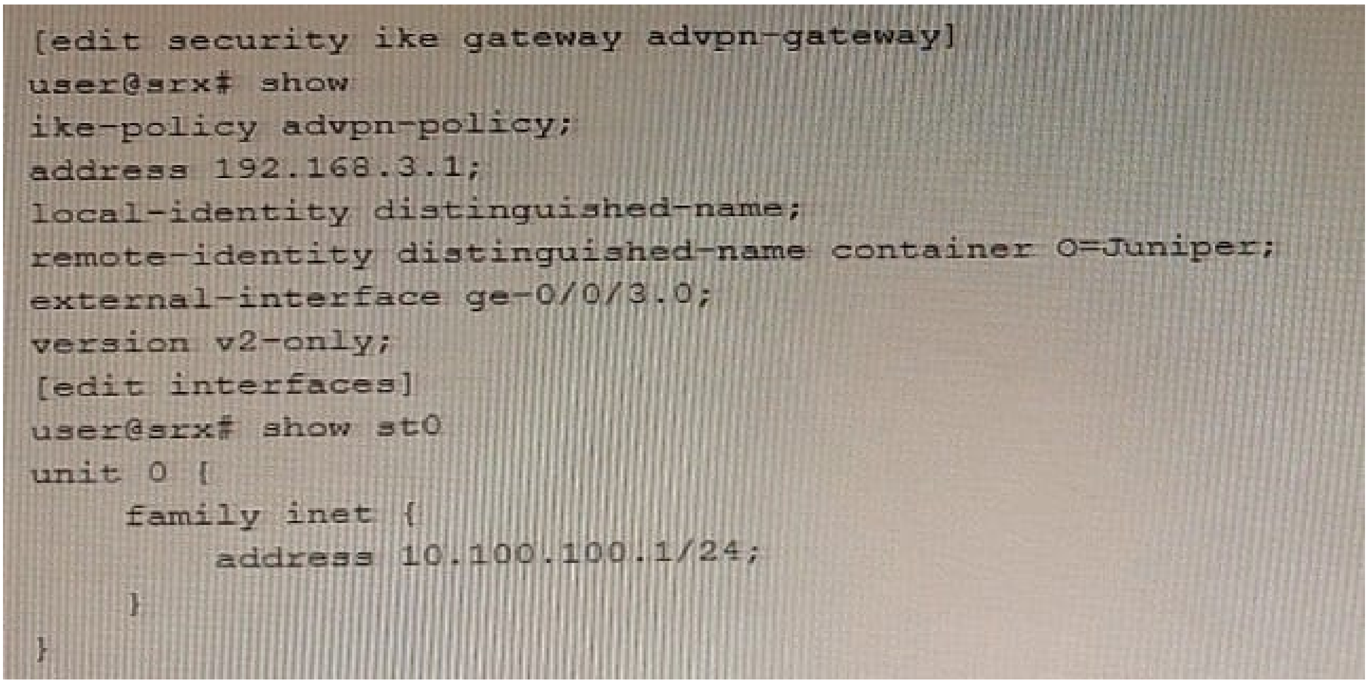
JN0-636$^{\text{Q\&As}}$

Service Provider Routing and Switching Professional (JNCIP-SP)

Pass Juniper JN0-636 Exam with 100% Guarantee

QUESTION 1

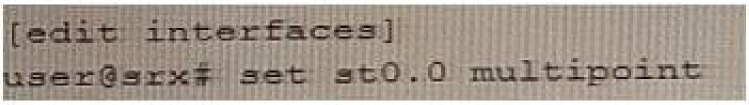
Exhibit



```
[edit security ike gateway advpn-gateway]
user@srx# show
ike-policy advpn-policy;
address 192.168.3.1;
local-identity distinguished-name;
remote-identity distinguished-name container O=Juniper;
external-interface ge-0/0/3.0;
version v2-only;
[edit interfaces]
user@srx# show st0
unit 0 {
    family inet {
        address 10.100.100.1/24;
    }
}
```

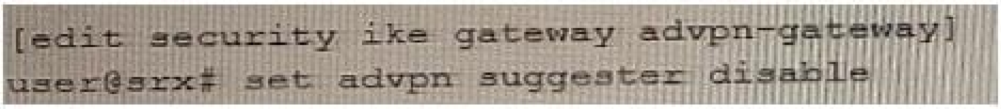
Referring to the exhibit, a spoke member of an ADVPN is not functioning correctly. Which two commands will solve this problem? (Choose two.)

