Cours 11 :

Pare-feu

JACQUEMIN Mathieu

Disclaimer

- Ce cours a été créé dans le but d'informer et d'éduquer les participants sur les sujets liés à la cybersécurité. L'ensemble des techniques présentées le sont à titre pédagogique et préventif afin de pouvoir se prémunir d'attaque potentiel.
- Certaines des techniques présentées sont illégales et dangereuses si elles sont utilisées à mauvais escient, sans maitrise, et sans consentement.
- Il est interdit d'utiliser ces techniques contre toute entité dont vous ne disposez pas le consentement. Dans le cadre d'un accord pour audit, il est obligatoire d'agir dans le cadre d'un contrat parfaitement défini, écrit, et signé par les deux parties.
- Vous devez respecter la loi en vigueur ainsi qu'utilisez les techniques avec éthique et responsabilité.
- Je me dédouane de toute responsabilité en cas de problème ou d'incidents à la suite de ce cours.
- Vous êtes seul responsable de l'usage fait des connaissances enseignées.

Rappel DICT

Les indicateurs de sécurité informatique

Disponibilité

Intégrité

Confidentialité

Traçabilité

Rappel DICT

Les indicateurs de sécurité informatique

Disponibilité → Accessible et utilisable

Intégrité → Source sure et non modifiée

Confidentialité → Seulement les personnes habilitées

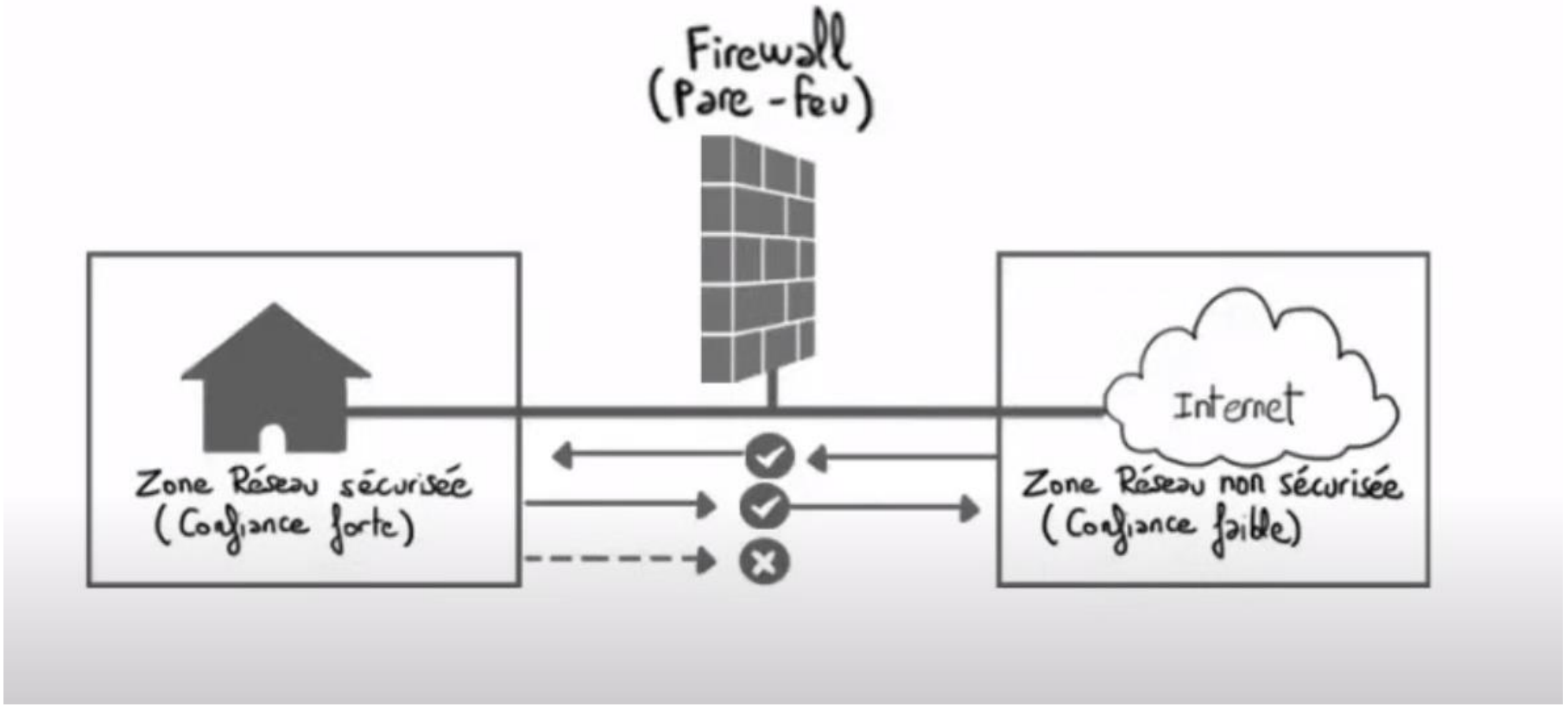
Traçabilité → Impossible de nier

Introduction

Firewall ou Pare-feu

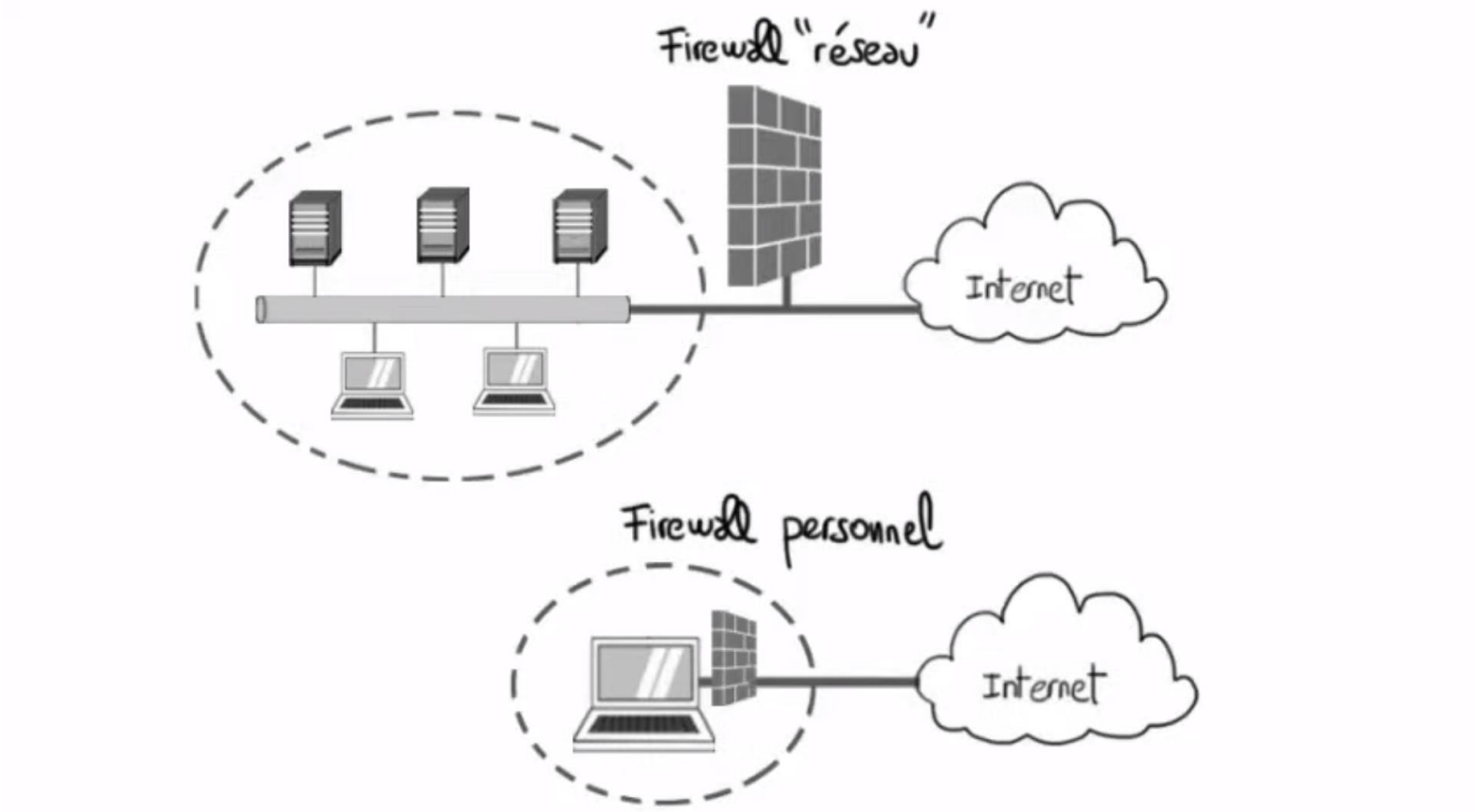
- Elément du réseau informatique
- Logiciel ou matériel
- Son rôle est de sécuriser un réseau en définissant les communications autorisées ou interdites
- Il permet d'interconnecter 2 réseaux ou plus de niveau de sécurité différent

Introduction



Le firewall joue un rôle de sécurité, en contrôlant les flux de données qui le traversent (en entrée ou en sortie)

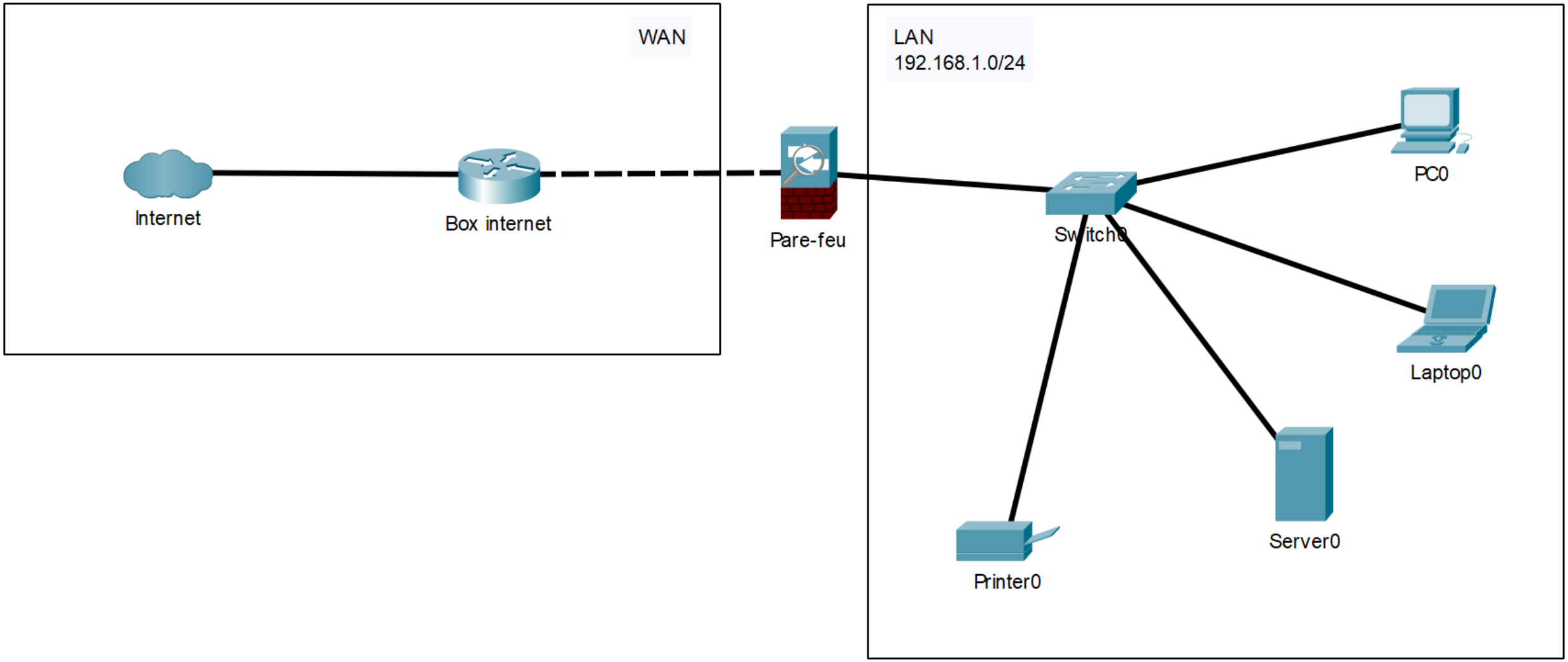
Introduction



Le firewall personnel permet de contrôler l'accès au réseau des applications installées sur ce seul poste de travail

A quoi ça ressemble ?

L'architecture



La politique de sécurité

C'est le fait d'exposer les besoins de l'entreprise (son utilisation d'Internet) et d'en déduire les règles qui lui permettent son bon fonctionnement, tout en sécurisant au maximum l'entreprise.

Bloquez tout et autorisez petit à petit

- Les utilisateurs ont besoin d'accéder au Web = ouverture port HTTP.
- Les utilisateurs ont besoin d'accéder à leurs mails = ouverture port POP ou IMAP.
- Le serveur doit être accessible depuis Internet = ouverture port HTTP

La politique de sécurité

Il n'y a pas de règles prédéfinies, chaque entreprise a un besoin particulier que vous devrez comprendre et analyser.

Les règles Firewall sont séquentielles, elles sont lues dans l'ordre. Les plus globales sont placées à la fin et les plus fines au début.

Les règles firewall

Voici les 3 arguments minimums qu'il vous faut pour créer une règle de pare-feu :

