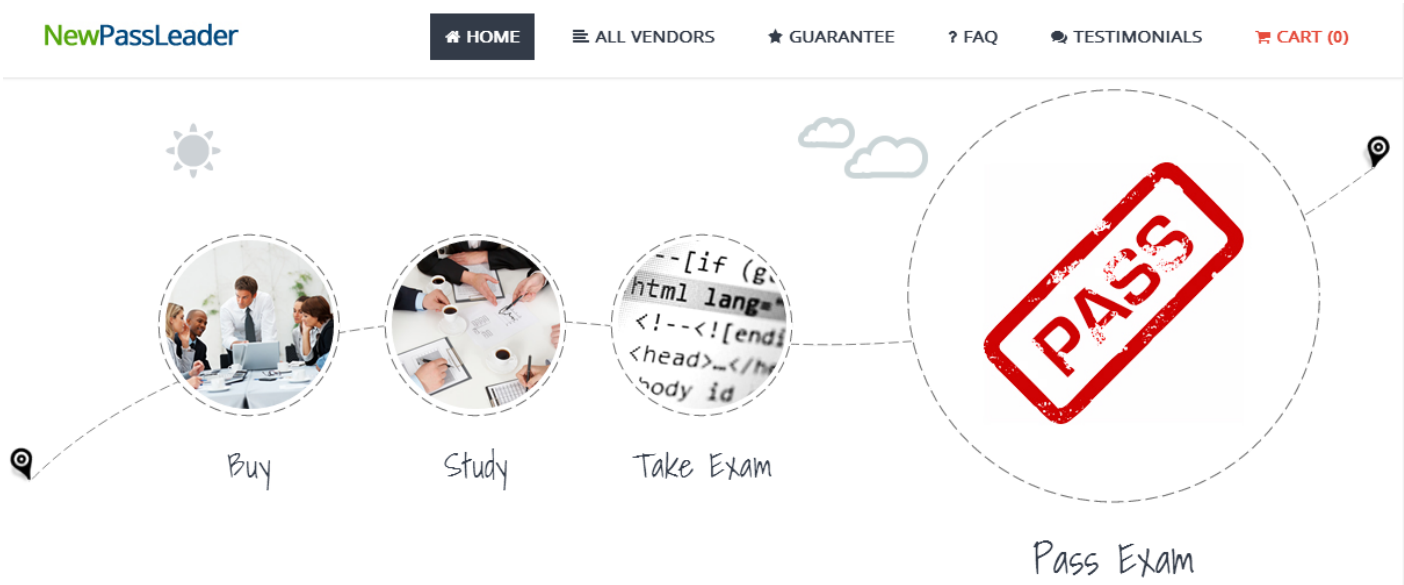
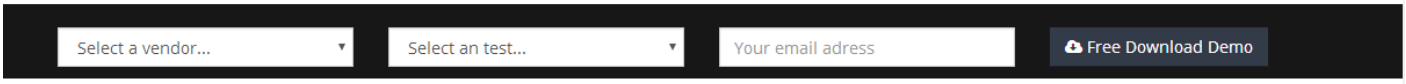
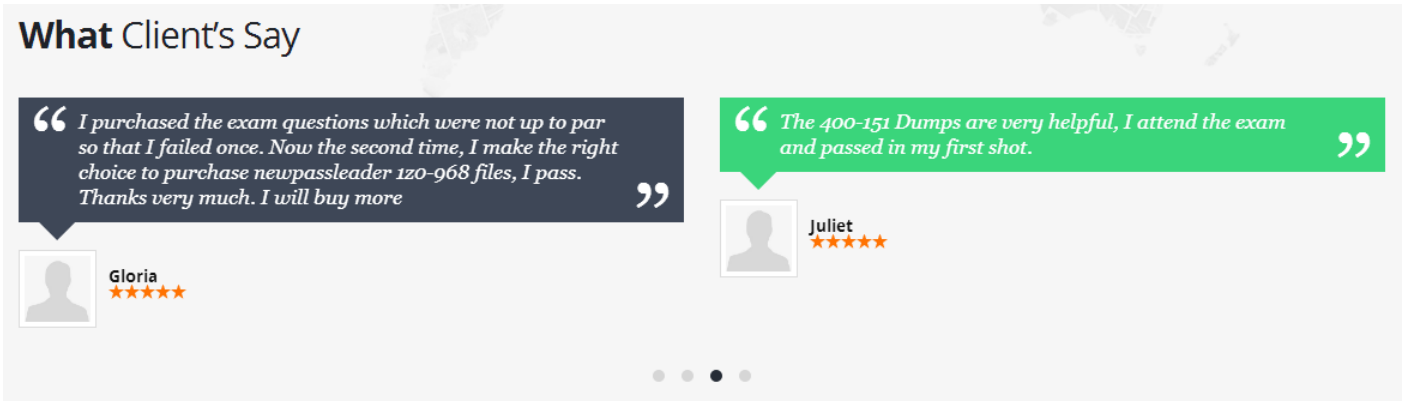
NewPassleader





