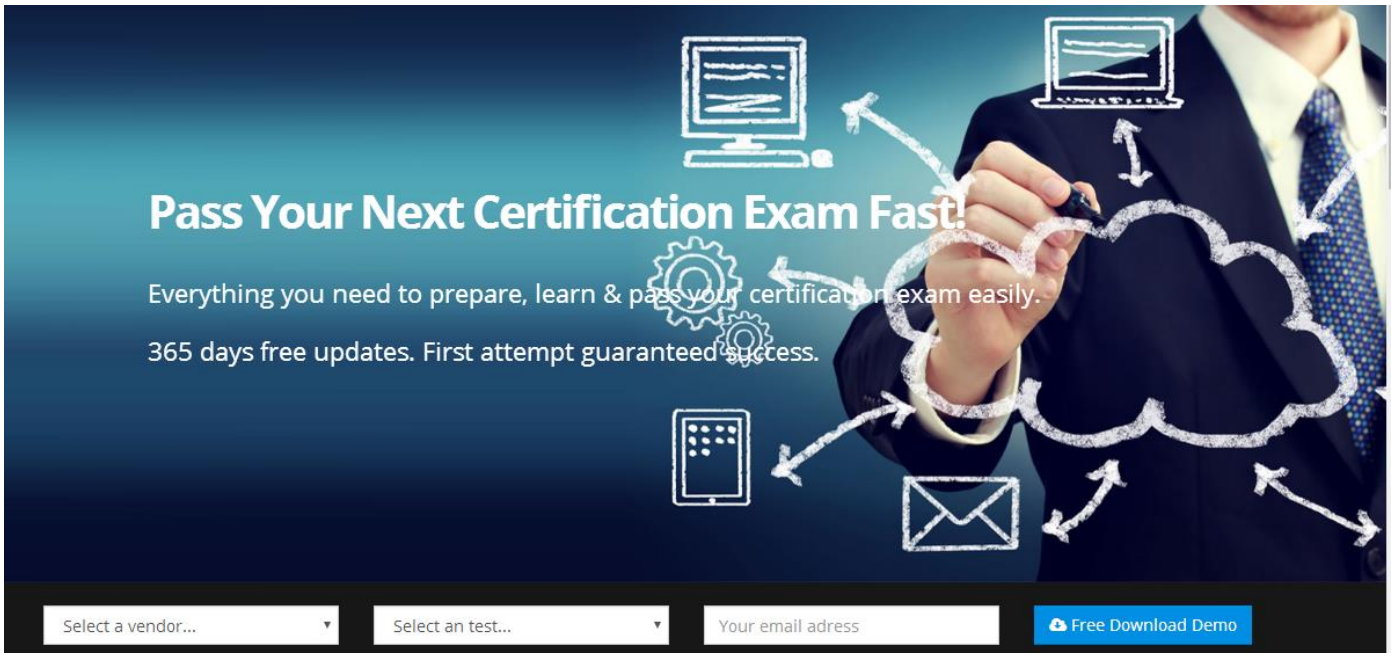
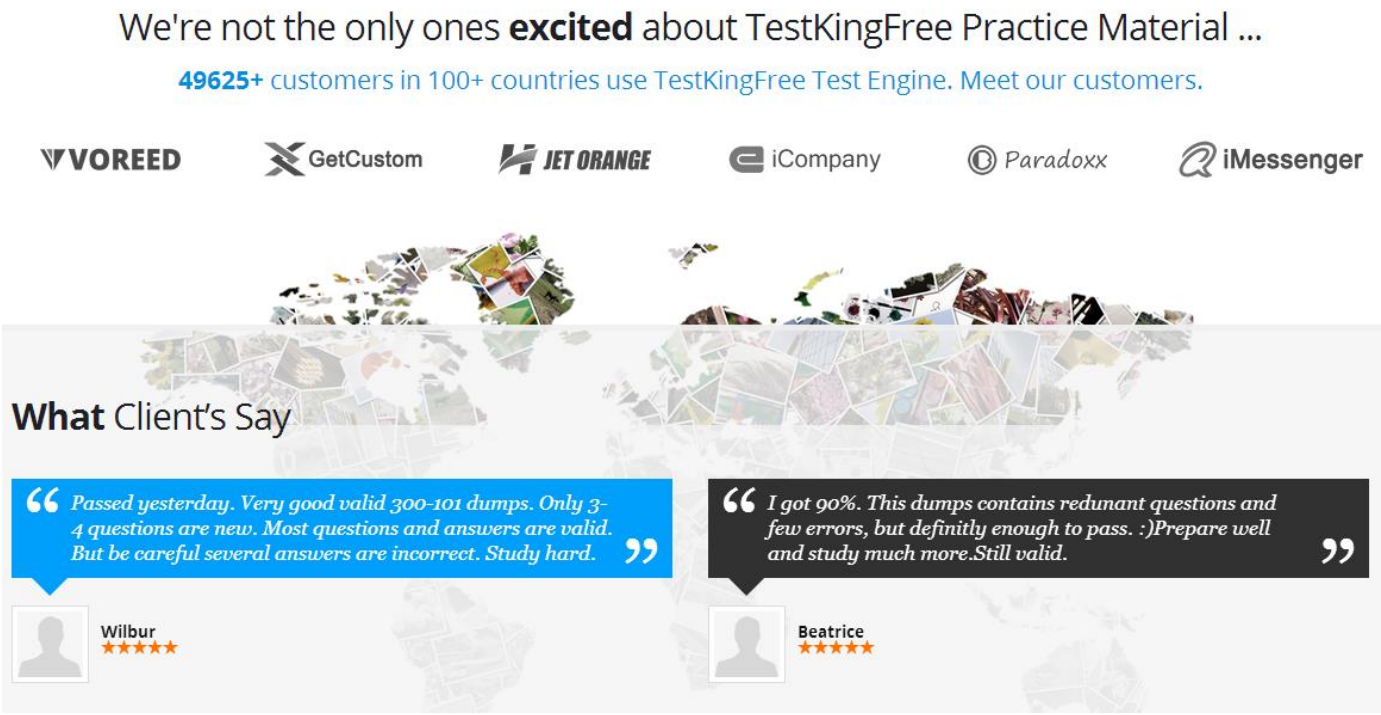
TestKingfree





