13 octobre 2015

La sécurité des SAN

Présentation à l'OSSIR / Groupe Paris

Pierre-Charles Wagrez

Architecte Référent Réseaux & Télécoms

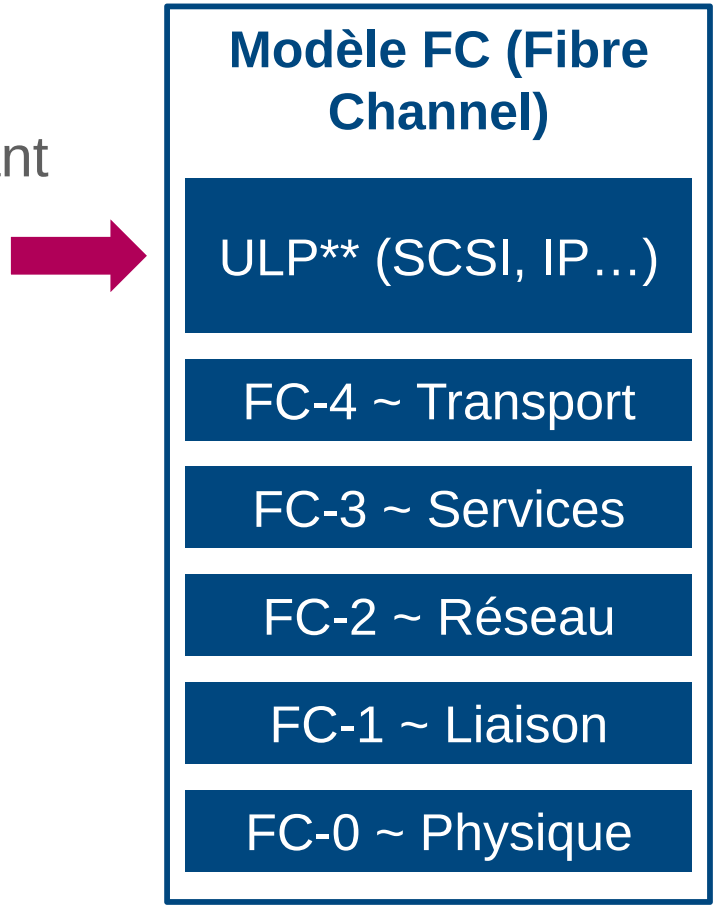
solucom
management & IT consulting

Agenda

1. Un SAN c'est quoi ? Rappels
2. Quelles menaces ?
3. Que peut et doit on faire ?
4. Quel impact de la convergence LAN/SAN ?
5. Quid des NAS ?
6. Liens utiles

Le SAN : un réseau d'accès au stockage

- **SAN** = ***Storage Area Network***
- Un réseau et une couche de protocoles permettant de transporter des trames **SCSI***
- Hiérarchie comparable au modèle OSI
- Les différents protocoles sont définis dans les standards FC-BBx *(x étant le numéro de révision)*
- Les SAN sont apparus avec les besoins de consolidation du stockage
- Le SAN constitue actuellement un élément incontournable de la majorité des DataCenter
- Les alternatives sont : **DAS** (Directly Attached Storage) et le **NAS** (Network Attached Storage)

