Projet de sécurité des systèmes d'information

Groupe défense

Benjamin Aguila
Cindy Candiago
Ibrahim Manroufou
Nordine Medjadj
Marc Moisand
Romain Montoya
Christophe Ortiz
Laurent Perarnaud
Yannick Poirier
Julien Puntus
Pierre Quentel
Peno Heriniaina Rajaonarison
Enrique Renard
Nicolas Robert
Lionel Rouvellat
Charlie Salvan
Willy Woung

Plan de présentation

STRI
| Télécoms & Réseaux |

I - Présentation du projet sécurité
II - Organisation de l'équipe
III - Coordination de l'équipe
IV - Architectures mises en places
V - Services mis en places
VI - Bilan des confrontations
VII- Bilan du projet

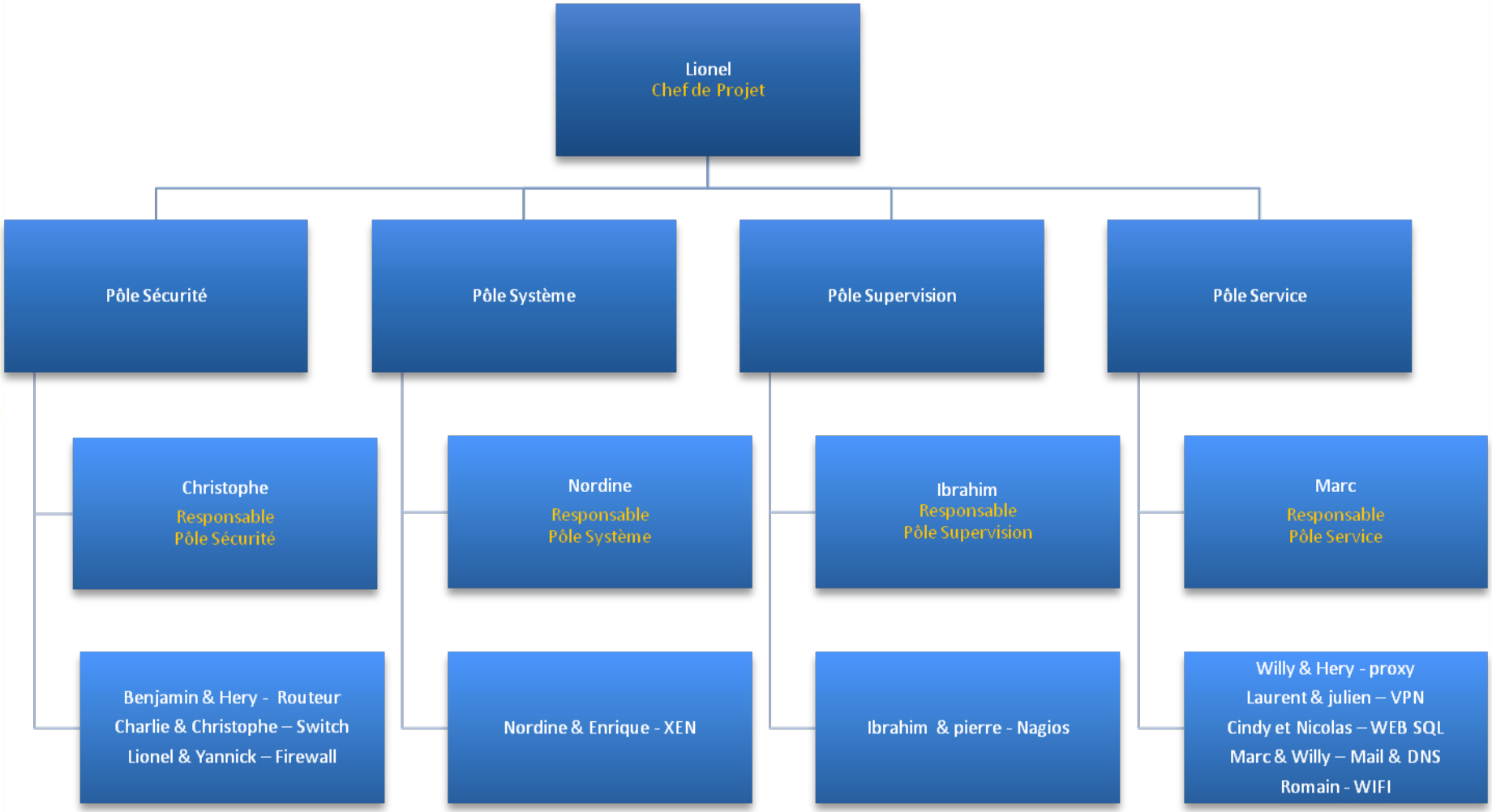
Organisation de l'équipe

STRI
| Télécoms & Réseaux |

- Création de différents pôles de compétences
  - Pôle sécurité
  - Pôle système
  - Pôle supervision
  - Pôle service

