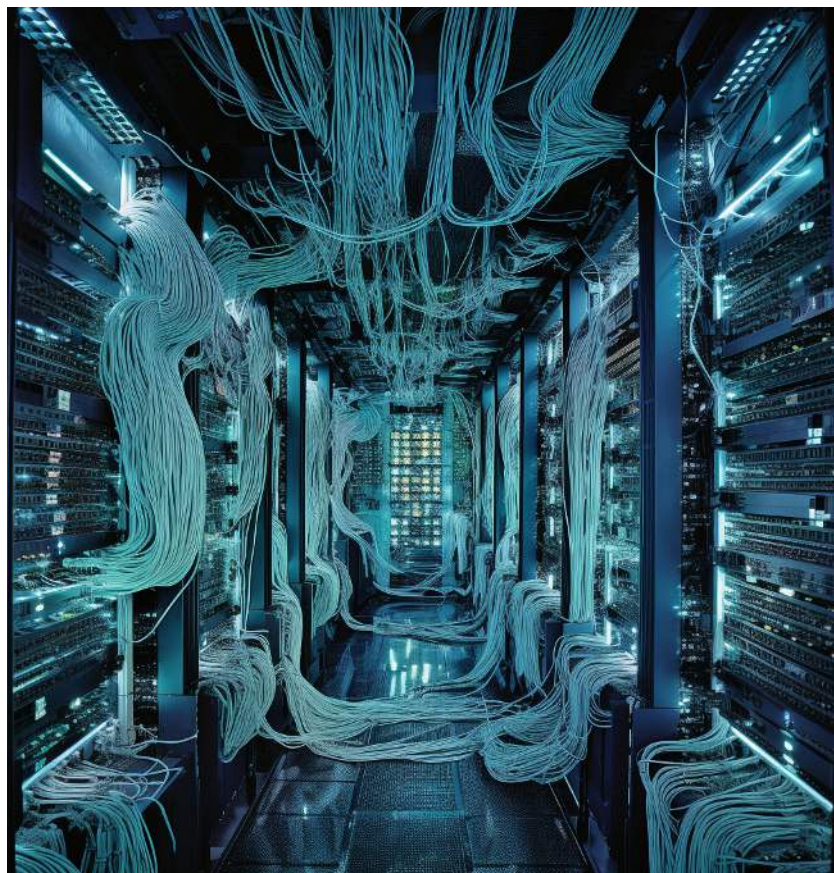


Dossier Technique Infrastructure et Réseau



Introduction.....	1
Description et Configuration du Réseau.....	1
1. Interface WAN :	1
2. Interface LAN:.....	2
3. Interface DMZ :	3
Diagramme du Réseau.....	5
Stratégies de Sécurité du Réseau.....	6
1. LAN :	6
2. WAN :	7
3. DMZ :	7
Conclusion.....	9

