

MINISTÈRE DE LA FORMATION ET DE L'ENSEIGNEMENT PROFESSIONNELS

INSTITUT NATIONAL SPÉCIALISÉ DE FORMATION PROFESSIONNELLE

IMARZOUKEN MOHAMED AREZKI

TIZI-OUZOU



MÉMOIRE FIN DE FORMATION

Spécialité : Système Numérique

Option : Informatique et Réseaux informatiques

Thème :

Mise en place d'une solution de sécurité dans un réseau local à l'aide d'équipements Aruba et FortiGate

Cas : Réalisé par SNC RAM ELECTRO



Réalisé par :
LOUNES SID ALI

Dirigé par : Z. LEBOUR
Encadré par : A. TOUAT

Session : Année 2025

Remerciements

Tout d'abord, je remercie Dieu de m'avoir accordé la force de mener à bien ce travail, car toute chose vient d'**Allah**.

Je tiens à exprimer ma profonde gratitude la plus sincère à ma famille : ma mère, mon père, mes frères et mes sœurs, pour leur soutien indéfectible tout au long de ce parcours.

J'adresse ma gratitude à mon enseignante, Mme Z. Lebour, pour ses efforts, sa présence et ses précieux conseils tout au long de la rédaction de ce mémoire et durant l'ensemble de ma formation.

J'adresse ma sincère gratitude aux responsables de la **SNC RAMELECTRO** pour m'avoir accueilli au sein de leur entreprise et mis à ma disposition tous les moyens nécessaires dont j'avais besoin à la bonne réalisation de mon stage, ainsi qu'à l'ensemble du personnel, particulièrement à mes maîtres de stage.

Enfin, je tiens à remercier les membres du jury d'avoir consacré de leur temps à la lecture de ce mémoire et d'avoir accepté de faire partie de mon jury de soutenance.

LISTE DES ABBREVIATIONS

ACK	Acknowledgment
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
ASIC	Application-Specific Integrated Circuit
BID	Bridge ID
CA	Certificate Authority
CLI	Command-Line Interface
CST	Common Spanning Tree
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
DPI	Deep Packet Inspection
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
FTP	File Transfer Protocol
GMT/UTC	Greenwich Mean Time/Universal Time Coordinated
GNS3	Graphical Network Simulator-3
GUI	Graphical User Interface
HCI	Hyper-Converged Infrastructure
hda	Hard Disk A

hdb	Hard Disk B
HPE	Hewlett Packard Enterprise
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IA	Artificial intelligence
ICMP	Internet Control Message Protocol
IDC	International Data Corporation
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPS	Intrusion Prevention System
KVM	Kernel-based Virtual Machine
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MD5	Message Digest Algorithm 5
MITM	Man-in-the-middle
MSTP	Multiple Spanning Tree Protocol
NAT	Network Address Translation
NGFW	Next-Generation Firewall
NTP	Network Time Protocol
NVRAM	Non-Volatile Random-Access Memory
OSI	Open Systems Interconnection
PING	Packet Internet Groper
PME	Petite et Moyenne Entreprise
PVST+	Per-VLAN Spanning Tree Plus
Qemu	Quick Emulator
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RN	Revision Number
RSA	Rivest–Shamir–Adleman
RSH	remote shell
RST	Reset

RSTP	Rapid Spanning Tree Protocol
RTP	Real-time Transport Protocol
SD-WAN	Software-Defined Wide Area Network
SDN	Software-Defined Networking
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNMPv2c	Simple Network Management Protocol version 2c
SNMPv3	Simple Network Management Protocol version 3
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
SYN	Synchronize
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTL	Time To Live
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VLAN	virtual local area network
VMDK	Virtual Machine Disk
VoIP	Voice over IP
VPN	Virtual Private Network
VTP	VLAN Trunking Protocol
WEP	Wired Equivalent Privacy
WI-FI	wireless fidelity

TABLE DES FIGURES

1.1	Organigramme RAMELECTRO	5
1.2	Schéma réseau de l'entreprise	11
1.3	Partie réseau étudié	11
2.1	Les objectifs de la sécurité informatique	14
3.1	VLAN par port	31
3.2	Authentification 802.1X	34
4.1	Pare-feu : matériel et logiciels	49
4.2	Architecture simple	51
4.3	Architecture sensible	51
4.4	Zone démilitarisée (DMZ)	54
5.1	Architecture du réseau local avec la solution proposée	56
5.2	Choix d'Aruba par rapport à Cisco	60
5.3	l'environnement GNS3	61
5.4	Interface principale de GNS3 avec la liste des périphériques disponibles.	62
5.5	Options de création d'un nouveau modèle dans GNS3	63
5.6	Liste des appliances disponibles depuis le serveur GNS3.	63
5.7	Sélection du type de serveur pour l'installation de l'appliance.	64
5.8	Configuration du binaire Qemu pour exécuter l'appliance.	64
5.9	Création d'une nouvelle version de l'appliance (7.0.9).	65
5.10	Sélection de l'image disque principale (hda) pour FortiGate.	65
5.11	Sélection de l'image disque secondaire (hdb).	66
5.12	Interface de navigation pour sélectionner les fichiers image.	66
5.13	Liste des versions disponibles de FortiGate et leurs fichiers associés.	67
5.14	Confirmation finale pour installer FortiGate version 7.0.9.	67
5.15	Instructions d'utilisation après installation.	68
5.16	Menu de sélection des appliances dans GNS3.	69
5.17	Liste des appliances Windows disponibles.	69
5.18	Sélection du serveur d'exécution.	70
5.19	Configuration du binaire Qemu.	70
5.20	Téléchargement du fichier VMDK (6.8GB pour Win10).	71
5.21	Statut des fichiers après téléchargement.	71
5.22	Confirmation finale avant installation.	72

5.23 Instructions post-installation	72
5.24 Menu principal de GNS3 avec l'option d'import d'appliance.	73
5.25 Navigation vers le fichier appliance Aruba (.gns3a).	73
5.26 Sélection du type de serveur (GNS3 VM recommandé).	74
5.27 Configuration du binaire Qemu (version 8.0.4).	74
5.28 Sélection de la version d'Aruba AOS-CX	75
5.29 Sélection du fichier image VMDK pour Aruba.	75
5.30 Confirmation d'installation de la version 10.15.0005.	76
5.31 Instructions post-installation pour Aruba AOS-CX.	76
5.32 Configuration initiale via CLI	77
5.33 Interface de connexion web du FortiGate	78
5.34 Tableau de bord du FortiGate	79
5.35 Interface graphique pour la création d'une nouvelle interface VLAN	80
5.36 Configuration du VLAN secrétariat	80
5.37 Activation des accès administratifs	81
5.38 Paramètres avancés du VLAN secrétariat	81
5.39 Configuration du VLAN invité (vlan80)	82
5.40 Configuration des accès administratifs et du serveur DHCP	82
5.41 Paramètres avancés du VLAN invité	83
5.42 Configuration du VLAN gestion (vlan100)	84
5.43 Configuration des accès administratifs et du serveur DHCP	84
5.44 Configuration du VLAN VoIP (vlan90)	85
5.45 Liste des interfaces VLAN créées	86
5.46 Liste des interfaces VLAN créées	86
5.47 Configuration de la zone "routage inter vlan"	87
5.48 Routage entre les service et VoIP	88
5.49 Routage entre VoIP et les service	88
5.50 Configuration d'une route statique	89
5.51 Liste des profils de filtrage web par défaut	90
5.52 Clonage du profil default avec un nouveau nom filtre zone	90
5.53 Configuration du profil filtre zone	91
5.54 Création d'une nouvelle politique nommée "zone to wan"	91
5.55 Configuration de la politique avec inspection	92
5.56 Ajout de profils de sécurité	92
5.57 Politique VLAN invité (vlan80) vers Internet via wan (port1)	93
5.58 Politique pour le VLAN invité avec inspection	93
5.59 Menu des profils de sécurité dans FortiGate (section Web Filter).	94
5.60 Création d'un nouveau profil de filtrage web.	94
5.61 Ajout d'une règle de filtrage pour facebook.com.	95
5.62 Vérification des paramètres du filtre URL.	95
5.63 Liste finale des profils avec le nouveau "block Facebook".	96
5.64 Application du profil à une politique firewall.	96
5.65 Politique d'isolation entre vlan80 (invite) et routage inter vlan	97
5.66 Politique d'isolation entre vlan80 (invite) et vlan100 (gestion)	98
5.67 Liste des politiques créées	98
5.68 Interface vide des politiques de gestion de trafic	99
5.69 Création d'une nouvelle politique nommée " QoS _VoIP "	99
5.70 Création groupe de service	100

5.71	groupe de services VoIP _ Services et l'application VoIP	100
5.72	Édition d'un shaper partagé	101
5.73	Création d'une classe d'identification de trafic	101
5.74	La politique "QoS _ VoIP"	102
5.75	"QoS _ VoIP" avec ses paramètres de source, destination, et priorisation.	102
5.76	Configuration NTP	103
5.77	Lancement d'une nouvelle session série dans MobaXterm.	104
5.78	Paramétrage avancé de la connexion série.	104
5.79	Configuration initiale via console série (USB COM3).	105
5.80	Page de connexion à l'interface web.	106
5.81	Dashboard principal de l'interface ArubaOS.	106
5.82	Création d'un nouveau VLAN (ID 100).	107
5.83	Configuration détaillée du VLAN 100.	107
5.84	Configuration IP du VLAN 100.	108
5.85	Table VLAN finale avec le nouveau VLAN 100.	108
5.86	(VLAN cabinet) : Connectivité vers VLAN 20 (succès) et VLAN 80 (échec)	123
5.87	(VLAN invité) : Échec des requêtes vers les VLAN des services	124
5.88	(vlan secretariat) : Connectivité vers VLAN 10 (succès) et VLAN 80 (échec)	124
5.89	Configuration réseau d'une machine dans VLAN cabenet	125
5.90	Message de blocage lors de la tentative d'accès à Facebook	125
5.91	Switch du rez-de-chaussée	126
5.92	Switch du 1 ^{er} étage	126
5.93	Switch du 2 ^{ème} étage	127

LISTE DES TABLEAUX

1.1	Liste des équipements	10
2.1	ARP Poisoning (ARP Spoofing)	18
2.2	IP Spoofing (Usurpation d'adresse IP)	19
3.1	Structure du Bridge ID	39
3.2	Coûts STP par bande passante selon le protocole	40
3.3	Comparaison des versions STP	42
4.1	Avantages et inconvénients d'un pare-feu matériel	52
5.1	Plan d'adressage du réseau local	57
5.2	Affectation des VLAN aux ports de chaque switch	58

TABLE DES MATIÈRES

Table des matières	xiii
1 Présentation de l'organisme d'accueil	3
1.1 Présentation de l'entreprise SNC RAMELECTRO	3
1.1.1 Profil général de la société	3
1.1.1.1 Nom et raison social de la société	3
1.1.1.2 Domaine d'activité	3
1.1.2 Les valeurs de l'entreprise	4
1.1.2.1 L'innovation technologique	4
1.1.2.2 L'innovation organisationnelle	4
1.1.3 Organigramme SNC RAMELECTRO	5
1.1.4 Références clients	5
1.1.4.1 Principaux Clients	5
1.1.4.2 Principaux projets réalisés des trois dernières années	6
1.1.4.3 Projets en cours	9
1.1.5 Mode opératoire pour réaliser le projet :	9
1.1.5.1 Descriptif de la solution technique	9
1.1.5.2 Moyens organisationnels	9
1.2 Présentation du champ d'étude (Entreprise publique)	10
1.2.1 Infrastructure Informatique	10
1.2.2 Schéma de réseau	10
1.2.3 Analyse et amélioration du réseau local	12
1.2.3.1 Les critiques	12
1.2.3.2 Solutions proposées	12
2 La sécurité informatique	13
2.1 Sécurité d'un réseau	13
2.1.1 Les causes de l'insécurité	13
2.1.2 Les services de sécurité	13
2.2 Les pirates informatiques	14
2.3 Malveillance informatique	15
2.3.1 Logiciels malveillants	16
2.3.1.1 Virus	16
2.3.1.2 Vers	16

2.3.1.3	Chevaux de Troie	16
2.3.1.4	Portes dérobées (Backdoors)	16
2.3.1.5	Bombes logiques	16
2.3.1.6	Logiciels espions (Spyware)	16
2.3.2	Courrier électronique non sollicité (Spam)	16
2.3.3	Injection SQL (SQLi)	17
2.4	Les attaques réseau	17
2.4.1	Attaques de découverte du réseau	17
2.4.2	Attaques d'écoute du trafic réseau	17
2.4.3	Attaques d'interférence avec une session réseau	18
2.4.3.1	ARP Spoofing	18
2.4.3.2	IP Spoofing	18
2.4.4	Attaques par déni de service (DoS)	19
2.4.5	Attaques sur les protocoles de routage	19
2.4.6	Attaques sur les accès Wi-Fi	19
2.5	Mécanismes de Sécurité	20
2.5.1	Sécurité Physique	20
2.5.2	Protection des Accès	20
2.5.3	Les pare-feu	20
2.5.4	Accès à distance sécurisé SSH (Secure Shell)	20
2.5.5	Les VPN (Réseaux Privés Virtuels)	20
2.5.6	Les antivirus	21
2.6	Sécurité des équipements réseau	21
2.6.1	Sécurité physique	21
2.6.2	Sécurité du système d'exploitation	21
2.6.3	Sécurité logique	21
2.7	Assurer la confidentialité des connexions	22
2.7.1	Algorithmes cryptographiques	22
2.7.1.1	Cryptographie symétrique (à clé secrète)	22
2.7.1.2	Cryptographie asymétrique (à clé publique)	23
2.7.2	Certificats numériques	23
2.7.3	Fonctions de hachage	23
2.8	La surveillance réseau	23
3	La sécurité dans les Switch	25
3.1	Définition d'un réseau local (LAN)	25
3.2	Les réseaux locaux virtuels	25
3.2.1	Concept fondamental d'un VLAN	25
3.2.2	Avantages clés des VLANs	26
3.2.3	Cas d'usage typique en entreprise	26
3.3	Types de VLANs et leurs Configurations	27
3.3.1	VLAN de données	27
3.3.1.1	Configuration sur ArubaOS-Switch	27
3.3.1.2	Configuration sur Cisco	27
3.3.2	VLAN par défaut	28
3.3.2.1	Configuration sur ArubaOS-Switch	28
3.3.2.2	Configuration sur Cisco	28
3.3.3	VLAN natif	28

3.3.3.1	Configuration sur ArubaOS-Switch	28
3.3.3.2	Configuration sur Cisco	29
3.3.4	VLAN de gestion	30
3.3.4.1	Configuration sur ArubaOS-Switch	30
3.3.4.2	Configuration sur Cisco	30
3.3.5	VLAN privé (Private VLAN – PVLAN)	30
3.4	Typologie de vlan	31
3.4.1	VLAN niveau 1	31
3.4.1.1	Avantages du VLAN par port	31
3.4.1.2	Inconvénients	32
3.4.2	VLAN de Niveau 2	32
3.4.2.1	Avantages	32
3.4.2.2	Inconvénients	32
3.4.3	VLAN de Niveau 3 (VLAN par Sous-Réseaux)	33
3.4.3.1	Avantages	33
3.4.3.2	Inconvénients	33
3.4.4	VLAN avec le standard IEEE 802.1X	33
3.4.4.1	Fonctionnement de l'authentification 802.1X avec RADIUS	33
3.5	Les trunks	34
3.6	Le protocole VTP	35
3.6.1	Présentation	35
3.6.2	Risques et précautions	36
3.6.3	Les modes VTP	36
3.6.4	Les messages VTP	37
3.6.5	La synchronisation	37
3.6.6	Procédure de configuration du protocole VTP	38
3.7	Protocole Spanning-Tree (STP)	38
3.7.1	Présentation de STP	38
3.7.2	Principe de fonctionnement STP	38
3.7.2.1	Identifiants clés	39
3.7.2.2	Explication technique	39
3.7.3	Algorithme STP	39
3.7.4	Optimisation et configuration	39
3.7.4.1	Influence sur l'élection	39
3.7.4.2	Variation des Coûts de Ports selon le Protocole STP	40
3.7.5	États et temporisation des ports	40
3.7.6	Sécurité STP	41
3.7.7	Variantes de STP	41
3.7.7.1	STP (IEEE 802.1D)	41
3.7.7.2	RSTP (IEEE 802.1w)	41
3.7.7.3	MSTP (IEEE 802.1s)	42
3.7.8	Problèmes courants et dépannage	42
3.7.9	Commandes utiles	43
3.7.10	Glossaire des termes	43

4 ACLs et pare-feu	44
4.1 Les Listes de Contrôle d'Accès (ACLs)	44
4.1.1 Présentation Générale	44
4.1.2 Les Différents Types d'ACLs	44
4.1.2.1 ACL Standard	45
4.1.2.2 ACL Étendue	45
4.1.2.3 ACL Nommée	45
4.1.3 Algorithme de Vérification	45
4.1.4 Masque Générique	46
4.1.5 Configuration des ACLs	46
4.1.5.1 Configuration des ACLs Standards	46
4.1.5.2 Configuration des ACLs Étendues	47
4.1.5.3 Configuration des ACLs Nommées	47
4.1.5.4 Mise en Place et Vérification des ACLs	48
4.1.6 Avantages et Inconvénients des ACLs	48
4.1.6.1 Avantages :	48
4.1.6.2 Inconvénients :	48
4.2 Le pare-feu	49
4.2.1 Définition du pare-feu	49
4.2.2 Évolution des firewalls	49
4.2.3 Exemples de marques et modèles de firewalls	50
4.2.4 Architectures courantes de pare-feu	50
4.2.4.1 Architecture simple	50
4.2.4.2 Architecture sensible (ou complexe)	51
4.2.5 Les différents types de pare-feu	52
4.2.5.1 Pare-feux logiciels	52
4.2.5.2 Pare-feux matériels	52
4.2.6 Les différents types de filtrage	52
4.2.6.1 Filtrage de paquets	53
4.2.6.2 Filtrage applicatif	53
4.3 Pare-feu avec zone démilitarisée (DMZ)	53
5 Conception et Réalisation	55
5.1 Conception	55
5.1.1 Architecture du réseau avec la solution	55
5.1.2 Solutions techniques	57
5.1.3 Synthèse	59
5.1.4 Choix d'Aruba par rapport à Cisco	59
5.2 Réalisation	61
5.2.1 Présentation du logiciel utilisé (GNS3)	61
5.2.2 Installation des périphériques	62
5.2.2.1 FortiGate	62
5.2.2.2 Windows 10	69
5.2.2.3 Switch Aruba	73
5.2.3 Pare-feu	77
5.2.3.1 Accéder au FortiGate	77
5.2.3.2 Création des VLANs du service	79
5.2.3.3 Création du VLAN invité	82

5.2.3.4	Création du VLAN gestion	83
5.2.3.5	Création du VLAN VoIP	85
5.2.3.6	Les VLANs créés	85
5.2.3.7	Routage inter VLAN	87
5.2.3.8	Route statique	89
5.2.3.9	Filtrage web	89
5.2.3.10	Accès à Internet	91
5.2.3.11	Bloquer Facebook via un filtre web	94
5.2.3.12	Izolation du trafic	97
5.2.3.13	Politique créée	98
5.2.3.14	QoS pour VoIP	99
5.2.3.15	Configuration de NTP	103
5.2.4	Accéder à l'interface graphique de ArubaOS-Switch	104
5.2.4.1	Navigation dans l'interface	106
5.2.4.2	Configuration des VLAN	106
5.2.4.3	Vérification	108
5.2.5	Configuration des switch	109
5.2.5.1	Crée les VLANs	109
5.2.5.2	Configuration des Points d'Accès Aruba en Mode Auto-Détection	110
5.2.5.3	Switch du rez-de-chaussée	111
5.2.5.4	Switch du 1 ^{er} étage	112
5.2.5.5	Switch du 2 ^{me} étage	113
5.2.5.6	Explication de la configuration sur chaque Switch	114
5.2.5.7	Configuration de MSTP	116
5.2.5.8	Configuration SSH Sécurisée	119
5.2.5.9	Configuration SNMPv3 Sécurisée	120
5.2.5.10	Configuration Syslog	121
5.2.5.11	Configuration NTP	122
5.2.5.12	Schéma de Flux SNMPv3, SYSLOG, NTP	122
5.2.6	Vérification	123
5.2.6.1	Connectivité entre les VLAN	123
5.2.6.2	Accès à Facebook	125
5.2.6.3	Configuration MSTP	125

INTRODUCTION GÉNÉRALE

Dans un monde de plus en plus interconnecté, les réseaux informatiques constituent le socle des échanges de données au sein des entreprises et des institutions. Cette interconnexion croissante engendre cependant une multiplication des risques liés à la sécurité des systèmes d'information. Les cyberattaques, les intrusions non autorisées, ou encore les logiciels malveillants représentent aujourd'hui des menaces majeures pour l'intégrité, la confidentialité et la disponibilité des informations.

Dans ce contexte, il devient essentiel pour les structures disposant d'un réseau local (LAN) de mettre en place des mesures efficaces de sécurisation, non seulement pour prévenir les attaques, mais aussi pour garantir un fonctionnement optimal et fiable de leurs infrastructures.

C'est dans cette optique que s'inscrit le présent mémoire, qui porte sur la sécurisation d'un réseau local à travers la mise en place de mécanismes de protection tels que les switchs configurés avec des VLANs et les pare-feu, en prenant comme cas d'étude une entreprise publique.

Ce mémoire est réalisé dans le cadre d'un stage au sein de la société SNC RAMELECTRO, spécialisée dans le déploiement de solutions informatiques et réseaux.

Pour bien mener notre travail, on la structuré comme suit : on a commencé par une présentation du contexte d'intervention et des structures concernées, nous aborderons en suite les différentes menaces informatiques et les concepts clés liés à la sécurité réseau. Enfin, nous détaillerons la mise en œuvre des mécanismes de protection (VLAN, pare-feu, filtrage d'accès, etc...) appliqués au réseau local, en mettant l'accent sur leurs impact en termes de performance et de sécurité.

Problématique

Le réseau local actuel de l'entreprise anonyme présente plusieurs vulnérabilités majeures liées à l'absence de segmentation, de mécanismes de sécurité et de redondance. En effet, tous les utilisateurs et services partagent un même réseau plat sans VLAN, favorisant la propagation de malwares, l'exposition des données sensibles et une surcharge en trafic broadcast. De plus, l'absence de réseau sans fil et de solution VoIP limite les possibilités d'évolution et de modernisation des services. Enfin, la non-interconnexion redondante des équipements ainsi que l'absence de configuration du protocole STP exposent le réseau à des risques de pannes et de tempêtes de broadcast.

Dès lors, la problématique principale est la suivante :

Comment concevoir et mettre en œuvre une solution de sécurité adaptée au réseau local de l'entreprise, permettant à la fois de segmenter, sécuriser et assurer la résilience de l'infrastructure, tout en intégrant les services modernes (Wi-Fi, VoIP) nécessaires à son évolution ?

L'objectif principal de ce travail est donc de proposer une démarche pragmatique et structurée pour améliorer renforcer la sécurité d'un réseau local en s'appuyant sur des outils et technologies standards, adaptés au contexte et aux besoins de l'organisation.

CHAPITRE 1

PRÉSENTATION DE L'ORGANISME D'ACCUEIL

Ce chapitre présente le profils de **SNC RAMELECTRO** et présentation du champ d'étude de l'entreprise anonyme.

Nous détaillons d'abord SNC RAMELECTRO (identité, valeurs, projets et méthodes de travail), puis analysons le champ d'étude (Infrastructure informatique, Schéma de réseau et propositions d'amélioration).

Cette étude prépare l'analyse des enjeux techniques et organisationnels abordés dans ce mémoire.

1.1 Présentation de l'entreprise SNC RAMELECTRO

1.1.1 Profil général de la société

1.1.1.1 Nom et raison social de la société

- Raison Sociale : SNC RAMELECTRO AIT RAMDANE ET CIE
- Siège social : Zhun Sud Quartier B ilot 03 Bis local 46, 47, 55, 56 Nouvelle Ville TIZI-OUZOU
- Téléphone : 026.18.24.88/89/90 / Fax : 026.18.24.91
- Mobile : 0561 68 48 62 / 64
- E-mail : ram@ramelectro.dz
- Date de création de la société : 25/08/1998
- siège social est constitué de deux étages d'une superficie de 360m²

1.1.1.2 Domaine d'activité

- Ventes en gros de matériels informatique et de machines de bureau, leurs accessoires et fournitures.
- Installation de réseaux et traitement de données.
- Réparation matériel informatique et bureautique
- Bureau d'étude et de conseil en informatique (consulting).

1.1.2 Les valeurs de l'entreprise

Depuis 27 ans, cette entreprise s'est spécialisée dans l'informatique, développant un savoir-faire solide grâce à la persévérance et l'ambitieux d'y aller de l'avant avec une équipe expérimentée. La réussite repose avant tout sur la collaboration de tous et leurs implication dans une démarche qualité continue à travers des formations, des réunions de sensibilisation et une responsabilisation quotidienne.

Sur le terrain, leur compétence et leur autonomie leur permettent de prendre des décisions rapides, assurant ainsi réactivité et respect des délais. La proximité et la disponibilité des équipes garantissent un service adapté aux besoins des clients.

1.1.2.1 L'innovation technologique

Dans un secteur en constante évolution comme l'informatique, il est facile de perdre le fil ou de faire des choix inadaptés si l'on ne connaît pas les solutions existantes. Pour rester compétitive et réactive dans cet environnement, l'entreprise s'appuie sur une veille technologique rigoureuse afin de disposer d'informations fiables et actualisées pour orienter ses décisions.

Une équipe dédiée est chargée de cette mission. Elle s'informe en permanence à travers plusieurs canaux :

- Échanges réguliers avec les partenaires
- Participation à des séminaires et conférences
- Revue de presse spécialisée et suivi de l'actualité en ligne
- Programmes de formation continue

Grâce à cette démarche, l'entreprise est en mesure de proposer à ses clients des solutions innovantes et adaptées aux évolutions technologiques.

1.1.2.2 L'innovation organisationnelle

Grâce à son expérience dans la réalisation de réseaux de grande envergure, l'entreprise a mis en place un mode opératoire structuré pour l'organisation de ses chantiers.

Ce fonctionnement permet un suivi rigoureux, une traçabilité claire des étapes, et garantit le respect des délais ainsi que des contraintes propres à chaque client.

Pour chaque phase du projet, les responsabilités sont précisément définies, ce qui favorise une coordination efficace. L'information circule de manière organisée, assurant ainsi la bonne exécution des travaux.

1.1.3 Organigramme SNC RAMELECTRO

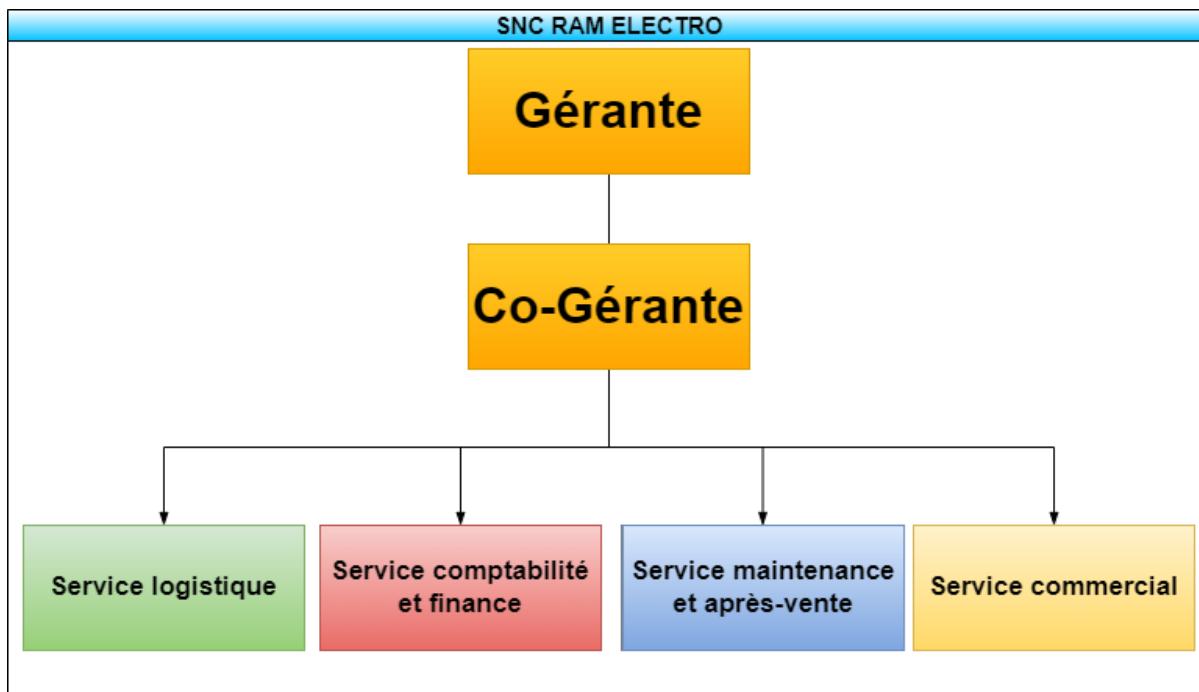


FIGURE 1.1 : Organigramme RAMELECTRO

1.1.4 Références clients

1.1.4.1 Principaux Clients

- Université Abderrahmane-Mira de Béjaïa (Tasdawit n'Bgayet)
- Université Mouloud-Mammeri de Tizi Ouzou **UMMTO** (Tasdawit Lmulud At Memmar)
- Université Saâd Dahlab de Blida
- Université de Ghardaïa
- Université Yahya Fares - Médéa
- Université M'Hamed Bougara de Boumerdès **UMBB**
- Université des Sciences et de la Technologies HOUARI – BOUMEDIENE **USTHB**
- Ministère de l'Intérieur, des Collectivités Locales et de l'Aménagement du Territoire
- Directions de wilayas à travers l'échelle nationale
- Agence Nationale de l'Emploi **ANEM** (direction générale, agence TIZI OUZOU, agence Boumerdes)
- TéléDiffusion d'Algérie **TDA**
- Air Algérie
- Compagnie Algérienne des Assurances **CAAT**
- Caisse Nationale des Assurances Sociales **CNAS**
- Caisse Nationale de Sécurité Sociale des Non-Salariés **CASNOS**
- Algérie Télécom Satellite **ATS**
- Algérie poste

1.1.4.2 Principaux projets réalisés des trois dernières années

- CAAT Direction générale : acquisition de matériel informatique.

Ministère de l'enseignement supérieur et de la recherche scientifique

- Université de bejaia
 1. Réseau informatique au campus El Kseur - **Université de bejaia** : Lot9 (Actif réseau), Lot 11 (Datacenter)
 2. Réseau informatique au pôle de recherche - **Université de béjaia** : Lot1 (réseau), Lot2 (Datacenter), Lot3 (Sécurité).
 3. Équipement en mobilier et matériel du **centre national de recherche en langues et cultures amazighes** - lot 10 : Réseau informatique (actif réseau, firewall et serveurs).
- Université de ghardaïa : extension du réseau intranet de l'université.
- Université de médéa : installation et mise en service du réseau internet au pôle universitaire (8000 places).
- Université des sciences et de la technologie mohamed boudiaf oran : acquisition, installation et mise en service des équipements informatiques au profit des facultés de l'USTOMB pour les travaux pratiques et pédagogiques.
- Université des sciences et de la technologie houari boumediene bab ezzouar : acquisition, avec installation et mise en service, d'équipements scientifiques et informatiques pour le laboratoire de recherche valorisation et recyclage de la matière pour le développement durable Lot N° 05 : matériel informatique.
- Université akli mohand oulhadj bouira : acquisition et installation des équipements pour les laboratoires de langues pour la faculté de lettres et langues de l'université de bouira.

Ministère de l'éducation nationale

- Direction de l'éducation de tizi-ouzou
 1. Renouvellement des équipements scolaires et ses composants pour le cycle secondaire de la wilaya de Tizi-Ouzou.
 2. Renouvellement des équipements scolaires et ses composants pour le cycle moyen de la wilaya de Tizi-Ouzou.
 3. Acquisition des équipements scolaires au profit d'une école primaire au niveau du site 1500 logements LPL à oued falli (Cites D'habitat Intégrées 2017).
 4. Acquisition des équipements scolaires au profit d'une école primaire au niveau du site 1500 logements LPL Au pôle d'excellence wilaya de Tizi-Ouzou (cites d'habitat intégrées 2017).
 5. Acquisition des équipements scolaires au profit d'un Collège au niveau du site 1500 logement LPL pôle d'excellence wilaya de tizi ouzou (cité d'habitat intégrées 2017).
- Centre wilaya d'enseignement et de formation à distance de tizi ouzou : Matériels techniques d'imprimerie, informatique et audiovisuel.

CHAPITRE 1. PRÉSENTATION DE L'ORGANISME D'ACCUEIL

Ministère de la formation et de l'enseignement professionnel

— DEF P Tizi-Ouzou :

1. Acquisition et renouvellement des équipements informatiques, mobiliers de bureau et de climatisation au profit des établissements de la formation professionnelle, **INSFP** : Oued Aissi,Tizi-Ouzou ; Tizi-Ouzou2, Ouaguenoun Et **CFPA** : Talla Allam, K Rachid, Boukhalfa RA, Djemaa Saharidj, Boghni ; Tadmaït, Tigzirt, Larbaa Nath Irathen, Draa El Mizane ,Boukha/Fa A T, Azazga, Draa Ben Khedda, Mechtras, Azeffoune ; Iferhounene.
2. Équipement du siège de la direction de la formation professionnelle avec logement du directeur, matériel informatique et bureautique.
3. Équipement du **CFPA** Ain El Hammam.

— DEF P Bouira : Equipement de l'IEP 1000 PF/300 lits à bouira.

Ministère des finances

- Direction générale du trésor et de la gestion comptable des opérations financières de l'état : Acquisition de matériel informatique.
- Direction des impôts de la wilaya de bejaia : Equipment des centres CPI et CDI des **impôts de bejaïa**.
- Direction des impôts de la wilaya de blida : Equipment des centres CPI et CDI des **impôts blida**.
- Direction des impôts de la wilaya de mostaganem : Equipment des centres CPI et CDI des **impôts mostaganem**.
- Direction des impôts de la wilaya de biskra : Equipment des centres CPI et CDI des **impôts de beskra**.

Ministère du commerce intérieur et de la régulation du marché national

- Centre national du registre du commerce : Acquisition d'équipements et de logiciels informatiques
 1. **CNRC Azazga** : réseau informatique, téléphonique et courant ondulé pour le nouveau siège.
 2. **CNRC Zéralda** : réseau informatique, téléphonique et courant ondulé pour le siège.
- Direction du commerce de la wilaya de tizi ouzou

Ministère de l'intérieur des collectivités locales et de l'aménagement du territoire

- Ministère de l'intérieur : acquisition des équipements informatiques au profit des nouvelles structures de l'administration centrale du ministère.
- APC DRAA BEN KHEDDA : réalisation d'un réseau informatique et équipement informatique pour la numération de l'état civil de l'APC.
- APC FREHA : acquisition d'équipements informatiques.
- APC BOGHNI : acquisition matériels informatiques au siège APC.
- APC Alger centre : fourniture et pose matériel informatique et impression.

CHAPITRE 1. PRÉSENTATION DE L'ORGANISME D'ACCUEIL

Ministère de la jeunesse et des sports

- Direction de la jeunesse et des sports de tizi ouzou
 1. Acquisition Des Equipements Au Profit Des Etablissements Sportifs De Jeunesse en matériel Informatique.
 2. Étude, Réalisation et équipement d'une salle polyvalente à IRDJEN en matériel informatique.
 3. Acquisition des équipements au profit des établissements sportifs de jeunesse et de loisirs : matériel informatique.
- Direction de la jeunesse et des sports de boumerdes : étude, construction et équipement d'une base nautique à Cap Djinet en équipement bureaux
- Direction de la jeunesse et des sports de blida : acquisition des équipements informatiques pour le Centre de Loisir Scientifique de blida.
- direction de la jeunesse et des sports de bouira : étude, réalisation et équipement informatiques d'un centre de loisir et scientifique à bouira.

Ministère du travail, de l'emploi et de la sécurité sociale

- Caisse nationale des retraites
 1. Acquisition de matériel informatique Au profit de l'agence locale CNR de bejaia.
 2. Acquisition de matériel informatique Au profit de l'agence locale CNR de ghardaïa.
- Direction générale de l'ANEM : acquisition d'équipements informatiques.
- CNAS Tizi-Ouzou : acquisition d'équipements informatiques.
- CASNOS Agence tizi ouzou : acquisition du matériel informatique.
- CASNOS Agence alger

Ministère de l'habitat de l'urbanisme et de la ville

- DEP ORAN : acquisition et mise en service de réseaux spécifiques au profit de la cour de justice d'oran, fourniture et pose d'équipements actifs.
- Laboratoire national de l'habitat et de la construction : acquisition de matériel informatique

Ministère de la poste et des télécommunications

- Algérie poste : acquisition d'armoire de brassage au profit des bureaux de poste de la wilaya de tizi ouzou.
- Algérie telecom de bouira : acquisition matériel informatique.
- Algérie telecom satellite (ATS) : acquisition matériel informatique

Ministère de la communication

- Télé diffusion algérie (TDA) : acquisition de matériels informatique et réseau

Ministère des transports

- Air algérie catering (SPA) : fourniture matériels informatiques.
- Sogral SPA : acquisition du matériels et équipements informatique.

Ministère de l'énergie, des mines et des énergies renouvelables

- Agence du service géologique (ASGA) : matériel informatique

1.1.4.3 Projets en cours

- Université de tiaret : extension du réseau intranet et internet de l'université de tiaret - serveurs et sécurité.
- université de souk ahras : renouvellement de matériel réseau de l'ancien pôle à l'université de souk ahras.
- Université de relizane : extension du réseau informatique et traitement des données.
- Observatoire national de la société civile (ONSC) : équipement du siège de l'observatoire national de la société civile. Fourniture, installation et mise en service d'une solution informatique.

1.1.5 Mode opératoire pour réaliser le projet :

1.1.5.1 Descriptif de la solution technique

L'entreprise s'appuie sur son expérience dans le domaine de l'informatique ainsi que sur des partenariats solides avec des fournisseurs reconnus pour proposer à ses clients du matériel fiable et performant.

Le choix des équipements tient compte de plusieurs critères essentiels :

- Collaboration avec des fournisseurs leaders dans leur domaine pour chaque type de produit.
- Intégration des technologies les plus récentes.
- Respect des exigences techniques des clients, avec des performances souvent supérieures aux attentes.
- Exclusion de tout matériel en fin de vie ou proche de l'obsolescence, afin de garantir la durabilité des équipements, la disponibilité des pièces détachées, et un service après-vente de qualité.

1.1.5.2 Moyens organisationnels

Moyens humains

Pour répondre aux besoins variés de ses clients, l'entreprise mobilise une équipe pluridisciplinaire, capable d'intervenir avec autonomie et initiative dans la réalisation des prestations demandées.

Moyens matériels

L'entreprise met à disposition les véhicules et les outils nécessaires à la bonne exécution des travaux. En cas de besoins spécifiques ou d'envergure particulière, elle peut également faire appel à la sous-traitance pour renforcer ses moyens.

Chaque équipe est équipée d'un outillage complet, comprenant aussi bien des outils électroportatifs que l'ensemble des équipements adaptés aux exigences du métier.

1.2 Présentation du champ d'étude (Entreprise publique)

Ce mémoire contient des informations généralisées et des simulations hypothétiques afin de respecter les contraintes de confidentialité imposées par les institutions et organisations concernés. Toute donnée spécifique ou sensible (la structure de l'entreprise et situation informatique) a été omise ou anonymisée pour des raisons de sécurité.

1.2.1 Infrastructure Informatique

L'infrastructure informatique comprend des équipements bureautiques standards, ainsi que des équipements réseaux, l'ensemble assure une connectivité basique via câbles cuivre et fibre optique.

Le tableau 1.1 ci-dessous présente ces différents équipements.

Equipment	Nombre d'équipement
PC	60
Imprimante	20
Commutateurs	3
Pare-feu	1

TABLE 1.1 : Liste des équipements

1.2.2 Schéma de réseau

Le réseau LAN de l'organisme repose sur une architecture structurée, intégrant des équipements modernes pour assurer connectivité, performance et sécurité. Voici l'architecture :

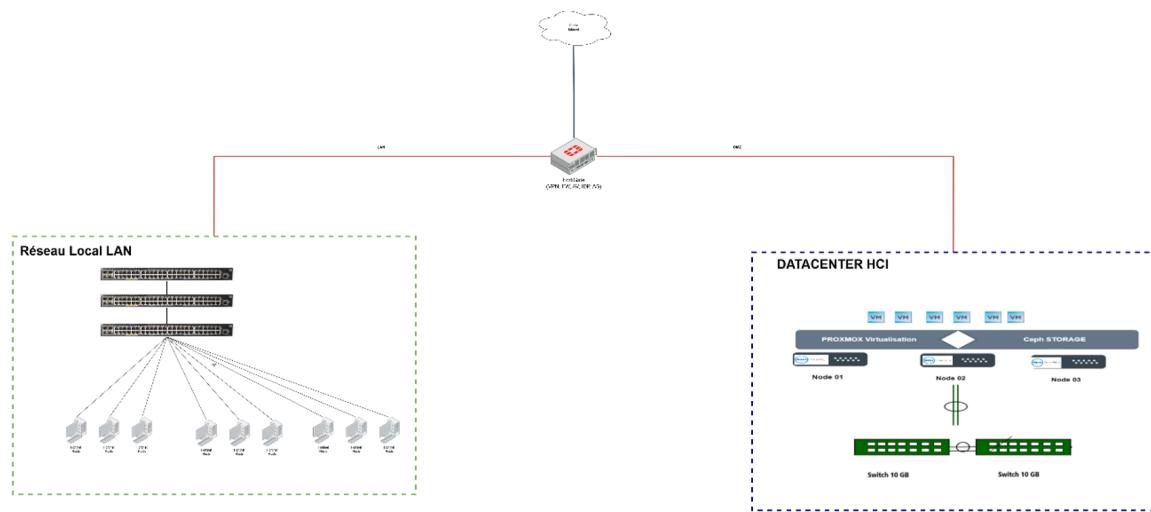


FIGURE 1.2 : Schéma réseau de l'entreprise

Notre étude s'intéresse uniquement sur la partie de réseau local figure 1.3, est non pas de datacenter.

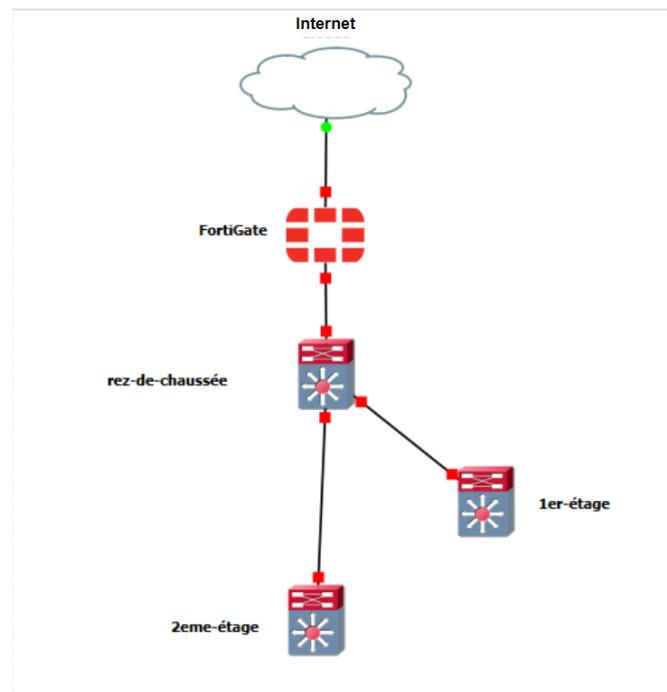


FIGURE 1.3 : Partie réseau étudié

1.2.3 Analyse et amélioration du réseau local

Notre étude se limite au réseau local (LAN) et ne prend pas en compte les infrastructures de centres de données HCI (Hyper-Converged Infrastructure).

1.2.3.1 Les critiques

Après une analyse approfondie du réseau local actuel, les principales lacunes identifiées sont :

- Tous les utilisateurs et services sur le même réseau plat (partage le même domaine de diffusion), ce qui engendre les conséquences suivantes :
 - Propagation facilitée des virus/malwares
 - Exposition des données sensibles
 - Trafic broadcast excessif
- Absence complète de réseau sans fil
- Pas de solution VoIP déployée
- Les switchs Aruba de 1er et 2ème étages ne sont pas interconnectés par une liaison redondante
- Aucune configuration STP (Spanning Tree Protocol) en place. Risque de tempêtes de broadcast en cas d'ajout de liens redondants

1.2.3.2 Solutions proposées

- Segmenter le réseau LAN en VLANs ;
- Routage inter-VLAN via sous-interfaces dans le fortigate ;
- Services DHCP/DNS centralisés ;
- Déploiement du réseau sans fil (Wi-Fi) ;
- Déploiement de solution VoIP ;
- Ajout d'une liaison redondante entre les switchs des 1er et 2ème étages ;
- Configuration du MSTP (Multiple Spanning Tree Protocol) ;
- Filtrage avancé des flux dans le FortiGate ;
- Politiques de sécurité ;
- Supervision et synchronisation.

Conclusion

Ce chapitre a permis de décrire **SNC RAMELECTRO** (son activité et ses innovations) et d'examiner le champ d'étude (son réseau et ses axes d'optimisation).

Ces éléments servent de base pour les analyses ultérieures, notamment les solutions proposées pour moderniser l'infrastructure de réseau local.

La suite du mémoire approfondira ces pistes d'amélioration.