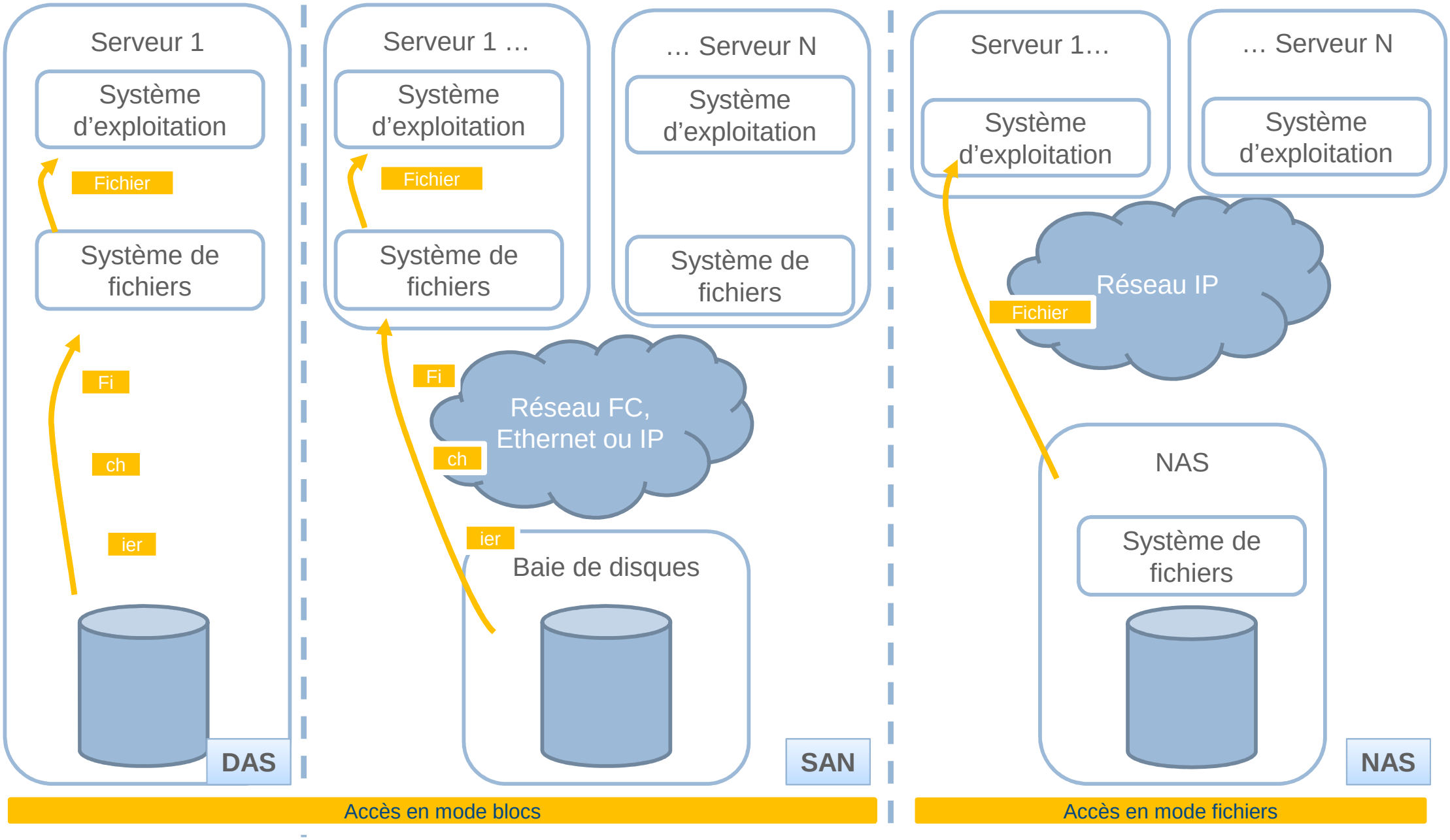


Les mainframes IBM utilisent plutôt FICON (ESCON sur fibre), assez proche de FC

** Protocole d'accès disque en mode blocs, comme IDE ou SATA*

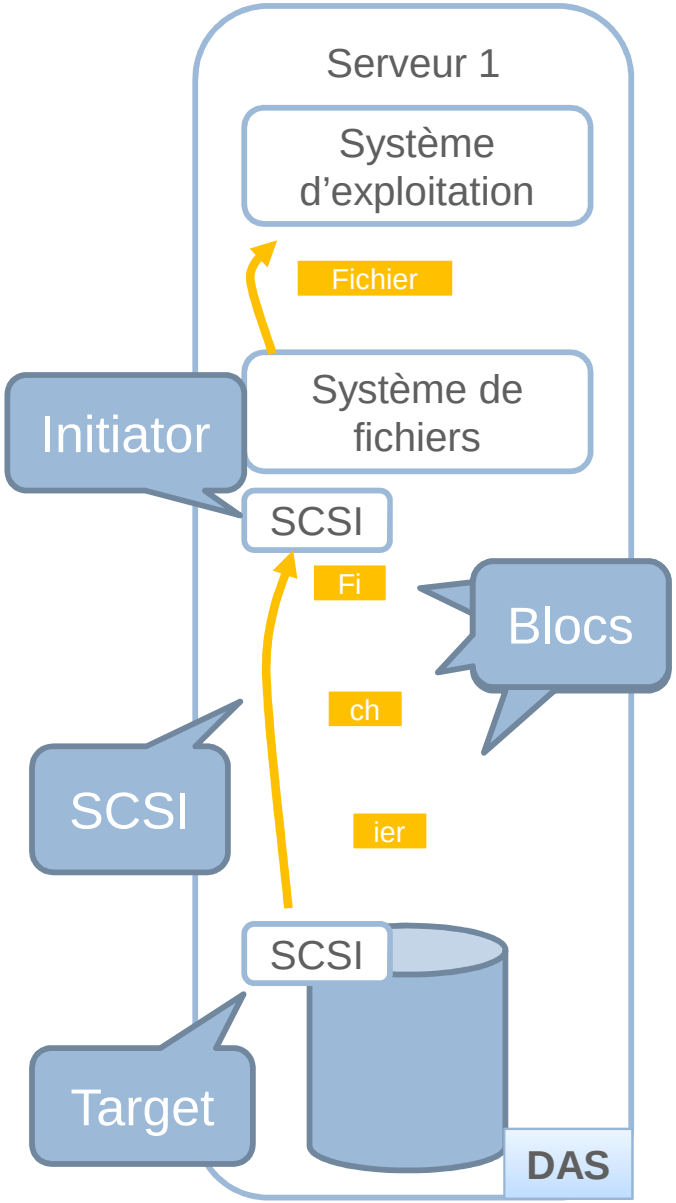
*** ULP = « Upper Layer Protocol »*

Repositionnement des modèles d'accès au stockage



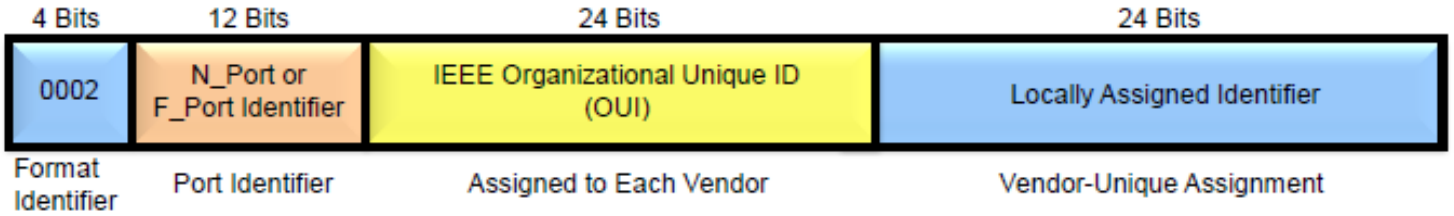
Zoom sur SCSI

- **SCSI** = ***Small Computer System Interface***
- SCSI définit des « **Initiator** » et des « **Target** »
- Les disques sont définis par des « **LUN** » (Logical Unit Number), un id de 64 bit
- Accès aux disques en mode « **blocs** » *(par opposition au mode « **fichiers** » sur un serveur de fichiers)*
- SCSI peut être transporté sur des câbles cuivre directement *(modèle DAS)*, Fibre Channel *(SAN)* ou IP *(ex : iSCSI)*



Zoom sur Fibre Channel
Les communications

- Les communications Fibre Channel s'appuient sur
  - **World Wide Name** ~ Nom, inscrit en dur dans le composant comme une @MAC
    - World Wide Node Names => Nom logique d'un nœud (1 par serveur)
    - World Wide Port Names => Nom logique d'un port (1 par port de carte sur le serveur)

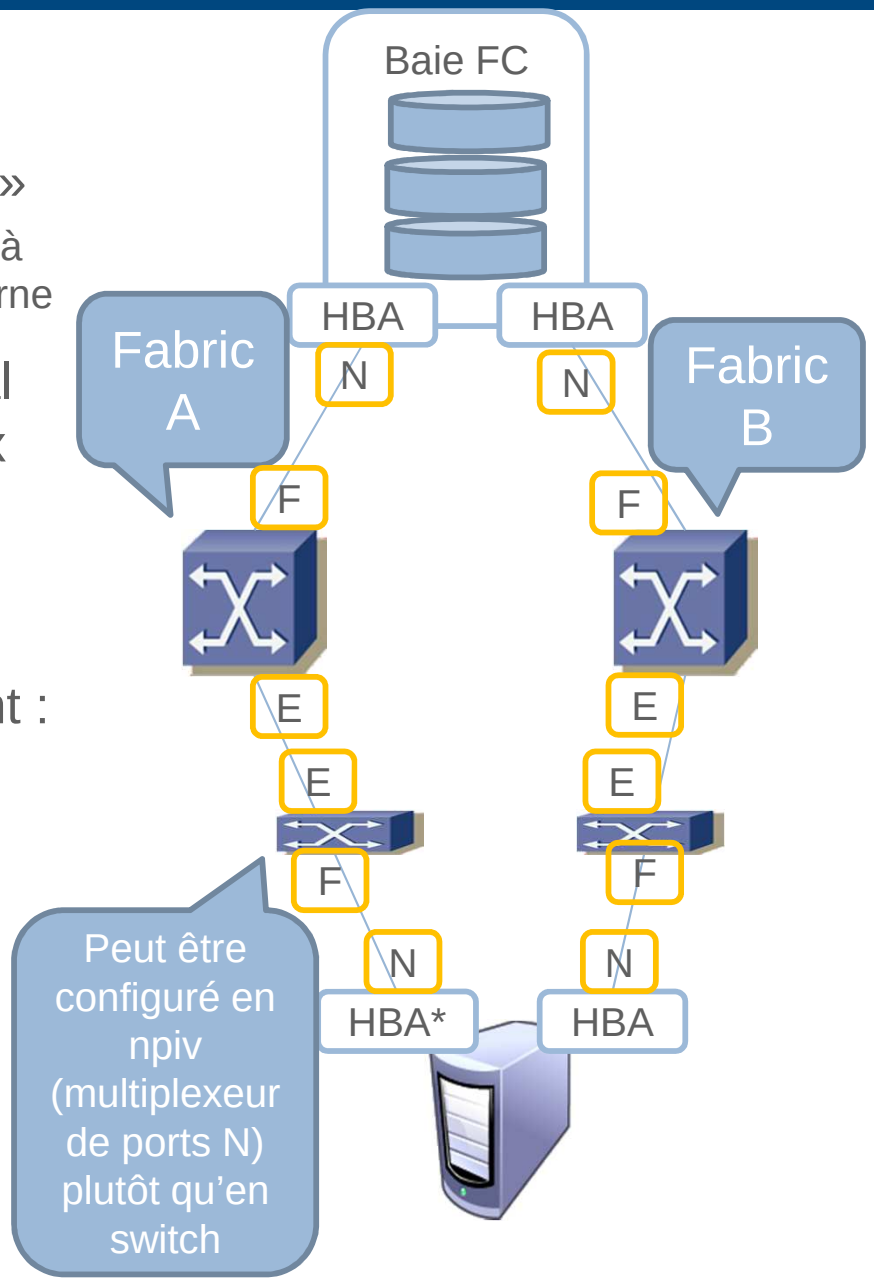


  - **FCID** ~ Adresse IP, attribuée dynamiquement par le SAN
    - Domain-ID du switch (8bits) – Aire (8 bits) – ID machine (8 bits)
- Le routage Fibre Channel s'appuie sur les FCID uniquement
- Les tables de routage sont construites dynamiquement grâce au protocole **FSPF** (Fabric Shortest Path First), comparable à OSPF dans le monde IP
- Afin d'assurer le transport des trames SCSI sans perte, Fibre Channel utilise un mécanisme de **Buffer-to-Buffer Credit**
  - Un port ne peut envoyer une trame vers le port de destination que s'il a reçu une information de ce port indiquant qu'un Credit y était disponible

