JN0-637 Q&As

Security - Professional (JNCIP-SEC)

Pass Juniper JN0-637 Exam with 100% Guarantee

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

https://www.leads4pass.com/jn0-637.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

In a multinode HA environment, which service must be configured to synchronize between nodes?

A. Advanced policy-based routing

B. PKI certificates

C. IPsec VPN

D. IDP

Correct Answer: D

Intrusion Detection and Prevention (IDP) services require synchronization between nodes in a multinode HA setup to maintain consistent attack detection and prevention across the network. This ensures seamless failover and accurate threat

mitigation. For more information, see Juniper IDP HA Configuration Guide.

In a multinode HA environment, IDP (Intrusion Detection and Prevention) services must be synchronized between nodes to ensure that the same threat detection and prevention rules are consistently applied across both nodes in the HA

cluster. When IDP is used, the state and configuration of IDP signatures and actions need to be synchronized to ensure that failover or switchover between nodes does not cause discrepancies in security policies and inspection. IDP

Synchronization: The synchronization ensures that both nodes are consistently analyzing traffic for threats and applying the same intrusion prevention mechanisms. If this service is not synchronized, the secondary node might fail to detect

threats after a failover.

Juniper References:

Juniper IDP Synchronization: Explains the importance of synchronizing IDP services across HA nodes to maintain consistent security posture across both devices.

QUESTION 2

You are asked to see if your persistent NAT binding table is exhausted.

Which show command would you use to accomplish this task?

A. show security nat source persistent-nat-table summary

B. show security nat source summary

C. show security nat source pool all

D. show security nat source persistent-nat-table all

Correct Answer: D

The command show security nat source persistent-nat-table all provides a comprehensive view of all entries in the persistent NAT table, enabling administrators to monitor and manage resource exhaustion. Refer to Juniper NAT Monitoring

Guide for more.

In Junos OS, when persistent NAT is configured, a binding table is created to keep track of NAT sessions and ensure that specific hosts are allowed to initiate sessions back to internal hosts. To check if the persistent NAT binding table is full

or exhausted, the correct command must display theentire table.

Correct Command (D):

The command show security nat source persistent-nat-table all will display the entire persistent NAT binding table. This allows you to check whether the table is exhausted or if there is space available for new persistent NAT sessions.

Incorrect Options:

Option A: The command show security nat source persistent-nat-table summary provides a summary view but does not give detailed insights into whether the table is exhausted. Option Band Option C : These commands deal with general

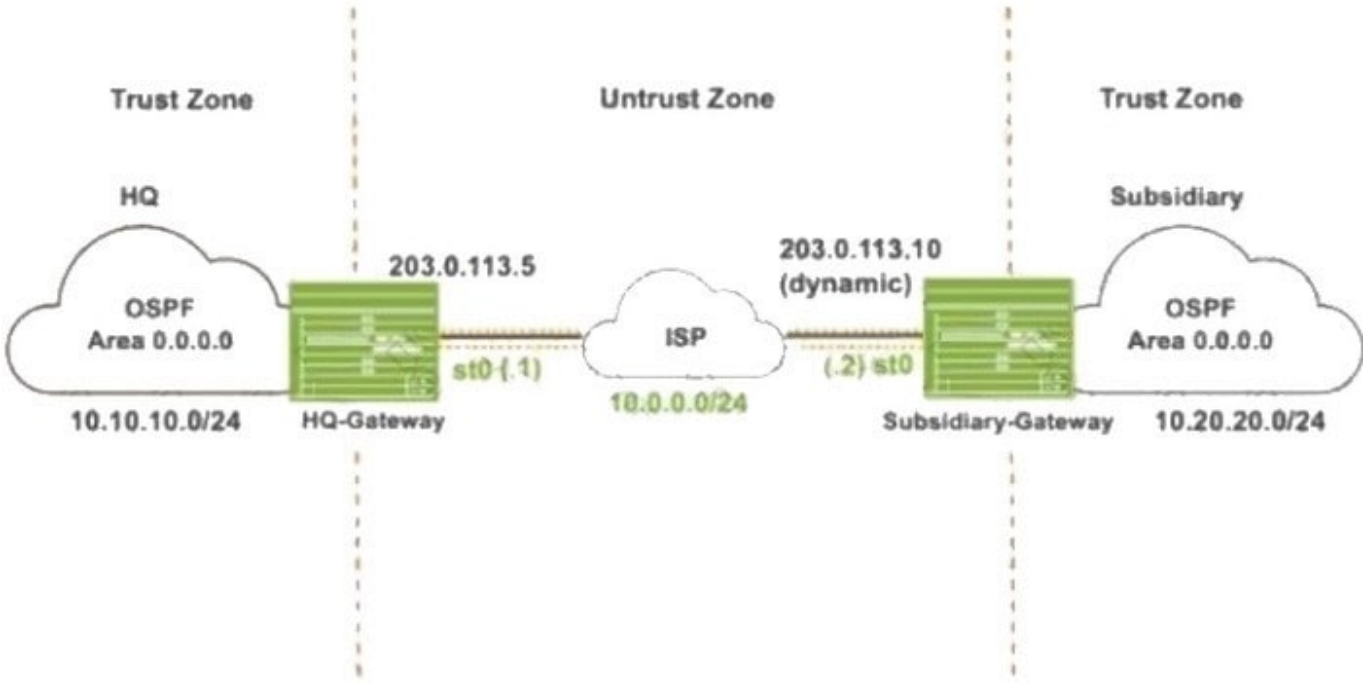
NAT source summaries or pools, which are not related specifically to persistent NAT bindings.

Juniper References:

Juniper Persistent NAT Documentation: Describes the persistent NAT binding table and the commands used to monitor its status.

QUESTION 3

Referring to the exhibit.



Which IKE mode will be configured on the HQ-Gateway and Subsidiary-Gateway?

A. Main mode on both the gateways

B. Aggressive mode on both the gateways

C. Main mode on the HQ-Gateway and aggressive mode on the Subsidiary-Gateway

D. Aggressive mode on the HQ-Gateway and main mode on the Subsidiary-Gateway

Correct Answer: C

Referring to the exhibit, we can see that the HQ-Gateway has a static IP address (203.0.113.5), while the Subsidiary-Gateway has a dynamic IP address (203.0.113.10). This difference in IP addressing is crucial in determining the correct IKE

mode configuration.

Main Mode for Static IP (HQ-Gateway): Main mode is typically used when both VPN peers have static IP addresses. Main mode provides more security because it completes the IKE negotiation in six messages, hiding the identity of the

participants until the key exchange occurs. Since the HQ-Gateway has a static IP address, main mode is appropriate here.

Aggressive Mode for Dynamic IP (Subsidiary-Gateway): Aggressive mode is used when one or both VPN peers have dynamic IP addresses. In this mode, the initiator (Subsidiary-Gateway in this case) can present its identity in the first

message, which is necessary because the dynamic IP may not be known ahead of time. This allows the negotiation to complete more quickly with fewer messages. Hence, aggressive mode is the correct choice for the Subsidiary-Gateway.

Main mode on the HQ-Gateway and aggressive mode on the Subsidiary- Gateway, because the Subsidiary-Gateway has a dynamic IP, while the HQ-Gateway has a static IP.

Juniper References:

Juniper IKE Documentation: Provides details on when to use main mode versus aggressivemode in IPsec VPN configurations based on the static or dynamic nature of IP addresses.

QUESTION 4

You are enabling advanced policy-based routing. You have configured a static route that has a next hop from the inet.0 routing table. Unfortunately, this static route is not active in your routing instance.

In this scenario, which solution is needed to use this next hop?

A. Use RIB groups.

B. Use filter-based forwarding.

C. Use transparent mode.

D. Use policies.

Correct Answer: A

To enable advanced policy-based routing in Junos OS and activate a static route with a next-hop address in the inet.0 table within your routing instance, you should utilize RIB groups. RIB groups allow you to import routes from one routing

table to another. In this scenario, the static route within the routing instance needs access to the inet.0 routes, which is facilitated by configuring a RIB group. Juniper\\'s documentation outlines RIB groups as a necessary component for

handling instances where routes need to be shared across routing tables, thereby ensuring seamless traffic flow through specified routes. For more details, refer to the Juniper Networks Documentation on RIB Groups.

In Junos OS for SRX Series devices, when enabling advanced policy-based routing and configuring a static route with a next-hop from the inet.0 routing table, the issue arises because the static route is not being used in the routing instance.

This is a common scenario when the next-hop belongs to a different routing table or instance, and the routing instance is not aware of that next-hop.

To resolve this, RIB (Routing Information Base) groups are used. RIB groups allow routes from one routing table (RIB) to be shared or imported into another routing table. This means that the routing instance can import the necessary routes

from inet.0 and make them available for the routing instance where the policy- based routing is applied.

Detailed Steps:

Configure the Static Route:First, configure the static route pointing to the next-hop in inet.0. Here\\'s an example:

bash

Copy code

set routing-options static route 10.1.1.0/24 next-hop 192.168.1.1

This static route will be placed in the inet.0 routing table by default.

Create and Apply a RIB Group:To import routes from inet.0 into the routing instance, create a RIB group configuration. This will allow the static route from inet.0 to be visible within the routing instance.

Example configuration for the RIB group:

bash

Copy code

set routing-options rib-groups RIB-GROUP import-rib inet.0

set routing-options rib-groups RIB-GROUP import-rib .inet.0

This configuration ensures that routes from inet.0 are imported into the specified routing instance.

Apply the RIB Group to the Routing Instance:Once the RIB group is configured, apply it to the appropriate routing instance:

bash

Copy code

set routing-instances routing-options rib-group RIB-GROUP

Verify Configuration:Use the following command to verify that the static route has been imported into the routing instance:

bash

Copy code

show route table .inet.0

The output should now display the static route imported from inet.0.

