

Encadré par :  
Dr bouraghba khalid

Realisé par :  
El arrouchi fatima ezzahra

# NAP (Network Access Protection)

## Plan :

- 1 Définition du NAP
- 2 Différence entre NAP et NAC
- 3 Les Rôles de NAP
- 4 Avantages du NAP
- 5 Exemples des réseaux contenant NAP
- 6 Composants du NAP
- 7 Fonctionnement du NAP
- 8 Implémentation dans un réseau
- 9 Cas pratiques
- 10

## Définition :

La protection d'accès réseau (NAP) est une technique développée par Microsoft en collaboration avec Cisco pour contrôler l'accès au réseau d'un ordinateur en fonction de l'état de santé de son système. Cette technologie garantit que seuls les appareils conformes aux politiques de sécurité définies peuvent accéder aux ressources du réseau. Cela inclut la vérification de critères comme la mise à jour des correctifs de sécurité, la présence d'antivirus, et l'état du pare-feu.

## NAP

## #

Technologie spécifique développée par Microsoft pour contrôler l'accès au réseau en vérifiant l'état de santé des appareils. Elle est centrée sur les environnements Windows et offre un niveau de vérification basé sur les politiques de sécurité Microsoft.

Terme plus large utilisé dans l'industrie pour désigner les solutions de contrôle d'accès au réseau, qui incluent des technologies variées de différents fournisseurs (comme Cisco, Aruba). Il couvre une gamme plus étendue de fonctionnalités, telles que l'authentification, l'autorisation, et l'application des politiques de sécurité, indépendamment du système d'exploitation.

# Les Rôles de NAP

## 01 Vérification de la conformité des appareils:

NAP s'assure que les appareils respectent les politiques de sécurité définies.

EX: Pare-feu activé.

## 02 Contrôle de l'accès au réseau:

NAP décide si un appareil peut avoir accès au réseau ou non :

- Appareil conforme : Accès complet.
- Appareil non conforme: Accès limité (quarantaine) ou refusé.

# Les Avantages de NAP

## 01 Sécurité renforcée:

Le réseau est bien protégé contre les virus, les pirates et les appareils non sécurisés.

## 02 Conformité aux règles de sécurité:

Tous les appareils respectent les mêmes règles de sécurité (comme avoir un antivirus ou être à jour).

03

## Réduction des interventions:

Les problèmes sont détectés et corrigés automatiquement, donc moins de travail pour les techniciens.

## 04 Protection contre les menaces:

NAP bloque les appareils à risque avant qu'ils ne causent des problèmes dans le réseau.

## 05 Expérience utilisateur améliorée:

Les utilisateurs peuvent se connecter facilement et travailler sans problèmes grâce à un réseau sécurisé.

# Exemples des réseaux contenant NAP

## □ Réseaux d'entreprise:

- Exemple : Une société multinationale utilise NAP pour s'assurer que tous les ordinateurs portables des employés respectent les règles de sécurité (antivirus à jour, pare-feu activé).

## □ Réseaux des établissements éducatifs

- Le NAP s'assure que les appareils des étudiants respectent des règles minimales (comme l'absence de logiciels malveillants) pour protéger le réseau principal.

## □ Réseaux de santé (hôpitaux et cliniques)

- Le NAP garantit que seuls les appareils conformes et sécurisés peuvent accéder aux données sensibles, comme les dossiers médicaux.

## □ Réseaux cloud et VPN d'entreprise

- Le NAP vérifie que les appareils distants (ordinateurs personnels, tablettes) sont sécurisés avant de leur permettre d'accéder au réseau de l'entreprise.

# Architecture NAP

El arrouchatima ezzahra

## Composants côté client NAP :

### Agents de Santé du Système (SHA) :

Surveillent des éléments comme l'antivirus ou les mises à jour. Vérifient si le client respecte les exigences de santé.

### Agent NAP :

Il collecte les informations de santé fournies par les SHA et les envoie au serveur.

### Déclaration de Santé (SoH) :

Rapport envoyé au serveur qui décrit l'état de conformité de la machine.

# Composants côté serveur NAP :

## System Health Validators (SHV):

Vérifient les informations de santé envoyées par le client. Chaque SHA a un SHV correspondant côté serveur.

## NAP Enforcement Server (ES) :

Applique la décision en autorisant ou restreignant l'accès réseau selon la conformité.

## NAP Health Policy Server (NPS) :

Définit les politiques de santé et décide du niveau d'accès à accorder.

## Remediation Server:

Fournit des outils de correction (comme des mises à jour) pour les clients non conformes.

## Méthodes de renforcement:

- Application DHCP: les clients reçoivent des adresses IP en fonction de leur état de santé. Des plages d'adresses IP limitées peuvent être attribuées aux clients non conformes.
- Application d'IPsec : les clients doivent s'authentifier avant de pouvoir communiquer avec d'autres systèmes.
- Application VPN: des contrôles de santé sont effectués lorsque des clients distants se connectent au réseau via VPN.
- Application de la norme 802.1X : utilise l'authentification réseau pour contrôler l'accès aux réseaux sans fil ou filaires.

- Configuration des composants NAP
- Configuration de l'accès VPN
- Configuration des paramètres clients pour prendre en charge la protection d'accès réseau (NAP)

