Construire un réseau informatique pour une petite structure

SAÉ 2.01

Auteur : Alexis TAHON

Formation : BUT Réseaux et Télécommunications

Date : 14 juin 2026

Table des matières

1 Introduction, Enjeux et Cahier des Charges

1.1 Contexte du Projet

Ce projet s'inscrit dans le cadre de la SAÉ 2.01 et consiste à concevoir, déployer et sécuriser l'infrastructure réseau ainsi que les services applicatifs de trois structures distinctes et interconnectées : une Très Petite Entreprise (TPE), une première PME (PME 1) et une seconde PME d'envergure supérieure (PME 2). L'ensemble de ces architectures transite par un cœur de réseau simulant un Fournisseur d'Accès Internet (FAI) interconnecté à sa propre zone de serveurs publics.

1.2 Objectifs de Sécurité et de Résilience

L'architecture a été pensée pour répondre à des critères industriels de disponibilité et de protection des données :

- **Dual-Stack (IPv4/IPv6) :** Déploiement simultané et transparent des deux protocoles de couche 3 sur l'ensemble des segments compatibles pour assurer la transition technologique.
- **Haute Disponibilité (PME 2) :** Utilisation de l'agrégation de liens physiques via le protocole LACP (EtherChannel) et sécurisation contre les boucles de commutation par le protocole Rapid-PVST+ afin d'éliminer tout point unique de défaillance (SPOF).
- **Approche Zero-Trust et Cloisonnement :** Séparation stricte des flux par l'usage de VLANs sectoriels, isolation des serveurs stratégiques dans des zones démilitarisées (DMZ), masquage de la topologie interne par translation d'adresses (NAT/PAT), et restriction absolue des accès d'administration.
- **Contrôle d'accès d'administration :** Seule la PME 2 expose des liaisons de gestion à distance via le protocole sécurisé SSHv2. Ces liaisons sont bridées électroniquement par des listes de contrôle d'accès (ACL) afin de n'autoriser qu'un unique terminal d'administration dédié.

2 Ingénierie de l'Adressage Logique (Dual-Stack)

Le tableau suivant répertorie l'intégralité des configurations logiques injectées sur les équipements de la maquette.

Table 1: Plan d'adressage global et affectation des interfaces

Équipement	Interface / VLAN	Rôle	IPv4 / Masque	IPv6 / Préfixe
R-INTERNET	Gi0/0.80	WAN Interco.	80.1.1.1 /24	2001:db8:ffff:12::1/64
	Gi0/0.200	Zone Serveurs FAI	200.1.1.254 /24	2001:db8:ffff:200::254/64
R-TPE	Gi0/0	LAN Interne TPE	192.168.1.254/24	–
	Gi0/1	Lien WAN (FAI)	80.1.1.2 /24	–
R-PME1	Gi0/1	Lien WAN (FAI)	80.1.1.3 /24	2001:db8:80::3/64
	Gi0/0.10	VLAN 10 (DMZ - Web)	192.168.10.254/24	2001:db8:1:10::254/64
	Gi0/0.20	VLAN 20 (LAN)	192.168.20.254/24	2001:db8:1:20::254/64
R-PME2	Gi0/1	Lien WAN (FAI)	80.1.1.4 /24	2001:db8:ffff:12::4/64
	Gi0/0.10	VLAN 10 (Bureau)	172.16.10.254/24	2001:db8:1:10::254/64
	Gi0/0.20	VLAN 20 (Prod)	172.16.20.254/24	2001:db8:1:20::254/64
	Gi0/0.30	VLAN 30 (Admin)	172.16.30.254/24	2001:db8:1:30::254/64
	Gi0/0.40	VLAN 40 (DMZ Publique)	198.51.100.30/27	2001:db8:1:40::254/64
SW-CORE	VLAN 30	SVI Gestion	172.16.30.250/24	–
SW-ACCES	VLAN 30	SVI Gestion	172.16.30.251/24	–

