

Fortinet

Exam NSE8

Fortinet Network Security Expert 8 Written Exam

Version: Demo

[Total Questions: 10]

Question No : 1

Which VPN protocol is supported by FortiGate units?

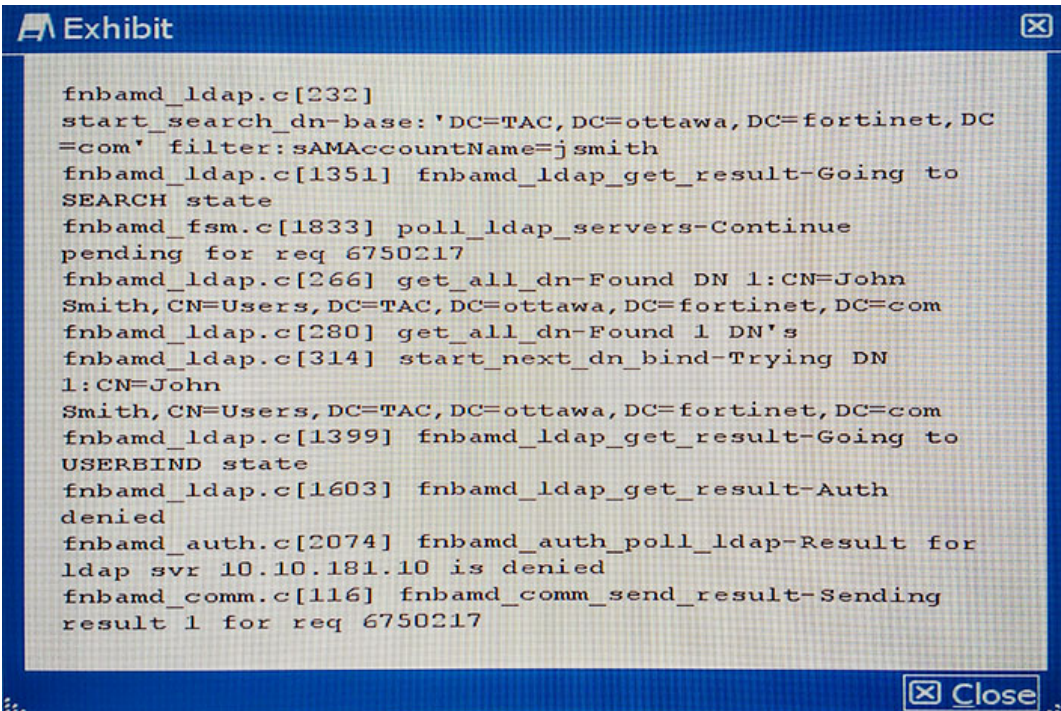
- A. E-LAN
- B. PPTP
- C. DMVPN
- D. OpenVPN

Answer: B,C

Question No : 2

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?



```
Exhibit
fnbamd_ldap.c[232]
start_search_dn-base: 'DC=TAC, DC=ottawa, DC=fortinet, DC=com' filter: sAMAccountName=jsmith
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
Close
```

- 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.

