

Topic 1 - Exam A**Question #1***Topic 1*

Which two criteria should a zone-based security policy include? (Choose two.)

- A. a source port
- B. a destination port
- C. zone context
- D. an action

Question #2*Topic 1*

You are assigned a project to configure SRX Series devices to allow connections to your web servers. The web servers have a private IP address, and the packets must use NAT to be accessible from the Internet. You do not want the web servers to initiate connections with external update servers on the Internet using the same IP address as customers use to access them.

Which two NAT types must be used to complete this project? (Choose two.)

- A. static NAT
- B. hairpin NAT
- C. destination NAT
- D. source NAT

Question #3*Topic 1*

You are asked to verify that a license for AppSecure is installed on an SRX Series device. In this scenario, which command will provide you with the required information?

- A. user@srx> show system license
- B. user@srx> show services accounting
- C. user@srx> show configuration system
- D. user@srx> show chassis firmware

Click the Exhibit button.

```
[edit security policies]
user@vSRX-1# edit from-zone trust to-zone dmz policy Trust-DMZ-Access
[edit security policies from-zone trust to-zone dmz policy Trust-DMZ-Access]
user@vSRX-1# exit
```

Referring to the exhibit, a user is placed in which hierarchy when the exit command is run?

- A. [edit security policies from-zone trust to-zone dmz]
user@vSRX-1#
- B. [edit]
user@vSRX-1#
- C. [edit security policies]
user@vSRX-1#
- D. user@vSRX-1>

You want to enable the minimum Juniper ATP services on a branch SRX Series device. In this scenario, what are two requirements to accomplish this task? (Choose two.)

- A. Install a basic Juniper ATP license on the branch device.
- B. Configure the juniper-atp user account on the branch device.
- C. Register for a Juniper ATP account on <https://sky.junipersecurity.net>.
- D. Execute the Juniper ATP script on the branch device.

SRX Series devices have a maximum of how many rollback configurations?

- A. 40
- B. 60
- C. 50
- D. 10

Unified threat management (UTM) inspects traffic from which three protocols? (Choose three.)

- A. FTP
- B. SMTP
- C. SNMP
- D. HTTP
- E. SSH

When are Unified Threat Management services performed in a packet flow?

- A. before security policies are evaluated
- B. as the packet enters an SRX Series device
- C. only during the first path process
- D. after network address translation

When configuring antispam, where do you apply any local lists that are configured?

- A. custom objects
- B. advanced security policy
- C. antispam feature-profile
- D. antispam UTM policy

Screens on an SRX Series device protect against which two types of threats? (Choose two.)

- A. IP spoofing
- B. ICMP flooding
- C. zero-day outbreaks
- D. malicious e-mail attachments

Which statement about global NAT address persistence is correct?

- A. The same IP address from a source NAT pool will be assigned for all sessions from a given host.
- B. The same IP address from a source NAT pool is not guaranteed to be assigned for all sessions from a given host.
- C. The same IP address from a destination NAT pool will be assigned for all sessions for a given host.
- D. The same IP address from a destination NAT pool is not guaranteed to be assigned for all sessions for a given host.

You are asked to configure your SRX Series device to block all traffic from certain countries. The solution must be automatically updated as IP prefixes become allocated to those certain countries.

Which Juniper ATP solution will accomplish this task?

- A. Geo IP
- B. unified security policies
- C. IDP
- D. C&C feed

Which two statements are correct about IKE security associations? (Choose two.)

- A. IKE security associations are established during IKE Phase 1 negotiations.
- B. IKE security associations are unidirectional.
- C. IKE security associations are established during IKE Phase 2 negotiations.
- D. IKE security associations are bidirectional.

You want to deploy a NAT solution.

In this scenario, which solution would provide a static translation without PAT?

- A. interface-based source NAT
- B. pool-based NAT with address shifting
- C. pool-based NAT with PAT
- D. pool-based NAT without PAT

Which Juniper Networks solution uses static and dynamic analysis to search for day-zero malware threats?