TABLE 1: Plan d'adressage global et affectation des interfaces

Équipement	**Interface / VLAN**	**Rôle**	**IPv4 / Masque**	**IPv6 / Préfixe**
PC-ADMIN	Port Fa0/4	Poste Admin	172.16.30.10/24	2001:db8:1:30::10/64

3 Guide d'Implémentation Théorique et Pratique de SSHv2

Pour valider les exigences de sécurité du cahier des charges, l'utilisation du protocole obsolète et non chiffré Telnet a été bannie au profit de **SSHv2** (Secure Shell Version 2). Contrairement à Telnet qui fait circuler les identifiants et les flux d'administration en texte clair sur le réseau, SSHv2 s'appuie sur des algorithmes de chiffrement asymétriques et symétriques pour garantir la confidentialité et l'intégrité des données d'administration.

L'implémentation sur l'IOS Cisco requiert obligatoirement le respect strict de 6 étapes configurées en mode de configuration globale :

Étape 1 : Modification du nom d'hôte (`hostname`)

```
Router(config)# hostname R-PME2
```

Analyse technique : Un équipement Cisco ne peut pas générer de clés cryptographiques s'il conserve son nom d'usine générique (`Router` ou `Switch`). La modification du nom d'hôte est le prérequis premier, car ce nom servira de composant initial pour définir l'identité de la clé de chiffrement.

Étape 2 : Définition du nom de domaine IP (`ip domain-name`)

```
R-PME2(config)# ip domain-name rt.sae201.fr
```

Analyse technique : SSH nécessite que l'appareil appartienne à un domaine logique. Le système d'exploitation Cisco IOS va combiner mathématiquement le `hostname` (R-PME2) et l' `ip domain-name` (rt.sae201.fr) afin de constituer le Nom de Domaine Pleinement Qualifié (FQDN) de l'équipement : `R-PME2.rt.sae201.fr`. C'est ce FQDN qui sera signé de manière unique par la clé de sécurité.

Étape 3 : Génération de la paire de clés de chiffrement RSA

```
R-PME2(config)# crypto key generate rsa
```

Lors de l'exécution dans le CLI de Packet Tracer, le système interrompt le script pour demander une saisie interactive :

```
How many bits in the modulus [512]: 2048
```

Analyse technique : Le nombre de bits détermine la robustesse de la clé face aux attaques par force brute. Si la valeur choisie est inférieure à 768 bits, Cisco IOS considère la sécurité comme insuffisante et refusera purement et simplement d'activer le démon SSH. Une taille de module de **2048 bits** a été injectée pour assurer un niveau de sécurité maximal et conforme aux standards actuels.

Étape 4 : Forçage de la version de sécurité (`ip ssh version 2`)

```
R-PME2(config)# ip ssh version 2
```

Analyse technique : Par défaut, si cette commande n'est pas spécifiée, l'équipement peut accepter des négociations descendantes vers SSHv1 pour des raisons de rétrocompatibilité. SSHv1 présentant des failles critiques documentées (vulnérabilité aux attaques de type *Man-In-The-Middle*), cette ligne verrouille logiciellement l'usage exclusif du protocole SSH version 2.

Étape 5 : Création du compte utilisateur local avec privilèges élevés

```
R-PME2(config)# username admin privilege 15 secret cisco123!
```

Analyse technique : Le paramètre `secret` implique l'utilisation d'un algorithme de hachage fort pour stocker le mot de passe dans le fichier de configuration, empêchant sa lecture en clair lors d'un `show running-config`. Le paramètre `privilege 15` attribue immédiatement le niveau d'accréditation maximal de Cisco (équivalent au mode `enable`). Ainsi, l'administrateur arrivant en SSH is directement positionné dans le prompt privilégié, éliminant le besoin de ressaisir un second mot de passe d'activation.