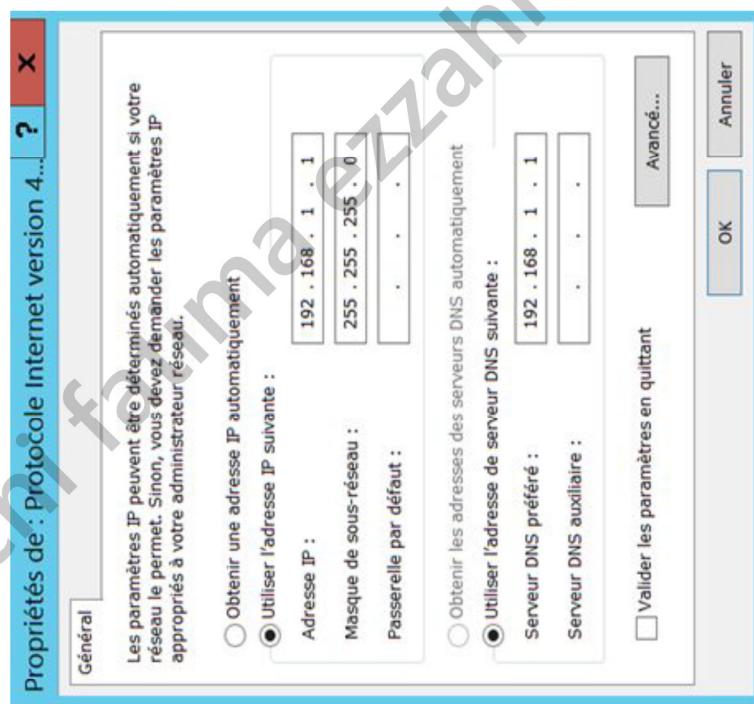
## ETAPES

### D'IMPLEMENTATION

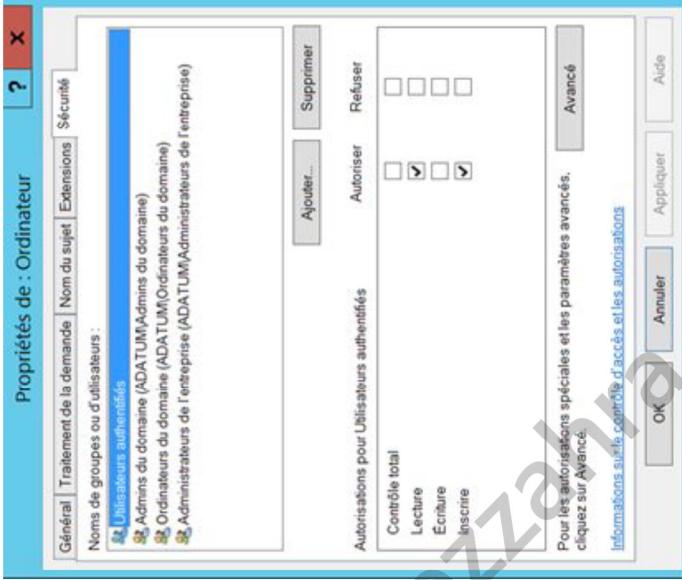
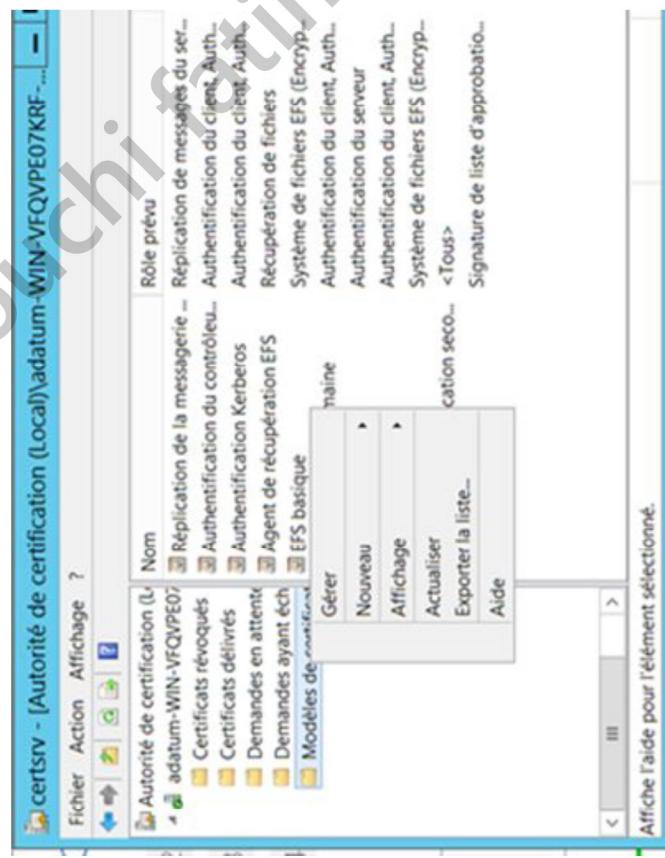
# Configuration des composants NAP

## Serveur:

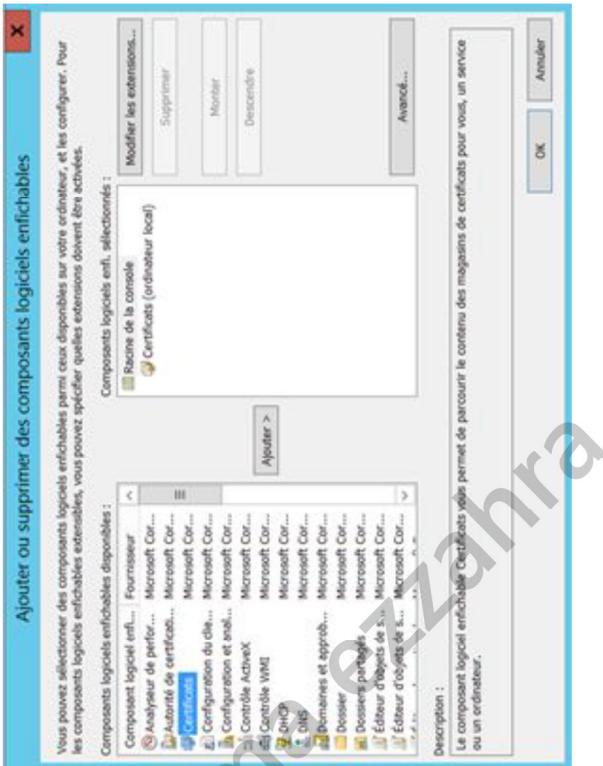
### Configuration de IPv4 de serveur



# Configurer les exigences des certificats clients et de serveur



## Ajout ou suppression des composants logiciels enfichables - Configuration des certificats



## Demander des certificats



# Configurer les stratégies de contrôle d'intégrité

## Installation de NPS (network policy services)



## Configuration des paramètres d'intégrité système

The image shows two windows side-by-side. The top window is titled "Windows Security Health Validator" and displays a configuration dialog for "Choose policy settings for Windows Security Health Validator". It includes sections for Firewall Settings (with a checked checkbox for "A firewall is enabled for all network connections") and Spyware Protection Settings (with three checkboxes: "An antivirus application is on", "Antivirus is up to date", and "Antivirus is up to date"). The bottom window is titled "Serveur NPS (Network Policy Server)" and shows the "Paramètres" (Parameters) tab of the NPS (Local) configuration. It lists various policy components like Clients et serveurs RA, Stratégies, Protection d'accès réseau, Programmes de validation, Programme de validation, Codes d'erreur, Groupes de serveur, Gestion, and Gestion des modèles.