○ A.



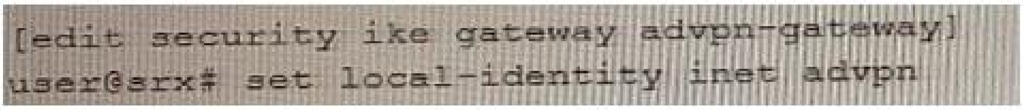
```
[edit interfaces]
user@srx# set st0.0 multipoint
```

○ B.



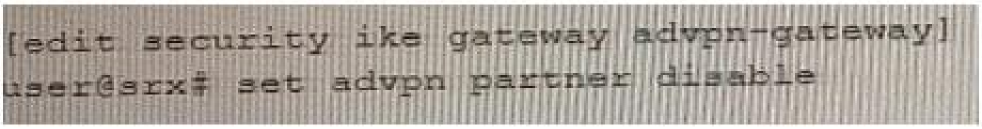
```
[edit security ike gateway advpn-gateway]
user@srx# set advpn suggester disable
```

○ C.



```
[edit security ike gateway advpn-gateway]
user@srx# set local-identity inet advpn
```

○ D.



```
[edit security ike gateway advpn-gateway]
user@srx# set advpn partner disable
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: C

QUESTION 2

You are asked to detect domain generation algorithms

Which two steps will accomplish this goal on an SRX Series firewall? (Choose two.)

A. Define an advanced-anti-malware policy under [edit services].

B. Attach the security-metadata-streaming policy to a security

C. Define a security-metadata-streaming policy under [edit

D. Attach the advanced-anti-malware policy to a security policy.

Correct Answer: BD

Explanation: To detect domain generation algorithms (DGAs) on an SRX Series firewall, you can use the security-metadata-streaming and advanced-anti-malware features. The first step is to define a security-metadata-streaming policy under

[edit services], which allows the firewall to receive and process metadata from a third- party security intelligence service. This metadata includes information about DGAs, which the firewall can use to identify and block malicious traffic. The

second step is to attach the security-metadata-streaming policy to a security policy, this will enable the firewall to inspect traffic against the DGA domains provided by the intelligence service.

The third step is to enable the advanced-anti-malware feature on the firewall, and attach an advanced-anti-malware policy to a security policy. This allows the firewall to detect and block malware based on signatures and behavioral analysis,

which can also detect and block traffic associated with DGAs.

QUESTION 3

You want to enroll an SRX Series device with Juniper ATP Appliance. There is a firewall device in the path between the devices. In this scenario, which port should be opened in the firewall device?

A. 8080

B. 443

C. 80

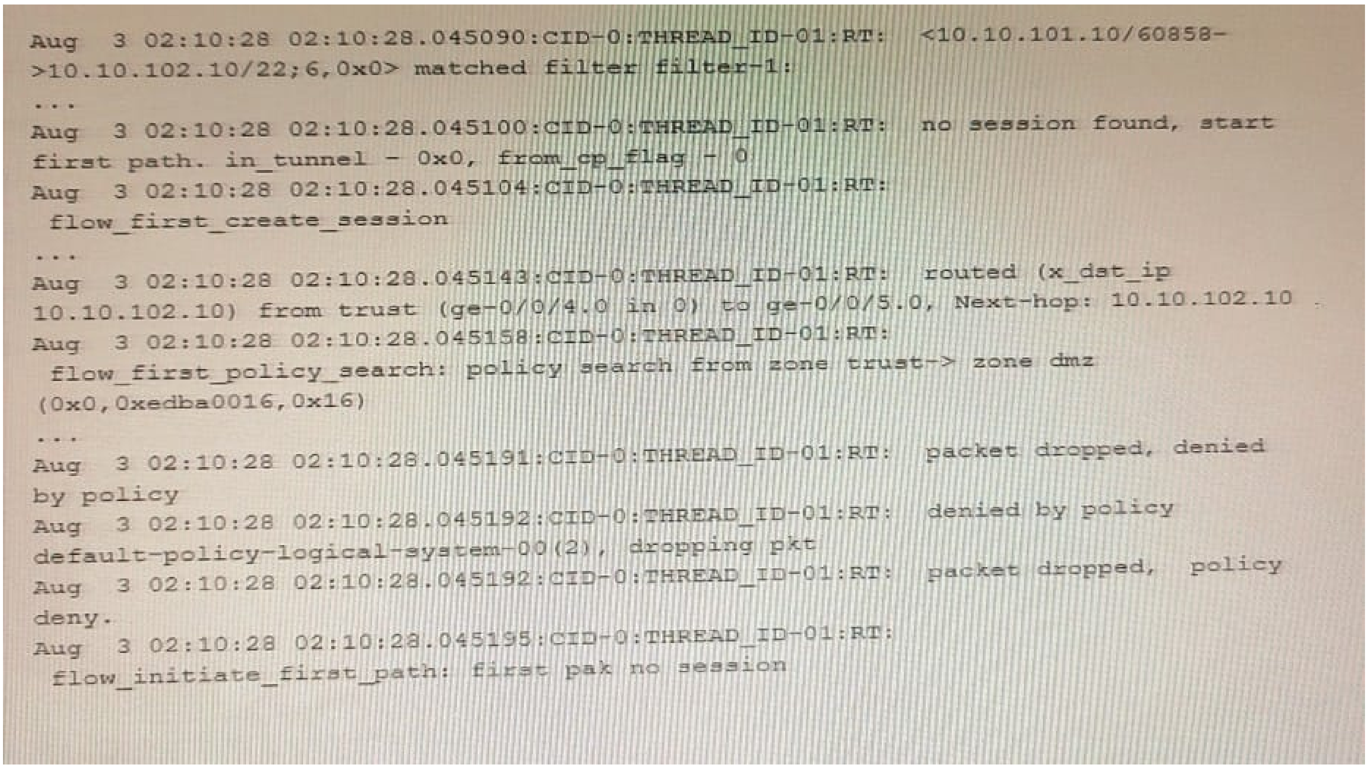
D. 22

Correct Answer: B

Explanation: This is the port used for encrypted communication between the SRX series device and the Juniper ATP Appliance In order to enroll an SRX Series device with Juniper ATP Appliance, the firewall device must have port 443 open. Port 443 is the default port used for HTTPS traffic, the communication between the SRX Series device and the ATP Appliance needs to be encrypted, that\\'s why this port should be opened.

QUESTION 4

Exhibit



