JN0-636$^{\text{Q\&As}}$

Service Provider Routing and Switching Professional (JNCIP-SP)

Pass Juniper JN0-636 Exam with 100% Guarantee

QUESTION 1

You have designed the firewall filter shown in the exhibit to limit SSH control traffic to yours SRX Series device without affecting other traffic. Which two statement are true in this scenario? (Choose two.)

A. The filter should be applied as an output filter on the loopback interface.

B. Applying the filter will achieve the desired result.

C. Applying the filter will not achieve the desired result.

D. The filter should be applied as an input filter on the loopback interface.

Correct Answer: CD

Explanation: https://www.juniper.net/documentation//en_US/junos/topics/concept/firewall- filter-ex-series-evaluation-understanding.html

QUESTION 2

You want to enforce I DP policies on HTTP traffic.

In this scenario, which two actions must be performed on your SRX Series device? (Choose two)

A. Choose an attacks type in the predefined-attacks-group HTTP-All.

B. Disable screen options on the Untrust zone.

C. Specify an action of None.

D. Match on application junos-http.

Correct Answer: AD

Explanation: To enforce IDP policies on HTTP traffic on an SRX Series device, the following actions must be performed:

Choose an attacks type in the predefined-attacks-group HTTP-All: This allows the SRX Series device to match on specific types of attacks that can occur within HTTP traffic. For example, it can match on SQL injection or cross-site scripting

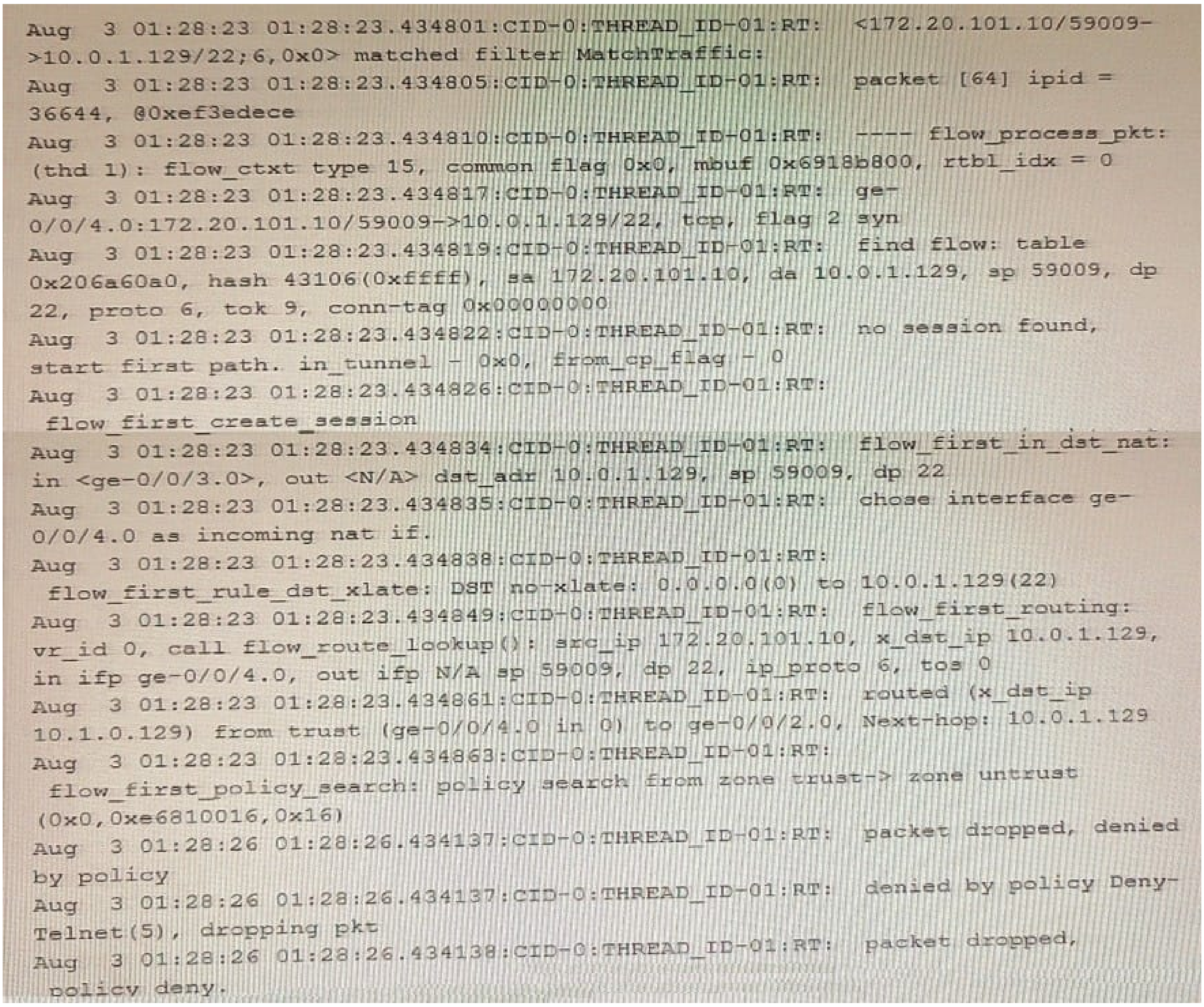
(XSS) attacks.

