PRINCE TOGBLE

REALISATION

MISE EN PLACE DU WI-FI POUR LES EMPLOYÉS ET LES VISITEURS

RADIUS
WiFi

I. CONTEXTE

StadiumCompany est une société qui gère un grand stade.

Lors de la construction de ce stade, le réseau qui prenait en charge ses bureaux commerciaux et ses services de sécurité proposait des fonctionnalités de communication de pointe. Au fil des ans, la société a ajouté de nouveaux équipements et augmenté le nombre de connexions sans tenir compte des objectifs commerciaux généraux ni de la conception de l'infrastructure à long terme.

Certains projets ont été menés sans souci des conditions de bande passante, de définition de priorités de trafic et autres, requises pour prendre en charge ce réseau critique de pointe. À présent, la direction de StadiumCompany veut améliorer la satisfaction des clients en ajoutant des fonctions haute technologie et en permettant l'organisation de concerts, mais le réseau existant ne le permet pas.

La direction sait qu'elle ne dispose pas du savoir-faire nécessaire pour mener cette mise à niveau.
Elle décide donc de faire appel à des consultants réseau pour :

- concevoir la nouvelle architecture,
- gérer le projet,
- mettre en œuvre la solution.

Le projet se déroule en **trois phases**, dont la première consiste à planifier et préparer la conception réseau de haut niveau.

Besoin de la mission

Actuellement, le stade possède un accès aux différentes ressources de StadiumCompany (fichiers, impression, internet, bases de données…).
Mais cet accès n'est possible **qu'en filaire**.

La direction souhaite étendre cet accès aux services équipés d'un terminal WiFi.

StadiumCompany a acquis :

- plusieurs switchs PoE,
- des bornes WiFi Cisco.

Vous êtes chargé :

- d'implémenter une solution WiFi pour les salariés,
- d'implémenter un accès WiFi sécurisé pour les visiteurs (internet uniquement).

Cahier des charges :

- Chaque service dispose d'un AP 802.11 b/g/n PoE.
- SSID non diffusé par VLAN (sauf VLAN visiteurs).
- Confidentialité assurée par **WPA2 Enterprise**, puis renforcement ultérieur.
- Authentification des salariés via le réseau sans fil.
- Accès visiteurs limité à Internet.

Phase 1

- Proposer une solution d'infrastructure réseau et système permettant l'accès sans fil aux salariés et visiteurs sans interruption de service.
- Proposer un schéma réseau logique et physique.
- Définir la démarche et l'ordonnancement des tâches.

Phase 2

- Configurer le matériel et les systèmes nécessaires.
- Proposer une batterie de tests pour valider l'infrastructure.
- Documentation technique sur les switchs et AP.
- Documentation technique sur le cryptage des données.

II. SOLUTIONS

1 – Authentification utilisateur

Pour le réseau des visiteurs médicaux, nous utilisons un **serveur RADIUS**.

RADIUS (Remote Authentication Dial-In User Service) est un protocole client-serveur permettant de **centraliser les données d'authentification**.

Fonctionnement :

1. Le poste utilisateur envoie une requête d'accès au client RADIUS.
2. Le client demande les informations d'identification (login + mot de passe).
3. Le client RADIUS transmet une requête d'accès au serveur RADIUS.
4. Le serveur, couplé à l'annuaire AD, valide ou refuse l'accès.

2 – Sécurité des communications

WPA2 propose deux types de chiffrement :

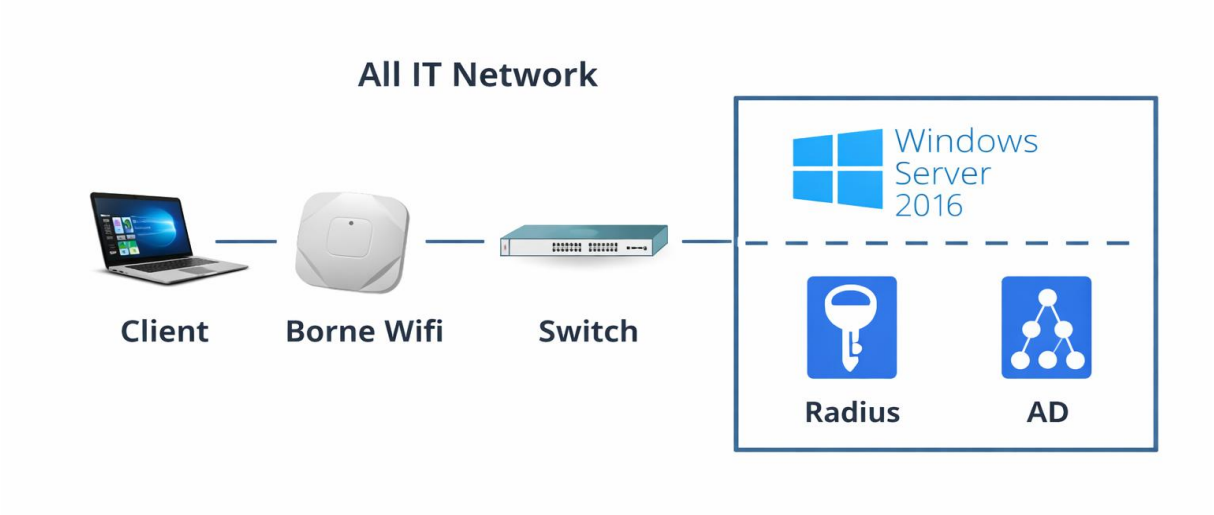
TKIP (Temporal Key Integrity Protocol)

