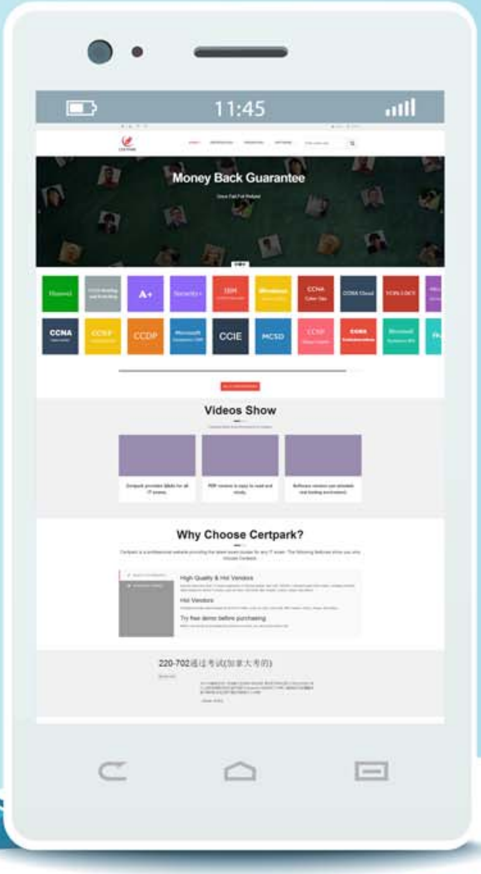


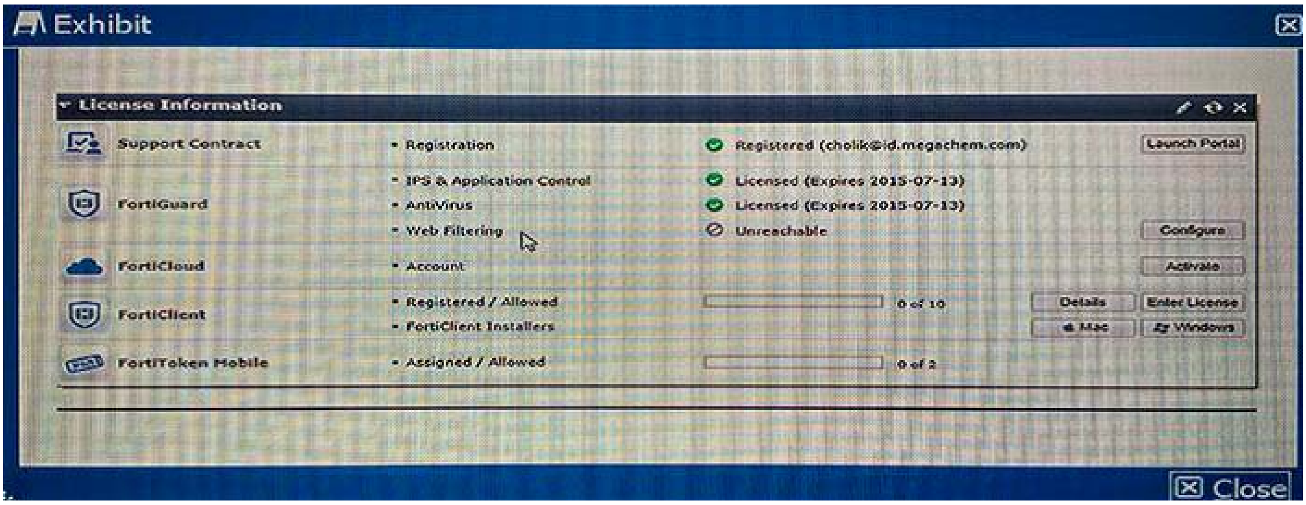
11:45
Money Back Guarantee
Huawei
A+
Security+
CCNA
CCNP
CCDP
CCIE
MCSD
Videos Show
Why Choose Certpark?
High Quality & Hot Vendors
Hot Vendors
Try free demo before purchasing

Exam : **NSE8**

Title : Fortinet Network Security
Expert 8 Written (800)

Version : DEMO

1.The dashboard widget indicates that FortiGuard Web Filtering is not reachable. However, AntiVirus, IPS, and Application Control have no problems as shown in the exhibit.



Support Contract	• Registration	Registered (cholik@id.megachem.com)
FortiGuard	• IPS & Application Control	Licensed (Expires 2015-07-13)
	• AntiVirus	Licensed (Expires 2015-07-13)
	• Web Filtering	Unreachable
FortiCloud	• Account	
FortiClient	• Registered / Allowed	0 of 10
	• FortiClient Installers	
FortiToken Mobile	• Assigned / Allowed	0 of 2

You contacted Fortinet’s customer service and discovered that your Fortiguard Web Filtering contract is still valid for several months.

