

AP BTS SIO

CONFIGURATION PARE-FEU.....	1
Infrastructure Réseau.....	1
Règles de Filtrage.....	2
CONFIGURATION WIFI.....	3
Paramètres du point d'accès Wifi.....	3
Autorité de Certification.....	7
Serveur Radius.....	9

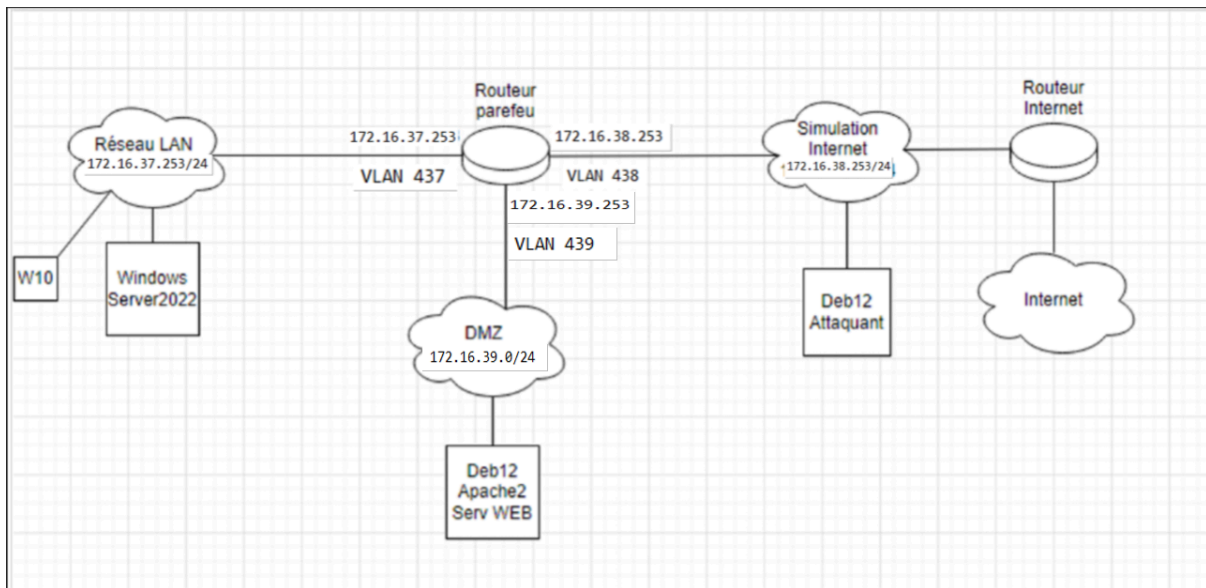
Au cours de l'AP, deux domaines ont été particulièrement étudiés. Tout d'abord le pare-feu, incluant son installation ainsi que la mise de règles de filtrage, en plus de la configuration de redirections de ports via le protocole DNAT.

Ensuite, le second domaine traité concerne le wifi, avec l'installation d'un serveur radius sur les commutateurs et les bornes wifi avec le support d'une autorité de certification.

CONFIGURATION PARE-FEU

Infrastructure Réseau


* Schéma du réseau, avec un réseau LAN (vlan 437), Internet (vlan 438) et une DMZ (vlan 439). On doit ensuite, configurer le pare-feu pour créer les règles de filtrages



Règles de Filtrage

* On voit les différents réseaux connectés au pare-feu

← → ↻ ⚠ Non sécurisé | <https://172.16.37.253:444/cgi-bin/index.cgi>

**ipfire.localdomain**

Système Statut Réseau Services Pare-feu IPFire Journaux Traffic: In 0.00 bit/s Out 2.70 kbit/s

Page principale

Réseau	Adresse IP	Statut
Internet	172.16.39.253	Connecté - (25m 26s)
Nom hôte :	ipfire.localdomain	
Passerelle :	172.16.39.254	
Réseau	Adresse IP	Statut
DMZ	172.16.31.253/24	Proxy inactif
DMZ	172.16.39.253/24	Online

Note

Veuillez s'il vous plaît activer le service Firewall.

