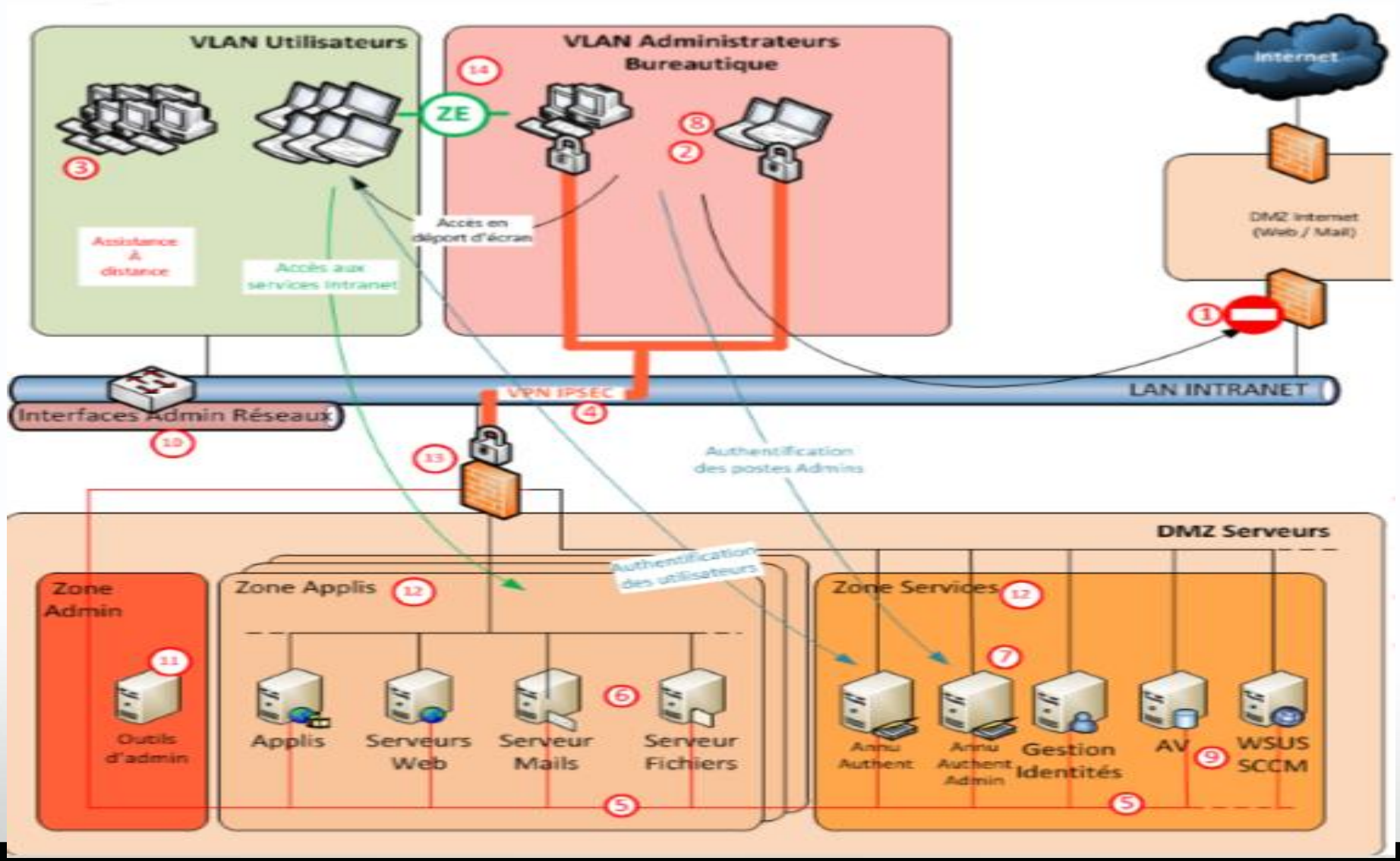
Architectures Sécurisées

Pôle Écoles Méditerranée

Architecture sécurisée

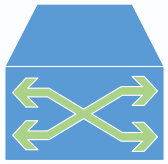


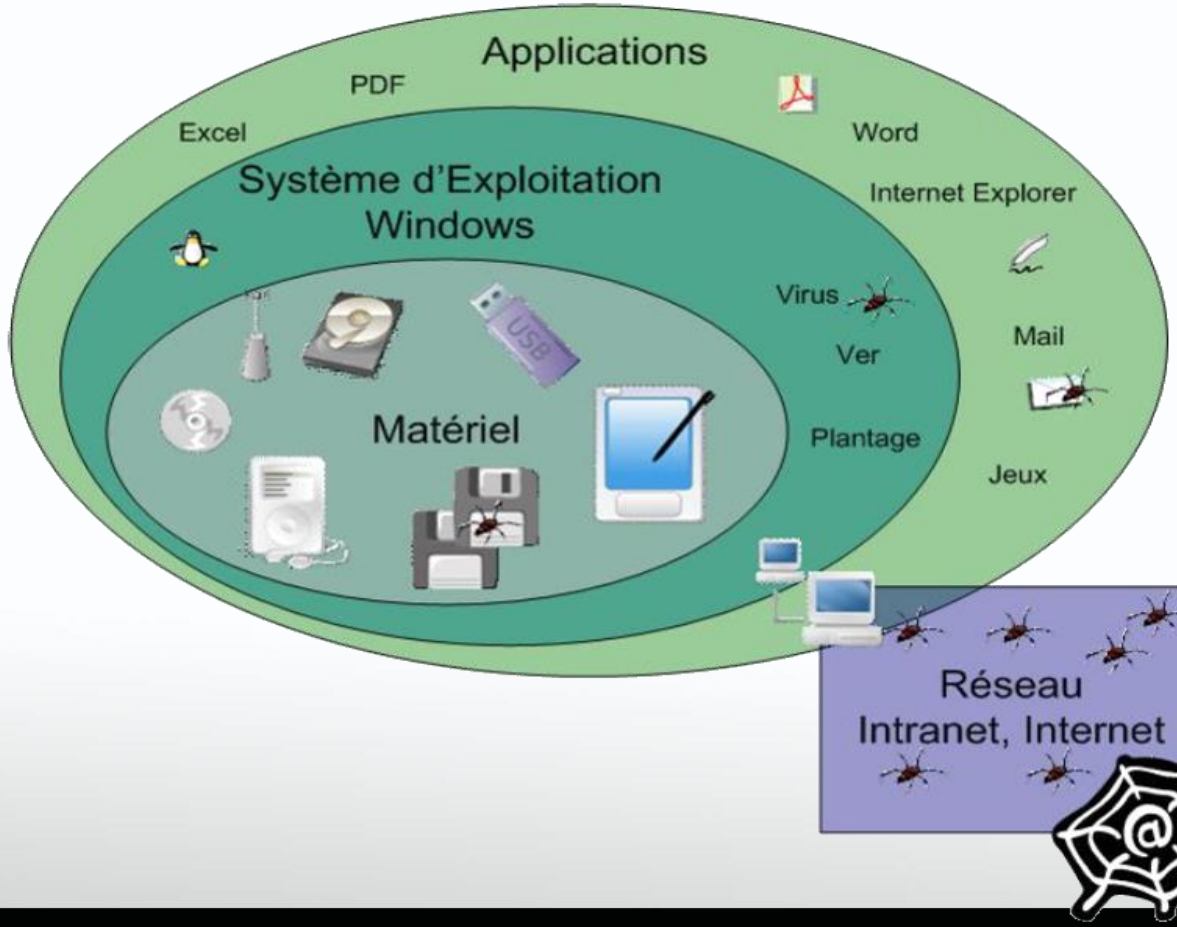
Architecture sécurisée

Connaitre son SI

- Bien ou actif
- Quelles sont les vulnérabilités ?
- Types de réseau ?
- Quelles peuvent être les menaces ?
- Quelles peuvent être les sources de menaces ?
- On en déduit des risques
- On met en place les mesures de sécurité adaptées
  - Besoin, niveau de sécurité
  - Compétence en SSI
  - Coût financier

