Nomadismes...

Stratégies de gestion *du* nomadisme et de la délocalisation, en terme de coûts, de risques et de services.

JSSI 2006 - 22 mai 2006

Jean-Luc Parouty
Institut de Biologie Structurale (IBS)

Cette présentation est strictement factuelle et technique et ne saurait engager l'IBS ou le CNRS d'une quelconque manière.

Version 2.01

IBS Grenoble
41, rue Jules Horowitz
38027 Grenoble Cedex 1 France

Plan :

1/ Problématiques

2/ Caractérisations des besoins

3/ Stratégies

4/ Exemples de solutions

Remarque :
Cette présentation ne prétend pas répondre à toute la problématique du nomadisme ;-)
Tout au plus présenter quelques éléments de décors, de contexte et... d'expérience... !

1 / Problématique

...des besoins utilisateurs, au pragmatisme des administrateurs...

Problématique...

Quelques données du problème...

- ***Nos intérêts « divergent » :***
  - Les utilisateurs ont des besoins :
    - Avoir un libre accès à leurs ressources
    - Pouvoir se connecter librement à l'Internet
    - Pourvoir accueillir librement leurs partenaires
  - Les administrateurs ont des contraintes :
    - Garantir le bon fonctionnement du SI
    - Protéger l'accès au système d'information
    - Protéger le SI des infections et des attaques

Problématique...

- ***Le monde change :***
  Les évolutions de l'Internet rendent caduques nos vieilles stratégies sécurités :
  - Portables, LiveCD, clefs USB :
    - Où sont les postes de travail ?
    - Où sont les données ?
  - Cable, ADSL, WiFi, etc. :
    - La connectivité devient omniprésente :
      Où est le réseau ?
  - Anonymisation progressive de l'Internet :
    - Tunnelisation, VPN, chiffrement :
      Où sont nos utilisateurs ?
    - Firewall, on peut tout faire avec ou sans eux ;-)
  - Chat, P2P, Skype, services distants, etc.
    - Où sont les services ?

Problématique...

- La concurrence est ouverte :
  - Services : Google mail (gratuit) :
    - 2.6 Go
    - 38 langues, POP3, Forwarding, anti-spam, etc.
  - Connectivité : Free (29€ / mois) :
    - Téléphone « presque gratuit »
    - 5-15 Mb/s
    - Transfert de gros fichiers (1Go)
    - Chat, pages personnelles, etc.
  - Hébergement : Bluehost (7€/mois) :
    - 10 Go hébergé, 250 Go/mois
    - 6 domaines hébergés, 100 bases MySQL/PostgreSQL
    - 2500 adresses mail (POP, IMAP, Webmail, etc.)
    - SSH, FTP, SSL, Statistiques, PHP, Python, Perl, etc.
  - ...

Problématique...

Le problème n'est plus de mettre en oeuvre « sa » solution et de l'imposer à « ses » utilisateurs, mais de rechercher le meilleur compromis avec eux...

Cette solution doit être :

- Adaptée aux besoins
- Etre Acceptée et adoptée par les utilisateurs
- Etre « raisonnable » en terme de sécurité

Note : Principe de symétrie

- La logique voudrait que nos visteurs puissent disposer du même confort chez nous que nos utilisateurs chez eux

2/

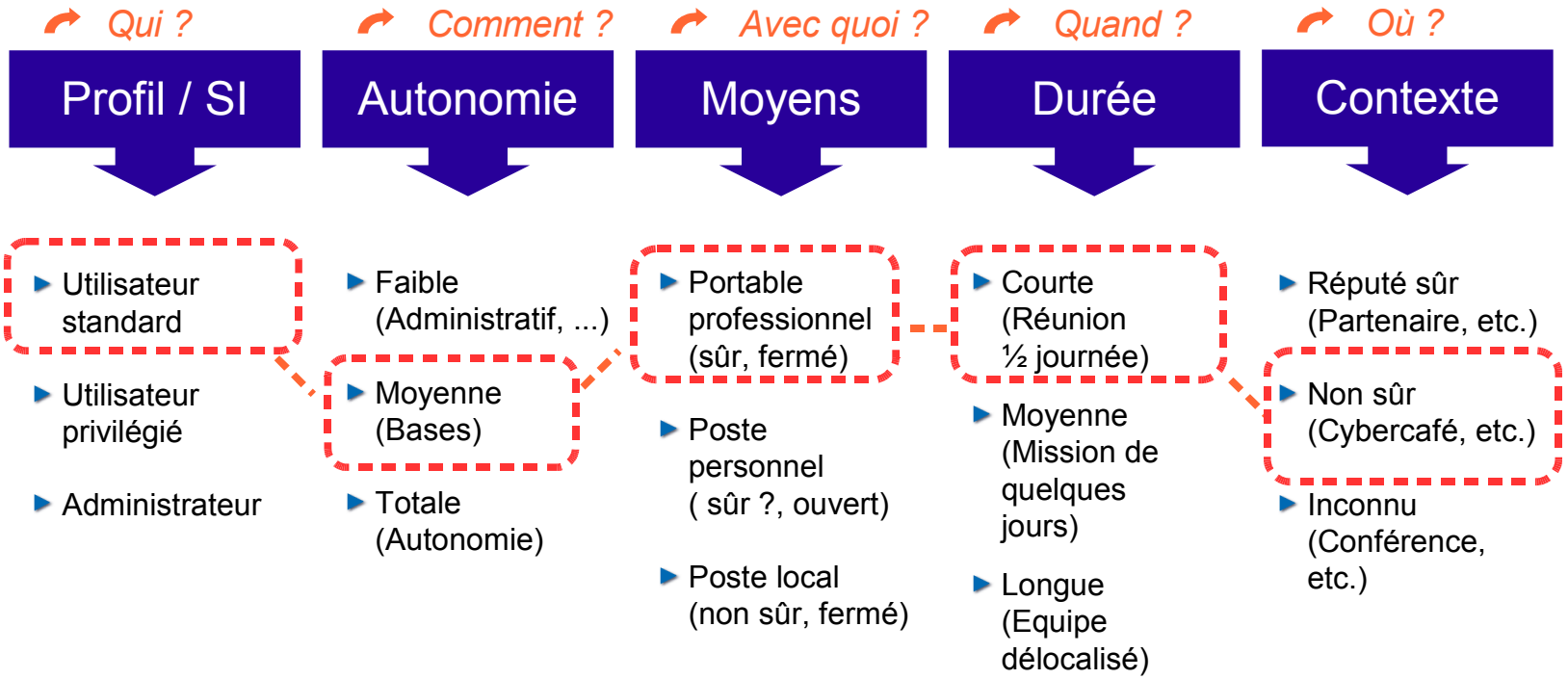
Caractérisation des besoins...

Qui sont les nomades ?
Quels sont leurs besoins ?

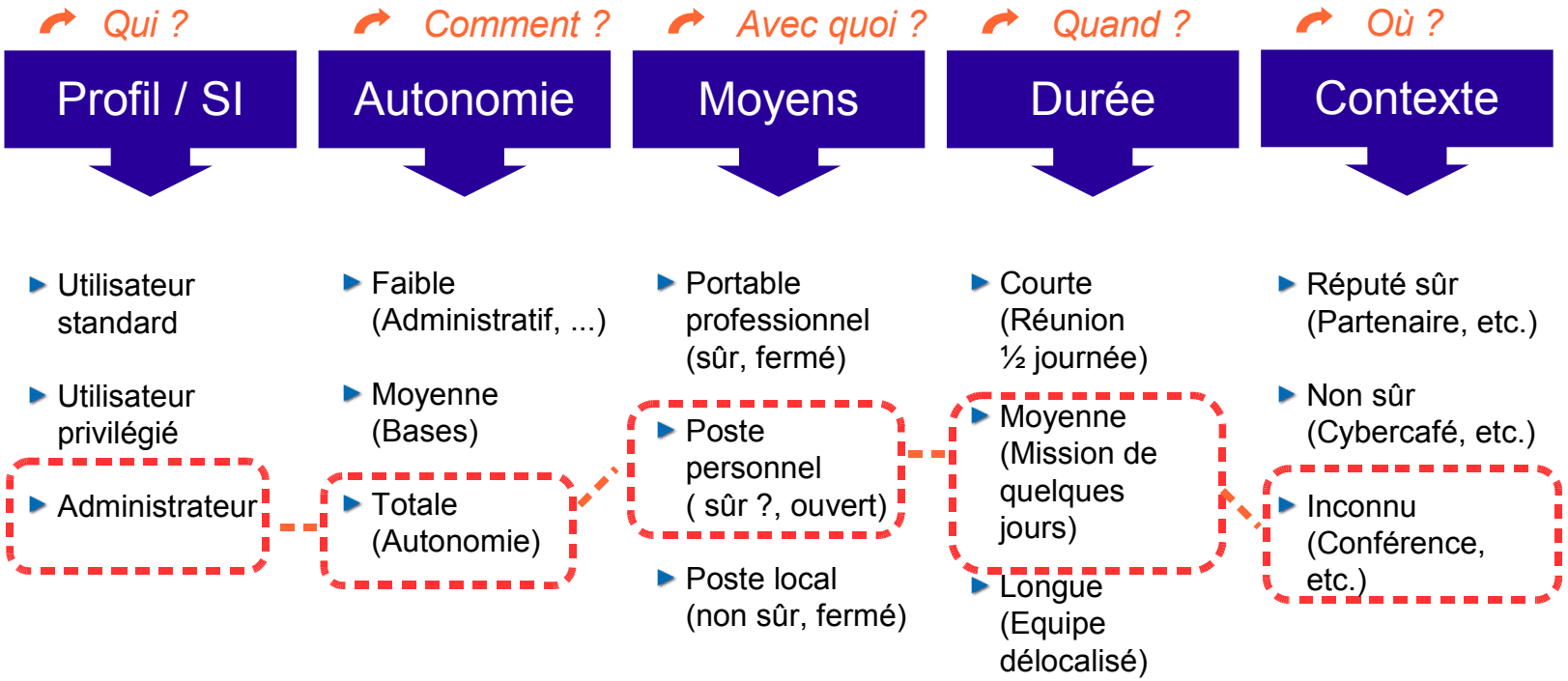
Profils des nomades

Qui ?	Comment ?	Avec quoi ?	Quand ?	Où ?
Profil / SI	Autonomie	Moyens	Durée	Contexte
▸ Utilisateur standard	▸ Faible (Administratif, ...)	▸ Portable professionnel (sûr, fermé)	▸ Courte (Réunion ½ journée)	▸ Réputé sûr (Partenaire, etc.)
▸ Utilisateur privilégié	▸ Moyenne (Bases)	▸ Poste personnel (sûr ?, ouvert)	▸ Moyenne (Mission de quelques jours)	▸ Non sûr (Cybercafé, etc.)
▸ Administrateur	▸ Totale (Autonomie)	▸ Poste local (non sûr, fermé)	▸ Longue (Equipe délocalisé)	▸ Inconnu (Conférence, etc.)

Profils des nomades



Profils des nomades



Quels services ?

★★★ Service exigé

★★ Demande forte

★ Excusé

En plus et par défaut :

Ne pas oublier :

- Protection des données embarquées
  - Contre le vol
  - Contre la perte

3/ Stratégies de réponses aux besoins

Quels services, pour quels nomades ?

Stratégies de réponses

Objectifs (rappel) :

- Répondres aux besoins des utilisateurs
  - Nous sommes là pour ça !
  - Eviter les frondes
- Protéger les utilisateurs exposés :
  - Minimiser les risques
  - Maximiser la simplicité (gage d'utilisation)

Stratégies de réponses (3 points)

1/ Couvrir les besoins essentiels :

- Besoins standards [nomadisme simple] :
  Accés par services : Tunnels (SSL)
  - POP, IMAP, SMTP, Web (peu critiques)
  - Tout environnement
- Besoins étendus [nomadisme privilégié] :
  Accés global : VPN (SSL)
  - Tous services (dont critiques)
  - Environnement controlés
- Protection des données embarquées [tous]

Stratégies de réponses (3 points)

2/ Minimiser les risques :

- Authentification forte
- Chiffrement

} SSL + IGC

3/ Faire simple :

- Formation / documentation
- Kits d'installation accessibles à tous utilisateur
- Clients ultra-légers « plug and play »
- Une seule technologie pour toutes les architectures, pour tous les clients.

Stratégies de réponses

Pour les nomades entrant : connectivité

- Accés ip vers l'Internet
- Solutions de type *hotspot* :
  - On veut savoir qui est sur notre réseau
  - La sécurisation est du ressort du nomade

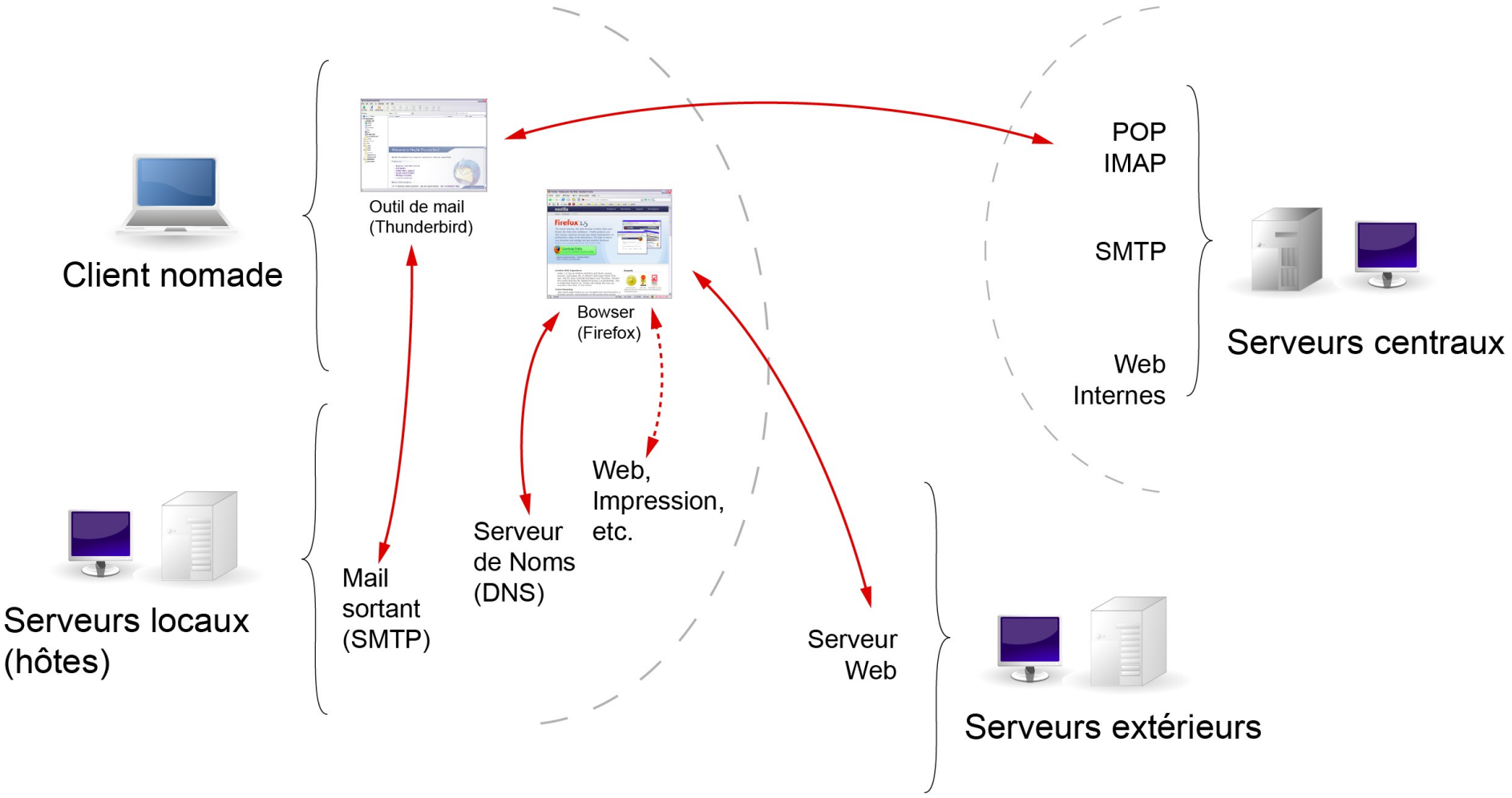
4/ Exemples de solutions :

Tunnelisation SSL (Nomadisme simple)
VPN SSL (nomadisme étendu)
Anonymisation
25g pour garder contact...

Pourquoi privilégier SSL et pas IPsec & co. ?

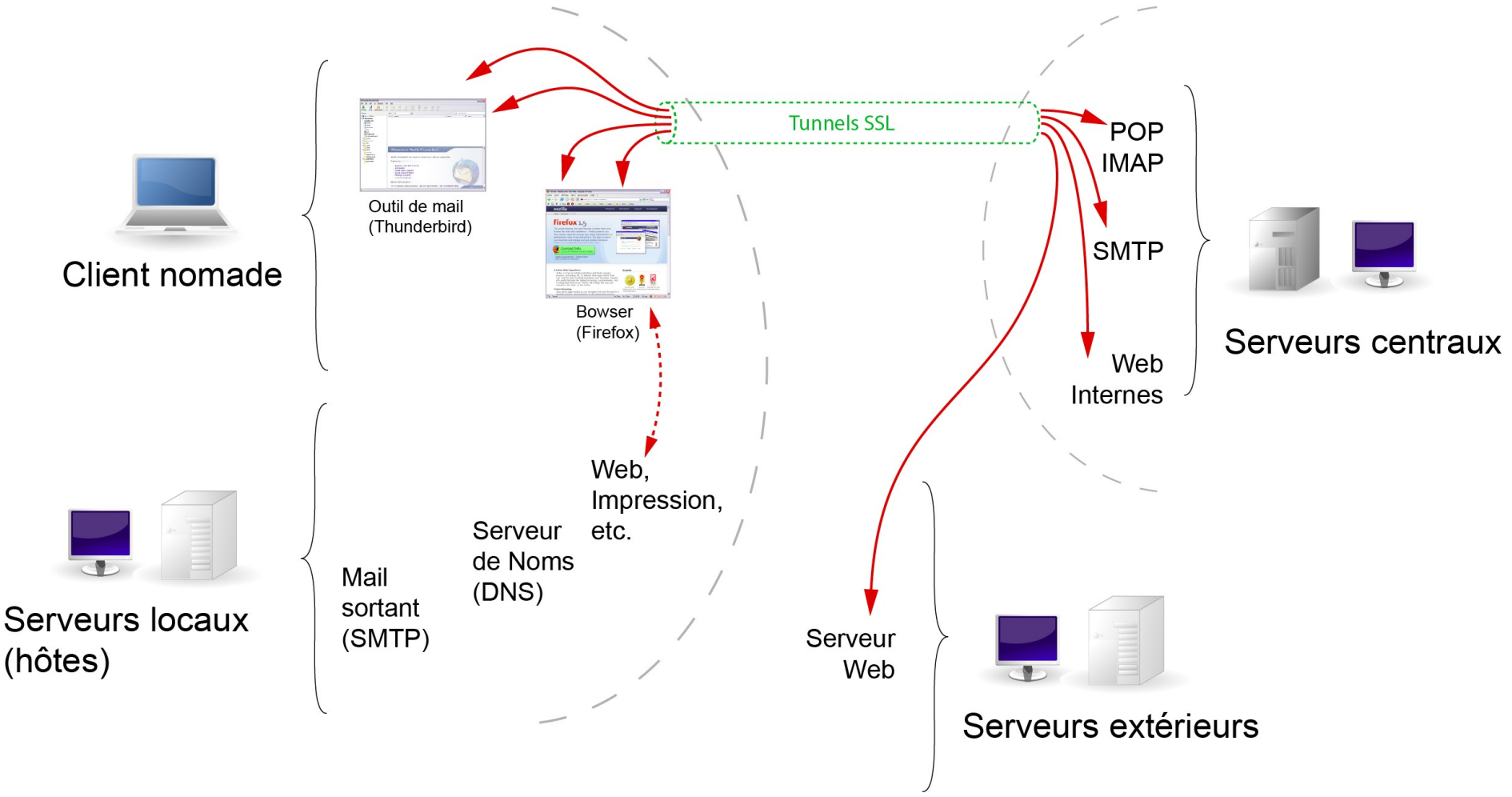
- Pas besoin de patcher les kernels
- Support complet de X509
- Passage aisé à travers les firewalls (via les proxy web, s'il le faut ;-)
- Granularité applicative : traitement par flux
- Réellement interopérable / multi-plateformes
- Support aisé de NAT
- Une seule technologie pour tout
- Solutions *OpenSource* validées
- ...

Tunnelisation



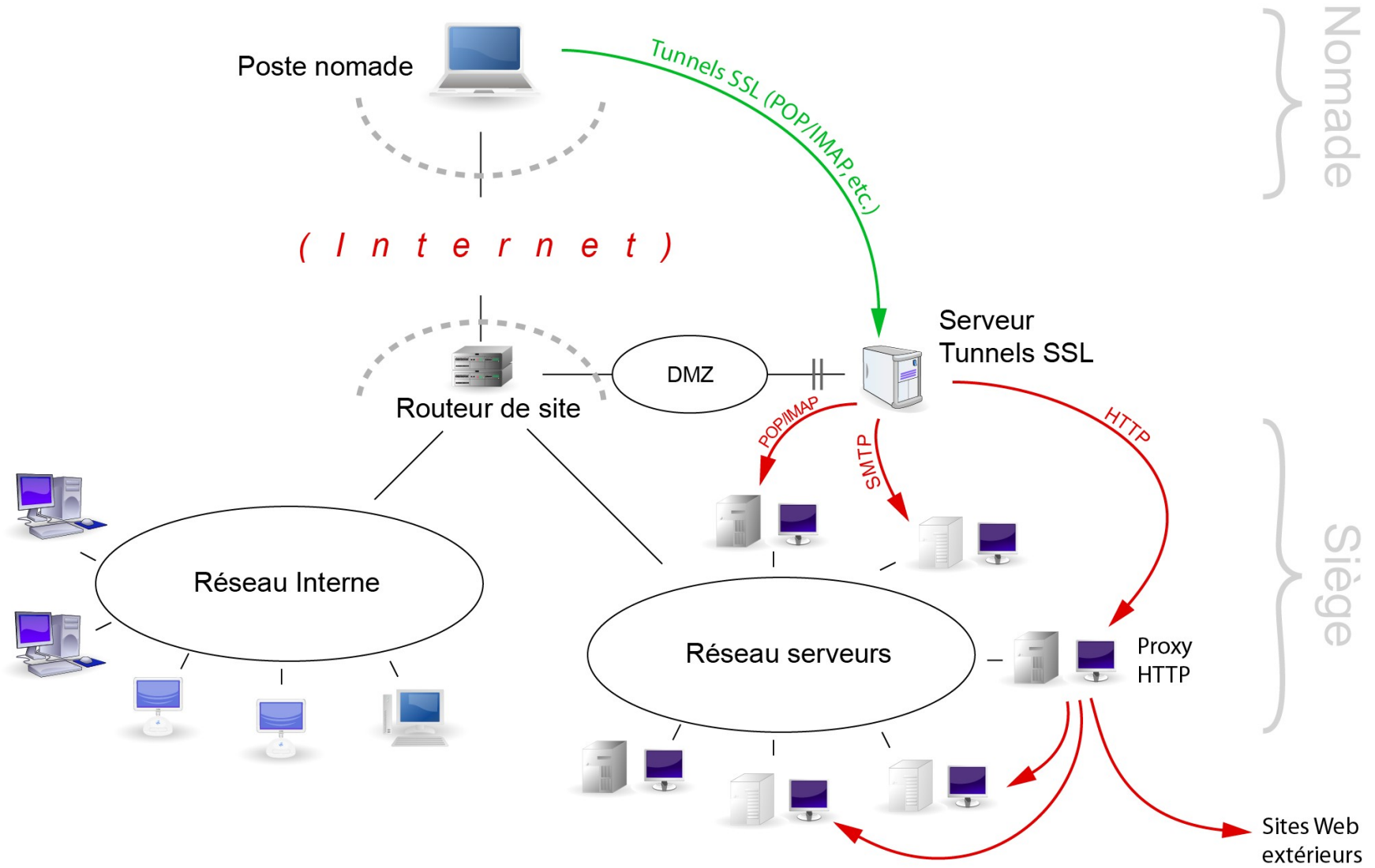
Les échanges « à risques » du « nomade standard »

Tunnelisation



Principe de la tunnelisation SSL

Tunnelisation



Exemple d'architecture d'une solution de tunnelisation SSL

Tunnelisation : Mise en oeuvre

- Mise en oeuvre technique : Stunnel [2]
  - Basé sur OpenSSL [1]
  - Multi-architecture
    - Windows
    - MacOs X
    - Linux
  - Simple, efficace, rustique, ergonomique et... gratuit !
- Mise en oeuvre aisée (via Devil-Linux [5])
  - 1 PC
  - 1 CD
  - 1 clef USB
  - (certificats)

} ½ journée
1 PC
Coût / support : modéré

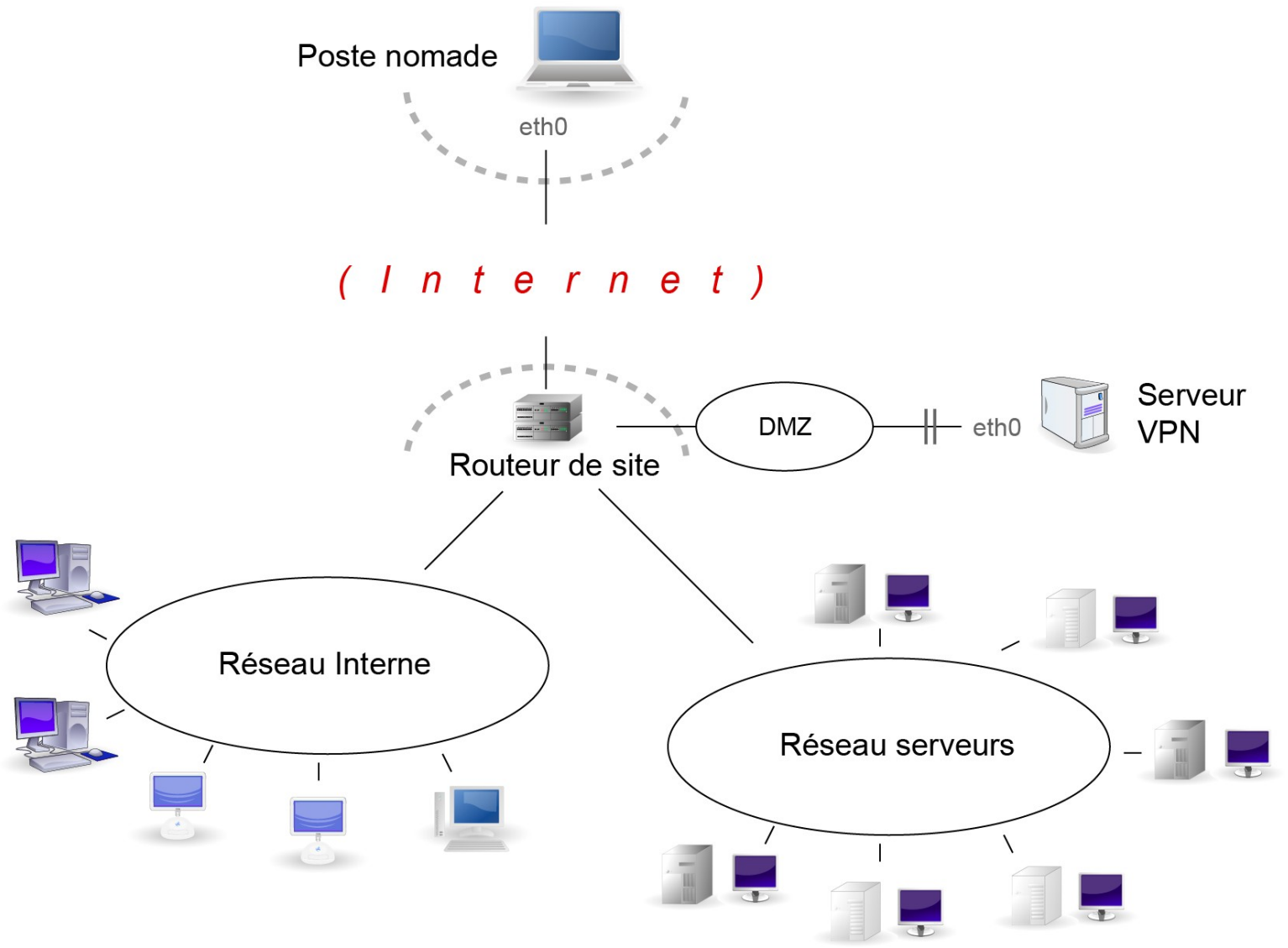
Tunnelisation : Risques

Risques :

(Dans le contexte de la tunnelisation pour le nomade simple)

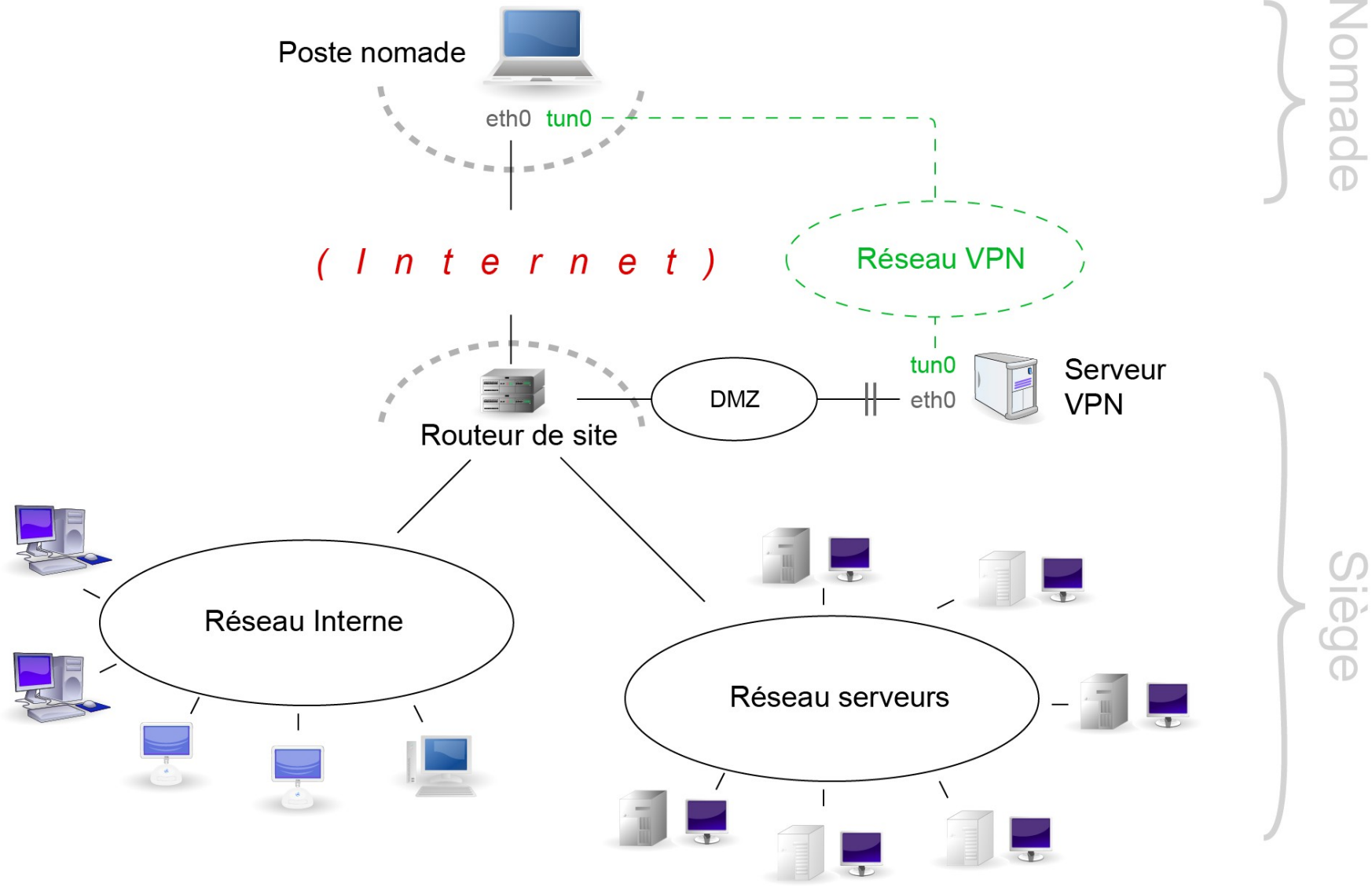
- Accès illicite aux serveurs POP/IMAP
  - Vol de courrier ?
  - Dénis de service
- Accès illicite au serveur SMTP
  - Envois illicite de courrier (spam...)
- Accès illicite aux serveurs Web
  - Accès à des informations internes
  - Accès à des applications internes

