Exam : 925-201b

Title : Principles of Network Security and FortiGate Configurations

Ver : 08.12.08

QUESTION 1:

Which of the following default factory setting is true about Fortigate unit? Select all that apply.

A. internal : 192.168.1.99 /24 ; http , https , ping , ssh access is enabled
B. external : 192.168.100.99/24 ; ping is enabled
C. internal : 192.168.1.99 /24 ; https , ping , ssh access is enabled
D. external : 192.168.100.99/24 ; ping & https is enabled

Answer: A , B

QUESTION 2:

Which of the following firmware upgrade method will cause configuration reset?

A. WebUI
B. CLI
C. Fortimanager
D. interrupt booting procedure by CLI

Answer: D

QUESTION 3:

Which of the following statement about TCP MTU for Fortigate is true? Select all that apply.

A. default MTU is 1500 bytes
B. For manual and DHCP addressing mode the MTU size can be from 576 to 1500 bytes
C. for PPPOE addressing mode the MTU size can be from 576 to 1492 bytes
D. default MTU is 1492 bytes

Answer: A , B, C

QUESTION 4:

What is the valid method to fixup Fortigate interface speed&duplex?

A. via web GUI
B. via CLI
C. via auto update
D. via foritlog

Answer: B

Explanation :
via CLI ,
configsystem interface
edit internal
set speed ?
100full 100M full-duplex
100half 100M half-duplex
10full 10M full-duplex
10half 10M half-duplex
auto auto adjust speed

QUESTION 5:

What are the necessary procedure before using Xauth? Select all that apply.

A. create user group
B. create firewall policy
C. enable IPSEC VPN
D. enable PPTP

Answer: A , B, C

QUESTION 6:

Which one is the most efficient way to block MSN traffic by Fortigate unit ?

A. Use IPS module by applying protection profile
B. Use Antivirus engine
C. Use firewall policy
D. Use content filtering

Answer: A

QUESTION 7:

What is the valid web script filtering option for web filtering? Select all that apply.

A. Java Applet
B. Worm
C. ActiveX
D. Cookie

Answer: A, C, D

QUESTION 8:

What is the best way to implement Fortigate HA ?

A. connect corresponding interface to individual switch
B. connect all interface to the same hub or switch
C. connect corresponding interface directly using cross-over cable
D. connect corresponding interface directly using straight-through cable

Answer: A

QUESTION 9:

What is the valid address object in Fortigate unit ?

A. 10.1.1.1 / 255.255.255.0
B. 10.1.1.1 / 255.255.255.255
C. 10.1.1.1 / 255.255.255.248
D. 10.1.1.1 / 255.255.255.252

Answer: B

QUESTION 10:

What is the valid network in Fortigate? Select all that apply.

A. 10.1.1.0 / 255.255.255.0
B. 10.1.1.1 / 255.255.255.0
C. 10.1.1.0 / 255.255.255.255
D. 10.1.1.0 / 255.255.0.0

Answer: B, D

QUESTION 11:

What is the valid ipsec phase 1 option

A. des
B. 3des
C. md5
D. sha1

Answer: A , B

QUESTION 12:

What is the valid ipsec phase 2 option? Select all that apply.

A. des
B. 3des
C. md5
D. sha1

Answer: C, D

QUESTION 13:

What is valid router object of Fortigate unit? Select all that apply.

A. prefix list
B. route map
C. key chain list
D. access list

Answer: A , B, C

QUESTION 14:

What service can protection profile protect? Select all that apply.

A. ftp
B. IMAP
C. POP3
D. http
E. SMTP

Answer: A , B, C , D , E

QUESTION 15:

What is the default protection profile? Select all that apply.

A. strict
B. scan
C. web
D. unfiltered

Answer: A , B, C , D

QUESTION 16:

What are the valid option in web filtering? Select all that apply.

A. content block
B. url block
C. exempt list
D. script filtering

Answer: A , B, C , D

QUESTION 17:

What is the valid IPS option? Select all that apply.

A. IPS signature
B. IPS anomaly
C. IPS engine
D. IPS list

Answer: A , B
Valid IPS options are IPS Signature and IPS anomaly.
Not D: IPS list do not exist

QUESTION 18:

Which logging can enable when enable protection profile content log? Select all that apply.

A. HTTP
B. FTP
C. IMAP
D. POP3
E. SMTP

Answer: A , B, C , D

QUESTION 19:

What is the valid option of Fortigate HA schedule? Select all that apply.

A. none , hub , least-connection , round-robin
B. weighted round-robin , random , ip , ip port
C. switch , ip , ip port
D. priority , hub , least-connection

Answer: A , B

QUESTION 20:

Which command can show HA status? Select all that apply.

A. get system status
B. diag sys ha status
C. exec ha maga 1
D. get sys lic
E. config ha

Answer: A , B ,C

QUESTION 21:

Exhibit:
1. Monitor port priority.
2. Age.
3. Unit Priority.
4. Serial number
What is the correct match order to choose a cluster master?

A. 1 , 2 , 3 , 4
B. 1 , 3 , 2 , 4
C. 2 , 1 , 3 , 4
D. 2 , 4 , 1 , 3
E. 4 , 1 , 3 , 2

Answer: A

QUESTION 22:

IPSEC VPN support which of the following DH group? Select all that apply.

A. 1
B. 2
C. 3
D. 4
E. 5

Answer: A , B, E

QUESTION 23:

what is the mechanism for processing DH group

A. to generate session key

B. to generate pre-share key
C. to generate public key
D. to generate private key

Answer: A

QUESTION 24:

Fortigatesupport which of the following client mode? Select all that apply.

A. ipsec
B. latp
C. pptp
D. l2f

Answer: A , B, C

QUESTION 25:

Fortigateuse port 9443 to do what function

A. to communicate with proxy server
B. to run push update
C. to communicate with syslog server
D. to communicate with Fortilog server

Answer: B

Explanation :
Update center
You can configure the FortiGate unit to connect to the FortiProtect Distribution Network (FDN) to update the antivirus (including grayware), Spam Filter and attack
definitions and engines.
Before the FortiGate unit can receive antivirus and attack updates, it must be able to connect to the FortiProtect Distribution Network (FDN). The FortiGate unit uses HTTPS on port 443 to connect to the FDN. The FortiGate unit must be able to route packets to the Internet using port 443.
You can also configure the FortiGate unit to allow push updates. Push updates are provided to the FortiGate unit from the FDN using HTTPS on UDP port 9443. To receive push updates, the FDN must be able to route packets to the FortiGate unit using UDP port 9443.
The FDN is a world-wide network of FortiProtect Distribution Servers (FDSs). When the FortiGate unit connects to the FDN it connects to the nearest FDS. To do this, all FortiGate units are programmed with a list of FDS addresses sorted by nearest time zone according to the time zone configured for the FortiGate unit.

The FortiGate unit supports the following antivirus and attack definition update features:
User-initiated update from the FDN,
Hourly,daily,or weekly scheduled antivirus and attack definition and antivirus
engine updates from the FDN,
Push update from the FDN,
Update status including version members, expiry date ,and update dates and times,
Push updates through a NAT device.
To receive scheduled updates and push updates, you must register the FortiGate unit
on the Fortinet support web page.

QUESTION 26:

What's the difference between RIP V1 & V2? Select all that apply.

A. carry more information
B. support simple authentication
C. support subnet mask
D. support encryption

Answer: A , B, C

QUESTION 27:

Which one of the following command could show HA information of fortigate?
Select all that apply.

