M2 STRI

Jean-Thierry EMOH ZOGO
Arnaud GALONNIER
Walter GIN
Libasse HANNE
Jean Pierre HOANG
Osnelle HOUANSOU
Thomas ISSOLAH
Frédéric JAMOIS
Sami KACHA
Aleksandar KALEV
Pooya KHADEMI
Sylvain LACOUE
Olivier LANNRETONNE
Julien LEBRETON
Dimitri LEGALLAIS
Nicolas LEYMARIE
Jérémy MACHETO
Nicolas MADELAINE

Sécurité Réseau

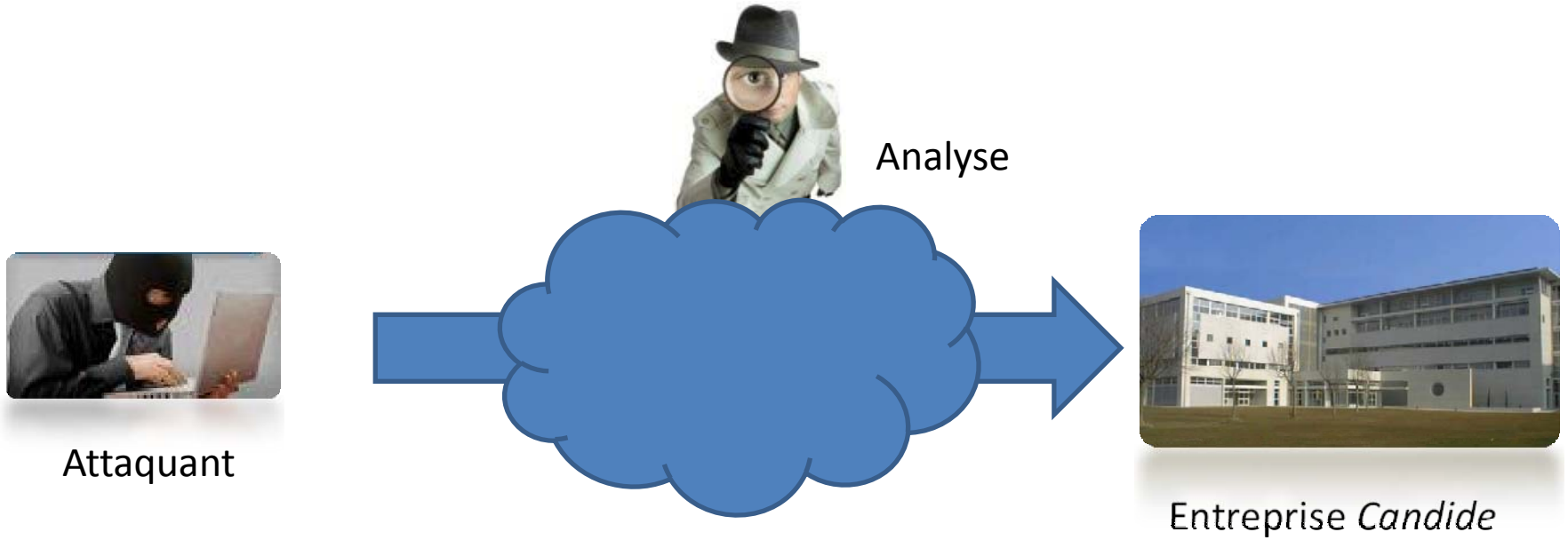
Groupe ANALYSE

15 décembre 2008

Sommaire

I/ Présentation du projet

1) Le contexte



1) Le contexte

- ✓ Travailler en équipe avec une bonne coordination
- ✓ Communiquer avec les différents groupes (Défense et Attaque)
- ✓ Découvrir le métier d'audit de réseau informatique
- ✓ Savoir prédire les failles du système de sécurité mis en place par la défense
- ✓ Superviser le réseau et conseiller le groupe Défense
- ✓ Dégager les responsabilités, les objectifs et les moyens mis en œuvre en les explicitant dans un contrat avec la Défense
- ✓ Analyser les logs pour informer la Défense de l'état de son réseau
- ✓ Faire preuve de réactivité en cas de déni de service sur le réseau

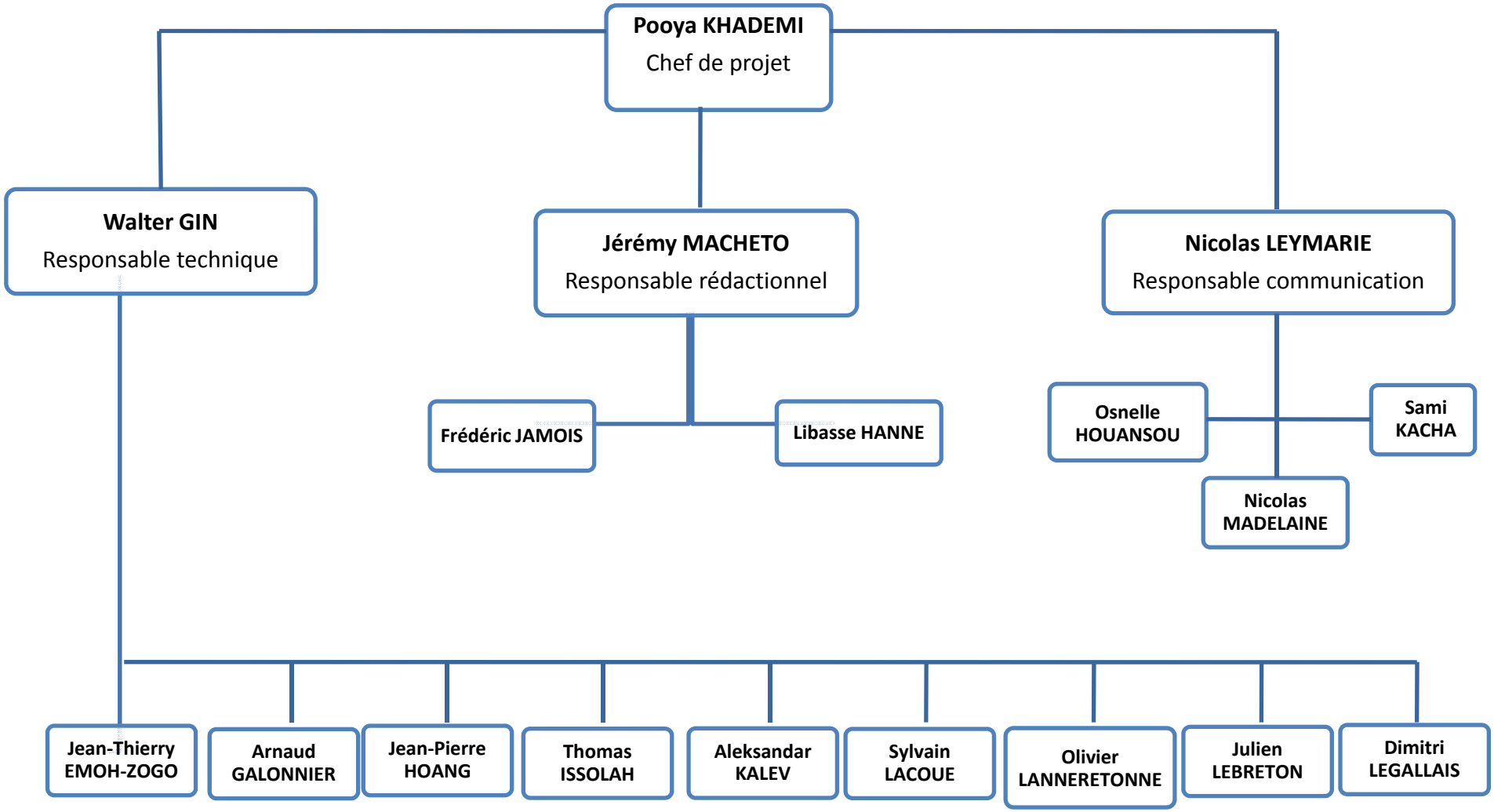
1) Le contexte

Groupe communication

Groupe technique

Groupe rédactionnel

2) Diagramme organisationnel et évolutions



3) L'audit, qu'est ce que c'est ?

OBJECTIFS

- ✓ Evaluer les risques encourus par le système d´information
- ✓ Préconiser des parades

~~Installation et configuration d'un simple pare-feu~~
~~Tests de vulnérabilités automatisés depuis Internet~~
~~Vérification du code source des applications maison~~

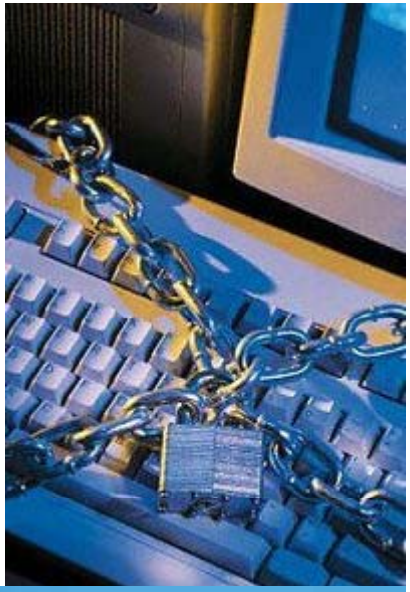
L'audit c'est :
- ✓ Une prestation interne
- ✓ Des équipes dépêchées sur site afin de pratiquer des mesures
- ✓ La découverte des faiblesses et la proposition obligatoire de solutions pour chacune d´elles.

3) L'audit, qu'est ce que c'est ?

Un audit de sécurité n'est il pas une perte de temps et d'argent ?

Informatique = risques = menaces pour l'activité de l'entreprise

- Risques naturels, pas dramatiques en eux-mêmes
- C'est le fait de les ignorer qui est dramatique.



Ignorer un risque ne le supprime pas mais augmente le danger qu'il représente.

L'audit de sécurité a pour but de contrôler le risque informatique en l'identifiant, en le quantifiant puis en le maîtrisant.

3) L'audit, qu'est ce que c'est ?

2 TYPES D'AUDITS :

ORGANISATIONNEL

Couvre l´ensemble du système d´information de l´entreprise, de son personnel à ses procédures.

TECHNIQUE

Etude détaillée d'une architecture particulière (passerelle, interconnexion, application...).

II/ Coordination du groupe

1) Les outils de communication

Les e-mails

Live Messenger

Skype

Wiki

Clés USB

2) Notre politique de sécurité et ses évolutions

A éviter

E-mails

Clés USB

- boites mails non sécurisées
- mots de passe mails non sûrs
- Perte/vol des clés USB
- Données éparpillées

A privilégier

- ✓ Informations chiffrées
- ✓ Centralisation des données
- ✓ Authentification par mot de passe
- ✓ Collaboratif

2) Notre politique de sécurité et ses évolutions

3 NIVEAUX

Niveau 1 : confidentialité peu élevé par e-mail

- ✓ Informations d'ordre générale
- ✓ Heures et lieu de rendez vous
- ✓ Remarques

