3ème année

Sécurité des Systèmes Informatiques

SUPAERO

Rodolphe Ortalo
RSSI - CARSAT Midi-Pyrénées
rodolphe.ortalo@free.fr
(rodolphe.ortalo@carsat-mp.fr)
http://rodolphe.ortalo.free.fr/ssi.html

Plan (2/2)

- Protection utilisées dans la pratique
  - **Protection réseau et *firewall***
  - Systèmes d'authentification
  - Chiffrement de flux et VPN
- Digressions (RàZ, OpenBSD, 1984)
- Surveiller, analyser et gérer
  - Détection d'intrusion
  - Audit, tests d'intrusion
  - Administration, exploitation et suivi de la sécurité
  - Observation et surveillance
- Protection des applications usuelles

Solutions commerciales

- Leaders
  - FireWall-1 (CheckPoint)
  - ASA (Cisco)
- Challengers
  - Netscreen
  - Cyberguard
  - ISA Server (Microsoft)
  - IOS FW ? (Cisco)
  - …
- Solutions SOHO
  - SonicWall
  - WatchGuard
- Français
  - Netasq
  - Netwall (Evidian/Bull)
  - M>Wall (Matranet)
  - Arkoon
- …

Solutions open-source

- Linux/IPTable (Netfilter)
- Linux/IPChains
- IPFilter (Linux/Solaris/…)
- OpenBSD pf
- FreeBSD ~~ipfw~~ pf

Relais (*proxy*)

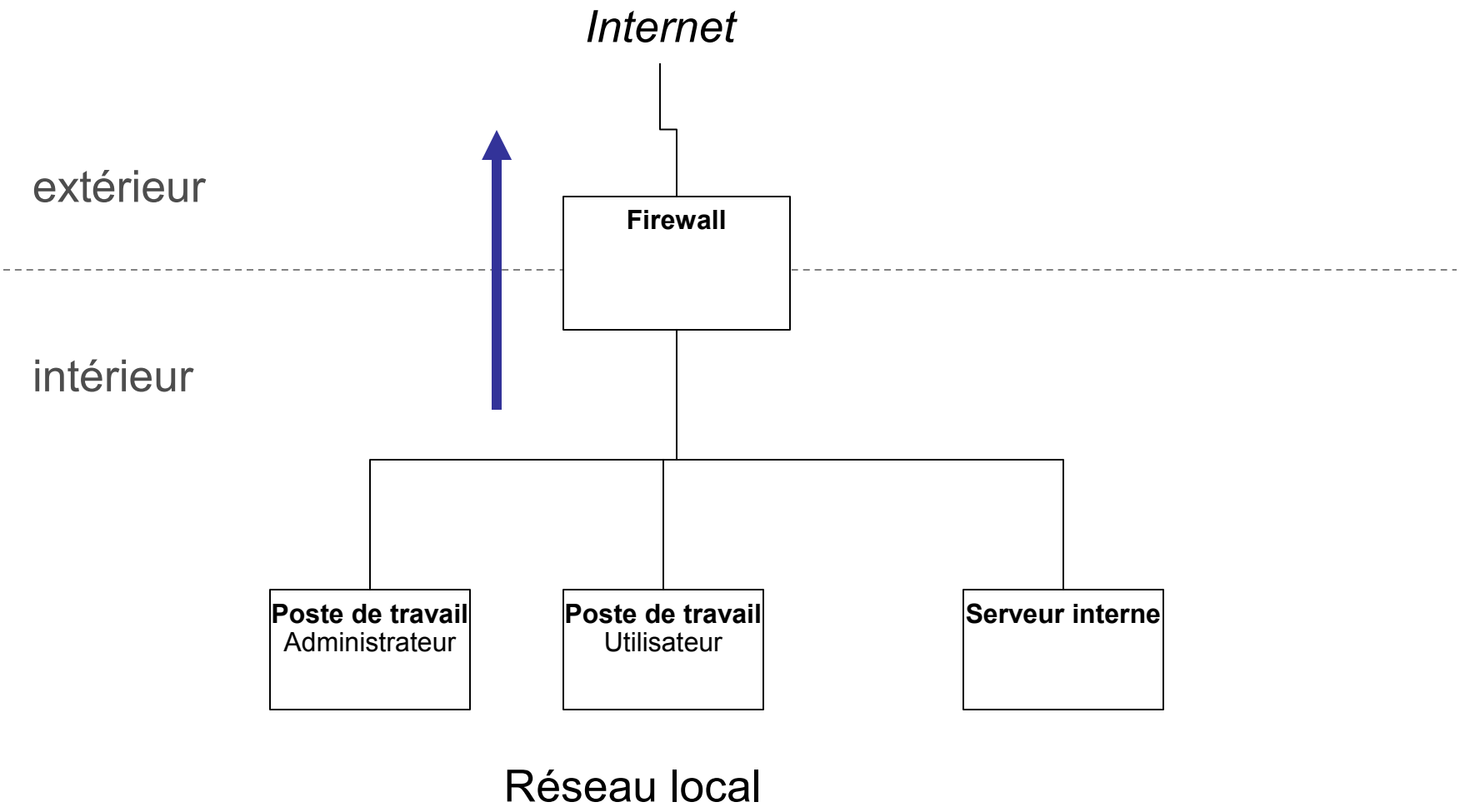
- Associé à des protocoles particuliers
  - HTTP
  - FTP
  - Telnet
  - X11
  - SOCKS
  - H.323 & co. ?
- Principaux intérêts
  - Prendre en charge des protocoles compliqués (comme FTP actif/passif)
  - Ajouter une autre authentification (si possible transparente)
  - Contrôler la validité protocolaire
  - Permettre un filtrage des commandes
- *Transparent proxying* : couplage noyau et *proxy*

Aspects architecturaux

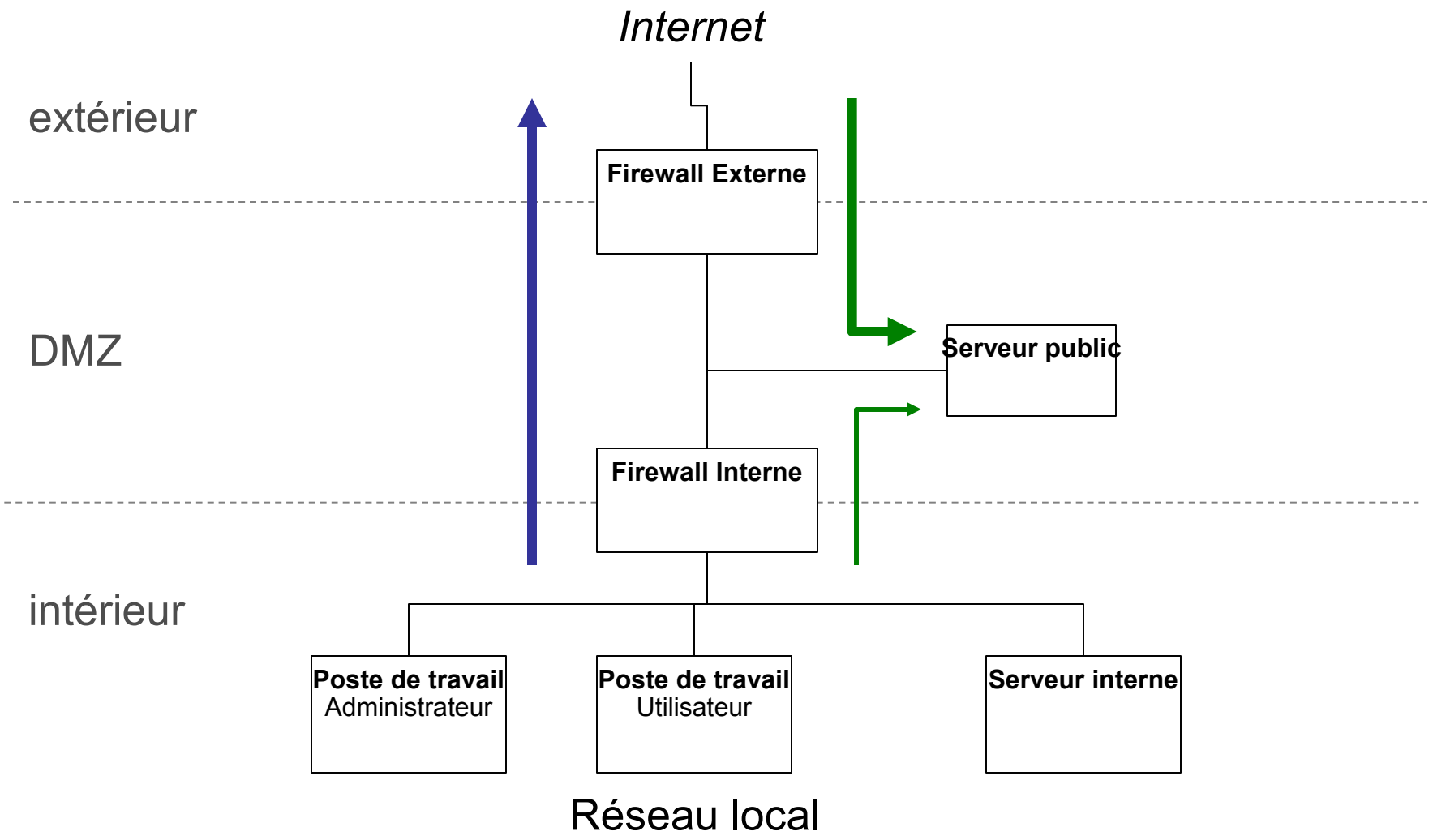
- Principes de fonctionnement
  - « niveaux » de sécurité et zones (DMZ)
  - Administration
  - Relais
  - Diversification
  - Environnement réels

Cheswick and S.M. Bellovin, *Firewalls and Internet security*, AddisonWesley, 1994

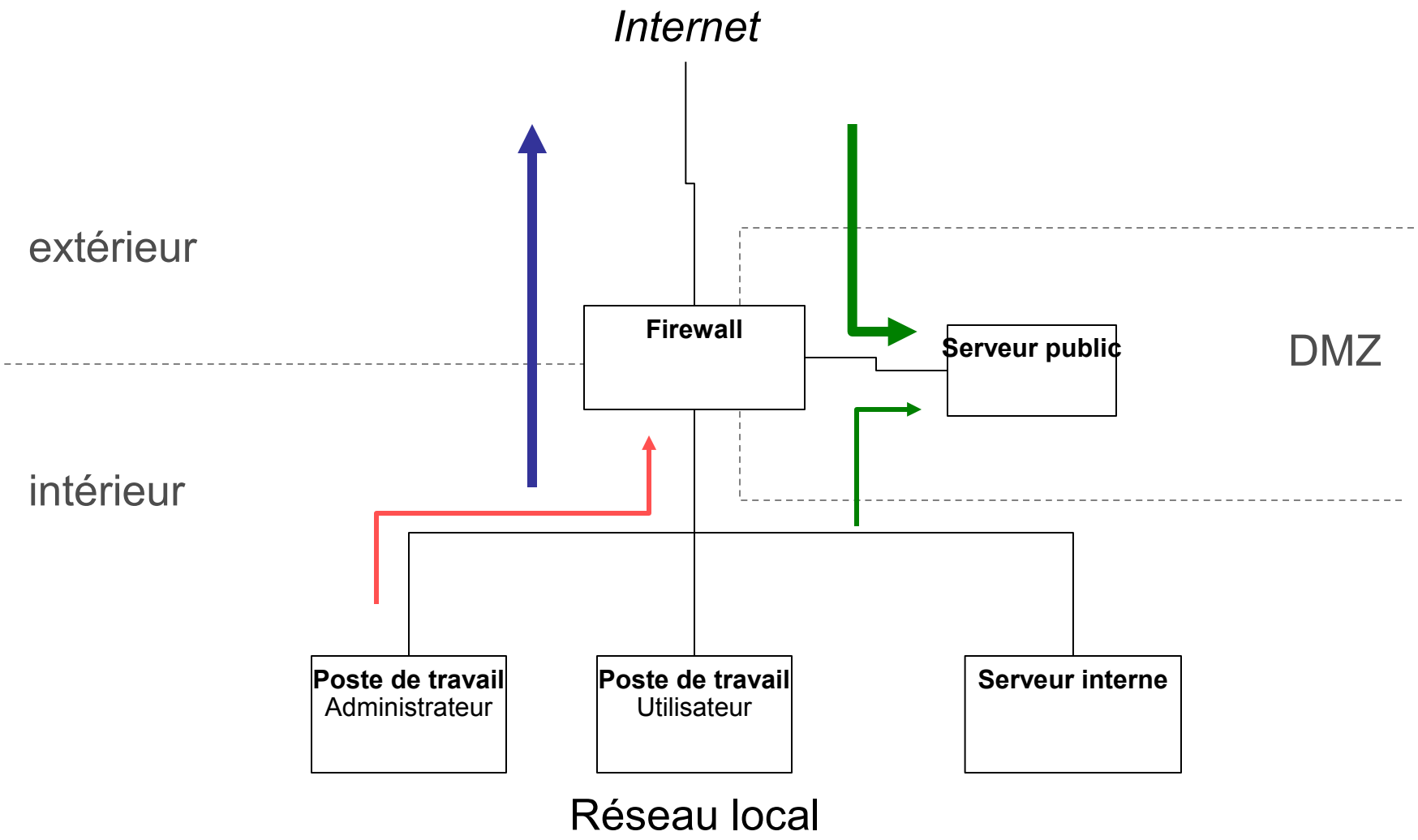
Diode


Internet
extérieur
intérieur
Firewall
Poste de travail
Administrateur
Poste de travail
Utilisateur
Serveur interne
Réseau local

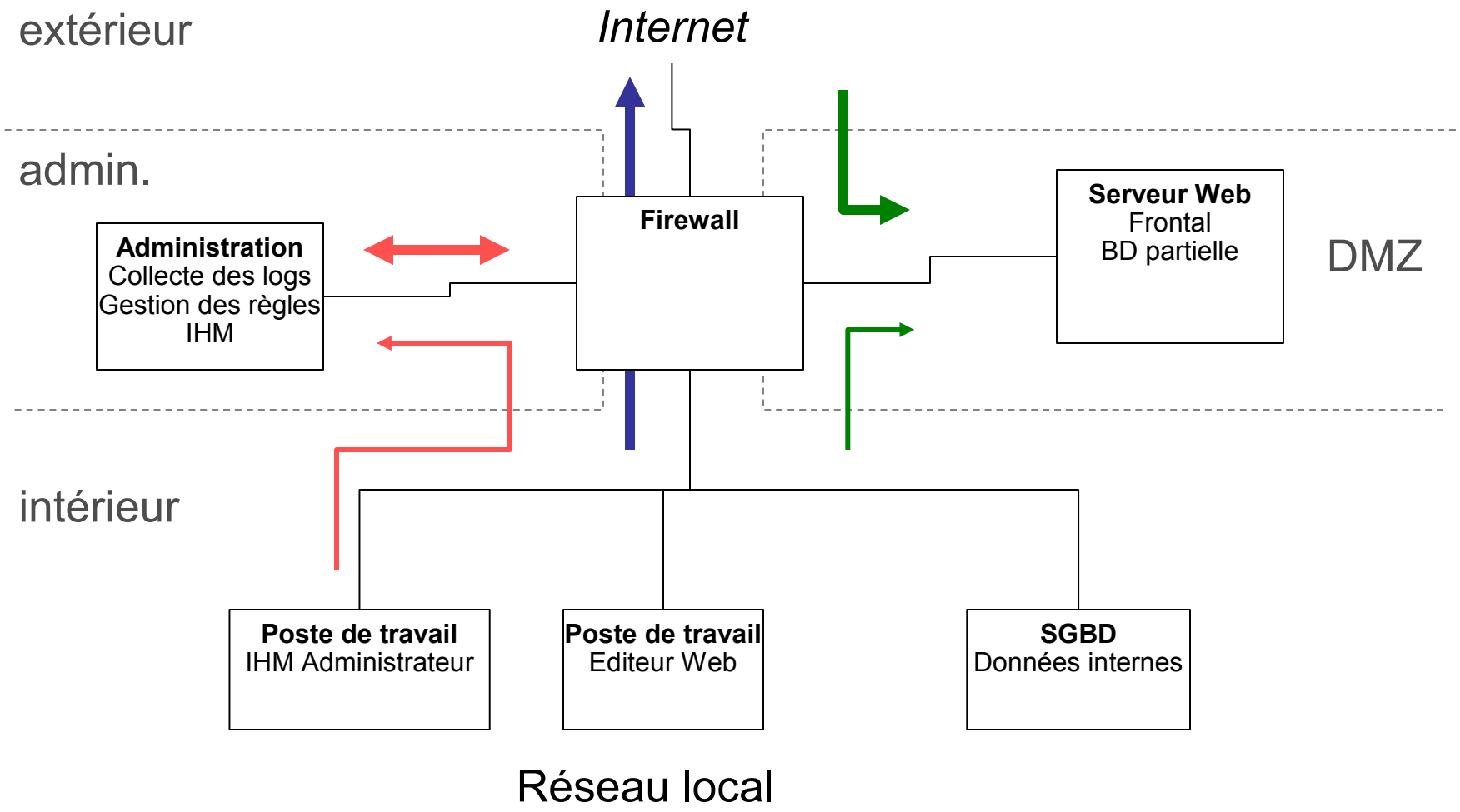
« DMZ » - Version historique



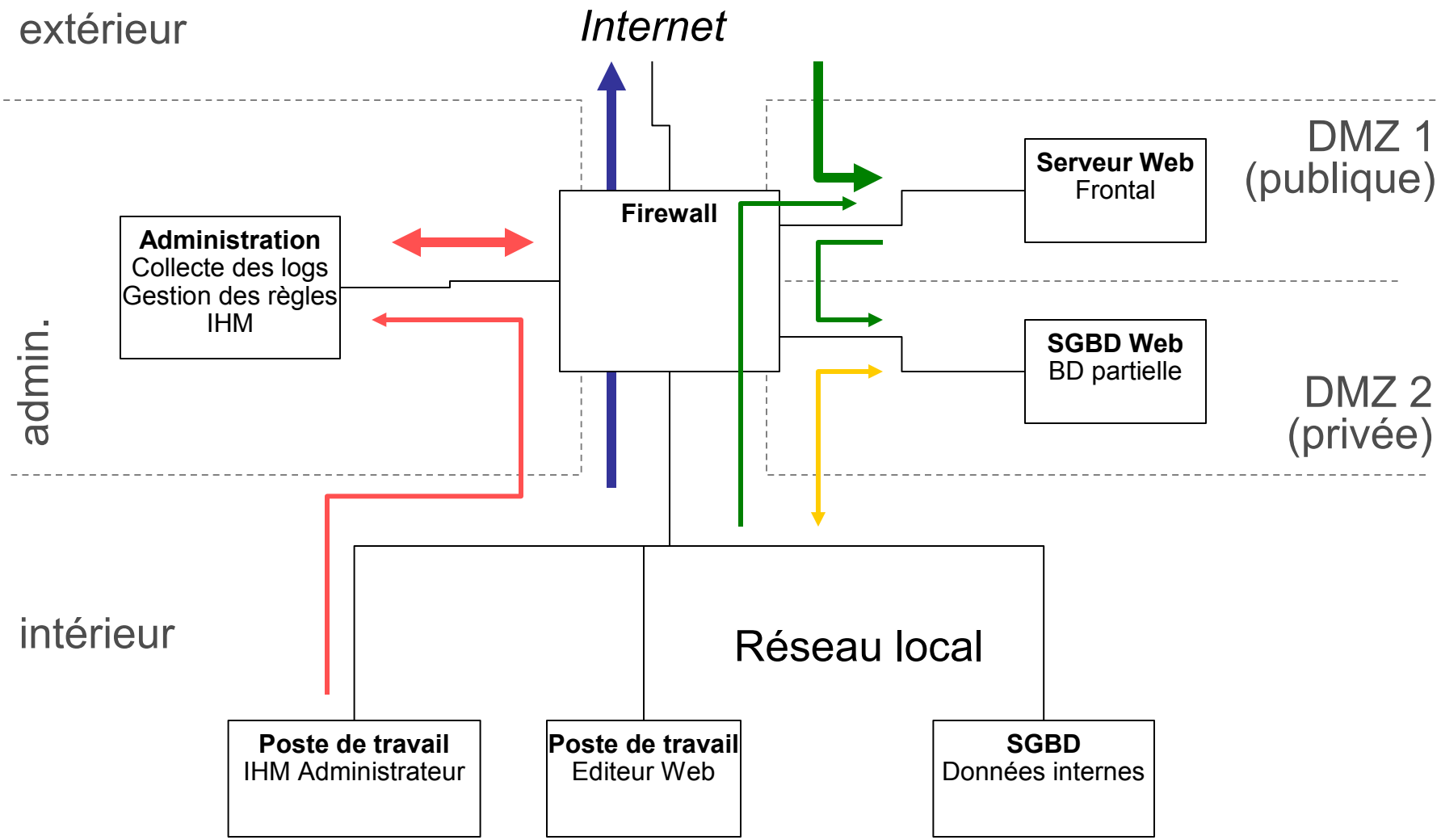
« DMZ » - Situation actuelle



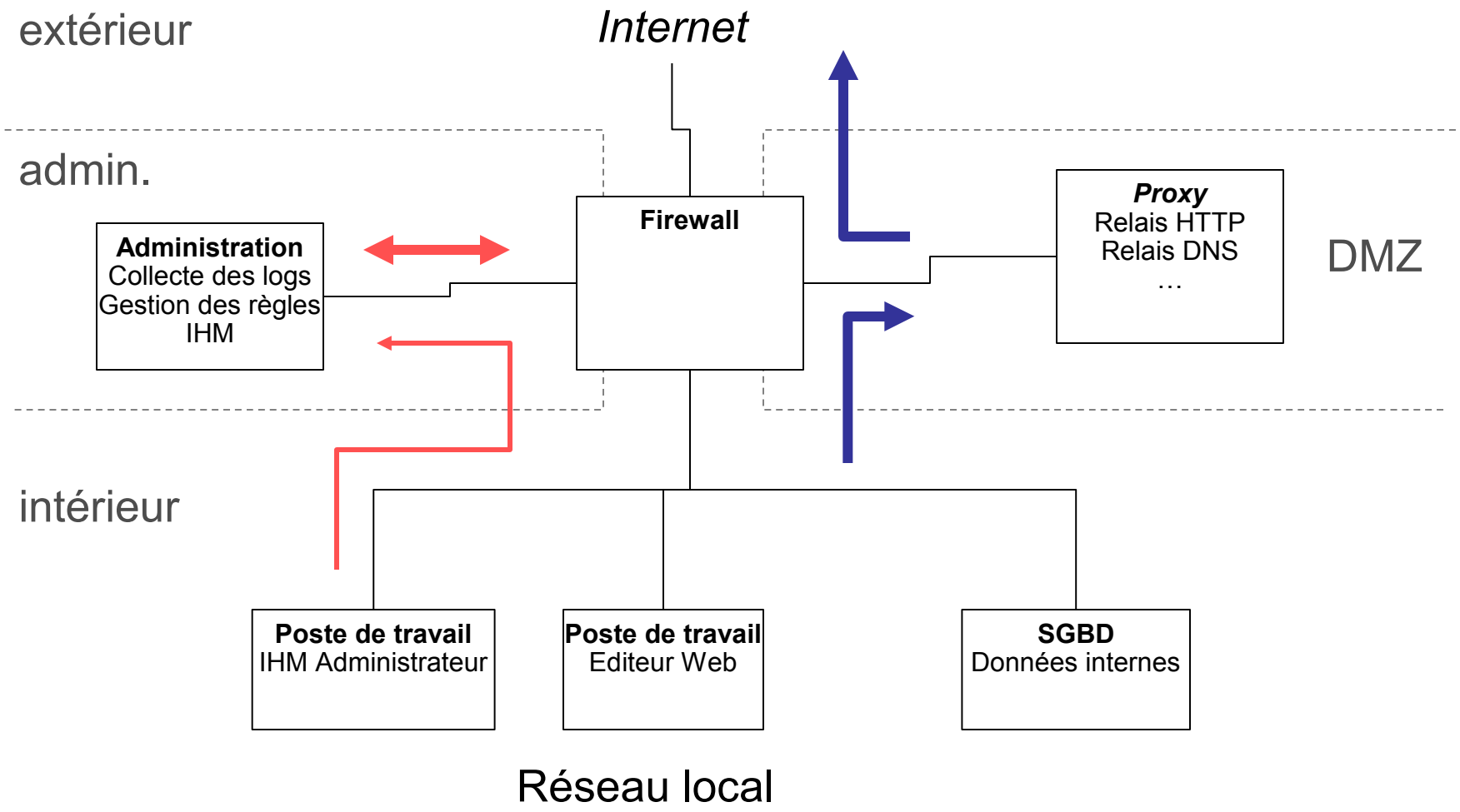
Administration



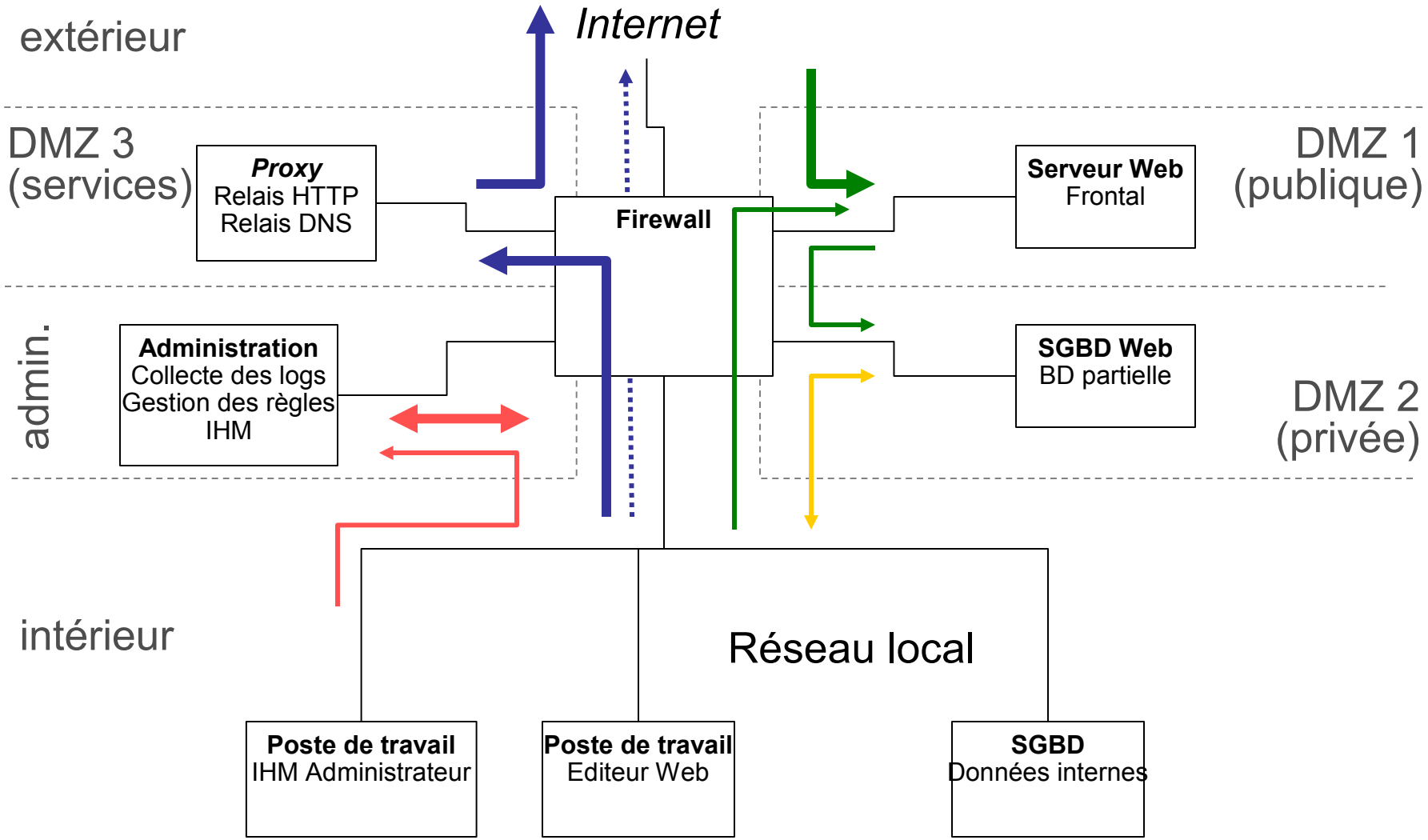
« 2 DMZ » – 5 interfaces



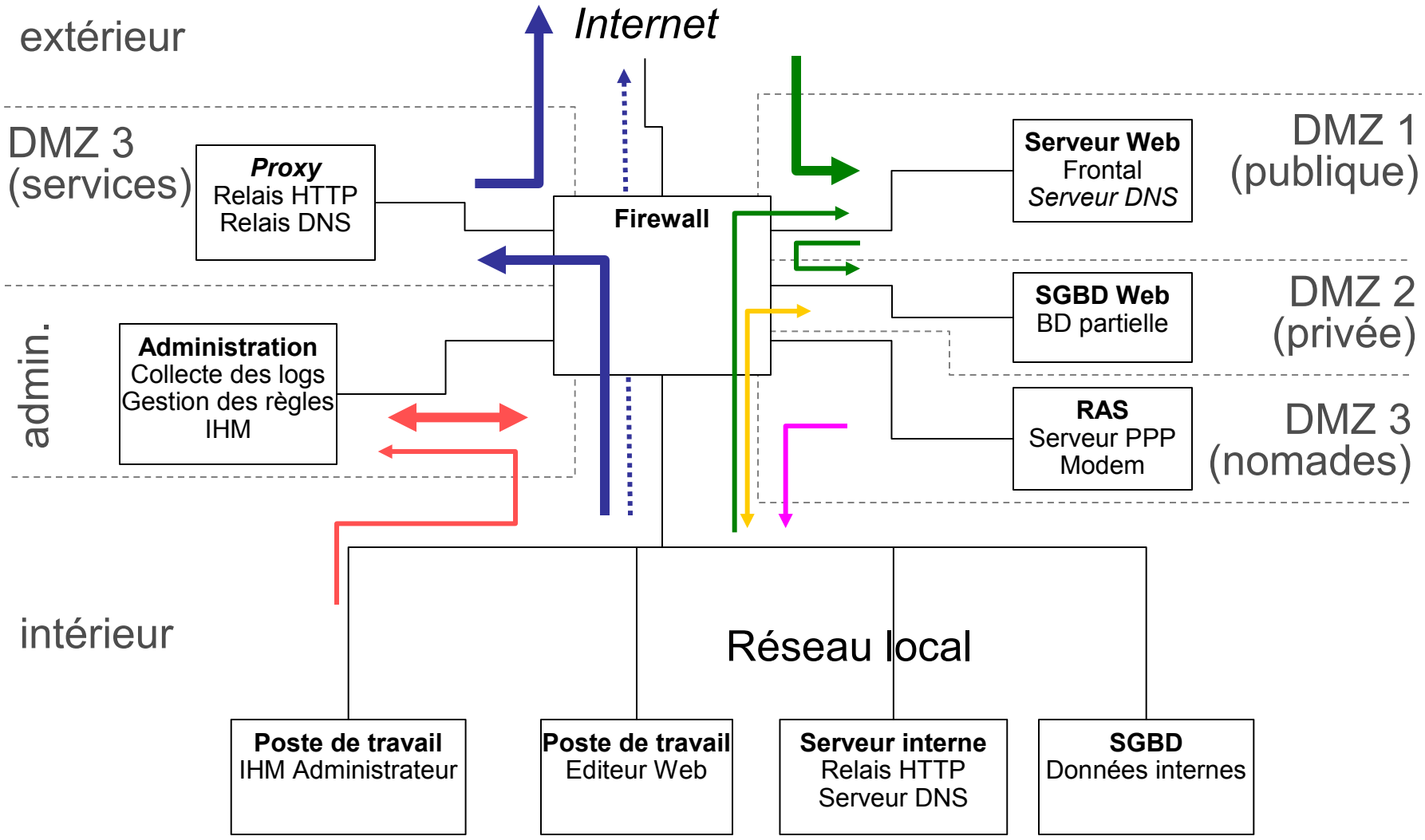
Autre usage d'une DMZ



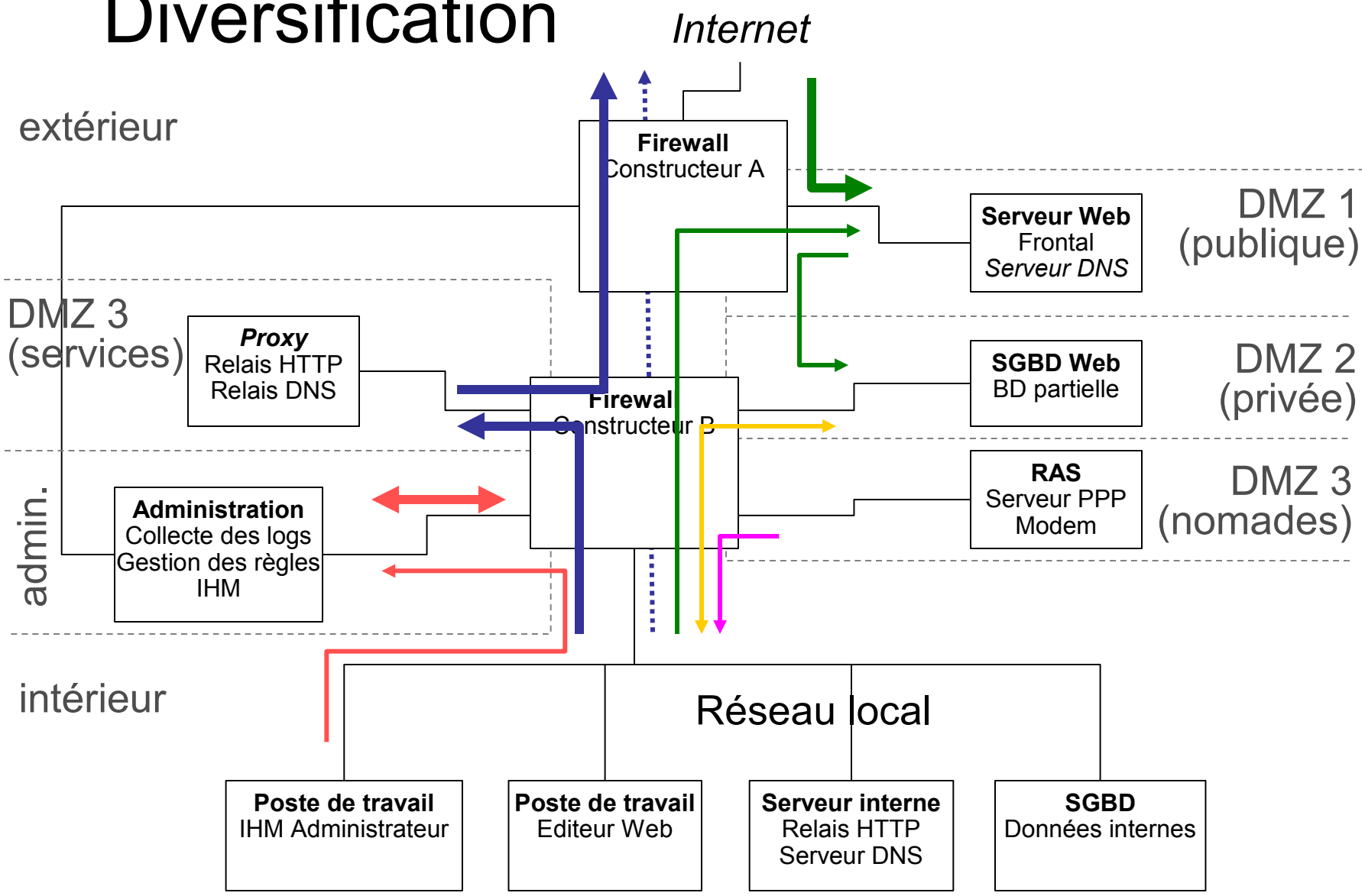
« 3 DMZ » – 6 interfaces



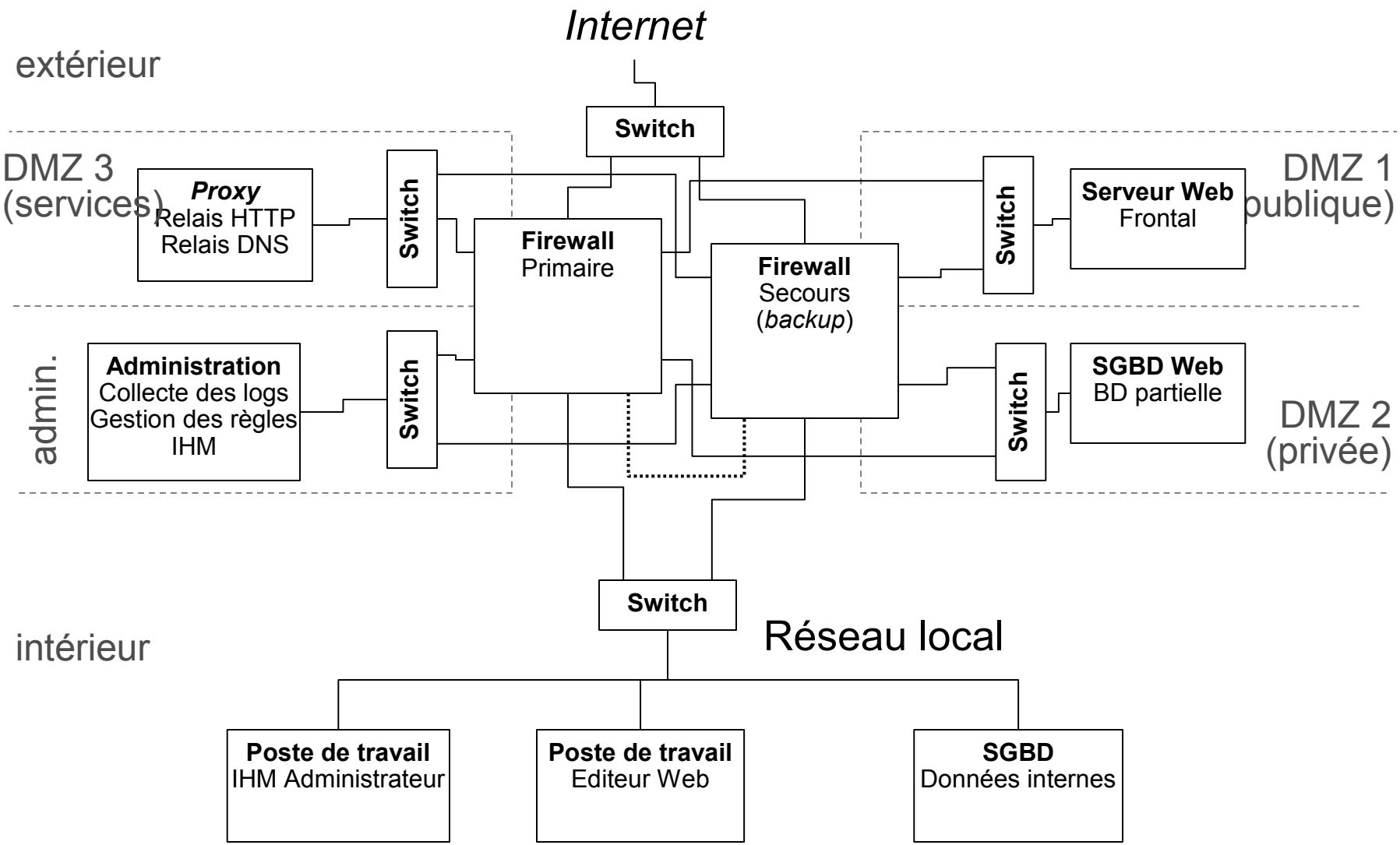
7 interfaces



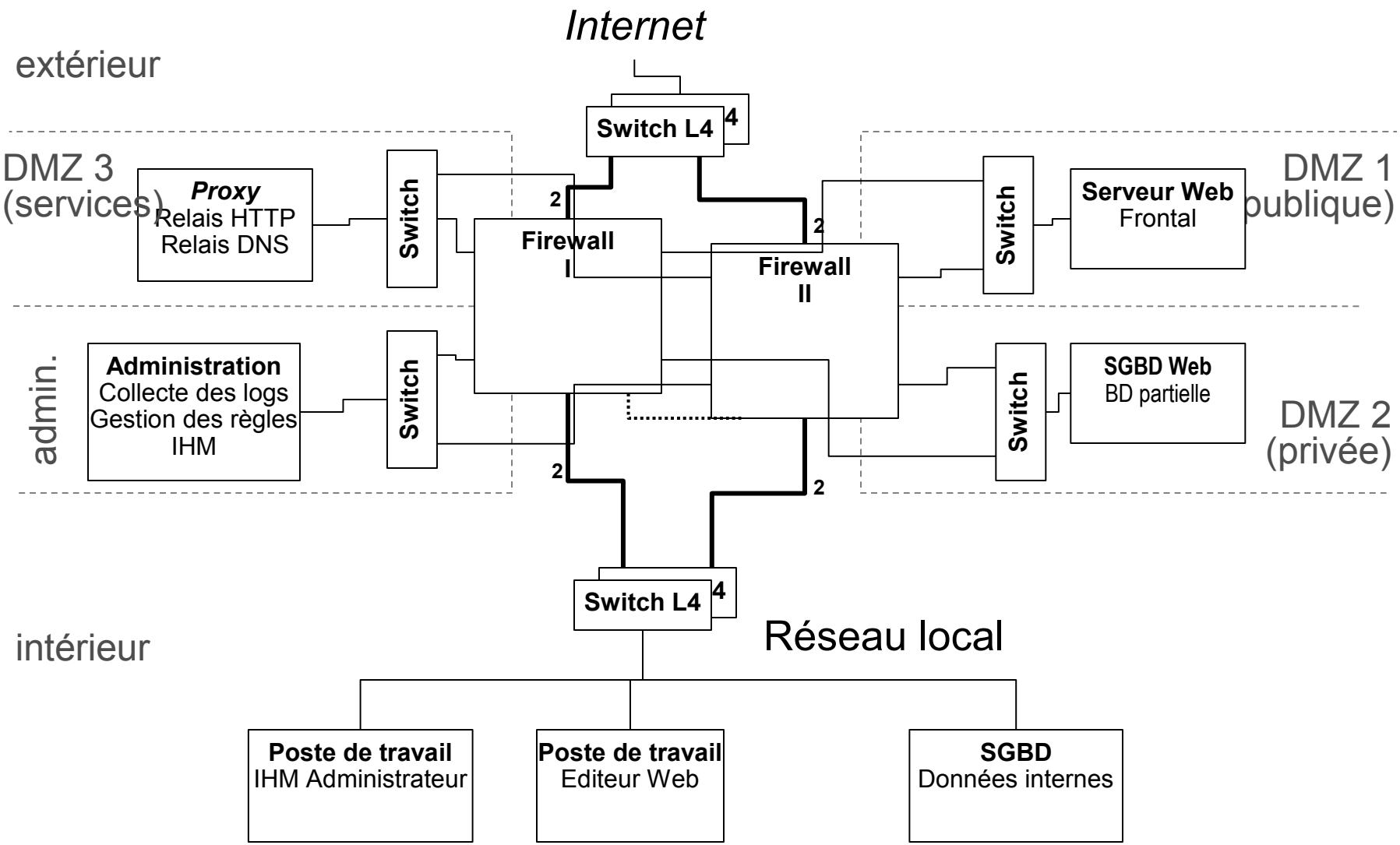
Diversification



Haute-disponibilité: *failover*



Haute-disponibilité : *load balancing*



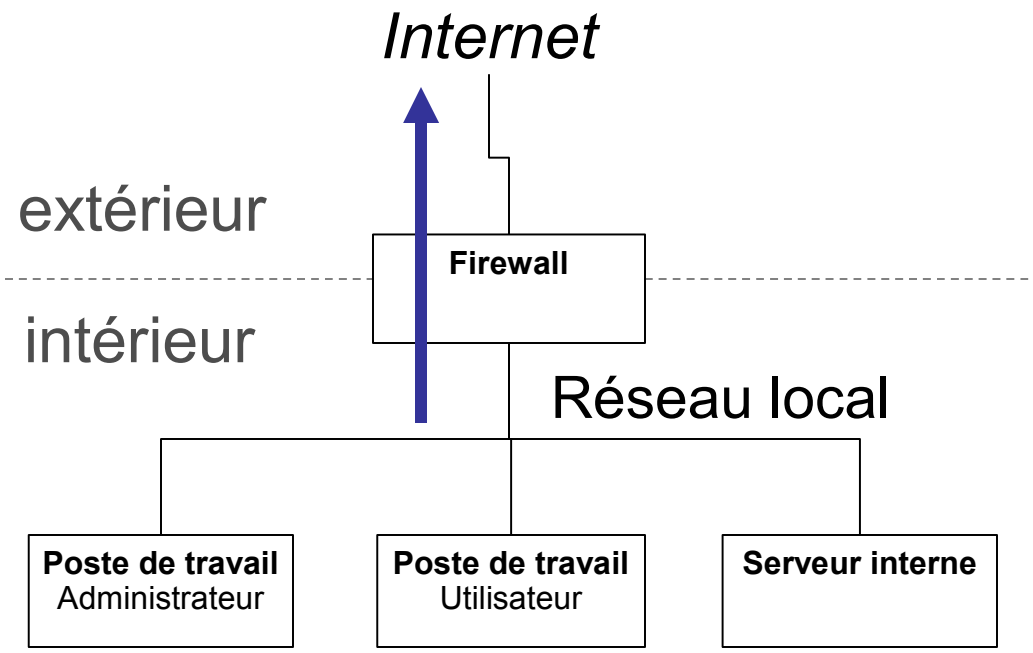
Diversification *et* haute-disponibilité avec équilibrage de charge pour un grand nombre de DMZ mises en oeuvre via des VLAN 802.1q

C’est possible.

Mais est-ce souhaitable ?

Translation d'adresses (NAT)

Multiplexage *N* @IP $\rightarrow$ *P* @IP (*NAT*)
Multiplexage *N* @(IP,TCP) $\rightarrow$ *P*@(IP,TCP) (*PAT*)
Association *N* @IP $\leftrightarrow$ *N* @IP (*static NAT*)



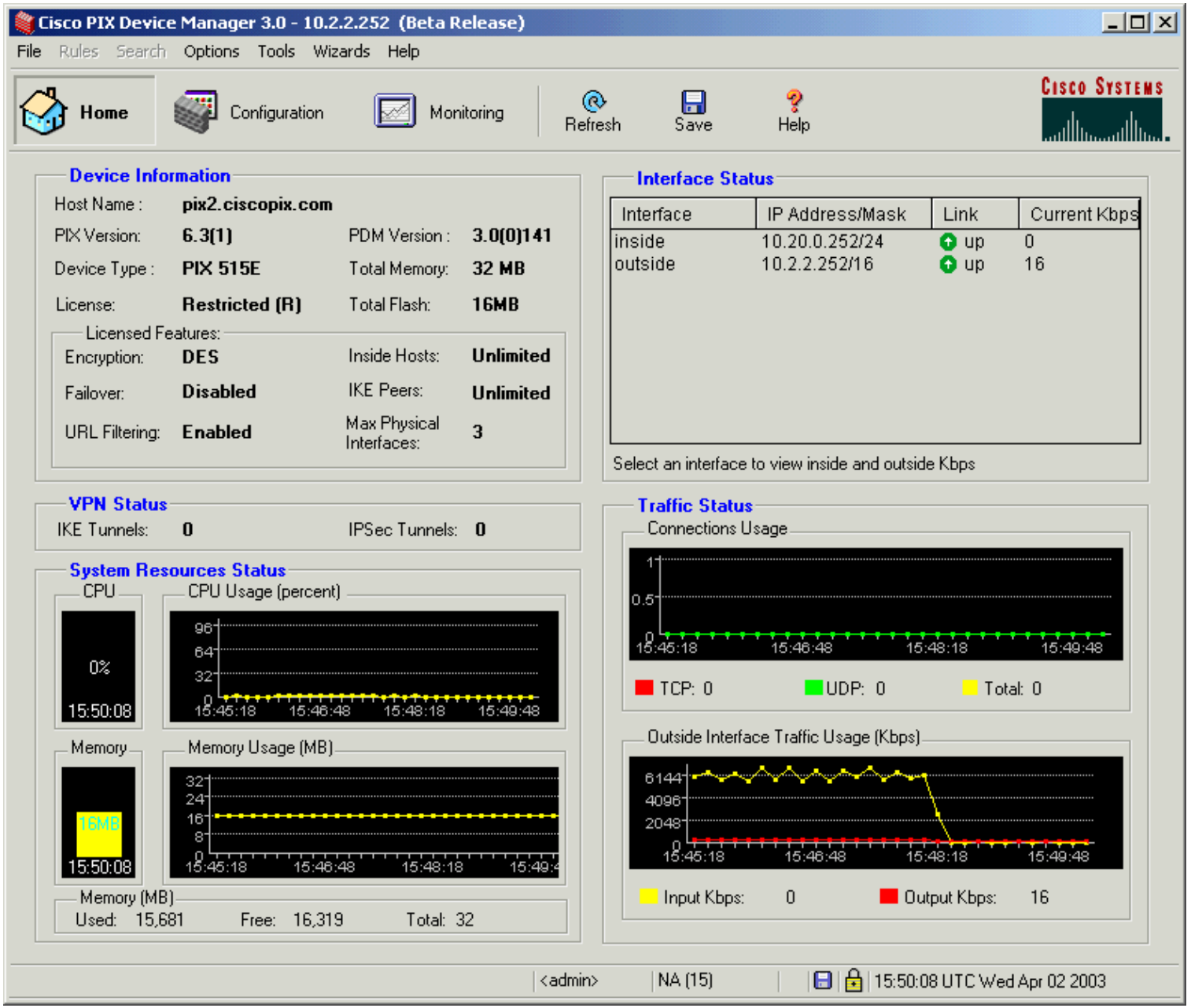
Translation d'adresses : compléments

- Le multiplexage est surtout naturel vis à vis du protocole orienté connexion (TCP) (à partir du port source)
- Il est également possible sur UDP, dans le cas des protocoles impliquant requête puis réponse (par ex.: DNS, etc.)
- Il peut aussi être introduit pour ICMP

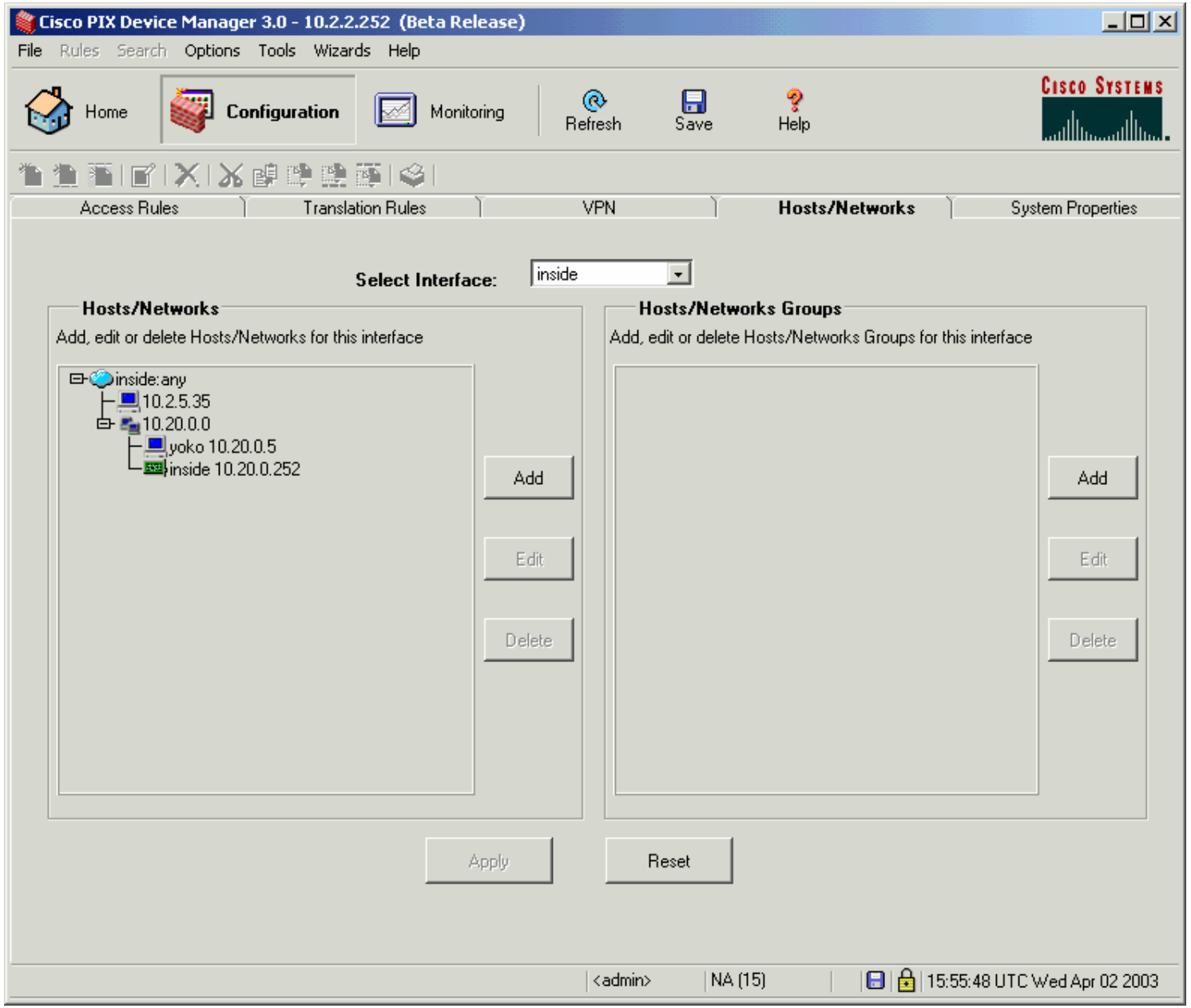
Firewall : fonctionnement interne

- Tables gérées
  - Tables d'état
  - Tables de translation
- Traces
- Fonctions de normalisation des paquets
- Analyses et fonctions avancées
  - Substitution des numéros de séquence
  - Inspection voire suivi protocolaire en mode noyau
  - Redirection vers des *proxy* en mode utilisateur

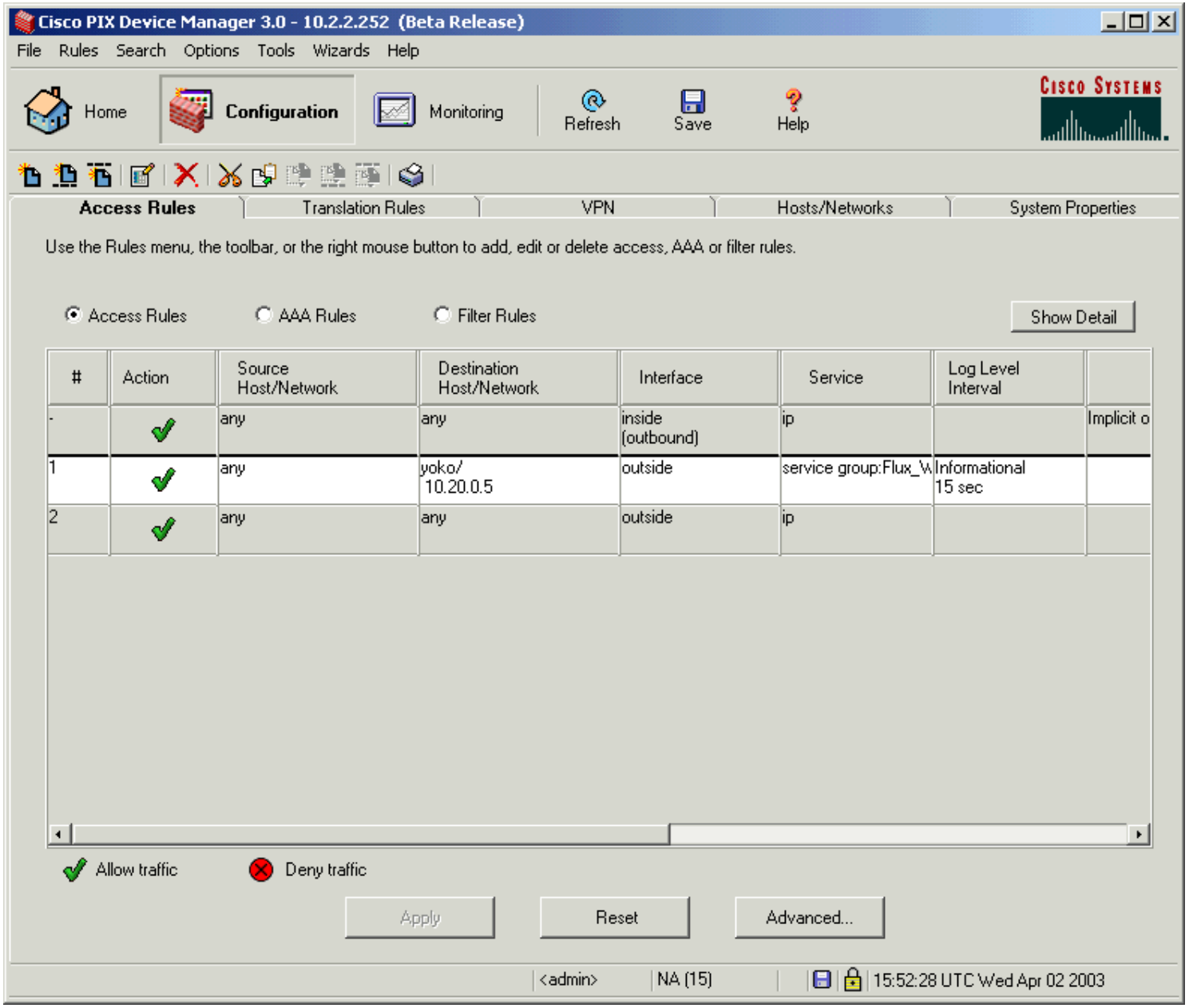
Exemple : Cisco PIX



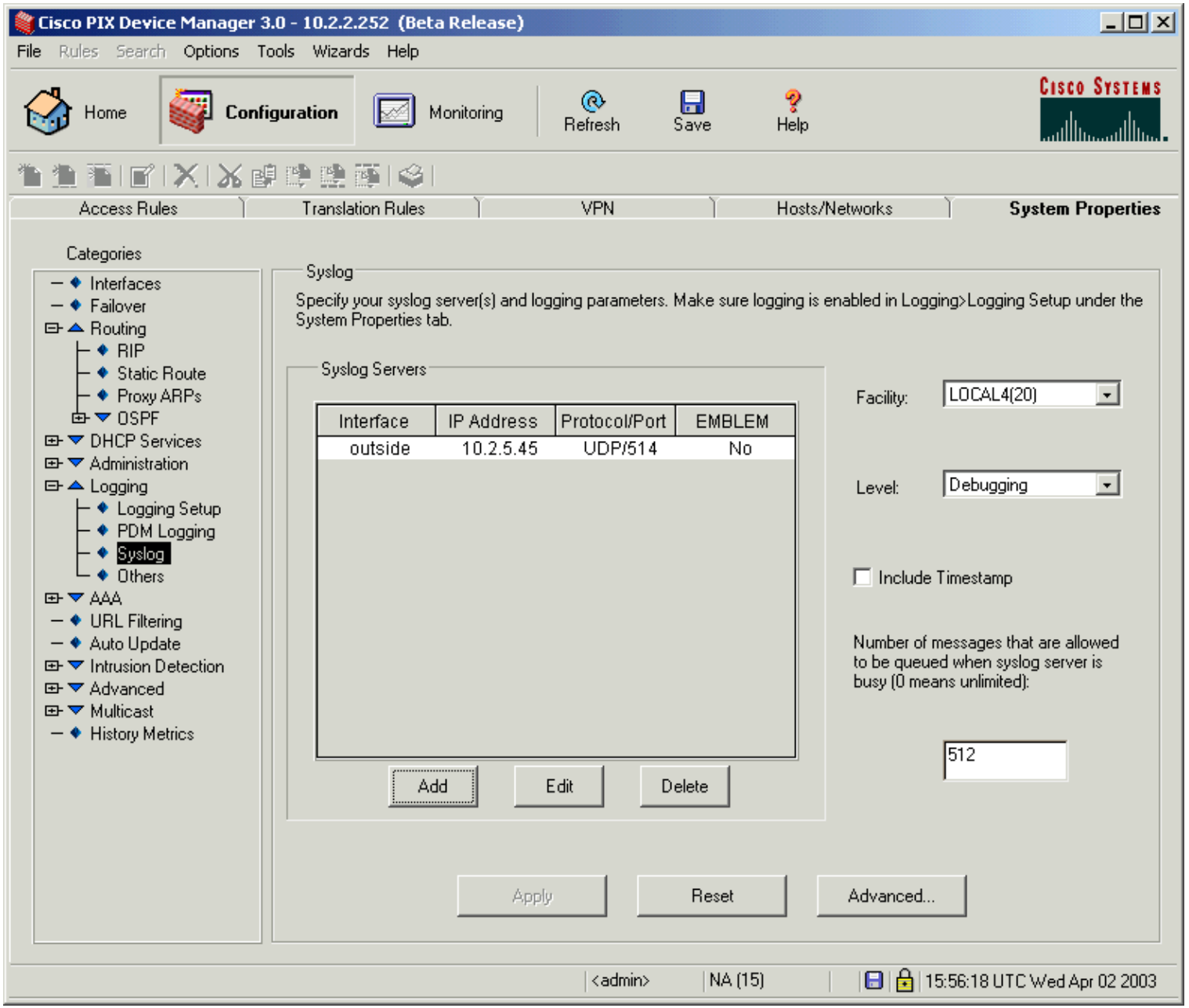
Exemple : Cisco PIX



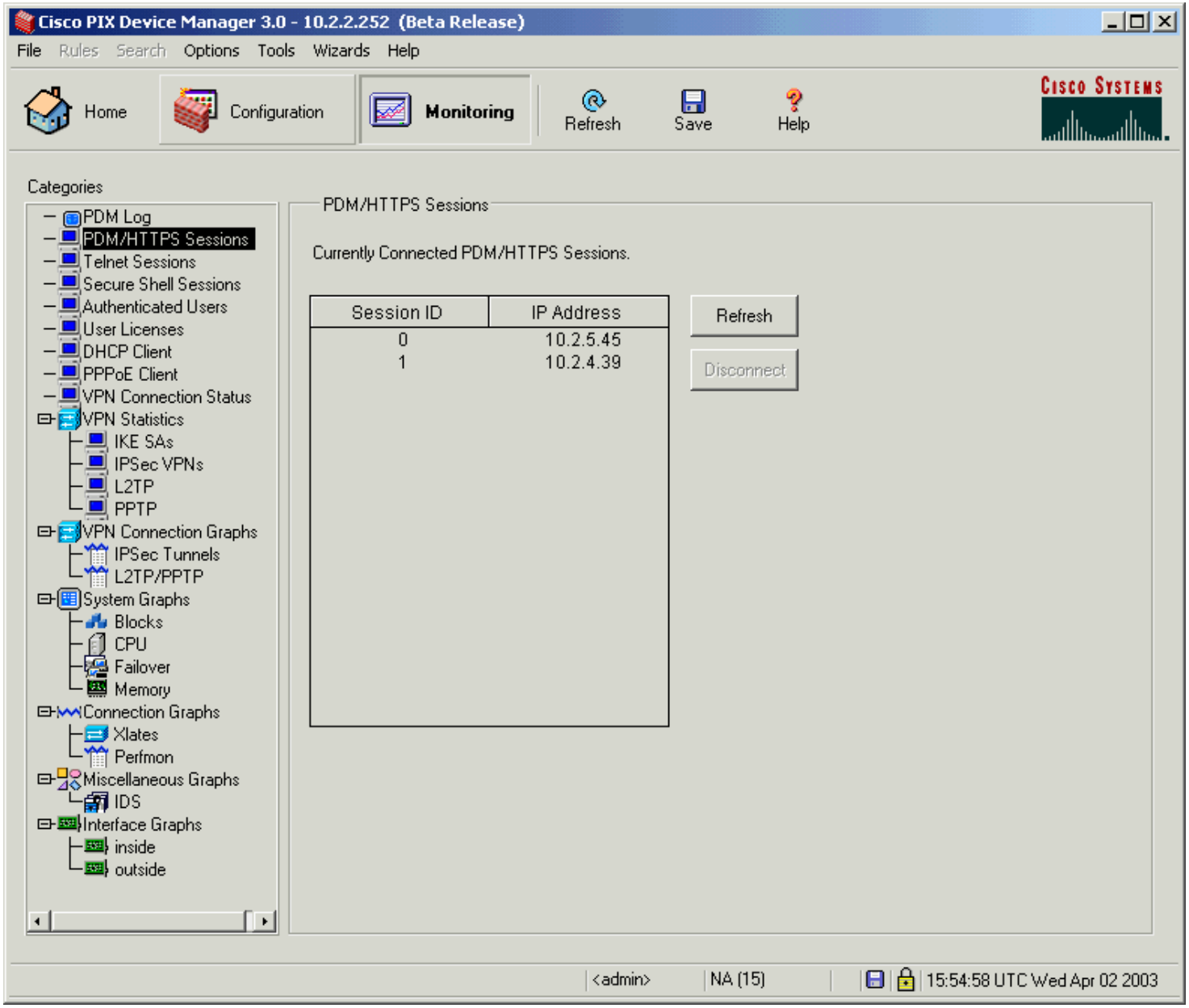
Exemple : Cisco PIX



Exemple : Cisco PIX



Exemple : Cisco PIX



Ex. : CheckPoint Firewall-1

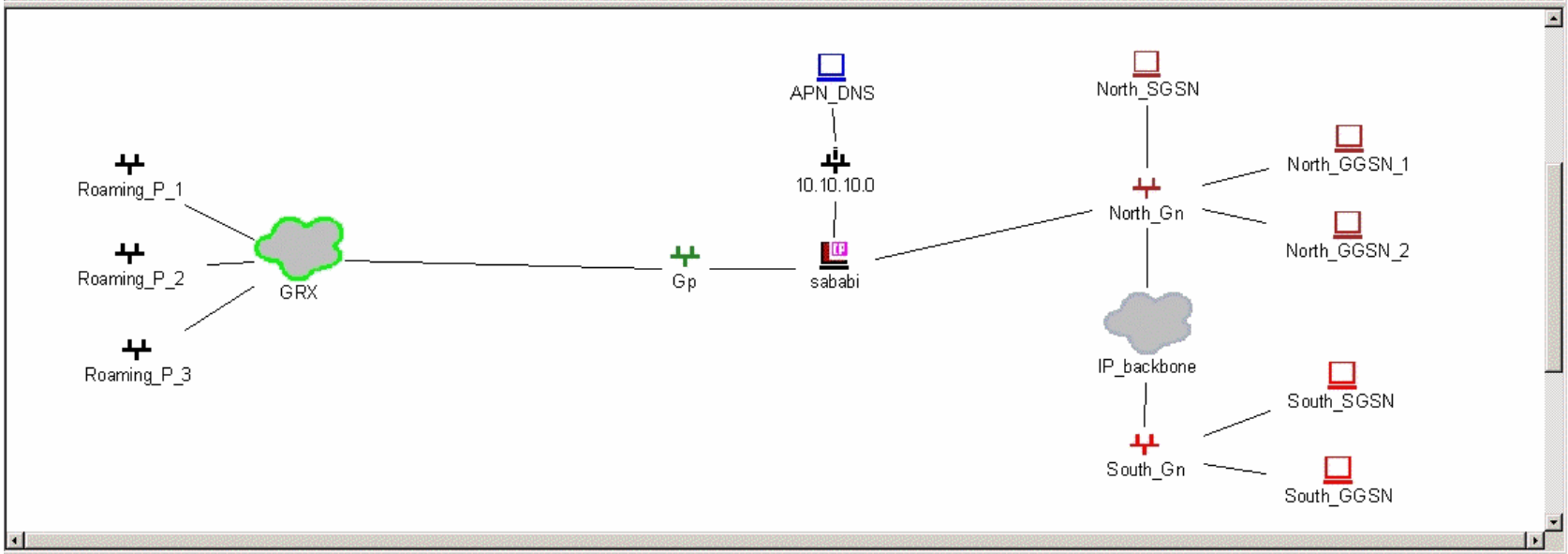
62.90.111.145 - Policy Editor - Standard

File Edit View Manage Rules Policy Topology Search Window Help

Setup VPN... Setup Extranet...

Security - Standard | Address Translation - Standard | Desktop Security - Standard

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	North_SGSN South_SGSN	* Any	gtp_default	accept	None	* Policy Targets	* Any	
2	Roaming_P_1	North_GGSN_1 North_GGSN_2 South_GGSN	gtp_default	accept	Log	* Policy Targets	* Any	
3	Roaming_P_2	South_GGSN	gtp_citibank	accept	Log	* Policy Targets	* Any	
4	Roaming_P_2 Roaming_P_3	North_GGSN_1	gtp_default	Encrypt	None	* Policy Targets	* Any	
5	Roaming_P_1 Roaming_P_3 Roaming_P_2	APN_DNS	dns	accept	None	* Policy Targets	* Any	



For Help, press F1 62.90.111.145 Read/Write NUM

Start | wewa - ... | sababi ... | Inbox - ... | joni - jo... | wewa - ... | Rationa... | wewa - ... | RE: Ima... | Tue 12 Feb 18:24

vlvl - C... | C:\Doc... | 62.90.1... | XnView ... | Z:\gtp\... | Captain... | logs for... | 62.90.1...

Ex. : CheckPoint Firewall-1

*local - Policy Editor - Standard

File Edit View Manage Rules Policy Topology Search Window Help

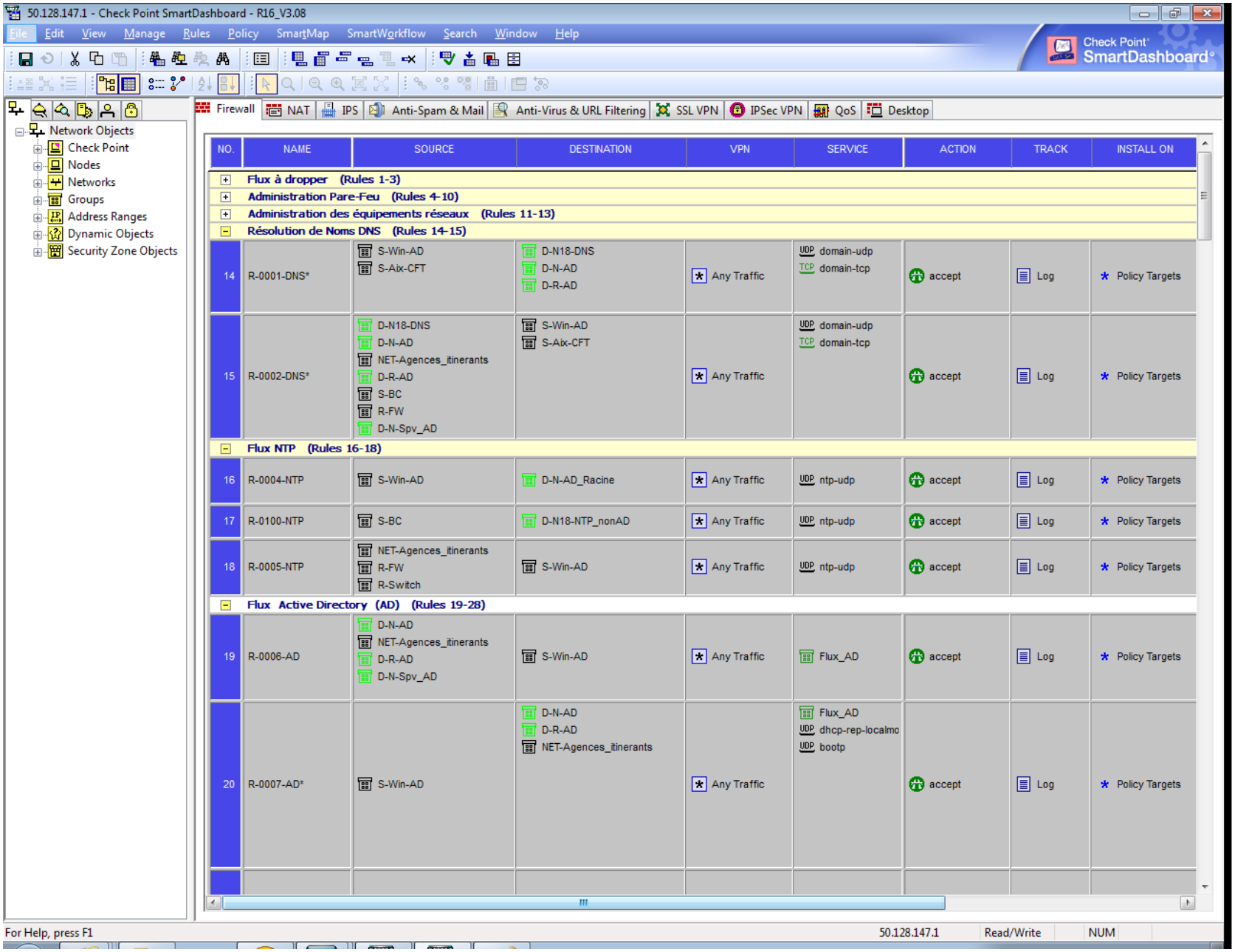
Setup VPN... Setup Extranet...

Security - Standard | Address Translation - Standard | QoS - Standard | Desktop Security - Standard

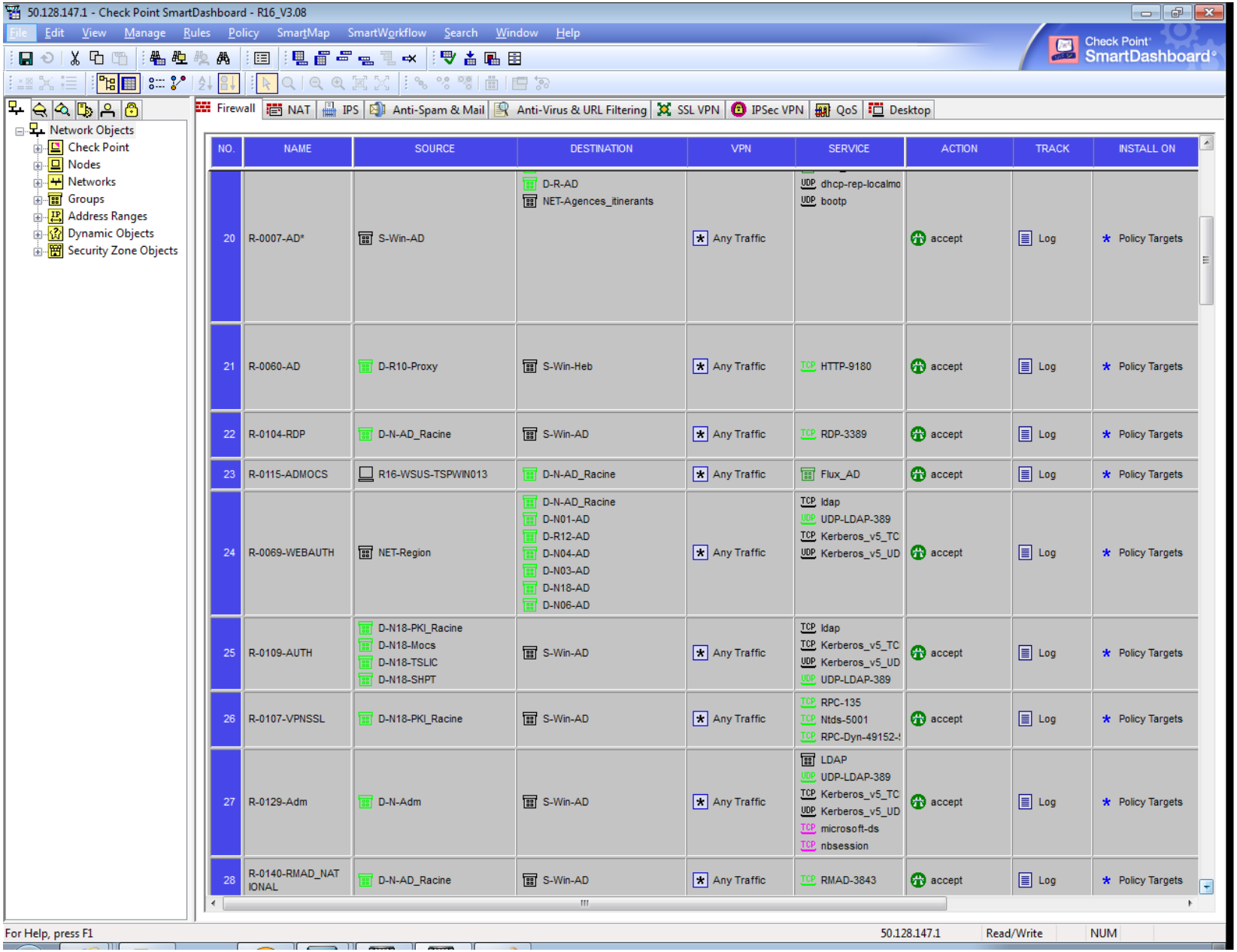
NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
3	* Any	LocalMachine	* Any	Drop	Alert	Dynamic_Addre:	* Any	Stealth the DAG
4	DMZ_net	Remote_Net Local_Net	* Any	Reject	Alert	* Policy Targets	* Any	Protect the Enterprise networks t the DMZ.
5	Sales@Any	Email_Server Local_Intranet_S Remote_Intranet Web_Server Public_FTP_Serv	pop-3 http ftp smtp	Client Encrypt	Log	* Policy Targets	* Any	VPN for selected Enterprise empl accessing servers via the Interne
6	Remote_VPN_Dc Net_Behind_Dyr	Local_Intranet_S	http	Encrypt	Log	* Policy Targets	* Any	Allow encrypted access to the lc intranet server
7	Net_Behind_Dyr Local_Net	Remote_Intranet	http	Encrypt	Log	* Policy Targets	* Any	Allow encrypted access to the re intranet server
8	Remote_Net Net_Behind_Dyr	Email_Server	pop-3 smtp	Encrypt	Log	* Policy Targets	* Any	Encrypt E-mail traffic with Remot
9	Local_Net	Email_Server	pop-3	accept	Log	Local_Gateway	* Any	Allow E-mail retrieval from Local
10	* Any	Email_Server	smtp	accept	Log	Local_Gateway	* Any	Allow access to Mail server.
11	Email_Server	* Any	smtp	accept	Log	Local_Gateway	* Any	Allow outgoing Mail traffic.
12	* Any	Web_Server Public_FTP_Serv	http ftp	accept	Log	Local_Gateway	* Any	Allow access to public Web and servers.
13	Local_Net	* Any	Internet_Service:	accept	Log	Local_Gateway	* Any	Allow selective outgoing traffic.
14	Remote_Net	* Any	Internet_Service:	accept	Log	Remote_Cluster	* Any	Allow selective outgoing traffic.
15	* Any	* Any	* Any	Drop	Alert	* Policy Targets	* Any	Disallow all other traffic and send an alert if encountered.

For Help, press F1 *local Read/Write NUM

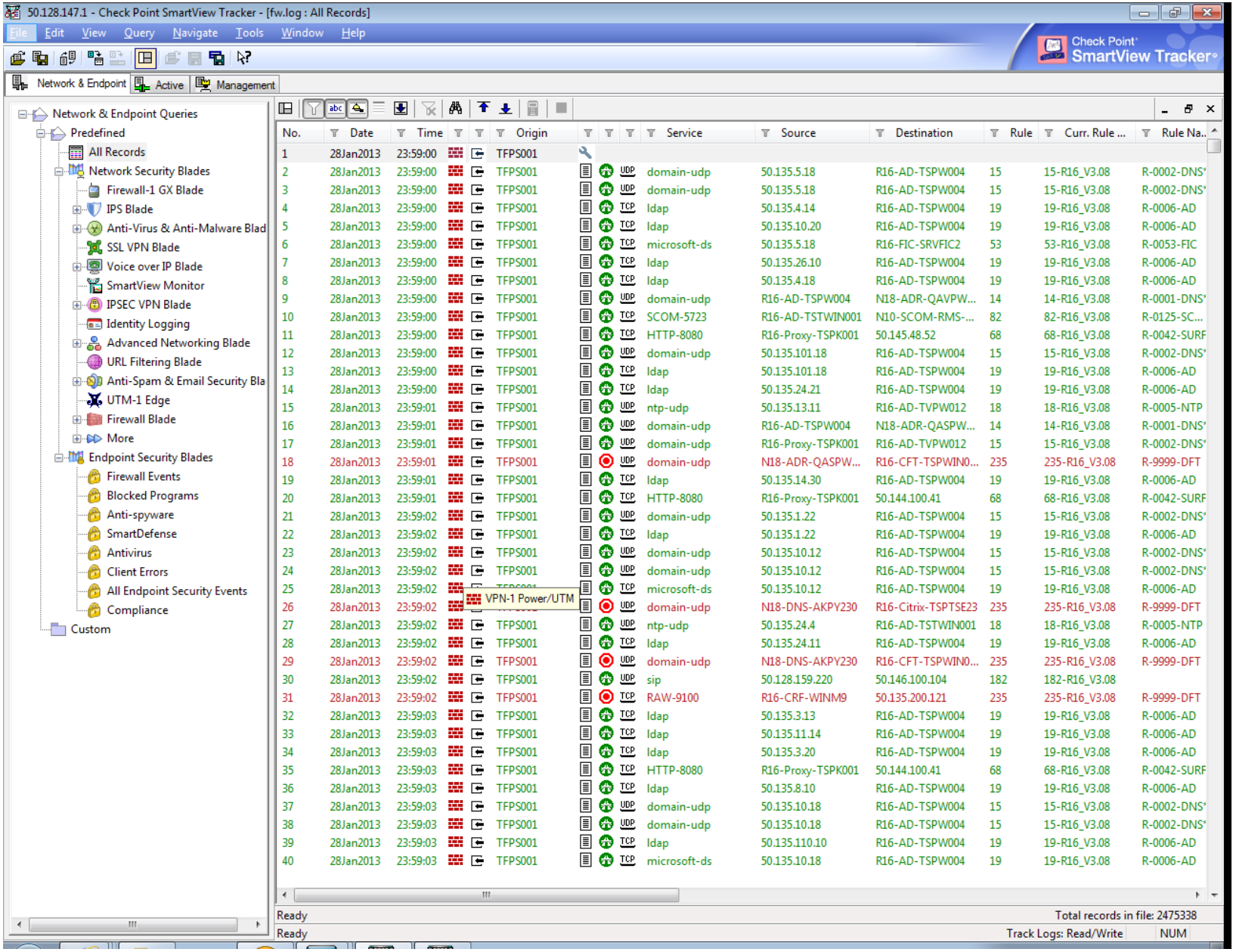
Ex. : CheckPoint Firewall-1



Ex. : CheckPoint Firewall-1



Ex. : CheckPoint Firewall-1



Comment gérer une autorisation dans la pratique ?

- Une application
  - vlc (césaco?)
  - http://mafreebox.freebox.fr/freeboxtv/playlist.m3u (on comprend mieux)
- Ne « marche pas », « Un numéro de porte ? »
- Premier pas

```
ortalo@hurricane:~$ ping -c 1 mafreebox.freebox.fr
PING freeplayer.freebox.fr (212.27.38.253) 56(84) bytes of data.
64 bytes from freeplayer.freebox.fr (212.27.38.253): icmp_seq=1 ttl=64
   time=1.16 ms
--- freeplayer.freebox.fr ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.168/1.168/1.168/0.000 ms
ortalo@hurricane:~$ tethereal -i eth1 host 212.27.38.253
```

...rien...

- Déterminer (toutes) les sources et destinations impliquées
  - IP_{eth1} et `212.27.38.253` (hmm...)
- Approche expérimentale : repérer les échecs les uns après les autres tout en contrôlant le trafic réseau

```
DROPPED IN= OUT=eth1 SRC=81.56.84.23 DST=212.27.38.253 LEN=52 TOS=0x00
   PREC=0x00 TTL=64 ID=48783 DF PROTO=TCP SPT=1047 DPT=80 SEQ=1610765695
   ACK=0 WINDOW=5840 RES=0x00 SYN URGP=0 OPT (020405B401010402010303 00)
DROPPED IN= OUT=eth1 SRC=81.56.84.23 DST=212.27.38.253 LEN=52 TOS=0x00
   PREC=0x00 TTL=64 ID=48784 DF PROTO=TCP SPT=1047 DPT=80 SEQ=1610765695
   ACK=0 WINDOW=5840 RES=0x00 SYN URGP=0 OPT (020405B401010402010303 00)
DROPPED IN= OUT=eth1 SRC=81.56.84.23 DST=212.27.38.253 LEN=52 TOS=0x00
   PREC=0x00 TTL=64 ID=1506 DF PROTO=TCP SPT=1048 DPT=80 SEQ=1611201085
   ACK=0 WINDOW=5840 RES=0x00 SYN URGP=0 OPT (020405B401010402010303 00)
```

- On ré-autorise HTTP

```
DROPPED IN= OUT=eth1 SRC=81.56.84.23 DST=212.27.38.253 LEN=52 TOS=0x00
   PREC=0x00 TTL=64 ID=22928 DF PROTO=TCP SPT=1082 DPT=554 SEQ=2534727009
   ACK=0 WINDOW=5840 RES=0x00 SYN URGP=0 OPT (020405B401010402010303 00)
DROPPED IN= OUT=eth1 SRC=81.56.84.23 DST=212.27.38.253 LEN=52 TOS=0x00
   PREC=0x00 TTL=64 ID=22929 DF PROTO=TCP SPT=1082 DPT=554 SEQ=2534727009
   ACK=0 WINDOW=5840 RES=0x00 SYN URGP=0 OPT (020405B401010402010303 00)
```

- On autorise TCP/554 sortant (?)

```
DROPPED IN=eth1 OUT= MAC=00:50:bf:29:e7:88:00:07:cb:05:ec:fc:08:00
   SRC=212.27.38.253 DST=81.56.84.23 LEN=1356 TOS=0x00 PREC=0xE0 TTL=57
   ID=18727 DF PROTO=UDP SPT=32803 DPT=1044 LEN=1336
DROPPED IN=eth1 OUT= MAC=00:50:bf:29:e7:88:00:07:cb:05:ec:fc:08:00
   SRC=212.27.38.253 DST=81.56.84.23 LEN=1356 TOS=0x00 PREC=0xE0 TTL=57
   ID=18982 DF PROTO=UDP SPT=32803 DPT=1044 LEN=1336
```

- La liste de diffusion arrive
- On autorise UDP entrant (>1025)

```
hurricane:~# dmesg | grep 212
DROPPED IN= OUT=eth1 SRC=81.56.84.23 DST=212.27.38.253 LEN=80 TOS=0x00
   PREC=0x00 TTL=64 ID=6 DF PROTO=UDP SPT=1065 DPT=32769 LEN=60
DROPPED IN= OUT=eth1 SRC=81.56.84.23 DST=212.27.38.253 LEN=44 TOS=0x00
   PREC=0x00 TTL=64 ID=7 DF PROTO=UDP SPT=1065 DPT=32769 LEN=24
```

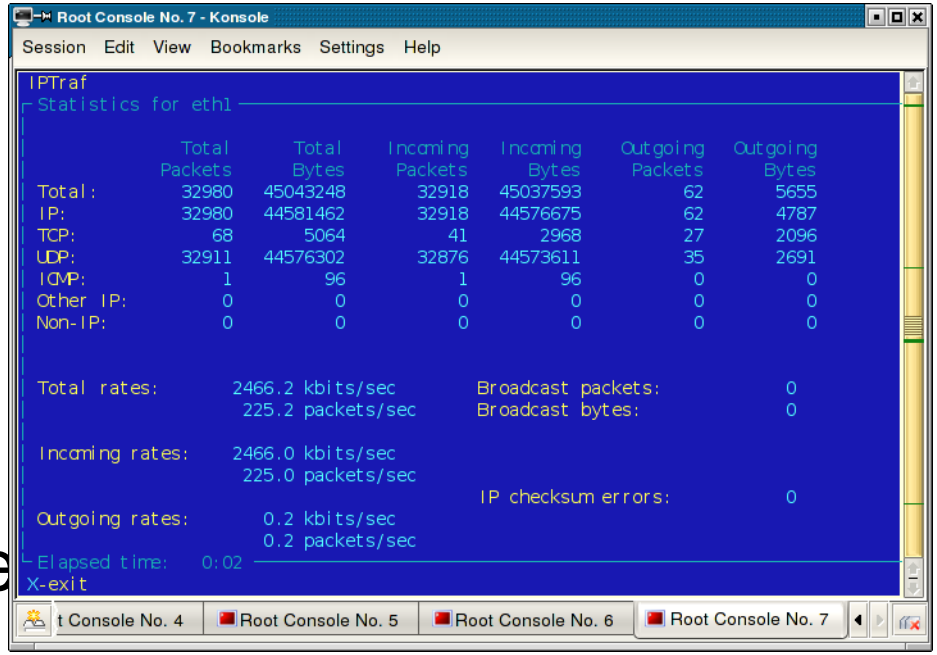
- Tiens, une émission sur les dinosaures...

- Les chaînes défilent toutes seules (?!?)

```
hurricane:~# dmesg | grep 212
DROPPED IN= OUT=eth1 SRC=81.56.84.23 DST=212.27.38.253 LEN=80 TOS=0x00
   PREC=0x00 TTL=64 ID=6 DF PROTO=UDP SPT=1065 DPT=32769 LEN=60
DROPPED IN= OUT=eth1 SRC=81.56.84.23 DST=212.27.38.253 LEN=44 TOS=0x00
   PREC=0x00 TTL=64 ID=7 DF PROTO=UDP SPT=1065 DPT=32769 LEN=24
```

- On autorise l'UDP sortant vers la plage 32000-33999
- « Ca marche. »

```
hurricane:~# dmesg | grep 212
hurricane:~# iptraf
hurricane:~#
```



- Au fait... la docume

Plan (2/2)

- Protection utilisées dans la pratique
  - Protection réseau et *firewall*
  - **Systèmes d'authentification**
  - Chiffrement de flux et VPN
- Digressions (RàZ, OpenBSD, 1984)
- Surveiller, analyser et gérer
  - Détection d'intrusion
  - Audit, tests d'intrusion
  - Administration, exploitation et suivi de la sécurité
  - Observation et surveillance
- Protection des applications usuelles

Authentification

- Codes d'accès (« Sésame, ouvre-toi ! »)
- Numéros (pistes ISO, codes barres, RFID, etc.)
- Nom d'utilisateur / mot de passe
- Clef publiques/clefs privés: RSA, DSA pour SSH, IKE, etc.
- Authentification forte des utilisateurs
  - S/Key
  - Mots de passe jetables
  - Cartes à puce et *token*
- …et les applications ?

Méthodes d'authentification

- Authentification locale
  - danger: divulgation du mot de passe en clair
    ⇒ chiffrement spécifique
- Défi réponse
  - défi: $\{aléa\}_{Ku}$ réponse: $\{aléa+1\}_{Ku}$
- Mots de passe jetables
- Systèmes cartes à puce (clé symétrique)
  - $K_{fille} = \{id\}_{K_{mère}}$
- Authentification « *zero knowledge* »

Le mot de passe

- C’est toujours la technique reine
- Elle combine l’identifiant (le nom d’utilisateur) et l’authentifiant (mot de passe secret)
- Cet authentifiant est stocké à disposition du système d’authentification
  - sous forme « obscurcie »
  - sous forme chiffrée
  - sous une forme chiffrée résistante
  - parfois en clair
- Ne pas confondre avec un(e) « *passphrase* »

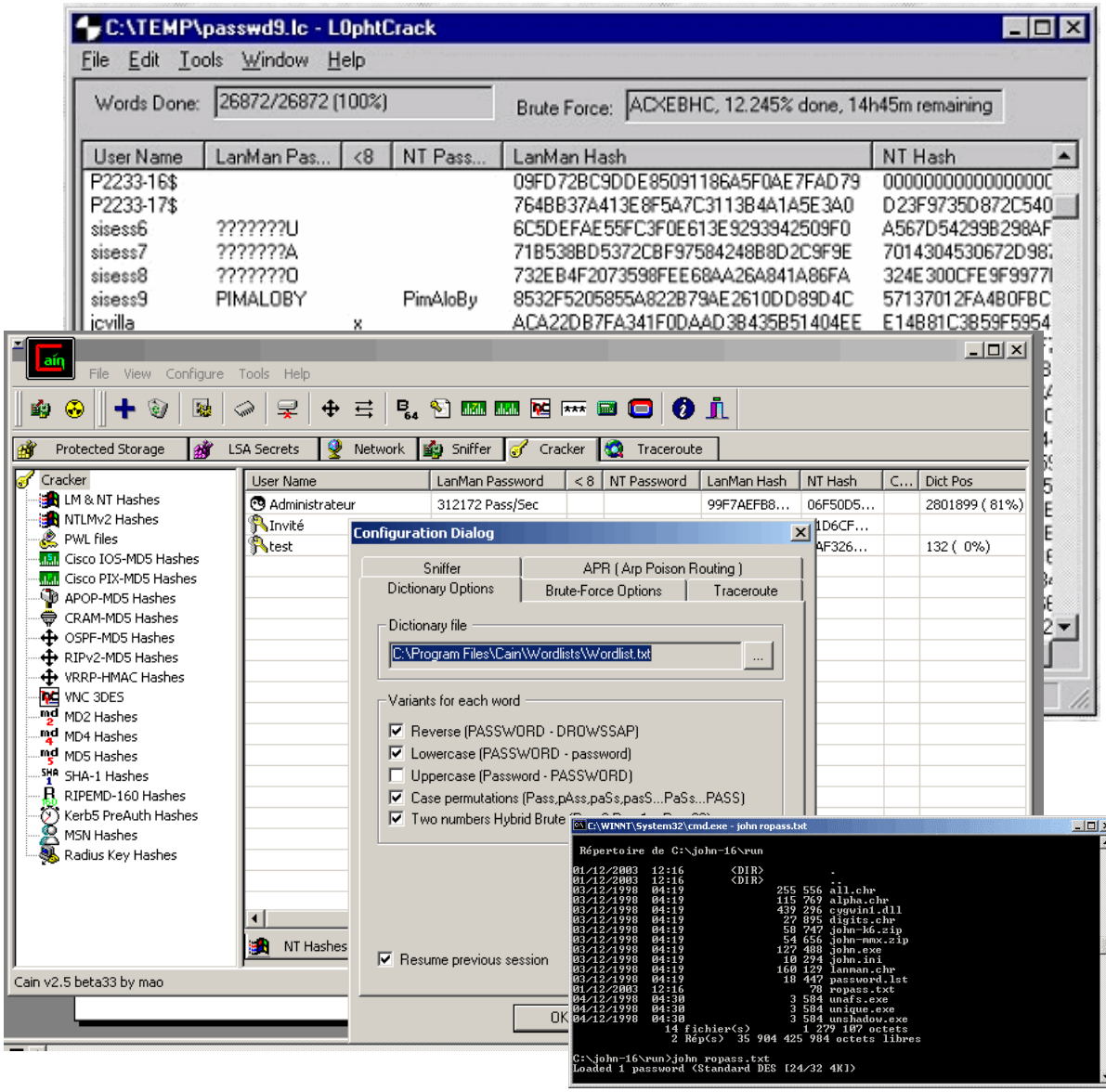
Un bon mot de passe

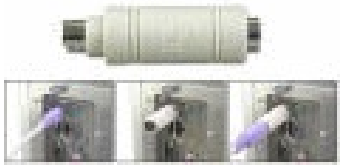
- Personnel
  spécifique à chaque individu
- Fiable
  durablement mémorisé
- Résistant
  qui ne soit pas facile à deviner pour un tiers

L’attaque des mots de passe

- Demander à l’utilisateur
- Dans la poubelle (ou sous le clavier)
- A la source (Cheval de Troie, enregistreur clavier)
- Inversion du codage
- Attaque par dictionnaire (*password cracking*)
  - Nécessite le vol de la forme stockée (chiffrée)
  - Essais successifs par rapport à un dictionnaire pré-établi
  - Prise en compte de règles de combinaison simples (à l’envers, ajout d’un ou deux chiffres)
  - La recherche exhaustive est accessibles sur les alphanumériques (avec une longueur limitée : 6 en général)
  - Surtout intéressant sur un ensemble de comptes
  - Forme directe d’une attaque générale (*codebook-based*)
  - Le choix du dictionnaire est important (prénoms, acronymes)

Des outils



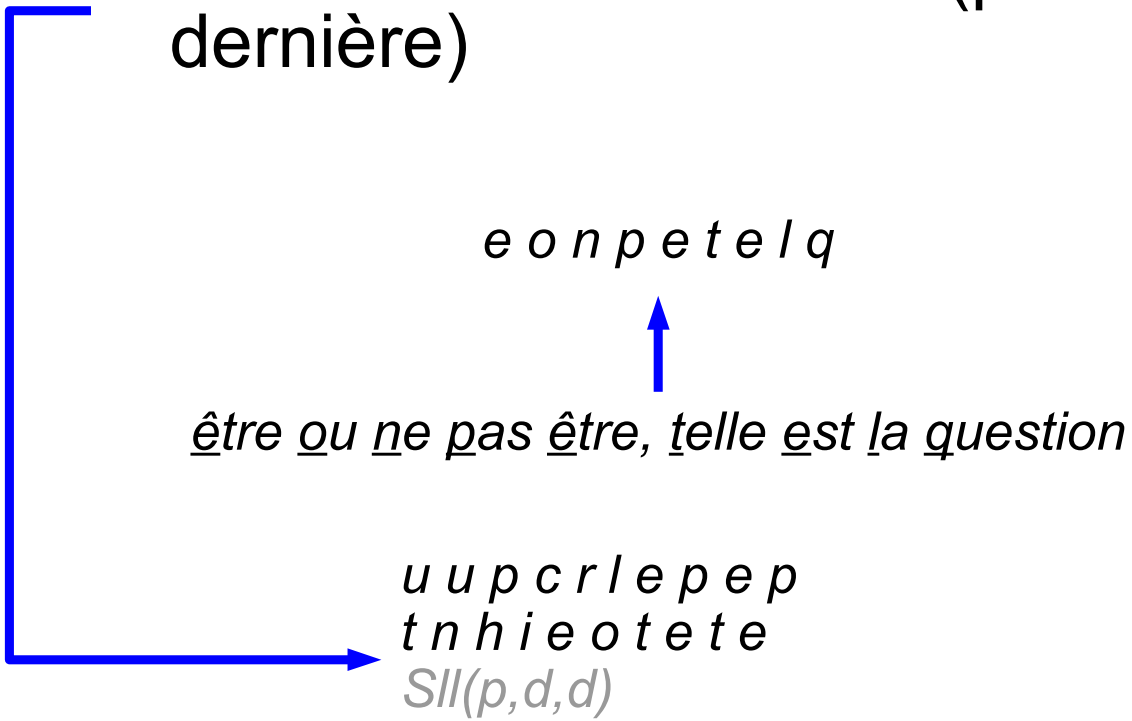


> 10^6 $pass_{NT}$ / s

http://lasecpc13.epfl.ch/ntcrack/

Un bon mot de passe

- Utiliser une phrase (citation) relativement longue et peut-être personnelle
- Sélectionner les lettres (première, deuxième, dernière)



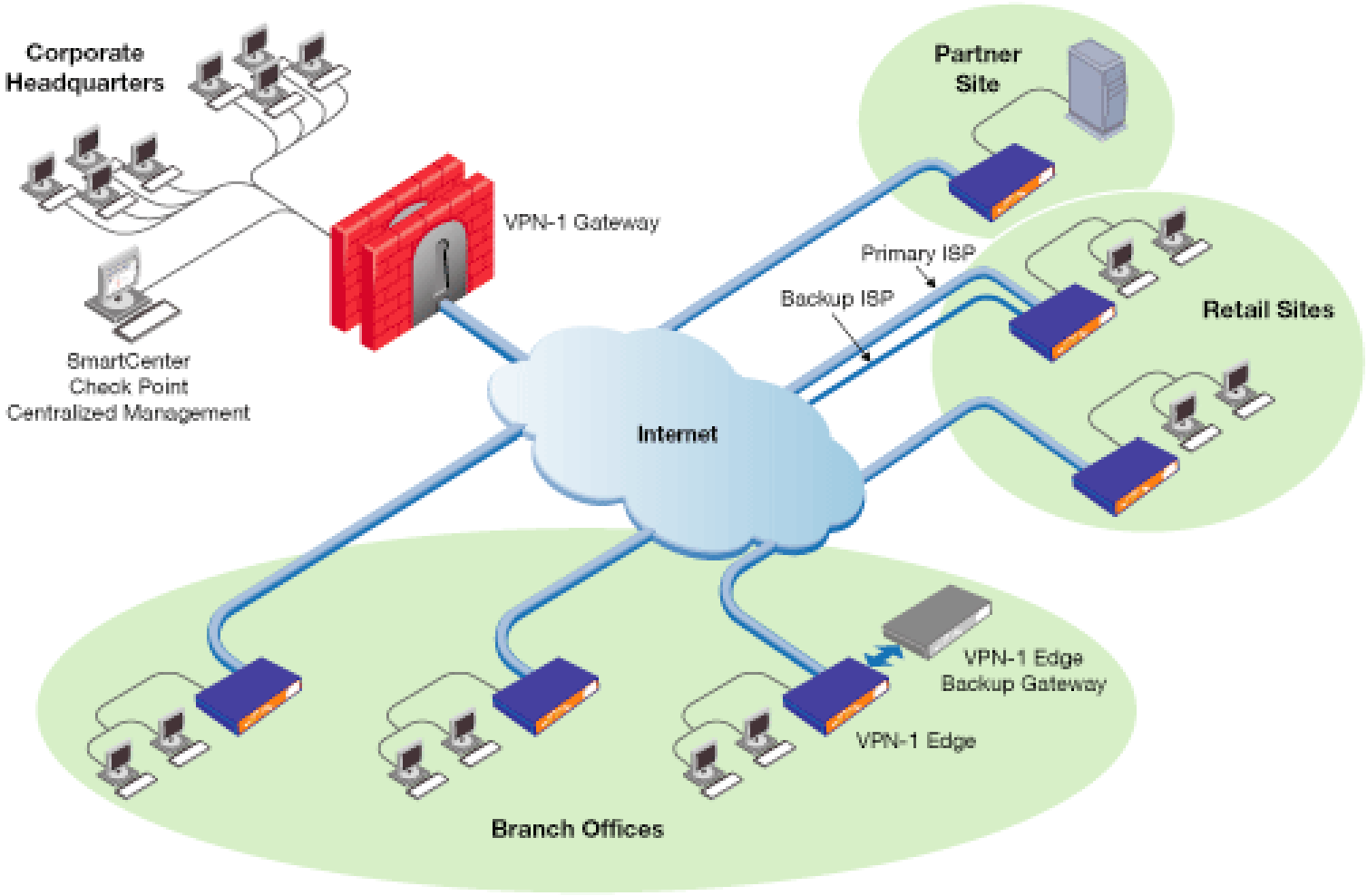
Plan (2/2)

- Protection utilisées dans la pratique
  - Protection réseau et *firewall*
  - Systèmes d'authentification
  - **Chiffrement de flux et VPN**
- Digressions (RàZ, OpenBSD, 1984)
- Surveiller, analyser et gérer
  - Détection d'intrusion
  - Audit, tests d'intrusion
  - Administration, exploitation et suivi de la sécurité
  - Observation et surveillance
- Protection des applications usuelles

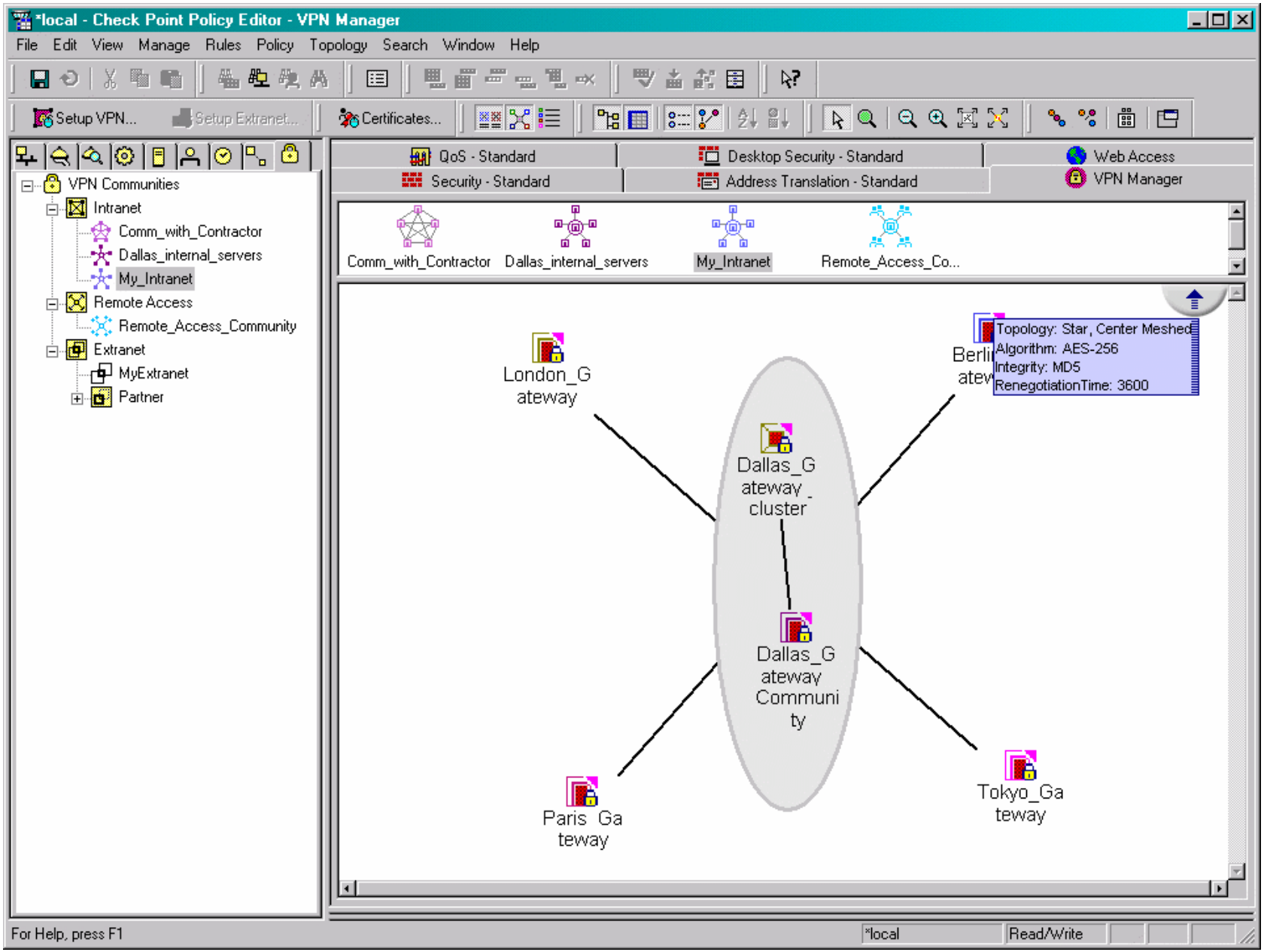
VPN

- IPSEC/IKE
  - Site à site (*gateway* ↔ *gateway*, *hosts* ↔ *hosts*)
  - Client à site (nomade, *host* ↔ *gateway*)
- SSH
- SSL (OpenVPN)
- Clients VPN « personnels » (authentification de l'utilisateur)
- Exemples de solutions commerciales

Ex. : CheckPoint VPN-1

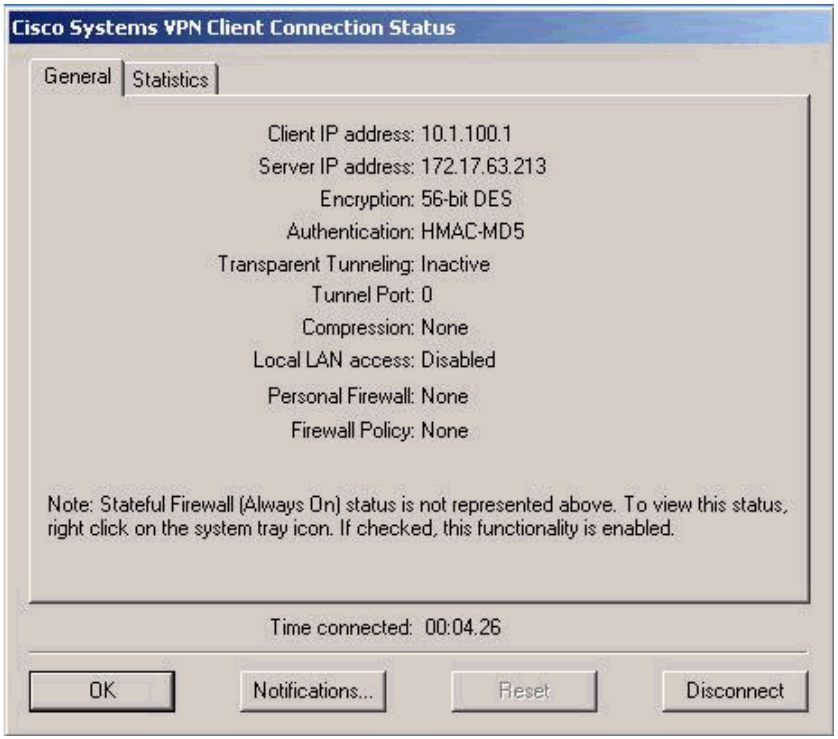


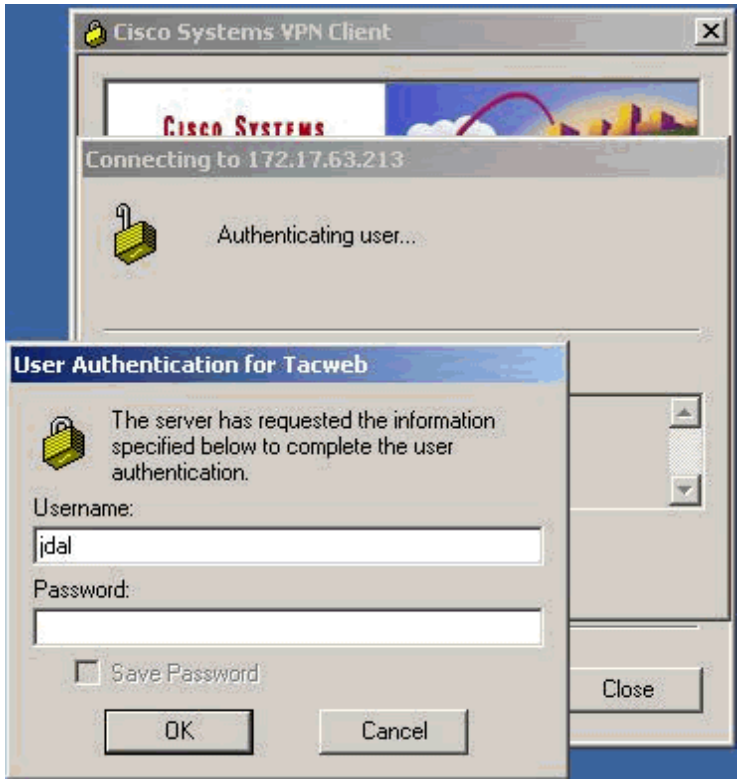
Ex. : CheckPoint VPN-1



IPSEC et X-AUTH

- Extension non-standard
- Sorte d'insertion d'une authentification de l'utilisateur par mot de passe (à la RADIUS) entre les deux phases IKE





SSL/TLS – IPSEC/IKE – HTTPS

- Utiliser des certificats plutôt que des mots de passe pour les tunnels VPN
- Générer si besoin ces certificats via `openssl` (réduire la gestion de clefs au minimum)
- X.509
- Ce genre d'action est toutefois préparatoire à la compréhension d'autres notions
  - Comment délivrer des certificats à tous les utilisateurs
  - Comment garantir un niveau de sécurité
  - Pour quoi faire : accès nomade, relevé de comptes bancaires, déclaration de revenu, et puis …