MINISTÈRE
DE LA DÉFENSE

Les pare-feux : concepts

Premier Maître Jean Baptiste FAVRE
DCSIM / SDE / SIC / Audit SSI
jean-baptiste.favre@marine.defense.gouv.fr

sersim

C'est quoi un pare-feu ?

- Assure une interconnexion sécurisée de plusieurs réseaux
- Protège une partie d'un réseau du reste
- Permet de mettre en place (et d'appliquer) une politique de sécurité

MINISTÈRE
DE LA DÉFENSE

Au menu

- Les principaux types de pare-feu
  - Filtres de paquets
  - Serveurs « proxies » ou relais applicatifs
  - Serveurs VPN
  - IDS / IPS
- La translation d'adresses
- Le chiffrement
- La journalisation

sersim

MINISTÈRE
DE LA DÉFENSE

Filtre de paquets

- Agit aux niveaux 3 et 4 (IP et TCP)
- Permet de masquer les machines internes (« IP masquerading »)
- Assure le suivi des paquets (« statefull inspection »)
  - Permet de ne prendre en compte que le premier paquet d'une connexion TCP (SYN)
  - Gère les connexions « en relation » (reste d'une connexion TCP ou session FTP par exemple)

sersim

MINISTÈRE
DE LA DÉFENSE

Serveurs « proxies »

- Agit aux niveaux applicatifs entre les clients et les serveurs
- Effectue les connexions clients à leur places
- Inspecte les requêtes à la recherche de motifs interdits (pattern matching)
- Permet de « greffer » des examens externes (anti-virus) de façon transparente pour le client
- Ralentissement du trafic (relatif)
- Il faut un serveur par protocole applicatif

sersim

MINISTÈRE
DE LA DÉFENSE

Serveur VPN

- Permet de raccorder 2 réseaux physiquement distants au travers d'un réseau non sûr
- Permet de donner un accès transparent aux ressources du réseau interne à une ou des machines au travers d'un réseau non sûr
- Doit garantir:
  - L'authentification des interlocuteurs
  - La confidentialité par le chiffrement de paquets
  - L'intégrité par la signature de paquets
  - L'anti-rejeu de paquets

sersim

IDS / IPS: un effet de mode ?

- Intrusion Detection Systems
  - Détecte une intrusion
  - Fonctionne principalement par « pattern matching »
  - Fonctionne en mode réactif (comme les anti-virus)
- Intrusion Prevention Systems
  - Affirme pouvoir empêcher une intrusion en « s'adaptant »
  - Dans l'idéal, n'a pas besoin de mises à jour.
  - Encore peu répandu

MINISTÈRE
DE LA DÉFENSE

La translation d'adresses

- Permet de masquer le plan d'adressage interne
- Autorise plusieurs machines en IP « privées » (RFC 1918) à accéder à Internet par une seule IP « publique »
- Empêche les connexions entrantes depuis Internet vers un client en RFC 1918 (non routable sur internet)
- Peut être statique (1:1) ou dynamique (1:n)

sersim

La translation d'adresses statique

- A une adresse officielle (celle du pare-feu), on fait correspondre une seule adresse (celle du serveur)
- Utilisation:
  - Serveurs devant être accessibles depuis Internet (Site web, mail, DNS, ...)

MINISTÈRE
DE LA DÉFENSE

La translation d'adresses dynamique

- A toute adresse interne, on fait correspondre 1 seule adresse officielle (celle du pare-feu)
- Utilisation
  - Accès des clients à Internet
- Avantages
  - Économie d'adresses IP Internet
- Inconvénients
  - Difficulté avec certains protocoles à négociation de port (ftp, H323, ...)

Chiffrement / Signature

- Couche IP: IPSEC
- Couche Application: SSL, SSH, ...
- Avantages:
  - Authentification de l'émetteur et/ou du destinataire du paquet
  - Assure l'intégrité et la confidentialité de la communication
- Inconvénients:
  - Quand c'est chiffré, on ne voit RIEN !
  - Peut être problématique avec la translation d'adresses (IPSEC)