- Authentification + protection des données
- Génère une clé par paquet
- Mélange les paquets pour assurer l'intégrité
- Hérité de WEP → moins sécurisé, plus lourd

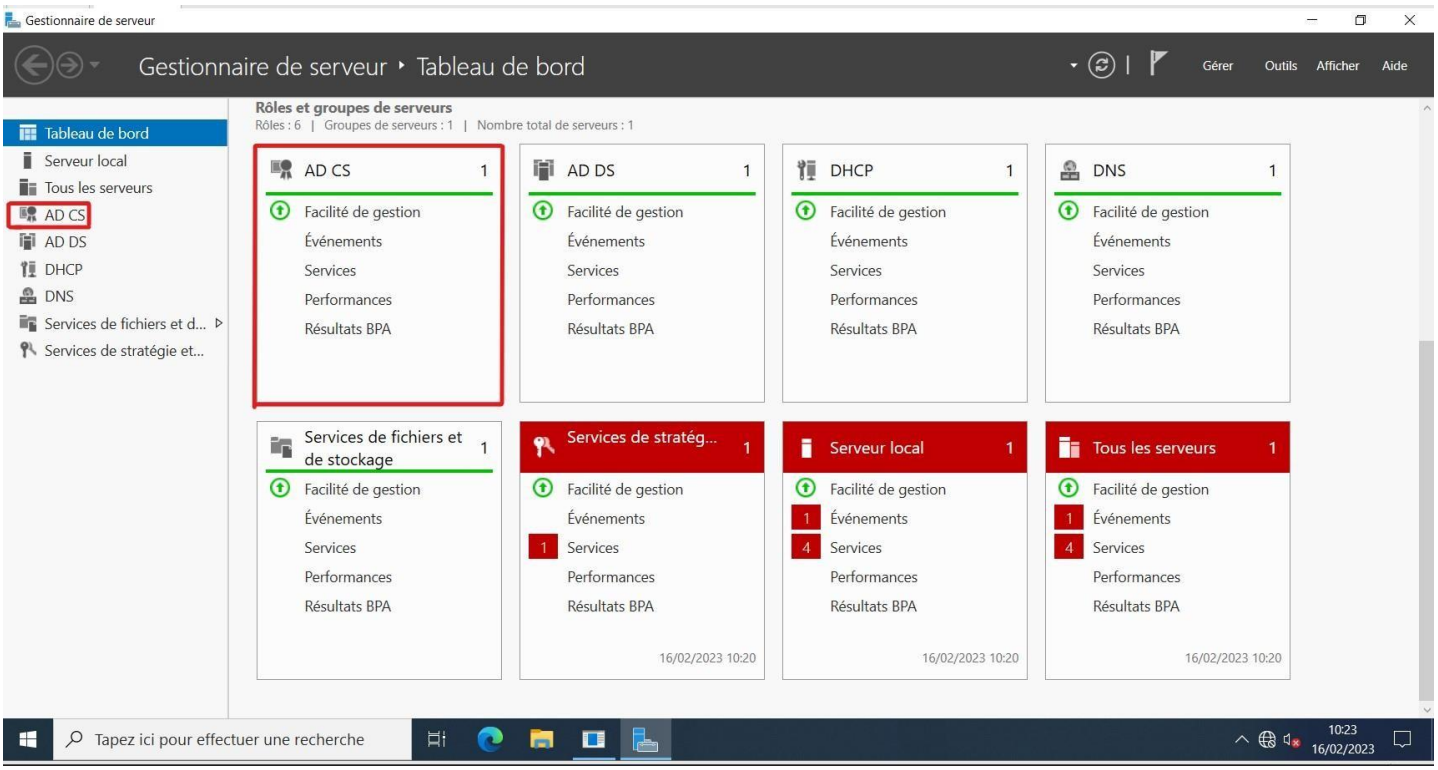
AES (Advanced Encryption Standard)