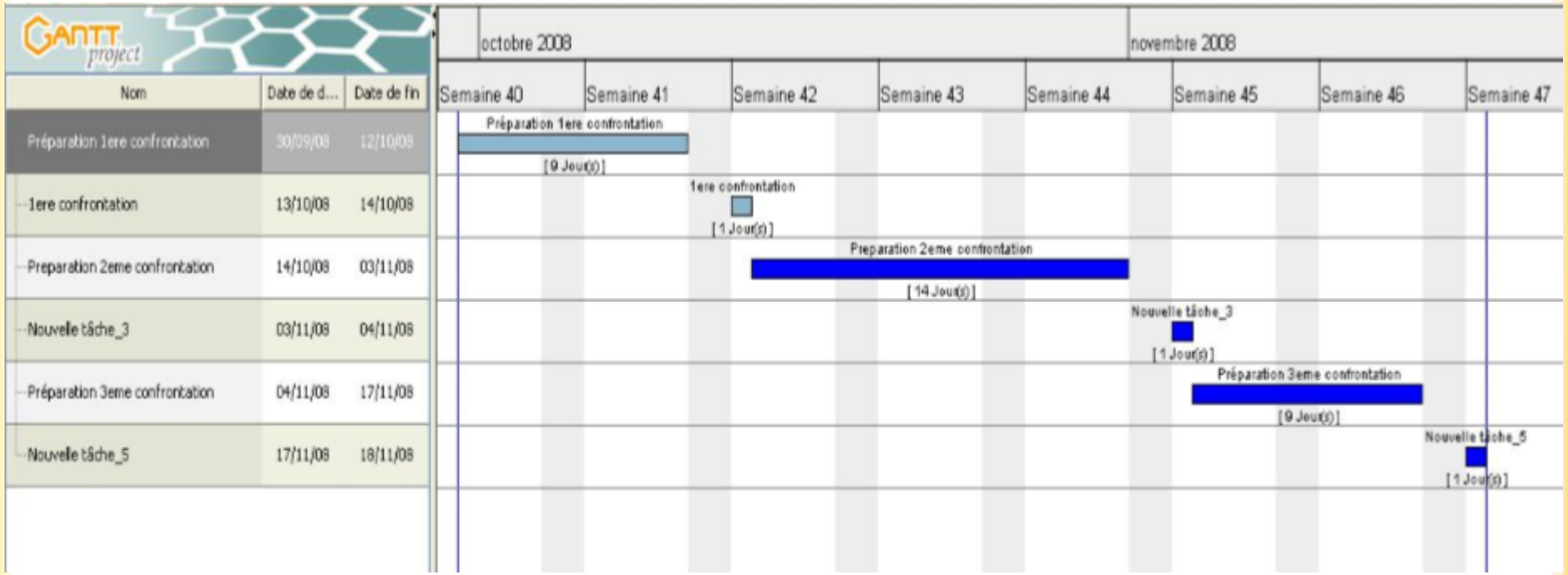
Organisation de l'équipe

STRI
| Télécoms & Réseaux |



Gestion de projet

- Planification des différentes tâches / confrontations



Gestion de projet: outils de coordination

STRI | Télécoms & Réseaux |

- Mailing List m2-stri.defense@iut-tlse3.fr
  - volontairement ignorée au début : changement de groupe.
  - utilisée en fin de projet.

- Compte Gmail
  - Avantages
    - Inconnu des attaquants
    - Nous laissais le temps de nous organiser
    - pratique pour centraliser 18 Personnes
    - politique de sécurité

Gmail by Google BETA

Gestion de projet: outils de coordination

STRI
| Télécoms & Réseaux |

- Réunions
  - Outils principal: Qualité / Rapidité / Présence
  - Nombreuses:
    - Formelles / informelles
    - Par pôles / groupe entier
    - Minimum 1 par semaines

Gestion de projet

STRI
| Télécoms & Réseaux |

- Google docs
  - Outils principal de centralisation de données
  - Avantages:
    - Rédaction communes
    - Disponibilité
    - Stockage:
      - PDF, fichier d'aides
      - procédures
      - rapport d'activité
  - Inconvénient :
    - Gestion des partages à 18 personnes
    - version beta

Google Documents BETA

Gestion de projet

STRI
| Télécoms & Réseaux |

Interaction avec les analyste

- signature et contrat
  - Clause de confidentialité
  - Politique de sécurité
- Négociation sur les équipement
  - Nature
  - Positionnement
  - Politique de sécurité
  - Accès
- Intégration des équipements : redirection de traffic.
- Création de vlan spécifique.

Politique de sécurité

- Charte Informatique
  - Stipule les droits et obligations des utilisateurs
- Plan de reprise d'activité
  - Définit les tâches à accomplir lors d'un incident
- Audit de sécurité
- Sécurité du réseau
  - Droits des utilisateurs sur leurs postes
  - Choix des mots de passes
  - Les services authorisés
- Gestion de la sécurité
  - Mises à jour
  - Éléments à surveiller (logs, problèmes matériels, etc ...)

