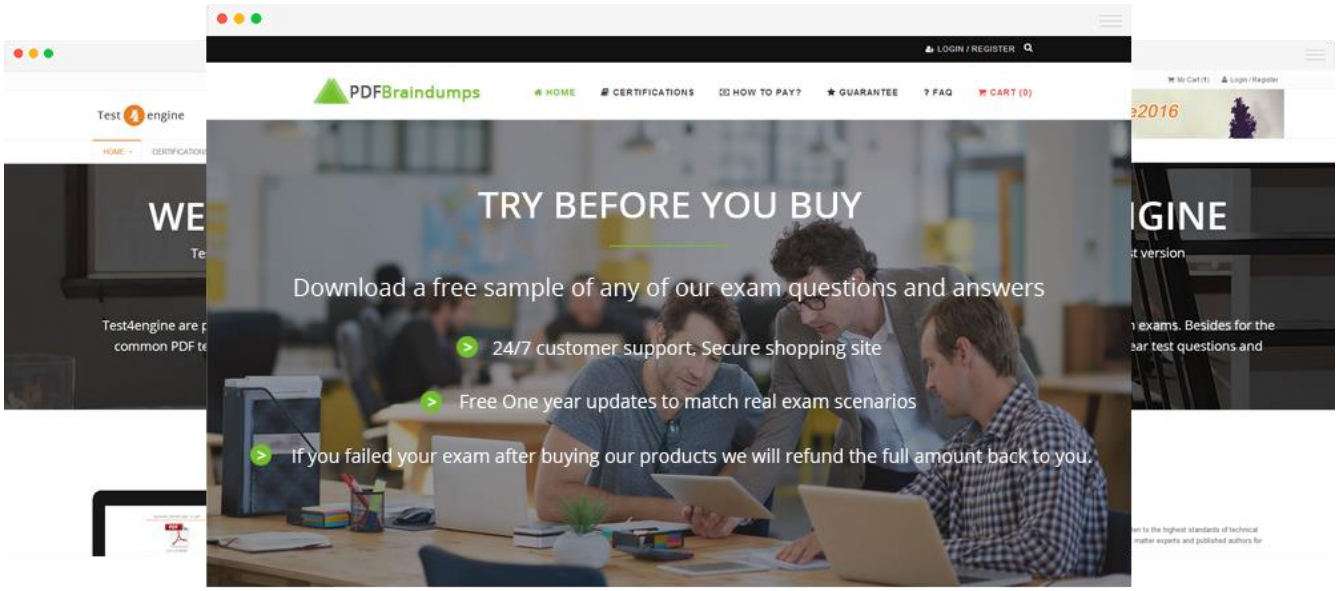
PDFBraindumps



Latest Pdf Braindumps

- LRP-614
- C-SRM-72
- BCABA
- ACMP-6.3
- JN0-740
- 1z0-100
- 250-405
- FM0-308
- DS-200
- C_SRM_72
- SDM_2002001040
- ACMP_6.3
- ST0-250
- 1z0-062
- H12-221
- A4120-784
- M2180-716

Top Certifications

- ISEB Certification
- HCNP
- OCE
- IFPUG Certifications
- NVIDIA Certifications
- dotMobi Certification
- Network+
- SCMA
- IBM Certified Integrat
- MCSD
- CCDH
- NCLP
- IBM Certified Advanc
- XMLMaster Certificat
- eserver Certified Spe
- CS5
- SAP-Certifications
- CHA
- Network Appliance N

Top Vendors

- ISEB
- Fortinet
- ASTQB
- Ericsson
- Aruba
- Liferay
- Data Center Universit
- Novell
- HRCI
- Huawei
- CIW
- RSA
- Patchlink
- MYSQL
- International Consorti
- ISM
- Acme-Packet
- CheckPoint

http://www.pdfbraindumps.com

Latest pdf braindumps provider, high pass rate

Exam : **156-315.80**

Title : Check Point Certified Security Expert - R80

Vendor : CheckPoint

Version : DEMO

NO.1 What are the blades of Threat Prevention?
A. IPS, DLP, AntiVirus, AntiBot, Sandblast Threat Emulation/Extraction
B. IPS, AntiVirus, AntiBot, Sandblast Threat Emulation/Extraction
C. IPS, AntiVirus, AntiBot
D. DLP, AntiVirus, QoS, AntiBot, Sandblast Threat Emulation/Extraction
Answer: B

