Garde-barrière à l'Observatoire de Strasbourg

- **Genèse du projet « Pare-feu pour les laboratoires CNRS-Alsace »**
- **Choix et fonctionnalités du produit choisi**
- **Implémentation à l'Observatoire de Strasbourg**

L'expression des besoins (1)

- Conséquences de la formation SIARS 2001-2002 donnée à 40 IARS à Strasbourg :
  - Nécessité de faire quelque chose tout de suite
    - Avec très peu de ressources humaines
    - Avec quelques moyens financiers

L'expression des besoins (2)

Avec très peu de ressources humaines

- Refus de « bidouille » beaucoup trop chronophage:
  - Matériel : PC => Ok
  - OS : Choix, formation, configuration, patches
  - Logiciel : Choix, formation, paramétrage, mise à jour

L'expression des besoins (3)

Avec quelques moyens financiers

- Apparition de solutions de type « appliance »:
  - Coût raisonnable de 1 à 10 K€ proportionnel à la taille et donc aux moyens des laboratoires
  - Pilotage ergonomique réduisant l'investissement « temps »
  - Un seul interlocuteur
  - Des services: formation, assistance, mise à jour, maintenance

L'expression des besoins (4)

Choix d'un fournisseur commun sur la région

- Négociation facilitée
- Formation assurée en commun
- Entraide
- Partage d'expériences
- Effet d'entraînement

Retombées positives

- Prise de conscience des dirigeants
- Sensibilisation des utilisateurs
- Mise en place « forcée » d'une politique de sécurité:
  - Organisation nécessaire pour la matrice des flux
  - Mise en place de règles de filtrage et procédures
  - Traitement des accès distants

Critères de choix du matériel (1)

- Fournisseur maîtrisant intégralement son produit
  - OS minimum et complètement sécurisé
  - Pas de juxtaposition de briques d'origines diverses
- Ne pas surestimer nos besoins
  - Éviter la course au suréquipement technique (débit, etc.)
  - Privilégier une construction progressive et maîtrisée
- Prévoir de la redondance
  - Faire face à la panne quand le responsable système est aux Caraïbes

Critères de choix du matériel (2)

- Intégration dans la politique de PKI du CNRS
- Fournisseur français
  - Contacts facilités
  - Établissement de partenariat possible
  - Meilleure garantie contre la « guerre économique », backdoor, etc.

Choix du constructeur

Constructeur Européen de solutions Firewall & VPN

NETASQ

Secure Internet Connectivity

Société Netasq

- Société française créée en 1998
- Capital 426 K€
- CA en progression de 80% en 2002
- 68 personnes
- Support, R&D, fabrication française
- Développement international principalement européen

Marché des pare-feu type appliance

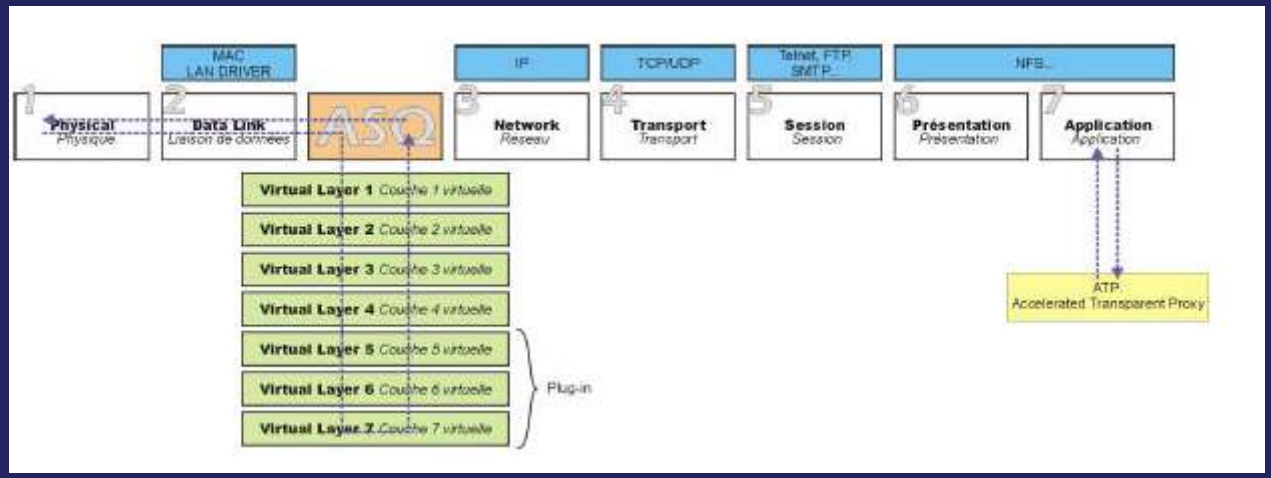
- France: Prévisions 2003: +35 %
- 3 principaux segments:
  - 1K€ < FW 27%
  - 1K€ < FW < 10 K€ 31 %
  - FW > 10 K€ 42 %

Gamme Netasq

- F50 : 3 interfaces 100 Mb/s, 4000 sessions simultanées, débit utile 25 Mb/s
- F200 : 4 interfaces 100 Mb/s, 32000 sessions simultanées, débit utile 130 Mb/s
- F500 : 4 interfaces 100 Mb/s, 65000 sessions simultanées, débit utile 170 Mb/s
- F1000 : 12 interfaces 100 Mb/s
- F2000 : 16 interfaces 100 Mb/s, 4 interfaces Gb/s

Spécifications techniques Netasq

- ASQ: pare-feu classique type « stateful inspection » + pare-feu applicatif
  - Détection intrusion temps réel (IPS: Intrusion Prevention System)
  -



Spécifications techniques ASQ

- Analyse IP
  - Conformité du format des paquets au niveau 3 et 4
  - Bugs et dénis de service
- Analyse des fragments
  - Cohérence du datagramme
- Analyse globale
  - Mémorisation du contexte
- Filtrage
  - De type « Stateful Inspection » + optimisation dans l'analyse des règles
- Analyse des protocoles applicatifs
  - Conformité aux RFC

Spécifications ASQ

- Plugins
  - Génériques (data-tracking) (Suivi de données)
  - HTTP (Détection d'attaques : encodage, buffer overflow,etc.)
  - FTP (Commandes inconnues, force brute, buffer overflow, etc.)
  - RIP
  - DNS (Cohérence requêtes et réponses ID spoofing, empoisennement cache DNS, etc.)
  - H323 (Ouverture automatique de connexions filles)
  - Edonkey (Prévention d'attaques et traces des fichiers partagés)

Spécifications ASQ

- Filtrage – Translation
  - Filtrage des VLAN 802.1q
  - Gestion horaire
  - Gestion de bande passante
  - Gestion de la saturation par règle
  - 4 types de translation: map, map bidir, redirection, split (basé sur IPFilter 3.4.30)
- Antivirus optionnel Kaspersky

Spécifications ASQ

- Authentification
  - LDAP interne ou externe
  - Kerberos, Active directory
  - Compatibilité Radius
  - Méthodes plain, certificat, SRP, Radius
- PKI interne en option
- VPN
  - VPN Ipsec
  - 5 algorithmes de chiffrement
  - Clefs 256 bits
  - Hub and Spoke

Spécifications ASQ

- Routage
  - Mode routage
  - Mode transparent
  - Mode hybride
  - Multi-IPs par interface
  - Routage par interface
  - Load balancing

Spécifications ASQ

- Services
  - Client NTP
  - Serveur DHCP
  - Serveur cache DNS (transparent ou non)
  - SNMP
- Proxies
  - HTTP (filtrage d'URLs, authentification, etc.) en option
  - SMTP (permet l'intégration d'un antivirus...)

Spécifications ASQ

- Haute disponibilité
  - 2ème boîtier en fonctionnement maître/esclave
  - Liaison Ethernet ou série sécurisée AES 128 bits
  - Redémarrage automatique
  - Conservation du contexte des connexions
  - Transfert de mise à jour vers le boîtier passif

