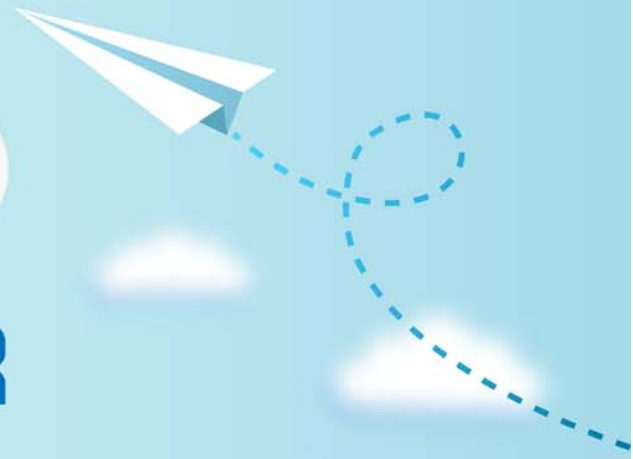


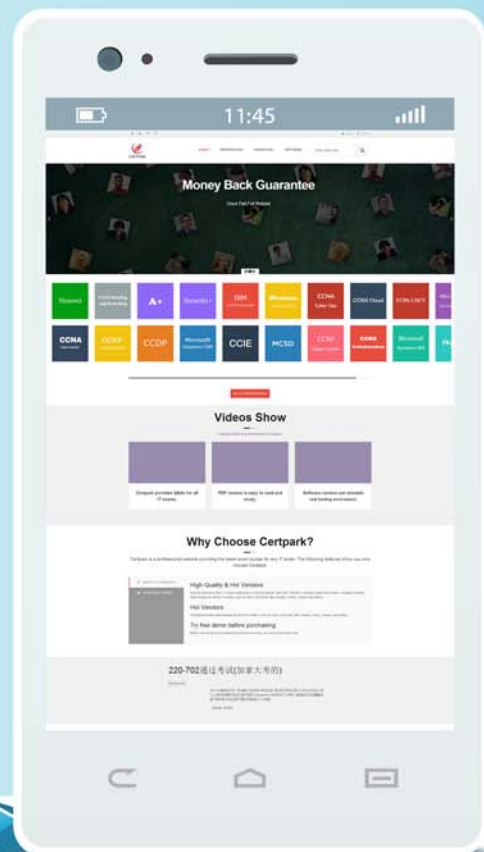
CERTPARK

QUESTION & ANSWER



CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



<https://www.certpark.com>

Exam : **NSE7_LED-7.0**

Title : Fortinet NSE 7 - LAN Edge
7.0

Version : DEMO

1.Refer to the exhibits

SSID Profiles

Device & Groups > Map View > WIFI Templates > AP Profile SSID WIDS Profile Bluetooth Profile	+ Create New Edit Clone Delete Where Used Import Column Settings				
	<input type="checkbox"/>	Name	SSID	Traffic Mode	Security Mode
	<input type="checkbox"/>	▼ SSIDs (4)			
	<input type="checkbox"/>	CompanyPrinters	Corp_Printers	Tunnel	WPA2 Personal
	<input type="checkbox"/>	Employees-Red	employees	Tunnel	WPA2 Enterprise

<input type="checkbox"/>	Guest-CorpPort	fortinet-cp	Tunnel	Captive Portal
<input type="checkbox"/>	PSK	PSK	Tunnel	WPA2 Personal

AP Profile

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

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: D

Explanation:

In the exhibit provided, if the Access Points (APs) are not broadcasting the SSIDs as defined by the AP profile on the FortiManager, here's what could be changed to enable the SSID broadcast:

In the SSIDs section enable Manual and assign the networks manually.

Enabling the Manual option and then assigning the networks manually ensures that the SSIDs are actively configured for broadcast. SSID profiles need to be explicitly associated with the AP or AP group to take effect.

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.

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.

4.Refer to the exhibit.

The screenshot shows the FortiManager NAC Policies configuration interface on the left and the FortiGate CLI output on the right.

