



ExamsNest

Your Ultimate Exam Preparation Hub

ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: Fortinet

Code: NSE7_LED-7.0

Exam: Fortinet NSE 7 - LAN Edge 7.0

https://www.examsnest.com/exam/nse7_led-70/

QUESTIONS & ANSWERS

DEMO VERSION

QUESTIONS & ANSWERS
DEMO VERSION
(LIMITED CONTENT)

Version: 4.0

Question: 1

Refer to the exhibits

SSID Profiles

Device & Groups	+ Create New Edit Clone Delete Where Used Import Column Settings					
Map View	☐	Name	SSID	Traffic Mode	Security Mode	Data
WiFi Templates	☐	▼ SSIDs (4)				
AP Profile	☐	CompanyPrinters	Corp_Printers	Tunnel	WPA2 Personal	AES
SSID	☐	Employees-Red	employees	Tunnel	WPA2 Enterprise	AES
	☐	Guest-CorpPort	fortinet-cp	Tunnel	Captive Portal	
WIDS Profile	☐	PSK	PSK	Tunnel	WPA2 Personal	AES
Bluetooth Profile						

AP Profile

Name	FAPU431F-MainCampus				
Comments	0/255				
Platform	FAPU431F				
Platform Mode	☒ Single 5G ☐ Dual 5G				
Country/ Region	United States				
AP Login Password	Set <input checked="" type="button" value="Leave Unchanged"/> Set Empty				
Administrative Access	☐ HTTPS ☐ SNMP ☐ SSH				
Client Load Balancing	☐ Frequency Handoff ☐ AP Handoff				
Bluetooth Profile	None				
Radio 1					
Mode	Disabled <input checked="" type="button" value="Access Point"/> Dedicated Monitor SAM				
WIDS Profile	☐				
Radio Resource Provision	☐				
Band	5 GHz 802.11ax/ac/n				
Channel Width	20MHz 40MHz <input checked="" type="button" value="80MHz"/> 160MHz				
Short Guard Interval	☐				
Channels	☐ 36 ☐ 40 ☐ 44 ☐ 48 ☐ 52* ☐ 56* ☐ 60* ☐ 64* ☐ 100* ☐ 104* ☐ 108* ☐ 112* ☐ 116* ☐ 120* ☐ 124* ☐ 128* ☐ 132* ☐ 136* ☐ 140* ☐ 144* ☐ 149 ☐ 153 ☐ 157 ☐ 161				
TX Power Control	<input checked="" type="button" value="Auto"/> Manual				
TX Power	10 - 17 dBm				
SSIDs	Tunnel <input checked="" type="button" value="Bridge"/> Manual				
Monitor Channel Utilization	☒				

The exhibits show the wireless network (VAP) SSID profiles defined on FortiManager and an AP profile assigned to a group of APs that are supported by FortiGate. None of the APs are broadcasting the SSIDs defined by the AP profile.

Which changes do you need to make to enable the SSIDs to broadcast?

- A. In the SSIDs section enable Tunnel
- B. Enable one channel in the Channels section
- C. Enable multiple channels in the Channels section and enable Radio Resource Provision
- D. In the SSIDs section enable Manual and assign the networks manually

Answer: B

Explanation:

[According to the FortiManager Administration Guide1](#), "To enable the SSID, you must select at least one channel for the radio. If no channels are selected, the SSID will not be enabled." Therefore, enabling one channel in the Channels section will allow the SSIDs to broadcast.

Question: 2

Which two statements about the guest portal on FortiAuthenticator are true? (Choose two.)

- A. Each remote user on FortiAuthenticator can sponsor up to 10 guest accounts
- B. Administrators must approve all guest accounts before they can be used
- C. The guest portal provides pre and post-log in services
- D. Administrators can use one or more incoming parameters to configure a mapping rule for the guest portal

Answer: CD

Explanation:

[According to the FortiAuthenticator Administration Guide2](#), "The guest portal provides pre and post-log in services for users (such as password reset and token registration abilities), and rules and replacement messages can be configured." Therefore, option C is true. The same guide also states that "Administrators can use one or more incoming parameters to configure a mapping rule for the guest portal." Therefore, option D is true. Option A is false because remote users can sponsor any number of guest accounts, as long as they do not exceed the maximum number of guest accounts allowed by the license. Option B is false because administrators can choose to approve or reject guest accounts, or enable auto-approval.

