Juniper JNCIP-SEC Certification JN0-634 Exam

- **Vendor: Juniper**
- **Exam Code: JN0-634**
- **Exam Name: Juniper Networks Certified Professional Security (JNCIP-SEC)**

QUESTION 1
Which statement about transparent mode on an SRX340 is true?

A. You must reboot the device after configuring transparent mode.
B. Security policies applied to transparent mode zones require Layer 2 address matching.
C. Screens are not supported in transparent mode security zones.
D. All interfaces on the device must be configured with the ethernet-switching protocol family.

Answer: A

QUESTION 2
Referring to the security policy shown in the exhibit, which two actions will happen as the packet is processed? (Choose two.)

```
user@host# show security idp
idp-policy base-policy {
     rulebase-ips {
          rule R1 {
               match {
                    from-zone trust;
                    source-address any;
                    to-zone untrust;
                    destination-address any;
                    application default;
                    attacks {
                         predefined-attack-groups HTTP-Critical;
                    }
               }
               then {
                    action {
                         mark-diffserv {
                              10;
                         }
                    }
               }
          }
     }
}
```

A. It passes unmatched traffic after modifying the DSCP priority.
B. It marks and passes matched traffic with a high DSCP priority.
C. It marks and passes matched traffic with a low DSCP priority.
D. It passes unmatched traffic without modifying DSCP priority.

Answer: BD

QUESTION 3

```
user@host> show ethernet-switching global-information
Global Configuration:

MAC aging interval          : 300
MAC learning                : Enabled
MAC statistics              : Disabled
MAC limit Count             : 65535
MAC limit hit               : Disabled
MAC packet action drop      : Disabled
LE aging time               : 1200
LE VLAN aging time          : 1200
Global Mode                 : Switching
```

Referring to the exhibit, which two statements are true? (Choose two.)

A. You can secure inter-VLAN traffic with a security policy on this device.
B. You can secure intra-VLAN traffic with a security policy on this device.
C. The device can pass Layer 2 and Layer 3 traffic at the same time.
D. The device cannot pass Layer 2 and Layer 3 traffic at the same time.

Answer: AC

QUESTION 4
You are using IDP on your SRX Series device and are asked to ensure that the SRX Series device has the latest IDP database, as well as the latest application signature database. In this scenario, which statement is true?

A. The application signature database cannot be updated on a device with the IDP database installed.
B. You must download each database separately.
C. The IDP database includes the latest application signature database.
D. You must download the application signature database before installing the IDP database.

Answer: C

QUESTION 5

```
[edit security utm]
user@host# show
custom-objects {
     url-pattern {
          allow {
               value "user@example.com";
          }
          reject {
               value "user@example.com";
          }
     }
}
feature-profile {
     anti-spam {
          address-whitelist allow;
          address-blacklist reject;
          sbl {
               profile AS {
                    sbl-default-server;
                    spam-action block;
                    custom-tag-string SPAM;
               }
          }
     }
}
```

Referring to the exhibit, which statement is true?

A. E-mails from the user@example.com address are marked with SPAM in the subject line by the spam block list server.
B. E-mails from the user@example.com address are blocked by the spam list server.
C. E-mails from the user@example.com address are blocked by the reject blacklist.
D. E-mails from the user@example.com address are allowed by the allow whitelist.

Answer: D

QUESTION 6
Your manager has identified that employees are spending too much time posting on a social media site. You are asked to block user from posting on this site, but they should still be able to access any other site on the Internet. In this scenario, which AppSecure feature will accomplish this task?

