EXAMTOPICS

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



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

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

A. a source port

B. a destination port

C. zone context

D. an action

Suggested Answer: *C, D*

gpt_test Most Recent 2 years, 1 month ago

Selected Answer: CD

C. zone context and D. an action

Explanation:

Zone context: A zone-based security policy defines rules based on zones, which group interfaces with similar security requirements. The policy needs to specify the source and destination zones to determine the flow of traffic between them. Action: Every security policy includes an action to specify what should happen when the traffic matches the policy. Actions typically include allow, deny, or log. Other options:

Source port and destination port: While these can be part of a policy, they are not required criteria for a zone-based security policy. The primary elements of such a policy are zones and the action to take.

upvoted 1 times

quraitulain 2 years, 6 months ago

C D is the answer

upvoted 1 times

westh4m1234 2 years, 7 months ago

YEP CD

upvoted 1 times

longanghi 2 years, 7 months ago

Selected Answer: CD

CD is correct

upvoted 1 times

JaredM 2 years, 8 months ago

Selected Answer: CD

Ports not required in zone based policies

upvoted 1 times

Engg_flint 3 years ago

C and D

upvoted 1 times

Taweke 3 years, 3 months ago

no need source port and destination port but use application

upvoted 1 times

fosi130 3 years, 5 months ago

CD is the answer

upvoted 1 times

Rbrahmi 3 years, 8 months ago

Selected Answer: CD

CD are the correct answers

upvoted 2 times

bigmokey 3 years, 9 months ago

Selected Answer: CD

no mention of port, does have application Security Policy Structure + Name + Context + From-zone & to-zone + Rules + Match criteria + Source address + Destination address + Application + Identity (user-based firewall) + Action

upvoted 1 times

mohdema 3 years, 11 months ago

Selected Answer: AB

A security policy is a set of statements that controls traffic from a specified source to a specified destination using a specified service. A policy permits, denies, or tunnels specified types of traffic unidirectionally between two points.

Each policy consists of:

A unique name for the policy. A from-zone and a to-zone, for example: user@host# set security policies from-zone untrust to-zone untrust A set of match criteria defining the conditions that must be satisfied to apply the policy rule. The match criteria are based on a source IP address, destination IP address, and applications. The user identity firewall provides greater granularity by including an additional tuple, source-identity, as part of the policy statement. A set of actions to be performed in case of a match—permit, deny, or reject. Accounting and auditing elements—counting, logging, or structured system logging.

~~~~Action is not a match criteria

https://www.juniper.net/documentation/us/en/software/junos/security-policies/topics/topic-map/security-policy-configuration.html

upvoted 2 times

mohdema 3 years, 11 months ago

In a Junos OS stateful firewall, the security policies enforce rules for transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on traffic as it passes through the firewall. From the perspective of security policies, the traffic enters one security zone and exits another security zone. This combination of a from-zone and to-zone is called a context. Each context contains an ordered list of policies. Each policy is processed in the order that it is defined within a context.

upvoted 2 times

Bubu3k 3 years, 11 months ago

Selected Answer: CD

I think it should be the zone context (from zone to zone) and an action

upvoted 3 times

mohdema 3 years, 11 months ago

I think it's src and dst https://www.juniper.net/documentation/us/en/software/junos/security-policies/topics/topic-map/security-policy-configuration.html

upvoted 2 times
~~~~

Question #2 *Topic 1*

You are assigned a project to configure SRX Series devices to allow connections to your webservers. The webservers have a private IP address, and the packets must use NAT to be accessible from the Internet. You do not want the webservers to initiate connections with external update servers on the Internet using the same IP address as customers use to access them.
Which two NAT types must be used to complete this project? (Choose two.)

A. static NAT

B. hairpin NAT

C. destination NAT

D. source NAT

Suggested Answer: *C, D*

netsolutionghy Most Recent 2 years ago
Static NAT is not because, Static NAT uses the same IP for imcoming & outgoing traffic. Correct answer is Source NAT & Destination NAT i.e. C & D
upvoted 1 times

gpt_test 2 years, 1 month ago
Selected Answer: AC
A. static NAT and C. destination NAT

Explanation:

Static NAT: This type of NAT is used to map a public IP address to a private IP address, allowing external clients to access internal resources like webservers. The public IP will always map to the same private IP, ensuring consistent access. Destination NAT: This type of NAT is used to translate the destination IP address of incoming packets to the private IP address of the webservers. This allows traffic directed at a public IP address to be forwarded to the correct internal server. Other options:

Hairpin NAT: This is used when internal clients need to access services hosted on the same internal network via their public IP address, which is not relevant here. Source NAT: This is typically used for internal hosts to access external networks, which is not needed since the webservers are not initiating outbound connections.
upvoted 1 times

Fr3k411 2 years, 8 months ago
Static NAT defines a one-to-one mapping from one IP subnet to another IP subnet. The mapping includes destination IP address translation in one direction and source IP address translation in the reverse direction. From the NAT device, the original destination address is the virtual host IP address while the mapped-to address is the real host IP address.

So not Static NAT
upvoted 2 times

66dc178 2 years, 9 months ago
A. Static NAT D. Source NAT

Static NAT is used to provide a consistent, unchanging public IP address for your webservers when accessed from the Internet, allowing inbound connections to them.

