Question #1 *Topic 1*

You are modifying the NAT rule order and you notice that a new NAT rule has been added to the bottom of the list.
In this situation, which command would you use to reorder NAT rules?

A. insert

B. run

C. top

D. up

Suggested Answer: *A*

Community vote distribution

A (100%)

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

Question #2 *Topic 1*

Which two statements are correct about the Junos OS? (Choose two.)

A. It is a network operating system.

B. It is supported on physical and virtual devices.

C. It is a network management system for Juniper devices.

D. It is a network operating system for IoT devices.

Suggested Answer: *A, B*

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

Question #3 *Topic 1*

An SRX Series Firewall operates in which two modes? (Choose two.)

A. flow mode

B. packet mode

C. route mode

D. wireless mode

Suggested Answer: *A, B*

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

Question #4 *Topic 1*

In which order does Junos OS process the various forms of NAT?

A. destination NAT, source NAT, static NAT

B. static NAT, destination NAT, source NAT

C. source NAT, static NAT, destination NAT

D. source NAT, destination NAT, static NAT

Suggested Answer: *B*

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

Question #5 *Topic 1*

On the SRX Series Firewalls, which type of NAT is bi-directional?

A. source NAT without PAT

B. static NAT

C. source NAT

D. destination NAT

Suggested Answer: *B*

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

Question #6 *Topic 1*

Which two settings does the host-inbound-traffic zone configuration parameter control? (Choose two.)

A. transit traffic

B. protocols on the zone's physical interfaces

C. exception traffic

D. protocols on the zone's logical interfaces

Suggested Answer: *B, D*

Community vote distribution

CD (100%)

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

Question #7 *Topic 1*

Which two statements are correct about the Junos OS architecture? (Choose two.)

A. Junos is built using a collection of interdependent software processes.

B. Junos is built using independent software processes.

C. Restarting a single software process causes synchronization issues until other processes are restarted.

D. Individual software processes can be restarted without impacting the others.

Suggested Answer: *B, D*

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

Question #8 *Topic 1*

You plan to use unified security policies to identify and control nested HTTP applications.
In this scenario, which two actions must you perform on your SRX Series Firewall? (Choose two.)

A. Install the application identification (AppID) feature license on the SRX Series Firewall.

B. Include dynamic application objects in your security policies.

C. Create all the unified security policies in the global zone.

D. Disable the default security policy.

Suggested Answer: *A, B*

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

Question #9 *Topic 1*

What must also be enabled when using source NAT if the address pool is in the same subnet as the interface?

A. proxy ARP

B. dynamic DNS

C. static NAT

D. destination NAT

Suggested Answer: *A*

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

Question #10 *Topic 1*

Which statement is correct about security policies?

A. Security policies are evaluated before screen in first path processing.

B. Zone-based security policies reference both source and destination zones.

C. Security policies are evaluated in both first path and fast path processing.

D. Zone-based security policies only apply to intra-zone traffic.

Suggested Answer: *B*

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

Question #11 *Topic 1*

What happens when traffic is matched by a unified security policy?

A. Further processing stops and traffic is assigned a dynamic application.

B. Processing continues until it matches three or more policies.

C. Further policy processing stops and applies the action.

D. Processing continues to any additional unified policies.

Suggested Answer: *C*

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

Question #12 *Topic 1*

You are troubleshooting traffic traversing the SRX Series Firewall and require detailed information showing how the flow module is handing the traffic.
How would you accomplish this task?

A. Review the forwarding table.

B. Review the flow session table.

C. Enable flow trace options.

D. Enable firewall filters.

Suggested Answer: *C*

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

Question #13 *Topic 1*

Referring to the exhibit, which statement is correct?

```
[edit security policies from-zone Trust to-zone Untrust]
user@SRX# show
policy policy1 {
   match {
      source-address any;
      destination-address any;
      application junos-http;
   }
   then {
      permit;
   }
}
policy policy2 {
   match {
      source-address any;
      destination-address any;
      application junos-https;
   }
   then {
      permit;
   }
}
policy policy3 {
   match {
      source-address any;
      destination-address any;
      application junos-http;
   }
   then {
      deny;
   }
}
```

A. policy2 will be shadowed because it matches the same application as policy1.

B. policy3 will be shadowed because it matches the same application as policy1.

C. policy1 will be shadowed because it matches the same application as policy3.

D. None of the policies will be shadowed.

Suggested Answer: *B*

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

Question #14 *Topic 1*

Which two statements are correct about enabling the Avira Antivirus engine on an SRX Series Firewall? (Choose two.)

A. A license is required.

B. A license is not required.

C. A reboot is required.

D. A reboot is not required.

Suggested Answer: *A, D*

Community vote distribution

AC (100%)

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

Question #15 *Topic 1*

Which statement is correct about exception traffic?

