Fortinet

NSE8-812

Fortinet NSE 8 Written Exam

Question #48 Section 1

Consider the following configuration setting:

```
config user setting
    set auth-type https ftp
    set auth-cert "Fortinet_Factory"
    set auth-timeout 5
    set auth-timeout-type hard-timeout
    set auth-blackout-time 15
    set auth-lockout-threshold 5
    set auth-lockout-duration 10
end
```

Which two statements about local authentication are true? (Choose two.)

- A. The FortiGate will allow the TCP connection when a ClientHello message indicating a renegotiation is received.
- B. The user's IP address will be blocked 15 seconds after five login failures.
- C. The user will be blocked 15 seconds after five login failures.
- D. The user will need to re-authenticate after five minutes.

Answer: BD

Question #49 Section 1

You are asked to implement a single FortiGate 5000 chassis using Session-aware Load Balance Cluster (SLBC) with Active-Passive FortiControllers. Both FortiControllers have the configuration shown below, with the rest of the configuration set to the default values.

```
config system ha
    set mode dual
    set password fortinetnse8
    set group-id 5
    set chassis-id 1
    set minimize-chassis-failover enable
    set hbdev "b1"
end
```

Both FortiControllers show Master status.
What is the problem in this scenario?

- A. The b1 interface of the two FortiControllers do not see each other.
- B. The management interface of both FortiControllers was connected on the same network.
- C. The chassis ID settings on FortiController on slot 2 should be set to 2.
- D. The priority should be set higher for FortiController on slot-1.

Answer: A

Question #50 Section 1

You must create a High Availability deployment with two FortiWebs in Amazon Web Services (AWS); each on different Availability Zones (AZ) from the same region. At the same time, each FortiWeb should be able to deliver content from the Web servers of both of the AZs.
Which deployment would fulfill this requirement?

- A. Configure the FortiWebs in Active-Active HA mode and use AWS Elastic Load Balancer (ELB) for the internal Web servers.
- B. Use AWS Elastic Load Balancer (ELB) for both the FortiWebs in standalone mode and the internal Web servers in an ELB sandwich.

- C. Configure the FortiWebs in Active-Active HA mode and use AWS Route 53 to load balance the internal Web servers.
- D. Use AWS Route 53 to load balance the FortiWebs in standalone mode and use AWS Virtual Private Cloud (VPC) Peering to load balance the internal Web servers.

Answer: B

Question #51 Section 1

Refer to the exhibit.
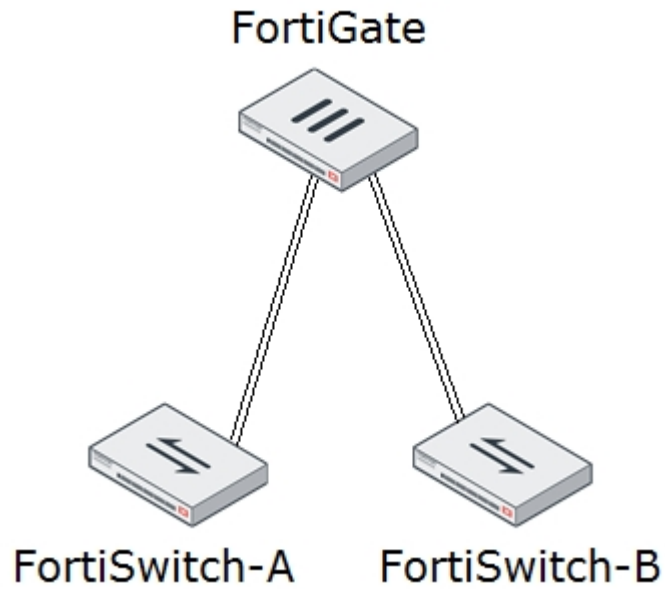
An administrator wants to implement a multi-chassis link aggregation (MCLAG) solution using two FortiSwitch 448D devices and one FortiGate 3700D. As described in the network topology shown in the exhibit, two links are already connected from the FortiGate to each FortiSwitch.
What is required to implement this solution? (Choose two.)

- A. Replace the FortiGate as this one does not have an ISF.
- B. Create two separate link aggregated (LAG) interfaces on the FortiGate side for each FortiSwitch.
- C. Add set fortilink-split-interface disable on the FortiLink interface.
- D. An ICL link between both FortiSwitch devices needs to be added.

