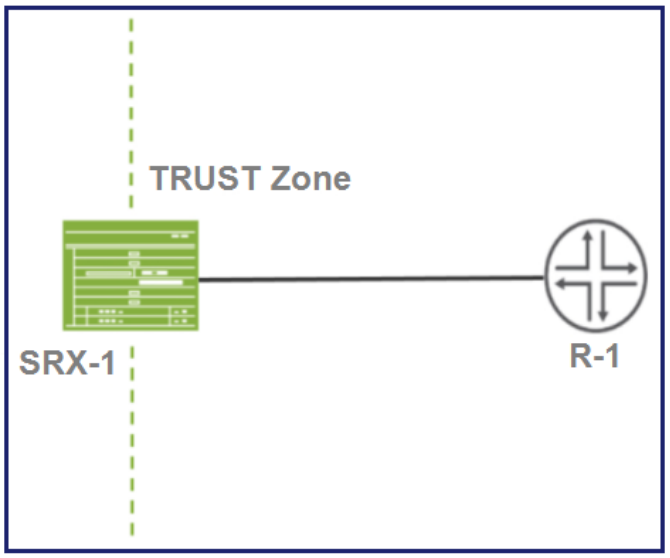
Question #1 *Topic 1*

Click the Exhibit button.



You can use SSH from SRX-1 to R-1 but not telnet. Both telnet and SSH services are enabled on R-1.
Referring to the exhibit, which configuration on SRX-1 is denying the access?

A. The security policy from the junos-host zone to the TRUST zone is denying port 22.

B. The security policy from the TRUST zone to the junos-host zone is denying port 22.

C. The security policy from the junos-host zone to the TRUST zone is denying port 23.

D. The security policy from the TRUST zone to the junos-host zone is denying port 23.

Suggested Answer: *D*

Community vote distribution

C (100%)

inmymind84 3 months ago

Selected Answer: C

if connection is made from SRX to R-1 policy should be from junos-host (locally on SRX) to Trust (host in Trust zone, in this case it is R1 router).

upvoted 2 times

Question #2 *Topic 1*

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

A. PKI certificated

B. IDP

C. IPsec VPN

D. advanced policy-based routing

Suggested Answer: *B*

Community vote distribution

A (50%) C (50%)

75e7ed9 4 days, 6 hours ago

Selected Answer: A

Wording is not the best

But for sure the answer is A, pki certificates

https://www.juniper.net/documentation/us/en/software/junos/high-availability/topics/topic-map/mnha-introduction.html

You must synchronize the certificates from the active node to backup

upvoted 1 times

inmymind84 3 months ago

Selected Answer: C

non of above. Something is wrong with this question imo.

upvoted 1 times

Question #3 *Topic 1*

Click the Exhibit button.

```
security {
     advance-policy-based-routing {
          profile profile1 {
               rule Web-Proxy {
                    match {
                         dynamic-application [ junos:HTTP junos: HTTPS ];
                    }
                    then {
                         routing-instance R1;
                    }
               }
               rule DNS {
                    match {
                         dynamic-application-group junos:DNS;
                    }
                    then {
                         routing-instance R2;
                    }
               }
          }
     }
}
routing-instances {
     R1 {
          instance-type forwarding;
          routing-options {
               static {
                    route 192.168.0.0/16 next-hop 10.1.0.1;
               }
          }
     }
     R2 {
          instance-type forwarding;
          routing-options {
               static {
                    route 192.168.0.0/16 next-hop 10.2.0.1;
               }
          }
     }
}
routing-options {
     interface-routes {
          rib-group inet abpr_group;
     }
     rib-groups {
          apbr_group {
               import-rib [ inet.0 ];
          }
     }
}
```

Referring to the exhibit, which statement about TLS 1.2 traffic is correct?

A. TLS 1.2 traffic will be sent to routing instance R2 but not forwarded to the next hop.

B. TLS 1.2 traffic will be sent to routing instance R2 and forwarded to next hop 10.2.0.1.

C. TLS 1.2 traffic will be sent to routing instance R1 and forwarded to next hop 10.1.0.1.

D. TLS 1.2 traffic will be sent to routing instance R1 but not forwarded to the next hop.

Suggested Answer: *C*

Community vote distribution

D (60%) C (40%)

75e7ed9 5 days, 6 hours ago

Selected Answer: D

Correct answer is D, because RIB groups is not configured correctly, because of that, routing instance "R1" does not have the ARP entry or the interface to send the packets to its next hops

upvoted 1 times

inmymind84 3 months ago

Selected Answer: D

Sorry. Not correct. There is no main routing instance import so traffic wont be directed to the host.

upvoted 2 times

inmymind84 3 months ago

Selected Answer: C

correct

upvoted 2 times

Question #4 *Topic 1*

You are deploying threat remediation to endpoints connected through third-party devices.
In this scenario, which three statements are correct? (Choose three.)

A. All third-party switches must support AAA/RADIUS and Dynamic Authorization Extensions to the RADIUS protocol.

B. The connector uses an API to gather endpoint MAC address information from the RADIUS server.

C. All third-party switches in the specified network are automatically mapped and registered with the RADIUS server.

D. The connector queries the RADIUS server for the infected host endpoint details and initiates a change of authorization (CoA) for the infected host.