Source NAT is used for outbound connections initiated by your webservers to external servers, allowing you to translate their private IP addresses to a different public IP address, ensuring that the IP used for incoming web traffic is not the same as the one used for the servers' outbound connections.
upvoted 1 times

fosi130 3 years, 3 months ago
CD as response
upvoted 2 times

Question #3 *Topic 1*

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

A. user@srx> show system license

B. user@srx> show services accounting

C. user@srx> show configuration system

D. user@srx> show chassis firmware

Suggested Answer: *A*

gpt_test Most Recent 2 years, 1 month ago

Selected Answer: A

A. user@srx> show system license

Explanation: The show system license command provides detailed information about the licenses installed on an SRX Series device, including whether the AppSecure license is present. This command will display the status, expiration dates, and other relevant license details.

Other options:

B. show services accounting: This command provides information about service usage, but not about installed licenses. C. show configuration system: This command shows the system configuration but does not provide license details. D. show chassis firmware: This command displays firmware details for the device chassis, which is unrelated to licenses.

upvoted 1 times

Question #4 *Topic 1*

Click the Exhibit button.

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

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

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

B. [edit] user@vSRX-1#

C. [edit security policies] user@vSRX-1#

D. user@vSRX-1>

Suggested Answer: *C*

Bubu3k Highly Voted 3 years, 11 months ago

Selected Answer: C

It's C

upvoted 12 times

gpt_test Most Recent 2 years, 1 month ago

Selected Answer: C

The user will be placed in the following hierarchy when the exit command is run:

C. [edit security policies] user@vSRX-1#

Explanation:

The exit command moves the user up one level in the hierarchy. In the exhibit, the user is currently in the [edit security policies from-zone trust to-zone dmz policy Trust-DMZ-Access] hierarchy. When the exit command is issued, the user will move one level up, which is [edit security policies].

upvoted 1 times

westh4m1234 2 years, 8 months ago

its is C because there are two edit commands involved [edit security policies] then you need to type edit from-zone abc to-zone def policy blah-blah which gives you the prompt below [edit security policies from-zone abc to-zone def policy blah-blah] when you exit it takes you back one step [edit security policies]

upvoted 1 times

davidrsr 3 years ago

Selected Answer: C

Tested on physical SRX. It's C.

upvoted 1 times

ars92 3 years ago

Selected Answer: C

The correct answer is C. Look carefully on the exhibit.

upvoted 1 times

TECH3K3 3 years, 1 month ago

How can so many people have confirmed on real equipment and have different results? What a joke.

upvoted 1 times

much2furious 3 years, 5 months ago

Selected Answer: B

It is B, Tested on vSRX sandbox from Juniper

jcluser@vSRX-0#

[edit security policies from-zone trust to-zone untrust] jcluser@vSRX-0# exit

[edit] jcluser@vSRX-0#

upvoted 1 times

Rbrahmi 3 years, 8 months ago

Selected Answer: A

Verified on the real device

upvoted 1 times

Rbrahmi 3 years, 7 months ago

The correct answer is C, Moderator please correct my answer

upvoted 1 times

kopcink 3 years, 8 months ago

Selected Answer: C

The answer is C - exit command takes you back to the level prior the last edit command, or exit from configuration mode - JNCIA-Junos subject.

Also, I've verified it on a device:

[edit] root# edit security policies

[edit security policies] root# edit from-zone trust to-zone dmz policy Trust-DMZ-Access

[edit security policies from-zone trust to-zone dmz policy Trust-DMZ-Access] root# exit error: missing mandatory statement: 'match' error: missing mandatory statement: 'then'

[edit security policies] root#

upvoted 2 times

OJ1 3 years, 1 month ago

C is the best answer, below is my test on a device. srx5600> edit Entering configuration mode

[edit] srx5600# edit security policies

[edit security policies] srx5600# edit from-zone trust to-zone dmz policy Trust-DMZ_access

[edit security policies from-zone trust to-zone dmz policy Trust-DMZ_access] srx5600# exit

[edit security policies] srx5600#

upvoted 1 times

bigmokey 3 years, 9 months ago

Selected Answer: B

exit Moves up the hierarchy to the previous level where you were working. This command is, in effect, the opposite of the edit command. Alternatively, you can use the quit command; exit and quit are interchangeable.

upvoted 1 times

sajiby3k 3 years, 9 months ago

Selected Answer: A

Verified by typing the command in real device.

upvoted 1 times

Question #5 *Topic 1*

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

A. Install a basic Juniper ATP license on the branch device.

B. Configure the juniper-atp user account on the branch device.

C. Register for a Juniper ATP account on https://sky.junipersecurity.net.

D. Execute the Juniper ATP script on the branch device.

Suggested Answer: *C, D*

longanghi Most Recent 2 years, 8 months ago

Selected Answer: CD

CD is correct, without license you still can use some basic feature of ATP check ATP manual for more detail.

upvoted 1 times

Adzriciz 2 years, 8 months ago

Selected Answer: AC

A & C are correct. Without have an account or license you cannot enroll the device.

upvoted 1 times

66dc178 2 years, 9 months ago

Configuring a specific user account on the device for Juniper ATP (Option B) and executing a Juniper ATP script on the device (Option D) are not standard requirements for enabling basic Juniper ATP services on an SRX device. The essential steps involve having the appropriate license and registering the device with the Juniper ATP cloud for threat management and analysis.

