JUNIPER JN0-541 EXAM QUESTIONS & ANSWERS

Number: JN0-541
Passing Score: 800
Time Limit: 120 min
File Version: 45.5

http://www.gratisexam.com/

JUNIPER JN0-541 EXAM QUESTIONS & ANSWERS

Exam Name: IDP, Associate(JNCIA-IDP)

Examsheets

QUESTION 1
Which statement is true about the attack object database update process?

A. Each sensor updates its own attack object database automatically; however they must be able to access the Juniper site on TCP port 443.
B. The attack object database update must be manually performed by the administrator, and the administrator must manually install it on each sensor.
C. The attack object database update can be initiated manually or automatically.
D. The attack object database update can be automatically scheduled to occur using the Security Manager GUI.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
On a sensor, which command will indicate if log messages are being sent to Security Manager?

A. scio vr list
B. serviceidp status
C. scio agentstats display
D. scio getsystem

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
After you enable alerts for new hosts that are detected by the Enterprise Security Profiler, where do you look in Security Manager to see those alerts? ActualTests.com

A. Security Monitor > Profiler > Application Profiler tab
B. Security Monitor > Profiler > Violation Viewer tab
C. Security Monitor > Profiler > Network Profiler tab
D. Log Viewer > Profiler Log

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
When connecting to a sensor using SSH, which account do you use to login?

A. admin

B. super
C. netscreen
D. root

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which OSI layer(s) of a packet does the IDP sensor examine?

A. layers 2-7
B. layers 2-4
C. layer 7 only
D. layers 4-7

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Which rule base would detect netcat?

A. SYN protector
B. traffic anomalies
C. backdoor
D. exempt

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com 3
Juniper JN0-541: Practice Exam

QUESTION 7
Which three fields in a packet must match an IDP rule before that packet is examined for an attack? (Choose three.)

A. terminate match
B. service
C. destination address
D. source address
E. attack object

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
A newly re-imaged sensor is running IDP 4.0 code. You want to assign IP address 10.1.1.1 to the sensor. Which method do you use to do this?

ActualTests.com

A. Connect to the sensor's console port, login as root, and answer theEasyConfig
B. Use SSH to connect to the sensor at IP 192.168.1.1.Login as root, and run ipconfig.
C. Connect to the sensor's console port, login as admin, and answer theEasyConfig
D. Use SSH to connect to the sensor at IP 192.168.1.1.Login as admin, and run ipconfig.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which statement is true regarding IDP rule matching on a sensor?

A. Each rule in the IDP rule base that matches on the source IP, destination IP, and service will be processed further.
B. Each rule in the IDP rule base that matches on the source IP, destination IP, and service will be processed further, unless the particular rule is terminal.
C. Each rule in the IDP rule base that matches on the source IP, destination IP, service, and attack object will be processed further.
D. Each rule in the IDP rule base that matches on the source IP, destination IP, service, and attack object will be processed further, unless the particular rule is terminal.
ActualTests.com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which TCP port is used for communication between Security Manager and an IDP sensor?

A. 7801

B. 7800
C. 7803
D. 443

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com 5
Juniper JN0-541: Practice Exam

QUESTION 11
Which statement about the Enterprise Security Profiler (ESP) is true?

ActualTests.com

A. The ESP must be configured and started using the IDP sensor CLI before it is used.
B. The administrator must manually initiate Security Manager to sensor polling to retrieve ESP data.
C. The ESP must be configured and started on each IDP sensor manually, using the Security Manager GUI.
D. The ESP is started by default in IDP version 4.0 or newer.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
What is one use of an IP action?

"Pass Any Exam. Any Time." - www.actualtests.com 6
Juniper JN0-541: Practice Exam

A. It blocks subsequent connections from specific IP addresses.
B. It modifies the IP header to redirect the attack.
C. It modifies the IP header to prevent the attack.
D. It permits or denies the traffic, based on the IP header.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which three actions must be taken prior to deploying an IDP sensor (in transparent mode) in a network?

A. Assign an IP to the management interface IP.
B. Establish communication between Security manager and the sensor.
C. Assign an IP to all forwarding interfaces.
D. Configure the sensor mode.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com 8
Juniper JN0-541: Practice Exam

QUESTION 14
Exhibit:

Time Received	Src Addr	Dst Addr	Protocol	Dst Port	Subcategory
8/29/06 10:20:08 AM	10.1.3.50	0.0.0.0	HOPOPT	0	TSIG Session Rate Exceeded
8/29/06 10:20:48 AM	10.1.3.50	0.0.0.0	HOPOPT	0	TSIG Session Rate Exceeded

You work as an administrator at Certkiller .com. Study the exhibit carefully. In the exhibit, which rule base would have generated the log message?

A. traffic anomaly
B. backdoor
C. networkhoneypot
D. SYN protector

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
What is "a unique pattern that always exists within an attack"?

A. attack severity
B. attack signature
C. context
D. protocol anomaly

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
ActualTests.com

QUESTION 16
Which sensor command can be used to determine if profiler data is being sent to Security Manager?

A. scio getsystem
B. sctop "s" option
C. scio agentconfig list
D. scio agentstats display

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com 9
Juniper JN0-541: Practice Exam

QUESTION 17
Which three statements are true as they relate to a transparent mode IDP deployment? (Choose three.)

A. Can actively prevent attacks on all traffic.
B. Can be installed in the network without changing IP addresses or routes.
C. Uses paired ports, such that packets arriving on one port go out the other associated port.
D. An IP address must be defined on each forwarding interface.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Which sensor process handles all communication between the sensor and Security Manager?

A. agent
B. idp
C. sciod
D. profiler

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which three columns can be seen in the Application View of the Enterprise Security Profiler? (Choose three.)

ActualTests.com

A. Service
B. Src OS Name
C. Src and Dest IPs
D. Context
E. Access Type

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
In Enterprise Security Profiler (ESP), what is a permitted object?

A. Any object that violates the security policy configured in ESP.
B. Any object that defines valid network connections on the network.
C. Any object that violates application context.
D. Any object that defines the configuration of ESP.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Given the following steps:

A. Attach the sensor to the management network.
B. Place the sensor inline in network.
C. Create and install a policy on the sensor.
D. Establish communication between Security Manager and the IDP sensor.
E. Configure the sensor deployment mode and management interface IP.
F. Test connectivity through the sensor.
Which order is correct when initially deploying a sensor in a network?
G. b, f, e, a, d, c
H. e, a, d, c, b, f
I. e, a, d, b, f, c
J. a, e, d, c, f, b

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
ActualTests.com
You can remotely administer the IDP sensor using which two methods? (Choose two.)

A. theWebUI ACM over HTTPS
B. theWebUI ACM over HTTP
C. an SSH connection
D. a telnet connection

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23

You want Enterprise Security Profiler (ESP) to capture layer 7 data of packets traversing the network. Which two steps must you perform? (Choose two.) "Pass Any Exam. Any Time." - www.actualtests.com 11 Juniper JN0-541: Practice Exam

A. Configure ESP to enable application profiling, and select the contexts to profile.
B. Under the Violation Viewer tab, create a permitted object, select that object, and then click Apply.
C. Start or restart the profiler process.
D. Create a filter in the ESP to show only tracked hosts.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which two statements are true regarding static and dynamic attack object groups? (Choose two.)

A. Attack objects in a dynamic group can be added or updated during the attack object database update process.
B. You create a dynamic attack object group by specifying particular filters to apply to the attack object database, such as severity, product, and service.
C. The critical attack object group is a static group.
D. Dynamic groups require that an administrator manually add new attack objects after an attack database update.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which command will display the mode of the IDP sensor?

A. sctop "m" option
B. scio agentconfig list
ActualTests.com
C. scio getsystem
D. scio agentstats display

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which three actions must be taken prior to deploying an IDP sensor (in transparent mode) in a network?

A. Assign an IP to all forwarding interfaces.
B. Establish communication between Security manager and the sensor.
"Pass Any Exam. Any Time." - www.actualtests.com 12

C. Assign an IP to the management interface IP.
D. Configure the sensor mode.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which statement is true regarding policy installation on an IDP sensor?

A. A policy version is created when a new policy is successfully installed.
B. Thepkid process on the sensor handles the policy installation.
C. Thepolicy.set file is updated on the sensor.
D. The sensor stops processing traffic when the policy is being installed.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
In IDP Sensor clustering, which port is used to send state synchronization information to other devices in the cluster?

A. eth2
B. eth1
C. eth0
D. console port

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
ActualTests.com

QUESTION 29
Which three fields in a packet must match an IDP rule before that packet is examined for an attack? (Choose three.)

A. destination address
B. service
C. terminate match
D. source address
E. attack object

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com 13
Juniper JN0-541: Practice Exam

QUESTION 30
What is one use of an IP action?

A. It modifies the IP header to prevent the attack.
B. It blocks subsequent connections from specific IP addresses.
C. It permits or denies the traffic, based on the IP header.
D. It modifies the IP header to redirect the attack.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which two statements are true about the Enterprise Security Profiler (ESP)? (Choose two.)

A. The ESP indicates when existing hosts or protocols are being used.
B. The ESP indicates when a specific machine has been attacked.
C. The ESP indicates which hosts are talking with each other, and which protocols are being used.
D. The ESP provides a summary of protocols and contexts on each host.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which type of cable do you use for a console connection to an IDP sensor?

A. straight-through serial cable
B. null-modem cable
ActualTests.com
C. CAT 5 cable
D. Juniper proprietary cable

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which sctop option will display current TCP flows through the sensor?

A. f

B. t
C. u
D. k

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which TCP port is used for communication between ACM and an IDP sensor?

