Sécurisation Lan

Résumer protection switch :

Stratégies de sécurité pour le switch:

// Port security

switchport port-security maximum 1 — switchport port-security violation shutdown — shutdown + switchport access vlan 999

//désactiver les ports inutiles

//vlan de management

//bannière et timeout

//désactiver CDP/LLDP sur les interface non trunk ou exposées

// DHCP Snooping

// désactiver dtp

//changer le vlan natif

interface vlan 99

//mots de passe chiffrés

//ssh

//dynamic arp inspection

//ip source guard

//802.1x

Résumer protection Routeur :

sécurité pour le routeur:

// Accès & authentification

//Désactivation des services inutiles
no service tcp-small-servers — no cdp enable — no ip http server — no ip proxy-arp — no ip directed-broadcast

//Sécurité des protocoles de routage
ip ospf authentication message-digest — ip authentication mode eigrp 1 md5 — passive-interface default — neighbor x.x.x.x password <clé>

//Hardening avancé

Lignes Routeur:

// Accès & authentification

! Mot de passe enable chiffré
enable secret <mdp>
service password-encryption
username admin privilege 15 secret <mdp>

! Génération clé RSA + SSH v2
crypto key generate rsa modulus 2048
ip ssh version 2

! Sécurisation lignes VTY (sécurisation connexion ssh)
line vty 0 4
 transport input ssh

```
 exec-timeout 5 0
 login local
 access-class ACL_ADMIN in

! Sécurisation console
line console 0
 exec-timeout 5 0
 login local

! Bannière légale
banner motd ^Acces autorise uniquement^

// Désactivation des services inutiles

no service tcp-small-servers
no service udp-small-servers
no service finger       (Désactive le protocole Finger (port 79), qui permettait de lister les utilisateurs connectés sur le routeur)

! Services IP dangereux
no ip bootp server     (Désactive le serveur BOOTP. Évite que le routeur réponde à des requêtes d'amorçage réseau non sollicitées)
no ip http server      (Désactive l'interface web d'administration en HTTP (non chiffré))
no ip http secure-server    (https)
no ip proxy-arp      (Empêche le routeur de répondre aux requêtes ARP à la place d'autres machines. Réduit les risques de ARP spoofing)
no ip directed-broadcast     (Bloque les broadcasts dirigés vers un sous-réseau)
no ip source-route     (Désactive la possibilité pour un paquet IP de dicter son propre chemin dans le réseau)

! Désactiver CDP globalement
no cdp run    (cache certaines configuration)

// acl

! Bloquer adresses RFC 1918 et bogons en entrée WAN
ip access-list extended ACL_ANTI_SPOOF
 deny ip 10.0.0.0 0.255.255.255      any
 deny ip 172.16.0.0 0.15.255.255   any
 deny ip 192.168.0.0 0.0.255.255   any
 deny ip 127.0.0.0 0.255.255.255   any
```

```
 permit ip any any

! Application sur interface WAN + uRPF
interface GigabitEthernet0/0
 ip access-group ACL_ANTI_SPOOF in
 ip verify unicast source reachable-via rx

 // Sécurité des protocoles de routage

! Authentification OSPF MD5
router ospf 1
 area 0 authentication message-digest

interface GigabitEthernet0/1
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 <clé>

! Interfaces passives par défaut
router ospf 1
 passive-interface default
 no passive-interface GigabitEthernet0/1

! Authentification EIGRP MD5
router eigrp 1
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 <keychain>
```

Lignes switch:

```
// Sécurité des VLANs

! Déclaration des VLANs
vlan 10
 name USERS
vlan 20
 name FINANCE
vlan 99
```

```
 name MANAGEMENT
vlan 999
 name BLACKHOLE

! Interface de management
interface vlan 99
 ip address 192.168.99.1 255.255.255.0
 no shutdown

! Sécurisation des trunks
switchport trunk native vlan 999
switchport trunk allowed vlan 10,20,99

// Sécurité des ports access

! Ports utilisateurs (Fa0/1 - 20)
interface range FastEthernet 0/1 - 20
 switchport mode access
 switchport access vlan 10
 switchport nonegotiate
 switchport port-security maximum 1        (Limite à une seule adresse MAC autorisée sur ce port. Si un deuxième équipement est branché)
 switchport port-security violation shutdown     (Définit l'action en cas de violation : le port passe en mode err-disabled (shutdown automatique). Il faudra alors faire un shutdown puis no shutdown)

 switchport port-security     (Active la sécurité de port sur l'interface. Sans cette ligne, les deux précédentes n'ont aucun effet)
 spanning-tree portfast
 spanning-tree bpduguard enable
 no cdp enable
 no shutdown

! Ports inutilisés → VLAN blackhole + shutdown
interface range FastEthernet 0/21 - 24
 switchport mode access
 switchport access vlan 999
 shutdown

//Protection L2 (DHCP / ARP / IP)
```

```
! DHCP Snooping
//plus pour les ports
ip dhcp snooping ou ip dhcp snooping trust
ip dhcp snooping limit rate 6
//plus pour les vlans
ip dhcp snooping vlan 10,20
no ip dhcp snooping information option

interface GigabitEthernet 0/1
 ip dhcp snooping trust

! Dynamic ARP Inspection (DAI)
ip arp inspection vlan 10,20

interface GigabitEthernet 0/1
 ip arp inspection trust

! IP Source Guard sur ports access
interface range FastEthernet 0/1 - 20
 ip verify source (port untrusted tel que pc ou visiteur etc..)
 //ou pour filtrage ip + mac (ip verify soyrce port-security)

// spanning-tree

! PortFast + BPDU Guard globaux
spanning-tree portfast default    (Active PortFast sur tous les ports d'accès du switch globalement.)
spanning-tree portfast bpduguard default
```

Revision #3
Created 26 March 2026 10:03:38 by Ilian
Updated 26 March 2026 10:10:19 by Ilian