A. get system status
B. diag sys ha status
C. exec ha mamane 1
D. diag deb ena

Answer: A , B, C

QUESTION 28:

What is the max hop of RIP ?

A. 13
B. 14
C. 15
D. 16

Answer: C

QUESTION 29:

What is the max metric can be configured in route distribution?

A. 13
B. 14
C. 15
D. 16

Answer: D

QUESTION 30:

What are the valid dhcp server option?

A. none
B. dhcp server
C. dhcp relay agent
D. dhcp forwarding

Answer: A , B, C

QUESTION 31:

what port is used between Fortigate to transmit log message to Foritlog

A. tcp 514
B. udp 514
C. tcp 69
D. udp 69

Answer: B

QUESTION 32:

What is the correct protocol number for TCP?

A. TCP / 6 , UDP / 17
B. TCP / 16 , UDP 117
C. TCP / 66 , UDP / 77
D. TCP / 106 , UDP / 107

Answer: A

QUESTION 33:

Which of the following Fortigate components can not be rename? Select all that apply.

A. schedule
B. predefine service
C. address group
D. network range

Answer: A , B, C , D

QUESTION 34:

Which of the following Traffic shaping parameter can be configured? Select all that apply.

A. schedule
B. traffic priority
C. max bandwidth
D. guarantee bandwidth

Answer: B, C , D

QUESTION 35:

What is the correct policy order ,

A. encrypt->accept->deny all
B. encrypy->deny->accept->deny all
C. accept->encrypt->deny
D. deny->encrypt->accept

Answer: A

QUESTION 36:

Best describe the feature of firewall policy :

A. if there is no preceding matching policy the packet is dropped
B. the primary function of firewall
C. policy can not be applied on user group
D. policy can not be applied with protection profile

Answer: A

QUESTION 37:

Where can protection profile be applied on? Select all that apply.

A. policy
B. group
C. service
D. url filter

Answer: A , B

QUESTION 38:

What is the valid log storage for Fortigate unit? Select all that apply.

A. syslog server
B. webtrend
C. local disk
D. memory buffer
E. fortilog

Answer: A , B, C , D, E

QUESTION 39:

What is the valid IPS action when configure IPS signature? Select all that apply.

A. log
B. drop
C. reset client , reset server
D. pass
E. clear session
F. reset

Answer: A , B, C , D , E , f

QUESTION 40:

What is the most efficient way to disable IPS signature? Select all that apply.

A. set action to pass
B. no logging
C. set to drop
D. set to clear

Answer: A , B

QUESTION 41:

Which of the following predefined dissector signature have configurable

parameter? Select all that apply.

A. http header
B. IM
C. P2P
D. rpc decoder
E. cp-reassemble

Answer: A , B, C , D , E

QUESTION 42:

What is the statistical anomaly type for the TCP , UDP , & ICMP protocols that Fortigate IPS identified? Select all that apply.

A. flooding
B. scan
C. source
D. destination session limit

Answer: A , B, C , D

QUESTION 43:

When creating protection profile with configuring antivirus scanning , what service can be protected by enabling virus scan & file blocking? Select all that apply.

A. HTTP
B. FTP
C. IMAP , POP3 , SMTP
D. TELNET

Answer: A , B, C

QUESTION 44:

When creating protection profile with configuring antivirus scanning , we can disabling passing of fragment emails for ?

A. HTTP
B. FTP
C. IMAP , POP3 , SMTP
D. TELNET

Answer: C

QUESTION 45:

When creating protection profile with configuring antivirus scanning ,we can select an action (pass or block) for oversized file and emails for? Select all that apply.

A. HTTP
B. FTP
C. IMAP , POP3 , SMTP
D. TELNET

Answer: A , B, C , D

QUESTION 46:

Which of the following file type can be blocked by Fortigate Antivirus engine file block function? Select all that apply.

A. bat , com , dll , doc , exe
B. gz , hta , ppt , rar , tar , tgz
C. vb? , wps , xl? , zip , pif , cpe
D. pdf , doc , xls

Answer: A , B, C

QUESTION 47:

What is the valid format that can be entered in url blocking list? Select all that apply.

A. a top-level URL to block access to all pages on the website
B. an IP address to block access to all page on the website
C. a partial URL to block sub-domains
D. a top-level domain suffix to block all URLs with the suffix

Answer: A , B, C , D

QUESTION 48:

What port does Foritgate unit use to filtering web url in transparent mode?

A. 8888
B. 8887
C. 8886
D. 8885

Answer: A

QUESTION 49:

Exhibit:
1. Outbound encrypt policy.
2. Inbound encrypt policy.
3) Default non-encrypt policy.
What is the correct order of the recommend policy order of spoke Fortigate unit in hub & spoke environment?

A. 1 , 2 , 3
B. 2 , 1 , 3
C. 2 , 3 , 1
D. 3 , 2 , 1

Answer: A

QUESTION 50:

Which of the following description describe the same function? Select all that apply.

A. deny splitting tunneling
B. dedicate tunnel
C. internet browsing
D. Intranet browsing

Answer: A , B, C

QUESTION 51:

What can we do by using Forticlient software? Select all that apply.

A. create VPN connection to remote networks
B. scan your computer for virus
C. configure real-time protection against virus and unauthorized modification of the Windows registry
D. restrict access to your system and application by setting up firewall policies

Answer: A , B, C , D

QUESTION 52:

What of following is true? Select all that apply.

A. dialup vpn only can be used in NAT mode
B. pptp can be used in NAT/Route mode

C. l2tp can be used in NAT/Route mode
D. l2f can be used in NAT/Route mode

Answer: A , B, C

QUESTION 53:

Which of the following statement is true about NAT/Route mode FortiGate unit?
Select all that apply.

A. The FortiGate unit is used to hide the internal network from other netwok
B. The FortiGate unit acts as a router with firewall capabilities
C. The FortiGate Unit used to apply firewall policies and services to traffic on a network without having to make any change to the network
D. All its interfaces are on different subnets
E. External is the interface to the external network(usually the internet)
F. Internal is the interface to the internal network
G. DMZ/HA is the interface to the DMZ network , DMZ/HA can also be connected to other FortiGate units if you are installing an HA cluster

Answer: A , B, G

QUESTION 54:

Security policies control the flow of traffic based on which of the following part of the packet? Select all that apply.

A. Source address
B. Destination address
C. (c) Service port
D. Payload

Answer: A , B, C , ,D

QUESTION 55:

How many network segments can be connected to FortiGate unit to control traffic between these network segments when using transparent mode

A. 1
B. 2
C. 3
D. 4
E. 5

Answer: C

QUESTION 56:

What is the default mode of FortiGate unit

A. NAT/Route mode
B. Transparent mode
C. NAT mode
D. Route mode
E. Firewall mode

Answer: A

QUESTION 57:

What is the default ip address of FortiGate unit? Select all that apply.

A. internal 192.168.1.99
B. external 192.168.100.99
C. internal 192.168.1.1
D. external 192.168.100.1

Answer: A , B

QUESTION 58:

What is the default username / password of FortiGate unit?

A. admin , no password
B. admin , fortigate
C. administrator , fortigate
D. fortigate , fortigate

Answer: A

QUESTION 59:

How to connect FortiGate unit when configuring factory-default? Select all that apply.

