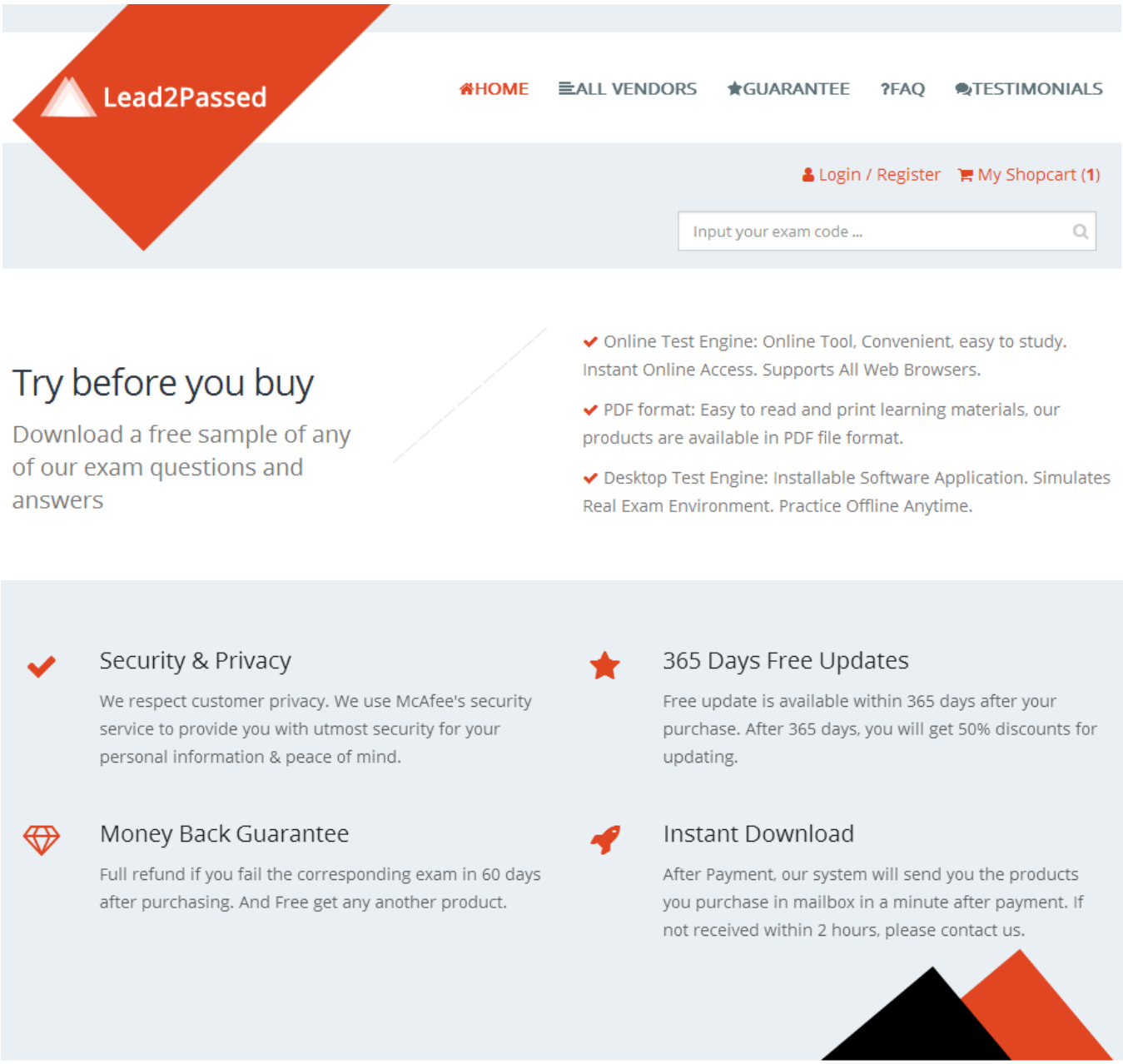
Lead2Passed



http://www.lead2passed.com

Valid Certification Exam Dumps Materials and Study Guide - Lead2Passed

Exam : **NSE7_SDW-7.2**

Title : Fortinet NSE 7 - SD-WAN 7.2

Vendor : Fortinet

Version : DEMO

NO.1 What are two reasons why FortiGate would be unable to complete the zero-touch provisioning process?
(Choose two.)
A. The FortiGate cloud key has not been added to the FortiGate cloud portal.
B. FortiDeploy has connected with FortiGate and provided the initial configuration to contact FortiManager
C. The zero-touch provisioning process has completed internally, behind FortiGate.
D. FortiGate has obtained a configuration from the platform template in FortiGate cloud.
E. A factory reset performed on FortiGate.
Answer: A C

