

# Politique de filtrage pour les réseaux sans fil mis à disposition des nomades

*Ou comment sécuriser un réseau sans fil  
tout en permettant aux nomades de travailler.*

## Introduction

Ce document de préconisations a pour objectif de faciliter la vie des personnes dites « nomades » utilisant les réseaux sans fil mis à leur disposition par le site « hôte » pour assurer la connectivité vers leur établissement de rattachement ainsi qu'à l'Internet global.

Le niveau de qualité de la connectivité via réseau sans fil est fonction :

- du niveau de débit correct autorisant le transfert de volumes substantiels de données sans perte de temps (~1Mb/s par utilisateur);
- la « solidité » de la protection du lien radio et de la stratégie d'authentification, associée à la facilité de connexion; (solidité ne devant pas signifier difficulté pour se connecter);
- du nombre de ports réseau ouverts (en sortie particulièrement) permettant à l'utilisateur de travailler sans difficultés ;

Le présent document traite uniquement du dernier point. Il est porté à la connaissance de l'ensemble des sites RENATER, invités à mettre en oeuvre les propositions explicitées ci-dessous.

## Politique de filtrage des flux sortants d'un réseau sans fil

Le tableau ci-dessous propose un ensemble minimum de services à ouvrir en sortie des réseaux d'accueil afin que tout nomade puisse travailler sans blocage inutile, et sans pour autant que le réseau d'accueil ne soit lui-même mis en péril.

Les services minimum auxquels tout nomade doit pouvoir accéder sont les suivants:

- les services WEB, non sécurisés et sécurisés;
- les services de messagerie (consultation et soumission) sous différents protocoles, afin de ne pas contraindre l'utilisateur à passer par un service de type WebMail pour gérer son courrier électronique.
- des accès sécurisés aux serveurs distants avec possibilité d'encapsuler d'autres protocoles (type VPN) afin d'avoir un accès transparent et sécurisé aux environnements de son lieu de travail habituel.
- Les services non applicatifs, mais cependant indispensables, comme le DNS et ICMP.

## Préconisation d'une liste de ports à ouvrir

Service	Protocole applicatif	Prot. IP	Port local	Port distant	sens	
Accès WEB	HTTP	TCP	*	80	Sortie	
	HTTPS	TCP	*	443	Sortie	
Courrier électronique consultation	POP	TCP	*	110	Sortie	Deux protocoles non sécurisés. Les utilisateurs doivent être sensibilisés Il est conseillé (voir IANA) d'utiliser TLS comme sécurisation en conservant les mêmes numéros de ports.
	IMAP	TCP	*	143	Sortie	
	POPS	TCP	*	995	Sortie	Accès sécurisé
	IMAPS	TCP	*	993	Sortie	Accès sécurisé
Courrier électronique envoi	SMTP submission	TCP	*	587	Sortie	Soumission sécurisée de message
	SMTPTS	TCP	*	465	Sortie	Non officiel. Cependant utilisé en lieu et place de 587
SSH	SSH	TCP	*	22	Sortie	Accès sécurisé pour l'administration système et tunneling application
OpenVPN		UDP et TCP	*	1194	Sortie	
IPSec	AHP	AHP	N/A	N/A	E/S	
	ESP	ESP	N/A	N/A	E/S	
	Isakmp	UDP	500	500	E/S	
IPSec NAT-T	NAT-T	UDP	4500	4500	E/S	NAT Traversal
IPSec Cisco	Cisco	TCP	*	10000	Sortie	Encapsulation VPN Cisco dans TCP (solution largement utilisée)
DNS	DNS	UDP	*	53	Sortie	Normalement le site d'accueil doit offrir un service de résolution DNS via DHCP
ICMP	ICMP	ICMP	N/A	N/A		Uniquement pour les fonctions « écho » et « reply »
NTP	NTP	UDP	*	123	Sortie	Ce service peut être fourni par le site d'accueil via annonce DHCP

\* signifie numéro de port supérieur à 1023.

N/A : Non Applicable