EXAMTOPICS

-Expert Verified, Online, **Free**.



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

Which two configuration settings change the behavior for content-inspected traffic while FortiGate is in conserve mode? (Choose two.)

A. IPS failopen

B. mem failopen

C. AV failopen

D. UTM failopen

Suggested Answer: *A, C*

Angel123 Highly Voted 5 years, 7 months ago

Correct - A and C according NSE7_EF_6.2 Manual p.64 and p.65

upvoted 5 times

ni Most Recent 4 years, 3 months ago

A and C correct

upvoted 1 times

Primo_SP 5 years ago

A and C correct

upvoted 1 times

MunzerR 5 years, 5 months ago

A,C are correct

upvoted 1 times

Question #2 *Topic 1*

Refer to the exhibit, which contains the partial output of a diagnose command.

Based on the output, which two statements are correct? (Choose two.)

```
Spoke-2 # dia vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------------------------------------------
name=VPN ver=1 serial=1 10.200.5.1:0 -> 10.200.4.1:0
bound_if=3 lgwy=statistic/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refernt=15 ilast=10 olast=792 auto-discovery=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqmo=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN proto=0 sa=1 ref=2 serial=1
     src: 0:10.1.2.0/255.255.255.0:0
     dst: 0:10.1.1.0/255.255.255.0:0
     SA: ref=3 options=2e type=00 soft=0 mtu=1438 expire=42403/0B replaywin=204B seqno=1
esn=replaywin_lastseq=00000000
     life: type=01 bytes=0/0 timeout=43177/43200
     dec: spi=ccc1f66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
            ah=sha1 key=20 c68091d68753578785de6a7a6b276b506e527
```

A. Anti-replay is enabled.

B. DPD is disabled.

C. Remote gateway IP is 10.200.4.1.

D. Quick mode selectors are disabled.

Suggested Answer: *A, C*

Angel123 Highly Voted 5 years, 7 months ago

Correct - A and C according NSE7_EF_6.2 Manual p.440

upvoted 7 times

adolfunkz 5 years, 5 months ago

I'm unsure about this, because the replaywin value on Manual is 1024 but in the screen is other value, I'm going to check this on a lab

upvoted 1 times

ni Most Recent 4 years, 3 months ago

Correct - A and C

upvoted 1 times

MunzerR 5 years, 5 months ago

Correct - A and C

upvoted 1 times

Question #3 *Topic 1*

Refer to the exhibit, which contains the output of a diagnose command.
Which two statements regarding the output in the exhibit are true? (Choose two.)

```
FGT # diagnose debug rating
Locale        : english
Service       : Web-filter
Status        : Enable
License       : Contract
Service       : Antispam
Status        : Disable
Service       : Virus Outbreak Prevention
Status        : Disable
 -=- Server List (Mon Apr 19 10:41:32 20xx) -=-
IP                   Weight  RTT    Flags    TZ   Packets   Curr Lost     Total Lost
64.26.151.37         10      45              -5   262432    0             846
64.26.151.35         10      46              -5   329072    0             6806
66.117.56.37         10      75              -5   71638     0             275
65.210.95.240        20      71              -8   36875     0             92
209.222.147.36       20      103     DI      -8   34784     0             1070
208.91.112.194       20      107     D       -8   35170     0             1533
96.45.33.65          60      144              0   33728     0             120
80.85.69.41          71      226              1   33797     0             192
62.209.40.74         150     97               9   33754     0             145
121.111.236.179      45      44      F       -5   26410     26226         26227
```

A. FortiGate will probe 121.111.236.179 every fifteen minutes for a response.

B. Servers with a negative TZ value are experiencing a service outage.

C. Servers with the D flag are considered to be down.

D. FortiGate used 209.222.147.36 as the initial server to validate its contract.

Suggested Answer: *A, D*

Angel123 Highly Voted 5 years, 7 months ago
Correct - A and D according NSE7_EF_6.2 Manual p.176 and p.177
upvoted 5 times

ni Most Recent 4 years, 3 months ago
A & D correct
upvoted 1 times

yadavarya97 4 years, 11 months ago
A & D correct
upvoted 1 times

FortiSherlock 4 years, 11 months ago
B is wrong because TZ indicates the difference of the time zones the FortiGate and the FortiGuard Server are in. C is wrong because D does not stand for Down but for DNS. Meaning the servers were found via name resolution.
upvoted 1 times

asdfsadfsdsdf 4 years, 10 months ago
D = Default = IP address of servers received from DNS resolution. I = Initial= Server contacted to request contact information and updates F = Failed = server connection failed, Fortigate pings every 15min to check if the server has come back. TZ = Timezone of the server (not the difference)
upvoted 3 times

Primo_SP 5 years ago
A and D correct
upvoted 1 times

Dee244 5 years, 4 months ago
A & D, Study Guide 6.4 page 178
upvoted 3 times

MunzerR 5 years, 5 months ago
Correct - A and D
upvoted 3 times

Question #4 *Topic 1*

Which two statements about application layer test commands are true? (Choose two.)

A. They are used to filter real-time debugs.

B. They display real-time application debugs.

C. Some of them can be used to restart an application.

D. Some of them display statistics and configuration information about a feature or process.

Suggested Answer: *C, D*

ni Most Recent 4 years, 3 months ago

C & D correct

upvoted 1 times

yadavarya97 4 years, 11 months ago

C & D are correct.

upvoted 1 times

Primo_SP 5 years ago

Application layer test commands don't display information in real time. So C and D are correct.

upvoted 1 times

MunzerR 5 years, 5 months ago

Correct - C and D

upvoted 1 times

Angel123 5 years, 7 months ago

Correct - C and D according NSE7_EF_6.2 Manual p.59

upvoted 2 times

Question #5 *Topic 1*

Refer to the exhibits, which contain configuration on FortiGate and partial session information.
All traffic to the Internet currently egresses from port1. The exhibit shows partial session information for Internet traffic from a user on the internal network.
If the priority on route ID 1 were changed from 5 to 20, what would happen to traffic matching that user's session?

```
config system global
     set snat-route-change disable
end
config router static
     edit 1
          set gateway 10.200.1.254
          set priority 5
          set device "port1"
     next
     edit 2
          set gateway 10.200.2.254
          set priority 10
          set device "port2"
     next
end
```

```
PGT # diagnose sys session list
session info: proto=6 proto_state=01 duration=600 expire=3179 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty npu f00
statistic(bytes/packets/allow_err): org=3208/25/1 reply=11144/29/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4 gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907->54.239.158.170:80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80->10.200.1.1:64907(10.0.1.10:64907)
pos/ (before, after) 0/ (0,0), 0/(0,0)
src_mac=b4:f7:a1:e9:91:97
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00317c5b tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000c00
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=
0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
```

A. The session would remain in the session table, but its traffic would now egress from both port1 and port2.

B. The session would remain in the session table, and its traffic would still egress from port1.

C. The session would remain in the session table, and its traffic would start to egress from port2.

D. The session would be deleted, so the client would need to start a new session.

Suggested Answer: *B*

habualrob Most Recent 4 years, 2 months ago
B is the correct
upvoted 1 times

ni 4 years, 3 months ago
Correct - B
upvoted 2 times

Ahmed_Elswify 4 years, 11 months ago

Enterprise_Firewall_6.4_Study_Guide page#148,149

upvoted 3 times

fottyfan 5 years, 3 months ago

B because it is a SNATed session

upvoted 2 times

MunzerR 5 years, 5 months ago

Correct - B

upvoted 1 times

MunzerR 5 years, 5 months ago

because this is related to same session of the user

upvoted 1 times

Angel123 5 years, 7 months ago

Correct - B according NSE7_EF_6.2 Manual p.149

upvoted 4 times

Question #6 *Topic 1*

Which three conditions are required for two FortiGate devices to form an OSP adjacency? (Choose three.)

