JN0-103^{Q&As}

Junos - Associate (JNCIA-Junos)

Pass Juniper JN0-103 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/jn0-103.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Juniper Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Which two interfaces are considered logical interfaces? (Choose two.)

A. xe-1/1/1

B. ge-2/0/2.0

C. et-5/0/0

D. ae1.1

Correct Answer: CD

QUESTION 2

You must archive log messages for an extended period of time for audit and troubleshooting purposes.

Which syslog setting should you configure on the Junos device in this scenario?

A. severity

B. facility

C. host

D. console

Correct Answer: C

QUESTION 3

Which two commands will provide the current configuration of the MX1-PE1 BGP group on your router? (Choose two.)

A. user@router# show groups | display set | match MX1-PE1

B. user@router> show configuration | display set | match MX1-PE1

C. user@router> show configuration | match set | match MX1-PE1

D. user@router# show | display set | match MX1-PE1

Correct Answer: BD

QUESTION 4
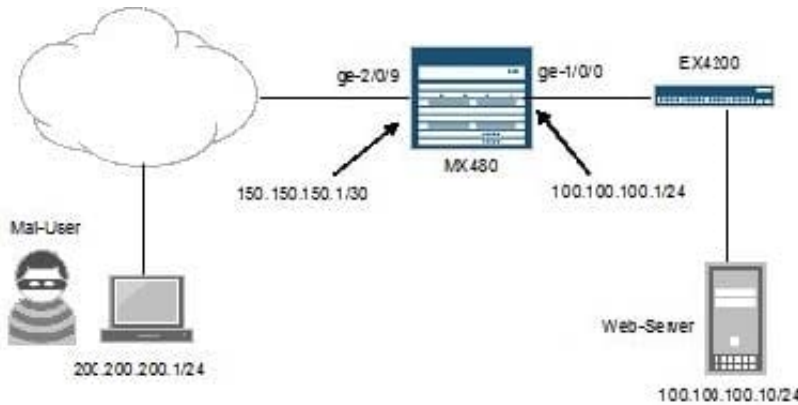
Referring to the exhibit, you are asked to rate-limit traffic from Web-Server to the subnet where Mal-User is located. All other traffic should be permitted.

Which firewall filter configuration do you use?

A. [edit firewall]user@router# showpolicer LIMIT-MAL-USER {if-exceeding {bandwidth-limit 400k;burstsize-limit 100k;}then discard;}familyinet {filter STOP-MAL-USER {term one {from {source-address {100.100.100.10/32;}destination-address {200.200.200.0/24;}}thenpolicer LIMIT-MAL-USER;}term two {then accept;}}}

B. [edit firewall]user@router# showpolicer LIMIT-BAD-USER {if-exceeding {bandwidth-limit 400k;burstsize-limit 100k;}then discard;}familyinet {filter STOP-MAL-USER {term one {from {source-address {100.100.100.10/32;}destination-address {200.200.200.0/24;}}thenpolicer LIMIT-MAL-USER;}term two {then accept;}}}

C. [edit firewall]user@router# showpolicer LIMIT-MAL-USER {if-exceeding {bandwidth-limit 400k;burstsize-limit 100k;}then discard;}familyinet {filter STOP-MAL-USER {term one {from {source-address {100.100.100.10/32;}destination-address {200.200.200.0/24;}}thenpolicer LIMIT-MAL-USER;}term two {then reject;}}}

D. [edit firewall]user@router# showpolicer LIMIT-MAL-USER {if-exceeding {bandwidth-limit 400k;burstsize-limit 100k;}then discard;}familyinet {filter STOP-MAL-USER {term one {from {source-address {200.200.200.0/24;}destination-address {100.100.100.10/32;}}thenpolicer LIMIT-MAL-USER;}term two {then accept;}}}

Correct Answer: A

QUESTION 5

```
user@router> show route forwarding-table
Routing table: default.inet
Internet:
Enabled protocols: Bridging,
Destination          Type  RtRef  Next hop          Type  Index  NhRef  Netif
default              perm     0                     rjct     36      1
0.0.0.0/32           perm     0                     dscd     34      1
10.5.0.0/16          user     0   10.102.70.254     ucst    355     18   fxp0.0
10.10.0.0/16         user     0   10.102.70.254     ucst    355     18   fxp0.0
10.12.14.0/24        intf     0                     rslv    589      1   ge-2/0/0.0
10.12.14.0/32        dest     0   10.12.14.0        recv    587      1   ge-2/0/0.0
10.12.14.254/32      intf     0   10.12.14.254      locl    588      2
10.12.14.254/32      dest     0   10.12.14.254      locl    588      2
10.12.14.255/32      dest     0   10.12.14.255      bcst    586      1   ge-2/0/0.0
10.13.10.0/23        user     0   10.102.70.254     ucst    355     18   fxp0.0
10.84.0.0/16         user     0   10.102.70.254     ucst    355     18   fxp0.0
10.102.70.0/24       intf     0                     rslv    354      1   fxp0.0
224.0.0.0/4          perm     0                     mdsc     35      1
224.0.0.1/32         perm     0   224.0.0.1         mcst     31      2
224.0.0.5/32         user     0   224.0.0.5         mcst     31      2
255.255.255.255/32   perm     0                     bcst     32      1
```

Referring to the exhibit, what happens to a packet that has a destination address of 172.17.0.1?

A. The packet is forwarded to the next hop of the management network.

B. The packet is rejected and an ICMP network unreachable message is sent to the source address.

C. The packet is silently discarded.

D. The packet is forwarded to the next hop defined in the default route.

Correct Answer: B