KillTest

Higher Quality, Better Service!

Q&A

http://www.killtest.com

We offer free update service for one year.

Exam : **156-215.70**

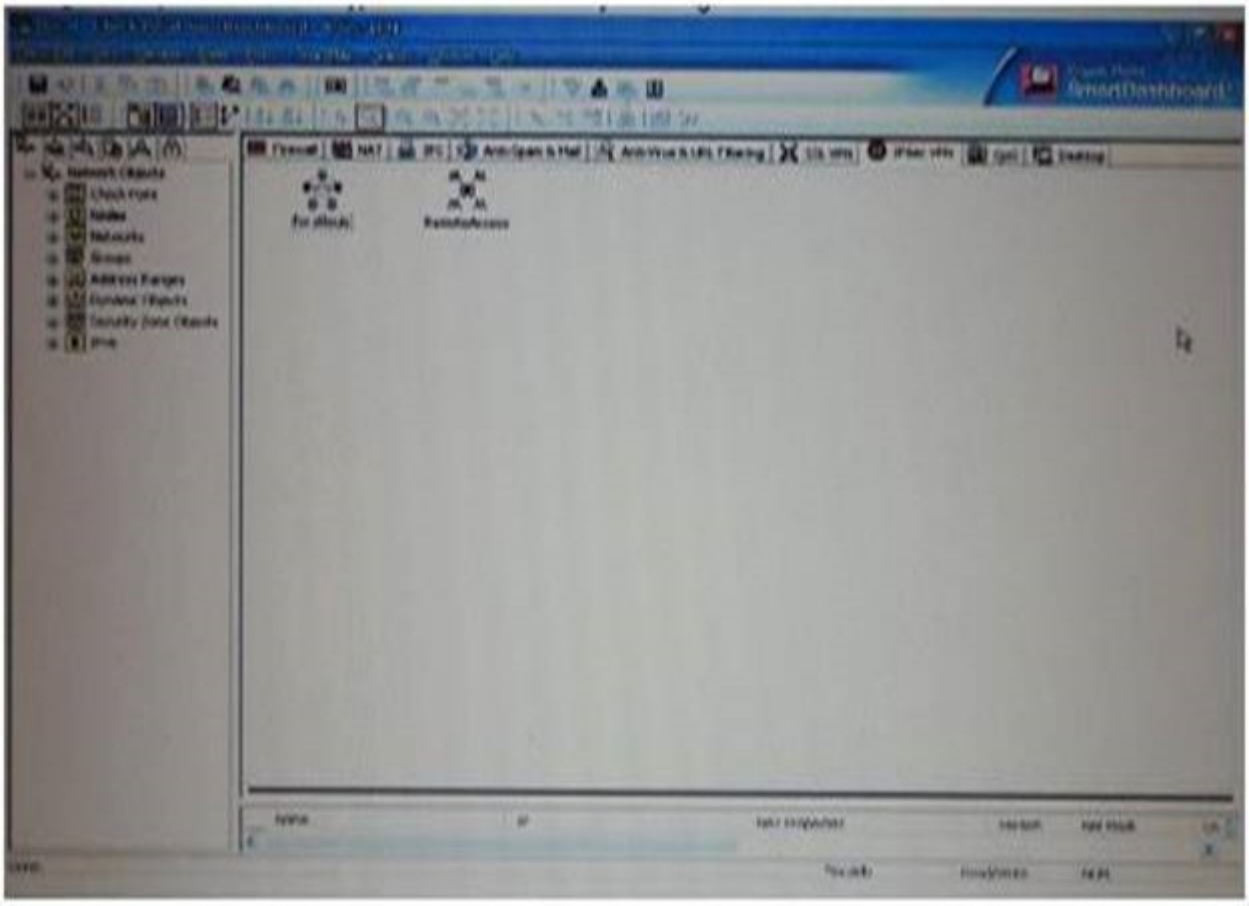
Title : Check Point Certified Security Administrator R70

Version : DEMO

1.You have blocked an IP address via the Block Intruder feature of SmartView Tracker How can you view the blocked addresses'?
A.Run f wm blockedview.
B.In SmartView Monitor, select the Blocked Intruder option from the query tree view
C.In SmartView Monitor, select Suspicious Activity Rules from the Tools menu and select the relevant Security Gateway from the list
D.In SmartView Tracker, click the Active tab.and the actively blocked connections displays
Answer: C

2.John is the Security Administrator in his company He installs a new R70 Security Management Server and a new R70 Gateway He now wants to establish SIC between them.After entering the activation key, the message "Trust established" is displayed in SmartDashboard, but SIC still does not seem to work because the policy won't install and interface fetching still does not work.What might be a reason for this?
A.This must be a human error.
B.The Gateway's time is several days or weeks in the future and the SIC certificate is not yet valid.
C.SIC does not function over the network.
D.It always works when the trust is established.
Answer: B

3.Using the output below, what type of VPN Community is configured for fw-stlouis?