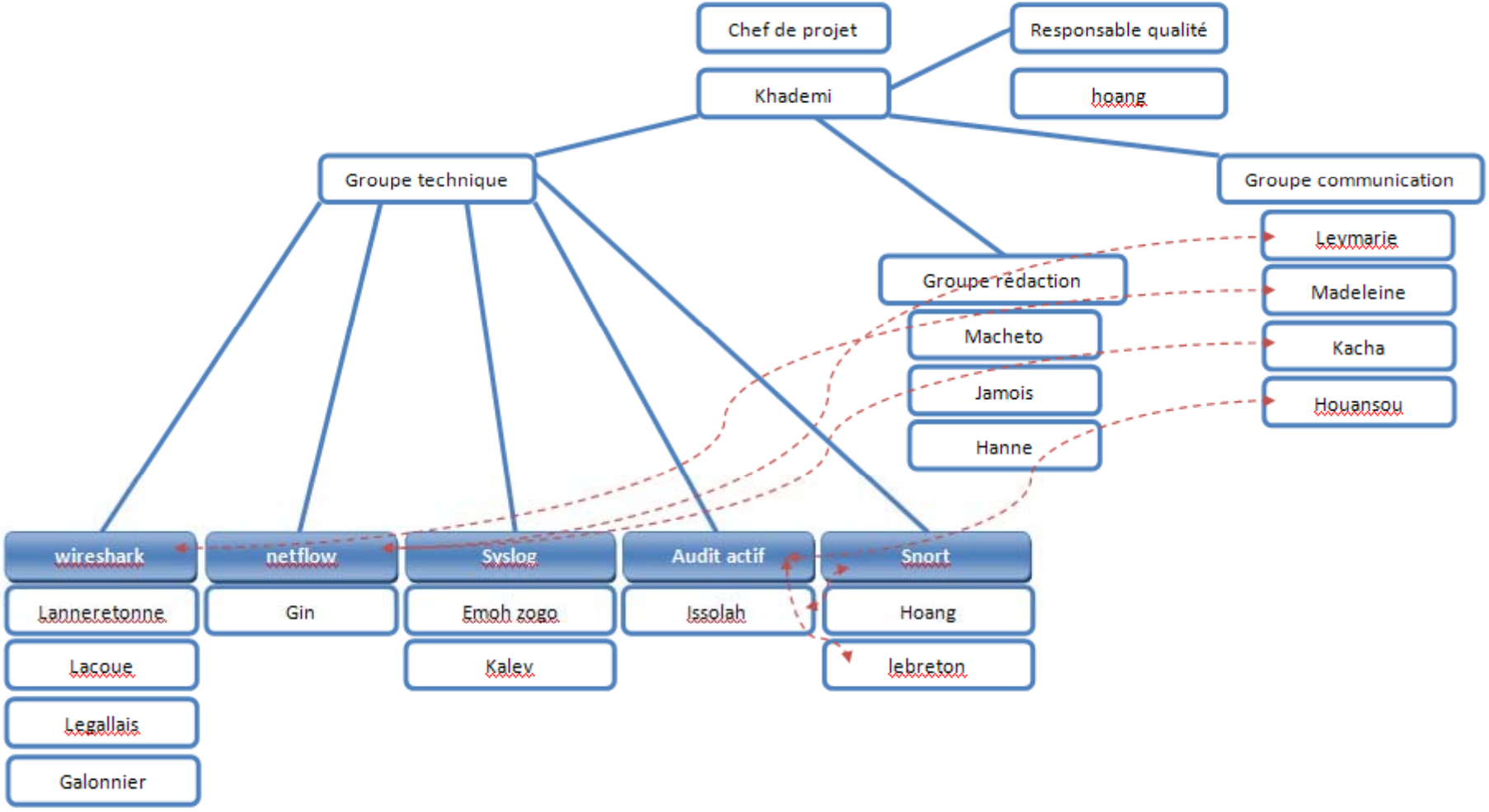
Niveau 2 : connexion à l'espace collaboratif docuWiki

- ✓ Informations confidentielles
- ✓ Ne pas divulguer les paramètres d'accès au wiki
- ✓ Ne pas prêter son login/mot de passe