Politique de sécurité

Sécurisation des machines

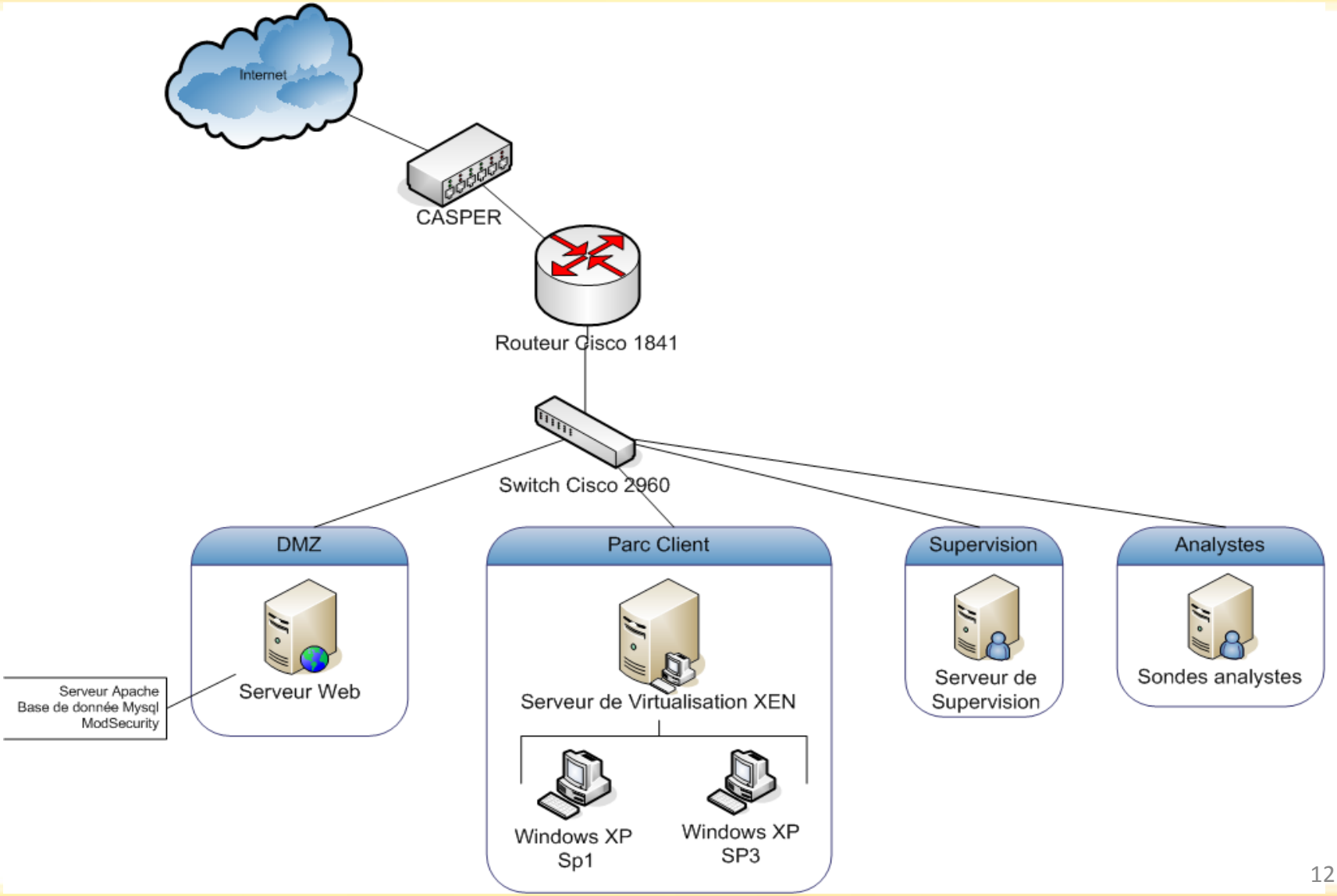
- Sécurisation du boot :
  - Mot de passe au démarrage des machines
  - Empêcher le démarrage depuis Disquette, Cdrom, Usb

/	10 Go
/home	10 Go
/var	10 Go
/var/log	5 Go
/tmp	5 Go
/usr	10 Go
swap	1 Go

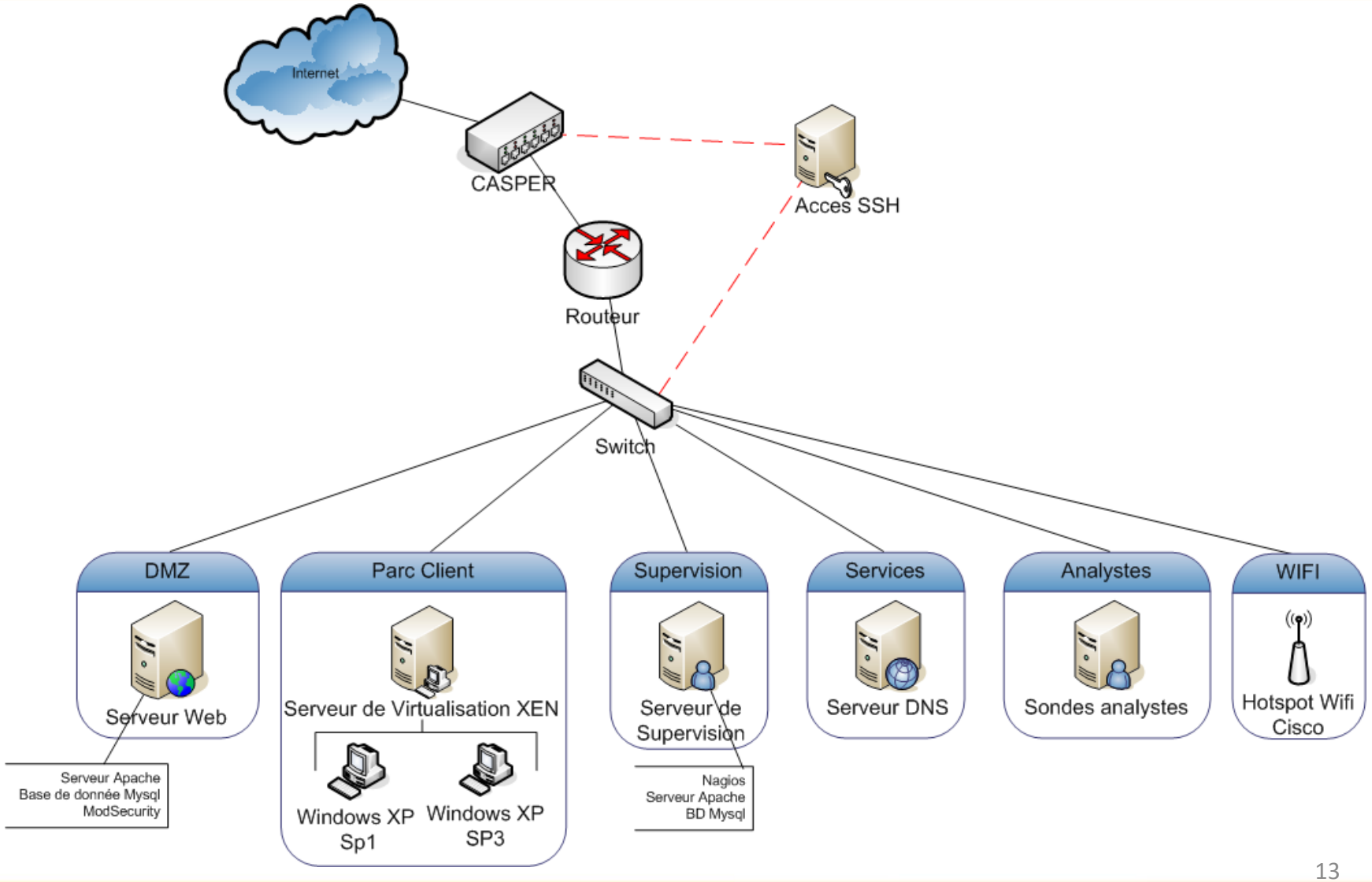
- Système d'exploitation
  - OS choisi : Debian Etch
  - Partitionnement du disque : système de fichier Reiserfs