Étape 6 : Configuration et sécurisation des lignes virtuelles (`line vty`)

```
R-PME2(config)# line vty 0 4
R-PME2(config-line)# login local
R-PME2(config-line)# transport input ssh
```

Analyse technique : Les lignes VTY (*Virtual Teletype*) représentent les canaux d'accès virtuels pour les connexions réseau distantes. La commande `login local` indique aux lignes d'interroger la base de données interne de l'appareil (où réside le compte `admin` créé à l'étape précédente). Enfin, la commande `transport input ssh` applique un pare-feu protocolaire strict : l'équipement n'acceptera plus que le flux chiffré SSH, rejetant toute tentative de connexion non sécurisée (comme Telnet).

4 Scripts de Configuration Complets par Site

4.1 Cœur de Réseau Internet (FAI)

Conformément aux exigences d'étanchéité, l'accès distant (VTY) est totalement condamné sur ce périmètre via la commande `transport input none` pour empêcher toute tentative d'intrusion extérieure.

```
enable
configure terminal
hostname SW-INTERNET-CENTRAL

vlan 80
 name WAN_INTERCONNEXION
vlan 200
 name SERVEURS_INTERNET_PUBLICS
exit

interface range fastEthernet 0/1 - 5
 switchport mode access
 switchport access vlan 80
 spanning-tree portfast
 no shutdown
exit

interface range fastEthernet 0/10 - 15
 switchport mode access
 switchport access vlan 200
 spanning-tree portfast
 no shutdown
exit

interface gigabitEthernet 0/1
 switchport mode trunk
 switchport trunk allowed vlan 80,200
 no shutdown
exit

line vty 0 15
 transport input none
exit
end
write
```

Listing 1 – Configuration du Switch Internet Central

```
enable
configure terminal
hostname R-INTERNET
ipv6 unicast-routing

interface GigabitEthernet0/0
 no ip address
 no shutdown
exit

interface GigabitEthernet0/0.80
 encapsulation dot1Q 80
 ip address 80.1.1.1 255.255.255.0
```

```
 ipv6 address 2001:db8:ffff:12::1/64
 ipv6 address fe80::1 link-local
exit

interface GigabitEthernet0/0.200
 encapsulation dot1Q 200
 ip address 200.1.1.254 255.255.255.0
 ipv6 address 2001:db8:ffff:200::254/64
 ipv6 address fe80::1 link-local
exit

! Declaration des routes de retour vers les r seaux publics de la PME 2
ip route 198.51.100.0 255.255.255.224 80.1.1.4

router ospf 1
 router-id 1.1.1.1
 network 80.1.1.0 0.0.0.255 area 0
exit

ipv6 router ospf 1
 router-id 1.1.1.1
exit

interface GigabitEthernet0/0.80
 ipv6 ospf 1 area 0
exit

line vty 0 4
 transport input none
exit
end
write
```

