🔒 GUIDE DE SÉCURISATION DU RÉSEAU D'ENTREPRISE

Table des matières

---

1. SÉCURISATION DES ACCÈS AUX ÉQUIPEMENTS

A. Configuration des mots de passe

```bash
```

```
enable
configure terminal

# Mot de passe enable (mode privilégié) - CHIFFRÉ avec secret
enable secret Cisco@2025!

# Mot de passe console
line console 0
password Console@2025
login
exit

# Mot de passe VTY (Telnet/SSH)
line vty 0 4
password VTY@2025
login
transport input ssh
exit

# Chiffrer TOUS les mots de passe dans la config
service password-encryption

# Bannière de sécurité (dissuasion légale)
banner motd #
**************************************
ACCES NON AUTORISE INTERDIT
Toute tentative sera enregistrée et poursuivie
Système surveillé 24/7
**************************************
#

end
write memory
```

B. Configuration SSH (recommandé au lieu de Telnet)

Pourquoi SSH ?

- Chiffrement de toutes les communications
- Authentification forte
- Protection contre l'interception (Man-in-the-Middle)

```
bash
```

```
enable
configure terminal

# Définir le nom d'hôte et le domaine (requis pour SSH)
hostname R1
ip domain-name entreprise.local

# Générer les clés de chiffrement RSA
crypto key generate rsa
# Choisir 2048 bits minimum (4096 pour sécurité maximale)

# Configurer SSH version 2 (plus sécurisé que v1)
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 3

# Créer des comptes utilisateurs locaux
username admin privilege 15 secret Admin@2025!
username technicien privilege 7 secret Tech@2025!
username auditeur privilege 1 secret Audit@2025!

# Configurer les lignes VTY pour SSH uniquement
line vty 0 4
transport input ssh
login local
exec-timeout 10 0
exit

end
write memory
```

C. Désactiver les comptes par défaut

```
bash

# Supprimer ou désactiver le compte par défaut
no username cisco
```

---

2. SÉCURISATION DES VLANs

A. Listes de Contrôle d'Accès (ACL)

Les ACL permettent de filtrer le trafic entre les VLANs selon des règles définies.

Exemple 1 : Empêcher le VLAN Sales (10) d'accéder aux Servers (40)

```bash
enable
configure terminal

# ACL étendue
access-list 100 remark Bloquer Sales vers Servers
access-list 100 deny ip 172.16.10.0 0.0.0.255 172.16.11.96 0.0.0.15
access-list 100 permit ip any any

# Appliquer sur l'interface du routeur
interface fa0/1.10
ip access-group 100 in
exit

end
write memory
```

Exemple 2 : Autoriser uniquement Management à administrer les équipements

```bash
# ACL pour SSH/Telnet
access-list 10 remark Autoriser uniquement Management
access-list 10 permit 172.16.11.64 0.0.0.31
access-list 10 deny any

# Appliquer sur les lignes VTY
line vty 0 4
access-class 10 in
exit
```

Exemple 3 : Contrôle granulaire par service

```bash
# Bloquer HTTP/HTTPS du VLAN Research vers Internet
access-list 101 deny tcp 172.16.11.0 0.0.0.63 any eq 80
access-list 101 deny tcp 172.16.11.0 0.0.0.63 any eq 443
access-list 101 permit ip any any

interface fa0/1.20
ip access-group 101 in
exit
```

B. Private VLANs (PVLANs)

Isoler les machines dans un même VLAN (utile pour les zones invités ou IoT).

```bash
# Sur le switch
vlan 50
private-vlan primary
private-vlan association 51,52
exit

vlan 51
private-vlan isolated
exit

vlan 52
private-vlan community
exit

# Appliquer sur les interfaces
interface range fa0/10-15
switchport mode private-vlan host
switchport private-vlan host-association 50 51
exit
```

---

3. SÉCURISATION DU ROUTAGE

A. Désactiver les services inutiles

```bash
```

```
enable
configure terminal

# Désactiver HTTP/HTTPS
no ip http server
no ip http secure-server

# Désactiver CDP (révèle des infos sur la topologie)
no cdp run

# Désactiver les services dangereux
no service finger
no ip bootp server
no ip source-route
no ip domain-lookup

# Désactiver l'interface de management si non utilisée
interface vlan 1
shutdown
exit

end
write memory
```

B. Authentification des mises à jour de routage

Pour les protocoles dynamiques (OSPF, EIGRP) :

```
bash

# OSPF avec authentification MD5
router ospf 1
area 0 authentication message-digest
exit

interface fa0/0
ip ospf message-digest-key 1 md5 SecureKey@2025
exit
```

---

4. SÉCURISATION DES PORTS (Port Security)

Limite le nombre d'adresses MAC autorisées par port, empêchant les attaques par usurpation MAC.

Configuration de base

```bash
enable
configure terminal

# Configuration sur un port d'accès
interface fa0/5
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security violation shutdown
switchport port-security mac-address sticky
exit

end
write memory
```

Configuration avancée

```bash
# Sur plusieurs ports simultanément
interface range fa0/1-20
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security aging time 120
switchport port-security aging type inactivity
exit
```

Types de violations

Mode	Comportement
protect	Bloque le trafic des MAC non autorisées silencieusement
restrict	Bloque + envoie une alerte SNMP + incrémente un compteur
shutdown	Désactive le port (err-disabled) - **LE PLUS SÉCURISÉ**

Récupération après violation (shutdown)

```bash
```

```
# Réactiver un port désactivé
interface fa0/5
shutdown
no shutdown
exit

# Ou configurer la récupération automatique
errdisable recovery cause psecure-violation
errdisable recovery interval 300
```

---

5. SÉCURISATION DU SPANNING TREE

Protéger contre les attaques STP qui peuvent perturber toute la topologie.

A. BPDU Guard

Désactive immédiatement un port si une BPDU est reçue (empêche un switch malveillant).

```
bash

enable
configure terminal

# Sur les ports d'accès (end-users)
interface range fa0/1-20
spanning-tree portfast
spanning-tree bpduguard enable
exit

# Global (tous les ports PortFast)
spanning-tree portfast bpduguard default

end
write memory
```

B. Root Guard

Empêche un port de devenir le port racine (protection contre l'élection d'un faux root bridge).

```
bash

# Sur les ports trunk
interface fa0/24
spanning-tree guard root
exit
```

C. Loop Guard

Protège contre les boucles créées par des liens unidirectionnels.

```bash
spanning-tree loopguard default
```

---

6. DHCP SNOOPING

Protège contre les attaques de faux serveurs DHCP et l'empoisonnement DHCP.

Configuration

```bash
enable
configure terminal

# Activer DHCP Snooping globalement
ip dhcp snooping
ip dhcp snooping vlan 10,20,30,40

# Définir les ports de confiance (vers les vrais serveurs DHCP/routeurs)
interface fa0/24
ip dhcp snooping trust
exit

# Limiter le taux sur les ports non-fiables (DOS protection)
interface range fa0/1-20
ip dhcp snooping limit rate 10
exit

# Activer l'insertion Option 82
ip dhcp snooping information option

end
write memory
```

Vérification

```bash
show ip dhcp snooping
show ip dhcp snooping binding
```

7. DYNAMIC ARP INSPECTION (DAI)

Protège contre les attaques ARP spoofing et Man-in-the-Middle.

Prérequis : DHCP Snooping doit être activé

Configuration

```bash
enable
configure terminal

# Activer DAI sur les VLANs
ip arp inspection vlan 10,20,30,40

# Définir les ports de confiance
interface fa0/24
ip arp inspection trust
exit

# Limiter le taux ARP (protection DOS)
interface range fa0/1-20
ip arp inspection limit rate 15
exit

# Validation supplémentaire
ip arp inspection validate src-mac dst-mac ip

end
write memory
```

Vérification

```bash
show ip arp inspection
show ip arp inspection statistics
```

---

8. SÉCURISATION WIFI (amélioration)

A. Masquer le SSID

Sur l'Access Point :

- **SSID Broadcast** : Désactivé (sécurité par l'obscurité - faible mais utile)

B. Filtrage MAC

Créer une liste blanche d'adresses MAC autorisées :

```
# Sur l'Access Point
- Activer le filtrage MAC
- Ajouter uniquement les adresses MAC autorisées
```

C. Utiliser WPA3 (si disponible)

- **WPA3-Personal** : Meilleure protection que WPA2-PSK
- **WPA3-Enterprise** : Avec serveur RADIUS pour authentification individuelle

D. Segmentation WiFi

Créer des réseaux WiFi séparés :

```bash
# VLAN pour invités (isolé du réseau principal)
vlan 99
name Guest-WiFi
exit

# VLAN pour employés
vlan 10
name Employee-WiFi
exit
```

E. Désactiver WPS

Le WPS (WiFi Protected Setup) est vulnérable aux attaques brute-force.

---

9. LOGGING ET MONITORING

A. Configuration des logs

```bash
```

```
enable
configure terminal

# Activer les logs
logging on
logging buffered 51200
logging console critical
logging monitor informational
logging trap warnings

# Envoyer les logs vers un serveur Syslog externe
logging host 10.10.10.10
logging source-interface fa0/0

# Horodatage précis
service timestamps log datetime msec localtime show-timezone
service timestamps debug datetime msec

# Numérotation des messages
service sequence-numbers

end
write memory
```

B. SNMP sécurisé

```bash
# SNMPv3 (recommandé - chiffré et authentifié)
snmp-server group ADMIN v3 priv
snmp-server user admin ADMIN v3 auth sha AuthPass@2025 priv aes 128 PrivPass@2025

# Limiter l'accès SNMP
access-list 20 permit 172.16.11.64 0.0.0.31
snmp-server community SecureR3ad RO 20
snmp-server community SecureWr1te RW 20

# Informations de localisation
snmp-server location "Salle Serveurs - Batiment A"
snmp-server contact "admin@entreprise.fr"

# Activer les traps
snmp-server enable traps
```

C. Vérification des logs

```bash
show logging
show logging history
```

---

10. SAUVEGARDE ET REDONDANCE

A. Sauvegarde automatique

```bash
# Sauvegarde vers un serveur TFTP
copy running-config tftp://10.10.10.10/backups/R1-config-$(date).cfg

# Script de sauvegarde automatique (via Kron ou EEM)
kron occurrence BACKUP-DAILY at 2:00 recurring
policy-list BACKUP-POLICY
exit

kron policy-list BACKUP-POLICY
cli copy running-config tftp://10.10.10.10/backup-R1.cfg
exit
```

B. Redondance avec HSRP

Hot Standby Router Protocol - deux routeurs partagent une IP virtuelle.

```bash
```

```
# Sur R1 (routeur principal)
interface fa0/1.10
standby 10 ip 172.16.10.254
standby 10 priority 110
standby 10 preempt
standby 10 authentication md5 key-string HSRPKey@2025
exit

# Sur R2 (routeur de secours)
interface fa0/1.10
standby 10 ip 172.16.10.254
standby 10 priority 100
standby 10 preempt
standby 10 authentication md5 key-string HSRPKey@2025
exit
```

C. Stackwise / VSS pour les switches

Combine plusieurs switches physiques en un seul switch logique.

---

11. FIREWALL ET NAT

A. Zone-Based Firewall (ZBF)

bash

```
# Définir les classes de trafic
class-map type inspect match-any INTERNET-TRAFFIC
match protocol tcp
match protocol udp
match protocol icmp
exit

# Définir la politique
policy-map type inspect INTERNET-POLICY
class type inspect INTERNET-TRAFFIC
inspect
exit
class class-default
drop
exit

# Créer les zones de sécurité
zone security INSIDE
zone security OUTSIDE
zone security DMZ

# Créer les paires de zones et appliquer les politiques
zone-pair security IN-TO-OUT source INSIDE destination OUTSIDE
service-policy type inspect INTERNET-POLICY
exit

zone-pair security OUT-TO-IN source OUTSIDE destination INSIDE
service-policy type inspect RETURN-POLICY
exit

# Assigner les interfaces aux zones
interface fa0/1
zone-member security INSIDE
exit

interface se0/3/0
zone-member security OUTSIDE
exit
```

B. NAT/PAT (Network Address Translation)

bash

```
# Définir les réseaux internes
access-list 1 permit 172.16.0.0 0.0.255.255
access-list 1 permit 10.0.0.0 0.255.255.255

# Configurer les interfaces
interface se0/3/0
ip nat outside
exit

interface fa0/1
ip nat inside
exit

# NAT Overload (PAT) - plusieurs IPs internes -> 1 IP publique
ip nat inside source list 1 interface se0/3/0 overload

# NAT statique pour les serveurs (DMZ)
ip nat inside source static 172.16.11.97 88.40.12.10
```

---

12. SEGMENTATION SUPPLÉMENTAIRE

A. Créer une DMZ

Zone démilitarisée pour les serveurs accessibles depuis Internet.

bash

```
# Créer le VLAN DMZ
vlan 50
name DMZ
exit

# Configuration routeur
interface fa0/1.50
encapsulation dot1Q 50
ip address 192.168.50.254 255.255.255.0
exit

# ACL restrictive pour la DMZ
access-list 110 permit tcp any host 192.168.50.10 eq 80
access-list 110 permit tcp any host 192.168.50.10 eq 443
access-list 110 deny ip any any

interface fa0/1.50
ip access-group 110 in
exit
```

B. VLANs par type d'équipement

bash

```
# VLAN Imprimantes
vlan 60
name Printers
exit

# VLAN IoT (objets connectés)
vlan 70
name IoT
exit

# VLAN VoIP (téléphonie)
vlan 80
name Voice
exit

# VLAN Caméras de surveillance
vlan 90
name CCTV
exit
```

---

13. AUTHENTIFICATION 802.1X

Authentification réseau basée sur un serveur RADIUS (AAA).

A. Configuration du serveur RADIUS

Sur le serveur RADIUS, configurer :

- Utilisateurs et leurs credentials
- Politiques d'accès
- Attributs VLAN dynamiques

B. Configuration sur le switch

```bash
enable
configure terminal

# Activer AAA
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius

# Configurer le serveur RADIUS
radius-server host 10.10.10.5 key RadiusKey@2025!
radius-server timeout 5
radius-server retransmit 3

# Configuration globale 802.1X
dot1x system-auth-control

# Configuration par port
interface range fa0/1-20
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast
exit

# Fallback en cas d'échec RADIUS
aaa authentication dot1x default group radius local

end
write memory
```

C. Vérification

```bash
show dot1x all
show authentication sessions
```

---

14. VPN (Virtual Private Network)

Connexions sécurisées chiffrées pour les accès distants.

A. Site-to-Site VPN (IPsec)

```bash
```

```
# Phase 1 - ISAKMP Policy
crypto isakmp policy 10
encryption aes 256
hash sha256
authentication pre-share
group 14
lifetime 86400
exit

# Clé pré-partagée
crypto isakmp key VPN@SecureKey2025! address 88.40.11.1

# Phase 2 - Transform Set
crypto ipsec transform-set TRANSFORM esp-aes 256 esp-sha256-hmac
mode tunnel
exit

# Définir le trafic à chiffrer
access-list 110 permit ip 172.16.10.0 0.0.0.255 172.16.12.0 0.0.0.255

# Crypto Map
crypto map VPNMAP 10 ipsec-isakmp
set peer 88.40.11.1
set transform-set TRANSFORM
match address 110
exit

# Appliquer sur l'interface
interface se0/3/0
crypto map VPNMAP
exit

end
write memory
```

B. Remote Access VPN (SSL VPN / IPsec VPN)

Pour les utilisateurs nomades.

```
bash
```

```
# Créer un pool d'adresses pour les clients VPN
ip local pool VPN-POOL 192.168.100.1 192.168.100.50

# Configuration AAA pour VPN
aaa authentication login VPN-AUTH local
aaa authorization network VPN-AUTHOR local

# Créer un groupe VPN
crypto isakmp client configuration group VPN-GROUP
key VPN@GroupKey2025!
pool VPN-POOL
exit
```

🎯 PRIORITÉS DE SÉCURITÉ

NIVEAU 1 - ESSENTIEL ⚠️ (À faire immédiatement)

Priorité	Mesure	Impact	Difficulté
1	Mots de passe forts	Élevé	Faible
2	SSH au lieu de Telnet	Élevé	Faible
3	Service password-encryption	Moyen	Faible
4	Port Security	Élevé	Faible
5	ACL de base	Élevé	Moyen
6	Désactiver services inutiles	Moyen	Faible

Temps estimé : 2-4 heures

NIVEAU 2 - IMPORTANT ⚡ (Court terme - 1 semaine)

Priorité	Mesure	Impact	Difficulté
7	DHCP Snooping	Élevé	Moyen
8	BPDU Guard / Root Guard	Élevé	Faible
9	Logging centralisé	Moyen	Moyen
10	Bannières de sécurité	Faible	Faible
11	Sauvegardes automatiques	Élevé	Moyen

Temps estimé : 1-2 jours

NIVEAU 3 - AVANCÉ 🔒 (Moyen terme - 1 mois)

Priorité	Mesure	Impact	Difficulté
12	Dynamic ARP Inspection	Moyen	Moyen
13	Zone-Based Firewall	Élevé	Élevé
14	NAT/PAT	Élevé	Moyen
15	Segmentation avancée (DMZ)	Élevé	Moyen
16	SNMP sécurisé	Moyen	Faible

Temps estimé : 3-5 jours

NIVEAU 4 - EXPERT 🛡️ (Long terme - 3-6 mois)

Priorité	Mesure	Impact	Difficulté
17	802.1X avec RADIUS	Très élevé	Élevé
18	Site-to-Site VPN	Élevé	Élevé
19	Remote Access VPN	Élevé	Élevé
20	HSRP / Redondance	Élevé	Moyen
21	IPS/IDS intégré	Très élevé	Très élevé

Temps estimé : 1-2 semaines

📊 MATRICE DE RISQUES

Menace	Probabilité	Impact	Risque	Mesure de protection
Accès non autorisé	Élevée	Critique	**CRITIQUE**	SSH + mots de passe forts + 802.1X
Attaque MITM	Moyenne	Élevé	**ÉLEVÉ**	DHCP Snooping + DAI
Usurpation MAC	Élevée	Moyen	**ÉLEVÉ**	Port Security
Attaque STP	Faible	Critique	**MOYEN**	BPDU Guard + Root Guard
Serveur DHCP malveillant	Moyenne	Élevé	**ÉLEVÉ**	DHCP Snooping
Accès inter-VLAN non autorisé	Moyenne	Élevé	**ÉLEVÉ**	ACL + Firewall
Fuite d'informations	Faible	Moyen	**FAIBLE**	Désactiver CDP + bannières

---

🔍 AUDIT DE SÉCURITÉ - CHECKLIST

Accès et authentification

- [ ] Tous les mots de passe sont complexes (12+ caractères, majuscules, minuscules, chiffres, symboles)
- [ ] SSH activé, Telnet désactivé
- [ ] Authentification locale ou RADIUS configurée
- [ ] Bannières d'avertissement présentes
- [ ] Timeout de session configuré (10 minutes)

Configuration réseau

- [ ] VLANs correctement segmentés
- [ ] ACL configurées entre VLANs sensibles
- [ ] Port Security activé sur tous les ports d'accès
- [ ] DHCP Snooping activé
- [ ] Dynamic ARP Inspection activé
- [ ] BPDU Guard / Root Guard configurés

Services et protocoles

- [ ] Services inutiles désactivés (HTTP, CDP, etc.)
- [ ] SSH v2 uniquement (pas v1)
- [ ] SNMP v3 ou communautés fortes
- [ ] NTP configuré pour synchronisation horaire
- [ ] Syslog centralisé configuré

Sauvegardes et redondance

- [ ] Sauvegardes automatiques quotidiennes
- [ ] Sauvegardes stockées hors site
- [ ] Redondance des équipements critiques (HSRP/VRRP)
- [ ] Plan de reprise après sinistre (DRP)

Monitoring

- [ ] Logs centralisés et archivés
- [ ] Alertes configurées pour événements critiques
- [ ] Surveillance SNMP active
- [ ] Audits de sécurité réguliers planifiés

📚 RESSOURCES COMPLÉMENTAIRES

Documentation Cisco

- Cisco Security Configuration Guide
- Cisco IOS Hardening Guide

Standards de sécurité

- **ISO 27001** : Gestion de la sécurité de l'information
- **NIST Cybersecurity Framework** : Framework de cybersécurité
- **CIS Controls** : Contrôles de sécurité critiques

Outils d'audit

- **Nmap** : Scan de vulnérabilités réseau
- **Wireshark** : Analyse de trafic
- **Nessus** : Scanner de vulnérabilités
- **OpenVAS** : Scanner open-source

🚨 EN CAS D'INCIDENT

Procédure d'urgence

1. **Isoler** : Déconnecter le segment compromis
2. **Identifier** : Analyser les logs pour comprendre l'attaque
3. **Éradiquer** : Supprimer la menace
4. **Récupérer** : Restaurer depuis les sauvegardes
5. **Documenter** : Rapport d'incident détaillé
6. **Améliorer** : Mettre à jour les procédures

Contacts d'urgence

- Administrateur réseau : [Contact]
- RSSI : [Contact]
- Support Cisco TAC : +33 1 58 04 01 01
- CERT-FR : cert-fr.cossi@ssi.gouv.fr

📝 NOTES FINALES

Ce guide couvre les mesures de sécurité essentielles à avancées pour un réseau d'entreprise. La sécurité est un processus continu nécessitant :

- **Veille technologique** constante
- **Mises à jour régulières** des équipements
- **Formation** continue des équipes
- **Audits** de sécurité périodiques
- **Tests d'intrusion** réguliers
- **Revue** des politiques de sécurité

La sécurité à 100% n'existe pas. L'objectif est de rendre l'attaque suffisamment difficile et coûteuse pour décourager les attaquants.

Document créé pour le TP Réseau Cisco - SIO SISR2 2025 Dernière mise à jour : Octobre 2025