Match on application junos-http: This allows the SRX Series device to match on HTTP traffic specifically, as opposed to other types of traffic. It is necessary to properly identify the traffic that needs to be protected. Disabling screen options on

the Untrust zone and specifying an action of None are not necessary to enforce IDP policies on HTTP traffic. The first one is a feature used to prevent certain types of attacks, the second one is used to take no action in case of a match.

QUESTION 3

Exhibit



```
Aug  3 01:28:23 01:28:23.434801:CID-0:THREAD_ID-01:RT:  <172.20.101.10/59009-
>10.0.1.129/22;6,0x0> matched filter MatchTraffic:
Aug  3 01:28:23 01:28:23.434805:CID-0:THREAD_ID-01:RT:  packet [64] ipid =
36644, @0xef3edece
Aug  3 01:28:23 01:28:23.434810:CID-0:THREAD_ID-01:RT:  ---- flow_process_pkt:
(thd 1): flow_ctxt type 15, common flag 0x0, mbuf 0x6918b800, rtbl_idx = 0
Aug  3 01:28:23 01:28:23.434817:CID-0:THREAD_ID-01:RT:  ge-
0/0/4.0:172.20.101.10/59009->10.0.1.129/22, tcp, flag 2 syn
Aug  3 01:28:23 01:28:23.434819:CID-0:THREAD_ID-01:RT:  find flow: table
0x206a60a0, hash 43106(0xffff), sa 172.20.101.10, da 10.0.1.129, sp 59009, dp
22, proto 6, tok 9, conn-tag 0x00000000
Aug  3 01:28:23 01:28:23.434822:CID-0:THREAD_ID-01:RT:  no session found,
start first path. in_tunnel - 0x0, from_cp_flag - 0
Aug  3 01:28:23 01:28:23.434826:CID-0:THREAD_ID-01:RT:
 flow_first_create_session
Aug  3 01:28:23 01:28:23.434834:CID-0:THREAD_ID-01:RT:  flow_first_in_dst_nat:
in <ge-0/0/3.0>, out <N/A> dst_adr 10.0.1.129, sp 59009, dp 22
Aug  3 01:28:23 01:28:23.434835:CID-0:THREAD_ID-01:RT:  chose interface ge-
0/0/4.0 as incoming nat if.
Aug  3 01:28:23 01:28:23.434838:CID-0:THREAD_ID-01:RT:
 flow_first_rule_dst_xlate: DST no-xlate: 0.0.0.0(0) to 10.0.1.129(22)
Aug  3 01:28:23 01:28:23.434849:CID-0:THREAD_ID-01:RT:  flow_first_routing:
vr_id 0, call flow_route_lookup(): src_ip 172.20.101.10, x_dst_ip 10.0.1.129,
in ifp ge-0/0/4.0, out ifp N/A sp 59009, dp 22, ip_proto 6, tos 0
Aug  3 01:28:23 01:28:23.434861:CID-0:THREAD_ID-01:RT:  routed (x_dst_ip
10.1.0.129) from trust (ge-0/0/4.0 in 0) to ge-0/0/2.0, Next-hop: 10.0.1.129
Aug  3 01:28:23 01:28:23.434863:CID-0:THREAD_ID-01:RT:
 flow_first_policy_search: policy search from zone trust-> zone untrust
(0x0,0xe6810016,0x16)
Aug  3 01:28:26 01:28:26.434137:CID-0:THREAD_ID-01:RT:  packet dropped, denied
by policy
Aug  3 01:28:26 01:28:26.434137:CID-0:THREAD_ID-01:RT:  denied by policy Deny-
Telnet(5), dropping pkt
Aug  3 01:28:26 01:28:26.434138:CID-0:THREAD_ID-01:RT:  packet dropped,
 policy deny.
```