Zoom sur Fibre Channel
La topologie

- La topologie la plus courante en entreprise est la « **Fabric** », à base de switchs et/ou « **Directeurs** »
  - Les switches sont nommés « **Directeurs** » s'ils répondent à un cahier des charges strict en termes de redondance interne
- La perte de l'accès à ses disques étant en général fatale à un serveur, on utilise le plus souvent deux Fabric complètement séparées
  - Un driver sur la baie et le serveur (**MPIO driver**) assure partage de charge et bascule
- Les ports ont des rôles définis, les principaux étant :
  - **F Port** = Port d'accès d'une Fabric
  - **N Port** = Port de nœud (serveur ou baie)
  - **E Port** = Expansion Port, un port entre deux switches
- Un des switchs est élu comme « Principal » et porte les services de la Fabric, dont entre autres :
  - Attribution des Domain-ID aux switches
  - Serveur de Nom WWPN – FCID
  - Login à la Fabric

HBA : Host Bus Adapter, la carte de raccordement à un SAN Fibre Channel



Zoom sur Fibre Channel
La connexion à la Fabric et à un LUN

❶ FLOGI (Fabric Login) et attribution du FCID

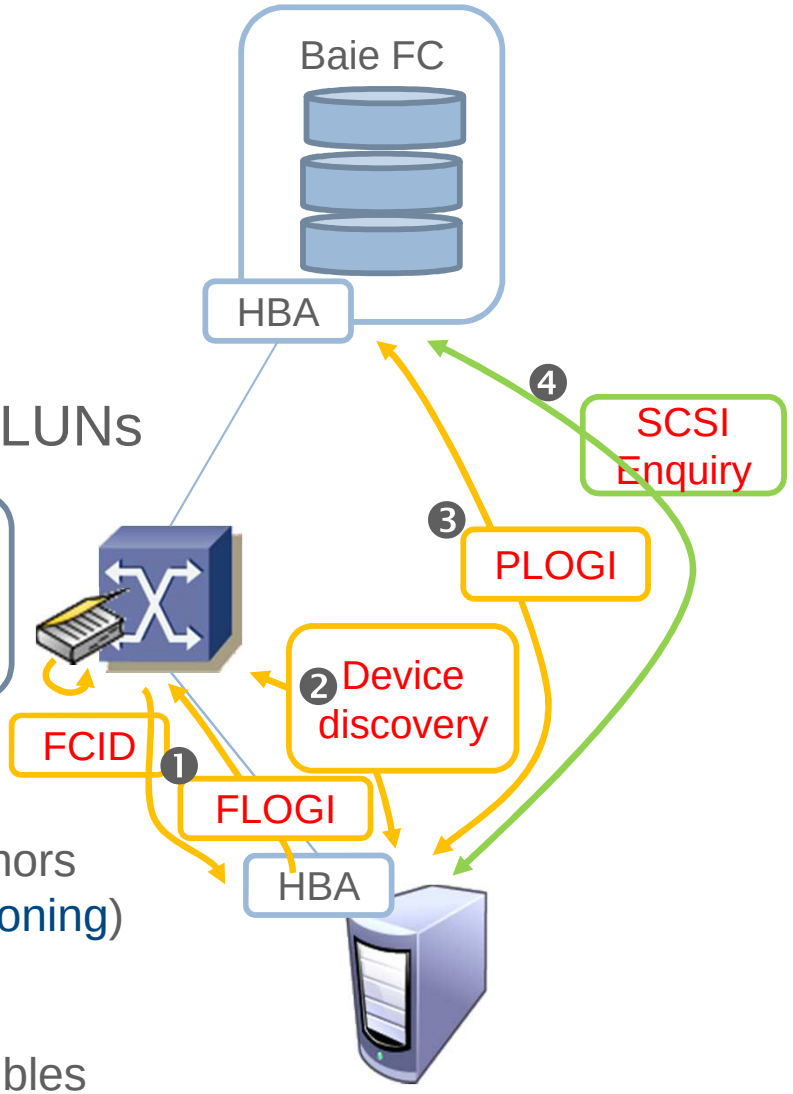
↳ Inscription dans l'annuaire de la Fabric (Name Server)

❷ Requête pour obtenir la liste des targets via le service de noms

❸ PLOGI (Port Login) aux targets identifiées

❹ Scan SCSI des targets pour obtenir la liste des LUNs

Tout LUN exposé est « acquis » par le serveur…
d'où utilisation de « Zoning » et « LUN masking »



- **Zoning** ***(par WWN ou par port)***
  - Filtrage au niveau de la Fabric empêchant ceux en dehors d'une zone de se voir (soft zoning) et/ou parler (hard zoning)
- **LUN Masking**
  - Filtrage au niveau de la baie restreignant les LUNs visibles par un serveur donné

Agenda

1. Un SAN c'est quoi ?
2. Quelles menaces ?
3. Que peut et doit on faire ?
4. Quel impact de la convergence LAN/SAN ?
5. Quid des NAS ?
6. Liens utiles

Une liste de menaces classique

Reconnaissance

Atteinte à la confidentialité des informations

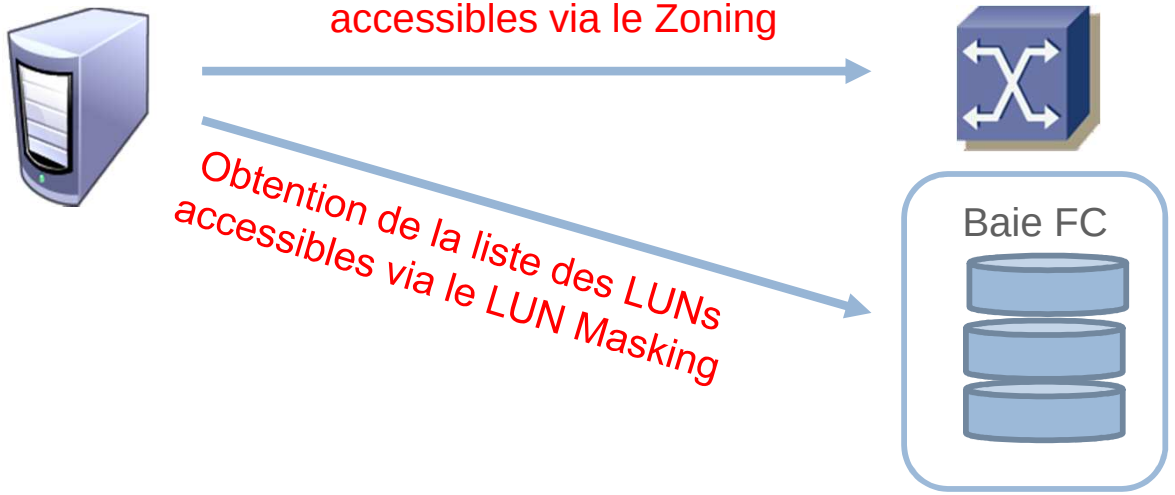
Déni de Service

Atteinte à l'intégrité des informations

- Cette présentation se focalise sur la sécurité du SAN, donc le réseau d'accès au stockage…
- … il est bien évident que d'autres vecteurs d'attaques du stockage existent
  - Via les **outils d'administration** du stockage
  - Via les **infrastructures de sauvegarde**

Attaques de reconnaissance

- Attaques de reconnaissance en tant que client (N_Port)
  - Le SAN permet naturellement à un client de découvrir tous les autres nœuds qui lui sont accessibles au travers du Zoning
  - Sur chaque baie le client peut voir tous les LUNs qui ne lui sont pas masqués



