Reliez une succursale à l'aide d'un VPN

1 INTRODUCTION

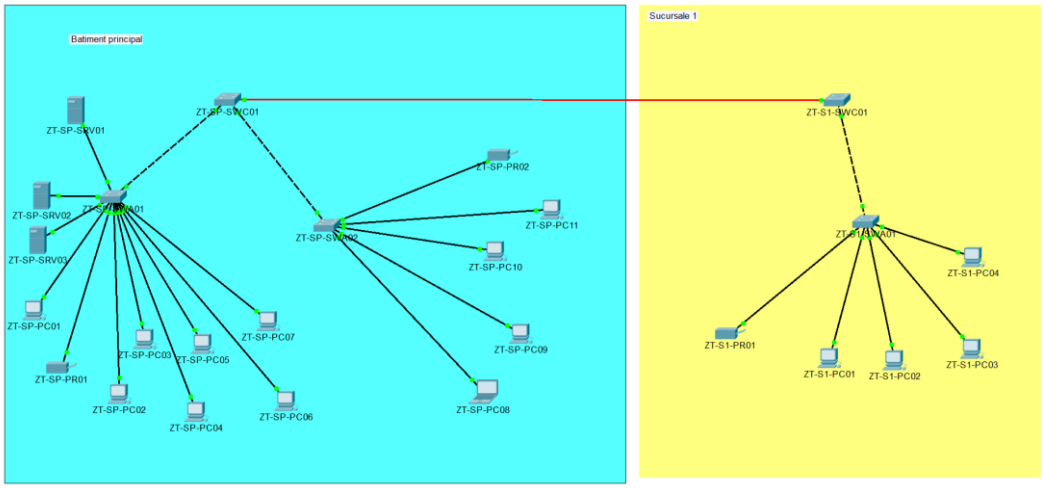
- Fichier joint : E-146-08-VPN_Site-site-LJI.pkt
- Durée estimée : 90 minutes

1.1 Objectifs

- Configuration du NAT
- Configuration route statique par défaut
- Configuration d'un serveur DHCP sur un routeur Cisco
- Configuration d'un VPN Site à Site avec IPSEC

1.2 Scénario

Au cours de cet exercice, vous allez configurer le réseau de la deuxième succursale de l'entreprise Zirtech. Dans un deuxième temps, vous allez mettre en service un tunnel VPN IPSec de site à site afin que les périphériques puissent communiquer de manière transparente.



Type	Nom	Interface	IP	Fonction
Serveur	www.google.ch	Fa0	8.8.8.8	- Serveur représentant Internet - Serveur DNS
Routeur	ZT-S2-RTR01	Gi0/0	145.10.10.2 /255.255.255.0	Routeur de la succursale 2
		Gi0/1	192.168.1.1 / 255.255.255.0	
Routeur	ZT-SP-RTR01	Gi0/0	163.25.10.2 / 255.255.255.0	Routeur de l'entreprise Zirtech
		Gi0/1	192.168.0.1/ 255.255.255.0	
PC	ZT-S2-PC01		Via DHCP	Ordinateur succursale 2

2 CREATION ET CONFIGURATION DE LA SUCCURSALE 2

- Créez le bâtiment « Succursale 2 » dans la ville Home City
- Créez une nouvelle armoire de brassage dans le bâtiment « Succursale 2 »
- Ajoutez un routeur Cisco 2911 et nommez le ZT-S2-RTR01
- Ajoutez un switch Cisco 2960 et nommez le ZT-S2-SWC01
- Ajoutez un modem câble et nommez le ZT-S2-MDM01
- Connectez la ligne coaxiale du modem avec le port Coaxial5 du nuage câbloopérateur
- Connectez l'interface Gi0/0 du routeur ZT-S2-RTR01 avec le modem ZT-S2-MDM01
- Connectez l'interface Gi0/1 du routeur ZT-S2-RTR01 avec l'interface Gi0/1 du switch ZT-S2-SWC01

2.1.1 Configuration de base du routeur ZT-S2-RTR01

- Configurez l'adresse IP public 145.10.10.2 sur l'interface G0/0
- Configurez l'adresse IP privé 192.168.1.1 sur l'interface G0/1
- Configurez la route par défaut par l'interface G0/0
- Configurez une liste de contrôle d'accès étendue pour le NAT

Attention pour la suite de l'exercice les paquets qui seront envoyés à travers le tunnel VPN ne devront pas être traduits