A. OSPF costs match

B. OSPF peer IDs match

C. Hello and dead intervals match

D. OSPF IP MTUs match

E. IP addresses are in the same subnet

Suggested Answer: *C, D, E*

habualrob Most Recent 4 years, 2 months ago

C , D and E

upvoted 1 times

ni 4 years, 3 months ago

C,D,E are correct

upvoted 1 times

yadavarya97 4 years, 11 months ago

C,D,E are correct. Peer ID should be different.

upvoted 1 times

Kevin_Howard 5 years, 3 months ago

C, D and E according NSE7_EF_6.4 Manual p.281

upvoted 1 times

MunzerR 5 years, 5 months ago

C, D, and E

upvoted 1 times

Angel123 5 years, 7 months ago

Correct - C, D and E according NSE7_EF_6.2 Manual p.274

upvoted 4 times

Question #7 *Topic 1*

Which two statements about bulk configuration changes using FortiManager CLI scripts are correct? (Choose two.)

A. When executed on the Device Database, you must use the installation wizard to apply the changes to the managed FortiGate.

B. When executed on the Policy Package, ADOM database, changes are applied directly to the managed FortiGate.

C. When executed on the All FortiGate in ADOM, changes are automatically installed without creating a new revision history.

D. When executed on the Remote FortiGate directly, administrators do not have the option to review the changes prior to installation.

Suggested Answer: *A, D*

habualrob Most Recent 4 years, 2 months ago
A and D
upvoted 1 times

ni 4 years, 3 months ago
A & D are correct.
upvoted 1 times

yadavarya97 4 years, 11 months ago
A & D are correct.
upvoted 1 times

Primo_SP 5 years ago
A and D correct
upvoted 1 times

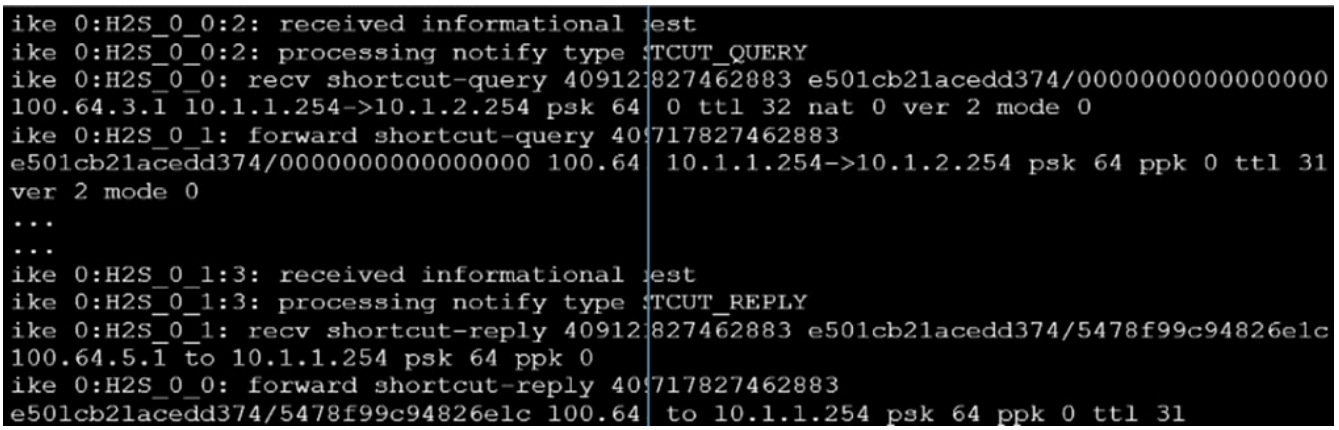
Triquix 5 years ago
A and D NSE7_EF_6.4 Pag 255
upvoted 1 times

MunzerR 5 years, 5 months ago
A and D
upvoted 1 times

Angel123 5 years, 7 months ago
Correct - A and D according NSE7_EF_6.2 Manual p.248
upvoted 4 times

Question #8 *Topic 1*

Refer to the exhibit, which contains a partial output of an IKE real-time debug.
Based on the debug output, which phase-1 setting is enabled in the configuration of this VPN?



