

# CHAPITRE 5 :

## TEST ET VALIDATION

Une fois la solution mise en place, nous procédons à la phase de test dans le but de nous assurer du bon fonctionnement des équipements et de la configuration. La vérification consiste à essayer de se connecter, aux réseaux filaire et sans fil,

# I. LES RESEAUX FILAIRES

## 1. Le premier test

Le premier test à effectuer nous permettra de nous garantir du bon déroulement de l'authentification au domaine et de la validation de posture pour un utilisateur du réseau câblé. Par défaut sur un système Windows, l'authentification 802.1X est désactivée sur les cartes réseau Ethernet. Par conséquent, nous devons ajouter et démarrer le service « Configuration automatique de réseau câblé », responsable de l'exécution de l'authentification IEEE 802.1X sur les interfaces Ethernet. Après avoir lancé "services.msc" et cliqué sur le service correspondant, la fenêtre suivante s'affiche pour démarrer le service.

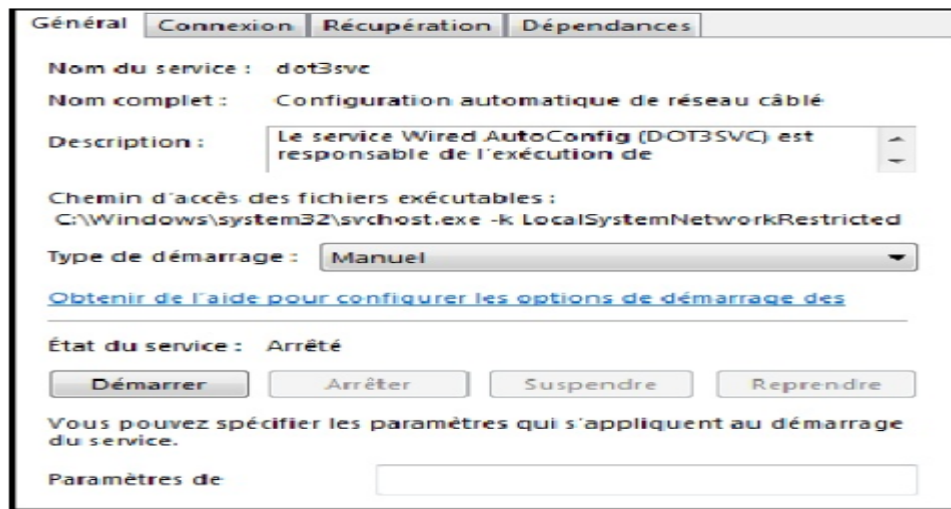


Figure 20 : Ajout et démarrage du service DOT1X

L'étape consiste à activer l'authentification 802.1X sur l'interface Ethernet. La méthode d'authentification par défaut. PEAP a été conservée par la plate-forme ISE.