ZT-S2-RTR01(config)#**ip access-list extended nat**
ZT-S2-RTR01(config-ext-nacl)#**deny ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.0.255**
ZT-S2-RTR01(config-ext-nacl)#**permit ip 192.168.1.0 0.0.0.255 any**

- Configurez le NAT afin de sortir simultanément sur Internet depuis plusieurs ordinateurs en utilisant l'interface G0/0 du routeur.
- Configurez l'interfaces externe et interne

2.1.2 Configuration d'un serveur DHCP sur ZT-S2-RTR01

Pour attribuer les adresses IP aux ordinateurs de la deuxième succursale, il est nécessaire de configurer le router en tant que serveur DHCP.

- Créez un pool dhcp nommé succursale2
- Déclarez le sous-réseau 192.168.1.0 255.255.255.0
- Déclarez l'adresse IP de la passerelle de votre réseau
- Déclarez l'adresse IP du serveur DNS
- Pour terminer la configuration du DHCP, il faut exclure les dix premières adresses de la plage

ZT-S2-RTR01(config)#**ip dhcp pool *succursale2***
ZT-S2-RTR01(dhcp-config)#**network *192.168.1.0 255.255.255.0***
ZT-S2-RTR01(dhcp-config)#**default-router *192.168.1.1***
ZT-S2-RTR01(dhcp-config)#**dns-server 8.8.8.8**
ZT-S2-RTR01(dhcp-config)#**exit**
*ZT-S2-RTR01(config)#***ip dhcp excluded-address 192.168.1.1 192.168.1.10**

2.1.3 Test du réseau local de la succursale 2

Avant de passer à la configuration du tunnel VPN, il est nécessaire de valider le bon fonctionnement du réseau dans la succursale 2

- Ajoutez un ordinateur et nommez le ZT-S2-PC01
- Connectez-le au port fa0/1 du switch ZT-S2-SWC01
- Enumérez ci-dessous les tests que vous effectueriez pour valider le bon fonctionnement du réseau de la succursale 2

_____

_____

_____

_____

_____

_____

2.2 Modification de la configuration de ZT-SP-RTR-01

Etant fortement déconseillé de configurer un VPN sur une adresse IP dynamique. Changez l'adresse IP de G0/0 sur ZT-SP-RTR01 en 163.25.10.2

Tout comme sur le routeur de la succursale 2, vous devez ici corriger la configuration originale du NAT :

- Créez une liste de contrôle étendue nommée **nat** avec les options suivantes :
    - Refus de tous les paquets IP du sous-réseau 192.168.0.0 à destination du sous-réseau 192.168.1.0
    - Autorisation de tous les paquets IP du sous-réseau 192.168.0.0 à destination de tous les autres réseaux

```
ZT-SP-RTR01(config)#ip access-list extended nat
ZT-SP-RTR01(config-ext-nacl)#deny ip 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255
ZT-SP-RTR01(config-ext-nacl)#permit ip 192.168.0.0 0.0.0.255 any
```

2.2.1 Test de la connectivité

Avant de configurer le VPN, envoyez un ping à partir de ZT-SP-RTR01 vers l'adresse IP de ZT-S2-RTR01 et inversement. En cas d'échec vérifiez les points précédents de votre configuration

3 CONFIGURATION DU TUNNEL VPN SITE A SITE AVEC IPSEC

3.1 Activez le module securityk9

La licence du pack technologique de sécurité doit être activée pour pouvoir effectuer cet exercice.
Exécutez la commande ***show version*** en mode d'exécution utilisateur ou en mode d'exécution privilégié pour vérifier que la licence du pack technologique de sécurité est activée.

```
-----------------------------------------------------------------
Technology Technology-package Technology-package
           Current            Type            Next reboot
-----------------------------------------------------------------
ipbase     ipbasek9           Permanent       ipbasek9
security   securityk9         Evaluation      securityk9
uc         None               None            None
```

Si ce n'est pas le cas (par ex. *security None None None*), activez le module securityk9 pour le prochain démarrage du routeur, acceptez la licence, enregistrez la configuration et redémarrez.

```
ZT-S2-RTR01(config)#license boot module c2900 technology-package securityk9
Acceptez la licence : ACCEPT? [yes/no] yes
ZT-S2-RTR01(config)#end
ZT-S2-RTR01#copy running-config startup-config
ZT-S2-RTR01#reload
```

- Répétez les étapes du point 3.1 sur ZT-SP-RTR01

Remarque :
Si l'activation du module securityk9 ne fonctionne pas, une des trois étapes ci-dessous devrait résoudre votre problème :

1. Vérifiez que vous avez sélectionné le bon modèle de routeur CISCO **2911**
2. Éteignez le routeur, attendez 10 secondes et allumez-le
3. Dans quelques rares cas, désinstallez **Packet Tracer** et réinstallez-le.
4. Déplacez le fichier pkt en local (par ex. sur le disque C:) pour activer la licence.