upvoted 2 times

Engg_flint 2 years, 11 months ago

A & C correct answers

upvoted 2 times

ars92 3 years ago

Selected Answer: CD

https://www.juniper.net/documentation/us/en/software/sky-atp/atp-cloud-user-guide/topics/concept/sky-atp-install-overview.html

upvoted 1 times

Ptxpto 3 years, 2 months ago

Selected Answer: CD

https://www.juniper.net/documentation/us/en/software/sky-atp/sky-atp/topics/concept/sky-atp-install-overview.html

upvoted 1 times

ggroch 3 years, 10 months ago

CD https://manuals.plus/m/95fded847e67e8f456453182a54526ba3224a61a337c47177244d345d1f3b19e.pdf

upvoted 4 times

Question #6 *Topic 1*

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

A. 40

B. 60

C. 50

D. 10

Suggested Answer: *C*

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

Question #7 *Topic 1*

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

A. FTP

B. SMTP

C. SNMP

D. HTTP

E. SSH

Suggested Answer: *A, B, D*

longanghi Most Recent 2 years, 7 months ago

Selected Answer: ABD

A B D is correct

upvoted 1 times

Adzriciz 2 years, 8 months ago

Selected Answer: ABD

its ABD

upvoted 1 times

66dc178 2 years, 9 months ago

Protocols like SNMP (Simple Network Management Protocol) and SSH (Secure Shell) are generally used for network management and secure remote access, respectively, and are not typically the focus of UTM inspection for threats in the same way as FTP, SMTP, and HTTP traffic.

upvoted 1 times

juanjoleandro16 2 years, 10 months ago

Selected Answer: ABD

Correct answer: ABD

upvoted 1 times

Engg_flint 2 years, 11 months ago

its ABD

upvoted 1 times

ars92 3 years ago

Selected Answer: ABD

Unified Threat Management (UTM) solutions typically inspect traffic from a variety of protocols to provide comprehensive security. While the specific protocols may vary based on the UTM solution and its capabilities, here are three common protocols that UTM systems often inspect:

HTTP (Hypertext Transfer Protocol): UTM devices commonly inspect web traffic over HTTP to detect and prevent threats such as malicious websites, phishing attempts, and malware downloads.

SMTP (Simple Mail Transfer Protocol): Email traffic is a significant vector for cyber threats. UTM solutions often inspect SMTP traffic to identify and block spam, malware attachments, and phishing emails.

FTP (File Transfer Protocol): UTM devices may inspect FTP traffic to ensure that file transfers do not involve malicious content. This helps in preventing the spread of malware through file-sharing activities.

upvoted 3 times

enkar 3 years, 2 months ago

ABD, C is wrong

upvoted 1 times

fosi130 3 years, 2 months ago

ABD for me

upvoted 1 times

libm2 3 years, 3 months ago

Selected Answer: ABD

It's ABD

upvoted 2 times

Dulgoldur 3 years, 4 months ago

Selected Answer: ABD

It's ABD

upvoted 1 times

Rbrahmi 3 years, 7 months ago

Selected Answer: ABD

It's ABD

upvoted 1 times

Bubu3k 3 years, 11 months ago

Selected Answer: ABD

It's ABD

upvoted 4 times

Totalstranger 3 years, 11 months ago

Selected Answer: ABD

https://www.inetzero.com/blog/unified-threat-management-deeper-dive-traffic-inspection/

upvoted 3 times

Question #8 *Topic 1*

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

A. before security policies are evaluated

B. as the packet enters an SRX Series device

C. only during the first path process

D. after network address translation

Suggested Answer: *D*

fosi130 Most Recent 3 years, 2 months ago

D for me

upvoted 1 times

ggroch 3 years, 10 months ago

D https://iosonounrouter.wordpress.com/2018/07/07/how-does-a-flow-based-srx-work/

upvoted 2 times

Question #9 *Topic 1*

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

A. custom objects

B. advanced security policy

C. antispam feature-profile

D. antispam UTM policy

Suggested Answer: *A*

mohdema Highly Voted 3 years, 11 months ago

Selected Answer: A

user@host# set security utm custom-objects url-pattern url-pattern-name

https://www.juniper.net/documentation/us/en/software/junos/utm/topics/topic-map/security-local-list-antispam-filtering.html

upvoted 11 times

asho22 Most Recent 2 years, 6 months ago

where do you apply any local lists that are configured? >>>feature-profile ...answer is C

upvoted 1 times

quraitulain 2 years, 6 months ago

A is the answer

upvoted 1 times

westh4m1234 2 years, 7 months ago

A is correct: For each Content Security feature, configure feature parameters in the following order:

Configure Content Security custom objects for the feature: content_copy zoom_out_map user@host# set security utm custom-objects

upvoted 1 times

Cradical 2 years, 8 months ago

Selected Answer: D

Antispam UTM Policy: This is where you would apply any local lists that you have configured for antispam purposes. In UTM (Unified Threat Management) configurations, the antispam UTM policy is the specific area where you define how the system should handle spam, including the use of local lists like blacklists or whitelists. This policy directly influences how the antispam system processes incoming mail and which email addresses or domains are blocked or allowed.