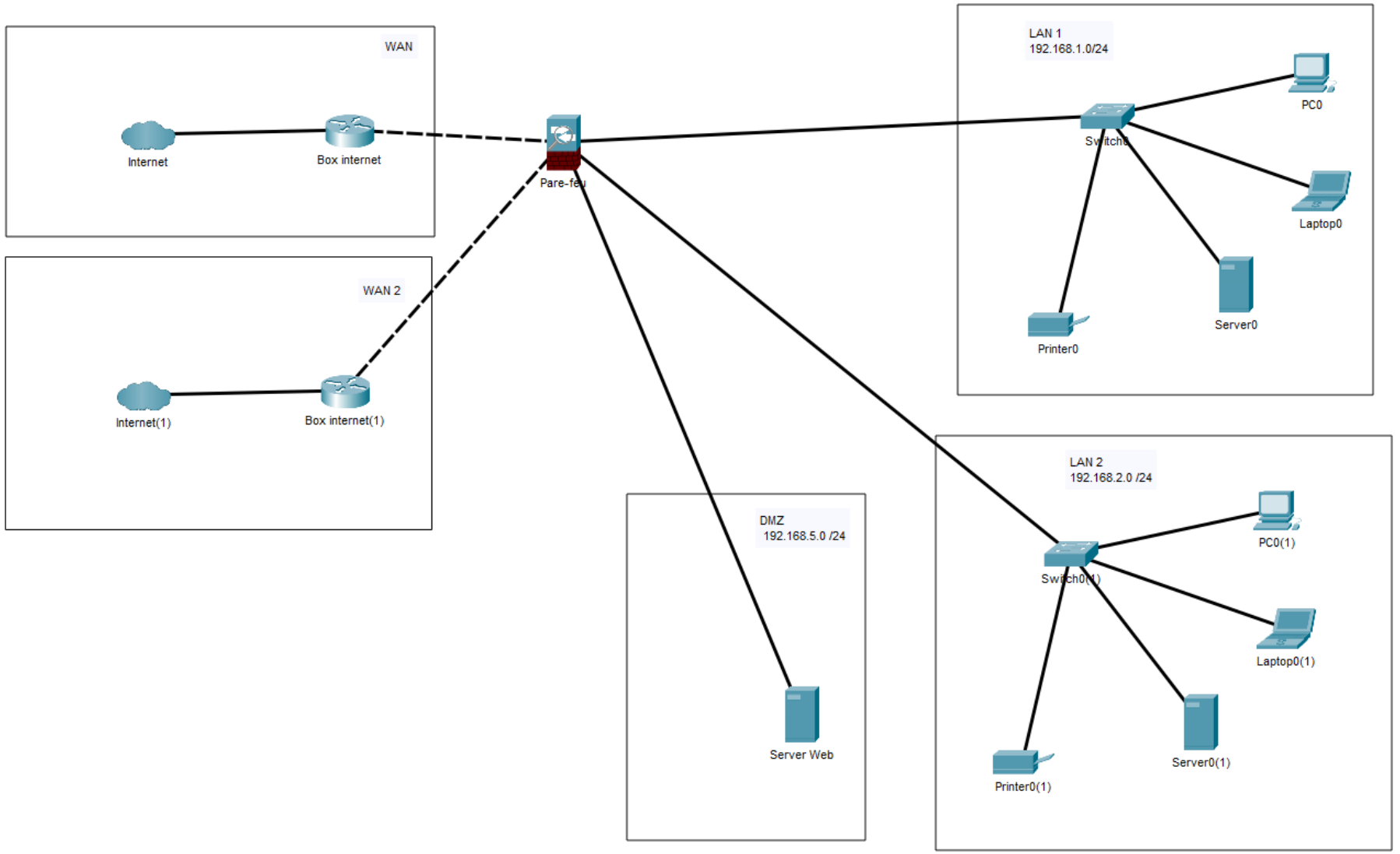
- **Interdiction ou autorisation du trafic**
- **Adresses sources et destinations**
- **Ports sources et destinations**

Exemple de règles

Règle	IP Source	Port Source	IP destination	Port destination	Protocole de transport
Autorise	*	*	*	80	TCP
Autorise	*	*	*	443	TCP
Interdit	*	*	*	*	*

Règle	IP Source	Port Source	IP destination	Port destination	Protocole de transport
Autorise	IP admin	22	IP serveur	22	TCP
Interdit	*	*	*	*	*

D'autres possibilités ?

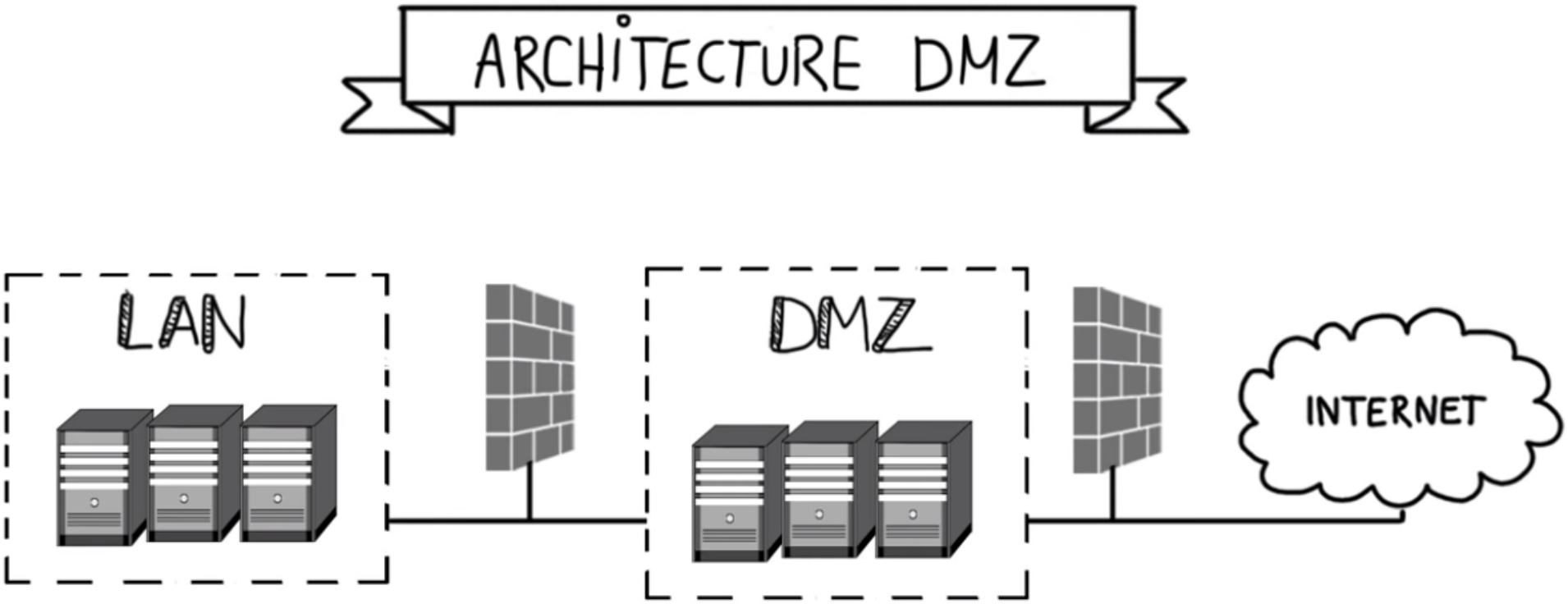


DMZ

Zone démilitarisée
Il s'agit d'un réseau séparé du réseau local et isolé de celui-ci ainsi que d'Internet par un pare-feu

Ce réseau contient les machines étant susceptibles d'être accédées depuis Internet, et qui n'ont pas besoin d'accéder au réseau local

DMZ



Les autres possibilités ?

IPS / IDS (Intrusion Prevention / Detection Systèmes) : L'IDS va analyser le trafic réseau pour détecter des signatures correspondant à des cyberattaques connues et l'IPS va protéger en bloquant les paquets en fonction du type d'attaques qu'il détecte, ce qui contribue à stopper ces attaques

Blocage par géolocalisation : Pour n'autoriser le contrôle à distance que depuis les pays que vos collaborateurs visitent, ou l'accès à votre FTP que depuis les pays où vous avez des clients.

Gestion par réputation : Cette défense consiste généralement à bloquer l'accès aux IP et aux URLs de sites connus comme dangereux ou potentiellement dangereux.

Contrôle applicatif : Permet de bloquer directement une application ou un service à la place d'une adresse IP ou d'un port.

Les autres possibilités ?

Bouclier Anti-DDOS : Certains Firewall fournissent des filtres spéciaux et combinent les boucliers IPS, Réputation et Géolocalisation des IP pour nettoyer les flux entrants, jeter les paquets provenant de sources indésirables et réduire l'impact des attaques.

Antivirus : Détecter et bloquer les malwares avant qu'ils n'entrent sur le réseau.

Antispam : Celui-ci analyse tous les emails entrants et élimine automatiquement ceux réputés comme dangereux soit parce qu'ils contiennent une pièce attachée vérolée, soit parce qu'ils contiennent un lien vers un site de phishing ou d'attaques par exploits.

Fonction DLP (Data Leak Prevention), Contrôle des utilisateurs, Outils de supervision, etc..

Lien sur Discord