What are two reasons for this problem? (Choose two.)

A. You have another security device in front of FortiGate blocking ports 8888 and 53.

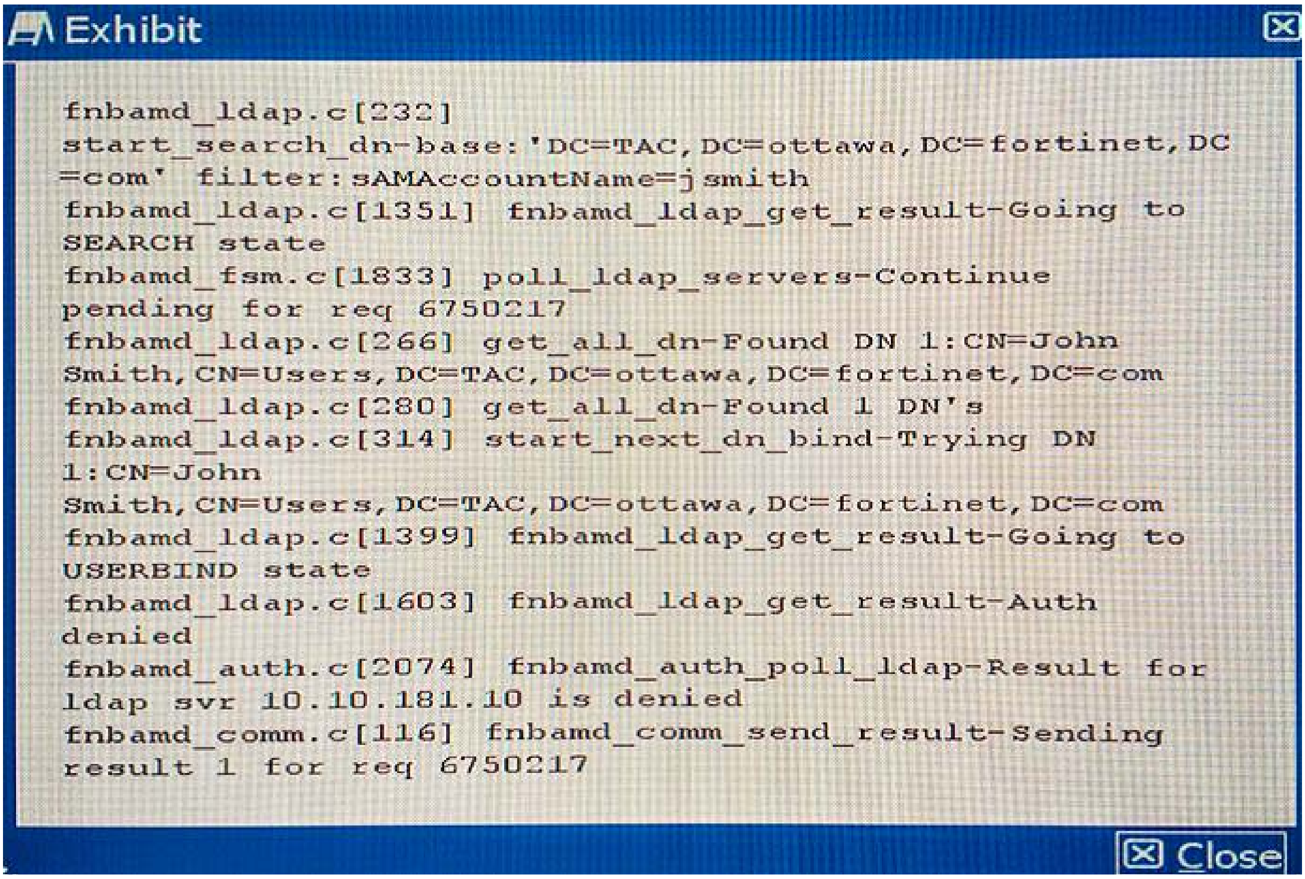
B. FortiGuard Web Filtering is not enabled in any firewall policy.

C. You did not enable Web Filtering cache under Web Filtering and E-mail Filtering Options.

D. You have a firewall policy blocking ports 8888 and 53.

Answer: B,D

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:



```
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
```