A. AppQoS
B. AppTrack
C. APpFW
D. APBR

Answer: C

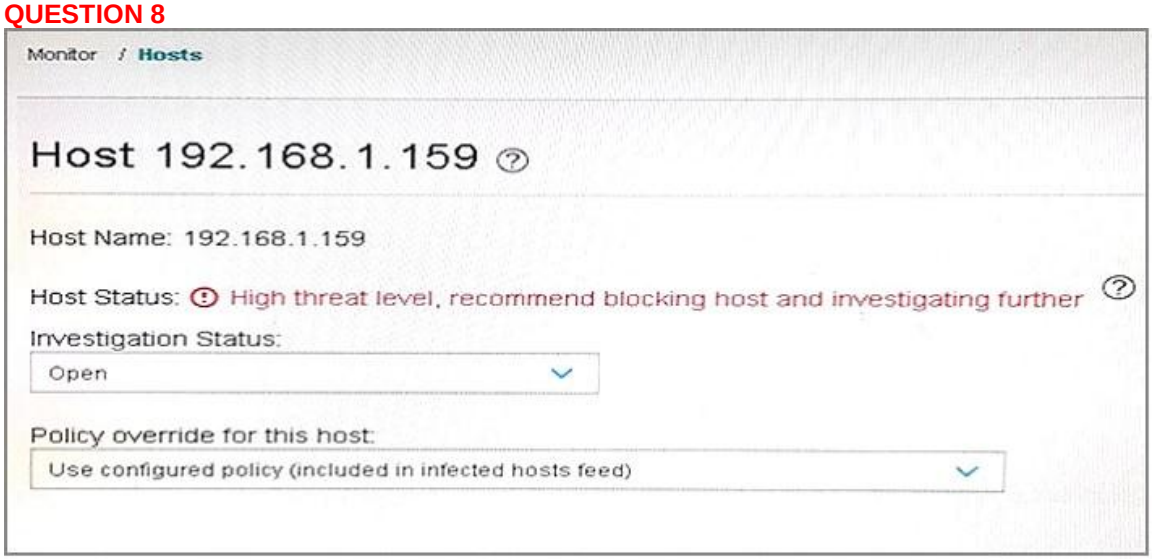
QUESTION 7
While reviewing the Log and Reporting portion of Security Director, you find that multiple objects reference the same address. You want to use a standardized name for all of the objects. In this scenario, how would you create a standardized object name without searching the entire policy?

A. Remove the duplicate objects.

B. Merge the duplicate objects.
C. Rename the duplicate objects.
D. Replace the duplicate objects.

Answer: B

QUESTION 8



Referring to the exhibit, the host has been automatically blocked from communicating on the network because a malicious file was downloaded. You cleaned the infected host and changed the investigation status to Resolved - fixed. What does Sky ATP do if the host then attempts to download a malicious file that would result in a threat score of 10?

A. Sky ATP does not log the connection attempt and an SRX Series device does not allow the host to communicate on the network.
B. Sky ATP logs the connection attempt and an SRX Series device does not allow the host to communicate on the network.
C. Sky ATP logs the connection attempt and an SRX Series device allows the host to communicate on the network.
D. Sky ATP does not log the connection attempt and an SRX Series device allows the host to communicate on the network.

Answer: C

QUESTION 9

You have implemented APBR on your SRX Series device and are verifying that your changes are working properly. You notice that when you start the application for the first time, it does not follow the expected path. What are two reasons that would cause this behavior? (Choose two.)

A. The application system cache does not have an entry for the first session.
B. The application system cache has been disabled.
C. The application system cache already has an entry for this application.
D. The advanced policy-based routing is applied to the ingress zone and must be moved to the egress zone.

Answer: AB

QUESTION 10

Referring to the configuration shown in the exhibit, which statement explains why traffic matching

the IDP signature DNS:OVERFLOW:TOO-LONG-TCP-MSG is not being stopped by the SRX Series device?

A. The security policy dmz-pol1 has an action of permit.
B. The IDP policy idp-pol1 is not configured as active.
C. The IDP rule r2 has an ip-action value of notify.
D. The IDP rule r1 has an action of ignore-connection.

Answer: B

QUESTION 11
Your network includes SRX Series devices at the headquarters location. The SRX Series devices at this location are part of a high available chassis cluster and are configured for IPS. There has been a node failover. In this scenario, which two statements are true? (Choose two.)

