
INSA
INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
HAUTS-DE-FRANCE
Université
Polytechnique
HAUTS-DE-FRANCE
Le Pare-feu - Firewall
Diapo 1

Introduction

Définition d'un pare-feu

- Un pare-feu est un **système de sécurité** qui **contrôle et limite l'accès entre deux réseaux**,
  - entre un réseau interne et le réseau Internet.
  - Son objectif est de protéger le réseau interne en empêchant les connexions non autorisées venant de l'extérieur.
- Le pare-feu agit comme une barrière de sécurité qui **contrôle et filtre le trafic réseau** entrant et sortant.
  - en fonction des politiques de sécurité de l'organisation.
- pare-feu **matériels**, les pare-feu **logiciels** et les pare-feu de **nouvelle génération** combinant plusieurs fonctionnalités
- .

- Enfin, il est important de souligner que les pare-feu ne garantissent pas une **sécurité absolue**.

- Ils constituent simplement **une mesure de sécurité parmi d'autres** dans la stratégie de sécurité globale d'une organisation

Objectifs d'un pare-feu

1. **Contrôler l'accès aux ressources** : Les pare-feux sont conçus pour contrôler l'accès aux ressources réseau en autorisant ou en bloquant les connexions entrantes et sortantes en fonction de certaines règles et politiques.

2. **Protéger contre les attaques** et ainsi **Assurer la disponibilité des ressources** : Ils sont capables de détecter et de bloquer les tentatives d'intrusion et les attaques de différents types, tels que les attaques par déni de service (DoS), les attaques de force brute, les attaques par exploitation de vulnérabilités connues, etc.

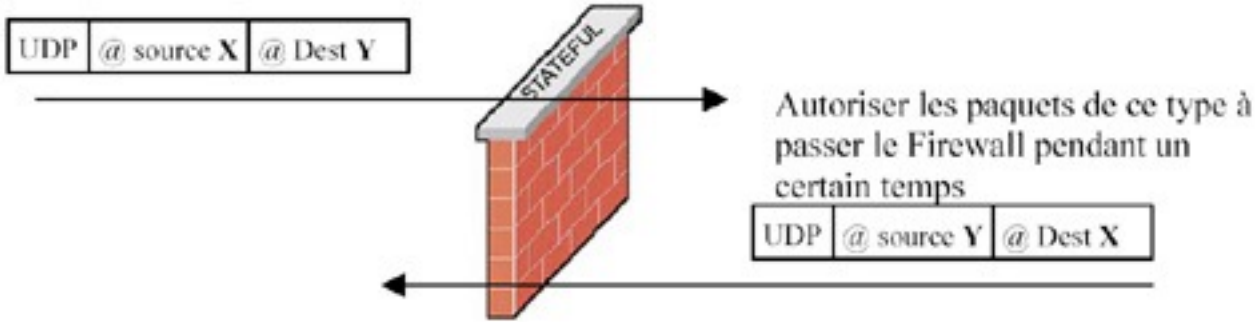
Les pare-feu filtrant

Fonctionnement général

- Le fonctionnement général d'un pare-feu est basé sur **une série de règles de filtrage**

➢ qui déterminent si un paquet de données **doit être autorisé ou bloqué** en fonction de son adresse IP, de son port de destination, de son protocole et de son contenu.

➢ Les règles de filtrage sont généralement basées sur des adresses IP, des numéros de port et des protocoles.



Fonctionnement général

- Le pare-feu **examine les en-têtes IP et TCP/UDP** du paquet pour
  - ➢ déterminer son origine, sa destination, le protocole utilisé et le numéro de port.
  - ➢ Si le paquet correspond à une règle de filtrage, il est autorisé à passer. Sinon, il est bloqué.
- .

Détail de fonctionnement

- Les règles de filtrage sont basées sur des informations telles que
- l'a**dresse IP** source et de destination,
- les **ports** source et de destination,
- le **protocole** de la couche de transport (TCP, UDP, ICMP, etc.)
- …

Détail : Les principaux types de filtrage sont :

- Filtrage par **adresse IP** : Le filtrage par adresse IP permet de spécifier les adresses IP sources et/ou destinations qui sont autorisées ou bloquées pour accéder au réseau.

- Filtrage par **port** : Le filtrage par port permet de spécifier les numéros de port sources et/ou destinations qui sont autorisés ou bloqués pour accéder au réseau. Il peut s'agir de ports TCP ou UDP.

- Filtrage par **protocole** : Le filtrage par protocole permet de spécifier les protocoles qui sont autorisés ou bloqués pour accéder au réseau. Les protocoles courants tels que HTTP, FTP, SMTP, etc. peuvent être autorisés ou bloqués.

- Filtrage par **type de trafic** : Le filtrage par type de trafic permet de spécifier le type de trafic qui est autorisé ou bloqué pour accéder au réseau. Par exemple, le trafic ICMP peut être bloqué pour empêcher les attaques de type ping-flood.

- Filtrage par **contenu** : Le filtrage par contenu permet de spécifier les types de données qui sont autorisés ou bloqués pour accéder au réseau. Par exemple, les fichiers exécutables peuvent être bloqués pour empêcher les virus.

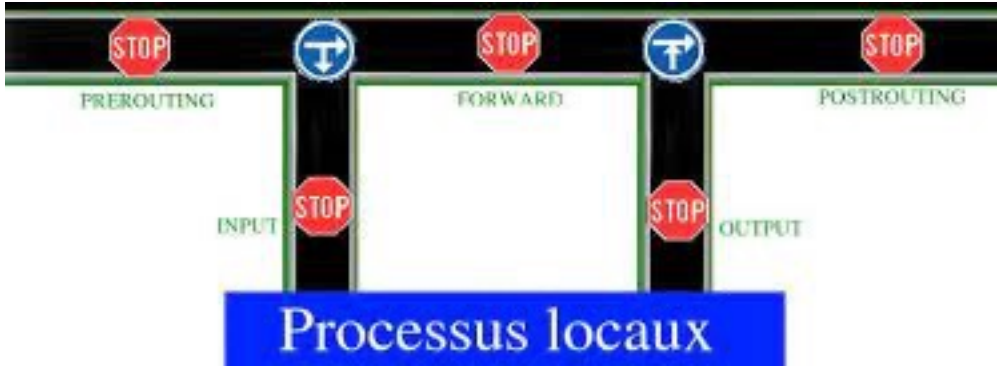
Inconvénients

- Ne peut pas protéger contre les attaques basées sur des protocoles autorisés ou des ports ouverts (tels que les attaques de phishing).

- Une attaque venant de l'intérieur vers l'extérieur via une adresse du réseau local va être laissée par le firewall

Inconvénients (Suite)

- Peut ralentir le trafic réseau si les règles de filtrage sont trop restrictives ou si le matériel n'est pas suffisamment puissant.



- Peut nécessiter
  - **une configuration et une maintenance approfondies**
  - pour s'assurer que les règles de filtrage sont toujours à jour et efficaces.

Inconvénients (Suite 2)

- N’est pas suffisant, il fait parti d’un **arsenal** mais doit être complété par des mesures d’une politique de sécurité de l’entreprise, d’autres équipements de sécurité, la détection d’intrusion

Pare-feu applicatif

Présentation

- Un pare-feu applicatif, également connu sous le nom de firewall applicatif ou **WAF (Web Application Firewall)**, est un type de pare-feu qui est spécifiquement conçu pour **protéger les applications web** contre les attaques.

- Contrairement aux pare-feux traditionnels
  - qui se concentrent sur les connexions réseau et les paquets de données,
- les pare-feux applicatifs sont **capables**
  - **d'analyser le trafic applicatif en utilisant des algorithmes avancés pour détecter les attaques** sur les applications web.

Présentation

- Ils peuvent détecter et bloquer
  - les tentatives de piratage,
  - les injections de code malveillant,
  - les attaques par déni de service (DoS),
  - les attaques de phishing
  - et d'autres types d'attaques ciblant les applications web.

