# Documentation technique

## Projet Infra-Site – RIOCA, groupe 3

BTS SIO 2e année, option SISR – Lycée Saint Adjutor

AP Infra-Site : cloisonnement et interconnexion des zones LAN, DMZ et Internet

Version du 6 octobre 2026

# Sommaire

**1. Périmètre et architecture** ..... 3
Zones et adressage ..... 3
Équipements ..... 3
Maquette physique ..... 3
**2. Switch DMZ (SwDmz_Grp3)** ..... 4
Remise à zéro ..... 4
Configuration de base ..... 6
**3. Switch Internet (SwNET_Grp3)** ..... 7
Remise à zéro ..... 7
Configuration de base ..... 7
**4. Routeur Internet (RNET_GRP3)** ..... 8
Interfaces ..... 8
NAT overload (PAT) et publication des serveurs web ..... 8
**5. Pare-feu RParefeu : configuration de base** ..... 9
Mise en service ..... 9
Interfaces et zones ..... 10
**6. Routage RIP v2** ..... 10
SwCoeur (SW_COEUR_GRP3) ..... 10
RParefeu ..... 11
RNET_GRP3 ..... 11
Problèmes rencontrés ..... 12
Vérification ..... 12
**7. Administration distante sécurisée** ..... 14
SSH sur les lignes VTY ..... 14
VLAN d'administration externe ..... 14
Contrôle d'accès ..... 14
Bannière d'avertissement ..... 14
Vérification ..... 15
**8. Sauvegarde automatique des configurations** ..... 16
Serveur TFTP ..... 16
Équipements Cisco : tâches kron ..... 17
SwNET, Sw1e et Sw2e : applets EEM ..... 17
Pare-feu Zyxel : script et cron sur le serveur ..... 18
Vérification ..... 19
**9. Règles de pare-feu implémentées** ..... 20
Objets créés ..... 21
Tableau des règles ..... 21
Durcissement des règles par défaut ..... 22
**10. ACL du LAN sur SwCoeur** ..... 22
Contenu de l'ACL ..... 22
Application sur les interfaces VLAN ..... 23
Vérification ..... 23

*Chaque ligne est un lien cliquable (Ctrl + clic dans Word). Pour actualiser les numéros de page après une modification : Ctrl + A puis F9.*

# 1. Périmètre et architecture

Le projet Infra-Site ajoute au LAN de RIOCA une zone DMZ et une zone Internet, séparées par le pare-feu RParefeu. Ce document rassemble les configurations réalisées sur les nouveaux équipements et sur SwCoeur, pour le transfert de compétence prévu par la lettre de mission.

## Zones et adressage

| Zone | Réseau | Éléments |
|---|---|---|
| LAN | 172.19.0.0/16 (VLAN 10 à 100, en 172.19.x.0/24) | Postes des services, VLAN IT 172.19.60.0/24, serveurs du VLAN 100 (contrôleur de domaine AD, serveur TFTP 172.19.100.5). Routage inter-VLAN par SwCoeur. |
| DMZ | 10.3.0.0/16 | WebPrimaire 10.3.10.1, WebSecondaire 10.3.10.2, pare-feu 10.3.10.254, SwDmz |
| Internet | 192.168.3.248/29 | RNET1 192.168.3.251, RNET2 192.168.3.252, pare-feu 192.168.3.253, SwNET 192.168.3.254 |
| Campus (Internet réel) | 192.168.4.0/24 | RNET1 192.168.4.31, routeur du labo 192.168.4.254 (non administrable par le groupe) |

## Équipements

| Équipement | Hostname | Matériel | Rôle |
|---|---|---|---|
| Switch DMZ | SwDmz_Grp3 | Cisco Catalyst 2960, IOS 12.2(55)SE7 | Raccorde les serveurs web de la DMZ au pare-feu |
| Switch Internet | SwNET_Grp3 | Cisco Catalyst 2960-X | Relie le pare-feu aux routeurs Internet |
| Routeur Internet | RNET_GRP3 | Cisco 2900 | Sortie vers le campus, NAT |
| Pare-feu | RParefeu | Zyxel USG Flex 500 | Contrôle les flux entre LAN, DMZ et Internet |
| Switch cœur | SW_COEUR_GRP3 | Cisco Catalyst 3650 | Routage inter-VLAN, RIP v2, ACL du LAN |

## Maquette physique

La maquette est montée dans une baie : de haut en bas, les switchs d'étage (SW2E, SW1ER, SWRDC), le switch cœur SWCOEUR, le pare-feu Zyxel, puis les switchs de la DMZ et d'Internet et les routeurs Cisco.

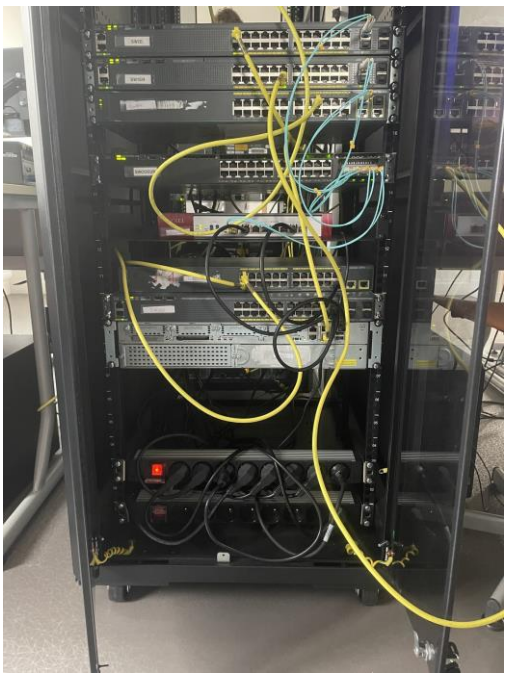


*Photo : baie de la maquette (face avant).*

# 2. Switch DMZ (SwDmz_Grp3)

SwDmz_Grp3 a été remis à zéro, puis configuré avec une IP de management dans la DMZ, le domaine VTP RIOCA en mode client et un accès distant protégé par mot de passe.

## Remise à zéro

Le switch contenait une ancienne configuration. Depuis le bootloader (invite `switch:`), il faut supprimer les fichiers de configuration et de VLAN, y compris les copies `.renamed`, sinon l'ancienne configuration revient au redémarrage.

```
switch: flash_init
switch: dir flash:
switch: del flash:config.text
switch: del flash:config.text.renamed
switch: del flash:vlan.dat
switch: del flash:vlan.dat.renamed
switch: boot
```

```
Initializing Flash...
flashfs[0]: 545 files, 19 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 32514048
flashfs[0]: Bytes used: 13543936
flashfs[0]: Bytes available: 18970112
flashfs[0]: flashfs fsck took 11 seconds.
...done Initializing Flash.

switch: dir flash:
Directory of flash:/

    2  -rwx  616       <date>              vlan.dat
    3  -rwx  1156      <date>              vlan.dat.renamed
    4  -rwx  7210      <date>              config.text.renamed
    5  -rwx  9017      <date>              private-config.text.renamed
    6  drwx  192       <date>              c2960-lanbasek9-mz.122-55.SE7
  562  -rwx  2723      <date>              config.text
  563  -rwx  4120      <date>              multiple-fs
  565  -rwx  5486      <date>              private-config.text

18970112 bytes available (13543936 bytes used)
```

*Captures : initialisation du flash et liste des fichiers.*

```
switch: del flash:vlan.dat.renamed
Are you sure you want to delete "flash:vlan.dat.renamed" (y/n)?y
File "flash:vlan.dat.renamed" deleted

switch: del flash:config.text.renamed
Unknown cmd: del

switc
Unknown cmd:

switch: del flash:config.text.renamed
Are you sure you want to delete "flash:config.text.renamed" (y/n)?y
File "flash:config.text.renamed" deleted
```

*Captures : suppression des fichiers .renamed.*

```
switch: del flash:config.text
Are you sure you want to delete "flasjg.t:config.text" (y/n)?y
File "flasjg.t:config.text" not deleted -- no such device

switch: del flash:config.text
Are you sure you want to delete "flash:config.text" (y/n)?y
File "flash:config.text" deleted

switch: del flash:vlan.dat
Unknown cmd: del

switch: del flash:vlan.dat
Are you sure you want to delete "flash:vlan.dat" (y/n)?y
File "flash:vlan.dat" deleted
```

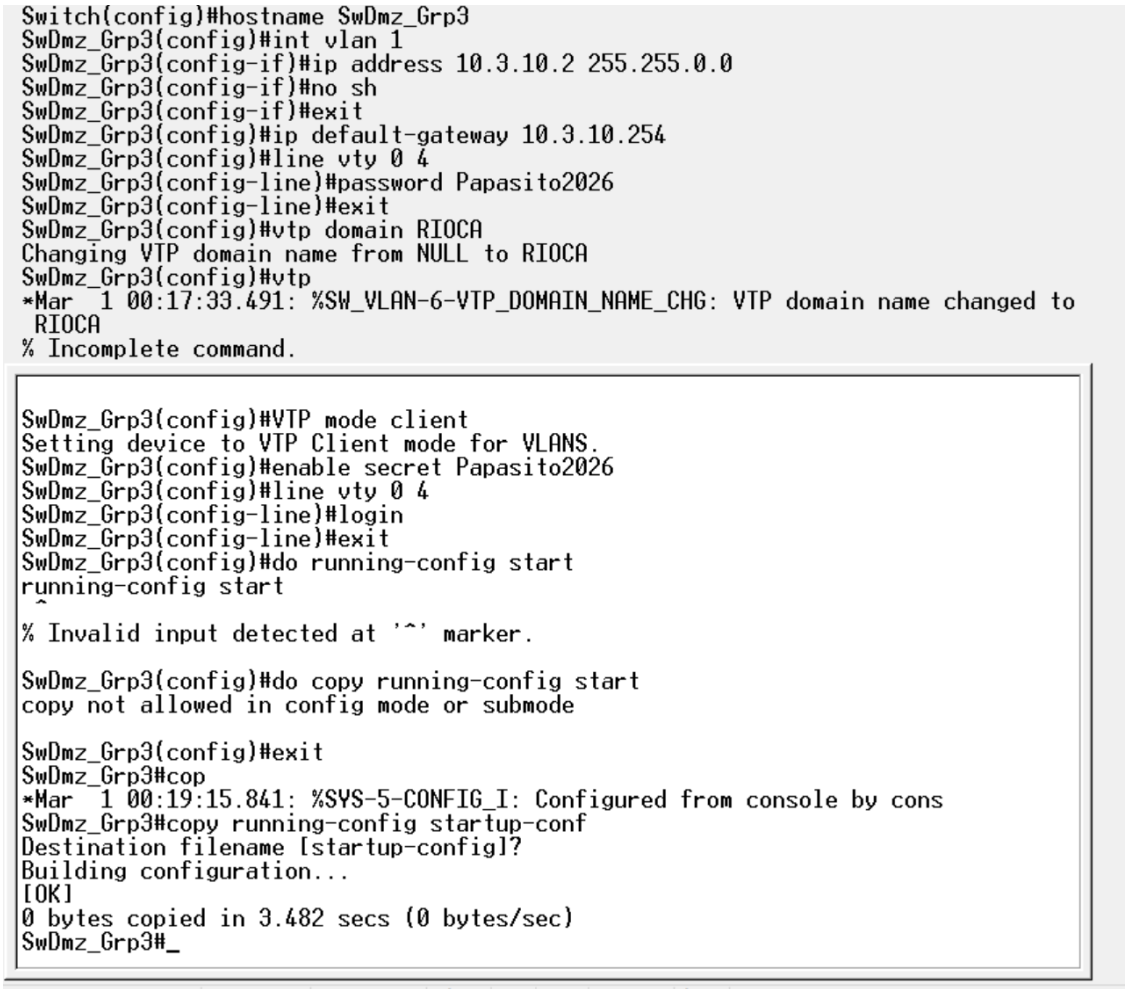
*Captures : suppression de config.text et de vlan.dat.*

## Configuration de base

```
hostname SwDmz_Grp3
enable secret Papasito2026
!
interface vlan 1
 ip address 10.3.10.2 255.255.0.0
 no shutdown
!
ip default-gateway 10.3.10.254
!
vtp domain RIOCA
vtp mode client
!
line vty 0 4
 password Papasito2026
 login
```

- `enable secret` protège le mode privilégié ; le mot de passe est stocké chiffré.
- `interface vlan 1` donne au switch son IP de management ; la passerelle est l'interface DMZ du pare-feu (10.3.10.254).
- `vtp mode client` : le switch reçoit les VLAN du domaine RIOCA sans pouvoir les modifier.
- `line vty 0 4` ouvre l'accès distant avec mot de passe, en Telnet dans un premier temps, puis en SSH (section 7).

La configuration est enregistrée avec `copy running-config startup-config`.




*Capture : configuration de base saisie sur SwDmz_Grp3.*

# 3. Switch Internet (SwNET_Grp3)

SwNET_Grp3 relie le pare-feu aux routeurs Internet ; il porte une IP de management dans le réseau 192.168.3.248/29 et n'accepte que SSH sur ses lignes VTY.

## Remise à zéro

Le mode privilégié de l'ancienne configuration n'était pas protégé : elle a été effacée directement depuis l'IOS, sans passer par le bootloader.

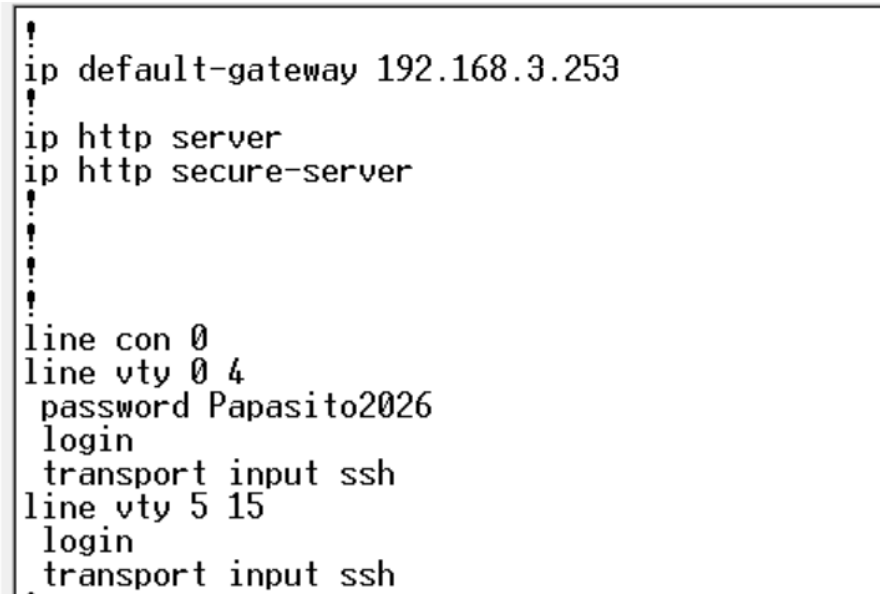
## Configuration de base

```
hostname SwNET_Grp3
enable secret Papasito2026
!
interface Vlan1
 ip address 192.168.3.254 255.255.255.248
!
ip default-gateway 192.168.3.253
!
line vty 0 4
 password Papasito2026
 login
 transport input ssh
line vty 5 15
 login
 transport input ssh
```

- `interface Vlan1` donne l'IP de management (192.168.3.254) ; la passerelle est l'interface du pare-feu côté Internet (192.168.3.253).
- `transport input ssh` refuse Telnet sur les 16 lignes VTY (section 7).
- VTP est configuré comme sur SwDmz : domaine RIOCA, mode client.

```
hostname SwNET_Grp3
!
boot-start-marker
boot-end-marker
!
enable secret 9 $9$E8Alq6RmICiret$YS7FEFAORu5iC8nrrKUaQDTUs6x3xKigOATVwmbDRaU
```

*Capture : début du running-config de SwNET_Grp3 (hostname et enable secret chiffré).*




*Capture : passerelle par défaut et lignes VTY de SwNET_Grp3 (SSH uniquement).*

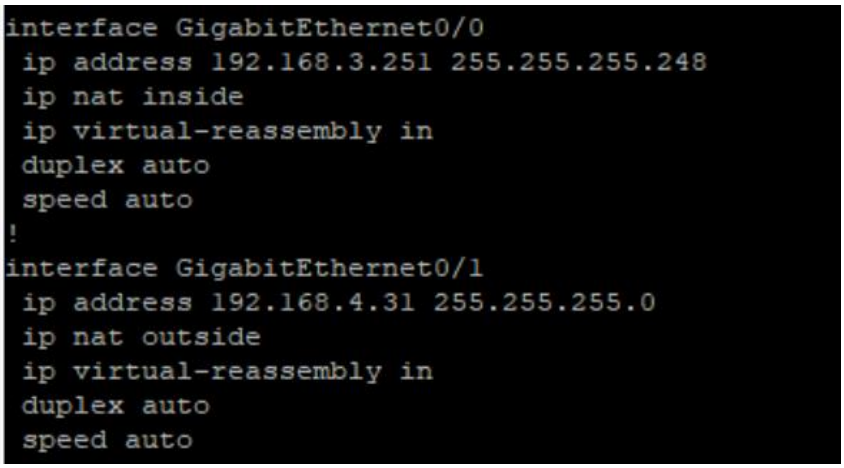
# 4. Routeur Internet (RNET_GRP3)

RNET_GRP3 relie la zone Internet de la maquette au réseau du campus et traduit les adresses du LAN et des serveurs web de la DMZ en NAT overload, car le routeur du labo (192.168.4.254) n'est pas administrable.

## Interfaces

```
interface GigabitEthernet0/0
 ip address 192.168.3.251 255.255.255.248
 ip nat inside
!
interface GigabitEthernet0/1
 ip address 192.168.4.31 255.255.255.0
 ip nat outside
```

- Gi0/0 est le côté maquette (SwNET, pare-feu) : `ip nat inside`.
- Gi0/1 est le côté campus : `ip nat outside`.
- `show ip interface brief` affiche les deux interfaces en up/up.