A. 443
B. 80
C. 7800
D. 7801

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

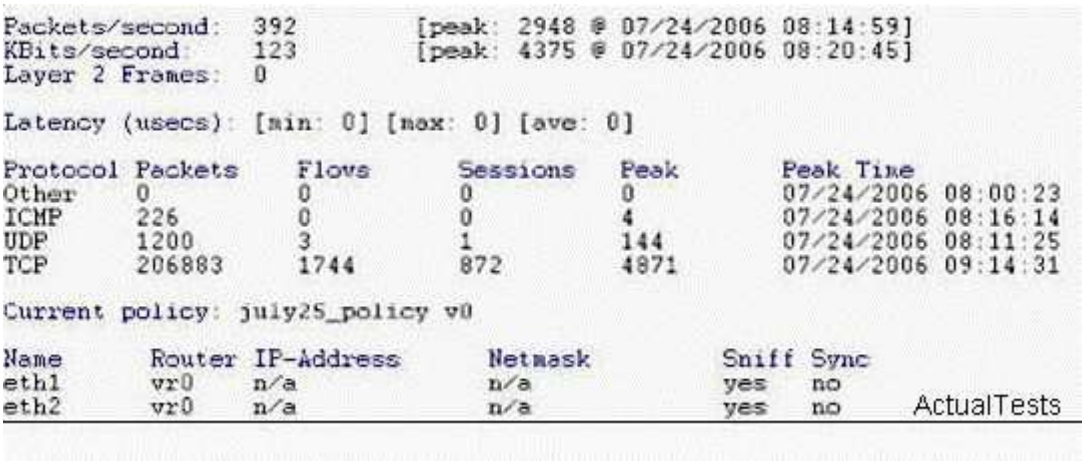
QUESTION 35
Which account do you use to login when connecting to a sensor using SSL?

A. super
B. netscreen
C. admin
D. root

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Exhibit:
You work as an administrator at Certkiller .com. Study the exhibit carefully.



```
Packets/second:   392          [peak: 2948 @ 07/24/2006 08:14:59]
KBits/second:     123          [peak: 4375 @ 07/24/2006 08:20:45]
Layer 2 Frames:   0

Latency (usecs): [min: 0] [max: 0] [ave: 0]

Protocol  Packets    Flows      Sessions   Peak       Peak Time
Other     0          0          0          0          07/24/2006 08:00:23
ICMP      226        0          0          4          07/24/2006 08:16:14
UDP       1200       3          1          144        07/24/2006 08:11:25
TCP       206883     1744       872        4871       07/24/2006 09:14:31

Current policy: july25_policy v0

Name      Router IP-Address      Netmask         Sniff Sync
eth1      vr0    n/a             n/a             yes   no
eth2      vr0    n/a             n/a             yes   no      ActualTests
```

A. scio policy list s0
B. sctop "s" option
"Pass Any Exam. Any Time." - www.actualtests.com 15
Juniper JN0-541: Practice Exam
C. scio getsystem
D. sctop "t" option

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
You want Enterprise Security Profiler (ESP) to capture layer 7 data of packets traversing the network. Which two steps must you perform? (Choose two.)

A. Configure ESP to enable application profiling, and select the contexts to profile.
B. Under the Violation Viewer tab, create a permitted object, select that object, and then click Apply.
C. Start or restart the profiler process.
D. Create a filter in the ESP to show only tracked hosts.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
On a newly re-imaged sensor, which three TCP ports are open on its eth0 interface? (Choose three.)

A. 7801
B. 7803
C. 22
D. 443
E. 80
ActualTests.com

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which tool will allow you to change a sensor's deployment mode?

A. ACM
B. ifconfig
C. sctop
D. Security Manager

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com 16
Juniper JN0-541: Practice Exam

QUESTION 40
Which sensor command will unload the current policy?

A. scio policy unload
B. scio agentconfig policy unload
C. scio policy unload s0
D. sctop "u" option

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which sctop option will display current throughput rate for the sensor?

A. u
B. s
C. t
D. r

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which three are assigned as a result of running EasyConfig? (Choose three.)

A. sensor eth1 IP address
ActualTests.com
B. sensor default gateway
C. sensor HA configuration
D. sensor eth0 IP address
E. sensor deployment mode

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Within the SYN protector rule base, what is the function of relay action?

A. It will create a session with the server only if the client completes the three-step TCP handshake with the sensor.
"Pass Any Exam. Any Time." - www.actualtests.com 17
Juniper JN0-541: Practice Exam
B. It will monitor new connections to a protected server, but not prevent them.
C. It will relay all SYN connections to a fake IP.
D. It will not monitor incoming SYN requests.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Which sensor process handles policy installation?

A. idp
B. sciod
C. agent
D. profiler
E. idpLogReader

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which two statements are true? (Choose two.)

A. If the source IP, target IP, and service in a packet match a particular IDP rule, the rule's action will be performed.
B. All of the rules in the IDPrulebase are examined until either the end of the list is reached, or a matching rule has the Terminate Match button checked.

C. One packet can match on multiple IDP rules.
D. Once the IDP sensor stops comparing a packet against the list of IDP rules, it performs only the first action in the matching rules.
ActualTests.com

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which two statements describe action versus IP action? (Choose two.)

A. IP action responds to matching traffic by dropping or closing current attack packets or connection.
B. Action responds to matching traffic by dropping or closing current attacking packets or connection.
C. IP Action responds to future traffic based on a previous match by blocking or dropping future connections.
"Pass Any Exam. Any Time." - www.actualtests.com 18
Juniper JN0-541: Practice Exam
D. Action responds to future traffic based on a previous match by blocking or dropping future connections.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Exhibit:

a. On target machine, start capturing packets with a protocol analyzer.
b. On sensor, examine scio ccap output.
c. Compile attack code on attacker machine.
d. On sensor, run scio ccap all.
e. On attacker machine, run attack code against target.

ActualTests

In order to obtain attack information so that you can create a new attack object definition, you must follow certain steps. Given the steps in the exhibit, assume you have acquired the attack source code. What is the correct order for these steps?

A. c, e, b, d, a
B. c, d, a, e, b
C. c, d, e, a, b
D. e, c, d, b, a

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48

If the power is lost to an IDP sensor, which feature allows the traffic to continue to flow through the ActualTests.com
device?

A. NIC bypass
B. peer port modulation
C. protocol anomaly detection
D. stateful inspection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
You implement Traffic Anomaly detection and you find numerous alerts of port scans from your security auditing team that you want to ignore. You create an address book entry for the security audit team specifying the IP addresses of those machines. What should you do next? "Pass Any Exam. Any Time." - www.actualtests.com 19
Juniper JN0-541: Practice Exam

A. Create a rule at the top of the Traffic Anomaly rule base to ignore traffic from security audit team, and make this a terminal rule.
B. Create a rule at the top of the Traffic Anomalyrulebase to ignore traffic from security audit team.
C. Create a rule at the top of the IDPrulebase to ignore traffic from security audit team, and make this a terminal rule.
D. Create an exempt rule for the security audit team in the Exemptrulebase to ignore Traffic Anomalies.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Which three actions should be taken on a rule in the IDP rule base when the sensor is in transparent mode? (Choose three.)

A. Close client and server.
B. Drop stream.
C. Drop connection.
D. Drop packet.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

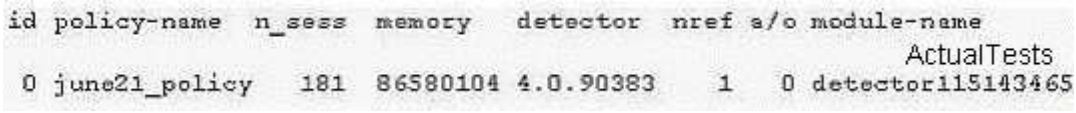
QUESTION 51
What contains instructions on how the sensor should decode protocols?

A. PCAP files
B. policy.set
C. detector.o
ActualTests.com
D. ACM

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Exhibit:



You work as an administrator at Certkiller .com. Study the exhibit carefully. In the exhibit, which command would have produced this output?

A. sctop "p" option
B. scio agentstats policy list
C. scio policy list vr0
D. scio policy list s0

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
What is the function of Terminate Match?

A. makes a rule terminal when the source IP, destination IP, service, and attack object match
B. makes a rule terminal when the source IP, destination IP, and service match
C. terminates the connection if a rule is matched
D. terminates all connections from a source if the rule is matched

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
When creating a new signature-based attack object, which four components must be specified? (Choose four.)

A. target platform
B. IP header values
C. time binding
D. service binding
E. context
F. attack pattern
ActualTests.com

Correct Answer: ADEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Which OSI layer(s) of a packet does the IDP sensor examine?

A. layers 4-7
B. layers 2-7
C. layers 2-4
D. layer 7 only
"Pass Any Exam. Any Time." - www.actualtests.com 21
Juniper JN0-541: Practice Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
When configuring a honeypot rule, which three fields must you specify? (Choose three.)

A. Attack Object
B. Service
C. Source Address
D. Destination Address

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Which statement is true about packet capture in the IDP sensor?

A. Packet capture records all packets flowing through the sensor.
B. You can configure a particular number of packets to capture before and after an attack.
C. The Log Viewer has no indication of whether a log message has associated packet captures.
D. You can only log packets after an attack packet.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which sensor utility is used to decode the contexts of a sequence of packets?

ActualTests.com

A. scio pcap
B. scio ccap
C. netstat
D. tcpreplay

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which sensor command will capture packets on a particular interface?

A. sctop
"Pass Any Exam. Any Time." - www.actualtests.com 22
Juniper JN0-541: Practice Exam
B. tcpdump
C. tcpreplay
D. netstat

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
What is the function of a compound attack object?

A. Combines multiple signature based attack objects, or anomaly-based attack objects, into a single attack object.
B. Allows the sensor to perform custom actions based on combinations of attacks.
C. Combines multiple attacks in a single rule base.
D. Looks for multiple occurrences of the same attack.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
How does the IDP sensor emulate a honeypot?

