Examens : Réseau sans fil sécurisé

Comprendre l'administration de WLAN

Dans le monde actuel, les réseaux sans fil sont omniprésents. Leur **bonne administration** est essentielle pour garantir leur efficacité et leur sécurité. Dans cet article, nous allons explorer l'administration des réseaux **WLAN**, avec un accent particulier sur la sécurité.

Pourquoi choisir une sécurité des réseaux sans fil ?

La **santé** des réseaux sans fil est primordiale pour éviter des **accès non autorisés**. Des informations sensibles peuvent être compromises si le réseau n'est pas correctement sécurisé. Une bonne pratique consiste à utiliser des **protocoles robustes** qui protègent contre les menaces.

Voici comment configurer votre WLAN

Configurer un réseau WLAN ne doit pas être compliqué. Tout d'abord, accédez au *panneau d'administration* de votre routeur. Assurez-vous de :

- **Modifier le SSID**
- **Choisir un mot de passe fort**
- **Désactiver le SSID broadcast** pour plus de sécurité

Gestion des utilisateurs WLAN

Un aspect crucial de l'administration de WLAN est **la gestion des utilisateurs**. Il est essentiel de savoir qui a accès au réseau et de limiter l'accès aux personnes autorisées. Pour cela, utilisez des fonctionnalités comme le **filtrage MAC**.

Protocoles de sécurité sans fil recommandés

Il existe plusieurs protocoles de sécurité pour protéger votre réseau sans fil. **WPA2** est l'un des plus recommandés, car il offre un niveau de sécurité élevé. Il est important de toujours se tenir à jour avec les *données de sécurité* les plus récentes. Pour en savoir plus,

consultez également ce lien.

Conseils pour sécuriser votre WLAN

En plus de configurer votre réseau correctement, voici quelques *conseils supplémentaires* :

- Maintenez le **firmware** de votre routeur à jour
- Utilisez un **réseau pour les invités** pour les visiteurs
- Surveillez régulièrement les **appareils connectés**

Conclusion

La **sécurité** de votre réseau sans fil est un enjeu majeur dans notre monde numérique. En suivant ces recommandations, vous pouvez garantir un **WLAN sûr** et **efficace** pour tous vos utilisateurs. L'administration correcte et proactive permet d'éviter de nombreux problèmes potentiels.

Fortinet

FCP_FWF_AD-7.4 Exam

FCP - Secure Wireless LAN 7.4 Administrator

Thank you for Downloading FCP_FWF_AD-7.4 exam PDF Demo

You can Buy Latest FCP_FWF_AD-7.4 Full Version Download

https://www.certkillers.net/Exam/FCP_FWF_AD-7.4

Version: 4.0

Question: 1

Refer to the exhibit.

Access Point	SSIDs	Channel	Clients	OS Version	FortiAP Profile	Connected Via
Online 2						
FP231FT	R1 All Tunnel Mode SSIDs R2 All Tunnel Mode SSIDs R3 N/A	R1 1 R2 140 R3 N/A	11	v7.4.2 build0634	FAP231F	APs
FP23JFT	R1 N/A R2 N/A R3 N/A	R1 N/A R2 N/A R3 N/A	0	v7.4.2 build0634	FAP23JF	APs

An administrator authorizes two FortiAP devices connected to this wireless controller However, one FortiAP is not able to broadcast the SSIDs. What must the administrator do to fix the issue?

A. Enable the radios on the FAP23JF FortiAP profile.
B. Replace the FortiAP device model to match the other device
C. Disable the override setting on the FortiAP that is preventing it from broadcasting SSIDs
D. Assign the FAP231F FortiAP profile to the problematic FortiAP device

Answer: A

Question: 2

How can you find the upstream and downstream link rates of a wireless client connected to a FortiAP?

A. On the FortiGate GUI using the WiFi Client monitor
B. On the FortiAP CLI using the cw_diag ksta command
C. On the FortiGate CL! using the diagnose wireless-controller wlac -d sta command
D. On the FortiAP CLI using the cw_diag -d sea command

Answer: B

Question: 3

Which two threats on wireless networks are detected by WIDS? (Choose two.)