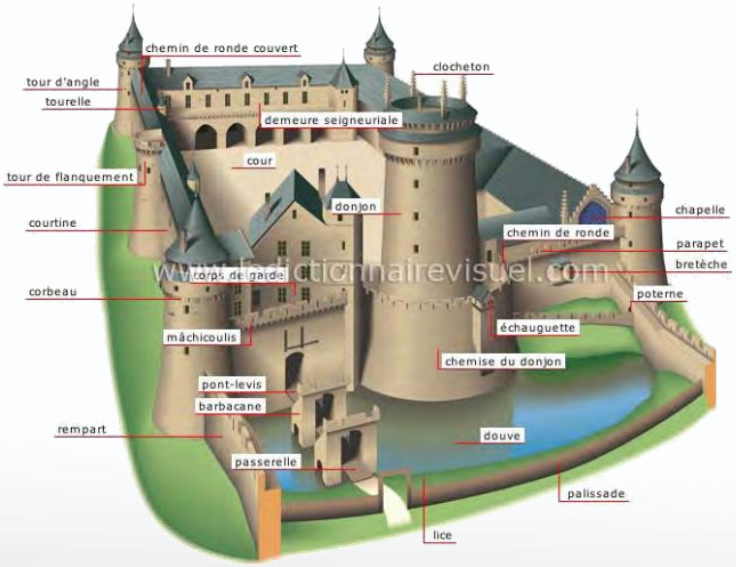
Architecture sécurisée

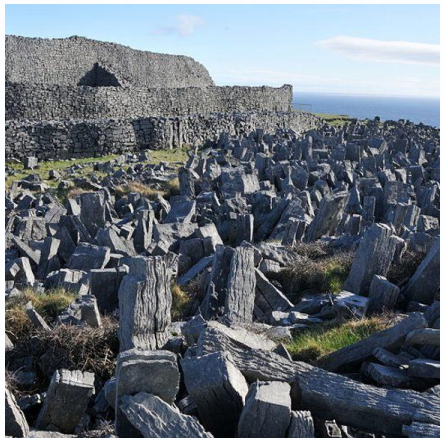


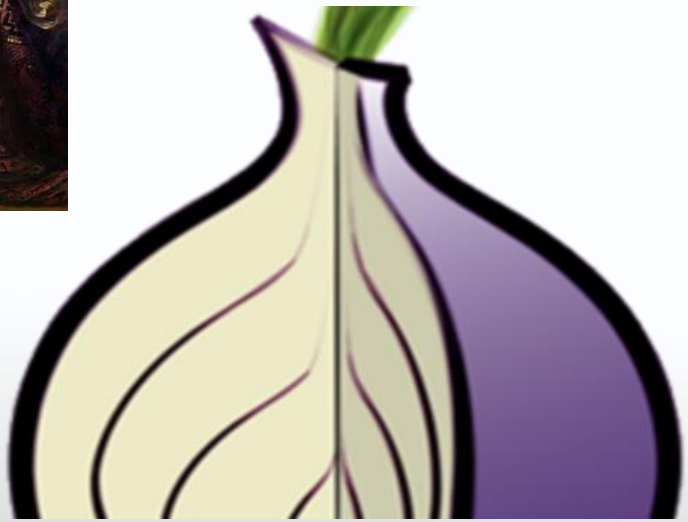


Faiblesse du modèle OSI

Principe de défense en profondeur





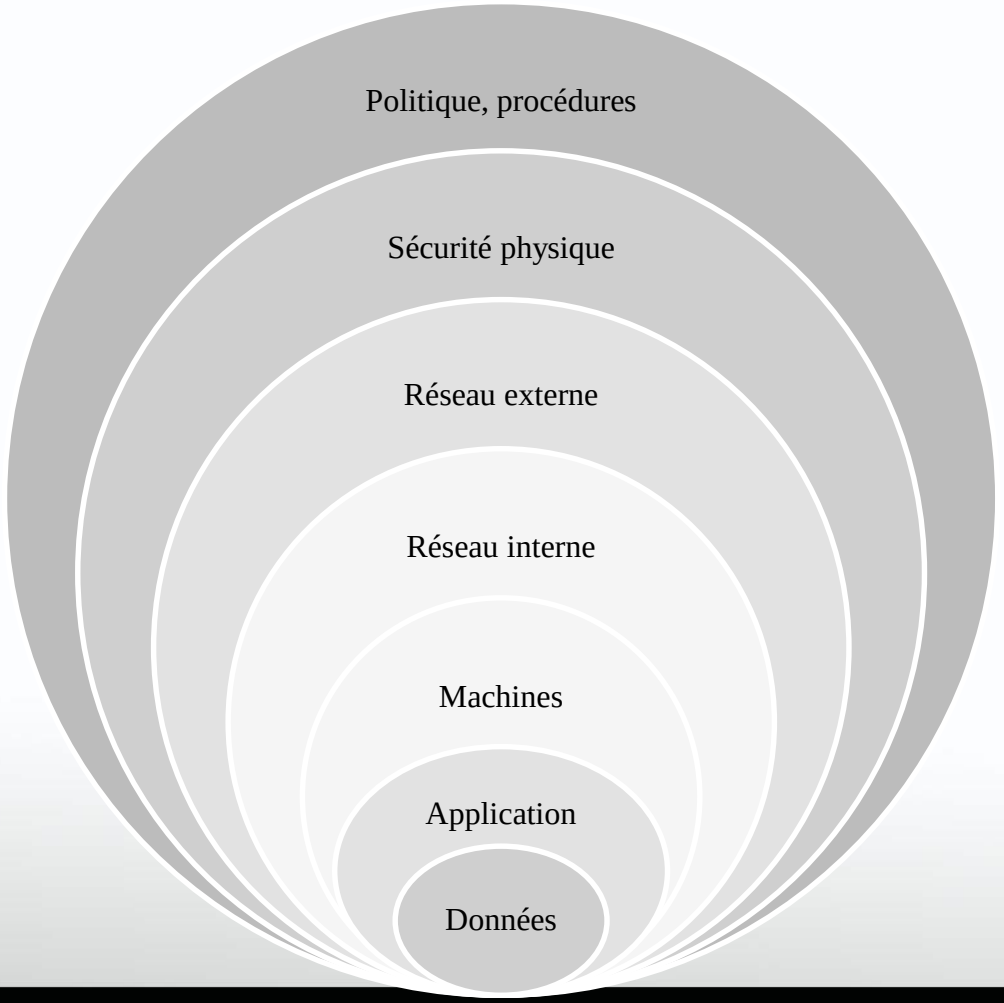


Sébastien Le Prestre, Marquis de Vauban

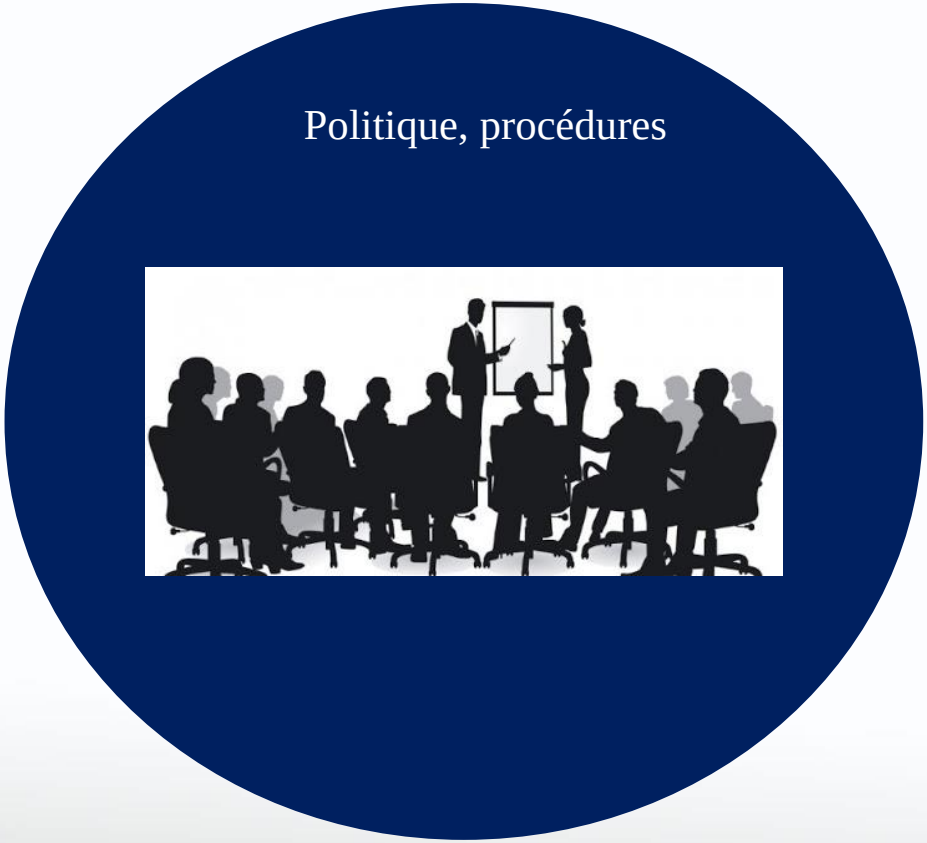
Défense En Profondeur en SSI

Ce principe peut être divisée en trois domaines :

- Administratif
- Physique
- Technique



Défense En Profondeur en SSI



- Administratif

- La sensibilisation
- Connaissance de la PSSI-A
- La formation

Défense En Profondeur en SSI

- Physique

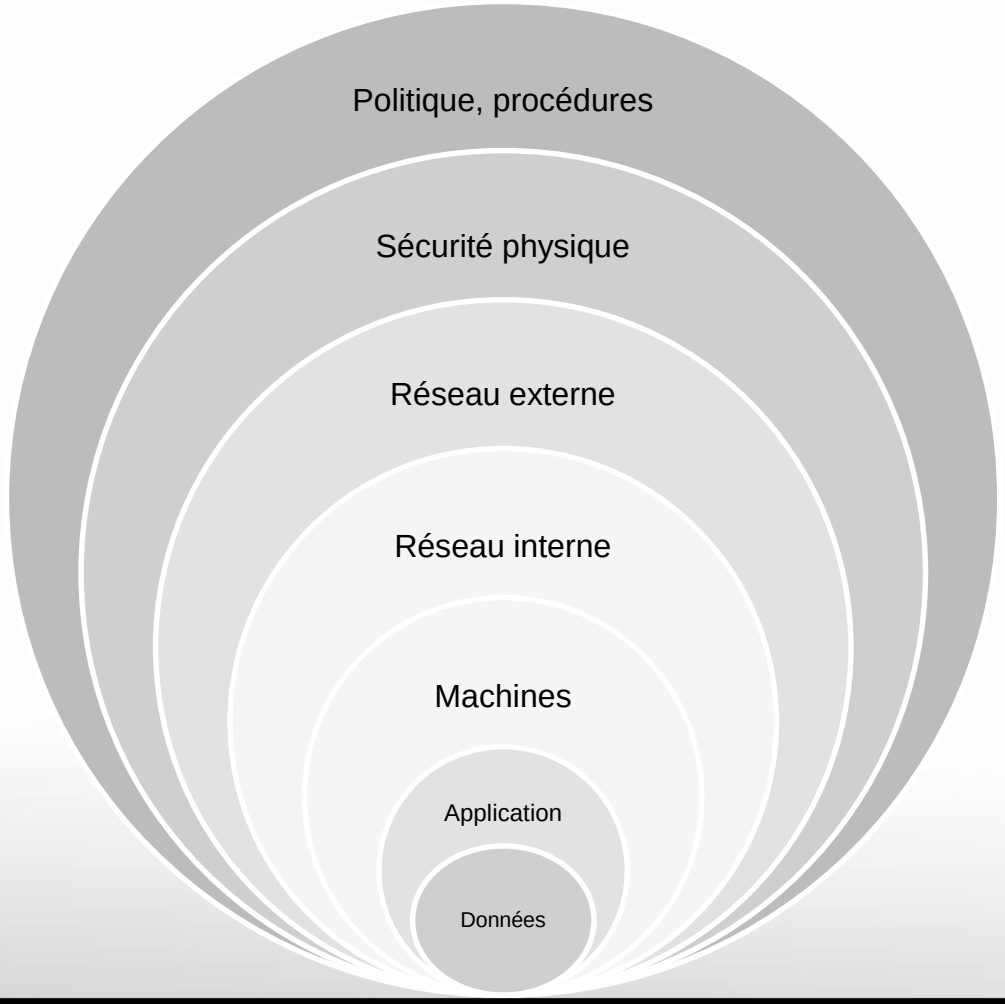
- Protection des locaux et des biens matériels.

- Déploiement de lecteurs biométriques pour réguler l'accès des zones sensibles

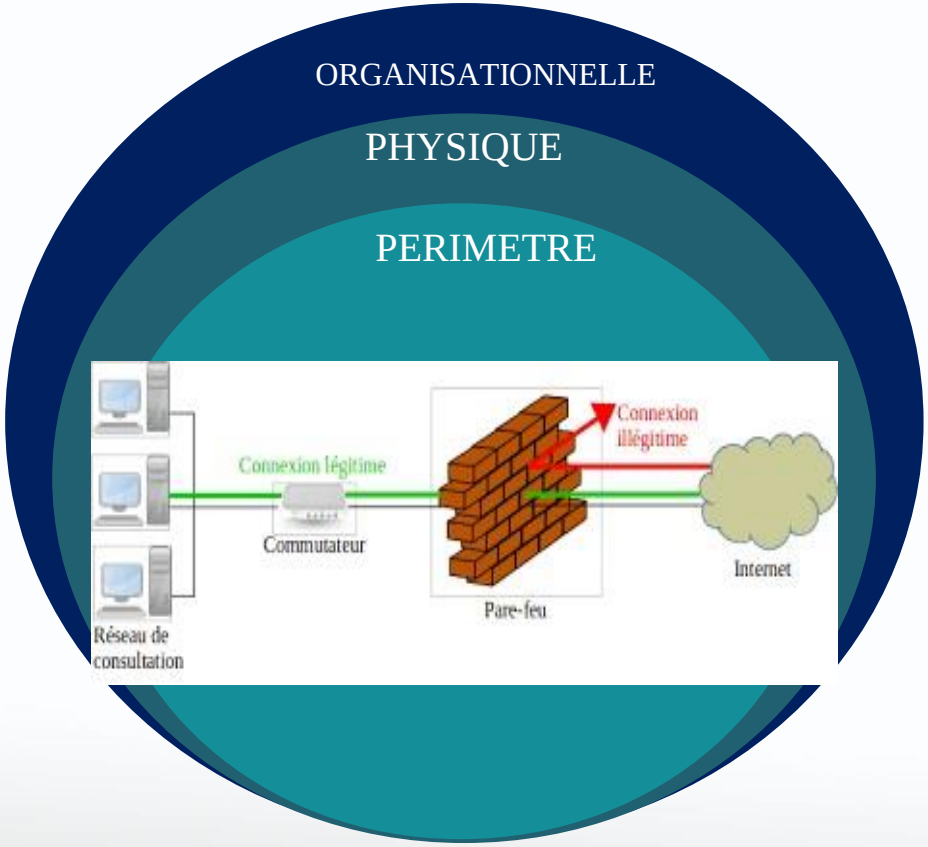
Défense En Profondeur en SSI

- Sécurité technique

  - Réseau externe
  - Réseau interne
  - Machines
  - Applications
  - Données



Défense En Profondeur en SSI

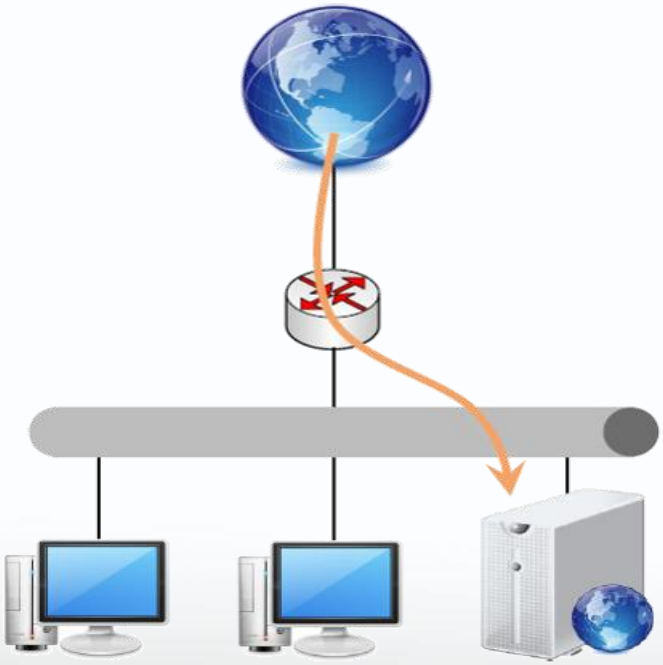


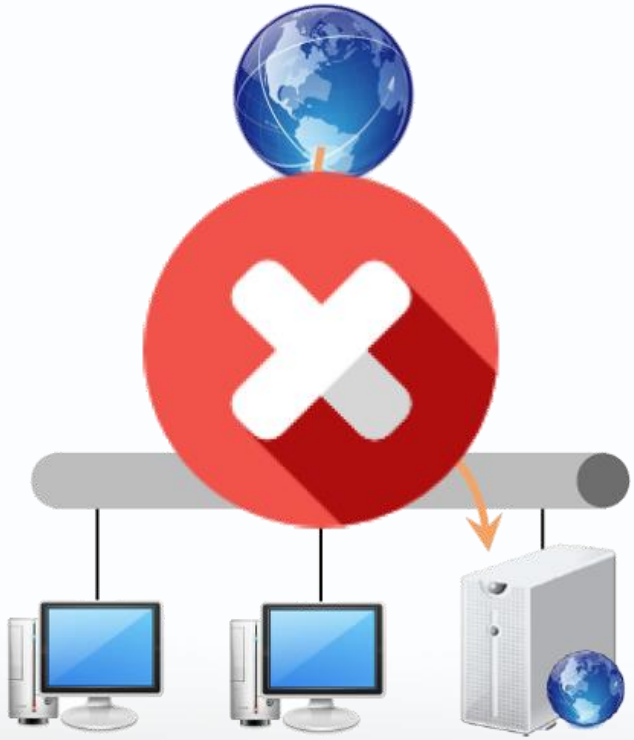
- **Firewall**
- **DMZ**
- **Proxys**
- **IDS/IPS**
- Etc

Contrôle qui a le droit d'accéder à quoi

Défense En Profondeur en SSI

- Réseau externe



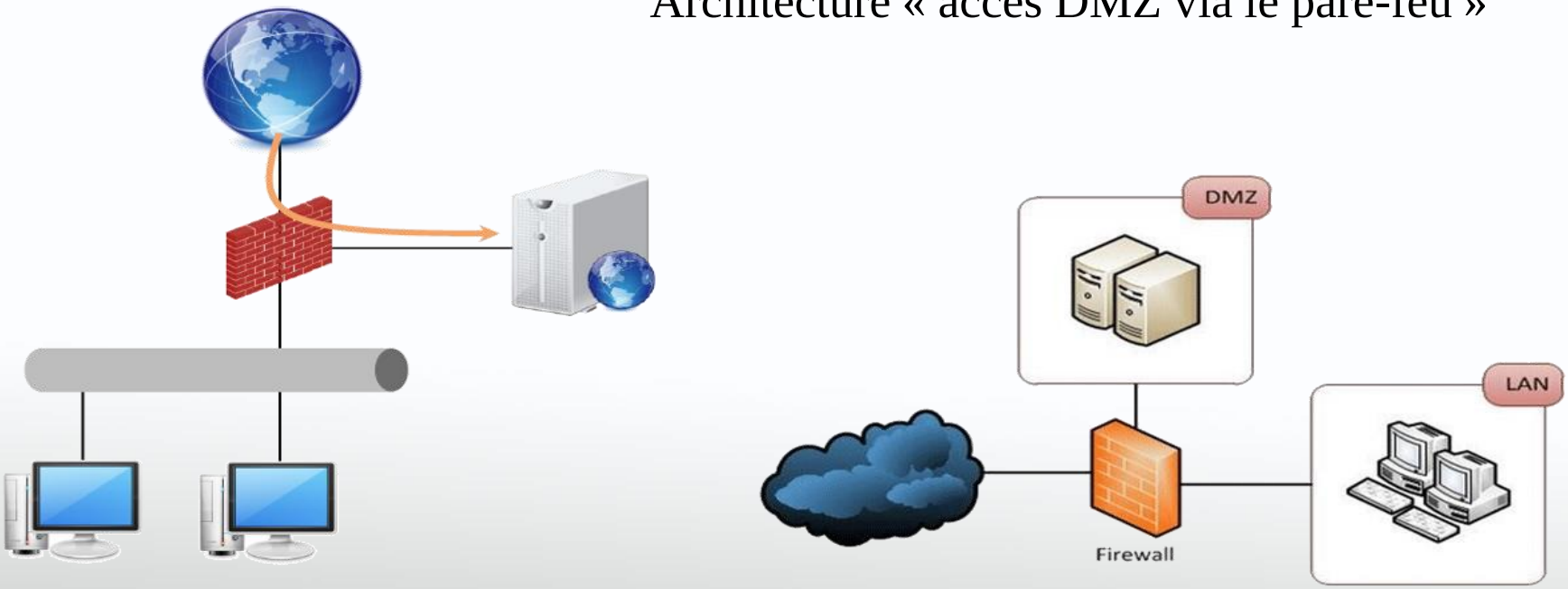


Défense En Profondeur en SSI

- Réseau externe

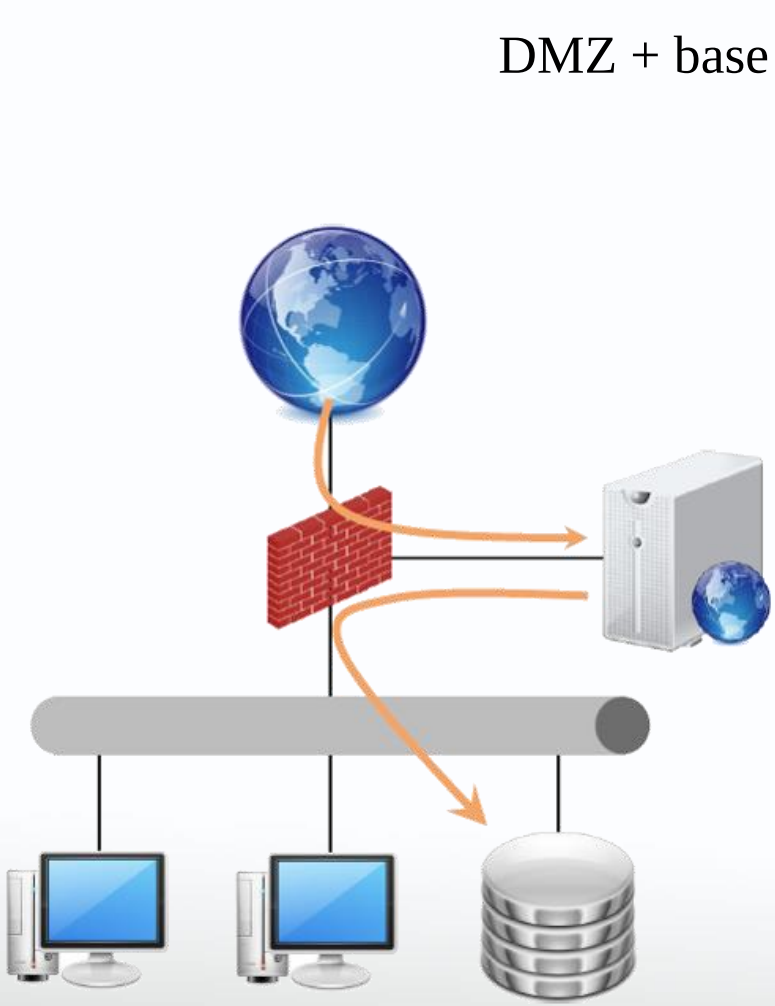
Déplacés les serveurs devant être accessibles de l'extérieur

