



Firewall et VPN

Alain Corpel


Enseignant-Chercheur en SSI
alain.corpel@utt.fr

Plan (1/2)



- Introduction
- Définition et objectif d'un pare-feu
- Exemple d'architecture
- Politique de Vlan
- Politique et règles d'un pare-feu
- Exemples de règles
- Différents types de filtrage
- Protocoles à surveiller
- Ce que protège un pare-feu
- Limites d'un pare-feu
- Les 7 péchés capitaux
- Pare-feu vs Routeur
- Exemple de logs
- Protection des applications Web

Plan (2/2)

- 
- Cas du WAF
 - Cas du pare-feu personnel
 - Définition et objectif d'un VPN
 - Architecture d'un VPN
 - Différents types de protocoles
 - Ce que protège un VPN
 - Exemple de logs
 - Cas du VPN SSL
 - Conclusion



Introduction

- Les outils de sécurité les plus connus et qui ont été les premiers à être déployés au niveau des systèmes d'informations sont les antivirus. Juste après sont venus les outils permettant de se protéger des attaques extérieures, c'est à dire les pare-feux encore appelés garde-barrières ou firewalls. Ils sont apparus, il y a environ une vingtaine d'années.
- Les pare-feux sont apparus lorsque les réseaux ont commencé à se multiplier et s'interconnecter. La nécessité de cloisonnement s'est alors imposée notamment après plusieurs intrusions dans les réseaux universitaires
- La notion de Réseau Privé Virtuel (VPN) est arrivé beaucoup plus tard. Elle répond à 2 problématiques : l'accès au système d'information par des utilisateurs distants et l'interconnexion de réseaux en utilisant des réseaux publics beaucoup moins onéreux que les interconnexions via des liaisons spécialisées
- La solution de connexion devait évidemment avoir un niveau de sécurité équivalent à ce que l'on avait avec des liaisons privées au moins en terme de confidentialité et d'intégrité des données transitant entre les réseaux interconnectés



Définition et objectif d'un pare-feu

- Un pare-feu est un dispositif physique (matériel) et/ou logique (logiciel) permettant de contrôler des flux entre deux réseaux
- Il permet notamment de filtrer les paquets de données échangés entre un réseau privé (Lan d'entreprise par exemple) et un réseau public (comme l'Internet), il s'agit avant tout d'une passerelle filtrante
- L'objectif principal est de bloquer les attaques ou connexions suspectes venant d'un réseau tiers (Internet, partenaire...) mais il permet également de contrôler les flux de données vers l'extérieur de l'entreprise
- Un pare-feu peut aussi servir à cloisonner un réseau avec la création de zones démilitarisées (DMZ) pour séparer différentes parties du réseau en périmètres de sécurité différents
- C'est également l'endroit idéal pour surveiller et auditer les flux transitant dans l'entreprise car c'est non seulement un point de passage obligé pour l'ensemble des flux mais les informations fournies sont très précises et exhaustives

**A l'origine, le pare-feu était à la périphérie du réseau.
Maintenant, il est également au cœur du réseau.**

RAPPEL : VLAN



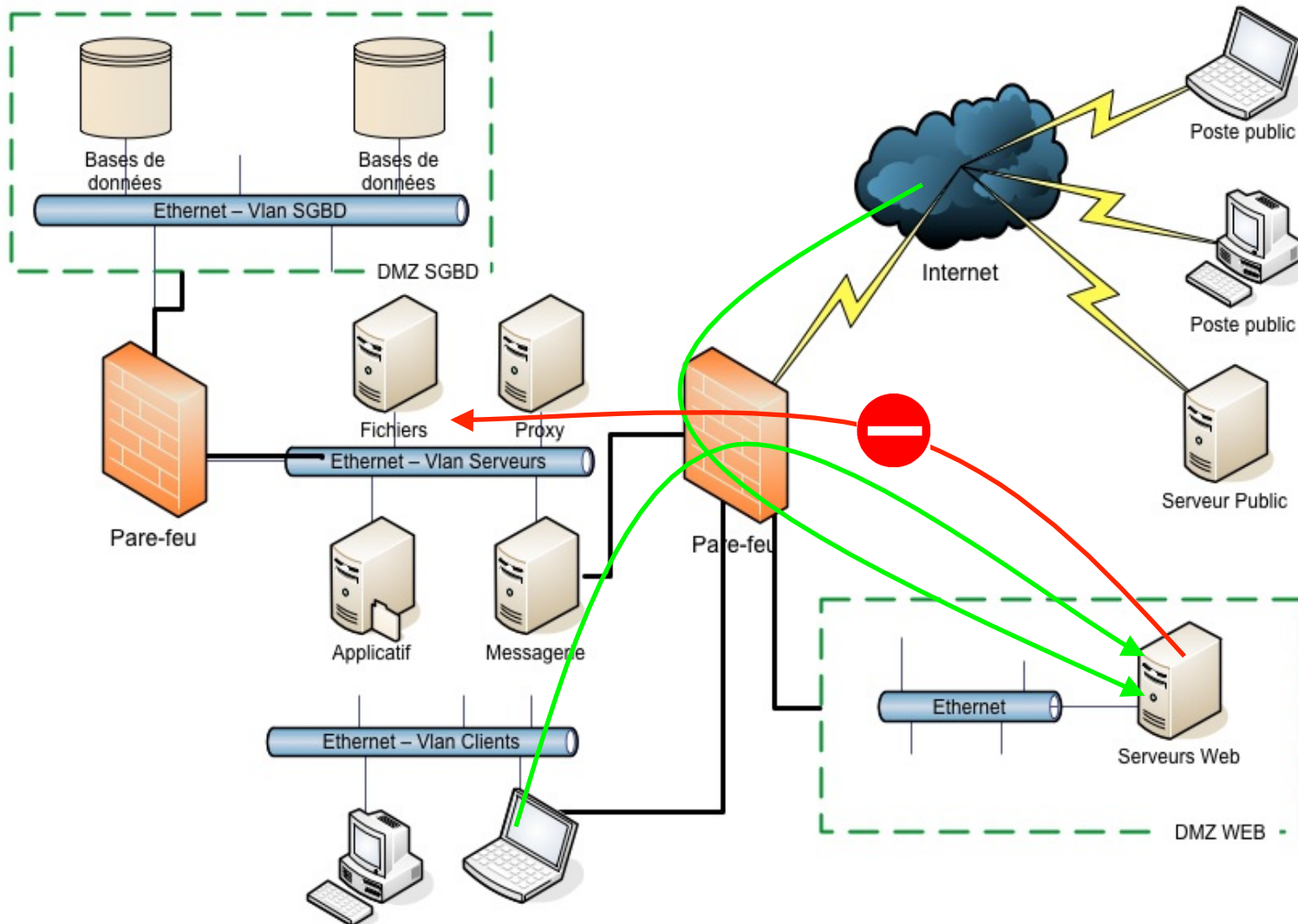
■ **Définition** : Un réseau local virtuel, communément appelé VLAN (Virtual LAN) est un réseau informatique **logique** indépendant. De nombreux VLANs peuvent coexister sur un même switch (commutateur réseau).

■ **Avantages** :

- Améliorer la gestion du réseau
- Optimiser la bande passante.
- Séparer les flux
- Segmentation : réduire la taille d'un domaine de broadcast,
- Permet de créer un ensemble logique isolé. Le seul moyen pour communiquer entre des machines appartenant à des VLANs différents est alors de passer par un ou plusieurs switches et donc de pouvoir mettre en place des **ACLs** (Access Control List) permettant de filtrer les flux.

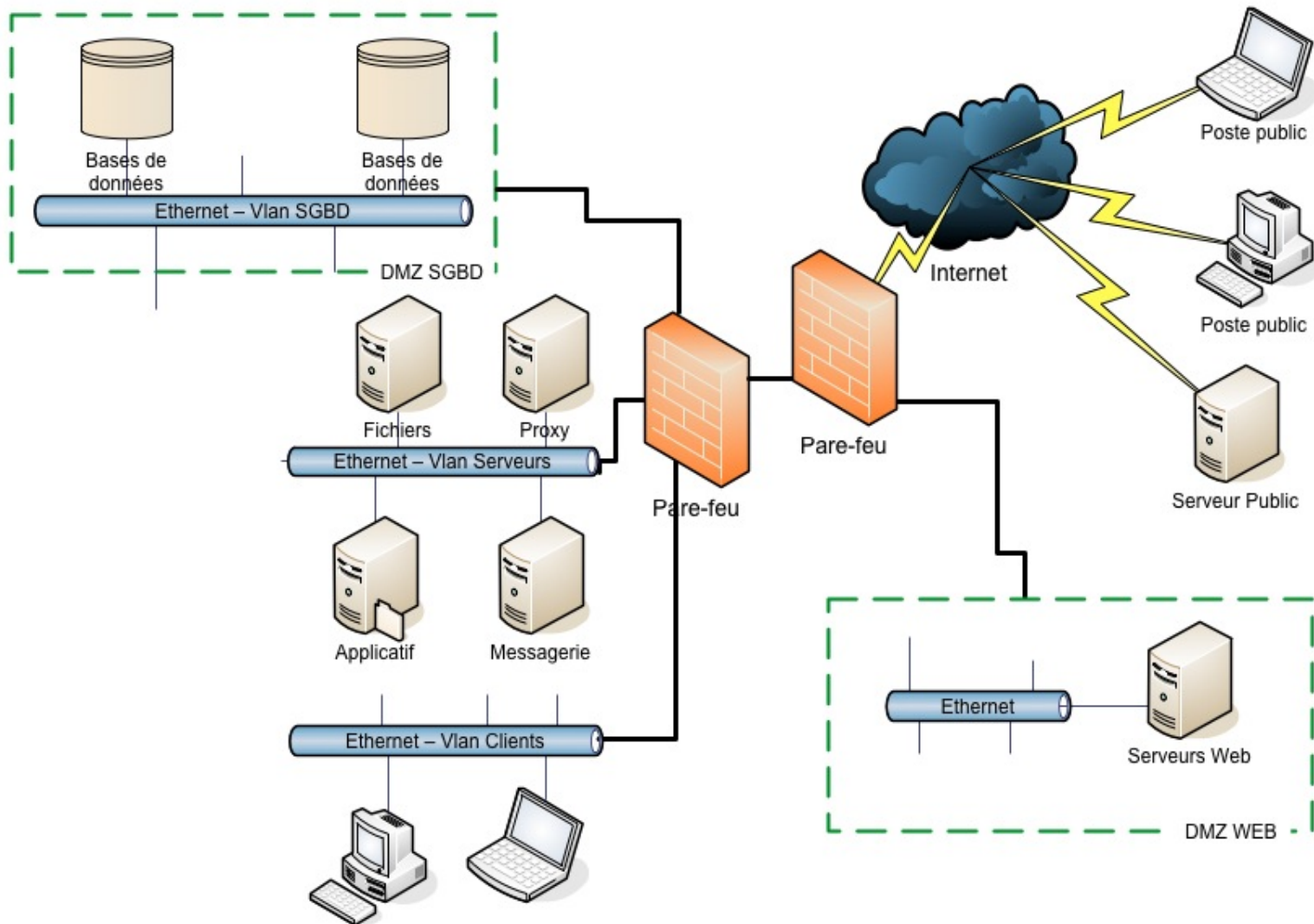


Exemple d'architecture (1/2)





