Vendor: Fortinet

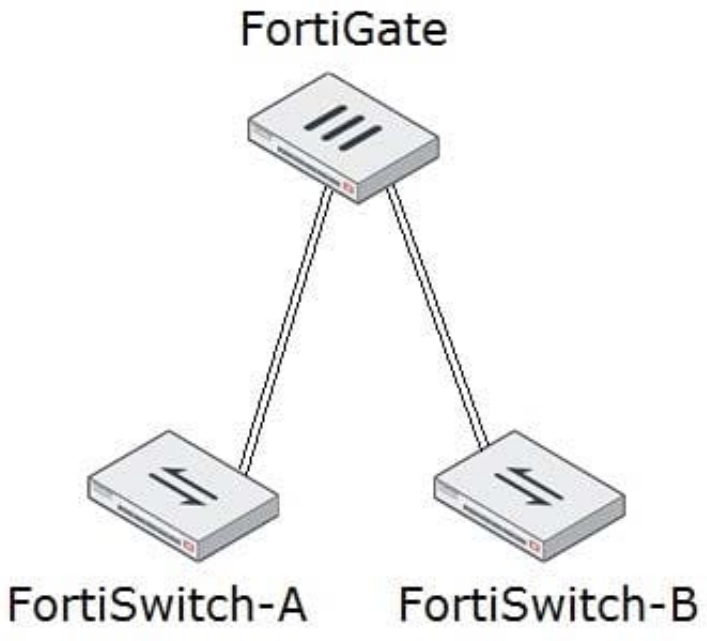
Exam Code:NSE8_811

Exam Name: Fortinet NSE 8 Written Exam (NSE8_811)

Version: Demo

QUESTION 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.

Correct Answer: CD

QUESTION 2

Refer to the exhibit.

```
FWB (HC-Combo) # show
config server-policy health
    edit "HC-Combo"
        config health-list
            edit 1
                set type tcp-half-open
            next
            edit 2
                set type http
                set url-path /index.html
                set match-type response-code
            next
            edit 3
                set type icmp
            next
        end
    next
end
```

You created a custom health-check for your FortiWeb deployment. Given the output shown in the exhibit, which statement is true?

A. The FortiWeb must receive an RST packet from the server.

B. The FortiWeb must receive an HTTP 200 response code from the server.

C. The FortiWeb must match the hash value of the page index.html.

D. The FortiWeb must receive an ICMP Echo Request from the server.

Correct Answer: B

QUESTION 3

A customer is experiencing problems with a legacy L3/L4 firewall device and the IPv6 SIP VoIP traffic. Their device is dropping SIP packets, consequently, it cannot process SIP voice calls.

Which solution will solve the customer\\'s problem?

A. Replace their legacy device with a FortiGate and deploy a FortiVoice to extract information from the body of the IPv6 SIP packet.

B. Deploy a FortiVoice and enable IPv6 SIP.

C. Deploy a FortiVoice and enable an IPv6 SIP session helper.

D. Replace their legacy device with a FortiGate and configure it to extract information from the body of the IPv6 SIP packet.

Correct Answer: A

QUESTION 4

A customer wants to enable SYN flood mitigation in a FortiDDoS device. The FortiDDoS must reply with one SYN/ACK packet per SYN packet from a new source IP address. Which SYN flood mitigation mode must the customer use?

A. SYN retransmission

B. SYN/ACK cookie

C. SYN cookie

D. ACK cookie

Correct Answer: C

QUESTION 5

You want to manage a FortiGate with the FortiCloud service. The FortiGate shows up in your list of devices on the FortiCloud Web site, but all management functions are either missing or grayed out.

Which statement is correct in this scenario?

A. The management tunnel mode on the managed FortiGate must be changed to normal.

B. The managed FortiGate is running a version of FortiOS that is either too new or too old for FortiCloud.

C. The managed FortiGate requires that a FortiCloud management license be purchased and applied.

D. You must manually configure system central-management on the FortiGate CLI and set the management type to fortiguard.

Correct Answer: D

QUESTION 6

Refer to the exhibit.

