156-315.77 Q&As

Check Point Certified Security Expert

Pass CheckPoint 156-315.77 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/156-315-77.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CheckPoint Official Exam Center

QUESTION 1

A trackedSmart EventCandidate in a Candidate Pool becomes an Event. What does NOT happen in the Analyzer Server?

A. Smart Eventprovides the beginning and end time of the Event.

B. The Correlation Unit keeps adding matching logs to the Event.

C. The Event is kept open, but condenses many instances into one Event.

D. Smart Eventstops tracking logs related to the Candidate.

Correct Answer: D

QUESTION 2

Identity Agent is a lightweight endpoint agent that authenticates securely with Single Sign- On (SSO). Which of the following is NOT a recommended use for this method?

A. When accuracy in detecting identity is crucial

B. Identity based enforcement for non-AD users (non-Windows and guest users)

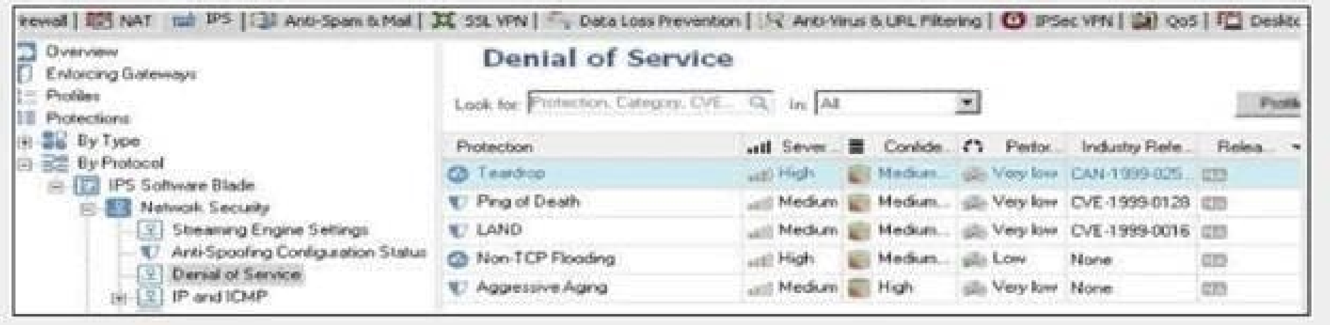
C. Protecting highly sensitive servers

D. Leveraging identity for Data Center protection

Correct Answer: B

QUESTION 3

You are responsible for the IPS configuration of your Check Point firewall. Inside the Denial of service section you need to set the protection parameters against the Teardrop attack tool with high severity. How would you characterize this attack tool? Give the BEST answer.


irewall | NAT | IPS | Anti-Spam & Mail | SSL VPN | Data Loss Prevention | Anti-Virus & URL Filtering | IPSec VPN | QoS | Deskt
Overview
Enforcing Gateways
Profiles
Protections
By Type
By Protocol
IPS Software Blade
Network Security
Streaming Engine Settings
Anti-Spoofing Configuration Status
Denial of Service
IP and ICMP
Look for: Protection, Category, CVE...
In: All
Profi

Denial of Service

Protection	Sever...	Confide...	Perfor...	Industry Refe...	Relea...
Teardrop	High	Medium...	Very low	CAN-1999-025...	
Ping of Death	Medium	Medium...	Very low	CVE-1999-0128	
LAND	Medium	Medium...	Very low	CVE-1999-0016	
Non-TCP Flooding	High	Medium...	Low	None	
Aggressive Aging	Medium	High	Very low	None	

A. Hackers can send high volumes of non-TCP traffic in an effort to fill up a firewall State Table. This results in a Denial of Service by preventing the firewall from accepting new connections. Teardrop is a widely available attack tool that exploits this vulnerability.

B. A remote attacker may attack a system by sending a specially crafted RPC request to execute arbitrary code on a vulnerable system. Teardrop is a widely available attack tool that exploits this vulnerability.

C. Some implementations of TCP/IP are vulnerable to packets that are crafted in a particular way (a SYN packet in which the source address and port are the same as the destination, i.e., spoofed). Teardrop is a widely available attack tool that exploits this vulnerability

D. Some implementations of the TCP/IP IP fragmentation re-assembly code do not properly handle overlapping IP fragments. Sending two IP fragments, the latter entirely contained inside the former, causes the server to allocate too much memory and crash. Teardrop is a widely available attack tool that exploits this vulnerability.