upvoted 3 times

66dc178 2 years, 9 months ago

Define the custom object : set security utm custom-objects dns-blacklist address name [BLACKLIST_NAME] value [DOMAIN_TO_BLOCK] set security utm custom-objects dns-whitelist address name [WHITELIST_NAME] value [DOMAIN_TO_ALLOW]

configure the antispam UTM policy : set security utm feature-profile anti-spam sbl profile [PROFILE_NAME] blacklist custom-object [BLACKLIST_NAME]

upvoted 1 times

Engg_flint 2 years, 11 months ago

its c, answer

upvoted 2 times

davidrsr 3 years ago

C. # set security utm feature-profile anti-spam ? Possible completions: address-blacklist Anti-spam blacklist address-whitelist Anti-spam whitelist + apply-groups Groups from which to inherit configuration data > sbl SBL settings > traceoptions Trace options for anti-spam feature

upvoted 2 times

subsonline 3 years, 3 months ago

sorry, it is applied on security policies same URL.. https://supportportal.juniper.net/s/article/SRX-Example-How-to-set-up-the-UTM-Anti-Spam-feature?language=en_US

upvoted 1 times

subsonline 3 years, 3 months ago

C anti-spam feature profile https://supportportal.juniper.net/s/article/SRX-Example-How-to-set-up-the-UTM-Anti-Spam-feature?language=en_US

upvoted 2 times

manojkp 2 years, 8 months ago

The antispam feature-profile is where you apply any local lists that are configured. The feature-profile also includes the configuration for the default spam action. Note that when you configure the antispam profile, you must either enable or disable the SBL server.

upvoted 1 times

Question #10 *Topic 1*

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

A. IP spoofing

B. ICMP flooding

C. zero-day outbreaks

D. malicious e-mail attachments

Suggested Answer: *A, B*

fosi130 Most Recent 3 years, 2 months ago

AB is correct

upvoted 1 times

mohdema 3 years, 11 months ago

Selected Answer: AB

ICMP flood

Use the ICMP flood IDS option to protect against ICMP flood attacks. An ICMP flood attack typically occurs when ICMP echo requests use all resources in responding, such that valid network traffic can no longer be processed.

The threshold value defines the number of ICMP packets per second (pps) allowed to be send to the same destination address before the device rejects further ICMP packets. IP spoofing

Use the IP address spoofing IDS option to prevent spoofing attacks. IP spoofing occurs when an invalid source address is inserted in the packet header to make the packet appear to come from a trusted source.

https://www.juniper.net/documentation/us/en/software/junos/denial-of-service/topics/topic-map/security-introduction-to-adp.html

upvoted 2 times

Question #11 *Topic 1*

Which statement about global NAT address persistence is correct?

A. The same IP address from a source NAT pool will be assigned for all sessions from a given host.

B. The same IP address from a source NAT pool is not guaranteed to be assigned for all sessions from a given host.

C. The same IP address from a destination NAT pool will be assigned for all sessions for a given host.

D. The same IP address from a destination NAT pool is not guaranteed to be assigned for all sessions for a given host.

Suggested Answer: *A*

mohdema Most Recent 3 years, 11 months ago

Selected Answer: A

Use the persistent-nat feature to ensure that all requests from the same internal transport address are mapped to the same reflexive transport address (the public IP address and port created by the NAT device closest to the STUN server). The source NAT rule action can use a source NAT pool (with or without port translation) or an egress interface.

upvoted 1 times

Question #12 *Topic 1*

You are asked to configure your SRX Series device to block all traffic from certain countries. The solution must be automatically updated as IP prefixes become allocated to those certain countries.
Which Juniper ATP solution will accomplish this task?

A. Geo IP

B. unified security policies

C. IDP

D. C&C feed

Suggested Answer: *A*

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

Question #13 *Topic 1*

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

A. IKE security associations are established during IKE Phase 1 negotiations.

B. IKE security associations are unidirectional.

C. IKE security associations are established during IKE Phase 2 negotiations.

D. IKE security associations are bidirectional.

Suggested Answer: *A, D*

westh4m1234 Most Recent 2 years, 7 months ago

A+D for me - ike Sa are bidirectional and phase1

upvoted 1 times

Totalstranger 3 years, 11 months ago

Selected Answer: AD

https://www.juniper.net/documentation/us/en/software/junos/security-services/topics/concept/ipsec-ike-overview.html

upvoted 2 times

Question #14 *Topic 1*

You want to deploy a NAT solution.
In this scenario, which solution would provide a static translation without PAT?

A. interface-based source NAT

B. pool-based NAT with address shifting

C. pool-based NAT with PAT

D. pool-based NAT without PAT

Suggested Answer: *B*

ggroch Highly Voted 3 years, 10 months ago

Selected Answer: B

Translation of the original source IP address to an IP address from a user-defined address pool by shifting the IP addresses. This type of translation is one-to-one, static, and without port address translation. If the original source IP address range is larger than the IP address range in the user-defined pool, untranslated packets are dropped. https://www.juniper.net/documentation/us/en/software/junos/nat/topics/topic-map/nat-security-source-and-source-pool.html

upvoted 6 times

nailtwo Most Recent 2 years, 7 months ago

pool-based NAT with address shifting is correct answer this type of translation is one to one static and without PAT

pool-based NAT without PAT the assoiciation between the original source IP Add is dynamic

upvoted 1 times

66dc178 2 years, 8 months ago

Selected Answer: D

address shifting" doesn't explicitly rule out the use of PAT, and without more context, it's not clear that this would provide a static translation without PAT.