The exhibit shows the configuration of a service protection profile (SPP) in a FortiDDoS device. Which two statements are true about the traffic matching being inspected by this SPP? (Choose two.)

A. Traffic that does not match any SPP policy will be inspected by this SPP.

B. FortiDDoS will not send a SYN/ACK if a SYN packet is coming from an IP address that is not in the legitimate IP (LIP) address table.

C. FortiDDoS will start dropping packets as soon as the traffic exceeds the configured minimum threshold.

D. SYN packets with payloads will be dropped.

Correct Answer: AD

QUESTION 7

Refer to the exhibit.

```
config waf url-rewrite url-rewrite-rule
    edit "NSE8-rule"
        set action redirect
        set location "https://$0/$1"
        set host-status disable
        set host-use-pserver disable
        set referer-status disable
        set referer-use-pserver disable
        set url-status disable
config match-condition
    edit 1
        set reg-exp "(.*)"
        set protocol-filter enable
    next
    edit 2
        set object http-url
        set reg-exp "^/(.*)$"
    next
end
    next
end
config waf url-rewrite url-rewrite-policy
    edit "nse8-rewrite"
config rule
    edit 1
        set url-rewrite-rule-name "NSE8-rule"
    next
    end
    next
end
```

The exhibit shows the steps for creating a URL rewrite policy on a FortiWeb. Which statement represents the purpose of this policy?

A. The policy redirects all HTTPS URLs to HTTP.

B. The policy redirects all HTTP URLs to HTTPS.

C. The policy redirects only HTTP URLs containing the ^/(.*)$ string to HTTPS.

D. The policy redirects only HTTPS URLs containing the ^/(.*)$ string to HTTP.

Correct Answer: B

QUESTION 8

You are building a FortiGate cluster which is stretched over two locations. The HA connections for the cluster are terminated on the local switches in the data centers. Once the FortiGate devices have booted, they do not form a cluster. The network operators inform you that CRC errors are present on the switches where the FortiGate devices are connected.

What should you do to solve this problem?

A. Set the speed/duplex setting to 1 Gbps / Full Duplex.

B. Replace the cables where the CRC errors occur.

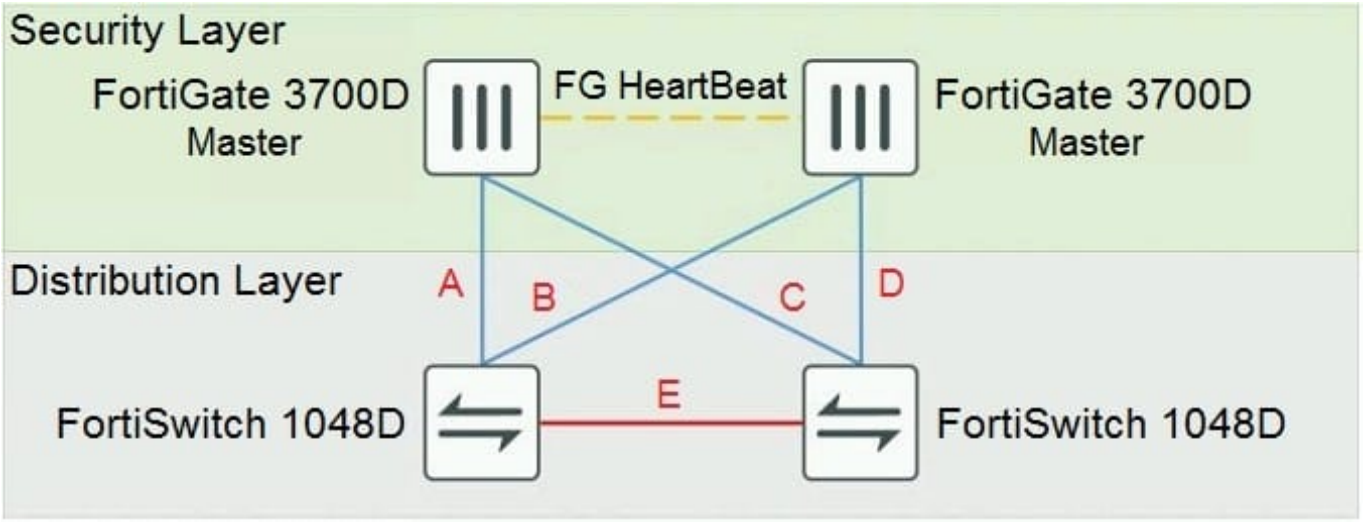
C. Place the HA interfaces in dedicated VLANs.