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

A. The LDAP administrator password in the FortiGate configuration is incorrect.

B. The user, John Smith, does have an account in the LDAP server.

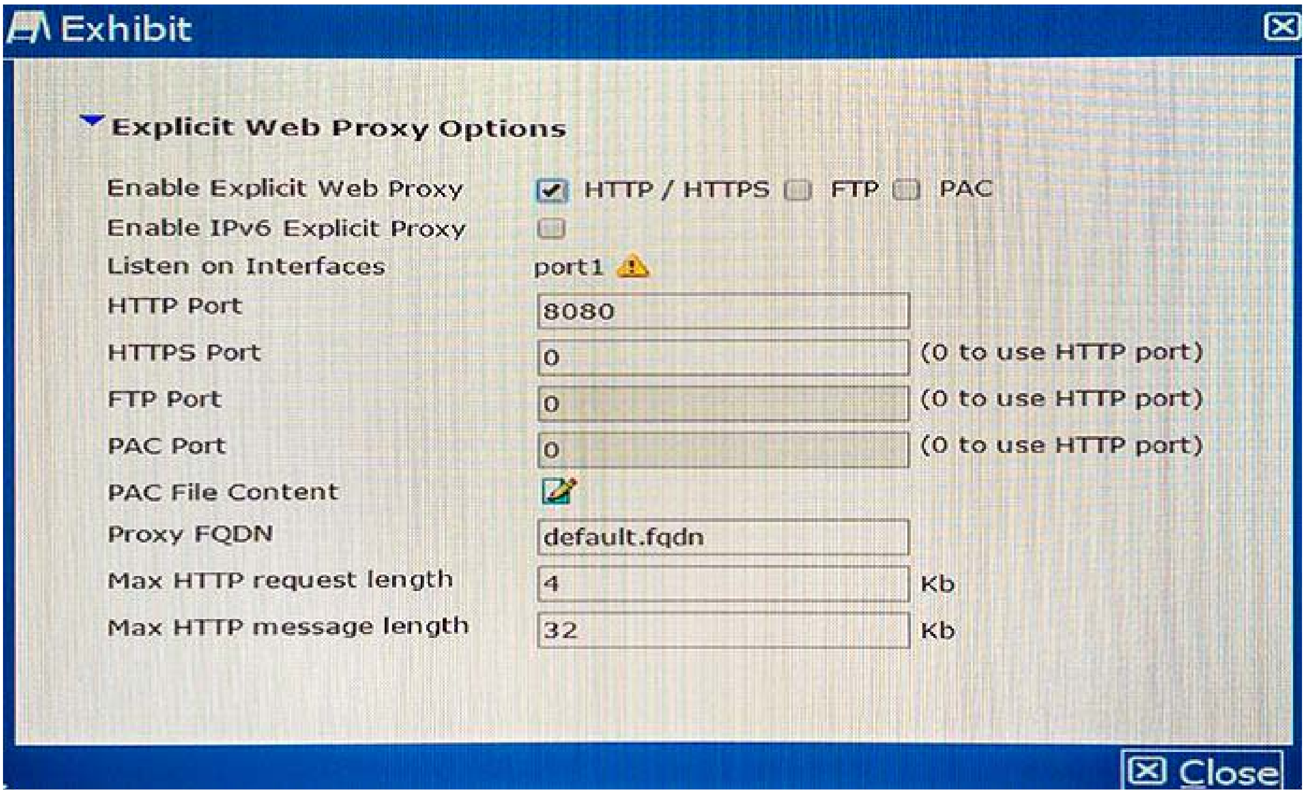
C. The user, John Smith, does not belong to any allowed user group.

D. The user, John Smith, is using an incorrect password.

Answer: A

3.The exhibit shows an explicit Web proxy configuration in a FortiGate device. The FortiGate is installed between a client with the IP address 172.16.10.4 and a Web server using port 80 with the IP address 10.10.3.4. The client Web browser is properly sending HTTP traffic to the FortiGate Web proxy IP address 172.16.10.254.

Which two sniffer commands will capture this HTTP traffic? (Choose two.)

