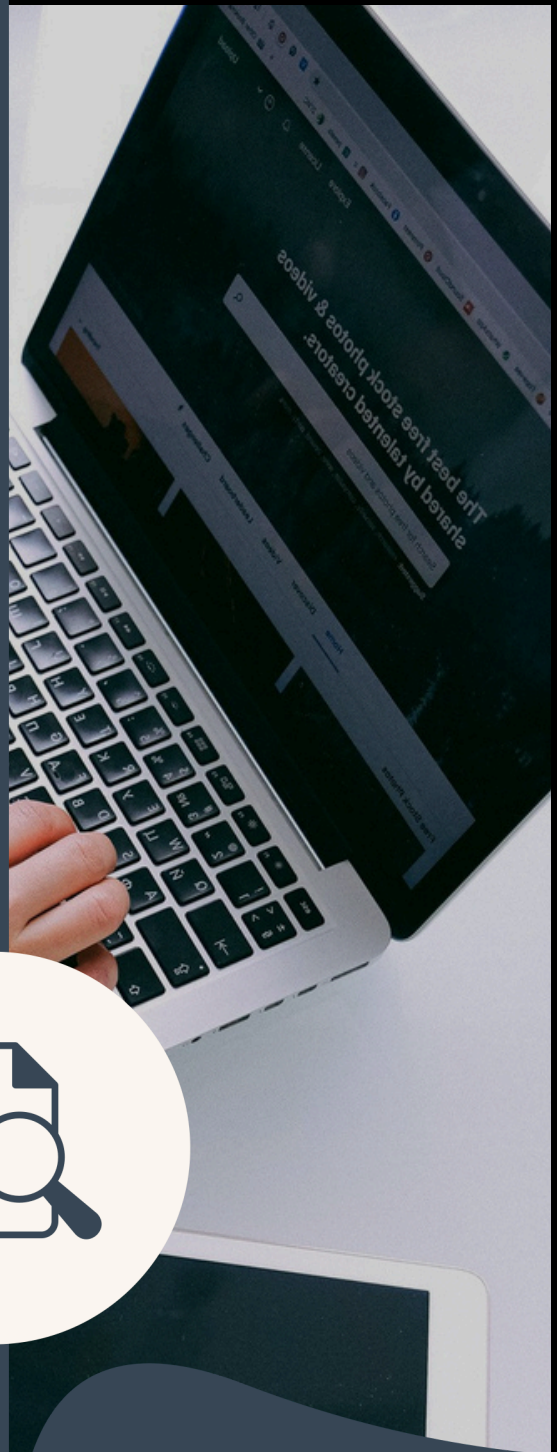


Rapport SAE 03

Concevoir un réseau
informatique multi-sites



SOMMAIRE

INTRODUCTIONP2

CAHIER DES CHARGESP3-4

PRÉSENTATION DE LA MAQUETTE.....P5

PROTOCOLE UTILISÉS.....P6-13

CONCLUSION.....P14

La **SAE**, ou **situation d'apprentissage** et **d'évaluation**, regroupe plusieurs tâches que les étudiants réalisent dans le but d'atteindre un objectif précis. Elle offre aux élèves l'opportunité de développer et d'exercer des compétences essentielles pour valider leur parcours universitaire. Inspirée de situations concrètes issues du monde professionnel, la SAE permet également aux enseignants d'évaluer l'évolution des compétences des étudiants tout en les accompagnant dans leur progression.



Voilà les consignes demandé dans cette SAE :

Objectifs et problématique professionnelle :

L'objectif pour le groupe est de concevoir et déployer une infrastructure multi-sites sécurisée, tout en justifiant les choix techniques réalisés à partir d'un cahier des charges précisant les besoins réseau de l'entreprise.

Une attention particulière doit être accordée aux vulnérabilités potentielles et connues des équipements réseau et du système d'information mis en place. Le réseau doit également évoluer de manière régulière pour garantir l'accès sécurisé des différents sites aux services et ressources de l'entreprise, tout en assurant une qualité optimale des services multimédias tels que la téléphonie IP et la vidéosurveillance.

La consigne précise que nous devons commencer par élaborer un cahier des charges détaillant les besoins spécifiques d'une entreprise en matière de réseau.

Voici le cahier des charges que nous avons écrit, nous simulons une entreprise nommé NetConnect Solutions:

Notre entreprise NetConnect Solutions est déployée sur 3 sites géolocalisés dans les 3 villes suivantes : Paris, Lyon, Marseille.

Les 3 sites contiennent des informations plus ou moins importantes. C'est pour cette raison que nous souhaiterions renforcer la sécurité de ces bâtiments

Au total, chaque bâtiment comprend un effectif de 1000 salariés, 500 terminaux et 4 serveurs, le tout réparti sur 3 étages gérant chacun un pôle.
Nous vous fournissons un tableau répertoriant tout nos effectifs

Voici les demandes que nous souhaiterions apporter à l'architecture réseau de nos sites :

- Pour commencer, mettre en place une infrastructure réseau permettant des échanges rapides et sécurisés entre les sites de Paris, Lyon, et Marseille.
- De plus, utiliser des technologies avancées telles que OSPF pour le routage dynamique et MPLS pour optimiser les transferts de données, garantissant une gestion efficace du trafic réseau.
- Déployer des pare-feu sur VM Debian et des tunnels VPN pour sécuriser les communications inter-sites et créer une DMZ pour isoler les services publics et protéger les données sensibles contre les cybermenaces.
- Configurer des VLAN pour chaque étage afin d'isoler les flux de données, améliorer la gestion du réseau et renforcer la sécurité interne.
- Utiliser GNS3 pour simuler et tester l'infrastructure, garantissant la fiabilité et la conformité des configurations.

- La mise en place de l'architecture réseau devra être conforme à la norme ISO/IEC 27001:2013 sur la sécurité de l'information, assurant ainsi la mise en œuvre de pratiques de sécurité robustes :

Actions spécifiques :

- Déployer des pare-feu Debian pour renforcer la sécurité et garantir la protection des données sensibles.
- Mettre en place une segmentation VLAN et des tunnels VPN pour assurer la confidentialité et la fluidité des échanges entre les sites de Paris, Lyon, et Marseille.

Critères de réussite :

- Maintenir un taux de disponibilité des services supérieur à 99,9 %.
- Valider les configurations réseau via des tests de simulation effectués dans GNS3 pour garantir leur fiabilité.

Nous restons disponibles pour toute précision sur les demandes et vous transmettons les accès nécessaires aux équipements de nos sites.



PRÉSENTATION DE LA MAQUETTE

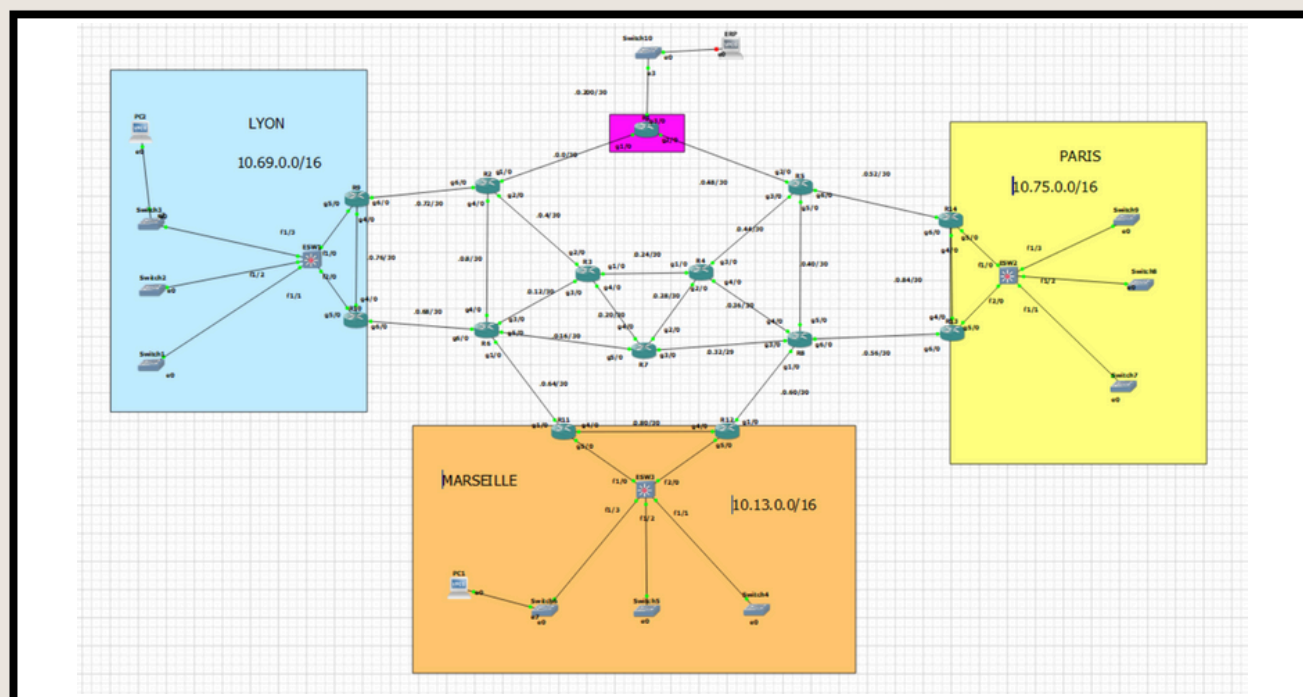
Maintenant que nous avons les contextes et les détails du projet, nous allons à présent passer à la partie pratique :

Nous avons tout d'abord choisi **GNS3** comme logiciel pour créer notre maquette. Ce choix s'est imposé car **GNS3** permet de modéliser des environnements réalistes grâce à l'utilisation d'images IOS réelles et à la prise en charge d'équipements multi-vendeurs. Cela offre une flexibilité accrue pour tester des configurations complexes tout en restant proche des conditions réelles.

Nous avons commencé par concevoir une maquette représentant notre entreprise avec trois sites principaux : **Paris, Lyon, et Marseille**. Chaque site possède une segmentation logique basée sur des VLAN, un plan d'adressage spécifique, et des routeurs configurés en HSRP pour assurer la redondance locale.



















Pour relier ces sites, un backbone MPLS a été intégré à notre maquette, permettant une interconnexion performante et sécurisée. Par souci de sécurité, nous ne divulguons pas les adresses IP utilisées dans ce backbone.

Enfin, un serveur ERP a été centralisé sur le site de Lyon. Ce serveur est configuré pour être accessible depuis les autres sites via le réseau MPLS et bénéficie d'une sécurité renforcée grâce à des tunnels VPN et un routage dynamique OSPF. Nous expliquerons en détail les protocoles et technologies utilisés dans la rubrique dédiée.



Une fois la maquette constituée, nous devons commencer à la configurer :
Pour cela, nous devons utiliser des protocoles qui vont nous permettre un bon fonctionnement.

Vous trouverez ci-dessous tous les protocoles utilisés lors de la configuration, accompagnés de leur contexte, de leur paramétrage et d'une démonstration de leur fonctionnement.

	HSRP		Facile
	OSPF		Moyenne
	802.1Q		Facile
	DNS		Facile
	MPLS		Compliqué
	VPN		Compliqué
	DHCP		Facile
	QoS		Compliqué
	NTP		Facile

Blocage du trafic RDP

Le blocage du port 3389, utilisé par le protocole RDP (Remote Desktop Protocol), est essentiel pour protéger le réseau contre les tentatives de connexion non autorisées ou les attaques exploitant ce service.

Une ACL étendue a été créée sur le routeur R1 pour bloquer ce trafic :

- Règle 10 : deny tcp any any eq 3389 – Bloque tout trafic TCP destiné au port 3389.
- Règle 20 : permit ip any any – Autorise tout autre trafic réseau.

Objectif :

Empêcher tout accès RDP aux appareils du réseau tout en permettant le fonctionnement normal des autres services.

Cette configuration garantit une protection renforcée contre les failles liées à RDP, tout en maintenant une flexibilité dans les autres communications réseau.

```
R1#show access-lists BLOCK_RDP
Extended IP access list BLOCK_RDP
 10 deny tcp any any eq 3389
 20 permit ip any any (70 matches)
```


Configuration des VLAN et HSRP

La segmentation VLAN et la redondance HSRP (Hot Standby Router Protocol) sont mises en œuvre pour assurer une gestion optimisée et une disponibilité continue des réseaux locaux.

VLAN :

- Chaque site est segmenté en trois VLAN principaux (10, 20, 30).
- Les routeurs utilisent 802.1Q pour taguer les VLAN et garantir l'isolation des flux.

HSRP :

- Sur chaque site, deux routeurs sont configurés :
 - Routeur actif avec une priorité plus élevée (120).
 - Routeur standby avec une priorité inférieure (100).
 -
- Une IP virtuelle .254 est définie comme passerelle par défaut pour chaque VLAN.

Objectif :

Assurer une redondance des passerelles locales et éviter toute interruption en cas de panne d'un routeur

```
R10
GigabitEthernet5/0.10    10.69.10.3    YES NVRAM  up
GigabitEthernet5/0.20    10.69.20.3    YES NVRAM  up
GigabitEthernet5/0.30    10.69.30.3    YES NVRAM  up
GigabitEthernet6/0       10.0.0.70     YES NVRAM  up
Loopback0                10.10.10.10   YES NVRAM  up

R10#
R10#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R10(config)#interface GigabitEthernet5/0.20
R10(config-subif)# ip helper-address 10.69.10.3
R10(config-subif)#interface GigabitEthernet5/0.30
R10(config-subif)# ip helper-address 10.69.10.3
R10(config-subif)#end
R10#write memory
Building configuration...
[OK]
R10#
*Dec 31 12:40:32.583: %SYS-5-CONFIG_I: Configured from console by console
R10#

R9
GigabitEthernet5/0.10    10.69.10.2    YES NVRAM  up
GigabitEthernet5/0.20    10.69.20.2    YES NVRAM  up
GigabitEthernet5/0.30    10.69.30.2    YES NVRAM  up
GigabitEthernet6/0       10.0.0.74     YES NVRAM  up
Loopback0                9.9.9.9       YES NVRAM  up

R9#
R9#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R9(config)#interface GigabitEthernet5/0.20
R9(config-subif)# ip helper-address 10.69.10.2
R9(config-subif)#interface GigabitEthernet5/0.30
R9(config-subif)# ip helper-address 10.69.10.2
R9(config-subif)#end
R9#write memory
Building configuration...
[OK]
R9#
```

Grâce à HSRP, les sites bénéficient d'une continuité de service réseau, et la segmentation VLAN améliore la sécurité et l'organisation des flux.

```
ESW1#show interface trunk

Port      Mode      Encapsulation  Status        Native vlan
Fa1/0     on        802.1q         trunking      1
Fa2/0     on        802.1q         trunking      1

Port      Vlans allowed on trunk
Fa1/0     1-4094
Fa2/0     1-4094

Port      Vlans allowed and active in management domain
Fa1/0     1,10,20,30
Fa2/0     1,10,20,30

Port      Vlans in spanning tree forwarding state and not pruned
Fa1/0     1,10,20,30
Fa2/0     1,10,20,30
ESW1#
```

Infrastructure Backbone

L'interconnexion des trois sites (Paris, Lyon, Marseille) repose sur un backbone MPLS et un routage dynamique OSPF (Open Shortest Path First).

- Backbone MPLS :
 - Garantit un transfert de données rapide et sécurisé entre les sites.
- OSPF :
 - Permet la propagation des sous-réseaux VLAN dans tout le réseau.
 - Assure un routage dynamique et une redondance en cas de panne.

Objectif :

Optimiser les échanges entre sites tout en garantissant la résilience du réseau.

Conclusion :

L'utilisation conjointe de MPLS et OSPF améliore la performance et la fiabilité de l'interconnexion multi-sites.

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst                src                state                conn-id status
IPv6 Crypto ISAKMP SA
```

Configuration des trunks

Les trunks permettent de transporter plusieurs VLAN entre les équipements réseau tout en maintenant leur isolation logique.

Configuration :

- Sur le switch SW1, les ports Fa1/0 et Fa2/0 sont configurés en mode trunk 802.1Q.
- VLAN transportés : 10, 20, et 30.

Objectif :

- Assurer la communication inter-VLAN entre les équipements tout en maintenant l'intégrité des données.

Conclusion :

La configuration des trunks garantit une connectivité optimale entre les VLAN sur le réseau.

```
ESW1#show interface trunk

Port      Mode      Encapsulation  Status        Native vlan
Fa1/0     on        802.1q         trunking      1
Fa2/0     on        802.1q         trunking      1

Port      Vlans allowed on trunk
Fa1/0     1-4094
Fa2/0     1-4094

Port      Vlans allowed and active in management domain
Fa1/0     1,10,20,30
Fa2/0     1,10,20,30

Port      Vlans in spanning tree forwarding state and not pruned
Fa1/0     1,10,20,30
Fa2/0     1,10,20,30
ESW1#
```

Configuration DHCP Relay

Le DHCP relay permet de centraliser la gestion des adresses IP tout en desservant plusieurs sous-réseaux.

Configuration :

- Sur les routeurs R9 et R10 (site de Lyon) :
- La commande ip helper-address est utilisée pour relayer les demandes DHCP vers le serveur central.

Objectif : Simplifier la gestion des adresses IP sur les VLAN des sites tout en assurant une attribution dynamique.

Conclusion :

Cette configuration centralisée garantit une gestion IP flexible et efficace.

