ADMINISTRATION ET SÉCURITÉ DES RÉSEAUX

UE 42 - **M4210C**

Infrastructures de sécurité

2ème semestre 2015/2016

(CM:6h /TD:6h /TP:18h)

Xavier NICOLAY – IGR au LIM –

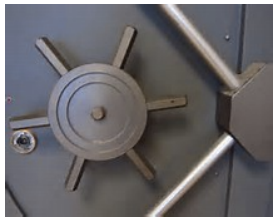
Administration et sécurité des réseaux

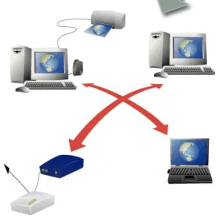
OBJECTIF :

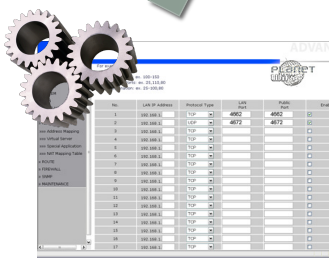
Connaissance du domaine de la sécurité des réseaux

Administration et sécurité des réseaux

Compétences visées







Administration et sécurité des réseaux

Notion de règlement de sécurité, d'audit, de vulnérabilité et de détection d'intrusion

Sécurité des Systèmes d'Informations

Administration et sécurité des réseaux

Notion de règlement de sécurité, d'audit, de vulnérabilité et de détection d'intrusion

Sécurité des Systèmes d'Informations

a. Les Attentes

Administration et sécurité des réseaux

Notion de règlement de sécurité, d'audit, de vulnérabilité et de détection d'intrusion

Sécurité des Systèmes d'Informations

a. Les Attentes
b. Les Attentes Secondaires

Administration et sécurité des réseaux

Notion de règlement de sécurité, d'audit, de vulnérabilité et de détection d'intrusion

Sécurité des Systèmes d'Informations

a. Les Attentes
b. Les Attentes Secondaires
c. Démarche Générale

Administration et sécurité des réseaux

Notion de règlement de sécurité, d'audit, de vulnérabilité et de détection d'intrusion

Sécurité des Systèmes d'Informations

a. Les Attentes
b. Les Attentes Secondaires
c. Démarche Générale
d. Conséquences

Administration et sécurité des réseaux

Notion de règlement de sécurité, d'audit, de vulnérabilité et de détection d'intrusion

Sécurité des Systèmes d'Informations

a. Les Attentes
b. Les Attentes Secondaires
c. Démarche Générale
d. Conséquences
e. Périmètre

Administration et sécurité des réseaux

Notion de règlement de sécurité, d'audit, de vulnérabilité et de détection d'intrusion

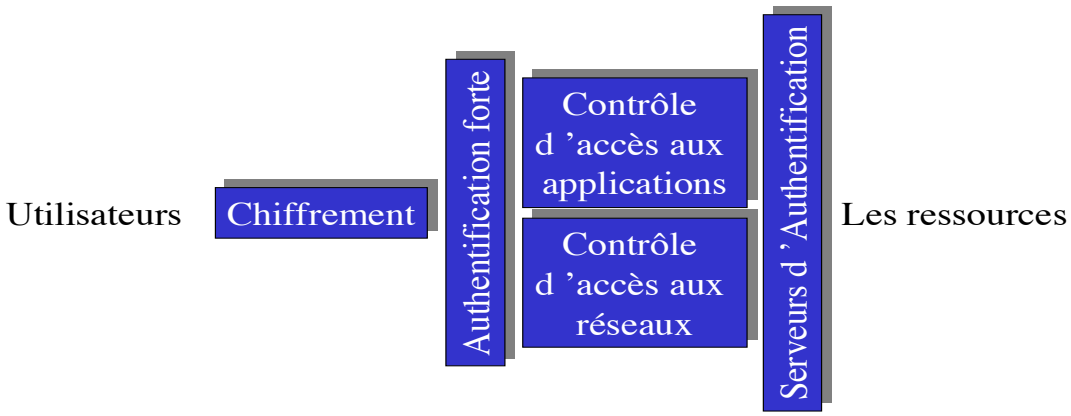
Sécurité des Systèmes d'Informations

a. Les Attentes
b. Les Attentes Secondaires
c. Démarche Générale
d. Conséquences
e. Périmètre
f. RAPPEL

Administration et sécurité des réseaux

Notion de règlement de sécurité, d'audit, de vulnérabilité et de détection d'intrusion

La chaîne de sécurité applicative par fonction

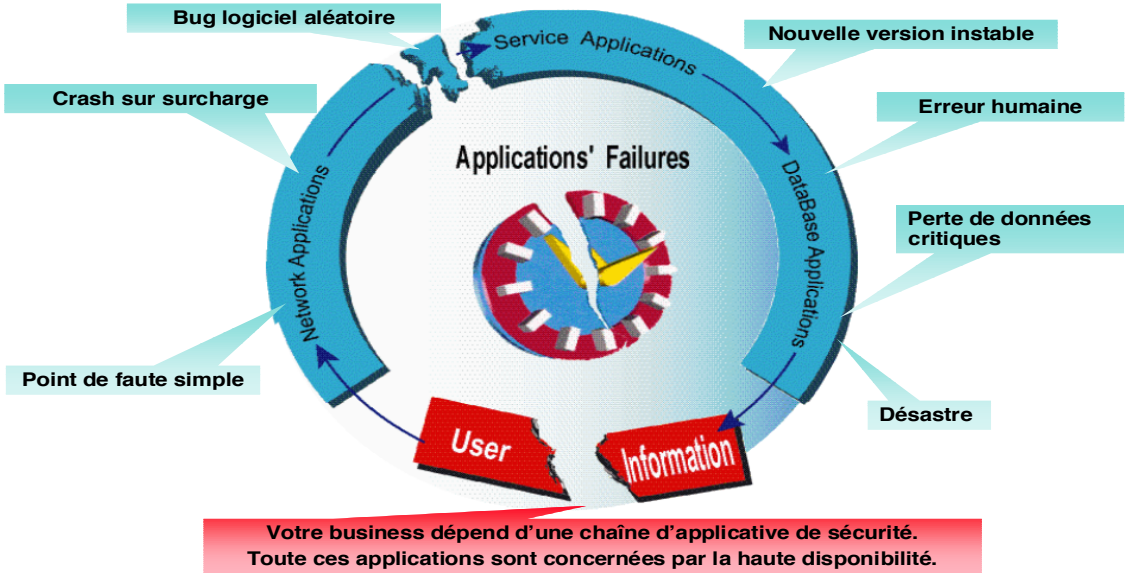


Si un maillon se brise, c'est toute la chaine qui se brise !

Administration et sécurité des réseaux

Notion de règlement de sécurité, d'audit, de vulnérabilité et de détection d'intrusion

Une chaîne d'applications de sécurité



Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique

Administration et sécurité des réseaux

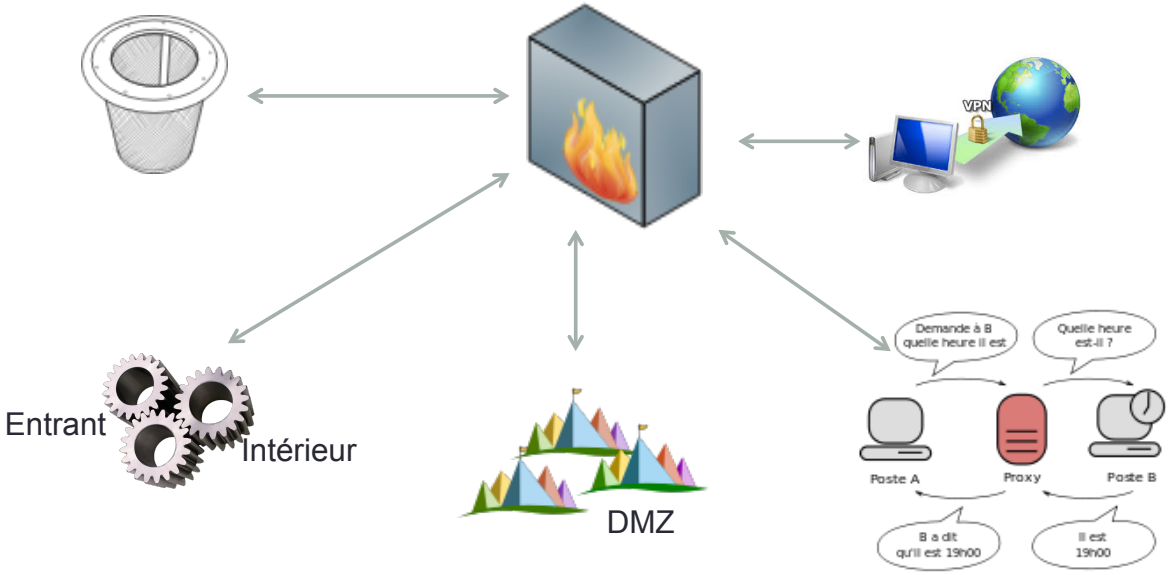
Les équipements dédiés à la sécurité informatique

