NSE8^{Q&As}

NSE8^{Q&As}

Fortinet Network Security Expert 8 Written (800)

Pass Fortinet NSE8 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/nse8.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

```
# diag npu np6 port-list
Chip XAUI Ports Max   Cross-chip
                Speed offloading
------ ---- ------- ----- ----------
np6_0 0 port26 10G No
      1 port25 10G No
      2 port28 10G No
      3 port27 10G No
------ ---- ------- ----- ----------
np6_1 0 port30 10G No
      1 port29 10G No
      2 port32 10G No
      3 port31 10G No
------ ---- ------- ----- ----------
np6_2 0 port5 10G Yes
      0 port9 10G Yes
      0 port13 10G Yes
      1 port6 10G Yes
      1 port10 10G Yes
      1 port14 10G Yes
      2 port7 10G Yes
      2 port11 10G Yes
      3 port8 10G Yes
      3 port12 10G Yes
      0-3 port1 40G Yes
          port2 10G Yes
------ ---- ------- ----- ----------
np6_3 0 port15 10G Yes
      0 port19 10G Yes
      0 port23 10G Yes
      1 port16 10G Yes
      1 port20 10G Yes
      1 port24 10G Yes
```

Referring to the exhibit, you want to know if aggregating port7 and port22 will work. Which statement is correct?

A. Yes, LACP is supported on all ports regardless if they are connected to the same NP6.

B. No, LACP is not supported on NP6 platforms.

C. No, LACP is only supported on ports connected to the same NP6.

D. Yes, LACP is supported on ports that are linked together with integrated Switch Fabric.

Correct Answer: C

References: http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-hardware-acceleration-52/NP6.htm

QUESTION 2

Your company uses a cluster of two FortiGate 3600C units in active-passive mode to protect the corporate network. The FortiGate cluster sends its logs to a FortiAnalyzer and you have configured scheduled weekly reports for the Internet

bandwidth usage of each corporate VLAN. During a scheduled maintenance window, you make a series of configuration changes. When the next FortiAnalyzer weekly report is generated, you notice that Internet bandwidth usage reported by

the FortiAnalyzer is far less than expected.

What is the reason for this discrepancy?

A. You applied an antivirus profile on some of the policies, and no traffic can be accelerated.

B. You disabled all security profiles on some of the firewall policies, and the traffic matching those policies is now accelerated.

C. You enabled HA session-pickup, which is turn disabled session accounting.

D. You changed from active-passive to active-active, causing the session traffic counters to become inaccurate.

Correct Answer: D

Because of Active/Active failover traffic segregate to boxes where it reduces the bandwidth utilization

QUESTION 3

Which three configuration scenarios will result in an IPsec negotiation failure between two FortiGate devices? (Choose three.)

A. mismatched phase 2 selectors

B. mismatched Anti-Replay configuration

C. mismatched Perfect Forward Secrecy

D. failed Dead Peer Detection negotiation

E. mismatched IKE version

Correct Answer: C

In IPsec negotiations, Perfect Forward Secrecy (PFS) ensures that each new cryptographic key is unrelated to any previous key. Either enable or disable PFS on both the tunnel peers; otherwise, the LAN-to-LAN (L2L) IPsec tunnel is not established

QUESTION 4

A FortiGate is deployed in the NAT/Route operation mode. This operation mode operates at which OSI layer?

A. Layer 4

B. Layer 1

C. Layer 3

D. Layer 2

Correct Answer: C

QUESTION 5

A company wants to protect against Denial of Service attacks and has launched a new project. They want to block the attacks that go above a certain threshold and for some others they are just trying to get a baseline of activity for those types of attacks so they are letting the traffic pass through without action. Given the following:

-The interface to the Internet is on WAN1.

-There is no requirement to specify which addresses are being protected or protected from.

-

The protection is to extend to all services.

-

The tcp_syn_flood attacks are to be recorded and blocked.

-

The udp_flood attacks are to be recorded but not blocked.

-

The tcp_syn_flood attack\\'s threshold is to be changed from the default to 1000. The exhibit shows the current DoS-policy.

Exhibit ☒

```
config firewall DoS-policy
    edit 1
        set status disable
        set interface "wan1"
        set service "ALL_TCP" "ALL_UDP"
        config anomaly
            edit "tcp_syn_flood"
                set threshold 2000
            next
            edit "udp_flood"
                set threshold 2000
            next
        end
```

Close

Which policy will implement the project requirements?

A.

```
config firewall DoS-policy
    edit 1
        set status enable
        set interface "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL_TCP" "ALL_UDP"
            config anomaly
                edit "tcp_syn_flood"
                    set status enable
                    set log enable
                    set action block
                    set threshold 1000
                next
                  edit "udp_flood"
                    set status enable
                    set log enable
                    set threshold 1000
                next
    end
```

B.

```
config firewall DoS-policy
    edit 1
        set status enable
        set interface "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL_TCP" "ALL_UDP"
            config anomaly
                edit "tcp_syn_flood"
                    set status enable
                    set log enable
                    set action block
                    set threshold 1000
                next
                  edit "udp_flood"
                    set status enable
                    set log enable
                    set threshold 2000
                next
```

A. B.

C.

D.

```
config firewall DoS-policy
    edit 1
        set status enable
        set interface "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL_TCP" "ALL_UDP"
            config anomaly
                edit "tcp_syn_flood"
                    set status enable
                    set log enable
                    set action block
                    set threshold 1000
                next
                  edit "udp_flood"
                    set log enable
                    set status enable
                    set action block
                    set threshold 1000
                next
    end

config firewall DoS-policy
    edit 1
        set status enable
        set interface "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL_TCP" "ALL_UDP"
            config anomaly
                edit "tcp_syn_flood"
                    set status enable
                    set action block
                    set threshold 1000
                next
                  edit "udp_flood"
                    set status enable
                    set log enable
                    set threshold 2000
                next
```

Correct Answer: BD

BandD both have same policy which fulfills the above criteria. http://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-firewall-52/Examples/Example-%20DoS%20Policy.htm

[NSE8 PDF Dumps](#)   [NSE8 Study Guide](#)   [NSE8 Braindumps](#)

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

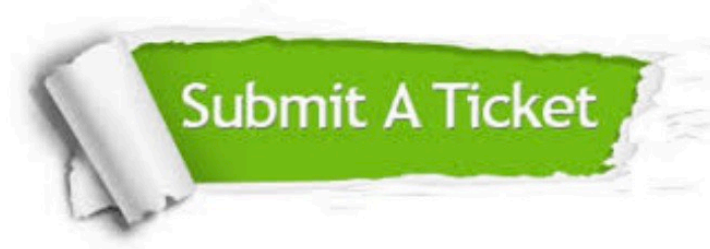100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.passapply.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: