PROJET SÉCURITÉ

Equipe Défense

Pôle Interconnexion :

- Ilias DJOUAI
- Fabien PEYRONNET

Pôle Services :

- Guillaume COTTIN
- Youri JEAN-MARIUS

Pôle Utilisateurs :

- Philippe BEAUGENDRE
- Vincent LARRIBAU

Pôle Communication :

- Emmanuelle DANG
- Cécile FOSSEN

21 Décembre 2006

SOMMAIRE

- PRESENTATION DE LA GESTION DE PROJET
- PHASE 0 : Le déploiement
- PHASE 1 : Après la 1ère attaque
- PHASE 2 : Après la 2ème attaque
- PHASE 3 : Après la 3ème attaque
- BILAN

La Gestion du Projet

Gestion des équipes

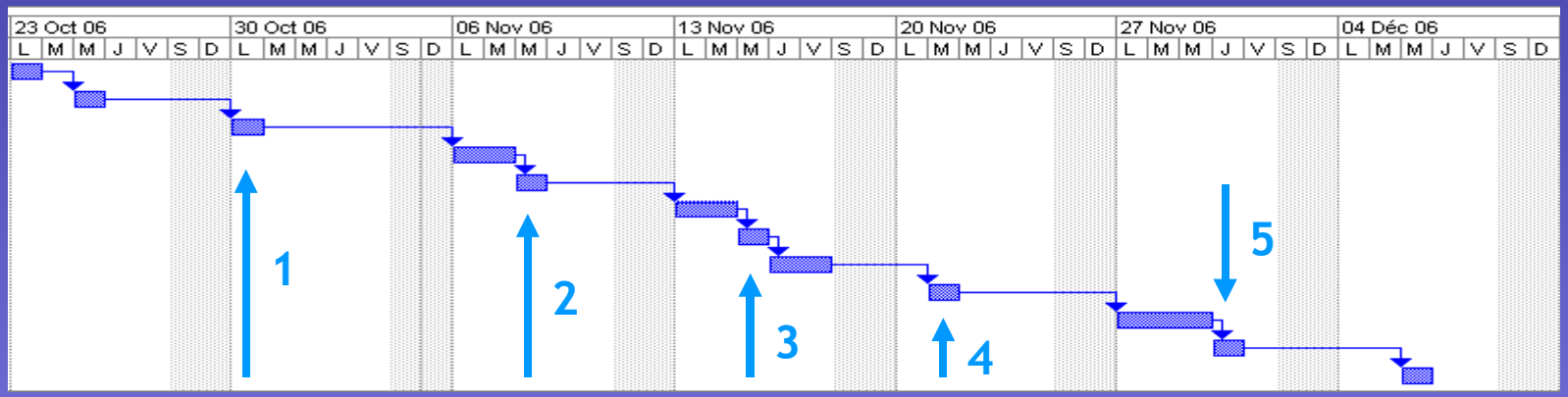
- Décomposition en 4 pôles :
  - Pôle Utilisateurs
  - Pôle Services
  - Pôle Interconnexion
  - Pôle Communication

Gestion des étapes

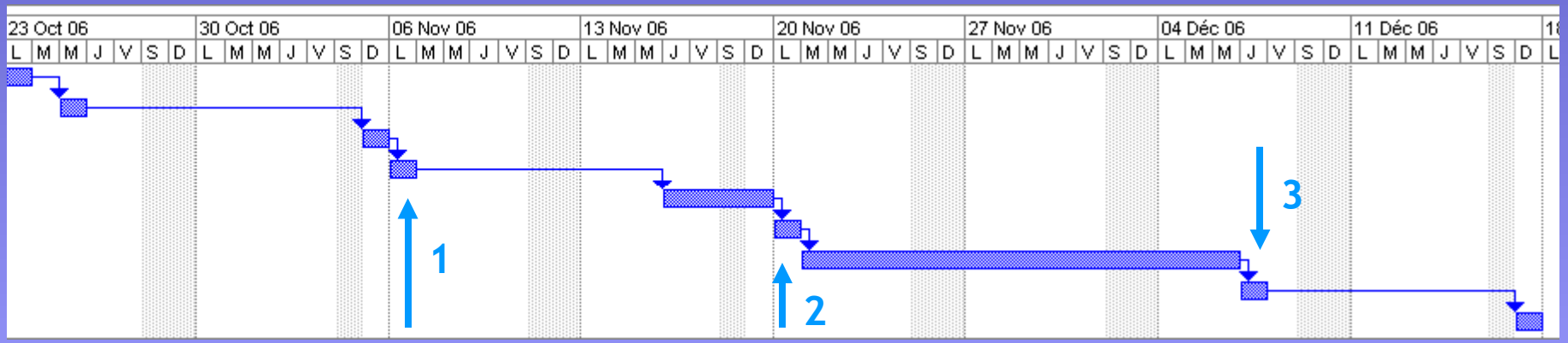
- Concertation avec l'équipe « Attaque » pour convenir des attaques
- Rappel aux différents pôles de l'avancement du projet
- Communication avec l'équipe « Audit »