- A. firewall filters
- B. UTM
- C. Juniper ATP Cloud
- D. IPS

You are configuring an SRX Series device. You have a set of servers inside your private network that need one-to-one mappings to public IP addresses.

Which NAT configuration is appropriate in this scenario?

- A. source NAT with PAT
- B. destination NAT
- C. NAT-T
- D. static NAT

You want to provide remote access to an internal development environment for 10 remote developers.

Which two components are required to implement Juniper Secure Connect to satisfy this requirement? (Choose two.)

- A. an additional license for an SRX Series device
- B. Juniper Secure Connect client software
- C. an SRX Series device with an SPC3 services card
- D. Marvis virtual network assistant

You are deploying an SRX Series firewall with multiple NAT scenarios.

In this situation, which NAT scenario takes priority?

- A. interface NAT
- B. source NAT
- C. static NAT
- D. destination NAT

Your ISP gives you an IP address of 203.0.113.0/27 and informs you that your default gateway is 203.0.113.1. You configure destination NAT to your internal server, but the requests sent to the webserver at 203.0.113.5 are not arriving at the server.

In this scenario, which two configuration features need to be added? (Choose two.)

- A. firewall filter
- B. security policy
- C. proxy-ARP
- D. UTM policy

Click the Exhibit button.

```
user@vSRX-VR> ping 10.10.102.10 count 5 routing-instance DMZ
PING 10.10.102.10 (10.10.102.10): 56 data bytes
64 bytes from 10.10.102.10: icmp_seq=0 ttl=64 time=0.037 ms
64 bytes from 10.10.102.10: icmp_seq=1 ttl=64 time=0.045 ms
64 bytes from 10.10.102.10: icmp_seq=2 ttl=64 time=0.054 ms
64 bytes from 10.10.102.10: icmp_seq=3 ttl=64 time=0.047 ms
64 bytes from 10.10.102.10: icmp_seq=4 ttl=64 time=0.070 ms
--- 10.10.102.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.037/0.051/0.070/0.011 ms
user@vSRX-VR>
```

Referring to the exhibit, which two statements are correct about the ping command? (Choose two.)

- A. The DMZ routing-instance is the source.
- B. The 10.10.102.10 IP address is the source.
- C. The 10.10.102.10 IP address is the destination.
- D. The DMZ routing-instance is the destination.

Which IPsec protocol is used to encrypt the data payload?

- A. ESP
- B. IKE
- C. AH
- D. TCP

What are three primary match criteria used in a Junos security policy? (Choose three.)

- A. application
- B. source address
- C. source port
- D. class
- E. destination address

You have an FTP server and a webserver on the inside of your network that you want to make available to users outside of the network. You are allocated a single public IP address.

In this scenario, which two NAT elements should you configure? (Choose two.)

- A. destination NAT
- B. NAT pool
- C. source NAT
- D. static NAT

Which three Web filtering deployment actions are supported by Junos? (Choose three.)

- A. Use IPS.
- B. Use local lists.
- C. Use remote lists.
- D. Use Websense Redirect.
- E. Use Juniper Enhanced Web Filtering.

Which two IPsec hashing algorithms are supported on an SRX Series device? (Choose two.)

- A. SHA-1
- B. SHAKE128
- C. MD5
- D. RIPEMD-256

Click the Exhibit button.

```
[edit]
user@SRX# show security zones
security-zone Internal {
  host-inbound-traffic {
    system-services {
      http {
        except;
      }
      all;
    }
  }
  interfaces {
    ge-0/0/1.0;
  }
}
```

What is the purpose of the host-inbound-traffic configuration shown in the exhibit?

- A. to permit host inbound HTTP traffic and deny all other traffic on the internal security zone
- B. to deny and log all host inbound traffic on the internal security zone, except for HTTP traffic
- C. to permit all host inbound traffic on the internal security zone, but deny HTTP traffic
- D. to permit host inbound HTTP traffic on the internal security zone

When operating in packet mode, which two services are available on the SRX Series device? (Choose two.)

