Présentation du stage 7b

Olivier Levillain

ANSSI/CyberEdu

Journée CyberEdu à Nantes
19 avril 2018

Table des matières

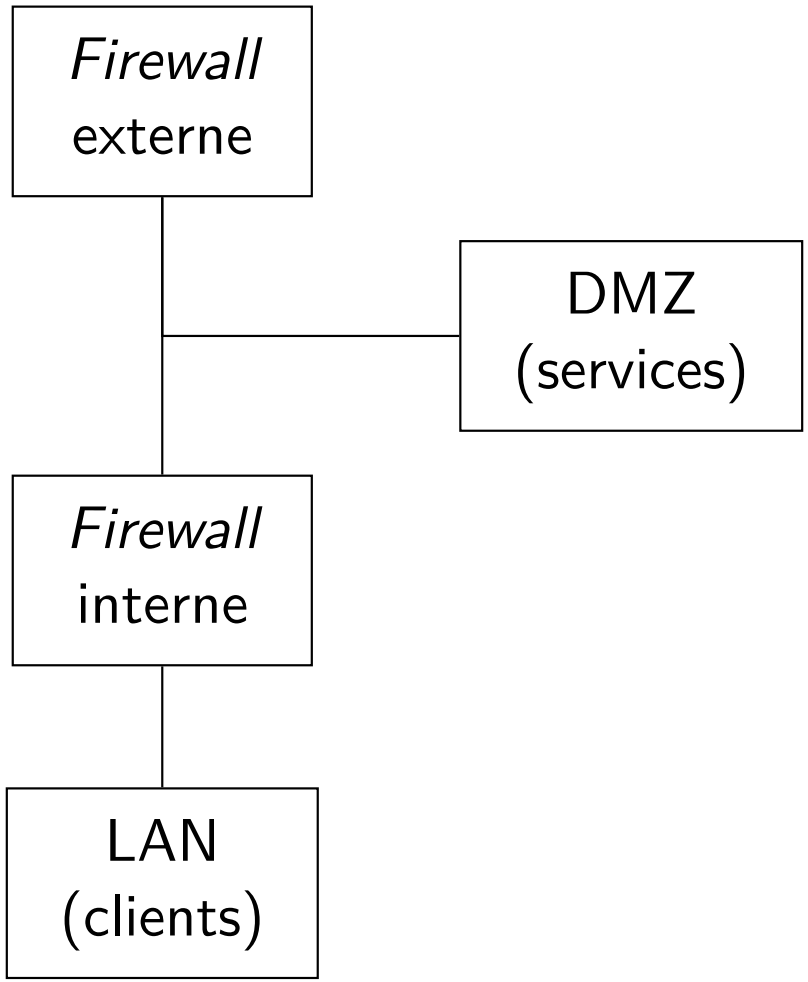
Table des matières

Aperçu

Stage 7b :

- 5 jours de TP
- installation de plusieurs systèmes d'exploitation
- mise en œuvre du filtrage réseau
- mise en place de plusieurs services (DNS, *mail*)
- sécurisation des échanges (TLS, S/MIME)
- nomadisme et tunnels IPsec

Architecture cible



Objectifs pédagogiques

Public visé

- administrateurs système et réseau
- architectes

Objectifs pédagogiques

Public visé

- administrateurs système et réseau
- architectes

Grands principes du stage

- notions d'architecture
  - la DMZ comme point de passage imposé
  - pour permettre le filtrage et la journalisation
- principe du moindre privilège
  - tout interdire, puis autoriser
  - réduction du périmètre sur les interfaces d'écoute
  - aspects système (OpenBSD, configuration fine)

Objectifs pédagogiques

Public visé

- administrateurs système et réseau
- architectes

Grands principes du stage

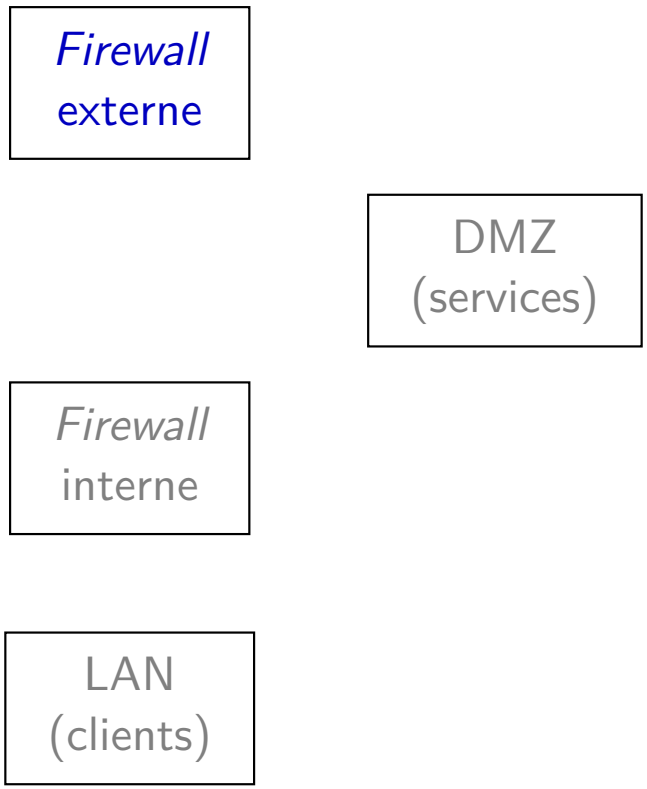
- notions d'architecture
  - la DMZ comme point de passage imposé
  - pour permettre le filtrage et la journalisation
- principe du moindre privilège
  - tout interdire, puis autoriser
  - réduction du périmètre sur les interfaces d'écoute
  - aspects système (OpenBSD, configuration fine)

