



- Expert Verified, Online, **Free**.

Regarding static attack object groups, which two statements are true? (Choose two.)

- A. Matching attack objects are automatically added to a custom group.
- B. Group membership automatically changes when Juniper updates the IPS signature database.
- C. Group membership does not automatically change when Juniper updates the IPS signature database.
- D. You must manually add matching attack objects to a custom group.

Suggested Answer: CD

Community vote distribution

AB (100%)

 **Dimsop_Technology** 1 month ago

Selected Answer: CD

C and D is correct <https://www.juniper.net/documentation/mx/es/software/junos/idp-policy/topics/topic-map/security-idp-attack-objects-groups.html>

upvoted 1 times

 **quraitulain** 6 months ago

C and D is correct

upvoted 2 times

 **masterkingkhan** 8 months ago

A static attack group is essentially a group to which you manually add attack objects and groups (both predefined and custom) that will not add members during attack updates. If attack objects are modified as part of an attack update, they are updated in the group; if they are deleted, they are removed from the group. No new attack objects are added to this group, however. Static groups are very useful if you want strict control over adding new attacks into attack groups during signature updates to ensure that you don't cause unexpected results with new attack objects. The only things you need to define for static groups are the members that are added to this group.

upvoted 1 times

 **masterkingkhan** 8 months ago

Dynamic attack groups provide administrators with a powerful ability to adjust to new threats when new attack objects are downloaded from Juniper. Whereas static attack groups allow you to create groups that don't automatically change with signature attack updates, dynamic attack groups do change. And they have very intelligent controls for defining what should be added or removed with attack updates. Dynamic attack groups use filters to define the attributes of attack objects that would select them to be implemented in the group. Additionally, you can override members in the groups to exclude them if need be.

upvoted 1 times

 **masterkingkhan** 8 months, 1 week ago

for dynamci - A dynamic group contains attack objects that are automatically added or deleted based on specified criteria for the group

upvoted 1 times

 **masterkingkhan** 8 months, 1 week ago

the only difference is one says static and q93 says dynamic, i think for static its C+D


static attack object groups are predefined groups of attack objects that are included in Juniper's IPS signature database. These groups do not change automatically when Juniper updates the database2.

upvoted 1 times

 **masterkingkhan** 8 months, 1 week ago

hi 66dc178

upvoted 1 times

 **66dc178** 8 months, 2 weeks ago

Selected Answer: AB

duplicate with question 93

upvoted 1 times

You are asked to reduce the load that the JIMS server places on your corporate domain controller. Which action should you take in this situation?

- A. Connect JIMS to the RADIUS server.
- B. Connect JIMS to the domain Exchange server.
- C. Connect JIMS to the domain SQL server.
- D. Connect JIMS to another SRX Series device.

Suggested Answer: A


Community vote distribution

A (75%)

B (25%)

 **quraitulain** 6 months ago


I think B since its either Domain controller or the exchange server
upvoted 1 times

 **66dc178** 9 months, 2 weeks ago

Selected Answer: A

Connect JIMS to the RADIUS server: RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. By connecting JIMS to a RADIUS server, authentication requests can be offloaded from the domain controller to the RADIUS server. This reduces the load on the domain controller because the RADIUS server can handle a portion of the authentication and authorization tasks.

upvoted 3 times

 **66dc178** 8 months, 3 weeks ago

If JIMS is configured to use a RADIUS server for authentication requests, the RADIUS server would handle these requests instead of the domain controllers. Since RADIUS servers are designed to handle a large volume of authentication and accounting requests, this could offload a significant amount of work from the domain controllers.

upvoted 1 times

 **tk24** 1 year ago

B are Corret
upvoted 1 times

 **ChillingAgain** 1 year ago

Selected Answer: B

JIMS uses eventlogs on Domain contollers or Exchange Servers to determine logon events. So to decrease the load on a Domain Controller you could use the Exchange Server to read logs.

upvoted 1 times

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

- A. Unified security policies require an advanced feature license.
- B. Unified security policies are evaluated after global security policies.
- C. Traffic can initially match multiple unified security policies.
- D. APPID results are used to determine the final security policy match.

