KillTest

質量更高　服務更好

學習資料

http://www.killtest.net

一年免費更新服務

Exam : **FCSS_LED_AR-7.6**

Title : Fortinet NSE 6 - LAN Edge 7.6 Architect

Version : DEMO

1.A network engineer is deploying FortiGate devices using zero-touch provisioning (ZTP). The devices must automatically connect to FortiManager and receive their configurations upon first boot. However, after powering on the devices, they fail to register with FortiManager.
What could be a possible cause of this issue?
A. The FortiGate device requires manual intervention to accept the FortiManager connection.
B. In this scenario, the ZTP process works only when devices are connected using a console cable.
C. The FortiGate device must be preloaded with a configuration file before ZTP can function.
D. The FortiManager IP address is not reachable over TCP port 541.
Answer: D
Explanation:
Zero-Touch Provisioning (ZTP) for FortiGate devices is handled throughFortiDeploy, which automatically connects a FortiGate toFortiManagerso the device can download configuration templates and be centrally managed.
For ZTP to work, the newly booted FortiGate must successfully reach FortiManager. One of thecritical requirementsis connectivity over theFGFM (FortiGate–FortiManager) management protocol, which uses:
TCP Port 541
This is clearly stated in multiple Fortinet documents:
FortiGate Cloud Admin Guidelists port541as the management channel used for FortiGate → FortiManager / FortiGate Cloud communications:“Management... Protocol: TCP, Port:541”
FortiOS Administration Guidealso confirms this:“FortiManager provides remote management of FortiGate devices overTCP port 541.”
Since ZTP uses FortiDeploy to push the FortiManager IP to the device and relies on FGFM (port 541) for registration and configuration delivery,any failure on this port breaks the entire ZTP workflow.
Why option D is correct
If the FortiGate cannot reach FortiManager onTCP/541, itcannot register, cannot be authorized, and cannot receive its configuration — leading to a ZTP failure.
This is themost common causein real deployments:
Firewall blocking TCP/541
Upstream NAT device not forwarding 541
ISP restrictions
Incorrect FortiManager IP or routing issue
ZTP device behind a network that does not allow outbound 541
Why the other options are incorrect
A. The FortiGate device requires manual intervention to accept the FortiManager connection.
Incorrect.
ZTP is built specifically to avoid manual intervention. Once the FortiDeploy key is used, the device auto-connects to FortiManager without needing local acceptance.
B. ZTP works only when devices are connected using a console cable.
Incorrect.
ZTP requiresno console cable— that's the whole point. It relies on DHCP, WAN connectivity, and FortiDeploy auto-join.
C. The FortiGate device must be preloaded with a configuration file before ZTP can function.
Incorrect.
Preloading configuration defeats the purpose of ZTP.

ZTP delivers the initial configuration automatically from FortiManager using FortiDeploy.
LAN Edge 7.6 Architect Context
LAN Edge deployments often use FortiManager as the central orchestrator for:
FortiSwitch management via FortiLink
FortiAP wireless provisioning
SD-Branch configuration templates
Security Fabric automation
For all of this, ZTP enables remote sites to deploy FortiGate, FortiSwitch, and FortiAP withno on-site expertise.
If TCP/541 to FortiManager is blocked, the entire LAN Edge deployment pipeline fails, making optionDthe only valid and document-supported answer.

