e-Xpert Solutions SA | 29, route de Pré-Marais | CH 1233 Bernex-Genève | Tél +41 22 727 05 55 | Fax +41 22 727 05 50

La citadelle électronique
Sécurité contre l'intrusion informatique
volume 2

Sylvain Maret / version 1.1

Octobre 2002

“ L’art de fortifier ne consiste pas dans des règles et des systèmes mais uniquement dans le bon sens et l’expérience ”

Sebastien le Prestre de Vauban
Ingénieur Architecte 1633-1707

Agenda

- La citadelle électronique
- Les firewalls
- Les proxy
- Contrôle d'URL
- Contrôle de contenu
- Anti Virus
- Web application firewall
- IDS
- FIA

Agenda

- Honeypot
- VPN
  - IPSEC
  - SSL
  - SSH
- Cartes à puce
- Sécurisation des serveurs
- Sécurisation des postes de travail

Agenda

- Analyse comportementale
- S/Mime
- Technologie PKI
- Systèmes d’authentification

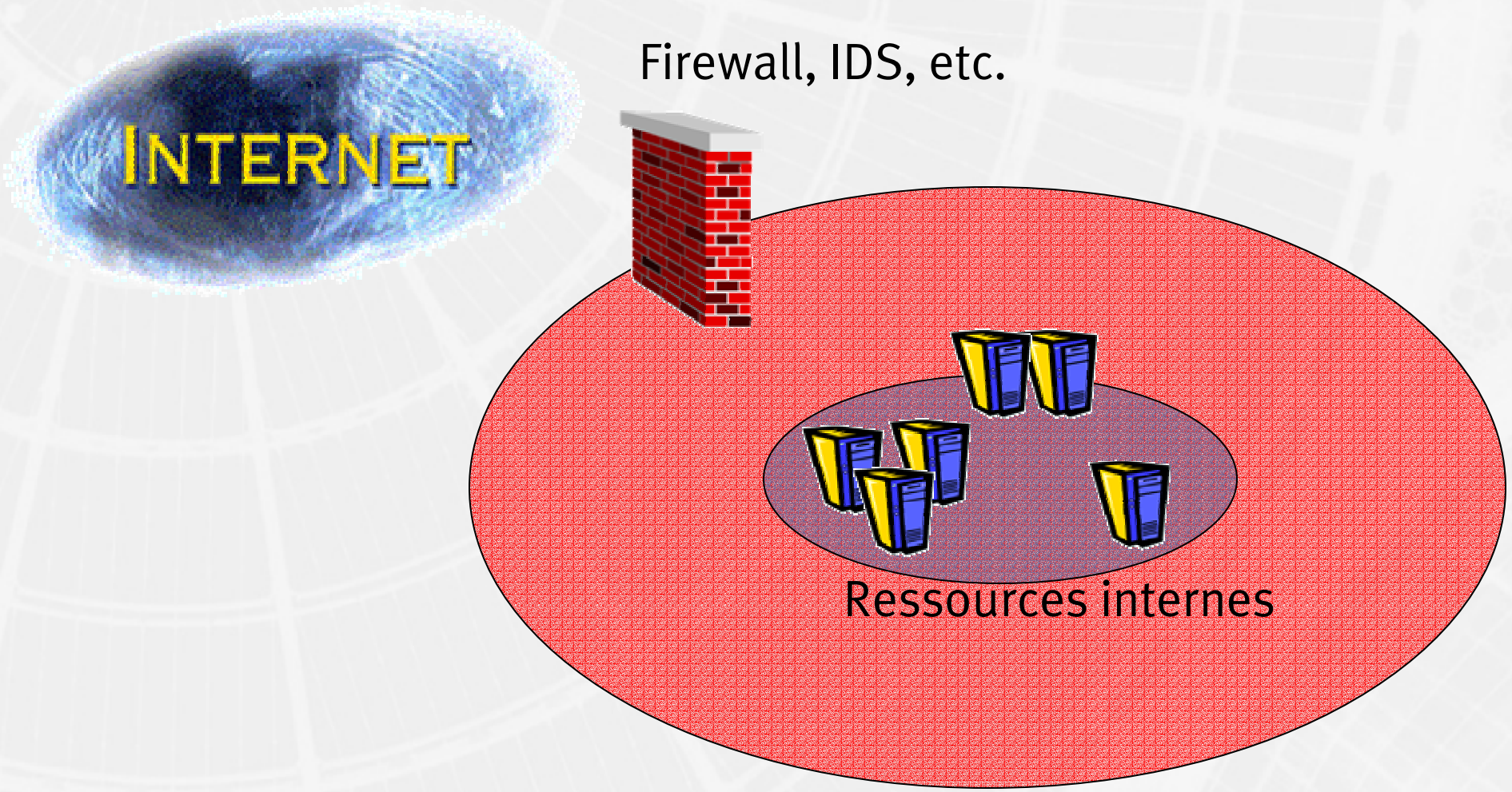
Modèle de sécurité classique

- Approches « produit » et périmètre
- Des solutions spécifiques, des cellules isolées
  - Firewall
  - Antivirus
  - VPN
  - Contrôle de contenu
  - Systèmes de détection d'intrusion
  - Authentification périphérique

Les inconvénients du modèle classique

- Des solutions très spécifiques
- Un manque de cohérence et de cohésion
- L'approche en coquille d'œuf
  - Des remparts
  - Des applications (le noyau) vulnérables

- Schématiquement…



Les enjeux pour le futur

- Fortifier le cœur des infrastructures
  - Principalement les applications
- Améliorer la cohérence
- Simplicité d'utilisation
- Définir une norme suivie par les constructeurs & éditeurs
- Amener la confiance dans les transactions électroniques

La citadelle électronique

- Modèle de sécurité émergent
- Approche en couches ou en strates
- Chaque couche hérite du niveau inférieur
- Les applications et les biens gravitent autour d'un noyau de sécurité

- Approche en couche

- 1) Architecture
- 2) Protocoles réseaux
- 3) Systèmes d'exploitations
- 4) Applications

Architecture

- Sécurisation des accès bâtiments
- Segmentation & Cloisonnement IP
- Segmentation & Cloisonnement physique
- Choix d'environnement (Switch, hub, etc)
- Mise en place de Firewall
- Configuration de routeur (ACL)
- Disponibilité
- Etc.

Protocoles réseaux

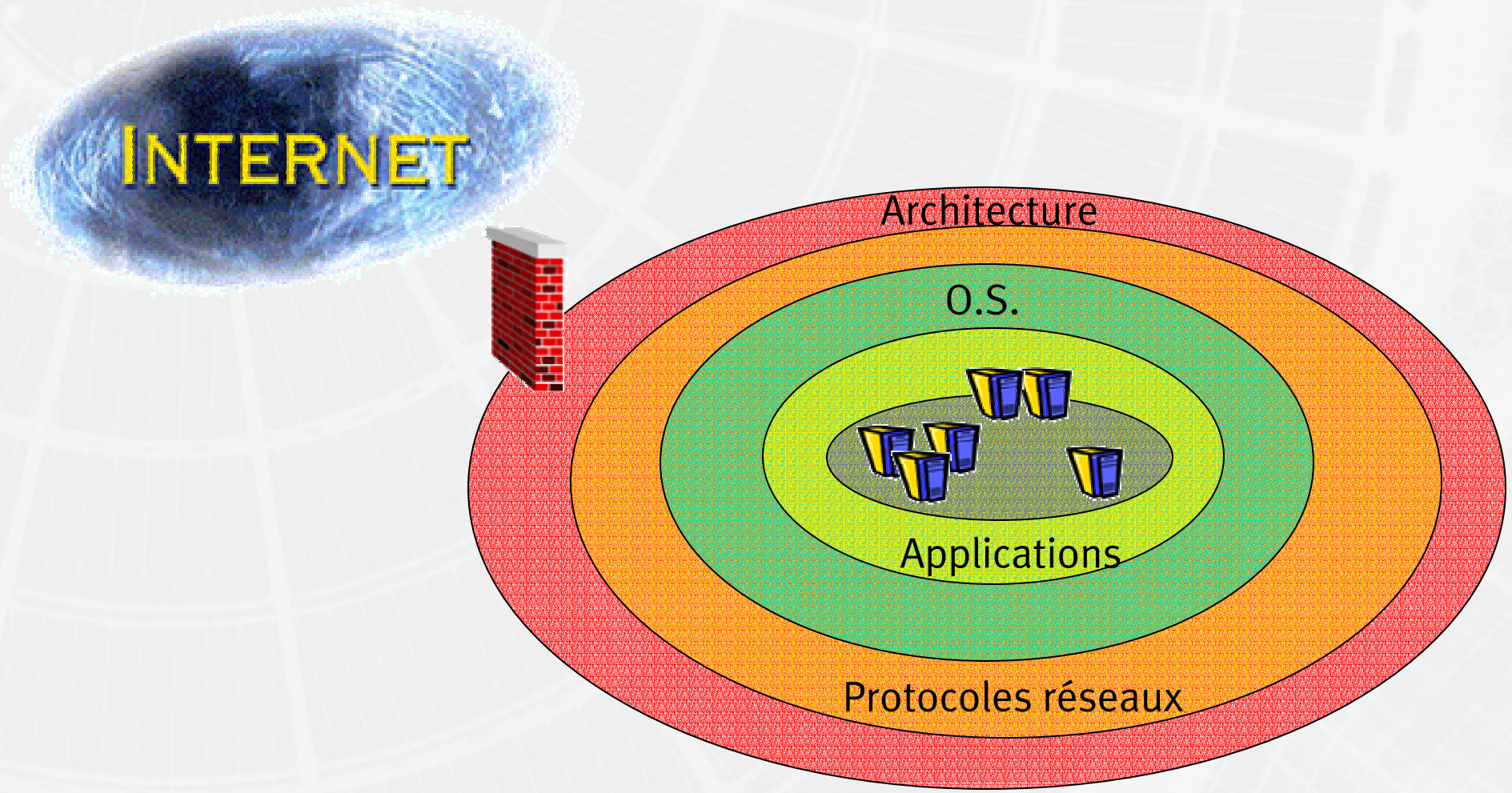
- TCP/IP, IPSec, L2TP, PPTP, etc.
- Anti SYNFlooding
- Anti spoofing
- « Kernel » réseau à sécuriser
- DoS, DDoS
- Architecture réseaux (routeurs et switchs)
- Etc.

Systèmes d'exploitation

- Sécurisation des OS
- Restriction des services
- Mise en place de FIA
- Détection d'intrusions sur les OS
- Analyse comportementale
- Authentification forte
- Sécurisation de l'administration
- Sauvegarde régulière
- Logging & Monitoring

- Chaque application est sécurisée
  - BoF
  - Contrôle de qualité du code
- Cryptage des données sensibles
  - DB, Cartes de crédits
  - Base d'utilisateurs
  - Etc.
- Authentification forte des accès
- Signature électronique
- Etc.

- Schématiquement…



- Pour répondre à ce challenge ?

- Une démarche
  - La politique de sécurité
- Des services de sécurité
  - Authentification
  - Confidentialité
  - Intégrité
  - Non répudiation
  - Autorisation
  - Disponibilité

- Et des technologies…

- Firewalls
- IDS
- Analyse de contenu
- FIA
- AntiVirus
- VPN
- Systèmes d’authentifications
- PKI…

e-Xpert Solutions SA | 29, route de Pré-Marais | CH 1233 Bernex-Genève | Tél +41 22 727 05 55 | Fax +41 22 727 05 50

Les outils de sécurité

Sécurité contre l'intrusion informatique
La citadelle électronique

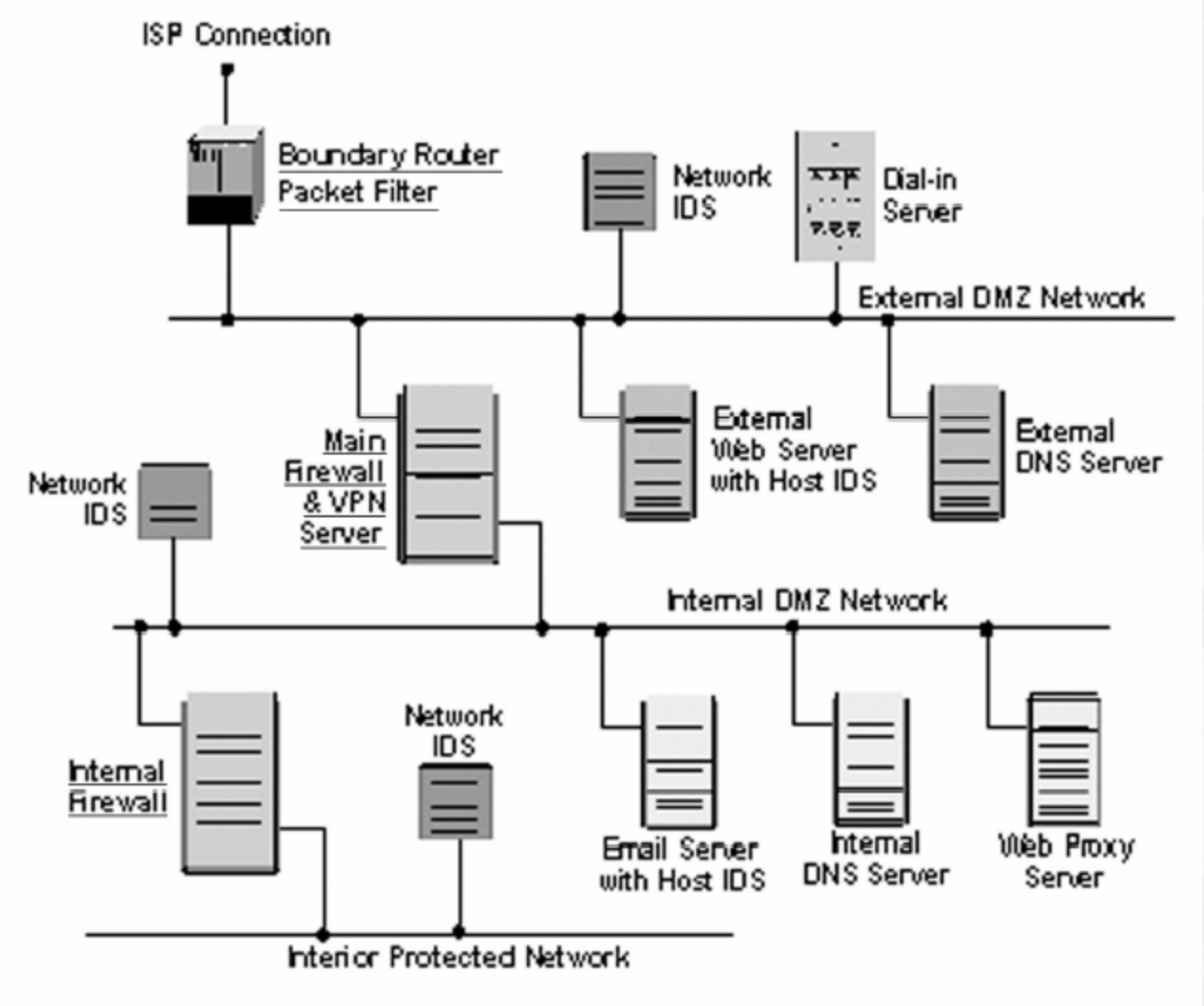
info@e-xpertsolutions.com | www.e-xpertsolutions.com

- Outil de contrôle des communications réseaux
  - Agit comme un filtre
  - Contrôle en temps réel les communications
- Trois grandes familles
  - Proxy ou relais applicatifs (niveau 7)
  - Packet Filter (niveau 3)
  - Stateful Inspection (niveau 3)
- Outil de base de la sécurité…
  - N'est plus suffisant !

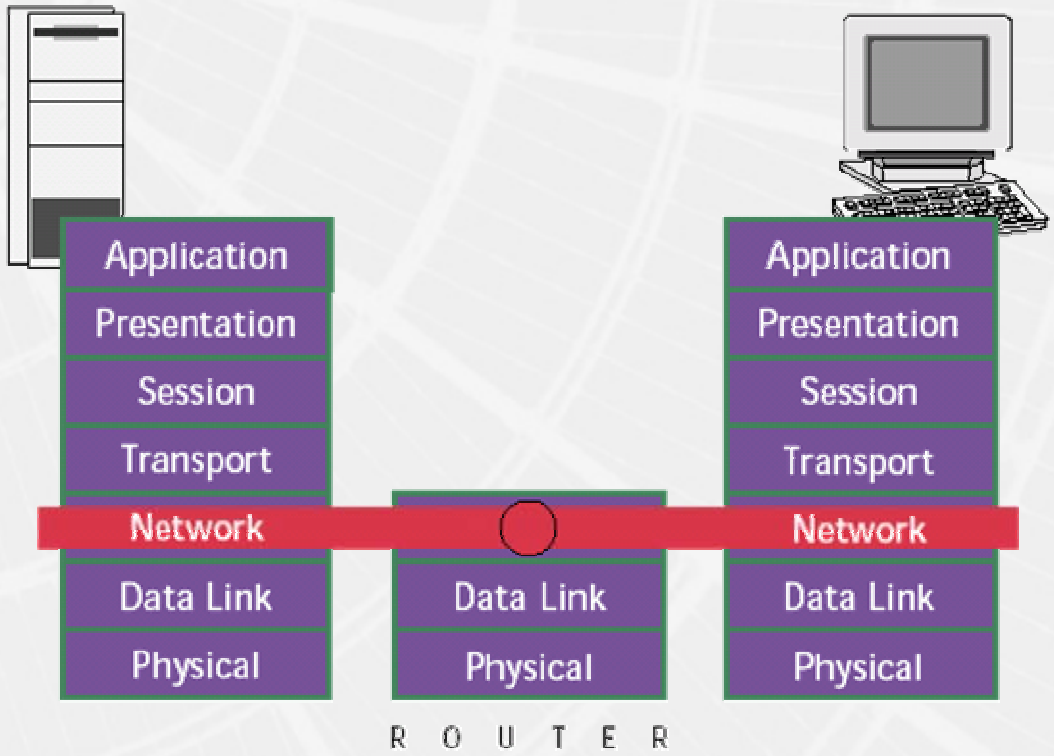
Les firewalls

- Les services standards du firewall
  - Contrôle d'accès
  - Accounting
  - Authentification
  - Translation d'adresse (NAT)
- Les autres services
  - VPN
  - IDS
  - Authentification
  - Contrôle de contenu (AV, filtrage d'URL, Code mobile, etc.)
  - Haute disponibilité
  - Etc.

- Exemple d'implémentation



- Firewall « packet filter »



PROS

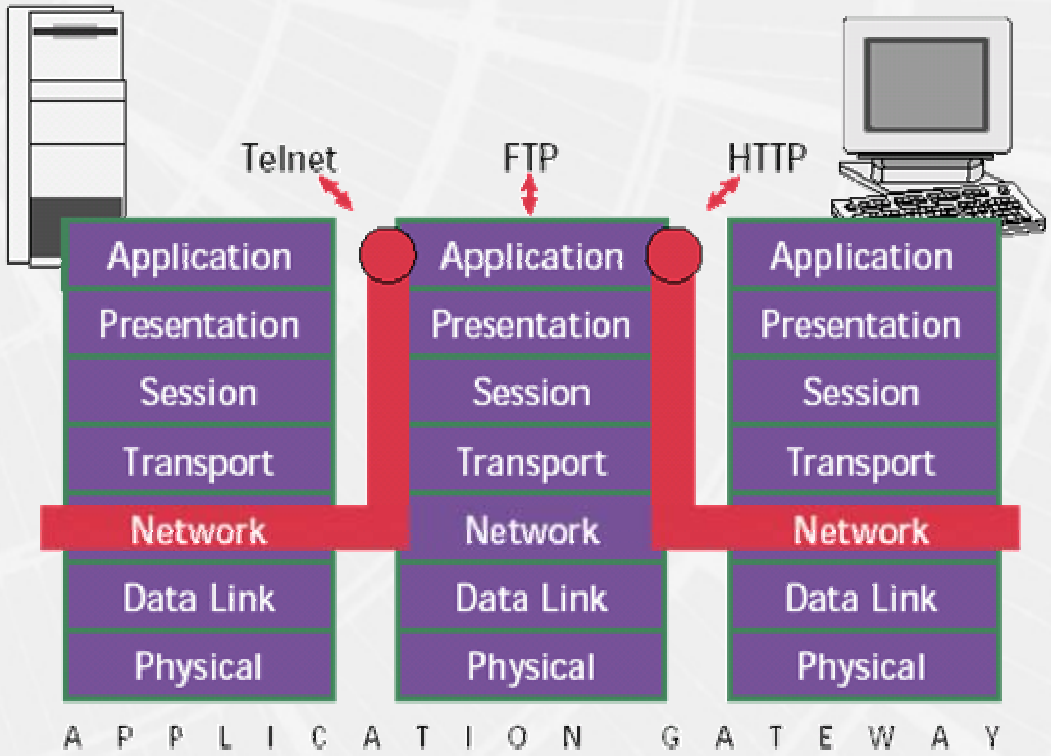
- Application Independence
- High Performance
- Scalability

CONS

- Low Security
- No Screening Above Network Layer (No 'state' or application-context information)

Source: Checkpoint 2002

- Firewall « proxy »

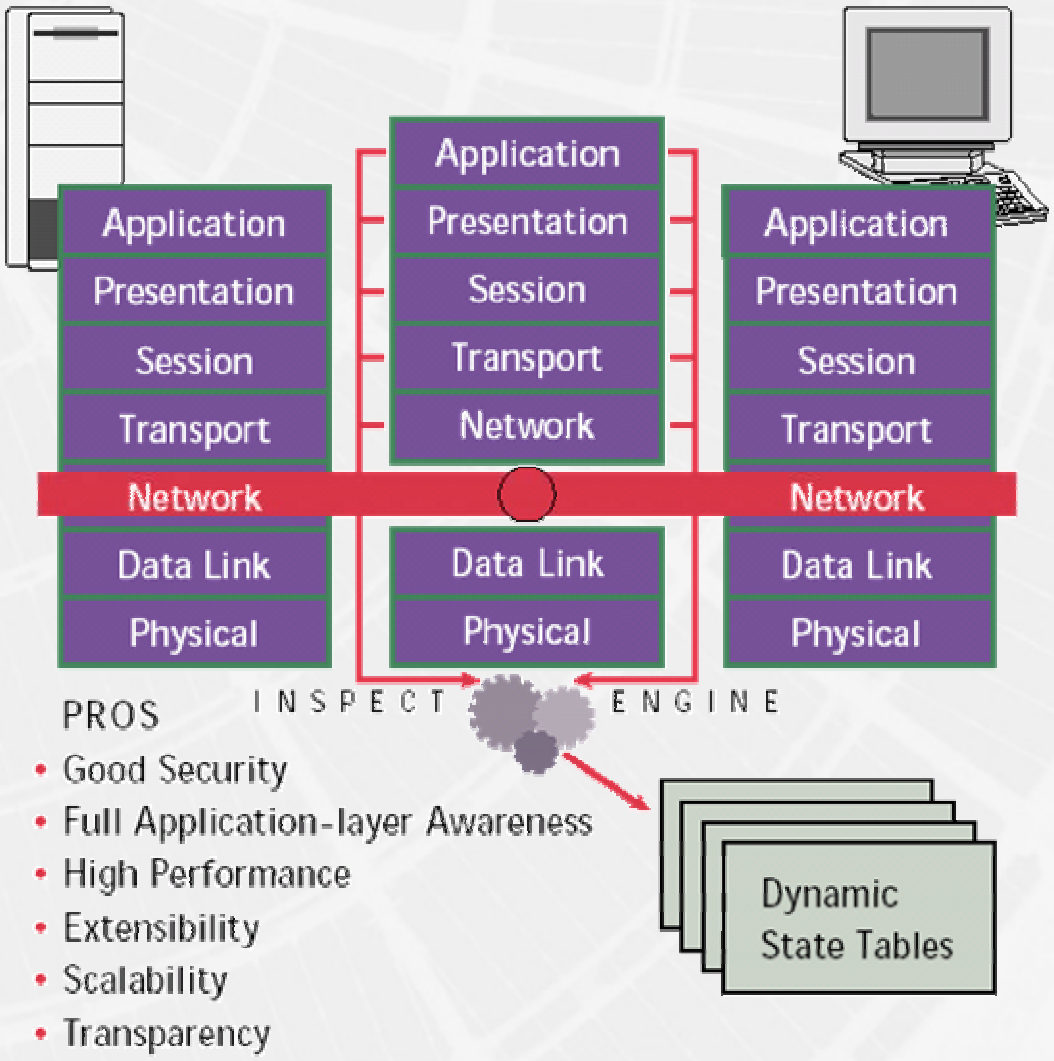


PROS
- Good Security
- Full Application-layer Awareness

CONS
- Poor Performance
- Limited Application Support
- Poor Scalability (Breaks client/server model)

Source: Checkpoint 2002

- Firewall « Stateful Inspection »

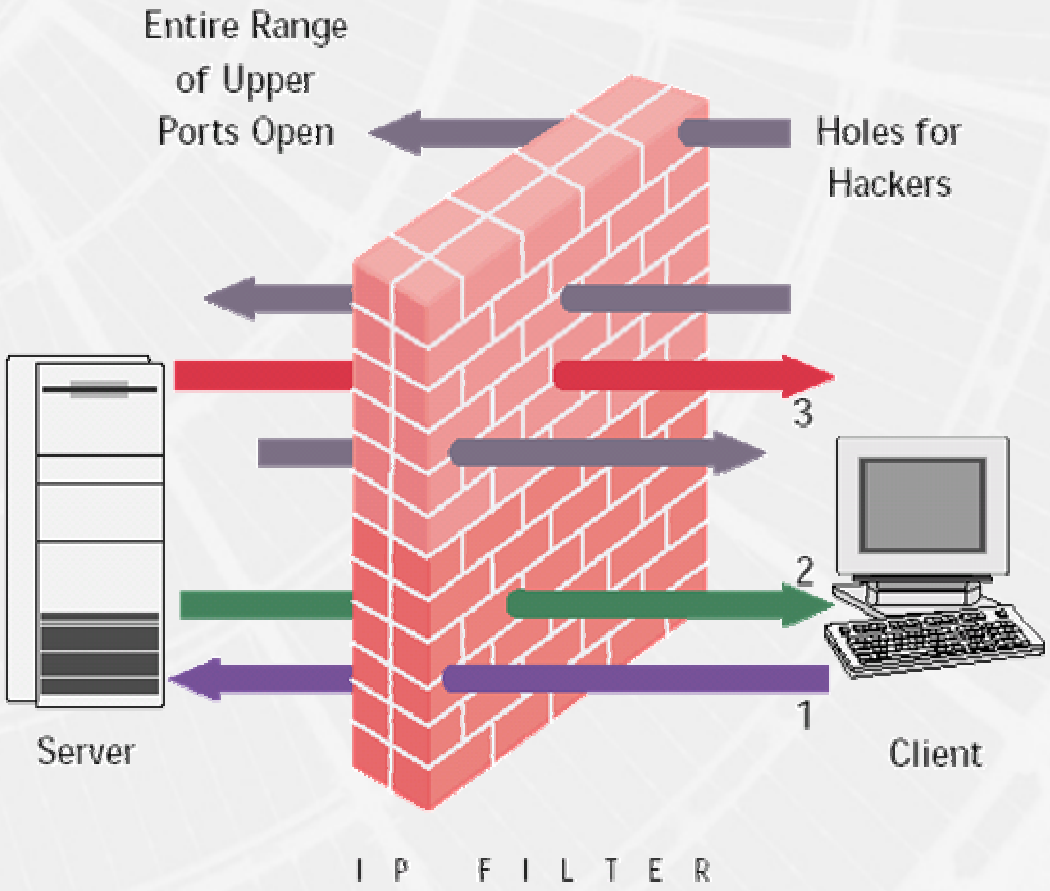


PROS

- Good Security
- Full Application-layer Awareness
- High Performance
- Extensibility
- Scalability
- Transparency