- A. MPLS
- B. UTM
- C. CoS
- D. IDP

Which two statements are correct about the default behavior on SRX Series devices? (Choose two.)

- A. The SRX Series device is in flow mode.
- B. The SRX Series device supports stateless firewalls filters.
- C. The SRX Series device is in packet mode.
- D. The SRX Series device does not support stateless firewall filters.

Which two statements are correct about functional zones? (Choose two.)

- A. Functional zones must have a user-defined name.
- B. Functional zone cannot be referenced in security policies or pass transit traffic.
- C. Multiple types of functional zones can be defined by the user.
- D. Functional zones are used for out-of-band device management.

What must be enabled on an SRX Series device for the reporting engine to create reports?

- A. packet capture
- B. security logging
- C. system logging
- D. SNMP

You are assigned a project to configure SRX Series devices to allow connections to your web servers. The web servers have a private IP address, and the packets must use NAT to be accessible from the Internet. The web servers must use the same address for both connections from the Internet and communication with update servers.

Which NAT type must be used to complete this project?

- A. source NAT
- B. destination NAT
- C. static NAT
- D. hairpin NAT

Which two user authentication methods are supported when using a Juniper Secure Connect VPN? (Choose two.)

- A. certificate-based
- B. multi-factor authentication
- C. local authentication
- D. active directory

Click the Exhibit button.

```

policies {
  from-zone untrust to-zone trust {
    policy permit-all {
      [...]
      then {
        permit;
      }
    }
    policy deny-all {
      [...]
      then {
        deny;
      }
    }
    policy reject-all {
      [...]
      then {
        reject;
      }
    }
  }
}

```

Which two statements are correct about the partial policies shown in the exhibit? (Choose two.)

- A. UDP traffic matched by the deny-all policy will be silently dropped.
- B. TCP traffic matched by the reject-all policy will have a TCP RST sent.
- C. TCP traffic matched from the zone trust is allowed by the permit-all policy.
- D. UDP traffic matched by the reject-all policy will be silently dropped.

You are monitoring an SRX Series device that has the factory-default configuration applied.
In this scenario, where are log messages sent by default?

- A. Junos Space Log Director
- B. Junos Space Security Director
- C. to a local syslog server on the management network
- D. to a local log file named messages

When transit traffic matches a security policy, which three actions are available? (Choose three.)

- A. Allow
- B. Discard
- C. Deny
- D. Reject
- E. Permit

Which two services does Juniper Connected Security provide? (Choose two.)

- A. protection against zero-day threats
- B. IPsec VPNs
- C. Layer 2 VPN tunnels
- D. inline malware blocking

You are creating Ipsec connections.

In this scenario, which two statements are correct about proxy IDs? (Choose two.)

- A. Proxy IDs are used to configure traffic selectors.
- B. Proxy IDs are optional for Phase 2 session establishment.
- C. Proxy IDs must match for Phase 2 session establishment.
- D. Proxy IDs default to 0.0.0.0/0 for policy-based VPNs.

Which two components are configured for host inbound traffic? (Choose two.)

- A. zone
- B. logical interface
- C. physical interface
- D. routing instance

Which two security features inspect traffic at Layer 7? (Choose two.)

- A. IPS/IDP
- B. security zones
- C. application firewall
- D. integrated user firewall

Which two UTM features should be used for tracking productivity and corporate user behavior? (Choose two.)

- A. the content filtering UTM feature
- B. the antivirus UTM feature
- C. the Web filtering UTM feature
- D. the antispam UTM feature

What is the order in which malware is detected and analyzed?

- A. antivirus scanning -> cache lookup -> dynamic analysis -> static analysis
- B. cache lookup -> antivirus scanning -> static analysis -> dynamic analysis
- C. antivirus scanning -> cache lookup -> static analysis -> dynamic analysis
- D. cache lookup -> static analysis -> dynamic analysis -> antivirus scanning

What are two valid address books? (Choose two.)