Niveau 3 : comptes rendus de réunion et comptes rendus techniques

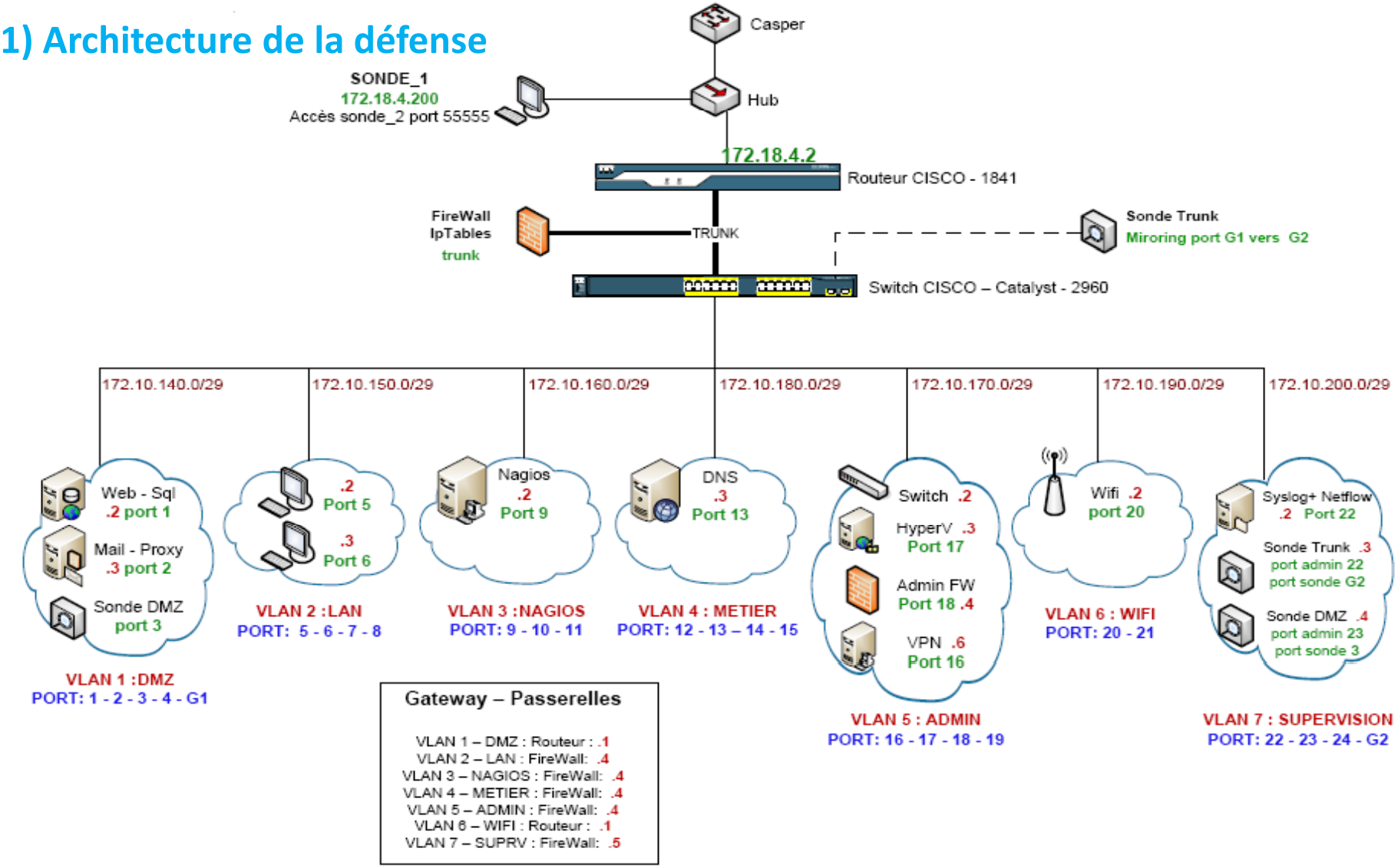
- ✓ Compression en .RAR chiffrée

3) Evolution des groupes



III/ Les outils utilisés

1) Architecture de la défense



2) Ce que l'on veut analyser

- Collecter des informations sur le trafic IP des équipements
- Récolter des informations sur le trafic passant par le routeur CISCO
- Effectuer en temps réel les analyses de trafic
- Logger les paquets IP transitant sur le réseau

3) Implémentation et outils

NETFLOW

Protocole CISCO mais aussi **open-source**
Permet de collecter des informations sur le trafic IP des équipements IOS (**I**nternetwork **O**perating **S**ystem).