D. The RADUIS server sends Status-Server messages to update infected host information to the connector.

Suggested Answer: *ABD*

Community vote distribution

ABD (100%)

inmymind84 3 months ago

Selected Answer: ABD

THERE IS TWO D ANSWERS. looks valid.

upvoted 1 times

Question #5 *Topic 1*

Click the Exhibit button.

```
user@srx> show chassis high-availability information
Node failure codes:
     HW Hardware monitoring  LB Loopback monitoring
     MB Mbuf monitoring      SP SPU monitoring
     CS Cold Sync monitoring SU Software Upgrade
Node Status: ONLINe
Local-id:
Local-IP: 10.10.1.1
HA Peer Information:
     Peer Id: 2          IP address: 10.10.1.2    Interface: ge-0/0/1.0
     Routing Instance:    default
     Encrypted: NO  Conn State: UP
     Cold Sync Status:  COMPLETE
Services Redundancy Group: 0
          Current State: ONLINE
          Peer Information:
               Peer Id: 2
SRG failure event codes:
     BF BFD monitoring
     IP IP monitoring
     IF Interface monitoring
     CP Control Plane monitoring
Services Redundancy Group: 1
          Deployment Type: SWITCHING
          Status: ACTIVE
          Activeness Priority: 200
          Preemption: ENABLED
          Process Packet In Backup State: NO
          Control Plane State: READY
          System Integrity Check: N/A
          Failure Events: NONE
          Peer Information:
               Peer Id: 2
               Status: BACKUP
               Health Status: HEALTHY
               Failover Readiness: READY
```

Referring to the exhibit, which three statements about the multinode HA environment are true? (Choose three.)

A. Session state is synchronized on both nodes.

B. IP monitoring has failed for the services redundancy group.

C. Node 1 will host services redundancy group 1 unless it is unavailable.

D. Node 2 will process transit traffic that it receives for services redundancy group 1.

E. Two services redundancy groups are available.

Suggested Answer: *ACE*

Community vote distribution

ACE (100%)

inmymind84 3 months ago

Selected Answer: ACE

A - Default action on this multinode HA

B - there is no Fauilure in logs (NONE)

C - Logs are from active node and it is active

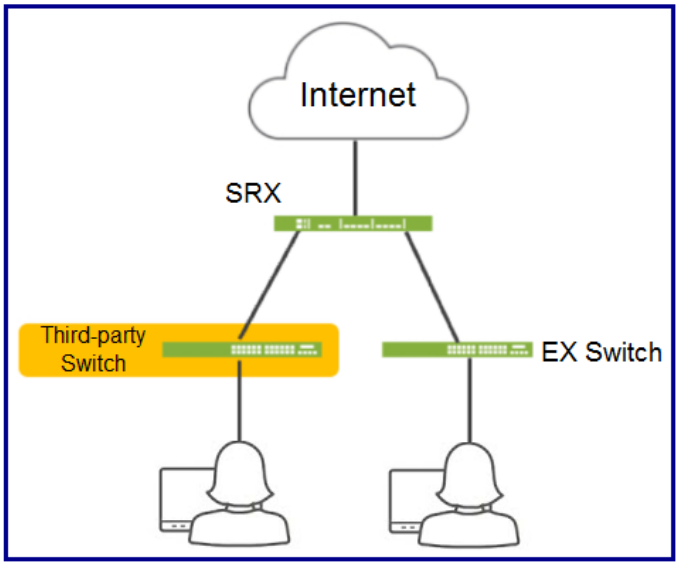
D - no this answer is oposit to C

E - multinode HA requires to SRG to work SRG0 and SRG1, so if HA works then there must be 2 of them :)

upvoted 3 times

Question #6 *Topic 1*

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. Deploy Juniper Secure Analytics.

B. Use a third-party connector.

C. Configure AppTrack on the SRX Series device.

D. Enroll the SRX Series device with Juniper ARP Cloud.

E. Deploy Security Director with Policy Enforcer.

Suggested Answer: *BCE*

Community vote distribution

BDE (100%)

inmymind84 3 months ago

Selected Answer: BDE

A - JSA is a siem and will not help here

B - required for Third-party Switches

C - not required for identification

D - SRX must be enrolled in the cloud to identify malware.

E - Main component of this solution, required.

upvoted 1 times

Question #7 *Topic 1*

Click the Exhibit button.

```
user@vSRX-1> show security ipsec statistics
ESP Statistics:
     Encrypted bytes:        2640
     Decrypted bytes:           0
     Encrypted packets:        22
     Decrypted packets:         0
AH Statistics:
     Input bytes:               0
     Output bytes:              0
     Input packets:             0
     Output packets:            0
Errors:
     AH authentication failures: 0, Replay errors: 18
     ESP authentication failures: 0, ESP decryption failures: 0
     Bad headers: 0, Bad trailers: 0
```

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

A. Every VPN packet that the SRX receives from the VPN peer is outside the ESP sequence window.

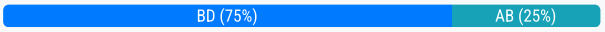
B. The SRX is sending traffic into the tunnel and out toward the VPN peer.

C. The SRX is not sending any packets to the VPN peer.

D. The SRX is not receiving any packets from the VPN peer.

Suggested Answer: *BD*

Community vote distribution



75e7ed9 5 days, 6 hours ago

Selected Answer: AB

I am not sure about this one, D could not be valid, because the SRX is receiving packets, just out of the window, and because of that there are anti reply errors, I would say A and B could be a valid answer

upvoted 1 times

inmymind84 3 months ago

Selected Answer: BD

looks fine.

upvoted 3 times

Question #8 *Topic 1*

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. EX Series switch

B. Juniper ATP Cloud

C. Policy Enforcer

D. Security Director

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

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 persistent-nat-table all

C. show security nat source pool all

D. show security nat source summary

Suggested Answer: *A*

Community vote distribution

A (100%)

inmymind84 3 months ago

Selected Answer: A

valid. tested.

upvoted 2 times

Question #10 *Topic 1*

Click the Exhibit button.

```
SRX(ttyp0)
login: User1
Password:
--- JUNOS 22.4R1.9 built 2023-03-24 12:52:33 UTC
User1@SRX:LSYS-1>
```

Referring to the exhibit, which two statements about User1 are true? (Choose two.)