A. auto-discovery-receiver

B. auto-discovery-forwarder

C. auto-discovery-sender

D. auto-discovery-shortcut

Suggested Answer: *C*

Angel123 Highly Voted 5 years, 7 months ago
Correct - C according NSE7_EF_6.2 Manual p.459 and p.460 auto-discovery-sender is enabled - a shortcut-query and shortcut-reply messages are passing through
upvoted 6 times

adolfunkz 5 years, 5 months ago
I'm unsure regarding C, could be A because on NSE7_EF_6.2 Manual p.463 it says "enable auto-discovery-receiver allows a device to receive SHORTCUT-OFFER" and I' seeing it on the image, but I'm going to try this on a lab
upvoted 1 times

Akiva 5 years, 4 months ago
For it to receive a short cut query it must have sent a short cut offer first, so C looks right
upvoted 4 times

znhl Most Recent 2 years, 11 months ago
Selected Answer: C
C Correct
upvoted 1 times

habualrob 4 years, 2 months ago
C is the correct
upvoted 1 times

ni 4 years, 3 months ago
C correct
upvoted 1 times

Null0 4 years, 10 months ago
C is correct. Quick hint: "forward" only in case of the hub can forward. spoke will be either initiator or responder or both but not forwarder.
upvoted 2 times

yadavarya97 4 years, 11 months ago
C is the correct answer.
upvoted 1 times

FortiSherlock 4 years, 11 months ago

receiver - configured on spokes to send and receive shortcuts forwarder - configured in multi-hub topology so that the 2nd hub can forward a shortcut offer to its connected spokes that were send by the 1st hub sender -configured on hubs that create the shortcut offers shortcut - does not exist

upvoted 1 times

Question #9 *Topic 1*

What is the diagnose test application ipsmonitor 99 command used for?

A. To enable IPS bypass mode

B. To provide information regarding IPS sessions

C. To disable the IPS engine

D. To restart all IPS engines and monitors

Suggested Answer: *D*

ni Most Recent 4 years, 3 months ago

Correct - D

upvoted 1 times

simobell 4 years, 12 months ago

D it's correct - You can see the NSE7_EF_6.4 Study Guide p.406

upvoted 2 times

Angel123 5 years, 7 months ago

Correct - D according NSE7_EF_6.2 Manual p.400

upvoted 4 times

Question #10 *Topic 1*

Refer to the exhibit, which contains a session table entry.
Which statement about FortiGate inspection of this session is true?

```
FGI # diagnose sys session  list
session info: proto=6 proto_state-11 duration-35 expire-265  timeout=300 flags=00000000
sockflag=00000000 sockport-0 av_idx=0 use-4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state-redir local may_dirty none app_ntf
statistic(bytes/packets/allow_err): org-3208/25/1 reply=11144/29/1 tuples-2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=7->6/ 6->7 gwy=172.20.12.2/10.0.0.2
hook=post dir=org act=snat 192.167.1.100:4954->216.58.216.238:443(172.20.121.96:49545)
hook=pre dir=reply act=dnat 216.58.216.238:443->172.20.121.96:49545
(192.167.1.100:49545)
pos/ (before, after) 0/(0,0), 0/(0,0)
src_mac-08:5b:0e:6c:7b:7a
misc=0 policy_id-21 auth_info=0 chk_client_info=0 vd=0
serial-007f2948 tos-ff/ff app_list=0 app-0 url_cat-41
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=00000000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=
0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
```

A. FortiGate applied proxy-based inspection.

B. FortiGate applied flow-based NGFW policy-based inspection.

C. FortiGate applied flow-based inspection.

D. FortiGate forwarded this session without any inspection.

Suggested Answer: *A*

ni Most Recent 4 years, 3 months ago
Correct - A
upvoted 1 times

Ahmed_Elswify 4 years, 11 months ago
Enterprise_Firewall_6.4_Study_Guide page#360
upvoted 1 times