Suite d'outils **NFDUMP:**

Collecteur

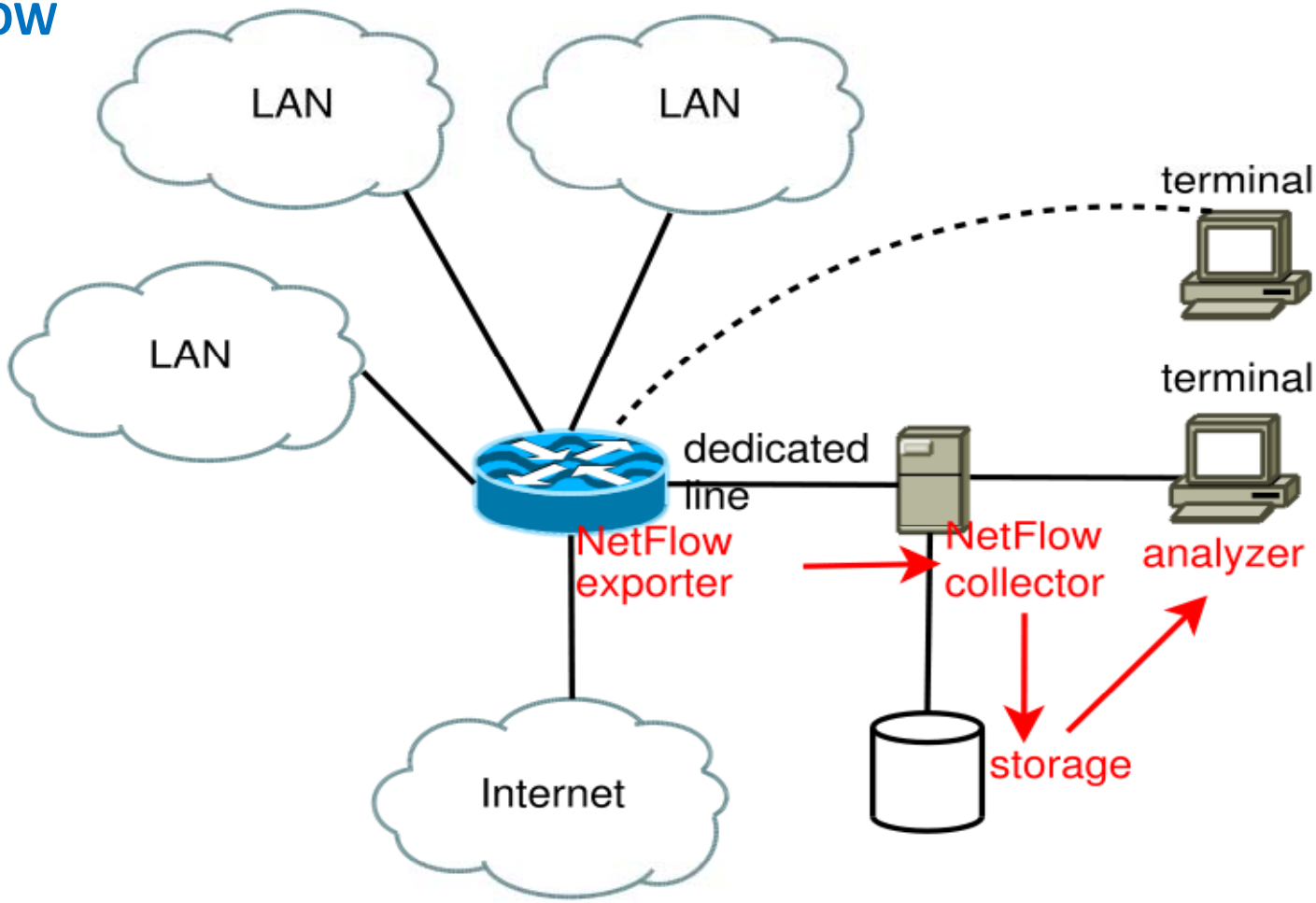
netflow capture daemon

Analyseur

netflow dump
Nfsen

3) Implémentation et outils

NETFLOW



3) Implémentation et outils

Les outils

SNORT

3 modes de fonctionnement:

- sniffer de paquets,
- Logger de paquets,
- Système de détection/prévention d'intrusions.

2 sondes SNORT installées sur le réseau afin de capturer le trafic :

1ère sonde, placée juste avant le réseau de l'entreprise: permet de capturer toutes les attaques qui sont destinées au réseau;

2ème sonde, placée juste après le firewall : permet de voir toutes les attaques bloquées et surtout analyser celles qui seront passées pour renforcer la sécurité du réseau;

3) Implémentation et outils

SONDES

But/pourquoi :

- ✓Analyser en temps réel les transactions sur le réseaux
- ✓Détecter les attaques connues
- ✓Générer des alertes

Comment :

- ✓Snort en mode IDS
- ✓Barnyard => interface snort et base Mysql

Configuration

- ✓Preprocesseurs : notamment http_inspect

AVANTAGE

- Equipement passif

INCONVENIENT

- Mode promiscuité => Deux interfaces

3) Implémentation et outils

CAPTURE DE TRAMES

Cahier des charges

- ✓ Analyse de trame
- ✓ Constituer un outil d'analyse

But/Pourquoi

- ✓ Récupérer le maximum de trames transitant sur le réseau
- ✓ Données au format PCAP pour analyse avec outils graphiques et lignes de commande

Comment

- ✓ TCPDUMP wrapper dans un script de lancement en fond de tache

3) Implémentation et outils

INTERFACE WEB

OUTILS :

- ✓ APACHE mode SSL
- ✓ PHP
- ✓ MySQL
- ✓ AcideBase
- ✓ rrdtools

AVANTAGE

➢ Outils largement déployés et bonne tenue en charge

INCONVENIENTS

➢ MySQL inapte à gérer plus de 5 Millions d'entrées
➢ Ouverture de la sonde

3) Implémentation et outils

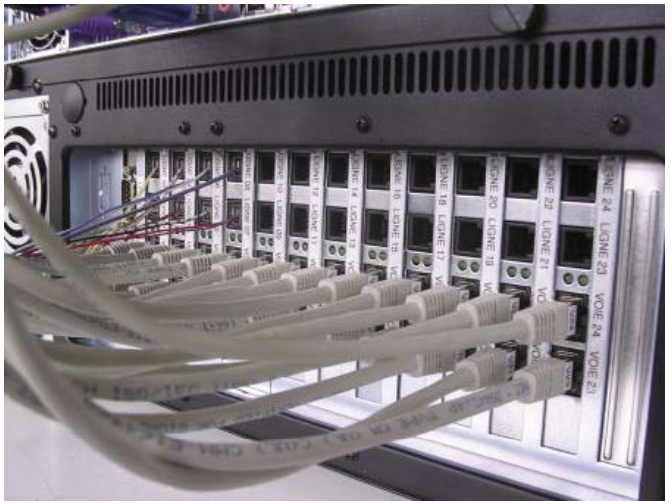
STATISTIQUES RESEAUX

Cahier des charges

- ✓ Analyser en temps réel ce qu'il se passe sur le réseau

Outils :

- ✓ Mise en place de NTOP sur les sondes
- ✓ Ecoute sur interface capture
- ✓ Fonctionne sur interface de loopback
- ✓ Apache mode proxy pour accès distant SSH



3) Implémentation et outils

STATISTIQUES RESEAUX

AVANTAGES

- ✓ suivi des courbes d'utilisation du réseaux
- ✓ Segmentation par protocole
- ✓ Segmentation par adresse

INCONVENIENTS

- ✓ Lourdeur de NTOP
- ✓ Recuperation des données laborieuse
- ✓ Necessite ouverture de la sonde

3) Implémentation et outils

SECURISATION DES SONDES

Première confrontation

Une seule interface (critique)

- Administration et capture
- Sonde accessible => attaques possibles

Seconde et troisième confrontation

Deux interfaces distinctes

Une interface admin (vlan supervision)

Une interface écoute (SPAN)

- Meilleure sécurité
- Mise en place d'IPTables
- Interdire le saut de VLAN => désactiver DTP switch

3) Implémentation et outils

SECURISATION DES SONDES

Sécurisation Apache + php + mysql

Restriction accès par certificats

Sécurisation SSH

Pas de login root

Pas de X11forwarding

Sécurisation interface admin

Mise en place IPTABLES restrictives

3) Implémentation et outils

LOGS

Cahier de charges

principe général - collecter/centraliser des logs depuis machines différentes (hétérogènes)

mise en place

nous utilisons une machine qui nous est propre

avantages

on s'assure qu'il n'y a pas de pertes de données(logs) provoquées par des dysfonctionnements dans le réseau/config de la défense

Maitrise du collecteur

inconvénients

produire une config stable et pertinente...

