

CH8 Divers

**Storage : DAS, NAS, SAN**

## **Storage : DAS, NAS, SAN**

- **Direct Attached Storage**
- Network Attached Storage
- Storage Area Network

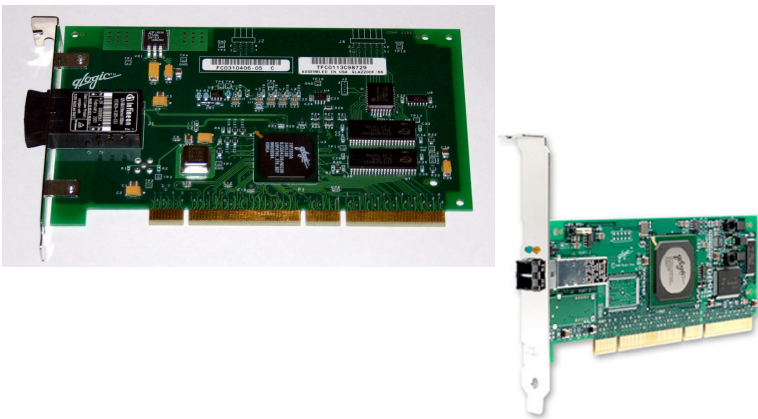
## **Direct Attached Storage**

- Terme créé quand on a commencé à parler de NAS et SAN
- Désigne les moyens de stockage directement attachés à un serveur ou une workstation
  - Sans réseau de stockage entre les deux
  - Typiquement : disques durs, RAID arrays
- Protocoles les plus courants : SCSI, Fiber Channel

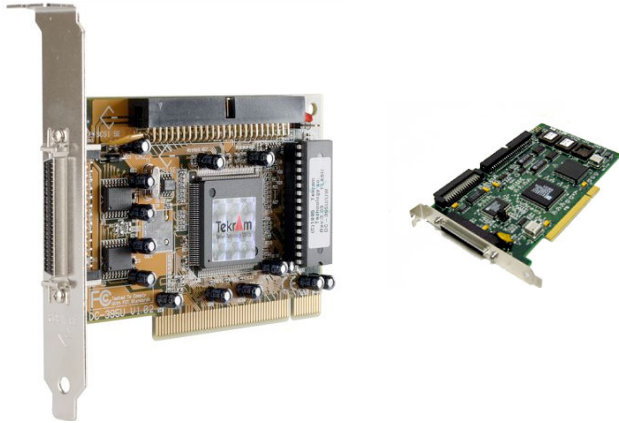
## Direct Attached Storage

- Généralement : armoire externe avec contrôleur et disques
  - Le contrôleur gère le RAID
  - Le contrôleur est parfois dédoublé (redondance)
  - HBA = Host Bus Adapter : interface entre la machine et le storage
    - carte SCSI, carte Fibre Channel
- Armoire parfois partagée entre 2-4 serveurs
  - Utilisé pour les clusters
  - Se rapproche des SAN d'entrée de gamme

## HBA : carte Fiber Channel

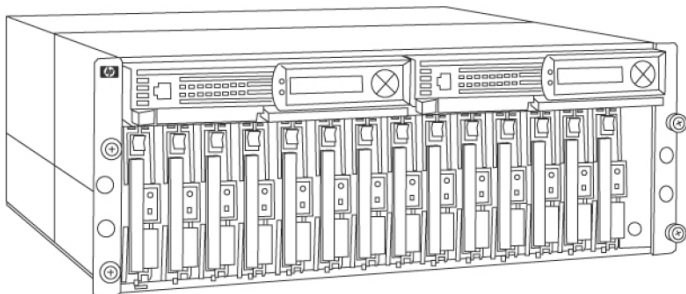


## HBA : carte SCSI



## Exemple : MSA 1000

- HP StorageWorks 1000 Modular Smart Array (utilisable en DAS mais aussi connectable à un SAN)



## Direct Attached Storage

- Résumé
  - Type de stockage assez basique
  - Moins cher que NAS et SAN
  - Espace de stockage accédé via le serveur attaché (→ disponibilité dépendante du serveur)
  - Pas réellement de partage de l'espace de stockage (1 armoire par serveur)
  - Redondance : RAID
  - Utilisation typique : PME, serveurs départementaux...

## Storage : DAS, NAS, SAN

- Direct Attached Storage
- **Network Attached Storage**
- Storage Area Network

## Network Attached Storage

- Désigne les moyens de stockage directement accessibles par le réseau TCP/IP
  - Sans passer par un serveur
  - Permet l'accès depuis plusieurs machines à un même espace de stockage
  - Via les protocoles classiques SMB/CIFS, NFS, AppleTalk, FTP, HTTP...
  - On parle de « logical file system storage »
- Bref, sorte de 'disque dur partagé' accessible sur le réseau

## Network Attached Storage

- Concrètement : disque(s) + mini operating system
- IP fixe ou DHCP
- Temps d'accès dépendants du réseau et de sa charge, ainsi que de la mémoire cache (RAM)
- Facile d'utilisation
  - Utilisé dans les PME et chez les particuliers
- Redondance : RAID
- Sécurité dépendante du mini-OS embarqué
- Moins utilisé dans le monde de l'entreprise (qui aura plutôt des file servers = serveur + DAS, ou un SAN)

## Storage : DAS, NAS, SAN

- Direct Attached Storage
- Network Attached Storage
- **Storage Area Network**

## Storage Area Network

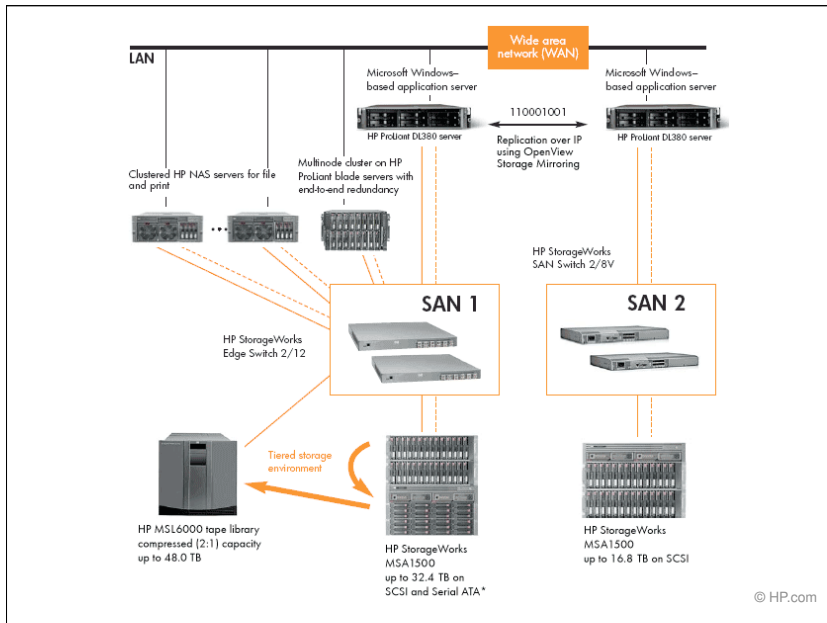
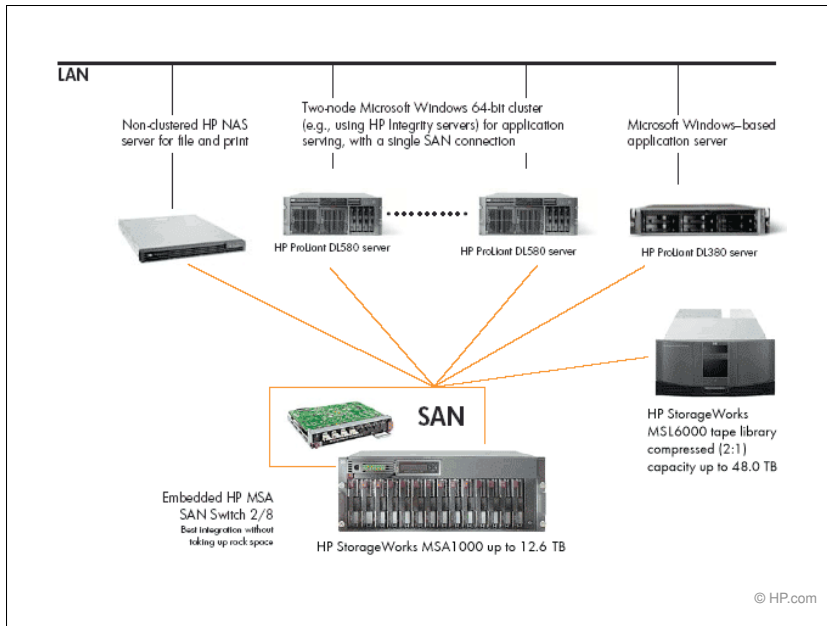
- Réseau de haute performance dédié au stockage
  - Utilisé pour le transfert de données, par blocs, entre des serveurs et des *storage devices* (armoires disques, tape libraries...)
  - Réseau séparé du LAN, généralement en fibre optique, avec des switches
    - Ensemble de switches = « fabric »
  - Sophistiqué et assez cher → utilisé dans les gros data centres, pour les applications critiques, databases...

## Storage Area Network

- Réseau de haute performance dédié au stockage
  - Utilise le protocole Fiber Channel
    - Meilleure bande passante que SCSI, gigabit, supporte les longues distances... (utilise le set de commandes SCSI)
  - Architecture distribuée, possibilités de load balancing et répartition des blocs sur différents storage devices
    - Meilleures performances, supporte un grand nombre d'accès simultanés...
  - Redondance au niveau des serveurs : dual Fiber Channel HBA (par exemple)
  - Redondance au niveau des storage devices : RAID...

## Storage Area Network

- Un storage device (exemple : HP MSA 1000) va contenir un certain nombre de disques durs
  - SCSI, SAS (Serial Attached SCSI), SATA...
- Combinés en « RAID arrays » (extensibles)
  - Ensemble de disques en RAID fournissant un array
- Découpés en « volumes logiques » (redimensionnables)
  - Exemple : un RAID 5 array de 1 TB découpé en 5 volumes de 200 GB
- Ces volumes logiques sont vus comme des « disques durs » par les serveurs connectés au SAN
  - Système d'ACL pour que tel volume soit visible uniquement par tel serveur par exemple (chez HP : « *Selective Storage Presentation* »)



## **SAN vs NAS**

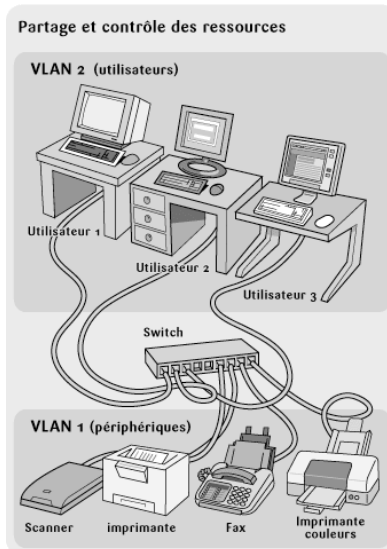
- SAN = accès au niveau « blocs », NAS = accès au niveau « fichier »
- Un NAS peut très bien utiliser un SAN comme espace de stockage
- NAS = relation « many to one » (plusieurs serveurs accèdent le même espace de stockage)
- SAN = relation « one to one » car chaque LUN (*Logical Unit Number*, i.e. disque SCSI virtuel) est utilisé par un seul serveur
  - Sauf clusters par exemple (gestion des accès concurrents au niveau software OS / clustering pour cohérence des accès disque)

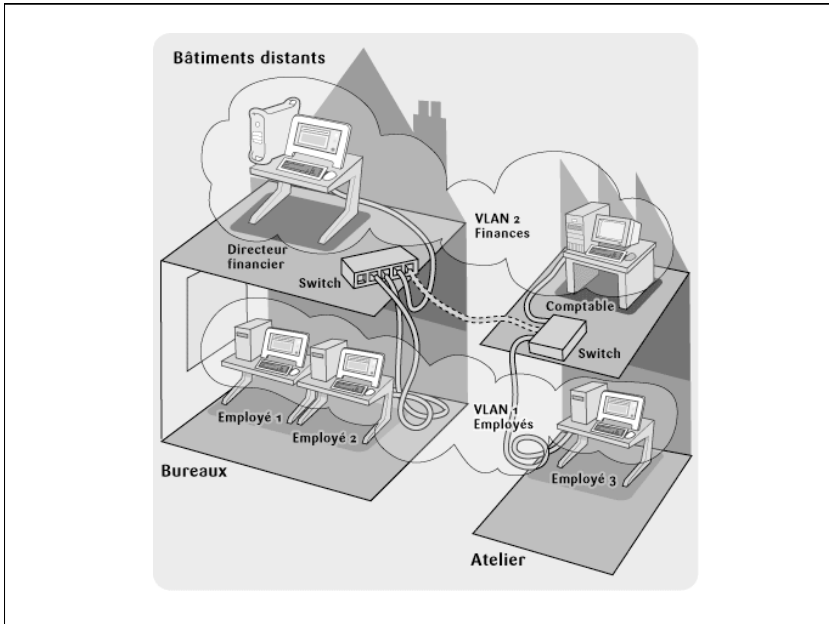
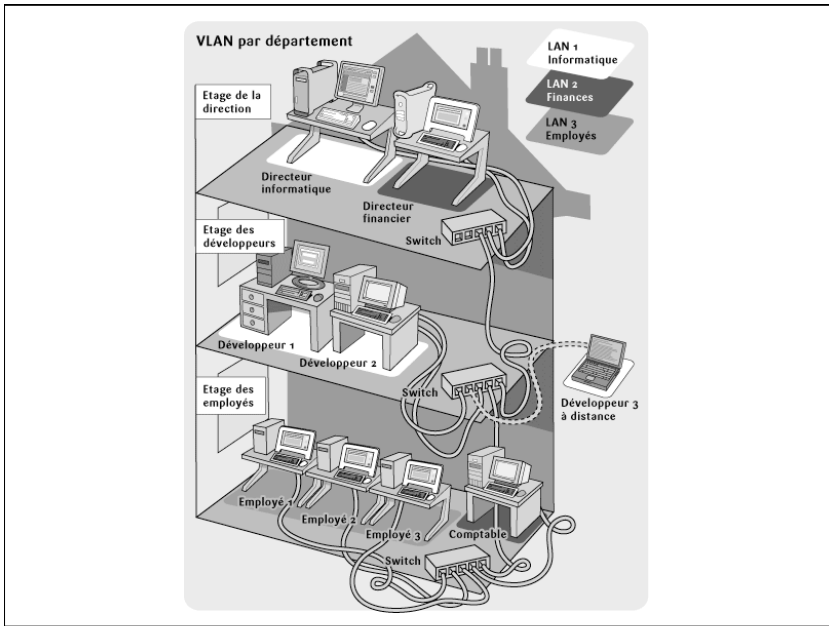
## **VLAN – 802.1Q**

# VLAN – 802.1Q

- **VLAN = Virtual LAN**

- Permet de segmenter logiquement le réseau en couche 2
- Plusieurs VLANs peuvent coexister sur un même switch
  - S'il n'y a pas de routage entre les VLANs, les machines des différents VLANs ne se 'voient' absolument pas
- Utilise le protocole 802.1Q
- Indépendance de la découpe physique du réseau
  - Pratique pour les déménagements de postes (pas de reconfiguration réseau!)





## VLAN – 802.1Q

- **VLAN = Virtual LAN**

- Fonctionne par tagging des paquets Ethernet
  - Ajout d'un VLAN ID (12 bits → max. 4096 VLANs dans un réseau switché)
- Entre les switches : trunking
  - Trunk = lien transportant tous les VLANs
- Souvent un subnet IP (layer 3) associé à un VLAN
  - mais un VLAN peut être utilisé pour plusieurs subnets
- Il faut un routeur (logique ou physique) pour transporter les paquets entre VLANs

## VLAN – 802.1Q

- **VLAN = Virtual LAN**

- Permet de limiter les domaines de broadcasts IP (layer 3) et MAC (layer 2)
- Utilisé pour
  - Implémenter de la sécurité
  - Rendre le réseau plus facilement gérable
  - Améliorer les performances du réseau
  - La flexibilité de la segmentation qui n'est plus physique

## VLAN – 802.1Q

- Avec l'apparition des liens Ethernet fibre haut débit entre sites, on va jusqu'à transporter des VLANs entre des sites distants
- Exemple d'utilisation intéressante : un VLAN de quarantaine
  - Au lieu de débrancher une machine infectée par un virus ou pas à jour, on la met dans un VLAN spécial avec uniquement les updates antivirus, des outils, etc.
- Autre exemple : VLAN pour les visiteurs
- Protocole 802.1x : permet d'assigner dynamiquement un VLAN en fonction de critères (antivirus à jour ? Windows avec les derniers patches de sécurité ?...)
  - Ancêtre de 802.1x : VMPS (*VLAN Membership Policy Server*) – protocole de Cisco, assignation du VLAN sur base de l'@ MAC

## Politique de sécurité

## Politique de sécurité

- De plus en plus, les organisations formalisent un ensemble de règles d'utilisation et de gestion des systèmes d'information sous forme d'un document appelé **Politique de Sécurité** (Security Policy)
- Ce n'est pas une démarche initiée par les informaticiens mais bien par le **business**
  - dans le cadre de la **gestion du risque** que fait toute entreprise
- La mise en place d'une Politique de Sécurité nécessite l'appui du **management**
  - nécessaire pour que les utilisateurs en perçoivent le caractère stratégique...
  - ... et se sentent obligés de la respecter !

## Politique de sécurité

- **Objectifs :**
  - fixer des règles et des guidelines (recommandations) communes et connues de tous – tant **techniques** qu'**organisationnelles**
  - dans le but de protéger l'**information** (ce qui passe notamment par la protection des **systems**)
  - dans le but de garantir l'utilisabilité du système d'information pour leurs utilisateurs
  - dans le but de donner confiance aux utilisateurs en leur système d'information
  - de plus en plus, dans le but d'être **conforme** avec différents aspects légaux

#### Google Apps Service Level Agreement

**Google Apps SLA.** During the Term of the applicable Google Apps Agreement, the Google Apps Covered Services web interface will be operational and available to Customer at least 99.9% of the time in any calendar month (the "Google Apps SLA"). If Google does not meet the Google Apps SLA, and if Customer meets its obligations under this Google Apps SLA, Customer will be eligible to receive the Service Credits described below. This Google Apps SLA states Customer's sole and exclusive remedy for any failure by Google to provide the Service.

**Definitions.** The following definitions shall apply to the Google Apps SLA.

"**Downtime**" means, for a domain, if there is more than a five percent user error rate. Downtime is measured based on server side error rate.