- Les Firewalls
- VPN
- IDS / IPS
- Matériels dédiés à l'Authentification
  - Biométrique
  - Clés type RSA ou OTP
  - Annuaires (AD / LDAP, …)
  - Radius

Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Les Firewalls –

Le firewall

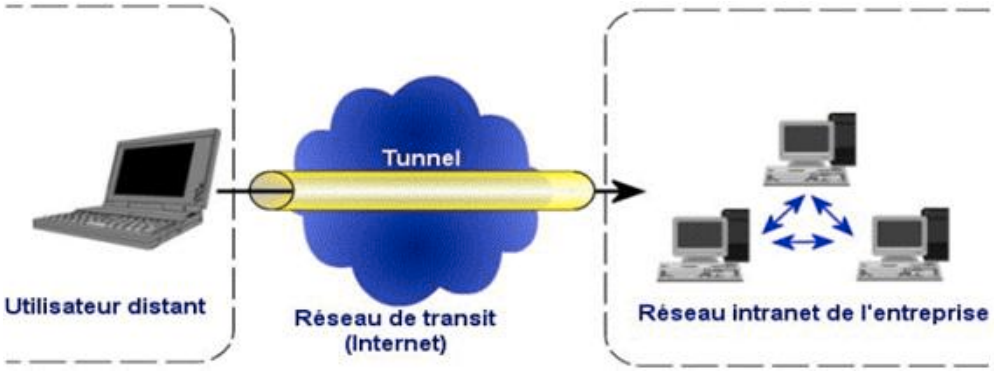


Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Les VPNs –

Les VPNs

Host to Site

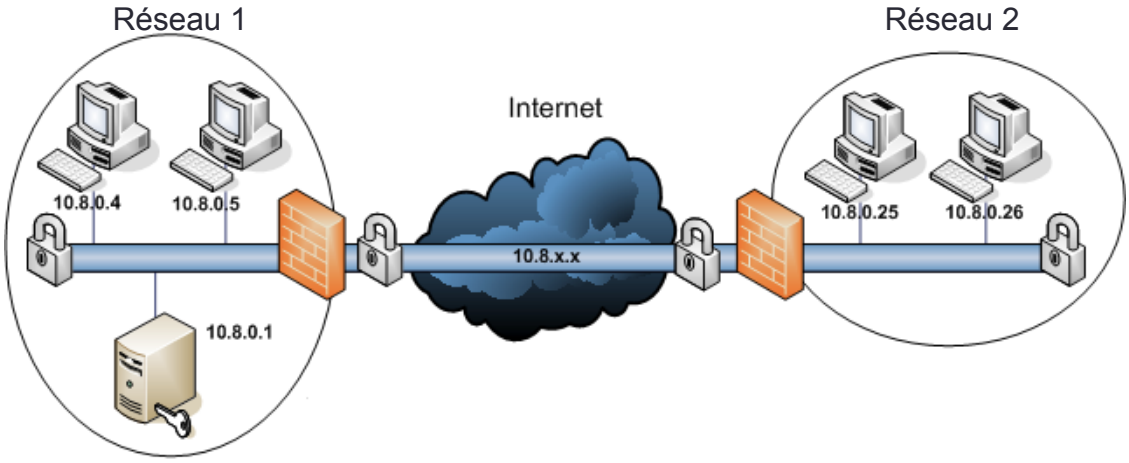


Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Les VPNs –

Les VPNs

Site to Site

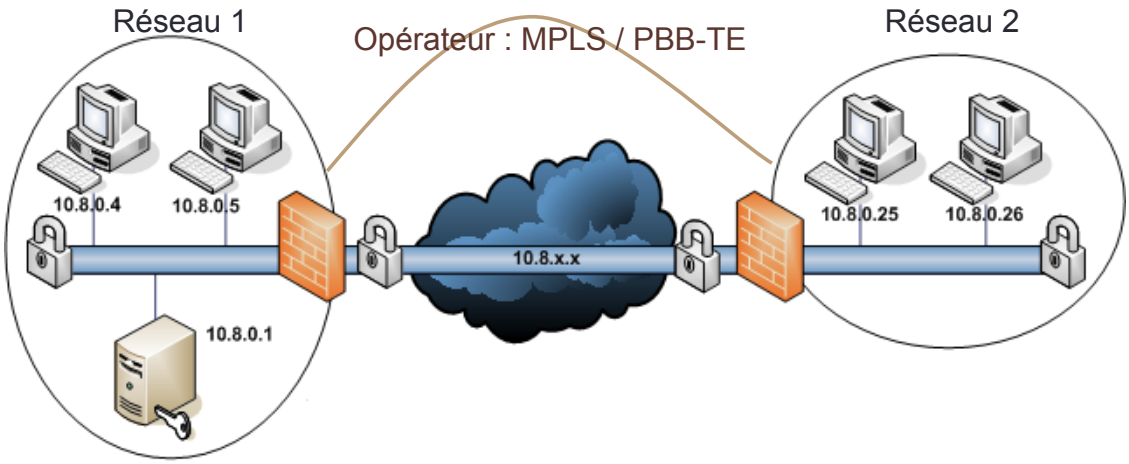


Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Les VPNs –

Les VPNs Opérateur

Site to Site

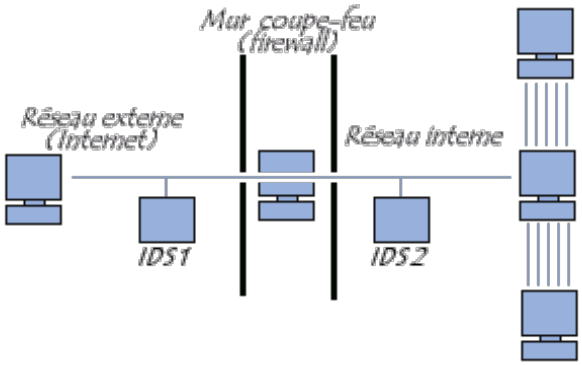


Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – IDS –

IDS (Intrusion Detection System)

N-IDS vs H-IDS



Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – IDS –

IDS (Intrusion Detection System)