contraintes

- configuration spéciale pour chaque source(machine) de la défense

3) Implémentation et outils

LOGS

+ Outils
 + syslog-ng - le successeur de l'outil syslog unix classique
  + avantages
   - outil très souple, permet de collecter, filtrer et acheminer des logs en format texte
   - facile a configurer
   - bien documenté
  + inconvenients :
-dépends d'un horodatage
-intégrité et authenticité

3) Implémentation et outils

LOGS

+ Perl - Practical Extraction and Reporting Language
  + avantages
    - logs hétérogénes (windows xp, cisco router, cisco switch) - besoin d'un outil souple, perl permet de le forcer
    - logs hétérogènes - dépendance de la defence
  + inconvénients
    - exige des connaissances en Perl
  + exemples (simple one-liners):

```
$perl -wn -e 's/\<142\>/\n/g; print;cisco1841_notice_n | $perl -wn -e
's/\<142\>/\n/g; print;' cisco1841_info_n | perl -wnla -e 'if ($F[2] eq '3') { print; }'
```

3) Implémentation et outils

LOGS

+ Vim
  + avantages
    - facilité d'utilisation des expressions régulières
    - visualisation facile des matchs (resultats d'une recherche)

3) Implémentation et outils

AUDIT ACTIF

Cahier des charges

- ✓ Faire une étude des éléments actifs sur le réseau
- ✓ Point critique
- ✓ Recommandations clients

Comment

- ✓ Nessus scanner vulnérabilités
- ✓ Nmap scanner de ports

3) Implémentation et outils

AUDIT ACTIF : NESSUS

Outil d'audit actif : scanner de vulnérabilité

- ✓Déterminer machines actives du réseau
- ✓ Déterminer les ports ouverts (1→ 1024)
- ✓ Déterminer les versions OS + applications
- ✓ Vérification des points critiques
- ✓ Rapport html

3) Implémentation et outils

AUDIT ACTIFS : SERVEUR MAIL

Cahier des charges

- Analyser les fichiers de configuration de la messagerie

OUTILS

- best practise de POSTFIX
- Openssl
- inscription dans le DNS

IV/ Les confrontations

1) Démarches de l'analyse

- Récupération des logs
- Segmentation des traces avec filtrage
- Recensement des attaques
- Répartition des attaques relevées
- Analyse approfondie des attaques
- Recherche de parades

Présentation à l'équipe Défense des résultats
Envoi document de recommandations

✓ Démarche de travail qui a évolué
✓ des problèmes de coordination au début
✓ Mise en place d'une méthode de travail

2) Exemples d'attaques détectées

MAC flooding

✓ envoi massif de requêtes ARP.

<u>But:</u> saturation mémoire du Switch qui fonctionne alors en HUB (reception reply ARP par l'attaque)

Mail bombing

✓envoi massif de mails

<u>But</u>: saturer la bande passante du serveur Mail

Reverse VNC par HTTP

✓injection de code par exploit via http

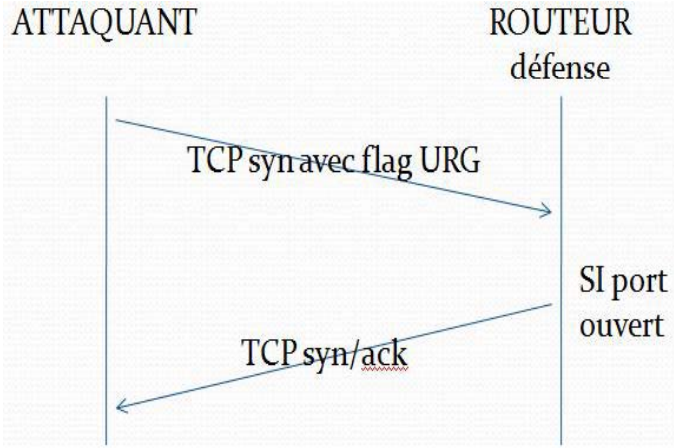
<u>But</u>: Prendre le control d'un PC grâce à un tunnel VNC

DNS Hijacking

✓ fait partie du "man in the Middle"

