DOSSIER TECHNIQUE : INTERCONNEXION SÉCURISÉE SITE-À-SITE

Gildas CHERAUD BOISTEAU

BTS Service Informatique aux Organisations option SISR

Sommaire

1. Descriptif du Projet et Compétences

1.1 Descriptif

Ce projet vise à concevoir et déployer une infrastructure réseau répartie sur deux sites géographiques pour une PME. L'objectif est d'interconnecter les réseaux locaux via un tunnel VPN IPsec sécurisé pour que l'entreprise puisse assurer le partage de fichiers sensibles d'un site à un autre..

1.1.1 Objectif du service

Le service mis à disposition permet aux utilisateurs des deux sites d'accéder de manière sécurisée aux ressources réseau distantes (partages, serveurs, applications internes), tout en garantissant la confidentialité des échanges.

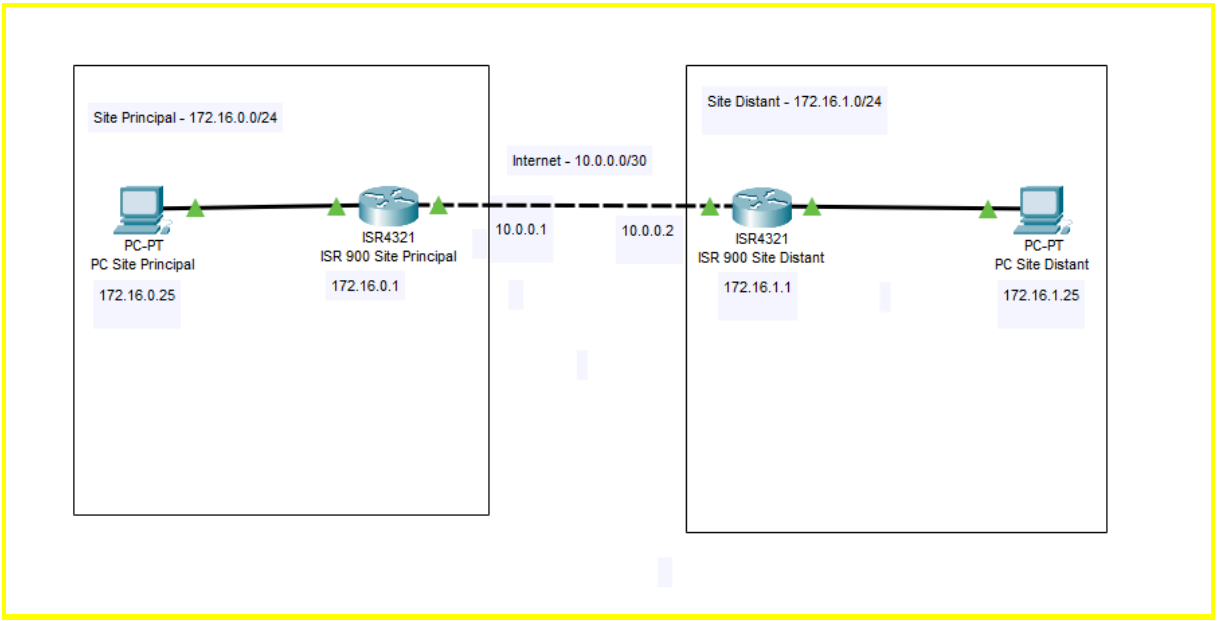
1.1.2 Utilisateurs concernés

Ce service est destiné aux utilisateurs des sites principaux et distant ayant besoin d'accéder aux ressources internes de l'entreprise dans le cadre de leurs activités professionnelles.