Réalisable nativement et aisément depuis n'importe quel serveur raccordé au SAN… mais les informations sont celles autorisées par le zoning

Si le filtrage n'est pas soigné un serveur a naturellement visibilité sur beaucoup de choses

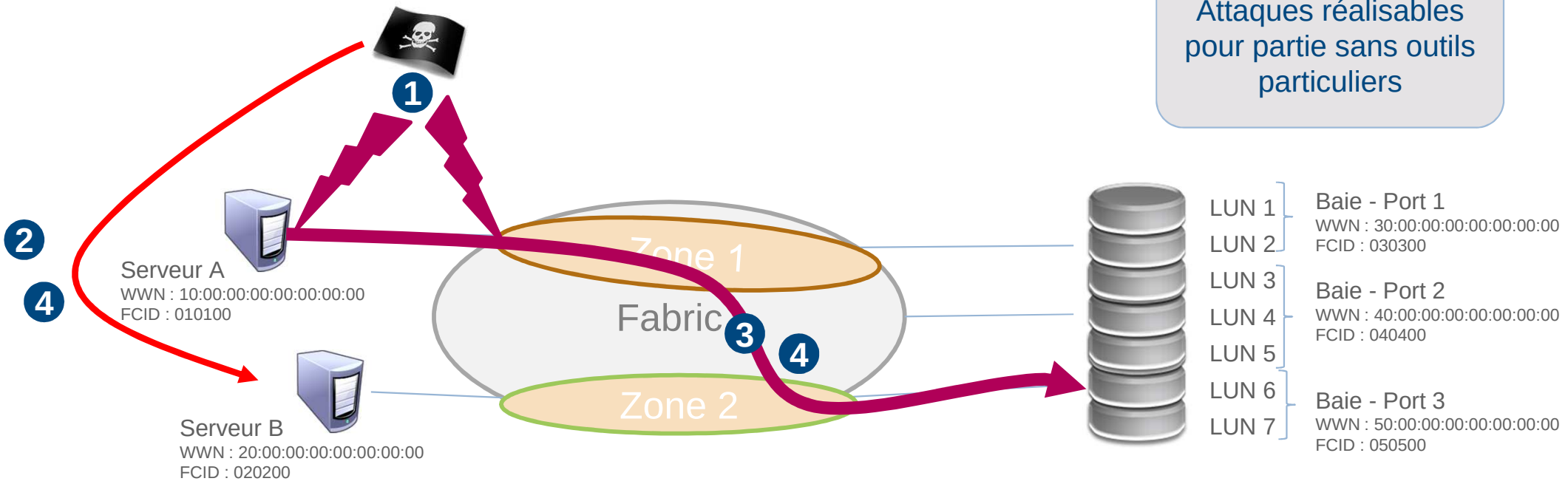
Attaques de reconnaissance

- Attaques de reconnaissance en tant que switch (E_port)
  - Lorsqu'un switch intègre la Fabric, il reçoit copie de la configuration et notamment du Zoning, des Alias éventuellement configurés et a accès à la table de noms. On parle de « E_Port Replication ».
  - Il est aussi possible de tenter de forger les trames FC permettant d'accéder au Fabric Management Service

Un switch accepté par la Fabric a accès à l'intégralité de la configuration et peut la modifier

Accès illégitime aux données par usurpation

Attaques réalisables pour partie sans outils particuliers



1 Compromission d'un serveur raccordé au SAN ou raccordement à un port du SAN

2 Collecte d'informations sur le réseau SAN et récupération des informations d'identification du serveur B

Écoute au niveau d'une HBA / Compromission switch … ou bien requêtes WMI sur le serveur B (obtention WWN, pWWN, modèle HBA…)

↳ http://gallery.technet.microsoft.com/scriptcenter/Find-HBA-and-WWPN-53121140

3 Usurpation de l'identité du serveur B : rebond de la zone 1 vers la zone 2

{ou

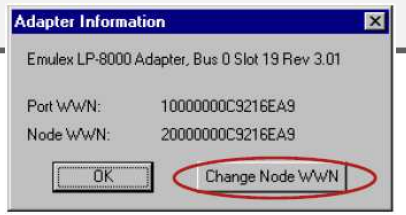
A. Pollution du Name Server pour contourner un zoning par WWN ⇨ Ecrasement de l'entrée existante pour le serveur B

B. Changer le WWN pour contourner le zoning par WWN et le LUN masking ⇨ Usurper le pWWN du serveur B

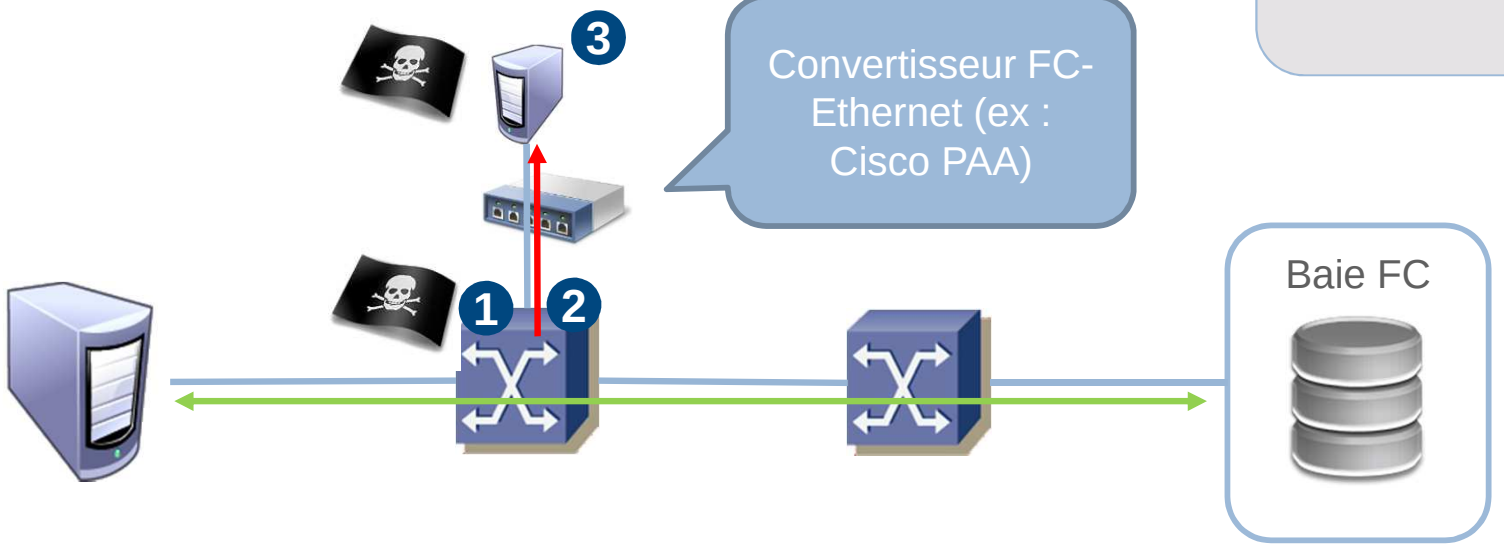
4 Déni de service sur le serveur B ou requête forgée pour démonter le LUN du serveur B

Permet d'utiliser le disque sans perturbations

Modification du WWN via les outils du driver de la HBA ⇨



Accès illégitime aux données par interception



1. **Compromission d'un switch SAN ou insertion d'un switch pirate (ou d'un boîtier TAP fibre)**
   Note : l'usage de TAP ne fonctionnera pas si le lien est chiffré (ex : Cisco TrustSec)
2. **Reconfiguration du switch pour copier les flux vers le serveur pirate**
3. **Capture des flux SCSI transportés dans FC en continu et donc reconstitution des blocs de disques accédés par les serveurs**

Déni de service

- Plusieurs moyens de déni de service
  - **Envois répétés de RSCN** *(Register State Change Notification)* pour interrompre les I/Os et provoquer une reconfiguration des devices de la Zone
    - Chaque nœud recevant un RSCN va s'interrompre, interroger le switch pour connaître les changements puis scanner d'éventuelles nouvelles targets SCSI
    - Un trop grand nombre peut provoquer des I/Os erreurs au niveau de l'OS du serveur, voire des crashes
  - Prise de contrôle de LUNs pour **écraser les données**
  - **Corruption des données de configuration de la baie** via le LUN de configuration sur les baies le permettant
  - Envoi de fortes volumétries sur le SAN pour tenter de **provoquer des congestions** sur le SAN, et donc des ralentissements, ou une surcharge de la baie

Agenda

1. Un SAN c'est quoi ?
2. Quelles menaces ?
3. Que peut et doit on faire ?
4. Quel impact de la convergence LAN/SAN ?
5. Quid des NAS ?
6. Liens utiles

Que faire ?