- Par exemple : vérifie les requêtes et les réponses HTTP pour détecter les tentatives d'attaques,
  - les injections SQL,
  - les attaques de cross-site scripting (XSS),

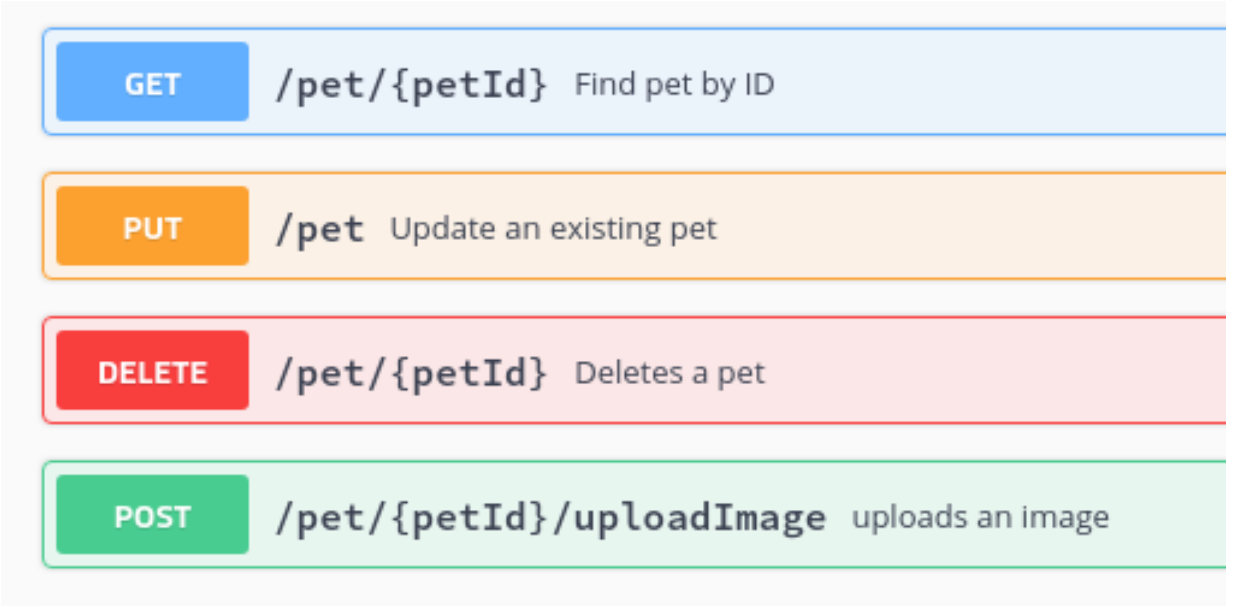
Les différents types de filtrage

- **Filtrage de contenu** : Il s'agit d'un type de filtrage qui examine le contenu de la communication entre l'application et l'utilisateur.
  - Le pare-feu peut être configuré pour bloquer certains types de contenu,
    - tels que les fichiers exécutables
    - ou les scripts.

- **Filtrage d'URL** : Ce type de filtrage examine l'URL de la requête pour déterminer si elle est autorisée ou non.
  - Le pare-feu peut être configuré pour bloquer les requêtes vers des sites Web spécifiques ou vers des pages Web spécifiques.

Les différents types de filtrage

- **Filtrage de méthodes** : Ce type de filtrage examine les méthodes HTTP utilisées dans les requêtes. Le pare-feu peut être configuré pour bloquer les méthodes non autorisées, telles que les méthodes de modification de données.
  - UPDATE
  - DELETE
  - ETC …



Avantages

- Ils offrent une protection
  - **plus ciblée et spécifique pour les applications**,
  - en bloquant uniquement les activités suspectes ou malveillantes qui se produisent à l'intérieur de l'application elle-même.

- Ils offrent une meilleure visibilité sur le trafic entrant et sortant de l'application, ce qui permet de **mieux comprendre les activités** malveillantes et de les bloquer plus efficacement.

- Ils permettent aux organisations de mettre en œuvre des politiques de **sécurité plus granulaires** et personnalisées pour chaque application.

Inconvénients

- Ils peuvent être **difficiles à configurer et à maintenir**,

car ils nécessitent une connaissance approfondie de l'application cible.

- Ils peuvent entraîner des retards ou des perturbations dans

les **performances** de l'application, en particulier si les règles de filtrage sont trop restrictives ou mal configurées.

- Ils peuvent ne pas offrir une protection suffisante **contre les attaques de couche réseau** ou de couche **transport**, qui peuvent contourner les règles de filtrage applicatif.

Les pare-feu nouvelle génération

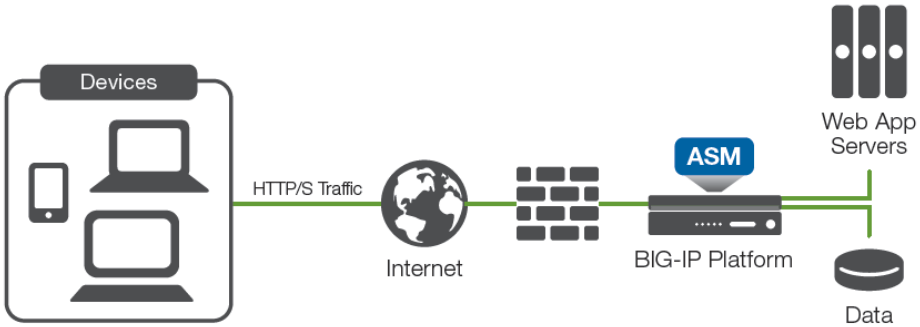
- Les pare-feu de nouvelle génération (**Next-Generation Firewalls** ou **NGFW**) sont des équipements de sécurité informatique plus avancés que les pare-feu traditionnels.

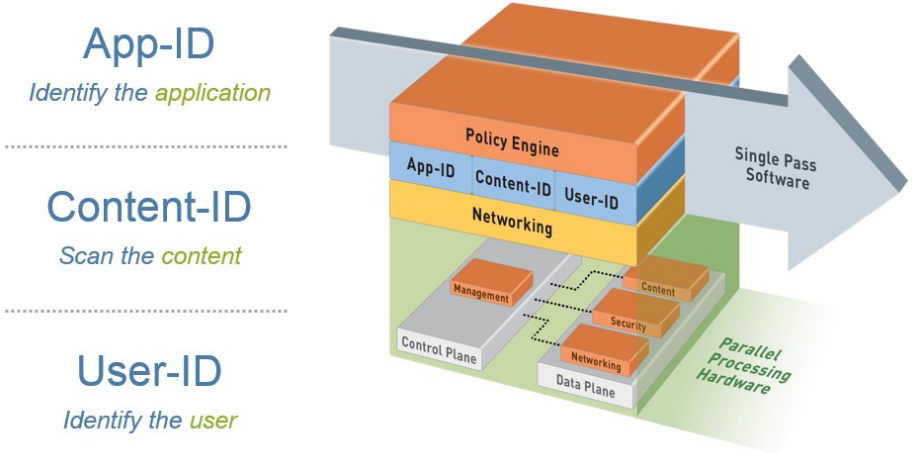
- **NGFW** offre des fonctionnalités standard de filtrage des paquets.
- Intègre des outils avancés :
  - DPI (inspection approfondie des paquets)
  - antivirus,
  - IPS (la prévention contre les intrusions)

- Permet des politiques de sécurité personnalisées par application ou utilisateur.
- Sécurité renforcée à travers les couches réseau, transport et application.

En résumé :

- un **WAF** est spécifique à la protection des applications web,
- tandis qu'un **NGFW** offre une protection plus large et plus profonde sur l'ensemble du réseau, incluant mais ne se limitant pas aux applications web.



