CHAPITRE 3 :
Solutions pour protéger un réseau TCP/IP

Mohammed SABER

Département Électronique, Informatique et Télécommunications
École Nationale des Sciences Appliquées "ENSA"
Université Mohammed Premier OUJDA

Année Universitaire : 2017-2018

Plan de chapitre

1. Introduction
2. Règles élémentaires d'une stratégie de sécurité réseau
3. Solutions pour isoler et protéger un réseau TCP/IP
4. La technique de filtrage

Plan de chapitre

1. Introduction
2. Règles élémentaires d'une stratégie de sécurité réseau
3. Solutions pour isoler et protéger un réseau TCP/IP
4. La technique de filtrage

Introduction

- Les solutions faisant partie de la sécurité active représentent tout ce qui permet de protéger "**activement**" un réseau contre les différentes attaques.
- Ces solutions sont dites de sécurité active dans la mesure où elles agissent sur les données qui transitent sur le réseau, en décidant de :
  - Laisser passer ces données ou Les bloquer $\Rightarrow\Rightarrow$ Filtrage/Contrôle d'accès.
  - Les chiffrer $\Rightarrow\Rightarrow$ Cryptage.
- La décision à prendre vis à vis d'un paquet de données, par exemple, peut se baser sur un mécanisme d'authentification de l'origine des données ou de leur destination, etc.
- On va classer ces solutions selon les mécanismes sur lesquels elles se basent :
  - Les solutions basées sur le filtrage/contrôle d'accès ;
  - Les solutions basées sur le cryptage ;

Plan de chapitre

1 Introduction

2 Règles élémentaires d'une stratégie de sécurité réseau

3 Solutions pour isoler et protéger un réseau TCP/IP

4 La technique de filtrage

Règles élémentaires d'une stratégie de sécurité réseau

Lors de l'établissement d'une stratégie de sécurité, il faut toujours garder à l'esprit quelques règles afin de se prémunir des erreurs possibles dans le choix de contre-mesures :

- **Simplicité :** plus une stratégie est complexe, plus il est difficile de l'appliquer, de la maintenir dans le temps ou de la faire évoluer ;
- **Variété des protections :** La variété des solutions mises en place pour assurer la sécurité ne doit pas se fonder sur un seul type de logiciel, de pare-feu ou de détection d'intrusion ;
- **Séparation logique et physique des protections de sécurité :** pour ne pas concentrer la sécurité en un seul point. Séparer par exemple le routeur de la passerelle IPSec et du pare-feu.
- **Implémentation en profondeur des mécanismes de sécurité :** la sécurité ne doit jamais reposer sur un seul mécanisme de sécurité. Un imbrication de mécanismes offre une garantie de sécurité supérieure. Pour peu que le premier élément de sécurité vienne à faillir. Un 1^{er} élément peut être des ACL, un 2ème élément authentifie l'accès via IPSec ou SSH, etc . . .
- **Prise en comte de la sécurité dans les nouveaux projets** (extension réseau, implémentations, ...).

Exemples de Stratégies de sécurité réseau

- **Stratégie des périmètres de sécurité :** le réseau est découpé en périmètres de sécurité logique regroupant des entités ou fonctions afin de mettre en place des niveaux de sécurité à la fois imbriqués et séparés ;
- **Stratégie d'authentification en profondeur :** des contrôles d'authentification sont mis en place afin d'authentifier les accès aux périmètres de sécurité ;
- **Stratégie du moindre privilège :** un utilisateur ne dispose que des privilèges dont il a besoin ;
- **Stratégie de confidentialité des flux réseau :** toute communication inter-site transitant sur des réseaux publics est chiffrée si elle contient des données confidentielles ;
- **Stratégie de séparation des pouvoirs :** des entités séparées sont crées, chacune responsable de zones de sécurité spécifiques du réseau ;
- **Stratégie anti-virus :** tout document numérique ou tout autre vecteur de propagation de virus fait l'objet d'un contrôle avant de pénétrer dans un périmètre de sécurité ;
- **Stratégie de contrôle régulier :** l'application de la politique de sécurité est validée par un contrôle de sécurité régulier ;

Plan de chapitre

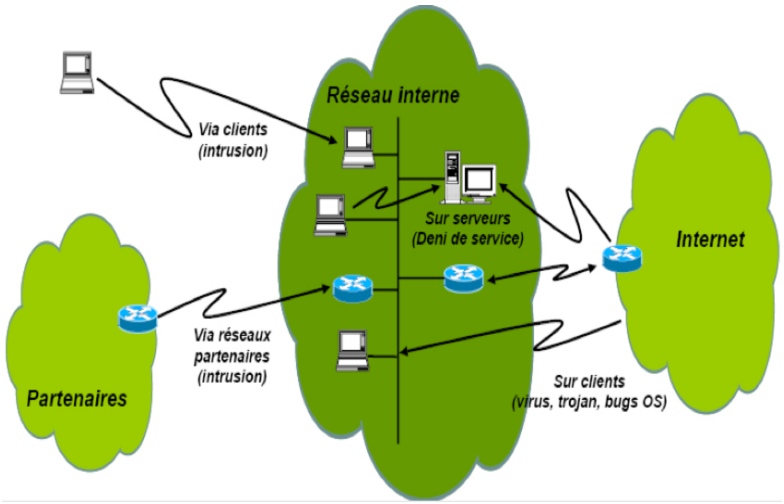
1 Introduction

2 Règles élémentaires d'une stratégie de sécurité réseau

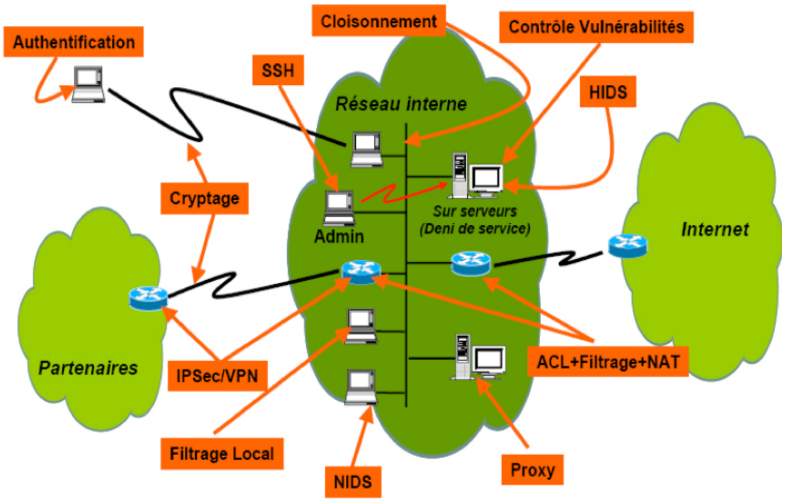
3 Solutions pour isoler et protéger un réseau TCP/IP