- A. 66.129.239.128/25
- B. 66.129.239.154/24
- C. 66.129.239.0/24
- D. 66.129.239.50/25

What is the order of the first path packet processing when a packet enters a device?

- A. security policies -> screens -> zones
- B. screens -> security policies -> zones
- C. screens -> zones -> security policies
- D. security policies -> zones -> screens

Which two components are part of a security zone? (Choose two.)

- A. inet.0
- B. fxp0
- C. address book
- D. ge-0/0/0.0

Which statement is correct about packet mode processing?

- A. Packet mode enables session-based processing of incoming packets.
- B. Packet mode works with NAT, VPNs, UTM, IDP, and other advanced security services.
- C. Packet mode bypasses the flow module.
- D. Packet mode is the basis for stateful processing.

Which two traffic types are considered exception traffic and require some form of special handling by the PFE? (Choose two.)

- A. SSH sessions
- B. ICMP reply messages
- C. HTTP sessions
- D. traceroute packets

What is the correct order in which interface names should be identified?

- A. system slot number -> interface media type -> port number -> line card slot number
- B. system slot number -> port number -> interface media type -> line card slot number
- C. interface media type -> system slot number -> line card slot number -> port number
- D. interface media type -> port number -> system slot number -> line card slot number

What are two characteristics of a null zone? (Choose two.)

- A. The null zone is configured by the super user.
- B. By default, all unassigned interfaces are placed in the null zone.
- C. All ingress and egress traffic on an interface in a null zone is permitted.
- D. When an interface is deleted from a zone, it is assigned back to the null zone.

Which two statements are correct about screens? (Choose two.)

- A. Screens process inbound packets.
- B. Screens are processed on the routing engine.
- C. Screens process outbound packets.
- D. Screens are processed on the flow module.

Which statement about NAT is correct?

- A. Destination NAT takes precedence over static NAT.
- B. Source NAT is processed before security policy lookup.
- C. Static NAT is processed after forwarding lookup.
- D. Static NAT takes precedence over destination NAT.

Which statement is correct about global security policies on SRX Series devices?

- A. The to-zone any command configures a global policy.
- B. The from-zone any command configures a global policy.
- C. Global policies are always evaluated first.
- D. Global policies can include zone context.

What information does the show chassis routing-engine command provide?

- A. chassis serial number
- B. resource utilization
- C. system version
- D. routing tables

Corporate security requests that you implement a policy to block all POP3 traffic from traversing the Internet firewall.

In this scenario, which security feature would you use to satisfy this request?

- A. antivirus
- B. Web filtering
- C. content filtering
- D. antispam

Which statement is correct about unified security policies on an SRX Series device?

- A. A zone-based policy is always evaluated first.
- B. The most restrictive policy is applied regardless of the policy level.
- C. A global policy is always evaluated first.
- D. The first policy rule is applied regardless of the policy level.

Click the Exhibit button.

```
[edit security policies]
user@SRX# show
from-zone trust to-zone untrust {
  policy Rule-1 {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      deny;
    }
  }
  policy Rule-2 {
    match {
      source-address any;
      destination-address any;
      application [ junos-ping junos-ssh ];
    }
    then {
      permit;
    }
  }
}
```

You are asked to allow only ping and SSH access to the security policies shown in the exhibit.

Which statement will accomplish this task?

- A. Rename policy Rule-2 to policy Rule-0.
- B. Insert policy Rule-2 before policy Rule-1.
- C. Replace application any with application [junos-ping junos-ssh] in policy Rule-1.
- D. Rename policy Rule-1 to policy Rule-3.

What are two features of the Juniper ATP Cloud service? (Choose two.)

- A. sandbox
- B. malware detection
- C. EX Series device integration
- D. honeypot

You want to prevent other users from modifying or discarding your changes while you are also editing the configuration file.