A. The sensor will prompt the user for user names and passwords, but does not provide further protocol emulation.
B. The sensor will reply to TCP and UDP connection requests, but will not perform any further protocol emulation.
C. The sensor will reply to TCP connection requests, and emulate the requested protocol.
D. When the sensor receives a TCP SYN request, the sensor will reply with a SYN/ACK.
ActualTests.com

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which two statements are true about the Enterprise Security Profiler (ESP)? (Choose two.)

A. The ESP indicates when existing hosts or protocols are being used.
B. The ESP indicates which hosts are talking with each other, and which protocols are being used.
C. The ESP provides a summary of protocols and contexts on each host.
D. The ESP indicates when a specific machine has been attacked.
"Pass Any Exam. Any Time." - www.actualtests.com 23
Juniper JN0-541: Practice Exam

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
On a sensor, which command will list the status of the IDP processes?

A. scio getsystem
B. scio agentconfig list
C. scio vr list
D. sctop "s" option
E. serviceidp status

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
What is the default admin account password on the sensor?

A. juniper01
B. password
C. admin
D. abc123

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
How do you access the ACM interface on an IDP sensor? ActualTests.com

A. https://<IP address of sensor>
B. http://<IP address of sensor>
C. use the IDP user interface
D. use the SSH interface

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
In which two ways can you view the IP address of a sensor's eth0 interface? (Choose two.)

A. ipconfig
B. ACM
C. the Security Manager GUI
D. tcpdump

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
What is a TCP connect scan?

A. A machine sends UDP request packets to a target to determine which ports are open.
B. A machine sends ICMP echo request packets to multiple targets to determine which targets are alive.
C. A machine sends SYN packets to a target to determine which ports are open. If a SYN ACK is received from the target, an ACK packet is sent.
D. A machine sends SYN packets to a target to determine which ports are open. If a SYN ACK is received from the target, no further packets are sent.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Which three devices support clustering? (Choose three.)

A. IDP 1100
B. IDP 10
C. IDP 600
D. IDP 200
ActualTests.com
E. IDP 50

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
On a sensor in transparent mode, how many virtual circuits are assigned to a virtual router?

A. 2
B. 1
C. 1 or 2
D. 3 or more
"Pass Any Exam. Any Time." - www.actualtests.com 25
Juniper JN0-541: Practice Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Which three columns can be seen in the Network View of the Enterprise Security Profiler? (Choose three.)

A. Src and Dest IPs
B. Packet Capture
C. Src OS Name
D. Service

E. Context and Context Data

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
What does the action "close client" instruct the sensor to do?

A. Send a TCP reset to the client and server.
B. Send a UDP reset to the client.
C. Drop all packets from the client's IP address.
D. Send a TCP reset to the client.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

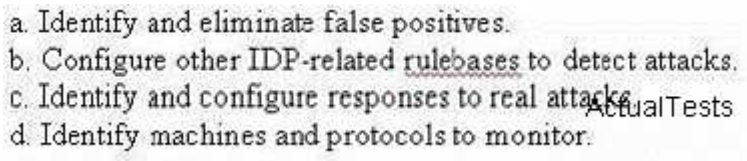
QUESTION 72
ActualTests.com
Which three functions does the IDP sensor perform? (Choose three.)

A. detects new hosts on the network
B. forwards logs and status messages to Security Managerserver
C. displays logs in Security Manager GUI
D. performs attack detection and prevention

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Exhibit:



Given the information in the exhibit
What is the proper order when fine tuning a policy?

A. d, a, b, c

B. d, c, a, b
C. d, a, c, b
D. b, d, a, c

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
What is the function of a dynamic attack object group?

A. To create a custom grouping of attack objectswhich will be automatically updated during an attack database update
B. To create a custom grouping of attack objects that will not be modified during an attack object database update.
C. To allow an administrator to group together user-defined attack objects only.
D. To allow Juniper engineers to specify a particular group of attack objects.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
ActualTests.com

QUESTION 75
Which two tasks can be performed using the ACM? (Choose two.)

A. Disable a security a policy.
B. View a list of current TCP flows.
C. Change the One-Time Password.
D. Enable or disable SSH access, and restrict which networks can SSH to the sensor.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76

When the action "close client" is performed by an IDP sensor on an FTP session, which message will be displayed to the client when using FTP on the command line?

A. no message is seen, the connection is unresponsive
B. packet dropped
C. connection closed by foreign host
D. no message is seen, the connection continues as normal

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
You implement backdoor detection and you notice that an alert is generated each time an SSH session is established with the protected servers. What must you do to correct the situation?

A. You create an exempt rule for SSH in the exempt rule base.
B. There is no way to disable alerting on SSH if you have backdoor detection enabled.
C. You modify the IDP rule base to include the SSH protocol in the top rule, and specify action Ignore.
D. You modify the backdoor rule base to include the SSH protocol in the top rule, and specify action Ignore.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Which interface does IDP use to communicate with Security Manager?

A. eth0

B. console port
C. eth1
D. HA port

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Within the SYN protector rule base, what is the function of relay action?

A. It will create a session with the server only if the client completes the three-step TCP handshake with the sensor.

B. It will not monitor incoming SYN requests.
C. It will relay all SYN connections to a fake IP.
D. It will monitor new connections to a protected server, but not prevent them.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Exhibit:

Time Received	Src Addr	Dst Addr	Protocol	Dst Port	Subcategory
8/29/06 10:20:08 AM	10.1.3.50	0.0.0.0	HOPOPT	0	TSIG Session Rate Exceeded
8/29/06 10:20:48 AM	10.1.3.50	0.0.0.0	HOPOPT	0	TSIG Session Rate Exceeded

You work as an administrator at Certkiller .com. Study the exhibit carefully. In the exhibit, which rule base would have generated the log message?

A. traffic anomaly
B. networkhoneypot
C. backdoor
D. SYN protector

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Assume that Enterprise Security Profiler (ESP) has already captured data for your network. You want to view traffic that does not match the following protocols: HTTP, HTTPS, DNS. Which steps must you perform?

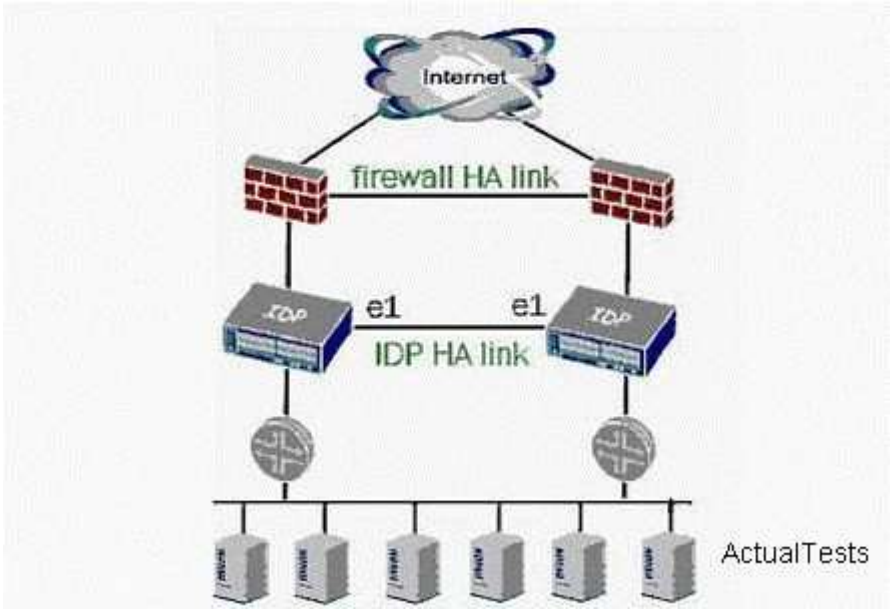
A. Under the Violation Viewer tab, create a permitted object, select that object, and then click Apply.
B. Under the Violation Viewer tab, create a filter to show only tracked hosts.
C. Under the Violation Viewer tab, create a violation object, select that object, and then click Apply.
D. Under the Application View tab, create a permitted object, select that object, and then click Apply.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
"Pass Any Exam. Any Time." - www.actualtests.com 29
Juniper JN0-541: Practice Exam

Exhibit:



You work as an administrator at Certkiller .com. Study the exhibit carefully. In the exhibit both firewalls are active/active, which two statements are true for this scenario? (Choose two.)

A. Only one firewall is actively passing traffic.
B. Upon failure of a sensor, user traffic will be sent over the IDP HA link.
C. Routers are running a redundancy protocol.
D. Firewalls are running a redundancy protocol.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
ActualTests.com

QUESTION 83
What is "the location of an attack pattern protocol stream"?

A. context
B. attack signature
C. protocol anomaly
D. dynamic attack object group

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
"Pass Any Exam. Any Time." - www.actualtests.com 30
Juniper JN0-541: Practice Exam

What does the action "drop packet" instruct the sensor to do?

A. Drop the specific session containing the attack pattern.
B. Drop any packet matching this source IP, destination IP, and service.
C. Drop all packets from the attacker's IP address.
D. Drop only the specific packet matching the attack object.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

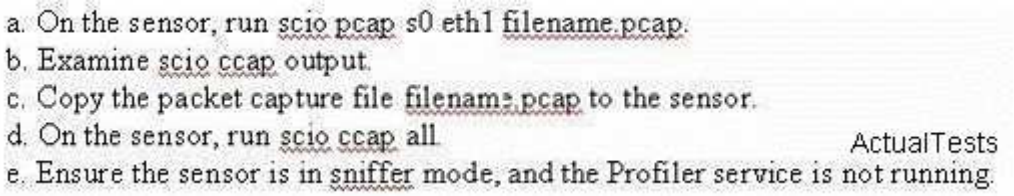
QUESTION 85
What is "a signature or protocol anomaly combined with context information"?

A. attack object
B. context
C. attack signature
D. protocol anomaly

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Exhibit:



ActualTests.com
In order to obtain attack information so that you can create a new attack object definition, you must follow certain steps. Given the steps displayed in the exhibit, assume you have acquired a packet capture of the attack.
What is the correct order for these steps?