- Sécurisation du système
  - Déconnection automatique des utilisateurs
  - Suppression des services inutiles (Telnet, Portmap, dhcp, ...)
  - Accès SSH : Pas d'accès root, modification du Welcome Message

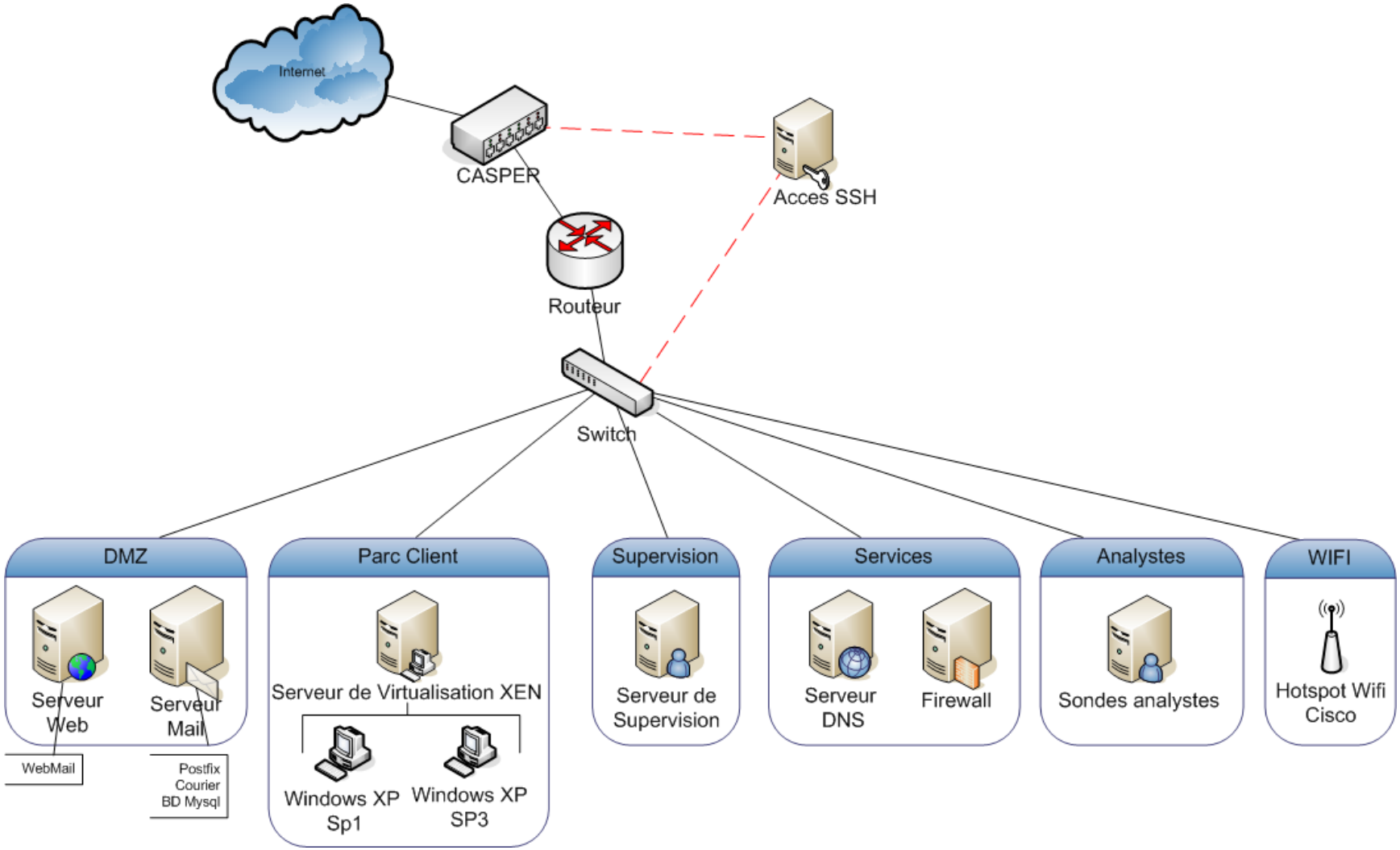
Architecture réseau: 1ere confrontation



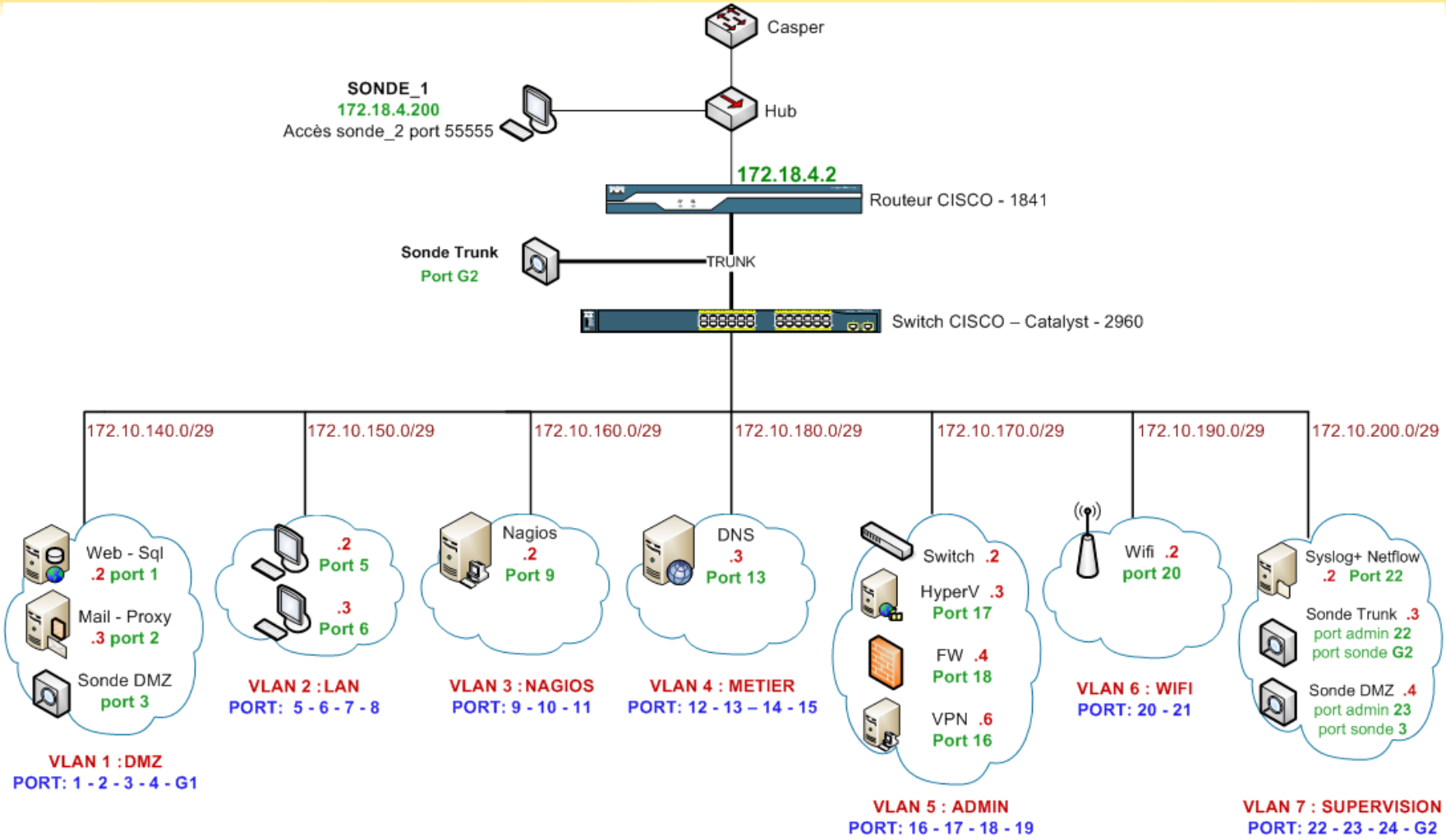
Architecture réseau: 2eme confrontation



Architecture réseau: 3eme confrontation



Architecture réseau: Vlan & IP



Passerelle – Gateway : **.1** de chaque réseau
ex : gateway DMZ = **172.10.140.1**

Routeur - 1ere confrontation

STRI | Télécoms & Réseaux |

- Configuration:
  - Accès sécurisé SSH v2
  - Création des VLAN et du mode Trunk
  - NAT dynamique afin de sécuriser les adresses internes
  - Accès distants aux machines Analyse
  - Envoi de donnée à l'équipe Analyse Syslog
- Résultat:
  - Déconnexion manuelle du routeur pendant 5 minutes (NAT FLOODING)

Switch - 1eme confrontation

STRI
| Télécoms & Réseaux |

- choix des vlan par port
  - sécurité / simplicité
  - durée de vie sur 3 confrontations
  - par ip et mac : pb nouvelles machines – risque d'usurpation
- Liaison routeur
