Question #1 *Topic 1*

What is the primary benefit of the LAN Edge solution?

A. It integrates wired networking with advanced firewall capabilities.

B. It focuses on enhancing wireless network performance.

C. It provides centralized management, simplifies operations, and uses AI/ML.

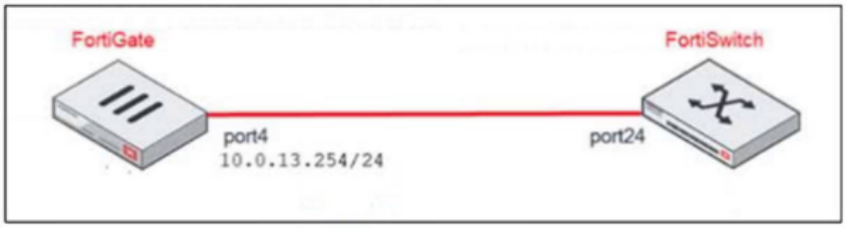
D. It supports scalable and adaptable networking.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Refer to the exhibits.

Network topology



FortiSwitch status

Name	Switch Group	Status	Model
FortiLink: fortilink (1)			
FortiSwitch		Offline	FortiSwitch 224E-POE

fortilink interface settings in FortiGate

```
FortiGate (fortilink) # show
config system interface
    edit "fortilink"
        set vdom "root"
        set fortilink enable
        set ip 10.0.13.254 255.255.255.0
        set allowaccess ping fabric
        set type aggregate
        set member "port4"
        set device-identification enable
        set lldp-reception enable
        set lldp-transmission enable
        set role lan
    set snmp-index 14
    set auto-auth-extension-device enable
    set ip-managed-by-fortiipam disable
    set switch-controller-nac "fortilink"
    set switch-controller-dynamic "fortilink"
    set swc-first-create 255
    set lacp-mode static
next
```

IP server setting for fortilink

```
configsystem dhcp server
   edit 1
       set dns-service default
       set ntp-service local
       set default-gateway 10.0.13.254
       set netmask 255.255.255.0
       set interface "fortilink"
       config ip-range
           edit 1
               set start-ip 10.0.13.1
               set end-ip 10.0.13.253
           next
       end
       set vci-match enable
       set vci-string "FortiExtender"
   next
```

You are adding a new FortiSwitch to FortiGate for management. All necessary settings have been configured on FortiGate, but FortiSwitch remains offline. The cabling has been verified and is correctly connected.

Which misconfiguration might be preventing FortiGate from detecting FortiSwitch?

A. The DHCP server setting vci-string is misconfigured.

B. The Fortilink interface has the wrong interface member.

C. The Fortilink interface setting ip-managed-by-fortiipam must be enabled.

D. The Fortilink interface setting type must be physical.

Suggested Answer: *D*

Community vote distribution

A (100%)

64019f4 1 week, 1 day ago

Selected Answer: A

I agree. Correct answer is A

upvoted 1 times

krian 1 month, 1 week ago

Selected Answer: A

En el DHCP server de la interfaz FortiLink tienes vci-match enable con vci-string "FortiExtender". Un FortiSwitch envía el VCI "FortiSwitch"; al no coincidir, no recibe IP (ni las opciones para discovery), por lo que el FortiGate no lo detecta y queda offline

upvoted 3 times

Refer to the exhibits.

FortiGate VLAN AP settings

```
config system interface
    edit "APs"
        set vdom "root"
        set ip 10.10.100.254 255.255.255.0
        set allowaccess ping
        set alias "AP Management"
        set device-identification enable
        set role lan
        set snmp-index 118
        set ip-managed-by-fortiipam disable
        set interface "fortilink"
        set vlanid 100
    next
end
```

DHCP configuration

```
config system dhcp server
    edit 7
        set dns-service default
        set default-gateway 10.10.100.254
        set netmask 255.255.255.0
        set interface "APs"
        config ip-range
            edit 1
                set start-ip 10.10.100.1
                set end-ip 10.10.100.253
            next
        end
    next
end
```

FortiSwitch port1 VLAN AP assignment

```
        set dns-service default
        set default-gateway 10.10.100.254
        set netmask 255.255.255.0
        set interface "APs"
        config ip-range
            edit 1
                set start-ip 10.10.100.1
                set end-ip 10.10.100.253
            next
        end
    next
end
```