```
R10#
R10#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R10(config)#interface GigabitEthernet5/0.20
R10(config-subif)# ip helper-address 10.69.10.3
R10(config-subif)#interface GigabitEthernet5/0.30
R10(config-subif)# ip helper-address 10.69.10.3
R10(config-subif)#end
R10#write memory
Building configuration...
[OK]
R10#
*Dec 31 12:40:32.583: %SYS-5-CONFIG_I: Configured from console by console
R10#

R9#
R9#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R9(config)#interface GigabitEthernet5/0.20
R9(config-subif)# ip helper-address 10.69.10.2
R9(config-subif)#interface GigabitEthernet5/0.30
R9(config-subif)# ip helper-address 10.69.10.2
R9(config-subif)#end
R9#write memory
Building configuration...
[OK]
R9#
```

Sécurisation des flux réseau

La sécurisation des flux réseau est primordiale pour prévenir les attaques et garantir un environnement stable.

UFW (Linux Firewall) :

- Autorise uniquement les ports essentiels :
 - Port 53 (DNS)
 - Port 8000 (Application)
 - Port 22 (SSH)

Objectif :

Restreindre l'accès aux services non autorisés et renforcer la sécurité globale.

Conclusion :

L'utilisation d'un pare-feu UFW protège efficacement les services critiques contre les accès non autorisés.

```
etudiant@etudiant:~$ sudo ufw enable
sudo ufw status verbose
Firewall is active and enabled on system startup
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
```

To	Action	From
--	-----	----
53	ALLOW IN	10.100.0.0/24
8000	ALLOW IN	10.100.0.0/24
22	ALLOW IN	10.0.0.0/24

Serveur ERP

Le serveur ERP est un composant clé pour centraliser les opérations et la gestion des données de l'entreprise.

Configuration :

- Localisé sur le site de Lyon dans le sous-réseau 10.100.0.0/24.
- Sécurisé par :
 - Tunnels VPN pour les échanges inter-sites.
 - Résolution DNS interne (erp.netconnectsolutions.local).

Objectif :

- Offrir un accès centralisé sécurisé et performant aux services ERP.

Conclusion :

L'hébergement centralisé et la sécurisation du serveur ERP garantissent une efficacité opérationnelle accrue.

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
IPv6 Crypto ISAKMP SA
```

Ainsi, pour conclure, dans le cadre du déploiement d'une infrastructure réseau multi-sites sécurisée pour l'entreprise NetConnect Solutions, nous avons pris en compte les besoins spécifiques de chaque site géolocalisé à Paris, Lyon, et Marseille.

Avec une segmentation par VLAN et des solutions redondantes via HSRP, notre priorité était de garantir la sécurité et la fiabilité des communications tout en assurant une gestion optimale du réseau. Grâce à l'intégration de OSPF et MPLS, nous avons optimisé les échanges inter-sites, offrant une connectivité performante et évolutive entre les différents sites.

Conformément à la norme ISO/IEC 27001, nous avons renforcé la sécurité des données en déployant des pare-feu Debian, en créant des tunnels VPN pour les connexions sécurisées, et en centralisant le serveur ERP sur le site de Lyon. La mise en place de tests réguliers via GNS3 a permis de valider la fiabilité des configurations avant leur déploiement.

De plus, nous avons veillé à :

- Maintenir une haute disponibilité grâce aux mécanismes de redondance et aux sauvegardes automatisées.
- Offrir une traçabilité des activités réseau, facilitant ainsi la gestion des incidents et l'analyse statistique.
- Garantir un accès sécurisé pour les employés en télétravail, tout en restreignant les communications entre les différents étages pour répondre aux exigences de sécurité interne.

En résumé, notre infrastructure réseau répond pleinement aux besoins de sécurité, de connectivité, et de résilience de NetConnect Solutions, positionnant ainsi l'entreprise pour relever les défis technologiques de demain tout en soutenant ses activités actuelles.