Gestion du planning

- Définition d'un planning au départ

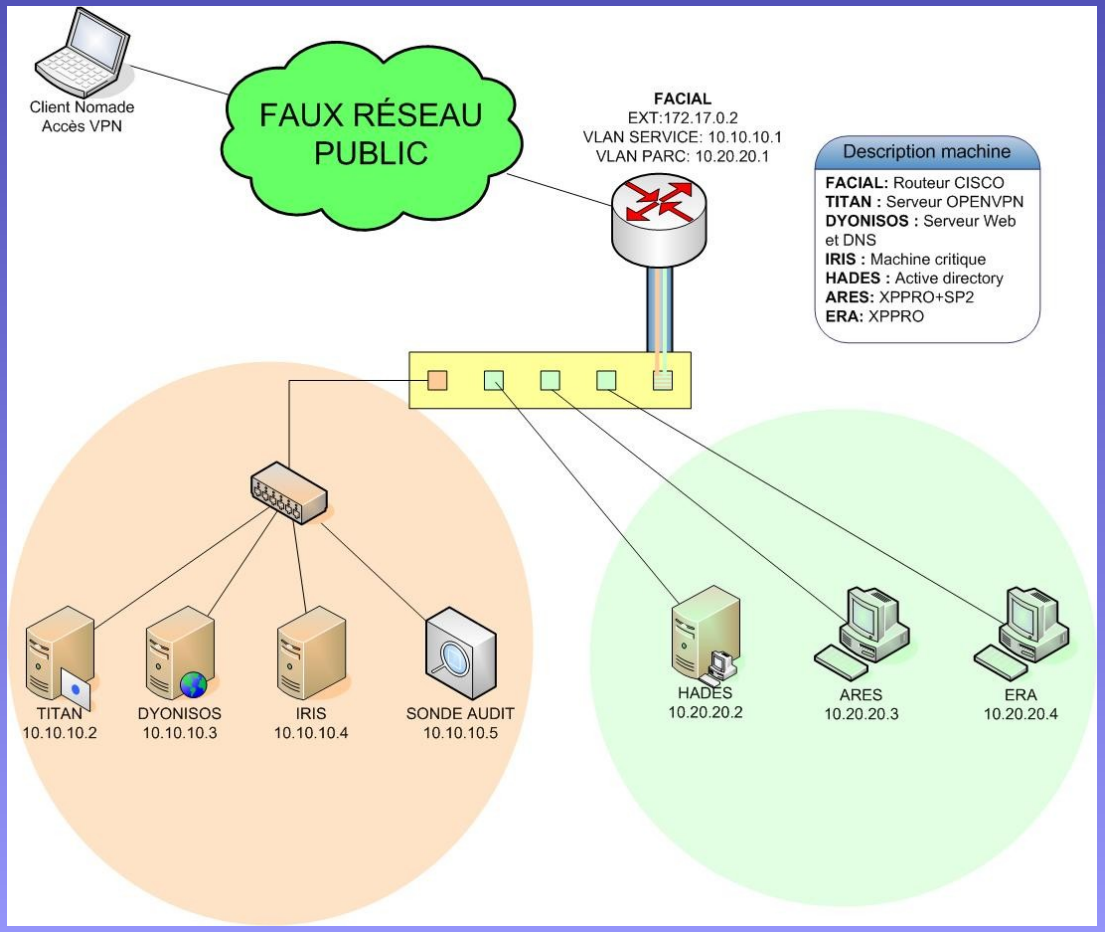


- Planning final



Phase 0

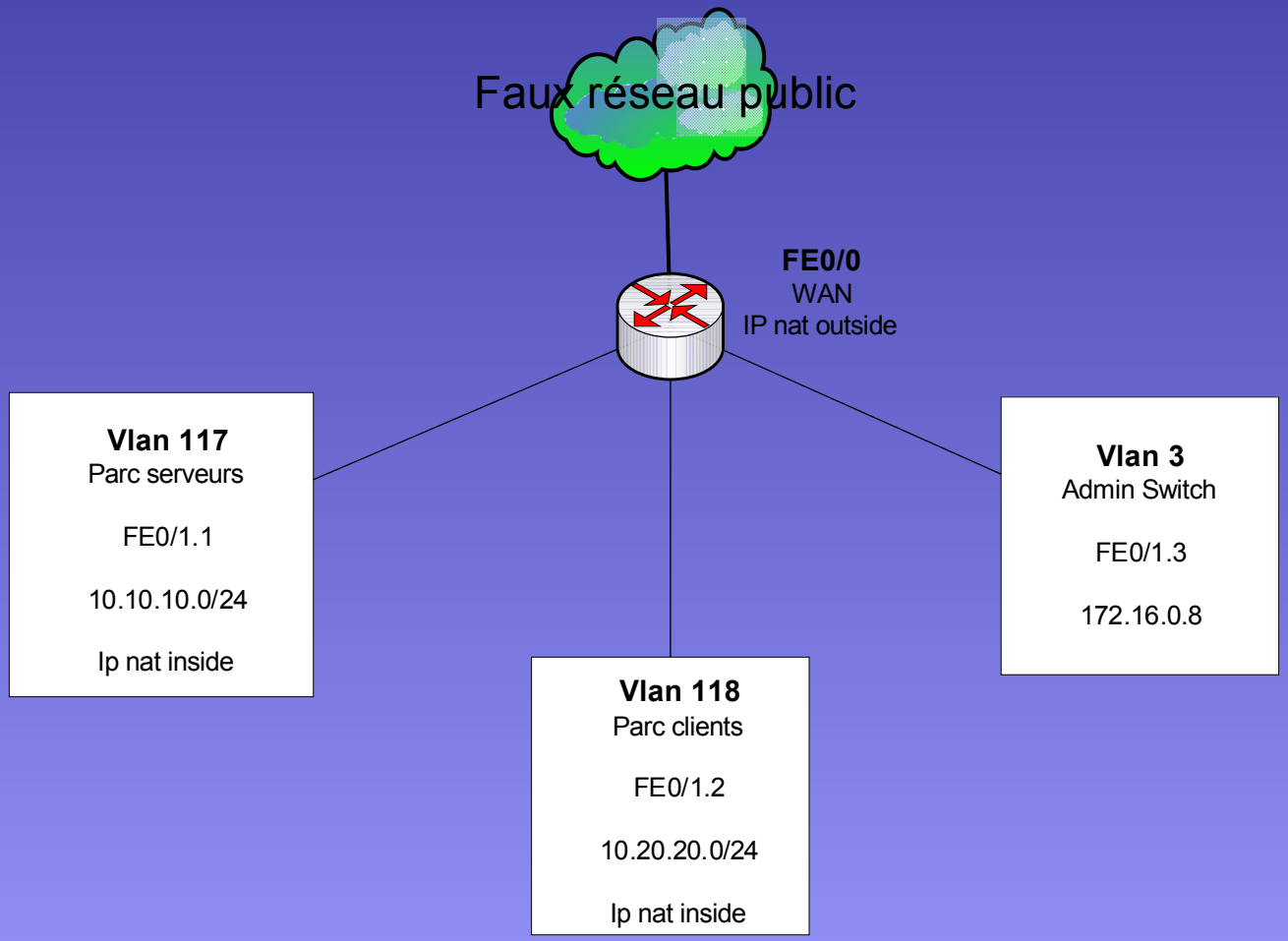
Le déploiement de l'architecture



Pôle Interconnexion

- Mise en place du matériel :
  - Mise en place du routeur
  - Mise à jour de l'IOS
  - Sécurisation des accès Telnet et console par mot de passe (AES)
  - Mise en place d'un mot de passe sur le routeur (AES)

