



Nomadisme : problématiques et solutions

Eric JULLIEN

Patrick PETIT

David ROUMANET



Plan

- **La solution nomade actuelle**
- **Tests de solutions complémentaires**
- **La future solution nomade**
- **Conclusion**



Plan

- ➔ - **La solution nomade actuelle**
- Tests de solutions complémentaires
- La future solution nomade
- Conclusion

Le contexte académique sur Grenoble

La solution actuelle

Les solutions testées

La future solution

Conclusion

- **5 universités:**
 - **Université Joseph Fourier**
 - **Université Pierre Mendès France**
 - **Université Stendhal**
 - **Institut National Polytechnique de Grenoble**
 - **Université de Savoie**
- **Une population diversifiée (plus de 60000 étudiants, personnels, enseignants, ...) aux besoins hétérogènes**
- **Plusieurs campus communs, des sites distants**
- **Des bâtiments partagés**
- ⇒ **Situation complexe**
- ⇒ **Nombreux acteurs avec des rythmes, des budgets, des compétences propres**

Solution nomade Unique mutualisée sur tous les campus

Solution retenue : VPN-IPSec

La solution actuelle

Les solutions testées

La future solution

Conclusion

- ❑ **Des bornes sans fils qui présentent un SSID ouvert avec des adresses de classes privées (10.X.X.X)**
- ❑ **Accès restreints vers les concentrateurs VPN et le site Web de diffusion du logiciel client VPN-IPSec**
- ❑ **Chaque établissement**
 - ❑ **déploie son architecture VPN**
 - ❑ **réalise l'identification/authentification de ses utilisateurs**

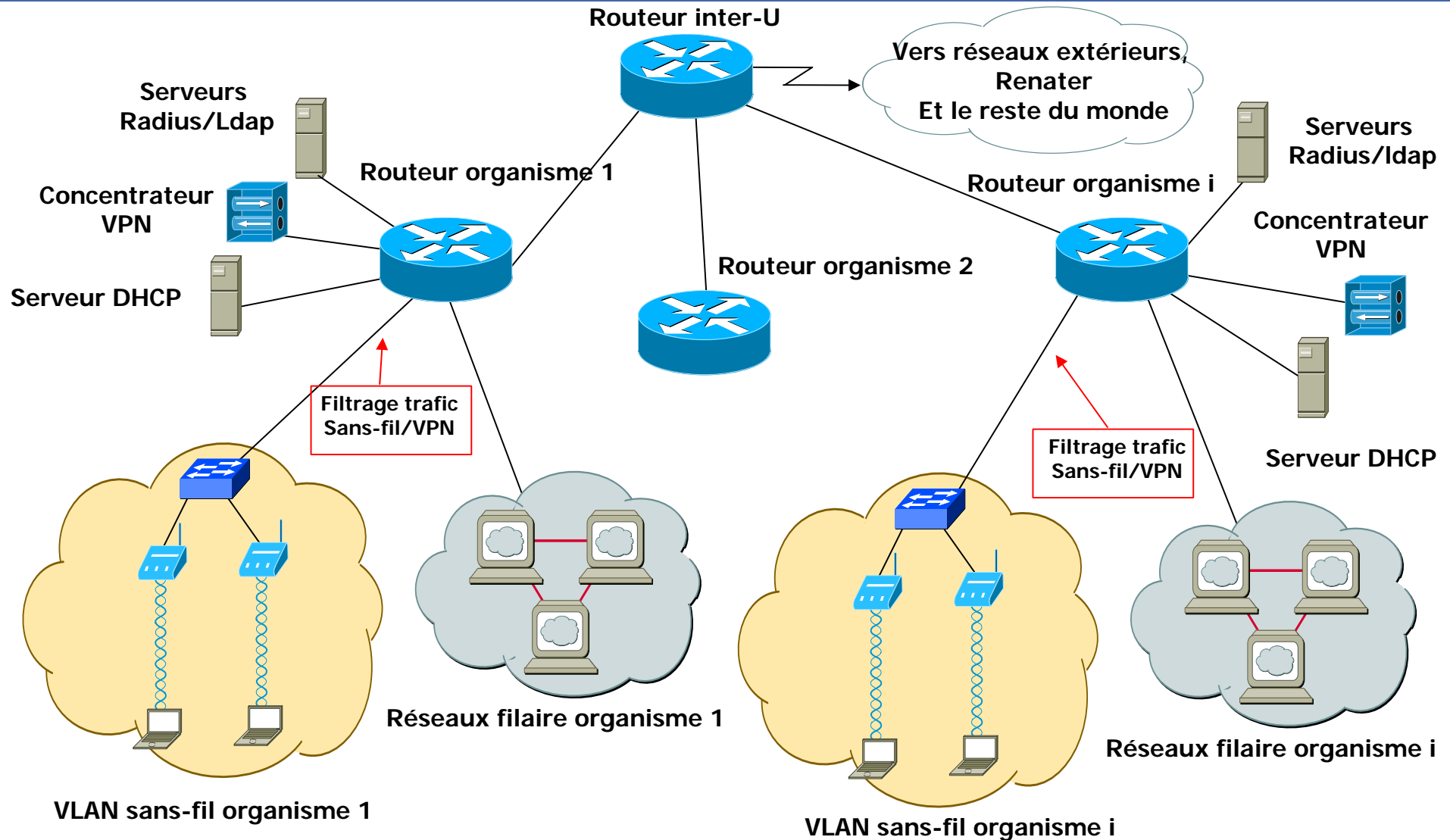
Principe d'architecture solution VPN

La solution actuelle

Les solutions testées

La future solution

Conclusion



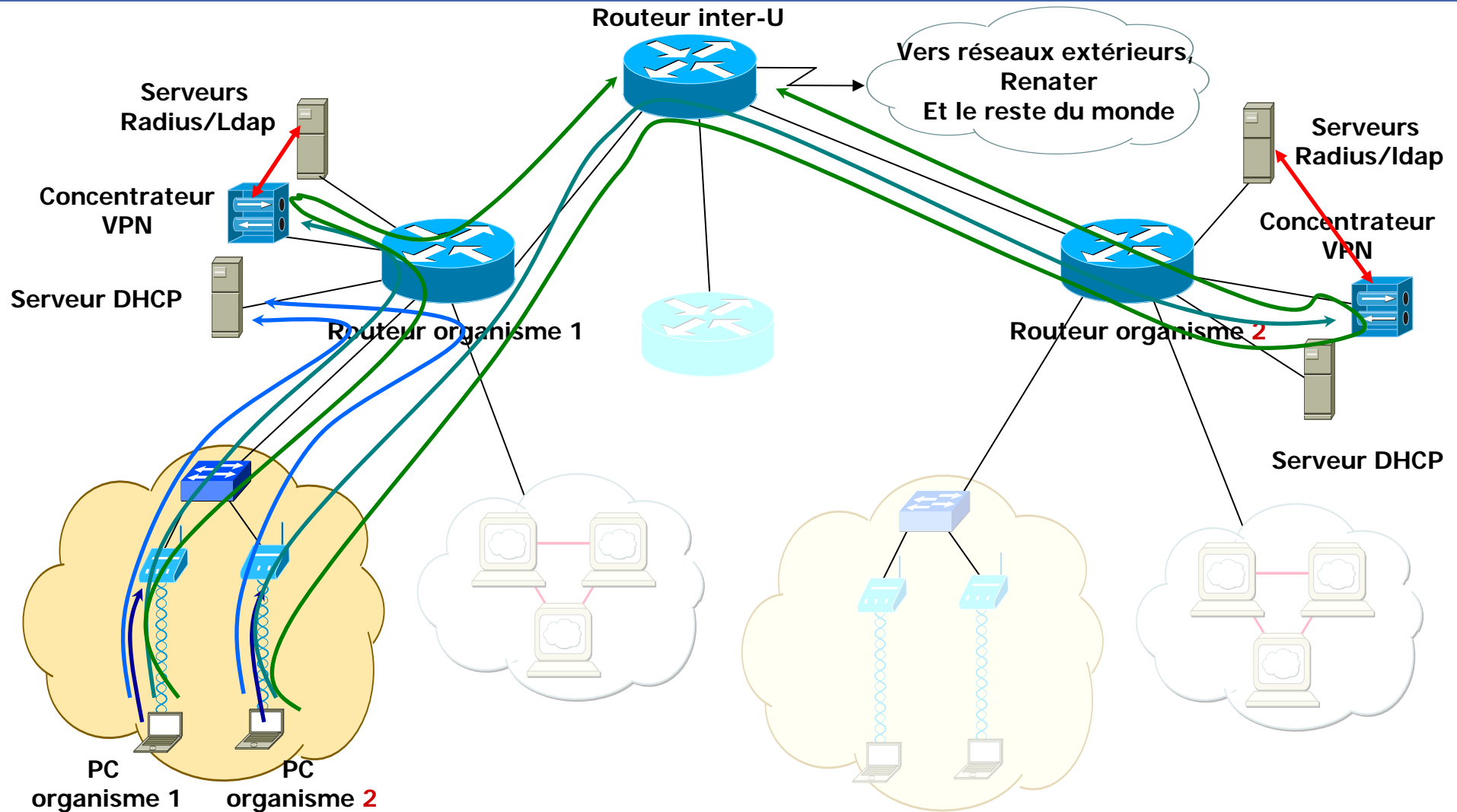
Scénario de connexion VPN-IPSec

La solution actuelle

Les solutions testées

La future solution

Conclusion



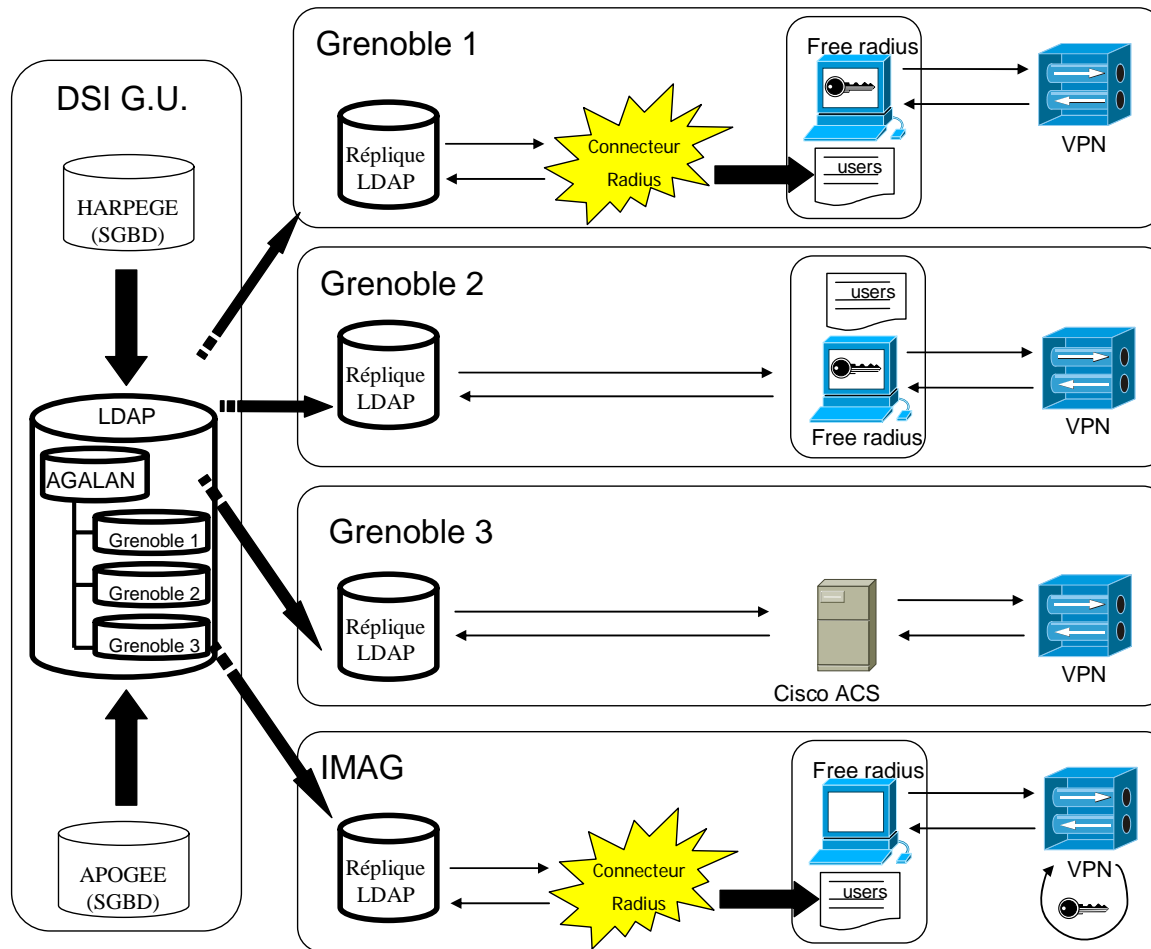
Principe d'authentification

La solution actuelle

Les solutions testées

La future solution

Conclusion



Avantages de la solution

La solution actuelle

Les solutions testées

La future solution

Conclusion

● Homogénéité

- Solution unique sur tous les campus

● Confidentialité des échanges

- Chiffrement robuste inclus

● Respect des chartes

- Gestion des traces

● Solution utilisable « en nomade »

- Les connexions utilisables sont nombreuses (maison, étranger, ...).

● Gestion des accès par type de population

Contraintes de la solution

La solution actuelle

Les solutions testées

La future solution

Conclusion

- ④ **Solution centralisée**
- ④ **Le chiffrement grève les performances**
- ④ **Téléchargement et configuration d'un logiciel client**
 - ④ **Nécessité d'avoir un serveur Web commun**
- ④ **Gestion des visiteurs**
 - ④ **Certains scénarios sont difficiles à gérer (congrès, invitations, visites).**

Retours d'expérience : solution de + en + utilisée

La solution actuelle

Les solutions testées

La future solution

Conclusion

MAIS...

- ❁ **Problématique de téléchargement et d'installation du client VPN-IPsec**
- ❁ **Les usagers ne sont pas toujours dans les annuaires**
- ❁ **Apparition de problèmes liés à l'utilisation du sans fils (vol de portable, password,...).**
- ❁ **Apparition de l'utilisation de portables personnels et ennuies qui vont avec :**
 - ❁ **Postes non à jour (patches, spywares, virus)**
 - ❁ **Problème de responsabilité des CRI**
 - ❁ **=> expérimentation en cours : cellule d'assistance basée sur des étudiants formés par les CRIs.**



Plan

- La solution nomade actuelle
- ➔ - **Tests de solutions complémentaires**
- La future solution nomade
- Conclusion

Tests de solutions complémentaires

La solution actuelle

Les solutions testées

La future solution

Conclusion

« cahier des charges précis » : « 90 % des besoins des nomades sont de type web pur »

