Lab – mise en œuvre d'une communication inter-sites avec le protocole DMVPN

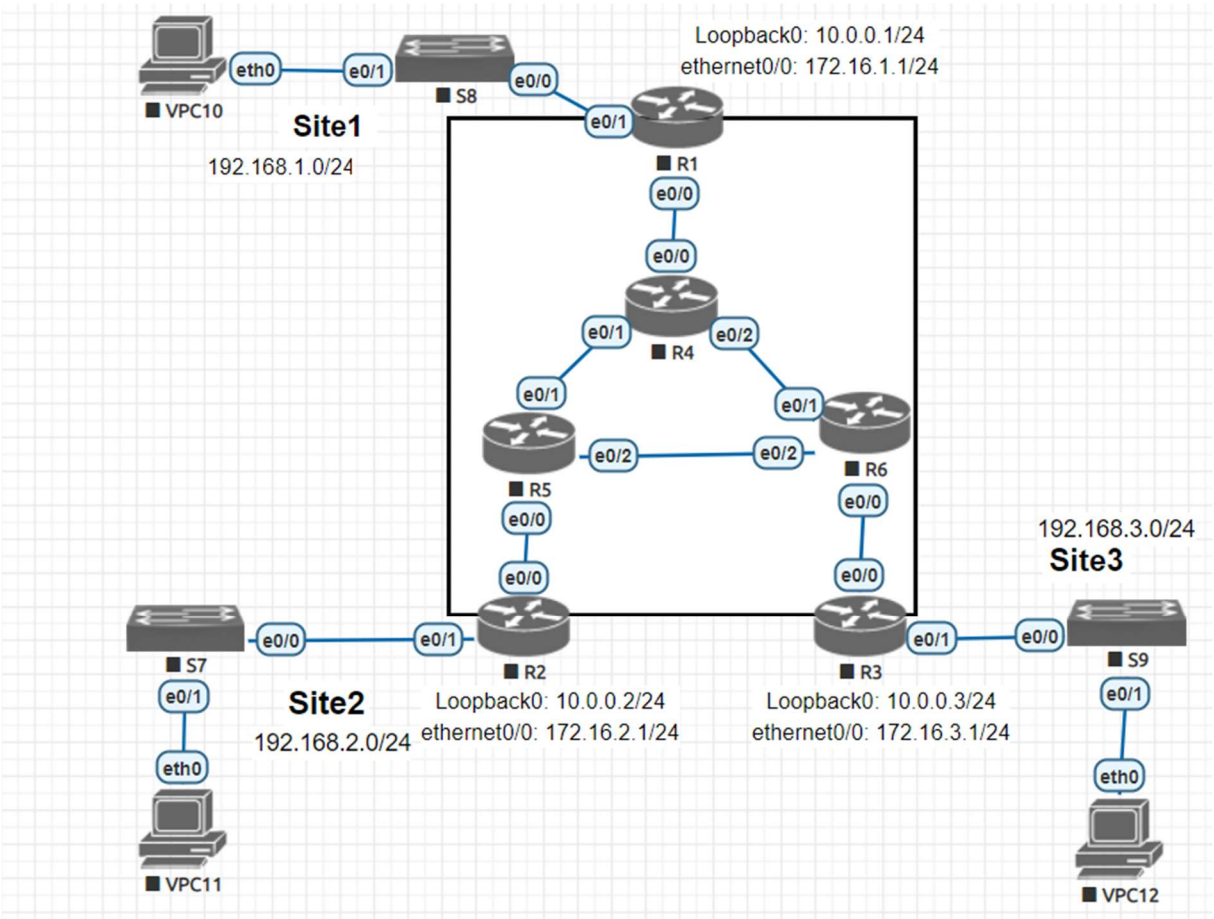
Objectif :

Le but de ce TP est de vous familiariser avec le protocole DMVPN et les mécanismes de tunneling pour mettre en œuvre une communication inter-sites et sa sécurité

Topologie

Vous avez Trois sites distants interconnectés par votre FAI. Les sites sont identifiés par des réseaux privés 192.168.x.0/24, où « x » désigne le numéro du site.

Le réseau FAI utilise une adresse réseau IP 88.1.xx.0/24. Le routeur du Site1 joue le rôle du HUB et les autres SPOKE. Les adresses IP des Tunnels utilisent le réseau IP 172.16.x.0/24



Travail effectué :

- Complétez la configuration des interfaces des routeurs
- Vous utilisez deux protocoles de routage : ospf pour le réseau adjacent (underlying) et RIP version 2 appliqué au réseau overlay et le réseau LAN
- Activez le routage ospf en ajoutant que les routes externes

- Affichez la table de routage de R1, R2 et R3 : assurez-vous que toutes les routes figurent dans chaque table de routage
- Testez la connectivité entre le Hub et les autres Spoke
- Configurez le Routeur R1 comme routeur Hub : l'adresse du tunnel DMVPN est 10.0.0.x/24
- Configurez les routeurs R2 et R3 pour jouer le rôle de Spoke, l'adresse du tunnel doit être dans la plage du tunnel configuré du routeur Hub (10.0.0.xx/24)
- De côté du routeur Hub afficher le résultat du « show ip nhrp » et vérifiez que toutes les adresses des tunnels sont bien mappées
- Vérifiez pour les autres routeurs Spoke
- Avec la commande « show dmvpn » visualisez l'état des peers VPN
- Routage Overlay, le but est de router les adresses privées dans les tunnels GRE. Dans les routeurs Hub et les deux Spoke, activez le routage RIP en ajoutant l'adresse du réseau LAN et celle du tunnel.
- N'oubliez pas d'ajouter aux interfaces tunnels « no ip split-horizon »
- Affichez la table de routage rip de chaque routeur « show ip route rip » et vérifiez les réseaux appris
- Depuis les machines de chaque réseau LAN, effectue des tests de communications entre les sites
- Une fois le test de connectivité entre le site2 et site3 est effectué, vérifiez la table dmvpn avec la commande « show dmvpn » sur les routeurs Spoke
- Depuis la machine du site2 affichez le chemin emprunté pour atteindre la machine du Site3, qu'observez-vous ?
- Une fois la communication entre les sites est réussie, vous devez sécurisez les tunnels mGRE avec du IPsec
- Appliquez la politique d'IPsec le mot de passe utlisé est « cesi20xx » où « xx » représente l'année en cours
- Pour vérifier si les tunnels sont fonctionnels, effectuez une communication entre le site 1 et le site2, ensuite entre le site1 et site3
- Vérifiez avec la commande « show crypto iskamp sa » si l'association est activée
- Pour plus de détail utilisez la commande 'show crypto ipsec sa »