Try **PDF Demo** before you buy

Online Test Engine: Online Tool, Convenient, easy to study. Instant Online Access. Supports All Web Browsers.
PDF format: Easy to read and print learning materials, our products are available in PDF file format.
Desktop Test Engine: Installable Software Application. Simulates Real Exam Environment. Practice Offline Anytime.



http://www.newpassleader.com/

Attentive Service Exam Torrent and Valid Dumps - NewPassLeader

Exam : **NSE7_EFW-6.0-JPN**

Title : Fortinet NSE 7 - Enterprise Firewall 6.0

Vendor : Fortinet

Version : DEMO

QUESTION NO: 1
IKEリアルタイムデバッグの部分的な出力を含む展示を表示して、以下の質問に答えてください。

```
ike 0:H2S_0_1: shortcut 10.200.5.1.:0   10.1.2.254->10.1.1.254
…
ike 0:H2S_0_1:15:  sent IKE msg (SHORTCUT-OFFER):  10.200.1.1:500->10.200.5.1:500,
len=164, id=4134df8580d5cdd/ce54851612c7432f:a21f14fe
ike 0: comes 10.200.5.1:500->10.200.1.1:500,ifindex=3….
ike 0: IKEv1 exchange=Informational id=4134df8580d5bcdd/ce54851612c7432f:6266ee8c
len=196

ike 0:H2S_0_1:15: notify msg received: SHORTCUR-QUERY
ike 0:H2S_0_1: recv shortcut-query 16462343159772385317

ike 0:H2S_0_0:16:  senr IKE msg (SHORTCUT-QUERY): 10.200.1.1:500->10.200.3.1:500,
len=196, id=7c6b6cca6700a935/dba061eaf51b89f7:b326df2a
ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=3….
ike 0: IKEv1 exchange=Informational id=7c6b6cca6700a935/dba061eaf51b89f7:1c1dbf39
len=188

ike 0:H2S_0_0:16: notify msg received: SHORTCUT-REPLY
ike 0:H2S_0_0: recv shortcut-reply 16462343159772385317
f97a7565a441e2aa/667d3e2e3442211e 10.200.3.1 to 10.1.2.254 psk 64
ike 0:H2S_0_0: shortcut-reply route to 10.1.2.254 via H2S_0_1 29
ike 0:H2S: forward shortcut-reply 16462343159772385317
f97a7565a441e2aa/667d3e2e3442211e 10.200.3.1 to 10.1.2.254 psk 64 ttl 31
ike 0:H2S_0_1:15: enc
…
ike 0:H2S_0_1:15: sent IKE msg (SHORTCUT-REPLY): 10.200.1.1:500->10.200.5.1:500,
len=188, id=4134df8580d5bcdd/ce54851612c7432f:70ed6d2c
```

デバッグ出力に基づいて、このフェーズ1の設定はこのVPNの構成で有効になっていますか？
A. auto-discovery-sender
B. auto-discovery-forwarder
C. auto-discovery-shortcut
D. auto-discovery-receiver
Answer: D

QUESTION NO: 2
管理者が、2つのメンバーを持つHAクラスターでHAセッション同期を有効にしました。プライマリユニットのセッションに追加され、セカンダリユニットと同期されたことを示すフラグはどれですか？
A. redir.