3.2 Identifiez le trafic devant traverser le tunnel

Pour débuter, il faut définir le trafic IP qui devra être envoyé à travers le tunnel. Dans notre cas, il y a deux catégories de trafic intéressant :

- Le trafic IP de la succursale 2 à destination du siège principal
- Le trafic IP du siège principal à destination de la succursale 2

```
ZT-SP-RTR01(config)#access-list 110 permit ip 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255
ZT-S2-RTR01(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.0.255
```

3.2.1 Configurez les propriétés de la phase 1 du tunnel IPSec

Durant la première phase, il y a un établissement d'une session ISAKMP entre les deux routeurs. C'est dans cet phase que sont négociés les protocoles de chiffrement (aes) et de hachage (sha) ainsi que la clé partagée pour l'authentification (cisco dans notre exemple). Il est également nécessaire de définir l'adresse IP du routeur homologue.

```
ZT-SP-RTR01(config)#crypto isakmp policy 10
ZT-SP-RTR01(config-isakmp)#encryption aes
ZT-SP-RTR01(config-isakmp)#authentication pre-share
ZT-SP-RTR01(config-isakmp)#group 2
ZT-SP-RTR01(config-isakmp)#exit
ZT-SP-RTR01(config)#crypto isakmp key cisco address 145.10.10.2

ZT-S2-RTR01(config)#crypto isakmp policy 10
ZT-S2-RTR01(config-isakmp)#encryption aes
ZT-S2-RTR01(config-isakmp)#authentication pre-share
ZT-S2-RTR01(config-isakmp)#group 2
ZT-S2-RTR01(config-isakmp)#exit
ZT-S2-RTR01(config)#crypto isakmp key cisco address 163.25.10.2
```

3.2.2 Configurez les propriétés de la phase 2 du tunnel IPSec sur ZT-SP-RTR01

Durant la deuxième étape, il faut créer un jeu de transformation (transform-set), nommé VPN-SET dans notre exemple. Il définit l'algorithme de cryptage ESP-3DES et l'algorithme de hachage ESP-SHA-HMAC. Ensuite il faut créer une crypto-map (VPN-MAP) qui établit le lien avec les paramètres ISAKMP de phase 1. Pour terminer, il faut appliquer la crypto map sur l'interface de sortie des routeurs

```
ZT-SP-RTR01(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
ZT-SP-RTR01(config)# crypto map VPN-MAP 10 ipsec-isakmp
ZT-SP-RTR01(config-crypto-map)#set peer 145.10.10.2
ZT-SP-RTR01(config-crypto-map)#set transform-set VPN-SET
ZT-SP-RTR01(config-crypto-map)#match address 110
ZT-SP-RTR01(config-crypto-map)#exit
ZT-SP-RTR01(config)#int G0/0
ZT-SP-RTR01(config-if)#crypto map VPN-MAP
ZT-SP-RTR01(config-if)#exit

ZT-S2-RTR01(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
ZT-S2-RTR01(config)#crypto map VPN-MAP 10 ipsec-isakmp
ZT-S2-RTR01(config-crypto-map)#set peer 163.25.10.2
ZT-S2-RTR01(config-crypto-map)#set transform-set VPN-SET
ZT-S2-RTR01(config-crypto-map)#match address 110
ZT-S2-RTR01(config-crypto-map)#exit
ZT-S2-RTR01(config)#int G0/0
ZT-S2-RTR01(config-if)#crypto map VPN-MAP
ZT-S2-RTR01(config-if)#exit
```

4 TEST DE VOTRE CONFIGURATION

Vous devez pouvoir atteindre à l'aide d'un ping l'ensemble des ordinateurs du sous-réseaux 192.168.0.0 depuis le sous-réseaux 192.168.1.0 et vice-versa.

- Exécutez un ping depuis ZT-SP-PC01 vers ZT-S2-PC01.

Il est probable que les premiers pings soient perdus