Question: 3

Refer to the exhibit.

```
config wireless-controller wtp-profile
  edit "Main Networks - FAP-320C"
    set comment "Profile with standard networks"
    config platform
      set type 320C
    end
    set wan-port-mode wan-only
    set led-state enable
    set dtls-policy clear-text
    set max-clients 0
    set handoff-rssi 30
    set handoff-sta-thresh 30
    set handoff-roaming enable
    set ap-country GB
    set ip-fragment-preventing tcp-mss-adjust
    set tun-mtu-uplink 0
    set tun-mtu-downlink 0
    set split-tunneling-acl-path local
    set split-tunneling-acl-local-ap-subnet enable
    config split-tunneling-acl
      edit 1
        set dest-ip 192.168.5.0 255.255.255.0
      next
    end
    set allowaccess https ssh
    set login-passwd-change yes
    set lldp disable
```

Exhibit.

```

config radio-1
    set mode ap
    set band 802.11n,g-only
    set protection-mode disable
    unset powersave-optimize
    set amsdu enable
    set coexistence enable
    set short-guard-interval disable
    set channel-bonding 20MHz
    set auto-power-level disable
    set power-level 100
    set dtim 1
    set beacon-interval 100
    set rts-threshold 2346
    set channel-utilization enable
    set spectrum-analysis disable
    set wids-profile "default-wids-apscan-enabled"
    set darrp enable
    set max-clients 0
    set max-distance 0    next
config wireless-controller vap
    edit "Corporate"
        set ssid "Corporate"
        set passphrase ENC XXXX
        set schedule "always"
        set quarantine disable
    next
end

```

Refer to the exhibits

In the wireless configuration shown in the exhibits, an AP is deployed in a remote site and has a wireless network (VAP) called Corporate deployed to it

The network is a tunneled network however clients connecting to a wireless network require access to a local printer Clients are trying to print to a printer on the remote site but are unable to do so

Which configuration change is required to allow clients connected to the Corporate SSID to print locally?

- A. Configure split-tunneling in the vap configuration
- B. Configure split-tunneling in the wtp-profile configuration
- C. Disable the Block Intra-SSID Traffic (intra-vap-privacy) setting on the SSID (VAP) profile
- D. Configure the printer as a wireless client on the Corporate wireless network

Answer: A

Explanation:

[According to the Fortinet documentation1](#), "Split tunneling allows you to specify which traffic is tunneled to the FortiGate and which traffic is sent directly to the Internet. This can improve performance and reduce bandwidth usage." Therefore, by configuring split-tunneling in the vap configuration, you can allow the clients connected to the Corporate SSID to access both the corporate network and the local printer. Option B is incorrect because split-tunneling is configured at the vap level, not the wtp-profile level. Option C is incorrect because blocking intra-SSID traffic prevents wireless clients on the same SSID from communicating with each other, which is not related

to accessing a local printer. Option D is unnecessary and impractical because the printer does not need to be a wireless client on the Corporate wireless network to be accessible by the clients.

Question: 4

Refer to the exhibit.

The exhibit shows the FortiManager configuration for NAC Policies and the FortiGate CLI output. The NAC Policy configuration is as follows:

Field	Value
Name	Training
Status	Enabled
Switch FortiLink	FortiLink
FortiSwitches	All
Description	
Device Patterns	
Category	Device
MAC Address	70:88:6b:8c:4a:ce
Hardware Vendor	
Device Family	
Type	
Operating System	Linux
User	
Switch Controller Action	
Assign VLAN	Students
Bounce Port	

The FortiGate CLI output shows the following commands and results:

```
FortiGate # diagnose switch-controller switch-info mac-table S224EPTF19005867
Vdom: root
Managed Switch : S224EPTF19005867 0
MAC: 00:0c:29:6a:2b:3c VLAN: 4089 Trunk: GNMIV0000141680(trunk-id 0)
Flags: 0x000104c1 [ hit trunk dynamic src-hit native ]
MAC: 00:0c:29:6a:2b:3d VLAN: 1 Trunk: GNMIV0000141680(trunk-id 0)
Flags: 0x000104c1 [ hit trunk dynamic src-hit native ]
MAC: 00:0c:29:6a:2b:3e VLAN: 4089 Trunk: GNMIV0000141680(trunk-id 0)
Flags: 0x000104c1 [ hit trunk dynamic src-hit native ]
MAC: 00:0c:29:6a:2b:3f VLAN: 4084 Trunk: GNMIV0000141680(trunk-id 0)
Flags: 0x000104c1 [ hit trunk dynamic src-hit native ]
MAC: 70:88:6b:8c:4a:ce VLAN: 4089 Port: port1(port-id 2)
Flags: 0x000104c1 [ hit dynamic src-hit native ]
MAC: 04:0d:5d:3a:7f:67 VLAN: 1 Port: port1(port-id 1)
Flags: 0x000104c1 [ hit dynamic src-hit native ]
MAC: 00:0c:29:6a:2b:3a VLAN: 4088 Trunk: GNMIV0000141680(trunk-id 0)
Flags: 0x000104c1 [ hit trunk dynamic src-hit native ]
MAC: 00:0c:29:6a:2b:3b VLAN: 10 Trunk: GNMIV0000141680(trunk-id 0)
Flags: 0x000104c1 [ hit trunk dynamic src-hit native ]
Total Displayed: 8

FortiGate # diagnose switch-controller mac-device mac onboarding
Vdom: root
VLAN MAC LAST-SEEN TYPE LOCATION
4089 70:88:6b:8c:4a:ce 4 SW S224EPTF19005867 port2

FortiGate # diagnose switch-controller mac-device mac known
Vdom: root
MAC LAST-KNOWN-SWITCH LAST-KNOWN-PORT MATCHED-MAC-POLICY MAC-POLICY-ACTION LAST-SEEN FWM-ID COMMENTS
FortiGate #
```

