



**Vendor:** Fortinet

**Exam Code:** NSE7\_LED-7.0

**Exam Name:** Fortinet NSE 7 - LAN Edge 7.0

**Version:** DEMO

### QUESTION 1

You are investigating a report of poor wireless performance in a network that you manage. The issue is related to an AP interface in the 5 GHz range. You are monitoring the channel utilization over time.

What is the recommended maximum utilization value that an interface should not exceed?

- A. 85%
- B. 95%
- C. 75%
- D. 65%

**Answer: C**

**Explanation:**

Enhanced Wireless

**DO NOT REPRINT  
© FORTINET**

**Regular Monitoring Is Essential**

Wireless capacity	Wireless health
<ul style="list-style-type: none"><li>As a guide, a healthy interface should maintain rates of:<ul style="list-style-type: none"><li>Utilization &lt; 75%</li><li>Client count &lt; 30</li><li>Temporary peaks above this are expected</li></ul></li></ul>	<ul style="list-style-type: none"><li>Noise<ul style="list-style-type: none"><li>Ideally -92 or weaker</li><li>High -80s is OK</li><li>Low -80s or stronger is not good</li></ul></li><li>Signal strength<ul style="list-style-type: none"><li>Should match or better design criteria</li><li>In general should be -64 or stronger</li></ul></li><li>SnR<ul style="list-style-type: none"><li>Should 15 minimum</li><li>25 or more is preferable</li></ul></li><li>Best possible link rates<ul style="list-style-type: none"><li>Be aware of a client's capabilities</li><li>Ensure they are connected to the most suitable interface</li></ul></li></ul>

**NSE Training Institute** © Fortinet, Inc. All Rights Reserved. 54

### QUESTION 2

Refer to the exhibit. By default, FortiOS creates the following DHCP server scope for the FortiLink interface as shown in the exhibit.

What is the objective of the vci-string setting?

```
config system dhcp server
  edit 1
    set ntp-service local
    set default-gateway 169.254.1.1
    set netmask 255.255.255.0
    set interface "fortilink"
    config ip-range
      edit 1
        set start-ip 169.254.1.2
        set end-ip 169.254.1.254
      next
    end
    set vci-match enable
    set vci-string "FortiSwitch" "FortiExtender"
  next
end
```

- A. To ignore DHCP requests coming from FortiSwitch and FortiExtender devices
- B. To reserve IP addresses for FortiSwitch and FortiExtender devices
- C. To restrict the IP address assignment to FortiSwitch and FortiExtender devices
- D. To restrict the IP address assignment to devices that have FortiSwitch or FortiExtender as their hostname

**Answer:** C

**Explanation:**

According to the exhibit, the DHCP server scope for the FortiLink interface has a vci-string setting with the value "Cisco AP c2700". This setting is used to match the vendor class identifier (VCI) of the DHCP clients that request an IP address from the DHCP server. The VCI is a text string that uniquely identifies a type of vendor device.

### QUESTION 3

Which CLI command should an administrator use to view the certificate verification process in real time?

- A. diagnose debug application foauthd -1
- B. diagnose debug application radiusd -1
- C. diagnose debug application authd -1
- D. diagnose debug application fnbamd -1

**Answer:** D

**Explanation:**

DO NOT REPRINT  
© FORTINET

### Real-Time Debug

```
# diagnose debug application fnbamd -l
[2601] handle_req-Rcvd auth_cert req id=400354293, len=1065
[751] __fnbamd_load_certs_from_req-1 cert(s) in req.
[779] __fnbamd_build_cert_chain-1 cert(s) after re-org.
[3236] fnbamd_ca_chain_issuer_info-check local CA cache
[3288] fnbamd_ca_chain_build-check local CA cache
[787] fnbamd build cert chain-2 cert(s) after local cache search.
[788] __fnbamd_build_cert_chain-Chain is complete.
[393] __fnbamd_cert_verify-Following cert chain depth 0
[463] __fnbamd_cert_verify-Trusted CA found: CA_Cert_1
[393] __fnbamd_cert_verify-Following cert chain depth 1
[1755] cert_check_group_list-checking group type 1 group name 'SSLVPN'
[1466] peer_subject_cn_check-Cert subject 'CN = student'
[1630] check_add_peer-check peer user 'student' in group 'SSLVPN', result is 0
[1566] add_group_list-Add group 'SSLVPN'
```

Checking the chain of trust

CA found and trusted

FortiGate user group

Checking certificate subject

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

33

The Fortinet non-blocking authentication daemon (**fnbamd**) is the process that validates user certificates. The output of its real-time debug shows, step-by-step, what the non-blocking authentication daemon does when a user certificate is received and must be validated.