Correct Answer: D

QUESTION 4

Which of the following statements is TRUE concerning MEP VPN\\'s?

A. State synchronization betweenSecurityGateways is required.

B. MEP VPN\\'s are not restricted to the location of the gateways.

C. The VPN Client is assigned a Security Gateway to connect to based on a priority list, should the first connection fail.

D. MEP Security Gateways cannot be managed by separate Management Servers.

Correct Answer: B

QUESTION 5

Fill in the blank. To enter the router shell, use command __________ .

A. cligated

B.

C.

D.

Correct Answer: A

QUESTION 6

Which of the following is NOT a ClusterXL mode?

A. Multicast

B. Legacy

C. Broadcast

D. New

Correct Answer: C

QUESTION 7

Which is NOT a method through which Identity Awareness receives its identities?

A. GPO

B. Captive Portal

C. AD Query

D. Identity Agent

Correct Answer: A

QUESTION 8

When upgrading a cluster in Full Connectivity Mode, the first thing you must do is see if all cluster members have the same products installed. Which command should you run?

A. fw fcu

B. cphaprob fcustat

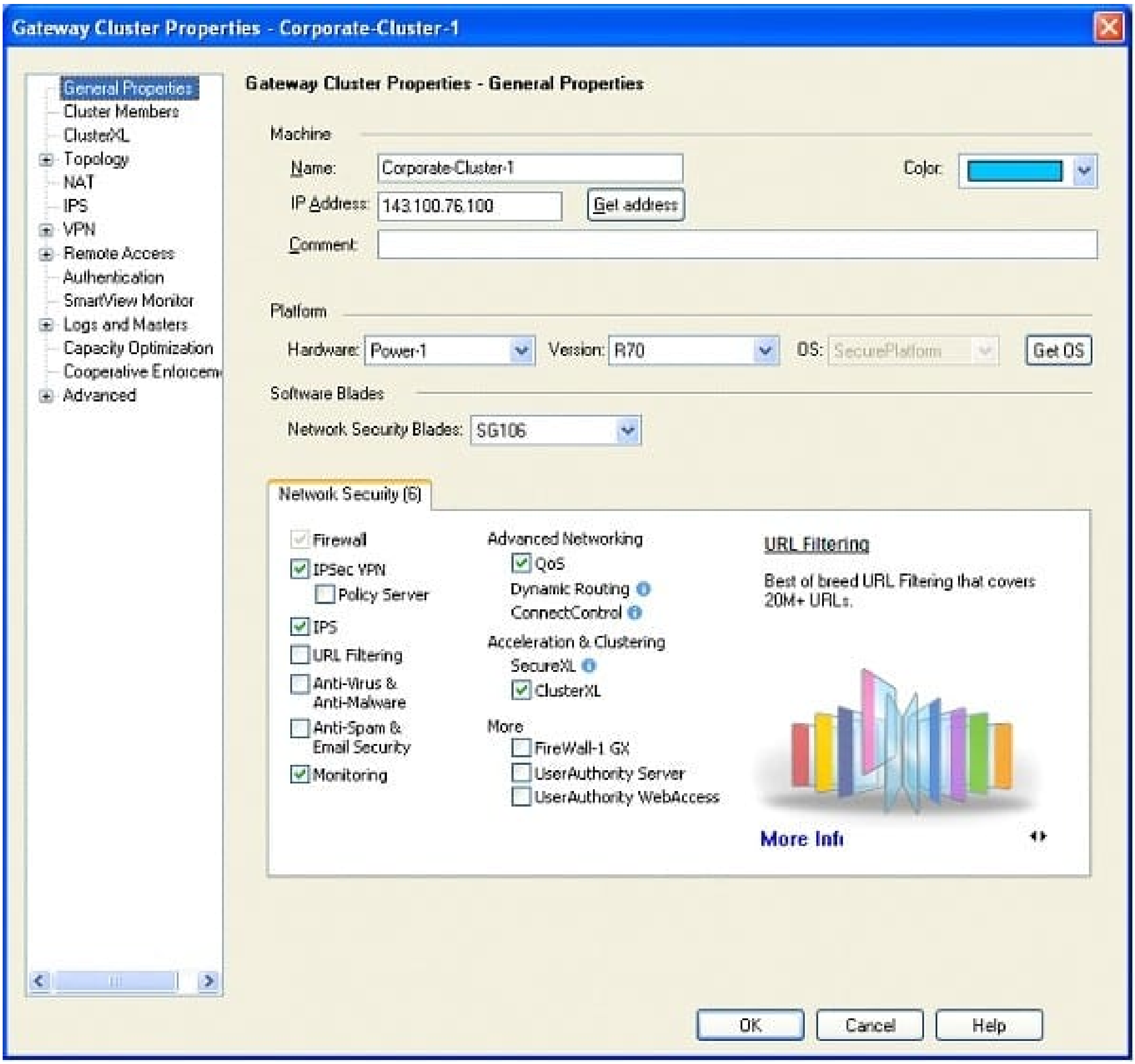
C. cpconfig

D. fw ctl conn -a

Correct Answer: D

QUESTION 9

John is configuring a new R76Gateway cluster but he can not configure the cluster as Third Party IP Clustering because this option is not available in Gateway Cluster Properties.



Gateway Cluster Properties - General Properties

Machine

Name: Corporate-Cluster-1

IP Address: 143.100.76.100

Comment:

Color:

Platform

Hardware: Power-1 Version: R70 OS: SecurePlatform

Software Blades

Network Security Blades: SG106

Network Security (6)

☑ Firewall
☑ IPSec VPN
