Cours N°4 Sécurité des Réseaux :

Généralités :

La sécurité d'un réseau est un niveau de garantie que l'ensemble des machines du réseau fonctionnent de façon optimale et que les utilisateurs possèdent uniquement les droits qui leur ont été octroyé. Il peut s'agir de:

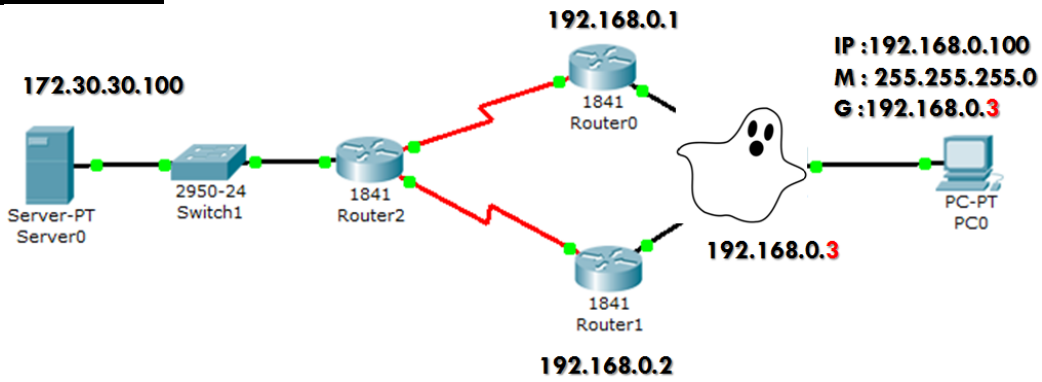
- Empêcher des personnes non autorisées d'agir sur le système de façon malveillante
- Empêcher les users d'effectuer des opérations involontaires capables de nuire au système
- Sécuriser les données en prévoyant les pannes
- Garantir la non interruption d'un service

La sûreté de fonctionnement a pour objectif de prévoir la capacité de survie du système (continuité de service).

Les solutions sont essentiellement matérielles :

- Une redondance de tout ou partie des matériels actifs
- Une redondance des liaisons Télecoms ainsi que des contrats de maintenance avec GTI & GTR
- Backup/Restore : Operating System , configurations.

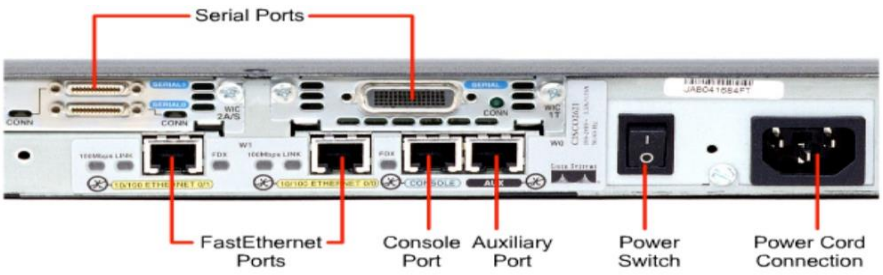
Les protocoles FHRP :



Caractéristique		HSRP	VRRP	GLBP
Déploiement		Propriétaire	Standard	Propriétaire
Timers	Intervalle : Hello	3 sec	1 sec	3 sec
	Intervalle : Dead	10 sec	3.6 sec	10 sec
Adresse IP virtuelle		Différente de celle configurée	Pouvant être l'adresse configurée	Différente de celle configurée
Adresse MAC virtuelle		0000.0C07.AC***xx*** 0000.0C9F.F***xxx*** Ou ***xx*** / ***xxx*** est la valeur hex du groupe HSRP	0000.5E00.01***xx*** Ou *xx* est la valeur hex du groupe VRRP	0007.B400.***xxyy*** Ou ***xx*** est la valeur hex du groupe GLBP et ***yy*** est un différent nombre pour chaque routeur (1, 2, 3, ou 4)
Partage de charge (Par défaut)		Non	Non	Oui
Rôle / Communication		Active Standby 224.0.0.2 UDP 1985	Master Backup 224.0.0.18 UDP 112	AVG AVF 224.0.0.102 UDP 3222

Gestion des équipements :

1) Accès physique : Empêcher l'accès physique aux équipements réseau (Salle d'équipements) :
   - Bouton Marche/Arrêt
   - Port console
   - Interfaces Ethernet



2) Telnet : Mot de passe à choisir judicieusement
   - Utilisez des ACL pour filtrer les accès
   - Accès via un VLAN d'administration
   - De préférence utilisez SSH
   - Utilisation d'un protocole d'authentification tel que RADUIS ou KERBEROS .

```
C:> telnet 192.168.1.30
User Access Verification
Password: *****
SwitchA> enable
Password: ****
Switch#  show vlan id 1

VLAN  NAME     STATUS    PORTS
----  -------  --------  -----------
1     default  active    fe0/1,fe0/2,fe0/3,
                         fe0/4,fe0/5,fe0/6,
                         fe0/7,fe0/8
```

3) Interface WEB :
   - A désactiver sur ce type d'équipement
   - Si nécessaire -> VLAN d'administration
   - Utilisation d'un protocole d'authentification tel que RADUIS ou KERBEROS .

4) SNMP :
   - Éviter le Community String public / private
   - A désactiver si non utilisé
   - Accès via un VLAN d'administration
   - Utilisation de SNMPv3
   - Utilisation d'un protocole d'authentification tel que RADUIS ou KERBEROS .

Access Control List (ACLs) :

Création → Attribution → Direction

1) Standard :
   - De 1 à 99
   - Adresse IP Source
   - **access-list** *number* {**permit** |**deny**} *Source-ip-address* Source-*wildcard-mask*
   - *EX :* Access-list 20 permit 172.16.0.0 0.0.255.255

2) Extended
   - De 100 à 199
   - Adresse IP Source & Destination
   - Protocole
   - Numéro de port
   - **access-list** *number* {**permit**|**deny**} *protocol Source-ip-address Source-wildcard-mask Destination-ip-address Destination-wildcard-mask* **eq** *port-number*
   - EX : Access-list 110 permit TCP 172.16.1.1 0.0.0.0 0.0.0.0 255.255.255.255 eq 80

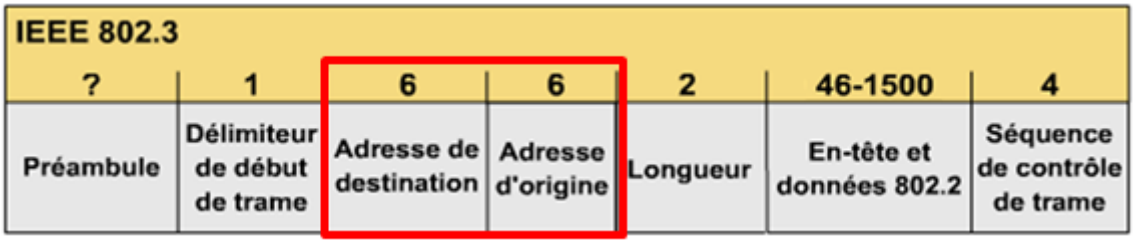
172.16.16.16 0.0.0.0 → Host 172.16.16.16
0.0.0.0 255.255.255.255 → Any

A la fin de chaque ACL : Implicit deny → Deny Any or Deny IP Any Any

Sécurité Niveau 2 (OSI) :

L'identité (Au niveau des réseau LAN) est l'adresse MAC :

- Identifiant unique codé sur 48bits
- Peut être administrée localement
- Elle identifie mais n'authentifie pas



Les protocoles rencontrés sont :

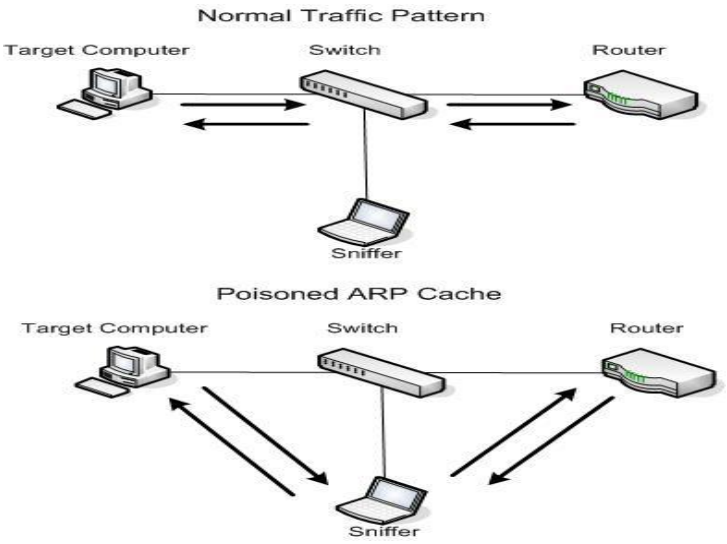
- ARP – Address resolution protocol
- CDP – Cisco Discovery protocol
- STP – Spanning Tree Protocol 802.1d
- VLAN – Virtual LAN 802.1q
- VTP – VLAN Trunking Protocol (cisco)

Type des trames : Unicast , Multicast , Broadcast .

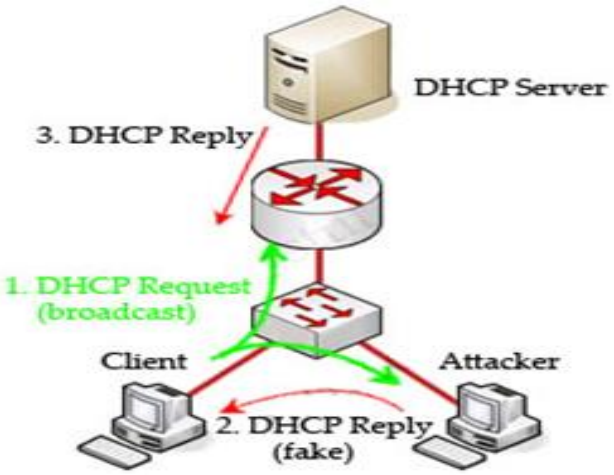
Type d'attaque Niveau 2

Les commutateurs sont la cible d'attaques telles que:

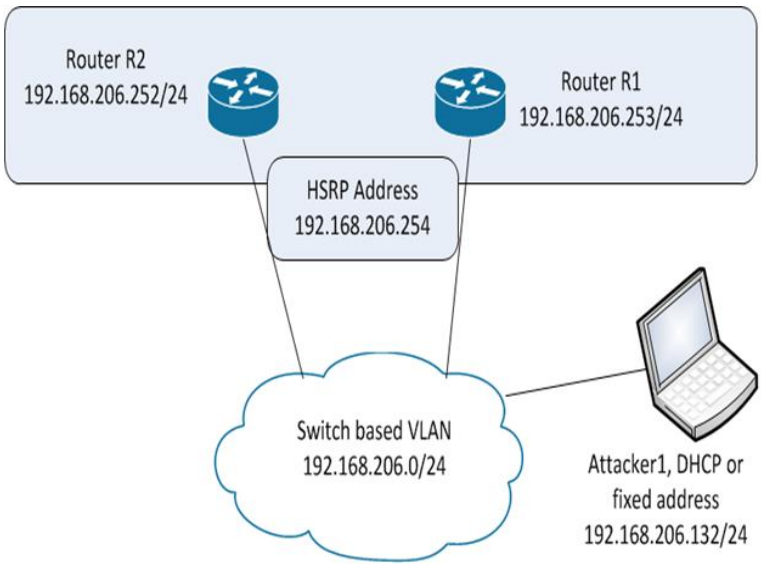
- ARP cache poisoning
  (MAC address Flooding)



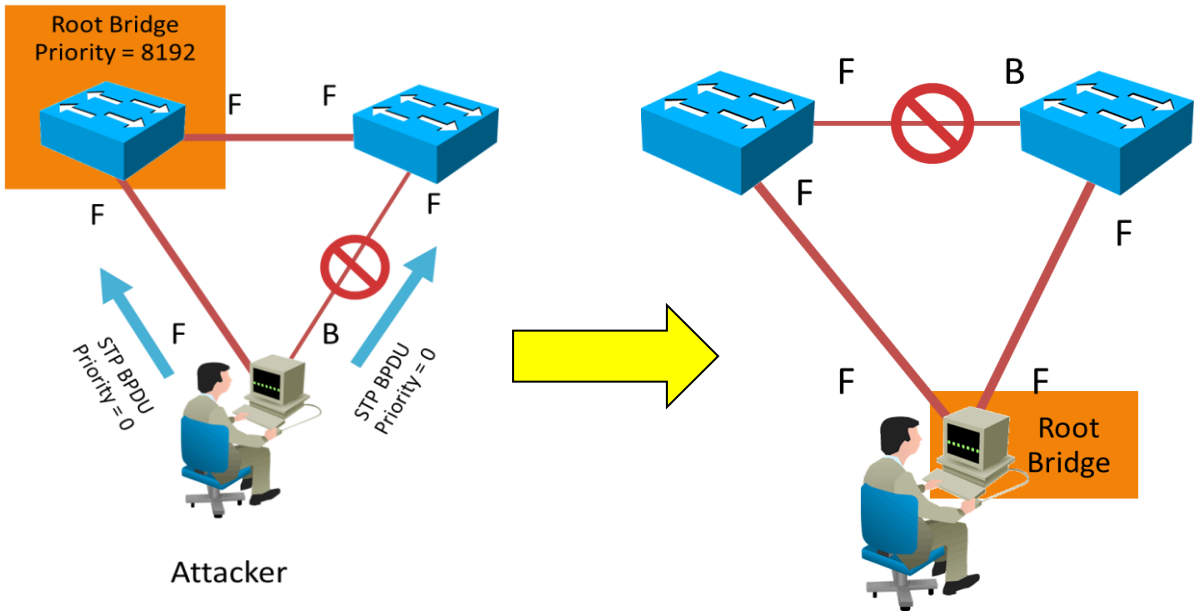
- DHCP spoofing



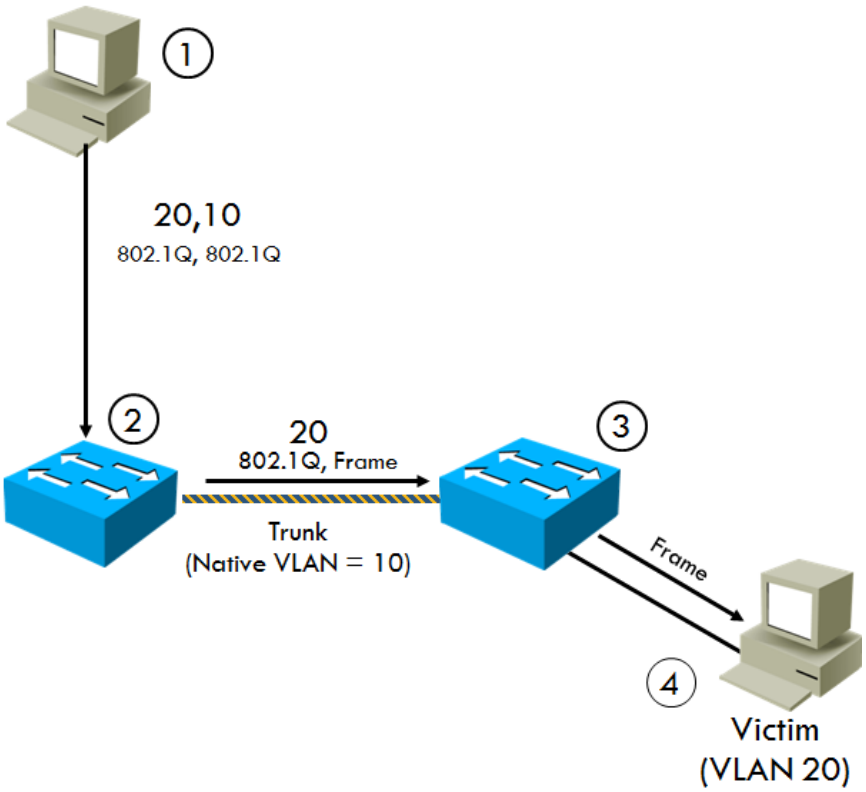
- HSRP spoofing



- STP/VTP attacks

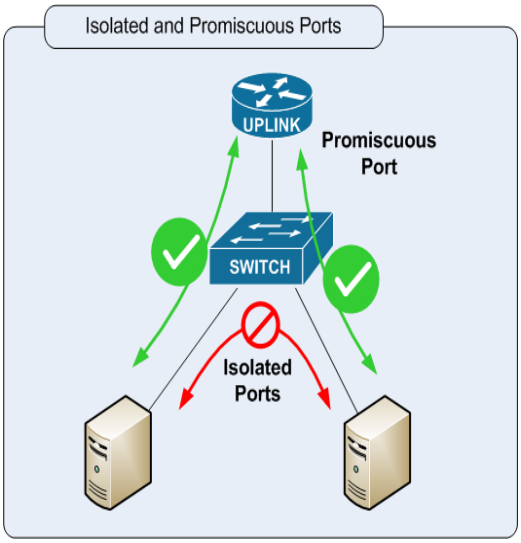


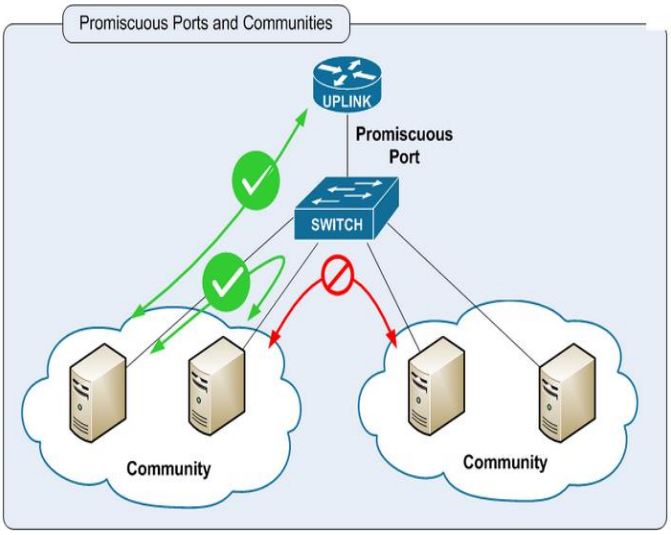
- VLAN Jumping (ISL/DTP) : Attaques : VLAN « jumping » (injection de frame 802.1q) est possible si : DTP (Dynamic Trunking Protocol) est activé et si le port est dans le même VLAN que le native VLAN (VLAN 1 par défaut)



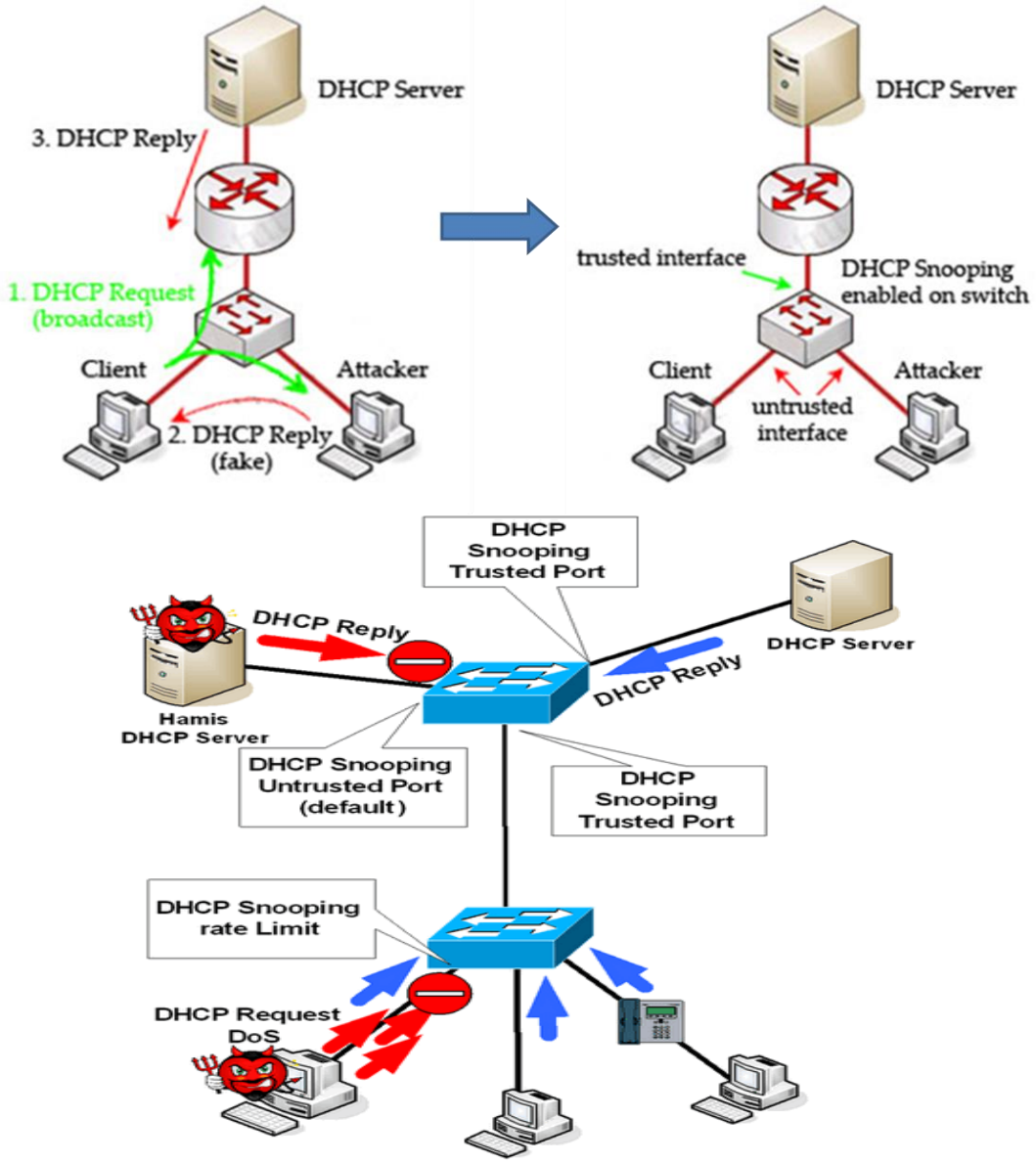
Comment se protéger ??

- Augmenter le nombre des domaines de broadcast .
- Création des sous réseau en faisant abstraction de l'organisation physique des équipements.
- Ne pas utiliser le VLAN 1 (VLAN par Défaut) , ni pour la communication ni pour la gestion
- Filtrage des adresse MAC par port : Cisco « port security » par exemple
- Activer le BPDU-Guard qui désactive un port si un BPDU est reçu via celui-ci
- Limiter le taux de broadcast
- Utiliser l'authentification MD5 pour HSRP
- Notion de Private VLAN
  - Le segment devient « Multi-Access Non Broadcast »
  - Des équipements d'un même VLAN ne peuvent pas communiquer directement entre eux.





- VTP (VLAN Trunking Protocol) – Cisco
  - Server / Client / Transparent
  - Par défaut le Mode Server sans mot de passe
  - Affecter un domaine et un mot de passe
- DTP (Dynamic Trunking Protocol)
  - Les ports sont en mode auto par défaut
  - Choisir le mode Off pour tous les ports non utilisés pour des interconnections de commutateurs



Sécurité Niveau 3 (OSI)

L'identité est l'adresse IP (TCP/IP)

- ❑ Identifiant codé sur 32 bits
- ❑ Aisément modifiable
- ❑ Identifie mais n'authentifie pas
- ❑ N'intègre aucun mécanisme de sécurité

Les protocoles rencontrés sont :

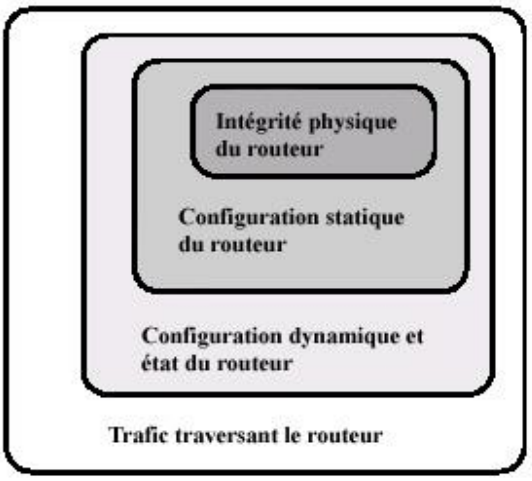
- ❑ IP – ICMP
- ❑ RARP
- ❑ Les protocoles de routages : RIP, RIPv2, IGRP, EIGRP, OSPF, BGP,…
- ❑ ……

Types des Paquets : Unicast , Multicast , Broadcast

Sécurité des routeurs

- Les routeurs assurent les services essentiels au bon fonctionnement des infrastructures de communication
- La compromission d'un routeur amène un certain nombre de problèmes favorisants la compromission des SI , la dégradation des performances, des dénis de service et l'exposition des données sensibles
- En général un routeur bien configuré permet d'améliorer grandement le niveau de sécurité global du système d'information
- La sécurité du routeur doit être le reflet de la politique de sécurité globale du SI

- Vision en couche de la sécurité du routeur



Vue en couche de la sécurité des routeurs

Acces correspondants

* Accès physiques
* Accès électriques

* Accès administratifs
* Mises à jour logicielles

* Protocoles de routage
* Protocoles d'administration

* Accès aux réseaux desservis par le routeur

Protocoles de routage

- En général
  - Utiliser « passive-interface » pour toutes les interfaces ne devant pas participer au processus de routage
  - L'enregistrement systématique de l'activité de l'équipement via les protocoles de supervision (SNMP, Syslog, …) permet de disposer en temps de crise, des informations essentielles à l'identification des problèmes
- RIP / IGRP : pas de mécanisme de sécurité, à éviter…
- RIPv2 : prévoit l'authentification
- EIGRP : prévoit l'authentification des échanges
- OSPF
  - Prévoit l'authentification des échanges (password MD5)
  - N'utilise que des mises à jour Unicast/Multicast (Pas de Broadcast)
  - Il est possible de filtrer les MAJ reçues
- BGP
  - Prévoit l'authentification des échanges
  - Ne pas utiliser le même mot de passe pour tous les routeurs
  - Si possible utiliser IPSEC

Routeur filtrant

- Le rôle principal du « routeur filtre de paquets » est de permettre ou d'empêcher le passage des paquets de données reçus.
- Le routeur examine tous les datagrammes par rapport à des règles de filtrage, basées sur le contenu informationnel de l'entête du datagramme
- Le filtrage s'effectue aux niveaux 2,3,4 du modèle OSI
- Méthode d'intrusion typique contournant le filtrage de paquets : la fragmentation de paquet. Cette technique consiste à utiliser la propriété de fragmentation de IP afin de créer de tous petits fragments et de forcer l'en-tête TCP à être fragmentée elle aussi, l'espoir étant que seul le premier fragment sera analysé par le routeur, laissant alors passer tout le reste.

Les solutions de sécurité sont encore majoritairement basées sur l'emploi unique de routeurs filtrants. Cela s'explique pour plusieurs raisons :

- le coût généralement faible d'un routeur filtrant
- les performances sont généralement bonnes
- la transparence aux utilisateurs et aux applications
- fiable car les contrôles sont simples et peu sujets à erreurs d'implémentation

Les limites des routeurs filtrants sont mises en évidence par le besoin de contrôle du contenu informationnel des échanges :

- Les performances du routeur diminuent avec le nombre de règles à appliquer
- Le routeur filtrant ne peut pas comprendre le contexte du service qu'il rend : il ne peut pas, par exemple bloquer l'entrée de mails ou de newsgroup concernant certains sujets
- Ne traite que des informations du type en-tête du paquet
- Pas ou peu de statistiques sur l'usage des filtres
- La protection du réseau connecté à l'Internet est minimale