Politique de filtrage pour les réseaux invités

L'ensemble des sites RENATER est invité à mettre en œuvre les propositions explicitées ci-dessous.

Objectif

Permettre le télétravail des personnes nomades utilisant les réseaux mis à leur disposition par les établissements et organismes de la communauté RENATER.

Ces préconisations sont valables pour les réseaux sans fil ainsi que pour les réseaux filaires invités.

Moyens

Définition d'une liste de ports et protocoles à laisser ouverts en sortie des réseaux invités pour permettre aux utilisateurs nomades d'accéder aux services essentiels de leur établissement de rattachement tout en se conformant à la politique de sécurité de celui-ci.

Précisions importantes

Ce document ne doit pas être considéré comme une préconisation de sécurisation des réseaux invités, mais bien comme une préconisation d'ouverture d'une liste précise de ports en sortie de ces réseaux.

Un document complémentaire (« Préconisation pour la protection des réseaux sans fil ») évoque les différentes méthodes et mesures à prendre en considérations pour sécuriser les environnements de réseaux sans fil.

Un bon niveau de sécurisation des réseaux sans fil ne doit en rien empêcher l'ouverture des ports préconisés ci-dessous.

Liste des ports à ouvrir en sortie

La liste des ports précisés dans le tableau ci-dessous, est issue des préconisations « eduroam » et est communément admise comme étant celle qui doit permettre à tout utilisateur de travailler sans phénomène de blocage.

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

- les services WEB, non sécurisés (HTTP) et sécurisés (HTTPS);
- les services de messagerie (consultation et soumission) sous différents protocoles sécurisés, afin de ne pas contraindre l'utilisateur à passer par un service de type WebMail pour gérer son courrier électronique. Les services POP et IMAP non chiffrés ne devraient être ouverts que sous réserve du chiffrement du lien radio.
- 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.

Le tableau ci-dessous précise la liste et les caractéristiques des ports à ouvrir.

Par défaut les autres ports peuvent être bloqués.

Service	Protocole applicatif	Trans port	Port local	Port distant	Sens	Commentaires
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
	SMTPS	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 / 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		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