Règles de Filtrage Réseau et Applicatifs

Les firewall face à la cybersécurité

- Logiciels malveillants
- Phishing
- Intrusions sur un réseau/un système
- Exploitation de vulnérabilités
- Attaque par déni de service

Les principes de base

- Liste de règles d’autorisation/d’interdiction
- Tout ce qui n’est pas autorisé est interdit: Philosophie de la sécurité
- Blocage du traffic entrant/autorisation du traffic
- Firewall StateFull (avec état)/Firewall StateLess

Firewall: principes

- Accès sécurisé et transparent aux serveurs de l ’Internet
- Filtrage sur protocoles de communication
- Filtrage sur les applications
- Filtrage sur les utilisateurs
- Fichiers logs et statistiques d’utilisation
- Gestion possible de réseaux complexe (VPN, DMZ, NAT)

Les Firewalls: Fonctionnalités et principes

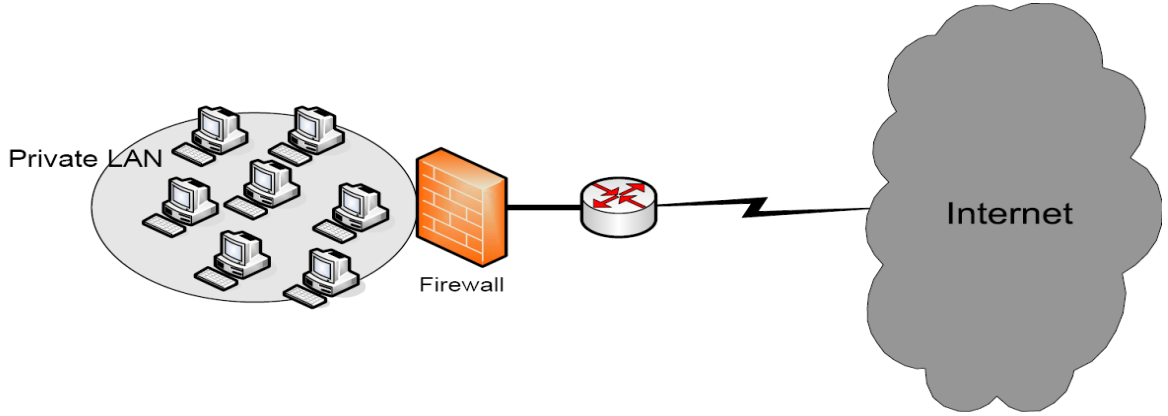
- Avantages
  - Gestion de la sécurité centralisée
    - Tout passe par le firewall
  - Configuration et périmètre du réseau sont indépendants
  - Capacité d'audit du trafic du réseau
    - Tout passe par le firewall
    - Possibilité de traces
  - S'applique sur:
    - une partie du réseau
    - Sur tout le réseau
  - Ouvert au module (add)
  - Aucune modification sur les postes clients ni serveurs

Firewall : Fonctionnalités et principes

- Composant logiciel ou matériel
  - Assure une fonction de filtrage
  - S'appuie sur des règles de filtrage
    - Les règles ou filtres portent des noms différents selon l'éditeur
    - Access Control List ou ACL (CISCO), Policy (Juniper Networks)
  - Règles définies par l'administrateur de réseaux
  - Règles issues d'une politique de sécurité

- Un Firewall peut être placé entre:
  - Un réseau Interne et le réseau Internet global
  - Au sein du réseau pour le cloisonnement

Filtrage sur protocoles
Filtrage sur les applications
Filtrage sur les utilisateurs
Fichiers logs et statistiques
Gestion possible de réseaux complexe :VPN, DMZ, NAT
IDS/IPS



Firewall : Fonctionnalités et principes

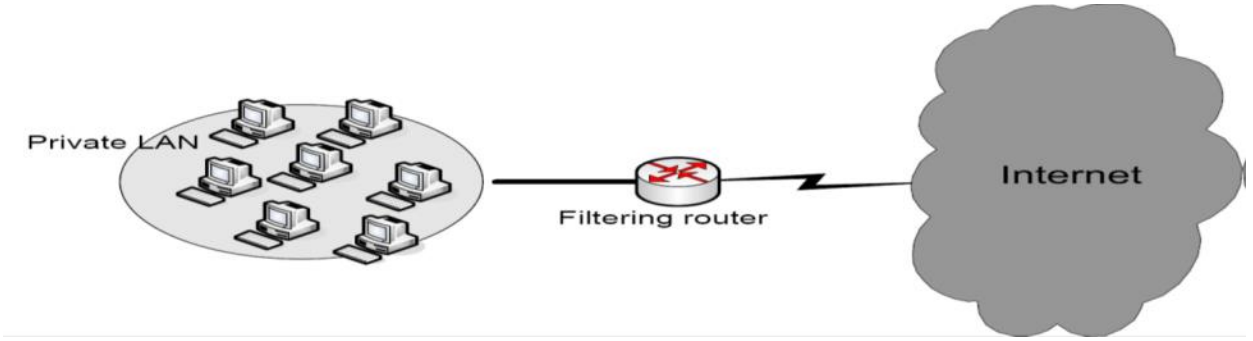
- Inconvénients
  - Goulet d'étranglement du réseau
  - Point névralgique du réseau (Cible favori des hackers)
  - Syntaxe spécifiques pour chaque éditeur
  - Absence de standard à tous niveaux
    - Architectures, règles, gestion, certification, interface
  - Nécessite
    - La maîtrise totale des protocoles traversés (TCP/IP, RTP, RTSP, SIP, HTTP,FTP, H323, SQL,…)
    - Compréhension du fonctionnement du pare-feu (interface entre les divers niveaux de filtrage, la traduction d'adresse,…)
  - n'assure pas:
    - la confidentialité des données mais possibilité de VPN
    - l'intégrité des données possibilité d'interfacer un firewall avec un anti-virus pour vérifier l'intégrité de données
  - ne protège pas le trafic qui ne passe pas par lui
  - ne protège pas contre des menaces internes

Les Firewalls: Fonctionnalités et principes

- Routeurs Filtrants
  - Le routeur fait le lien entre un réseau Internet et un réseau Interne ou privé
  - Il assure par définition l'acheminement des paquets IP
  - Son architecture matériel et logicielle est conçu pour des fonctions d'acheminement
  - Le routeur peut filtrer ou sélectionner les paquets sur la base de règles:
    - On le nomme ROUTEUR FILTRANT
  - Un routeur filtrant est considéré comme un firewall
    - On dit qu'il est stateless car il n'a pas de mémoire quant aux flux

Les Firewalls

- Routeurs Filtrants
  - Filtrage efficace sur les champs des protocoles de communication (adresse IP…)
  - Intégré à la plupart des routeurs du marché
  - Bien adapté au réseau de type PME
  - Nécessite une bonne connaissance technique des protocoles
  - Spécifique par routeur avec une syntaxe de bas niveau
  - Généralement pas de fichiers logs et de statistiques exploitables



Firewall : Différents types

- Sur châssis propriétaire (Appliance)
  - Avantages: robustesse
  - Inconvénients: évolutivité limitée
- Sur OS Sécurisé (Unix bsd)
  - Avantages: Implémentation sur architecture PC
  - Inconvénients:
    - Interaction étroite Firewall&OS
    - Problème de mise à jour

Firewall
Différents types de Firewall.

