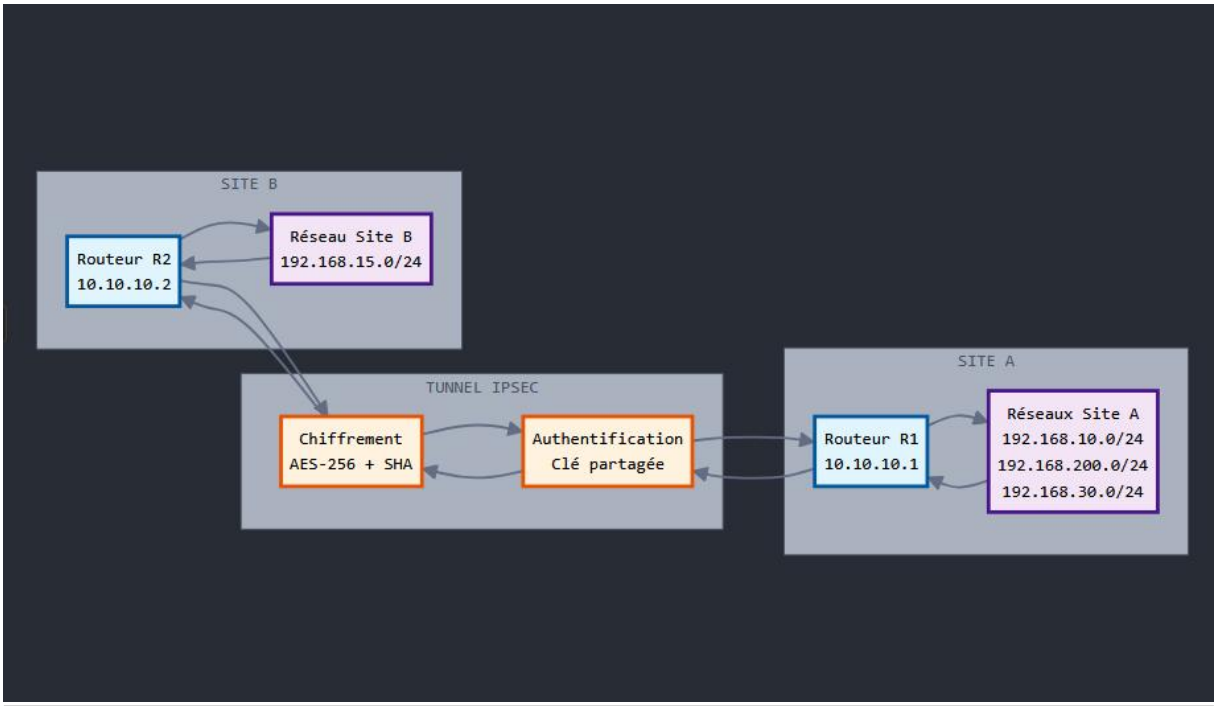
Configuration du VPN

Introduction

Dans le cadre de l'interconnexion sécurisée entre deux sites distants de l'entreprise SmartTech, nous avons mis en place un tunnel VPN site-à-site basé sur le protocole IPSec. Ce type de connexion permet d'établir une liaison privée et chiffrée entre deux routeurs situés dans des réseaux géographiquement séparés, en transitant par Internet de manière sécurisée.

La configuration repose sur l'utilisation de **protocoles ISAKMP/IKE pour la négociation de clés** et **d'une crypto map** pour associer les paramètres de sécurité à une interface réseau. L'objectif est de garantir la confidentialité, l'intégrité et l'authenticité des données échangées entre les deux sites, tout en maintenant une communication transparente entre les réseaux locaux respectifs.

Schéma Explicatif :



A. Configuration R1 :

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#! ISAKMP
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encr aes 256
R1(config-isakmp)#hash sha
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#lifetime 86400
R1(config-isakmp)#exit
R1(config)#crypto isakmp key vpnkey123 address 10.10.10.2
R1(config)#! Transform-set
R1(config)#crypto ipsec transform-set MY-TRANSFORM esp-aes esp-sha-hmac
R1(cfg-crypto-trans)#mode tunnel
```

```
R1(cfg-crypto-trans)#access-list 100 permit ip 192.168.10.0 0.0.0.255 192.168.$
```