  - en Trunk pour la visibilité de tout les Vlan par le routeur
- Intégration Analystes
  - Redirection du traffic vers sonde analyste:
  - Mirroring de port : mode SPAN

Routeur - 2eme confrontation

STRI | Télécoms & Réseaux |

- Configuration:
  - Création des ACL sur l'interface externe
  - Création NAT IP interne.
  - Envoi des données à l'équipe Analyse
  - Paramétrage du Control Plane.
  - Limitation du nombre d'entrées NAT
- Résultat:
  - Scan des ports internes (Erreur ACL).

Switch – 2eme confrontation

- Sécurité
  - éviter le vlan Hopping sur le trunk
    cause: wifi ouvert & attaque de l'intérieur.
    - Suppression du Dynamic Trunking Protocol ou DTP
  - Eviter attaques par dénis de service
    - risque: récupération du traffic par l'attaquant
    - activer BPDU guard, BPDU Filtering et ROOT guard
- Intégration Analystes
  - nouvelle sonde: dans DMZ
  - Mirroring du vlan DMZ vers le port de cette sonde

Routeur - 3eme confrontation

STRI
| Télécoms & Réseaux |

- Configuration:
  - @MAC du DNS insérée en statique.
  - Création des ACL sur les VLAN.
  - Autorisation de lecture sur le serveur SNMP.
  - Mise de place de l'IPInspect.