A. e, c, d, b, a
B. e, c, a, d, b
C. d, e, c, a, b
D. e, c, d, a, b

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which two statements are true? (Choose two.)

A. In transparent mode, a virtual circuit maps one-to-one with a physical interface.
B. A virtual circuit is not a forwarding interface.
C. Virtual circuits on a sensor can be listed using the commandsctop vc list.
D. A virtual circuit is a communications path in and out of the sensor.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

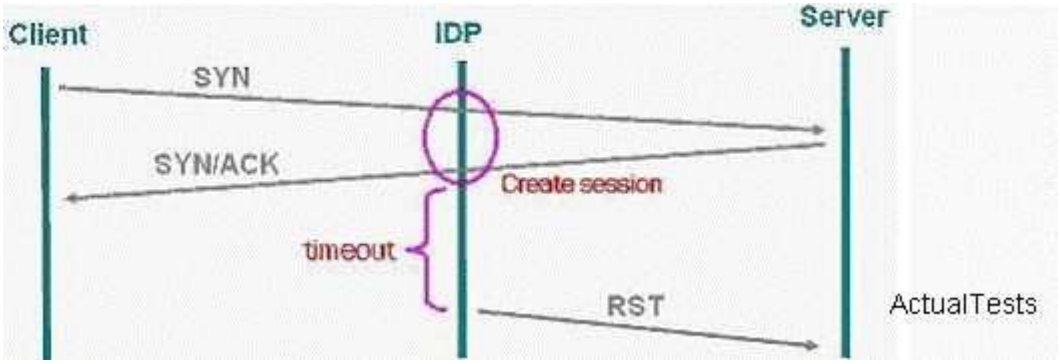
QUESTION 88
You want Enterprise Security Profiler (ESP) to generate a message when a new host is detected on a network. Which two steps must you perform? (Choose two.)

A. Under the Violation Viewer tab, create a permitted object, select that object, and then click Apply.
B. Configure ESP to enable application profiling, and select the contexts to profile.
C. Start or restart the profiler process.
D. Configure ESP to enable alerts for new host detected.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Exhibit:



ActualTests.com

You work as an administrator at Certkiller .com. Study the exhibit carefully. In the exhibit, which SYN protector mode is the IDP using?

A. protective
B. passive
C. handshake

D. relay

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
How can you monitor real-time IP flows through the IDP sensor?

A. Use the sensor commandsctop.
B. Use the Security Manager GUI traffic logs.
C. Use the Security Manager GUI dashboard.
D. Enable debug flow basic on the sensor.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
If an IDP sensor finds that a packet matchesa particular IDP rule, and then finds a matching exempt rule, what does the sensor do?

A. Creates a log entry for the matching rule, performs the action in the IDP rule, and then examines the next IDP rule in the list.
B. Does not create a log entry, does not perform the action in the matching rule, and then examines the next IDP rule in the list.
C. Creates a log entry for the matching rule, does not perform the action in the IDP rule, and then examines the next IDP rule in the list.
D. Does not create a log entry or perform the action in the matching rule, and then stops examining the remainder of the IDP rules for that particular packet.
ActualTests.com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Which two tasks can be performed using the ACM? (Choose two.)

A. Upgrade the firmware on the IDP sensor.
B. Install a policy on the IDP sensor.
C. Change the mode in which the sensor is operating.
D. Change the management IP address for the IDP sensor.

Correct Answer: CD

Section: (none)
Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com 33
Juniper JN0-541: Practice Exam

QUESTION 93
Which statement is NOT true?

A. Target platform of idp-sos3.0 indicates the platform is software that runs on an ISG1000 or ISG 2000.
B. Target platform of sos.5.0.0 indicates the platform runs Screen OS software that supports Deep Inspection.
C. Target platform sos-av.5.0.0 indicates the platform is Screen OS software that supports the Anti-Virus feature.
D. Target platform of idp-4.0.0 indicates the platform is software that runs on an IDP sensor.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
In which three situations would you create a compound attack object? (Choose three.)

A. When the pattern "@@@@@@@@" and context "ftp-get-filename" completely define the attack.
B. When attack objects must occur in a particular order.
C. When one of the attack objects is a protocol anomaly.
D. When the pattern needs to be defined using a stream 256 context.
E. You have at least two attack objects that define a single attack.

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
ActualTests.com

QUESTION 95
When you have two IDP sensors in a cluster, and the sensors are using external HA, which three devices will be performing the failure detection and failover execution? (Choose three.)

A. bypass units connected to the sensors
B. firewalls running a redundancy protocol
C. routers running a redundancy protocol
D. IDP sensors
E. load balancers

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com 34

QUESTION 96
What contains instructions on how the sensor should decode protocols?

A. detector.o
B. policy.set
C. ACM
D. PCAP files

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Which sensor process records unique network activity at layers 3, 4, and 7?

A. idpLogReader
B. sciod
C. profiler
D. idp
E. agent

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Given the following steps:

A. Attach the sensor to the management network.
ActualTests.com
B. Place the sensor inline in network.
C. Create and install a policy on the sensor.
D. Establish communication between Security Manager and the IDP sensor.
E. Configure the sensor deployment mode and management interface IP.
F. Test connectivity through the sensor.
Which order is correct when initially deploying a sensor in a network?
G. b, f, e, a, d, c
H. e, a, d, c, b, f
I. a, e, d, c, f, b
J. e, a, d, b, f, c

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which interface does IDP use to communicate with Security Manager?

A. eth0
B. console port
C. eth1
D. HA port

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
In the Enterprise Security Profiler, what would you define under Permitted Objects?

A. Define traffic that violates your security policy.
B. Definevalid, permitted activity on the network.
C. Define any attacks that violate your security policy.
D. Define violations of permitted activity on the network.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
What two statements are true about the attack object database update process? (Choose two.)
ActualTests.com

A. Attack objects are downloaded from the Juniper web site over TCP port 443 and are stored on Security Manager.
B. Attack object database update can be scheduled using the commands guiSvrCli.sh and cron.
C. Attack object database update can be scheduled using the two commands idpSvrCli.sh andcron.
D. The administrator is given the choice of which static groups to update.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102

Which three actions should be taken on a rule in the IDP rule base when the sensor is in transparent mode?

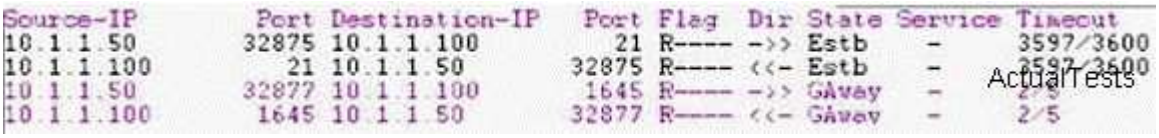
(Choose three.)

A. Drop packet.
B. Close client and server.
C. Drop connection.
D. Drop stream.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
Exhibit:



Source-IP	Port	Destination-IP	Port	Flag	Dir	State	Service	Timeout
10.1.1.50	32875	10.1.1.100	21	R-----	->>	Estb	-	3597/3600
10.1.1.100	21	10.1.1.50	32875	R-----	<<-	Estb	-	3597/3600
10.1.1.50	32877	10.1.1.100	1645	R-----	->>	GAway	-	2/5
10.1.1.100	1645	10.1.1.50	32877	R-----	<<-	GAway	-	2/5

You work as an administrator at Certkiller .com. Study the exhibit carefully. In the exhibit, which sensor command would have produced this display?

A. scio subs qmodules s0
B. sctop "t" option
C. sctop "s" option
D. scio policy list s0

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
ActualTests.com
Which sensor utility will replay pcap files?

A. scio pcap
B. scio ccap
C. tcpdump
D. netstat

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
In a packet, which three must match an IDP rule before an action is performed on that packet or connection? (Choose three.)

A. service
B. source/destination address
C. terminate match
D. source/destinationnetmask
E. attack object

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
You have a rule in your IDP policy that detects all HTTP signatures that are targeted towards your Web server. You notice a log message is generated each time a Web user accesses the SQL database with the default passwords. Your Webmaster does not want to reprogram the Web page to use more secure SQL passwords. How do you disable alerts on this false positive?

A. Create a rule in the Exempt rule base; specify target address of your Web server; include only the specific HTTP SQL default password signature.
B. Create a rule at the top of the Exempt rule base; specify target address of your Web server; include all HTTP signatures.
C. Create a rule at the top of the IDP rule base for any traffic destined to your Web server; specify action of Exempt.
D. Create a rule at the top of the Exempt rule base; specify target address of your Web server; include all HTTP signatures; make this a terminal rule.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
ActualTests.com
Which two statements about Log Viewer filters are true? (Choose two)

A. Logs can be filtered based on time.
B. Fitters once applied cannot be cleared.
C. Fitters created and saved as view are visible to all users.
D. Fitters applied to a current view are seen at the bottom of the User Interface screen.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108

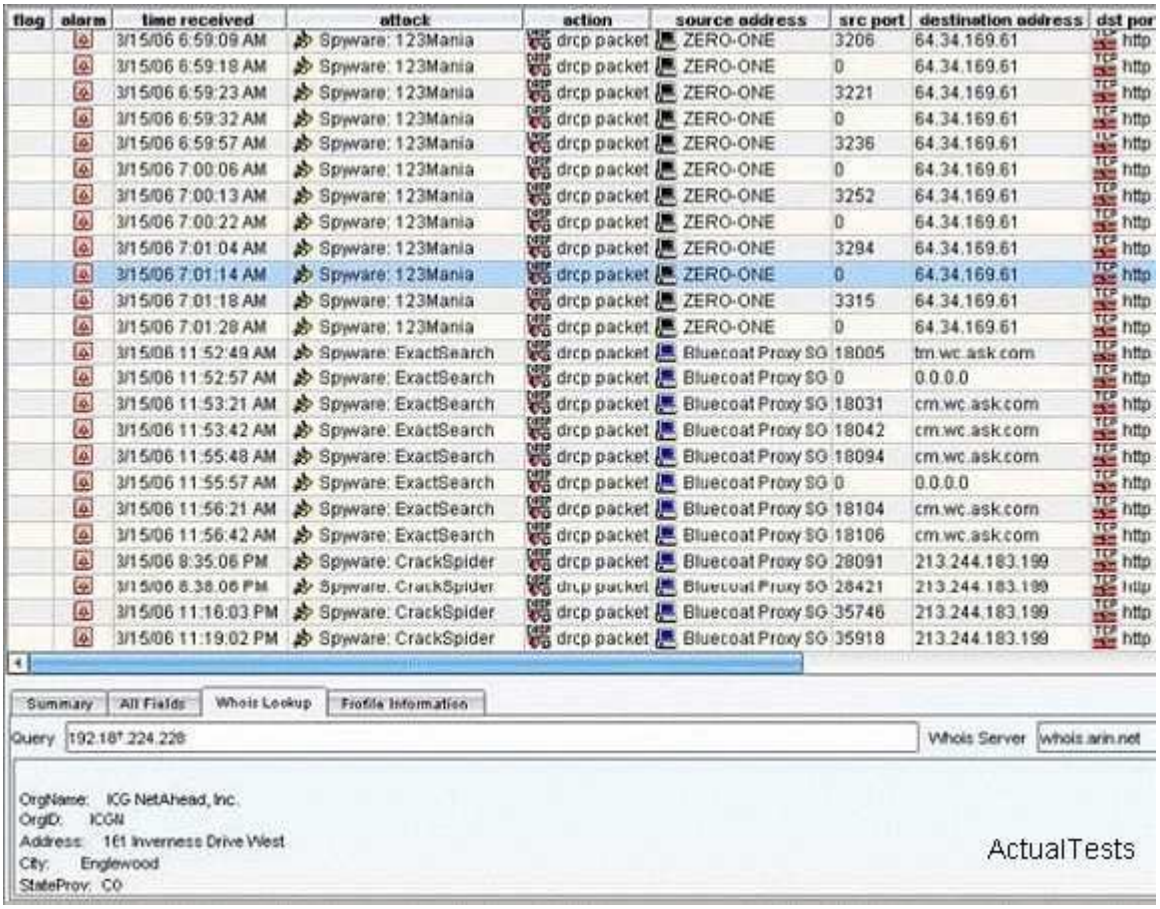
When Address Resolution is enabled in the Log Viewer, which machine is responsible for performing the DNS Lookups?

"Pass Any Exam. Any Time." - www.actualtests.com 38
Juniper JN0-541: Practice Exam

A. IDP Sensor
B. WHOIS Servers
C. IDP User Interface
D. IDP Management Server

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:



QUESTION 109
ActualTests.com
You have a false positive in the Log Viewer that you want to exclude from further detection. What should you do?

A. right-click on that event, selectExempt
B. go to the Exempt rules and add that Attack Object
C. right-click on that event, choose Filter - Not this Value

D. create a policy in the top of the rulebase that ignores that event and make it a Terminal rule

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
"Pass Any Exam. Any Time." - www.actualtests.com 39
Juniper JN0-541: Practice Exam

Which statement is true about log suppression?

A. Log suppression is not supported inNetScreen-IDP.
B. Log suppression suppresses alerting on specific logs.
C. Log suppression suppresses recurring log messages into a single log entry.
D. Log suppression preventsa IDP Sensor from sending logs to the IDP Management Server.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
Which two statements about disk management on the IDP Sensor are true?

A. IDP Management Server can be configured to send disk space alerts.
B. If the IDP Sensor disk is full, the IDP Sensor will not store any additional logs or packet captures.
C. If the IDP Sensor disk is full IDPSensore starts oldest log entries first, and packet captures second.
D. If the IDP Management Server disk is full, the oldest packet captures are purged first, and the log messages are purged second.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
Which two statements are true about packet logging? (Choose two.)

A. Packets captured are stored inpcap format.
B. IDP senor will tag all replayed packets are offline.

C. Packets logged can be replayed back into the IDP Sensor.
D. Packets captured cannot be replayed back into the IDP Sensor

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
In which three fields does Log Investigator allow you to create reports and view logs? (Choose three.)

A. Time
B. Attack

C. Destination Port
D. Sensor IP Address

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
Which statement is true about Packet Logging in IDP?

A. Packet captures are stored on each IDP Sensor.
B. Packet captures are stored on the Management Server.
C. Packets are not cryptographicallytimestamped or authenticated.
D. Packets are cryptographicallytimestamped and authenticated using PKI.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
Log Investigator identified26 attacks from a specific source to a specific destination.
How can you view the details of these 26 attacks?

A. right-click on the 26 value, select View by Key
B. right-click on the 26 value, select View in Log Viewer
C. go to the Log Viewer and filter that specific source and destination address
D. go to the Log Investigator and filter that specific source and destination address

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
ActualTests.com

QUESTION 116
Which three statements about the ESP are true? (Choose three.)

A. ESP can log policy violations.

B. ESP can detect network changes.
C. ESP can work in all deployment modes of the IDP Sensor.
D. ESP uses an object database that is stored only on the IDP Sensor.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
"Pass Any Exam. Any Time." - www.actualtests.com 41
Juniper JN0-541: Practice Exam

What information is provided by the host table (Choose three.)

A. IP address
B. Subnet mask
C. MAC address
D. VLAN information

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
Which two does ESP use to help identify applications running on certain hosts? (Choose two.)

A. value
B. service
C. context
D. VLAN Information

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
What is a Violation Object in ESP?

A. any object that defines configuration of ESP
B. any object that violates application context in ESP
C. any object that violates the Security Policy configured in ESP
D. any object that defines valid network connections on the network ActualTests.com

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
"Violation objects are objects that contain simple rules , consisting only of source IP, destination IP, service. The implied action is "permit". Use the object to define what you should see on the network - as opposed to an attack object which defines what you don't want to see" Juniper Networks Product training : Release 3.0A, May 2004 Undisclosed author, page4-20

QUESTION 120
"Pass Any Exam. Any Time." - www.actualtests.com 42
Juniper JN0-541: Practice Exam

On which three fields can ESP filter data? (Choose three.)

A. Time
B. Service
C. Access Type
D. IP address (Source IP or Destination IP)

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
You want ESP to alert on abnormal activities in a network. Which two actions should you take to accomplish this? (Choose two.)

A. create a Violation Object
B. Create a filter in the Profiler to show only tracked hosts
C. Create rule in the Profilerrulebase to log traffic from any internal source
D. From the Profiler configuration, select the Alert tab and select all options

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
Which three columns can be seen in the Application view of Profiler? (Choose three.)

A. Protocol
B. Context and Context Value
C. Source and Destination IPs
D. Date First Seen and Last Seen
ActualTests.com

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
Which two statements about ESP are true? (Choose two.)

A. ESP is started try default in IDP version 3.0 or newer.
B. ESP must be configured and started on the IDP Sensor CLI before it is used.
C. ESP must be synchronized manually by the administrator to view the latest data.
D. ESP must be configured and started on each IDP Sensor manually, through the IDP User Interface.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
Which statement is true about reverting Security Policies?

A. The Security Policy cannot be reverted.
B. The Security Policy can be reverted from the ACM of each IDP Sensor.
C. The Security Policy can be reverted at any time from the IDP User interface to a previously installed policy.
D. If you save a copy of your Security Policy from the IDP Sensor, you can revert back by loading the previous copy from the CLI.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
Which statement is true about the Attack Object Update process?

A. The Attack Update can be automatically scheduled by the administrator in control.
B. The Attack Update must be manually downloaded by the administrator from the Juniper site and installed on each Sensor.
C. The Administrator in control must initiate a signature update or the User Interface can be configured to check for updates on startup.
D. Each Sensor updates its own Attack Objectsautomatically, however they must be able to access the Jumper site on TCP/443 (SSL).

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
ActualTests.com

QUESTION 126
Which command from the IDP Sensor CLI can be used to display the sensor statistics, the policy information, and mode of sensor deployment?

A. sctop -s option
B. scio sensor stat
C. scio list s0 sensor stat
D. sensor statistics can be displayed only from the UI

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com 44
Juniper JN0-541: Practice Exam

Explanation:
sctop Commands
Use sctop commands to monitor the Sensor connection tables and view Sensor status :
/ usr /bin
Location
Syntax sctop options
Options Function
-h Displays help for the sctop utility.
-a Displays the ARP/MAC table.
-I Displays the IP flows.
-c Displays the ICMP flows.
-u Displays the UDP flows.
-t Displays the TCP flows.
-r Displays the RPC program table.
-x Displays the RPC XID table.
-s Displays status information about the Sensor. -m Displays system memory statistics.
-l Displays Q-module statistics.
-e Displays rulebase statistics.
-g Displays aggregate statistics.
-k Displays attack statistics.
-p Displays Spanning Tree Protocol (STP) information.
-b Displays IP Action table.
-z Displays packet distribution.
-d Displays the strip chart, a text-based chart for packet/second, kbits /second, and the sessions that the UI sees.
-f Displays fragment chain.
-w Displays HA status.
-y Displays IDS cache statistics.
ActualTests.com
-v Sorts in reverse order.
-0 Disables sorting.
-1 Sorts by bytes per session.
-2 Sorts by packets per session.
-3 Sorts by expiration.
-4 Sort by service.
-5 Sorts by destination port.
-6 Sorts by source address.
-7 Sorts by destination address.
* Juniper Networks Intrusion Detection and Prevention, Concepts and Examples Release 4.1, Page 204
* Juniper Networks Inc,
* Writer: Mark Schlagenhauf

* Editor: Lisa Eldridge

QUESTION 127
Which two statements are true concerning the licensing of IDP Sensors? (Choose two.)

A. There is no license file to be concerned with in IDP.
B. You must manually load a license on your Sensor before placing in-line.
C. You manually back up your license using the utilities provided by Juniper.
D. Each IDP Sensor has a license file loaded. If the license file is lost through disk corruption, it cannot be recovered.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
What should you do to purge logs for certain days from your IDP Management Server?

A. purge the logs from the IDP User Interface
B. Logs cannot be purged until the disk is full.
C. Purge the logs manually from the CLI of each IDP Sensor
D. Purge the logs manually from the CLI of the IDP Management Server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
ActualTests.com
Which two types of reports can be created? (Choose two.)

A. user-based
B. time-based
C. count-based
D. attack-based

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
Which two statements are true about quick reports? (Choose two.)

A. Maximum duration is restricted to 12 hours.

B. Quick reports are ideal for zero day investigation.
C. Quick reports can be created only from the Log Viewer.
D. Once a quick report is created, the report options cannot be modified.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
Which statement is true about the NetScreen IDP Closed Loop Investigation (CLI)?

A. CLI describes the IDP Sensor command line utilities.
B. CLI provides easy navigation between Log Viewer and Log Investigator.
C. CLI provides easy navigation between Log Investigator, Log Viewer, Profiler information and quick reports.
D. CLI provides easy navigation between Log Investigator, Log Viewer, Profiler information and pre-defined reports.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
Which columns are available for creating time-based report?

A. Time
B. Attack Object
C. Source and Destination Address
D. Columns options are not available.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
Which statement is true about exporting reports?

A. Reports must be exported manually into PDF format.
B. Reports must be exported manually into HTML format.
C. Reports can be exported automatically into PDF format.
D. Reports can be exported automatically into HTML format.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com 47
Juniper JN0-541: Practice Exam

QUESTION 134
Which layers of the OSI Model does IDP look into when inspecting a packet?

A. Layers 2-7
B. Layers 3-7
C. Layer 7 only
D. Layers 2-4 only

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
What are two limitations of traditional IDS systems? (Choose two.)

A. do not detect internal attacks
B. do not use signatures for known attacks
C. do not operate inline so they cannot effectively block all attacks
D. frequentlyhave false positives due to less accurate packet signatures

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
Which method of detection does IDP Sensor use to detect attacks against a fake system on the network?

ActualTests.com

A. NetworkHoneypot
B. Spoofing Detection
C. Stateful Signatures
D. Backdoor Detection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
Which method of detection does IDP Sensor use to detect rootkits or Trojans present on internal systems?

A. Protocol Anomaly
B. NetworkHoneypot
C. Stateful Signatures
D. Backdoor Detection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
Which method of detection does IDP Sensor use to detect a network scan or portscan?

A. DOS Detection
B. Traffic Anomaly
C. Protocol Anomaly
D. Backdoor Detection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
Which two statements are true about Trojans? (Choose two.)

A. They are executables that infect only executable programs.
B. They are programs often used to gather information about a host.
C. They can secretly permit access to an infected computer from an outside host.
D. They are programs that target onlywebservers by overwhelming them with traffic.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
ActualTests.com

QUESTION 140
What are three functions of the IDP Management Server? (Choose three.)

A. blocks attacks
B. stores Security Policies and Attack Objects
C. consolidates logs from the various IDP Sensors in a network
D. receives and manages connections from IDP User Interfaces

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com 49
Juniper JN0-541: Practice Exam

QUESTION 141
What is a buffer overflow attack?

A. amisconfigured application that has a known security hole
B. an attack that overflows a server with many connections until it crashes
C. an attack that takes advantage of a backdoor within a vulnerable application
D. an attack which injects just the right amount of data into a vulnerable application, causing the application to execute the malicious code that was injected

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
Which statements are true about the IDP Management Server? (Choose two.)

A. One IDP Management Server can manage multiple IDP Sensors.
B. Each IDP Sensor must have its own Management Server component.
C. The IDP Management Server process can be run on a IDP Sensor for evaluation purposes.
D. Supported operating systems for IDP Management Server are Windows 2000, BSD UNIX, and Linux.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
Which IDP Sensors support the NetScreen IDP bypass unit? (Choose two.)

A. IDP-10
ActualTests.com
B. IDP-100
C. IDP-500
D. IDP-1000

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
On which two operating systems can the IDP Management Server be installed? (Choose two.)

A. Linux

B. Solaris
"Pass Any Exam. Any Time." - www.actualtests.com 50
Juniper JN0-541: Practice Exam
C. Windows
D. Any Java capable operating system

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
Which command verifies the IDP Management Server process?

A. service MgtSvr status
B. server mgtSvr status
C. servicemgtServer status
D. service management status

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The correct command is listed below thanks.
[root@idpmanager ~]# cd /
[root@idpmanager /]# ls
bin dev home lib lost+found misc opt root selinux sys usr boot etc initrd lib64 media mnt proc sbin srv tmp var
[root@idpmanager /]# cd usr / mgtsvr
-bash: cd : usr / mgtsvr : No such file or directory [root@idpmanager /]# cd usr / idp / mgtsvr /bin
-bash: cd : usr / idp / mgtsvr /bin: No such file or directory [root@idpmanager /]# cd usr / idp
[root@idpmanager idp]# ls
mgt- svr
[root@idpmanager idp]# cd mgt- svr /bin
ActualTests.com
[root@idpmanager bin]# ls
dbLogExporter logReceiver.sh mgtSvr.sh statusReceiver dbLogExporter.sh logWalker mLogPurger
statusReceiver.sh guiDaemon logWalker.sh mLogPurger.sh
guiDaemon.sh mailSender statusMonitor
logReceiver mailSender.sh statusMonitor.sh
[root@idpmanager bin]# service mgtSvr status
Retrieving status...
statusMonitor (pid 2622)... ...ON
logReceiver (pid 2633)... ..ON
guiDaemon (pid 2663)... .ON
statusReceiver (pid 2752)... ..ON
mLogPurger (pid 2696)... ...ON
logWalker (pid 2632)... .ON

"Pass Any Exam. Any Time." - www.actualtests.com 51
Juniper JN0-541: Practice Exam

dbLogExporter (pid 2733)... ...ON
[root@idpmanager bin]#

QUESTION 146
What is the function of the Device Monitor?

A. debugs IP flows through an IDP Sensor
B. monitors the status of all critical devices in a network
C. monitors the status of all configured IDP Sensors and the Management Server
D. view physical memory usage and CPU utilization for IDP Sensors and the Management Server

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
What information is necessary to register an IDP Sensor with the IDP Management Server? (Choose three.)

A. IDP Sensor VIN#
B. IDP Sensor hostname
C. IDP Sensor management IP address
D. IDP Sensor One-time Password (OTP)

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
ActualTests.com
How do you access the webUI ACM Interface on a IDP Sensor?

A. through the SSH Interface
B. http://<IP Address of Sensor>
C. https://<IP Address of Sensor>
D. through the IDP User Interface

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
"Pass Any Exam. Any Time." - www.actualtests.com 52
Juniper JN0-541: Practice Exam

Which two statements are true as they relate to a sniffer mode IDP Sensor deployment? (Choose two.)

A. An IP address must be assigned to the sniffer interface.
B. It does not affect the performance or availability of the network.
C. It provides passive monitoring only with limited attack prevention.

D. IDP Sensor cannot be managed by the IDP Management Server Sniffer mode.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

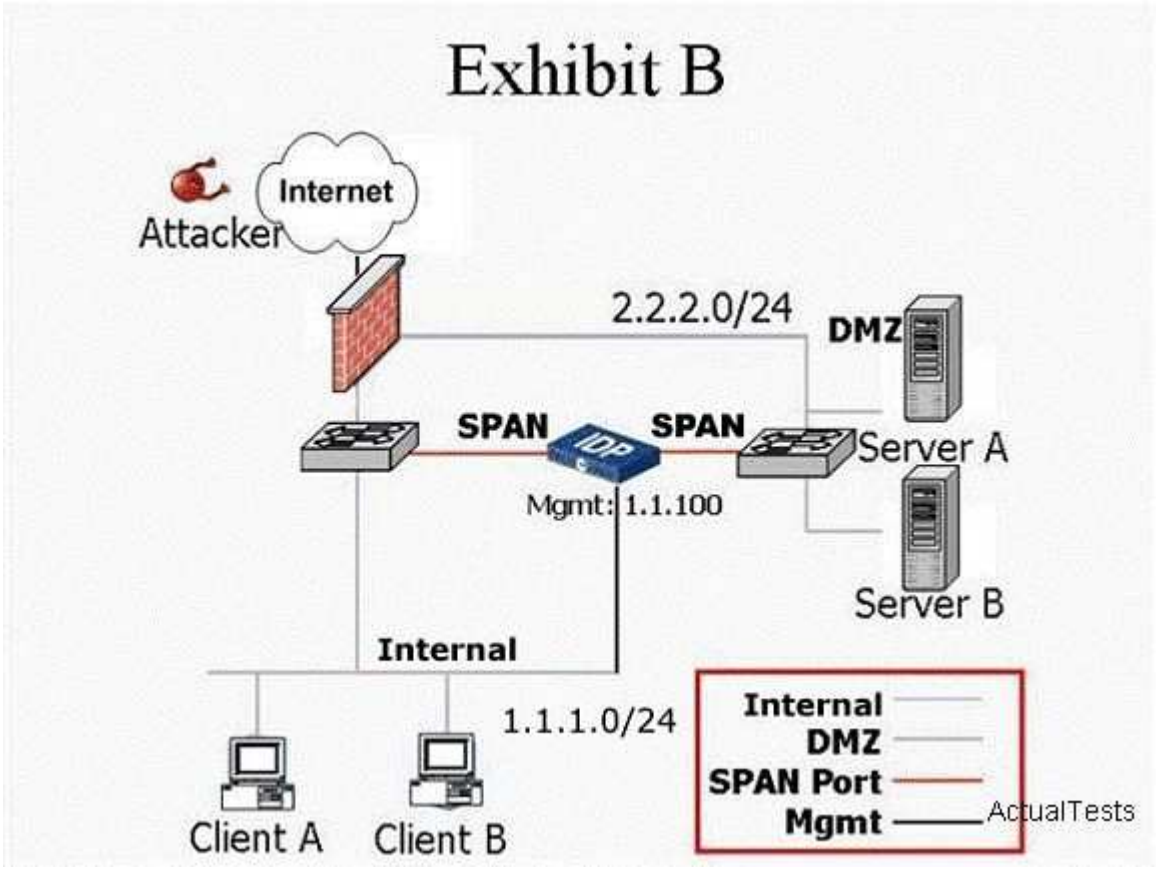
QUESTION 150
On which two operating systems can the IDP User Interface be installed? (Choose two.)

A. Linux
B. Solaris
C. Windows
D. Any Java capable operating system

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
Exhibit:
You work as an administrator at Certkiller .com. Study the exhibit carefully. Which three statements are true about the capabilities of IDP when deployed as shown in the exhibit? (Choose three.)
Exhibit:
ActualTests.com



A. IDP Sensor can detect attacks between Client A and Server A in this mode.
B. IDP Sensor can detect attacks between Server A and Server B in this mode.
C. IDP Sensor can only drop offending TCP traffic by sending TCP Resets in this mode.
D. IDP can drop any offending traffic between internal and DMZ networks in this mode.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
Which two tasks can be performed from the ACM? (Choose two.)

A. change the mode which IDP Sensor is operating
ActualTests.com
B. upgrade the firmware on the IDP Sensor
C. install a Security Policy on the IDP Sensor
D. change the Management IP address of a IDP Sensor

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
When migrating from Sniffer mode to inline mode, what changes should you make so IDP Sensor can effectively drop attacks?

A. re-install the IDP Sensor software
"Pass Any Exam. Any Time." - www.actualtests.com 54
Juniper JN0-541: Practice Exam
B. change the IDP Sensor mode from the ACM
C. delete and re-add your IDP Sensor object to the Network Objects as an inline Device
D. modify the rule action to "Drop Packet" or "Drop Connection" on rules that you want to drop attacks, and install the modified security policy

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
What is the function of Terminate Match?

A. terminates the connection if the rule is matched
B. terminates all connections from a source if the rule is matched
C. makes a rule terminal when the Source IP, Destination IP and service match
D. makes a rule terminal when the Source IP, Destination IP and Attack Object match

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
Which two are IP Actions? (Choose two.)

A. IDP Notify
B. IDP CLOSE
C. IDP TCP RST
D. IDP Drop packet

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
ActualTests.com

QUESTION 156
What does a Drop Connection action do?

A. drops all packets from the attacker's IP
B. drops any packet matching thissrc/dst/protocol

C. drops the specific session containing the attack pattern
D. drops only the specific packet matching the attack pattern

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com 55
Juniper JN0-541: Practice Exam

QUESTION 157
How do ignore and None actions in the Main Rulebase differ?

A. None actions cause IDP NOT to perform any AttackMatching on this rule.
B. Ignore actions cause IDP NOT to perform any Attack Matching on this rule.
C. Ignore actions cause IDP to ignore and subsequently drop all traffic matching this rule.
D. Ignore actions will cause IDP to disregard and further attack matching when an attack object is matched.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
You implement Backdoor Detection and you notice that an alert is generated each time an SSH session is established with the protected servers. What must you do to correct the situation?

A. You create an Exempt rule for SSH in the Exemptrulebase.
B. You modify the Mainrulebase to include the SSH Protocol in the top Ignore rule.
C. There is no way to disable alerting on SSH if you have Backdoor Detection enabled.
D. You modify the Backdoor Detectionrulebase to include the SSH Protocol ports in the top Ignore rule.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
When a security policy is installed on a IDP Sensor, which statement is true? (Choose two.)
ActualTests.com

A. A Security policy must first be verified before it is installed.
B. A policy version is created when is successfully installed.
C. Thepolicy.set file is deleted and a new file is created.
D. IDP Sensor stops processing traffic when policy is being installed.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
You update your attack Object database from the IDP User Interface. What must you do before the new signature attack objects become active on your IDP Sensor?

A. You restart the IDP Sensor.
B. You restart the IDP Service on the IDP Sensor (IDP restart).
C. No changes are required other than saving the policy changes.
D. You install the updated Security policy on that IDP Sensor from the IDP User Interface.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
What is the function of an IP action?

A. modifies the IP Header to prevent the attack
B. modifies the IP Header to redirect the attack
C. permits or denies the traffic, based on the IP Header
D. blocks subsequent connections from specific IP addresses

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
What is the function of a Dynamic Attack Object Group?

A. groups together only user-defined Attack Objects
B. a group of Predefined Attack Groups created automatically by Juniper IDP
C. creates a custom grouping of Attack Objects that are not changed during Signature Update
D. creates a custom grouping of attacks, which are automatically updated during Signature Update

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
ActualTests.com

QUESTION 163
What are two ways to verify that your rules in the Security Policies are not being shadowed? (Choose two.)

A. You can verify your security policy from the CLI of the Sensor.
B. You can verify your security policy from the IDP User Interface.
C. IDP Management Server can verify your Security policy automatically from the CLI of the Management Server.
D. You must manually verify your rules by hand to ensure they do not shadow each other.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com 57
Juniper JN0-541: Practice Exam

QUESTION 164
What are two differences between Action and IP Action? (Choose two.)

A. Action responds to matching traffic by dropping, or closing current attacking packets or connection.
B. IP Action responds to matching traffic by dropping, or closing current attacking packets or connection.
C. Action responds to future traffic based on a previous match by blocking or dropping future connections.
D. IP Action responds to future traffic based on a previous match by blocking or closing future connections.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Action deals with immediate attacks and IP Actions deal with future attacks.

QUESTION 165
What is the advantage of defining the Service field in a rule for a specific server?

A. it allows you to permit and deny specific services.
B. It allows you to drop traffic that does not match the service.
C. There is no advantage to defining the Service field in any rule.
D. It makes the rule more efficient, allowing IDP to only match attacks against services that would actually affect that server.
ActualTests.com

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
Which three statements are true about Compound Attack Objects? (Choose three.)

A. The maximum number of objects is limited to 32.
B. All entries must use the same protocol for service binding.
C. You can create custom signatures within the Compound Attack Object.
D. For a Compound Attack Object to match, only one Attack Object must match.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com 58
Juniper JN0-541: Practice Exam

QUESTION 167
Which command from the IDP Sensor CLI can be used to display the sensor statistics, the policy information, and mode of s ensor deployment?

A. sctop -s option
B. scio list s0 sensor stat
C. scio sensor stat
D. sensor statistics can be displayed only from the UI

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
You implement all HTTP Signatures for your Web Server and notice an alert is generated each time a web user accesses the SQL database with the default passwords. Your webmaster does not want to reprogram the page to use valid SQL passwords. How do you disable alerting on this False Positive?

A. create an Exempt rule for any traffic destined to your Web Server, include all HTTP:LOW level attacks; make this a Terminal rule
B. create an Exempt rule for any traffic destined to your Web Server, include only the specific HTTP SQL default password signature
C. create an Exempt rule for any traffic destined to your Web Server, include all HTTP:LOW level attacks
D. create an Exempt rule for any traffic generated by your Webserver, include only the specific HTTP SQL default password signature
ActualTests.com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
What is the function of a Compound Attack Object?

A. looks for multiple occurrences of the same attack
B. combines multiple attacks in a singlerulebase

C. combines multiple attack signatures objects or anomalies objects into a single attack object
D. allows you to take custom actions based on combinations of attacks

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com 59
Juniper JN0-541: Practice Exam

QUESTION 170
Which three actions must be taken prior to deploying an IDP Sensor in a network? (Choose three.)

A. An IP address must be defined on all forwarding interfaces.
B. IDP Sensor must be configured with the ACM and assigned a Management IP address.
C. A Security Policy must be configured for this IDP Sensor.
D. The IDP Sensor object must be configured in the IDP Management Server.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
Which three are Predefined reports? (Choose three.)

A. Top Rules
B. Top Attacks
C. Attacks by User
D. Attacks over Time

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
What best describes Reconnaissance attacks?

A. disabling or corrupting networks, systems, or services with the intent to deny the service to ActualTests.com intended users
B. transmission of ping packets of certain size to crash a remote host
C. unauthorized discovery and mapping of systems, services, or vulnerabilities
D. transmission of TCP SYN requests from a spoofed IP address

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
You can remotely administer the IDP Sensor through _____. (Choose two.)

A. theWebUI ACM over HTTPS
"Pass Any Exam. Any Time." - www.actualtests.com 60
Juniper JN0-541: Practice Exam
B. theWebUI ACM over HTTP
C. a Telnet Console
D. an SSH Console

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
When migrating from Sniffer mode to Inline mode, what three changes need to be made so that the IDP can effectively prevent attacks? (Choose three.)

A. reconnect the IDP Sensors forwarding interfaces appropriately
B. from the ACM, change the IDP Sensor mode from Sniffer to Inline
C. reconfigure management interface IP
D. modify the rule action to drop or close

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
What should you do to build effective security policies?

A. create specific rules for critical servers first, which look for attacks that are relevant to those servers (such as HTTP attacks onWebservers); DO NOT make these rules Terminate Match
B. create specific rules for critical servers first, which look for attacks that are relevant to those servers (such as HTTP attacks onWebservers); make these rules Terminate Match C. create an Any/Any rule to look for all attacks and make this rule#1; DO NOT select Terminate Match
ActualTests.com
C. create an Any/Any rule to look for all attacks and make this rule#1; select Terminate Match

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
Which three statements are true about ESP? (Choose three.)

A. ESP indicates when new hosts or protocols are being used.
B. ESP provides a summary of protocols and contexts on each host.
C. ESP indicates when a specific machine has been attacked.