Introduction

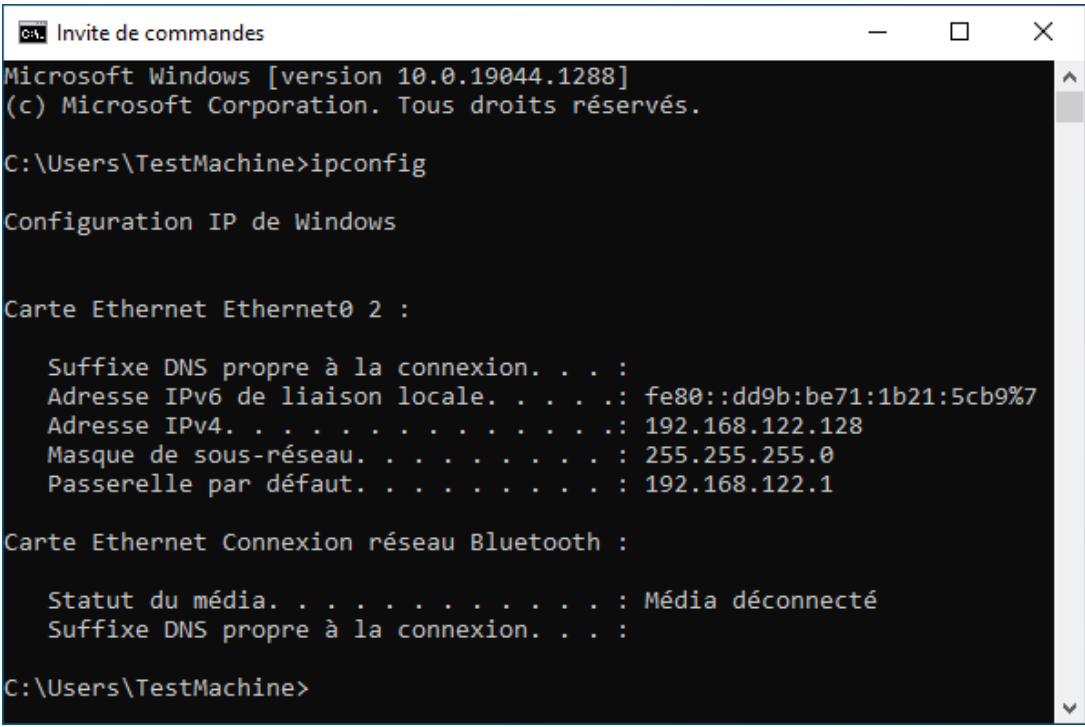
Ce dossier détaille l'architecture et la configuration d'une infrastructure réseau sophistiquée développée dans l'environnement de simulation GNS3. Le pivot de cette infrastructure est le routeur firewall pfSense, qui gère trois interfaces réseau distinctes : LAN, WAN et DMZ.

Description et Configuration du Réseau

Notre réseau est conçu pour optimiser la sécurité, la flexibilité et l'efficacité opérationnelle. Le routeur firewall pfSense, au centre de notre architecture, offre une sécurité de pointe et un contrôle précis du trafic réseau.

1. Interface WAN :

L'interface WAN, avec l'adresse IP statique `192.168.122.149`, est reliée à un switch qui gère le trafic vers un PC Windows 10 et un dispositif NAT, agissant comme passerelle vers Internet.



```
Invite de commandes
Microsoft Windows [version 10.0.19044.1288]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\TestMachine>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet0 2 :

    Suffixe DNS propre à la connexion. . . : 
    Adresse IPv6 de liaison locale. . . . : fe80::dd9b:be71:1b21:5cb9%7
    Adresse IPv4. . . . . : 192.168.122.128
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.122.1

Carte Ethernet Connexion réseau Bluetooth :

    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . : 

C:\Users\TestMachine>
```

2. Interface LAN:

Cette interface, configurée avec l'adresse IP statique `192.168.77.1`, est connectée à un switch dédié qui dessert deux PC clients

Interfaces / LAN (em1)

General Configuration

Enable

☒ Enable interface

Description

LAN

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

Static IPv4 Configuration

IPv4 Address

192.168.77.1

/

24

IPv4 Upstream gateway

None

+ Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.

On local area network interfaces the upstream gateway should be "none".

Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).

Gateways can be managed by [clicking here](#).

3. Interface DMZ :

L'interface DMZ, ayant l'adresse IP statique `192.168.90.1`, est connectée à un switch séparé qui est ensuite relié à un serveur Ubuntu, établissant ainsi une zone démilitarisée pour minimiser les risques de sécurité.

The screenshot shows the Mikrotik WinBox configuration page for the interface **DMZ (em2)**. The page is divided into two main sections: **General Configuration** and **Static IPv4 Configuration**.

General Configuration:

- Enable:** ☒ Enable interface
- Description:** DMZ (with a placeholder text: "Enter a description (name) for the interface here.")
- IPv4 Configuration Type:** Static IPv4

Static IPv4 Configuration:

- IPv4 Address:** 192.168.90.1 / 24
- IPv4 Upstream gateway:** None (with a green button: "+ Add a new gateway")
- Help text:** "If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the 'Add' button. On local area network interfaces the upstream gateway should be 'none'. Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface. Gateways can be managed by clicking here."