VPN SSL



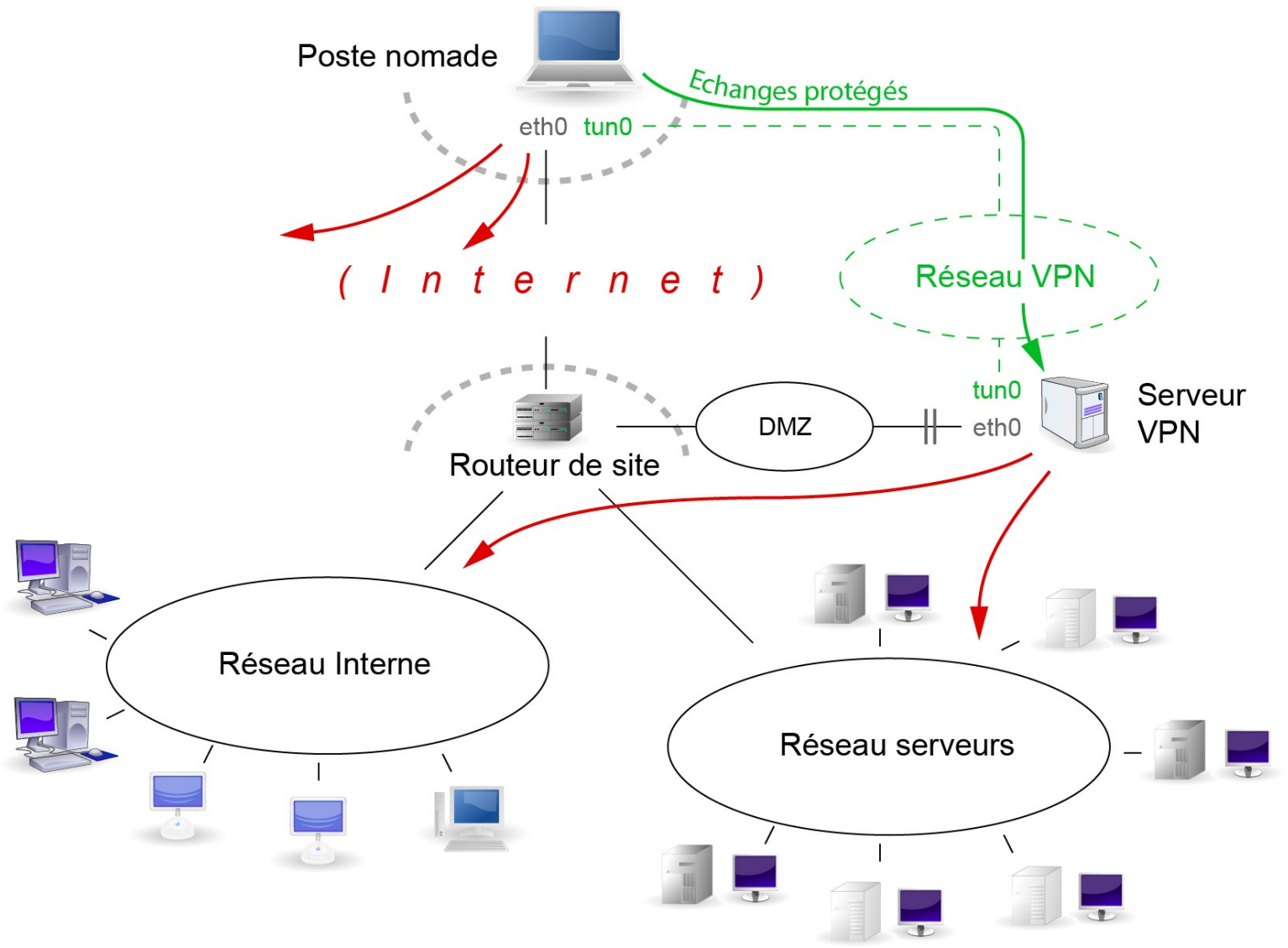
Principe d'un VPN (1/3)

VPN SSL



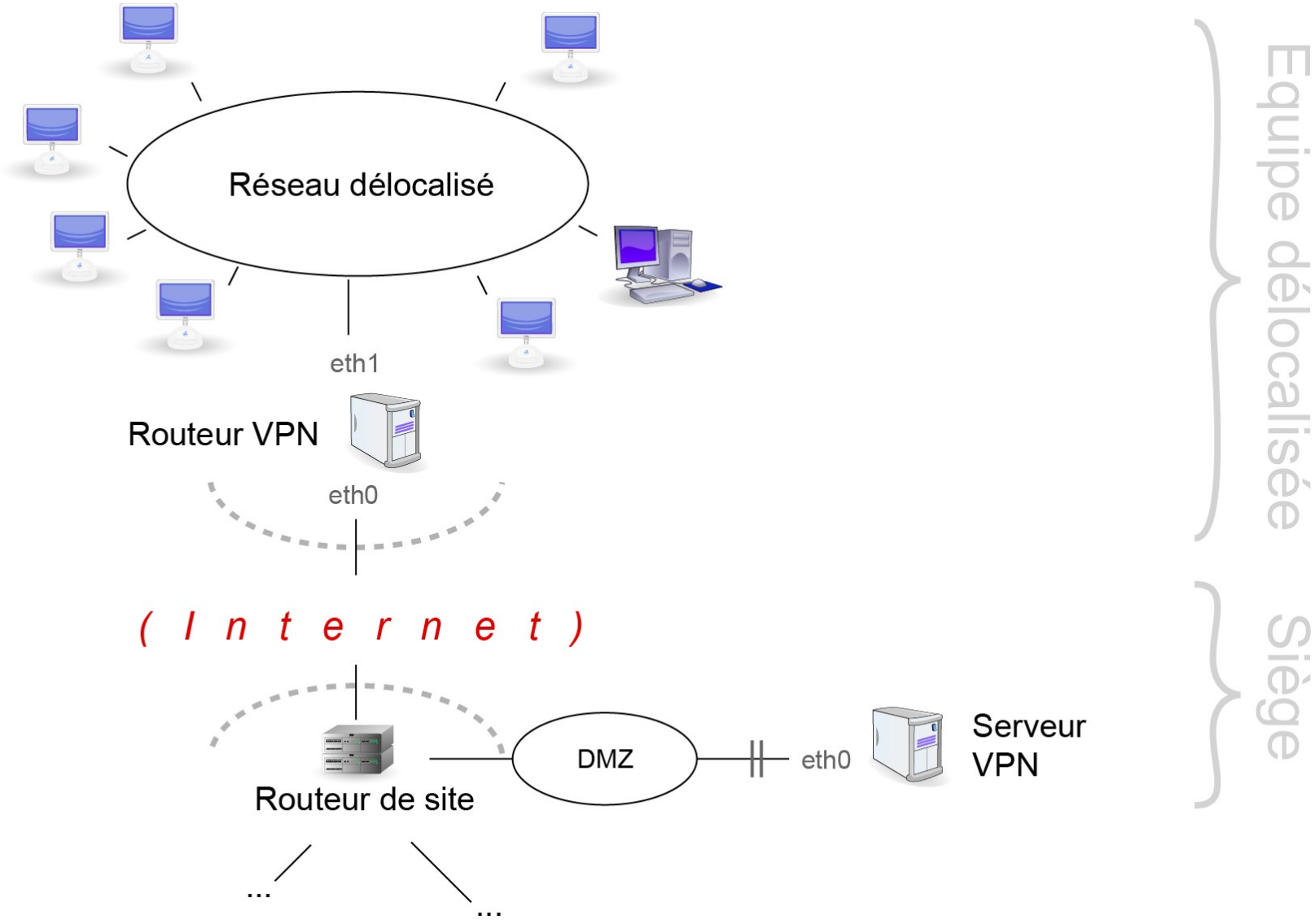
Principe d'un VPN (2/3)

