2021

Network Access Protection

Présentation et configuration

Olivier D.

Table des matières

1 Présentation

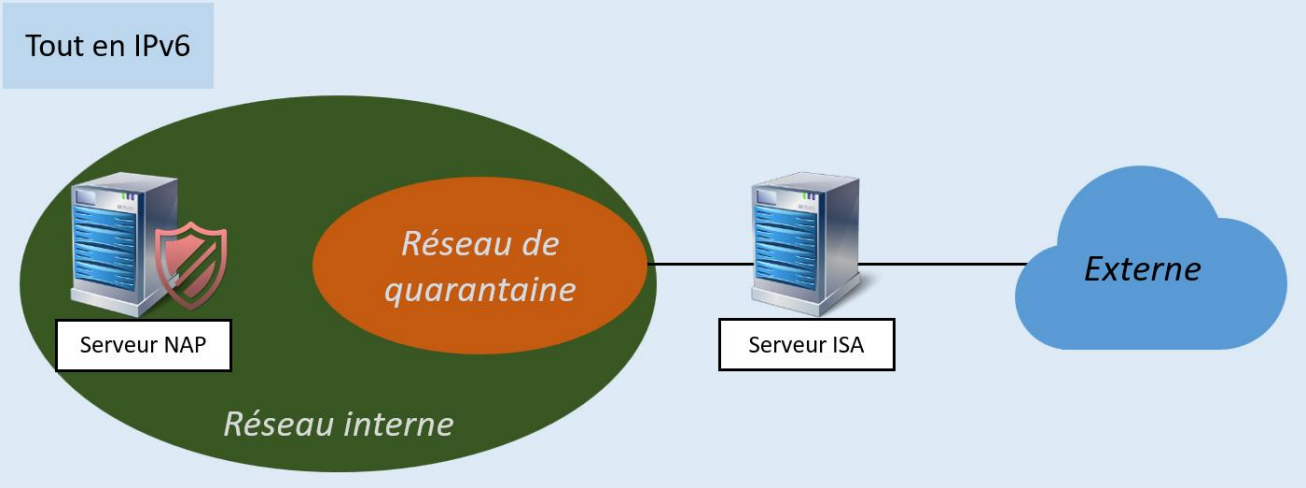
NAP est un service serveur. Network Policy Service (NPS)

Installer le rôle **Services de stratégies et d'accès réseau** et les fonctionnalités requises (outils)

Documentation

Documentation officielle Microsoft : Protection d'accès réseau (NAP) - Win32 apps | Microsoft Docs

Impact d'IPv6 au sein des infrastructures de réseau



Les impacts liés à IPv6 : La DMZ disparait et il n'y a plus de NAT.

Il faut obligatoirement faire du cryptage, de l'intégrité, **Utilisation obligatoire des certificats.**

Rôle de NAP

Contrôler l'état d'intégrité du système selon plusieurs paramètres :

- Antivirus ?
- Pare-feu ?
- Correctifs de sécurité ?
- Stratégie locale / GPO ?
- Certificat d'intégrité présent (besoin d'une PKI et d'une HRA) ?

Un client NAP peut être :

