KillTest

Higher Quality, Better Service!

Q&A

http://www.killtest.com

We offer free update service for one year.

Exam : **156-915**

Title : Accelerated CCSE NGX (156-915.1).....

Version : Demo

1.You have two Nokia Appliances one IP530 and one IP380. Both Appliances have IPSO 39 and VPN-1 Pro NGX installed in a distributed deployment Can they be members of a gateway cluster?

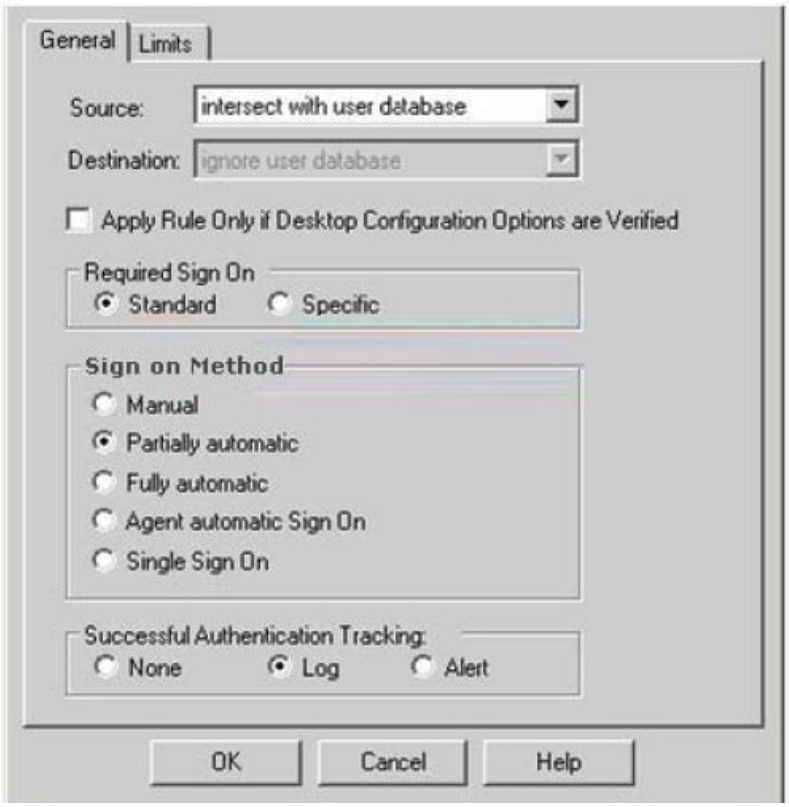
A. No, because the Gateway versions must not be the same on both security gateways
B. Yes, as long as they have the same IPSO version and the same VPN-1 Pro version
C. No, because members of a security gateway cluster must be installed as stand-alone deployments
D. Yes, because both gateways are from Nokia, whether they have the same VPN-1 PRO version or not
E. No, because the appliances must be of the same model (Both should be IP530orIP380.)
Answer: B

2.You want VPN traffic to match packets from internal interfaces. You also want the traffic to exit the Security Gateway, bound for all site-to-site VPN Communities, including Remote Access Communities. How should you configure the VPN match rule?

A. Internal_clear>- All_GwToGw
B. Communities >- Communities
C. Internal_clear>- External_Clear
D. Internal_clear>- Communitis
E. Internal_clear>-All_communitis
Answer: E

3.Review the following rules and note the Client Authentication Action properties screen, as shown in the exhibit.

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1		Customer@Any	* Any	* Any Traffic	TCP http TCP ftp TCP telnet	Client Auth	Log
2		* Any	* Any	* Any Traffic	* Any	drop	Log



After being authenticated by the Security Gateway when a user starts an HTTP connection to a Web site the user tries to FTP to another site using the command line. What happens to the user?
The....