Remarque : Une mise à jour est disponible depuis la version 160 vers 180

IPFire 2.27 (x86_64) - Core Update 160 IPFire.org • Soutenez le projet IPFire avec votre don

* Ensuite, les règles de filtrage présentes sur le pare-feu, ainsi qu'une disposition de redirection de ports sur la DMZ

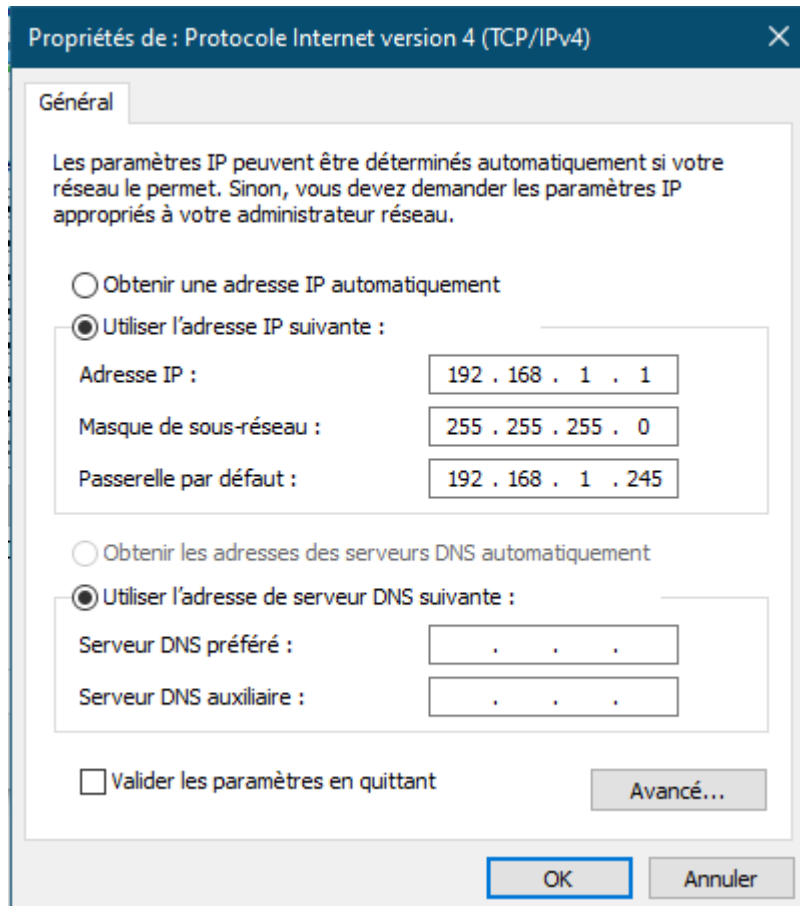
Règles de pare-feu

#	Protocole :	Source	Log	Destination	Action					
1	TCP	VERT	<input type="checkbox"/>	ORANGE: HTTP	<input checked="" type="checkbox"/>					
2	TCP	VERT	<input type="checkbox"/>	ORANGE: SSH	<input checked="" type="checkbox"/>					
3	TCP	VERT	<input type="checkbox"/>	ROUGE: HTTP	<input checked="" type="checkbox"/>					
4	TCP	VERT	<input type="checkbox"/>	ROUGE: HTTPS	<input checked="" type="checkbox"/>					
5	TCP	ORANGE: 80	<input type="checkbox"/>	VERT	<input checked="" type="checkbox"/>					
6	TCP	ORANGE: 22	<input type="checkbox"/>	VERT	<input checked="" type="checkbox"/>					
7	TCP	ORANGE: 80	<input type="checkbox"/>	ROUGE	<input checked="" type="checkbox"/>					
8	TCP	ROUGE	<input type="checkbox"/>	Pare-feu (ROUGE): 8081 ->172.16.39.1: 80	<input checked="" type="checkbox"/>					
9	TCP	ROUGE	<input type="checkbox"/>	Pare-feu (ROUGE): 8081 ->172.16.39.1: 443	<input checked="" type="checkbox"/>					
10	TCP	ROUGE: 2222	<input type="checkbox"/>	ORANGE: 22	<input checked="" type="checkbox"/>					
11	Tous	Tout	<input type="checkbox"/>	Tout	<input checked="" type="checkbox"/>					
VERT ORANGE		Internet (Autorisé) Internet (Autorisé)			ORANGE (Autorisé) VERT (Bloqué)					
Politique: Autorisé										