VPN SSL



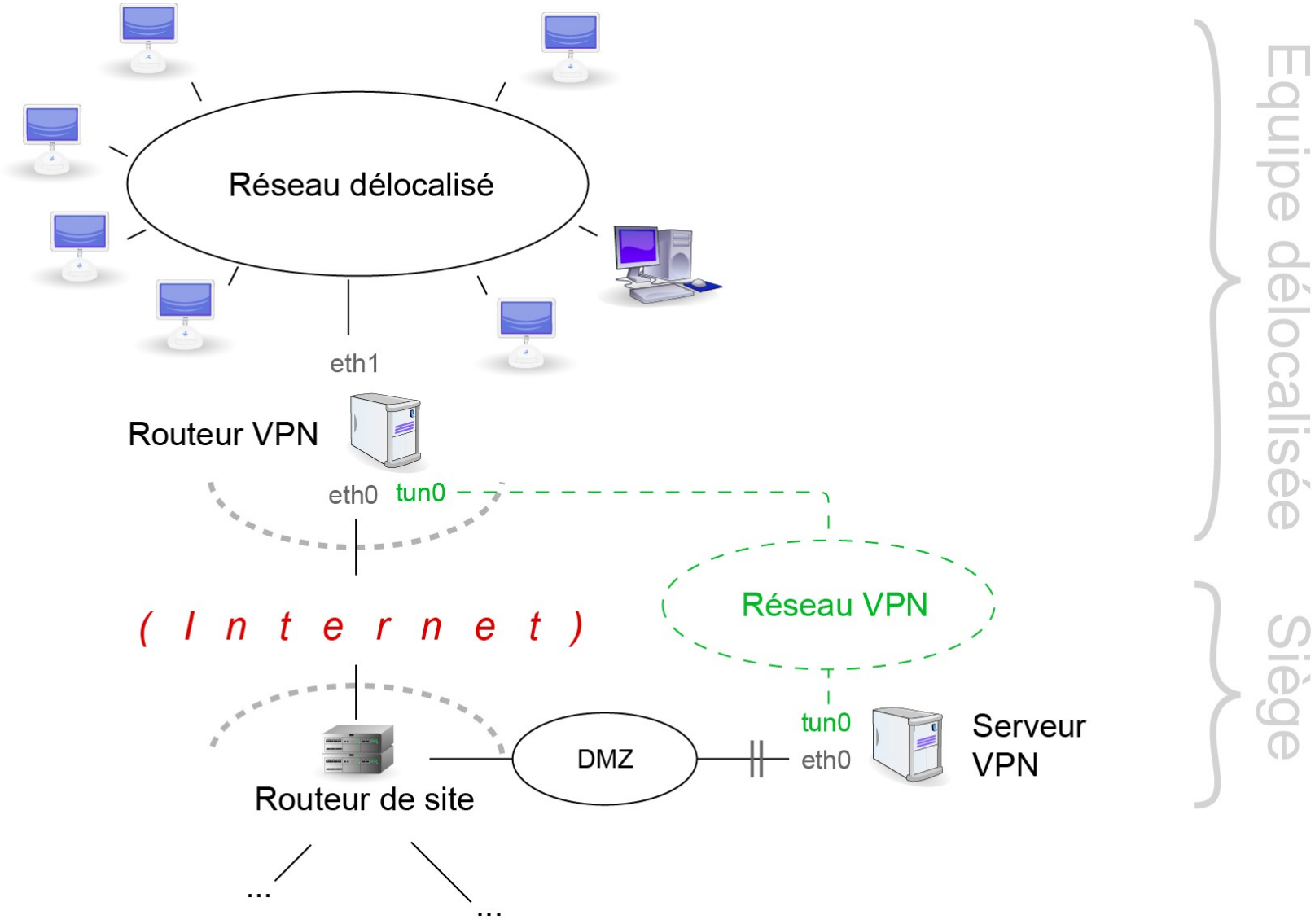
Principe d'un VPN (3/3)

VPN SSL



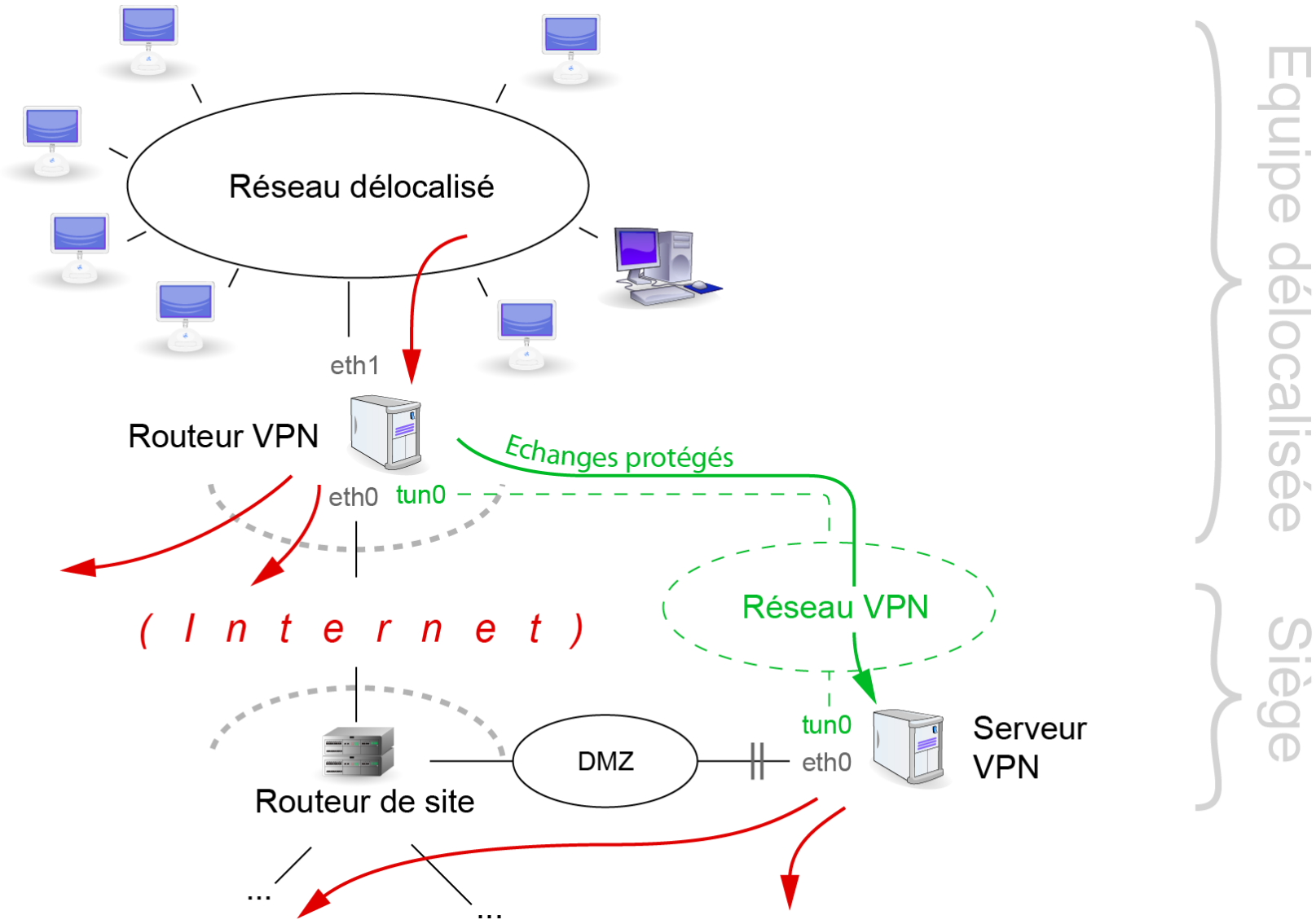
Cas de l'équipe délocalisée (1/3)