- Chiffrement symétrique moderne
- Très sécurisé
- Peu de ressources nécessaires
- Recommandé pour WPA2 Enterprise

3 – Schéma réseau



III- Mise en place



1 - Mise en place de l'autorité de certification (CA) sur l'Active Directory

```
!
hostname SW-SERVER
!
!
no aaa new-model
ip subnet-zero
!
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface GigabitEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet0/3
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet0/4
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet0/5
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet0/6
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet0/7
```

2 – Configuration du switch

3 – Configuration du routeur / AP Cisco

```
username Cisco password 7 05280F1C2243
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode wep mandatory
 !
 ssid wifi-stade-elliot
 !
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 !
 encryption mode wep mandatory
 !
 ssid wifi-stade-elliot
 !
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
```



```
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
 hold-queue 160 in
!
interface BVI1
 ip address 172.20.2.5 255.255.255.128
 no ip route-cache
!
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
radius-server attribute 32 include-in-access-req format %h
radius-server host 172.20.0.10 auth-port 1645 acct-port 1646 key 7 15301F1F567A7977
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
!
end
```

4 – Configuration AP

```
Building configuration...

Current configuration : 2506 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
enable secret 5 $1$l3Lk$xIjgNwwvhpoGhWzSrvzBY.
!
ip subnet-zero
ip domain name corp.stadiumcompany.com
ip name-server 8.8.8.8
!
!
aaa new-model
!
!
aaa group server radius rad_eap
 server 172.20.0.10 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
```

```
!
username Cisco password 7 05280F1C2243
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode wep mandatory
 !
 ssid wifi-stade-elliot
 !
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 !
 encryption mode wep mandatory
 !
 ssid wifi-stade-elliot
 !
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
```

```
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
 hold-queue 160 in
!
interface BVI1
 ip address 172.20.2.5 255.255.255.128
 no ip route-cache
!
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
radius-server attribute 32 include-in-access-req format %h
radius-server host 172.20.0.10 auth-port 1645 acct-port 1646 key 7 15301F1F567A7977
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
!
end
```

