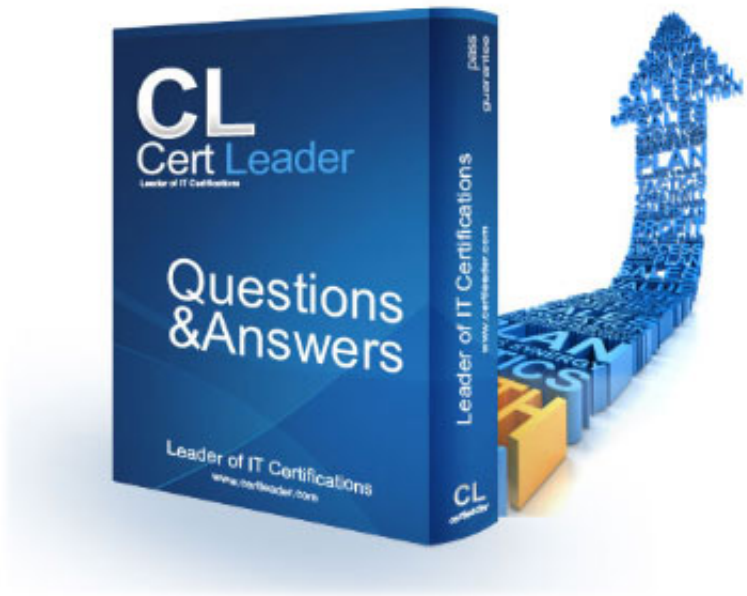
NSE4 - Fortinet Network Security Expert 4 Written Exam (400)

http://www.certleader.com/NSE4-dumps.html



1. Examine at the output below from the diagnose sys top command: # diagnose sys top 1 Run Time: 11 days, 3 hours and 29 minutes 0U, 0N, 1S, 99I; 971T, 528F, 160KF sshd 123 S 1.9 1.2 ipsengine 61 S < 0.0 5.2 miglogd 45 S 0.0 4.9

pyfcgid 75 S 0.0 4.5

pyfcgid 73 S 0.0 3.9

Which statements are true regarding the output above? (Choose two.)

A. The sshd process is the one consuming most CPU.

B. The sshd process is using 123 pages of memory.

C. The command diagnose sys kill miglogd will restart the miglogd process.

D. All the processes listed are in sleeping state.

Answer: A,D

2. Examine the following output from the diagnose sys session list command:

session info: proto=6 proto_state=65 duration=3 expire=9 timeout=3600 flags=00000000 sockflag=00000000 sockport=443 av_idx=9 use=5 origin-shaper=guarantee-100kbps prio=2 guarantee 12800Bps max 134217728Bps traffic

13895Bps

reply-shaper=guarantee-100kbps prio=2 guarantee 12800Bps max 134217728Bps traffic

13895Bps

state=redir local may_dirty ndr npu nlb os rs

statistic(bytes/packets/allow_err): org=864/8/1 reply=2384/7/1 tuples=3

orgin->sink: org pre->post, reply pre->post dev=7->6/6->7 gwy=172.17.87.3/10.1.10.1

hook=post dir=org act=snat 192.168.1.110:57999->74.201.86.29:443(172.17.87.16:57999)

hook=pre dir=reply act=dnat 74.201.86.29:443-

>172.17.87.16:57999(192.168.1.110:57999)

hook=post dir=reply act=noop 74.201.86.29:443->192.168.1.110:57999(0.0.0.0:0)

misc=0 policy_id=1 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0

npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0/0

Which statements are true regarding the session above? (Choose two.)

A. Session Time-To-Live (TTL) was configured to 9 seconds.

B. FortiGate is doing NAT of both the source and destination IP addresses on all packets coming from the 192.168.1.110 address.

C. The IP address 192.168.1.110 is being translated to 172.17.87.16.

D. The FortiGate is not translating the TCP port numbers of the packets in this session.

Answer: C,D

3. In which process states is it impossible to interrupt/kill a process? (Choose two.)

A. S – Sleep

B. R – Running

C. D – Uninterruptable Sleep

D. Z – Zombie

Answer: C,D

4. What functions can the IPv6 Neighbor Discovery protocol accomplish? (Choose two.)

A. Negotiate the encryption parameters to use.

B. Auto-adjust the MTU setting.

C. Autoconfigure addresses and prefixes.

D. Determine other nodes reachability.

Answer: C,D

5. Which statements are true regarding IPv6 anycast addresses? (Choose two.)

A. Multiple interfaces can share the same anycast address.

B. They are allocated from the multicast address space.

C. Different nodes cannot share the same anycast address.

D. An anycast packet is routed to the nearest interface.

Answer: A,D

6. Which statements are correct regarding an IPv6 over IPv4 IPsec configuration? (Choose two.)

A. The source quick mode selector must be an IPv4 address.

B. The destination quick mode selector must be an IPv6 address.

C. The Local Gateway IP must be an IPv4 address.

D. The remote gateway IP must be an IPv6 address.

Answer: B,C

7. Which IP packets can be hardware-accelerated by a NP6 processor? (Choose two.)

A. Fragmented packet.

B. Multicast packet.

C. SCTP packet.

D. GRE packet.

Answer: B,C

8. Which statements are true about offloading antivirus inspection to a Security Processor (SP)? (Choose two.)

A. Both proxy-based and flow-based inspection are supported.

B. A replacement message cannot be presented to users when a virus has been detected.

C. It saves CPU resources.

D. The ingress and egress interfaces can be in different SPs.

Answer: B,C

9. Two FortiGate units with NP6 processors form an active-active cluster. The cluster is doing security profile (UTM) inspection over all the user traffic. What statements are true regarding the sessions that the master unit is offloading to the slave unit for inspection? (Choose two.)

A. They are accelerated by hardware in the master unit.

B. They are not accelerated by hardware in the master unit.

C. They are accelerated by hardware in the slave unit.

D. They are not accelerated by hardware in the slave unit.

Answer: A,D

10. Which is one of the conditions that must be met for offloading the encryption and decryption of IPsec traffic to an NP6 processor?

A. No protection profile can be applied over the IPsec traffic.

B. Phase-2 anti-replay must be disabled.

C. Both the phase 1 and phases 2 must use encryption algorithms supported by the NP6.

D. IPsec traffic must not be inspected by any FortiGate session helper.

Answer: C

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 NSE4 Exam with Our Prep Materials Via below:

http://www.certleader.com/NSE4-dumps.html