Juniper Security Reference: RIB Groups Overview: Juniper\\'s documentation provides detailed information on how RIB groups function and how to use them to share routes between different routing tables. This is essential for scenarios involving policy-based routing where routes from one instance (like inet.0) need to be available in another instance. Reference: Juniper Networks Documentation on RIB Groups. By using RIB groups, you ensure that the static route from inet.0 is available in the appropriate routing instance for policy-based routing to function correctly. This avoids the need for other methods like filter- based forwarding or transparent mode, which do not address the specific issue of static route visibility across routing instances.

QUESTION 5

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

```
[edit security nat]
user@srx# show
source {
    interface {
        port-overloading off;
    }
    rule-set rule1 {
        from zone trust;
        to zone untrust;
        rule allow {
            match {
                source-address 172.16.1.0/24;
                destination-address 0.0.0.0/0;
            }
            then {
                source-nat {
                    interface {
                        persistent-nat {
                            permit target-host;
                        }
                    }
                }
            }
        }
    }
}
```

A. Both the internal and the external host can initiate a session after the initial translation.

B. Only a specific host can initiate a session to the reflexive address after the initial session.

C. Any external host will be able to initiate a session to the reflexive address.

D. The original destination port is used for the source port for the session.

Correct Answer: BD

The NAT setup allows only specific external hosts to reach the internal network post-initial session, providing controlled access. Reflexive NAT preserves the source port from the original request, maintaining continuity. More on this can be

found in Juniper NAT Configuration Documentation. Looking at the NAT configuration, we observe the use of persistent NAT with the keyword permit target-host . Here\\'s a detailed breakdown:

Persistent NAT (Correct: Option B):When persistent NAT is configured with the permit target-host option, it allows the internal host (from the 172.16.1.0/24 network) to initiate communication with an external host. After the initial session is

established, only the specific external host (target host) is allowed to initiate subsequent sessions to the internal host using the reflexive address. This ensures that random external hosts cannot initiate sessions, which enhances security.

Original Destination Port Reuse (Correct: Option D):In this configuration, theinterface-based source NAT uses the original destination port of the incoming session as the source port for the outbound session. This maintains port transparency

for NATed traffic, which can be crucial for certain types of applications that depend on consistent port numbers.

Incorrect Options:

Option Ais incorrect because persistent NAT with target-host does not allow both internal and external hosts to initiate sessions freely. Only the specific external hostcan initiate a session after the initial session is established by the internal

host.

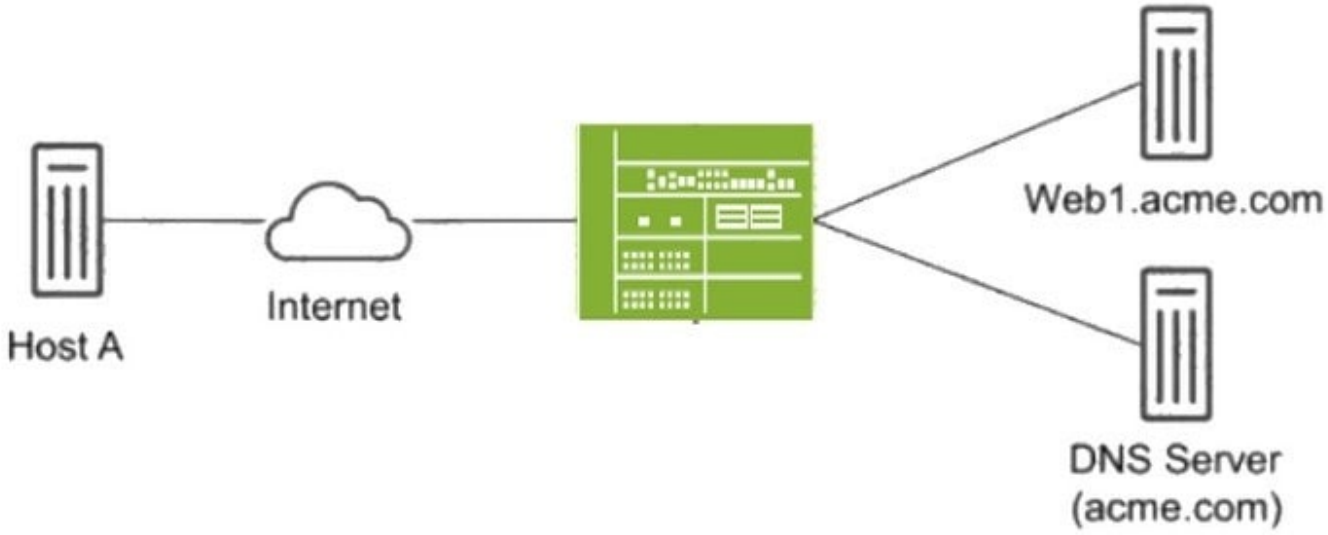
Option Cis incorrect because only the specific external host can initiate subsequent sessions, not any random external host.

Juniper References:

Juniper NAT Documentation: Describes the behavior of persistent NAT and how target-host restrictions work for enhanced security.

QUESTION 6

Referring to the exhibit.