Vérifications :

- Vérification de la pile protocolaire
- Vérification des protocoles applicatifs
- Reconnaissance des attaques par "Pattern Matching"

Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – IDS –

IDS (Intrusion Detection System)

Actions !

- Reconfiguration d'équipement tierces (firewall, ACL sur routeurs)
- Envoi d'une trap SNMP à un hyperviseur tierce
- Envoi d'un e-mail à un ou plusieurs utilisateurs
- Journalisation (log) de l'attaque
- Sauvegarde des paquets suspicieux
- Démarrage d'une application
- Envoi d'un "ResetKill »
- Notification visuelle de l'alerte

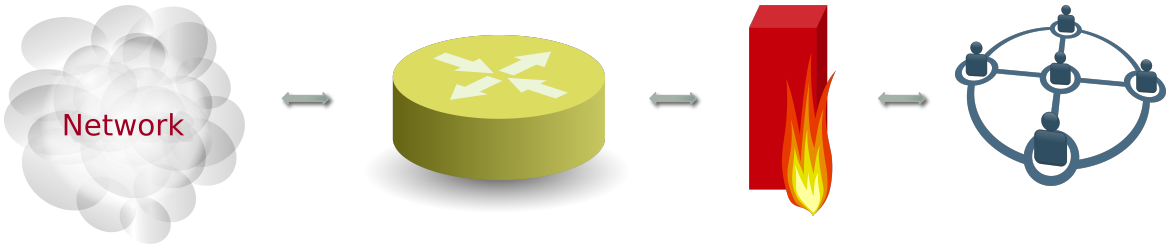
Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – IDS / IPS –

IDS vs IPS

IPS: Intrusion Prevention System

Positionnement



Internet Routeur Firewall LAN

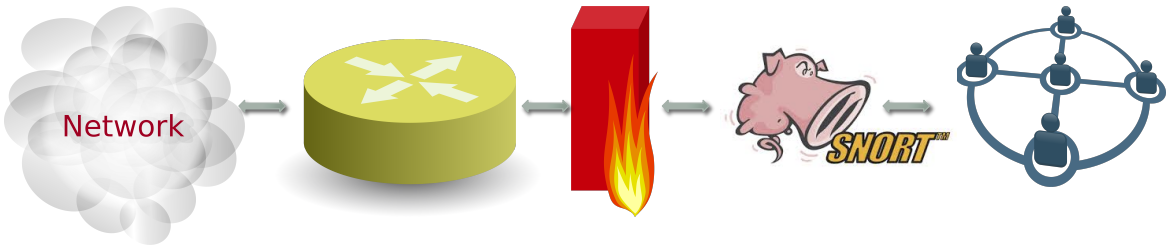
Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – IPS –