A. The IP action table is synchronized between the chassis cluster nodes.
B. Cached SSL session ID information for existing sessions is not synchronized between nodes.
C. The IP action table is not synchronized between the chassis cluster nodes.
D. Cached SSL session ID information for existing session is synchronized between nodes.

Answer: CD

QUESTION 12
What is the correct application mapping sequence when a user goes to Facebook for the first time through an SRX Series device?

A. first packet > process packet > check application system cache > classify application > process packet > match and identify application
B. first packet > check application system cache > process packet > classify application > match and identify application
C. first packet > check application system cache > classify application > process packet > match and identify application
D. first packet > process packet > check application system cache > classify application > match and identify application

Answer: D

QUESTION 13
After downloading the new IPS attack database, the installation of the new database fails. What caused this condition?

A. The new attack database no longer contained an attack entry that was in use.
B. The new attack database was revoked between the time it was downloaded and installed.
C. The new attack database was too large for the device on which it was being installed.
D. Some of the new attack entries were already in use and had to be deactivated before installation.

Answer: A

QUESTION 14
Which interface family is required for Layer 2 transparent mode on SRX Series devices?

A. LLDP

B. Ethernet switching
C. inet
D. VPLS

Answer: B

QUESTION 15
You want to review AppTrack statistics to determine the characteristics of the traffic being monitored. Which operational mode command would accomplish this task on an SRX Series device?

A. show services application-identification statistics applications
B. show services application-identification application detail
C. show security application-tracking counters
D. show services security-intelligence statistics

Answer: A

QUESTION 16
Which Junos security feature is used for signature-based attack prevention?

A. RADIUS
B. AppQoS
C. IPS
D. PIM

Answer: C

QUESTION 17

```
user@host> show security application-firewall rule-set all
Rule-set: demo-tracking_1
     Rule: web-applications
          Dynamic Applications: junos:CNN
          Dynamic Application Groups: junos:social-networking,
          junos:web:advertisments, junos:social-networking:applications,
          junos:web:file-sharing, junos:web:applications, junos:web:gaming
          SSL-Encryption: no
          Action:permit
          Number of sessions matched: 13205
          Number of sessions redirected: 0
Default rule:permit
          Number of sessions matched: 132056
          Number of sessions redirected: 0
Number of sessions with appid pending: 9
```

Referring to the exhibit, which two statements are true? (Choose two.)

A. The application firewall rule is not inspecting encrypted traffic.
B. There are two rules configured in the rule set.
C. The rule set uses application definitions from the predefined library.
D. The configured rule set matches most analyzed applications.

Answer: AC

QUESTION 18

```
policy allow-all {
     match {
          source-address any;
          destination-address any;
          application any;
     }
     then {
          permit {
               application-services {
                    idp;
                    utm-policy wf-policy_websense-home;
                    application-firewall {
                         rule-set demo-tracking_1;
                    }
               }
          }
          log {
               session-init;
               session-close;
          }
     }
}
```

According to the policy shown in the exhibit, which application-services traffic will be processed first?

A. the application traffic matchings the IDP rules
B. the application traffic matchings the utm-policy log rule set
C. the application traffic matchings the utm-policy wf-policy_websense-home rules
D. the application traffic matchings the application-firewall rule-set demo-tracking_1 rule

Answer: A

QUESTION 19
You are using the integrated user firewall feature on an SRX Series device. Which three parameters are stored in the Active Directory authentication table? (Choose three.)

A. IP address
B. MAC address
C. group mapping
D. username
E. password

Answer: ACD

QUESTION 20

```
[edit security policies global policy int-FW]
user@host# show
match {
     source-address any;
     destination-address any;
     application any;
}
then {
     permit;
}

user@host> show security user-identification local-authentication-table all

user@host>
```

You have configured integrated user firewall on the SRX Series devices in your network. However, you noticed that no users can access the servers that are behind the SRX Series devices. Referring to the exhibit, what is the problem?