A. User1 can add logical units to an interface that a primary administrator has not previously assigned.

B. User1 can view outputs from other user logical systems.

C. User1 is logged in to logical system LSYS-1.

D. User1 has access to the configuration specific to their assigned logical system.

Suggested Answer: *CD*

Community vote distribution

CD (100%)

inmymind84 3 months ago

Selected Answer: CD

looks fine. logical.

upvoted 1 times

Question #11 *Topic 1*

You are asked to create multiple virtual routers using a single SRX Series device. You must ensure that each virtual router maintains a unique copy of the routing protocol daemon (RPD) process.
Which solution will accomplish this task?

A. tenant system

B. secure wire

C. transparent mode

D. logical system

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

You want to test how the device handles a theoretical session without generating traffic on the Junos security device.
Which command is used in this scenario?

A. show security policies

B. request security policies check

C. show security match-policies

D. show security flow session

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

You are attempting to ping an interface on your SRX Series device, but the ping is unsuccessful.
What are three reasons for this behavior? (Choose three.)

A. The interface is not assigned to a security zone.

B. The interface's host-inbound-traffic security zone configuration does not permit ping.

C. The ping traffic is matching a firewall filter.

D. The device has J-Web enabled.

E. The interface has multiple logical units configured.

Suggested Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

You are deploying a large scale VPN spanning six sites. You need to choose a VPN technology that satisfies the following requirements: all sites must have secure reachability to all other sites. new spoke sites can be added without explicit configuration on the hub site. all spoke-to-spoke communication must traverse the hub site.
Which VPN technology will satisfy these requirements?

A. ADVPN

B. AutoVPN

C. secure connect VPN

D. group VPN

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

You want to create a connection for communication between tenant systems without using physical revenue ports on the SRX Series device. What are two ways to accomplish this task? (Choose two.)

A. Use an interconnect VPLS switch.

B. Use a secure wire.

C. Use a point-to-point logical tunnel.

D. Use an external router.

Suggested Answer: *BC*

Community vote distribution

AC (100%)

5000a98 1 month, 3 weeks ago

Selected Answer: AC

A. The VPLS switch enables both transit traffic and traffic terminated at a tenant system to pass between tenant systems with a single logical tunnel. Logical tunnel interfaces should be configured in the same subnet to allow traffic between tenant systems.

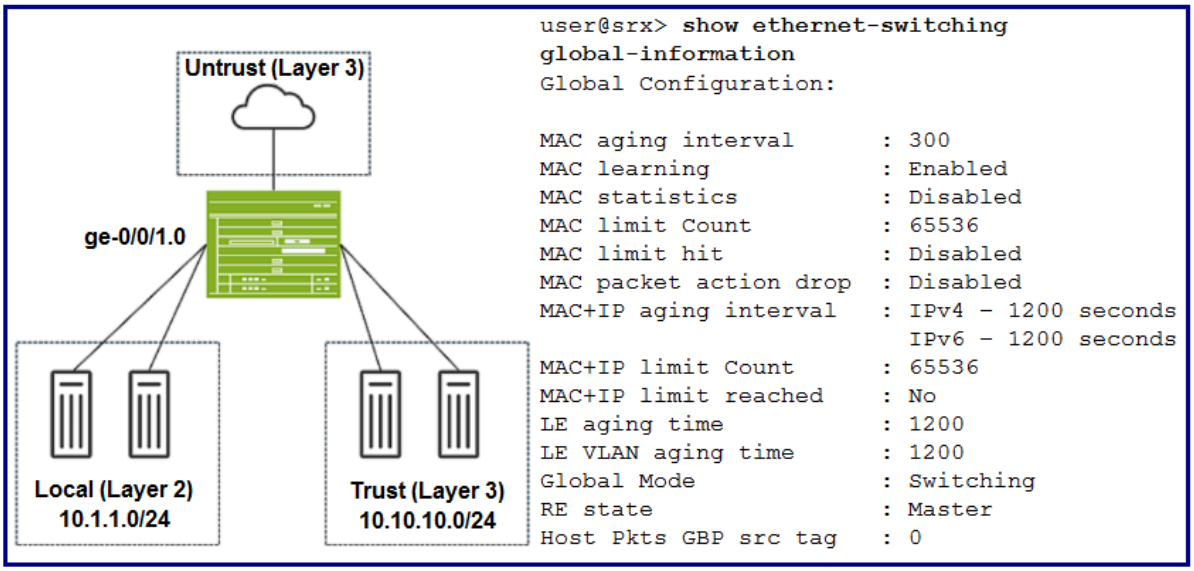
B. is incorrect -> Secure wire doesn't support: Tenant system, Interconnect logical system (https://www.juniper.net/documentation/us/en/software/junos/logical-system-security/topics/topic-map/secure-wire-logical-systems.html)

C. To connect two routing instances with a logical connection, you configure a logical tunnel interface for each instance. Then you configure a peer relationship between the logical tunnel interfaces, thus creating a point-to-point connection.

upvoted 1 times

Question #16 *Topic 1*

Click the Exhibit button.