http://www.testkingfree.com/

Pass For sure Certification Exam Guide and Exam Dumps - TestKingFree

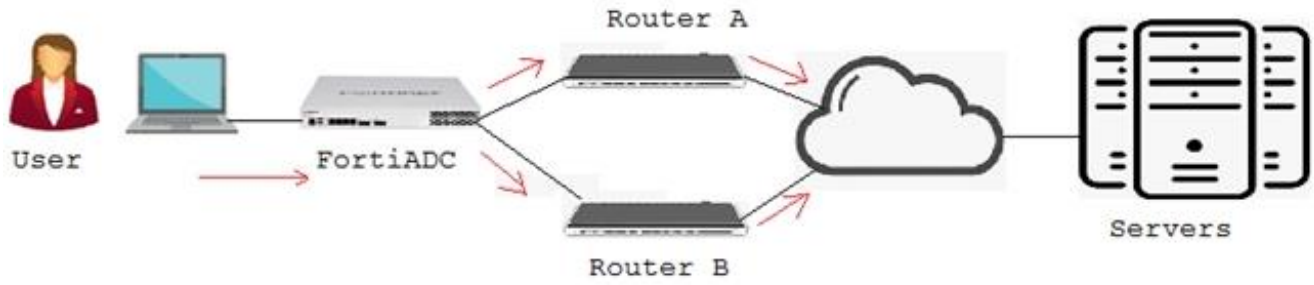
Exam : **NSE8_810**

Title : Fortinet Network Security Expert 8 Written Exam (NSE8 810)

Vendor : Fortinet

Version : DEMO

NO.1 Click the Exhibit button.



Referring to the exhibit, a FortiADC is load balancing IPv4 traffic between two next-hop routers. The FortiADC does not know the IP addresses of the servers. Also, the FortiADC is doing Layer 7 content inspection and modification.
In this scenario, which application delivery control is configured in the FortiADC?