MINISTÈRE
DE LA DÉFENSE

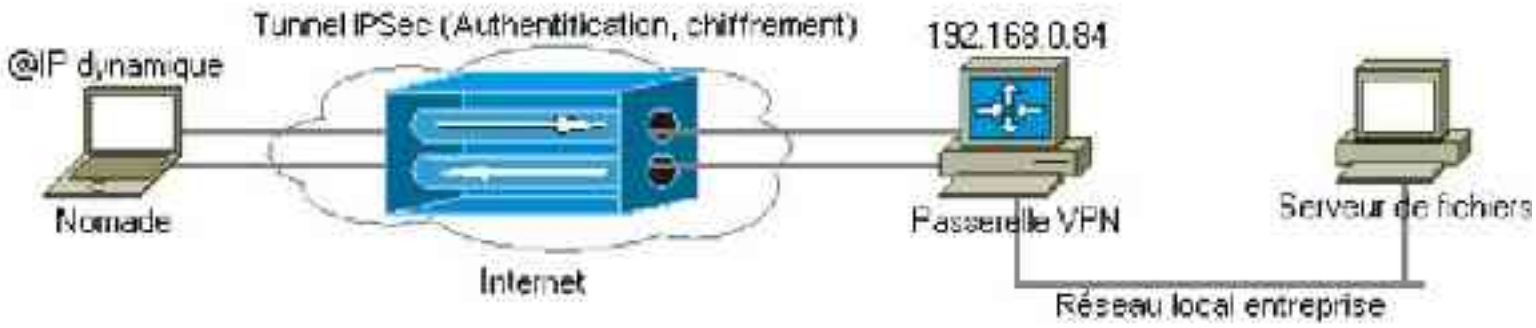
Le chiffrement IP: IPSEC

- 3 protocoles
  - AH (Authentication Header)
    - Authentification, anti-rejeu
  - ESP (Encapsulated Security Payload)
    - Chiffrement, authentification, anti-rejeu
  - ISAKMP (Internet Security and Key Management protocol)
- 2 modes
  - Transport (accès nomade, accès sécurisé au sein d'un réseau)
  - Tunnel (VPN entre 2 réseaux distants)

sersim

Le chiffrement IP: IPSEC Transport

- Mode transport
  - Utilisé pour offrir un accès distant sécurisé aux nomades via un réseau non sûr (Internet)
  - Connexion point-à-point non-permanente
  - NAT délicate



Ipsec en mode transport

Le chiffrement IP: IPSEC

Mode Tunnel

- Utilisé pour relier 2 réseaux distants au travers d'un réseau non sûr.
- En général, connexion permanente
- Le passage par le réseau non sûr est transparent
- Plus de soucis de NAT

Ipsec en mode tunnel

Le chiffrement applicatif: SSL

Avantages

- Permet de relier 2 réseaux ou permettre un accès distant à une ou plusieurs machines (nomades).
- Très facile à mettre en place, en tout cas plus facile qu'IPSEC
- Bénéficie de l'existence éventuelle d'une IGC

Inconvénients

- Pas d'authentification au niveau de la couche Internet
- Sensible aux attaques visant les couches Internet et Transport

MINISTÈRE
DE LA DÉFENSE

L'administration en questions

- Techniques
  - Centralisée (à distance) ou « par machine »
    - Prise en compte de différents pare-feux (règles au format propriétaire)
    - Format propriétaire des logs (cf. journalisation)
    - Cohérence des règles
- Organisationnelle
  - Que dit la politique de sécurité ?
  - Qui modifie la politique de filtrage ?
  - On teste, ou on ne teste pas ? (et qui le fait ?)
  - Qui coupe tout ?
  - Réactions en cas d'attaque ?

sersim

MINISTÈRE
DE LA DÉFENSE

La journalisation

- Doit permettre d'assurer un suivi du niveau de sécurité de l'architecture de sécurité
  - Peut-être plus important que toutes les fonctionnalités possibles d'un pare-feu...
  - ... Mais souvent le parent pauvre
- Enregistrer les échecs... et les succès ?
- Centraliser pour faciliter l'analyse
- Format souvent propriétaires
- Outils d'analyse et de corrélation avec d'autres équipements (IDS, Serveurs, ...)

sersim

MINISTÈRE
DE LA DÉFENSE

Pare-feu: Concepts

- Beaucoup d'équipements plus ou moins utiles
- Dépend essentiellement du niveau de maturité SSI
  - Filtres de paquets
  - Proxy / Relais applicatifs
  - IDS / IPS
- Ne se met pas en place n'importe comment (Architecture)
- Il faut l'administrer. (ce n'est pas un « pose et oublie »)

sersim

Pare-feu: Concepts

Questions ?