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

A. Hosts in the Local zone can communicate with hosts in the Trust zone with a security policy.

B. Hosts in the Local zone can be enabled for control plane access to the SRX.

C. You can configure security policies for traffic flows between hosts in the Local zone.

D. An IRB interface is required to enable communication between the Trust and the Untrust zones.

Suggested Answer: *AC*

Community vote distribution

AB (100%)

inmymind84 3 months ago

Selected Answer: AB

C - Global mode switching disable ability to control traffic betweend hosts in local zone

D - Untrust and trust are L3 interfaces so IRB is not required (IRB is only for L2).

upvoted 2 times

Question #17 *Topic 1*

Click the Exhibit button.

```
[edit routing-instances]
user@vSRX-1# show
APBR-1 {
     routing-options {
          static {
               route 0.0.0.0/0 next-hop 172.16.9.2;
          }
     }
}
[edit routing-instances]
user@vSRX-1# show
interface-routes {
     rib-group inet APBR-group;
}
static {
     route 0.0.0.0/0 next-hop 192.168.101.1;
}
rib-groups {
     APBR-group {
          import-rib [inet.0 APBR-1.inet.0];
     }
}
[edit security advance-policy-based-routing]
user@vSRX-1# show
profile APBR-profile {
     rule ssh {
          match {
               dynamic-application junos:SSH;
          }
          then {
               routing-instance APBR-1;
          }
     }
}
from-zone DC9-zone {
     policy move-ssh {
          match {
               source-address any;
               destination-address any;
               application any;
          }
          then {
               application-services {
                    advance-policy-based-routing-profile APBR-profile;
               }
          }
     }
}
```

Referring to the exhibit, you are having problems configuring advanced policy-based routing.

What should you do to solve the problem?

A. Apply a policy to the ABPR RIB group to only allow the exact routes you need.

B. Remove the default static route from the main instance configuration.

C. Change the routing instance to a forwarding instance.

D. Change the routing instance to a virtual router instance.

Suggested Answer: *B*

Community vote distribution

C (100%)

5000a98 1 month, 3 weeks ago

Selected Answer: C

C - indeed, tested on srx550. There is no explicit config for the instance-type in APBR-1 and defaults to non-forwarding: show route instance APBR-1
Instance Type
Primary RIB Active/holddown/hidden
APBR-1 non-forwarding
APBR-1.inet.0 18/0/1
Setting instance type to forwarding will fix the issue.
B can be dismissed as only the connected and local routes are imported from inet.0 to be able to resolve next-hops set in APBR-1.inet.0 route-table .

upvoted 1 times

inmymind84 3 months ago

Selected Answer: C

There is no definition of type of instance so it is default (virtual router) and then default route will be added to instance to. This is a reason why it will not work. nice hard question.

upvoted 1 times

Question #18 *Topic 1*

Which two statements are correct about automated threat mitigation with Security Director? (Choose two.)

A. Infected hosts are tracked by their IP address.

B. Infected hosts are tracked by their user identity.

C. Infected hosts are tracked by their chassis serial number.

D. Infected hosts are tracked by their MAC address.

Suggested Answer: *AD*

Community vote distribution

AD (100%)

inmymind84 3 months ago

Selected Answer: AD

verified.

upvoted 1 times

Question #19 *Topic 1*

You have deployed two SRX Series devices in an active/passive multinode HA scenario.
In this scenario, which two statements are correct? (Choose two.)

A. Services redundancy group 0 (SRG0) is used for services that have a control plane state.

B. Services redundancy group 1 (SRG1) is used for services that have a control plane state.

C. Services redundancy group 0 (SRG0) is used for services that do not have a control plane state.

D. Services redundancy group 1 (SRG1) is used for services that do not have a control plane state.

Suggested Answer: *CD*

Community vote distribution

BC (100%)

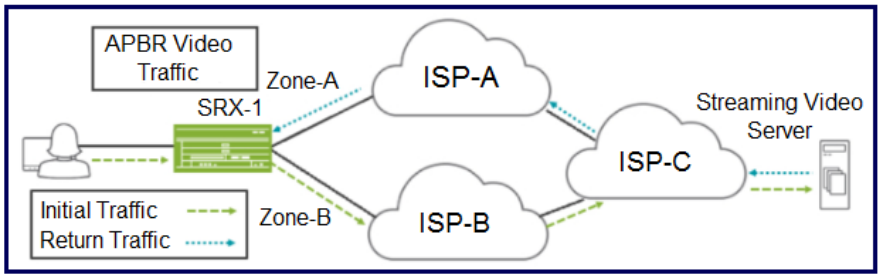
inmymind84 3 months ago

Selected Answer: BC

SRG0 - do not have control plane state
SRG1 - have control plane state
upvoted 2 times

Question #20 *Topic 1*

Click the Exhibit button.



Referring to the exhibit, a default static route on SRX-1 sends all traffic to ISP-A. You have configured APBR to send all requests for streaming video traffic to ISP-B. However, the return traffic from the streaming video server is coming through ISP-A, and the traffic is being dropped by SRX-1. You can only make changes on SRX-1.

How do you solve this problem?

A. Configure BGP to control the return path of the streaming video traffic.

B. Place both ISP-facing interfaces in the same zone.

C. Change the APBR routing instance from a forwarding instance to a virtual router instance.

D. Enable AppTrack to keep track of the sessions and zones for the streaming video traffic.

Suggested Answer: *D*

Community vote distribution

B (100%)

5000a98 1 month, 3 weeks ago

Selected Answer: B

B Indeed - you can use FBF for service-provider selection when you have Internet
connectivity provided by different Internet service providers (ISPs).If the return traffic were to arrive at an interface assigned to a separate security zone, the Junos OS would drop the traffic due to a zone mismatch. To avoid this scenario, we recommend that both egress interfaces reside in the same security zone.

upvoted 1 times

inmymind84 3 months ago

Selected Answer: B

B - the same zone will help to identify traffic as located ine the same locationa and asimetric routing will not be identified.