- **Plusieurs types de solutions ont été étudiés dans ce cadre :**
 - Simple en manipulation
 - Accès web pur
 - Trace des utilisateurs
 - Taxonomie propriétaire des solutions testées :
 - L'approche Proxy avec Auto détection (sans client)
 - L'approche Proxy Transparent (sans client)
 - L'approche VPN-SSL (client léger)
 - L'approche « portail captif » (sans client)
- **En parallèle de ces tests, étude d'une architecture basée sur la norme 802.11i**

Auto détection de Proxy

La solution actuelle

Les solutions testées

La future solution

Conclusion

● La solution

- L'implémentation de l'auto détection de proxy en DHCP n'a été validée que sous Windows avec IE
- L'implémentation de l'auto détection de proxy par DNS a été vérifiée
 - sous Windows avec IE et Firefox,
 - sous linux avec Firefox,
 - sous Mac avec Firefox. (Sous Mac OS X 10.3 Safari et IE n'implémentent pas cette méthode).

● Avantages

- on peut facilement prendre en compte d'autres protocoles que le http et le https, la gestion des authentifications est prise en compte, trace des utilisateurs complète
- Possibilité de gérer des « crédits temps » avec SurfPass pour Squid (à valider)
- Le navigateur s'exploite naturellement

● Inconvénients

- L'auto détection n'est pas vraiment transparente pour les utilisateurs (il faut avoir coché la case si elle existe!!!)
- Elle n'est pas prise en compte par tous les systèmes et tous les navigateurs
- Pas de sécurisation des données

Proxy transparent

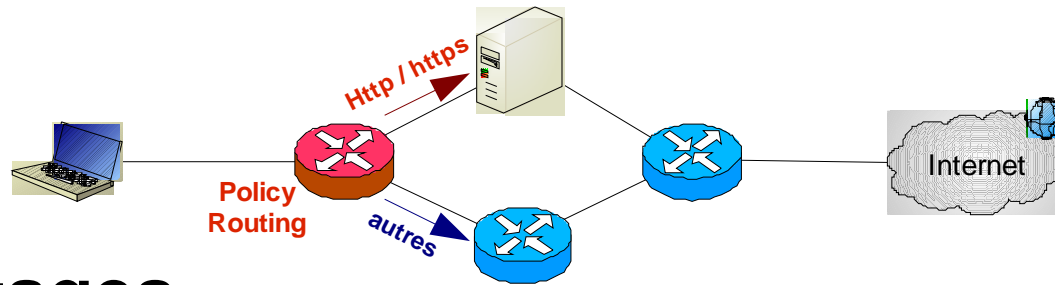
La solution actuelle

Les solutions testées

La future solution

Conclusion

❶ Pré-requis : policy routing



❷ Avantages

- ❶ L'usage du navigateur reste inchangé (on peut exploiter ses favoris)

❸ Inconvénients

- ❶ Pas de sécurisation des données
- ❶ Moins modulable qu'un proxy normal

Proxy Transparent

La solution actuelle

Les solutions testées

La future solution

Conclusion

Solution testée	Avantages	Inconvénients
Squid v2.5 en mode transparent	<ul style="list-style-type: none">• Solution libre	<ul style="list-style-type: none">• Pas d'authentification à l'heure actuelle donc pas de trace des utilisateurs
WinGate	<ul style="list-style-type: none">• Solution peu onéreuse• Trace utilisateurs complète	<ul style="list-style-type: none">• Le client doit accepter les « pop-up »,• Interpréteur java indispensable,• Problèmes de fonctionnement avec certains sites (bureau virtuel Rhône-Alpes)• Authentification en Active directory uniquement
BlueCoat	<ul style="list-style-type: none">• Authentification ldap, radius,...• Trace des utilisateurs complète,• Respect des sessions https,• Gestion des sessions http par cookie	<ul style="list-style-type: none">• Https géré via une période de temps et avec adresse IP• Ftp en mode transparent OK mais obligation de forcer le client en mode passif si non automatique

VPN-SSL (client léger)

La solution actuelle

Les solutions testées

La future solution

Conclusion

❶ Avantages

- ❷ Sécurisation des données

❸ Inconvénients

- ❹ Le champ d'url du navigateur n'est plus exploitable,
- ❺ Les favoris du navigateur ne le sont plus non plus,
- ❻ Il faut disposer d'un interpréteur Java ou autre (activeX)

VPN-SSL (client léger)

La solution actuelle

Les solutions testées

La future solution

Conclusion

Solution testée	Avantages	Inconvénients
Cisco VPN 30xx	<ul style="list-style-type: none">• Solution incluse sur les boîtiers VPN en standard• Authentification identique à la solution VPN• Fonctionne avec tous les sites web	<ul style="list-style-type: none">• Interface• Gourmant en ressources (facteur 3 par rapport à du VPN IPSec en théorie, facteur 10 en pratique)• Traces utilisateurs insuffisantes dans notre contexte
Array Network SPX 3000	<ul style="list-style-type: none">• performances• Traces utilisateurs complètes	<ul style="list-style-type: none">• La version testée ne fonctionne pas avec certains sites (hotmail.com par exemple)