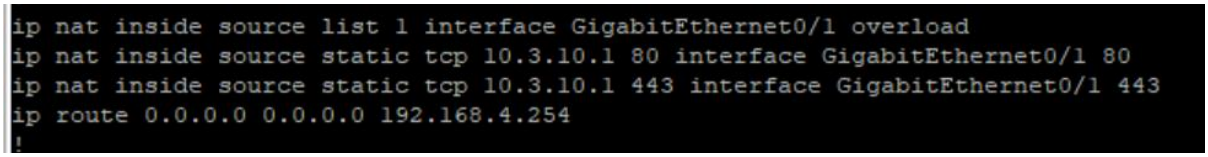



*Capture : interfaces de RNET_GRP3 dans le running-config.*

## NAT overload (PAT) et publication des serveurs web

```
access-list 1 permit 172.19.0.0 0.0.255.255
access-list 1 permit host 10.3.10.1
access-list 1 permit host 10.3.10.2
ip nat inside source list 1 interface GigabitEthernet0/1 overload
ip nat inside source static tcp 10.3.10.1 80 interface GigabitEthernet0/1 80
ip nat inside source static tcp 10.3.10.1 443 interface GigabitEthernet0/1 443
ip route 0.0.0.0 0.0.0.0 192.168.4.254
```

- L'ACL 1 désigne les adresses autorisées à être traduites : le LAN 172.19.0.0/16 et les deux serveurs web de la DMZ.
- `overload` fait sortir toutes ces adresses derrière l'IP de Gi0/1 (192.168.4.31), en différenciant les connexions par leur port.
- Les deux règles `static tcp` publient le serveur web 10.3.10.1 (WebPrimaire) sur l'IP de Gi0/1, ports 80 et 443 : il est ainsi joignable depuis le campus.
- La route par défaut envoie le trafic vers le routeur du labo.




*Capture : NAT overload, publication des ports 80 et 443 et route par défaut dans le running-config.*

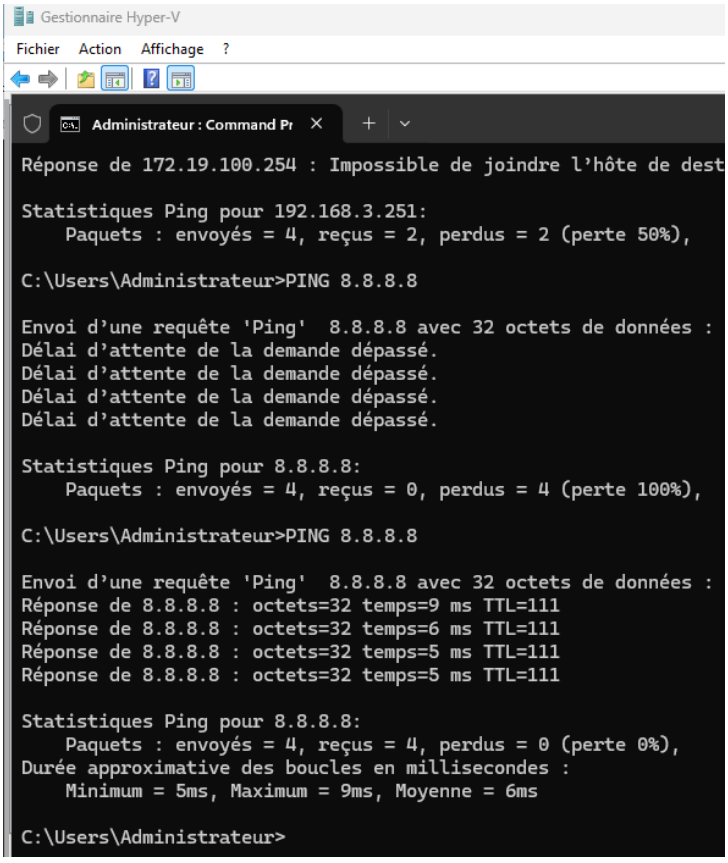
```
RNET_GRP3(config-std-nacl)#do show access-list 1
Standard IP access list 1
    30 permit 10.3.10.2
    20 permit 10.3.10.1
    10 permit 172.19.0.0, wildcard bits 0.0.255.255 (4231 matches)
```

*Capture : `show access-list 1`, avec les deux serveurs web de la DMZ (10.3.10.1 et 10.3.10.2) et le LAN (4231 correspondances).*

Test réalisé : ping vers 8.8.8.8 depuis un serveur du LAN.

```
RNET_GRP3(config)#ip nat inside source list 1  interface gi0/1 overload
RNET_GRP3(config)#do ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
RNET_GRP3(config)#
```

*Capture : ping vers 8.8.8.8 depuis RNET.*




*Capture : ping vers 8.8.8.8 depuis un serveur du LAN (en échec avant le NAT, réussi après).*

# 5. Pare-feu RParefeu : configuration de base

RParefeu est un Zyxel USG Flex 500 configuré depuis son interface web ; il porte une interface par zone et sert de point de contrôle unique entre le LAN, la DMZ et Internet.

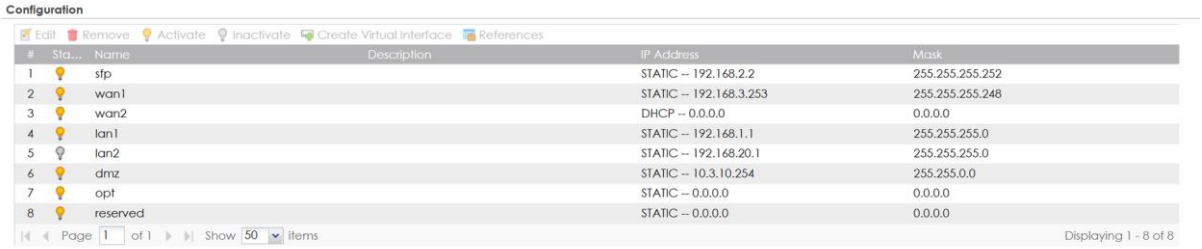
## Mise en service

1. Se connecter à l'interface web sur l'adresse par défaut 192.168.1.1.
2. Suivre l'assistant d'installation.
3. Changer le mot de passe du compte `admin`.
4. Donner une adresse IP à chaque interface.
5. Associer chaque interface à sa zone.

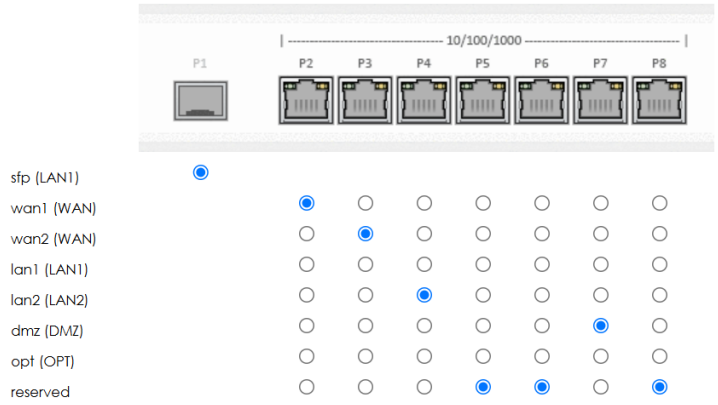
### Interfaces et zones

| Interface | Zone | Adresse | Port | Reliée à |
|---|---|---|---|---|
| sfp | LAN1 | 192.168.2.2/30 | P1 | SwCoeur |
| dmz | DMZ | 10.3.10.254/16 | P7 | SwDmz |
| wan1 | WAN | 192.168.3.253/29 | P2 | SwNET |

Les autres interfaces ne servent pas au flux de production : `wan2` (P3) reste en DHCP, `lan2` (P4, 192.168.20.1/24) est l'interface de secours, et les ports P5, P6 et P8 sont en zone `reserved`. Le pare-feu désigne par ZyWALL les flux qui lui sont destinés (administration, RIP). Les règles de filtrage entre zones sont décrites en section 9.




*Capture : interfaces du Zyxel (Configuration > Network > Interface), avec leurs IP et masques.*




*Capture : affectation des ports physiques (P1 à P8) aux interfaces et aux zones.*

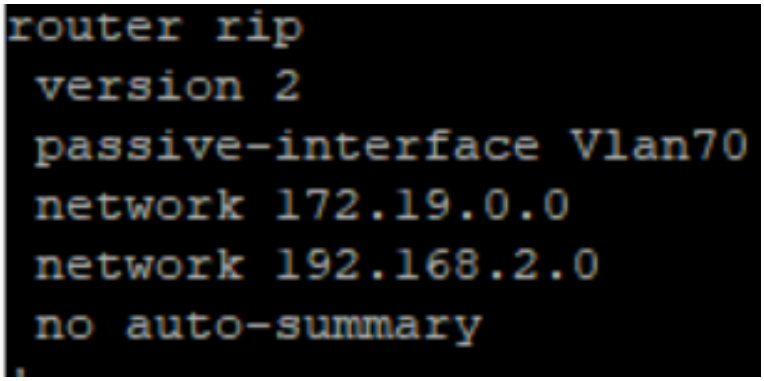
## 6. Routage RIP v2

RIP v2 est activé sur SwCoeur, RParefeu et RNET_GRP3 : chaque équipement apprend automatiquement les réseaux du LAN, de la DMZ et de la zone Internet, et RNET diffuse sa route par défaut vers Internet.