NO.2 What are two advantages of using an IPsec recommended template to configure an IPsec tunnel in a hub-and- spoke topology? (Choose two.)
A. VPN monitor tool provides additional statistics for tunnels defined with an IPsec recommended template.
B. FortiManager automatically installs IPsec tunnels to every spoke when they are added to the FortiManager ADOM.
C. IPsec recommended template guides the administrator to use Fortinet recommended settings.
D. IPsec recommended template ensures consistent settings between phase1 and phase2
Answer: B C
Explanation:
According to the SD-WAN 7.2 Study Guide, IPsec recommended templates are designed to simplify the configuration of IPsec tunnels in a hub-and-spoke topology. They have the following advantages:
* FortiManager automatically installs IPsec tunnels to every spoke when they are added to the FortiManager ADOM. This reduces the manual effort and ensures that all spokes have the same configuration.
* IPsec recommended template guides the administrator to use Fortinet recommended settings, such as encryption algorithms, key lifetimes, and dead peer detection. This ensures optimal performance and security of the IPsec tunnels.

NO.3 Which two interfaces are considered overlay links? (Choose two.)
A. LAG
B. IPsec
C. Physical
D. GRE
Answer: B D

NO.4 Refer to the exhibit.

```
branch1_fgt # diagnose sys sdwan service 1

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(2):
    1: Seq_num(3 T_INET_0_0), alive, selected
    2: Seq_num(4 T_INET_1_0), alive, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255


branch1_fgt # diagnose sys sdwan member | grep T_INET_
Member(3): interface: T_INET_0_0, flags=0x4 , gateway: 100.64.1.1, priority: 10 1024,
weight: 0
Member(4): interface: T_INET_1_0, flags=0x4 , gateway: 100.64.1.9, priority: 0 1024,
weight: 0

branch1_fgt # get router info routing-table all | grep T_INET_
S       10.0.0.0/8 [1/0] via T_INET_1_0 tunnel 100.64.1.9
```

An administrator is troubleshooting SD-WAN on FortiGate. A device behind branch1_fgt generates traffic to the 10.0.0.0/8 network. The administrator expects the traffic to match SD-WAN rule ID 1 and be routed over T_INET_0_0. However, the traffic is routed over T_INET_1_0.
Based on the output shown in the exhibit, which two reasons can cause the observed behavior? (Choose two.)

A. The traffic matches a regular policy route configured with T_INET_1_0 as the outgoing device.

B. T_INET_1_0 has a lower route priority value (higher priority) than T_INET_0_0.

C. T_INET_0_0 does not have a valid route to the destination.

D. T_INET_1_0 has a higher member configuration priority than T_INET_0_0.

Answer: A C

Explanation:
SD-WAN strategy is Lowest Cost (SLA) as indicated by the "Mode(sla)" flag. Cost SLA uses SLA target, cost, and priority (i.e., interface preference - or order of config unless manually overridden by admin config) as the criteria -- in that order. Both members meet the target, both have 0 cost, and therefore member 3 (T_INET_0) wins the "priority" tiebreaker. So if there is a valid route to the destination through member 3, it will win. The fact that it does not has nothing to do with the configured static route/member priority, which according to SG page 197 "is used as a tiebreaker for ECMP routes when matching implicit SD-WAN rule."

NO.5 Refer to the exhibits.
Exhibit A

```
config system sdwan
    config health-check
        edit "Passive"
            set detect-mode passive
            set members 3 4
        next
    end
end

config system sdwan
    config service
        edit 1
            set name "Facebook-YouTube"
            set src "all"
            set internet-service enable
            set internet-service-app-ctrl 15832 31077
            set health-check "Passive"
            set priority-member 3 4
            set passive-measurement enable
        next
    end
end

branch1_fgt # get application name status | grep "id: 15832" -B1
app-name: "Facebook"
id: 15832

branch1_fgt # get application name status | grep "id: 31077" -B1
app-name: "YouTube"
id: 31077
```

Exhibit B

```
config firewall policy
    edit 1
        set name "DIA"
        set uuid b973e4ec-5f90-51ec-cadb-017c830d9418
        set srcintf "port5"
        set dstintf "underlay"
        set action accept
        set srcaddr "LAN-net"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set passive-wan-health-measurement enable
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set application-list "default"
        set logtraffic all
        set auto-asic-offload disable
        set nat enable
    next
end

branch1_fgt # diagnose sys sdwan zone | grep underlay -A1
Zone underlay index=3
          members(2): 3(port1) 4(port2)
```

Exhibit A shows the SD-WAN performance SLA configuration, the SD-WAN rule configuration, and the application IDs of Facebook and YouTube. Exhibit B shows the firewall policy configuration and the underlay zone status.