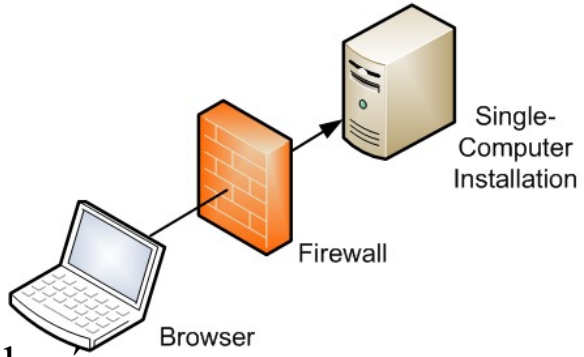


Architecture de sécurité à un niveau

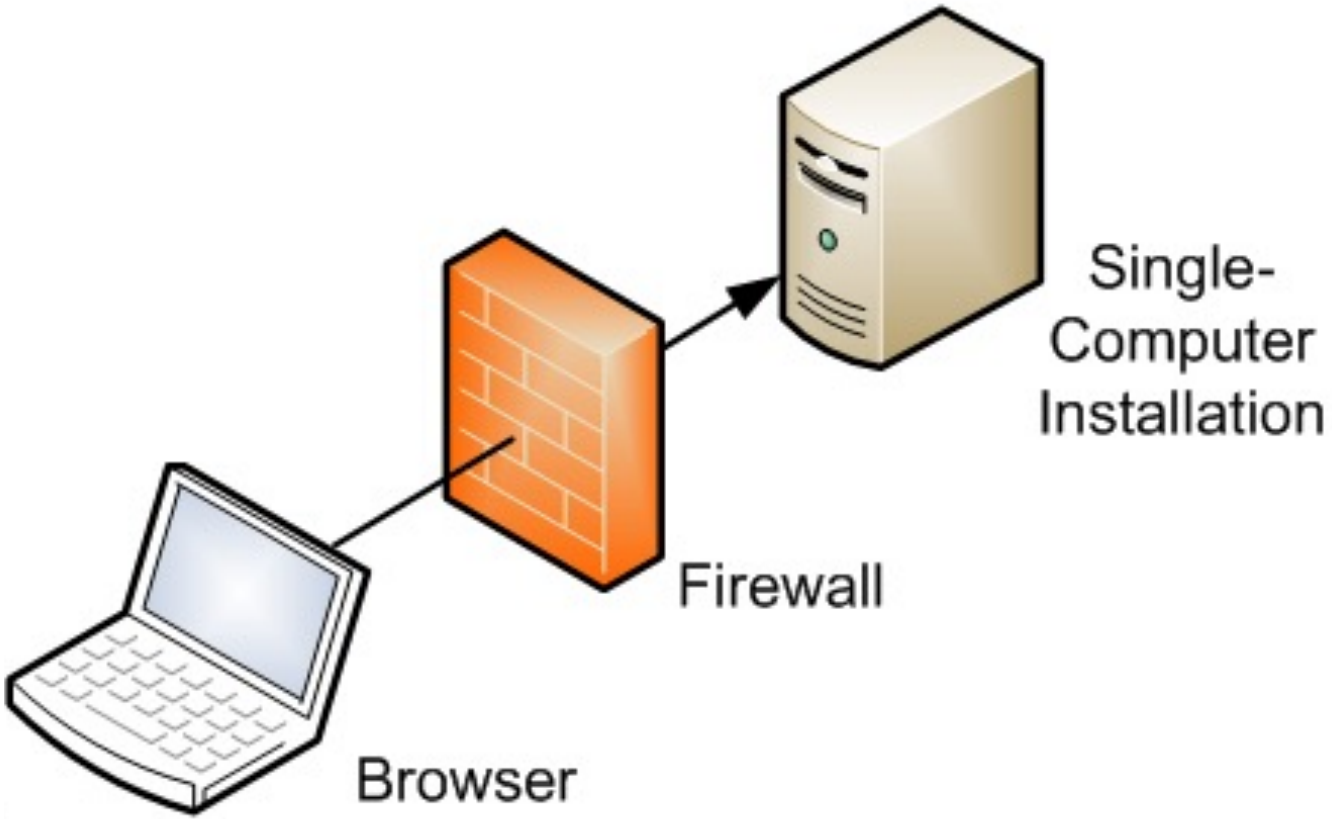
Présentation

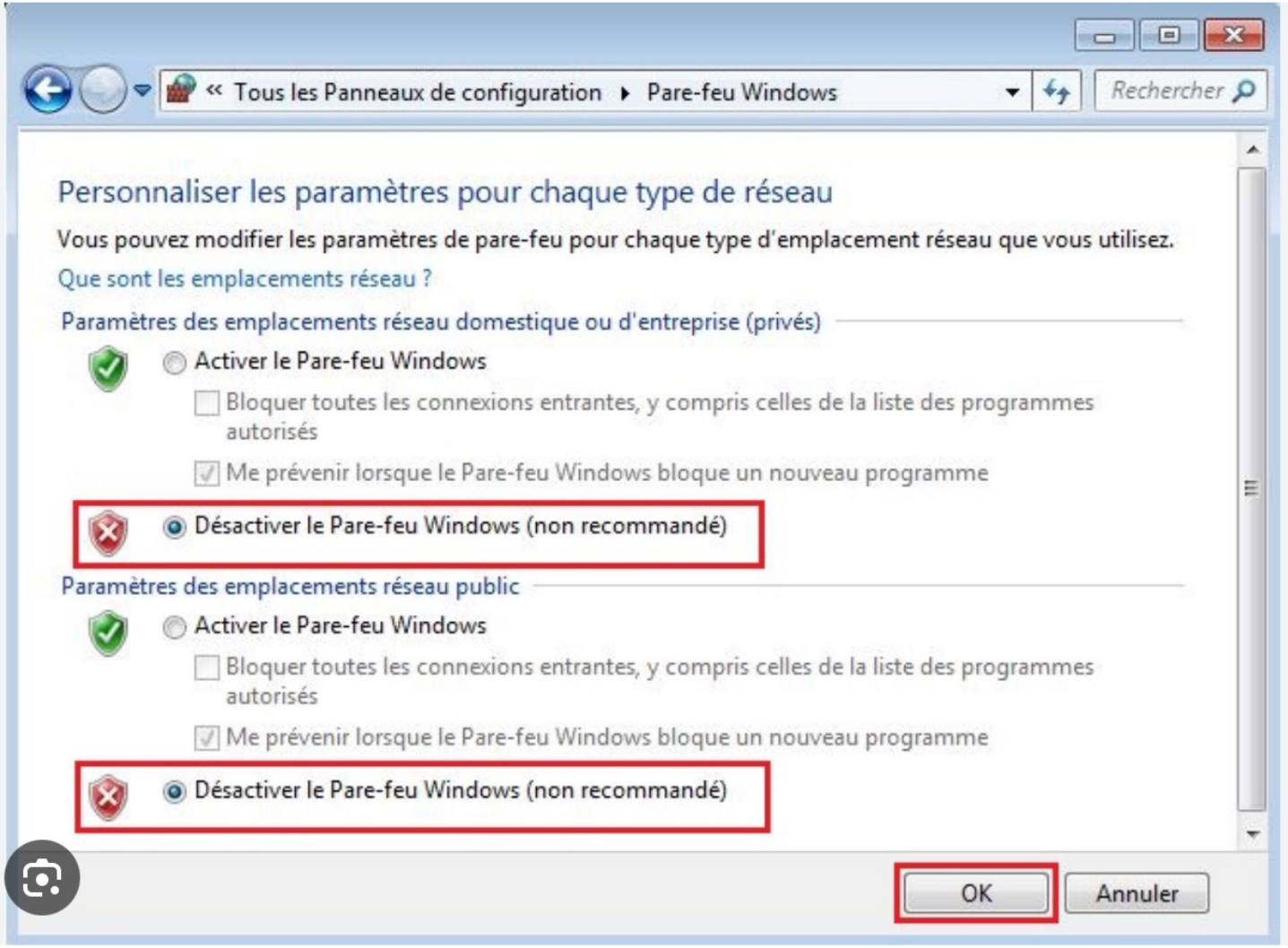
- Un pare-feu à un **seul niveau sans DMZ** est une architecture **où tous les équipements sont connectés** sur un même réseau et sont contrôlés par un seul pare-feu. Le pare-feu joue le rôle de gardien du réseau et contrôle toutes les entrées et sorties du réseau.

