Checkpoint.Pre.156-215.81.50q - DEMO

Number: 156-215.81
Passing Score: 800
Time Limit: 120 min

Exam Code: 156-215.81
Exam Name: Check Point Certified Security Administrator R81
Website: https://VCEup.com/

Exam A

QUESTION 1
Which set of objects have an Authentication tab?

A. Templates, Users
B. Users, Networks
C. Users, User Group
D. Networks, Hosts

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
Which rule is responsible for the user authentication failure?

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track
1	0	NetBIOS	Any	Any	Any Traffic	NBT	drop	None
2	0	Management	webSingapore	fwsingapore	Any Traffic	ssh https	accept	None
3	0	Stealth	Any	fwsingapore	Any Traffic	Any	drop	Log
4	0	User Auth	Any	webSingapore	Any Traffic	http	User Auth	Log
5	0	Partner City	net_singapore net_rome	net_rome net_singapore	rome_singapore	http	accept	Log
6	0	Network Traffic	net_singapore net_sydney	Any	Any Traffic	http dns icmp-proto ftp https	accept	Log
7	0	Cleanup	Any	Any	Any Traffic	Any	drop	Log

A. Rule 4
B. Rule 6
C. Rule 3
D. Rule 5

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
Which tool CANNOT be launched from SmartUpdate R77?

A. IP Appliance Voyager
B. snapshot
C. GAiA WebUI
D. cpinfo

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 4

Which of the following is a hash algorithm?

A. 3DES
B. IDEA
C. DES
D. MD5

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 5
Katie has been asked to do a backup on the Blue Security Gateway. Which command would accomplish this in the Gaia CLI?

A. Blue > add local backup
B. Expert&Blue#add local backing
C. Blue > set backup local
D. Blue > add backup local

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
You want to establish a VPN, using certificates. Your VPN will exchange certificates with an external partner. Which of the following activities sh you do first?

A. Create a new logical-server object to represent your partner's CA
B. Exchange exported CA keys and use them to create a new server object to represent your partner's Certificate Authority (CA)
C. Manually import your partner's Certificate Revocation List.
D. Manually import your partner's Access Control List.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
What must a Security Administrator do to comply with a management requirement to log all traffic accepted through the perimeter Security Gateway?

A. In Global Properties > Reporting Tools check the box Enable tracking all rules (including rules marked as None in the Track column). Send these logs to a secondary log server for a complete logging history. Use your normal log server for standard logging for troubleshooting.
B. Install the View Implicit Rules package using SmartUpdate.
C. Define two log servers on the R77 Gateway object. Lof Implied Rules on the first log server. Enable Log Rule Base on the second log server. Use SmartReporter to merge the two log server records into the same database for HIPPA log audits.
D. Check the Log Implied Rules Globally box on the R77 Gateway object.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 8
What is the appropriate default Gaia Portal address?

A. HTTP://[IPADDRESS]
B. HTTPS://[IPADDRESS]:8080
C. HTTPS://[IPADDRESS]:4434
D. HTTPS://[IPADDRESS]

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 9
Your boss wants you to closely monitor an employee suspected of transferring company secrets to the competition. The IT department discovered the suspect installed a WinSCP client in order to use encrypted communication. Which of the following methods is BEST to accomplish this task?

A. Use SmartView Tracker to follow his actions by filtering log entries that feature the WinSCP destination port. Then, export the corresponding entries to a separate log file for documentation.
B. Use SmartDashboard to add a rule in the firewall Rule Base that matches his IP address, and those of potential targets and suspicious protocols. Apply the alert action or customized messaging.
C. Watch his IP in SmartView Monitor by setting an alert action to any packet that matches your Rule Base and his IP address for inbound and outbound traffic.
D. Send the suspect an email with a keylogging Trojan attached, to get direct information about his wrongdoings.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 10
Match the following commands to their correct function. Each command has one function only listed.

Command	Function
C1 cp_admin_convert	F1: export and import different revisions of the database.
C2 cpca_client	F2: export and import policy package
C3 cp_merge	F3: transfer Log data to an external database.
C4 cpwd_admin	F4: execute operations on the ICA.
	F5: invokes and monitors critical processes such as Check Point daemons on the local machine.
	F6: automatically export administrator definitions that were created in `cpconfig` to SmartDashboard.