A. Brute-force dictionary attacks
B. Unauthorized wireless connection
C. Rogue access points
D. WPA2 authentication vulnerabilities

Answer: B, C

Question: 4

When enabling a Security Fabric connection on a FortiGate interface to manage FortiAP devices, which two types of CAPWAP communication channels are established between FortiGate and the FortiAP devices'? (Choose two)

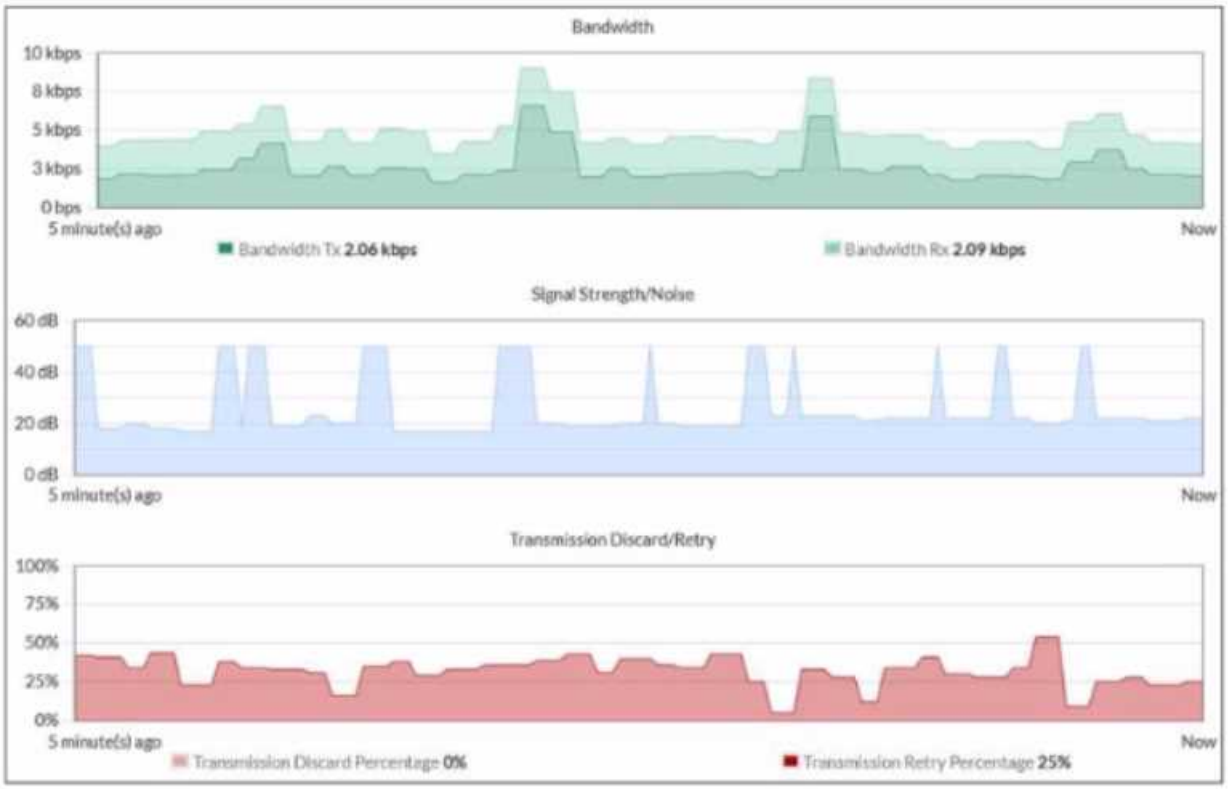
A. Control channels
B. Data channels
C. Security channels
D. Fortlink channels

Answer: A, B

Question: 5

Exhibit.

Performance monitor



Refer to the exhibit of a wireless client performance monitor Which performance metric is abnormal for this wireless client?

A. The wireless client has been experiencing high background noise within the last 5 minutes
B. The wireless client has been dropping half of the packets transmitted within the last 5 minutes.
C. The wireless client has been transmitting traffic with all performance metrics within the normal levels
D. The wireless client has been switching between available wireless bands within the last 5 minutes

Answer: B

Thank You for trying FCP_FWF_AD-7.4 PDF Demo

To Buy New FCP_FWF_AD-7.4 Full Version Download visit link below

https://www.certkillers.net/Exam/FCP_FWF_AD-7.4

Start Your FCP_FWF_AD-7.4 Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your FCP_FWF_AD-7.4 preparation with actual exam questions.