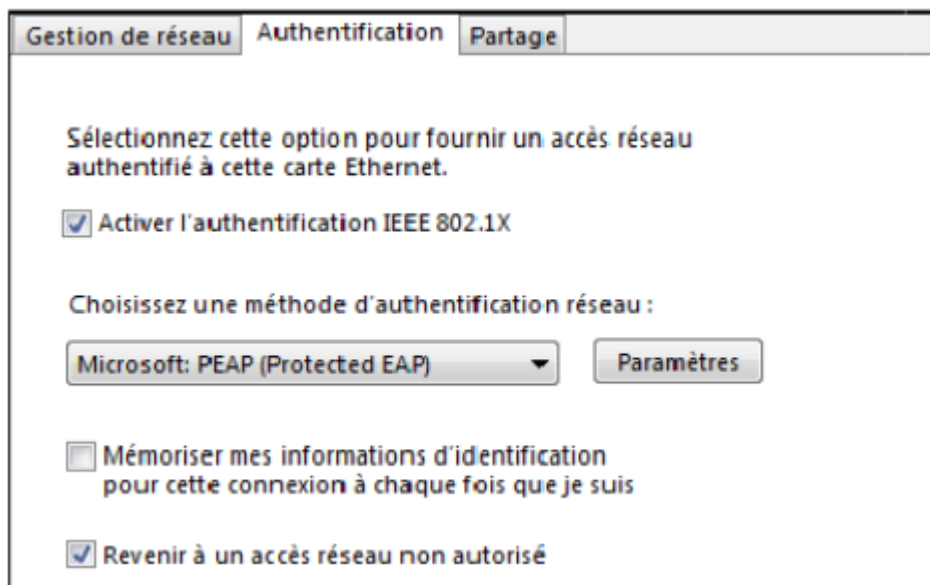


Figure 21 : Activation de DOT1X sur la carte Ethernet

Dès le branchement du câble sur l'interface Ethernet, une fenêtre s'affiche demandant de saisir le nom d'utilisateur et le mot de passe pour s'authentifier au niveau du domaine du moment que les données de la session existante ne sont pas automatiquement utilisées

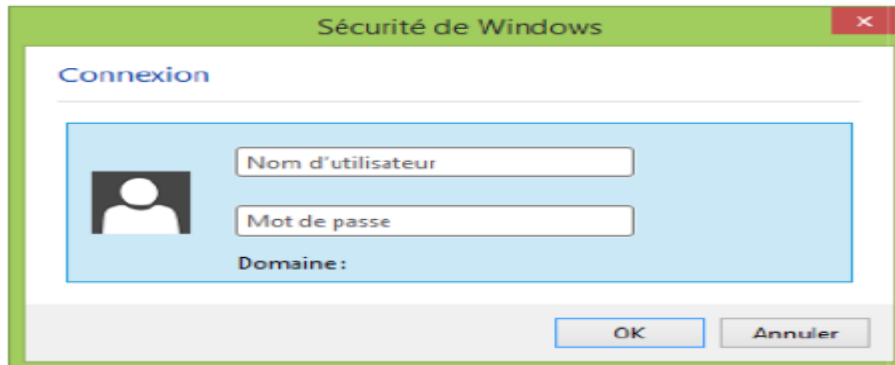


Figure 22 : Fenêtre d'authentification

Après avoir saisi les données du compte utilisateur, et en essayant d'accéder à la page <http://www.google.fr>, nous nous sommes trouvés vers la page de CLIENT PROVISIONNING fournissant l'Agent NAC persistant.

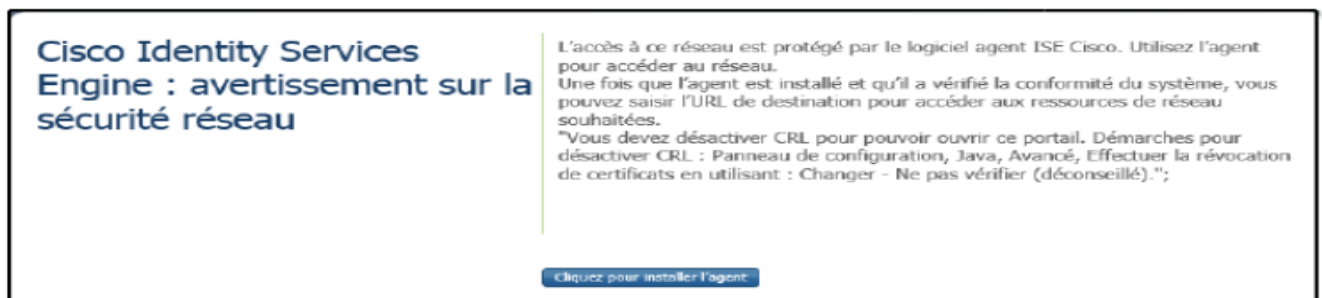


Figure 23 : Redirection vers la page de client Provisionning

En cliquant sur le bouton « Cliquer pour installer l'agent », le téléchargement de l'Agent se lance. En l'exécutant, nous recevons un message indiquant la non-conformité de notre machine avec la politique de sécurité et fournissant un accès temporaire pour télécharger le fichier de remédiation tant que l'antivirus McAfee n'est pas disponible sur notre machine. La figure qui suit représente une capture du message reçu au niveau de l'Agent.