A. FTP session is dropprd by the implicit Cleanup Rule.
B. User is prompted from the FTP site only, and does not need to enter username nad password for the Client Authentication.
C. FTP connection is dropped by rule 2.
D. FTP data connection is dropped, after the user is authenticated successfully.
E. User is prompted for authentication by the Security Gateway again.
Answer: B

4.After being authenticated by the Security Gateway, When a user starts an HTTP connection to a Web site, the user tries to FTP to another site using the command line. What happens to the user? The:

A. FTP session is dropped by the implicit Cleanup Rule

B. user is prompted from that FTP site on~, and does not need to enter username and password for Client Authentication
C. FTP connection is dropped by rule2
D. FTP data connection is dropped, after the user is authenticated successfully
E. User is prompted for authentication by the Security Gateway aqain
Answer: B

5.You want to upgrade a SecurePlatform NG with Application Intelligence (AI) R55 Gateway to SecurePlalform NGX R60 via SmartUpdate. Which package is needed in the repository before upgrading?

A. SVN Foundation and VPN-1 Express/Pro
B. VPN-1 and FireWall-1
C. SecurePlalform NGX R60
D. SVN Foundation
E. VPN-1 ProfExpress NGX R60
Answer: C

6.What is the command to see the licenses of the Security Gateway Certkiller from your SmartCenter Server?

A. print Certkiller
B. fw licprint Certkiller
C. fw tab -t fwlic Certkiller
D. cplic print Certkiller
E. fw lic print Certkiller
Answer: D

7.You set up a mesh VPN Community, so your internal network can access your partners network, and vice versa . Your Security Policy encrypts only FTP and HTTP traffic through a VPN tunnel. All traffic among your internal and partner networks is sent in clear text. How do you configure VPN Community?

A. Disable 'accept all encrypted traffic', and put FTP and http in the Excluded services in the Community object Add a rule in the Security Policy for services FTP and http, with the Community object in the VPN field
B. Disable "accept all encrypted traffic" in the Community, and add FTP and http services to the Security Policy, with that Community object in the VPN field
C. Enable "accept all encrypted traffic", but put FTP and http in the Excluded services in the Community. Add a rule in the Security Policy with services FTP and http, and the Community object in theVPN field
D. Put FTP and http in the Excluded services in the Community object Then add a rule in the Security Policy to allow any as the service, with the Community object in the VPN field

Answer: B

8.Ophelia is the security Administrator for a shipping company. Her company uses a custom application to update the distribution database. The custom application includes a service used only to notify remote sites that the distribution database is malfunctioning. The perimeter Security Gateways Rule Base includes a rule to accept this traffic. Ophelia needs to be notified, via atext message to her cellular phone, whenever traffic is accepted on this rule. Which of the following options is MOST appropriate for Ophelia's requirement?

A. User-defined alert script
B. Logging implied rules
C. SmartViewMonitor
D. Pop-up API
E. SNMP trap
Answer: A

9.You are reviewing SmartView Tracker entries, and see a Connection Rejection on a Check Point QoS rule. What causes the Connection Rejection?

A. No QoS rule exists to match the rejected traffic
B. The number of guaranteed connections is exceeded. The rule's action properties are not set to accept additional connections
C. The Constant Bit Rate for a Low Latency Class has been exceeded by greater than 10%, and the Maximal Delay is set below requirements
D. Burst traffic matching the Default Rule is exhausting the Check Point QoS global packet buffers
E. The guarantee of one of the rule's sub-rules exceeds the guarantee in the rule itself
Answer: B

10.Choose the BEST sequence for configuring user management on Smart Dash board, for use with an LDAP server

A. Enable LDAP in Global Properties, configure a host-node object for the LDAP Server, and configure a server object for the LDAP Account Unit
B. Configure a workstation object for the LDAP server, configure a server object for the LDAP Account Unit, and enable LDAP in Global Properties
C. Configure a server object for the LDAP Account Unit, enable LDAP in Global Properties, and create an LDAP server using an OPSEC application
D. Configure a server object for the LDAP Account Unit, enable LDAP in Global Properties, and create an LDAP resource object
E. Configure a server object for the LDAP Account Unit, and create an LDAP resource object
Answer: A

11.Which of the following is the final step in an NGXbackup?

A. Test restoration in a non-production environment, using the upgrade_import command
B. Move the *.tgz file to another location
C. Run the upgrade_export command
D. Copy the conf directory to another location
E. Run the cpstop command
Answer: B

12.Gail is the security administrator for a marketing firm. Gail is working with the networking team, to troubleshoot user complaints regarding access to audio-streaming material from the internet. The networking team asks Gail to check the object and rule configuration settings for the perimeter Security Gateway. Which SmartConsole application should Gail use to check these objects and rules?

