Séminaire de Formation:

Mise en place et sécurisation des réseaux LAN et WAN

07, 08 et 09 Décembre 2009
Nefta-Tozeur, Tunisie

Atelier 2:
Mise en place d'une zone démilitarisée (DMZ)

Intervenant : Hedi MAGROUN

Plan

- Concept de DMZ
  - Besoin
  - Définition et Principe
  - Adressage
  - Placement des services
  - DMZ multiples
- Manipulation

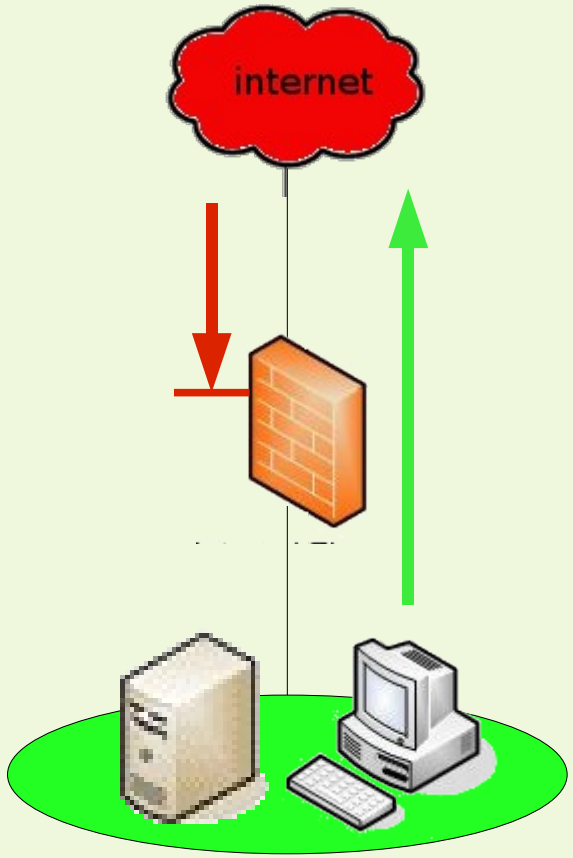
Concept de « DMZ »

Besoin

- Une entreprise (ou un organisme) a **besoin** d'**accéder** à des ressources sur Internet, d'en **exporter** mais aussi de se **protéger**
- L'architecture du réseau de l'entreprise est définie selon les **besoins**:
  - **accéder + protéger**
  - **accéder + exporter + protéger**

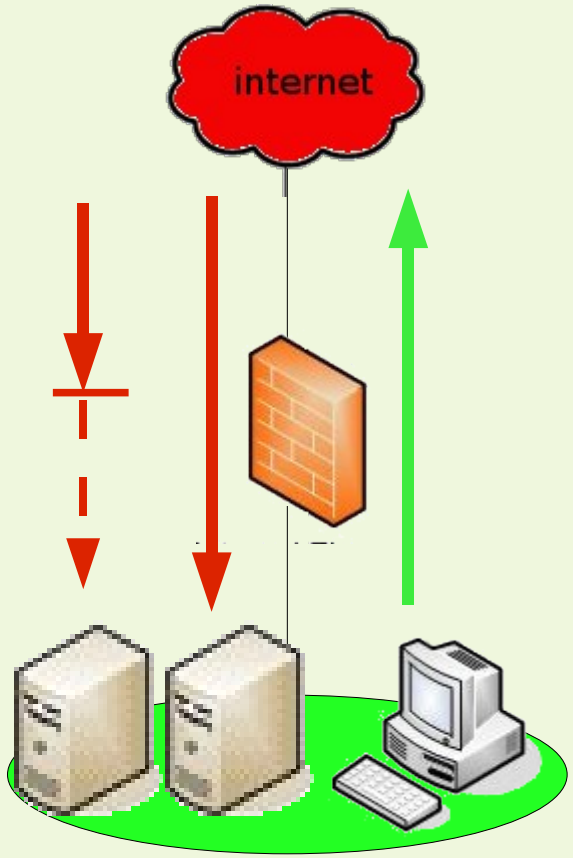
Besoin : accéder + protéger

- Réseau interne (privé):
  - Accès à l'extérieur
  - **Contient des données privées** *(exemple : s. BD, ...)*
- Réseau externe (Internet):
  - Considéré peuplé de volontés malfaisantes
- Pare-feu (firewall):
  - Règle:
    Réseau externe **NE DOIT PAS** accéder au réseau interne



Besoin : accéder + exporter + protéger

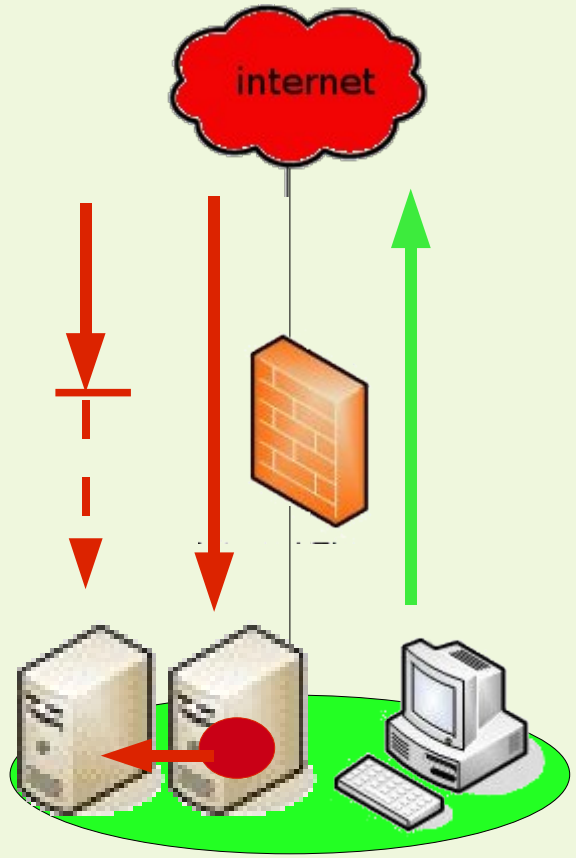
- Réseau interne (privé):
  - **Contient des données privées**
  - **Contient des données publique** *(exemple : s. web)*
  - Accès à l'extérieur
- Réseau externe (Internet):
  - Considéré peuplé de volontés malfaisantes
- Pare-feu (firewall)
  - Règle : Réseau externe accède aux **données publique** mais pas aux **données privées**



Besoin : accéder + exporter + protéger

PROBLEME :

*un attaquant obtenant **un accès** sur une machine contenant des **données publiques** peut **attaquer** à partir de là les machines contenant des **données privées***



Besoin : accéder + exporter + protéger

SOLUTION :

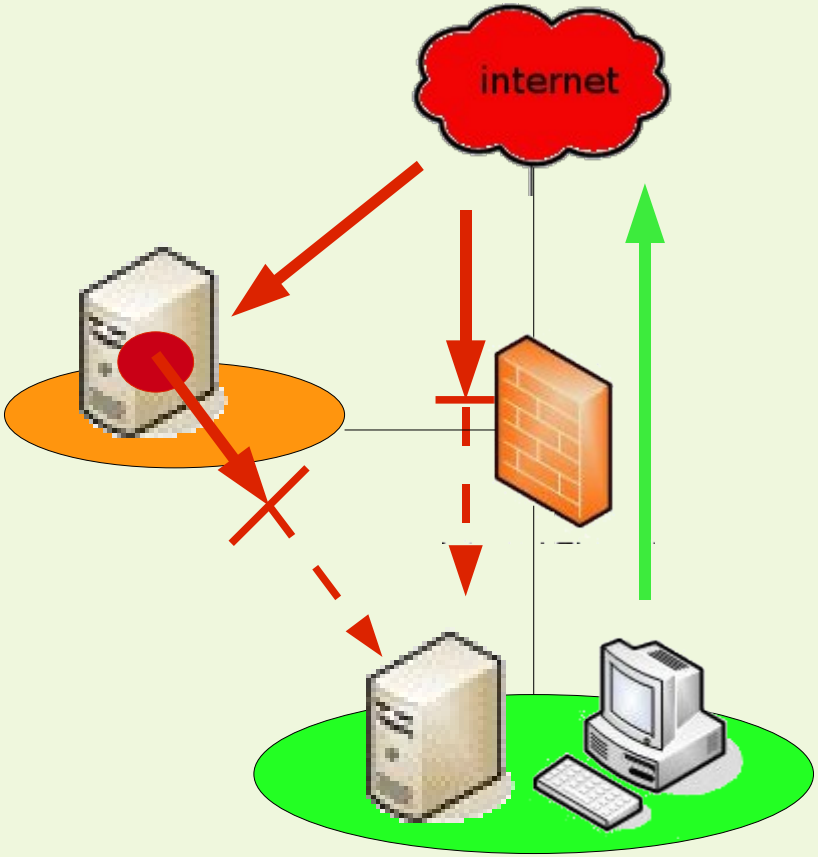
- Diviser le réseau interne en 2 sous-réseaux:
  - Réseau internet 1:
    - **Contient des données publique**
  - Réseau internet 2:
    - **Contient des données privées**
    - Accès à l'extérieur
- Pare-feu:
  - ...
  - Contrôler le trafic entre les réseaux internes 1 et 2

Besoin : accéder + exporter + protéger

SOLUTION : (suite)

*un attaquant obtenant un **accès** sur une machine contenant des **données publiques** peut **attaquer** à partir de là une autre machine contenant des **données publiques** mais **pas** celles contenant des **données privées***

« C'est le découpage en DMZ »



Définition et principe

- DMZ = **D**e**M**ilitarised **Z**one
  (zone démilitarisée)
- Définition:

  *Une **zone démilitarisée** est un sous-réseau isolé par un pare-feu. Ce sous-réseau contient des machines se situant entre :*

  - *un **réseau interne** (réseau privé) et*
  - *un **réseau externe** (Internet)*

Définition et principe

Découpage en DMZ :

1 Réseau** est divisé en **3 Réseaux ou +

1. Réseau interne (réseau privé) :

- Contenant les postes clients ayant besoin d'accéder à l'extérieur
- Contient des **données privées** qui ne doivent pas être consultées de l'extérieur

-> ***besoin de sécurité interne***

2. Réseau externe (Internet) :

- Considéré peuplé de volontés malfaisantes

Définition et principe

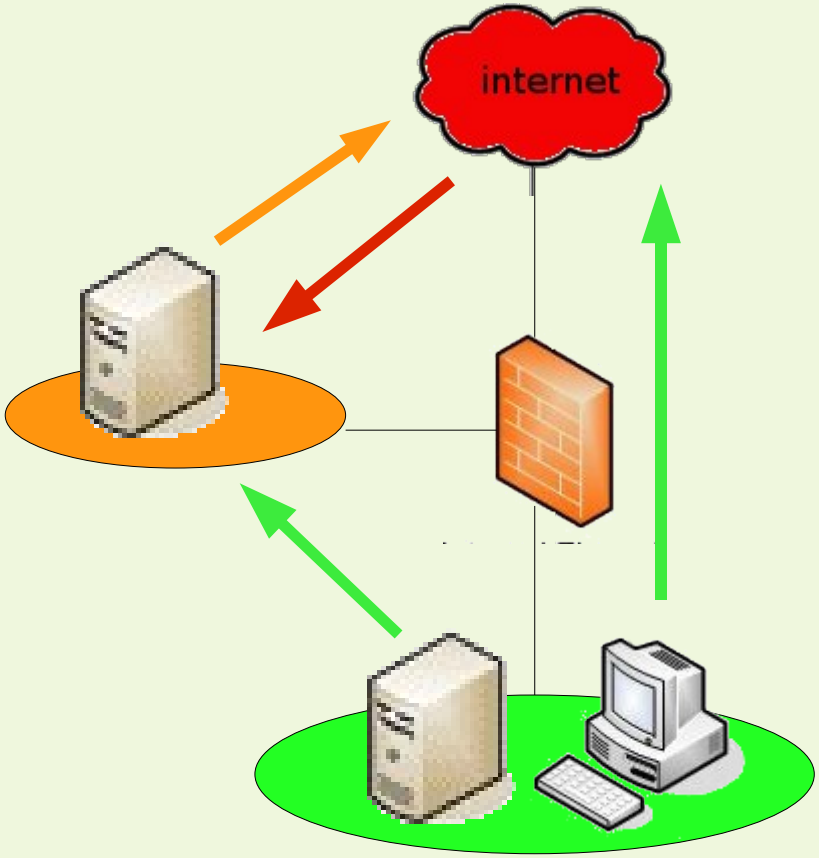
- Découpage en DMZ :

  3. DMZ

  - **Visible** du réseau interne et du réseau externe
  - Exemple : cas d'un réseau contenant:

    - **Un serveur web :**
      visible de l'Internet et des utilisateurs internes
    - **Une passerelle SMTP :**
      accessible des postes clients et des serveurs SMTP d'Internet

-> besoin de visibilité de l'extérieur


internet

Adressage

- Adressage des serveurs de la DMZ:
  - **Séparer** les différents réseaux en terme d'adressage IP
  - être **économe** en terme d'adresses **IP publiques**
- 2 solutions:
  - Sous-réseaux IP
  - NAT/PAT

Adressage : Solution 1

- Couper la plage d'adresses IP publiques en 2 (pas forcément égales)
  - 1ère moitié sera dédiée à l'interface publique du **filtre** de paquets
  - 2ème aux machines de la **DMZ**
- Le pare-feu est capable de séparer les deux réseaux en se basant sur leur masque de réseau
- Cette solution peut se révéler **coûteuse** en termes d'adresses IP

Adressage : Solution 2

- NAT/PAT :
  - Les adresses IP publiques sont affectées sur l'interface publique du pare-feu
  - **DMZ : adressage intranet**
  - Pare-feu
    - Service **NAT** : DMZ vers Internet

      NAT : Network Adress Translation
    - Service **PAT** : Internet vers DMZ

      PAT :Port Address Translation

Placement des services

- Postes clients : **réseau interne**
- **Serveurs web** publics : **DMZ**
- **Serveur SMTP ?**
  - un rôle de messagerie interne : ***réseau interne***
  - Envoi/réception de courriers vers/depuis l'Internet: ***DMZ***
- **Serveur DNS ?**
  - Résolution des noms de machines internes: ***réseau interne***
  - Résolution des noms des machines Internet: ***DMZ***

Placement des services: Serveur SMTP

- Solution 1: **UN** serveur de messagerie
  - le serveur est placé en **DMZ**
    - Il reçoit et envoie les courriers directement de l'Internet
    - Les postes clients lisent leur courrier via POP3 ou IMAP directement sur ce serveur
    - La **messagerie interne** passe également par ce serveur
  - **Problème** : *les messages électroniques internes (**données confidentielles**) sont stockés sur un serveur potentiellement accessible de l'Internet*

Placement des services: Serveur SMTP

- Solution 2 : **DEUX** serveurs de messagerie
  - le serveur de messagerie est dupliqué:
    - **un** serveur de messagerie sur le **réseau interne**:
      - se charge de délivrer les **courriers internes** et de conserver les messages
      - Il **relaie** les courriers à destination de l'Internet à un serveur de messagerie placé sur la DMZ
    - **un** serveur de messagerie placé sur la **DMZ**:
      - C'est le seul à communiquer avec l'Internet
      - **Relaie** les courriers en provenance de l'Internet au serveur du réseau interne

Placement des services: Serveur DNS

- Solution 1 : **UN** serveur DNS
  - le serveur est placé en **DMZ**:
    - répondre aux requêtes de l'Internet
    - Autorité pour les machines internes
  - **Problème** : *la résolution des noms internes est assurée par un serveur potentiellement accessible de l'Internet*

Placement des services: Serveur DNS

- Solution 2 : **DEUX** serveurs DNS
  - **Un** serveur DNS sur la **DMZ:**
    - répondre aux requêtes de **l'Internet**
  - **Un** autre serveur DNS dans le **réseau Interne**:
    - **Autorité** pour les machines internes
    - **Passe par le DNS public** pour résoudre les noms de machines de l'Internet.

DMZ multiples

- Certains cas de partitionnement de réseau peuvent faire appel à **plusieurs DMZ**:
  - *rendre publics certains serveurs mais il **n'est pas possible** en terme de sécurité de les faire **cohabiter** sur le même réseau:*
    serveurs de sensibilité différente
  - *il est parfois souhaitable de placer les services du réseau interne sur une **DMZ « interne »:***
    où se trouveraient les serveurs de messagerie interne, le DNS interne, l'annuaire LDAP, etc.

Conclusion

- La **sécurité** d'un système d'information
  = une **chaîne** de maillons
- **Pare-feu** + découpage en **DMZ**
  = **1 maillon** de la chaîne
- *La sécurité du système d'information doit être abordée dans un contexte **global***
  *= il faut pas négliger les **autres maillons***

Manipulation

Mise en place d'une DMZ