□ Policy Server
☑ IPS
□ URL Filtering
□ Anti-Virus & Anti-Malware
□ Anti-Spam & Email Security
☑ Monitoring

Advanced Networking
☑ QoS
Dynamic Routing
ConnectControl

Acceleration & Clustering
SecureXL
☑ ClusterXL

More
□ FireWall-1 GX
□ UserAuthority Server
□ UserAuthority WebAccess

URL Filtering

Best of breed URL Filtering that covers 20M+ URLs.

What\\'s happening?

A. Third Party Clustering is not available for R76Security Gateways.

B. John is not using third party hardware as IP Clustering is part of Check Point\\'s IP Appliance.

C. ClusterXL needs to be unselected to permit 3rd party clustering configuration.

D. John has an invalid ClusterXL license.

Correct Answer: C

QUESTION 10

Remote clients are using SSL VPN to authenticate via LDAP server to connect to the organization. Which gateway process is responsible for the authentication?

A. vpnd

B. cpvpnd

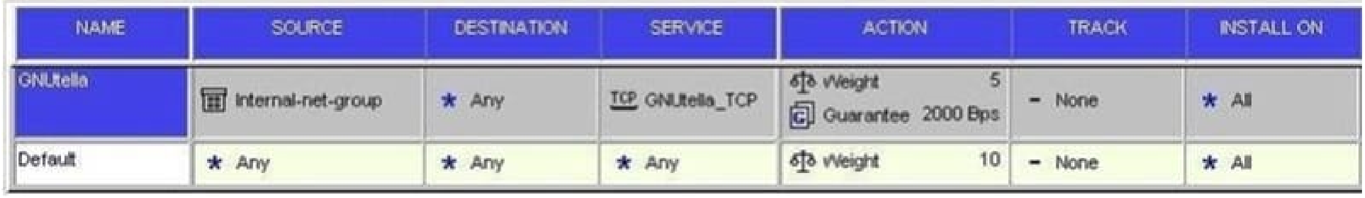
C. fwm

D. fwd

Correct Answer: B

QUESTION 11

Using the output below,why is the QoS rule not limiting the internal users to 2000 Bps of GNUtella traffic?



NAME	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON
GNUtella	Internal-net-group	★ Any	TCP GNUtella_TCP	Weight 5 Guarantee 2000 Bps	- None	★ All
Default	★ Any	★ Any	★ Any	Weight 10	- None	★ All

A. Rule Guarantee needs to be changed to Rule Limit

B. Rule Weight needs to be changed to 10

C. The Source and Destination columns need to be reversed

D. Encrypted traffic needs to be added to the Action field

Correct Answer: A

QUESTION 12

How would you configure a rule in a Security Policy to allow SIP traffic from end point Net_Ato end point Net_B, through an NGX Security Gateway?

