…….

DIC2-M1GLS-INFO

TPN°3: Configuration et Vérification de VPN IPsec Site-à-Site en ligne de commande

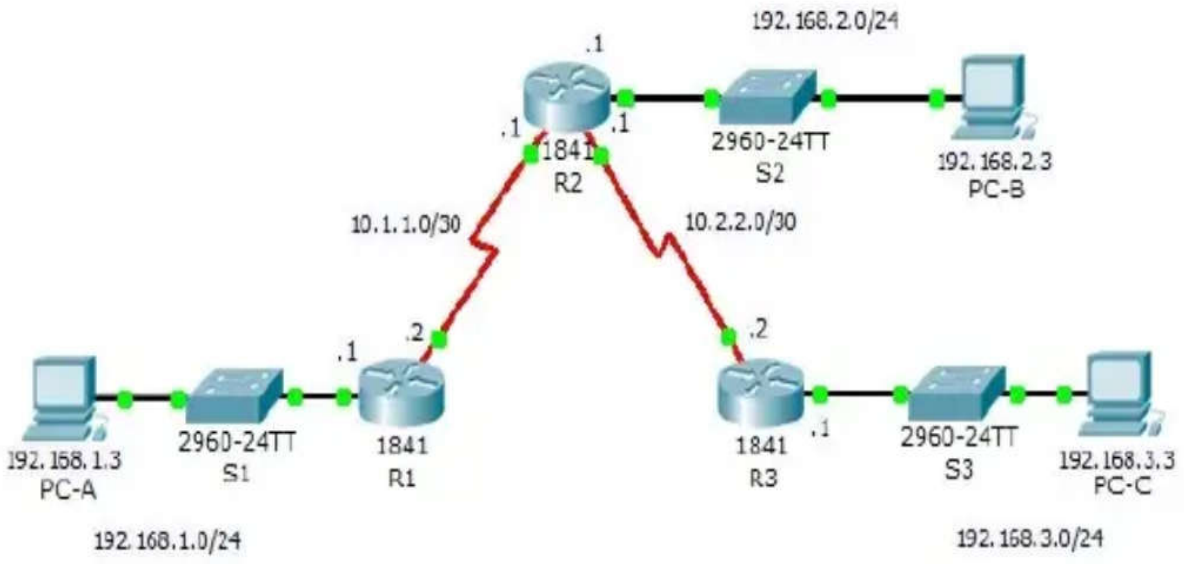
Objectifs du Travail

- Vérifier la connectivité à travers le réseau.
- Configurer le routeur R1 pour supporter le VPN IPsec site-à-site avec R3.

Introduction

La topologie réseau présente trois routeurs. Votre travail est de configurer les routeurs R1 et R3 pour supporter le VPN IPsec site à site quand le trafic traverse leur LANs respectifs. Le tunnel VPN est entre le routeur R1 et R3 via R2. R2 agit comme un passe-travers et n'a aucune connaissance du VPN. IPsec fourni une transmission sécurisée pour les informations sensible sur des réseaux non protégés comme Internet.

Topologie



NB : Les routeurs sont préconfigurés

Table d'adressage

Equipement	Interface	Adresse IP	Masque Sous-reseau
R1	Fa0/0	192.168.1.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
R2	S0/0/0	10.1.1.1	255.255.255.252
	Fa0/0	192.168.2.1	255.255.255.0
	S0/0/1	10.2.2.1	255.255.255.252
R3	S0/0/1	10.2.2.2	255.255.255.252
	Fa0/0	192.168.3.1	255.255.255.0
PC-A	NIC	192.168.1.3	255.255.255.0
PC-B	NIC	192.168.2.3	255.255.255.0
PC-C	NIC	192.168.3.3	255.255.255.0

ISAKMP Phase 1 Paramètres Policy

Paramètres		**R1**	**R3**
Méthode de distribution de clef	Manuelle ou ISAKMP	ISAKMP	ISAKMP
Algorithme de cryptage	DES, 3DES, or AES	AES	AES
Algorithme de hashage	MD5 or SHA-1	SHA-1	SHA-1
Méthode d'authentification	Clefs partagées (pre-share ou Rsa)	Pre-share	Pre-share
Echange de clefs	DH group 1,2 ou 5	DH 2	DH2
Durée de vie d'IKE SA (lifetime)	86400 second ou moins	86400	86400
Clefs ISAKMP		Vpnpa55	Vpnpa55

IPsec Phase 2 Paramètres Policy

paramètres	R1	R3
Transform set	VPN-SET	VPN-SET
Peer Host Name	R3	R1
Peer IP Address	10.2.2.2	10.1.1.2
Réseau qui sera crypté	192.168.1.0/24	192.168.3.0/24
Nom du crypto MAP	VPN-MAP	VPN-MAP
Etablissement du SA	IPsec-ISAKMP	IPsec-ISAKMP

Activité 1: Configuration des paramètres IPsec sur R1

Etape 1. Test de connectivité.
Ping de PC-A à PC-C.

