

100% Money Back
Guarantee

Vendor:Juniper

Exam Code:JN0-634

Exam Name:Security, Professional (JNCIP-SEC)

Version:Demo

QUESTION 1

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

- A. LLDP
- B. Ethernet switching
- C. inet
- D. VPLS

Correct Answer: B

QUESTION 2

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

Correct Answer: A

QUESTION 3

Click the Exhibit button.

```
[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.

Correct Answer: D

QUESTION 4

Click the Exhibit button.

```
user@host > show services user-identification authentication-table
authentication-source active-directory
Domain: example
Total entries: 1
Source IP      Username      groups (Ref by policy)      state
192.168.50.8  user1         grpl                         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 which currently resides on the Routing Engine.

Correct Answer: A

QUESTION 5

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

Correct Answer: ABE

QUESTION 6

Click the Exhibit button.

```
<12>1 2016-02-18T01:32:50.391Z utm-srx550-b RT_UTM - WEBFILTER_URL_BLOCKED
[junos@2636.1.1.1.2.86 source-address="192.0.2.3" source-port="32056"
destination-address="198.51.100.2" destination-port="80" category="cat1"
reason="BY_BLACK_LIST" profile="uf1" url="www.example.com" obj="/"
username="N/A" roles="N/A] WebFilter: ACTION="URL Blocked" 192.0.2.3(32056)-
>198.51.100.2(80) CATEGORY="cat1" REASON="BY_BLACK_LIST" PROFILE="uf1"
URL=www.example.com OBJ=/ username N/A roles N/A
```

A customer submits a service ticket complaining that access to <http://www.example.com/> has been blocked.

Referring to the log message shown in the exhibit, why was access blocked?

- A. All illegal source port was utilized.
- B. The URI matched a profile entry.
- C. The user/role permissions were exceeded.
- D. There was a website category infraction.

Correct Answer: B

QUESTION 7

Click the Exhibit button.

```

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

Correct Answer: A

QUESTION 8

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

- A. Sky ATP
- B. antispan
- C. content filtering

D. antivirus

E. Web filtering

Correct Answer: BCE

QUESTION 9

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.

Correct Answer: CD

QUESTION 10

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

Correct Answer: D

QUESTION 11

Click the Exhibit button.

```

user@host# show interfaces
ge-0/0/0 {
  unit 0 {
    family inet {
      dhcp-client;
    }
  }
}
ge-0/0/1 {
  unit 0 {
    family inet {
      address 192.168.161.154/24;
    }
  }
}
ge-0/0/2 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members v10;
      }
    }
  }
}
ge-0/0/3 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members v10;
      }
    }
  }
}
fxp0 {
  unit 0 {
    family inet {
      dhcp-client;
    }
  }
}

```

```

user@host# show security zones

```

```

security-zone trust {
  tcp-rst;
  host-inbound-traffic {
    system-services {
      all;
    }
    protocols {
      all;
    }
  }
  interfaces {
    ge-0/0/1.0;
    ge-0/0/2.0;
  }
}
security-zone untrust {
  screen untrust-screen;
  host-inbound-traffic {
    system-services {
      dhcp;
      ping;
      ssh;
      ike;
    }
  }
  interfaces {
    ge-0/0/0.0;
  }
}
security-zone protected {
  host-inbound-traffic {
    system-services {
      dhcp;
      ping;
      ssh;
      ike;
    }
  }
  interfaces {
    ge-0/0/3.0;
  }
}

```

```

user@host# show vlans

```

```

v10 {
  vlan-id 10;
}

```


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.

Correct Answer: B

QUESTION 12

You are implementing user authentication on your network using an SRX Series device and want to ensure that there are redundant forms of authentication for users to access the network. You have configured the device with the integrated user firewall and user role firewall features. You are testing failover methods using the default priority values.

In this scenario, which two statements are true? (Choose two.)

- A. If the user fails local authentication, then the Junos OS will attempt to authenticate the user with a user role firewall.
- B. If the user fails user role firewall authentication, then the Junos OS will attempt to authenticate the user with an integrated user firewall.
- C. If the user fails integrated user firewall authentication, then the Junos OS will attempt to authenticate with a user role firewall.
- D. If the user fails local authentication, then the Junos OS will attempt to authenticate the user with an integrated user firewall.

Correct Answer: CD