A. The Kerberos service is not configured correctly on the Active Directory server.
B. There are no authentication entries in the SRX Series device for the users.
C. The security policy on the SRX Series device is configured incorrectly.
D. The SAML service is not configured correctly on the Active Directory server.

Answer: C

QUESTION 21
What are three types of content that are filtered by the Junos UTM feature set? (Choose three.)

A. IMAP
B. HTTP
C. SIP
D. SSL
E. FTP

Answer: ABE

QUESTION 22

```
[edit]
user@host# show security application-tracking
first-update-interval 1;

[edit]
user@host# show security zones security-zone trust
tcp-rst;
host-inbound-traffic {
     system-services {
          all;
     }
}
interfaces {
     ge-0/0/2.0;
}
application-tracking;
```

Referring to the exhibit, how many AppTrack logs will be generated for an HTTP session lasting 12 minutes?

A. 4
B. 2
C. 1
D. 3

Answer: A

QUESTION 23

```
[edit services advanced-anti-malware policy SKY_policy1]
user@host# show
match {
     application HTTP;
     verdict-threshold 6;
}
then {
     action block;
     notification {
          log;
     }
}
inspection-profile Test_Profile;
fallback-options {
     action permit;
     notification {
          log;
     }
}
default-notification {
     log;
}
whitelist-notification {
     log;
}
blacklist-notification {
     log;
}
```

Referring to the exhibit, you have configured a Sky ATP policy to inspect user traffic. However, you have noticed that encrypted traffic is not being inspected. In this scenario, what must you do to solve this issue?

A. Change the policy to inspect HTTPS traffic.
B. Configure the PKI feature.
C. Configure the SSL forward proxy feature.
D. Change the policy to inspect TLS traffic.

Answer: C

QUESTION 24
You have enabled mixed mode on an SRX Series device. You are unable to commit the configuration shown in the exhibit. What is the problem in this scenario?

A. A Layer 3 interface has not been configured on VLAN v10.
B. The trust zone cannot contain both Layer 2 and Layer 3 interfaces.
C. STP is not enabled under the host-inbound-traffic system services hierarchy on the trust and protected security zones.
D. An IRB interface has not been configured.

Answer: B

QUESTION 25
Your network includes SRX Series devices at all headquarter, data center, and branch locations.

The headquarter and data center locations use high-end SRX Series devices, and the branch locations use branch SRX Series devices. You are asked to deploy IPS on the SRX Series devices using one of the available IPS deployment modes. In this scenario, which two statements are true? (Choose two.)

A. Inline tap mode provides enforcement.
B. Inline tap mode can be used at all locations.
C. Integrated mode can be used at all locations.
D. Integrated mode provides enforcement.

Answer: CD

QUESTION 26

```
[edit]
user@host# show interfaces ge-0/0/4
unit 0 {
     family ethernet-switching {
          interface-mode access;
          vlan {
               members SV;
          }
     }
}

[edit]
user@host# show interfaces ge-0/0/5
unit 0 {
     family ethernet-switching {
          interface-mode access;
          vlan {
               members SV;
          }
     }
}

[edit]
user@host# show vlans
SV {
     vlan-id 101;
}

[edit]
user@host# show security forwarding-options
secure-wire {
     access-sw {
          interface [ ge-0/0/4 ge-0/0/5 ];
     }
}

[edit]
user@host# commit
[edit security forwarding-options secure-wire access-sw]
     'interface ge-0/0/4'
          Interface name ge-0/0/4 is not valid
[edit security forwarding-options secure-wire access-sw]
     'interface ge-0/0/4'
          Error: two and only two logical interfaces are required for a
secure-wire
error: configurartion check-out failed
```

You are trying to implement secure wire on your SRX Series device. However, you are receiving the commit error shown in the exhibit. What must you do to solve the problem?