VPN SSL



Cas de l'équipe délocalisée (2/3)

VPN SSL



Cas de l'équipe délocalisée (3/3)

VPN SSL : Mise en oeuvre

- Mise en oeuvre technique : OpenVPN [3]
  - Basé sur OpenSSL [1]
  - Multi-architecture
    - Windows
    - MacOs X
    - Linux
  - Simple, efficace, rustique, ergonomique et gratuit !
- Mise en oeuvre aisée sous Devil-Linux [5]
  - 1 PC
  - 1 CD
  - 1 clef USB
  - (certificats)

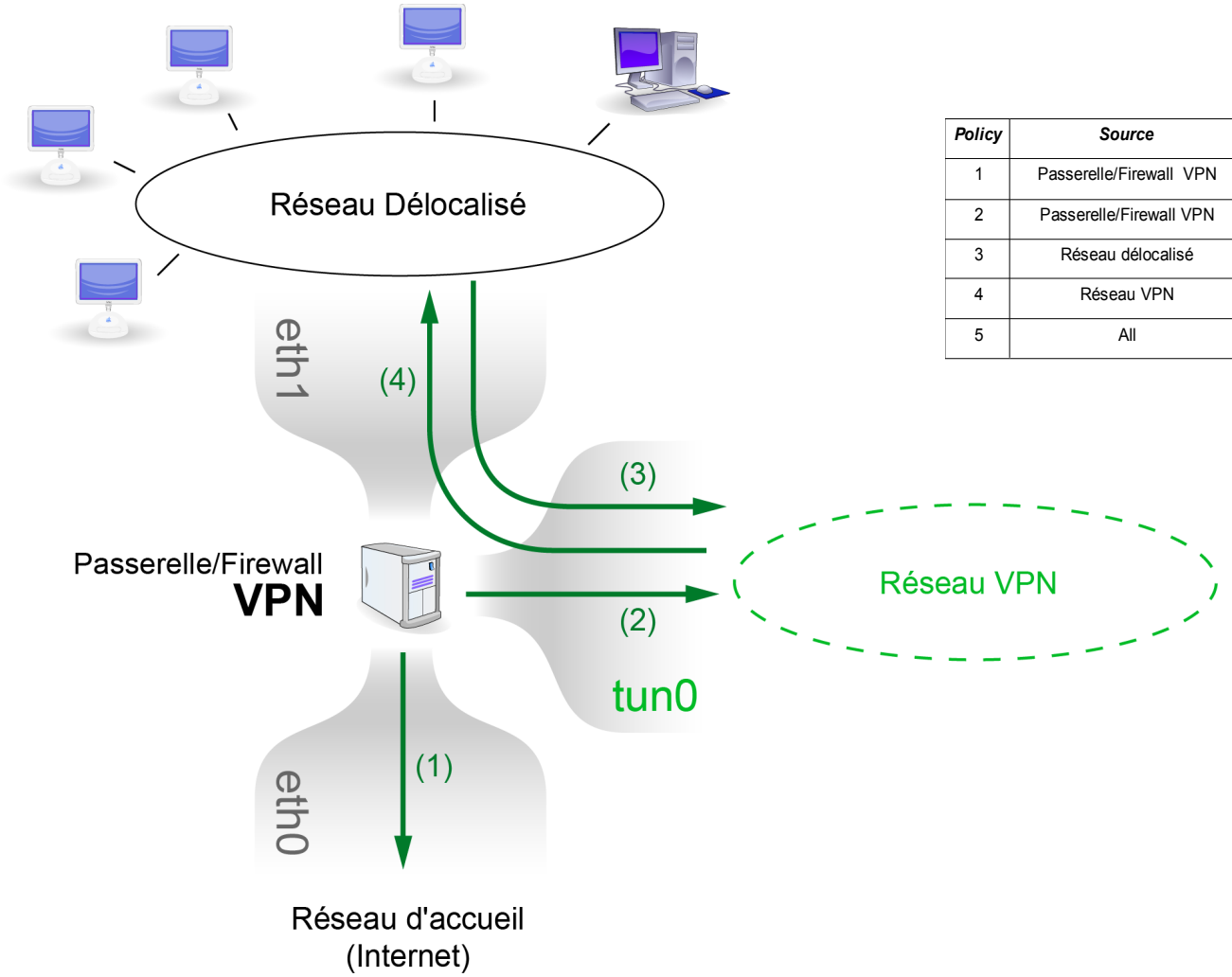
} 1 ou 2 semaines
1 PC (serveur)
Coût / support : moyens

VPN SSL : Risques

Risques :

- Potentiellement importants :
  - Accès à l'ensemble des ressources, sans discriminations...
    - Vrais, si configuration basique
    - Faux, si configuration évoluée, « à la carte »
    - Mais ne serait-ce pas là l'objectif ?
  - Clients nomades transformés en passerelles
    - Presque imparable...
- Nécessite de sécuriser le client VPN :
  - Politique de routage
  - Filtrage
  - Sécurisation du client et du serveur [4]