Listing 2 – Configuration du Routeur Internet FAI

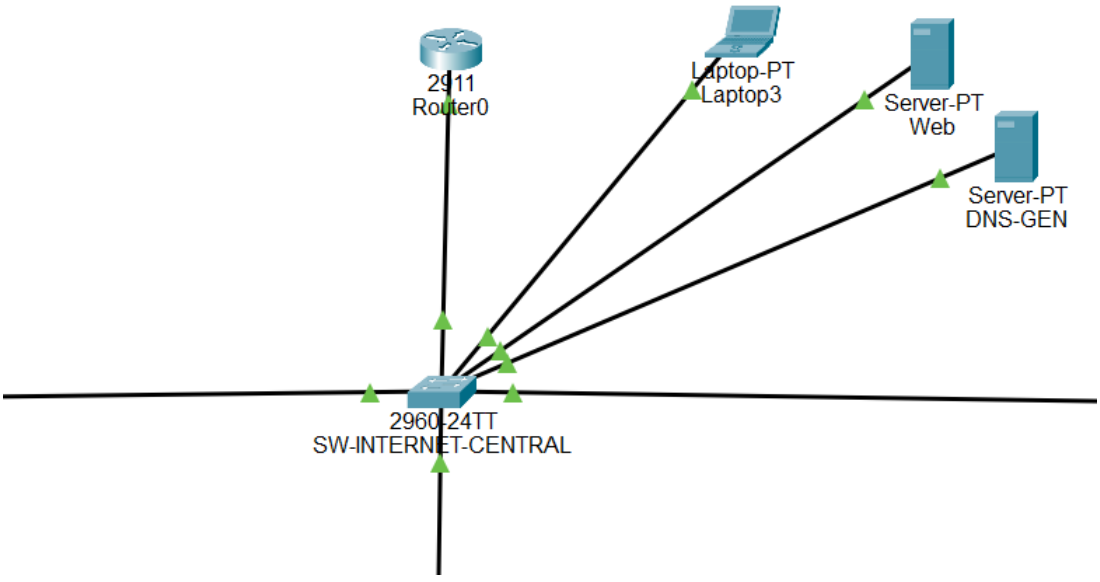

FIGURE 1 – Topologie globale et interconnexions de la zone opérateur FAI.

4.2 Configuration du Site TPE

Le site TPE utilise un adressage IPv4 privé dynamique pour ses hôtes via un pool DHCP interne, protégé de l'extérieur par une translation d'adresse dynamique globale (NAT Overload/PAT) sur son interface WAN.

```
enable
configure terminal
hostname R-TPE

ip dhcp excluded-address 192.168.1.254
ip dhcp excluded-address 192.168.1.1 192.168.1.10
ip dhcp pool POOL_LAN_TPE
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.254
 dns-server 200.1.1.1
exit

interface GigabitEthernet0/0
 ip address 192.168.1.254 255.255.255.0
 ip nat inside
 no shutdown
exit

interface GigabitEthernet0/1
 ip address 80.1.1.2 255.255.255.0
 ip nat outside
 no shutdown
exit

access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 interface GigabitEthernet0/1 overload
ip route 0.0.0.0 0.0.0.0 80.1.1.1

line vty 0 4
 transport input none
exit
end
write
```