CONFIGURATION WIFI

Paramètres du point d'accès Wifi

* **Modification de la passerelle du poste, pour pouvoir se connecter à la borne wifi**



* **On va ensuite sur Internet, pour pouvoir afficher les paramètres de la borne wifi**



* Cette page nous montre l'adresse IP de la borne wifi ainsi que son hostname

192.168.1.245/Setup.htm

The screenshot shows the Linksys WAP200 Setup page. The top navigation bar includes 'Setup', 'Wireless', 'AP Mode', 'Security Monitor', 'Administration', and 'Status'. The 'Setup' tab is active, and the 'Basic Setup' sub-tab is selected. The page displays the 'Host Name' as 'LaTeamB' and the 'Device Name' as 'WAP200'. Under 'Network Setup', the 'IP Settings' section shows a 'Static IP Address' dropdown set to 'Static IP Address'. Below this, there are input fields for 'Local IP Address' (192.168.1.245), 'Subnet Mask' (255.255.255.0), 'Default Gateway' (0.0.0.0), 'Primary DNS' (0.0.0.0), and 'Secondary DNS' (0.0.0.0). At the bottom right, there are 'Save Setting' and 'Cancel Changes' buttons. The Cisco Systems logo is visible in the bottom right corner.

* Les identifiants en tant qu'administrateur pour se connecter à la borne wifi

The screenshot shows the Linksys WAP200 Administration page. The top navigation bar includes 'Setup', 'Wireless', 'AP Mode', 'Security Monitor', 'Administration', and 'Status'. The 'Administration' tab is active, and the 'Management' sub-tab is selected. The page displays the 'User Name' as 'admin' and the 'AP Password' as '*****'. Below this, there are input fields for 'Re-enter to confirm' (*****). Under 'Web Access', there are radio buttons for 'Web HTTPS Access' (Enabled/Disabled) and 'Wireless Web Access' (Enabled/Disabled). Under 'SNMP', there are radio buttons for 'SNMP V1 & V2' (Selected) and 'SNMP V3'. Below this, there are input fields for 'Contact', 'Device Name', 'Location', 'Security user name', 'Authentication password', and 'Privacy password'. At the bottom right, there are 'Save Setting' and 'Cancel Changes' buttons. The Cisco Systems logo is visible in the bottom right corner.

* Et enfin, le mode de sécurité (ici, wpa2) et le mot de passe pour qu'un utilisateur puisse se connecter à la borne wifi depuis son appareil

LINKSYS®
A Division of Cisco Systems, Inc.

Firmware Version: 1.0.22-ETSI

Wireless

Wireless-G Access Point

WAP200

Setup

Wireless

AP Mode

Security Monitor

Administration

Status

Basic Wireless Settings

Wireless Security

Wireless Connection Control

Advanced Wireless Settings

VLAN & QoS

Wireless Security

Select SSID:

LaTeamB

Wireless Isolation
(between SSID):

Enabled

Security Mode:

WPA2-Personal Mixed

Wireless Isolation
(within SSID):

Disabled

Encryption:

TKIP or AES

Shared Secret:

lewifidePARKAL

Key Renewal Timeout:

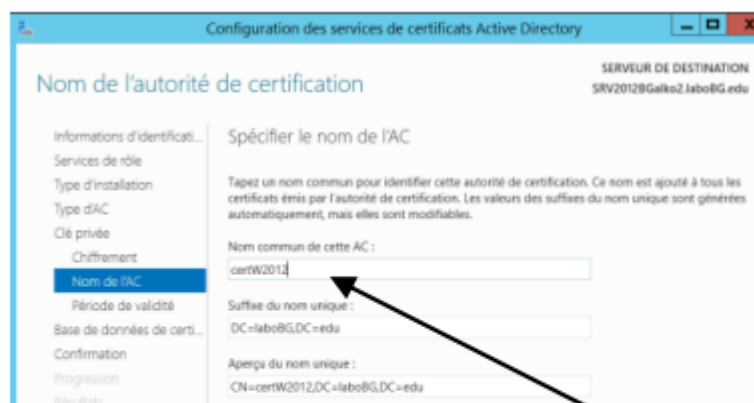
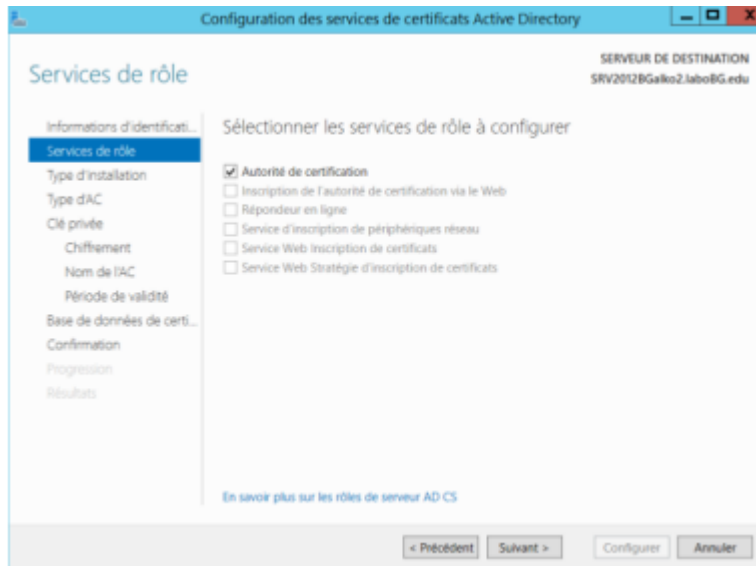
3600

 seconds

Help...

Autorité de Certification

* Dans l'AD, on installe une autorité de certification pour pouvoir utiliser le wifi sur le poste



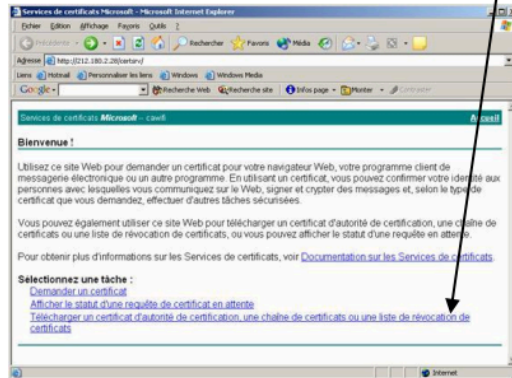
Choisir un **nom** pour l'autorité de certification :

Exemple : **certW2016-><lettreBaie+N°>**

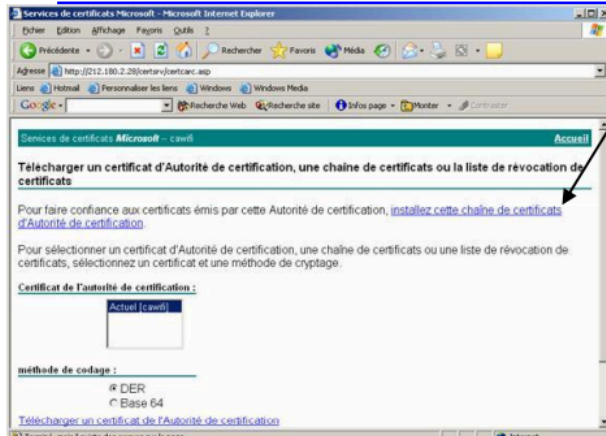
Ex : certW2016A1

* On ouvre une page Internet, et on inscrit notre adresse IP avec à la fin le nom du certificat. On tombe sur une page, qui nous propose de télécharger le certificat