CHAPITRE 2

LA SÉCURITÉ INFORMATIQUE

Ce chapitre introduit les notions fondamentales de la sécurité informatique. Nous y abordons les menaces, les risques et les actions malveillantes susceptibles d'affecter les systèmes d'information. Nous présenterons également les différentes techniques et méthodes permettant d'assurer leur protection. Toutes ces informations proviennent de la référence [16], et pour approfondir ce domaine, nous vous proposons ces livres [5], [11], [7], [10], [13], [4] et la référence [3].

2.1 Sécurité d'un réseau

La sécurité d'un réseau consiste à garantir que l'ensemble des machines communiquent de manière fiable et que chaque utilisateur dispose uniquement des droits qui lui sont octroyés.

Les objectifs de la sécurité informatique sont les suivants :

- **Prévention** : mettre en œuvre des mesures pour empêcher les attaques ;
- **Détection** : identifier les attaques, déterminer leurs origines, leurs natures et les ressources affectées ;
- **Réaction** : appliquer des contre-mesures pour restaurer les systèmes et limiter l'impact des attaques.

2.1.1 Les causes de l'insécurité

Deux grandes formes d'insécurité peuvent être distinguées :

- (A) **Insécurité active** : c'est la non-connaissance par l'utilisateur des fonctionnalités du système, dont certaines pouvant lui être nuisible (par exemple la non désactivation de services réseaux non nécessaires à l'utilisateur).
- (B) **Insécurité passive** : c'est lorsque l'administrateur (ou l'utilisateur) d'un système ne connaît pas les dispositifs de sécurité dont il dispose.

2.1.2 Les services de sécurité

Un service de sécurité a pour but de renforcer la protection des échanges de données et des traitements informatiques. Il repose sur des mécanismes techniques spécifiques.

On distingue cinq grands services de sécurité, que l'on peut déployer selon les besoins de l'organisation :

- **Authentification** : vérifie l'identité des acteurs de la communication.
Mécanismes utilisés : cryptage, signature numérique, notarisation.
- **Confidentialité** : protège les données contre tout accès non autorisé.
Mécanisme utilisé : cryptage.
- **Intégrité des données** : garantit que les données n'ont pas été altérées.
Mécanismes utilisés : cryptage, signature numérique, contrôle d'accès, contrôle d'intégrité.
- **Non-répudiation** : empêche un acteur de nier avoir envoyé ou reçu un message.
Mécanismes utilisés : signature numérique, notarisation.
- **Disponibilité** : assure que les utilisateurs autorisés peuvent accéder aux ressources en toute fiabilité.
Mécanismes utilisés : filtrage (pare-feu), antivirus, contrôle d'accès.

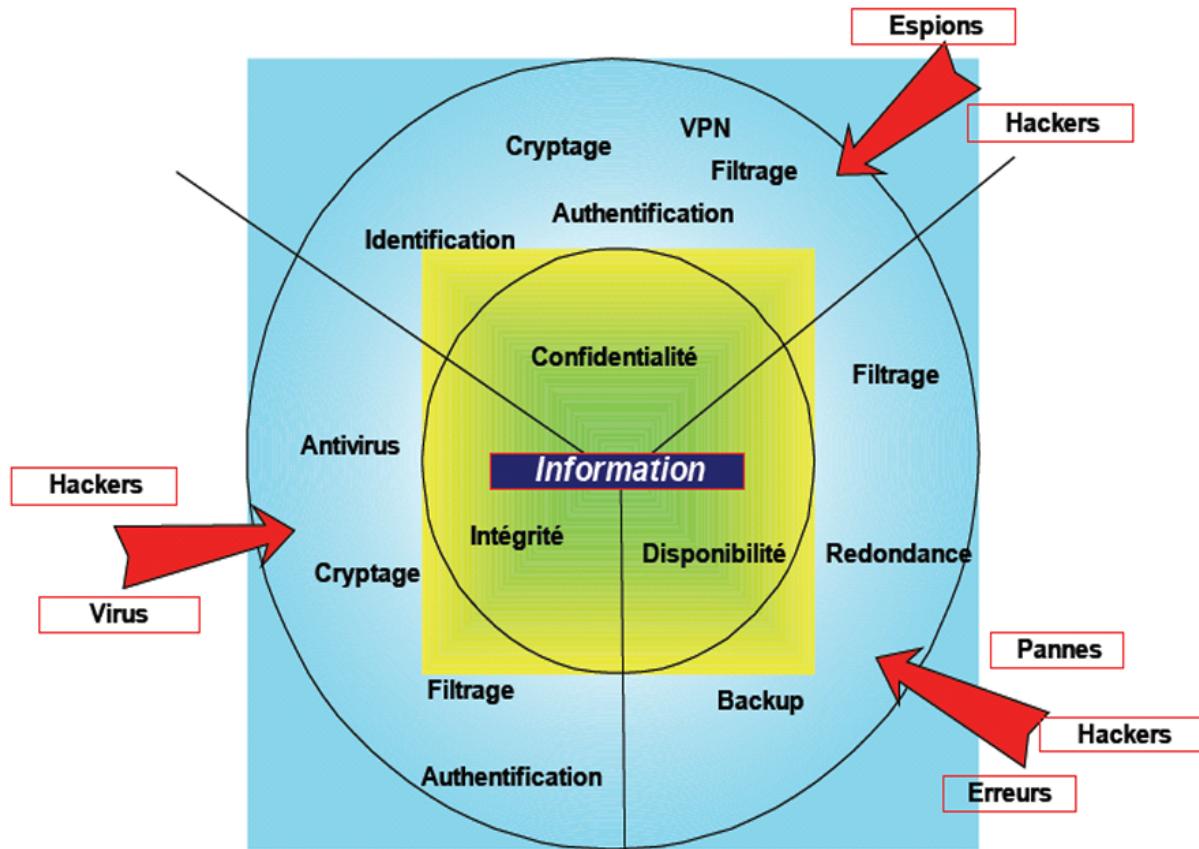


FIGURE 2.1 : Les objectifs de la sécurité informatique

2.2 Les pirates informatiques

À l'origine, le terme *hacker*, issu de l'anglais, signifie « bricoleur » ou « bidouilleur ». En informatique, il désigne des programmeurs ingénieux dotés de compétences techniques

élevées. Les hackers sont généralement des passionnés, curieux, et avides de connaissances, n'hésitant pas à explorer les limites des systèmes.

Ils sont souvent capables de détourner un logiciel ou un dispositif de son usage initial, dans le but de découvrir des informations ou des fonctionnalités auxquelles ils ne sont normalement pas censés accéder. Le hacking ne se résume donc pas à la programmation : il reflète un véritable état d'esprit.

Les hackers cultivent souvent une connaissance approfondie de leur domaine, de son histoire, de ses figures emblématiques, et de son évolution technique et sociale. Le jargon informatique les classe en plusieurs catégories selon leurs intentions, leurs compétences et leur respect (ou non) de la légalité. Cette classification s'inspire des westerns : les héros portent des chapeaux blancs, les antagonistes des chapeaux noirs.

- **White hats (chapeaux blancs)** : Ce sont des professionnels de la sécurité (consultants, administrateurs réseau...) qui réalisent des tests d'intrusion de manière légale et encadrée, dans le but d'identifier les failles de sécurité. Certains white hats peuvent agir sans autorisation, mais toujours avec une intention préventive.
- **Blue hats (chapeaux bleus)** : Il s'agit de spécialistes chargés de détecter et corriger des failles avant le déploiement d'un système (site web, logiciel, OS). Microsoft utilise ce terme pour désigner ses ingénieurs en cybersécurité.
- **Black hats (chapeaux noirs)** : Ce sont les pirates malveillants — créateurs de virus, cybercriminels, cyberespions — qui agissent illégalement dans le but de nuire, de voler des données ou de tirer un profit financier.
- **Grey hats (chapeaux gris)** : Ils opèrent à la frontière de la légalité. Ils peuvent s'introduire dans un système sans autorisation, sans intention malveillante. Leur motivation est souvent technique : prouver qu'ils en sont capables. Cependant, leurs actions restent juridiquement répréhensibles.
- **Script kiddies (ou lamers)** : Utilisateurs peu qualifiés qui se servent de programmes créés par d'autres pour lancer des attaques. Leur manque de compréhension profonde les distingue des véritables hackers.
- **Hacktivistes** : Hackers motivés par des causes politiques ou sociales. Ils utilisent le piratage pour attaquer ou perturber des organisations, notamment des gouvernements, dans une logique militante.

2.3 Malveillance informatique

Les attaques contre les systèmes d'information prennent de nombreuses formes, mais une attention particulière doit être portée aux logiciels malveillants (ou *malware*), un terme anglophone désignant des programmes conçus pour nuire. Ces programmes se propagent principalement via les réseaux : par accès direct à une machine, par courriel, sites web piégés, ou encore par des supports amovibles (clé USB, CD-ROM...).

Leur objectif est d'infiltrer un système, d'y causer des dommages et souvent de se propager à d'autres machines.

2.3.1 Logiciels malveillants

2.3.1.1 Virus

Un virus est un programme qui se réplique lui-même, en s'insérant dans d'autres fichiers exécutables ou systèmes. Il peut ralentir le système, corrompre ou supprimer des données. Certains virus envoient même des informations confidentielles par e-mail à l'insu de l'utilisateur. Même lorsqu'ils ne causent pas de dégâts directs, leur propagation peut affecter les performances globales du système.

2.3.1.2 Vers

Les vers sont des programmes autonomes capables de se propager sans intervention humaine. Ils utilisent généralement les pièces jointes d'e-mails ou les failles de sécurité pour s'infiltrer. Ils recherchent ensuite des adresses e-mail ou fichiers pour s'envoyer automatiquement à d'autres cibles, usurpant souvent l'identité de l'expéditeur. Leur principal impact est de saturer les réseaux et ralentir les performances des systèmes.

2.3.1.3 Chevaux de Troie

Les chevaux de Troie se cachent dans des programmes apparemment inoffensifs. Une fois activés, ils ouvrent une brèche dans le système, permettant à un pirate d'y accéder. Contrairement aux virus ou vers, ils ne se propagent pas par eux-mêmes mais sont souvent introduits via des téléchargements, e-mails piégés ou autres malwares.

2.3.1.4 Portes dérobées (Backdoors)

Une porte dérobée est un programme furtif souvent installé par un cheval de Troie, qui permet à un attaquant de contrôler l'ordinateur à distance via le réseau, sans que l'utilisateur n'en soit conscient.

2.3.1.5 Bombes logiques

Il s'agit de fonctionnalités malveillantes dissimulées dans un logiciel, qui se déclenchent à une date ou condition précise (ex. : ouverture d'un fichier, arrivée à une date). Elles peuvent supprimer des fichiers, ralentir un système ou causer d'autres perturbations.

2.3.1.6 Logiciels espions (Spyware)

Ces programmes recueillent des informations personnelles à l'insu de l'utilisateur (historique de navigation, frappes clavier, etc.) ou modifient le comportement du système (changement de page d'accueil, pop-ups publicitaires). Ils s'installent souvent en parallèle d'autres logiciels gratuits ou lors de la visite de certains sites web.

2.3.2 Courrier électronique non sollicité (Spam)

Le *spam* désigne des messages électroniques non sollicités, le plus souvent à but publicitaire, envoyés massivement à des utilisateurs. Leur coût d'envoi très faible encourage les spameurs à inonder les boîtes mail, ce qui engendre une surcharge des serveurs, un gaspillage de bande passante, et une gêne pour les utilisateurs. Ils peuvent également contenir des liens vers des logiciels malveillants.

2.3.3 Injection SQL (SQLi)

L'injection SQL est une technique qui consiste à exploiter une faille dans une application interagissant avec une base de données, permettant d'exécuter des requêtes non autorisées. Il existe plusieurs types d'injection SQL :

- **Blind-based SQLi** : l'attaquant envoie des requêtes modifiées et déduit les données caractère par caractère selon les réponses (ou absences de réponse) du serveur.
- **Error-based SQLi** : utilise les messages d'erreur retournés par le serveur pour extraire des informations de la base de données.
- **Union-based SQLi** : exploite la commande SQL UNION pour récupérer en une seule fois un grand volume de données.
- **Stacked queries** : permet d'exécuter plusieurs requêtes successives ; la plus dangereuse car elle permet des modifications complètes de la base si la configuration le permet.

2.4 Les attaques réseau

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Une **attaque** est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel, ou même erreur humaine) à des fins non autorisées. On peut classer les attaques réseau selon leurs objectifs.

2.4.1 Attaques de découverte du réseau

Ces attaques visent à analyser l'architecture du réseau cible pour en identifier les composants.

- **Cartographie du réseau** : l'outil traceroute permet de découvrir les routeurs intermédiaires grâce à l'exploitation du champ TTL des paquets IP qui déclenche des réponses ICMP time_exceeded.
- **Balayage TCP (TCP Scan)** : consiste à envoyer des requêtes TCP SYN à différents ports. Une réponse SYN (Synchronize)/ACK (Acknowledgment) signifie que le port est ouvert, tandis qu'une réponse RST (Reset) signifie que le port est fermé.

2.4.2 Attaques d'écoute du trafic réseau

Ces attaques permettent à un attaquant d'intercepter des données sensibles comme des mots de passe.

- **Sniffing** : sur un réseau Ethernet en mode broadcast, les trames sont visibles par toutes les interfaces. Des outils comme Wireshark ou TCPDump permettent de capturer et analyser ces trames.
- **Attaque de commutateur** : des techniques comme le VLAN hopping ou l'ARP spoofing permettent de casser la séparation entre VLANs. Par exemple, en envoyant des trames 802.1q falsifiées, un attaquant peut forcer un port à se comporter comme un port trunk.

2.4.3 Attaques d’interférence avec une session réseau

Ce type d’attaque vise à intercepter ou perturber les communications établies entre deux hôtes d’un réseau. Les attaquants cherchent à se faire passer pour l’un des correspondants afin de manipuler, observer ou détourner les échanges. Deux techniques majeures dans ce domaine sont l’ARP Spoofing et l’IP Spoofing.

2.4.3.1 ARP Spoofing

ARP Spoofing (ou empoisonnement ARP), cette attaque cible le protocole ARP (Address Resolution Protocol) , utilisé dans les réseaux locaux pour associer une adresse IP à une adresse MAC (niveau 2) . L’attaquant envoie des paquets ARP falsifiés sur le réseau, faisant croire à la victime que l’adresse IP de la passerelle (ou d’un autre hôte) correspond à sa propre adresse MAC. Cela provoque une redirection du trafic réseau vers l’attaquant.

Aspect	Description
Objectif	Intercepter, modifier ou bloquer le trafic réseau échangé entre deux machines (souvent entre une victime et une passerelle réseau).
Méthode	En injectant de fausses réponses ARP (sans requête préalable), l’attaquant empoisonne le cache ARP des machines cibles.
Conséquences	Une fois le trafic redirigé vers lui, l’attaquant peut : <ul style="list-style-type: none">— Mettre en œuvre une attaque <i>Man-in-the-Middle</i> (MITM),— Enregistrer des mots de passe,— Injecter du contenu malveillant,— Effectuer un déni de service (DoS) .
Exemple	Si la victime veut envoyer un paquet à la passerelle (ex : 192.168.1.1), elle consulte son cache ARP pour obtenir l’adresse MAC. Si le cache est empoisonné, le paquet sera envoyé à l’attaquant, qui peut ensuite le transmettre à la vraie passerelle (attaque transparente).

TABLE 2.1 : ARP Poisoning (ARP Spoofing)

2.4.3.2 IP Spoofing

IP Spoofing (ou usurpation IP), cette technique consiste à modifier l’adresse IP source d’un paquet IP pour se faire passer pour un autre hôte. Cela peut permettre à l’attaquant de contourner des mécanismes de sécurité basés sur les adresses IP, ou de tromper un système cible en se faisant passer pour une source de confiance.

Aspect	Description
Objectif	Accéder à des ressources protégées, brouiller l'origine d'une attaque, ou injecter des paquets dans une communication existante.
Méthode	L'attaquant forge manuellement les paquets IP (en utilisant des outils comme Scapy ou hping) avec une adresse source falsifiée. Dans le cas d'une communication bidirectionnelle, le spoofing est plus difficile car la victime envoie les réponses à l'adresse usurpée (et non à l'attaquant).
Conséquences	Cette technique est fréquemment utilisée dans les attaques par déni de service distribué (DDoS), rendant difficile l'identification de l'origine des paquets malveillants. Elle peut aussi être utilisée dans certaines attaques plus sophistiquées comme le <i>TCP Session Hijacking</i> .
Limite	Dans les communications nécessitant une réponse (comme TCP), le spoofing ne permet pas à l'attaquant de recevoir les réponses du serveur à moins qu'il n'ait aussi compromis le routage.

TABLE 2.2 : IP Spoofing (Usurpation d'adresse IP)

2.4.4 Attaques par déni de service (DoS)

- **Attaque Smurf** : envoie de requêtes ICMP echo avec l'adresse source de la victime vers une adresse de diffusion, ce qui provoque un flot de réponses vers la victime.
- **DDoS (Distributed Denial of Service)** : l'attaquant utilise un réseau de machines compromises (bots) pour submerger la cible via un serveur de commande.

2.4.5 Attaques sur les protocoles de routage

Ces attaques visent à détourner ou perturber le trafic réseau.

- **Black Hole** : un routeur malveillant annonce des routes inexistantes à faible coût.
- **Man-in-the-middle (MITM)** : l'attaquant se place entre deux hôtes en annonçant des routes attrayantes, intercepte ou modifie les paquets.
- **Numéro de séquence maximal (OSPF)** : en envoyant un LSA avec un numéro de séquence élevé, un pirate force les routeurs à mettre à jour leur table avec des informations falsifiées.

2.4.6 Attaques sur les accès Wi-Fi

- **Bit Flipping (modification de paquet)** : le protocole WEP utilise un checksum linéaire, ce qui permet de modifier un paquet chiffré (et son checksum) sans que le récepteur ne détecte l'altération.
- **Redirection d'adresse IP** : en modifiant un paquet capturé pour rediriger la destination vers un ordinateur contrôlé, le pirate obtient une version en clair du paquet après déchiffrement, permettant une attaque par texte clair connu.

2.5 Mécanismes de Sécurité

2.5.1 Sécurité Physique

La sécurité physique constitue la première barrière de protection du système d'information. Elle repose principalement sur le contrôle strict des accès aux locaux techniques grâce à des systèmes d'identification (badges, biométrie), la sécurisation des salles serveurs et des baies réseau, ainsi que la protection contre le vol ou les manipulations non autorisées des équipements. Ces mesures garantissent l'intégrité physique des infrastructures critiques.

2.5.2 Protection des Accès

La protection logique des accès réseau complète la sécurité physique en établissant plusieurs lignes de défense. Elle implique la définition de périmètres de sécurité clairs, la réduction des points d'entrée au réseau, et l'implémentation de solutions techniques comme les pare-feux, les systèmes de détection d'intrusion et des mécanismes d'authentification renforcée. La journalisation systématique des activités permet par ailleurs le suivi et l'analyse des incidents de sécurité.

2.5.3 Les pare-feu

Un **pare-feu** (ou firewall) est un système matériel ou logiciel qui filtre le trafic réseau selon un ensemble de règles prédéfinies. Il détermine quelles communications sont autorisées ou bloquées, en fonction de l'origine, de la destination, du protocole utilisé ou encore du port concerné.

Lorsqu'un ordinateur communique via Internet, les données circulent par des *ports* logiques. Chaque machine peut utiliser jusqu'à 65 536 ports pour établir ou recevoir des connexions. Ces ports constituent autant de points d'entrée potentiels pour des attaques.

Sans dispositif de filtrage, un attaquant pourrait facilement :

- scanner les ports ouverts,
- injecter des logiciels malveillants,
- détourner des communications sensibles.

2.5.4 Accès à distance sécurisé SSH (Secure Shell)

Le protocole SSH est une version sécurisée des anciens outils de connexion à distance comme `rlogin` ou `RSH`. Fonctionnant au niveau de la couche application du modèle OSI , il permet d'établir une session distante chiffrée avec une machine cible via un terminal.

SSH repose sur la couche TCP pour transporter les données, mais y ajoute des mécanismes de cryptographie (chiffrement, authentification, intégrité). Ce protocole est devenu la norme pour les connexions distantes sécurisées dans les environnements professionnels.

2.5.5 Les VPN (Réseaux Privés Virtuels)

Un VPN (Virtual Private Network) permet d'établir un tunnel sécurisé entre deux points distants, même si ceux-ci sont reliés par un réseau non fiable comme Internet. Les

données échangées sont alors encapsulées et chiffrées, empêchant leur interception ou leur modification par des tiers.

Les VPN sont particulièrement utiles pour :

- connecter des sites distants d'une entreprise,
- permettre aux employés d'accéder au réseau interne depuis l'extérieur,
- garantir la confidentialité des échanges.

2.5.6 Les antivirus

Les antivirus sont des programmes conçus pour détecter, neutraliser et, si possible, supprimer les logiciels malveillants (virus, vers, chevaux de Troie, etc.). Lorsqu'un fichier infecté est détecté, l'antivirus tente d'en extraire le virus tout en préservant l'intégrité du fichier original.

Cependant, certaines infections peuvent être trop profondes pour un nettoyage complet ; dans ce cas, la suppression du fichier est parfois nécessaire.

2.6 Sécurité des équipements réseau

La protection d'un réseau repose aussi sur la sécurisation de ses équipements physiques et logiciels. Trois axes principaux doivent être considérés :

2.6.1 Sécurité physique

Elle consiste à protéger les équipements réseau contre les risques environnementaux tels que :

- incendies,
- inondations,
- coupures d'électricité.

Des dispositifs comme les onduleurs, les extincteurs ou les climatiseurs de salle serveur contribuent à cette protection.

2.6.2 Sécurité du système d'exploitation

Les routeurs, commutateurs ou serveurs réseau fonctionnent souvent avec des systèmes d'exploitation spécialisés. Il est essentiel de :

- appliquer des mises à jour régulières,
- corriger les vulnérabilités détectées,
- effectuer des tests de sécurité et de non-régression.

2.6.3 Sécurité logique

Elle concerne la bonne configuration des équipements réseau. Une mauvaise configuration (ex : ports ouverts inutilement, protocoles activés par défaut) peut exposer le réseau à des attaques. Il est donc recommandé de :

- désactiver les services inutiles,

- utiliser des mots de passe forts,
- appliquer des règles de filtrage rigoureuses.

Même si la sécurité du système d'exploitation peut être difficile à maîtriser (souvent à cause de logiciels propriétaires), la sécurité physique et logique doit être traitée avec une attention particulière.

Le pare-feu agit alors comme un douanier numérique : il surveille les flux entrants et sortants, bloque les tentatives suspectes et autorise uniquement les échanges conformes à la politique de sécurité définie.

2.7 Assurer la confidentialité des connexions

La protection des données en transit sur un réseau repose principalement sur le chiffrement. Le chiffrement garantit que seuls les interlocuteurs autorisés peuvent lire ou interpréter les informations échangées. Cette technique est essentielle pour préserver la confidentialité dans les communications numériques.

2.7.1 Algorithmes cryptographiques

La cryptographie est un ensemble de méthodes mathématiques, de logiciels et de dispositifs matériels visant à sécuriser les échanges d'informations. Elle repose sur la transformation de messages lisibles (*texte clair*) en messages inintelligibles (*texte chiffré*), lisibles uniquement par les destinataires autorisés.

La cryptographie moderne, fondée sur des principes mathématiques solides, offre des garanties de sécurité élevées, notamment contre l'interception, la falsification ou l'usurpation d'identité.

Les principaux objectifs de la cryptographie sont :

1. **Confidentialité** : garantir que seuls les destinataires autorisés peuvent accéder au contenu du message.
2. **Authentification** : permettre aux parties impliquées de prouver leur identité mutuelle.
3. **Intégrité des données** : assurer que le message n'a pas été altéré pendant son transfert.
4. **Non-répudiation** : empêcher l'émetteur de nier avoir envoyé un message donné.

2.7.1.1 Cryptographie symétrique (à clé secrète)

La cryptographie symétrique utilise une seule clé secrète, partagée entre l'émetteur et le récepteur, pour chiffrer et déchiffrer les données.

- La même clé est utilisée dans les deux sens (émission et réception).
- La transmission sécurisée de cette clé est cruciale.
- Les algorithmes symétriques (comme AES ou DES) sont généralement rapides et performants.
- Les clés sont relativement courtes.
- Cependant, pour n utilisateurs souhaitant communiquer entre eux, il faut $\frac{n(n-1)}{2}$ clés différentes, ce qui rend la gestion complexe à grande échelle.

2.7.1.2 Cryptographie asymétrique (à clé publique)

La cryptographie asymétrique repose sur une paire de clés distinctes :

- Une **clé publique**, utilisée pour chiffrer les données, est librement distribuée.
- Une **clé privée**, utilisée pour déchiffrer les données, est conservée secrète par son propriétaire.

Avantages de ce système :

- La gestion des clés est simplifiée : seule la clé publique circule, la clé privée reste protégée.
- Il n'est plus nécessaire de transmettre une clé secrète à chaque correspondant.
- Ce type de chiffrement est idéal pour les signatures électroniques et la vérification d'identité.

Inconvénients :

- Les algorithmes asymétriques (comme RSA ou ECC) sont plus lents que les algorithmes symétriques.
- Les longueurs de clés sont plus importantes pour assurer un niveau de sécurité équivalent.

2.7.2 Certificats numériques

Les certificats numériques pallient les limites de la simple vérification de signature en authentifiant l'identité associée à une paire de clés cryptographiques. Émis par une autorité de certification (CA) tierce de confiance, ces fichiers électroniques lient de manière fiable une identité (personne ou organisation) à sa clé publique.

Un certificat comprend essentiellement : un identifiant unique, les informations du titulaire, sa clé publique, les références de l'autorité émettrice, sa signature numérique, ainsi que des métadonnées comme la période de validité. La **CA** garantit ainsi à la fois l'identité du détenteur et l'authenticité de la clé publique, établissant une chaîne de confiance essentielle pour les échanges sécurisés.

2.7.3 Fonctions de hachage

Les fonctions de hachage sont des algorithmes cryptographiques qui transforment des données de taille variable en une empreinte numérique fixe (condensat). Leur caractère irréversible empêche toute reconstruction des données originales à partir du hachage, tandis que leur résistance aux collisions garantit l'unicité statistique des empreintes.

En sécurité informatique, ces fonctions vérifient l'intégrité des données via un processus simple : l'émetteur génère et joint l'empreinte (ex : SHA-256) du message, que le destinataire recalcule pour comparer avec la valeur reçue. Une correspondance valide l'absence d'altération. Parmi les implémentations courantes, on trouve MD5, SHA-1 et SHA-256, ce dernier offrant actuellement le meilleur niveau de sécurité.

2.8 La surveillance réseau

Une bonne sécurisation du réseau passe par une gestion rigoureuse de tous les services d'infrastructure. En effet, nombre d'attaques peuvent être évitées si les services de gestion réseau sont correctement protégés et configurés.

La gestion sécurisée du réseau concerne plusieurs aspects essentiels :

- **Routage sécurisé** : garantir que les informations de routage ne puissent être manipulées par des entités non autorisées.
- **Supervision et journalisation** : surveiller en permanence l'état du réseau et enregistrer les événements importants.
- **Résolution des noms de domaine (DNS)** : empêcher les détournements ou falsifications de réponses DNS.
- **Synchronisation des horloges (NTP)** : s'assurer que tous les équipements réseau disposent d'une heure correcte pour éviter les erreurs de journalisation et faciliter les audits de sécurité.
- **Simple Network Management Protocol (SNMP)** : en français « *protocole simple de gestion de réseau* », est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.

Une gestion centralisée, sécurisée et bien documentée de ces services constitue un pilier fondamental pour garantir la résilience d'un système d'information.

Conclusion

Dans ce chapitre on a expliquer les différents attaques réseau qui exploitent diverses faiblesses, mais des contre-mesures existent pour les prévenir ou en limiter l'impact. Une approche proactive combinant prévention, détection et réaction est essentielle pour assurer la sécurité des systèmes.

CHAPITRE 3

LA SÉCURITÉ DANS LES SWITCH

Introduction

Les commutateurs sont au cœur des réseaux locaux (LAN), garantissant une communication fluide tout en étant exposés à des risques comme les boucles réseau ou les accès non autorisés. Ce chapitre explore les mécanismes essentiels pour sécuriser et optimiser ces réseaux, en abordant la définition des LAN, les réseaux virtuels (VLAN), les trunks, le protocole VTP et le protocole Spanning-Tree (STP) avec ses variantes. L'objectif est de fournir une vue d'ensemble des outils permettant de renforcer la sécurité et la résilience des réseaux commutés.

3.1 Définition d'un réseau local (LAN)

Un **réseau local** (Local Area Network) désigne une infrastructure réseau limitée géographiquement à un site unique. Ses particularités incluent :

- Des débits élevés entre équipements connectés
- Une absence de coût de transit via des opérateurs externes
- Une administration centralisée

Remarque : Bien que local, un LAN peut couvrir une zone étendue. La segmentation en sous-réseaux devient nécessaire au-delà d'un certain nombre d'appareils connectés.

3.2 Les réseaux locaux virtuels

3.2.1 Concept fondamental d'un VLAN

Un Réseau Local Virtuel VLAN (Virtual Local Area Network) est un réseau local regroupant un ensemble de machines de façon logique et non physique. Pour plus d'informations sur les VLAN, consultez le livre [12].

Les VLANs (Virtual LANs) permettent de :

- Créer des réseaux logiques indépendants de la topologie physique
- Segmenter un réseau existant sans modification matérielle

- Isoler des groupes de machines selon divers critères (fonction, sécurité, etc.)

3.2.2 Avantages clés des VLANs

- **Performance réseau améliorée :**
 - Réduction significative des domaines de broadcast (diffusion) grâce à la segmentation logique
 - Diminution des collisions et du trafic superflu sur les ports non concernés
 - Exemple : Dans un réseau de 200 machines sans VLAN, un broadcast atteint tous les équipements. Avec 4 VLANs de 50 machines, le trafic broadcast est réduit de 75%.
- **Flexibilité organisationnelle :**
 - Reconfiguration dynamique sans intervention sur le câblage physique
 - Possibilité de regrouper des utilisateurs par fonction plutôt que par localisation
 - Exemple : Déplacer un utilisateur du VLAN "Comptabilité" au VLAN "Marketing" en quelques commandes CLI
- **Sécurité renforcée :**
 - Isolation des flux sensibles entre VLANs (nécessite un routeur ou L3 Switch pour communiquer)
 - Implémentation plus facile des politiques de sécurité par groupe fonctionnel
 - Exemple : Le VLAN "Administration" peut être configuré pour n'accepter que du trafic chiffré
- **Efficacité économique :**
 - Réduction du nombre de commutateurs physiques nécessaires
 - Optimisation de l'utilisation de la bande passante existante
 - Exemple : Un seul switch 48 ports peut héberger 4 VLANs distincts au lieu d'acheter 4 switches séparés

3.2.3 Cas d'usage typique en entreprise

- **Gestion de projets transversaux :**
 - Création de VLANs temporaires pour des équipes projet inter-départements
 - Durée de vie alignée sur le projet (ex : VLAN "ProjetX" actif 6 mois)
 - Configuration type : Accès limité aux ressources partagées du projet
- **Isolation des services critiques :**
 - VLAN dédié aux systèmes financiers avec politiques d'accès strictes
 - VLAN séparé pour l'infrastructure RH avec journalisation avancée
 - Exemple : Switch Cisco configuré avec VACL pour filtrer le trafic vers le VLAN "Finances"
- **Réseau invité sécurisé :**
 - VLAN invité avec accès Internet uniquement (pas d'accès au réseau interne)
 - Limitation de bande passante et filtrage de contenu
 - Configuration type : Authentification 802.1X pour les accès invités

- Gestion des accès par rôle :
 - VLAN "Enseignants" et "Étudiants" dans un campus universitaire
 - VLAN "IoT" pour les objets connectés avec restrictions spécifiques
 - Exemple : Politiques QoS différentes entre VLAN "VoIP" (prioritaire) et VLAN "Web"
- Conformité réglementaire :
 - Segmentation pour répondre aux exigences PCI-DSS (cartes de crédit)
 - Isolation des systèmes de santé pour HIPAA aux États-Unis
 - VLAN dédié aux systèmes de supervision conforme à la norme ISO 27001

3.3 Types de VLANs et leurs Configurations

Il existe quatre principales catégories de VLANs : les VLANs de données, les VLANs par défaut et les VLANs natifs. Ci-dessous, nous détaillons chaque type avec des exemples de configuration pour un commutateur ArubaOS-Switch 2930F et un commutateur Cisco.

3.3.1 VLAN de données

Un VLAN de données est conçu pour transporter le trafic généré par les utilisateurs. Il est distinct des VLANs dédiés au trafic de voix ou de gestion, car il est recommandé de séparer ces types de trafic. Ce type de VLAN, parfois appelé VLAN utilisateur, permet de segmenter le réseau en groupes d'utilisateurs ou d'appareils.

3.3.1.1 Configuration sur ArubaOS-Switch

```
1     configure
2       vlan 10
3         name "DATA_VLAN"
4         untagged 1
5         no ip address
6         exit
7       write memory
```

Listing 3.1: Configuration VLAN de données sur ArubaOS-Switch

3.3.1.2 Configuration sur Cisco

```
1     configure terminal
2       vlan 10
3         name DATA_VLAN
4         exit
5       interface GigabitEthernet0/1
6         switchport mode access
7         switchport access vlan 10
8         spanning-tree portfast
9         exit
10        write memory
```

Listing 3.2: Configuration VLAN de données sur Cisco

3.3.2 VLAN par défaut

Sur les commutateurs Cisco et Aruba, le VLAN par défaut est le VLAN 1. Ce VLAN ne peut être ni renommé ni supprimé. Par défaut, tout le trafic de contrôle de couche 2 est associé au VLAN 1.

3.3.2.1 Configuration sur ArubaOS-Switch

```
1  configure
2  vlan 1
3  name "DEFAULT_VLAN"
4  untagged 2
5  no ip address
6  exit
7  write memory
```

Listing 3.3: Configuration VLAN par défaut sur ArubaOS-Switch

3.3.2.2 Configuration sur Cisco

```
1  configure terminal
2  vlan 1
3  name DEFAULT_VLAN
4  exit
5  interface GigabitEthernet0/2
6  switchport mode access
7  switchport access vlan 1
8  spanning-tree portfast
9  exit
10 write memory
```

Listing 3.4: Configuration VLAN par défaut sur Cisco

3.3.3 VLAN natif

Les ports trunk servent de connexions entre commutateurs, transportant le trafic de plusieurs VLAN (trafic étiqueté) ainsi que le trafic non associé à un VLAN spécifique (trafic non étiqueté). Les trames non étiquetées reçues sur un port trunk 802.1Q sont automatiquement assignées au VLAN natif, qui, sur les commutateurs Cisco et Aruba, est par défaut le VLAN 1.

3.3.3.1 Configuration sur ArubaOS-Switch

```
1  configure
2  vlan 1
3    name "NATIVE_VLAN"
4    exit
5  vlan 10
6    name "DATA_VLAN"
7    exit
8  vlan 20
9    name "VOICE_VLAN"
10   exit
11  vlan 1
12    untagged 48
13    vlan 10,20
14    tagged 48
15    exit
16  write memory
```

Listing 3.5: Configuration VLAN natif sur ArubaOS-Switch

Vous pouvez aussi utiliser cette méthode :

```
1  configure
2  vlan 1
3    name "NATIVE_VLAN"
4    exit
5  vlan 10
6    name "DATA_VLAN"
7    exit
8  vlan 20
9    name "VOICE_VLAN"
10   exit
11  interface 48
12    tagged vlan 10,20
13    untagged vlan 1
14    exit
15  write memory
```

Listing 3.6: Configuration VLAN natif sur ArubaOS-Switch

3.3.3.2 Configuration sur Cisco

```
1  configure terminal
2  vlan 10
3    name DATA_VLAN
4    exit
5  vlan 20
6    name VOICE_VLAN
7    exit
8  interface GigabitEthernet0/3
9    switchport mode trunk
10   switchport trunk native vlan 1
```

```

11    switchport trunk allowed vlan 1,10,20
12    exit
13    write memory

```

Listing 3.7: Configuration VLAN natif sur Cisco

3.3.4 VLAN de gestion

Le VLAN de gestion (Management VLAN) est dédié au trafic d'administration des équipements réseau. Il permet un accès sécurisé aux interfaces de gestion (SSH, SNMP, Web) tout en isolant ce trafic sensible du trafic utilisateur.

3.3.4.1 Configuration sur ArubaOS-Switch

```

1    configure
2    vlan 100
3    name "MGMT_VLAN"
4    ip address 192.168.100.1 255.255.255.0
5    tagged 24
6    exit
7    write memory

```

Listing 3.8: Configuration VLAN de gestion sur ArubaOS-Switch

3.3.4.2 Configuration sur Cisco

```

1    configure terminal
2    vlan 100
3    name MGMT_VLAN
4    exit
5    interface vlan100
6    description "Interface de gestion"
7    ip address 192.168.100.1 255.255.255.0
8    no shutdown
9    exit
10   interface GigabitEthernet0/24
11   switchport mode trunk
12   switchport trunk allowed vlan 100
13
14   exit
15   write memory

```

Listing 3.9: Configuration VLAN de gestion sur Cisco

3.3.5 VLAN privé (Private VLAN – PVLAN)

- Permet une isolation fine au sein d'un même VLAN.
- Utilisé dans les datacenters pour isoler les clients tout en conservant un adressage commun.

- Types :
 - **Primary VLAN** : VLAN principal.
 - **Isolated VLAN** : machines isolées (ne peuvent pas communiquer entre elles).
 - **Community VLAN** : sous-groupes de machines qui peuvent communiquer entre elles, mais pas avec les autres.

3.4 Typologie de vlan

Pour attribuer un équipement à un réseau VLAN, quatre méthodes sont généralement utilisées :

- Les réseaux VLAN basés sur les ports ;
- Les réseaux VLAN basés sur les adresses MAC ;
- Les réseaux VLAN basés sur les protocoles ;
- Les réseaux VLAN basés sur l'authentification IEEE 802.1X.

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue :

3.4.1 VLAN niveau 1

Un VLAN de niveau 1 (aussi appelés VLAN par port, en anglais *Port-Based VLAN*) définit un réseau virtuel en fonction des ports de raccordement sur le Switch ou commutateur.

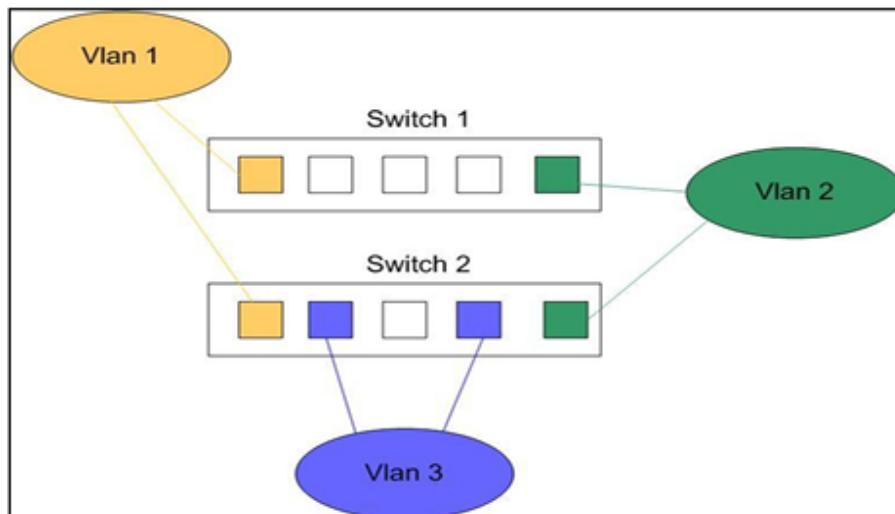


FIGURE 3.1 : VLAN par port

3.4.1.1 Avantages du VLAN par port

(A) Étanchéité maximale des VLANs :

- La segmentation par port offre une isolation renforcée entre les VLANs.
- Une attaque externe nécessite un accès physique au port tagué, limitant les risques d'intrusion à distance.

- Un pirate doit obligatoirement se connecter physiquement à un port du VLAN ciblé pour tenter une intrusion.

(B) **Gestion simplifiée par l'administrateur :**

- L'assignation des VLANs se fait directement sur les ports du switch, sans dépendre des adresses MAC ou des protocoles des machines connectées.
- L'administrateur peut configurer et modifier les VLANs de manière centralisée, sans nécessiter d'interaction avec les appareils finaux.
- Flexibilité accrue pour réattribuer des ports à différents VLANs selon les besoins, sans reconfiguration des équipements réseau.

3.4.1.2 Inconvénients

(A) Configuration lourde

- Nécessite une configuration manuelle sur chaque Switch
- À chaque déplacement de poste, modification nécessaire sur les Switchs concernés
- Maintien complexe de la qualité de service lors des changements

(B) Absence de centralisation

- Pas d'architecture centralisée de gestion
- Chaque Switch possède sa table de correspondance indépendante
- Configuration à reproduire manuellement sur chaque équipement
- Risque d'incohérence entre les différents Switchs

Cette méthode combine **sécurité renforcée** et **administration simplifiée**, ce qui en fait une solution robuste pour les réseaux nécessitant une segmentation stricte.

3.4.2 VLAN de Niveau 2

Le **VLAN de niveau 2**, également appelé *VLAN MAC* ou *VLAN par adresse IEEE* (en anglais MAC Address-Based VLAN), consiste à définir un réseau virtuel en fonction des adresses MAC des stations. Ce type de VLAN est beaucoup plus souple que le VLAN par port, car le réseau est indépendant de la localisation physique de la station.

3.4.2.1 Avantages

- Les VLANs de niveau 2 assurent une sécurité basée sur l'adresse MAC. Un pirate souhaitant accéder au VLAN doit d'abord obtenir une adresse MAC valide appartenant à ce VLAN.
- Ils permettent la centralisation des tables VLAN associées aux adresses MAC. Chaque commutateur interroge cette table pour obtenir les informations nécessaires à la gestion du trafic pour une adresse MAC donnée.

3.4.2.2 Inconvénients

- La sécurité est moindre comparée au VLAN par port, car il est possible de falsifier (spoofing) une adresse MAC.
- Il n'existe pas de contrôle de flux spécifique, ce qui nécessite un bon dimensionnement du réseau pour éviter les problèmes de performance.

3.4.3 VLAN de Niveau 3 (VLAN par Sous-Réseaux)

Les **VLANs de niveau 3** permettent de regrouper plusieurs machines en fonction du sous-réseau auquel elles appartiennent. Leur mise en place repose sur l'utilisation d'un protocole routable, tel que l'IP ou d'autres protocoles propriétaires.

L'attribution des VLANs s'effectue automatiquement en analysant les paquets jusqu'à l'adresse source au niveau de la couche 3 (adresse IP). Cette adresse détermine le VLAN auquel la machine est rattachée, ce qui facilite la gestion dynamique des VLANs indépendamment de leur emplacement physique.

3.4.3.1 Avantages

- Attribution automatique des VLANs basée sur l'adresse IP, simplifiant la configuration des clients.
- Possibilité de séparer différents protocoles au sein de VLAN distincts, améliorant l'organisation et la sécurité du réseau.

3.4.3.2 Inconvénients

- Performances plus faibles que les VLANs de niveau 1 et 2, car le commutateur doit décapsuler le paquet jusqu'à la couche 3 pour lire l'adresse IP.
- Sécurité réduite, le spoofing d'adresse IP étant plus facile à réaliser que le spoofing d'adresse MAC.
- Nécessité d'utiliser un protocole routable pour identifier le VLAN, ce qui peut limiter certains déploiements.

3.4.4 VLAN avec le standard IEEE 802.1X [6]

La norme IEEE 802.1x définit un protocole de contrôle d'accès et d'authentification basé sur le serveur client qui empêche les périphériques non autorisés de se connecter à un réseau local via des ports accessibles au public. 802.1x contrôle l'accès au réseau en créant deux points d'accès virtuels distincts sur chaque port. Un point d'accès est un port non contrôlé ; l'autre est un port contrôlé. Tout le trafic via le port unique est disponible pour les deux points d'accès. 802.1x authentifie chaque périphérique utilisateur connecté à un port de commutateur et attribue le port à un VLAN avant de rendre disponibles tous les services proposés par le commutateur ou le réseau local. Tant que le périphérique n'est pas authentifié, le contrôle d'accès 802.1x n'autorise que le trafic EAP (Extensible Authentication Protocol) sur le LAN (EAPOL) via le port auquel le périphérique est connecté. Une fois l'authentification réussie, le trafic normal peut passer par le port.

3.4.4.1 Fonctionnement de l'authentification 802.1X avec RADIUS

- **Serveur RADIUS** : Effectue l'authentification réelle du client. Le serveur RADIUS valide l'identité du client et indique au commutateur si le client est autorisé ou non à accéder aux services du réseau local et du commutateur. Ici, le serveur RADIUS est configuré pour l'authentification et l'affectation de VLAN.
- **Commutateur (Switch)** : Contrôle l'accès physique au réseau en fonction de l'état d'authentification du client. Le commutateur agit comme un intermédiaire (proxy) entre le client et le serveur RADIUS, demandant des informations d'identité au

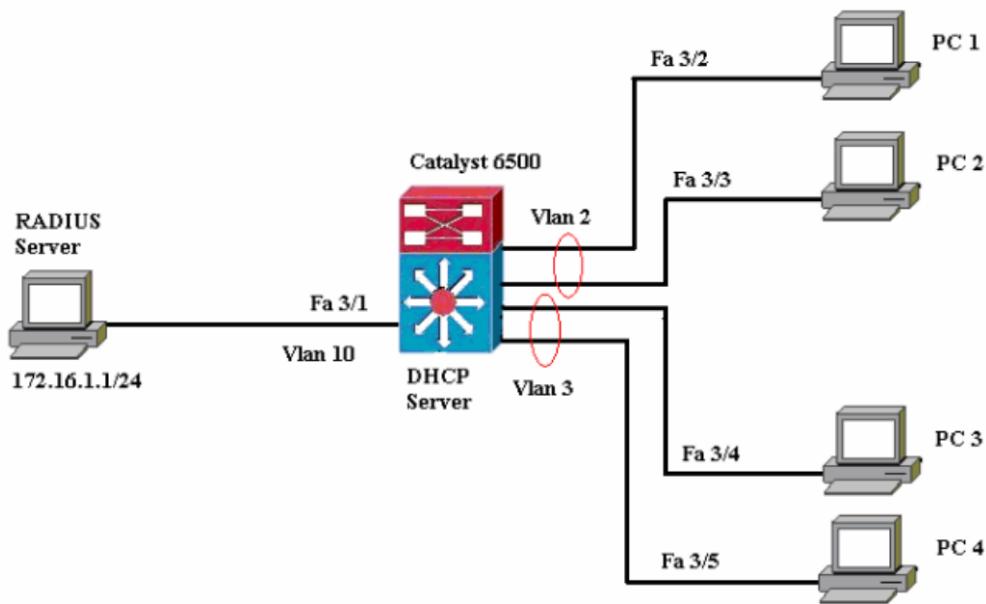


FIGURE 3.2 : Authentification 802.1X

client, vérifiant ces informations avec le serveur RADIUS et relayant une réponse au client.

