Free Questions for NSE7_NST-7.2 by dumpssheet

Shared by Schwartz on 03-06-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- You can configure automation stitches on any FortiGate device in a Security Fabric environment.

B- You can create automation stitches to run diagnostic commands and attach the results to an email message when CPU or memory usage exceeds specified thresholds.

C- An automation stitch configured to execute actions sequentially can take parameters from previous actions as input for the current action.

D- You can set an automation stitch configured to execute actions in parallel to insert a specific delay between actions.

Answer:

B, C

Explanation:

Automation Stitches Overview:

Automation stitches in FortiOS allow administrators to automate responses to specific events, such as running diagnostic commands or taking corrective actions when certain thresholds are exceeded.

Diagnostic Commands and Alerts:

Automation stitches can be configured to run diagnostic commands and attach the results to email alerts. This is useful for monitoring and troubleshooting purposes, particularly when CPU or memory usage exceeds set thresholds.

Sequential Execution with Parameters:

When actions are executed sequentially, each action can take parameters from the previous action as input. This enables more complex workflows and automation sequences where the output of one action influences the next.

Fortinet Documentation: Configuring and using automation stitches (Welcome to the Fortinet Community!) (Hammertux).

Fortinet Community: Automation stitches and their applications in FortiOS (Hammertux) (Fortinet GURU).

Question 2

Question Type: MultipleChoice

Refer to the exhibit, which shows the output of diagnose sys session stat. Which statement about the output shown in the exhibit is correct?

Options:

A- All the sessions in the session table are TCP sessions.

B- 162 sessions have been deleted because of memory page exhaustion.

C- There are 166 TCP sessions waiting to complete the three-way handshake.

D- There are two sessions that have not been removed in case of any out-of-order packets that arrive.

Answer:

C

Explanation:

Session Table Overview:

The session table in FortiOS tracks all active and pending sessions. It includes details like the type of session (TCP, UDP, etc.), status, and statistics.

Interpreting the Exhibit:

The exhibit from the diagnose sys session stat command shows detailed session statistics.

The specific value indicating '166 TCP sessions waiting to complete the three-way handshake' reflects the number of sessions that have initiated but not yet completed the TCP three-way handshake process (SYN, SYN-ACK, ACK).

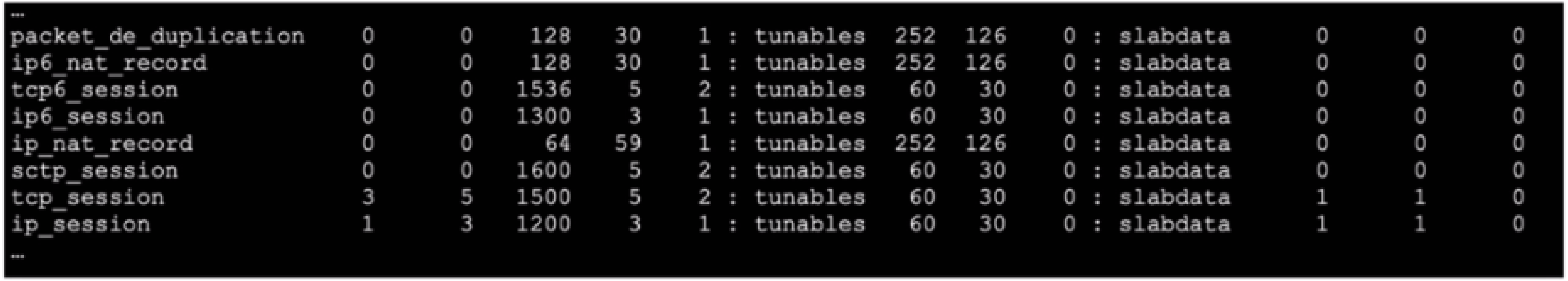
Fortinet Documentation: Understanding and troubleshooting session tables (Hammertux).

Fortinet Community: Explanation of session states and statistics (Welcome to the Fortinet Community!) (Hammertux).