Exemple d'architecture (2/2)





Politique de Vlan

■ Au niveau des Vlan, il est important de les définir suivant leur niveau de sécurité. On pourrait par exemple utiliser la politique suivante :

- Vlan utilisateurs (utilisateurs standards, IT, VIP ...)
- Vlan serveurs bureautiques (mail, fichiers ...)
- Vlan serveurs d'infrastructure (AD, DHCP, DNS)
- Vlan applications métiers (SAP, CRM ...)
- Vlan serveurs de SGBD (Oracle ...)
- Vlan serveurs extranet bureautiques
- Vlan serveurs Webs extranet
- Vlan serveurs Webs intranet
- Vlan administrateurs sécurité (système, réseau, sécurité ...)
- Vlan serveurs de sécurité (FW, Antivirus, IDS/IPS, proxy, ...)
- Vlan postes nomades utilisateurs
- Vlan postes nomades visiteurs
- Vlan VOIP
- Vlan de quarantaine
- ...



Politique et règles d'un pare-feu

■ Il existe 2 politiques en terme de pare-feu

- Tout ce qui n'est pas explicitement interdit est autorisé → à bannir
- **Tout ce qui n'est pas explicitement autorisé est interdit → règle d'or**

■ Pour les règles, elles sont définies de la manière suivante :

- Adresse IP de la machine source
- Adresse IP de la machine cible
- Type de paquet (ip, tcp, udp, icmp...)
- Numéro de port (correspond à un service connu ou à une application réseau)
- Action (accept, reject, drop)

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACKING	INSTALLATION	TIME	COMMENT
1	✗ Corporate-internal-net	Corporate-gw	* Any	drop	!	* F	* /	Stealth rule - prevent the firewall host from being scanned or attacked
2	* Any	Corporate-dmz-net	TCP http TCP https TCP smtp	accept	L	* F	* /	Allow incoming connections to the mail and web servers
3	Corporate-mail-server	✗ Corporate-internal-net	TCP smtp	accept	L	* F	* /	Allow outgoing SMTP connections, but don't allow the mail server to initiate connections to the internal networks, in case it is compromised
4	Corporate-internal-net	* Any	* Any	accept	L	* F	* /	User access to DMZ servers and Internet
5	* Any	* Any	* Any	drop	L	* F	* /	Clean up rule - block all other connections



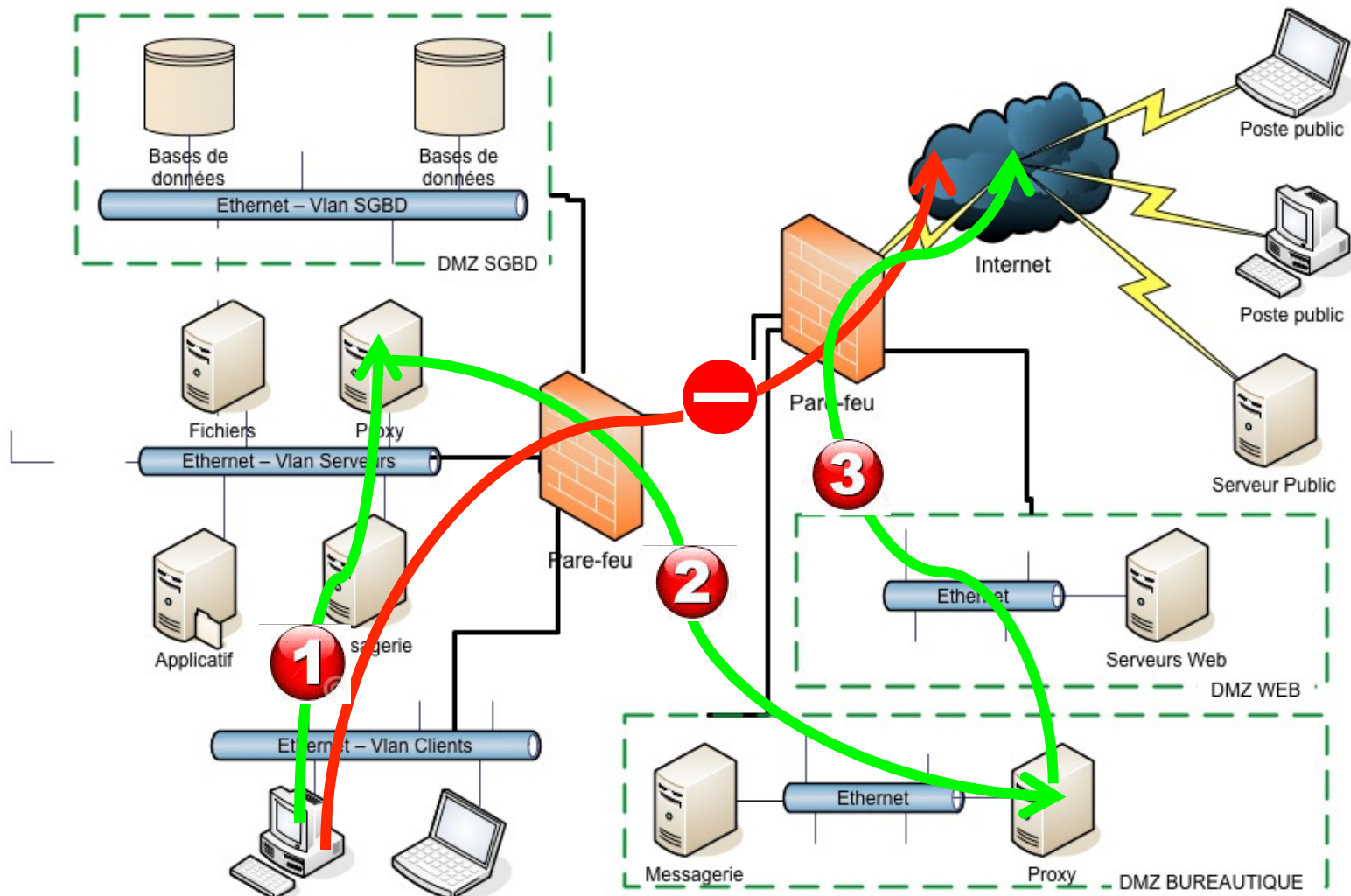
Exemple de règles (1/4)

Process	Source	Destination	Service	Action	Log
Messagerie	Serveur Interne	Serveur DMZ	SMTP	Accept	Yes
Messagerie	Serveur DMZ	Internet	SMTP	Accept	Yes
Internet Users	Postes Users	Proxy Interne	HTTP	Accept	Yes
Internet Users	Proxy Interne	Proxy Externe	HTTP	Accept	Yes
Internet Users	Proxy Externe	Internet	HTTP	Accept	Yes
Internet Users	Postes Users	Internet	HTTP	Deny	Yes
Interdit	Internet	Tout	Ftp, Telnet	Drop	Yes
Interdit	Internet	Tout	Netbios	Drop	Yes
Internet Users	Postes Users	Internet	Tout	Drop	Yes
Administration	Vlan Users Admin.	Vlan Sécurité	Spécifiques	Accept	Yes
Administration	Vlan Users	Vlan Sécurité	Tout	Drop	Yes
ERP	Vlan Serveurs	Vlan SGBD	Spécifiques	Accept	Yes
ERP	Vlan Users	Vlan SGBD	Tout	Drop	Yes
Reste	Tout	Tout	Tout	Drop	No



Exemple de règles (2/4)