"**Downtime Period**" means, for a domain, a period of ten consecutive minutes of Downtime. Intermittent Downtime for a period of less than ten minutes will not be counted towards any Downtime Periods.

"**Google Apps Covered Services**" means the Gmail, Google Calendar, Google Talk, Google Docs, and Google Sites components of the Service. This does not include the Gmail Labs functionality or Gmail Voice and Video Chat components of the Service.

"**Monthly Uptime Percentage**" means total number of minutes in a calendar month minus the number of minutes of Downtime suffered from all Downtime Periods in a calendar month, divided by the total number of minutes in a calendar month.

"**Scheduled Downtime**" means those times where Google notifies Customer of periods of Downtime at least five days prior to the commencement of such Downtime. There will be no more than twelve hours of Scheduled Downtime per calendar year. Scheduled Downtime is not considered Downtime for purposes of this Google Apps SLA, and will not be counted towards any Downtime Periods.

"**Service**" means the service provided by Google to Customer under the applicable Google Apps Agreement.

"**Service Credit**" means the following:

Monthly Uptime Percentage	Days of Service added to the end of the Service term, at no charge to Customer
< 99.9% - ≥ 99.0%	3
< 99.0% - ≥ 95.0%	7
< 95.0%	15

## Politique de sécurité

- Une politique de sécurité est généralement axée sur les trois principes 'CIA' :
  - **Confidentialité** : Est-ce que la confidentialité des informations est garantie ?
  - **Intégrité** : Est-ce que les informations sont authentiques, complètes et fiables, non altérées ?
  - **Accessibilité** : Est-ce que les informations sont disponibles pour les personnes concernées ?
- Il existe des normes sur lesquelles se baser pour créer sa Security Policy, en particulier →

# Politique de sécurité

- **ISO/CEI 17799 (devenu ISO/IEC 27002)**
  - Norme internationale concernant la sécurité de l'information
    - publiée en décembre 2000 par l'ISO (2<sup>nd</sup>e édition juin 2005)
  - Titre : *Code de pratique pour la gestion de sécurité d'information*
  - Ensemble de best practices pour la mise en place ou la maintenance des systèmes de gestion de la sécurité des informations
  - Suit également les trois principes 'CIA'
  - Norme → pas obligatoire pour les entreprises, mais est parfois imposée contractuellement

ISO : International Organization for Standardization  
CEI : Commission Electrotechnique Internationale

# Politique de sécurité

- **ISO/CEI 17799**
  - Décomposée en une dizaine de sections principales
  - Couvre la sécurité tant dans ses aspects techniques qu'organisationnels
  - Pour chaque section :
    - **Objectifs** à atteindre
    - Ensemble de **contrôles** / best practices pour les atteindre
  - NB : l'équivalent national au Royaume-Uni est **BS7799**, également fort connu / utilisé

# Politique de sécurité

- **Les sections de la norme ISO/CEI 17799**
  - La politique de sécurité
  - L'organisation de la sécurité
  - Classement en contrôle des informations
  - Facteurs humains
  - Sécurité physique
  - Gestion des communications et des opérations
  - Contrôles des accès
  - Développement et maintenance d'applications
  - Gestion des incidents de sécurité
  - Continuation de l'activité
  - Respect des lois, licences, règlements, etc.

# Politique de sécurité

- **Quelques exemples (1/5)**
  - Sécurisation du matériel, des périphériques et autres
    - Cadenas pour les laptops, fermeture des portes à clé
    - Contrôle d'accès à la salle serveur
    - Utilisation d'UPS
    - Stockage des tapes de backup dans un coffre-fort
    - ...
  - Contrôle des accès à l'information
    - Gestion des utilisateurs et des mots de passe
    - Password policy (nombres de caractères, expiration...)
    - Accès distants
    - Accès aux informations par des tiers
    - Gestion des permissions
    - Utilisation des modems (ex. déconnectés en entrée)

# Politique de sécurité

- **Quelques exemples (2/5)**

- Traitement de l'information
  - Gestion des réseaux
  - Gestion des opérations et administration
  - Email policy
  - Règles en matière d'attachements des mails (pas de fichiers exécutables...)
  - World Wide Web / règles relatives au surf
  - Backups
  - Recovery
  - Archivage
  - Protection des fichiers
  - Encryption de documents
  - ...

# Politique de sécurité

- **Quelques exemples (3/5)**

- Gestion des achats et de la maintenance des logiciels achetés
  - Règles concernant les achats
  - Installations de logiciels
  - Maintenance et mises à jour
  - ...
- Développement de logiciels
  - Contrôle du code
  - Testing
  - Documentation
  - ...
- Cyber criminalité
  - Politique en matière de virus / antivirus
  - Spyware et autres malware
  - ...

# Politique de sécurité

- **Quelques exemples (4/5)**

- Aspects légaux
  - Conservation des logs
  - Conservation des archives
  - Engagement de la responsabilité de la société
  - ...
- Business Continuity
  - Disaster Recovery Plan (DRP)
  - Business Continuity Planning (BCP)
  - ...
- Personnel
  - Départ d'employés de la société
  - Traitement et protection des informations personnelles
  - ...

# Politique de sécurité

- **Quelques exemples (5/5)**

- Training
  - Security awareness
  - Training
  - ...
- Security incidents
  - Détection et résolution d'incidents sécurité
  - Investigations
  - Actions légales
  - ...
- Classification de l'information
  - Niveaux de confidentialité
  - Notion d'information owner
  - ...

# Sécurisation de Windows

Source : « *Windows 2003 and Windows XP security checklist* », document publié par l'ISF (Internet Security Forum - <http://www.securityforum.org>)

## Windows 2003 / XP security checklist

### 1. Créer une infrastructure gérable

- Cela passe par une bonne **découpe de l'AD en OUs** pour la gestion de la sécurité (par GPO en particulier)
- Grouper les users, groups, computers dans des OUs particulières
- Ne mettre les users que dans des **Global groups**
- Ne mettre des permissions sur les ressources que via des **Local groups**
- Eviter la création de users locaux (i.e. ne faisant pas partie d'un domaine – ex. users locaux à une workstation)

## Windows 2003 / XP security checklist

### 2. Etablir des GPO appropriées

- Définition de GPO au niveau du Domaine, qui s'appliquent à tous les users et/ou tous les computers
  - password policy
  - account lockout policy
- La gestion des GPO peut être complexe
  - créer un groupe restreint d'administrateurs gérant les GPO
- Utiliser des GPO pour protéger les stations et les serveurs
  - exemple : interdiction pour un user non administrateur de se logguer sur un Domain Controller
- Verouillage des stations de travail par GPO

## Windows 2003 / XP security checklist

### 3. Restreindre l'utilisation des 'trusts'

- Utiliser les trusts avec la plus grande prudence
  - attention à la transitivité
- Restreindre en particulier les trusts avec des domaines externes à la forêt
- Eviter les trusts entre forêts

## Windows 2003 / XP security checklist

### 4. Implémenter des restrictions au niveau authentification

- Eviter l'affichage du login de la dernière personne qui s'est logguée sur un poste (par GPO)
- Restreindre le nombre de 'cache logons' (par GPO)
  - nombre de fois qu'on peut s'authentifier sur base du caching de ses credentials parce qu'il n'y a pas de Domain Controller disponible
- Afficher un disclaimer avant l'écran de logon
- Utiliser des smart cards pour l'authentification
- Kicker les users qui n'ont pas fait logoff après les heures de bureau
- Utiliser Kerberos
  - désactiver NTLM v1 si pas de 'vieilles' stations NT

## Windows 2003 / XP security checklist

### 5. Implémenter NT File System (NTFS)

- Utiliser NTFS plutôt que FAT32
- Avoir au moins deux partitions sur les serveurs, pour séparer le système des data
  - facilités pour le recovery
- Utiliser du RAID
- Ne pas stocker de données sur les PCs mais bien sur serveur
  - si on stocke quand même des données sur les PCs, utiliser une partition séparée du système pour les données
- Attention, les permissions NTFS sont d'application quand le disque est dans le PC... si on vole le disque il sera lisible dans une autre machine
  - par exemple un Linux avec support NTFS se fiche des permissions présentes sur le disque
  - NB : attention aux 'live CDs' du genre *Knoppix* → protéger physiquement les machines

## Windows 2003 / XP security checklist

### 6. File encryption

- EFS = *Encrypted File System*
- Etablir une politique d'utilisation de EFS et former les utilisateurs à ses avantages et ses dangers
- Faire usage des 'data recovery agents'
  - pour quand même pouvoir retrouver les données en cas de perte de mot de passe ou clé privée par l'utilisateur

## Windows 2003 / XP security checklist

### 7. Stockage de fichiers

- Utiliser le système de quotas
  - pour éviter un déni de service par remplissage de tout l'espace
- Utiliser la fonctionnalité '*Folder redirection*' pour stocker de manière transparente sur serveur certains folders de C:\ (*My Documents, Application Data, Desktop, Start Menu*)
  - évite qu'un autre user se loguant sur le PC y ait accès
  - permet que ces éléments soient backupés
- En cas d'utilisation des '*Offline folders*', attention aux permissions NTFS sur la copie locale des fichiers

## Windows 2003 / XP security checklist

### 8. Empêcher le chargement d'un autre OS

- Protection au niveau du BIOS pour empêcher de booter sur une disquette, un CD, une clé USB...
- Ne pas stocker les données sur les PCs
- Installer un outil tiers d'encryption du disque dur
  - empêchant que le disque soit lisible si un autre OS est booté ou le disque branché dans une autre machine

## Windows 2003 / XP security checklist

### 9. Supprimer les programmes inutiles et désactiver les services inutiles

- N'installer que le strict nécessaire
  - par exemple, éviter d'installer IIS (serveur web) si ce n'est pas requis
- Désactiver les services suivants, sauf besoins spécifiques :
  - Alerter, Certificate Services, DHCP Server, DNS Server, FTP Publishing, IMAPI CD – Burning COM Service, Infrared Monitor, IIS Admin, NNTP, SMTP, Telnet, Terminal Services / Remote Desktop, TFTP, WINS, Wireless Configuration, WWW Publishing...
- Restreindre l'accès aux programmes tels que les éditeurs de la Registry (regedit, regedt32), exécutables du style Telnet, FTP, finger, attrib, cacls, dialer, hyperterm...
  - via les permissions NTFS
  - par GPO

## Windows 2003 / XP security checklist

### 10. Protéger la disponibilité des serveurs

- Restreindre qui peut s'y loguer
- Restreindre les connexions à distance aux seuls administrateurs
- Restreindre qui peut faire un shutdown/reboot
- Mettre en place un système d'alerte en cas de problème / plantage ('stop errors' en particulier)

### 11. Se protéger des pannes de courant

- Utiliser des UPS

## Windows 2003 / XP security checklist

### 12. Protéger l'Active Directory

- Mettre adéquatement les permissions sur les objets de l'AD
- Mettre des permissions NTFS correctes sur le répertoire \SYSVOL des domaines contrôleurs
  - ce répertoire (souvent sur un volume distinct) stocke les fichiers relatifs à l'AD
- S'assurer de la présence d'un Global Catalog dans chaque site géographique / physique
- Faire une bonne découpe en Sites
  - et fine-tuner la réplication inter-site pour qu'elle ne pénalise pas le trafic entre sites (ex. réplication nocturne...)

## Windows 2003 / XP security checklist

### 13. Protéger le contenu de la Registry

- Utiliser des GPO pour empêcher les users de modifier des clés de registry sur leur PC / en restreindre l'accès
- Backuper le répertoire qui contient la registry
  - \WINDOWS\System32\Config

## Windows 2003 / XP security checklist

### 14. Restreindre l'environnement utilisateur

- Utilisation de GPO pour...
  - empêcher l'exécution de programmes (suppression de la fonction 'Run' du menu Démarrer)
  - restreindre l'accès au Control Panel des PCs
  - mettre un screen saver avec password
  - locker les stations automatiquement après quelques minutes d'inactivité
  - restreindre les heures auxquelles un utilisateur peut se loguer
  - éviter la fonction d'auto-logon

## Windows 2003 / XP security checklist

### 19. Mettre en œuvre un contrôle des mots de passe

- Utiliser les fonctions relatives aux passwords
  - password age
  - password length
  - password history
  - password complexity requirements
- Prévoir le locking des users qui se trompent de mot de passe un peu trop
  - par exemple au bout de trois erreurs
- Utiliser l'option '*User must change password at next logon*' lors de la création d'un compte
- Mettre des requirements plus stricts (longueur etc.) sur les mots de passe des comptes administrateur

