
Answer: (SHOW ANSWER)
Central Deployment allows administrators to upgrade Security Management Servers, individual Gateways, and Cluster members in a coordinated manner, ensuring consistent software versions across the deployment.

NEW QUESTION: 47
When the Management Server Database is exported using the migrate_server tool, what is exported?
A. The current database revision and unpublished changes that are saved are all exported
B. All previous and current revisions of the database are exported
C. Last 3 revisions of the database are exported
D. Only the current database revision is exported, unpublished changes are not exported
Answer: (SHOW ANSWER)

When using the migrate_server tool, both the current active database revision and any unpublished changes that have been saved are exported, ensuring a complete snapshot of the management configuration for migration.

NEW QUESTION: 48
Alice & Bob are tasked from their security team lead for deploying Advanced Security Monitoring for all their Check Point Security Gateway(s)/Cluster(s). Which of the features and capabilities of SmartEvent is included?
A. Statistics forensics and log Investigation
B. Real-time logging and status Investigation
C. Historical forensics and Real-time Investigation
D. Real-time forensics and event Investigation
Answer: (SHOW ANSWER)
SmartEvent provides real-time forensics and event investigation by correlating security events as they occur, enabling administrators to analyze incidents promptly and respond effectively.

NEW QUESTION: 49
As part of the SmartEvent Initial Settings which option is not automatically configured initially and needs to be configured manually during the deployment?
A. Correlation Units
B. Offline Jobs
C. Internal Networks
D. SmartEvent Servers
Answer: C (LEAVE A REPLY)
Internal Networks must be defined manually during SmartEvent deployment because the system cannot automatically determine which networks are considered internal, and this information is required for accurate event correlation and traffic direction analysis.

NEW QUESTION: 50
What is insights?
A. An application that can show internal configuration for each ElasticXL members
B. An excellent monitoring dashboard for Scalable Platforms
C. A command that gives consolidated information about threats that were discovered in internal network
D. An excellent tool for discovering network names in environment
Answer: (SHOW ANSWER)
Insights is a monitoring dashboard designed for Scalable Platforms like ElasticXL, providing administrators with real-time visibility into cluster performance, resource utilization, and overall system health.

NEW QUESTION: 51

The installation of a package via SmartConsole CANNOT be applied on
A. Multiple Security Gateways and/or Clusters
B. A full Security Cluster (All Cluster Members included)
C. A single Security Gateway
D. R81.20 Security Management Server
Answer: (SHOW ANSWER)

NEW QUESTION: 52
What are valid Policy Types in R81.X?
A. Access Control, Threat Prevention, QoS, Desktop Security
B. Access Control, RemoteAccess VPN, NAT, IPS
C. Access Control, IPS, Threat Emulation, NAT
D. Access Control, IPS, QoS, DLP
Answer: (SHOW ANSWER)

NEW QUESTION: 53
When deploying hotfixes with Smart Console, how many concurrent installations can take place?
A. 20
B. 10
C. 5
D. 15
Answer: (SHOW ANSWER)
SmartConsole allows up to 10 concurrent hotfix installations during a deployment, enabling administrators to update multiple gateways or servers simultaneously while controlling system load.