upvoted 1 times

Question #21 *Topic 1*

Click the Exhibit button.

```
user@SRX show log flow-log | find "policy search"
Jan 9 14:19:37 14:19:37.520231:CID-0:THREAD_ID-01:LSYS_ID-00:RT:flow_first_policy_search:
policy search from zone Linux-9-zone-> zone junos-host (0x0, 0x94c80016, 0x16), result:
0x5ed4b468, pending: 0?, is_http_cached = 0
Jan 9 14:19:37 14:19:37.520232:CID-0:THREAD_ID-01:LSYS_ID-00:RT:flow_first_policy_search:
dynapp_none_policy: TRUE, uc_none_policy: TRUE, is_final: 0x0, is_explicit: 0x0,
policy_meta_data: 0x0
Jan 9 14:19:37 14:19:37.520233:CID-0:THREAD_ID-01:LSYS_ID-00:RT: app 22, timeout 1800s,
curr ageout 20s
Jan 9 14:19:37 14:19:37.520234:CID-0:THREAD_ID-01:LSYS_ID-00:RT: packet dropped, denied by
policy
Jan 9 14:19:37 14:19:37.520234:CID-0:THREAD_ID-01:LSYS_ID-00:RT: denied by policy deny-ssh
(7), dropping pkt
Jan 9 14:19:37 14:19:37.520235:CID-0:THREAD_ID-01:LSYS_ID-00:RT: packet dropped, policy
denied
```

You are using trace options to troubleshoot a security policy on your SRX Series device.

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

A. The security policy controls traffic destined to the SRX device.

B. The SSH traffic matches an existing session.

C. No entries are created in the SRX session table.

D. The traffic is not destined for the root logical system.

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

Click the Exhibit button.

```
[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;
                              }
                         }
                    }
               }
          }
     }
}
```

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

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

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

Suggested Answer: *BC*

Community vote distribution

BD (100%)

inmymind84 3 months ago

Selected Answer: BD

target-host means that only specific host can initiate a session. C is wrong answer.

upvoted 2 times

Question #23 *Topic 1*

Click the Exhibit button.

```
[edit]
user@srx# show security nat
source {
     pool ipv4-source-pool {
          address {
               10.10.101.10/32;
          }
     }
     rule-set ipv6-source {
          from zone trust;
          to zone untrust;
          rule ipv6-host-source {
               match {
                    source-address 2001:db8::1/128;
               }
               then {
                    source-nat {
                         pool {
                              ipv4-source-pool;
                         }
                    }
               }
          }
     }
}
```

You are configuring NAT64 on your SRX Series device. You have committed the configuration shown in the exhibit. Unfortunately, the communication with the 10.10.201.10 server is not working. You have verified that the interfaces, security zones, and security policies are all correctly configured.
In this scenario, which action will solve this issue?

A. Configure destination NAT to translate return traffic from the IPv4 address to the IPv6 address of your source device.

B. Configure source NAT to translate return traffic from IPv4 address to the IPv6 address of your source device.

C. Configure proxy-ndp on the IPV6 interface for the 2001:db8::1/128 address.

D. Configure proxy-arp on the external IPv4 interface for the 10.10.201.10/32 address.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

Which two statements are true regarding NAT64? (Choose two.)

A. An SRX Series device should be in flow-based forwarding mode for IPv4.

B. An SRX Series device should be in packet-based forwarding mode for IPv4.

C. An SRX Series device should be in packet-based forwarding mode for IPv6.

D. An SRX Series device should be in flow-based forwarding mode for IPv6.

Suggested Answer: *BC*

Community vote distribution

AD (100%)

inmymind84 3 months ago

Selected Answer: AD

flow mode is required to NAT64

upvoted 1 times

Question #25 *Topic 1*

You need to set up source NAT so that external hosts can initiate connections to an internal device but only if a connection to the device was first initiated by the internal device.
Which type of NAT solution provides this functionality?

A. persistent NAT with any remote host

B. static NAT

C. persistent NAT with target host

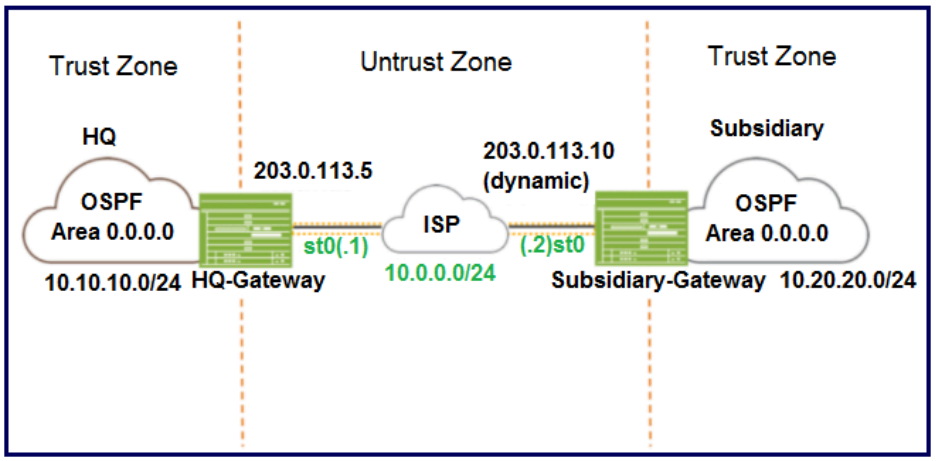
D. address persistent

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

Click the Exhibit button.



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. main mode on the HQ-Gateway and aggressive mode on the Subsidiary-Gateway

C. aggressive mode on both the gateways

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

Which two statements are true about the procedures the Junos security device uses when handling traffic destined for the device itself? (Choose two.)