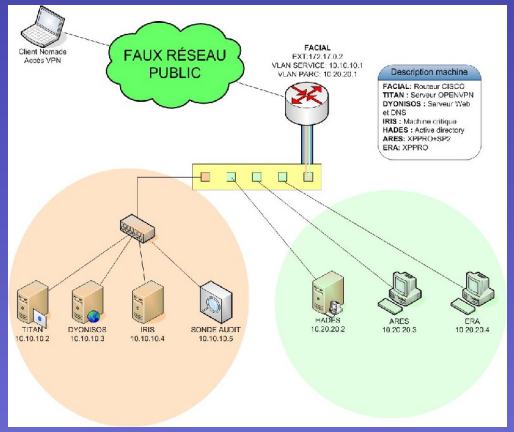
Pôle Interconnexion



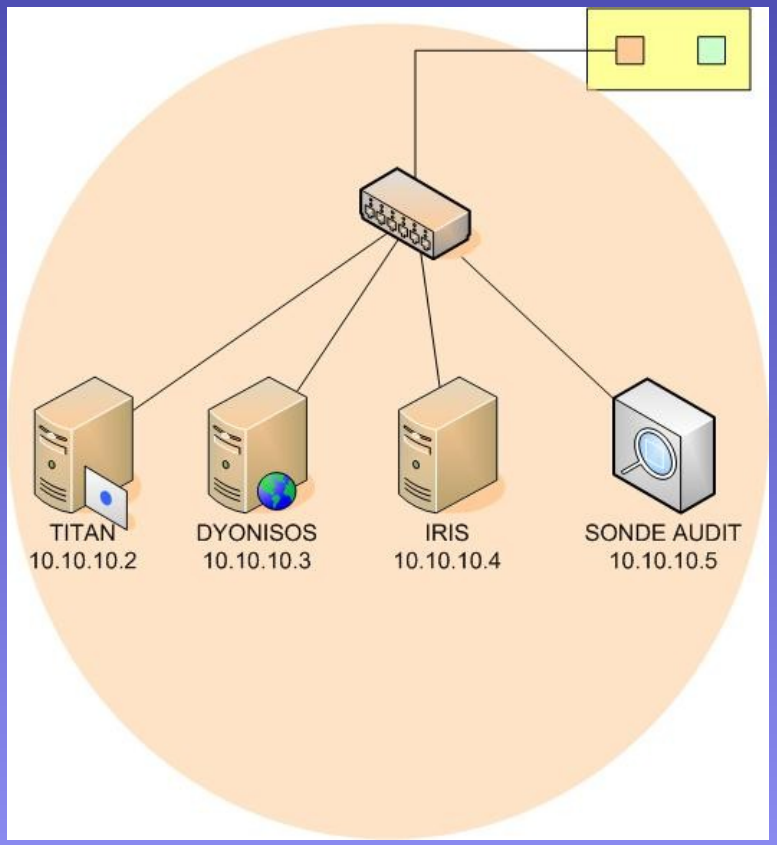
Pôle Services

- Les besoins :
  - Un serveur WEB
  - Un serveur de base de données
  - Un serveur DNS
  - Un serveur de messagerie
  - Un serveur VPN

