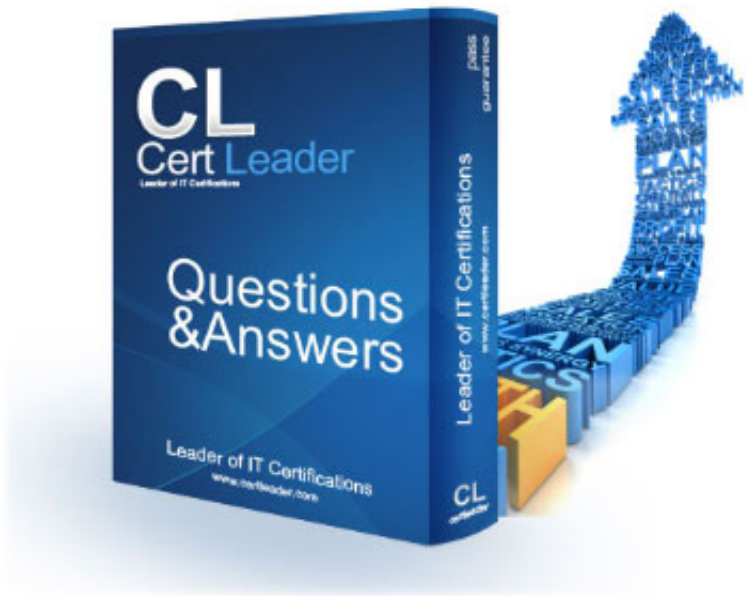
JN0-633 - Security, Professional (JNCIP-SEC)

http://www.certleader.com/JN0-633-dumps.html



1.What are two network scanning methods? (Choose two.)

A. SYN flood

B. ping of death

C. ping sweep

D. UDP scan

Answer: C, D

2.What are two intrusion protection mechanisms available on SRX Series Services Gateways? (Choose two.)

A. routing update detection

B. traffic anomaly detection

C. NAT anomaly protection

D. DoS protection

Answer: B, D

3.What is a benefit of using a dynamic VPN?

A. It provides a layer of redundancy on top of a point-to-point VPN mesh architecture.

B. It eliminates the need for point-to-point VPN tunnels.

C. It provides a way to grant VPN access on a per-user-group basis.

D. It simplifies IPsec access for remote clients.

Answer: D

4.What is a benefit of using a group VPN?

A. It provides a layer of redundancy on top of a point-to-point VPN mesh architecture.

B. It eliminates the need for point-to-point VPN tunnels.

C. It provides a way to grant VPN access on a per-user-group basis.

D. It simplifies IPsec access for remote clients.

Answer: B

5.Which statement is true about Layer 2 zones when implementing transparent mode security?

A. All interfaces in the zone must be configured with the protocol family mpls.

B. All interfaces in the zone must be configured with the protocol family inet.

C. All interfaces in the zone must be configured with the protocol family bridge.

D. All interfaces in the zone must be configured with the protocol family inet6.

Answer: C

6.What are two AppSecure modules? (Choose two.)

A. AppDoS

B. AppFlow

C. AppTrack

D. AppNAT

Answer: A, C

7.You are working as a security administrator and must configure a solution to protect against distributed botnet attacks on your company\'s central SRX cluster.

How would you accomplish this goal?

A. Configure AppTrack to inspect and drop traffic from the malicious hosts.

B. Configure AppQoS to block the malicious hosts.

C. Configure AppDoS to rate limit connections from the malicious hosts.

D. Configure AppID with a custom application to block traffic from the malicious hosts.

Answer: C

8.You are asked to change the configuration of your company\'s SRX device so that you can block nested traffic from certain Web sites, but the main pages of these Web sites must remain available to users.

Which two methods will accomplish this goal? (Choose two.)

A. Enable the HTTP ALG.

B. Implement a firewall filter for Web traffic.

C. Use an IDP policy to inspect the Web traffic.

D. Configure an application firewall rule set.

Answer: B, D

9.You are using the AppDoS feature to control against malicious bot client attacks. The bot clients are using file downloads to attack your server farm. You have configured a context value rate of 10,000 hits in 60 seconds. At which threshold will the bot clients no longer be classified as malicious?

A. 5000 hits in 60 seconds

B. 8000 hits in 60 seconds

C. 7500 hits in 60 seconds

D. 9999 hits in 60 seconds

Answer: B

10.Your company\'s network has seen an increase in Facebook-related traffic. You have been asked to restrict the amount of Facebook-related traffic to less than 100 Mbps regardless of congestion.

What are three components used to accomplish this task? (Choose three.)

A. IDP policy

B. application traffic control

C. application firewall

D. security policy

E. application signature

Answer: B, D, E

11.You recently implemented application firewall rules on an SRX device to act upon encrypted traffic. However, the encrypted traffic is not being correctly identified.

Which two actions will help the SRX device correctly identify the encrypted traffic? (Choose two.)