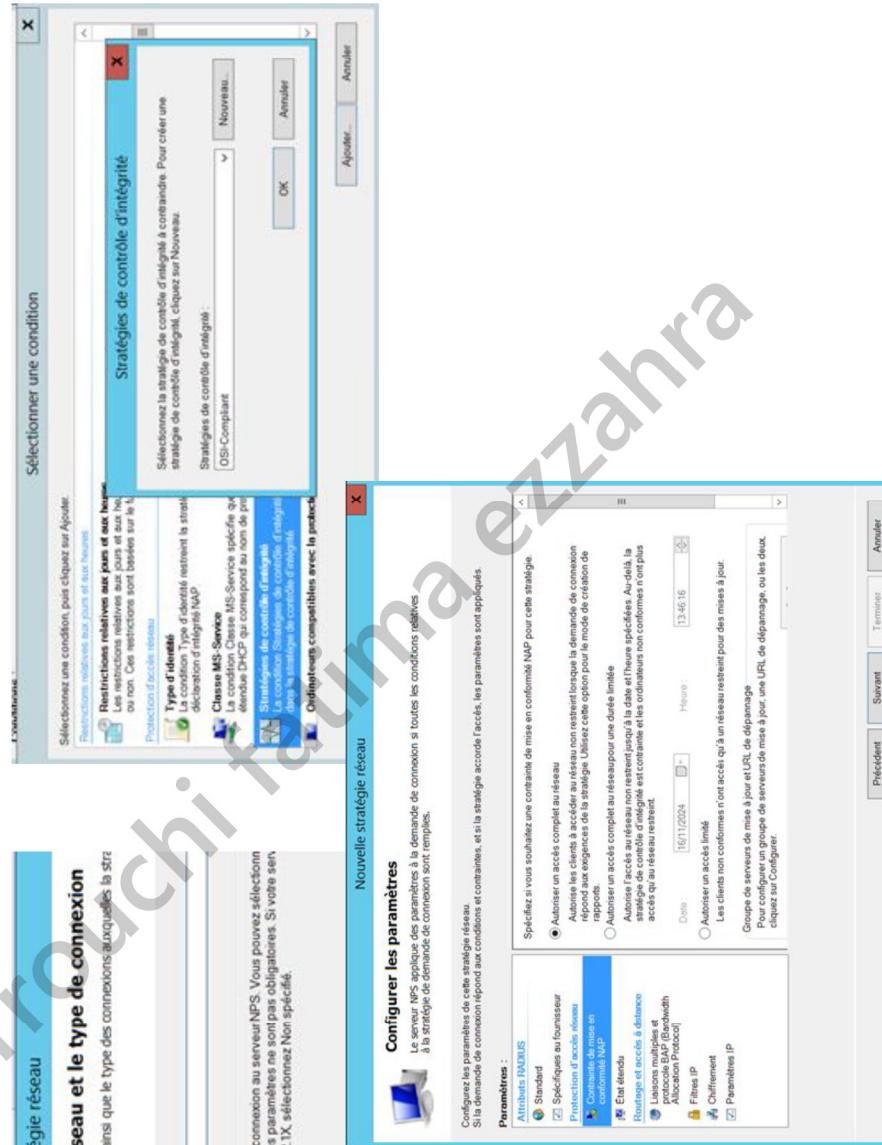
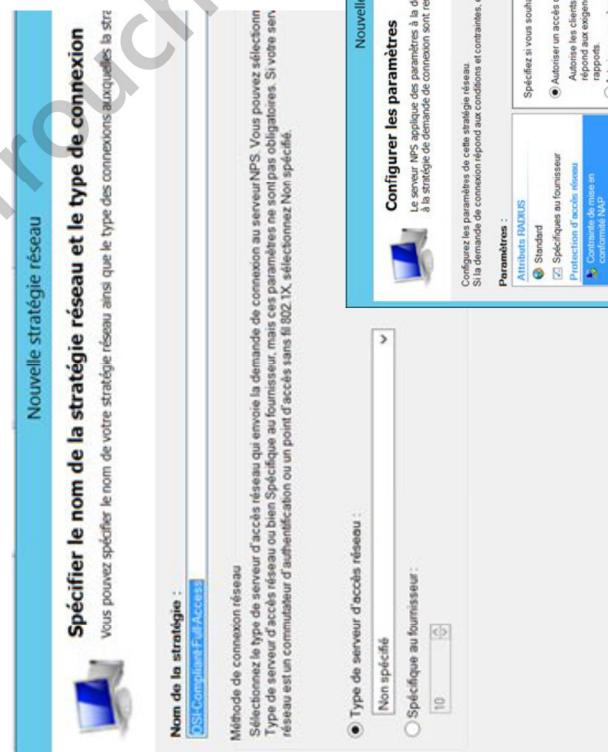
## Configuration des paramètres d'intégrité système

The screenshot shows two windows related to Network Policy Server (NPS) configuration:

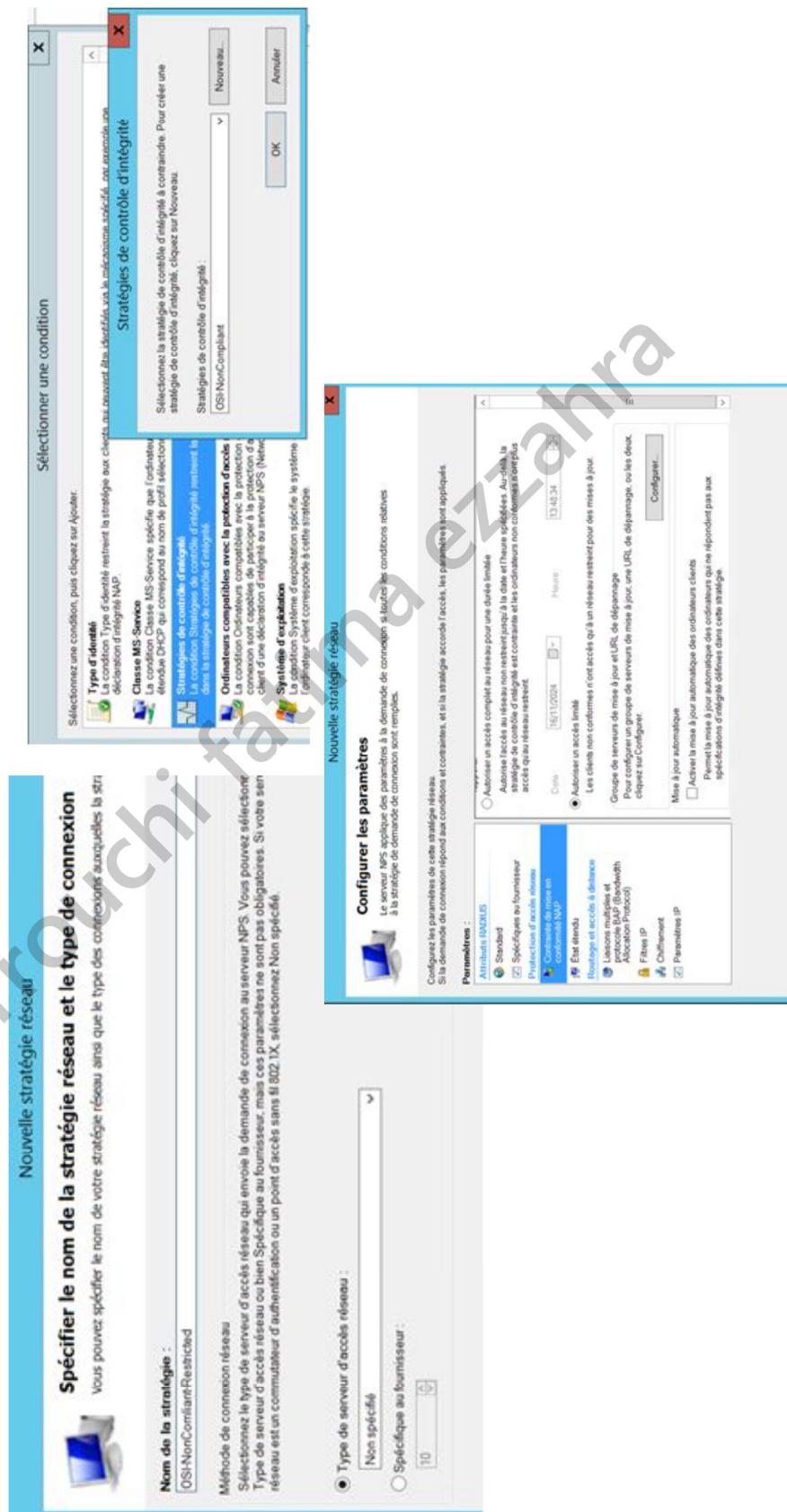
- Top Window: "Créer une stratégie de contrôle d'intégrité"**
  - Paramètres**: Configurez les paramètres de stratégie de contrôle d'intégrité. Pour mettre en application la stratégie de contrôle d'intégrité, ajoutez celle-ci derrière à la condition Stratégies de contrôle d'intégrité d'une ou de plusieurs stratégies réseau.
  - Sélectionner un modèle existant: [dropdown menu]
  - Nom de la stratégie: **OSI-NonCompliant**
  - Contrôles du client par les programmes de validation d'intégrité système (S/N):
    - Réussite de tous les contrôles S/N pour le client
  - Programmes de validation d'intégrité système (S/N) utilisés dans cette stratégie de contrôle d'intégrité:
    - Nom**:  Programme de validation
    - Paramètre**: Configuration par défaut
- Bottom Window: "Serveur NPS (Network Policy Server)"**
  - Fichier Action Affichage ?
  - Stratégies de contrôle d'intégrité
    - Les stratégies de contrôle d'intégrité sont utilisées conjointement avec la protection d'accès réseau (NAP) et vous permettent de spécifier la configuration nécessaire aux ordinateurs clients NAP pour accéder au réseau.
    - Nom de la stratégie: **OSI-Compliant**
  - Programmes de validation
    - Programme de validation
    - Paramètres
    - Codes d'erreur
  - Gestion
    - Gestion des groupes de serveur
    - Gestion des modèles