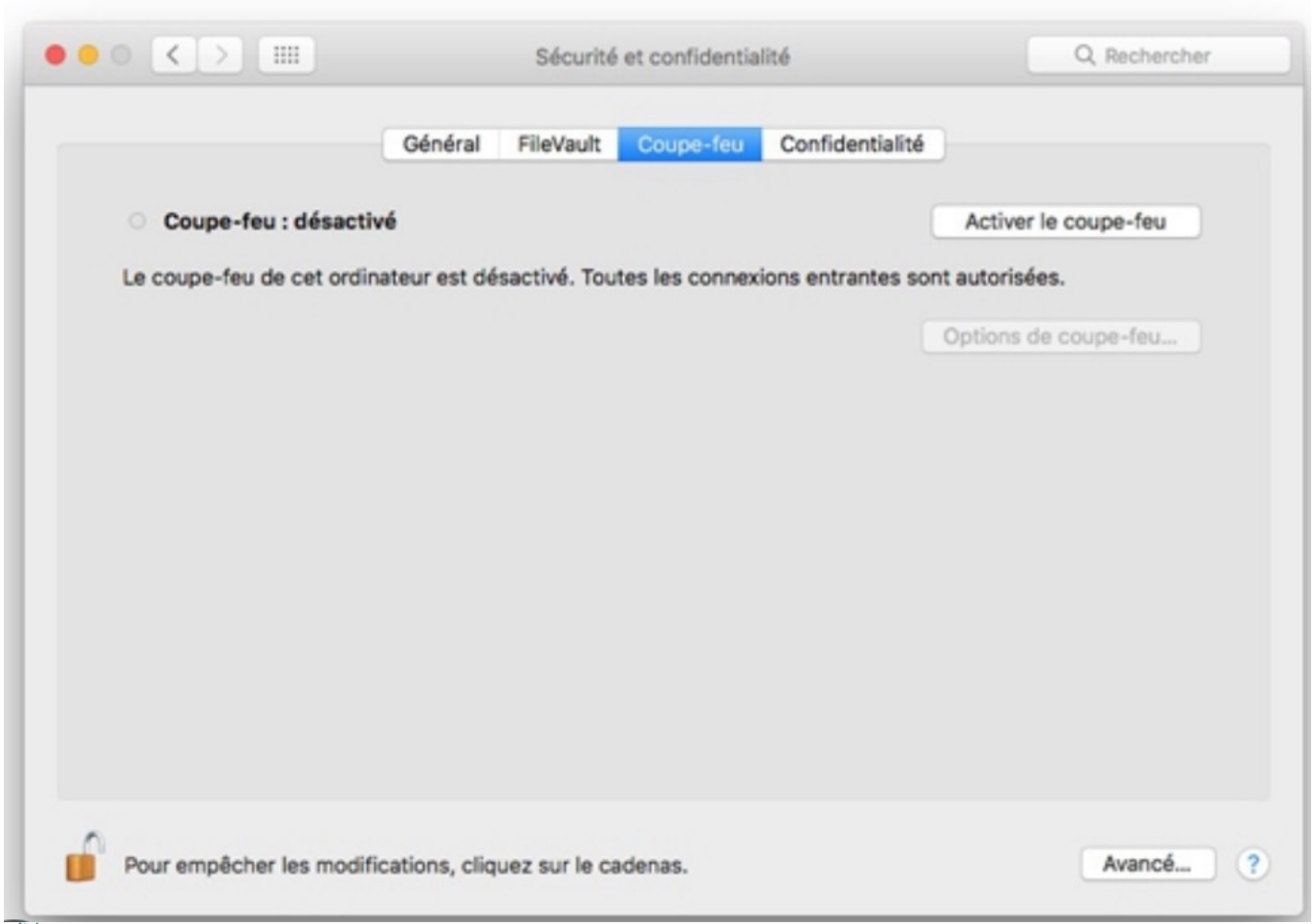
- Dans cette architecture, le pare-**feu est installé entre le réseau interne et le réseau externe (Internet)**. Toutes les communications entre les deux réseaux doivent donc passer par le pare-feu.

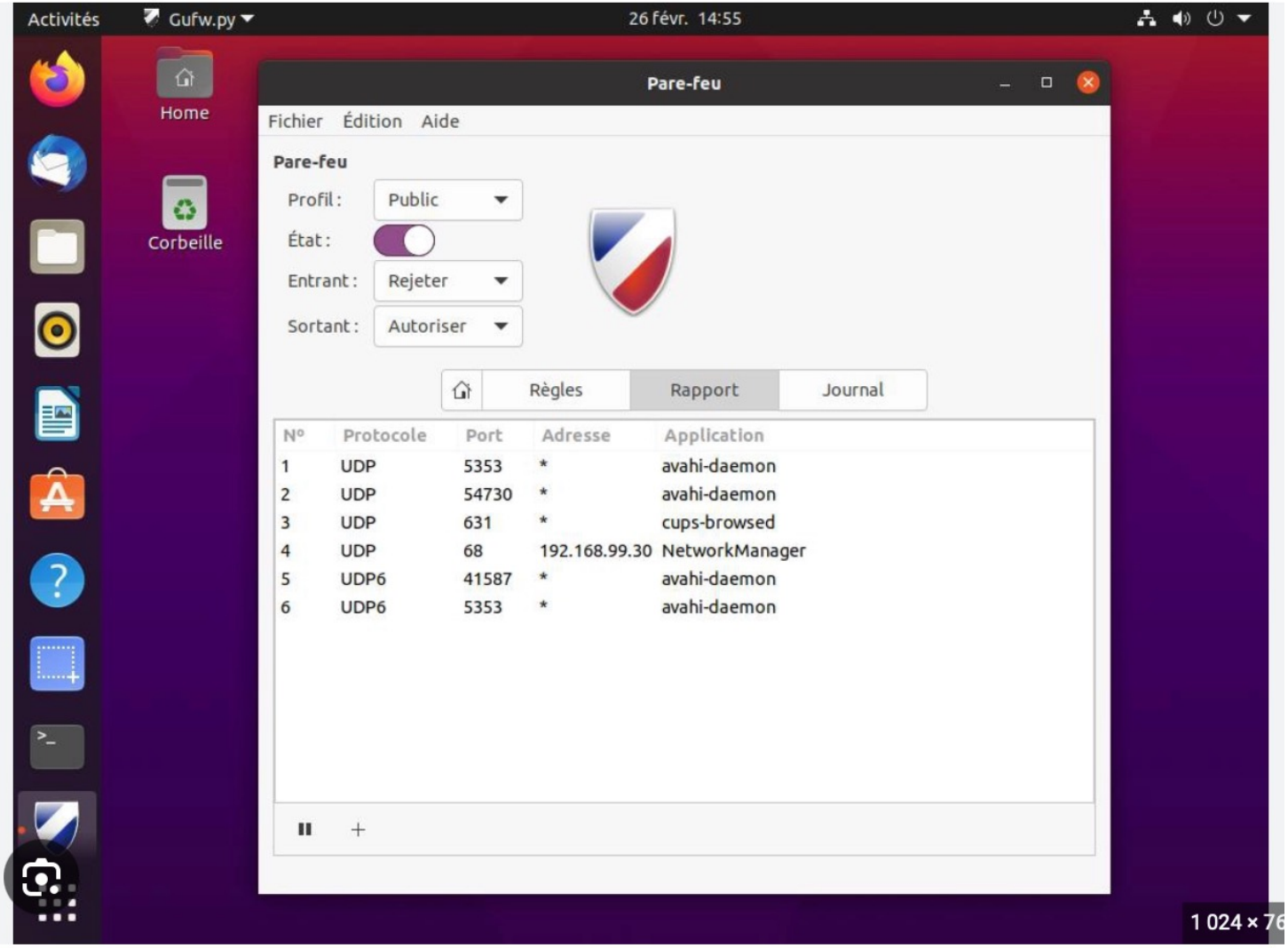


- Avantages
  - Facile à gérer
  - Économique
- Inconvénient : sécurité si réussite à entrer dans le réseau


Single-
Computer
Installation
Firewall
Browser


« Tous les Panneaux de configuration ▸ Pare-feu Windows
Rechercher
Personnaliser les paramètres pour chaque type de réseau
Vous pouvez modifier les paramètres de pare-feu pour chaque type d'emplacement réseau que vous utilisez.
Que sont les emplacements réseau ?
Paramètres des emplacements réseau domestique ou d'entreprise (privés)
Activer le Pare-feu Windows
Bloquer toutes les connexions entrantes, y compris celles de la liste des programmes autorisés
Me prévenir lorsque le Pare-feu Windows bloque un nouveau programme
Désactiver le Pare-feu Windows (non recommandé)
Paramètres des emplacements réseau public
Activer le Pare-feu Windows
Bloquer toutes les connexions entrantes, y compris celles de la liste des programmes autorisés
Me prévenir lorsque le Pare-feu Windows bloque un nouveau programme
Désactiver le Pare-feu Windows (non recommandé)
OK
Annuler


Sécurité et confidentialité
Rechercher
Général
FileVault
Coupe-feu
Confidentialité
Coupe-feu : désactivé
Activer le coupe-feu
Le coupe-feu de cet ordinateur est désactivé. Toutes les connexions entrantes sont autorisées.
Options de coupe-feu...
Pour empêcher les modifications, cliquez sur le cadenas.
Avancé...
?


Activités
Gufw.py
26 févr. 14:55
Home
Corbeille
Pare-feu
Fichier Édition Aide
Pare-feu
Profil : Public
État :
Entrant : Rejeter
Sortant : Autoriser
Règles
Rapport
Journal
N° Protocole Port Adresse Application
1 UDP 5353 * avahi-daemon
2 UDP 54730 * avahi-daemon
3 UDP 631 * cups-browsed
4 UDP 68 192.168.99.30 NetworkManager
5 UDP6 41587 * avahi-daemon
6 UDP6 5353 * avahi-daemon

Architecture avec une DMZ

DMZ ?

- Quelques fois, les entreprises permettent l'accès à certains serveurs : web, messagerie ou FTP.

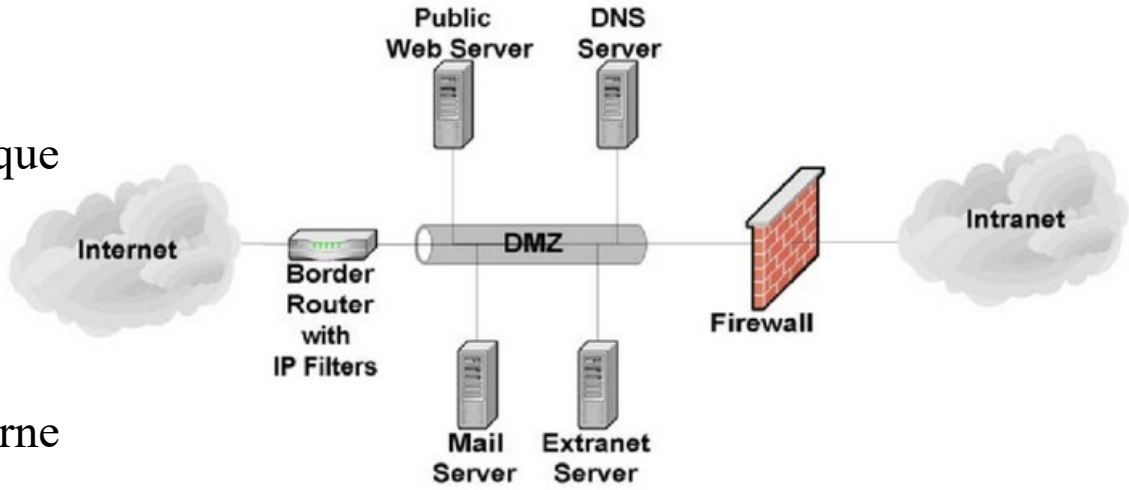
- Pour des raisons de sécurité, ces machines ne peuvent se trouver à l'intérieur du réseau mais en même temps doivent se trouver physiquement à côté.

- Aussi, ces serveurs sont isolés dans des zones démilitarisé (**DMZ pour DeMilitarized Zone**) du reste du réseau.

Si il a intrusion dans cette zone tampon, le reste du réseau ne risque rien, au pire des cas, on arrête les machines du DMZ.

Firewall avec une DMZ

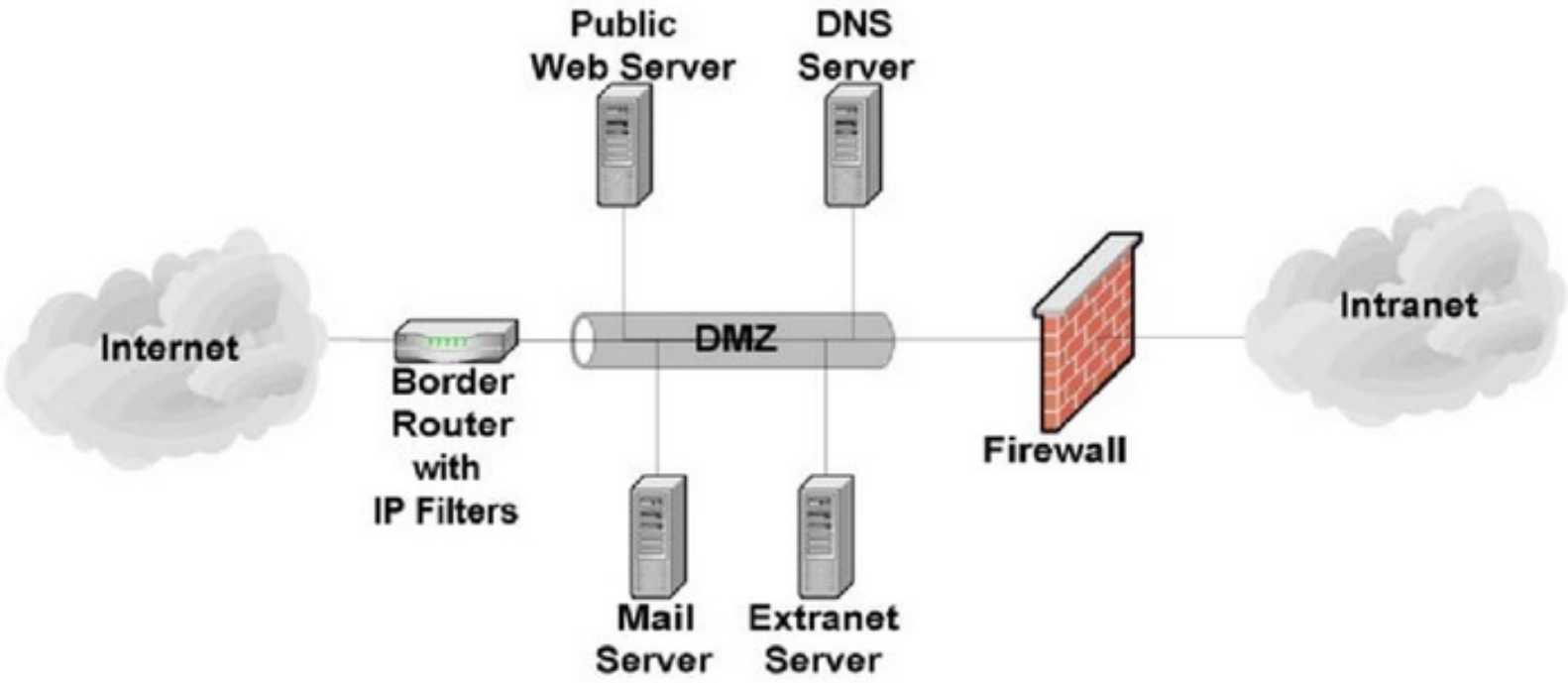
- L'architecture méthode classique

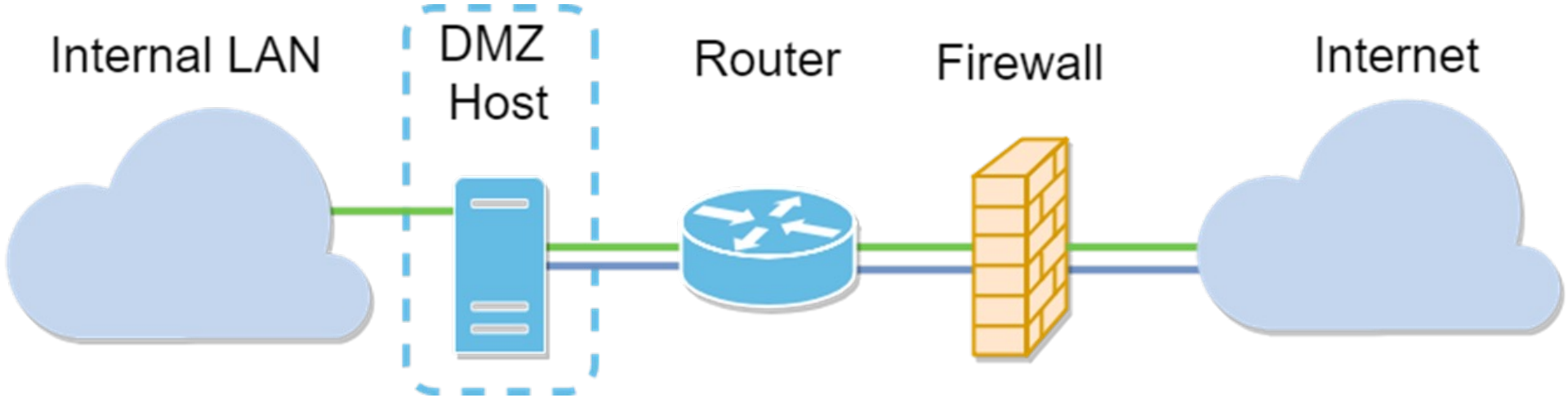


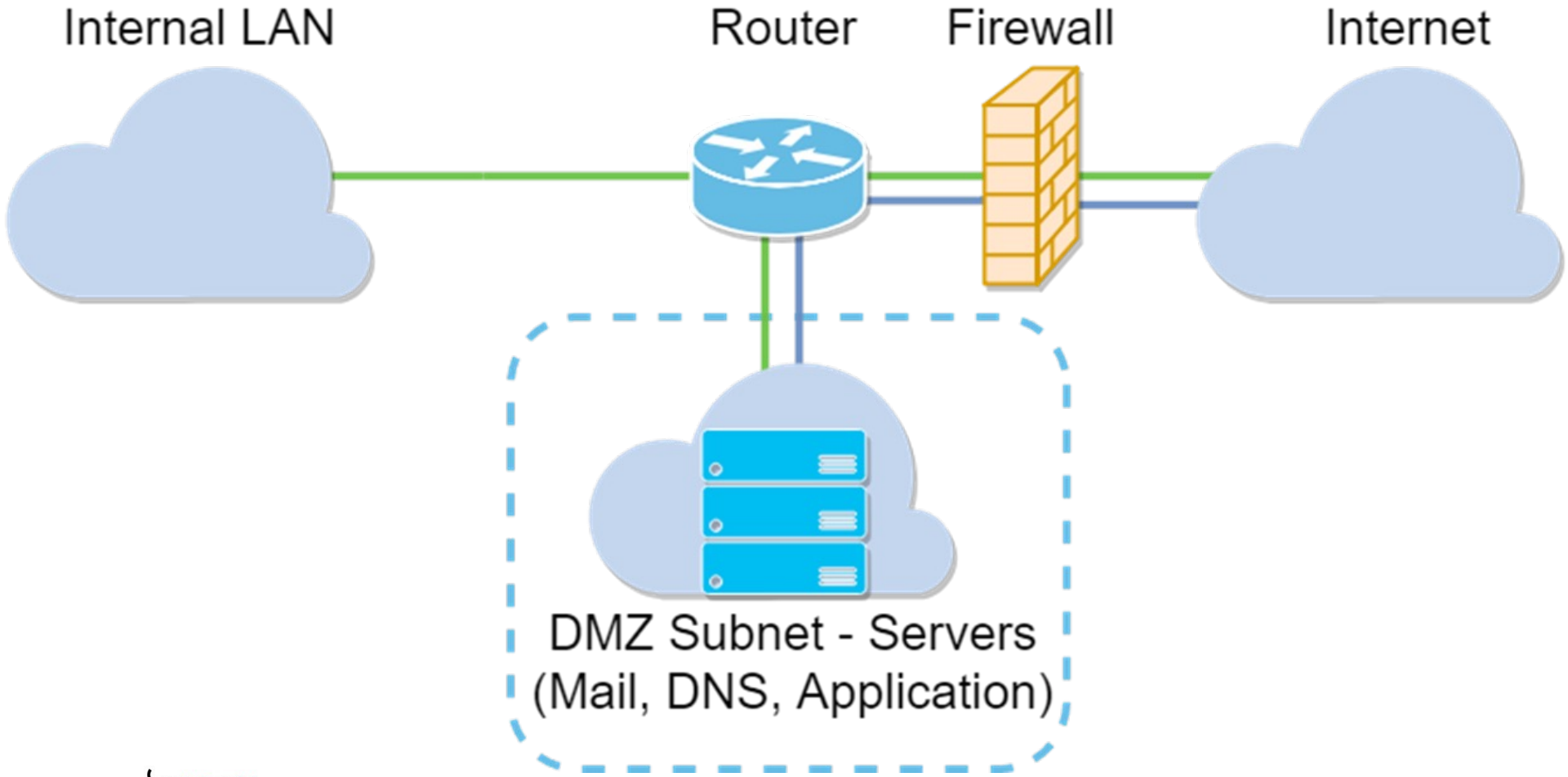
- Le pare-feu
  - est placé **entre** le réseau interne
  - et la DMZ,
  - et il filtre les paquets en fonction de règles de sécurité pour déterminer s'ils sont autorisés à passer à travers le pare-feu.

- Les paquets autorisés peuvent passer de la DMZ au réseau interne, tandis que les paquets non autorisés sont bloqués.

Cas une DMZ avec un pare-feu




Internal LAN
DMZ
Host
Router
Firewall
Internet

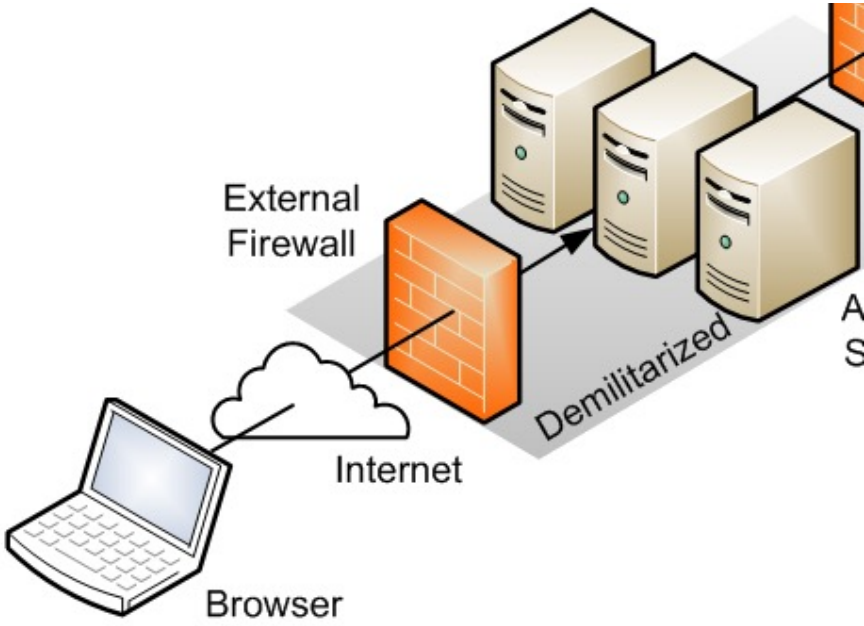

Internal LAN
Router
Firewall
Internet
DMZ Subnet - Servers
(Mail, DNS, Application)

Architecture avec une DMZ avec deux firewalls

Une architecture avec une DMZ utilisant deux pare-feu

- Est conçue pour fournir un niveau de sécurité accru

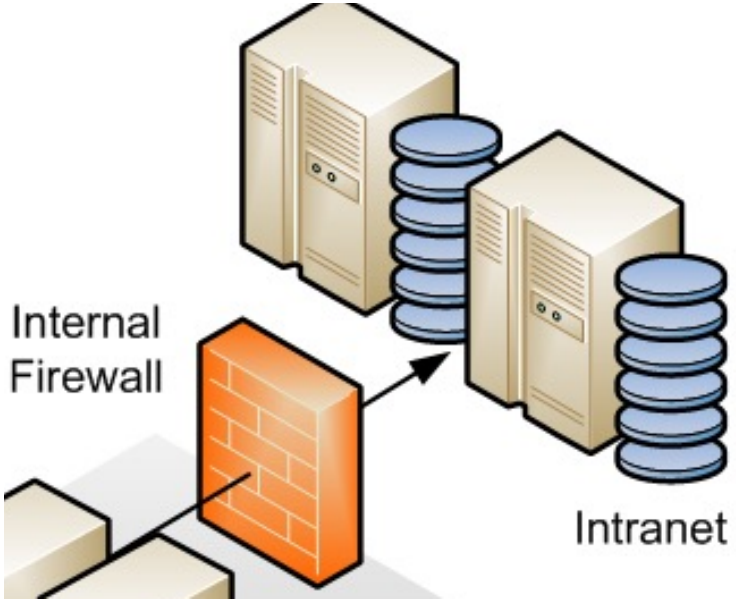
- Le premier pare-feu est placé entre le Internet et DMZ
  - Il filtre le trafic entrant,
  - permettant uniquement les connexions spécifiques aux services exposés dans la DMZ (serveurs web ou de messagerie).
  - La DMZ agit comme un tampon, isolant le réseau interne des accès directs depuis l'extérieur.



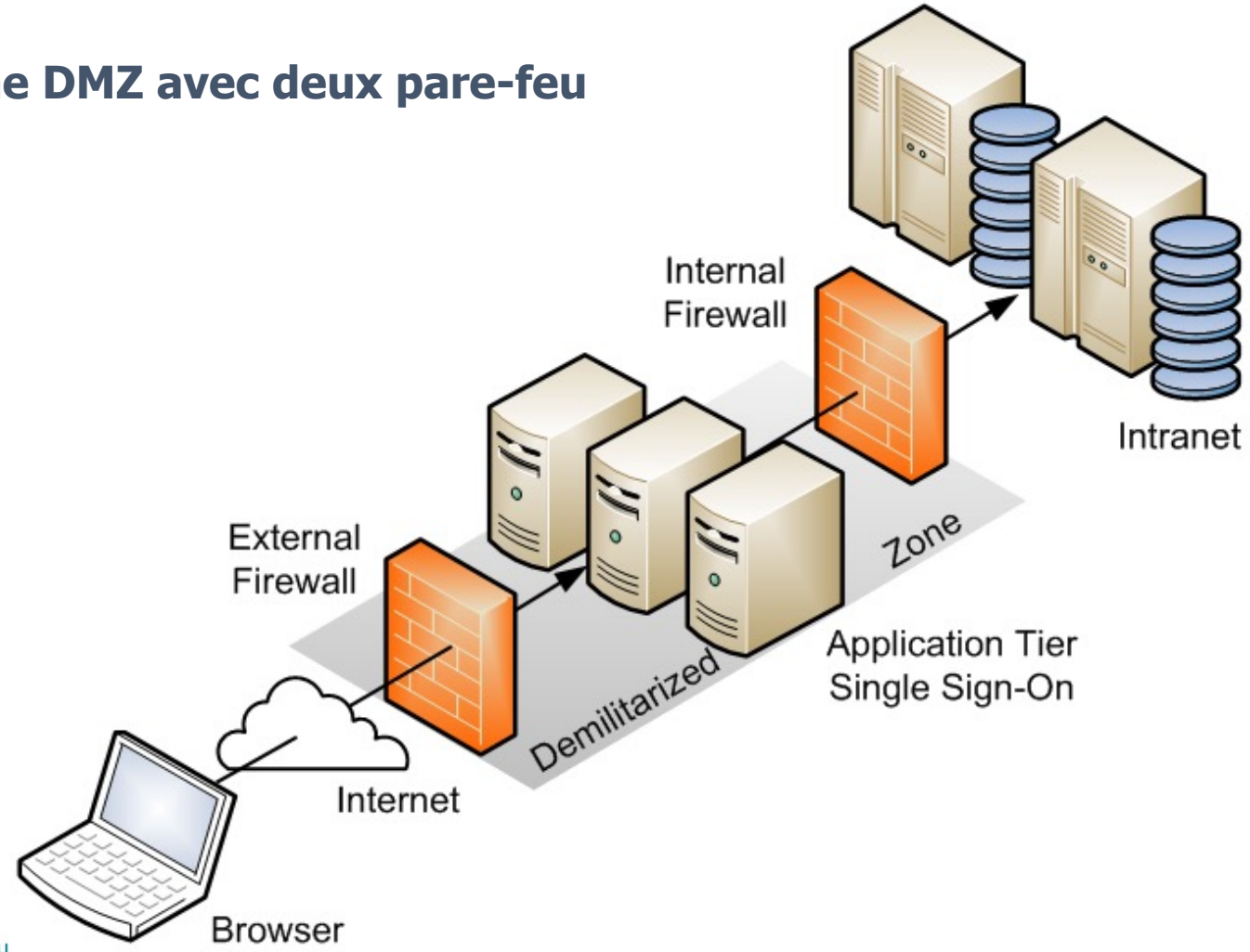
Une architecture avec une DMZ utilisant deux pare-feu

- Le second pare-feu contrôle l'accès
  - entre la DMZ et le réseau interne
  - garantissant que seul le trafic autorisé peut atteindre les ressources sensibles de l'entreprise.

  - permet de protéger les systèmes internes même en cas de compromission des services dans la DMZ.



Cas une DMZ avec deux pare-feu



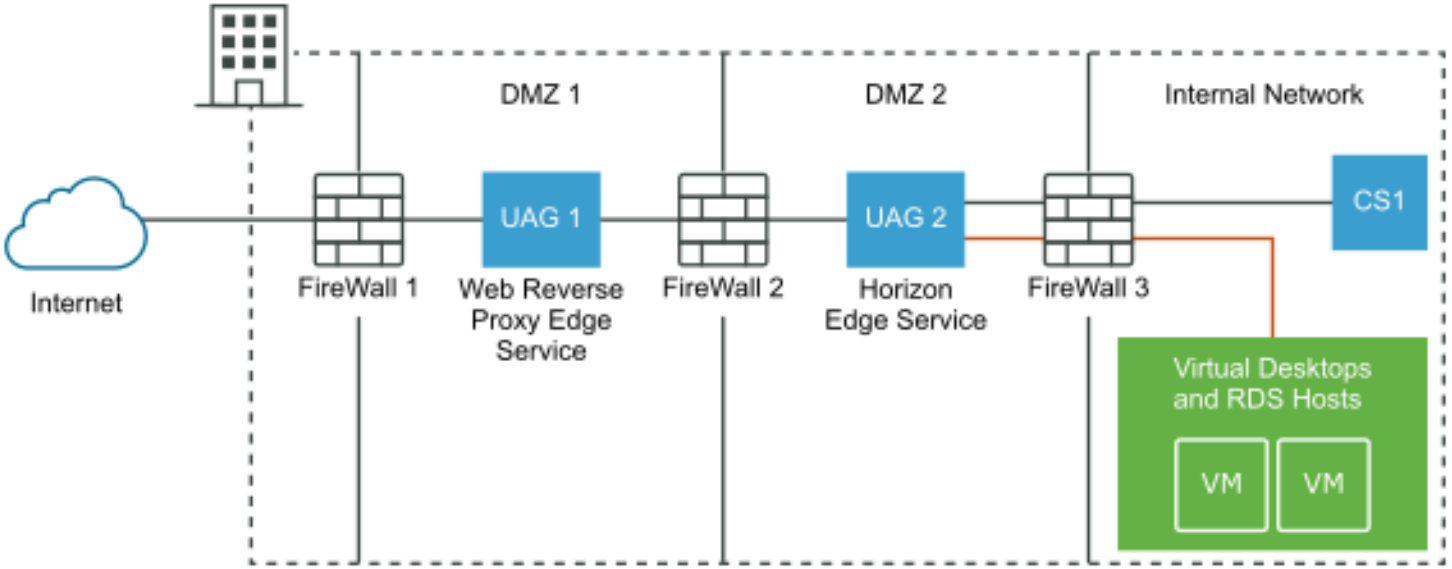
L'architecture à deux niveaux (DMZ)

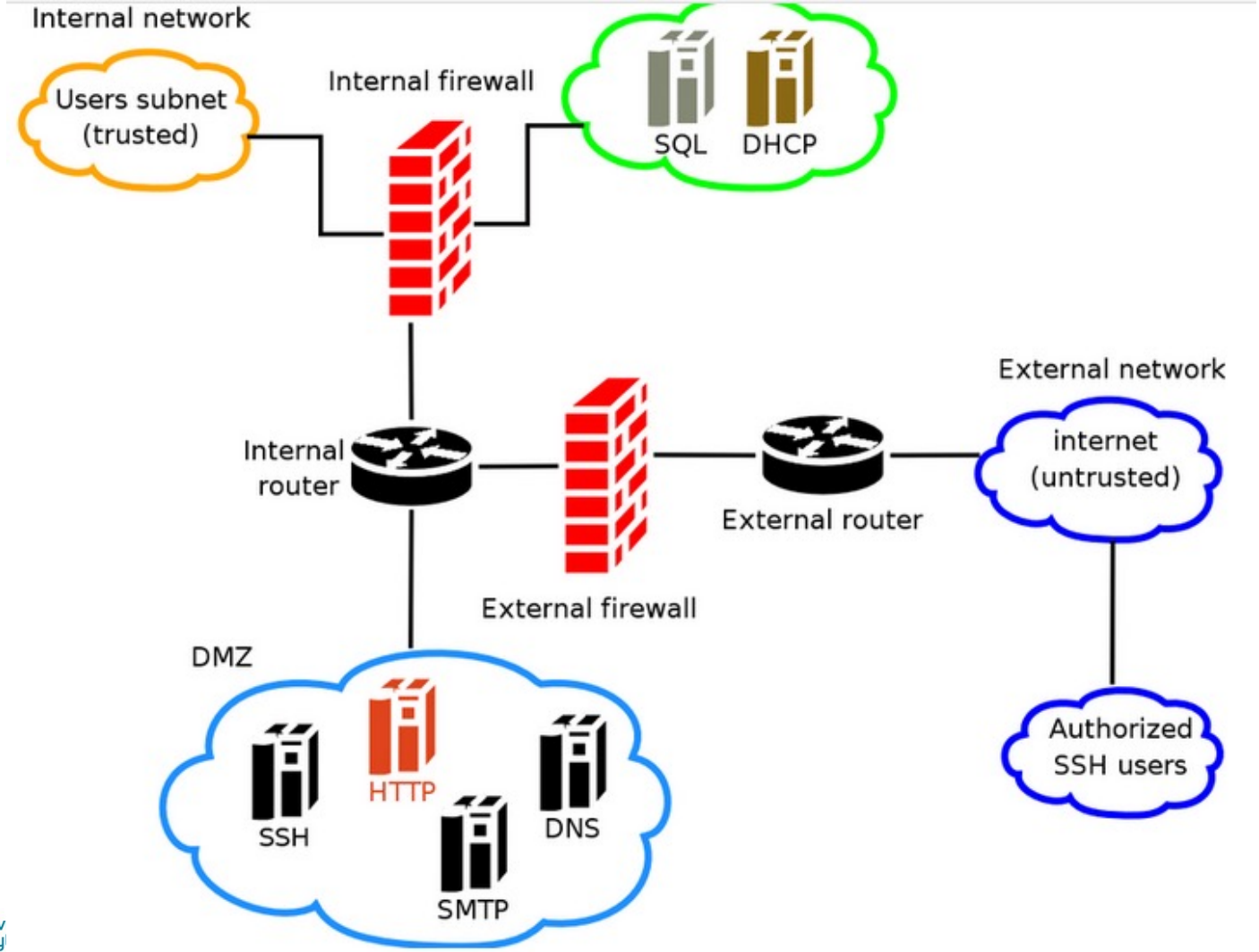
Principe

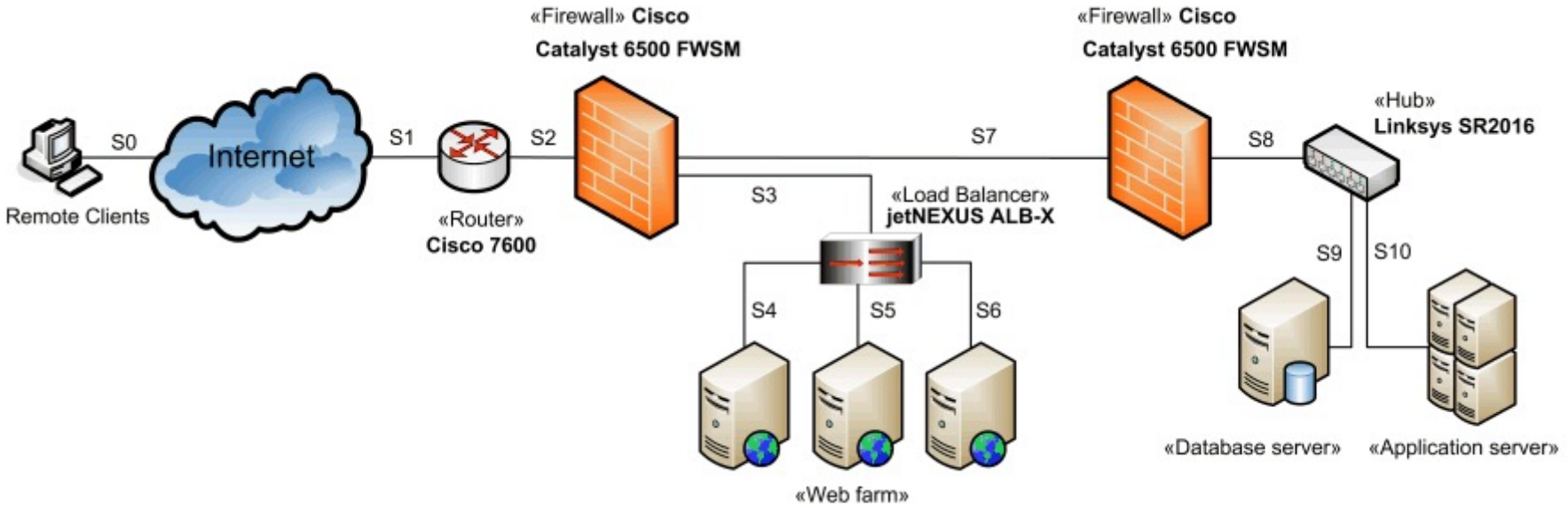
- L'architecture à **deux niveaux de DMZ (ou "double DMZ")** :
  - Elle implique la création de **deux zones** démilitarisées (DMZ)
  - distinctes
- **La première DMZ, ou "DMZ externe"**,
  - est située entre le pare-feu et le réseau Internet.
  - Elle contient des **serveurs accessibles publiquement**, tels que des serveurs Web ou de messagerie, qui nécessitent une connectivité Internet.

Principe

- **La deuxième DMZ, ou "DMZ interne",**
  - est située entre le **pare-feu et le réseau local de l'organisation**.
  - Elle contient des serveurs qui nécessitent un accès à la fois depuis Internet et depuis le réseau local.
  - Les serveurs dans cette zone sont souvent des serveurs de bases de données ou des serveurs d'authentification.
- En séparant les serveurs accessibles publiquement de ceux qui nécessitent un accès à partir du réseau local, les organisations peuvent mieux contrôler l'accès à leurs ressources sensibles.

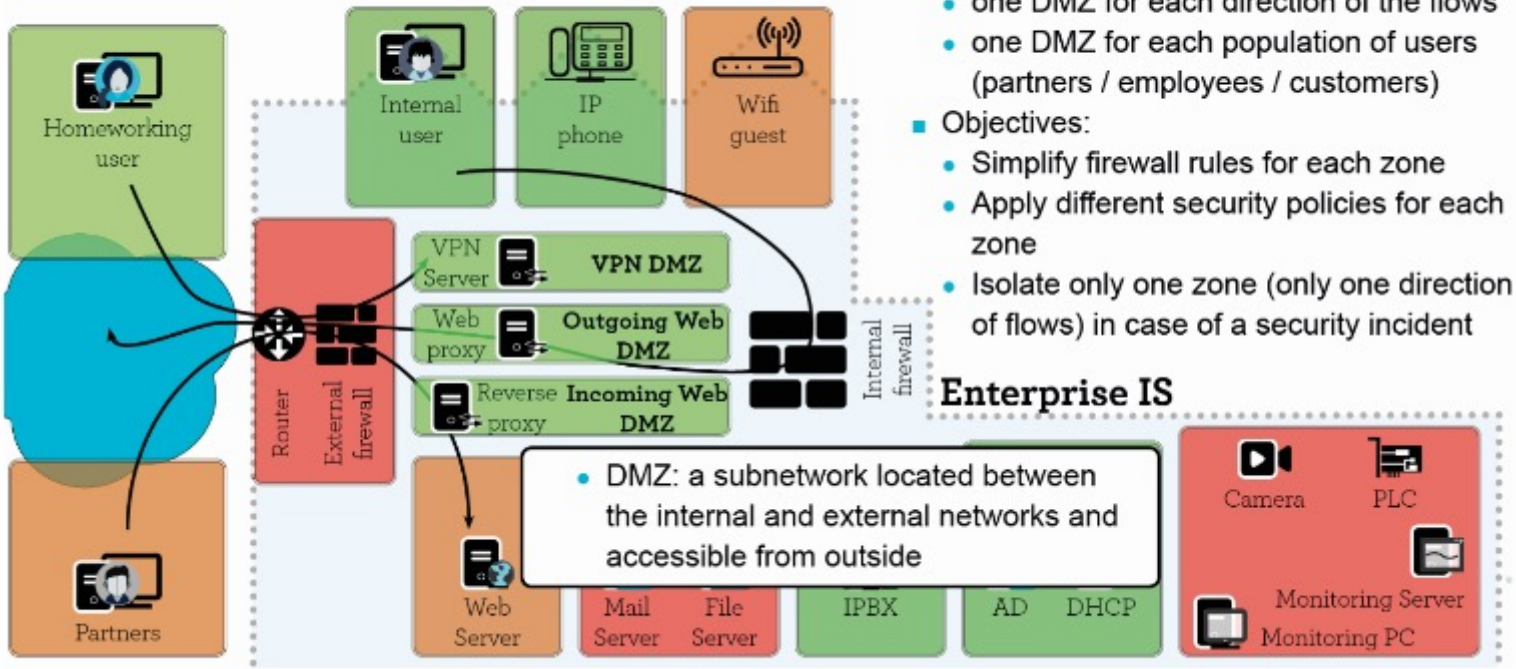

DMZ 1
DMZ 2
Internal Network
Internet
FireWall 1
UAG 1
Web Reverse
Proxy Edge
Service
FireWall 2
UAG 2
Horizon
Edge Service
FireWall 3
CS1
Virtual Desktops
and RDS Hosts
VM
VM


Internal network
Users subnet
(trusted)
Internal firewall
SQL
DHCP
External network
Internal
router
internet
(untrusted)
External router
External firewall
DMZ
HTTP
SSH
DNS
SMTP
Authorized
SSH users


«Firewall» Cisco
Catalyst 6500 FWSM
«Firewall» Cisco
Catalyst 6500 FWSM
«Hub»
Linksys SR2016
S0
Internet
S1
S2
S7
S8
Remote Clients
«Router»
Cisco 7600
S3
«Load Balancer»
jetNEXUS ALB-X
S9
S10
S4
S5
S6
«Database server»
«Application server»
«Web farm»

L'architecture à plusieurs

Several DMZ zones to separate incoming/outgoing accesses



- Several DMZs dedicated relatively to the purpose of the flows:
  - one DMZ for each direction of the flows
  - one DMZ for each population of users (partners / employees / customers)
- Objectives:
  - Simplify firewall rules for each zone
  - Apply different security policies for each zone
  - Isolate only one zone (only one direction of flows) in case of a security incident


FIN
INSA
INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
HAUTS-DE-FRANCE
Université
Polytechnique
HAUTS-DE-FRANCE