Limitations

- ce n'est pas une liste de recettes à appliquer directement
- pas de modélisation de la supervision et de l'administration à distance
- pas de service d'annuaire

Table des matières

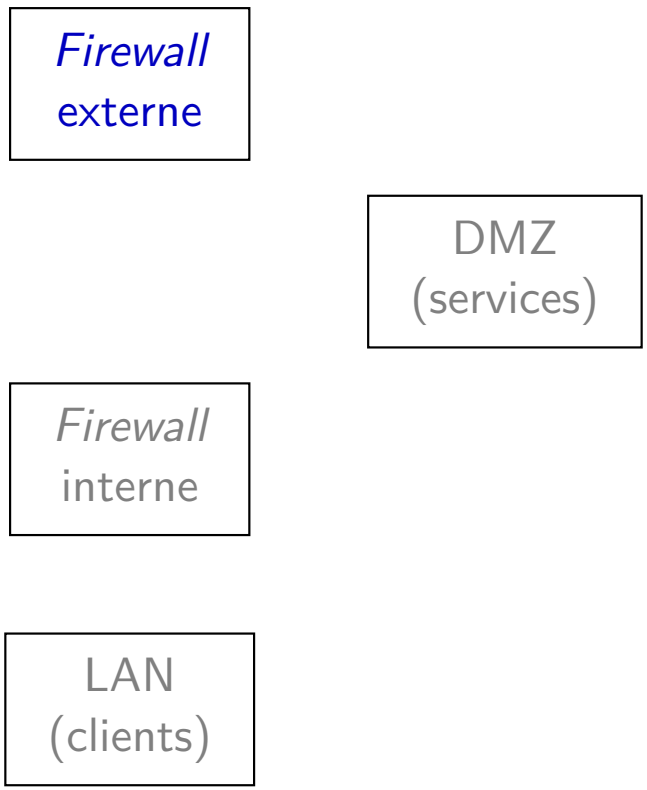
Jour 1 : installation du *firewall* externe



Firewall externe

- installation d'une distribution Debian
- configuration du système
- recompilation du noyau
- configuration du réseau

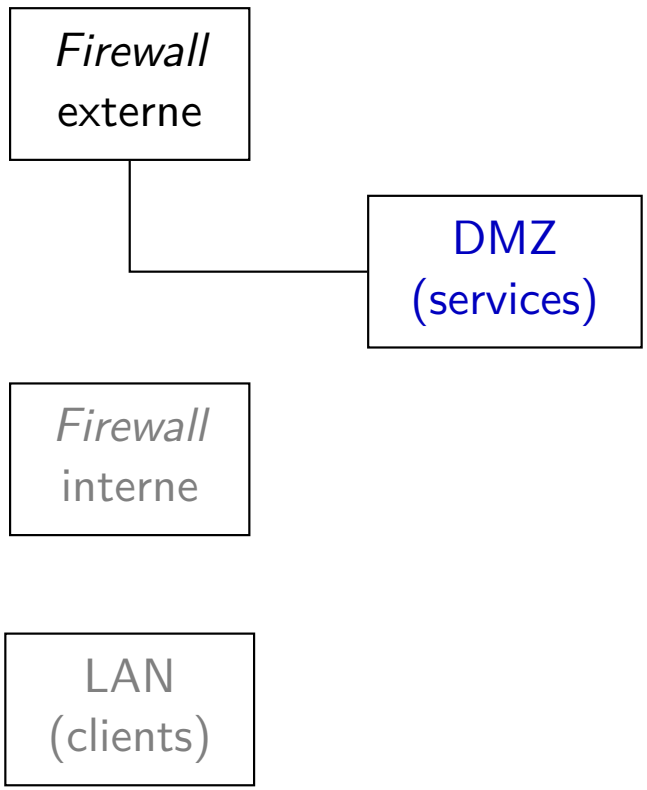
Jour 2 (matin) : configuration des règles de filtrage



Firewall externe

- prise en main d'`iptables`
- écriture des premières règles de filtrage
  - tout bloquer
  - autoriser la DMZ à sortir
- tests entre deux FWe