Serveur Web – 1ere confrontation

STRI | Télécoms & Réseaux |

- Architecture mise en place
  - Apache 2.2 - PHP 5 - MySQL 5 - phpMyAdmin
- Sécurisation
  - Mot de passe BIOS
  - Interdiction BOOT sur CD
  - Ghost serveur WEB
  - Suppression des services et paquets inutiles
  - Changement régulier des mots de passe
  - Suppression du compte « root » sur MySQL
  - Création du compte « admincandide » pour administrer la BD
  - Installation de « ModSecurity » par les sources

Serveur Web – 1ere confrontation

STRI | Télécoms & Réseaux |

- Difficultés rencontrées
  - Installation de « ModSecurity » par les sources
    - Dépendances avec d'autres paquets
- Bilan
  - Aucun dénis de service

Serveur Web – 2eme confrontation

STRI
| Télécoms & Réseaux |

- Evolutions
  - Mise en place du SSL avec redirection automatique du HTTP sur HTTPS
  - Installation de MySQLTuner
  - Restriction sur les demandes de connections d'Apache et MySQL à 300
  - Mise en place des règles pour ModSecurity
  - Ajout des sources du nouveau site interne
  - Changement propriétaire du répertoire « /var/www/candide » en « www-data.www-data »
  - Changements des droits sur le répertoire « /var/www/candide »
    - « 755 » sur les répertoires
    - « 644 » sur les fichiers
  - Demande du groupe Analyse : Redirection des logs d'Apache

Serveur Web – 2eme confrontation

STRI
| Télécoms & Réseaux |

- Difficultés rencontrées
  - Trouver et mettre en places les règles de sécurités pour ModSecurity
  - Difficultés à créer les certificats avec Apache 2 pour SSL
    - Solution : Recherche d'informations dans la documentation d'Apache

- Bilan
  - Attaquants ont atteint le seuil maximum des demandes de connections par heure à la BD
    - Réaction immédiate : mise à jour du seuil en illimité
  - A la demande du groupe Attaque ajout de code dans une page du site WEB
    - Code erroné : disfonctionnement du serveur WEB
    - Solution : suppression du code

Serveur Web – 3eme confrontation

STRI | Télécoms & Réseaux |

- Evolutions envisagées
  - Eclatement du serveur WEB
    - Présentation : Apache en mode Proxy avec Squid + « ModSecurity »
    - Middleware : Apache + PHP
    - Données : MySQL
  - Manque de machine éclatement du serveur WEB
    - Présentation : Apache en mode Proxy avec Squid + « ModSecurity »
    - Middleware : Apache + PHP + MySQL

Serveur Web – 3eme confrontation

STRI | Télécoms & Réseaux |

- Problème dans la mise en place de Squid
  - Impossible d'éclater le serveur WEB
  - Présentation : Apache + « ModSecurity » + PHP + MySQL
- Evolutions
  - Ajout de règles supplémentaires pour « ModSecurity »
- Bilan
  - Injection SQL bloquée par les règles mises en place avec « ModSecurity »
  - Aucune attaque majeure
  - Pas de dénis de service

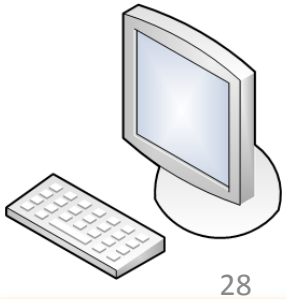
La virtualisation : XEN

STRI
| Télécoms & Réseaux |

- Hôte : Linux Gentoo
  - Optimisation
  - Légèreté du Système
- VM :
  - 2 PC Windows
  - Hôte (Gentoo)
- Avantage :
  - Transparence
  - Légèreté
- Inconvénient :
  - Accès TSE
  - Implémentation manuelle

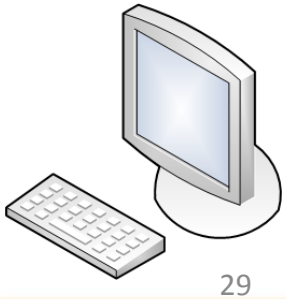
Xen™

- Sécurisation
  - Mot de passe BIOS
  - Copie des fichiers des machines virtuelles
  - Cloner le disque dur
  - Création d'un compte utilisateur et administrateur
  - Désactivation du compte invité
  - Politique de sécurité sur les mots de passes



Parc Client: 1ere confrontation

- Configuration des machines
  - Pc non protégé (SP1)
    - Windows XP SP2
    - Aucun pare-feu
    - Aucun antivirus
  - Pc protégé (SP3)
    - Windows XP SP3
    - Pare-feu XP
    - AVG antivirus



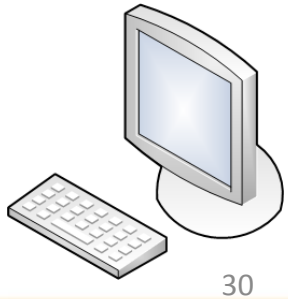
STRI | Télécoms & Réseaux |

Bilan

Consigne : accéder à différents liens internet et lancement d'un point bat

- Aucune attaque détectée
- Aucune dégradation

site web : http://stri-attaque.ifrance.com



Evolutions

- PC client SP1 :
  - Installation de Windows XP service pack1
  - Installation du Framework 1.1
  - Changement des mots de passes administrateurs et utilisateurs
  - Installation du logiciel SNARE et NAGIOS pour la supervision des logs
  - Configuration IP : changement de l'adresse DNS