Etape 2. Identifier le trafic intéressant vpn sur R1.

Configurer un ACL 110 pour identifier le trafic du LAN sur le R1 vers R3 comme trafic VPN. Ce trafic va déclencher le VPN IPSec qui sera implémenté à chaque fois que le trafic passe entre les LANs de R1 et R3. Tous les autres trafics ne seront pas cryptés. Souvenez-vous du fait qu'il y un deny all implicite, il n'y aura pas besoin de configurer un deny any any.

R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192. 168.3.0 0.0.0.255

Etape 3. Configurer les propriétés d'ISAKMP Phase 1 sur R1.

Configurer les propriétés du crypto ISAKMP policy 10 sur R1 avec la clef partagée (shared crypto key) vpnpa55. Referez-vous de ISAKMP Phase 1 dans le tableau pour les paramètres spécifiques à configure. Les valeurs par défaut ne devront plus être configures cependant seulement le cryptage,la méthode d'échange de clef, la méthode DH doivent être configurées.

R1(config)#crypto isakmp enable
R1(config)#crypto isakmp policy 10
R1(config -isakmp)#encryption aes
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 vpnpa55 address 10.2. 2.2

Etape 4. Configurer les propriétés d'ISAKMP Phase 2 sur R1.

Créer le transform-set VPN-SET pour utiliser esp-3des et esp-sha-hmac. Par la suite on crée le crypto map VPN-MAP qui va lier tous les paramètres de la Phase 2 ensemble. Utiliser la séquence de nombre 10 et identifier ça comme un map ipsec-isakmp.

R1(config)# crypto ipsec transform -set VPN-SET esp-3des esp-sha-hmac
R1(cfg -crypto -trans)#exit
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config -crypto -map)# set peer 10. 2.2.2
R1(config -crypto -map)# set transform -set VPN-SET
R1(config -crypto -map)# set security -association lifetime second 43200
R1(config -crypto -map)# match address 110

R1(config -crypto -map)# EXIT

Etape 5. Configurer le crypto map sur l'interface sortante.

Enfin, liez le crypto map VPN-MAP sur l'interface sortante Serial 0/0/0.

R1 (config)# interface S0/0/0
R1(config-if)# crypto map VPN-MAP

Activité 2: Configure IPsec Paramètres sur R3

Etape 1 : configurer le routeur R3 pour supporter le VPN site to site avec R1, maintenant configurer les paramètres inverses sur R3, configurer l'ACL 110 pour identifier le trafic intéressant du LAN vers R1.

R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192. 168.1.0 0.0.0.255

Etape 2: configure les paramètres ISAKMP phase 1 sur le routeur R3
Configurer les propriétés crypto ISAKMP policy 10 sur R3 avec la clef partagée (shared crypto key) vpnpa55

R3(config)#crypto isakmp enable
R3(config)#crypto isakmp policy 10
R3(config -isakmp)#encryption aes
R3(config -isakmp)#hash sha
R3(config -isakmp)#authentication pre-share
R3(config -isakmp)#group 2
R3(config -isakmp)#lifetime 86400
R3(config -isakmp)#exit
R3(config)# crypto isakmp key vpnpa55 address 10.1. 1.2

Etape 3. Configurer les propriétés d'ISAKMP Phase 2 sur R3.
Comme vous l'aviez fait sur R1, crée le transform-set VPN-SET pour utiliser esp-3des et esp-sha-hmac. Par la suite on crée le crypto map VPN-MAP qui va lier tous les paramètres de la Phase 2 ensemble. Utiliser la séquence de nombre 10 et identifier ça comme un map ipsec-isakmp.
R3(config)# crypto ipsec transform -set VPN-SET esp-3des esp-sha-hmac
R3(cfg -crypto -trans)#exit
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
R3(config -crypto -map)# set peer 10. 1.1.2
R(config -crypto -map)# set transform -set VPN-SET
R3(config -crypto -map)# set security -association lifetime second 43200
R3(config -crypto -map)# match address 110
R3(config -crypto -map)# EXIT
Etape 4. Configurer le crypto map sur l'interface sortante.
Enfin, liez le crypto map VPN-MAP sur l'interface sortante Serial 0/0/1.
R3(config)# interface S0/0/1
R3(config-if)# crypto map VPN-MAP

Activité 3: Vérification du VPN IPsec

Etape 1. Vérifier le tunnel un peu avant le Traffic intéressant.
Tapez la commande show crypto ipsec sa sur R1.
Notez que le nombre de paquets encapsulés, cryptés, désencapsulés et décryptés est à 0.
Etape 2. Créer le trafic intéressant.
Du PC-A, Ping PC-C.