NO.2 Joey wants to upgrade from R75.40 to R80 version of Security management. He will use Advanced Upgrade with Database Migration method to achieve this.
What is one of the requirements for his success?
A. Size of the /var/log folder of the target machine must be at least 25% of the size of the /var/log directory on the source machine
B. Size of the $FWDIR/log folder of the target machine must be at least 30% of the size of the $FWDIR/log directory on the source machine
C. Size of the /var/log folder of the source machine must be at least 25% of the size of the /var/log directory on the target machine
D. Size of the /var/log folder of the target machine must be at least 25GB or more
Answer: A

NO.3 Fill in the blank: The R80 feature _____ permits blocking specific IP addresses for a specified time period.
A. Adaptive Threat Prevention
B. Suspicious Activity Monitoring
C. Local Interface Spoofing
D. Block Port Overflow
Answer: B
Explanation:
Suspicious Activity Rules Solution
Suspicious Activity Rules is a utility integrated into SmartView Monitor that is used to modify access privileges upon detection of any suspicious network activity (for example, several attempts to gain unauthorized access).
The detection of suspicious activity is based on the creation of Suspicious Activity rules. Suspicious Activity rules are Firewall rules that enable the system administrator to instantly block suspicious connections that are not restricted by the currently enforced security policy. These rules, once set (usually with an expiration date), can be applied immediately without the need to perform an Install Policy operation.

NO.4 In a Client to Server scenario, which inspection point is the first point immediately following the tables and rule base check of a packet coming from outside of the network?
A. Big I
B. Little o
C. Big O
D. Little i
Answer: A

NO.5 Which statement is true regarding redundancy?
A. Machines in a ClusterXL High Availability configuration must be synchronized.
B. System Administrators know when their cluster has failed over and can also see why it failed over by using the cphaprob -f if command.
C. Both ClusterXL and VRRP are fully supported by Gaia and available to all Check Point appliances, open servers, and virtualized environments.
D. ClusterXL offers three different Load Sharing solutions: Unicast, Broadcast, and Multicast.
Answer: C

NO.6 Which command shows detailed information about VPN tunnels?
A. cat $FWDIR/conf/vpn.conf
B. cpview
C. vpn tu
D. vpn tu tlist
Answer: D

NO.7 Which web services protocol is used to communicate to the Check Point R80 Identity Awareness Web API?
A. XLANG
B. XML-RPC
C. REST
D. SOAP
Answer: C
Explanation:
The Identity Web API uses the REST protocol over SSL. The requests and responses are HTTP and in JSON format.

NO.8 How would you enable VMAC Mode in ClusterXL?
A. Cluster Object -> Edit -> ClusterXL and VRRP -> Use Virtual MAC
B. Cluster Object -> Edit -> Cluster Members -> Edit -> Use Virtual MAC
C. cphaconf vmac_mode set 1
D. fw ctl set int vmac_mode 1
Answer: A
Explanation:
Explanation
Reference:
eventSubmit_doGoviewsolutiondetails=&solutionid=sk50840

NO.9 In what way is Secure Network Distributor (SND) a relevant feature of the Security Gateway?
A. SND is used to distribute packets among Firewall instances
B. SND is a feature of fw monitor to capture accelerated packets
C. SND is an alternative to IPSec Main Mode, using only 3 packets
D. SND is a feature to accelerate multiple SSL VPN connections

Answer: A

NO.10 Can multiple administrators connect to a Security Management Server at the same time?
A. Yes, every administrator has their own username, and works in a session that is independent of other administrators.
B. No, only one can be connected
C. Yes, but only one has the right to write.
D. Yes, all administrators can modify a network object at the same time
Answer: A

NO.11 In what way are SSL VPN and IPSec VPN different?
A. IPSec VPN does not support two factor authentication, SSL VPN does support this
B. IPSec VPN uses an additional virtual adapter; SSL VPN uses the client network adapter only.
C. SSL VPN adds an extra VPN header to the packet, IPSec VPN does not
D. SSL VPN is using HTTPS in addition to IKE, whereas IPSec VPN is clientless
Answer: B

NO.12 Which software blade does NOT accompany the Threat Prevention policy?
A. Anti-virus
B. Application Control and URL Filtering
C. IPS
D. Threat Emulation
Answer: B

NO.13 What is the protocol and port used for Health Check and State Synchronization in ClusterXL?
A. CCP and 8116
B. CPC and 8116
C. CCP and 257
D. CCP and 18190
Answer: A