A.Meshed
B.Domain-Based

C.Star
D.Traditional
Answer: A

4.What are you required to do before running upgrade__ export?
A.Run cpconfig and set yourself up as a GUI client.
B.Run a cpstop on the Security Management Server
C.Run a cpstop on the Security Gateway.
D.Close all GUI clients
Answer: B,C,D

5.You are installing a Security Management Server Your security plan calls for three administrators for this particular server.How many can you create during installation'?
A.Depends on the license installed on the Security Management Server
B.Only one with full access and one with read-only access
C.One
D.As many as you want
Answer: C

6.You are installing your R70Security Gateway.Which is NOT a valid option for the hardware platform?
A.Crossbeam
B.Solaris
C.Windows
D.IPSO
Answer: B

7.A Security Policy installed by another Security Administrator has blocked all SmartDashboard connections to the stand-alone installation of R70.After running the fw unloadlocal command, you are able to reconnect with SmartDashboard and view all changes.Which of the following change is the most likely cause of the block?
A.A Stealth Rule has been configured for the R70 Gateway.
B.The Allow control connections setting in Policy > Global Properties has been unchecked.
C.The Security Policy installed to the Gateway had no rules in it
D.The Gateway Object representing your Gateway was configured as an Externally Managed VPN Gateway.
Answer: B

8.In previous version, the full TCP three-way handshake was sent to the firewall kernel for inspection.How is this improved in current Flows/SecureXL?
A.Only the initial SYN packet is inspected The rest are handled by IPSO
B.Packets are offloaded to a third-party hardware card for near-line inspection
C.Packets are virtualized to a RAM drive-based FW VM
D.Resources are proactively assigned using predictive algorithmic techniques
Answer: A

9.Which command displays the installed Security Gateway version?
A.fw stat
B.cpstat -gw
C.fw ver
D.tw printver
Answer: C

10.Which statement defines Public Key Infrastructure? Security is provided
A.by authentication.
B.by Certificate Authorities, digital certificates, and two-way symmetric-key encryption.
C.by Certificate Authorities, digital certificates, and public key encryption.
D.via both private and public keys, without the use of digital Certificates.
Answer: C

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

12.What is a 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.
Answer: B

13.What CANNOT be configured for existing connections during a policy install?
A.Keep all connections
B.Keep data connections
C.Reset all connections
D.Re-match connections
Answer: C

14.Which OPSEC server can be used to prevent users from access.ng certain Web sites?
A.LEA
B.AMON
C.UFP
D.CVP
Answer: C

15.Assume an intruder has compromised your current IKE Phase 1 and Phase 2 keys.Which of the following options will end the intruder's access after the next Phase 2 exchange occurs?
A.Perfect Forward Secrecy
B.SHA1 Hash Completion
C.Phase 3 Key Revocation
D.M05 Hash Completion
Answer: A

16.Your R70 enterprise Security Management Server is running abnormally on Windows 2003 Server You decide to try reinstalling the Security Management Server, but you want to try keeping the critical Security Management Server configuration settings intact (i.e., all Security Policies, databases, SIC, licensing etc) What is the BEST method to reinstall the Server and keep its critical configuration?
A.1.Create a database revision control backup using the SmartDashboard
2.Create a compressed archive of the *FWDlR*\ conf and FWDiR8\lib directories and copy them to another networked machine.
3.Uninstall all R70 packages via Add/Remove Programs and reboot.
4.Install again as a primary Security Management Server using the R70 CD.
5.Reboot and restore the two archived directories over the top of the new installation, choosing to overwrite existing files.
B.1.Download the latest upgrade_export utility and run it from a c; \temp directory to export the configuration into a .tgz file
2.Skip any upgarde__verification warnings since you are not upgrading
3.Transfer the .tgz file to another networked machine
4.Download and run the cpclean utility and reboot
5.Use the R70 CD-ROM to select the uuarade import ootion to import the confiauration
C.1.Download the latest upqrade_expoct utility and run it from a \temp directory to export the configuration into a .tgz file
2.Perform any requested upgcade_veri¡êic tion sugested steps
3.Uninstall all R70 packages via Add/Remove Programs and reboot
4.Use SmartUpdate to reinstall the Security Management Server and reboot
5.Transfer the tgz file back to the local \temp
6.Run upgrade__import to import the configuration
D.1.Insert the F70 CD-ROM, and select the option to export the configuration using the latest upgrade utilities
2.Perform any requested upgrade_verification suggested steps and re-export the configuration if needed
3.Save the export " tgz file to a local c: \temp directory
4.Uninstall all R70 packages via Add/Remove Programs and reboot
5.Install again using the R70 CD-ROM as a primary Security Management Server and reboot
6.Run upgrade_import to import the configuration
Answer: C