Based on the exhibits, which two statements are correct about the health and performance of port1 and port2?

(Choose two.)

A. The performance is an average of the metrics measured for Facebook and YouTube traffic passing through the member.

B. FortiGate is unable to measure jitter and packet loss on Facebook and YouTube traffic.

C. FortiGate identifies the member as dead when there is no Facebook and YouTube traffic passing through the member.

D. Non-TCP Facebook and YouTube traffic are not used for performance measurement.

Answer: A D

Explanation:

Study Guide 7.2, pages 103 - 104. Another comment said "because without using application Control on the firewall policy, SDWAN can't work" but there is a app control "default" defined on config.

NO.6 Refer to the exhibit, which shows the IPsec phase 1 configuration of a spoke.

```
config vpn ipsec phase1-interface
    edit "T_INET_0_0"
        set interface "port1"
        set ike-version 2
        set keylife 28800
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384
chacha20poly1305-prfsha256
        set comments "[created by FMG VPN Manager]"
        set idle-timeout enable
        set idle-timeoutinterval 5
        set auto-discovery-receiver enable
        set remote-gw 100.64.1.1
        set psksecret ENC
6D5rVsaK1MeAyVYt1z95BS24Psew761wY023hnFVviwb6deItSc51tCa+iNYhujT8gycfD4+WuszpmuIv8rRzrVh
7DFkHaW2auAAprQ0dHUfaCzjOhME7mPw+8he2xB7Edb9ku/nZEHb0cKLkKYJc/p9J9IMweV2lZUgFjvIpXNxHxpH
LReOFShoH01SPFKz5IYCVA==
    next
end
```

What must you configure on the IPsec phase 1 configuration for ADVPN to work with SD-WAN?

A. You must set ike-version to 1.

B. You must enable net-device.

C. You must enable auto-discovery-sender.

D. You must disable idle-timeout.

Answer: B

NO.7 What are two common use cases for remote internet access (RIA)? (Choose two.)

A. Provide direct internet access on spokes

B. Provide internet access through the hub

C. Centralize security inspection on the hub

D. Provide thorough inspection on spokes

Answer: B C

Explanation:

B: Provide internet access through the hub: This involves routing branch or remote office internet traffic through a central hub, ensuring consistent security policies and possibly better management of network resources.

C: Centralize security inspection on the hub: With this approach, all internet-bound traffic from various spokes is inspected at the hub, leveraging centralized security mechanisms for thorough inspection and policy enforcement.

NO.8 Refer to the exhibits.

Exhibit A

	#	Name	From	To	Source	Destination
☑	1	DIA	D-LAN LAN	underlay	LAN-net	all
☐	Implicit (2/2 Total:1)					
☐	2	Implicit Deny	any	any	all all	all all

Exhibit B

View Install Log

```
Copy device global objects

validation error on firewall policy 1, by dynamic interface check

Vdom copy failed:
error 42 - entry not exist. detail: Dynamic interface "LAN" mapping undefined for device branch2_fgt

Copy objects for vdom root
```

Exhibit A shows a policy package definition Exhibit B shows the install log that the administrator received when he tried to install the policy package on FortiGate devices.
Based on the output shown in the exhibits, what can the administrator do to solve the Issue?

A. Create dynamic mapping for the LAN interface for all devices in the installation target list.

B. Use a metadata variable instead of a dynamic interface to define the firewall policy.

C. Dynamic mapping should be done automatically. Review the LAN interface configuration for branch2_fgt.

D. Policies can refer to only one LAN source interface. Keep only the D-LAN, which is the dynamic LAN interface.

Answer: A

NO.9 Refer to the exhibit.

```
config system interface
    edit "port2"
        set vdom "root"
        set ip 192.2.0.9 255.255.255.248
        set allowaccess ping
        set type physical
        set role wan
        set snmp-index 2
        set preserve-session-route enable
    next
end
```

Based on the exhibit, which two actions does FortiGate perform on traffic passing through port2? (Choose two.)

A. FortiGate does not change the routing information on existing sessions that use a valid gateway, after a route change.

B. FortiGate performs routing lookups for new sessions only, after a route change.

C. FortiGate always blocks all traffic, after a route change.

D. FortiGate flushes all routing information from the session table, after a route change.

Answer: A B

NO.10 Which two protocols in the IPsec suite are most used for authentication and encryption? (Choose two.)

A. Encapsulating Security Payload (ESP)

B. Secure Shell (SSH)

C. Internet Key Exchange (IKE)

D. Security Association (SA)

Answer: A C