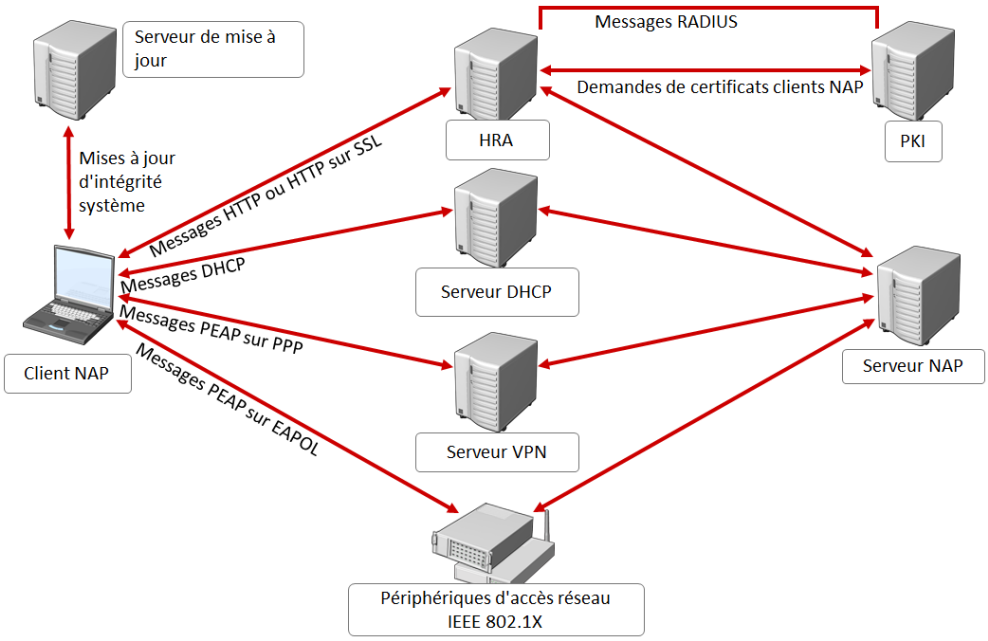
- conforme
- non-conforme

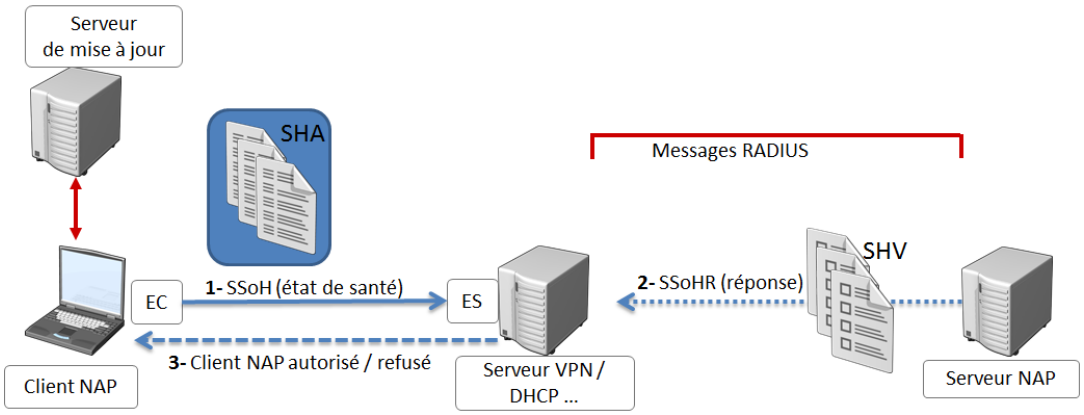
Domaine d'application

- Clients en interne, via IPsec (mode transport)
- Clients NAP en interne (lourd à gérer)
- Conformité des postes en interne (contrôle des mises à jour WSUS)
- Ordinateurs externes à l'entreprise

Nota : pour les ordinateurs en VPN, cela requiers L2TP + IPsec + RADIUS + NAP. C'est une usine à gaz !

2 Architecture





Vocabulaire lié à NAP

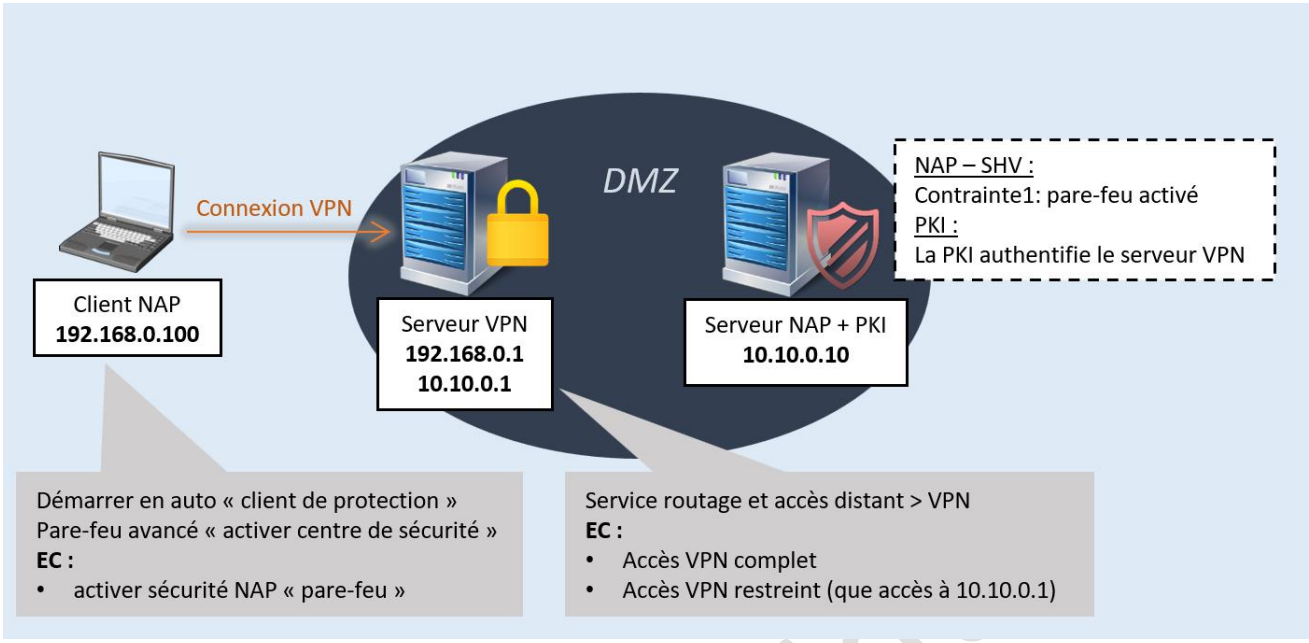
- **SSoH** : bulletin d'état de santé
- **SSoHR** : réponse (conforme / non conforme)
- **EC** : client de contrainte (réglage via la console mmc)
- **ES** : serveur de contrainte