IV. VERIFICATION

3 – Security

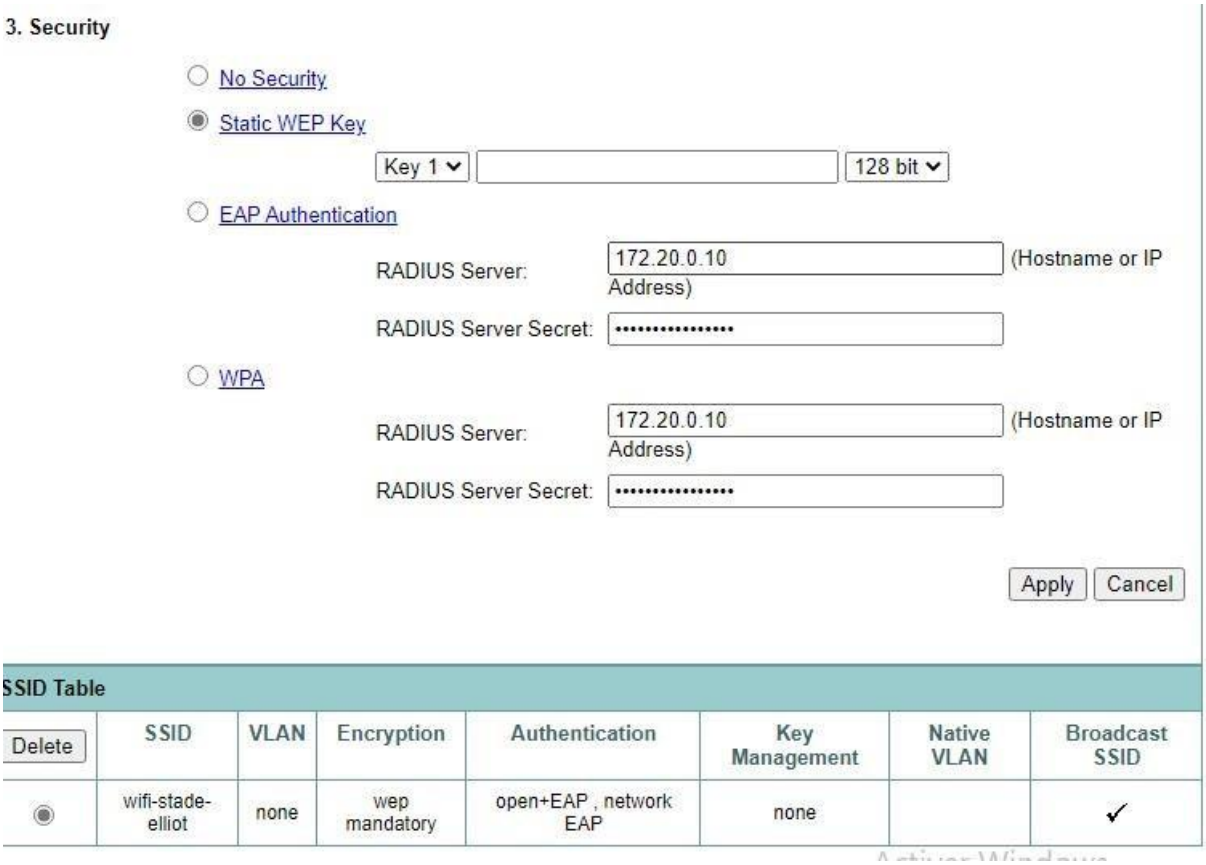
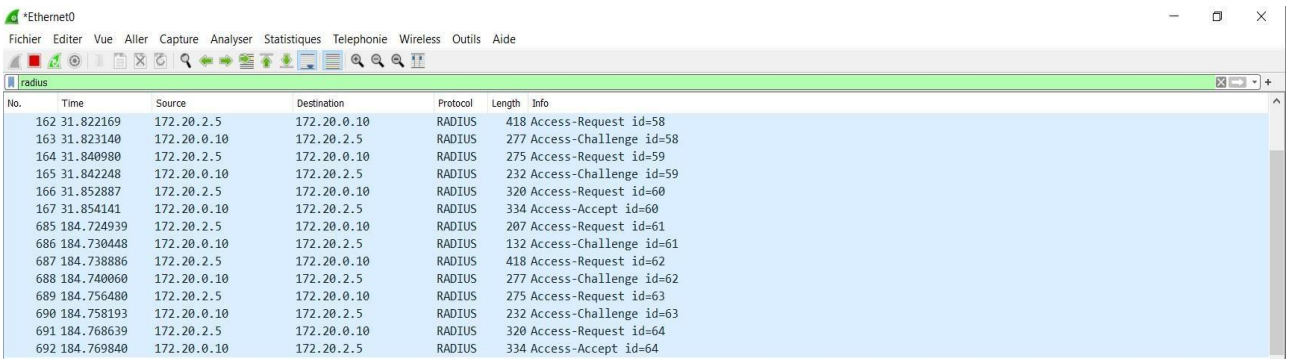


Table SSID

Delete	SSID	VLAN	Encryption	Authentication	Key Mgmt	Native VLAN	Broadcast
☒	wifi-stade-elliot	none	wep mandatory	open+EAP, network EAP	none		☒

Analyse de trame



No.	Time	Source	Destination	Protocol	Length	Info
162	31.822169	172.20.2.5	172.20.0.10	RADIUS	418	Access-Request id=58
163	31.823140	172.20.0.10	172.20.2.5	RADIUS	277	Access-Challenge id=58
164	31.840980	172.20.2.5	172.20.0.10	RADIUS	275	Access-Request id=59
165	31.842248	172.20.0.10	172.20.2.5	RADIUS	232	Access-Challenge id=59
166	31.852887	172.20.2.5	172.20.0.10	RADIUS	320	Access-Request id=60
167	31.854141	172.20.0.10	172.20.2.5	RADIUS	334	Access-Accept id=60
685	184.724939	172.20.2.5	172.20.0.10	RADIUS	207	Access-Request id=61
686	184.730448	172.20.0.10	172.20.2.5	RADIUS	132	Access-Challenge id=61
687	184.738886	172.20.2.5	172.20.0.10	RADIUS	418	Access-Request id=62
688	184.740060	172.20.0.10	172.20.2.5	RADIUS	277	Access-Challenge id=62
689	184.756480	172.20.2.5	172.20.0.10	RADIUS	275	Access-Request id=63
690	184.758193	172.20.0.10	172.20.2.5	RADIUS	232	Access-Challenge id=63
691	184.768639	172.20.2.5	172.20.0.10	RADIUS	320	Access-Request id=64
692	184.769840	172.20.0.10	172.20.2.5	RADIUS	334	Access-Accept id=64

Tableau des trames RADIUS (repris mot-pour-mot du document).

V. Conclusion

L’analyse des trames montre que :

- le service RADIUS est opérationnel,
- l’authentification passe bien par l’Active Directory,
- toute connexion WiFi nécessite un compte AD valide.