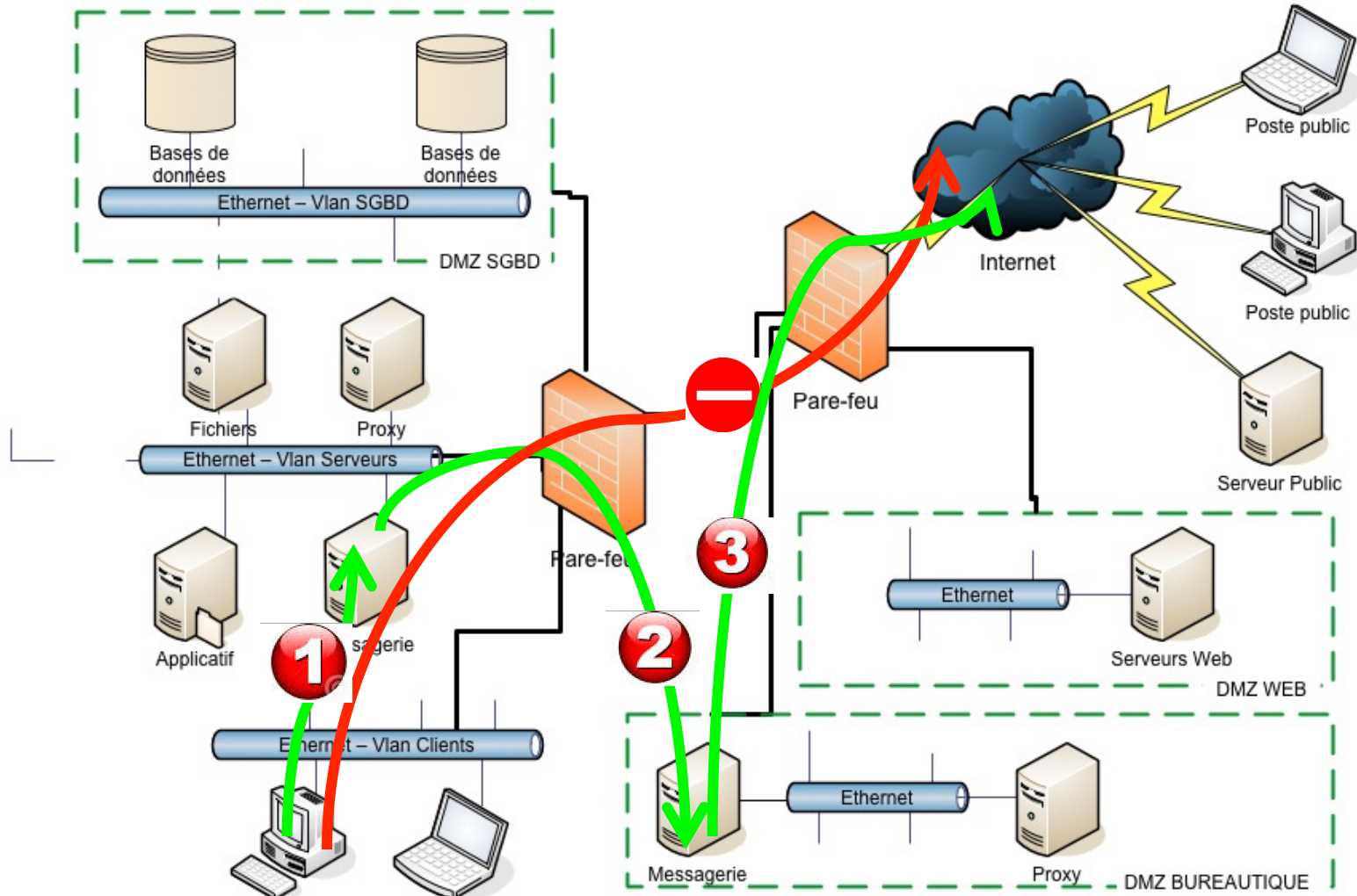
Accès à Internet





Exemple de règles (3/4)

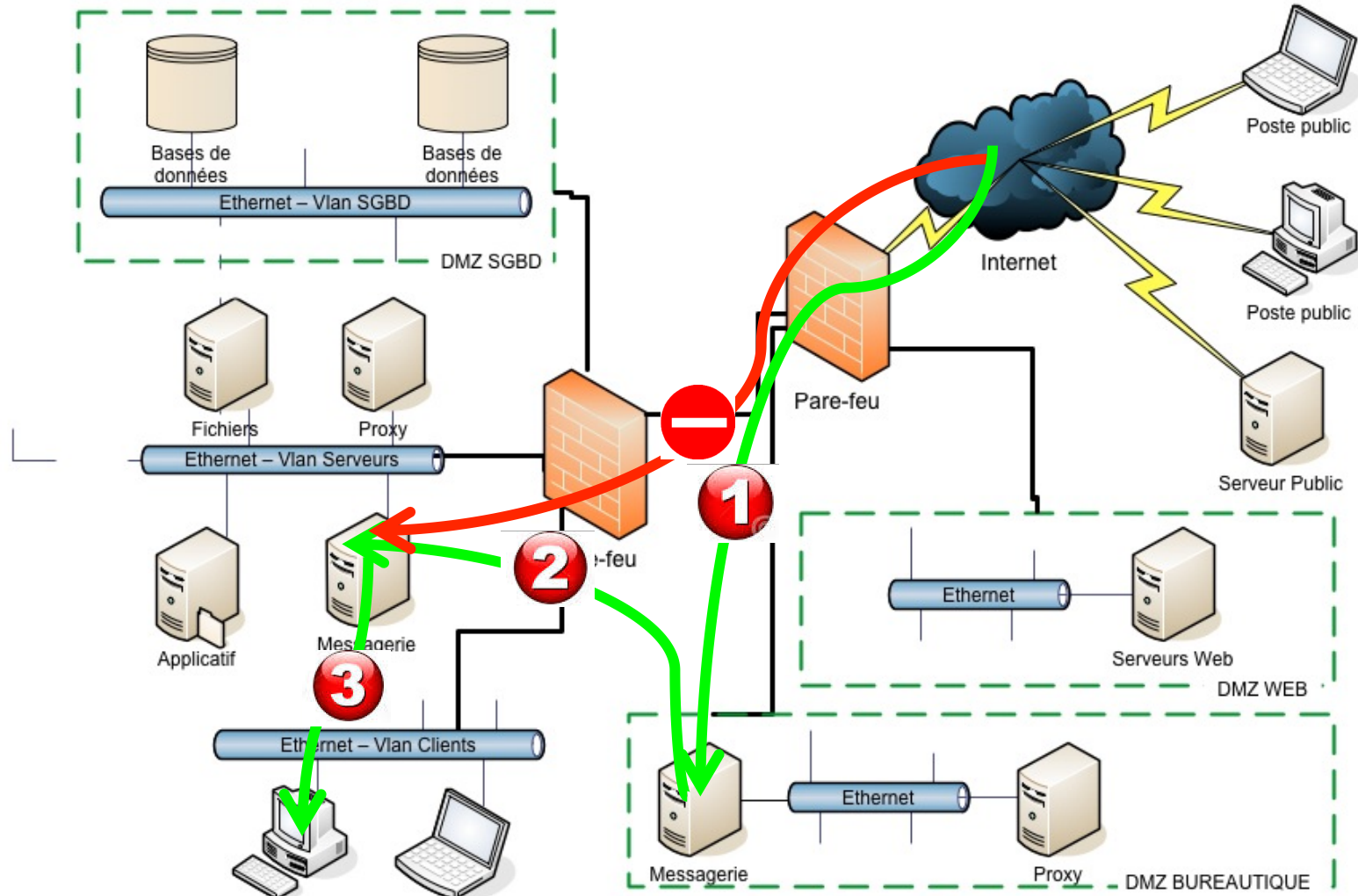
Envoi d'un e-mail





Exemple de règles (4/4)

Réception d'un e-mail





Différents types de filtrage (1/3)

- Il existe 3 types de pare-feu ou filtrage
- Le filtrage simple de paquet (stateless packet)
 - Méthode la plus simple. Elle intervient au niveau de la couche réseau du modèle OSI
 - Le filtrage se base sur : les adresses IP source et destination, les numéros de port source et destination, le protocole de niveau 3 (IP : couche Réseau)
 - Problème → les paquets sont examinés indépendamment les uns des autres or la plupart des connexions sont basées sur le protocole TCP qui gère la notion de session et ouvre de manière dynamique des ports sur la machine source. Il y a donc obligation d'ouvrir de nombreux ports (par exemple, pour pouvoir naviguer sur internet, on est obligé d'ouvrir tous les ports à partir de 1025)
 - Ce type de pare-feu n'est pratiquement plus utilisé sauf éventuellement dans les routeurs



Différents types de filtrage (2/3)

■ Le filtrage dynamique (stateful inspection ou stateful packet filtering)

- Par rapport au filtrage précédent, le filtrage dynamique permet de suivre une connexion entre le client et le serveur. On n'indique plus dans les règles le port source mais seulement le port destination. Il tient compte des anciens paquets
- Ici on travaille sur les couches 3 (IP : couche Réseau) et 4 (TCP : couche Transport) du modèle OSI
- Attention pour les paquets UDP et ICMP, il n'y a pas de mode connecté. Pour les paquets UDP, il faut autoriser pendant un délai raisonnable les réponses et interdire les paquets ICMP
- Le filtrage se base sur : les adresses IP source et destination, le numéro de destination (service), le protocole de niveau 3 (couche IP)
- Il est évidemment plus performant que le filtrage simple mais il ne protège pas contre les failles applicatives



Différents types de filtrage (3/3)

- Le filtrage applicatif (passerelle applicative ou proxy)
 - Il permet de filtrer les flux application par application (analyse protocolaire). Il intervient donc au niveau 7 de la couche OSI (couche Application). Il vérifie que les requêtes sont bien conformes aux spécifications RFCs des protocoles
 - Il faut une très bonne connaissance des applications notamment les applications métiers → grande complexité pour la création des règles
 - Il faut également une grande puissance de calcul car chaque paquet est analysé de manière très fine et des ralentissements dans les communications sont perceptibles
 - Autre problème, comme le pare-feu interprète les requêtes qui lui sont transmises, il peut donc être facilement vulnérable. Pour remédier à cela, on peut dissocier la partie pare-feu dynamique de la partie pare-feu proxy
 - Ce type de pare-feu peut également être utilisé pour faire du filtrage aussi bien au niveau du contenu que des Urls consultés ainsi que certains types de téléchargements



Protocoles à surveiller (1/2)

■ Certains protocoles sont à surveiller (aussi bien en entrée qu'en sortie) car :

- Ils peuvent être utilisés pour des attaques
- Ils ne sont pas sécurisés
- Ils ont régulièrement des vulnérabilités

■ Protocoles utilisées pour les attaques :

- HTTP (port par défaut 80), autres ports -- > 8080, 8088 ...
- HTTPS (port par défaut 443), autres ports -- > 443, 4443 ...