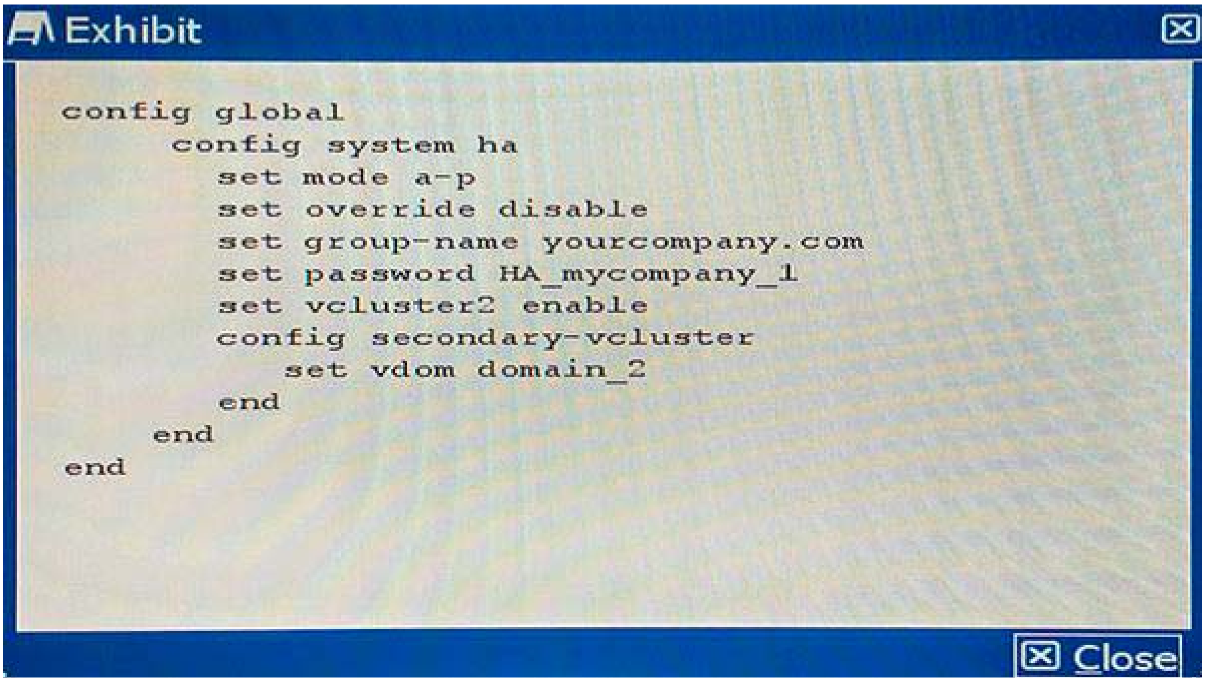


Explicit Web Proxy Options

Enable Explicit Web Proxy ☑ HTTP / HTTPS ☐ FTP ☐ PAC
Enable IPv6 Explicit Proxy ☐
Listen on Interfaces port1 ⚠
HTTP Port 8080
HTTPS Port 0 (0 to use HTTP port)
FTP Port 0 (0 to use HTTP port)
PAC Port 0 (0 to use HTTP port)
PAC File Content
Proxy FQDN default.fqdn
Max HTTP request length 4 Kb
Max HTTP message length 32 Kb

A. diagnose sniffer packet any 'host 172.16.10.4 and host 172.16.10.254' 3
B. diagnose sniffer packet any 'host 172.16.10.254 and host 10.10.3.4' 3
C. diagnose sniffer packet any 'host 172.16.10.4 and port 8080' 3
D. diagnose sniffer packet any 'host 172.16.10.4 and host 10.10.3.4' 3
Answer: C,D

4.Your colleague has enabled virtual clustering to load balance traffic between the cluster units. You notice that all traffic is currently directed to a single FortiGate unit. Your colleague has applied the configuration shown in the exhibit.



```
config global
     config system ha
        set mode a-p
        set override disable
        set group-name yourcompany.com
        set password HA_mycompany_1
        set vcluster2 enable
        config secondary-vcluster
           set vdom domain_2
        end
     end
end
```

Which step would you perform to load balance traffic within the virtual cluster?
A. Issue the diagnose sys ha reset-uptime command on the unit that is currently processing traffic to enable load balancing.
B. Add an additional virtual cluster high-availability link to enable cluster load balancing.
C. Input Virtual Cluster domain 1 and Virtual Cluster domain 2 device priorities for each cluster unit.
D. Use the set override enable command on both units to allow the secondary unit to load balance traffic.
Answer: C

5.A data center for example.com hosts several separate Web applications. Users authenticate with all of them by providing their Active Directory (AD) login credentials. You do not have access to Example, Inc.'s AD server. Your solution must do the following:
- provide single sign-on (SSO) for all protected Web applications
- prevent login brute forcing
- scan FTPS connections to the Web servers for exploits
- scan Webmail for OWASP Top 10 vulnerabilities such as session cookie hijacking, XSS, and SQL injection attacks

Which solution meets these requirements?
A. Apply FortiGate deep inspection to FTPS. It must forward FTPS, HTTP, and HTTPS to FortiWeb. Configure FortiWeb to query the AD server, and apply SSO for Web requests. FortiWeb must forward FTPS directly to the Web servers without inspection, but proxy HTTP/HTTPS and block Web attacks.
B. Deploy FortiDDos to block brute force attacks. Configure FortiGate to forward only FTPS, HTTP, and HTTPS to FortiWeb. Configure FortiWeb to query the AD server, and apply SSO for Web requests. Also configure it to scan FTPS and Web traffic, then forward allowed traffic to the Web servers.
C. Use FortiGate to authenticate and proxy HTTP/HTTPS; to verify credentials, FortiGate queries the AD server. Also configure FortiGate to scan FTPS before forwarding, and to mitigate SYN floods. Configure FortiWeb to block Web attacks.
D. Install FSSO Agent on servers. Configure FortiGate to inspect FTPS. FortiGate will forward FTPS, HTTP, and HTTPS to FortiWeb. FortiWeb must block Web attacks, then forward all traffic to the Web servers.
Answer: D