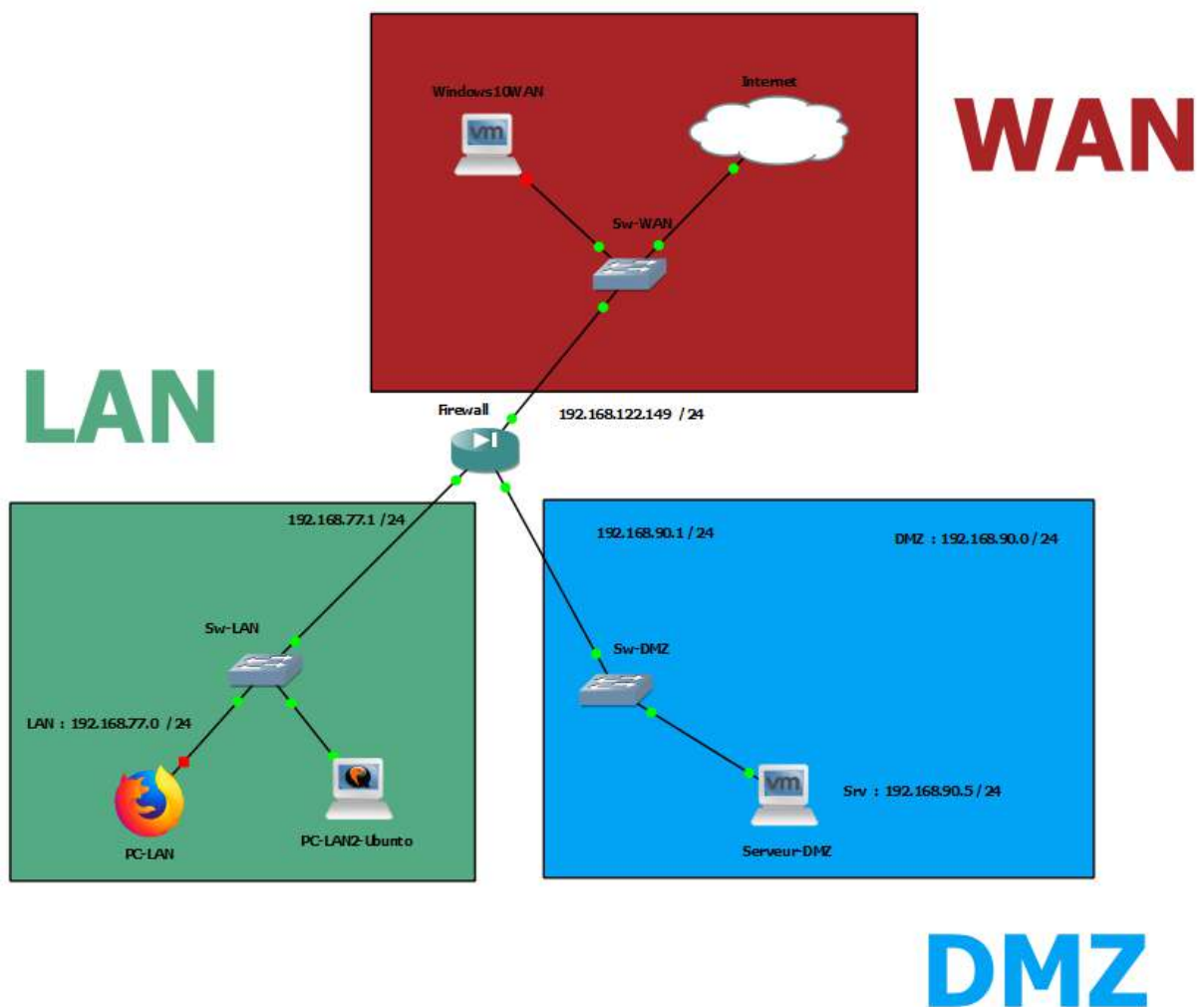
The screenshot shows the terminal window of **Ubuntu Server2 - VMware Workstation**. The terminal is running the **nano** text editor, editing the file **/etc/netplan/00-installer-config.yaml**. The configuration is for the **ens33** interface, set to static IP **192.168.90.5/24** with a gateway of **192.168.90.1**. The terminal output is as follows:

```
GNU nano 4.8 /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  renderer: networkd
  ethernets:
    ens33:
      dhcp4: no
      addresses: [192.168.90.5/24]
      gateway4: 192.168.90.1
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1]
      dhcp6: no
  version: 2
```

At the bottom of the terminal window, it says: "To return to your computer, press Ctrl+Alt."