A. Add the correct logical units to the interfaces in the secure wire.
B. Put the ge-0/0/4 and ge-0/0/5 interfaces in separate secure wires.
C. Change the Ethernet switching mode from access to trunk for the ge-0/0/4 and ge-0/0/5 interfaces.
D. Add the ge-0/0/4 and ge-0/0/5 interfaces to the SV VLAN.

Answer: A

QUESTION 27
Which browser is supported by Security Director with Logging and Reporting?

A. Firefox
B. Agora
C. PowerBrowser
D. Mosaic

Answer: A

QUESTION 28
The Software-Defined Secure Networks Policy Enforcer contains which two components? (Choose two.)

A. SRX Series device
B. Sky ATP
C. Policy Controller
D. Feed Connector

Answer: CD

QUESTION 29

```
[edit]
user@host# show interfaces
ge-0/0/3 {
     unit 0 {
          family inet {
               address 10.1.1.1/24;
          }
     }
}
ge-0/0/4 {
     unit 0 {
          family ethernet-switching {
               interface-mode access;
               vlan;
                    members SV;
               }
          }
     }
}
ge-0/0/5 {
     unit 0 {
          family ethernet-switching {
               interface-mode access;
               vlan {
                    members SV;
               }
          }
     }
}
irb {
     unit 0 {
          family inet {
               address 172.20.101.101/24;
          }
     }
}

[edit]
user@host# show vlans
SV {
     vlan-id 101;
     13-interface irb.0;
}

[edit]
user@host# show security zones security-zone L2
interfaces {
     irb.0;
}

[edit]
user@host# show security polciies

[edit]
user@host#

[edit]
user@host# run show ethernet-switching global-information
Global Configuration:

MAC aging interval       : 300
MAC learning             : Enabled
MAC statistics           : Disabled
MAC limit Count          : 65535
MAC limit hit            : Disabled
MAC packet action drop   : Disabled
LE aging time            : 1200
LE VLAN aging time       : 1200
Global Mode              : Transparent bridge
```

Two hosts on the same subnet are connected to an SRX340 using interfaces ge-0/0/4 and ge-0/0/5. The two hosts can communicate with each other, but they cannot communicate with hosts outside of their subnet. Referring to the exhibit, which three actions would you take to solve this problem? (Choose three.)

A. Add the ge-0/0/4 and ge-0/0/5 interfaces to the L2 zone.
B. Remove the irb.0 interface from the L2 zone.
C. Set the SRX340 to Ethernet switching mode.
D. Configure a security policy to permit the traffic.
E. Reboot the SRX340.

Answer: CDE

QUESTION 30
You are creating an IPS policy with multiple rules. You want traffic that matches rule 5 to silently be dropped, along with any future packets that match the appropriate attributes of the incoming traffic. In this scenario, which ip-action parameter should you use?

A. ip-block
B. ip-close
C. log-create
D. timeout

Answer: A

QUESTION 31
You have been notified by your colocation provider that your infrastructure racks will no longer be adjacent to each other. In this scenario, which technology would you use to secure all Layer 2 and Layer 3 traffic between racks?

A. IPsec
B. GRE
C. 802.1BR
D. MACsec

Answer: D

QUESTION 32
Which IDP rule configuration will send an RST to any new session that meets the action criteria?

A. ip-action block
B. action close-client-and-server
C. ip-action close
D. action drop-connection

Answer: C

QUESTION 33
Using content filtering on an SRX Series device, which three types of HTTP content are able to be blocked? (Choose three.)

A. PDF files

B. ZIP files
C. Java applets
D. Active X
E. Flash

Answer: BCD

QUESTION 34
A customer has recently deployed a next-generation firewall, sandboxing software, cloud access security brokers (CASB), and endpoint protection. In this scenario, which tool would provide the customer with additional attack prevention?

A. Junos Space Cross Provisioning Platform
B. Contrail
C. Security Director Policy Enforcer
D. Network Director Inventory Manager

Answer: C

QUESTION 35
After using Security Director to add a new firewall policy rule on an SRX Series device, you notice that the hit count on the policy is not increasing. Upon further investigation, you find that the devices listed in the new rule are able to communicate as expected. Your firewall policy consists of hundreds of rules. Using only Security Director, how do you find the rule that is allowing the communication to occur in this scenario?