Primo_SP 5 years ago
State - Redir - proxy-based. A correct
upvoted 2 times

Kevin_Howard 5 years, 3 months ago
A (NSE7_EF_6.4 Manual p.360)
upvoted 2 times

Angel123 5 years, 7 months ago
Correct - A according NSE7_EF_6.2 Manual p.353 - state=redir
upvoted 4 times

Question #11 *Topic 1*

Refer to the exhibit, which contains the output of a debug command.
Which two statements about the exhibit are true? (Choose two.)

```
FGT # get router info ospf interface port4
port4 is up, line protocol is up
  Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
  Process ID 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROther, Priority 1
  Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2
  Backup Designated Router (ID) 0.0.0.1, Interface Address 172.20.121.239
  Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Neighbor Count is 4, Adjacent neighbor count is 2
  Crypt Sequence Number is 411
  Hello received 106 sent 27, DD received 6 sent 3
  LS-Req received 2 sent 2, LS-Upd received 7 sent 17
  LS-Ack received 4 sent 3, Discarded 1
```

A. The local FortiGate OSPF router ID is 0.0.0.4.

B. The local FortiGate is the backup designated router.

C. In the network connected to port4, two OSPF routers are down.

D. Port4 is connected to the OSPF backbone area.

Suggested Answer: *A, D*

Angel123 Highly Voted 5 years, 7 months ago
Correct - A and D according NSE7_EF_6.2 Manual p.289

A. Router ID is 0.0.0.4 B. It is not backup designated router (state DROther) C. Only 2 out of 4 routers are adjecent, but the others are not down - just not adjacent D. Area for port4 is 0.0.0.0 (backbone area)
upvoted 8 times

ni Most Recent 4 years, 3 months ago
Correct - D,A
upvoted 1 times

Ahmed_Elswify 4 years, 11 months ago
Enterprise_Firewall_6.4_Study_Guide page#276
upvoted 1 times

Saleham 5 years, 2 months ago
OSPF routers on a broadcast network will elect a DR (designated router) and BDR (backup designated router) with which all non-designated routers (like this) will form an adjacency. That is why we see 2 adjacent neighbors.
upvoted 2 times

Question #12 *Topic 1*

Refer to the exhibit, which contains the output of diagnose sys session stat.
Which two statements about the output shown are correct? (Choose two.)

```
NGFW-1 # diagnose sys session stat
misc info:          session_count=591 setup_rate=0 exp_count clash=162
     memory_tension_drop=0 ephemeral=0/65536 removable=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
     166 in NONE state
     1 in ESTABLISHED state
     3 in SYN_SENT state
     2 in TIME_WAIT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_rev=00000000
fqdn_count=00000006
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0
```

A. No sessions have been deleted because of memory pages exhaustion.

B. There are 0 ephemeral sessions.

C. There are 168 TCP sessions waiting to complete the three-way handshake.

D. All the sessions in the session table are TCP sessions.

Suggested Answer: *A, B*

Angel123 Highly Voted 5 years, 7 months ago
Correct - A and B according NSE7_EF_6.2 Manual p.67

A. memory_tension_drop=0 B. ephemeral=0/65536 C. Usually ICMP sessions (they don't have ESTABLISHED, SYN_SENT and so on states) D. Total number of sessions: session_count=591; TCP: 166+1+3+2=172
upvoted 9 times

habualrob Most Recent 4 years, 2 months ago
A, B yes
upvoted 1 times

ni 4 years, 3 months ago
Correct - A and B
upvoted 1 times

Ahmed_Elswify 4 years, 11 months ago
Enterprise_Firewall_6.4_Study_Guide page#66,67
upvoted 4 times