In the output shown on this slide, FortiGate checks the chain of trust first, until it finds that the certificate is signed by a trusted CA. Then, FortiGate finds the user group that the PKI user belongs to and checks the certificate subject.

#### QUESTION 4

Refer to the exhibits. 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.

## SSID Profiles

Device & Groups >	+ Create New	Edit	Clone	Delete	Where Used	Import	Column Settings	
Map View >								
WiFi Templates >								
AP Profile								
SSID								
WIDS Profile								
Bluetooth Profile								

  

<input type="checkbox"/>	Name	SSID	Traffic Mode	Security Mode	Data Encryption	Maximum Clients
<input type="checkbox"/>	▼ SSIDs (4)					
<input type="checkbox"/>	CompanyPrinters	Corp_Printers	Tunnel	WPA2 Personal	AES	0
<input type="checkbox"/>	Employees-Red	employees	Tunnel	WPA2 Enterprise	AES	0
<input type="checkbox"/>	Guest-CorpPort	fortinet-cp	Tunnel	Captive Portal		0
<input type="checkbox"/>	PSK	PSK	Tunnel	WPA2 Personal	AES	0

## AP Profile

Name: FAPU431F-MainCampus

Comments:

Platform: FAPU431F

Platform Mode: Single 5G Dual 5G

Country/ Region: United States

AP Login Password: Set Leave Unchanged Set Empty

Administrative Access: ☐ HTTPS ☐ SNMP ☐ SSH

Client Load Balancing: ☐ Frequency Handoff ☐ AP Handoff

Bluetooth Profile: None

**Radio 1**

Mode: Disabled Access Point Dedicated Monitor SAM

WIDS Profile: ☐

Radio Resource Provision: ☐

Band: 5 GHz 802.11ax/ac/n

Channel Width: 20MHz 40MHz 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: Auto Manual

TX Power: 10 - 17 dBm

SSIDs: Tunnel Bridge Manual

Monitor Channel Utilization: ☒

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:**

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 5

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:**

The guest portal on FortiAuthenticator can offer services both before and after a guest logs in, such as displaying terms of use before login and providing access to network resources after successful authentication.

Administrators have the ability to configure mapping rules for the guest portal using various incoming parameters. This allows for flexible and dynamic handling of guest account creation and access permissions based on different criteria.

#### QUESTION 6

Refer to the exhibit. Examine the FortiGate user group configuration and the Windows AD LDAP group membership information shown in the exhibit.

FortiGate is configured to authenticate SSL VPN users against Windows AD using LDAP. The administrator configured the SSL VPN user group for SSL VPN users. However the administrator noticed that both the student and j.smith users can connect to SSL VPN.

Which change can the administrator make on FortiGate to restrict the SSL VPN service to the student user only?

**Edit User Group**

Name:

Type:

Members:  +

**Remote Groups**

+ Add Edit Delete

Remote Server	Group Name
	Training-Lab

1

```
Administrator: Command Prompt
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>dsquery user -samid student ! dsget user -memberof
"CN=SSLVPN,CN=Users,DC=trainingAD,DC=training,DC=lab"
"CN=Domain Users,CN=Users,DC=trainingAD,DC=training,DC=lab"

C:\Users\Administrator>dsquery user -samid jsmith ! dsget user -memberof
"CN=Administrators,CN=Builtin,DC=trainingAD,DC=training,DC=lab"
"CN=Domain Users,CN=Users,DC=trainingAD,DC=training,DC=lab"

C:\Users\Administrator>
```

- A. In the SSL VPN user group configuration, set Group Name to CN=SSLVPN,CN=Users,DC=trainingAD,DC=training,DC=lab.
- B. In the SSL VPN user group configuration, change Name to CN=SSLVPN,CN=Users,DC=trainingAD,DC=training,DC=lab.
- C. In the SSL VPN user group configuration, set Group Name to CN=Domain Users,CN=Users,DC=trainingAD,DC=training,DC=lab.
- D. In the SSL VPN user group configuration, change Type to Fortinet Single Sign-On (FSSO).

**Answer: A**

**Explanation:**

The Group Name is the name of the LDAP group that you want to use for authentication. The name must match exactly the name of the LDAP group on the LDAP server.



## Thank You for Trying Our Product

### Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



JUNIPER  
NETWORKS



EMC²  
where information lives

**10% Discount Coupon Code: ASTR14**