Host A shown in the exhibit is attempting to reach the Web1 webserver, but the connection is failing. Troubleshooting reveals that when Host A attempts to resolve the domain name of the server (web.acme. com), the request is resolved to the private address of the server rather than its public IP.

Which feature would you configure on the SRX Series device to solve this issue?

A. Persistent NAT

B. Double NAT

C. DNS doctoring

D. STUN protocol

Correct Answer: C

DNS doctoring modifies DNS responses for hosts behind NAT devices, allowing them to receive the correct public IP address for internal resources when queried from the public network. This prevents issues where private IPs are returned

and are not reachable externally. For details, visit Juniper DNS Doctoring Documentation.

In this scenario, Host A is trying to resolve the domain name web.acme.com , but the DNS resolution returns the private IP address of the web server instead of its public IP. This is a common issue in networks where private addresses are

used internally, but public addresses are required for external clients.

of Answer C (DNS Doctoring):

DNS doctoringis a feature that modifies DNS replies as they pass through the SRX device. In this case, DNS doctoring can be used to replace the private IP address returned in the DNS response with the correct public IP address for Host A.

This allows external clients to reach internal resources without being aware of their private IP addresses.

Configuration Example:

bash

Copy code

set security nat dns-doctoring from-zone untrust to-zone trust

Juniper Security Reference:

DNS Doctoring Overview: DNS doctoring is used to modify DNS responses so that external clients can access internal resources using public IP addresses. Reference: Juniper DNS Doctoring Documentation.

QUESTION 7

Referring to the exhibit.

```
[edit]
user@RemoteSite1# show interfaces
ge-0/0/2 {
    unit 0 {
        family inet {
            dhcp;
        }
    }
}
st0 {
    unit 0 {
        family inet {
            address 10.0.0.2/30;
        }
    }
}
[edit security zones]
user@RemoteSite1# show security-zone untrust
interfaces {
    ge-0/0/2.0 {
        host-inbound-traffic {
            system-services {
                ike;
                dhcp;
            }
        }
    }
}
```

```
[edit security ike]
user@RemoteSite1# show
policy ike-policy-1 {
    mode main;
    proposal-set standard;
    pre-shared-key ascii-text "$9$6st6CpOhSeX7V1R7VWYZG1AB"; ## SECRET-DATA
}
gateway gateway-1 {
    ike-policy ike-policy-1;
    address 203.0.113.5;
    local-identity hostname "RemoteSite1@srx.juniper.net";
    external-interface ge-0/0/2;
}
[edit security ike]
user@corporate# show
policy ike-policy-site1 {
    mode main;
    proposal-set standard;
    pre-shared-key ascii-text "$9$6st6CpOhSeX7V1R7VWYZG1AB"; ## SECRET-DATA
}
gateway gateway-site1 {
    ike-policy ike-policy-site1;
    dynamic hostname "RemoteSite1@srx.juniper.net";
    external-interface ge-0/0/1;
}
```

You are troubleshooting a new IPsec VPN that is configured between your corporate office and the RemoteSite1 SRX Series device. The VPN is not currently establishing. The RemoteSite1 device is being assigned an IP address on its gateway interface using DHCP.

Which action will solve this problem?

A. On the RemoteSite1 device, change the IKE gateway external interface to st0.0.

B. On both devices, change the IKE version to use version 2 only.

C. On both devices, change the IKE policy proposal set to basic.

D. On both devices, change the IKE policy mode to aggressive.

Correct Answer: D

Aggressive mode is required when an IP address is dynamically assigned, such as through DHCP, as it allows for faster establishment with less identity verification. More details are available in Juniper IKE and IPsec Configuration Guide.

The configuration shown in the exhibit highlights that the RemoteSite1 SRX Series device is using DHCP to obtain an IP address for its external interface (ge-0/0/2). This introduces a challenge in IPsec VPN configurations when the public IP

address of the remote site is not static, as is the case here.

Aggressive modein IKE (Internet Key Exchange) is designed for situations where one or both peers have dynamically assigned IP addresses. In this scenario, aggressive mode allows the devices to exchange identifying information, such as

hostnames, rather than relying on static IP addresses, which is necessary when the remote peer (RemoteSite1) has a dynamic IP from DHCP. Correct Action (D): Changing the IKE policy mode to aggressive will resolve the issue by allowing

the two devices to establish the VPN even though one of them is using DHCP. In aggressive mode, the initiator can present its identity (hostname) during the initial handshake, enabling the VPN to be established successfully.

Incorrect Options:

Option A: Changing the external interface to st0.0 is incorrect because the st0 interface is used for the tunnel interface, not for the IKE negotiation.

Option B: Changing to IKE version 2 would not resolve the dynamic IP issue directly, and IKEv1 works in this scenario.

Option C: Changing the IKE proposal set to basic doesn\\'t address the dynamic IP challenge in this scenario.

Juniper References:

Juniper IKE and VPN Documentation: Provides details on when to use aggressive mode, especially when a dynamic IP address is involved.

