WLAN Security Switch 2250
version 1.0

Présentation technique

Arnaud LOIR
Ingénieur Avant-Vente
arnaud.loir@nortelnetworks.com

NORTEL NETWORKS

NORTEL NETWORKS CONFIDENTIAL

Agenda

- Principes de base
- Méthodes d'Accès
- Roaming
- Portail Web du WSS
- Authentification
- Détection des AP non-autorisées
- Premières évolutions prévues

Nortel Networks Wireless LAN Solution

WLAN-Security Switch 2250

- Centralise la sécurité et l'administration des Access Point

WLAN-Access Point 2220

- Dual-mode 802.11a&b
- Maintient un premier niveau de sécurité dans le réseau

Mobile VoIP Clients

- Clients Voix sur IP

WLAN 2200 Family

WLAN-Mobile Adapter 2201

- 802.11 a&b CardBus

WLAN – Security Switch 2250

Load Balancing

Distribution du Trafic

Bandwidth Management

Adaptive
Secures

Manages
Scales

Mobile Adaptive Tunneling

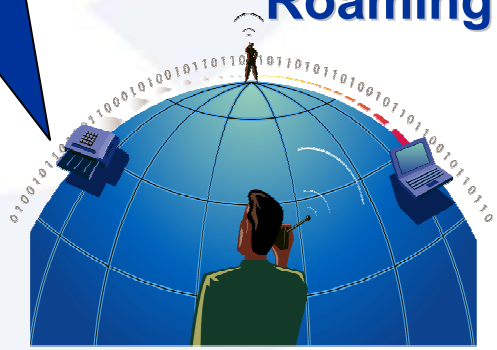
Portail d'accès :

- **Droits d'accès avec niveaux de priorité**
- **Info personnalisée**

Détection des AP non-autorisées

Détection et isolation des Rogue & Free AP

Roaming



Véritable roaming à travers toute l'Entreprise (y compris inter-subnet IP)

Une Platforme Wireless sécurisée

Niveaux de Sécurité

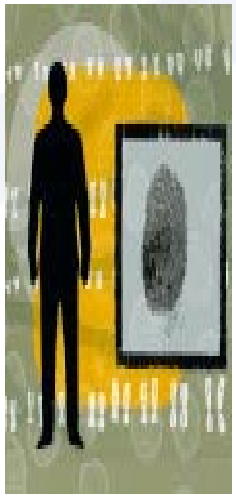
Premier niveau

WPA (TKIP)
Authentification
EAP/TLS & RADIUS
Access List (MAC)

WLAN Access Point

Avancé

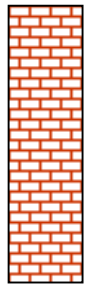
Encryption SSL,
Détection Rogue et free
Agent AP, Clientless …

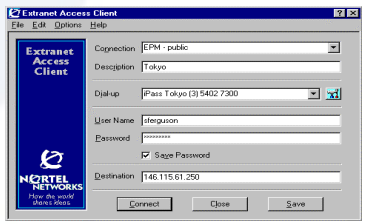


WLAN Security Switch

Spécialisé

IPSEC VPN, Firewall,…





Contivity client

Approche Multi-couche pour sécuriser les WLANs

WSS 2250

- **Auteur 1U**
- **6 ports**
  - 2 10/100/1000 Cuivre
  - 4 10/100 Cuivre
- **Gère jusqu'à 30 APs et 500 clients**
- **Module d'encryption Hardware**
  - Plus de 1000 tps SSL
  - 500 IPSEC tunnels (futur)
  - Plus de 200 Mbits/sec en 3DES (futur)

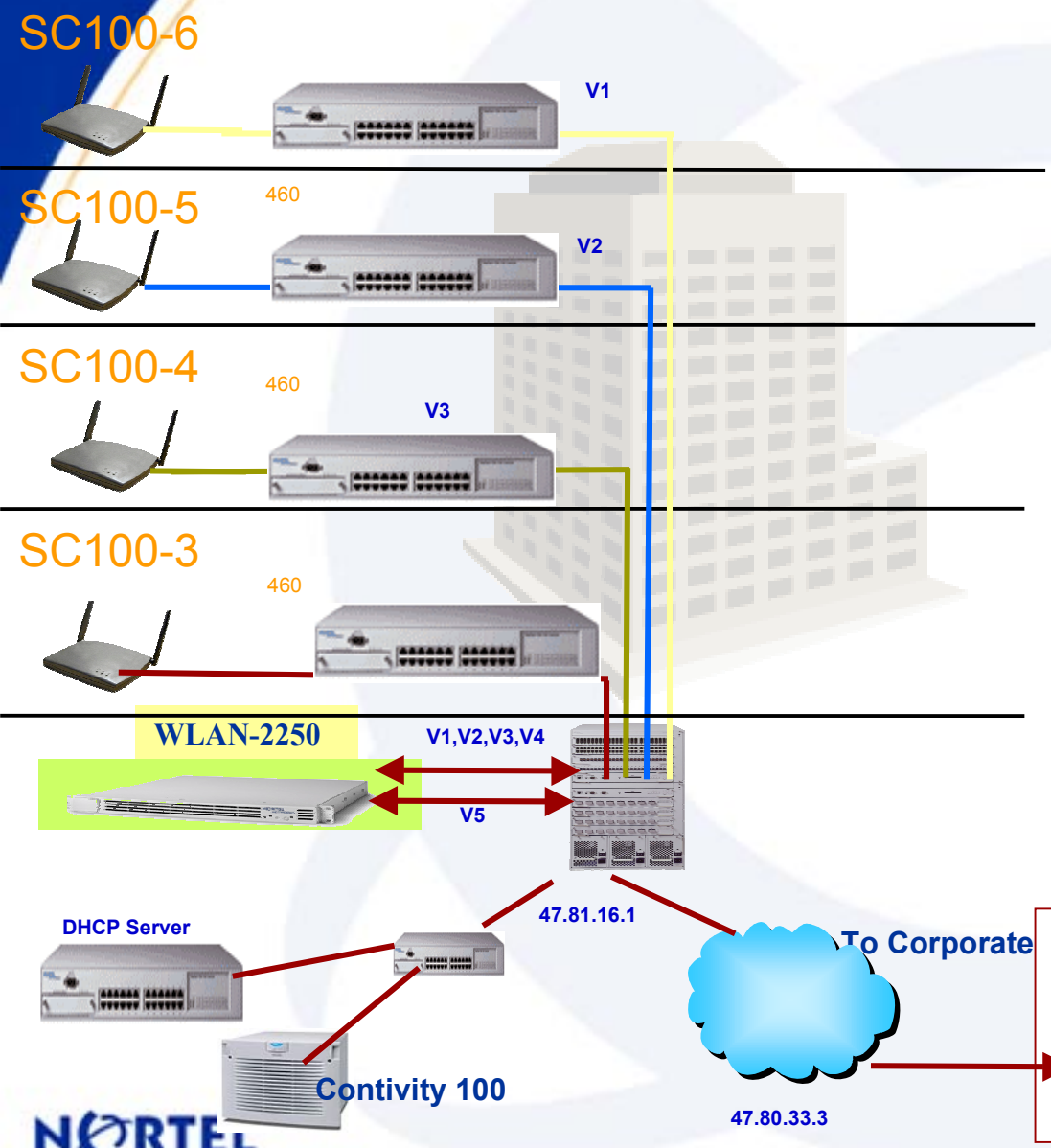
Interfaces du WSS

- **Routeur entre le monde WLAN et le monde Trusted Intranet**
- **Chaque commutateur WSS a au moins 3 interfaces**
  - Au moins une connectée au WLAN → **WIP**
  - Une connectée à l'Intranet → **IIP**
  - Une connectée à lui-même → **VIP**
- **NOTE : La VIP est dans un subnet séparé des autres interfaces!**
- **Un Cluster détient en plus une adresse de Management → MIP**

Interfaces WLAN

- **Un “port” fait référence à une interface physique**
- **Une “interface”est soit :**
  - Un port unique non-taggé
  - Un groupe de ports non-taggé (MLT ou actif-standby)
  - Un port unique avec tag de VLAN
  - Un groupe de ports avec tag de VLAN
- **Les interfaces sont bridgées entre elles au niveau 2, lorsqu’elles sont labellisées WLAN**
  - Les Unicasts sont forwardées en utilisant le Transparent Bridging
  - Les Broadcast sont filtrées, exceptées les ARPs Request, et les broadcast AP-AP.