But: détourner le trafic réseau

2) Exemples d'attaques détectées



Scan de ports

réalisé avec le logiciel NMAP

souvant venant de INTEL_b8:4e:2c

ports ouverts sur le réseau candide détectés

conseil de mise en place SCANLOGD + IPTables

No. .	Time	Source	Destination	Protocol	Info
2280	0.220644	47.56.31.0	172.18.4.2	TCP	37526 > http [SYN, URG] Seq=0 Win=1564, bogus TCP header length (0, must be at least
7297	0.786003	55.108.117.0	172.18.4.2	TCP	37526 > http [SYN, URG] Seq=0 Win=13343, bogus TCP header length (0, must be at leas
7605	0.815526	172.18.4.202	172.16.97.10	TCP	http > 37526 [SYN, ACK] Seq=0 Ack=0 Win=5792 Len=0 MSS=1460 TSV=1765422 TSER=1671581
59390	12.815532	172.18.4.202	172.16.97.10	TCP	http > 37526 [SYN, ACK] Seq=0 Ack=0 Win=5792 Len=0 MSS=1460 TSV=1768422 TSER=1671581
59418	32.654881	172.16.97.10	172.18.4.202	HTTP	GET /acidbase//base_qry_alert. [Packet size limited during capture]
59419	32.654979	172.18.4.202	172.16.97.10	TCP	http > 37526 [ACK] Seq=1 Ack=534 Win=858 Len=0 TSV=1773381 TSER=1682591
59420	33.280286	172.18.4.202	172.16.97.10	HTTP	HTTP/1.1 200 OK [Packet size limited during capture]
59421	33.280396	172.18.4.202	172.16.97.10	HTTP	Continuation or non-HTTP traffic[Packet size limited during capture]
59422	33.284448	172.16.97.10	172.18.4.202	TCP	37526 > http [ACK] Seq=534 Ack=1355 Win=137 Len=0 TSV=1682748 TSER=1773538
59423	33.284669	172.18.4.202	172.16.97.10	HTTP	Continuation or non-HTTP traffic[Packet size limited during capture]
59424	33.284783	172.18.4.202	172.16.97.10	HTTP	Continuation or non-HTTP traffic[Packet size limited during capture]
59425	33.288092	172.16.97.10	172.18.4.202	TCP	37526 > http [ACK] Seq=534 Ack=2709 Win=182 Len=0 TSV=1682749 TSER=1773538
59426	33.288297	172.18.4.202	172.16.97.10	HTTP	Continuation or non-HTTP traffic[Packet size limited during capture]
59427	33.288412	172.18.4.202	172.16.97.10	HTTP	Continuation or non-HTTP traffic[Packet size limited during capture]
59428	33.289188	172.16.97.10	172.18.4.202	TCP	37526 > http [ACK] Seq=534 Ack=4063 Win=227 Len=0 TSV=1682749 TSER=1773539
59429	33.289283	172.18.4.202	172.16.97.10	HTTP	Continuation or non-HTTP traffic[Packet size limited during capture]
59430	33.290886	172.16.97.10	172.18.4.202	TCP	37526 > http [ACK] Seq=534 Ack=5417 Win=273 Len=0 TSV=1682749 TSER=1773539
59431	33.291131	172.18.4.202	172.16.97.10	HTTP	Continuation or non-HTTP traffic[Packet size limited during capture]
59432	33.292686	172.16.97.10	172.18.4.202	TCP	37526 > http [ACK] Seq=534 Ack=6771 Win=318 Len=0 TSV=1682750 TSER=1773540
59433	33.294280	172.16.97.10	172.18.4.202	TCP	37526 > http [ACK] Seq=534 Ack=8125 Win=363 Len=0 TSV=1682750 TSER=1773540
59434	33.294283	172.16.97.10	172.18.4.202	TCP	37526 > http [ACK] Seq=534 Ack=8401 Win=406 Len=0 TSV=1682750 TSER=1773540
59435	33.334113	172.16.97.10	172.18.4.202	TCP	37526 > http [ACK] Seq=534 Ack=9546 Win=451 Len=0 TSV=1682751 TSER=1773540
59436	33.334489	172.16.97.10	172.18.4.202	HTTP	GET /acidbase/styles/ossim.sty [Packet size limited during capture]

3) Nos préconisations

ETUDE DE LA POLITIQUE DE SECURITE

- Définition du domaine à protéger
- Définition de l'architecture
- Plan de reprise sur incident
- Charte de confidentialité pour l'équipe Défense
- Charte de confidentialité pour l'équipe Analyse
- Définition des droits et accès des équipements

3) Nos préconisations

RECOMMANDATIONS

✓ Bloquer certain ports laissés ouverts sur le routeur.

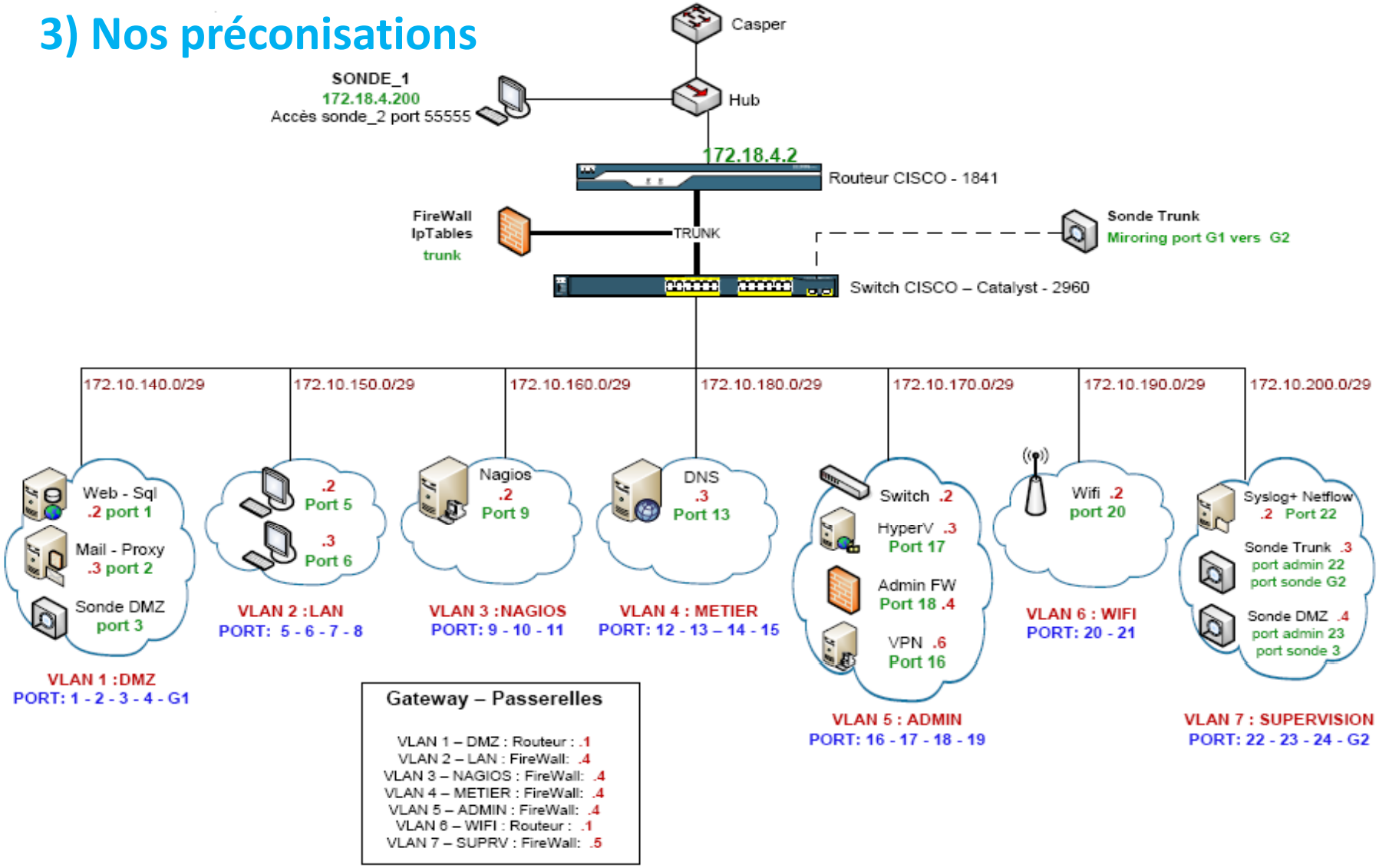
✓ Configurer votre pare-feu pour empêcher les scans