4 La technique de filtrage

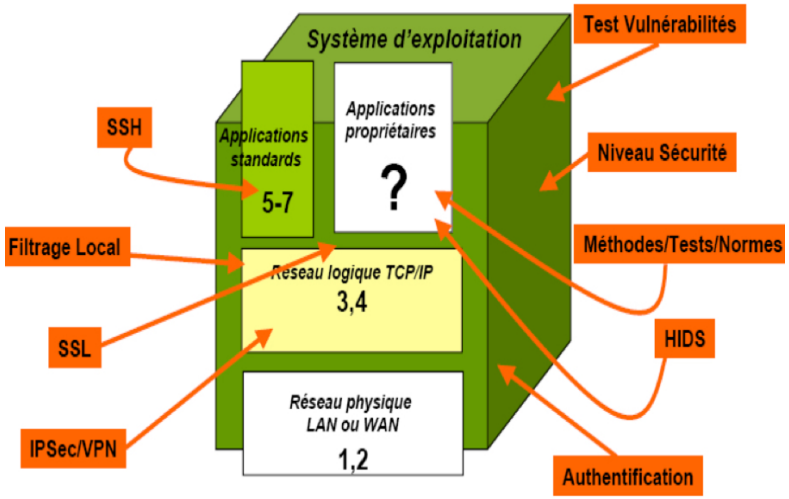
Architecture réseau



Architecture réseau avec éléments de sécurité

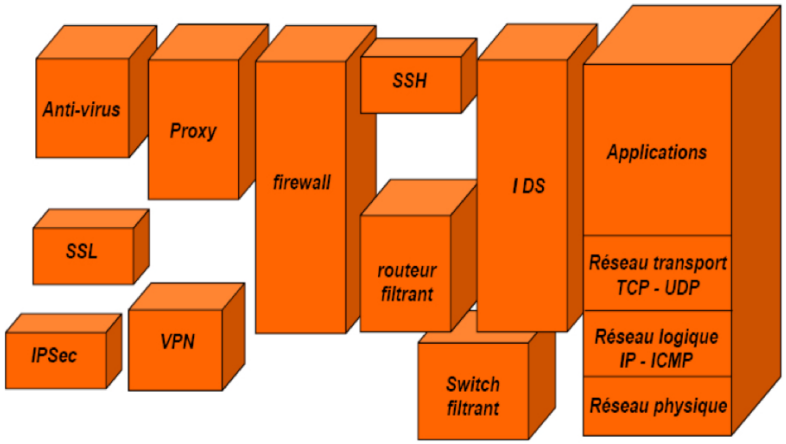


Architecture d'une application en réseau



Éléments de la solution globale

- Diviser pour mieux régner ;
- Dédier pour mieux résister.



Plan de chapitre

1 Introduction

2 Règles élémentaires d'une stratégie de sécurité réseau

3 Solutions pour isoler et protéger un réseau TCP/IP

4 La technique de filtrage

Principes

- C'est lui qui permet de filtrer le trafic de part et d'autre d'un réseau.
- Ce filtrage porte sur les paquets IP.
- Il peut être réalisé par un matériel (exemple : routeur) ou un logiciel de filtrage ou les deux.
- Il est utilisé généralement pour assurer la sécurité d'un réseau vis à vis des réseaux externes auxquels il est connecté, notamment, Internet.
- Il est indépendant des utilisateurs.

Mise en œuvre

A l'entrée du réseau (cas classique)

- **Outils :** routeurs, "firewalls".
- **But :** protéger le réseau des flux venant de l'extérieur (et vice versa).

Sur un serveur

- **Outils :** iptables sur un serveur Unix, etc.
- **But :** contrôler l'accès au serveur lui-même.

Critères de base pour le filtrage

- Adresse IP source ;
- Adresse IP destination ;
- Type du protocole au dessus de IP ;
- Numéro de port source ;
- Numéro de port destination ;
- Port d'entrée ou de sortie physique du filtre (si plus d'un).

Fonctionnement

- **Principe de base :** les paquets interdits de passage sont arrêtés, les paquets autorisés passent ;
- Actions possibles sur les paquets autorisés :
  - Routage vers un autre port que celui mentionné dans le paquet ;
  - Routage vers le port destination mais avec envoi d'une copie vers un autre port ;
  - Application d'une translation d'adresses IP ;
  - Routage vers un tunnel d'encapsulation IP, etc.
- Actions possibles sur les paquets interdits :
  - Suppression ;
  - Journalisation :
    - Sans informer l'émetteur ;
    - En informant l'émetteur avec un message d'erreur.
- **Politique de filtrage :**
  - Les types de paquets autorisés sont listés dans une liste exhaustive, les paquets dont le type est dans la liste passent, les autres sont arrêtés ;
  - Les types de paquets interdits sont listés dans une liste exhaustive, les paquets dont le type n'est pas dans la liste passent, les autres sont arrêtés ;
  - Un ensemble de règles de filtrage qui déterminent les paquets autorisés et ceux interdits.

QUESTIONS ?