Diagramme du Réseau

Le diagramme de réseau visuel donne une représentation claire de l'architecture globale du réseau, montrant comment chaque composant est interconnecté pour fournir un système réseau solide et sécurisé.



Stratégies de Sécurité du Réseau

Un aspect critique de notre réseau est sa robustesse en matière de sécurité. Nous avons mis en place des politiques de sécurité spécifiques pour chaque segment du réseau :

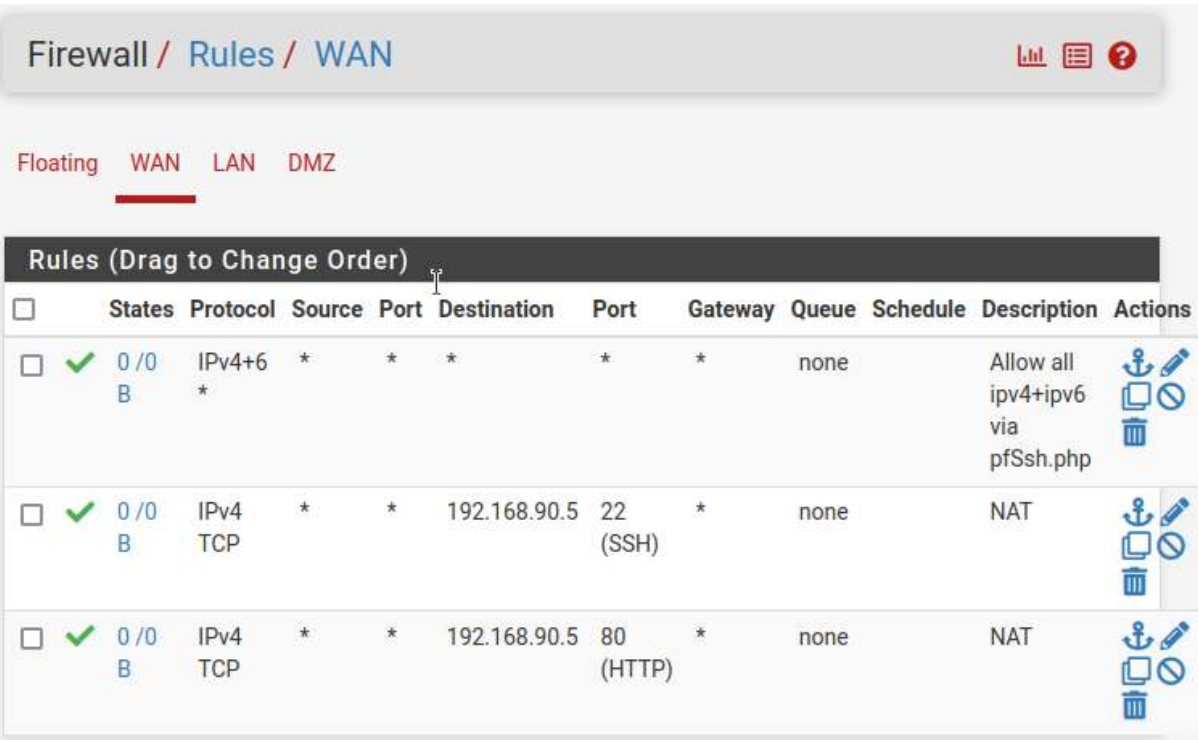
1. LAN :

Les PC clients sur le LAN ont accès à tous les autres segments du réseau, offrant une flexibilité maximale aux utilisateurs internes.

