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 : **JN0-330**

Title : JN0-330-Enhanced Services, Specialist(JNCIS-ES)

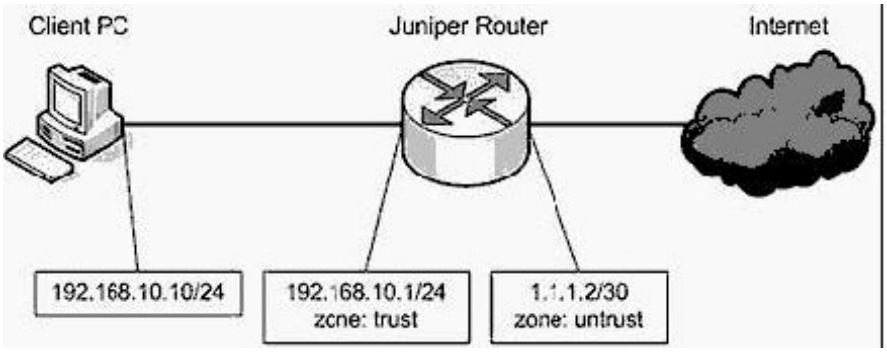
Version : Demo

1. Click the Exhibit button.

```
user@host# run show security nat source-nat pool pool-1
Pool name            Address         Status   Host           References PAT
pool-1               1.1.1.10        free     10.1.1.10               0 no
pool-1               1.1.1.11        free     10.1.1.11               0 no
pool-1               1.1.1.12        free     10.1.1.12               0 no
pool-1               1.1.1.13        free     10.1.1.13               0 no
pool-1               1.1.1.14        free     10.1.1.14               0 no
```

Which type of source NAT is configured in the exhibit?
A. static source pool
B. interface source pool
C. source pool with PAT
D. souce pool without PAT
Answer:A

2. Click the Exhibit button.
Based on the exhibit, client PC 192.168.10.10 cannot ping 1.1.1.2.
Which is a potential cause for this problem?



A. The untrust zone does not have a management policy configured.
B. The trust zone does not have ping enabled as host-inbound-traffic service.
C. The security policy from the trust zone to the untrust zone does not permit ping.
D. No security policy exists for the ICMP reply packet from the untrust zone to the trust zone.
Answer: C

3. A traditional router is better suited than a firewall device for which function?
A. VPN establishment
B. packet-based forwarding
C. stateful packet processing
D. network address translation
Answer: B

4. You must configure a SCREEN option that would protect your router from a session table flood.
Which configuration meets this requirement?
A. [edit security screen]
user@hostl# show
ids-option protectFromFlood {

icmp {
ip-sweep threshold 5000;
flood threshold 2000;
}
B. [edit security screen]
user@hostl# show
ids-option protectFromFlood {
tcp {
syn-flood {
attack-threshold 2000;
destination-threshold 2000;
}
C. [edit security screen]
user@hostl# show
ids-option protectFromFlood {
udp {
flood threshold 5000;
}
D. [edit security screen]
user@hostl# show
ids-option protectFromFlood {
limit-session {
source-ip-based 1200;
destination-ip-based 1200;
}
Answer: D

5. Click the Exhibit button.

```
Router A:
[edit]
user@RouterA# show interfaces ge-0/0/1
unit 0 {
    family inet {
        address 192.168.1.253/24 {
            vrrp-group 100 {
                virtual-address 192.168.1.1;
                priority 110;
                no-preempt;
            }
        }
    }
}

Router B:
[edit]
user@RouterB# show interfaces ge-0/0/1
unit 0 {
    family inet {
        address 192.168.1.254/24 {
            vrrp-group 100 {
                virtual-address 192.168.1.1;
                no-preempt;
            }
        }
    }
}
```

In the exhibit, what is the priority for Router B in VRRP group 100?