Listing 3 – Configuration du Routeur TPE

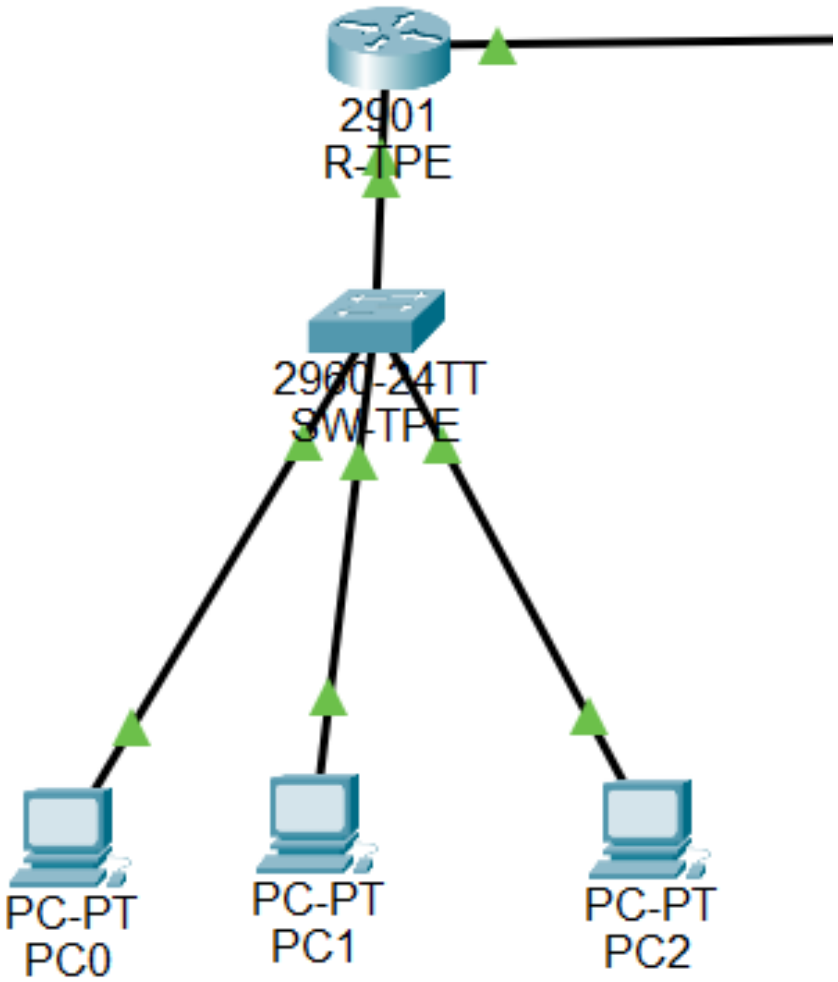

FIGURE 2 – Topologie locale du réseau de la TPE.

4.3 Configuration du Site PME 1 (Double Pile & Publication HTTP)

La PME 1 implémente un routage inter-VLAN de type *Router-on-a-Stick* associé à une translation NAT Statique pour rendre son serveur Web interne accessible depuis l'Internet public via l'IP publique WAN. Elle intègre également l'IPv6 natif de bout en bout (sans NAT) grâce à l'activation du routage unicast.

```
enable
configure terminal
hostname R-PME1
ipv6 unicast-routing

! --- CONFIGURATION INTERFACES PHYSIQUES ---
interface GigabitEthernet0/0
 no ip address
 no shutdown
exit

interface GigabitEthernet0/1
 ip address 80.1.1.3 255.255.255.0
 ip nat outside
 ipv6 address 2001:db8:80::3/64
 ipv6 enable
 no shutdown
exit

! --- ROUTAGE INTER-VLAN (ROAS) ---
! VLAN 10 : Zone DMZ h bergeant le serveur Web
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.254 255.255.255.0
 ip nat inside
 ipv6 address 2001:db8:1:10::254/64
 ipv6 enable
 no shutdown
exit

! VLAN 20 : Zone LAN
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.254 255.255.255.0
 ip nat inside
 ipv6 address 2001:db8:1:20::254/64
 ipv6 enable
 no shutdown
exit

! --- ROUTAGE & TRANSLATION (NAT) ---
ip route 0.0.0.0 0.0.0.0 80.1.1.1
ipv6 route ::/0 2001:db8:80::1

no ip http server
no ip http secure-server

! Reglique de NAT Statique pour le serveur Web du VLAN 10
ip nat inside source static tcp 192.168.10.10 80 80.1.1.3 80

line vty 0 4
 transport input none
```

```
exit
end
write memory
```

Listing 4 – Configuration du Routeur PME 1

```
enable
configure terminal
hostname SW-PME1

vlan 10
 name DMZ
vlan 20
 name LAN
exit

interface gigabitEthernet 0/1
 switchport mode trunk
 switchport trunk allowed vlan 10,20
 no shutdown
exit

interface fastEthernet 0/10
 switchport mode access
 switchport access vlan 10
 no shutdown
exit

interface range fastEthernet 0/1 - 3
 switchport mode access
 switchport access vlan 20
 no shutdown
exit
end
write memory
```