A. If the received packet is addressed to the ingress interface, then the device first performs a security policy evaluation for the junos-host zone.

B. If the received packet is addressed to the ingress interface, then the device first examines the host -inbound-traffic configuration for the ingress interface and zone.

C. If the received packet is destined for an interface other than the ingress interface, then the device performs a security policy evaluation based on the ingress and egress zone.

D. If the received packet is destined for an interface other than the ingress interface, then the device performs a security policy evaluation for the junos-host zone.

Suggested Answer: *AB*

Community vote distribution

BC (100%)

inmymind84 3 months ago

Selected Answer: BC

A,B be are oposit, and first hostinbound is checked.

C - non-inbound interface means that traffic must go through 2 zones (and then policies), next is host inbound and at the end junos host.

upvoted 2 times

Question #28 *Topic 1*

Which two statements are correct about mixed mode? (Choose two.)

A. IRB interfaces cannot be used to route traffic.

B. Layer 2 and Layer 3 interfaces can use separate security zones.

C. IRB interfaces can be used to route traffic.

D. Layer 2 and Layer 3 interfaces can use the same security zone.

Suggested Answer: *CD*

Community vote distribution

AB (100%)

inmymind84 3 months ago

Selected Answer: AB

valid, check in documentation.

upvoted 2 times

Question #29 *Topic 1*

You are asked to configure tenant systems.
Which two statements are true in this scenario? (Choose two.)

A. Tenant systems have their own configuration database.

B. A tenant system can have only one administrator.

C. You can commit multiple tenant systems at a time.

D. After successful configuration, the changes are merged into the primary database for each tenant system.

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

You have deployed automated threat mitigation using Security Director with Policy Enforcer, Juniper ATP Cloud, SRX Series devices, Forescout, and third-party switches.
In this scenario, which device is responsible for communicating directly to the third-party switches when infected hosts need to be blocked?

A. Forescout

B. Juniper ATP cloud

C. SRX Series device

D. Policy Enforcer

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

Click the Exhibit button.

```
Aug 3 02:10:28 02:10:28.045090:CID-0:THREAD_ID-01:RT: <10.10.101.10/60858->
10.10.102.10/22;6,0x0>
matched filter filter-1:
…
Aug 3 02:10:28 02:10:28.045100:CID-0:THREAD_ID-01:RT: no session found, start
first path. in_tunnel - 0x0, from_cp_flag - 0
Aug 3 02:10:28 02:10:28.045104:CID-0:THREAD_ID-01:RT: flow_first_create_session
…
Aug 3 02:10:28 02:10:28.045143:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.10.102.10) from trust (ge-0/0/4.0 in 0) to ge-0/0/5.0, Next-hop:
10.10.102.10
Aug 3 02:10:28 02:10:28.045158:CID-0:THREAD_ID-01:RT: flow_first_policy_search:
policy search from zone trust-> zone dmz (0x0, 0xedba0016, 0x16)
…
Aug 3 02:10:28 02:10:28.045191:CID-0:THREAD_ID-01:RT: packet dropped, denied by
policy
Aug 3 02:10:28 02:10:28.045192:CID-0:THREAD_ID-01:RT: denied by policy default-
policy-logical-system-00(2), dropping pkt
Aug 3 02:10:28 02:10:28.045192:CID-0:THREAD_ID-01:RT: packet dropped, policy
denied
Aug 3 02:10:28 02:10:28.045195:CID-0:THREAD_ID-01:RT: flow_initiate_first_path:
first pak no session
```

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

A. The data shown requires a traceoptions flag of host-traffic.

B. The data shown requires a traceoptions flag of basic-datapath.

C. The packet is dropped by a configured security policy.

D. The packet is dropped by the default security policy.

Suggested Answer: *CD*

Community vote distribution

BD (100%)

inmymind84 3 months ago

Selected Answer: BD

C,D are oposit.

B basic datapath helps to identify traffic.

upvoted 1 times

Question #32 *Topic 1*

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

A. softwire concentrator

B. softwire initiator

C. STUN client

D. STUN server

Suggested Answer: *A*

Community vote distribution

A (100%)

inmymind84 3 months ago

Selected Answer: A

valid.

upvoted 1 times

Question #33 *Topic 1*

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

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

D. User logical systems support Layer 2 traffic processing.

Suggested Answer: *AC*

Community vote distribution

BC (100%)

inmymind84 3 months ago

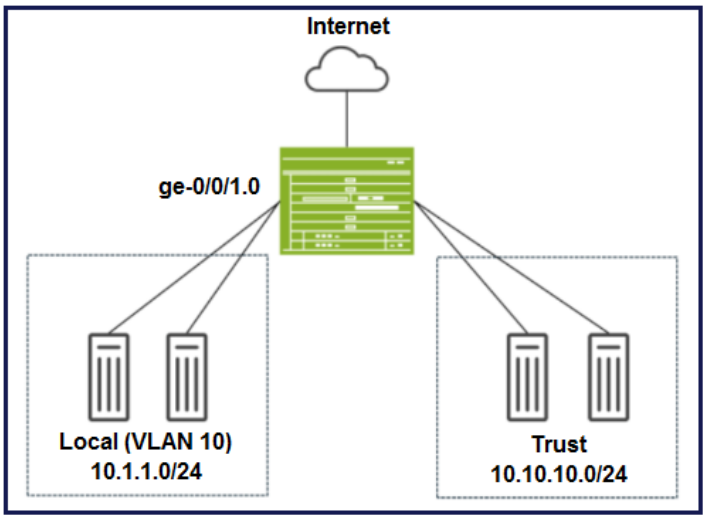
Selected Answer: BC

B and C looks fine.

upvoted 1 times

Question #34 *Topic 1*

Click the Exhibit button.