B. dirty.
C. synced
D. nds.
Answer: C
Explanation
The synced sessions have the 'synced' flag. The command 'diag sys session list' can be used to see the sessions on the member, with the associated flags.

QUESTION NO: 3
診断コマンドの出力を含む展示を表示して、以下の質問に答えてください。

```
     diagnose sys session list expectation

session info: proto=6 proto_state-00 duration=3 expire=26 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
ha_id-0 policy_dir=1 tunnel=/
state=new complex
statistic(bytes/packets/allow_err): org=0/0/0 reply-0/0/0 tuples=2
orgin->sink: org pre->post, reply pre->post dev=2->4/4->2 gwy=10.0.1.10/10.200.1.254
hook=pre dir-org act=dnat 10.171.121.38:0->10.200.1.1:60426(10.0.1.10:50365)
hook-pre dir-org act-noop 0.0.0.0:0->0.0.0.0:0(0.0.0.0:0)
pos/(before, after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=000000e9 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

出力に関して正しい記述は何ですか？（2つ選択してください。）
A.これは、セッションヘルパーによって作成される予定のセッションです。
B.元の方向のトラフィック（IPアドレス10.171.122.38から来る）は、ネクストホップIPアドレス10.0.1.10にルーティングされます。
C.元の方向のトラフィック（IPアドレス10.171.122.38から来る）は、ネクストホップIPアドレス10.200.1.1にルーティングされます。
D.これは、アプリケーション制御プロファイルによって作成される予定のセッションです。
Answer: A C

QUESTION NO: 4
展示に表示される「ips anomaly
listの診断」コマンドの出力を調べます。以下の質問に答えてください。

```
# diagnose ips anomaly list

list nids meter:
id=ip_dst_session      ip=192.168.1.10    dos_id=2  exp=3646  pps=0  freq=0
id=udp_dst_session     ip=192.168.1.10    dos_id=2  exp=3646  pps=0  freq=0
id=udp_scan            ip=192.168.1.110   dos_id=1  exp=649   pps=0  freq=0
id=udp_flood           ip=192.168.1.110   dos_id=2  exp=653   pps=0  freq=0
id=tcp_src_session     ip=192.168.1.110   dos_id=1  exp=5175  pps=0  freq=8
id=tcp_port_scan       ip=192.168.1.110   dos_id=1  exp=175   pps=0  freq=0
id=ip_src_session      ip=192.168.1.110   dos_id=1  exp=5649  pps=0  freq=30
id=udp_src_session     ip=192.168.1.110   dos_id=1  exp=5649  pps=0  freq=22
```

このコマンドの出力にはどのIPアドレスが含まれますか？
A.トラフィックがDoSポリシーに一致するもの。
B.トラフィックがIPSセンサーと一致するもの。
C.トラフィックが一致するDoSポリシーのしきい値を超えたもの。
D.IPSセンサーによってトラフィックが異常として検出された人。
Answer: A

QUESTION NO: 5
CLIコマンドset Intelligent-mode <enable |
disable>は、IPSエンジンの適応スキャン動作を制御します。次のステートメントのうち、IPS適応スキャンについて説明しているものはどれですか？
A.システム負荷に基づいて必要なIPSエンジンの最適数を決定します。
B.スキャン要件に基づいて、FDSからオンデマンドで署名をダウンロードします。
C.セッショントラフィックのスキャンを停止するのに十分な安全性を確保します。
D.使用可能なメモリと実行されている検査のタイプに基づいて、一致するアルゴリズムを選択します。
Answer: C
Explanation
Configuring IPS intelligenceStarting with FortiOS 5.2, intelligent-mode is a new adaptive detection method. This command is enabled the default and it means that the IPS engine will perform adaptive scanning so that, for some traffic, the FortiGate can quickly finish scanning and offload the traffic to NPU or kernel. It is a balanced method which could cover all known exploits. When disabled, the IPS engine scans every single byte.
config ips globalset intelligent-mode {enable|disable}end

QUESTION NO: 6
展示に表示されている「diagnose vpn tunnel
list」コマンドの出力を調べます。以下の質問に答えてください。