Ici, le commutateur Catalyst 6500 est également configuré en tant que serveur DHCP. La prise en charge de l'authentification 802.1x pour le protocole DHCP (Dynamic Host Configuration Protocol) permet au serveur DHCP d'attribuer les adresses IP aux différentes classes d'utilisateurs finaux en ajoutant l'identité d'utilisateur authentifié dans le processus de détection DHCP.

- **Clients** : Périphériques (stations de travail) qui demandent l'accès aux services LAN et de commutation et répondent aux demandes du commutateur.
Ici, les PC 1 à 4 sont les clients qui demandent un accès réseau authentifié. Les PC 1 et 2 utilisent les mêmes informations d'identification de connexion que dans le VLAN 2. De même, les PC 3 et 4 utilisent des informations d'identification de connexion pour VLAN 3. Les clients PC sont configurés pour obtenir l'adresse IP à partir d'un serveur DHCP.

Remarque : Dans cette configuration, tout client qui échoue à l'authentification ou tout client non compatible 802.1x se connectant au commutateur se voit refuser l'accès au réseau en les déplaçant vers un VLAN inutilisé à l'aide de l'échec d'authentification et des fonctionnalités du VLAN invité.

3.5 Les trunks

Dans une architecture réseau multi-VLAN, les réseaux locaux virtuels sont véhiculés entre les équipements grâce à des liaisons logiques spécifiques appelées **trunks**. Un trunk est une liaison physique unique capable de transporter simultanément le trafic de plusieurs VLAN.

Les trames circulant sur un trunk sont marquées à l'aide d'un identifiant de VLAN (*VLAN ID*), ce qui permet de préserver l'appartenance de chaque trame à son domaine de diffusion d'origine. Cette méthode d'encapsulation permet ainsi de conserver l'isolation logique entre les différents VLANs, même lorsqu'ils transitent par une même interface physique.

Les trunks peuvent être utilisés dans plusieurs configurations :

- **Entre deux commutateurs** : il s'agit de l'usage le plus courant. Cela permet de propager les informations de plusieurs VLANs à travers l'infrastructure réseau ;
- **Entre un commutateur et un hôte** : cette configuration doit être utilisée avec précaution. En effet, un hôte compatible avec le trunking peut être en mesure de capturer ou analyser le trafic de tous les VLANs transitant sur cette liaison ;
- **Entre un commutateur et un routeur** : ce mode permet d'activer les fonctions de routage inter-VLAN, assurant ainsi l'interconnexion entre différents VLANs via un seul lien trunk.

3.6 Le protocole VTP [16]

3.6.1 Présentation

Le **VLAN Trunking Protocol (VTP)** est un protocole de couche 2 développé par Cisco pour simplifier la gestion et la configuration des VLANs dans un réseau d'entreprise. Il permet la distribution centralisée des informations VLAN à l'ensemble des commutateurs d'un même domaine VTP, facilitant ainsi la cohérence de la configuration à travers le réseau. Pour ce protocole nous invitent de voir cette référence [1].

À mesure que les réseaux gagnent en taille et en complexité, la gestion manuelle des VLANs devient laborieuse et source d'erreurs. Sans VTP, chaque VLAN doit être configuré individuellement sur chaque commutateur. Toute erreur de saisie ou oubli de configuration peut provoquer des incohérences réseau majeures.

Le protocole VTP répond à cette problématique en automatisant la distribution des informations VLAN depuis un commutateur serveur vers tous les autres commutateurs du domaine. Les mises à jour VTP ne sont pas routées au-delà du segment local : elles sont limitées aux commutateurs connectés via des trunks.

Chaque message VTP contient :

- Le nom du domaine de gestion VTP ;
- Un numéro de révision de la configuration ;
- La liste des VLANs connus ;
- Les paramètres associés à chaque VLAN.

Ces messages sont envoyés à une adresse de multidiffusion afin que tous les équipements voisins puissent les recevoir. Chaque commutateur VTP conserve une base de données VLAN dans sa mémoire non volatile. Lorsqu'un message de mise à jour contenant un numéro de révision supérieur est reçu, le commutateur met à jour automatiquement sa propre base de données.

Le numéro de version commence à 0 et s'incrémenter à chaque modification jusqu'à atteindre la valeur maximale de 2 147 483 648, avant d'être remis à zéro (un redémarrage du commutateur a également cet effet).

3.6.2 Risques et précautions

Une problématique critique peut survenir lorsqu'un nouveau commutateur, doté d'un numéro de version plus élevé, est introduit dans le réseau sans avoir été réinitialisé : sa base de données, bien que potentiellement vide ou erronée, risque d'écraser les données valides sur les autres commutateurs. En effet, tous les commutateurs sont par défaut configurés en mode *serveur*.

Pour éviter ce genre d'incident :

- Il est recommandé d'**attribuer un mot de passe VTP** pour authentifier les mises à jour ;
- Avant d'ajouter un commutateur au réseau, **le redémarrer** afin de réinitialiser son numéro de révision ;
- S'assurer que le nouveau commutateur est configuré en mode *client* ou *transparent* si un serveur VTP existe déjà dans le réseau.

3.6.3 Les modes VTP

Un commutateur Cisco peut fonctionner selon trois modes VTP : **serveur**, **client** ou **transparent**. Par défaut, certains modèles de commutateurs Cisco sont configurés en mode *serveur*, mais cela peut varier selon la version du logiciel ou le modèle.

- **Mode client** :
 - Associé à un domaine VTP existant ;
 - Ne permet pas de créer, modifier ou supprimer des VLANs localement ;
 - Reçoit les annonces VTP du serveur et met à jour automatiquement sa base de données VLAN ;
 - Réplique ces informations aux autres commutateurs du domaine.
- **Mode transparent** :
 - Peut être associé ou non à un domaine VTP ;
 - Ne traite pas les annonces VTP reçues (n'intègre pas les VLANs dans sa base locale) ;
 - Transmet les messages VTP reçus aux autres commutateurs (fonction de relais) ;
 - La base de données VLAN est locale et n'est pas modifiée par les messages VTP.
- **Mode serveur** :
 - Mode actif par défaut ;
 - Permet la création, la modification ou la suppression de VLANs ;
 - Diffuse les informations de la base VLAN à tous les autres commutateurs du domaine ;
 - Stocke la base VLAN dans la mémoire NVRAM pour persistance après redémarrage.

3.6.4 Les messages VTP

Le protocole VTP utilise différents types de messages pour maintenir la synchronisation des bases de données VLAN entre les commutateurs :

- **Annonces de type résumé :**
 - Émises toutes les 5 minutes ou après chaque modification de la base de données VLAN ;
 - Contiennent le nom du domaine VTP et le numéro de révision de la configuration ;
 - Permettent aux clients de détecter s'ils doivent actualiser leur propre base de données.
- **Annonces de type sous-ensemble :**
 - Envoyées immédiatement après une annonce de type résumé ;
 - Contiennent les détails des VLANs nouvellement créés, modifiés ou supprimés ;
 - Plusieurs annonces peuvent être nécessaires si plusieurs VLANs sont concernés.
- **Requêtes d'annonces :**
 - Émises par les clients VTP lorsqu'ils détectent une version de configuration plus récente ;
 - Permettent aux commutateurs de demander une mise à jour complète de la base VLAN ;
 - Utilisées également après une réinitialisation ou un changement de nom de domaine.

3.6.5 La synchronisation

Le protocole VTP repose sur un mécanisme de synchronisation basé sur une variable appelée **RN (Revision Number)**. Ce numéro de révision est incrémenté automatiquement à chaque modification de la base de données VLAN (création, suppression ou modification d'un VLAN).

- La valeur initiale du RN est 0, puis elle augmente de 1 à chaque modification ;
- Lorsqu'un changement est effectué sur un commutateur en mode *serveur*, celui-ci envoie une annonce VTP contenant le nouveau RN ;
- Les commutateurs clients comparent cette valeur à leur propre numéro de révision local ;
- Si le RN reçu est supérieur, ils acceptent la nouvelle base de données VLAN et effectuent une mise à jour automatique.

Par défaut, les annonces VTP contenant le RN sont envoyées immédiatement après chaque modification, ainsi que périodiquement toutes les 5 minutes pour assurer la cohérence du domaine VTP.

3.6.6 Procédure de configuration du protocole VTP

Pour configurer le protocole VTP sur un commutateur Cisco, les étapes suivantes sont à respecter :

1. **Définir un domaine VTP** : Tous les commutateurs souhaitant échanger des informations VLAN doivent être associés au même domaine ;
2. **Spécifier le mode VTP** : Choisir entre les modes *serveur*, *client* ou *transparent*, selon le rôle attendu du commutateur dans la gestion des VLANs ;
3. **Configurer un mot de passe VTP (optionnel)** : Permet de sécuriser les échanges VTP et d'éviter les mises à jour non autorisées.

3.7 Protocole Spanning-Tree (STP)

Toutes les informations présentées dans cette section sont tirées de la référence [8], pour plus d'information voir le livre [14].

3.7.1 Présentation de STP

Le Spanning-Tree Protocol (STP), standardisé sous IEEE 802.1D, est un protocole de couche 2 utilisé en cas de présence d'une liaison redondante. Une bonne configuration est strictement recommandée afin d'éviter les problèmes ci-dessous.

- **Tempêtes de broadcast** : Les trames de diffusion (broadcast) et multicast sont répliquées indéfiniment, saturant le réseau.
- **Duplication de trames** : Absence de TTL (Time To Live) au niveau Ethernet (couche 2), entraînant des boucles infinies.
- **Instabilité des tables CAM** : Apprentissage erroné des adresses MAC dû à des trames reçues sur des ports incorrects.

Mécanisme de solution : STP résout ces problèmes en :

- Créant une topologie logique sans boucle tout en conservant la redondance physique.
- Désactivant sélectivement certains ports pour éviter les boucles, tout en permettant une réactivation rapide en cas de défaillance.

3.7.2 Principe de fonctionnement STP

STP opère selon une logique d'arbre couvrant (spanning tree) avec ces caractéristiques :

- **Chemin optimal** : Basé sur la somme des coûts des liens, inversement proportionnels au débit (par exemple, lien 1 Gbps = coût 4).
- **États des ports** :
 - Forwarding : Port actif, transmet et reçoit des données.
 - Blocking : Port bloqué, écoute uniquement les BPDU pour détecter les changements.
- **Échanges BPDU** : Envoyés en multicast sur l'adresse 01:80:C2:00:00:00 toutes les 2 secondes par défaut.

3.7.2.1 Identifiants clés

Élément	Composition
Bridge ID (BID)	Priorité (4 bits) + VLAN ID (12 bits) + Adresse MAC
Priorité par défaut	32768 (valeur modifiable par multiples de 4096)

TABLE 3.1 : Structure du Bridge ID

3.7.2.2 Explication technique

Le **Bridge ID (BID)** est un identifiant unique attribué à chaque commutateur dans le cadre du protocole **STP** (*Spanning Tree Protocol*). Il est utilisé pour déterminer le **Root Bridge** (commutateur racine).

- **Priorité (4 bits)** : valeur configurable qui permet d'influencer l'élection du Root Bridge. La valeur par défaut est **32768**.
- **VLAN ID (12 bits)** : utilisé notamment dans les variantes comme **PVST+** pour distinguer les instances STP par VLAN.
- **Adresse MAC** : identifiant physique du commutateur, utilisé en cas d'égalité de priorité pour départager les candidats.

Note : La priorité étendue est codée sur 16 bits, dont les **12 bits de poids faible sont réservés au VLAN ID**. Par conséquent, la priorité ne peut être configurée que par **multiples de 4096** (ex. : 0, 4096, 8192, ..., 61440).

3.7.3 Algorithme STP

L'algorithme procède en 4 phases :

1. **Élection du Root Bridge** : Le commutateur avec le BID le plus faible (priorité + MAC) est élu et tous ses ports passent en état *Forwarding*.
2. **Sélection des Root Ports** : Sur chaque commutateur non-racine, le port avec le coût cumulé le plus faible vers le Root Bridge est choisi comme Root Port.
3. **Désignation des ports** : Un seul Designated Port par segment de réseau, choisi en fonction du coût le plus faible ou du BID en cas d'égalité.
4. **Transition des états** : Les ports sélectionnés (Root et Designated) passent à l'état *Forwarding*, tandis que les autres ports redondants passent à l'état *Blocking*.

3.7.4 Optimisation et configuration

3.7.4.1 Influence sur l'élection

```
(config)# spanning-tree vlan 10 root primary      ! Priorité = 24576
(config)# spanning-tree vlan 10 priority 8192     ! Valeur manuelle
```

3.7.4.2 Variation des Coûts de Ports selon le Protocole STP

Les valeurs de coût des ports varient effectivement selon le protocole STP utilisé (**CST**, **PVST+**, **RSTP**, **MSTP**) , principalement en raison :

- des différences de standards **IEEE**,
- des **méthodes de calcul**,
- de la **prise en charge des VLANs**.

Voici une analyse détaillée :

Bandé Passante	CST (802.1D)	PVST+ (Cisco)	RSTP (802.1W)	MSTP (802.1s)
10 Mbps	100	100	2 000 000	2 000 000
100 Mbps	19	19	200 000	200 000
1 Gbps	4	4	20 000	20 000
10 Gbps	2	2	2 000	2 000

TABLE 3.2 : Coûts STP par bande passante selon le protocole

Explications

- **CST / PVST+** : utilisent des valeurs de coût **historiques** avec une **échelle réduite**, héritées du standard original 802.1D.
- **RSTP / MSTP** : utilisent une **échelle de coût étendue** pour permettre une **granularité accrue** dans les calculs de topologie.
- **PVST+** : reprend les mêmes valeurs de coût que CST, mais les **applique indépendamment par VLAN**.

Configuration manuelle :

```
(config-if)# spanning-tree cost 10
```

3.7.5 États et temporisation des ports

- **Blocking** → Listening (Max Age = 20s) : Écoute uniquement des BPDU, sans apprentissage ni transmission de données.
- **Listening** → Learning (Forward Delay = 15s) : Écoute des BPDU, sans transmission de données ni apprentissage MAC.
- **Learning** → Forwarding (Forward Delay = 15s) : Apprentissage des adresses MAC, mais pas encore de transmission de données.
- **Forwarding** : Transmission et réception complètes, avec apprentissage MAC.

3.7.6 Sécurité STP

- **PortFast** : Active immédiatement les ports d'accès (ex. : vers les hôtes), évitant les délais de convergence.
- **BPDU Guard** : Désactive les ports recevant des BPDU inattendus, protégeant contre les commutateurs non autorisés.
- **Root Guard** : Empêche un commutateur non désiré de devenir Root Bridge.

3.7.7 Variantes de STP

Les variantes de STP ont été développées pour répondre aux limitations du protocole original, notamment en termes de temps de convergence et de gestion des VLAN. Voici une analyse détaillée de quelques variantes :

3.7.7.1 STP (IEEE 802.1D)

- **Description** : Version originale du protocole, conçue pour éliminer les boucles dans les réseaux Ethernet.
- **Temps de convergence** : 30 à 50 secondes, en raison des longs délais de transition (Listening et Learning).
- **Avantages** :
 - Standard universellement supporté par tous les commutateurs.
 - Simple à configurer dans les petits réseaux.
- **Limitations** :
 - Convergence lente, inadaptée aux réseaux critiques nécessitant une haute disponibilité.
 - Une seule instance d'arbre couvrant pour tout le réseau, ce qui limite l'utilisation des liens redondants.
- **Utilisation** : Convient aux réseaux simples ou legacy, mais rarement utilisé dans les environnements modernes.

3.7.7.2 RSTP (IEEE 802.1w)

- **Description** : Rapid Spanning Tree Protocol, une évolution de STP qui réduit drastiquement le temps de convergence.
- **Temps de convergence** : 1 à 2 secondes, grâce à l'introduction de rôles de ports (Root Port, Designated Port, Alternate Port) et d'états simplifiés (Discarding, Learning, Forwarding).
- **Avantages** :
 - Convergence rapide en cas de changement de topologie (ex. : panne de lien).
 - Détection proactive des pannes via des BPDU envoyés plus fréquemment.
 - Compatible avec STP (802.1D) pour une transition progressive.
- **Limitations** :
 - Toujours une seule instance d'arbre couvrant, ce qui ne permet pas une utilisation optimale des VLAN.

- Moins flexible pour les grands réseaux avec de multiples VLAN.
- **Utilisation** : Idéal pour les réseaux d'entreprise nécessitant une résilience rapide sans configuration complexe.
- **Configuration** :

```
(config)# spanning-tree mode rapid
```

3.7.7.3 MSTP (IEEE 802.1s)

- **Description** : Multiple Spanning Tree Protocol, qui permet de créer plusieurs instances d'arbres couvrants, chacune associée à un groupe de VLAN.
- **Temps de convergence** : 1 à 2 secondes, similaire à RSTP, avec une gestion optimisée des VLAN.
- **Avantages** :
 - Répartition de charge : Différents VLAN peuvent utiliser différents chemins, optimisant l'utilisation des liens.
 - Évolutivité : Supporte les grands réseaux avec de nombreux VLAN.
 - Hérite des améliorations de RSTP (convergence rapide).
- **Limitations** :
 - Configuration plus complexe, nécessitant une planification des instances.
 - Consommation accrue de ressources (CPU/mémoire) sur les commutateurs.
- **Utilisation** : Recommandé pour les réseaux d'entreprise complexes avec de multiples VLAN, comme les datacenters ou campus.
- **Configuration** :

```
(config)# spanning-tree mode mst
(config)# spanning-tree mst configuration
(config-mst)# instance 1 vlan 10,20
```

Version	Convergence	Avantage	Limitation
STP (802.1D)	30-50s	Standard de base	Convergence lente
RSTP (802.1w)	1-2s	Transition rapide	Une seule instance
MSTP (802.1s)	1-2s	Multi-VLAN, répartition	Configuration complexe

TABLE 3.3 : Comparaison des versions STP

3.7.8 Problèmes courants et dépannage

Voici quelques problèmes fréquents liés à STP et leurs solutions :

- **Boucle temporaire** :
 - *Cause* : Mauvaise configuration ou câblage incorrect.

- *Solution* : Vérifier les journaux avec `debug spanning-tree events` et activer BPDU Guard.
- **Convergence lente** :
 - *Cause* : Utilisation de STP classique (802.1D).
 - *Solution* : Passer à RSTP ou ajuster les temporisations (ex. : réduire Forward Delay).
- **Root Bridge inattendu** :
 - *Cause* : Priorité non configurée ou commutateur avec MAC plus basse.
 - *Solution* : Forcer la priorité avec `spanning-tree vlan X root primary`.

3.7.9 Commandes utiles

```
# show spanning-tree summary      ! Vue globale
# show spanning-tree vlan 10      ! Détails par VLAN
# debug spanning-tree events     ! Dépannage
# show spanning-tree blockedports ! Ports bloqués
```

3.7.10 Glossaire des termes

- **BPDU** : Bridge Protocol Data Unit, trame utilisée pour échanger des informations STP.
- **Root Bridge** : Commutateur central de référence dans la topologie STP.
- **Cost** : Valeur attribuée à un lien, inversement proportionnelle au débit.
- **Designated Port** : Port responsable de la transmission des données sur un segment.

Conclusion

Ce chapitre a mis en lumière les technologies clés pour sécuriser les réseaux basés sur des commutateurs. Les VLAN segmentent le trafic, les trunks facilitent l'interconnexion, VTP simplifie la gestion des VLAN, et STP, avec ses évolutions comme RSTP et MSTP, prévient les boucles tout en assurant la redondance. Ensemble, ces mécanismes, soutenus par des fonctionnalités comme l'authentification 802.1X, garantissent des réseaux performants et protégés, indispensables pour répondre aux besoins des entreprises modernes.

CHAPITRE 4

ACLS ET PARE-FEU

Introduction

Les **Listes de Contrôle d’Accès (ACLS)** et les **pare-feu** sont des mécanismes essentiels pour sécuriser un réseau. Ce chapitre explore leur fonctionnement, leurs types, leurs configurations et leurs limites, afin de comprendre leur rôle dans la protection des infrastructures informatiques. Les fondements théoriques concernant les ACL proviennent de la référence [16], et ceux relatifs au pare-feu de la référence [15].

4.1 Les Listes de Contrôle d’Accès (ACLS)

4.1.1 Présentation Générale

Les listes de contrôle d'accès, plus communément appelées *ACLs* (Access Control Lists), sont des ensembles de règles permettant de contrôler le trafic réseau entrant ou sortant à travers les interfaces d'un routeur. Elles constituent un mécanisme fondamental pour assurer la sécurité et la gestion du trafic dans les infrastructures réseaux.

Les ACLs permettent notamment :

- d'autoriser ou de bloquer certains paquets, en entrée ou en sortie d'interface ;
- de filtrer le trafic selon des critères définis ;
- de restreindre l'accès au réseau à des utilisateurs ou des hôtes spécifiques.

Le fonctionnement des ACLs repose sur une lecture séquentielle des règles : chaque paquet est comparé aux instructions dans l'ordre. Dès qu'une correspondance est trouvée, l'action (autoriser ou refuser) est immédiatement appliquée, sans considérer les règles suivantes. Si aucune règle n'est satisfaite, une règle implicite de refus (*deny*) s'applique automatiquement.

Chaque ACL agit dans une direction précisée par les mots-clés **in** (entrée) ou **out** (sortie), selon le sens du trafic par rapport à l'interface.

4.1.2 Les Différents Types d'ACLS

Chaque ACL peut être identifiée par un numéro, utilisé pour déterminer son type et le protocole concerné. Cette numérotation suit une plage définie :

- **1 à 99 et 1300 à 1999** : ACLs standard ;
- **100 à 199 et 2000 à 2699** : ACLs étendues.

4.1.2.1 ACL Standard

Une ACL standard permet de filtrer le trafic uniquement sur la base de l'adresse IP source. Elle est simple à mettre en œuvre et peu consommatrice de ressources. Ces ACLs sont généralement utilisées pour :

- autoriser ou interdire une plage d'adresses IP ;
- contrôler la diffusion des mises à jour de routage.

4.1.2.2 ACL Étendue

Les ACLs étendues offrent un filtrage plus fin et plus puissant. Elles permettent d'appliquer des règles en fonction de plusieurs critères :

- le protocole (par exemple : TCP, UDP, ICMP) ;
- l'adresse IP source ;
- l'adresse IP de destination ;
- le numéro de port ou le type de service.

Ce type d'ACL est utile pour autoriser ou bloquer un trafic spécifique selon son contenu et son contexte.

4.1.2.3 ACL Nommée

Introduites à partir de la version 11.2 de Cisco IOS, les ACLs nommées permettent une gestion plus flexible et plus lisible. Elles peuvent être de type standard ou étendu, et sont identifiées par un nom alphanumérique plutôt que par un simple numéro.

Cette méthode favorise une meilleure organisation dans les configurations complexes et facilite les modifications ou extensions futures.

Les principales utilisations des ACLs nommées sont :

- l'identification claire des ACLs via un nom descriptif ;
- la configuration simultanée de plusieurs ACLs standards et étendues pour un même protocole sur un routeur.

4.1.3 Algorithme de Vérification

Lorsqu'un routeur reçoit un paquet, le logiciel Cisco IOS applique un algorithme de vérification pour décider si ce paquet doit être autorisé ou bloqué. Ce processus consiste à comparer le paquet à chaque condition définie dans la liste de contrôle d'accès, dans l'ordre d'apparition des instructions.

Le fonctionnement suit les étapes suivantes :

- Le paquet est comparé successivement aux règles de l'ACL ;
- Dès qu'une condition est satisfaite, l'action définie (autoriser ou refuser) est immédiatement appliquée ;
- Si le paquet ne correspond à aucune des conditions explicites, il est rejeté par défaut en raison de la règle implicite `deny any` présente à la fin de chaque ACL.

Ce comportement garantit un traitement déterministe et hiérarchisé des paquets, essentiel pour une politique de filtrage efficace.

4.1.4 Masque Générique

Le masque générique (ou *wildcard mask*) est un ensemble de 32 bits, répartis en quatre octets de 8 bits chacun. Il est utilisé dans les ACLs pour spécifier quelles parties d'une adresse IP doivent être comparées ou ignorées lors du filtrage.

Les principes d'interprétation du masque sont les suivants :

- Un bit à **0** indique que le bit correspondant de l'adresse IP doit être strictement comparé ;
- Un bit à **1** signifie que la valeur du bit correspondant est ignorée (pas de comparaison).

Grâce au masquage générique, il est possible de spécifier une seule adresse, un sous-réseau, ou une plage d'adresses IP dans une instruction ACL.

Exemple de logique binaire :

- Si le XI^e bit du masque est égal à 0, alors le XI^e bit de l'adresse du paquet doit être identique à celui de l'adresse de référence dans la liste ;
- Si le XI^e bit du masque est égal à 1, alors aucune correspondance n'est exigée entre les deux adresses à ce niveau.

4.1.5 Configuration des ACLs

La mise en œuvre des listes de contrôle d'accès (ACLs) se déroule en deux étapes principales :

1. **Création de l'ACL** : définition des règles de filtrage (autorisations ou refus) ;
2. **Application de l'ACL** : affectation de l'ACL à une interface réseau dans une direction spécifique (in ou out).

4.1.5.1 Configuration des ACLs Standards

Les ACLs standards sont configurées dans le mode de configuration globale à l'aide de la syntaxe suivante :

```
access-list {numéro} {permit|deny} {adresse IP} {masque générique} [log]
access-list {numéro} remark {commentaire}
```

Remarques importantes :

- Si le masque générique n'est pas précisé, la valeur par défaut 0.0.0.0 est utilisée, ce qui impose une correspondance exacte ;
- L'option **log** permet de journaliser les paquets correspondant à la règle ;
- L'instruction **remark** permet d'ajouter un commentaire descriptif à l'ACL ;
- L'ordre des règles est séquentiel et non modifiable après la création : toute nouvelle règle est ajoutée à la fin, et il n'est pas possible de supprimer une règle individuellement.

4.1.5.2 Configuration des ACLs Étendues

Pour définir une ACL étendue, on utilise la syntaxe suivante :

```
access-list {numéro} {permit|deny} {protocole}
{IP source} {masque source} [opérateur opérande]
{IP destination} {masque destination} [opérateur opérande]
[icmp-type] [log] [established]
```

Explications des paramètres :

- **protocole** : peut être spécifié par son nom (ip, tcp, udp, icmp, etc.) ou son numéro (0 à 255) ;
- **established** : utilisé uniquement avec le protocole TCP, permet de filtrer les connexions déjà établies (présence de drapeaux ACK, FIN, etc.) ;
- **icmp-type** : applicable uniquement au protocole ICMP, permet de spécifier un type précis de message ICMP ;
- Les mêmes règles de création, d'ordre et de modification que les ACLs standards s'appliquent.

4.1.5.3 Configuration des ACLs Nommées

Cisco IOS permet également la création d'ACLs nommées, avec la commande suivante :

```
ip access-list {standard|extended} {nom}
```

Dans le mode de configuration d'une ACL nommée, on utilise les instructions suivantes :

- **ACL standard** :

```
{permit|deny} {adresse IP} [masque] [log]
```

- **ACL étendue** :

```
{permit|deny} {protocole} {IP source} {masque source}
[opérateur opérande] {IP destination} {masque destination}
[opérateur opérande] [icmp-type] [log] [established]
```

- **Commentaire** :

```
remark {commentaire}
```

Avantages des ACLs nommées :

- Identification plus lisible grâce à des noms explicites ;
- Flexibilité accrue dans la configuration et la gestion ;
- Possibilité d'ajouter des commentaires directement au sein des règles.

4.1.5.4 Mise en Place et Vérification des ACLs

Une fois les ACLs définies, il est nécessaire de les appliquer aux interfaces ou aux lignes du routeur. Pour cela, les commandes suivantes sont utilisées :

1. Application des ACLs :

- `ip access-group {numéro|nom} {in|out}`
 - À utiliser en mode de configuration d'interface ;
 - Applique l'ACL sur l'interface spécifiée pour filtrer le trafic entrant ou sortant.
- `ip access-class {numéro|nom} {in|out}`
 - À utiliser en mode de configuration de ligne ;
 - Filtre les accès sur la ligne de terminal (console ou Telnet/SSH).
- `no access-list {numéro}`
 - À utiliser en mode de configuration globale ;
 - Supprime entièrement une ACL numérotée.

2. Vérification des ACLs :

- `show access-lists {numéro|nom}`
 - Affiche toutes les ACLs configurées, leurs instructions et les statistiques de correspondances.
- `show ip interface [{type} {numéro}]`
 - Permet de visualiser les ACLs appliquées sur les interfaces, ainsi que la direction du filtrage.

4.1.6 Avantages et Inconvénients des ACLs

4.1.6.1 Avantages :

- Renforcement de la sécurité en filtrant les paquets selon des critères précis (adresses, protocoles, ports, etc.) ;
- Contrôle précis du trafic réseau sans nécessiter de matériel additionnel ;
- Utilisation flexible selon les besoins (filtrage d'accès, contrôle de flux, restrictions d'administration).

4.1.6.2 Inconvénients :

- Traitement supplémentaire à chaque paquet, pouvant engendrer une augmentation de la latence ;
- Consommation de ressources processeur (CPU), en particulier sur les routeurs de faible capacité ;
- Gestion parfois complexe dans des environnements avec de nombreuses règles.

4.2 Le pare-feu

4.2.1 Définition du pare-feu

Un **pare-feu** (ou *firewall*) est un dispositif de sécurité destiné à assurer une protection entre un réseau local et un autre réseau, tel qu'un second réseau interne ou Internet.

Il remplit deux fonctions principales :

- **Contrôler et protéger** les hôtes du réseau local contre :
 - la divulgation non autorisée d'informations ;
 - les programmes malveillants tels que les virus ou chevaux de Troie.
- **Protéger les serveurs accessibles depuis Internet** contre :
 - des commandes potentiellement dangereuses (ex. : Telnet) ;
 - la modification ou l'altération non souhaitée des données hébergées.

Un pare-feu peut être constitué d'une **partie matérielle** (comme un ordinateur ou un équipement réseau spécialisé) associée à un ou plusieurs **logiciels** dédiés à la gestion et au filtrage du trafic réseau.

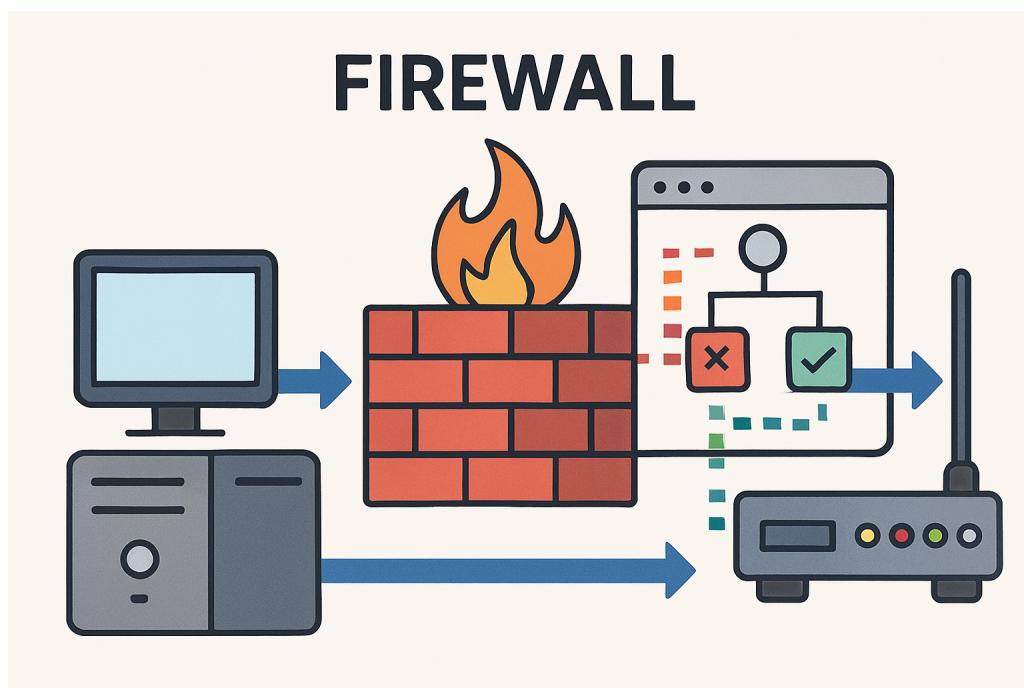


FIGURE 4.1 : Pare-feu : matériel et logiciels

4.2.2 Évolution des firewalls

Depuis leur apparition au début des années 1990, les firewalls ont considérablement évolué pour répondre aux nouvelles menaces et aux besoins de performance croissants :

1. **Première génération (années 1990)** : les firewalls de filtrage de paquets fonctionnaient principalement sur la base d'ACLs simples, sans inspection approfondie du trafic. Ils contrôlaient uniquement l'adresse IP source/destination, le protocole et le port.

2. **Deuxième génération (fin des années 1990)** : apparition des firewalls à inspection dynamique (stateful inspection) capables de maintenir l'état des connexions réseau et de vérifier la légitimité d'un paquet par rapport à une session active.
3. **Troisième génération (années 2000)** : introduction des firewalls applicatifs ou proxy firewalls, capables d'analyser le trafic au niveau des applications (HTTP, FTP, etc...) afin de détecter les comportements suspects.
4. **Quatrième génération (années 2010)** : émergence des Next-Generation Firewalls (NGFW) intégrant plusieurs fonctions : inspection profonde des paquets (DPI), prévention des intrusions (IPS), contrôle des applications, filtrage web et parfois antivirus.
5. **Tendances actuelles** : montée en puissance des firewalls cloud et des solutions basées sur le modèle Zero Trust avec intégration au SD-WAN et à la sécurité des environnements hybrides (datacenters + cloud public).

4.2.3 Exemples de marques et modèles de firewalls

Sur le marché, plusieurs constructeurs dominent le secteur avec une large gamme de solutions adaptées aux entreprises de toutes tailles :

- **Cisco Systems** : avec les gammes **ASA** (Adaptive Security Appliance) et **Firepower** (NGFW).
- **Palo Alto Networks** : pionnier des NGFW avec des modèles tels que **PA-220**, **PA-850** et les séries **PA-3200**.
- **Fortinet** : série FortiGate, réputée pour ses performances et sa gestion unifiée. avec la gamme **FortiGate**, couvrant des modèles pour **PME** (FortiGate 40F) jusqu'aux grandes entreprises et opérateurs (FortiGate 6000F).
- **Check Point** : Appliances de sécurité réseau très présentes en milieu bancaire et gouvernemental. avec la série **Quantum Security Gateways**, largement déployée dans les grandes organisations.
- **Juniper Networks** : gamme **SRX Series**, utilisée notamment dans les environnements opérateurs et datacenters.
- **Sophos** : XG Firewall, connu pour son intégration avec les solutions de sécurité endpoint.
- **Solutions open source** : comme **pfSense**, **OPNsense** ou **IPFire**, très utilisées dans les environnements académiques et par les petites structures.

4.2.4 Architectures courantes de pare-feu

Il existe deux grandes familles d'architectures de pare-feu : les architectures dites **simples**, et les architectures **sensibles** (ou complexes), plus adaptées aux environnements critiques.

4.2.4.1 Architecture simple

Dans une architecture simple, le pare-feu agit principalement comme un filtre de paquets placé entre le réseau local et le réseau externe. Ce modèle est généralement utilisé dans des environnements où les exigences de sécurité restent basiques. Il permet une première barrière de protection tout en assurant une simplicité de mise en œuvre.

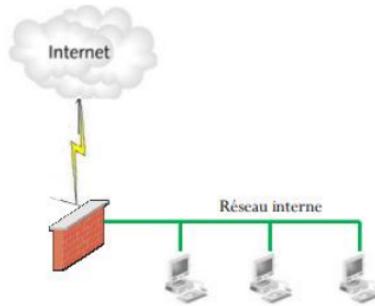


FIGURE 4.2 : Architecture simple

4.2.4.2 Architecture sensible (ou complexe)

L'architecture sensible est plus avancée que l'architecture simple. Elle est conçue pour des environnements où la sécurité est critique, tels que les systèmes d'information d'entreprise ou les réseaux exposés à de fortes menaces.

Elle présente plusieurs avantages :

- **Filtrage intelligent des connexions** selon des règles évoluées et contextuelles ;
- **Inspection approfondie des flux** afin de détecter d'éventuels contenus malveillants (ex : analyse de signatures de virus ou de comportements suspects) ;
- **Mise en cache de contenus fréquemment consultés**, ce qui améliore la performance et réduit la charge réseau.

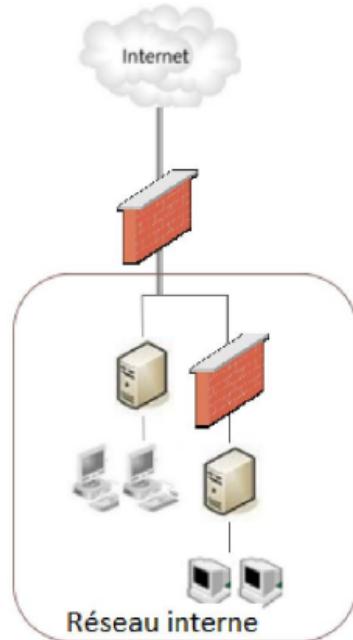


FIGURE 4.3 : Architecture sensible

4.2.5 Les différents types de pare-feu

On distingue plusieurs catégories de pare-feux selon leur mode de déploiement et leur rôle dans l'architecture réseau. Les principales sont les pare-feux logiciels, pare-feux matériels, et les pare-feux de nouvelle génération (NGFW).

4.2.5.1 Pare-feux logiciels

Les pare-feux logiciels sont des applications installées sur des machines (serveurs ou postes clients) qui permettent de filtrer le trafic réseau entrant et sortant. On en distingue principalement deux types :

1. **Pare-feux personnels** : ils protègent des machines individuelles (PC, postes nomades) contre les connexions non autorisées. Intégrés à la plupart des systèmes d'exploitation modernes (comme Windows Defender Firewall), ils sont généralement simples à configurer mais restent limités en matière de protection avancée.
2. **Pare-feux logiciels avancés sur serveurs Linux** : grâce à des outils comme `Netfilter/iptables`, `nftables`, ou `Firewalld`, les systèmes Linux peuvent être configurés comme des pare-feux puissants. Ces outils permettent une gestion fine des flux réseau et peuvent intégrer des fonctions de routage, NAT, ou même de proxy. Des distributions spécialisées comme `OPNsense`, `pfSense` ou `VyOS` permettent de transformer un serveur ou un équipement dédié en pare-feu complet, souvent utilisé dans les environnements open source ou à budget contraint.

4.2.5.2 Pare-feux matériels

Les pare-feux matériels sont des dispositifs dédiés intégrant leur propre système d'exploitation et configurés pour sécuriser le périmètre réseau. Ils sont commercialisés par des fournisseurs comme Fortinet (FortiGate), Cisco (ASA, Firepower), Palo Alto Networks, Check Point, etc.

Avantages	Inconvénients
Intégration optimale avec l'infrastructure matérielle	Moins de souplesse que les solutions logicielles libres
Performances élevées grâce au traitement matériel dédié (ASIC)	Coût plus élevé
Moindre vulnérabilité aux attaques logicielles par isolement du système d'exploitation	Maintenance spécifique (licences, mises à jour, support constructeur)
Fonctionnement autonome, sans impact sur les performances des serveurs	

TABLE 4.1 : Avantages et inconvénients d'un pare-feu matériel

4.2.6 Les différents types de filtrage

Un pare-feu repose sur un ensemble de règles définies par l'administrateur, généralement selon le principe suivant :

« *Tout ce qui n'est pas explicitement autorisé est interdit.* »

Les pare-feux appliquent des règles de sécurité basées sur différents types de filtrage, correspondant à des couches spécifiques du modèle OSI.

4.2.6.1 Filtrage de paquets

1. **Filtrage statique** (stateless) : Chaque paquet est analysé indépendamment des autres. Les critères incluent l'IP source, l'IP destination, le protocole, et les ports. Ce filtrage est rapide mais ne permet pas de suivre l'état des connexions.
2. **Filtrage dynamique** (stateful) : Le pare-feu maintient une table d'état des connexions actives. Il suit les sessions (TCP, UDP) et permet une meilleure gestion des flux, notamment pour les protocoles complexes (ex. FTP). Ce mécanisme reste limité face aux attaques applicatives.

4.2.6.2 Filtrage applicatif

Opérant sur la couche 7 (application) du modèle OSI, le filtrage applicatif permet d'analyser le contenu des communications en fonction des protocoles utilisés (HTTP, SMTP, DNS, etc.).

Il est généralement mis en œuvre via :

- Des proxys applicatifs : qui interceptent les requêtes, analysent et filtrent le trafic ;
- Des moteurs DPI intégrés aux NGFW.

Ce type de filtrage permet :

- d'identifier des usages suspects (ex. tunneling DNS) ;
- de bloquer des applications spécifiques (ex. réseaux sociaux, peer-to-peer) ;
- de détecter des signatures d'attaques ou de logiciels malveillants.

4.3 Pare-feu avec zone démilitarisée (DMZ)

La DMZ (Demilitarized Zone) est une architecture classique visant à exposer certains services au public (serveurs Web, Mail, DNS...) tout en isolant le réseau interne (LAN). Elle repose généralement sur trois zones logiques :

- **Le réseau local (LAN)** : réseau interne, hautement sécurisé ;
- **La DMZ** : zone intermédiaire, hébergeant des serveurs accessibles depuis l'extérieur ;
- **Internet** : réseau public.

Un ou plusieurs pare-feux assurent la segmentation, le contrôle d'accès et la journalisation. La DMZ limite l'impact d'une compromission en maintenant les services exposés séparés des ressources critiques internes.

Remarque : les architectures modernes tendent à évoluer vers des modèles Zero Trust ou micro-segmentation via SDN ou solutions cloud-native, qui remettent en question l'approche périphérique classique.

Dans cette configuration, un pare-feu est placé entre Internet, la DMZ et le LAN. Il agit comme un point de contrôle centralisé permettant :

- de filtrer les trames en fonction de règles internes définies par les administrateurs réseau ;

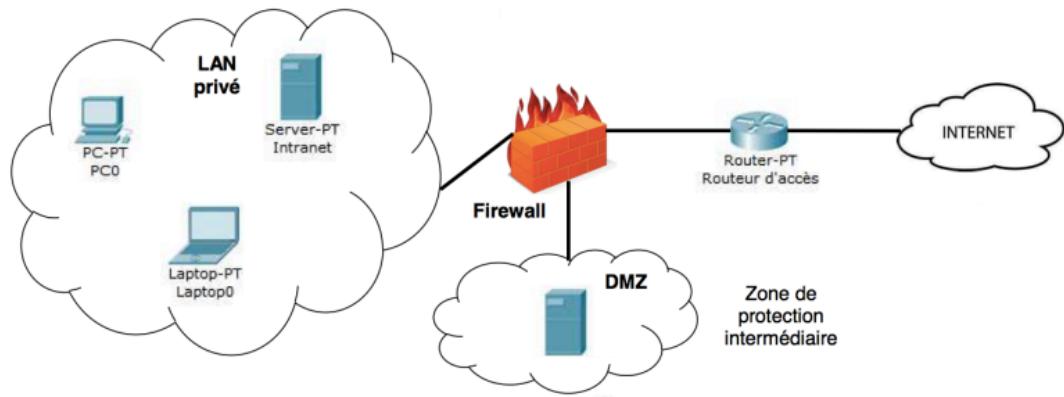


FIGURE 4.4 : Zone démilitarisée (DMZ)

- de rediriger le trafic vers la zone appropriée (LAN ou DMZ) ;
- de limiter les risques de compromission du réseau interne en isolant les services exposés dans la DMZ.

La DMZ joue ainsi le rôle de zone tampon, servant à protéger le LAN tout en permettant l'accès public à certains services essentiels.

Conclusion

En résumé, les ACLs et les pare-feu constituent des outils clés pour le filtrage et la sécurité réseau. Bien qu'efficaces, ils présentent des limites qui nécessitent une combinaison avec d'autres solutions pour une protection optimale. Leur maîtrise est indispensable dans toute stratégie de cybersécurité moderne.

CHAPITRE 5

CONCEPTION ET RÉALISATION

Ce chapitre présente les étapes clés de la conception et réalisation du réseau, incluant l'architecture globale, le plan d'adressage, et les configurations techniques des équipements (Aruba, FortiGate). L'objectif est de déployer un réseau sécurisé, performant et facile à superviser.

Remarque : Les configurations suivantes sont basées sur une simulation GNS3 générique et ne reflètent pas d'infrastructure réelle pour des raisons de confidentialité.

5.1 Conception

L'objectif de cette section est de concevoir une infrastructure réseau répondant aux lacunes identifiées : Absence de Wi-Fi, de VoIP, de redondance de liaison, de segmentation logique et de sécurité. La conception s'appuie sur les solutions proposées et vise à garantir performance, résilience et évolutivité, en intégrant les switchs Aruba ProVision, le pare-feu FortiGate, des points d'accès Wi-Fi et de VoIP.

5.1.1 Architecture du réseau avec la solution

L'architecture adoptée est hiérarchique (cœur, distribution, accès). Le FortiGate assure le routage inter-VLAN et la sécurité au niveau cœur. Les ArubaOS (AOS-Switch) de rez-de-chaussée, 1^{er} et 2^{eme} étages qui gèrent la distribution et l'accès, tandis que des points d'accès Wi-Fi et VoIP répondent aux besoins de connectivité sans fil et de téléphonie. La figure 5.1 illustre cette topologie.

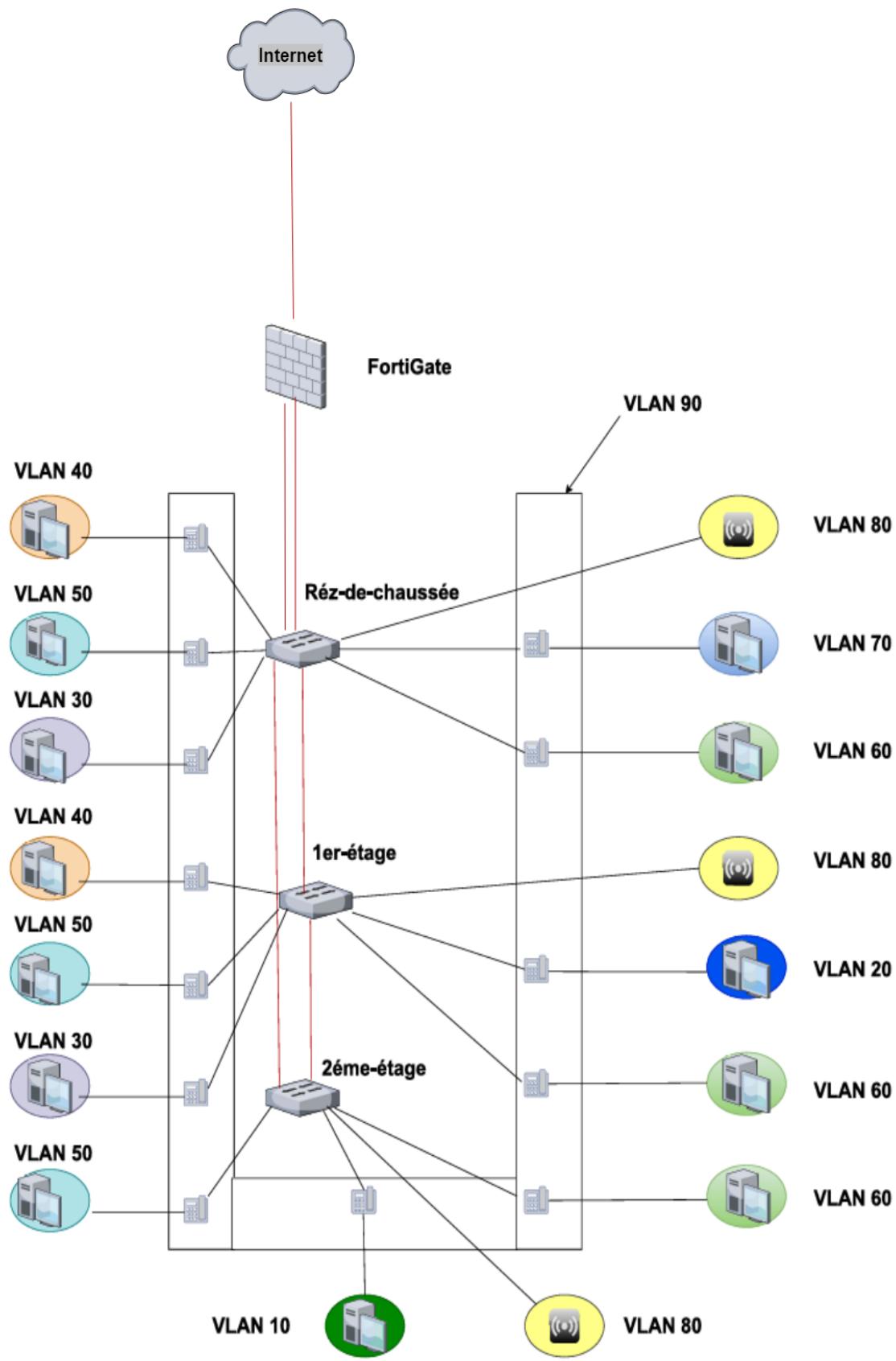


FIGURE 5.1 : Architecture du réseau local avec la solution proposée

5.1.2 Solutions techniques

1. Création des VLANs 10, 20, 30, 40, 50, 60, 70, 80, 90, 101, 102 et 100 (tableau 5.1), et services DHCP/DNS centralisés dans le FortiGate.
2. Un plan d’adressage basé sur la plage 192.168.0.0/16 a été défini pour supporter la segmentation en VLANs et faciliter la gestion des adresses IP. Le tableau 5.1 présente les sous-réseaux attribués.

VLAN	Nom	Plage	Passerelle	Hôtes	Utilisation
10	cabinet	192.168.10.0/24	192.168.10.1	254	Un service
20	secretariat	192.168.20.0/24	192.168.20.1	254	Un service
30	sysinfo	192.168.30.0/24	192.168.30.1	254	Un service
40	administra-tion	192.168.40.0/24	192.168.40.1	254	Un service
50	relations	192.168.50.0/24	192.168.50.1	254	Un service
60	communica-tion	192.168.60.0/24	192.168.60.1	254	Un service
70	reunion	192.168.70.0/24	192.168.70.1	254	Un service
80	invite	192.168.80.0/24	192.168.80.1	254	Wi-Fi
90	voip	192.168.90.0/24	192.168.90.1	254	VoIP
100	gestion	192.168.100.0/24	192.168.100.1	254	Switchs, FortiGate, AP
101	natif	—	—	—	VLAN natif pour les trunk
102	desactive	—	—	—	Port désactivé

TABLE 5.1 : Plan d’adressage du réseau local

3. Les switchs Aruba attribuent les ports, et le FortiGate gère le routage inter-VLAN avec la méthode **router-on-a-stick** via les sous-interfaces. L’affectation des VLANs non-étiqueté (untagged) et VLANs étiqueté (tagged) aux ports de chaque switch est présenté dans le tableau 5.2.

Switch	Ports	VLAN (untagged / tagged)
Rez-de-chaussée	1–4	VLAN 30 / VLAN 90
Rez-de-chaussée	5–12	VLAN 40 / VLAN 90
Rez-de-chaussée	13–14	VLAN 50 / VLAN 90
Rez-de-chaussée	15–16	VLAN 60 / VLAN 90
Rez-de-chaussée	17–20	VLAN 70 / VLAN 90
Rez-de-chaussée	21	VLAN 100 / VLAN 80
Rez-de-chaussée	49–50	VLAN 101 / VLAN 10, 20, 30, 40, 50, 60, 70, 80, 90, 100
Rez-de-chaussée	51	VLAN 101 / VLAN 10, 20, 30, 40, 50, 60, 70, 80
Rez-de-chaussée	52	VLAN 101 / VLAN 80, 100

Suite à la page suivante

Switch	Ports	VLAN (untagged / tagged)
Rez-de-chaussée	22–48	VLAN 102 / – (shutdown)
1er étage	1–7	VLAN 20 / VLAN 90
1er étage	8–12	VLAN 30 / VLAN 90
1er étage	13–23	VLAN 40 / VLAN 90
1er étage	24	VLAN 50 / VLAN 90
1er étage	25	VLAN 100 / VLAN 80
1er étage	49–50	VLAN 101 / VLAN 10,20,30,40,50,60,70,80,90,100
1er étage	26–48, 51–52	VLAN 102 / – (shutdown)
2ème étage	1–28	VLAN 10 / VLAN 90
2ème étage	29	VLAN 50 / VLAN 90
2ème étage	30	VLAN 60 / VLAN 90
2ème étage	31	VLAN 100 / VLAN 80
2ème étage	49–50	VLAN 101 / VLAN 10,20,30,40,50,60,70,80,90,100
2ème étage	32–48, 51–52	VLAN 102 / – (shutdown)

TABLE 5.2 : Affectation des VLAN aux ports de chaque switch

4. Politiques FortiGate avec ACL et filtrage des flux pour réduire les risques.
 - configuration d'une route statique pour diriger le trafic vers internet.
 - Configuration du profil nommé **filtre zone** qui bloque la catégories **Internet Radio and TV**.
 - création d'une politique nommée **zone to wan** pour permettre l'accès à Internet depuis les VLANs (10,20,30,40,50,60,70) et en associe le profils de sécurité **filtre zone**.
 - Création d'une politique nommée **invité to internet** pour permettre l'accès à Internet depuis le VLAN 80 et en associe le profils de sécurité par défaut.
 - Créer et appliquer un **profil de filtrage web** pour bloquer l'accès à **Facebook** (Vlan 10,20,30,40,50,60,70).
 - Politique d'isolation entre **vlan80 (invite)** et les autre **vlan**
5. Les téléphones IP reçoivent des adresses (192.168.90.2–192.168.90.254) à partir de standard téléphonique dans le VLAN 90. QoS priorise le trafic RTP pour la qualité vocale.
6. Ajout d'une liaison entre le switchs Aruba premier étage et deuxième étage . MSTP est configuré pour éviter les boucles réseau, adapté aux VLANs multiples.
7. Activation de SNMPv3 (VLAN 100) pour le serveur SNMP et NTP pour synchronisation avec le FortiGate.
8. Déploiement de points d'accès pour chaque étage (VLAN 80 : 192.168.80.1–192.168.80.254 pour invités).

5.1.3 Synthèse

La conception répond aux critiques identifiées via une architecture hiérarchique, un plan d'adressage structuré et des solutions techniques adaptées. Des simulations sur **GNS3** ont validé la faisabilité des configurations VLAN, MSTP et QoS.

5.1.4 Choix d'Aruba par rapport à Cisco

Le choix d'Aruba, une société d'Hewlett Packard Enterprise (**HPE**) , s'explique par son positionnement stratégique en tant que **leader sur le marché des réseaux et de la sécurité**, confirmé par plusieurs cabinets d'analyse tels que Gartner et IDC . Aruba s'est distinguée ces dernières années par une approche innovante centrée sur la **sécurité intégrée (Zero Trust, Dynamic Segmentation)**, la **simplicité de gestion** grâce à ses solutions cloud natives (Aruba Central), ainsi que par une forte orientation vers les environnements modernes tels que le **SD-Branch**, le **SD-WAN** et les **architectures Campus hautement sécurisées**.

Comparativement à Cisco, qui reste un acteur historique incontournable, Aruba a su se différencier par une **agilité technologique** et un **rapport coût/performance attractif**, permettant aux organisations de bénéficier de fonctionnalités avancées sans complexité excessive. De plus, Aruba s'impose comme un pionnier dans la convergence **réseau + sécurité**, ce qui réduit la dépendance à des solutions tierces. Ce positionnement de leader reconnu, allié à une roadmap technologique claire et tournée vers l'IA et l'automatisation, motive le choix d'Aruba pour une infrastructure réseau moderne, évolutive et sécurisée, répondant pleinement aux exigences actuelles des entreprises et institutions.



FIGURE 5.2 : Choix d'Aruba par rapport à Cisco

5.2 Réalisation

5.2.1 Présentation du logiciel utilisé (GNS3)

GNS3 est un logiciel de simulation réseau permettant de modéliser des équipements virtuels et d'interconnecter des dispositifs réels, tels que des commutateurs **Aruba**, des pare-feux **FortiGate**, des téléphones IP ou des postes clients. Contrairement à des émulateurs basiques comme Packet Tracer, GNS3 s'appuie sur des systèmes d'exploitation réseau complets, offrant ainsi des fonctionnalités avancées identiques à celles des appareils physiques.

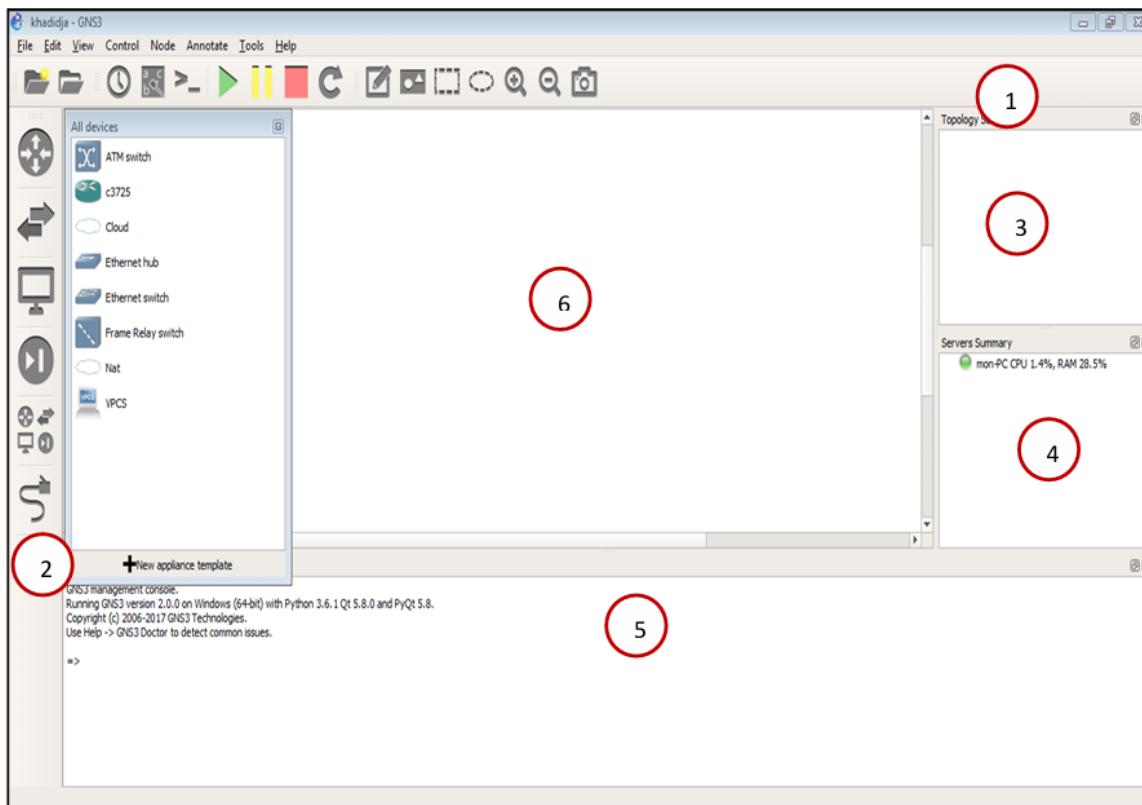


FIGURE 5.3 : l'environnement GNS3

L'un des avantages clé de GNS3 est l'intégration transparente entre équipements virtuels et réseau physique existant.

L'interface GNS3 structuré comme suit : Structure de

1. **Barre d'outils GNS3**
Contrôle principal (démarrage/arrêt des dispositifs)
2. **Équipements réseau**
Bibliothèque d'appareils (Aruba, FortiGate, routeurs Cisco)
3. **Topology Summary**
Vue d'ensemble de l'état du réseau
4. **Server Summary**
Gestion des ressources serveur

5. Console

Accès CLI pour configuration avancée

6. Espace de travail

Zone de conception des topologies

5.2.2 Installation des périphériques

5.2.2.1 FortiGate

Cette section décrit les étapes pour installer FortiGate dans GNS3 en utilisant des modèles préconfigurés (appliances).

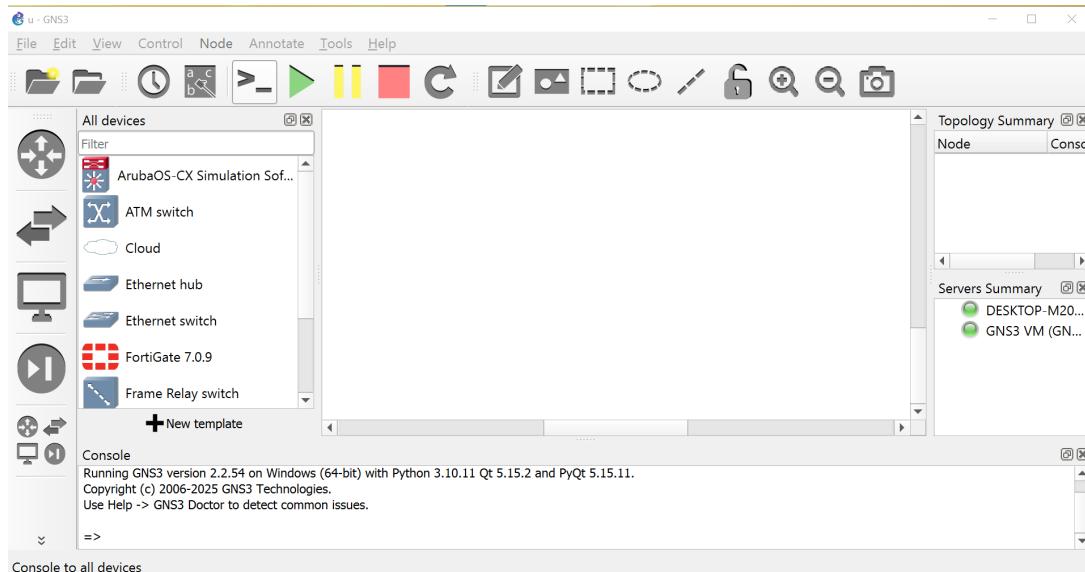


FIGURE 5.4 : Interface principale de GNS3 avec la liste des périphériques disponibles.

La figure 5.4 montre l’interface principale de GNS3. Pour ajouter un nouveau périphérique, il faut d’abord créer un nouveau modèle (+New template) en sélectionnant l’option appropriée.

Comme illustré dans la figure 5.5, trois options sont proposées :

- Installation d’une appliance depuis le serveur GNS3 (recommandé)
- Importation d’un fichier d’appliance (.gns3a)
- Création manuelle d’un nouveau modèle

CHAPITRE 5. CONCEPTION ET RÉALISATION

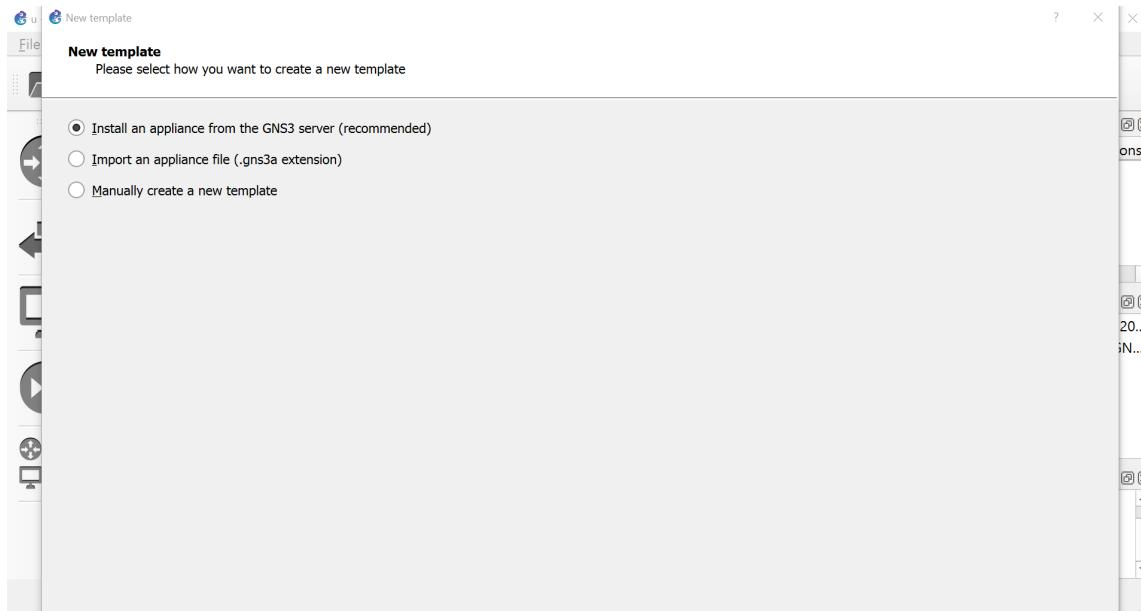


FIGURE 5.5 : Options de création d'un nouveau modèle dans GNS3

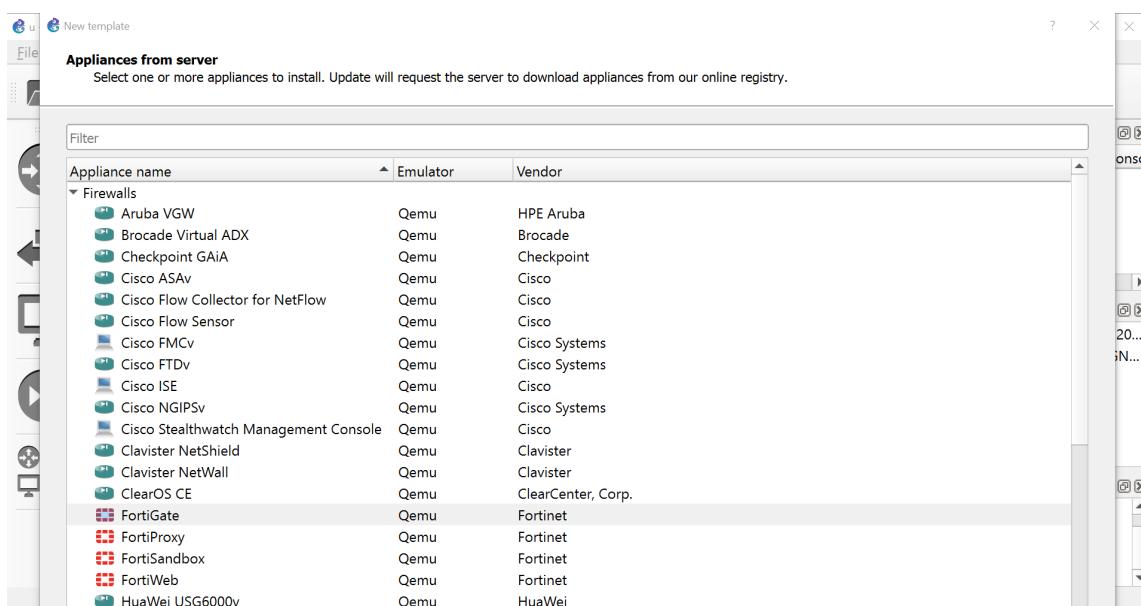


FIGURE 5.6 : Liste des appliances disponibles depuis le serveur GNS3.

La figure 5.6 présente la liste des appliances disponibles. FortiGate y apparaît comme une option, utilisant l'émulateur Qemu et développé par Fortinet.

La figure 5.7 montre les options pour choisir l'emplacement d'installation :

- Serveur distant
- GNS3 VM (recommandé)
- Ordinateur local

CHAPITRE 5. CONCEPTION ET RÉALISATION

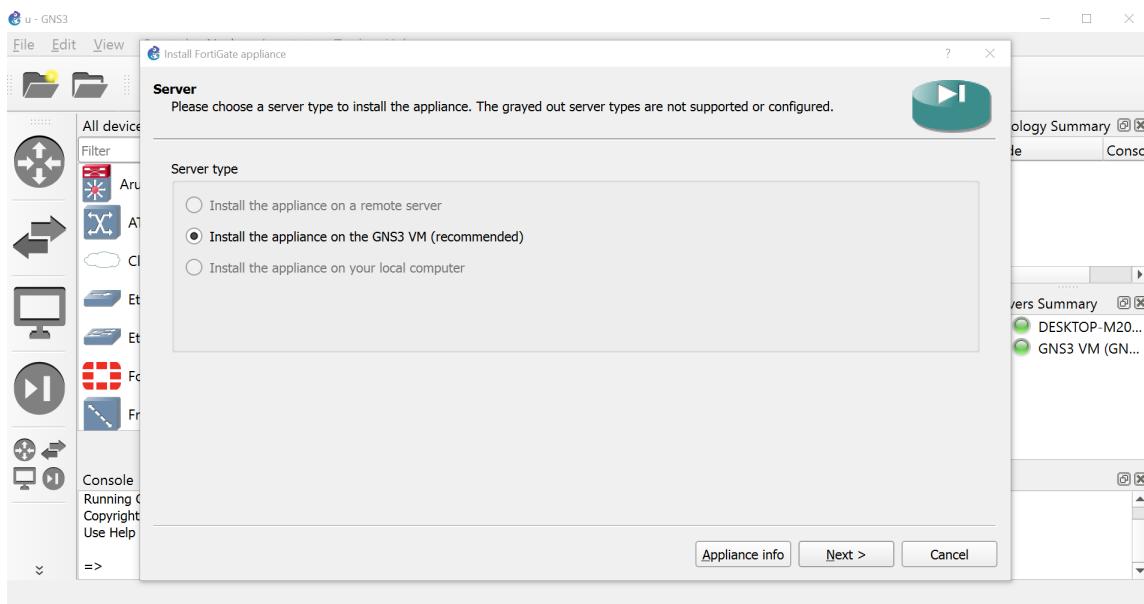


FIGURE 5.7 : Sélection du type de serveur pour l'installation de l'apppliance.

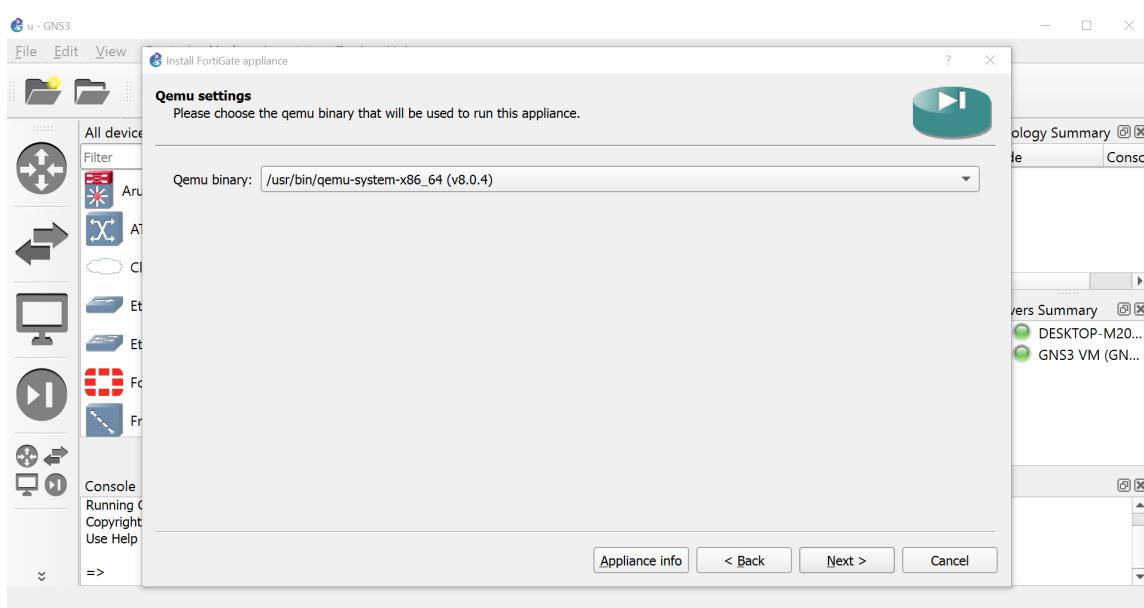


FIGURE 5.8 : Configuration du binaire Qemu pour exécuter l'apppliance.

La figure 5.8 permet de configurer le binaire Qemu (Quick Emulator) qui sera utilisé pour exécuter l'apppliance FortiGate. Le chemin et la version du binaire sont affichés (/usr/bin/qemu-system-x86_64 v8.0.4 dans cet exemple).

Comme montré dans la figure 5.9, il est nécessaire de spécifier une version pour l'apppliance FortiGate. La version 7.0.9 est sélectionnée dans notre cas.

CHAPITRE 5. CONCEPTION ET RÉALISATION

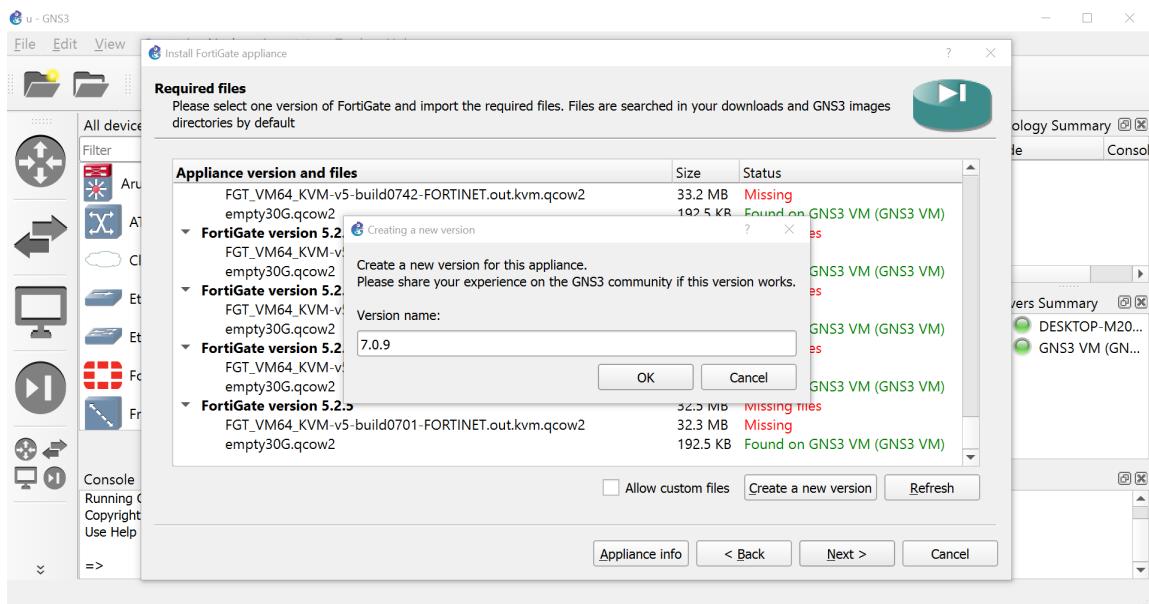


FIGURE 5.9 : Création d'une nouvelle version de l'apppliance (7.0.9).

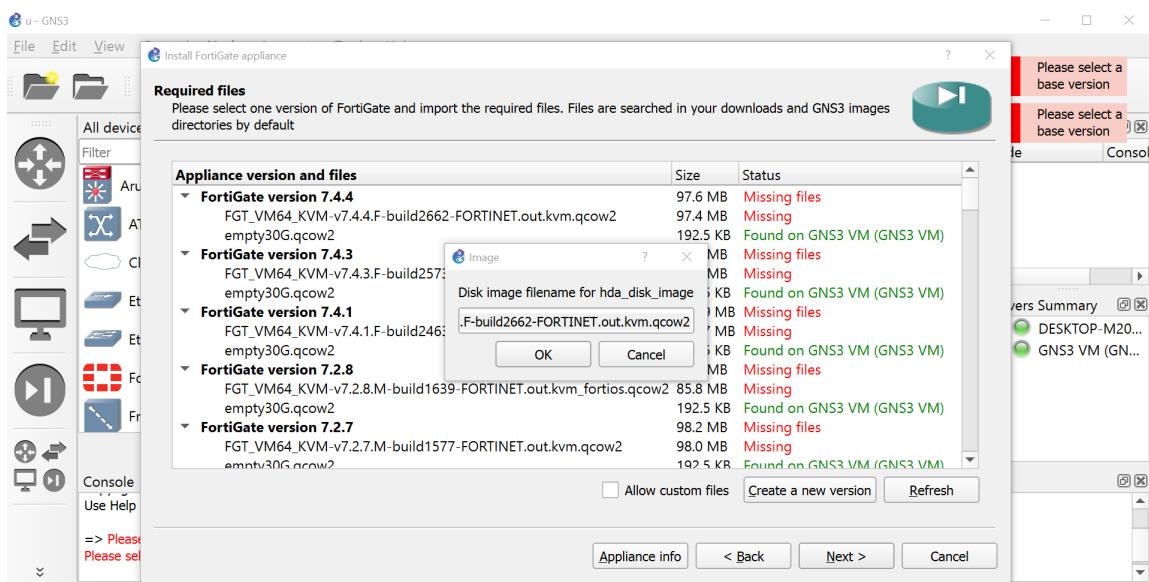


FIGURE 5.10 : Sélection de l'image disque principale (hda) pour FortiGate.

Les figures 5.10 et 5.11 illustrent la sélection des images disques :

- hda_disk_image : Contient le système d'exploitation FortiOS (F-build2662-FORTINET.out.kvm.qcow2)
- hdb_disk_image : Disque de stockage secondaire (empty30G.qcow2)

CHAPITRE 5. CONCEPTION ET RÉALISATION

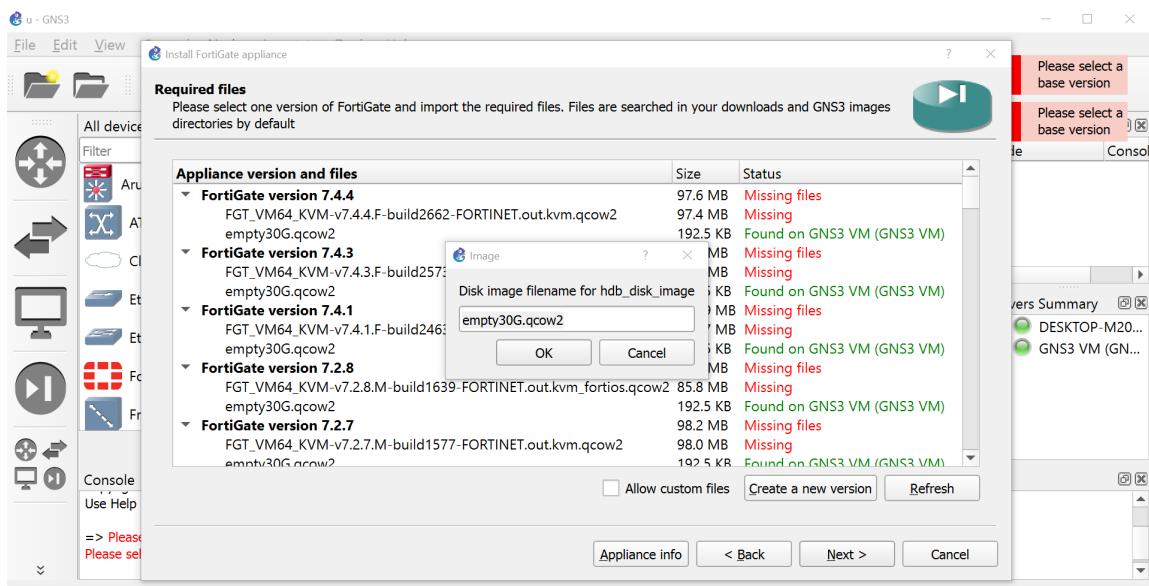


FIGURE 5.11 : Sélection de l'image disque secondaire (hdb).

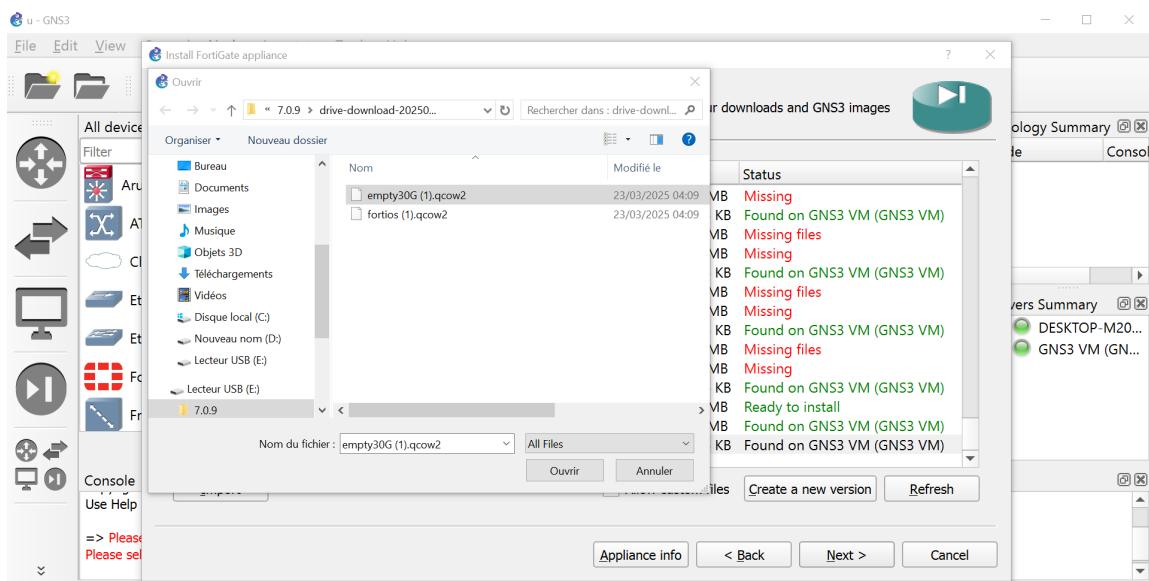


FIGURE 5.12 : Interface de navigation pour sélectionner les fichiers image.

La figure 5.12 montre l'interface de sélection des fichiers, permettant de naviguer dans l'arborescence des dossiers locaux pour trouver les images requises.

La figure 5.13 présente différentes versions de FortiGate disponibles, avec pour chaque version :

- Le nom du fichier image KVM
- Le fichier de disque vide associé (30GB)
- La possibilité de créer une nouvelle version personnalisée

CHAPITRE 5. CONCEPTION ET RÉALISATION

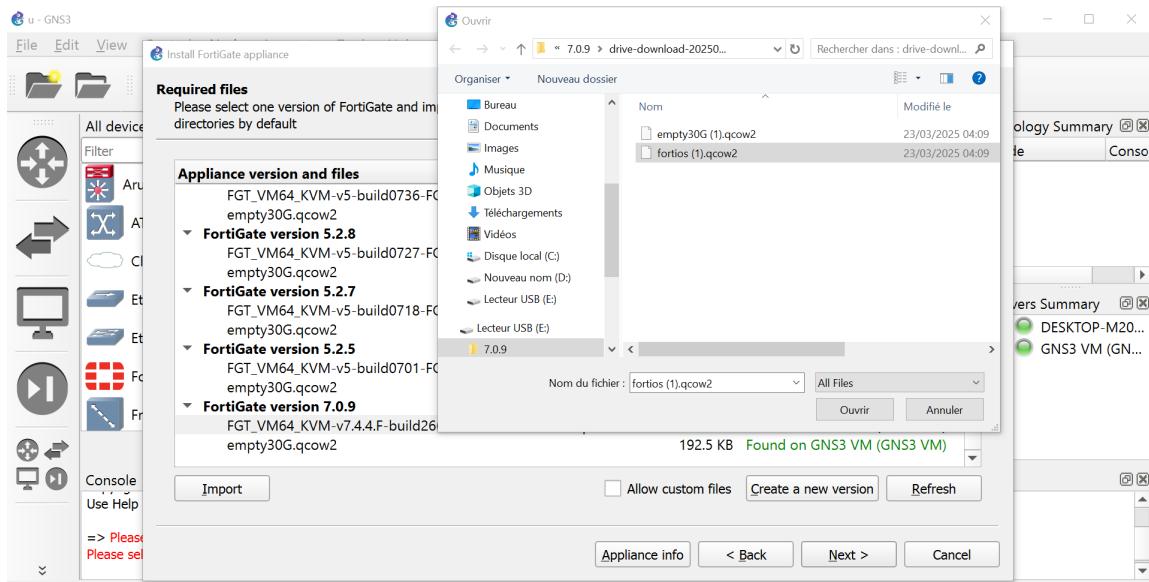


FIGURE 5.13 : Liste des versions disponibles de FortiGate et leurs fichiers associés.

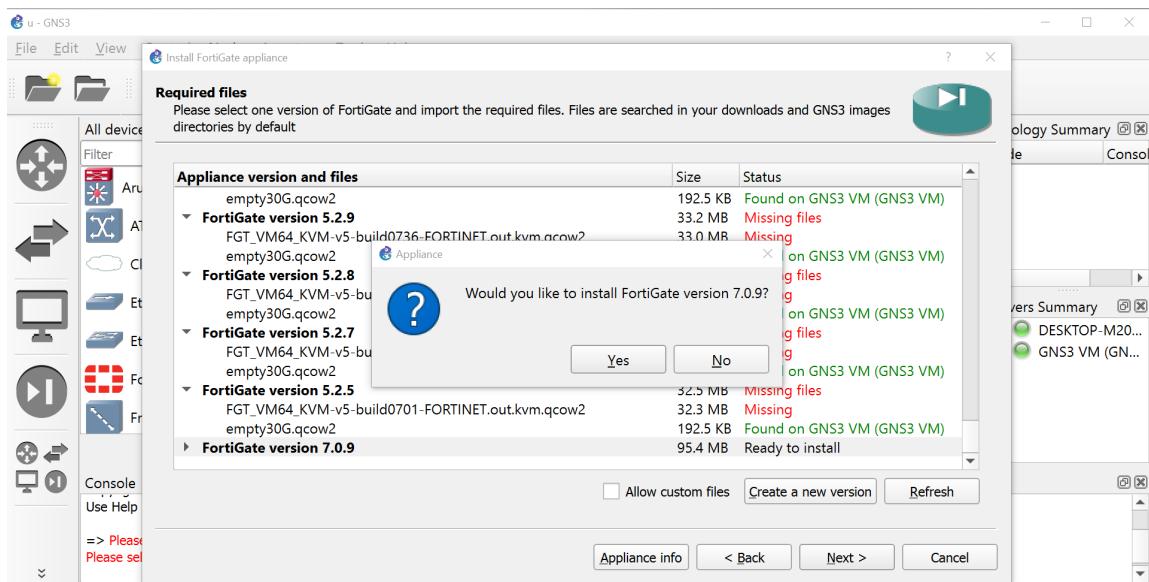


FIGURE 5.14 : Confirmation finale pour installer FortiGate version 7.0.9.

Avant l'installation (figure 5.14), GNS3 demande une confirmation finale. Cette étape permet de vérifier que la bonne version a été sélectionnée.

Après installation (figure 5.15), GNS3 fournit des informations importantes :

- Identifiants par défaut : admin (sans mot de passe)
- Exigences matérielles : 2GB RAM minimum pour les versions $\geq 7.0.0$
- Avertissement sur les limitations des licences d'essai pour versions $> 7.2.0$
- Emplacement du modèle : Catégorie "Firewall"

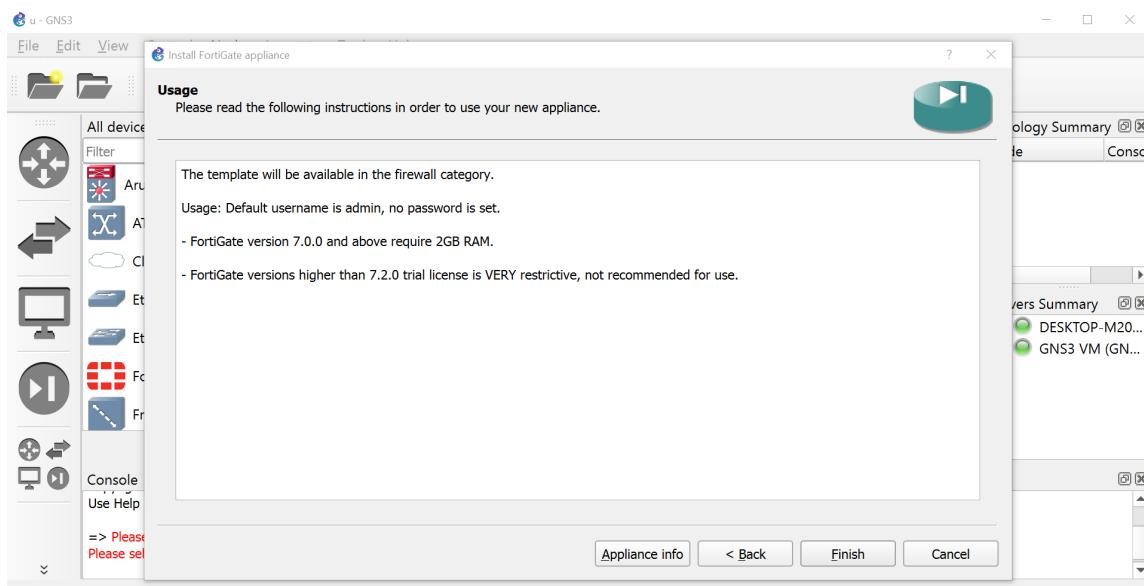


FIGURE 5.15 : Instructions d'utilisation après installation.

Processus complet résumé :

1. Création d'un nouveau modèle
2. Sélection de l'appliance FortiGate depuis le serveur
3. Choix de l'emplacement d'installation (GNS3 VM recommandé)
4. Configuration du binaire Qemu
5. Cr éation d'une version sp cifique (7.0.9)
6. S election des images disques (hda et hdb)
7. Navigation dans l'arborescence pour localiser les fichiers
8. V erification des versions disponibles
9. Confirmation de l'installation
10. Lecture des instructions post-installation

5.2.2.2 Windows 10

Cette section explique comment installer une machine virtuelle Windows 10 dans GNS3 à partir des appliances disponibles.

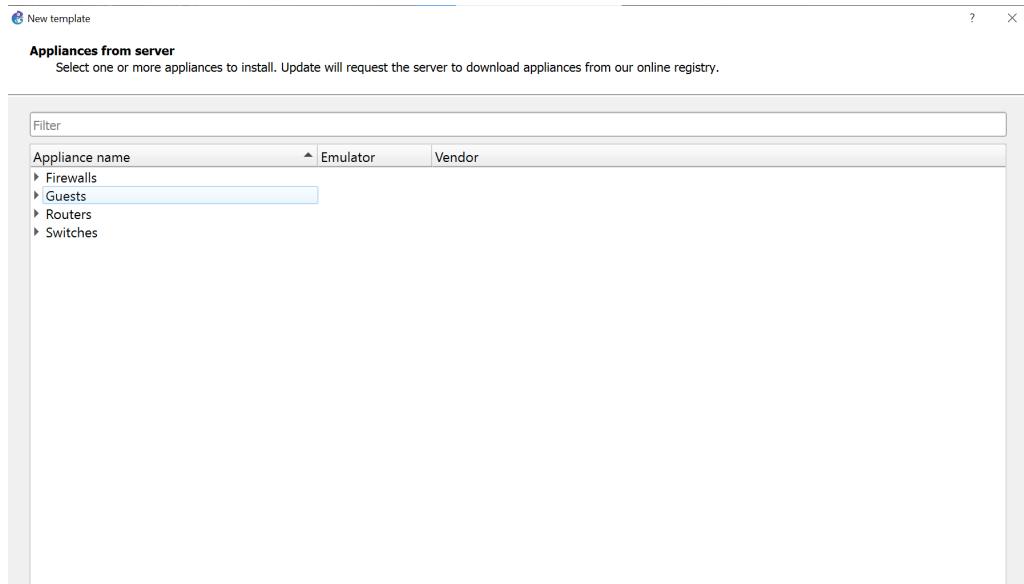


FIGURE 5.16 : Menu de sélection des appliances dans GNS3.

Pour commencer (figure 5.16) :

1. Créez un nouveau template via **[+New template]**
2. Sélectionnez **Appliances from server**
3. Filtrez par catégorie "Guests" ou recherchez "Windows"

The screenshot shows the same 'Appliances from server' selection screen as Figure 5.16, but with a different focus. The 'Windows' appliance is now highlighted with a blue selection bar. The table below lists various appliances with their details:

Appliance name	Emulator	Vendor
ReactOS	Qemu	ReactOS Project
RHEL	Qemu	Red Hat
RockyLinux	Qemu	Rocky Enterprise Software Foundation
Security Onion	Qemu	Security Onion Solutions, LLC
Sophos iView	Qemu	Sophos
SteelHead	Qemu	Riverbed Technology
TacacsGUI	Qemu	TacacsGUI
Tiny Core Linux	Qemu	Team Tiny Core
Toolbox	Docker	Ubuntu
TrueNAS	Qemu	iSystems
Ubuntu Cloud Guest	Qemu	Canonical Inc.
Ubuntu Desktop Guest	Qemu	Canonical Inc.
Ubuntu Docker Guest	Docker	Canonical
vRIN	Qemu	Andras Dosztal
webterm	Docker	webterm
Windows	Qemu	Microsoft
Windows Server	Qemu	Microsoft
Windows XP	Qemu	Microsoft
Windows-11-Dev-Env	Qemu	Microsoft
WordPress	Docker	Turnkey Linux

FIGURE 5.17 : Liste des appliances Windows disponibles.

La figure 5.17 montre les versions disponibles :

- Windows 10 avec Edge (recommandé)
- Windows 8.1/7 avec différentes versions d'IE
- Taille : 6.8GB à 10.2GB selon la version

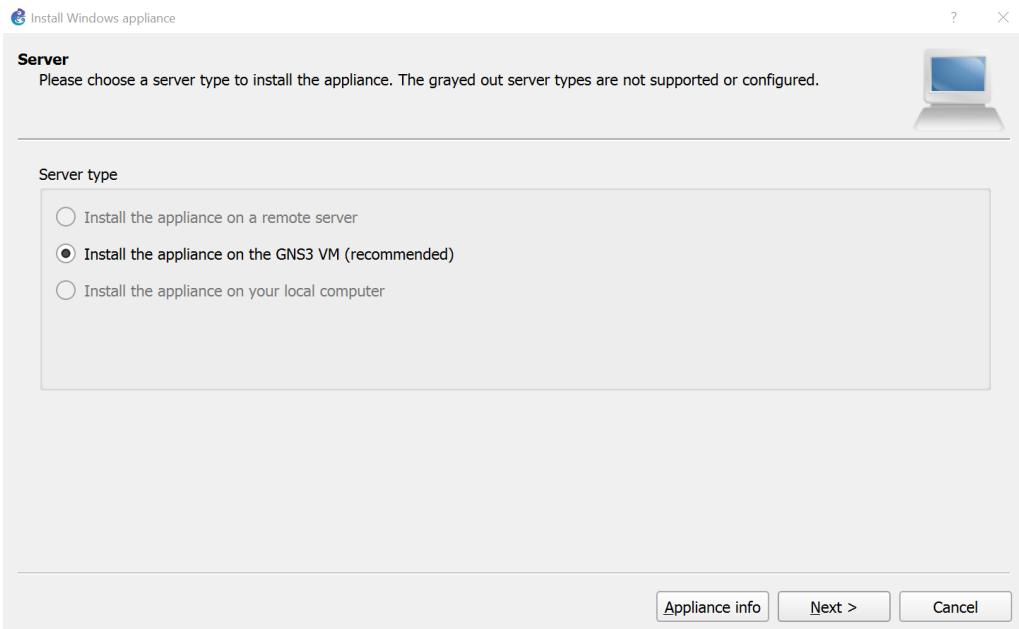


FIGURE 5.18 : Sélection du serveur d'exécution.

Configuration du serveur (figure 5.18) :

- Choisissez **GNS3 VM** pour de meilleures performances
- Alternative : Ordinateur local (si ressources suffisantes)

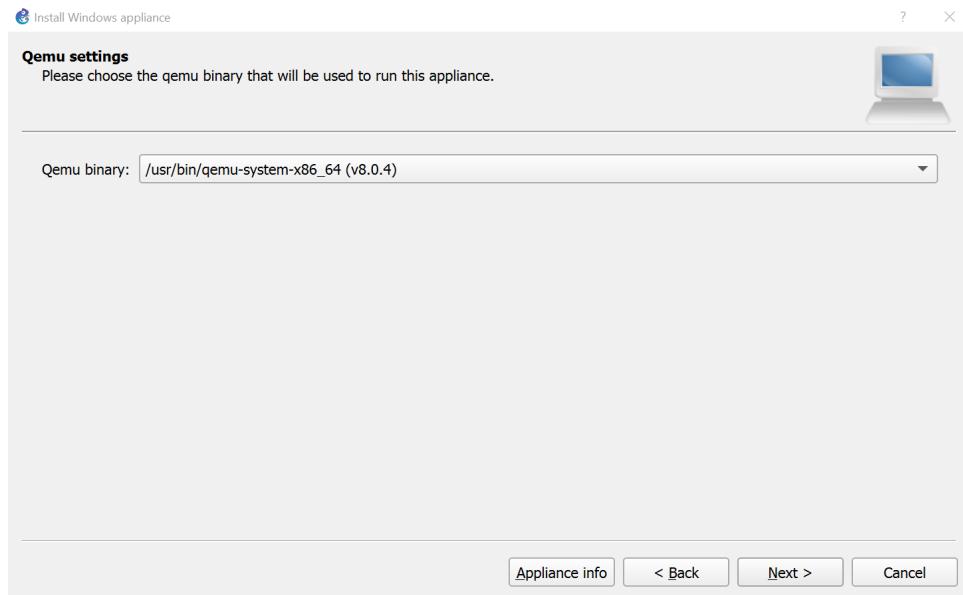


FIGURE 5.19 : Configuration du binaire Qemu.

La figure 5.19 montre la configuration requise :

- Binaire Qemu : `/usr/bin/qemu-system-x86_64`
- Version : 8.0.4 (minimum recommandé)

CHAPITRE 5. CONCEPTION ET RÉALISATION

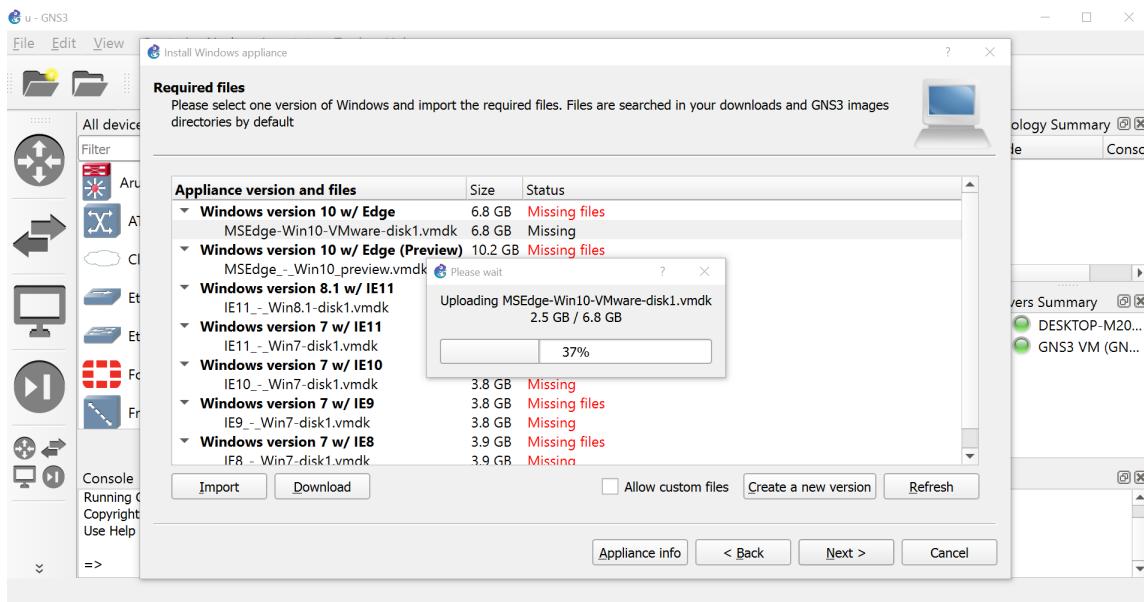


FIGURE 5.20 : Téléchargement du fichier VMDK (6.8GB pour Win10).

Processus de téléchargement (figure 5.20) :

- Fichier requis : MSEdge-Win10-VMware-disk1.vmdk
- Progression affichée (37% dans l'exemple)
- Temps estimé : Variable selon la connexion internet

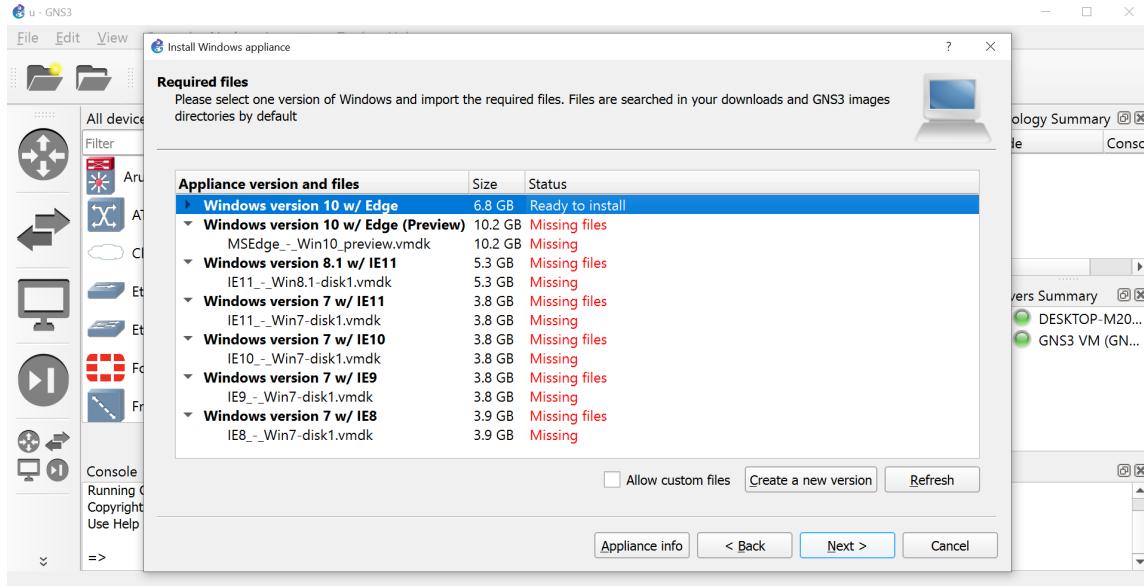


FIGURE 5.21 : Statut des fichiers après téléchargement.

La figure 5.21 confirme :

- Statut : **Ready to install** pour Windows 10
- Taille effective : 6.8GB
- Versions alternatives toujours manquantes

Avant installation (figure 5.22) :

CHAPITRE 5. CONCEPTION ET RÉALISATION

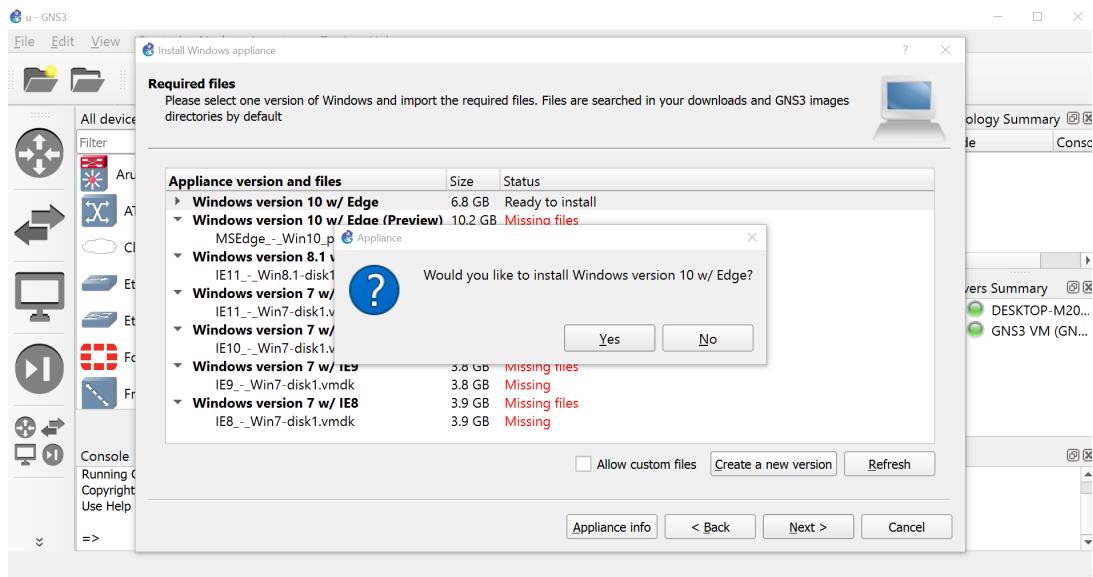


FIGURE 5.22 : Confirmation finale avant installation.

- Confirmez avec **Yes**
- Option de création de version personnalisée disponible

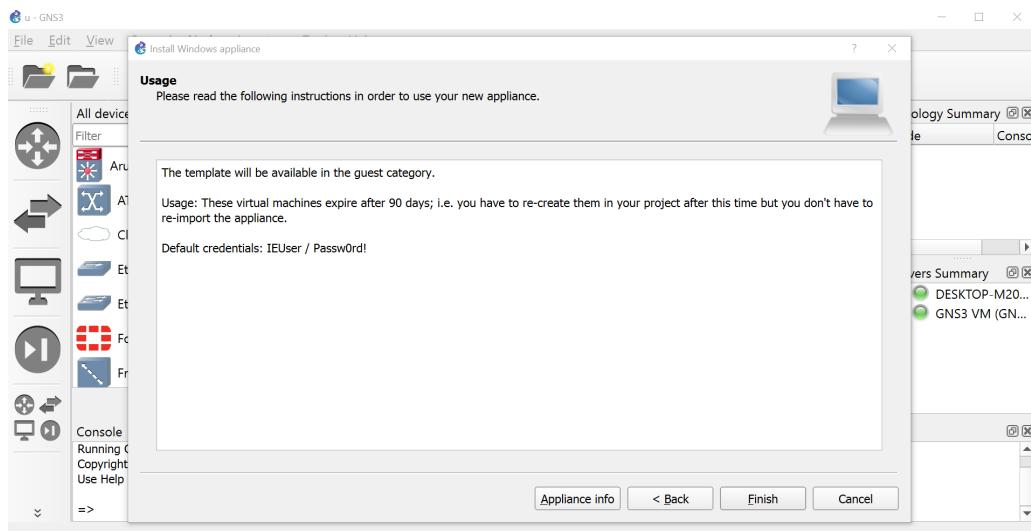


FIGURE 5.23 : Instructions post-installation.

Après installation (figure 5.23) :

- Catégorie : **Guest**
- Identifiants par défaut :
 - Login : **IEUser**
 - Mot de passe : **Passw0rd!**
- Durée de vie : 90 jours (recréation nécessaire ensuite)

Remarque importante : Ces images sont fournies par Microsoft à des fins de test et expireront après 90 jours. Pour une utilisation permanente, utilisez une licence Windows valide.

5.2.2.3 Switch Aruba

Cette section décrit le processus d'installation du simulateur Aruba AOS-CX dans GNS3.

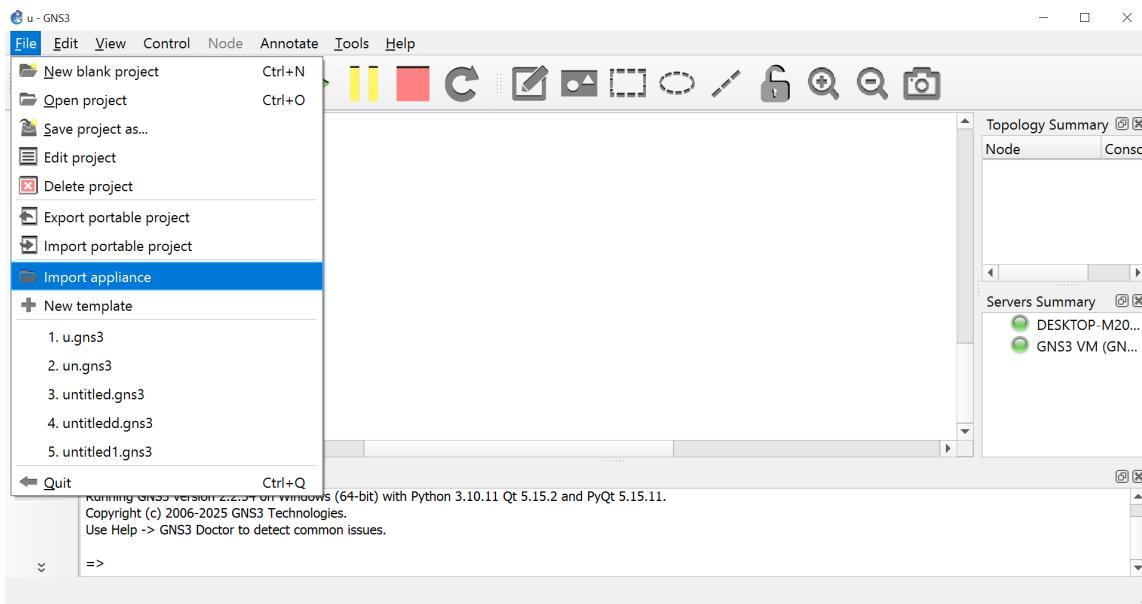


FIGURE 5.24 : Menu principal de GNS3 avec l'option d'import d'appliance.

Comme illustré dans la figure 5.24, le processus commence par sélectionner **Import appliance** dans le menu principal de GNS3.

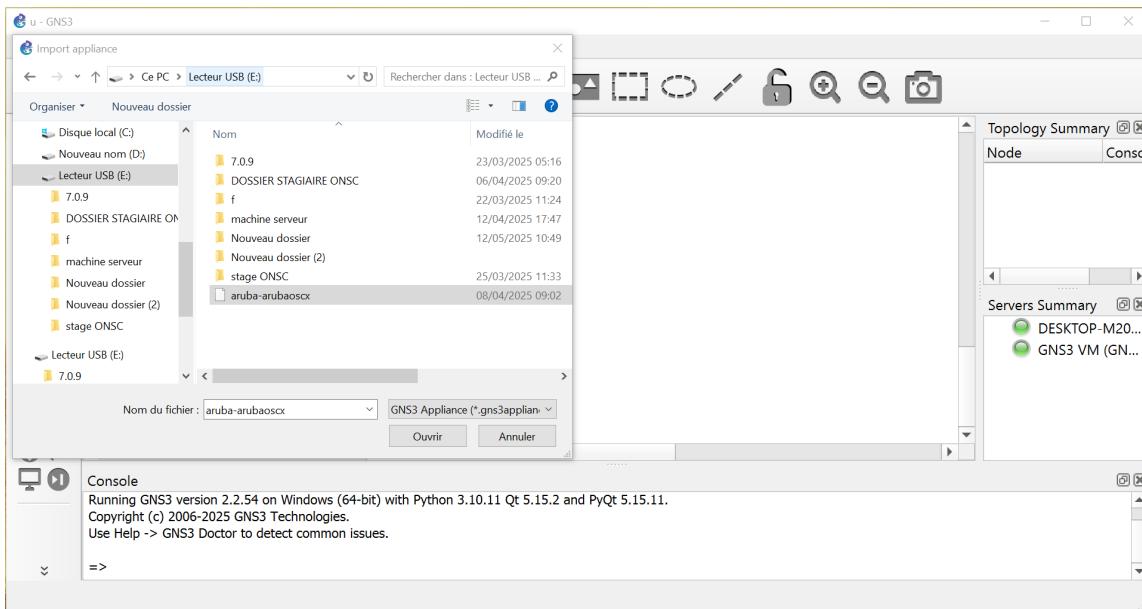


FIGURE 5.25 : Navigation vers le fichier appliance Aruba (.gns3a).

La figure 5.25 montre la sélection du fichier appliance depuis un lecteur USB. Le fichier spécifique à Aruba (aniba-anibaoosc.gns3a dans cet exemple) doit être localisé.

CHAPITRE 5. CONCEPTION ET RÉALISATION

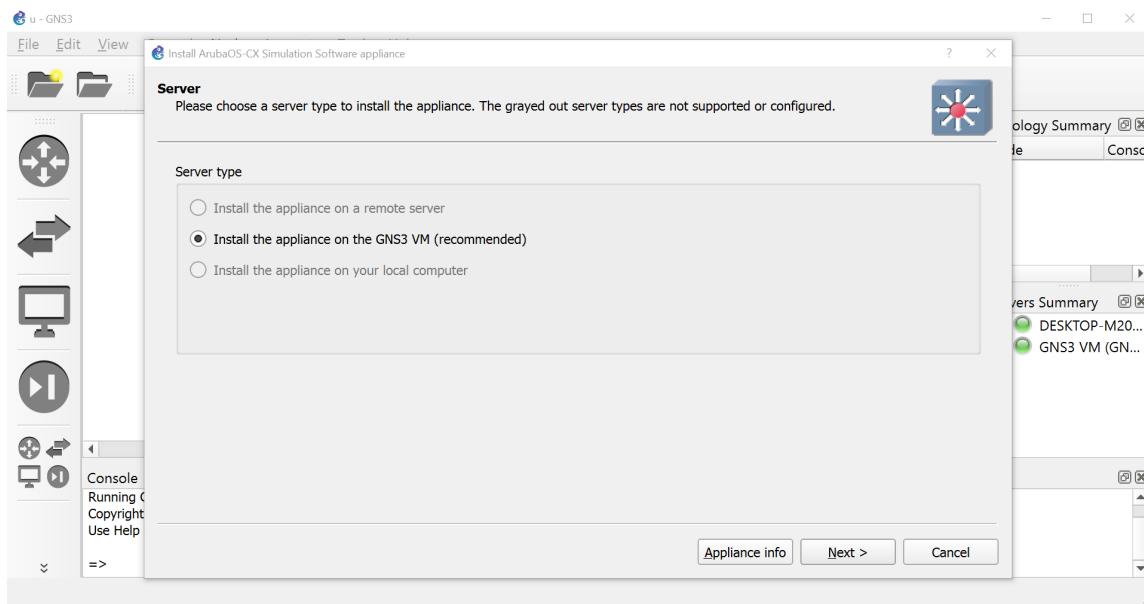


FIGURE 5.26 : Sélection du type de serveur (GNS3 VM recommandé).

Comme visible dans la figure 5.26, il est recommandé d'installer l'appliance sur la **GNS3 VM** pour des performances optimales.

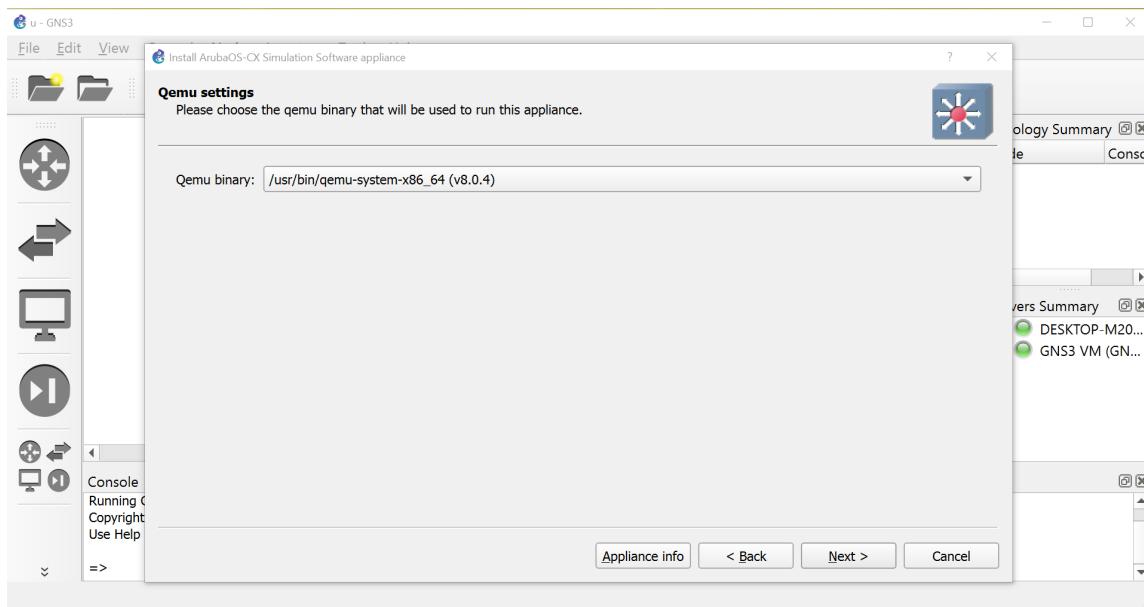


FIGURE 5.27 : Configuration du binaire Qemu (version 8.0.4).

La figure 5.27 montre la configuration du binaire Qemu qui exécutera le simulateur Aruba. Le chemin par défaut est `/usr/bin/qemu-system-x86_64`.

La figure 5.28 présente les différentes versions disponibles :

- **10.15.0005** : Prête à installer (400.6 MB)
- Versions antérieures : Fichiers manquants

CHAPITRE 5. CONCEPTION ET RÉALISATION

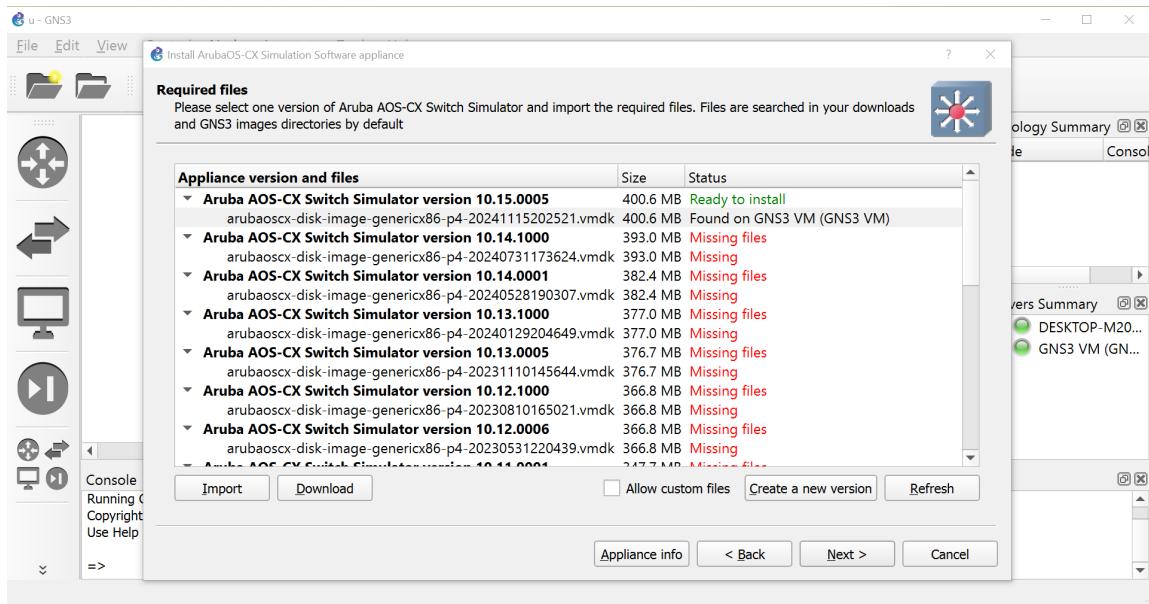


FIGURE 5.28 : Sélection de la version d'Aruba AOS-CX .

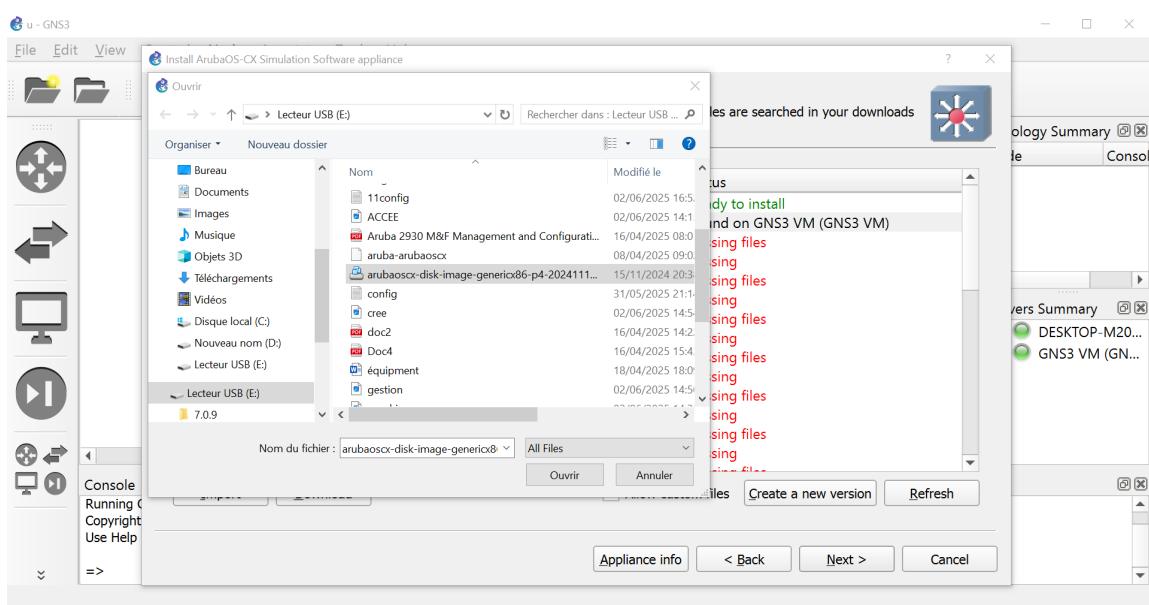


FIGURE 5.29 : Sélection du fichier image VMDK pour Aruba.

La figure 5.29 montre la navigation vers le fichier image requis :

- Nom du fichier : arubaoscx-disk-image-genericx86-p4-20241115202521.vmdk
- Taille : 400.6 MB
- Localisation : Lecteur USB (E)

Avant l'installation (figure 5.30), une confirmation finale est demandée pour la version 10.15.0005.

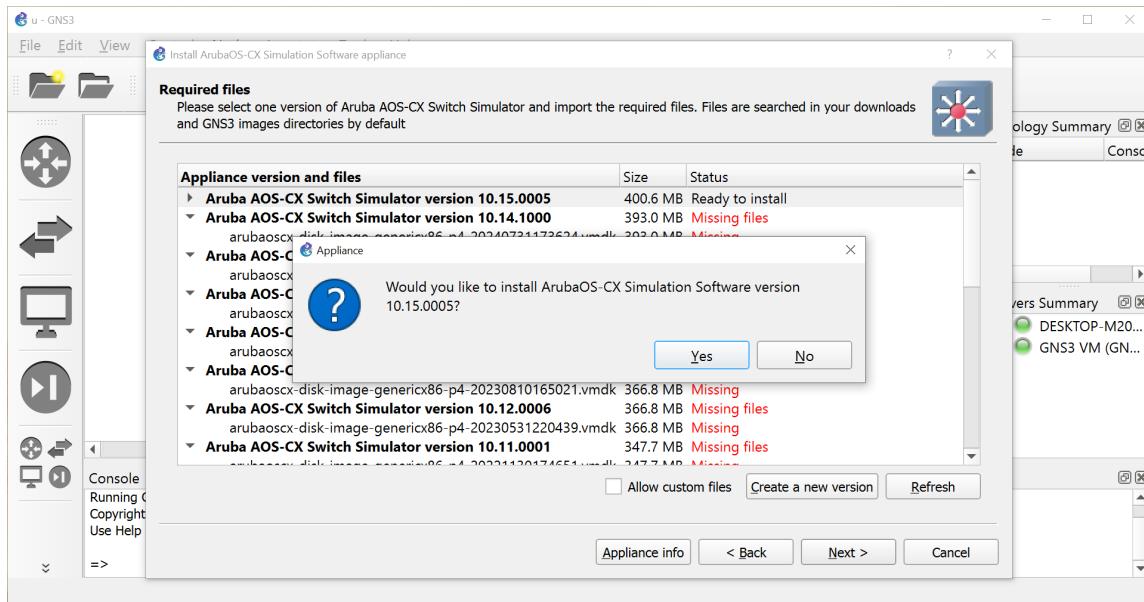


FIGURE 5.30 : Confirmation d’installation de la version 10.15.0005.

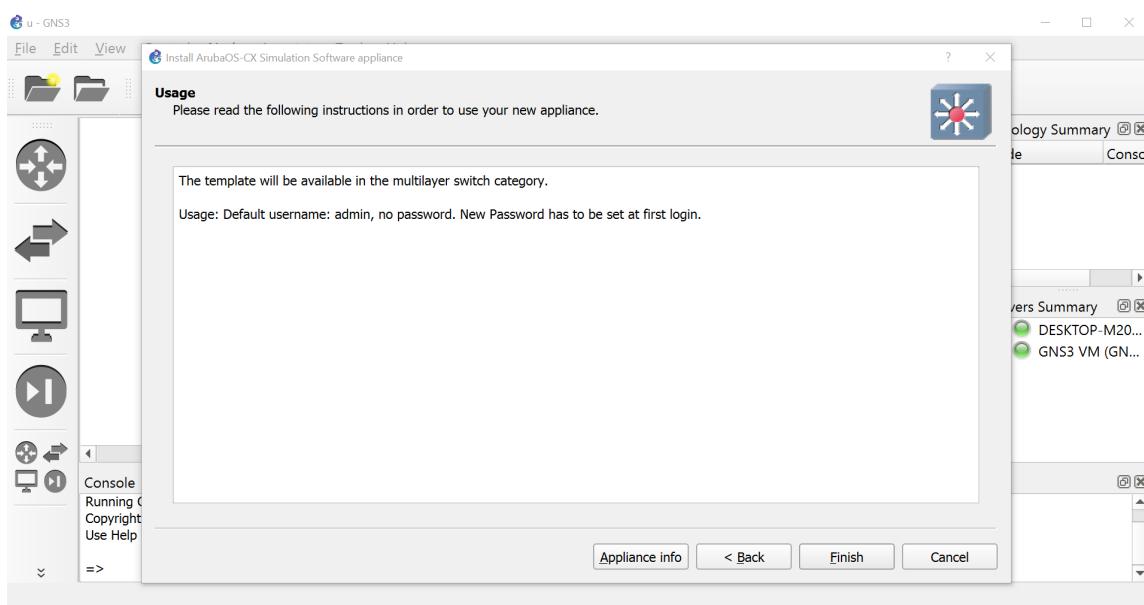


FIGURE 5.31 : Instructions post-installation pour Aruba AOS-CX.

Après installation (figure 5.31), GNS3 fournit les informations importantes :

- Catégorie : **Multilayer switch**
- Identifiants : admin (pas de mot de passe initial)
- Obligation de définir un mot de passe au premier login

Processus complet résumé :

1. Importer l’appliance (.gns3a) depuis le stockage local
2. Choisir la GNS3 VM comme serveur cible
3. Configurer le binaire Qemu

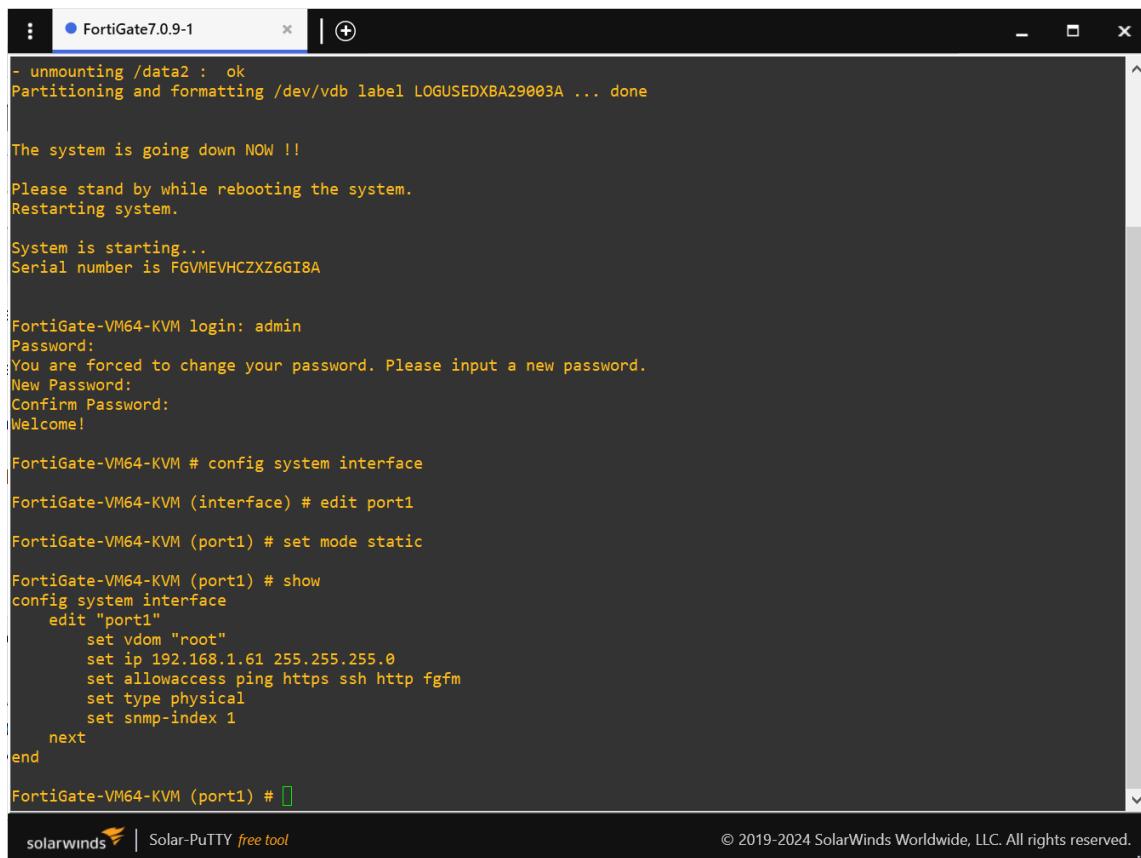
4. Sélectionner la version 10.15.0005 (si disponible)
5. Localiser le fichier image VMDK correspondant
6. Confirmer l'installation
7. Noter les informations de connexion

5.2.3 Pare-feu

Cette sous-section présente la mise en œuvre pratique d'un pare-feu FortiGate VM64-KVM, une solution de sécurité réseau largement utilisée dans les environnements virtuels. Nous détaillons ici les étapes d'accès, de configuration initiale et de surveillance, en mettant en avant les outils et les interfaces utilisés.

5.2.3.1 Accéder au FortiGate

L'accès au pare-feu FortiGate peut se faire de deux manières principales : via l'interface en ligne de commande (CLI) pour une configuration précise et via l'interface graphique (GUI) pour une gestion simplifiée. Cette section décrit ces deux approches, en commençant par la configuration initiale via CLI.



The screenshot shows a terminal window titled "FortiGate7.0-9-1". The session is running on a FortiGate-VM64-KVM. The terminal output is as follows:

```
- unmounting /data2 : ok
Partitioning and formatting /dev/vdb label LOGUSEDXBA29003A ... done

The system is going down NOW !!

Please stand by while rebooting the system.
Restarting system.

System is starting...
Serial number is FGVMEVHCZXZ6GI8A

FortiGate-VM64-KVM login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Welcome!

FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit port1
FortiGate-VM64-KVM (port1) # set mode static
FortiGate-VM64-KVM (port1) # show
config system interface
  edit "port1"
    set vdom "root"
    set ip 192.168.1.61 255.255.255.0
    set allowaccess ping https ssh http fgfm
    set type physical
    set snmp-index 1
  next
end
FortiGate-VM64-KVM (port1) # 
```

SolarWinds logo | Solar-PuTTY free tool © 2019-2024 SolarWinds Worldwide, LLC. All rights reserved.

FIGURE 5.32 : Configuration initiale via CLI

La Figure 5.32 illustre les premières étapes de configuration du pare-feu FortiGate VM64-KVM via l'interface en ligne de commande (CLI), accessible à l'aide d'un outil tel que Solar-PuTTY. Lors de la première connexion, le système redémarre après le partitionnement et le formatage du disque (`/dev/vdb`). Une fois le démarrage terminé, l'utilisateur se connecte avec le compte `admin` et est immédiatement invité à modifier le mot

de passe par défaut pour des raisons de sécurité. Ensuite, la commande `config system interface` est utilisée pour accéder à la configuration de l'interface réseau `port1`. La sous-commande `edit port1` permet de définir les paramètres réseau : `set mode static` configure l'interface en mode statique, `set ip 192.168.1.61 255.255.255.0` attribue une adresse IP statique, et `set allowaccess ping https ssh http` active les services nécessaires pour l'accès à distance et la gestion (ping pour le dépannage, HTTPS et HTTP pour l'interface web, SSH pour un accès CLI sécurisé). Enfin, `set snmp-index 1` définit un index SNMP pour la gestion réseau. Cette configuration initiale est essentielle pour établir une connectivité réseau fonctionnelle et sécurisée, permettant l'accès au pare-feu via son adresse IP.

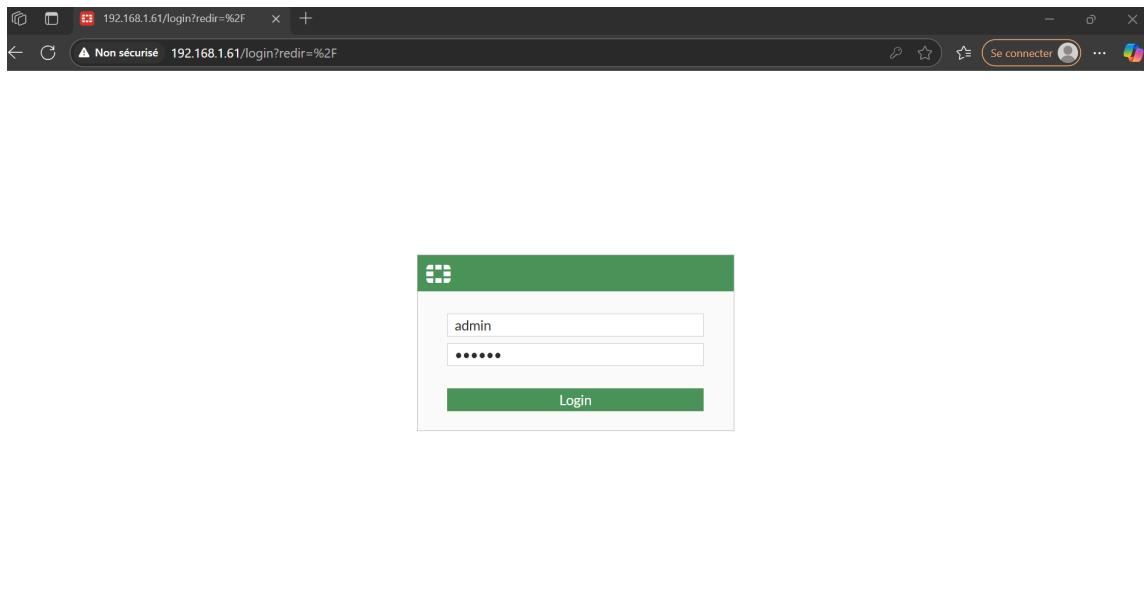


FIGURE 5.33 : Interface de connexion web du FortiGate

Une fois la connectivité réseau établie, l'interface graphique (GUI) du FortiGate devient accessible, comme illustré dans la Figure 5.33. Cette interface web, accessible via un navigateur à l'adresse 192.168.1.61, permet une gestion simplifiée du pare-feu. L'utilisateur se connecte avec les identifiants administrateur (`admin` et le mot de passe défini précédemment). Il est à noter que l'accès via HTTP/HTTPS nécessite une connexion non sécurisée (HTTP) dans cet exemple, ce qui est signalé par le navigateur comme "non sécurisé". Dans un environnement de production, il est recommandé d'activer un certificat SSL pour sécuriser les communications. Cette interface web offre une alternative conviviale à la CLI, particulièrement pour les administrateurs novices ou pour des tâches de configuration rapide, telles que la gestion des politiques de sécurité ou la surveillance des performances.