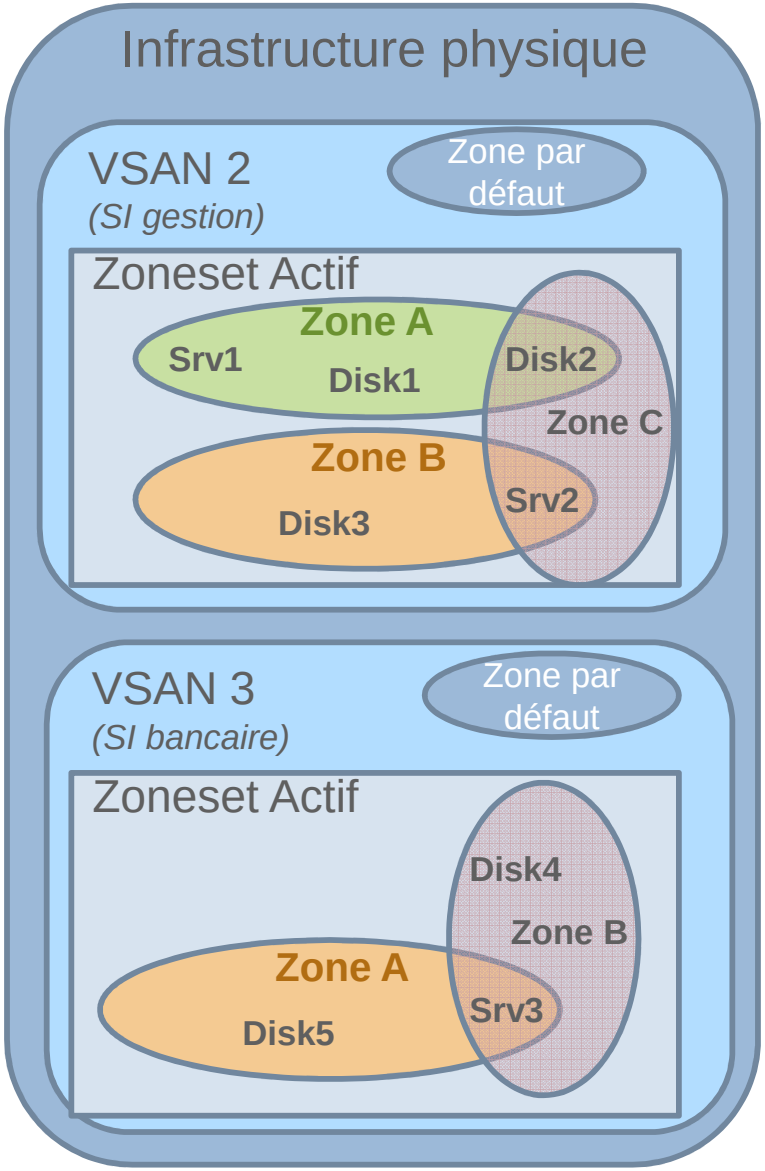
- **Sécuriser l'accès en administration** des équipements SAN et des baies
- **Protéger les services internes** du SAN et plus globalement l'infrastructure
- **Sécuriser le raccordement** au SAN
- **Contrôler** les possibilités **d'échanges entre nœuds**
- **Contrôler l'accès aux données**
- Assurer la **confidentialité des données**
- **Surveiller les événements**

Que faire ?
Sécuriser l'accès en administration

- Les règles de sécurisation sont les règles classiques
  - **Filtrer et sécuriser l'accès** aux interfaces d'administration des équipements ainsi qu'aux serveurs d'administration/supervision
    - **Réseau IP Out Of Band** entre les équipements et les serveurs d'administration
      - Si l'administration est effectuée In-Band, recourir à **CT-Authentication** (Common Transport Authentication protocol) du standard FC-SP pour authentifier les échanges d'administration (toujours vrai pour les cartes HBA)
    - **Filtrage** restreignant l'accès aux seuls serveurs d'administration
    - Restreindre les protocoles aux seuls **protocoles sécurisés** (SNMPv3 avec authentification + chiffrement, HTTPS, SSH)
  - Dans le cas de l'utilisation de **Symcli** sur les baies EMC, contrôler les accès via les commandes **Symacl** pour limiter les hosts autorisés à modifier la base de données de configuration de la baie
  - Effectuer un **contrôle strict par rôle** (RBAC)
    - **Authentification nominative** auprès d'un référentiel d'authentification appliquant des restrictions sur les mots de passe
    - **Droits d'accès fins par profil**, aussi bien en termes de périmètres (équipements) qu'en termes de fonctionnalités
  - **Tracer** tous les événements d'administration

Que faire ?
Protéger les services internes et l'infrastructure SAN

- **Interdire** l'inscription de **WWN en doublon** dans le serveur de noms
  - Il n'est pas habituel qu'un serveur soit déplacé
- **Utiliser les VSANs** pour isoler les SANs
  - Chaque VSAN dispose de ses propres services et la portée d'une attaque est ainsi limitée
  - Le routage inter VSAN est possible mais est à configurer et se base également sur des Zones
- **Utiliser le Zoning** pour limiter les effets des RSCN, qui ne toucheront que les éléments de la zone
  - Single-Initiator Zoning ! Une zone par couple port serveur/port baie pour assurer une isolation maximale
  - La Default-zone doit interdire les communications
- **Fixer** au besoin **le timer** entre l'envoi de RSCN aux nœuds de la zone (par défaut 2s sur Cisco)
  - Les switches sont capables d'agréger plusieurs RSCN et de limiter les envois
- **Mettre en œuvre de la QoS** pour protéger les flux critiques des autres flux
  - *ex : flux SAN liés aux activités transactionnelles et flux liés aux sauvegardes*



Que faire ?
Contrôler le raccordement au SAN

- **Fixer le mode des ports** en N port et empêcher la négociation d'un E_port
  - Permet de bloquer les attaques de type E_Port replication
- Activer **Fabric Binding** pour contrôler les switchs autorisés dans la Fabric
  - Protection de base en dehors de mécanismes d'authentification
- Activer le **port security (ou « port binding »)** pour verrouiller un WWN sur un port (serveur, baie, switch…)
  - Permet de lutter contre le spoofing de WWN
- Implémenter **l'authentification mutuelle** des appareils (baie de stockage, switchs, serveurs) en utilisant CHAP. Privilégier **DH-CHAP** du standard FC-SP (T11) pour l'authentification mutuelle
  - Permet de bloquer la connexion des machines non autorisées

Que faire ?
Contrôler l'accès aux LUNs

- Le mécanisme le plus courant est le **LUN Masking**
  - Soit implémenté **sur le client**
    - La sécurité reposant sur le serveur client… **aucune protection en cas de compromission du serveur !**
  - Soit implémenté **sur la baie de stockage**
    - Cas le plus courant : la sécurité est confiée à l'équipe en charge des LUNs elles-mêmes
- Il est également possible d'effectuer du **LUN Zoning**, donc d'effectuer un filtrage des LUNs par les switches
  - Rarement effectué pour des difficultés d'exploitation, la gestion des LUNs étant effectuée par les administrateurs des baies et non du SAN
- **Attention** : pour rappel certaines baies exposent un **LUN de configuration**
  - Cet accès permet aux serveurs des manipulations sur les LUNs et est donc absolument à sécuriser

Que faire ?
Assurer la confidentialité des données

- Le **chiffrement** des flux **en transit** (« in-flight ») permet de les protéger pendant leur transport
  - Utilisation d'un VPN IPSec lors du transport sur IP (FCIP notamment)
  - FC-SP prévoit le chiffrement par les ports FC depuis 2007…
  - … mais quasiment aucune implémentation… hormis entre switches (Cisco TrustSec) et donc à la **couverture limitée**
- Le **chiffrement** des données **sur les disques**
  - Protection ultime, y compris contre un accès physique aux baies
  - Peut être pris en charge par
    - L'OS du serveur
    - La HBA (ex : Emulex Secure)
    - Le disque (SED pour Self Encrypting Disk)
    - La baie

Protègent aussi pendant le transport

} Sujets à backdoors...