You have deployed an SRX Series device as shown in the exhibit. The devices in the Local zone have recently been added but their SRX interfaces have not been configured. You must configure the SRX to meet the following requirements: devices in the 10.1.1.0/24 network can communicate with other devices in the same network, but not with other networks or the SRX. you must be able to apply security policies to traffic flows between devices in the Local zone.

Which three configuration elements will be required as part of your configuration? (Choose three.)

A. set protocols 12-learning global-mode switching

B. set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan-members 10

C. set security zones security-zone Local interfaces ge-0/0/1.0

D. set protocols 12-learning global-mode transparent-bridge

E. set security zones security-zone Local interfaces irb.10

Suggested Answer: *BCE*

Community vote distribution

BCD (100%)

inmymind84 3 months ago

Selected Answer: BCD

B,C,D are required.

upvoted 1 times

Question #35 *Topic 1*

Click the Exhibit button.

```
user@srx> show ethernet-switching global-information
Global Configuration:
MAC aging interval       : 300
MAC learning             : Enabled
MAC statistics      : Disabled
MAC limit Count          : 65536
MAC limit hit            : Disabled
MAC packet action drop   : Disabled
MAC+IP aging interval    : IPv4 - 1200 seconds
                      IPv6 - 1200 seconds
MAC+IP limit Count       : 65536
MAC+IP limit reached     : No
LE aging time            : 1200
LE VLAN aging time       : 1200
Global Mode              : Transparent bridge
RE state                 : Master
VXLAN Overlay load bal   : Disabled
VXLAN ECMP               : Disabled
Fast Update              : Disabled
Host Pkts GBP src tag    : 0
[edit interfaces]
user@srx# show
ge=0/0/0 {
     unit 0 {
          family ethernet-switching {
               vlan {
                    members v100;
               }
          }
     }
}
ge=0/0/1 {
     unit 0 {
          family inet {
               address 172.16.0.1./24;
          }
     }
}
```

Referring to the exhibit, in which mode is the SRX Series device?

A. transparent

B. packet

C. mixed

D. Ethernet switching

Suggested Answer: *A*

Community vote distribution

C (100%)

inmymind84 3 months ago

Selected Answer: C

there are l3 interfaces so it is mixed mode not transparent.

upvoted 2 times

Question #36 *Topic 1*

You are asked to connect two hosts that are directly connected to an SRX Series device. The traffic should flow unchanged as it passes through the SRX, and routing or switch lookups should not be performed. However, the traffic should still be subjected to security policy checks.
What will provide this functionality?

A. transparent mode

B. secure wire

C. MACsec

D. mixed mode

Suggested Answer: *A*

Community vote distribution

B (100%)

75e7ed9 5 days, 4 hours ago

Selected Answer: B

Secure Wire is a feature that binds two interfaces together at Layer 2, forwarding traffic between them without routing or switching lookups.

upvoted 1 times

Question #37 *Topic 1*

How does an SRX Series device examine exception traffic?

A. The device examines the host-outbound traffic for the ingress interface and zone.

B. The device examines the host-inbound traffic for the ingress interface and zone.

C. The device examines the host-outbound traffic for the egress interface and zone.

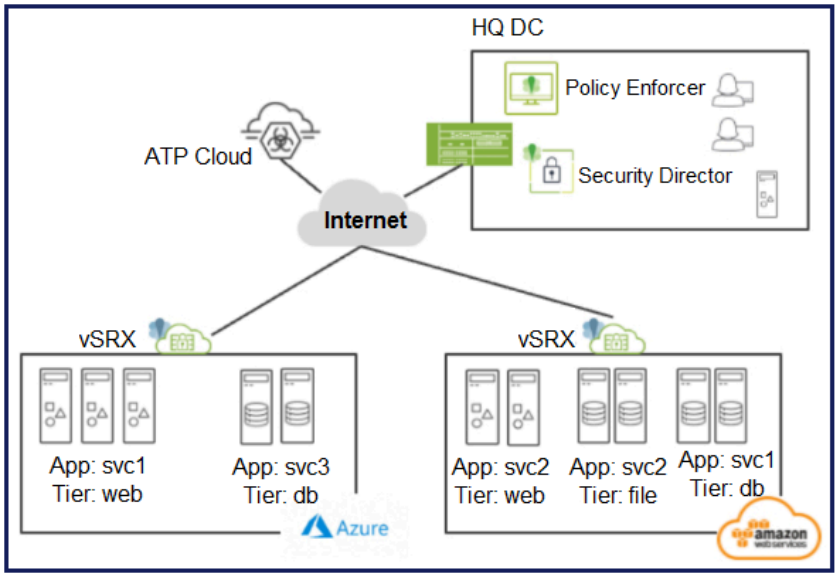
D. The device examines the host-inbound traffic for the egress interface and zone.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #38 *Topic 1*

Click the Exhibit button.



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 security tags in the security policies.

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

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

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #39 *Topic 1*

Click the Exhibit button.

```
[edit class-of-service]
user@srx# show
classifiers {
dscp ba-classifier {
     import default;
     forwarding-class best-effort {
          loss-priority high code-points 000000;
     }
     forwarding-class ef-class {
          loss-priority high code-points 000001;
     }
     forwarding-class af-class {
          loss-priority high code-points 001010;
     }
     forwarding-class network-control {
          loss-priority high code-points 000011;
     }
     forwarding-class res-class {
          loss-priority high code-points 000100;
     }
     forwarding-class web-data {
          loss-priority high code-points 000101;
     }
     forwarding-class control-data {
          loss-priority high code-points 000111;
     }
     forwarding-class voip-data {
          loss-priority high code-points 000110;
     }
     forwarding-class DB-data {
          loss-priority high code-points 111111;
     }
   }
}
```

You have configured a CoS-based VPN that is not functioning correctly.
Referring to the exhibit, which action will solve the problem?