1.3 Tableau des compétences mobilisées

Code	Compétence
C1.1	Recueillir les besoins et les contraintes techniques
C2.1	Installer et configurer les équipements réseau
C2.2	Sécuriser les équipements et les flux réseau
C3.1	Administrer les services réseau (VPN, routage)
C3.2	Diagnostiquer et corriger les dysfonctionnements
C4.1	Rédiger une documentation technique claire et structurée

1.4 Schéma Réseau Technique



1.5 Justification du choix matériel et du mode de configuration

Les équipements utilisés dans cette réalisation sont des **routeurs Cisco ISR 900 Series**, disposant de **ports Ethernet intégrés de type switch (Layer 2)**.
Sur cette gamme de matériels, les interfaces physiques fonctionnent par défaut en **mode commuté**, ce qui implique l'utilisation de **VLAN** et d'**interfaces virtuelles SVI (interface Vlan X)** pour assurer le routage de niveau 3.

Dans ce contexte :

- Les ports physiques sont configurés en `switchport access` et associés à un VLAN dédié (LAN ou WAN).
- Les adresses IP et les fonctions de routage sont portées par les **interfaces VLAN**, conformément au fonctionnement des ISR 900.
- Le lien WAN est simulé via un VLAN spécifique, ce qui permet de représenter une interconnexion inter-sites dans un environnement maîtrisé sans équipement opérateur intermédiaire.

Ce choix matériel et cette architecture sont cohérents avec les capacités natives des **ISR 900 Series** et permettent de mettre en œuvre :

- le routage IP,
- le VPN site-à-site IPsec,
- les ACL appliquées sur l'interface logique WAN,

tout en restant dans un cadre réaliste d'infrastructure PME.

1.6 Recensement des ressources matérielles et logicielles

Les ressources composant le patrimoine informatique mobilisé pour ce projet sont :

- Deux routeurs Cisco ISR 900 Series assurant l'interconnexion sécurisée entre les sites
- Des interfaces VLAN pour la séparation des réseaux LAN et WAN
- Un tunnel VPN IPsec garantissant la confidentialité des échanges
- Des postes clients utilisés pour la validation du service

1.7 Référentiels et bonnes pratiques

La mise en œuvre du VPN s'appuie sur les bonnes pratiques de sécurisation des flux réseau, notamment l'utilisation du chiffrement IPsec et le filtrage des communications via des ACL.

2. Architecture et Plan d'Adressage

L'architecture est simplifiée à deux routeurs ISR 900 Series connectés directement en GigabitEthernet pour la simulation WAN.

2. 1 Plan d'adressage IP

- **Lien WAN (Inter-routeurs) :** `10.0.0.0/30`
  - **R-PRINCIPAL (Interface WAN Gi0/0/0) :** `10.0.0.1`
  - **R-DISTANT (Interface WAN Gi0/0/0) :** `10.0.0.2`
- **Site Principal (LAN) :** `172.16.0.0/24`
  - **Passerelle (SVI Vlan 1) :** `172.16.0.1`
- **Site Distant (LAN) :** `172.16.1.0/24`
  - **Passerelle (SVI Vlan 1) :** `172.16.1.1`