A. Exception traffic refers to malformed IP packets received on the Packet Forwarding Engine.

B. Exception traffic is only handled on the Packet Forwarding Engine.

C. Exception traffic is rate-limited on the connection between the Packet Forwarding Engine and the Routing Engine.

D. Exception traffic is anything that is rejected by security policies and requires additional processing.

Suggested Answer: *C*

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

Question #16 *Topic 1*

Which two products will allow security policy management on SRX Series devices? (Choose two.)

A. Juniper Mist

B. Security Director

C. JIMS

D. JSA

Suggested Answer: *B, C*

Community vote distribution

AB (100%)

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

Question #17 *Topic 1*

Which two security policies are installed by default on SRX 300 Series Firewalls? (Choose two.)

A. a security policy to allow all traffic from the trust zone to the trust zone

B. a security policy to allow all traffic from the trust zone to the untrust zone

C. a security policy to allow all traffic from the untrust zone to the trust zone

D. a security policy to allow all traffic from the management zone to the trust zone

Suggested Answer: *A, C*

Community vote distribution

AB (100%)

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

Question #18 *Topic 1*

What are three requirements for creating a custom application? (Choose three.)

A. You must define the port number.

B. You must define the security policy.

C. You must define the application name.

D. You must define the source address.

E. You must define the protocol.

Suggested Answer: *A, C, E*

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

Question #19 *Topic 1*

When a new traffic flow enters an SRX Series device, in which order are these processes performed?

A. screens --> zones --> security policies --> routes

B. routes --> zones --> screens --> security policies

C. screens --> routes --> zones --> security policies

D. screens --> security policies --> zones --> routes

Suggested Answer: *C*

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

Question #20 *Topic 1*

You want to enable NextGen Web Filtering in SRX Series devices.
In this scenario, which two actions will accomplish this task? (Choose two.)

A. Generate a CA-signed certificate.

B. Generate a self-signed certificate.

C. Configure an SSL initiation profile.

D. Configure an SSL proxy profile.

Suggested Answer: *B, D*

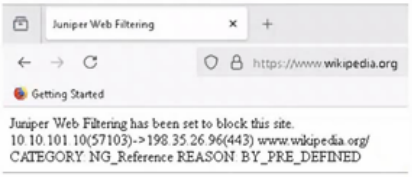
Community vote distribution

BC (100%)

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

Question #21 *Topic 1*

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



A. The URL matches a predefined Web filtering category.

B. The NextGen Web Filtering type is being used.

C. This is a custom Web filtering block message.

D. The SRX firewall does not have an SSL proxy configuration.

Suggested Answer: *A, B*

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

Question #22 *Topic 1*

Which type of NAT performs port address translation?

A. interface-based source NAT

B. static NAT

C. source NAT with address shifting

D. destination NAT without port forwarding

Suggested Answer: *A*

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

Question #23 *Topic 1*

What are two valid security address objects within Juniper Networks? (Choose two.)

A. global address object

B. prefix address object

C. routing address object

D. MAC address object

Suggested Answer: *A, B*

Community vote distribution

AD (100%)

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

Question #24 *Topic 1*

You are not able to ping an interface on an SRX Series Firewall.
Which two actions should you take to solve this issue? (Choose two.)

A. Configure the ICMP protocol for host-inbound-traffic.

B. Create a security policy to allow ping traffic.

C. Assign the interface to a security zone.

D. Assign the interface to the null zone.

Suggested Answer: *A, C*

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

Question #25 *Topic 1*

Which two statements are correct about security policies in SRX Series Firewalls? (Choose two.)

A. A security policy can only control inter-zone traffic.

B. A security policy can control both transit traffic and self-traffic.

C. A security policy can control both intra-zone traffic and inter-zone traffic.

D. A security policy can only control transit traffic.

Suggested Answer: *C, D*

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

Question #26 *Topic 1*

What are two purposes of configuring application sets? (Choose two.)

A. to organize multiple applications into a single group

B. to open dynamic ports used by particular applications for the duration of a session

C. to organize multiple addresses into a single group

D. to change the applications referenced in a security policy without editing the security policy

Suggested Answer: *A, D*

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

Question #27 *Topic 1*

You need to ensure that the security policy is configured correctly for a flow with both source NAT and destination NAT involved.
In this scenario, which two match conditions are valid for source and destination addresses? (Choose two.)

A. post-NAT destination address

B. pre-NAT source address

C. post-NAT source address

D. pre-NAT destination address

Suggested Answer: *A, B*

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

Question #28 *Topic 1*

Which two statements about the Juniper NGWF are correct? (Choose two.)

A. You can re-categorize a URL using the Junos configuration.

B. You can re-categorize a URL using a Junos operational mode command.

C. There is a predefined set of URL categories.

D. You cannot add a custom URL category.

Suggested Answer: *B, C*

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

Question #29 *Topic 1*

Which security policy action will cause traffic to drop and a message to be sent to the source?