## Windows 2003 / XP security checklist

### 20. Minimiser l'utilisation du compte *Administrator*

- Ne pas travailler en tant qu'administrateur quand ce n'est pas strictement nécessaire
- Attribuer à chaque administrateur un compte personnel avec les droits admin
  - exemple : travailler en tant que *delavaa* quand pas besoin de privilèges admin
  - travailler en tant que *admin-delavaa* quand privilèges admin nécessaires
  - ne pas travailler en tant que *Administrator*
- Désactiver le compte *Administrator* local sur les stations et member servers
- Créer un compte *Administrator* local bidon avec aucun droit et l'audit activé

## Windows 2003 / XP security checklist

### 21. Restreindre le nombre de membres des groupes Domain Admin, Administrators

- et autres groupes ayant des privilège de niveau administrateur

## Windows 2003 / XP security checklist

### 22. Permissions sur les folders et fichiers

- Windows 2003 met par défaut des permissions restrictives sur la racine de chaque partition, ce qui n'est pas le cas de Windows XP
  - modifier ces permissions sur Windows XP
- Utiliser le groupe '*Authenticated users*' plutôt que '*Everyone*'
- Ne pas attribuer de permissions '*Full control*' sauf aux administrateurs
  - utiliser plutôt '*Modify*'
- D'une manière générale, implémenter des permissions en ligne avec la Security Policy
- Utiliser l'outil '*Security Configuration and Analysis*'
  - pour faire un review / une analyse des permissions
  - pour créer des templates de permissions applicables par GPO

## Windows 2003 / XP security checklist

### 23. Restreindre l'accès aux ressources partagées

- Utilisation des *shares* avec prudence, et sur des filesystems NTFS plutôt que FAT32
- Mettre les permissions les plus restrictives possibles au niveau des *shares*
  - utiliser '*Authenticated users*' plutôt que '*Everyone*'
- Ne pas permettre les accès non sécurisés aux *shares*
  - interdire par exemple les mots de passe à blanc (vide)
- Restreindre les permissions sur les imprimantes partagées
  - via le *Control Panel* → *Printers*
- Placer les données sur serveur et les rendre accessibles via des *share* pour qu'elles soient partagées
  - éviter les *shares* sur les PCs

## Windows 2003 / XP security checklist

### 24. Appliquer les mises à jour de sécurité fournies par Microsoft

- Après un testing approprié
- Au moyen de Windows Server Update Services (**WSUS**)
- Au moyen d'un produit de distribution logiciel
- Appliquer également les Service Packs
- Utiliser **MBSA** (*Microsoft Baseline Security Analyser*) pour inventoriser les patches installés / manquants

## Windows 2003 / XP security checklist

### 25. Restreindre les protocoles réseau

- Si possible n'activer / n'utiliser que TCP/IP
- Activer le firewall intégré de Windows 2003 et Windows XP Service Pack 2
- Activer le logging complet du serveur DHCP

### 26. Remote Access Server

- N'activer la fonction RAS sur un serveur que si c'est requis (en ligne avec la Security Policy)
- Utiliser MS-CHAPv2 ou MS-CHAP pour l'authentification plutôt que PAP (non encrypté)
- Désactiver l'option '*Allow remote system to connect without authentication*' (!)
- ...

## Windows 2003 / XP security checklist

### 27. Dial-out

- Empêcher, sauf si c'est strictement nécessaire, le dial-out au niveau des machines
  - pour éviter par exemple qu'un PC soit en même temps connecté au LAN par un câble réseau et à Internet par modem
- Utiliser une GPO pour empêcher les utilisateurs de modifier les éventuelles configurations dialup de leur PC
- Activer le firewall de Windows XP sur les connexions dialup
- Bloquer l'*Internet Connection Sharing* (ICS) pour éviter de créer des passerelles entre réseau local et réseau distant appelé par modem

## Windows 2003 / XP security checklist

### 28. Envisager l'utilisation d'IPSec

- IPSec peut tout à fait être utilisé sur un réseau interne, par exemple entre stations et serveurs sensibles
  - peut être géré par GPO

### 29. Protéger le DNS

- Eviter le DNS poisoning
  - c'est-à-dire le fait d'aller polluer le DNS avec de fausses informations
  - pouvant amener un client à se connecter à un 'faux' serveur
- En ne permettant pas les '*unsecure dynamic updates*'
- En utilisant les droits ad hoc
  - utilisation du groupe *DnsAdmins*
- Seul un *Enterprise Admin* peut 'autoriser' un serveur DHCP

## UNIX Security Checklist v2.0

### 1. Patches

- Toujours installer (après test) les derniers patches tant pour l'operating system que les applications qui tournent dessus (Bind, Apache, Sendmail...)
- Vérifier la signature prouvant l'authenticité du patch (PGP, GnuPG...) et / ou la checksum du fichier (MD5...)

# UNIX Security Checklist v2.0

## 2. Network services

- Points d'attention :
  - *inetd* : considérer son remplacement par *xinetd* ou sa désactivation
  - *finger* : désactiver le service si pas nécessaire
  - commandes « r » (*rlogin*, *rcp*, *rsh*...) à désactiver ; limiter les machines dans */etc/hosts.equiv* ; interdire les fichiers *\$HOME/.rhost*
  - */etc/login.access* permet de restreindre qui peut se logger, par exemple à distance
    - éviter de permettre le login à distance en tant que *'root'*
    - utiliser plutôt un compte utilisateur normal puis faire *'su'*
  - attention à la config. de PAM
  - désactiver le *portmapper* si pas nécessaire
  - ...

# UNIX Security Checklist v2.0

## 3. Network administration

- Packet filtering :
  - utiliser un filtre de paquets, tel qu'*IPTABLES* sous Linux, pour restreindre le trafic autorisé au strict nécessaire
  - désactiver le routage IP s'il n'est pas nécessaire
    - *echo 0 > /proc/sys/net/ipv4/ip\_forward* (sous Linux)
- Denial of Service (DoS)
  - prendre les mesures nécessaires pour ne pas être utilisé pour une attaque de type DoS (ex. filtrer également en sortie)
- Encryption and Strong Authentication
  - pour les connexions d'administration par exemple (typiquement, **SSH** avec clés)

# UNIX Security Checklist v2.0

## 4. File system security

- Mount
  - utiliser les options *nosuid*, *noexec* quand c'est possible
  - utiliser des quotas
- Vérifier les permissions sur les startup/shutdown scripts
- Faire attention aux permissions d'une manière générale
  - en particulier sur les binaires, scripts
- Utiliser par exemple **Tripwire**
  - outil d'auditing permettant de voir les modifications de fichiers, ownership, permissions... (<http://sourceforge.net/projects/tripwire/>)
- ...