```
R1(config)#! Crypto map
R1(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#set peer 10.10.10.2
R1(config-crypto-map)#set transform-set MY-TRANSFORM
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exit
```

1. Configuration ISAKMP (Phase 1)

crypto isakmp policy 10

encr aes 256 # Chiffrement AES-256

hash sha # Hashing SHA-1

authentication pre-share # Authentification par clé pré-partagée

group 2 # Groupe Diffie-Hellman 2 (1024 bits)

lifetime 86400 # Durée de vie des SA (1 jour)

exit

crypto isakmp key vpnkey123 address 10.10.10.2 # Clé pré-partagée pour le peer

Objectif : Établir une connexion sécurisée pour négocier les paramètres IPSec.

2. Configuration du Transform-Set (Phase 2)

crypto ipsec transform-set MY-TRANSFORM esp-aes esp-sha-hmac

mode tunnel # Mode tunnel (masquage des IP d'origine)

exit

Objectif : Définir comment les données seront chiffrées (AES) et authentifiées (SHA).

3. ACL pour le Trafic à Protéger

access-list 100 permit ip 192.168.10.0 0.0.0.255 192.168.15.0 0.0.0.255

Objectif : Autoriser uniquement le trafic entre le sous-réseaux local (LAN) et le réseau distant (192.168.15.0/24).

4. Configuration de la Crypto-Map

crypto map VPN-MAP 10 ipsec-isakmp

set peer 10.10.10.2 # Adresse IP du routeur distant (R2)

set transform-set MY-TRANSFORM # Applique le transform-set

match address 100 # Lie l'ACL 100 au VPN

exit

Objectif : Lier tous les éléments (ISAKMP, transform-set, ACL) pour créer le VPN.

```
R1(config-router)#int s1/0
R1(config-if)#ip add 10.10.10.1 255.255.255.0
R1(config-if)#router rip
R1(config-router)#version 2
R1(config-router)#network 10.0.0.0
R1(config-router)#no auto
R1(config-router)#no auto-summary
R1(config-router)#int s1/0
R1(config-router)#int s1/0
R1(config-if)#crypto map VPN-MAP
R1(config-if)#
*Mar  1 00:22:46.403: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#no sh
R1(config-if)#
*Mar  1 00:22:59.231: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
R1(config-if)#
*Mar  1 00:23:00.235: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R1(config-if)#end
```

Dans cette capture Nous attribuer une ip sur l'interface de sortie vers R2.

Puis nous activons le routage dynamique tout en annoncant notre reseau au autres routeurs.

Et enfin nous Activons le VPN.

B. Configuration R2 :

```
R2(config)#int fa0/0
R2(config-if)#ip add 192.168.15.1 255.255.255.0
R2(config-if)#no sh
R2(config-if)#
*Mar  1 00:05:28.279: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:05:29.279: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
 up
```

Tout d'abord Nous attribuons une IP à R2 sur l'Interface de sont réseau local (fa0/0).

```
R2(config-if)#exit
R2(config)#! ISAKMP
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#encr aes 256
R2(config-isakmp)#hash sha
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 2
R2(config-isakmp)#lifetime 86400
R2(config-isakmp)#exit
R2(config)#crypto isakmp key vpnkey123 address 10.10.10.1
R2(config)#! Transform-set
R2(config)#crypto ipsec transform-set MY-TRANSFORM esp-aes esp-sha-hmac
R2(cfg-crypto-trans)#mode tunnel
R2(cfg-crypto-trans)#! ACL VPN
R2(cfg-crypto-trans)#access-list 100 permit ip 192.168.15.0 0.0.0.255 192.168.$
```

```
R2(config)#! Crypto map
R2(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R2(config-crypto-map)#set peer 10.10.10.1
R2(config-crypto-map)#set transform-set MY-TRANSFORM
R2(config-crypto-map)#match address 100
R2(config-crypto-map)#exit
```

Puis nous entrons a peu près les mêmes commandes que dans R1.

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 192.168.15.0
R2(config-router)#network 10.0.0.0
R2(config-router)#no auto
R2(config-router)#no auto-summary
R2(config-router)#int s1/0
R2(config-if)#ip add 10.10.10.2 255.255.255.0
R2(config-if)#crypto map VPN-MAP
R2(config-if)#
*Mar  1 00:18:26.775: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R2(config-if)#no sh
R2(config-if)#
*Mar  1 00:18:32.951: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
R2(config-if)#
*Mar  1 00:18:33.955: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R2(config-if)#end
```

Nous activons le routeur dynamique en annoncant aussi nos reseau au niveau du routeur R2

Puis nous lui attribuons une IP sur l'Interface de sortie vers R1 et enfin nous activons le VPN