A. 1

B. 100

C. 110

D. 255

Answer: B

6. In a JSRP cluster with two J6350 routers, the interface ge-7/0/0 belongs to which device?

A. This interface is a system-created interface.

B. This interface belongs to NODE0 of the cluster.

C. This interface belongs to NODE1 of the cluster.

D. This interface will not exist because J6350 routers have only six slots.

Answer: C

7. Click the Exhibit button.

Based on the configuration shown in the exhibit, what will happen to the traffic matching the security policy?

```
[edit schedulers]
user@host# show
scheduler now {
    monday all-day;
    tuesday exclude;
    wednesday {
        start-time 07:00:00 stop-time
18:00:00;
    }
    thursday {
        start-time 07:00:00 stop-time
18:00:00;
    }
}

[edit security policies from-zone Private
to-zone External]
user@host# show
policy allowTransit {
    match {
        source-address PrivateHosts;
        destination-address ExtServers;
        application ExtApps;
    }
    then {
        permit {
            tunnel{
              ipsec-vpn myTunnel;
            }
        }
    }
    scheduler-name now;
}
```

A. The traffic is permitted through the myTunnel IPSec tunnel only on Tuesdays.
B. The traffic is permitted through the myTunnel IPSec tunnel daily, with the exception of Mondays.
C. The traffic is permitted through the myTunnel IPSec tunnel all day on Mondays, Wednesdays between 7:00 am and 6:00 pm, and Thursdays between 7:00 am and 6:00 pm.
D. The traffic is permitted through the myTunnel IPSec tunnel all day on Mondays, Wednesdays between 6:01 pm and 6:59 am, and Thursdays between 6:01 pm and 6:59 am.
Answer: C

8. Which parameters must you select when configuring operating system probes SCREEN options?
A. syn-fin, syn-flood, and tcp-no-frag
B. syn-fin, port-scan, and tcp-no-flag
C. syn-fin, fin-no-ack, and tcp-no-frag
D. syn-fin, syn-ack-ack-proxy, and tcp-no-frag
Answer: C
9. A route-based VPN is required for which scenario?

A. when the remote VPN peer is behind a NAT device
B. when multiple networks need to be reached across the tunnel
C. when the remote VPN peer is a dialup or remote access client
D. when a dynamic routing protocol such as OSPF is required across the VPN
Answer: D

10. On which three traffic types does firewall pass-through authentication work? (Choose three.)
A. ping
B. FTP
C. Telnet
D. HTTP
E. HTTPS
Answer: BCD

11. Which three parameters are configured in the IKE policy? (Choose three.)
A. mode
B. preshared key
C. external interface
D. security proposals
E. dead peer detection settings
Answer: ABD

12. Click the Exhibit button.

```
[edit chassis]
user@host# show
cluster {
    reth-count 3;
    node 0;
    node 1;
    redundancy-group 1 {
        node 0 priority 1;
        node 1 priority 100;
    }
}
```

In the exhibit, which statement is correct?
A. Three physical interfaces are redundant.
B. You must define an additional Redundancy Group.
C. node 0 will immediately become primary in the cluster.
D. You must issue an operational command and reboot the system for the above configuration to take effect.
Answer: D

13. Which command allows you to view the router's current priority for VRRP group 100 on interface ge-0/0/1.0?

A. show vrrp
B. show vrrp group 100
C. show interfaces ge-0/0/1.0 vrrp group 100
D. show interfaces vrrp ge-0/0/1.0 group 100
Answer:A

14. Which statement is true about interface-based static NAT?
A. It also supports PAT.
B. It requires you to configure address entries in the junos-nat zone.
C. It requires you to configure address entries in the junos-global zone.
D. The IP addresses being translated must be in the same subnet as the incoming interface.
Answer: D

15. Which two are components of the enhanced services software architecture? (Choose two.)
A. Linux kernel
B. routing protocol daemon
C. session-based forwarding module
D. separate routing and security planes
Answer: BC

16. Which two are characteristics of link-state routing protocols? (Choose two.)
A. Routers choose a best path for a destination based on the SPF algorithm.
B. All routers in a given area or level build a consistent database describing the network's topology.
C. Routers choose the best path for a destination based on the interface on which they received the link stateadvertisement with the lowest cost.
D. All routers in a given area or level forward link state advertisements between interfaces in the same area or level,
adding their metric to the link state advertisement's cost information when they forward it.
Answer:AB

17. Which two are components of the JUNOS software's routing policy? (Choose two.)
A. route-map
B. prefix-list
C. distribute-list
D. policy-statement
Answer: BD

18. Click the Exhibit button.

```
[edit security policies from-zone HR to-zone
trust]
user@host# show
policy two {
    match {
        source-address subnet_a;
        destination-address host_b;
        application [ junos-telnet junos-ping
];
    ...
    then {
        reject;
    ...
}
policy one {
    match {
        source-address host_a;
        destination-address subnet_b;
        application any;
    ...
    then {
        permit;
    ...
}
```

host_a is in subnet_a and host_b is in subnet_b.
Given the configuration shown in the exhibit, which statement is true about traffic from host_a to host_b?
A. DNS traffic is denied.
B. Telnet traffic is denied.
C. SMTP traffic is denied.
D. Ping traffic is permitted.
Answer: B