Pôle Services



- Titan → Linux Debian
- Dyonisos → Linux Debian
- Iris → W2k3 server



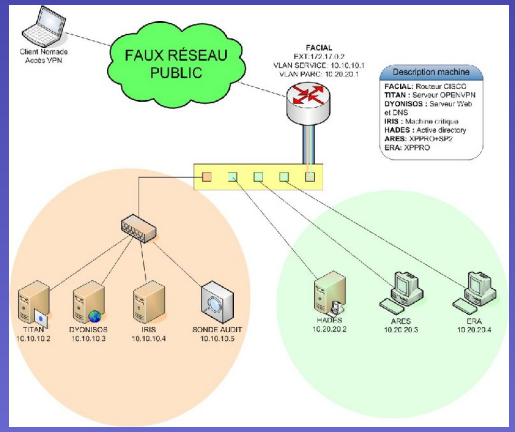
Pôle Services

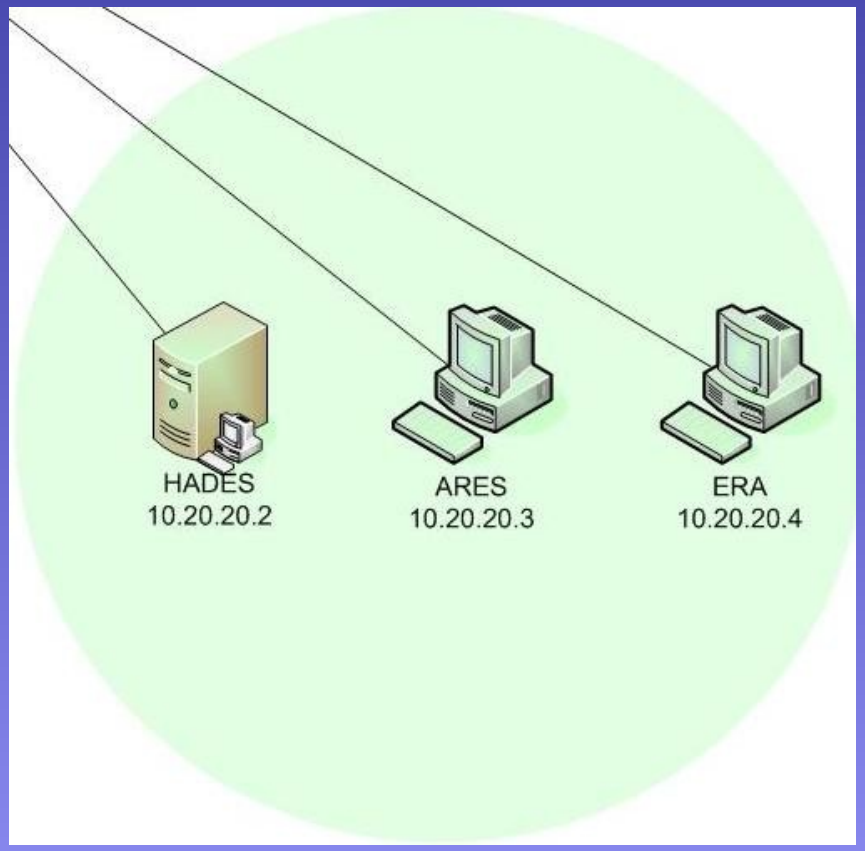
- Titan, le serveur VPN :
  - OpenVPN
  - Certificat commun aux utilisateurs
  - Translation d'adresse
- Dyonisos, le serveur LAMP + DNS :
  - Apache2 + PHP4 + MySLQ4 + PhpMyAdmin
  - Bind9; domaine : candide-sa.com
- Iris, le serveur de messagerie :
  - Difficulté de configuration et de liaison avec le contrôleur de domaine

Pôle Utilisateurs

- Les besoins :
  - Un serveur de domaine Active Directory
  - Un client XP « sécurisé », SP2
  - Un client XP non sécurisé, sans SP2 ni patchs

Pôle Utilisateurs





- Installation des postes :
  - Contrôleur de domaine sous Windows 2003 Server
  - Deux clients Windows XP professionnel

Pôle Utilisateurs

- Intégration des postes dans le domaine
- Aspects sécurité :
  - Politique de sécurité de mots de passe
  - Désactivation du « boot » sur CD et disquette
  - Mot de passe pour le BIOS