Question 3

Question Type: **MultipleChoice**

Refer to the exhibit, which shows the omitted output of FortiOS kernel slabs.



```
...
packet_de_duplication    0      0    128   30     1 : tunables  252  126     0 : slabdata      0      0      0
ip6_nat_record           0      0    128   30     1 : tunables  252  126     0 : slabdata      0      0      0
tcp6_session             0      0   1536    5     2 : tunables   60   30     0 : slabdata      0      0      0
ip6_session              0      0   1300    3     1 : tunables   60   30     0 : slabdata      0      0      0
ip_nat_record            0      0     64   59     1 : tunables  252  126     0 : slabdata      0      0      0
sctp_session             0      0   1600    5     2 : tunables   60   30     0 : slabdata      0      0      0
tcp_session              3      5   1500    5     2 : tunables   60   30     0 : slabdata      1      1      0
ip_session               1      3   1200    3     1 : tunables   60   30     0 : slabdata      1      1      0
...
```

Which statement is true?

Options:

A- The total slab size of the tcp_sessior. slab Is 7500 kB and is associated with the kernel.

B- The total slab size of the ip6_session slab is 1300 kB and is associated with the kernel.

C- The total slab size of the sctp_session slab is 0 kB and is associated with the user space

D- The total slab size of the ip_session slab is 3600 kB and is associated with the user space.

Answer:

B

Explanation:

Kernel Slabs Overview:

The slab allocator in the Linux kernel is used for efficient memory management. It groups objects of the same type into caches, which are divided into slabs.

Each slab contains multiple objects and helps to minimize fragmentation and enhance memory allocation efficiency.

Interpreting the Exhibit:

The exhibit shows output related to various kernel slab caches.

The line for ip6_session indicates that there are 1300 kB allocated for this slab, which means the total memory size allocated for IPv6 session objects in the kernel is 1300 kB.

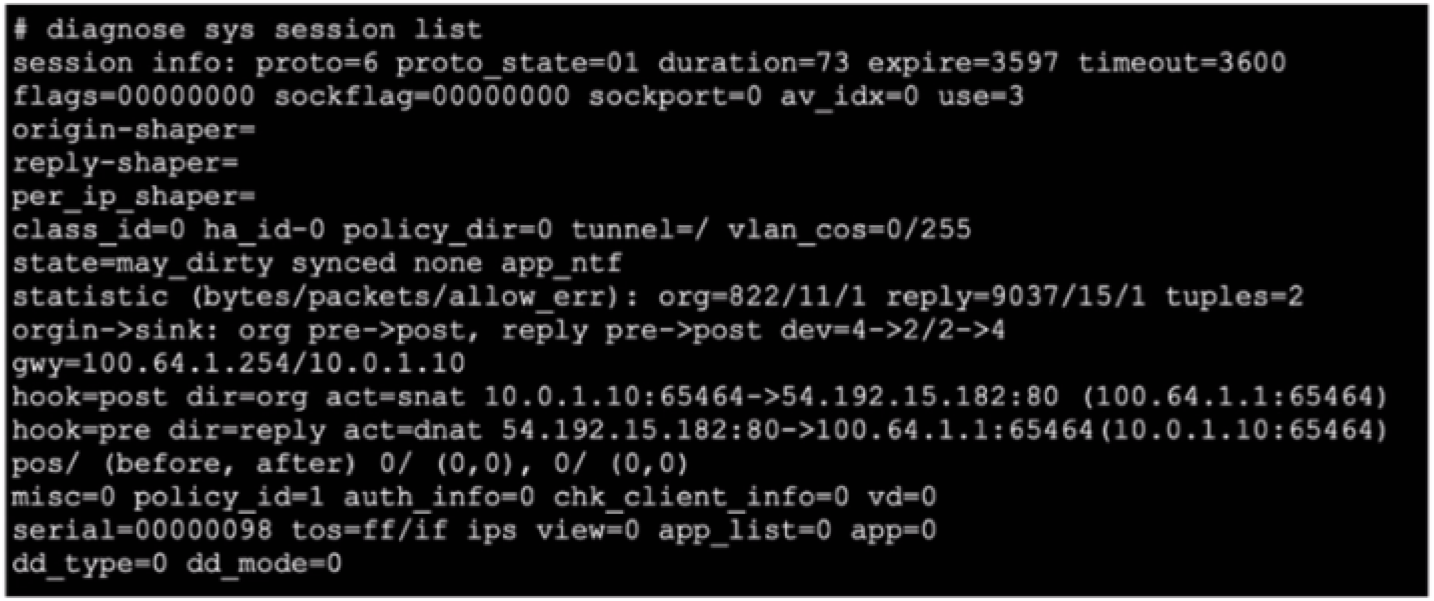
Fortinet Community: Explanation of kernel slab allocation and usage (Welcome to the Fortinet Community!) (Hammertux).