IPS

IPS: Intrusion Prevention System

Positionnement



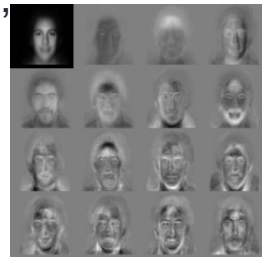
Internet Routeur Firewall IPS LAN

Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Matériels Biométriques –

Biométrique : mesure du vivant

- Les empreintes digitales,
- L'iris / les réseaux veineux de la rétine,
- Reconnaissance de visage,
- Reconnaissance vocale,
- La dynamique des signatures,
- La dynamique des frappes au clavier,

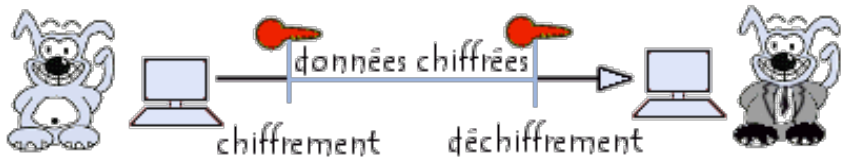


Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Chiffrement –

Chiffrement symétrique

```
Message clair : wikipedia
Mot clé : crypto
Message chiffre : yzixisfzy
```

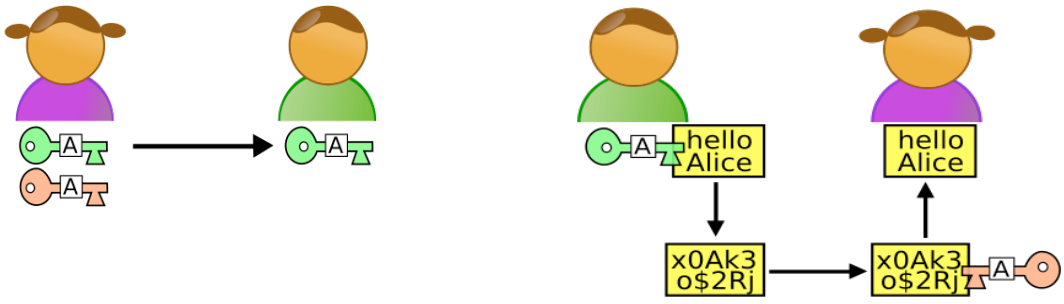


Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Chiffrement –

Chiffrement asymétrique (1976)

Clé privée vs Clé publique



Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Chiffrement –

Chiffrement asymétrique

Soit P et Q, ces **deux nombres premiers**
On pose : $N=P\times Q$ **et** $M=(P-1)\times(Q-1)$.

choisir un nombre C, qui soit premier avec M.
La clé publique est composée de (N, C).

Etienne Bezout : {a,b} premier ssi il existe u & v (entiers)
tels que $a\times u+b\times v=1$

$C\times U+M\times V=1$ ➔ Clef privée : (U,N)

Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Chiffrement –

Chiffrement asymétrique (N= 5141, C = 7)

Le modulo !!!

$B \Leftrightarrow 66 \Rightarrow 66^7 mod(5141) = 386$
$o \Leftrightarrow 111 \Rightarrow 111^7 mod(5141 = 1858$
$n \Leftrightarrow 110 \Rightarrow 110^7 mod(5141) = 2127$
$j \Leftrightarrow 106 \Rightarrow 106^7 mod(5141) = 2809$
$o \Leftrightarrow 111 \Rightarrow 111^7 mod(5141) = 1858$
$u \Leftrightarrow 117 \Rightarrow 117^7 mod(5141) = 1774$
$r \Leftrightarrow 114 \Rightarrow 114^7 mod(5141) = 737$

