



# Les services de sécurité des réseaux

Ramzi Ouafi

Assistant Technologue

ESPRIT

e-mail : [Ramzi.ELOUAFI@esprit.ens.tn](mailto:Ramzi.ELOUAFI@esprit.ens.tn)

# Plan du chapitre

- Rappel : les couches OSI
- Contrôle d'accès
  - Listes d'accès (**ACL**).
  - Translation d'adresses (**NAT**).
  - Le filtrage par Firewall.
- Les moyens cryptographiques.
  - Cryptage/décryptage (chiffrement).
  - Hachage cryptographique.
  - Intégrité et authentification La signature numérique

## 2. Les fonctions de Filtrage

# Contrôle d'accès

- N'autoriser que ce qui est nécessaire
- Interdire par défaut + journaliser les tentatives
- Contrôle d'accès
  - Identification et authentification
  - Filtrage, dans la pile TCP/IP ou par des relais applicatifs
  - Bonne journalisation : tracer et auditer le trafic entre le réseau interne et le réseau externe
  - Faciliter l'administration en regroupant les opérations de surveillance et de contrôle
  - Contrôle des messages entrants (Spamming, virus)

## 2.1. Access lists

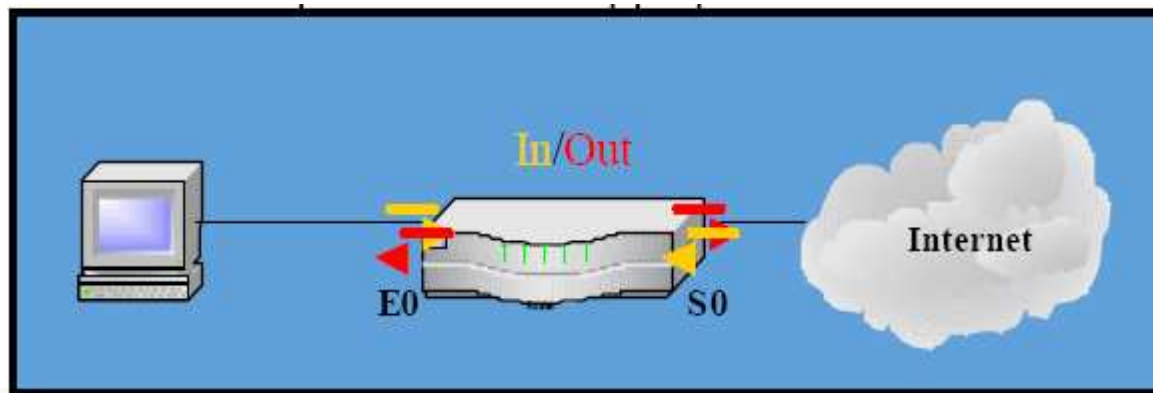
# Les Access-lists

- Utilisent les possibilités de filtrage du routeur pour implémenter la politique de sécurité.
- Principe: filtrage des paquets pour contrôler le trafic depuis l'extérieur (WAN) vers l'intérieur d'un réseau local.
- Critères de filtrage :
  - Direction du trafic : depuis, vers.
  - L'Interface.
  - Le type de protocole : IP, ICMP, TCP, UDP, IPX
  - L'adresse IP source et destination
  - Les ports TCP et UDP source et destination.
- Le paramétrage de l'ACL décide quel hôte ou groupe d'hôtes peut (**permit**) ou ne peut pas (**deny**) transiter par le routeur.



# Création des ACLs

- Les ACLs sont créées puis elles doivent ensuite être affectée à un ou plusieurs ports (ou interfaces).
- Il est possible de faire le contrôle sur un réseau, un sous-réseau, un hôte ou une catégorie d'hôtes.
- Le paramètre In / Out (Inbound-Outbound)
  - Par défaut, ce paramètre est configuré out .
  - La valeur In (vers le routeur) ou Out se place sur l'interface à laquelle on veut appliquer la liste d'accès



# ACL standard ou étendue ?

- Les listes de contrôles standards filtrent l'accès :
  - A partir de l'adresse source uniquement (standards).
- Les listes de contrôle étendues peuvent filtrer l'accès :
  - Selon l'adresse source et l'adresse destination ;
  - Selon les types de protocole de transport (TCP, UDP)
  - Selon le numéro de port (couche application).

Type de liste d'accès	Numéros d'identification
IP Standard Extended	1-99 100-199 Named (Cisco IOS 11.2 and later)
IPX Standard SAP filters	800-899 1000-1099
Apple Talk	600-699



# Règles d'écriture des ACLs

- Par défaut, dès qu'une liste d'accès est créée, elle refuse le passage à tout ce qui n'est pas spécifiquement autorisé.
- De façon implicite (cela n'apparaît pas à la ligne de commande) la liste de contrôle d'accès se termine par l'instruction «**refuse tout**».
- En général, l'administrateur devrait définir des permissions (**permit**) plutôt que des interdictions (**deny**).
- Une seule ACL par direction, par interface et par protocole.
- ACL IP standard (1-99) et étendue (100-199)
- Par défaut, l'ACL s'applique sur la sortie (**out**).



## **2.2. Network Address Translation**

# Le NAT: Network Address Translation

- La NAT: **Network Address Translation**". est décrit dans la [RFC 1631](#), (Mai 1994) mécanisme destiné à faire **correspondre** un réseau entier (ou des réseaux) à une seule ou plusieurs adresses.
- Adresses privées -> adresses publiques:
  - La NAT permet de bénéficier des blocs d'adressage privés décrits dans la [RFC 1918](#). Typiquement, le réseau interne sera paramétré pour utiliser un ou plusieurs des blocs réseau suivants :
    - 10.0.0.0/8 (10.0.0.0 - 10.255.255.255)
    - 172.16.0.0/16(172.16.0.0 - 172.31.0.0)
    - 192.168.0.0/24 (192.168.0.0 - 192.168.255.0)

# NAT & PAT

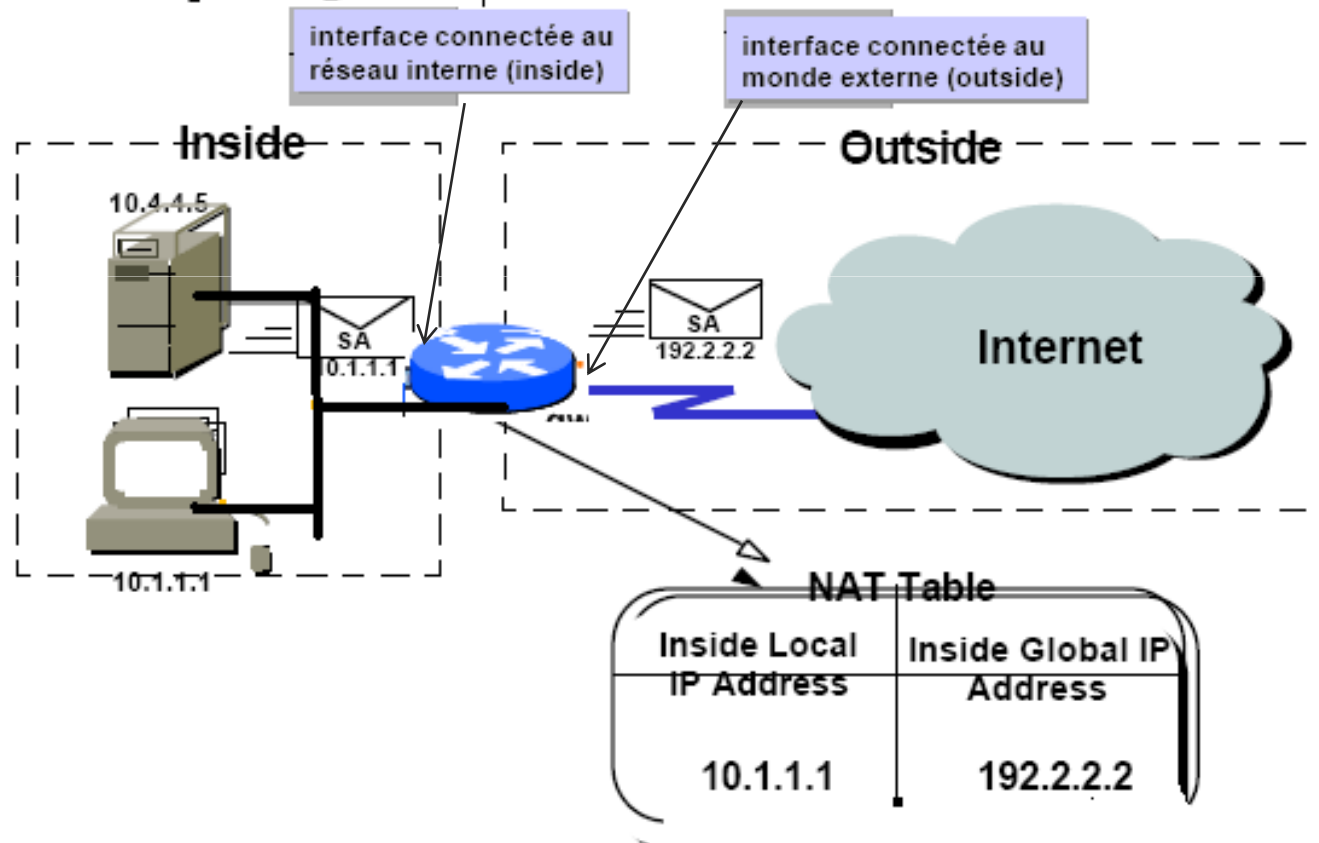
- Translation d'adresses **statique**, correspondance entre 1 @ privée → 1 @ publique (serveurs).
- Translation d'adresses **dynamique**, les @ publiques sont attribuées à la demande (clients)
  - Par rapport à un pool d'adresses n @ privée → m @ publique
  - Par rapport à un pool de ports (Port Address Translation ou **PAT**)
- Triple objectif :
  - Protéger certaines machines
  - Procédé sûr vis à vis de l'extérieur
  - Permet en même temps d'économiser des adresses IP.
- **NAT cache l'identité "réelle" des hosts ou des applications**