A. C1>F6; C2>F4; C3>F2; C4>F5
B. C1>F2; C2>F1; C3>F6; C4>F4
C. C1>F2; C2>F4; C3>F1; C4>F5
D. C1>F4; C2>F6; C3>F3; C4>F5

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 11
Which of the following is NOT an option for internal network definition of Anti-spoofing?

A. Specific – derived from a selected object
B. Route-based – derived from gateway routing table
C. Network defined by the interface IP and Net Mask
D. Not-defined

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12
MegaCorp's security infrastructure separates Security Gateways geographically. You must request a central license for one remote Security Gateway.
How do you apply the license?

A. Using the remote Gateway's IP address, and attaching the license to the remote Gateway via SmartUpdate.
B. Using your Security Management Server's IP address, and attaching the license to the remote Gateway via SmartUpdate.
C. Using the remote Gateway's IP address, and applying the license locally with command cplic put.
D. Using each of the Gateway's IP addresses, and applying the licenses on the Security Management Server with the command cprlic put.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 13
A digital signature:

A. Guarantees the authenticity and integrity of a message.
B. Automatically exchanges shared keys.
C. Decrypts data to its original form.
D. Provides a secure key exchange mechanism over the Internet.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 14
According to Check Point Best Practice, when adding a 3rd party gateway to a Check Point security solution what object SHOULD be added? A(n):

A. Interoperable Device
B. Network Node
C. Externally managed gateway
D. Gateway

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 15
You find a suspicious connection from a problematic host. You decide that you want to block everything from that whole network, not just the problematic host. You want to block this for an hour while you investigate further, but you do not want to add any rules to the Rule Base. How do you achieve this?

A. Use dbedit to script the addition of a rule directly into the Rule Bases_5_0.fws configuration file.
B. Select Block intruder from the Tools menu in SmartView Tracker.
C. Create a Suspicious Activity Rule in Smart Monitor.
D. Add a temporary rule using SmartDashboard and select hide rule.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
When launching SmartDashboard, what information is required to log into R77?

A. User Name, Management Server IP, certificate fingerprint file
B. User Name, Password, Management Server IP
C. Password, Management Server IP
D. Password, Management Server IP, LDAP Server IP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 17
A Cleanup rule:

A. logs connections that would otherwise be dropped without logging by default.
B. drops packets without logging connections that would otherwise be dropped and logged by default.
C. logs connections that would otherwise be accepted without logging by default.
D. drops packets without logging connections that would otherwise be accepted and logged by default.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 18
You manage a global network extending from your base in Chicago to Tokyo, Calcutta and Dallas.
Management wants a report detailing the current software level of each Enterprise class Security Gateway. You plan to take the opportunity to create a proposal outline, listing the most cost-effective way to upgrade your Gateways. Which two SmartConsole applications will you use to create this report and outline?

A. SmartView Tracker and SmartView Monitor
B. SmartLSM and SmartUpdate
C. SmartDashboard and SmartView Tracker
D. SmartView Monitor and SmartUpdate

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 19
Which of the below is the MOST correct process to reset SIC from SmartDashboard?

A. Run cpconfig, and click Reset.
B. Click the Communication button for the firewall object, then click Reset. Run cpconfig on the gateway and type a new activation key.
C. Run cpconfig, and select Secure Internal Communication > Change One Time Password.
D. Click Communication > Reset on the Gateway object, and type a new activation key.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 20
Which of the following authentication methods can be configured in the Identity Awareness setup wizard?

A. Check Point Password
B. TACACS
C. LDAP
D. Windows password

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 21
An internal router is sending UDP keep-alive packets that are being encapsulated with GRE and sent through your R77 Security Gateway to a partner site. A rule for GRE traffic is configured for ACCEPT/LOG. Although the keep-alive packets are being sent every minute, a search through the SmartView Tracker logs for GRE traffic only shows one entry for the whole day (early in the morning after a Policy install).
Your partner site indicates they are successfully receiving the GRE encapsulated keep-alive packets on the 1-minute interval.
If GRE encapsulation is turned off on the router, SmartView Tracker shows a log entry for the UDP keep-alive packet every minute.
Which of the following is the BEST for this behavior?