A. internal , https://192.168.1.99
B. internal , https://192.168.10.99
C. internal , http://192.168.1.99
D. internal , http://192.168.10.99

Answer: A , C

QUESTION 60:

Which of the following statement about Fortimanager is true? Select all that apply.

A. Fortimanager server connect with Fortigate unit using ssh to view
B. Fortimanager server connect with Fortigate unit using https for firmware upgrade
C. all communications between server and devices is encrypted and authenticated
D. devices logs are forwarding to the server using syslog / IPSEC

Answer: A , B, C , D

QUESTION 61:

Which of one the following can improve the security of Fotigate remote administration? Select all that apply.

A. use secure administrative user passwords
B. change these password regularly
C. enable secure administrative access to this interface using only HTTPS or SSH
D. use transparent mode

Answer: A , B, C

QUESTION 62:

Which one of the following statement about Fortigate logging is true? Select all that apply.

A. logging message are divided into 7 levels : Informational , Notification , Warning , Error , Critical , Alert , Emergency
B. if we choose logging level as Emergency , then all 7 level messages will be logged
C. logging message are divided into 5 levels : Informational , Notification , Warning , Alert , Emergency
D. logging message are divided into 5 levels : Informational , Warning , Error , Critical , Emergency

Answer: A , B

QUESTION 63:

Which one of the following user authentication method is supported in Fortigate unit? Select all that apply.

A. Ldap
B. Radius

C. ad
D. local

Answer: A, B, C, D

Explanation :
You can control access to network resources by defining lists of authorized users, called user groups. To use a particular resource, such as a network or a VPN tunnel, the user must belong to one of the user groups that is allowed access. The user then must correctly enter a user name and password to prove his or her identity. This is called authentication.
You can configure authentication in:
any firewall policy wiith action set ACCEPT
IPSec,PPTP and L2TP VPN configurations
When the user attempts to access the resource, the FortiGate unit requests a user name and password. The FortiGate unit can verify the user's credentials locally or using an external LDAP or RADIUS server.
Authentication expires if the user leaves the connection idle for longer than the authentication timeout period.
You need to determine the number and membership of your user groups appropriate
to your authentication needs.

QUESTION 64:

Fortigatesupport Windows XP client for establishing IPSEC connection ?

A. true
B. False

Answer: B
Explanation : Fortigate support IPSEC for fortiglient;windows XP client is a hybrid type of IPSEC + L2TP .

QUESTION 65:

How many recipients can be entered when configuring alert email setting ?

A. 1
B. 2
C. 3
D. 4

Answer: C

QUESTION 66:

The following type of malware changes its code every time it replicates and infects a new file . These changes prevent the malware from detected by an antivirus program . Choose the best answer .

A. Transformer virus
B. Polymorphic virus
C. Parasitic virus
D. Cavity virus
E. Polyphonic virus
F. Camoflage virus
G. (g) Chemeleon vorus

Answer: B
Explanation
Polymorphic Virus
A virus that can change its byte pattern when it replicates. This allows the virus to avoid detection by string-scanning techniques. Sophisticated spyware can also deploy polymorphic characteristics.

QUESTION 67:

Which one of the following about Hash function is ture ?

A. generate variable-sized output for fixed input
B. generate fixed-sized output variable input
C. generate fixed-sized output for fixed input
D. generate variable-sized output for variable input

Answer: A

Explanation :
A hash function H is a transformation that takes a variable-size input m and returns a fixed-size string, which is called the hash value h (that is, h = H(m)). Hash functions with just this property have a variety of general computational uses, but when employed in cryptography the hash functions are usually chosen to have some additional properties.
The basic requirements for a cryptographic hash function are:
1. the input can be of any length,
2. the output has a fixed length,
3. H(x) is relatively easy to compute for any given x ,
4. H(x) is one-way,
5. H(x) is collision-free.
A hash function H is said to be one-way if it is hard to invert, where "hard to invert" means that given a hash value h, it is computationally infeasible to find some

input x such that H(x) = h.
If, given a message x, it is computationally infeasible to find a message y not equal to x such that H(x) = H(y) then H is said to be a weakly collision-free hash function.
A strongly collision-free hash function H is one for which it is computationally infeasible to find any two messages x and y such that H(x) = H(y).
The hash value represents concisely the longer message or document from which it Was comuted;one can think of a messages digest as a "digital fingerprient"of the larger document. Examples of well-known hash functions are MD2 and MD5 and SHA

QUESTION 68:

It has been decided that Key-Chain will be used in your corporate enterprise routing environment . A key-Chain can ....

A. only be used with OSPF
B. can be used with RIP v1
C. can be used with RIP v2
D. can be used with RIP v3

Answer: C

QUESTION 69:

Which one is the most secure method for encryption and authentication

A. des & md5
B. 3des & md5
C. aes & md5
D. aes & sha1

Answer: D

QUESTION 70:

What does the Fortigate SOHO model DNS forwarding function do?

A. forwards DNS queries from a pc to the DNS servers defined in the pc's tcp/ip settings
B. become the DNS server , pc send DNS query to the Fortigate unit
C. pass it's DNS setting to the PC in the local network
D. forward DNS query to DNS servers and returns the answer to the pc that made the request

Answer: B

Explanation :

Several FortiGate functions, including Alert E-mail and URL blocking, use DNS. You can add the IP addresses of the DNS servers to which your FortiGate unit can connect. DNS server IP addresses are usually supplied by your ISP.
You can configure primary and secondary DNS server addresses, or you can configure the FortiGate unit to obtain DNS server addresses automatically. To obtain addresses automatically, at least one interface must use the DHCP or PPPoE addressing mode.
If you enable DNS Forwarding on an interface, hosts on the attached network can use the interface IP address as their DNS server. DNS requests sent to the interface are forwarded to the DNS server addresses you configured or that the FortiGate unit obtained automatically.

QUESTION 71:

Default radius port can be changed ?

A. True
B. False

Answer: A

Explanation :

system global command keywords and variables (Continued)

Keywords and variables	Description	Default	Availability
radius_port <port_integer>	Change the default RADIUS port. The default port for RADIUS traffic is 1812. If your RADIUS server is using port 1645 you can use the CLI to change the default RADIUS port.	1812	All models.

QUESTION 72:

In the FortiOS 2.80 , which of the following feature can be configured per-VD?
Select all that apply.

A. physical interface
B. (b) vlan sub interface
C. routing
D. firewall policy
E. vpn
F. protection profile
G. log & report

Answer: A, B, C, D, E
Explanation : from the administration guide of FG-60 page148 - 152 , physical interface , clan sub interface , routing information , firewall policy , vpn setting ca be configured per-virtual domain basis .

QUESTION 73:

Which of the following ensure that the routing information is reliable ?

A. key-chain list
B. access-list
C. prefix-list
D. rip
Answer : A

Explanation :
RIP version 2 uses authentication keys to ensure that the routing information exchanged between routers is reliable. For authentication to work both the sending and receiving routers must be set to use authentication, and must be configured with the same keys.
A key chain is a list of one or more keys and the send and receive lifetimes for each key. Keys are used for authenticating routing packets only during the specified lifetimes. The FortiGate unit migrates from one key to the next according to the scheduled send and receive lifetimes. The sending and receiving routers should have their system dates and times synchronized, but overlapping the key lifetimes ensures that a key is always available even if there is some difference in the system times.

QUESTION 74:

Which one of the following is unnecessary for create a port mapping vip for external 10.1.1.1 : 80 to internal 172.31.1.1 : 443 ?