Listing 5 – Configuration du Switch SW-PME1

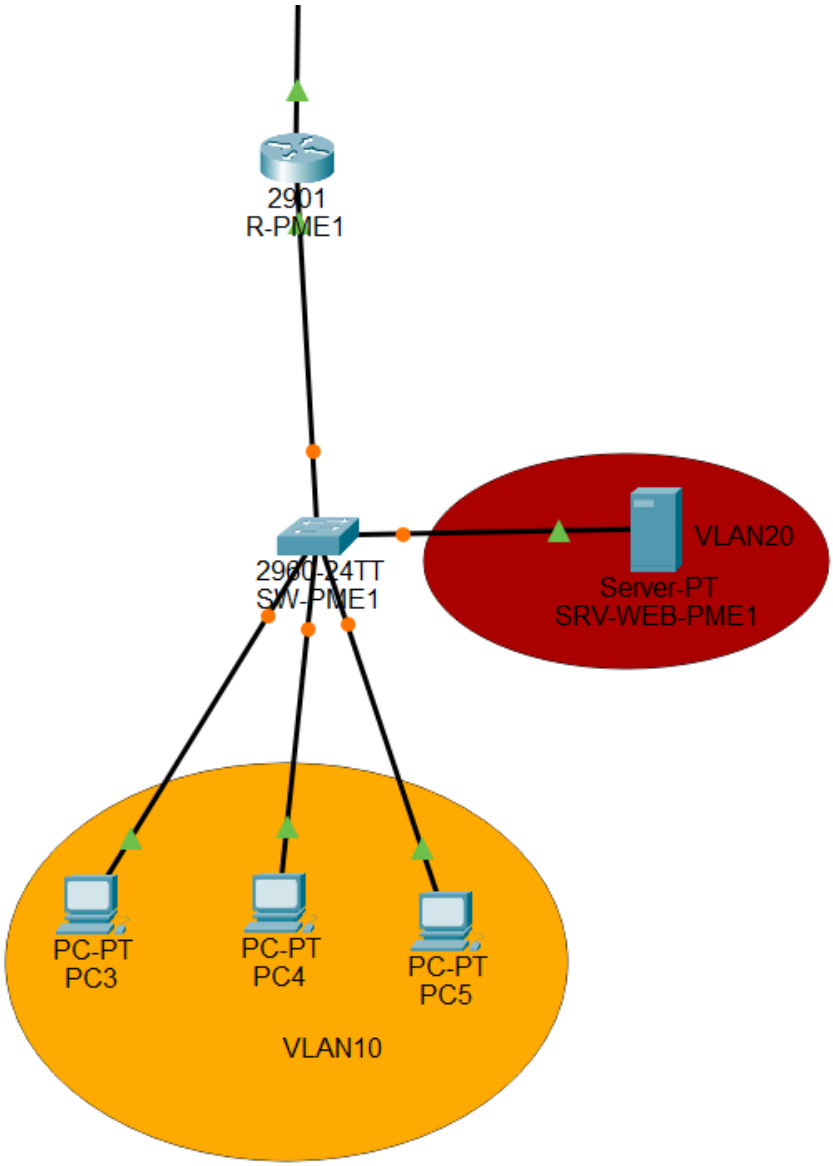

FIGURE 3 – Architecture réseau de la PME 1 et publication du serveur Web.

4.4 Configuration du Site PME 2 (Périmètre Haute Sécurité)

Commutateur d'Accès : `SW-PME2-ACCES`

Ce commutateur héberge le PC d'administration sur son port `Fa0/4` au sein du VLAN 30. Les ports de liaison montante en diagonale (`Fa0/1-2`) sont configurés en mode Trunk.

```
enable
configure terminal
hostname SW-PME2-ACCES
ip domain-name rt.sae201.fr

service password-encryption
enable secret class
username admin privilege 15 secret cisco123!

crypto key generate rsa
2048
ip ssh version 2

spanning-tree mode rapid-pvst

vlan 10
 name Bureautique
vlan 20
 name Production
vlan 30
 name Informatique_Admin
vlan 40
 name DMZ_PME2
vlan 999
 name VLAN_MORT_PORT_SHUTDOWN
exit

! Configuration des ports Trunks d'interconnexion en cascade vers SW-PME2-
   CORE
interface range fastEthernet 0/1 - 2
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40
 no shutdown
exit

! Affectation du PC d'administration sur le port physique Fa0/4
interface fastEthernet 0/4
 switchport mode access
 switchport access vlan 30
 spanning-tree portfast
 no shutdown
exit

! Interface Virtuelle de Gestion (SVI)
interface vlan 30
 ip address 172.16.30.251 255.255.255.0
 no shutdown
exit
ip default-gateway 172.16.30.254

access-list 10 permit 172.16.30.0 0.0.0.255
```

```
line vty 0 15
 login local
 transport input ssh
 access-class 10 in
exit
end
write
```