A. Layer 2
B. Layer 3
C. Laye.4
D. Layer 7
Answer: A

NO.2

Exhibit

```
INVITE sip:PhoneB@172.20.120.30 SIP/2.0
Via: SIP/2.0/UDP 10.31.101.20:5060
From:PhoneA <sip:PhoneA@10.31.101.20>
To:PhoneB <sip:PhoneB@172.20.120.30>
Call-ID: 314159@10.31.101.20
CSeq: 1 INVITE
Contact: sip:PhoneA@10.31.101.20
v=0
o=PhoneA 5462346 332134 IN IP4 10.31.101.20
c=IN IP4 10.31.101.20
m=audio 49170 RTP 0 3
```

Click the Exhibit button.
A FortiGate with the default configuration is deployed between two IP phones. FortiGate receives the INVITE request shown in the exhibit form Phone A (internal)to Phone B (external). Which two actions are taken by the FortiGate after the packet is received? (Choose two.)

A. a pinhole will be opened to accept traffic sent to FortiGate's WAN IP address and ports 49l70 and 49171.

B. The phone A IP address will be translated for the WAN IP address in all INVITE header fields and the SDP statement remains intact.

C. The phone A IP address will be translated lo the WAN IP address in all INVITE header fields and the m: field of the SDP statement.