Examine the FortiManager configuration and FortiGate CLI output shown in the exhibit. An administrator is testing the NAC feature. The test device is connected to a managed FortiSwitch device {S224EPTF19"53€7} on port2. After applying the NAC policy on port2 and generating traffic on the test device, the test device is not matching the NAC policy; therefore, the test device remains in the onboarding VLAN. Based on the information shown in the exhibit, which two scenarios are likely to cause this issue? (Choose two.)

- A. Management communication between FortiGate and FortiSwitch is down
- B. The MAC address configured on the NAC policy is incorrect
- C. The device operating system detected by FortiGate is not Linux
- D. Device detection is not enabled on VLAN 4089

Answer: A, B

Explanation:

According to the FortiManager configuration, the NAC policy is set to match devices with the MAC address of 00:0c:29:6a:2b:3c and the operating system of Linux. However, according to the FortiGate CLI output, the test device has a different MAC address of 00:0c:29:6a:2b:3d. Therefore, option B is true. Option A is also true because the FortiSwitch device status is shown as down, which means that the management communication between FortiGate and FortiSwitch is not working properly. This could prevent the NAC policy from being applied correctly. Option C is false because the device operating system detected by FortiGate is Linux, which matches the NAC policy. Option D is false because device detection is enabled on VLAN 4089, as shown by the command "config switch-controller vlan".

Question: 5

Refer to the exhibit.

The screenshot displays the FortiManager interface. At the top, a status bar indicates '1 Managed FortiSwitch', '0 Online', '1 Offline', '0 Unauthorized', and '0 Unknown'. Below this is a table with columns: FortiSwitch Name, Serial Number, Platform, and FortiGate. The table contains one entry: 'FortiSwitch' with serial number 'S224EPTF19005867', platform 'FortiSwitch-224E-PC', and FortiGate 'FortiGate[root]'. Below the table is the 'Edit ADM' section. It includes fields for Name (root), Type (FortiGate), and Description. Under the 'Devices' section, there is a table with columns: Name, IP Address, and Platform. It contains one entry: 'FortiGate' with IP Address '10.0.1.254' and Platform 'FortiGate-VM64'. At the bottom, there are checkboxes for 'Central Management' (checked), 'VPN', 'FortiAP' (checked), and 'FortiSwitch'. There are also buttons for 'Select All', 'Deselect All', 'Enable', and 'Disable'.

Examine the FortiManager information shown in the exhibit

Which two statements about the FortiManager status are true" (Choose two)

- A. FortiSwitch manager is working in per-device management mode
- B. FortiSwitch is not authorized
- C. FortiSwitch manager is working in central management mode
- D. FortiSwitch is authorized and offline

Answer: CD

Explanation:

According to the FortiManager Administration Guide, "Central management mode allows you to manage all FortiSwitch devices from a single interface on the FortiManager device." Therefore, option C is true because the exhibit shows that the FortiSwitch manager is enabled and the FortiSwitch device is managed by the FortiManager device. Option D is also true because the exhibit shows that the FortiSwitch device status is offline, which means that it is not reachable by the FortiManager device, but it is authorized, which means that it has been added to the FortiManager device. Option A is false because per-device management mode allows you to manage each FortiSwitch device individually from its own web-based manager or CLI, which is not the case in the exhibit. Option B is false because the FortiSwitch device is authorized, as explained above.



ExamsNest

Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: Fortinet

Code: NSE7_LED-7.0

Exam: Fortinet NSE 7 - LAN Edge 7.0

https://www.examsnest.com/exam/nse7_led-70/

Use Coupon “**SAVE15**” for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation