La Rochelle Université

Réseaux & Télécoms

Portfolio

SAE3.03 - Concevoir un réseau informatique sécurisé multi-sites

I - Observation et description

a) Objectif d'apprentissage de la SAE

L'objectif principal de la SAÉ 3.ROM.03 était de concevoir et d'administrer un réseau multimédia adapté aux besoins spécifiques d'une entreprise multi-sites. Cet apprentissage visait à renforcer mes compétences techniques en intégrant des technologies avancées comme la QoS, les VPN IPsec, et la téléphonie IP tout en respectant les contraintes d'un environnement professionnel.

b) Contextualisation

Cette SAÉ a été réalisée dans le cadre de ma formation Réseaux et Télécommunications. L'objectif était d'adapter une infrastructure réseau multi-sites pour supporter des services multimédias tout en garantissant une sécurité et une qualité de service (QoS) optimales. Le projet impliquait une approche méthodique pour analyser les besoins, concevoir une solution technique, la déployer, et valider ses performances.

c) Présentation de la trace et de la compétence

La trace choisie pour cette partie du portfolio est la configuration du VPN IPsec sur le routeur R-A1. Cette configuration reflète ma capacité à concevoir et sécuriser des communications inter-sites en utilisant des technologies de cryptographie avancées. Elle met en évidence la compétence de gestion des infrastructures réseaux d'opérateurs (AC21.01) et la mise en œuvre de politiques de sécurité réseau (AC21.02).

Détails de la configuration VPN IPsec sur le routeur R-A1

```
en
conf t
license boot module c2900 technology-package securityk9
yes
end
copy run start

crypto isakmp policy 1
hash sha
encryption aes 256
authentication pre-share
group 5
lifetime 3600

crypto isakmp key la_clef address 69.1.24.1

        !ACL_map
```

```
access-list 101 permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255


        !suite_IP_Sec
crypto ipsec transform-set 1_LR_LY esp-aes esp-sha-hmac

        !crypto_Map
crypto map LR-LY_1_map 10 ipsec-isakmp
match address 101
set transform-set 1_LR_LY
set peer 69.1.24.1
set pfs group5
set security-association lifetime seconds 900

int G0/0/0
crypto map LR-LY_1_map
```

Analyse de la configuration

Cette configuration met en place une politique ISAKMP (Internet Security Association and Key Management Protocol) pour négocier et établir des connexions sécurisées entre deux sites. Les éléments clés incluent :

- **Algorithmes cryptographiques sécurisés :** SHA pour le hachage et AES-256 pour le chiffrement.
- **Authentification pré-partagée :** Une clé partagée entre les deux sites pour garantir une communication sécurisée.
- **ACL (Access Control List) :** Définition des flux autorisés dans le tunnel VPN.
- Transform-set IPsec : Application des mécanismes de chiffrement et d'authentification pour les paquets.
- **Mapping VPN sur l'interface :** Association de la configuration VPN à l'interface réseau concernée (G0/0/0).

d) Compétence du référentiel travaillée

Les compétences travaillées dans cette SAÉ incluent :

- La configuration et le dépannage de réseaux complexes (AC21.01).
- La mise en œuvre de la QoS et des politiques de sécurité réseau (AC21.02).
- L'administration de services multimédias avancés, notamment la téléphonie IP multi-sites (AC25.01ROM).

e) Lien entre la trace et la compétence du référentiel

La trace illustre la mise en œuvre d'un VPN IPsec pour interconnecter deux sites distants de manière sécurisée. Cette réalisation montre ma maîtrise des outils de configuration réseau et de la sécurisation des échanges, tout en reflétant la compréhension des exigences liées à la QoS pour les flux multimédias.

II - Analyse et auto-évaluation

a) Connaissances et enseignements mobilisés

Cette SAÉ m'a permis de mobiliser des connaissances fondamentales sur les protocoles réseau (OSPF, IPsec), les mécanismes de QoS (classification, marquage, gestion de la bande passante), et les technologies multimédias (téléphonie IP, vidéoconférence). J'ai également renforcé mes compétences en configuration d'équipements réseau (routeurs et commutateurs Cisco).

b) Points sur l'apprentissage

1. **Qu'ai-je appris ?**
   J'ai appris à concevoir une architecture réseau adaptée à des besoins précis tout en tenant compte des contraintes techniques et organisationnelles. J'ai également approfondi mes compétences dans la mise en œuvre de politiques de QoS et la sécurisation des communications via des VPN.

2. **Leçons tirées et compétences développées**
   J'ai appris à équilibrer performance, sécurité, et simplicité dans le cadre d'un projet réseau. Les compétences développées incluent la gestion des priorités, la résolution de problèmes en temps réel, et la rédaction d'une documentation technique.

3. **Aspects les plus formateurs**
   La configuration des VPN et la gestion de la QoS ont été particulièrement formatrices, car elles nécessitent une compréhension fine des mécanismes sous-jacents et une attention aux détails lors de la mise en œuvre.

c) Difficultés rencontrées et solutions

1. **Difficultés rencontrées**
   L'un des principaux défis était de garantir une QoS optimale pour les flux vidéo tout en limitant l'impact sur d'autres types de trafic réseau. Une autre difficulté concernait le diagnostic des problèmes de connectivité liés à la configuration initiale des VPN.

2. **Solutions mises en œuvre**
   Pour la QoS, j'ai utilisé une approche basée sur des classes de trafic et des politiques de priorisation. Pour les VPN, une analyse approfondie des journaux des routeurs et des captures de trames a permis d'identifier et de corriger des erreurs de configuration.

3. **Ressenti sur la tâche**
   J'ai apprécié le caractère concret et pratique du projet, bien qu'il ait parfois été frustrant de résoudre des problèmes complexes. Toutefois, ces défis ont renforcé ma

satisfaction personnelle une fois les obstacles surmontés.

d) Perspectives

1. **Réutilisation des compétences**
   Ces compétences sont directement transférables dans des contextes professionnels, comme la conception de réseaux d'entreprise ou la sécurisation des communications pour des sites distants.

2. **Ce que j'aurais pu faire différemment**
   J'aurais pu planifier davantage de temps pour les tests intermédiaires afin de repérer les problèmes en amont, réduisant ainsi les délais liés à la résolution en phase finale.

3. **Autres approches possibles**
   Une approche alternative aurait consisté à virtualiser certains équipements pour accélérer les tests et ajustements, tout en réduisant les coûts matériels.

4. **Approche pour une situation similaire**
   À l'avenir, je commencerais par établir un protocole de tests systématique pour vérifier chaque composant avant de passer à la phase suivante.

III - Plan d’action

1. Renforcer mes compétences en virtualisation pour accélérer les tests et réduire les coûts.
2. M’inscrire à une formation ou réaliser des certifications sur les technologies de QoS avancées et les VPN.
3. Participer à des projets collaboratifs pour continuer à développer mes compétences transversales, comme la communication technique et la gestion de projet.
4. Utiliser davantage d’outils d’automatisation pour gagner en efficacité dans les déploiements futurs.