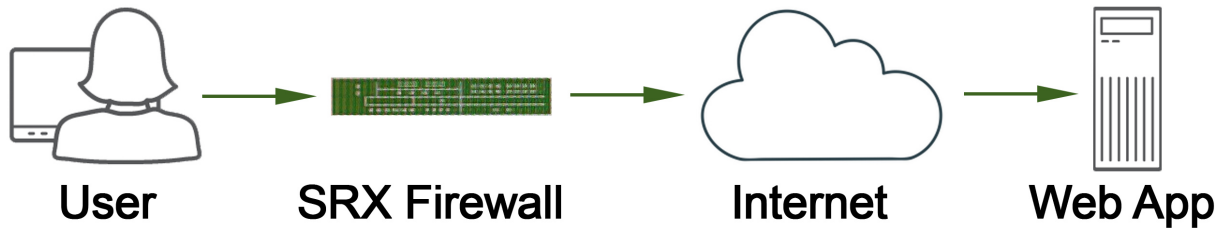
Suggested Answer: *CD*

  **quraitulain** 6 months ago

C and D are correct

upvoted 1 times

Click the Exhibit button.



Referring to the exhibit, which two statements describe the type of proxy used? (Choose two.)

- A. forward proxy
- B. client protection proxy
- C. server protection proxy
- D. reverse proxy

Suggested Answer: AB

Community vote distribution

AB (100%)

e990bbd 3 months, 2 weeks ago

Correct A B

SRX Series Firewall support following types of SSL proxy:

-Client-protection SSL proxy also known as forward proxy—The SRX Series Firewall resides between the internal client and outside server. Proxying outbound session, that is, locally initiated SSL session to the Internet. It decrypts and inspects traffic from internal users to the web.

-Server-protection SSL proxy also known as reverse proxy—The SRX Series Firewall resides between the internal server and outside client. Proxying inbound session, that is, externally initiated SSL sessions from the Internet to the local server.

upvoted 1 times

quraitulain 6 months ago

Forward and client protection ssl certificate

upvoted 1 times

masterkingkhan 8 months ago

A+B correct

upvoted 1 times

longanghi 1 year ago

Selected Answer: AB

A,B correct

upvoted 3 times

ChillingAgain 1 year ago

A,B Correct

upvoted 2 times

gondaliya 1 year, 1 month ago

A and B are Correct

upvoted 2 times

You have deployed an SRX300 Series device and determined that files have stopped being scanned. In this scenario, what is a reason for this problem?

- A. The software license is a free model and only scans executable type files.
- B. The infected host communicated with a command-and-control server, but it did not download malware.
- C. The file is too small to have a virus.
- D. You have exceeded the maximum files submission for your SRX platform size.

Suggested Answer: *D*

  **quraitulain** 6 months ago

D is correct

upvoted 1 times

Which three statements about SRX Series device chassis clusters are true? (Choose three.)

- A. Chassis cluster control links must be configured using RFC 1918 IP addresses.
- B. Chassis cluster member devices synchronize configuration using the control link.
- C. A control link failure causes the secondary cluster node to be disabled.
- D. Recovery from a control link failure requires that the secondary member device be rebooted.
- E. Heartbeat messages verify that the chassis cluster control link is working.

Suggested Answer: BCE

Community vote distribution

BE (67%)

BCE (33%)

🗨️ 👤 **Hyde** 10 months ago

B, C, & E are correct.
upvoted 1 times

🗨️ 👤 **OkoJun** 10 months, 1 week ago

B,C,E are correct answers
upvoted 2 times

🗨️ 👤 **longanghi** 1 year ago

Selected Answer: BCE

C also correct <https://supportportal.juniper.net/s/article/SRX-Secondary-node-of-a-Chassis-Cluster-is-in-Disabled-state-how-do-you-find-the-cause>
upvoted 1 times

🗨️ 👤 **gondaliya** 1 year, 1 month ago

Selected Answer: BE

only two is correct. B and E
upvoted 2 times

When a security policy is deleted, which statement is correct about the default behavior for active sessions allowed by that policy?

- A. The active sessions allowed by the policy will be dropped.
- B. The active sessions allowed by the policy will be marked as a legacy flow and will continue to be forwarded.
- C. The active sessions allowed by the policy will be reevaluated by the cached policy rules.
- D. The active sessions allowed by the policy will continue unchanged.