2.1 Configuration de la protection

Configuration des SHV :

- Rejeter la demande d'accès
- Réseau restreint (+ serveurs de mise à jour pour mettre à jour les postes client. Par exemples les antivirus)
- Autoriser la demande

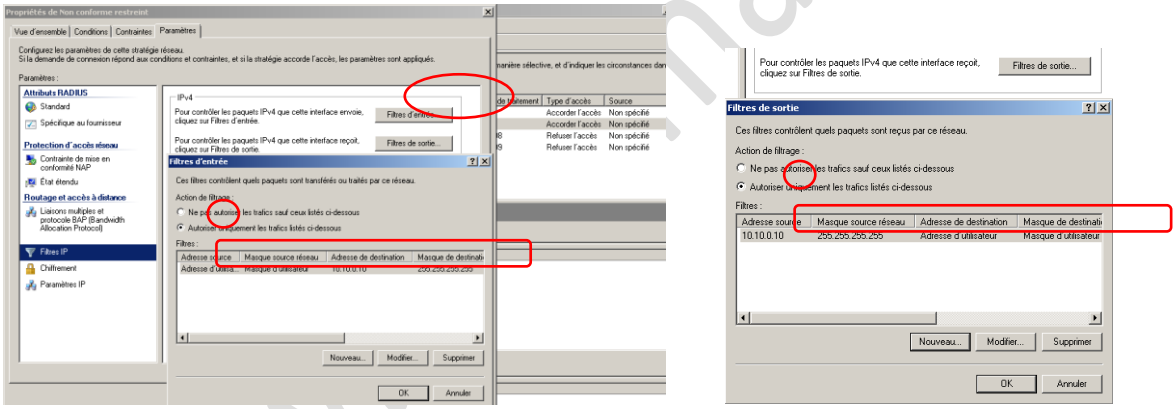
3 Pas à pas - configurer NAP pour VPN

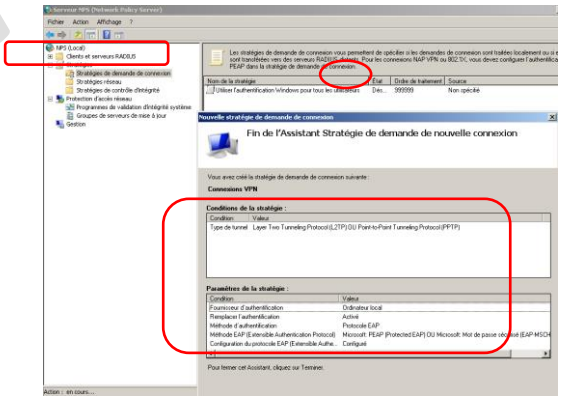


Résultat à obtenir

Coté serveur NAP

Console Serveur NPS > Stratégie « Non conforme restreint »