upvoted 1 times

Cradical 2 years, 8 months ago

Selected Answer: D

D. Pool-based NAT without PAT: This is the solution that aligns with your requirement. Pool-based NAT without PAT implies that each internal IP address is statically mapped to a specific external IP address from a pool, without using different port numbers to distinguish between multiple internal hosts. This provides a static, one-to-one translation for each host, which is what you're looking for.

upvoted 1 times

davidrsr 3 years ago

Selected Answer: B

Just think, which one has one to one "static" mapping.

upvoted 1 times

P0wned 3 years, 2 months ago

Selected Answer: D

The correct answer is D. pool-based NAT without PAT.

In the scenario where you want to provide a static translation without Port Address Translation (PAT), you would use pool-based NAT without PAT. This solution allows for a one-to-one mapping between the internal private IP addresses and external public IP addresses without modifying the port numbers. This is often used when you need to maintain a direct correlation between internal and external IP addresses, which is useful for specific applications or scenarios.

upvoted 2 times

Juiz 3 years, 2 months ago

Selected Answer: D

https://www.juniper.net/documentation/us/en/software/junos/nat/topics/topic-map/nat-security-source-and-source-pool.html#id-understanding-source-nat-pools-without-pat

upvoted 2 times

Question #15 *Topic 1*

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

A. firewall filters

B. UTM

C. Juniper ATP Cloud

D. IPS

Suggested Answer: *C*

fosi130 Most Recent 3 years, 2 months ago

C as good response

upvoted 1 times

mohdema 3 years, 11 months ago

Selected Answer: C

Malware Sandboxing Detect and stop zero-day and commodity malware within web, email, data center, and application traffic targeted for Windows, Mac, and IoT devices. https://www.juniper.net/us/en/products/security/advanced-threat-prevention.html

upvoted 3 times

Question #16 *Topic 1*

You are configuring an SRX Series device. You have a set of servers inside your private network that need one-to-one mappings to public IP addresses.
Which NAT configuration is appropriate in this scenario?

A. source NAT with PAT

B. destination NAT

C. NAT-T

D. static NAT

Suggested Answer: *D*

P0wned Most Recent 3 years, 2 months ago

Selected Answer: D

The correct answer is D. static NAT.

In the scenario where you need one-to-one mappings of internal servers to public IP addresses, you would use static NAT. Static NAT, also known as one-to-one NAT, allows you to create a direct, fixed mapping between an internal private IP address and a specific public IP address. This ensures that incoming traffic destined for the public IP address gets translated to the corresponding internal private IP address.

So, for your scenario, configuring static NAT would be the appropriate choice.

upvoted 1 times

fosi130 3 years, 2 months ago

D : one to one

upvoted 1 times

mohdema 3 years, 11 months ago

Selected Answer: D

One to one !

upvoted 2 times

Question #17 *Topic 1*

You want to provide remote access to an internal development environment for 10 remote developers.
Which two components are required to implement Juniper Secure Connect to satisfy this requirement? (Choose two.)

A. an additional license for an SRX Series device

B. Juniper Secure Connect client software

C. an SRX Series device with an SPC3 services card

D. Marvis virtual network assistant

Suggested Answer: *A, B*

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

Question #18 *Topic 1*

You are deploying an SRX Series firewall with multiple NAT scenarios.
In this situation, which NAT scenario takes priority?

A. interface NAT

B. source NAT

C. static NAT

D. destination NAT

Suggested Answer: *C*

66dc178 Most Recent 2 years, 9 months ago

static NAT generally takes priority over the other types of NAT. This is because static NAT is typically configured for inbound traffic to provide consistent, one-to-one mapping of public IP addresses to private IP addresses, which is crucial for services that need to be accessible from outside the network, such as web or mail servers.

upvoted 1 times

Question #19 *Topic 1*

Your ISP gives you an IP address of 203.0.113.0/27 and informs you that your default gateway is 203.0.113.1. You configure destination NAT to your internal server, but the requests sent to the webserver at 203.0.113.5 are not arriving at the server.
In this scenario, which two configuration features need to be added? (Choose two.)

A. firewall filter

B. security policy

C. proxy-ARP

D. UTM policy

Suggested Answer: *B, C*

Cradical Most Recent 2 years, 8 months ago

Selected Answer: BC

Security Policy (B): To allow the incoming traffic through the firewall to reach the internal server. Proxy-ARP (C): To enable the SRX device to respond to ARP requests for the public IP address mapped to the internal server. These two configurations should address the issue of requests not arriving at your internal server when using destination NAT.

upvoted 1 times

Question #20 *Topic 1*

Click the Exhibit button.

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

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

A. The DMZ routing-instance is the source.

B. The 10.10.102.10 IP address is the source.

C. The 10.10.102.10 IP address is the destination.

D. The DMZ routing-instance is the destination.

Suggested Answer: *A, C*

P0wned Most Recent 3 years, 2 months ago

AC , because as you can see it's just pinging itself.

upvoted 1 times

fosi130 3 years, 2 months ago

AC as result

upvoted 1 times

Question #21 *Topic 1*

Which IPsec protocol is used to encrypt the data payload?