C. <u>Tests et Captures Wireshark :</u>

```
R1#show crypto isakmp sa
dst             src             state          conn-id slot status
10.10.10.2      10.10.10.1      QM_IDLE              1    0 ACTIVE

R1#show crypto ipsec sa

interface: Serial1/0
    Crypto map tag: VPN-MAP, local addr 10.10.10.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.15.0/255.255.255.0/0/0)
   current_peer 10.10.10.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
     current outbound spi: 0xC4E91505(3303609605)

     inbound esp sas:
      spi: 0x2A13F100(705949952)
        transform: esp-aes esp-sha-hmac ,
 --More--
```

1. **show crypto isakmp sa (Phase 1 - Échange de clés ISAKMP)**

Analyse des champs :

- **dst (10.10.10.2)** : Adresse IP du pair distant (R2).
- **src (10.10.10.1)** : Adresse IP locale (R1).
- **state: QM_IDLE** :
    - **QM_IDLE** signifie que la **Phase 1 (ISAKMP)** est terminée avec succès et que le tunnel est prêt pour la **Phase 2 (IPSec)**.
    - C'est l'état normal après une négociation réussie.
- **conn-id et slot** : Identifiants internes pour la session.
- **status: ACTIVE** : La session est active et opérationnelle.

2. **show crypto ipsec sa (Phase 2 - Tunnel IPSec)**

Ces résultats nous montrent que le Tunnel actif avec trafic chiffré (AES/SHA).

D. <u>Capture wireshark :</u>

```
/ # ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10): 56 data bytes
64 bytes from 192.168.10.10: seq=0 ttl=62 time=32.471 ms
64 bytes from 192.168.10.10: seq=1 ttl=62 time=38.559 ms
64 bytes from 192.168.10.10: seq=2 ttl=62 time=35.471 ms
64 bytes from 192.168.10.10: seq=3 ttl=62 time=32.250 ms
^C
--- 192.168.10.10 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 32.250/34.687/38.559 ms
```

Depuis le client nous faisons un ping vers le serveur Nextcloud du LAN.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 64, returned sequence 62
2	1.879370	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 63, returned sequence 64
3	3.569549	10.10.10.1	224.0.0.9	RIPv2	176	Response
4	4.600298	10.10.10.2	10.10.10.1	ESP	156	ESP (SPI=0xd64397df)
5	4.608529	10.10.10.1	10.10.10.2	ESP	156	ESP (SPI=0x26a113ed)
6	5.509302	10.10.10.2	224.0.0.9	RIPv2	56	Response
7	5.600841	10.10.10.2	10.10.10.1	ESP	156	ESP (SPI=0xd64397df)
8	5.608439	10.10.10.1	10.10.10.2	ESP	156	ESP (SPI=0x26a113ed)
9	6.600611	10.10.10.2	10.10.10.1	ESP	156	ESP (SPI=0xd64397df)
10	6.608360	10.10.10.1	10.10.10.2	ESP	156	ESP (SPI=0x26a113ed)
11	7.599287	10.10.10.2	10.10.10.1	ESP	156	ESP (SPI=0xd64397df)
12	7.609468	10.10.10.1	10.10.10.2	ESP	156	ESP (SPI=0x26a113ed)
13	8.597478	10.10.10.2	10.10.10.1	ESP	156	ESP (SPI=0xd64397df)
14	8.607562	10.10.10.1	10.10.10.2	ESP	156	ESP (SPI=0x26a113ed)
15	9.817205	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 65, returned sequence 63
16	11.523623	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 64, returned sequence 65
17	13.908012	10.10.10.2	10.10.10.1	ESP	156	ESP (SPI=0xd64397df)
18	13.927550	10.10.10.1	10.10.10.2	ESP	156	ESP (SPI=0x26a113ed)

Comme on peut le voir toute la communication est encrypter avec le protocole ESP.

Conclusion

Dans le cadre de ce projet, nous avons mis en place un VPN site-à-site basé sur le protocole IPsec entre deux routeurs Cisco. Cette configuration permet désormais d'établir une liaison sécurisée entre deux réseaux distants via un tunnel chiffré, garantissant ainsi **la confidentialité, l'intégrité et l'authentification des données échangées**.

La mise en œuvre s'est appuyée sur :

- La définition des politiques ISAKMP (phase 1) pour établir une session sécurisée,
- La configuration du tunnel IPsec (phase 2) pour chiffrer le trafic entre les deux sites,
- L'utilisation d'ACLs permettant de sélectionner le trafic à sécuriser.

Après application et test, les vérifications ont confirmé le bon établissement du tunnel. Le trafic entre les deux LANs est désormais chiffré et acheminé correctement, comme attendu.