Linux Kernel Documentation: Slab Allocator details (Hammertux).

Question 4

Question Type: MultipleChoice

Exhibit.



```
# 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/if ips view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

Refer to the exhibit, which shows the output of diagnose sys session list.

If the HA ID for the primary device is 0. what happens if the primary fails and the secondary becomes the primary?

Options:

A- The session will be removed from the session table of the secondary device because of the presence of allowed error packets, which will force the client to restart the session with the server.

B- The session state is preserved but the kernel will need to re-evaluate the session because NAT was applied.

C- Traffic for this session continues to be permitted on the new primary device after failover. without requiring the client to restart the session with the server.

D- The secondary device has this session synchronized; however, because application control is applied, the session is marked dirty and has to be re-evaluated after failover.

Answer:

C

Explanation:

Session Synchronization:

FortiGate HA (High Availability) ensures that active sessions are synchronized between the primary and secondary devices. This synchronization allows for seamless failover and continuity of sessions.

Handling NAT Sessions:

The session in the exhibit has NAT applied, as indicated by the hook=post dir=org act=snat entry. FortiGate's HA setup is designed to handle such sessions, ensuring that traffic continues without interruption during failover.

Session Preservation:

Even with the presence of NAT, the session state is preserved across the HA devices. This means that ongoing sessions do not require re-establishment by the client, thus providing a seamless experience.

Fortinet Documentation: HA session synchronization and failover

Fortinet Community: Understanding session synchronization in FortiGate HA

Question 5

Question Type: MultipleChoice

There are four exchanges during IKEv2 negotiation.

Which sequence is correct?

Options:

A- IKE_Proposal, ID_Auth, PiggyBack_CHILD and Informational

B- lnit_Req, Wait_lnit_Req, ID_Auth_Req and Create_CHILD_SA

C- INIT_Re, INIT_Auth, ID_Child and SET_Nonce

D- IKE_SAJNIT, IKE_Auth, Create_CHILD_SA and Informational

Answer:

D

Explanation:

IKE_SA_INIT:

This is the first exchange in IKEv2. It establishes a secure, authenticated channel between peers and negotiates cryptographic algorithms and keys.

IKE_Auth:

The second exchange authenticates the IKE SA (Security Association) using the previously negotiated keys and algorithms. This exchange also establishes the first IPsec SA.

Create_CHILD_SA:

This exchange creates additional IPsec SAs after the initial authentication. It can also be used to rekey existing IPsec SAs to maintain security.

Informational:

This is a generic exchange used for various purposes such as error notification, deletion of SAs, and other control messages.

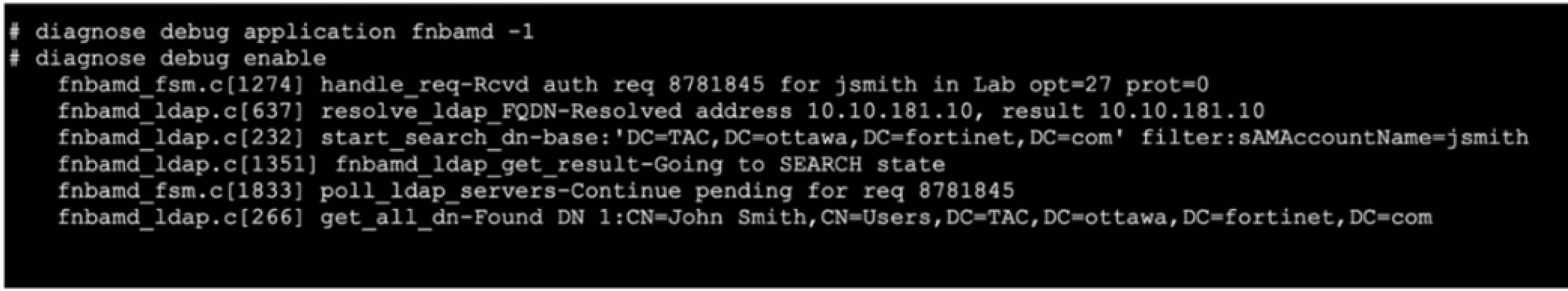
Fortinet Community: IKEv2 packet exchanges and troubleshooting

Fortinet Documentation: IPsec VPN Concepts

Question 6

Question Type: **MultipleChoice**

Refer to the exhibit, which shows a truncated output of a real-time LDAP debug.