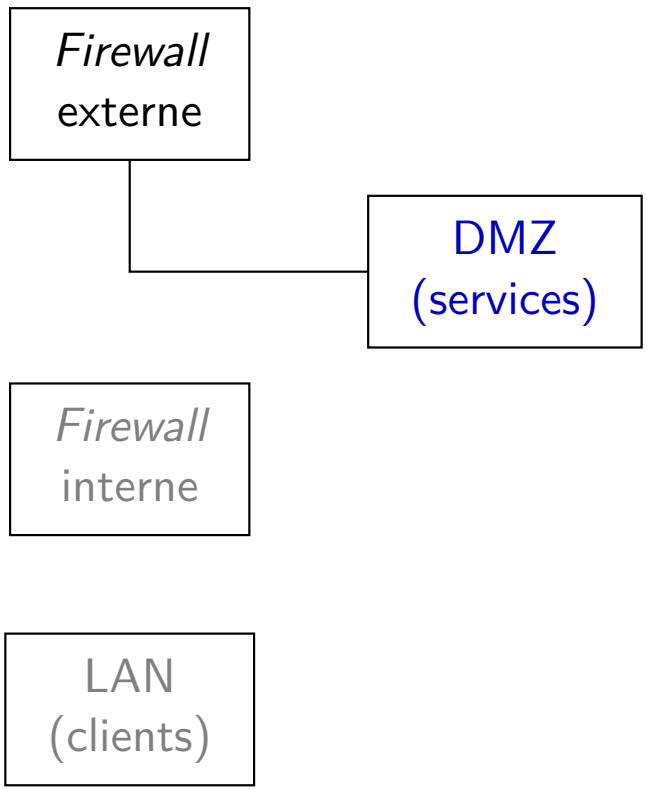
Jour 2 (après-midi) : installation de la machine DMZ



DMZ

- installation d'OpenBSD
- analyse de sécurité du système
  - `chroot` et descente de privilège
  - processus lancés
  - services en écoute

Jour 2 (après-midi) : installation de la machine DMZ



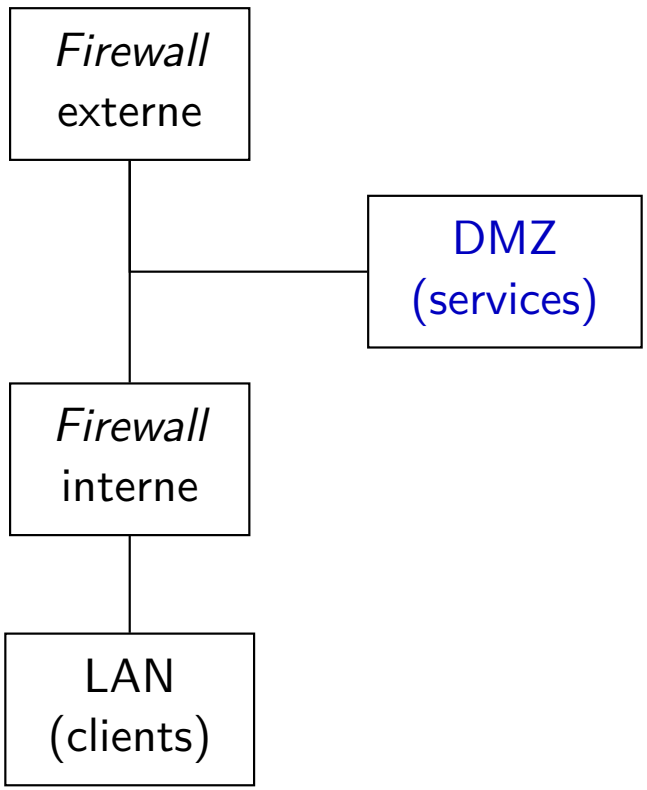
DMZ

- installation d'OpenBSD
- analyse de sécurité du système
  - `chroot` et descente de privilège
  - processus lancés
  - services en écoute

Firewall externe

- test des règles de filtrage depuis la DMZ

Jour 2 (après-midi) : installation de la machine DMZ



DMZ

- installation d'OpenBSD
- analyse de sécurité du système
  - `chroot` et descente de privilège
  - processus lancés
  - services en écoute