A. deny

B. next-policy

C. reject

D. permit

Suggested Answer: *C*

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

Question #30 *Topic 1*

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

A. The management functional zone contains all available revenue ports until they are assigned to a user-defined security zone.

B. The management functional zone cannot be referenced in any security policies.

C. The management functional zone is automatically created on the SRX Series Firewalls.

D. The management functional zone is used to control the management-related traffic that is allowed to access your device.

Suggested Answer: *C, D*

Community vote distribution

BD (100%)

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

Question #31 *Topic 1*

You want to verify the effectiveness of Web filtering on the SRX Series Firewall.
How would you accomplish this task?

A. by examining the content filtering policies

B. by checking the file extensions of blocked content

C. by installing a local NGWF server

D. by attempting to access permitted or blocked URLs

Suggested Answer: *D*

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

Question #32 *Topic 1*

A new packet arrives on an interface on your SRX Series Firewall that is assigned to the trust security zone.
In this scenario, how does the SRX Series Firewall determine the egress security zone?

A. by examining the destination port

B. by performing a route lookup

C. by examining the ingress security zone properties

D. by performing a session lookup

Suggested Answer: *B*

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

Question #33 *Topic 1*

Which two statements are correct about security zones on an SRX Series device? (Choose two.)

A. Security zones can be shared between routing instances.

B. Multiple security zones cannot be configured on an SRX Series device.

C. Security zones cannot be shared between routing instances.

D. Intrazone and interzone traffic both require security policies.

Suggested Answer: *C, D*

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

Question #34 *Topic 1*

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

```
[edit security utm utm-policy content-filter-1]
user@SRX# show
content-filtering {
    rule-set rule-set-1 {
        rule rule-1 {
            match {
                applications http;
                direction download;
                file-types exe;
            }
            then {
                action block;
                notification {
                    log;
                }
            }
        }
    }
}
```

A. .exe files will not be allowed to be downloaded over HTTP.

B. There will be an e-mail sent to the user about why the SRX is blocking the file.

C. There will be a notice added to the SRX log file about the file being blocked.

D. .exe files will not be allowed to be uploaded over HTTP.

Suggested Answer: *A, C*

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

Question #35 *Topic 1*

Referring to the exhibit, which action would you take to permit the traffic shown in the exhibit?

```
user@SRX> show security packet-drop records
09:45:04.425799:LSYS-ID-00 10.20.30.40/1-->192.168.100.1/4584;icmp,ipid-
40954,ge-0/0/1.0,Dropped by FLOW:First path Ifp in Null Zone
Total packet-drop records: 1
```

A. Assign the ge-0/0/1.0 interface to a security zone.

B. Assign the fxp0.0 interface to a security zone.

C. Enable flow-mode processing for family mpls.

D. Enable flow-mode processing for family inet.

Suggested Answer: *A*

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

Question #36 *Topic 1*

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

```
user@SRX> show security flow session
Session ID: 116421, Policy name: private-server-access/6, State: Stand-alone, Timeout: 1774,
Valid
  In: 192.0.2.212/49862 --> 203.0.113.199/22;tcp, Conn Tag: 0x0, If: ge-0/0/3.0, Pkts: 19,
Bytes: 3409,
  Out: 10.10.101.10/22 --> 192.0.2.212/49862;tcp, Conn Tag: 0x0, If: ge-0/0/4.0, Pkts: 16,
Bytes: 3517,
```

A. The SRX Series Firewall is performing destination NAT.

B. The SRX Series Firewall is performing source NAT.

C. The SRX Series Firewall is not performing PAT.

D. The SRX Series Firewall is performing PAT.

Suggested Answer: *A, D*

Community vote distribution

AC (100%)

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

Question #37 *Topic 1*

Which two security features are applied in a security policy? (Choose two.)

A. SSL proxy

B. firewall authentication

C. captive portal authentication

D. MAC bypass

Suggested Answer: *A, B*

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

Question #38 *Topic 1*

What are two system-defined zones created on the SRX Series Firewalls? (Choose two.)

A. junos-host

B. null

C. DMZ

D. management

Suggested Answer: *A, B*

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

Question #39 *Topic 1*

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

A. You create only one functional zone called management.

B. Functional zones consist of logical interfaces belonging to multiple zones.

C. You reference the management functional zone in a security policy.

D. The management functional zone controls management access to the firewall.

Suggested Answer: *C, D*

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

Question #40 *Topic 1*

Which two characteristics of destination NAT and static NAT are correct? (Choose two.)