QUESTION 8

You have configured the backup signal route IP for your multinode HA deployment, and the ICL link fails. Which two statements are correct in this scenario? (Choose two.)

A. The current active node retains the active role.

B. The active node removes the active signal route.

C. The backup node changes the routing preference to the other node at its medium priority.

D. The active node keeps the active signal route.

Correct Answer: AD

In multinode HA, the active node retains its role and maintains the active signal route even if the ICL link fails, as long as a backup signal route IP is configured. This backup ensures continuity in failover scenarios. For detailed information,

refer to Juniper Multinode HA Documentation.

In a multinode HA (High Availability) deployment with SRX devices, the Inter-Chassis Link (ICL) is critical for communication between the active and backup nodes. If the ICL link fails, the system relies on thebackup signal route to continue

monitoring the state of the HA deployment.

of Answer A (Active Node Retains Active Role):

If the ICL link fails but the backup signal route is still operational, the active node will retain its role as the active node. This is because the signal route allows the active node to confirm its operational state.

of Answer D (Active Node Keeps Signal Route):

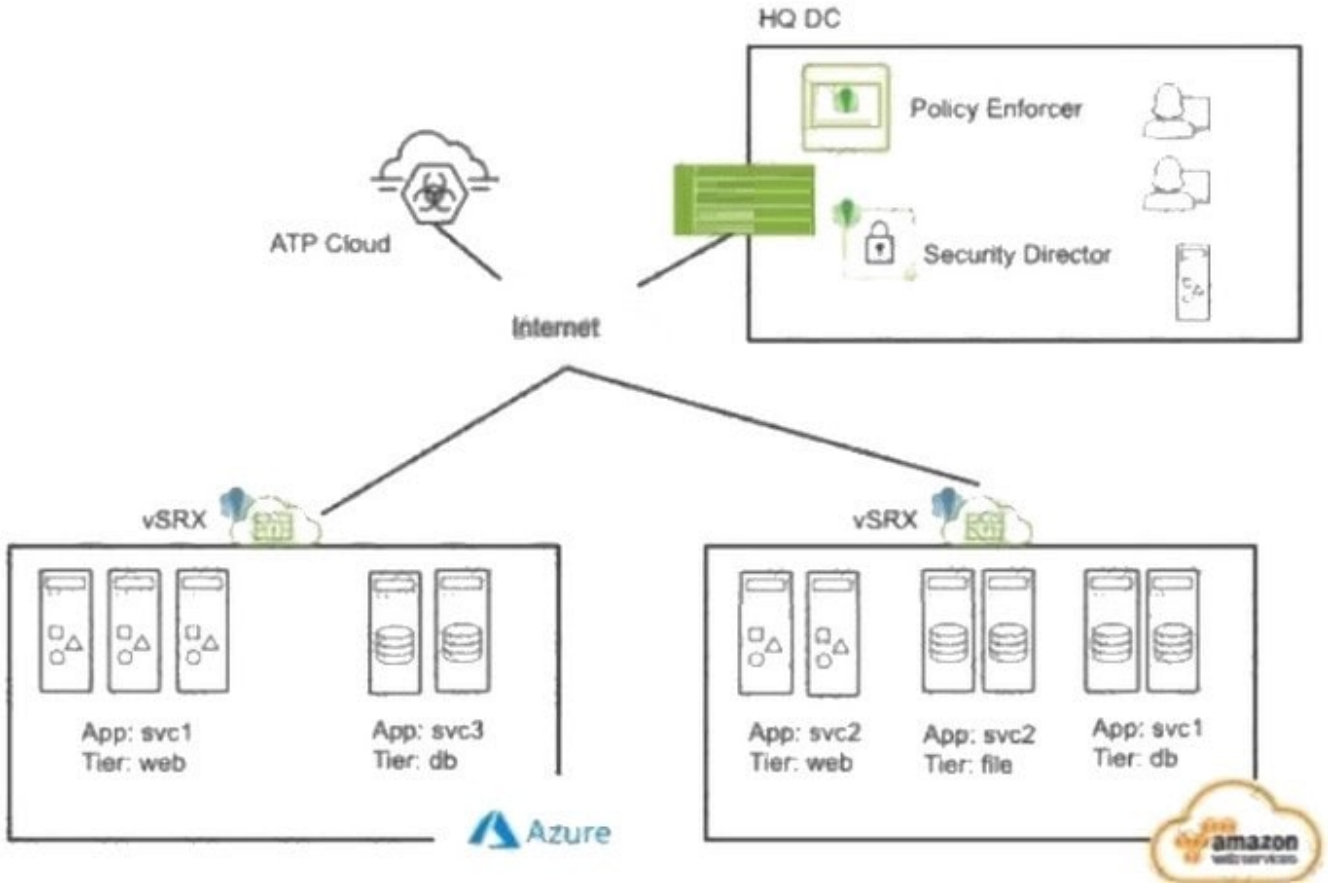
The active node will maintain the signal route if the backup signal route remains operational. The backup node will not preemptively take over the active role unless it detects that the active node has failed entirely.