Suggested Answer: A

Community vote distribution

A (60%)

B (40%)

🗨️ 👤 **quraitulain** 6 months ago

A is the right answer
upvoted 1 times

🗨️ 👤 **masterkingkhan** 8 months ago

sorry bit confused now-
if you deactivate/rename/DELETE a policy that has an existing session the default behaviour is to drop, even if you have the policy re-match enabled it still drops the active session

if you change the src/dest/app default behaviour is "continue to open session" with policy re-match it re-evaluates

if you change action from permit to deny - default behaviour is "continue to open session" with policy re-match it drops the active session
upvoted 2 times

🗨️ 👤 **masterkingkhan** 8 months ago

The details of the session flow are placed in a session table which is a real time list of current sessions on the srx. Only connections that are active or havent timed out show up in the session table.

which means if the policy is deleted the active sessions are still in the session table and eventually will time out
upvoted 3 times

🗨️ 👤 **masterkingkhan** 8 months, 1 week ago

B is correct -
To solve this you have to enable "policy-rematch" under security policies... otherwise existing sessions are kept open until they time out. Enabling policy-rematch existing sessions will be reevaluated with the newly updated ruleset.
upvoted 1 times

🗨️ 👤 **66dc178** 8 months, 3 weeks ago

Selected Answer: B

When a security policy is deleted in a Juniper SRX device, the default behavior for active sessions that were allowed by that policy is that they continue to flow as long as the session remains active. New flows will not be created under the deleted policy, but existing flows stay active until they age out. The "policy-rematch" feature can be configured to cause all active sessions to be re-evaluated against the security policies upon a commit, and sessions will be torn down if they are no longer permitted
upvoted 2 times

🗨️ 👤 **RickyB** 8 months, 4 weeks ago

B is correct as flows will timeout eventually but are not immediately dropped. Need re-match enabled for that.
upvoted 1 times

🗨️ 👤 **OkoJun** 10 months, 1 week ago

sorry my mistake. A is correct If the rule is deleted all sessions are dropped.
upvoted 1 times

🗨️ 👤 **OkoJun** 10 months, 3 weeks ago

D is Correct
Traffic matching an established session will continue to flow as long as that session remains active. You need to configure "set security policies

policy-rematch" if you want to delete the active sessions.

see : <https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/statement/security-edit-policy-rematch.html>

upvoted 1 times

  **TECH3K3** 10 months, 2 weeks ago

The link you provided does not support your claim, If anything it supports answer A

upvoted 1 times

  **longanghi** 1 year ago

Selected Answer: A

A correct



upvoted 1 times

  **ChillingAgain** 1 year ago

Selected Answer: A

A is correct. Deleted policy always immediately drops current sessions. Does not matter if policy rematch is enabled or not.

upvoted 1 times

  **gondaliya** 1 year, 1 month ago

Selected Answer: A

A is correct

upvoted 1 times

How does the SSL proxy detect if encryption is being used?

- A. It uses application identity services.
- B. It verifies the length of the packet.
- C. It queries the client device.
- D. It looks at the destination port number.

Suggested Answer: D

Community vote distribution

A (100%)

  **ChillingAgain** Highly Voted 1 year ago

Correct answer is A:

SSL proxy uses application identification services to dynamically detect if a particular session is SSL encrypted.

<https://www.juniper.net/documentation/us/en/software/junos/application-identification/topics/topic-map/security-ssl-proxy-unified-policies.html>

upvoted 5 times

  **MM_NSS** Most Recent 3 months, 2 weeks ago

Selected Answer: A

SSL proxy uses application identification services to dynamically detect if a particular session is SSL encrypted.

upvoted 2 times

  **quraitulain** 6 months ago

A is correct .SSL proxy uses application identification services to dynamically detect if a particular session is SSL encrypted.



upvoted 1 times

  **masterkingkhan** 8 months, 1 week ago

A is correct

SSL proxy uses application identification services to dynamically detect if a particular session is SSL encrypted.

upvoted 1 times

  **OkoJun** 10 months, 2 weeks ago

A is correct

APPID is used for APPTrack, APPFW, APPQoS, SSL proxy and IPS

upvoted 1 times

Which two statements are correct when considering IPS rule base evaluation? (Choose two.)

- A. IPS evaluates rules concurrently.
- B. IPS applies the most severe action to traffic matching multiple rules.
- C. IPS evaluates rules sequentially.
- D. IPS applies the least severe action to traffic matching multiple rules.

Suggested Answer: BC

Community vote distribution

BC (100%)

🗨️ **masterkingkhan** 8 months ago

B+C are correct

the policy rules are evaluated in numerical order policy1 before policy2 and so on
upvoted 1 times

🗨️ **66dc178** 8 months, 3 weeks ago

Selected Answer: BC

C. IPS evaluates rules sequentially. This means that the rules within an IPS policy are processed in a specific order, typically from top to bottom.