WLAN intégrée dans l'architecture LAN

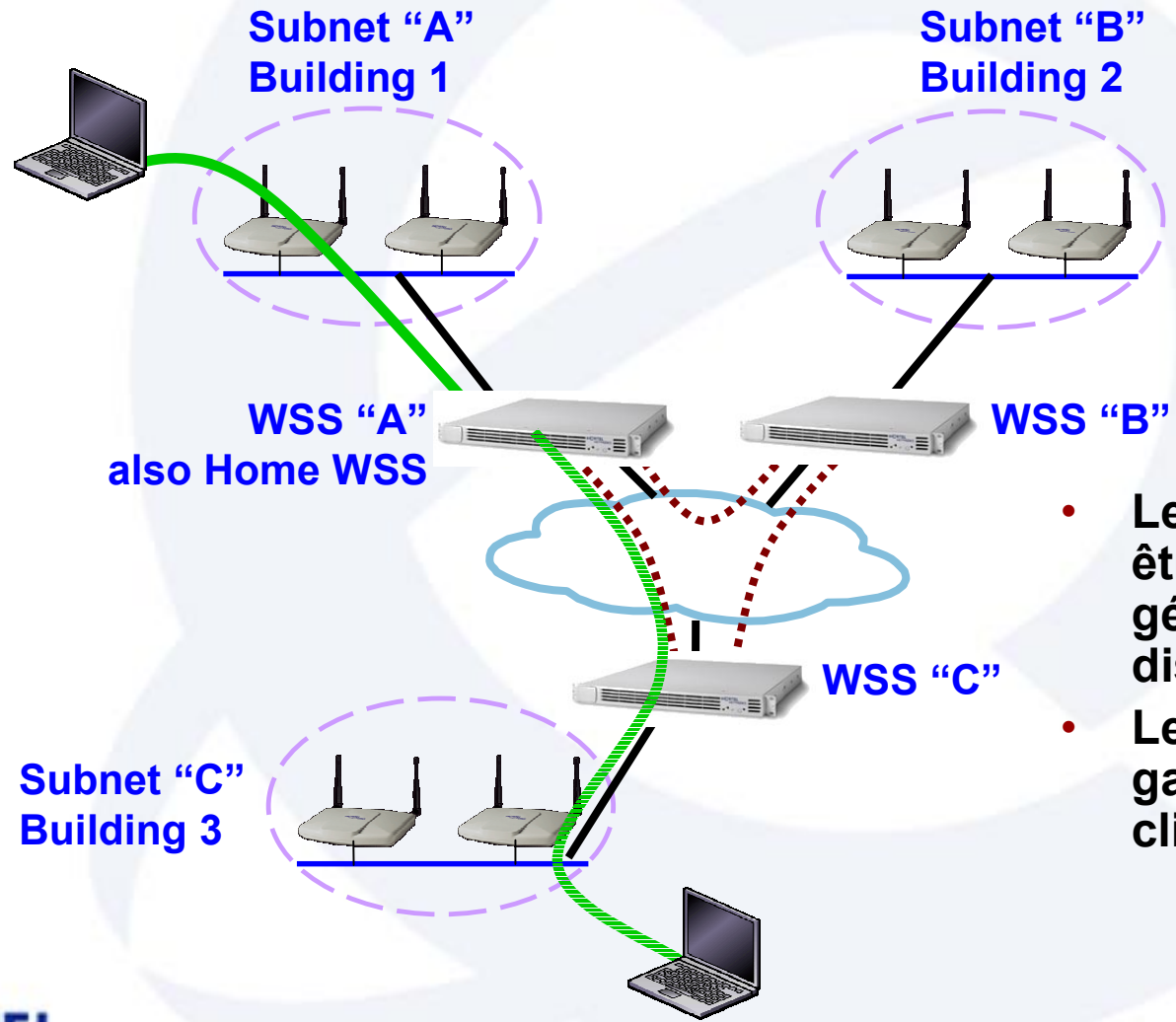


- Des VLANs sont dédiés pour les WLANs
- Le WSS gère le tagging 802.1q
- Des Routes statiques sont configurées sur le 8600 pour faire pointer le flux destiné à V1,V2,V3,V4 vers le WSS

Clusters de WSS

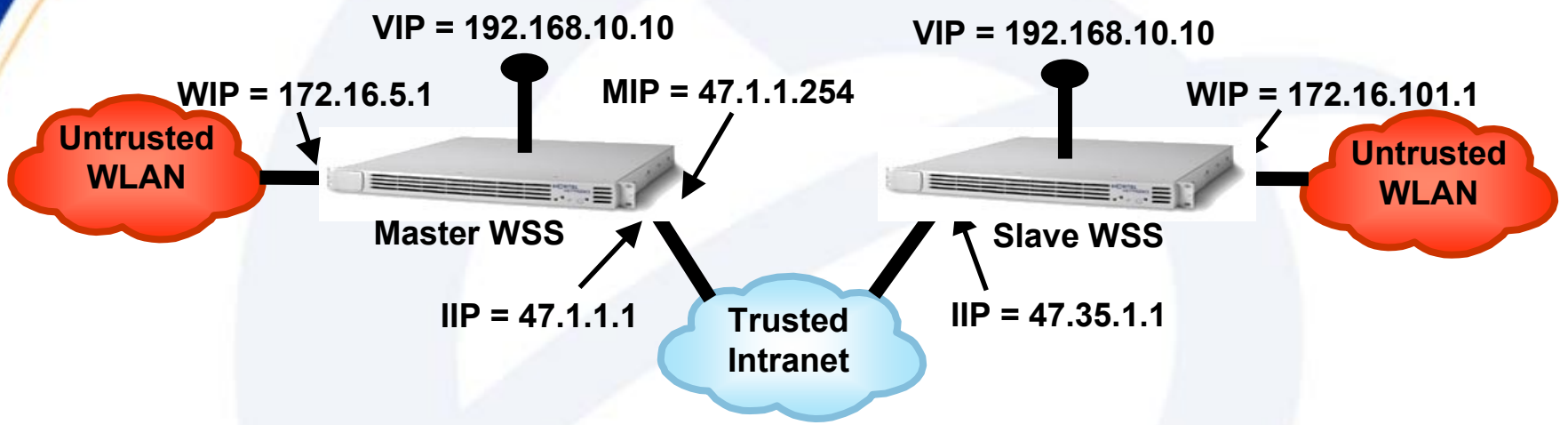
- **Un cluster de WSS est un domaine WLAN administratif**
- **Administration centralisée par une unique adresse IP MIP**
- **Roaming actif entre les WSS d'un même cluster**
  - Création automatique de Mobile Adaptive Tunnels (tunnel « Ethernet IP », ajoutant un en-tête IP/UDP) entre WSS
  - Topology Full Mesh des tunnels
- **16 WSS maximum par cluster**

Vue Conceptuelle



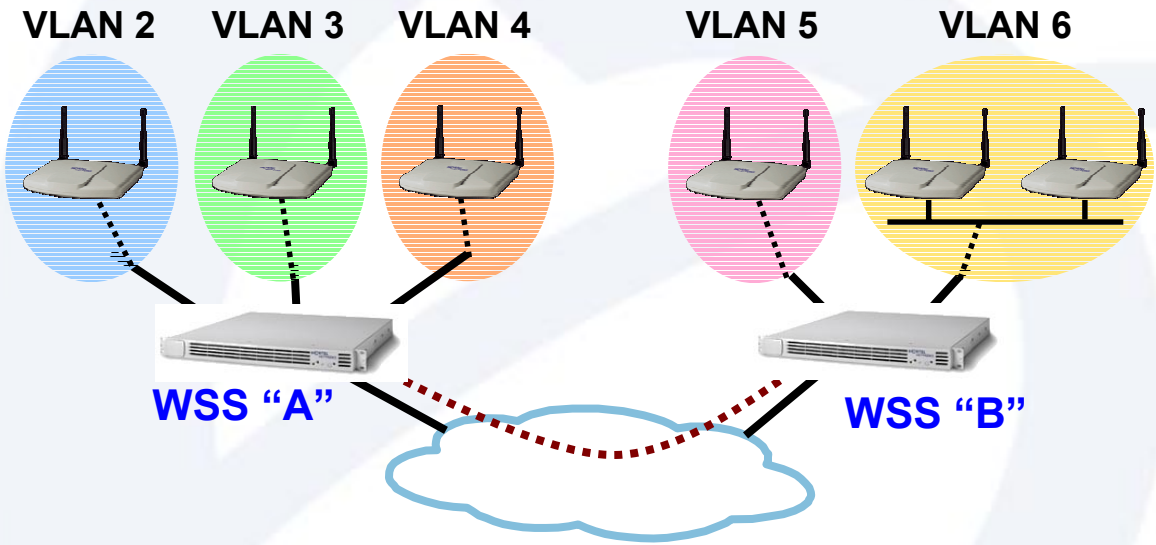
- Les WSS peuvent être géographiquement dispersées.
- Le WSS est la default gateway de ses clients WIFI

Interfaces WSS dans un Cluster



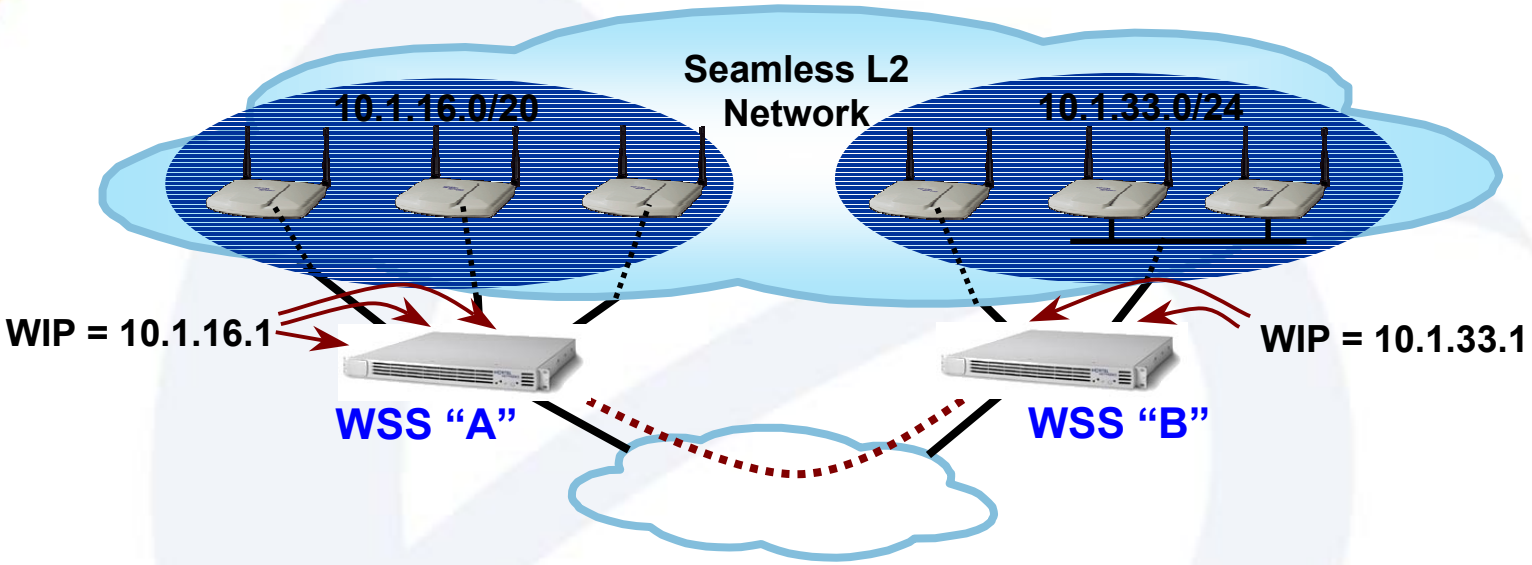
- **Le Master contrôle l'adresse IP de Management**
- **Les Slaves sont situés n'importe où dans l'Intranet**
  - Des tunnels sont bâtis au dessus de l'infrastructure routée
- **Les Slaves sont contrôlés par les Masters:**
  - Configuration (cluster + local), Management, Status changes, etc.
  - Sans Master, la config est bloquée, mais les données continuent d'être transmises
- **15 Slaves max par cluster**
- **Chaque WSS a la même VIP localement**