A. Generate a Top Firewall Rules report.
B. Generate a Policy Analysis report.
C. Generate a Top Source IPs report.
D. Generate a Top Firewall Events report.

Answer: D

QUESTION 36
To which three UTM components would the custom-objects parameter apply? (Choose three.)

A. Sky ATP
B. antispam
C. content filtering
D. antivirus
E. Web filtering

Answer: BCE

QUESTION 37
SRX Series devices with AppSecure support which three custom signatures? (Choose three.)

A. MAC address-based mapping
B. latency detection mapping
C. IP protocol-based mapping
D. ICMP-based mapping

E. Layer 7-based signatures

Answer: CDE

QUESTION 38

```
[edit security utm]
user@host# show
feature-profile {
     content-filtering {
          profile web-traffic-profile {
               block-content-type {
                    zip;
               }
          }
     }
}
utm-policy utm-web-policy {
     content-filtering {
          http-profile web-traffic-profile;
     }
}
```

The UTM policy shown in the exhibit has been applied to a security policy on a branch SRX Series device. In this scenario, which statement is true?

A. HTTP downloads of ZIP files will be blocked.
B. FTP downloads of ZIP files will be blocked.
C. E-mail downloads of ZIP files will be blocked.
D. ZIP files can be renamed with a new extension to pass through the filter.

Answer: A

QUESTION 39
Which two statements about enabling MACsec using static CAK security mode keys are true? (Choose two.)

A. CAK secures the data plane traffic.
B. SAK secures the data plane traffic.
C. SAK secures the control plane traffic.
D. CAK secures the control plane traffic.

Answer: BD

QUESTION 40
You need to add all of the sites in the domain example.com to urllist2. You decide to use wildcards to account for any changes made to the domain in the future. In this scenario, which two commands would you use to meet this requirement? (Choose two.)

A. set custom-objects url-pattern urllist2 value http://*.example.com
B. set custom-objects url-pattern urllist2 value http://*example.com
C. set custom-objects url-pattern urllist2 value http://*.example.???
D. set custom-objects url-pattern urllist2 value http://*.example.*

Answer: AC

QUESTION 41

```
user@host > show services user-identification authentication-table
authentication-source active-directory
Domain: example
Total enteries: 1
Source IP      Username       groups(Ref by policy)          state
192.168.50.8   user1          grp1                           Initial
```

Which statement explains the current state value of the command output shown in the exhibit?

A. A valid response was received from a domain PC probe, and the user is a valid domain user programmed in the PFE.
B. An invalid response was received from a domain PC probe, and the user is an invalid domain user.
C. A probe event generated an entry in the authentication table, but no probe response has been received from the domain PC.
D. The user-to-address mapping was successfully read from the domain controller event logs, and an entry was added to the authentication table witch currently resides on the Routing Engine.

Answer: A

QUESTION 42
Your network includes SRX Series devices configured with AppSecure. Which two statements regarding the application identification engine are true? (Choose two.)

A. Applications are only matched in traffic flows associated with client-to-server sessions.
B. Applications are matched in traffic flows associated with client-to-server and server-to-client sessions.
C. If the packets entering the engine match a known application, then processing continues.
D. If the packets entering the engine match a known application, then processing stops.

Answer: BD

QUESTION 43
You have recently committed the IPS policy shown in the exhibit. When evaluating the expected behavior, you notice that you have a session that matches all of the rules in your IPS policy. In this scenario, which action would be taken?

A. ignore-connection
B. drop packet
C. no-action
D. close-client-and-server

Answer: C

QUESTION 44
Which two statements about the integrated user firewall feature of the Junos OS are true? (Choose two.)

A. The maximum number of supported active directory servers is ten.
B. IPv6 addresses are not supported.
C. The maximum number of supported active directory servers is five.
D. IPv6 addresses are supported.