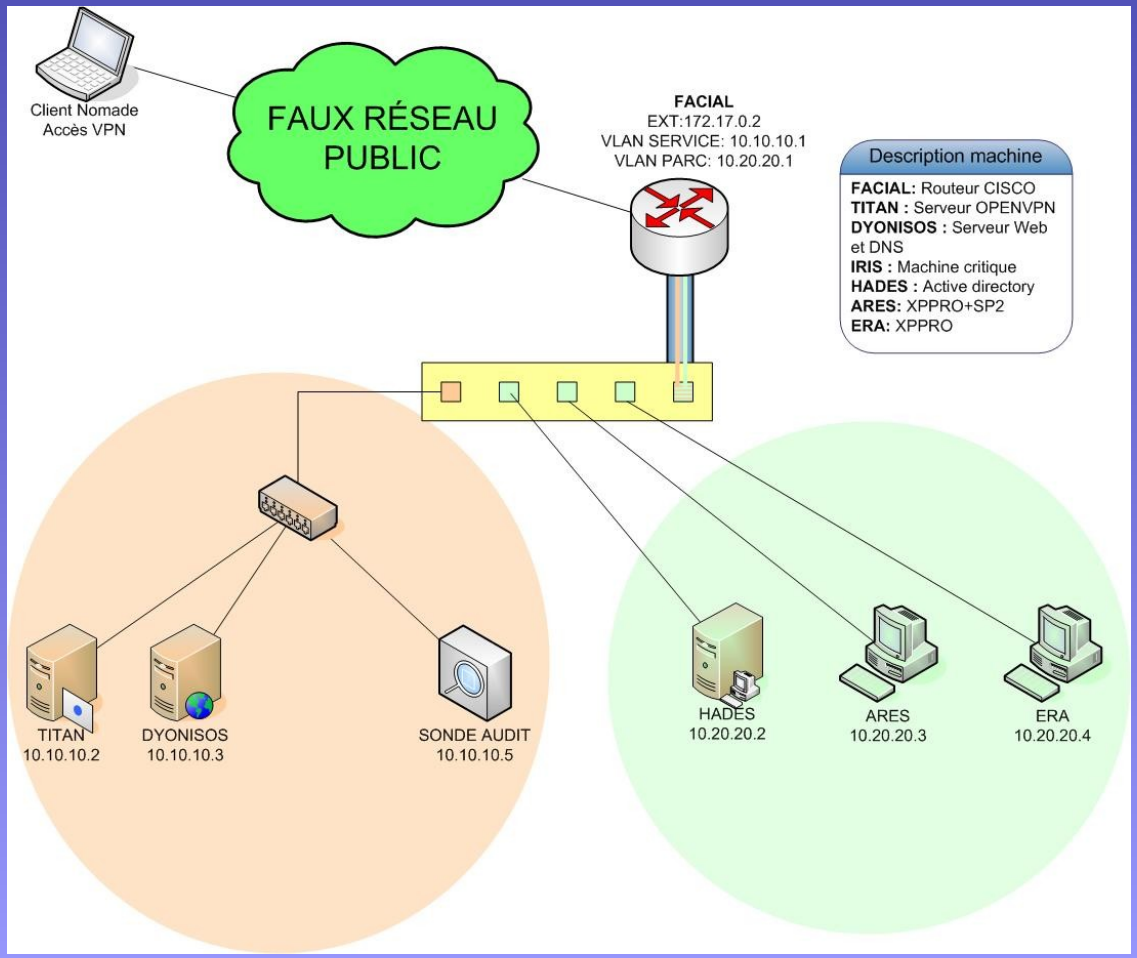
Rapport Audit

- Bilan de sécurité n°1 :
  - Recommandation : consulter les logs d'apache
  - Action effectuée : transfert des logs sur la machine audit