Listing 6 – Configuration de SW-PME2-ACCES

Commutateur de Distribution : `SW-PME2-CORE`

Le commutateur de cœur gère l'interconnexion montante et l'autorité Spanning-Tree pour la PME 2.

```
enable
configure terminal
hostname SW-PME2-CORE
ip domain-name rt.sae201.fr

service password-encryption
enable secret class
username admin privilege 15 secret cisco123!

crypto key generate rsa
2048
ip ssh version 2

spanning-tree mode rapid-pvst
vlan 10
vlan 20
vlan 30
vlan 40
exit

spanning-tree vlan 10,20,30,40 priority 4096

! Configuration des ports Trunks vers le switch d'acces inf rieur
interface range fastEthernet 0/1 - 2
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40
 no shutdown
exit

! Liaison montante Trunk vers le Routeur R-PME2
interface gigabitEthernet 0/1
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40
 no shutdown
exit

interface vlan 30
 ip address 172.16.30.250 255.255.255.0
 no shutdown
exit
ip default-gateway 172.16.30.254

access-list 10 permit 172.16.30.0 0.0.0.255

line vty 0 15
 login local
 transport input ssh
 access-class 10 in
exit
end
write
```

Listing 7 – Configuration de SW-PME2-CORE

Routeur de Tête : `R-PME2` (Routage Pur sans NAT)

Passerelle de la PME 2, configurée en routage IP public strict pour la zone DMZ.

```
enable
configure terminal
hostname R-PME2
ip domain-name rt.sae201.fr
ipv6 unicast-routing

service password-encryption
enable secret class
username admin privilege 15 secret cisco123!

crypto key generate rsa
2048
ip ssh version 2

interface GigabitEthernet0/1
 ip address 80.1.1.4 255.255.255.0
 ipv6 address 2001:db8:ffff:12::4/64
 no shutdown
exit

interface GigabitEthernet0/0
 no ip address
 no shutdown
exit

interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.16.10.254 255.255.255.0
 ipv6 address 2001:db8:1:10::254/64
exit

interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 172.16.20.254 255.255.255.0
 ipv6 address 2001:db8:1:20::254/64
exit

interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.16.30.254 255.255.255.0
 ipv6 address 2001:db8:1:30::254/64
exit

! SOUS-INTERFACE DMZ : Routage Pur sans aucun NAT
interface GigabitEthernet0/0.40
 encapsulation dot1Q 40
 ip address 198.51.100.30 255.255.255.224
 ipv6 address 2001:db8:1:40::254/64
exit

ip route 0.0.0.0 0.0.0.0 80.1.1.1
ipv6 route ::/0 2001:db8:ffff:12::1

access-list 10 permit 172.16.30.0 0.0.0.255
```

```
line vty 0 4
 login local
 transport input ssh
 access-class 10 in
exit
end
write
```

Listing 8 – Configuration du Routeur R-PME2

5 Architecture des Services Applicatifs (DNS mixte)

La topologie DNS intègre un mécanisme hybride de résolution centralisée directe pour la PME 1 et de délégation d'autorité complète par zone pour la PME 2.

5.1 Serveur DNS Central Operator (`R-INTERNET` / Zone FAI)

Ce serveur externe simule le serveur DNS racine mondial. Ne trouvant pas de serveur DNS interne à la PME 1, il résout directement ses enregistrements, tandis qu'il délègue la gestion de la zone `pme2.lan` au serveur dédié de l'entreprise.

