KTest

更に上のクオリティ　更に上のサービス

問題集

http://www.ktest.jp

1年で無料進級することに提供する

Exam : **JN0-106**

Title : Junos, Associate (JNCIA-Junos)

Version : DEMO

1.Click the Exhibit button.

Exhibit

```
family inet {
    filter Packet-Filter {
        term 1 {
            from {
                source-address {
                    192.168.1.1/32;
                }
                destination-address {
                    8.8.8.8/32;
                }
                protocol tcp;
            }
            then accept;
        }
        term 2 {
            from {
                source-address {
                    192.168.2.0/24;
                }
                destination-address {
                    8.8.8.8/32;
                }
                protocol udp;
                port domain;
```

Referring to the exhibit, with firewall filter Packet-Filter attached to an interface, if traffic is sent from 192.168.1.1 to 8.8.8.8 for a UDP DNS query, what will happen to the traffic?

A. The traffic will match term 1 and be forwarded.

B. The traffic will match the default last term and be forwarded.

C. The traffic will match the default last term and be discarded.

D. The traffic will match term 3 and be forwarded.

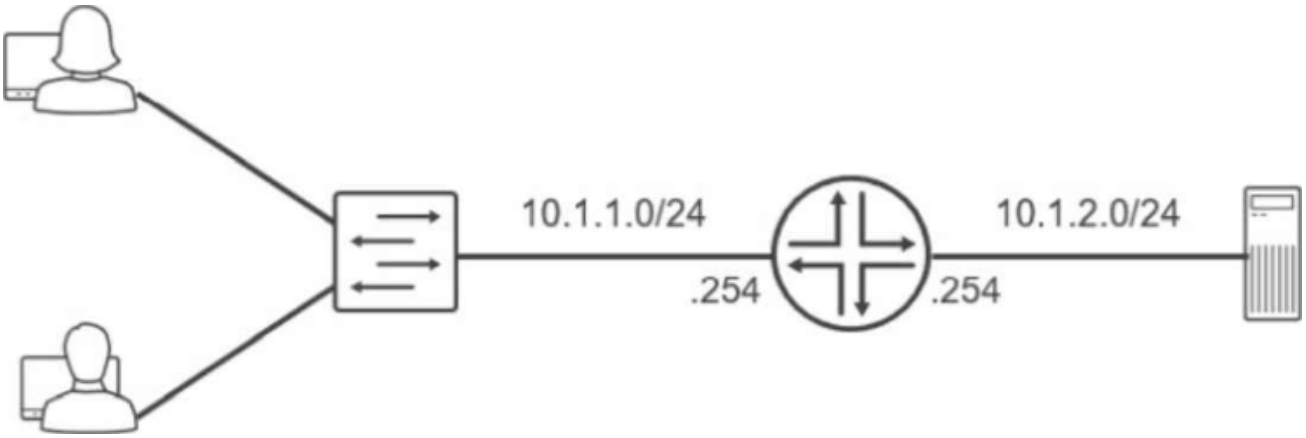
Answer: C

Explanation:

Junos OS firewall filters operate on a first-match basis, evaluating terms sequentially from top to bottom. In this scenario, a UDP DNS packet (destination port 53) is sent from 192.168.1.1 to 8.8.8.8. Evaluation begins with term 1, which matches the correct source and destination IP addresses but specifies protocol tcp. Because the actual traffic uses UDP, term 1 is not a match. Evaluation then moves to term 2. While term 2 correctly identifies protocol udp and port domain (port 53), it requires the source-address to reside within the 192.168.2.0/24 subnet. Since the source is 192.168.1.1, term 2 also fails to match. When a packet fails to match any explicitly defined terms in a Junos firewall filter, it is subject to the implicit deny action. This default "last term" is a hardcoded safety mechanism that automatically discards all traffic that has not been explicitly permitted. Consequently, because neither term provides a match for the specific combination of source IP, protocol, and destination port, the DNS query is silently dropped

by the Packet Forwarding Engine. This behavior ensures that Junos devices maintain a "deny-by-default" security posture, requiring administrators to define precise permit statements for all required transit or management traffic. Routing Policy and Firewall Filters, Firewall Filter Evaluation, Implicit Discard.

