



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.lead4pass.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 customer is authenticating users using a FortiGate and an external LDAP server. The LDAP user, John Smith, cannot authenticate. The administrator runs the debug command diagnose debug application fnbamd 255 while John Smith

attempts the authentication:

Based on the output shown in the exhibit, what is causing the problem?

```
fnbamd_ldap.c[232]
start_search_dn-base: 'DC=TAC, DC=ottawa, DC=fortinet, DC
=com' filter:sAMAccountName=j.smith
fnbamd_ldap.c[1351] fnbamd_ldap_get_result-Going to
SEARCH state
fnbamd_fsm.c[1833] poll_ldap_servers-Continue
pending for req 6750217
fnbamd_ldap.c[266] get_all_dn-Found DN 1:CN=John
Smith, CN=Users, DC=TAC, DC=ottawa, DC=fortinet, DC=com
fnbamd_ldap.c[280] get_all_dn-Found 1 DN's
fnbamd_ldap.c[314] start_next_dn_bind-Trying DN
1:CN=John
Smith, CN=Users, DC=TAC, DC=ottawa, DC=fortinet, DC=com
fnbamd_ldap.c[1399] fnbamd_ldap_get_result-Going to
USERBIND state
fnbamd_ldap.c[1603] fnbamd_ldap_get_result-Auth
denied
fnbamd_auth.c[2074] fnbamd_auth_poll_ldap-Result for
ldap svr 10.10.181.10 is denied
fnbamd_comm.c[116] fnbamd_comm_send_result-Sending
result 1 for req 6750217
```

Clearer pictures and no water-mask in the Premium Product

- A. The LDAP administrator password in the FortiGate configuration is incorrect.
- B. The user, John Smith, does have an account in the LDAP server.
- C. The user, John Smith, does not belong to any allowed user group.
- D. The user, John Smith, is using an incorrect password.

Correct Answer: A

Fortigate not binded with LDAP server because of failed authentication. Reference:
<http://kb.fortinet.com/kb/documentLink.do?externalID=FD31886>

QUESTION 2



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
```

Clearer pictures and no water-mask in the Premium Product

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
    end
```

Clearer pictures and no water-mask in the Premium Product



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
```

Clearer pictures and no water-mask in the Premium Product

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 3

A customer wants to implement a RADIUS Single Sign On (RSSO) solution for multiple FortiGate devices. The customer's network already includes a RADIUS server that can generate the logon and logoff accounting records. However, the

RADIUS server can send those records to only one destination.

What should the customer do to overcome this limitation?

- A. Send the RADIUS records to an LDAP server and add the LDAP server to the FortiGate configuration.
- B. Send the RADIUS records to an RSSO Collector Agent.
- C. Send the RADIUS records to one of the FortiGate devices, which can replicate them to the other FortiGate units.
- D. Use the RADIUS accounting proxy feature available in FortiAuthenticator devices.

Correct Answer: B

References: <http://docs.fortinet.com/uploaded/files/1937/fortigate-authentication-52.pdf>

QUESTION 4



```
Exhibit
diagnose wireless-controller wlaac -c byod_detected

INDEX VFID      MAC          ACT
TYPE                                USER

-----wlan(root/0, staff) acl
(staff-devices)-----
  0    0 00:0b:7d:26:2b:4d  accept
Windows PC          tom
  1    0 00:25:bc:45:a5:55  accept
iPhone sam
  2    0 00:c0:ca:65:f1:ff  accept
Linux PC liz
  3    0 18:34:51:43:12:52  accept
iPhone ben
  4    0 40:a6:d9:70:c5:28  accept
iPhone sue
  5    0 48:60:bc:10:c5:2f  accept
iPhone bob
  6    0 58:94:6b:53:9f:80  accept
Windows PC          jon
  7    0 a0:0b:ba:b5:ed:2c  deny
Android Phone cat
  8    0 b4:07:f9:0b:58:cd  deny
Android Phone caz
  9    0 d0:23:db:35:46:12  accept
iPhone pat
 10    0 e0:b9:a5:6f:f4:20  deny
Android Phone pam

-----wlan(root/0, guest) acl
(no )-----
Clearer pictures and no water-mask in the Premium Product
Close
```

The wireless controller diagnostic output is shown in the exhibit. Which three statements are true? (Choose three.)

- A. Firewall policies using device types are blocking Android devices.
- B. An access control list applied to the VAP interface blocks Android devices.
- C. This is a CAPWAP control channel diagnostic command.
- D. There are no wireless clients connected to the guest wireless network.
- E. The "src-vis" process is active on the staff wireless network VAP interface.

Correct Answer: A

References: <http://docs.fortinet.com/uploaded/files/1083/fortigate-managing-devices-50.pdf>



QUESTION 5

Your NOC contracts the security team due to a problem with a new application flow. You are instructed to disable hardware acceleration for the policy shown in the exhibit for troubleshooting purposes.

```
config firewall policy
  edit 3
    set uuid
9957c4d6-560f-51e4-3914-6d9366f64e8d
    set srcintf "dmz5"
    set dstintf "wan1"
    set srcaddr "bookings"
    set dstaddr "partners"
    set action accept
    set schedule "always"
    set service "customtelnet"
    set utm-status enable
    set av-profile "default"
    set ips-sensor "default"
    set logtraffic all
    set spamfilter-profile "default"
    set profile-protocol-options "default"
  next
end
config ips sensor
  edit "default"
    set comment "prevent critical attacks"
    config entries
      edit 1
        set severity medium high
      critical
    next
  end
next
end
```

Clearer pictures and no water-mask in the Premium Product

Which command will disable hardware acceleration for the new application policy?



- A.

```
config firewall policy
edit 3
set hardware-accel-mode none
end
```
- B.

```
config ips global
set hardware-accel-mode none
end
```
- C.

```
config ips sensor
set hardware-accel-mode engine-no-pickup
end
```

A. B. C.

```
config firewall policy
edit 3
set auto-asic-offload disable
end
```

D.

Correct Answer: D

References: <http://docs.fortinet.com/uploaded/files/1607/fortigate-hardware-accel-50.pdf>



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.lead4pass.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 <p>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.</p>	 <p>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.</p>	 <p>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.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © lead4pass, All Rights Reserved.