Juniper Security Reference:

Multinode HA Overview: The backup signal route in multinode HA ensures that the active node retains control as long as it can maintain a signal route. Reference: Juniper HA Documentation.

QUESTION 9

Referring to the exhibit.



What do you use to dynamically secure traffic between the Azure and AWS clouds?

A. You can dynamically secure traffic between the clouds by using user identities in the security policies.

B. You can dynamically secure traffic between the clouds by using advanced connection tracking in the security policies.

C. You can dynamically secure traffic between the clouds by using security tags in the security policies.

D. You can dynamically secure traffic between the clouds by using URL filtering in the security policies.

Correct Answer: C

Security tags facilitate dynamic traffic management between cloud environments like Azure and AWS. Tags allow flexible policies that respond to cloud-native events or resource changes, ensuring secure inter-cloud communication. For more

information, see Juniper Cloud Security Tags.

In the scenario depicted in the exhibit, where traffic needs to be dynamically secured between Azure and AWS clouds, the best method to achieve dynamic security is by using security tags in the security policies.

of Answer C (Security Tags in Security Policies):

Security tagsallow dynamic enforcement of security policies based on metadata rather than static IP addresses or zones. This is crucial in cloud environments, where resources and IP addresses can change dynamically. Using security tags

in the security policies, you can associate traffic flows with specific applications, services, or virtual machines, regardless of their underlying IP addresses or network locations. This ensures that security policies are automatically updated as

cloud resources change.

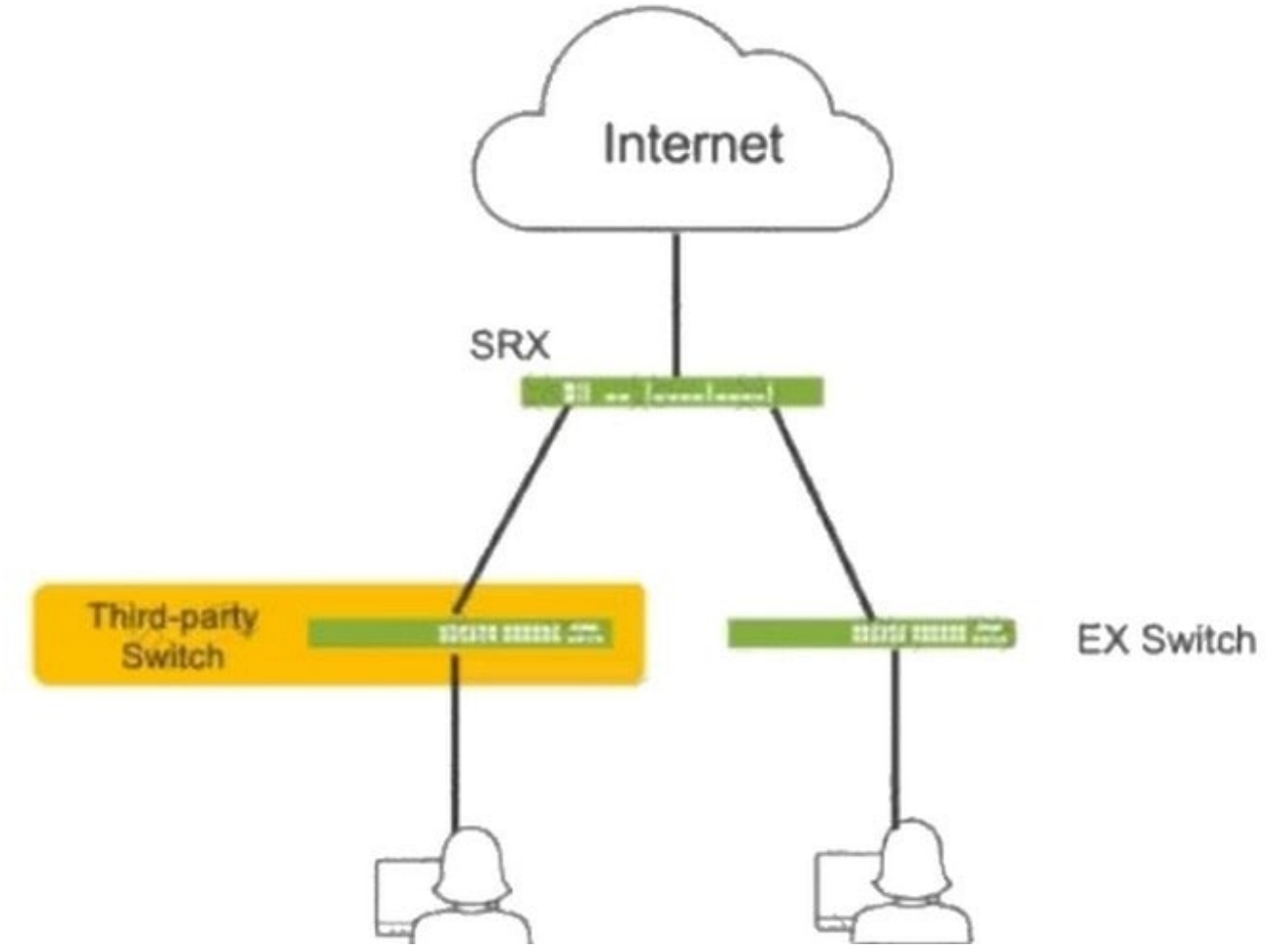
Juniper Security Reference:

Dynamic Security with Security Tags: This feature allows you to dynamically secure cloud-based traffic using metadata and tags, ensuring that security policies remain effective even in dynamic environments. Reference: Juniper Security

Tags Documentation.

