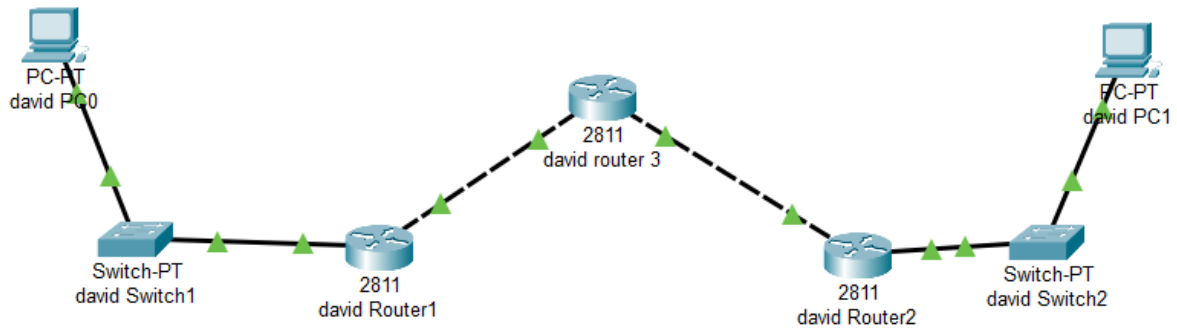
Rapport sur les Travaux Pratiques :

VPN IP sec CISCO de site à site

Introduction :

Dans le cadre de notre session de travaux pratiques, nous avons mis en place une liaison d'interconnexion site à site utilisant un tunnel VPN IP sec à travers un réseau non sécurisé tel qu'Internet. L'objectif principal était de sécuriser une connexion entre deux sites distincts en utilisant le protocole ISAKMP avec un secret partagé.

Nous avons reproduit l'image de deux petits réseaux locaux, chacun accédant à Internet via un routeur NAT avec la fonction 'Overlord'. La topologie utilisée pour notre maquette impliquait l'utilisation de routeurs Cisco 2811.



Configuration de base des routeurs :

Nous avons commencé par configurer de manière basique les trois routeurs impliqués dans la mise en place du VPN IP sec.

Routeur1 :

```
Router1(config)#do wr
Building configuration...
[OK]
Router1(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 30.0.0.0 0.255.255.255
Router1(config)#access-list 100 permit ip 10.0.0.0 0.255.255.255 any
Router1(config)#ip nat inside source list 100 interface Serial 0/0/0 overload
                                                                    ^
% Invalid input detected at '^' marker.

Router1(config)#ip nat inside source list 100 interface Serial 2/0 overload
Router1(config)#do wr
Building configuration...
[OK]
Router1(config)#
```

```
)uter>enable
)uter#configure terminal
ıter configuration commands, one per line.  End with CN
)uter(config)#hostname Router1
)uter1(config)#interface Fastethernet 0/0
)uter1(config-if)#no shutdown

)uter1(config-if)#
.INK-5-CHANGED: Interface FastEthernet0/0, changed stat

.INEPROTO-5-UPDOWN: Line protocol on Interface FastEthe

)uter1(config-if)#ip address 10.0.0.254 255.0.0.0
)uter1(config-if)#ip nat inside
)uter1(config-if)#exit
)uter1(config)#interface Serial 0/0/0
                                 ^
 Invalid input detected at '^' marker.

)uter1(config)#interface Serial 0/0/0
                                 ^
 Invalid input detected at '^' marker.

)uter1(config)#interface Serial0/0/0
                                ^
 Invalid input detected at '^' marker.

)uter1(config)# interface Serial 0/0/0
                                  ^
 Invalid input detected at '^' marker.

)uter1(config)#
)uter1(config)#
)uter1(config)# interface Serial 2/0
)uter1(config-if)#no shutdown

.INK-5-CHANGED: Interface Serial2/0, changed state to d
)uter1(config-if)#ip address 101.0.0.253 255.0.0.0
)uter1(config-if)#ip nat inside
)uter1(config-if)#exit
)uter1(config)#ip route  0.0.0.0 0.0.0.0 101.0.0.254
)uter1(config)#do wr
ıilding configuration...
)K]
```