A. Net_A/Net_B/sip/accept

B. Net_A/Net_B/sip and sip_any/accept

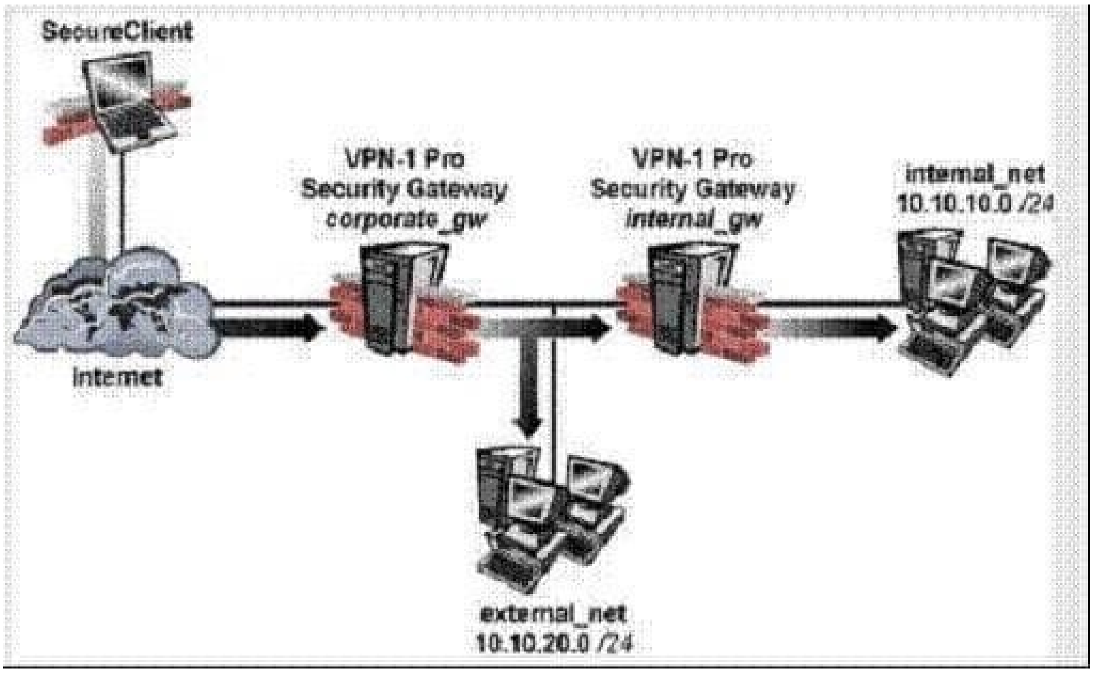
C. Net_A/Net_B/VoIP_any/accept

D. Net_A/Net_BM3lP/accept

Correct Answer: A

QUESTION 13

The following diagram illustrates how a VPN-1 SecureClient user tries to establish a VPN with hosts in the external_net and internal_net from the Internet. How is the Security Gateway VPN Domain created?



A. Internal Gateway VPN Domain = internal_net; External VPN Domain = external net + external gateway object + internal_net.

B. Internal Gateway VPN Domain = internal_net. External Gateway VPN Domain = external_net + internal gateway object

C. Internal Gateway VPN Domain = internal_net; External Gateway VPN Domain = internal_net + external_net

D. Internal Gateway VPN Domain = internal_net. External Gateway VPN Domain = internal VPN Domain + internal gateway object + external_net

Correct Answer: D

QUESTION 14

What is the bit size of DES?

A. 56

B. 112

C. 168

D. 128

E. 32

F. 64

Correct Answer: A

QUESTION 15

You have an internal FTP server, and you allow downloading, but not uploading. Assume Network Address Translation is set up correctly, and you want to add an inbound rule with:

Source: Any

Destination: FTP server

Service: FTP resources object.

How do you configure the FTP resource object and the action column in the rule to achieve this goal?

A. Enable only the "Get" method in the FTP Resource Properties, and use this method in the rule, with action accept.

B. Enable only the "Get" method in the FTP Resource Properties and use it in the rule, with action drop.

C. Enable both "Put" and "Get" methods in the FTP Resource Properties and use them in the rule, with action drop.

D. Disable "Get" and "Put" methods in the FTP Resource Properties and use it in the rule, with action accept.

E. Enable only the "Put" method in the FTP Resource Properties and use it in the rule, with action accept.

Correct Answer: A