Question #13 *Topic 1*

Refer to the exhibit, which contains central management configuration.
Which server will FortiGate choose for antivirus and IPS updates if 10.0.1.243 is experiencing an outage?

```
config system central-management
    set type fortimanager
    set fmg "10.0.1.242"
    config server-list
        edit 1
            set server-type rating
            set addr-type ipv4
            set server-address 10.0.1.240
        next
        edit 2
            set server-type update
            set addr-type ipv4
            set server-address 10.0.1.243
        next
        edit 3
            set server-type rating
            set addr-type ipv4
            set server-address 10.0.1.244
        next
    end
    set include-default-servers enable
end
```

A. 10.0.1.242

B. 10.0.1.244

C. Public FortiGuard servers

D. 10.0.1.240

Suggested Answer: *C*

Angel123 Highly Voted 5 years, 7 months ago
Correct - C according NSE7_EF_6.2 Manual p.186

By default include-default-servers is enabled. This allows FortiGate to communicate with the public FortiGuard servers, if the FortiManager devices (configured in server-list) are unavailable.
upvoted 7 times

FortiSherlock 4 years, 11 months ago
Additional info: The two other configured servers are set to "rating" and therefore only apply for web filtering and antispam, not for anti virus, what the question is looking for. 10.0.1.243 is the only configured anti virus server and if it fails the public servers are contacted.
upvoted 2 times

Traino12 Most Recent 4 years, 1 month ago
I VOTE FOR - C
upvoted 1 times

ni 4 years, 3 months ago
Correct - C
upvoted 1 times

armandolubaba 4 years, 6 months ago
C is correct answer
upvoted 1 times

Question #14 *Topic 1*

Refer to the exhibit, which contains the output of diagnose sys session list.
If the HA ID for the primary unit is zero (0), which statement about the output is true?

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty synced none app_ntf
statistic(bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=100.64.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:65464->54.192.15.182:80(100.64.1.1:65464)
hook=pre dir=reply act=dnat 54.192.15.182:80->100.64.1.1:65464(10.0.1.10:65464)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

A. This session cannot be synced with the slave unit.

B. The inspection of this session has been offloaded to the slave unit.

C. The master unit is processing this traffic.

D. This session is for HA heartbeat traffic.

Suggested Answer: *C*

Angel123 Highly Voted 5 years, 7 months ago
Correct - C according NSE7_EF_6.2 Manual p.221
upvoted 6 times

ni Most Recent 4 years, 3 months ago
Correct - C
upvoted 1 times

Kevin_Howard 5 years, 3 months ago
Since the Primary unit is 0, and ha_id=0, this means that the master is processing, 6.4 Guide p.227
upvoted 4 times

Question #15 *Topic 1*

Refer to the exhibit, which contains the partial output of an IKE real-time debug.
Why did the tunnel not come up?

```
ike 0:c49e59846861b0f6/0000000000000000:278: responder
message…
…
ike 0:c49e59846861b0f6/0000000000000000:278: incoming proposal:
ike 0:c49e59846861b0f6/0000000000000000:278: proposal id=0:
ike 0:c49e59846861b0f6/0000000000000000:278:      protocol id = IMAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278:         trans_id = KEY_IKE.
ike 0:c49e59846861b0f6/0000000000000000:278:         encapsulation = IKE/none
ike 0:c49e59846861b0f6/0000000000000000:278:             type=OAKLEY_ENCRYPT_ALG;
val=3DES_CBC.
ike 0:c49e59846861b0f6/0000000000000000:278:             type=OAKLEY_HASH_ALG,
val=SHA2_256
ike 0:c49e59846861b0f6/0000000000000000:278:            type=AUTH_METHOD,
val=PRESHARED_KEY
ike 0:c49e59846861b0f6/0000000000000000:278:           type=OAKLEY_GROUP,
val=MODP2048
ike 0:c49e59846861b0f6/0000000000000000:278:  ISAKMP SA lifetime=86400
…
ike 0:c49e59846861b0f6/0000000000000000:278: my proposal, gw VPN:
ike 0:c49e59846861b0f6/0000000000000000:278: proposal id =1;
ike 0:c49e59846861b0f6/0000000000000000:278:  protocol id = ISAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278:       trans_id = KEY_IKE.
ike 0:c49e59846861b0f6/0000000000000000:278:       encapsulation = IKE/none
ike 0:c49e59846861b0f6/0000000000000000:278:         type=OAKLEY_ENCRYPT_ALG,
val=AES_CBC, key-len=256
ike 0:c49e59846861b0f6/0000000000000000:278:         type=OAKLEY_HASH_ALG,
val=SHA2_256
ike 0:c49e59846861b0f6/0000000000000000:278:         type=AUTH_METHOD,
val=PRESHARED_KEY
ike 0:c49e59846861b0f6/0000000000000000:278:         type=OAKLEY_GROUP,
val=MODP2048.
ike 0:c49e59846861b0f6/0000000000000000:278: ISAKMP SA lifetime=86400
…
ike 0:c49e59846861b0f6/0000000000000000:278: negotiation failure
ike Negotiate ISAKMP SA Error: ike ike 0:c49e59846861b0f6/0000000000000000:278: no SA
proposal chosen
```