Referring to the exhibit, which statement is true?

A. This custom block list feed will be used before the Juniper Seclntel

B. This custom block list feed cannot be saved if the Juniper Seclntel block list feed is configured.

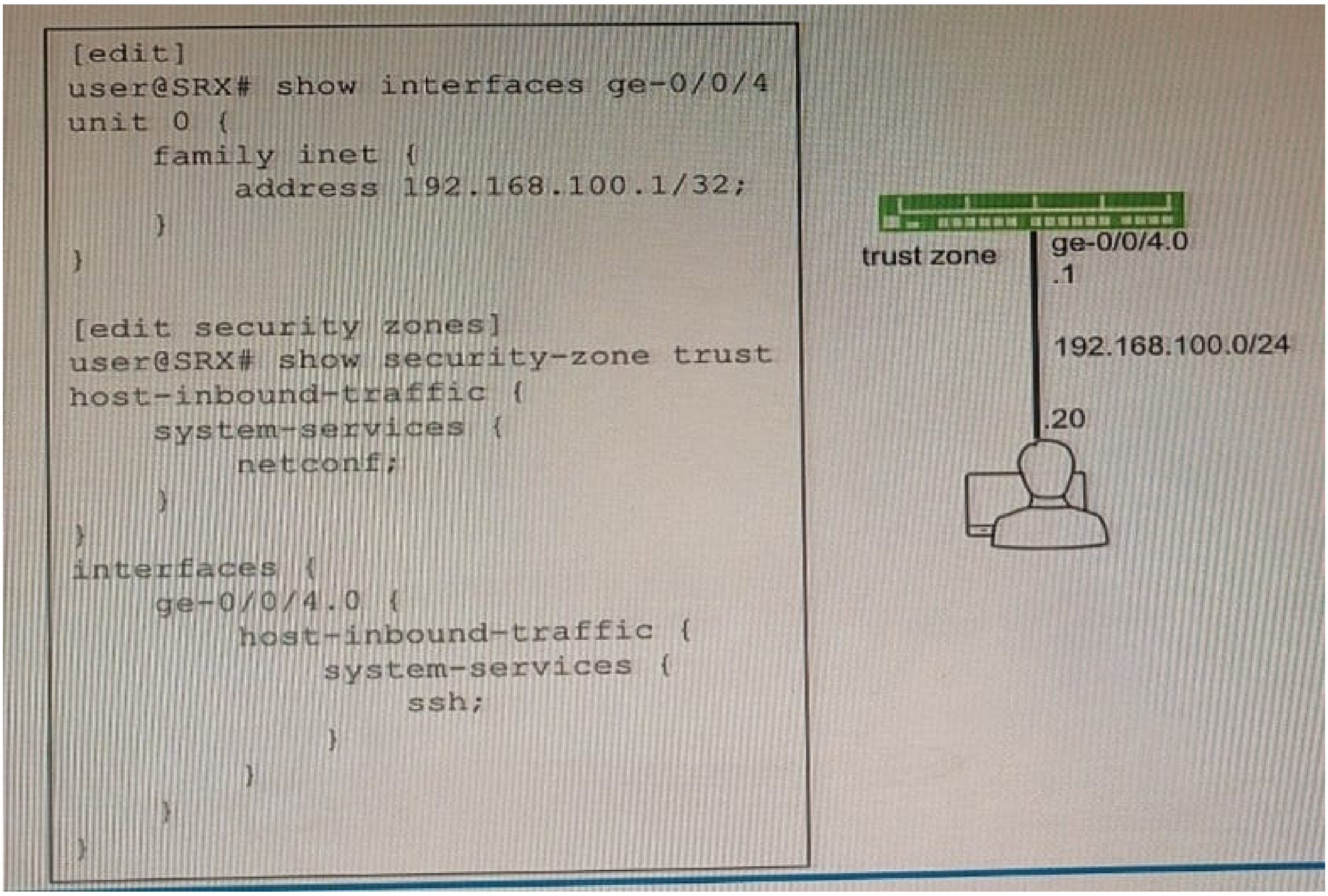
C. This custom block list feed will be used instead of the Juniper Seclntel block list feed