A. You must change the loss priorities of the forwarding classes to low.

B. You must delete one forwarding class.

C. You must change the code point for the DB-data forwarding class to 10000.

D. You must use inet precedence instead of DSCP.

Suggested Answer: *C*

Community vote distribution

B (100%)

5000a98 1 month, 2 weeks ago

Selected Answer: B

You can configure up to 8 forwarding classes (FC) for a VPN with the multi-sa forwarding-classes configuration statement at the [edit security ipsec vpn vpn-name] hierarchy level. The number of IPsec SAs negotiated with a peer gateway is based on the number of FCs configured for the VPN (https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topic-map/security-cos-based-ipsec-vpns.html)

upvoted 1 times

Question #40 *Topic 1*

You configure two Ethernet interfaces on your SRX Series device as Layer 2 interfaces and add them to the same VLAN. The SRx is using the default 12-learning setting. You do not add the interfaces to a security zone.
Which two statements are true in this scenario? (Choose two.)

A. You cannot add Layer 2 interfaces to a security zone.

B. You are unable to apply stateful security features to traffic that is switched between the two interfaces.

C. The interfaces will not forward traffic by default.

D. You are able to apply stateful security features to traffic that enters and exits the VLAN.

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #41 *Topic 1*

You are enabling advanced policy-based routing. You have configured a static route that has a next hop from the inet0 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 filter-based forwarding.

B. Use policies.

C. Use RIB groups.

D. Use transparent mode.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #42 *Topic 1*

Click the Exhibit button.

```
user@peer1> show chassis high-availability information
Node failure codes:
HW Hardware monitoring LB Loopback monitoring
MB Mbuf monitoring SP SPU monitoring
CS Cold Sync monitoring SU Software Upgrade
Node Status: ONLINE
Local-id: 1
Local-IP: 10.10.1.1
HA Peer Information:
Peer Id: 2 IP address: 10.10.1.2 Interface: ge-0/0/1.0
Routing Instance: default
Encrypted: NO Conn State: UP
Cold Sync Status: COMPLETE
Services Redundancy Group: 0
Current State: ONLINE
Peer Information:
Peer Id: 2
SRG failure event codes:
BF BFD monitoring
IP IP monitoring
IF Interface monitoring
CP Control Plane monitoring
Services Redundancy Group: 1
Deployment Type: SWITCHING
Status: ACTIVE
Activeness Priority: 200
Preemption: ENABLED
Process Packet In Backup State: No
Control Plane State: READY
System Integrity Check: N/A
Failure Events: NONE
Peer Information:
Peer Id: 2
Status: BACKUP
Health Status: HEALTHY
Failover Readiness: READY
```

Referring to the exhibit, which statement is true?

A. SRG1 is configured in hybrid mode.

B. The ICL is encrypted.

C. If SRG1 moves to peer 2, peer 1 will forward packets sent to the SRG1 interfaces.

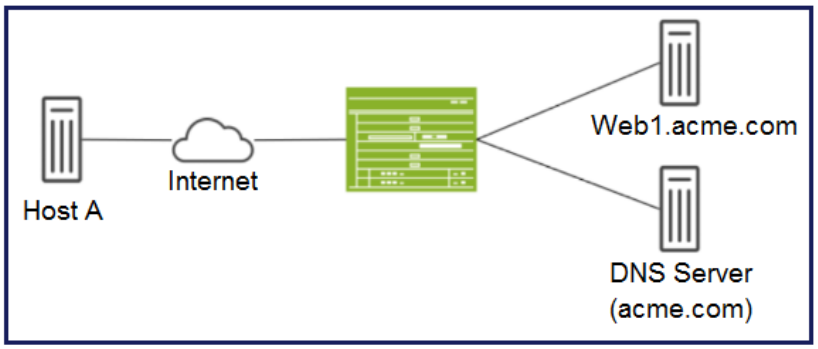
D. If SRG1 moves to peer 2, peer 1 will drop packets sent to the SRG1 interfaces.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #43 *Topic 1*

Click the Exhibit button.



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. double NAT

B. STUN protocol

C. DNS doctoring

D. persistent NAT

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #44 *Topic 1*

Your IPsec tunnel is configured with multiple security associations (SAs). Your SRX Series devices supports the CoS-based IPsec VPNs with multiple IPsec SAs feature. You are asked to configure CoS for this tunnel.
Which two statements are true in this scenario? (Choose two.)

A. A maximum of four forwarding classes can be configured for a VPN with the multi-sa forwarding-classes statement.

B. The local and remote gateways do not need the forwarding classes to be defined in the same order.

C. A maximum of eight forwarding classes can be configured for a VPN with the –multi-sa forwarding-classes– statement.

D. The local and remote gateways must have the forwarding classes defined in the same order.

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #45 *Topic 1*

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. persistent NAT

B. address persistence

C. STUN

D. double NAT

Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #46 *Topic 1*

Click the Exhibit button.

```
[edit protocols ospf]
user@ADVP-HUB# show
area 0.0.0.0 {
     interface st0.0 {
          demand-circuit;
     }
     interface ge-0/0/3.0 {
          passive;
     }
}
```

An ADVPN configuration has been verified on both the hub and spoke devices and it seems fine. However, OSPF is not functioning as expected. Referring to the exhibit, which two statements under interface st0.0 on both the hub and spoke devices would solve this problem? (Choose two.)

A. passive

B. dynamic-neighbors

C. interface-type p2mp

D. interface-type p2p

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!