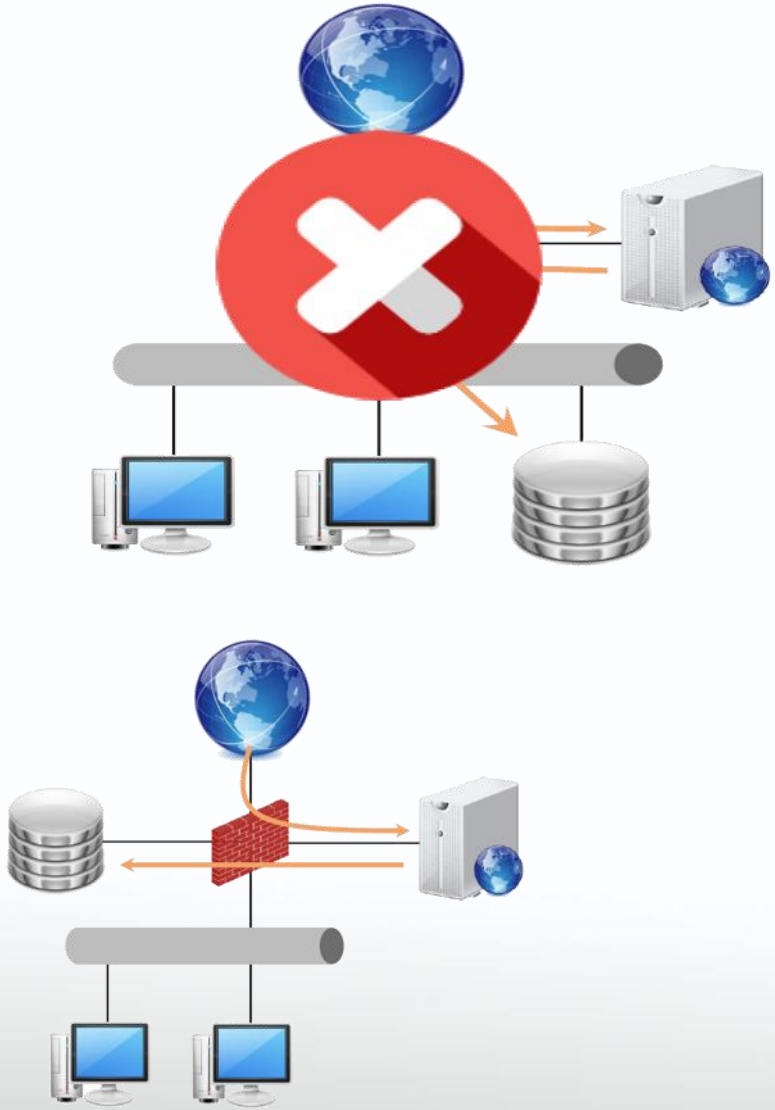
Architecture « accès DMZ via le pare-feu »



Principe de défense en profondeur

DMZ + base interne

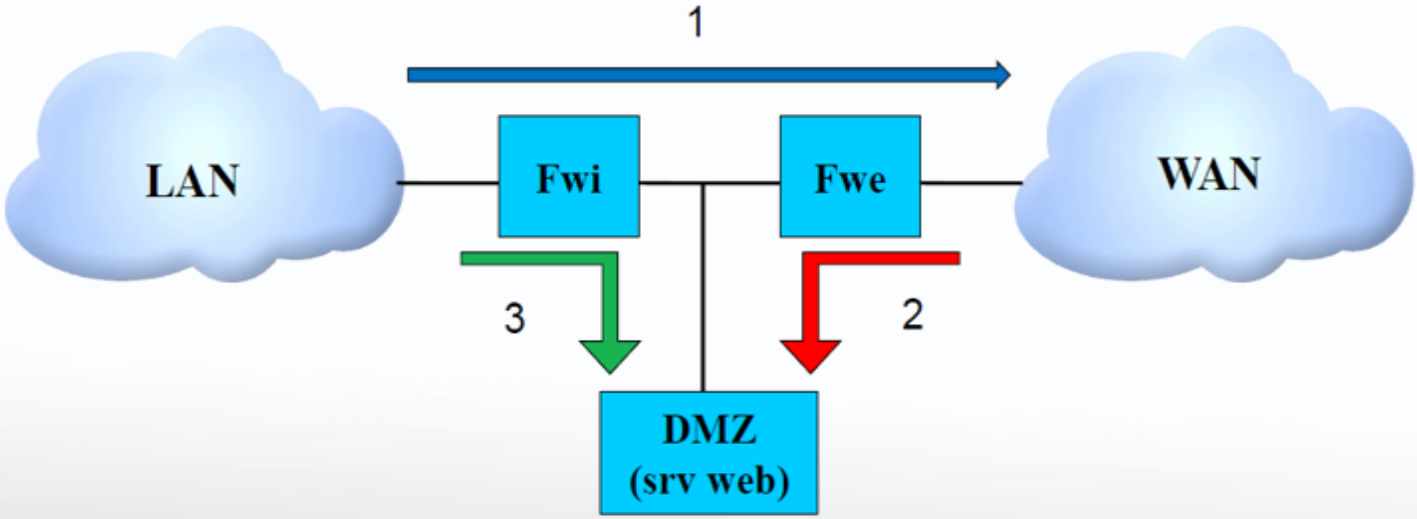




Principe de défense en profondeur

- Réseau externe

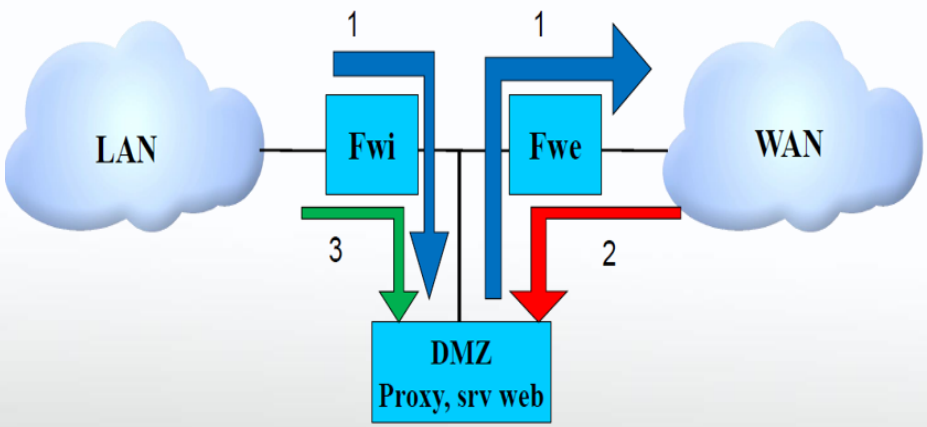
Architecture basée sur deux pare-feux

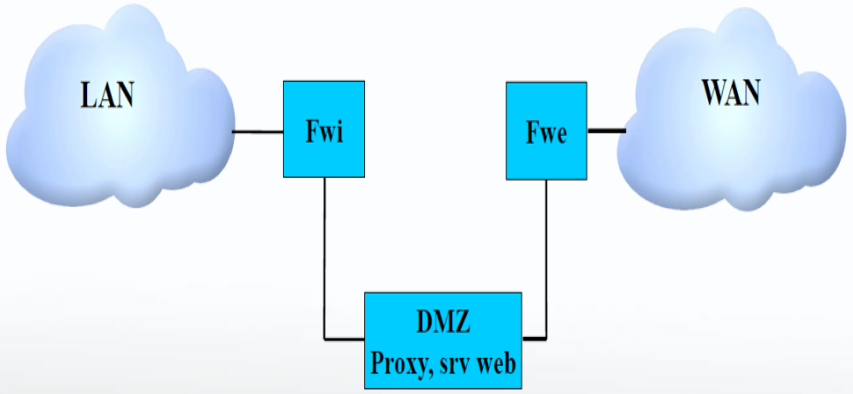


Principe de défense en profondeur

- Réseau externe

Architecture basée sur deux pare-feux avec serveur mandataire



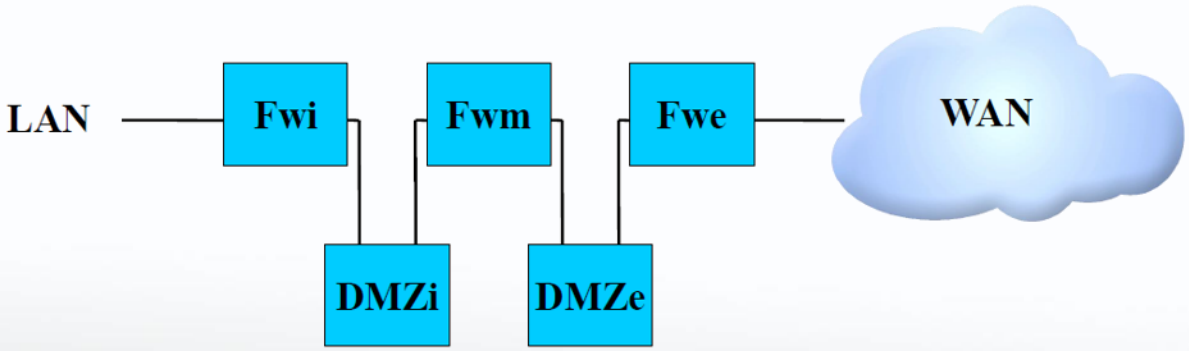


Architecture avec deux DMZ en coupure physique

Principe de défense en profondeur

- Réseau externe

Architecture avec deux DMZ en coupure physique



Principe de défense en profondeur

- Réseau externe

Principes de sécurisation appliquées sur les pare feux et les serveurs ?

- Pare feux

  - ✓ Principe de la **diversité à tous les niveaux**
    - au niveau du système d'exploitation
    - au niveau du moteur de filtrage
    - au niveau du matériel.
  - ✓ Principe de la **panne sans danger**
  - ✓ Principe de l'**interdiction par défaut**

Principe de défense en profondeur

- Réseau externe

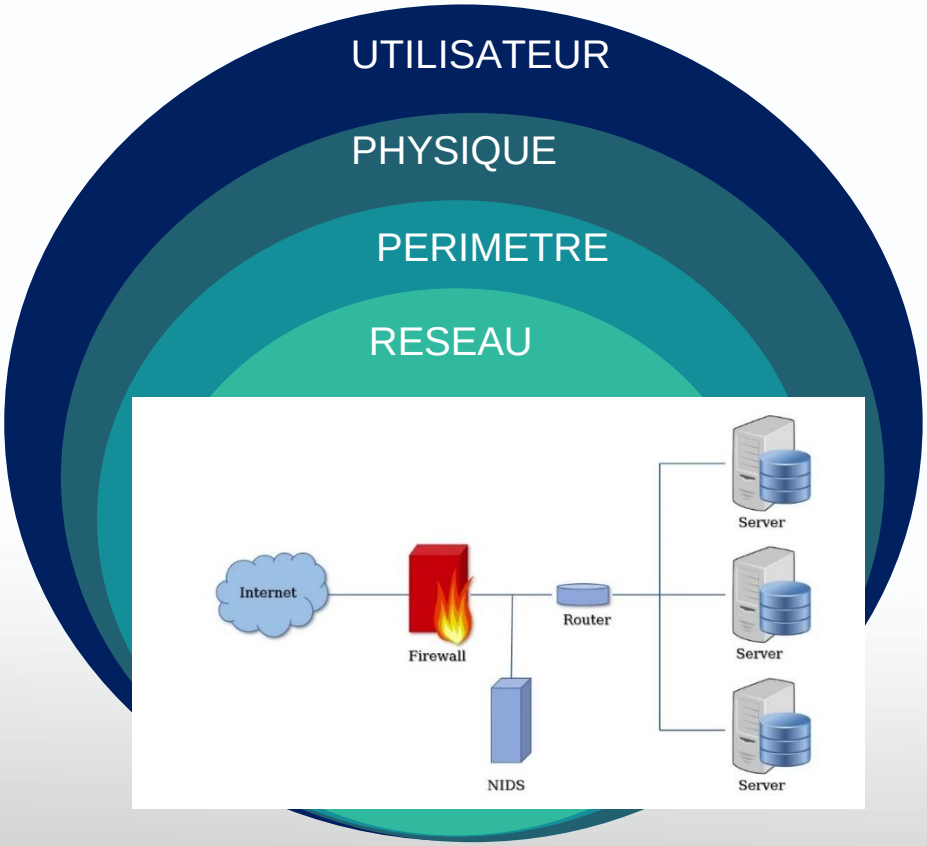
Principes de sécurisation appliquées sur les pare feux et les serveurs ?

- Serveurs

  - Principe de l'**unicité de fonction,**
  - Principe du **moindre privilège,**
  - Principe du **maillon le plus faible**

Principe de défense en profondeur

- Réseau Interne

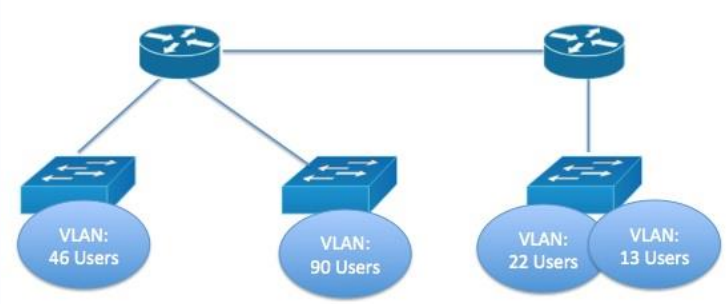


- Sécuriser les équipements d'interconnexion
- Gérer les utilisateurs
- Sécuriser les terminaux
- Sécuriser les services et processus

Principe de défense en profondeur

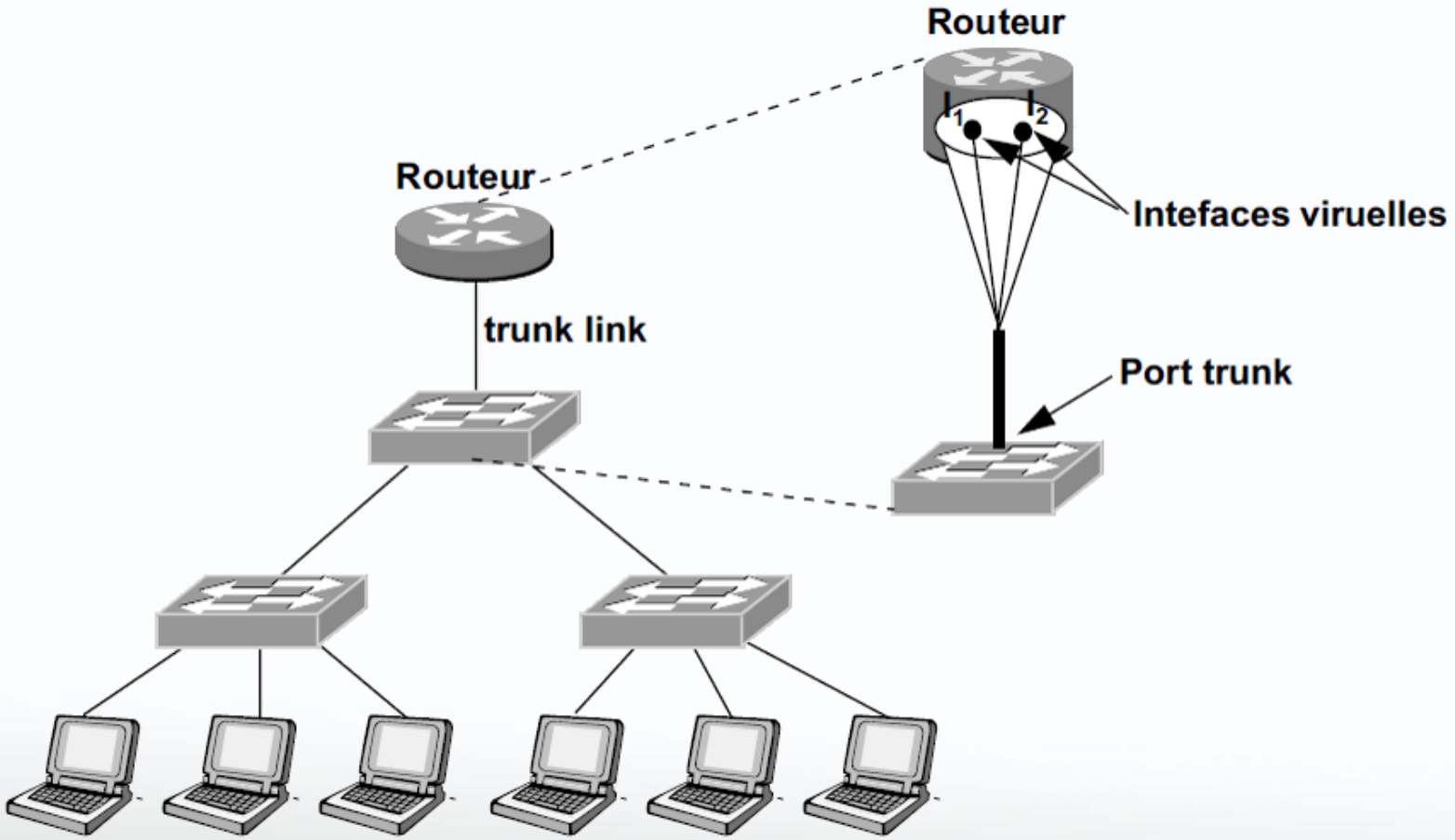
- Réseau Interne

Sécuriser les équipements d'interconnexion



Recommandations de l'ANSSI

Principe de défense en profondeur



Principe de défense en profondeur

- Réseau Interne

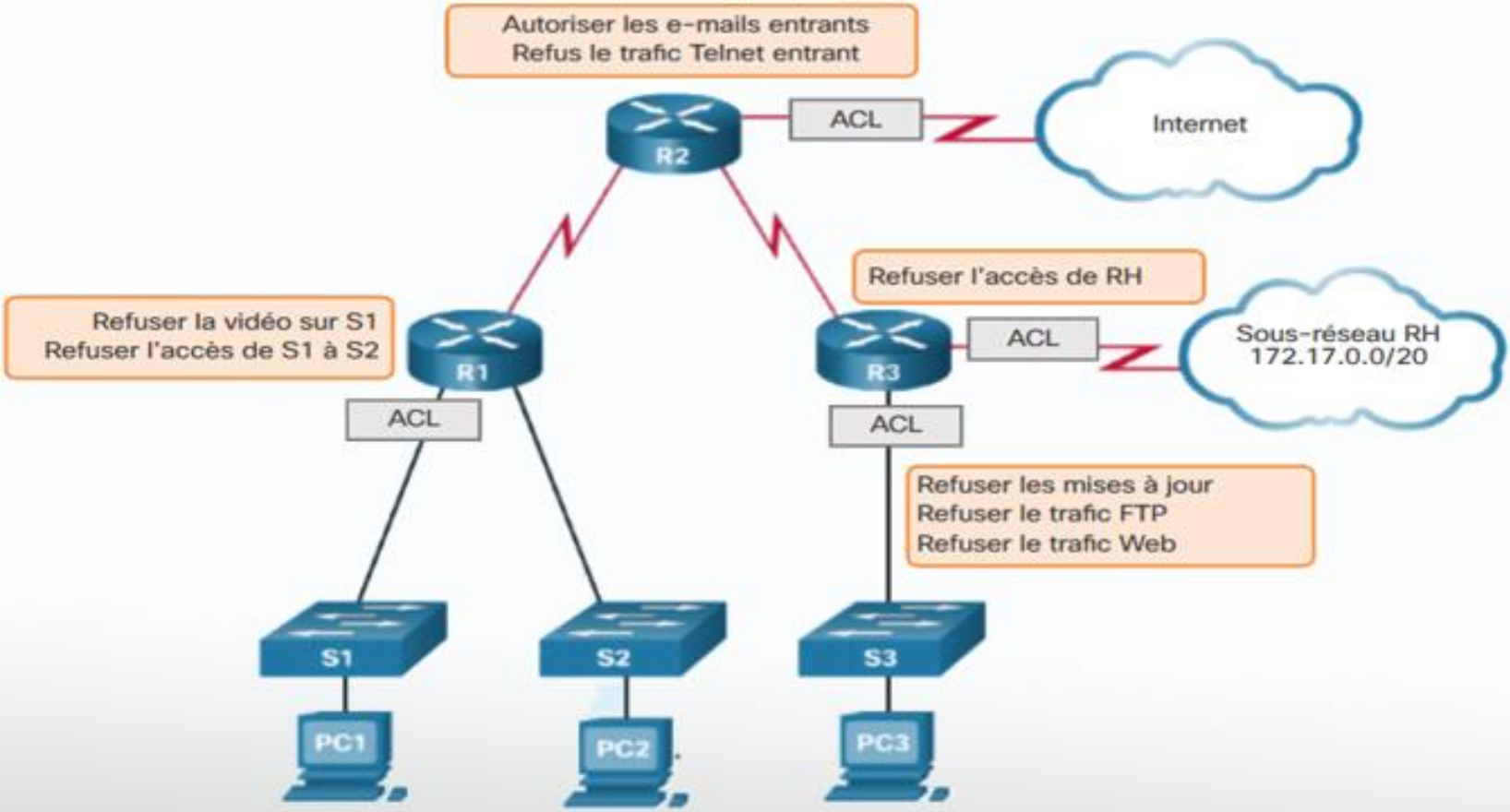
Sécuriser les équipements d'interconnexion

Exigences de sécurité des routeurs :

- Séparer les adresses internes des adresses publiques tout en assurant la correspondance entre elles.
- Filtrer le trafic entre réseaux IP en tenant compte des connexions et de leur sens.
- Préserver la confidentialité et l'intégrité des échanges.
- Disposer d'une redondance IP sûre pour la route par défaut.
- Sécuriser les protocoles de routage
- Désactiver les protocoles et services non utiles et non utilisés
- Se protéger des attaques TCP
- Etc

Principe de défense en profondeur

ACL ?



Principe de défense en profondeur

- ACL (Acces Control List)

Il existe deux types d'ACLs :

- ACL simple (**standard**)
- ACL plus complexe (**étendue**)

```
Router(config)#access-list ?
  <1-99>     IP standard access list
  <100-199>  IP extended access list
```

Peuvent être identifiées soit par un numéro ACL « numériques » soit par un nom ACL « nommées »

- Les numéros 1 à 99 et 1300 à 1999 sont réservés aux ACL standards.
- Les numéros 100 à 199 et 2000 à 2699 sont réservés aux ACL étendues.

Principe de défense en profondeur

- Réseau Interne

❑ ACL (Acces Control List)

- ACL simple (**standard**)
  - uniquement adresse IPv4 source
- ACL plus complexe (**étendue**)
  - type de protocole,
  - adresses IPv4 source ou destination
  - et ports source ou destination

- Action :

```
Router(config)#access-list 100 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment
```

Principe de défense en profondeur

- ACL (Acces Control List)

```
Router(config)#access-list 100 permit tcp 192.168.2.1 ?
  A.B.C.D  Source wildcard bits
```

```
Router(config)#access-list 100 permit tcp 192.168.2.1 0.0.0.255 host ?
  A.B.C.D  Destination address
```

Les listes d'accès utilisent des masques génériques (wildcard mask)

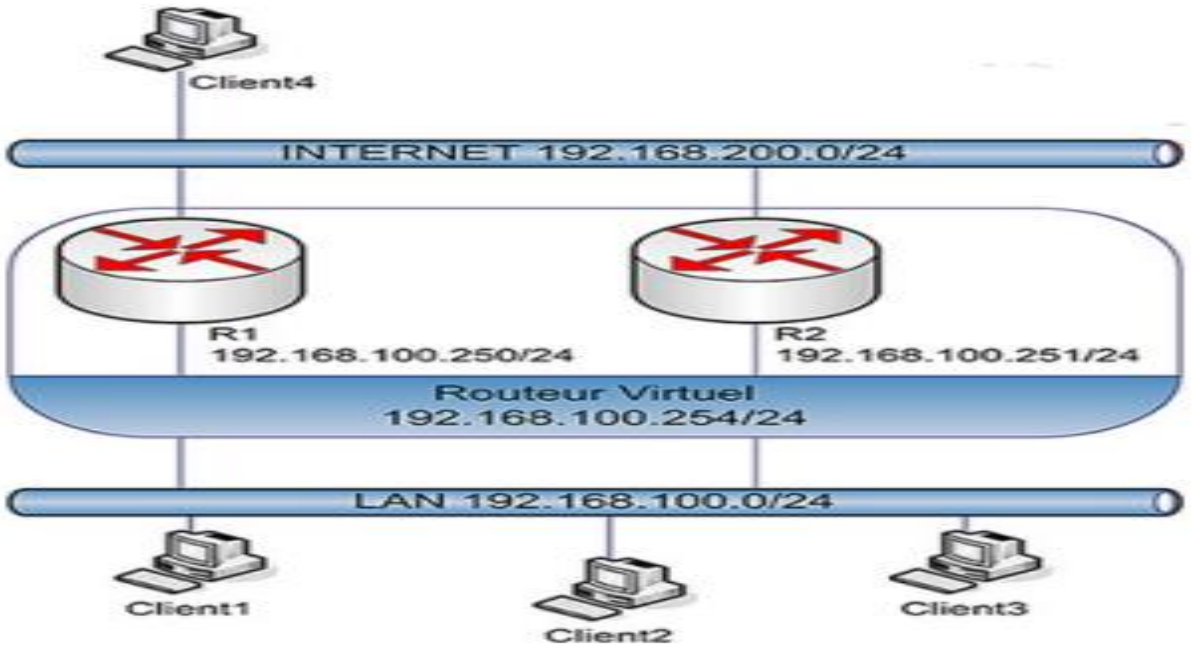
- Permet le filtrage
- Permet de mettre en évidence les bits hôtes
- Lorsqu'un bit aura une valeur de 0 dans le masque, il y aura vérification de ce bit

Soustraire le masque de la valeur suivante :
255.255.255.255

```
  255.255.255.255
- 255.255.255.0
-----------------
  0.  0  .  0.  255
```

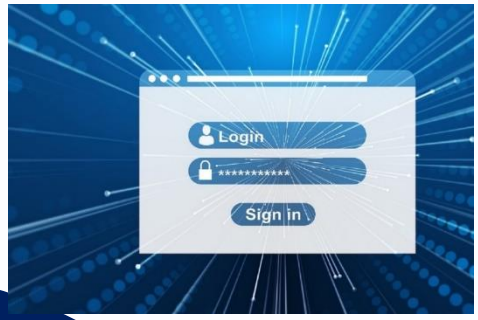
Conception d'un réseau local

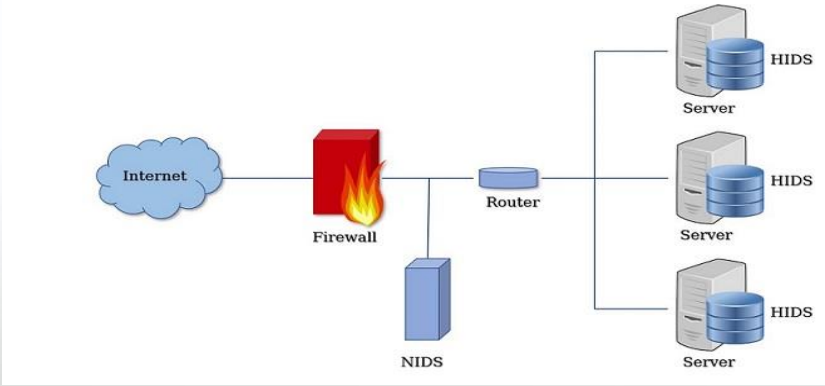
Redondance de passerelles de routeurs



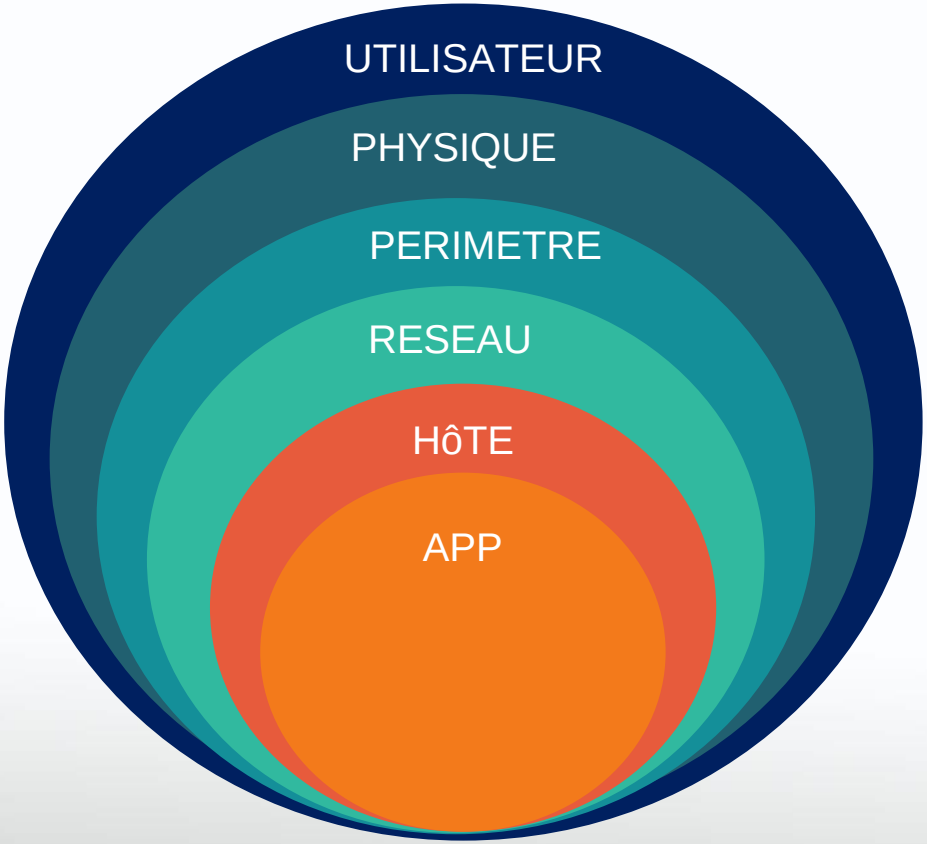
HSRP *Hot Standby Routing Protocol*
GLBP *Gateway Load Balancing Protocol*
VRRP *Virtual Router Redundancy Protocol*

Principe de défense en profondeur



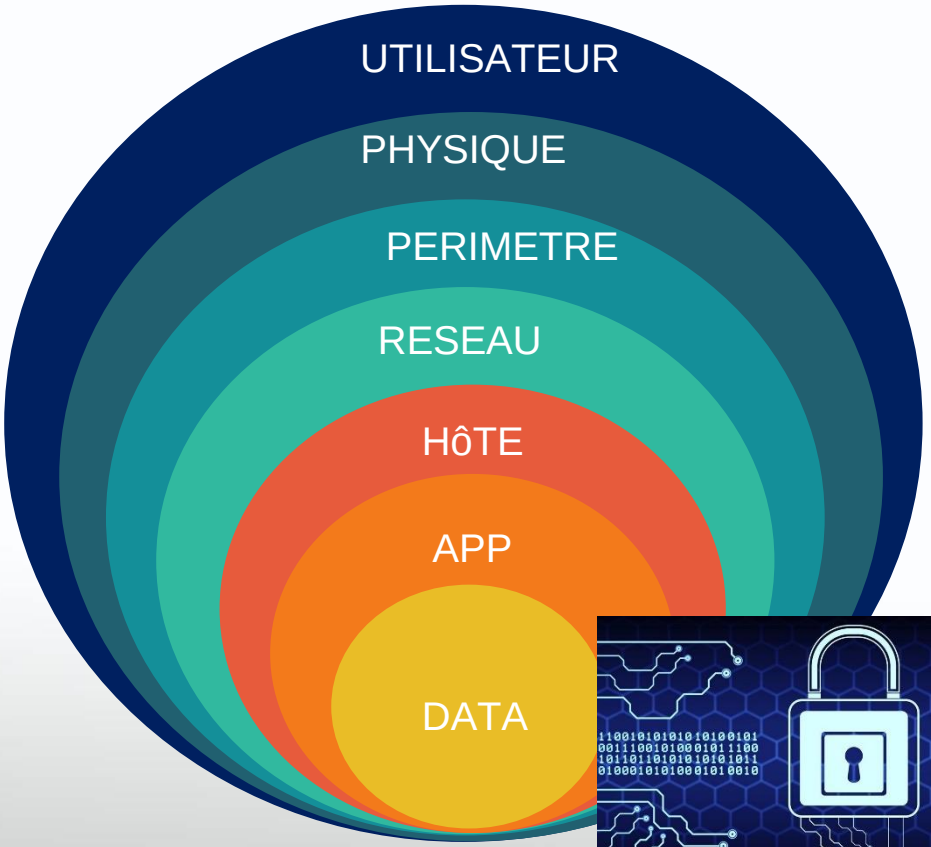


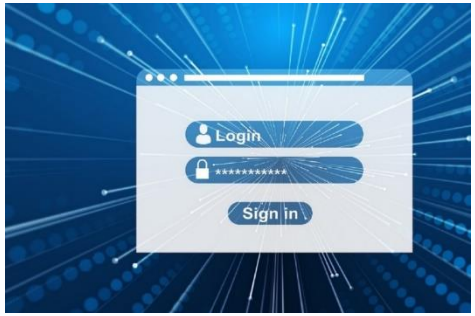
Principe de défense en profondeur



- Développement sécurisé,
- Contrôle d'intégrité,
- Test d'intrusion,
- Communication(https, …),
- etc

Principe de défense en profondeur

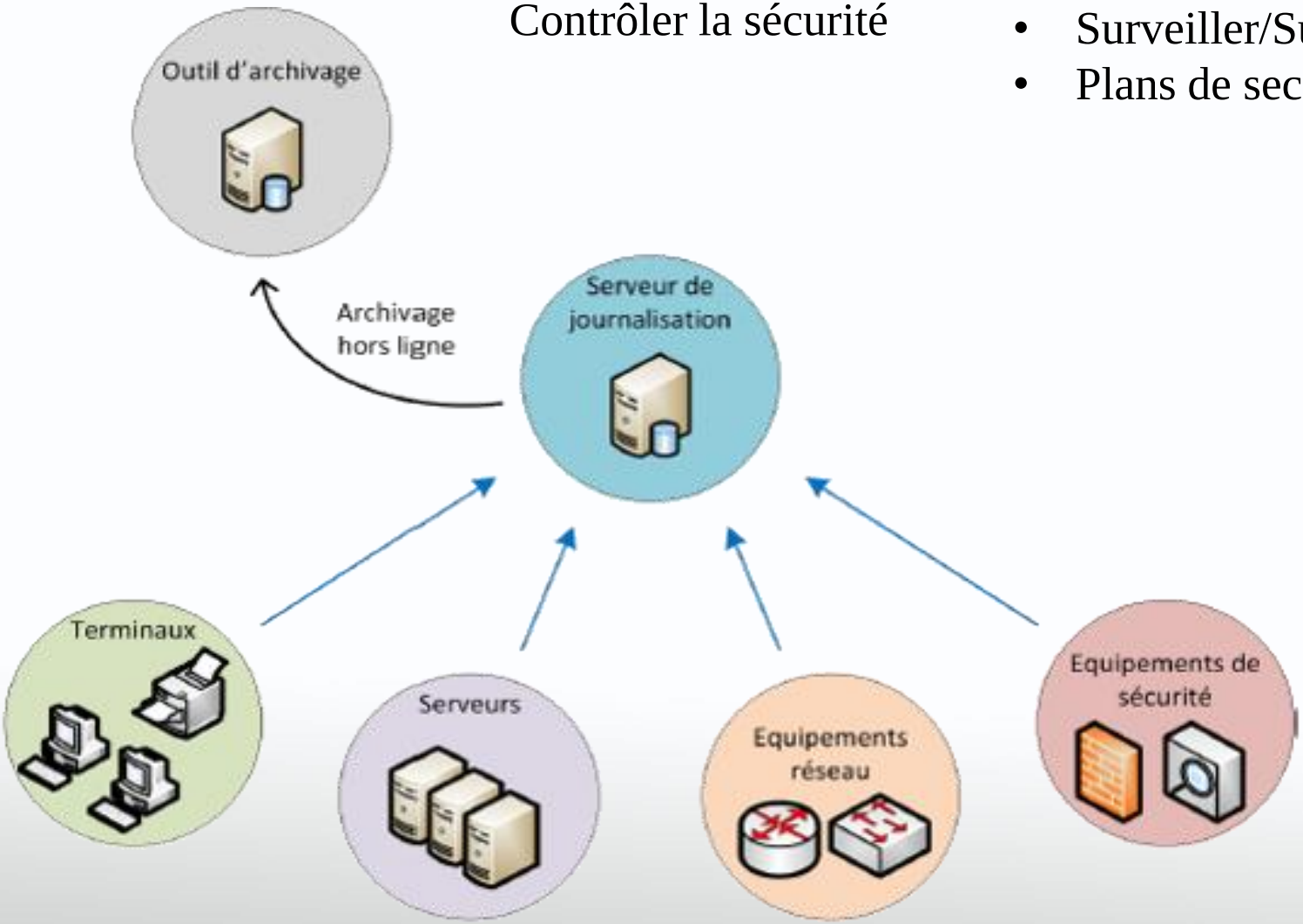




Principe de défense en profondeur

Contrôler la sécurité

- Surveiller/Superviser
- Plans de secours



Principe de défense en profondeur

Plan de secours

Plan de secours en cas de dysfonctionnement important (électrique, télécom…) :

- Double alimentation
- Onduleur, batterie de secours, groupe électrogène

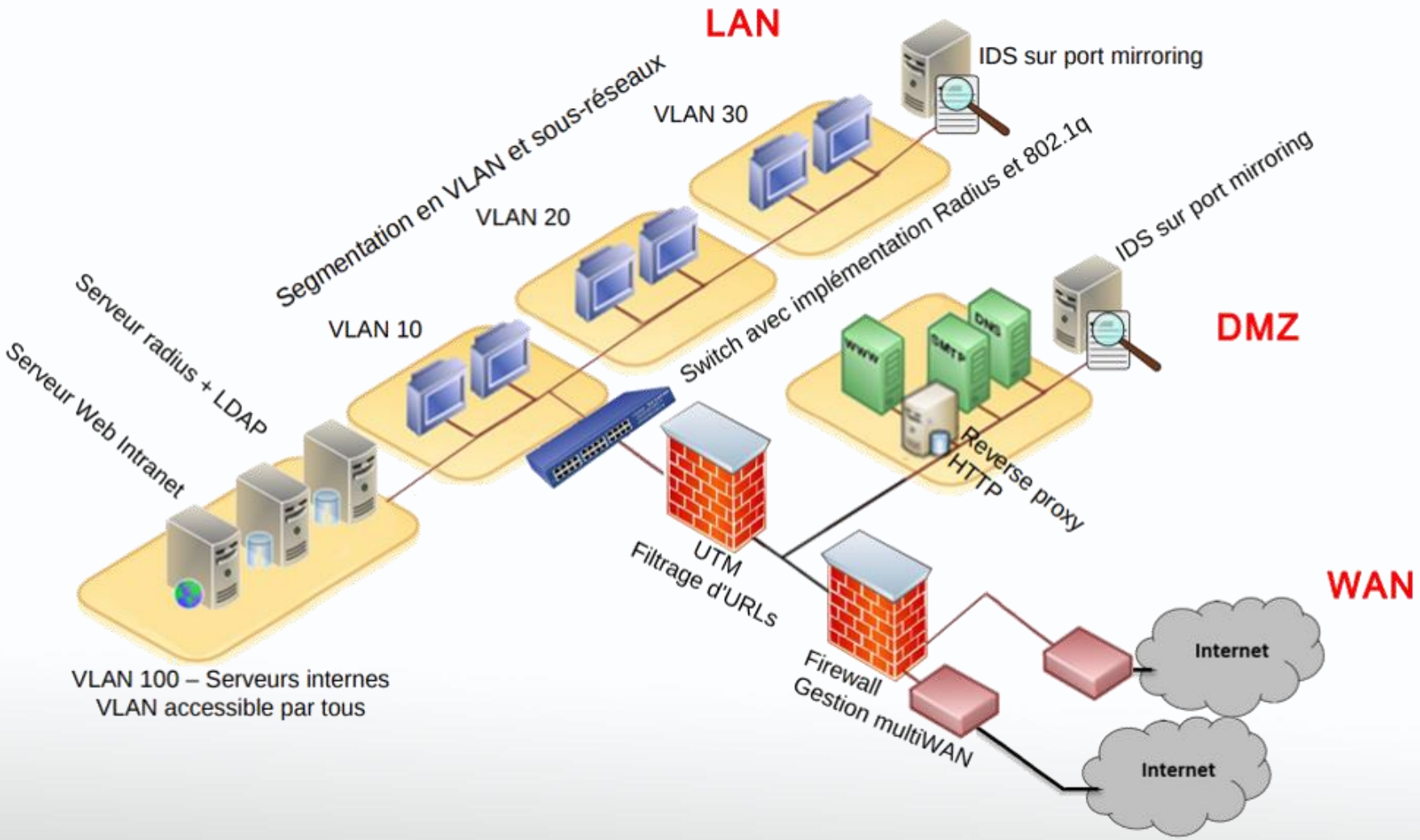
Accès Internet :

- Souscription à une offre Internet comme ligne de secours fournie par un opérateur différent.

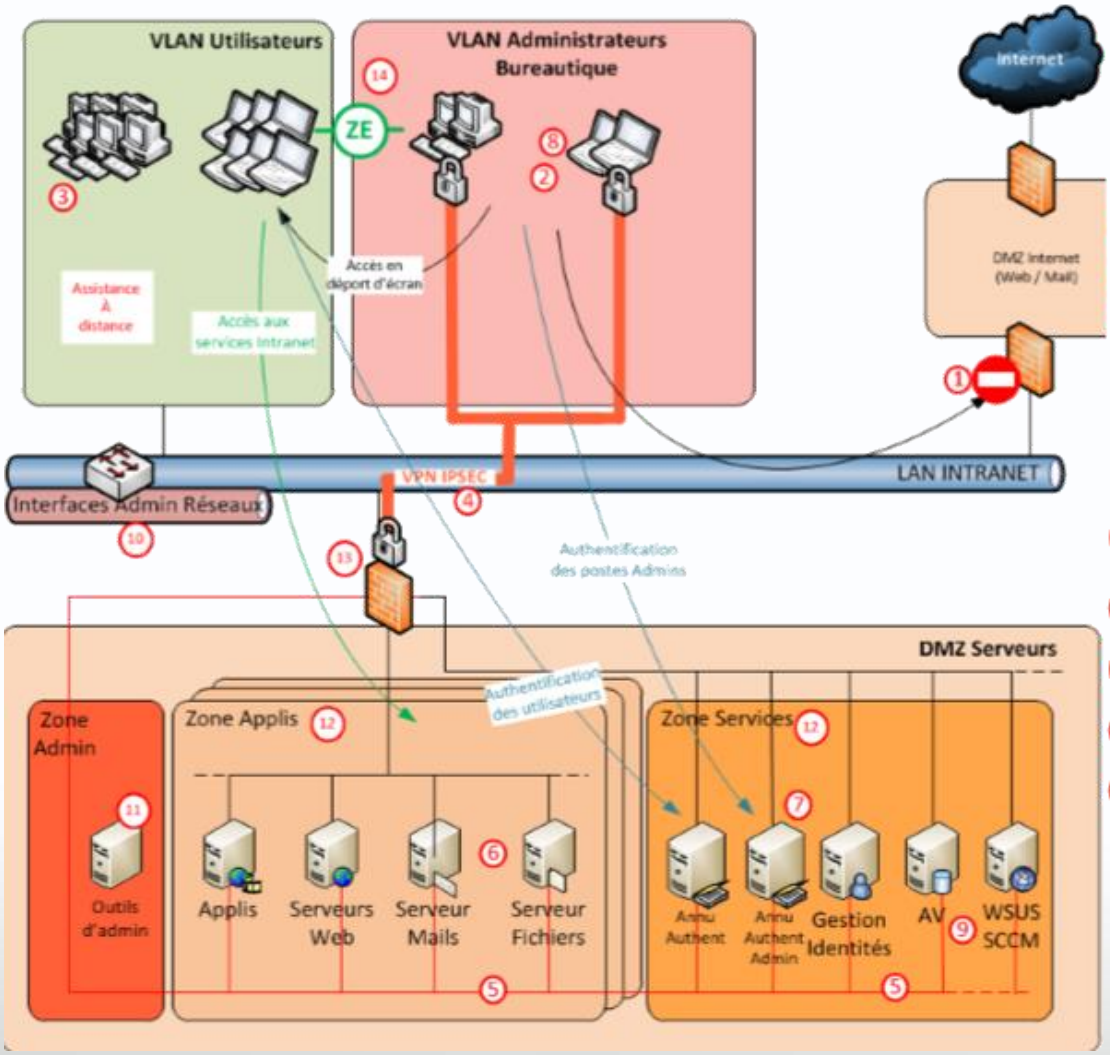
Avoir une sauvegarde de ses données

- PRA : Plan de Reprise d'Activité
- PCA : Plan de Continuité d'Activité

Architecture sécurisée

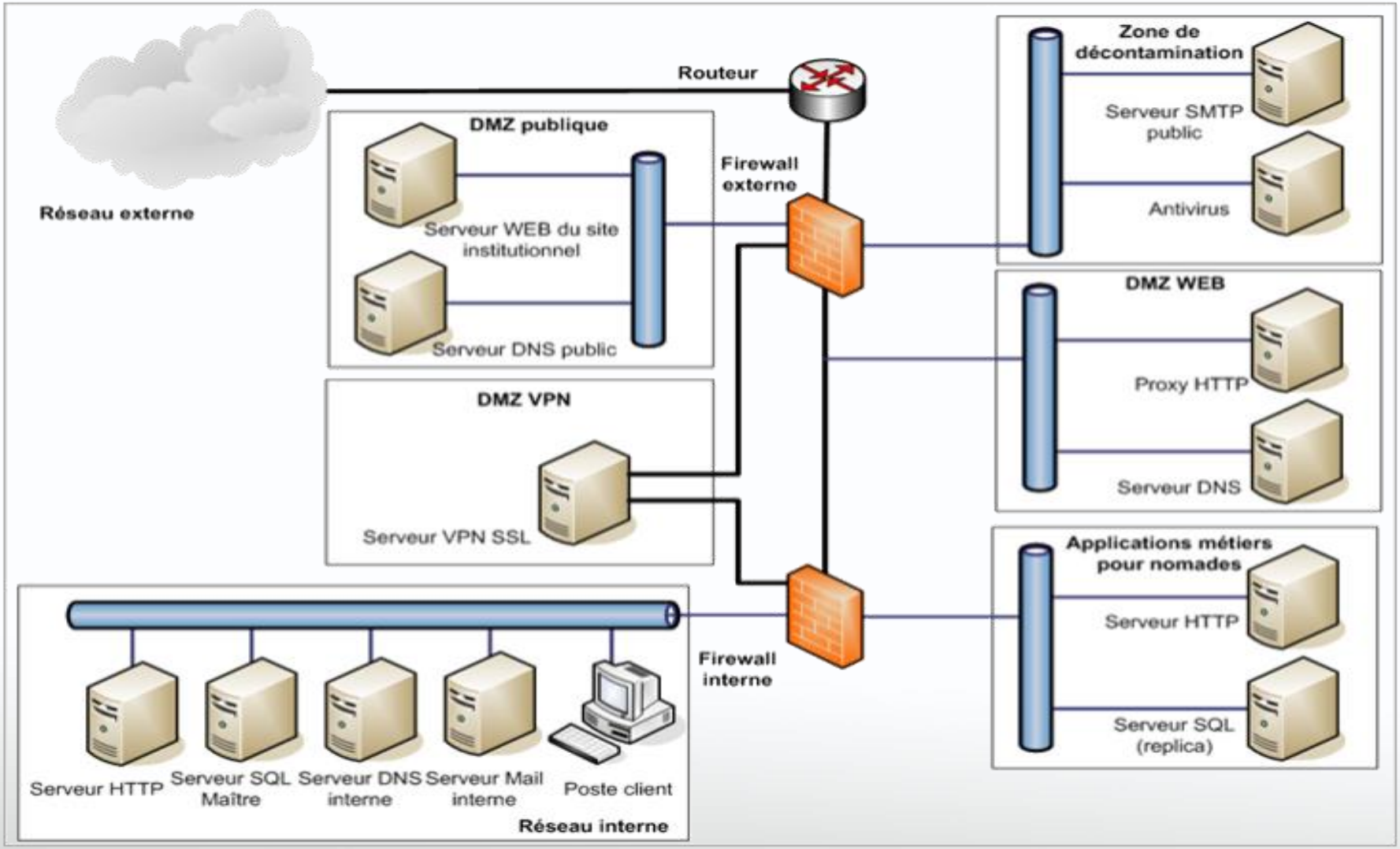


Architecture sécurisée



1. Pas d'accès Internet depuis les postes Administrateur
2. Comptes Administrateurs dédiés
3. Pas d'ouverture de session avec des comptes Admins en local sur des postes utilisateurs
4. Utilisation d'un VPN IPsec logiciel depuis les PC Admin et la DMZ Serveur pour l'administration (ex : The Green Bow)
5. Utilisation d'interfaces réseaux dédiées à l'administration pour les serveurs
6. Désactivation de l'IP_Forwarding sur les serveurs
7. Annuaire dédié aux administrateurs
8. Activation du pare-feu local des postes d'administrateur, notamment pour interdire les flux entrant sur les services d'administration à distance (ex: SSH, RDP, ...)
9. A partir de W2008, il est possible de dédier l'interface Ethernet d'admin en utilisant WSMAN sur certains services
10. Interface Ethernet dédiée à l'administration et règles de filtrage n'autorisant l'accès aux services d'admin qu'aux IP des postes d'admin
11. Mise en œuvre de serveurs « outils » pour l'administration (console centralisée d'admin des équipements réseaux, client lourd, RSAT ou WSMAN pour Windows, etc.)
12. Cloisonnement des serveurs dans différentes zones en fonction des besoins de l'entité
13. Si possible, dissocier les fonctions de filtrage et VPN IPSEC
14. Passerelle d'échange permettant le transfert d'informations et initié par la zone d'administration vers le réseau bureautique

Architecture sécurisée



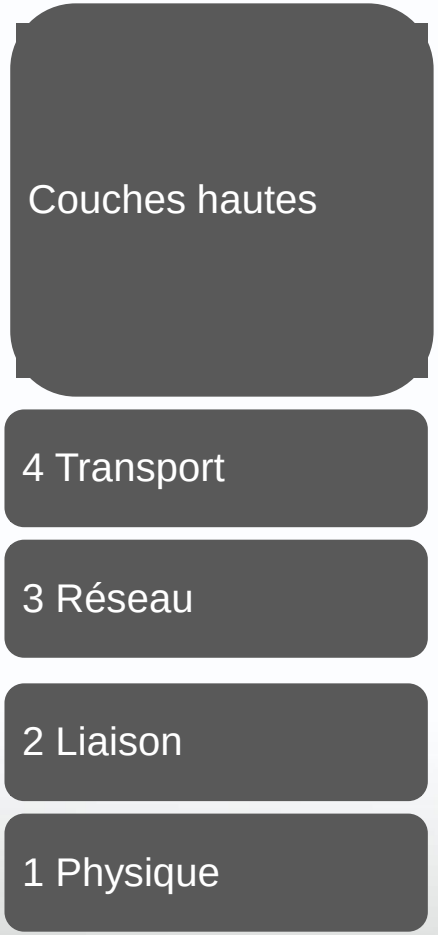
Conclusion

Le S.I. est un tout, un maillon faible affaiblir tout l'ensemble.

- L'attaque peut réussir par l'exploitation **d'une seule** vulnérabilité ;
- Tandis que la défense doit prendre en compte **l'ensemble** du système.

Conclusion

- Appliquez la DEP sur le modèle OSI



Séparation fonctionnelle, filtrage applicatif

Chiffrement de la communication

Filtrage, segmentation sous rzo, chiffrement de la com

Cloisonnement virtuel, contrôle d'accès logique

Utilisation d'équipement différents, contrôle d'accès physique

Architecture sécurisée

Norme et guides nationaux

- La réglementation:
  - Référentiel Général de Sécurité (RGS),
  - II 901 systèmes d'information dit « sensibles »
  - Systèmes classifiés de défense: IGI 1300, II 920, etc.
- Les normes: ISO 2700X (27001, 27002, 27005, etc.), etc.
- Les méthodes:
  - Les méthodes de gestion des risques (par ex: EBIOS) ;
  - Le guide d'intégration de la SSI dans les projets;
  - Le guide externalisation
- Les guides de sécurisation (ANSSI, CLUSIF, etc.)
  - mementodep-v1-1
  - anssi-guide-passerelle_internet_securisee-v3 (Plus de 50 recommandations)
  - nt_commutateurs
  - etc
- ETC

Maintenant, c'est à vous !

A vos souris !