19. You want to create a policy allowing traffic from any host in the Trust zone to hostb.example.com (172.19.1.1) in the
Untrust zone. How do you do create this policy?
A. Specify the IP address (172.19.1.1/32) as the destination address in the policy.
B. Specify the DNS entry (hostb.example.com.) as the destination address in the policy.
C. Create an address book entry in the Trust zone for the 172.19.1.1/32 prefix and reference this entry in the policy.
D. Create an address book entry in the Untrust zone for the 172.19.1.1/32 prefix and reference this entry in the policy.
Answer: D

20. In JUNOS software with enhanced services, which three packet elements are inspected to determine if a session
already exists? (Choose three.)

A. IP protocol
B. IP time-to-live
C. source and destination IP address
D. source and destination MAC address
E. source and destination TCP/UDP port
Answer:ACE

21. Using a policy with the policy-rematch flag enabled, what happens to the existing and new sessions when you change the policy action from permit to deny?
A. The new sessions matching the policy are denied. The existing sessions are dropped.
B. The new sessions matching the policy are denied. The existing sessions, not being allowed to carry any traffic, simply timeout.
C. The new sessions matching the policy might be allowed through if they match another policy. The existing sessions are dropped.
D. The new sessions matching the policy are denied. The existing sessions continue until they are completed or their timeout is reached.
Answer:A

22. Host A opens a Telnet connection to Host B. Host A then opens another Telnet connection to Host B. These connections are the only communication between Host A and Host B. The security policy configuration permits both connections. How many flows exist between Host A and Host B?
A. 1
B. 2
C. 3
D. 4
Answer: D

23. Which two statements regarding asymmetric key encryption are true? (Choose two.)
A. The same key is used for encryption and decryption.
B. It is commonly used to create digital certificate signatures.
C. It uses two keys: one for encryption and a different key for decryption.
D. An attacker can decrypt data if the attacker captures the key used for encryption.
Answer: BC

24. You want to enable SSH and Telnet access to the router's CLI. Under which configuration hierarchy would you enable these protocols?
A. [edit system cli]
B. [edit security cli]
C. [edit system services]
D. [edit security services]
Answer: C

25. You are not able to telnet to the interface IP of your JUNOS software with enhanced services device from a PC on the same subnet. What is causing the problem?

A. Telnet is not being permitted by self policy.
B. Telnet is not being permitted by security policy.
C. Telnet is not allowed because it is not considered secure.
D. Telnet is not enabled as a host-inbound service on the zone.
Answer: D

26. Users can define policy to control traffic flow between which two components? (Choose two.)
A. from a zone to the router itself
B. from a zone to the same zone
C. from a zone to a different zone
D. from one interface to another interface
Answer: BC

27. Which three security concerns can be addressed by a tunnel mode IPSec VPN secured by AH? (Choose three.)
A. data integrity
B. data confidentiality
C. data authentication
D. outer IP header confidentiality
E. outer IP header authentication
Answer:ACE

28. Interface ge-0/0/2.0 of your router is attached to the Internet and is configured with an IP address and network mask
of 71.33.252.17/24. A host with IP address 10.20.20.1 is running an HTTP service on TCP port 8080. This host isattached to the ge-0/0/0.0 interface of your router. You must use interface-based static NAT to make the HTTP service on the host reachable from the Internet.
On which IP address and TCP port can Internet hosts reach the HTTP service?
A. IP address 10.10.10.1 and TCP port 8080
B. IP address 71.33.252.17 and TCP port 80
C. IP address 71.33.251.19 and TCP port 80
D. IP address 71.33.252.19 and TCP port 8080
Answer: D

29. Click the Exhibit button.
In the exhibit, what is the purpose of this OSPF configuration?

```
[edit protocols ospf]
user@host# show traceoptions
file debugOSPF;
flag hello send;
flag lsa-update;
```

A. The router sends the file debugOSPF (containing hellos sent and LSA updates) to the syslog server.
B. The router traces both OSPF hellos sent and LSA updates, and stores the results in the debugOSPF

file.
C. The router traces both OSPF hellos sent and LSA updates, and sends the results to the syslog process with the debugOSPF facility.
D. The router traces all OSPF operations, stores the results in the debugOSPF file, and marks both hellos sent and LSAupdates in the file with a special flag.
Answer: B