2.Which FortiGuard licenses are required for FortiLink device detection to enable device identification and vulnerability detection?
A. FortiGuard Vulnerability Management and FortiGuard Endpoit Protection
B. FortiGuard Threat Intelligence and FortiGuard IoT Detection
C. FortiGuard Threat Intelligence and FortiGuard Endpoint Protection
D. FortiGuard Attack Surface Security and FortiGuard IoT Detection
Answer: D
Explanation:
FortiLink device detection relies on FortiGate'sDevice IdentificationandIoT Detectioncapabilities to classify devices connected to FortiSwitch ports.
To enabledevice identificationandvulnerability detectionfor IoT/endpoint devices in LAN Edge deployments, FortiGate must subscribe to the correct FortiGuard services.
1. Required FortiGuard License for Device Identification (IoT Detection) The FortiOS documentation clearly states:
“IoT detection service… requires anAttack Surface Security Rating service licenseto download the IoT signature package.”
Additionally:
“The following settings are required for IoT device detection:
A validAttack Surface Security Rating service licenseto download the IoT signature package.”
This service provides:
IoT signature package
IoT device classification
Device behavior profiling
This makesAttack Surface Securitymandatory for FortiLink device detection.
2. Required FortiGuard License for Device Vulnerability Detection
FortiOS further clarifies that IoT vulnerabilities require theIoT Detection license, which is included under the same Attack Surface service entitlement:
“To detect IoT vulnerabilities the FortiGate must have a validIoT Definitions license…”
The IoT Definitions license comeswith the Attack Surface Security Rating serviceand is used for:
Scanning connected devices
Identifying IoT/endpoint vulnerabilities
Reporting vulnerability severity

Enabling NAC-based remediation (VLAN steering, port isolation)
In LAN Edge Architect, this license combination is emphasized as a foundational requirement for:
FortiSwitch NAC
FortiLink device profiling
Automated quarantine actions
IoT device classification
Vulnerability-based segmentation
3.
Why the Correct Answer Is Option D OptionDlists:
✓FortiGuard Attack Surface Security
✓FortiGuard IoT Detection
These are exactly the services required per FortiOS 7.4.1:
Attack Surface Security Rating→ provides IoT signature package + vulnerability data IoT Detection (Definitions)→ enables actual device-type and vulnerability identification
Together they powerFortiLink Device DetectionandIoT Vulnerability Detection, which are essential LAN Edge security functions.
4.
Why Other Options Are Incorrect
A. Vulnerability Management + Endpoint Protection
Not used for FortiLink device detection; Endpoint detection relies on IoT service, not FortiClient.
B. Threat Intelligence + IoT Detection
Threat Intelligence (ThreatIntel DB) is used for FAZ IOC, not LAN Edge device detection.
C. Threat Intelligence + Endpoint Protection
Same issue—does not provide IoT device classification or vulnerability scanning.
LAN Edge 7.6 Architect Context Summary
In LAN Edge designs:
FortiGate acts as the controller for FortiSwitch via FortiLink.
Device detection is done at the FortiGate level using NAC/IoT signature capabilities.
Vulnerability detection enables dynamic segmentation decisions (e.g., move device to quarantine VLAN).
To support this, two licenses aremandatory:
Attack Surface Security(includes Security Rating + IoT Detection DB)
IoT Detection(part of the same entitlement, but explicitly required for vulnerability detection)
Thus the verified answer aligns perfectly with LAN Edge operational requirements and Fortinet documentation.

3.Refer to the exhibits.

VAP configuration

```
config wireless-controller vap
    edit "Corporate"
        set ssid "Corp"
        set security wpa2-only-enterprise
        set auth radius
        set radius-server "FAC-Lab"
        set intra-vap-privacy enable
        set schedule "always"
        set vlan-pooling wtp-group
        config vlan-pool
            edit 101
                set wtp-group "Floor_1"
            next
            edit 102
                set wtp-group "Office"
            next
        end
    next
end
```

Wi-Fi zone table

The exhibits show the VAP configuration. Wi-Fi SSIDs. and zone table.
Which two statements describe how FortiGate handles VLAN assignment for wireless clients? (Choose two.)
A. FortiGate will load balance clients using VLAN 101 and VLAN 102 and assign them an IP address from the 10.0.3.0/24 subnet.
B. All clients connecting to the Corp Zone will receive an IP address from the 10.0.20.0/24 subnet.
C. Clients connecting to APs in the Floor 1 group will not be able to receive an IP address.
D. Clients connecting to APs in the Office group will be assigned to VLAN 102.
Answer: C,D
Explanation:
The VAP configuration clearly showsVLAN pooling using WTP-groups:
set vlan-pooling wtp-group

config vlan-pool
edit 101
set wtp-group "Floor_1"
edit 102
set wtp-group "Office"
How VLAN assignment works in this mode
VLAN-pooling with wtp-group modemeans:
Each AP group (WTP group) is tied to exactly one VLAN in the pool.
The FortiGate doesnot load balanceVLANs.
Instead, VLANs are mappedper AP group, not per client.
Now verify each answer option:
A. FortiGate will load balance clients using VLAN 101 and 102...
❌Incorrect.
FortiGatedoes NOT load-balance clientswhen vlan-pooling is set towtp-group.
Each AP group receivesonly the VLAN mapped to it.
B. All clients in the Corp zone get IPs from 10.0.20.0/24
❌Incorrect.
In the Wi-Fi zone table, onlyCorp.102has an IP subnet:
Corp.101 →0.0.0.0/0.0.0.0(no IP assigned → clients get no DHCP)
Corp.102 →10.0.20.1/255.255.255.0
Thus, clients associated to VLAN 101cannotget IPs.
C. Clients connecting to APs in the Floor_1 group cannot receive an IP address
✓Correct.
Reason:
Floor_1 WTP-group → VLAN101
VLAN 101 hasno IPin the Wi-Fi table →0.0.0.0/0.0.0.0
No DHCP =Clients receive no IP address
D. Clients connecting to APs in the Office group will be assigned to VLAN 102
✓Correct.
Reason:
Office WTP-group maps to VLAN102
VLAN 102 has subnet10.0.20.0/24
So Office group clients get an IP in that range

4.You've configured the FortiLink interface, and the DHCP server is enabled by default.
The resulting DHCP server settings are shown in the exhibit.

```
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
```

What is the role of the vci-string setting in this configuration?

A. To ignore DHCP requests coming from FortiSwitch and FortiExtender devices.

B. To restrict the IP address assignment to devices that have FortiSwitch or FortiExtender as their hostname.

C. To connect, devices must match the VCI string; otherwise, they will not receive an IP address.

D. To reserve IP addresses for FortiSwitch and FortiExtender devices.

Answer: C

Explanation:

The DHCP configuration shows:

set vci-match enable

set vci-string "FortiSwitch" "FortiExtender"

What this means

VCI = Vendor Class Identifier (DHCP option 60)

When vci-match is enabled, the DHCP server will only respond to DHCP requests from clients whose VCI string matches the configured vendor identifiers.

FortiSwitch and FortiExtender both send DHCP option 60 with:

"FortiSwitch"

"FortiExtender"

This is used in FortiLink deployments so only these devices receive IP addresses on the FortiLink network.

Therefore:

C. To connect, devices must match the VCI string; otherwise, they will not receive an IP address.

✓Correct.

This perfectly matches FortiGate FortiLink DHCP behavior.

Summary of incorrect options

A — Ignore FortiSwitch/FortiExtender

❌Opposite behavior.

B — Restrict based on hostname

❌VCI does NOT check hostname.

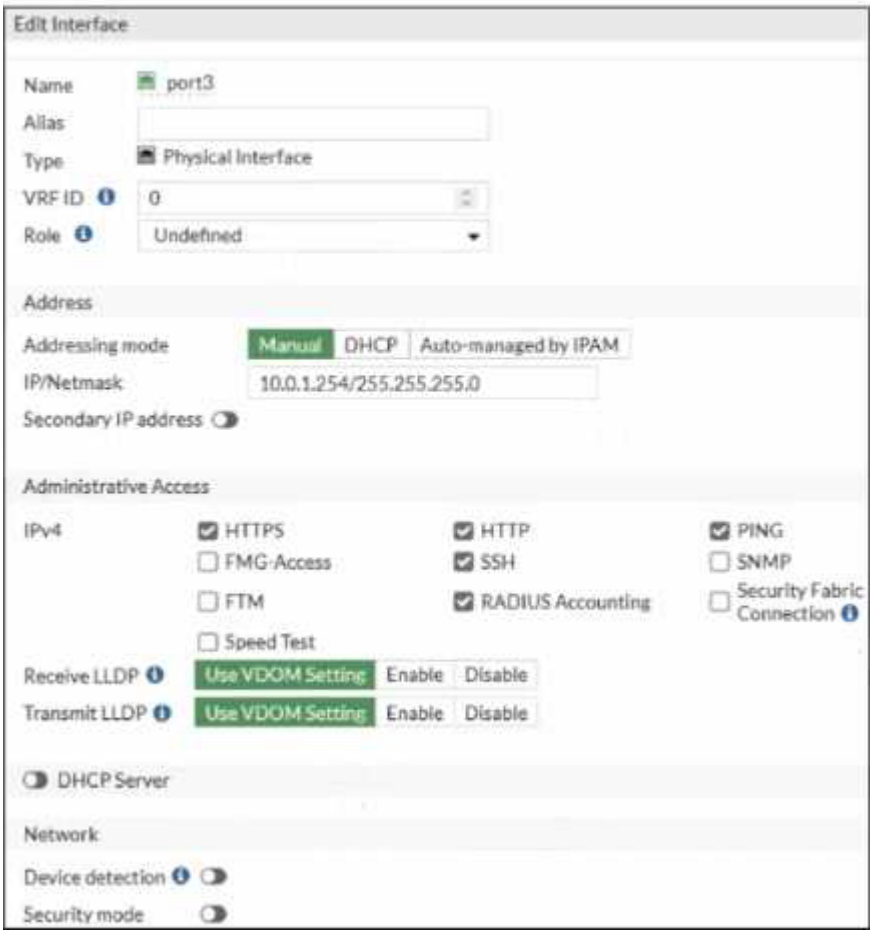
D — Reserve IPs

❌No reservation occurs; it's filtering, not reserving.

5.Refer to the exhibits.

FortiGate RSSO configuration

FortiGate interface configuration



Examine the FortiGate RSSO configuration shown in the exhibit.

FortiGate is set up to use RSSO for user authentication. It is currently receiving RADIUS accounting messages through port3. The incoming RADIUS accounting messages contain the username in the User-Name attribute and group membership in the Class attribute. You must ensure that the users are

authenticated through these RADIUS accounting messages and accurately mapped to their respective RSSO user groups.
Which three critical configurations must you implement on the FortiGate device? (Choose three.)
A. The RADIUS Attribute Value setting configured for an RSSO user group should match the class RADIUS attribute value in the RADIUS accounting message.
B. RSSO user groups should be assigned to all firewall policies.
C. Device detection and Security Fabric Connection should be enabled on port3
D. The sso-attribute CLI setting in the RSSO agent configuration should be set to Class.
E. The rsso-endpoint-attribute CLI setting in the RSSO agent configuration should be set to User-Name.
Answer: A,D,E
Explanation:
The problem states:
FortiGate receivesRADIUS accounting messagesonport3.
User-Nameattribute contains the username.
Classattribute contains the group membership.
Goal: authenticate users through RSSO and map them to the correct user groups.
To achieve this, three critical components must be configured:
✓A. RADIUS Attribute Value in the RSSO group must match the Class attribute
This is mandatory because:
RSSO user groups on FortiGate match users based onthe value inside the RADIUS attribute(usually Class).
For group assignment to work, FortiGate must compare:
RSSO User Group → RADIUS Class Attribute Value
This isexactly how FortiGate maps RSSO users to groups.
✓D. RSSO agent's sso-attribute must be set to Class Thesso-attributedefineswhich RADIUS attribute contains the group information. Because group membership is carried in: ➞Class attribute
You must configure:
config user radius
set sso-attribute Class
end
This tells FortiGate:
"Use the Class attribute to derive user group membership."
✓E. rsso-endpoint-attribute must be set to User-Name
This identifieswhich RADIUS attributecarries the actualusername.
In this scenario:
RADIUS accounting messages contain the username inUser-Name.
So the correct setting is:
config user radius
set rsso-endpoint-attribute User-Name
end
This ensures the RSSO user object uses the correct username.
❌Incorrect Options Explained
B. Assign RSSO user groups to all firewall policies
Not required.

You only assign them to policies where RSSO authentication is used.
C. Device detection and Security Fabric Connection should be enabled on port3 Totally irrelevant to RSSO.
RSSO only needs RADIUS accounting, not device detection or Fabric services.