- **Configuration du Service DNS (Central) :**
  - `www.pme1.lan` → Type `A` (Direct) → `80.1.1.3` (IP Publique du NAT R-PME1)
  - `www.pme1.lan` → Type `AAAA` (Direct) → `2001:db8:80::3`
  - `pme2.lan` → Type `NS` (Délégation) → `dns.pme2.lan`
  - `dns.pme2.lan` → Type `A` (Glue Record) → `198.51.100.1`

5.2 Serveur DNS/Web Local (`SRV-WEB-PME2` – DMZ PME 2)

Le serveur de la PME 2 cumule les fonctions applicatives de serveur Web HTTP et de serveur DNS faisant autorité déléguée sur sa zone.

- **Configuration Réseau de l'Hôte :**
  - **IP Address :** `198.51.100.1` | **Subnet Mask :** `255.255.255.224`
  - **Default Gateway :** `198.51.100.30`
- **Base de données DNS locale :**
  - `www.pme2.lan` → Type `A` → `198.51.100.1`

6 Journal de Recette, Audit et Dépannage

6.1 Rapport d'Incident 1 : Résolution du Blocage des Liaisons Trunks de la PME 1

Description de l'anomalie : Les requêtes HTTP externes vers le serveur Web de la PME 1 échouaient systématiquement, alors que l'IP publique répondait au ping. Le message d'erreur du simulateur indiquait une perte de paquets étiquetés au niveau du switch.

Investigation et Diagnostic : La commande `show vlan brief` sur `SW-PME1` a mis en évidence que le port de liaison montante `Gig0/1` vers le routeur n'était pas configuré en mode Trunk, isolant de fait le trafic du VLAN 10 (DMZ).

Résolution : L'activation explicite du protocole d'encapsulation et du mode Trunk sur l'interface `Gig0/1` a permis l'ouverture de l'autoroute de commutation des VLANs 10 et 20, restaurant immédiatement les accès HTTP.

6.2 Rapport d'Incident 2 : Échec d'accès HTTP et correction du Routage Pur sur la PME 2

Description de l'anomalie : Les pings vers le serveur Web public de la PME 2 se soldaient par des *Request timed out* et le mode simulation affichait l'erreur CEF : *"The NAT table does not have a matched entry for this packet"*.

Investigation et Diagnostic : L'analyse approfondie a démontré que l'application d'un mécanisme de NAT par port perturbait le fonctionnement du routeur `R-PME2`. La DMZ de l'entreprise utilisant déjà des adresses publiques réelles (`198.51.100.0/27`), le NAT était superflu. De surcroît, le routeur central du FAI ne possédait pas la route de retour pour ce sous-réseau spécifique.

Résolution : Le NAT a été entièrement purgé sur `R-PME2`. Une route statique retour a été injectée sur le routeur central FAI (`ip route 198.51.100.0 255.255.255.224 80.1.1.4`). Enfin, la liaison

d'interconnexion en cascade entre les deux commutateurs de la PME 2 a été passée en Trunking pour permettre la redescente des trames du VLAN 40 jusqu'au serveur. Les flux HTTP et ICMP se sont instantanément débloqués.

7 Conclusion

L'architecture finale simulée remplit l'intégralité des clauses de sécurité requises pour la SAÉ. L'intégration de verrous de sécurité directement au niveau de la couche 2 (commutation par trunks dédiés, extinction et mise au "trou noir" des ports physiques orphelins) couplée aux filtres de couche 4 (listes d'accès restrictives appliquées sur des terminaux VTY exclusivement chiffrés en SSHv2) assure à la PME 2 un périmètre de gestion hermétique. La maquette est entièrement validée sur le plan logique et fonctionnel, prête pour un déploiement sur des équipements matériels physiques de production.