A. set the vip to static nat
B. set the vip external port to 80
C. set the external ip to 10.1.1.1
D. add a firewall policy from external to internal , set the destination to the name of the vip

Answer: A

QUESTION 75:

Which of the following statements is not true about address and address group ?

A. you can not change the name of address or address group
B. the same address range can not be assigned to another address name
C. if a address group I used in a firewall policy , it can be deleted only if it is removed from the policy
D. if a address is assigned in a address group , it can not be deleted until it is removed from that address group

Answer: B

Explanation :
You can add, edit, and delete firewall addresses as required. You can also organize related addresses into address groups to simplify policy creation.
A firewall address can be configured with a name, an IP address, and a netmask, or a name and IP address range.
You can enter an IP address and netmask using the following formats.
1. x.x.x.x/x.x.x.x, for example 64.198.45.0/255.225.255.0
2. x.x.x.x/x, for example 64.195.45.0/24
3. You can enter an IP address range using the following formats.
4. x.x.x.x.-x.x.x.x, for example 192.168.110.100-192.168.110.120
5. x.x.x[x-x], for example 192.168.110.[100-120]
6. x.x.x.*,for example 192.168.110.* to represent all addresses on the subnet

---

QUESTION 76:

Which of the following greatest impact the security of VPN tunnel

A. aggressive mode
B. main mode
C. short keep alive
D. key life based on bytes rather than seconds
E. PFS
F. use fewer proposals for encryption and authentication

Answer: A

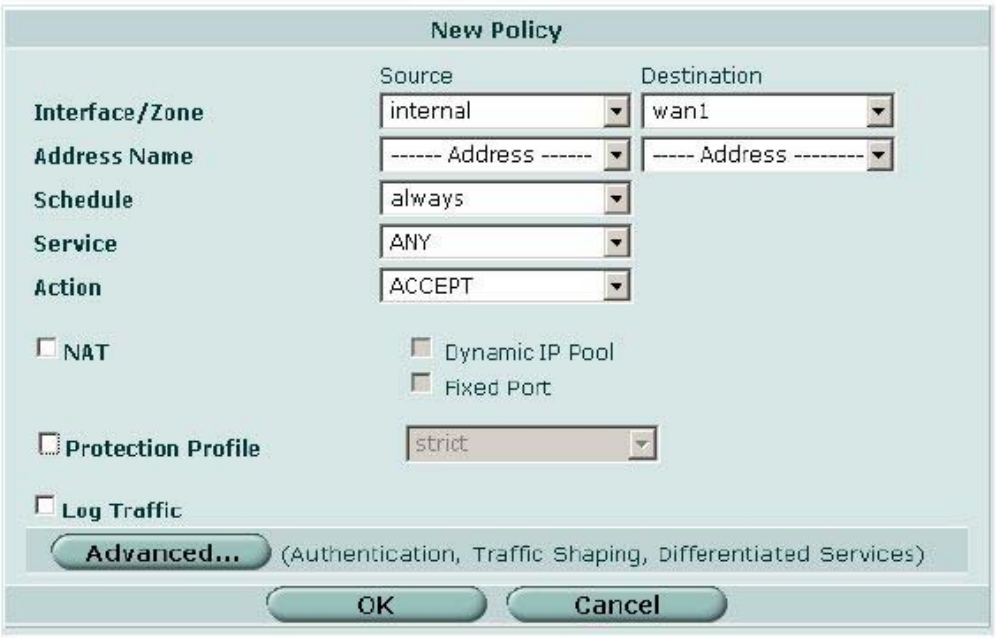
QUESTION 77:

Which one of the following can not be added in security policy ?

A. source address group
B. (b) custom service
C. (c) predefined service
D. (d) URLS
E. (e) one-time schedule

Answer: D

Explanation :
Policy options
Policy options are configurable when creating or editing a firewall policy.
Figure 89: Standard policy options



Interface / Zone
Select the source and destination interface or zone for the firewall policy. Interfaces and zones are listed and configured in System > Network. See "Interface" on page 51
for information about interfaces. See "Zone" on page 62 for information about zones.
Address Name
Select the source and destination firewall addresses for the firewall policy. Before adding addresses to a policy, you must add them to the FortiGate firewall configuration. To add firewall addresses, see "Address" on page 211.
For NAT/Route mode policies where the address on the destination network is hidden
from the source network using NAT, the destination can also be a virtual IP that maps the
destination address of the packet to a hidden destination address. See "Virtual IP" on page 227.
Source Select the name of the source interface or zone for the policy. The source interface or zone receives the packets to be matched by the policy.
Destination Select the name of the destination interface or zone for the policy. Packets matched by the policy exit the FortiGate unit from the destination interface or zone.
Source Select the name of a firewall address or address group that matches the source address of the packets to be matched with this policy.
Destination Select the name of a firewall address or address group that matches the destination address of the packets to be matched with this policy.
Schedule
Select a schedule that controls when the policy is available to be matched with connections. See "Schedule" on page 224.
Service

Select the name of a service or service group that matches the service or protocol of the packets to be matched with this policy. You can select from a wide range of predefined services or add custom services and service groups. See "Service" on page 216.

Action

Select how you want the firewall to respond when the policy matches a connection attempt.

VPN Tunnel

Select a VPN tunnel for an ENCRYPT policy. You can select an AutoIKE key or Manual Key tunnel.

ACCEPT Accept connections matched by the policy. You can also configure NAT, protection profiles, log traffic, traffic shaping, authentication, and differentiated services. You can also add a comment to the policy.

DENY Select deny to reject connections matched by the policy. The only other policy
options that you can configure are log traffic (to log the connections denied by this policy) and differentiated services. You can also add a comment to the policy.

ENCRYPT Select encrypt to make this policy an IPSec VPN policy. An IPSec VPN policy
causes the FortiGate unit to accept IPSec packets. When encrypt is selected the VPN Tunnel Options appear. You can also configure protection profiles, log traffic, traffic shaping, and differentiated services. You can also add a comment to the policy. You cannot configure NAT or add authentication to an encrypt policy. For more information, see "Adding firewall policies for IPSec VPN tunnels" on page 280.

Allow Inbound Select Allow inbound so that traffic from the remote network or host can start
the IPSec VPN tunnel.

Allow outbound Select Allow outbound if traffic from the local network can start the tunnel.

Inbound NAT Select Inbound NAT to translate the source address of incoming packets to
the FortiGate internal IP address.

Outbound NAT Select Outbound NAT to translate the source address of outgoing packets to
the FortiGate external IP address.