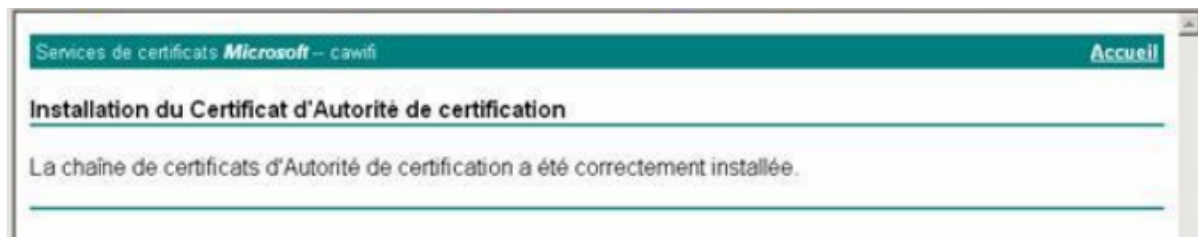
Cliquer sur le lien **Télécharger un certificat d'autorité de certification, une chaîne de certificats ou une liste de révocation de certificats.**



Cliquer sur [installez cette chaîne de certificats d'Autorité de certification](#)



* En suivant les étapes, on réussit à installer le certificat d'autorité de certification



* Enfin, dans les paramètres réseau, il faut choisir le certificat d'autorité pour permettre d'accéder au wifi

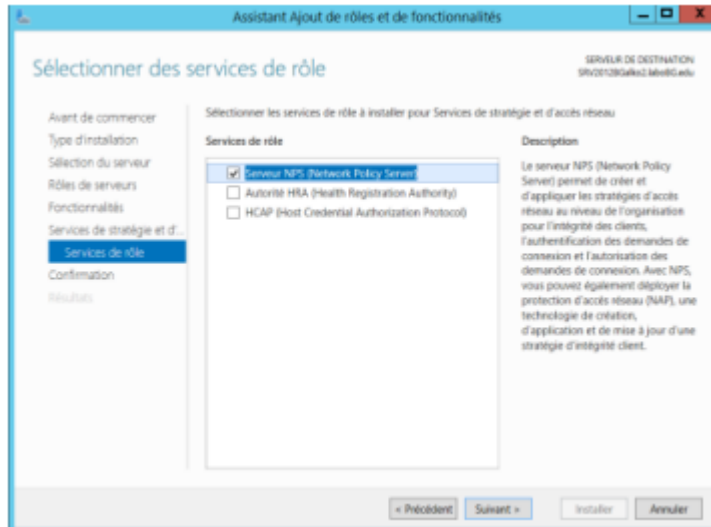
Démarrer le service "Configuration automatique de réseau câblé".

Dans les **propriétés de la carte réseau**, onglet **Authentification**, cocher Activer l'authentification IEEE 802.1X et choisir la méthode d'authentification réseau, dans notre cas :

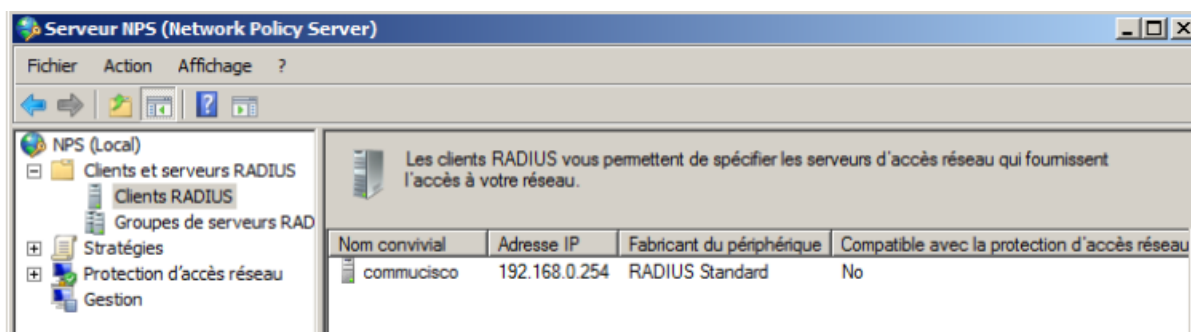
Microsoft : Carte à puce ou autre certificat,
et définir le certificat installé précédemment dans **Paramètres**.

Serveur Radius

* On installe le service NPS, pour faire du radius qui permettra de propager le wifi, soit à partir d'une borne wifi, soit à partir d'un commutateur



* On crée un serveur radius à partir d'une adresse IP et avec certaines stratégies



* Représentation de tous les clients radius