A. The pre-shared keys do not match

B. The remote gateway phase 1 configuration does not match the local gateway phase 1 configuration.

C. The remote gateway phase 2 configuration does not match the local gateway phase 2 configuration.

D. The remote gateway is using aggressive mode and the local gateway is configured to use main mode.

Suggested Answer: *B*

Angel123 Highly Voted 5 years, 7 months ago
Correct - B, according NSE7_EF_6.2 Manual p.431

its a phase1 communication - ike remote OAKLEY_ENCRYPT_ALG: 3DES_CBC local OAKLEY_ENCRYPT_ALG: AES_CBC, key-len:256
upvoted 8 times

ni Most Recent 4 years, 3 months ago
Correct - B
upvoted 1 times

yadavarya97 4 years, 11 months ago
B is correct. 3 Des is not there on the local.
upvoted 2 times

mai340 5 years, 2 months ago

Val=Preshared_Key claim this message is on phase1, so B it´s correct

upvoted 1 times

Question #16 *Topic 1*

An administrator has configured two FortiGate devices for an HA cluster. While testing the HA failover, the administrator notices that some of the switches in the network continue to send traffic to the former primary unit. The administrator decides to enable the setting link-failed-signal to fix the problem.
Which statement about this command is true?

A. It forces the former primary device to shut down all its non-heartbeat interfaces for one second while the failover occurs.

B. It disables all the non-heartbeat interfaces in all the HA members for two seconds after a failover.

C. It sends a link failed signal to all connected devices.

D. It sends an ARP packet to all connected devices, indicating that the HA virtual MAC address is reachable through a new master after a failover.

Suggested Answer: *A*

ni Most Recent 4 years, 3 months ago
A is correct
upvoted 1 times

armandolubaba 4 years, 6 months ago
A is correct
upvoted 1 times

yadavarya97 4 years, 11 months ago
A is correct.
upvoted 1 times

Ahmed_Elswify 4 years, 11 months ago
Enterprise_Firewall_6.4_Study_Guide page#208
upvoted 2 times

mai340 5 years, 1 month ago
A it´s correct
upvoted 1 times

Angel123 5 years, 7 months ago
Correct - A, according NSE7_EF_6.2 Manual p.207
upvoted 4 times

Question #17 *Topic 1*

What does the dirty flag mean in a FortiGate session?