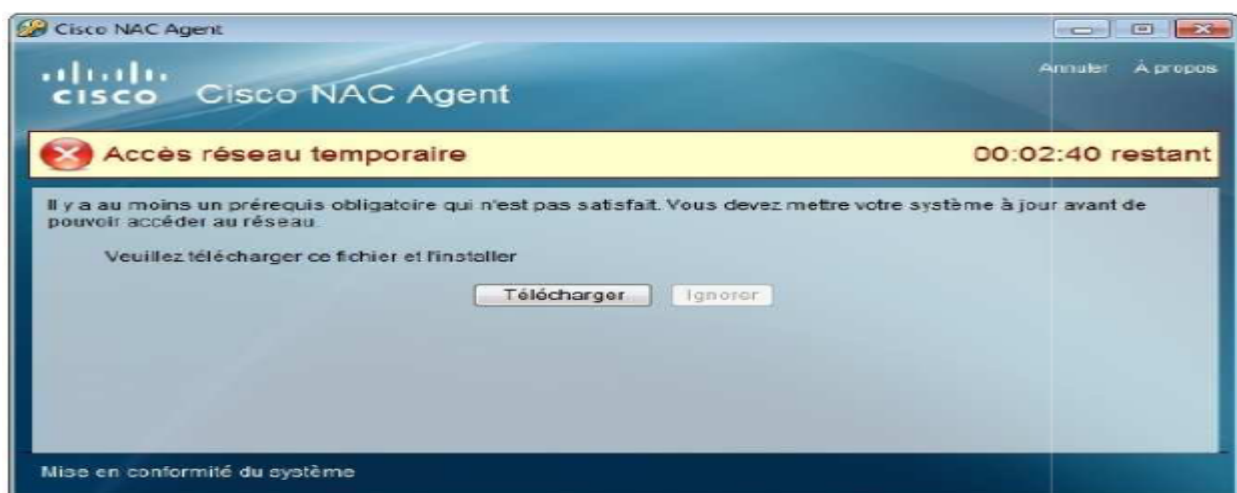


Figure 24 : Message obtenu sur l'Agent NAC

## 2. Deuxième partie

Le deuxième test que nous effectuons consiste à vérifier l'authentification MAB. Pour le faire, nous désactivons l'authentification 802.1X sur l'interface pour que l'authentification par l'adresse MAC soit automatiquement utilisée.

Au niveau du switch, nous pouvons observer le déroulement de l'authentification.

```
*Mar 1 00:32:37.942: %DOT1X-5-FAIL: Authentication failed for client (Unknown MAC) on Interface Fa0/24
*Mar 1 00:32:37.942: %AUTHMGR-7-RESULT: Authentication result 'no-response' from 'dot1x' for client (Unknown MAC) on Interface Fa0/24
*Mar 1 00:32:37.942: %AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client (Unknown MAC) on Interface Fa0/24
*Mar 1 00:32:38.219: %AUTHMGR-5-START: Starting 'mab' for client (a0b3.cc84.7580) on Interface Fa0/24
*Mar 1 00:32:39.109: %MAB-5-SUCCESS: Authentication successful for client (a0b3.cc84.7580) on Interface Fa0/24
*Mar 1 00:32:39.109: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client (a0b3.cc84.7580) on Interface Fa0/24
*Mar 1 00:32:40.124: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up
*Mar 1 00:32:40.149: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (a0b3.cc84.7580) on Interface Fa0/24
```

Figure 25 : Evènement d'authentification observés au commutateur

Pour s'assurer de la bonne affectation du profil d'autorisation, nous pouvons avoir recours au commutateur et utiliser la commande **show authentication session interface ID detail**

## II. LES RESEAUX SANS FIL

Nous débutons par la vérification de la diffusion des SSID. (Dans notre cas il s'agit de DigitalworldGuest et DigitalworldGuest2) et en consultant la liste des réseaux sans fil disponible depuis notre PC.

Nous choisissons de se connecter à « DigitalworldGuest » et après avoir activé l'authentification 802.1X, les deux champs s'affichent demandant de saisir le com d'utilisateur et le mot de passe comme illustré sur la figure suivante.