Routeur2 :

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Routeur2
Routeur2(config)#interface FastEthernet 0/0
Routeur2(config-if)#no shutdown

Routeur2(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Routeur2(config-if)#ip address 30.0.0.254 255.0.0.0
Routeur2(config-if)#ip nat inside
Routeur2(config-if)#exit
Routeur2(config)#interface Serial 2/0
Routeur2(config-if)#no shutdown

Routeur2(config-if)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

Routeur2(config-if)#ip address 102.0.0.253 255.0.0.0
Routeur2(config-if)#ip nat outside
Routeur2(config-if)#exit
Routeur2(config)#ip route 0.0.0.0 0.0.0.0 102.0.0.254
Routeur2(config)#do wr
Building configuration...
[OK]
Routeur2(config)#
```

```
Routeur2(config-if)#ip address 102.0.0.253 255.0.0.0
Routeur2(config-if)#ip nat outside
Routeur2(config-if)#exit
Routeur2(config)#ip route 0.0.0.0 0.0.0.0 102.0.0.254
Routeur2(config)#do wr
Building configuration...
[OK]
Routeur2(config)#
Routeur2(config)#access-list 100 deny ip 30.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
Routeur2(config)#access-list 100 permit ip 30.0.0.0 0.255.255.255 any
Routeur2(config)#ip nat inside source list 100 interface Serial 2/0 overload
Routeur2(config)#do wr
Building configuration...
[OK]
Routeur2(config)#
```

Routeur3 (routeur central) :

IOS Command Line Interface

```
        --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:

Press RETURN to get started!



Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Routeur2
Routeur2(config)#inter
Routeur2(config)#hostname Routeur3
Routeur3(config)#interface Serial 2/0
Routeur3(config-if)#clock rate 2000000
This command applies only to DCE interfaces
Routeur3(config-if)#no shutdown

Routeur3(config-if)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

Routeur3(config-if)#ip address 101.0.0.254 255.0.0.0
Routeur3(config-if)#exit
Routeur3(config)#interface Serial 3/0
Routeur3(config-if)#clock rate 2000000
Routeur3(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial3/0, changed state to down
Routeur3(config-if)#ip address 102.0.0.254 255.0.0.0
Routeur3(config-if)#exit
Routeur3(config)#ip route 10.0.0.0 255.0.0.0 101.0.0.253
Routeur3(config)#ip route 30.0.0.0 255.0.0.0 102.0.0.253
Routeur3(config)#do wr
Building configuration...
[OK]
Routeur3(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
```

<u>Mise en place du tunnel VPN IP sec :</u>

La configuration du tunnel VPN IP sec implique plusieurs étapes, divisées en phases.

Phase 1 (Négociation des clés) :

Configuration de l'ISAKMP avec les paramètres spécifiés

Activation de la négociation des clés et spécification de la clé pré-partagée

Routeur 1 :

```
Routeur1>enable
Routeur1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Routeur1(config)#crypto isakmp enable
Routeur1(config)#crypto isakmp policy 10
Routeur1(config-isakmp)#encryption aes
Routeur1(config-isakmp)#authentication pre-share
Routeur1(config-isakmp)#hash sha
Routeur1(config-isakmp)#group 2
Routeur1(config-isakmp)#lifetime 86400
Routeur1(config-isakmp)#exit
Routeur1(config)#crypto isakmp key CLESECRETE address 102.0.0.253
Routeur1(config)#
```

Routeur 2 :