A. Enable heuristics to detect the encrypted traffic.

B. Disable the application system cache.

C. Use the junos:UNSPECIFIED-ENCRYPTED application signature.

D. Use the junos:SPECIFIED-ENCRYPTED application signature.

Answer: A, C

12.You have just created a few hundred application firewall rules on an SRX device and applied them to the appropriate firewall polices. However, you are concerned that the SRX device might become overwhelmed with the increased processing required to process traffic through the application firewall rules.

Which three actions will help reduce the amount of processing required by the application firewall rules? (Choose three.)

A. Use stateless firewall filtering to block the unwanted traffic.

B. Implement AppQoS to drop the unwanted traffic.

C. Implement screen options to block the unwanted traffic.

D. Implement IPS to drop the unwanted traffic.

E. Use security policies to block the unwanted traffic.

Answer: A, C, E

13.Referring to the following output, which command would you enter in the CLI to produce this result?

Pic2/1 Ruleset Application Client-to-server Rate(bps) Server-to-client Rate(bps)

http-App-QoS HTTP ftp-C2S 200 ftp-C2S 200

http-App-QoS HTTP ftp-C2S 200 ftp-C2S 200

ftp-App-QoS FTP ftp-C2S 100 ftp-C2S 100

A. show class-of-service interface ge-2/1/0

B. show interface flow-statistics ge-2/1/0

C. show security flow statistics

D. show class-of-service applications-traffic-control statistics rate-limiter

Answer: D

14.You are asked to apply individual upload and download bandwidth limits to YouTube traffic.

Where in the configuration would you create the necessary bandwidth limits?

A. under the [edit security application-firewall] hierarchy

B. under the [edit security policies] hierarchy

C. under the [edit class-of-service] hierarchy

D. under the [edit firewall policer <policer-name>] hierarchy

Answer: D

15.You want to verify that all application traffic traversing your SRX device uses standard ports. For example, you need to verify that only DNS traffic runs through port 53, and no other protocols. How would you accomplish this goal?

A. Use an IDP policy to identify the application regardless of the port used.

B. Use a custom ALG to detect the application regardless of the port used.

C. Use AppTrack to detect the application regardless of the port used.

D. Use AppID to detect the application regardless of the port used.

Answer: A

16.You are asked to establish a baseline for your company\'s network traffic to determine the bandwidth usage per application. You want to undertake this task on the central SRX device that connects all segments together. What are two ways to accomplish this goal? (Choose two.)

A. Configure a mirror port on the SRX device to capture all traffic on a data collection server for further investigation.

B. Use interface packet counters for all permitted and denied traffic and calculate the values using Junos scripts.

C. Send SNMP traps with bandwidth usage to a central SNMP server.

D. Enable AppTrack on the SRX device and configure a remote syslog server to receive AppTrack messages.

Answer: A, D

17.Microsoft has altered the way their Web-based Hotmail application works. You want to update your application firewall policy to correctly identify the altered Hotmail application.

Which two steps must you take to modify the application? (Choose two.)

A. user@srx> request services application-identification application copy junos:HOTMAIL

B. user@srx> request services application-identification application enable junos:HOTMAIL

C. user@srx# edit services custom application-identification my:HOTMAIL

D. user@srx# edit services application-identification my:HOTMAIL

Answer: A, D

18.Two companies, A and B, are connected as separate customers on an SRX5800 residing on two virtual routers (VR-A and VR-B). These companies have recently been merged and now operate under a common IT security policy. You have been asked to facilitate communication between these VRs. Which two methods will accomplish this task? (Choose two.)

A. Use instance-import to share the routes between the two VRs.

B. Create logical tunnel interfaces to interconnect the two VRs.

C. Use a physical connection between VR-A and VR-B to interconnect them.

D. Create a static route using the next-table action in both VRs.

Answer: A, D

19.You have been asked to configure traffic to flow between two virtual routers (VRs) residing on two unique logical systems (LSYSs) on the same SRX5800.

How would you accomplish this task?

A. Configure a security policy that contains the context from VR1 to VR2 to permit the relevant traffic.

B. Configure a security policy that contains the context from LSYS1 to LSYS2 and relevant match conditions in the rule set to allow traffic between the IP networks in VR1 and VR2.

C. Configure logical tunnel interfaces between VR1 and VR2 and security policies that allow relevant traffic between VR1 and VR2 over that link.

D. Configure an interconnect LSYS to facilitate a connection between LSYS1 and LSYS2 and relevant policies to allow the traffic.

Answer: C

20.You are responding to a proposal request from an enterprise with multiple branch offices. All branch offices connect to a single SRX device at a centralized location. The request requires each office to be segregated on the central SRX device with separate IP networks and security considerations. No single office should be able to starve the CPU from other branch offices on the central SRX device due to the number of flow sessions. However, connectivity between offices must be maintained. Which three features are required to accomplish this goal? (Choose three.)

A. Logical Systems

B. Interconnect Logical System

C. Virtual Tunnel Interface

D. Logical Tunnel Interface

E. Virtual Routing Instance

Answer: A, B, D

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your JN0-633 Exam with Our Prep Materials Via below:

http://www.certleader.com/JN0-633-dumps.html