### SwCoeur (SW_COEUR_GRP3)

```
ip routing
!
router rip
 version 2
 passive-interface Vlan70
 network 172.19.0.0
 network 192.168.2.0
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 192.168.2.2
```

- `ip routing` active le routage sur le switch de niveau 3.
- `network 172.19.0.0` annonce les VLAN du LAN ; `network 192.168.2.0` active RIP sur le lien vers le pare-feu.
- `passive-interface Vlan70` n'envoie pas d'annonces RIP dans le VLAN d'administration.
- `no auto-summary` conserve les masques réels au lieu de résumer par classe.
- La route par défaut de SwCoeur est une route statique vers l'interface sfp du pare-feu (192.168.2.2) : elle apparaît avec le code `S*` dans `show ip route`.

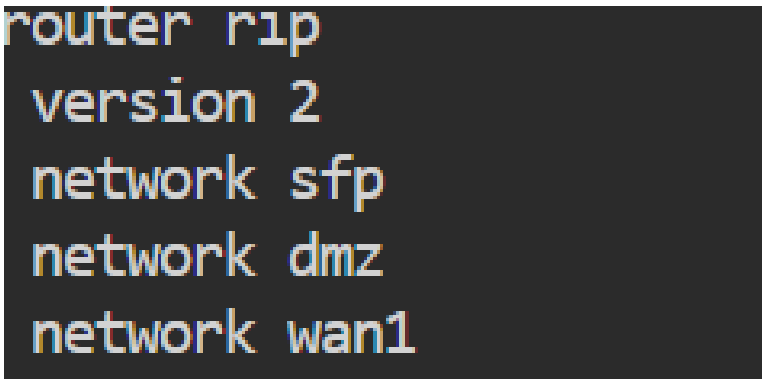



*Capture : configuration RIP de SwCoeur.*

## RParefeu

```
router rip
 version 2
 network sfp
 network dmz
 network wan1
```

Sur le Zyxel, RIP se déclare par nom d'interface : `sfp` (vers SwCoeur), `dmz` et `wan1` (vers SwNET). La règle de pare-feu `Allow_RIPv2` autorise ces échanges (section 9).

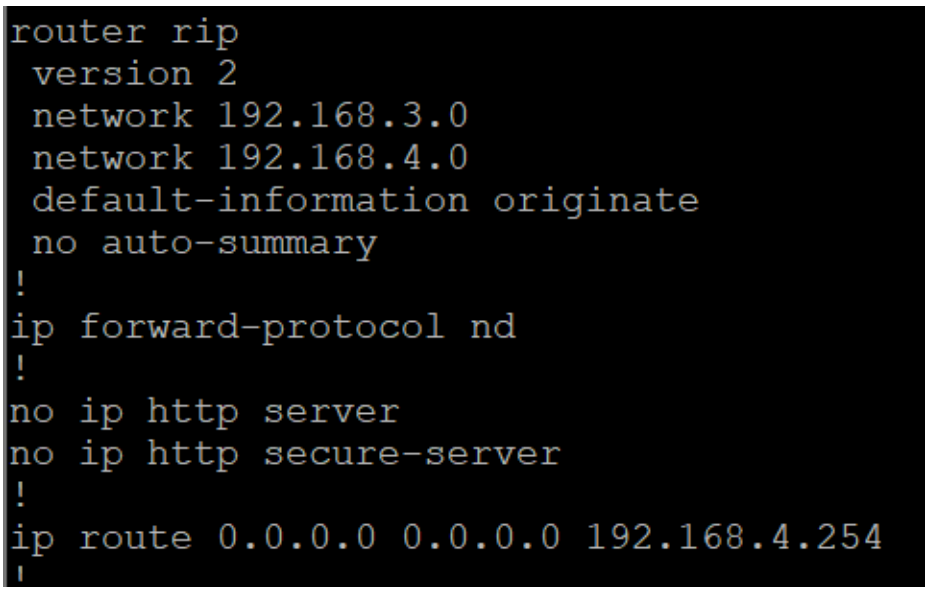



*Capture : configuration RIP du Zyxel.*

## RNET_GRP3

```
router rip
 version 2
 network 192.168.3.0
 network 192.168.4.0
 default-information originate
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 192.168.4.254
```

`default-information originate` diffuse en RIP la route par défaut de RNET vers le reste de la maquette.




*Capture : configuration RIP de RNET_GRP3.*

## Problèmes rencontrés

| Problème | Cause | Correction |
|---|---|---|
| Lien SwCoeur – pare-feu | L'interface du pare-feu avait la même IP que celle de SwCoeur | Une IP distincte par interface sur le lien |
| Lien pare-feu – RNET | Les interfaces du lien étaient dans des VLAN différents | Même VLAN des deux côtés du lien |

## Vérification

- `show ip route` sur chaque équipement Cisco : les routes apprises portent la lettre `R`.
- Ping depuis un serveur du LAN vers l'interface campus de RNET (192.168.4.31).

Sur RNET, les neuf sous-réseaux du LAN (172.19.x.0/24), le réseau de la DMZ (10.3.0.0/16) et le lien SwCoeur – pare-feu (192.168.2.0/30) sont appris en RIP via le pare-feu (192.168.3.253).

```
RNET_GRP3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.4.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.4.254
      10.0.0.0/16 is subnetted, 1 subnets
R        10.3.0.0 [120/1] via 192.168.3.253, 00:00:22, GigabitEthernet0/0
      172.19.0.0/24 is subnetted, 9 subnets
R        172.19.10.0 [120/2] via 192.168.3.253, 00:00:22, GigabitEthernet0/0
R        172.19.20.0 [120/2] via 192.168.3.253, 00:00:22, GigabitEthernet0/0
R        172.19.30.0 [120/2] via 192.168.3.253, 00:00:22, GigabitEthernet0/0
R        172.19.40.0 [120/2] via 192.168.3.253, 00:00:22, GigabitEthernet0/0
R        172.19.50.0 [120/2] via 192.168.3.253, 00:00:22, GigabitEthernet0/0
R        172.19.60.0 [120/2] via 192.168.3.253, 00:00:22, GigabitEthernet0/0
R        172.19.70.0 [120/2] via 192.168.3.253, 00:00:22, GigabitEthernet0/0
R        172.19.80.0 [120/2] via 192.168.3.253, 00:00:22, GigabitEthernet0/0
R        172.19.100.0 [120/2] via 192.168.3.253, 00:00:22, GigabitEthernet0/0
      192.168.2.0/30 is subnetted, 1 subnets
R        192.168.2.0 [120/1] via 192.168.3.253, 00:00:22, GigabitEthernet0/0
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.248/29 is directly connected, GigabitEthernet0/0
L        192.168.3.251/32 is directly connected, GigabitEthernet0/0
      192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.4.0/24 is directly connected, GigabitEthernet0/1
L        192.168.4.31/32 is directly connected, GigabitEthernet0/1
```

*Capture : `show ip route` sur RNET_GRP3.*

Sur SwCoeur, la DMZ (10.3.0.0/16), le réseau Internet (192.168.3.248/29) et le campus (192.168.4.0/24) sont appris en RIP via le pare-feu (192.168.2.2, interface Vlan90).

```
SW_COEUR_GRP3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 192.168.2.2 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.2.2
      10.0.0.0/16 is subnetted, 1 subnets
R        10.3.0.0 [120/1] via 192.168.2.2, 00:00:20, Vlan90
      172.19.0.0/16 is variably subnetted, 18 subnets, 2 masks
C        172.19.10.0/24 is directly connected, Vlan10
L        172.19.10.254/32 is directly connected, Vlan10
C        172.19.20.0/24 is directly connected, Vlan20
L        172.19.20.254/32 is directly connected, Vlan20
C        172.19.30.0/24 is directly connected, Vlan30
L        172.19.30.254/32 is directly connected, Vlan30
C        172.19.40.0/24 is directly connected, Vlan40
L        172.19.40.254/32 is directly connected, Vlan40
C        172.19.50.0/24 is directly connected, Vlan50
L        172.19.50.254/32 is directly connected, Vlan50
C        172.19.60.0/24 is directly connected, Vlan60
L        172.19.60.254/32 is directly connected, Vlan60
C        172.19.70.0/24 is directly connected, Vlan70
L        172.19.70.1/32 is directly connected, Vlan70
C        172.19.80.0/24 is directly connected, Vlan80
L        172.19.80.254/32 is directly connected, Vlan80
C        172.19.100.0/24 is directly connected, Vlan100
L        172.19.100.254/32 is directly connected, Vlan100
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/30 is directly connected, Vlan90
L        192.168.2.1/32 is directly connected, Vlan90
      192.168.3.0/29 is subnetted, 1 subnets
R        192.168.3.248 [120/1] via 192.168.2.2, 00:00:20, Vlan90
R     192.168.4.0/24 [120/2] via 192.168.2.2, 00:00:20, Vlan90
```

*Capture : `show ip route` sur SW_COEUR_GRP3.*

# 7. Administration distante sécurisée

L'administration à distance se fait en SSH, depuis le VLAN IT uniquement, sur les huit équipements : Sw2e, Sw1e, SwRDC, SwCoeur, SwDmz, SwNET, RNET et RParefeu. Une bannière d'avertissement s'affiche à la connexion.