■ Protocoles non sécurisés (non exhaustif)

- FTP (port par défaut 21) → SFTO ou FTPS ou VPN
- TELNET (port par défaut 23) → SSH (22) ou VPN
- SMTP (port par défaut 25) → a encapsuler dans TLS/SSL
- POP3 (port par défaut 110) → a encapsuler dans TLS/SSL
- IMAP (port par défaut 143) → a encapsuler dans TLS/SSL



Protocoles à surveiller (2/2)

- Protocoles ayant régulièrement des vulnérabilités (non exhaustif) :
 - NETBIOS (port par défaut 137,138,139) → utilisé par AD
 - SMB (port par défaut 445) → partage de fichiers

- Si c'est possible, il est faudrait interdire l'utilisations des protocoles suivant depuis l'Internet :
 - ICMP
 - UDP



Ce que protège un pare-feu

- Il protège des connexions et attaques suspectes extérieures pouvant provenir des virus, vers, chevaux de Troie...et il permet de les tracer
- Il protège des connexions "sauvages" de l'intérieur vers le domaine public
- Il empêche la prolifération de virus dans un réseau quand celui-ci est cloisonné par des pare-feux
- Il protège des menaces d'intrusions internes lorsque les Vlan utilisateurs traversent le pare-feu pour accéder aux serveurs
- Il permet une défense en profondeur lorsque le réseau est cloisonné par plusieurs pare-feux → la compromission d'un serveur dans une DMZ ne peut pas être utilisée pour rebondir sur un autre serveur dans une autre DMZ



Limites d'un pare-feu

- Un pare-feu n'est qu'une brique de sécurité parmi d'autres
- Pour qu'un pare-feu soit efficace, il faut **obligatoirement** que tous les flux entrant et sortant du système d'information passent par lui
- Ce n'est pas un antivirus même si certains implémentent des fonctions antivirus → un mail contenant un virus traversera sans problème un pare-feu même applicatif
- Il n'est pas protégé des DOS et DDOS et c'est d'ailleurs souvent un **"single point of failure"** → si le pare-feu « tombe », le système d'information se retrouve soit isolé du Monde soit accessible sans aucune restriction
- Certains virus présents à l'intérieur du réseau peuvent toujours communiquer en utilisant des techniques de tunneling
- Attention aux protocoles HTTP et surtout HTTPS qui peuvent encapsuler de nombreux contenus actifs



Les 7 péchés capitaux (1/2)

- **1. L'orgueil** : même si le pare-feu est un élément indispensable et incontournable dans une architecture, il n'est pas suffisant. D'autres briques doivent être déployées.
- **2. L'avarice** : certains équipements bon marché permettent d'avoir en même temps les fonctions suivantes → pare-feu, VPN, IDS/IPS, antivirus, filtrage d'URL, serveur d'authentification, donner la météo ...
- **3. L'envie** : attention un pare-feu n'est pas un iPhone. En acheter un par snobisme pour faire comme tout le monde n'est pas la meilleure approche. Il doit correspondre à un besoin autant pour le choix de la technologie que pour ses performances et fonctionnalités.
- **4. La colère** : des utilisateurs, administrateurs réseaux ... en cas de problème (intrusion, ralentissement du réseau, filtrage trop sévère ou blocage des applications ...) c'est toujours la faute du pare-feu.



■ **7. La paresse** : tout autorisé sauf au lieu de tout interdire sauf facilite la vie de l'administrateur (et évite la colère) mais est bien peu sécurisé. Attention également aux dérives permissives.



Pare-feu vs Routeur

- Pourquoi utiliser un pare-feu plutôt qu'un routeur pour faire du filtrage ?
- **Sécurité** : séparation de la fonction de filtrage de celle de routage. Le routeur peut également filtrer un amont certaines plages d'adresses IPs de manière à « soulager » le pare-feu de certains flux indésirables et facilement filtrables.
- **Performance** : les capacités de filtrage des routeurs ne sont plus adaptées aux flux de données et à leur complexité croissants.
- **Management** : la gestion au quotidien des règles de filtrage est beaucoup plus simple sur les pare-feux que sur les routeurs.



Exemple de logs

	Date	Time	Product	Interface	Origin	Type	Action	Service	Source	Destination	Prc
35	30Oct2002	20:15:54	VPN-1 & FireWall-1	El90x1	Alaska_RND_GW	Log	Accept	http	10.111.254.11	www.fbi.gov	TCP tcp
36	30Oct2002	20:28:59	VPN-1 & FireWall-1	hme1	Alaska_member1	Log	Drop	32799	berry.abc-corp.biz		TCP tcp
37	30Oct2002	21:20:14	VPN-1 & FireWall-1	lo0	Alaska_member1	Log	Drop		California.LAN.Gauss	Alaska_member1	UDP udp
38	30Oct2002	22:29:20	VPN-1 & FireWall-1	daemon	Alaska_member2	Control					
39	30Oct2002	22:35:14	VPN-1 & FireWall-1	El90x2	Florida_GW	Log	Drop	http	152.11.41.19	Florida_GW	TCP tcp
40	1Nov2002	1:10:55	VPN-1 & FireWall-1	lo0	Alaska_member1	Log	Drop		California.LAN.Gauss	Alaska_member1	UDP udp
41	1Nov2002	1:10:59	VPN-1 & FireWall-1	daemon	Alaska_member1	Control					
42	1Nov2002	1:11:02	VPN-1 & FireWall-1	daemon	Alaska_member1	Control					
43	1Nov2002	1:11:29	VPN-1 & FireWall-1	daemon	Alaska_member1	Control					
44	1Nov2002	15:00:41	VPN-1 & FireWall-1	daemon	California_GW	Log	Accept	smtp	California.LAN.hamilton	durden.abc-corp.biz	TCP tcp
45	1Nov2002	15:06:33	VPN-1 & FireWall-1	daemon	California_GW	Log	Accept	smtp	California.LAN.hamilton	durden.abc-corp.biz	TCP tcp
46	1Nov2002	15:41:29	VPN-1 & FireWall-1	daemon	California_GW	Log	Accept	smtp	California.LAN.kummer	California_GW	TCP tcp
47	1Nov2002	16:43:13	VPN-1 & FireWall-1	hme1	California_GW	Log	Accept	sip	voip	California_GW	UDP udp
48	1Nov2002	17:43:28	VPN-1 & FireWall-1	hme1	California_GW	Log	Accept				
49	1Nov2002	18:35:11	VPN-1 & FireWall-1	daemon	California_GW	Log	Accept	smtp	California.LAN.jacob...	pc1.abc-hq.com1	TCP tcp
50	1Nov2002	18:35:14	VPN-1 & FireWall-1	El90x1	California_GW	Log	Drop	1039	35.12.10.129	California_GW	TCP tcp
51	1Nov2002	18:39:42	VPN-1 & FireWall-1	El90x1	Alaska_RND_GW	Log	Accept	http	10.111.254.11	www.ietf.org	TCP tcp
52	2Nov2002	8:10:20	VPN-1 & FireWall-1	El90x1	Alaska_cluster	Log	Reject	ftp	robot.ftp.domain.com	Alaska_DMZ_intern...	TCP tcp
53	2Nov2002	8:11:22	VPN-1 & FireWall-1	El90x1	Alaska_cluster	Log	Drop	ftp	robot.ftp.domain.com	Alaska_DMZ_intern...	TCP tcp
54	2Nov2002	8:11:30	VPN-1 & FireWall-1	El90x1	Alaska_cluster	Log	Reject	ftp	robot.ftp.domain.com	Alaska_DMZ_intern...	TCP tcp
55	2Nov2002	8:12:29	VPN-1 & FireWall-1	El90x1	Alaska_cluster	Log	Reject	ftp	robot.ftp.domain.com	Alaska_DMZ_intern...	TCP tcp
56	2Nov2002	8:14:36	VPN-1 & FireWall-1	El90x1	Alaska_cluster	Log	Reject	ftp	robot.ftp.domain.com	Alaska_DMZ_intern...	TCP tcp
57	2Nov2002	8:14:38	VPN-1 & FireWall-1	daemon	Alaska_member1	Control					
58	3Nov2002	11:14:26	VPN-1 & FireWall-1	El90x1	Alaska_cluster	Log	Reject	ftp	robot.ftp.domain.com	Alaska_DMZ_intern...	TCP tcp
59	15Mar2003	1:00:1	VPN-1 & FireWall-1	aemon	Primary_Managem...	Control					
60	15Mar2003	2:14:36	VPN-1 & FireWall-1	aemon	Alaska_cluster	Alert	Reject	http	resolved.hosts.com	Alaska_DMZ_intern...	TCP tcp
61	15Mar2003	2:19:21	VPN-1 & FireWall-1	100B0	Alaska_Finance_GW	Log	Drop	microsoft-ds	Alaska.IT.Bentli	10.112.254.9	TCP tcp
62	15Mar2003	10:9:29	VPN-1 & FireWall-1	100B1	Alaska_RND_GW	Log	Accept	8080	10.111.254.31	192.168.9.111	TCP tcp
63	15Mar2003	10:9:30	VPN-1 & FireWall-1	100B1	Alaska_RND_GW	Log	Reject	8080	10.111.254.31	192.168.9.111	TCP tcp
64	15Mar2003	10:9:31	VPN-1 & FireWall-1	100B1	Alaska_RND_GW	Log	Reject	8080	10.111.254.31	192.168.9.111	TCP tcp



Protection des applications Web (1/3)

■ L'omniprésence des sites Web font qu'ils constituent une cible de choix des pirates informatiques. Ils sont également très vulnérables car :

- Ils ont souvent un haut degré de complexité
- Ils utilisent régulièrement des bibliothèques tierces intégrées
- Ils incorporent souvent des fonctionnalités, des technologies et des protocoles d'avant-garde (c'est-à-dire pas encore éprouvés)
- Les développeurs et responsables commerciaux qui favorisent les fonctionnalités et la rapidité de mise sur le marché au détriment de l'amélioration de la qualité du code et de la réduction des vulnérabilités
- La maintenance est souvent laissé à des tiers ou à l'abandon
- Pas de veille sur les nouvelles vulnérabilités et nouvelles technologies de sécurisation

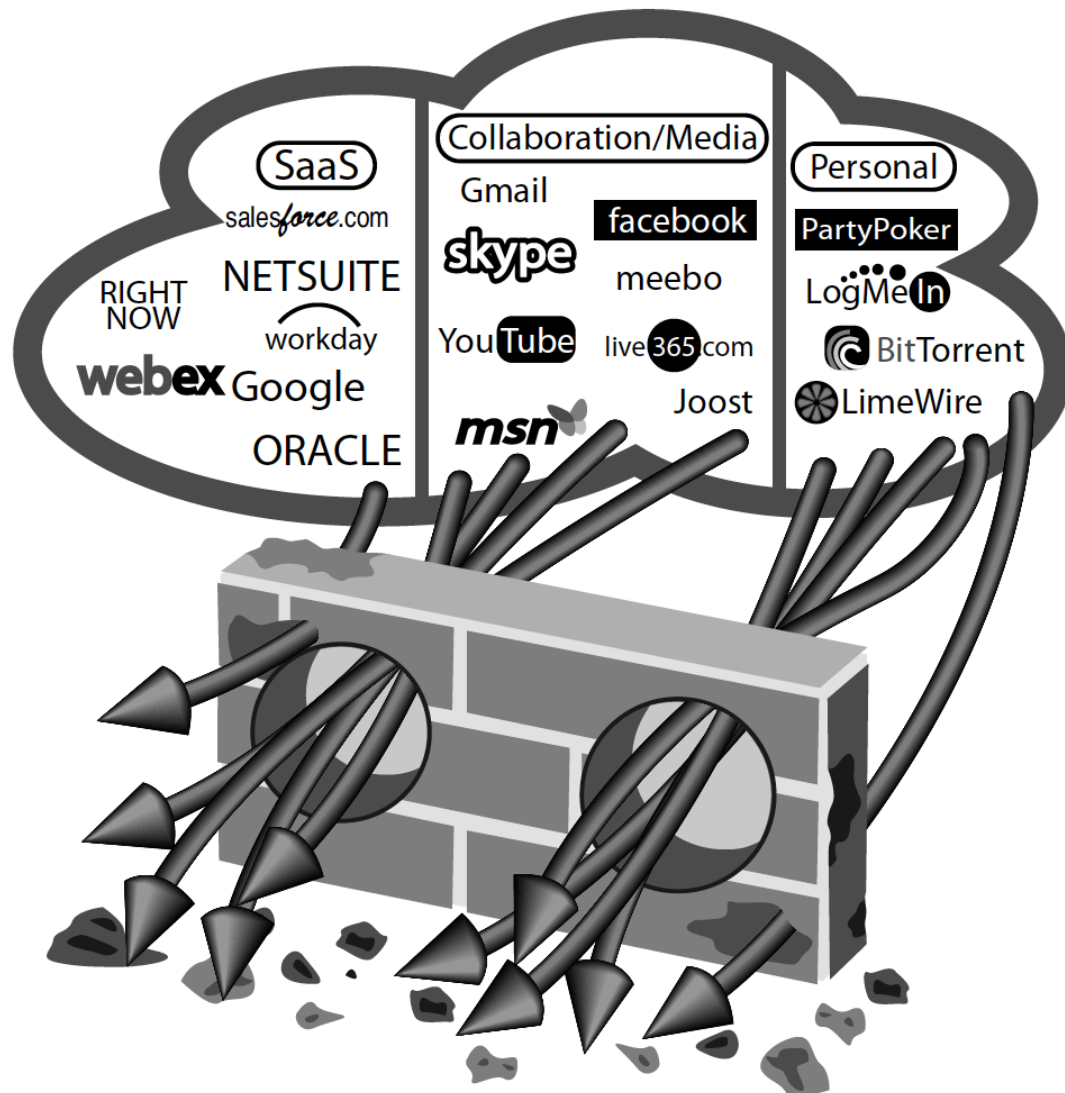


Protection des applications Web (2/3)

■ Quelques circonstances aggravantes :

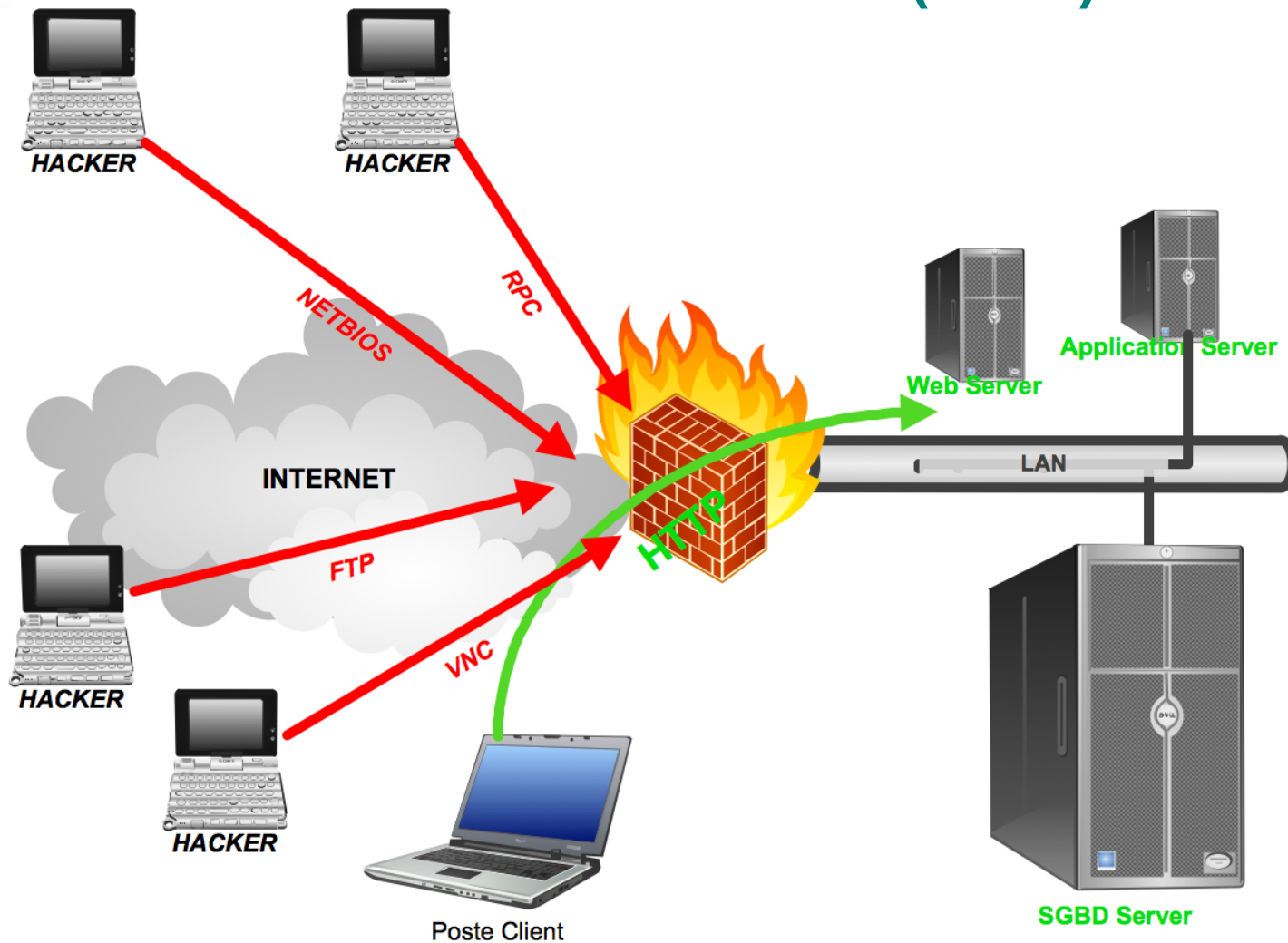
- Les applications Webs servent de canaux d'accès à des données sensibles et/ou bancaires, spécifications de produits propriétaires, des dossiers médicaux ainsi que la multitude de données d'identification personnelles
- Une fois qu'un pirate parvient à pénétrer la porte d'entrée généralement très conviviale d'une application Web orientée client, il lui suffit de récupérer un ou plusieurs chemins configurés menant aux bases de données d'arrière-plan associées

Protection des applications Web (3/3)





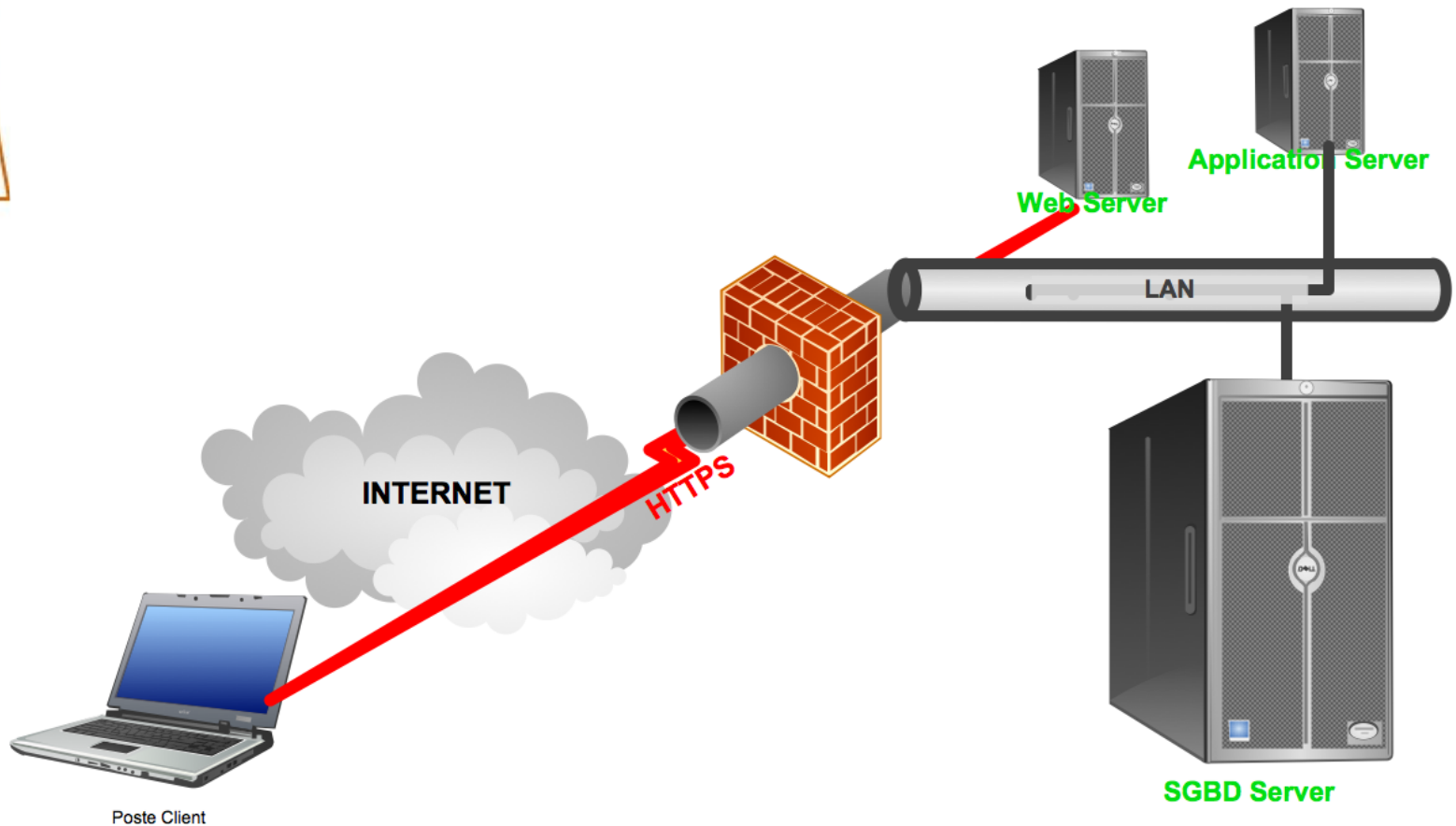
Cas du WAF (1/9)



La problématique N°1



Cas du WAF (2/9)

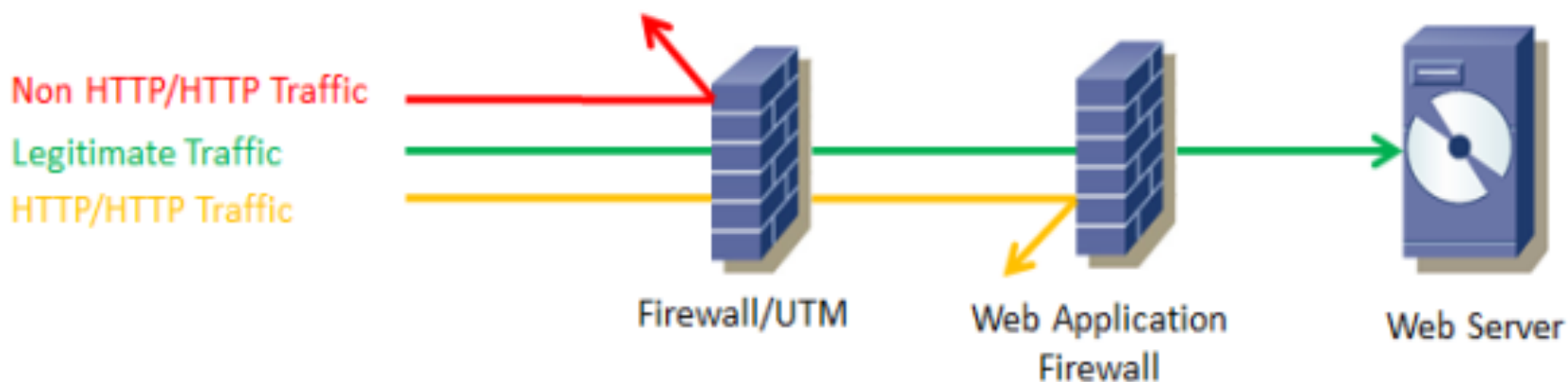


La problématique N°2



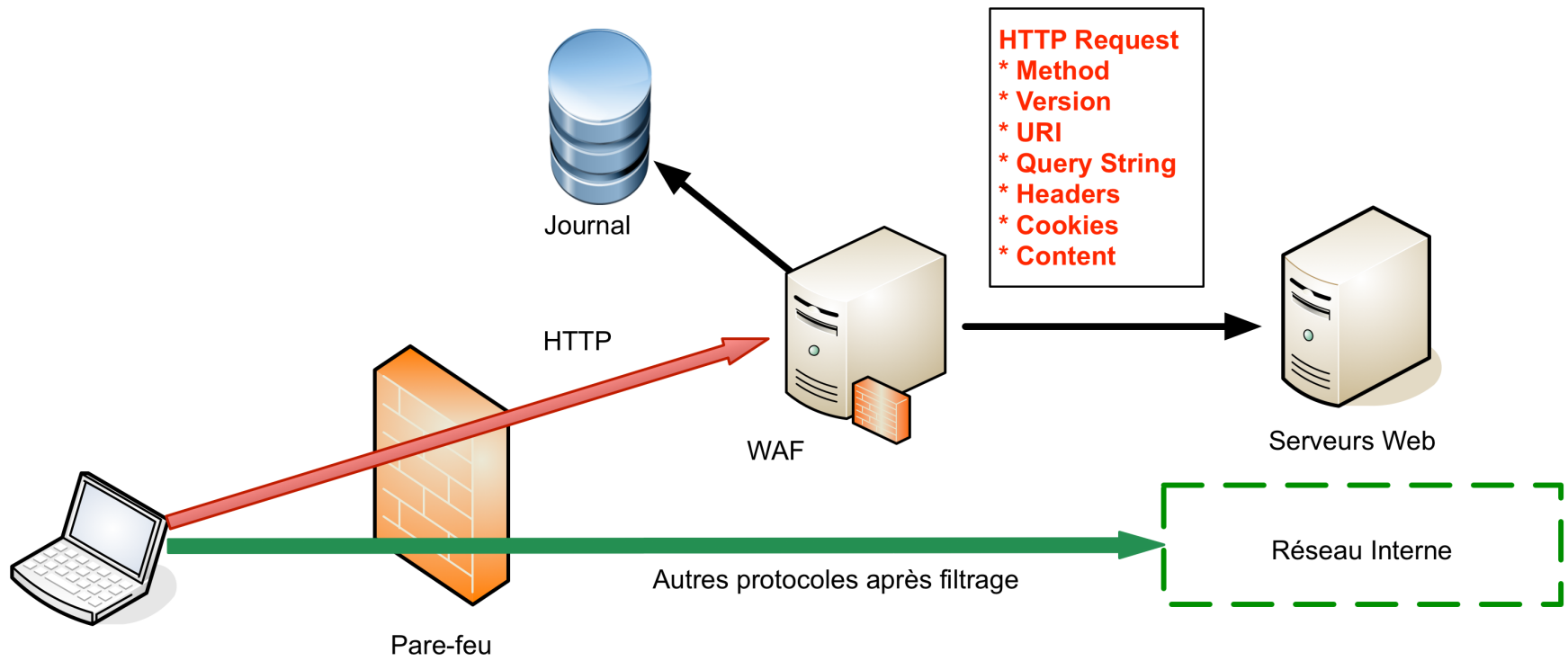
Cas du WAF (3/9)

- Un Web Application Firewall est un pare-feu applicatif qui intervient au niveau de la couche 7 du modèle OSI
- Un WAF analyse seulement le de trafic HTTP/HTTPS/XML/SOAP → fonctions de normalisation et de reporting
- Il permet de patcher virtuellement les problèmes → plus ou moins efficace suivant le modèle de sécurité (positif ou négatif)
- Cacher tout ou partie de l'infrastructure (mode reverse proxy)



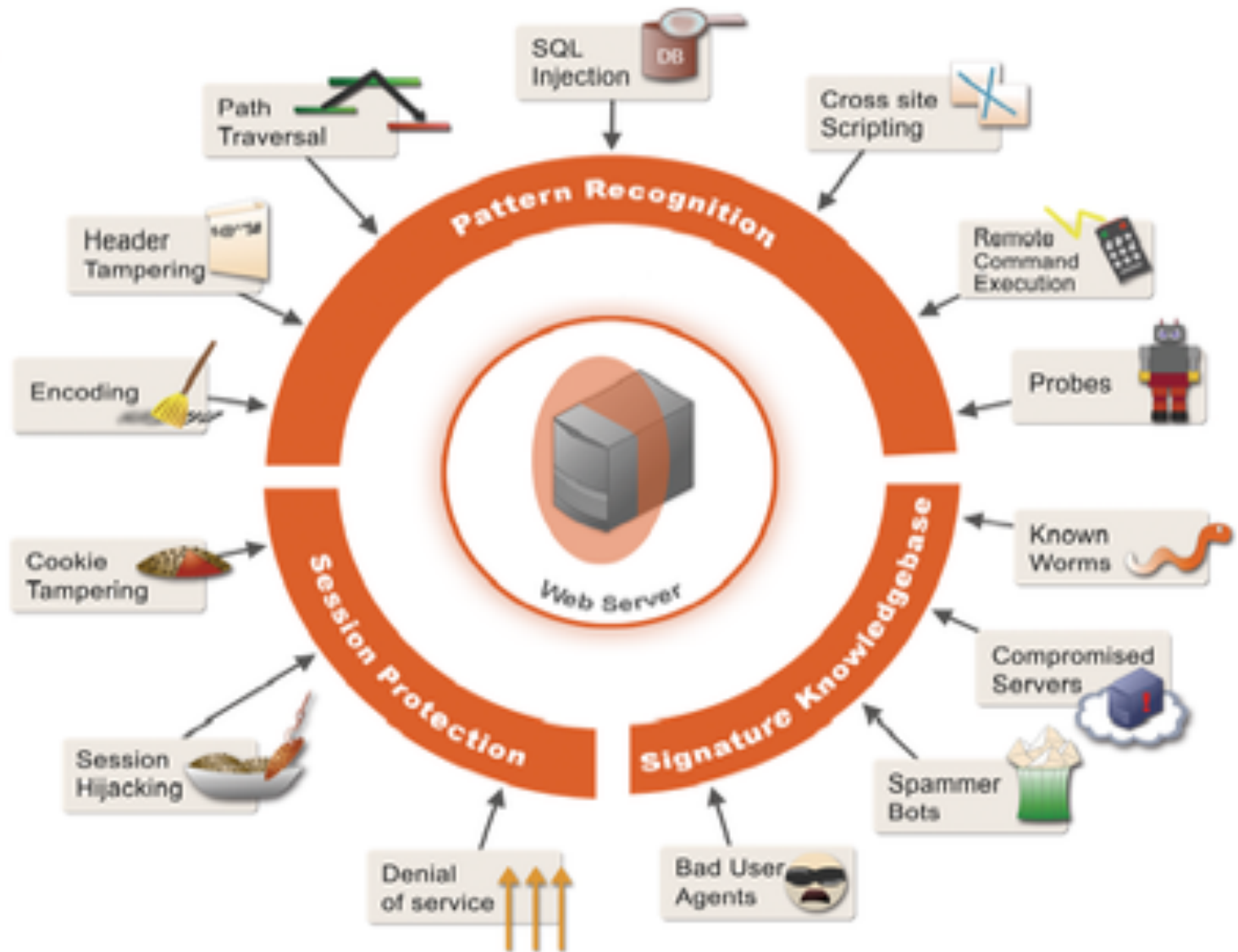


Cas du WAF (4/9)





Cas du WAF (5/9)





Cas du WAF (6/9)

- Un WAF doit avoir au minimum les fonctionnalités suivantes :
 - Valider les entrées : stopper les attaques par injection SQL, cross-site scripting ou directory traversal
 - Détecter les attaques par modification de cookie, de session ou de paramètre
 - Stopper l'exfiltration des données sensibles via l'identification et le blocage au niveau des objets
 - Inspecter complètement le trafic chiffré SSL pour tous les types de menaces intégrées
 - Assurer une protection efficace contre les attaques par les attaques par déni ciblant la couche applicative
 - Masquer de façon dynamique les données de réponse des serveurs, potentiellement utiles aux pirates
 - Assurer une protection XML complète, comprenant la validation de schéma pour les messages SOAP et des défenses contre l'injection XPath, et identifier et bloquer les pièces jointes XML hébergeant un contenu malveillant



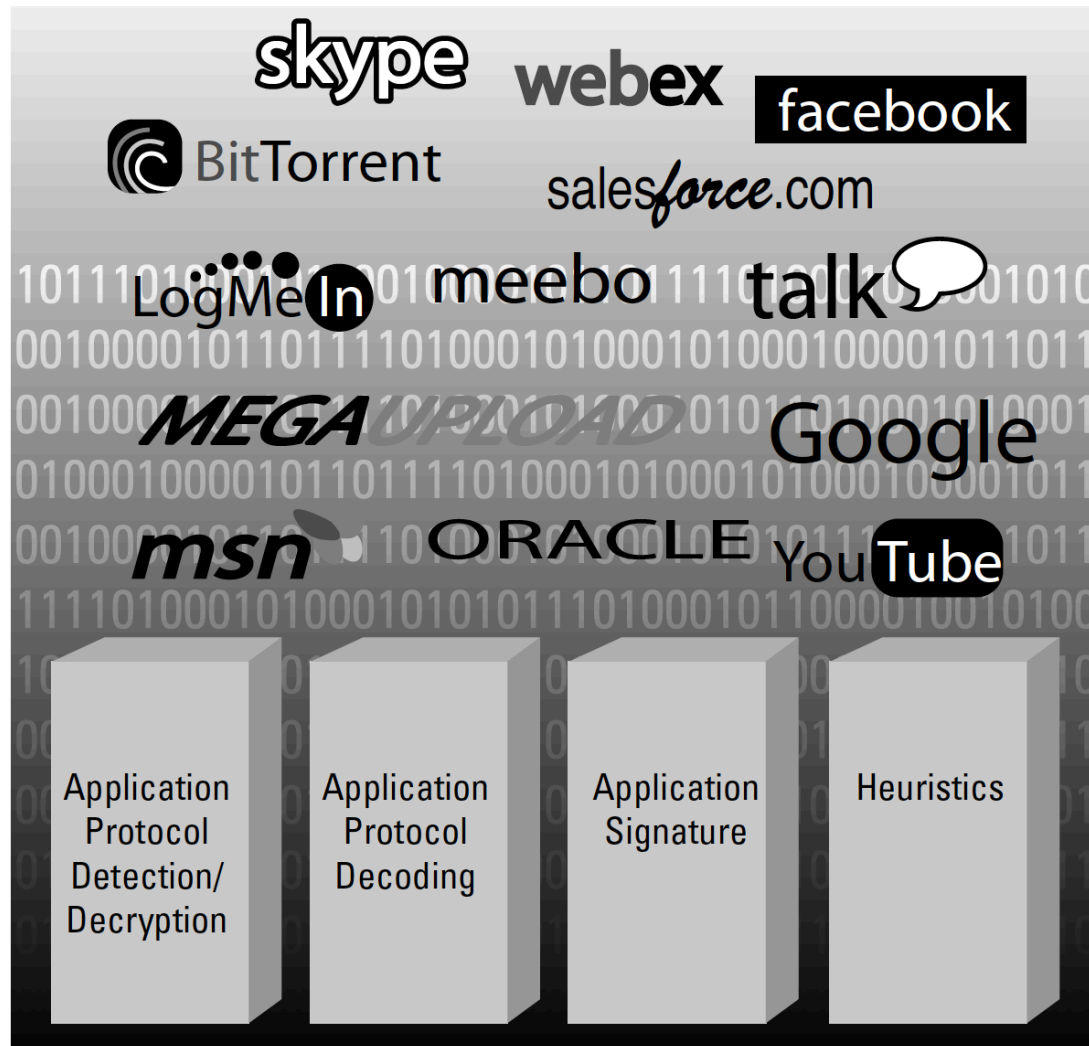
Cas du WAF (7/9)

- Un WAF fonctionne selon 2 modèles de sécurité :
 - **Soit Positif** : tout ce qui n'est pas explicitement autorisé est interdit (définition de manière exhaustive de l'ensemble des pages, des arguments de la **query string**, des données postées)
 - **Soit Négatif** : tout ce qui n'est pas explicitement interdit est autorisé (notamment avec une base sur une liste de signatures)

- Ces 2 modèles n'étant pas suffisant, on peut intégrer d'autres technologies :
 - **Canonisation** : normalisation des données avant de les envoyer au moteur d'analyse → ré-encodage des données
 - **Stateful** : différent du « stateful » des pare-feu classiques → sécurisation des éléments de suivi de session (cookies, paramètres dans l'URL ...)
 - **Antivirus**
 - **Lutte contre le DOS** : pas indispensable et à double tranchant
 - **IPS/IDS** : pas son job, à utiliser dans le cas où il n'y a pas d'IDS/IPS dédié



Cas du WAF (8/9)



Techniques d'identification des applications



Cas du WAF (9/9)

	Négatif	Positif
Concept	Le WAF reconnaît les attaques et les bloque, il autorise tous les accès.	Le WAF connaît le trafic légitime et rejette tout le reste.
Avantages	<ul style="list-style-type: none">• Aucun besoin de personnalisation• Protection standard• Simple à déployer	<ul style="list-style-type: none">• Bloque les attaques inconnues• N'est pas dépendant d'une base de signature.• Détection précise
Inconvénients	<ul style="list-style-type: none">• Extrêmement dépendant des signatures• Pas très précis	<ul style="list-style-type: none">• Configuration complexe• Sensible aux faux positifs



Cas du pare-feu personnel

- Un pare-feu personnel est un pare-feu installé sur un poste de travail et ne protégeant que celui-ci
- Il s'apparente beaucoup à un pare-feu applicatif → les règles sont définies au niveau des **applications** bien que quelques pare-feux vont un peu plus loin et peuvent également définir des règles au niveau **réseau**
- Il est utilisé pour contrer les connexions provenant de l'extérieur mais également les connexions sortantes non autorisées → notamment les chevaux de Troie
- Il intègre souvent des fonctions de contrôle d'intégrité → utilisation de fonctions de hachage au niveau des fichiers systèmes et des applications installées
- Il intègre ou est souvent intégré à un antivirus
- Il intègre quelque fois un HIPS
- Attention les pare-feux personnels sont faillibles → utilisation de failles dans ceux-ci pour les désactiver ou injecter du code

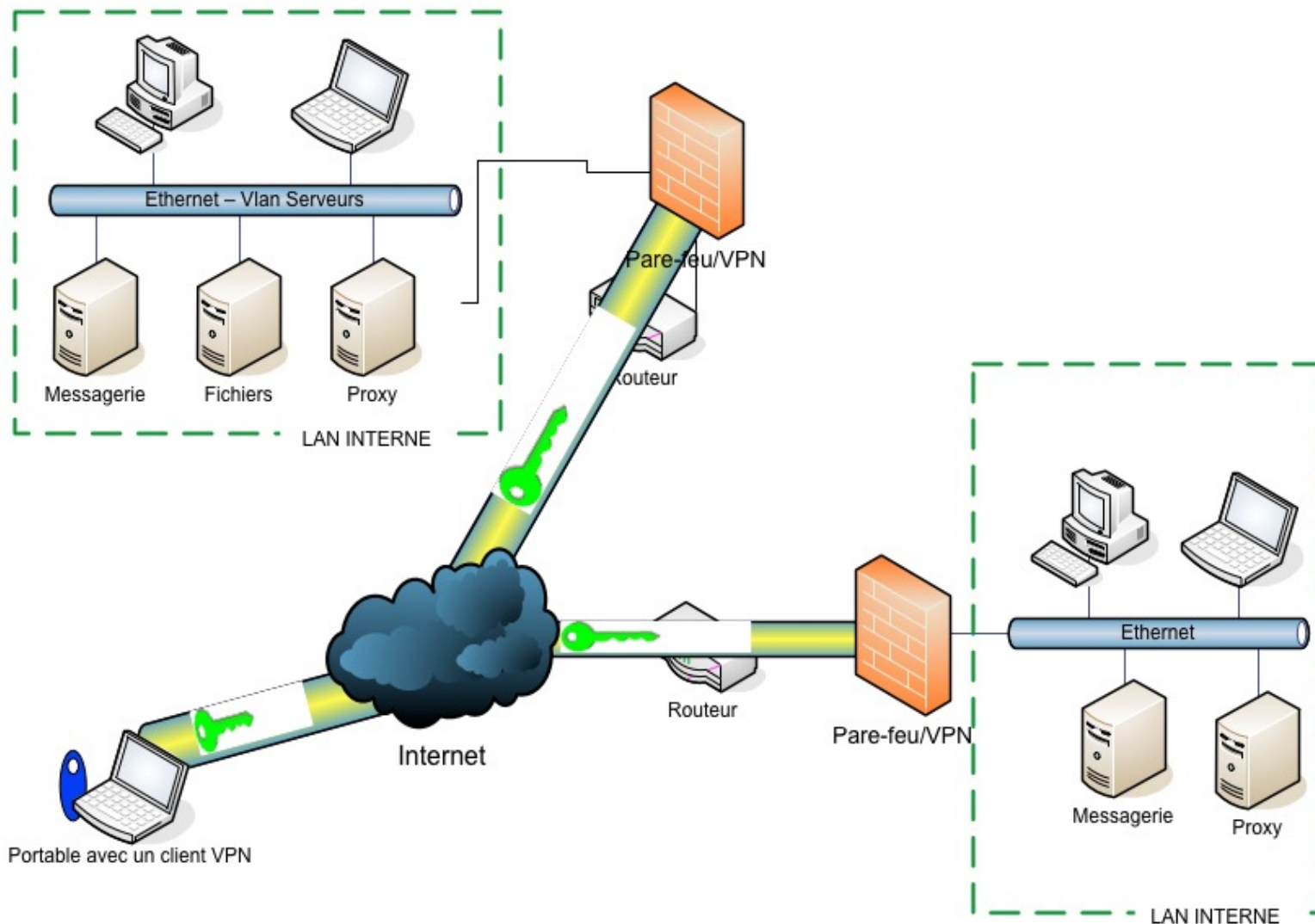


Définition et objectif d'un VPN

- Un réseau privé virtuel (Virtual Private Network ou VPN) est un réseau artificiellement créé en utilisant l'architecture du réseau public (Internet)
- On dit "**Virtuel**" car on relie 2 réseaux physiques par une liaison non fiable (Internet) sur laquelle l'entreprise n'a aucune certitude de la qualité de service ou de la sécurité
- On dit "**Privé**" car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent échanger des données
- Un VPN permet d'obtenir une liaison sécurisée à moindre coût et facilement déployable : les données sont chiffrées (on parle de tunneling) au travers du réseau et l'utilisation d'authentification forte est possible
- Un VPN est utilisé dans 3 cas :
 - Tunnel de type intranet → entre 2 sites d'une entreprise
 - Tunnel de type accès distant → entre le site d'une entreprise et un poste de travail via un réseau public filaire ou sans-fil
 - Tunnel de type extranet → entre le site d'une entreprise et ses partenaires, ses fournisseurs, ses clients.....



Architecture d'un VPN





Différents types de protocoles

- PPTP (Point to Point Tunneling Protocol) → protocole de niveau 2 développé entre autres par Microsoft, il utilise le protocole PPP (très connu pour les communications séries)
- L2F (Layer Two Forwarding) → protocole de niveau 2 développé entre autres par Cisco, c'est un protocole qui n'est quasiment plus utilisé
- L2TP (Layer Two Tunneling Protocol) → issu des travaux de l'IETF (Internet Engineering Task Force) pour réunir les protocoles PPTP et L2F, c'est un protocole de niveau 2 s'appuyant sur PPP
- **IPSEC** (Internet Protocol SECurity) → c'est un protocole de niveau 3, il est issu des travaux de l'IETF. C'est le protocole le plus utilisé et le plus sécurisé (chiffrement, intégrité, confidentialité, authentification...)
- **MPLS** (Multi-Protocol Label Switching) → utilisé à l'origine pour améliorer le trafic IP, ce protocole est très largement utilisé par les opérateurs pour mettre en place des VPNs



Ce que protège un VPN

- Il protège contre l'écoute d'un réseau (sniffing) → confidentialité assurée par le chiffrement des communications
- Il protège contre l'usurpation d'identité et les attaque du type Man in the Middle → authentification forte et authentification mutuelle entre les 2 réseaux
- Il protège contre la modification du flux → intégrité des paquets envoyés assurée par le chiffrement des communications
- Il protège contre les attaques de type replay → impossibilité de rejouer une session
- Il protège contre les attaques par rebond → le tunnel est seulement "ouvert" entre les réseaux autorisés



Exemple de logs

D.	Date	Time	Origin	Type	Action	Service	Source	Destination	Proto.	User
	1Jan2003	22:54:13	Alaska_cluster	Log	Key Install		California.LAN.jacob...	Alaska_cluster		MR. TEST
	1Jan2003	22:54:13	Alaska_cluster	Log	Login		California.LAN.jacob...			MR. TEST
	15Jan2003	22:59:34	California_GW	Log	Encrypt	nbssession	California.LAN.hamilton	Alaska.LAN.Chincilla	TCP	tcp
	15Jan2003	22:54:14	Alaska_cluster	Log	Decrypt	http	Alaska.Fin.Deasel	Florida.LAN.euclid	TCP	tcp
	29Jan2003	22:53:49	Delaware_cluster	Log	Decrypt	nbssession	California.LAN.hamilton	Alaska.LAN.Chincilla	TCP	tcp
	2Feb2003	22:59:35	California_GW	Log	Encrypt	http	Alaska.Fin.Deasel	Florida.LAN.euclid	TCP	tcp
	2Feb2003	22:54:14	Alaska_cluster	Log	Key Install		California.LAN.jacob...	Alaska_cluster		MR. TEST
	4Feb2003	22:59:35	California_GW	Log	Encrypt	http	Alaska.Fin.Deasel	Florida.LAN.euclid	TCP	tcp
	12Feb2003	22:54:14	Alaska_cluster	Log	Decrypt	http	Alaska.Fin.Deasel	Florida.LAN.euclid	TCP	tcp
	17Feb2003	22:54:15	Alaska_cluster	Log	Decrypt	http	Alaska.Fin.Deasel	Florida.LAN.euclid	TCP	tcp
	19Mar2003	22:59:36	California_GW	Log	Encrypt	http	Alaska.Fin.Deasel	Florida.LAN.euclid	TCP	tcp
	19Mar2003	23:23:59	Alaska_cluster	Log	Decrypt	http	Alaska.Fin.Deasel	Florida.LAN.euclid	TCP	tcp
	19Mar2003	23:23:59	Alaska_cluster	Log	Decrypt	http	Alaska.Fin.Deasel	Florida.LAN.euclid	TCP	tcp
	19Mar2003	23:29:21	California_GW	Log	Encrypt	http	Alaska.Fin.Deasel	Florida.LAN.euclid	TCP	tcp
	19Mar2003	23:24:00	Alaska_cluster	Log	Decrypt	http	Alaska.Fin.Deasel	Florida.LAN.euclid	TCP	tcp
	19Mar2003	23:29:21	California_GW	Log	Encrypt	http	Alaska.Fin.Deasel	Florida.LAN.euclid	TCP	tcp
	19Mar2003	23:29:21	Florida_GW	Log	Key Install		Florida_GW	Alaska_cluster		
	19Mar2003	23:29:22	California_GW	Log	Encrypt	nbssession	California.DMZ.Lagr...	Alaska.LAN.Chincilla	TCP	tcp
	19Mar2003	23:24:01	Alaska_cluster	Log	Decrypt	http	Alaska.Fin.Deasel	Florida.LAN.euclid	TCP	tcp
	19Mar2003	23:24:01	Alaska_cluster	Log	Key Install		Florida_GW	Alaska_cluster		
	19Mar2003	23:24:01	Alaska_cluster	Log	Decrypt	nbssession	host6	Alaska.LAN.Chincilla	TCP	tcp
	19Mar2003	23:29:22	California_GW	Log	Encrypt	http	Alaska.Fin.Deasel	Florida.LAN.euclid	TCP	tcp



Cas du VPN SSL

■ Arrivés depuis peu dans le monde des VPNs, les VPNs SSL (basés sur la couche 4 : Transport) sont très intéressants par rapport aux VPNs "classiques" :

- Au lieu d'utiliser un client "lourd" ou un équipement spécifique pour créer un tunnel, les VPNs SSL utilisent un client "léger" de type Internet Explorer
- Pas d'installation du côté client et peu de modifications du côté des administrateurs, pas de mise à jour pour le client "lourd" → très pratique pour déployer des applications vers un grand nombre de personnes
- Utilisable partout et sur toutes les plateformes car tous les flux passent en Https (SSL) : hôtel, cybercafé, hotspot public, PDA, téléphones

■ Même si cette solution est très séduisante, elle pose les problèmes suivants :

- Le navigateur lui-même est soumis à des vulnérabilités
- La gestion des certificats (si on en utilise) n'est pas simple pour un utilisateur novice
- Maintenance des applets Java ou ActiveX pour faire fonctionner les applications "webisées"
- Ne sécurise que le niveau applicatif



Cas du VPN MPLS


■ Le VPN MPLS (Multi-Protocol Label Switching) est un VPN utilisé par les opérateurs pour pouvoir relier différents sites sans avoir un chiffrement point à point. Les différentes avantages d'un tel réseau sont :

- Maillage any-to-any
- Meilleure gestion des priorités de flux et de la bande passante
- Rapidité de commutation
- Réseau entièrement géré par l'opérateur
- Utilisation de la VOIP possible
- Coût des commutateurs réduits

■ Malgré cela cette solution présente quelques inconvénients :

- Configuration des routeurs du backbone assez complexe
- Manque d'interopérabilité entre les opérateurs → problème pour les déploiements internationaux
- Coût et lourdeur de la mise en place de la solution

Conclusion

- 
- Les pare-feux sont des briques indispensables dans la mise en place de la sécurité dans un système d'information mais ce n'est pas suffisant
 - Attention également à bien configurer les pare-feux et surtout la "dérive" qui suit leur mise en place. En effet, un pare-feu impose de nombreuses contraintes et il est facile, sous la contrainte des utilisateurs et des informaticiens eux-mêmes d'avoir des règles beaucoup trop permissives → faire auditer les pare-feux et notamment règles
 - De même les pare-feux applicatifs de nouvelles générations inclus des modules IDS/IPS ce qui n'est pas sans poser des contraintes d'administration au quotidien → attention aux discours marketing
 - Les avantages des VPNs sont tels notamment en terme de coût que ceux-ci ont très rapidement supplanter les liaisons louées ou spécialisées
 - Pour les VPNs, les 2 grandes tendances qui émergent sont les solutions à base de MPLS (technologie réseau → n'importe quel flux peut donc y transiter de manière sécurisé) car elles intègrent également les solutions de téléphonie sur IP et les solutions de VPN SSL car elles sont facilement déployables à grande échelle et utilisable partout