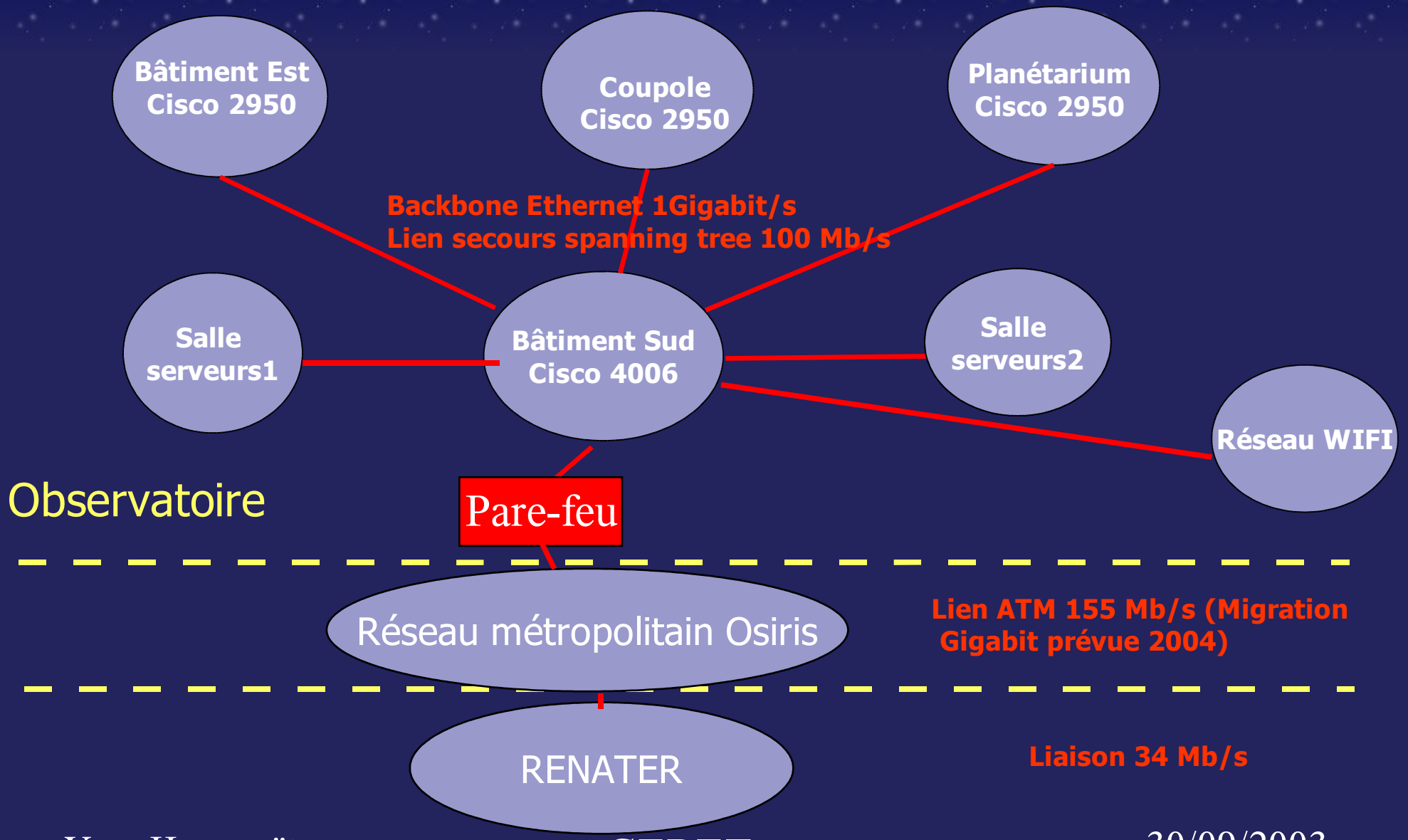
Suite d'administration Netasq (Windows)

- Firewall Manager
  - Interface graphique
  - Gestion du pare-feu et des logs
  - Sauvegarde et restauration
  - Configuration ASQ (Plugins, alarme, etc.)
  - Envoi d'alarmes par Email
  - Gestion du serveur SSH
- Gestion des logs
  - Syslog externe chiffré
  - Alarmes, connexion, filtrage, URL
  - Rotation des logs
  - Gestion de la taille des fichiers

Suite d'administration Netasq (suite)

- Firewall Monitor
  - Visualisation temps réel
  - Alarmes ASQ, traces, bande passante, débit, utilisateurs,hôtes, VPN, HA, statistiques
- Firewall Reporter
  - Extraction par périodes
  - Tris, graphiques, exportation de résultats
- Log Analyser (depuis version 5)
  - Outil de centralisation de logs
  - Base de requêtes SQL

Contexte réseau de l'Observatoire Astronomique de Strasbourg



Contexte scientifique de l'Observatoire Astronomique de Strasbourg (CDS)

- Un des nœuds de l'astronomie mondiale
  - Sous contrat avec la NASA, l'ESA, l'ESO, le NAO
  - Bases de données :
    - SIMBAD : 3.200.000 objets, 8.000.000 d'identifiants; 15000 requêtes/jour
    - VIZIER : 3.918 catalogues de données, spectres, images, données temporelles en astronomie; 10.000 requêtes/jour
    - ALADIN : 40 téraoctets d'images du ciel; 1 million de requêtes/an
    - Bibliographie : 1 téraoctet; 3 millions d'abstracts; 170.000 articles; 10.000 requêtes/jour
  - Copies miroir Japon, Canada, USA
  - Pipeline données satellite XMM

Observatoire Astronomique de Strasbourg (CDS)

- Contraintes opérationnelles : Service 24h/24

=> Pare-feu Haute Disponibilité

  - 20 à 30 % des 100Mbs disponibles en pointe
  - 300 connexions simultanées entrantes en moyenne
  - 200 connexions simultanées sortantes en moyenne

- Prochainement mise en place de VPNs (PKI CNRS)

Conclusion

- Des listes d'accès sur routeur ou équipement de niveau 3 ne suffisent plus
- Outil réellement efficace et d'installation très aisée
- Mises à niveau logicielle et matérielle sont assurées par des ingénieurs dont c'est le métier
- En 10 mois, 1 release majeure et 3 releases mineures
- Rapport qualité/prix intéressant
- Il faut se donner les moyens de sa politique de sécurité