## SSH sur les lignes VTY

```
line vty 0 4
 password Papasito2026
 login
 transport input ssh
line vty 5 15
 login
 transport input ssh
```

`transport input ssh` refuse Telnet : seules les connexions SSH sont acceptées (extrait de SwNET_Grp3, section 3). La connexion se fait avec le compte `admin-it`.

## VLAN d'administration externe

```
vlan 71
 name VLAN_ADMIN_EXT
!
interface vlan 71
 ip address 192.168.2.9 255.255.255.248
 no shutdown
```

## Contrôle d'accès

| Où | Restriction |
|---|---|
| SwCoeur, ACL ACL_INTER_VLAN | SSH (port 22) autorisé uniquement depuis le VLAN IT 172.19.60.0/24 vers le reste du LAN (section 10) |
| SwCoeur, ACL ACL_ADMIN_IT | ACL standard qui n'autorise que le VLAN IT (172.19.60.0/24) et le VLAN d'administration externe (192.168.2.8/29), et refuse et journalise le reste (section 10) |
| RParefeu, règle Admin_IT_Local | Le VLAN IT administre SwDmz, SwNET et RNET en SSH, HTTP et HTTPS |
| RParefeu, règle Admin_IT_Distant | Le VLAN IT administre le pare-feu lui-même |
| RParefeu, règle Admin_IT_Externe | Le service IT administre le pare-feu depuis l'extérieur, uniquement depuis l'adresse IT_EXTERNE |

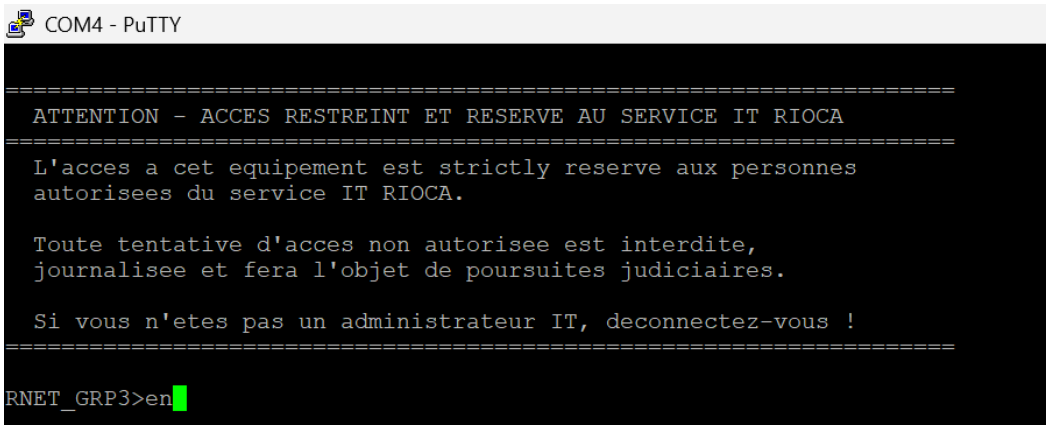
## Bannière d'avertissement

```
================================================================
  ATTENTION - ACCES RESTREINT ET RESERVE AU SERVICE IT RIOCA
================================================================
  L'acces a cet equipement est strictly reserve aux personnes
  autorisees du service IT RIOCA.

  Toute tentative d'acces non autorisee est interdite,
  journalisee et fera l'objet de poursuites judiciaires.

  Si vous n'etes pas un administrateur IT, deconnectez-vous !
================================================================
```

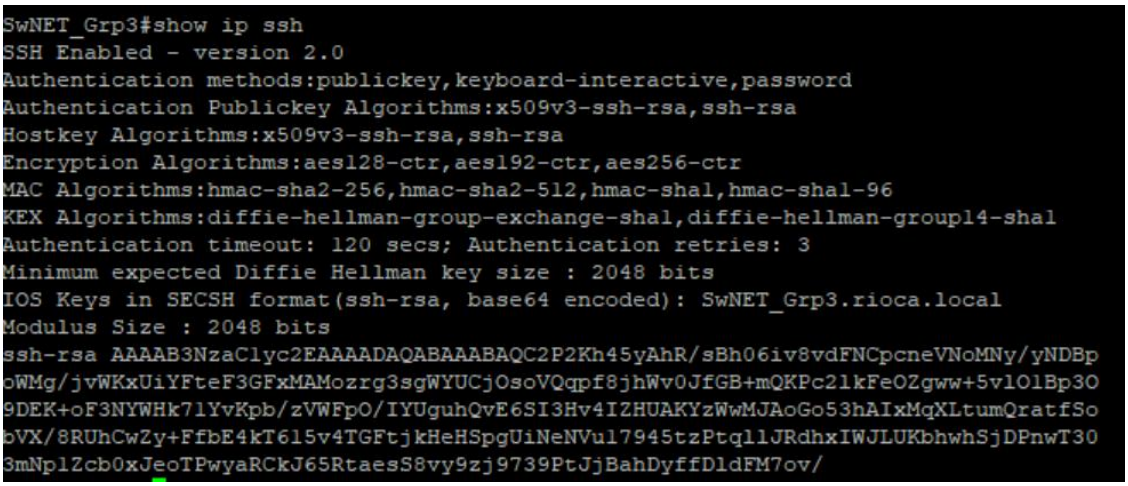
La bannière est en place sur Sw2e, Sw1e, SwRDC, SwCoeur, SwDmz, SwNET et RNET.




*Capture : bannière affichée à la connexion sur RNET_GRP3.*

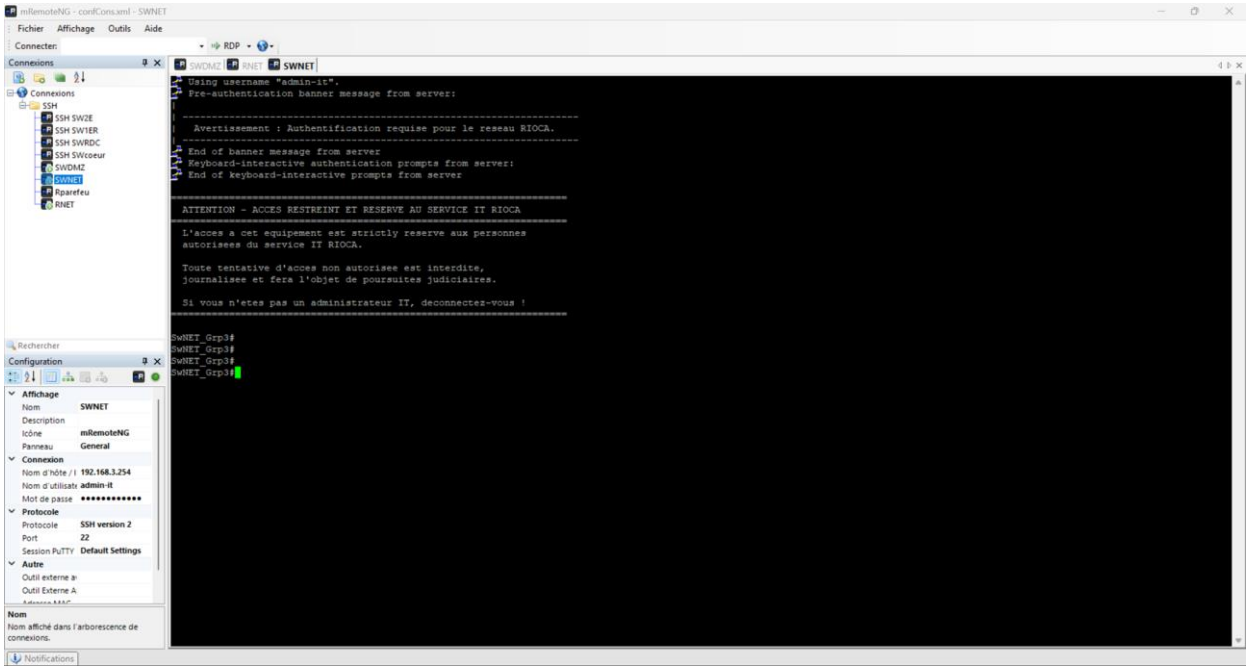
## Vérification

`show ip ssh` sur SwNET confirme que SSH version 2 est actif, avec une clé RSA de 2048 bits (domaine `rioca.local`), un chiffrement AES en mode CTR, un délai d'authentification de 120 secondes et 3 tentatives maximum.




*Capture : `show ip ssh` sur SwNET_Grp3.*

Les huit équipements sont déclarés dans mRemoteNG (SSH version 2, port 22). La capture montre la connexion à SwNET (192.168.3.254) avec le compte `admin-it` : la bannière s'affiche avant l'authentification, puis l'invite du switch.