A. SmartView Monitor
B. SmartUpdate
C. SmartViewTracker
D. SmartDashboard
E. SmartViewStatus
Answer: A

13.Which mechanism is used to export Check Point logs to third party applications?

A. OPSE
B. CPLogManager
C. LEA
D. SmartViewTracker
E. ELA
Answer: C

14.In NGX, what happens if a Distinguished Name (ON) is NOT found in LADP?

A. NGX takes the common-name value from the Certificate subject, and searches the LADP account unit for a matching user id
B. NGX searches the internal database for the username
C. The Security Gateway uses the subject of the Certificate as the ON for the initial lookup
D. If the first request fails or if branches do not match, NGX tries to map the identity to the user id attribute
E. When users authenticate with valid Certificates, the Security Gateway tries to map the identities with users registered in the extemal LADP user database
Answer: D

15.You are preparing to configure your VolP Domain Gatekeeper object. Which two other objects should you have created first?

A. An object to represent the IP phone network, AND an object to represent the host on which the proxy is installed
B. An object to represent the PSTN phone network, AND an object to represent the IP phone network
C. An object to represent the IP phone network, AND an object to represent the host on which the gatekeeper is installed
D. An object to represent the Q931 service origination host, AND an object to represent the H.245 termination host
E. An object to represent the call manager, AND an object to represent the host on which the transmission router is installed
Answer: C

16.Certkiller .com has two headquarters, one in London, one in new York. Each headquarters includes several branch offices. The branch offices only need to communicate with the headquarters in their country, not with each other, and only the headquarters need to communicate directly. What is the BEST configuration for VPN Communities among the branch offices and their headquarters, and between the two headquarters? VPN Communities comprised of:

A. Two star and one mesh Community; each star Community is set up for each site, with headquarters as the center of the Community, and branches as satellites. The mesh Communities are between the New York and London headquarters
B. Three mesh Communities: one for London headquarters and its branches, one for New York headquarters and its branches, and one for London and New York headquarters
C. Two mesh Communities, one for each headquarters and their branch offices; and one star Community, in which London is the center of the Community and New York is the satellite
D. Two mesh Communities, one for each headquarters and their branch offices; and one star Community, where New York is the center of the Community and London is the satellite
Answer: A

17.When you change an implicit rule's order from "last" to "first" in Global Properties, how do you make the change effective?

A. Close SmartDashboard, and reopen it
B. Select install database from the Policy menu
C. Select save from the file menu
D. Reinstall the Security Policy
E. Run fw fetch from the Security Gateway

Answer: D

18.Which command allows you to view the contents of an NGX table?

A. fw tab -s <tablename>-
B. fw tab -t <tablename>-
C. fw tab -u <tablename>-
D. fw tab -a <tablename>-
E. fw tab -x <tablename>-
Answer: B

19.Jack's project is to define the backup and restore section of his organization's disaster recovery plan for his organization's distributed NGX instaliation. Jack must meet the following required and desired objectives .
* Required Objective The security policy repository must be backed up no less frequent~ than every 24 hours
* Desired Objective The NGX components that enforce the Security Policies should be backed up no less frequently than once a week
* Desired Objective Back up NGX logs no less frequently than once a week
Jack's disaster recovery plan is as follows. See exhibit.

1. Use the cron utility to run the *upgrade_export* command each night on the SmartCenter Servers. Configure the organization's routine backup to back up the files created by the *upgrade_export* command
2. Configure the SecurePlalform backup utility to backup the SecuriтyGateways every Saturday night
3. Use the cron utility to run the *upgrade_export* command each Saturday night on the Log Servers. Configure an automatic, nightly logswitch. Configure the organization's routine backup software to backup the switched logs every night

Jack's plan:

A. Meets the required objective but does not meet either desired objective
B. Does not meet the required objective
C. Meets the required objective and only one desired objective
D. Meets the required objective and both desired objectives
Answer: D
Explanation: Logs can be viewed after exported.

20.You want to upgrade a cluster with two members to VPN-1 NGK The SmartCenter Server and both members are version VPN-1/FireWall-1 NG FP3, with the latest Hotfix. What is the correct upgrade procedure?