- Le **chiffrement** des données **par l'application**
  - **Seule solution assurant la protection de bout en bout**

Que faire ?
Surveiller les événements

- Contrôler le réseau : mettre en place un mécanisme de **surveillance du SAN**
  - **Journaliser les évènements** se déroulant sur la Fabric (modification d'entrée dans le Name Server, demande de montage/démontage de LUN…)
  - **Collecter** les journaux et les **analyser**
  - Utiliser des **règles d'analyse automatique** pour détecter, par exemple :
    - **Duplication de WWN**
    - **Bruteforce** WWN / FCID / LUN / sur les différents équipements de la Fabric
    - Activation des fonctions de **SPAN** sur un switch FC

Agenda

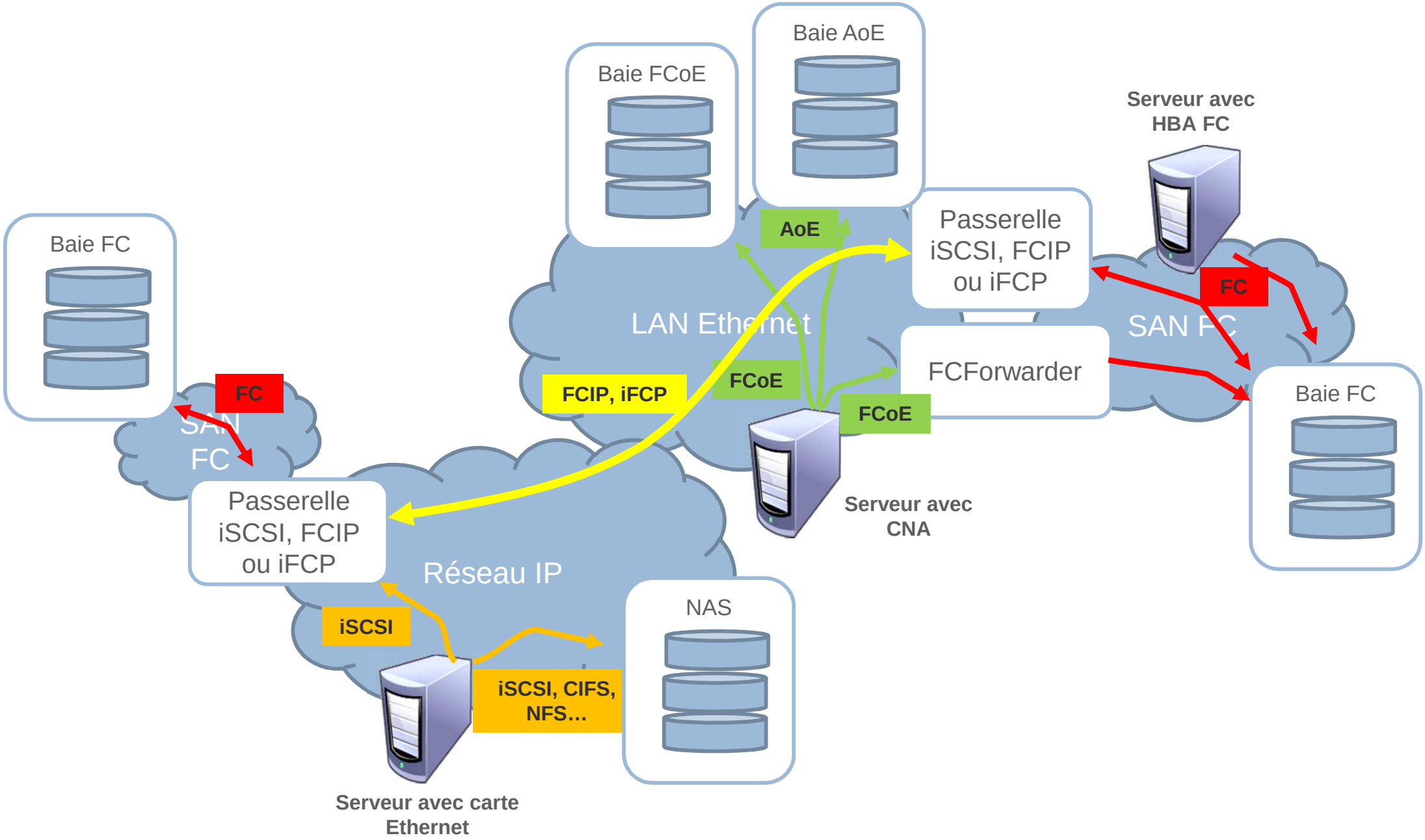
1. Un SAN c'est quoi ?
2. Quelles menaces ?
3. Que peut et doit on faire ?
4. Quel impact de la convergence LAN/SAN ?
5. Quid des NAS ?
6. Liens utiles

Quel impact de la convergence LAN/SAN ?

- La convergence LAN/SAN peut prendre de nombreuses formes :
  - Transporter les flux de stockage sur Ethernet ⇨ FCoE (voire AoE*…)
  - Transporter les flux de stockage sur IP ⇨ iSCSI
  - Basculer vers un NAS
    - En basculant en mode fichiers ⇨ NFS, SMB, …
- Ces technologies profitent des mécanismes de sécurité des LAN : Vlans, ACLs, 802.1x, ARP Inspection, IP Source Guard…
- FCoE intègre des mécanismes de protection (ACLs MAC dynamiques)
- AoE quant à lui est orienté simplicité et performances… pas sécurité

*ATA over Ethernet

Positionnement des protocoles



Quel impact de la convergence LAN/SAN ?
Focus sur FCoE

- **FCoE transporte FC dans Ethernet** mais avec de nombreux pré-requis
  - Utilisation de cartes **CNA** (Converged Network Adapter) 10G Ethernet
  - Support minimal des **baby jumbo frames** par les switches ethernet (2K)
  - Support de **DCBX** par les switches ethernet de raccordement

- En **FC natif**, les nœuds FC et commutateurs sont connectés par des **liens point à point** FC