In this scenario, which command would accomplish this task?

- A. configure master
- B. cli privileged
- C. configure exclusive
- D. configure

Which order is correct for Junos security devices that examine policies for transit traffic?

- A. 1. zone policies
2. global policies
3. default policies
- B. 1. default policies
2. zone policies
3. global policies
- C. 1. default policies
2. global policies
3. zone policies
- D. 1. global policies
2. zone policies
3. default policies

What is an IP addressing requirement for an IPsec VPN using main mode?

- A. One peer must have dynamic IP addressing.
- B. One peer must have static IP addressing.
- C. Both peers must have dynamic IP addresses.
- D. Both peers must have static IP addressing.

What does the number "2" indicate in interface ge-0/1/2?

- A. the physical interface card (PIC)
- B. the flexible PIC concentrator (FPC)
- C. the interface logical number
- D. the port number

Which Juniper ATP feed provides a dynamic list of known botnet servers and known sources of malware downloads?

- A. infected host cloud feed
- B. Geo IP feed
- C. C&C cloud feed
- D. blacklist feed

Which two IKE Phase 1 configuration options must match on both peers to successfully establish a tunnel? (Choose two.)

- A. VPN name
- B. gateway interfaces
- C. IKE mode
- D. Diffie-Hellman group

What are three Junos UTM features? (Choose three.)

- A. screens
- B. antivirus
- C. Web filtering
- D. IDP/IPS
- E. content filtering

You are investigating a communication problem between two hosts and have opened a session on the SRX Series device closest to one of the hosts and entered the show security flow session command.

What information will this command provide? (Choose two.)

- A. The total active time of the session.
- B. The end-to-end data path that the packets are taking.
- C. The IP address of the host that initiates the session.
- D. The security policy name that is controlling the session.

A security zone is configured with the source IP address 192.168.0.12/255.255.0.255 wildcard match.

In this scenario, which two IP packets will match the criteria? (Choose two.)

- A. 192.168.1.21
- B. 192.168.0.1
- C. 192.168.1.12
- D. 192.168.22.12

Which statement about service objects is correct?

- A. All applications are predefined by Junos.
- B. All applications are custom defined by the administrator.
- C. All applications are either custom or Junos defined.
- D. All applications in service objects are not available on the vSRX Series device.

You want to block executable files (*.exe) from being downloaded onto your network.

Which UTM feature would you use in this scenario?

- A. IPS
- B. Web filtering
- C. content filtering
- D. antivirus

What are two Juniper ATP Cloud feed analysis components? (Choose two.)

- A. IDP signature feed
- B. C&C cloud feed
- C. infected host cloud feed
- D. US CERT threat feed

Which two statements are correct about global policies? (Choose two.)

- A. Global policies are evaluated after default policies.
- B. Global policies do not have to reference zone context.
- C. Global policies are evaluated before default policies.
- D. Global policies must reference zone contexts.

Which statement is correct about Web filtering?

- A. The Juniper Enhanced Web Filtering solution requires a locally managed server.
- B. The decision to permit or deny is based on the body content of an HTTP packet.
- C. The decision to permit or deny is based on the category to which a URL belongs.
- D. The client can receive an e-mail notification when traffic is blocked.

You have configured a UTM feature profile.

Which two additional configuration steps are required for your UTM feature profile to take effect? (Choose two.)

- A. Associate the UTM policy with an address book.
- B. Associate the UTM policy with a firewall filter.
- C. Associate the UTM policy with a security policy.
- D. Associate the UTM feature profile with a UTM policy.

You want to verify the peer before IPsec tunnel establishment.

What would be used as a final check in this scenario?

- A. traffic selector
- B. perfect forward secrecy
- C. st0 interfaces
- D. proxy ID

Which feature would you use to protect clients connected to an SRX Series device from a SYN flood attack?

- A. security policy
- B. host inbound traffic
- C. application layer gateway
- D. screen option