- Bilan de sécurité n°2 :
  - Pas besoin de mettre une sécurité supplémentaire

Phase 1

Après la 1ère attaque du 5 novembre



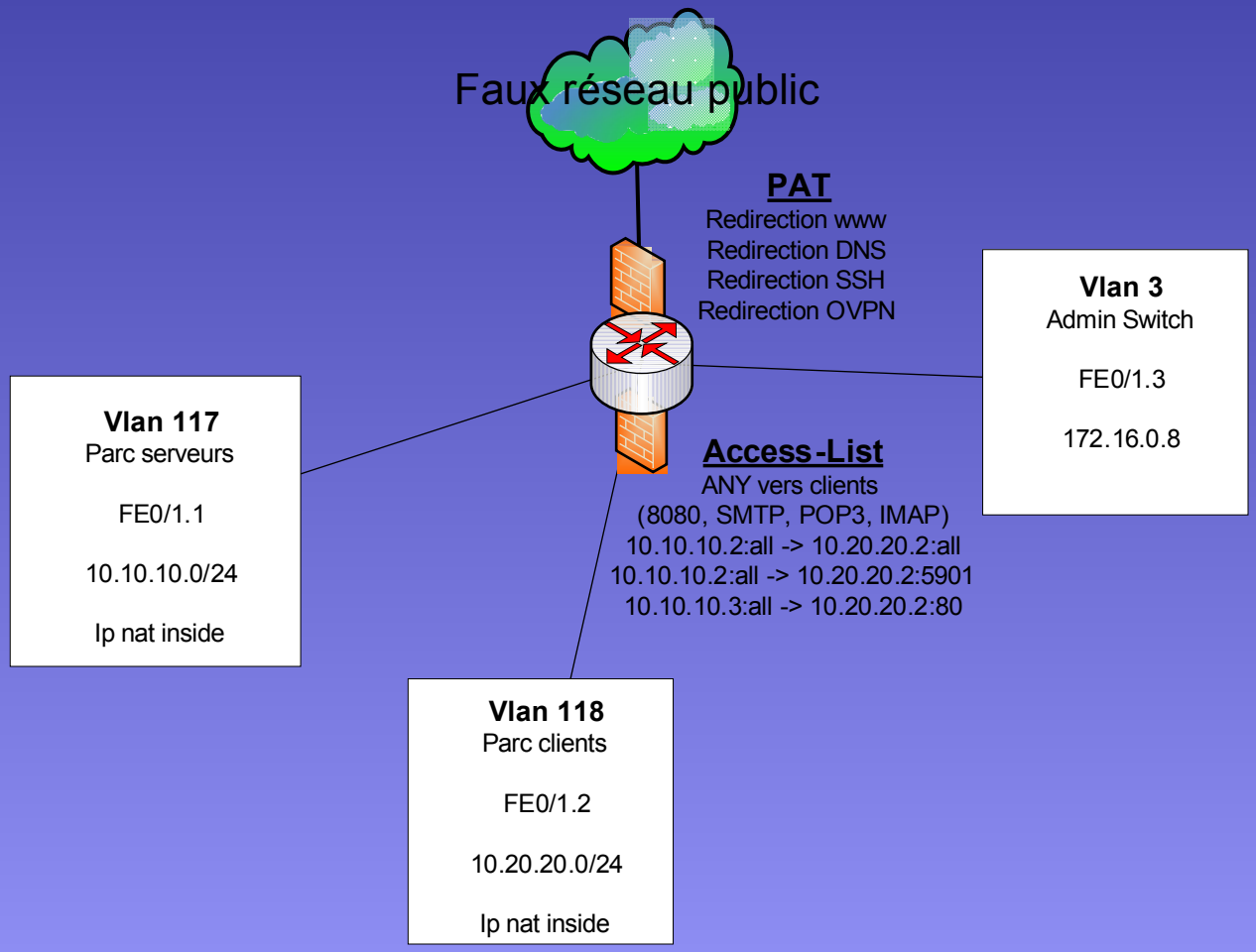
Rapport Audit

- Bilan de sécurité n°3 :
  - Actions de l'attaque détectées :
    - ✓ Attaques sur le serveur web
    - ✓ Exploitation SSL
    - ✓ DNS spoofing
  - Pas de recommandation

Pôle Interconnexion

- Access-list entre le parc serveur et client
- Inspection des flux du port mirroring
- Mise en place de mesure anti-spoofing

Pôle Interconnexion



Pôle Services

- Observations de l'attaque :
  - Saturation du livre d'or
  - DNS Spoofing
- Impacts :
  - Impressions réelles noyées
  - Récupération des accès au site de nos partenaires

Pôle Services

- Sécurisation après 1ère attaque :
  - Sécurisation du serveur WEB
    - ✓ mod-security
  - Sécurisation du serveur DNS
    - ✓ limitation des requêtes extérieures
  - Édition de politique de sécurité
    - ✓ consignes du bon navigateur sur Internet
  - Développement d'un espace restreint