NO.14 Which Check Point software blade provides protection from zero-day and undiscovered threats?
A. Firewall
B. Threat Emulation
C. Application Control
D. Threat Extraction
Answer: B

NO.15 What is the responsibility of SOLR process on R80.10 management server?
A. Communication between SmartConsole applications and the Security Management Server
B. It generates indexes of data written to the database
C. Writing all information into the database

D. Validating all data before it's written into the database
Answer: B

NO.16 What is a best practice before starting to troubleshoot using the "fw monitor" tool?
A. Disable SecureXL
B. Clear the connections table
C. Run the command: fw monitor debug on
D. Disable CoreXL
Answer: A

NO.17 When requiring certificates for mobile devices, make sure the authentication method is set to one of the following, Username and Password, RADIUS or _____.
A. SecurID
B. TacAcs
C. Complexity
D. SecureID
Answer: A

NO.18 Which of the following is NOT a valid type of SecureXL template?
A. NAT Template
B. Deny template
C. Accept Template
D. Drop Template
Answer: B

NO.19 NAT rules are prioritized in which order?
1. Automatic Static NAT
2. Automatic Hide NAT
3. Manual/Pre-Automatic NAT
4. Post-Automatic/Manual NAT rules
A. 1, 4, 2, 3
B. 3, 1, 2, 4
C. 1, 2, 3, 4
D. 4, 3, 1, 2
Answer: C

NO.20 What is mandatory for ClusterXL to work properly?
A. The number of cores must be the same on every participating cluster node
B. The Magic MAC number must be unique per cluster node
C. If you have "Non-monitored Private" interfaces, the number of those interfaces must be the same on all cluster members
D. The Sync interface must not have an IP address configured
Answer: B

NO.21 Can Check Point and Third-party Gateways establish a certificate-based Site-to-Site VPN tunnel?
A. No, they cannot share certificate authorities
B. No, Certificate based VPNs are only possible between Check Point devices
C. Yes, but they have to have a pre-shared secret key
D. Yes, but they need to have a mutually trusted certificate authority
Answer: D

NO.22 Which Mobile Access Application allows a secure container on Mobile devices to give users access to internal website, file share and emails?
A. Check Point Capsule Remote
B. Check Point Remote User
C. Check Point Mobile Web Portal
D. Check Point Capsule Workspace
Answer: C

NO.23 In the Firewall chain mode FFF refers to:
A. No Match
B. All Packets
C. Stateful Packets
D. Stateless Packets
Answer: B

NO.24 What traffic does the Anti-bot feature block?
A. Command and Control traffic from hosts that have been identified as infected
B. Network traffic that is directed to unknown or malicious servers
C. Network traffic to hosts that have been identified as infected
D. Command and Control traffic to servers with reputation for hosting malware
Answer: A

NO.25 Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this?
A. TCP port 265
B. UDP port 256
C. TCP port 256
D. UDP port 265
Answer: C
Explanation:
Synchronization works in two modes:
Full Sync transfers all Security Gateway kernel table information from one cluster member to another. It is handled by the fwd daemon using an encrypted TCP connection on port 256.
Delta Sync transfers changes in the kernel tables between cluster members. Delta sync is handled by

the Security Gateway kernel using UDP connections on port 8116.

NO.26 What is true about the IPS-Blade?
A. In R80, IPS Exceptions cannot be attached to "all rules"
B. In R80, the GeoPolicy Exceptions and the Threat Prevention Exceptions are the same
C. In R80, IPS is managed by the Threat Prevention Policy
D. In R80, in the IPS Layer, the only three possible actions are Basic, Optimized and Strict
Answer: C

NO.27 Which one of the following is NOT a configurable Compliance Regulation?
A. ncipa
B. soci
C. cjis
D. glba
Answer: D

NO.28 The essential means by which state synchronization works to provide failover in the event an active member goes down, _____ is used specifically for clustered environments to allow gateways to report their own state and learn about the states of other members in the cluster.
A. cphad
B. cphaconf
C. cphastart
D. ccp
Answer: D

NO.29 Which command is used to add users to or from existing roles?
A. Add rba user <User Name> roles <List>
B. Add user <User Name>
C. Add user <User Name> roles <List>
D. Add rba user <User Name>
Answer: A

NO.30 ClusterXL is fully supported by Gaia and available to all Check Point appliances. Which command is NOT related to redundancy and functions?
A. cphaprob stat
B. cphaprob -I list
C. cphaprob -a if
D. cphaprob all show stat
Answer: D