QUESTION 10

Click the Exhibit button.



Referring to the exhibit, which three actions do you need to take to isolate the hosts at the switch port level if they become infected with malware? (Choose three.)

A. Enroll the SRX Series device with Juniper ATP Cloud.

B. Use a third-party connector.

C. Deploy Security Director with Policy Enforcer.

D. Configure AppTrack on the SRX Series device.

E. Deploy Juniper Secure Analytics.

Correct Answer: ACD

To isolate hosts at the switch port level when they become infected with malware, the SRX Series device must integrate with advanced threat detection and network management tools. Here\\'s how the actions contribute to achieving this:

of Answer A (Enroll SRX with Juniper ATP Cloud):

Enrolling the SRX Series device with Juniper ATP Cloud allows for advanced malware detection and prevention. Juniper ATP (Advanced Threat Prevention) Cloud provides a cloud-based sandboxing solution that analyzes files and traffic for

malicious behavior, helping to identify infected hosts.

Once the SRX is enrolled, it can receive real-time threat intelligence from the cloud, enabling proactive isolation of compromised hosts.

of Answer C (Deploy Security Director with Policy Enforcer):

Security Directorwith Policy Enforcer allows for centralized security management and automated responses. Policy Enforcer can dynamically update policies to block infected hosts and isolate them based on detected threats. This is critical

for automating the isolation process at the switch port level.

With Policy Enforcer, you can quarantine infected devices automatically.

of Answer D (Configure AppTrack on SRX):

AppTrackis used to monitor and track application usage on the network. By configuring AppTrack on the SRX, you can detect abnormal behavior that may indicate malware infections, such as unusual application usage patterns. AppTrack

can also generate logs and alerts to assist in isolating infected hosts at the switch port level.

This provides visibility into which applications are being used, helping to identifymalicious traffic.

Juniper Security Reference:

Juniper ATP Cloud Overview: Integrates advanced malware detection and threat intelligence for proactive defense.

Security Director with Policy Enforcer: Automates policy changes in response to threats, ensuring fast isolation of infected hosts. Reference: Juniper Security Director Documentation.

AppTrack: Provides application visibility, monitoring, and threat detection. Reference: Juniper AppTrack Documentation.

QUESTION 11

You have deployed automated threat mitigation using Security Director with Policy Enforcer, Juniper ATP Cloud, SRX Series devices, and EX Series switches.

In this scenario, which device is responsible for blocking the infected hosts?

A. Policy Enforcer

B. Security Director

C. Juniper ATP Cloud

D. EX Series switch

Correct Answer: A

Policy Enforcer interacts with other network elements like EX switches to enforce blocking of infected hosts based on threat intelligence from ATP Cloud and other sources. For more information, refer to Juniper Policy Enforcer

Documentation.

In a Juniper automated threat mitigation setup involving Security Director Policy Enforcer Juniper ATP , , Cloud SRX Series , , and EX Series switches, the Policy Enforcer is the component responsible for blocking infected hosts. The role of

each component is as follows:

Policy Enforcer (Correct: Option A):Policy Enforcer receives threat intelligence from Juniper ATP Cloud and instructs SRX devices and EX Series switches to block or quarantine infected hosts. Policy Enforcer pushes policies to these devices

to enforce the mitigation actions.

Security Director (Incorrect):Security Director provides centralized management and visibility but does not directlyenforce policies. Juniper ATP Cloud (Incorrect):Juniper ATP Cloud is responsible for analyzing threats and providing

intelligence but does not take direct mitigation actions. EX Series Switch (Incorrect):EX Series switches can enforce the policy pushed by Policy Enforcer but are not responsible for deciding which hosts to block.

Juniper References:

Juniper ATP Cloud and Policy Enforcer Documentation: Details the roles of each component in the automated threat mitigation architecture.

QUESTION 12

You have deployed an SRX Series device at your network edge to secure Internet-bound sessions for your local hosts using source NAT. You want to ensure that your users are able to interact with applications on the Internet that require more than one TCP session for the same application session.

Which two features would satisfy this requirement? (Choose two.)

A. address persistence

B. STUN

C. persistent NAT

D. double NAT

Correct Answer: AC

Address persistence ensures that the same NAT IP address is used for all sessions originating from a single source IP. Persistent NAT maintains connections for applications needing multiple sessions, like VoIP. Additional details are available in Juniper NAT Documentation.