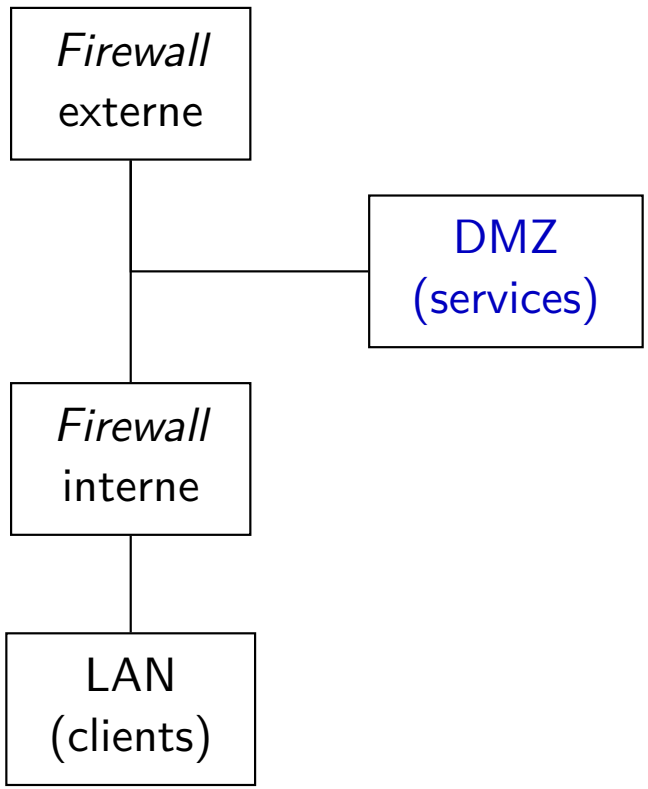
Firewall externe

- test des règles de filtrage depuis la DMZ

Firewall interne et LAN préinstallés

- test des flux

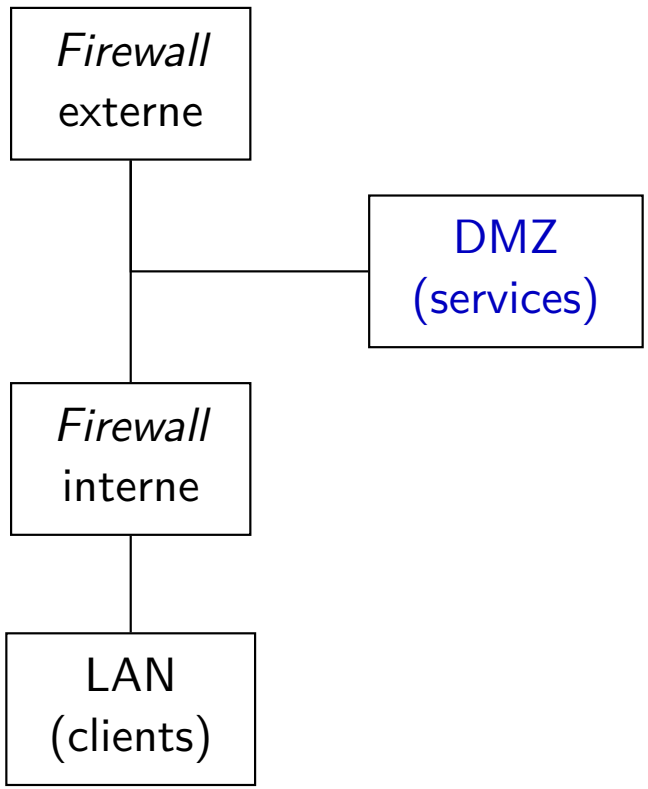
Jour 3 (matin) : service DNS



DMZ

- installation de `bind`
- configuration de deux vues
  - vue publique des services
  - vue interne pour le LAN

Jour 3 (matin) : service DNS



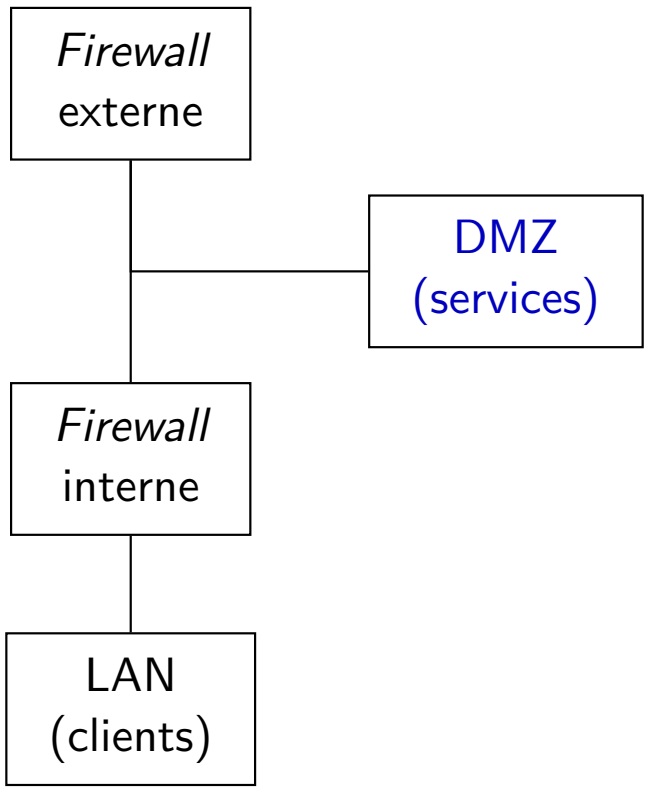
DMZ

- installation de `bind`
- configuration de deux vues
  - vue publique des services
  - vue interne pour le LAN

Firewall externe

- ajout de règles pour ouvrir le flux depuis l'extérieur

Jour 3 (matin) : service DNS



DMZ

- installation de `bind`
- configuration de deux vues
  - vue publique des services
  - vue interne pour le LAN

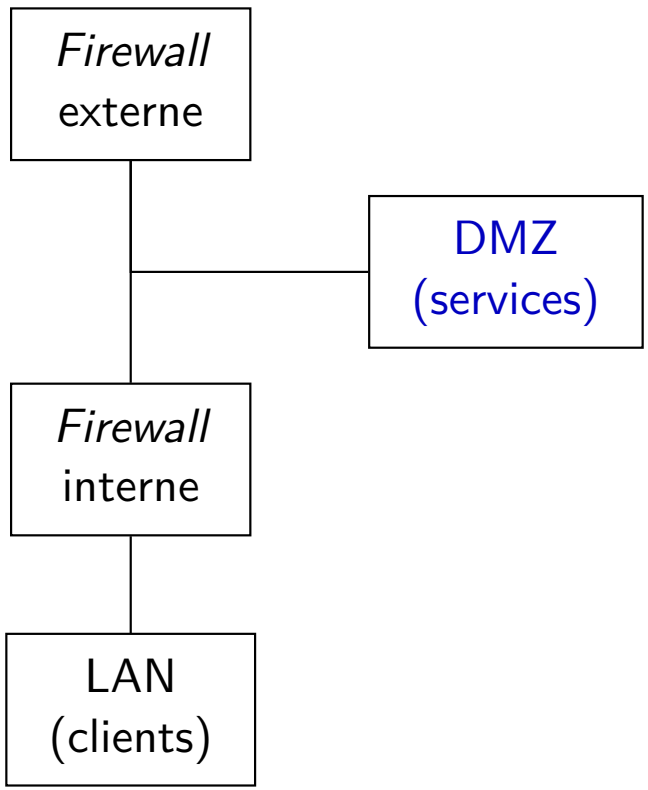
Firewall externe

- ajout de règles pour ouvrir le flux depuis l'extérieur

LAN

- test DNS local
- test DNS dans d'autres groupes

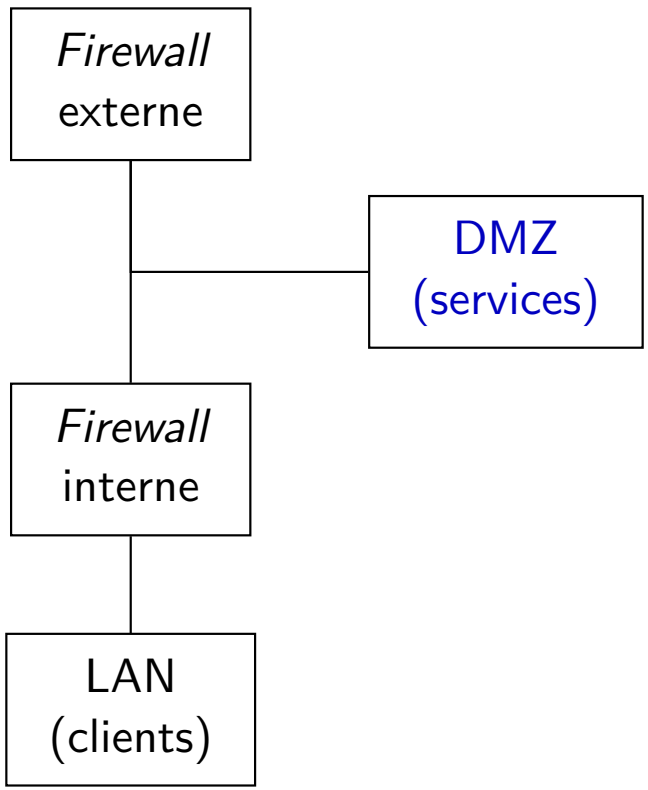
Jour 3 (après-midi) : messagerie électronique (1/2)



DMZ

- installation de `postfix`
  - étude de l'architecture de `postfix`
- deux serveurs SMTP
  - service public
  - service interne

Jour 3 (après-midi) : messagerie électronique (1/2)



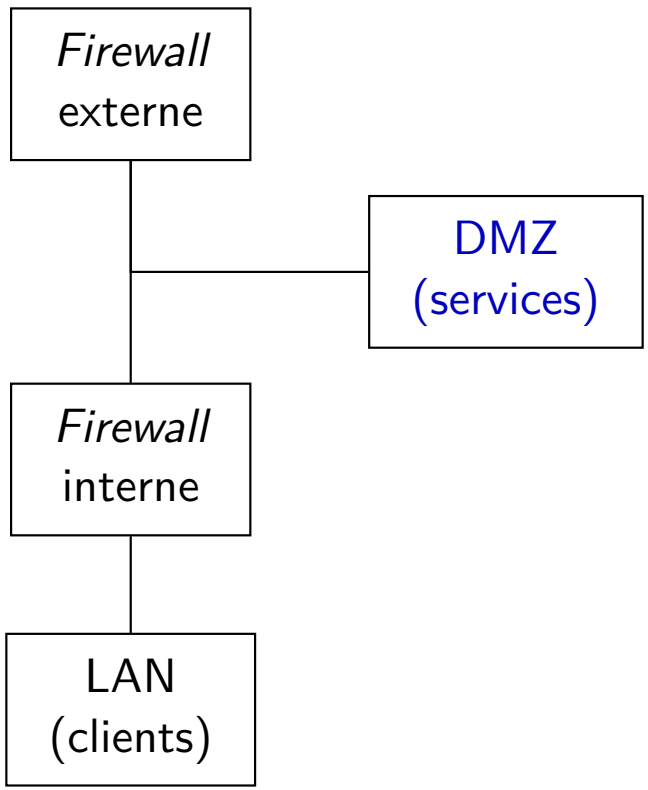
DMZ

- installation de `postfix`
  - étude de l'architecture de `postfix`
- deux serveurs SMTP
  - service public
  - service interne

Firewall externe

- ajout de règles pour ouvrir le flux depuis l'extérieur

Jour 3 (après-midi) : messagerie électronique (1/2)



DMZ

- installation de `postfix`
  - étude de l'architecture de `postfix`
- deux serveurs SMTP
  - service public
  - service interne

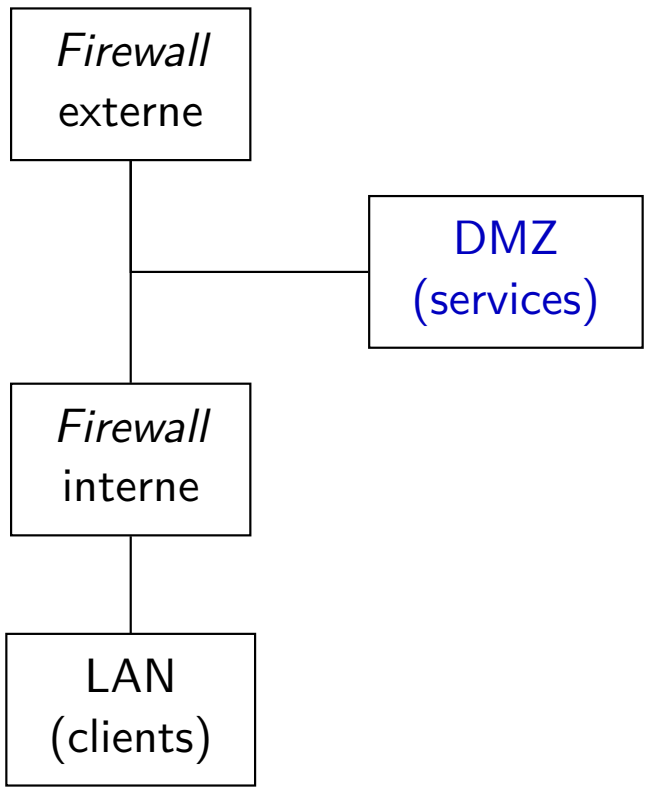
Firewall externe

- ajout de règles pour ouvrir le flux depuis l'extérieur

DMZ

- test local et entre deux DMZ

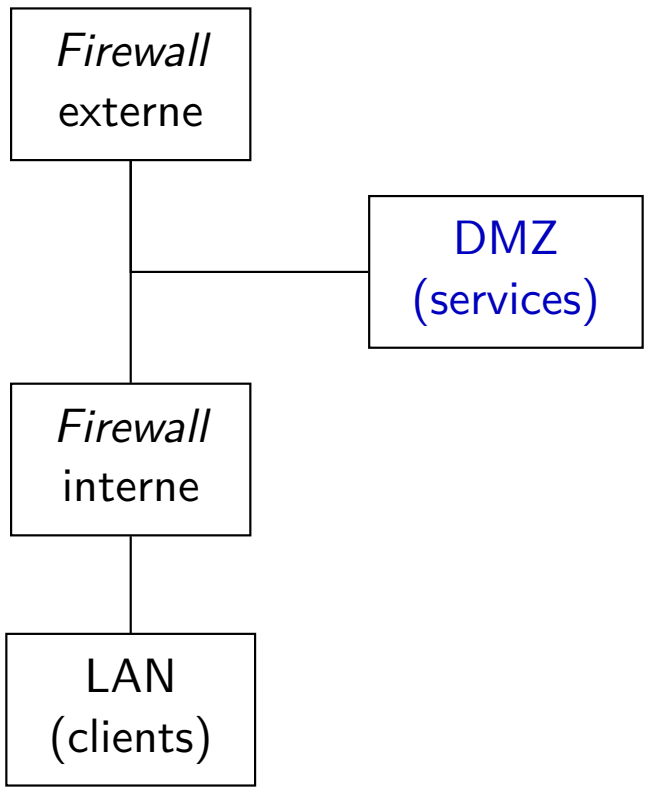
Jour 3 (après-midi) : messagerie électronique (2/2)



DMZ

- installation de `cyrus`
- gestion de l'authentification
- branchement de `postfix`

Jour 3 (après-midi) : messagerie électronique (2/2)



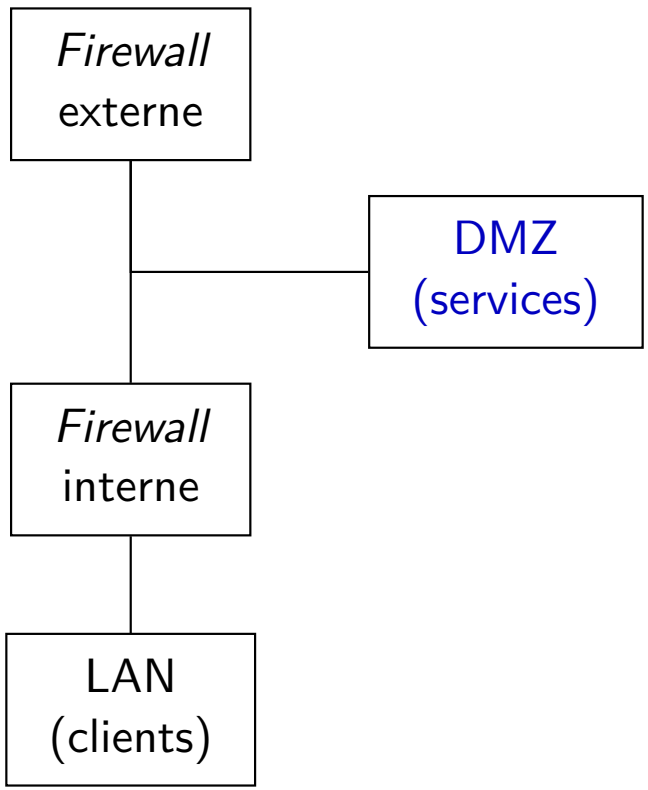
DMZ

- installation de `cyrus`
- gestion de l'authentification
- branchement de `postfix`

Firewall externe

- ajout de règles pour ouvrir le flux depuis l'extérieur

Jour 3 (après-midi) : messagerie électronique (2/2)



DMZ

- installation de `cyrus`
- gestion de l'authentification
- branchement de `postfix`

Firewall externe

- ajout de règles pour ouvrir le flux depuis l'extérieur

LAN

- tests SMTP (local/distant)
- tests IMAP

Jour 4 (matin) : IGC

Constat : les mails sont stockés en clair et sont modifiables sur la DMZ

Jour 4 (matin) : IGC

Constat : les mails sont stockés en clair et sont modifiables sur la DMZ

- création d'une autorité de certification locale
- raccrochage à une racine
- génération de certificats S/MIME

Jour 4 (matin) : IGC

Constat : les mails sont stockés en clair et sont modifiables sur la DMZ

- création d'une autorité de certification locale
- raccrochage à une racine
- génération de certificats S/MIME

- installation des certificats sur le client

Jour 4 (matin) : IGC

Constat : les mails sont stockés en clair et sont modifiables sur la DMZ

- création d'une autorité de certification locale
- raccrochage à une racine
- génération de certificats S/MIME

- installation des certificats sur le client

- tests avec différents logiciels
- vérification sur la DMZ et atteinte à l'intégrité

Jour 4 (après-midi) : TLS

Constat : les communications ne sont pas protégées

Jour 4 (après-midi) : TLS

Constat : les communications ne sont pas protégées

- présentation de TLS
  - objectifs de sécurité
  - TLS implicite ou explicite ?
  - paramètres nécessaires : activation, certificat, clé privée, chaîne
  - paramètres complémentaires : suites, version

Jour 4 (après-midi) : TLS

Constat : les communications ne sont pas protégées

- présentation de TLS
  - objectifs de sécurité
  - TLS implicite ou explicite ?
  - paramètres nécessaires : activation, certificat, clé privée, chaîne
  - paramètres complémentaires : suites, version
- génération de certificats TLS
- installation sur `postfix` et `cyrus`

Jour 4 (après-midi) : TLS

Constat : les communications ne sont pas protégées

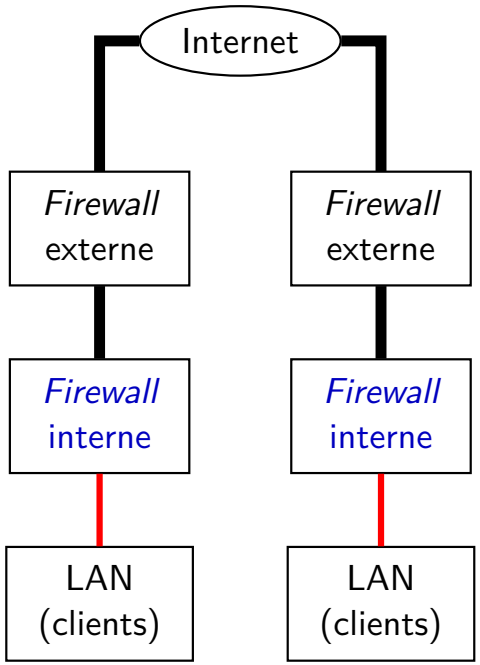
- présentation de TLS
  - objectifs de sécurité
  - TLS implicite ou explicite ?
  - paramètres nécessaires : activation, certificat, clé privée, chaîne
  - paramètres complémentaires : suites, version
- génération de certificats TLS
- installation sur `postfix` et `cyrus`
- tests avec `openssl s_client`
- tests avec les clients du LAN et `wireshark`

Jour 4 (après-midi) : TLS

Constat : les communications ne sont pas protégées

- présentation de TLS
  - objectifs de sécurité
  - TLS implicite ou explicite ?
  - paramètres nécessaires : activation, certificat, clé privée, chaîne
  - paramètres complémentaires : suites, version
- génération de certificats TLS
- installation sur `postfix` et `cyrus`
- tests avec `openssl s_client`
- tests avec les clients du LAN et `wireshark`
- lorsque le temps le permet, HTTP et HTTPS avec authentification client par certificat

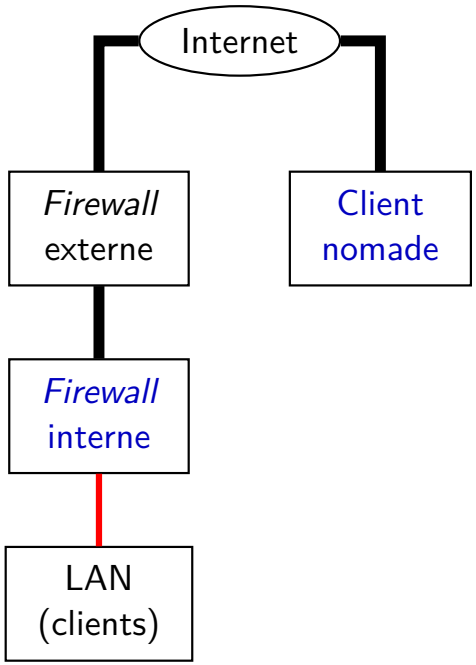
Jour 5 : IPsec (1/2)



Mise en place d'IPsec entre deux groupes

- présentation des concepts
- configuration de `strongswan` sur FWi
- autorisation des flux sur FWe
- test entre deux LAN distants

Jour 5 : IPsec (2/2)



Mise en place d'IPsec pour le nomadisme

- configuration de la pile IPsec Windows sur le client nomade
- test d'interopérabilité
- accès aux services de la DMZ

Table des matières

Comprendre et résoudre les problèmes

En marge du *happy path* décrit jusqu'ici, des problèmes peuvent apparaître

- erreur de règles de filtrage
- mauvaise configuration réseau
- services mal configurés
- problèmes de droits sur certains fichiers

Comprendre et résoudre les problèmes

En marge du *happy path* décrit jusqu'ici, des problèmes peuvent apparaître

- erreur de règles de filtrage
- mauvaise configuration réseau
- services mal configurés
- problèmes de droits sur certains fichiers

Comment identifier et réparer les problèmes

- toujours impliquer les stagiaires dans la démarche
- outils classiques pour analyser la situation
  - `tcpdump`
  - `iptables -L -v -n`
  - journaux dans `/etc/log` pour les services

Simplifier et séparer les usages

Plusieurs exemples de séparation permettant une architecture plus simple

- la DMZ en sandwich
- les deux vues DNS
- les deux serveurs SMTP

Simplifier et séparer les usages

Plusieurs exemples de séparation permettant une architecture plus simple

- la DMZ en sandwich
- les deux vues DNS
- les deux serveurs SMTP

Intérêt de cette simplification

- configuration plus simple et plus auditable
  - pas de serveur DNS récursif pour l'extérieur
  - pas de relais ouvert SMTP
- flux plus maîtrisés

Comprendre et tester

Objectif : comprendre le fonctionnement des protocoles et des services

- présentation des concepts avec des rappels de cours

Comprendre et tester

Objectif : comprendre le fonctionnement des protocoles et des services

- présentation des concepts avec des rappels de cours
- utilisation d'outils *bas niveau* pour comprendre
  - établissement de connexions TLS avec `openssl`
  - étude des *mails* stockés par `cyrus`
  - suivi des connexions avec `iptables -L -v`

Comprendre et tester

Objectif : comprendre le fonctionnement des protocoles et des services

- présentation des concepts avec des rappels de cours
- utilisation d'outils *bas niveau* pour comprendre
  - établissement de connexions TLS avec `openssl`
  - étude des *mails* stockés par `cyrus`
  - suivi des connexions avec `iptables -L -v`
- tests de sécurité (tests négatifs)
  - les services écoutent-ils en clair
  - STARTTLS est-il contournable
  - vérification de la détection d'une atteinte à l'intégrité d'un message

Conclusion

Le stage 7b propose une vision technique de la mise en place d'un système d'information

- un stage qui a 15 ans
- objectif principal : comprendre les concepts et les mécanismes

Conclusion

Le stage 7b propose une vision technique de la mise en place d'un système d'information

- un stage qui a 15 ans
- objectif principal : comprendre les concepts et les mécanismes

- prise en compte des évolutions dans les technologies
- des revues de programme régulières

Conclusion

Le stage 7b propose une vision technique de la mise en place d'un système d'information

- un stage qui a 15 ans
- objectif principal : comprendre les concepts et les mécanismes

- prise en compte des évolutions dans les technologies
- des revues de programme régulières

- les sujets abordés ne se cantonnent pas au réseau (système, crypto)
- la sécurité est un tout

Conclusion

Le stage 7b propose une vision technique de la mise en place d'un système d'information

- un stage qui a 15 ans
- objectif principal : comprendre les concepts et les mécanismes

- prise en compte des évolutions dans les technologies
- des revues de programme régulières

- les sujets abordés ne se cantonnent pas au réseau (système, crypto)
- la sécurité est un tout

Des limitations connues et assumées

- utilisation d'un système peu courant (OpenBSD)
- pas de supervision ni d'administration à distance
- pas de gestion de l'annuaire

Questions ?

Merci de votre attention.