Firewall / Rules / LAN											
Floating WAN LAN DMZ											
Rules (Drag to Change Order)											
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	2 /1.06 MiB	*	*	*	LAN Address	80	*	*		Anti- Lockout Rule	
☐	☒ 4 /2.84 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
☐	☒ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

2. WAN :

L'accès du WAN est limité à la DMZ. Cela permet au PC-WAN d'accéder au serveur Ubuntu via le service SSH en utilisant Putty, grâce à une règle spécifique ajoutée dans le menu de configuration de pfSense sous Firewall/NAT/Port Forward. Cela empêche toute communication directe avec le LAN, minimisant ainsi les risques de sécurité.



Firewall / Rules / WAN											  
Floating WAN LAN DMZ											
Rules (Drag to Change Order)											
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	 0/0 B	IPv4+6 *	*	*	*	*	*	none		Allow all ipv4+ipv6 via pfSsh.php	    
☐	 0/0 B	IPv4 TCP	*	*	192.168.90.5	22 (SSH)	*	none		NAT	    
☐	 0/0 B	IPv4 TCP	*	*	192.168.90.5	80 (HTTP)	*	none		NAT	    

3. DMZ :

La DMZ est strictement isolée, sans accès ni au LAN ni au WAN, limitant ainsi l'exposition du serveur Ubuntu aux autres segments du réseau, à l'exception de l'accès autorisé au PC-WAN via SSH ou HTTP.