Comment le WSS voit-il les WLANs



- **Conseil de Design : Bâtir des petits domaines de broadcast WLAN**
  - Le Trafic Broadcast est envoyé au taux le plus bas supporté, afin de garantir la réception dans l'ensemble de la zone de couverture radio, soit :
    - 802.11b: 1 Mbps
    - 802.11a: 6 Mbps
  - Les flux Broadcast prennent donc plus de temps à être transmis que les flux Unicast en Wireless (jusqu'à 9 fois plus que les Unicast en 802.11a)
- **La configuration optimum consiste à allouer un VLAN par AP (dans la limite des contraintes d'exploitation)**
- **Ne pas mettre des clients « câblés » dans un VLAN Wireless**

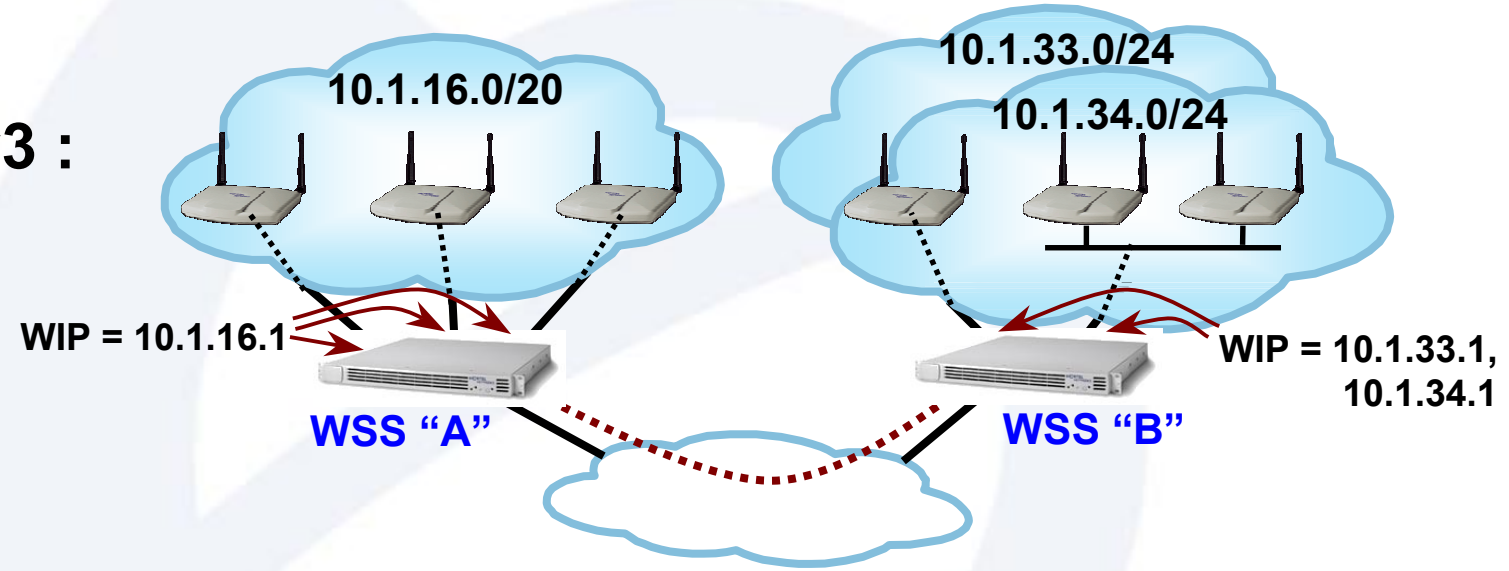
Comment le WSS voit-il les WLANs



- **Tous les WLANs sont fondamentalement traités comme un réseau géant de niveau 2**
  - …sans tenir compte du nombre de VLANs utilisés
  - Cependant un filtrage intelligent des broadcast permet de solutionner les problèmes inhérents aux grands réseaux de niv 2
  - Seuls les Unicast et les broadcast « ARP request » et les communications « AP-AP », peuvent traverser les VLANs
- **Ceci permet de ne plus tenir compte de la position physique du client**
- **Les Tunnels prennent part dans le mécanisme de bridging**
- **Pour simplifier l'architecture, nous conseillons d'utiliser un subnet IP par WSS**

Comment le WSS voit-il les WLANs

Au niv3 :



- **Design possible pour simplifier l'architecture : Utiliser un subnet par WSS (ex : WSS "A")**
- **WSS "B" représente un scénario d'évolution, où un autre subnet a été ajouté**
  - Les Subnets sont définis globalement et multinettés sur toutes les interfaces WLAN
  - Requiert la fonction Superscope sur le serveur DHCP
    - **Win2k alloue les adresses séquentiellement**
    - **Linux alloue les adresses en mode round-robin par (sub)-scope**

Comment l'utilisateur accède-t-il au WSS ...

Client

Associate Request

Access Point

WLAN Security Switch

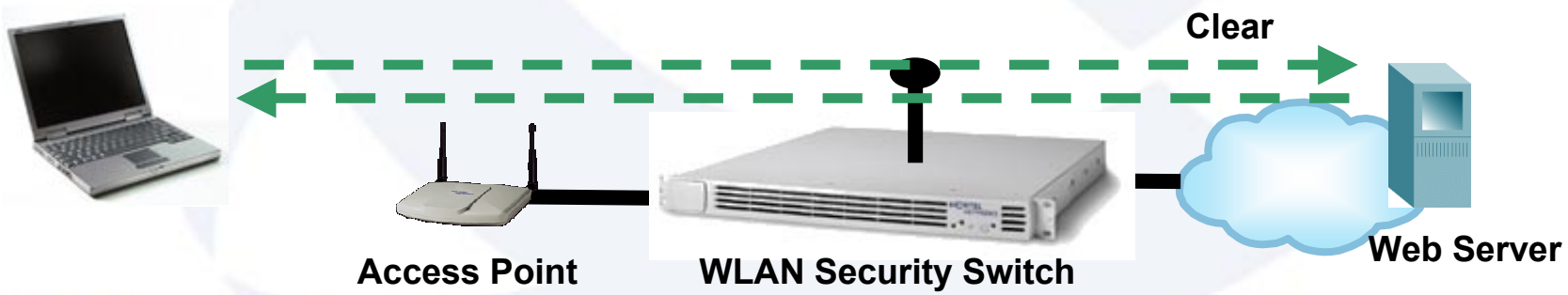
1 DHCP Request

DHCP Response

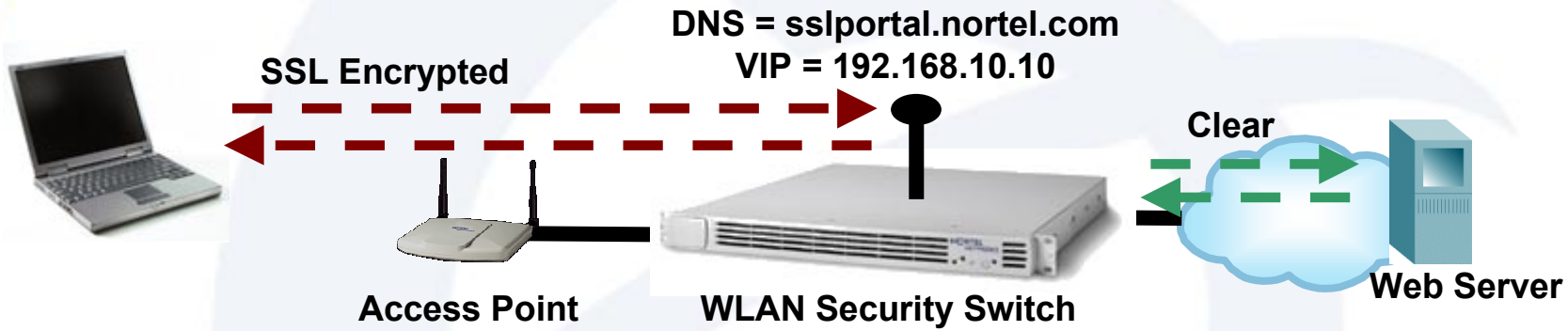
1	https://wireless.com **SSL Exchange**	SSL Exchange
2	**IPSEC Pass through**	Pass through
3	**PPTP**	One Time Password
4	**Clear**	Pass through

Méthode Clear Access

- Accès non chiffré, non sécurisé vers l'Intranet/Internet
- Si aucun chiffrement de Niv2 est utilisé (WEP, TKIP, AES), Le trafic n'est absolument pas protégé
- Le mode Clear access doit être contrôlé avec attention en cas d'accès à certaines ressources de l'intranet
- La configuration par défaut permet le clear access vers tout sauf les réseaux "Intranet"configurés dans le WSS (ex 10.0.0.0/8, 192.168.0.0/16,…).
- L'accès Internet est disponible

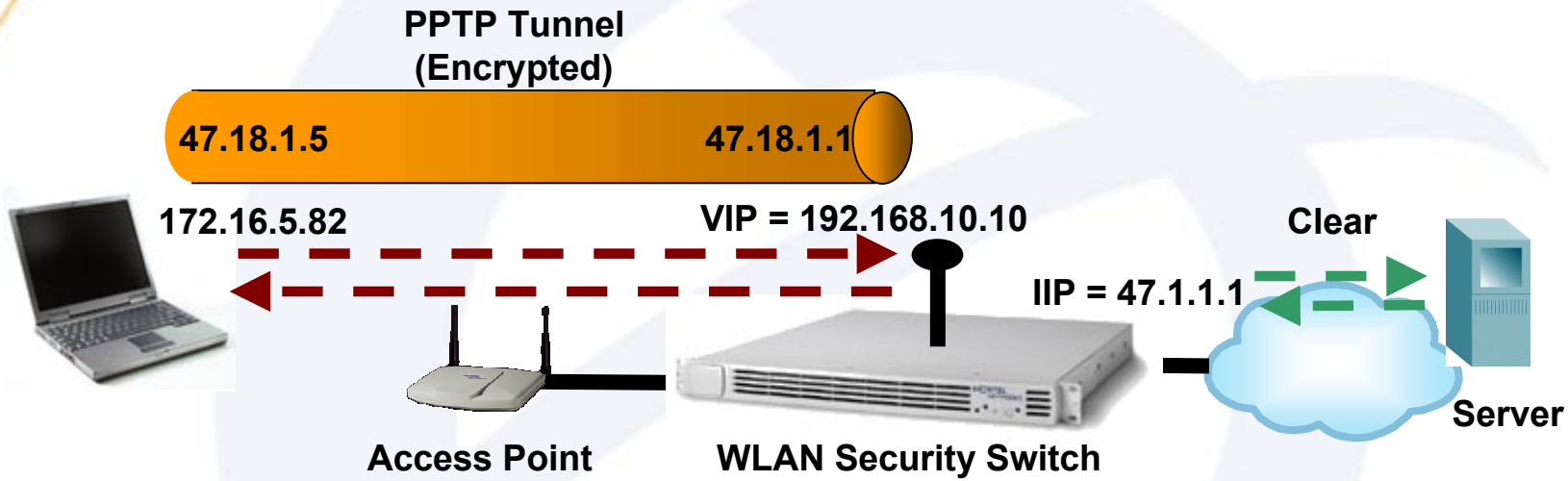


Méthode d'accès SSL



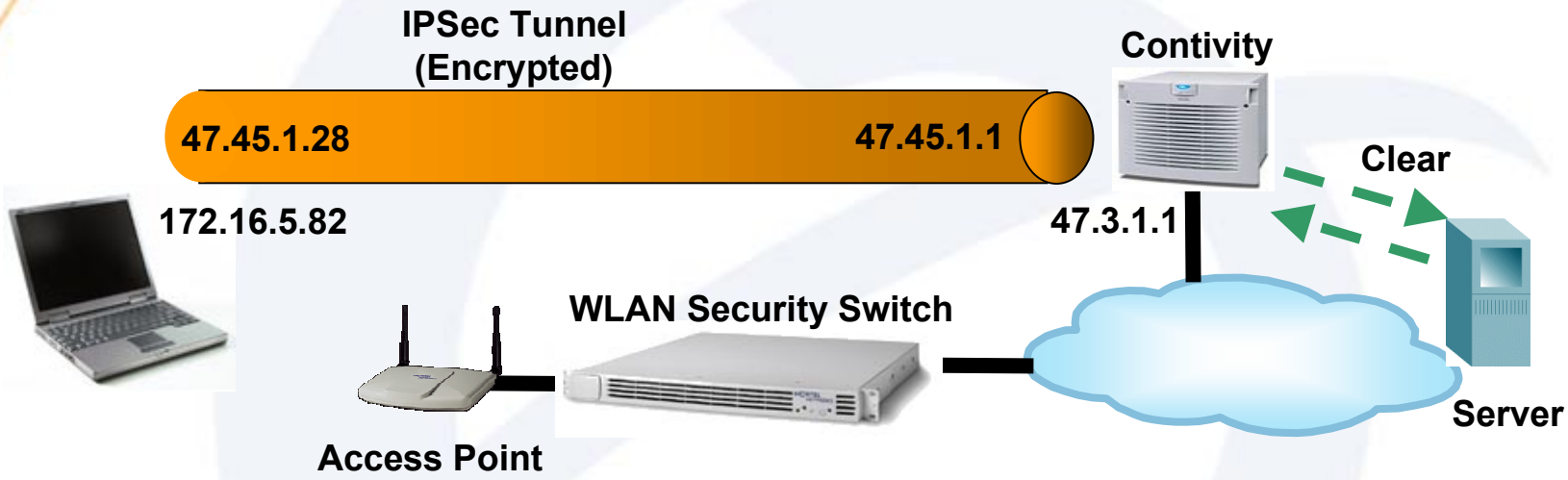
- **Le Client se log sur le portail web via une connexion SSL**
  - Il s'agit de son WSS Home (déterminé par le subnet du WLAN)
  - Session chiffrée entre la VIP et le Client IP
  - Non chiffrée sur l'Intranet
- **L'accès Intranet/Internet est virtuellement le même au travers du VPN SSL**
- **Support du client Nortel SSL VPN (avec couche Socks au dessus de SSL)**

Méthode d'accès PPTP



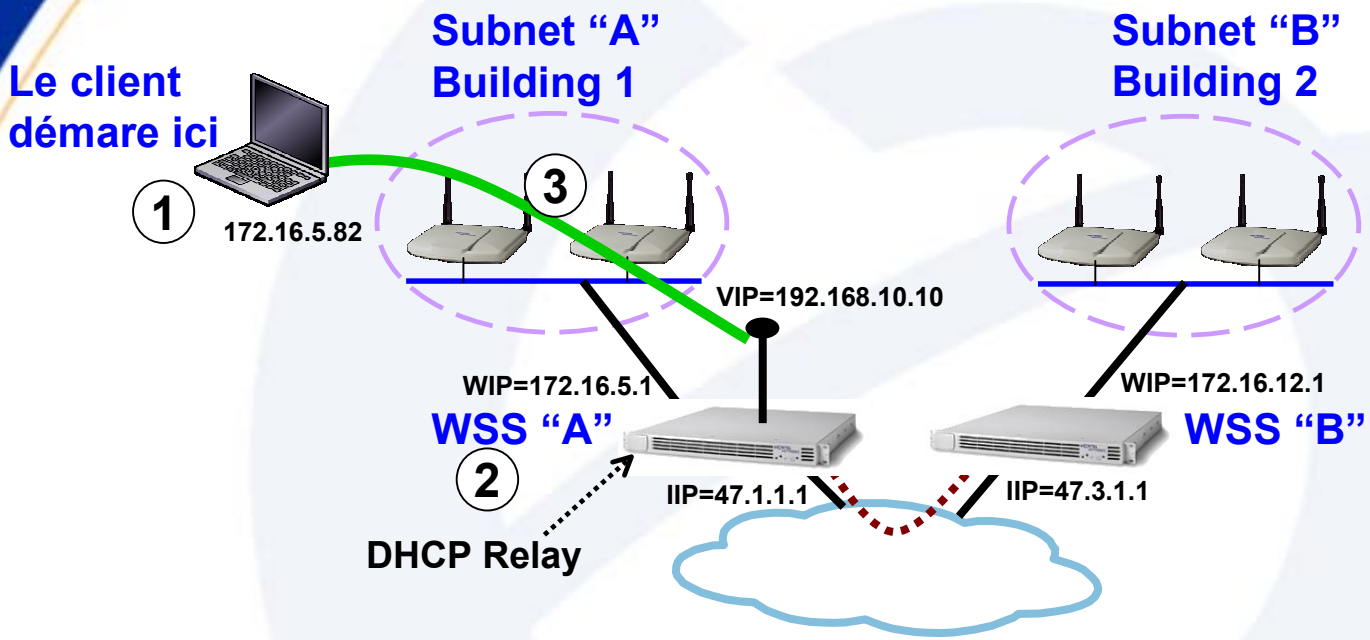
- **Le Client se log sur le portail web via une connexion SSL**
  - Récupère un One-time password du portail web
    - Permet d'éviter les attaques sur dictionaire PPTP
- **Tunnel PPTP entre Client IP et la VIP**
- **Compatible avec le client MS VPN avec le paramétrage standard**

Méthode d'accès IPSec (Passthrough)



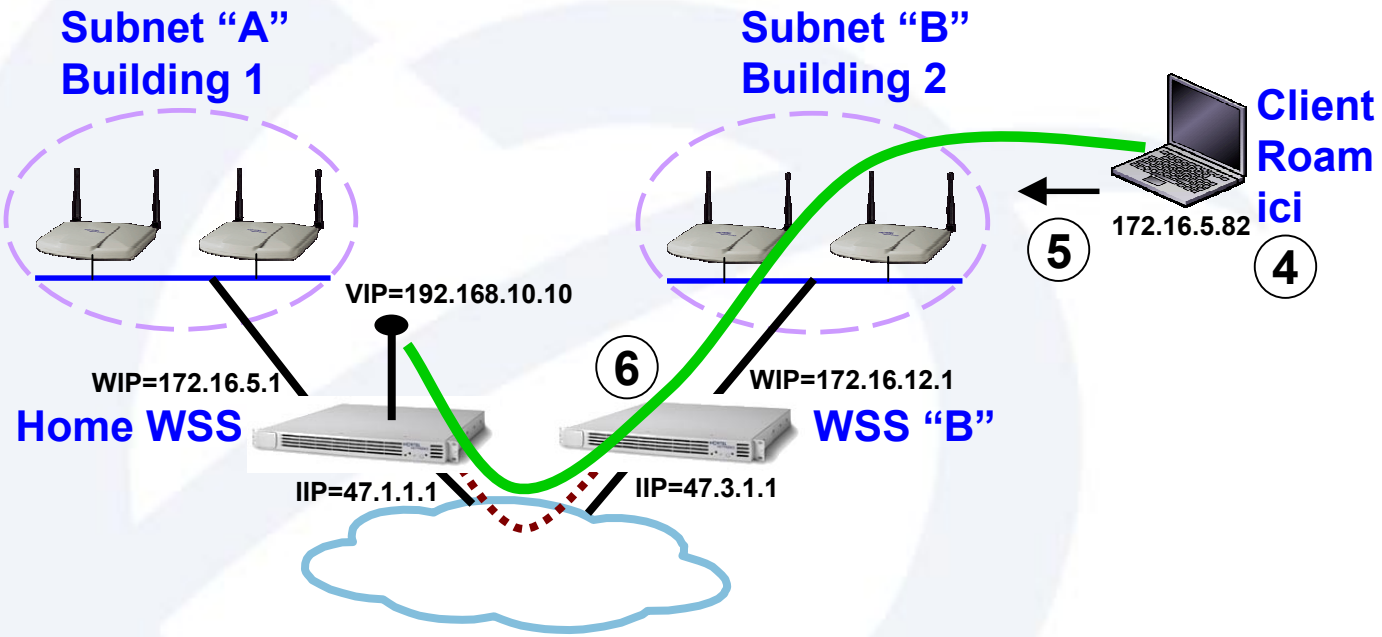
- Pas de login client sur le WSS; L'AAA est bypassé sur le WSS
- Tunnel IPSec entre Client IP et Contivity
- Les tunnels IPSec peuvent également venir d'une solution autre que Contivity

Roaming : Point de départ du Client



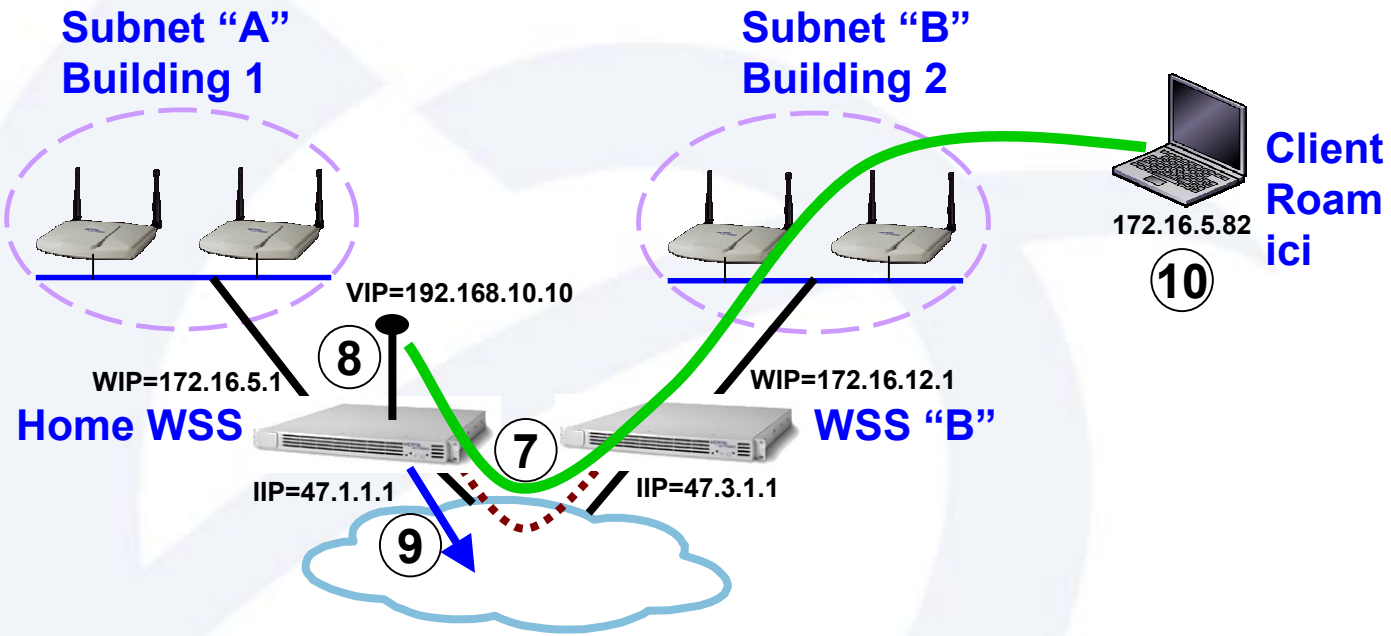
- Le Client initialise un DHCP Discover. Le WSS le relaye vers le serveur DHCP. Le Client reçoit son adresse IP dans son subnet WLAN; la WIP est assignée comme Default gateway.
- Le WSS "A" devient officiellement son Home WSS (en fonction du subnet du client)
- Le Client se log au Portail du Home WSS, ou initialise un tunnel IPSec vers un Contivity

Roaming : Déplacement du Client



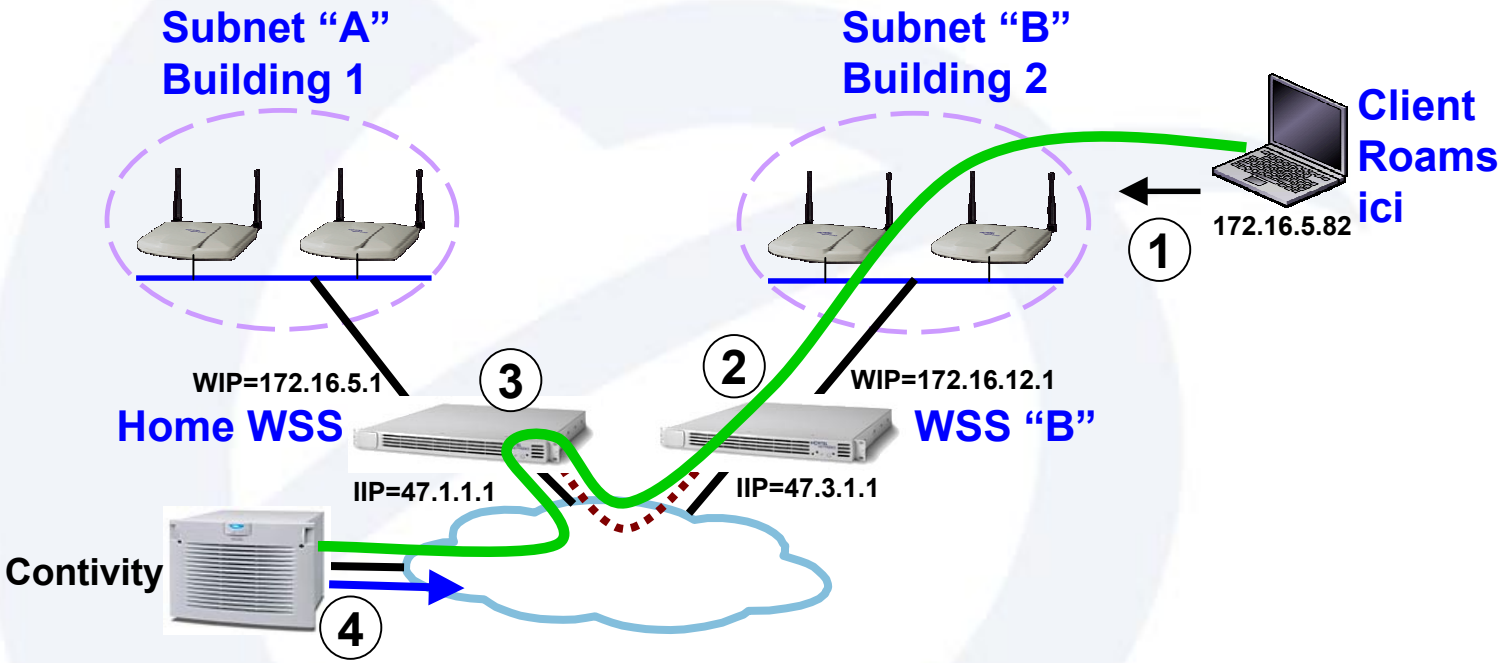
- Le Client se déplace. L'adresse IP et la default gateway restent les mêmes
- Les paquets Ethernet sont adressés à l'adresse MAC de la WIP du WSS Home
- Le WSS "B" reconnaît que cette adresse MAC appartient au WSS "A" (chaque WSS connaît la liste des adresses MACs de chacun des ports de WSS présents dans le cluster)

Roaming : Déplacement du Client



- Le WSS "B" encapsule les trames Ethernet en UDP/IP (Mobile Adaptive Tunnel) et les transmet au WSS Home
- Le WSS Home dés-encapsule et décrypte les paquets SSL (ou les paquets PPTP)
- Le WSS Home transmet les données décryptées vers le monde trusted Intranet
- Plus tard, un DHCP renewal est envoyé en Unicast à destination du Serveur. Le même mécanisme d'interception MAC permet de s'assurer que le subnet ne change pas.

Roaming: IPSec



- Comme précédemment, le paquet IPSec est envoyé à la default gateway en utilisant l'adresse MAC de l'interface WLAN du WSS "A"
- Le Paquet est encapsulé et transmis vers le WSS Home
- Le WSS Home laisse passer l'IPSec au travers de son firewall et le route vers l'Intranet
- Le Contivity décrypte et transmet aux ressources de l'Intranet

Roaming Récapitulatif

- **L'adresse IP et la Gateway du Client ne changent pas lors du roaming**
- **Le WSS Home ne change plus, une fois que le client s'est attaché au réseau**
- **Le WSS Home est déterminé par l'adresse IP du Client**
  - Les client adressés en statique peuvent forcer un WSS distant à devenir leur WSS Home
- **Le Home WSS effectue le chiffrement, le traitement firewall, le contrôle d'accès, le management de bande passante, … des clients qui lui sont affectés**

Firewall interne

- **Firewall basé sur Linux**
- **Stateful**
- **Per-user firewall**
- **Certains types de paquets sont acceptés par défaut :**
  - RADIUS (utilisé lorsque l'AP utilise 802.1x)
  - DHCP
  - DNS
- **La configuration IPSec Passthrough ouvre un trou dans le firewall vers l'adresse IP du serveur spécifié**
- **Des ouvertures manuelles peuvent être configurées si besoin**
- **Le WSS accepte les accès réseaux initialisés à partir du côté « trusted », ex : Telnet vers AP**

Fonctionnalités du Portail

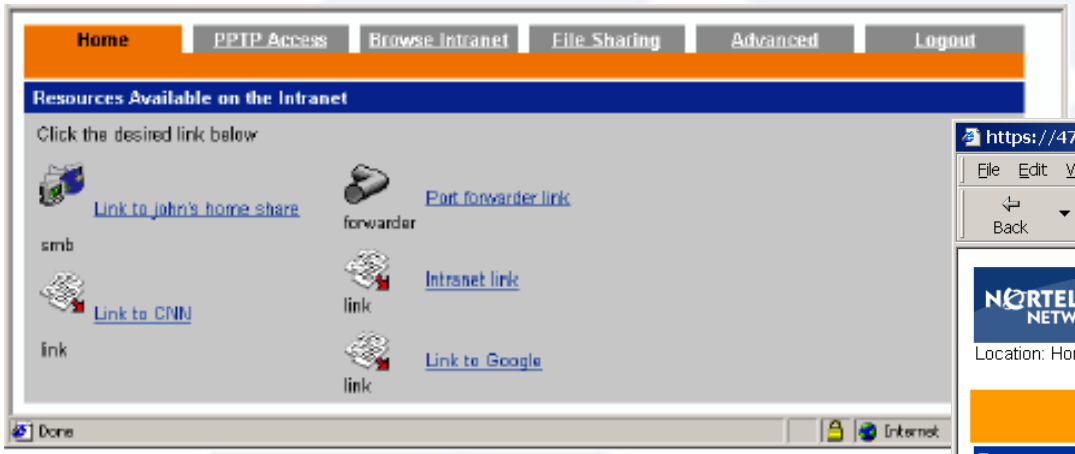
- **A le même Look and feel que celui du produit SSL VPN**
- **Fournit un accès aux applications Web**
- **Fournit un accès aux pages Web Intranet**
- **Fournit un accès vers les fichiers des serveurs de l'Intranet**
  - FTP et SMB
- **Fournit un accès vers Telnet et les serveurs SSH depuis le browser**
- **Fournit un accès vers n'importe quel serveur de l'Intranet utilisant du TCP**
- **Fournit tous les accès précédent de façon chiffrée avec SSL**

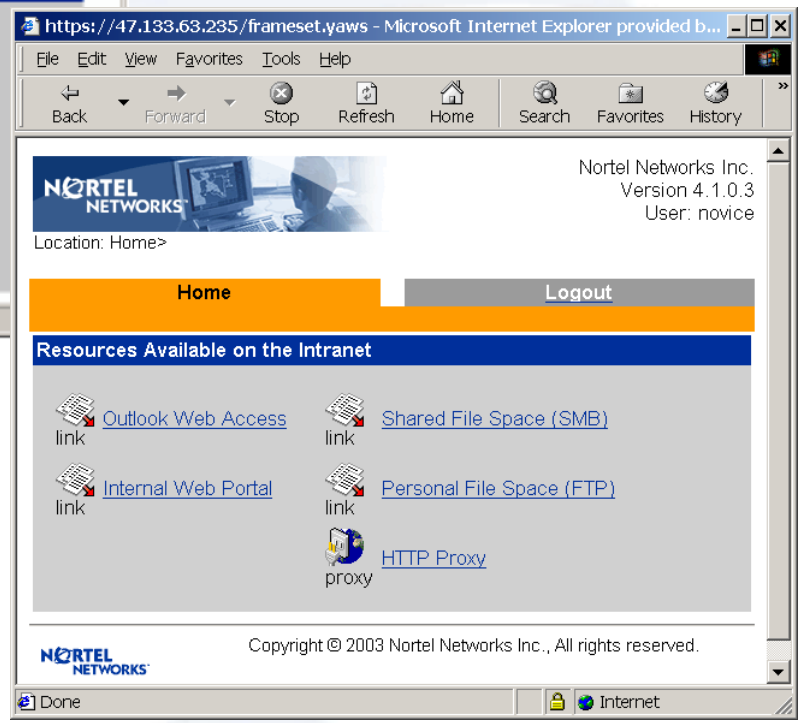
Les différents modes de VPN SSL

Mode	Fonctionnalité	Bénéfice	Notes
Basic Browser-Based Mode	**Intranet-Web Browsing** **Intranet Fileserver via FTP et/ou SMB** **Intranet Email via Outlook Web Access** **Applications Web Intranet**	**Pas de Reconfiguration du Browser** **Pas besoin de Java VM** **Pas d'installation de logiciel client** **Le mode le plus simple du point de vu du client**	
Enhanced Browser-Based Mode	**Tout ce qui est au dessus, PLUS …** **Telnet et SSH vers l'Intranet via Java Terminal Applet** **HTTP proxy Java applet pour les applications qui ne peuvent pas analyser un contenu SSL-VPN** **Port-Forwarding (application tunneling) via SSL/SOCKS Java applet.**	**Fournit un accès vers les applications traditionnelles basées sur du texte ou des consoles d'admin** **Assure la compatibilité avec toutes les application web possibles** **Fournit des accès aux applications client/server.**	**Il faut installer Java VM sur le poste.** **HTTP Proxy Java Applet disponibles à ce jour :** Emulation terminaux: TN3270/5250, VT100/320 via telnet et SSHv1 Windows Terminal Services Lotus Notes/Domino natif Client Citrix ICA Microsoft Outlook natif (Q4)
Transparent Mode	**Le client SSL VPN redirige les communications TCP/IP vers la gateway SSL VPN**	**Accès aux applications identiques en utilisant les clients natifs.** **Pas besoin de reconfigurer les applications ou de lancer un proxy/port-forwarder**	**Le logiciel SSL VPN client doit être installé et configuré sur le poste**

Rq : Le client SSL VPN doit être installé après les drivers de la carte WLAN 2201.

Portail





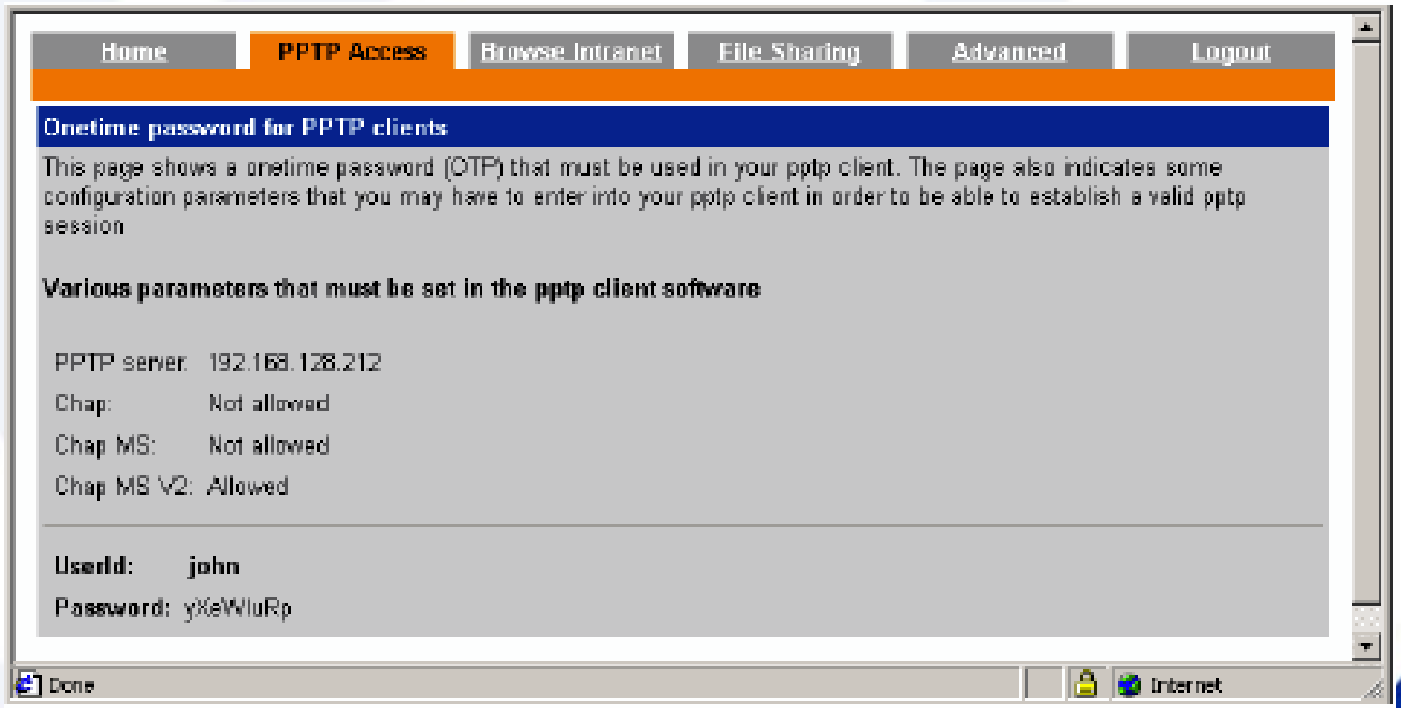
- **Les User Groups sont assignés à un “UserType” du portail qui peut être Novice/Medium/Advanced**
- **Les onglets disponibles sur le portail sont restreints en fonction de ce paramétrage :**
  - **Novice : Home / Logout**
  - **Medium : Home / PPTP / Browse Intranet / File Sharing / Logout**
  - **Advanced : idem + Advanced**

Onglet Home : Liens

- **Types de liens :**
  - Lien vers une URL intranet ou externe
  - Lien de logon automatique pour protéger par mot de passe les URL intranet ou externes
  - Lien vers un serveur FTP ou SMB
  - Lien Port Forwarder via SOCKS
  - Lien HTTP Proxy
  - Lien vers serveur SSHv1 ou Telnet
- **shortcuts pré-définis**
- **Une “Intranet” URLs prend la forme :** http://wlan.nortel.com/http/www.yahoo.com/home.html
- **Une URL “External ” prend la forme** http://www.yahoo.com/home.html

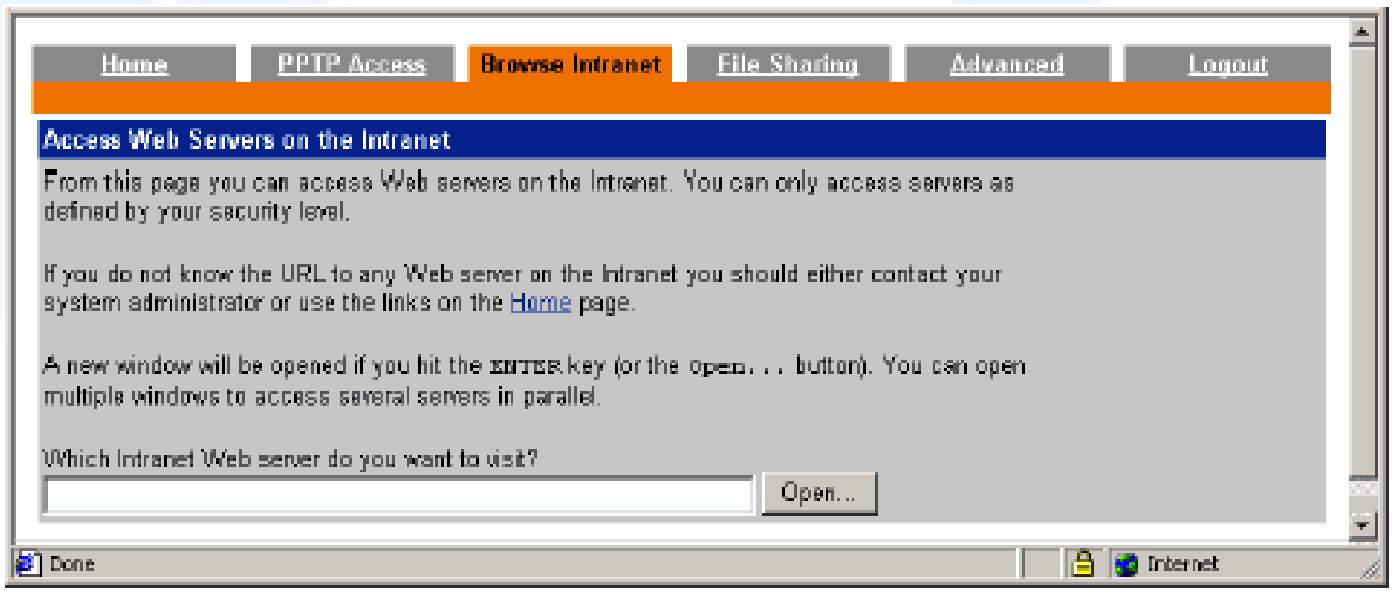
Onglet PPTP

- Fournit l'information nécessaire au paramétrage information du client MS VPN pour se connecter au portail
- Génère un one-time client password
- Les paramétrages PPTP par défaut du WSS fonctionne avec le paramétrage par défaut du client VPN de Win2k