FortiManager NAC Policies Configuration:

- Name:** Training
- Status:** Enabled
- Switch FortiLink:** fortlink
- FortiSwitches:** All (1 Entry Selected)
- Description:**
- Device Patterns:**
 - Category:** Device
 - MAC Address:** 70B8A63c:face
 - Hardware Vendor:**
 - Device Family:**
 - Type:**
 - Operating System:** Linux
 - User:**
- Switch Controller Action:**
 - Assign VLAN:** Students
 - Source Port:**

FortiGate CLI Output:

```
FortiGate # diagnose switch-controller switch-info mac-table S224EPTF19055E7
Name: root
Managed Switch : S224EPTF19055E7 0
MAC: 00:0c:29:e6:ead2 VLAN: 4089 Trunk: 0001V0000141680(trunk-id 0)
Flags: 0a000104c1 [ hit trunk dynamic src-hit native ]
MAC: 00:0c:29:e6:ead2 VLAN: 1 Trunk: 0001V0000141680(trunk-id 0)
Flags: 0a000104c1 [ hit trunk dynamic src-hit native ]
MAC: 00:0c:29:e6:ead2 VLAN: 4093 Trunk: 0001V0000141680(trunk-id 0)
Flags: 0a000104c1 [ hit trunk dynamic src-hit native ]
MAC: 00:0c:29:e6:ead2 VLAN: 4094 Trunk: 0001V0000141680(trunk-id 0)
Flags: 0a000104c1 [ hit trunk dynamic src-hit native ]
MAC: 70:b8:a6:3c:face VLAN: 4089 Port: port2(port-id 2)
Flags: 0a00010441 [ hit dynamic src-hit native ]
MAC: 04:a5:b0:3a:a7:09 VLAN: 1 Port: port1(port-id 1)
Flags: 0a00010441 [ hit dynamic src-hit native ]
MAC: 00:0c:29:e6:ead2 VLAN: 4088 Trunk: 0001V0000141680(trunk-id 0)
Flags: 0a000104c1 [ hit trunk dynamic src-hit native ]
MAC: 00:0c:29:e6:ead2 VLAN: 10 Trunk: 0001V0000141680(trunk-id 0)
Flags: 0a000104c1 [ hit trunk dynamic src-hit native ]
Total Displayed: 9

FortiGate # diagnose switch-controller mac-device mac onboarding
Name: root
VLAN MAC LAST-SEEN TYPE LOCATION
4089 70:b8:a6:3c:face 4 S224EPTF19055E7 port2

FortiGate # diagnose switch-controller mac-device mac known
Name: root
MAC LAST-KNOWN-SWITCH LAST-KNOWN-PORT MATCHED-MAC-POLICY MAC-POLICY-ACTION LAST-SEEN FOR-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)onpOrt2

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 m 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: B, D

Explanation:

From the exhibit, which shows the FortiManager configuration and FortiGate CLI output related to a Network Access Control (NAC) test, the two scenarios that are likely causing the issue where the test device is not matching the NAC policy and remains in the onboarding VLAN could be:

If the MAC address in the NAC policy does not match the MAC address of the test device, the policy would not be applied correctly, and the device would not be moved to the appropriate VLAN as intended. For the NAC policy to apply correctly, device detection needs to be enabled on the VLAN to which the device is connected. If it's not enabled on VLAN 4089, where the device is currently located, the NAC policy won't be able to identify the device and apply the correct policy.

5.Refer to the exhibit.

The screenshot displays the FortiManager interface. At the top, a summary bar shows: 1 Managed FortiSwitch, 0 Online, 1 Offline, 0 Unauthorized, and 0 Unknown. Below this is a table of managed devices:

FortiSwitch Name	Serial Number	Platform	FortiGate
FortiSwitch	S224EPTF19005867	FortiSwitch-224E-PC	FortiGate[root]

Below the table is the 'Edit ADM' configuration page for the FortiGate. The 'Name' field is 'root', 'Type' is 'FortiGate', and 'Version' is '7.0'. The 'Devices' section shows a table with one device:

Name	IP Address	Platform
FortiGate	10.0.1.254	FortiGate-VM64

At the bottom, there are checkboxes for 'Central Management', 'VPN', 'FortiAP', and 'FortiSwitch'. The 'FortiAP' checkbox is checked, and the 'FortiSwitch' checkbox is unchecked.

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: AC

Explanation:

Based on the FortiManager information shown in the exhibit, the two true statements about the FortiManager status are:

The information indicates that there is one FortiSwitch managed, which suggests a per-device management mode where each FortiSwitch is individually listed and managed.

The fact that the FortiSwitch is shown within the FortiManager indicates that it's being managed centrally, which is the purpose of using FortiManager.