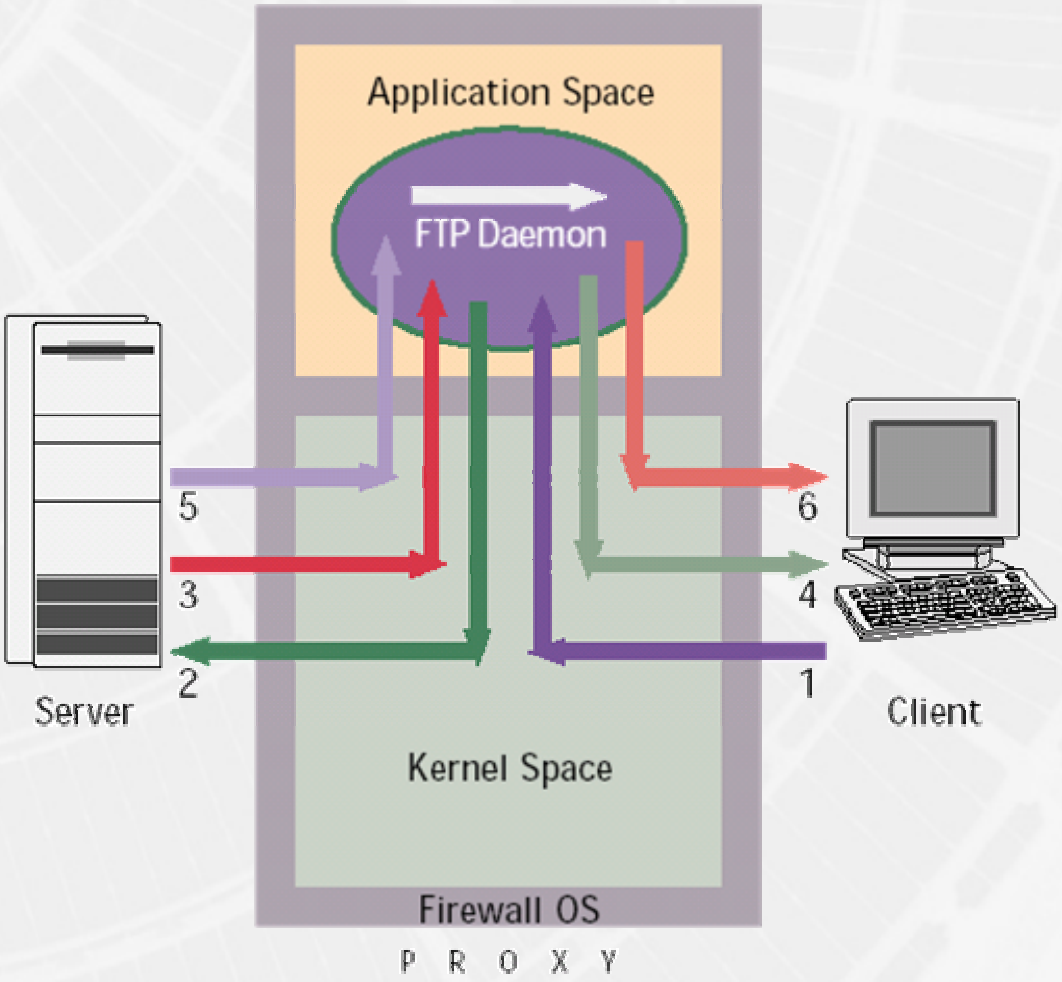
Source: Checkpoint 2002

- Exemple avec FTP: packet filter



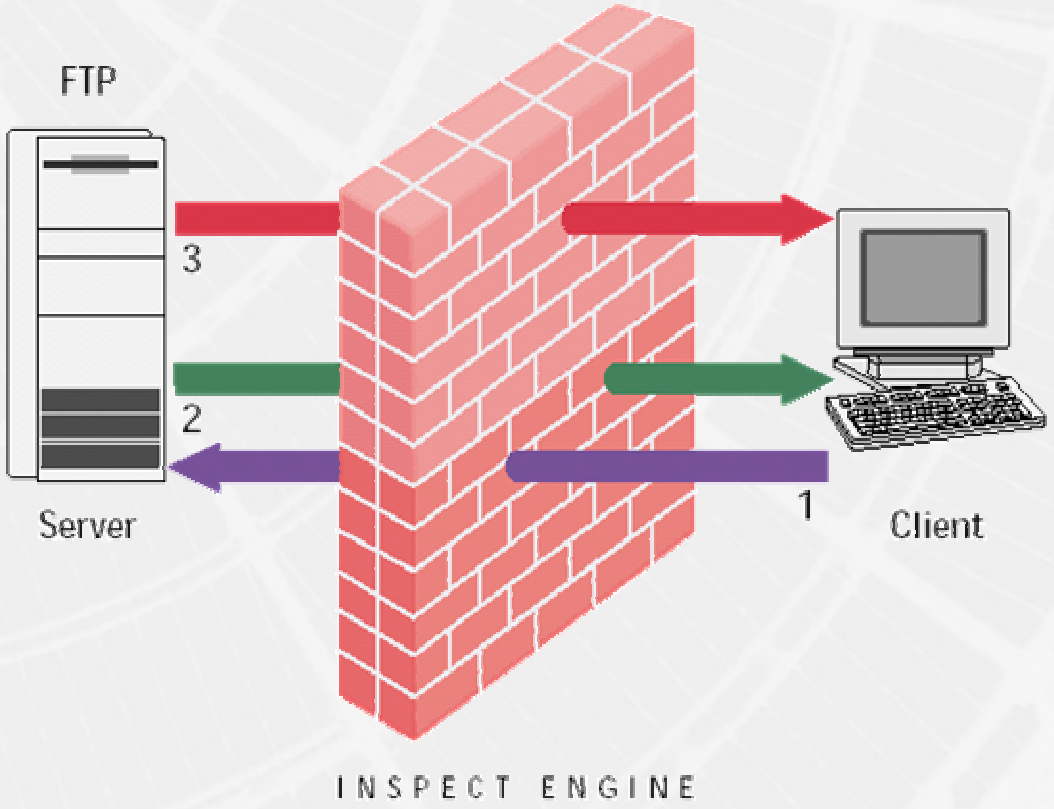
Source: Checkpoint 2002

- Exemple avec FTP: proxy



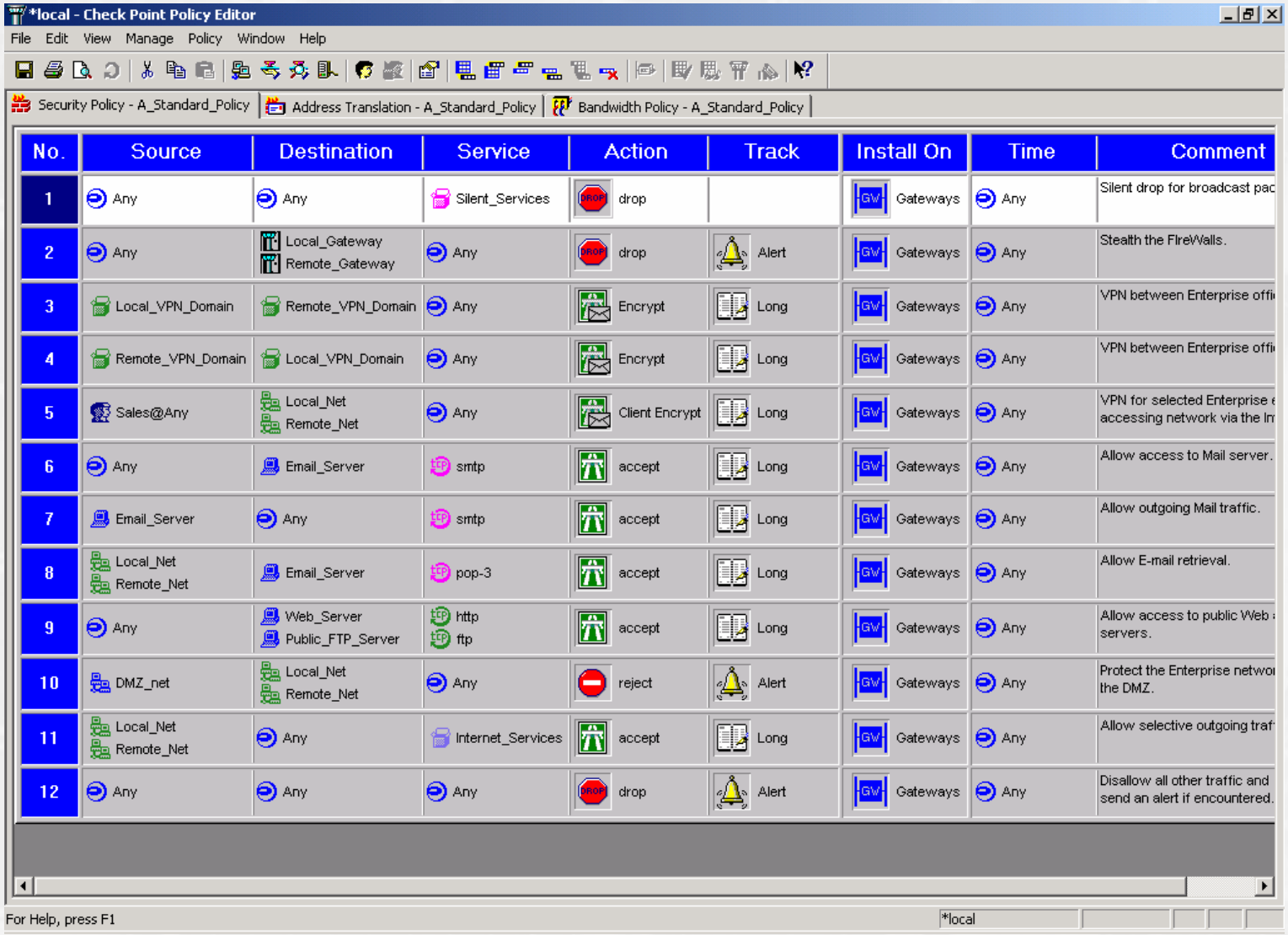
Source: Checkpoint 2002

- Exemple avec FTP: stateful inspection



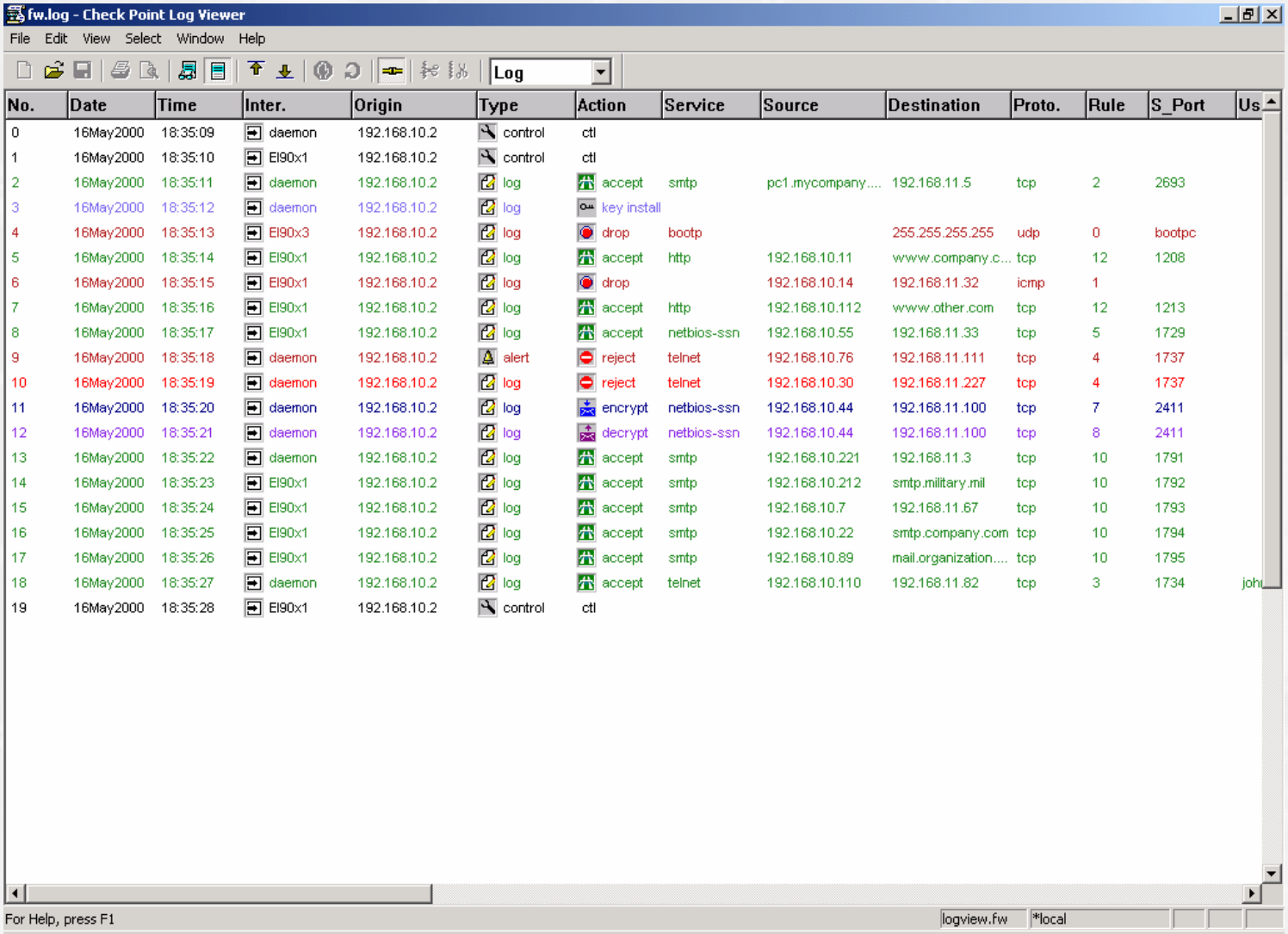
Source: Checkpoint 2002

Exemple de règles firewall: Checkpoint



No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	Any	Any	Silent_Services	drop		Gateways	Any	Silent drop for broadcast pac
2	Any	Local_Gateway Remote_Gateway	Any	drop	Alert	Gateways	Any	Stealth the FIreWalls.
3	Local_VPN_Domain	Remote_VPN_Domain	Any	Encrypt	Long	Gateways	Any	VPN between Enterprise offi
4	Remote_VPN_Domain	Local_VPN_Domain	Any	Encrypt	Long	Gateways	Any	VPN between Enterprise offi
5	Sales@Any	Local_Net Remote_Net	Any	Client Encrypt	Long	Gateways	Any	VPN for selected Enterprise accessing network via the In
6	Any	Email_Server	smtp	accept	Long	Gateways	Any	Allow access to Mail server.
7	Email_Server	Any	smtp	accept	Long	Gateways	Any	Allow outgoing Mail traffic.
8	Local_Net Remote_Net	Email_Server	pop-3	accept	Long	Gateways	Any	Allow E-mail retrieval.
9	Any	Web_Server Public_FTP_Server	http ftp	accept	Long	Gateways	Any	Allow access to public Web servers.
10	DMZ_net	Local_Net Remote_Net	Any	reject	Alert	Gateways	Any	Protect the Enterprise netwo the DMZ.
11	Local_Net Remote_Net	Any	Internet_Services	accept	Long	Gateways	Any	Allow selective outgoing traf
12	Any	Any	Any	drop	Alert	Gateways	Any	Disallow all other traffic and send an alert if encountered.

Exemple de « log » avec Checkpoint

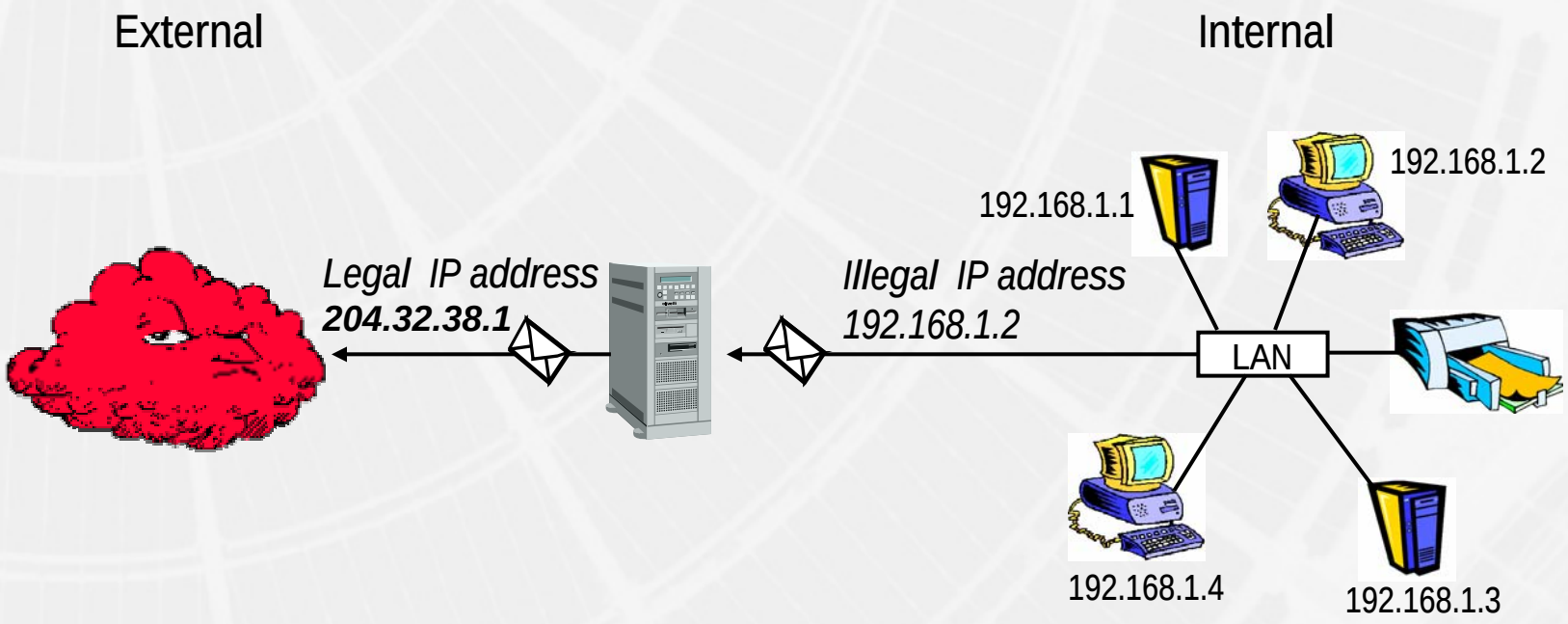


No.	Date	Time	Inter.	Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port	Us
0	16May2000	18:35:09	daemon	192.168.10.2	control	ctl							
1	16May2000	18:35:10	EI90x1	192.168.10.2	control	ctl							
2	16May2000	18:35:11	daemon	192.168.10.2	log	accept	smtp	pc1.mycompany....	192.168.11.5	tcp	2	2693	
3	16May2000	18:35:12	daemon	192.168.10.2	log	key install							
4	16May2000	18:35:13	EI90x3	192.168.10.2	log	drop	bootp		255.255.255.255	udp	0	bootpc	
5	16May2000	18:35:14	EI90x1	192.168.10.2	log	accept	http	192.168.10.11	www.company.c...	tcp	12	1208	
6	16May2000	18:35:15	EI90x1	192.168.10.2	log	drop		192.168.10.14	192.168.11.32	icmp	1		
7	16May2000	18:35:16	EI90x1	192.168.10.2	log	accept	http	192.168.10.112	www.other.com	tcp	12	1213	
8	16May2000	18:35:17	EI90x1	192.168.10.2	log	accept	netbios-ssn	192.168.10.55	192.168.11.33	tcp	5	1729	
9	16May2000	18:35:18	daemon	192.168.10.2	alert	reject	telnet	192.168.10.76	192.168.11.111	tcp	4	1737	
10	16May2000	18:35:19	daemon	192.168.10.2	log	reject	telnet	192.168.10.30	192.168.11.227	tcp	4	1737	
11	16May2000	18:35:20	daemon	192.168.10.2	log	encrypt	netbios-ssn	192.168.10.44	192.168.11.100	tcp	7	2411	
12	16May2000	18:35:21	daemon	192.168.10.2	log	decrypt	netbios-ssn	192.168.10.44	192.168.11.100	tcp	8	2411	
13	16May2000	18:35:22	daemon	192.168.10.2	log	accept	smtp	192.168.10.221	192.168.11.3	tcp	10	1791	
14	16May2000	18:35:23	EI90x1	192.168.10.2	log	accept	smtp	192.168.10.212	smtp.military.mil	tcp	10	1792	
15	16May2000	18:35:24	EI90x1	192.168.10.2	log	accept	smtp	192.168.10.7	192.168.11.67	tcp	10	1793	
16	16May2000	18:35:25	EI90x1	192.168.10.2	log	accept	smtp	192.168.10.22	smtp.company.com	tcp	10	1794	
17	16May2000	18:35:26	EI90x1	192.168.10.2	log	accept	smtp	192.168.10.89	mail.organization....	tcp	10	1795	
18	16May2000	18:35:27	daemon	192.168.10.2	log	accept	telnet	192.168.10.110	192.168.11.82	tcp	3	1734	joh
19	16May2000	18:35:28	EI90x1	192.168.10.2	control	ctl							

Translation d'adresses: « NAT »

- Mécanisme de modification des adresses IP source ou/et destination
  - Eventuellement changement des ports: PAT
- NAT « Static »
  - 1 vers 1
  - En source ou en destination
- NAT « Hide »
  - N vers 1
  - Utilise de la PAT
  - Utiliser pour cacher un réseau (accès Internet)

- Exemple de « NAT »



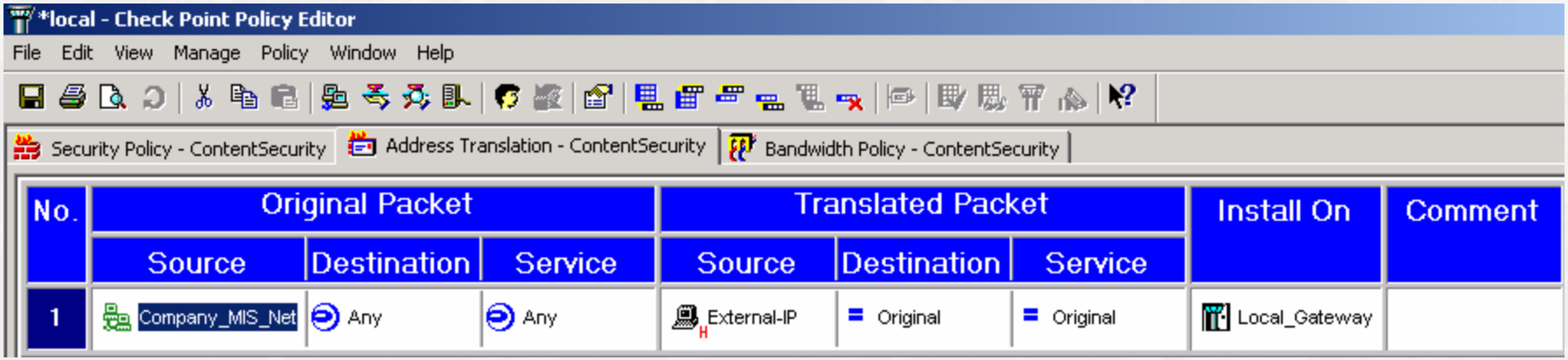
- Exemple de « NAT » avec Checkpoint

*local - Check Point Policy Editor

File Edit View Manage Policy Window Help

Security Policy - ContentSecurity | Address Translation - ContentSecurity | Bandwidth Policy - ContentSecurity

No.	Original Packet			Translated Packet			Install On	
	Source	Destination	Service	Source	Destination	Service		
1	Email_Server	Any	Any	Email_Server (Valid Address)	= Original	= Original	All	Automatic rule
2	Any	Email_Server (Valid Address)	Any	= Original	Email_Server	= Original	All	Automatic rule



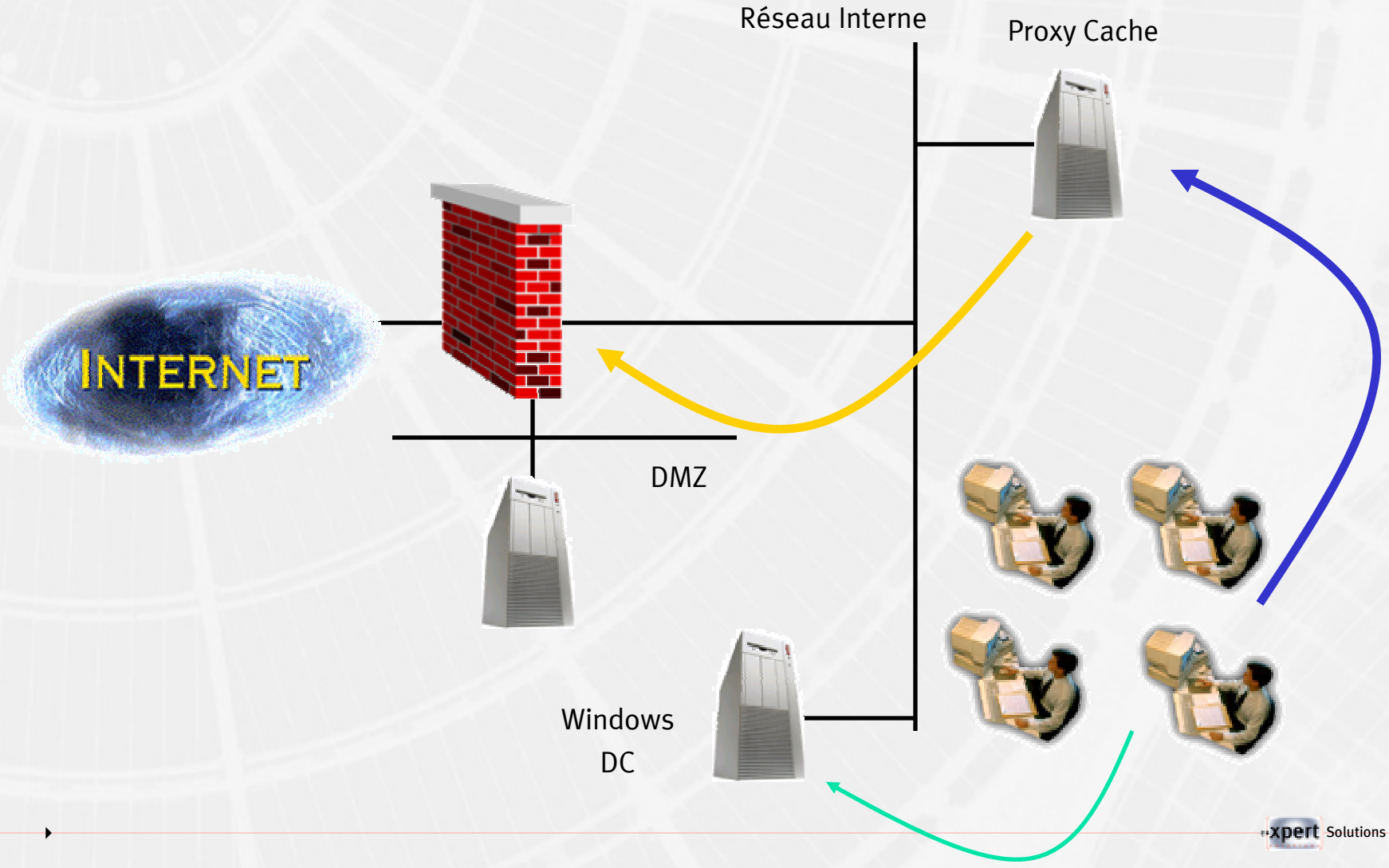
Firewalls: tendance des Appliances

- Concept de « black box »
- Est considéré comme un élément classique du réseau
  - Routeur, Switchs, RAS, etc.
- Facilité d'exploitation
- Facilité d'utilisation
- Niveau de sécurité élevé
- Gestion par SSL et/ou SSH
- Performance
- OS de type Unix / Linux

Les proxy

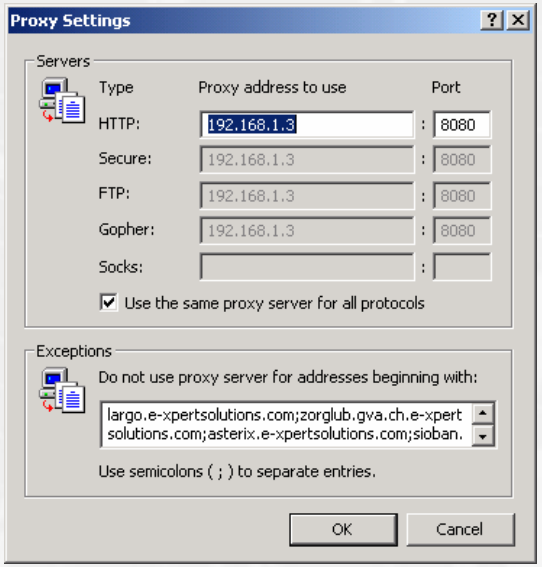
- Complémentaire au firewall
- Caching (gain de performance)
  - HTTP, FTP, Streaming Vidéo ou Audio
- Auditing
  - Fichier de logs
  - Qui, Quand, Où
- Authentification (NTLM, Radius, ldap, etc.)
- Interface pour un contrôle de contenu
  - ICAP ou Plug-IN
  - Analyse virale
  - URL Filtering
  - Analyse code mobile

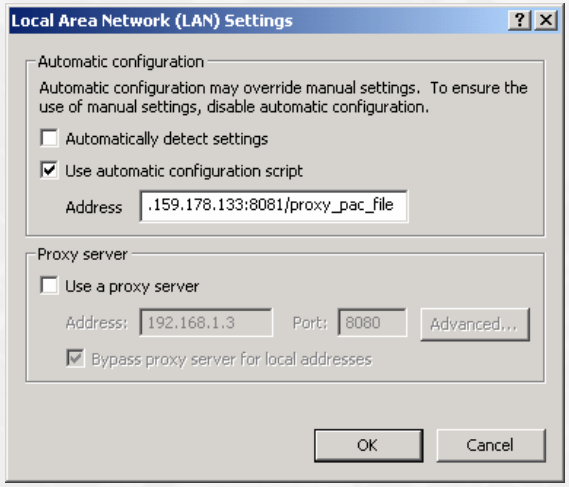
- Exemple d'implémentation avec authentification Microsoft



Les proxy: configuration des postes clients

- Configuration du navigateur avec adresse IP (ou le nom) et le « port » du proxy
- Proxy Pac
  - Fichier de configuration
- Solution transparente
  - WCCP
- Ne pas oublier la gestion des exceptions !



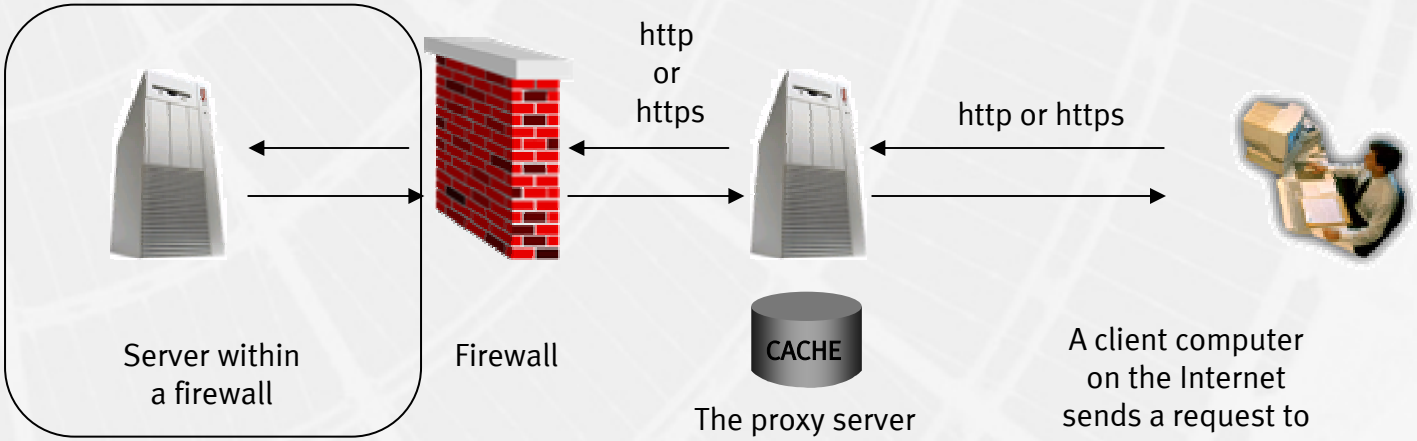


Reverse Proxy

- Permet d'accéder à un service web via le Reverse Proxy
- Protection du site web (firewall applicatif)
  - Filtrage d'url
  - Authentification
  - Protection DoS (IIS)
- Terminaison SSL
  - IDS
  - Performance
- Accès aux ressources internes
  - Messagerie, extranet, etc.

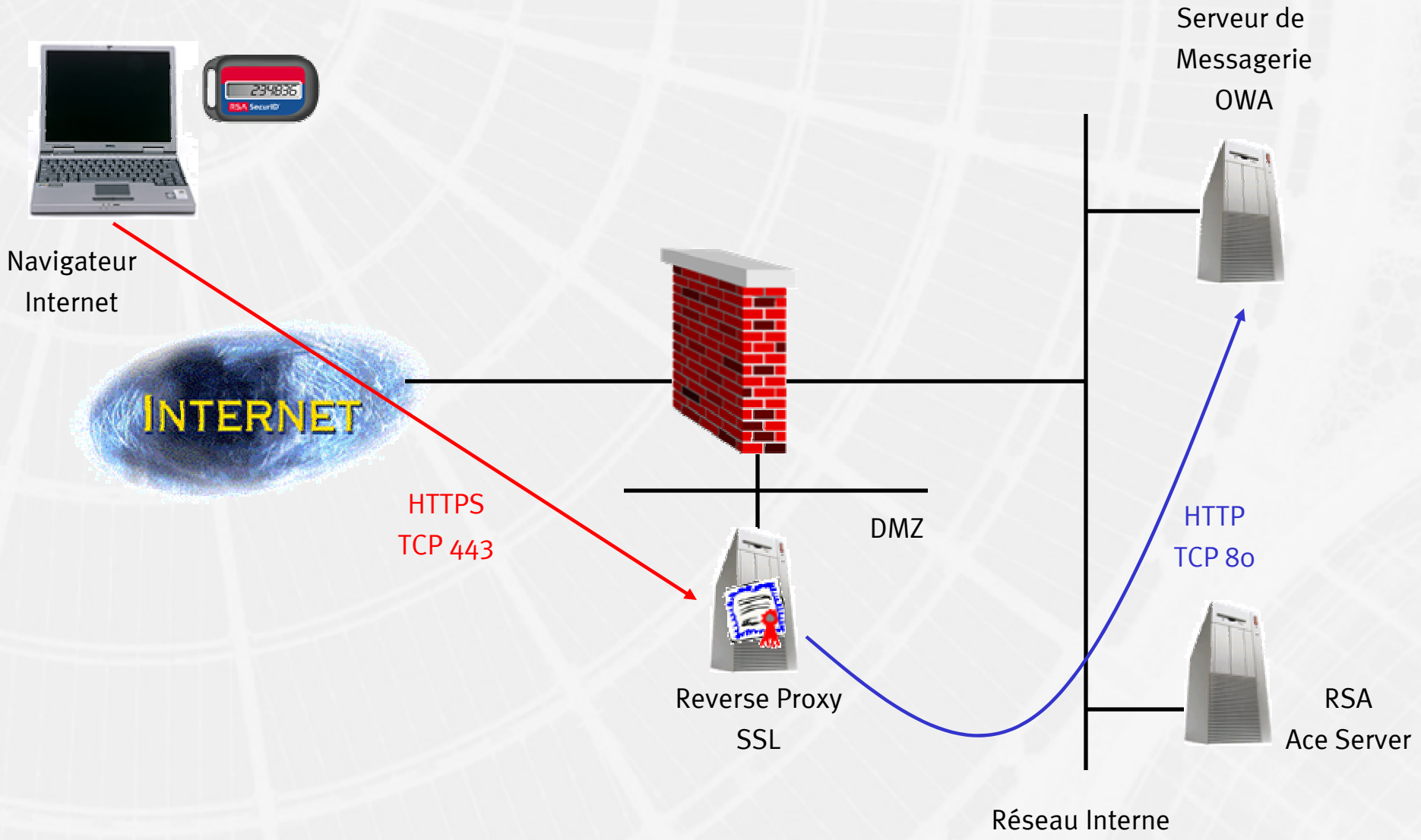
Reverse Proxy

The proxy server uses a regular mapping to forward the client request to the internal content server



You can configure the firewall router to allow a specific server on a specific port (in this case, the proxy on its assigned port) to have access through the firewall without allowing any other machine in or out.

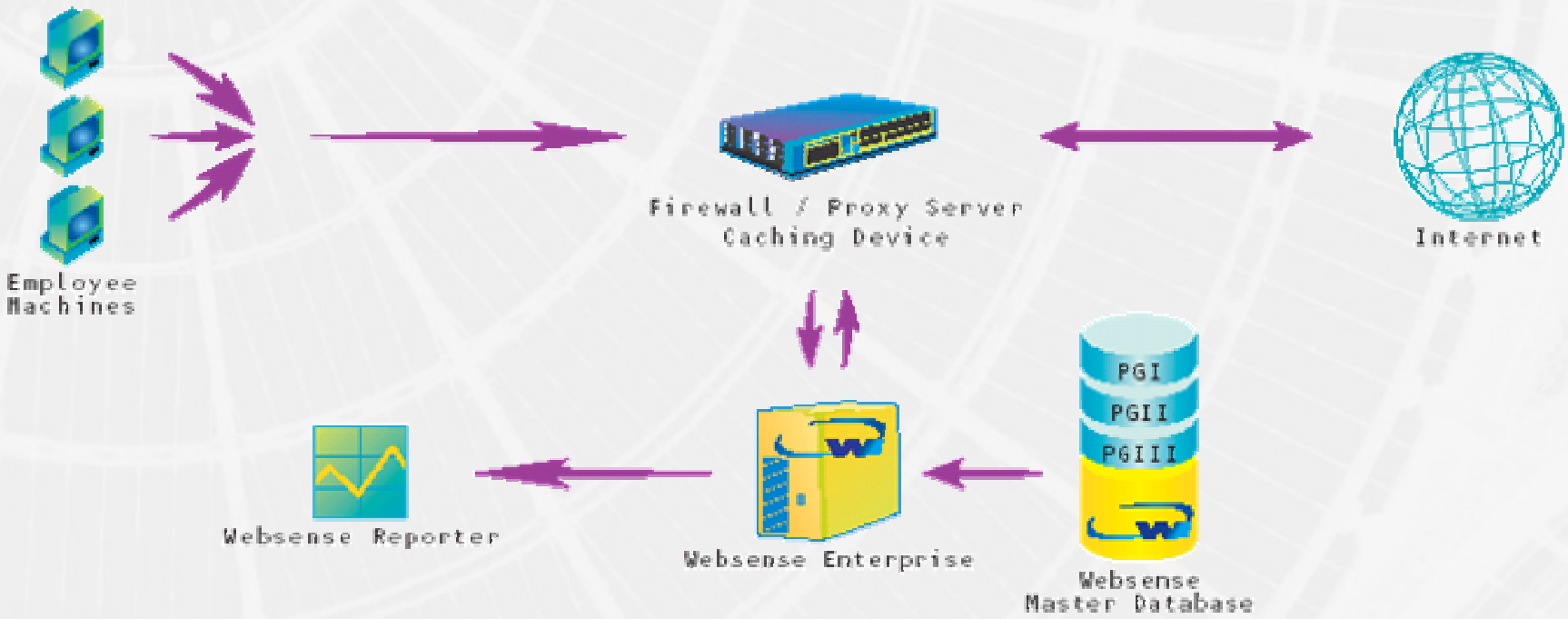
- Reverse Proxy: exemple d'implémentation avec authentification forte



Filtrage d'URL

- Contrôle d'accès aux sites Internet
- Très utilisé dans les entreprises
  - Banques, Industries, Assurances, etc.
- Plusieurs techniques:
  - Base de données
  - Reconnaissance de mots clés
  - Analyse des images
  - RSAC
  - Etc.
- Peut être utilisé pour la protection des codes mobiles

- Exemple d'implémentation avec un proxy



Source: Websense 2002

Catégorie Websense

MASTER DATABASE

Abortion Advocacy
- Pro-Life
- Pro-Choice

Advocacy Groups

Adult Material
- Adult Content
- Nudity
- Sex
- Sex Education
- Lingerie & Swimsuit

Business & Economy
- Financial Data & Services

Drugs
- Abused Drugs
- Prescribed Medications
- Supplements/Unregulated Compounds
- Marijuana

Education
- Educational Institutions
- Cultural Institutions
- Educational Materials

Entertainment
- MP3

Gambling

Games

Government
- Military
- Political Groups

Health

Illegal/Questionable

Information Technology
- Hacking
- Proxy Avoidance Systems
- Search Engines & Portals
- Web Hosting
- URL Translation Sites

Internet Communication
- Web Chat
- Web-based Email

Job Search

Militancy/Extremist

News & Media
- Alternative Journals

Racism/Hate

Religion
- Non-Traditional Religions
- Traditional Religions

Shopping
- Internet Auctions
- Real Estate

Society & Lifestyle
- Alcohol/Tobacco
- Gay & Lesbian Issues
- Personals/Dating
- Restaurants & Dining
- Hobbies
- Personal Web Sites

Special Events

Sports
- Sport Hunting/Gun Clubs

Tasteless

Travel

Vehicles

Violence

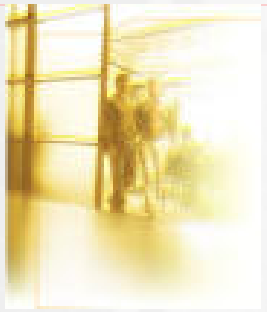
Weapons

Premium Group I (PGI) - Productivity Management

- Advertisements
- Freeware/Software Download
- Instant Messaging
- Message Boards & Clubs
- Online Brokerage & Trading
- Pay-to-Surf

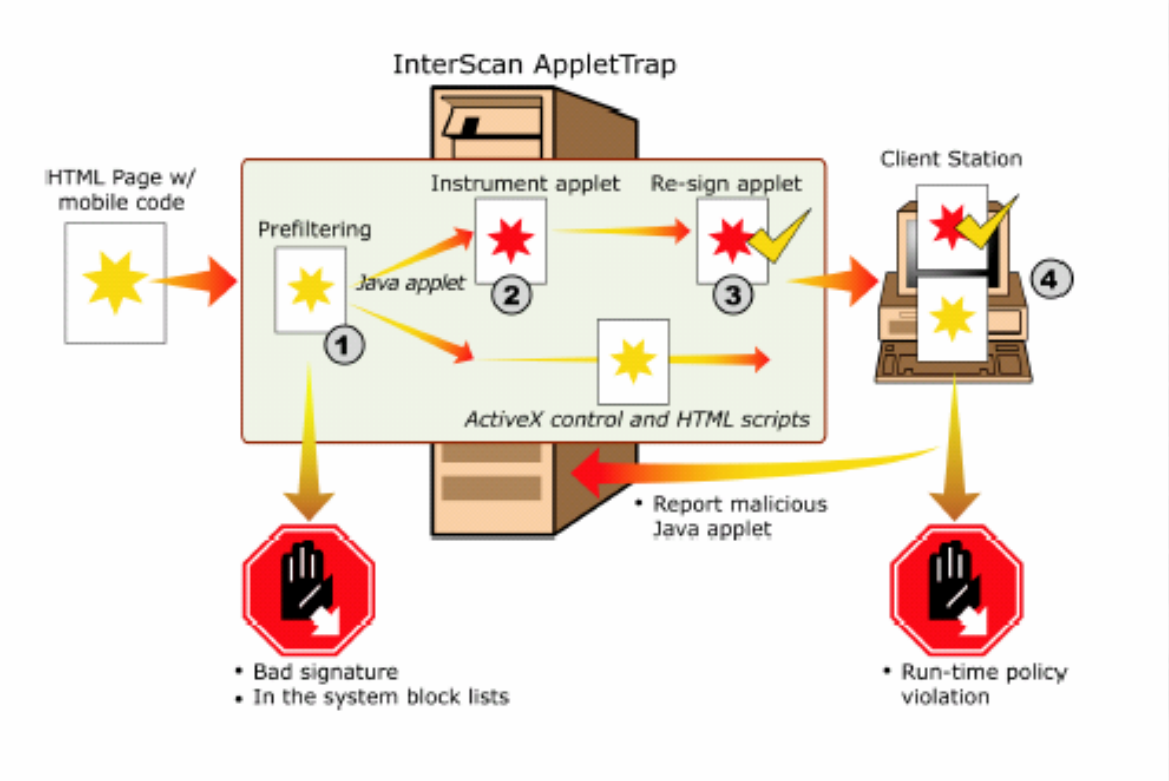
Premium Group II (PGII) - Bandwidth Management

- Internet Radio & TV
- Peer-to-Peer File Sharing
- Personal Network Storage/Backup
- Internet Telephony
- Streaming Media



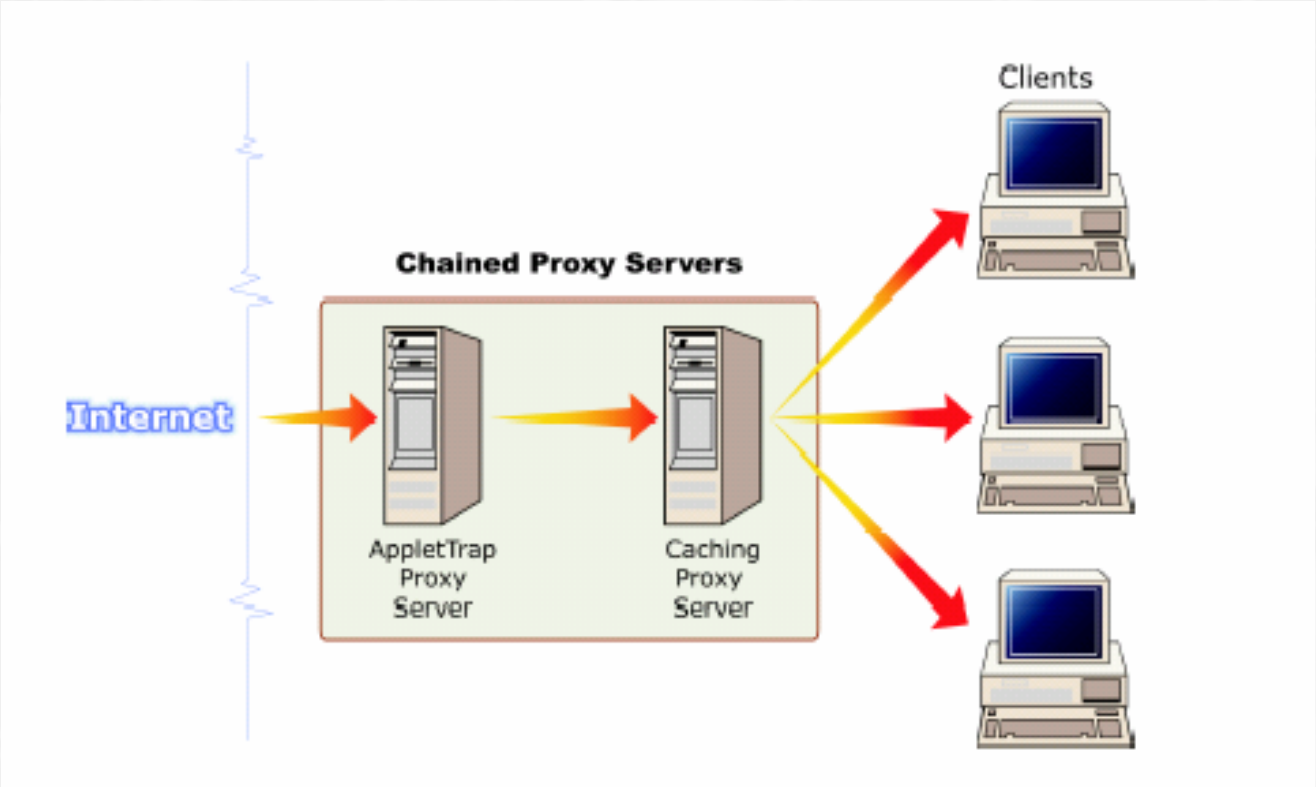
- Analyse du contenu des flux de communications
  - Analyse des Emails
    - Virus
    - Taille
    - Type de fichiers
    - Analyse lexicale
    - Etc.
  - Analyse des flux HTTP et FTP
    - Virus
    - Download de fichiers
    - Codes mobiles
    - Etc.

- Contrôle des codes mobiles

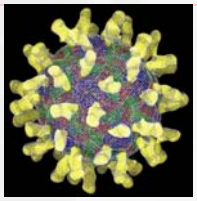


Source: Trendmicro 2002

- Exemple d'implémentation: codes mobiles



Source: Trendmicro 2002

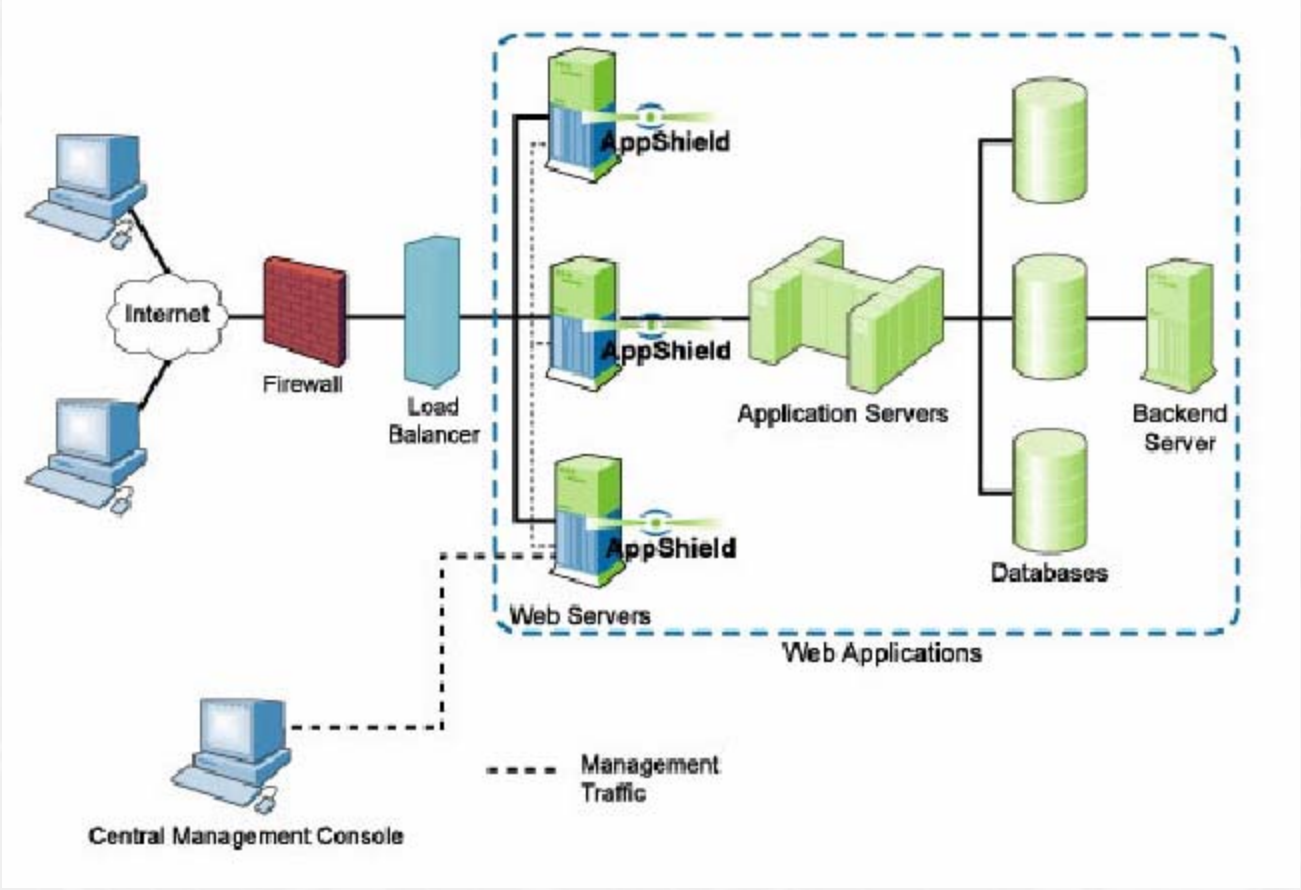


- Outils classiques de sécurité
- Plusieurs catégories
  - AV pour les serveurs
  - AV pour les postes clients
  - AV HTTP et FTP
  - AV spécifique
    - Messagerie (Exchange, Notes, Mailsweeper, etc.)
- La mise à jour doit être très rapide
  - Backweb, http, ftp, etc.

Web application firewall: la nouvelle tendance

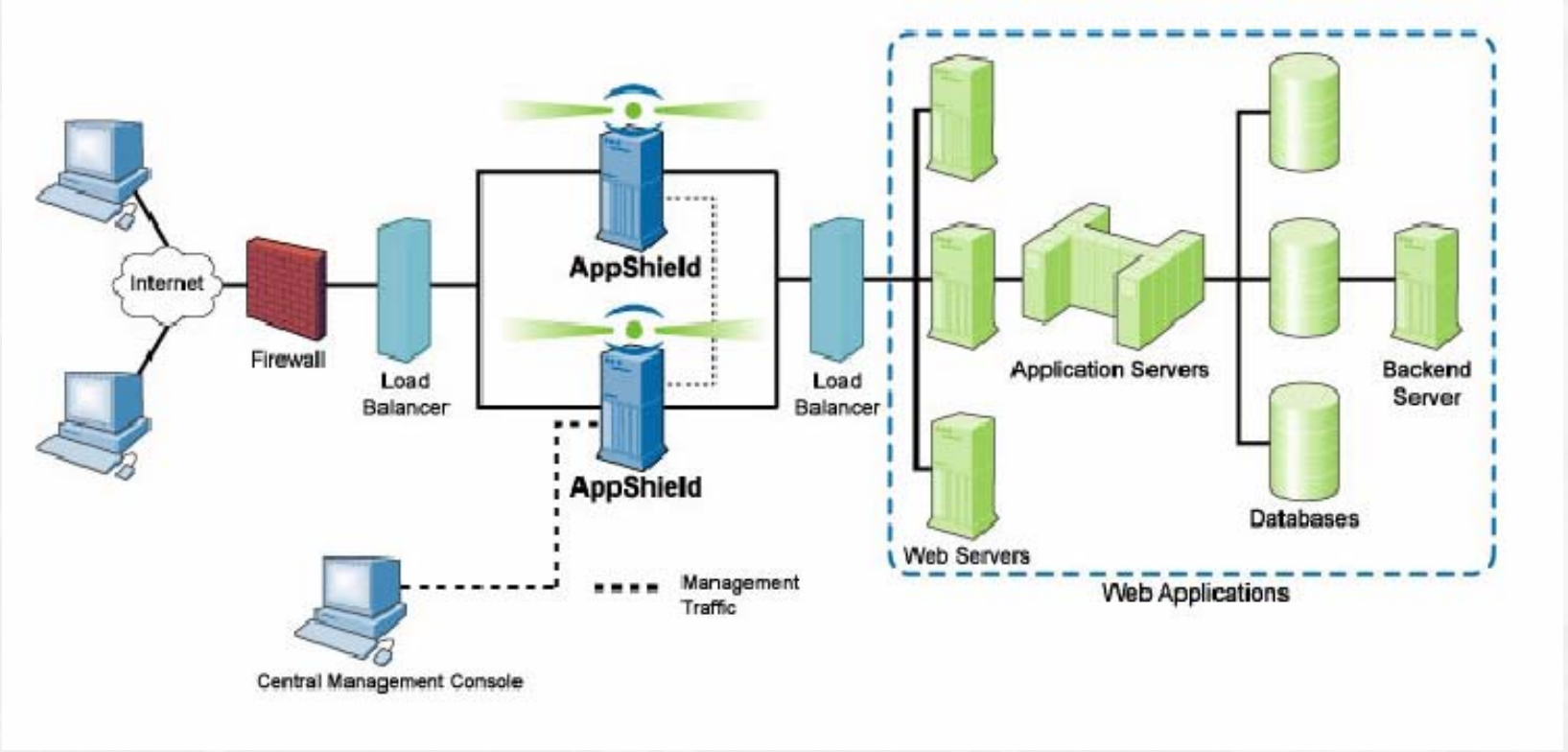
- Protection des services Web par un filtrage des URL
  - BoF
  - Bad URL
  - Back Door
  - Cookie poisoning
  - Etc.
- Deux approches
  - Reverse Proxy
  - Agent sur le frontal Web

- Agent sur le frontal Web



Source: Sanctum 2002

- Approche Reverse Proxy



Source: Sanctum 2002

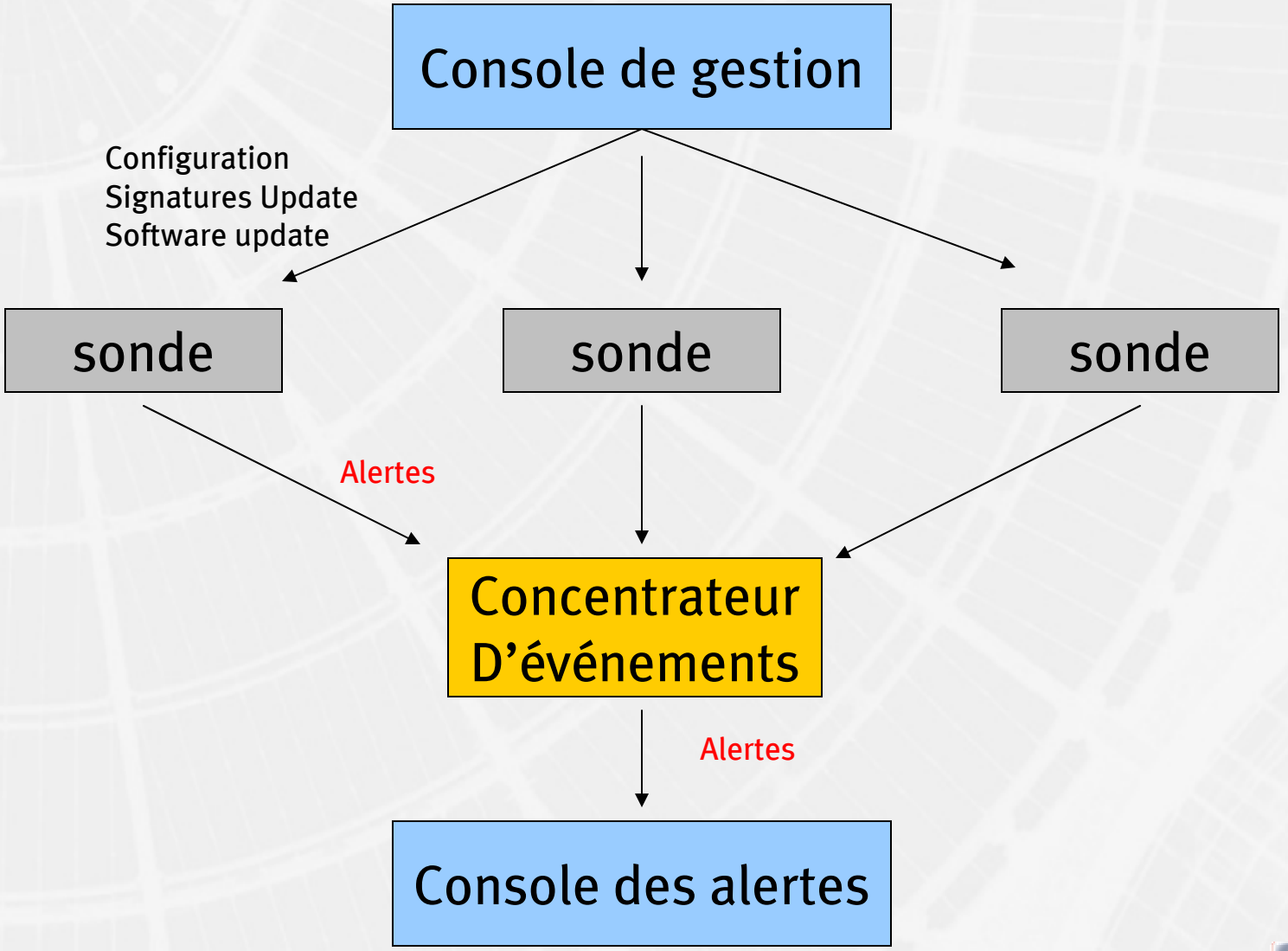
Système de détection d'intrusions: définition

- Système d'analyse d'informations visant à détecter des événements signalant une intrusion potentielle
- Ces informations peuvent être:
  - journal system (logs)
  - Journal applicatif
  - Sonde réseau (sniffer)
  - Sonde « host »
  - Etc.
- IDS = Intrusion Detection System

Système de détection d'intrusion: architecture

- Outils modernes présentant les éléments structuraux suivants:
  - les sondes
  - Les concentrateurs d'événements
  - La ou les console(s) de gestion
  - La ou les console(s) des alertes

- Système de détection d'intrusions: architecture



- Système de détection d'intrusion: la sonde

Système de détection d'intrusions: type de sonde

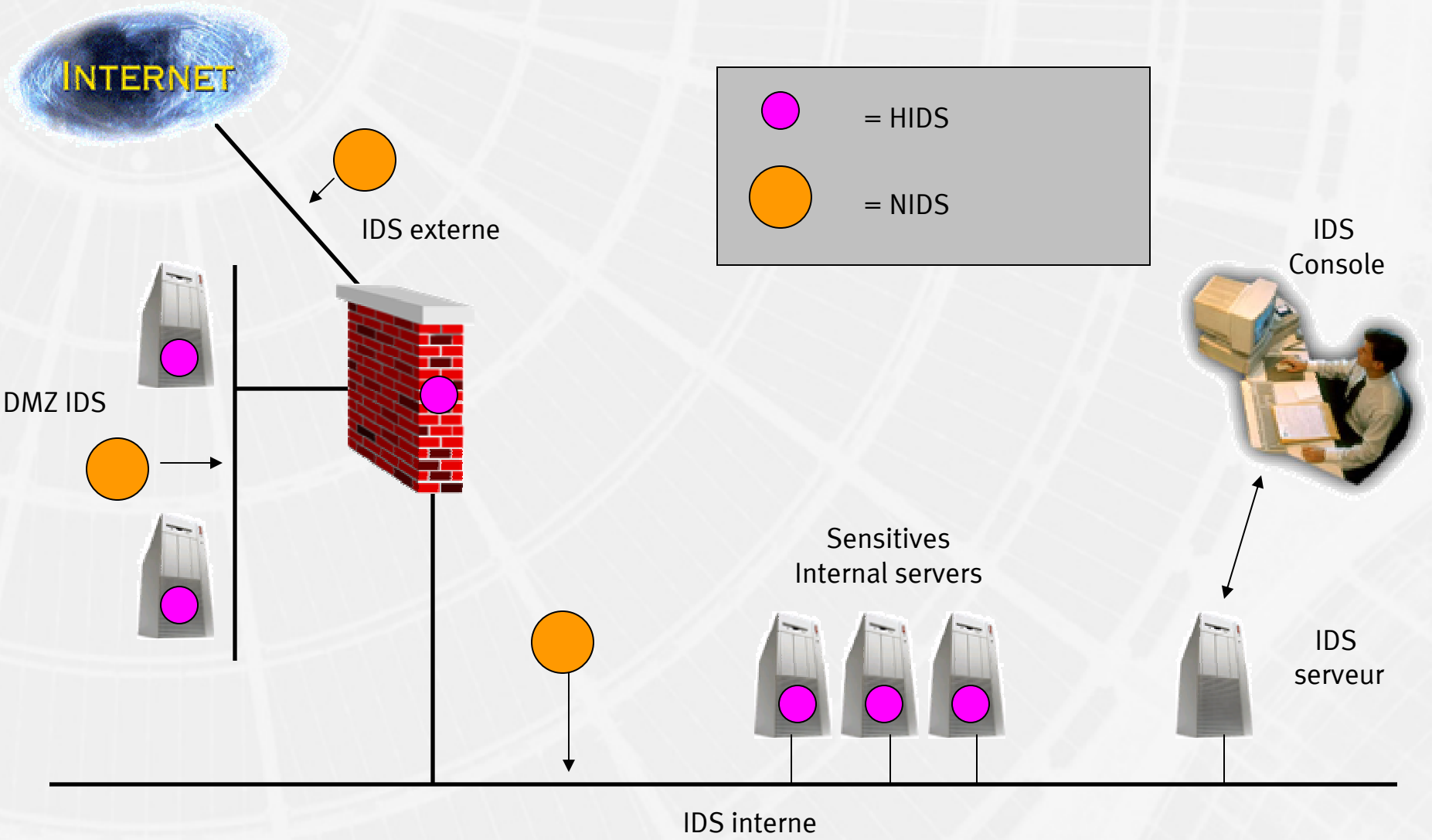
- Sondes systèmes: HIDS
  - Analyse des événements de type système et/ou de type application (serveur web, db, etc.)
- Sonde réseau: NIDS
  - Analyse des événements réseaux
  - Généralement en écoute sur un HUB ou switch (copy port)
  - Embarquée dans le switch
- Sonde mixte: Mixed IDS
  - Analyse réseau sur un host

Système de détection d'intrusions: algorithmes d'analyse

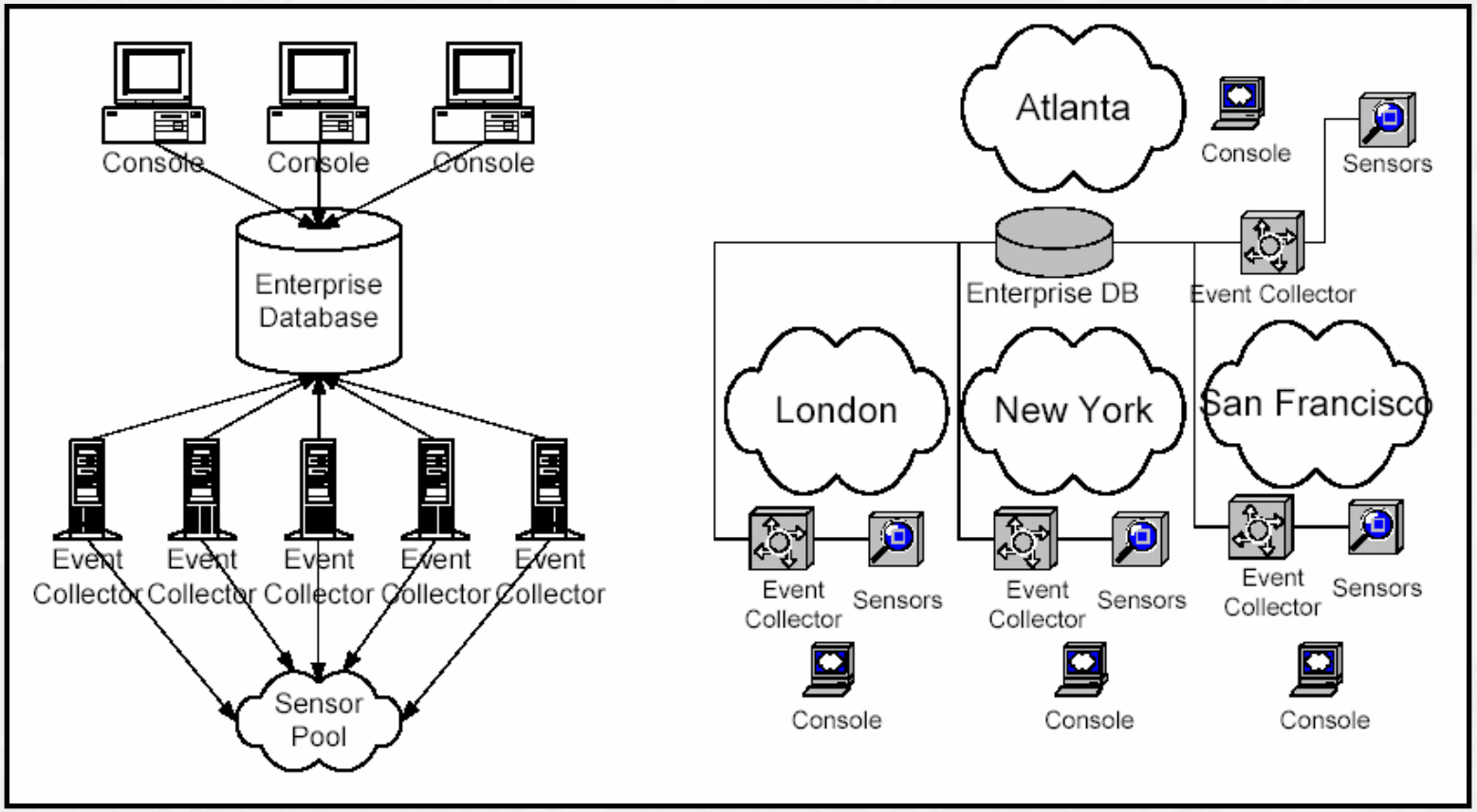
- Actuellement 2 approches
  - Approche scénario (knowledge base scenario)
    - Basée sur une base d'attaques connues
  - Approche comportementale (Anomaly Detection)
    - Définition du comportement « normal » des systèmes informatiques
    - Exclusion des événements non-standards
    - Actuellement en phase de test

- Possibilité de générer une contre-mesure suite à une attaques
  - Interaction avec un firewall
    - SAM de Checkpoint
  - Isolement d'une machine attaquée (Islanding)
  - Ralentissement de la connexion avec l'attaquant (throlting)
  - Etc.
- Attention au DoS …

- Système de détection d'intrusions: exemple d'implémentation



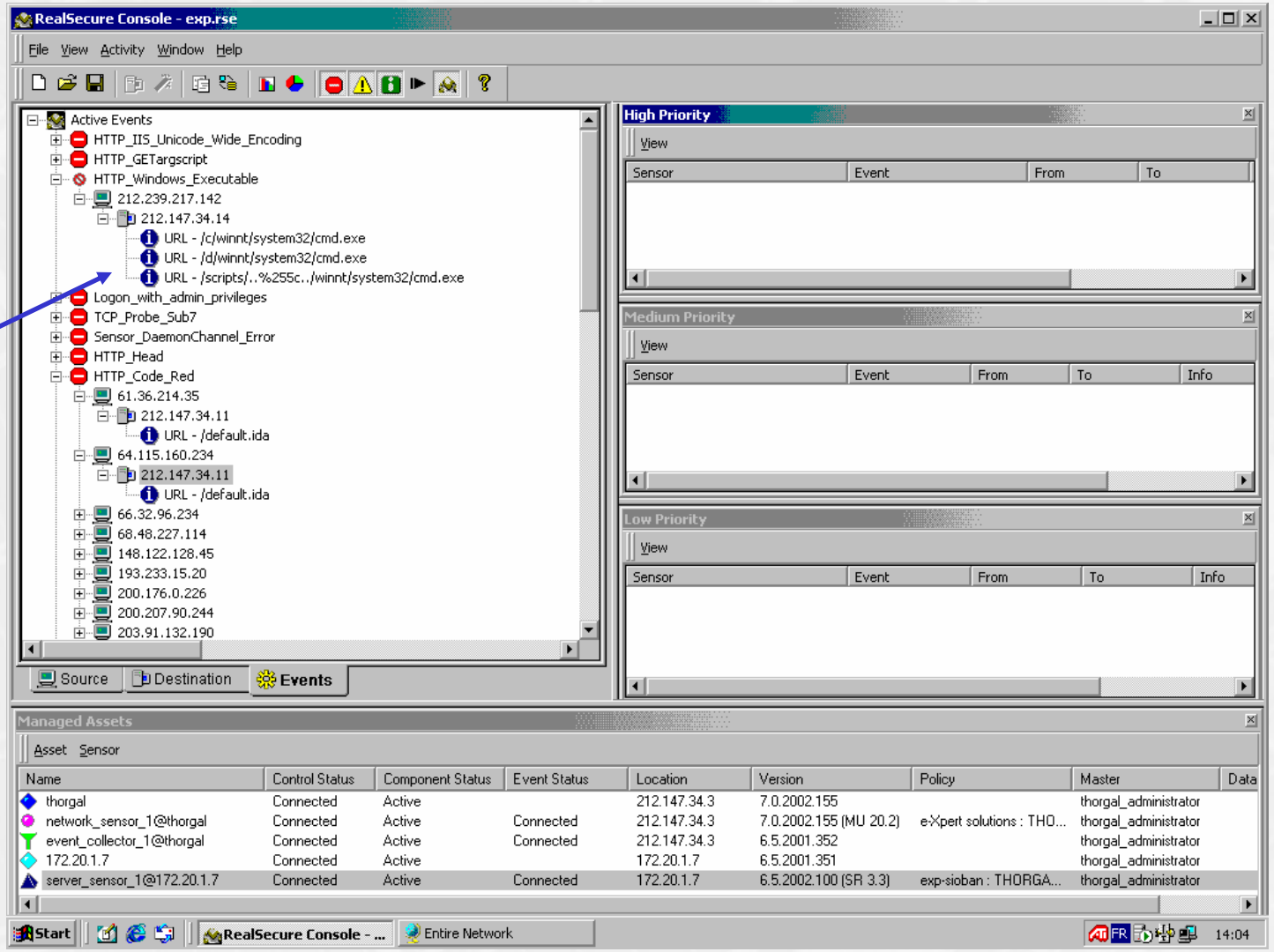
- ISS RealSecure: architecture distribuée



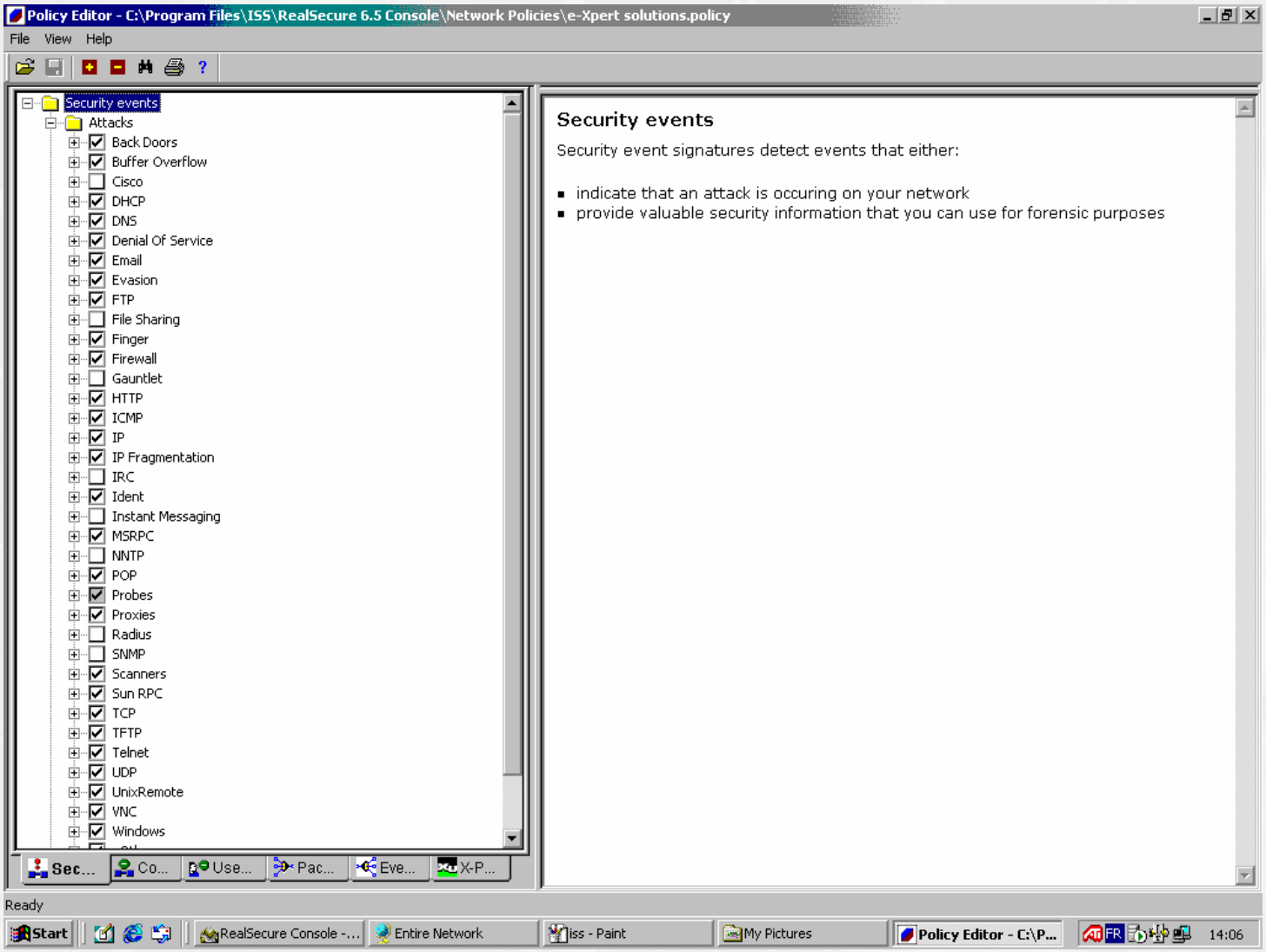
Source:
ISS 2002

ISS RealSecure: console des alertes

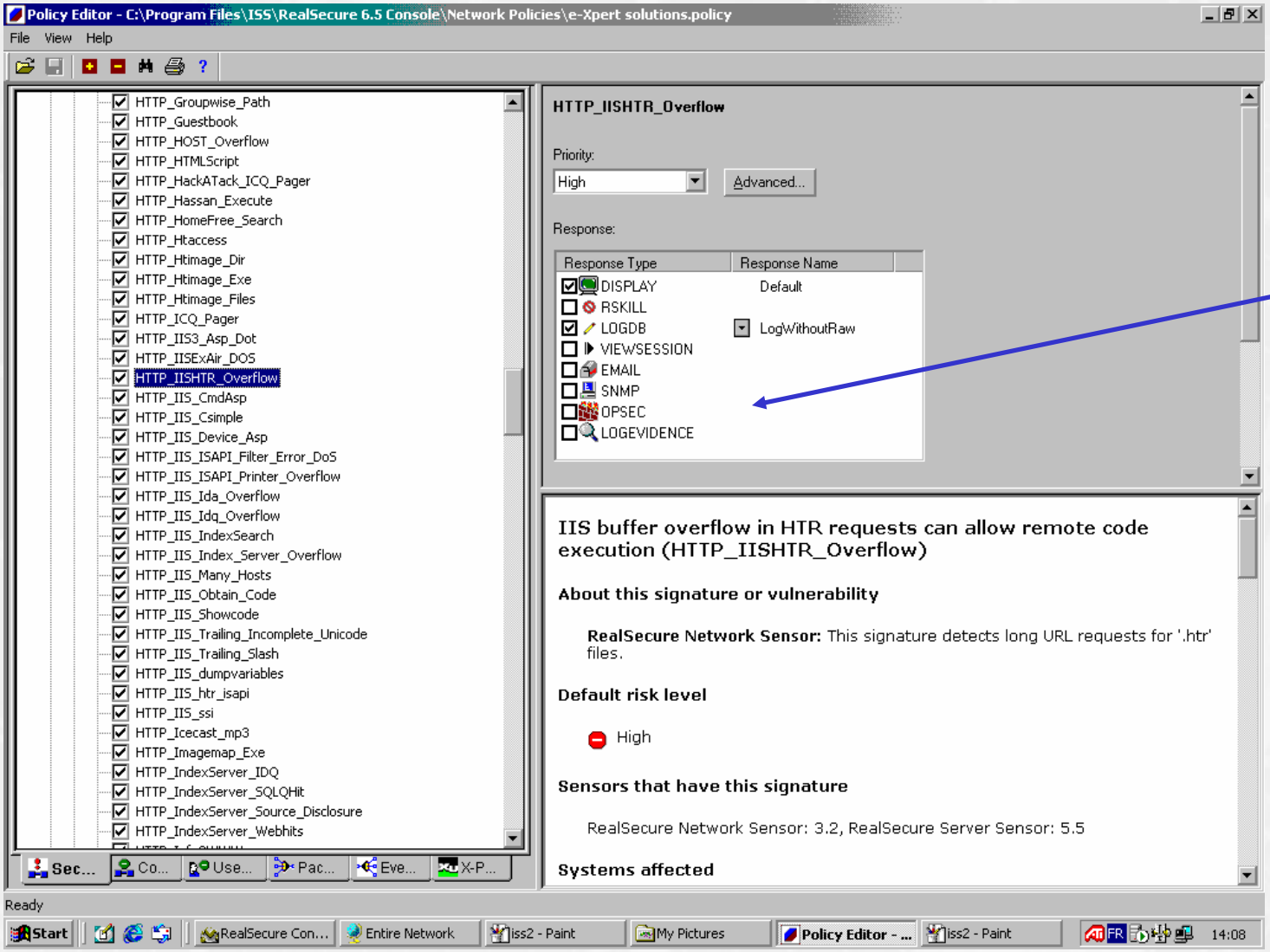
Exemple:
http cmd.exe
IIS Serveur



- ISS RealSecure: console de configuration d'une sonde



ISS Real Secure: configuration d'une contre mesure



Display
Log DB
Etc.

- Système de détection d'intrusions: domaine public

- Très bon outils
  - Mais… demande du temps à mettre en œuvre et au suivi
  - Excellent comme outil didactique
- Projet Snort
  - http://www.snort.org
- Projet Prelude
  - http://www-prelude-ids.org

Système de détection d'intrusion: les limitations

- Ne pas se baser uniquement sur la mise en œuvre d'un IDS
  - Possibilité de contourner les IDS
  - Analyse comportementale
    - Nouvelles attaques pas connues !

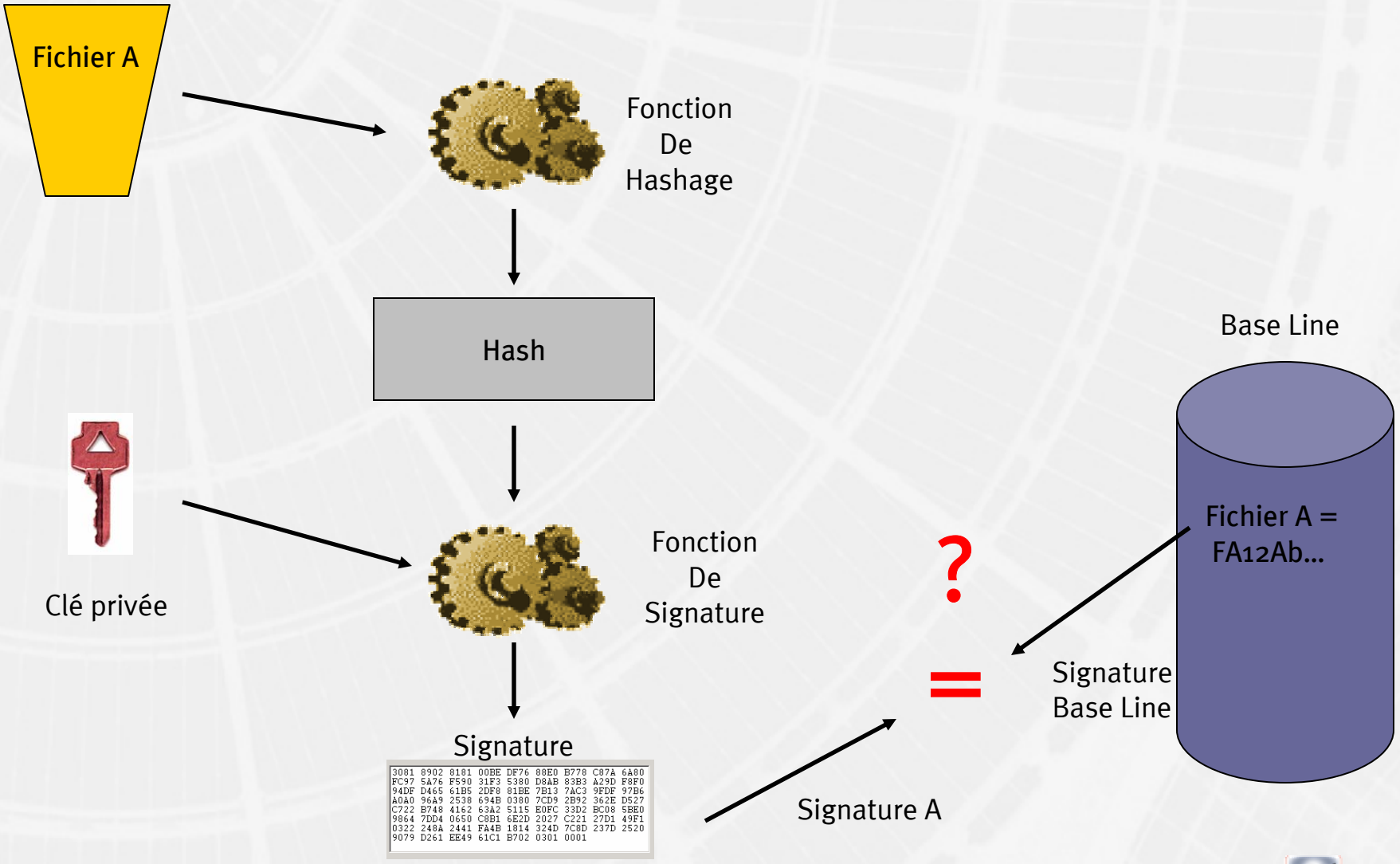
Contrôle d'intégrité des systèmes (FIA)

- Famille des IDS
- Outil très puissant pour détecter les altérations des systèmes
  - Complément des HIDS et NIDS
- FIA = File Integrity Assesment

Contrôle d'intégrité des systèmes (FIA): fonctionnement

- Utilisation de fonctions crytographiques
  - Fonctions de hashage (md5, sha1, etc,)
  - Fonctions de signatures électroniques (RSA, DSA)
- Création d'une « Base Line » des fichiers surveillés
  - « Photo du système »
- Comparaison régulière avec la « Base Line » de référence

Contrôle d'intégrité des systèmes (FIA): fonctionnement



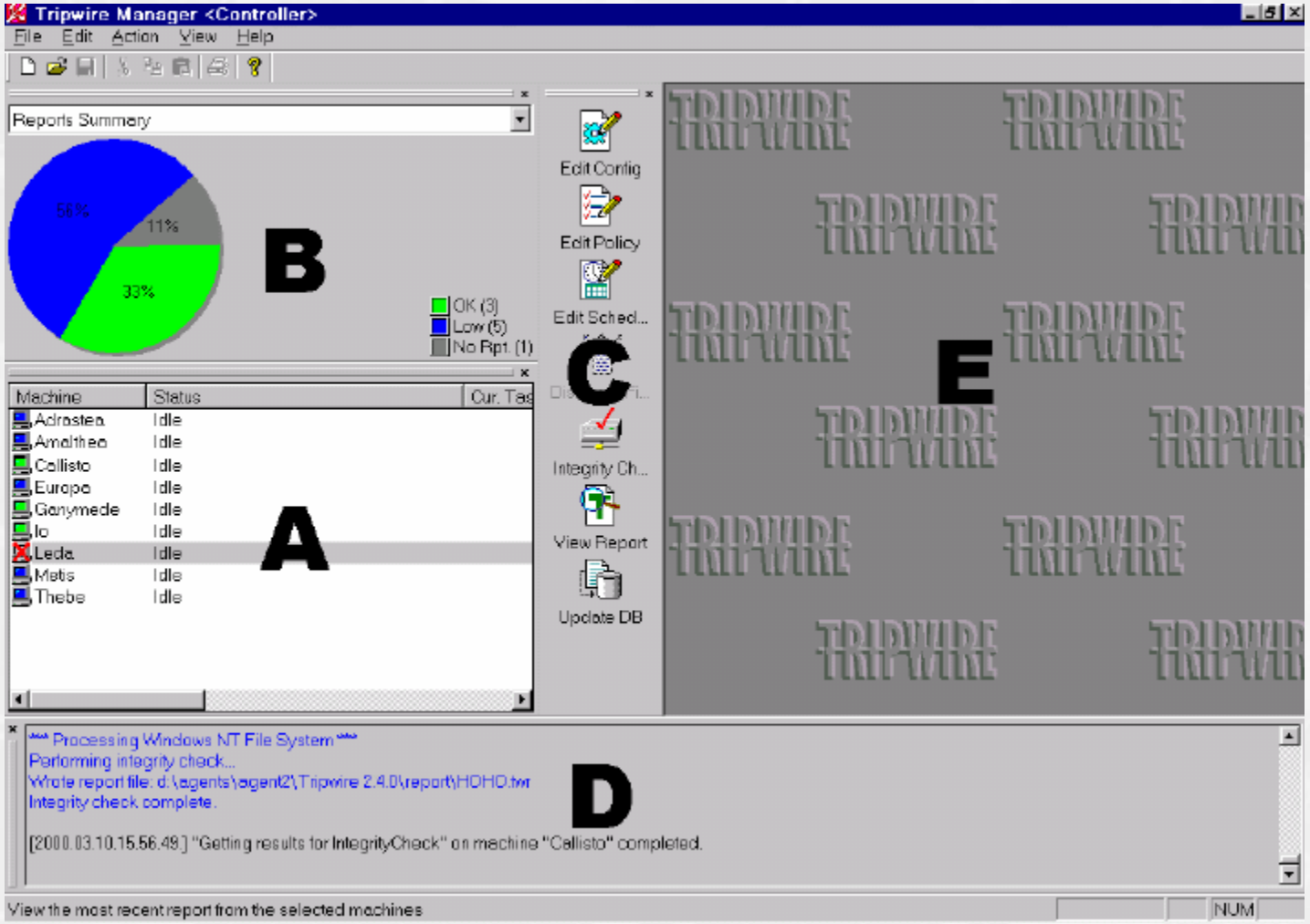
Contrôle d'intégrité des systèmes (FIA): mise en œuvre

- Définition des fichiers a surveiller
- Deux approches
  - Approche inclusive
  - Approche exclusive
- Définition du type de fichier
  - Logs, configuration, drivers, registry, etc.
- Définition de la périodicité des « Checks »
  - Attention ressources CPU
- Mise en production

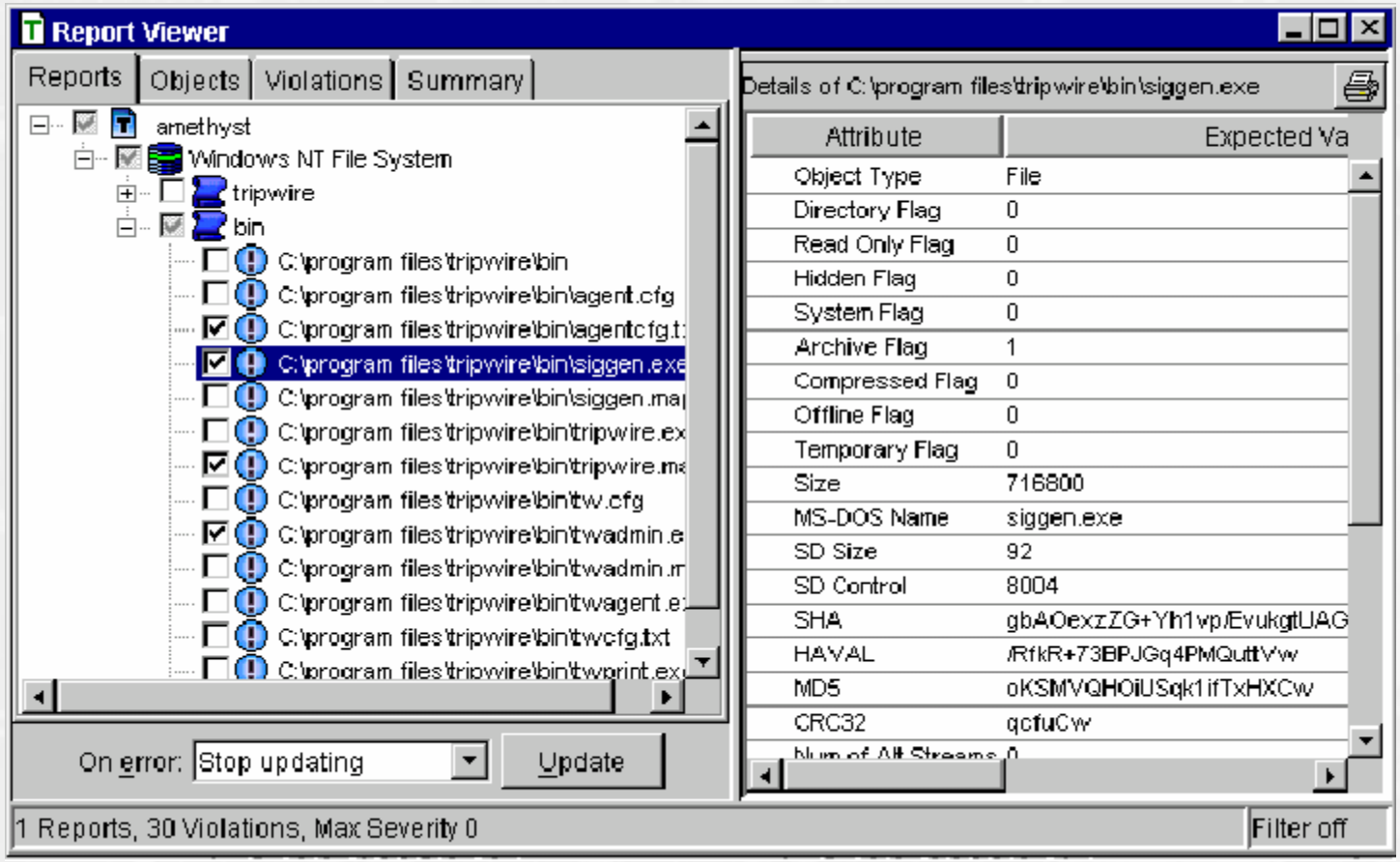
Contrôle d'intégrité des systèmes (FIA): Tripwire

- Leader du marché FIA
- Architecture distribuée
  - Tripwire server
  - Tripwire Manager (Console de management)
- Création de « Policy File »
  - Spécification « directory » et fichiers à surveiller
  - Maintenant avec un « Wizard » !

- Contrôle d'intégrité des systèmes (FIA): Tripwire Manager



- Contrôle d'intégrité des systèmes (FIA): Tripwire Reporting

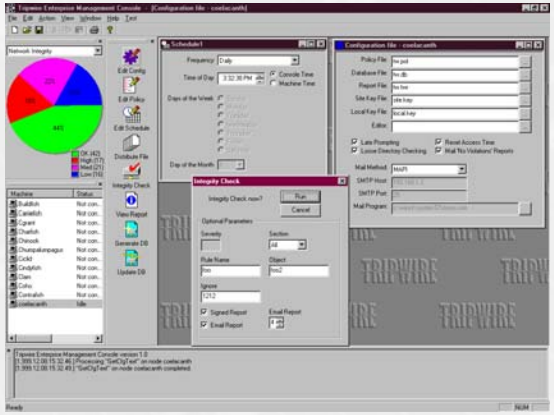


- Contrôle d'intégrité des systèmes (FIA): exemple d'implémentation

Unix
Solaris, Aix, HP, Linux

Cisco

Microsoft
NT 4.0, Win2K



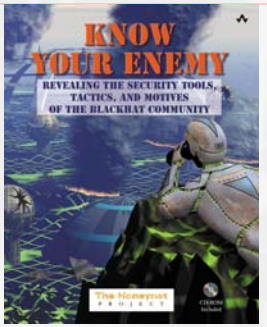
Web Serveur
IIS, Apache

- Leurres pour les « Black Hat »…
- Permet aux « Black Hat » d'attaquer et de compromettre le système
- But principal: apprendre les techniques d'attaques
  - Compléments aux IDS
  - Permet de déceler les attaques « à la source »
  - Un outil de recherche

Honeypot: fonctionnement

- Emulation d'un système ou de plusieurs systèmes d'exploitation
- Emulation d'une application ou de plusieurs applications (service)
  - Web Server, DNS, etc.
- Tous les accès sont « logger »
  - Tout trafic vers le Honeypot est considéré comme suspect !

Honeypot: références



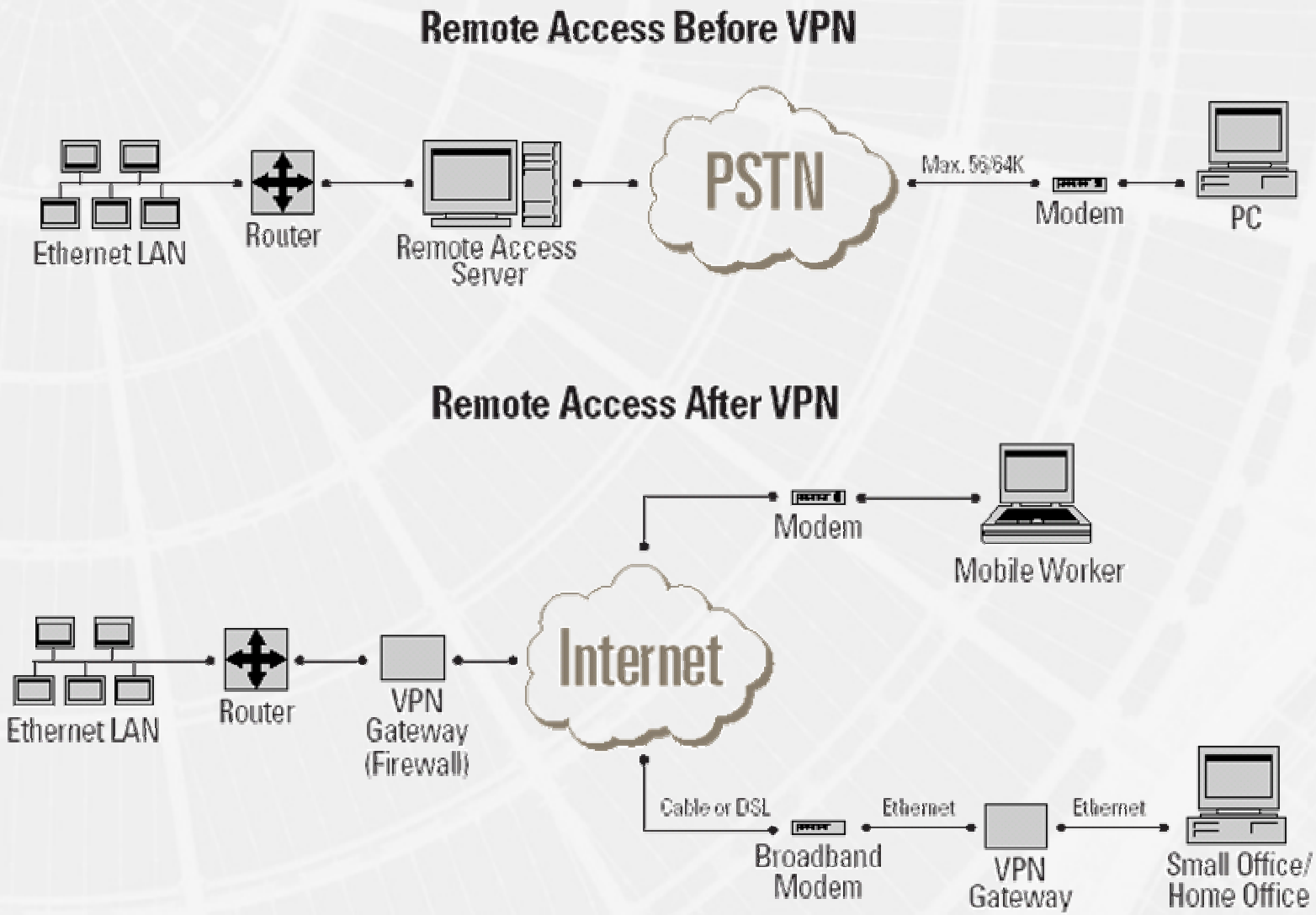
- Projet Honeynet
  - http://project.honeynet.org
  - http://www.tracking-hackers.com
- Produits
  - ManTrap
  - Specter
  - Back Officer Friendly
  - Honeyd
  - Deception Tool Kit
- Livre: Know You Enemy

VPN

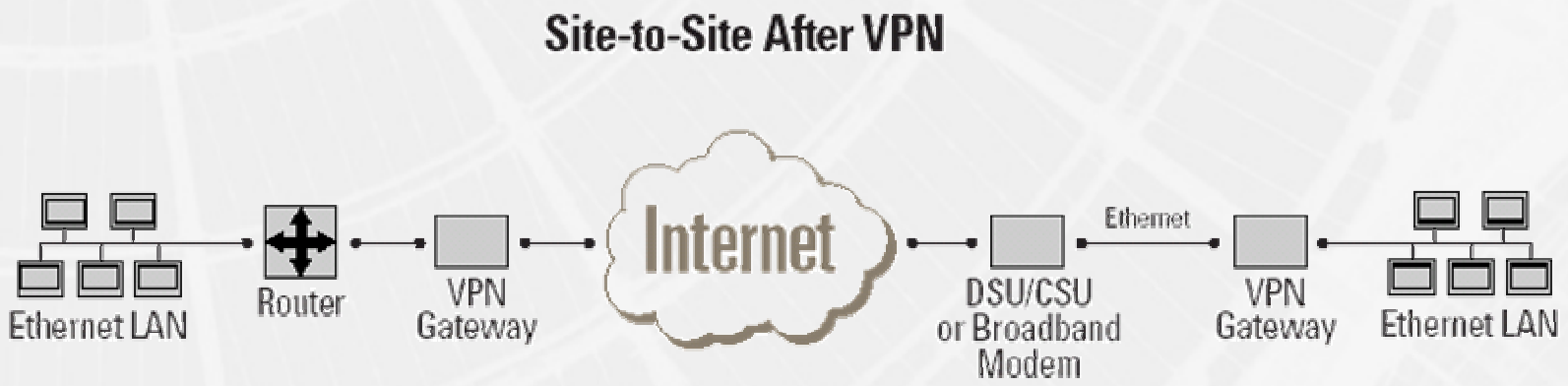
- Technologie pour sécuriser les communications
  - Intégrité
  - Authentification
  - Confidentialité
- Plusieurs approches
  - IPSEC
  - SSL
  - SSH
  - PPTP
  - L2TP
  - Etc.

- Différentes topologies
  - Client à site (Accès distant)
  - Site à site
  - Client à serveur
  - Serveur à serveur
  - Client à client

- Exemple VPN: Accès distants



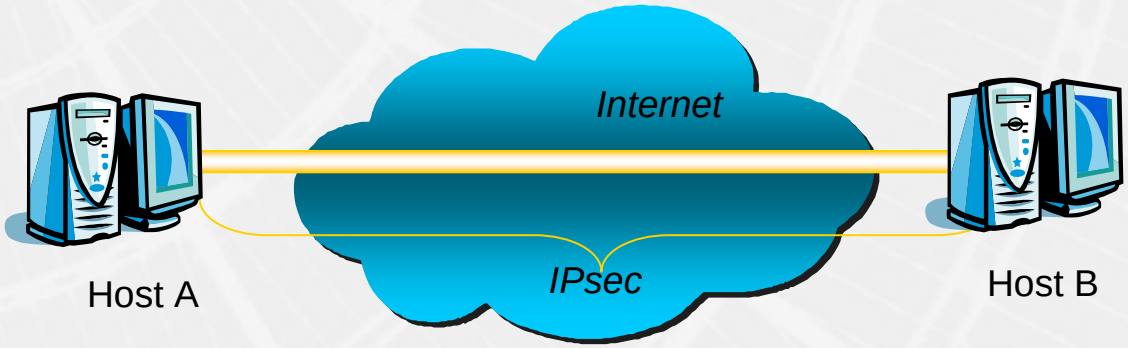
- Exemple VPN: Site à site



- IPSEC = IP Security
- IETF (RFCs 2401-2406)
- Fournit du chiffrement et intégrité au paquets IP
  - Authentification mutuelle
- Support de PKI
  - Certificat pour les « gateway »
  - Certificat pour les clients
  - Support de la révocation

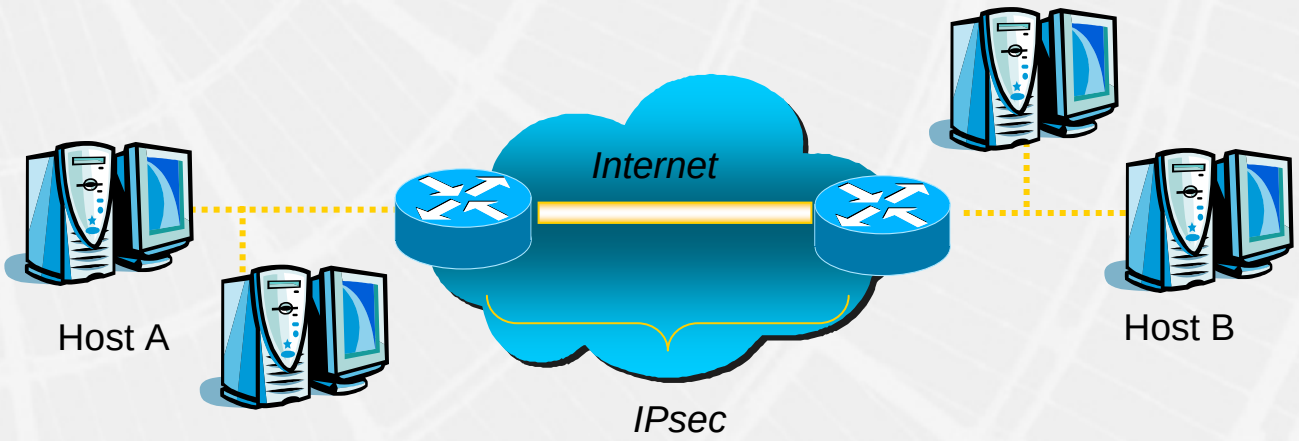
- Deux option de sécurité
  - AH: Intégrité et authentification
  - ESP: Intégrité, authentification et confidentialité
- AH et ESP peuvent être utilisé en:
  - Mode Transport
  - Mode Tunnel

IPSEC: Transport Mode



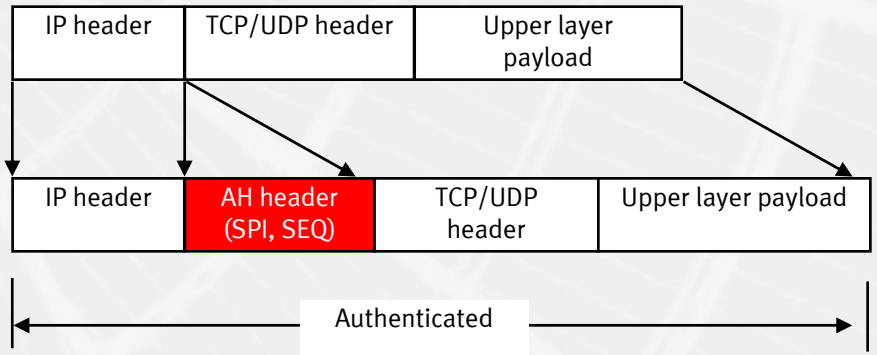
Source: SSH.COM 2002

IPSEC: Tunnel Mode

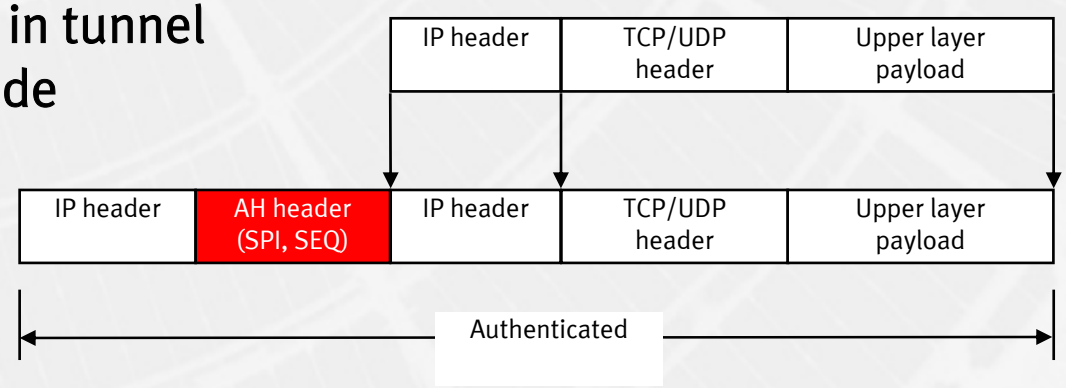


Source: SSH.COM 2002

AH in transport mode



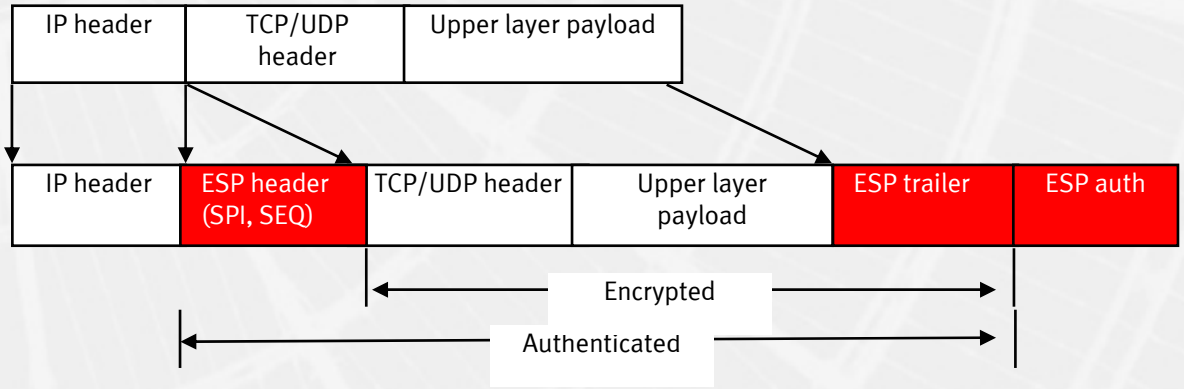
AH in tunnel mode



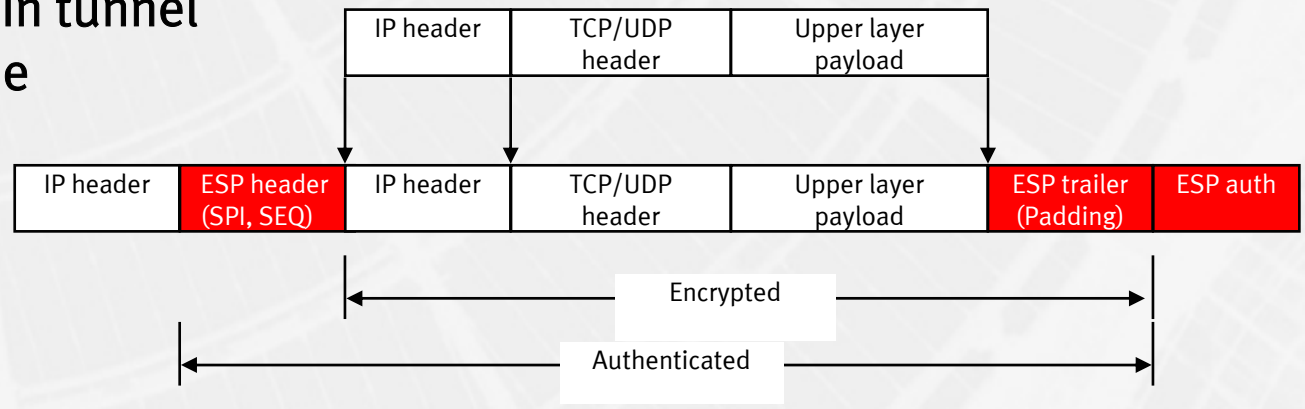
Source: SSH.COM 2002

IPSEC: ESP

ESP in transport mode

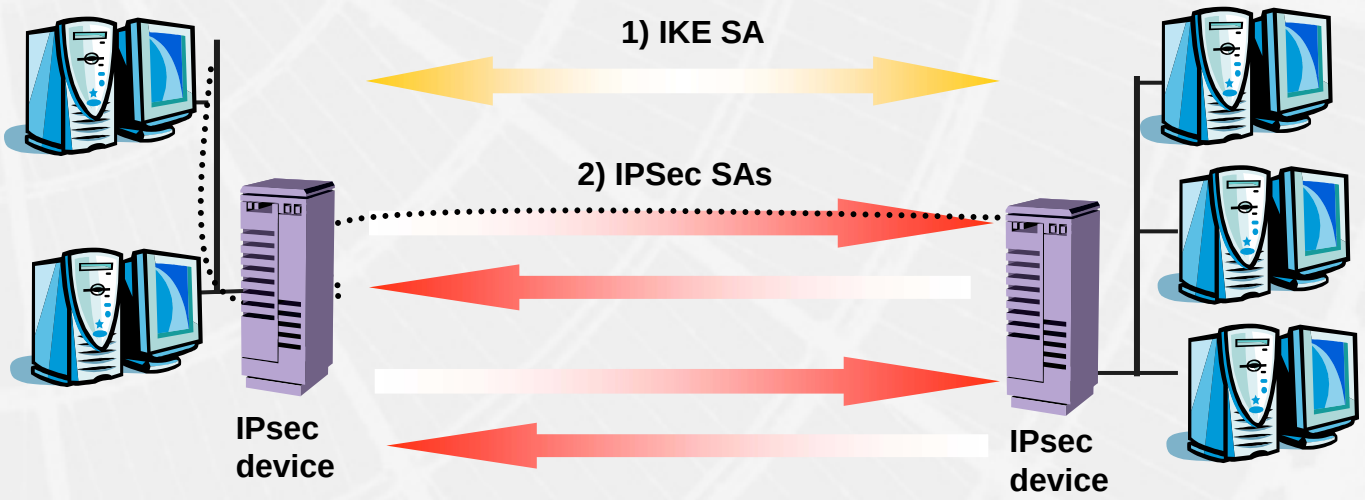


ESP in tunnel mode



Source: SSH.COM 2002

IPSEC: échange des clés (IKE)



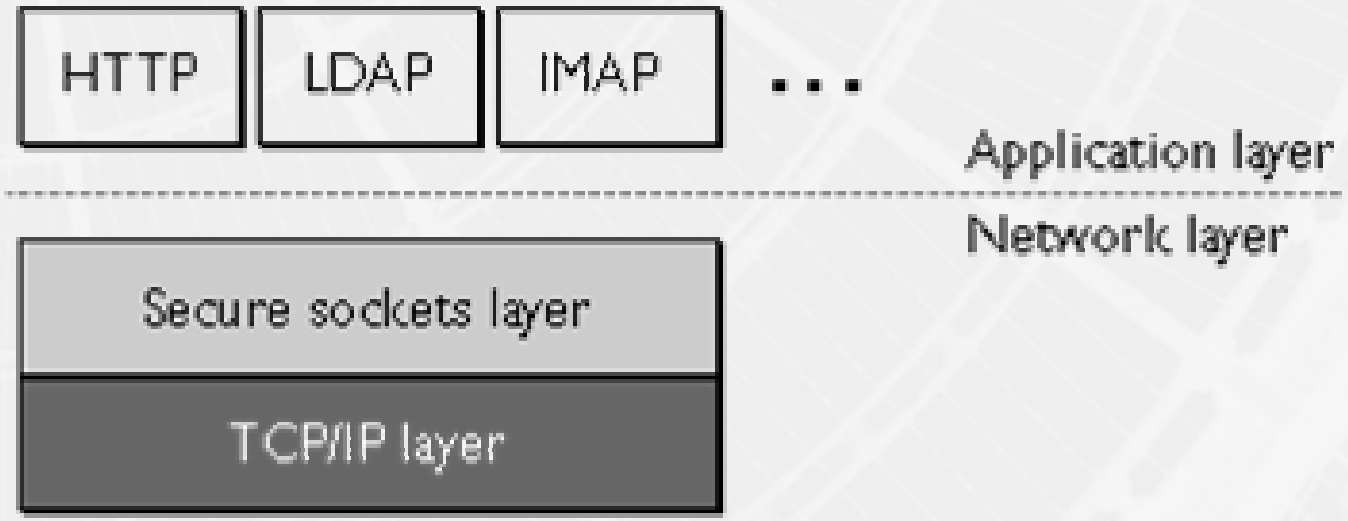
Source: SSH.COM 2002

SSL: technologie PKI par excellence

- Secure Sockets Layer TCP/IP socket encryption
- Fournit des mécanismes de protection des communications
  - Confidentialité
  - Contrôle d'intégrité
  - Authentification
- Utilise la technologie PKI (certificat) pour l'authentification du serveur et la négociation SSL
  - Certificat public (Verisign, Thawte, etc.)
- Eventuellement peut authentifier le client (option)
  - PKI Interne par exemple

- SSL v1 par Netscape en 1994
  - Usage Interne seulement
- SSL v2 avec Navigator 1.0 and 2.0
- SSL v3 dernière version
- TLS v1 repris par l'IETF
  - Aka SSL v3.1

- Entre la couche applicative et TCP

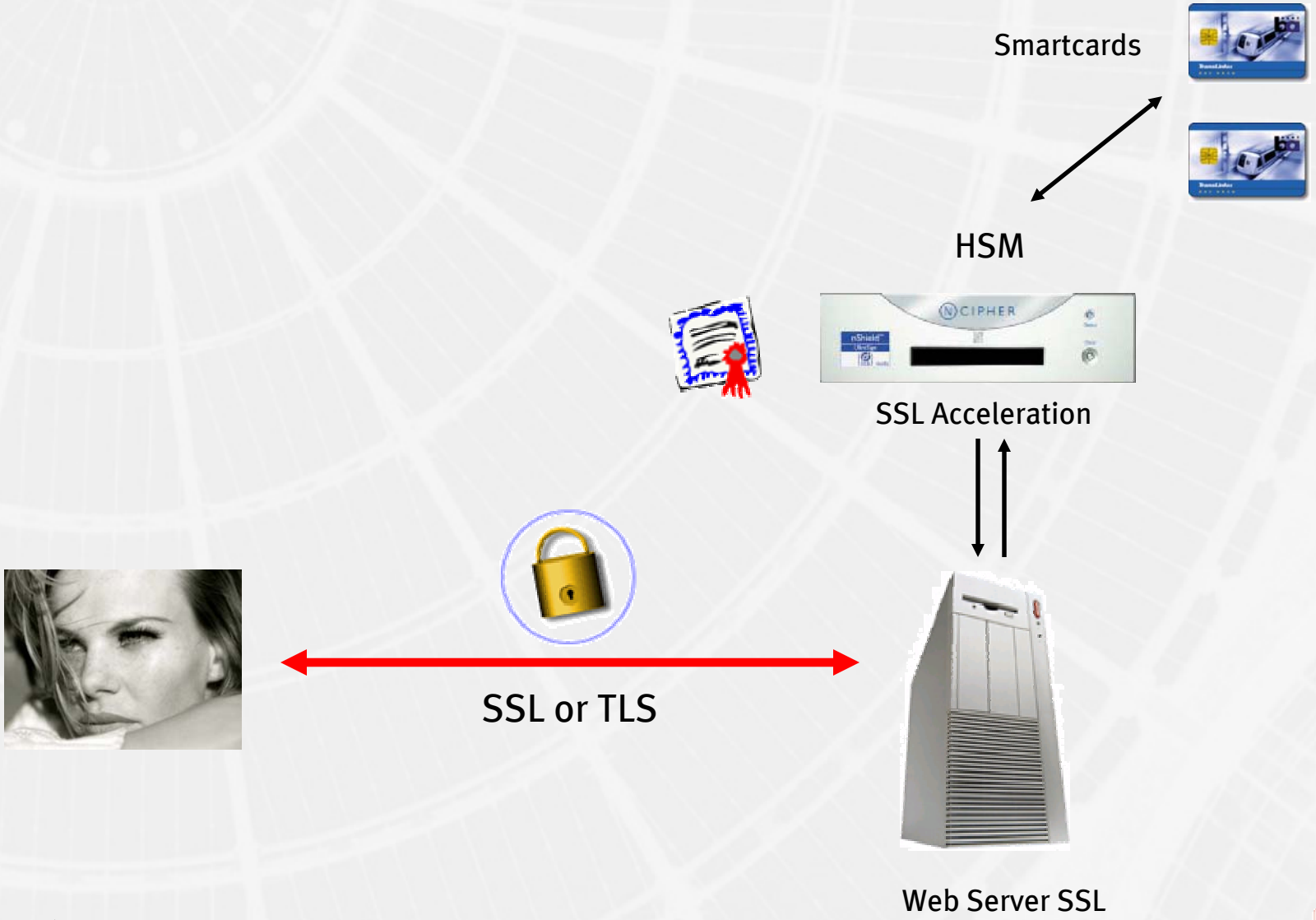


Ports SSL (IANA)

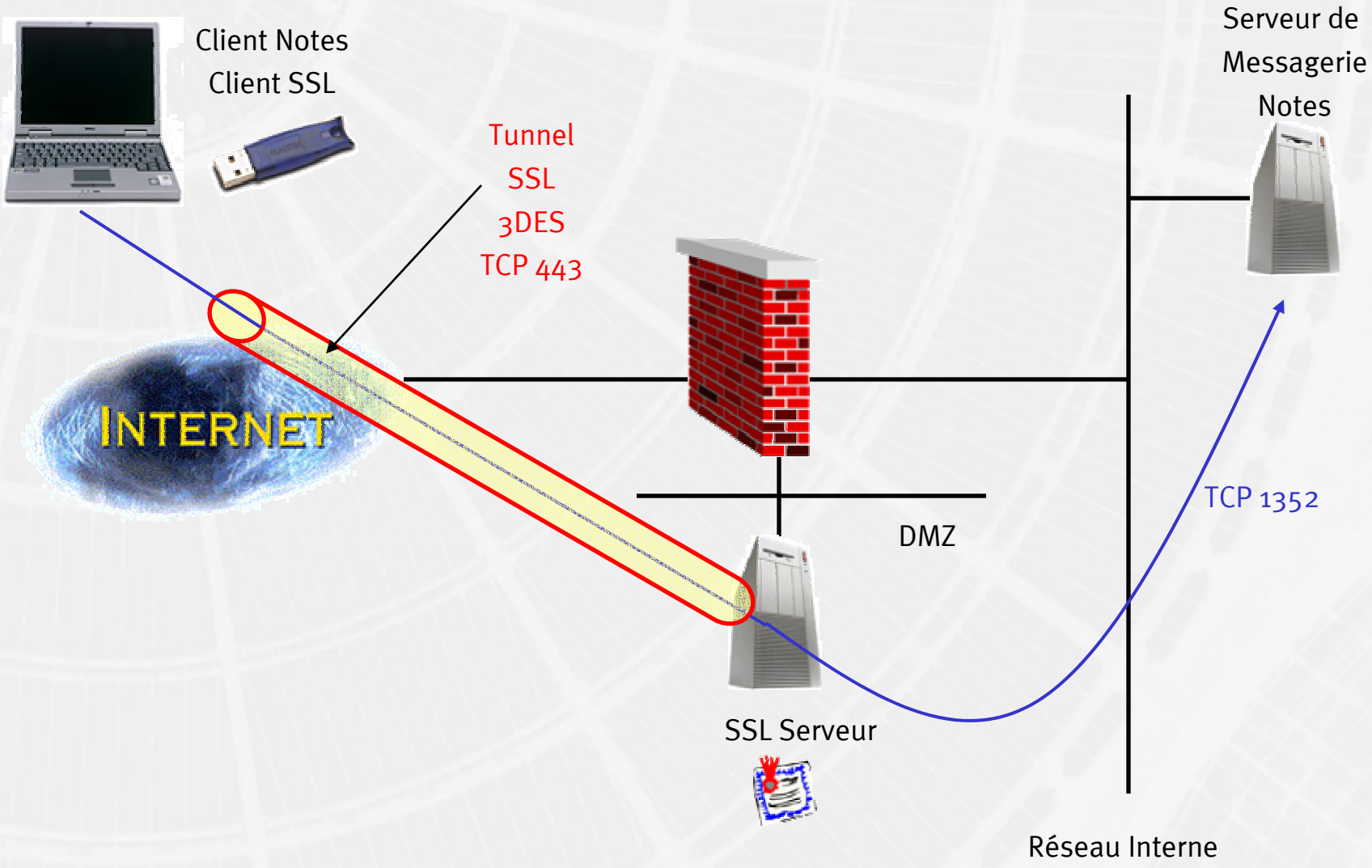
- nsiiops 261/tcp # IIOP Name Service over TLS/SSL
- https 443/tcp # http protocol over TLS/SSL
- smtps 465/tcp # smtp protocol over TLS/SSL (was ssmtp)
- nntps 563/tcp # nntp protocol over TLS/SSL (was snntp)
- imap4-ssl 585/tcp # IMAP4+SSL (use 993 instead)
- sshell 614/tcp # SSLshell
- ldaps 636/tcp # ldap protocol over TLS/SSL (was sldap)
- ftps-data 989/tcp # ftp protocol, data, over TLS/SSL
- ftps 990/tcp # ftp protocol, control, over TLS/SSL
- telnets 992/tcp # telnet protocol over TLS/SSL
- imaps 993/tcp # imap4 protocol over TLS/SSL
- ircs 994/tcp # irc protocol over TLS/SSL
- pop3s 995/tcp # pop3 protocol over TLS/SSL (was spop3)
- msft-gc-ssl 3269/tcp # Microsoft Global Catalog with LDAP

- SSL: authentification client avec certificat X509

- SSL: sécurisation du serveur (HSM)



SSL / TLS tunneling



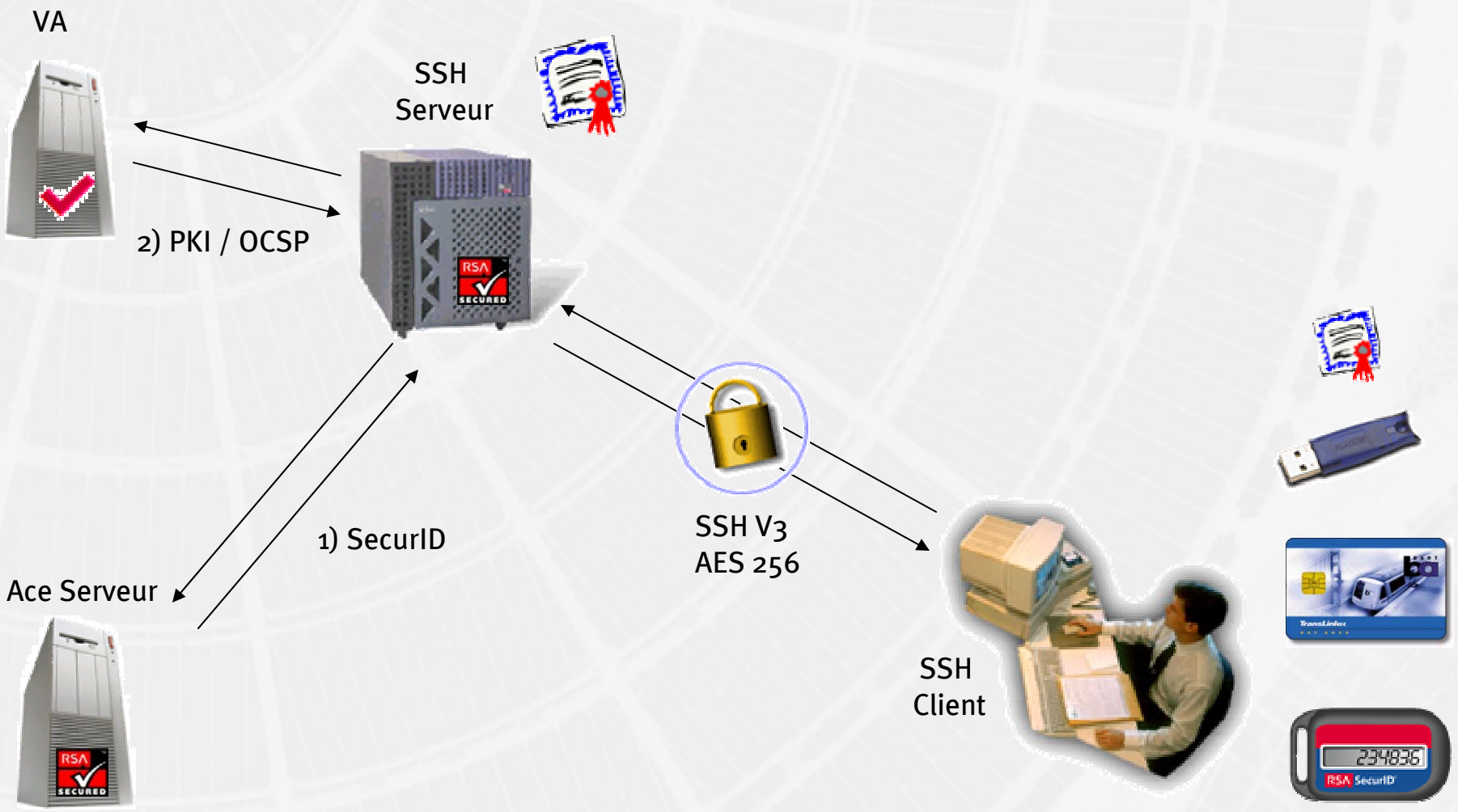
SSH

- Famille des VPN
- SSH = Secure Shell
- Defacto Standard maintenant
  - Environ 8 millions utilisateurs
- Solution de remplacement de telnet, ftp et les commandes R (Unix)
- Existe pour toutes les plates-formes Unix et aussi NT
- Fournit
  - Chiffrement (AES, DES, 3DES, etc.)
  - Intégrité
  - Authentification
- Très recommander dans les environnements UNIX
- Simple à mettre en œuvre

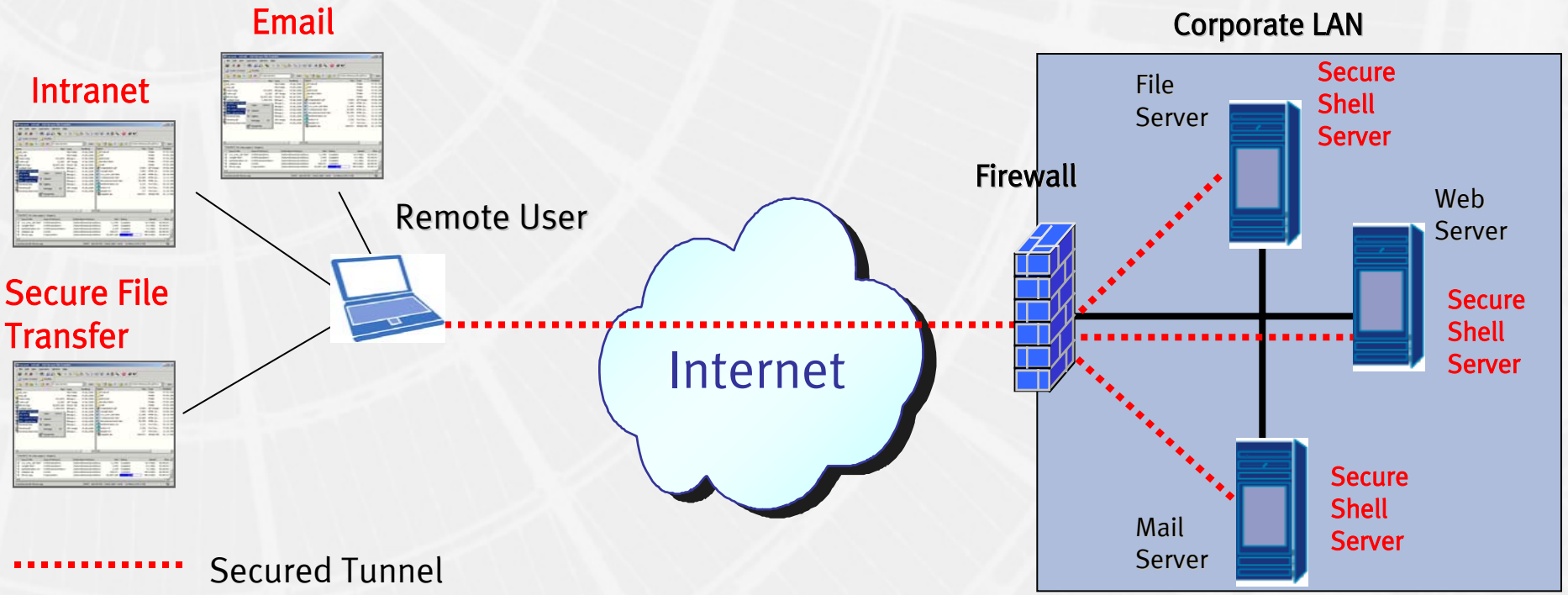
SSH: système d'authentification

- Supporte plusieurs modes d'authentications
- Authentifications « Classiques »
  - SecurID
  - Public Key
  - Pam
  - Kerberos
  - Etc.
- Authentifications basées sur PKI
  - Utilisation d'un certificat X509
    - Smartcard ou clé USB
  - Validation des certificats (OCSP ou CRL)
- Solutions éprouvées et robustes

- Exemple d'implémentation SSH: authentification forte



- Solution VPN avec SSH



Chiffrement de fichiers

- Deux approches
  - Chiffrement du disque dur
  - Chiffrement de certains fichiers
- Bonne solution pour les « laptop »
- Intégration avec les cartes à puces ou USB
- Gestion des clés de chiffrement
  - Key Recovery !
- Chiffrement de base de données

- Carte à puce ou Smartcard (ISO 7810 54x85x0.8mm)
- Carte mutli-applications
  - Pay TV
  - Banques (EC, Carte bleu, Visa, etc.)
  - GSM
  - Médical
  - Informatique
  - Etc.

- Souvent couplée au stockage des clés privées et certificats X509 (PKI)
- Peux contenir des « Credentials »
  - Windows NT4, voir 2000
  - Reduce Sign-On
- Fournit de l'authentification forte
  - PIN et la carte
- Protégées contre la « Brute Force »

- Deux types de cartes
  - Carte mémoire
  - Carte avec un Processeur Cryptographique (RSA, DSA, etc.)
- Applications:
  - Sign Sign ON (Windows 2000 et PKINIT)
  - Messagerie
  - Chiffrement de fichiers
  - Signature de documents
  - Portail Web
  - VPN (Accès distant)
  - Etc.

Tokens USB

- Même approche que les cartes à puces
- Deux types de cartes
  - Carte mémoire
  - Carte avec un Processeur Cryptographique (RSA, DSA, etc.)
- Moins de sécurité que les cartes à puces
  - Accès physique moins compliqué
- Grand succès pour les postes nomades

- Exemple avec Windows 2000: Smartcard Logon

PIN Number

Support natif des cartes à puces
Norme PC/SC Crypto API

- Sécurisation de l'accès aux serveurs
  - Authentification forte (SecurID, Carte à puce, etc.)
  - Technologie VPN (SSH, IPSEC, etc.)
- Mise en œuvre d'une politique d'application des « Patchs »
  - Machines de tests
  - Backup
- Mise en place d'une politique de backup
- Segmentation (firewall)
- Haute disponibilité (HA)

- Sécurisation de l'OS
  - Restriction des services
  - Accounting (Syslog, SNMP, etc.)
  - FIA
  - Blindage du stack IP (DoS)
  - Firewall (ACL, TCP Wrapper, etc.)
  - Gestion des droits
  - Jail (UNIX)
  - Analyse comportementale
  - Etc.

Sécurisation des postes clients

- L’accès à Internet amène des problématique de sécurité pour les postes de travail
  - Virus, Pests, Trojan, Backdoor
  - Lié à la messagerie et au surf
- L’idée est de garantir l’intégrité des postes
- Ces postes ont accès à des informations sensibles
  - ERP, Back Office, Bases de données, etc.
- La problématique pour la sécurisation:
  - Gestion du parc des postes de travail

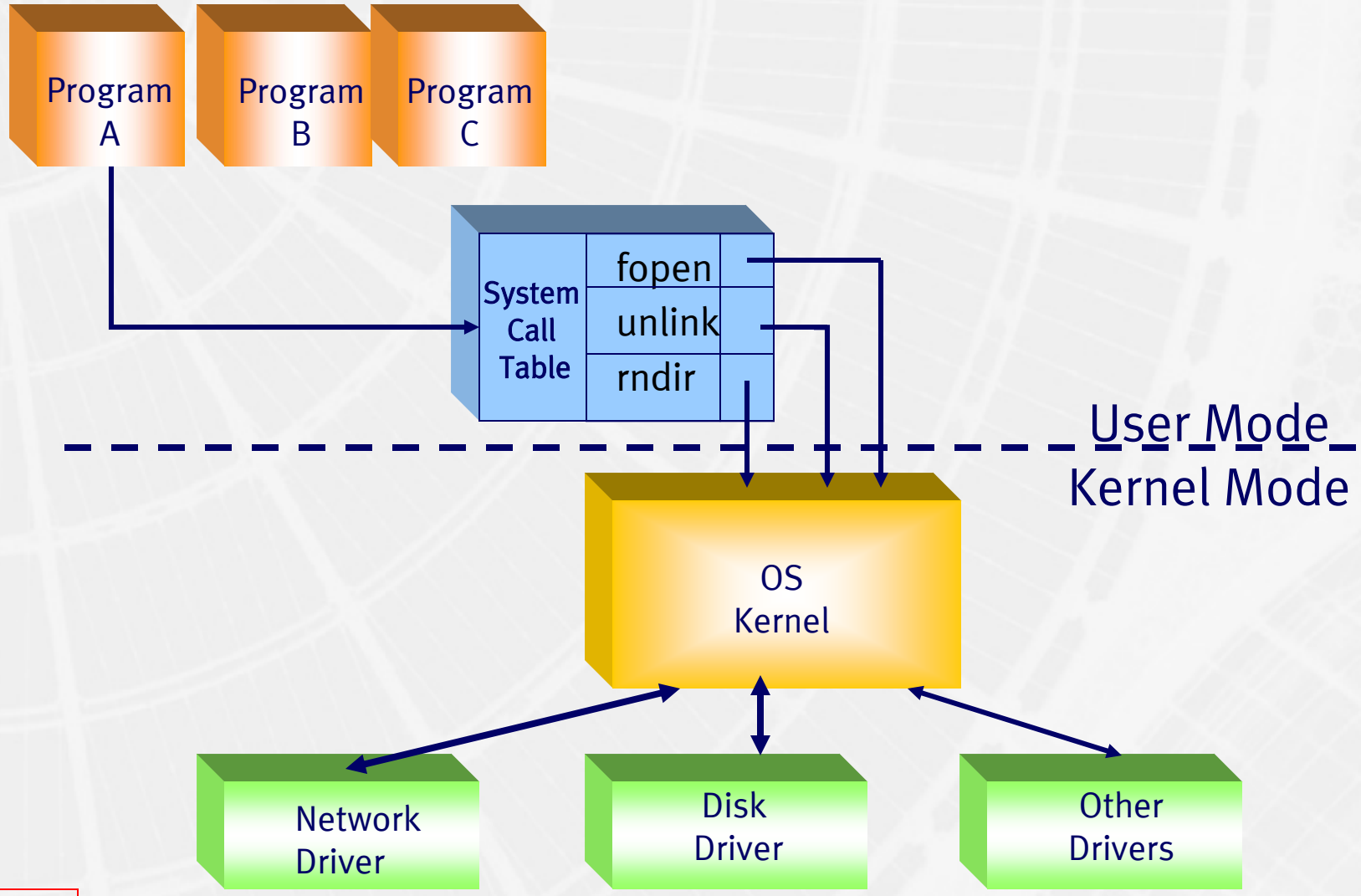
Sécurisation des postes clients

- L'approche classique
  - Anti Virus
  - Gestion des droits (par exemple GPO Win2k)
- La tendance
  - Firewall personnel
  - Analyse comportementale
  - Contrôle des codes mobiles
  - Contrôle d'intégrité (FIA)
  - Authenfication forte

- Fonctionnalités de base
  - Filtrage IP en entrée et sortie
  - Lien entre les filtres et les applications
  - Apprentissage automatique (POP-UP)
- Fonctionnalités avancées
  - Code mobiles (Sandbox)
  - Contrôle des cookies
  - IDS
  - Analyse du comportement
  - Etc.

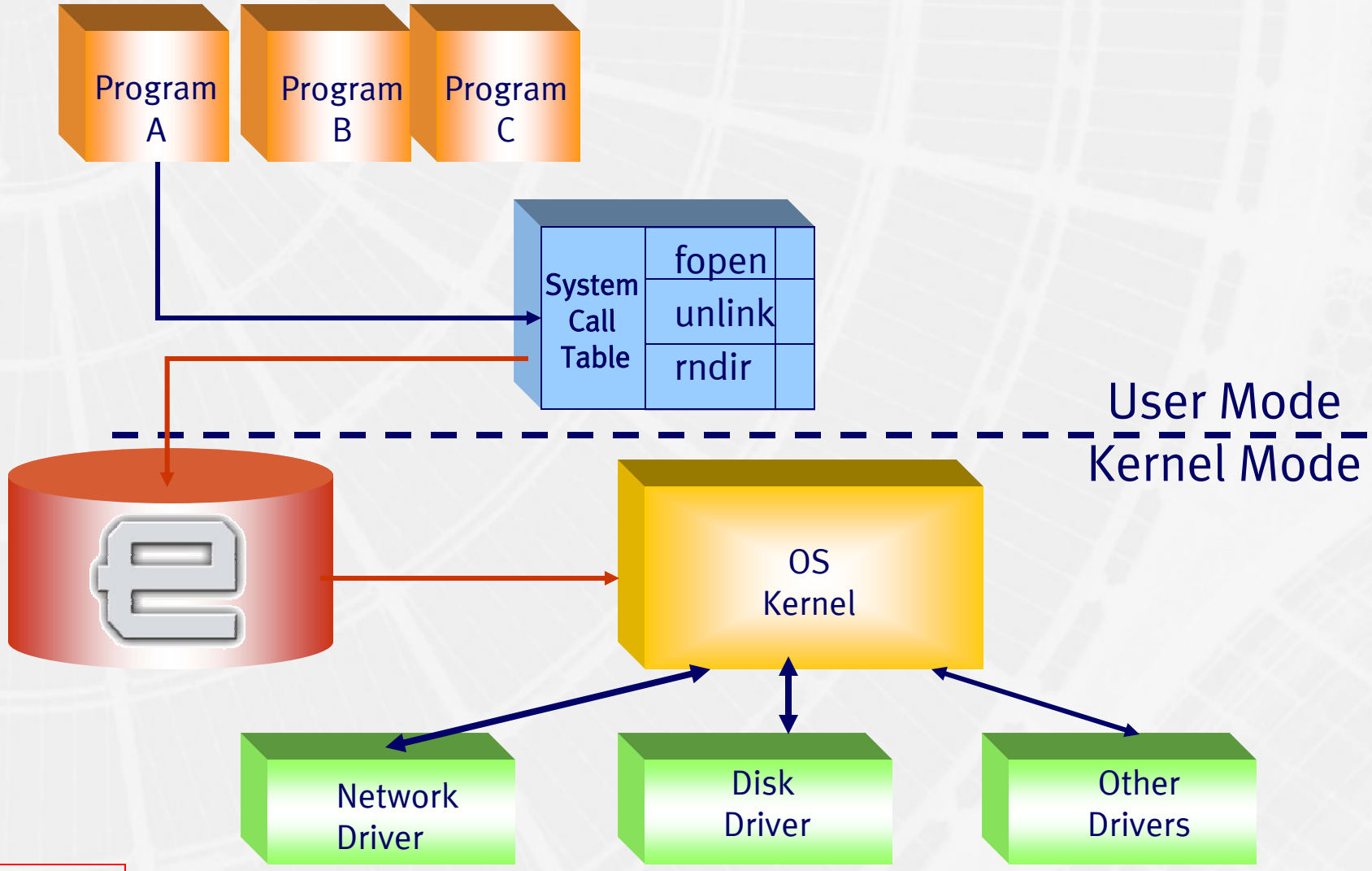
- Nouveaux outils de sécurité
  - Prévention des intrusions
- Capable de bloquer les attaques inconnues
  - Détecte les intrusions et les bloques
- Blocage des attaques de BoF
  - (60% des attaques selon le CERT 2002)
- Simple à mettre en œuvre

- System Call Interception : la technologie de base



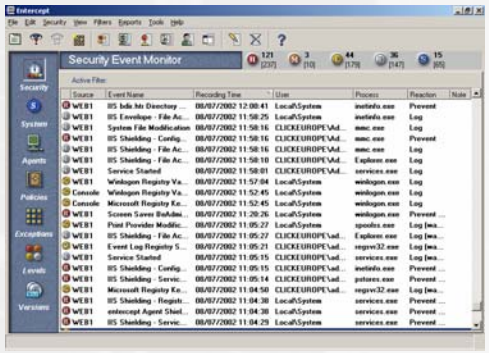
Source: Entercept 2002

- System Call Interception: la technologie de base



Source: Entercept 2002

Solution Entercept



Notification

Reporting

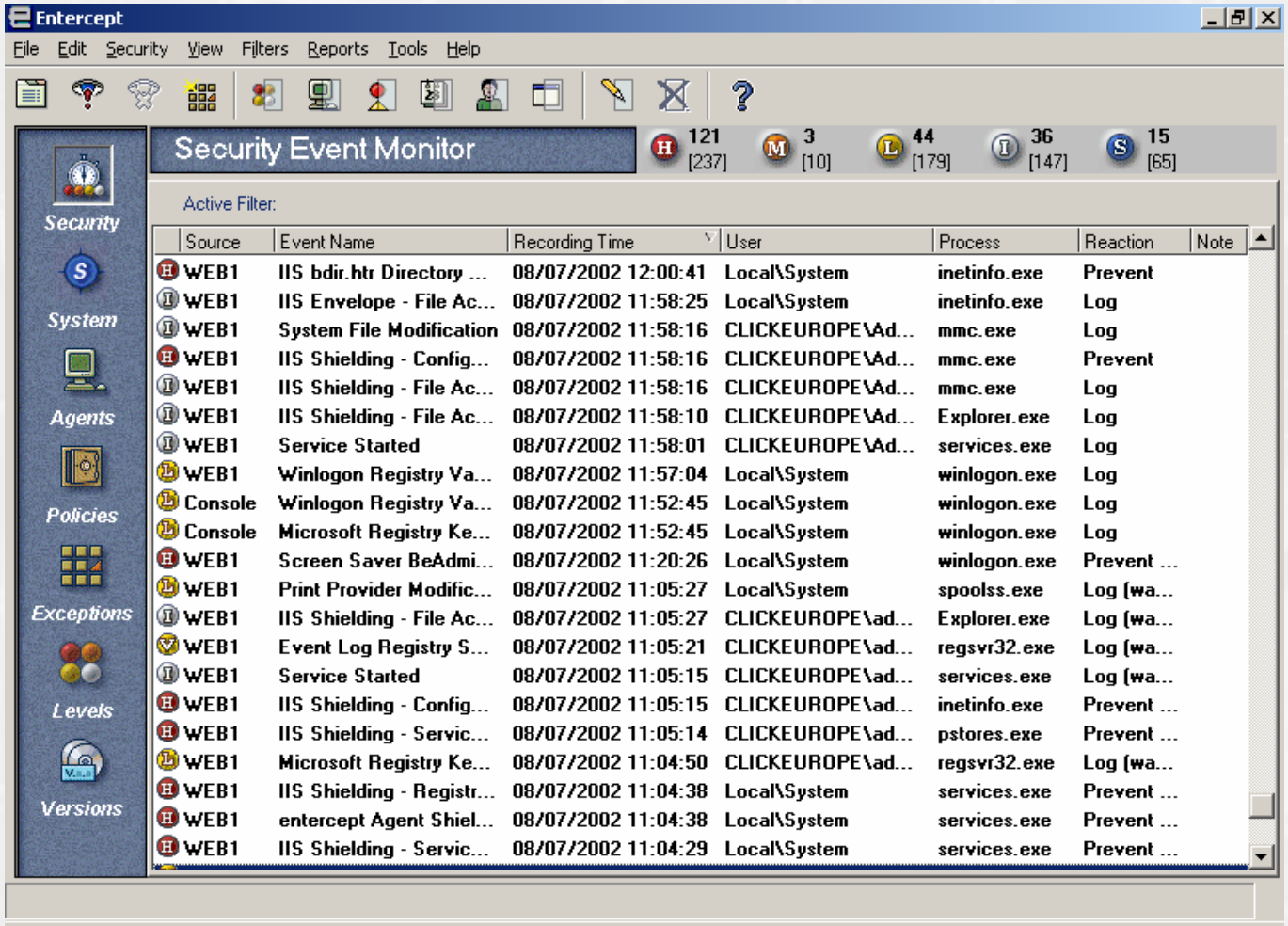
Management

Serveur NT et 2000

Serveur WEB

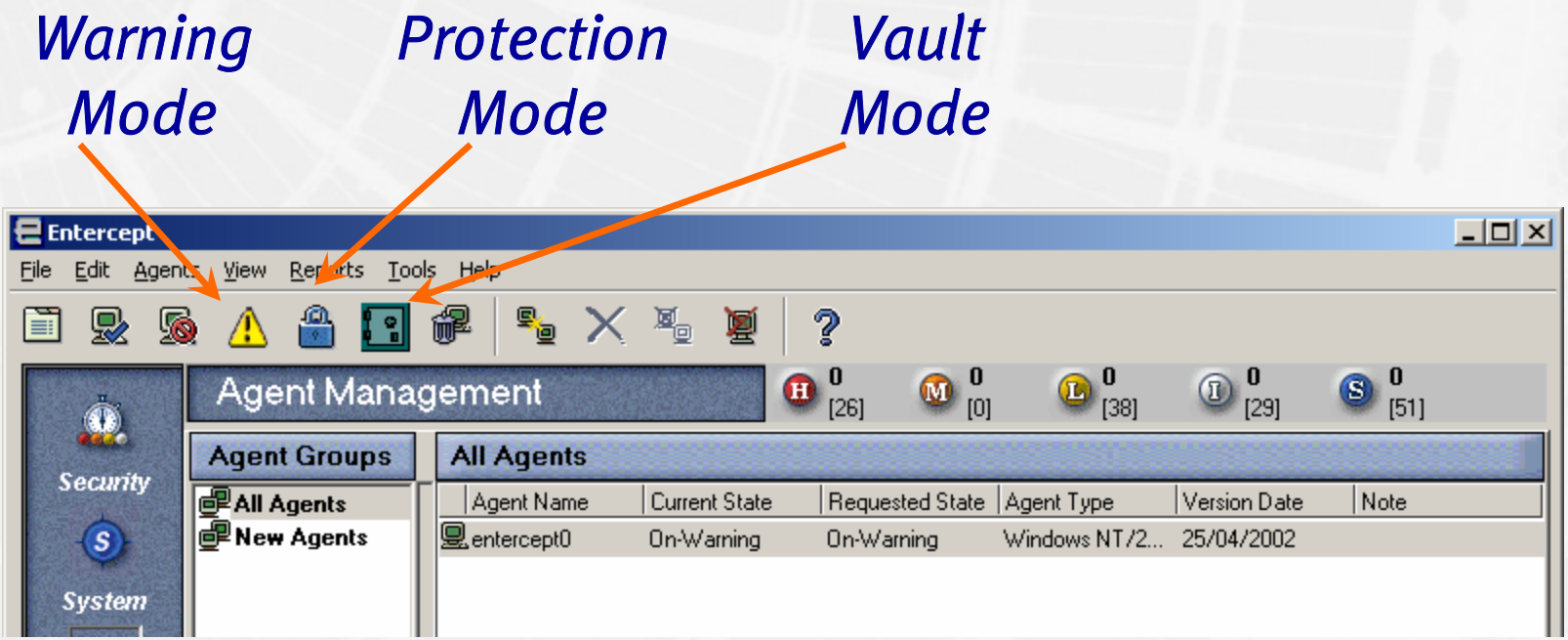
Serveur Unix

Entercept: Console



Source: Entercept 2002

- Entercept: SecureSelect



Increasing Security

Source: Entercept 2002

S/MIME

- Secure Mime
  - Solution de sécurisation de la messagerie
- Standard IETF
  - Microsoft, Lotus, Laboratoires RSA, etc.
- Services de sécurité
  - L'authentification
  - La confidentialité
  - L'intégrité
  - La non-répudation

S/MIME

- Utilise la technologie PKI
  - Certificats personnels X509
  - Autorité de certification publique ou privée
- Support des algorithmes symétriques
  - DES, 3DES, RC2, etc.
- Application très simple à utiliser
  - Support natif dans Outlook, Lotus, Netscape, etc.

S/MIME

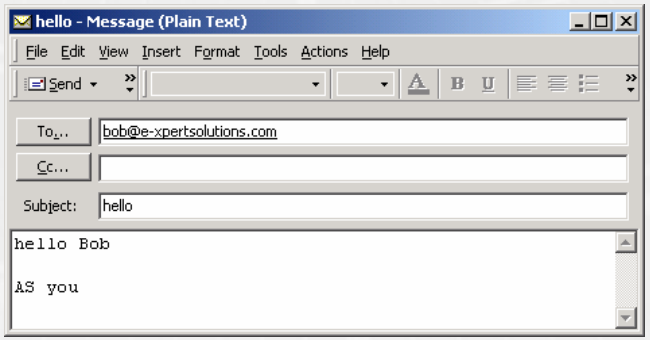
Autorité
de certification
public ou privée

Certificat
Personnel

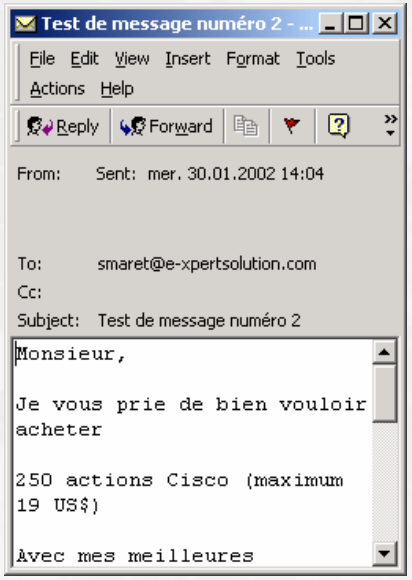
Bob

Alice

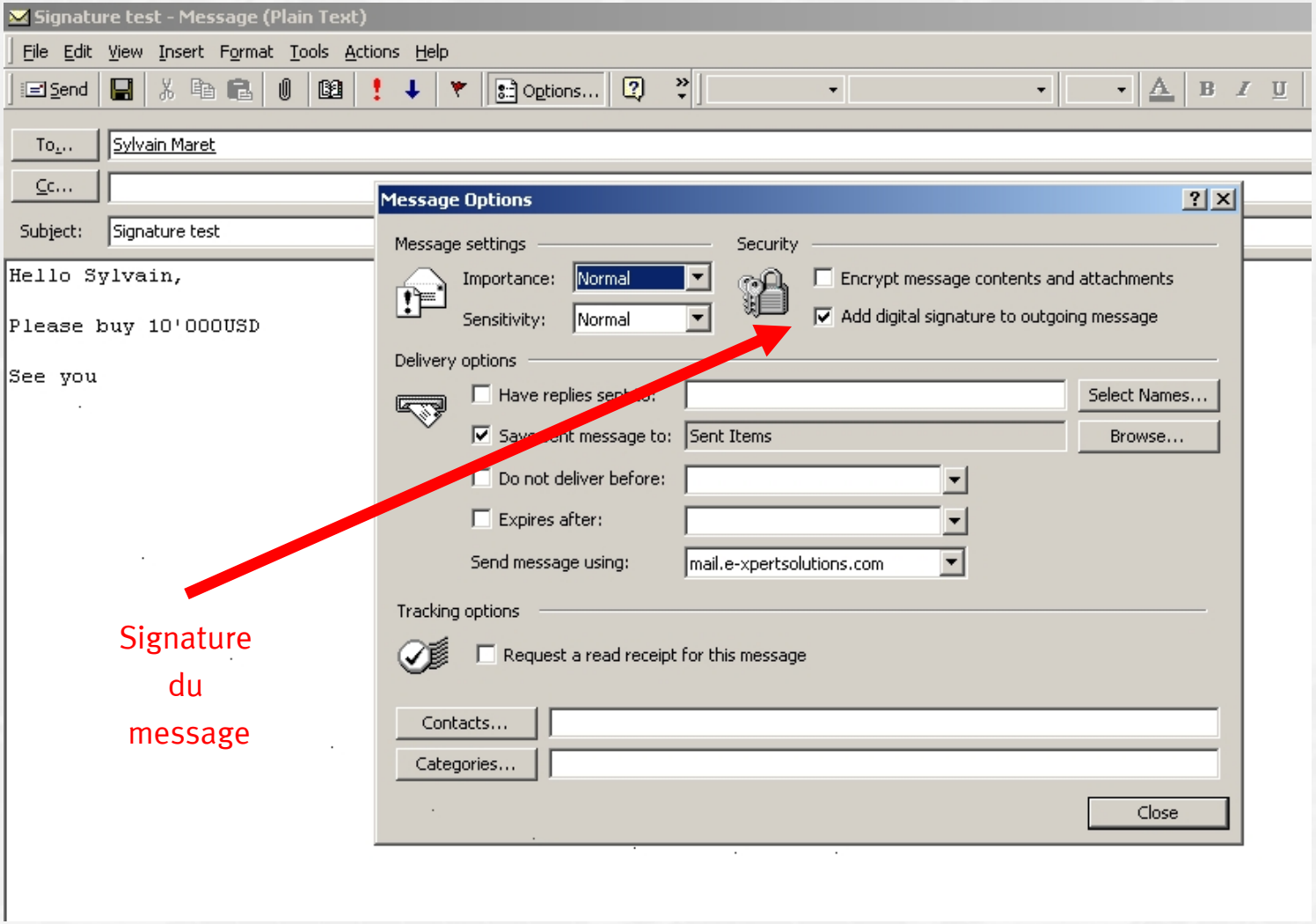
Certificat
Personnel



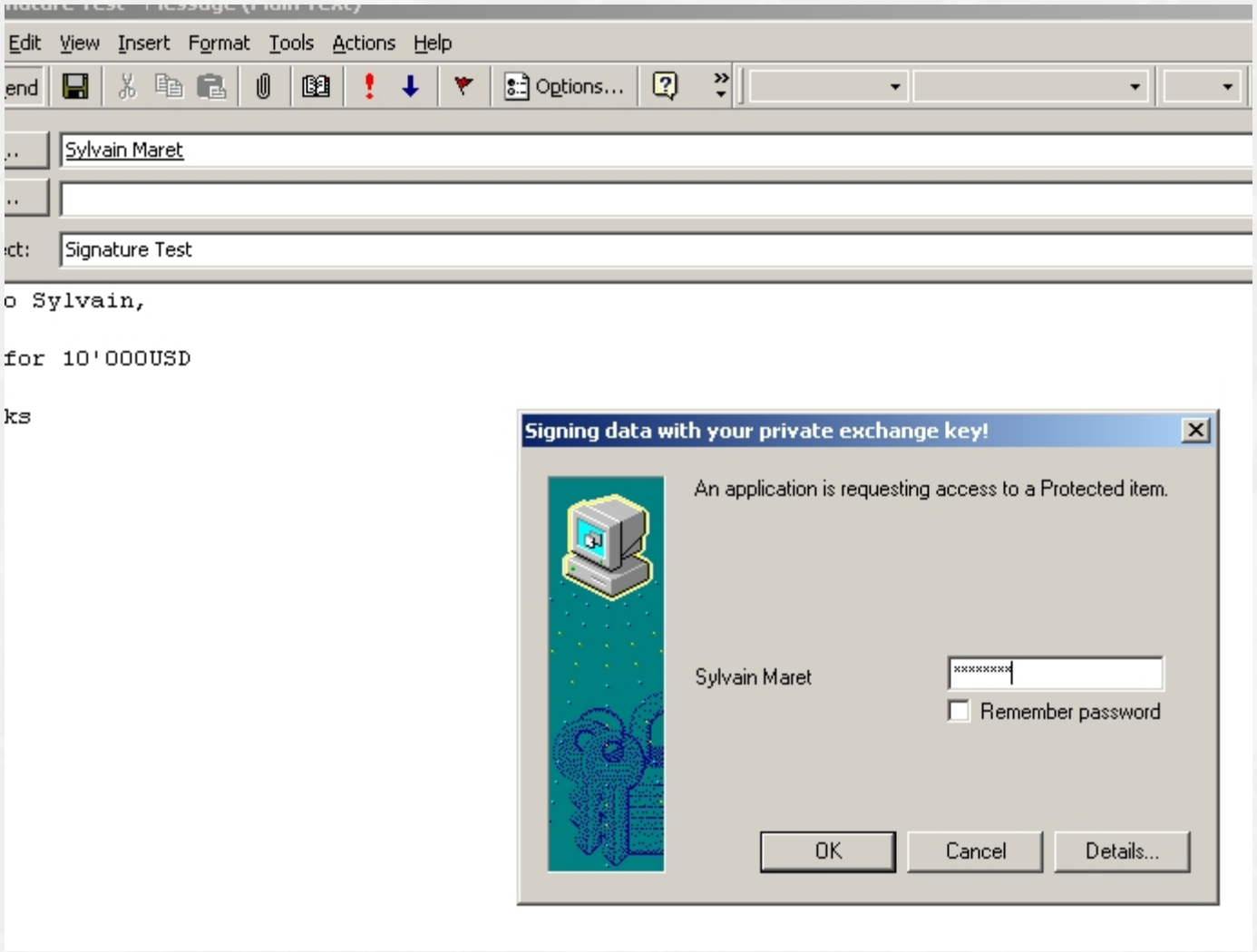
S/Mime
3DES / RSA Signature



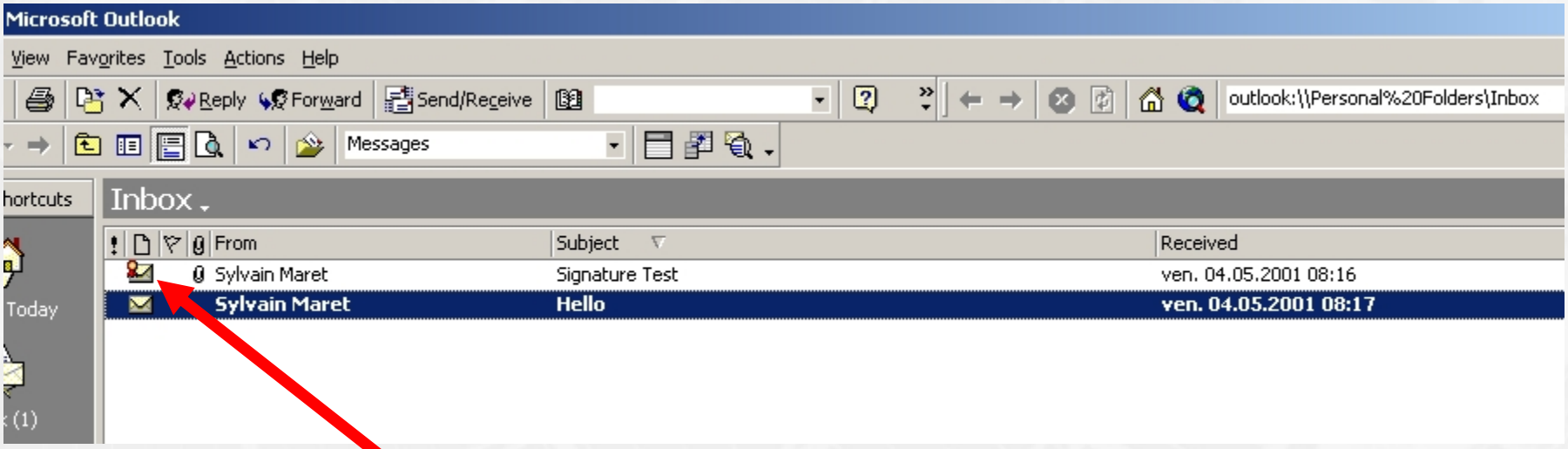
S/MIME: exemple avec Outlook



- S/MIME: exemple avec Outlook

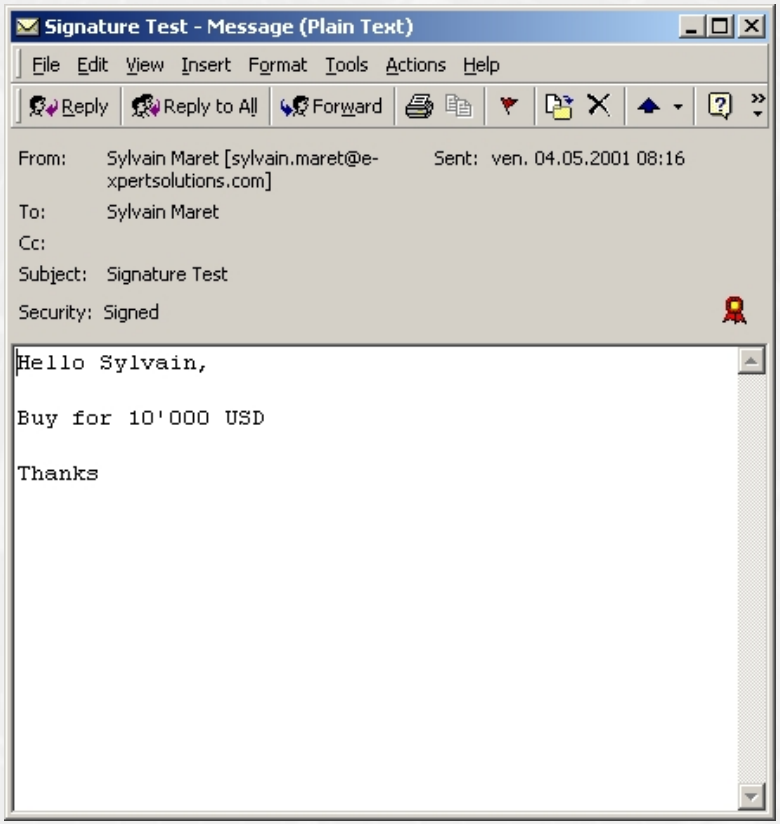


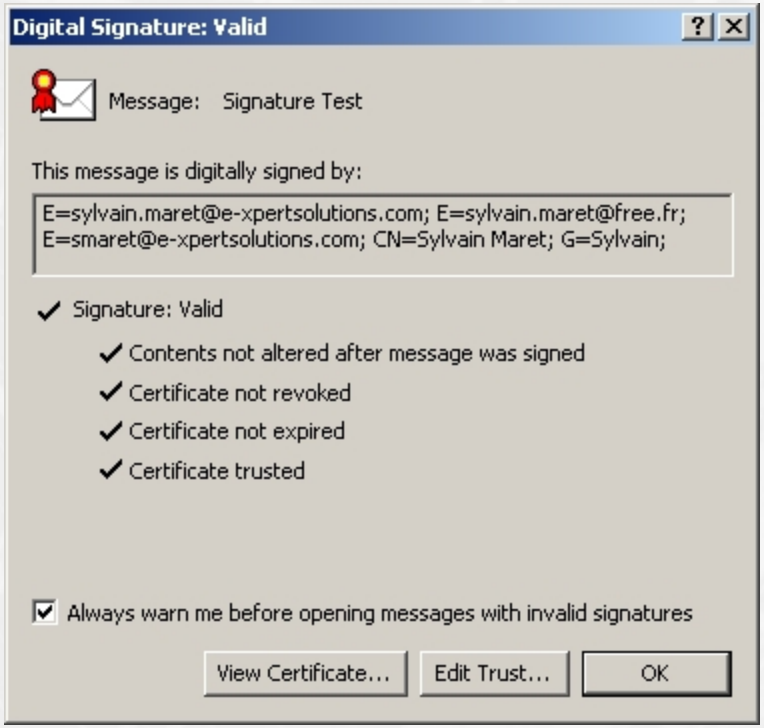
- S/MIME: exemple avec Outlook



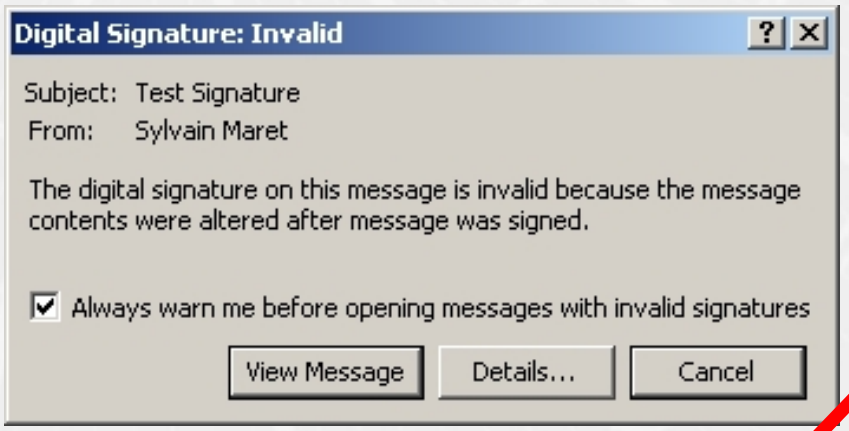
Message signé

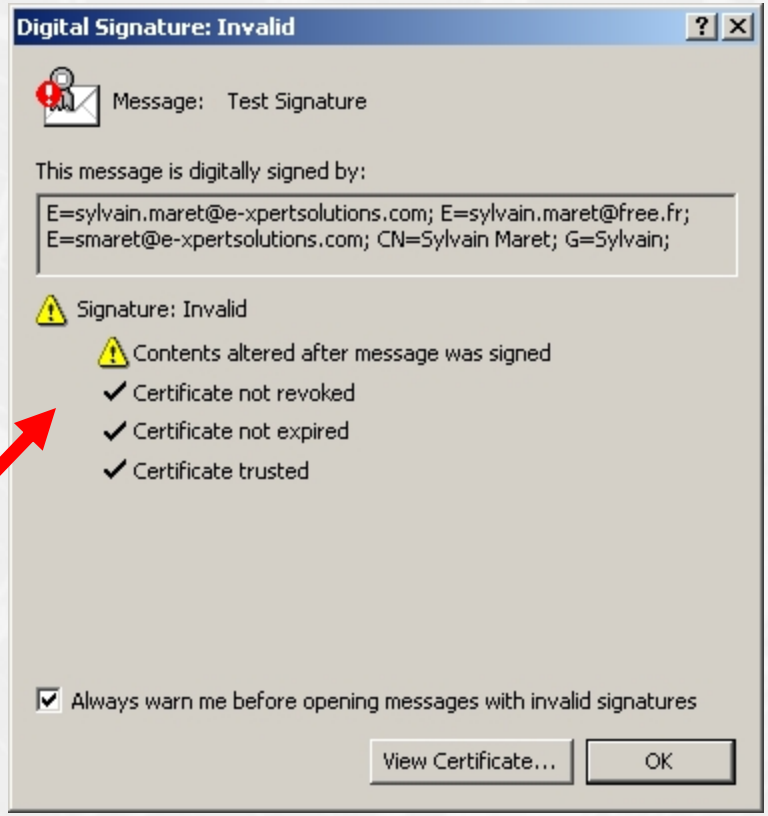
- S/MIME: exemple avec Outlook





- S/MIME: exemple avec Outlook





Message modifié

e-Xpert Solutions SA | 29, route de Pré-Marais | CH 1233 Bernex-Genève | Tél +41 22 727 05 55 | Fax +41 22 727 05 50

Technologie PKI

Introduction à la sécurité informatique
La citadelle électronique

info@e-xpertsolutions.com | www.e-xpertsolutions.com

Technolgie PKI: définition

- Infrastructure pour la gestion des clés publiques
  - Software et hardware
  - Procédures
- Fournit des mécanismes:
  - Authentification
  - Signature
  - Non-repudation
  - Confidentialité
  - Intégrité
- Utilise la notion de certificats (X509)

- Secret Key
- Public Key
- Message Digest
- Nombres aléatoire
- Signature numérique
- Certificat numérique
- PKI
  - RA, CA, Revocation, ldap

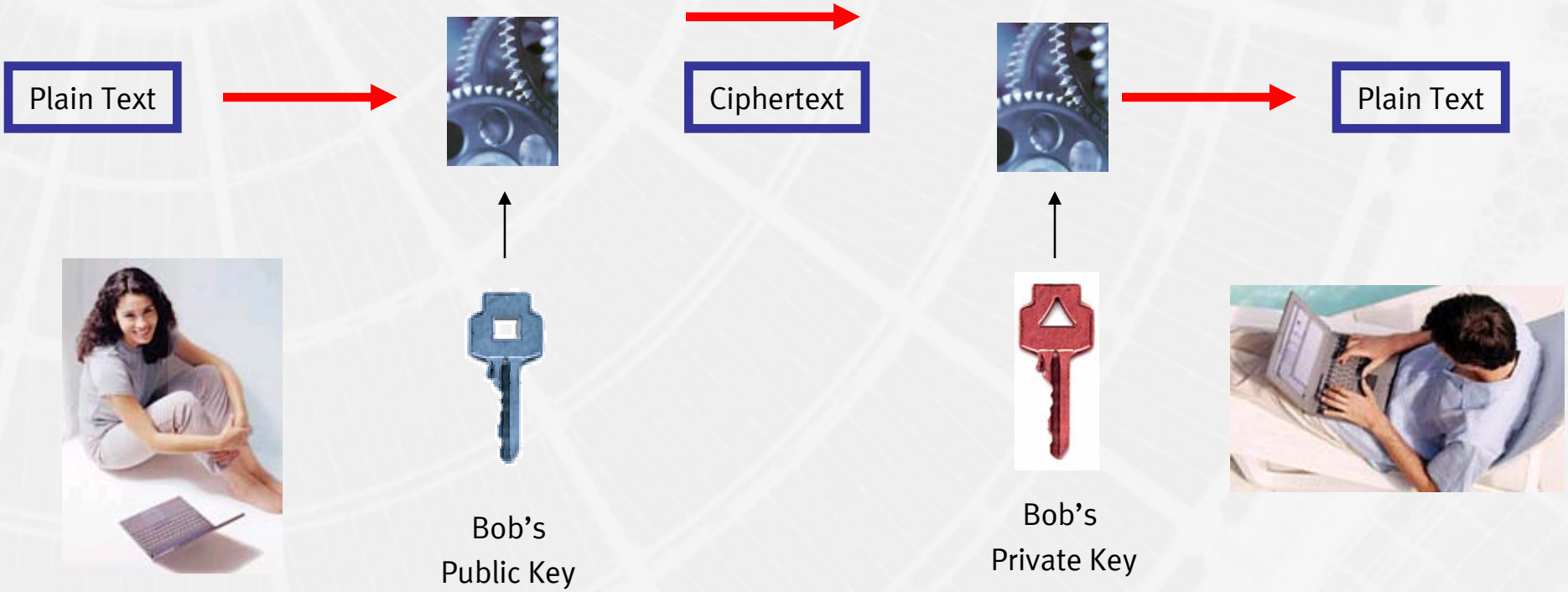
- Secret Key: Alice et Bob

Secret Key: avantages et inconvénients

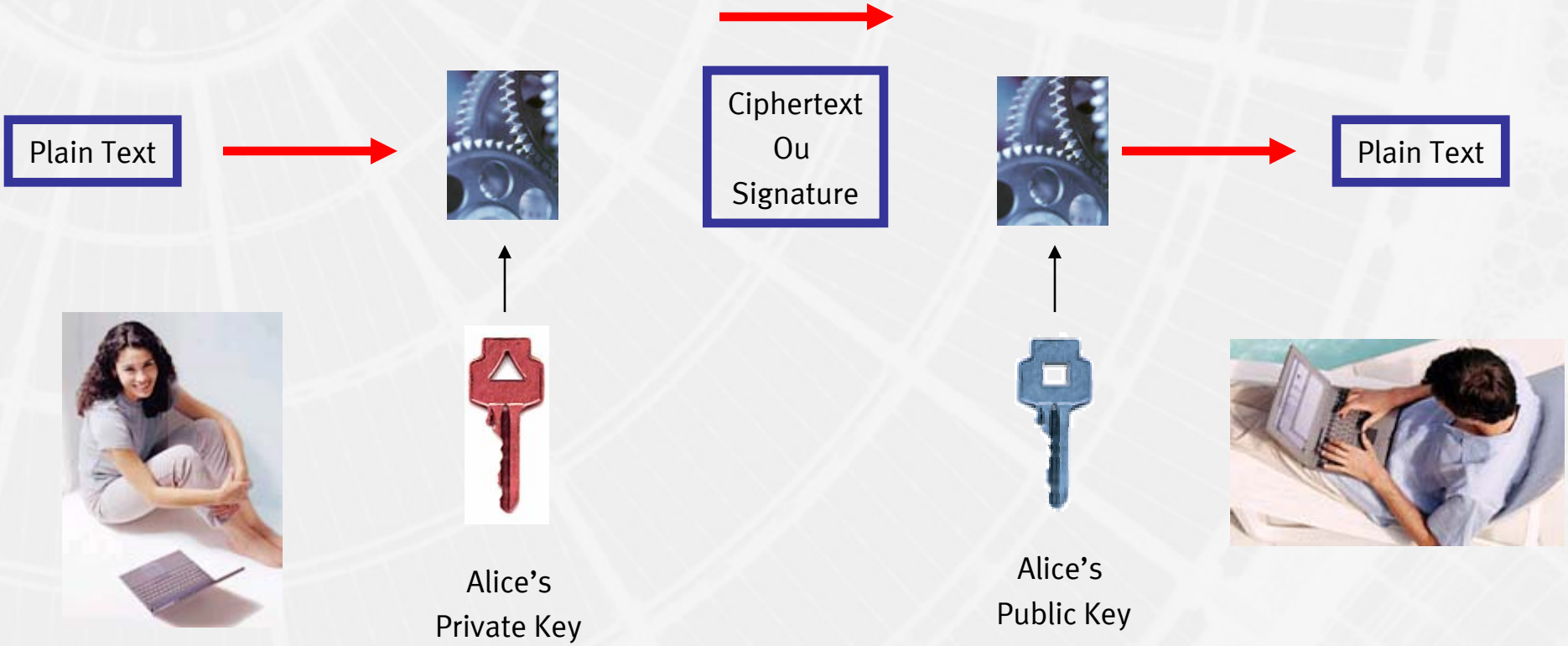
- Avantages
  - Rapidité
  - Simplicité
  - Fiabilité
- Inconvénients
  - Gestion des clés complexes
  - Partage de la clé secrète
  - Grand nombres de clés

- Quelques algorithmes
  - DES
  - 3DES
  - AES
  - RC4
  - Etc.
- Technologies qui les utilisent…
  - IPSEC
  - SSL
  - SSH
  - Etc.

- Public Key: Alice and Bob (Chiffrement)



- Public Key: Alice and Bob (Signature)



Public Key: avantages et inconvénients

- Avantages
  - Gestion des clés
  - Pas de partage de secret
  - Signature numérique
- Inconvénients
  - Pas rapide
  - Longueur des clés (1024, 2048, etc.)

- Exemple d'algorithmes
  - RSA
  - DSA
  - El Gamal
- RSA est dit réversible
  - Chiffrement et signature
- Utilisation
  - PKI
  - SSL, IPSEC, SSH
  - Etc.

Message digest

Input

S'IL SYMBOLISE L'ESPRIT FRONDEUR DE TOUT UN PEUPLE, MANNEKEN-PIS POSSÈDE DES ORIGINES MAL ÉCLAIRCIES. UNE LÉGENDE DIT QU'AU XIII ÈME SIÈCLE, UN PETIT GARÇON AURAIT SAUVÉ LA VILLE EN ÉTEIGNANT, À SA MANIÈRE, LA MÈCHE À L'AIDE DE LAQUELLE LES ENNEMIS VOULAIENT METTRE LE FEU À LA CITÉ. ON DIT AUSSI QU'UN RICHE BOURGEOIS AURAIT PERDU SON FILS UNIQUE DANS LA FOULE, AU COURS D'UNE FÊTE. IL PROMIT À LA VIERGE, S'IL LE RETROUVAIT, DE FAIRE DON À LA VILLE D'UNE STATUE QUI LE MONTRERAIT TEL QU'IL ÉTAIT LORSQUE SON PÈRE LE RETROUVERAIT. LE VOEUX FUT EXAUCÉ ET MANNEKEN-PIS MONTRE ENCORE AUJOURD'HUI CE QUE FAISAIT LE PETIT PERDU AU MOMENT DE L'HEUREUSE RETROUVAILLE.

Fonction Hash

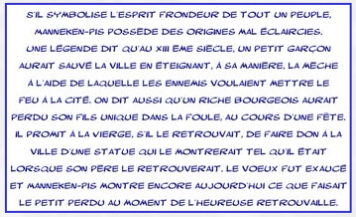
Output / Résultat

Digest

- Fonction de hashage
  - Md3, Md4
  - MD5
  - Sha1
  - Ripemd
- Utilisation
  - signature numérique
  - Crontôle de « checksum »
  - Outils FIA
  - MAC
  - Etc.

- Deux familles
  - PRNG
  - Vrai nombres aléatoires
- Très important pour la cryptographie
  - Génération des clés de session

- Signature numérique: exemple de création avec RSA et md5



Vers BOB

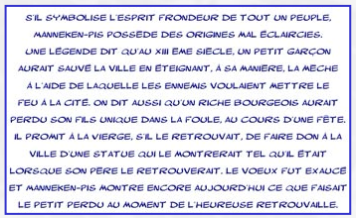
MD5

Digest

Alice's
Private Key

RSA

Signature numérique: vérification



MD5

Digest A'

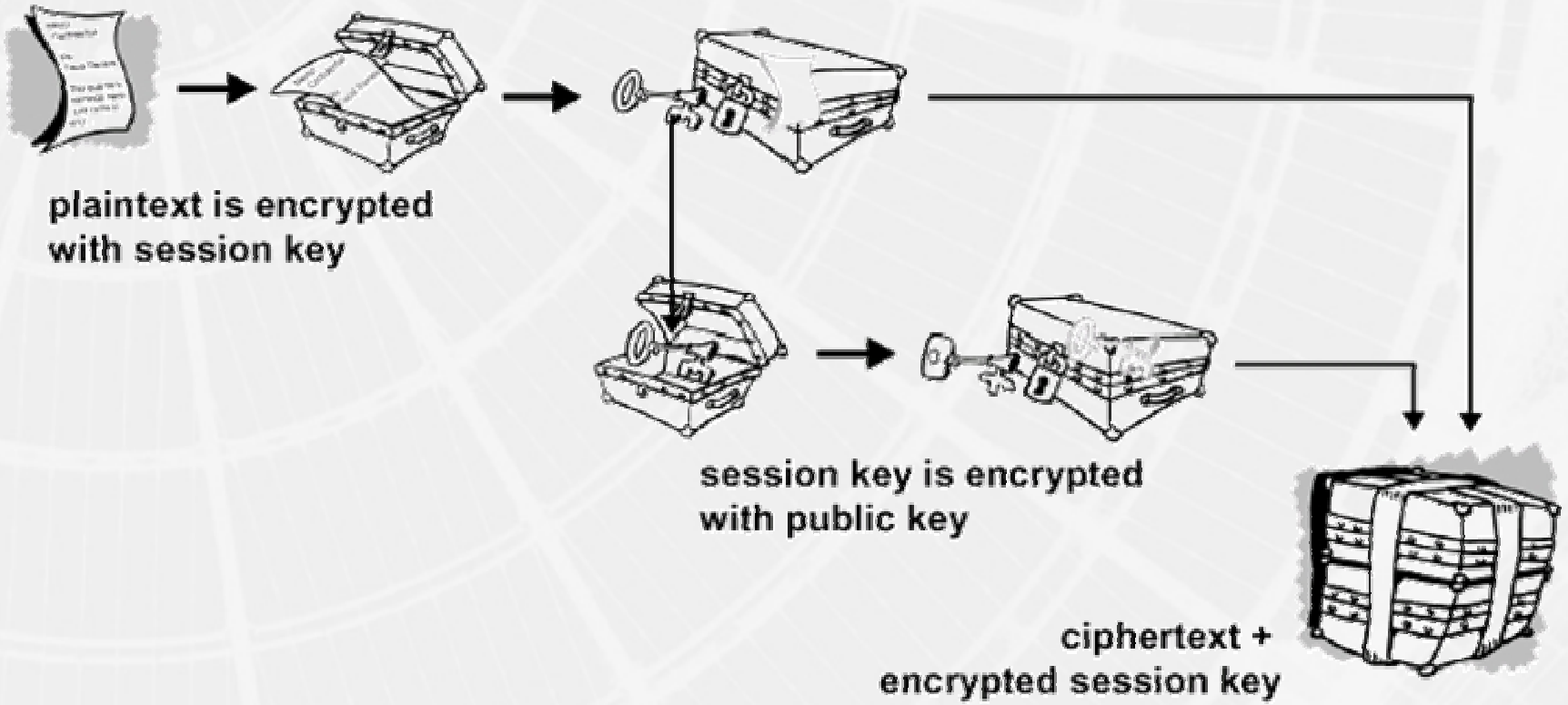
?

Alice's
Public Key

Digest A

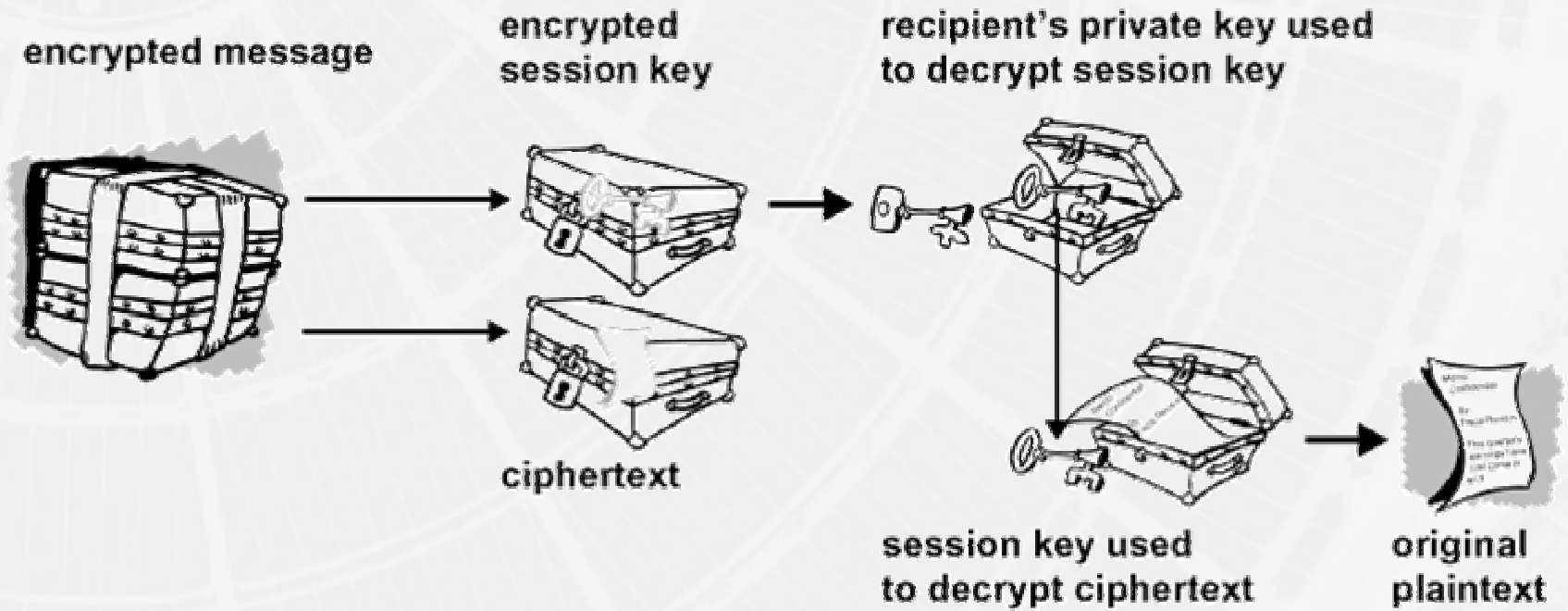
RSA

- RSA Key Wrapping



Source: PGP

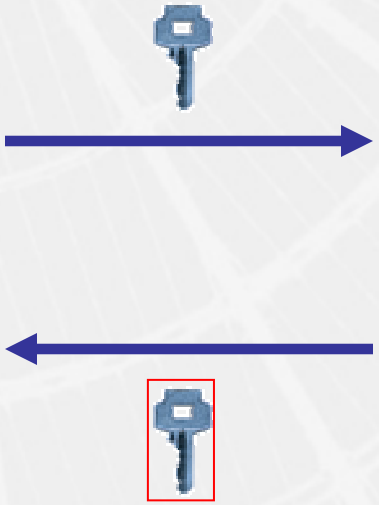
- RSA Key Wrapping

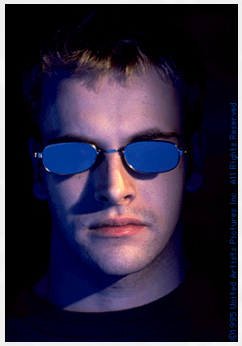


Source: PGP

- Man in the Midle !

Alice





Charly

Interception des clés publique

Bob

- Notion de confiance

Autorité de certification

Alice

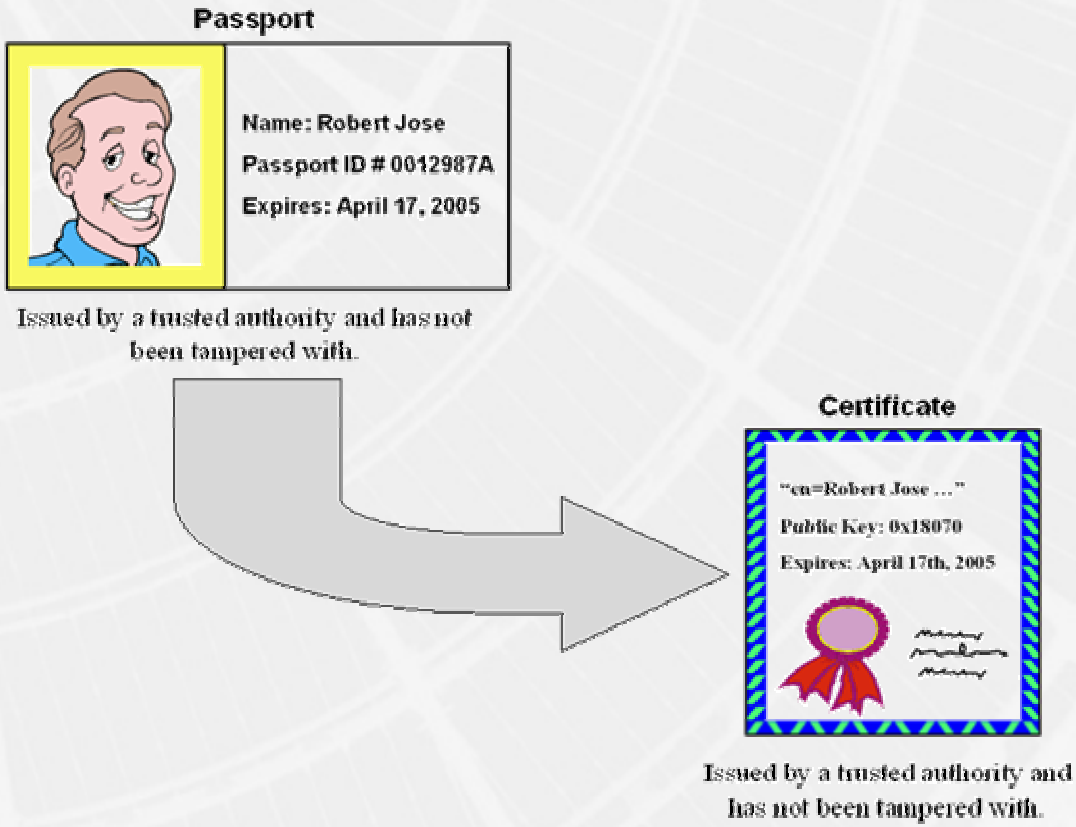
Charly

Bob

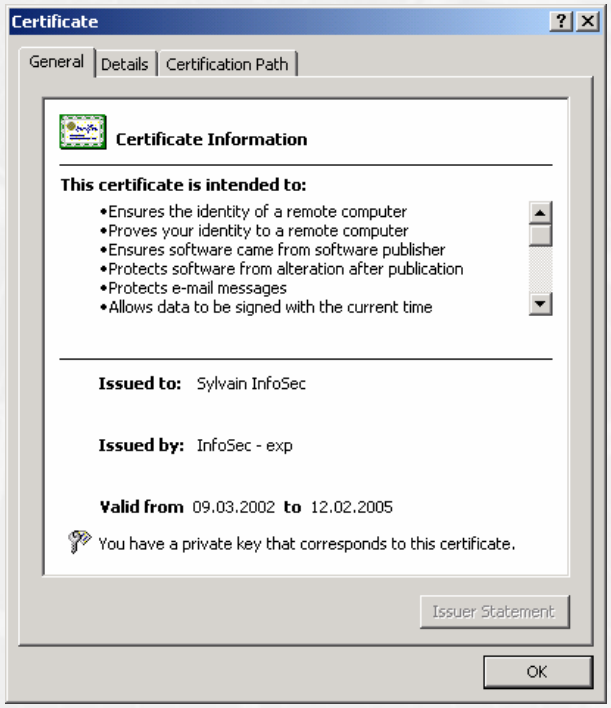
Notion de certificat numérique

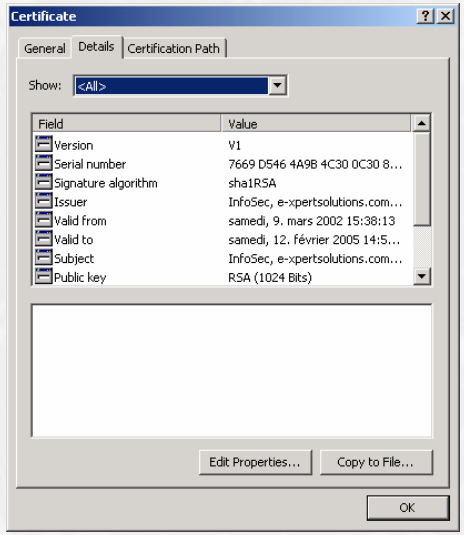
- Lien entre une entité et une clé publique
- L'entité peut être:
  - Une personne
  - Une machine
  - Une entreprise
  - Etc.
- La signature digitale garantit ce lien (certificat)
- Il existe une norme: X509

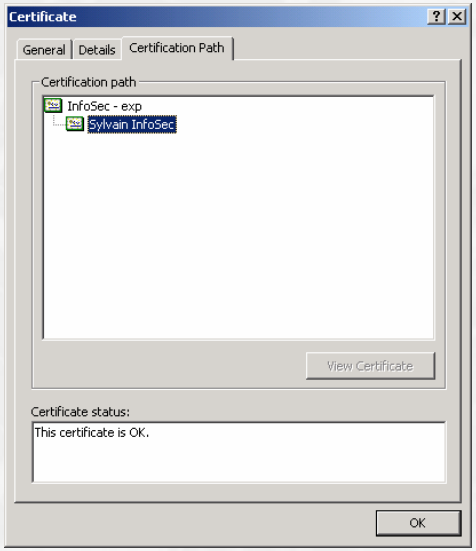
- Le certificat est analogue à un passeport



Certificat X509







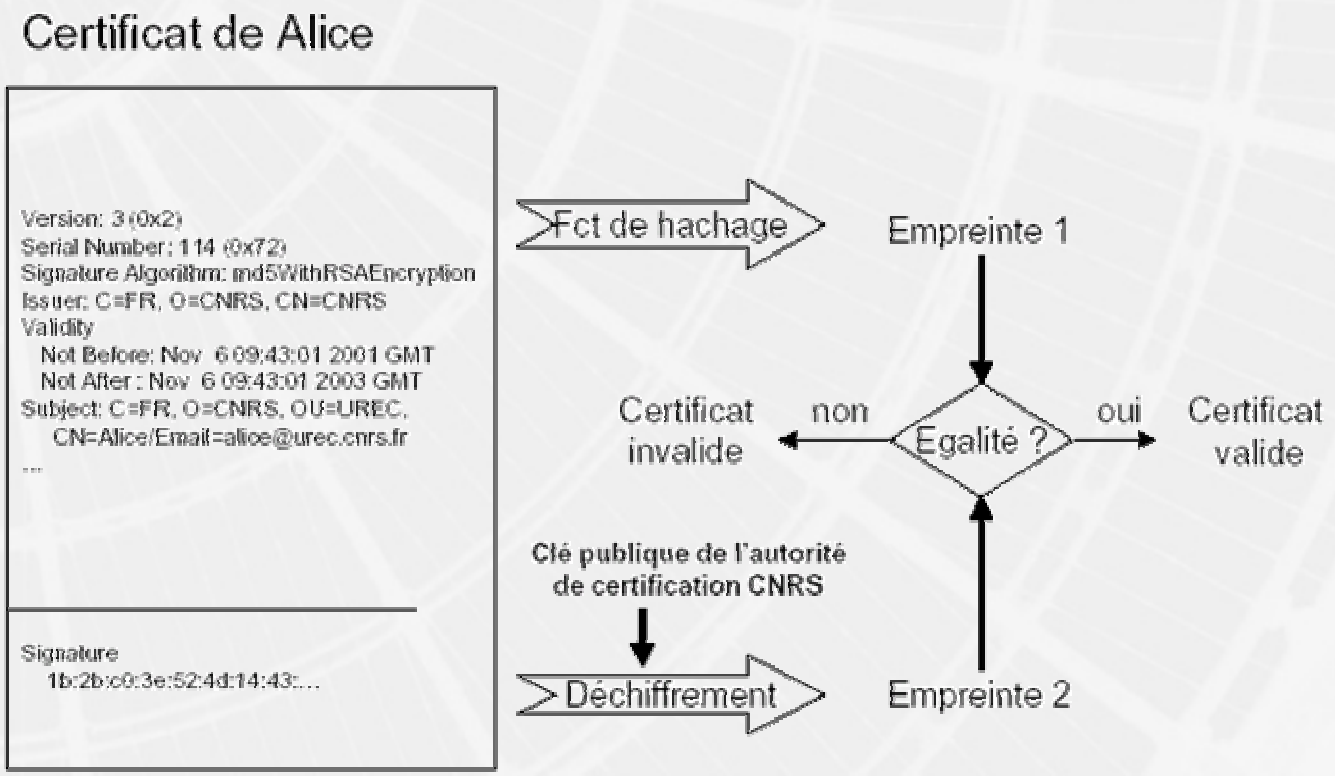
- Format Certificat X509

Data	Version
	Serial Number
	Signature Algorithm
	Issuer
	Validity
	Subject
	Subject Public Key Info
	X509v3 extensions Extension1: [critical] Valeur extension1 Extension2: [critical] Valeur extension2 … Extension*n*: [critical] Valeur extension*n*
Signature	Signature Algorithm
	Signature

- Format Certificat X509

Version	Indique à quelle version de X.509 correspond ce certificat.
Serial number	Numéro de série du certificat (propre à chaque autorité de certification).
Signature Algorithm	Type de signature utilisée.
Issuer	Distinguished Name (Subject) de l'autorité de certification qui a émis ce certificat.
Validity	Période de validité.
Subject	Distinguished Name du propriétaire de ce certificat.
Subject public key info	Infos sur la clef publique de ce certificat.
X509v3 Extensions	Extensions génériques optionnelles, introduites avec la version 3 de X.509.
Signature	Signature numérique de l'AC sur l'ensemble des champs précédents.

- Vérification du certificat



Architecture PKI: les composants de bases

- Certificats X509
- Autorité de certification (CA)
- Autorité d'enregistrement (RA)
- Autorité de validation (VA)
- Annuaires
- Archivage

Autorité de certification (CA)

- L’entité qui délivre les certificats
- Le tiers de confiance
- L’entité qui publie les certificats dans un annuaire
- L’entité qui génère les listes de révocation

Autorité de souscription (RA)

- Bureau d’enregistrement
- Reçoit les requêtes de certification
- Obéit à la structure granulaire de l’entreprise
- Identification du requérant

Autorité de validation (VA)

- Service on-line
- Contrôle de validité des certificats
- Réponse: valide/invalide/inconnue
- Plus efficace que les CRLs
  - Minimise le trafique
  - Etat en temps réel

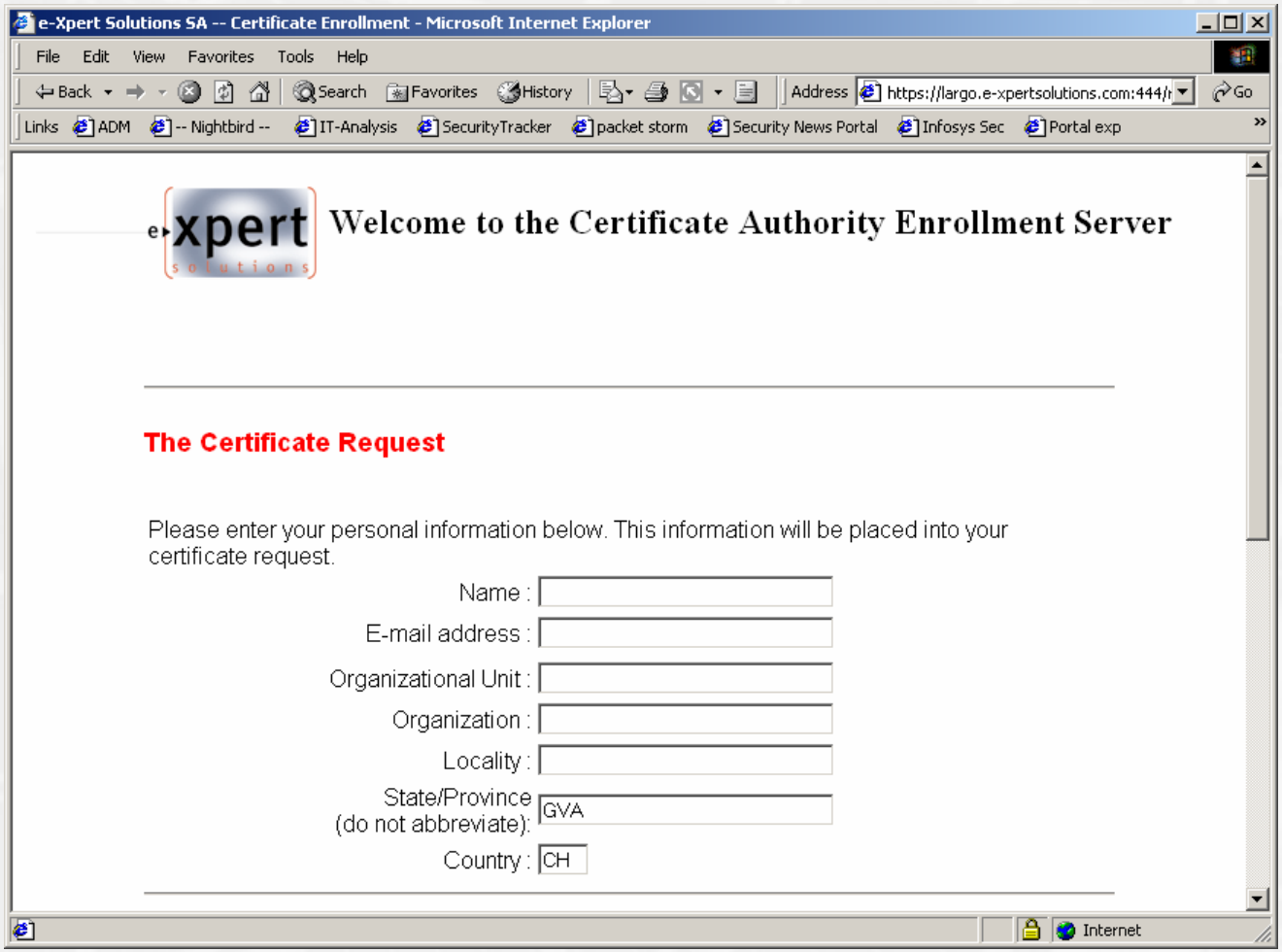
Annuaires

- Structure hiérarchisée de type x.500
- Liste des liens entre utilisateurs et certificats
- Peut contenir des listes de révocation (CRL)

Archivage

- Stockage à long terme des clés de chiffrement
- Key recovery
  - Perte des clés
  - Vol
  - Etc.
- Procédure de récupération des clés
- Pas de stockage des clés de signature
  - Non répudiation

- Exemple: obtention d'un certificat



- Exemple: obtention d'un certificat

User enrolls for certificate

http://www

User mailed ack.

User mailed retrieval PIN

User retrieves certificate

http://www

Certificate installed

RA

Admin mailed notification

CA

Admin Approves request

http://www

LDAP

Les applications PKI

- Sécurisation de la messagerie
- VPN, Accès distants
- Portail Web, e-commerce
- Transactions électroniques
- Publications électroniques
- Single Sign On
- Etc.

e-Xpert Solutions SA | 29, route de Pré-Marais | CH 1233 Bernex-Genève | Tél +41 22 727 05 55 | Fax +41 22 727 05 50

Systèmes d'authentification

Introduction à la sécurité informatique
La citadelle électronique

info@e-xpertsolutions.com | www.e-xpertsolutions.com

Systèmes d'authentification: introduction

- Tour d'horizon des technologies d'authentification
- Clé de voûte pour la construction de la citadelle électronique
  - 1er besoin pour la sécurité du système d'information

- L'identification et l'authentification: des services de sécurité de base
  - Autorisation
  - Auditing
  - Non-répudiation
  - Confidentialité

- Systèmes d'authentification: identification et authentification ?

- Identification
  - Qui êtes vous ?
- Authentification
  - Prouvez le !

Les 6 éléments d'un système d'authentification

- Entité ou personne
- Caractéristique unique
- Propriétaire du système
- Mécanisme d'authentification
- Mécanisme de contrôle d'accès
- Mécanisme d'archivage

- Exemple avec Ali Baba …

- Entité
  - La personne qui connait le *mot de passe*
- Caractéristique Unique
  - Le mot de passe: « Sésame, ouvre toi ! »
- Le propriétaire de la caverne
  - Ali Baba et Les 40 voleurs

- Exemple avec Ali Baba…

- Mécanisme d’authentification
  - Elément magique qui répond au mot de passe
- Mécanisme de contrôle d’accès
  - Mécanisme pour rouler la pierre ou les pierres
- Mécanisme d’archivage
  - Journal des événements

- Login par mot de passe

Mécanisme
d'authentification

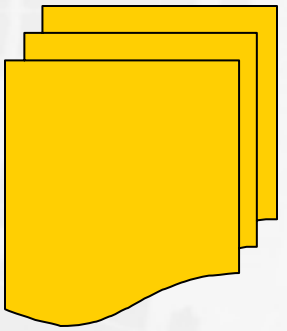
Caractéristique unique
Mot de passe

La personne

Login
Process

Mécanisme
de contrôle
D'accès

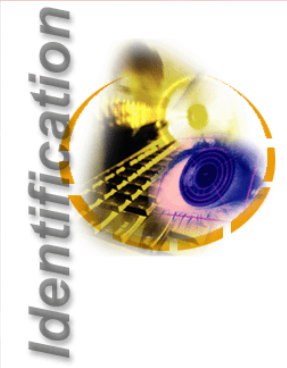
Computer
Ressources



Mécanisme
D'archivage

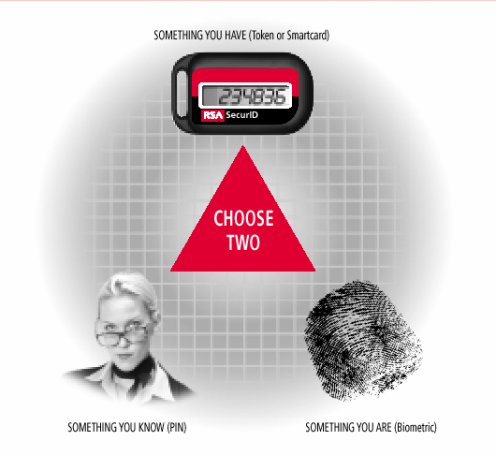
Propriétaire

Les facteurs d'authentification



- Quelque chose que l'on connait
  - PIN, Mot de passe, etc.
- Quelque chose que l'on possède
  - Tokens, Carte à puce, badge, etc.
- Quelque chose que l'on est
  - Biométrie

- Authentification forte



- Un minimum de deux facteurs
  - Smartcard + PIN
  - Token + PIN
  - Biométrie avec Smartcard
  - Etc.

Que sécuriser ?

- Equipements réseaux
  - Routeurs, Switchs, etc.
- Systèmes d'accès aux réseaux
  - Remote access
  - Firewall
- Serveurs du système d'information
  - Unix, NT, Main Frame, AS400, etc.
- Postes de travail
  - Windows (NT, 2000, XP, etc.)
- Applications
  - Web, ERP, Back office, etc.

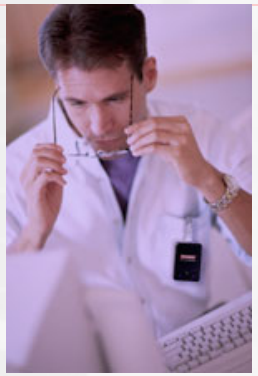
- Quelle technologie d'authentification ?

- Password standard
- Tokens
- Challenge Response
- Authentification indirecte
  - Radius, Tacacs+
- Kerberos
- Biométrie
- PKI (Smartcard, Tokens USB)
- Etc.

Les « Tokens »

- Quelque chose que vous possédez
  - Généralement authentification forte (PIN+Token)
- Deux grandes familles
  - Passive Tokens
  - Active Tokens

Passive Tokens



- Contient un secret unique (Base Secret)
  - Secret unique partagé
- Type de Tokens
  - Badge de proximité
  - Carte magnétique
  - Etc.
- Généralement authentification « faible »
  - Pas de deuxième facteur

- Mode de fonctionnement

Base Secret

=

Base Secret

Token + (PIN)

Active Tokens

- Contient un secret unique (Base Secret)
  - Secret unique partagé
  - Facteur commun changeant
- Résultat: One Time Password (OTP)
- Mode de fonctionnement dit synchrone
  - Counter Based
  - Clock Based
  - Hybride

Mode de fonctionnement

Facteur commun changeant

Facteur commun changeant

=

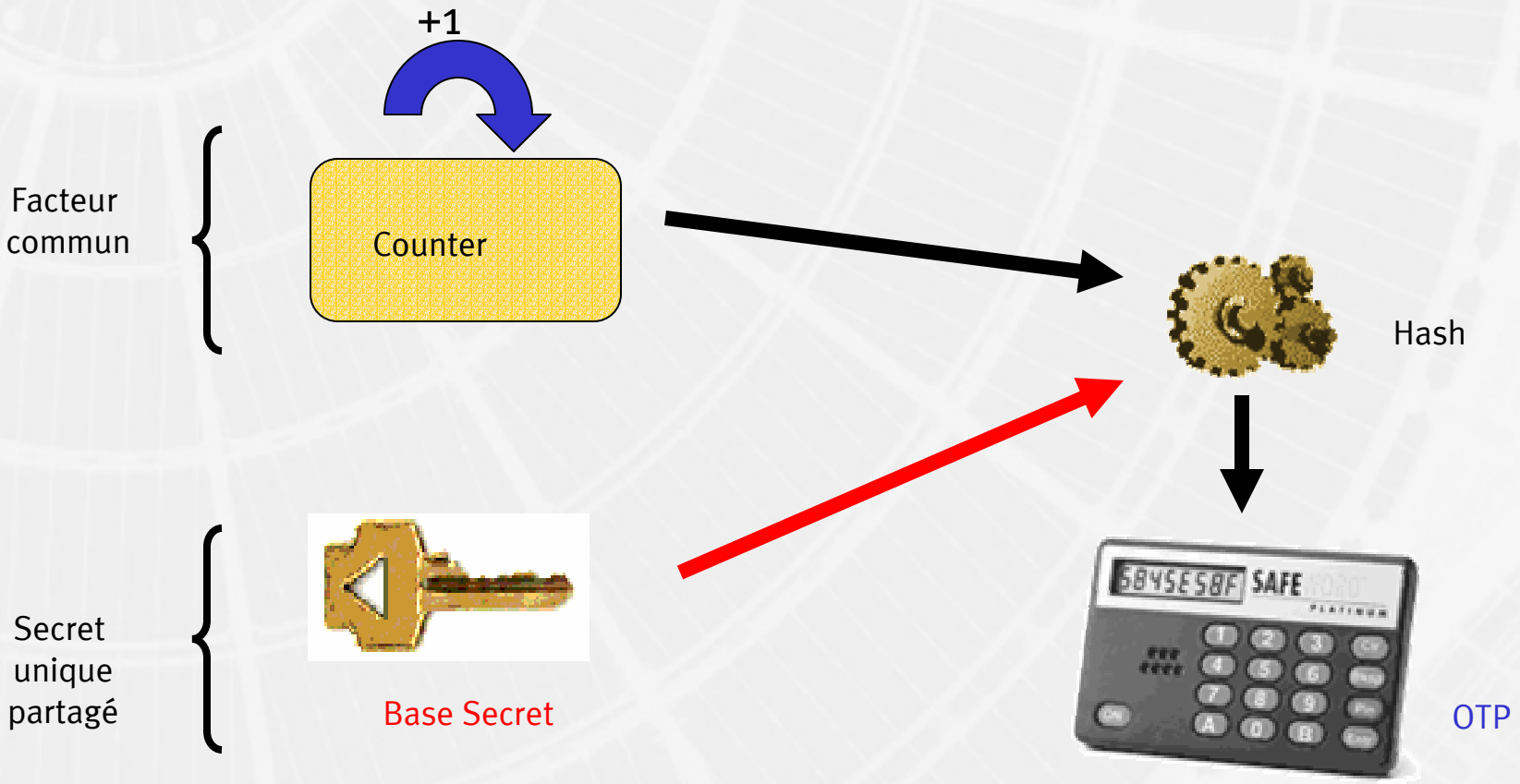
Token + (PIN)

=

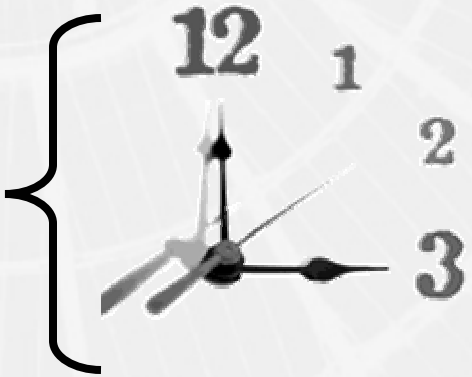
Base Secret

Base Secret

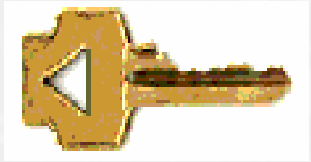
Counter Based Tokens



Clock Based Tokens



Hash



Base Secret

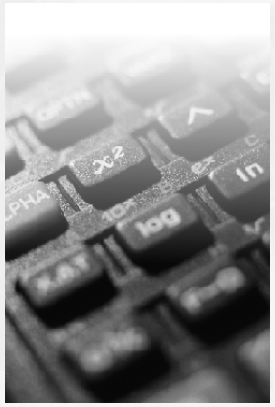
Secret unique partagé

OTP

Protection des tokens

- Deuxième facteur par PIN
  - Personal Identifier Number
- Deux solutions
  - PIN externe
  - PIN interne

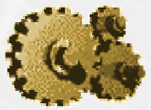
- PIN Code interne



PIN unlock
Base Secret

Clock or
Counter

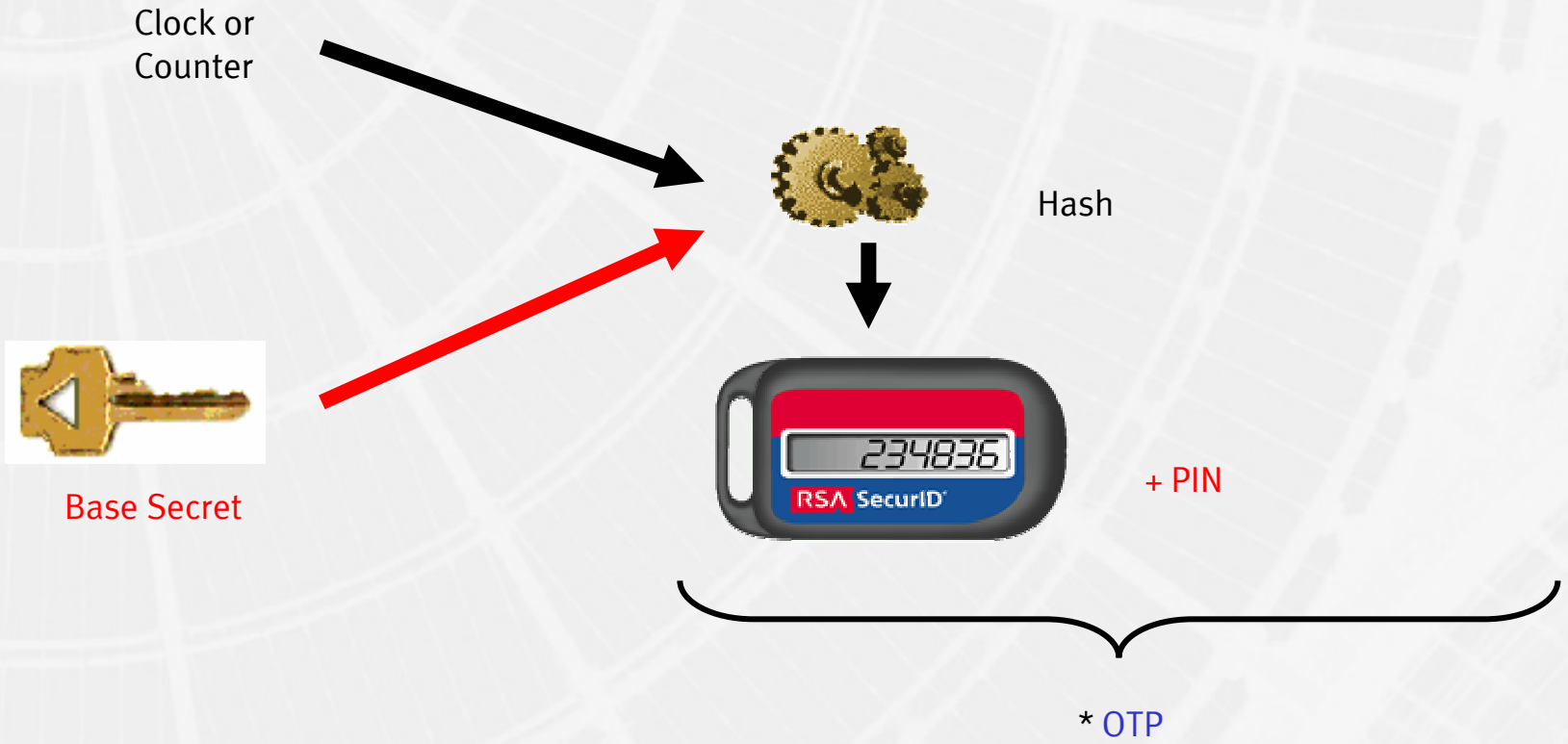
Base Secret



Hash

OTP

PIN Code externe

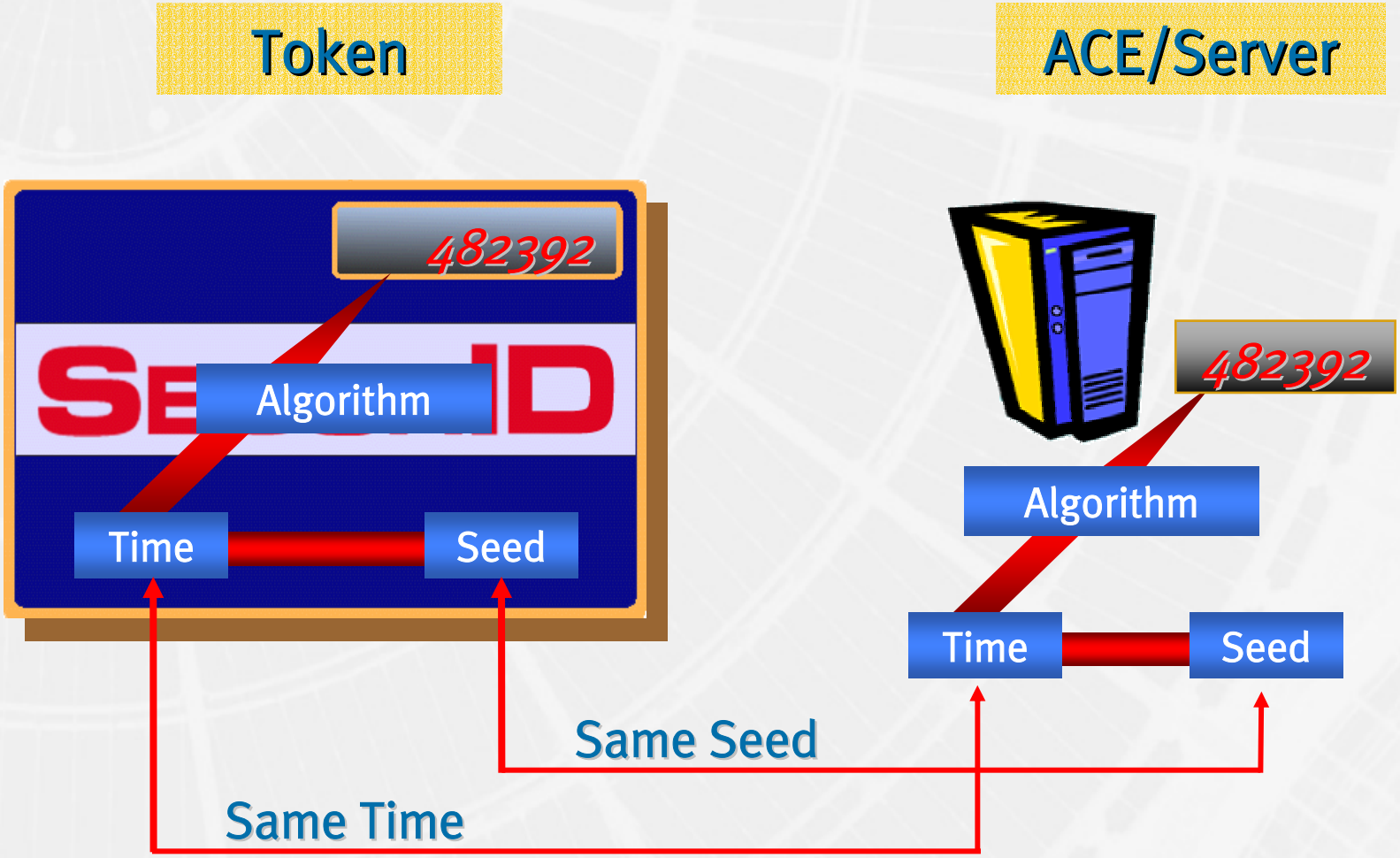


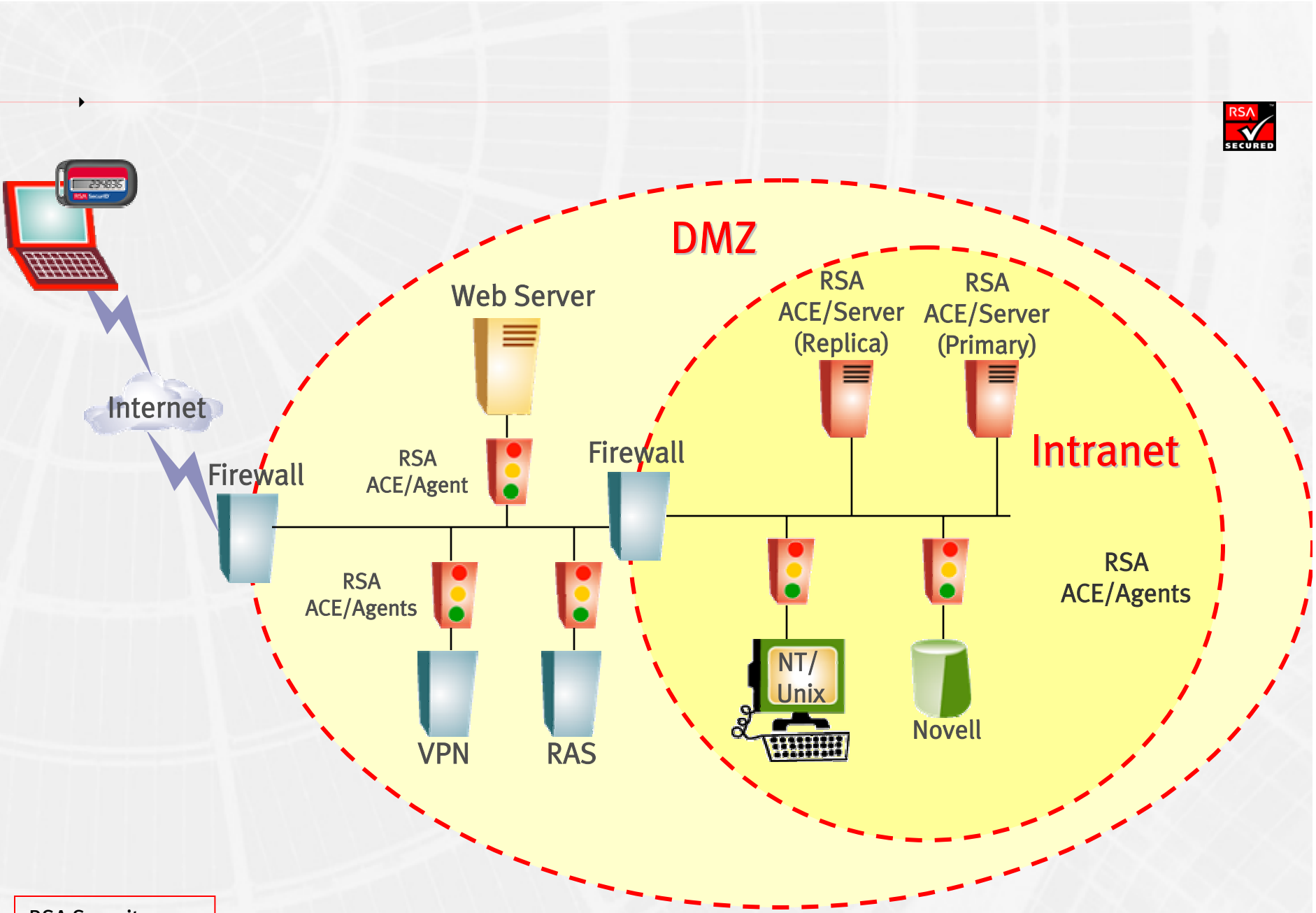
** Shoud use encryption (SSL, IPSEC, SSH*

RSA SecurID

- De facto standard
  - Grandes banques, industries, gouvernements
- Système basé sur le temps
- Très portable
- Grand nombre d'agents (env. 300)
- Facilité d'utilisation

- RSA SecurID


Token
ACE/Server
482392
Algorithm
Time
Seed
482392
Algorithm
Time
Seed
Same Seed
Same Time


DMZ
Web Server
RSA
ACE/Server
(Replica)
RSA
ACE/Server
(Primary)
Internet
Firewall
RSA
ACE/Agent
Firewall
Intranet
RSA
ACE/Agents
RSA
ACE/Agents
NT/
Unix
Novell
VPN
RAS

Challenge Response

- Basé sur un challenge (**nonce**)
- Basé sur un secret unique
- Calcul du challenge avec une fonction de hachage
- Mode de fonctionnement dit asynchrone

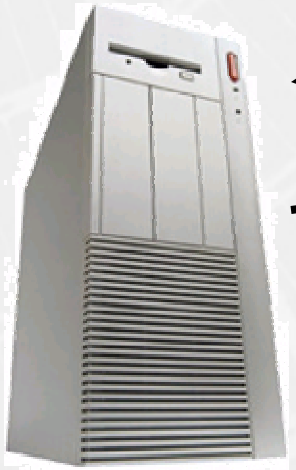
- Mode de fonctionnement

Base Secret

=

Base Secret

nonce
(adf341gf)



dupont

nonce = adf341gf

response = ff747dgd4

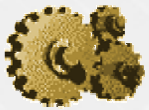
Norme X9.9

- Standard ouvert pour Challenge Response
  - US Gouvernement
  - American Bankers Association
- Utilisation de « DES » comme Hash
  - Problème de « Password Guessing »
- Migration vers « AES »

- Norme X9.9

Random
Challenge
Nonce

Hash
(DES encrypt)



OTP
Response

Base Secret

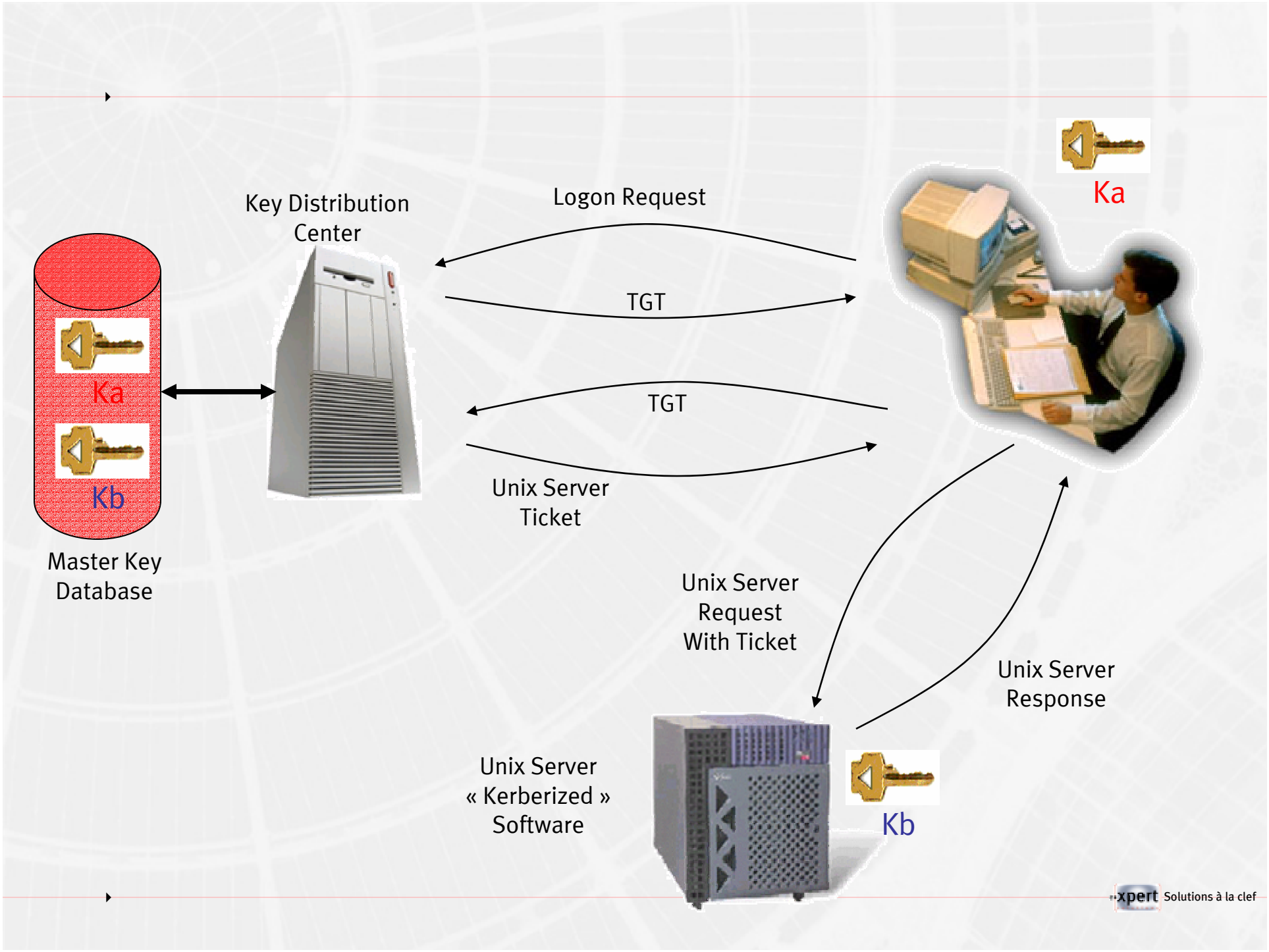
- Protocole de sécurité pour l'authentification
- Architecture Single Sign-On
- Développé par le MIT en 1985
  - Version 4.0
  - Version 5.0 (IETF) rfc 1510 et 1964
  - Open Software pour environnement Unix

Kerberos

- Fournit du chiffrement de session
  - Secure Single Sign-On
- Fournit l'authentification mutuelle
  - Entre clients et serveurs
- Utilisation du protocole par Windows 2000
  - Nouvelle vie pour Kerberos

Kerberos: concept de base

- Utilisation de secret partagé
  - Chiffrement symétrique
- Utilisation d'un tiers de confiance pour le partage des secret partagés (clés)
  - Key Distribution Center
- Utilisation de tickets distribués par le KDC
  - Credential ou ticket de session
  - Validité des tickets dans le temps


Key Distribution Center
Logon Request
TGT
TGT
Unix Server Ticket
Ka
Kb
Master Key Database
Ka
Unix Server Request With Ticket
Unix Server Response
Unix Server « Kerberized » Software
Kb

- Protocole d'authentification de Windows 2000
  - Remplacement de NTLM
- Utilisation de Active Directory pour le stockage des clés Kerberos
- Architecture Single Sign-On
- Kerberos Version 5.0

Extension du protocole Kerberos

- Logon initial remplacé par la technologie PKI
  - PKINIT (IETF)
  - Utilisation des smartcards
  - Authentification basé sur un certificat X509
- KDC vérifie le certificat
  - « Trust » et les « Path »
  - Validation du certificat (CRL)

- Système « ancien »
  - 1930 - carte d'identité avec photo
  - Reconnaissance de la voix
  - Etc.
- Deux familles
  - Mesure des traits physiques uniques
  - Mesure d'un comportement unique

Mesure des traits physiques

- Empruntes digitales
- Géométrie de la main
- Les yeux
  - Iris
  - Rétine
- Reconnaissance du visage
- Nouvelles voies
  - ADN, odeurs, oreille et « thermogram »

- Mesure d’un comportement

- Reconnaissance vocale
- Signature manuscrite
- Dynamique de frappe
  - Clavier

Promesses et réalité

- Difficultés liées aux « false rejection »
- Mais aussi les « false acceptance »
- « Replay Attacks » et « Spoofing »
  - Ajout d'un PIN Code ou Smartcard
- Prix ?
  - Les bons capteurs sont onéreux (600 CHF/poste)

Personnel
trait

Biometric
Reader

Feature
Extraction

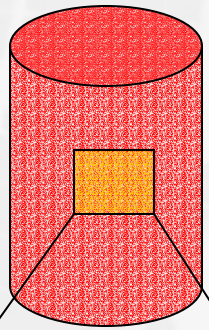
1=127
2=126
3=456
4=987

Biometric
Signature

Biometric
Matching

?

Biometric
Pattern



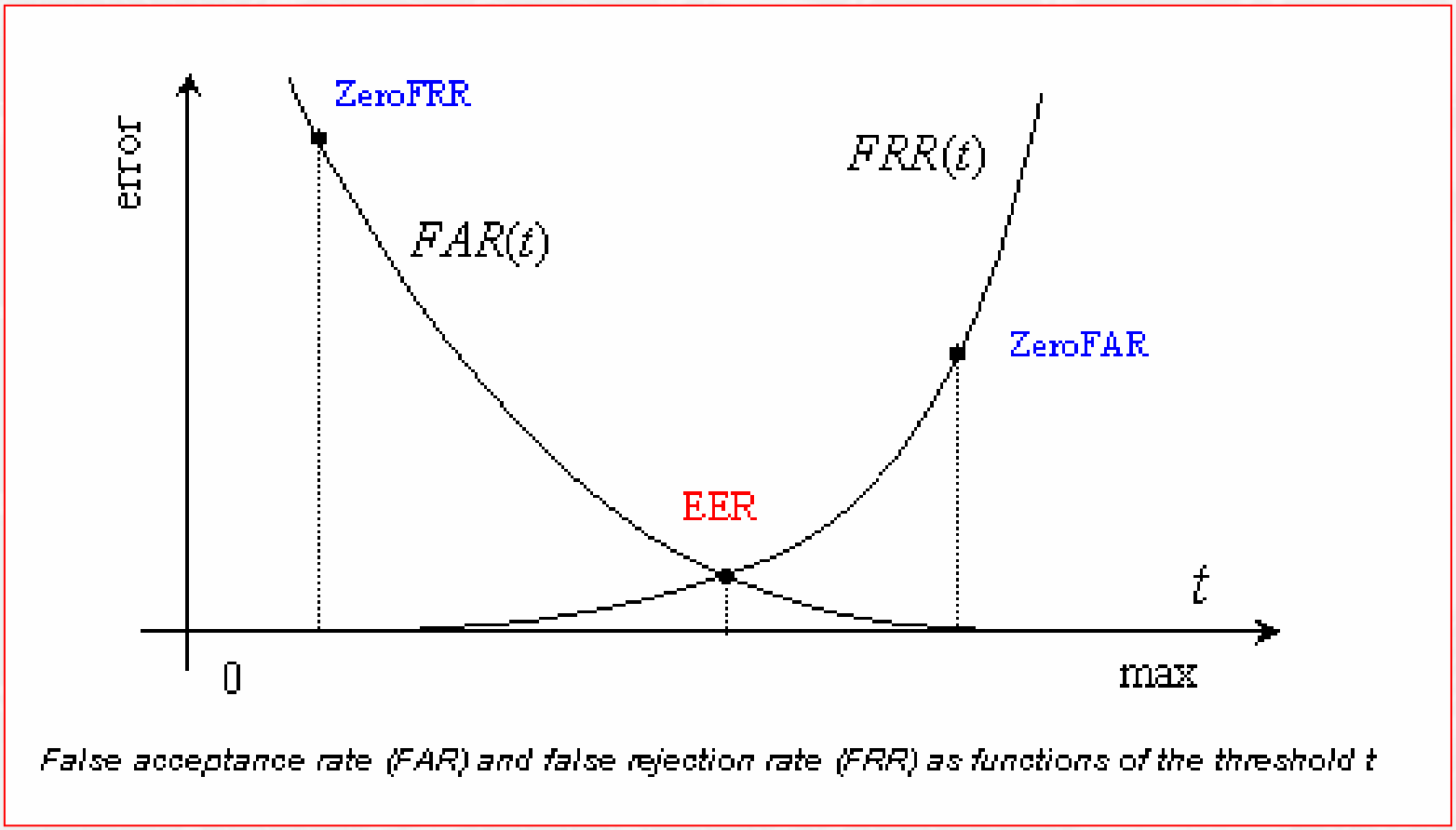
dupont: 1=127,2=
deraud: 1=878,2=
marcus: 1=656,2=

- Par serveur d'authentification
  - Requêtes par réseau
  - Problème de la sécurité
  - Problème de confidentialité
  - Problème de disponibilité
- Sur une smartcard
  - Meilleure sécurité
  - Mode « offline »
  - Prix plus élevé
  - MOC = Match On card

Précision Biométrique

- False Acceptance
  - FAR (False Acceptance Rate) in %
  - Lecteur sale, mauvaise position, etc
- False Rejection
  - FRR (False Rejection Rate) in %
  - Usurpation, falsification

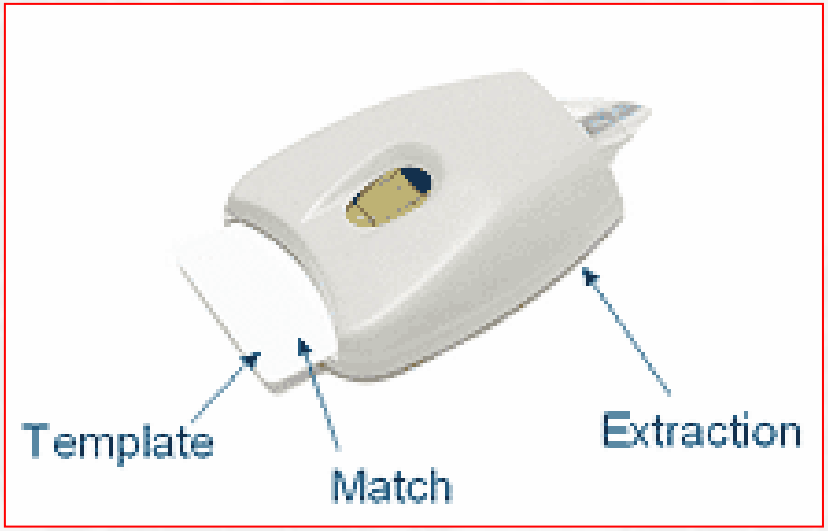
- Equal Error Rate (EER)



False acceptance rate (FAR) and false rejection rate (FRR) as functions of the threshold t

- Authentification forte

- Deux facteurs
  - Une carte à puce
  - Un PIN code



- Questions ?

e-Xpert Solutions S.A. est une société Suisse de services spécialisée en sécurité informatique dont les fondateurs ont fait de leur passion leur métier :

La sécurité des systèmes d'information

Fort de leurs convictions et de leur expérience, nos ingénieurs conçoivent, déploient et maintiennent au quotidien des architectures de sécurité au moyen de solutions pragmatiques, basées sur des technologies fondamentales et novatrices, adaptées aux exigences de la clientèle.

Cette approche, associée à des collaborateurs motivés, flexibles et au bénéfice d'une intégrité irréprochable, nous a permis d'assurer une croissance continue et de gagner la confiance d'une clientèle issue de tout domaine d'activité et de toute taille.

Notre siège à Bernex/Genève et notre agence de Morges/Lausanne vous garantissent un contact de proximité.

http://www.e-xpertsolutions.com