Evolutions

- PC client SP3 :
  - Installation du Framework 3.5
  - Changement des mots de passes administrateurs et utilisateurs
  - Mise à jour de l'antivirus
  - Analyse antivirus
  - Installation du logiciel SNARE et NAGIOS pour la supervision des logs
  - Configuration IP : changement de l'adresse DNS

Bilan

Consigne : accéder à différents liens internet et lancement d'un point bat

- SP1 et SP3 : aucune dégradation dans un premier temps
- Prise en main du SP1 lors de l'accès à leur site web dans un deuxième temps
- Exploitation d'une faille de sécurité du SP1

site web : http://stri-attaque.ifrance.com

Evolutions

- PC CLIENT SP1 et SP3 :
  - Configuration IP : changement de l'adresse de passerelle (firewall)
  - Remise à neuf des machines
  - Changement des mots de passes administrateurs et utilisateurs
  - Installation du viewer Excel

Bilan

Consigne : accéder à différents liens internet et lancement d'un point bat

- Prise en main du SP1 lors de l'accès à leur site web
- Exploiter une faille de sécurité du SP1
- Attaques de fichiers Excel non testés à cause du viewer
- Connexion ssh échoué dû à la politique de sécurité
- SP3 : aucune attaque observée

site web : http://stri-attaque.ifrance.com

Services mis en place:

Serveurs métiers :

Rôle : Implémenter les Services des Usagers dans l'entreprise.

3 Services Principaux :

- Acces Web : DNS
- Distribution de Courrier : Mail / WebMail
- Protection (Firewall)

Le DNS

STRI
| Télécoms & Réseaux |

- Résolution d'adresse pour les sous-réseaux locaux
- Implémentation : Bind 9 sous Linux Debian 4.0
- Sources :
  - Racines DNS
  - DNS www.stri
- Sécurisation :
  - Résolution DNS locale uniquement
  - Accès DNS et HTTP Sortant
  - Accès DNS Entrant

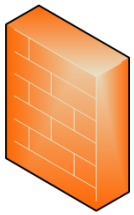
Mail / Webmail

- Accès Double :
  - IMAP
  - Webmail
- Implémentation : POSTFIX/Courier + Apache (WebMail)
- Difficulté rencontrées :
  - Communication entre Server Web (WebMail) et Serveur Mail (Postfix +DB)
  - Utilisateurs Virtuels POSTFIX
- Fonctionnalités envisagées :
  - Anti-Spam
  - Anti-Virus

Le Firewall

Les restrictions suivantes ont été implémentés afin de sécuriser les postes utilisateurs :

- Accès Internet Http https
- Accès server IMAP Métier
- Connexion TSE aux Postes de Travail Virtualisés
- Passerelle pour le Parc Informatique Entreprise et les outils de supervision (Filtrage du traffix)
- IPtables Statefull & Stateless



Supervision Nagios

STRI | Télécoms & Réseaux |

- Objectifs
  - Etre informé sur l'état des machines et des services sur l'ensemble du parc
  - Observer pour comprendre les origines des anomalies
- nagios n'est ni:
  - Un outil de détection d'intrusion
  - Un outil de prévention d'intrusion

Nagios®

Supervision Nagios

- Architecture

Supervision Nagios

STRI
| Télécoms & Réseaux |

- Plugins
  - nrpe pour les postes sous linux
  - NSClient ++ pour les postes sous windows
  - SNMP pour le routeur
- Utilisation de centreon:
  - Gestion de la configuration

Nagios®

Supervision Nagios

STRI | Télécoms & Réseaux |

- Bilan première confrontation
  - Service ping sur les serveurs et les postes du parc
- Difficultés:
  - L'installation nécessite beaucoup de composants
  - Changement de technologie : SNMP → NRPE
  - Configuration du plugin sur les postes Windows à superviser

Nagios®

Supervision Nagios

STRI
| Télécoms & Réseaux |

- Bilan deuxième confrontation
  - D'autres services tels que charges CPU, charge mémoire, occupation de l'espace disque…
  - Intégration du module SSL d'apache

- Difficultés:
  - graphique des éléments observés
  - Poste windows sans mise à jour ne remonte pas les informations
  - Les informations du routeur ne sont pas remontées

Nagios®

Supervision Nagios

STRI
| Télécoms & Réseaux |

- Bilan troisième confrontation
  - Supervision du routeurs sur les services tels que charges CPU, charge mémoire, occupation de l'espace disque…
- Eléments prévu et non implémenté:
  - graphique des éléments observés
  - Remonter les alertes via le serveur email de la société