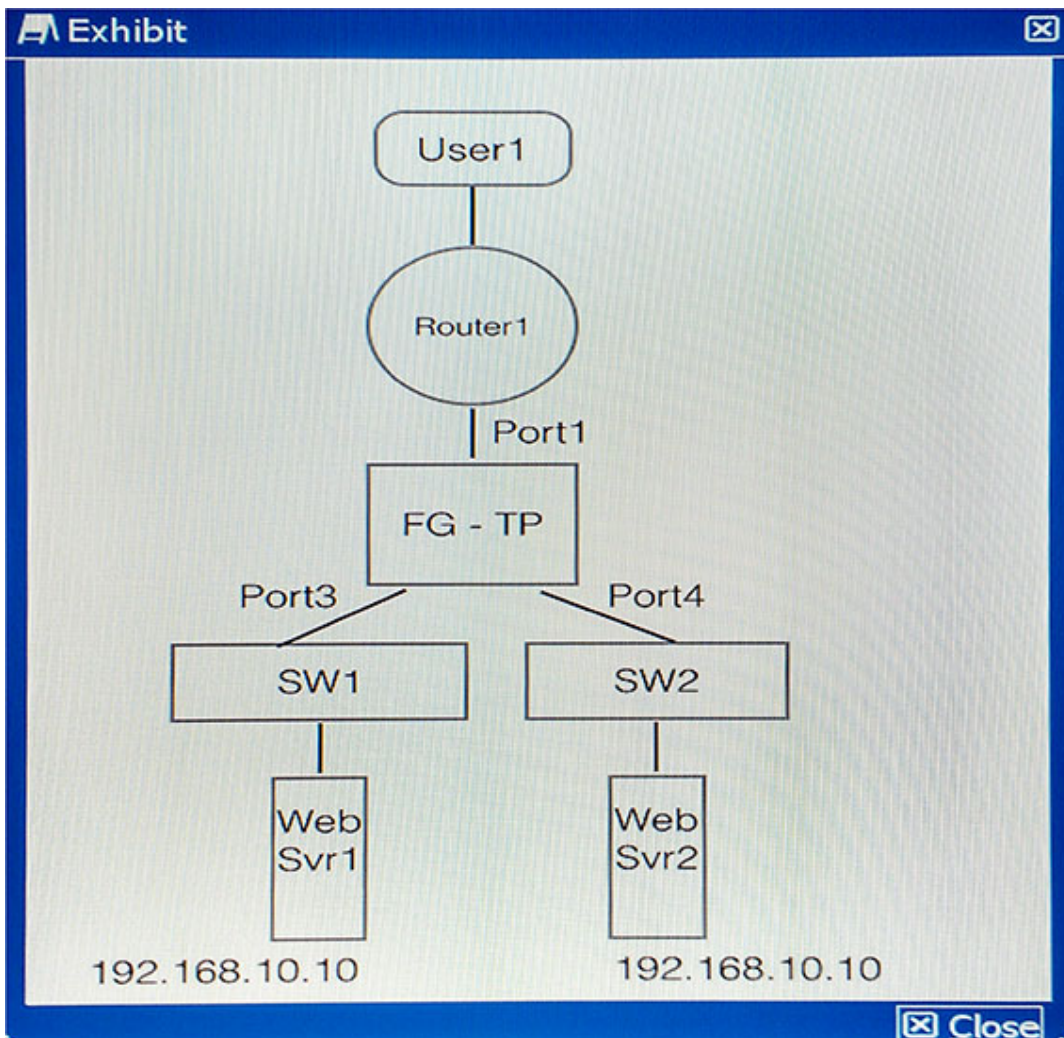
Answer: A

Explanation:

Fortigate not binded with LDAP server because of failed authentication.

References:

Question No : 3



You have implemented FortiGate in transparent mode as shown in the exhibit. User1 from the Internet is trying to access the 192.168.10.10 Web servers.

Which two statements about this scenario are true? (Choose two.)

- A. User1 would be able to access the Web server intermittently.
- B. User1 would not be able to access any of the Web servers at all.
- C. FortiGate learns Web servers MAC address when the Web servers transmit packets.
- D. FortiGate always flood packets to both Web servers at the same time.

Answer: A,C

Explanation:

Both servers have same ip address, so there will be intermittent we server connectivity from outside and whichever web server forwards packets fortigate learns its mac address.

Question No : 4

You are asked to write a FortiAnalyzer report that lists the session that has consumed the most bandwidth. You are required to include the source IP, destination IP, application, application category, hostname, and total bandwidth consumed.

Which dataset meets these requirements?

- A. `select from _itime(itime) as timestamp, srcip, dstip, app, appcat, hostname, sum(coalesce('sentbyte', 0) +coalesce('recbyte', 0)) as bandwidth from $log where $filter LIMIT 1`
- B. `select from _itime(itime) as timestamp, srcip, dstip, app, appcat, hostname, sum(coalesce('sentbyte', 0) +coalesce('rcvbyte', 0)) as bandwidth from $log where $filter LIMIT 1`
- C. `select from _itime(itime) as timestamp, srcip, dstip, app, appcat, hostname, sum(coalesce('sentbyte', 0) +coalesce('rcvdbyte', 0)) as bandwidth from $log where $filter LIMIT 1`
- D. `select from _itime(itime) as timestamp, sourceip, destip, app, appcat, hostname, sum(coalesce('sentbyte', 0)+coalesce('rcvdbyte', 0)) as bandwidth from $log where $filter LIMIT 1`

Answer: C

Explanation:

References:

<http://docs.fortinet.com/uploaded/files/2617/fortianalyzer-5.2.4-dataset-reference.pdf>

Question No : 5

Which two features are supported only by FortiMail but not by FortiGate? (Choose two.)

- A. DNSBL
- B. built-in MTA
- C. end-to-end IBE encryption
- D. FortiGuard Antispam

Answer: A,B

Question No : 6

```
diagnose wireless-controller wlac -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
(none)-----
```

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.

