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.pass4lead.com/nse8.html

100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

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.


```
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
```

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

QUESTION 2

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 3

⊟⊼Exhibit ⊠

```
session info: proto=6 proto_state=01 duration=649
expire=3574 timeout=3600 flags=00000000
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 hakey=49722
policy_dir=0 tunnel=/
state=log may_dirty npu synced
statistic(bytes/packets/allow_err): org=13730/26/1
reply=5092/26/1 tuples=3
orgin->sink: org pre->post, reply pre->post
dev=29->32/32->29 gwy=10.209.101.204/195.219.251.249
hook=pre dir=org act=dnat
176.63.92.110:50085->195.219.248.105:80(10.209.101.2
04:80)
hook=post dir=reply act=snat
10.209.101.204:80->176.63.92.110:50085(195.219.248.1
05:80)
hook=post dir=org act=noop
176.63.92.110:50085->10.209.101.204:80(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=96 id_policy_id=0 auth_info=0
chk_client_info=0 vd=0
serial=000e1d9b tos=ff/ff ips_view=1 app_list=0
app=0
dd_type=0 dd_rule_id=0
per_ip_bandwidth meter: addr=176.63.92.110, bps=1006
npu_state=00000000
npu info: flag=0x81/0x81, offload=4/4,
ips_offload=0/0, epid=35/32, ipid=32/35, vlan=0/0
```

Clearer pictures and no water-mask in the Premium Product

⊠ Close

Referring to the configuration shown in the exhibit, which three statements are true? (Choose three.)

A. Traffic logging is disabled in policy 96.

B. TCP handshake is completed and no FIN/RST has been forwarded.

C. No packet has hit this session in the last five minutes.

D. No QoS is applied to this traffic.

E. The traffic goes through a VIP applied to policy 96.

Correct Answer: B

References: http://kb.fortinet.com/kb/viewContent.do?externalId=FD30042

QUESTION 4

show bridge control interface root.b host.
fdb: size=256, used=6, num=7, depth=2, simple=no
Bridge root.b host table

port no device devname mac addr ttl attributes
2   7 wan2 02:09:0f:78:69:00 0 Local Static
5   6 vlan_1 02:09:0f:78:69:01 0 Local Static
3   8 dmz 02:09:0f:78:69:01 0 Local Static
4   9 internal 02:09:0f:78:69:02 0 Local Static
3   8 dmz 00:80:c8:39:87:5a 194
4   9 internal 02:09:0f:78:67:68 8
1   3 wan1 00:09:0f:78:69:fe 0 Local Static

Referring to the command output shown in the exhibit, how many hosts are connected to the FortiGate?

A. 7

B. 6

C. 2

D. 256

Correct Answer: B

References: http://cookbook.fortinet.com/troubleshooting-fortigate-installation/

QUESTION 5

Which command syntax would you use to configure the serial number of a FortiGate as its host name?

A.
```
config system global
set hostname &SerialNum
end
```

B.
```
config system global
set hostname @SerialNum
end
```

C.
```
config system global
set hostname $SerialNum
end
```

D.
```
config system global
set hostname SerialNum
end
```
Clearer pictures and no water-mask in the Premium Product

A. B. C. D.

Correct Answer: C

References:
http://docs.fortinet.com/uploaded/files/2002/FortiOS%20Handbook%20-%20System%20Administration%205.2.pdf

NSE8 VCE Dumps   **NSE8 Exam Questions**   **NSE8 Braindumps**

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
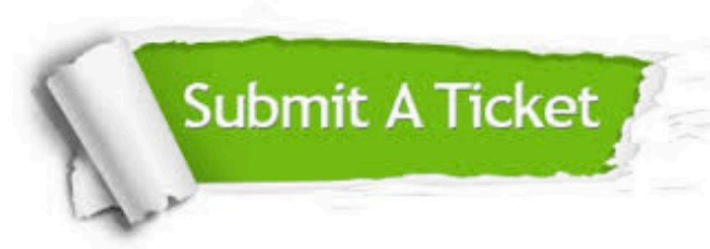Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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.pass4lead.com/allproducts

Need Help

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

One Year Free Update
Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee
To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy
We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.