A. ESP

B. IKE

C. AH

D. TCP

Suggested Answer: *A*

fosi130 Most Recent 3 years, 2 months ago

ESP is result

upvoted 2 times

Question #22 *Topic 1*

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

A. application

B. source address

C. source port

D. class

E. destination address

Suggested Answer: *A, B, E*

Engg_flint Most Recent 2 years, 11 months ago

ABE--The match criteria are based on a source IP address, destination IP address, and applications.

upvoted 2 times

davidrsr 3 years ago

Selected Answer: ABE

ABE Definitely source port is not important, coz it can be any number within 65535. How can someone tell the application from source port number?

upvoted 2 times

Juiz 3 years, 2 months ago

Selected Answer: ABE

These characteristics are called the match criteria. Each policy also has actions associated with it: permit, deny, reject, count, log, and VPN tunnel. You have to specify the match condition arguments when you configure a policy, source address, destination address, and application name.
https://www.juniper.net/documentation/us/en/software/junos/security-policies/topics/topic-map/security-policy-configuration.html

upvoted 1 times

P0wned 3 years, 2 months ago

Selected Answer: BCE

The correct answers are: B. source address C. source port E. destination address

In a Junos security policy, the three primary match criteria used are the source address, source port, and destination address. These criteria determine how traffic is matched and treated by the security policy. The application and class are not typically used as primary match criteria in security policies.

upvoted 1 times

fosi130 3 years, 2 months ago

ABE is good

upvoted 1 times

Question #23 *Topic 1*

You have an FTP server and a webserver on the inside of your network that you want to make available to users outside of the network. You are allocated a single public IP address.
In this scenario, which two NAT elements should you configure? (Choose two.)

A. destination NAT

B. NAT pool

C. source NAT

D. static NAT

Suggested Answer: *A, B*

sajiby3k Highly Voted 3 years, 9 months ago

Selected Answer: AB

With single Ip adress it is port forwarding. So, destination NAT and a pool address point to the single public IP of the internet facing interface.

upvoted 7 times

Wadakara Most Recent 2 years, 6 months ago

Selected Answer: AD

Answer is A D

upvoted 1 times

66dc178 2 years, 8 months ago

Selected Answer: AD

A. Destination NAT - To direct incoming traffic on specific ports to the corresponding internal servers. D. Static NAT could potentially be part of the solution if you were mapping the single public IP to an internal IP and then using DNAT rules to differentiate the services based on ports. However

upvoted 2 times

ars92 3 years ago

Selected Answer: AB

Destination NAT & NAT pool

upvoted 1 times

Question #24 *Topic 1*

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

A. Use IPS.

B. Use local lists.

C. Use remote lists.

D. Use Websense Redirect.

E. Use Juniper Enhanced Web Filtering.

Suggested Answer: *B, D, E*

fosi130 Most Recent 3 years, 2 months ago

my solution is : BDE

upvoted 1 times

mohdema 3 years, 11 months ago

Selected Answer: BDE

The Web filtering lets you to manage Internet usage by preventing access to inappropriate Web content. There are three types of Web filtering solutions:

Redirect Web filtering– Local Web filtering– Enhanced Web filtering–

upvoted 2 times

Bubu3k 3 years, 11 months ago

Selected Answer: BDE

https://www.juniper.net/documentation/us/en/software/junos/utm/topics/concept/utm-web-filtering-overview.html

upvoted 2 times

Question #25 *Topic 1*

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

A. SHA-1

B. SHAKE128

C. MD5

D. RIPEMD-256

Suggested Answer: *A, C*

fosi130 Most Recent 3 years, 2 months ago

My solution is AC

upvoted 1 times

Question #26 *Topic 1*

Click the Exhibit button.

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

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

A. to permit host inbound HTTP traffic and deny all other traffic on the internal security zone

B. to deny and log all host inbound traffic on the internal security zone, except for HTTP traffic

C. to permit all host inbound traffic on the internal security zone, but deny HTTP traffic

D. to permit host inbound HTTP traffic on the internal security zone

Suggested Answer: *C*

quraitulain Most Recent 2 years, 6 months ago

C is the right answer

upvoted 1 times

teek808 3 years, 9 months ago

https://www.juniper.net/documentation/us/en/software/junos/security-policies/topics/topic-map/security-zone-configuration.html#id-example-controlling-inbound-traffic-based-on-traffic-types

upvoted 1 times

Question #27 *Topic 1*

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

A. MPLS

B. UTM

C. CoS

D. IDP

Suggested Answer: *A, C*

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

Question #28 *Topic 1*

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

A. The SRX Series device is in flow mode.

B. The SRX Series device supports stateless firewalls filters.

C. The SRX Series device is in packet mode.

D. The SRX Series device does not support stateless firewall filters.

Suggested Answer: *A, B*

westh4m1234 Most Recent 2 years, 7 months ago

AB - default mode is flow mode = statefull can support stateless in packet mode

upvoted 1 times

subsonline 3 years, 3 months ago

Selected Answer: AB

AB https://www.juniper.net/documentation/us/en/software/junos/flow-packet-processing/topics/topic-map/security-srx-devices-processing-overview.html