- Netfilter/Iptables (Linux 2.4),
- PacketFilter (OpenBsd)
- IP-Filter (FreeBsd, NetBsd, HPUX, Solaris)
- Checkpoint software (Firewall-1)
- Palo Alto Networks
- Fortinet
- Cisco (PIX, Centri Firewall)
- Dell SonicWall
- F5
- Intel Security (McAfee)
- Netscreen (Juniper Networks)
- Netasq et Arkoon
- Barracuda Networks
- Huawei
- WatchGuard, Sophos, Stormshield, AhnLab, Sangfor

Figure 1. Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls)

Source: Gartner (September 2018)

Gartner

https://www.gartner.com/reviews/market/network-firewalls

Les Firewalls

- Netfilter / Iptables
  - Netfilter un Firewall au niveau noyau Linux
    - Les paquets sont traité au niveau du noyau par des modules intégrés au noyau (Kernel space).
    - Le noyau prévoit des points d’accroches « hooks » dans le parcours des paquets dans la pile protocolaire.
    - Netfilter est la plateforme qui gère ces hooks en offrant la possibilité à des modules d’enregistrer des fonctions de traitements supplémentaires sur les paquets et de faire retourner les résultats sous formes d’actions spécifiques.
    - Un hook ne renseigne pas sur la manière dont le paquet doit être manipulé, mais juste l’endroit où ce dernier sera traité.

Netfilter / Iptables

- Netfilter est le module du noyau Linux implémentant un pare-feu (filtrage + manipulation paquets)
  - Filtrage niveau 2 : interface, @MAC
  - Filtrage niveau 3 : @source, @dest, ToS (Type of Service), TTL, protocole
  - Filtrage niveau 4 : ports, flags TCP
  - Filtrage suivant taux d'arrivée
- Netfilter permet:
  - Rejet paquet (en informant émetteur)
  - Destruction paquet (sans informer émetteur)
  - Réécriture paquet (@IP, ports, TTL …)
  - Notification dans journal
  - Acceptation et traitement dans espace utilisateur
  - Comportement de netfilter est défini par des règles appartenant à l'une des 3 trois tables (mangle, nat, filter)

Les Firewalls

- Netfilter / Iptables

- iptables est un outil de traitement de paquets (ip v4) conçu sur la plateforme Netfilter
  - ***ip6tables*** l'outil de traitement du protocole ipv6
  - ***arptables*** l'outil dédié au protocole arp « trois hooks seulement »
  - Fonctionnent au niveau de l'espace utilisateur (user-space).
  - N'enregistrent pas directement des fonctions dans les hooks de Netfilter (situé au niveau du noyau).
  - Utilisent un système de tables pour gérer des règles de filtrage dans ces tables.
  - iptables utilise essentiellement Trois tables:
    - La table MANGLE
    - La table NAT
    - La table FILTER

Netfilter / Iptables

Chaque table regroupe ensemble de règles avec même utilisation

- **Table FILTER** :règles pour filtrage des paquets (acceptation, destruction, rejet ...)
- **Table NAT** : Nat : règles permettant les translations d'adresses
- **Table MANGLE** : règles modifiant des paquets (modification TTL, application QoS, ...) .

Table	Description	Chaînes principales	Exemple d'action
FILTER	Filtrage standard des paquets réseau	INPUT, OUTPUT, FORWARD	ACCEPT, DROP, REJECT
NAT	Traduction d'adresses réseau (NAT)	PREROUTING, POSTROUTING, OUTPUT	SNAT, DNAT, MASQUERADE
MANGLE	Modification des paquets	PREROUTING, OUTPUT, FORWARD, POSTROUTING	MARK, TOS, CONNMARK

Les Firewalls:

- Netfilter / Iptables
  - Iptables:
    - Iptables est l'outil en ligne de commandes qui permet d'écrire des règles pour Netfilter.
    - Format d'une règle dans iptables:

-t filter -A INPUT –p tcp -s 192.168.10.2 ––sport 1024 --dport 21 --syn -j ACCEPT

Chaque règle est composée – d'une chaîne – de conditions – de cibles

Netfilter / Iptables

- Chaînes définissent des points traversés par les paquets lors du processus de filtrage
  - INPUT : paquets entrant à destination de la machine locale
  - OUTPUT : paquets sortant émis par machine local
  - FORWARD : paquets traversant la machine par une interface et sortant par une autre
  - PREROUTING : paquets reçu du réseau
- DNAT : modification @destination

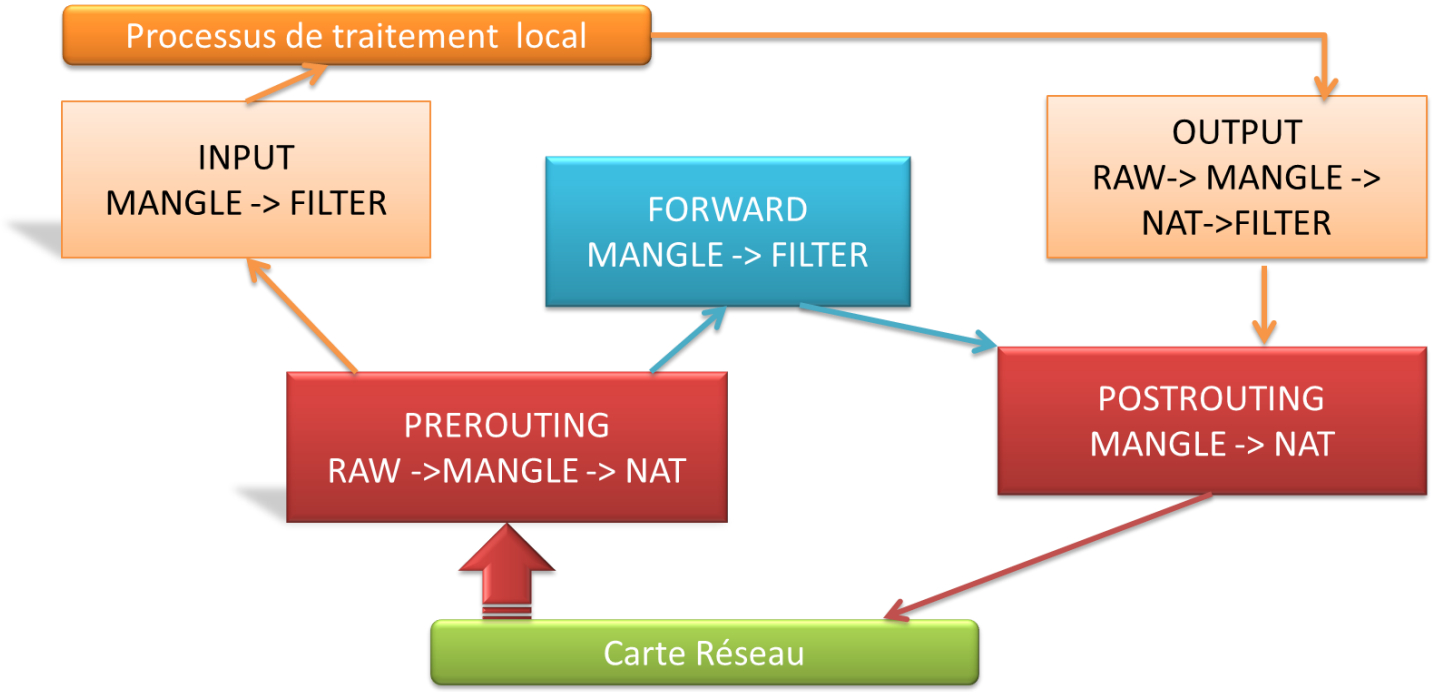
– POSTROUTING : paquets émis sur le réseau après décision de routage