Firewall / NAT / Port Forward

Port Forward

1:1

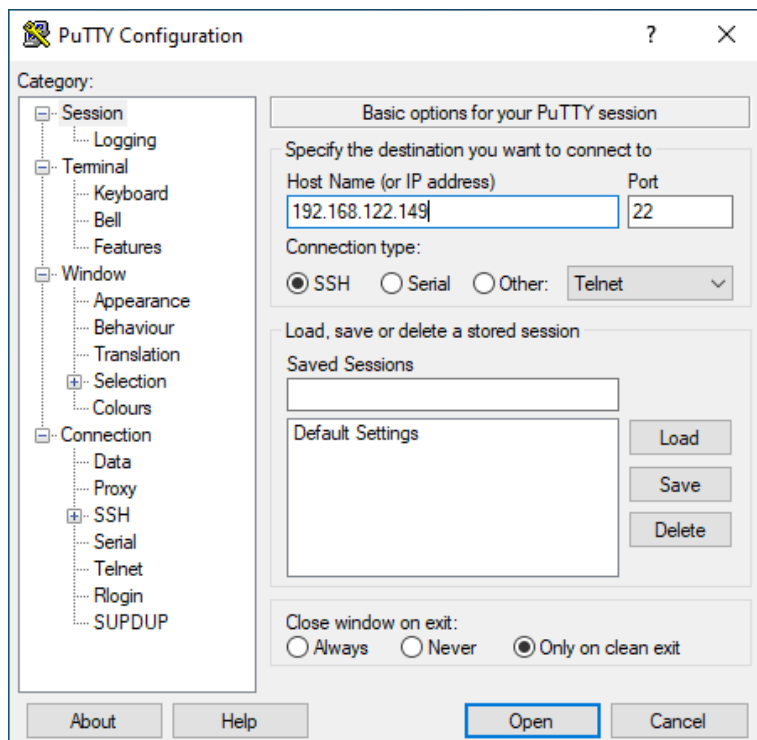
Outbound

NPt

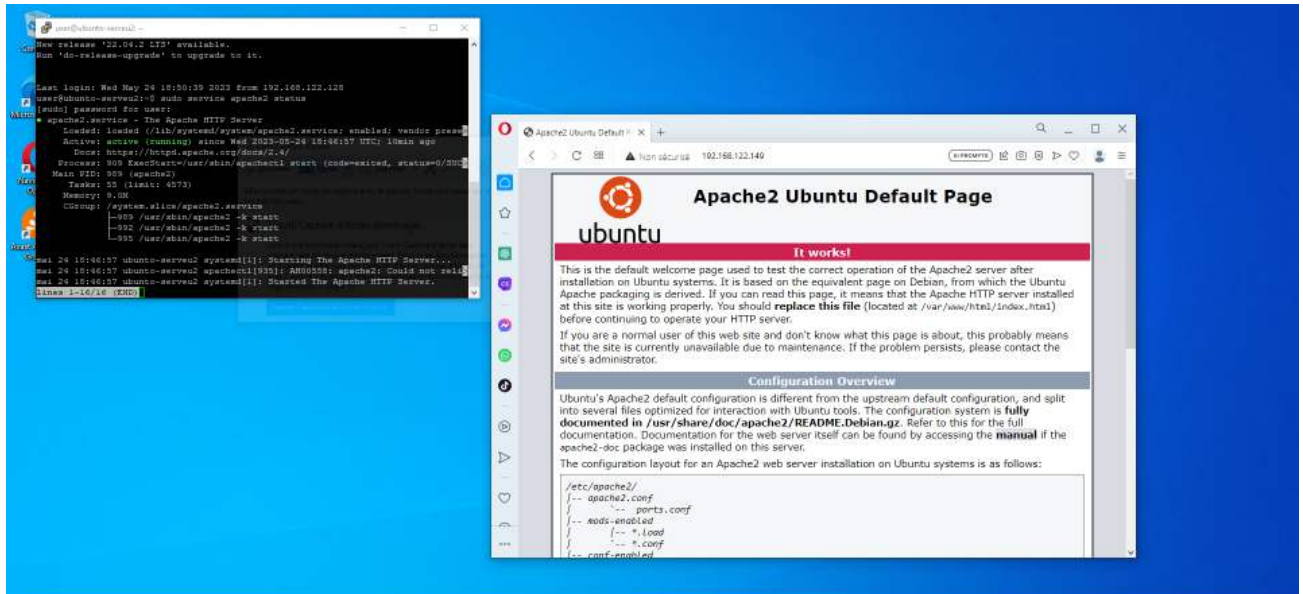
Rules

		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
☐	☒	☒	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.90.5 80 (HTTP)		  
☐	☒	☒	WAN	TCP	*	*	WAN address	22 (SSH)	192.168.90.5 22 (SSH)		  

En complément de ces politiques d'accès, nous avons mis en œuvre une règle de Port Forwarding, redirigeant certains ports et protocoles du WAN vers la DMZ. Cette règle renforce la sécurité en minimisant les ports directement exposés à Internet tout en permettant l'accès nécessaire au serveur.



Ce niveau d'accès a été mis en place en ajoutant une règle spécifique dans le menu de configuration de pfSense sous Firewall/NAT/Port Forward. Cette règle autorise le PC-WAN à accéder au serveur Ubuntu via le service SSH en utilisant Putty. Cela assure que le PC-WAN peut atteindre le serveur quand nécessaire, tout en maintenant la séparation stricte du LAN pour minimiser les risques de sécurité.



Conclusion

En somme, ce dossier technique offre un aperçu de la complexité liée à la conception, à la configuration et à la gestion d'une infrastructure réseau performante et sécurisée. Les différentes stratégies de sécurité mises en œuvre démontrent un équilibre entre flexibilité et sécurité, permettant à chaque segment du réseau de fonctionner efficacement tout en minimisant les risques.

Le déploiement de GNS3 et de pfSense dans ce projet illustre leurs puissantes capacités à créer des environnements de réseau sécurisés et opérationnels. Cela souligne le potentiel des outils modernes dans la construction et la gestion des infrastructures réseau.

En guise de conclusion, ce projet étudiant met en exergue la sophistication de la construction d'une infrastructure réseau. Il met en lumière les compétences essentielles et les connaissances requises pour répondre aux défis de sécurité et aux besoins variés dans l'environnement dynamique du réseau moderne. Ce projet est un témoignage du travail rigoureux et de l'expertise nécessaire pour naviguer dans le paysage toujours en évolution de la technologie réseau.