Answer: CD

Question #52 Section 1

Refer to the exhibit.
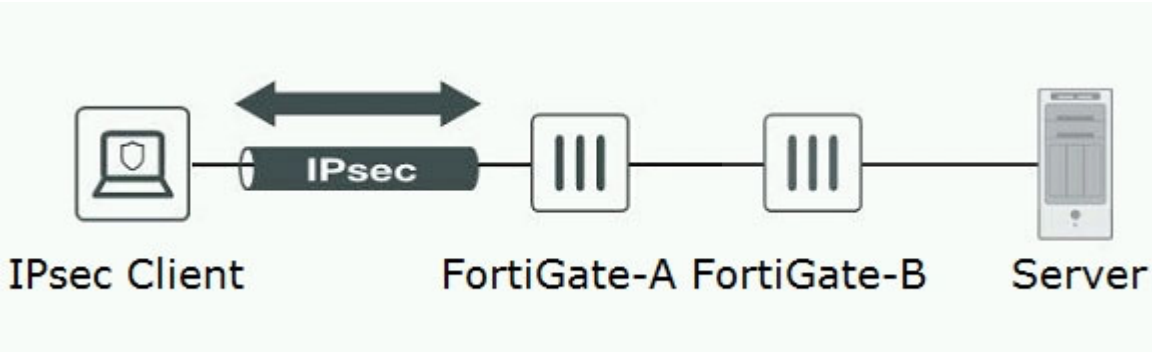
Only users authenticated in FortiGate-B can reach the server. A customer wants to deploy a single sign-on solution for IPsec VPN users. Once a user is connected and authenticated to the VPN in FortiGate-A, the user does not need to authenticate again in FortiGate-B to reach the server.
Referring to the exhibit, which two actions satisfy this requirement? (Choose two.)

- A. Use Kerberos authentication.
- B. Use the Collector Agent.
- C. Use FortiAuthenticator.
- D. FortiGate-A must generate a RADIUS accounting packet.

Answer: CD

Question #53 Section 1

A FortiGate is used as a VPN hub for a number of remote spoke VPN units (Group A) spokes using a phase 1 main mode dial-up tunnel and pre-shared keys. You are asked to establish VPN connectivity for a newly acquired organization's sites for which new devices will be provisioned Group B spokes.
Both existing Group A and new Group B spoke units are dynamically addressed through a single public IP Address on the hub. You are asked to ensure that spokes from Group B have different access permissions than the existing VPN spokes units Group A.
Which two solutions meet the requirements for the new spoke group? (Choose two.)

- A. Implement a new phase 1 dial-up main mode tunnel with a different pre-shared key than the Group A spokes.
- B. Implement a new phase 1 dial-up main mode tunnel with certificate authentication.
- C. Implement a new phase 1 dial-up main mode tunnel with pre-shared keys and XAuth.
- D. Implement separate phase 1 dial-up aggressive mode tunnels with a distinct peer ID.

Answer: CD

Question #54 Section 1

You configured a firewall policy with only a Web filter profile for accessing the Internet. Access to websites belonging to the "Information Technology" category are blocked and to the "Business" category are allowed. SSL deep inspection is not enabled on this policy.
A user wants to access the website https://www.it-acme.com which presents a certificate with CN=www.acme.com. The it-acme.com domain is categorized as
"Information Technology" and the acme.com domain is categorized as "Business".
Which statement regarding this scenario is correct?

- A. The FortiGate is able to read the URL within HTTPS sessions when using SSL certificate inspection so the website will be blocked by the "Information Technology".
- B. The website will be blocked by category "Information Technology" as the SNI takes precedence over the certificate name.
- C. The website will be allowed by category "Business" as the certificate name takes precedence over the URL.
- D. Only with SSL deep inspection enabled will the FortiGate be able to categorized this website.

Answer: B

Question #55 Section 1

Refer to the exhibit.

```
config system interface
    edit "port1"
        set ip 10.10.10.3 255.255.255.0
    next
end

config firewall ippool
    edit "secondary_ip"
        set startip 172.16.1.254
        set endip 172.16.1.254
    next
end

config firewall central-snat-map
    edit 1
        set orig-addr "internal"
        set srcintf "port2"
        set dst-addr "all"
        set dstintf "port1"
        set nat-ippool "secondary_ip"
        set protocol 6
    next
end
```

Central NAT was configured on a FortiGate firewall. A sniffer shows ICMP packets out to a host on the Internet egresses with the port1 IP address instead of the virtual IP (VIP) that was configured
Referring to the exhibit, which configuration change will ensure that ICMP traffic is also translated?

A.
```
config firewall central-snat-map
    edit 1
        set protocol 1
    next
end
```

B.
```
config firewall central-snat-map
    edit 1
        unset protocol
    next
end
```

C.
```
config firewall ippool
    edit "secondary_ip"
        set arp-intf 'port1'
    next
end
```

D.

```
config firewall central-snat-map
    edit 1
        set orig-addr "all"
    next
end
```

Answer: B

Question #56 Section 1

A company has just rolled out new remote sites and now you need to deploy a single firewall policy to all of these sites to allow Internet access using FortiManager. For this particular firewall policy, the source address object is called LAN, but its value will change according to the site the policy is being installed. Which statement about creating the object LAN is correct?

- A. Create a new object called LAN and enable per-device mapping.
- B. Create a new object called LAN and promote it to the global database.
- C. Create a new object called LAN and use it as a variable on a TCL script.
- D. Create a new object called LAN and set meta-fields per remote site.