- SNAT : modification @source

Autre chaîne utilisateur : possibilité de créer sa propre chaîne dans une table

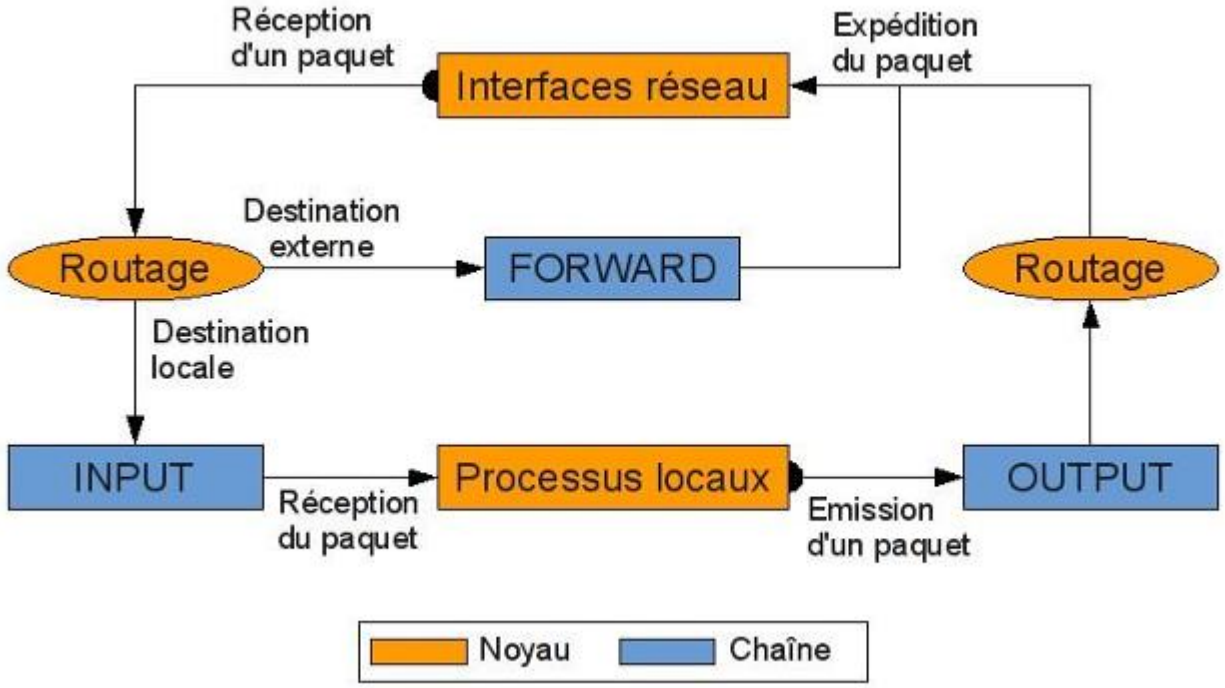
Les Firewalls

- Netfilter / Iptables
  - Iptables:



Netfilter / Iptables

- Schéma de fonctionnement de la table filter de Netfilter



- Une cible spécifie l'action à appliquer au paquet
  – 2 types de cibles : terminales ou non-terminales
- Cibles terminales
  – ACCEPT : acceptation du paquet
  – DROP : destruction du paquet (silencieusement, source non avertie)
  – REJECT : rejet du paquet et envoie message à l'expéditeur (avec code ICMP ou TCP)
  – SNAT : translation adresse source
  – MIRROR : renvoie à l'envoyeur
- **Cibles non-terminales**
- MARK : marquage paquet pour action ultérieure
- LOG : ajout entrée dans le journal
- QUEUE : traitement paquet dans espace utilisateur

Netfilter : politiques

- Politique par défaut pour chaque chaîne
  - Utilisation politique par défaut si aucune règle applicable
- Politiques possibles
  - ACCEPT : acceptation du paquet
  - DROP : rejet silencieux du paquet
- Conseillé d'utiliser DROP pour politique par défaut
- Fermer tous les ports
- Ouvrir uniquement ports nécessaires

Exemple

- Réinitialiser les règles existantes
- `iptables -F`
- `iptables -X`
- `iptables -t nat -F`
- `iptables -t nat -X`
- Activer le forwarding (si nécessaire)
- `echo 1 > /proc/sys/net/ipv4/ip_forward`
- `# Définir les politiques par défaut`
- `iptables -P INPUT DROP`
- `iptables -P OUTPUT DROP`
- `iptables -P FORWARD DROP`

Exemples de règles iptables

- Interdire un paquet s'il ne provient pas de localhost

```
iptables -A INPUT ! -s 127.0.0.1 -j DROP
```

- Politique par défaut (rejet total et silencieux) :

```
iptables -F INPUT && iptables  -P INPUT DROP
```

- Interdire le protocole ICMP à destination de localhost

```
iptables -A INPUT -d 127.0.0.1 -p icmp -j DROP
```

- Interdire toute tentative d'initialisation de connexion TCP provenant de eth0

```
iptables -A INPUT -i eth0 -p tcp --syn -j DROP
```

Exemples de règles iptables

:

```
iptables - A INPUT - p tcp - m tcp - s 10.1.1.0/24 -- dport 22 - j ACCEPT
```

- Suppression règle n°1 chaîne INPUT :
- `iptables - D INPUT 1`
- Acceptation connexions UDP sur port 53 (DNS) ne venant pas de 10.1.1.23 :

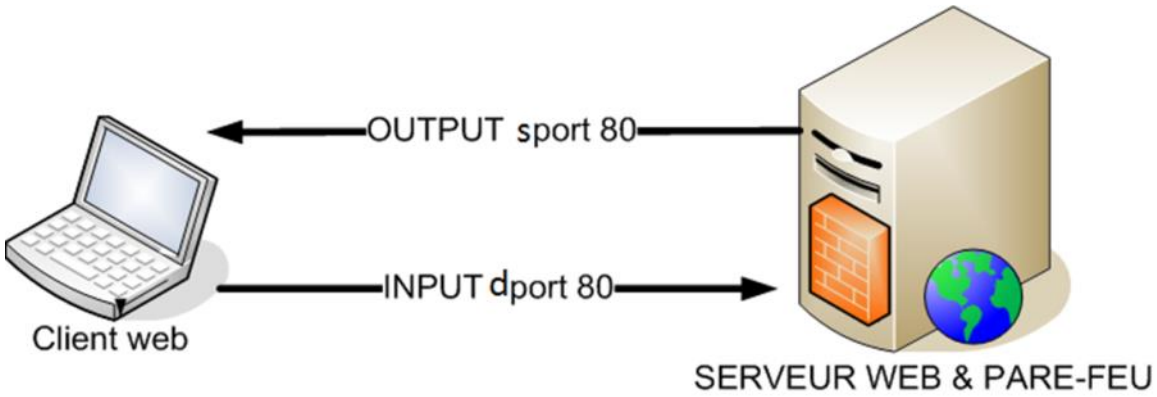
```
iptables  -A INPUT - p udp - m udp - s ! 10.1.1.23 -- dport 53 - j ACCEPT
```

- Acceptation connexions TCP vers port 3306 (MySQL) uniquement via interface loopback (local)
- `iptables - A INPUT - p tcp - m tcp - i lo -- dport 3306 - j ACCEPT`
- le module multiport permet de 'matcher' plusieurs ports en une règle
- `iptables  -A INPUT - m multiport - p tcp - s 10.1.1.1 -- dports smtp,imap,pop3 - j ACCEPT`
- Enregistrement dans journal système (syslog) connexion extérieure sur serveur MySQL
- `iptables  -A INPUT - p tcp - m tcp ! - i lo  --dport 3306  -j LOG --logprefix "MSG : "`

Exemples de règles iptables

Exemple Filtrage Web

- Autoriser un client à se connecter sur un serveur web équipé d'un pare-feu.