Answer: A,C,D

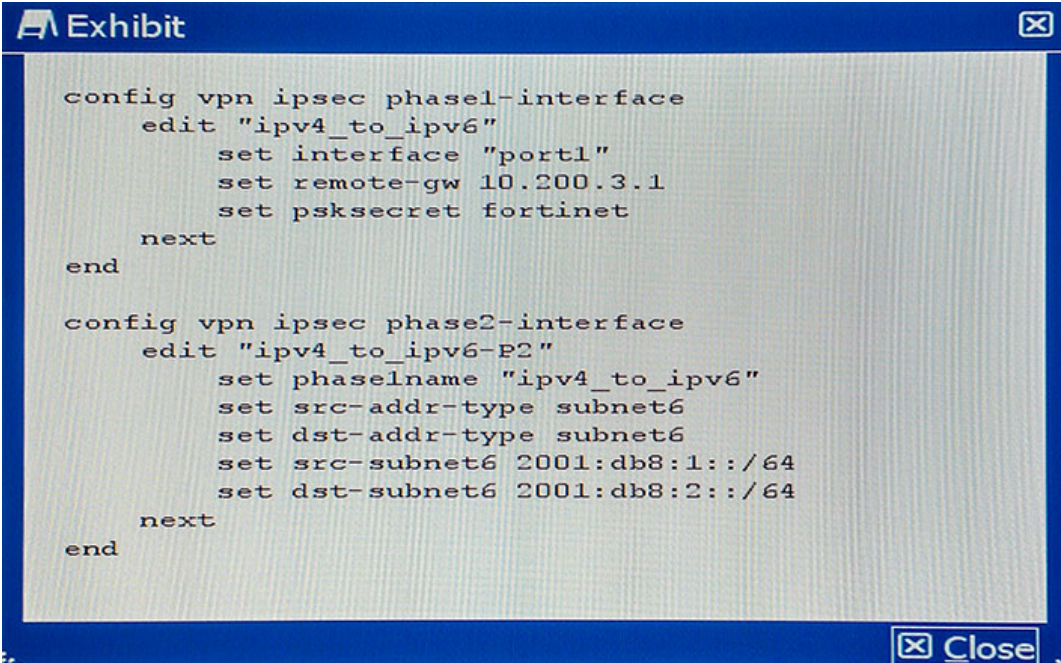
Explanation:

References:

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

Question No : 7

You want to enable traffic between 2001:db8:1::/64 and 2001:db8:2::/64 over the public IPv4 Internet.



```
config vpn ipsec phase1-interface
  edit "ipv4_to_ipv6"
    set interface "port1"
    set remote-gw 10.200.3.1
    set psksecret fortinet
  next
end

config vpn ipsec phase2-interface
  edit "ipv4_to_ipv6-P2"
    set phaselname "ipv4_to_ipv6"
    set src-addr-type subnet6
    set dst-addr-type subnet6
    set src-subnet6 2001:db8:1::/64
    set dst-subnet6 2001:db8:2::/64
  next
end
```

Given the CLI configuration shown in the exhibit, which two additional settings are required on this device to implement tunneling for the IPv6 transition? (Choose two.)

- A. IPv4 firewall policies to allow traffic between the local and remote IPv6 subnets.
- B. IPv6 static route to the destination phase2 destination subnet.
- C. IPv4 static route to the destination phase2 destination subnet.
- D. IPv6 firewall policies to allow traffic between the local and remote IPv6 subnets.

Answer: B,D

Explanation:

References:

<http://docs.fortinet.com/uploaded/files/1969/IPv6%20Handbook%20for%20FortiOS%205.2.pdf>

Question No : 8

A university is looking for a solution with the following requirements:

- wired and wireless connectivity
- authentication (LDAP)
- Web filtering, DLP and application control
- data base integration using LDAP to provide access to those students who are up-to-date with their monthly payments
- support for an external captive portal

Which solution meets these requirements?