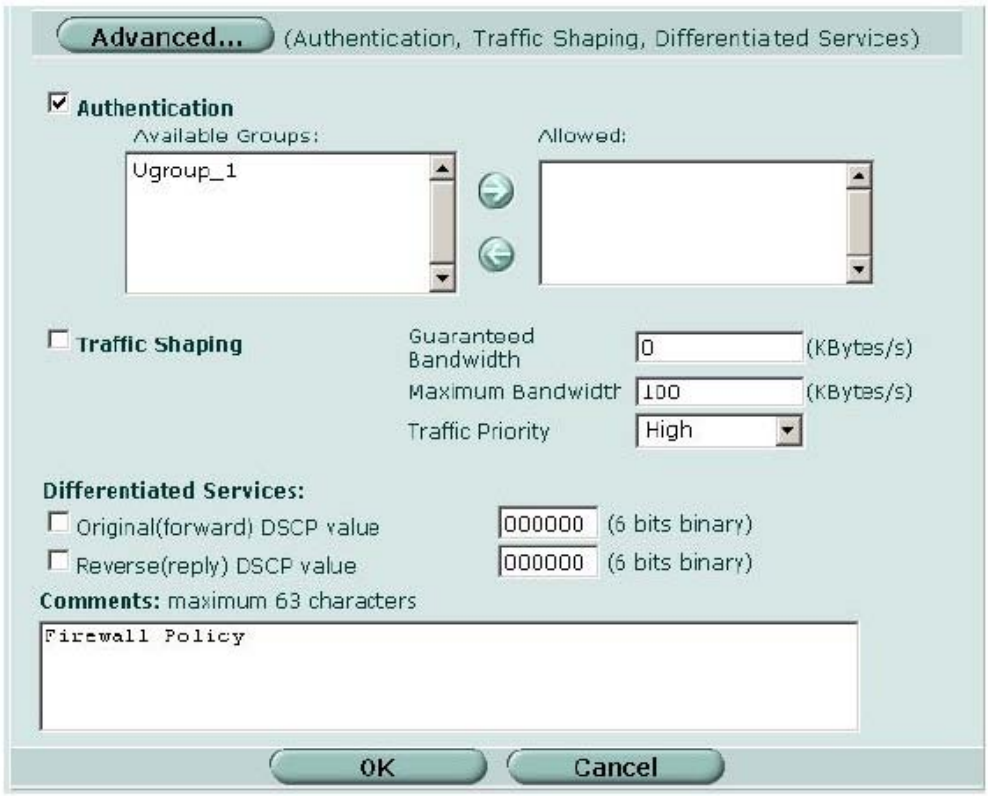
NAT

Select NAT to enable Network Address Translation for the policy. NAT translates the source address and port of packets accepted by the policy. If you select NAT, you can also select Dynamic IP Pool and Fixed Port. NAT is not available in Transparent mode.

Protection Profile

Select a protection profile to configure how antivirus, web filtering, web category filtering, spam filtering, IPS, and content archiving are applied to a firewall policy. For information about adding and configuring Protection profiles, see "Protection

profile" on page 235.
If you are configuring authentication in the advanced settings, you do not need to choose a protection profile since the user group chosen for authentication are already
tied to protection profiles. For more information about adding authentication to firewall
policies, see "Authentication" on page 207.
Log Traffic
Select Log Traffic to record messages to the traffic log whenever the policy processes
a connection. You must also enable traffic log for a logging location (syslog, WebTrends, local disk if available, memory, or FortiLog) and set the logging severity
level to Notification or lower. For information about logging see "Log & Report" on page 353.
Advanced
Select advanced to show advanced policy options.
Dynamic IP Pool Select Dynamic IP Pool to translate the source address to an address randomly selected from an IP Pool. An IP Pool can be a single IP address or an IP address range. An IP pool list appears if IP Pool addresses have been added to the destination interface or zone.
Select ANY IP Pool to cause the FortiGate unit to select any IP address in any IP Pool added to the destination interface or zone.
Select the name of an IP Pool added to the destination interface or zone cause the FortiGate unit to translate the source address to one of the addresses defined by this IP Pool.
You cannot select Dynamic IP Pool if the destination interface, VLAN subinterfaceor if one of the interfaces or VLAN subinterfaces in the destination zone is configured using DHCP or PPPoE.
For information about adding IP Pools, see "IP pool" on page 232.
Fixed Port Select Fixed Port to prevent NAT from translating the source port. Some applications do not function correctly if the source port is changed. In most cases, if you select Fixed Port, you would also select Dynamic IP pool. If you do not select Dynamic IP pool, a policy with Fixed Port selected can only allow one connection at a time.
Advanced policy options
When configuring a firewall policy, select Advanced to configure advanced firewall policies.
Figure 90: Advanced policy options



Authentication

You must add users and a firewall protection profile to a user group before you can select Authentication. For information about adding and configuring user groups, see

"User group" on page 251.

Select Authentication and select one or more user groups to require users to enter a user name and password before the firewall accepts the connection.

Figure 91: Selecting user groups for authentication

You can select Authentication for any service. Users can authenticate with the firewall

using HTTP, Telnet, or FTP. For users to be able to authenticate you must add an HTTP, Telnet, or FTP policy that is configured for authentication. When users attempt

to connect through the firewall using this policy they are prompted to enter a firewall

username and password.

If you want users to authenticate to use other services (for example POP3 or IMAP)

you can create a service group that includes the services for which you want to require authentication, as well as HTTP, Telnet, and FTP. Then users could authenticate with the policy using HTTP, Telnet, or FTP before using the other service.
In most cases you should make sure that users can use DNS through the firewall without authentication. If DNS is not available users cannot connect to a web, FTP, or
Telnet server using a domain name.
Traffic Shaping
Traffic Shaping controls the bandwidth available to and sets the priority of the traffic
processed by the policy. Traffic Shaping makes it possible to control which policies have the highest priority when large amounts of data are moving through the FortiGatedevice. For example, the policy for the corporate web server might be given
higher priority than the policies for most employees' computers. An employee who needs unusually high-speed Internet access could have a special outgoing policy set up with higher bandwidth.
If you set both guaranteed bandwidth and maximum bandwidth to 0 (zero), the policy
does not allow any traffic.
Differentiated Services
Differentiated Services describes a set of end-to-end Quality of Service (QoS) capabilities. End-to-end QoS is the ability of a network to deliver service required by
specific network traffic from one end of the network to another. By configuring differentiated services you configure your network to deliver particular levels of service
for different packets based on the QoS specified by each packet.
Differentiated Services (also called DiffServ) is defined by RFC 2474 and 2475 as enhancements to IP networking to enable scalable service discrimination in the IP network without the need for per-flow state and signalling at every hop. Routers that
can understand differentiated services sort IP traffic into classes by inspecting the DS
field in IPv4 header or the Traffic Class field in the IPv6 header.
Note: Policies that require authentication must be added to the policy list above matching
policies that do not ;otherwise,the policy that does not requre authentication is selected first.
Guaranteed
Bandwidth
You can use traffic shaping to guarantee the amount of bandwidth available through the firewall for a policy. Guarantee bandwidth (in Kbytes) to make sure that there is enough bandwidth available for a high-priority service.
Maximum

Bandwidth
You can also use traffic shaping to limit the amount of bandwidth available through the firewall for a policy. Limit bandwidth to keep less important services from using bandwidth needed for more important services.
Traffic Priority Select High, Medium, or Low. Select Traffic Priority so that the FortiGate unit
manages the relative priorities of different types of traffic. For example, a policy for connecting to a secure web server needed to support e-commerce traffic should be assigned a high traffic priority. Less important services should be assigned a low priority. The firewall provides bandwidth to lowpriority connections only when bandwidth is not needed for high-priority connections.
You can use the FortiGate Differentiated Services feature to change the DSCP (Differentiated Services Code Point) value for all packets accepted by a policy. The network uses these DSCP values to classify, mark, shape, and police traffic, and to perform intelligent queuing. DSCP features are applied to traffic by configuring the routers on your network to apply different service levels to packets depending on the DSCP value of the packet.
You can configure policies to apply DSCP values for both original (or forward) traffic and reverse (or reply) traffic. These values are optional and may be enabled independently from each other. When both are disabled, no changes to the DS field are made.
Comments
You can add a description or other information about the policy. The comment can be up to 63 characters long, including spaces.
Original
(forward) DSCP
value
Set the DSCP value for packets accepted by the policy. For example, for an Internal->External policy the value is applied to outgoing packets as they exit the external interface and are forwarded to their destination.
Reverse (reply)
DSCP value
Set the DSCP value for reply packets. For example, for an Internal->External policy the value is applied to incoming reply packets before they exit the internal interface and returned to the originator.

