

3ème année

# Sécurité des Systèmes Informatiques

SUPAERO

Rodolphe Ortalo

RSSI - CARSAT Midi-Pyrénées

[rodolphe.ortalo@free.fr](mailto:rodolphe.ortalo@free.fr)

([rodolphe.ortalo@carsat-mp.fr](mailto: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

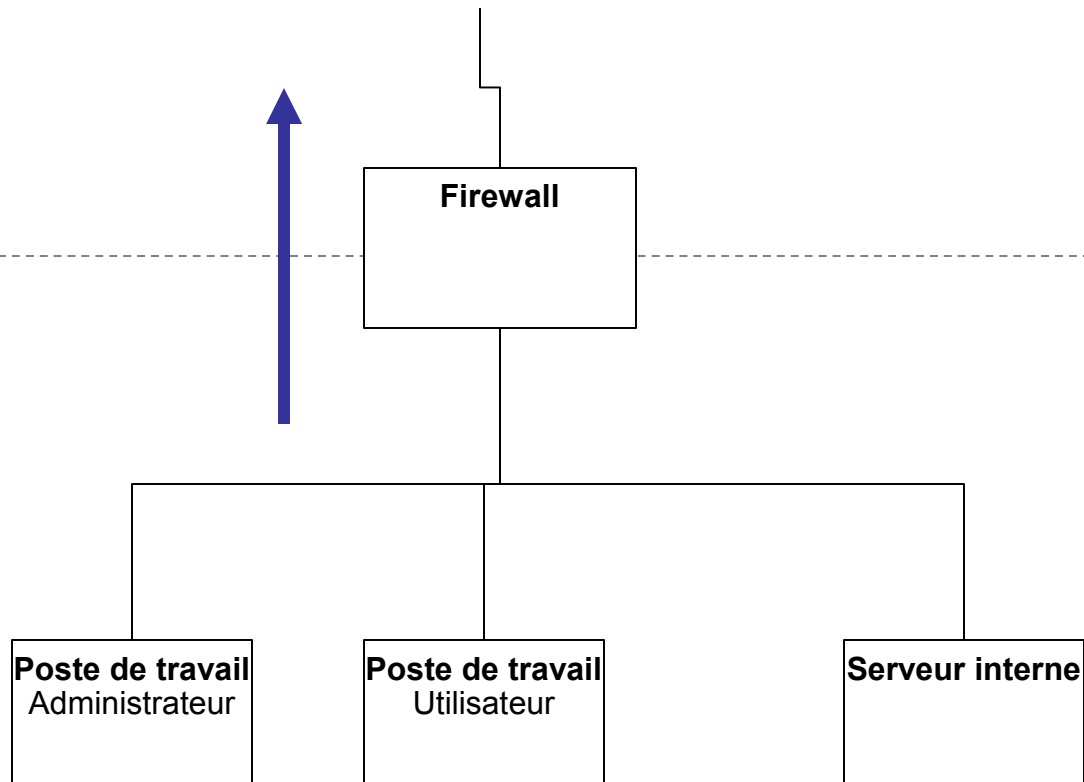
Cheswick and S.M. Bellovin, *Firewalls and Internet security*, AddisonWesley, 1994

# Diode

*Internet*

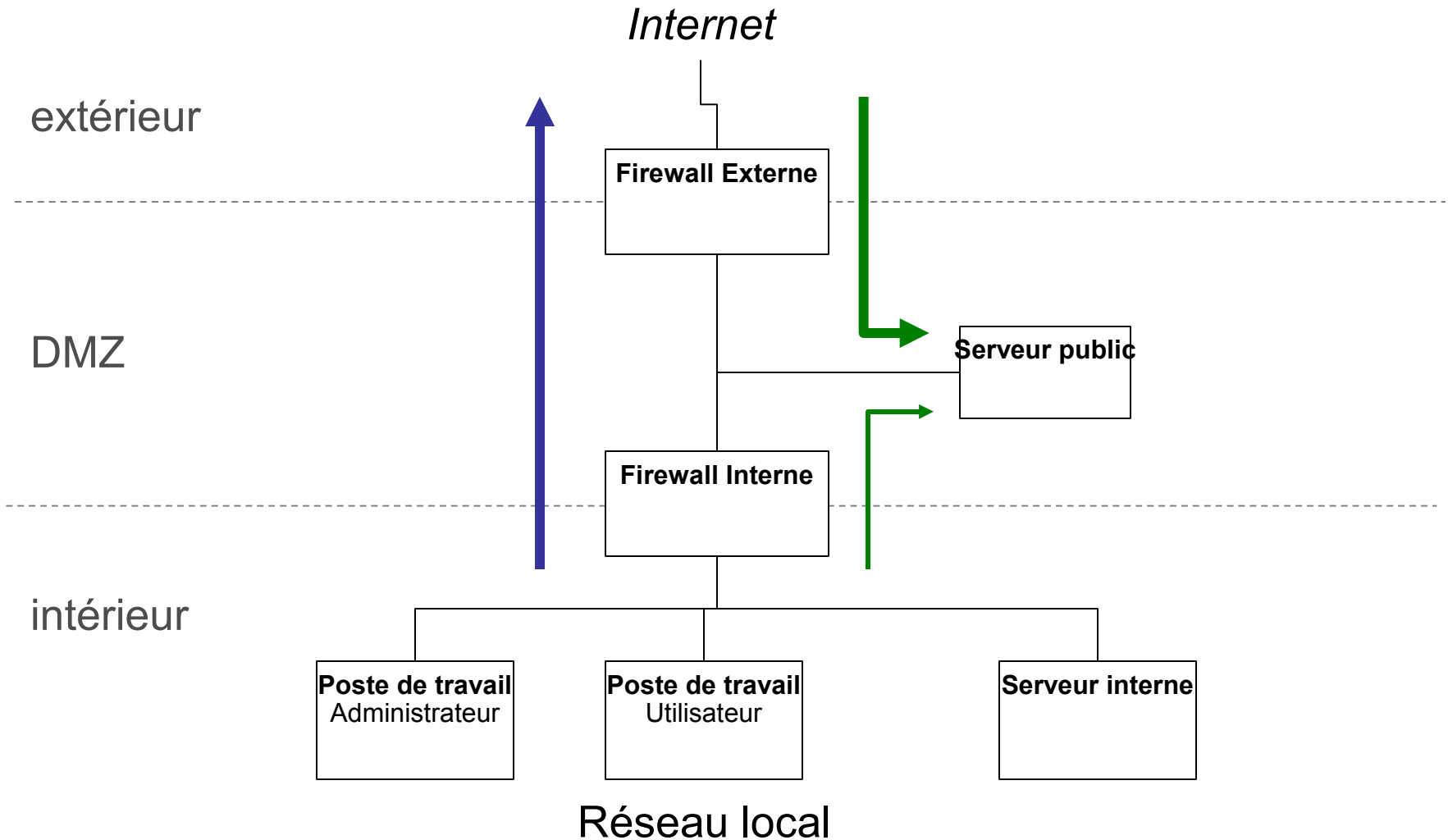
extérieur

intérieur



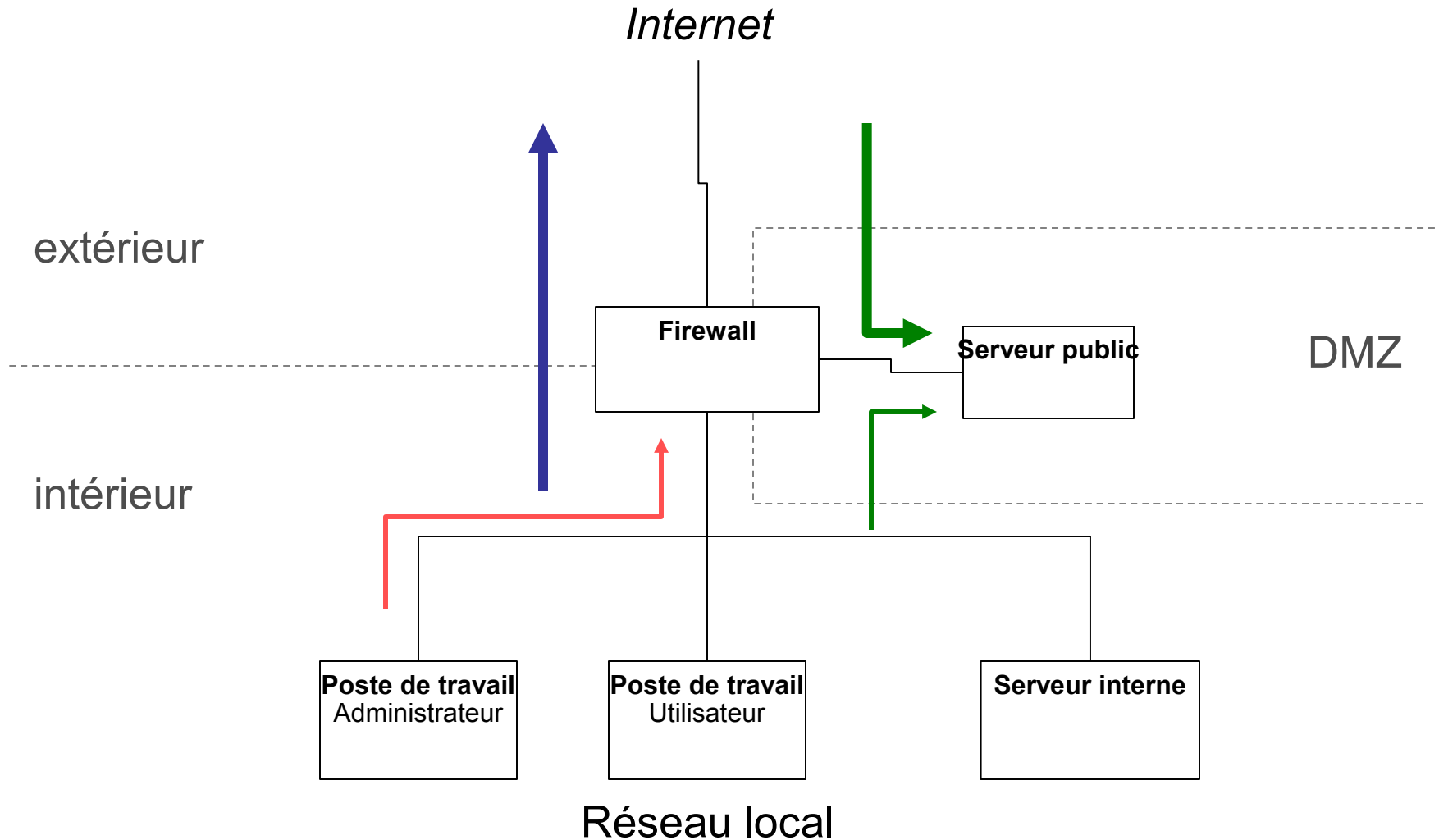
Réseau local

# « DMZ » - Version historique

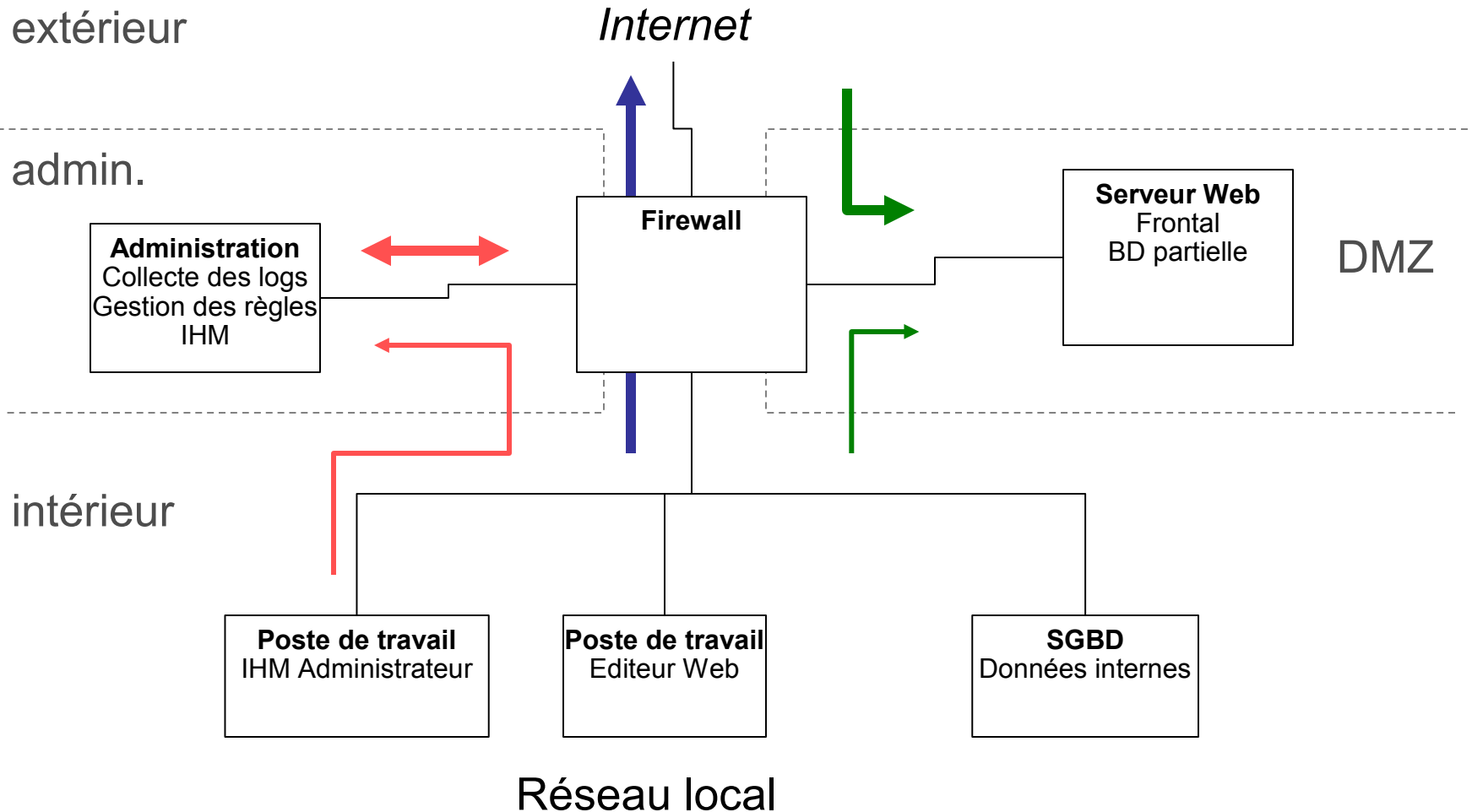




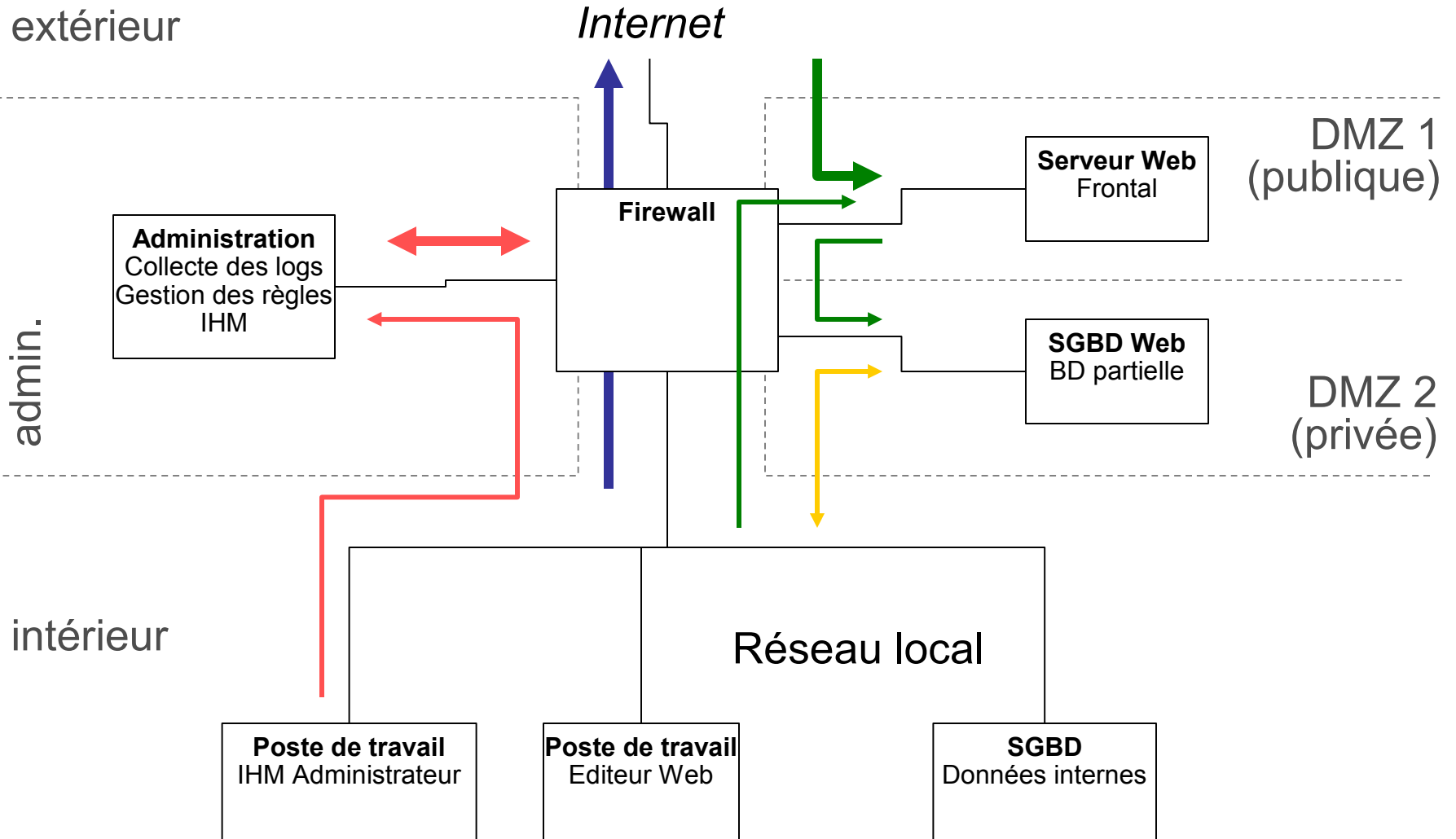
# « DMZ » - Situation actuelle



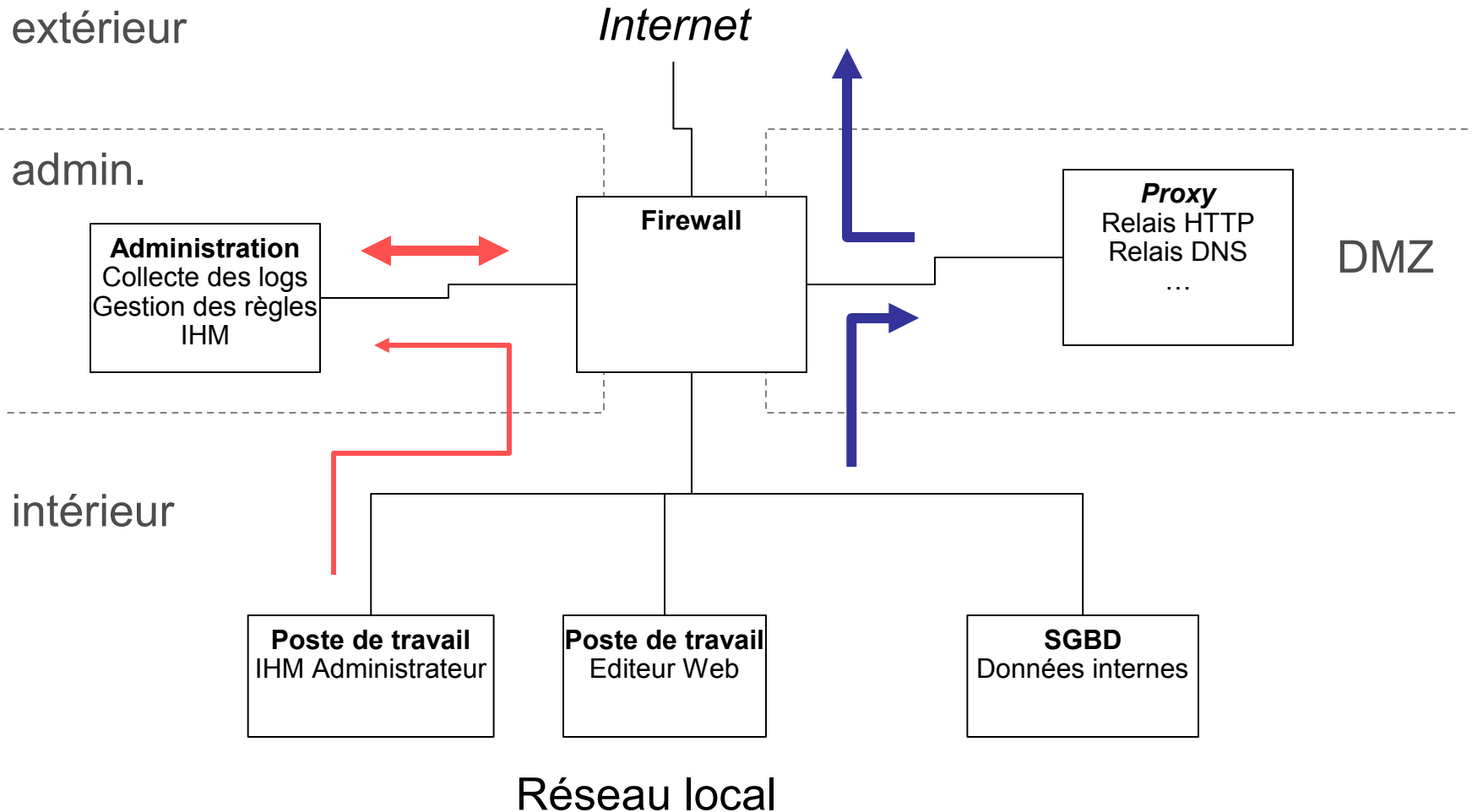
# Administration



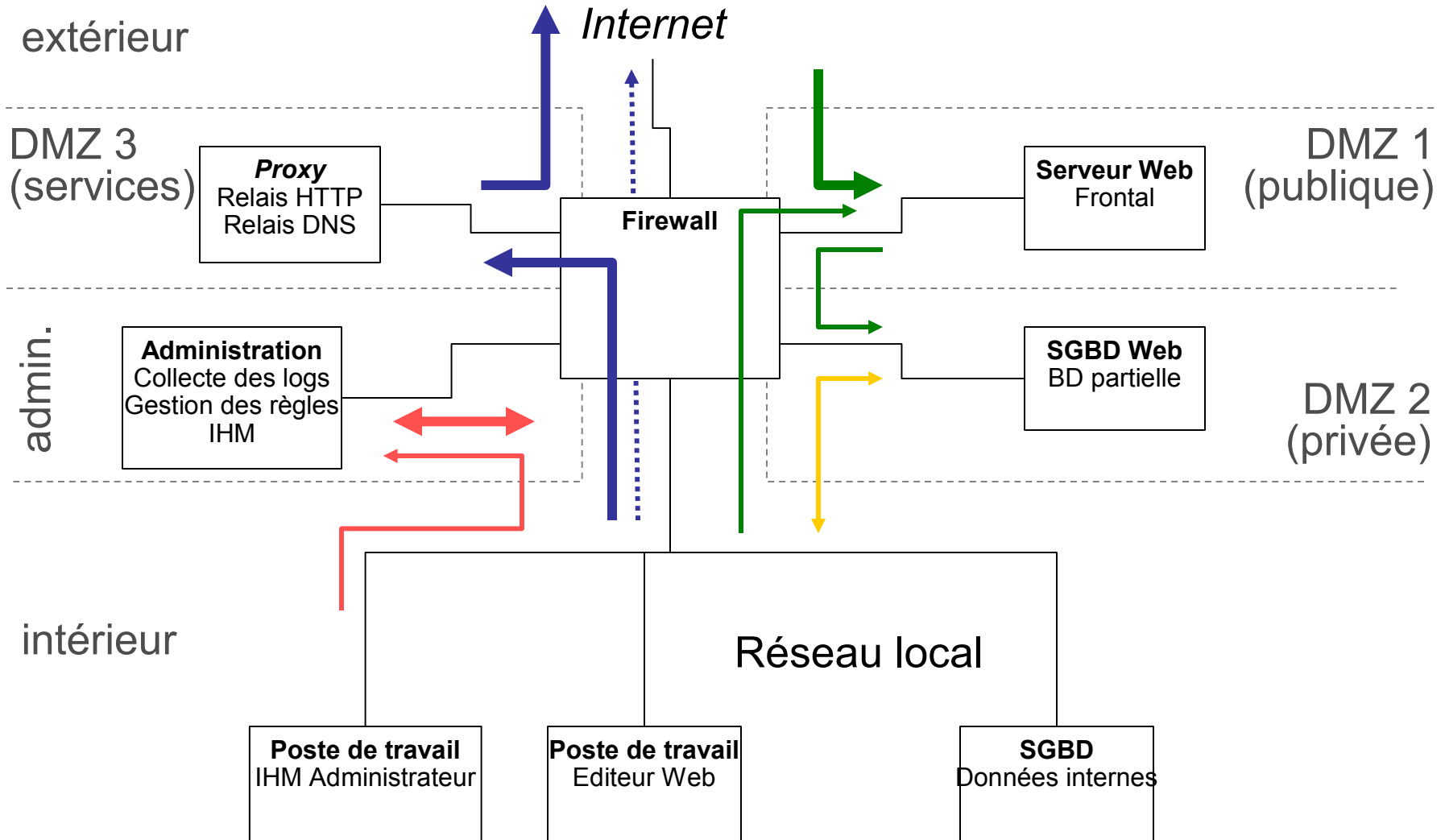
# « 2 DMZ » – 5 interfaces



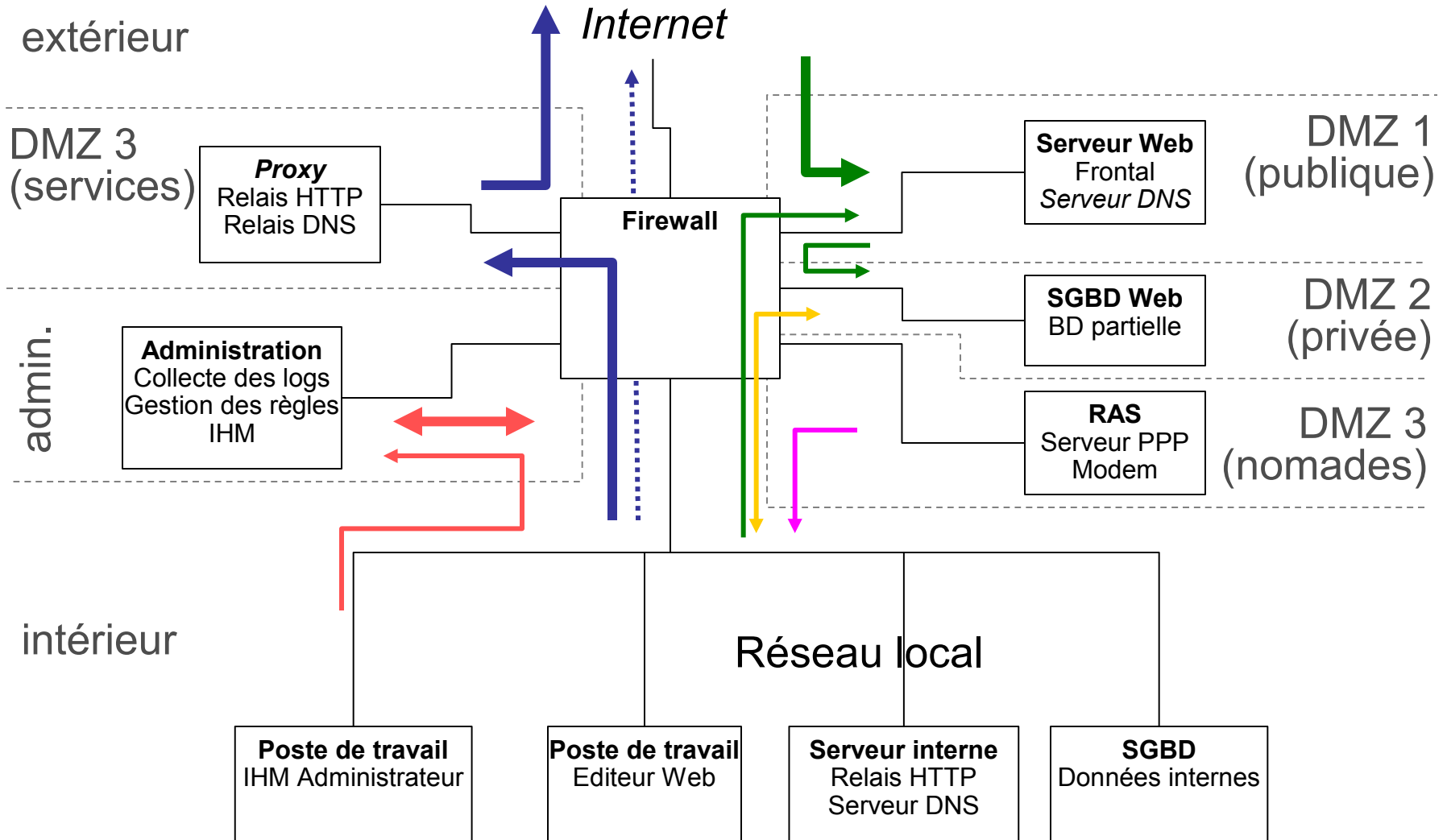
# Autre usage d'une DMZ



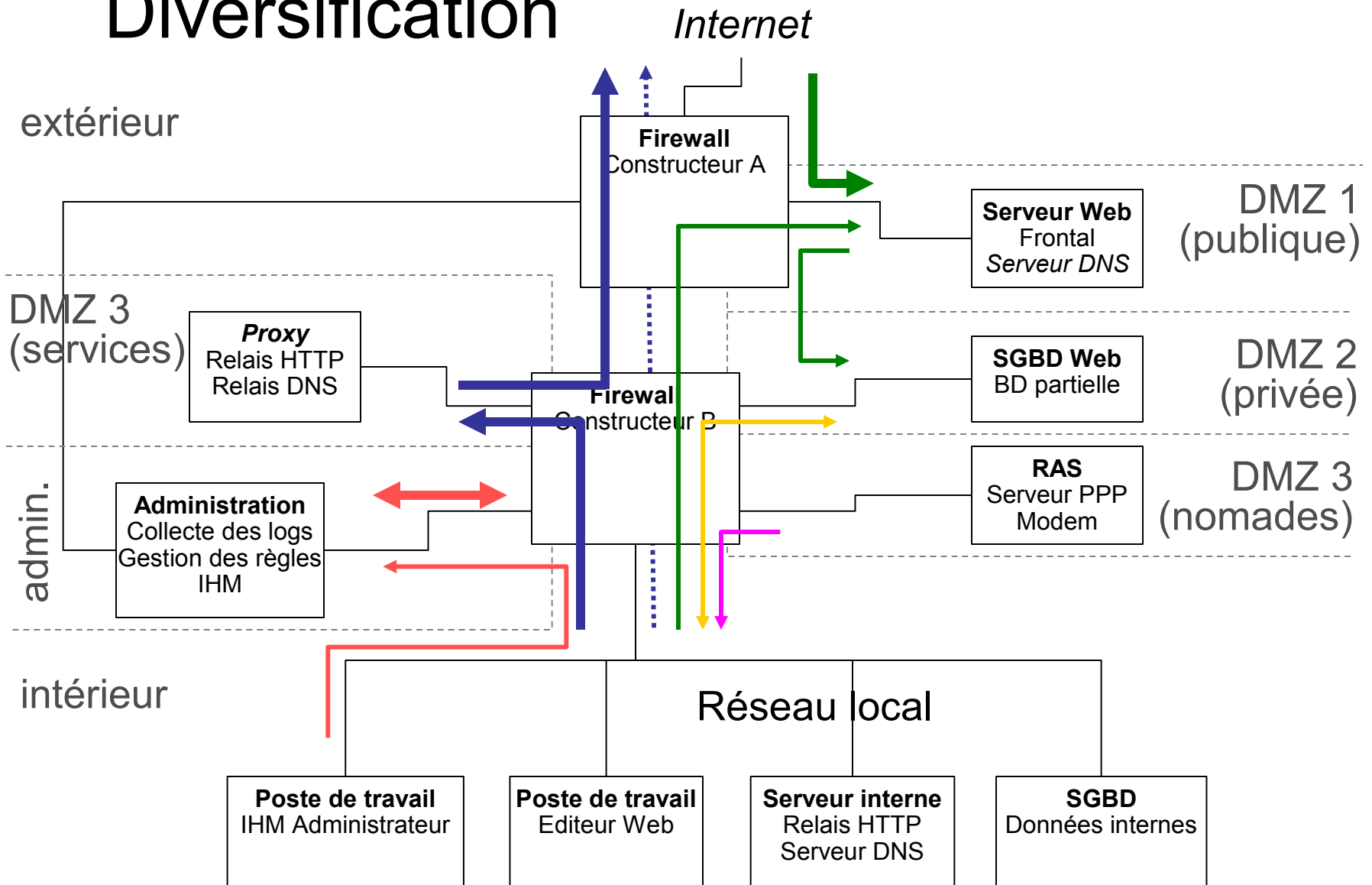
# « 3 DMZ » – 6 interfaces



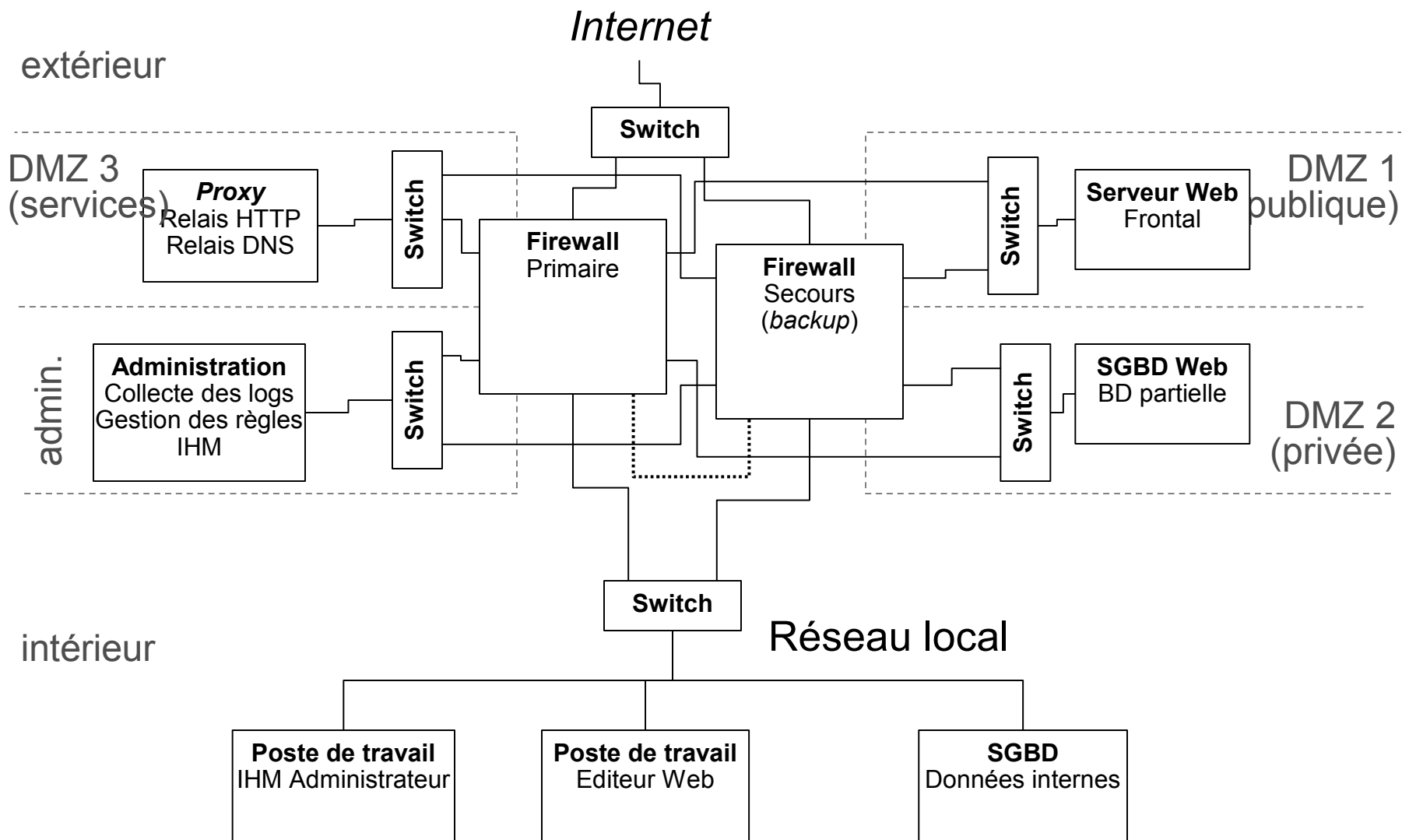
# 7 interfaces



# Diversification

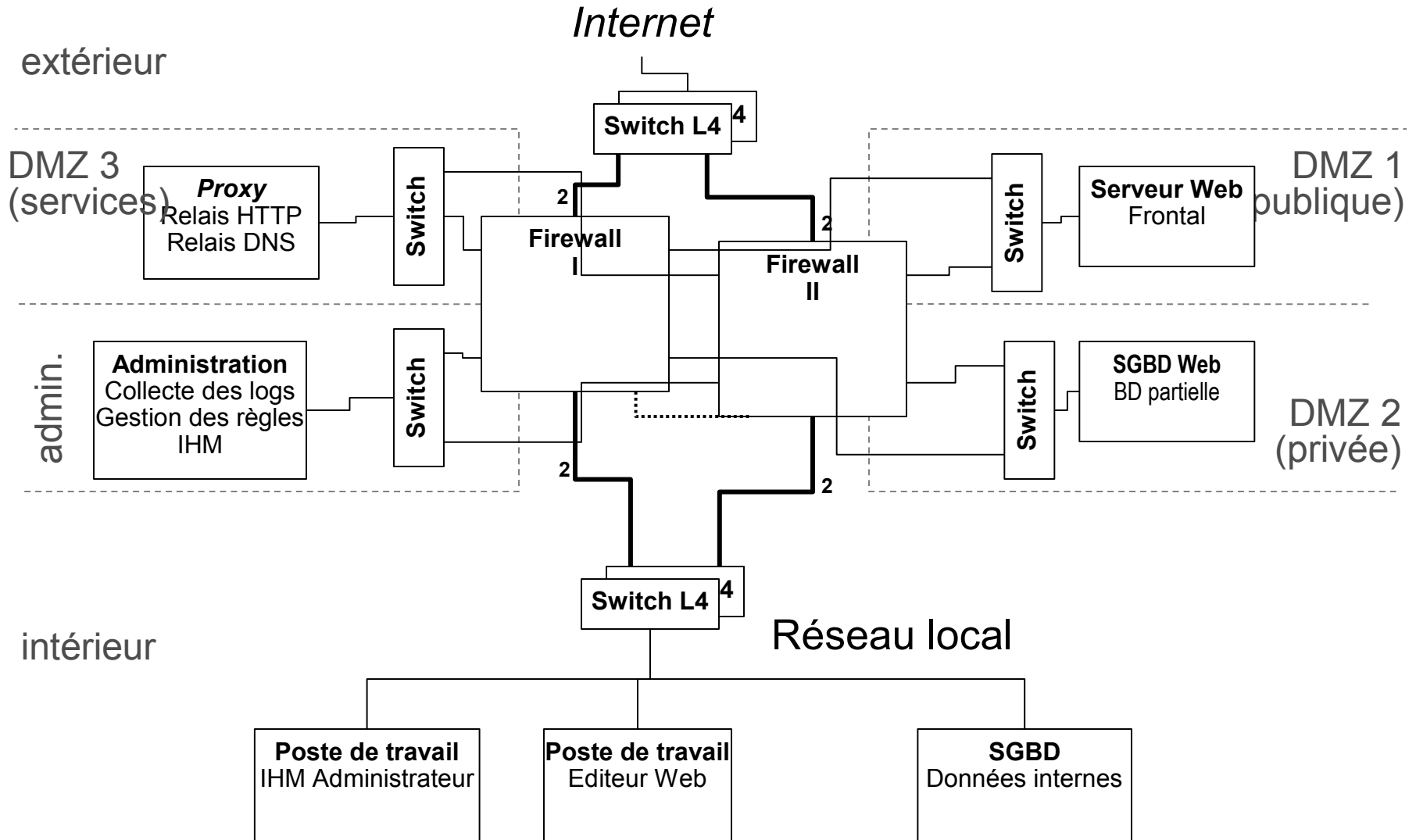


# Haute-disponibilité: *failover*





# 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.

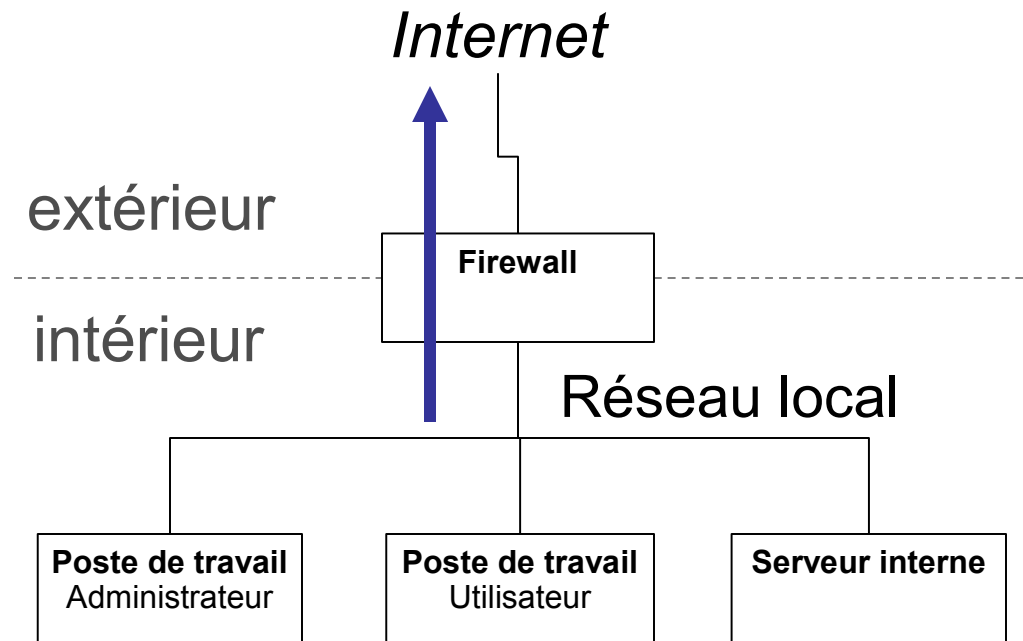
Mais est-ce souhaitable ?

# 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

**Cisco PIX Device Manager 3.0 - 10.2.2.252 (Beta Release)**

File Rules Search Options Tools Wizards Help

Home Configuration Monitoring Refresh Save Help

**Device Information**

Host Name : **pix2.ciscopix.com**  
PIX Version: **6.3(1)** PDM Version : **3.0(0)141**  
Device Type : **PIX 515E** Total Memory: **32 MB**  
License: **Restricted (R)** Total Flash: **16MB**

Licensed Features:

Encryption: **DES** Inside Hosts: **Unlimited**  
Failover: **Disabled** IKE Peers: **Unlimited**  
URL Filtering: **Enabled** Max Physical Interfaces: **3**

**Interface Status**

Interface	IP Address/Mask	Link	Current Kbps
inside	10.20.0.252/24	up	0
outside	10.2.2.252/16	up	16

Select an interface to view inside and outside Kbps

**VPN Status**

IKE Tunnels: **0** IPsec Tunnels: **0**

**System Resources Status**

**CPU**

CPU Usage (percent)

0%  
15:50:08

**Memory**

Memory Usage (MB)

16MB  
15:50:08

Memory (MB)  
Used: 15,681 Free: 16,319 Total: 32

**Traffic Status**

Connections Usage

0.5  
15:45:18 15:46:48 15:48:18 15:49:48

TCP: 0 UDP: 0 Total: 0

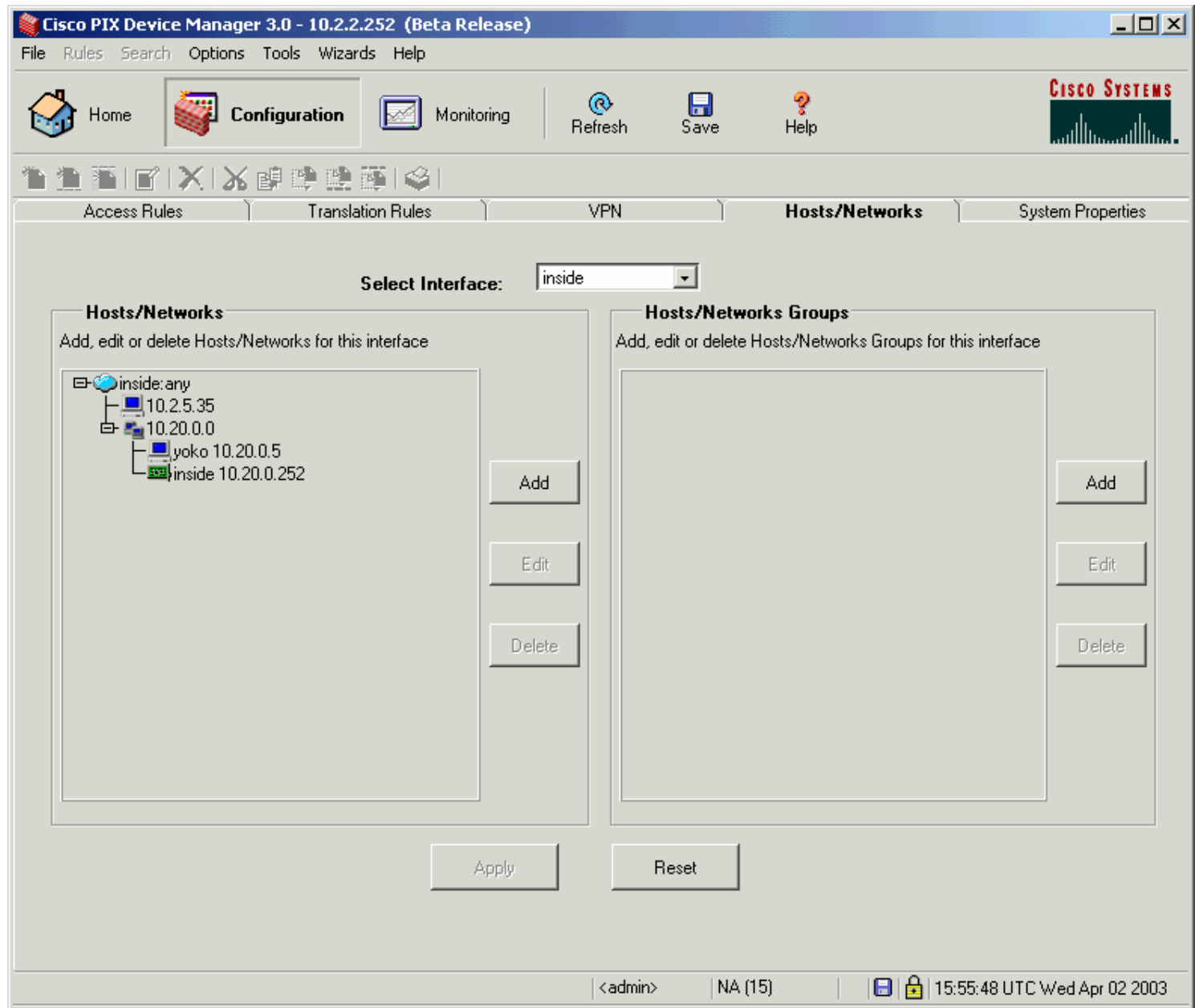
Outside Interface Traffic Usage (Kbps)

6144  
4096  
2048  
0  
15:45:18 15:46:48 15:48:18 15:49:48

Input Kbps: 0 Output Kbps: 16

<admin> | NA (15) | 15:50:08 UTC Wed Apr 02 2003

# Exemple : Cisco PIX



# Exemple : Cisco PIX

Use the Rules menu, the toolbar, or the right mouse button to add, edit or delete access, AAA or filter rules.

Access Rules  AAA Rules  Filter Rules Show Detail

#	Action	Source Host/Network	Destination Host/Network	Interface	Service	Log Level Interval	
-	✓	any	any	inside (outbound)	ip		Implicit o
1	✓	any	yoko/10.20.0.5	outside	service group:Flux_w	Informational 15 sec	
2	✓	any	any	outside	ip		

✓ Allow traffic    ✗ Deny traffic

Apply Reset Advanced...

< admin > | NA (15) | 15:52:28 UTC Wed Apr 02 2003



# Exemple : Cisco PIX

Cisco PIX Device Manager 3.0 - 10.2.2.252 (Beta Release)

File Rules Search Options Tools Wizards Help

Home Configuration Monitoring Refresh Save Help

Access Rules Translation Rules VPN Hosts/Networks System Properties

Categories

- Interfaces
- Failover
- [-] Routing
  - ◆ RIP
  - ◆ Static Route
  - ◆ Proxy ARPs
- [-] OSPF
- [-] DHCP Services
- [-] Administration
- [-] Logging
  - ◆ Logging Setup
  - ◆ PDM Logging
  - ◆ **Syslog**
  - ◆ Others
- [-] AAA
  - URL Filtering
  - Auto Update
- [-] Intrusion Detection
- [-] Advanced
- [-] Multicast
  - History Metrics

Syslog

Specify your syslog server(s) and logging parameters. Make sure logging is enabled in Logging>Logging Setup under the System Properties tab.

Syslog Servers

Interface	IP Address	Protocol/Port	EMBLEM
outside	10.2.5.45	UDP/514	No

Facility: LOCAL4(20)

Level: Debugging

Include Timestamp

Number of messages that are allowed to be queued when syslog server is busy (0 means unlimited):

512

Add Edit Delete

Apply Reset Advanced...

<admin> NA (15) 15:56:18 UTC Wed Apr 02 2003

# Exemple : Cisco PIX

The screenshot displays the Cisco PIX Device Manager interface. The title bar reads "Cisco PIX Device Manager 3.0 - 10.2.2.252 (Beta Release)". The menu bar includes "File", "Rules", "Search", "Options", "Tools", "Wizards", and "Help". The navigation bar shows "Home", "Configuration", and "Monitoring" (which is selected). There are also "Refresh", "Save", and "Help" buttons. The Cisco Systems logo is in the top right corner.

The main content area is divided into two sections. On the left is a "Categories" tree view with the following items:

- PDM Log
- **PDM/HTTPS Sessions**
- Telnet Sessions
- Secure Shell Sessions
- Authenticated Users
- User Licenses
- DHCP Client
- PPPoE Client
- VPN Connection Status
- [-] VPN Statistics
  - IKE SAs
  - IPSec VPNs
  - L2TP
  - PPTP
- [-] VPN Connection Graphs
  - IPSec Tunnels
  - L2TP/PPTP
- [-] System Graphs
  - Blocks
  - CPU
  - Failover
  - Memory
- [-] Connection Graphs
  - Xlates
  - Perfmon
- [-] Miscellaneous Graphs
  - IDS
- [-] Interface Graphs
  - inside
  - outside

On the right, the "PDM/HTTPS Sessions" section is active. It contains the text "Currently Connected PDM/HTTPS Sessions." and a table with the following data:

Session ID	IP Address
0	10.2.5.45
1	10.2.4.39

Below the table are two buttons: "Refresh" and "Disconnect".

The status bar at the bottom shows "<admin> | NA (15) | 15:54:58 UTC Wed Apr 02 2003".

# 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 gtp_default	accept	None	* Policy Targets	* Any	
2	Roaming_P_1	North_GGSN_1 North_GGSN_2 South_GGSN	GTP gtp_default	accept	Log	* Policy Targets	* Any	
3	Roaming_P_2	South_GGSN	GTP gtp_citibank	accept	Log	* Policy Targets	* Any	
4	Roaming_P_2 Roaming_P_3	North_GGSN_1	GTP 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

# 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 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 Intern
6	Remote_VPN_Dc Net_Behind_Dyr	Local_Intranet_S	http	Encrypt	Log	* Policy Targets	* Any	Allow encrypted access to the lo 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

50.128.147.1 - Check Point SmartDashboard - R16\_V3.08

File Edit View Manage Rules Policy SmartMap SmartWorkflow Search Window Help

Firewall NAT IPS Anti-Spam & Mail Anti-Virus & URL Filtering SSL VPN IPsec VPN QoS Desktop

Network Objects

- Check Point
- Nodes
- Networks
- Groups
- Address Ranges
- Dynamic Objects
- Security Zone Objects

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON
<b>Flux à dropper (Rules 1-3)</b>								
<b>Administration Pare-Feu (Rules 4-10)</b>								
<b>Administration des équipements réseaux (Rules 11-13)</b>								
<b>Résolution de Noms DNS (Rules 14-15)</b>								
14	R-0001-DNS*	S-Win-AD S-Aix-CFT	D-N18-DNS D-N-AD D-R-AD	* Any Traffic	UDP domain-udp TCP domain-tcp	accept	Log	* Policy Targets
15	R-0002-DNS*	D-N18-DNS D-N-AD NET-Agences_tinerants D-R-AD S-BC R-FW D-N-Spv_AD	S-Win-AD S-Aix-CFT	* Any Traffic	UDP domain-udp TCP domain-tcp	accept	Log	* Policy Targets
<b>Flux NTP (Rules 16-18)</b>								
16	R-0004-NTP	S-Win-AD	D-N-AD_Racine	* Any Traffic	UDP ntp-udp	accept	Log	* Policy Targets
17	R-0100-NTP	S-BC	D-N18-NTP_nonAD	* Any Traffic	UDP ntp-udp	accept	Log	* Policy Targets
18	R-0005-NTP	NET-Agences_tinerants R-FW R-Switch	S-Win-AD	* Any Traffic	UDP ntp-udp	accept	Log	* Policy Targets
<b>Flux Active Directory (AD) (Rules 19-28)</b>								
19	R-0006-AD	D-N-AD NET-Agences_tinerants D-R-AD D-N-Spv_AD	S-Win-AD	* Any Traffic	Flux_AD	accept	Log	* Policy Targets
20	R-0007-AD*	S-Win-AD	D-N-AD D-R-AD NET-Agences_tinerants	* Any Traffic	Flux_AD UDP dhcp-rep-localmd UDP bootp	accept	Log	* Policy Targets

For Help, press F1

50.128.147.1 Read/Write NUM

# Ex. : CheckPoint Firewall-1

The screenshot displays the Check Point SmartDashboard interface for Firewall rule configuration. The left sidebar shows a tree view of Network Objects, including Check Point, Nodes, Networks, Groups, Address Ranges, Dynamic Objects, and Security Zone Objects. The main area shows a table of firewall rules with the following columns: NO., NAME, SOURCE, DESTINATION, VPN, SERVICE, ACTION, TRACK, and INSTALL ON.

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON
20	R-0007-AD*	S-Win-AD	D-R-AD NET-Agences_itinerants	* Any Traffic	udp dhcp-rep-localm udp bootp	accept	Log	* Policy Targets
21	R-0060-AD	D-R10-Proxy	S-Win-Heb	* Any Traffic	TCP HTTP-9180	accept	Log	* Policy Targets
22	R-0104-RDP	D-N-AD_Racine	S-Win-AD	* Any Traffic	TCP RDP-3389	accept	Log	* Policy Targets
23	R-0115-ADMOCS	R16-WSUS-TSPWIN013	D-N-AD_Racine	* Any Traffic	Flux_AD	accept	Log	* Policy Targets
24	R-0069-WEBAUTH	NET-Region	D-N-AD_Racine D-N01-AD D-R12-AD D-N04-AD D-N03-AD D-N18-AD D-N06-AD	* Any Traffic	TCP ldap UDP-LDAP-389 TCP Kerberos_v5_TC UDP Kerberos_v5_UD	accept	Log	* Policy Targets
25	R-0109-AUTH	D-N18-PKI_Racine D-N18-Mocs D-N18-TSLIC D-N18-SHPT	S-Win-AD	* Any Traffic	TCP ldap TCP Kerberos_v5_TC UDP Kerberos_v5_UD UDP-LDAP-389	accept	Log	* Policy Targets
26	R-0107-VPNSSL	D-N18-PKI_Racine	S-Win-AD	* Any Traffic	TCP RPC-135 TCP Ntfs-5001 TCP RPC-Dyn-49152-!	accept	Log	* Policy Targets
27	R-0129-Adm	D-N-Adm	S-Win-AD	* Any Traffic	LDAP UDP-LDAP-389 TCP Kerberos_v5_TC UDP Kerberos_v5_UD TCP microsoft-ds TCP nbssession	accept	Log	* Policy Targets
28	R-0140-RMAD_NAT IONAL	D-N-AD_Racine	S-Win-AD	* Any Traffic	TCP RMAD-3843	accept	Log	* Policy Targets



# Ex. : CheckPoint Firewall-1

No.	Date	Time	Origin	Service	Source	Destination	Rule	Curr. Rule	Rule Na...
1	28Jan2013	23:59:00	TFPS001						
2	28Jan2013	23:59:00	TFPS001	UDP domain-udp	50.135.5.18	R16-AD-TSPW004	15	15-R16_V3.08	R-0002-DNS'
3	28Jan2013	23:59:00	TFPS001	UDP domain-udp	50.135.5.18	R16-AD-TSPW004	15	15-R16_V3.08	R-0002-DNS'
4	28Jan2013	23:59:00	TFPS001	TCP ldap	50.135.4.14	R16-AD-TSPW004	19	19-R16_V3.08	R-0006-AD
5	28Jan2013	23:59:00	TFPS001	TCP ldap	50.135.10.20	R16-AD-TSPW004	19	19-R16_V3.08	R-0006-AD
6	28Jan2013	23:59:00	TFPS001	TCP microsoft-ds	50.135.5.18	R16-FIC-SRVFIC2	53	53-R16_V3.08	R-0053-FIC
7	28Jan2013	23:59:00	TFPS001	TCP ldap	50.135.26.10	R16-AD-TSPW004	19	19-R16_V3.08	R-0006-AD
8	28Jan2013	23:59:00	TFPS001	TCP ldap	50.135.4.18	R16-AD-TSPW004	19	19-R16_V3.08	R-0006-AD
9	28Jan2013	23:59:00	TFPS001	UDP domain-udp	R16-AD-TSPW004	N18-ADR-QAVPW...	14	14-R16_V3.08	R-0001-DNS'
10	28Jan2013	23:59:00	TFPS001	TCP SCOM-5723	R16-AD-TSTWIN001	N10-SCOM-RMS-...	82	82-R16_V3.08	R-0125-SC...
11	28Jan2013	23:59:00	TFPS001	TCP HTTP-8080	R16-Proxy-TSPK001	50.145.48.52	68	68-R16_V3.08	R-0042-SURF
12	28Jan2013	23:59:00	TFPS001	UDP domain-udp	50.135.101.18	R16-AD-TSPW004	15	15-R16_V3.08	R-0002-DNS'
13	28Jan2013	23:59:00	TFPS001	TCP ldap	50.135.101.18	R16-AD-TSPW004	19	19-R16_V3.08	R-0006-AD
14	28Jan2013	23:59:00	TFPS001	TCP ldap	50.135.24.21	R16-AD-TSPW004	19	19-R16_V3.08	R-0006-AD
15	28Jan2013	23:59:01	TFPS001	UDP ntp-udp	50.135.13.11	R16-AD-TVPW012	18	18-R16_V3.08	R-0005-NTP
16	28Jan2013	23:59:01	TFPS001	UDP domain-udp	R16-AD-TSPW004	N18-ADR-QASPW...	14	14-R16_V3.08	R-0001-DNS'
17	28Jan2013	23:59:01	TFPS001	UDP domain-udp	R16-Proxy-TSPK001	R16-AD-TVPW012	15	15-R16_V3.08	R-0002-DNS'
18	28Jan2013	23:59:01	TFPS001	UDP domain-udp	N18-ADR-QASPW...	R16-CFT-TSPWIN0...	235	235-R16_V3.08	R-9999-DFT
19	28Jan2013	23:59:01	TFPS001	TCP ldap	50.135.14.30	R16-AD-TSPW004	19	19-R16_V3.08	R-0006-AD
20	28Jan2013	23:59:01	TFPS001	TCP HTTP-8080	R16-Proxy-TSPK001	50.144.100.41	68	68-R16_V3.08	R-0042-SURF
21	28Jan2013	23:59:02	TFPS001	UDP domain-udp	50.135.1.22	R16-AD-TSPW004	15	15-R16_V3.08	R-0002-DNS'
22	28Jan2013	23:59:02	TFPS001	TCP ldap	50.135.1.22	R16-AD-TSPW004	19	19-R16_V3.08	R-0006-AD
23	28Jan2013	23:59:02	TFPS001	UDP domain-udp	50.135.10.12	R16-AD-TSPW004	15	15-R16_V3.08	R-0002-DNS'
24	28Jan2013	23:59:02	TFPS001	UDP domain-udp	50.135.10.12	R16-AD-TSPW004	15	15-R16_V3.08	R-0002-DNS'
25	28Jan2013	23:59:02	TFPS001	TCP microsoft-ds	50.135.10.12	R16-AD-TSPW004	19	19-R16_V3.08	R-0006-AD
26	28Jan2013	23:59:02	VPN-1 Power/UTM	UDP domain-udp	N18-DNS-AKPY230	R16-Citrix-TSPTSE23	235	235-R16_V3.08	R-9999-DFT
27	28Jan2013	23:59:02	TFPS001	UDP ntp-udp	50.135.24.4	R16-AD-TSTWIN001	18	18-R16_V3.08	R-0005-NTP
28	28Jan2013	23:59:02	TFPS001	TCP ldap	50.135.24.11	R16-AD-TSPW004	19	19-R16_V3.08	R-0006-AD
29	28Jan2013	23:59:02	TFPS001	UDP domain-udp	N18-DNS-AKPY230	R16-CFT-TSPWIN0...	235	235-R16_V3.08	R-9999-DFT
30	28Jan2013	23:59:02	TFPS001	UDP sip	50.128.159.220	50.146.100.104	182	182-R16_V3.08	
31	28Jan2013	23:59:02	TFPS001	TCP RAW-9100	R16-CRF-WINM9	50.135.200.121	235	235-R16_V3.08	R-9999-DFT
32	28Jan2013	23:59:03	TFPS001	TCP ldap	50.135.3.13	R16-AD-TSPW004	19	19-R16_V3.08	R-0006-AD
33	28Jan2013	23:59:03	TFPS001	TCP ldap	50.135.11.14	R16-AD-TSPW004	19	19-R16_V3.08	R-0006-AD
34	28Jan2013	23:59:03	TFPS001	TCP ldap	50.135.3.20	R16-AD-TSPW004	19	19-R16_V3.08	R-0006-AD
35	28Jan2013	23:59:03	TFPS001	TCP HTTP-8080	R16-Proxy-TSPK001	50.144.100.41	68	68-R16_V3.08	R-0042-SURF
36	28Jan2013	23:59:03	TFPS001	TCP ldap	50.135.8.10	R16-AD-TSPW004	19	19-R16_V3.08	R-0006-AD
37	28Jan2013	23:59:03	TFPS001	UDP domain-udp	50.135.10.18	R16-AD-TSPW004	15	15-R16_V3.08	R-0002-DNS'
38	28Jan2013	23:59:03	TFPS001	UDP domain-udp	50.135.10.18	R16-AD-TSPW004	15	15-R16_V3.08	R-0002-DNS'
39	28Jan2013	23:59:03	TFPS001	TCP ldap	50.135.110.10	R16-AD-TSPW004	19	19-R16_V3.08	R-0006-AD
40	28Jan2013	23:59:03	TFPS001	TCP microsoft-ds	50.135.10.18	R16-AD-TSPW004	19	19-R16_V3.08	R-0006-AD

# 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<sub>eth1</sub> 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 (020405B40101040201030300)
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 (020405B40101040201030300)
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 (020405B40101040201030300)

```

- 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 (020405B40101040201030300)
```

```
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 (020405B40101040201030300)
```

- 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
```

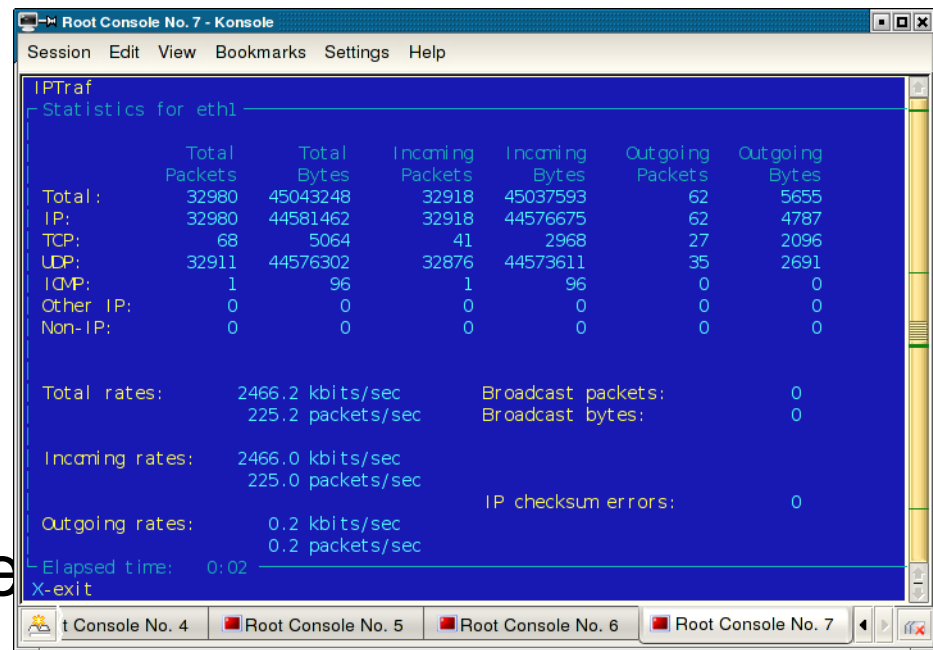
- On autorise l'UDP sortant vers la plage 32000-33999

- « 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*
  - **Systemes 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:  $\{\text{aléa}\}_{K_u}$  réponse:  $\{\text{aléa}+1\}_{K_u}$
- Mots de passe jetables
- Systèmes cartes à puce (clé symétrique)
  - $K_{\text{fille}} = \{\text{id}\}_{K_{\text{mère}}}$
- 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

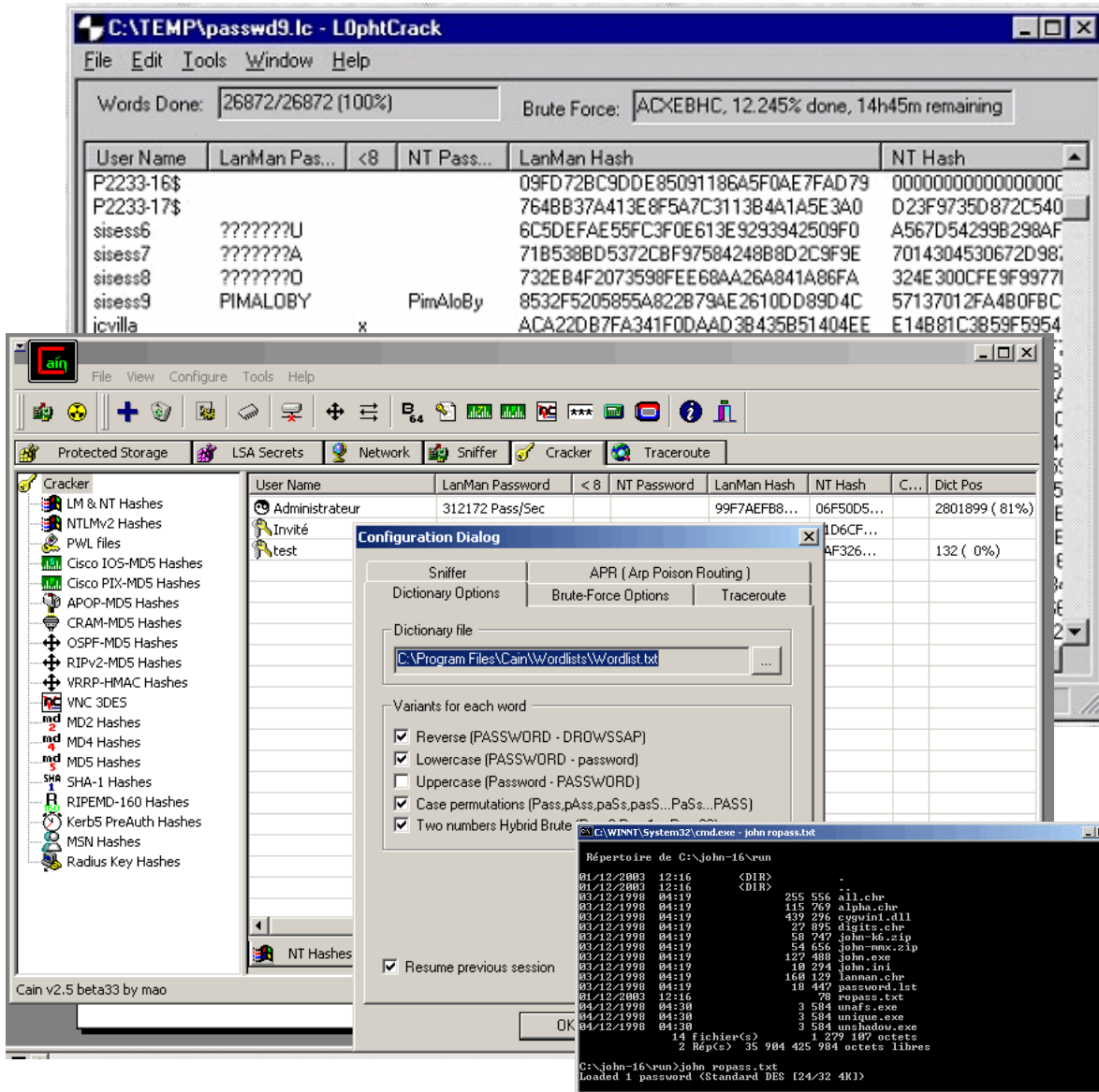
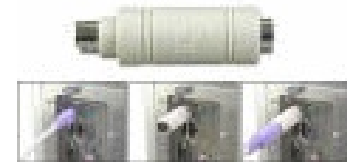
- **Personnel**  
spécifique à chaque individu
- **Fiable**  
durablement mémorisé
- **Résistant**  
qui ne soit pas facile à deviner pour un tiers



# 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 accessible 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



Words Done: 26872/26872 (100%) Brute Force: ADXEBHC, 12.245% done, 14h45m remaining

User Name	LanMan Pas...	<8	NT Pass...	LanMan Hash	NT Hash
P2233-16\$				09FD72BC9DDE85091186A5F0AE7FAD79	0000000000000000
P2233-17\$				7648B37A413E8F5A7C311384A1A5E3A0	D23F9735D872C540
sisess6	????????U			6C5DEFAE55FC3F0E613E9293942509F0	A567D54299B298AF
sisess7	????????A			71B538BD5372CBF975842488BD2C9F9E	7014304530672D98;
sisess8	????????D			732EB4F2073598FEE68AA26A841A86FA	324E300CFE9F9977I
sisess9	PIMALOBY		PimAloBy	8532F5205855A822B79AE2610D89D4C	57137012FA480FBC
icvilla		x		ACA22DB7FA341F0DAAD38435851404EE	E14881C3859F5954

Configuration Dialog: Sniffer: APR (Arp Poison Routing), Dictionary file: C:\Program Files\Cain\Wordlists\Wordlist.txt, Variants for each word: Reverse, Lowercase, Uppercase, Case permutations, Two numbers Hybrid Brute.

```
C:\WINNT\System32\cmd.exe - john ropass.txt
Répertoire de C:\john-16\run
01/12/2003 12:16 <DIR> .
01/12/2003 12:16 <DIR> ..
03/12/1998 04:19 255 556 all_chr
03/12/1998 04:19 115 769 alpha_chr
03/12/1998 04:19 439 296 cuguni_dll
03/12/1998 04:19 27 895 digits_chr
03/12/1998 04:19 58 747 john-k6.zip
03/12/1998 04:19 54 656 john-mex.zip
03/12/1998 04:19 127 488 john.exe
03/12/1998 04:19 10 294 john.in1
03/12/1998 04:19 168 129 lanman_chr
03/12/1998 04:19 10 447 password.let
01/12/2003 12:16 78 ropass.txt
04/12/1998 04:30 3 584 unafs.exe
04/12/1998 04:30 3 584 unique.exe
04/12/1998 04:30 3 584 unshadow.exe
14 fichier(s) 1 279 107 octets
2 Rép(s) 35 904 425 984 octets libres

C:\john-16\run>john ropass.txt
Loaded 1 password (Standard DES [24/32 4K])
```

$> 10^6 \text{ pass}_{\text{NT}} / \text{s}$

<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)

*e o n p e t e l q*



*être ou ne pas être, telle est la question*

*u u p c r l e p e p  
t n h i e o t e t e  
Sll(p,d,d)*

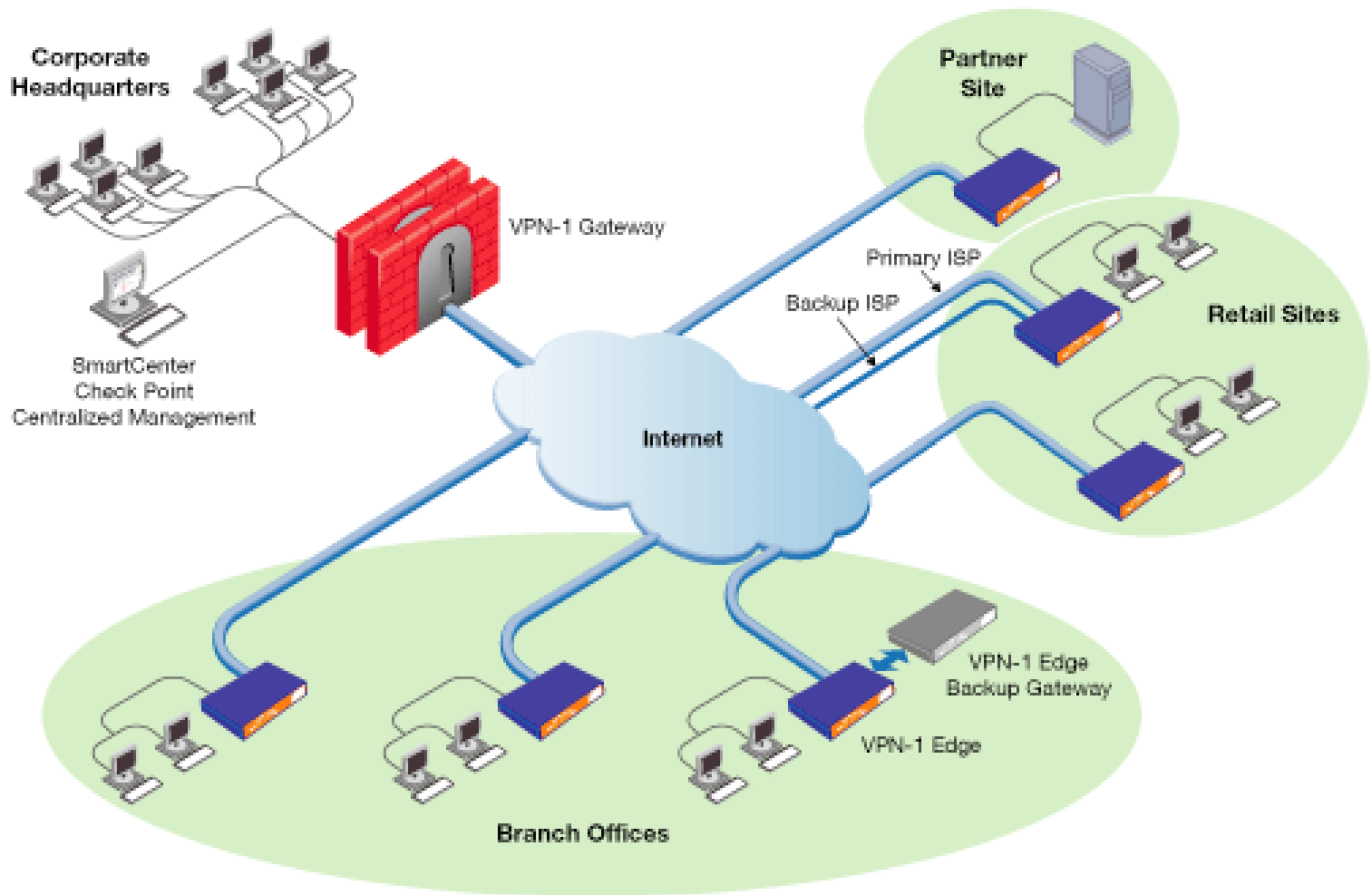
# Plan (2/2)

- 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

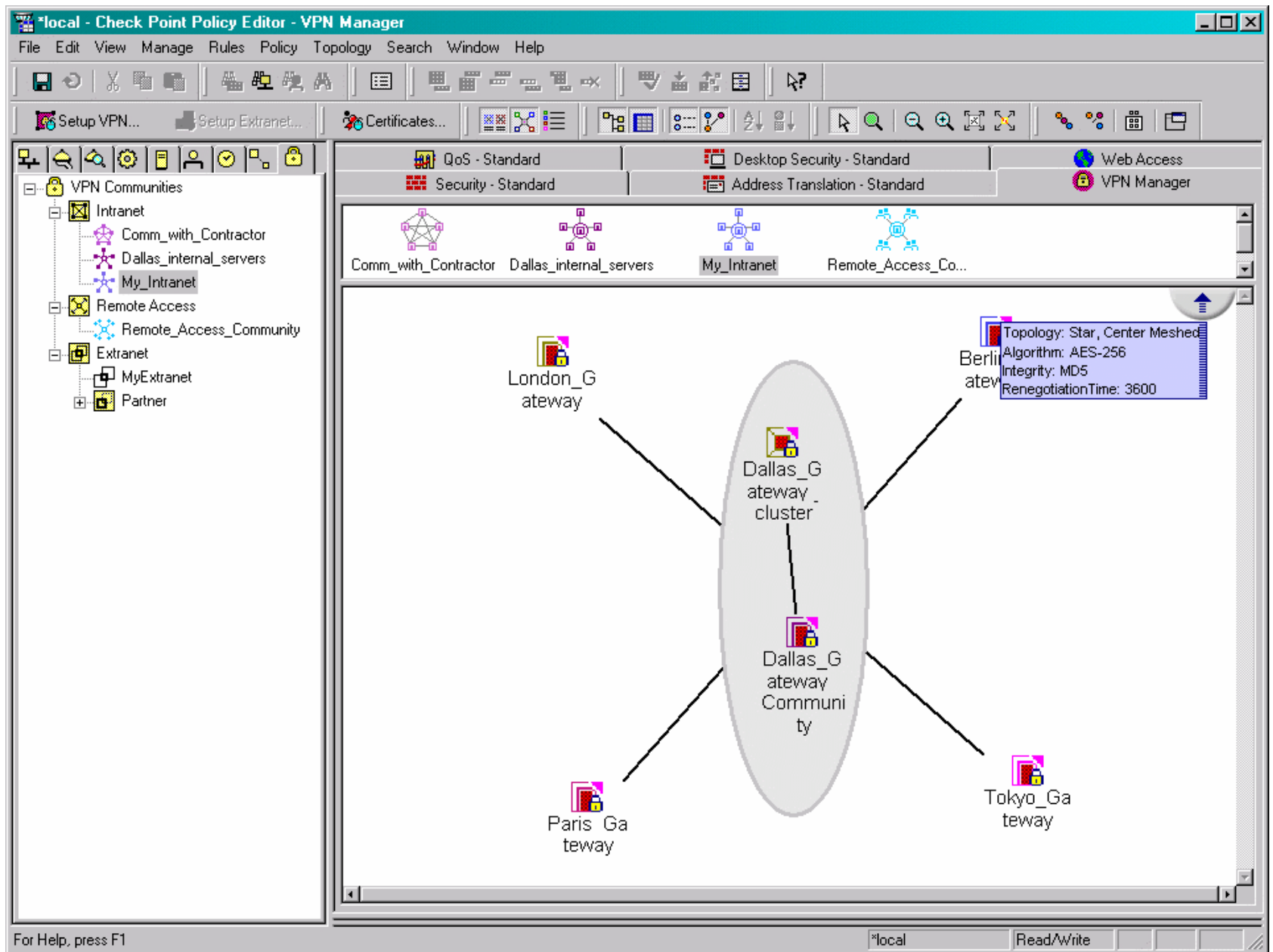
# VPN

- 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

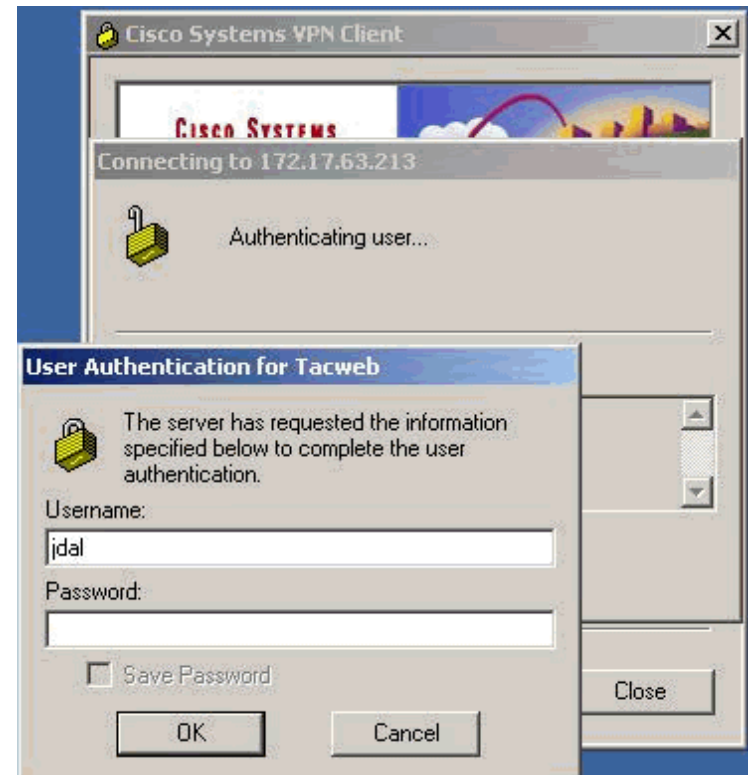
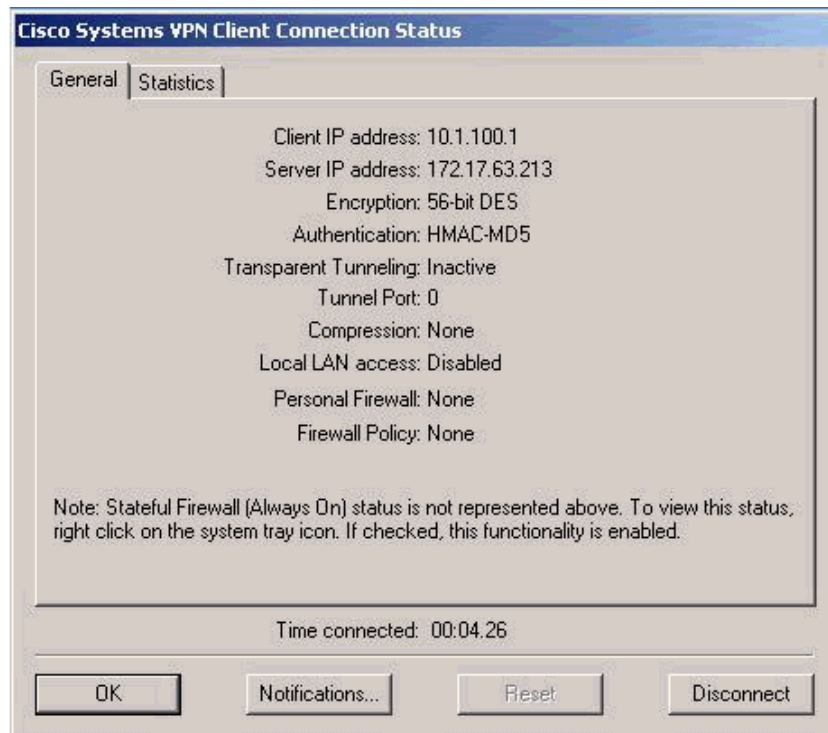


# Ex. : CheckPoint VPN-1



# 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 ...