*Capture : session SSH vers SwNET dans mRemoteNG, avec la liste des équipements administrés.*

# 8. Sauvegarde automatique des configurations

Les configurations sont envoyées automatiquement vers un serveur TFTP Ubuntu (172.19.100.5) : les équipements Cisco poussent leur configuration avec une tâche planifiée `kron` (des applets EEM sur SwNET, Sw1e et Sw2e), et le serveur récupère celle du Zyxel par un script planifié avec `cron`.

| Équipement | Méthode | Créneaux |
|---|---|---|
| Équipements Cisco (sauf SwNET, Sw1e et Sw2e) | kron, sur chaque équipement | Mardi et jeudi 17h30, vendredi 11h30 |
| SwNET, Sw1e et Sw2e | Applets EEM | Mardi et jeudi 17h30, vendredi 11h30 |
| RParefeu (Zyxel) | Script FTP + cron sur le serveur | Mardi, jeudi et vendredi 17h30 (crontab du serveur) |

## Serveur TFTP

Le serveur est une machine virtuelle Ubuntu (`srv-ubuntu-sauvegarde`) hébergée sur l'Hyper-V du groupe, dans le VLAN 100.

| Paramètre | Valeur |
|---|---|
| Adresse IP | 172.19.100.5 |
| Passerelle | 172.19.100.254 |
| Dossier des sauvegardes | /srv/tftp |

```
sudo apt update && sudo apt install tftpd-hpa
```

Fichier `/etc/default/tftpd-hpa` :

```
TFTP_USERNAME="TFTP"
TFTP_DIRECTORY="/srv/tftp"
TFTP_ADDRESS=":69"
TFTP_OPTIONS="--secure --create"
```

- `--secure` enferme le service dans `/srv/tftp`.
- `--create` autorise le dépôt de nouveaux fichiers, nécessaire pour recevoir les sauvegardes.

## Équipements Cisco : tâches kron

Chaque équipement Cisco exécute lui-même sa sauvegarde. Exemple sur SwDmz :

```
kron policy-list SAUVEGARDE_TFTP
 cli copy running-config tftp://172.19.100.5/SwDmz-confg
!
kron occurrence DEBUT_MAR at 17:30 Tue recurring
 policy-list SAUVEGARDE_TFTP
!
kron occurrence DEBUT_JEU at 17:30 Thu recurring
 policy-list SAUVEGARDE_TFTP
!
kron occurrence DEBUT_VEN at 11:30 Fri recurring
 policy-list SAUVEGARDE_TFTP
```

- `kron policy-list` contient la commande exécutée : la copie de la configuration courante vers le serveur TFTP. Le nom du fichier change d'un équipement à l'autre.
- Chaque `kron occurrence ... recurring` déclenche la liste chaque semaine : mardi et jeudi à 17h30, vendredi à 11h30.
- La même configuration est reprise sur les autres équipements Cisco équipés de kron, en changeant seulement le nom du fichier.

Ces créneaux correspondent aux fins de séances d'AP et ont été validés avec la professeure.




*Capture : configuration kron sur un équipement Cisco (SwDmz).*

## SwNET, Sw1e et Sw2e : applets EEM

Sur SwNET, Sw1e et Sw2e, la sauvegarde passe par deux applets EEM, aux mêmes créneaux que kron. Exemple sur SwNET (seul le nom du fichier change d'un équipement à l'autre) :

```
event manager applet BACKUP-MAR-JEU
 event timer cron cron-entry "30 17 * * 2,4"
 action 1.0 cli command "enable"
 action 1.1 cli command "configure terminal"
 action 1.2 cli command "file prompt quiet"
 action 1.3 cli command "end"
 action 2.0 cli command "copy running-config tftp://172.19.100.5/SwNet-confg"
event manager applet BACKUP-VEN
 event timer cron cron-entry "30 11 * * 5"
 action 1.0 cli command "enable"
 action 1.1 cli command "configure terminal"
 action 1.2 cli command "file prompt quiet"
 action 1.3 cli command "end"
 action 2.0 cli command "copy running-config tftp://172.19.100.5/SwNet-confg"
```

- `BACKUP-MAR-JEU` se déclenche le mardi et le jeudi à 17h30 (`cron-entry "30 17 * * 2,4"`), `BACKUP-VEN` le vendredi à 11h30.
- `file prompt quiet` supprime les questions de confirmation de la commande `copy`.
- La dernière action copie la configuration courante vers le serveur TFTP.




*Capture : applets EEM de sauvegarde sur SwNET_Grp3.*

## Pare-feu Zyxel : script et cron sur le serveur

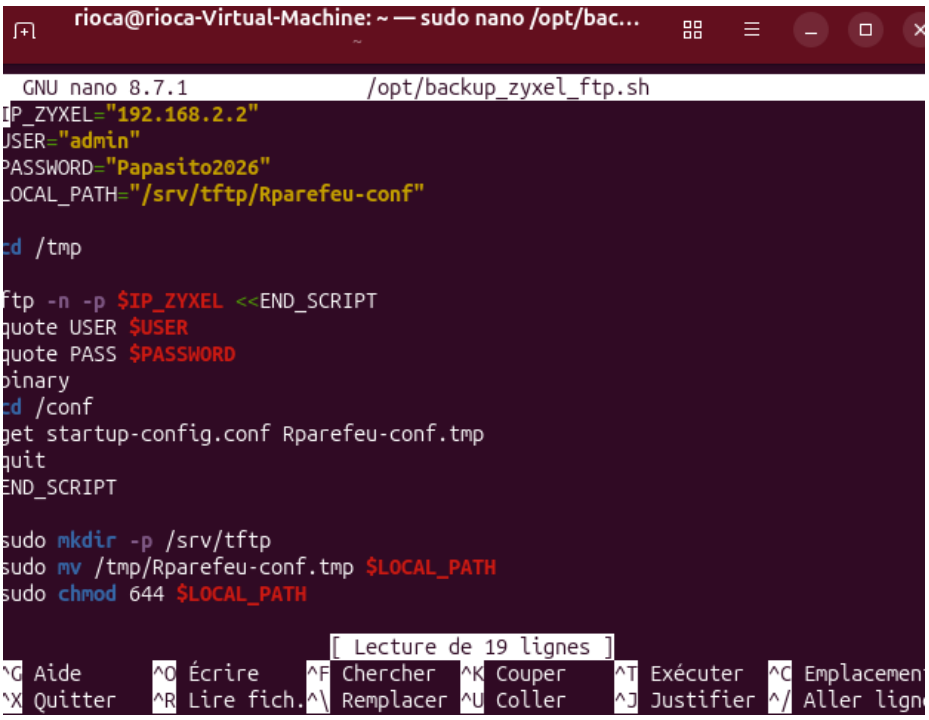
Le Zyxel ne permet pas de tâche planifiée de ce type. Le serveur va chercher lui-même son fichier `startup-config.conf` en FTP avec le script `/opt/backup_zyxel_ftp.sh` :

```
IP_ZYXEL="192.168.2.2"
USER="admin"
PASSWORD="Papasito2026"
LOCAL_PATH="/srv/tftp/Rparefeu-conf"

cd /tmp

ftp -n -p $IP_ZYXEL <<END_SCRIPT
quote USER $USER
quote PASS $PASSWORD
binary
cd /conf
get startup-config.conf Rparefeu-conf.tmp
quit
END_SCRIPT

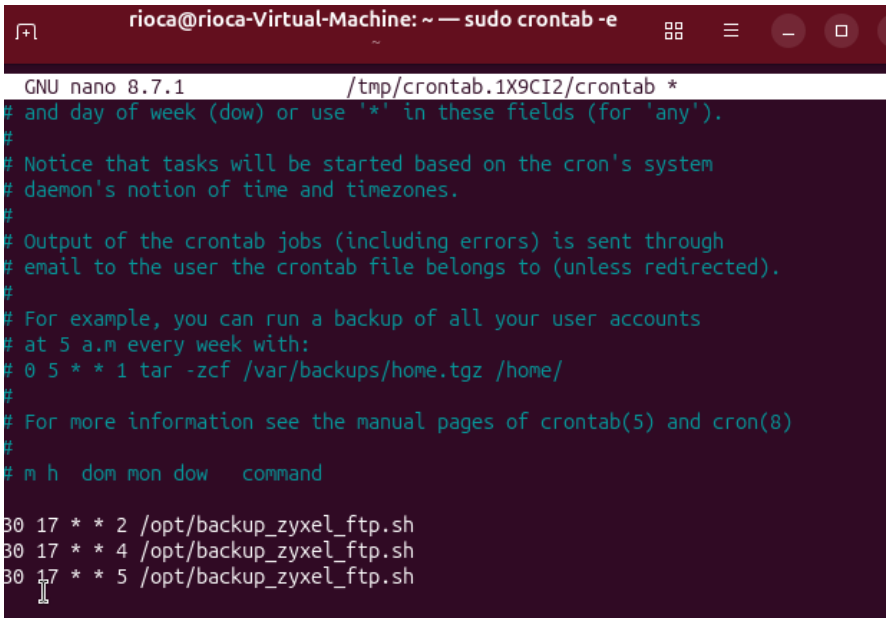
sudo mkdir -p /srv/tftp
sudo mv /tmp/Rparefeu-conf.tmp $LOCAL_PATH
sudo chmod 644 $LOCAL_PATH
```




*Capture : script /opt/backup_zyxel_ftp.sh sur le serveur.*

Planification dans la crontab de root (`sudo crontab -e`) :

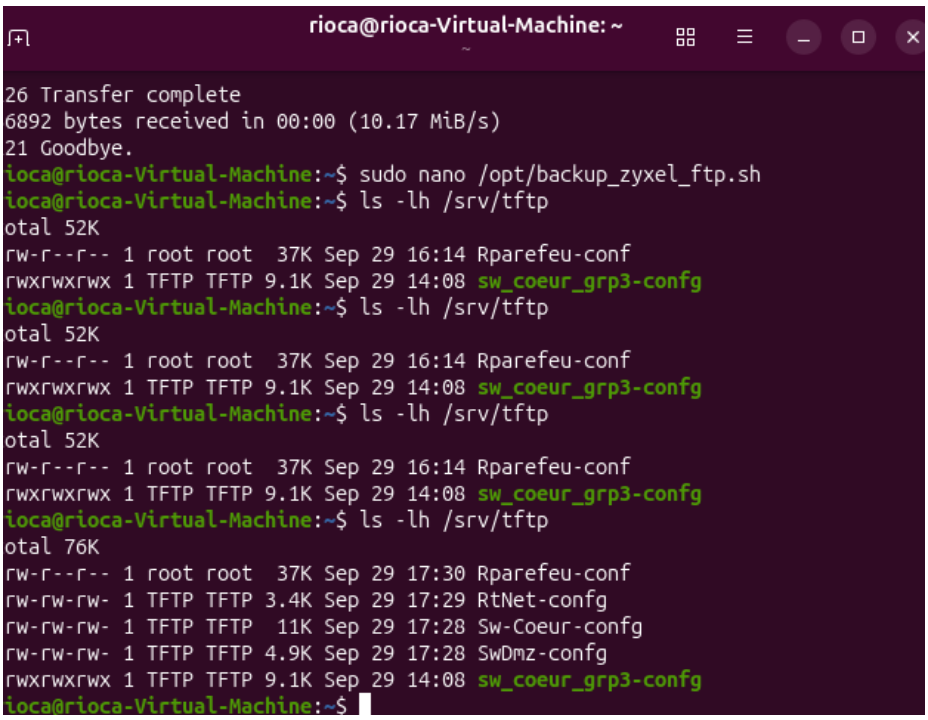
```
30 17 * * 2 /opt/backup_zyxel_ftp.sh
30 17 * * 4 /opt/backup_zyxel_ftp.sh
30 17 * * 5 /opt/backup_zyxel_ftp.sh
```




*Capture : crontab de root sur le serveur.*

## Vérification

- `ls -lh /srv/tftp` sur le serveur liste les fichiers reçus : la configuration du Zyxel (`Rparefeu-conf`) et celles des équipements Cisco.
- Depuis un poste du VLAN IT : `tftp -i 172.19.100.5 put test.txt` renvoie « Transfert réussi ».



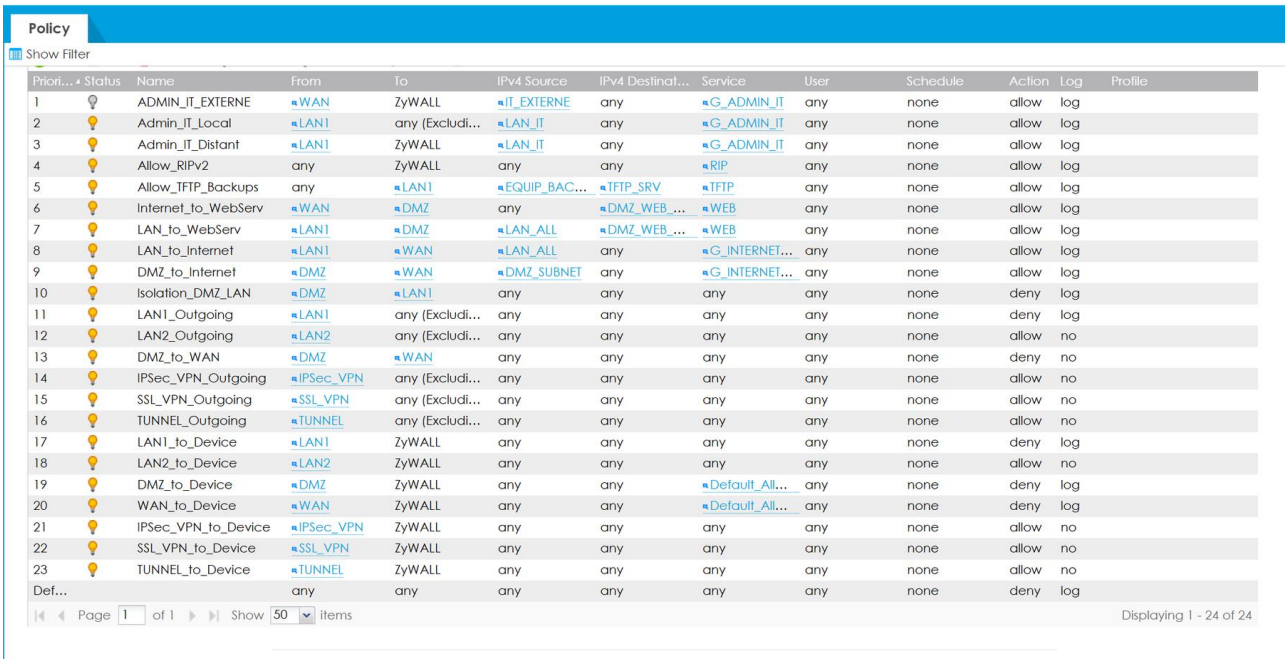

*Capture : contenu de /srv/tftp après exécution des sauvegardes automatiques.*

```
C:\Users\maxim>tftp -i 172.19.100.5 put "C:\Users\maxim\Downloads\test.txt"
Transfert réussi : 0 octets en 1 seconde(s), 0 octets/s
```

*Capture : envoi d'un fichier en TFTP depuis un poste du VLAN IT.*

## 9. Règles de pare-feu implémentées

Onze règles sont en place dans Configuration > Security Policy > Policy Control : elles ouvrent les seuls flux nécessaires, isolent la DMZ du LAN et refusent le reste des flux sortants du LAN. Le pare-feu applique la première règle qui correspond, dans l'ordre du tableau.


Policy

Show Filter

| Priori... | Status | Name | From | To | IPv4 Source | IPv4 Destinat... | Service | User | Schedule | Action | Log | Profile |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | ADMIN_IT_EXTERNE | WAN | ZyWALL | IT_EXTERNE | any | G_ADMIN_IT | any | none | allow | log | |
| 2 | | Admin_IT_Local | LAN1 | any (Excludi... | LAN_IT | any | G_ADMIN_IT | any | none | allow | log | |
| 3 | | Admin_IT_Distant | LAN1 | ZyWALL | LAN_IT | any | G_ADMIN_IT | any | none | allow | log | |
| 4 | | Allow_RIPv2 | any | ZyWALL | any | any | RIP | any | none | allow | log | |
| 5 | | Allow_TFTP_Backups | any | LAN1 | EQUIP_BAC... | TFTP_SRV | TFTP | any | none | allow | log | |
| 6 | | Internet_to_WebServ | WAN | DMZ | any | DMZ_WEB_... | WEB | any | none | allow | log | |
| 7 | | LAN_to_WebServ | LAN1 | DMZ | LAN_ALL | DMZ_WEB_... | WEB | any | none | allow | log | |
| 8 | | LAN_to_Internet | LAN1 | WAN | LAN_ALL | any | G_INTERNET... | any | none | allow | log | |
| 9 | | DMZ_to_Internet | DMZ | WAN | DMZ_SUBNET | any | G_INTERNET... | any | none | allow | log | |
| 10 | | Isolation_DMZ_LAN | DMZ | LAN1 | any | any | any | any | none | deny | log | |
| 11 | | LAN1_Outgoing | LAN1 | any (Excludi... | any | any | any | any | none | deny | log | |
| 12 | | LAN2_Outgoing | LAN2 | any (Excludi... | any | any | any | any | none | allow | no | |
| 13 | | DMZ_to_WAN | DMZ | WAN | any | any | any | any | none | deny | no | |
| 14 | | IPSec_VPN_Outgoing | IPSec_VPN | any (Excludi... | any | any | any | any | none | allow | no | |
| 15 | | SSL_VPN_Outgoing | SSL_VPN | any (Excludi... | any | any | any | any | none | allow | no | |
| 16 | | TUNNEL_Outgoing | TUNNEL | any (Excludi... | any | any | any | any | none | allow | no | |
| 17 | | LAN1_to_Device | LAN1 | ZyWALL | any | any | any | any | none | deny | log | |
| 18 | | LAN2_to_Device | LAN2 | ZyWALL | any | any | any | any | none | allow | no | |
| 19 | | DMZ_to_Device | DMZ | ZyWALL | any | any | Default_All... | any | none | deny | log | |
| 20 | | WAN_to_Device | WAN | ZyWALL | any | any | Default_All... | any | none | deny | log | |
| 21 | | IPSec_VPN_to_Device | IPSec_VPN | ZyWALL | any | any | any | any | none | allow | no | |
| 22 | | SSL_VPN_to_Device | SSL_VPN | ZyWALL | any | any | any | any | none | allow | no | |
| 23 | | TUNNEL_to_Device | TUNNEL | ZyWALL | any | any | any | any | none | allow | no | |
| Def... | | | any | any | any | any | any | any | none | deny | log | |