D. This custom block list feed will be used after the Juniper Seclntel block list feed.

Correct Answer: D

QUESTION 4

Exhibit

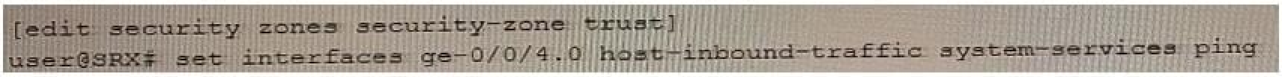


```
[edit]
user@SRX# show interfaces ge-0/0/4
unit 0 {
    family inet {
        address 192.168.100.1/32;
    }
}

[edit security zones]
user@SRX# show security-zone trust
host-inbound-traffic {
    system-services {
        netconf;
    }
}
interfaces {
    ge-0/0/4.0 {
        host-inbound-traffic {
            system-services {
                ssh;
            }
        }
    }
}
```

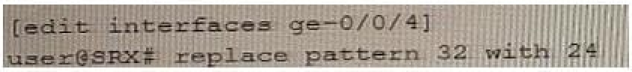
You are not able to ping the default gateway of 192.168 100 1 (or your network that is located on your SRX Series firewall. Referring to the exhibit, which two commands would correct the configuration of your SRX Series device? (Choose two.)

○ A.



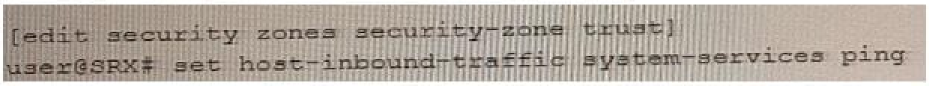
```
[edit security zones security-zone trust]
user@SRX# set interfaces ge-0/0/4.0 host-inbound-traffic system-services ping
```

○ B.



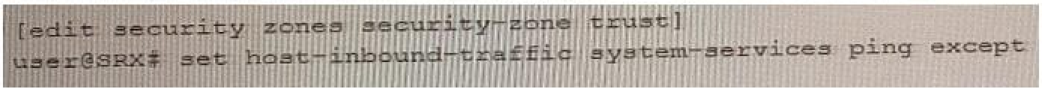
```
[edit interfaces ge-0/0/4]
user@SRX# replace pattern 32 with 24
```

○ C.



```
[edit security zones security-zone trust]
user@SRX# set host-inbound-traffic system-services ping
```

○ D.



```
[edit security zones security-zone trust]
user@SRX# set host-inbound-traffic system-services ping except
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: C

QUESTION 5

You are connecting two remote sites to your corporate headquarters site; you must ensure that all traffic is secured and only uses a single Phase 2 SA for both sites.

In this scenario, which VPN should be used?

A. An IPsec group VPN with the corporate firewall acting as the hub device.

B. Full mesh IPsec VPNs with tunnels between all sites.

C. A hub-and-spoke IPsec VPN with the corporate firewall acting as the hub device.

D. A full mesh Layer 3 VPN with the corporate firewall acting as the hub device.

Correct Answer: A

Explanation: https://www.juniper.net/us/en/local/pdf/app-notes/3500202-en.pdf