```
Routeur2>enable
Routeur2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Routeur2(config)#crypto isakmp
% Incomplete command.
Routeur2(config)#crypto isakmp enable
Routeur2(config)#crypto isakmp policy 10
Routeur2(config-isakmp)#encryption aes
Routeur2(config-isakmp)#authentication pre-share
Routeur2(config-isakmp)#hash sha
Routeur2(config-isakmp)#group 2
Routeur2(config-isakmp)#lifetime 86400
Routeur2(config-isakmp)#exit
Routeur2(config)# crypto isakmp key CLESECRETE address 101.0.0.253
```

Phase 2 (Chiffrement des données) :

Création d'une méthode de cryptage (transform-set) spécifiant les algorithmes de cryptage et d'authentification

Création d'une liste de contrôle d'accès (Access List) pour identifier le trafic à traiter par le tunnel VPN

Déclaration d'une carte de cryptage (crypto-map) spécifiant le pair distant, le transform-set et l'access-list

Nous avons ensuite appliqué la crypto-map à l'interface WAN de chaque routeur.

Routeur 1 :

```
Routeur1(config)#crypto ipsec transform-set VPNLABO esp-aes esp-sha-hmac
Routeur1(config)#crypto ipsec security-association lifetime seconds 86400
Routeur1(config)#ip access-list extended VPN
Routeur1(config-ext-nacl)#permit ip 10.0.0.0 0.255.255.255 30.0.0.0 0.255.255.25
Routeur1(config-ext-nacl)#exit
Routeur1(config)#crypto map CARTEVPN 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Routeur1(config-crypto-map)#match address VPN
Routeur1(config-crypto-map)#set peer 102.0.0.253
Routeur1(config-crypto-map)#set transform-set  VPNLABO
Routeur1(config-crypto-map)#exit
Routeur1(config)# interface FastEthernet 0/1
Routeur1(config-if)#crypto map CARTEVPN
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Routeur1(config-if)#do wr
Building configuration...
[OK]
Routeur1(config-if)#
```

Routeur 2 :

```
Routeur2(config)# crypto ipsec transform-set VPNLABO esp-aes esp-sha-hmac
Routeur2(config)#crypto ipsec security-association lifetime seconds 86400
Routeur2(config)#ip access-list extended VPN
Routeur2(config-ext-nacl)# permit ip 30.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
Routeur2(config-ext-nacl)#exit
Routeur2(config)# crypto map CARTEVPN 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Routeur2(config-crypto-map)# match address VPN
Routeur2(config-crypto-map)#set peer 101.0.0.253
Routeur2(config-crypto-map)#set transform-set VPNLABO
Routeur2(config-crypto-map)#exit
Routeur2(config)#interface FastEthernet 0/1
Routeur2(config-if)#crypto map CARTEVPN
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Routeur2(config-if)#do wr
Building configuration...
[OK]
Routeur2(config-if)#
```

Vérification du fonctionnement du tunnel VPN :

Pour vérifier le bon fonctionnement du tunnel VPN, nous avons effectué un ping entre les stations des deux réseaux locaux. Nous avons également utilisé plusieurs commandes pour vérifier l'état et le fonctionnement du tunnel VPN :

Show crypto isakmp policy

```
Routeur1>enable
Routeur1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Routeur1#
```

Show crypto isakmp sa

```
        lifetime:               86400 seconds, no volume limit
Routeur1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status

IPv6 Crypto ISAKMP SA


Routeur1#
```

Show crypto ipsec sa

```
Routeur1#show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: CARTEVPN, local addr 101.0.0.253

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.0.0.0/255.0.0.0/0/0)
   remote  ident (addr/mask/prot/port): (30.0.0.0/255.0.0.0/0/0)
   current_peer 102.0.0.253 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #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.: 101.0.0.253, remote crypto endpt.:102.0.0.253
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0x0(0)

     inbound esp sas:

 --More--
```

Conclusion :

La mise en place réussie de ce tunnel VPN IP sec de site à site démontre la capacité à sécuriser efficacement les communications entre deux sites distants. Ce TP a permis de mieux comprendre le fonctionnement et la configuration de base des VPN IP sec sur les routeurs Cisco, ainsi que les étapes nécessaires pour établir et vérifier le bon fonctionnement d'un tunnel VPN.

Par :

Coulibaly Daouda David (IRIC1)