FortiSwitch port1 VLAN AP assignment

```
config switch-controller managed-switch
    edit "FortiSwitch"
        set sn "S224EPTF19006016"
        set fsw-wan1-peer "fortilink"
        set fsw-wan1-admin enable
        set poe-detection-type 2
        set version 1
        set max-allowed-trunk-members 8
        set pre-provisioned 1
        set dynamic-capability 0x0000000000000000155102775 7dddfff7
        config ports
            edit "port1"
                set poe-capable 1
                set vlan "APs"
                set allowed-vlans "VLAN102" "VLAN101" "quarantine"
                set untagged-vlans "quarantine"
                set export-to "root"
                set mac-addr 04:d5:90:39:7d:8e
            next
```

A FortiSwitch is successfully managed by FortiGate. FortiAP is connected to port1 of the managed FortiSwitch.
On FortiGate, the VLAN AP is configured to detect and manage FortiAP, along with a DHCP server for the VLAN AP. Additionally, the VLAN AP is assigned to port1 of FortiSwitch.
However, FortiGate is unable to detect or manage FortiAP.
Which FortiGate misconfiguration is preventing the detection of FortiAP?

A. The VLAN is not tagged correctly on the FortiSwitch uplink port.

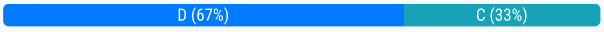
B. The FortiAP firmware is incompatible with the FortiGate firmware version.

C. The CAPWAP ports (UDP 5246 and 5247) are not open on FortiGate.

D. Security Fabric is disabled in the administrative access options of the VLAN.

Suggested Answer: *D*

Community vote distribution



Kanno 3 weeks, 1 day ago

Selected Answer: D

Indeed CAPWAP must me enabled on the VLAN but by default in the quarantine VLAN it is diabled so in the case shown on the exibits the corect answer is D because by default the CAPWAP ports are open on the FortiGate VLANs/Ports with Security Fabric Connection option enabled.

upvoted 2 times

33c70fb 4 weeks, 1 day ago

Selected Answer: D

ES LA D, porque al activar Security Fabric, activa CAPWAP en la interfaz

upvoted 4 times

viotech 1 month, 2 weeks ago

Selected Answer: C

The CAPWAP port must be enabled to detect the AP : correct answer is C

upvoted 3 times

Question #4 *Topic 1*

You need to optimize your wireless network to improve performance and reliability in a dynamic environment. The network must adapt to changes in the radio frequency (RF) environment, such as interference, new devices, and fluctuating traffic patterns.
Which role does FortiAIOps play in monitoring and automatically adjusting to changes in the radio frequency (RF) environment?

A. To detect and report interference and congestion, helping to optimize wireless performance and coverage

B. To limit the number of devices connected to each access point in a given area

C. To increase the signal strength of the network if required by modulating power levels on all access points

D. To monitor network traffic and recommend firewall rules in real time

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

You have decided to manage multiple FortiSwitch devices using FortiManager and its FortiSwitch Manager feature.
Which two statements accurately describe FortiSwitch Manager feature functionality? (Choose two.)

A. FortiSwitch Manager displays the following statuses for FortiSwitch: online, offline, unauthorized, and unknown.

B. Per-device management is useful for deploying multiple switches with the same configuration.

C. FortiSwitch Manager displays the following statuses for FortiSwitch: active, inactive, pending, and unknown.

D. In per-device management mode, you apply settings and profiles to individual FortiSwitch devices.

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

In public key infrastructure (PKI), what is the primary role of a certificate revocation list (CRL)?

A. To enable certificate authorities to update certificates with new public key information.

B. To list expired certificates and ensure they are not used for encryption.

C. To provide information about the revocation status of certificates in real time.

D. To maintain a list of certificates that have been revoked by the certificate authority (CA) before their expiration date.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

A conference center wireless network provides guest access through a captive portal, allowing unregistered users to self-register and connect to the network.
The IT team has been tasked with updating the existing configuration to enforce captive portal authentication over a secure HTTPS connection.
Which two steps should the administrator take to implement this change? (Choose two.)

A. Enable HTTP redirect in the user authentication settings.

B. Update the captive portal URL to use HTTPS on FortiGate and FortiAuthenticator.

C. Create a new SSID with the HTTPS captive portal URL.

D. Disable HTTP administrative access on the guest SSID to enforce HTTPS connection.

Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

Which two broad categories must be considered for wireless troubleshooting when evaluating key wireless metrics?

A. Wireless range and network speed

B. Signal interface and device compatibility

C. Network reliability and signal interference

D. Wireless health and wireless capacity

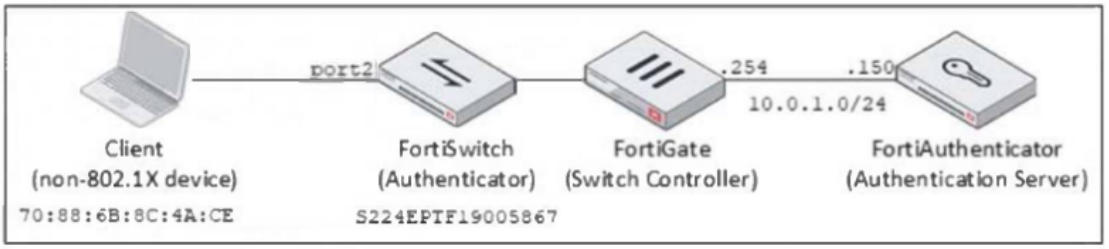
Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

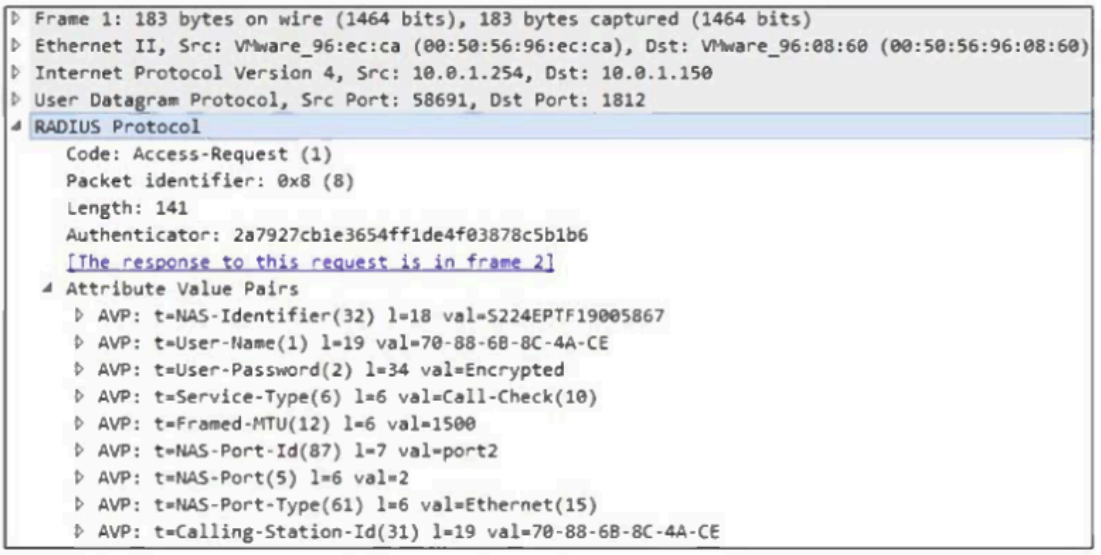
Question #9 *Topic 1*

Refer to the exhibits.

Network diagram



Packet capture output



Examine the network diagram and packet capture shown in the exhibit.

During packet capture analysis, a RADIUS Access-Request packet was detected being sent from FortiSwitch to FortiAuthenticator and passing through FortiGate. The capture shows that the User-Name attribute in the RADIUS Access-Request packet contains the client MAC address.

Why is the client MAC address contained in the User-Name attribute of the RADIUS Access-Request packet?

A. FortiAuthenticator is authenticating the client based on the device hostname.

B. FortiAuthenticator is performing machine authentication

C. MAC address-based authentication is being used for the client through MAC Authentication Bypass (MAB).

D. FortiGate is authenticating the client using 802.1X authentication.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

How does the Syslog-based single sign-on (SSO) feature in FortiAuthenticator function to correlate user activity with authentication events across multiple network devices?

A. It uses syslog messages to monitor authentication events and correlate them with user activities.

B. It modifies user credentials based on the outcome of authentication events.

C. It relies on external servers to analyze syslog messages for user authentication.

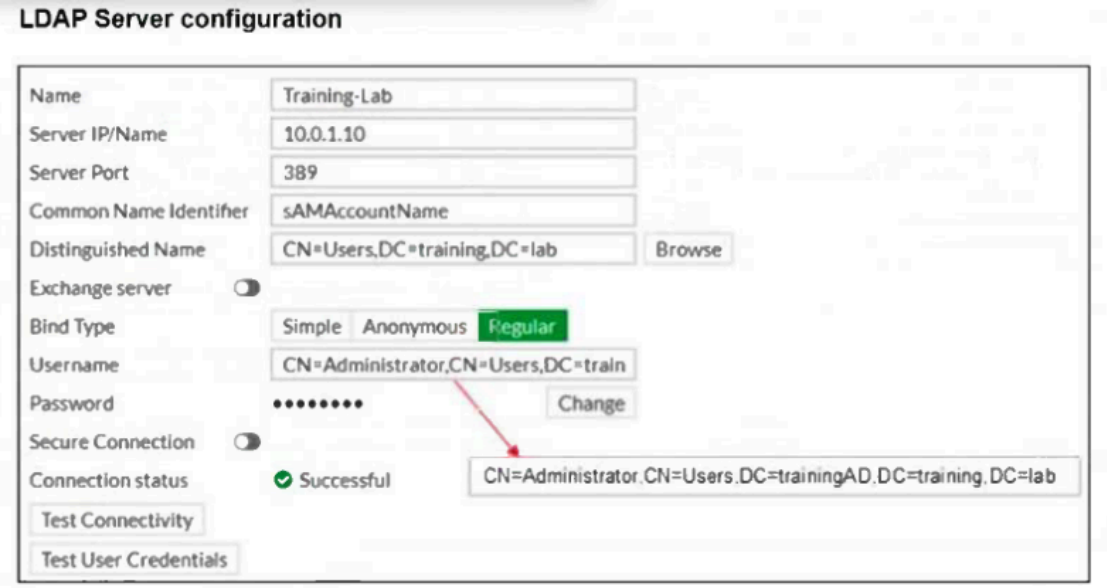
D. It authenticates users through a captive portal by monitoring login attempts.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

Refer to the exhibit.



The exhibit shows an LDAP server configuration with the Username setting has been expanded to display its full content.
The administrator has configured the LDAP settings on FortiGate and is troubleshooting for authentication issues.
As part of the troubleshooting steps, the administrator runs the command dsquery user -samid student on the Windows Active Directory (AD) server with an IP address 10.0.1.10 and received the output CN=student, CN=Users, DC=trainingAD, DC=training, DC=lab.
Based on the dsquery output, which LDAP setting on FortiGate is misconfigured?

A. The Common Name Identifier is incorrectly set, causing authentication failures.

B. The Bind Type is incorrectly configured, preventing FortiGate from connecting to the LDAP server.

C. The Distinguished Name setting is incorrectly configured, causing issues with user authentication.

D. Sever IP/Name is misconfigured so FortiGate can't reach the LDAP server.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

In a Windows environment using AD machine authentication, how does FortiAuthenticator ensure that a previously authenticated device is maintaining its network access once the device resumes operating after sleep or hibernation?

A. It sends a wake-on-LAN packet to trigger reauthentication.

B. It caches the MAC address of authenticated devices for a configurable period of time.

C. It temporarily assigns the device to a guest VLAN until full reauthentication is completed.

D. It uses machine authentication based on the device IP address.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

You are troubleshooting an issue where users are being intermittently redirected to an error page after submitting their login credentials on a captive portal. As part of your troubleshooting steps, you review the POST parameters sent from the client to the authentication server.
What should you check in the magic ID within the POST parameters to help resolve the issue?

A. Determine whether the magic ID has expired, which could cause the server to reject the authentication request.

B. Validate that the magic ID contains encryption keys for securing the user's password during transmission.

C. Verify whether the magi ID matches the session generated by the server to ensure the request is valid.

D. Confirm that the magic ID is tied to the correct redirection URL for the user session.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

You need to deploy FortiAPs at remote locations and want to avoid high latency by minimizing interference from FortiGate.
Which SSID traffic mode is best suited for this deployment?

A. Hybrid mode

B. Local mode

C. Bridge mode

D. Tunnel mode

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

When troubleshooting a FortLink connectivity issue between FortiGate and FortiSwitch, why is it important to verify their time and date settings?

A. Time synchronization is critical for the CAPWAP DTLS tunnel.

B. Time and date are used to determine the encryption algorithm on FortiLink.

C. Incorrect time synchronization may disrupt the FortiLink discovery protocol (LLDP or MCLAG).

D. Matching time settings ensure proper STP convergence on the FortiLink interface.

Suggested Answer: *A*

Community vote distribution

C (100%)

Owie 3 weeks, 5 days ago

Selected Answer: C

Pg 323 study guide - It disrupt the FortiLink Connection

upvoted 2 times

Question #16 *Topic 1*

In which two ways is layer 2 isolation applied to a quarantined device? (Choose two.)

A. By configuring route policy rules to restrict traffic.

B. By blocking communication based on the device's MAC address.

C. By blocking communication based on the device's IP address.

D. By assigning a null route based on the device's IP address.

E. By assigning the quarantined device to a separate VLAN.

Suggested Answer: *BE*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

A network administrator is configuring a RADIUS server on FortiGate to authenticate remote users. The administrator configures FortiGate to forward authentication requests to FortiAuthenticator, which then proxies these requests to a Windows Active Directory (AD) server using LDAP. Which is the primary benefit of using FortiAuthenticator in this configuration?

A. FortiAuthenticator encrypts the RADIUS authentication traffic between FortiGate and the AD server, securing communication.

B. This configuration provides a solution to the CHAP-to-LDAP dilemma, enabling MSCHAPv2 authentication.

C. FortiAuthenticator simplifies the configuration by allowing FortiGate to use LDAP directly for authentication without the need for RADIUS.

D. The configuration allows FortiGate to directly authenticate remote users against Windows Active Directory without the need for an intermediate proxy.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

A network administrator is deploying a new FortiGate firewall and wants to enable zero-touch provisioning with FortiManager. The administrator has not manually configured the FortiManager IP address or FQDN on FortiGate. However, FortiGate can still discover FortiManager automatically. In this situation, where can FortiGate learn the FortiManager IP address or FQDN for zero-touch provisioning?

A. By retrieving options 240 or 241 from a DHCP server

B. By querying the local ARP table for the FortiManager IP address.

C. By the default static route configuration on FortiGate.

D. By checking the FortiGate factory default configuration.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

What is the primary purpose of configuring an untagged VLAN on a FortiSwitch port in a network deployment?

A. To enable features like quarantine MAC or dynamic VLAN assignment.

B. To carry multiple VLANs on a single port.

C. To enable QoS (quality of service) on the port.

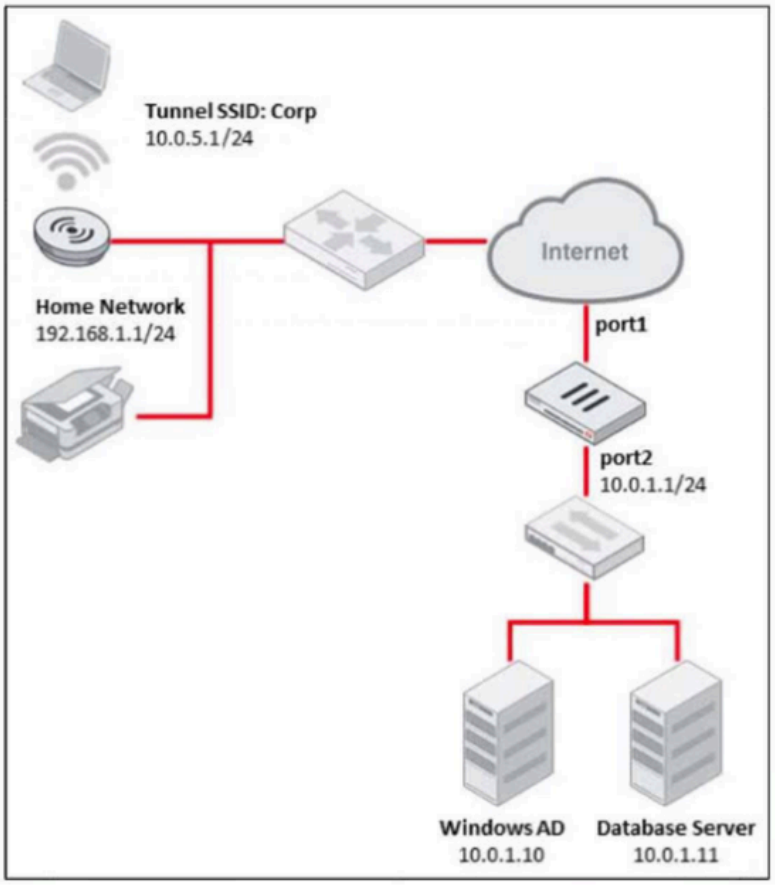
D. To automatically tag traffic from connected devices.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Refer to the exhibits.

Network diagram



VAP configuration

```
config wireless-controller wtp-profile
    edit "S231F"
        config platform
            set type 231F
        end
        set handoff-sta-thresh 30
        set ap-country US
        config radio-1
            set band 802.11n-2G 802.11ax-2G
            set auto-power-level enable
            set auto-power-high 20
            set darrp enable
            set arrp-profile "arrp-default"
            set vap-all manual
            set vaps "EmployeeHome"
            set channel "3" "5" "8"
        end
        config radio-2
            set band 802.11ac-5G
            set channel-bonding 40MHz
            set auto-power-level enable
            set darrp enable
            set arrp-profile "arrp-default"
            set vap-all manual
            set vaps "EmployeeHome"
            set channel "36" "44" "52"
        end
        config radio-3
            set mode monitor
        end
    next
end
```

The exhibits show the WTP profile and VAP CLI configurations on FortiGate managing a remote AP.
The AP is designed to grant a remote employee access to company network resources, including the database and AD servers. The employee can reach company resources but is unable to access a local printer at home.
What two solutions are required to fix this issue? (Choose two.)

A. Configure the S231F wtp-profile to add a split tunneling ACL with a destination subnet of 192.168.1.1/24, using the command set dest-ip 192.168.1.1/24

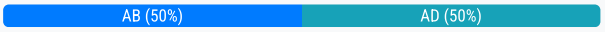
B. Configure the EmployeeHome VAP profile for local bridging using the command set local-bridging enable.

C. Configure the EmployeeHome VAP profile to disable host isolation using the command set intra-vap-privacy disable.

D. Configure the S231F wtp profile to enable split tunneling to the AP subnet using the command set split-tunneling-acl-local-ap-subnet enable.

Suggested Answer: *AD*

Community vote distribution



Teso80 3 weeks, 6 days ago

Selected Answer: AD

https://docs.fortinet.com/document/fortiap/7.4.2/fortiwifi-and-fortiap-configuration-guide/238787/remote-wlan-fortiaps
"
To override the split tunneling settings on a FortiAP:
If the FortiAP Profile split tunneling settings are not appropriate for a particular FortiAP, you can override the settings on that unit.

config wireless-controller wtp

edit FAP321C3X14019926

set override-split-tunnel enable

set split-tunneling-acl-local-ap-subnet enable

config split-tunneling-acl

edit 1

set dest-ip 192.168.10.0 255.255.255.0

end

end
"
upvoted 1 times

33c70fb 4 weeks ago

Selected Answer: AB

RESPUESTAS A Y B

Split tunneling (Opción A)

Permite que el tráfico destinado a la red local del usuario (por ejemplo, 192.168.1.0/24) no pase por el túnel corporativo, sino que se enrute directamente en la red doméstica.

Local bridging (Opción B)

Habilita que el tráfico de la VLAN virtual del AP pueda comunicarse localmente en la LAN del usuario, permitiendo acceder a la impresora y otros dispositivos locales.