Après connexion à l'interface web, le tableau de bord du FortiGate, présenté dans la Figure 5.34, fournit une vue d'ensemble des informations système et des performances de la machine virtuelle. Les informations clés incluent le nom d'hôte (`FortiGate-VM64-KVM`), le numéro de série (`FGVMEVHCXZ6G18A`), et la version du firmware (7.0.9 build0444, Mature). Le tableau de bord affiche également l'état des ressources allouées à la machine virtuelle : 1 vCPU utilisé à 100% et 2 Go de RAM à 98% d'utilisation, indiquant une charge élevée qui pourrait nécessiter une augmentation des ressources pour éviter des ralentissements. La section "Licenses" révèle un problème : le pare-feu n'a pas réussi à

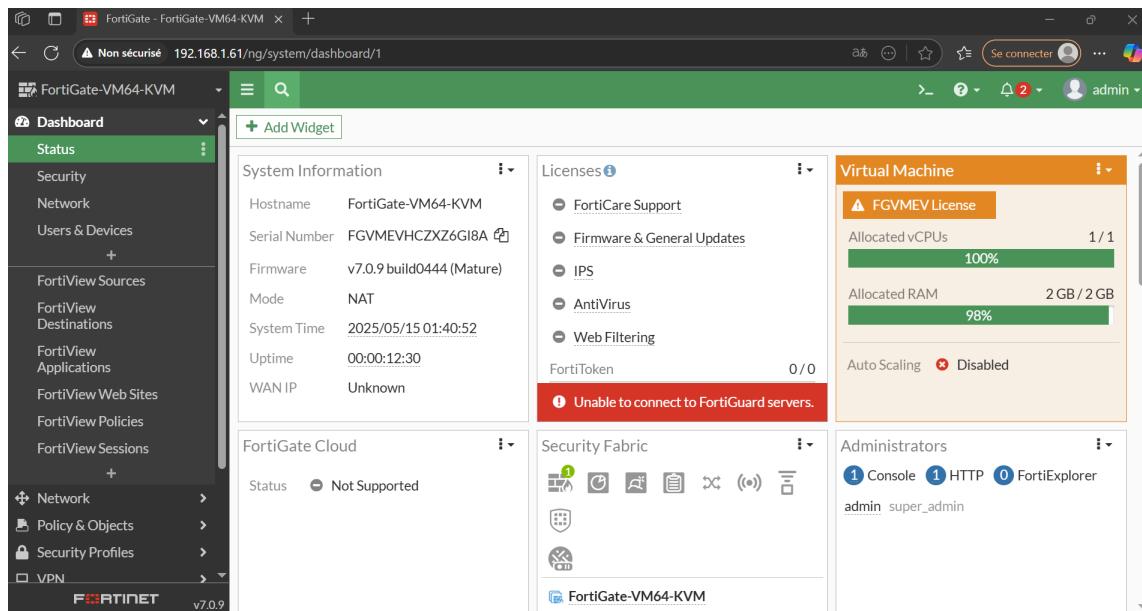


FIGURE 5.34 : Tableau de bord du FortiGate

se connecter aux serveurs FortiGuard, ce qui peut affecter les mises à jour de sécurité (antivirus, filtrage web, etc.). Ce problème pourrait être dû à une configuration réseau incorrecte ou à une licence non activée. Le tableau de bord est un outil précieux pour surveiller l'état du pare-feu, diagnostiquer les problèmes et planifier les ajustements nécessaires.

5.2.3.2 Création des VLANs du service

Pour isoler le réseau par service, un VLAN dédié est créé avec des paramètres spécifiques pour répondre aux besoins de ces services.

La Figure 5.35 montre l'interface graphique du FortiGate pour la création d'une nouvelle interface VLAN. À partir du menu **Network > Interfaces**, l'administrateur clique sur **Create New > Interface** pour ajouter une nouvelle interface. Cette étape est le point de départ pour configurer les VLANs, permettant de segmenter le réseau en sous-réseaux logiques.

La Figure 5.36 présente la configuration initiale du VLAN pour le secrétariat. L'interface est nommée **secretariat** avec un alias **vlan20**, utilisant le protocole 802.1Q sur l'interface physique **port2**. L'ID VLAN est défini à 20, et le rôle est **LAN**. L'adresse de la passerelle est configurée en mode manuel avec une adresse IP **192.168.20.1/24**, et un objet d'adresse correspondant (**secretariat_address**) est créé automatiquement pour faciliter la gestion des politiques de sécurité.

La Figure 5.37 détaille les paramètres d'accès et de DHCP pour le VLAN secrétariat. Les accès administratifs **HTTPS**, **SSH**, **PING**, et **SNMP** sont activés pour permettre la gestion et le dépannage de l'interface. Un serveur DHCP est activé (**DHCP Server > Enable**) avec une plage d'adresses **192.168.20.10 à 192.168.20.254**, un masque de sous-réseau **255.255.255.0**, et une passerelle par défaut correspondant à l'adresse de l'interface (**192.168.20.1**). Le serveur DNS est configuré pour utiliser le même DNS que le système, et la durée du bail DHCP est fixée à **604800** secondes (7 jours).

La Figure 5.38 montre les paramètres avancés pour le VLAN secrétariat. La détection de périphériques (**Device Detection**) est activée pour identifier les appareils connectés

CHAPITRE 5. CONCEPTION ET RÉALISATION

au VLAN, ce qui est utile pour le monitoring et la sécurité. La durée du bail DHCP est confirmée à 604800 secondes, et les options de mise en forme du trafic (**Traffic Shaping**) restent désactivées pour ce VLAN, car aucune limitation de bande passante n'est requise dans ce cas.

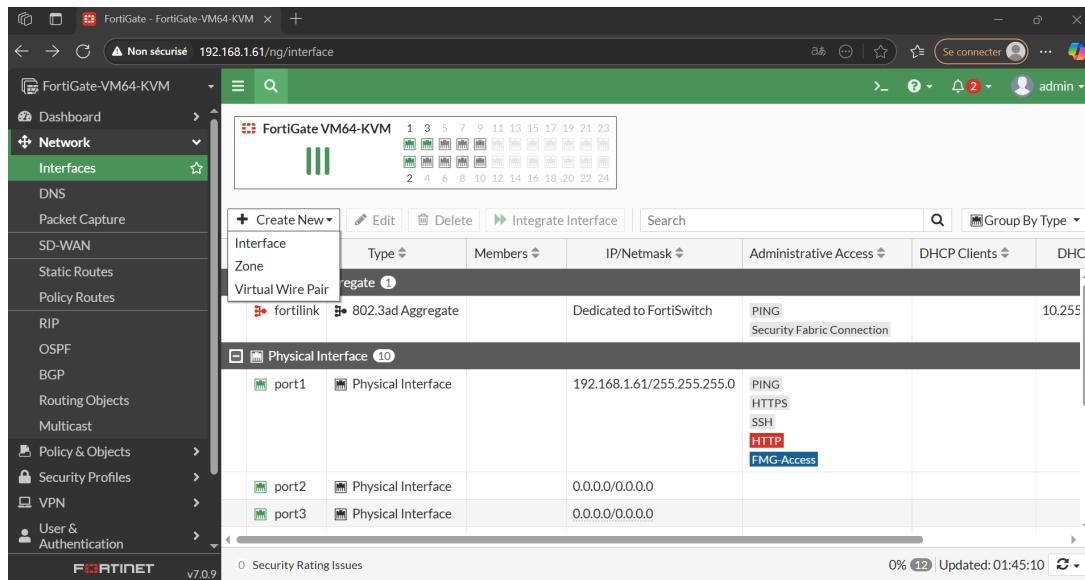


FIGURE 5.35 : Interface graphique pour la création d'une nouvelle interface VLAN

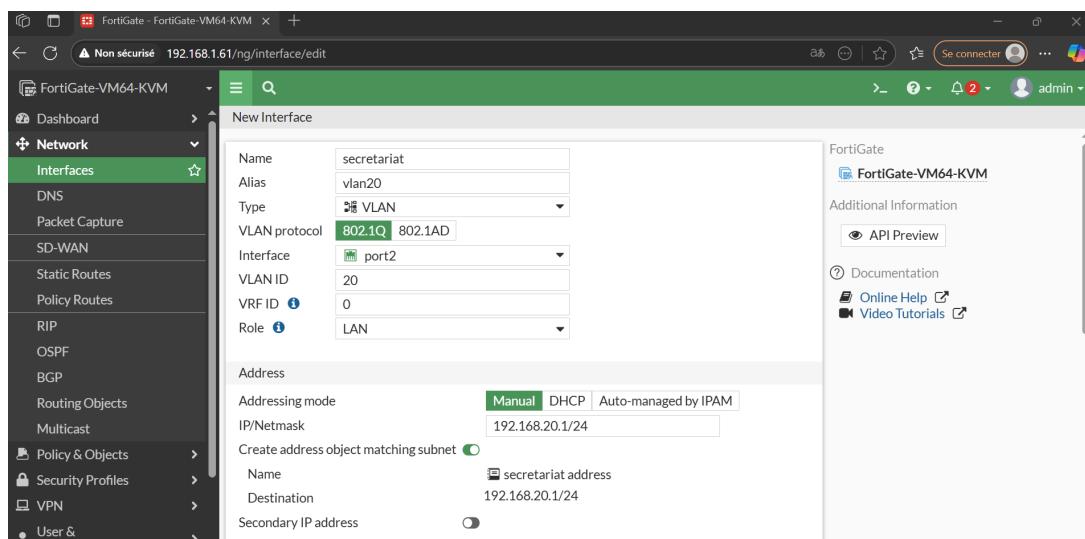


FIGURE 5.36 : Configuration du VLAN secrétariat

CHAPITRE 5. CONCEPTION ET RÉALISATION

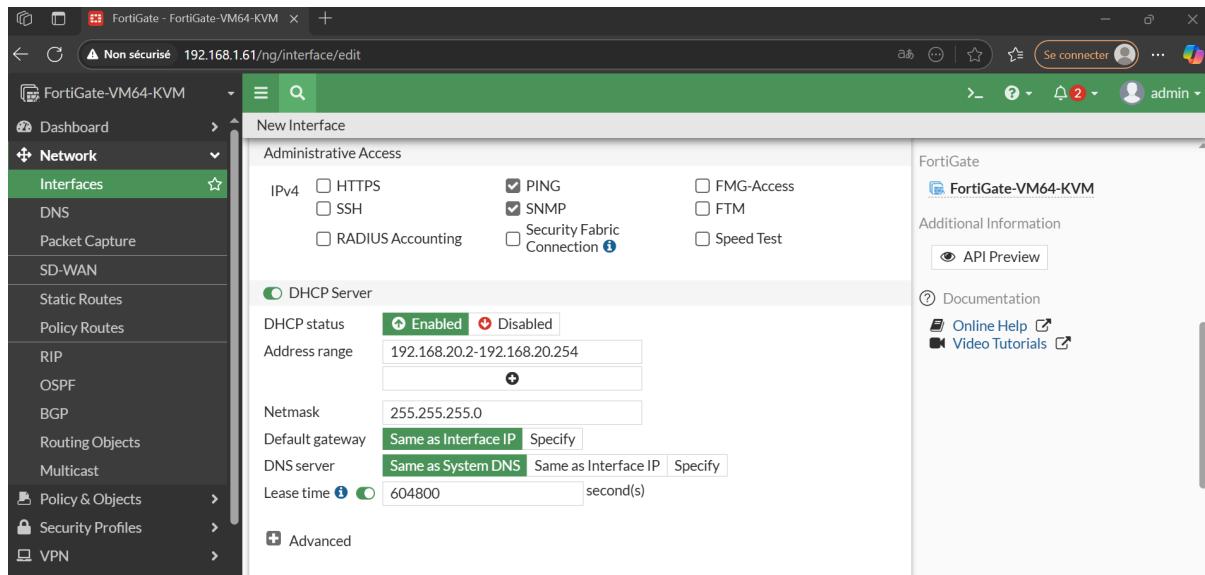


FIGURE 5.37 : Activation des accès administratifs

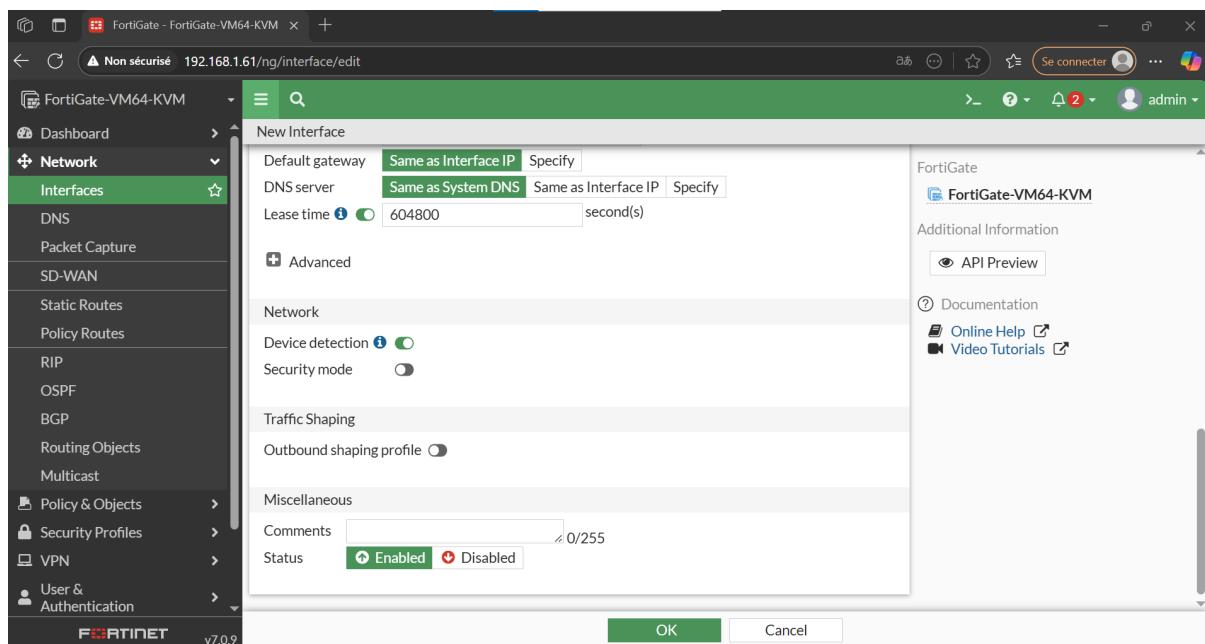


FIGURE 5.38 : Paramètres avancés du VLAN secrétariat

5.2.3.3 Crédit du VLAN invité

Un VLAN séparé est créé pour les invités afin d'isoler leur trafic du reste du réseau, limitant ainsi les risques de sécurité.

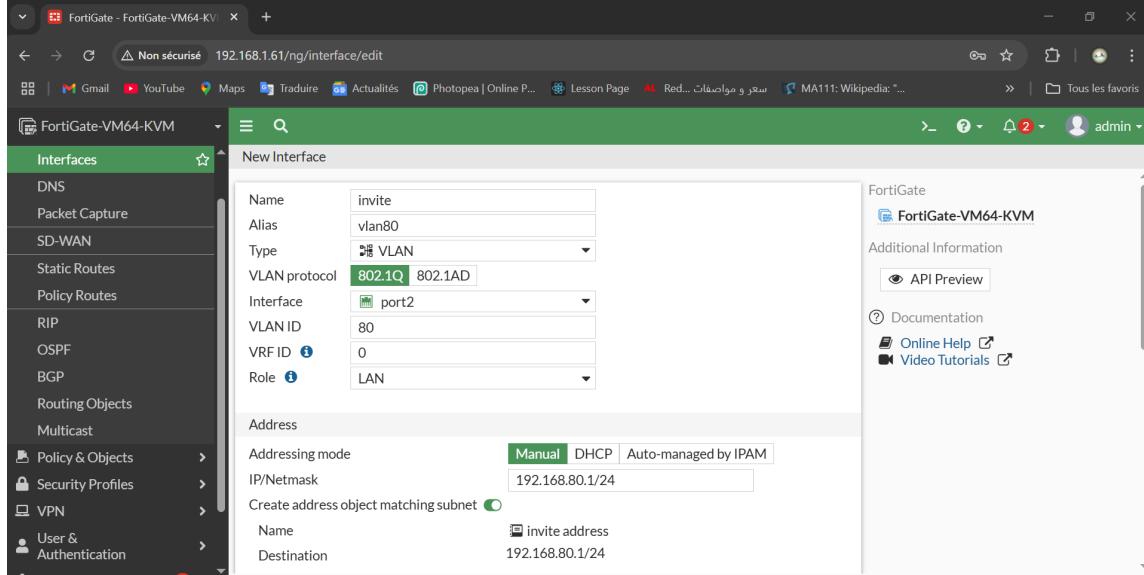


FIGURE 5.39 : Configuration du VLAN invité (vlan80)

La Figure 5.39 illustre la création du VLAN invité. L'interface est nommée `invite` avec un alias `vlan80`, utilisant le protocole 802.1Q sur l'interface `port2`. L'ID VLAN est 80, et le rôle est `LAN`. L'adresse IP est définie à `192.168.80.1/24`, avec un objet d'adresse `invite_address` créé automatiquement.

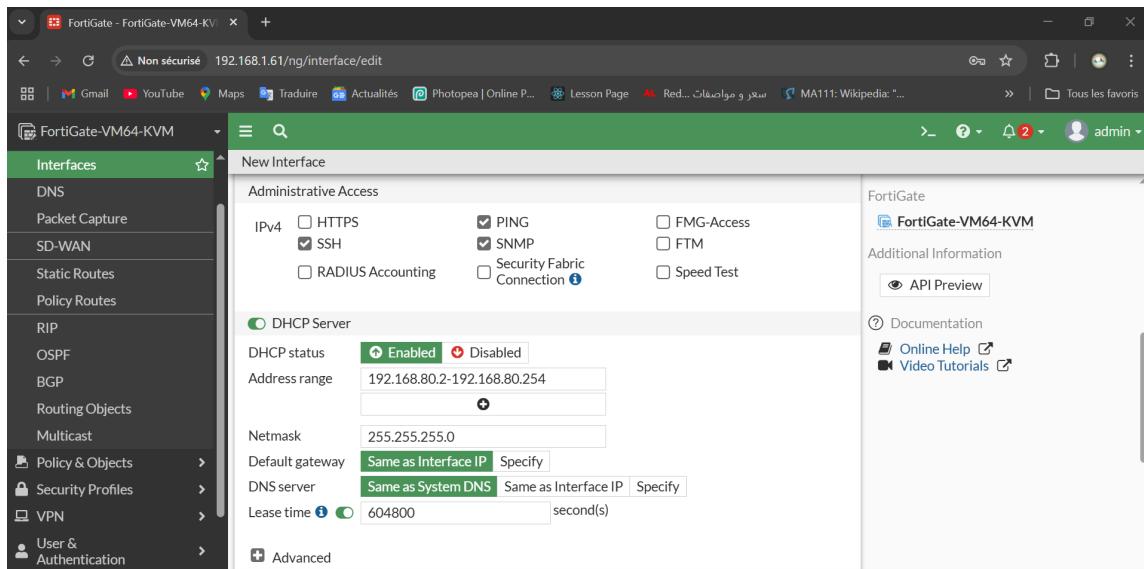


FIGURE 5.40 : Configuration des accès administratifs et du serveur DHCP

La Figure 5.40 montre les paramètres d'accès et de DHCP pour le VLAN invité. Les accès administratifs HTTPS, SSH, PING, et SNMP sont activés. Le serveur DHCP est activé avec une plage d'adresses 192.168.80.2 à 192.168.80.254, un masque 255.255.255.0, une passerelle 192.168.80.1, et un bail de 604800 secondes. Le serveur DNS utilise les paramètres système.

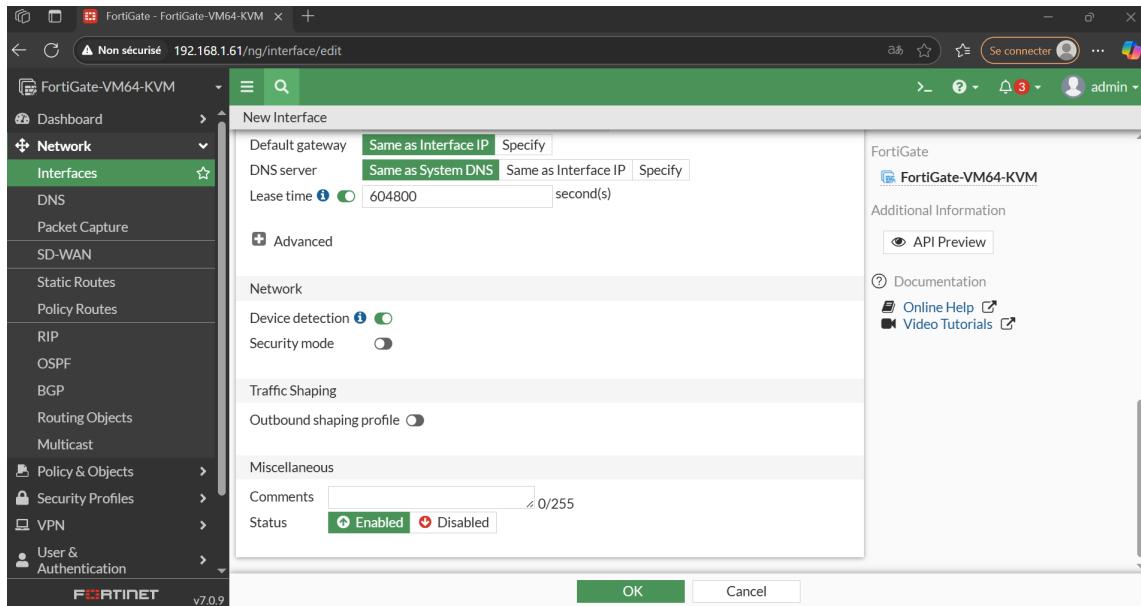


FIGURE 5.41 : Paramètres avancés du VLAN invité

La Figure 5.41 présente les paramètres avancés du VLAN invité. La détection de périphériques est activée, permettant de surveiller les appareils connectés. Les options de mise en forme du trafic restent désactivées, et la durée du bail DHCP est confirmée à 604800 secondes.

5.2.3.4 Cr éation du VLAN gestion

Le VLAN gestion est destiné aux administrateurs pour un accès sécurisé aux ressources critiques.

La Figure 5.42 montre la cr éation du VLAN gestion. L'interface est nommée **gestion** avec un alias **vlan100**, sur l'interface **port3** avec le protocole **802.1Q**. L'ID VLAN est **100**, le rôle est **LAN**, et l'adresse IP est **192.168.100.1/24**, avec un objet d'adresse **gestion_address**.

La Figure 5.43 d taille les accès administratifs (HTTPS, SSH, PING, SNMP) et sans serveur DHCP pour le VLAN gestion.

CHAPITRE 5. CONCEPTION ET RÉALISATION

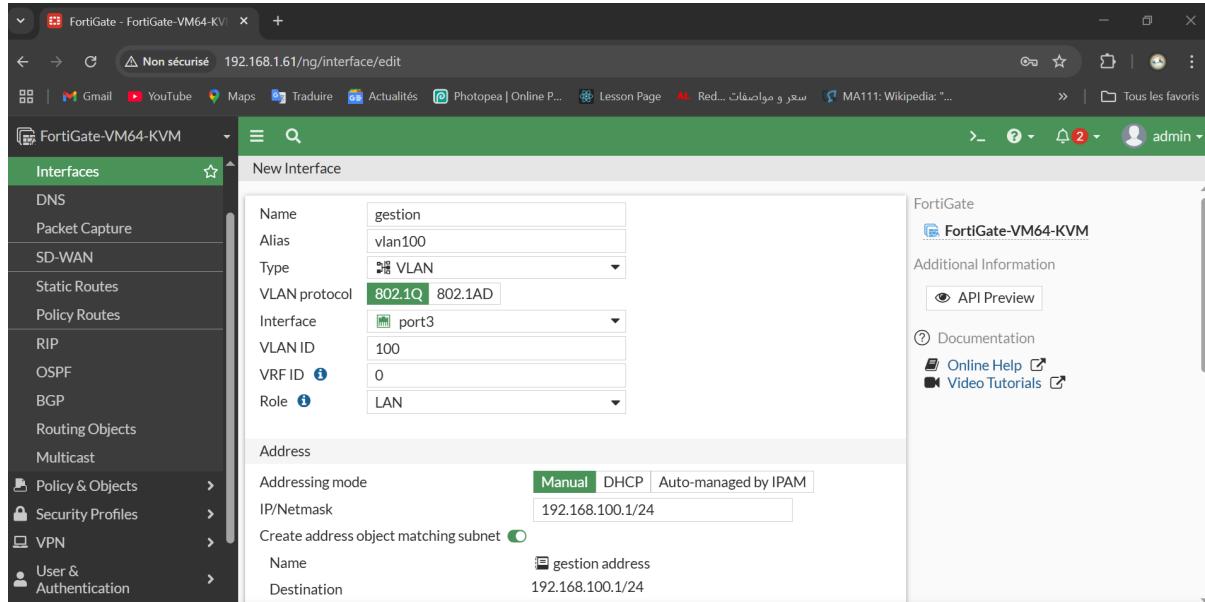


FIGURE 5.42 : Configuration du VLAN gestion (vlan100)

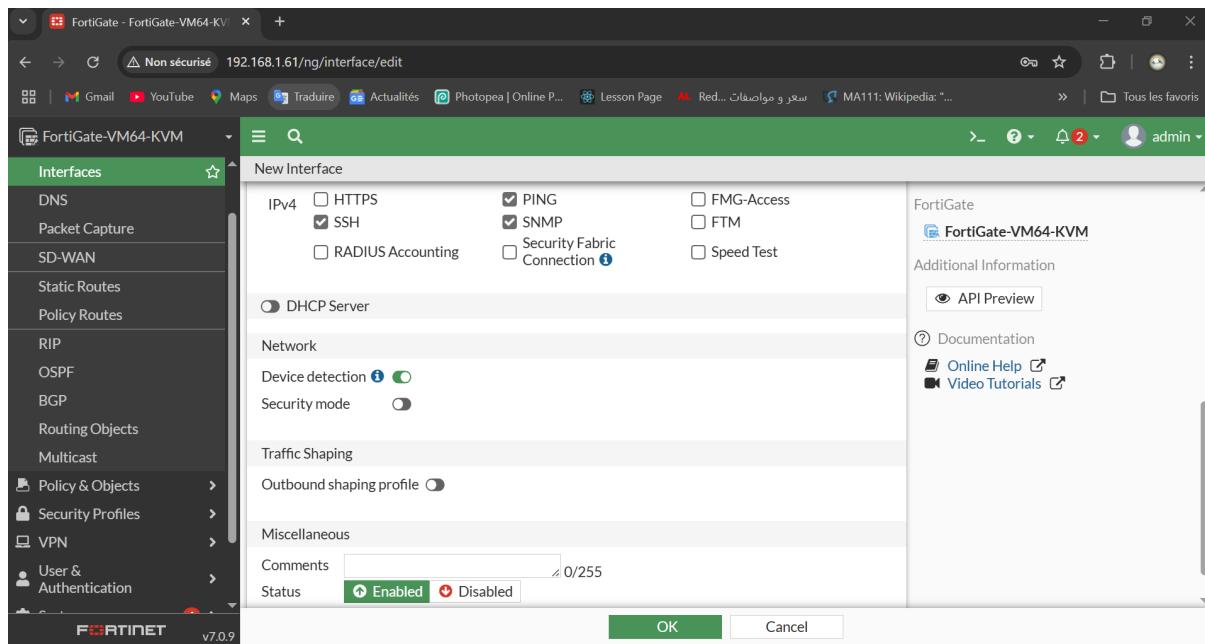


FIGURE 5.43 : Configuration des accès administratifs et du serveur DHCP

5.2.3.5 Crédation du VLAN VoIP

Le VLAN VoIP est configuré pour le trafic de voix sur IP, nécessitant une qualité de service (QoS) élevée.

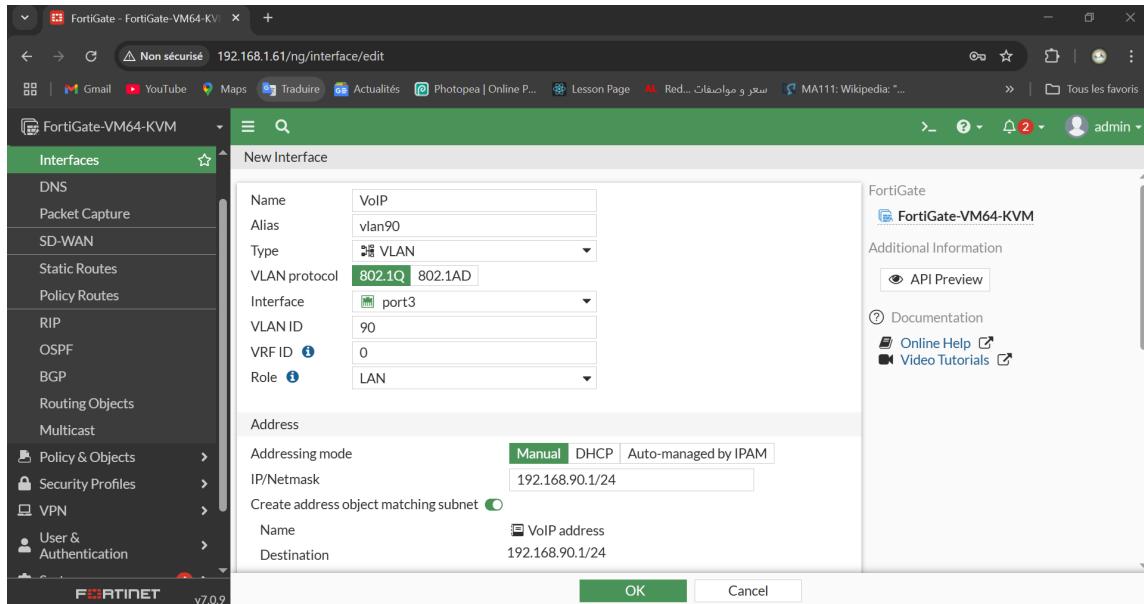


FIGURE 5.44 : Configuration du VLAN VoIP (vlan90)

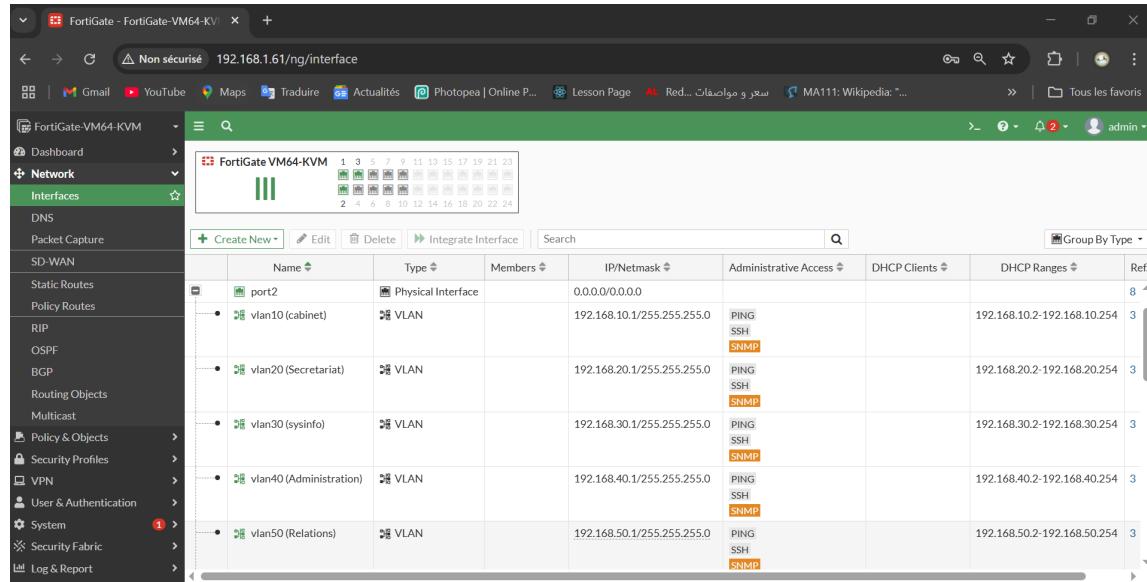
La Figure 5.44 illustre la création du VLAN VoIP. L’interface est nommée `voip` avec un alias `vlan90`, sur l’interface `port3` avec le protocole `802.1Q`. L’ID VLAN est 90, le rôle est `LAN`, et l’adresse IP est `192.168.90.1/24`, avec un objet d’adresse `voip_address`.

5.2.3.6 Les VLANs créés

Une fois les VLANs configurés, ils apparaissent dans la liste des interfaces, permettant de vérifier leur configuration.

La Figure 5.45 et La Figure 5.46 montre la liste des interfaces après la création des VLANs. L’interface physique `port1` (IP `192.168.1.61/24`), et les interfaces `port2` et `port3` (sans IP attribuée directement). Les VLANs créés apparaissent comme des sous-interfaces de ces ports physiques. On y trouve le VLAN `VLAN 10`, `VLAN 20`, `VLAN 30`, `VLAN 40`, `VLAN 50`, `VLAN 60`, `VLAN 70`, `VLAN 80`, `VLAN 90`, `VLAN 100`

CHAPITRE 5. CONCEPTION ET RÉALISATION



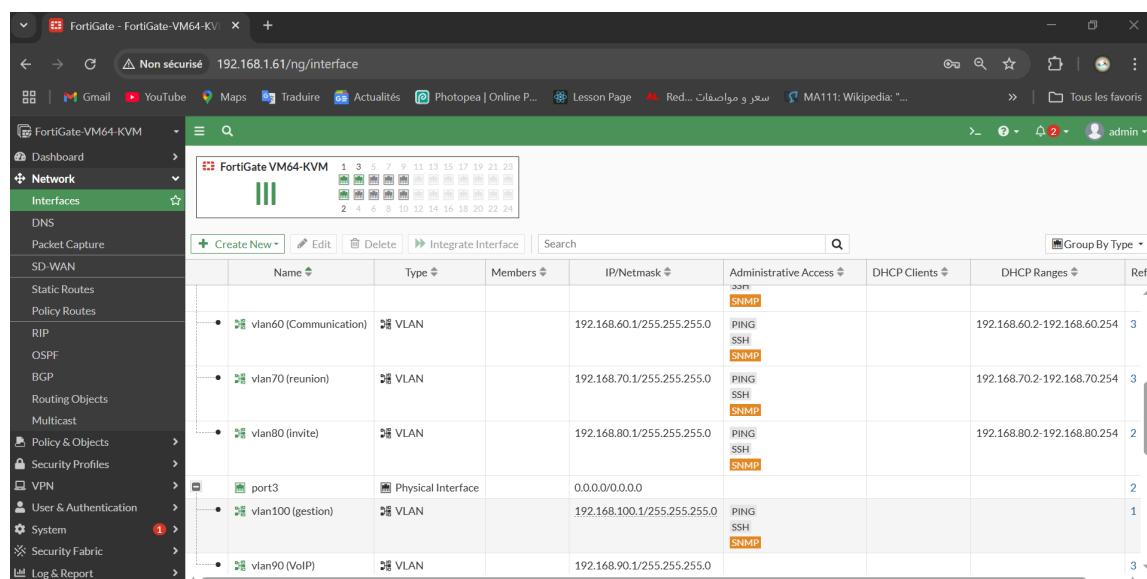
The screenshot shows the FortiGate management interface. The left sidebar is titled "FortiGate-VM64-KVM" and includes sections for Dashboard, Network (selected), Interfaces, DNS, Packet Capture, SD-WAN, Static Routes, Policy Routes, RIP, OSPF, BGP, Routing Objects, Multicast, Policy & Objects, Security Profiles, VPN, User & Authentication, System (with a red notification dot), Security Fabric, and Log & Report.

The main content area displays a network diagram of "FortiGate VM64-KVM" with numbered ports (1-24) and a legend indicating port types: Physical Interface (green), VLAN (blue), and Trunk (yellow).

A table lists the created VLAN interfaces:

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
port2	Physical Interface		0.0.0.0/0.0.0	PING SSH SNMP		192.168.10.2-192.168.10.254	8
vlan10 (cabinet)	VLAN		192.168.10.1/255.255.255.0	PING SSH SNMP		192.168.20.2-192.168.20.254	3
vlan20 (Secretariat)	VLAN		192.168.20.1/255.255.255.0	PING SSH SNMP		192.168.30.2-192.168.30.254	3
vlan30 (sysinfo)	VLAN		192.168.30.1/255.255.255.0	PING SSH SNMP		192.168.40.2-192.168.40.254	3
vlan40 (Administration)	VLAN		192.168.40.1/255.255.255.0	PING SSH SNMP		192.168.50.2-192.168.50.254	3
vlan50 (Relations)	VLAN		192.168.50.1/255.255.255.0	PING SSH SNMP		192.168.60.2-192.168.60.254	3

FIGURE 5.45 : Liste des interfaces VLAN créées



The sidebar and network diagram are identical to Figure 5.45.

The table lists the created VLAN interfaces:

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
vlan60 (Communication)	VLAN		192.168.60.1/255.255.255.0	PING SSH SNMP		192.168.60.2-192.168.60.254	3
vlan70 (reunion)	VLAN		192.168.70.1/255.255.255.0	PING SSH SNMP		192.168.70.2-192.168.70.254	3
vlan80 (invite)	VLAN		192.168.80.1/255.255.255.0	PING SSH SNMP		192.168.80.2-192.168.80.254	2
port3	Physical Interface		0.0.0.0/0.0.0				2
vlan100 (gestion)	VLAN		192.168.100.1/255.255.255.0	PING SSH SNMP			1
vlan90 (VoIP)	VLAN		192.168.90.1/255.255.255.0				3

FIGURE 5.46 : Liste des interfaces VLAN créées

5.2.3.7 Routage inter VLAN

Le routage inter VLAN permet de connecter les différents sous-réseaux créés par les VLANs. Une zone est configurée pour regrouper les interfaces VLAN et activer la communication entre elles.

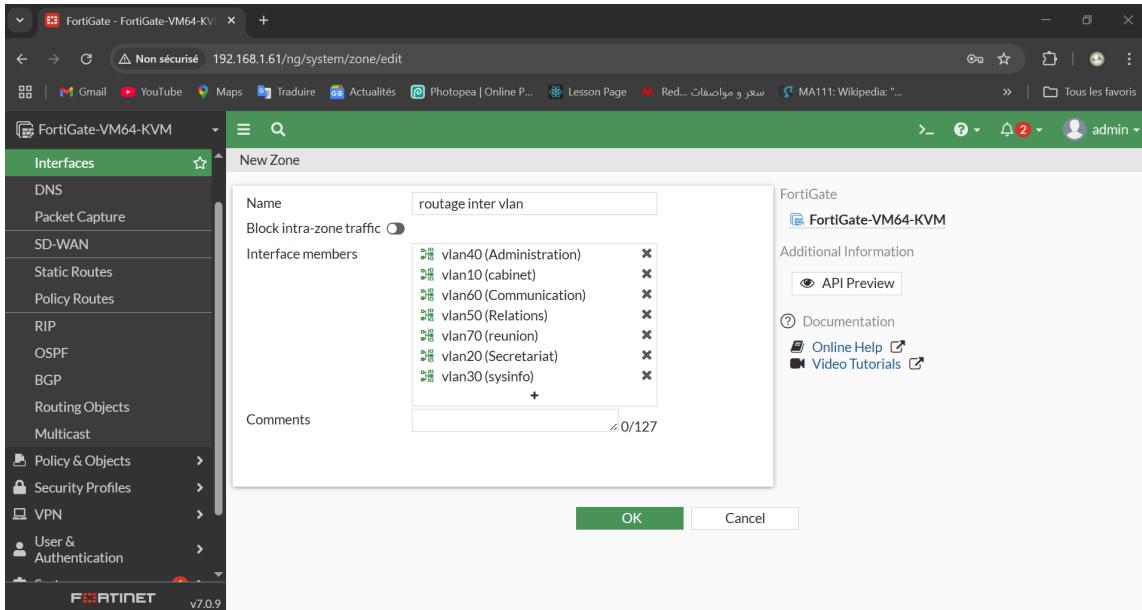


FIGURE 5.47 : Configuration de la zone "routage inter vlan"

La Figure 5.47 montre la création d'une zone nommée "routage inter vlan". Cette zone inclut les interfaces VLAN telles que `vlan40` (administration), `vlan60` (communication), ... L'option "Block intra-zone traffic" est désactivée pour autoriser le trafic entre les VLANs au sein de cette zone.

Routage entre VoIP et les services

Pour autoriser le routage inter-VLAN entre le VLAN VoIP et les VLANs des services, Nous devons configurer une politique de pare-feu qui permette ce trafic.

Les figures 5.48 et 5.49 montrent deux politiques de pare-feu configurées sur un FortiGate pour autoriser le trafic entre un **VLAN Services** et un **VLAN VoIP**.

CHAPITRE 5. CONCEPTION ET RÉALISATION

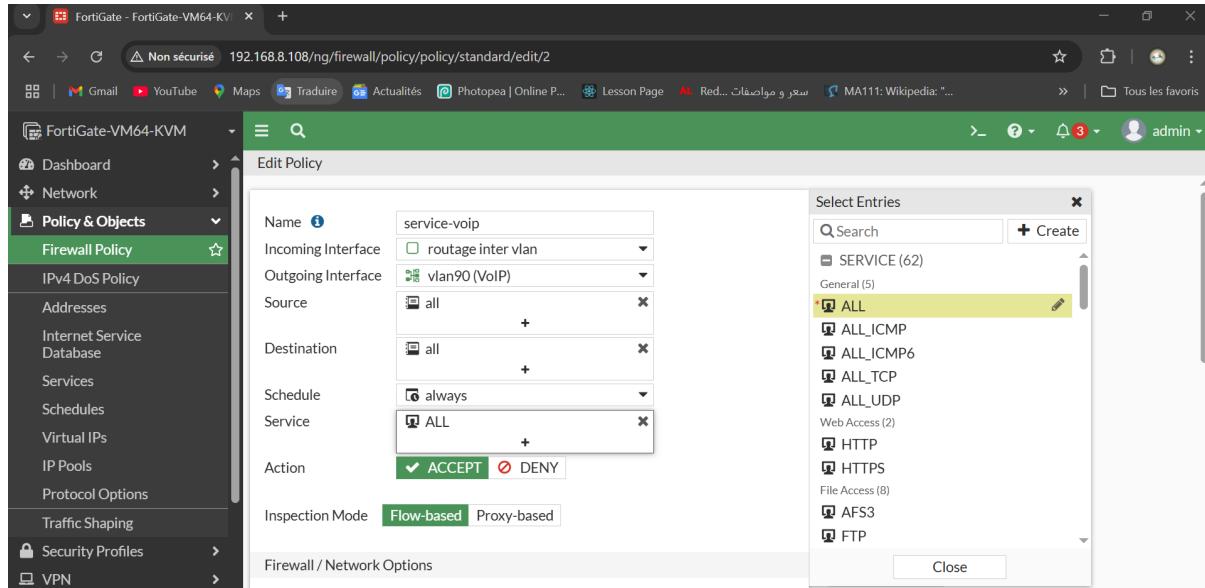


FIGURE 5.48 : Routage entre les service et VoIP

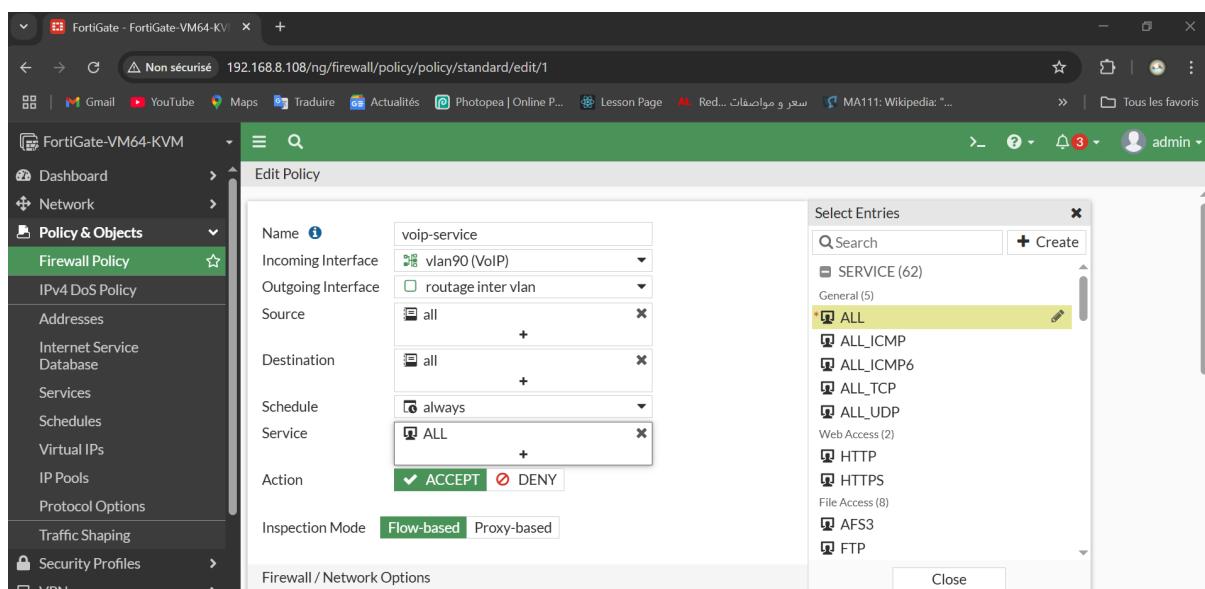


FIGURE 5.49 : Routage entre VoIP et les service

5.2.3.8 Route statique

Une route statique est configurée pour diriger le trafic vers un réseau externe via l'interface WAN.