B. IPS applies the most severe action to traffic matching multiple rules. When traffic matches more than one rule, the action taken will be the most severe one specified among the matching rules.

upvoted 1 times

🗨️ **longanghi** 1 year ago

Selected Answer: BC

B,C correct.

upvoted 1 times

🗨️ **ChillingAgain** 1 year ago

Selected Answer: BC

B and C are correct.

upvoted 1 times

🗨️ **ChillingAgain** 1 year ago

B and C are correct.

upvoted 1 times

🗨️ **gondaliya** 1 year, 1 month ago

Selected Answer: BC

B and C are Current



upvoted 2 times

You have implemented a vSRX in your VMware environment. You want to implement a second vSRX Series device and enable chassis clustering.

Which two statements are correct in this scenario about the control-link settings. (Choose two.)

- A. In the vSwitch security settings, accept promiscuous mode.
- B. In the vSwitch properties settings, set the VLAN ID to None.
- C. In the vSwitch security settings, reject forged transmits.
- D. In the vSwitch security settings, reject MAC address changes.

Suggested Answer: AB

  **e990bbd** 3 months, 2 weeks ago

Correct A and B

Creating the Control Link Connection Using VMware

<<https://www.juniper.net/documentation/us/en/software/vsrx/vsrx-consolidated-deployment-guide/vsrx-vmware/topics/task/security-vsrx-cluster-stage-provisioning-vmware.html#creating-the-control-link-connection-using-vmware>>

2.Click Add Networking to create a vSwitch for the control link

<snip>

Port Group Properties

Network Label: HA Control

VLAN ID: None(0) <<<<

<snip>

4.Set the promiscuous mode to Accept, and click OK, as shown in Figure 1 <<<

upvoted 1 times

  **quraitulain** 6 months ago

A and C are correct

upvoted 1 times

Your manager asks you to provide firewall and NAT services in a private cloud.

Which two solutions will fulfill the minimum requirements for this deployment? (Choose two.)

- A. a single vSRX
- B. a vSRX for firewall services and a separate vSRX for NAT services
- C. a cSRX for firewall services and a separate cSRX for NAT services
- D. a single cSRX



Suggested Answer: AD

  **Dimsop_Technology** 1 month ago

Selected Answer: AC



A y C la documentacion lo dice en microservicios de contenedores

upvoted 1 times

  **37660e8** 2 months, 2 weeks ago

A&C is correct

upvoted 1 times

  **subsonline** 2 months, 2 weeks ago

A & C

from Juniper Open learning JNCIS-SEC materials

upvoted 1 times


Which two statements are true about mixing traditional and unified security policies? (Choose two.)

- A. When a packet matches a unified security policy, the evaluation process terminates.
- B. Traditional security policies must come before unified security policies.
- C. Unified security policies must come before traditional security policies.
- D. When a packet matches a traditional security policy, the evaluation process terminates.

Suggested Answer: *BD*

Community vote distribution

BD (100%)

  **gondaliya** 1 year, 1 month ago

Selected Answer: BD

Correct answer B and D

upvoted 1 times

Which two features are configurable on Juniper Secure Analytics (JSA) to ensure that alerts are triggered when matching certain criteria? (Choose two.)

- A. building blocks
- B. assets
- C. events
- D. tests

Suggested Answer: AC

Community vote distribution

AC (100%)

🗳️ 👤 **pollzolo1** 7 months ago

B e C correct.
upvoted 2 times

🗳️ 👤 **66dc178** 8 months, 3 weeks ago

Selected Answer: AC

"building blocks" are predefined or customizable elements that can be used to construct more complex rules or criteria for monitoring and alerting within a system. They act as foundational components, encapsulating specific attributes, conditions, or logic, which can then be reused across various configurations to streamline the setup and maintenance of security policies or analytics. This modular approach enhances flexibility and efficiency in defining security rules and alerts

upvoted 2 times

🗳️ 👤 **kollie** 1 year ago

The two features that are configurable on Juniper Secure Analytics (JSA) to ensure that alerts are triggered when matching certain criteria are:

- B. assets
- C. events

Explanation:

Assets (Option B):

In JSA, assets refer to the entities within your network, such as hosts, routers, or switches. You can configure rules and alerts based on activities related to specific assets. For example, you might want to receive an alert when there is suspicious activity associated with a particular server or network device.

Events (Option C):

JSA collects and analyzes events from various sources, including logs and network traffic. You can configure rules and alerts based on specific events or patterns in the data. For instance, you might set up an alert for multiple failed login attempts or an unusual spike in network traffic.

Building blocks

upvoted 2 times

🗳️ 👤 **gondaliya** 1 year, 1 month ago

Selected Answer: AC

A,C correct
upvoted 2 times

Which two statements are correct about Juniper ATP Cloud? (Choose two.)