# UNIX Security Checklist v2.0

## 5. Account security

- Utiliser les *shadow passwords*
- Utiliser **PAM**
  - password aging et autres restrictions sur les mots de passe
- Utiliser *sudo* plutôt que de donner le mot de passe de '*root*' à plusieurs utilisateurs
- Auditer les logon failures
- Ne pas autoriser les accounts sans mot de passe (blank password)
- Désactiver les accounts non nécessaires, ne pas attribuer de shell aux accounts utilisés par des services (*/sbin/nologin* ou */bin/false*)
- Attention particulière au compte *root*
- Vérifier que *root* n'a pas « . » dans son \$PATH
- Faire tourner un password cracker de temps en temps, pour vérifier la fiabilité des mots de passe des utilisateurs
- ...

# UNIX Security Checklist v2.0

## 6. System monitoring

- Account security
  - expiration des mots de passe
  - logging des logons et tentatives
  - process accounting...
- Log files
  - utiliser syslog, logrotate
  - protéger et backuper les fichiers de log
  - exporter les logs vers une autre machine
- Garder un logbook des opérations effectuées sur le serveur
- ...

# UNIX Security Checklist v2.0

## 7. Name service

- Toujours utiliser la dernière version de BIND
- Désactiver les dynamic updates, sauf quand c'est nécessaire
  - utiliser des dynamic updates sécurisées (avec clé)
- Considérer l'utilisation de BIND dans un chroot

## UNIX Security Checklist v2.0

### 8. Electronic mail

- Attention à la sécurité de Sendmail
- Toujours utiliser la dernière version, appliquer les patches
- Configurer le MTA pour ne pas servir d'open relay
- Attention à l'exécution de commandes via */etc/aliases*
- Postfix est une alternative à Sendmail jugée plus sécurisée (et plus simple à configurer, ce qui est p-ê lié d'ailleurs)

## UNIX Security Checklist v2.0

### 9. Web security

- Envisager de faire fonctionner un serveur web, s'il est strictement nécessaire, en chroot
- Ne pas exécuter le daemon (*httpd* par exemple) en tant que root
- Attention aux permissions sur les scripts CGI
- Considérer l'utilisation de SSL (HTTPS)
- Eviter de permettre le listing des fichiers d'un directory
- ...

## UNIX Security Checklist v2.0

### 10. FTP

- Utiliser la dernière version du daemon serveur FTP de son choix
  - conseillé : *vsftpd (Very Secure FTP daemon)*
- Interdire la commande SITE EXEC
- Utiliser */etc/ftpusers* pour interdire à certains users (tels que root, bin...) de se connecter en FTP au serveur
- Ne pas permettre le FTP anonyme si ce n'est pas nécessaire
- Attention aux permissions
- Limiter les directories writable (par exemple */incoming*), utiliser des quotas
- ...

## UNIX Security Checklist v2.0

### 11. NFS

- Bloquer NFS sur les firewalls en bordure du réseau interne
- Toujours appliquer les (nombreux) patches de sécurité de NFS
- Considérer l'utilisation d'alternatives, telles que Samba
- Attention à */etc/exports*
  - limiter les entrées au strict nécessaire
  - utiliser le FQDN plutôt que hostname court d'une machine
  - quand c'est possible, limiter les experts en read-only
- Protection du client (qui n'a pas confiance en le serveur) : *nosuid, noexec*
- Protection du serveur (qui n'a pas confiance en le client) : *root\_squash*
- Restrictions au niveau de portmap (*/etc/hosts.deny* et */etc/hosts.allow*)

# UNIX Security Checklist v2.0

## 12. X Window

## Sécurisation de Linux – SE Linux

- Sous Linux,
  - **SELinux (Security Enhanced Linux)**
    - *SELinux is an enhancement to the Linux kernel that implements mandatory access control (MAC) and role-based access control (RBAC)*
  - Voir <http://www.nsa.gov/selinux/>
  - Philosophie différente
    - DAC : **Direct Access Control** – ne protège pas des logiciels buggués ou malicieux, un process qui tourne en temps que userX a accès à tous les fichiers (et autres) de userX (userX = parfois root...)
      - c'est le comportement par défaut de UNIX dont Linux
    - MAC : **Mandatory Access Control** – on définit des *polices* qui indiquent les interactions permises entre sujets (users, processes, programmes) et les objets (fichiers, devices)

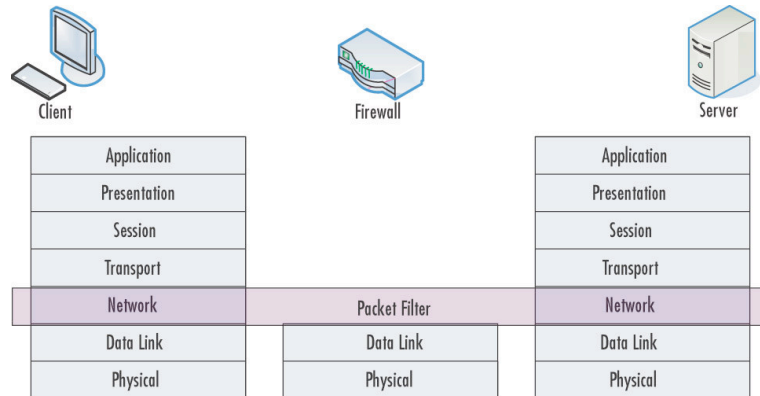
# Firewall

# Firewall

- Logiciel ou device hardware qui **permet de filtrer le trafic** entre différents segments réseau
- Constitué au minimum d'un **filtre de paquets**
  - filtrage sur base de l'IP source, de l'IP destination
  - du protocole (TCP, UDP...), du port
    - parfois on parle de « services » (FTP, HTTP, CIFS...)
  - parfois en fonction de l'interface
  - en fonction de certaines options (fragments IP...)
- Accessoirement, un firewall est un **routeur**
  - permet de **segmenter** le réseau en **zones** (LAN interne, Internet, zones démilitarisées, appelées **DMZ**...)