A. The session must be removed from the former primary unit after an HA failover.

B. Traffic has been blocked by the antivirus inspection.

C. Traffic has been identified as from an application that is not allowed.

D. The next packet must be re-evaluated against the firewall policies.

Suggested Answer: *D*

Angel123 Highly Voted 5 years, 7 months ago
Correct - D according NSE7_EF_6.2 Manual 444
upvoted 7 times

Angel123 5 years, 7 months ago
Correction: NSE7_EF_6.2 Manual p.98; FortiGate_Security_6.2_Study_Guide p.444
upvoted 4 times

Traino12 Most Recent 4 years, 1 month ago
D IS CORRECT
upvoted 1 times

ni 4 years, 3 months ago
Correct - D
upvoted 1 times

yadavarya97 4 years, 11 months ago
D is correct.
upvoted 1 times

Ahmed_Elswify 4 years, 11 months ago
Enterprise_Firewall_6.4_Study_Guide page#97
upvoted 1 times

Question #18 *Topic 1*

Refer to the exhibit, which contains partial outputs from two routing debug commands.
Which outbound interface will FortiGate use to route web traffic from internal users to the Internet?

```
FortiGate # get router info kernel
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0-> 0.0.0.0/0 pref=
0.0.0.0 gwy=100.64.1.254 dev=3(port1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=10 0.0.0.0/0.0.0.0/0-> 0.0.0.0/0 pref=
0.0.0.0 gwy=100.64.2.254 dev=6(port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0-> 10.1.0.0/24 pref=
10.1.0.254 gwy=0.0.0.0 dev=9(port3)

FortiGate # get router info routing-table all

S*   0.0.0.0/0 [10/0] via 100.64.1.254, port1
              [10/0] via 100.64.2.254, port2, [10/0]
C    10.1.0.0/24 is directly connected, port3
S    10.1.10.0/24 [10/0] via 10.1.0.1, port3
C    100.64.1.0/24 is directly connected, port1
C    100.64.2.0/24 is directly connected, port2
```

A. port3

B. port2

C. port1

D. Both port1 and port2

Suggested Answer: *C*

Angel123 Highly Voted 5 years, 7 months ago
Correct - C according NSE7_EF_6.2 Manual p.134
upvoted 6 times

MunzerR 5 years, 5 months ago
I agree with C ... (Priority is 0) and port 2 priority is 10
upvoted 3 times

Traino12 Most Recent 4 years, 1 month ago
Port 1 - C is correct
upvoted 1 times

ni 4 years, 3 months ago
Correct - C
upvoted 1 times

Ahmed_Elswify 4 years, 11 months ago
Enterprise_Firewall_6.4_Study_Guide page#154-156
upvoted 2 times

mai340 5 years, 2 months ago
10.64.2.254 has [10/0] at the end line which is an metric route from any routing protocol and no priority as long as metric 10 is worst to priority 0 (line up) so C it´s the correct
upvoted 2 times

Saleham 5 years, 2 months ago
C is connect https://kb.fortinet.com/kb/viewContent.do?externalId=FD32103
upvoted 2 times

Question #19 *Topic 1*

Refer to the exhibit, which contains the output of a debug command.
Which statement about this FortiGate is correct?

```
# diagnose hardware sysinfo conserve
memory conserve mode:                on
total RAM:                           3040 MB
memory used:                         2706 MB 89% of total RAM
Memory freeable:                      334 MB 11% of total RAM
memory used + freeable threshold extreme: 2887 MB 95% of total RAM
memory used threshold red:           2675 MB 88% of total RAM
memory used threshold green:         2492 MB 82% of total RAM
```

A. It is currently in system conserve mode because of high CPU usage.

B. It is currently in extreme conserve mode because of high memory usage.

C. It is currently in proxy conserve mode because of high memory usage.

D. It is currently in memory conserve mode because of high memory usage.

Suggested Answer: *D*

Angel123 Highly Voted 5 years, 7 months ago
Correct - D according NSE7_EF_6.2 Manual p.61
upvoted 6 times

ni Most Recent 4 years, 3 months ago
Correct - D
upvoted 1 times

armandolubaba 4 years, 6 months ago
D is correct
upvoted 1 times

DatBroNZ 4 years, 6 months ago
Correct - D NSE7_EF_6.4 Manual p.65
upvoted 1 times

yadavarya97 4 years, 11 months ago
D is correct.
upvoted 1 times

mai340 5 years, 1 month ago
D it´s correct
upvoted 1 times