Answer: A

Question #57 Section 1

Refer to the exhibit.
```
config antivirus settings
    set default-db extended
    set grayware disable
end
config antivirus heuristic
    set mode pass
end
config antivirus profile
    edit "default"
        config http
            set options scan
        end
        set av-virus-log enable
        set av-block-log enable
        set extended-log disable
        set scan-mode quick
    next
end
```

You are working on FortiGate 61E operating in flow-based inspection mode with various settings optimized for performance. The main Internet firewall policy is using the "default" antivirus profile. You found that some executable virus samples files downloaded over HTTP are not being blocked by the FortiGate.
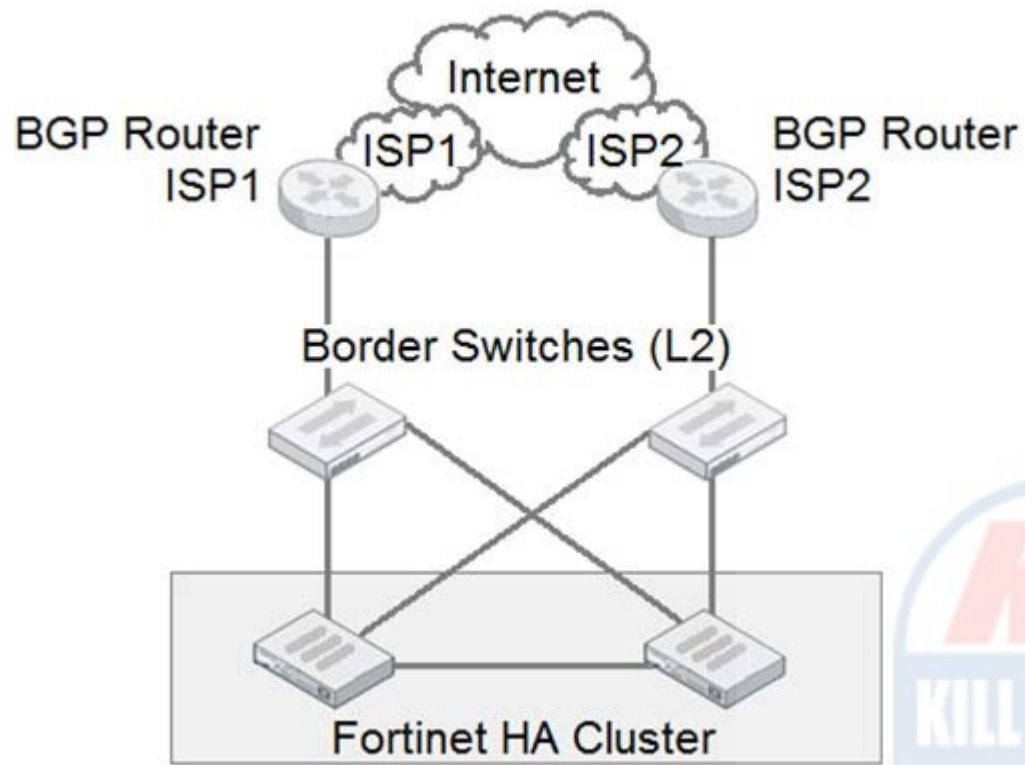Referring to the exhibit, how can this be fixed?

- A. Change the set scan-mode configuration to full.
- B. Disable the emulator feature.
- C. Change the set default-db configuration to extreme.
- D. Add set content-disarm enable to the configuration.

Answer: A

Question #58 Section 1

Refer to the exhibit.

An organization has a FortiGate cluster that is connected to two independent ISPs. You must configure the FortiGate failover for a single ISP failure to occur without disruption.
Referring to the exhibit, which two FortiGate BGP features are enabled to accomplish this task? (Choose two.)

- A. EBGP multipath
- B. Graceful restart
- C. Synchronization
- D. BFD

Answer: BD

Question #59 Section 1

A legacy router has been replaced by a FortiGate device. The FortiGate has inherited the management IP address of the router and now the network administrator needs to remove the router from the FortiSIEM configuration.
Which two statements about this operation are true? (Choose two.)

- A. FortiSIEM will move the router device into the Decommission folder.
- B. The router will be completely deleted from the FortiSIEM database.
- C. By default, FortiSIEM can only parser event logs for FortiGate devices.
- D. FortiSIEM will discover a new device for the FortiGate with the same IP.

Answer: AD

Question #60 Section 1

You have configured an HA cluster with two FortiGate devices. You want to make sure that you are able to manage the individual cluster members directly using port3.

```
config system ha
    set mode a-a
    set group-id 1
    set group-name main
    set hb_dev port2 100
    set session-pickup enable
end
```
Referring to the configuration shown, in which two ways can you accomplish this task? (Choose two.)

- A. Create a management VDOM and disable the HA synchronization for this VDOM, assign port3 to this VDOM, then configure specific IPs for port3 on both cluster members.
- B. Configure port3 to be a dedicated HA management interface; then configure specific IPs for port3 on both cluster members.
- C. Allow administrative access in the HA heartbeat interfaces.
- D. Disable the sync feature on port3; then configure specific IPs for port3 on both cluster members.

Answer: AB