For applications that require multiple TCP sessions for the same application session (such as VoIP or certain online games), the SRX device needs to handle NAT properly to maintain session continuity. Here\\'s what helps: Address Persistence (Answer A): Address persistence ensures that multiple sessions initiated by the same internal host are mapped to the same external IP address. This is crucial for applications that use multiple TCP sessions to maintain a stateful connection with the external server. Command Example: bash Copy code set security nat source persistent-nat address-persistence Persistent NAT (Answer C): This feature allows the external server to initiate new connections to the internal client using the same NAT translation. It\\'s essential for applications that require consistent NAT mappings across multiple sessions. Command Example: bash Copy code set security nat source persistent-nat permit target-host-port These features ensure that applications with multiple TCP sessions work seamlessly across NAT.

QUESTION 13

Which role does an SRX Series device play in a DS-Lite deployment?

A. Softwire concentrator

B. STUN server

C. STUN client

D. Softwire initiator

Correct Answer: D

In a DS-Lite deployment, the SRX device functions as the softwire initiator, which initiates IPv4-in-IPv6 tunneling to connect IPv4 hosts over an IPv6 infrastructure. For DS-Lite configurations and roles, check Juniper DS-Lite Documentation.

In a DS-Lite (Dual-Stack Lite) deployment, the SRX Series device typically acts as a softwire initiator. DS- Lite is an IPv6 transition technology that allows IPv6-enabled devices to communicate with IPv4 networks.

The softwire initiator is responsible for encapsulating IPv4 packets within an IPv6 header at the customer edge, which is then sent to the softwire concentrator (usually on the service provider\\'s side). Juniper SRX devices can be configured for

DS-Lite to support IPv6 clients while communicating with an IPv4 internet via this tunneling mechanism.

To configure DS-Lite on a Juniper SRX device, you\\'d follow these steps:

Configure the DS-Lite AFTR (Address Family Transition Router) with the correct IPv6 addressing and routing parameters.

Enable DS-Lite functionality on the SRX device using Junos OS commands.

Verify connectivity and ensure that traffic from IPv6 devices is correctly tunneled over IPv4 using tools like ping and traceroute over IPv6.

QUESTION 14

Which two statements are true when setting up an SRX Series device to operate in mixed mode? (Choose two.)

A. A physical interface can be configured to be both a Layer 2 and a Layer 3 interface at the same time.

B. User logical systems support Layer 2 traffic processing.

C. The SRX must be rebooted after configuring at least one Layer 3 and one Layer 2 interface.

D. Packets from Layer 2 interfaces are switched within the same bridge domain.

Correct Answer: CD

In mixed mode, SRX devices can simultaneously handle Layer 2 switching and Layer 3 routing, but a reboot is required when configuring Layer 2 and Layer 3 interfaces to ensure the configuration takes effect. Layer 2 packets are switched

within the defined bridge domain. Further guidance on SRX mixed mode can be found at Juniper Mixed Mode Documentation.

When an SRX Series device is configured in mixed mode , both Layer 2 switching and Layer 3 routing functionalities can be used on the same device. This enables the SRX to act as both a router and a switch for different interfaces.

However, there are certain considerations:

of Answer C (Reboot Requirement):

After configuring the SRX to operate with at least one Layer 2 interface and one Layer 3 interface, the device needs to be rebooted. This is required to properly initialize the mixed mode configuration, as the SRX needs to switch between

Layer 2 and Layer 3 processing modes.

of Answer D (Layer 2 Traffic Handling):

In mixed mode, traffic from Layer 2 interfaces is switched within the same bridge domain . A bridge domain defines a Layer 2 broadcast domain, and packets from Layer 2 interfaces are forwarded based on MAC addresses within that domain.

Juniper Security Reference:

Mixed Mode Overview: Juniper SRX devices can operate in mixed mode to handle both Layer 2 and Layer 3 traffic simultaneously. Reference: Juniper Mixed Mode Documentation.

QUESTION 15

You are deploying a large-scale VPN spanning six sites. You need to choose a VPN technology that satisfies the following requirements:

1.

All sites must have secure reachability to all other sites.

2.

New spoke sites can be added without explicit configuration on the hub site.

3.

All spoke-to-spoke communication must traverse the hub site.

Which VPN technology will satisfy these requirements?

A. ADVPN

B. Group VPN

C. Secure Connect VPN

D. AutoVPN

Correct Answer: D

AutoVPN simplifies deployment by dynamically establishing tunnels from spokes to the hub. This architecture supports easy scaling with minimal configuration changes, ensuring spoke-to-spoke traffic flows through the hub. For more information, see Juniper AutoVPN Overview.

In this scenario, you need a VPN solution that ensures secure, dynamic connectivity between multiple sites, with the following conditions:

1.

All sites must have secure reachability.

2.

New spoke sites can be added without explicit configuration on the hub site.

3.

Spoke-to-spoke communication must traverse the hub.

The correct technology to meet these requirements is AutoVPN . It simplifies VPN configurations by automating the setup between hub and spoke sites. Additionally, AutoVPN automatically establishes secure tunnels for new spoke sites without requiring manual configuration at the hub, and all spoke-to-spoke traffic is routed through the hub.