## Configurer les stratégies réseau

## OSI-Compliant-Full-access : Automatique d'intégrité.

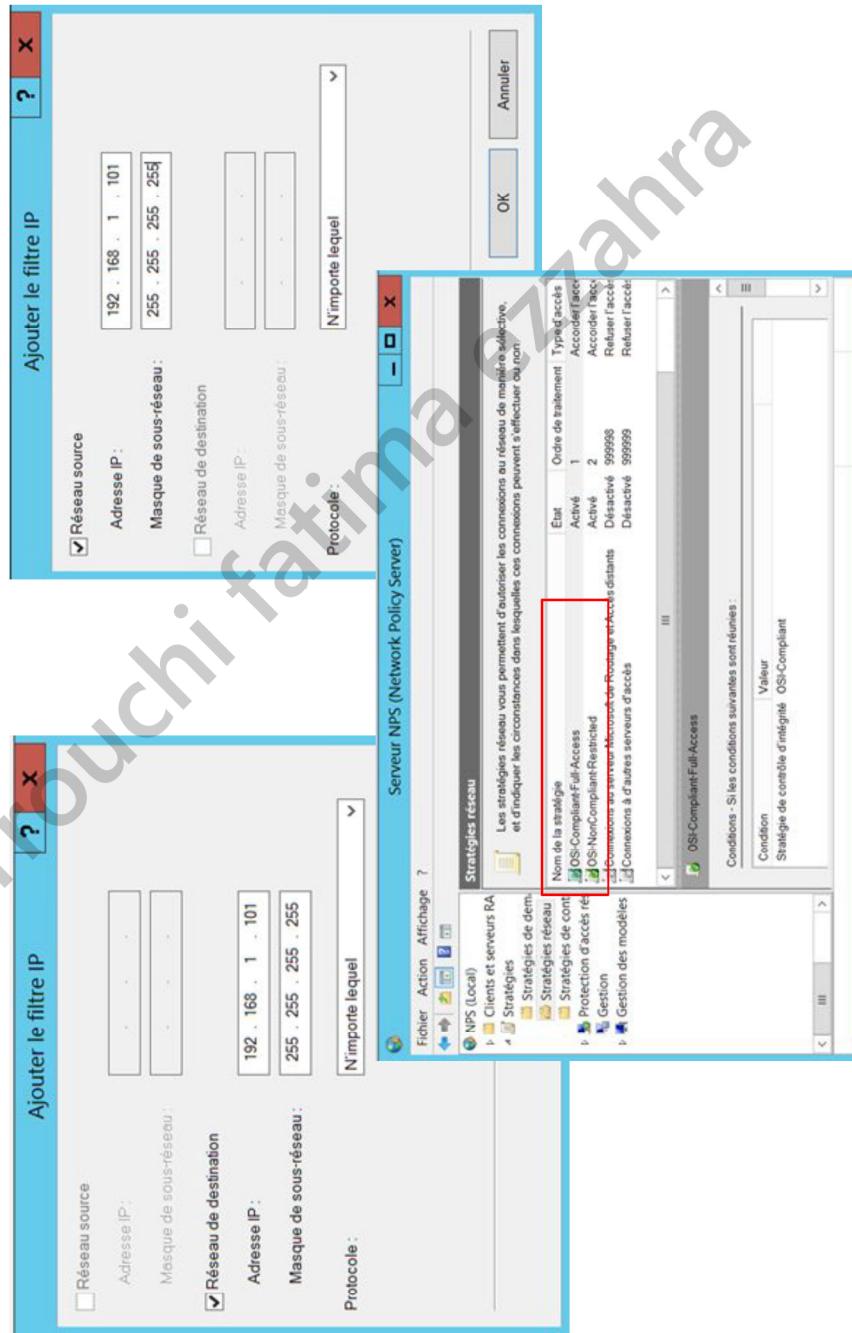


**OSI-NonCompliant-Restricted:** Limite l'accès des clients non conformes, tout en autorisant des communications spécifiques.



## Ajout des filtres IP pour la stratégie "OSI-NonCompliant-Restricted"

Ces filtres IP restreignent les communications des clients non conformes à un serveur spécifique (adresse IP : 192.168.1.1) et empêchent tout autre trafic réseau.



# Configurer des stratégies de demande de connexion pour VPN

## Création d'une nouvelle stratégie de demande de connexion VPN

Nouvelle stratégie de demande de connexion

**Spécifier le nom de la stratégie de demande de connexion et le type de connexion**

 Vous pouvez spécifier le nom de votre stratégie de demande de connexion ainsi que le type des connexions auxquelles cette stratégie s'applique.

**Nom de la stratégie :**

Méthode de connexion réseau

Sélectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une valeur « Type de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre serveur d'accès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X sélectionnez Non spécifié. »

Type de serveur d'accès réseau :  >

Spécifique au fournisseur :

# Spécification des conditions de connexion

**Sélectionner une condition**

Spécialisez une condition, puis cliquez sur Ajouter.

**Protocole de trames** La condition Protocole de trames restreint la stratégie aux clients qui spécifient un protocole de trames spécifique pour les paquets entrants, par exemple le protocole PPP ou SLIP.

**Type de service** La condition Type de service restreint la stratégie aux clients qui spécifient un certain type de service, par exemple les connexions Telnet ou PPP (Point to Point Protocol).

**Type de tunnel** La condition Type de tunnel restreint la stratégie aux clients qui créent un type de tunnel spécifique, par exemple via le protocole PPTP ou L2TP.

**Restrictions relatives aux jours et aux heures** Les restrictions relatives aux jours et aux heures indiquent les jours et les heures auxquels les tentatives de connexion sont autorisées ou non. Ces restrictions sont basées sur le filtre horaire du serveur NPS (Network Policy Server).

**Type d'identité**

**Type de tunnel**

Spécifiez les types de tunnels nécessaires pour correspondre à cette stratégie.

Types de tunnels pour connexions d'accès à distance et VPN standard

Generic Route Encapsulation (GRE)  
IP Encapsulating Security Payload in the Tunnel-mode (ESP)  
Layer Two Tunneling Protocol (L2TP)  
Point-to-Point Tunneling Protocol (PPTP)  
Secure Socket Tunneling Protocol (SSTP)

Types de tunnels pour connexions 802.1X standard

Virtual LANs (VLAN)

Autres

Ascend Tunnel Management Protocol (ATMP)  
Bay Dial Virtual Services (DVS)  
Generic Route Encapsulation (GRE)  
IP-in-IP Encapsulation (IP-IP)

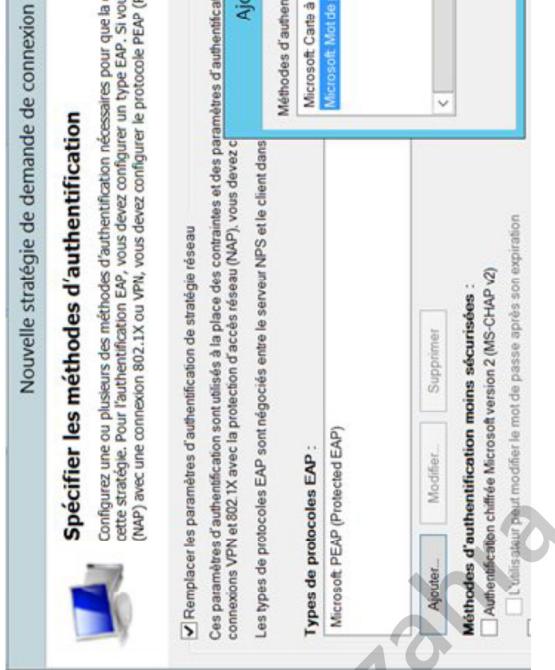
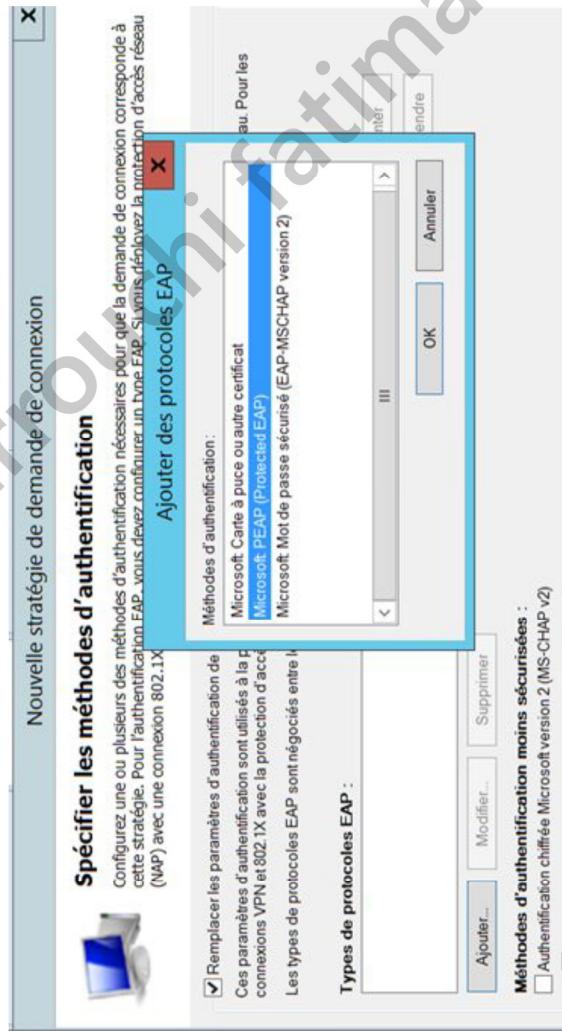
**Spécifier les conditions**

Spécifiez les conditions qui déterminent si cette stratégie de demande de connexion est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

**Conditions :**

Condition	Valeur
Type de tunnel	Layer Two Tunneling Protocol (L2TP) OU Point-to-Point Tunneling Protocol (P...