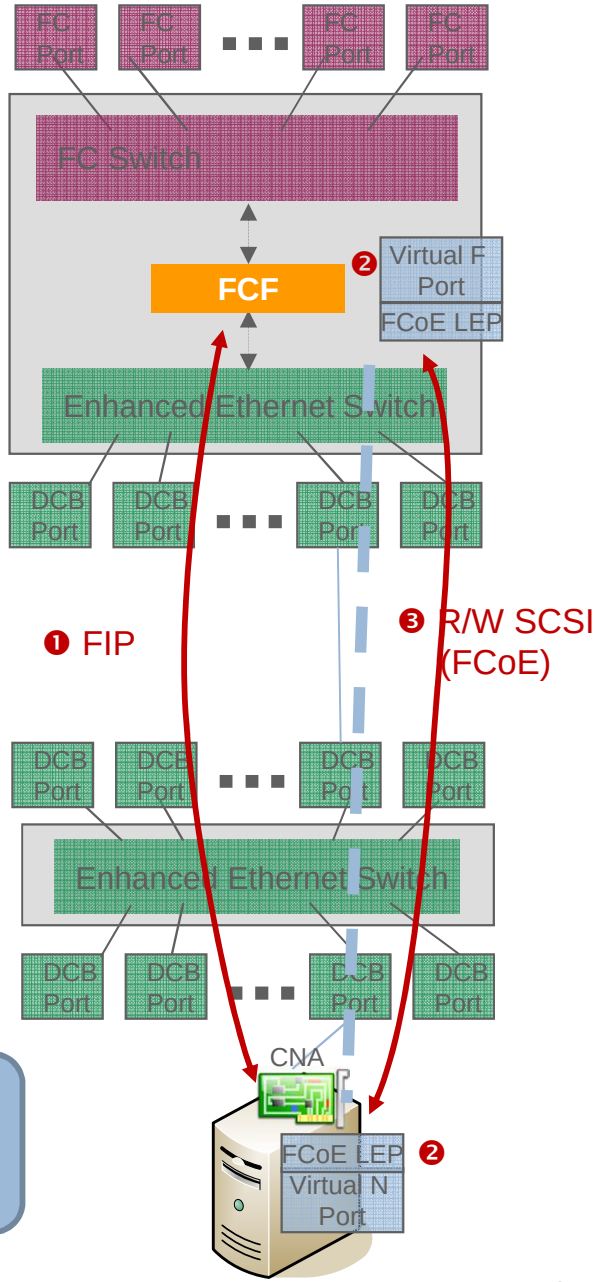
- En **FCoE**, les "Enodes" et les "FCF" (FC Forwarders) sont connectés par des **liens virtuels** au dessus d'un nuage Ethernet sans perte…

↳ …Il existe donc **des opportunités d'attaques à travers le nuage Ethernet** qui sont moins probables sur des liens point à point

- **La norme prévoit** un certain nombre de **mécanismes** pour **réduire ou supprimer ces opportunités d'attaques** supplémentaires liées au transport sur un nuage Ethernet

Quel impact de la convergence LAN/SAN ? Focus sur FCoE

- FCoE permet à des nœuds FC natifs de communiquer de manière transparente avec des nœuds raccordés à un réseau Ethernet
- L'élément qui fait office de **passerelle** entre les deux mondes est un « **Fibre Channel Forwarder** » (FCF)
- Sur Ethernet, la découverte et l'initialisation entre les nœuds et le FCF s'effectue via Fibre Channel Initialization Protocol (FIP)
  - Découverte du FCF
  - Fabric Login (FLOGI)
  - Attribution du FC-ID et relation @Mac – FC-ID
  - Établissement du lien FC virtuel au dessus du nuage Ethernet
- Le transport des trames FC utilise ensuite FCoE



Challenge : appliquer une isolation sur le lien virtuel proche de celle d'un lien physique en utilisant un média partagé

Quel impact de la convergence LAN/SAN ?
Focus sur FCoE

- FC-BB-5 prévoit un certain nombre de contrôles dans l'annexe D
  - D.3 Recommandation générique
    - Aucun vlan ne devrait transporter le flux de plus d'une Virtual Fabric
  - D.4 Recommandations de switching

    1. Tous les ports non connectés à un FCF devraient implémenter un filtrage MAC :
       - Filtrer toutes les trames FCoE et FIP si aucun traffic FCoE n'est attendu sur un port
       - Filtrer toutes les trames FIP qui ne sont pas à destination d'un FCF
       - Filtrer toutes les trames FCoE dont l'adresse MAC n'est pas un FCF ou bien n'a pas été attribuée à un Enode
    2. Sur un port entre switches :
       - Si le port doit recevoir des trames de la part d'Enodes : Filtrer les trames FIP ou FCoE non à destination de FCF ainsi que les trames entre FCFs
       - Si le port doit recevoir des trames de la part de FCFs : Filtrer toutes les trames FCoE et FIP n'émanant pas de FCF
    3. Un switch ne doit pas apprendre une adresse MAC qui aurait été filtrée par la recommandation 1 ou 2
    4. L'apprentissage des @MAC d'un vlan transportant le flux d'une Fabric doit être séparé de l'apprentissages des vlans transportant les flux d'autres Fabric
    5. Les ports devant filtrer en entrée les flux FCoE et FIP devraient se baser sur l'Ethertype
    6. Les switchs transportant du FCoE et du FIP ne devraient pas supprimer des trames sur congestion
  - D.5 Recommandations de filtrage sur les nœuds et FCFs
- Mais... ce ne sont que des recommandations...

Quel impact de la convergence LAN/SAN ?
Focus sur FCoE

- Les recommandations prévoient la mise en œuvre d'ACLs… dont la définition est heureusement effectuée dynamiquement…
  - Naturellement par les équipements comportant un FCF
  - En interprétant les échanges FIP les traversant (« FIP snooping ») pour les autres… mais avec des limites du fait des possibilités de chemins multiples
    - Seuls les switches « edge » peuvent réellement implémenter du filtrage
    - Les filtres ne peuvent concerner que les équipements directement attachés
- … sauf sur les switches non « FCoE aware » ou n'intégrant pas le FIP snooping

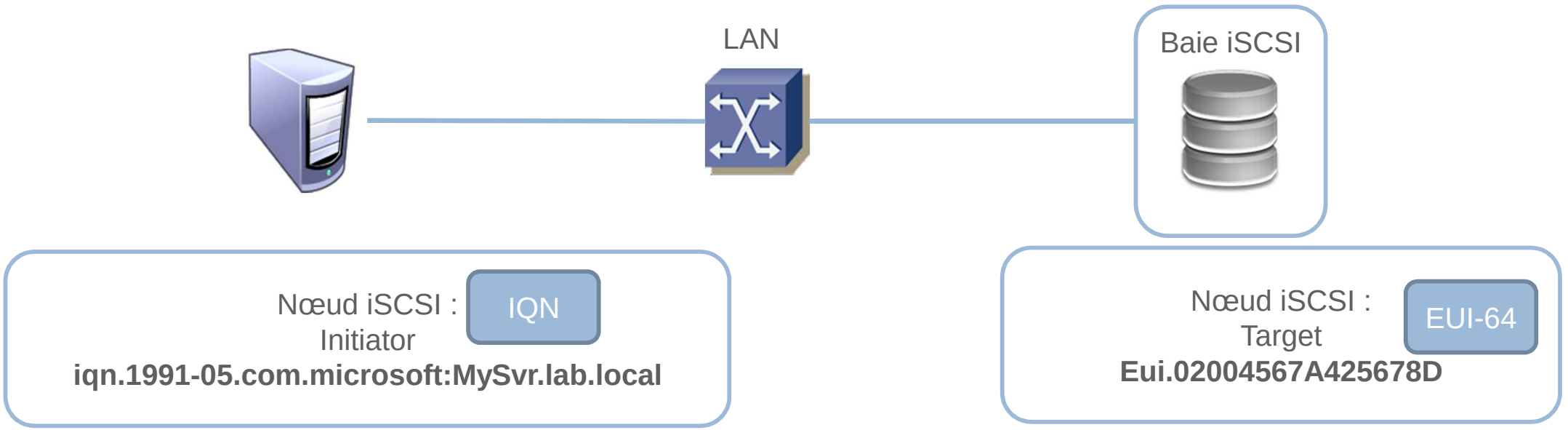
Il est important de s'assurer de ne pas insérer de brèche dans la sécurité que peuvent apporter les équipements en limitant ces flux aux seules zones identifiées et en recourant à des équipements capables d'intégrer automatiquement des filtrages