QUESTION 78:

Which of the following statement about IPS action DROP session is true ?

A. drop the packet that trigger the signature
B. drop the packet that trigger the signature , remove the session from session table without sending reset
C. drop the packet that trigger the signature , drop any other packets in the same session
D. drop the packet that trigger the signature , reset both client and server , remove the

session from session table

Answer: C

Explanation :

Table 27: Actions to select for each predefined signature

Action	Description
Pass	The FortiGate unit lets the packet that triggered the signature pass through the firewall. If logging is disabled and action is set to Pass, the signature is effectively disabled.
Drop	The FortiGate unit drops the packet that triggered the signature. Fortinet recommends using an action other than Drop for TCP connection based attacks.
Reset	The FortiGate unit drops the packet that triggered the signature, sends a reset to both the client and the server, and removes the session from the FortiGate session table. Used for TCP connections only. If you set this action for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset action is triggered before the TCP connection is fully established it acts as Clear Session.
Reset Client	The FortiGate unit drops the packet that triggered the signature, sends a reset to the client, and removes the session from the FortiGate session table. Used for TCP connections only. If you set this action for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset Client action is triggered before the TCP connection is fully established it acts as Clear Session.
Reset Server	The FortiGate unit drops the packet that triggered the signature, sends a reset to the server, and removes the session from the FortiGate session table. Used for TCP connections only. If you set this action for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset Server action is triggered before the TCP connection is fully established it acts as Clear Session.
Drop Session	The FortiGate unit drops the packet that triggered the signature and drops any other packets in the same session.
Clear Session	The FortiGate unit drops the packet that triggered the signature, removes the session from the FortiGate session table, and does not send a reset.
Pass Session	The FortiGate unit lets the packet that triggered the signature and all other packets in the session pass through the firewall.

QUESTION 79:

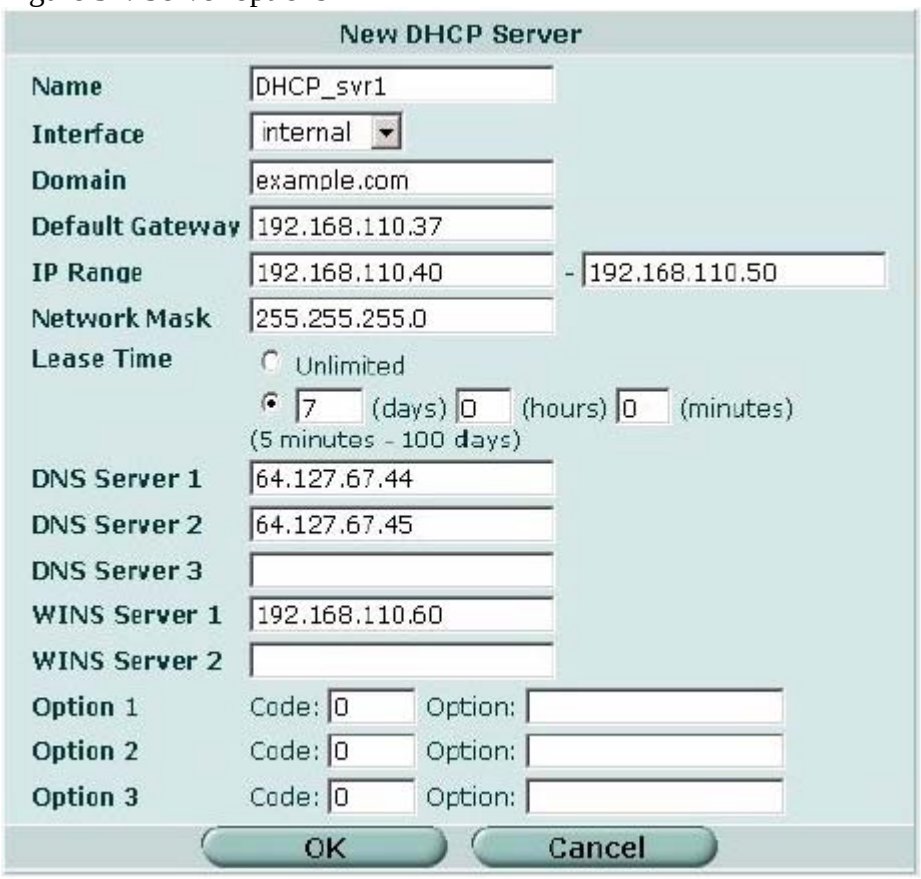
Fortigateunit can distribute WINS & DNS server address ?

A. true , dhcp relay also supported
B. false , but support dhcp relay
C. false
D. true

Answer: A

Explanation :
Server
You can configure one or more DHCP servers for any FortiGate interface. As a
DHCP

server, the interface dynamically assigns IP addresses to hosts on a network connected to the interface.
You can add more than one DHCP server to a single interface to be able to provide DHCP services to multiple networks.
DHCP server settings
Figure 31: Server options



Name Enter a name for the DHCP server configuration.
Interface Select the interface for which to configure the DHCP server.
Domain Enter the domain that the DHCP server assigns to DHCP clients.
Default Gateway Enter the IP address of the default gateway that the DHCP server assigns to DHCP clients.
IP Range Enter the starting IP and ending IP for the range of IP addresses that this DHCP server assigns to DHCP clients.
Network Mask Enter the netmask that the DHCP server assigns to DHCP clients.
Lease Time Select Unlimited for an unlimited lease time or enter the interval in days, hours, and minutes after which a DHCP client must ask the DHCP server for new settings. The lease time can range from 5 minutes to 100 days.
DNS Server Enter the IP addresses of up to 3 DNS servers that the DHCP server assigns to DHCP clients.
WINS Server Add the IP addresses of one or two WINS servers that the DHCP server assigns to DHCP clients.
Option Up to three custom DHCP options that can be sent by the DHCP server. Code is the DHCP option code in the range 1 to 255. Option is an even

number of hexadecimal characters and is not required for some option codes. For detailed information about DHCP options, see RFC 2132, DHCP Options and BOOTP Vendor Extensions.

QUESTION 80:

The auth timeout is applies to ?

A. administrator access
B. (b) vpn connections
C. (c) authentication users
D. (d) vpn authentication

Answer: C

Explanation :
Auth Timeout Set the firewall user authentication timeout to control how long an authenticated connection can be idle before the user must authenticate again. The maximum authtimeout is 480 minutes (8 hours). The default Auth Timeout is 15 minutes.

QUESTION 81:

What is the least disruption method to solve the problem of incorrect routing information ?

A. reoot
B. restart routing engine using webUI
C. restart routing engine using CLI
D. Bring down the related interface from WebUI

Answer: D

QUESTION 82:

Which one of the following is not included in a digital certificate ?

A. subject name
B. issuer name
C. hash algorism
D. encryption algorism

Answer: C

Explanation :
An attachment to an electronic message used for security purposes. The most

common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.
An individual wishing to send an encrypted message applies for a digital certificate from a Certificate Authority (CA). The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or perhaps on the Internet.
The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply.
The most widely used standard for digital certificates is X.509.