# Configuration des paramètres d'authentification

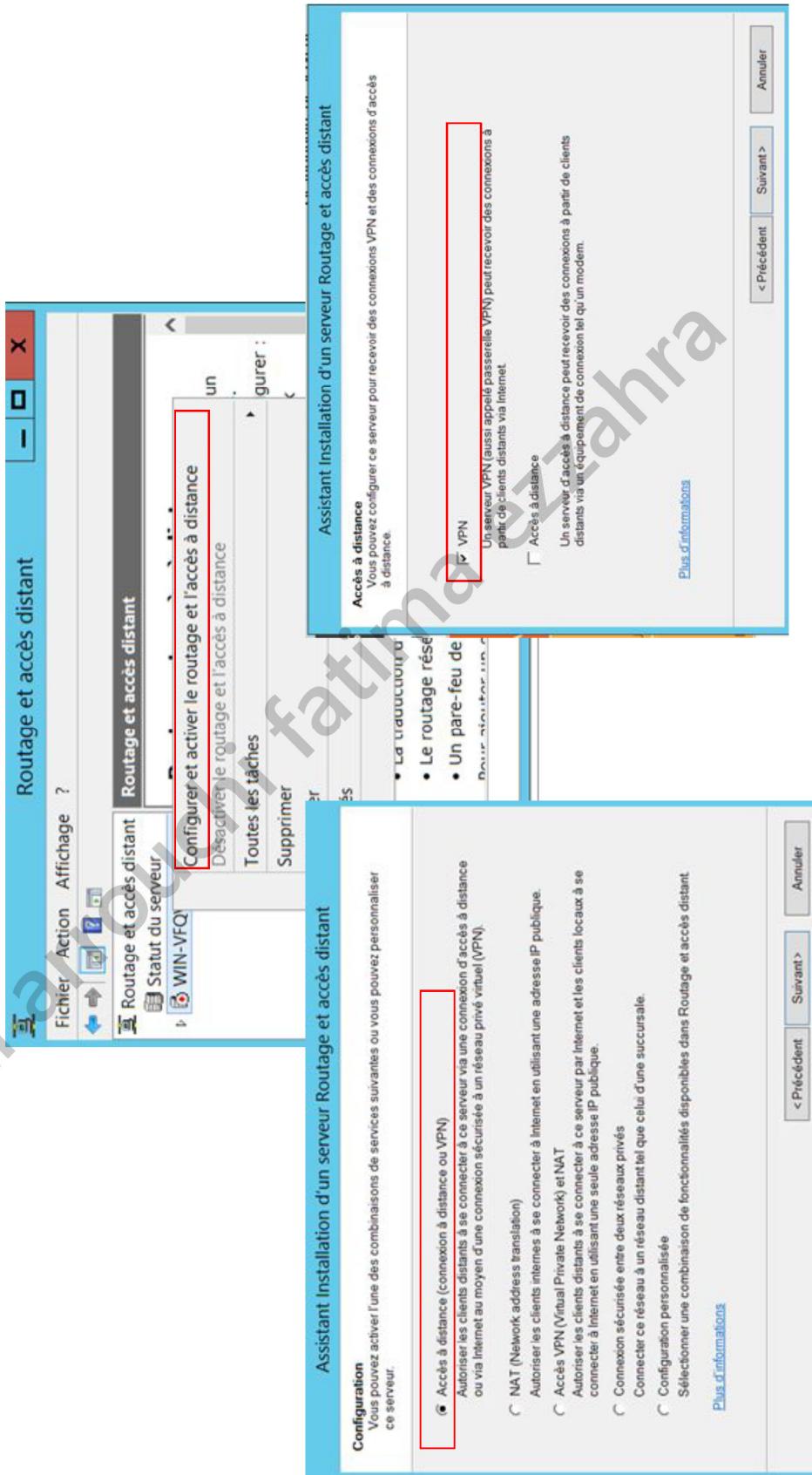


# Configuration de l'accès VPN

## Installation de 'routage et accès à distance'



## Configurer et activer le routage et l'accès distant



## Configurer l'interface réseau

Assistant Installation d'un serveur Routage et accès distant

**Connexion VPN**  
Au moins une interface réseau doit être connectée à Internet afin de permettre aux clients VPN de se connecter à ce serveur.

Sélectionnez l'interface réseau qui connecte ce serveur à Internet

Interfaces réseau :

Nom	Description	Adresse IP
Ethernet0	Connexion réseau Intel(R) 82... Connexion réseau Intel(R) 82...	192.168.1.1 192.168.18.148 (DHCP)
Ethernet1		

Sécuriser l'interface sélectionnée en configurant des filtres de paquet statiques  
Les filtres de paquets statiques ne permettent l'accès à ce serveur via l'interface sélectionnée qu'au trafic VPN.  
[Pour plus d'informations sur les interfaces réseau.](#)  
[Pour plus d'informations sur le filtrage des paquets.](#)

< Précédent Suivant > Annuler

# Configurer l'attribution d'adresses IP

Assistant Installation d'un serveur Routage et accès distant

**Attribution d'adresses IP**

Vous pouvez sélectionner la méthode d'attribution des adresses IP aux clients.

Comment voulez-vous que les adresses IP soient attribuées aux clients distants ?

Automatiquement  
Si vous utilisez un serveur DHCP pour attribuer des adresses, vérifiez qu'il est configuré correctement. Si vous n'utilisez pas de serveur DHCP, ce serveur générera les adresses.

À partir d'une plage d'adresses spécifiée

Assistant Installation d'un serveur Routage et accès distant

**Attribution de plages d'adresses**

Vous pouvez spécifier les plages d'adresses que ce serveur utilisera pour assigner des adresses aux clients distants.

Nouvelle plage d'adresse IPv4

Entre toute Plag De

Entrez une adresse IP de début et soit une adresse IP de fin, soit le nombre d'adresses contenues dans la plage d'adresses.