A. The setting Log does not capture this level of detail for GRE. Set the rule tracking action to Audit since certain types of traffic can only be tracked this way.
B. The log unification process is using a LUUID (Log Unification Unique Identification) that has become corrupt. Because it is encrypted, the R77 Security Gateway cannot distinguish between GRE sessions. This is a known issue with GRE. Use IPSEC instead of the non-standard GRE protocol for encapsulation.
C. The Log Server log unification process unifies all log entries from the Security Gateway on a specific connection into only one log entry in the SmartView Tracker. GRE traffic has a 10 minute session timeout, thus each keep-alive packet is considered part of the original logged connection at the beginning of the day.
D. The Log Server is failing to log GRE traffic properly because it is VPN traffic. Disable all VPN configuration to the partner site to enable proper logging.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 22

Choose the correct statement regarding Implicit Rules.

A. To edit the Implicit rules you go to: Launch Button > Policy > Global Properties > Firewall.
B. Implied rules are fixed rules that you cannot change.
C. You can directly edit the Implicit rules by double-clicking on a specific Implicit rule.
D. You can edit the Implicit rules but only if requested by Check Point support personnel.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 23
You find that Users are not prompted for authentication when they access their Web servers, even though you have created an HTTP rule via User Authentication. Choose the BEST reason why.

A. You checked the cache password on desktop option in Global Properties.
B. Another rule that accepts HTTP without authentication exists in the Rule Base.
C. You have forgotten to place the User Authentication Rule before the Stealth Rule.
D. Users must use the SecuRemote Client, to use the User Authentication Rule.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
You have two rules, ten users, and two user groups in a Security Policy. You create database version 1 for this configuration. You then delete two existing users and add a new user group. You modify one rule and add two new rules to the Rule Base. You save the Security Policy and create database version 2. After a while, you decide to roll back to version 1 to use the Rule Base, but you want to keep your user database. How can you do this?

A. Run fwm dbexport -1 filename. Restore the database. Then, run fwm dbimport -1 filename to import the users.
B. Run fwm_dbexport to export the user database. Select restore the entire database in the Database Revision screen. Then, run fwm_dbimport.
C. Restore the entire database, except the user database, and then create the new user and user group.
D. Restore the entire database, except the user database.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 25
Which of the following are available SmartConsole clients which can be installed from the R77 Windows CD? Read all answers and select the most complete and valid list.

A. SmartView Tracker, SmartDashboard, CPINFO, SmartUpdate, SmartView Status
B. SmartView Tracker, SmartDashboard, SmartLSM, SmartView Monitor
C. SmartView Tracker, CPINFO, SmartUpdate
D. Security Policy Editor, Log Viewer, Real Time Monitor GUI

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 26
You have configured SNX on the Security Gateway. The client connects to the Security Gateway and the user enters the authentication credentials. What must happen after authentication that allows the client to connect to the Security Gateway's VPN domain?

A. SNX modifies the routing table to forward VPN traffic to the Security Gateway.
B. An office mode address must be obtained by the client.
C. The SNX client application must be installed on the client.
D. Active-X must be allowed on the client.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 27
All R77 Security Servers can perform authentication with the exception of one. Which of the Security Servers can NOT perform authentication?

A. FTP
B. SMTP
C. HTTP
D. RLOGIN

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
Your users are defined in a Windows 2008 R2 Active Directory server. You must add LDAP users to a Client Authentication rule. Which kind of user group do you need in the Client Authentication rule in R77?

A. External-user group
B. LDAP group
C. A group with a genetic user
D. All Users

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 29
What is Consolidation Policy?

A. The collective name of the Security Policy, Address Translation, and IPS Policies.
B. The specific Policy written in SmartDashboard to configure which log data is stored in the SmartReporter database.
C. The collective name of the logs generated by SmartReporter.
D. A global Policy used to share a common enforcement policy for multiple Security Gateways.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 30
Where do you verify that UserDirectory is enabled?