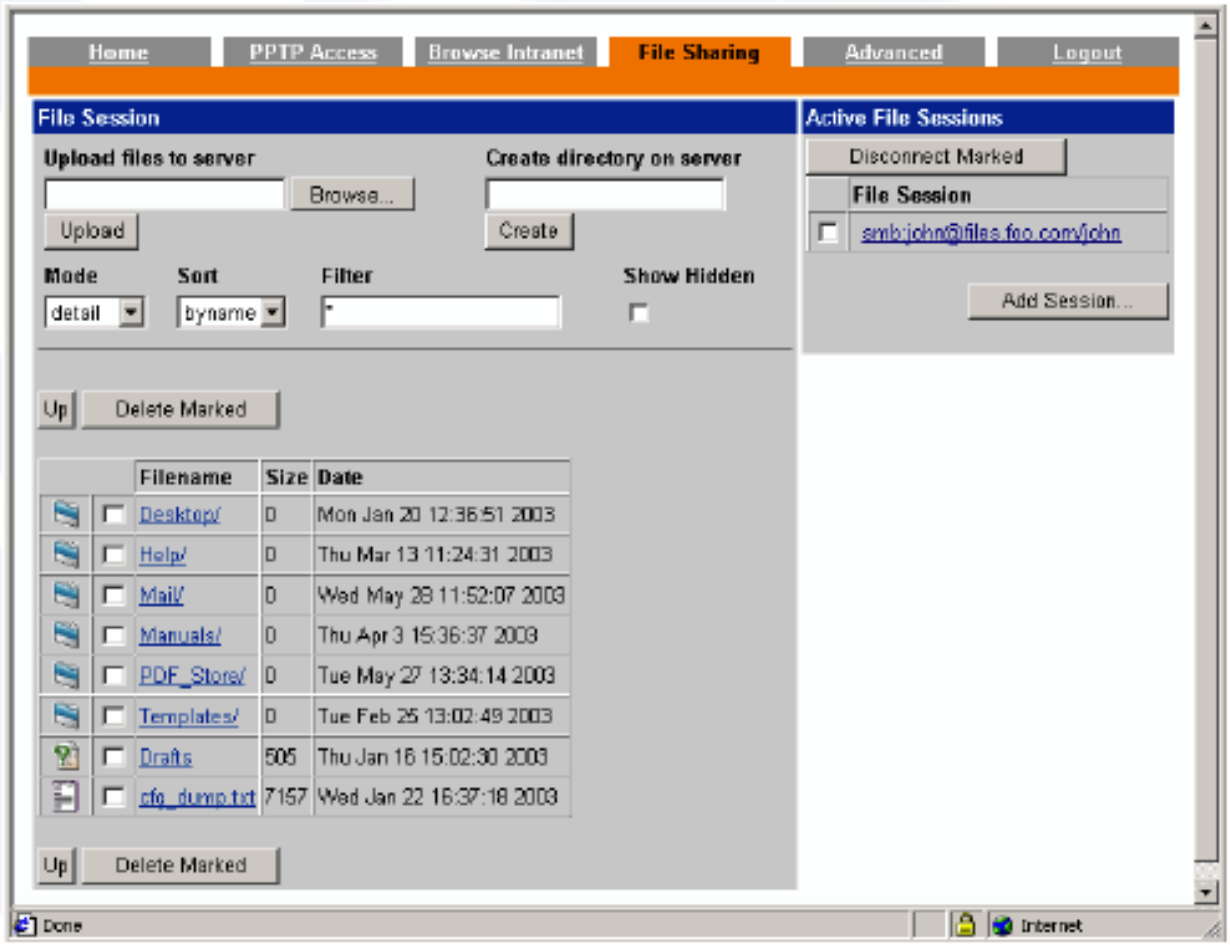
Onglet Browse Intranet

- **Rentrer l'URL dans le champs et clicker pour ouvrir**
- **Le portail "proxies" la page Web**
  - Ex : http://wlan.nortel.com/http/www.yahoo.com/home.html



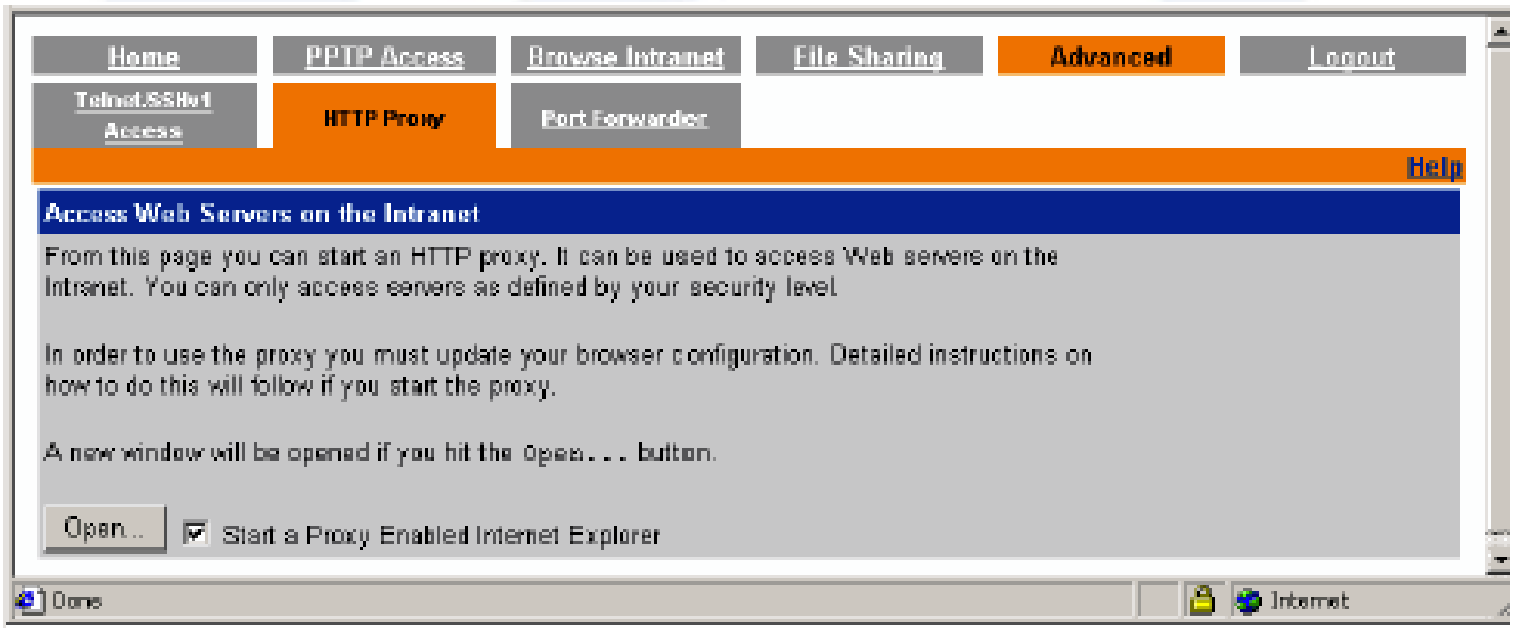
Onglet File Sharing

- Capacité à créer des répertoires avec partage de fichiers via SMB et transfert via FTP
- Affichage convivial des répertoires en partage de fichiers

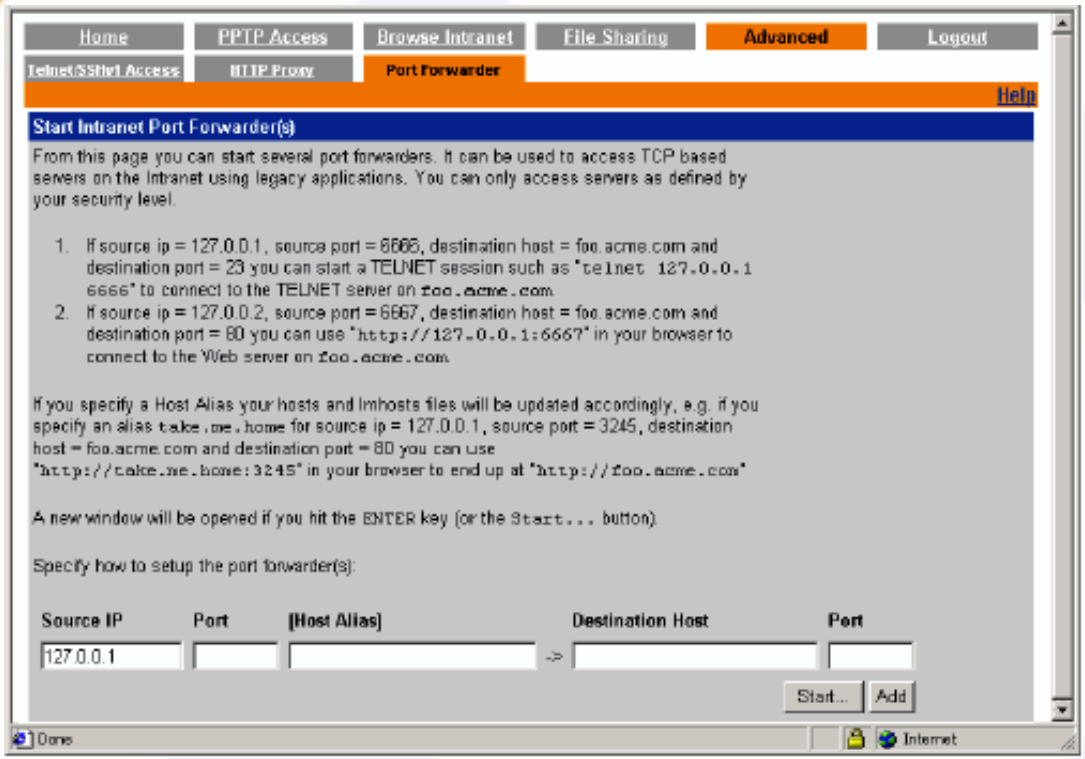


Advanced : Onglet HTTP Proxy

- **Checkbox pour activer automatiquement la configuration de IE afin d'utiliser l'Applet HTTP Proxy**