A. Destination NAT requires address range sizes that match the devices being translated.

B. Destination NAT supports port forwarding.

C. Static NAT automatically creates a matching rule for the opposite direction.

D. Static NAT uses Port Address Translation.

Suggested Answer: *B, C*

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

Question #41 *Topic 1*

You just made a configuration change to a security policy on your SRX Series Firewall. Your users alert you that an application that uses FTP is no longer working.
Referring to the exhibit, what are two ways to solve this problem? (Choose two.)

```
[edit security policies from-zone Trust to-zone Untrust]
user@SRX# show
inactive: policy ftp {
    match {
        source-address any;
        destination-address Server-1;
        application junos-ftp;
    }
    then {
        permit;
    }
}
policy web-smtp {
    match {
        source-address any;
        destination-address [ Web-1 Mail-Server-1 ];
        application [ junos-http junos-https junos-smtp ];
    }
    then {
        permit;
    }
}
```

A. Enter the rollback 1 command followed by a commit command.

B. Activate the ftp security policy and commit the configuration.

C. Insert the ftp security policy before the web-smtp security policy.

D. Change the destination address in the ftp security policy to any and commit the configuration.

Suggested Answer: *A, B*

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

Question #42 *Topic 1*

You are troubleshooting first path traffic not passing through an SRX Series Firewall. You have determined that the traffic is ingressing and egressing the correct interfaces using a route lookup.
In this scenario, what is the next step in troubleshooting why the device may be dropping the traffic?

A. Verify that the correct ALG is being used.

B. Verify that the interfaces are in the correct security zones.

C. Verify that source NAT is occurring.

D. Verify the routing protocol being used.

Suggested Answer: *B*

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

Question #43 *Topic 1*

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

```
user@SRX> show security nat source rule source-NAT-rule-1
source NAT rule: source-NAT-rule-1
  Rule set                    : source-NAT
  Rule Id                     : 2
  Rule position               : 1
  From zone                   : Trust
  To zone                     : Untrust
  Match
    Source addresses          : 0.0.0.0         - 255.255.255.255
  Action                      : interface
    Persistent NAT type       : N/A
    Persistent NAT mapping type : address-port-mapping
    Inactivity timeout        : 0
    Max session number        : 0
    Persistent NAT block session: disabled
  Translation hits            : 1423
    Successful sessions       : 1423
  Number of sessions          : 4
```

A. Traffic does not match this NAT rule.

B. All traffic that ingresses the trust security zone and egresses the untrust security zone matches this NAT rule.

C. Only traffic that matches the default route matches this NAT rule.

D. This is the first NAT rule in the rule set.

Suggested Answer: *B, D*

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

Question #44 *Topic 1*

Which two statements are true about content filtering on SRX Series devices? (Choose two.)

A. Content filtering requires a license.

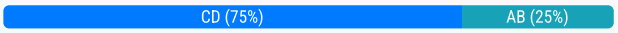
B. Content filtering examines the file extension to determine the file type.

C. Content filtering does not require a license.

D. Content filtering examines the file contents to determine the file type.

Suggested Answer: *C, D*

Community vote distribution



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

Question #45 *Topic 1*

Which two statements are correct about unified security policies on SRX Series Firewalls? (Choose two.)

A. Unified security policies with multiple matches use the most restrictive match.

B. Unified security policies match applications before processing policy statements.

C. Unified security policies can be zone-based or global.

D. Unified security policies use the application identification (AppID) engine.

Suggested Answer: *C, D*

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

Question #46 *Topic 1*

Which statement about the flow module is correct in the context of destination NAT?

A. The flow module performs NAT during both first path and fast path processing.

B. The flow module performs NAT only for source IP addresses.

C. The flow module performs NAT only during fast path processing.

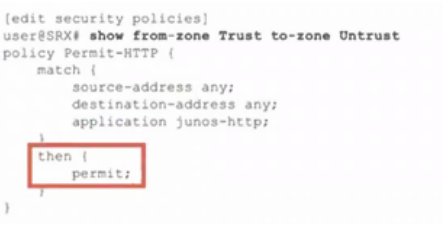
D. The flow module performs NAT only during first path processing.

Suggested Answer: *A*

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

Question #47 *Topic 1*

Which security policy component is highlighted in the exhibit?



A. security zone context

B. unique policy name

C. match criteria

D. policy action

Suggested Answer: *D*

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

Question #48 *Topic 1*

You are asked to permit users to read Reddit posts but prevent them from posting any new content.
Which two actions would you perform to achieve this task? (Choose two.)

A. Enable micro-application services at the zone level for application-tracking.

B. Include micro-application objects in traditional security policies.

C. Include micro-application objects in unified security policies.

D. Enable micro-application services for application-identification.

Suggested Answer: *C, D*

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

Question #49 *Topic 1*

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

A. A single screen can be associated with multiple security zones.

B. Screens are only used on first path traffic.

C. Screens only detect IP-based attacks.

D. Screens are applied on the security zone of the ingress interface.

Suggested Answer: *A, D*

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