A. Verify that Security Gateway > General Properties > Authentication > Use UserDirectory (LDAP) for Security Gateways is checked
B. Verify that Global Properties > Authentication > Use UserDirectory (LDAP) for Security Gateways is checked.
C. Verify that Security Gateway > General Properties > UserDirectory (LDAP) > Use UserDirectory (LDAP) for Security Gateways is checked.
D. Verify that Global Properties > UserDirectory (LDAP) > Use UserDirectory (LDAP) for Security Gateways is checked.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 31
Which of the following actions do NOT take place in IKE Phase 1?

A. Peers agree on encryption method.
B. Diffie-Hellman key is combined with the key material to produce the symmetrical IPsec key.
C. Peers agree on integrity method.
D. Each side generates a session key from its private key and peer's public key.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 32
Which R77 GUI would you use to see number of packets accepted since the last policy install?

A. SmartView Monitor
B. SmartView Tracker
C. SmartDashboard
D. SmartView Status

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 33
Which of the following firewall modes DOES NOT allow for Identity Awareness to be deployed?

A. Bridge
B. Load Sharing
C. High Availability
D. Fail Open

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 34
What is the Manual Client Authentication TELNET port?

A. 23
B. 264
C. 900
D. 259

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 35
Jennifer McHanry is CEO of ACME. She recently bought her own personal iPad. She wants use her iPad to access the internal Finance Web server. Because the iPad is not a member of the Active Directory domain, she cannot identify seamlessly with AD Query. However, she can enter her AD credentials in the Captive Portal and then get the same access as on her office computer. Her access to resources is based on rules in the R77 Firewall Rule Base.
To make this scenario work, the IT administrator must:
1) Enable Identity Awareness on a gateway and select Captive Portal as one of the Identity Sources.
2) In the Portal Settings window in the User Access section, make sure that Name and password login is selected.
3) Create a new rule in the Firewall Rule Base to let Jennifer McHanry access network destinations.
Select accept as the Action.
4) Install policy.
Ms McHanry tries to access the resource but is unable. What should she do?

A. Have the security administrator select the Action field of the Firewall Rule “Redirect HTTPconnections to an authentication (captive) portal”.
B. Have the security administrator reboot the firewall.
C. Have the security administrator select Any for the Machines tab in the appropriate Access Role.
D. Install the Identity Awareness agent on her iPad.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 36
How many packets does the IKE exchange use for Phase 1 Main Mode?

A. 12
B. 1
C. 3
D. 6

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 37
What is also referred to as Dynamic NAT?

A. Automatic NAT
B. Static NAT
C. Manual NAT
D. Hide NAT

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 38
A client has created a new Gateway object that will be managed at a remote location. When the client attempts to install the Security Policy to the new Gateway object, the object does not appear in the Install On check box. What should you look for?

A. Secure Internal Communications (SIC) not configured for the object.
B. A Gateway object created using the Check Point > Externally Managed VPN Gateway option from the Network Objects dialog box.
C. Anti-spoofing not configured on the interfaces on the Gateway object.
D. A Gateway object created using the Check Point > Secure Gateway option in the network objects, dialog box, but still needs to configure the interfaces for the Security Gateway object.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 39
Which of the following is NOT a valid option when configuring access for Captive Portal?

A. From the Internet
B. Through internal interfaces
C. Through all interfaces
D. According to the Firewall Policy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 40
As you review this Security Policy, what changes could you make to accommodate Rule 4?

No.	Hits	Name	Source	Destination	VPN	Service	Action
		Limit Access to Gateways (Rule 1)					
1	0	Stealth	Corporate-internal-net	GW-group	Any Traffic	Any	drop
		VPN Access Rules (Rules 2-5)					
2	0	Site-to-Site	Any	Any	Any Traffic	CIFS ftp-port http https smtp	accept
3	0	Remote Access	Mobile-vpn-user@Any	Any	RemoteAccess	CIFS http https imap	accept
4	0	Clientless VPN	Clientless-vpn-user@Any	Corporate-WA-proxy-server	Any Traffic	https	User Auth
5	0	Web Server	L2TP-vpn-user@Any Customers@Any	Remote-1-web-server	Any Traffic	http	accept

A. Remove the service HTTP from the column Service in Rule 4.
B. Modify the column VPN in Rule 2 to limit access to specific traffic.
C. Nothing at all
D. Modify the columns Source or Destination in Rule 4

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 41
What happens when you run the command: fw sam -J src [Source IP Address]?

A. Connections from the specified source are blocked without the need to change the Security Policy.
B. Connections to the specified target are blocked without the need to change the Security Policy.
C. Connections to and from the specified target are blocked without the need to change the Security Policy.
D. Connections to and from the specified target are blocked with the need to change the Security Policy.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 42
VPN gateways must authenticate to each other prior to exchanging information. What are the two types of credentials used for authentication?

A. 3DES and MD5
B. Certificates and IPsec
C. Certificates and pre-shared secret
D. IPsec and VPN Domains

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 43
According to Check Point Best Practice, when adding a non-managed Check Point Gateway to a Check Point security solution what object SHOULD be added? A(n):

A. Gateway
B. Interoperable Device
C. Externally managed gateway
D. Network Node

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 44
You are about to integrate RSA SecurID users into the Check Point infrastructure. What kind of users are to be defined via SmartDashboard?

A. A group with generic user
B. All users
C. LDAP Account Unit Group
D. Internal user Group

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 45
Where does the security administrator activate Identity Awareness within SmartDashboard?

A. Gateway Object > General Properties
B. Security Management Server > Identity Awareness
C. Policy > Global Properties > Identity Awareness
D. LDAP Server Object > General Properties

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 46
While in SmartView Tracker, Brady has noticed some very odd network traffic that he thinks could be an intrusion. He decides to block the traffic for 60 minutes, but cannot remember all the steps. What is the correct order of steps needed to set up the block?
1)Select Active Mode tab in SmartView Tracker.
2) Select Tools > Block Intruder.
3) Select Log Viewing tab in SmartView Tracker.
4) Set Blocking Timeout value to 60 minutes.
5) Highlight connection that should be blocked.

A. 1, 2, 5, 4
B. 3, 2, 5, 4
C. 1, 5, 2, 4
D. 3, 5, 2, 4

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 47
You are about to test some rule and object changes suggested in an R77 news group. Which backup solution should you use to ensure the easiest restoration of your Security Policy to its previous configuration after testing the changes?

A. Manual copies of the directory $FWDIR/conf
B. upgrade_export command
C. Database Revision Control
D. GAiA backup utilities

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 48
You are using SmartView Tracker to troubleshoot NAT entries. Which column do you check to view the NAT'd source port if you are using Source NAT?

URL List Version	☐	100
Unreachable directories	☐	100
Update Service	☐	100
Update Source	☐	100
Update Status	☐	100
User Action Comment	☐	100
User Additional Information	☐	100
User Check	☐	100
User DN	☐	100
User Directory	☐	100
User Display Name	☐	100
User Group	☐	100
User Reported Wrong Category	☐	100
User Response	☐	100
User SID	☐	100
User UID	☐	100
User's IP	☐	100
UserCheck ID	☐	100
UserCheck Interaction Name	☐	100
UserCheck Message to User	☐	100
UserCheck Scope	☐	100
UserCheck User Input	☐	100
VLAN ID	☐	100
VPN Feature	☐	100
VPN Peer Gateway	☐	100
Version	☐	100
Virtual Link	☐	100
Virus Name	☐	100
VoIP Duration	☐	100
VoIP Log Type	☐	100
VoIP Reject Reason	☐	100

A. XlateDst

B. XlateSPort
C. XlateDPort
D. XlateSrc

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 49
What happens if the identity of a user is known?

A. If the user credentials do not match an Access Role, the traffic is automatically dropped.
B. If the user credentials do not match an Access Role, the system displays a sandbox.
C. If the user credentials do not match an Access Role, the gateway moves onto the next rule.
D. If the user credentials do not match an Access Role, the system displays the Captive Portal.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 50
Your company enforces a strict change control policy. Which of the following would be MOST effective for quickly dropping an attacker's specific active connection?

A. Change the Rule Base and install the Policy to all Security Gateways
B. Block Intruder feature of SmartView Tracker
C. Intrusion Detection System (IDS) Policy install
D. SAM – Suspicious Activity Rules feature of SmartView Monitor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: