TD – ACL VPN ROUTAGE

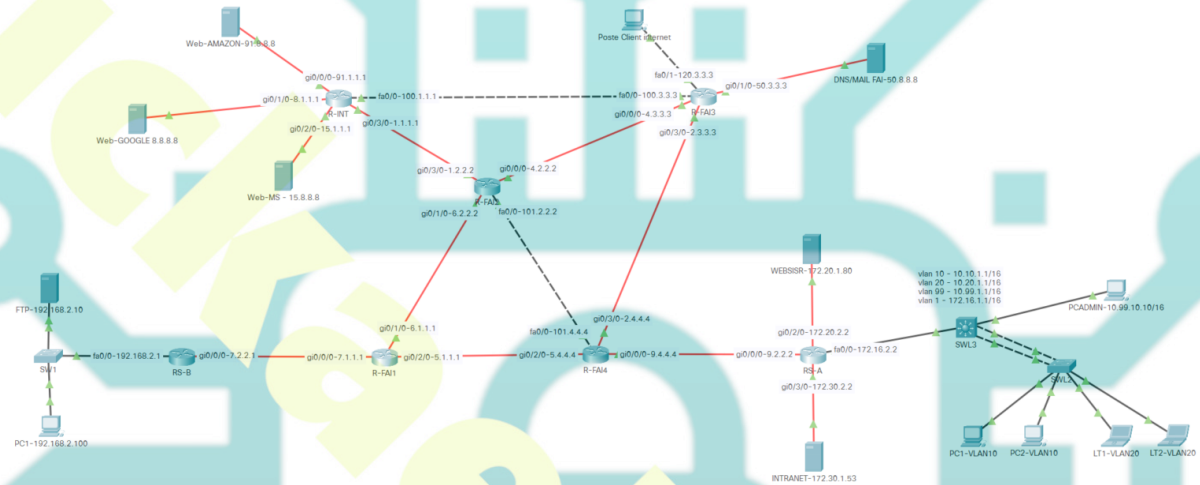

Schéma du TP

Consignes

- Les serveurs et le PC admin ont une adresse fixe
- Les clients des vlan sont clients DHCP
- Vous devez configurer le serveur DNS avec les différents enregistrements A pour tous les serveurs www
- Vous devez activer le mail sur le serveur et activer 3 boites aux lettres (PC Admin, PC1 du site 2 et PC1-VLAN10
- Un VPN permettra la communication entre le PC Admin du site et le serveur FTP du site B

- Le protocole OSPF sera utilisé pour la mise en place des routes
- L'accès des sites A et B à internet se fait via le NAT selon des restrictions protocolaires
- Des règles de sécurité seront mises en œuvre
- Les serveurs de la DMZ du site A seront accessibles depuis internet avec restrictions protocolaires

Réglages du R-INT

- Affecter les adresses IP
- Nommer le routeurs
- Indiquer la passerelle par défaut vers le routeur R-FAI2

Réglages des routeurs F-FAIx

- Affecter les adresses IP
- Nommer le routeurs
- Activer le protocole OSPF
- Sur le routeur R-FAI2 indiquer une route par défaut vers R-INT et redistribuer la route aux autres routeurs via OSPF

Réglages de base du routeur RS-B

- Affecter les adresses IP
- Nommer le routeurs
- Déclarer le nom de domaine **sisr.net**
- Activer le protocole OSPF uniquement sur le réseau WAN
- Activer le NAT sur les interfaces
- Activer SSH en indiquant un utilisateur **Admin** et un mot de passe **Pa$$**

Mise en place des ACL NAT RS-B

- Création d'une ACL étendue nommée NAT-VPN
- On interdit au FTP de passer par le NAT lors de l'accès vers le PC ADMIN
- On permet au LAN de passer par le NAT avec les protocoles http, https, smtp, pop et dns uniquement
- Création d'une ACL étendue nommée NAT-VPN

- On interdit au PC ADMIN de passer par le NAT lors de l'accès vers le FTP
- On autorise tous les protocoles pour le PC Admin dans le NAT
- On permet aux VLAN de passer par le NAT avec les protocoles http, https, smtp, pop et dns uniquement
- On affecte le NAT sur l'interface WAN en overload

Mise en place du vpn ipsec

- Chiffrement **AES**
- Hachage **SHA**
- Diffie Ellman **group 2**
- Authentification clé partagée (**Pa$$**)

Configuration de la négociation des clés (phase 1)

- Création d'un set nommé **VPNSISR**
- Création d'un ACL étendue nommée **VPN** permettant la communication entre le réseau 192.168.0.0 et le réseau 10.0.0.0

Configuration de la méthode de chiffrage des données (phase 2)

- Créer une crypto map nommée **CARTEVPN**
- Affecter la crypto map à l'interface wan

Réglages de base du routeur RS-A

- Affecter les adresses IP
- Nommer le routeurs
- Déclarer le nom de domaine **sisr.net**
- Activer le protocole OSPF uniquement sur le réseau WAN
- Créer des routes statiques
- Activer le NAT sur les interfaces
- Activer SSH en indiquant un utilisateur **Admin** et un mot de passe **Pa$$**
- Mise en œuvre une ACL SSH avec autorisation uniquement pour le PC ADMIN

Mise en place des ACL NAT RS-A

- Création d'une ACL étendue nommée NAT-VPN
- On interdit au PC ADMIN de passer par le NAT lors de l'accès vers le FTP
- On autorise tous les protocoles pour le PC Admin dans le NAT
- On permet aux VLAN de passer par le NAT avec les protocoles http, https, smtp, pop et dns uniquement
- On affecte le NAT sur l'interface WAN en overload
- Mettre en place une redirection (NAT inversé) vers la DMZ intranet en https et web en http

Mise en place du vpn ipsec

- Chiffrement **AES**
- Hachage **SHA**
- Diffie Ellman **group 2**
- Authentification clé partagée (**Pa$$**)

Configuration de la négociation des clés (phase 1)

- Création d'un set nommé **VPNSISR**
- Création d'un ACL étendue nommée **VPN** permettant la communication entre le réseau 10.0.0.0 et le réseau 192.168.0.0

Configuration de la méthode de chiffrage des données (phase 2)

- Créer une crypto map nommée **CARTEVPN**
- Affecter la crypto map à l'interface wan

Configuration du switch SWLV3

- Nommer le switch
- Déclarer le nom de domaine **sisr.net**
- Créer les vlan 10, 20 et 99
- Nommer les vlan
- Affecter le port fa0/19 au vlan 99
- affecter les adresses IP aux vlan

- Créer les routes nécessaires
- Configurer le **LACP** en trunk sur les ports Gi0/1 et Gi0/2
- Créer les 2 pools **DHCP** pour les vlan 10 et 20
- Activer **SSH** en indiquant un utilisateur **Admin** et un mot de passe **Pa$$**
- Mise en œuvre une ACL SSH avec autorisation uniquement pour le PC ADMIN
- Mettre en œuvre des **ACL** intervlan 10 vers 20 pour qu'ils ne communiquent pas

Configuration du switch SWLV2

- Nommer le switch
- Déclarer le nom de domaine **sisr.net**
- Créer les vlan 10, 20 et 99
- Nommer les vlan
- Affecter le port fa0/1 à 9 au vlan 10 et fa0/10 à 20 pour le vlan 20
- affecter une adresses IP au vlan 99
- Configurer le **LACP** en trunk sur les ports Gi0/1 et Gi0/2
- Activer **SSH** en indiquant un utilisateur **Admin** et un mot de passe **Pa$$**
- Mise en œuvre une ACL SSH avec autorisation uniquement pour le PC ADMIN