« portails captifs »

La solution actuelle

Les solutions testées

La future solution

Conclusion

- ❶ **La solution Monowall (pf-sense)**
 - ❶ Portail de « niveau 2 »
 - ❶ Se substitue à la passerelle par défaut
- ❷ **Avantages**
 - ❶ Peut proposer plus que du http et https
- ❸ **Inconvénients**
 - ❶ Se comporte comme un NAT/PAT : pas de sécurisation des données (usurpation d'adresse MAC possible)
 - ❶ Difficultés de déploiement dans notre environnement (1 portail par Vlan de bornes) lié a son fonctionnement : filtrage par adresses MACs

« portails captifs »

La solution actuelle

Les solutions testées

La future solution

Conclusion

- ❶ **La solution Talweg**
 - ❶ Portail de niveau « applicatif »
 - ❶ Pré-requis : avoir déployé du Policy-routing
- ❶ **Avantages**
 - ❶ Logiciel libre développé par le Crium (Université de Metz)
 - ❶ Gestion des logs complète
 - ❶ Facilité de déploiement dans notre contexte
 - ❶ Authentification et transport sécurisé des données sur le sans fil
 - ❶ Le mode de fonctionnement permet d'utiliser son navigateur naturellement, cependant la redirection ne permet pas de sauvegarder des URLs proprement dans ses favoris
- ❶ **Inconvénients**
 - ❶ La réécriture d'adresse a un coût

Autres solutions sans client et client léger

La solution actuelle


Les solutions testées

La future solution


Conclusion

Il en existe bien d'autres !

Certaines éliminées d'office (ne correspondant pas à notre contexte)

-  Chilispot, nocatauth, Aventail, Symantec 4400, Ucopia, Bluesocket, AEP networks Netilla, Permeo Technologies (ActiveX), SSL Explorer, OpenVPN, NuFW ...

Certaines n'ont pas été testées par manque de ressources

-  Juniper Netscreen, Menlo logic, Net Swift, iGate Safenet SSL-VPN, eGAP SSL-VPN, Arkoon, CyberGuard, ovisGate SSL, CheckPoint, F5 Networks Firepass 1000...

Tests solution 802.11i

La solution actuelle

Les solutions testées

La future solution

Conclusion

- ❶ **802.11 : la révolution sans fil MAIS...**
 - => Erreur de conception : WEP**
 - ❶ ... une mauvaise implémentation de RC4 menace le déploiement du standard 802.11

- ❷ **Les solutions : WPA**
 - ❶ WPA : 802.1x + TKIP
 - ❶ WPA2 : 802.1X + CCMP

802.1x est un « vieux » standard (PPP)