- A.** FortiGate for wireless controller and captive portalFortiAP for wireless connectivityFortiAuthenticator for user authentication and REST API for DB integrationFortiSwitch for PoE connectivityFortiAnalyzer for log and report
- B.** FortiGate for wireless controllerFortiAP for wireless connectivityFortiAuthenticator for user authentication, captive portal and REST API for DB integrationFortiSwitch for PoE connectivityFortiAnalyzer for log and report
- C.** FortiGate for wireless control and user authenticationFortiAuthenticator for captive portal and REST API for DB integrationFortiAP for wireless connectivityFortiSwitch for PoE connectivityFortiAnalyzer for log and report
- D.** FortiGate for wireless controllerFortiAP for wireless connectivity and captive portalFortiSwitch for PoE connectivityFortiAuthenticator for user authentication and REST API for DB integrationFortiAnalyzer for log and reports

Answer: A

Question No : 9

You are an administrator of FortiGate devices that use FortiManager for central

management. You need to add a policy on an ADOM, but upon selecting the ADOM drop-down list, you notice that the ADOM is in locked state. Workflow mode is enabled on your FortiManager to define approval or notification workflow when creating and installing policy changes.

What caused this problem?

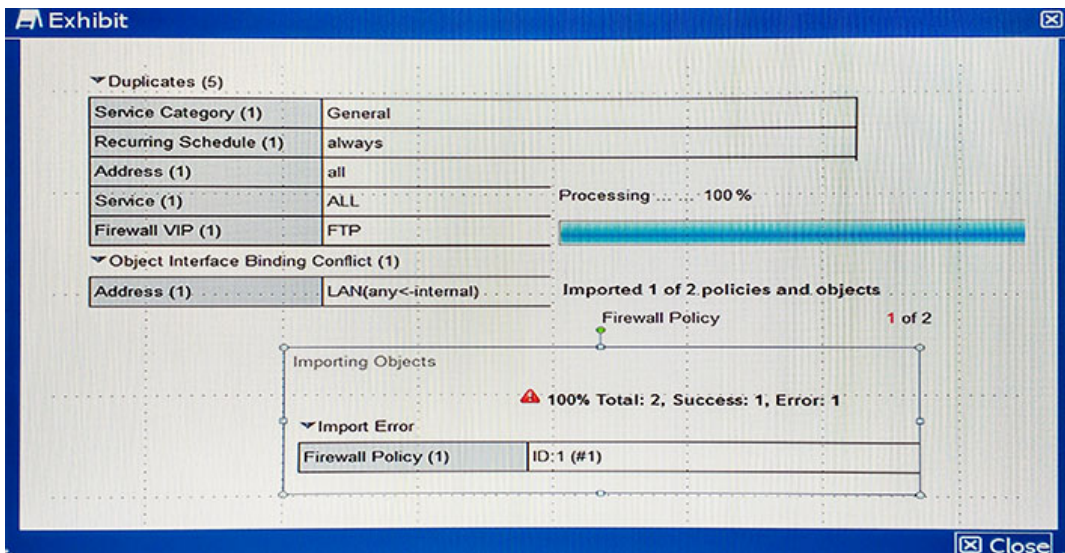
- A. Another administrator has locked the ADOM and is currently working on it.
- B. There is pending approval waiting from a previous modification.
- C. You need to use set workspace-mode workflow on the CLI.
- D. You have read-only permission on Workflow Approve in the administrator profile.

Answer: D

Explanation:

<http://docs.fortinet.com/uploaded/files/2250/FortiManager-5.2.1-Administration-Guide.pdf>

Question No : 10



Given the following error message:

Fortinet NSE8 : Practice Test

```
Start to import config from device(STUDENT-2) vdom(root) to adom(root), package(STUDENT-2)
"firewall service category",SUCCESS,"(name=General, oid=377, DUPLICATE)"
"firewall schedule recurring",SUCCESS,"(name=always, oid=473, DUPLICATE)"
"firewall address",SUCCESS,"(name=all, oid=364, DUPLICATE)"
"firewall service custom",SUCCESS,"(name=ALL, oid=426, DUPLICATE)"
"firewall vip",SUCCESS,"(name=FTP, iod=475, DUPLICATE)"
"firewall policy",FAIL"(name=ID:1 (#1), oid=513, reason=interface binding contradiction)"
"firewall policy", SUCCESS,"(name=3, oid=514, new object)"
```

FortiManager fails to import policy ID 1.

What is the problem?

- A.** FortiManager already has Address LAN which has interface mapping set to “internal” in its database, it is contradicting with the STUDENT-2 FortiGate device which has address LAN mapped to “any”.
- B.** FortiManager already has address LAN which has interface mapping set to “any” in its database; this conflicts with the STUDENT-2 FortiGate device which has address “LAN” mapped to “internal”.
- C.** Policy ID 1 for this managed FortiGate device already exists on the FortiManager policy package named STUDENT-2.
- D.** Policy ID 1 does not have interface mapping on FortiManager.

Answer: D

Explanation:

References:

<http://kb.fortinet.com/kb/documentLink.do?externalID=FD38544>