17.You are trying to save a custom log query in R70 SmartView Tracker, but getting the following error "Could not save 'query-name' (Error Database is Read Only).
Which of the following is a likely explanation for this?

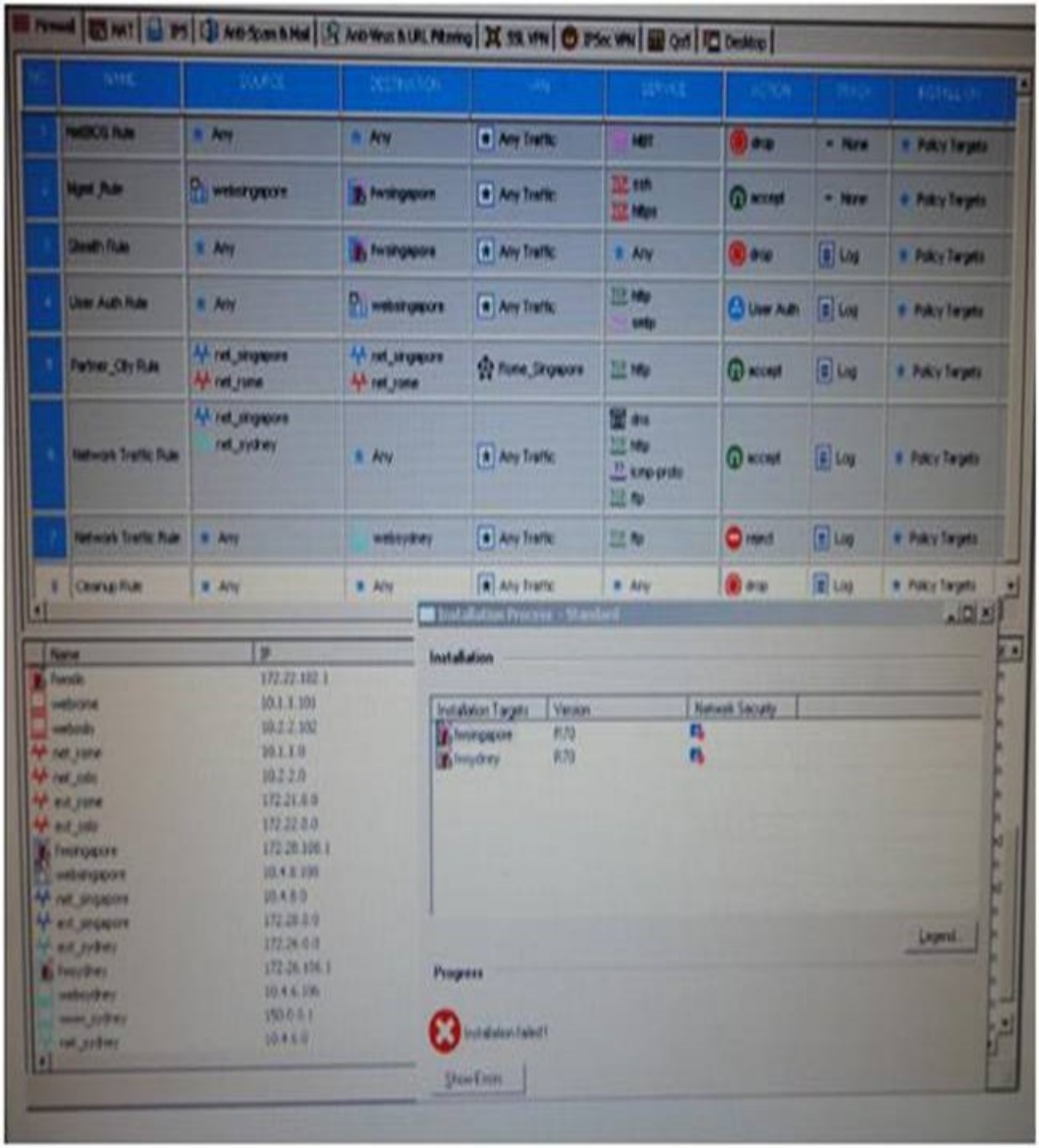
A.You have read-only rights to the Security Management Server catabase.
B.You do not have the explicit right to save a custom query in your administrator permission profile under SmartConsole customization
C.You do not have OS write permissions on the local SmartView Tracker PC in order to save the custom query locally
D.Another administrator is currently connected to the Security Management Server with read/write permissions which impacts your ability to save custom log queries to the Security Management Server.
Answer: A