Answer: AB

QUESTION 45
Which feature of Sky ATP is deployed with Software-Defined Secure Networks?

A. zero-day threat mitigation
B. software image snapshot support
C. device inventory management
D. service redundancy daemon configuration support

Answer: A

QUESTION 46

```
user@host# show security advance-policy-based-routing
profile profile1 {
     rule rule-app1 {
          match {
               dynamic-application junos:HTTP;
          }
          then {
               routing-instance R1;
          }
     }
     rule rule-app2 {
          match {
               dynamic-application junos:junos:web:social-networking;
          }
          then {
               routing-instance R2;
          }
     }
     rule rule-app3 {
          match {
               dynamic-application junos:YAHOO;
          }
          then {
               routing-instance R3;
          }
     }
}
```

Your organization requests that you direct Facebook traffic out a different link to ensure that the bandwidth for critical applications is protected. Referring to the exhibit, which forwarding instance will be used on your SRX Series device?

A. R3
B. R1
C. R2
D. inet.0

Answer: C

QUESTION 47

You have configured a log collector VM and Security Director. System logging is enabled on a branch SRX Series device, but security logs do not appear in the monitor charts. How would you solve this problem?

A. Configure a security policy to forward logs to the collector.
B. Configure application identification on the SRX Series device.
C. Configure security logging on the SRX Series device.
D. Configure J-Flow on the SRX Series device.

Answer: C

QUESTION 48
You have set up Sky ATP with the SRX Series devices in your network. However, your SRX Series devices are unable to communicate with the Sky ATP cloud because the communication is being blocked by a gateway network device. Which two actions should you take to solve the problem? (Choose two.)

A. Open destination port 443 inbound from the Internet on the gateway network device.
B. Open destination port 8080 outbound from the Internet on the gateway network device.
C. Open destination port 443 outbound from the Internet on the gateway network device.
D. Open destination port 8080 inbound from the Internet on the gateway network device.

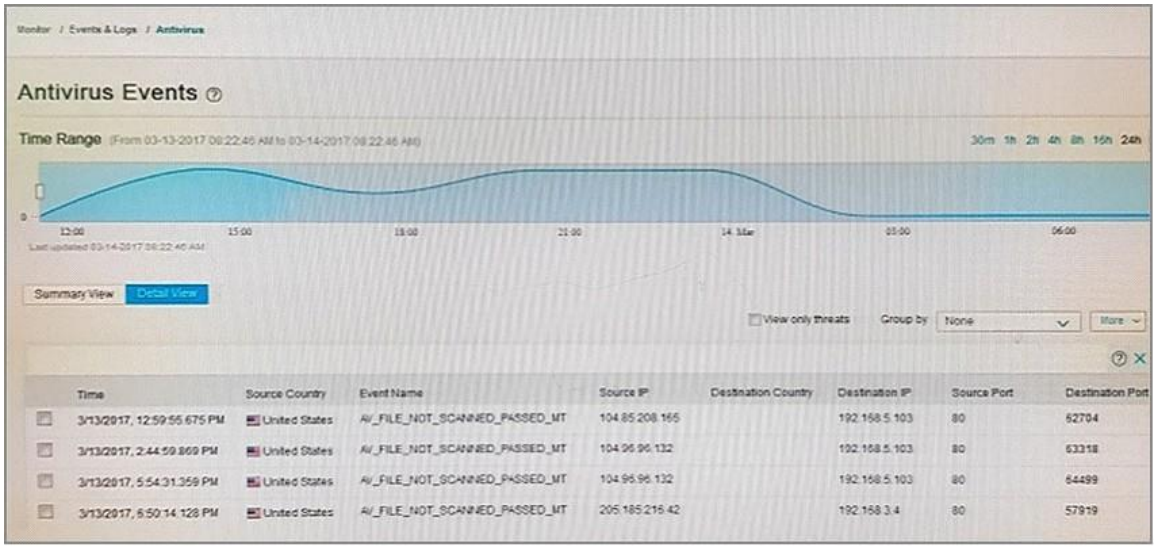
Answer: CD

QUESTION 49
Your network includes SRX Series devices at the headquarters location. The SRX Series devices at this location are part of a high availability chassis cluster and are expected to support several UTM features. Which two statements related to this environment are true? (Choose two.)

A. UTM features can be configured on either of the nodes within the cluster.
B. The chassis cluster must be configured for active/active mode.
C. UTM features must be configured on the primary node within the cluster.
D. The chassis cluster must be configured for active/backup mode.

Answer: AD

QUESTION 50



Security Director is reporting the events shown in the exhibit. If the fallback parameter is set to pass traffic, what would cause the events?

A. The files are too large for the antivirus engine to process.
B. The files are not scanned because they were permitted by a security policy.
C. The files are not scanned because they are the wrong file format.
D. The antivirus engine is unable to re-encrypt the files.

Answer: A

QUESTION 51
Your network includes SRX Series devices at the headquarters location. The SRX Series devices at this location are part of a high availability chassis cluster and are configured for IPS. There has been a node failover. In this scenario, which statement is true?

A. Existing sessions continue to be processed by IPS because of table synchronization.
B. Existing sessions are no longer processed by IPS and become firewall sessions.
C. Existing session continue to be processed by IPS as long as GRES is configured.
D. Existing sessions are dropped and must be reestablished so IPS processing can occur.

Answer: A

QUESTION 52
What are three components of Software-Defined Secure Networks? (Choose three.)

A. ContrailB. Sky ATP
B. SRX Series device
C. Security Director
D. Network Director

Answer: BCD

QUESTION 53
Which AppSecure feature identifies applications that are present in traffic?

A. AppID
B. AppTrack
C. AppFW
D. AppQoS

Answer: A

QUESTION 54
Which three components are part of the AppSecure services suite? (Choose three.)

A. IDP
B. Sky ATP
C. AppQoS
D. AppFW
E. Web filtering

Answer: ACD

QUESTION 55
What is a function of UTM?

A. AppFW
B. IPsec
C. content filtering
D. bridge mode

Answer: C

QUESTION 56

```
[edit security idp]
user@host# show
idp-policy example-idp-policy {
     rulebase-ips {
          rule r1 {
               match {
                    source-address 10.1.0.0/146;
                    attacks {
                         predefined-attack-groups "HTTP - All";
                    }
               }
               then {
                    action {
                         no-action;
                    }
                    notification {
                         log-attacks;
                    }
               }
          }
          rule r2 {
               match {
                    source-address 10.1.1.85/32;
                    attacks {
                         predefined-attack-groups "HTTP - All";
                    }
               }
               then {
                    action {
                         mark-diffserv {
                              8;
                         }
                    }
               }
          }
          rule r3 {
               match {
                    source-address 10.0.0.0/8;
                    attacks {
                         predefined-attack-groups "HTTP - All";
                    }
               }
               then {
                    action {
                         drop-connection;
                    }
               }
          }
          rule r4 {
               match {
                    source-address any;
                    attacks {
                         predefined-attack-groups "HTTP - All";
                    }
               }
               then {
                    action {
                         close-client-and-server;
                    }
               }
          }
     }
}
```

Referring to the exhibit, a user with IP address 10.1.1.85 generates a request that triggers the HTTP:EXT:DOT-LNK IDP signature that is a member of the "HTTP - All" predefined attack group. In this scenario, which statement is true?

A. The session will be closed and a reset sent to the client and server.
B. A Differentiated Services code point value of 8 will be applied.
C. No action will be taken and the attack information will be logged.
D. The session will be dropped with no reset sent to the client or server.

Answer: D

QUESTION 57
Which two parameters are required to match in an IDP rule for the terminal option to take effect? (Choose two.)

A. attacks custom-attacks
B. attacks predefined-attacks
C. application
D. source-address

Answer: .....