Adresse IP de début : 192 . 168 . 1 . 200

Adresse IP de fin : 192 . 168 . 1 . 219

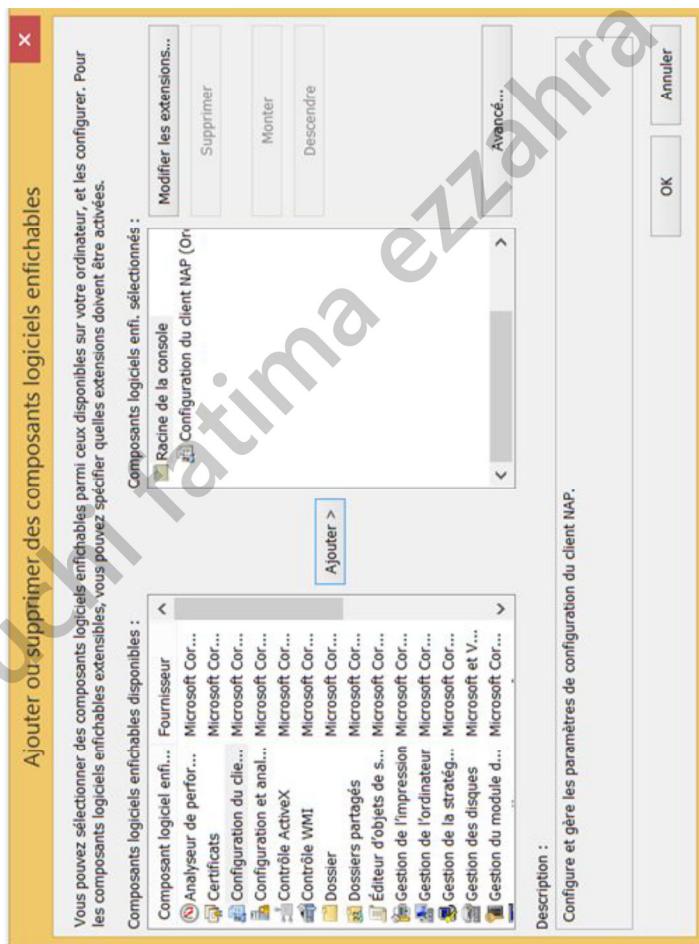
Nombre d'adresses : 20

OK Annuler

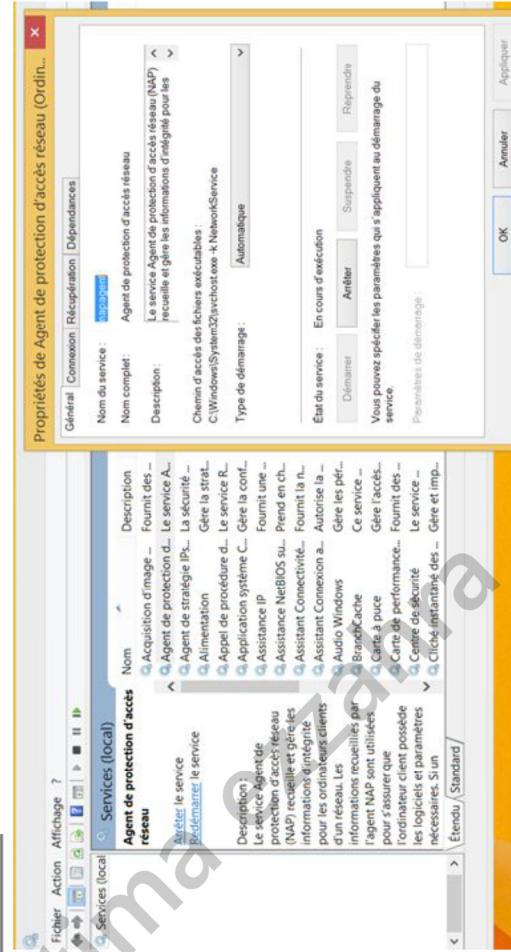
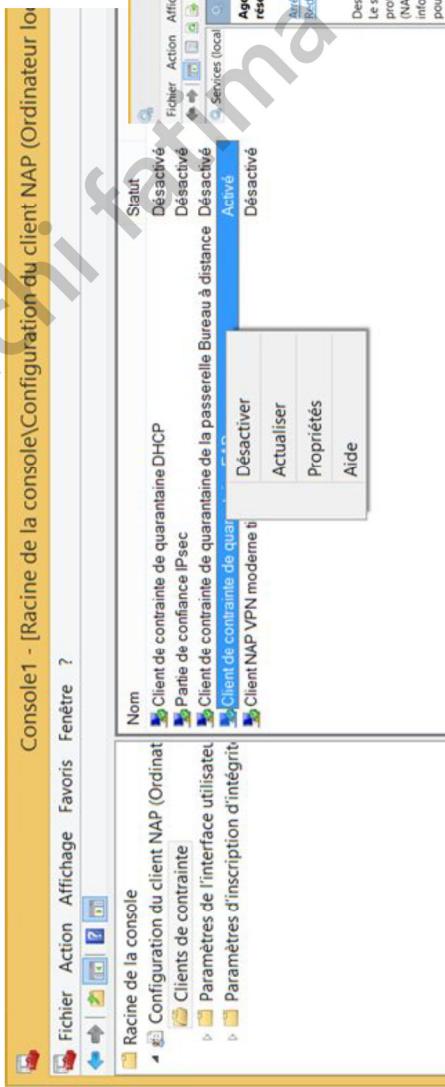
< Précédent Suivant > Annuler Annuler

# Configuration des paramètres clients pour prendre en charge la protection d'accès réseau (NAP)

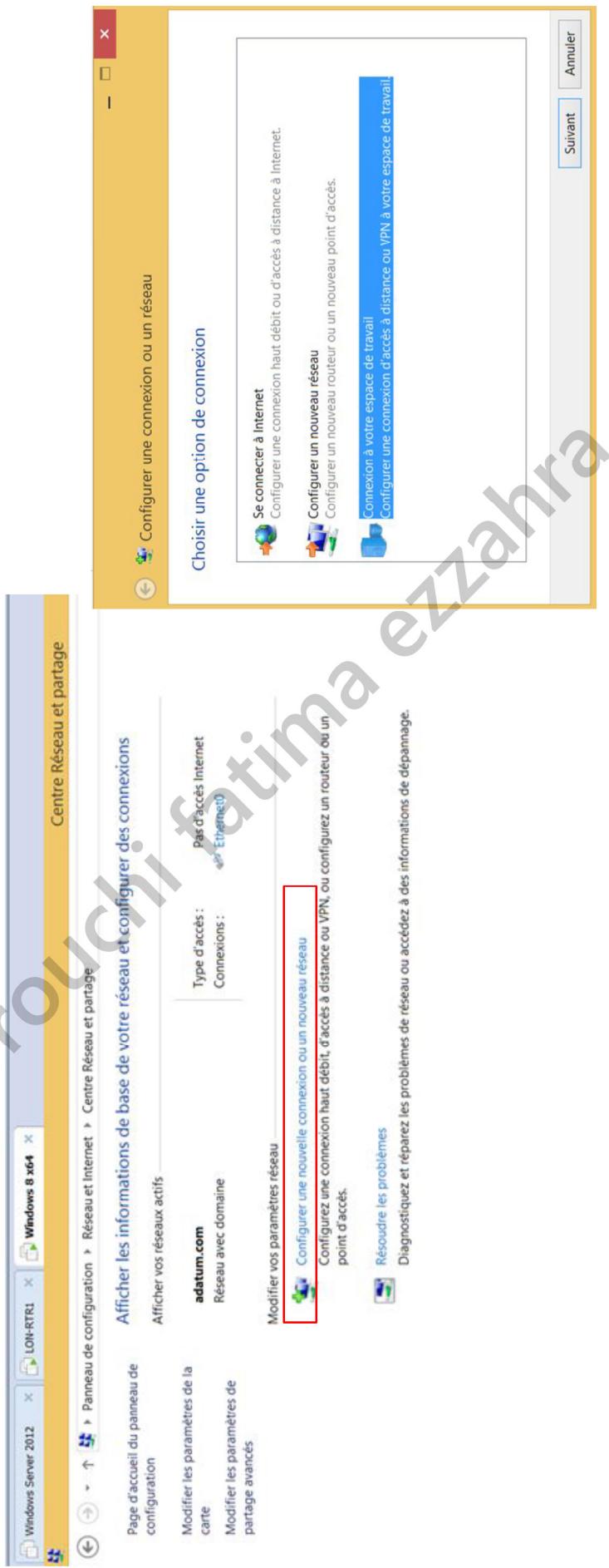
## Activer une méthode de contrainte de mise en conformité NAP d'un client



