SAS ELOY

Quality needs Precision

Rapport de stage

Audit et restructuration de l'infrastructure de la société SAS ELOY *mai-juin 2011*

par Mr FRANCISCO Nelson

Au-delà du perfectionnement de nos processus de production et de l'optimisation de la qualité, nous anticipons les besoins du marché afin de proposer à nos clients des solutions d'usinage et d'assemblage sur mesure à forte valeur ajoutée.

SOMMAIRE

Avant-propos

Dans le cadre d'une reconversion professionnelle, l'AFPA de Champs sur marne m'a proposé une formation diplômante de Technicien supérieur en réseaux informatiques et télécommunications. Cette formation a pour objectif de mettre sur le marché de l'emploi des diplômés capables de :

- Exploiter, superviser et garantir la continuité de service des réseaux informatiques et télécommunications de l'entreprise ;
- Contribuer à l'administration des réseaux informatiques et télécommunications de l'entreprise ;
- Participer aux études d'optimisation des réseaux informatiques et télécommunications de l'entreprise.

Au terme de la formation, l'étudiant est tenu d'effectuer une période d'application en entreprise d'une durée de huit semaines sanctionné par un mémoire dont la note porte sur le travail réalisé, le rapport de stage et la présentation orale effectuée.

Le présent rapport fait suite au stage effectué dans les locaux de la société SAS ELOY, 18 rue Condorcet 94430 Chennevières Sur Marne, du 26 avril au 17 juin 2011 sous le thème Audit et restructuration de l'infrastructure de la société SAS ELOY.

I. Présentation de la société ELOY

1. La société ELOY

Depuis sa création en 1919, la société ELOY est spécialisée dans la production de pièces mécaniques de haute précision en moyenne et grande série.

Au sein d'un site unique de production, d'une surface couverte de 5200 m^2, la production d'ELOY en pièces et ensemble de pièces équipe 4 millions de véhicules par an.

1.1 L'histoire d'ELOY en quelques dates :

- 1919 : Fabrique de la boulonnerie décolletée pour l'électricité et l'automobile.
- 1964 : A l'activité de décolletage automatique s'ajoutent les boîtiers à rotule à coussinets plastiques.
- 1978 : Diversification de la section décolletage vers l'usinage de fonderies, acquisition de machines à commandes numériques.
- 1992 : Première certification qualité (EAQF). Extension du site soit 5200 m2 de surface couverte.
- Aujourd'hui : Production de pièces de précision en moyennes et grandes séries. Une clientèle internationale dans différents domaines d'activité. ELOY est certifié ISO 9001 version 2000.

2. La production

2.1 Systèmes de production

À la pointe, performante et réactive, le système de production d'ELOY repose sur une organisation par îlots robotisés. Sous le contrôle d'un personnel qualifié, ces unités indépendantes regroupent des machines-outils, robots et convoyeurs pour une réduction maximale des temps logistiques et stocks tampon intermédiaires.

À la pointe, puisqu'ELOY dispose de 53 centres d'usinage et 28 tours numériques récents dont la capacité des magasins d'outils autorise l'enchaînement de toutes les opérations d'usinage en grande série.
En recherche permanente de compétitivité, ELOY investi régulièrement dans le renouvellement de son parc machine de production et de contrôle qualité.

Performant, car la durée des cycles de production est optimisée aux capacités maximales des machines-outils. Le système de filtration centralisé pour le lavage et la lubrification des machines autorise ces cadences élevées.

Réactif, car un atelier dédié au bureau d'études interne permet une réalisation rapide des outillages et prises de pièces adaptés à chaque projet.

2.2 Pièces mécaniques

Fournisseur système, ELOY est spécialiste de l'usinage de grande précision à partir de pièces de fonderie ou extrudées en moyenne et grande série notamment pour l'automobile, les poids lourds, l'industrie et la téléphonie.

Les outillages sont équipés pour usiner tous les métaux et principalement les aciers, les fontes et les alliages légers.

ELOY usine des pièces mécaniques d'un diamètre de 20 à 250 millimètres et de 20 gramme à 5 kilos.

Ces pièces ou sous-ensemble de pièces mécaniques sont des composants hydrauliques, pneumatiques ou de structure pour diverses fonctions essentielles telles que freinage/ABS, direction assistée, turbo, boîte de vitesse, châssis, liaison au sol…

ELOY propose également des solutions d'assemblage et de pré-assemblage telles ajouts de goujons, paliers, joints, roulements… De plus, pour les besoins qualificatifs spécifiques des produits soumis à pression, des contrôles par vision et d'étanchéité sont intégrés à l'outil de production.

2.3 Biellettes

ELOY fabrique des éléments de transmission de mouvements pour les boîtes de vitesse, les capteurs de hauteur, les embrayages…

2.4 Rotules

ELOY assemble des rotules en moyenne et grandes séries. Elle compte XX références standard et est capable de répondre à de nouvelles demandes d''assemblage dans des délais très courts.

3. Expertise & qualité

3.1 Expertise

Près de 90 ans, au cours desquels ELOY :

- A acquis une connaissance approfondie des constructeurs et équipementiers, de leurs enjeux, des spécialités de leurs organisations et de leurs méthodes de travail ;
- A développé une expertise métier dans différents domaines d'application : freinage, moteurs, boîtes de vitesse, châssis, direction …
- S'est forgé une solide expérience dans la construction d'une coopération étroite avec des industriels internationaux.

Son expertise repose avant tout sur les compétences et l'expérience de son personnel au sein d'une structure organisée.

Ces processus de production et de qualité sont régulièrement validés par les organismes de certification ISO et par des audits spécifiques de nos clients.

3.2 Qualité

ELOY est certifié ISO 9001 version 2000 et prochainement ISO/TS 16949.

Notre laboratoire de métrologie climatisé dispose des outils nécessaires récents pour les mesures de tolérance de pièce, nous y effectuons les contrôles et le suivi qualité de la production.

Pour les produits soumis à pression des contrôles par vision et d'étanchéité sont intégrés à l'outil de production.

Le service de gestion de la Qualité établit, pour chaque projet, les documents normatifs, indicateurs et statistiques de suivi de production selon les critères de certification ISO. Cette formalisation garantit le respect du cahier des charges de leurs clients.

4. Références

4.1 Clients

La clientèle d'ELOY est internationale et issue de domaines d'activités variés tels que l'automobile, les télécommunications, les poids lourds, le BTP…

Les principaux clients sont :

- BOSCH
- CITROËN
- Delphi
- DURA
- HPI
- JTEKT
- NORTEL NETWORKS
- PEUGEOT
- SNCF
- Suntec
- TRC
- ZF Lenksysteme

4.2 Les véhicules équipés

ELOY équipe plus de 4 millions de véhicules par an et sait répondre aux exigences du marché : la qualité et la technologie de pointe du haut de gamme, la robustesse des SUV et la performance économique des véhicules courants.

- Peugeot: 405, 206, 306, 307, 406, 407, 607, 408
- Citroën: Xantia, Berlingo, Xara, Jumpy, Picasso, C4, C4 Picasso, C3 Picasso, C5, C5 phase II, C6
- Alfa Romeo: 159, Brera
- Opel: Astra, Zafira
- Cadillac SRX
- Volvo: S40, V50
- Renault: Laguna III
- BMW: X1, série 3, série 5, série 7, X5
- Saab : 9-3
- Rolls Royce
- 200EX
- Volswagen : Multivan, Touareg, LADA
- Jaguar : X200, X400
- Porsche : Cayenne
- Audi Q7
- Aston Martin

II. Remerciements

Je tiens à remercier dans un premier temps, toute l'équipe pédagogique de l'AFPA et les intervenants professionnels responsables de la formation TSRIT, pour avoir assuré la partie théorique de celle-ci.

Je remercie également Madame Claire SOBESKY pour l'aide et les conseils concernant les missions évoquées dans ce rapport, qu'elle m'a apporté lors des différents suivis.

Je tiens à remercier tout particulièrement et à témoigner toute ma reconnaissance aux personnes suivantes, pour l'expérience enrichissante et pleine d'intérêt qu'elles m'ont fait vivre durant ces deux mois au sein de l'entreprise SAS ELOY :

Monsieur Barthélémy VIVES, PDG de la société, pour son accueil et la confiance qu'il m'a accordé dès mon arrivée dans l'entreprise.

Monsieur Thomas GUILBERT, responsable du service GESTION PRODUCTION de la société ELOY, mon tuteur, pour m'avoir intégré rapidement au sein de l'entreprise et m'avoir accordé toute sa confiance ; pour le temps qu'il m'a consacré tout au long de cette période, sachant répondre à toutes mes interrogations ; sans oublier sa participation au cheminement de ce rapport.

Monsieur Jean MATHIEU et madame Catherine PAOLI ainsi que l'ensemble du personnel d'ELOY pour leur accueil sympathique et leur coopération professionnelle tout au long de ces deux mois.

III. Objectifs de la mission technique

1. Sujet de stage

Audit et restructuration de l'infrastructure réseau de la société ELOY.

Le stagiaire devra participer aux études d'optimisation du réseau informatique, rechercher et évaluer des solutions techniques nouvelles incluant la sécurité en rencontrant des commerciaux, proposer des scénarios d'évolution de mise en œuvre et d'argumenter leur choix.

Le stagiaire devra dans un deuxième temps mettre en place les différents scénarii retenus.

2. Cahier des charges fonctionnel

Suite à une restructuration en 2007 et après la crise économique subie en France, la société ELOY a désiré rajeunir son installation informatique.

La société dispose de 3 serveurs :

- Un serveur linux où sont stockés tous les fichiers de la société.
- Un serveur SAGE
- Un serveur MAIL

La direction souhaite rassembler tous les services sur un seul serveur. Pour cela il faudra installer un nouveau serveur qu'il faudra sélectionner (l'achat d'un nouveau serveur sera indispensable pour regrouper ces services de manière optimale, les trois serveurs actuels étant vieillissant).

Un audit sur les ressources matérielles et logicielles de la société devra être réalisé.

Différents problèmes ont été évoqués par les employés concernant des ralentissements au niveau de l'accès au serveur, des délais trop longs pour l'envoi d'un mail en interne, etc…

3. Critères de validation du projet

Tous les utilisateurs devront avoir accès aux fichiers, soit à l'aide de l'ERP SAGE, soit grâce à un autre progiciel.

Le choix des différents scénarii d'évolution devront tenir compte :

- Du coût.
- De la simplicité d'utilisation

La mise en œuvre doit autant que possible être transparente pour l'utilisateur. La monopolisation des postes utilisateurs doit être réduite au maximum.

Les différents scénarii retenus devront être livré dans un état fonctionnel.

Des tutoriels ainsi que la topologie du réseau seront livré en fin de stage.

4. Moyens mis à disposition du stagiaire

L'accès aux trois serveurs nous est interdit. Les serveurs mail et fichiers étant maintenu par un prestataire de service qui annulerait les contrats de maintenance si l'accès était donné. Le troisième serveur (SAGE) étant aussi sous contrat de maintenance, les répercussions seraient les même.

L'accès extérieur est un routeur Cisco administré par Orange. Il n'est accessible qu'avec un login non modifiable détenu par orange.

La société met à notre disposition un bureau équipé d'un téléphone pour les contacts commerciaux, des devis réalisés en 2010 proposant des scénarii d'évolution au niveau infrastructure ou téléphonique, ainsi que divers documentations et logicielles utilisés par l'entreprise.

5. Planification du projet

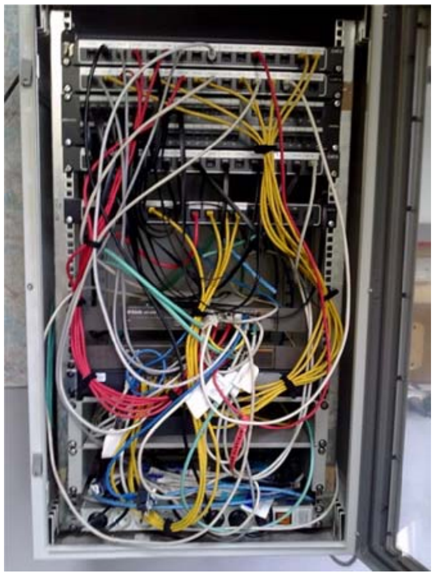
La première semaine est consacrée aux différents audits, la deuxième à l'étude des différents scénarii d'évolution via des recherches sur internet ou via des rencontres avec des commerciaux et leurs différents devis.

Les semaines suivantes seront employés à la réalisation du projet en virtualisant les différents scénarii avant de les déployés.

La dernière semaine sera employée aux différents peaufinages des installations, à l'écoute des dernières préoccupations du personnel de l'entreprise ainsi qu'à la réalisation de différents tutoriels.

IV. Conformité des installations et des équipements réseaux

1. Accès et état du local technique



Le local technique ou enfin la baie de brassage est situé dans un couloir qui joint les bureaux administratifs à l'atelier.

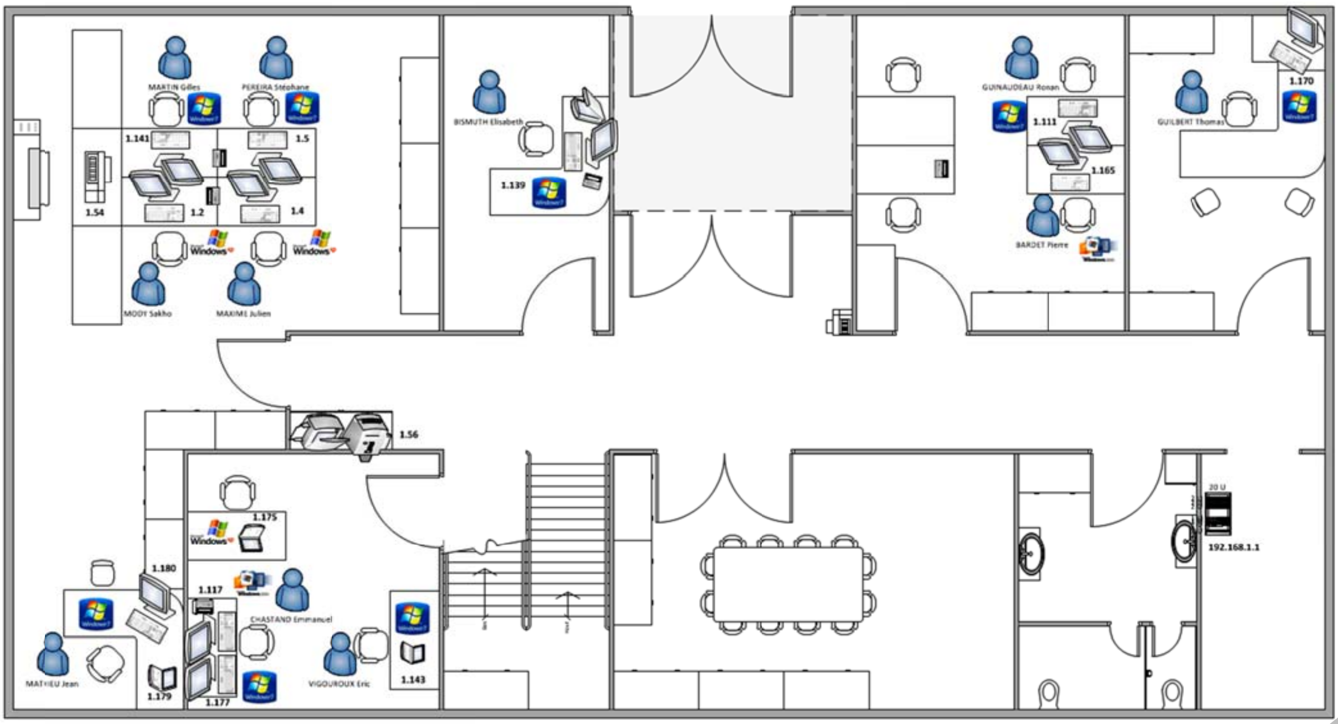
En effet, il n'existe pas de local technique dans la société.

On peut voir dans cette baie une installation initiale suivi de plusieurs rajout établit par les employés eux-mêmes. Des panneaux de brassage ainsi que des commutateurs ont été rajoutés au fil du temps.

Aucun étiquetage n'est présent sur les câbles. Une journée entière fut nécessaire pour savoir à quelle prise un câble était raccordé.

2. Etat de l'infrastructure de connexion réseau

2.1 Rez-de-chaussée de la société



Au niveau de la baie de brassage située au rez-de-chaussée, deux commutateurs DLINK et un 3COM sont relié en cascade et relie chaque prises ethernet de la société sans aucun ordre précis.

Seul le premier étage dispose de plusieurs prises ethernet par pièces. Au rez-de-chaussée les postes informatiques sont reliés via des câbles qui ont été passé par le plafond.

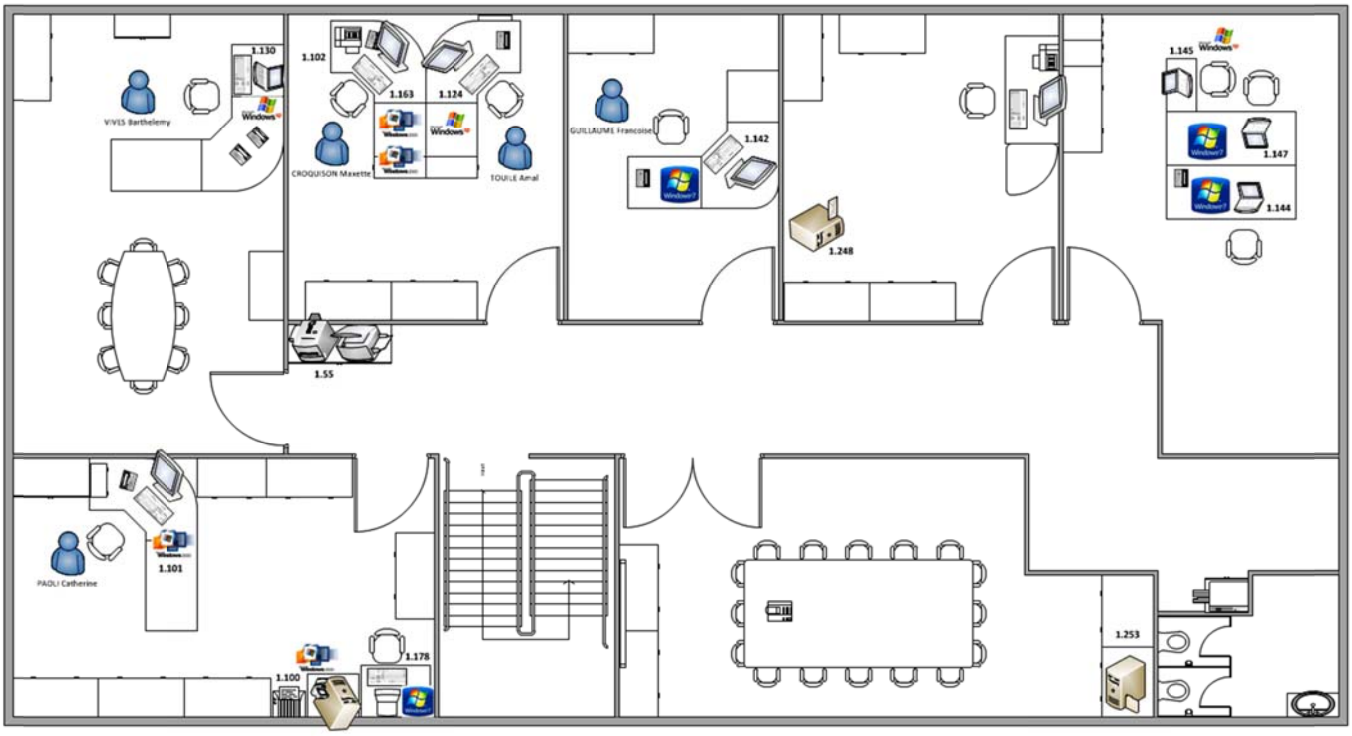
Les postes du bureau études (situé en haut à gauche sur le plan du rez-de-chaussée) sont reliés à un commutateur lui-même relié à la baie

Un câble traverse le couloir par le plafond vers la baie de brassage et les autres sont renvoyés par le plafond pour desservir une colonne au centre des bureaux dessins.

Un commutateur NETGEAR assure la liaison pour le bureau du chef projets ainsi que les bureaux des commerciaux.

Enfin pour relié l'atelier à la baie de brassage, un autre commutateur relie sept postes informatiques au réseau. Le câble reliant ce commutateur à la baie de brassage ne pouvant pas traverser l'atelier à cause des perturbations des machines, il a été passé par le toit à l'intérieur d'un tuyau d'arrosage.

2.2 1er étage de la société



Le premier étage, lui, dispose de six prises réseaux et 3 téléphoniques par pièces.

Le serveur de fichier est enfermé dans une armoire disposant d'une ventilation récupérée sur un ordinateur.

@ IP :

192.168.1.253

Serveur Mail @ IP : 192.168.1.248

Serveur SAGE @ IP : 192.168.1.100

2.3 Accès extérieur

2.3.1 *Lignes téléphoniques*

La société compte 4 lignes téléphoniques dédiées au FAX :

- 01.45.76.52.65
- 01.45.94.62.86
- 01.56.31.37.44
- 01.56.86.11.59

A droite de la baie de brassage se trouve un PABX Lucent Technologies.

Plus connu sous le nom de standard téléphonique, un PABX (Private Automatic Branch eXchange), n'est ni plus ni moins qu'un commutateur : à savoir, un appareil assurant automatiquement les connexions téléphoniques entre appelé et appelant, aussi bien au sein de l'entreprise que vers l'extérieur. D'où son autre nom : autocom pour « autocommutateur ».

4 liens BRI dessert le PABX, ce qui nous donne 8 canaux voies.

- 01 45 76 65 30
    - C1 15
    - C1 45
    - C1 62

Pour une société de plus de 100 personnes, ca peut paraître léger. Mais des dires des employés, pour l'instant personne ne s'est plaint.

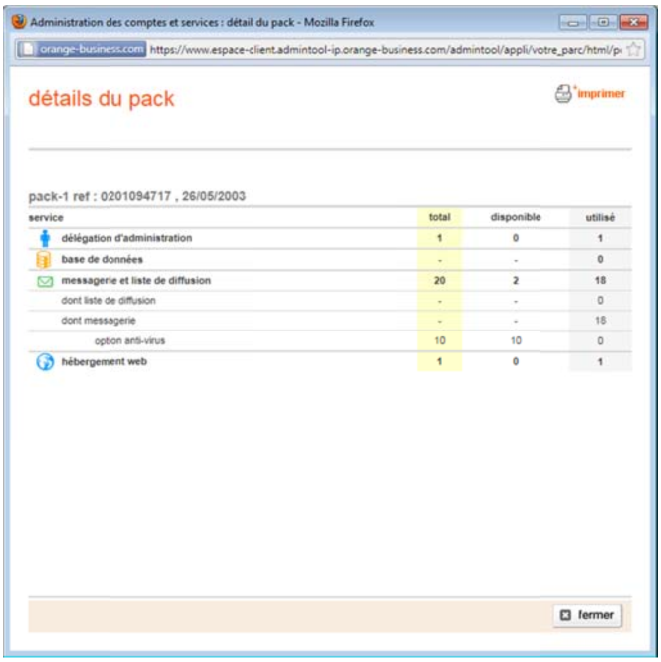
2.3.2 *Accès internet*

La société a souscrit à un pack Business Internet Office chez Oléane

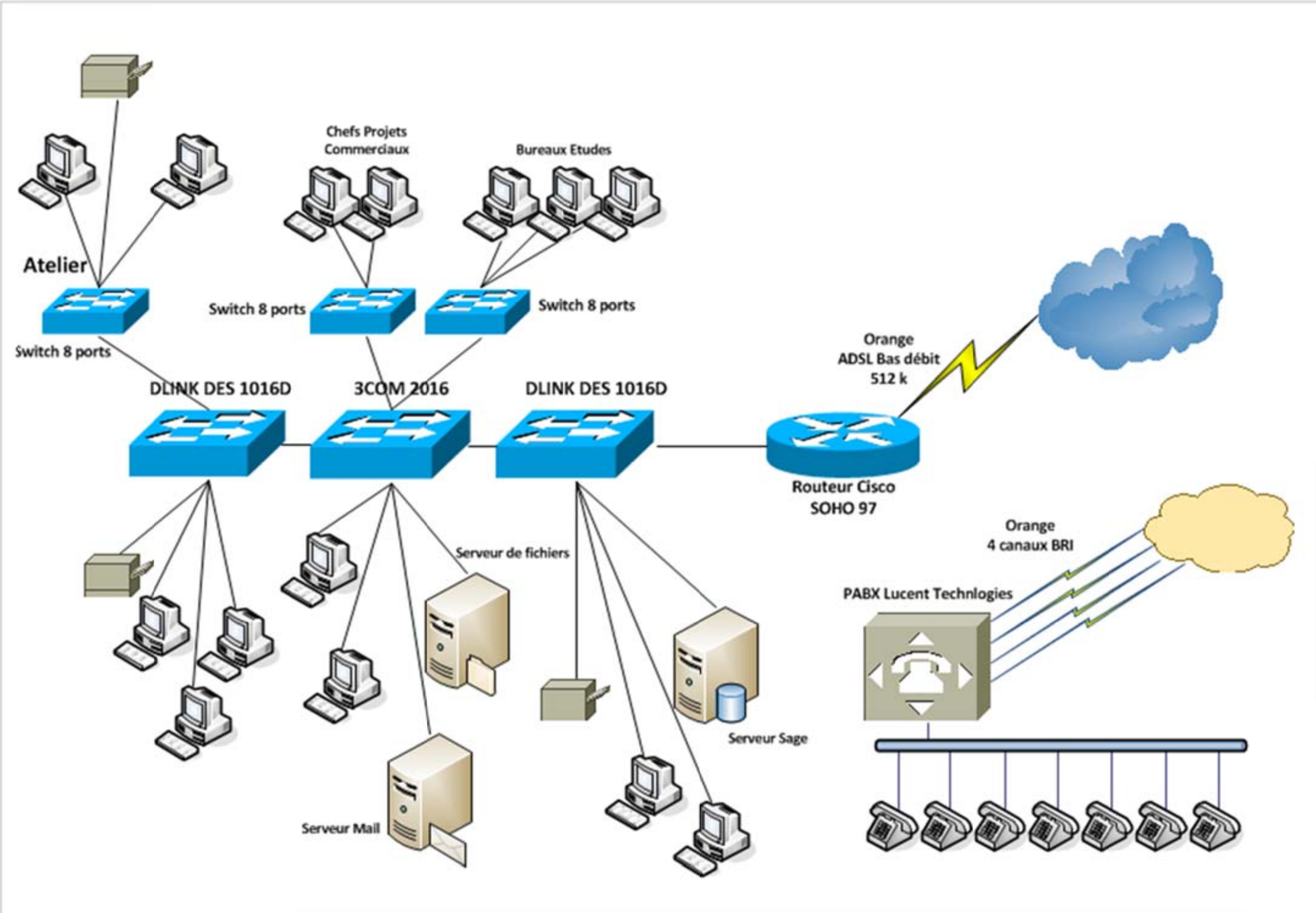
Oléane Open 3020 IP/ADSL bas débit (512k)

Nom de domaine pack eloy.fr

<u>Note :</u> il a été très difficile de pouvoir configurer les différents périphériques en ayant un DNS public gérer par un tiers. Oléane ne fonctionne qu'avec des envois de FAX, et encore, à ce jour, tous n'est pas réglé.



2.4 Topologie de la société Eloy



V. Analyse des ressources informatiques

1. Détection et cartographie

Divers outils ont été utilisés tels que DUDE ou NMAP pour se faire un aperçu du réseau.

Nous avons aussi utilisé WhatsUp Gold, qui avait été traité en mini-projet par Mr JAZAT Jérôme.

WhatsUp Gold est une solution puissante pour surveiller les réseaux et les applications. Le programme fournit aux directions informatiques des données réseaux facilement convertibles en informations métiers et en paramètres sur lesquels on peut agir.

En surveillant de façon proactive tous les périphériques et services critiques du réseau, WhatsUp réduit les délais d'interruption à la fois dommageables aux activités, frustrants et coûteux.

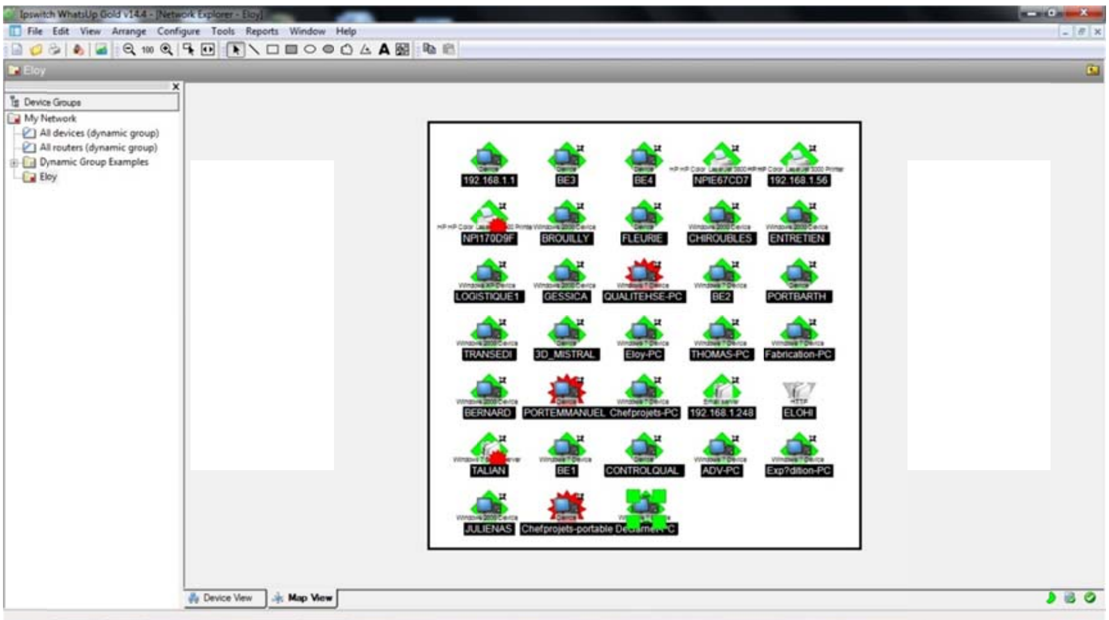
Grâce à sa toute nouvelle interface Web, WhatsUp Gold vous permet de contrôler votre infrastructure et ses applications, afin que votre travail stratégique impacte les résultats. Dans un marché à la complexité extrême, WhatsUp Gold procure un déploiement simple, une robustesse, une évolutivité, une facilité d'utilisation et un retour rapide sur investissement.

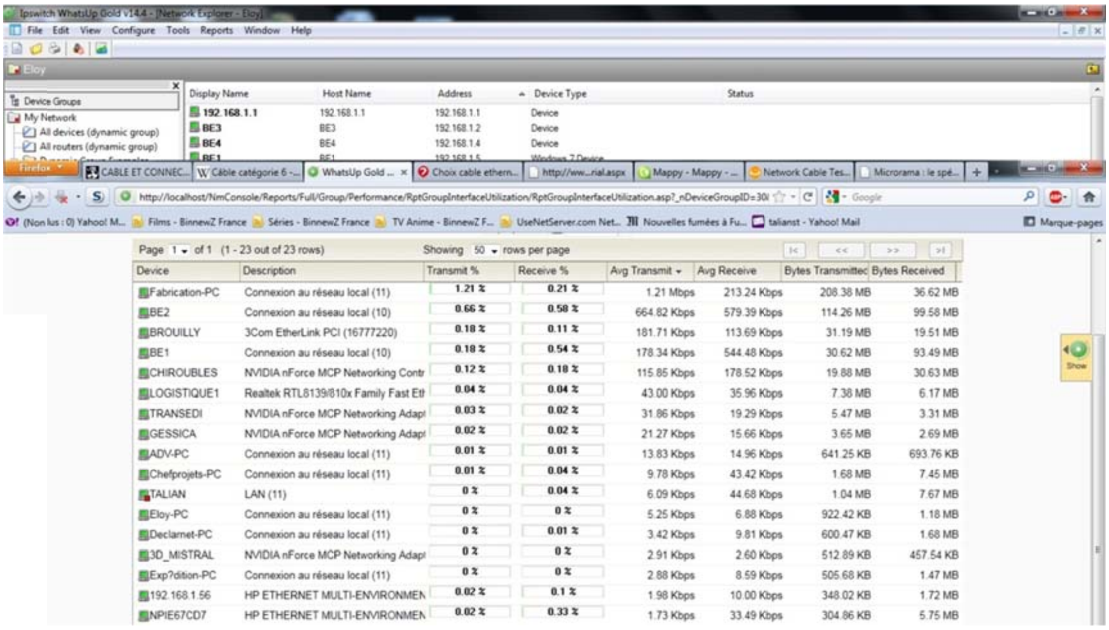
WhatsUp Gold isole les problèmes réseau et procure une connaissance fine des performances et et de la disponibilité du réseau. WhatsUp Gold:

- Découvre et cartographie tous les périphériques réseau
- Vous alerte lorsqu'un problème survient sur le réseau
- Récupère les informations du réseau au fil du temps puis génère des rapports
- Procure partout et tout le temps une surveillance fine du réseau

WhatsUp Gold est installé avec cinq moniteurs de performance qui surveillent certains types de données sur vos périphériques réseau:

- Utilisation CPU
- Utilisation disque
- Utilisation d'interface/de bande passante
- Utilisation mémoire
- Temps de latence Ping et disponibilité





La direction pensait avoir trois réseaux et voulait regrouper tous les utilisateurs sur un seul. Après analyse, seul un seul réseau était présent. Les postes informatiques étaient réparties dans trois groupes de travail et non sur trois réseaux.

La plus grande difficulté rencontrée fut de travailler sans avoir accès aux trois serveurs. En effet, la société qui était en charge de la maintenance ne voulait pas fournir les codes d'accès.

La société fonctionne sur un même réseau (192.168.1.0) mais sur plusieurs groupes de travail. Un serveur où est installé un ERP (SAGE) figure avec quatre autres hôtes dans le groupe de travail GESTION. Un serveur SAMBA gérant le partage et la sauvegarde de fichiers de la plupart des hôtes ainsi qu'un serveur Mail figure dans le groupe de travail WORKGROUP. Enfin quatre ordinateurs du bureau d'étude gérant leur propre sauvegarde et partage de fichiers figure dans le groupe de travail DESSIN.

2. Logiciels utilisés

Un remplacement du parc informatique de la société a déjà débuté et une dizaine de postes fonctionne sous Windows Seven. Mais il reste encore divers système d'exploitation en place. On peut rencontrer des Windows 2000, des XP 32bits et 64bits ainsi qu'un poste de travail sous Windows 3.1.

2.1 Solidworks

Créé en 1993 par l'éditeur américain éponyme, SolidWorks a été acheté le 24 juin 1997 par la société Dassault Systèmes1.

Parmi les plus grandes organisations utilisant SolidWorks, on peut citer Michelin, AREVA, Patek Philippe, Mega Bloks, Axiome, ME2C, SACMO, Le Boulch, Robert Renaud et le Ministère de l'Éducation nationale français

SolidWorks est un modeleur 3D utilisant la conception paramétrique. Il génère 3 types de fichiers relatifs à trois concepts de base : la pièce, l'assemblage et la mise en plan. Ces fichiers sont en relation. Toute modification à quelque niveau que ce soit est répercutée vers tous les fichiers concernés.

Un dossier complet contenant l'ensemble des relatifs à un même système constitue une maquette numérique. De nombreux logiciels viennent compléter l'éditeur SolidWorks. Des utilitaires orientés métiers (tôlerie, bois, BTP...), mais aussi des applications de simulation mécanique ou d'image de synthèse travaillent à partir des éléments de la maquette virtuelle.

2.2 Gessica

Gessica est un progiciel pour la gestion d'instruments de mesure et d'assistance à l'étalonnage.

Cetim Gessica est un logiciel adapté à toute entreprise qui veut gérer son parc d'instruments de mesure et maîtriser ses coûts d'étalonnage.
Il s'adresse généralement aux services métrologie et Qualité et, du fait de sa convivialité, il peut être utilisé par toute personne ayant besoin d'avoir accès aux données d'un instrument.

Il a été étudié pour répondre à divers besoins qui sont :

- Spécifier précisément vos moyens de mesure (identification, désignation, affectation, etc...)
- Planifier les interventions avec signalisation des retards
- Gérer les procédures avec l'association de documents sous environnement Windows
- Éditer des constats, des listings, des étiquettes
- Faire des recherches multicritères dans la base de données
- Optimiser la périodicité des étalonnages

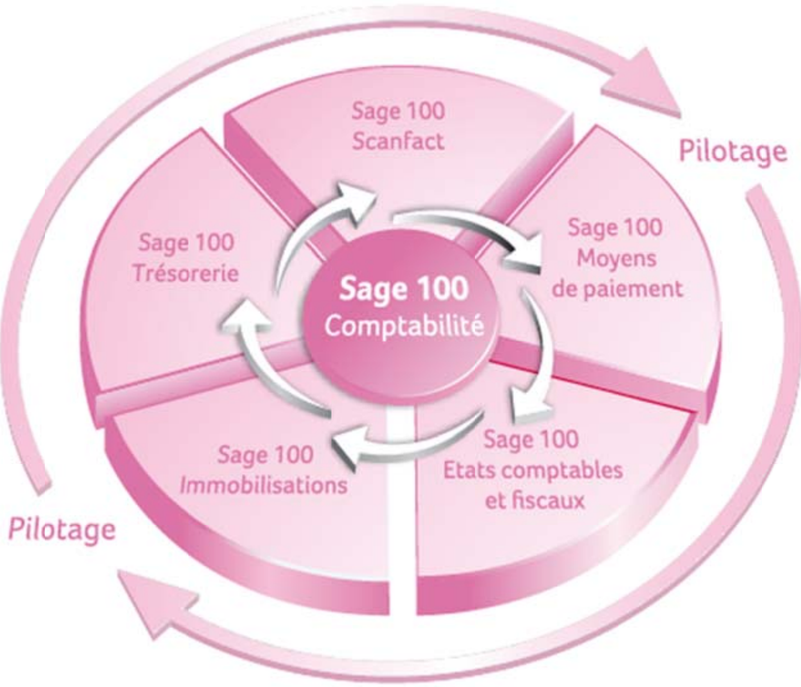
2.3 Sage 100

2.3.1 Comptabilité

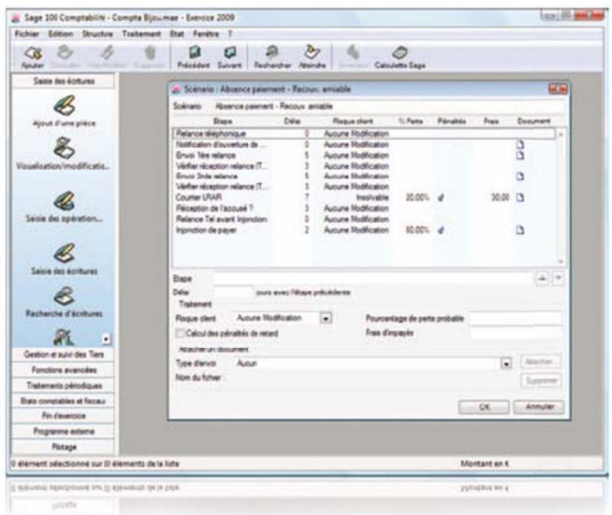
Sage 100 propose l'ensemble des éléments constitutifs d'une gestion comptable et financière efficiente : gestion de la comptabilité, du recouvrement, de la trésorerie, des immobilisations et des moyens de paiement. Bien plus encore, des outils d'aide à la décision et la toute dernière solution de dématérialisation de factures, Sage 100 Scanfact, en font un véritable centre de pilotage des données de l'entreprise axé sur le contrôle et l'analyse d'indicateurs clés dans une optique d'amélioration de la productivité.

Sage 100 Comptabilité offre par ailleurs la simplicité d'une base de données commune aux différents modules comptables et financiers, une grande interactivité avec votre environnement bureautique et la fluidité de la communication avec l'écosystème de l'entreprise, notamment via sa solution d'EDI fiscal.

La tenue rigoureuse de la comptabilité (générale, auxiliaire, analytique et budgétaire) est un besoin essentiel pour



toute entreprise. Compatible aux normes IAS/IFRS, Sage 100 Comptabilité apporte une réponse métier adaptée à vos attentes grâce à son ouverture, sa richesse fonctionnelle et sa performance : rapprochement automatique, relance clients, lettrage en euros et devises avec équilibrage automatique, gestion des écarts de change, TVA sur les encaissements, intégration des relevés de banque.

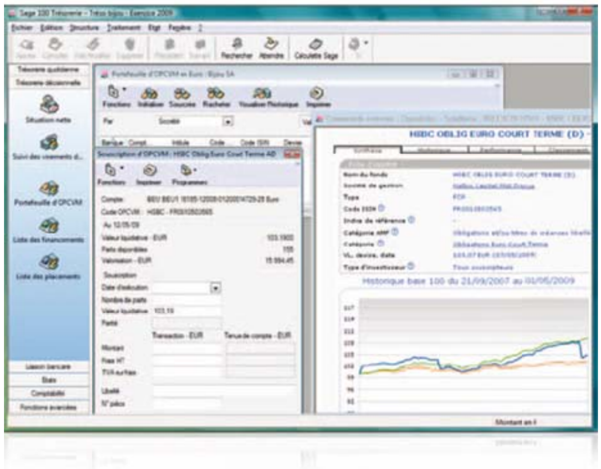


Justification de la comptabilité, respect des obligations légales, suivi de l'activité et de la rentabilité, maîtrise des équilibres financiers, Sage 100 Comptabilité vous permet d'aller plus loin dans la gestion de votre activité et vous apporte une réponse adaptée à votre métier.

Dans sa dernière édition, Sage 100 Comptabilité innove encore en intégrant la première offre pour la gestion du recouvrement des créances clients à destination des PME. Véritable outil de crédit management, Sage 100 Comptabilité fournit à l'utilisateur un processus de recouvrement simple et progressif, basé sur une succession d'étapes et un jeu d'alertes, le tout facilitant une relance clients efficace.

2.3.2 *Trésorerie*

L'actualité économique nous le montre chaque jour, la gestion de la trésorerie à un impact déterminant sur le fonctionnement et la santé des PME. Dans ce contexte, Sage 100 Trésorerie apporte des réponses pragmatiques en permettant de visualiser simplement sa situation de trésorerie, de la suivre de manière prévisionnelle et enfin de gérer les placements, les financements et les virements de trésorerie.



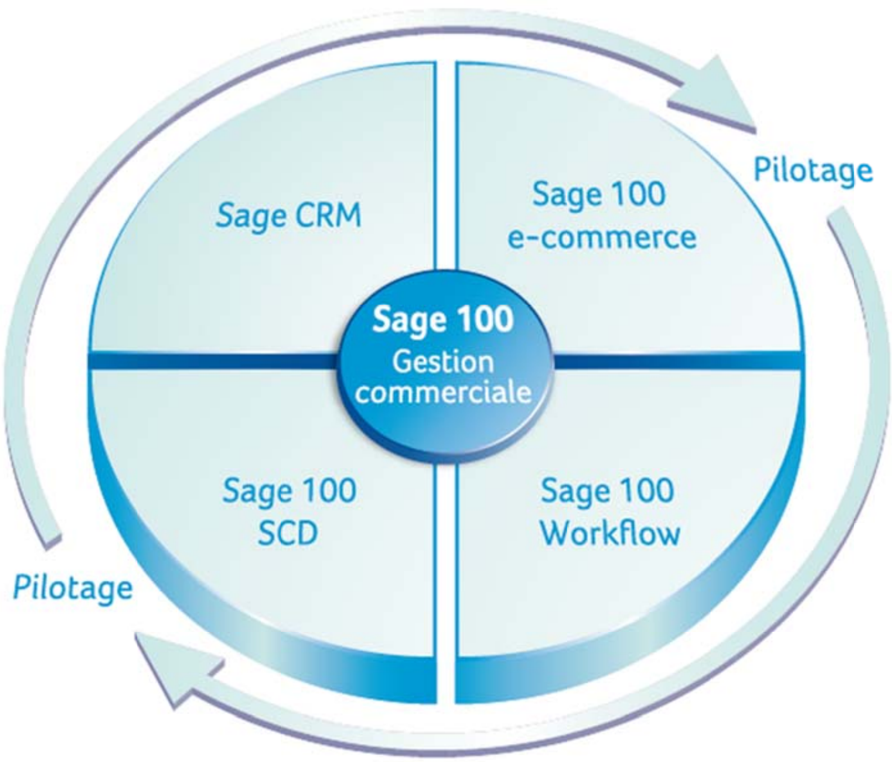
- Visualisation rapide de sa situation de trésorerie actuelle et à venir.
- Anticipation des risques.
- Amélioration rapide du cash.
- Identification des retards de paiement.
- Réduction des frais bancaires.

2.3.3 *Gestion commerciale*

La rentabilité d'une entreprise passe par l'augmentation du chiffre d'affaires et la maîtrise des coûts de gestion. Avec Sage 100 Gestion Commerciale, vous contrôlez votre activité à toutes les étapes de la chaîne commerciale :

- Ventes.
- Achats.
- Stocks.
- Fabrication.
- Prestations de services

Pour gérer, analyser et agir en cas de défaillance Sage 100 Gestion Commerciale Edition Pilotée propose de nombreux indicateurs clés. Selon votre métier (gestionnaire de stock, directeur commercial, responsable de fabrication, etc.), vous consultez des statistiques relatives aux stocks, achats, ventes, fabrication, services ou créez des scénarii de performance grâce au simulateur de chiffre d'affaires.



Maîtrise de l’intégralité de la chaîne commerciale

Gestion complète du cycle de vente

La gestion efficace de l’activité commerciale repose sur l’accélération des étapes de la vente : devis, commande, livraison et facturation. Le traitement rapide des devis contribue à transformer vos prospects en clients créateurs de valeur et augmente votre portefeuille d’activité. Accessible à partir de Sage 100 Gestion Commerciale, de nombreux assistants vous permettent de construire votre base commerciale simplement (structuration du catalogue d’articles, tarifs, comptabilité clients, etc.).

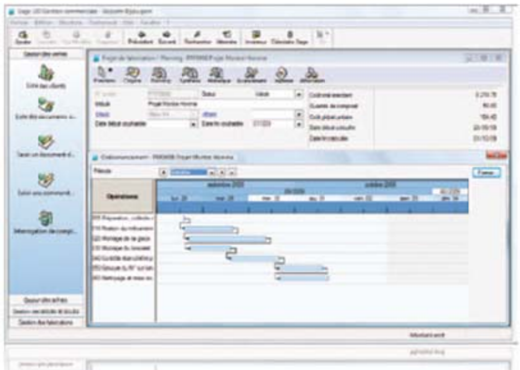
Contrôle des achats et approvisionnements

Acheter au bon prix, négocier la marge fournisseur et obtenir les meilleurs tarifs permet de proposer des prix compétitifs à vos clients et d’augmenter votre rentabilité. Avec Sage 100 Gestion Commerciale, vous pouvez, à tout moment, consulter la liste de vos fournisseurs et disposer de toutes les informations nécessaires à la prise de décision.

Maîtrise des stocks

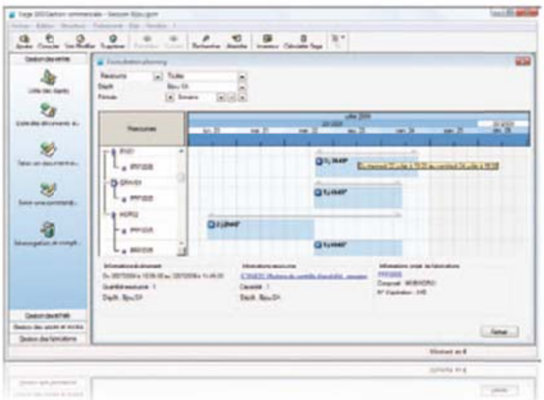
Les marchandises sont contrôlées quelle que soit leur provenance (fournisseur, atelier de fabrication), puis stockées (CMUP, LIFO, FIFO, N°lot, N°de série) et prêtes à être livrées selon les priorités clients.De nombreux indicateurs clés vous permettent également de contrôler le niveau de stocks (rupture, invendus).

Contrôle de la fabrication



Adaptée aux entreprises du secteur industriel (assemblage, sous-traitants, fabricants), notre solution permet de recenser les composants et ressources mobilisés, d’ordonner la fabrication, de contrôler le coût de revient, et de respecter les délais de fabrication afin d’honorer les commandes. Pour cela, vous accédez à de nombreux indicateurs clés.

Organisation des prestations de service



Quelle que soit l’activité (location de matériel, services aux entreprises, consulting, formation), vous réservez les ressources nécessaires à la réalisation de vos prestations de services, gérez les tâches dans l’outil de planning de la gestion commerciale et facturez vos prestations. Grâce à de nombreux indicateurs clés et tableaux de bord, vous disposez d’une vision précise de votre activité.

VI. Conclusion de l'audit

La baie de brassage n'est pas fermé à clef et situé dans un couloir proche de l'atelier, elle n'est pas à l'abri des sources de poussières diverses pouvant polluer l'air ambiant. Il n'existe pas d'alimentation électrique secourue par onduleur « on line » reliée directement au tableau général.

Les panneaux de brassage, ainsi que les divers raccordements effectués par les employés ne sont pas aux normes. Aucun étiquetage présent.

Un total de six commutateurs, le tout en cascade créent des nœuds au niveau du réseau. Tous les commutateurs étant des 100M, le serveur de fichiers est lui-même relié à un port 100M. De gros ralentissements sont constatés par les employés surtout que la majorité des fichiers de travail se trouve sur le serveur.

L'infrastructure du câblage du rez-de-chaussée doit être repensée.

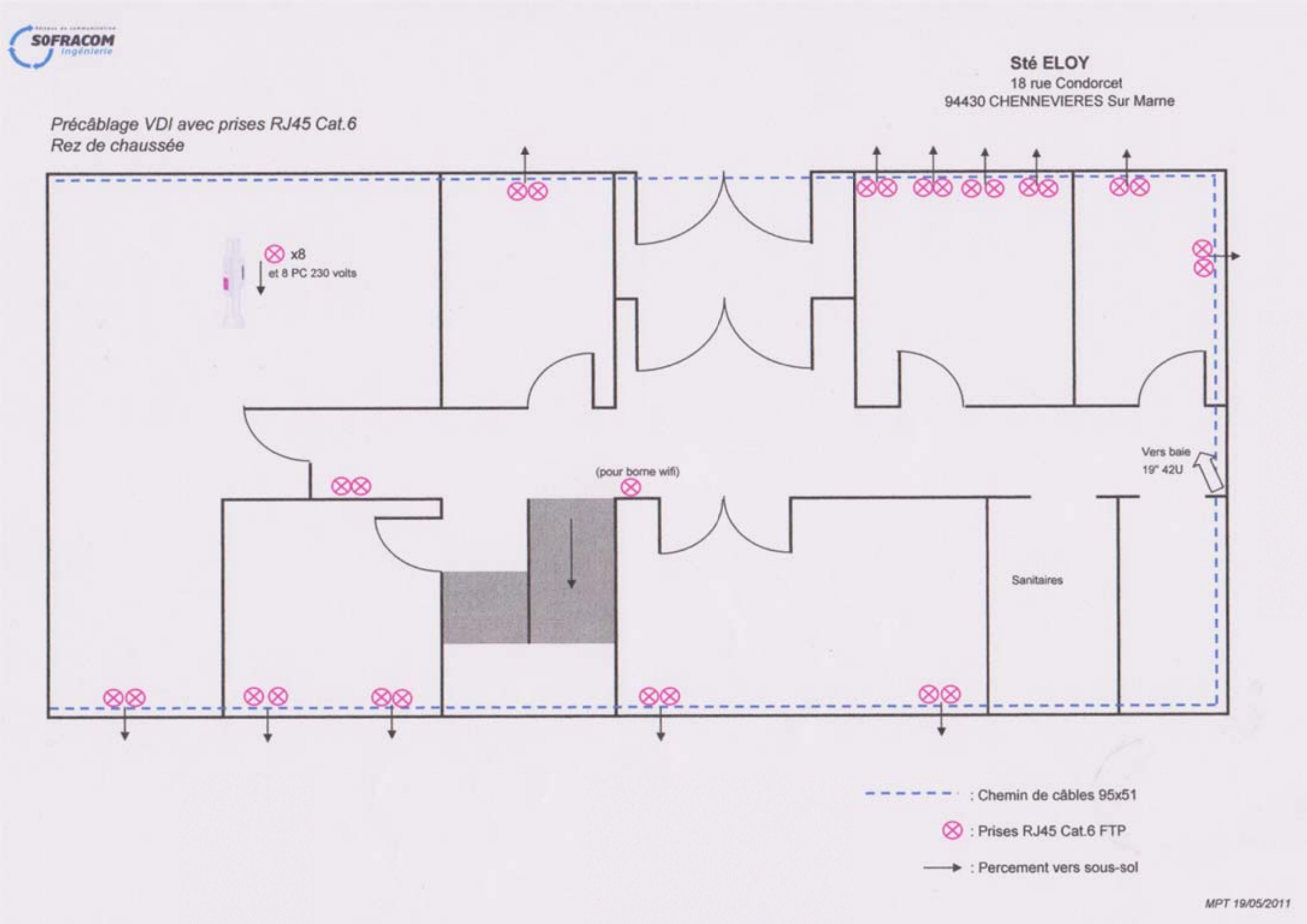
Le serveur de fichier n'est pas assez aéré et doit trouver un autre emplacement.

Il n'existe aucune protection informatique dans la société. Un tiers des postes détiennent un antivirus, aucun firewall matériel ou logiciel n'existe.

Les problèmes de lenteur au niveau de l'envoi de mails en interne viennent du fait que le serveur de messagerie ne joue pas intégralement son rôle. En effet, il est simplement chargé de récupérer les mails sur le serveur d'orange et n'effectue aucune transmission. Les postes clients pointent tous sur le serveur SMTP d'orange. Le prestataire de service sous contrat avec la société facture une sauvegarde des mails sur le serveur couplée à un filtre anti-spam.

VII. Installation d'une solution wifi

Pour combler les lacunes du rez-de-chaussée au niveau câblage, plusieurs solutions ont été étudiées. Différentes sociétés ont été contactés et seul une à retenu notre attention.



Un devis a été effectués pour le câblage du rez-de-chaussée, pour le déplacement de baie de brassage à l'étage, ainsi que la création d'un câblage VDI pour les ateliers avec passage d'un câble fibre optique depuis la nouvelle baie de brassage au 1er étage.

Comprenant qu'il n'était pas envisageable d'effectuer de tels travaux dans l'immédiat. Les devis ont été réalisés pour de futures évolutions de la société. En effet, un emplacement a été trouvé à l'étage pour un futur local technique. En attendant le nouveau serveur y trouvera sa place.

Ne pouvant pas laisser les raccordements du rez-de-chaussée dans un tel état, il a été décidé de recourir dans l'immédiat à une solution wifi.

Notre choix s'est porté sur un point d'accès CISCO Aironet 1142N autonome.

1. Configuration de l'AP 1142N

1.1 Introduction

Le Wi-Fi est de nos jours de plus en plus présents dans les entreprises. Son implémentation se fait souvent par étape en déployant le réseau sans-fil de manière progressive dans les locaux de l'entreprise. Dans certains cas, les bornes ne sont pas toutes achetées en même temps. L'entreprise peut donc se retrouver avec un équipement hétéroclite. Il est alors nécessaire de pouvoir rendre ces équipements inter opérables avec une transparence complète au niveau des utilisateurs. Le Wi-Fi a de nombreux avantages :

- Le déplacement libre du PC, des ordinateurs portables et des PDA.
- La possibilité de relier plusieurs machines ou périphériques en réseau.
- Le partage d'applications (connexion ADSL, imprimantes, visioconférence…).
- La diminution des frais de câblages

1.2 Configuration

Avant de configurer son AP, il faut déterminer ou recueillir les informations suivantes :

- Un nom de système
- Un SSID (Service Set Identifier) pour le réseau radio
- Une adresse IP unique (si l'AP n'utilise pas le serveur DHCP)
- Une passerelle par défaut et masque de sous réseau (si l'AP n'est pas sur le même sous réseau que le PC d'administration)
- Un nom de communauté SNMP et le fichier SNMP attribué (si SNMP est utilisé)

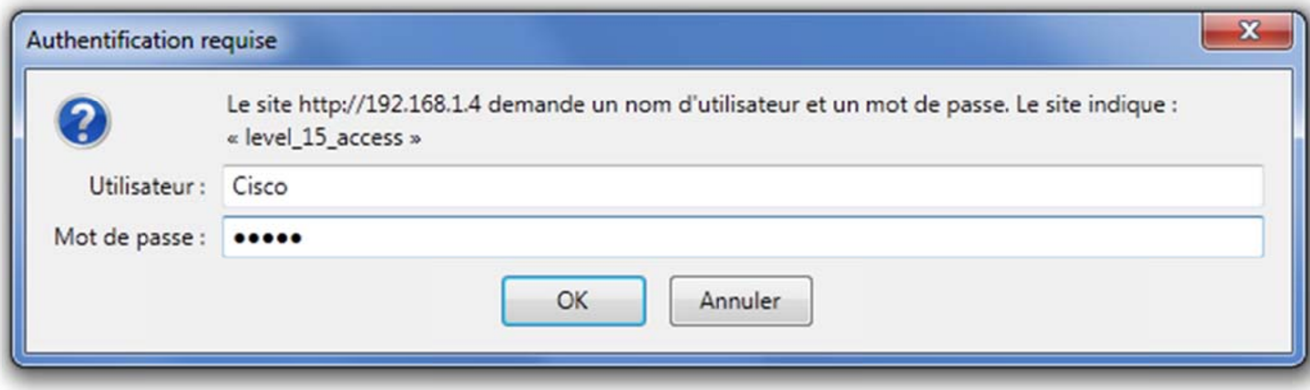
Il existe 2 interfaces permettant de configurer son AP, Pour administrer l'AP, le nom d'utilisateur par défaut est « Cisco » avec le mot de passe « Cisco » :

- Page d'accueil de la CLI (command-line interface), connexion console ou telnet :
- Page d'accueil de l'interface http (recommandé) – IOS GUI (Graphical User Interface), adresse par défaut http://10.0.0.1

Pour passer en mode privilégié sur l'AP, le mot de passe par défaut est : Cisco

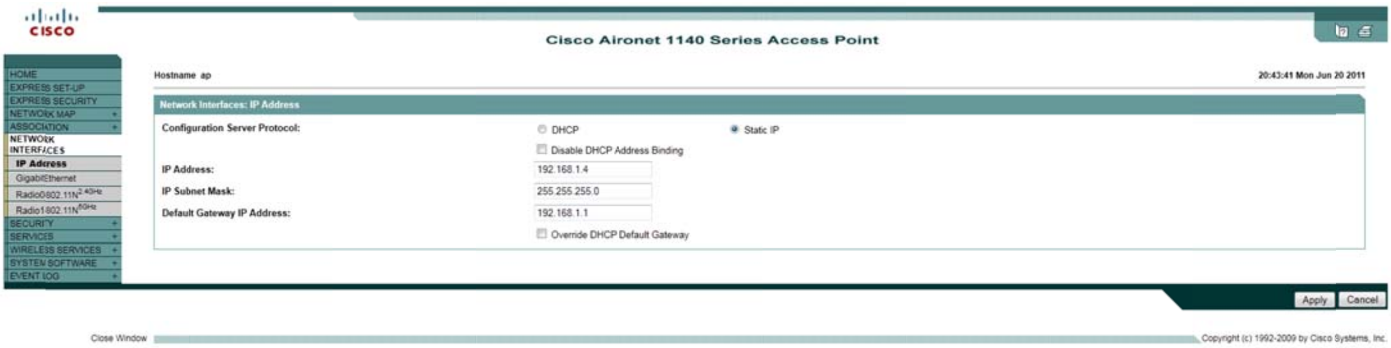
Ici nous resterons en mode Web, mais les commandes existent en CLI et sont similaires à tous les matériels Cisco

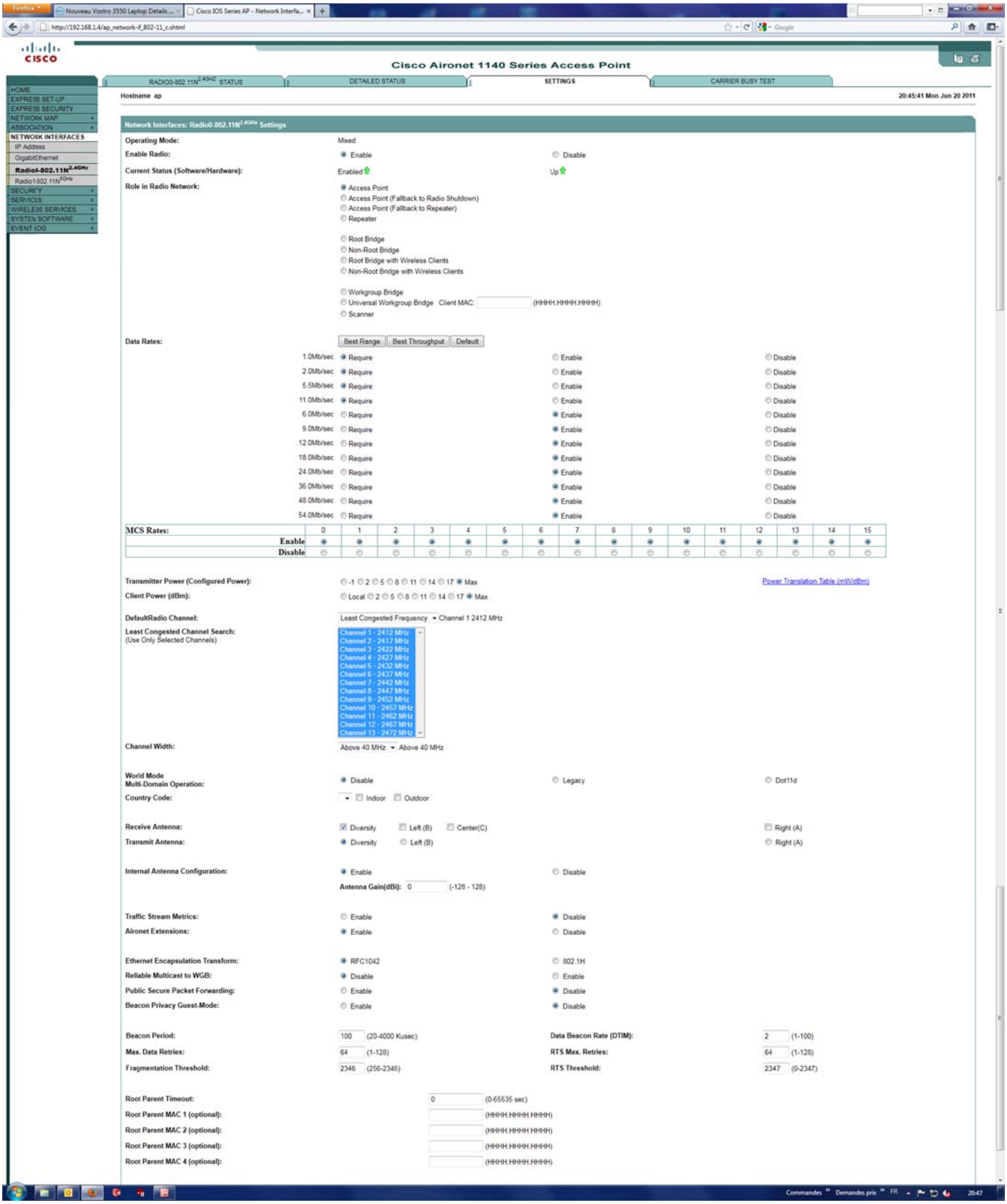
Nous allons commencer tout d'abord par quelques paramètres de base sur la page Express Setup :

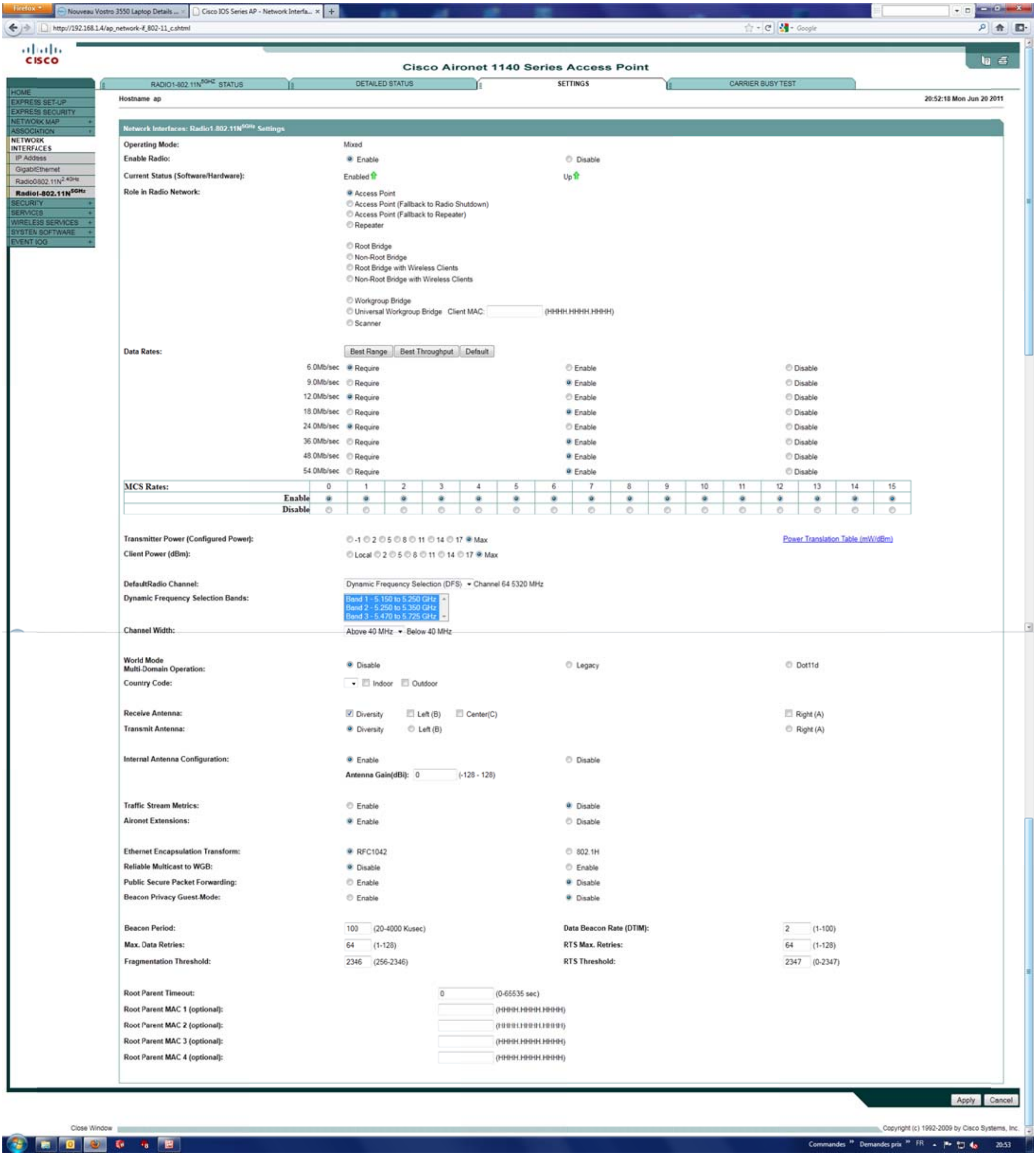


Nous retrouvons le paramétrage de l'adressage IP dans cette page

Il faut savoir que par défaut, la borne se met en 10.0.0.1 et fait un DHCP pour les clients. Dans le cadre d'un petit réseau domestique par exemple. Par contre il y a également la possibilité que la borne prenne une IP sur une plage définie par l'administrateur afin de rejoindre un LAN existant. Il faut toujours garder à l'esprit que ce type de borne n'est pas routeur, elle fonctionne au niveau 2 du modèle OSI et donc ne pourra pas traiter deux réseaux différents. La configuration basique est surtout sur l'interface Radio, nous allons utiliser quelques options de cette page (Network Interfaces, Radio0)




Cisco Aironet 1140 Series Access Point
RADIO0-802.11N2.4GHz STATUS
DETAILED STATUS
SETTINGS
CARRIER BUSY TEST
HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP
ASSOCIATION
NETWORK INTERFACES
IP Address
GigabitEthernet
Radio0-802.11N2.4GHz
Radio1-802.11N5GHz
SECURITY
SERVICES
WIRELESS SERVICES
SYSTEM SOFTWARE
EVENT LOG
Hostname ap
20:45:41 Mon Jun 20 2011
Network Interfaces: Radio0-802.11N2.4GHz Settings
Operating Mode: Mixed
Enable Radio: Enable Disable
Current Status (Software/Hardware): Enabled Up
Role in Radio Network:
Access Point
Access Point (Fallback to Radio Shutdown)
Access Point (Fallback to Repeater)
Repeater
Root Bridge
Non-Root Bridge
Root Bridge with Wireless Clients
Non-Root Bridge with Wireless Clients
Workgroup Bridge
Universal Workgroup Bridge Client MAC: (HHHH.HHHH.HHHH)
Scanner
Data Rates: Best Range Best Throughput Default
1.0Mb/sec Require Enable Disable
2.0Mb/sec Require Enable Disable
5.5Mb/sec Require Enable Disable
11.0Mb/sec Require Enable Disable
6.0Mb/sec Require Enable Disable
9.0Mb/sec Require Enable Disable
12.0Mb/sec Require Enable Disable
18.0Mb/sec Require Enable Disable
24.0Mb/sec Require Enable Disable
36.0Mb/sec Require Enable Disable
48.0Mb/sec Require Enable Disable
54.0Mb/sec Require Enable Disable
MCS Rates: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
Enable
Disable
Transmitter Power (Configured Power): -1 2 5 8 11 14 17 Max
Power Translation Table (mW/dBm)
Client Power (dBm): Local 2 5 8 11 14 17 Max
DefaultRadio Channel: Least Congested Frequency Channel 1 2412 MHz
Least Congested Channel Search: (Use Only Selected Channels)
Channel 1 - 2412 MHz
Channel 2 - 2417 MHz
Channel 3 - 2422 MHz
Channel 4 - 2427 MHz
Channel 5 - 2432 MHz
Channel 6 - 2437 MHz
Channel 7 - 2442 MHz
Channel 8 - 2447 MHz
Channel 9 - 2452 MHz
Channel 10 - 2457 MHz
Channel 11 - 2462 MHz
Channel 12 - 2467 MHz
Channel 13 - 2472 MHz
Channel Width: Above 40 MHz Above 40 MHz
World Mode Multi-Domain Operation: Disable Legacy Dot11d
Country Code: Indoor Outdoor
Receive Antenna: Diversity Left (B) Center(C) Right (A)
Transmit Antenna: Diversity Left (B) Right (A)
Internal Antenna Configuration: Enable Disable
Antenna Gain(dBi): 0 (-128 - 128)
Traffic Stream Metrics: Enable Disable
Aironet Extensions: Enable Disable
Ethernet Encapsulation Transform: RFC1042 802.1H
Reliable Multicast to WGB: Disable Enable
Public Secure Packet Forwarding: Enable Disable
Beacon Privacy Guest-Mode: Enable Disable
Beacon Period: 100 (20-4000 Kusec)
Data Beacon Rate (DTIM): 2 (1-100)
Max. Data Retries: 64 (1-128)
RTS Max. Retries: 64 (1-128)
Fragmentation Threshold: 2346 (256-2346)
RTS Threshold: 2347 (0-2347)
Root Parent Timeout: 0 (0-65535 sec)
Root Parent MAC 1 (optional): (HHHH.HHHH.HHHH)
Root Parent MAC 2 (optional): (HHHH.HHHH.HHHH)
Root Parent MAC 3 (optional): (HHHH.HHHH.HHHH)
Root Parent MAC 4 (optional): (HHHH.HHHH.HHHH)



http://192.168.1.4/ap_network-if_802-11_c.shtml
Cisco Aironet 1140 Series Access Point
RADIO1-802.11N5GHZ STATUS
DETAILED STATUS
SETTINGS
CARRIER BUSY TEST
HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP
ASSOCIATION
NETWORK INTERFACES
IP Address
GigabitEthernet
Radio0-802.11N2.4GHz
Radio1-802.11N5GHz
SECURITY
SERVICES
WIRELESS SERVICES
SYSTEM SOFTWARE
EVENT LOG
Hostname ap
20:52:18 Mon Jun 20 2011
Network Interfaces: Radio1-802.11N5GHz Settings
Operating Mode:
Mixed
Enable Radio:
Enable
Disable
Current Status (Software/Hardware):
Enabled
Up
Role in Radio Network:
Access Point
Access Point (Fallback to Radio Shutdown)
Access Point (Fallback to Repeater)
Repeater
Root Bridge
Non-Root Bridge
Root Bridge with Wireless Clients
Non-Root Bridge with Wireless Clients
Workgroup Bridge
Universal Workgroup Bridge
Client MAC:
(HHHH.HHHH.HHHH)
Scanner
Data Rates:
Best Range
Best Throughput
Default
6.0Mb/sec
9.0Mb/sec
12.0Mb/sec
18.0Mb/sec
24.0Mb/sec
36.0Mb/sec
48.0Mb/sec
54.0Mb/sec
Require
Enable
Disable
MCS Rates:
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
Enable
Disable
Transmitter Power (Configured Power):
-1 2 5 8 11 14 17 Max
Power Translation Table (mW/dBm)
Client Power (dBm):
Local 2 5 8 11 14 17 Max
DefaultRadio Channel:
Dynamic Frequency Selection (DFS)
Channel 64 5320 MHz
Dynamic Frequency Selection Bands:
Band 1 - 5.150 to 5.250 GHz
Band 2 - 5.250 to 5.350 GHz
Band 3 - 5.470 to 5.725 GHz
Channel Width:
Above 40 MHz
Below 40 MHz
World Mode
Multi-Domain Operation:
Disable
Legacy
Dot11d
Country Code:
Indoor
Outdoor
Receive Antenna:
Diversity
Left (B)
Center(C)
Right (A)
Transmit Antenna:
Diversity
Left (B)
Right (A)
Internal Antenna Configuration:
Enable
Disable
Antenna Gain(dBi):
0
(-128 - 128)
Traffic Stream Metrics:
Enable
Disable
Aironet Extensions:
Enable
Disable
Ethernet Encapsulation Transform:
RFC1042
802.1H
Reliable Multicast to WGB:
Disable
Enable
Public Secure Packet Forwarding:
Enable
Disable
Beacon Privacy Guest-Mode:
Enable
Disable
Beacon Period:
100
(20-4000 Kusec)
Data Beacon Rate (DTIM):
2
(1-100)
Max. Data Retries:
64
(1-128)
RTS Max. Retries:
64
(1-128)
Fragmentation Threshold:
2346
(256-2346)
RTS Threshold:
2347
(0-2347)
Root Parent Timeout:
0
(0-65535 sec)
Root Parent MAC 1 (optional):
(HHHH.HHHH.HHHH)
Root Parent MAC 2 (optional):
(HHHH.HHHH.HHHH)
Root Parent MAC 3 (optional):
(HHHH.HHHH.HHHH)
Root Parent MAC 4 (optional):
(HHHH.HHHH.HHHH)
Apply
Cancel
Close Window
Copyright (c) 1992-2009 by Cisco Systems, Inc.

Ci-dessus, les réglages sont par défaut. Il convient toutefois de vérifier 2 paramètres, le débit et les canaux. Pour le débit (Data Rates) toutes les vitesses sont listées, on peut les rendre obligatoires (Require), simplement les activer (Enable) ou les désactiver (Disable).

Explication des boutons :

- Best Range : La meilleure portée, les plus petites vitesses seront sélectionnées afin que le client puisse capter le plus loin possible. Ce choix de la portée se fera au détriment du débit.
- Best Throughput : Le meilleur débit. Les plus grandes vitesses seront sélectionnées afin que les clients aient un accès rapide. Ce choix du débit se fera au détriment de la portée.
- Default : Laisse les paramètres en réglage d'usine.

Pour notre configuration basique, les réglages par défaut sont satisfaisants.

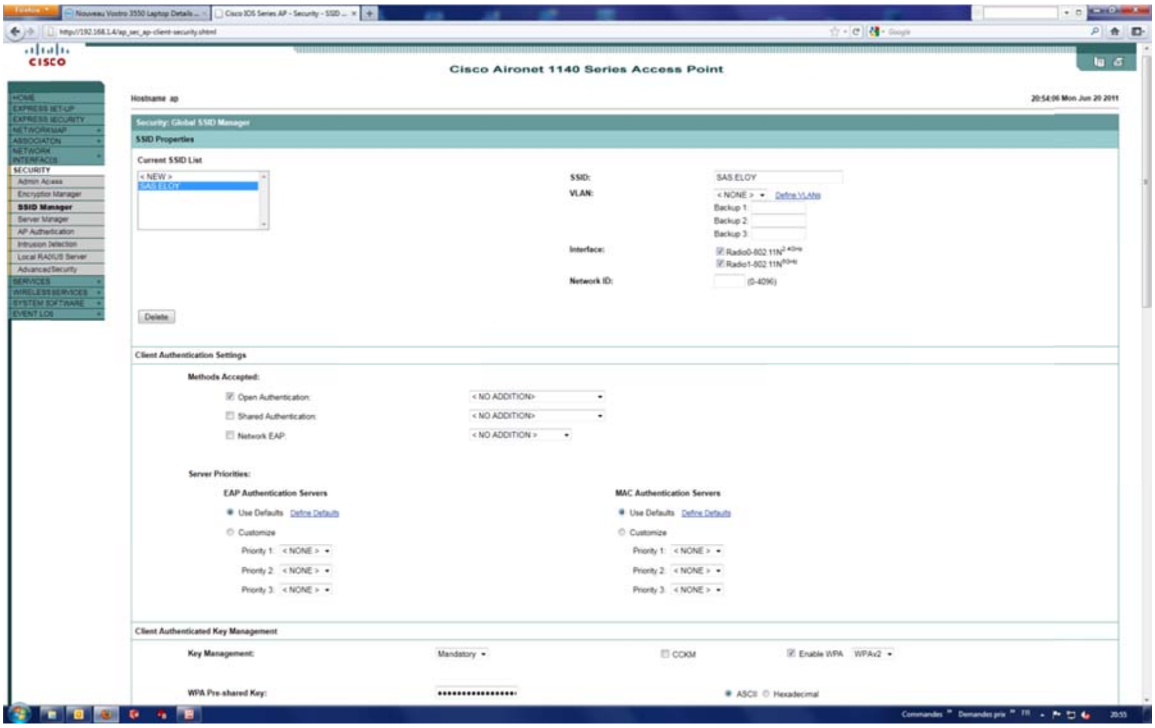
Channel :
La sélection du canal d'émission est très importante, aujourd'hui de nombreux points d'accès sont présents.
Le mieux est tout d'abord de vérifier la bande de fréquences avec un PC WIFI équipé par exemple avec netstumbler (http://www.netstumbler.com/).

Il y a 13 Channel autorisés en France, ce qui signifie que le choix est assez limité.
Astuce : La technologie utilisée répand le signal sur plusieurs canaux alentours. Il est fortement conseillé de choisir un canal libre d'au moins 3 à 4 canaux autour (Exemple Canal 1, 5, 9 et 13) sont parfaitement espacés pour ne pas avoir de perturbations)

La configuration peut également se faire avec le « Least Congested Frequency », la borne va alors scanner les canaux pour sélectionner le moins chargé. Cette option permet que le choix du canal soit dynamique même si de nouveaux AP environnants apparaissent.

Au niveau du Channel Width : les deux radios sont configurés à 40 mhz

Notre configuration Radio est terminée.



La borne est configurée en WPA2 Personal avec une Preshared Key.

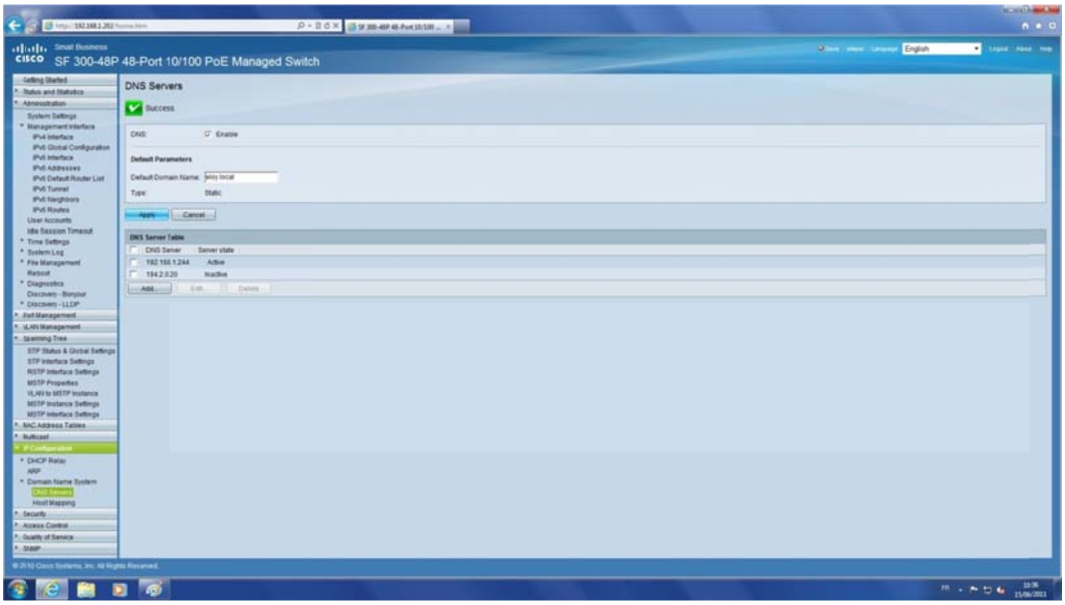
1.3 Configuration CLI de l'AP

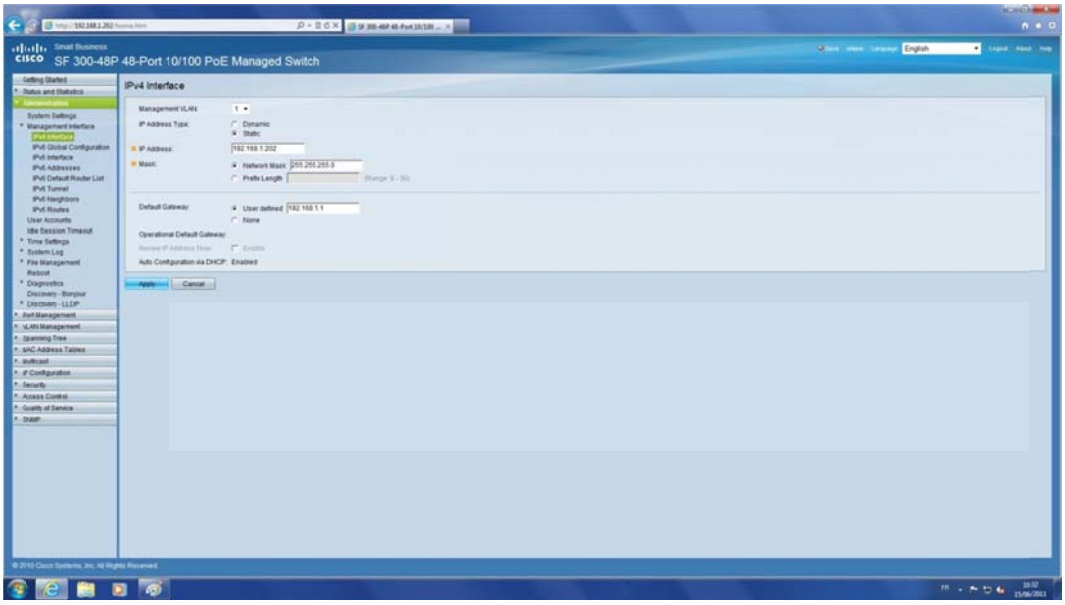
```
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname ap
enable secret 5 $1$SFti$Ny5/.6KmXTcYc1wZHY5en.
no aaa new-model
clock timezone +0200 2
dot11 syslog
dot11 ssid SAS.ELOY
   authentication open
   authentication key-management wpa version 2
   wpa-psk ascii 7 11080300050612190D253B353B3733251B0D1D
dot11 network-map
username Cisco password 7 13261E010803
bridge irb
interface Dot11Radio0
 bandwidth 300000
 no ip address
 no ip route-cache
 encryption mode ciphers aes-ccm
 ssid SAS.ELOY
 antenna gain 0
 channel width 40-above
 channel 2412
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
interface Dot11Radio1
 no ip address
 no ip route-cache
 encryption mode ciphers aes-ccm
 ssid SAS.ELOY
 antenna gain 0
 no dfs band block
 channel width 40-above
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
```

```
 bridge-group 1 spanning-disable
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex full
 speed auto
 no keepalive
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
interface BVI1
 bandwidth 600000
 ip address 192.168.1.4 255.255.255.0
 no ip route-cache
ip default-gateway 192.168.1.1
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
bridge 1 route ip
line con 0
 logging synchronous
line vty 0 4
 password 7 052B3C0A3358574F150A0E43595F50
 login
sntp server 192.168.1.244
sntp broadcast client
end
```

2. Commutateur Cisco Small Business SF 300-48P

Pour relier la borne au réseau, un commutateur Cisco Small Business SF 300-48P a été acheté. Il nous a permis de remplacer les trois commutateurs de la baie de brassage, de disposer de quatre ports gigabits nécessaire pour l'accès au serveur et aussi de disposer de ports POE pour l'alimentation du point d'accès.





VIII. Installation du nouveau serveur

Le désire de la société est de regrouper tous les services (SAGE, mail et serveur de fichier) sur un même serveur.

Le serveur choisi fut un DELL PowerEdge T610 châssis en rack pour jusqu'à 8x disques durs 3,5 pouces

- Processeur Intel Xeon E5620 (2,40GHz, 4C, 12Mo de mémoire cache, 5,86 GT/s QPI, 80W TDP, Turbo, HT), DDR3-1066MHz
- T610 EMEA1 Livraison Doc Pas de cordon d'alimentation (Anglais/Français/Allemand/Espagnol/Russe/Hébreu)
- 16Go de mémoire par 2 CPU (8x UDIMM 2Go Single Rank) 1333MHz
- Additional Intel Xeon E5620 Processor (2.40GHz, 4C, 12M Cache, 5.86 GT/s QPI, 80W TDP, Turbo, HT)
- 3 Disques durs Hot Plug 300Go SAS 6Gbit/s 15000tr/min 3,5 pouces
- PERC H700 Contrôleur RAID intégré, 512Mo de mémoire cache
- 16X DVD+/-RW Lecteur avec câble SATA
- 2 Européen 220V Cordon d'alimentation de rechange
- Sortie élevée Redondant Bloc d'alimentation (2 PSU) 870W, Paramètre BIOS de performances
- Onduleur Dell, Rack, 1920W, 2U, 230V, Pack Câble inclus

- Intégré Broadcom GbE Réseau local sur carte mère avec TOE
- iDRAC6 Express
- Microsoft SBS 2011, Standard Edition, French, Including 5 CALs, Factory Installed
- 5 x 5 licences d'accès client utilisateur pour SBS 2011 Édition standard
- PE T610 Documentation Electronic System et DVD OpenManage
- You have chosen not to take the Dell PowerEdge installation service
- Rails de rack coulissants prêts avec Bras de gestion de câbles pour configuration de rack
- C3 MSS R5 pour PERC 6i/H700, Min. 3 Max. 8 disques
- PowerEdge Order - France
- Base Warranty
- 3Yr Basic Warranty - Next Business Day - Minimum Warranty
- 3Yr ProSupport and Next Business Day On-Site Service
- Declined Proactive Maintenance
- Disques durs Hot Plug entièrement assemblés 500Go Near Line SAS 6Gbit/s 7200tr/min 3,5 pouces – Kit

Nous avons choisi 3 disques durs 300Go qui seront installés en raid 5 ainsi qu'un disque dur 500Go pour la sauvegarde du serveur.

Pour le système d'exploitation notre choix s'est porté sur Windows SBS 2011 pour sa convivialité.

1. Windows® Small Business Server 2011 Standard

Conçu et adapté pour les entreprises allant jusqu'à 75 utilisateurs, Windows® Small Business Server 2011 Standard (SBS 2011 Standard) vous offre la performance et de nombreuses fonctionnalités pour un coût réduit.

SBS 2011 Standard vous aide à protéger vos informations via des sauvegardes journalières automatisées et vous permet d'être plus productif en vous fournissant la plupart des fonctionnalités utilisées dans les grandes organisations : messagerie, connexion internet, intranet, accès à distance et partage de fichiers et d'imprimantes.

Vos données sécurisées et sauvegardées
SBS 2011 Standard vous permet de vous concentrer sur votre métier en vous garantissant une sauvegarde automatique locale et une restauration de toutes vos données critiques sur le serveur.

Une plateforme qui évolue avec vos besoins
SBS 2011 Standard vous permet de tirer profit d'une console performante et évolutive. Il vous est facile d'ajouter des utilisateurs, des serveurs, des applications ou de se tourner vers d'autres technologies Microsoft en fonction de vos attentes.

Travail à distance pour vos équipes en déplacement
SBS 2011 Standard vous permet de rapidement accéder à votre poste de travail à distance, vos e-mails, contacts, documents et calendrier, pour échanger avec vos intermédiaires, vendeurs ou fournisseurs de n'importe où.

1.1 Quoi de neuf par rapport à Windows® Small Business Server 2008 ?

Technologie Windows Server® 2008 R2 Standard

- Interface simple adaptée aux besoins des PME
- Suivi quotidien de l'état de santé des serveurs et postes clients via des rapports et des alertes emails
- Virtualisation optimisée (avec le complément Premium)

Installation/migration simplifiées

- Déploiement simplifié du serveur à l'aide des assistants d'installation + outils d'aide à la migration (à partir des versions 2003 de SBS et de Windows Server®)
- Finalisation de la configuration du serveur (nom de domaine Internet et messagerie, certificats, sauvegardes…)
- Déploiement simplifié des postes clients à l'aide des assistants de la console d'administration

Accès à distance plus efficace

- Nouvelle plateforme d'accès à distance simplifiée
- Accès aux dossiers partagés sur le serveur via un navigateur web

Gestion simplifiée des emails avec Exchange Server 2010 Standard SP1

- Interface Outlook® Web App (OWA), plus proche que jamais d'Office Outlook®
- Interface OWA personnalisable avec 27 thèmes par défaut
- Gestion de vos archives personnelles disponibles sur le serveur et via OWA

Collaboration en ligne optimisée, sécurisée avec SharePoint® Foundation services 2010

- Accéder et partager des documents de n'importe où sur votre PC, votre mobile via votre navigateur web
- Outils de suivi, alertes et administration intégrés à SharePoint®

Le Complément Premium pour SBS 2011

- Sous forme d'add-on, vous pouvez désormais ajouter à n'importe quel moment le Complément Premium de SBS 2011 pour faire tourner vos applications
- Le Complément Premium apporte à votre SBS, 1 licence Windows Server® 2008 R2 Standard et 1 licence SQL Server® 2008 R2 for Small Business Edition

Une base de données plus riche avec SQL Server® 2008 R2 for Small Business

- Outils de reporting et analyses plus riches et intégrés avec la suite Office
- Temps de backups réduits et réduction jusqu'à 60% de la taille des sauvegardes de données

1.2 Installation et configuration

L'installation de Windows SBS 2011 est automatisé et assez simple.

Petite subtilité par rapport à l'installation d'un Windows serveur plus ancien : pendant l'installation, il est demandé d'ajouter un compte administrateur réseau. Donc on remplit nom, prénom, nom d'utilisateur de l'administrateur ainsi que son mot de passe. Attention ce compte sera l'utilisateur qui sera l'administrateur par défaut de l'Active Directory dans SBS, le compte administrateur, en lui-même, étant désactivé. Mais il n'a pas que cette fonctionnalité, il créera en même temps le compte administrateur de restauration des services Active Directory. Donc si vous décidez à l'avenir de modifier le mot de passe de l'utilisateur qui vous sert d'administrateur par défaut de votre Active Directory, le mot de passe de restauration, lui, ne sera pas modifié.

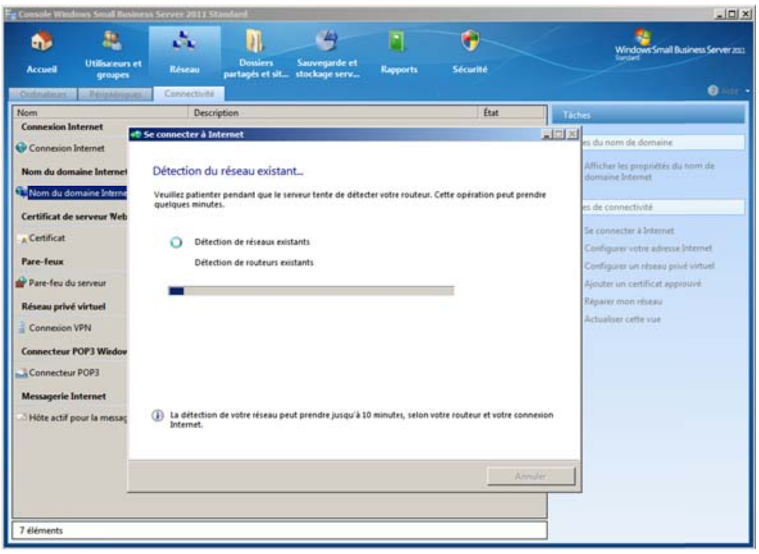
Une fois les informations fournies et qu'on clique sur suivant on ne peut plus revenir en arrière.

L'installation dure environ 45 minutes.

Ensuite on doit lancer la console d'administration et les assistants de finalisation d'installation.

1.2.1 Le premier assistant : se connecter à internet

a. Detection de serveur DHCP



Il cherche un serveur DHCP en lançant un DHCP request. S'il en trouve un, l'assistant s'arrête, il va annoncer qu'il y a déjà un serveur DHCP sur le segment du réseau et il va nous demander d'arrêter le service DHCP. Il est possible de garder le service DHCP autre que sur le serveur SBS mais il est conseiller de le désactiver le temps de lancer l'assistant « se connecter à internet » pour le laisser finir, et ensuite le remettre en service.

b. Détection de routeur

Après la recherche DHCP, l'assistant recherche un routeur (RFC 1256) avec des requêtes ARP sur du multicast. S'il n'y a pas de routeur qui s'annonce, on va lancer le protocole SSDP pour trouver un routeur qui a les fonctionnalités UPNP et s'il n'en trouve pas, il va lancer des requêtes ARP sur les « ranges » 192.168.*.*

c. Configuration DHCP et DNS local

Configuration du DHCP avec 10 adresses d'exclusions (1à10) ainsi que du DNS avec tous les enregistrements nécessaires MX txt etc…

d. Test connexion internet

Pour finir il lancera des requêtes pour vérifier si la connexion internet est bonne.

1.2.2 Gestion du nom de domaine

C'est lui qui va gérer les certificats, paramétrer exchange et c'est lui aussi qui va faire du port forwarding sur le routeur.

a. Création de nom de domaine public

- « Remote.mon-nom-de-domaine.public.com »
- Création des bons enregistrements sur le domaine public (A, MX, TXT…) ; pour notre part, le DNS public étant gérer par oléane, il a fallu leur envoyer un fax leur demandant d'effectuer les changements.
- Mise à jour du domaine public (comme DynDNS)

b. Paramétrage automatique des services

- Outlook Anywhere
- Exchange
- Remote web Access
- Utilitaire de connexions pour les websites
- Certificats

c. Paramétrage du routeur (si UPNP)

- TCP 443 (postes de travail web à distance, RD Gateway, OWA, Outlook anywhere)
- TCP 25 (messagerie)
- TCP 987 (Sharepoint)

1.2.3 Assistant "envoi des e-mails"

- Soit relai SMTP
- Soit Smart Host, à condition que le nom de domaine publc soit correctement parametrer au niveau du DNS (MX, TXT…)

1.2.4 Sauvegarde simplifiée

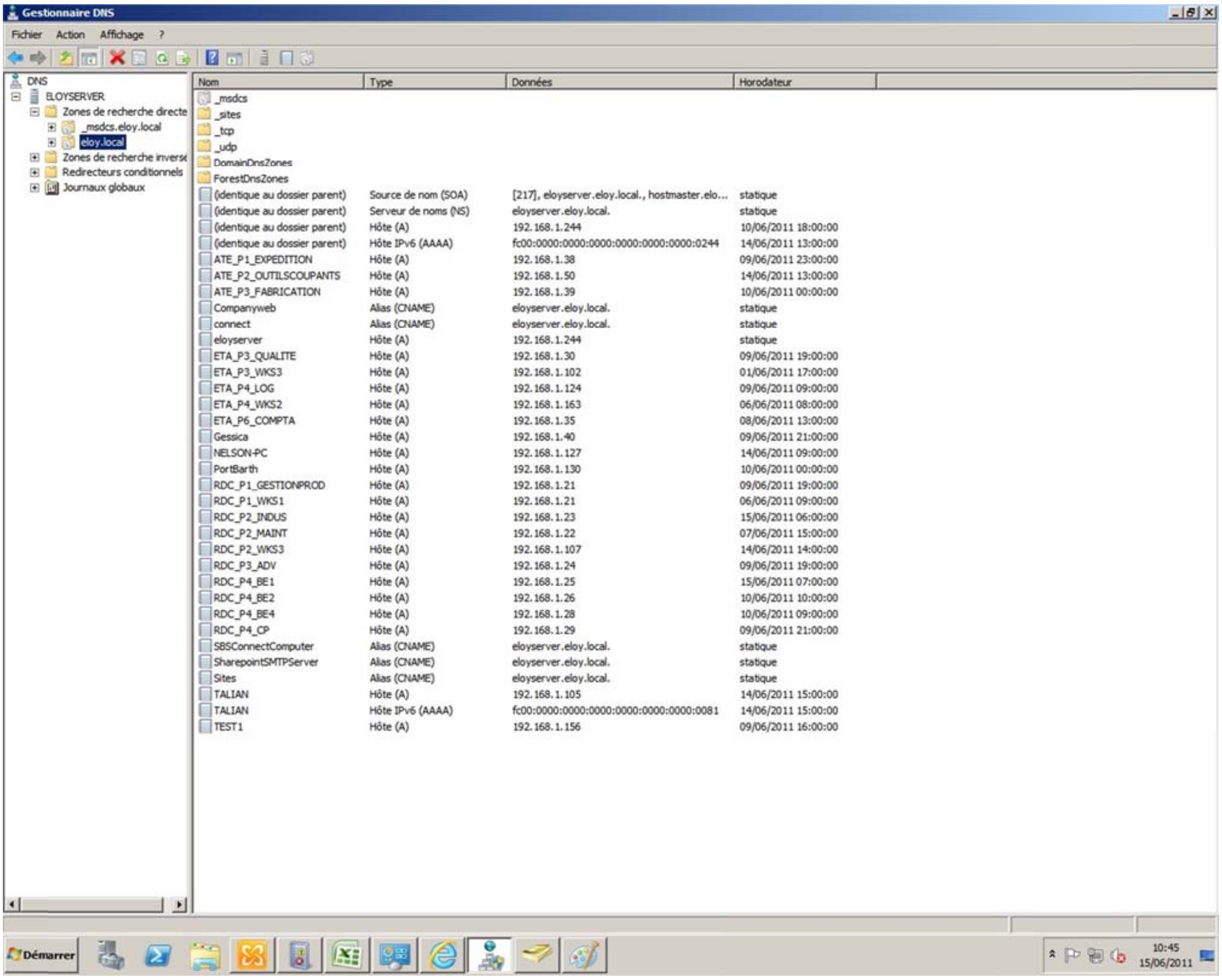
- Choix du disque (attention dédié)
- Choix des volumes à sauvegarder
- Paramétrage des heures de sauvegarde
- Sauvegarde immédiate
- Résumé des sauvegardes (Reporting)
- Restauration (Fichiers, Répertoires, Applications, Volumes, BMR…)

1.2.5 Déplacements des datas (console)

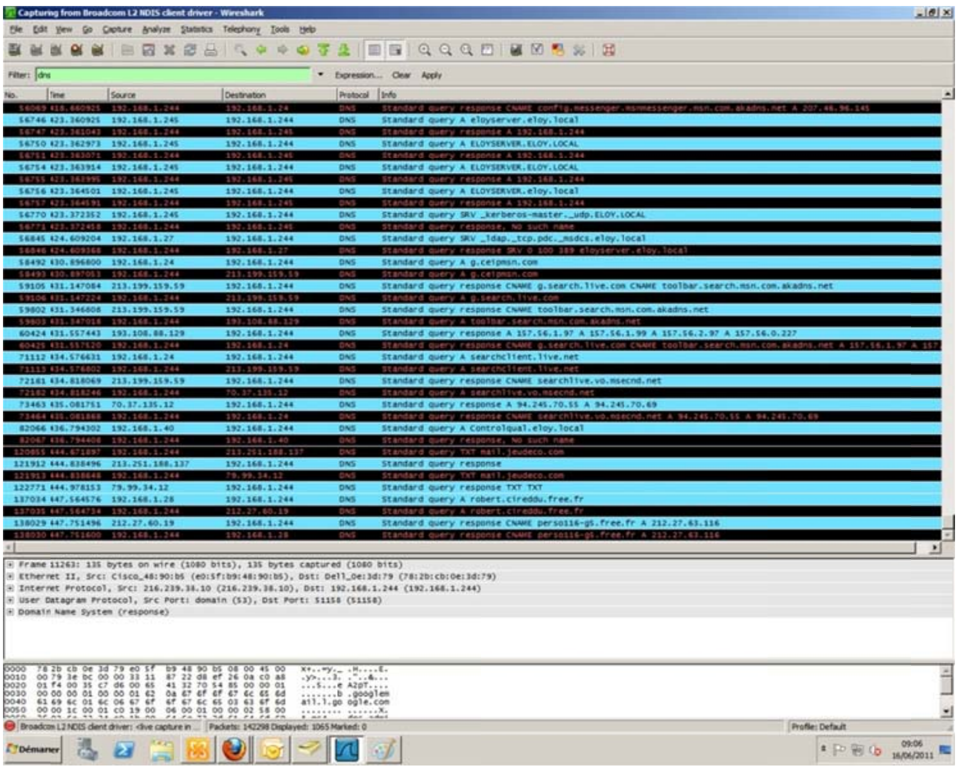
- Bases d'exchange server
- Base Sharepoint
- Partages utilisateurs
- Redirections utilisateurs
- Data WSUS

A la base tout se trouve dans C : \

1.3 DNS

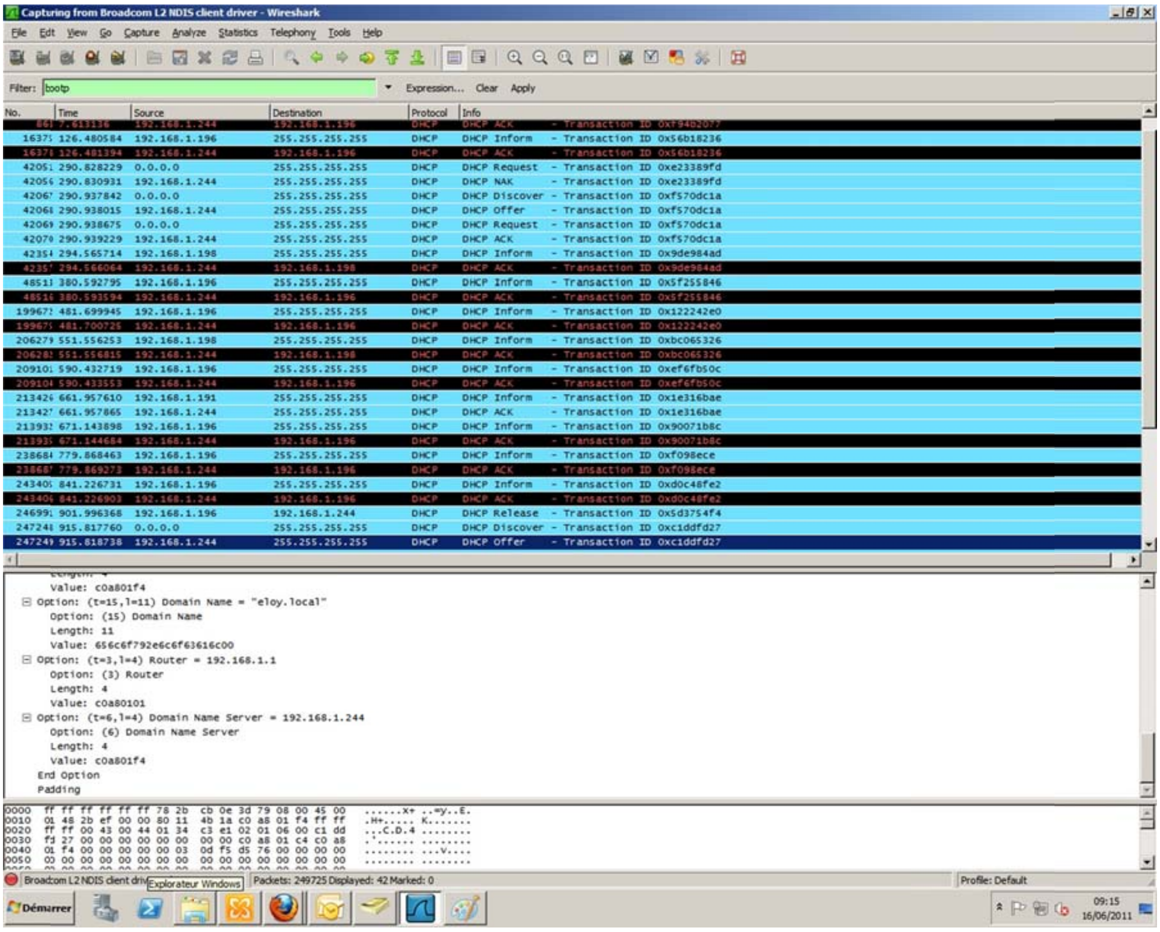


Gestionnaire DNS
Fichier Action Affichage ?
DNS
ELOYSERVER
Zones de recherche directe
_msdcs.eloy.local
eloy.local
Zones de recherche inverse
Redirecteurs conditionnels
Journaux globaux
Nom Type Données Horodateur
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
(identique au dossier parent) Source de nom (SOA) [217], eloyserver.eloy.local., hostmaster.elo... statique
(identique au dossier parent) Serveur de noms (NS) eloyserver.eloy.local. statique
(identique au dossier parent) Hôte (A) 192.168.1.244 10/06/2011 18:00:00
(identique au dossier parent) Hôte IPv6 (AAAA) fc00:0000:0000:0000:0000:0000:0000:0244 14/06/2011 13:00:00
ATE_P1_EXPEDITION Hôte (A) 192.168.1.38 09/06/2011 23:00:00
ATE_P2_OUTILSCOUPANTS Hôte (A) 192.168.1.50 14/06/2011 13:00:00
ATE_P3_FABRICATION Hôte (A) 192.168.1.39 10/06/2011 00:00:00
Companyweb Alias (CNAME) eloyserver.eloy.local. statique
connect Alias (CNAME) eloyserver.eloy.local. statique
eloyserver Hôte (A) 192.168.1.244 statique
ETA_P3_QUALITE Hôte (A) 192.168.1.30 09/06/2011 19:00:00
ETA_P3_WKS3 Hôte (A) 192.168.1.102 01/06/2011 17:00:00
ETA_P4_LOG Hôte (A) 192.168.1.124 09/06/2011 09:00:00
ETA_P4_WKS2 Hôte (A) 192.168.1.163 06/06/2011 08:00:00
ETA_P6_COMPTA Hôte (A) 192.168.1.35 08/06/2011 13:00:00
Gessica Hôte (A) 192.168.1.40 09/06/2011 21:00:00
NELSON-PC Hôte (A) 192.168.1.127 14/06/2011 09:00:00
PortBarth Hôte (A) 192.168.1.130 10/06/2011 00:00:00
RDC_P1_GESTIONPROD Hôte (A) 192.168.1.21 09/06/2011 19:00:00
RDC_P1_WKS1 Hôte (A) 192.168.1.21 06/06/2011 09:00:00
RDC_P2_INDUS Hôte (A) 192.168.1.23 15/06/2011 06:00:00
RDC_P2_MAINT Hôte (A) 192.168.1.22 07/06/2011 15:00:00
RDC_P2_WKS3 Hôte (A) 192.168.1.107 14/06/2011 14:00:00
RDC_P3_ADV Hôte (A) 192.168.1.24 09/06/2011 19:00:00
RDC_P4_BE1 Hôte (A) 192.168.1.25 15/06/2011 07:00:00
RDC_P4_BE2 Hôte (A) 192.168.1.26 10/06/2011 10:00:00
RDC_P4_BE4 Hôte (A) 192.168.1.28 10/06/2011 09:00:00
RDC_P4_CP Hôte (A) 192.168.1.29 09/06/2011 21:00:00
SBSConnectComputer Alias (CNAME) eloyserver.eloy.local. statique
SharepointSMTPServer Alias (CNAME) eloyserver.eloy.local. statique
Sites Alias (CNAME) eloyserver.eloy.local. statique
TALIAN Hôte (A) 192.168.1.105 14/06/2011 15:00:00
TALIAN Hôte IPv6 (AAAA) fc00:0000:0000:0000:0000:0000:0000:0081 14/06/2011 15:00:00
TEST1 Hôte (A) 192.168.1.156 09/06/2011 16:00:00
Démarrer
10:45
15/06/2011

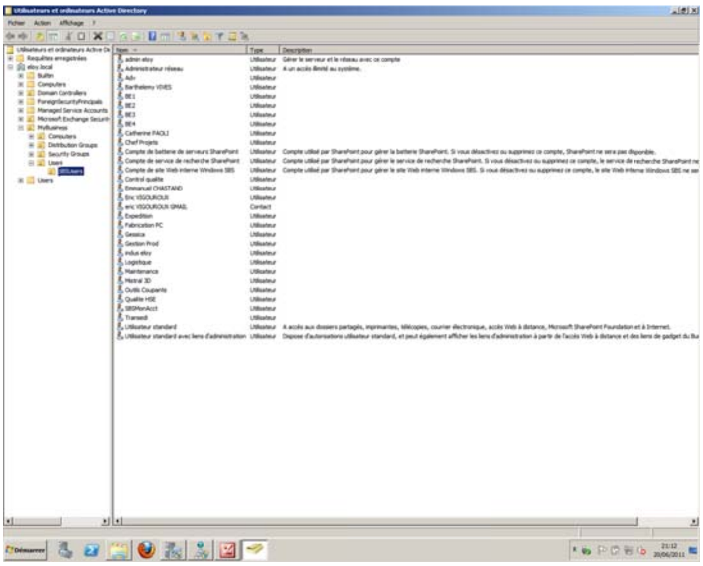


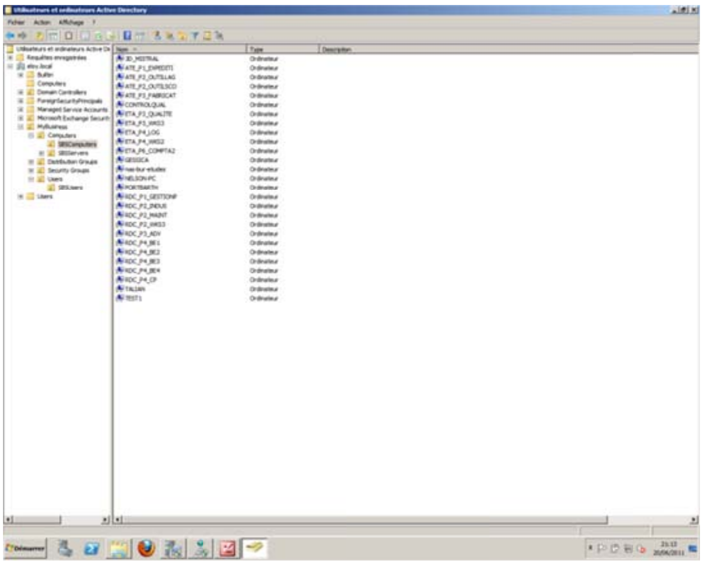
Capturing from Broadcom L2 NDIS client driver - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: dns
Expression... Clear Apply
No. Time Source Destination Protocol Info
Démarrer

1.4 DHCP



1.5 Active directory





2. Microsoft exchange 2010

Exchange est un produit qui a commencé sa carrière en 1996. À l'époque, Active Directory n'existait pas. Depuis l'apparition d'Active Directory en 1999, Exchange se base dessus. Les versions avant Exchange 2000 embarquaient donc leur propre annuaire pour gérer les utilisateurs. Aujourd'hui, nous sommes à la version 2010. Cette version apporte de nombreux changements par rapport à la version 2007, notamment sur la partie haute disponibilité et les besoins matériels (revus à la "baisse").

2.1 Les différents composants d’exchange

2.1.1 Les rôles

Depuis Exchange 2007, nous avons quatre rôles qui réalisent chacun une partie des fonctions d'Exchange. Cela permet une meilleure granularité pour le dimensionnement de votre architecture. Par exemple, si vous avez besoin de plus de puissance pour une fonction d'Exchange, il vous suffira d'isoler le rôle sur un ou plusieurs serveurs. À l'inverse, il sera possible de co-localiser différents rôles. Voyons quels sont ces rôles.

a. Rôle CAS : Client Access Server ou rôle d'accès client

Comme son nom l'indique, ce rôle va servir aux clients pour accéder à leur compte Exchange. Cela comprend les accès Outlook, Outlook Web App, Outlook AnyWhere et ActiveSync. C'est ici que les clients vont se connecter.

b. Rôle Mailbox : boîtes aux lettres

Ce rôle héberge les boîtes aux lettres de chaque utilisateur, matériel ou salle de l'organisation Exchange. Il héberge également les carnets d'adresses et permet la planification de réunions et des ressources associées.

c. Rôle Transport Hub : routage des messages

Ce rôle gère le routage et la remise des messages dans l'organisation Exchange. Il gère également la transmission de messages hors de l'organisation. Il peut également filtrer les messages ou appliquer des règles de routage configurées par l'administrateur. Ce rôle peut également journaliser les messages pour se conformer aux réglementations en vigueur.

d. Rôle Edge : passerelle email

Ce rôle est indépendant d'Active Directory et est généralement placé en DMZ. Il s'agit d'une passerelle email qui peut accepter les emails provenant d'Internet ou de serveurs d'organisations externes clairement identifiés. Ce serveur va pouvoir procéder à un scan antispam et antivirus grâce à Forefront Protection for Exchange. Les emails entrants ayant passé l'hygiène de messagerie seront routés vers les serveurs Transport Hub de l'organisation. Ce rôle ne peut pas être colocalisé avec d'autres rôles d'Exchange.

e. Rôle UM : Unified Messaging ou messagerie unifiée

Depuis Exchange 2007 SP1, un cinquième rôle a été ajouté : la messagerie unifiée. Ce rôle permet la réception des messages vocaux et fax dans la boîte aux lettres de l'utilisateur. Il permet également la consultation d'Exchange depuis un téléphone : vous pouvez ainsi écouter vos messages vocaux, emails et réunions. Vous pouvez également créer des messages ou contacter directement des personnes grâce à la consultation de votre carnet d'adresses. Le serveur vocal est capable de reconnaitre la voix (sans nécessiter de configuration préalable) ou alors de fonctionner en DTMF (touches numériques de votre téléphone).

2.1.2 Les noms des différentes technologies d'Exchange

a. Autodiscover

Il s'agit d'un service Web qui existe depuis Exchange 2007. Les clients Outlook savent utiliser ce service depuis la version 2007. Autodiscover permet de découvrir automatiquement les paramètres du serveur Exchange à partir de l'adresse email de l'utilisateur (à condition d'avoir son login et son mot de passe). Le client prend le domaine email de l'utilisateur, y préfixe Autodiscover et forme ainsi un domaine sur lequel Autodiscover doit être hébergé. Par exemple, si l'utilisateur entre l'adresse email utilisateur@mondomaine.fr, le client va aller interroger Autodiscover.mondomaine.fr. Ce service est accessible via HTTPS uniquement.

b. Outlook Web App

Avant Exchange 2010, cela s'appelait Outlook Web Access. Il s'agit d'une application Web qui permet l'accès à son compte Exchange depuis un simple navigateur. Outlook Web App est compatible avec la plupart des navigateurs du marché (autres que Microsoft). OWA permet d'accéder à la plupart des fonctions d'Outlook. L'interface est quasiment identique. Vous pourrez ainsi consulter et rédiger des emails, gérer votre agenda, vos contacts, vos messages vocaux, etc.

c. Outlook Anywhere

Il s'agit encore une fois d'un service Web disponible par HTTPS.

2.2 Outlook Web App

La redirection du port 443 a été effectuée par orange et redirigé sur l'adresse IP 192.168.0.3, qui est l'adresse IP globale interne du serveur SBS.

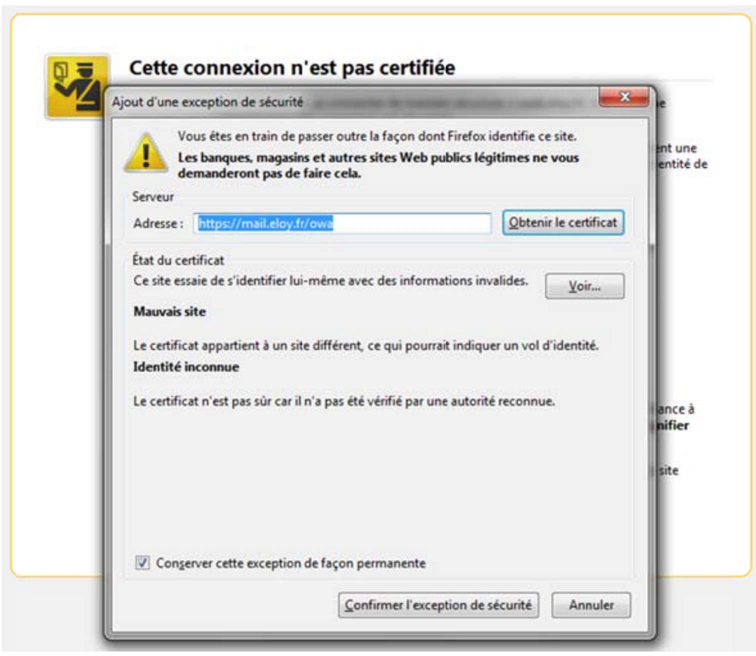
Le firewall étant configuré pour laisser passer le transit venant de l'extérieur vers l'adresse IP 192.168.0.3 et vers le port 443, le personnel de la société ELOY peut dorénavant consulter sa boite mail de chez soi sans aucun problème.

Etape 1 : Première connexion au site OWA via Firefox, qui est le seul à installer le certificat.

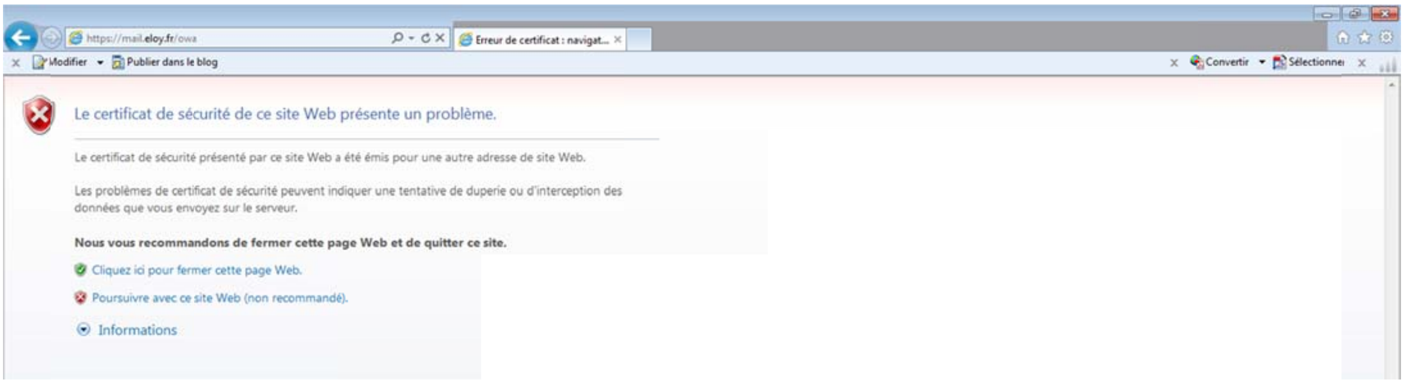
Cliquez sur ***« Je comprends les risques »***

Etape 2 : La fenêtre suivante s'ouvre

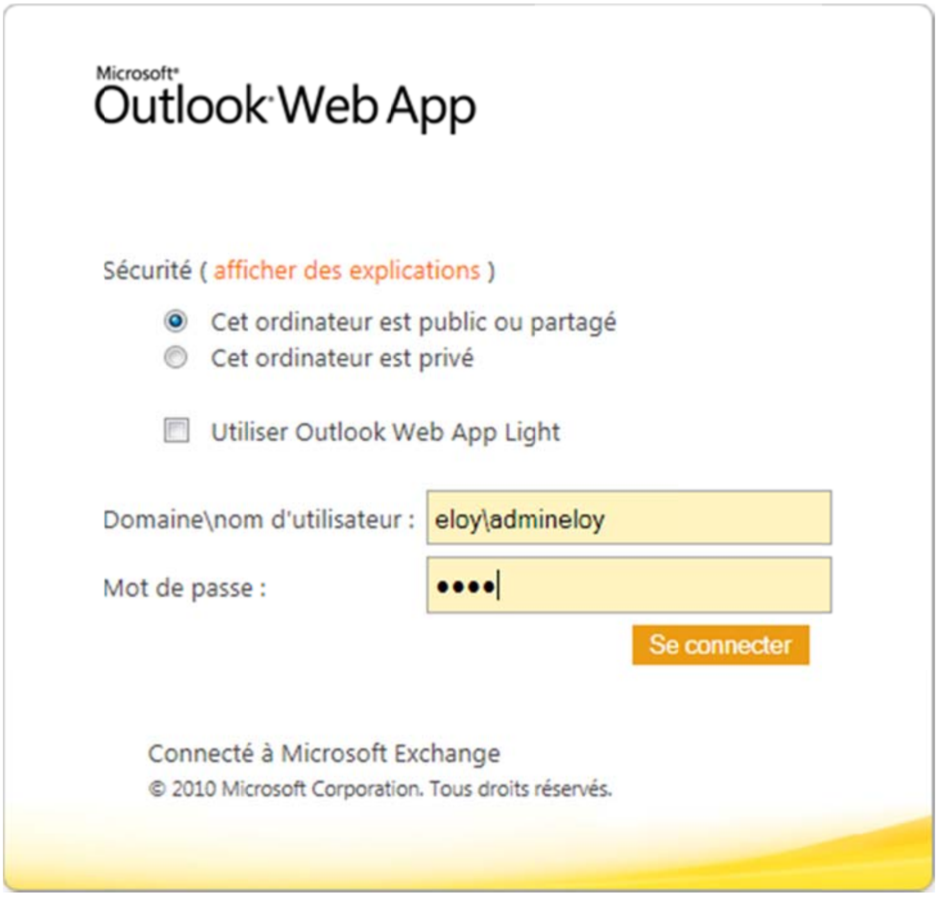
Cliquez sur ***« Confirmer l'exception de sécurité »*** vous passerez directement à l'étape 3.

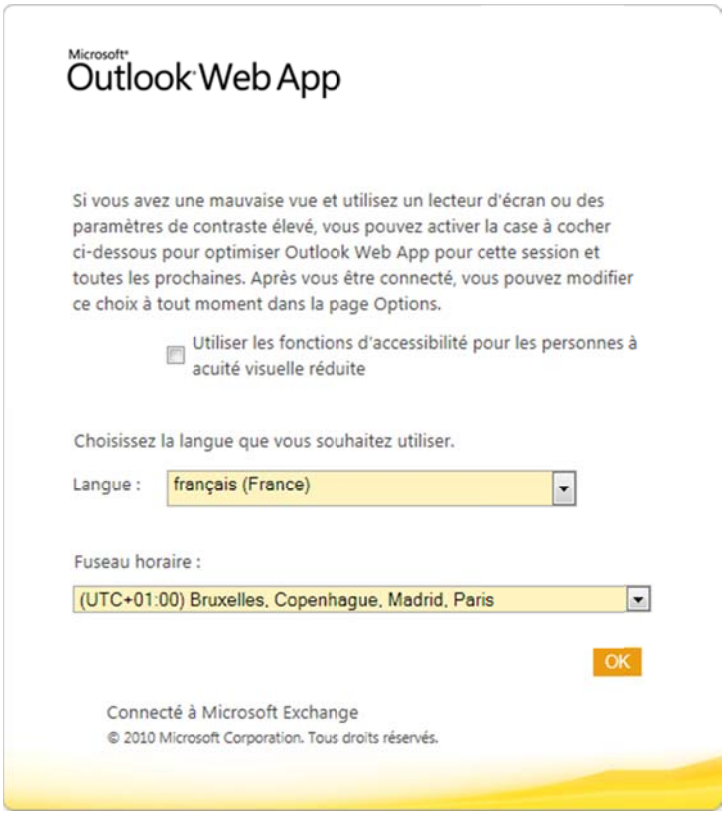


Etape 1 via Chrome ou Internet explorer : Cliquez sur poursuivre quand même, vous passerez directement à l'étape 3 mais votre communication ne sera pas sécurisé.

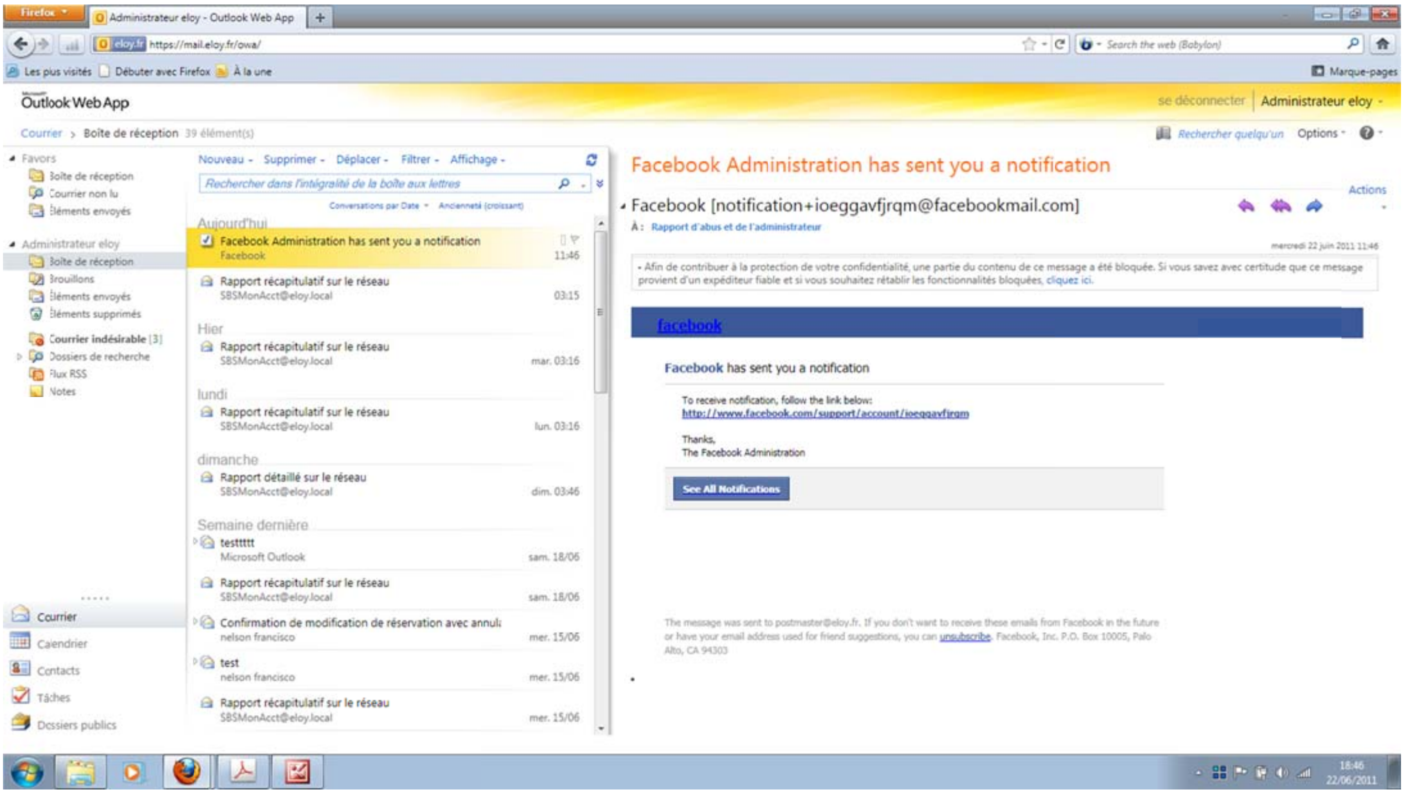


Etape 3 : renseignez le nom de domaine et votre identifiant comme dans l'exemple ci-dessous et entrez votre mot de passe qui est le même que vous utilisez pour vous connecter sur vos postes.





Etape 4 : Cliquez sur « OK »



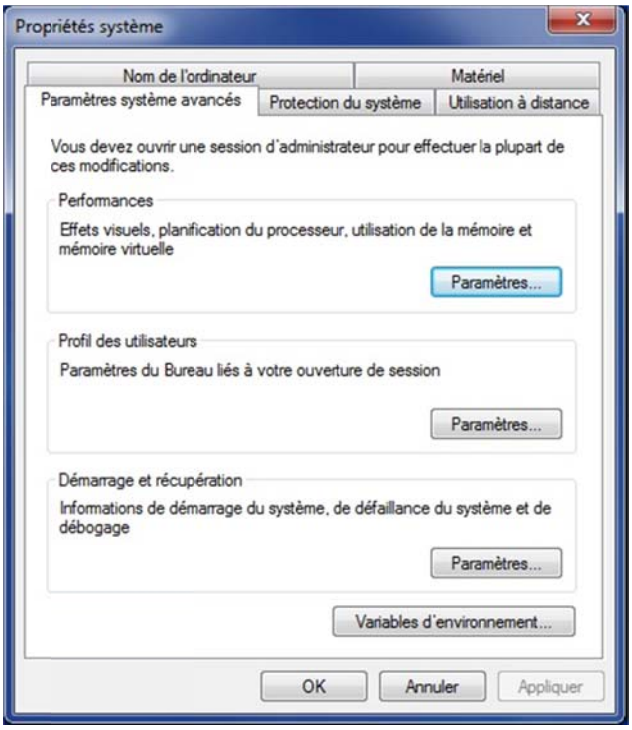
L'interface graphique d'Outlook Web App est assez comparable à celle que vous avez l'habitude d'utiliser sur vos postes.

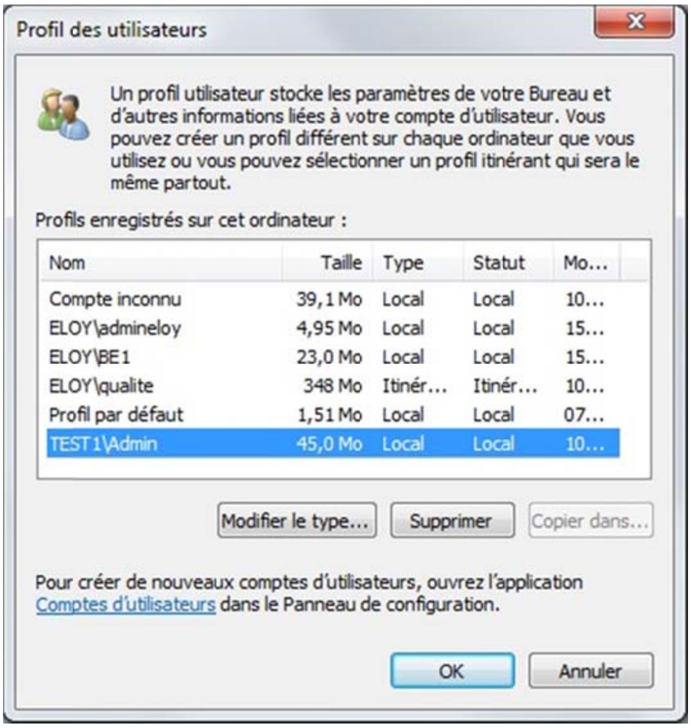
Vous y retrouverez vos contacts, calendrier, taches etc…

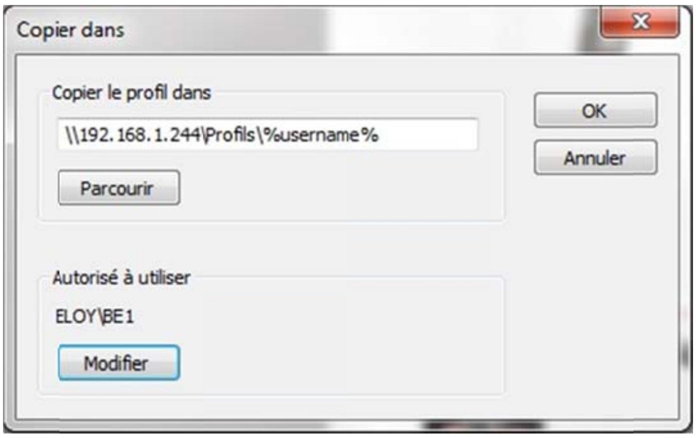
Vous pouvez aussi ouvrir l'accès à votre calendrier et messages à d'autres personnes. En haut, à droite, vous pouvez cliquer sur option et découvrir les divers choix qui vous sont offert.

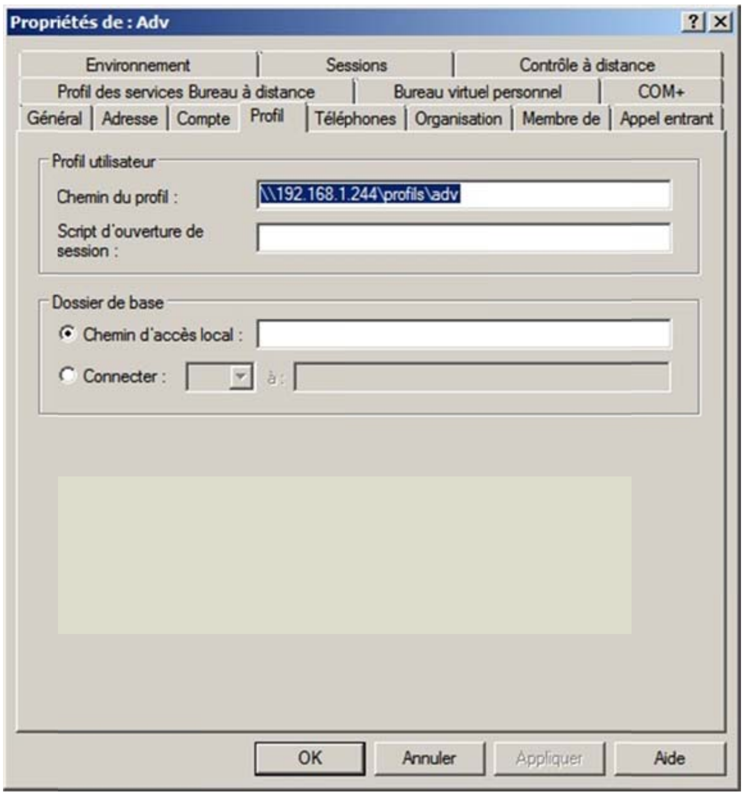
IX. Configuration des postes utilisateurs

1. Gestion des profils distants

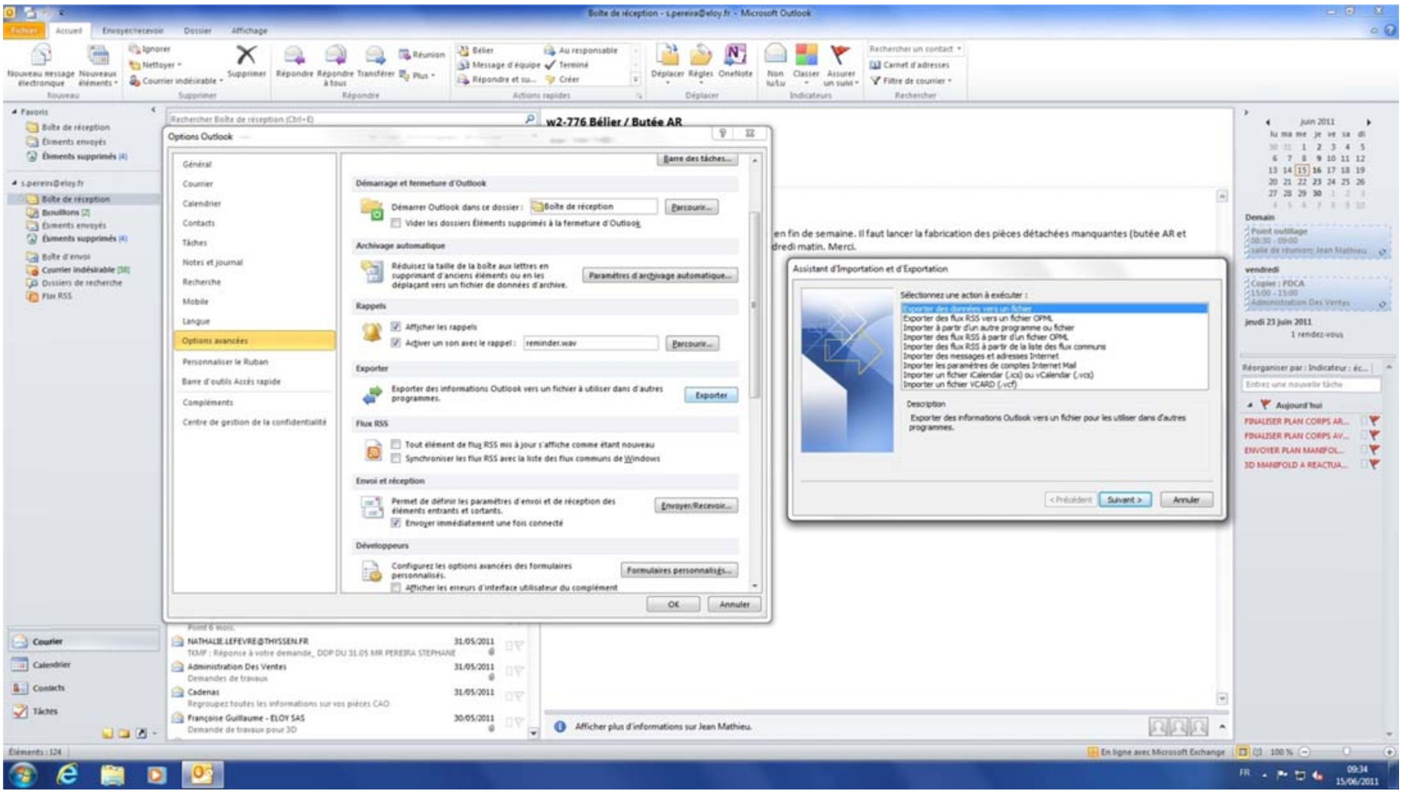


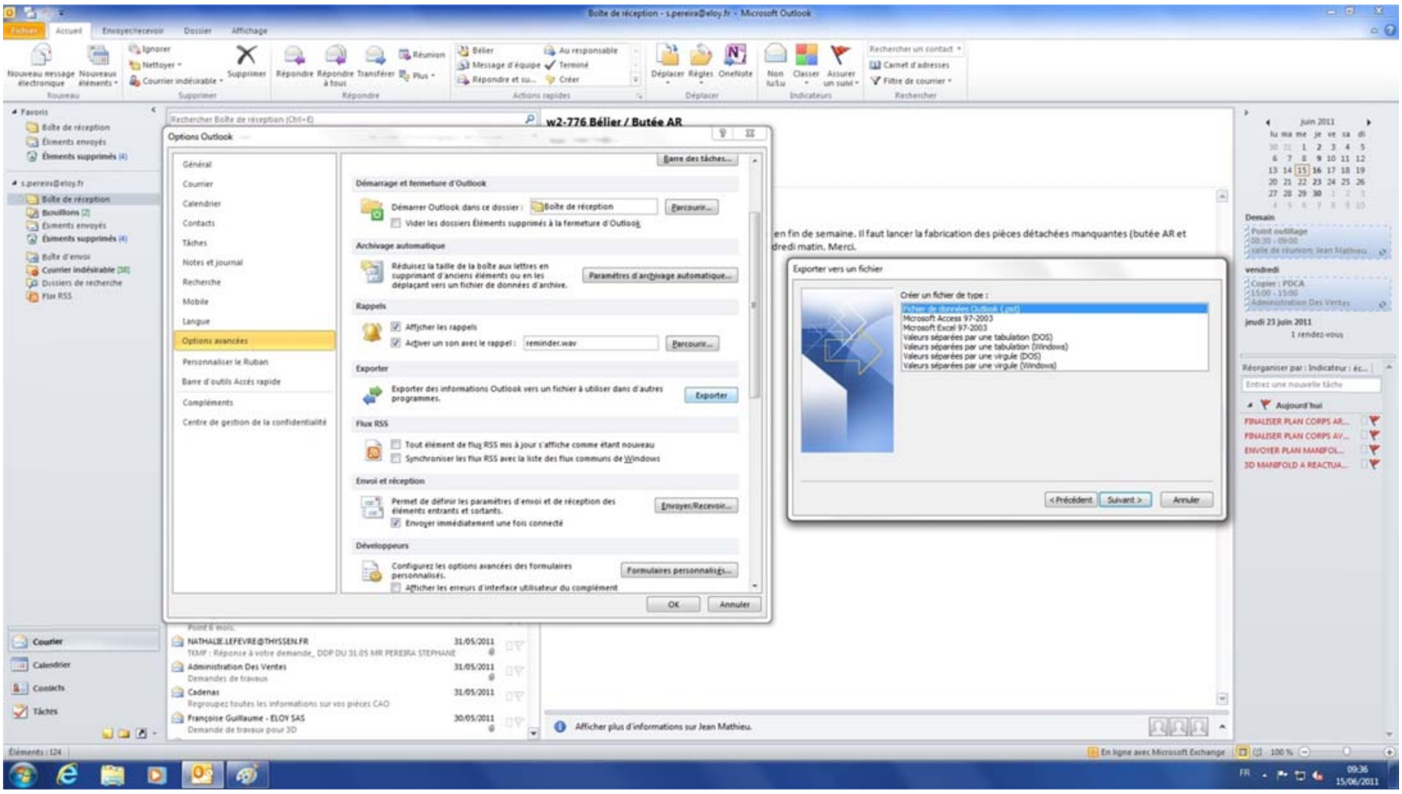


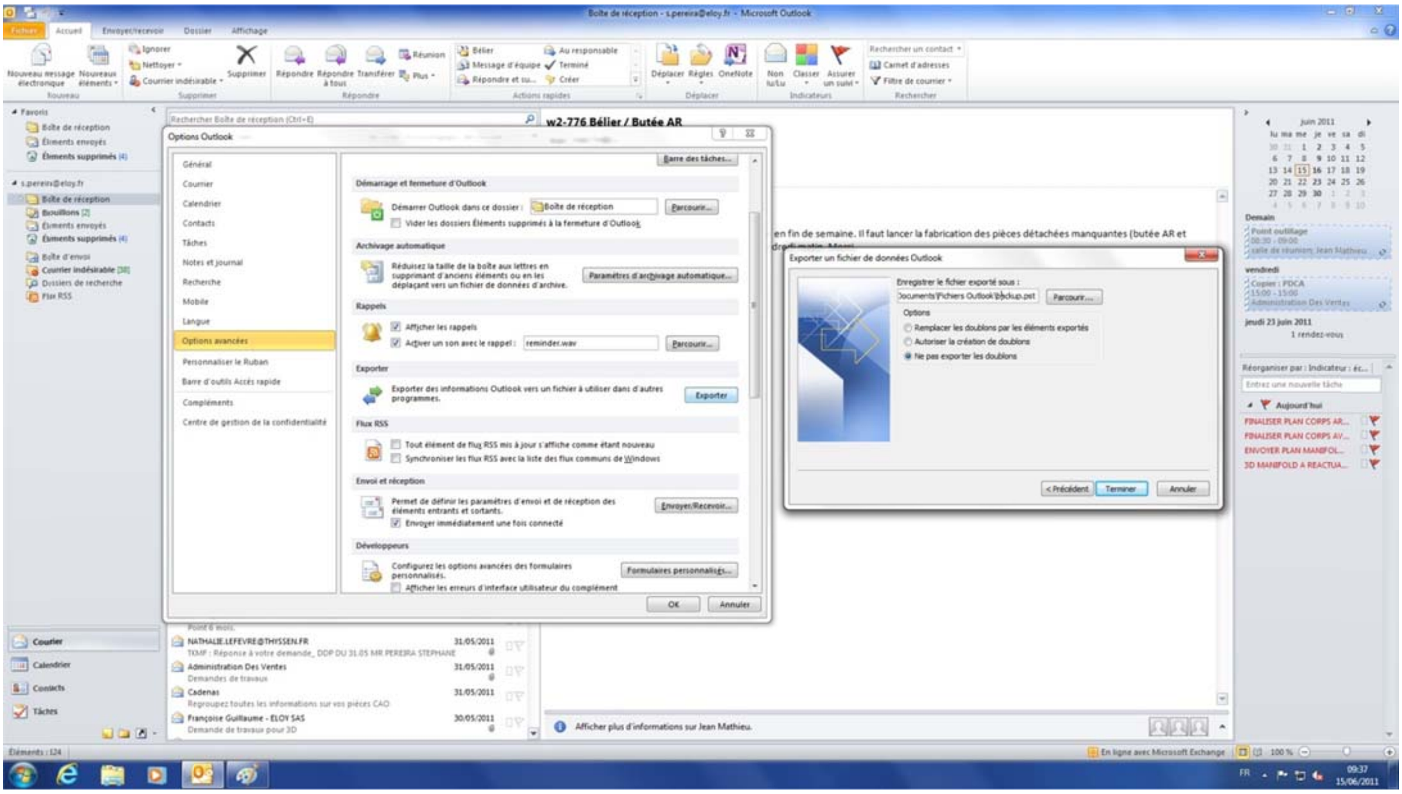


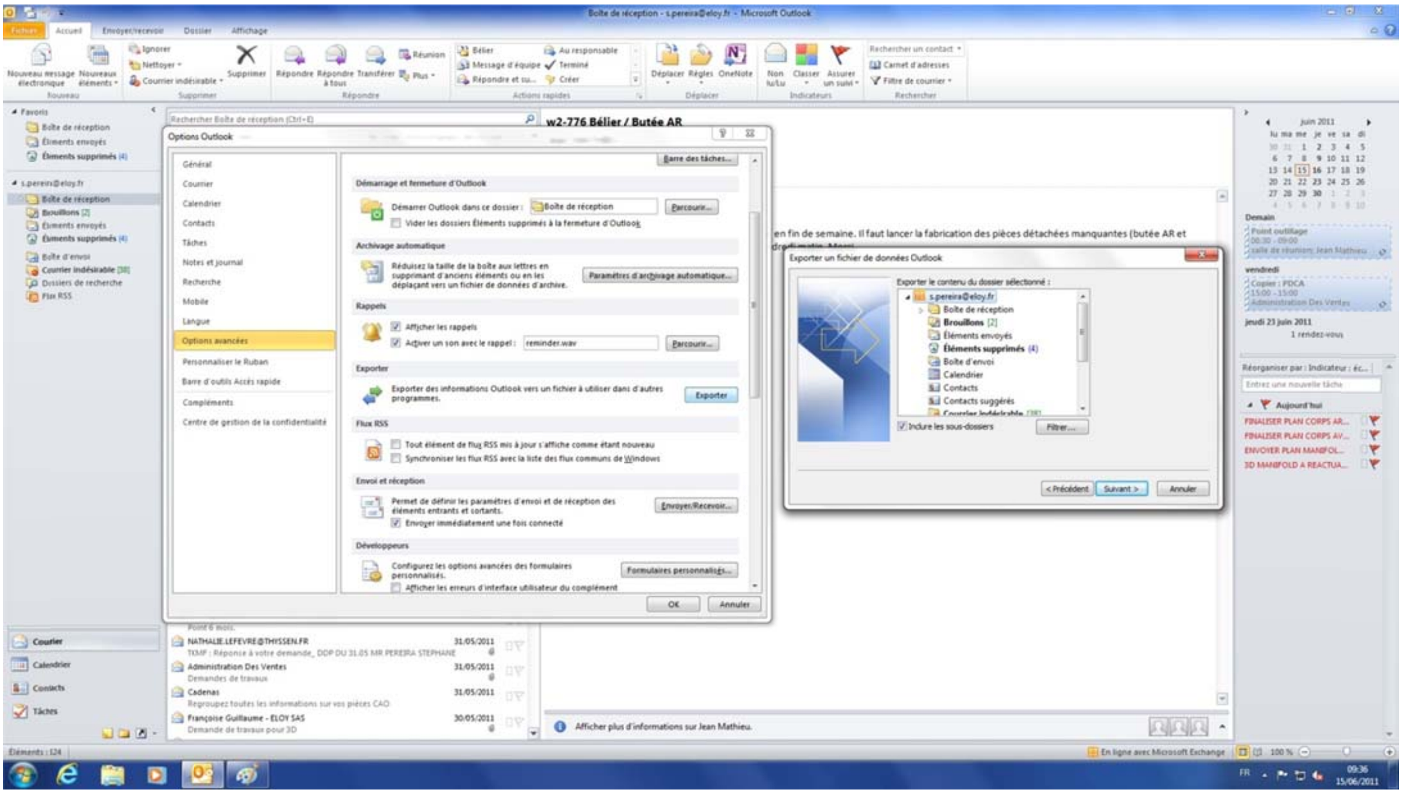


2. Export import des fichiers de données Outlook






Boîte de réception - s.pereira@eloy.fr - Microsoft Outlook
Options Outlook
Général
Courrier
Calendrier
Contacts
Tâches
Notes et journal
Recherche
Mobile
Langue
Options avancées
Personnaliser le Ruban
Barre d'outils Accès rapide
Compléments
Centre de gestion de la confidentialité
Démarrage et fermeture d'Outlook
Archivage automatique
Rappels
Exporter
Exporter des informations Outlook vers un fichier à utiliser dans d'autres programmes.
Flux RSS
Envoi et réception
Développeurs
OK
Annuler
w2-776 Bélier / Butée AR
Exporter un fichier de données Outlook
Enregistrer le fichier exporté sous :
Parcourir...
Options
Remplacer les doublons par les éléments exportés
Autoriser la création de doublons
Ne pas exporter les doublons
< Précédent
Terminer
Annuler


Boîte de réception - s.pereira@eloy.fr - Microsoft Outlook
Options Outlook
w2-776 Bélier / Butée AR
Exporter un fichier de données Outlook
Exporter le contenu du dossier sélectionné :
s.pereira@eloy.fr
Boîte de réception
Brouillons [2]
Éléments envoyés
Éléments supprimés (4)
Boîte d'envoi
Calendrier
Contacts
Contacts suggérés
Inclure les sous-dossiers
Filtrer...
< Précédent
Suivant >
Annuler

X. Bureau études

Le bureau études est composé de 4 utilisateurs travaillant sous Solidworks.

Jusqu'à maintenant les fichiers de travail étaient regroupés sur un des PC qui faisait office de serveur pour les trois autres. Une sauvegarde était effectuée mensuellement sur un disque dur externe.

Après leur entrée dans le domaine, nous avons essayé de déplacer ces fichiers sur le serveur. Des tests ont révélé que l'accès aux fichiers était beaucoup trop long pour pouvoir travailler correctement.

La solution retenue fut d'installer un NAS et un commutateur 8 ports gigabits.

1. Stockage smart Cisco SB NSS 322 2 baies

1.1 Description

Cisco® NSS300 Series Smart Storage assure une protection des données et une reprise sur sinistre complètes en combinant le stockage sur site et en ligne dans une solution unique, abordable et à hautes performances. Cisco Smart Storage propose une sauvegarde en ligne intégrée, optimisée par Mozy, pour centraliser et automatiser la sauvegarde de vos données professionnelles essentielles en toute simplicité.

Cisco Smart Storage inclut également des fonctionnalités professionnelles avancées, notamment plusieurs applications intégrées et compléments d'application qui étendent les capacités de la solution au-delà du simple stockage et offrent une valeur ajoutée supplémentaire à votre investissement. En outre, pour protéger votre investissement et garantir votre tranquillité d'esprit, le service d'assistance Cisco Small Business offre 3 ans de couverture à un prix abordable.

La gamme Cisco NSS300 Smart Storage présente les avantages suivants :

• Performances élevées : un périphérique de stockage en réseau NAS (Network-Attached Storage) représente le moyen le plus efficace et facile à gérer pour centraliser, protéger et partager les informations. Cisco Smart Storage offre des performances de pointe, accélère les sauvegardes et facilite le partage des informations.

• Sauvegarde en ligne intégrée : Cisco Smart Storage combine la sauvegarde sur site et la sauvegarde en ligne, ce qui en fait une solution de protection des données et de reprise sur sinistre complète et souple. La prise en charge intégrée de Mozy, service de sauvegarde en ligne réputé dans le monde entier, vous permet de centraliser et d'automatiser la sauvegarde des données critiques de l'entreprise. Choisissez ce que vous souhaitez stocker localement et ce que vous souhaitez sauvegarder en ligne, grâce à une interface intuitive.

• Applications intégrées et compléments d'application : allez au-delà du stockage avec des applications intégrées et la possibilité d'ajouter de nouvelles applications par la suite. L'exécution d'applications sur le périphérique NAS assure leur disponibilité permanente et permet d'éliminer le besoin de périphériques supplémentaires sur le réseau.

• Sécurité et cryptage des données : le cryptage des données sur disque, absent de la plupart des solutions de stockage pour PME, protège les données critiques de l'entreprise enregistrées sur disque, même en cas de vol des disques durs.

• Simplification de la configuration et de la gestion : Cisco Smart Storage peut être installé en quelques minutes et est facile à configurer et à gérer. Choisissez ce que vous souhaitez sauvegarder localement et ce que vous souhaitez sauvegarder en ligne, grâce à une interface intuitive, basée sur un navigateur.

• Flexibilité : Cisco Smart Storage prend en charge le partage de fichiers entre les plates-formes Microsoft Windows, Mac OS X et Linux. Plusieurs modes de sauvegarde en ligne et sur site sont disponibles, y compris PC/Mac vers Smart Storage, serveur vers Smart Storage ou Smart Storage vers Smart Storage. Vous pouvez aussi utiliser Cisco Smart Storage comme cible iSCSI pour les environnements virtualisés et en grappes.

• Conception fiable et à haute disponibilité : Cisco Smart Storage propose les configurations RAID (Redundant Array of Independent Disks) 0, 1, 5 et 6 pour la sauvegarde de vos données. La conception remplaçable à chaud permet de remplacer un disque en panne sans arrêter le périphérique Smart Storage.

• Fonctionnement écoénergétique : planifiez les mises sous et hors tension en fonction de vos heures de travail, et économisez l'énergie électrique grâce à la réduction de vitesse des disques durs en cas d'inactivité.

• Service d'assistance Cisco Small Business (facultatif) : protège votre investissement et offre une couverture de 3 ans à un prix abordable, pour votre tranquillité d'esprit. Fourni par Cisco, par l'intermédiaire de votre partenaire de confiance, ce service complet inclut des mises à jour logicielles, un accès au centre d'assistance Cisco Small Business et le remplacement du matériel le jour ouvrable suivant.

1.2 Installation et configuration

Avant de commencer l'installation, vérifiez que vous disposez bien des équipements et services suivants :

- Connexion Internet (en option)
- Petit tournevis cruciforme
- Routeur ou commutateur Ethernet
- Un ou deux disques durs SATA de 2,5 pouces ou disques durs de 3,5 pouces (non inclus avec certains modèles). Il n'est pas nécessaire que les disques durs aient la même taille physique.
- Onduleur (UPS), avec une connexion USB, capable de fournir une alimentation pendant au moins dix minutes avec une capacité d'au moins 200 watts. Il est vivement recommandé d'avoir une source d'alimentation de secours pour réduire les risques de dommages causés au système en cas de coupure d'électricité. Après l'installation initiale du périphérique NAS, voir le Cisco Small Business NSS 322, NSS 324, and NSS 326 Smart Storage Administration Guide (Guide d'administration de l'Espace de stockage intelligent Cisco Small Business NSS 322, NSS 324 et NSS 326) pour configurer le NAS afin qu'il puisse communiquer avec l'onduleur.
- Un bracelet antistatique correctement relié à la terre (recommandé)

1.2.1 Faire connaissance avec le NSS 322

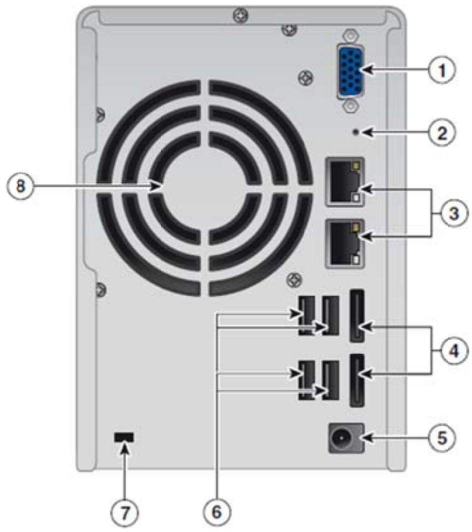
La section qui suit décrit les panneaux avant et arrière de l'Espace de stockage intelligent NSS 322.

a. Panneaux avant

Numéro	Indicateur DEL	Description
1	HDD1, HDD2	• (Vert) Clignote en vert lorsque le système accède aux données sur les unités de disque. L'indicateur reste allumé en vert lorsque l'unité de disque est accessible. • (Rouge) Il y a une erreur de lecture ou d'écriture sur un disque dur.
	LAN	(Orange) Clignote en cas de trafic réseau vers ou à partir du NAS. Est allumé en orange fixe lorsque le NAS est connecté au réseau.
	eSATA	(Orange) Clignote lorsque le système est en train d'accéder à un périphérique eSATA.
2	Alimentation	• (Éteint) Les unités de disque sont en mode veille ou le périphérique est hors tension. • (Vert fixe) Le NAS est prêt. • (Vert clignotant) Cela indique l'une ou plusieurs des conditions suivantes : - Le NAS est en train de démarrer. - Le NAS n'est pas configuré. - Unité de disque non formatée. • (Rouge clignotant) Le NAS est en mode dégradé. Défaillance de l'une des unités de disques dans la configuration RAID 1.
3	Copie d'une touche	(Bleu) Le périphérique USB est détecté.

Numéro	Élément	Description
2	Bouton Marche/ Arrêt	Appuyez sur Marche/Arrêt pour mettre le NAS sous ou hors tension.
3	Bouton Copie d'une touche	Appuyez sur Copie d'une touche pour copier les fichiers sur ou à partir d'une unité USB externe.
4	USB 2.0	Port USB permettant d'accéder à un périphérique de stockage USB connecté.
5	Verrou pour plateau à disque	Faites glisser la languette argentée vers le haut pour verrouiller le plateau à disque. Faites glisser la languette argentée vers le bas pour déverrouiller le plateau à disque.

b. Panneaux arrière



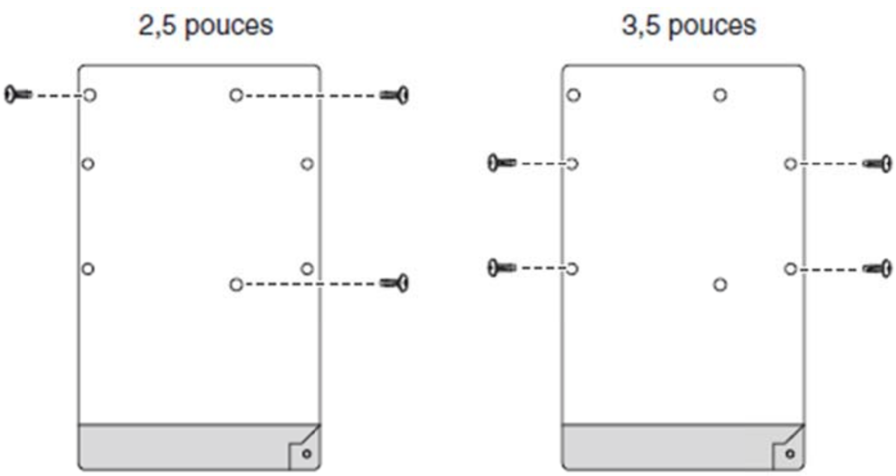
Numéro	Élément	Description
1	VGA	Sortie console pour le moniteur VGA. Utilisé pour la récupération du périphérique.
2	Réinitialisation	Permet de restaurer les paramètres réseau et le mot de passe aux valeurs usine par défaut.
3	Port Ethernet (2)	Deux ports Ethernet.
4	eSATA (2)	Ports eSATA permettant d'accéder aux périphériques de stockage sATA connectés. Utilisez un connecteur eSATA.
5	Connecteur d'alimentation	Permet de connecter le périphérique à l'adaptateur d'alimentation externe, qui lui-même se branche sur une prise standard du secteur.
6	USB 2.0 (4)	Ports USB permettant d'accéder aux périphériques de stockage USB connectés et à l'état UPS.
7	Emplacement pour verrou Kensington	Attachez un verrou Kensington pour protéger le périphérique contre le vol.
8	Ventilateur	Ventilateur du système.

1.2.2 Installations des unités de disques

- *Étape 1* Enlevez le contenu de la boîte d'emballage du NAS.
- *Étape 2* Placez le châssis droit sur une surface plane.
- *Étape 3* En commençant par la baie de disque 1, enlevez le plateau à disque.

Pour enlever le plateau à disque, faites glisser la languette argentée vers le bas pour déverrouiller le plateau, et appuyez sur la languette inférieure de façon à libérer le levier du plateau. À l'aide du levier du plateau, faites sortir le plateau.

- *Étape 4* Placez l'unité de disque dans le plateau pour disque. Les connecteurs électriques de l'unité de disque doivent être orientés vers l'arrière du plateau à unité.
- *Étape 5* Fixez l'unité de disque sur le plateau en insérant les vis pour unité de disque dans les quatre orifices sur la base du plateau et en les serrant avec un tournevis cruciforme.
  REMARQUE Utilisez les vis fournies dans la boîte avec le périphérique. L'utilisation d'autres vis risquerait d'endommager votre disque ou le plateau à disque.
  Il y a des orifices pour disque clairement marqués adaptés aux unités de disque suivantes :
  - Unité de disque de 3,5 pouces (utilisez les vis argentées fournies)
  - Unité de disque de 2,5 pouces (utilisez les vis noires fournies)



- *Étape 6* Remettez le plateau en suivant la séquence correcte dans la baie vide du châssis.
  REMARQUE Les plateaux à unités doivent toujours être échangés emplacement par emplacement.
  Il y a aussi une étiquette de séquence des disques durs dans l'emballage, qui peut être placée au sommet du châssis et qui montre la séquence des unités de disque. Par exemple, 1-2 pour le NSS 322.

Le numéro de séquence des unités de disque est également indiqué à l'intérieur du tiroir à disque.

- *Étape 7* Du pouce, appliquez une pression uniforme au milieu du plateau pendant que vous insérez le plateau doucement et entièrement en position dans le châssis.
  Le levier du plateau à disque devrait être en position ouverte.
- *Étape 8* Abaissez doucement le levier du plateau à disque jusqu'à ce que vous entendiez un déclic.
- *Étape 9* Répétez les étapes 3 à 8 pour installer la seconde unité de disque.

1.2.3 Verrouillage et déverrouillage des plateaux à disque

Une icône se trouve sur la languette argentée indiquant :

- Lorsque la languette est en position haute, le plateau à disque est verrouillé.
- Lorsque la languette est en position basse, le plateau à disque est déverrouillé.

Pour verrouiller le plateau à disque :

- *Étape 1* Vérifiez que le plateau à disque est bien complètement inséré dans le châssis lorsque le levier du plateau à disque est abaissé.
- *Étape 2* Faites glisser la languette argentée vers le haut pour verrouiller le plateau à disque.
- *Étape 3* Continuez sur Connexion de l'équipement, page 10.

Pour déverrouiller le plateau à disque :

- *Étape 1* Sur le plateau à disque, faites glisser la languette argentée vers le bas pour déverrouiller le plateau à disque.
- *Étape 2* Appuyez sur le bouton qui se trouve sous la languette argentée pour libérer le levier du plateau à disque.
- *Étape 3* À l'aide du levier du plateau à disque, faites doucement sortir le plateau à disque du châssis.

1.2.4 Connexion de l'équipement

- *Étape 1* Connectez le câble Ethernet fourni à l'un des ports Ethernet sur l'arrière du châssis.
- *Étape 2* Connectez l'autre extrémité du câble Ethernet sur un commutateur ou un routeur sur votre réseau.
- *Étape 3* Connectez l'adaptateur secteur fourni sur le port Alimentation à l'arrière du châssis. Connectez le cordon d'alimentation sur l'adaptateur secteur.
- *Étape 4* Branchez l'autre extrémité du cordon d'alimentation sur la sortie alimentée par batterie de l'onduleur, ou sur une prise standard du secteur si vous n'utilisez pas d'onduleur.
- *Étape 5* Pour démarrer le NAS, appuyez sur puis relâchez le bouton Marche/Arrêt sur le panneau avant. Vous devriez attendre un bip. Patientez une à deux minutes jusqu'à ce que le périphérique émette un nouveau bip. Le périphérique a démarré avec succès. L'indicateur d'alimentation s'allume en vert fixe lorsque le NAS est prêt à être utilisé.

1.2.5 Commencer la configuration du NAS

Après que vous avez connecté l'équipement et appuyé sur le bouton Marche/Arrêt, il faut quelques minutes au système pour s'initialiser. Vous devriez attendre un bip. Patientez une minute jusqu'à ce que vous entendiez u second bip. L'indicateur d'alimentation s'allume en vert fixe. Le périphérique NAS a démarré avec succès et vous pouvez le configurer à l'aide de l'Assistant de Première installation.

REMARQUE Si le pare-feu de Windows émet des alertes pendant le processus, vous devez autoriser l'application d'installation à déverrouiller les paramètres du pare-feu. Si l'installation ne démarre pas, il se peut que vous deviez aussi désactiver temporairement vos logiciels de sécurité sur votre ordinateur pour pouvoir exécuter l'Assistant de configuration.

- *Étape 1* Insérez le produit du CD et, sur la page Welcome (Bienvenue), cliquez sur NSS 322.
  La page NSS 322 Setup Menu (Menu de configuration du NSS 322) s'affiche.
- *Étape 2* Sous First Time Installation (Première installation), cliquez sur Setup (Configuration).
  La page First Time Installation Wizard (Assistant de Première installation) s'affiche.
- *Étape 3* Cliquez sur Next (Suivant) pour lancer l'assistant.
  La page End-User License Agreement (Accord de licence de l'utilisateur final) s'affiche.
- *Étape 4* Pour accepter l'Accord de l'utilisateur final, cochez la case I accept this agreement (J'accepte cet accord) et cliquez sur Next (Suivant).
  La page Hardware Installation Guide (Guide d'installation du matériel) s'affiche.
- *Étape 5* Cliquez sur Next (Suivant) et suivez les invites pour vérifier le contenu du paquet, installer les unités de disque et connecter l'équipement.
  REMARQUE Si vous avez déjà installé les unités de disque et connecté l'équipement, cliquez sur Skip (Ignorer) jusqu'à ce que vous arriviez à la page System Configuration (Configuration du système).
- *Étape 6* Sur la page System Configuration (Configuration du système), cliquez sur Next (Suivant) pour aller sur la configuration du NAS.
  La page NAS Configuration (Configuration du NAS) s'affiche.
- *Étape 7* Cliquez sur Next (Suivant).
  La page Discovering the NAS (Découverte du NAS) s'affiche et vous informe lorsque le périphérique non initialisé est détecté.
- *Étape 8* Cliquez sur Next (Suivant).
  La page Web Configuration (Configuration web) s'affiche.
- *Étape 9* L'Assistant de Première installation détecte le NAS et vous invite à suivre la procédure de configuration web. Dans la liste déroulante, sélectionnez un périphérique NAS.
- *Étape 10* Cliquez sur Next (Suivant) pour continuer. Vous êtes redirigé vers une page de configuration web pour procéder au paramétrage pas à pas.
  La page Welcome (Bienvenue) s'affiche.
- *Étape 11* Cliquez sur Next (Suivant).
  Vous êtes redirigé vers une page sur laquelle vous pouvez saisir un nom pour ce périphérique.
- *Étape 12* Dans le champ Device Name (Nom du périphérique), saisissez un nom pour identifier le périphérique NAS.
  Le nom du périphérique peut comporter au maximum 14 caractères, et seuls les caractères alphanumériques (a-z, 0-9) et les tirets (-) sont acceptés. Il est nécessaire que le nom du périphérique commence par une lettre et non par un chiffre. Le nom de périphérique n'accepte ni les espaces, ni les points (.)
- *Étape 13* Cliquez sur Next (Suivant).
  Vous êtes redirigé vers une page web sur laquelle vous pouvez modifier le mot de passe de l'administrateur.
- *Étape 14* Changez le mot de passe de l'administrateur en saisissant le nouveau mot de passe dans le champ Password (Mot de passe).
  Pour vérifier le mot de passe, saisissez-le à nouveau dans le champ Verify Password (Vérifier le mot de passe).
- *Étape 15* Cliquez sur Next (Suivant).

Vous êtes redirigé vers une page sur laquelle vous pouvez saisir la date, l'heure et le fuseau horaire pour ce périphérique.

- *Étape 16* Tapez la date, l'heure et le fuseau horaire pour le périphérique. Les options disponibles sont :
  - **Time Zone (Fuseau horaire)** —Sélectionnez un fuseau horaire dans le menu déroulant.
  - **Date/Time (Date/Heure)** —Sélectionnez la date et l'heure courantes dans les menus déroulants.
  - **Synchronize with an Internet time server automatically (Synchroniser automatiquement avec un serveur de temps Internet)** —Pour obtenir automatiquement l'heure à partir d'un serveur NTP, cochez cette case.
  - **Server (Serveur)** —Dans la liste déroulante, sélectionnez le nom du serveur NTP et cliquez sur TEST pour en vérifier l'état.
    Par exemple :
    - time-a.timefreq.bldrdoc.gov (valeur par défaut)
    - time-b.timefreq.bldrdoc.gov
    - time-c.timefreq.bldrdoc.gov
  - **Set the device time the same as your computer time (Aligner l'heure du périphérique sur celle de votre ordinateur)** —Pour synchroniser l'heure/l'horloge du périphérique avec l'heure/ l'horloge de votre ordinateur, cochez cette case.
- *Étape 17* Cliquez sur Next (Suivant).
  Vous êtes redirigé vers une page sur laquelle vous pouvez saisir l'adresse IP, le masque de sous-réseau et la passerelle par défaut pour le périphérique.
- Étape 18 Entrez l'adresse IP, le masque de sous-réseau et la passerelle par défaut pour ce périphérique. Vous pouvez choisir soit d'acquérir automatiquement l'adresse IP à partir d'un serveur DHCP, soit de configurer une adresse IP statique.
  - **Obtain TCP/IP settings automatically via DHCP (Obtenir les paramètres TCP/IP automatiquement via DHCP)** —Cochez cette case pour obtenir l'adresse IP à partir d'un serveur DHCP.
    Cette option est activée par défaut.
  - Cliquez sur **Use the following settings (Utiliser les paramètres suivants)** pour configurer une adresse IP statique :
    - **IP Address (Adresse IP)** —Saisissez une adresse IP pour le NAS.
    - **Subnet Mask (Masque de sous-réseau)** —Saisissez le masque de sous-réseau de votre réseau.
    - **Default Gateway (Passerelle par défaut)** —Saisissez l'adresse de la passerelle par défaut. Il s'agit en général de l'adresse IP de votre routeur.
    - **Primary DNS Server (serveur DNS primaire)** (optionnel) —Saisissez l'adresse IP du serveur DNS (Domain Name System). Cette adresse est en général fournie par votre fournisseur d'accès Internet (FAI).
    - **Secondary DNS Server (Serveur DNS secondaire)** (optionnel) —Saisissez un second serveur DNS.
- Étape 19 Cliquez sur Next (Suivant).
  Vous êtes redirigé vers une page sur laquelle vous pouvez sélectionner les services à activer.
- *Étape 20* Sélectionnez les services à activer. Ces services peuvent aussi être activés ou désactivés ultérieurement. Les options disponibles sont :
  - **Network services (Services réseau)** —Cochez la case pour activer Microsoft Networking, Apple Networking ou Unix/Linux NFS.
  - **File services (Services fichiers)** —Cochez la case pour activer Web File Manager (Gestionnaire de fichiers web), FTP Service (Service FTP) ou Download Station (Station de téléchargement).
  - **Multimedia services (Services multimédias)** —Cochez la case pour activer Multimedia Station (Station multimédia), le serveur multimédia UPnP ou le service iTunes.

- **Web server services (Services serveur web)** —Cochez la case pour activer Web Server (Serveur web) ou le serveur MySQL.

- *Étape 21* Cliquez sur Next (Suivant).
  Vous êtes redirigé vers une page web sur laquelle vous pouvez sélectionner la configuration du disque.
- *Étape 22* Sélectionnez la configuration du disque. Les options disponibles sont :
  - Disk configuration (Configuration de disque) :
    - **Do not set disk configuration (Ne pas définir la configuration de disque)** —Si vous avez créé une configuration de volume de disque ou prévoyez de créer des configurations de disque multiples, sélectionnez cette option pour ne pas initialiser les unités de disque.
    - **Single (Unique)** —Chaque disque est utilisé comme un disque autonome. Si un disque est endommagé, toutes les données sur le disque endommagé seront perdues.
    - **JBOD—JBOD** vous permet de combiner plusieurs disques de capacités différentes en un seul périphérique de stockage logique. La capacité de la matrice JBOD correspond à la somme des capacités totales des disques individuels membres de la matrice (en d'autres termes, vous ne subissez pas la limitation du mode RAID0 dans lequel vous perdez de a capacité lorsque vous utilisez des disques de tailles différentes). Le mode JBOD n'offre pas d'augmentation des performances par rapport aux disques membres de la matrice. Sa fiabilité est inférieure à celle des disques membres de la matrice, car la défaillance d'un seul disque provoque, en général, la défaillance de l'ensemble de la matrice.
    - **RAID 0**—Permet de distribuer les données sur deux disques (on parle d'entrelacement) de façon à avoir une vitesse améliorée tout en utilisant l'ensemble de la capacité. En cas de défaillance d'un disque, toutes les données sur tous les disques seront perdues.
    - **RAID 1**—Utilise deux disques (disques en miroir) qui contiennent tous deux les mêmes données, de sorte que les données ne sont pas perdues en cas de défaillance d'un disque. La capacité totale de la matrice équivaut à la capacité du plus petit des disques (par défaut).
  - File system (Système de fichiers) :
    - **EXT4—EXT4** est le successeur du système EXT3 et donne de meilleures performances car le système de fichiers EXT4 est capable de prendre en charge les volumes très volumineux (valeur par défaut).
    - **EXT3—EXT3** est couramment utilisé dans l'environnement Linux. EXT3 apporte des systèmes de fichiers fiables avec la prise en charge d'une capacité maximum de 16 téra-octets (To).
  - Encrypt disk volume (Crypter le volume de disque) :
    - **No (Non)** —Ne pas crypter le volume de disque (valeur par défaut).
    - **Yes (Oui)** —Crypter le volume de disque à l'aide d'un mot de passe.

  Si vous choisissez oui, le volume de disque est crypté avec un mot de passe et cela apporte une couche supplémentaire de sécurité contre le vol des données dans le cas où les disques seraient volés. Les performances de transfert des fichiers vers les volumes cryptés sont en général moindres que pour les volumes non cryptés. Le mot de passe de cryptage par défaut est le mot de passe du compte «admin».
- *Étape 23* Cliquez sur Next (Suivant).
  La fenêtre Finish (Terminer) affiche la configuration du périphérique.
- *Étape 24* Cliquez sur Start Installation (Lancer l'installation). Le système lance l'initialisation et la progression de la configuration est affichée.
  Lorsque la configuration est terminée, le système vous ramène sur la page Configuring the NAS (Configuration du NAS) dans l'Assistant de configuration.
- *Étape 25* Sur la page Configuring the NAS (Configuration du NAS), cliquez sur Next (Suivant) pour continuer sur Map a Network Drive (Mapper une unité réseau).
  La page Map a Network Drive (Mapper une unité réseau) s'affiche.

1.2.6 Mappage d'une unité réseau

Vous pouvez mapper une unité réseau soit par le biais de l'Assistant de configuration, soit à partir de Windows.

a. Mappage d'une unité réseau avec l'Assistant de configuration

REMARQUE Ignorez les étapes 1 à 5 si vous êtes déjà sur la page Map Network Drive (Mapper une unité réseau) dans l'Assistant de configuration.

- *Étape 1* Insérez le produit du CD et, sur la page Welcome (Bienvenue), cliquez sur **NSS 322**.
  La page NSS 322 Setup Menu (Menu de configuration du NSS 322) s'affiche.
- *Étape 2* Sous First Time Installation (Première installation), cliquez sur **Setup (Configuration)**.
  La page First Time Installation Wizard (Assistant de Première installation) s'affiche.
- *Étape 3* Cliquez sur **Next (Suivant)** pour lancer l'assistant.
  La page End-User License Agreement (Accord de licence de l'utilisateur final) s'affiche.
- *Étape 4* Pour accepter l'Accord de l'utilisateur final, cochez la case **I accept this agreement (J'accepte cet accord)** et cliquez sur **Next (Suivant)**.
  La page Hardware Installation Guide (Guide d'installation du matériel) s'affiche.
- *Étape 5* Cliquez sur **Skip (Ignorer)** jusqu'à ce que vous arriviez à la page Map Network Drive (Mapper une unité réseau).
- *Étape 6* Sur la page Map Network Drive (Mapper une unité réseau), cliquez sur **Next (Suivant)** pour commencer à mapper votre unité réseau.
  La page Discovering the NAS (Découverte du NAS) s'affiche et l'Assistant de Première installation cherche votre NAS initialisé.
- *Étape 7* Lorsque le NAS initialisé a été trouvé, cliquez sur **Next (Suivant)**.
  La page Select the NAS Device (Sélectionner le périphérique NAS) s'affiche.
- *Étape 8* Dans la liste déroulante, sélectionnez le périphérique NAS que vous voulez mapper comme unité réseau.
- *Étape 9* Cliquez sur **Next (Suivant)**.
  La page Mapping Drives (Mappage des unités) s'affiche.
- *Étape 10* Dans les listes déroulantes, sélectionnez un type de dossier et sélectionnez la lettre d'unité à mapper.
  Les types de dossiers sont :
  - **Public**—Partage réseau pour le partage de fichiers (valeur par défaut).
  - **Usb**—Partage réseau pour fonction de copie des données par le biais des ports USB.
  - **Web**—Partage réseau pour serveur web.
  - **Download (Téléchargement)** —Partage réseau pour Download Station (Station de téléchargement).
  - **Multimedia (Multimédia)** —Partage réseau pour Multimedia Station (Station multimédia).
  - **Network Recycle Bin 1 (Corbeille réseau 1)** —Corbeille du partage réseau.
- *Étape 11* À partir de la page d'ouverture de session d'authentification, tapez le nom d'utilisateur et le mot de passe du compte administrateur.
- *Étape 12* Cliquez sur **Next (Suivant)**.
  La page Mapping Success (Mappage réussi) s'affiche.
- *Étape 13* Cliquez sur **More (Plus)** pour mapper une autre unité ou cliquez sur **Next (Suivant)** pour continuer sur Client Utility Installation (Installation utilitaire client).

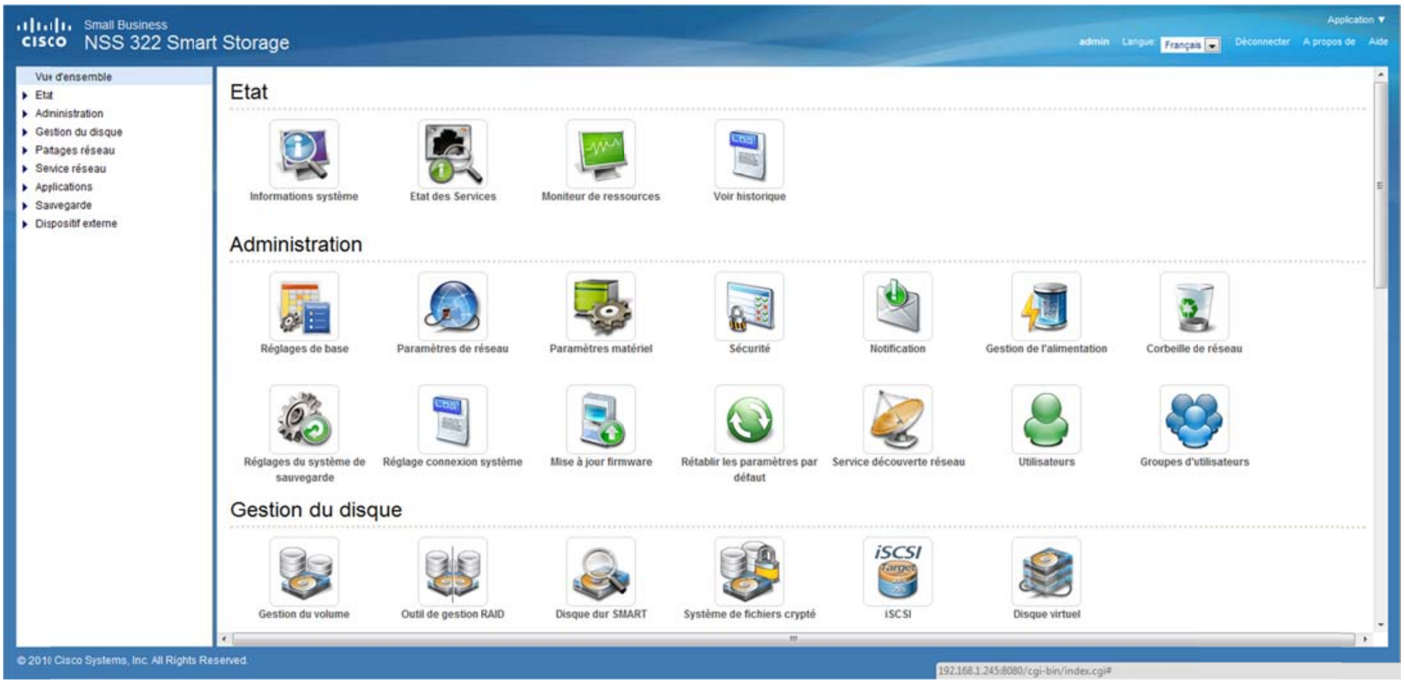
b. Mappage d'une unité réseau à partir de Windows

REMARQUE Si vous utilisez Windows Vista, il se peut que vous receviez une alerte de sécurité et que vous deviez temporairement désactiver tout logiciel de sécurité sur votre ordinateur.

- *Étape 1* Sur le bureau de Windows, cliquez sur l'icône **Poste de travail** pour ouvrir le Poste de travail.
- *Étape 2* Choisissez **Tools (Outils) > Map Network Drive (Mapper une unité réseau)**.
  La fenêtre Map a Network Drive (Mapper une unité réseau) s'affiche.
- *Étape 3* Dans les listes déroulantes, sélectionnez la lettre de l'unité à mapper.
- *Étape 4* Dans le champ Folder (Dossier), tapez le nom du dossier de partage que vous voulez mapper. Par exemple : **\\<adresse IP du NAS>\<nom du dossier de partage>**
- *Étape 5* Cliquez sur **OK**.
- *Étape 6* Cliquez sur **Finish (Terminer)**.
  REMARQUE Si le système vous demande de saisir un nom d'utilisateur et un mot de passe pour authentification, saisissez le nom d'utilisateur et le mot de passe du compte d'administrateur.
- *Étape 7* Ouvrez Windows Explorer pour afficher et utiliser le partage réseau comme une unité locale.

1.2.7 Accès à l'interface graphique de gestion à l'aide d'un navigateur web

- *Étape 1* Ouvrez un navigateur web et saisissez l'adresse IP du périphérique NAS. Il est important d'inclure le port 8080 après l'adresse IP.
  Par exemple :
  http://<adresse IP du NAS>:8080
- *Étape 2* Lorsque la page d'ouverture de session s'affiche, saisissez le nom d'utilisateur et le mot de passe administrateur.
  Le mot de passe par défaut est « admin » pour l'administrateur « admin ».

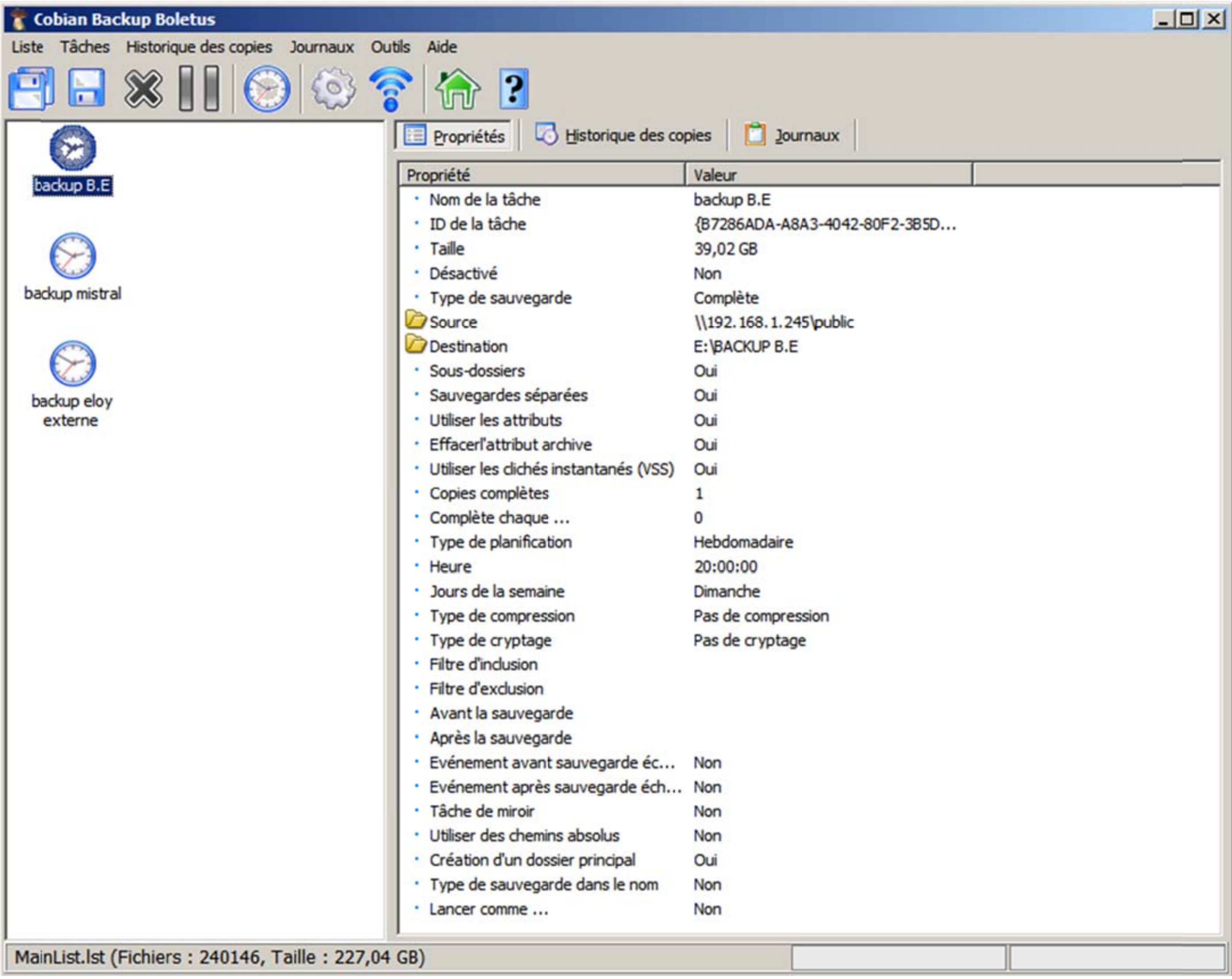


1.2.8 Sauvegarde du NAS

Les deux disques durs du NAS ont été installés en RAID 1, mais il a été demandé de faire une sauvegarde des données pour combler toutes erreurs de suppression malencontreuse.

Le NAS dispose de plusieurs systèmes de sauvegarde mais automatisé, il ne dispose que de sa réplication distante.

Le souci est qu'étant basé sur un O.S. Linux il ne peut répliquer ses données que vers un autre NAS ou un serveur Rsync. Après plusieurs essais pour installer un module rsync sur notre serveur SBS, j'ai pris le problème à l'envers et décider d'installer un logiciel de backup open source sur le serveur SBS qui lui, s'occupera de faire la sauvegarde périodiquement.



2. Commutateur Cisco SG 100D-08 (SD2008T), 8 ports Gigabit Ethernet.

La gamme des commutateurs de la gamme Cisco 100 est couverte par une garantie limitée à vie, avec retour atelier pour remplacement (garantie limitée de 1 an pour les ventilateurs et les alimentations). De plus, Cisco propose une assistance téléphonique gratuite les 12 premiers mois suivant la date de l'achat.

Caractéristiques SG 100D-08 (SD2008T) :

- Huit ports de commutation 10/100/1000 autosensing avec détection automatique de la liaison MDI/MDI-X
- Contrôle de flux 802.3x
- Commutation non bloquante
- Apprentissage d'adresse, dépassement d'adresse et contrôle du flux de données pour une fiabilité de transmission optimale
- Support des trames jumbo (9 Ko)
- Boitier robuste en métal
- Alimentation externe
- Montage mural possible
- Pas de ventilateur, totalement silencieux

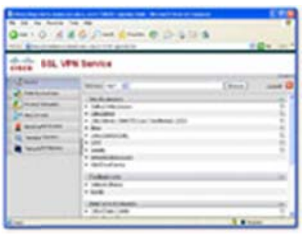
XI. Dispositifs de sécurité adaptative Cisco ASA 5505

1. Description

Réunissant sur une même plate- Réunissant sur une même plate-forme une combinaison puissante de nombreuses technologies éprouvées, la gamme Cisco ASA 5500 (Adaptive Security Appliance) donne à l'entreprise les moyens opérationnels et économiques de déployer des services de sécurité complets vers un grand nombre de sites

- Plus de sécurité, avec le support de nouveaux services de sécurité, tels l'IPS et l'Anti-X avec accélération matérielle (modules optionnels).
- Plus de performances et d'évolutivité.
- Une solution VPN-SSL avec ou sans client, dotée de fonctionnalités de haut niveau.
- Une migration douce, préservant les compétences acquises autour du PIX.

1.1 Technologie reconnue de firewall et VPN protégé contre les menaces



Développée autour de la même technologie éprouvée qui a fait le succès du serveur de Développée autour de la même technologie éprouvée qui a fait le succès du serveur de sécurité Cisco PIX et de la gamme des concentrateurs Cisco VPN 3000, la gamme Cisco ASA 5000 est la première solution à proposer des services VPN SSL (Secure Sockets Layer) et IPsec (IP Security) protégés par la première technologie de firewall du marché. Avec le VPN SSL, l'ASA 5500 est une passerelle SSL performante qui permet l'accès distant sécurisé au réseau d'un navigateur web banalisé pour les utilisateurs nomades.

1.2 Service évolué de prévention des intrusions

Les services proactifs de prévention des intrusions offrent toutes les fonctionnalités qui permettent de bloquer un large éventail de menaces – vers, attaques sur la couche applicative ou au niveau du système d'exploitation, rootkits, logiciels espions, messagerie instantanée, P2P, et bien plus encore. En combinant plusieurs méthodes d'analyse détaillée du trafic, l'IPS de l'ASA 5500 protège le réseau des violations de politique de sécurité, de l'exploitation des vulnérabilités des systèmes et du trafic anormal. L'IPS collabore avec d'autres systèmes Cisco de gestion de la sécurité pour assurer une mise à jour constante de la posture de sécurité du réseau et une réactivité totale aux nouvelles attaques ou vulnérabilités.

1.3 Systèmes ANTI-X à la pointe de l'industrie

La gamme Cisco ASA 5500 offre des services complets Anti-X à la pointe de la technologie – protection contre les virus, les logiciels espions, le courrier indésirable et le phishing ainsi que le blocage de fichiers, le blocage et le filtrage des URL et le filtrage de contenu – en associant le savoir-faire de Trend Micro en matière de protection informatique à une solution Cisco de sécurité réseau éprouvée. Ces services Anti-X embarqués dans le module d'extension hardware CSC SSM et le renouvellement des abonnements Trend Micro p la gamme ASA sont commercialisés par Cisco au travers de ses partenaires agréés.

1.4 Migration transparente pour l'utilisateur

Les utilisateurs actuels des serveurs de sécurité PIX n'auront aucune difficulté à s'adapter aux solutions Cisco ASA 5500. Les fichiers de configuration des Cisco PIX sont transposables sur les serveurs ASA 5500. Le logiciel d'administration graphique Cisco Adaptive Security Device Manager (ASDM) livré avec la gamme ASA est un logiciel puissant et facile à utiliser. Il accélère la création de politique de sécurité, et réduit la charge de travail et les erreurs humaines, grâce à des assistants graphiques, des outils de débogage et de surveillance. ASDM permet de gérer aussi bien des serveurs Cisco PIX que des serveurs ASA 5500, facilitant la migration vers la dernière génération de matériel et ses nouvelles fonctions.

1.5 ASA 5505

Le Cisco ASA 5505 est un Serveur de Sécurité Adaptatif complet de prochaine génération destiné aux petites entreprises, aux agences d'entreprise et aux environnements de télétravail. De conception modulaire et utilisable dès l'installation (« plug and pay »),il offre des services haute performance de firewall, de VPN SSL et IPSec ainsi que des services de réseau multifonctions. Son gestionnaire Web intégré, Cisco Adaptive Security Device Manager, permet de déployer rapidement et de gérer en toute simplicité le Cisco ASA 5505, contribuant ainsi à réduire les frais d'exploitation de l'entreprise. Le Cisco ASA 5505 est doté d'un commutateur Fast Ethernet à 8 ports qui peuvent être groupés dynamiquement afin de créer jusqu'à trois VLAN distincts pour l'utilisation domestique, les besoins professionnels et le trafic Internet – une répartition qui améliore la segmentation du trafic et la sécurité du réseau. Le Cisco ASA 5505 dispose également de deux ports à alimentation en ligne PoE (Power over Ethernet) pour simplifier le déploiement de téléphones IP Cisco avec leurs fonctionnalités VoIP automatiques sécurisées, et celui de points d'accès extérieurs sans fil pour apporter la mobilité au réseau. Particulièrement évolutif, comme les autres modèles de la gamme, le Cisco ASA 5505 protège les investissements grâce à sa conception modulaire et dispose d'un emplacement d'extension et de plusieurs ports USB en prévision de futurs services.

A mesure que les besoins de l'entreprise augmenteront, vous pourrez installer une licence Security Plus complémentaire qui permettra au Serveur de Sécurité Adaptatif Cisco ASA 5505 d'évoluer pour supporter des capacités plus importantes de connexion et un plus grand nombre d'utilisateurs VPN IPSec, le support d'une zone démilitarisée (DMZ) et l'intégration aux environnements de réseau commuté avec le support des lignes réseaux VLAN. Plus encore, cette licence de mise à niveau maximise la continuité de l'entreprise en offrant un support pour les connexions redondantes vers les fournisseurs d'accès Internet et des services de haute disponibilité à inspection d'état Actif/Veille. Grâce à cette combinaison de services de sécurité et VPN à la pointe de l'industrie, de fonctionnalités réseaux évoluées, de gestion à distance et d'extensibilité, le Cisco ASA 5505 constitue la solution idéale de sécurité haut de gamme pour les petites entreprises, les agences et les télétravailleurs.

1.6 Fonctionnalités et capacités du Serveur de Sécurité Adaptatif Cisco ASA 5505

Fonction	Description
Débit du firewall	Jusqu'à 150 Mbits/s
Débit du VPN	Jusqu'à 100 Mbits/s
Connexions	10 000 ; 25 000*
Homologues VPN IPsec	10 ; 25 *
Niveaux de licence des homologues VPN SSL**	10, ou 25
Interfaces	Commutateur Fast Ethernet 8 ports avec groupage dynamique des ports (dont 2 ports PoE)
Interfaces virtuelles (VLAN)	3 (sans support de l'agrégation de VLAN)/20 (avec support de l'agrégation de VLAN) *
Haute disponibilité	Non prise en charge ; mode actif/veille à inspection d'état et support ISP redondant *

* Mise à niveau disponible avec la licence Security Plus de Cisco ASA 5505

** Fonction fournie sous licence distincte ; licence pour 2 homologues incluse dans le système de base

2. Configuration

2.1 Configuration par défaut de l'ASA 5505

Les appliances de sécurité Cisco sont livrés par défaut avec une configuration d'usine qui leur permet un démarrage rapide. Cette configuration répond aux besoins de la plupart des environnements réseaux des petites et moyennes entreprises. Par défaut, l'appareil de sécurité est configuré comme suit :

L'interface interne est configuré avec un pool d'adresse DHCP par défaut

Configurez votre PC pour utiliser DHCP (pour recevoir automatiquement une adresse IP de l'appareil de sécurité), ou attribuer une adresse IP statique à votre PC en sélectionnant une adresse sur le réseau 192.168.1.0 (les adresses valides sont 192.168.1.2 à 192.168.1.254 avec un masque de 255.255.255.0 et la route par défaut 192.168.1.1.).

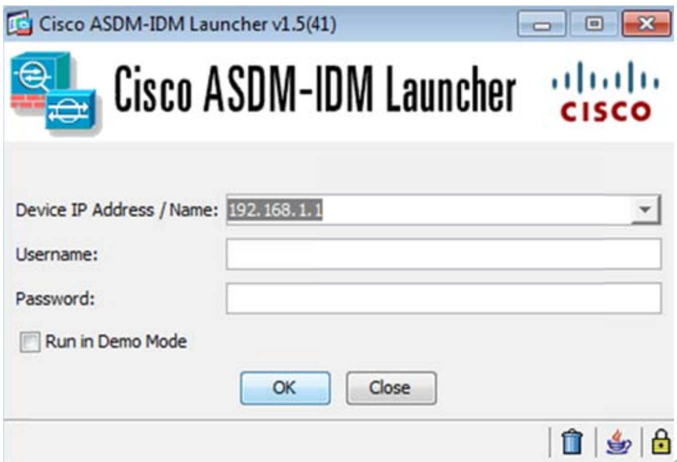
Cette configuration permet à un client du réseau interne d'obtenir une adresse DHCP de l'appareil de sécurité afin de s'y connecter. Les administrateurs peuvent alors configurer et gérer le dispositif de sécurité en utilisant ASDM

L'interface de sortie est configurée pour refuser tout trafic entrant par le biais de cette interface.

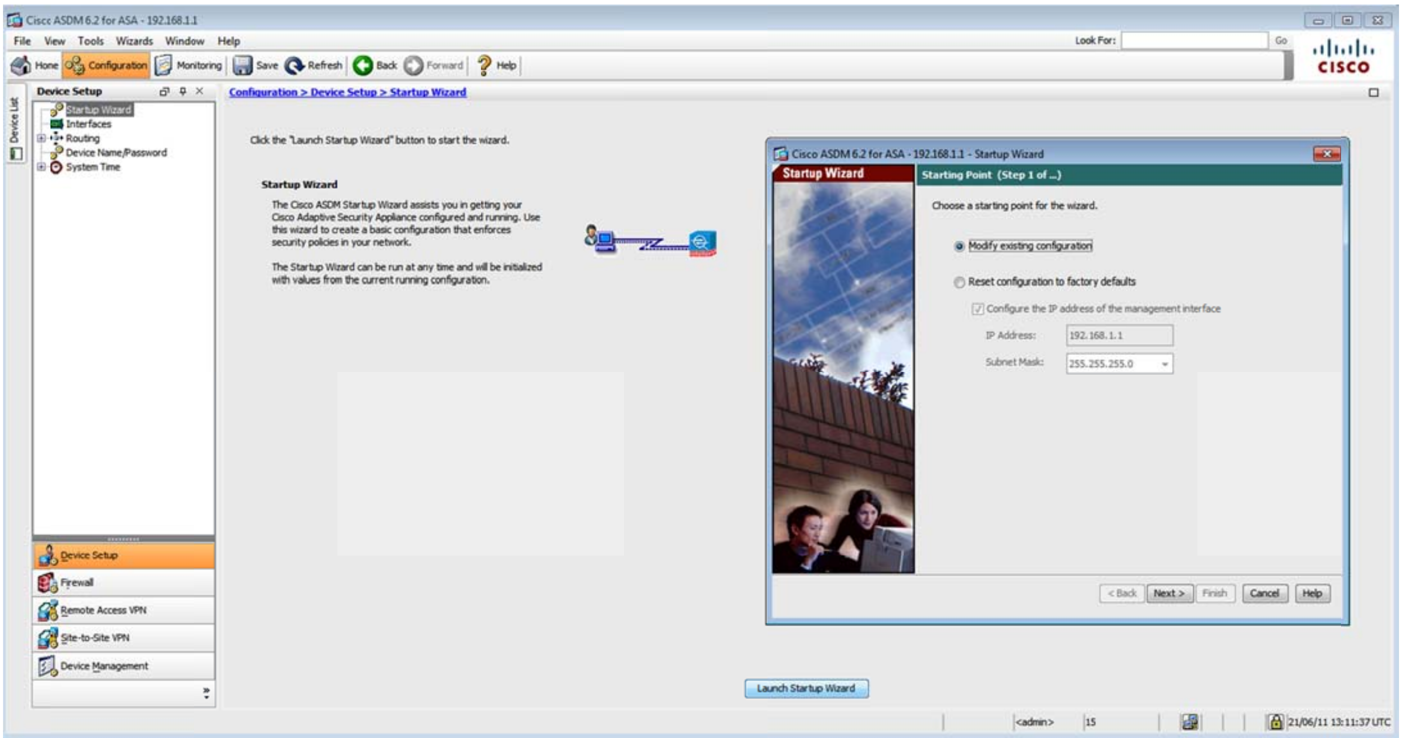
Cette configuration protège votre réseau interne de tout trafic non sollicité.

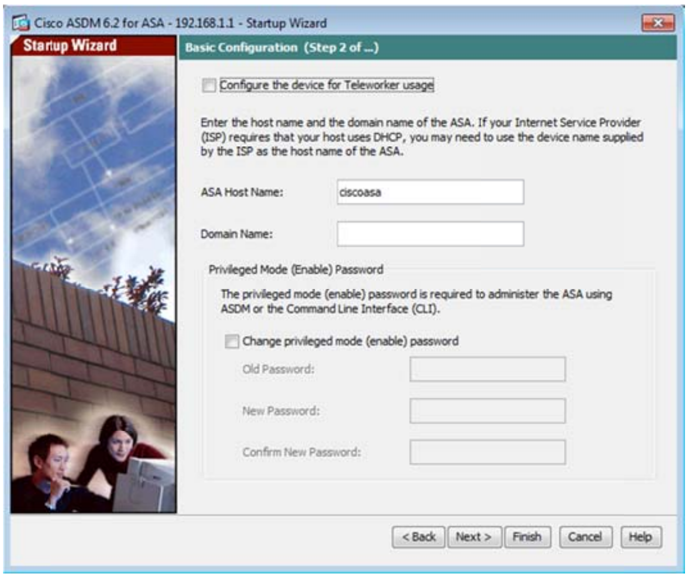
2.2 L'Adaptive Security Device Manager

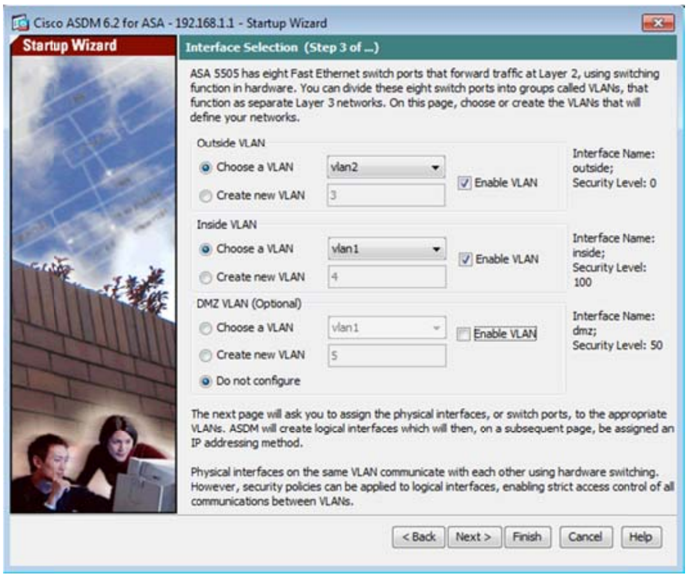
L'Adaptive Security Device Manager (ASDM) est une interface graphique riche en fonctionnalités qui vous permet de gérer et de surveiller l'appareil de sécurité. De conception basée sur le web, il offre un accès sécurisé pour vous permettre de vous y connecter en toute sécurité de n'importe quel endroit en utilisant un navigateur web.

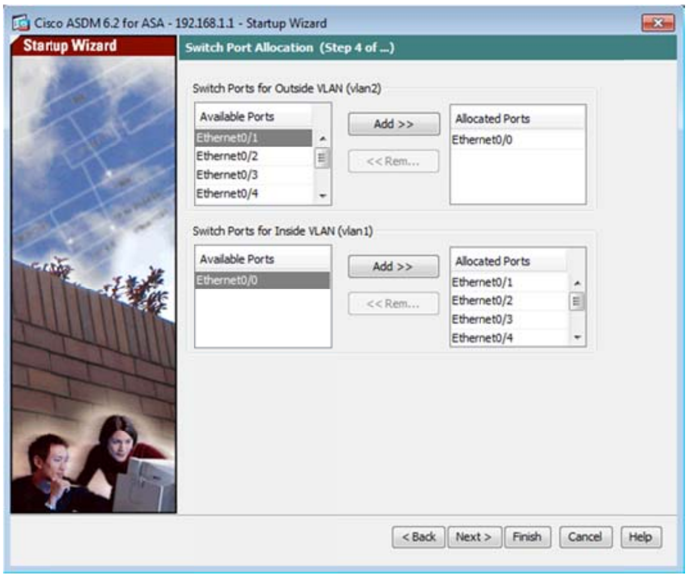


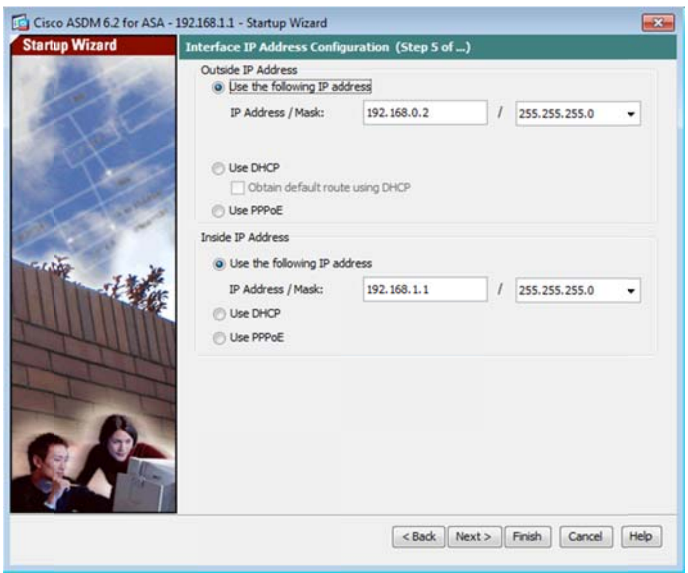
En complément des capacités de configuration et de gestion, ASDM simplifie et accélère le déploiement du dispositif de sécurité. Pour exécuter ASDM, vous devrez avoir une licence DES ou 3DES-AES. En outre Java et JavaScript doivent être activés dans votre navigateur web.