Page 1 of 1 Show 50 items Displaying 1 - 24 of 24

*Capture : liste complète des règles dans Policy Control.*

## Objets créés

| Objet | Type | Contenu |
|---|---|---|
| LAN_ALL | Adresse | 172.19.0.0/16 |
| LAN_IT | Adresse | 172.19.60.0/24 |
| DMZ_WEB_GRP | Groupe d'adresses | 10.3.10.1 et 10.3.10.2 |
| DMZ_SUBNET | Adresse | Réseau de la DMZ |
| TFTP_SRV | Adresse | 172.19.100.5 |
| G_ADMIN_IT | Groupe de services | SSH, HTTP, HTTPS |
| WEB | Groupe de services | HTTP, HTTPS |
| Groupe Internet | Groupe de services | HTTP, HTTPS, DNS, ICMP |
| Groupe mises à jour | Groupe de services | HTTP, HTTPS, DNS |
| EQUIP_BACKUP | Groupe d'adresses | IP de management de SwDmz, SwNET et RNET |
| IT_EXTERNE | Adresse | Adresse externe du service IT |

## Tableau des règles

| N° | Règle | De → vers | Source | Destination | Service | Action |
|---|---|---|---|---|---|---|
| 1 | Admin_IT_Externe | WAN → ZyWALL | IT_EXTERNE | Tous | G_ADMIN_IT | Autoriser |
| 2 | Admin_IT_Local | LAN1 → toutes zones sauf ZyWALL | LAN_IT | Tous | G_ADMIN_IT | Autoriser |
| 3 | Admin_IT_Distant | LAN1 → ZyWALL | LAN_IT | Pare-feu | G_ADMIN_IT | Autoriser |
| 4 | Allow_RIPv2 | Toutes zones → ZyWALL | Tous | Pare-feu | RIP (UDP 520) | Autoriser |
| 5 | Allow_TFTP_Backups | Toutes zones → LAN1 | EQUIP_BACKUP | TFTP_SRV | TFTP (UDP 69) | Autoriser |
| 6 | Internet_to_WebServ | WAN → DMZ | Tous | DMZ_WEB_GRP | WEB | Autoriser |
| 7 | LAN_to_WebServ | LAN1 → DMZ | LAN_ALL | DMZ_WEB_GRP | WEB | Autoriser |
| 8 | LAN_to_Internet | LAN1 → WAN | LAN_ALL | Tous | Groupe Internet | Autoriser |
| 9 | DMZ_to_Internet | DMZ → WAN | DMZ_SUBNET | Tous | Groupe mises à jour | Autoriser |
| 10 | Isolation_DMZ_LAN | DMZ → LAN1 | Tous | Tous | Tous | Refuser |
| 11 | LAN1_Outgoing | LAN1 → toutes zones sauf ZyWALL | Tous | Tous | Tous | Refuser |

- Les onze règles journalisent le trafic (log).
- `LAN1_Outgoing` est une règle par défaut du Zyxel, passée de allow à deny.
- Le filtrage est à état : les réponses aux connexions autorisées passent automatiquement.

La justification de chaque règle et le plan de tests sont dans le document `Regles_parefeu_flux_hors-LAN.docx`.

### Durcissement des règles par défaut

Les règles par défaut du Zyxel placées sous les règles du tableau sont passées en deny : tout flux qui n'est pas explicitement autorisé est refusé.

| Règle | De → vers | Action |
|---|---|---|
| DMZ_to_WAN | DMZ → WAN | Refuser |
| LAN1_to_Device | LAN1 → ZyWALL | Refuser |
| DMZ_to_Device | DMZ → ZyWALL | Refuser |
| WAN_to_Device | WAN → ZyWALL | Refuser |
| Default | Toutes zones → toutes zones | Refuser |

Les règles par défaut des zones non utilisées (`lan2`, IPSec_VPN, SSL_VPN, TUNNEL) restent en allow : aucun flux du projet ne passe par ces zones. La règle `Default` est passée en deny en dernier, après vérification de l'accès à l'interface web d'administration.

## 10. ACL du LAN sur SwCoeur

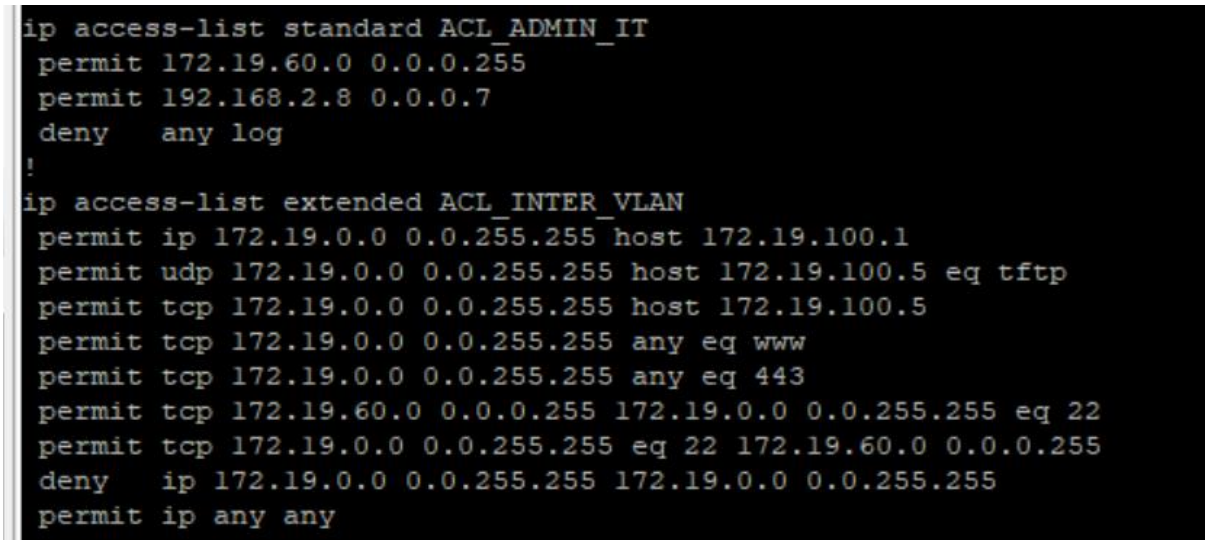
Deux ACL sont définies sur SwCoeur. `ACL_ADMIN_IT` est une ACL standard qui n'autorise que le VLAN IT (172.19.60.0/24) et le VLAN d'administration externe (192.168.2.8/29), et refuse et journalise le reste. `ACL_INTER_VLAN` est une ACL étendue unique, appliquée en entrée de chaque interface VLAN de service : elle autorise les flux communs (serveurs, web, SSH depuis l'IT), puis interdit toute communication entre services.

### Contenu de l'ACL

```
ip access-list standard ACL_ADMIN_IT
 permit 172.19.60.0 0.0.0.255
 permit 192.168.2.8 0.0.0.7
 deny any log
!
ip access-list extended ACL_INTER_VLAN
 10 permit ip 172.19.0.0 0.0.255.255 host 172.19.100.1
 20 permit udp 172.19.0.0 0.0.255.255 host 172.19.100.5 eq tftp
 30 permit tcp 172.19.0.0 0.0.255.255 host 172.19.100.5
 40 permit tcp 172.19.0.0 0.0.255.255 any eq www
 50 permit tcp 172.19.0.0 0.0.255.255 any eq 443
 60 permit tcp 172.19.60.0 0.0.0.255 172.19.0.0 0.0.255.255 eq 22
 70 permit tcp 172.19.0.0 0.0.255.255 eq 22 172.19.60.0 0.0.0.255
 73 permit udp host 172.19.100.5 172.19.0.0 0.0.255.255
 76 permit udp 172.19.60.0 0.0.0.255 host 172.19.100.5
 77 permit udp 172.19.70.0 0.0.0.255 host 172.19.100.5
 80 deny ip 172.19.0.0 0.0.255.255 172.19.0.0 0.0.255.255
 90 permit ip any any
```

| Lignes | Effet |
|---|---|
| 10 | Tout le LAN peut joindre le serveur 172.19.100.1 |
| 20, 30, 73, 76, 77 | Échanges avec le serveur de sauvegarde 172.19.100.5 (TFTP) |
| 40, 50 | HTTP et HTTPS autorisés vers toute destination |
| 60, 70 | SSH autorisé depuis le VLAN IT vers le LAN, et réponses vers le VLAN IT |
| 80 | Tout autre flux entre deux réseaux du LAN est refusé : les services ne communiquent pas entre eux |

| Lignes | Effet |
|---|---|
| 90 | Le reste (sorties vers la DMZ et Internet) passe et sera filtré par le pare-feu |




*Capture : ACL_ADMIN_IT et ACL_INTER_VLAN dans le running-config de SwCoeur.*

## Application sur les interfaces VLAN

```
interface Vlan10
 ip address 172.19.10.254 255.255.255.0
 ip access-group ACL_INTER_VLAN in
```

La même commande `ip access-group ACL_INTER_VLAN in` est présente sur les interfaces Vlan10, 20, 30, 40, 50, 60, 70 et 80. Chaque interface porte l'adresse 172.19.x.254, sauf Vlan70 (172.19.70.1).

## Vérification

`show access-lists` affiche pour chaque ligne le nombre de paquets correspondants : la ligne 80 compte les flux refusés entre services du LAN.