1. Change the version, in the General Properties of the gateway-cluster object
2. Upgrade the SmartCenter Server, and reboot after upgrade
3. Run cpstop on one member, while leaving the other member running. Upgrade one member at a time, and reboot after upgrade

4. Reinstall the Security Policy
A. 3,2,1,4
B. 2,4,3,1
C. 1,3,2,4
D. 2,3,1,4
E. 1,2,3,4
Answer: D

21.Certkiller needs to back up the routing, interface, and DNS configuration information from her NGX SecurePlatform Pro Security Gateway. Which backup-and-restore solution do you recommend for Certkiller?

A. Database Revision Control
B. Manual copies of the $FWDIR/conf directory
C. upgrade_export and upgrade_import commands
D. SecurePlatformbackup utilities
E. Policy Package management
Answer: D

22.The following is cphaprobstate command output from a New Mode High Availability cluster member:

Cluster Mode: New High Availability <Active Up>

Number	*Unique IP Addresses*	*Assigned Load*	*State*
1 <local>	*192.168.1.1*	*0%*	*down*
2	*192.168.1.2*	*100%*	*active*

Which machine has the highest priority?

A. 192.168.1.2,since its number is 2
B. 192.168.1.1,because its number is 1
C. This output does not indicate which machine has the highest priority
D. 192.168.1.2, because its state is active
Answer: B

23.What do you use to view an NGX Security Gateway's status, including CPU use, amount of virtual memory, percent of free hard-disk space, and version?

A. SmartLSM
B. SmartViewTracker
C. SmartUpdate
D. SmartViewMonitor
E. SmartViewStatus
Answer: D

24.Which of the following commands is used to restore NGX configuration

information?

A. cpcontig
B. cpinfo-i
C. restore
D. fwm dbimport
E. upgrade_import
Answer: E

25.Eric wants to see all URLs' ful destination path in the SmartView Tracker logs, not just the fully qualified domain name of the web servers. For Example, the information field of a log entry displays the URL http://hp.msn.com/css/home/hpcl1012.css. How can Eric best customize SmartView Tracker to see the logs he wants? Configure the URl resource, and select

A. "transparent" asthe connection method
B. "tunneling"as the connection method
C. "optimize URL logging"; use the URI resource in the rule, with action "accept"
D. "Enforce URI capability"; use the URI resource in the rule,with action "accept"
Answer: C

26.Which of the following commands shows full synchronizalion status?

A. cphaprob -i list
B. cphastop
C. fw ctl pstat
D. cphaprob -a if
E. fw hastat
Answer: C

27.By default, when you click File >- Switch Active File from SmartView Tracker, the SmartCenter Server

A. Opens a new window with a previously saved log file
B. Purges the current log file, and starts a new log file
C. Purges the current log, and prompts you for the new log's mode
D. Saves the current log file, names the log file by date and time, and starts a new log file
E. Prompts you to enter a filename, then saves the log file
Answer: D

28.The following is cphaprob state command output from a ClusterXL New mode High Availability member

Cluster Mode: New High Availability <Active Up>

Number	*Unique IP Addresses*	*Assigned Load*	*State*
1 <local>	*192.168.1.1*	*0%*	*standby*
2	*192.168.1.2*	*100%*	*active*

When member 192.168.1.2 fails over and restarts, which member will become actrve?

A. 192.168.1.2
B. 192.168.1.1
C. Both members' state will be standby
D. Both members' state will be active
Answer: B

29.Select the correct statement about Secure Internal Communications (SIC) Certificates? SIC Certificates:

A. for the SmartCenter Server are created during the SmartCenter Server configuration
B. decrease network security by securing administrative communication among the SmartCenter Servers and the Security Gateway
C. for NGX Security Gateways are created during the SmartCenter Server installation
D. uniquely identify Check Point enabled machines; they have the same function as VPN Certificates
E. are used for securing internal network communications between the SmartView Tracker and an OPSEC device
Answer: D

30.Which VPN Community object is used to configure VPN routing within the SmartDashboard?

A. Star
B. Mesh
C. Remote Access
D. Map
Answer: A