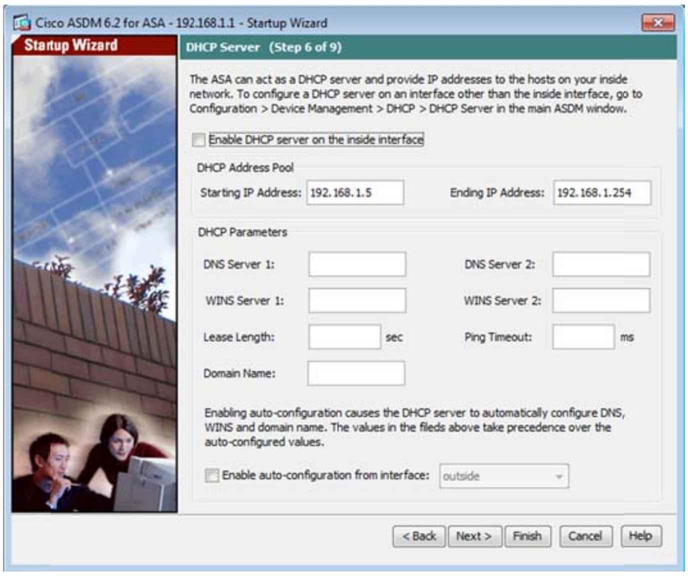

Cisco ASDM 6.2 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Look For:
Go
Device Setup
Startup Wizard
Interfaces
Routing
Device Name/Password
System Time
Configuration > Device Setup > Startup Wizard
Click the "Launch Startup Wizard" button to start the wizard.
Startup Wizard
The Cisco ASDM Startup Wizard assists you in getting your Cisco Adaptive Security Appliance configured and running. Use this wizard to create a basic configuration that enforces security policies in your network.
The Startup Wizard can be run at any time and will be initialized with values from the current running configuration.
Cisco ASDM 6.2 for ASA - 192.168.1.1 - Startup Wizard
Startup Wizard
Starting Point (Step 1 of ...)
Choose a starting point for the wizard.
Modify existing configuration
Reset configuration to factory defaults
Configure the IP address of the management interface
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
< Back Next > Finish Cancel Help
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Launch Startup Wizard
<admin> 15
21/06/11 13:11:37 UTC

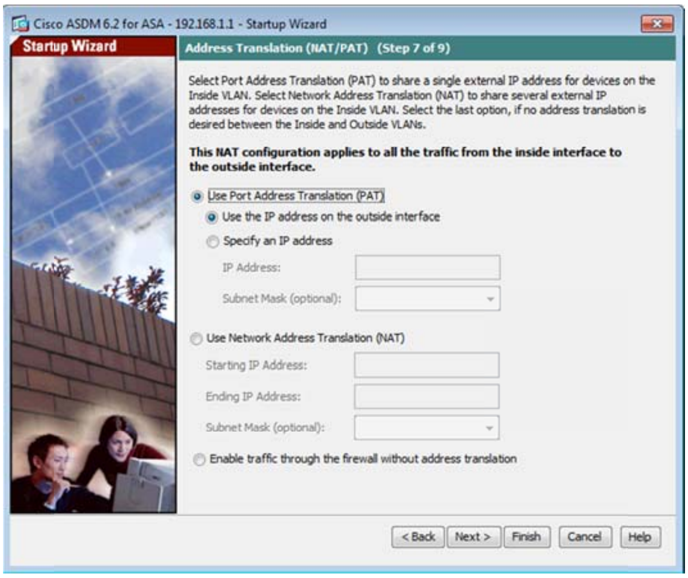

Cisco ASDM 6.2 for ASA - 192.168.1.1 - Startup Wizard
Startup Wizard
Basic Configuration (Step 2 of ...)
Configure the device for Teleworker usage
Enter the host name and the domain name of the ASA. If your Internet Service Provider (ISP) requires that your host uses DHCP, you may need to use the device name supplied by the ISP as the host name of the ASA.
ASA Host Name: ciscoasa
Domain Name:
Privileged Mode (Enable) Password
The privileged mode (enable) password is required to administer the ASA using ASDM or the Command Line Interface (CLI).
Change privileged mode (enable) password
Old Password:
New Password:
Confirm New Password:
< Back Next > Finish Cancel Help

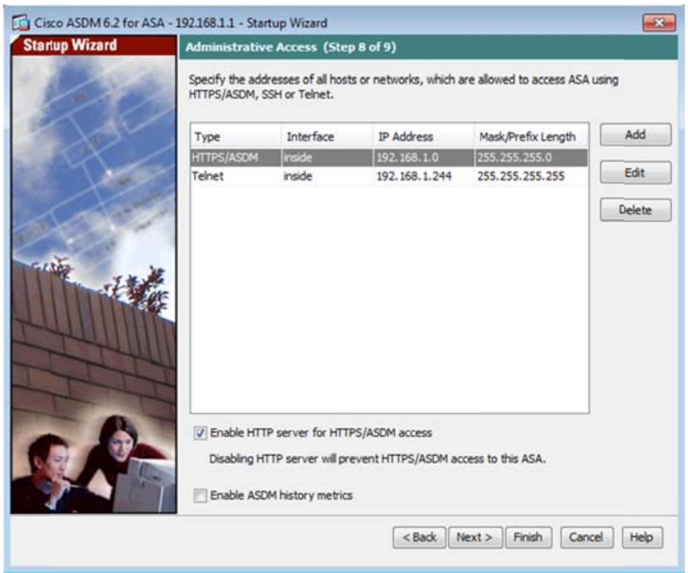

Cisco ASDM 6.2 for ASA - 192.168.1.1 - Startup Wizard
Startup Wizard
Interface Selection (Step 3 of ...)
ASA 5505 has eight Fast Ethernet switch ports that forward traffic at Layer 2, using switching function in hardware. You can divide these eight switch ports into groups called VLANs, that function as separate Layer 3 networks. On this page, choose or create the VLANs that will define your networks.
Outside VLAN
Choose a VLAN vlan2
Create new VLAN 3
Enable VLAN
Interface Name: outside; Security Level: 0
Inside VLAN
Choose a VLAN vlan1
Create new VLAN 4
Enable VLAN
Interface Name: inside; Security Level: 100
DMZ VLAN (Optional)
Choose a VLAN vlan1
Create new VLAN 5
Do not configure
Enable VLAN
Interface Name: dmz; Security Level: 50
The next page will ask you to assign the physical interfaces, or switch ports, to the appropriate VLANs. ASDM will create logical interfaces which will then, on a subsequent page, be assigned an IP addressing method.
Physical interfaces on the same VLAN communicate with each other using hardware switching. However, security policies can be applied to logical interfaces, enabling strict access control of all communications between VLANs.
< Back Next > Finish Cancel Help

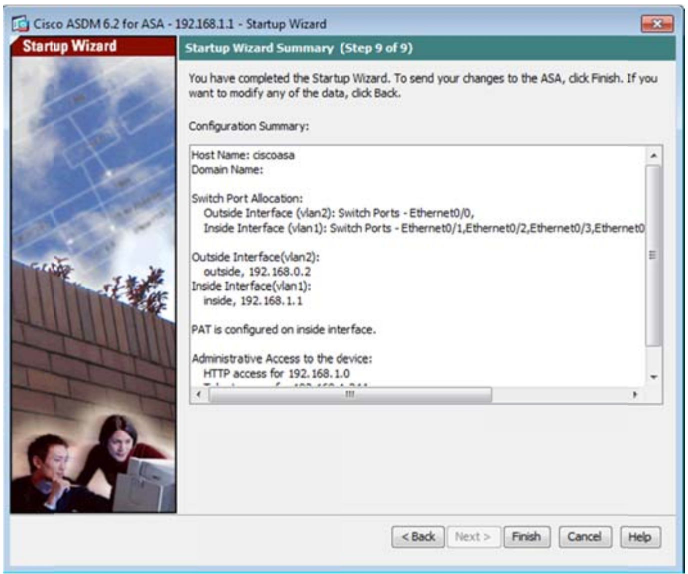

Cisco ASDM 6.2 for ASA - 192.168.1.1 - Startup Wizard
Startup Wizard
Switch Port Allocation (Step 4 of ...)
Switch Ports for Outside VLAN (vlan2)
Available Ports
Ethernet0/1
Ethernet0/2
Ethernet0/3
Ethernet0/4
Add >>
<< Rem...
Allocated Ports
Ethernet0/0
Switch Ports for Inside VLAN (vlan1)
Available Ports
Ethernet0/0
Add >>
<< Rem...
Allocated Ports
Ethernet0/1
Ethernet0/2
Ethernet0/3
Ethernet0/4
< Back Next > Finish Cancel Help

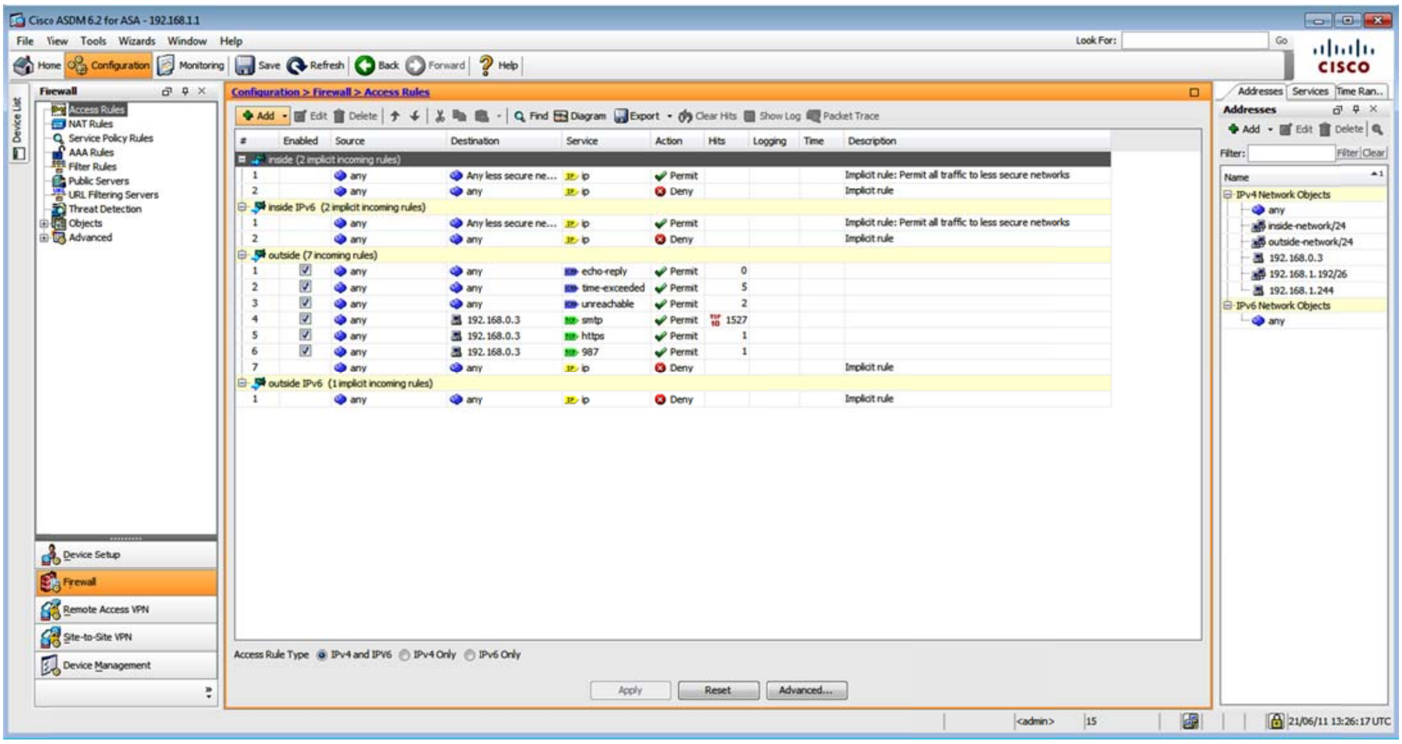

Cisco ASDM 6.2 for ASA - 192.168.1.1 - Startup Wizard
Startup Wizard
Interface IP Address Configuration (Step 5 of ...)
Outside IP Address
Use the following IP address
IP Address / Mask: 192.168.0.2 / 255.255.255.0
Use DHCP
Obtain default route using DHCP
Use PPPoE
Inside IP Address
Use the following IP address
IP Address / Mask: 192.168.1.1 / 255.255.255.0
Use DHCP
Use PPPoE
< Back Next > Finish Cancel Help


Cisco ASDM 6.2 for ASA - 192.168.1.1 - Startup Wizard
Startup Wizard
DHCP Server (Step 6 of 9)
The ASA can act as a DHCP server and provide IP addresses to the hosts on your inside network. To configure a DHCP server on an interface other than the inside interface, go to Configuration > Device Management > DHCP > DHCP Server in the main ASDM window.
Enable DHCP server on the inside interface
DHCP Address Pool
Starting IP Address: 192.168.1.5
Ending IP Address: 192.168.1.254
DHCP Parameters
DNS Server 1:
DNS Server 2:
WINS Server 1:
WINS Server 2:
Lease Length: sec
Ping Timeout: ms
Domain Name:
Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and domain name. The values in the fields above take precedence over the auto-configured values.
Enable auto-configuration from interface: outside
< Back
Next >
Finish
Cancel
Help


Cisco ASDM 6.2 for ASA - 192.168.1.1 - Startup Wizard
Startup Wizard
Address Translation (NAT/PAT) (Step 7 of 9)
Select Port Address Translation (PAT) to share a single external IP address for devices on the Inside VLAN. Select Network Address Translation (NAT) to share several external IP addresses for devices on the Inside VLAN. Select the last option, if no address translation is desired between the Inside and Outside VLANs.
This NAT configuration applies to all the traffic from the inside interface to the outside interface.
Use Port Address Translation (PAT)
Use the IP address on the outside interface
Specify an IP address
IP Address:
Subnet Mask (optional):
Use Network Address Translation (NAT)
Starting IP Address:
Ending IP Address:
Subnet Mask (optional):
Enable traffic through the firewall without address translation
< Back
Next >
Finish
Cancel
Help


Cisco ASDM 6.2 for ASA - 192.168.1.1 - Startup Wizard
Startup Wizard
Administrative Access (Step 8 of 9)
Specify the addresses of all hosts or networks, which are allowed to access ASA using HTTPS/ASDM, SSH or Telnet.
Type | Interface | IP Address | Mask/Prefix Length
HTTPS/ASDM | inside | 192.168.1.0 | 255.255.255.0
Telnet | inside | 192.168.1.244 | 255.255.255.255
Add
Edit
Delete
Enable HTTP server for HTTPS/ASDM access
Disabling HTTP server will prevent HTTPS/ASDM access to this ASA.
Enable ASDM history metrics
< Back
Next >
Finish
Cancel
Help


Cisco ASDM 6.2 for ASA - 192.168.1.1 - Startup Wizard
Startup Wizard
Startup Wizard Summary (Step 9 of 9)
You have completed the Startup Wizard. To send your changes to the ASA, click Finish. If you want to modify any of the data, click Back.
Configuration Summary:
Host Name: ciscoasa
Domain Name:
Switch Port Allocation:
Outside Interface (vlan2): Switch Ports - Ethernet0/0,
Inside Interface (vlan1): Switch Ports - Ethernet0/1,Ethernet0/2,Ethernet0/3,Ethernet0
Outside Interface(vlan2):
outside, 192.168.0.2
Inside Interface(vlan1):
inside, 192.168.1.1
PAT is configured on inside interface.
Administrative Access to the device:
HTTP access for 192.168.1.0
< Back
Next >
Finish
Cancel
Help


Cisco ASDM 6.2 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Look For:
Go
Home
Configuration
Monitoring
Save
Refresh
Back
Forward
Help
CISCO
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Objects
Advanced
Configuration > Firewall > Access Rules
Add
Edit
Delete
Find
Diagram
Export
Clear Hits
Show Log
Packet Trace
| Enabled | Source | Destination | Service | Action | Hits | Logging | Time | Description
inside (2 implicit incoming rules)
1 | | any | Any less secure ne... | ip | Permit | | | | Implicit rule: Permit all traffic to less secure networks
2 | | any | any | ip | Deny | | | | Implicit rule
inside IPv6 (2 implicit incoming rules)
1 | | any | Any less secure ne... | ip | Permit | | | | Implicit rule: Permit all traffic to less secure networks
2 | | any | any | ip | Deny | | | | Implicit rule
outside (7 incoming rules)
1 | | any | any | echo-reply | Permit | 0
2 | | any | any | time-exceeded | Permit | 5
3 | | any | any | unreachable | Permit | 2
4 | | any | 192.168.0.3 | smtp | Permit | 1527
5 | | any | 192.168.0.3 | https | Permit | 1
6 | | any | 192.168.0.3 | 987 | Permit | 1
7 | | any | any | ip | Deny | | | | Implicit rule
outside IPv6 (1 implicit incoming rules)
1 | | any | any | ip | Deny | | | | Implicit rule
Access Rule Type IPv4 and IPv6 IPv4 Only IPv6 Only
Apply
Reset
Advanced...
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Addresses
Services
Time Ran..
Add
Edit
Delete
Filter:
Filter
Clear
Name
IPv4 Network Objects
any
inside-network/24
outside-network/24
192.168.0.3
192.168.1.192/26
192.168.1.244
IPv6 Network Objects
any
<admin>
15
21/06/11 13:26:17 UTC

2.3 Configuration en mode CLI

```
ASA Version 8.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 192.168.0.2 255.255.255.0
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
ftp mode passive
access-list 100 extended permit icmp any any echo-reply
access-list 100 extended permit icmp any any time-exceeded
access-list 100 extended permit icmp any any unreachable
access-list 100 extended permit tcp any host 192.168.0.3 eq smtp
access-list 100 extended permit tcp any host 192.168.0.3 eq https
access-list 100 extended permit tcp any host 192.168.0.3 eq 987
access-list inside_nat0_outbound extended permit ip 192.168.1.0 255.255.255.0 192.168.1.192 255.255.255.192
pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
ip local pool vpn_pool 192.168.1.220-192.168.1.243 mask 255.255.255.0
```

```
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
global (inside) 1 192.168.1.244 netmask 255.255.255.255
global (outside) 1 interface
global (outside) 2 192.168.0.3 netmask 255.0.0.0
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 0.0.0.0 0.0.0.0
static (inside,outside) 192.168.0.3 192.168.1.244 netmask 255.255.255.255
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.0.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.1.0 255.255.255.0 inside
http authentication-certificate outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set pfs group1
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set transform-set ESP-AES-128-SHA ESP-AES-128-MD5
ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-
SHA ESP-DES-MD5
crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
```

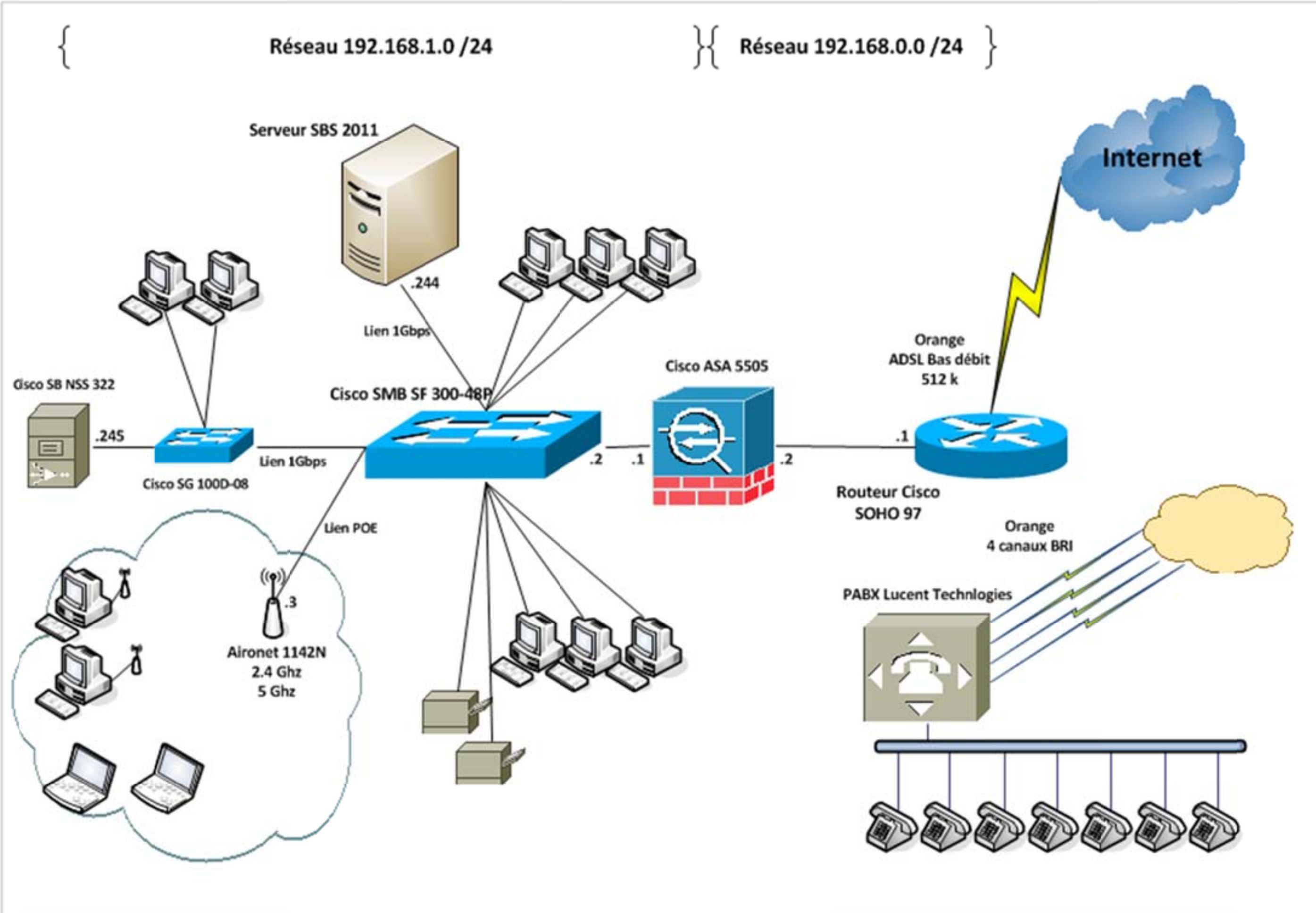
```
telnet 192.168.1.244 255.255.255.255 inside
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.254 inside
!

threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
group-policy remote_access internal
group-policy remote_access attributes
 dns-server value 192.168.1.244
 vpn-tunnel-protocol IPSec
 default-domain value eloy.local
username gestionprod password 5kecb/KYDxbJOZPg encrypted privilege 0
username gestionprod attributes
 vpn-group-policy remote_access
username logistique password TT0BKwQFLCo3UC90 encrypted privilege 0
username logistique attributes
 vpn-group-policy remote_access
username qualite password fSdA7eMuEG0DqxIh encrypted privilege 0
username qualite attributes
 vpn-group-policy remote_access
username transedi password e5UTJ1CWYtOcX1t0 encrypted privilege 0
username transedi attributes
 vpn-group-policy remote_access
username eric.vigouroux password lDhqioChs50Zioze encrypted privilege 0
username eric.vigouroux attributes
 vpn-group-policy remote_access
username chefprojets password Wf7KEaj54I3ueAmL encrypted privilege 0
username chefprojets attributes
 vpn-group-policy remote_access
username b.vives password zE8cu4J.Q6VW0uZF encrypted privilege 0
username b.vives attributes
 vpn-group-policy remote_access
username c.paoli password 70qQkpixnkIL4ZEi encrypted privilege 0
username c.paoli attributes
 vpn-group-policy remote_access
tunnel-group remote_access type remote-access
tunnel-group remote_access general-attributes
 address-pool vpn_pool
 default-group-policy remote_access
tunnel-group remote_access ipsec-attributes
 pre-shared-key *
!
```

```
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:68c0df732ea77e86e4679486770534d8
```

XII. Annexes

1. Topologie de la société après évolution



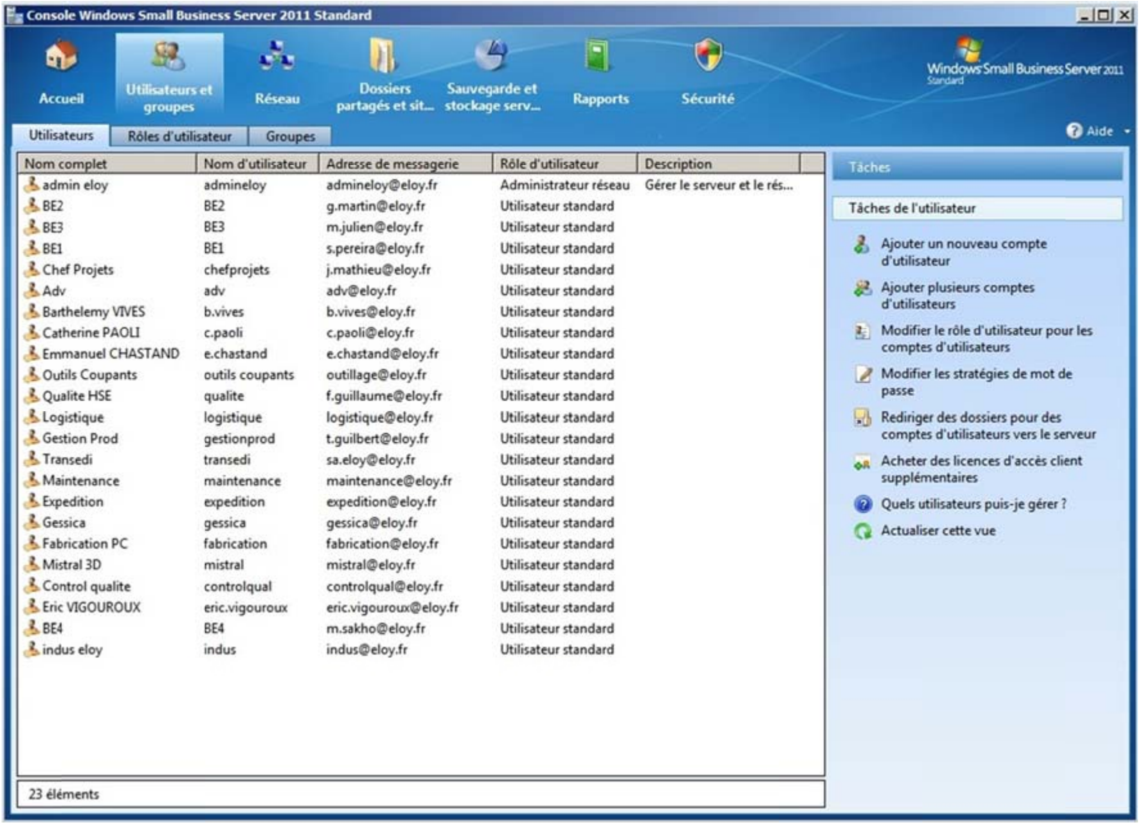
2. Tutoriel pour configuration utilisateur

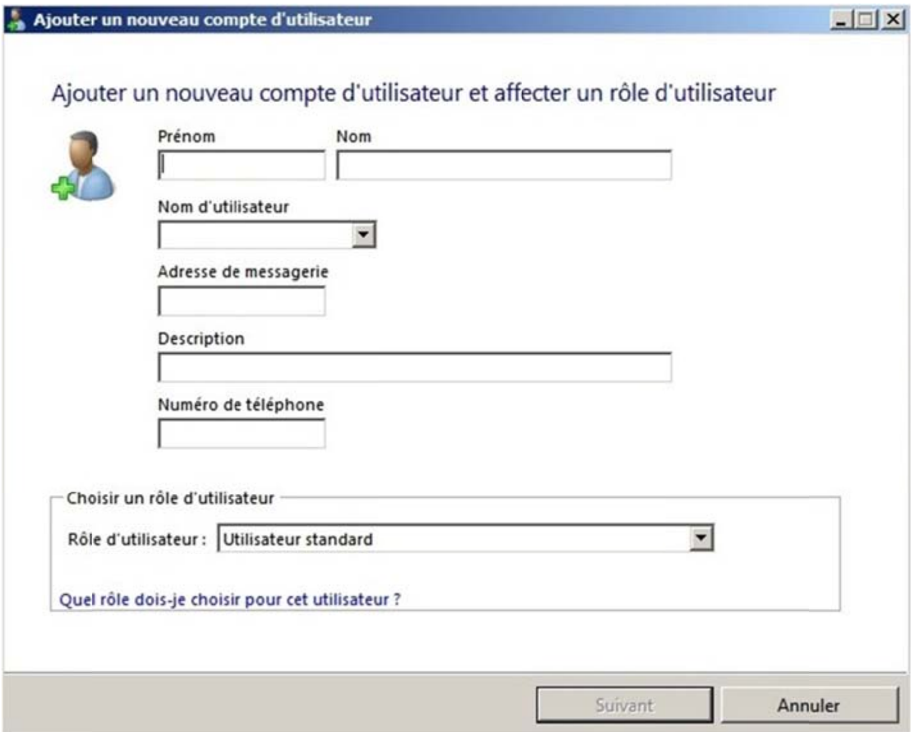
2.1 Création de compte / messagerie

Se logger sur le serveur avec le compte « admineloy » et le mot de passe « xxxx ».

La Console Windows Small Business Server 2011 Standard s'affiche sur l'écran.

Sélectionner l'onglet utilisateurs et groupes et cliquer sur « Ajouter un nouveau compte d'utilisateur »



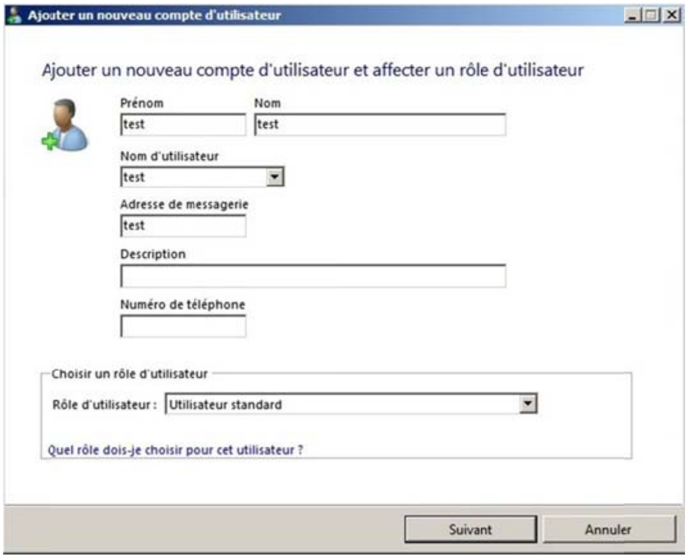


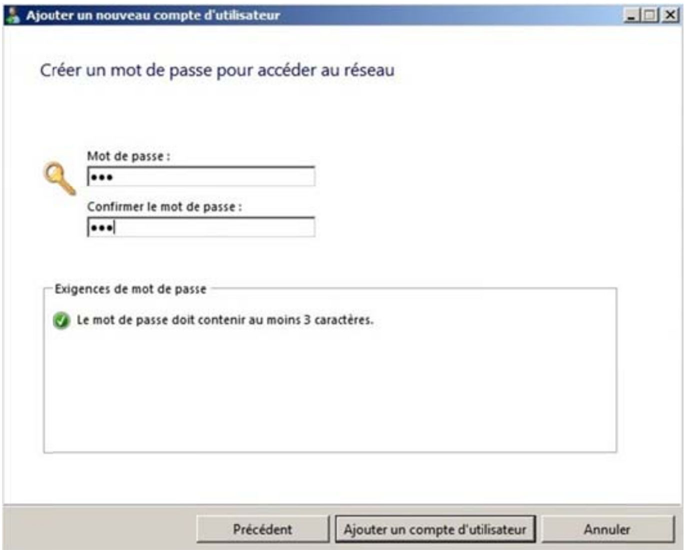
Renseigner les différents champs :

- Le nom d’utilisateur est le nom utilise pour logger sur Windows
- Pour la messagerie ne pas spécifier @eloy.fr, l’extension est rajoutée automatiquement.

Valider en cliquant sur suivant.

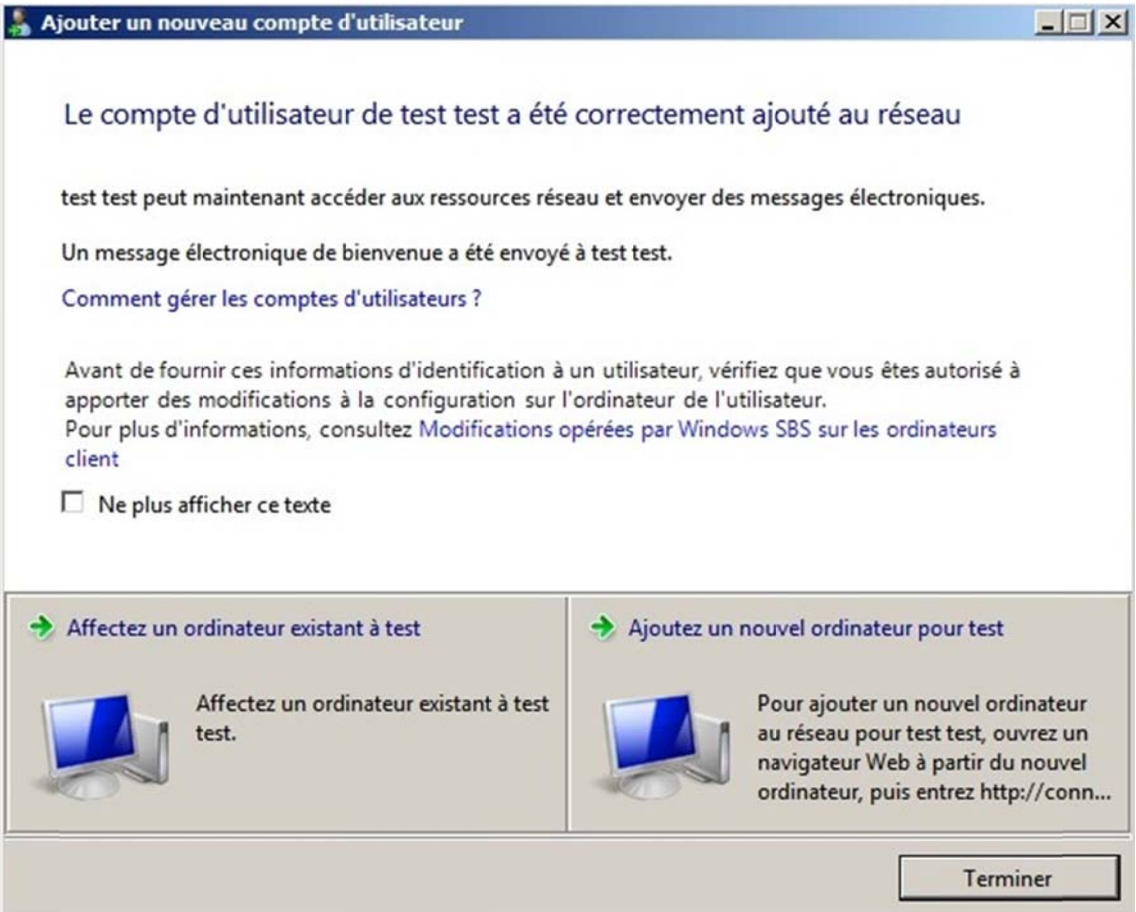
La fenêtre suivante permet de choisir le mot de passe utilise pour l’ouverture de session Windows.