D. Change the ethertype for the HA packets.

Correct Answer: D

QUESTION 9

Refer to the exhibit.



The exhibit shows a full-mesh topology between FortiGate and FortiSwitch devices. To deploy this configuration, two requirements must be met:

20 Gbps full duplex connectivity is available between each FortiGate and the FortiSwitch devices The FortiGate HA must be in AP mode

Referring to the exhibit, what are two actions that will fulfill the requirements? (Choose two.)

A. Configure the master FortiGate with one LAG and FortiLink split interface disabled on ports connected to cables A and C and make sure the same ports are used for cables B and D on the slave.

B. Configure the master FortiGate with one LAG and FortiLink split interface enabled on ports connected to cables A and C and make sure the same ports are used for cables B and D on the slave.

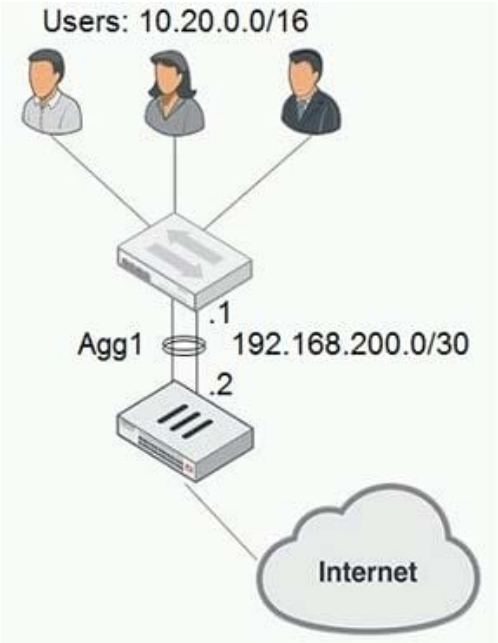
C. Configure both FortiSwitch devices as peers with ICL over cable E, create one MCLAG on ports connected to cables A and C, and create another MCLAG on ports connected to cables B and D.

D. Configure both FortiSwitch devices as peers with ISL over cable E, create one MCLAG on ports connected to cables A and C, and create another MCLAG on ports connected to cables B and D.

Correct Answer: AC

QUESTION 10

Refer to the exhibit.




```
config system interface
    edit "Agg1"
        set ip 192.168.200.2 255.255.255.252
        set type aggregate
        set member port1 port2
        set vdom "root"
        set weight 1
        set lacp-mode passive
        set min-links 1
        set algorithm L2
    next
end
```

You created an aggregate interface between a FortiGate and a switch consisting of two 1 Gbps links as shown in the exhibit. However, the maximum bandwidth never exceeds 1 Gbps and employees are reporting that the network is slow. After troubleshooting, you notice that only one member interface is being used. The configuration for the aggregate interface is shown in the exhibit.

In this scenario, which command will solve this problem?