QUESTION 83:

Exhibit:
1.Create internal lan ip address
2.Create remote lan private ip address
3.Define remote gateway ip address
4.Define IPSEC tunnel
5.Create firewall policy
What is the correct order when create IPSEC VPN connection?

A. 1,2,3,4,5
B. 2,1,4,3,5
C. 2,4,5,1,3
D. 3,1,2,4,5

Answer: A

QUESTION 84:

Which of the following should be done before setting Auth in IPSEC phase 1? Select all that apply.

A. purchase a license for it
B. choose dial-up user in phase 1
C. use specific FortiOS
D. Add a user group

Answer: B, D

QUESTION 85:

When setting PPTP you find the settings fields are grey in colour, which of the following is a possible cause ?

A. vpn is not installed
B. user group has not been created
C. PPTP is not enabled
D. IPSEC is used

Answer: C

QUESTION 86:

Create a external to internal policy is required when configuring a firewall policy for IPSEC SA

A. true
B. false

Answer: A

QUESTION 87:

What is the required step when setting up IPSEC SA? Select all that apply.

A. phase 1 setting
B. phase 2 setting
C. content filtering setting
D. Firewall policy setting
E. Administrator timeout setting

Answer: A , B, D

QUESTION 88:

Which of the following options support load balance & HA

A. all fortigate products
B. fg-60 and above
C. fg-300 and abov
D. fg-800 and above

Answer: B

QUESTION 89:

Which of the following statement is true about HA heartbeat device ?

A. only one interface can be configured as heartbeat device

B. up to 2 interfaces can be configured as heartbeat device
C. you can configure multiple heartbeat device , any physical interface can be heartbeat device
D. you can configure multiple heartbeat device , any physical interface & vlan sub-interface can be heartbeat device

Answer: C
Explanation
Heartbeat devices
A heartbeat device is an Ethernet network interface in a cluster that is used by the FGCP for HA heartbeat communications between cluster units. You can configure multiple network interfaces to be heartbeat devices. An interface becomes a heartbeat
device when it is assigned a heartbeat device priority. The HA configuration in Figure 2 shows port3 and port4/ha configured as heartbeat devices.

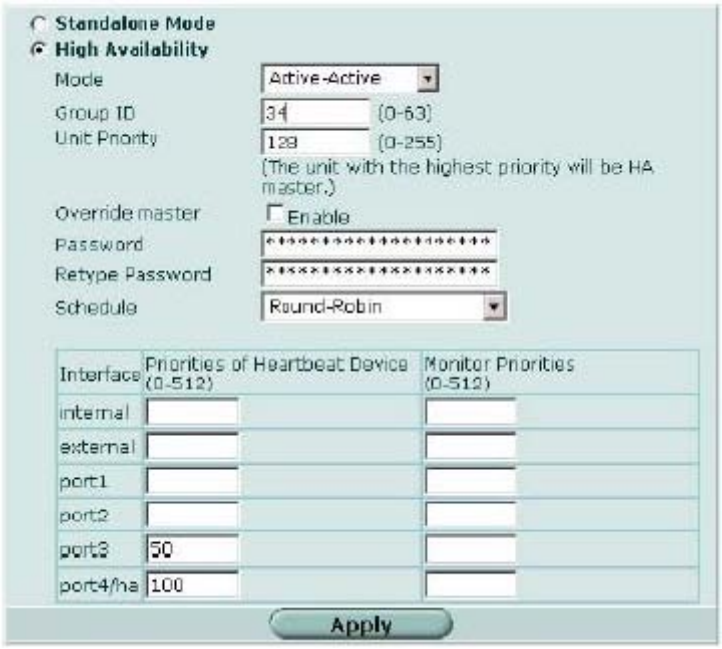


Figure 2: Example FortiGate-3000 heartbeat device configuration
The heartbeat device with the highest priority is the active heartbeat device. In Figure 2, port4/ha is the active heartbeat device. The active heartbeat device sends and receives all heartbeat communications. If the active heartbeat device fails or is disconnected on one or more of the cluster units, the heartbeat device with the next highest priority becomes the active heartbeat device. This is called heartbeat device failover. Heartbeat device failover occurs transparently, without interrupting the communication sessions being processed by the cluster and without affecting cluster synchronization.
By default, for all FortiGate units, two interfaces are configured to be heartbeat devices. The active heartbeat device has a priority of 100. A second, or backup heartbeat device has a priority of 50.
The fortiGate-300,400,500,800,1000,3000,and 3600 HA interfaces has the highest heartbeat device priority.

The fortiGate-60,100,200,and the Fortiwifi60 DMZ interface has the highest interfaces heartbeat device priority.
The FortiGate-100A and 200A DMZ2 interface has the highest heartbeat device priority.
The FortiGate-300A and 400A, and500A port4 interface has the highest heartbeat device priority.
The FortiGate-4000 out of band management interface has the highest heartbeat device priority.
The FortiGate-5000 has two dedicated HA heartbeat device (Port 9 and Port 10). Port 10 has the highest heartbeat device priority.
You can change the heartbeat device configuration as required. All interfaces can be assigned different heartbeat priorities. You can also configure only one interface to be a heartbeat device. You can set the heartbeat device priority for each interface to any number between 1 and 512. In all cases, the heartbeat device with the highest priority is used for all HA heartbeat communication. If this interface fails or becomes disconnected, the interface with the next highest priority handles all of the heartbeat traffic.
For the HA cluster to function correctly, at least one interface must be a heartbeat device. Also the heartbeat devices of all cluster units must be connected together. If heartbeat communication is interrupted and cannot fail over to a second heartbeat device, the cluster stops processing traffic.
Heartbeat device IP addresses
You do not need to assign IP addresses to the heartbeat device interfaces for them to be able to process heartbeat packets. The FGCP assigns virtual IP addresses to the heartbeat device interfaces. The primary unit heartbeat device IP address is 10.0.0.1.
Subordinate units are assigned heartbeat device IP addresses 10.0.0.2, 10.0.0.3, and so on.
For best results, isolate the heartbeat devices from your user networks by connecting the heartbeat devices to a separate switch that is not connected to any network. If the cluster consists of two FortiGate units you can connect the heartbeat device interfaces directly using a crossover cable. Heartbeat packets contain sensitive information about the cluster configuration. Heartbeat packets may also use a considerable amount of network bandwidth. For these reasons, it is preferable to isolate heartbeat packets from your user networks.
Both HA heartbeat and data traffic are supported on the same FortiGate interface.
In NAT/Route mode, if you decide to use the heartbeat device interfaces for processing network traffic or for a management connection, you can assign the interface any IP address. In Transparent mode, you can connect the interface to your network and configure management access to it. These configurations do not affect heartbeat traffic or the heartbeat device IP addresses.

QUESTION 90:

When configure meshed VPN , all traffic is routed through the hub at the central site ?

A. true
B. false

Answer: B

Explanation
Concentrator
In a hub-and-spoke configuration, connections to a number of remote peers radiate from a single, central FortiGate unit. Site-to-site connections between the remote peers do not exist; however, VPN tunnels between any two of the remote peers can be established through the FortiGate unit "hub".
In a hub-and-spoke network, all VPN tunnels terminate at the hub. The peers that connect to the hub are known as "spokes". The hub functions as a concentrator on the network, managing all VPN connections between the spokes. VPN traffic passes from one tunnel to the other through the hub.
You define a concentrator to include spokes in the hub-and-spoke configuration.