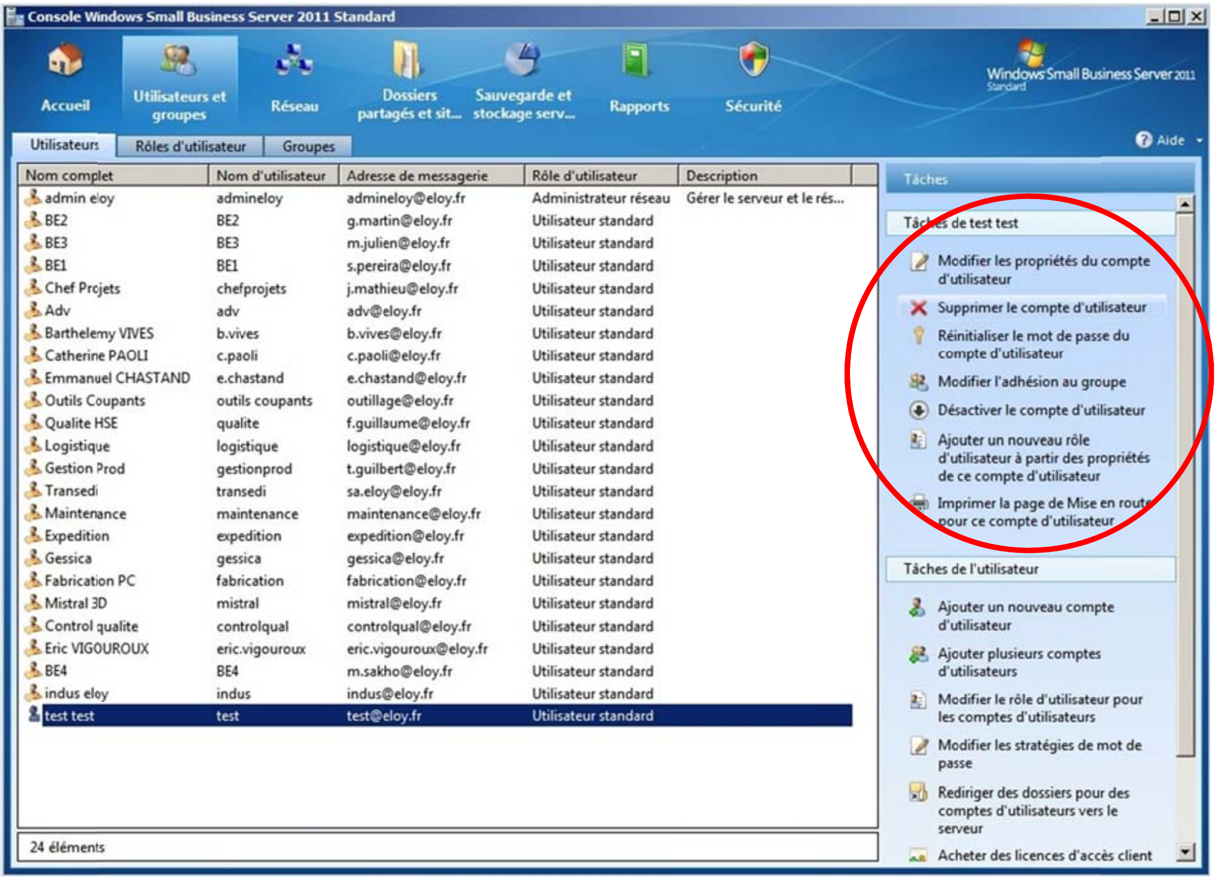


Valider en cliquant sur ajouter un compte utilisateur.

Si tout s’est bien déroulé la fenêtre suivante apparait à l’écran :

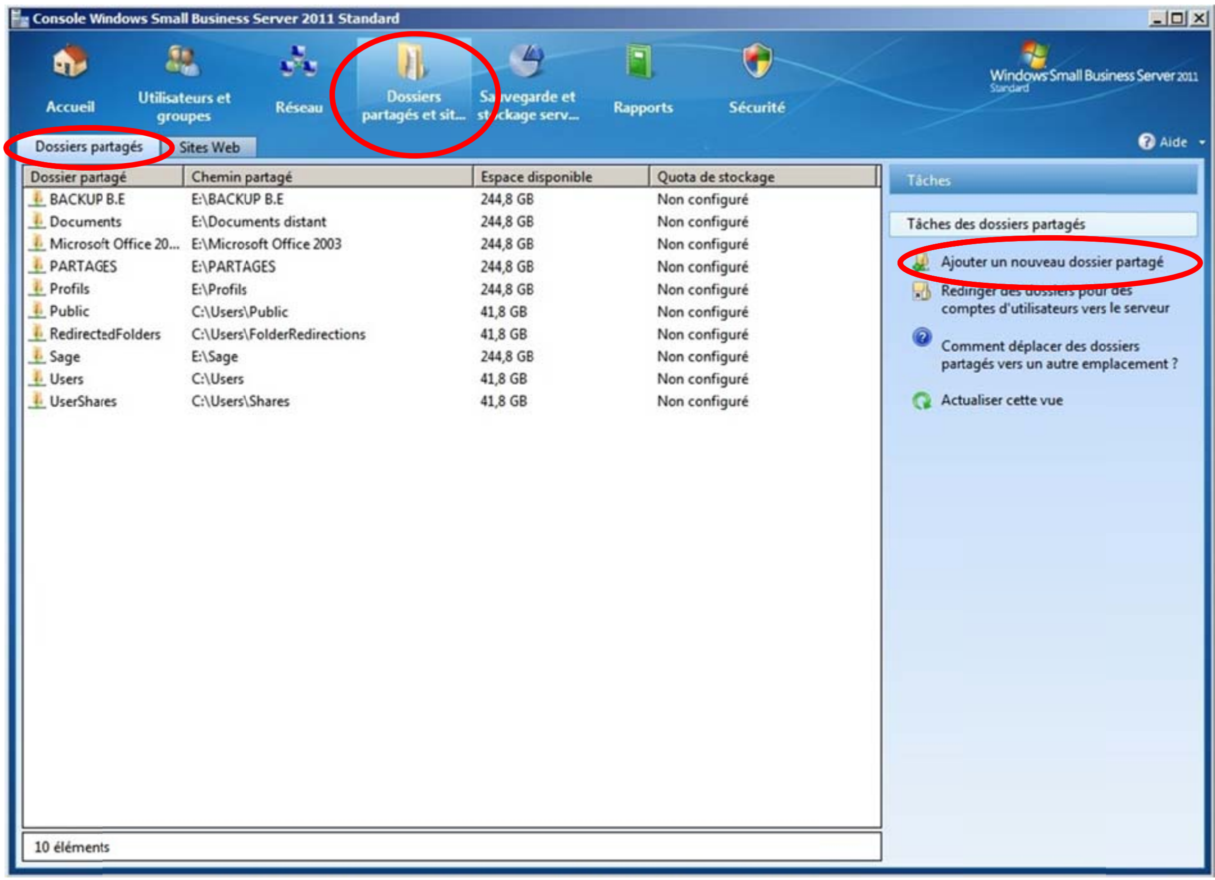


Les options sur la droite de la console permettent de changer le mot de passe d'ouverture de session d'un utilisateur ainsi que l'association avec la boite mail (propriétés du compte utilisateur).

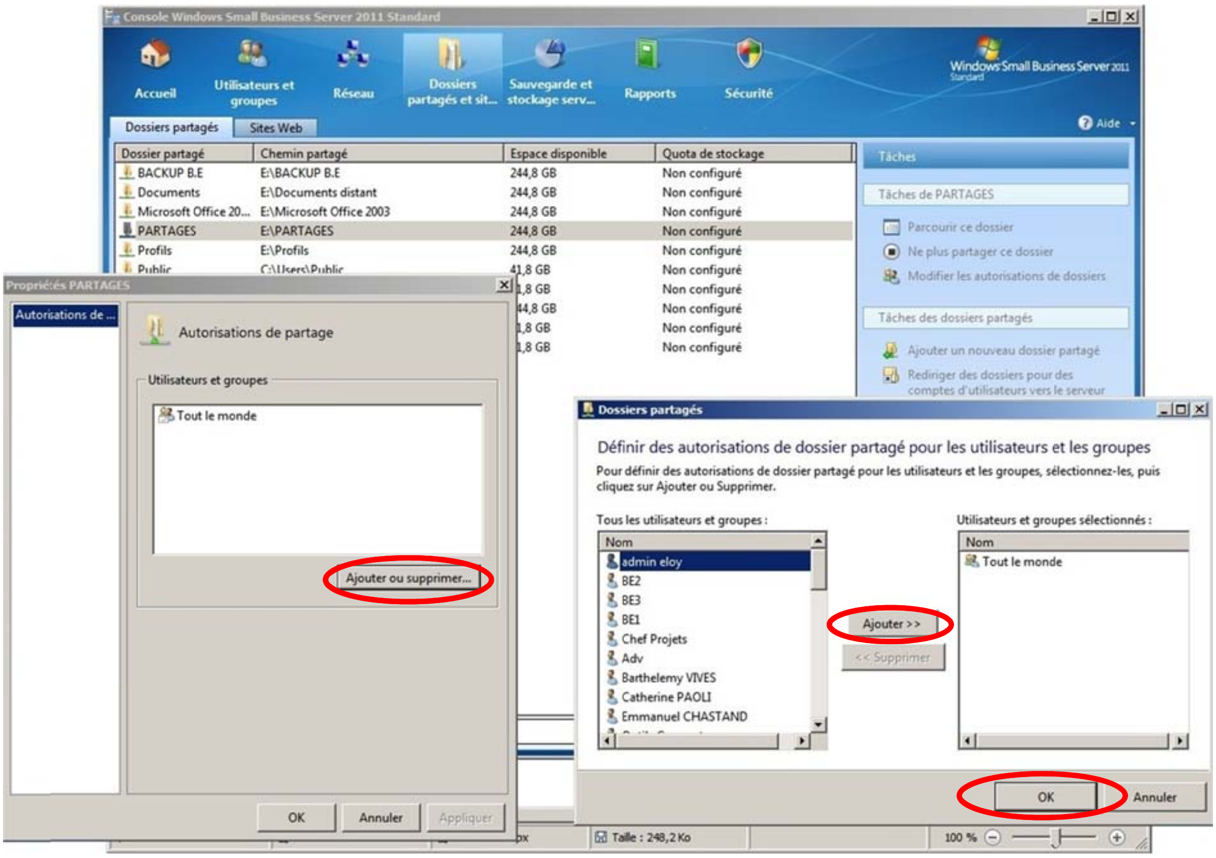


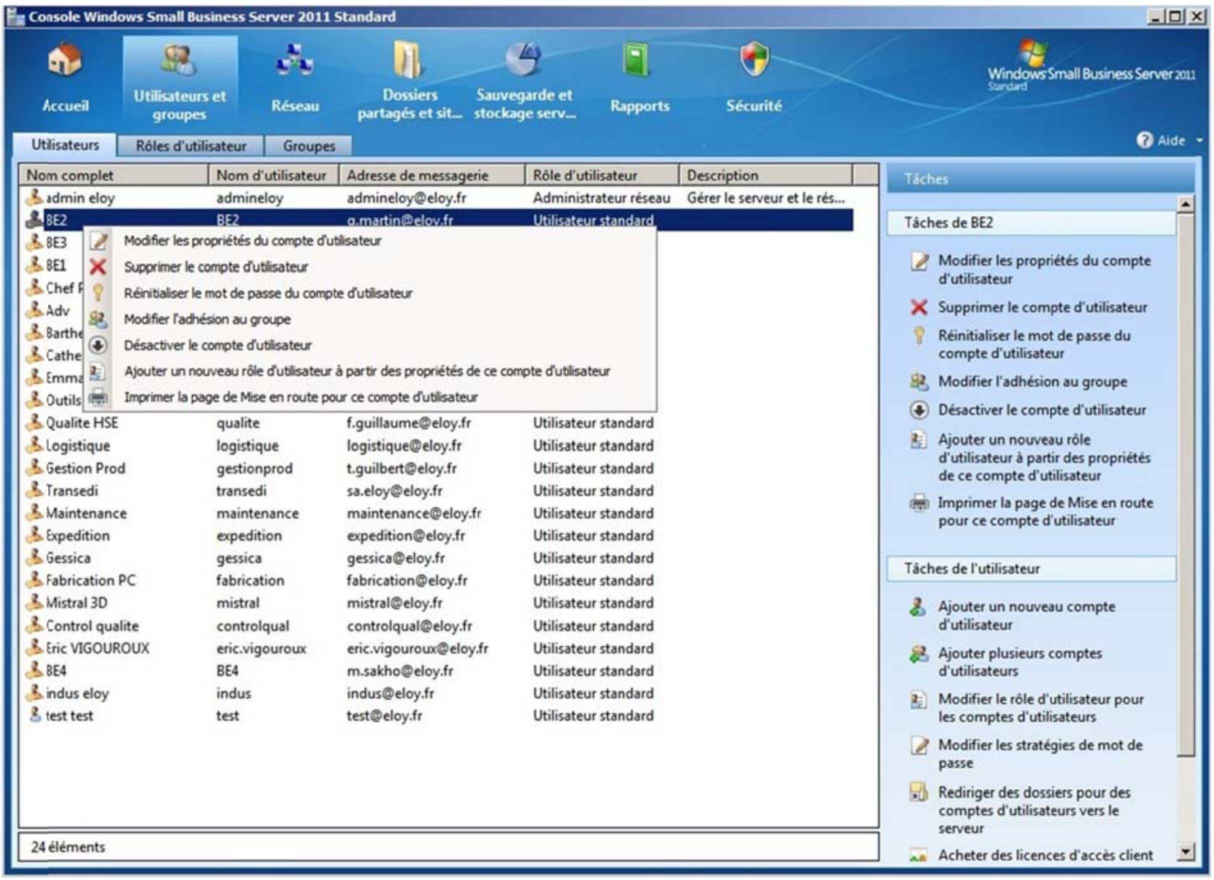
2.2 Dossiers partagés

Sélectionner l'onglet « dossiers partagés et sites » et ajouter un nouveau dossier dans le menu de droite.



Pour modifier les droits d'accès à un partage existant double cliquer sur le dossier, la fenêtre de propriétés du partage apparait, cliquer sur ajouter ou supprimer et cliquer sur les utilisateurs à ajouter ou supprimer.





3. Evolution vers téléphonie IP

3.1 Son objectif

- Réduire les coûts de communication et d'infrastructure
- Réduire les coûts de maintenance
- Communications intersites gratuites
- Communications des collaborateurs nomades gratuites
- Accéder à l'information en temps réel
- Améliorer la productivité des collaborateurs
- Pas d'appels entrant perdus

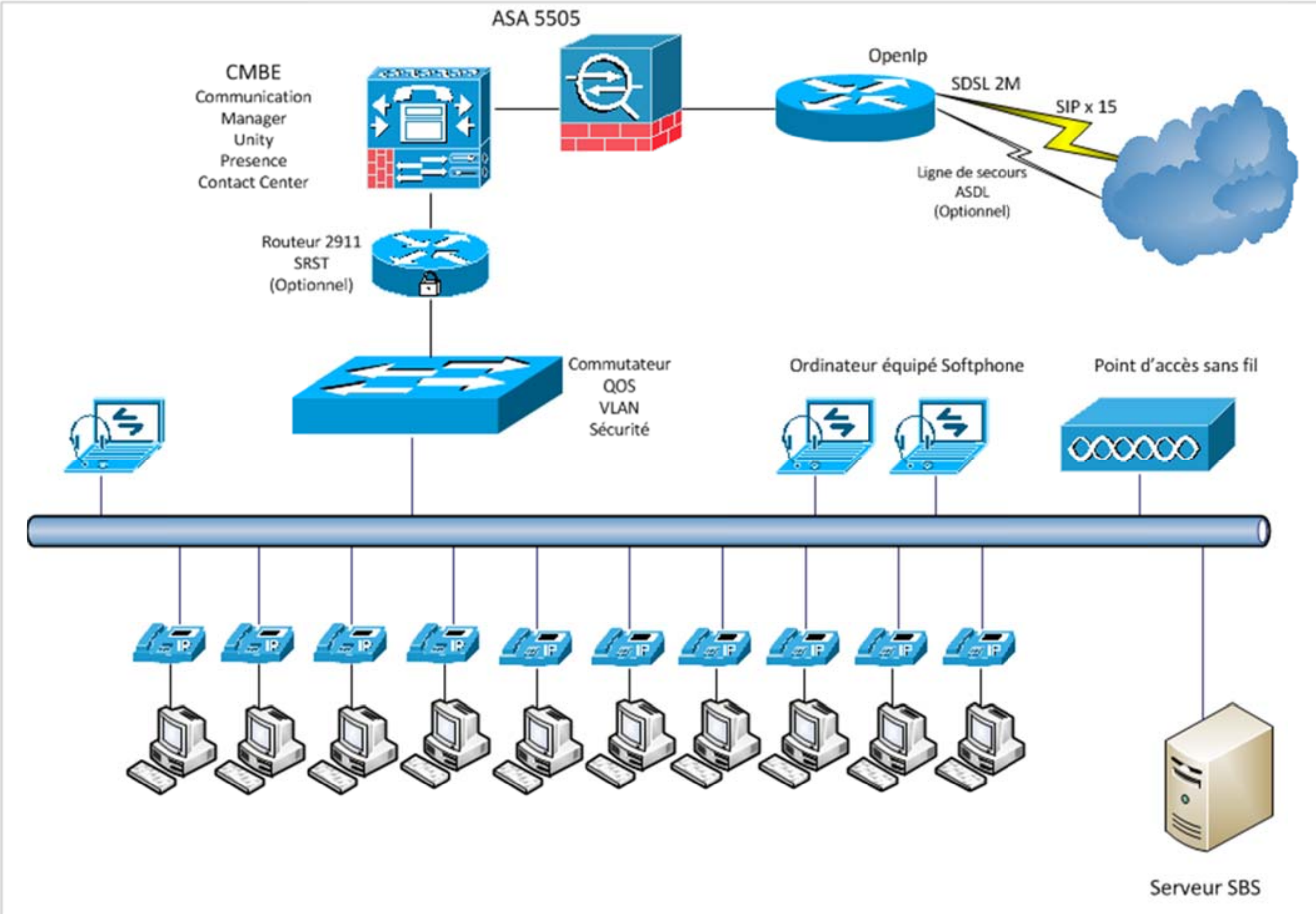
Une compétitivité boostée par la convergence des réseaux voix et données.

Une entreprise dynamisée par la puissance des communications unifiées.

Un manager, le responsable informatique ou le directeur des services généraux administrera seul toutes les fonctionnalités de la téléphonie traditionnelle. Il ne sera plus nécessaire de payer de simples interventions sur la téléphonie.

La téléphonie IP, c'est la simplicité d'une interface web pour des services à haute valeur ajoutée.

- Standard automatique,
- Attribution de lignes,
- Boîtes vocales personnelles,
- Annuaire partagé,
- Numérotation au clic,
- Messagerie instantanée,
- Visioconférence,
- Messagerie unifiée,
- Partage d'applications,
- Softphone,
- Téléphone SIP,
- Travail collaboratif,
- Gestion de présence…



3.2 Tarif

Actuellement, un total de 30 postes SIP serait suffisant.

Les services OpenVOICE d'Openip sont facturés selon le nombre d'appels simultanés souhaités.

	Abonnement mensuel	Mise en service
Trunk SIP par appel simultané	3€ HT	Gratuit
Forfait « fixes + 50 destinations illimitées » par appel simultané	10€ HT	Gratuit

L'avantage des offres par appel simultané, c'est qu'il ne prenne pas en compte le nombre de téléphone IP détenu par la société, contraire aux offres Centrex de SFR ou d'Orange. Ici la société peut détenir 50 ou 100 postes, elle ne paiera que pour 15 appel simultané (règle de 50%pour calculé le nombre de canaux à ouvrir). Avec une offre Centrex, si la société détient 50 postes, elle paiera 50 forfaits.

SIP 15 x 13 = 195 €

SDSL 150€ pour 2M (équivalent au tarif mensuel d'orange pour un bas-débit 512k)

Total = 345 € par mois

Auquel il faut ajouter en moyenne 20% pour les communications hors forfait, ce qui nous donne 414€ par mois

Les offres faites par un intégrateur seront calculé après étude des factures téléphoniques de la société et proposera un tarif mensuel inférieur au coût actuel des communications. Les téléphones IP ainsi que le serveur CMBE seront inclus dans ce tarif. La société réduira donc initialement ses factures téléphoniques les deux ou trois premières années de quelques pourcent, le temps d'amortir le matériel installés, et de 40 à 50%, les années suivantes.

3.3 Cisco Unified Communications Manager Business Edition

Le système de communications unifiées Cisco est une solution intégrant des produits et applications de voix, vidéo, données et de mobilité. Il propose des solutions de communications plus efficaces, plus sécurisées et adaptées à chaque utilisateur, améliorant directement leur productivité. Il met en relation les personnes au travers de nouvelles méthodes de communications qui s'adaptent à votre activité de travail et à vos déplacements. La sécurité est constamment présente et les informations sont toujours accessibles où et quand vous en avez besoin. Les systèmes de communications unifiées Cisco font parties d'une solution globale incluant une infrastructure réseau, des produits de sécurité, de mobilité et de gestion de réseaux ainsi que des options de déploiements simplifiés et de gestion externalisée, des solutions de financement, des applications de communications d'entreprises partenaires.

La solution Cisco Unified Communications Manager Business Edition est une solution simple à gérer qui combine des fonctions de traitement d'appels voix, vidéo, des services de mobilité sur un seul et même serveur afin de simplifier l'administration de cette solution et de réduire les coûts d'équipements et les coûts opérationnels. Cette solution consiste en une option de déploiement attractive pour les organisations de tailles moyennes avec des équipes Informatique et Télécom réduites qui souhaitent profiter des services proposés par Cisco Unified Communications Manager (aussi appelé Cisco Unified CallManager), Cisco Unity® Connection, Cisco Unified Mobility (aussi appelé Cisco Unified MobilityManager) et un outil de gestion intégré sur un seul serveur afin d'accélérer la migration vers les communications unifiées.

Cette solution intègre beaucoup de nouvelles fonctionnalités, imaginées spécifiquement pour les entreprises de tailles moyennes, comme les fonctions de 'Ne pas déranger', offre d'appel, messages d'indication d'attente audio, groupes de chasse, le téléphone IP Cisco 7931. Les fonctionnalités de reconnaissance vocale, messagerie intégrée, règles de routage d'appels et numéro unique sont également disponibles dans cette solution.

Pour permettre aux entreprises de se développer rapidement, cette solution s'agrémente d'options d'extensions en s'intégrant à l'ensemble de la gamme de produits de Communications unifiées comme le serveurs de présence, l'assistant personnel de communications, le système de centre d'appels Express, l'outil de collaboration MeetingPlace Express…

La solution Cisco Unified Communications Manager Business Edition s'intègre également avec l'outil de gestion, de supervision et de diagnostics Cisco netManager Unified Communications. Cisco netManager assiste les moyennes entreprises dans la gestion de leur système de communications en supervisant tous les composants de la solution.

3.3.1 Description du produit

La solution Cisco Unified Communications Manager Business Edition est destinée aux entreprises jusqu'à 500 salariés et 5 sites distants. Elle propose des services de voix, vidéo, mobilité et de messagerie sur une unique plate-forme. Cette solution simplifie considérablement l'installation, le support et la gestion de ce type de systèmes, réduisant ainsi le coût de possession de la solution. Avec la solution Cisco Unified Communications Manager Business Edition, les entreprises de moyennes tailles peuvent désormais facilement proposer les fonctionnalités de communications unifiées Cisco à leurs employés du site central mais également des sites distants.

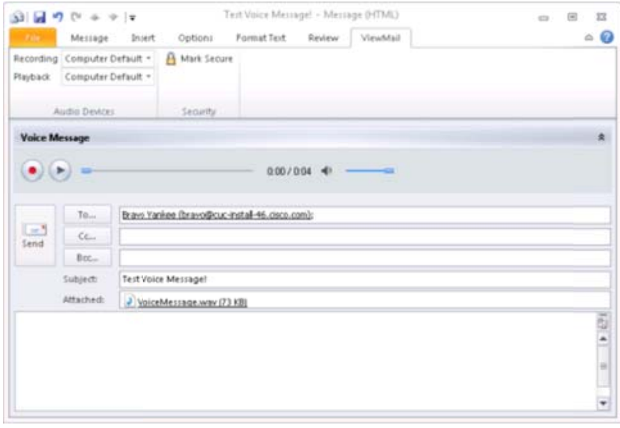
D'un point de vue logiciel, Cisco Unified Communications Manager Business Edition 6000 version 8.5 se compose des quatre principaux éléments suivants :

Cisco Unified Communications Manager version 8.5 est le moteur de traitement multimédia de Cisco Unified Communications Manager Business Edition 6000.

- Communications avancées : accès intégré à des fonctionnalités de communication avancées, avec notamment la possibilité de programmer les paramètres personnels des utilisateurs.

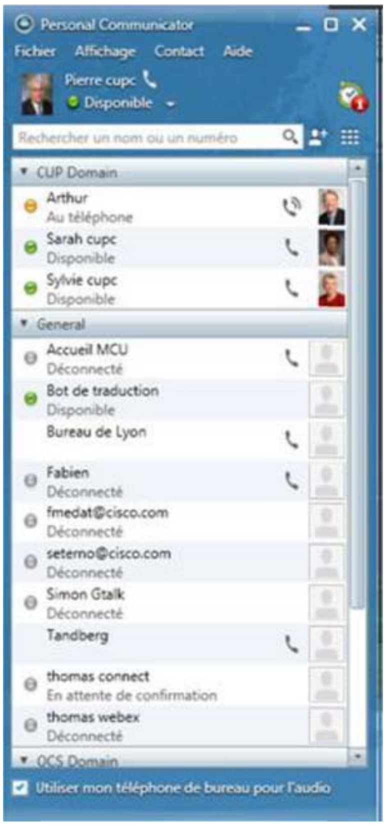
- Fonctions multimédias : pour donner du relief aux appels téléphoniques en y ajoutant simplement des fonctionnalités vidéo.
- Simplicité de configuration : des outils sont disponibles pour créer des profils utilisateurs qui pourront être copiés en toute simplicité afin de réduire les temps d'installation.

Outre les fonctions de traitement des appels, le logiciel Cisco Unified Communications Manager inclut des fonctionnalités qui améliorent la productivité des employés mobiles pendant leurs déplacements. Intitulé Cisco Unified Mobility, cet ensemble de fonctionnalités comprend par exemple une boîte de messagerie vocale unique ainsi qu'une application à numéro d'appel unique qui gère, filtre, achemine et connecte les appels de façon intelligente entre le téléphone de bureau IP d'un employé et son téléphone portable ou le téléphone de son domicile.



Cisco Unity® Connection version 8.5 est l'application de messagerie unifiée de Cisco Unified Communications Manager Business Edition 6000.

Consultation des messages vocaux depuis le client Outlook



Cisco Unified Presence 8.5 met en relation le personnel des différentes entreprises de la façon la plus efficace possible. Cette plate-forme ouverte et extensible facilite l'échange hautement sécurisé des informations de présence et de messagerie instantanée entre Cisco Unified Communications et les autres applications. Cisco Unified Presence facilite la prise de décision et améliore la productivité en sensibilisant les employés à l'importance de la fonction de présense.

Cisco Unified Contact Center Express 8.5 composant essentiel du système Cisco Unified Communications Manager Business Edition 6000, est une solution de gestion des interactions client élaborée pour 100 agents au maximum.

Cisco Unified Communications Manager Business Edition 6000 bénéficie ainsi d'un excellent positionnement prix.

Le niveau fonctionnel offert sur un serveur unique positionne la solution Cisco Unified Communications Manager Business Edition 6000, comme un produit de communications unifiées incontournable sur le marché.

3.4 Fonction Survivable Site Remote Telephony (SRST) sur Cisco Call Manager

La fonction SRST permet à un site distant disposant d'un routeur faisant office de passerelle voix de fonctionner en autonomie dans le cas où le Call Manager n'est plus joignable (panne, coupure réseau …).

Etant donné que beaucoup des fonctionnalités sont gérées par le Call Manager, certaines seront perdues lors du passage dans ce mode dégradé. Cependant, il est possible d'affiner le plus possible la configuration pour limiter la gêne des utilisateurs du système.

Au niveau du routeur, tout se passe dans le mode call-manager fallback

(En mode configuration terminal). Il est possible d'utiliser ensuite plusieurs commandes pour le paramétrer et le personnaliser un peu plus :

- user-locale PAYS : permet de définir la locale utilisée pour les téléphones, on utilisera ici le code pays comme FR pour French.
- system message MESSAGE : indique le message affiché sur le téléphone lorsqu'on passe en mode SRST
- alias ID PATTERN to NUMERO_TRANSLATE PREFERENCE : Cette commande permet de faire des alias pour simuler par exemple des numéros de groupement d'appel. Lorsque le Call Manager n'est plus accessible, ces groupements ne sont plus routés car non connus de la passerelle voix. Pour recréer un groupement, on peut choisir de créer plusieurs alias vers différents numéros et différentes préférences. Prenons par exemple le numéro 5000 qui est un numéro de standard. Ce numéro est retranscrit dans un Line Group avec quatre numéros, 5001, 5002, 5003 et 5004 qui sonne de manière ordonnée. Si on souhaite recréer ce fonctionnement en SRST, on créera les alias suivant :
    - alias 1 5000 to 5001 preference 1
    - alias 2 5000 to 5002 preference 2
    - alias 3 5000 to 5003 preference 3
    - alias 4 5000 to 5004 preference 4

De la même façon, si on souhaite recréer un groupement qui fonctionne en sonnerie parallèle broadcast), on fixera la même priorité à chacun de ces alias.

- max-dn NUMBER : Définit le nombre maximum d'entrée de répertoires que peut contenir le routeur en mode SRST. Ce nombre est fixé suivant les spécifications du routeur (modèle, quantité de mémoire), pour la déterminer il faut se rendre ici :
  http://www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/srs/srst31/srs31spc.htm

En cas de coupure de communication avec le Call Manager, il est possible de conserver le fonctionnement de la musique d'attente. Pour cela, il faut copier la musique au bon format sur le slot0: du routeur. Ensuite, toujours dans le mode call-manager fallback, il faut entrer la commande :

moh FICHIER

La musique sera alors multicastée sur le LAN en utilisant le codec G711 (~ 80 Kbps).

XIII. Bibliographie

1. Livres

FREDDI Philippe. Windows Server 2008-Installation, configuration, gestion et dépannage [2ième édition]. Edition ENI. 2008. 910 pages.

APRÉA Jean-François. Windows Server 2008 MCTS 70640 - Infrastructure Active Directory. Edition ENI. 2008. 768 pages.

SAURY Jean-Georges et CAICOYA Sylvain. Windows Server 2003 et Windows Server 2008 Tome 1. Micro Application. 2007. 1012 pages.

DEMAN Thierry, ELMALEH Freddy, CHATEAU Mathieu et NEILD Sébastien. Windows Server 2008-Administration avancée. Edition ENI. 2008. 500 pages.

ATELIN Philippe. Wi-Fi Réseaux sans fil 802.11 : Technologie - Déploiement – Sécurisation. Seconde édition. Edition ENI.2009. 406 pages.

ANDERRUTHY Jean-Noël. Maintenance et dépannage d'un PC en réseau. Nouvelle édition. Edition ENI. 2008. 444 pages.

FRAHIM Jazib et SANTOS Omar. Cisco ASA All in One Firewall IPS Anti X and VPN Adaptive Security Appliance 2nd. Cisco Press. 2010. 1124 pages.

WATKINS Michael et WALLACE Kevin. Cisco - CCNA 640-553 Security Official Exam Certification Guide. Cisco Press. 2008. 637 pages.

2. Articles de presse et dossiers thématiques

CHAIGNEAU Alexandre. Débuter avec un pare-feu Cisco. Hacking, N°1/2009, pages 48 à 57.

BLAVET Vincent. WIFI N – 300Mbps : rêve ou réalité ? Journal du Net, 07/05/2009.

3. Sites internet consultés

http://blogs.technet.com/b/pierrc/archive/2011/04/07/webcasts-sbs-2011-standard-et-essentials-aux-techdays-2011.aspx

http://social.technet.microsoft.com/Forums/fr-FR/windowsserver2008fr/thread/afa31613-431a-43b1-9ac4-156eb226cd13

http://www.cisco.com/en/US/products/ps6120/prod_configuration_examples_list.html

http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008054339e.shtml

http://www.commentcamarche.net/contents/wifi/wifiintro.php3

http://fablain.developpez.com/tutoriel/initiation-sharepoint/?page=sommaire

http://blog.developpez.com/michael/

http://www.dell.com/fr/entreprise/p/servers

http://www.bechtle.fr

XIV. Conclusion

Ainsi, j'ai effectué mon stage de fin de formation en Réseaux informatiques et Télécommunications au sein de l'entreprise ELOY. Lors de ce stage de 8 semaines, j'ai pu mettre en pratique mes connaissances théoriques acquises durant ma formation, de plus, je me suis confronté aux difficultés réelles de la gestion d'un parc informatique des plus homogènes.

Après ma rapide intégration dans la société, j'ai eu l'occasion de réaliser plusieurs tâches qui ont constitué une mission de stage globale.

Chacune de ces tâches, utiles au service et au bon déroulement de l'activité de l'entreprise, se sont inscrites dans la stratégie de celle-ci et plus précisément dans celle de son réseau informatique.

Je garde du stage un excellent souvenir, il constitue désormais une expérience professionnelle valorisante et encourageante pour mon avenir.

Je pense que cette expérience en entreprise m'a offert une bonne préparation à mon insertion professionnelle car elle fut pour moi une expérience enrichissante et complète qui conforte mon désir d'exercer mon futur métier de technicien supérieur en réseaux informatique.

Ce stage m'a permis de participer aux études d'optimisation d'un réseau informatique dans une entreprise, de pouvoir rechercher et évaluer des solutions techniques nouvelles incluant la sécurité en rencontrant des commerciaux. Et ensuite de proposer des scénarios d'évolution de mise en œuvre et d'argumenter leur choix.

Enfin, je tiens à exprimer ma satisfaction d'avoir pu travailler dans de bonnes conditions matérielles et un environnement agréable.