Quel impact de la convergence LAN/SAN ?
Focus sur iSCSI

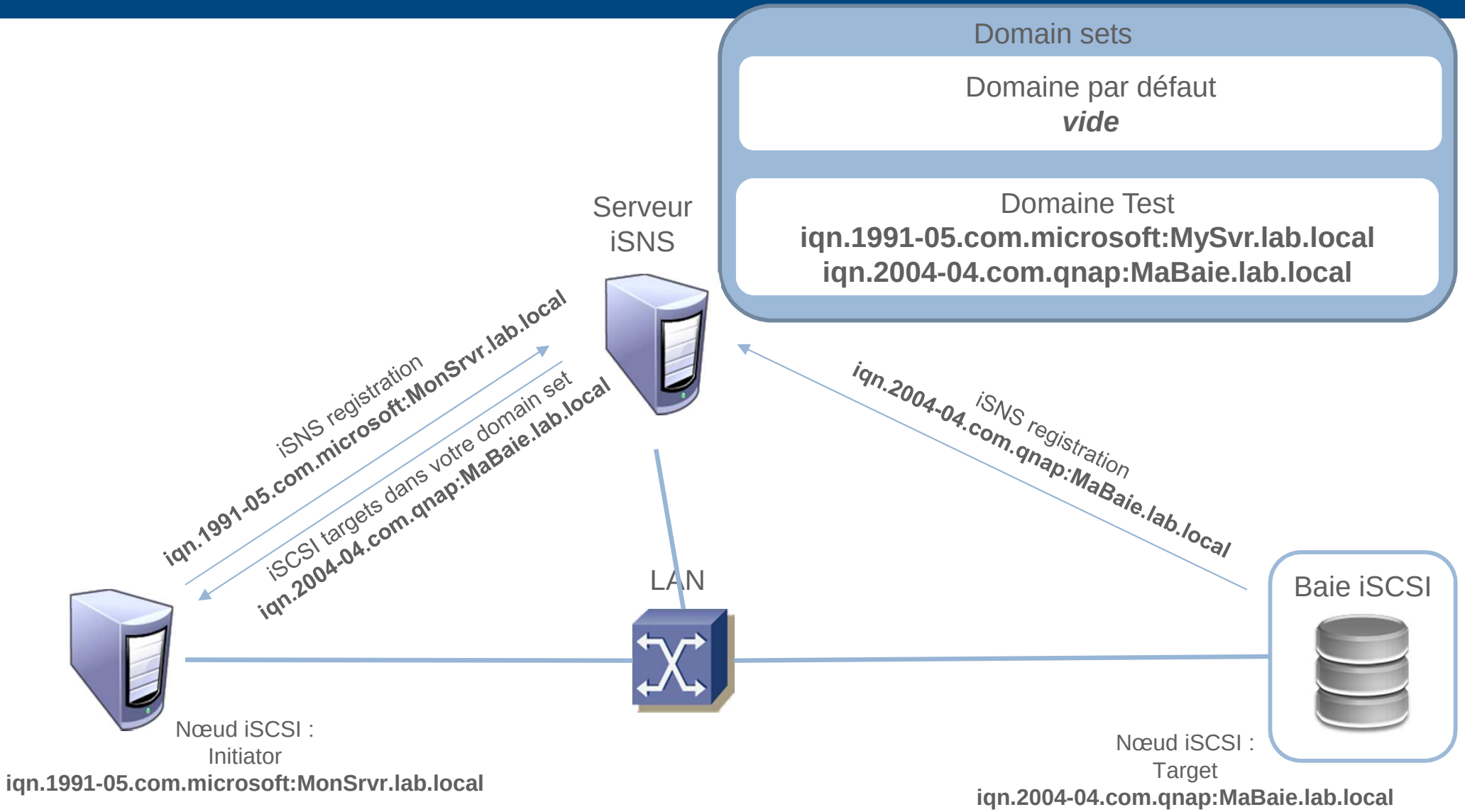
- iSCSI transporte les trames SCSI dans **TCP** (port 3260)
- iSCSI n'impose **pas de prérequis sur le réseau de transport** et peut être utilisé sur le WAN ou bien des débits faibles
  - TCP prend en charge la fragmentation et la réémission en cas de perte
- iSCSI peut s'appuyer sur un serveur **iSNS** (Internet Storage Name Service) pour la découverte des Targets disponibles
  - Chaque Target ou Initiator s'enregistre auprès du serveur iSNS
  - iSNS inclue des « Discovery Domains », comparables à du Soft Zoning dans le monde FC
  - iSNS est également utilisé par iFCP

Quel impact de la convergence LAN/SAN ?
Focus sur iSCSI

- iSCSI utilise des **WWUI** (World Wide Unique Identifier) pour désigner une entité unique : la couche iSCSI d'un nœud
  - Utilisé uniquement au login ou pendant la découverte
- iSCSI utilise également des adresses, comprenant le WWUI : l'IQN (iSCSI Qualified Name), ou bien au format EUI-64



Quel impact de la convergence LAN/SAN ?
Focus sur iSCSI



Quel impact de la convergence LAN/SAN ?
Focus sur iSCSI

- iSCSI intègre nativement des mécanismes de sécurité :
  - iSCSI supporte **plusieurs méthodes d'authentification** : Kerberos v5, SPKM1, SPKM2, SRP et CHAP
  - iSCSI permet un **contrôle d'accès** au niveau LUN

- iSCSI n'intègre **pas de chiffrement natif** mais peut s'appuyer sur une connexion **IPsec** mise en œuvre au niveau de l'OS du serveur. Le support côté baie dépendra du constructeur.

Agenda

1. Un SAN c'est quoi ?
2. Quelles menaces ?
3. Que peut et doit on faire ?
4. Quel impact de la convergence LAN/SAN ?
5. Quid des NAS ?
6. Liens utiles

Quid des NAS ?

- Un NAS n'est ni plus ni moins qu'un serveur de fichiers
- Les protocoles supportés embarquent leurs propres fonctionnalités d'authentification et de contrôle d'accès…
  - SMB supporte les différentes méthodes d'authentification disponibles dans le monde Microsoft et effectue un contrôle d'accès au niveau partage ainsi qu'au niveau fichiers
  - NFS supporte différentes méthodes d'authentification (kerberos avec NFSv4) ainsi qu'un contrôle d'accès au niveau partage et fichiers
- … ainsi que le chiffrement
  - SMBv3 (Windows server 2012 et Windows 8) supporte le chiffrement des flux AES-CCM
  - NFSv4 supporte le chiffrement des flux en transit en s'appuyant sur Kerberos v5

Les NAS apportent les risques du monde IP aux flux de stockage. Il est donc nécessaire d'appliquer les moyens de protection classiques du monde IP à ces flux.

Agenda

1. Un SAN c'est quoi ?
2. Quelles menaces ?
3. Que peut et doit on faire ?
4. Quel impact de la convergence LAN/SAN ?
5. Quid des NAS ?
6. Liens utiles

Liens utiles

- SNIA (Storage Networking Industry Association)
  - Sécurité du stockage : http://www.snia.org/forums/ssif
- Documents constructeurs
  - ftp://ftp-eng.cisco.com/ltd/mds_security_whitepaper16.pdf
  - http://www.brocade.com/downloads/documents/white_papers/Zoning_Best_Practices_WP-00.pdf
  - http://china.emc.com/collateral/hardware/technical-documentation/h8082-building-secure-sans-tb.pdf
- INCITS Technical Committees
  - SCSI et SAS : T10 (www.t10.org)
  - Fibre Channel : T11 (www.t11.org)
  - ATA et SATA : T13 (www.t13.org)
- IETF (Internet Engineering Task Force)
  - www.ietf.org

Voir aussi les numéros 75 et 76 de MISC, reprenant cette présentation de manière plus détaillée

The power of simplicity
«Ce qui est simple est fort»

www.solucom.fr

Contact

Pierre-Charles WAGREZ

Architecte Référent Réseaux & Télécoms

Tel : +33 (0)1 49 03 27 29

Mobile : +33 (0)6 23 15 31 96

Mail : pierre-charles.wagrez@solucom.fr