D. A pinhole will be opened to accept traffic sent to FortiGate's WAN IP address and ports 49169 and 49170.

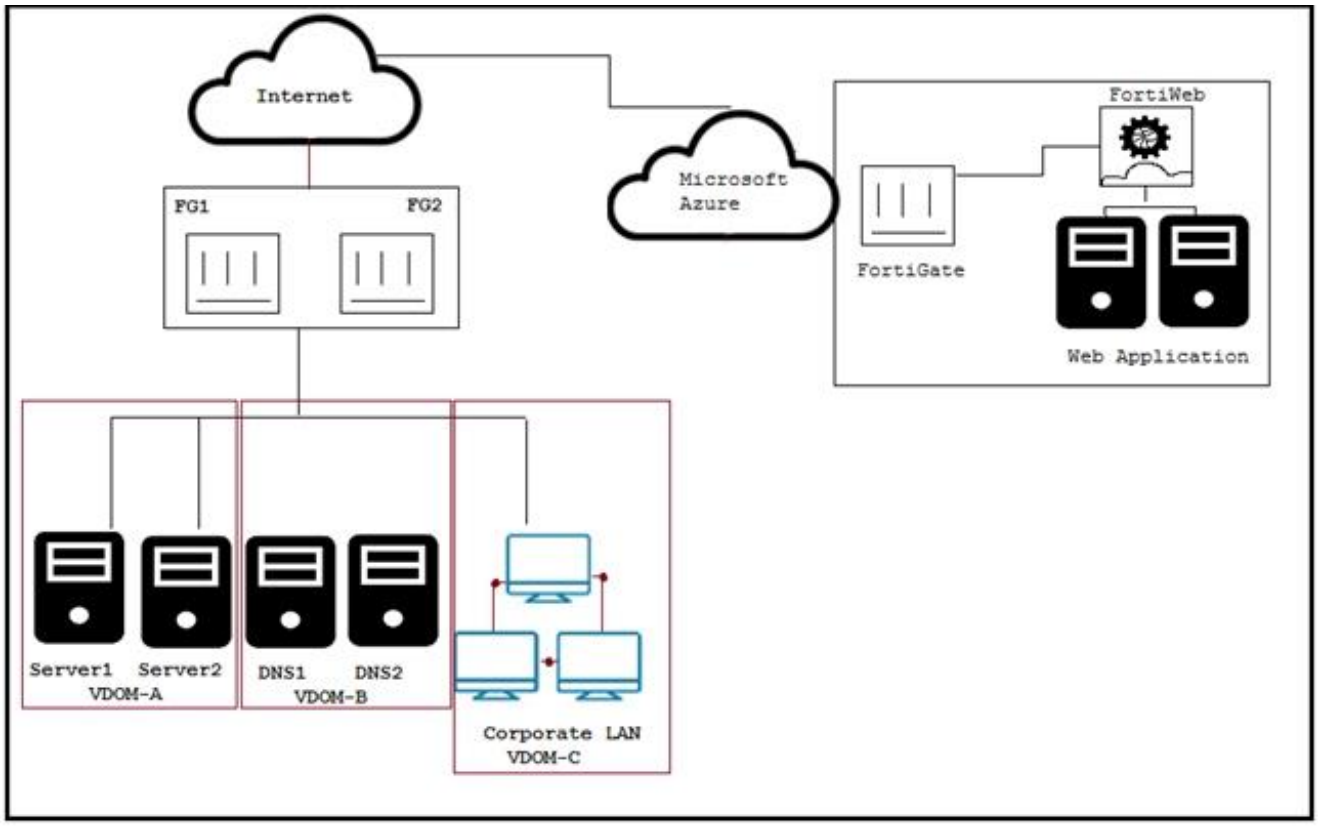
Answer: A,C

Explanation

"Also, the FortiGate must translate the addresses contained in the SIP headers and SDP body of the SIP messages.

The RTP port number as defined in the SIP message and an RTCP port number, which is the RTP port number plus 1"

NO.3 Click the Exhibit button.



A customer has just finished their Azure deployment to secure a Web application behind a FortiGate and a FortiWeb. Now they want to add components to protect against advanced threats (zero day attacks), centrally manage the entire environment, and centrally monitor Fortinet and non-Fortinet products.

Which Fortinet solutions will satisfy these requirements?

A. Use FotiAnalyzer lor monitor in Azure, FortiSIEM for managemnet, and FortiSandbox for zero day attacks on their local network.

B. Use FortiManager for management in Azure, FortSIEM for monitoring and FcrtiSandbox for zero day attacks on their local network.

C. Use Fortianalyzer for monitor Azure, FortiSiEM for management, and FortiGate has zero day attacks on their local network.

D. Use FortiSIEM for management Azure, FortiManager for management, and FortrGate for zero day attacks on their local network.

Answer: B

NO.4 Click the Exhibit button.

Referring to the exhibit, which command-line option for deep inspection SSL would have the FortiGate re-sign all untrusted self-signed certificates with the trusted Fortinet_CA_SSL certificate?

Exhibit

```
config firewall ssl-ssh-profile
   edit "custom-deep-inspection"
      config https
         set untrusted-cert {option}
   end
  next
end
```

A. inspect

B. ignore

C. allow

D. block

Answer: B

NO.5 Click the Exhibit button.

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 will ensure that ICMP traffic is also translated?

```
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
```

A. config firewall central-snat-map edit 1 set orig-addr "all" next end
B. config firewall central-snat-map edit 1 unset protocol next end
C. config firewall ippool edit "secondry_ip" set arp-intf 'port1' next end
D. config firewall central-snat-map edit 1 set protocol 1 next end
Answer: B

NO.6 Click the Exhibit button. Referring to the exhibit, which two statements are true? (Choose two.)

```
FGR # show firewall policy6
config firewall policy6
edit 1
set name "internet-ipv6"
set srcintf "port2"
set dstintf "port1"
set srcaddr "fd00:acd5:87a4:890d::10/128"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set utm-status enable
set users "nse8user"
set profile-type group
set-profile-group "nse8-pfg"
set nat enable
 next
end

FGR # show firewall policy
config firewall policy
edit 1
set name "Internet"
set srcintf "port2"
set dstintf "port1"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set utm-status enable
set logtraffic all
set fsso disable
set users "nse8user"
  set webfilter-profile "nse8-wf"
set dnsfilter-profile "nse8-wf-dns"
set profile-protocol-options "nse8-po"
set ssl-ssh-profile "certificate-inspection"
set nat enable
  next
end

FGR # show firewall profile group nse8-pfg
config firewall profile-group
edit "nse8-pfg"
set webfilter-profile "nse8-wf"
set dnsfilter-profile "nse8-wf-dns"
set profile-protocol-options "nse8-po"
set ssl-ssh-profile "certificate-inspection"
 next
end
```

A. The IPv6 traffic for nse8user is filtered using the DNS profile.
B. The Web traffic for nse8user is being filtered differently in IPv4 and IPv6.
C. The IPv4 policy is allowing security profile groups.
D. The IPv4 traffic for nse8user is filtered using the DNS profile.
Answer: B,D