18.Your company's Security Policy forces users to authenticate to the Gateway explicitly, before they can use any services.The Gateway does not allow the Telnet service to itself from any location.How would you configure authentication on the Gateway? With a:
A.Client Authentication for fully automatic sign on
B.Client Authentication rule using the manual sign-on method, using HTTP on port 900
C.Client Authentication rule, using partially automatic sign on
D.Session Authentication rule
Answer: B

19.Which opponent functions as the Internet Certificate Authority for R70?
A.Security Gateway
B.Management Server
C.Policy Server
D.SmartLSM
Answer: B

20.In a distributed management environment, the administrator has removed the default check from Accept Control Connections under the Policy > Global Properties > FireWall tab.In order for the Security Management Server to install a policy to the Firewall, an explicit rule must be created to allow the server to communicate to the Security Gateway on port_____.
A.256
B.80
C.900
D.259
Answer: A

21.Which rule is responsible for the installation failure?



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

22.External commands can be included in SmartView Tracker via the menu Tools > Custom Commands.The Security Management Server is running under SecurePlatform, and the GUI is on a system running Microsoft Windows.How do you run the command, traceroute on an IP address?

A.Use the program GUIdbedit to add the command traceroute to the properties of the Security Management Server.
B.Go to the menu Tools > Custom Commands and configure the Windows command tracert.exe to the list
C.There is no possibility to expand the three pre-defined options ping, whois, and Nslookup
D.Go to the menu.Tools > Custom Commands and configure the Linux command traceroute to the list
Answer: B

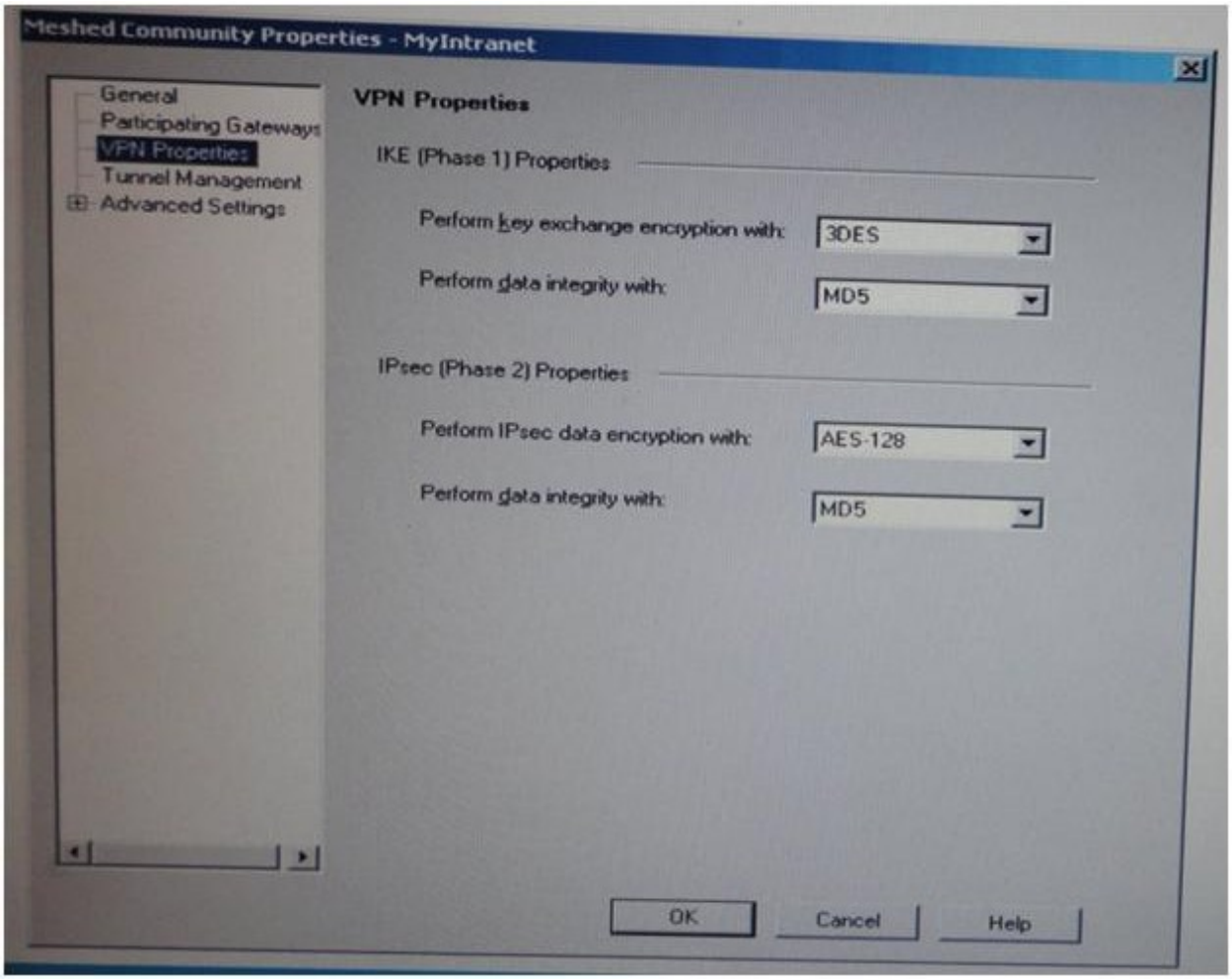
23.Which of the following are authentication methods that Security Gateway R70 uses to validate connection attempts? Select the response below includes that includes the MOST complete list of valid authentication methods:
A.Proxied, User, Dynamic, Session
B.Connection, User, Client
C.User, Client.Session
D.Connection, Proxied, Session
Answer: C