Nagios®

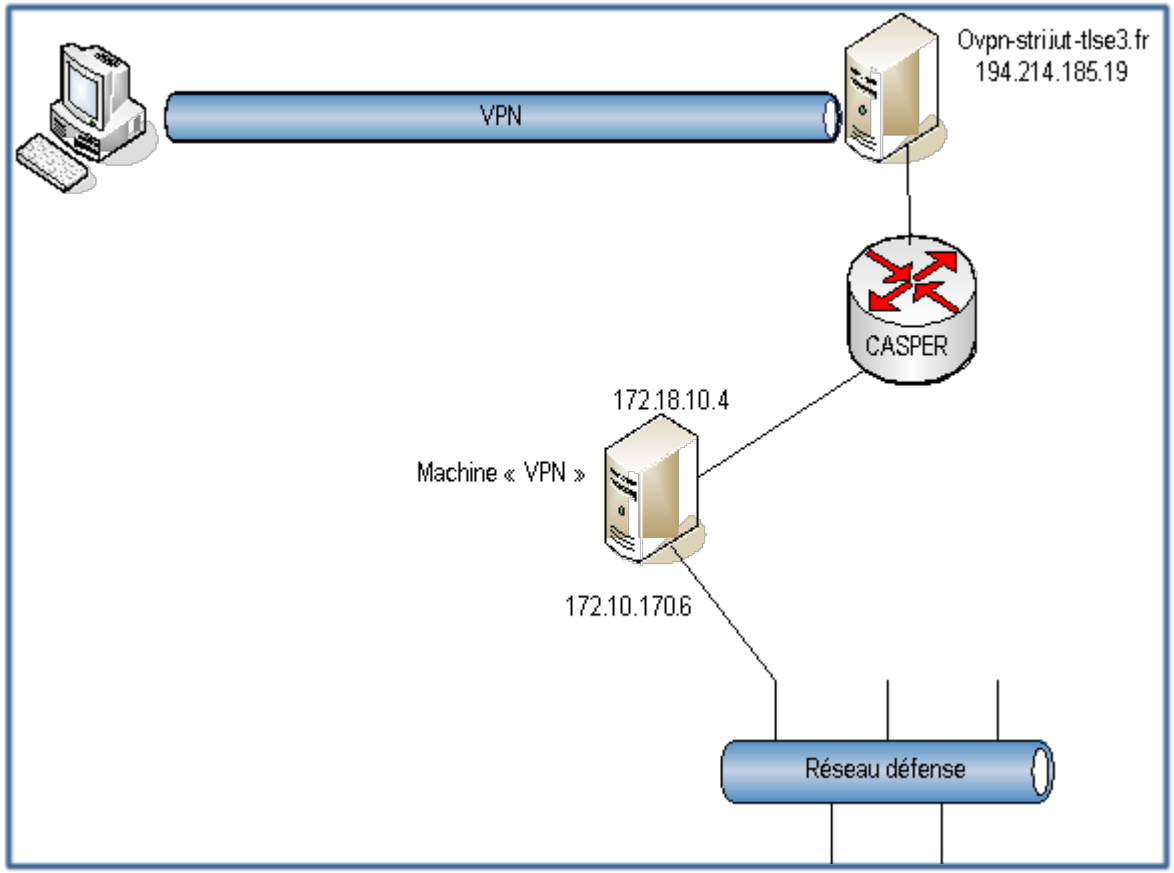
Supervision Nagios

STRI | Télécoms & Réseaux |

- Bilan
  - Observation des éléments du réseaux n'apporte pas des informations sur les origines (internes ou externes)
  - Nécessite de coupler ave un gestionnaire de logs et un outils de détection ou de prévention d'intrusion

Nagios®

Simulation Out Of Band

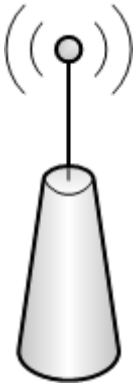


Liaison VPN

- Création Autorité et certificat
- Configuration serveur
- Configuration client
- Mise en place Iptables

HotSpot

- Pas de sécurisation bas niveau
  - Un Vlan Spécifique limité au Web
  - Adressage via DHCP
  - Pour les employés, connexion via vpn



Bilan des confrontation:
1ère confrontation

STRI | Télécoms & Réseaux |

Machine ou service attaqué	Nom de l'attaque	Risque	Recommandations de l'analyse	Adopté ?
Routeur	Scan de ports	Bas	-Configurer iptables du firewall	Oui
	DNS Spoofing	Moyen	-Empêcher l'ARP Spoofing =>serveur DHCP avec une liste fermée	Non
			-Configurer le DNS	Oui
Tout le réseau	SSPD (Universal plug Plug and Play)	Bas	-Bloquer les ports (5000/1900)	Non
			-Inhibition du service	Oui
Serveur Web	Remplissage de la base	Moyen	- Configuration du Mod security	Oui

Bilan des confrontation:

2 eme confrontation

STRI | Télécoms & Réseaux |

Machine ou service attaqué	Nom de l'attaque	Risque	Recommandations de l'analyse	Adopté ?
Routeur	Scan de ports	Bas	-Configurer iptables du firewall	Oui
	DNS Spoofing	Moyen	-Empêcher l'ARP Spoofing =>serveur DHCP avec une liste fermée	Non
			-Configurer le DNS	Oui
Machine Ciente SP0	Reverse VNC par http (site pirate)	Elevé	-Mettre à jour les SP clients XP	Non
Tout le réseau	Scan de ports UDP	Bas	-Bloquer les ports UDP sauf le port 53 utilisé par le DNS	Oui

Bilan des confrontation:

3 eme confrontation

STRI | Télécoms & Réseaux |

Machine ou service attaqué	Nom de l'attaque	Risque	Recommandations de l'analyse
Switch	Mac Flooding	Moyen	- Autoriser qu'une liste d'adresse MAC prédéfinie par port
			- Appliquer un filtre sur le nombre de correspondance maximum par port.
			- Utiliser l'authentification 802.1X
	Attaques STP	Moyen	- Activer uniquement sur les ports interconnecté à un autre commutateur
			- Activer STRG (Spanning Tree Root Guard)
			- Activer le BPDU Guard sur les Switchs
Serveur Web	Mail bombing	Moyen	-Utiliser eremove

Bilan du projet

- Travail d'équipe à 17 personnes
- Gestion de projet sur un projet complexe et long
- Favorise la communication et les échanges
- Mise en pratique des cours de sécurité

Conclusion

STRI
| Télécoms & Réseaux |

- Projet intéressant qui donne une bonne expérience avant de partir en entreprise

- Charge de travail inégale en comparaison des autres groupes, surtout au début du projet