```
Aug  3 02:10:28 02:10:28.045090:CID-0:THREAD_ID-01:RT:  <10.10.101.10/60858-
>10.10.102.10/22;6,0x0> matched filter filter-1:
...
Aug  3 02:10:28 02:10:28.045100:CID-0:THREAD_ID-01:RT:  no session found, start
first path. in_tunnel - 0x0, from_cp_flag - 0
Aug  3 02:10:28 02:10:28.045104:CID-0:THREAD_ID-01:RT:
 flow_first_create_session
...
Aug  3 02:10:28 02:10:28.045143:CID-0:THREAD_ID-01:RT:  routed (x_dst_ip
10.10.102.10) from trust (ge-0/0/4.0 in 0) to ge-0/0/5.0, Next-hop: 10.10.102.10
Aug  3 02:10:28 02:10:28.045158:CID-0:THREAD_ID-01:RT:
 flow_first_policy_search: policy search from zone trust-> zone dmz
(0x0,0xedba0016,0x16)
...
Aug  3 02:10:28 02:10:28.045191:CID-0:THREAD_ID-01:RT:  packet dropped, denied
by policy
Aug  3 02:10:28 02:10:28.045192:CID-0:THREAD_ID-01:RT:  denied by policy
default-policy-logical-system-00(2), dropping pkt
Aug  3 02:10:28 02:10:28.045192:CID-0:THREAD_ID-01:RT:  packet dropped,  policy
deny.
Aug  3 02:10:28 02:10:28.045195:CID-0:THREAD_ID-01:RT:
 flow_initiate_first_path: first pak no session
```

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

A. The packet is processed as host inbound traffic.

B. The packet matches the default security policy.

C. The packet matches a configured security policy.

D. The packet is processed in the first path packet flow.

Correct Answer: AB

QUESTION 5

You want to use selective stateless packet-based forwarding based on the source address.

In this scenario, which command will allow traffic to bypass the SRX Series device flow daemon?

A. set firewall family inet filter bypaa3_flowd term t1 then skip--services accept

B. set firewall family inet filter bypass_flowd term t1 then routing-instance stateless

C. set firewall family inet filter bypas3_flowd term t1 then virtual-channel stateless

D. set firewall family inet filter bypass__f lowd term t1 then packet--mode

Correct Answer: C