A.
```
config system interface
edit Agg1
   set algorithm L4
end
```

B.
```
config system interface
edit Agg1
   set weight 2
end
```

C.
```
config system interface
edit Agg1
   set lacp-mode active
end
```

D.
```
config system interface
edit Agg1
   set min-links 2
end
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 11

You cannot ping the FortiGate default gateway 10.10.10.1 from the FortiGate CLI. The FortiGate interface facing the default gateway is wan1 and its IP address is 10.10.10.254/24. During the initial troubleshooting tests, you confirm that you can ping other IP addresses in the 10.10.10.0/24 subnet from the FortiGate CLI without packets lost.

Which two CLI commands will help you to troubleshoot this problem? (Choose two.)

A. diagnose debug flow filter saddr 10.10.10.1 diagnose debug flow trace start 10

B. diagnose hardware deviceinfo nic wan1

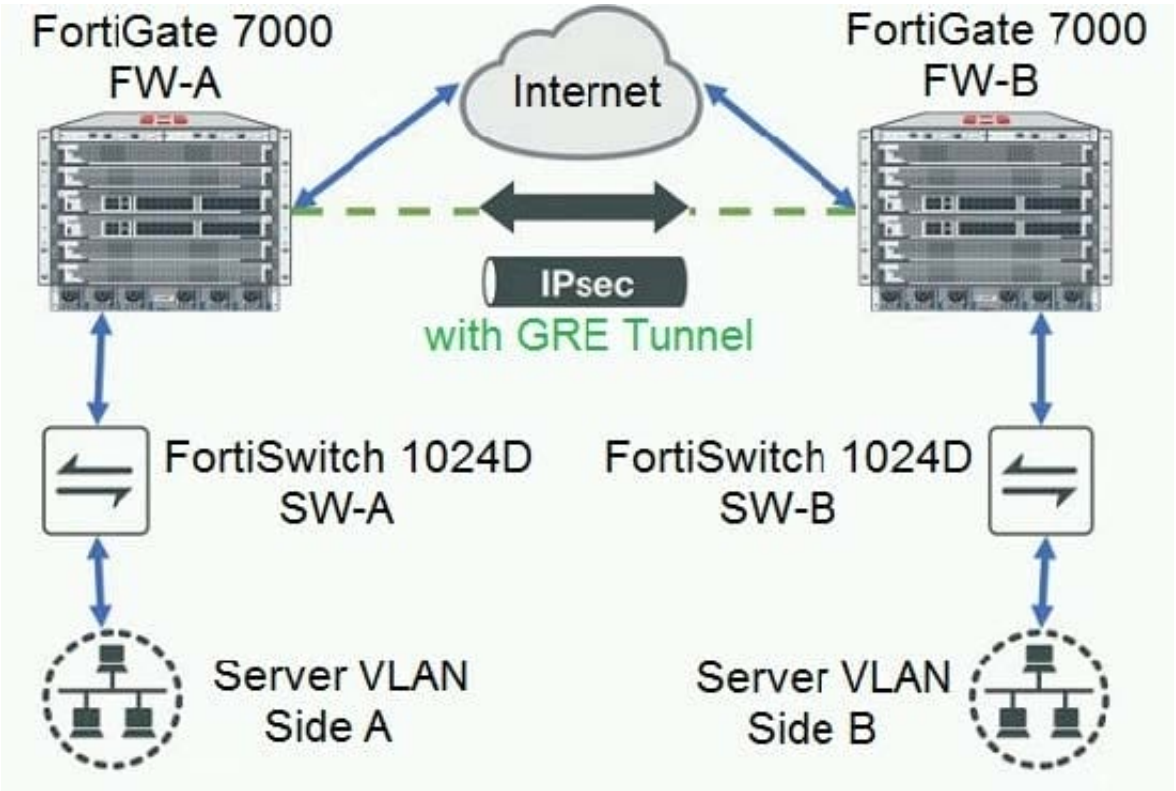
C. diagnose ip arp list

D. diag sniffer packet wan1 \\'arp and host 10.10.10.1\\'

Correct Answer: AC

QUESTION 12

Refer to the exhibit.



You have two data centers with a FortiGate 7000-series chassis connected by VPN. All traffic flows over an established generic routing encapsulation (GRE) tunnel between them. You are troubleshooting traffic that is traversing between Server VLAN A and Server VLAN B. The performance is lower than expected and you notice all traffic is only going through the FPM in slot 3 while nothing through the FPM in slot 4.

Referring to the exhibit, which statement is true?

A. Removing traffic shaping from the firewall policy allowing this traffic will allow for load-balancing to the other module.

B. Changing the algorithm to take source IP, destination IP and port into account will load balance this traffic to the other module.

C. There is no way to load-balance the traffic in this scenario.

D. Configuring a load-balance flow-rule in the CLI will load-balance this traffic.

Correct Answer: D