```
# diagnose debug application fnbamd -1
# diagnose debug enable
   fnbamd_fsm.c[1274] handle_req-Rcvd auth req 8781845 for jsmith in Lab opt=27 prot=0
   fnbamd_ldap.c[637] resolve_ldap_FQDN-Resolved address 10.10.181.10, result 10.10.181.10
   fnbamd_ldap.c[232] start_search_dn-base:'DC=TAC,DC=ottawa,DC=fortinet,DC=com' filter:sAMAccountName=jsmith
   fnbamd_ldap.c[1351] fnbamd_ldap_get_result-Going to SEARCH state
   fnbamd_fsm.c[1833] poll_ldap_servers-Continue pending for req 8781845
   fnbamd_ldap.c[266] get_all_dn-Found DN 1:CN=John Smith,CN=Users,DC=TAC,DC=ottawa,DC=fortinet,DC=com
```

What two conclusions can you draw from the output? (Choose two.)

Options:

A- The name of the configured LDAP server is Lab.

B- The user is authenticating using CN=John Smith.

C- FortiOS is able to locate the user in step 3 (Bind Request) of the LDAP authentication process.

D- FortiOS is performing the second step (Search Request) in the LDAP authentication process.

Answer:

C, D

Explanation:

LDAP Authentication Process:

LDAP (Lightweight Directory Access Protocol) authentication involves several steps: Bind Request, Search Request, and Bind Response.

The Bind Request is used to authenticate the client to the LDAP server.

The Search Request is used to find the directory entry that matches the provided criteria.

Analyzing the Exhibit:

The exhibit shows a real-time LDAP debug output.

The debug log includes a successful resolution of the LDAP FQDN, indicating that the LDAP server was reached.

The debug log also shows the start of a search using the distinguished name (DN) base and a filter to locate the user jsmith.

Conclusion:

Since FortiOS successfully resolved the LDAP server and initiated a search for the user jsmith, it indicates that the LDAP server was located, and the search request was performed.

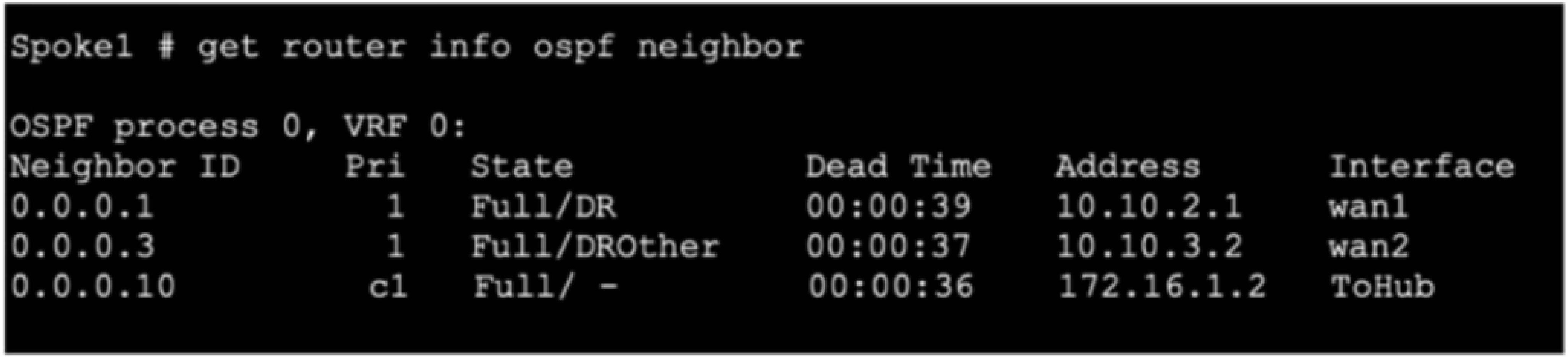
Fortinet Community: Understanding LDAP authentication steps and troubleshooting (Fortinet Docs).

Fortinet Documentation: LDAP integration and debugging in FortiOS (Welcome to the Fortinet Community!).

Question 7

Question Type: **MultipleChoice**

Refer to the exhibit, which shows the output of get router info ospf neighbor.