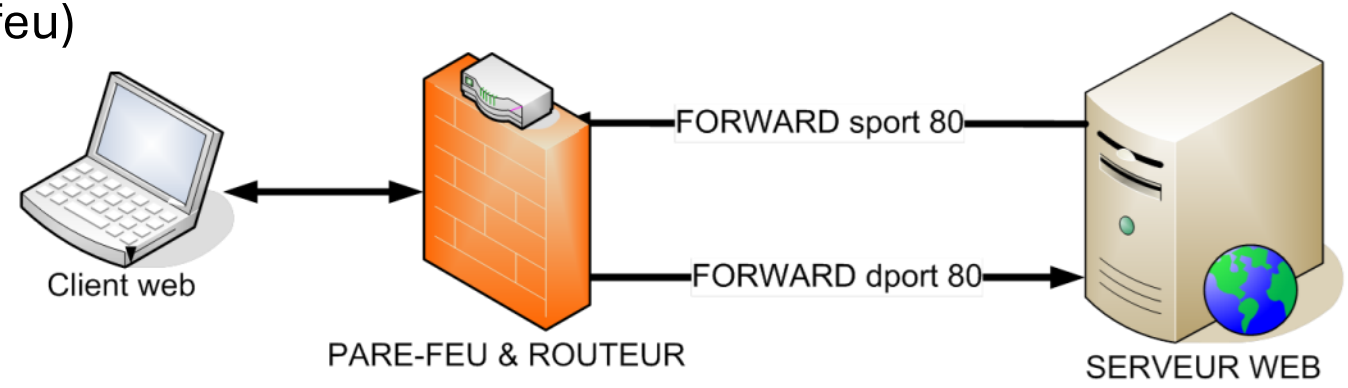



```
iptables -A INPUT -p tcp --sport 1024:65535 --dport 80 -m state --state
NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -p tcp --sport 80 --dport 1024:65535 -m state --state
ESTABLISHED -j ACCEPT
```

Les Firewalls

- Netfilter / Iptables
  - Iptables: Exemple Filtrage Web
    - Autoriser un client à se connecter sur un serveur web via un routeur filtrant (équipé d'un pare-feu)



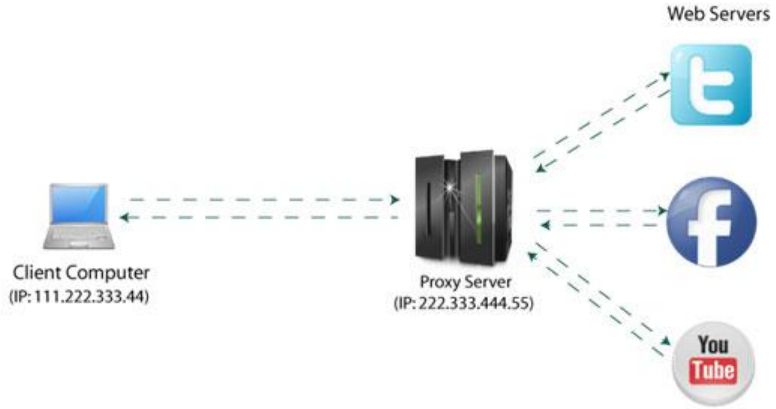

```
iptables -A FORWARD -p tcp --sport 1024:65535 --dport 80 -m state --state NEW,ESTABLISHED
-j ACCEPT
iptables -A FORWARD -p tcp --sport 80 --dport 1024:65535 -m state --state ESTABLISHED -j
ACCEPT
```

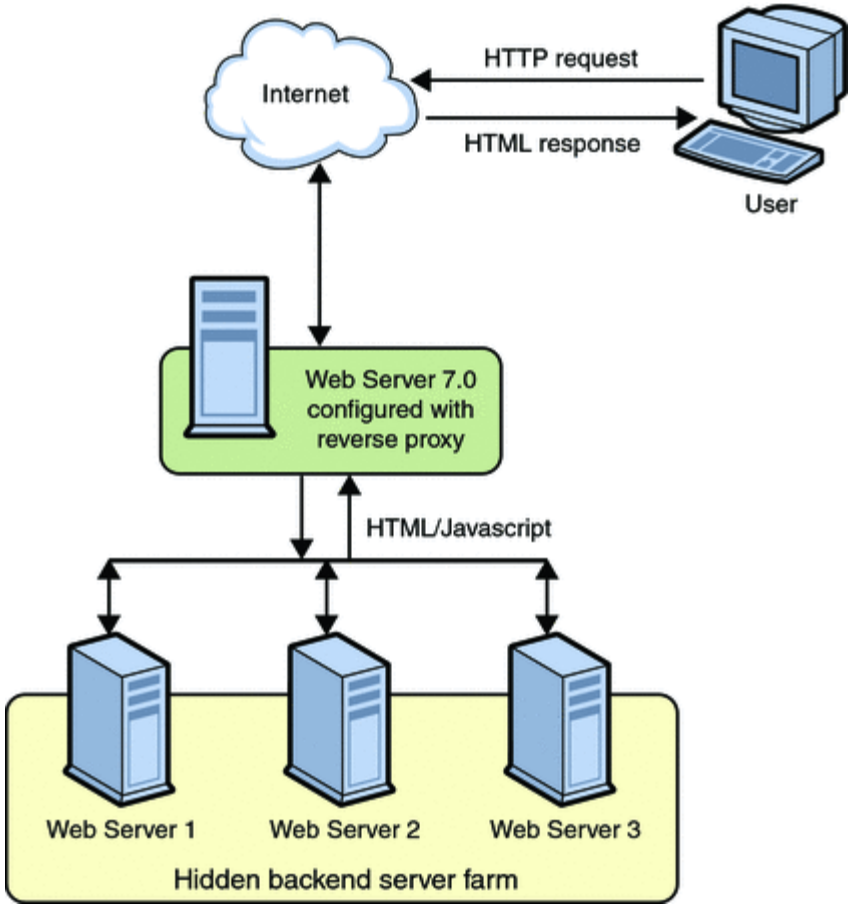
Relais applicatif : Proxy et Reverse proxy

- Les proxy sont des relais applicatifs dans le sens réseau interne vers le réseau externe
  - On les appelle également des ALG (Application Level Gateway)
  - Leur but est de protéger l'accès des clients internes vers des serveurs externes
- Reverse proxy (sens inverse de proxy)
  - On protège les serveurs internes des accès des clients externes

Relais applicatif : Proxy et Reverse proxy

- Proxy et reverse proxy





Explorer le marche

Relais applicatif : Proxy et Reverse proxy

- Free

Free proxy lists France (FR). French proxy servers.

Servers per page: 30 | ANM: All | SSL: All | Port: All | Sorted by: Date

Pages 0 1 Next page | 229 proxies | Permanent link to this page: http://spys.ru/free-proxy-list/FR/

Proxy address:port	Proxy type	Anonymity*	Country (city)	Hostname	Latency**	Speed***	Uptime	Check date (GMT+04)
1 163.172.39.180:3128	HTTP (Squid)	NOA	France	anguita.nom.es	4.555		79% (31) -	29-nov-2016 22:42 (20 minutes ago)
2 185.35.64.64:1994	HTTPS (Squid)	NOA	France (Paris)	host64-64-35-185.static.arubacloud.fr	3.194		84% (21) +	29-nov-2016 21:34 (1 hours ago)
3 46.105.58.9:443	HTTP	HIA	France	ip9.ip-46-105-58.eu	6.249		33% (2) +	29-nov-2016 21:31 (1 hours ago)
4 46.105.214.133:3128	HTTP (Squid)	NOA	France	46.105.214.133	20.905		59% (353) +	29-nov-2016 20:57 (2 hours ago)
5 213.32.58.122:8080	HTTPS	ANM	France	ip122.ip-213-32-58.eu	9.611		61% (27) +	29-nov-2016 20:17 (2 hours ago)
6 85.31.205.178:80	HTTP	HIA	France (Suresnes)	qosmail.isidev.com	9.083		57% (4) -	29-nov-2016 19:28 (3 hours ago)
7 89.38.148.172:3128	HTTPS (Squid)	NOA	France (Paris)	host172-148-38-89.static.arubacloud.fr	2.484		93% (26) +	29-nov-2016 19:25 (3 hours ago)
8 89.38.150.99:3128	HTTPS (Squid)	NOA	France (Paris)	host99-150-38-89.static.arubacloud.fr	3.357		64% (7) +	29-nov-2016 17:50 (5 hours ago)
9 37.187.142.151:3128	HTTP (Squid)	NOA	France	ns3012630.ip-37-187-142.eu	3.139		75% (3) -	29-nov-2016 17:49 (5 hours ago)
10 89.36.215.46:3128	HTTPS (Squid)	NOA	France (Paris)	host46-215-36-89.serverdedicati.aruba.it	2.127		100% (7) +	29-nov-2016 17:25 (5 hours ago)
11 87.98.147.195:3128	HTTP (Squid)	NOA	France	ip195.ip-87-98-147.eu	0.039		79% (132) +	29-nov-2016 17:08 (5 hours ago)
12 83.206.37.227:80	HTTP	HIA	France	imc002.infomedia.fr	7.805		80% (4) +	29-nov-2016 17:00 (6 hours ago)
13 94.177.240.183:8080	HTTP (Squid)	NOA	France (Paris)	host183-240-177-94.static.arubacloud.fr	0.414		100% (3) +	29-nov-2016 16:47 (6 hours ago)
14 51.254.132.238:80	HTTP	HIA	France	238.ip-51-254-132.eu	6.748		51% (453) -	29-nov-2016 15:27 (7 hours ago)
15 163.172.181.225:80	HTTPS (Squid)	NOA	France	225-181-172-163.rev.cloud.scaleway.com	4.534		96% (51) +	29-nov-2016 15:23 (7 hours ago)
16 37.59.37.41:3128	HTTP (Squid)	NOA	France	ns398234.ip-37-59-37.eu	7.952		87% (100) +	29-nov-2016 15:20 (7 hours ago)
17 89.38.149.66:3128	HTTPS (Squid)	NOA	France (Paris)	host66-149-38-89.static.arubacloud.fr	2.107		69% (41) +	29-nov-2016 15:15 (7 hours ago)
18 176.31.175.213:4444	HTTP	NOA	France	thp004.troglohost.com	0.041		29% (2)	29-nov-2016 15:11 (7 hours ago)
19 5.135.203.168:3128	HTTP (Squid)	NOA	France !!!	votre-compte-01.tk	1.039		100% (4) +	29-nov-2016 15:08 (7 hours ago)
20 94.177.241.76:3128	HTTPS (Squid)	NOA	France (Paris)	host76-241-177-94.static.arubacloud.fr	1.676		67% (20) +	29-nov-2016 15:08 (7 hours ago)
21 5.135.35.183:3128	HTTPS (Squid)	NOA	France !!!	5.135.35.183	0.812		54% (49) +	29-nov-2016 15:08 (7 hours ago)
22 94.177.243.181:1453	HTTP (Squid)	NOA	France (Paris)	host181-243-177-94.static.arubacloud.fr	0.18		new	29-nov-2016 15:08 (7 hours ago)
23 176.31.107.113:4444	HTTP	NOA	France	ns392845.ip-176-31-107.eu	0.281		82% (9) +	29-nov-2016 15:04 (7 hours ago)
24 89.40.115.244:3128	HTTP	ANM	France (Paris)	host244-115-40-89.static.arubacloud.fr	0.158		42% (38) -	29-nov-2016 14:59 (8 hours ago)
25 195.154.86.167:8118	HTTPS	HIA	France	cabri.xiasma.fr	0.945		new	29-nov-2016 14:57 (8 hours ago)
26 51.255.74.112:3128	HTTP (Squid)	NOA	France	ns3045348.ip-51-255-74.eu	1.044		100% (6) +	29-nov-2016 14:57 (8 hours ago)
27 151.80.135.147:3128	HTTP (Squid)	NOA	France (Roubaix)	147.ip-151-80-135.eu	4.084		56% (201) +	29-nov-2016 14:56 (8 hours ago)
28 5.135.164.181:3128	HTTPS (Squid)	ANM	France	ns3313718.ip-5-135-164.eu	3.151		92% (69) +	29-nov-2016 14:56 (8 hours ago)
29 92.222.109.54:3128	HTTP (Squid)	ANM	France (Paris)	e35.yes-full.fr	3.24		9% (1)	29-nov-2016 14:53 (8 hours ago)

Relais applicatif : Proxy et Reverse proxy

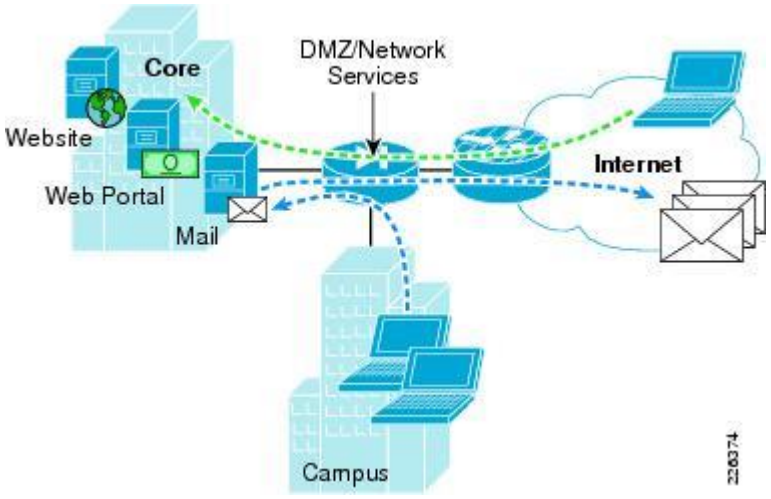
- Avantages
  - Filtrage de contenu (scripts, applets java, ActiveX,…) et sémantique
  - Interface possible avec les antivirus (CVP)
  - Authentification des utilisateurs possible
  - Masque les adresses des machines clientes
  - Processus en espace utilisateur
  - Anonymisation des clients ou des serveurs

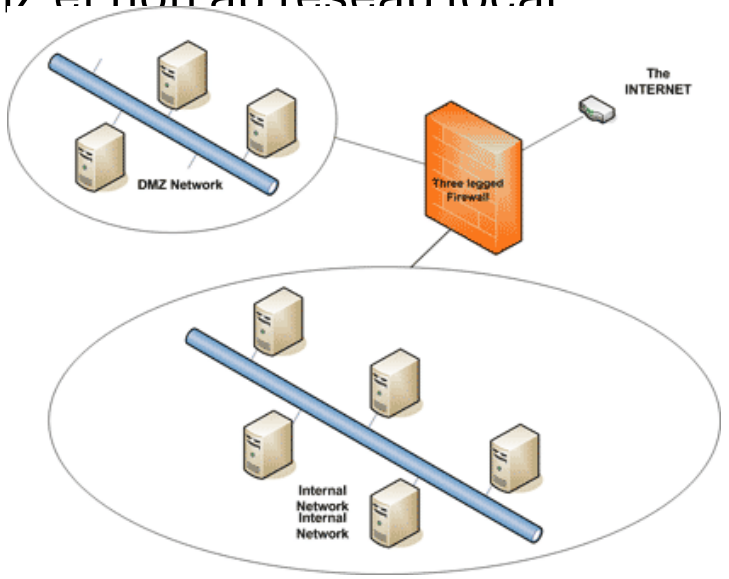
Relais applicatif : Proxy et Reverse proxy

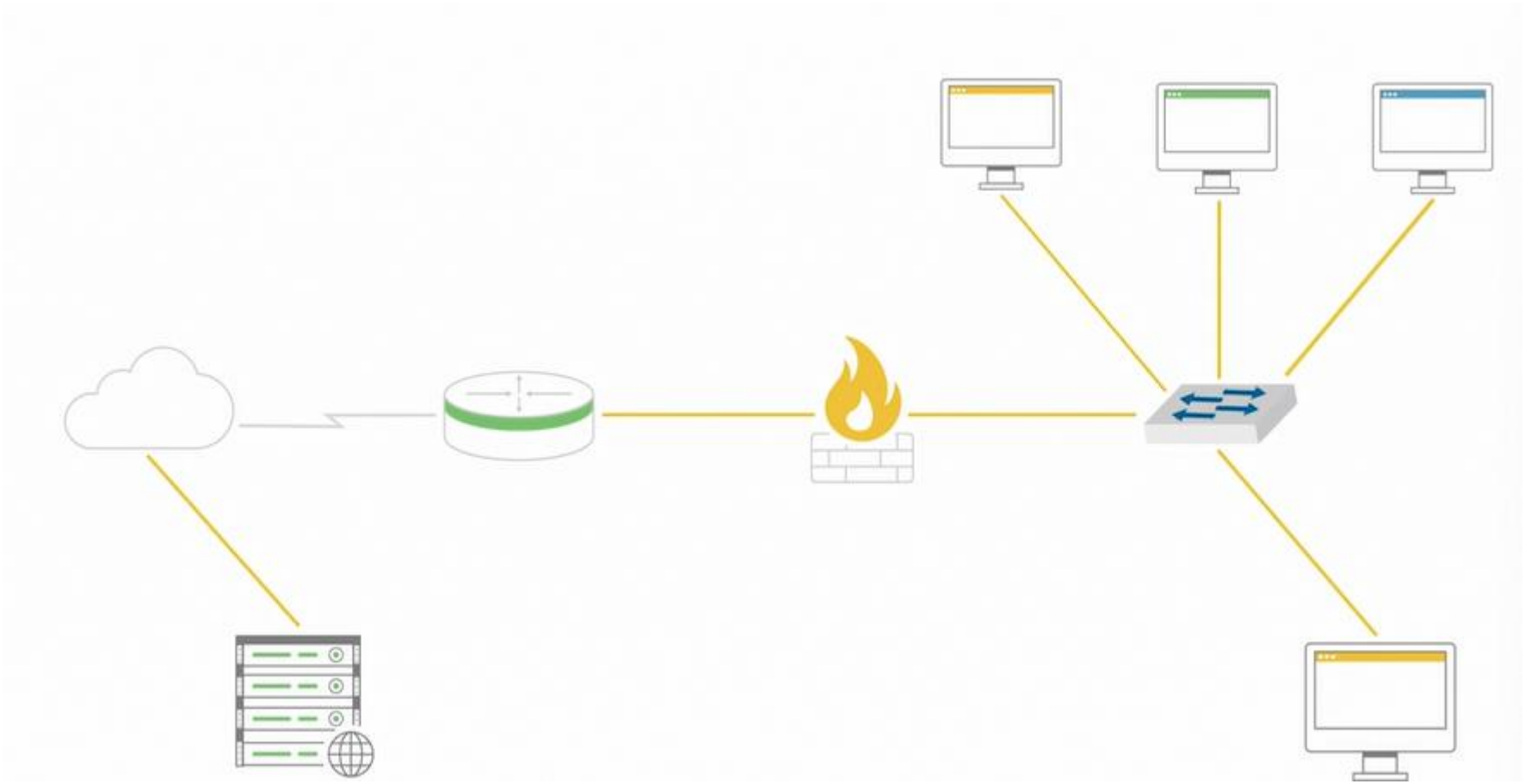
- Problème de finesse du filtrage réalisé par le proxy
  - Difficile de réaliser un filtrage qui ne laisse rien passer, vu le nombre de protocoles de niveau 7
  - Chaque service applicatif nécessite un proxy spécifique -> Connaître les règles protocolaires de chaque protocole filtré
  - Si une application n’est pas supportée par le proxy cela ne peut pas « fonctionner »
- Le filtrage applicatif apporte plus de sécurité que le filtrage de paquet avec état,
  - mais cela se paie en performance.
  - Ce qui exclut l'utilisation d'une technologie 100 % proxy pour les réseaux à gros trafic

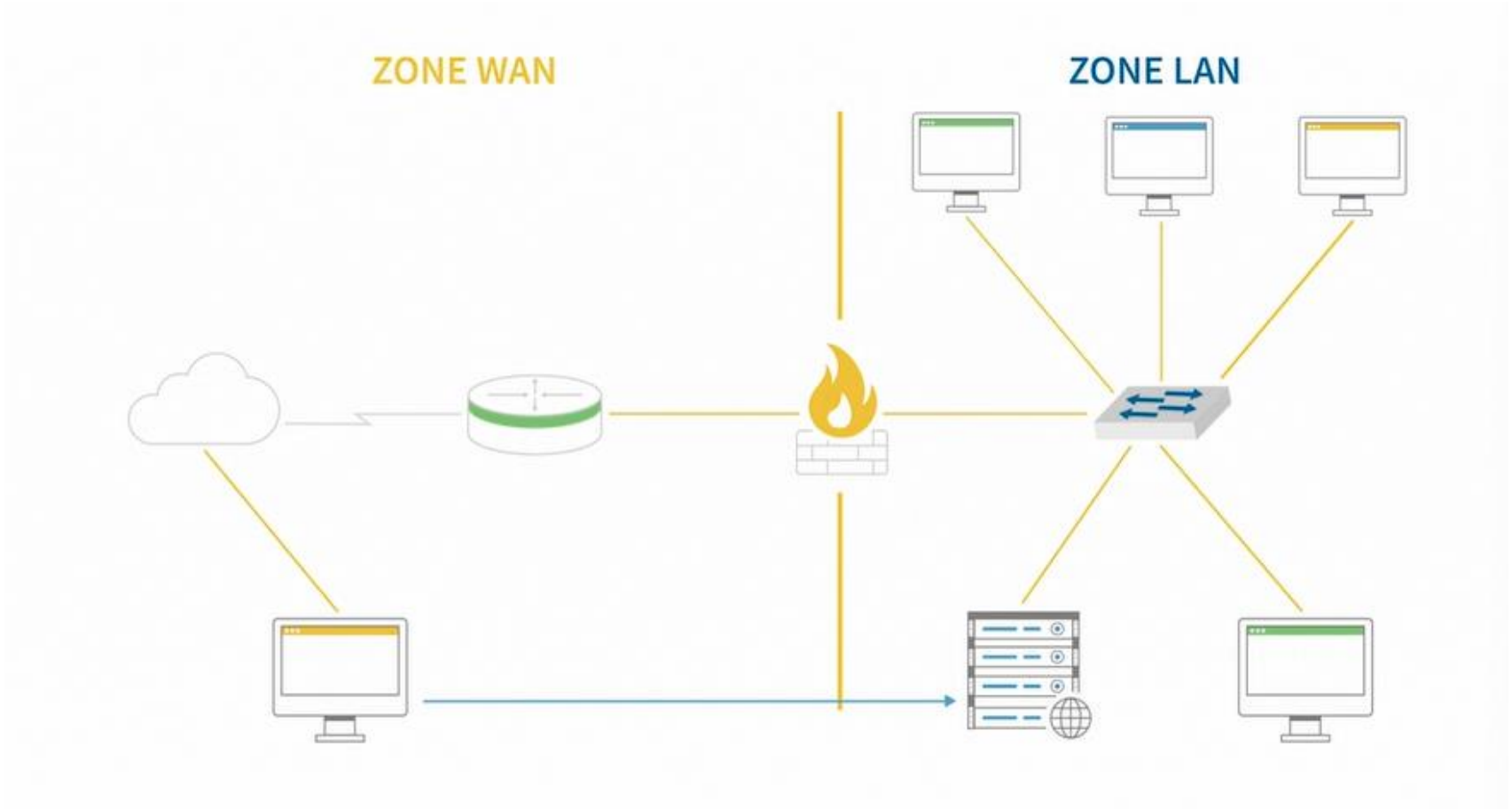
DeMiltarezed Zone : DMZ

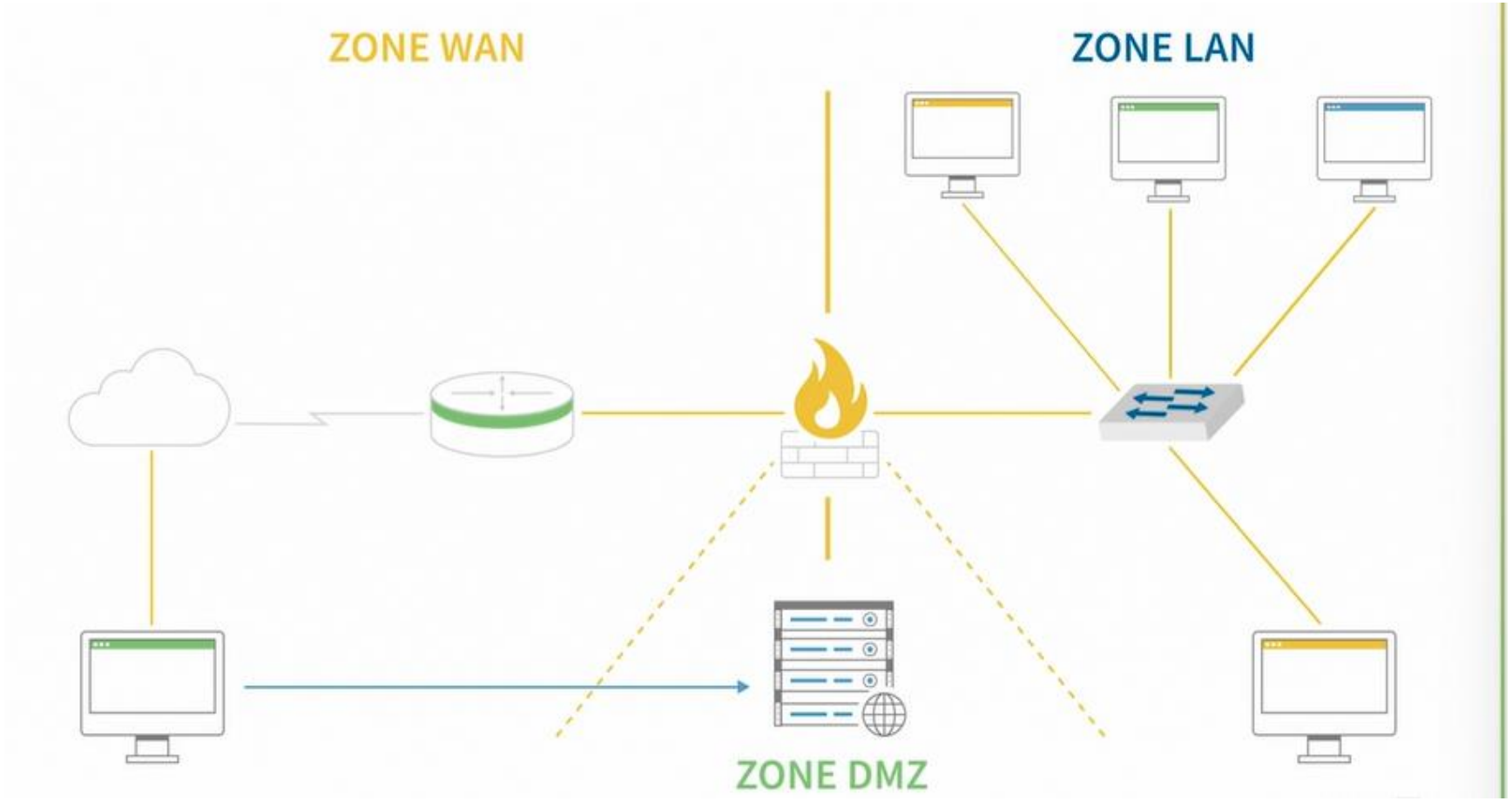
- Objectifs de la DMZ
  - Donner accès à des services tout en protégeant l'accès au réseau Interne
  - Contient les machines étant susceptibles d'être accédées depuis Internet
  - Mise en place d'une zone tampon entre le réseau externe et le réseau Interne
  - En cas de compromission d'un des services dans la DMZ, le pirate n'aura accès qu'aux machines de la DMZ et non au réseau local







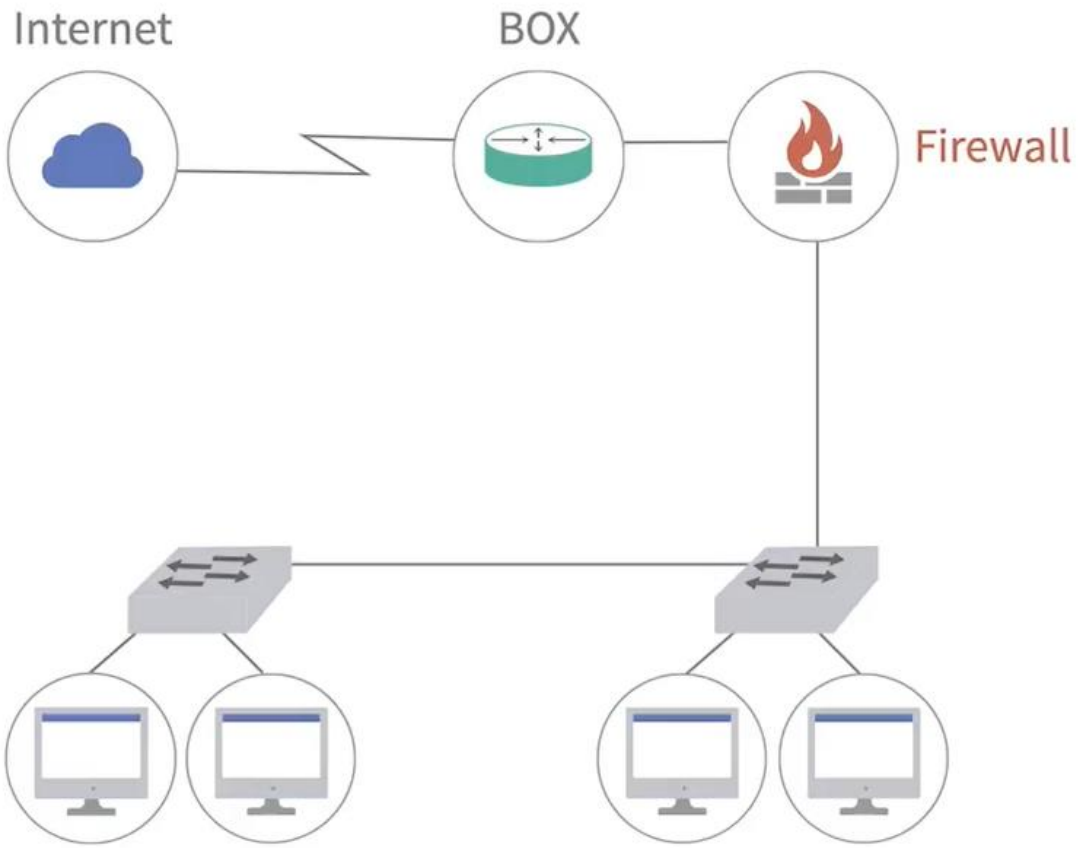

ZONE WAN
ZONE LAN

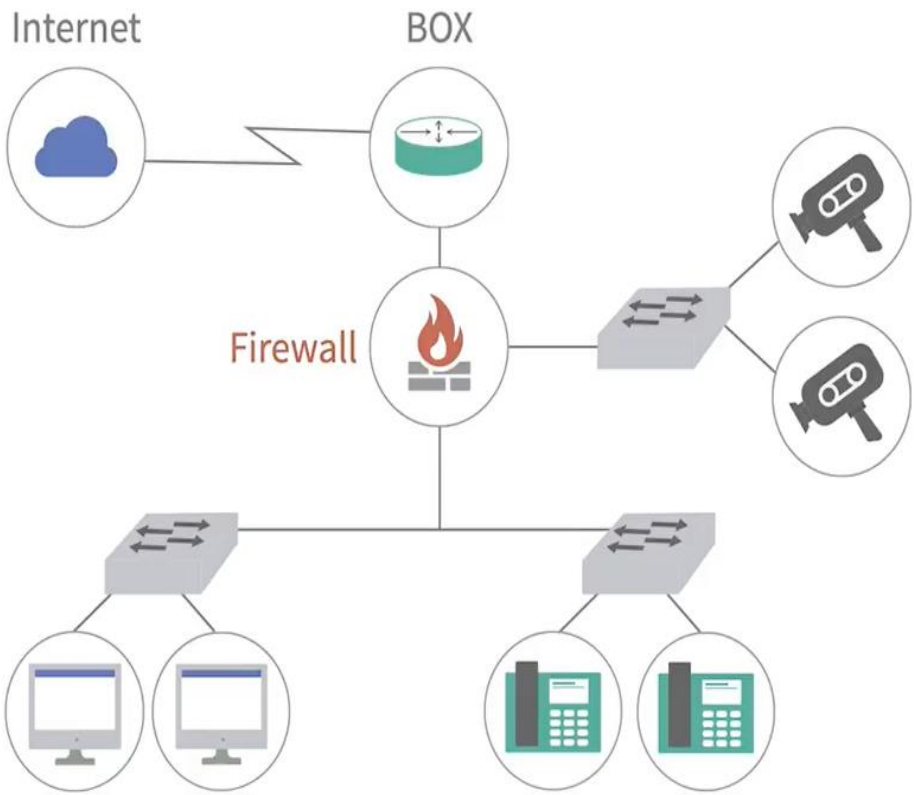

ZONE WAN
ZONE LAN
ZONE DMZ

NGFW vs UTM

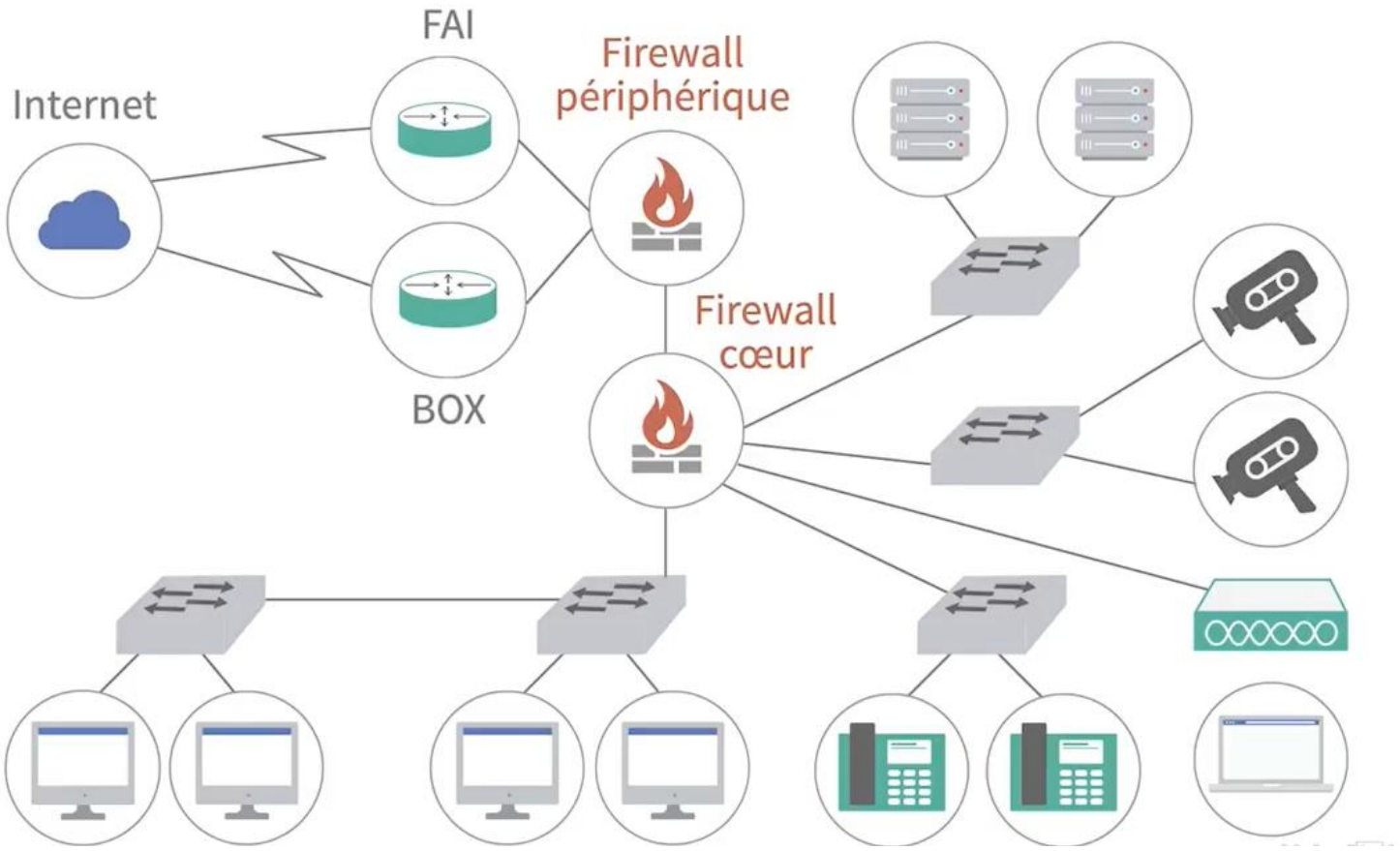
- NGFW reprend les fonctions UTM
- Analyse comportementale avancée du trafic au réseau
- Fonctionnalité
  - Récolte de donné sur le réseau et remplissage de la base de connaissance
  - Création de profils
  - création de profils de traffic en fonction du temps
- Surveillance: en cas d'anomalie alerte, blocage du traffic en corrélation avec profil donnée

Firewall en périphérique





Firewall en périphérique



Firewall en périphérique