upvoted 1 times

Question #29 *Topic 1*

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

A. Functional zones must have a user-defined name.

B. Functional zone cannot be referenced in security policies or pass transit traffic.

C. Multiple types of functional zones can be defined by the user.

D. Functional zones are used for out-of-band device management.

Suggested Answer: *B, D*

fosi130 Most Recent 3 years, 2 months ago

my choice is BD

upvoted 2 times

Question #30 *Topic 1*

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

A. packet capture

B. security logging

C. system logging

D. SNMP

Suggested Answer: *B*

quraitulain Most Recent 2 years, 6 months ago

B is the right answer

upvoted 1 times

Question #31 *Topic 1*

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

A. source NAT

B. destination NAT

C. static NAT

D. hairpin NAT

Suggested Answer: *C*

sajiby3k Highly Voted 3 years, 9 months ago

Selected Answer: C

Only static NAT with pool ensures both traffic initiated from inside and outside networks use the same IP address.

upvoted 6 times

66dc178 Most Recent 2 years, 8 months ago

Selected Answer: C

Static NAT provides a one-to-one mapping between the private IP address of your webservers and a public IP address. This type of NAT allows the servers to be reachable from the internet using the public IP address, and when the servers initiate connections (e.g., to update servers), they appear to come from the same public IP address. This maintains a consistent IP address for both inbound and outbound connections, meeting the project requirements.

upvoted 1 times

fosi130 3 years, 2 months ago

Static NAT

upvoted 1 times

alikhal 3 years, 3 months ago

Static NAT

upvoted 2 times

Question #32 *Topic 1*

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

A. certificate-based

B. multi-factor authentication

C. local authentication

D. active directory

Suggested Answer: *C, D*

Bubu3k Highly Voted 3 years, 11 months ago

Selected Answer: CD

"Local Authentication—In local authentication, the SRX Series device validates the user credentials by checking them in the local database. In this method, the administrator handles change of password or resetting of forgotten password. Here, it requires that an user must remember a new password. This option is not much preferred from a security standpoint. • External Authentication—In external authentication, you can allow the users to use the same user credentials they use when accessing other resources on the network. In many cases, user credentials are domain logon used for Active Directory or any other LDAP authorization system. This method simplifies user experience and improves the organization's security posture; because you can maintain the authorization system with the regular security policy used by your organization."

upvoted 6 times

joopgoof Highly Voted 3 years, 12 months ago

Selected Answer: CD

https://www.juniper.net/documentation/us/en/software/secure-connect/secure-connect-administrator-guide/topics/topic-map/secure-connect-getting-started.html

upvoted 5 times

fosi130 Most Recent 3 years, 2 months ago

CD is good

upvoted 1 times

Question #33 *Topic 1*

Click the Exhibit button.

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

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

A. UDP traffic matched by the deny-all policy will be silently dropped.

B. TCP traffic matched by the reject-all policy will have a TCP RST sent.

C. TCP traffic matched from the zone trust is allowed by the permit-all policy.

D. UDP traffic matched by the reject-all policy will be silently dropped.

Suggested Answer: *A, B*

dsabillonhn Most Recent 2 years, 8 months ago

Has no sense. The first term allows all connections. The other terms are invalid.

upvoted 1 times

OJ1 3 years, 1 month ago

https://www.juniper.net/documentation/us/en/software/junos/security-policies/topics/ref/statement/security-edit-reject.html

upvoted 1 times

OJ1 3 years, 1 month ago

AB best answer

upvoted 1 times

Question #34 *Topic 1*

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

A. Junos Space Log Director

B. Junos Space Security Director

C. to a local syslog server on the management network

D. to a local log file named messages

Suggested Answer: *D*

bigmokey Highly Voted 3 years, 9 months ago
By default, only critical messages are logged to a local file known as messages on the SRX Series device. The following configuration shows the default log settings: https://supportportal.juniper.net/s/article/SRX-Getting-Started-Configure-System-Logging?language=en_US
upvoted 5 times

westh4m1234 Most Recent 2 years, 7 months ago
By default, only critical messages are logged to a local file known as messages on the SRX Series device. The following configuration shows the default log settings:
upvoted 1 times

westh4m1234 2 years, 8 months ago
The SRX Series device is a syslog server, and by default, only critical system log messages are sent to a file on the device, which is known as messages (its D)
upvoted 1 times

ce57f43 3 years ago
Selected Answer: D
By default, it is stored in messages on SRX devices. For a remote syslog server, you have to give the IP address of the syslog server.

https://supportportal.juniper.net/s/article/SRX-Getting-Started-Configure-System-Logging?language=en_US
upvoted 2 times

penguin02007 3 years ago
D. Factory default always write to local file
upvoted 1 times

libm2 3 years, 3 months ago
D, its correct.
upvoted 3 times

achon 3 years, 6 months ago
D, whats local log server ip if default ?
upvoted 3 times

bigmokey 3 years, 9 months ago
Selected Answer: D
D:- By default, only critical messages are logged to a local file known as messages on the SRX Series device.
upvoted 3 times