- A. Once the target threshold is met, Juniper ATP Cloud continues looking for threats from 0 to 5 minutes.
- B. Once the target threshold is met, Juniper ATP Cloud continues looking for threats from 0 to 10 minutes.
- C. The threat levels range from 0-10.
- D. The threat levels range from 0-100.

Suggested Answer: AC

Community vote distribution

AC (100%)

  **longanghi** 1 year ago

Selected Answer: AC

A and C Correct
upvoted 2 times

  **kollie** 1 year ago

The correct statements about Juniper ATP Cloud are:

- B. Once the target threshold is met, Juniper ATP Cloud continues looking for threats from 0 to 10 minutes.
- C. The threat levels range from 0-10.

These statements reflect the behavior an
upvoted 3 times

  **gondaliya** 1 year, 1 month ago

Selected Answer: AC

A and C Correct
upvoted 3 times

You enable chassis clustering on two devices and assign a cluster ID and a node ID to each device.

In this scenario, what is the correct order for rebooting the devices?

- A. Reboot the secondary device, then the primary device.
- B. Reboot only the secondary device since the primary will assign itself the correct cluster and node ID.
- C. Reboot the primary device, then the secondary device.
- D. Reboot only the primary device since the secondary will assign itself the correct cluster and node ID.

Suggested Answer: A

Community vote distribution

C (100%)

🗨️ **masterkingkhan** 7 months, 3 weeks ago

C is correct

you connect to the console port on the primary device, give it a node ID, and identify the cluster it will belong to, and then reboot the system. You then connect the console port to the other device, give it a node ID, and assign it the same cluster ID you gave to the first node, and then reboot the system. In both instances, you can cause the system to boot automatically by including the reboot parameter in the CLI command line.

upvoted 1 times

🗨️ **longanghi** 1 year ago

Selected Answer: C

C is correct

upvoted 1 times

🗨️ **kollie** 1 year ago

In a Juniper Networks chassis clustering setup, when you enable chassis clustering on two devices and assign a cluster ID and a node ID to each device, the correct order for rebooting the devices is:

C. Reboot the primary device, then the secondary device.

Explanation:

After assigning the cluster ID and node ID to each device, it is a good practice to reboot the primary device first. This ensures that the primary device comes online with the specified cluster and node IDs.

Once the primary device is up and running, you can then reboot the secondary device. The secondary device will recognize the existing cluster and node IDs assigned to the primary device and join the cluster accordingly.

So, the correct sequence is to reboot the primary device first and then the secondary device to establish the chassis cluster in the desired configuration.

Option A is incorrect because the secondary device should be rebooted after the primary device.

Options B and D are not accurate because both devices need to be rebooted, and the order is important for proper clustering.

upvoted 3 times

You want to deploy a virtualized SRX in your environment.

In this scenario, why would you use a vSRX instead of a cSRX? (Choose two.)

- A. The vSRX supports Layer 2 and Layer 3 configurations.
- B. Only the vSRX provides clustering.
- C. The vSRX has faster boot times.
- D. Only the vSRX provides NAT, IPS, and UTM services.

Suggested Answer: AB

Community vote distribution

AB (100%)

  **ChillingAgain** 1 year ago

Selected Answer: AB

<https://www.juniper.net/documentation/us/en/software/csr/csr-linux-deployment/topics/concept/security-csr-docker-overview.html>
upvoted 2 times

Click the Exhibit button.

```
user@srx> show services user-identification authentication-table authentication-  
source identity-management extensive  
Logical System: root-logical-system  
Domain: juniper.net  
Total entries: 1  
  Source-ip: 172.25.11.140  
    Username: nancy  
      Groups:posture-healthy, administrators, users, domain admins, domain users,  
executives  
    State: Valid  
    Source: JIMS- Active Directory  
    Access start date: 2022-05-28  
    Access start time: 21:53:52  
    Last updated timestamp: 2022-05-29 10:43:44  
    Age time: 46
```

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

- A. Nancy logged in to the juniper.net Active Directory domain.
- B. The IP address of Nancy's client PC is 172.25.11.140.
- C. The IP address of the authenticating domain controller is 172.25.11.140.
- D. Nancy is a member of the Active Directory sales group.

Suggested Answer: AB

Community vote distribution

AB (100%)

 **RickyB** 8 months, 4 weeks ago

Selected Answer: AB

Domain

Domain:

Name of the domain that the users belong to. User identity and authentication information is display for all users who belong to the domain and for whom there are entries in the specified authentication source table or repository.

Source IP:

The IP address of the user's device. If a user is logged in to the network with more than one device, a separate entry is created for the user for each device. It showing the devices IP address.

upvoted 1 times