2.Click the Exhibit button.



Referring to the exhibit, which routing configuration is required for these two users to access the remote server?

A. Users and the server require a default gateway.
B. Trunk ports must be enabled on the switch.
C. Users must connect directly to the router.
D. A routing protocol must be enabled on the router.

Answer: A

Explanation:

The network topology illustrates two distinct IP subnets, 10.1.1.0/24 and 10.1.2.0/24, separated by a Layer 3 router. For hosts on the first subnet to communicate with the server on the second subnet, an intermediary device must perform inter-subnet routing. The router acts as the exit point for each local segment, utilizing its interfaces assigned with the .254 host address as the logical path to external networks.

The fundamental requirement for this communication is the configuration of a default gateway on all end-nodes. When the users (on 10.1.1.0/24) attempt to send data to the server (on 10.1.2.0/24), their local TCP/IP stack recognizes the destination is not on the local wire. Without a defined default gateway, the hosts would simply drop the traffic as unroutable. By setting the default gateway to 10.1.1.254 for users and 10.1.2.254 for the server, the hosts are instructed to forward all off-net traffic to the router. The router then consults its routing table—which contains these directly connected routes—and forwards the packets to the appropriate egress interface. While VLAN tagging or routing protocols could exist in more complex environments, the primary necessity for basic reachability between these two specific segments is a correctly configured gateway on the terminal devices. Networking Fundamentals, IP Routing Basics, Default Gateway Configuration.

3.Click the Exhibit button.

```
user@router> show route table inet.0
inet.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
0.0.0.0/0          *[Static/5] 2d 05:30:15
                    > to 203.0.113.1 via ge-0/0/0
10.0.0.0/8         *[Static/5] 1d 10:20:30
                    > to 192.168.1.1 via ge-0/0/1
10.50.0.0/16       *[OSPF/10] 08:15:22
                    > to 192.168.1.10 via ge-0/0/1
10.50.10.0/24      *[BGP/170] 02:45:10
                    > to 192.168.1.20 via ge-0/0/2
```

Referring to the exhibit, which route will be selected for a packet destined to IP address 10.50.10.55?
A. Route 0.0.0.0/0 will be selected using next hop 203.0.113.1 because the default route matches all destinations and has been active the longest.
B. Route 10.50.0.0/16 will be selected using next hop 192.168.1.10 because OSPF has a better preference value than BGP.
C. Route 10.50.10.0/24 will be selected using next hop 192.168.1.20 because it has the longest prefix match for the destination address.
D. Route 10.0.0.0/8 will be selected using next hop 192.168.1.1 because it was learned from the static routing protocol which has the lowest preference value.
Answer: C
Explanation:
In Junos OS, the Routing Information Base (RIB) selection process follows a strict hierarchy where the Longest Prefix Match (LPM) is the absolute primary tie-breaker. When a packet is destined for 10.50.10.55, the Routing Engine searches the inet.0 table for all matching entries. In this exhibit, four routes match: the default route (0.0.0.0/0), a general static route (10.0.0.0/8), an OSPF route (10.50.0.0/16), and a BGP route (10.50.10.0/24).
The LPM rule dictates that the router must select the most specific route available, which is defined as the entry with the highest number of matching bits in the subnet mask. The 10.50.10.0/24 route matches 24 bits of the destination address, making it more specific than the 16-bit, 8-bit, or 0-bit alternatives. It is critical to understand that route preference (e.g., Static at 5, OSPF at 10, or BGP at 170) is only evaluated if there are multiple paths to the exact same prefix and length. Because these prefixes vary in length, the length takes precedence over the protocol preference. Therefore, the BGP-learned route via 192.168.1.20 is selected as the active path, ensuring traffic follows the most granular routing information provided to the device. Routing Fundamentals, Routing Table Selection, Longest Prefix Match.