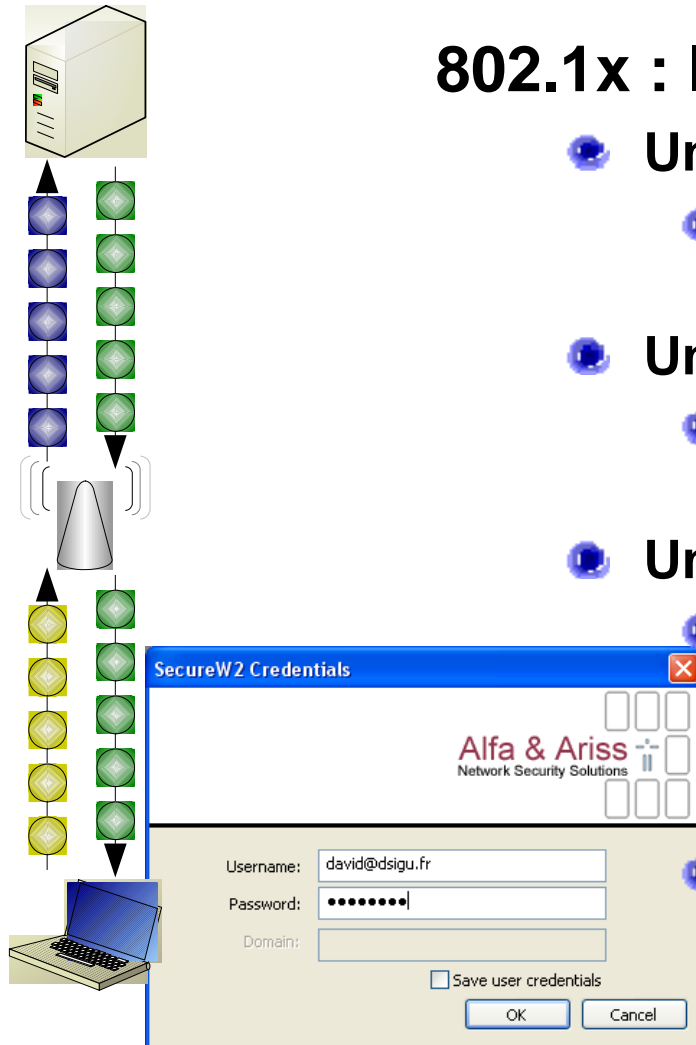
Tests solution 802.11i

La solution actuelle

Les solutions testées

La future solution

Conclusion



802.1x : la sécurité en 3 points

- **Un serveur d'authentification (AAA)**
 - Nous avons conservé FreeRADIUS : complet, gratuit, open-source, RADIUS
- **Un point d'accès (AP)**
 - Nous avons utilisé Cisco AP1100 : compatible WPA & WPA2 (même SSID)
- **Un suppliciant**
 - Nous avons choisis SecureW2 pour Windows : simple à mettre en œuvre, gratuit et open-source (support GINA en cours de développement)
 - WPASuppliciant pour les postes linux.

Tests solution 802.11i

La solution actuelle

Les solutions testées

La future solution

Conclusion

- ❶ **EAP : quel mécanisme choisir ?**
 - ❶ MD5 ? LEAP ? Pas assez robuste...
 - ❶ PEAP ? Pas sous Linux
 - ❶ TLS ? Nécessite une autorité de certification
 - ❶ TTLS ? **Un bon compromis dans notre contexte !**
- ❷ **AAA : Authentication, Autorization and Accounting**
 - ❶ Respect de la charte Renater → Accounting obligatoire

Tests 802.11i : l'accounting

La solution actuelle

Les solutions testées

La future solution

Conclusion



Deux démons :

- sql_dhcp surveille les syslog DHCP
- sql_ap surveille par SNMP les associations avec l'AP

➔ La corrélation @IP dynamique / identifiant RADIUS est faite

Tests 802.11i : résultats d'accounting sous forme SGBD

La solution actuelle

Les solutions testées

La future solution

Conclusion

Authentifiant + domaine

@MAC AP (géolocalisation)

Adresse IP supplicant

Estampillage horaire

User-Name	Calling-Station-Id	Client-IP-Address	Called-Station-Id	NAS-Port	Timestamp Start	Timestamp D
anonymous	000d.54a1.6e8e	130.190.195.126	000e.8440.bbb1	4741	2005-06-16 15:41:01	2005-06-16
anonymous	000d.54a1.6e8e	130.190.195.126	000e.8440.bbb1	4742	2005-06-16 16:22:41	2005-06-16
anonymous	000d.54a1.6e8e	130.190.195.126	000e.8440.bbb1	4743	2005-06-16 16:26:32	2005-06-16
david	000d.54a1.6e8e	130.190.195.126	000e.8440.bbb1	4756	2005-06-21 16:14:49	2005-06-21
david@dsgu.fr	000d.54a1.6e8e	130.190.195.126	000e.8440.bbb1	4757	2005-06-21 16:52:42	2005-06-21
david@dsgu.fr	000d.54a1.6e8e		000e.8440.bbb1	4758	2005-06-21 18:34:37	0000-00-00
david@dsgu.fr	000d.54a1.6e8e		000e.8440.bbb1	4759	2005-06-21 18:34:38	0000-00-00
david@dsgu.fr	000d.54a1.6e8e	130.190.195.126	000e.8440.bbb1	4760	2005-06-21 18:34:39	2005-06-21
david@dsgu.fr	000d.54a1.6e8e	130.190.195.250	000e.8440.bbb1	4761	2005-06-23 14:40:42	2005-06-23
david@dsgu.fr	000d.54aa.a39c	130.190.195.127	000e.8440.bbb2	4807	2005-06-23 17:30:31	2005-06-23
david	000d.54aa.a39c		000e.8440.bbb2	4825	2005-06-27 15:58:03	0000-00-00
roumanet@grenet.fr	000d.54aa.a39c		000e.8440.bbb2	4840	2005-06-29 12:08:52	0000-00-00
roumanet@grenet.fr	000d.54aa.a39c	130.190.195.127	000e.8440.bbb2	4842	2005-06-29 12:13:05	2005-06-29
*				0	0000-00-00 00:00:00	0000-00-00

Tests 802.11i : Radius

La solution actuelle

Les solutions testées

La future solution

Conclusion

La fonction de « Proxyfication » :

- Les serveurs RADIUS peuvent échanger des informations
- Le mécanisme d'authentification employé n'est pas dépendant du serveur RADIUS le plus proche de l'AP
- Il est possible d'envisager une authentification décentralisée → ARREDU et portail captif !