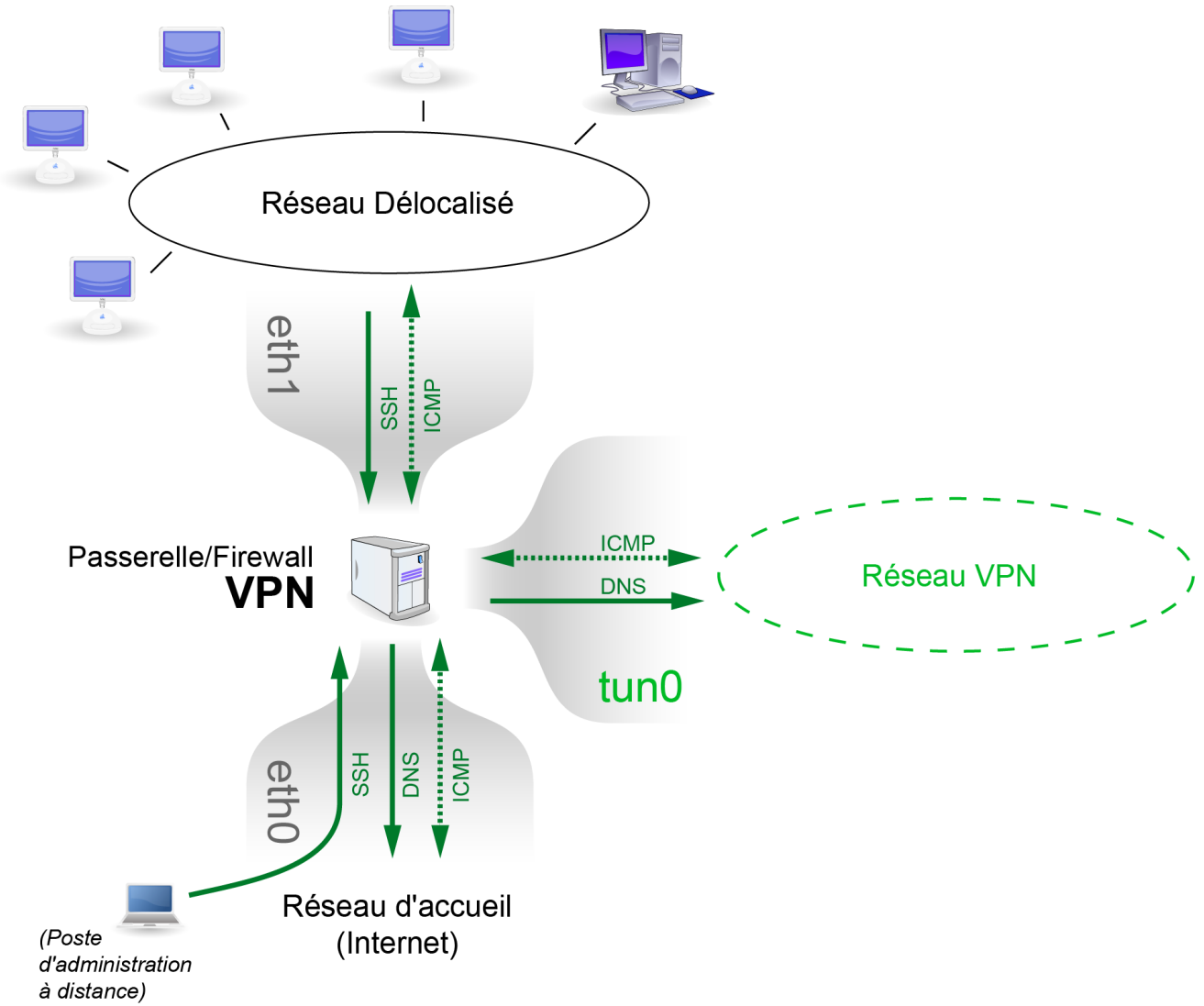
VPN SSL - Sécurisation



Policy	Source	Destination	Action
1	Passerelle/Firewall VPN	Réseau d'accueil / internet	ACCEPT
2	Passerelle/Firewall VPN	Réseau VPN	ACCEPT
3	Réseau délocalisé	Réseau VPN	ACCEPT
4	Réseau VPN	Réseau délocalisé	ACCEPT
5	All	All	REJECT

Politique de gestion des échanges entre « zones »
(Formalisation Shorewall [8])

VPN SSL - Sécurisation



Exceptions à la politique de gestion des échanges entre « zones »
(Formalisation Shorewall [8])

Anonymisation : Tor

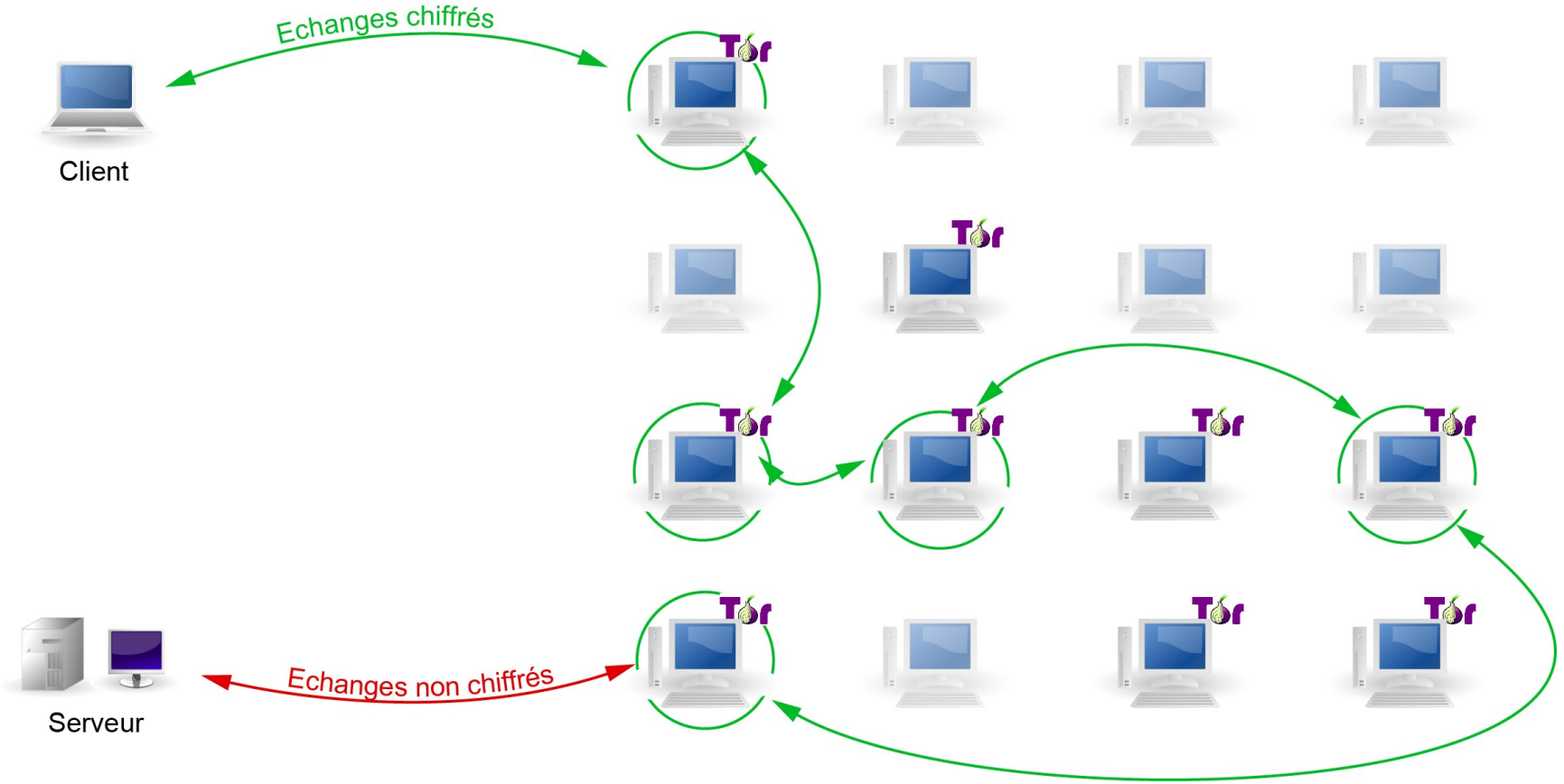
Approche furtive :

- Protéger ses échanges tcp (Web, etc.)
  - Contre l'analyse de trafic (opérateurs, etc.)
  - Contre la traçabilité des accés (sites visités, etc.)
- Approche « seul contre tous »
- « routeurs en peau d'oignons »
- Initié par « The Free Haven Project » (2002)
- Initialement financé par :
  - Electronic Frontier Foundation (EFF)
  - Naval Research Lab de l'US Navy
- Expérimental (mais très utilisable ;-)
- Air du temps : plusieurs projets (i2p, etc.)

Anonymisation : Tor

Requête classique : client et serveur en vis à vis direct...

Anonymisation : Tor



Requêtes via le réseau Tor : principe des routeurs en peau d'oignons

Problème paradoxal :

- Avantage du chiffrement :
  - Sans la clef, les donnnées sont inutilisables
- Inconvénient :
  - Sans la clef, les donnnées sont inutilisables

Protection des données

- Une solution de chiffrement doit :
  - Protéger les données (contre les vols)
    - Chiffrement fort
    - Code validé
    - Prise en compte du swap, de la corbeille, etc.
    - ...
  - Protéger les données (contre les pertes de clefs)
    - Recouvrement des clefs
    - Sauvegardes
    - ...
- Peu de solutions sont (finalement) disponibles
  - Problématique complexe
  - Expérimentation CNRS/UREC en cours...

Client ultra-léger...

Les 25g de bonheur du nomade ;-)

(démonstration)

Conclusion

Tunnels SSL pour le nomadisme simple :

- Simple, efficace et économique
- Satisfaction élevée
- Clef magique : satisfaction très élevée

VPN SSL (pour les délocalisés/administrateurs)

- Efficace et performant (90% bandwidth)
- Presque transparent
- Excellente intégration au SI (LDAP/X509)

Problème des firewalls & co...

- Faudra t-il systématiquement prévoir de les contourner ?
- Anonymisation de l'Internet : incontournable ?

(Quelques) références :

[1] OpenSSL
http://www.openssl.org/

[2] Stunnel
http://www.stunnel.org/

[3] OpenVPN
http://www.openvpn.net

[4] Sécurisation d'OpenVPN
http://www.urec.cnrs.fr/IMG/pdf/articles.05.OpenVPN.pdf

[5] Devil-Linux
http://www.devil-linux.org

[6] Applications portables
http://portableapps.com/

[7] Projet Tor
http://tor.eff.org/

[8] Shorewall
http://www.shorewall.net/