D. ESP indicates which hosts are talking with each other, and which protocols are being used.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
Which three Profiler tables does ESP use to store data? (Choose three.)

A. Value
B. User
C. Peer
D. Host

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
Which statement is true about exporting a Security Policy?

A. The appearance of the formatting can be changed.
B. The Security Policy can be exported to PDF from the IDP User Interface.
C. The Security Policy can only be printed.
D. The Security Policy can be exported to HTML from the IDP User Interface.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
ActualTests.com
How can you create a quick report?

A. right-click on an entry in the Log Investigator
B. right-click on a predefined report
C. right-click on an entry in the Log Viewer
D. Quick reports are available in the Dashboard only.

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 180
How can you see a "view all ESP events" for Violation Objects?

"Pass Any Exam. Any Time." - www.actualtests.com 62
Juniper JN0-541: Practice Exam

A. You must define a custom filter to view only Violation Objects.
B. You select Violation Objects in the Log Viewer screen.
C. You select the Violation view in the Profiler.
D. Violation Objects are not used in ESP.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
Which IDP Sensor is recommended to support onboard Management Server?

A. IDP-500
B. IDP-1000
C. IDP-100
D. IDP-10

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
What three statements about logging are true? (Choose three.)

A. When the communication is restored between the IDP Sensor and IDP Management Server, the IDP Sensor automatically reports any cached log messages to the Management Server.
B. If the communication between the IDP Sensor and IDP Management Server is down, the IDP Sensor will cache logs locally.
C. When the communication is restored between the IDP Sensor and IDP Management Server, the administrator must manually download the logs.
D. Log messages are forwarded from IDP Sensor to IDP Management Server in real time. ActualTests.com

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
What does the Host Watch List monitor?

A. the number of attacks targeted to specified hosts
B. the number of attacks initiated from specified hosts
C. all sessions directed to specified hosts
D. the status of specified hosts

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
Which three actions can be taken on a rule when deployed in inline mode? (Choose three.)

A. drop connection
B. drop stream
C. drop packet
D. close server and client

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
What is the function of the Log Packets notification action?

A. logs all packets the IDP Sensor sees
B. logs the packets containing the attack only
C. logs the packets used to give notification about a specific event (e.g.Syslog Traffic)
D. logs a specific number of packets before, after and during an attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186
What are two drawbacks of an IDS system blocking an IP address? (Choose two.)

A. might lead to denial-of-service situation where attacker can intentionally block valid users from accessing a network
B. works only on TCP traffic

C. might not block the attacker until the attack has already taken place
D. need to know the sequence number of the attacker's IP Header to successfully block the IP address

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187
What is the process for enabling packet logging?

A. in the notification column of a rule in the mainrulebase, select Enable logging and check "log packets" option
B. in the actions column of arulebase, select "log packets"
C. in the action column of arulebase, select logging and choose "log packets"
D. in the notification column of a rule in the mainrulebase check "log packets" option

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188
How can you monitor real-time IP flows through the IDP Sensor?

A. use the IDP UI Dashboard
B. use the CLI utilitysctop
C. use the IDP UI Traffic Logs
D. enable "debug flow basic" on the IDP Sensor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189
Which three functions can the IDP Sensor perform? (Choose three.)

A. performs attack detection and prevention
B. forwards logs and status messages to the IDP Management Server
C. collects and presents logs to the IDP User Interface
D. store logs locally when the IDP Management Server is unreachable

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
ActualTests.com

QUESTION 190
What are the limitations of using TCP Reset to block connections in an IDS? (Choose three.)

A. only works on TCP traffic
B. must know the correct packet size to successfully reset a connection
C. does not reset the connection until the attack has already taken place
D. resets all connections from a certain source-IP, which could lead to denial-of-service

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com 65
Juniper JN0-541: Practice Exam

QUESTION 191
Which IDP Sensors support High-Availability? (Choose three.)

A. NetScreen IDP-500
B. IDP-10
C. NetScreen IDP-100
D. NetScreen IDP-1000

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
Which two attack detection methods are unique to Juniper NetScreenIDP? (Choose two.)

A. Protocol Anomaly
B. Packet Signatures
C. Statefull Signatures
D. Backdoor Detection

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
What is the function of the IDP User Interface?

A. It downloads logs from various Sensors and displays them to the administrator.
B. It supplements the Command-Line Interface on the Sensor, but is not required.

C. It stores Security Policies and Attack Objects
D. It provides an interface for the administrator to view Logs/Reports and define Security Policies.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
ActualTests.com

QUESTION 194
Which two statements are true about packet logging in NetScreen IDP? (Choose two.)

A. Packet logging on anAny/Any rule is not recommended due to performance impact.
B. Logging all packets before and after the attack can have a performance impact.
C. Packet logging records all packets flowing through the IDP.
D. Packets can be logged only after an attack is matched.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195
Which three statements are true about custom reports? (Choose three.)

A. Creating reports using indexed columns is significantly faster.
B. All custom reports are stored on per user basis.
C. Log filters can be applied to custom reports.
D. You can export custom reports topdf format.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
Which three best describe denial-of-service attacks? (Choose three.)

A. transmission of ping packets of a certain size to crash a remote host
B. the unauthorized discovery and mapping of systems, services, or vulnerabilities
C. transmission of TCP SYN requests from a spoofed IP address to exhaust the resources of a victim
D. disabling or corrupting networks, systems, or services with the intent to deny the service to intended users

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197
What is a Close Server action?

A. drops all packets from the attacker's IP
B. drops any packet matching thissrc/dst/protocol
C. drops only the specific packet matching the attack pattern
D. issues a TCP Reset to the server only

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

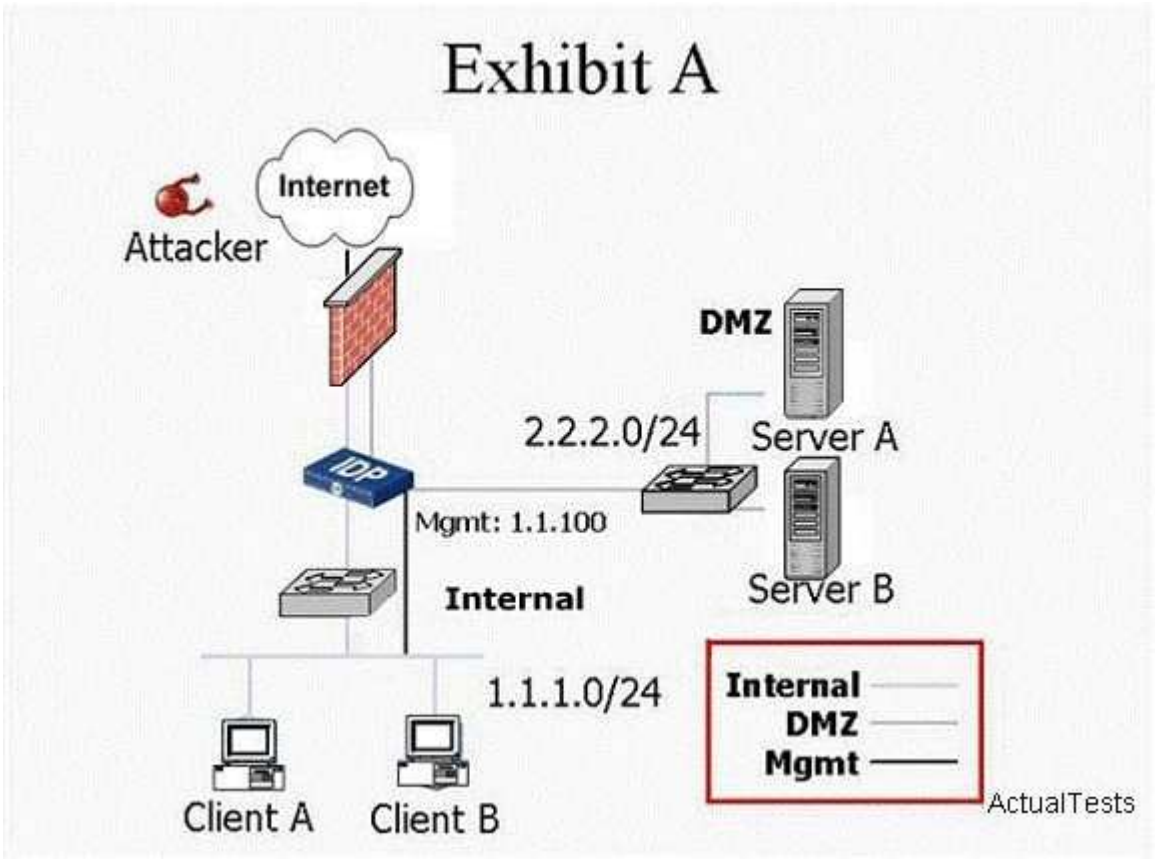
QUESTION 198
Which filters can be applied to reports?

A. Source IP/Port, Destination IP Port, Protocol, Attack, Time
B. Filters cannot be applied to reports.
C. any field in the Log Viewer
D. Source IP, Destination IP and Port, Protocol, Attack, Time

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 199
Exhibit:
You work as an administrator at Certkiller .com. Study the exhibit carefully. In the mode shown in the exhibit, IDP Sensor can protect Server A against attacks being initiated from which three hosts? (Choose three.)
Exhibit:



ActualTests.com

A. Attacker
B. Server B
C. Client B
D. Client A

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
"Pass Any Exam. Any Time." - www.actualtests.com 71
Juniper JN0-541: Practice Exam

QUESTION 200
Log Investigator identified 26 attacks from a specific source to a specific destination. How can you view the details of these 26 attacks?

A. go to the Log Viewer and filter that specific source and destination address
B. right-click on the 26 value, select View by Key
C. go to the Log Investigator and filter that specific source and destination address
D. right-click on the 26 value, select View in Log Viewer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

http://www.gratisexam.com/