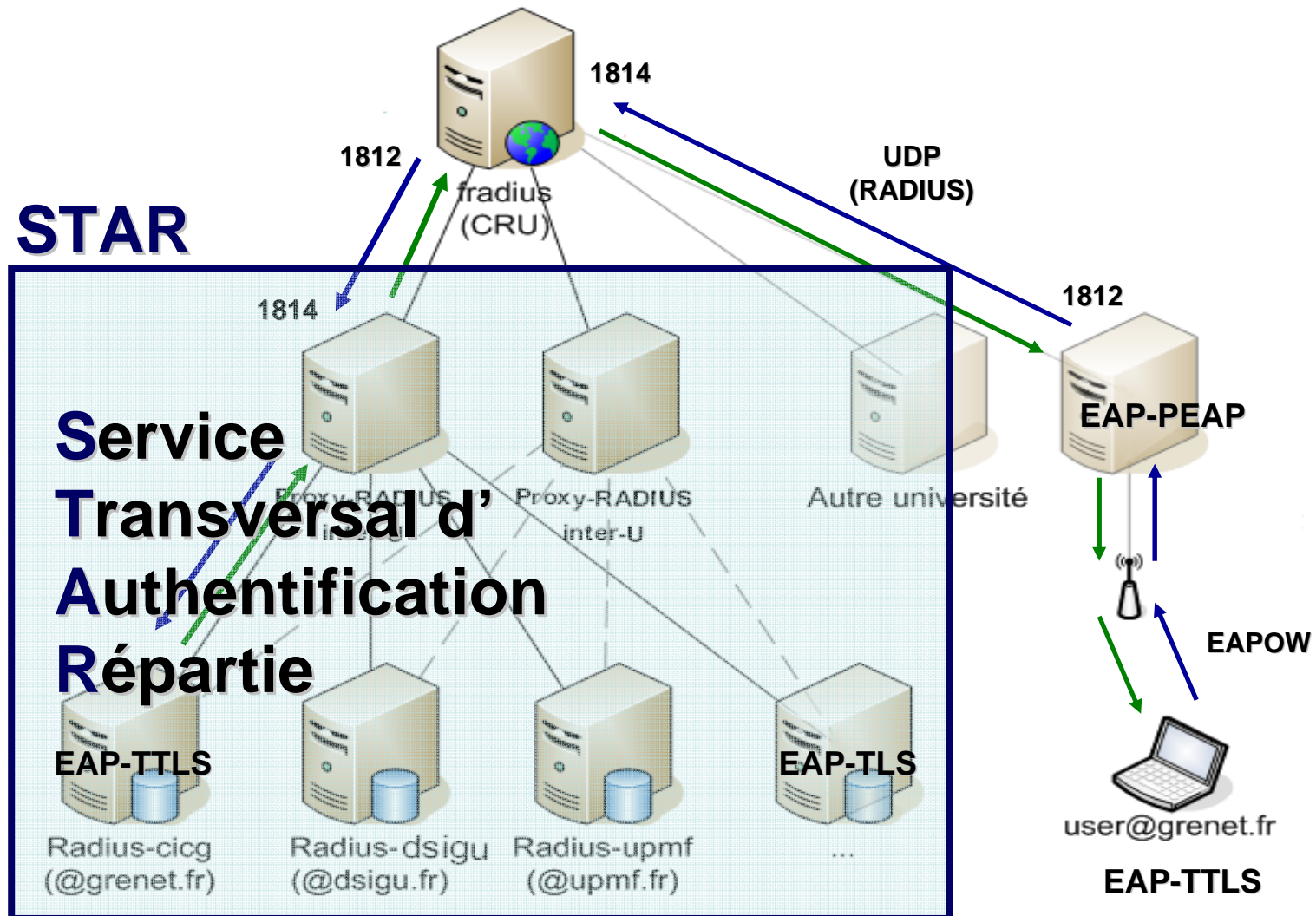
Tests 802.11i : Proxy radius, Architecture et cinématique

La solution actuelle

Les solutions testées

La future solution

Conclusion





Plan

- La solution nomade actuelle
- Etude de solutions complémentaires
- ➔ - **La future solution nomade**
- Conclusion

La nouvelle solution nomade

La solution actuelle

Les solutions testées

La future solution

Conclusion

A partir de toutes ces briques, nouvelle architecture proposée :

- On conserve le VPN pour tout accès nomade de nos utilisateurs
- Pour les accès sans-fil :
 - Adjonction d'une solution de simple accès web à la solution VPN de base pour « nos » utilisateurs
 - Création en parallèle d'une possibilité de se connecter en sans-fil dans le cadre du scénario ARREDU / EDUROAM

Aspects techniques pour le sans-fil

La solution actuelle

Les solutions testées

La future solution

Conclusion

- **Conservation du SSID ouvert**
 - pour accueillir informer les usagers des services sans-fil offerts
 - offrir un accès web simplifié,
 - Disposer d'un accès polyvalent sécurisé au moyen des tunnels VPN-IPSec

- **Création d'un nouveau SSID pour le scénario ARREDU/eduroam**
 - Solution valide pour tout scénario EAP TLS/TTLS/802.11i
- **Ajout d'un SSID pour la téléphonie sur IP**

Authentification et gestion des logs

La solution actuelle

Les solutions testées

La future solution

Conclusion

- ❶ **Nécessité des proxy radius**
 - ❶ **Pour l'accès au « web simplifié » par nos utilisateurs**
 - ❶ **Utilisable également à terme par les boîtiers VPN (sûreté de fonctionnement)**
 - ❶ **Pour le scénario ARREDU/EDUROAM**
 - ❶ **Utilisable par tout nomade dépendant d'un établissement ayant adhéré au projet**
- ❷ **Pour la gestion des logs**
 - ❶ **Déjà en fonction pour les accès VPN**
 - ❶ **Disponible sur le portail captif**
 - ❶ **Introduction des scripts de géo localisation pour la solution ARREDU/EDUROAM**