4.Click the Exhibit button.

```
[edit firewall]
user@router# show
family inet {
    filter mgmt_fill {
        term t1 {
            from {
                destination-port ssh;
            }
            then count c1;
        }
        term t2 {
            then accept;
        }
    }
}
[edit interfaces]
user@router# show
me0 {
    unit 0 {
        family inet {
            filter {
                output mgmt_fill;
            }
            address 192.168.1.1/24;
        }
    }
 }
```

Which two statements are true about the firewall filter configuration shown in the exhibit? (Choose two.)

A. It applies the filter to a physical interface.

B. It counts the number of SSH packets that egress from the source SSH interface.

C. It evaluates SSH packets egressing from the management interface.

D. It sends filtered data to a syslog file.

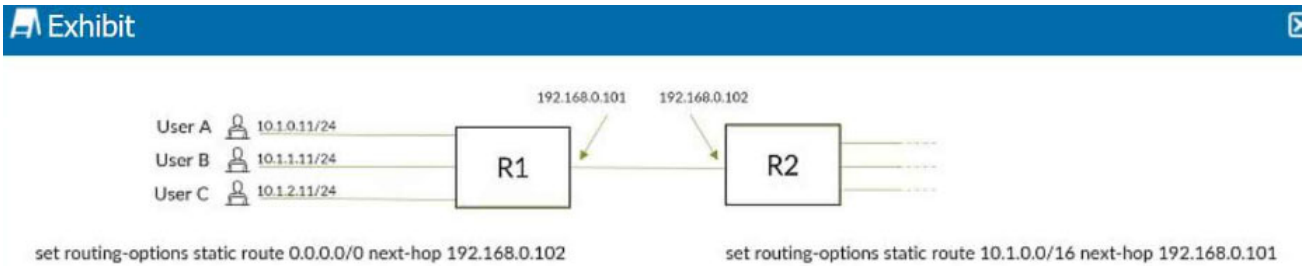
Answer: A, C

Explanation:

The exhibit illustrates the configuration of a firewall filter named mgmt_fill and its subsequent application to an interface. The first true statement is that the filter is applied to a physical interface. The configuration shows the filter attached to me0, which in Junos nomenclature represents the Management Ethernet port—a dedicated physical port for out-of-band management traffic. This is separate from logical or virtual interfaces, as me0 provides the physical link for administrative access.

The second true statement is that the filter evaluates SSH packets egressing from the management interface. In the provided snippet, term t1 specifically matches the destination-port ssh, and the filter is applied to the interface unit. When a filter is applied to an interface, it can monitor traffic entering or leaving the device. Furthermore, the filter utilizes a count action (count c1), which is a non-terminating action used to provide telemetry on specific traffic types passing through that physical port. There is no mention of a syslog or log action in the configuration, meaning that while packets are counted, they are not being written to the system log files. This configuration is a standard method for hardening the management plane and tracking administrative session activity on the Routing Engine. Routing Policy and Firewall Filters, Firewall Filter Actions, Management Interfaces.

5.Click the Exhibit button.



Which statement is correct about traffic flow in the network shown in the exhibit?

A. A routing loop can occur if one of the users sends packets to 10.1.99.1.

B. Only User A can reach destinations beyond Router R1.

C. Router R2 will drop packets destined for user B and user C.

D. Router R1 will discard all packets from all three users.

Answer: A

Explanation:

The configuration exhibit demonstrates a classic scenario where mismatched static routing leads to a routing loop. Router R1 is configured with a default route (0.0.0.0/0) pointing to R2 as its next hop. Conversely, R2 is configured with a broad static route for 10.1.0.0/16 pointing back to R1.

If a user sends a packet to an unassigned IP address such as 10.1.99.1, the following sequence occurs: R1 receives the packet and consults its routing table. Finding no specific match for the 10.1.99.1 host, it uses the default route and forwards the packet to R2.

R2 receives the packet and identifies that 10.1.99.1 falls within its defined static route for 10.1.0.0/16. Following its configuration, R2 forwards the packet back to R1. This process repeats indefinitely—or until the packet's Time to Live (TTL) reaches zero—because the broad summary on R2 encompasses addresses that R1 does not actually have a local path for. This illustrates the critical importance of ensuring that summary routes or default routes do not overlap in a way that creates circular forwarding paths for non-existent destinations. Routing Fundamentals, Static Route Configuration, Routing Loops and TTL.