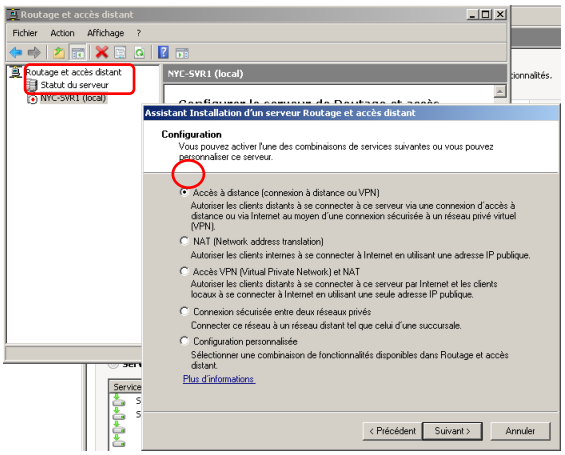


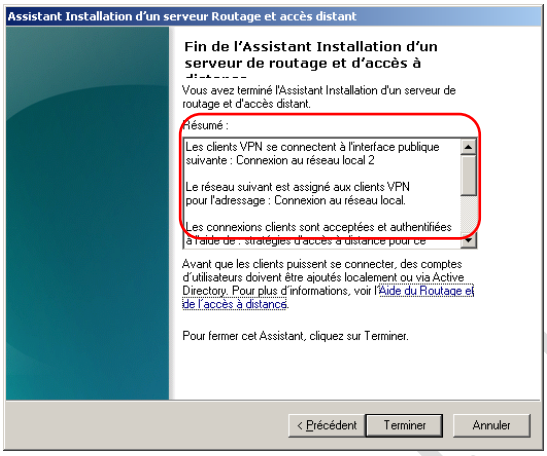


- *Paramétrage des stratégies du serveur NPS*

Côté serveur VPN

Console routage et accès distant

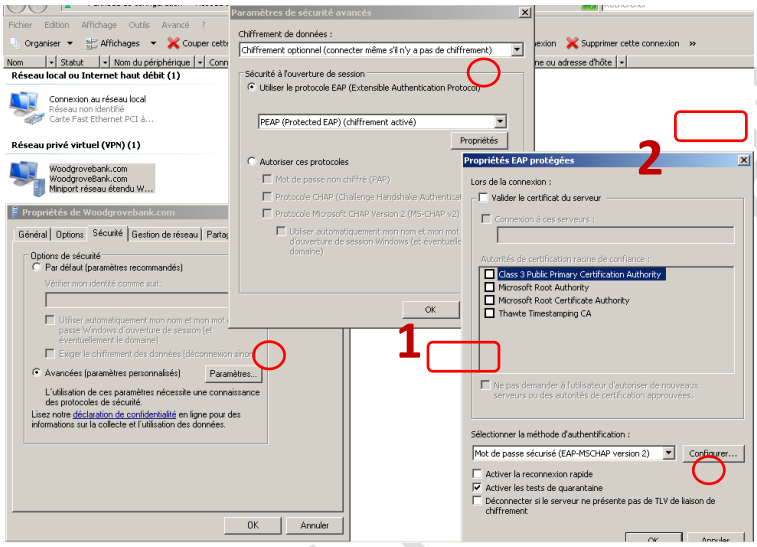




- *Paramétrage du service VPN*

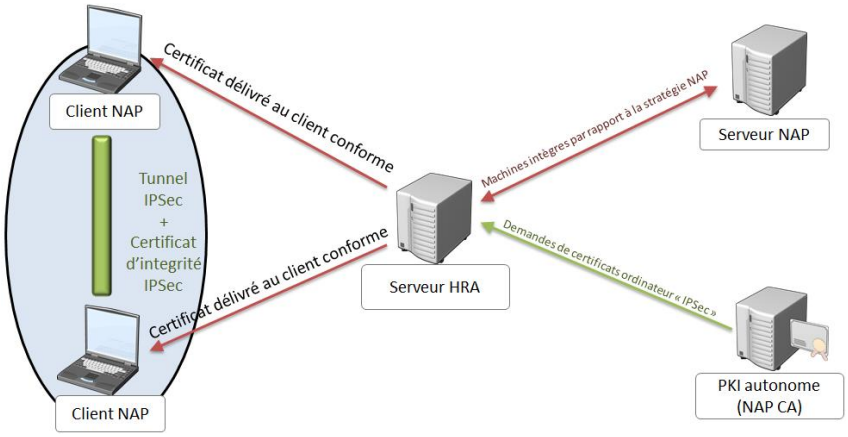
Coté client VPN

Réseau > Paramétrage de l'accès VPN



- *Paramétrage de NAP coté client VPN*

4 HRA



- *Fonctionnement de HRA*

Demandes de certificats par GPO ; certificat ordinateur IPSec

	durée de vie du certificat : quelques heures

Les machines, par le biais des protocoles IKE / AH / ESP, vont utiliser le certificat obtenu

5 IPSec + NAP

Client conforme ET avec certificat d'intégrité IPSec :

- réseau normal

Client conforme ET sans certificat d'intégrité IPSec :

- réseau de quarantaine : contact HRA pour obtenir un certificat

Client non conforme ET sans certificat d'intégrité IPSec :

- Pas d'accès au réseau

6 Pas à pas - configuration HRA