



**Vendor:** Juniper

**Exam Code:** JN0-230

**Exam Name:** Security, Associate (JNCIA-SEC)

**Version:** DEMO

### QUESTION 1

Firewall filters define which type of security?

- A. Stateful
- B. Stateless
- C. NGFW
- D. Dynamic enforcement

**Answer: B**

**Explanation:**

[https://www.juniper.net/documentation/en\\_US/junos/topics/concept/firewall-filter-types.html](https://www.juniper.net/documentation/en_US/junos/topics/concept/firewall-filter-types.html)

### QUESTION 2

Which UTM feature should you use to protect users from visiting certain blacklisted websites?

- A. Content filtering
- B. Web filtering
- C. Antivirus
- D. antispam

**Answer: B**

**Explanation:**

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

Redirect Web filtering—The redirect Web filtering solution intercepts HTTP and HTTPS requests and sends them to an external URL filtering server, provided by Websense, to determine whether to block the requests.

Redirect Web filtering does not require a license.

Local Web filtering—The local Web filtering solution intercepts every HTTP request and the HTTPS request in a TCP connection. In this case, the decision making is done on the device after it looks up a URL to determine if it is in the whitelist or blacklist based on its user-defined category.

Local Web filtering does not require a license or a remote category server.

Enhanced Web filtering—The enhanced Web filtering solution intercepts the HTTP and the HTTPS requests and sends the HTTP URL or the HTTPS source IP to the Websense

ThreatSeeker Cloud (TSC). The TSC categorizes the URL into one of the 151 or more categories that are predefined and also provides site reputation information. The TSC further returns the URL category and the site reputation information to the device. The device determines if it can permit or block the request based on the information provided by the TSC. Starting in Junos OS Release 17.4R1, Websense redirect support IPv6 traffic.

### QUESTION 3

Which management software supports metadata-based security policies that are ideal for cloud deployments?

- A. Security Director
- B. J-Web
- C. Network Director
- D. Sky Enterprise

**Answer: A**

**Explanation:**

[https://www.juniper.net/documentation/en\\_US/junos-space18.2/topics/concept/junos-space-metadata-overview.html](https://www.juniper.net/documentation/en_US/junos-space18.2/topics/concept/junos-space-metadata-overview.html)

#### QUESTION 4

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

- A. A functional zone uses security policies to enforce rules for transit traffic.
- B. Traffic received on the management interface in the functional zone cannot transit out other interface.
- C. Functional zones separate groups of users based on their function.
- D. A function is used for special purpose, such as management interface

**Answer:** BD

**Explanation:**

A functional zone is used for special purposes, like management interfaces. Currently, only the management (MGT) zone is supported. Management zones have the following properties: Management zones host management interfaces.

Traffic entering management zones does not match policies; therefore, traffic cannot transit out of any other interface if it was received in the management interface.

Management zones can only be used for dedicated management interfaces.

#### QUESTION 5

Which two actions are performed on an incoming packet matching an existing session? (Choose two.)

- A. Zone processing
- B. Security policy evolution
- C. Service ALG processing
- D. Screens processing

**Answer:** CD

**Explanation:**

If an incoming packet is matching an existing session it uses Fast Path - Screens, TCP, NAT, Services ALGs.

#### QUESTION 6

On an SRX device, you want to regulate traffic base on network segments. In this scenario, what do you configure to accomplish this task?

- A. Screens
- B. Zones
- C. ALGs
- D. NAT

**Answer:** B

**Explanation:**

A security zone is a collection of one or more network segments requiring the regulation of inbound and outbound traffic through policies. Security zones are logical entities to which one or more interfaces are bound. You can define multiple security zones, the exact number of which you determine based on your network needs.

[https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/security-zone-configuration.html](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-zone-configuration.html)

#### QUESTION 7

Which two match conditions would be used in both static NAT and destination NAT rule sets? (Choose two.)

- A. Destination zone
- B. Destination interface
- C. Source interface
- D. Source zone

**Answer:** CD

**Explanation:**

Destination NAT rules specify two layers of match conditions:

Traffic direction—Allows you to specify from interface, from zone, or from routing-instance.

Packet information—Can be source IP addresses, destination IP address or subnet, destination port numbers or port ranges, protocols, or applications.

#### QUESTION 8

Which statement about IPsec is correct?

- A. IPsec can be used to transport native Layer 2 packets.
- B. IPsec can provide encapsulation but not encryption
- C. IPsec is a standards-based protocol.
- D. IPsec is used to provide data replication

**Answer:** C

**Explanation:**

[https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/overview-of-ipsec.html](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/overview-of-ipsec.html)

#### QUESTION 9

Which statements is correct about global security policies?

- A. Global policies allow you to regulate traffic with addresses and applications, regardless of their security zones.
- B. Traffic matching global is not added to the session table.
- C. Global policies eliminate the need to assign interface to security zones.
- D. Global security require you to identify a source and destination zone.

**Answer:** A

**Explanation:**

Global policies do not reference specific source and destination zones. Global policies reference the predefined address “any” or user-defined addresses that can span multiple security zones. Global policies give you the flexibility of performing actions on traffic without any zone restrictions. For example, you can create a global policy so that every host in every zone can access the company website, for example, [www.juniper.net](http://www.juniper.net). Using a global policy is a convenient shortcut when there are many security zones. Traffic is classified by matching its source address, destination address, and the application that the traffic carries in its protocol header.

## Thank You for Trying Our Product

### Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



**10% Discount Coupon Code: ASTR14**