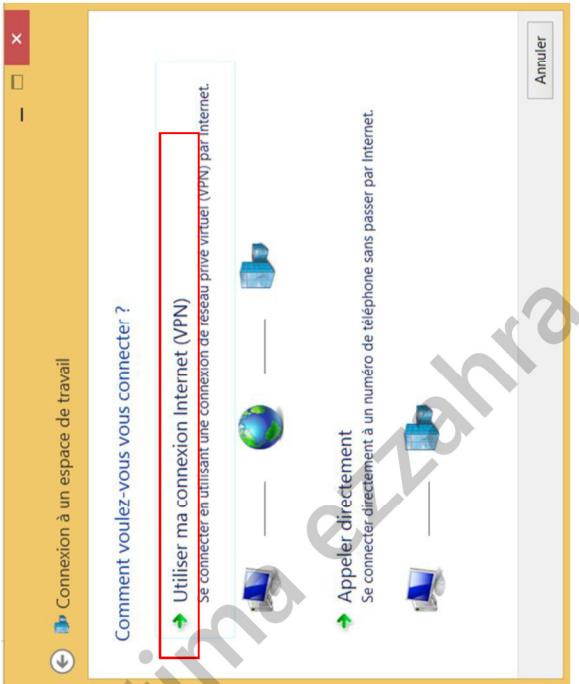
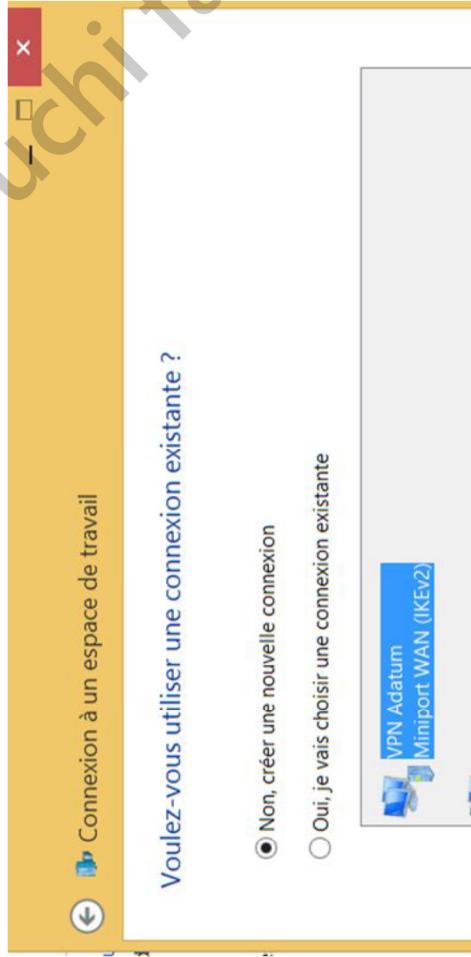
# Activer le client de contrainte EAP de quarantaine



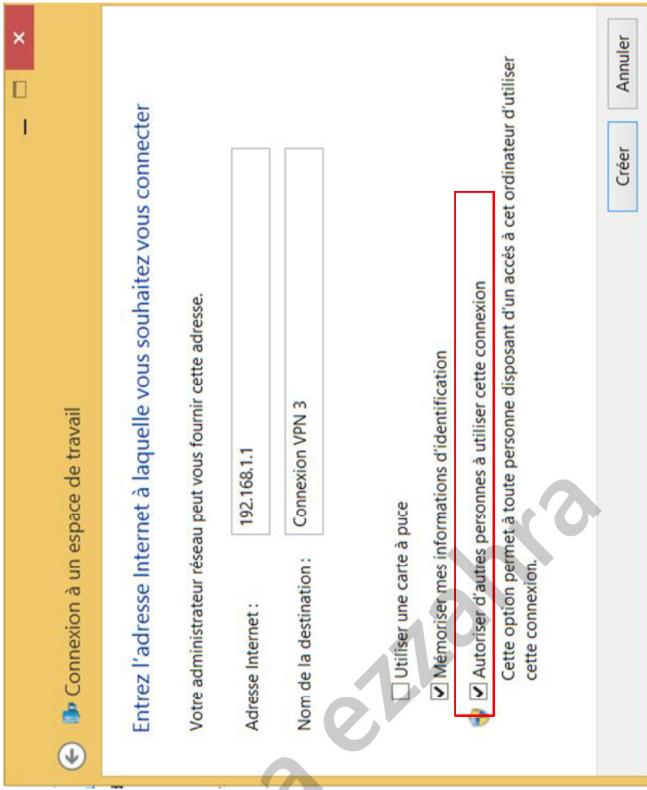
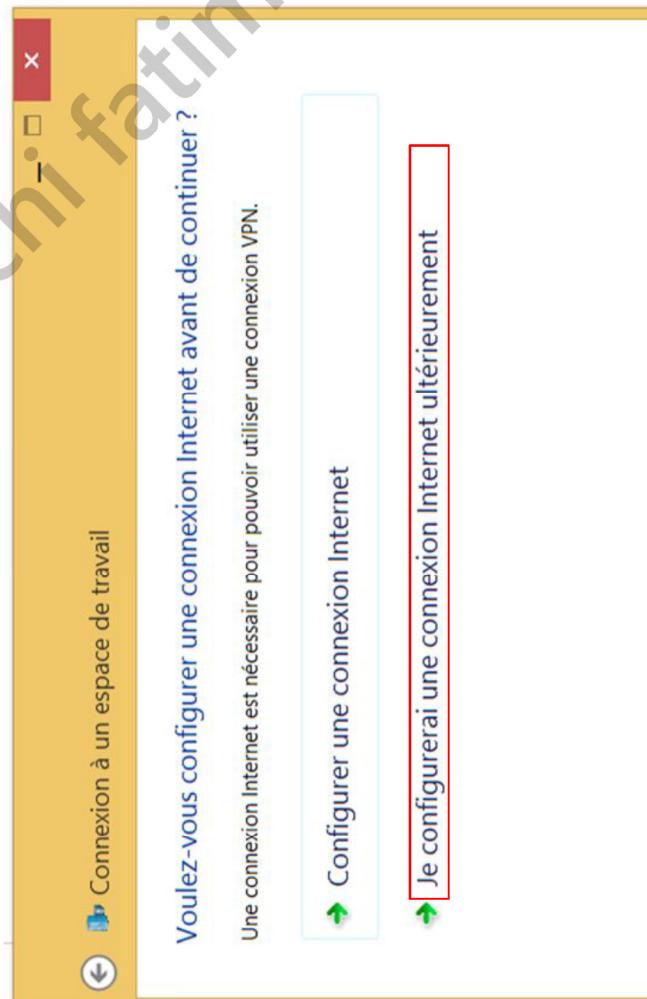
## Établir une connexion VPN



- Configurer une nouvelle connexion ou un nouveau réseau
- Choisir une méthode de connexion



## Saisir les informations du VPN



## Configurer les paramètres de sécurité