```
Spoke1 # get router info ospf neighbor

OSPF process 0, VRF 0:
Neighbor ID      Pri   State           Dead Time   Address       Interface
0.0.0.1            1   Full/DR         00:00:39    10.10.2.1     wan1
0.0.0.3            1   Full/DROther    00:00:37    10.10.3.2     wan2
0.0.0.10          c1   Full/ -         00:00:36    172.16.1.2    ToHub
```

What can you conclude from the command output?

Options:

A- The local FortiGate Is not a DROther.

B- All neighbors are in area 0.0.0.0.

C- The local FortiGate is the BDR.

D- The network type connecting the local Fortigate and OSPF neighbor 0.0.0.10 is point-to-point.

Answer:

A

Explanation:

Understanding OSPF Roles:

In OSPF (Open Shortest Path First), routers can have different roles: Designated Router (DR), Backup Designated Router (BDR), and DROther. These roles help manage and optimize the OSPF network traffic.

DR and BDR are elected to minimize the number of adjacencies and reduce the amount of routing information exchange.

DROther routers are neither DR nor BDR but can still participate in the OSPF network by maintaining adjacencies with DR and BDR.

Analyzing the Exhibit:

The exhibit shows the OSPF neighbor states for the local FortiGate.

Neighbor ID 0.0.0.1 is in the state Full/DR (Designated Router).

Neighbor ID 0.0.0.3 is in the state Full/DROther (DROther).

Neighbor ID 0.0.0.10 has no specific designation, implying it is neither DR nor BDR.

Conclusion:

Since the local FortiGate shows neighbors in Full/DR and Full/DROther states and itself does not have a state of DROther, it can be concluded that the local FortiGate is not a DROther.

Fortinet Community: Understanding OSPF roles and states (Welcome to the Fortinet Community!) (cyruslab).

Fortinet Documentation: OSPF neighbor states and elections (Fortinet Docs).

Question 8

Question Type: MultipleChoice

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

What can you conclude from the RTT value?

Options:

A- Its value represents the time it takes to receive a response after a rating request is sent to a particular server.

B- Its value is incremented with each packet lost.

C- It determines which FortiGuard server is used for license validation.

D- Its initial value is statically set to 10.

Answer:

A

Explanation:

RTT (Round Trip Time):

RTT in the context of the FortiGuard server list indicates the time it takes for a request to be sent to a FortiGuard server and for a response to be received.

This metric helps determine the latency between the FortiGate device and the FortiGuard servers, which is crucial for ensuring efficient and quick updates and responses for services like web filtering and antivirus updates.

Server Selection:

The FortiGate device uses RTT values to prioritize servers. Servers with lower RTT values are preferred as they respond faster, ensuring minimal delay in processing requests.

This improves the overall performance of FortiGuard services by reducing the time it takes to communicate with the servers.

Fortinet Community: Troubleshooting FortiGuard server connections and RTT values (Welcome to the Fortinet Community!) (Fortinet Docs).

Fortinet Documentation: FortiGuard server settings and RTT explanation (Welcome to the Fortinet Community!) (Fortinet Docs).

Question 9

Question Type: **MultipleChoice**

Which two statements about conserve mode are true? (Choose two.)

Options:

A- FortiGate starts dropping all new sessions when the system memory reaches the configured red threshold.

B- FortiGate starts taking the configured action for new sessions requiring content inspection when the system memory reaches the configured red threshold.

C- FortiGate enters conserve mode when the system memory reaches the configured extreme threshold.

D- FortiGate exits conserve mode when the system memory goes below the configured green threshold

Answer:

A, D

Explanation:

Conserve Mode Activation:

FortiGate enters conserve mode to prevent system crashes when the memory usage reaches critical levels. The 'red threshold' is the point at which FortiGate starts dropping new sessions to conserve memory.

When the system memory usage exceeds this threshold, the FortiGate will block new sessions that require significant memory resources, such as those needing content inspection.

Exiting Conserve Mode:

The 'green threshold' is the memory usage level below which FortiGate exits conserve mode and resumes normal operation.

Once the system memory usage drops below this threshold, FortiGate will start allowing new sessions again.

Fortinet Community: Understanding conserve mode and its thresholds (Welcome to the Fortinet Community!) (Welcome to the Fortinet Community!).

Fortinet Documentation: Memory conserve mode and thresholds (Welcome to the Fortinet Community!) (Fortinet GURU).