$f(x)=x^C mod(N)$

Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Chiffrement –

Décodage asymétrique (U = 4279, N = 5141)

$$386 \Rightarrow 386^{4279} \Rightarrow (386^{4279}) mod(5141) = 66 \quad \Leftrightarrow B$$
$$737 \Rightarrow 737^{4279} \Rightarrow (737^{4279}) mod(5141) = 114 \quad \Leftrightarrow r$$
$$970 \Rightarrow 970^{4279} \Rightarrow (970^{4279}) mod(5141) = 97 \quad \Leftrightarrow a$$
$$204 \Rightarrow 204^{4279} \Rightarrow (204^{4279}) mod(5141) = 118 \quad \Leftrightarrow v$$
$$1858 \Rightarrow 1858^{4279} \Rightarrow (1858^{4279}) mod(5141) = 111 \quad \Leftrightarrow o$$

$$f(x) = x^{U} mod(N)$$

Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Chiffrement –

Clé OTP

secret partagé unique

Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Chiffrement –

Clé RSA SecurID

Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Authentification : Annuaires –

Active Directory

UO (OU) : Unit Organisation
ACL

SAM : Security Account Manager

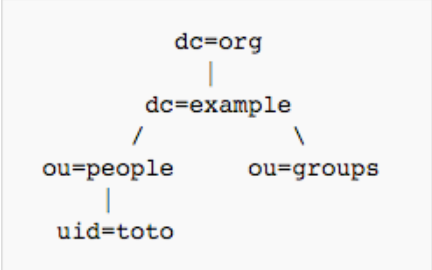
Kerberos, Samba

Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Authentification : Annuaires –

LDAP

Service TCP-IP
! Protocole
Dernière version : v3 (cf RFC4510)



Objectif : interagir avec les Annuaires X500

Arborescent
« Format d'échange »: LDIF

```
dn: cn=John Doe,dc=example,dc=org
cn: John Doe
givenName: John
sn: Doe
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```


Administration et sécurité des réseaux

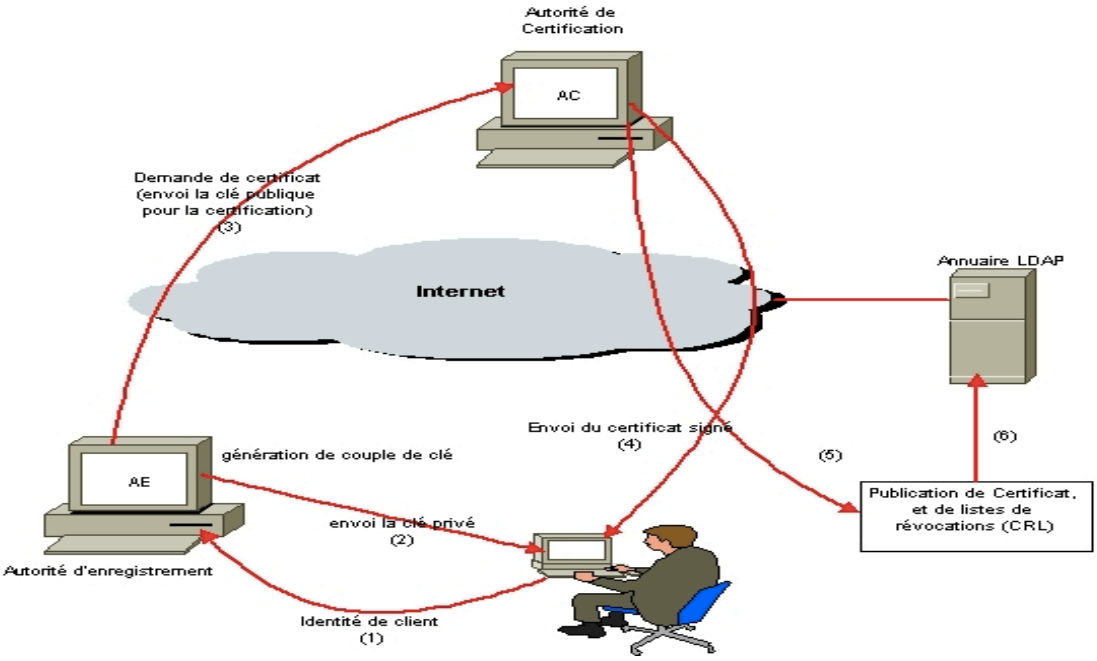
Les équipements dédiés à la sécurité informatique – PKI & Certificats –

La PKI

Gestion des clefs publiques (en volume)
→fiabilité
=> Confidentialité
=> Authentification
=> L'intégrité
=> non-répudiation

Administration et sécurité des réseaux

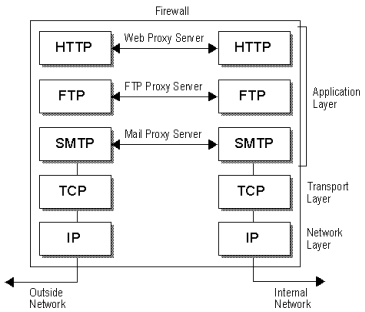
Les équipements dédiés à la sécurité informatique – PKI & Certificats –



Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Approfondissement –

Proxy-Firewall



NAT (rfc1918)(rfc1631)

NAT statique vs dynamique

ACL : *Access Control List*

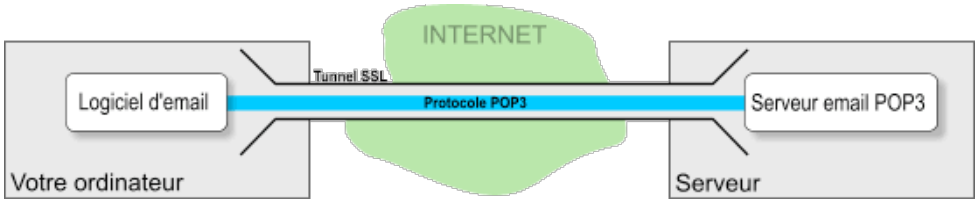
Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – ssl, https, …–

SSL = Secure Socket Layer (rfc 6101)

Confidentialité
Intégrité
Authentification

Les utilisations de SSL:
HTTPS, SSH, FTPS, POPS, IMAPS, SMTPS...



Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – ssl, https, …–

SSL = Secure Socket Layer

modèle OSI	pile de protocoles
7 - couche application	HTTP, SMTP, FTP, SSH, IRC, SNMP, SIP ...
6 - couche de présentation	
5 - couche de session	TLS, SSL,SSH-user, NetBIOS
4 - couche de transport	TLS, SSL,TCP, UDP, SCTP, RTP, DCCP ...
3 - couche réseau	IPv4, IPv6, ARP, IPX ...
2 - couche de liaison	Ethernet, 802.11 WiFi, Token ring, FDDI, ...
1 - couche physique	Câble, fibre optique, ondes radio...

Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – RADIUS –

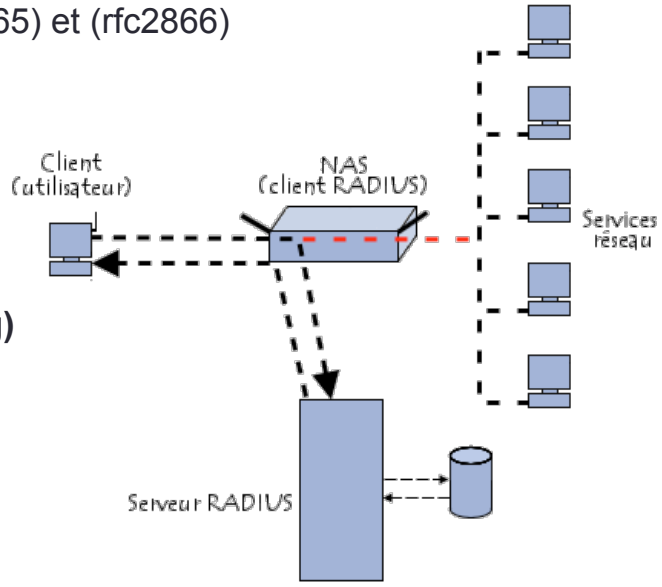
Remote Authentication Dial-In User Service

(rfc2865) et (rfc2866)

Autorisation

Et

Comptabilisation (accounting)



Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Diameter–

(rfc3588)

Successeur de RADIUS

- utilise TCP ou SCTP
- peut utiliser IPSec ou TLS
- utilise des attributs sur 32 bits au lieu de 8 (déjà présents dans certaines extensions EAP de RADIUS, notamment TTLS)
- a des mécanismes d'appel du client par le serveur

Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Déontologie–

– **Éthique** : vie privée, liberté de l'individu, bonne gouvernance: commerce et échange entreprise, démocratie : république numérique
– **Législation** : lois sur la cryptographie, autorisations, droits des sujets, droit d'utiliser un service, une application, propriété intellectuelle, gestion des droits de distribution des oeuvres
– **Réglementation** : Contrôle et filtrage de contenus (contenus illicites)
– **Technique** : Mathématique, traitement du signal, informatique, électronique, Ingénierie des réseaux & des architectures de systèmes
– **Méthodologie**: ITSEC, Critères Communs (CC)
– **Normes** : Standards cryptographiques (AES), protocoles (IPSec, ...), ..

Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Déontologie–

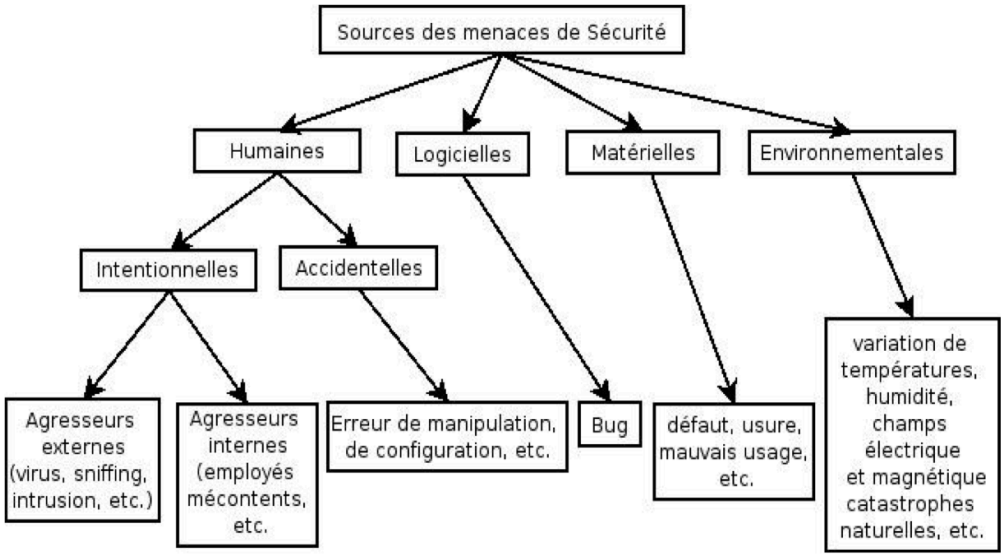
"Ce ne sont pas les murs qui protègent la citadelle, mais l'esprit de ses habitants"

Thudycite

Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Sources des menaces –

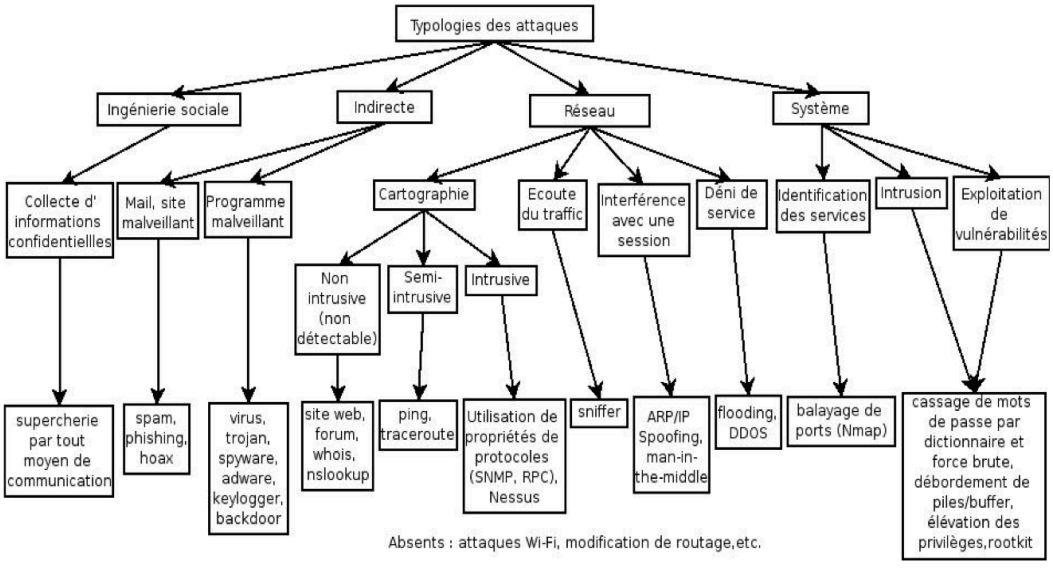
Typologie



Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Sources des attaques–

Typologie



Absents : attaques Wi-Fi, modification de routage,etc.

Administration et sécurité des réseaux

Les équipements dédiés à la sécurité informatique – Veille–

Quelques sites :

CERT: Computer Emergency Response Team
www.certa.ssi.gouv.fr

Hakin9 (revue): www.hakin9.org

Outils: sectools.org

Mailing Lists: seclists.org

Etc..