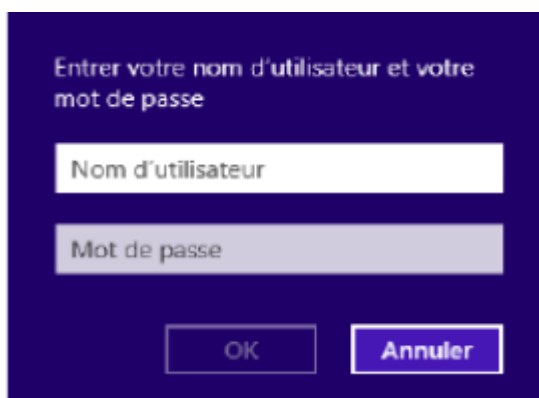


Figure 26 : Authentification DOT1X pour le SSID DigitalworldGuest

Après avoir inséré les coordonnées, nous sommes redigés vers la page CCP (Client Provisionning Portal) pour télécharger l'agent NAC. Une fois installé, cet Agent nous indique que notre accès au réseau est restreint pour raison de non-conformité tel qu'il est montré sur la figure et nous propose la réparation de la machine pour avoir un accès complet.

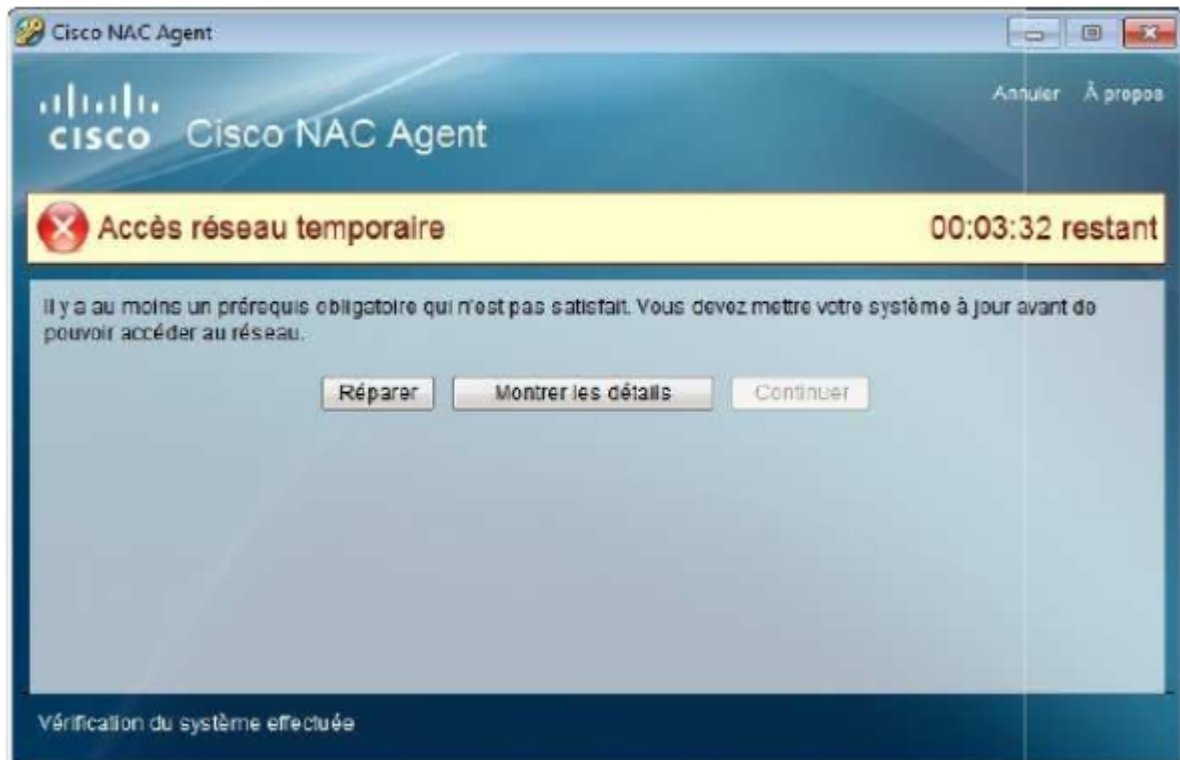


Figure 27 : Accès restreint à un utilisateur du réseau sans fil

Un invité, n'appartenant pas au domaine, est appelé à se connecter à DigitalWorldGuest2. Dès qu'il se connecte, il se trouve redirigé vers le portail captif sur son navigateur.