QUESTION 91:

How to quarantine infected file? Select all that apply.

A. AV scan with infected file block
B. AV scan with infected file pass
C. Enable quarantine infected files
D. disable quarantine infected file

Answer: A , C

QUESTION 92:

What protocol can be scanned for antivirus ?

A. http , ftp , imap , smtp , pop3
B. ttp , ftp , imap , tftp , pop3
C. http . ftp
D. http , imap , pop3 , smtp

Answer: A

Explanation :

Table 28: Antivirus and Protection Profile antivirus configuration

Protection Profile antivirus options	Antivirus setting
Virus Scan	Antivirus > Config > Virus List
Enable or disable virus scanning for each protocol (HTTP, FTP, IMAP, POP3, SMTP).	View a read-only list of current viruses.
File Block	Antivirus > File Block
Enable or disable file blocking for each protocol.	Configure file patterns to block, enable or disable blocking for each protocol.
Quarantine	Antivirus > Quarantine
Enable or disable quarantining for each protocol. Quarantine is only available on units with a local disk.	View and sort the list of quarantined files, configure file patterns to upload automatically to Fortinet for analysis, and configure quarantining options in AntiVirus.
Pass fragmented emails	
Enable or disable passing fragmented emails. Fragmented emails cannot be scanned for viruses.	
Oversized file/email	Antivirus > Config > Config
Configure the FortiGate unit to block or pass oversized files and emails for each protocol.	Set the size thresholds for files and emails for each protocol in Antivirus. Go to Antivirus > Config > Grayware to enable blocking grayware programs.
Add signature to outgoing emails	
Create and enable a signature to append to outgoing emails (SMTP only).	

QUESTION 93:

Virus scan is applied before blocking

A. true
B. False

Answer: B

Explanation:
Reference: Fortigate Multi-Threat Security Systems 1 (Course 201) Student Guide page 144

QUESTION 94:

How to block *.scr from HTTP download ?

A. file blocking is enabled by default
B. create or edit a protection profile , go to antivirus->file block , enable file block for http , add this protection profile to external -> internal policy
C. create or edit a protection profile , go to antivirus->file block , enable file block for http , add this protection profile to internal -> external policy
D. create or edit a protection profile , enable file block for http , add this protection profile to external -> internal policy

Answer: B

QUESTION 95:

Which of the following statement is true about web filtering? Select all that apply.

A. urls in exempt list are exempt from virus scaning
B. you can upload text file of exempt list which separate each url by ";"
C. Fortigate unit communicate with Fortigard using UDP 8888
D. url blocking dose not block ftp://ftp.fortinet.com

Answer: A, C, D

QUESTION 96:

Fortiguard rates URLs according to :

A. domains
B. path
C. page

Answer: B

QUESTION 97:

The precedence of web filtering is ?

A. exempt list , url block list , url pattern list , fortiguard , content block
B. url block list , url pattern list , exempt list , content block , fortiguard
C. content block , fortiguard , url block list , url pattern list , exempt list
D. url pattern list , fortiguard , content block , exempt list , url block list

Answer: B

QUESTION 98:

Fortigate is abe to check the banned word for both web and email

A. true
B. false

Answer: A

QUESTION 99:

IPSEC provide security service for ?

A. data-link layer
B. network lauer
C. transport layer
D. presentation layer

Answer: B

QUESTION 100:

The following type of malware spread itself through network ?

A. worm
B. trujan
C. download
D. exploit
E. phish

Answer: A

QUESTION 101:

MD5 is a example of a ?

A. encryption algorithm
B. digital signature
C. hashed mac
D. SA

Answer: D

Explanation :
IPSEC was developed by the Internet Engineering Task Force (IETF) to address certain vulnerabilities inherent in the popular IP protocol. Exploits in IP allowed for eavesdropping (sniffing) and identity masking (spoofing), so it was difficult to get guaranteed security over large networks. Prior solutions would provide security for only specific applications (PGP for email and SSL for web applications). IPSEC secures the network itself, so it also secures the applications using the network. IPSEC is a set of IP extensions that provide strong data authentication and privacy guarantees through the use of modern encryption techniques.
To have security on your network, you need to have confidence in three factors:

1. The person you are communicating with is really that person (authentication)
2. No one can eavesdrop on your communication (confidentiality)
3. The communication that you received has not been modified in transit (integrity)

IPSEC is comprised of three components that provide these security functions.

Authentication Header (AH) - A signature is tied to each packet, allowing you to verify the sender's identity and the integrity of the data. Currently MD5 and SHA-1 authentication schemes are supported.

Encapsulating Security Payload (ESP) - Uses strong encryption algorithms to encrypt the data in each packet to defeat common eavesdropping techniques. The most common encryption algorithm used by ESP is 56-bit DES, but ESP is an open protocol that allows support for most current (and even future) encryption algorithms.

Internet Key Exchange (IKE) - Allows nodes to agree on authentication methods, encryption methods, the keys to use and the keys' lifespan. IKE also allows smart secure key exchange.

AH and ESP provide the means to protect data from tampering, preventing eavesdropping and verifying the origin of the data. IKE provides a secure method of exchanging keys and negotiating protocols and encryption algorithms to use. The information negotiated IKE is stored in a Security Association (SA). The SA is like a contract laying out the rules of the VPN connection for the duration of the S

A. An SA is assigned a 32-bit number that, when used in conjunction with the destination IP address, uniquely identifies the S

A. This number is called the Security Parameters Index or SPI.

To tie this all together, let's look at an example. User A wants to send data to User B. User A's router (router A) has a security policy applied with a rule that says all traffic to User B needs to be encrypted. User B's router (router B) will be the other end of an IPSEC tunnel. Router A checks to see if an IPSEC SA exists between it and router B. If it doesn't, router A will request an IPSEC SA from IKE. If an IKE SA exists between the two routers, an IPSEC SA is issued. If an IKE SA does not exist, one has to be negotiated first, with the routers exchanging information signed by a third-party certificate authority (CA) that both routers trust. Once the IKE SA is agreed upon by the routers, an IPSEC SA can be issued, and secure, encrypted communications can begin. This process is transparent to User A and User B.

The basic steps for setting up an IPSEC connection are as follows:
1. Set up an IKE SA.
2. Agree upon the terms of communication and encryption algorithm. Create an IPSEC SA.
3. Start sending data.

QUESTION 102:

Which of the following malware attempt to scam the user into surrendering private information that will be used to identity theft ?

A. torjan
B. Phish
C. Downloader
D. Worm

Answer: B

QUESTION 103:

Which spam filter does not query DNS servers for an address record?

A. Return email DNS check
B. Hello DNS lookup
C. RBL/ORDBL list
D. BWL check

Answer: A, C

QUESTION 104:

Which action must be taken when creating a new DNSBL entry in Antispam to block spam SMTP email?

A. discard
B. spam
C. reject
D. clear

Answer: B

Explanation :
DNSBL & ORDBL options
DNSBL & ORDBL list has the following icons and features:
Create New Select Create New to add a server to the DNSBL & ORDBL list.

Total The number of items in the list.
The Page up, Page down, and Remove all entries icons.
DNSBL Server The current list of servers.Select the check box to enable all the DNSBL
and ORDBL servers in the list.
Action The action to take on email matched by the DNSBLs and ORDBLs.
Actions are: Mark as Spam to apply the spam action configured in the
protection profile, or Mark as Reject to drop the session.
The Delete and Edit/View icons.