Pôle Utilisateurs

- Manipulations pour l'attaque :
  - Navigation sur le site : stri.net avec les clients XP
  - Authentification sur le site
  - DNS Spoofing : site pirate

- Impacts :
  - Les clients se retrouvent sur un site pirate
  - L'attaque a pu récupérer les logins et mots de passe pour l'accès au vrai site stri.net

Pôle Utilisateurs

- Installation d'un serveur de mails sur le contrôleur de domaine :
  - Installation d'Outlook
  - Création des boîtes aux lettres à partir comptes de domaine

- Mise en place d'un service DHCP :
  - Plage de 10.20.20.3 à 10.20.20.5

Pôle Utilisateurs

- Problèmes rencontrés :
  - Problèmes hardware sur le client XP sans SP2
  - Tentative d'installation d'Exchange dans la DMZ infructueuse

Phase 2

Après la 2ème attaque du 20 novembre

?

Pôle Interconnexion

- Désactivation des services inutiles
- Protection de l'équipement :
  - Prévenir les sessions orphelines
  - Empêcher de bloquer le port console par trop de log
  - Cacher les mots de passes dans les fichiers de configuration
  - Protection des plantages ou blocage de process
  - En cas de crash : envoi d'un DUMP sur un serveur FTP

Pôle Interconnexion

- Gestion des droits d'accès :
  - Déclaration des users avec mot de passe crypté
  - Activation du modèle sécurisé AAA
- Changement des mots de passe

Pôle Services

- Observations de l'attaque :
  - Redirection du livre d'or sur un site de l'attaque

- Impacts :
  - Impossibilité d'affichage du livre d'or
  - Risque pour l'internaute de piratage

Pôle Services

- Evolutions après l'attaque :
  - Sécurisation du code PHP et de la BD
    - ✓ modification des types des champs dans la BD
  - Mise à jour des systèmes
  - Création d'images de sauvegarde

Pôle Utilisateurs

- Observations de l'attaque :
  - Mail bombing sur la boite de l'administrateur de domaine par défaut

- Impacts :
  - Faibles : ~3500 mails avec pièce jointe à supprimer

Pôle Utilisateurs

- Mise en place de Kiwisyslog :
  - Logs redirigés sur le poste de l'audit
- Ghost des postes clients XP
- Sécurisation du DHCP :
  - Attribution des IP en fonction de l'adresse MAC
  - Réduction de la plage à 2 adresses
- Désactivation du compte administrateur de domaine par défaut

Pôle Utilisateurs

- Problèmes rencontrés :
  - Ghost du serveur de domaine impossible avec notre version de Norton

Phase 3

Après la dernière attaque du 7 décembre

. . .

Rapport Audit

- Bilan de sécurité n°4 :
  - Plusieurs recommandations, par exemple :
    - ✓ désactivation du démon telnet sur l'interface extérieure du routeur
    - ✓ installation d'un antivirus sur les postes Windows, passage d'un scan
    - ✓ pas de phpMyAdmin en http (les mots de passe en clair seront récupérables sur le LAN)
    - ✓ passage du serveur exchange du LAN à la DMZ

Pôle Services

- Observations de l'attaque :
  - Paralysie totale de l'accès aux serveurs et aux services
  - Modification du site WEB
- Impacts :
  - Paralysie totale de la société Candide-SA
  - Perte de la crédibilité de la société

Pôle Services

- Réparations après attaque finale :
  - Récupération de la main sur les machines
  - Récupération des logs
  - Remise en état des machines

Le Bilan du Projet

Au sein de l'équipe

- Pas de problème d'entente
- Entraide toujours présente

- Du point de vue pôle Communication :
  - « difficulté » de diriger des personnes que l'on connait
  - anticipation sur les rapports

Avec les autres équipes

- Favoriser le travail de chaque équipe
- Se synchroniser avec les équipes
- Pas de problème de communication
- Une bonne entente en général

Bilan général

- Un tel projet :
  - permet d'avoir une meilleure vision du travail en équipe
  - nous montre l'approche gestion de projet
  - favorise la communication et les échanges

QUESTIONS…