24.If you experience unwanted traffic from a specific IP address, how can you stop it most quickly?
A.Check anti-spoofing settings
B.Configure a rule to block the address
C.Create a SAM rule
D.Activate an IPS protection
Answer: C

25.When launching SmartDashboard, what information is required to log into R70?
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
Answer: B

26.Which of following uses the same key to decrypt as it does encrypt?
A.Asymmetric encryption
B.Symmetric encryption
C.Certificate-based encryption
D.Dynamic encryption
Answer: B

27.You are evaluating the configuration of a mesh VPN Community used to create a site-to-site VPN.This graphic displays the VPN properties in this mesh Community



Which of the following would be a valid conclusion?

A.The VPN Community will perform IKE Phase 1 key-exchange encryption using the longest key Security Gateway R70 supports.

B.Changing the setting Perform IPsec data encryption with from AES-128 to 3DES will increase the encryption overhead.

C.Changing the setting Perform key exchange encryption with 3DES to DES will enhance the VPN Community's security, and reduce encryption overhead.

D.Change the data-integrity settings for this VPN CommunitybecauseMD5 is incompatible with AES.

Answer: B

28.You just installed a new Web server in the DMZ that must be reachable from the Internet You create a manual Static NAT rule as follows:

Source: Any

Destination: web_public_IP

Service: Any

Translated Source: original

Translated Destination: web_private_IP

Service: original

“web_publicIP" is the node Object that represents the public IP address of the new Web server."web_privateIP" is the node object that represents the new Web site's private P address You

enable all settings from Global Properties > NAT.
When you try to browse the Web server from the Internet, you see the error 'page cannot be displayed" Which of the following is NOT a possible reason?
A.There is no route defined on the Security Gateway for the public IP address to the private IP address of the Web server.
B.There is no Security Policy defined that allows HTTP traffic to the protected Web server.
C.There is an ARP entry on the Gateway but the settings Merge Manual proxy ARP and Automatic ARP configuration are enabled in Global Properties.The Security Gateway ignores manual ARP entries.
D.There is no ARP table entry for the public IP address of the protected Web server
Answer: A

29.Which of the following are available SmartConsole clients which can be installed from the R70 Windows CD? Read all answers and select the most complete and valid list.
A.SmartView Tracker, CPINFO, SmartUpdate
B.SmartView Tracker, SmartDashboard, SmartLSM, SmartView Monitor
C.SmartView Tracker, SmartDashboard, CPINFO, SmartUpdate.SmartView Status
D.Security Policy Editor, Log Viewer, Real Time Monitor GUI
Answer: B

30.Which of the following SSL Network Extender server-side prerequisites is NOT correct?
A.The Gateway must be configured to work with Visitor Mode.
B.There are distinctly separate access rules required for SecureClient users vs.SSL Network Extender users.
C.To use Integrity Clientless Security (ICS), you must install the IC3 server or configuration tool.
D.The specific Security Gateway must be configured as a member of the Remote Access Community
Answer: B