✓ Mettre en place un serveur DHCP avec une liste «fermée» de correspondance

✓ Configurez votre serveur DNS

✓ Mettre à jour les services pack et installation d'anti-virus pour les clients xp

3) Nos préconisations



V/ Les contraintes

1) Les difficultés humaines

a) Relations avec la défense

- ✓ Disponibilité des personnes
- ✓ Délai de réception des documents
- ✓ Chaque manipulation à faire pour l'analyse sur le réseau de la défense est très longue
- ✓ Tout archiver

1) Les difficultés humaines

b) Coordination du groupe

- ✓Gestion de la disponibilité des membres au sein des sous-groupes
- ✓Evolution des rôles de chacun
- ✓Division des tâches et des rôles
- ✓Gestion de l'information entre les groupes
- ✓Communication entre les sous-groupes
- ✓Confusion des postes
- ✓Politiques de sécurité

2) Les difficultés techniques

a) Matérielles

- Hardware :
  - nombre limité
  - puissance
  - dysfonctionnement de certains composants
- Software :
  - impossibilité d'utiliser des softwares payant (Ipswitch WhatsUp GOLD, NetfFlow Tracker, etc.)
- Accès au matériel
  - accès réduit aux heures d'ouvertures de la salle machine

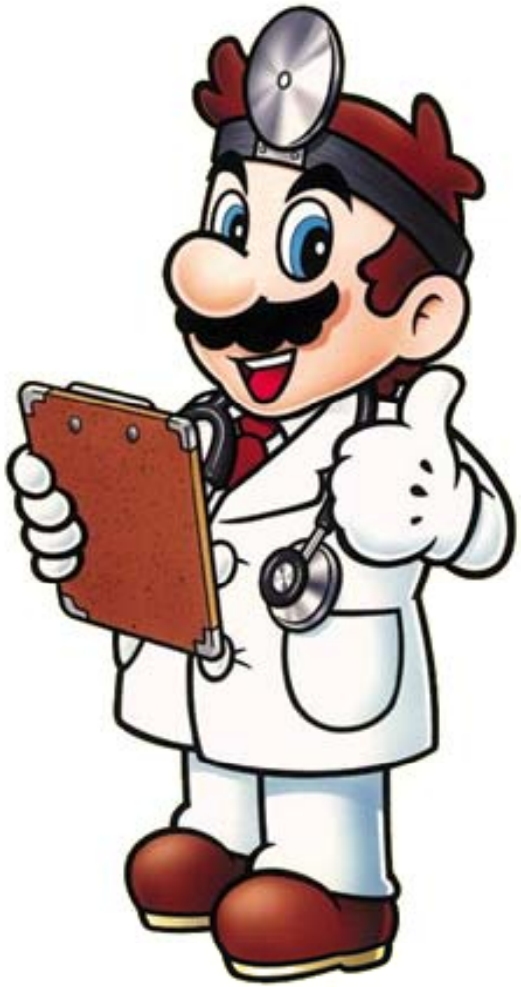
2) Les difficultés techniques

b) Timming

- Problèmes de synchronisation avec la défense
  - modifications techniques à effectuer
  - récupération des constations effectués par la défense lors des confrontations

- Corrélation des résultats inter-pôles
- Délais d'analyse des attaques parfois un peu court

VI/ Conclusion



Sur le plan gestion de projet et organisation

- Une équipe responsable et dynamique
- Bonne gestion dans l'ensemble
  - Répartition des taches
  - Des sous-groupes bien organisés
  - Moyens de communication
    - Respect de la politique de securité

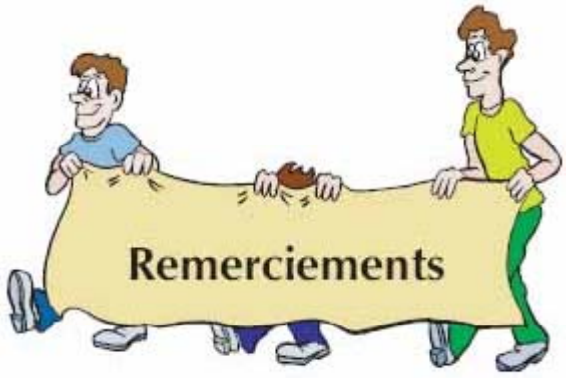
- Respect des délais
  - Communication avec les deux autres groupes
- Amelioration des contrats

Sur le plan technique

- Evolution par rapport aux attaques de la 1° à la 3° confrontation
  l'ajout d'une 2ème sonde
- L'architecture du réseau de la defense

Remerciements

- Les membres de l'equipe analyse
- Les enseignants M. Foucher et M. Latu
- Les défenseurs
- Les attaquants



Questions