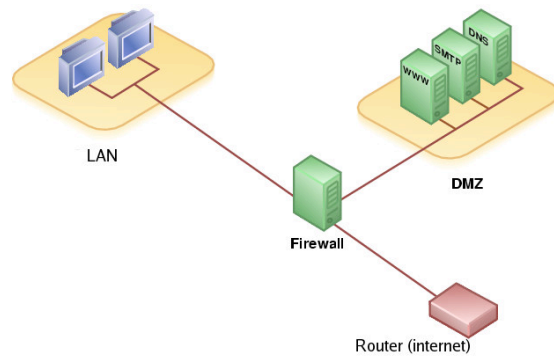
# Firewall

- Illustration du concept de *packet filter*



# Firewall

- Exemple de segmentation typique



# Firewall

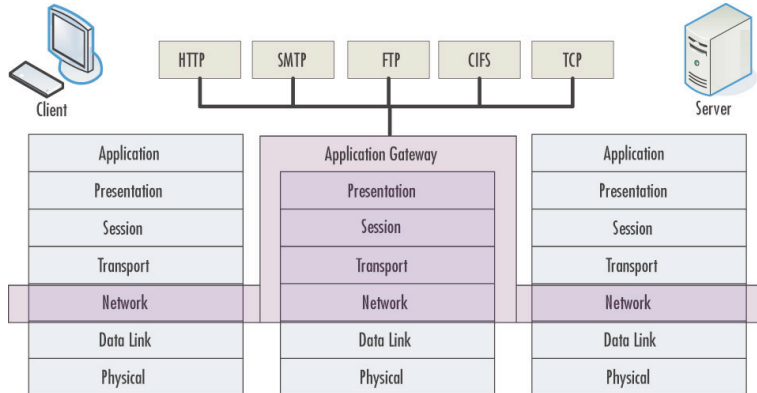
- Les premiers filtres de paquets étaient **stateless**
  - chaque paquet est analysé indépendamment des autres, et comparé à la liste de règles pré-configurée
  - mécanisme d'ACL de base implémenté dans beaucoup de routeurs
  - pas terrible car ne tient pas compte des états
    - exemple : dans le protocole TCP, un paquet ACK est envoyé en réponse d'un paquet SYN
- De nos jours tous les firewalls sont **statefull**
  - possèdent une table d'état
    - état des connections en cours
    - permet de décider si le paquet suivant sera accepté ou pas

# Firewall

- **Proxies / firewalls dits 'applicatifs'**
  - au dessus du filtre de paquets statefull, beaucoup de firewalls peuvent maintenant inspecter le contenu de certains protocoles
  - on parle de **proxies**, de **protocol inspection**, d'**application layer filtering**
  - par exemple, vérifier que c'est bien de l'HTTP qui passe via le port TCP 80
  - seuls les protocoles les plus populaires sont généralement inspectés : HTTP, FTP, DNS, telnet, CIFS, ...
  - permet également une meilleure sécurité pour les protocoles qui choisissent dynamiquement un port non privilégié
    - exemple, le canal data de FTP (commande PORT interceptée par le firewall qui n'ouvre alors que le port requis – avant il fallait ouvrir 1024 à 65535)

# Firewall

- Illustration du concept de *application layer filtering*



# Firewall

- Certains firewalls permettent même des **règles par user** plutôt que basé IP source / destination
- Historiquement, les firewalls sont utilisés pour séparer le réseau internet du monde extérieur (Internet)
  - de nos jours, le réseau interne n'est plus sûr et on voit de plus en plus de firewalls utilisés pour de la segmentation du LAN
    - par exemple pour filtrer le trafic entre PCs et data center (serveurs)
- On assiste de plus en plus à l'incorporation de fonctionnalités IDS/IPS directement dans les firewalls
  - attention à la consommation de ressources

# Firewall

- Les leaders du marché

- CheckPoint VPN-1/Firewall-1

- leader incontesté mais aussi le plus cher
    - software (pour Windows, Linux/SPLAT, Solaris)
    - interface de management inégalée
    - existe sous forme d'*appliances* : Nokia principalement



We Secure the Internet.

- Cisco PIX



- Juniper NetScreen



- ...

- Pour Linux, Netfilter/IPtables

The screenshot shows the Check Point SmartDashboard interface for Firewall-VPN. The main window displays a table of firewall rules with the following columns: SOURCE, DESTINATION, VPN, SERVICE, ACTION, and TRACK. The rules are as follows:

SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
Corporate-internal-net	GW-group	Any Traffic	Any	drop	Alert
Any	Any	All_GwToGw	CIFS, ftp, http, https, smtp	accept	Log
Any	Corporate-dmz-net	Any Traffic	http, https, smtp	accept	Log
Corporate-mail-server	Internal-net-group	Any Traffic	smtp	accept	Log
Internal-net-group	Any	Any Traffic	Any	accept	Log
Any	Any	Any Traffic	Any	drop	Log

Fin

Présentation du projet

# Rappel

- Powerpoint / PDF
- 20 minutes de présentation (testez!)
- Tout le monde parle

# L'examen

# Trois parties

- **Partie technique**  
Vous choisissez votre question!
- **Partie connaissances générales**
- **Questions sur votre projet**  
Assez technique, pour vérifier que vous avez participé.

# Question I : sujets

- Virtualisation
- Administration Unix: shell, utilisateurs, services, ...
- DNS
- LDAP
- NIS/Yellowpages, combinaison avec NFS

## Question I : sujets

- SNMP et administration centralisée
- E-mail
- Windows/Samba
- Politiques de sécurité
- Nagios
- Mercurial

## Question I : sujets

- Asterisk
- FAI

# Question 1

- Dans tous les cas (même si pas vu comme tel aux cours/TPs)
- Qu'est-ce que c'est? / Cas typique d'utilisation
- Comment ça s'installe/fonctionne?
- Détails techniques et théoriques (ex: DNS)

25% de la cote

# Question 2

- Sujet: le cours/TP
- Aucun détail
- Question tirée au hasard
- Exemple: Virtualisation: intérêts pour un administrateur système?

25% de la cote

## Question 3: votre projet

- 2 questions très rapides
- Quel est le sujet?
- Petite question technique issue du rapport...

50% de la cote

Merci