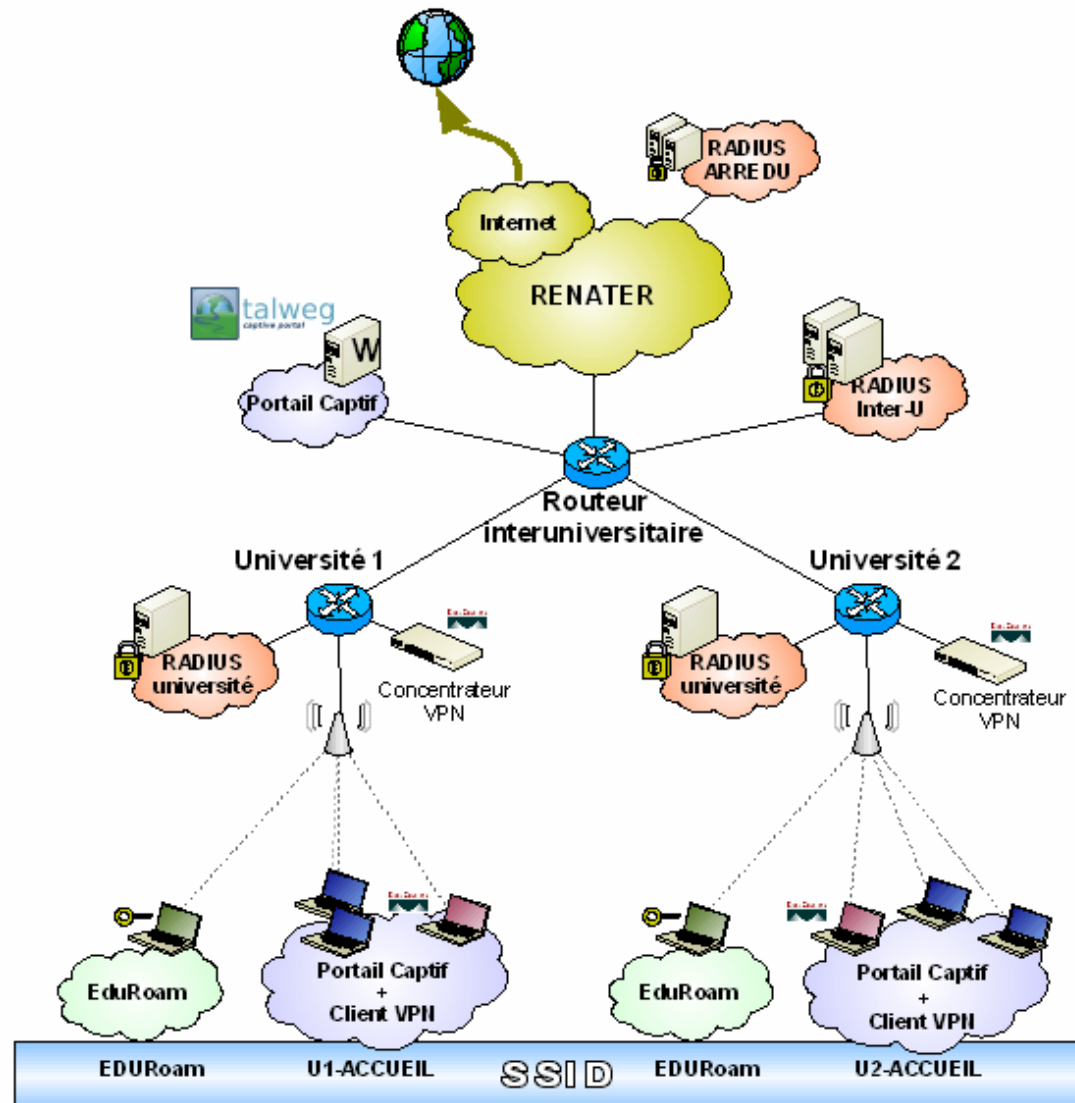
Synthèse de l'architecture

La solution actuelle

Les solutions testées

La future solution

Conclusion





Plan

- La solution nomade actuelle
- Etude de solutions complémentaires
- La future solution nomade
- ➔ - **Conclusion**

Nomadisme : problématiques et solutions

La solution actuelle

Les solutions testées

La future solution

Conclusion

- ④ **Les scénarios couverts sont de + en + vastes**
- ④ **Il faut travailler sur la salubrité des postes**
- ④ **A moyen terme : Attente...**
 - ④ **D'un Client 802.11i inclus dans les systèmes d'exploitation**
 - ④ **De la mobilité IPv6 pour s'affranchir de la solution de type VPN.**
(pilote en cours et en fonction pour certains scénarios à la DSI Grenoble Universités)