## Configuration NAT statique

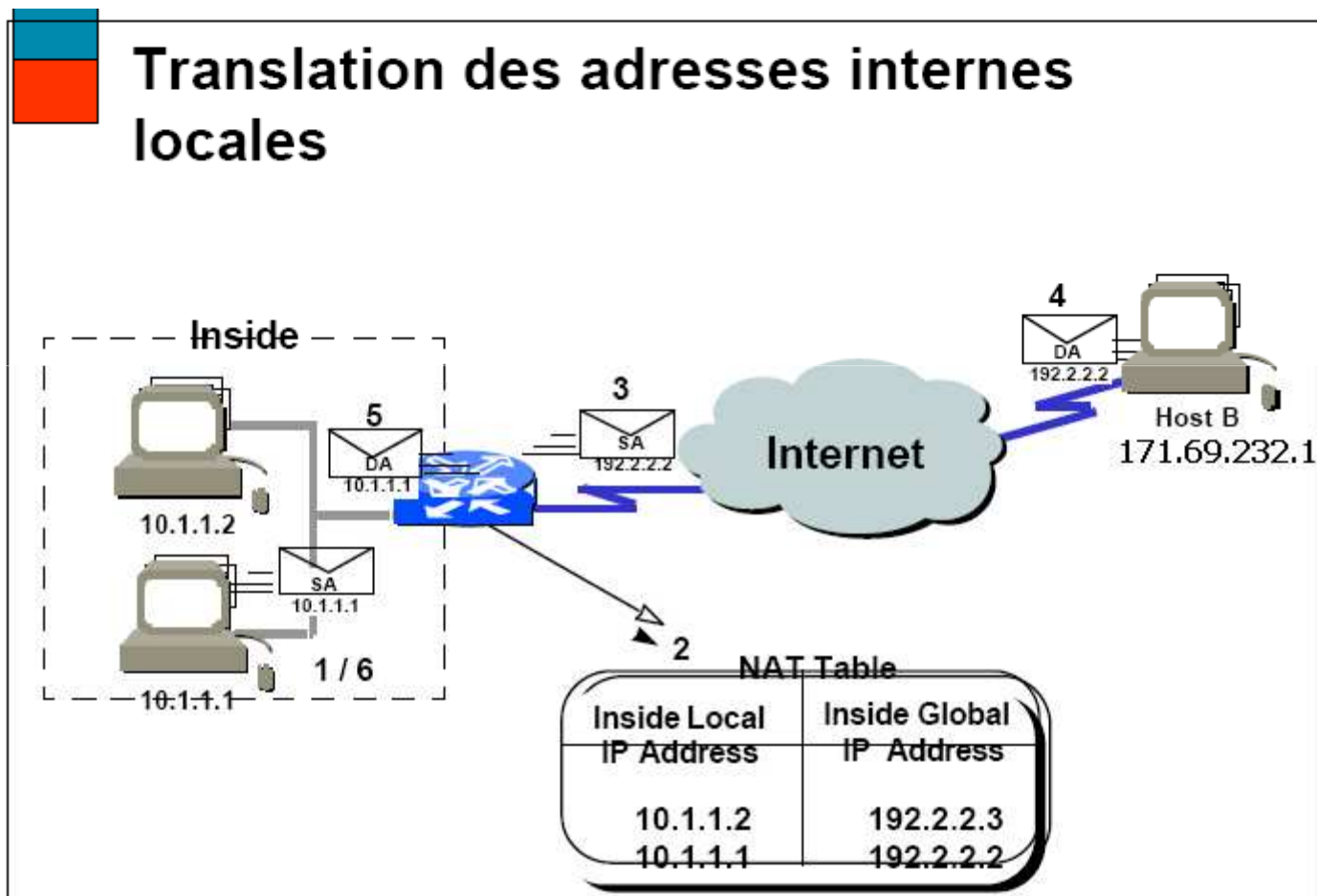
- Définition de l'interface **inside** :
  - Interface interne du routeur
- Définition de l'interface **outside** :
  - Interface externe du routeur
- Définition la translation statique
  - Translater l'@ privée 10.1.1.1 → l'@ publique 193.95.2.2

# NAT statique: exemple

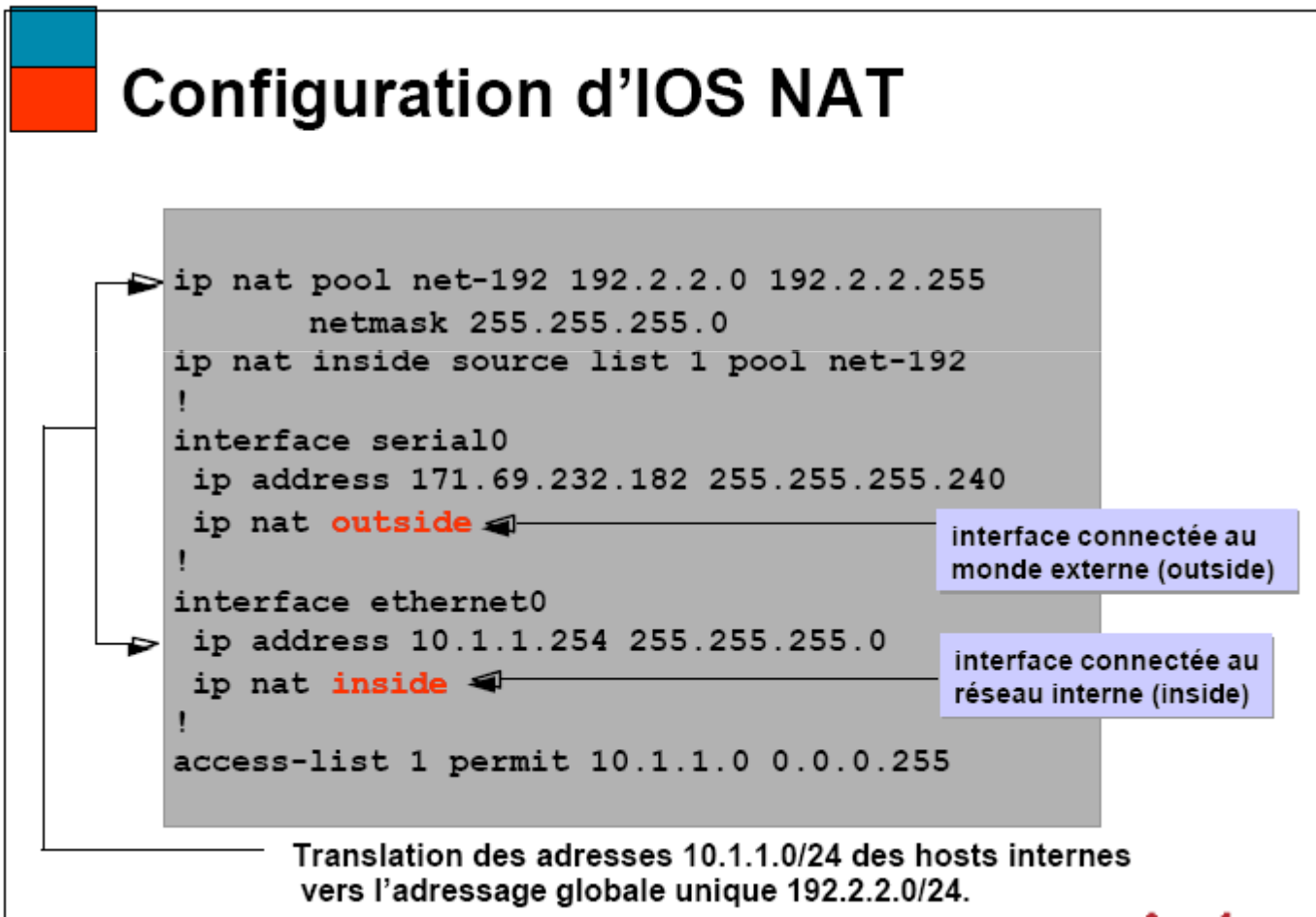
## 1er aperçu de NAT



# NAT dynamique (pool d'adresses)

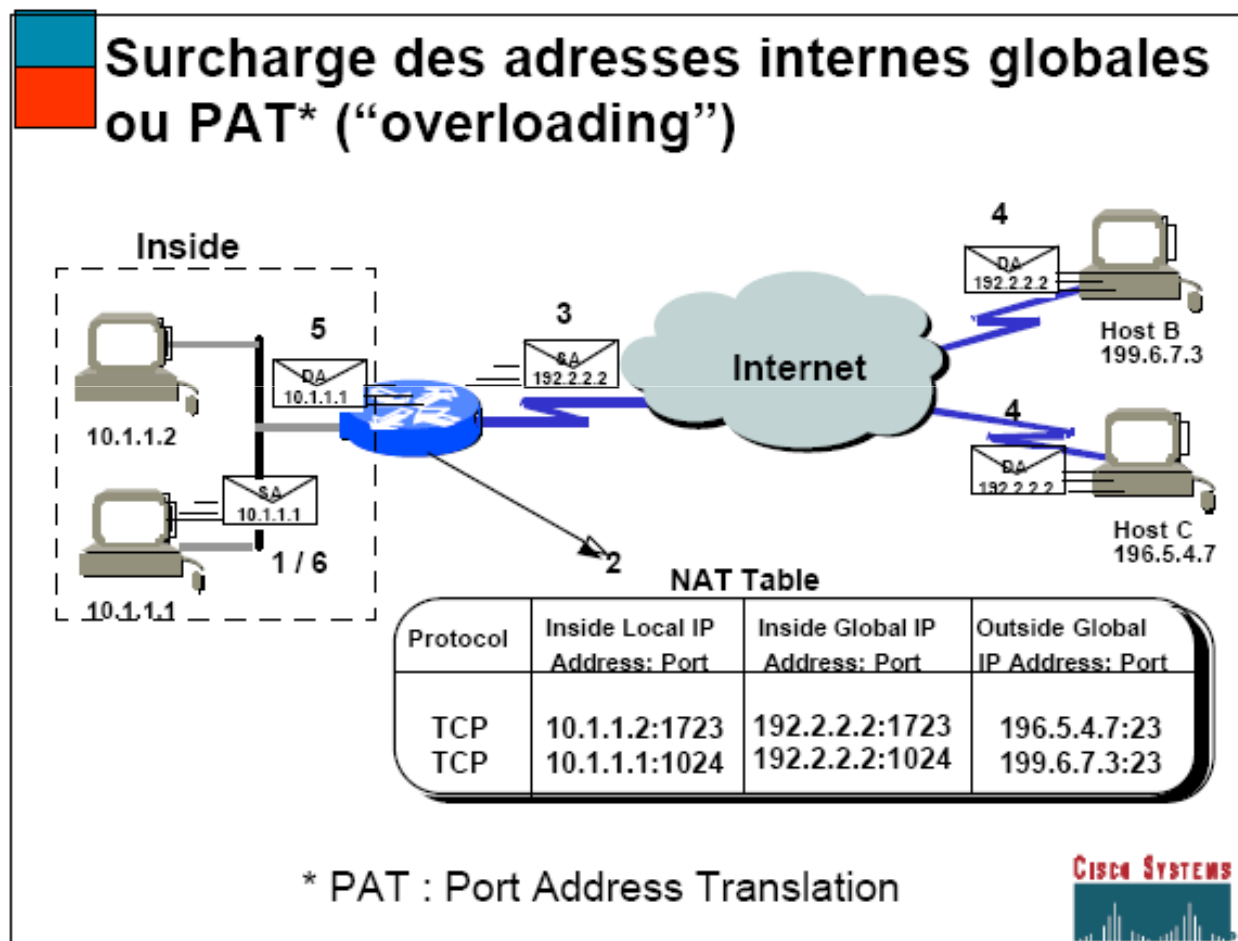


# Configuration NAT dynamique (pool d'adresses)





# PAT avec surcharge (overloading)



# Inconvénients du NAT

## Avantages de la fonction NAT

- Ménage le modèle d'adressage enregistré légalement.
- Augmente la souplesse des connexions vers le réseau public.
- Assure la cohérence des schémas d'adressage du réseau interne.
- Assure la sécurité du réseau.

## Inconvénients de la fonction NAT

- Les performances sont affectées.
- Les fonctionnalités de bout en bout sont affectées.
- La traçabilité IP de bout en bout est perdue.
- La transmission tunnel est plus compliquée.
- L'établissement de connexions TCP peut être perturbé.
- Les architectures doivent être remodelées pour tenir compte des modifications.



## 2.3.FIREWALL

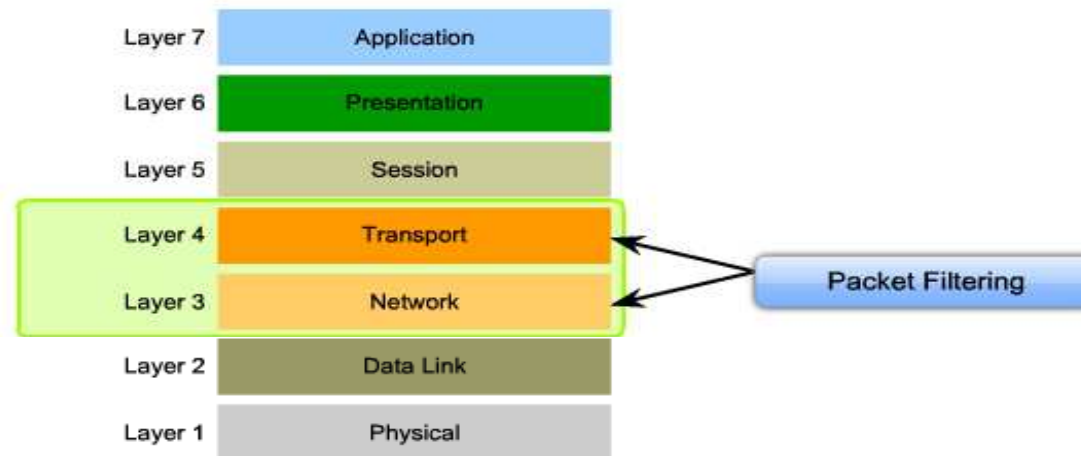
# Firewall

- Un **pare-feu** (appelé aussi **coupe-feu**, **garde-barrière** ou **firewall** en anglais), est un système permettant de constituer un intermédiaire entre le réseau local et un ou plusieurs réseaux externes notamment internet. Comportant au minimum les interfaces réseau suivantes:
  - une interface pour le réseau à protéger (réseau interne) ;
  - une interface pour le réseau externe.
- Le système firewall peut être un système logiciel, reposant parfois sur un matériel réseau dédiés. Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel système pourvu que :
  - La machine soit suffisamment puissante pour traiter le trafic ;
  - Le système soit sécurisé ;
  - Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.
- Dans le cas où le système pare-feu est fourni dans une boîte noire « clé en main », on utilise le terme d'« **appliance** ».

# Le Filtrage simple de paquets

- Un système pare-feu fonctionne sur le principe du filtrage simple de paquets (en anglais « ***stateless packet filtering*** ») ou « **Packet-filtering firewall** »
- Il analyse les en-têtes de chaque **paquet de données** (*datagramme*).
- Typiquement c'est un routeur avec filtrage niveau 3 et parfois niveau 4.
- Ainsi, les paquets de données échangée entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants, systématiquement analysés par le firewall :
  - @ IP source
  - @ IP de la machine réceptrice ;
  - Protocole.
  - N° du port Source.
  - N° du port Destination .

# Le filtrage simple de paquets



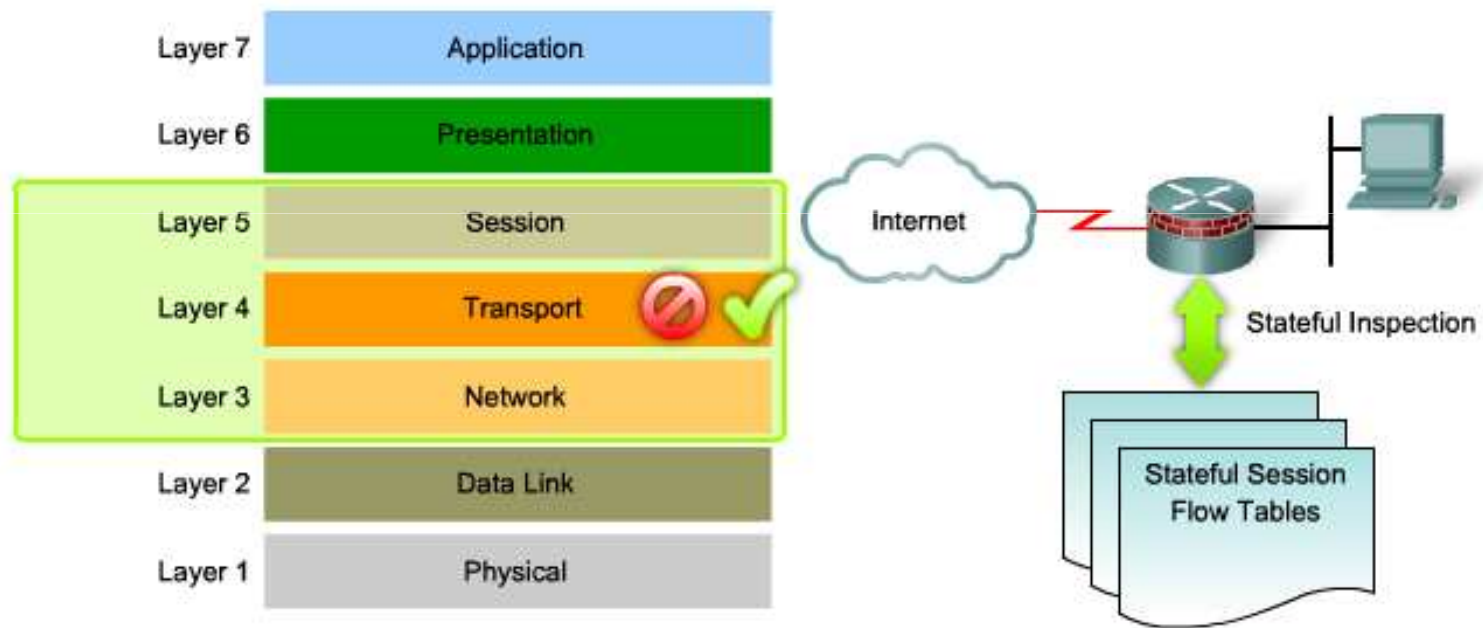
- Le tableau ci-dessous donne des exemples de règles de pare-feu :

Règle	Action	IP source	IP dest	Protocol	Port source	Port dest
1	Accept	192.168.10.20	194.154.192.3	tcp	any	25
2	Accept	any	192.168.10.3	tcp	any	80
3	Accept	192.168.10.0/24	any	tcp	any	80
4	Deny	any	any	any	any	any

# Le filtrage dynamique avec information de session

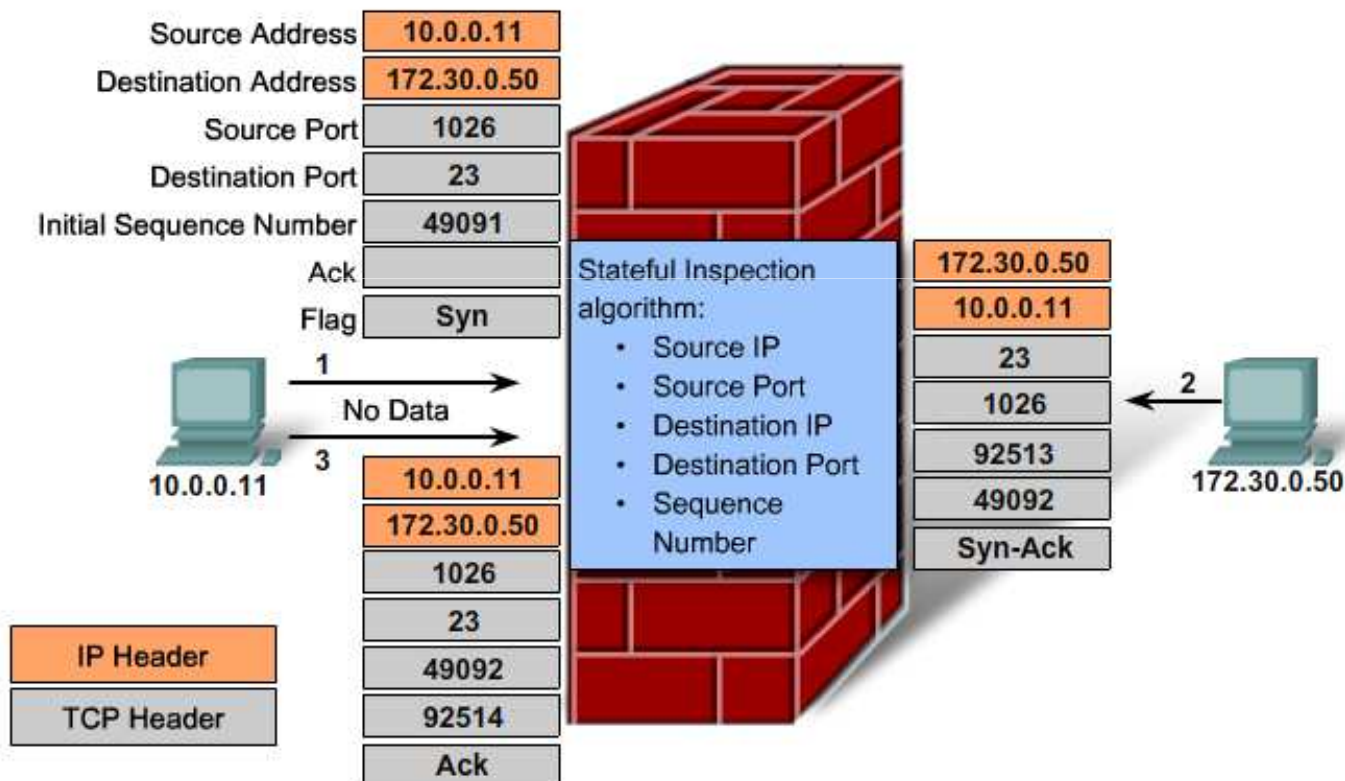
- Le « **stateful inspection** » inventé par **Check Point**.
- Le(**stateful inspection**) est basé en plus de l'inspection des couches 3 et 4 du modèle OSI sur le contrôle de :
  - La connexion est en cours d'initiation
  - Le transfert de données.
  - La connexion est en état de libération.
- Un dispositif pare-feu de type « stateful inspection » est ainsi capable d'assurer un suivi des échanges:
  - Contrôle de l'établissement d'une connexion **TCP (SYN)**
  - Les numéros de séquences TCP (**SEQ**).
  - Connexion FTP qui utilisent des ports dynamiques > **1023** (risques d'être bloqués par le firewall)
  - UDP based applications ( pas de distinction entre une **requête** et une **réponse**)
  - Etc.

# Le filtrage dynamique avec information de session

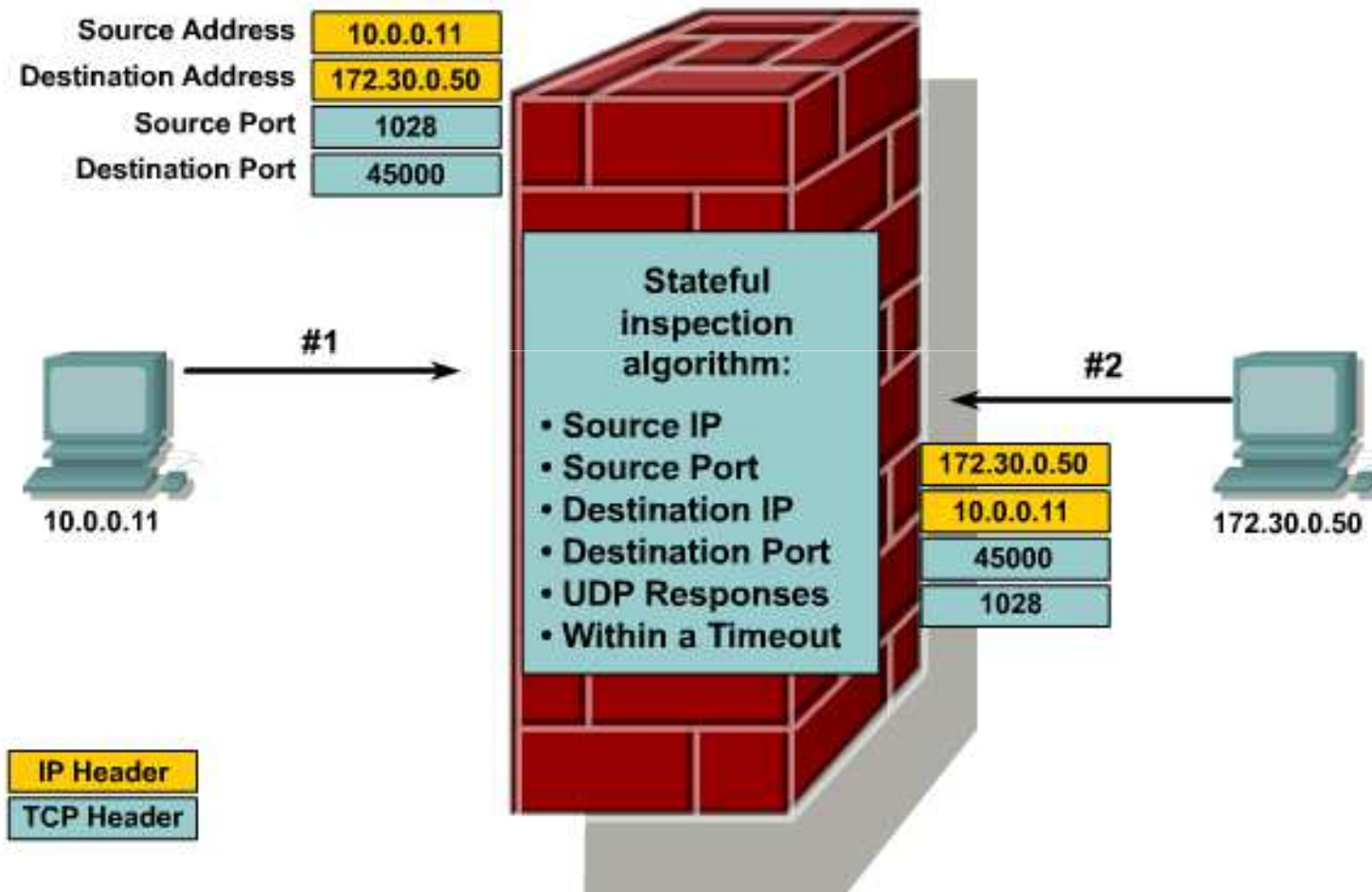




# Le filtrage dynamique avec information de session (TCP)



## Le filtrage dynamique (UDP)



# Le filtrage applicatif ou de contenu d'application

- Si le filtrage dynamique ne protège pas pour autant de l'exploitation des failles applicatives.
  - Pas de contrôle du contenu HTTP.
  - Quelques protocoles ne sont pas **stateful** UDP, ICMP.
  - Ne supporte pas l'authentification des utilisateurs ou des applications.
- Le filtrage applicatif (appelé « passerelle applicative » ou « proxy »), permet de filtrer les communications application par application. Il opère donc au niveau 7 (couche application) du modèle OSI,
  - Filtrer le contenu & détecter les intrusions
  - Limiter l'envoi & la réception de courriers non sollicités (SPAM).
  - Bloquer l'envoi & la réception de certains documents (.exe, multimédias, etc)
  - Empêcher certaines applications (*eMule*, *Kazaa*, *BitTorrent*, *Morpheus*...)
  - Empêcher certains scripts: ActiveX filter, invalid URL, Cookies Filter,
- Il s'agit d'un dispositif performant. En contrepartie, une analyse fine des données applicatives se traduit donc souvent par un ralentissement des communications, chaque paquet devant être finement analysé.
  - Solution: le filtrage niveau 3 et 4 fait par le routeur et décharger au maximum le firewall pour l'inspection applicative

# Récapitulatif des fonctions d'un Firewall(1)

## 1. Contrôle des attaques

- Denial of Service
  - Ping Of Death
  - Syn Flood attack
- Activité suspicieuse
  - Ip spoofing
  - Source routing
  - Port Scanning
  - TCP Hijacking
  - Trace route
  - IP fragmentation

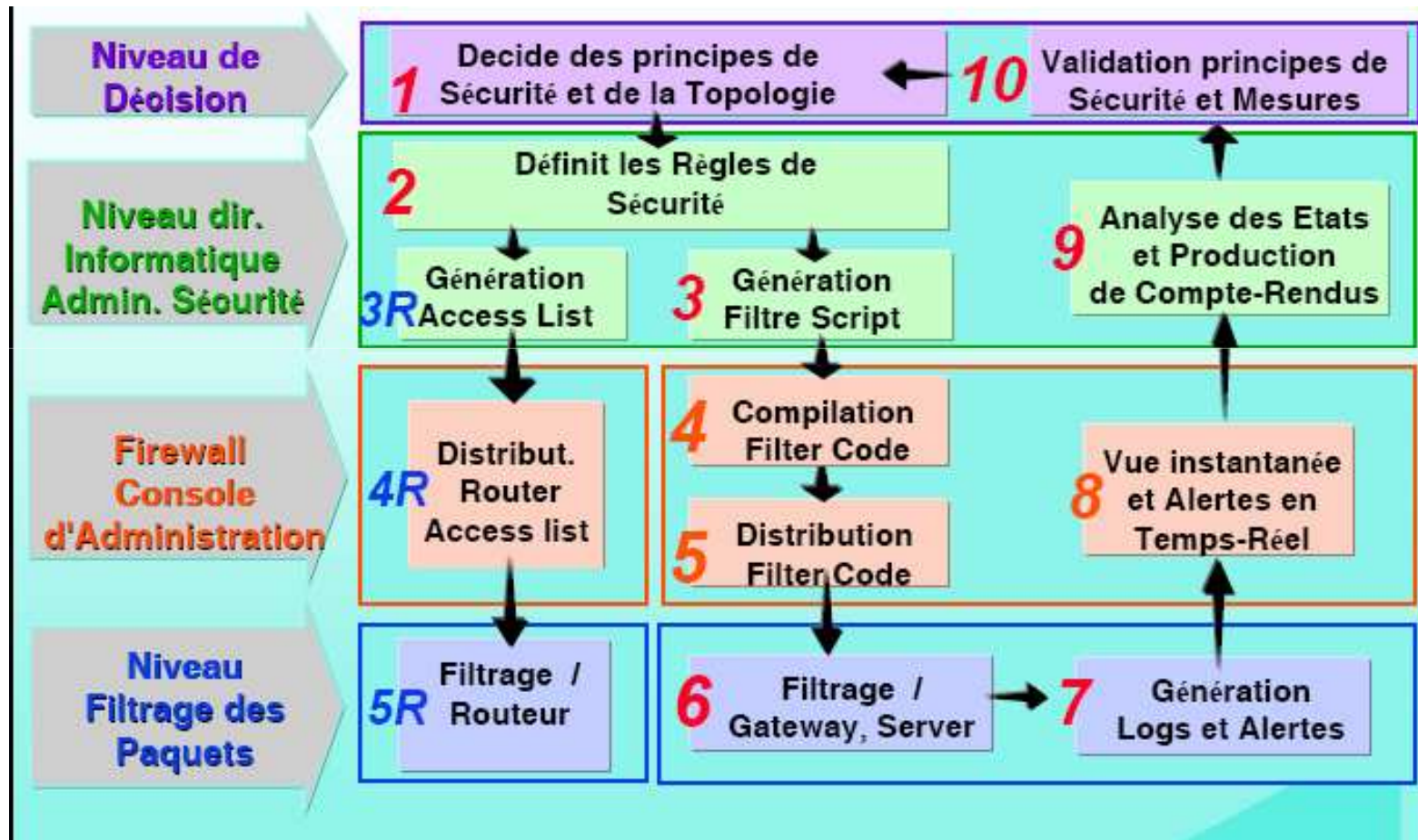
## 2. Analyse des flux de communication

- Filtrage
- Analyse de contenu
- Contrôle des communications hostiles

## 3. Autres fonctions

- Translation d'adresses
- Authentification
- VPN
- Translation d'adresse
- Sécurisation du contenu
- Audit
- Contrôle des connections

# Récapitulatif des fonctions d'un Firewall(2)

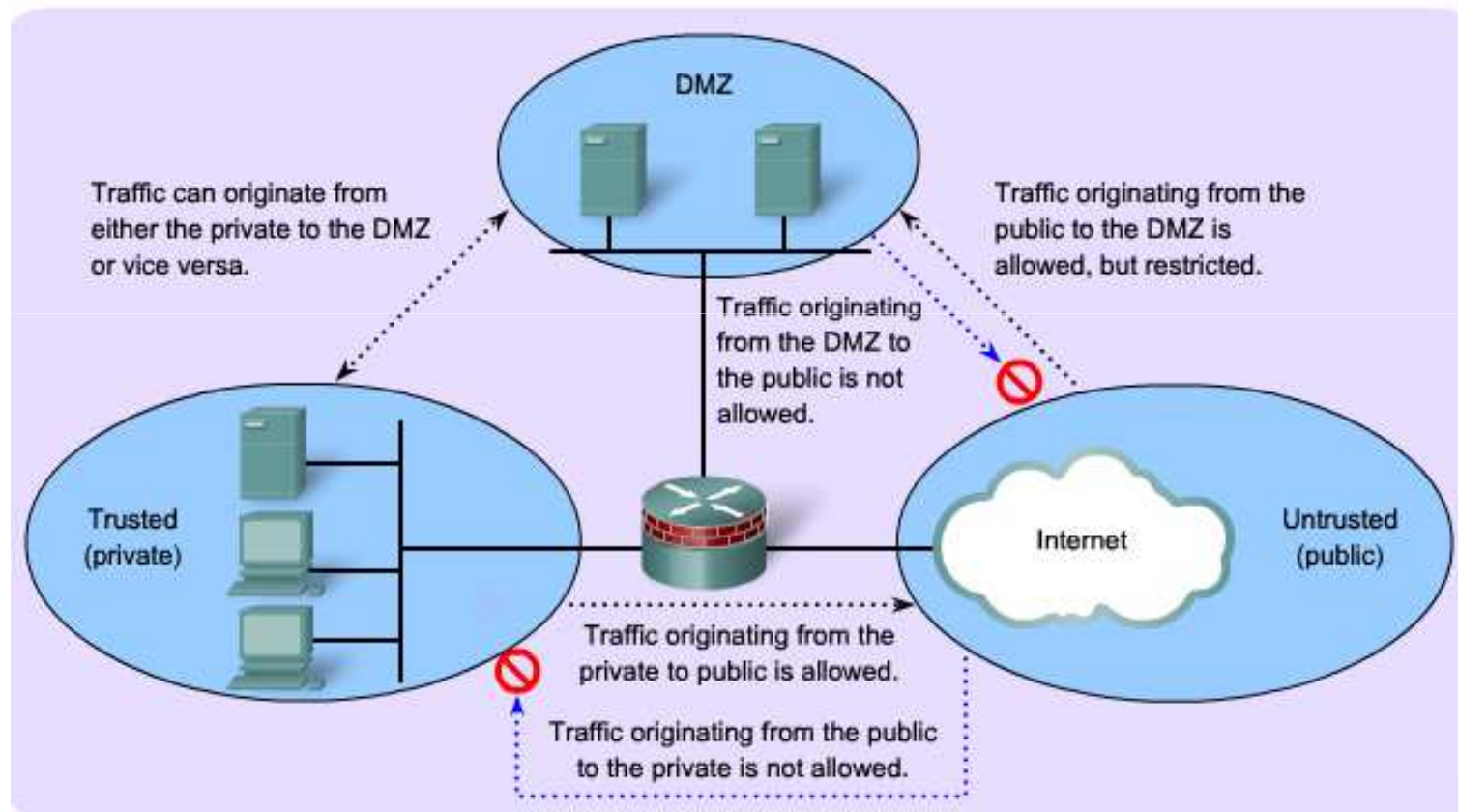


# Mise en œuvre des règles de sécurité

- Un système pare-feu contient un ensemble de règles prédéfinies permettant :
  - D'autoriser la connexion (**allow**) ; De bloquer la connexion (**deny**) ; De rejeter la demande de connexion sans avertir l'émetteur (**drop**).
- L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la **politique de sécurité** adoptée par l'entité.
- On distingue habituellement deux types de politiques de sécurité permettant :
  - Soit d'autoriser uniquement les communications ayant été explicitement autorisées.
  - Soit d'empêcher les échanges qui ont été explicitement interdits.
- La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication



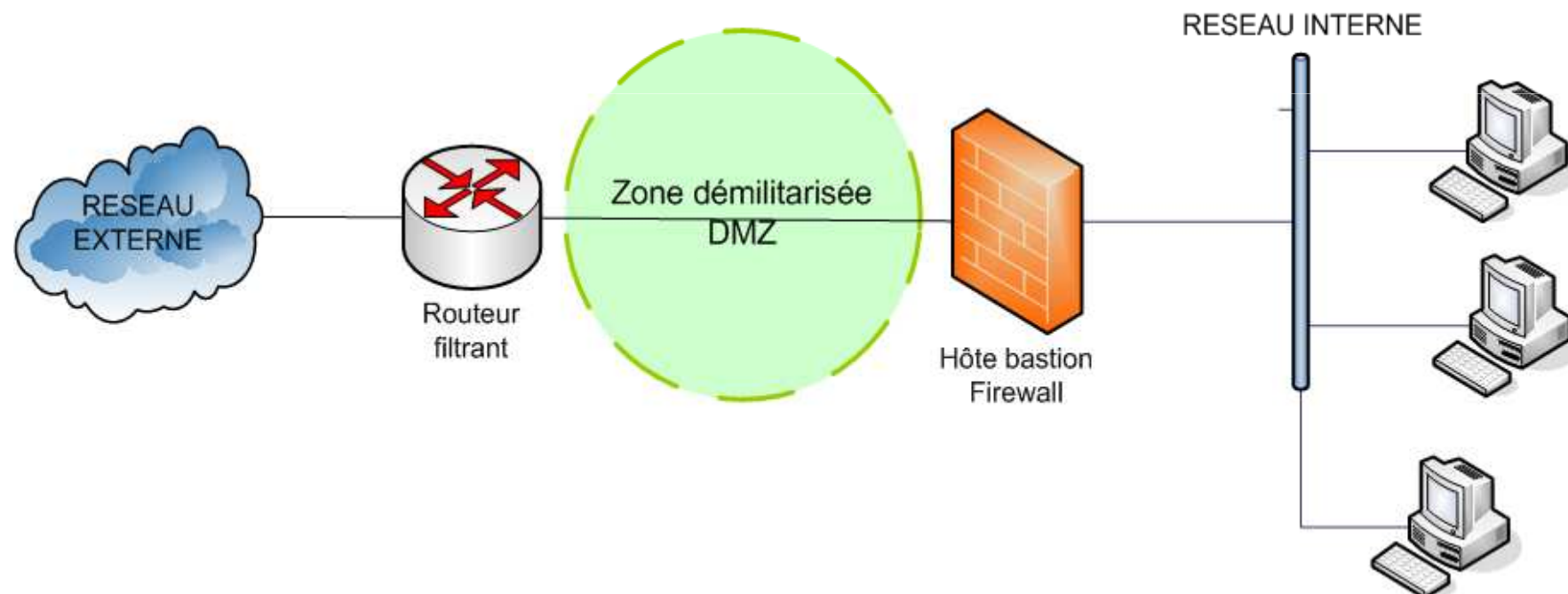
# Déploiement : Stratégie orientée zones



# Exemple de déploiement (1)

Le filtrage statique est assuré par un routeur

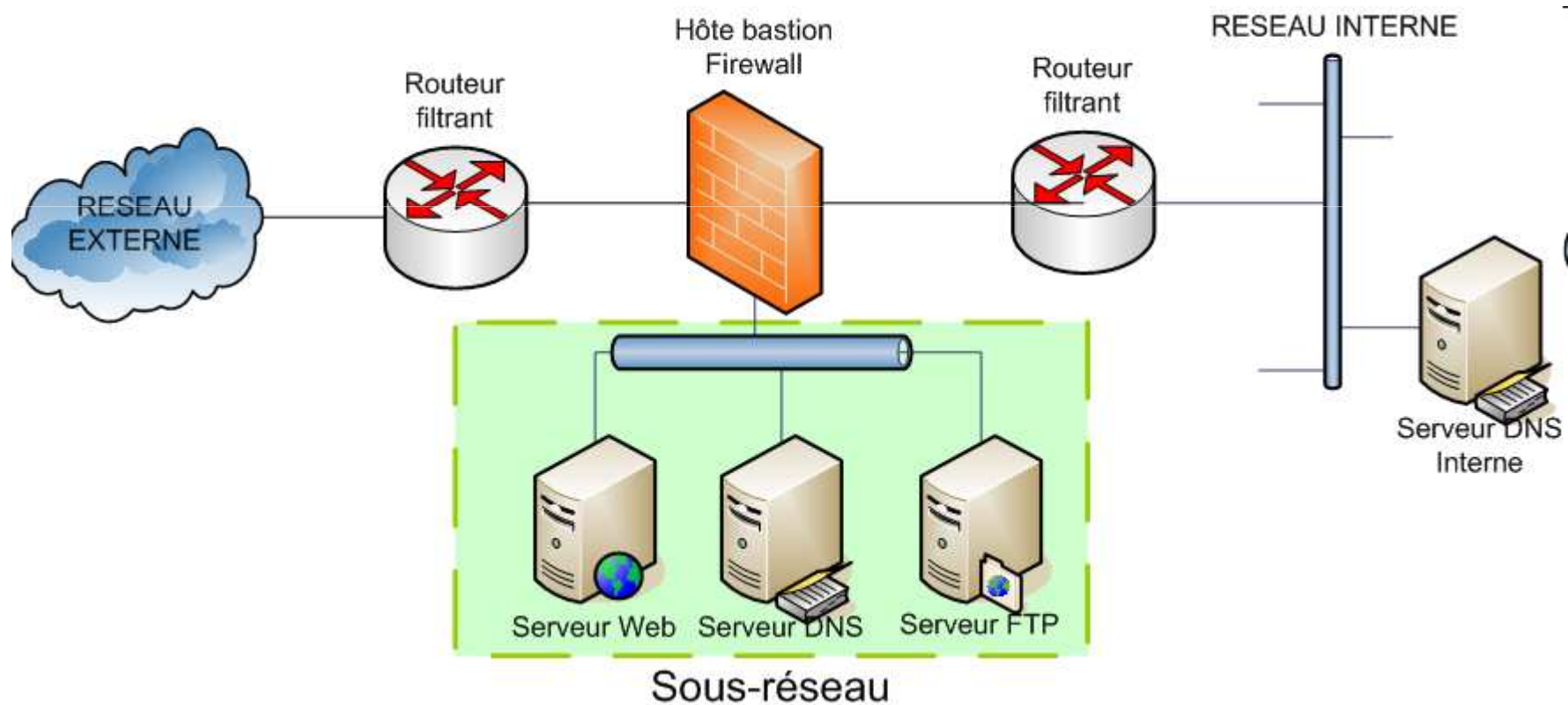
Le filtrage dynamique par un firewall





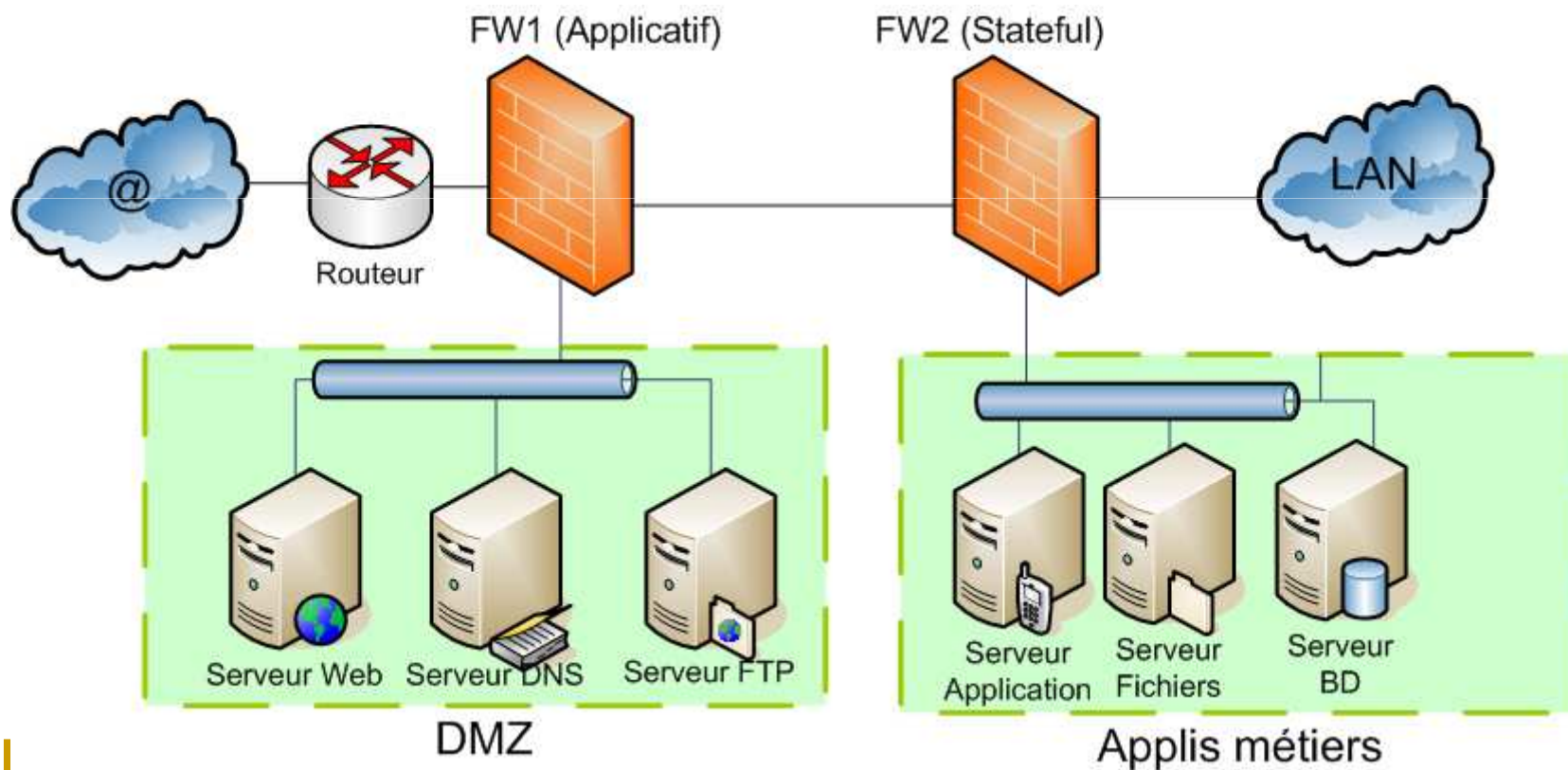
## Exemple de déploiement (2)

- Les serveurs publics sont placés dans un sous-réseau séparé et protégés par un firewall

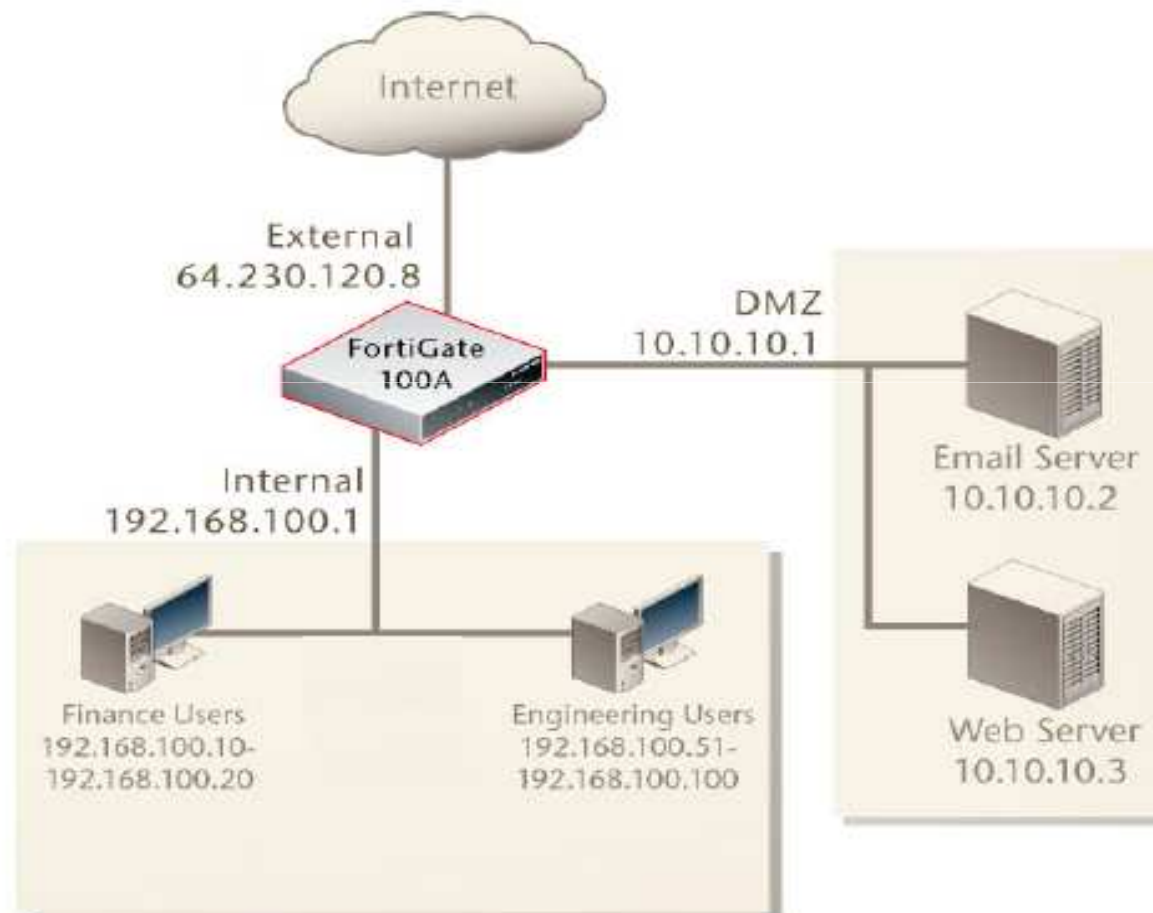


## Exemple de déploiement (3)

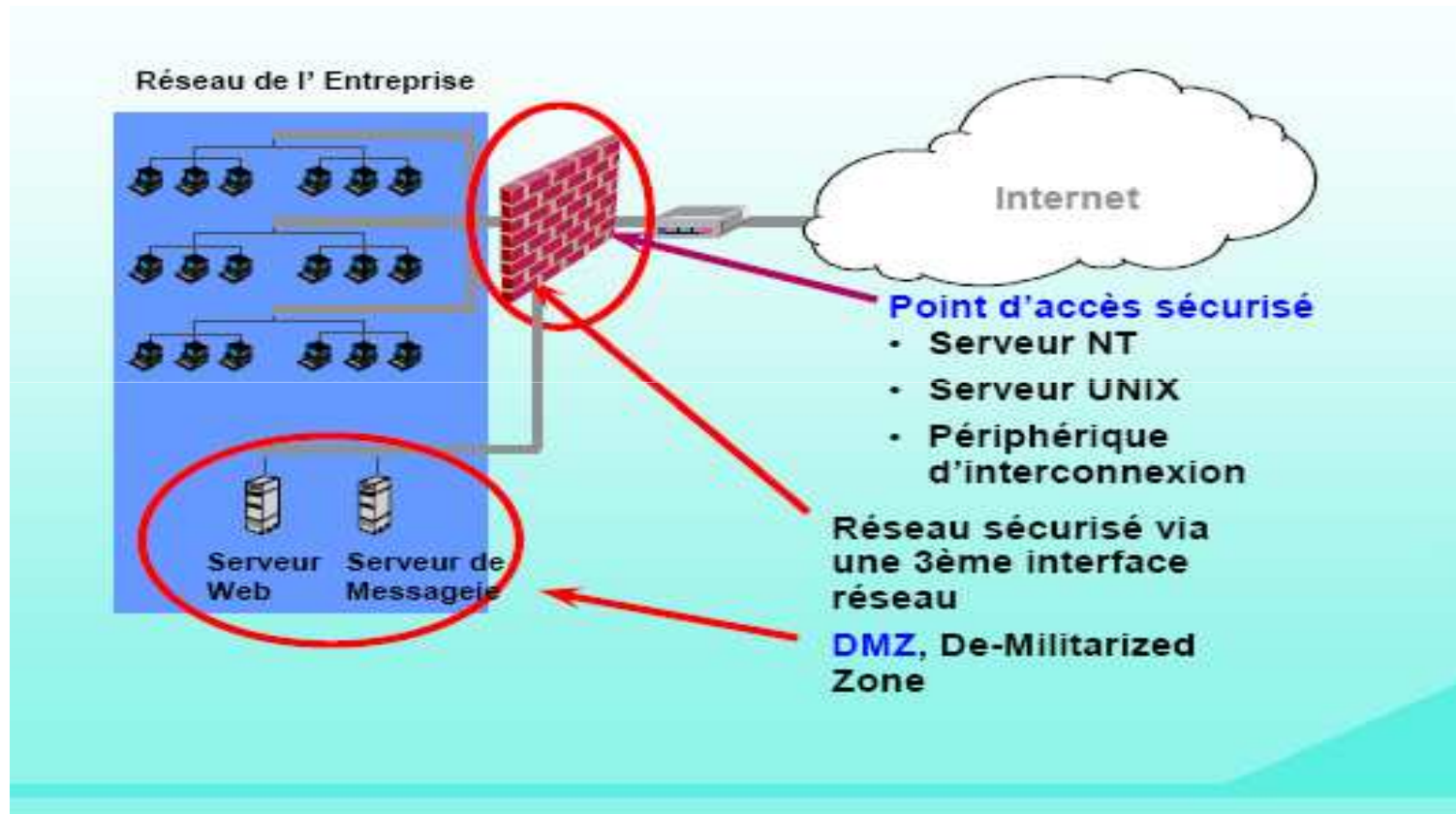
- Firewall 1 : Applicatif sur des applications bien identifiées
- Firewall 2 : Stateful pour des raisons de performances



# Etude de cas pratique

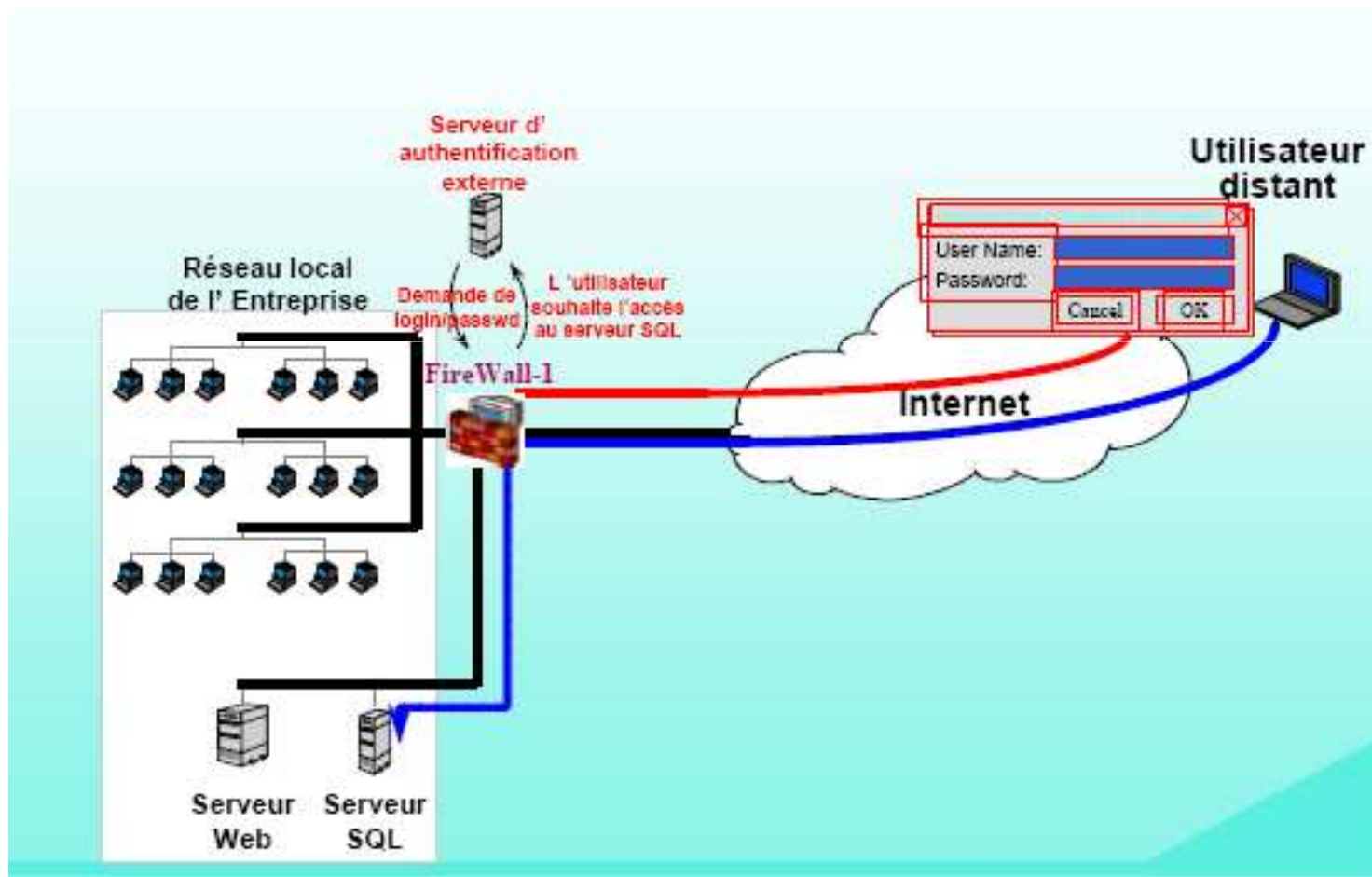


## Exemple de déploiement (2)

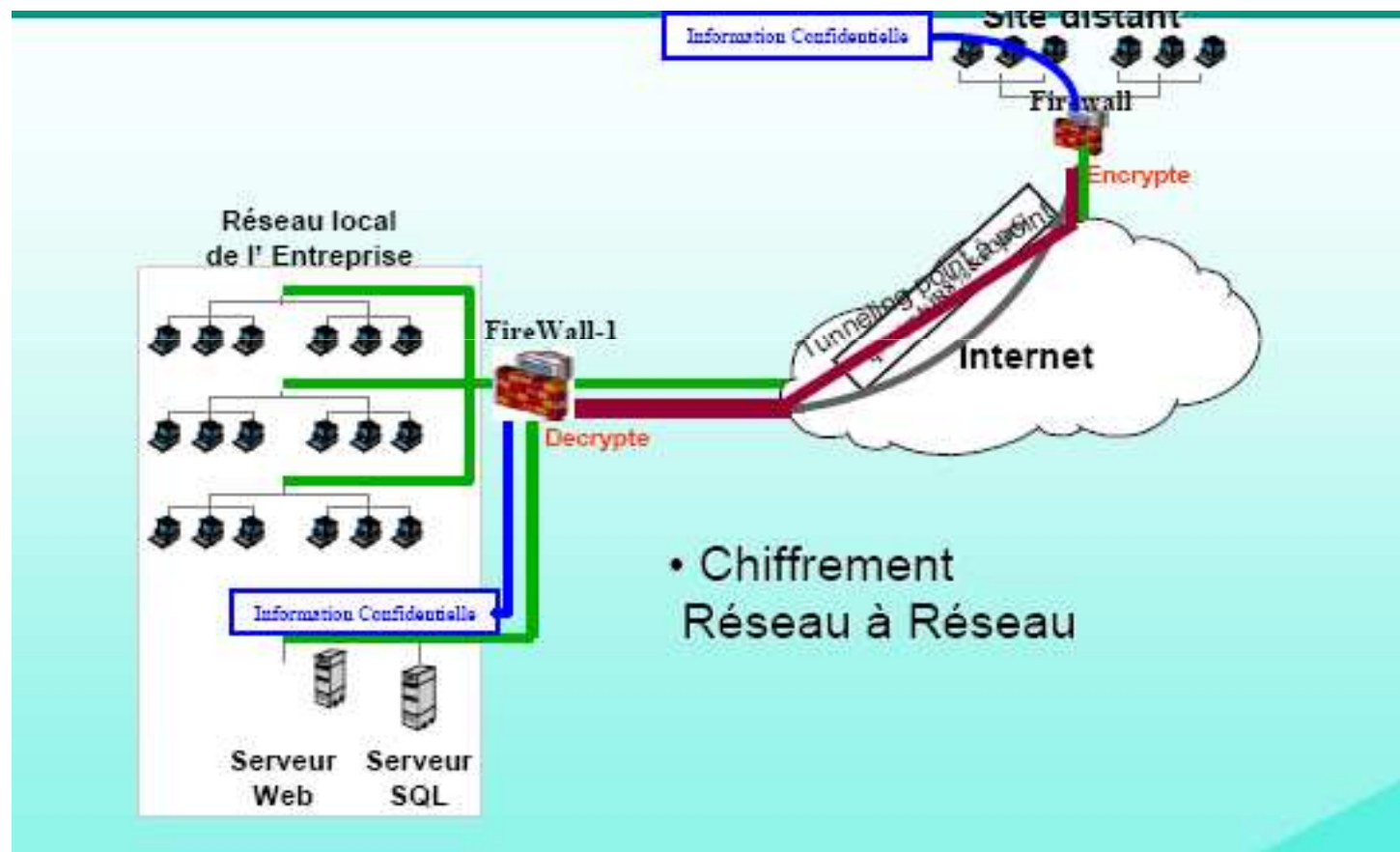


**DMZ: DeMilitarised Zone:** zone dans laquelle réside les serveurs publics de l'organisation

# Authentication

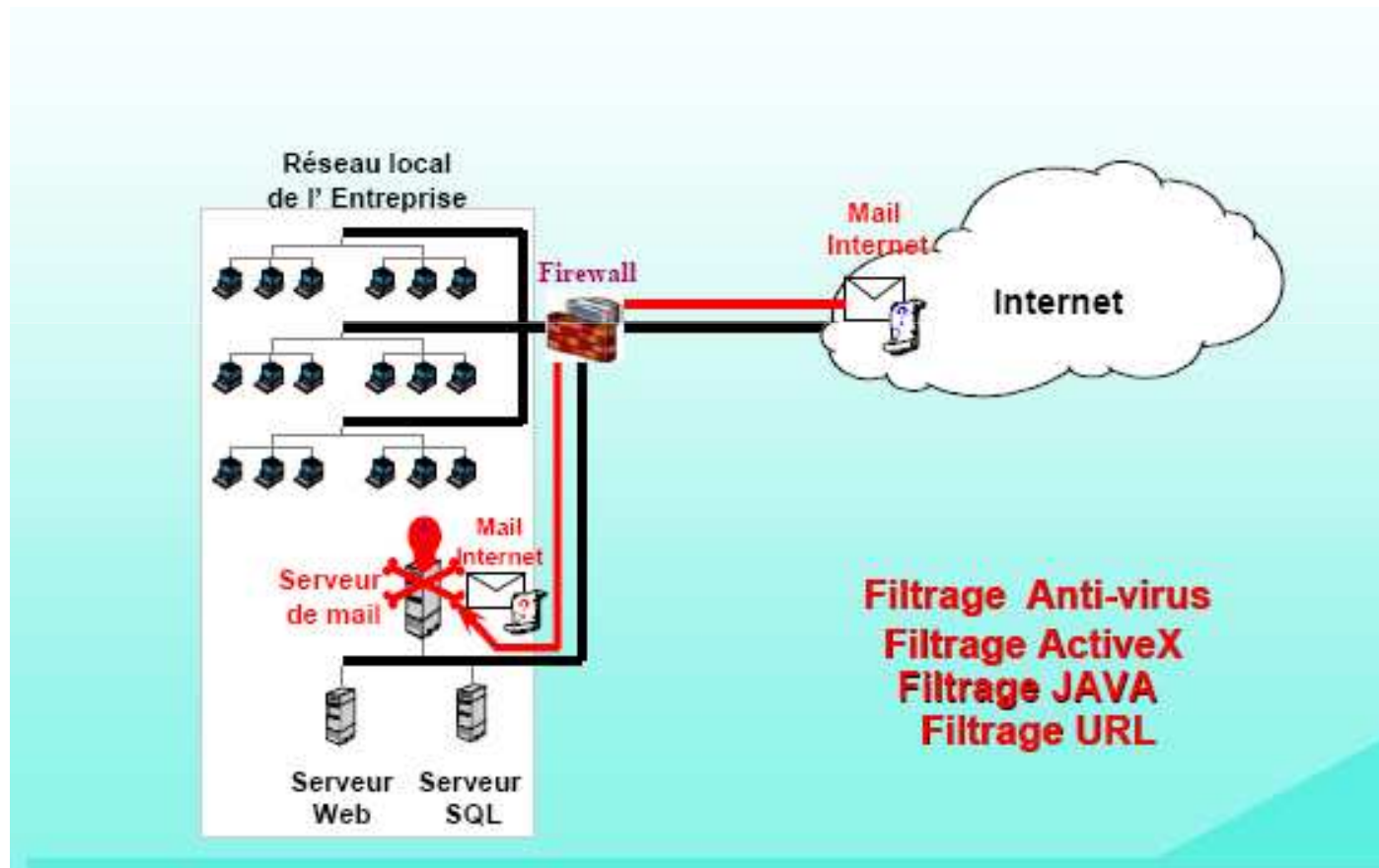


# Chiffrement





# Filtrage de contenu

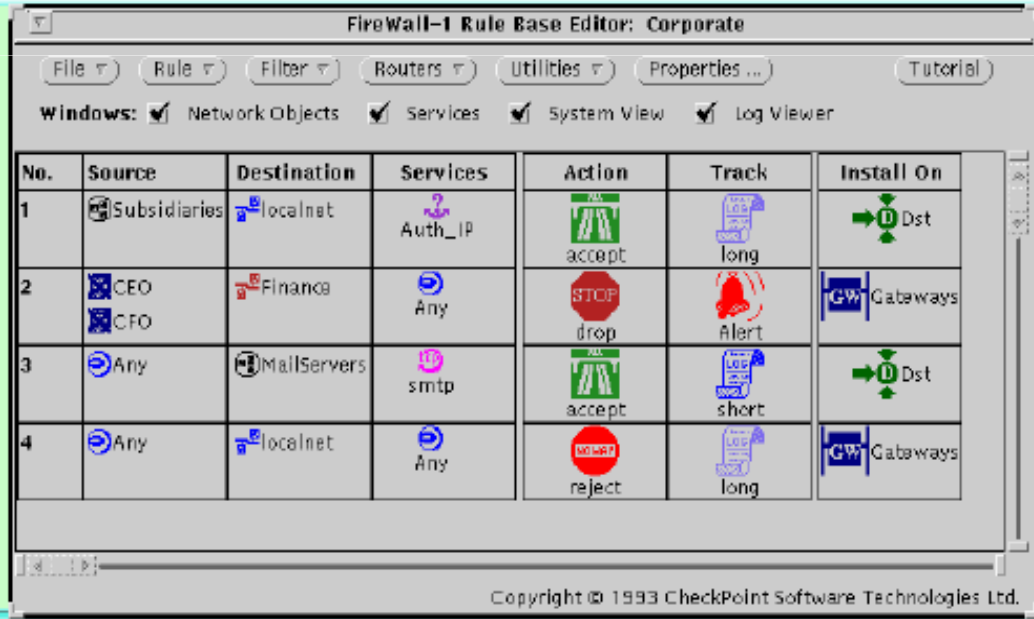


# Exemple de mise en oeuvre de règles

**Niveau de Décision**

- 1 Autoriser les communications authentifiées avec les filiales
- 2 Interdire l'accès au département financier sauf si l'origine est le directeur général (CEO) ou le directeur financier (CFO)
- 3 Autoriser uniquement le Mail au travers d'Internet et enregistrer toutes les communications

**Niveau dir. Informatique Admin. Sécurité**



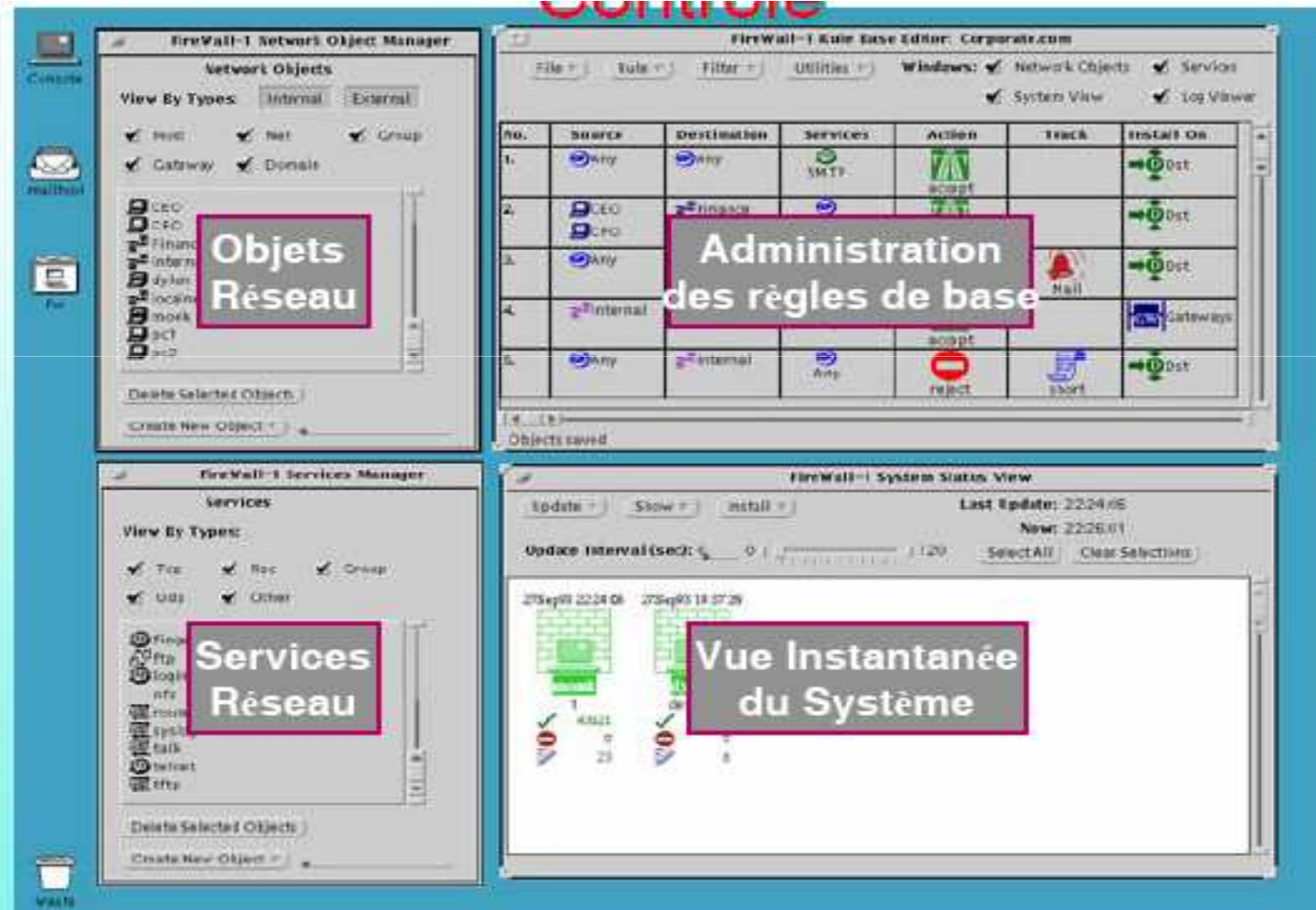
The screenshot shows the FireWall-1 Rule Base Editor interface. It contains a table with four rules. The interface includes a menu bar (File, Rule, Filter, Routers, Utilities, Properties, Tutorial) and a window bar (Network Objects, Services, System View, Log Viewer). The table has columns for No., Source, Destination, Services, Action, Track, and Install On.

No.	Source	Destination	Services	Action	Track	Install On
1	Subsidiaries	localnet	Auth_IP	accept	long	Dst
2	CEO CFO	Financa	Any	drop	Alert	Gateways
3	Any	MailServers	smtp	accept	short	Dst
4	Any	localnet	Any	reject	long	Gateways

Copyright © 1993 CheckPoint Software Technologies Ltd.



# Exemple de console d'administration



# Exemple de journalisation des alertes

- Personnalisation des alertes et traces
- Vue instantanée et états flexibles
- Outils de recherche et de suivi puissants

The screenshot displays the CheckPoint Firewall-1 Alert interface. At the top, a pink box highlights three key features: 'Personnalisation des alertes et traces', 'Vue instantanée et états flexibles', and 'Outils de recherche et de suivi puissants'. Below this, the main interface shows a list of alerts with columns for NUM, DATE, TIME, IP, ORIG, TYPE, ACTION, SERVICE, SRC, DST, and INFO. A detailed view of a specific alert is shown on the right, titled 'FireWall-1: Action Selection', which includes options for Action (In), Apply, and Reset.

NUM	DATE	TIME	IP	ORIG	TYPE	ACTION	SERVICE	SRC	DST	INFO
6	26Oct93	13:41:36	192.168.1.1	doors	finger	reject	finger	bones.eandm.co.il		
8	26Oct93	13:41:52	192.168.1.1	doors	shell	reject	shell	bones.eandm.co.il	doors	s_port port 1019
13	26Oct93	13:42:23	192.168.1.1	doors	login	reject	login	bones.eandm.co.il	doors	s_port port 1019
21	26Oct93	13:46:33	192.168.1.1	doors	login	reject	login	scotty.eandm.co.il	doors	s_port port 1021
27	26Oct93	14:19:24	192.168.1.1	doors	finger	reject	finger	bones.eandm.co.il		
30	26Oct93	14:20:24	192.168.1.1	doors	telnet	reject	telnet	bones.eandm.co.il		
34	26Oct93	14:44:19	192.168.1.1	doors	finger	reject	finger	virgo-mb.math.tau.ac.il	doors	s_port port 1371

# Best Practices

- Position firewalls at key security boundaries.
- Firewalls are the primary security device, but it is unwise to rely exclusively on a firewall for security.
- Deny all traffic by default, and permit only services that are needed.
- Ensure that physical access to the firewall is controlled.
- Regularly monitor firewall logs. Cisco Security Monitoring, Analysis, and Response System (MARS) is especially useful in monitoring firewall logs.
- Practice change management for firewall configuration changes.

# Critères de choix d'un firewall

- Certification (**ICSA Labs** : voir <http://www.icsalabs.com/>).
- Throughput (débit).
- Le type de filtre, le niveau de filtrage:
  - La nature et le nombre d'application appréhendées (FTP, messagerie, HTTP, SNMP, RealAudio, etc.)
- Les facilités d'enregistrement des actions à fin des audits, login, complet des paramètres de connexion, l'existence d'outils d'analyse,.
- Les outils et facilités d'administration
  - Interface graphique ou ligne de commandes, administration distante après authentification du gestionnaire
- La capacité de supporter un tunnel chiffré permettant si nécessaire des VPNs.
- La possibilité d'effectuer de l'équilibrage de charge / Haute disponibilité.
- Le dimensionnement du firewall:
  - Nombre de pattes nécessaires (inside, ouside, DMZ)