3. Configuration détaillée de R-PRINCIPAL

3.1 Initialisation et Interfaces

- Mode **Utilisateur** à **Privilégié :** Router> enable
- Mode **Privilégié** à **Configuration Globale :** Router# configure terminal

```
R-PRINCIPAL# configure terminal
R-PRINCIPAL(config)# hostname R-PRINCIPAL
R-PRINCIPAL(config)# no ip domain-lookup

! --- Configuration du LAN (Vlan 1) ---
R-PRINCIPAL(config)# interface Vlan 1
R-PRINCIPAL(config-if)# description LAN_SIÈGE
R-PRINCIPAL(config-if)# ip address 172.16.0.1 255.255.255.0
R-PRINCIPAL(config-if)# no shutdown
R-PRINCIPAL(config-if)# exit

! --- Configuration du WAN (Vlan 2) ---
R-PRINCIPAL(config)# interface Vlan 2
R-PRINCIPAL(config-if)# description WAN_INTERCONNEXION
R-PRINCIPAL(config-if)# ip address 10.0.0.1 255.255.255.252
R-PRINCIPAL(config-if)# no shutdown
R-PRINCIPAL(config-if)# exit

R-PRINCIPAL(config)#licence boot module c900 technology-package securityk9
R-PRINCIPAL(config)#yes
R-PRINCIPAL(config)#exit
R-PRINCIPAL#write
R-PRINCIPAL#reload

! --- Assignation des ports physiques au mode L2 ---
R-PRINCIPAL(config)# interface GigabitEthernet 0
R-PRINCIPAL(config-if)# switchport mode access
R-PRINCIPAL(config-if)# switchport access vlan 2
R-PRINCIPAL(config-if)# exit

R-PRINCIPAL(config)# interface GigabitEthernet 01
R-PRINCIPAL(config-if)# switchport mode access
R-PRINCIPAL(config-if)# switchport access vlan 1
R-PRINCIPAL(config-if)# exit

! --- Routage Statique vers le site distant ---
```

```
R-PRINCIPAL(config)# ip route 172.16.1.0 255.255.255.0 10.0.0.2
```

```
R-PRINCIPAl(config)#do show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0           unassigned      YES unset  down                  down
GigabitEthernet1           unassigned      YES unset  up                    up
GigabitEthernet2           unassigned      YES unset  down                  down
GigabitEthernet3           unassigned      YES unset  down                  down
GigabitEthernet4           unassigned      YES NVRAM  administratively down down
GigabitEthernet5           unassigned      YES NVRAM  administratively down down
Vlan1                      172.16.0.1      YES NVRAM  up                    up
Vlan2                      10.0.0.1        YES NVRAM  down                  down
R-PRINCIPAl(config)#
```

3.2 Paramétrage du VPN IPsec

```
! --- Phase 1 : ISAKMP Policy ---
R-PRINCIPAL(config)# crypto isakmp policy 10
R-PRINCIPAL(config-isakmp)# encryption aes
R-PRINCIPAL(config-isakmp)# hash sha256
R-PRINCIPAL(config-isakmp)# authentication pre-share
R-PRINCIPAL(config-isakmp)# group 14
R-PRINCIPAL(config-isakmp)# exit
R-PRINCIPAL(config)# crypto isakmp key VPNKEY address 10.0.0.2

! --- Phase 2 : IPsec Transform-Set ---
R-PRINCIPAL(config)# crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac
R-PRINCIPAL(cfg-crypto-trans)# mode tunnel
R-PRINCIPAL(cfg-crypto-trans)# exit

! --- ACL VPN (Trafic à chiffrer) ---
R-PRINCIPAL(config)# ip access-list extended VPN-TRAFFIC
R-PRINCIPAL(config-ext-nacl)# permit ip 172.16.0.0 0.0.0.255 172.16.1.0 0.0.0.255
R-PRINCIPAL(config-ext-nacl)# exit

! --- Crypto Map et Application sur la SVI WAN (Vlan 2) ---
R-PRINCIPAL(config)# crypto map VPN-MAP 10 ipsec-isakmp
R-PRINCIPAL(config-crypto-map)# set peer 10.0.0.2
R-PRINCIPAL(config-crypto-map)# set transform-set TRANSFORM
R-PRINCIPAL(config-crypto-map)# match address VPN-TRAFFIC
R-PRINCIPAL(config-crypto-map)# exit

R-PRINCIPAL(config)# interface Vlan 2
R-PRINCIPAL(config-if)# crypto map VPN-MAP
```

```
R-PRINCIPAl(config-if)#crypto map VPN-MAP
R-PRINCIPAl(config-if)#
*Jan 23 13:12:39.063: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
*Jan 23 13:12:40.063: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to up
```

4. Configuration détaillée de R-DISTANT

```
R-DISTANT# configure terminal
R-DISTANT(config)# hostname R-DISTANT

! --- Configuration du LAN (Vlan 1) ---
R-DISTANT(config)# interface Vlan 1
R-DISTANT(config-if)# description LAN_AGENCE
R-DISTANT(config-if)# ip address 172.16.1.1 255.255.255.0
R-DISTANT(config-if)# no shutdown
R-DISTANT(config-if)# exit

! --- Configuration du WAN (Vlan 2) ---
R-DISTANT(config)# interface Vlan 2
R-DISTANT(config-if)# description WAN_INTERCONNEXION
R-DISTANT(config-if)# ip address 10.0.0.2 255.255.255.252
R-DISTANT(config-if)# no shutdown
R-DISTANT(config-if)# exit

! --- Assignation des ports physiques ---
R-DISTANT(config)# interface GigabitEthernet 0
R-DISTANT(config-if)# switchport mode access
R-DISTANT(config-if)# switchport access vlan 2
R-DISTANT(config-if)# exit

R-DISTANT(config)# interface GigabitEthernet 01
R-DISTANT(config-if)# switchport mode access
R-DISTANT(config-if)# switchport access vlan 1
R-DISTANT(config-if)# exit

! --- Routage Statique de retour ---
R-DISTANT(config)# ip route 172.16.0.0 255.255.255.0 10.0.0.1

R-DISTANT(config)#licence boot module c900 technology-package securityk9
R-DISTANT(config)#yes
R-DISTANT(config)#exit
R-DISTANT#write
R-DISTANT#reload

R-DISTANT>en
R-DISTANT#configure terminal
R-DISTANT(config)# crypto isakmp policy 10
R-DISTANT(config-isakmp)# encryption aes
R-DISTANT(config-isakmp)# hash sha256
```

```
R-DISTANT(config-isakmp)# authentication pre-share
R-DISTANT(config-isakmp)# group 14
R-DISTANT(config-isakmp)# exit
R-DISTANT(config)# crypto isakmp key VPNKEY address 10.0.0.1
R-DISTANT(config)# crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac
R-DISTANT(cfg-crypto-trans)# mode tunnel
R-DISTANT(cfg-crypto-trans)# exit

R-DISTANT(config)# ip access-list extended VPN-TRAFFIC
R-DISTANT(config-ext-nacl)# permit ip 172.16.1.0 0.0.0.255 172.16.0.0 0.0.0.255
R-DISTANT(config-ext-nacl)# exit

R-DISTANT(config)# crypto map VPN-MAP 10 ipsec-isakmp
R-DISTANT(config-crypto-map)# set peer 10.0.0.1
R-DISTANT(config-crypto-map)# set transform-set TRANSFORM
R-DISTANT(config-crypto-map)# match address VPN-TRAFFIC
R-DISTANT(config-crypto-map)# exit

R-DISTANT(config)# interface Vlan 2
R-DISTANT(config-if)# crypto map VPN-MAP
```

5. Sécurisation et Filtrage WAN (ACL)

```
R-PRINCIPAL(config)# ip access-list extended ACL-SECURITE-WAN
R-PRINCIPAL(config-ext-nacl)# permit esp host 10.0.0.2 host 10.0.0.1
R-PRINCIPAL(config-ext-nacl)# permit udp host 10.0.0.2 host 10.0.0.1 eq isakmp
R-PRINCIPAL(config-ext-nacl)# permit icmp any any
R-PRINCIPAL(config-ext-nacl)# deny ip any any
R-PRINCIPAL(config-ext-nacl)# exit

R-PRINCIPAL(config)# interface Vlan 2
R-PRINCIPAL(config-if)# ip access-group ACL-SECURITE-WAN in
```

```
R-DISTANT(config)#ip route 172.16.0.0 255.255.255.0 10.0.0.1
*Jan 23 13:38:18.231: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up
R-DISTANT(config)#do show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0           unassigned      YES unset  up                    up
GigabitEthernet1           unassigned      YES unset  up                    up
GigabitEthernet2           unassigned      YES unset  down                  down
GigabitEthernet3           unassigned      YES unset  down                  down
GigabitEthernet4           unassigned      YES unset  administratively down down
GigabitEthernet5           unassigned      YES unset  administratively down down
Vlan1                      172.16.1.1      YES manual up                    up
Vlan2                      10.0.0.2        YES manual up                    up
R-DISTANT(config)#
```

6. Sauvegarde et Procédures de Validation

6.1 Sauvegarde des configurations

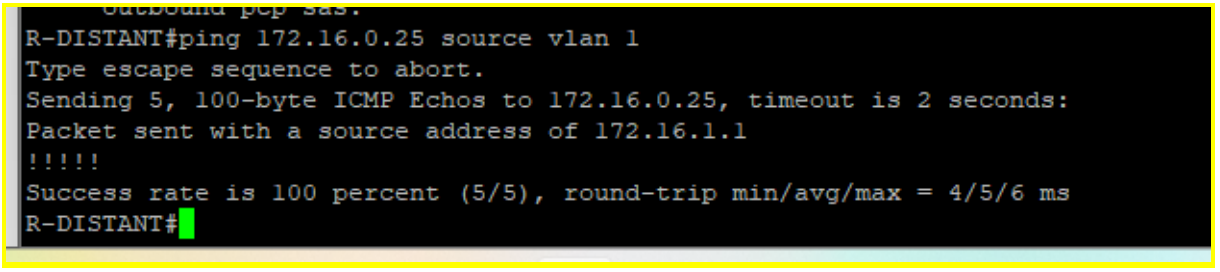
Une fois les tests concluants, la configuration est enregistrée en NVRAM.

- Sur les deux routeurs : `R-PRINCIPAL# copy running-config startup-config`

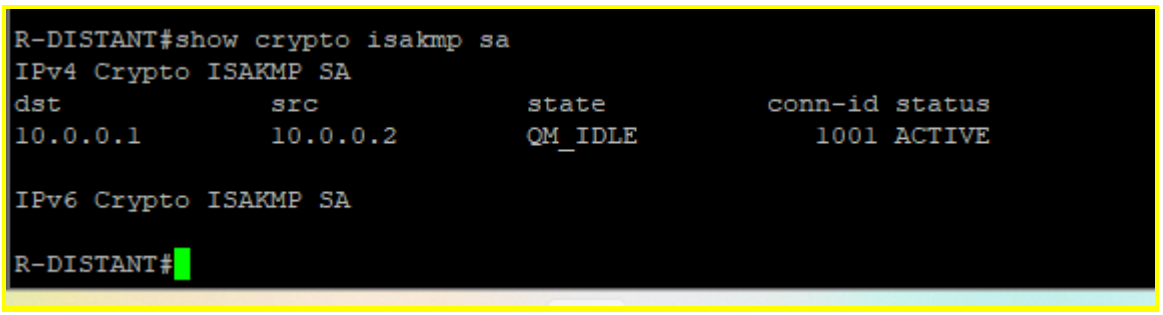
Cette commande sert à sauvegarder la configuration en run dans la NVRAM du routeur.

6.2 Validation technique

- **Test de connectivité :** Ping depuis un poste client Site Principal vers un poste client Site Distant.



- **Vérification du Tunnel (Phase 1) :** `show crypto isakmp sa` -> Doit afficher **QM_IDLE**.
- **Vérification du Chiffrement (Phase 2) :** `show crypto ipsec sa` -> Vérifier que les compteurs **#pkts encaps** et **#pkts decaps** augmentent.



```
R-DISTANT#show crypto ipsec sa

interface: Vlan2
    Crypto map tag: VPN-MAP, local addr 10.0.0.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (172.16.0.0/255.255.255.0/0/0)
   current_peer 10.0.0.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7
    #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.0.0.2, remote crypto endpt.: 10.0.0.1
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Vlan2
     current outbound spi: 0xA6508952(2790295890)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x4C038035(1275297845)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: Onboard VPN:1, sibling_flags 80004040, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4343173/3538)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xA6508952(2790295890)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: Onboard VPN:2, sibling_flags 80004040, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4343173/3538)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
R-DISTANT#
```

6.3 Exploitation et Supervision du service

L'état du tunnel VPN est vérifié régulièrement à l'aide des commandes de diagnostic (ISAKMP et IPsec). En cas de perte de connectivité inter-sites, ces vérifications permettent d'identifier rapidement l'origine du dysfonctionnement et de rétablir le service.

7. Lien avec le support

En cas d'incident impactant la communication inter-sites, une demande de support est ouverte afin de restaurer rapidement le service et garantir la continuité d'activité.