```
#diagnose vpn tunnel list
name-Dial Up_0 ver=1 serial=5 10.200.1.1:4500->10.200.3.2: 64916 lgwy=static
nun=intf mode=dial_inst.bound if=2
parent=DialUp index=0
proxyid_um=1 child_num=0 refcnt=8 ilast=4 olast=4
stat: rxp=104 txp=8 rxb=27392 txb=480
dpd: mode=active on=1 idle=5000ms retry=3 count=0 segno=70
natt: mode=silent draft=32 interval= 10 remote_port=64916
proxyid= DialUp proto=0 sa=1 ref=2 serial=1 add-route
  src: 0:0.0.0.0.-255.255.255.255:0
  dst: 0:10.0.10.10.-10.0.10.10:0
  SA: ref=3 options= 00000086 type=00 soft=0 mtu=1422 expire =42521
replaywin=2048 seqno=9
  life: type=01 bytes=0/0 timeout= 43185/43200
  dec: spi=cb3a632a esp=aes key=16  7365e17a8fd555ec38bffa47d650c1a2
       ah=sha1 key=20  946bfb9d23b8b53770dcf48ac2af82b8ccc6aa85
  enc: spi=da6d28ac  esp=aes  key=16  3dcf44ac7c816782ea3d0c9a977ef543
       ah=sha1 key=20   7cfde587592fc4635ab8db8ddf0d851d868b243f
dec:pkts/bytes=104/19926, enc:pkts/bytes=8/1024
```

どのコマンドを使用して、VPN
DialUP_0のESPトラフィックをスニッフィングできますか？

A. diagnose sniffer packet any 'port 500'

B. diagnose sniffer packet any 'esp'

C. diagnose sniffer packet any 'host 10.0.10.10'

D. diagnose sniffer packet any 'port 4500'

Answer: D

Explanation

NAT-T is enabled. natt: mode=silentProtocol ESP is used. ESP is encapsulated in UDP port 4500 when NAT-T is enabled.

QUESTION NO: 7

診断コマンドの部分的な出力を含む展示を表示して、以下の質問に答えてください。

```
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=static/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refcnt=15 ilast=10 olast=792 auto-discovery=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000 ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN proto=0 sa=1 ref=2 serial=1
  src: 0:10.1.2.0/255.255.0:0
  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=2048 seqno=1 esn=0
replaywin_lastseq=00000000
  life: type=01 bytes=0/0 timeout=43177/43200
  dec: spi=ccc1f66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
     ah=sha1 key=20 c68091d68753578785de6a7a6b276b506c527efe
  enc: spi=df14200b esp=aes key=16 b02a7e9f5542b69aff6aa391738ee393
  ah=sha1 key20 889f7529887c215c25950be2ba83e6fe1a5367be
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

出力に基づいて、次の記述のうち正しいものはどれですか？

A. Anti-replay is enabled.

B. DPD is disabled.

C. Quick mode selectors are disabled.

D. Remote gateway IP is 10.200.5.1.

Answer: A

QUESTION NO: 8

debugコマンドの出力を含む展示を表示して、以下の質問に答えてください。

```
#dia hardware sysinfo shm
SHM counter:           150
SHM allocated:           0
SHM total:       625057792
conserve mode: on - mem
system last entered: Mon Apr 24 16:36:37 2017
sys fd last entered: n/a
SHM FS total:  641236992
SHM FS free:   641208320
SHM FS avail:  641208320
SHM FS alloc:      28672
```

このFortiGateについて正しい記述は何ですか？

A.CPU使用率が高いため、現在システム保存モードです。

B.現在、FD節約モードです。
C.現在、メモリ使用量が多いため、カーネル保存モードになっています。
D.メモリ使用量が多いため、現在システム保存モードです。
Answer: D