Advanced : Onglet Port Forwarder



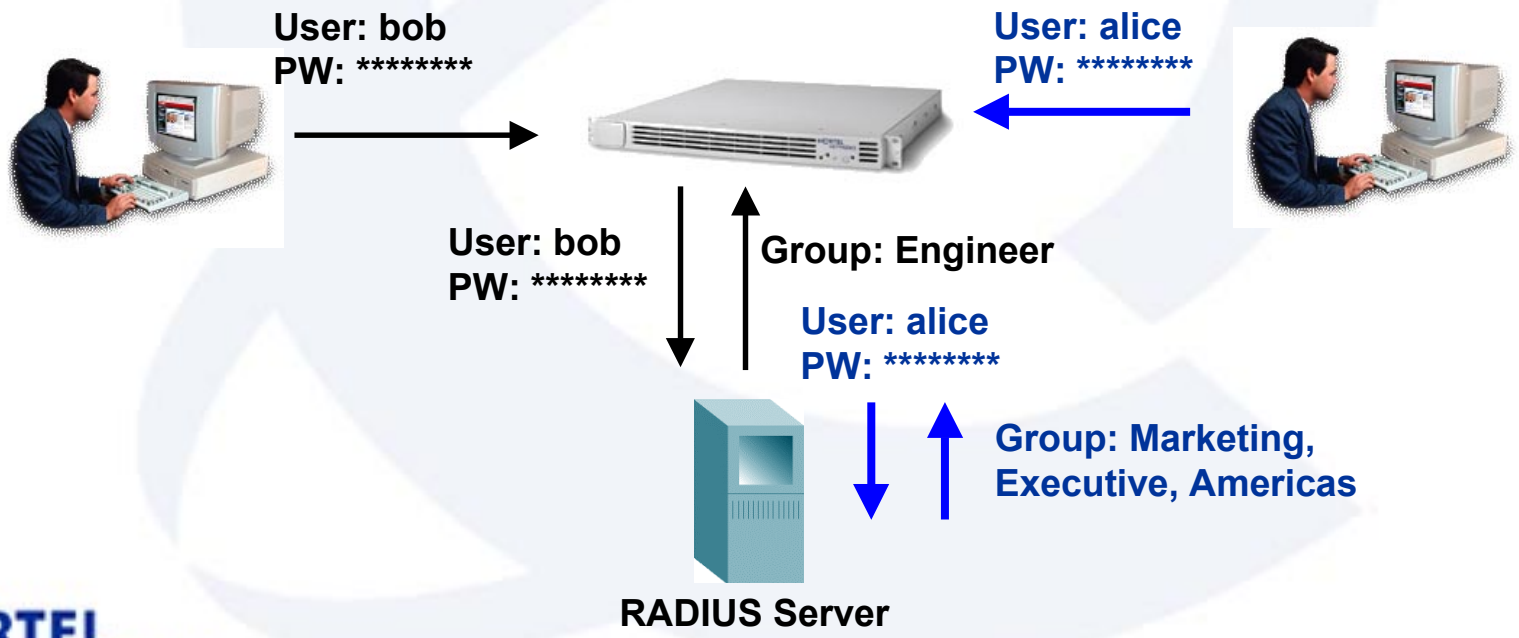
- Crée de Multiple connections TCP entre le client et le serveur avec une seule applet
- Des ports locaux dupliqués peuvent être utilisés via une unique adresse IP locale
- Adapté pour lancer de multiples instances d'une application avec des ports fixes
- Bouton "Add" permet de spécifier un nouveau forwarder.
- Bouton "Start" démarre l'applet avec tous les forwarders spécifiés

Captive Portal

- Si un utilisateur WLAN ouvre une fenêtre browser et tante d'accéder à un serveur Intranet/Internet sans une première authentification auprès du Portail, le web browser sera redirigé vers le portail
- Le Captive Portal n'affecte pas les clients équipés du SSL VPN client ou les accès réseau par IPSec

Authentification

- **Login sur le WSS**
  - Page web du portail ou client SSL VPN
- **Le Group membership est envoyé au WSS**
- **Le WSS l'associe au Group Profiles**
- **Si ce groupe n'existe pas, l'utilisateur est assigné au groupe par défaut**

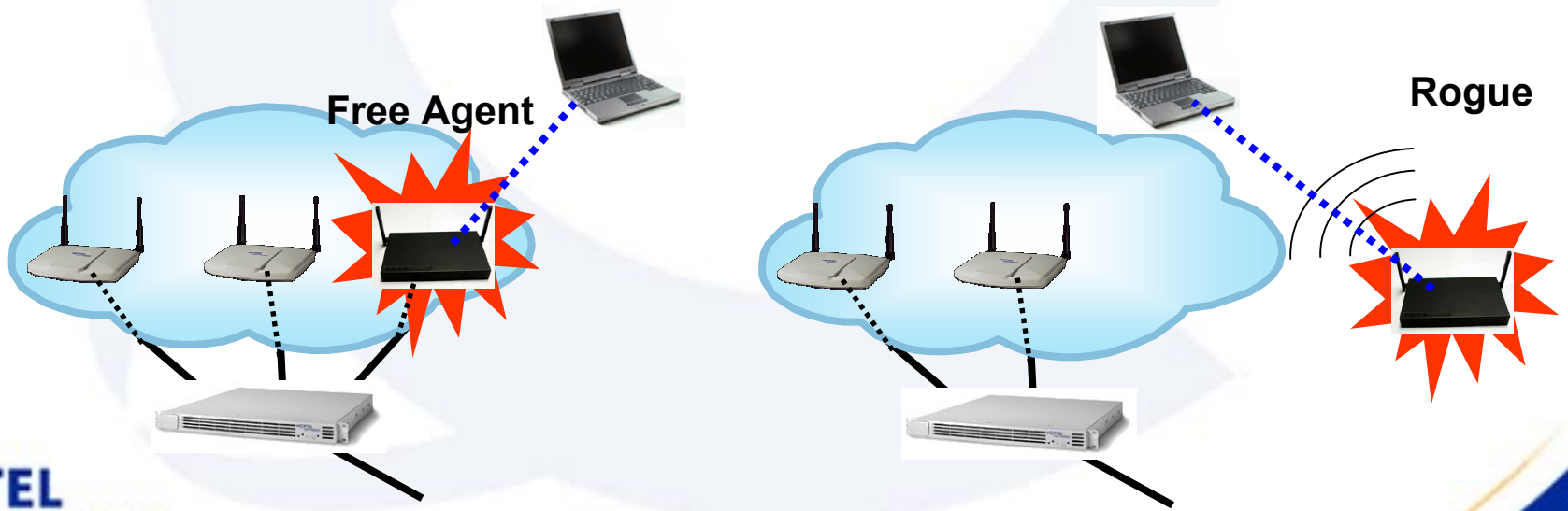


Serveurs d'Authentification

- **Support de :**
  - RADIUS
  - LDAP (incluant Active Directory)
  - NTLM
  - Local : Database locale
- **Multiple serveurs d'Authentification**
  - Chaque "serveur" spécifie le type et la liste des adresses IP (pour la redondance)
  - De multiple "serveurs" peuvent être spécifiés pour la recherche
  - Dés que le client est authentifié, la recherche s'arrête
    - Ex : 1) AD Server, 2) RADIUS#1, 3) RADIUS#2, 4) Local

Rogue et Free Agent AP

- **Free Agent AP: Un AP connecté sur le réseau local**
  - Ex : Un utilisateur qui connecterait sa propre AP dans le LAN
- **Rogue AP: Un AP non-autorisé qui se connecterait à partir d'un autre réseau, ou à aucun réseau**
  - ex #1: Un Hacker tentant de dérober des informations
  - ex #2: Une société voisine qui aurait mal configuré un AP



Détection des Rogue AP

- **Une liste d'AP autorisés est configurée**
  - Adresses MAC au format xx:xx:xx:xx:xx:xx
- **Tous les autres AP sont considérés comme non-autorisés**
- **La détection est basée sur l'écoute des broadcasts UDP envoyées entre AP lorsque qu'un utilisateur effectue du roaming (trames IAPP 802.11f)**
  - Ces Paquets contiennent les adresses MAC des APs
- **Lorsque le WSS détecte l'adresse MAC d'un AP non-autorisé :**
  - Message Syslog
  - Envoi d'un trap SNMP

Premières évolutions prévues : Q4 03

- **Release 2.0 :**
  - H-A (Master redondants dans un cluster, VRRP)
  - Hitless upgrade
  - Load balancing
  - Terminaison de tunnels IPSec
  - QoS (gestion de priorités par utilisateur)
  - Mise à jour des APs centralisée
  - DHCP Serveur
  - 64 WSS par Cluster
  - Tunnels GRE
- **2260**
  - Modèle pourvu de ports Giga fibre

Coûts du 2250

- DR4001B56 - WLAN 2250 Wireless Security Switch. Europe Power Cord.Includes hardware encryption module with 128-bit encryption :
  - **$ 7 995,00 PP HT**
- De base, le WSS 2250 permet de gérer 10 tunnels VPN simultanés. Un système de license permet d'accroître cette capacité :
- EB1639055 : License pour 100 tunnels VPN simultanés :
  - **$ 9 995, 00 PP HT**
- EB1639056 : License pour 250 tunnels VPN simultanés :
  - **14 995,00 PP HT**
- EB1639057 : License pour 500 tunnels VPN simultanés :
  - **24 995,00 PP HT**
- EB1639064 : License pour 1000 tunnels VPN simultanés :
  - **39 995,00 PP HT**

Coûts d'une solution Wireless Nortel

- Le nombre d'AP nécessaires pour un WLAN dépend de nombreux paramètres :
  - Physiques : Obstacles présents, nature de ces obstacles (verre, béton …)
  - Bande passante requise par utilisateur (en fonction des applications souhaitées)
  - Niveau de recouvrement souhaité entre les zones radio (pour faciliter le roaming)
- DR4001B55 - WLAN 2220 Access Point IEEE 802.11a/b EU cnfg. Accepts Power over Ethernet with power supply, Northern European power cord. Includes Software CD, Documentation CD, wall mount bracket, and Web Management Software :
  - **$ 949,00 PP HT**

NORTEL NETWORKS CONFIDENTIAL