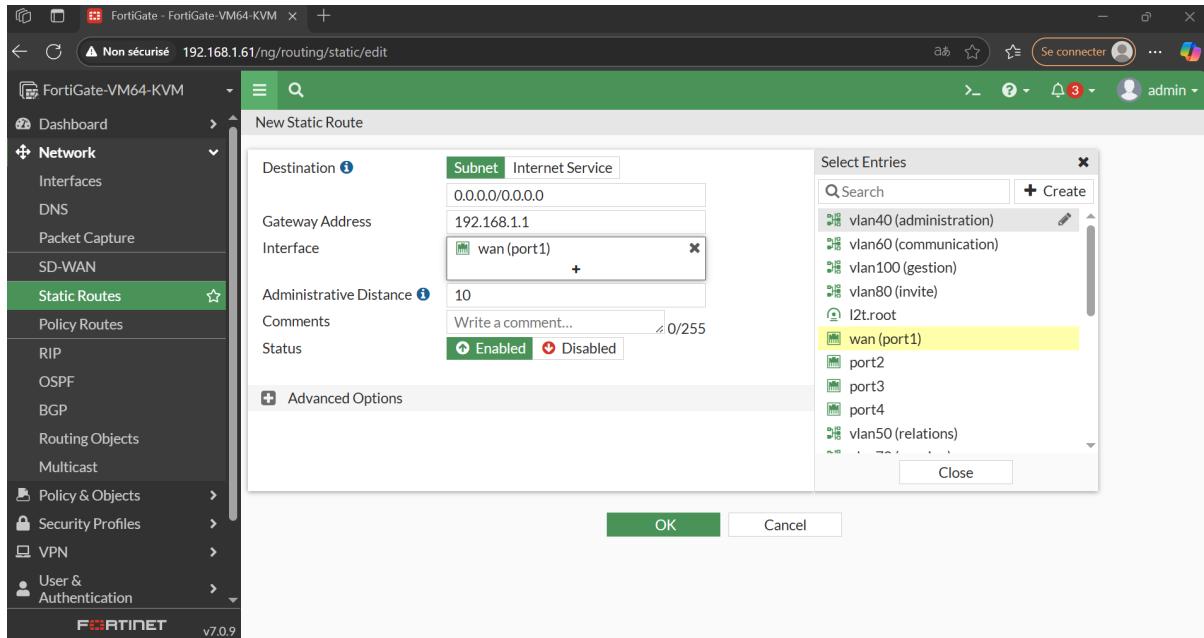


FIGURE 5.50 : Configuration d'une route statique

La Figure 5.50 illustre la configuration d'une route statique. La destination est définie comme 0.0.0.0/0 (tous les réseaux), la passerelle est 192.168.1.1, et l'interface sortante est wan (port1). Cette route permet au FortiGate de rediriger tout le trafic non local vers le réseau externe via la passerelle spécifiée.

5.2.3.9 Filtrage web

Le filtrage web est mis en place pour contrôler l'accès à certains types de contenu sur le réseau.

La Figure 5.51 présente la liste des profils de filtrage web existants. Les profils default, monitor-all (pour le suivi des URLs), et wifi-default (pour le trafic WiFi) sont affichés, avec une option pour créer un nouveau profil.

La Figure 5.52 montre le clonage du profil default pour créer un nouveau profil nommé **filtre zone**, permettant une personnalisation des règles de filtrage.

La Figure 5.53 détaille la configuration du profil **filtre zone**. Les catégories comme "Internet Radio and TV" est bloqué (Block), bien que cela soit autorisé dans le profil par défaut.

CHAPITRE 5. CONCEPTION ET RÉALISATION

The screenshot shows the FortiGate management interface with the URL `192.168.1.61/ng/utm/webfilter/profile`. The left sidebar is titled "FortiGate-VM64-KVM" and contains the following navigation items:

- Dashboard
- Network
- Policy & Objects
- Security Profiles
- AntiVirus
- Web Filter** (highlighted in green)
- Video Filter
- DNS Filter
- Application Control
- Intrusion Prevention
- File Filter
- SSL/SSH Inspection
- Application Signatures
- IPS Signatures
- Web Rating Overrides
- Web Profile Overrides

The main content area displays a table of web filtering profiles:

Name	Comments	Ref.
WEB default	Default web filtering.	0
WEB monitor-all	Monitor and log all visited URLs, flow-based.	0
WEB wifi-default	Default configuration for offloading WiFi traffic.	1

FIGURE 5.51 : Liste des profils de filtrage web par défaut

The screenshot shows the FortiGate management interface with the URL `192.168.1.61/ng/utm/webfilter/profile`. The left sidebar is identical to Figure 5.51. A modal dialog box titled "Clone 'default'" is open in the center:

Please enter the desired name for the clone

Name:

OK Cancel

FIGURE 5.52 : Clonage du profil `default` avec un nouveau nom `filtré zone`.

CHAPITRE 5. CONCEPTION ET RÉALISATION

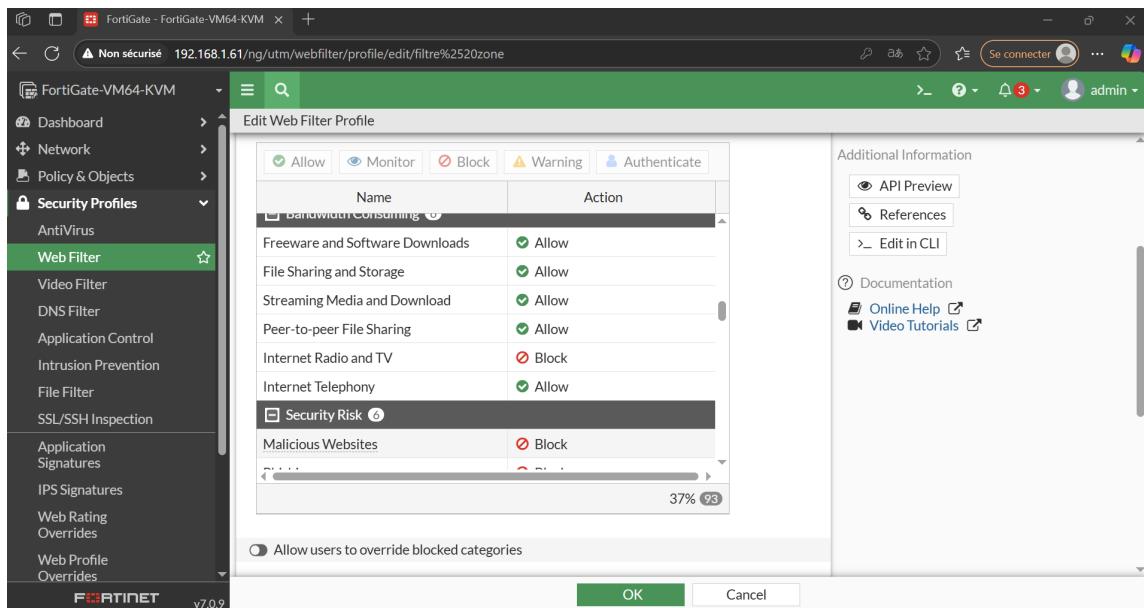


FIGURE 5.53 : Configuration du profil filtre zone

5.2.3.10 Accès à Internet

Des politiques de sécurité sont configurées pour permettre l'accès à Internet depuis les VLANs, avec des règles spécifiques.

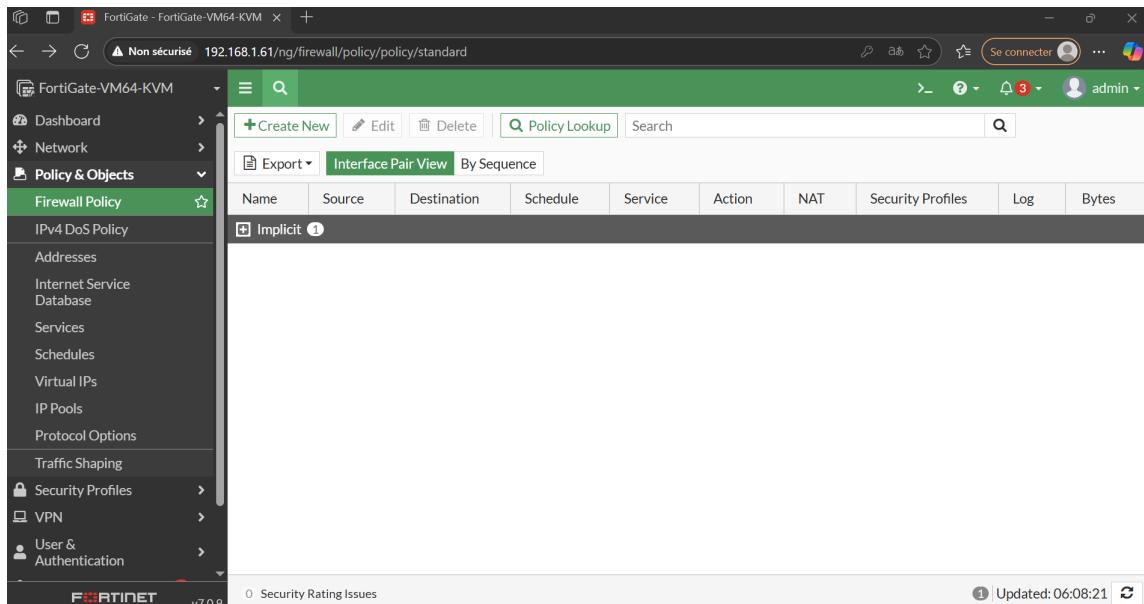


FIGURE 5.54 : Créeation d'une nouvelle politique nommée "zone to wan"

La Figure 5.54 montre la création d'une politique nommée "zone to wan". L'interface d'entrée est `routage inter vlan`, l'interface de sortie est `wan (port1)`, et l'action est définie sur `ACCEPT` pour autoriser le trafic.

La Figure 5.55 présente les options avancées de la politique. L'inspection est en mode "flow-based", et le NAT utilise l'adresse de l'interface sortante (`Use Outgoing Interface Address`).

CHAPITRE 5. CONCEPTION ET RÉALISATION

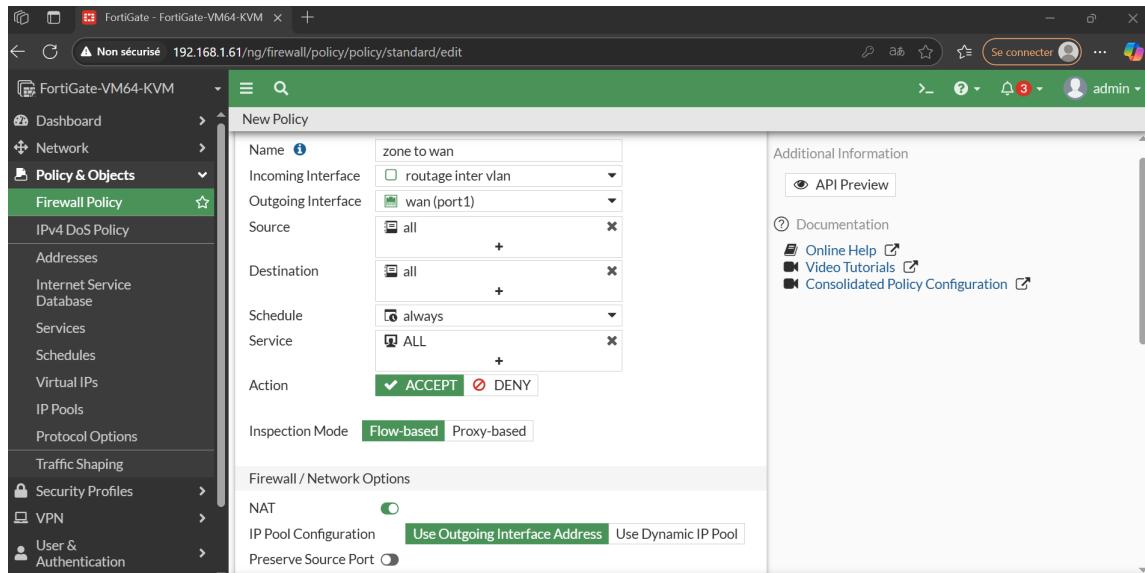


FIGURE 5.55 : Configuration de la politique avec inspection

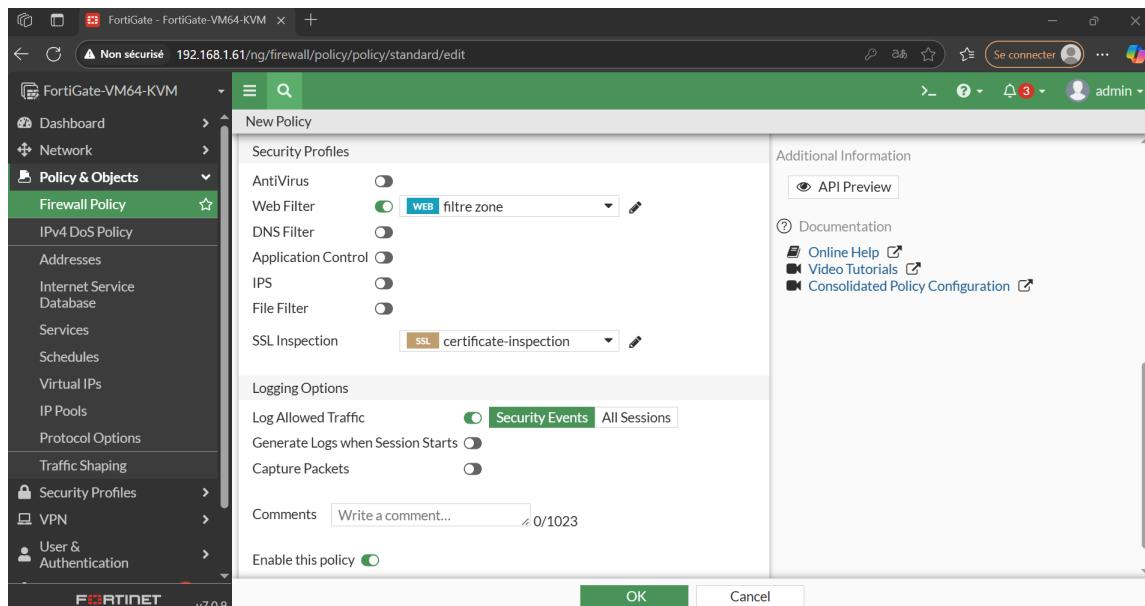


FIGURE 5.56 : Ajout de profils de sécurité

CHAPITRE 5. CONCEPTION ET RÉALISATION

La Figure 5.56 montre l'ajout de profils de sécurité. Le profil de filtrage web **filtre zone** et l'inspection SSL **certificate-inspection** sont activés, avec une journalisation des événements de sécurité ("Security Events").

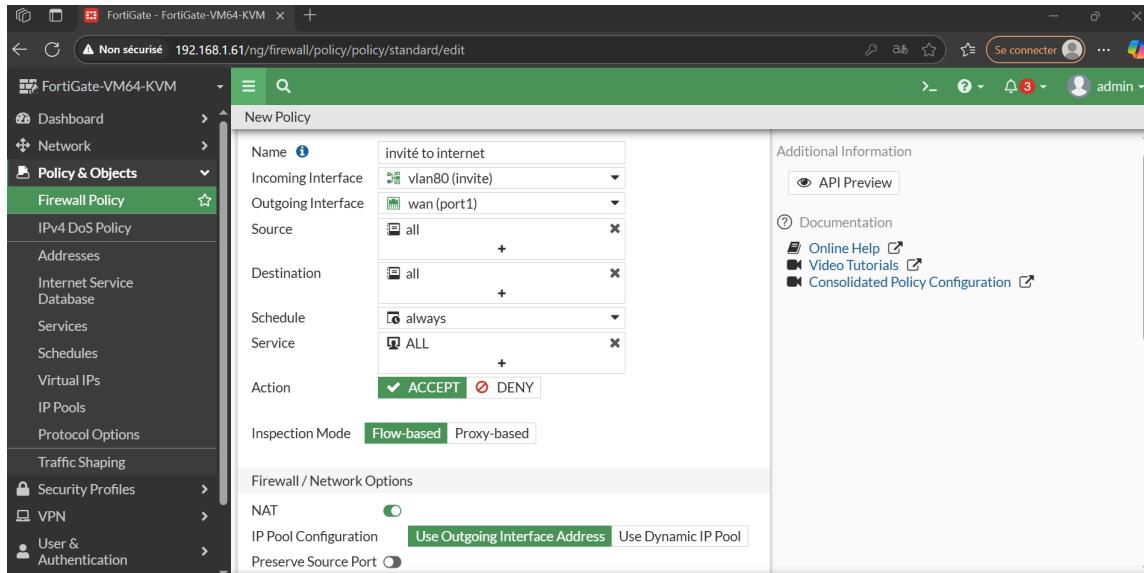


FIGURE 5.57 : Politique VLAN invité (vlan80) vers Internet via wan (port1)

La Figure 5.57 illustre la création d'une politique pour le VLAN invité. L'interface d'entrée est **vlan80 (invite)**, l'interface de sortie est **wan (port1)**, et l'action est **ACCEPT**.

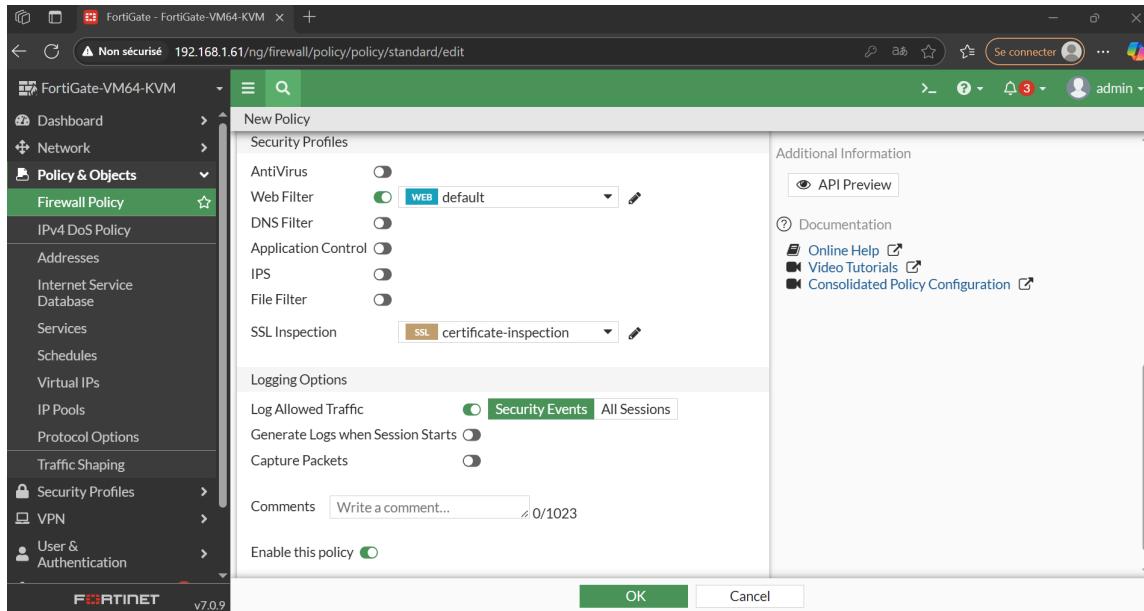


FIGURE 5.58 : Politique pour le VLAN invité avec inspection

La Figure 5.58 détaille les options de la politique pour le VLAN invité, avec inspection en mode "flow-based" et NAT basé sur l'adresse de l'interface sortante.

5.2.3.11 Bloquer Facebook via un filtre web

Cette section explique comment créer et appliquer un profil de filtrage web pour bloquer l'accès à Facebook sur un FortiGate.

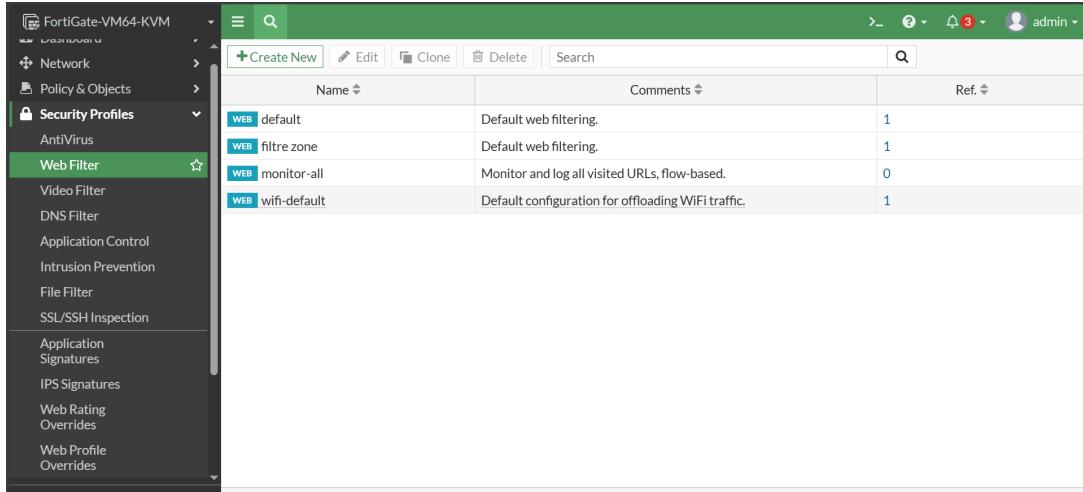


FIGURE 5.59 : Menu des profils de sécurité dans FortiGate (section Web Filter).

Comme montré dans la figure 5.59, la configuration se fait dans :

— **Security Profiles** > **Web Filter**

— Les profils existants sont listés (default, monitor-all, etc.)

La figure 5.60 montre la création d'un nouveau profil :

— Nom : **block Facebook**

— Type : **Flow-based**

— Options cochées :

— Allow users to override blocked categories

— URL Filter (à activer)

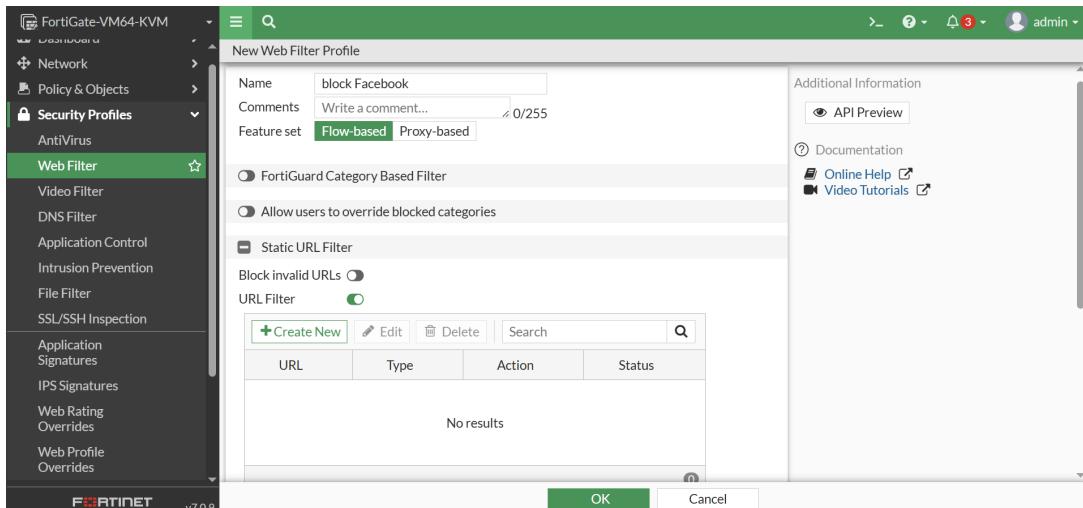


FIGURE 5.60 : Crédit d'un nouveau profil de filtrage web.

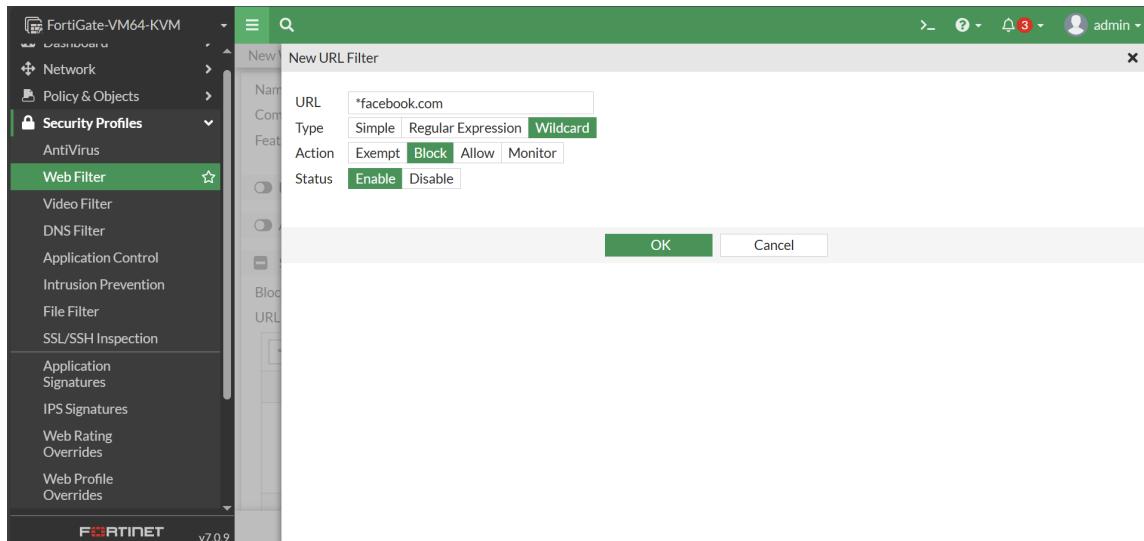


FIGURE 5.61 : Ajout d'une règle de filtrage pour facebook.com.

Dans la figure 5.61, on configure la règle spécifique :

- URL : *facebook.com (avec wildcard)
- Type : Wildcard (pour couvrir tous les sous-domaines)
- Action : Block
- Status : Enable

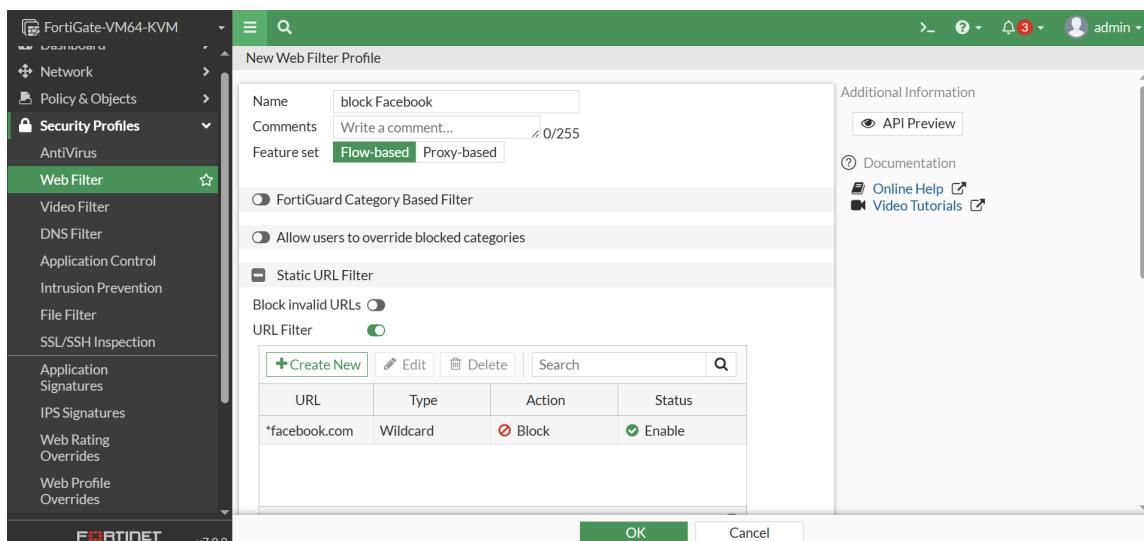


FIGURE 5.62 : Vérification des paramètres du filtre URL.

La figure 5.62 confirme que :

- La règle pour *facebook.com est active
- L'action est bien définie sur **Block**
- Le type **Wildcard** est sélectionné

CHAPITRE 5. CONCEPTION ET RÉALISATION

Après création (figure 5.63), le nouveau profil apparaît dans la liste avec :

- Nom : **block Facebook**
- Référence : 0 (pas encore appliqué à une politique)

Name	Comments	Ref.
WEB block Facebook		0
WEB default	Default web filtering.	1
WEB filtre zone	Default web filtering.	1
WEB monitor-all	Monitor and log all visited URLs, flow-based.	0
WEB wifi-default	Default configuration for offloading WiFi traffic.	1

FIGURE 5.63 : Liste finale des profils avec le nouveau "block Facebook".

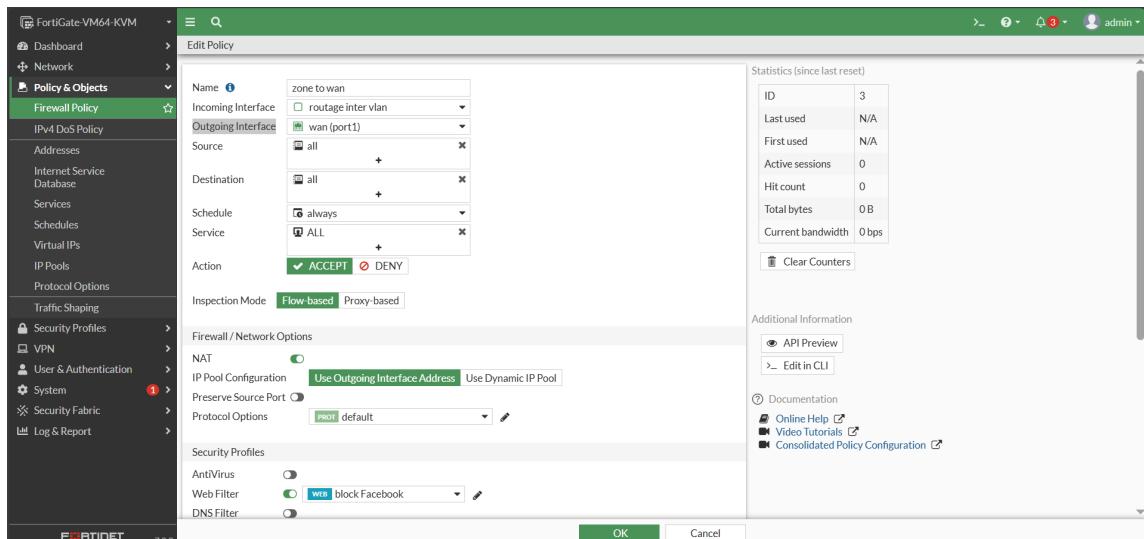


FIGURE 5.64 : Application du profil à une politique firewall.

Pour finaliser (figure 5.64) :

1. Aller dans **Policy & Objects** ➤ **Firewall Policy**
2. Éditer la politique cible
3. Dans **Security Profiles**, activer **Web Filter**
4. Sélectionner le profil **block Facebook**
5. Sauvegarder la politique

Options avancées :

- Utiliser **Regular Expression** pour des motifs complexes
- Combiner avec le filtrage par catégories FortiGuard
- Activer les logs pour surveiller les tentatives d'accès

Remarque importante : Le filtrage wildcard (*facebook.com) bloquera :

- facebook.com
- m.facebook.com
- *.facebook.com

5.2.3.12 Izolation du trafic

L'isolation du trafic vise à restreindre la communication entre certains VLANs pour améliorer la sécurité, en particulier entre le VLAN invité et le VLAN gestion.

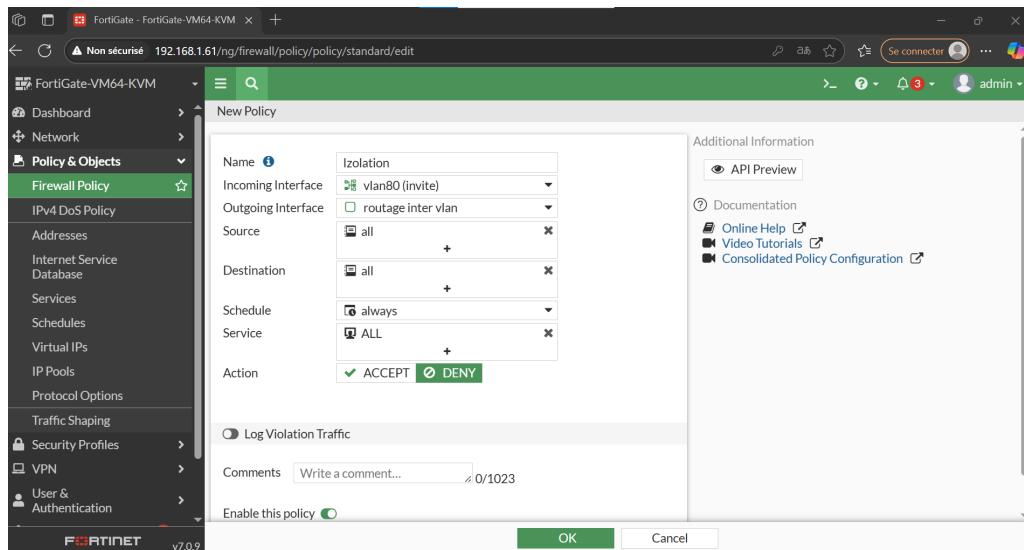


FIGURE 5.65 : Politique d'isolation entre vlan80 (invite) et routage inter vlan

La Figure 5.65 montre la création d'une politique nommée "Izolation". L'interface d'entrée est `vlan80 (invite)`, l'interface de sortie est `routage inter vlan`, et l'action est définie sur `DENY` pour empêcher le trafic sortant du VLAN invité vers les autres VLANs.

La Figure 5.66 illustre une politique nommée "Izolation gestion". L'interface d'entrée est `vlan80 (invite)`, l'interface de sortie est `vlan100 (gestion)`, et l'action est `DENY`, assurant que le VLAN gestion reste isolé du VLAN invité.

CHAPITRE 5. CONCEPTION ET RÉALISATION

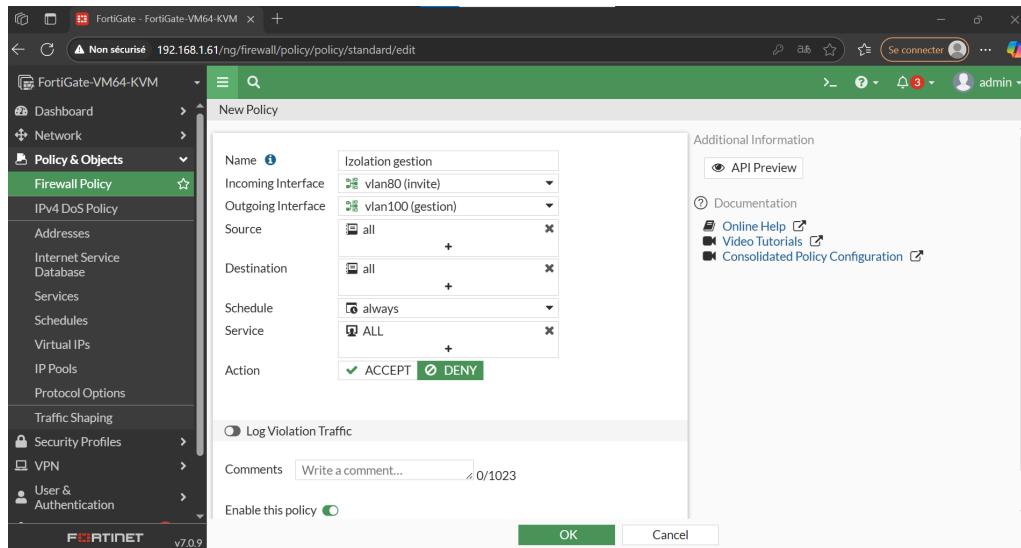


FIGURE 5.66 : Politique d’isolation entre vlan80 (invite) et vlan100 (gestion)

5.2.3.13 Politique créée

Cette section présente les politiques créées et leur état dans l’interface du FortiGate, reflétant les configurations d’accès et d’isolation.

Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log	Bytes
route inter vlan → vlan90 (VoIP)	service voip	all	all	always	ALL	✓ ACCEPT	✗ Disabled	ssl no-inspection
route inter vlan → wan (port1)	zone to wan	all	all	always	ALL	✓ ACCEPT	✓ Enabled	web filter zone ssl certificate-inspection
vlan80 (invite) → route inter vlan	izolation	all	all	always	ALL	✗ DENY		✗ Disabled
vlan80 (invite) → vlan100 (gestion)	izolation gestion	all	all	always	ALL	✗ DENY		✗ Disabled
vlan80 (invite) → wan (port1)	invite to wan	all	all	always	ALL	✓ ACCEPT	✓ Enabled	web default ssl certificate-inspection
vlan90 (VoIP) → route inter vlan	voip service	all	all	always	ALL	✓ ACCEPT	✗ Disabled	ssl no-inspection
Implicit	Implicit Deny	all	all	always	ALL	✗ DENY		✗ Disabled

FIGURE 5.67 : Liste des politiques créées

La Figure 5.67 affiche la liste des politiques configurées. On y trouve :

- “Izolation” (vlan80 vers `route inter vlan`, DENY).
- “zone to internet” (`route inter vlan` vers `wan`, ACCEPT avec profils WEB et SSL).
- “invite to internet” (vlan80 vers `wan`, ACCEPT avec profils WEB et SSL), démontrant une gestion différenciée du trafic.

5.2.3.14 QoS pour VoIP

La qualité de service (QoS) pour VoIP est configurée pour prioriser le trafic vocal sur le réseau, garantissant une latence et une perte de paquets minimales.

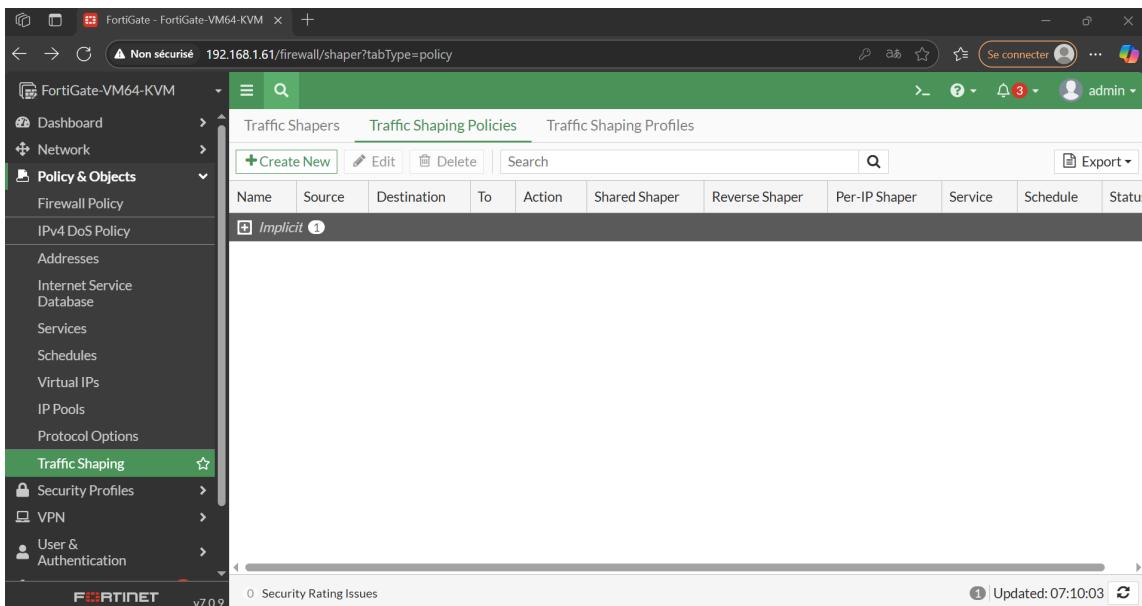


FIGURE 5.68 : Interface vide des politiques de gestion de trafic

La Figure 5.68 montre l'interface initiale des politiques de gestion de trafic, avec une politique implicite existante, avant la création d'une nouvelle politique QoS.

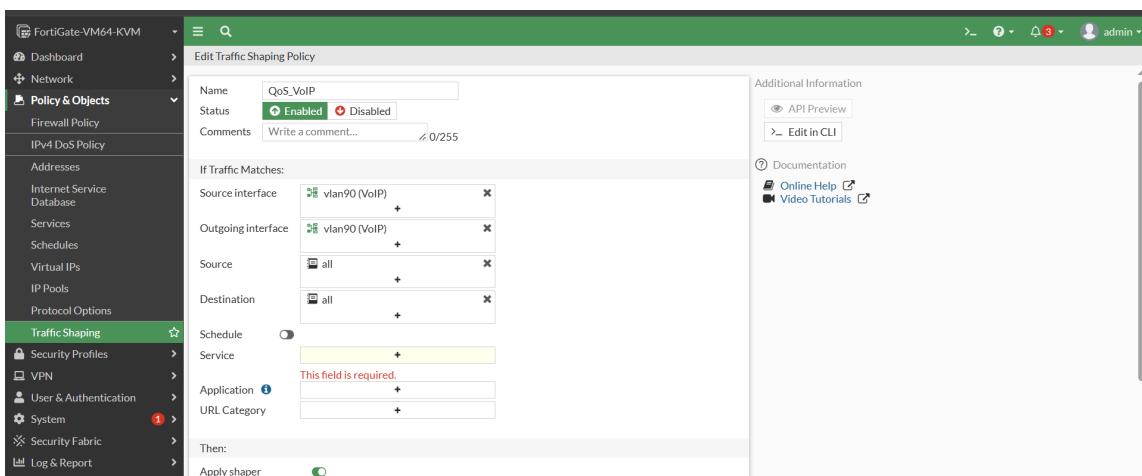


FIGURE 5.69 : Crédit d'une nouvelle politique nommée "QoS _VoIP"

La Figure 5.69 illustre la création d'une politique nommée "QoS _VoIP", avec les interfaces source et destination configurées sur voip.

CHAPITRE 5. CONCEPTION ET RÉALISATION

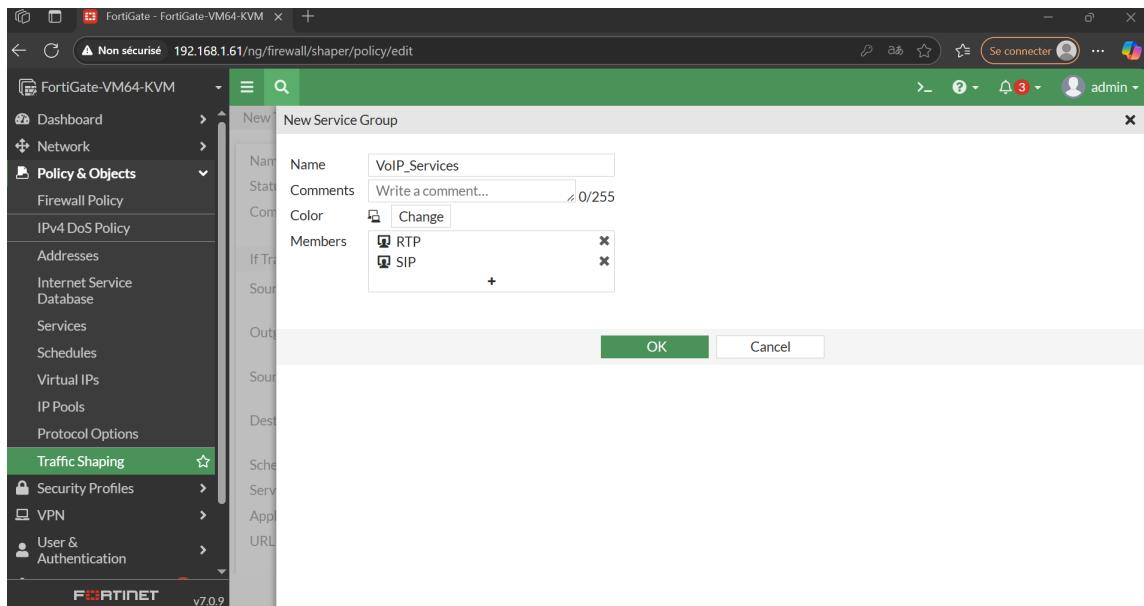


FIGURE 5.70 : Création groupe de service

La Figure 5.70 montre la création groupe du service avec les deux protocole (SIP et RTP).

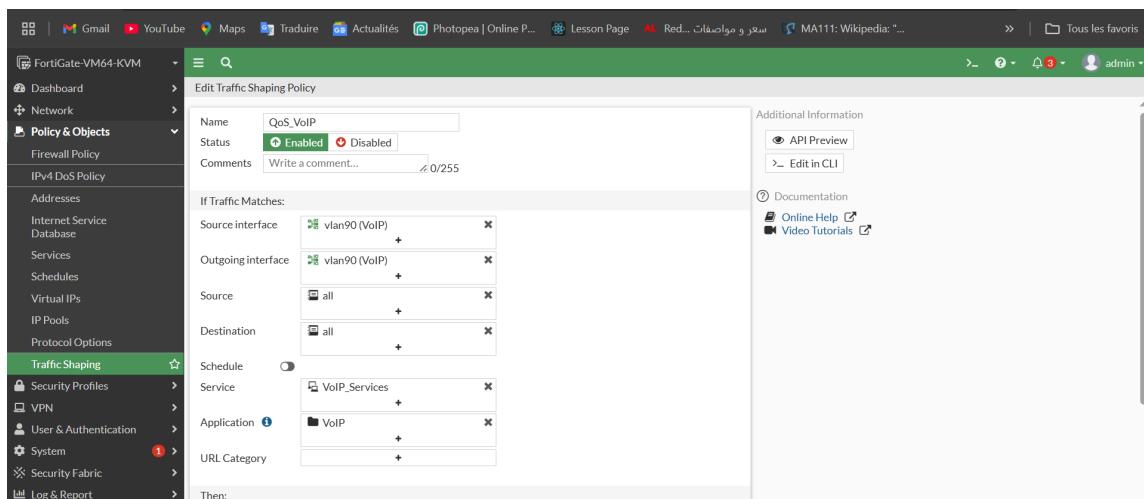


FIGURE 5.71 : groupe de services VoIP _Services et l'application VoIP

La Figure 5.71 présente la configuration des services, avec l'ajout du groupe VoIP _Services et de l'application VoIP pour prioriser ce trafic.