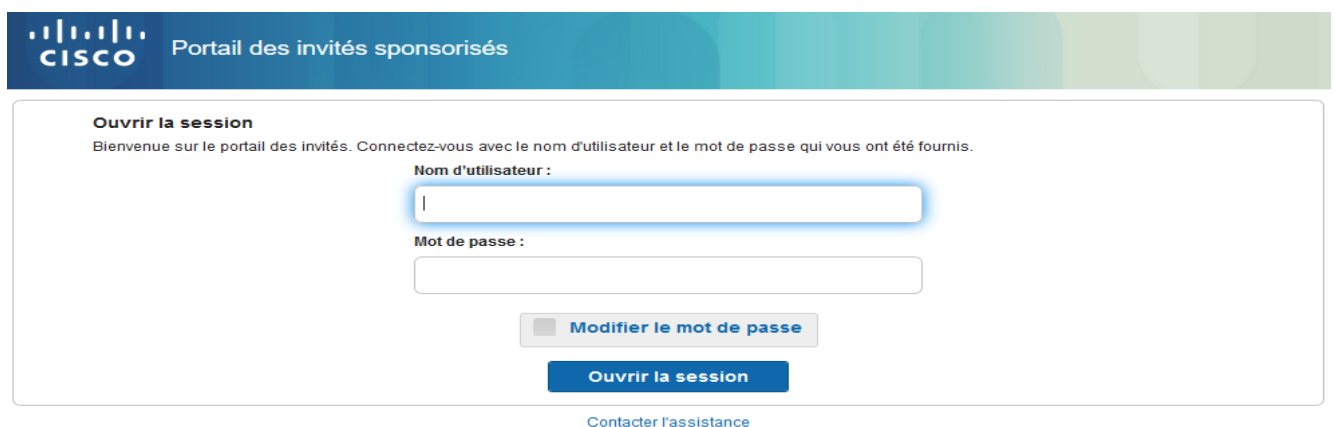


Figure 28 : Portail des invités sponsorisés

Le succès de la connexion fait ressortir cette fenêtre.

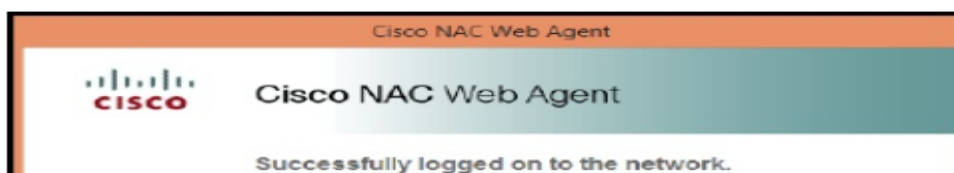


Figure 29 : Accès complet au réseau

En consultant le log de la plate-forme ISE, nous pouvons constater l'évolution suivante :

- Succès de l'authentification MAB
- Succès de l'authentification via le portail invité
- Validation de posture de la machine
- Succès de l'autorisation dynamique ou CoA (changement du profil d'autorisation de CWA à PermitAccess)







Time	Status	Details	Repeat at Count	Identity	IP Address	Authorization Profiles	Posture Status	Server	Event
2015-04-28 18:44:01.523	✓			bnasr02		PermitAccess	Compliant	ISE-CISCO	Authorize-Only succeeded
2015-04-28 18:44:01.508	✓						Compliant	ISE-CISCO	Dynamic Authorization succeeded
2015-04-28 18:43:59.495			0	bnasr02	172.25.0.55		Compliant	ISE-CISCO	Session State is Postured
2015-04-28 18:43:25.299	✓			bnasr02	172.25.0.55			ISE-CISCO	Guest Authentication Passed
2015-04-28 18:42:41.704	✓			ED:90:31:07:68:		CWA	NotApplicable	ISE-CISCO	Authentication succeeded

Figure 30 : Log de la plate-forme ISE

Cette partie du rapport était consacrée à l'essai de la solution avec la solution avec différents scénarios afin de prouver son bon fonctionnement et son efficacité et ce, en essayant de connecter une machine au réseau, ou encore en se référant aux services disponibles au sein des composants, tel que le système de journalisation de la plate-forme CISCO-ISE.