Question #35 *Topic 1*

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

A. Allow

B. Discard

C. Deny

D. Reject

E. Permit

Suggested Answer: *C, D, E*

fosi130 Most Recent 3 years, 2 months ago

CDE is correct for me

upvoted 2 times

Question #36 *Topic 1*

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

A. protection against zero-day threats

B. IPsec VPNs

C. Layer 2 VPN tunnels

D. inline malware blocking

Suggested Answer: *A, D*

66dc178 Most Recent 2 years, 9 months ago

Selected Answer: AD

While IPsec VPNs and Layer 2 VPN tunnels are services that Juniper devices can provide, they are generally considered part of Juniper's networking and VPN features rather than specific services offered by Juniper Connected Security, which focuses more on security aspects like threat prevention and policy enforcement.

upvoted 1 times

OJ1 3 years, 1 month ago

A & B are the best answer. Next generation firewall service is all about Juniper Connected Security which allows the safeguard of users, applications, and infrastructure, extending security to all connection points across the network https://www.juniper.net/documentation/en_US/tech-center/topics/concept/connected-security-index.html#:~:text=Juniper%20Connected%20Security%20allows%20you,malware%20from%20entering%20your%20network.

upvoted 1 times

OJ1 3 years, 1 month ago

Please ignore my typo above, A & D are the best answer. Next generation firewall service is all about Juniper Connected Security which allows the safeguard of users, applications, and infrastructure, extending security to all connection points across the network https://www.juniper.net/documentation/en_US/tech-center/topics/concept/connected-security-index.html#:~:text=Juniper%20Connected%20Security%20allows%20you,malware%20from%20entering%20your%20network.

upvoted 1 times

achon 3 years, 5 months ago

Selected Answer: BD

B&D is correct

upvoted 1 times

Question #37 *Topic 1*

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

A. Proxy IDs are used to configure traffic selectors.

B. Proxy IDs are optional for Phase 2 session establishment.

C. Proxy IDs must match for Phase 2 session establishment.

D. Proxy IDs default to 0.0.0.0/0 for policy-based VPNs.

Suggested Answer: *C, D*

achon Highly Voted 3 years, 6 months ago

Selected Answer: CD

https://supportportal.juniper.net/s/article/SRX-Understanding-how-proxy-IDs-are-generated-in-route-based-and-policy-based-VPNs?language=en_US

upvoted 5 times

OJ1 3 years, 1 month ago

CD are the best answers

upvoted 1 times

westh4m1234 Most Recent 2 years, 7 months ago

This question is doing my head in - its not clear if they are asking about route-based or policy based because for route-based answer would be A+D however for policy-based it would be C+D

upvoted 1 times

westh4m1234 2 years, 7 months ago

SORRY MEANT TO SAY A+B ARE CORRECT FOR POLICY BASED VPN

upvoted 1 times

westh4m1234 2 years, 7 months ago

after having a good read check the below statement i think its A+D as the answer

Proxy ID generation for ROUTE-BASED VPNs can be defined explicitly. If it is not defined, a default proxy ID will be used of 0.0.0.0 if no traffic selectors are configured at all then the default proxy id will be used and must match both peers,

Proxy ID generation for POLICY-BASED VPNs is based on the security policy that is bound to the VPN , and cannot be overwritten with the proxy-identity command under the set security ipsec vpn ike proxy-identity stanza.

upvoted 1 times

westh4m1234 2 years, 7 months ago

CD- Proxy IDs are a validated item during VPN tunnel establishment with the proxy IDs of the VPN peers needing to be an inverse match of one another:

SRX PEER

Local 192.168.1.0/24 \ / Local 10.10.10.5/32 Remote 10.10.10.5/32 / \ Remote 192.168.1.0/24

Proxy ID generation for route-based VPNs can be defined explicitly. If it is not defined, a default proxy ID will be used of 0.0.0.0 if no traffic selectors are configured at all then the default proxy id will be used and must match both peers

upvoted 1 times

westh4m1234 2 years, 8 months ago

C+D - i agree with 66dc178 When no proxy-identity is defined, the system uses a default proxy-identity, which is 0.0.0.0

upvoted 1 times

66dc178 2 years, 9 months ago

Selected Answer: CD

In the absence of specific proxy ID configurations in policy-based VPNs, the default traffic selectors are considered to be 0.0.0.0/0, indicating that all traffic is eligible for the VPN tunnel, subject to the policy definitions. This default setting facilitates the tunneling of all traffic as per the defined policies unless more specific traffic selectors are configured.

upvoted 1 times

Question #38 *Topic 1*

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

A. zone

B. logical interface

C. physical interface

D. routing instance

Suggested Answer: *A, B*

OJ1 Most Recent 3 years, 1 month ago

AB best answers. https://www.juniper.net/documentation/us/en/software/junos/multicast-l2/topics/ref/statement/security-edit-host-inbound-traffic.html

upvoted 1 times

Question #39 *Topic 1*

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

A. IPS/IDP

B. security zones

C. application firewall

D. integrated user firewall

Suggested Answer: *A, C*

fosi130 Most Recent 3 years, 2 months ago

AC for me

upvoted 1 times

Question #40 *Topic 1*

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

A. the content filtering UTM feature

B. the antivirus UTM feature

C. the Web filtering UTM feature

D. the antispam UTM feature

Suggested Answer: *A, C*

quraitulain Most Recent 2 years, 6 months ago

A and C

upvoted 1 times

fosi130 3 years, 2 months ago

ac is good

upvoted 1 times

fosi130 3 years, 2 months ago

AC for me

upvoted 1 times