Fortinet

NSE7_EFW-7.0 Exam

Fortinet NSE 7 - Enterprise Firewall 7.0

Version: 5.0

Question: 1

Refer to the exhibit, which contains partial output from an IKE real-time debug.

```
ike 0:624000:98: responder: main mode get 1st message...
ike 0:624000:98: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:624000:98: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:624000:98: incoming proposal:
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:    protocol id = ISAKMP:
ike 0:624000:98:       trans_id = KEY_IKE.
ike 0:624000:98:       encapsulation = IKE/none
ike 0:624000:98:          type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:          type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:          type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:          type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:    protocol id = ISAKMP:
ike 0:624000:98:       trans_id = KEY_IKE.
ike 0:624000:98:       encapsulation = IKE/none
ike 0:624000:98:          type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:          type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:          type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:          type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: my proposal, gw Remotesite:
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:    protocol id = ISAKMP:
ike 0:624000:98:       trans_id = KEY_IKE.
ike 0:624000:98:       encapsulation = IKE/none
iike 0:620000:98:          type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:          type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:          type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:          type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:    protocol id = ISAKMP:
ike 0:624000:98:       trans_id = KEY_IKE.
ike 0:624000:98:       encapsulation = IKE/none
ike 0:624000:98:          type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:          type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:          type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:          type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: negotiation failure
ike Negot:624ea7b1bba276fb/0000000000000000:98: no SA proposal chosen
```

The administrator does not have access to the remote gateway.
Based on the debug output, which configuration change can the administrator make to the local

gateway to resolve the phase 1 negotiation error?

A. In the phase 1 network configuration, set the IKE version to 2.
B. In the phase 1 proposal configuration, add AES128-SHA128 to the list of encryption algorithms.
C. In the phase 1 proposal configuration, add AESCBC-SHA2 to the list of encryption algorithms.
D. In the phase 1 proposal configuration, add AES256-SHA256 to the list of encryption algorithms.

Answer: D

Explanation:

https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/238852

Question: 2

Refer to the exhibit, which shows the output of a web filtering diagnose command.

```
# diagnose webfilter fortiguard statistics list        # diagnose webfilter fortiguard statistics list
                                                        ...

Rating Statistics:                                      Cache Statistics:
======================                                  ======================
DNS failures                    :       273             Maximum memory              :           0
DNS lookups                     :       280             Memory usage                :           0
Data send failures              :         0
Data read failures              :         0             Nodes                       :           0
Wrong package type              :         0               Leaves                    :           0
Hash table miss                 :         0               Prefix nodes              :           0
Unknown server                  :         0               Exact nodes               :           0
Incorrect CRC                   :         0
Proxy request failures          :         0             Requests                    :           0
Request timeout                 :         1             Misses                      :           0
Total requests                  :      2409             Hits                        :           0
Requests to FortiGuard servers  :      1182               Prefix hits               :           0
Server errored responses        :         0               Exact hits                :           0
Relayed rating                  :         0
Invalid profile                 :         0             No cache directives         :           0
                                                        Add after prefix            :           0
Allowed                         :      1021             Invalid DB put              :           0
Blocked                         :      3909             DB updates                  :           0
Logged                          :      3927
Blocked Errors                  :       565             Percent full                :          0%
Allowed Errors                  :         0               Branches                  :          0%
Monitors                        :         0               Leaves                    :          0%
Authenticates                   :         0               Prefix nodes              :          0%
Warnings:                       :        18               Exact nodes               :          0%
Ovrd request timeout            :         0
Ovrd send failures              :         0             Miss rate                   :          0%
Ovrd read failures              :         0             Hit rate                    :          0%
Ovrd errored responses          :         0               Prefix hits               :          0%
...                                                       Exact hits                :          0%
```

Which configuration change would result in non-zero results in the cache statistics section?

A. set server-type rating under config system central-management
B. set webfilter-cache enable under config system fortiguard
C. set webfilter-force-off disable under config system fortiguard
D. set ngfw-mode policy-based under config system settings

Answer: B

Explanation:

Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 362

Question: 3

Refer to the exhibits, which show the configuration on FortiGate and partial session information for internet traffic from a user on the internal network.


```
Configuration | 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
```

```
Configuration | Session

FGT # 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:
```

If the priority on route ID 2 were changed from 10 to 0, what would happen to traffic matching that user session?

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 egress from port2.
C. The session would be deleted, and the client would need to start a new session.
D. The session would remain in the session table, and its traffic would egress from port1.

Answer: D

Explanation:

https://community.fortinet.com/t5/FortiGate/Technical-Tip-Using-SNAT-route-change-to-update-existing-NAT/ta-p/198439

Question: 4

Refer to the exhibits, which show the configuration on FortiGate and partial internet session information from a user on the internal network.

Configuration 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
```

Configuration Session

```
FGT # 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:
```

An administrator would like to test session failover between the two service provider connections.
What changes must the administrator make to force this existing session to immediately start using
the other interface? (Choose two.)

A. Configure set snat-route-change enable.
B. Change the priority of the port2 static route to 5.
C. Change the priority of the port1 static route to 11.
D. unset snat-route-change to return it to the default setting.

Answer: AC

Explanation:

Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 148-149

Question: 5

What are two functions of automation stitches? (Choose two.)

A. Automation stitches can be configured on any FortiGate device in a Security Fabric environment.
B. An automation stitch configured to execute actions sequentially can take parameters from previous actions as input for the current action.
C. Automation stitches can be created to run diagnostic commands and attach the results to an email message when CPU or memory usage exceeds specified thresholds.
D. An automation stitch configured to execute actions in parallel can be set to insert a specific delay between actions.

Answer: BC

Explanation:

Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 23, 26

Thank You for trying NSE7_EFW-7.0 PDF Demo

To try our NSE7_EFW-7.0 practice exam software visit link below

https://www. braindumpscollection.com/NSE7_EFW-7.0.html

Start Your NSE7_EFW-7.0 Preparation

Use Coupon "20OFF" for extra 20% discount on the purchase of Practice Test Software. Test your NSE7_EFW-7.0 preparation with actual exam questions.