CHAPITRE 5. CONCEPTION ET RÉALISATION

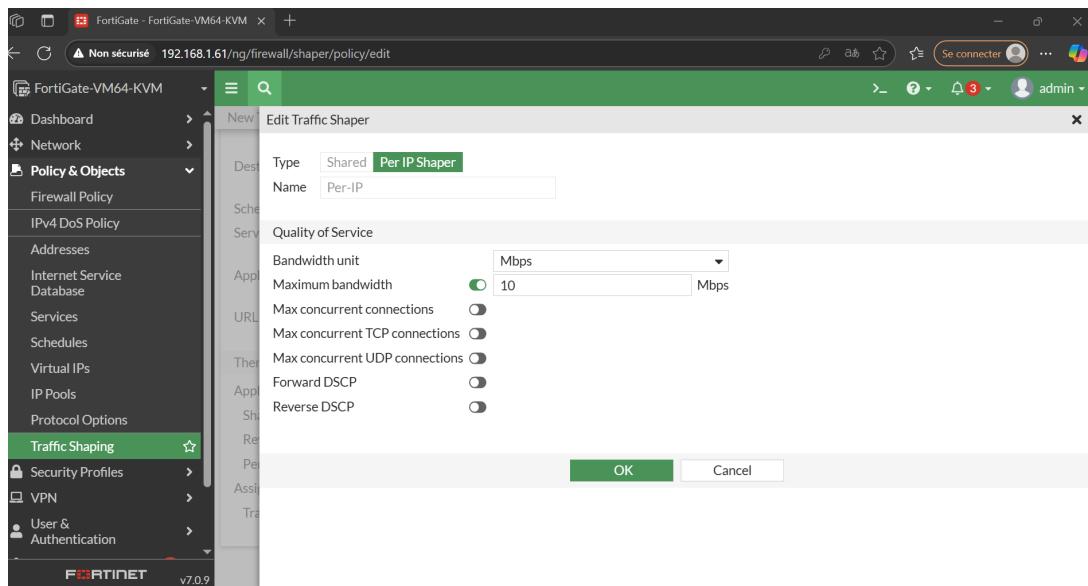


FIGURE 5.72 : Édition d'un shaper partagé

La Figure 5.72 montre l'édition d'un shaper partagé de type "Per IP Shaper", nommé "Per-IP", avec une bande passante maximale fixée à 10 Mbps.

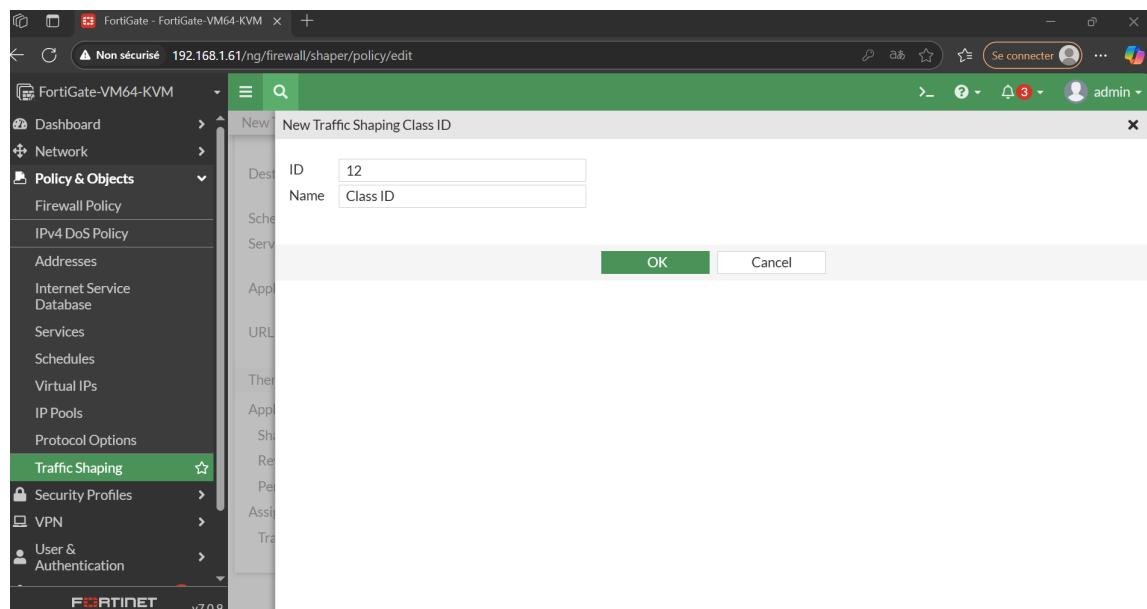


FIGURE 5.73 : Crédation d'une classe d'identification de trafic

La Figure 5.73 détaille la création d'une classe d'identification de trafic avec un ID 12 et un nom "Class ID".

CHAPITRE 5. CONCEPTION ET RÉALISATION

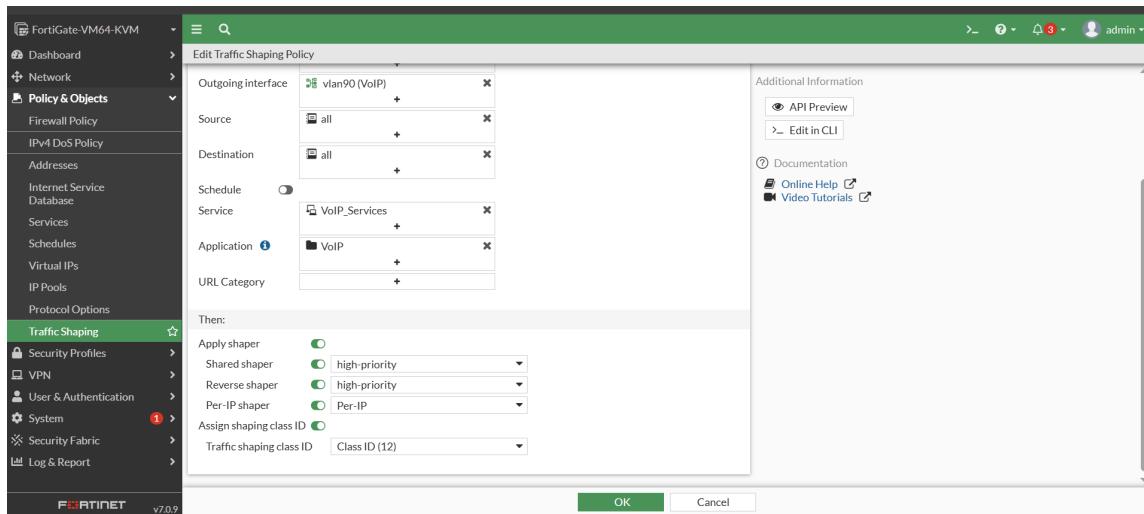


FIGURE 5.74 : La politique "QoS _VoIP"

La Figure 5.74 montre l'application de la politique QoS, utilisant un shaper partagé "high-priority" et la classe d'identification "Class ID (12)" pour le trafic VoIP.

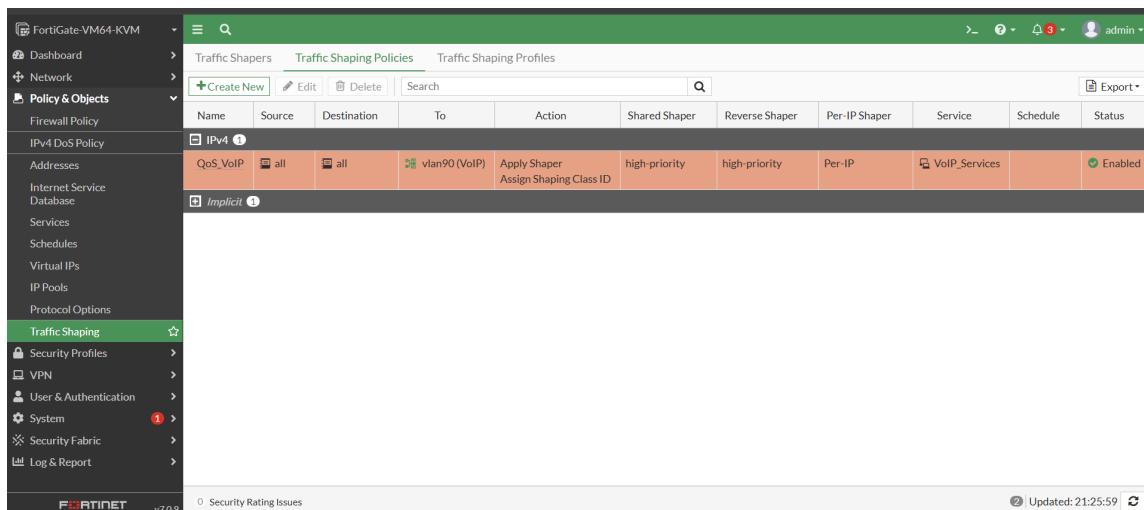


FIGURE 5.75 : "QoS _VoIP" avec ses paramètres de source, destination, et priorisation.

La Figure 5.75 offre une vue d'ensemble des politiques, confirmant la configuration de "QoS_VoIP" avec ses paramètres de source, destination et priorisation.

5.2.3.15 Configuration de NTP

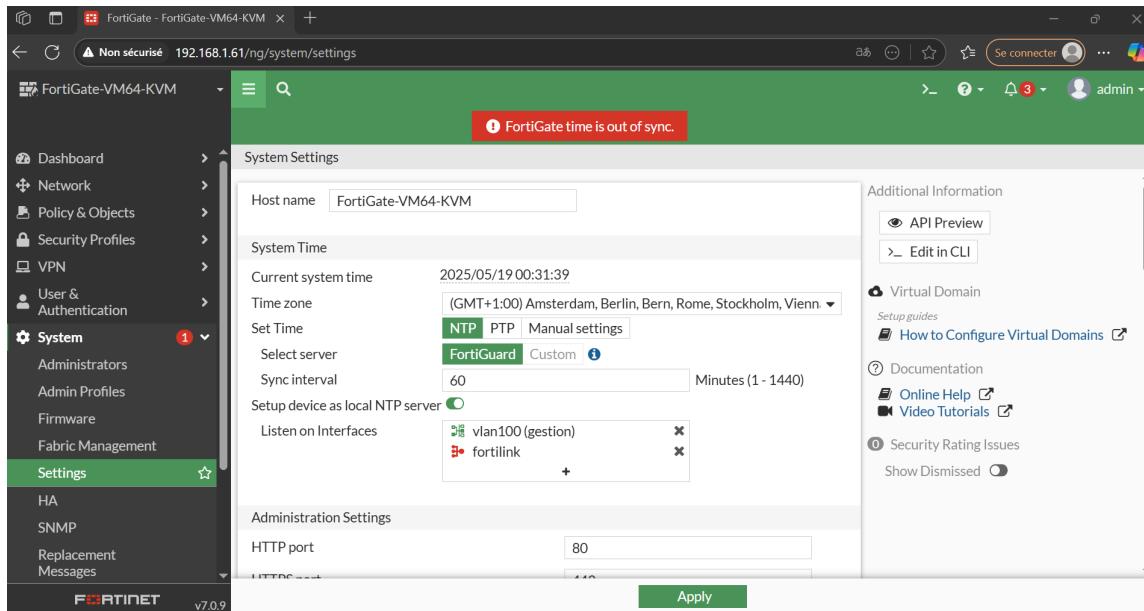


FIGURE 5.76 : Configuration NTP

La Figure 5.76 présente l'interface de configuration NTP d'un pare-feu FortiGate virtualisé. Voici l'explication des champs visibles :

- **Host name** : Identifie l'appareil (ici "FortiGate-VM64-KVM")
- **Current system time** : Affiche l'heure actuelle du système (2025/05/19 00:31:39)
- **Time zone** : Fuseau horaire configuré (GMT+1:00 pour l'Europe centrale)
- **Set Time** : Permet un réglage manuel de l'heure
- **Select server** : Menu de sélection des serveurs NTP externes
- **Sync interval** : Définit la fréquence de synchronisation avec le serveur NTP
- **Setup device as local NTP server** : Active la fonction de serveur NTP local
- **Listen on Interfaces** : Choix des interfaces réseau pour le service NTP

Cette configuration assure une synchronisation temporelle précise, cruciale pour :

- La corrélation des logs de sécurité
- La validité des certificats SSL/TLS
- La coordination entre équipements réseau

5.2.4 Accéder à l'interface graphique de ArubaOS-Switch

Cette section explique comment accéder à l'interface web sur un switch réel.

Pour configurer le switch Aruba via une connexion série, MobaXterm offre une interface complète avec gestion de sessions. Voici la procédure :

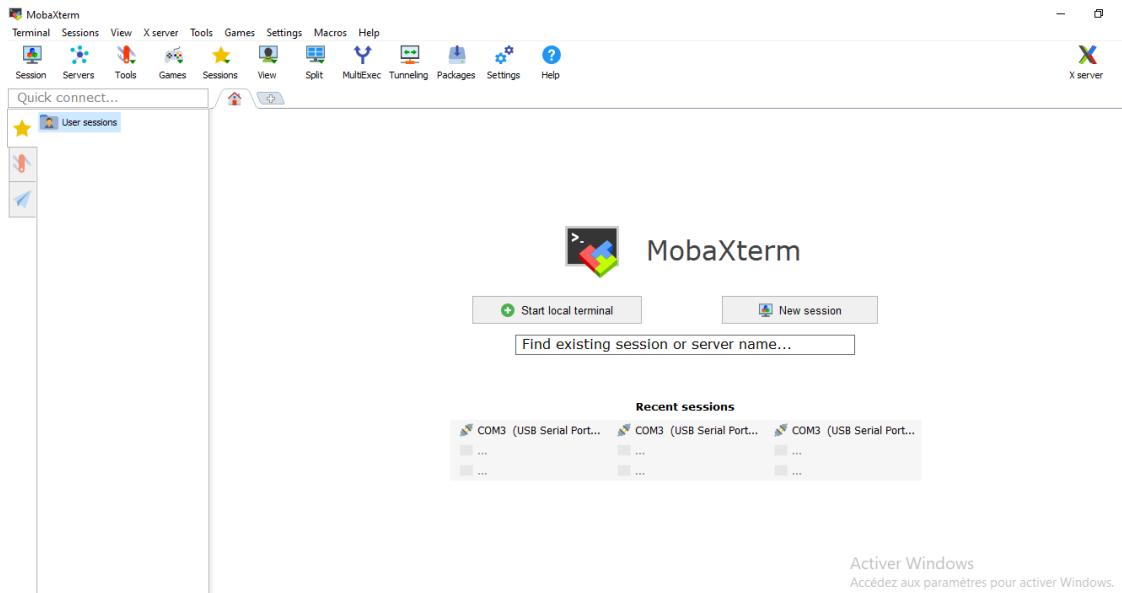


FIGURE 5.77 : Lancement d'une nouvelle session série dans MobaXterm.

Configuration initiale (figure 5.77) :

1. Lancez MobaXterm et cliquez sur **New Session**
2. Sélectionnez **Serial** dans les options disponibles
3. Choisissez la session existante COM3 ou créez-en une nouvelle

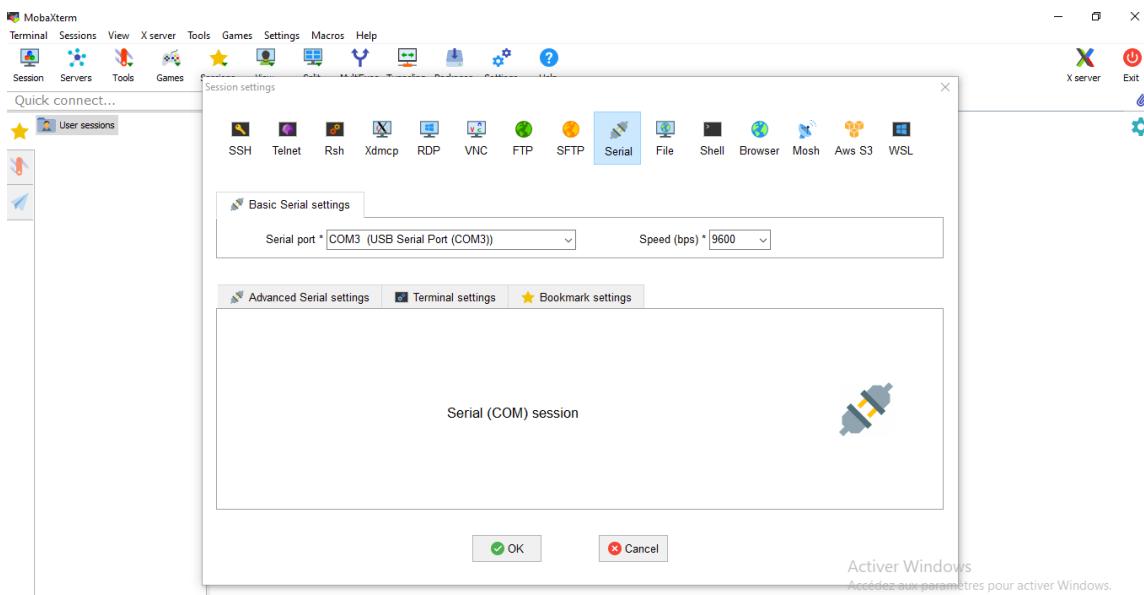


FIGURE 5.78 : Paramétrage avancé de la connexion série.

Paramètres critiques (figure 5.78) :

- **Port série :** COM3 (vérifiez le port dans le Gestionnaire de périphériques)
- **Vitesse :** 9600 bps (standard pour les switches Aruba)
- **Configuration terminal :**
 - Data bits : 8
 - Parity : None
 - Stop bits : 1
 - Flow control : None

Avantages de MobaXterm :

- Gestion des sauvegardes de sessions
- Historique des commandes
- Transfert de fichiers intégré (pour les firmware/mises à jour)
- Multi-onglets pour gérer plusieurs équipements

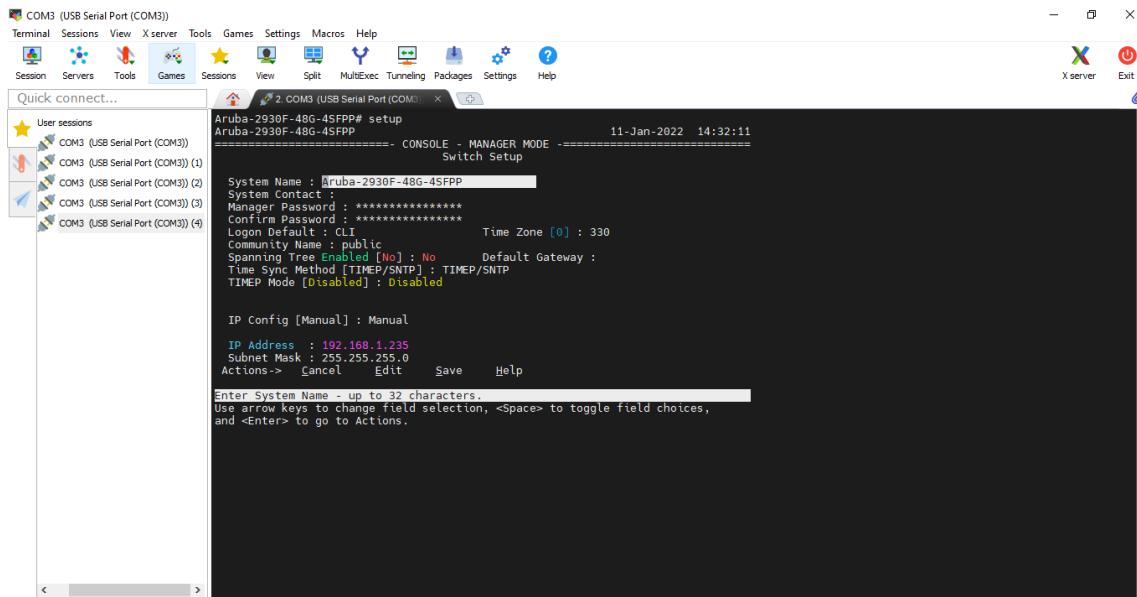


FIGURE 5.79 : Configuration initiale via console série (USB COM3).

Pour la première configuration (figure 5.79) :

1. Connectez-vous via le port console (USB COM3) avec un client terminal (MobaXterm)
 2. Configurez l'adresse IP du switch :
 - IP : 192.168.1.235
 - Masque : 255.255.255.0
 3. Définissez un mot de passe administrateur
- Accédez ensuite à l'interface web (figure 5.80) :
- URL : <https://192.168.1.235>
 - Identifiants par défaut :
 - Login : admin
 - Mot de passe : (celui configuré via console)

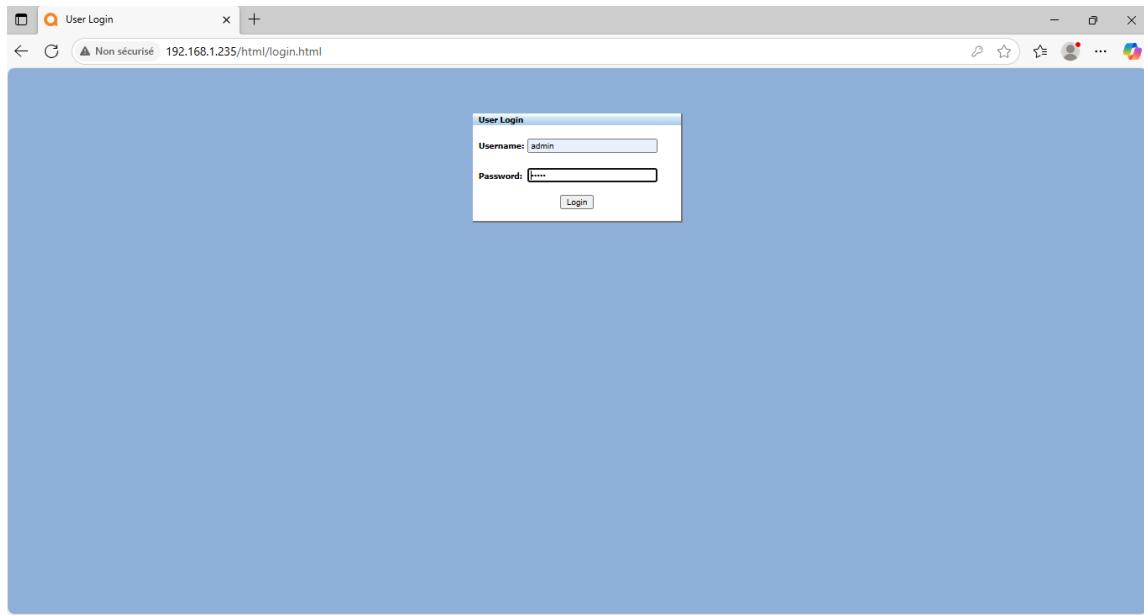


FIGURE 5.80 : Page de connexion à l'interface web.

5.2.4.1 Navigation dans l'interface

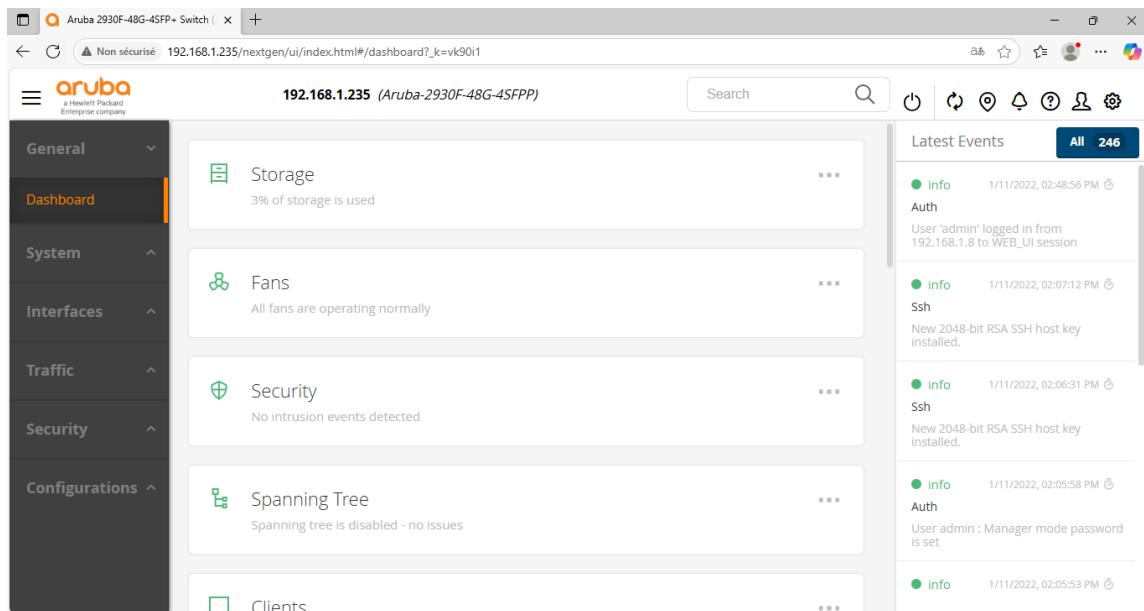


FIGURE 5.81 : Dashboard principal de l'interface ArubaOS.

L'interface principale (figure 5.81) propose :

- Vue globale du système (stockage, ventilateurs) **Interfaces** : Gestion des ports et VLAN
- Sécurité** : Configuration des politiques
- Journal des événements (logs de connexion)

5.2.4.2 Configuration des VLAN

Pour créer un VLAN (figure 5.82) :

CHAPITRE 5. CONCEPTION ET RÉALISATION

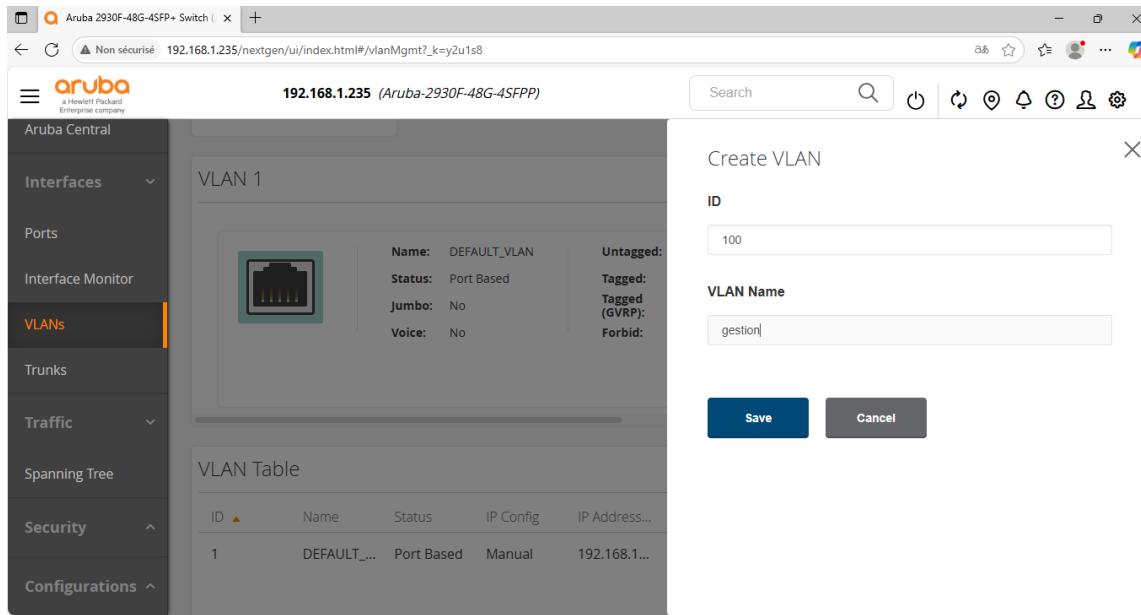


FIGURE 5.82 : Crédit d'un nouveau VLAN (ID 100).

1. Allez dans **Interfaces > VLANs**
2. Cliquez sur **Create VLAN**
3. Entrez :
 - ID : 100
 - Nom : gestion

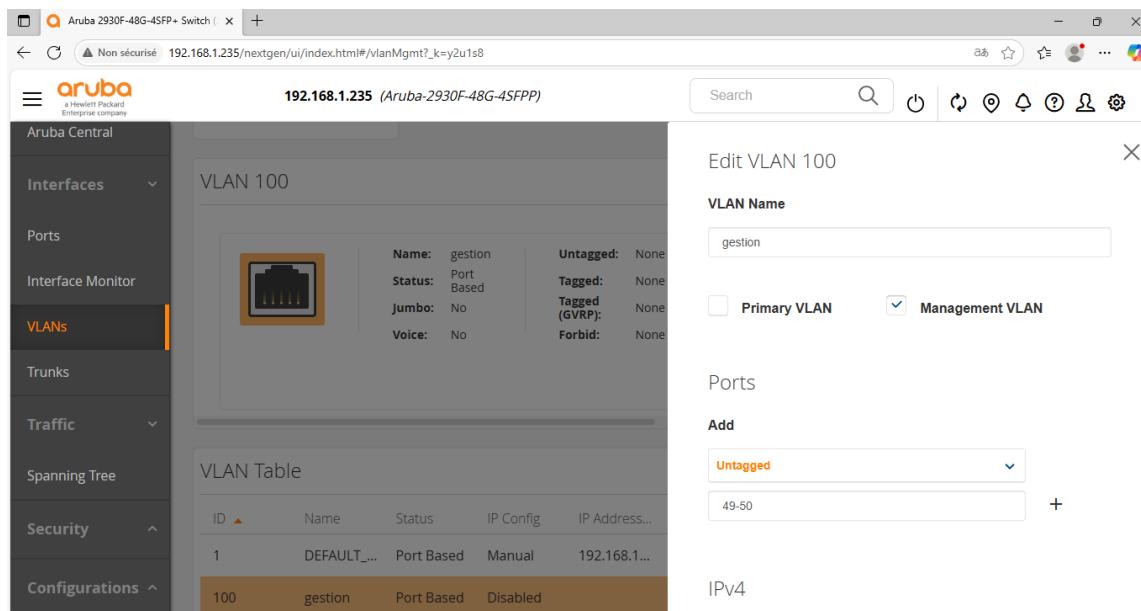


FIGURE 5.83 : Configuration détaillée du VLAN 100.

Configuration avancée (figures 5.83 et 5.84) :

- **Ports** : Affectez des ports au VLAN (untagged/tagged)
- **IPv4** : Configurez une IP de gestion si nécessaire

- Options :
 - Jumbo Frames : Désactivé
 - Voice VLAN : Non

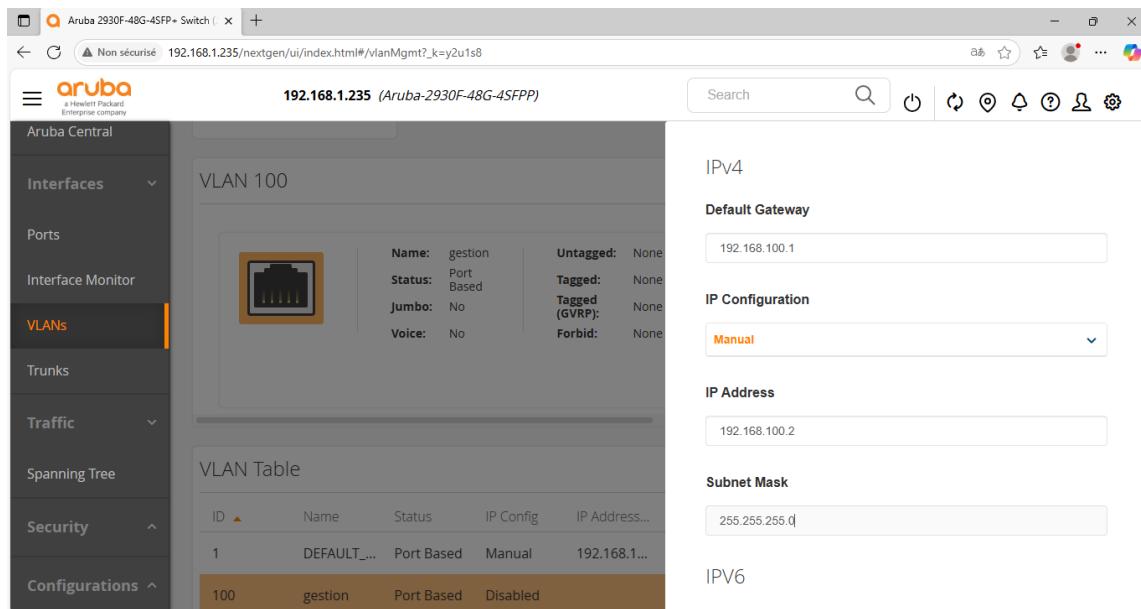


FIGURE 5.84 : Configuration IP du VLAN 100.

5.2.4.3 Vérification

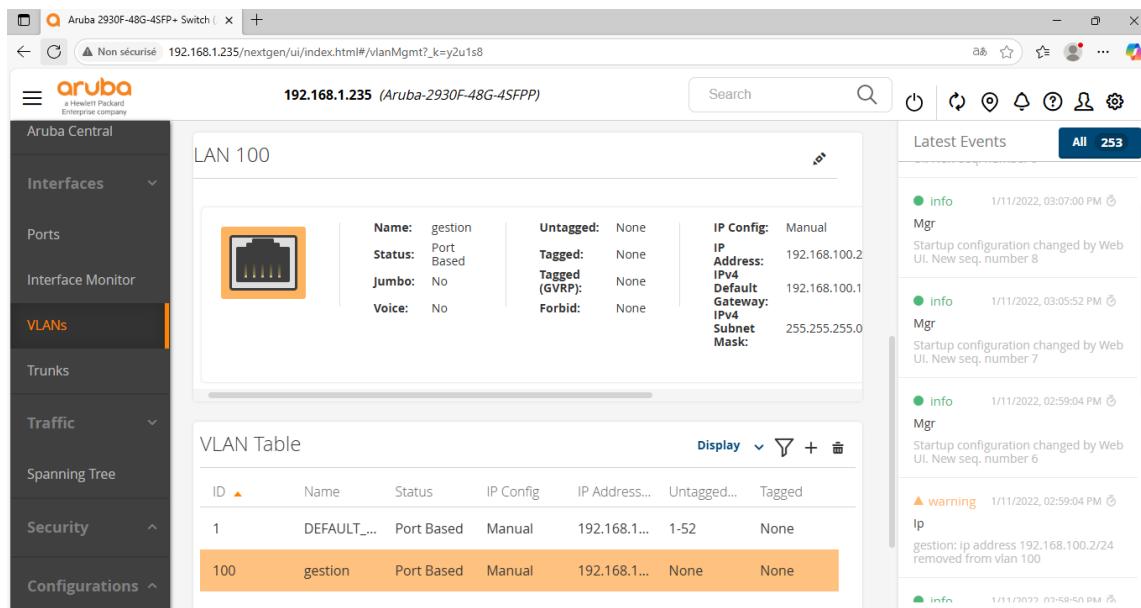


FIGURE 5.85 : Table VLAN finale avec le nouveau VLAN 100.

La table VLAN (figure 5.85) doit maintenant afficher :

- VLAN 1 (par défaut) : Ports 1-52 untagged
- VLAN 100 (gestion) : Aucun port attribué (à configurer)

5.2.5 Configuration des switch

Cette section affichera toutes les configurations effectuées sur les trois commutateurs LAN Aruba. Toutes ces commandes sont tirées du manuel officiel [2]. Concernant la VoIP la référence [9] configurer sur le même système d'exploitation.

5.2.5.1 Crée les VLANs

La configuration des VLANs sur les switches Aruba ProVision s'effectue via les commandes suivantes :

```
1      Aruba-2930F-486-4SFPP# configure terminal
2
3      ! VLANs creation
4      Aruba-2930F-486-4SFPP(config)# vlan 10
5      Aruba-2930F-486-4SFPP(vlan-10)# name cabinet
6      Aruba-2930F-486-4SFPP(vlan-10)# exit
7
8      Aruba-2930F-486-4SFPP(config)# vlan 20
9      Aruba-2930F-486-4SFPP(vlan-20)# name secretariat
10     Aruba-2930F-486-4SFPP(vlan-20)# exit
11
12     Aruba-2930F-486-4SFPP(config)# vlan 30
13     Aruba-2930F-486-4SFPP(vlan-30)# name sysinfo
14     Aruba-2930F-486-4SFPP(vlan-30)# exit
15
16     Aruba-2930F-486-4SFPP(config)# vlan 40
17     Aruba-2930F-486-4SFPP(vlan-40)# name administration
18     Aruba-2930F-486-4SFPP(vlan-40)# exit
19
20     Aruba-2930F-486-4SFPP(config)# vlan 50
21     Aruba-2930F-486-4SFPP(vlan-50)# name relations
22     Aruba-2930F-486-4SFPP(vlan-50)# exit
23
24     Aruba-2930F-486-4SFPP(config)# vlan 60
25     Aruba-2930F-486-4SFPP(vlan-60)# name communication
26     Aruba-2930F-486-4SFPP(vlan-60)# exit
27
28     Aruba-2930F-486-4SFPP(config)# vlan 70
29     Aruba-2930F-486-4SFPP(vlan-70)# name reunion
30     Aruba-2930F-486-4SFPP(vlan-70)# exit
31
32     Aruba-2930F-486-4SFPP(config)# vlan 80
33     Aruba-2930F-486-4SFPP(vlan-80)# name invite
34     Aruba-2930F-486-4SFPP(vlan-80)# exit
35
36     Aruba-2930F-486-4SFPP(config)# vlan 90
37     Aruba-2930F-486-4SFPP(vlan-10)# name voip
38     Aruba-2930F-486-4SFPP(vlan-10)# voice
39     Aruba-2930F-486-4SFPP(vlan-10)# qos dscp 101110
40     Aruba-2930F-486-4SFPP(vlan-10)# qos priority 6
41     Aruba-2930F-486-4SFPP(vlan-10)# exit
```

```

42
43     Aruba-2930F-486-4SFPP(config)# vlan 100
44     Aruba-2930F-486-4SFPP(vlan-100)# name gestion
45     Aruba-2930F-486-4SFPP(vlan-100)# exit
46
47     Aruba-2930F-486-4SFPP(config)# vlan 101
48     Aruba-2930F-486-4SFPP(vlan-101)# name natif
49     Aruba-2930F-486-4SFPP(vlan-101)# exit
50
51     Aruba-2930F-486-4SFPP(config)# vlan 102
52     Aruba-2930F-486-4SFPP(vlan-102)# name desactive
53     Aruba-2930F-486-4SFPP(vlan-102)# exit
54
55
56     Aruba-2930F-486-4SFPP(config)# write memory

```

Listing 5.1: Configuration des VLANs sur Aruba ProVision

Cette configuration est appliquée de manière similaire sur les trois switches, avec des adaptations spécifiques pour les ports d'accès selon la topologie physique.

5.2.5.2 Configuration des Points d'Accès Aruba en Mode Auto-Détection

```

1     Aruba-2930F-486-4SFPP# configure
2     ! Create a profile for the APs
3     Aruba-2930F-486-4SFPP(config)# device-profile name AP-PROFIL
4         -OFFICE
5     Aruba-2930F-48G-45FPP(device-profile)# untagged-vlan 100
6     Aruba-2930F-48G-45FPP(device-profile)# tagged-vlan 80
7     Aruba-2930F-48G-45FPP(device-profile)# poe-priority high
8     Aruba-2930F-48G-45FPP(device-profile)# allow-jumbo-frames
9     Aruba-2930F-48G-45FPP(device-profile)# exit
10
11     ! Enable auto-detection for Aruba APs
12     Aruba-2930F-48G-45FPP(config)# device-profile type aruba-ap
13         enable
14     Aruba-2930F-48G-45FPP(config)# device-profile type aruba-ap
15         associate AP-PROFIL-OFFICE

```

Listing 5.2: Configuration auto-detection des AP Aruba

Workflow d'Activation

1. L'AP envoie son identifiant via LLDP
2. Le switch reconnaît le type `aruba-ap`
3. Application instantanée du profil `AP-PROFIL-OFFICE`
4. Configuration du port :
 - Mode trunk avec VLAN 100 untagged
 - VLAN 80 autorisé en tagged
 - Priorité PoE élevée

Commandes de validation

```
1 ! Pour AP
2 Aruba-2930F-48G-45FPP# show device-profile config
3 Aruba-2930F-48G-45FPP# show device-profile status
4 ! Pour VoIP
5 Aruba-2930F-48G-45FPP# show lldp stats
6 Aruba-2930F-48G-45FPP# show lldp info remote-device
```

5.2.5.3 Switch du rez-de-chaussée

```
1 Aruba-2930F-48G-45FPP# configure
2 Aruba-2930F-48G-45FPP(config)# hostname rez-de-chaussee
3 ! Used ports
4
5 ! Sysinfo + VoIP (ports 1-4)
6 rez-de-chaussee(config)# interface 1-4
7 rez-de-chaussee(eth-1-4)# untagged vlan 30
8 rez-de-chaussee(eth-1-4)# tagged vlan 90
9 rez-de-chaussee(eth-1-4)# exit
10 rez-de-chaussee(config)# interface 5-12
11 rez-de-chaussee(eth-5-12)# untagged vlan 40
12 rez-de-chaussee(eth-5-12)# tagged vlan 90
13 rez-de-chaussee(eth-5-12)# exit
14 ! relations + VoIP (ports 13-14)
15 rez-de-chaussee(config)# interface 13-14
16 rez-de-chaussee(eth-13-14)# untagged vlan 50
17 rez-de-chaussee(eth-13-14)# tagged vlan 90
18 rez-de-chaussee(eth-13-14)# exit
19 ! Communication + VoIP (ports 15-16)
20 rez-de-chaussee(config)# interface 15-16
21 rez-de-chaussee(eth-15-16)# untagged vlan 60
22 rez-de-chaussee(eth-15-16)# tagged vlan 90
23 rez-de-chaussee(eth-15-16)# exit
24 ! reunion + VoIP (ports 17-20)
25 rez-de-chaussee(config)# interface 17-20
26 rez-de-chaussee(eth-17-20)# untagged vlan 70
27 rez-de-chaussee(eth-17-20)# tagged vlan 90
28 rez-de-chaussee(eth-17-20)# exit
29 ! Access point (port 21)
30 rez-de-chaussee(config)# interface 21
31 rez-de-chaussee(eth-21)# tagged vlan 80
32 rez-de-chaussee(eth-21)# untagged vlan 100
33 rez-de-chaussee(eth-21)# exit
34
35 ! Trunk ports
36 rez-de-chaussee(config)# interface 49-50
37 rez-de-chaussee(eth-49-50)# tagged vlan
38     10,20,30,40,50,60,70,80,90,100
      rez-de-chaussee(eth-49-50)# untagged vlan 101
```

```
39      rez-de-chaussee(eth-49-50)# no untagged vlan 1
40      rez-de-chaussee(eth-49-50)# exit
41      rez-de-chaussee(config)# interface 51
42      rez-de-chaussee(eth-51)# tagged vlan 10,20,30,40,50,60,70,80
43      rez-de-chaussee(eth-51)# untagged vlan 101
44      rez-de-chaussee(eth-51)# no untagged vlan 1
45      rez-de-chaussee(eth-51)# exit
46      rez-de-chaussee(config)# interface 52
47      rez-de-chaussee(eth-52)# tagged vlan 80,100
48      rez-de-chaussee(eth-52)# untagged vlan 101
49      rez-de-chaussee(eth-52)# no untagged vlan 1
50      rez-de-chaussee(eth-52)# exit
51
52
53      ! Unused ports
54      rez-de-chaussee(config)# interface 22-48
55      rez-de-chaussee(eth-22-48)# untagged vlan 102
56      rez-de-chaussee(eth-22-48)# shutdown
57      rez-de-chaussee(eth-22-48)# exit
58
59      ! Management interface
60      rez-de-chaussee(config)# vlan 100
61      rez-de-chaussee(vlan-100)# ip address 192.168.100.2
62          255.255.255.0
63      rez-de-chaussee(vlan-100)# exit
64
       rez-de-chaussee(config)# write memory
```

Listing 5.3: Configuration rez-de-chaussée

5.2.5.4 Switch du 1^{er} étage

```
1      Aruba-2930F-48G-45FPP# configure
2      Aruba-2930F-48G-45FPP(config)# hostname premier-etage
3      ! Used ports
4      ! Secretariat + VoIP (ports 1-7)
5      premier-etage(config)# interface 1-7
6      premier-etage(eth-1-7)# untagged vlan 20
7      premier-etage(eth-1-7)# tagged vlan 90
8      premier-etage(eth-1-7)# exit
9      ! Sysinfo + VoIP (ports 8-12)
10     premier-etage(config)# interface 8-12
11     premier-etage(eth-8-12)# untagged vlan 30
12     premier-etage(eth-8-12)# tagged vlan 90
13     premier-etage(eth-8-12)# exit
14     ! Administration + VoIP (ports 13-23)
15     premier-etage(config)# interface 13-23
16     premier-etage(eth-13-23)# untagged vlan 40
17     premier-etage(eth-13-23)# tagged vlan 90
18     premier-etage(eth-13-23)# exit
19     ! relations + VoIP (port 24)
```

```
20     premier-etage(config)# interface 24
21     premier-etage(eth-24)# untagged vlan 50
22     premier-etage(eth-24)# tagged vlan 90
23     premier-etage(eth-24)# exit
24     ! Access point (port 25)
25     premier-etage(config)# interface 25
26     premier-etage(eth-21)# tagged vlan 80
27     premier-etage(eth-21)# untagged vlan 100
28     premier-etage(eth-21)# exit
29
30     ! Fiber optic ports (trunk)
31     premier-etage(config)# interface 49-50
32     premier-etage(eth-49-50)# tagged vlan
33         10,20,30,40,50,60,70,80,90,100
34     premier-etage(eth-49-50)# untagged vlan 101
35     premier-etage(eth-49-50)# no untagged vlan 1
36     premier-etage(eth-49-50)# exit
37
38     ! Unused ports
39     premier-etage(config)# interface 26-48,51-52
40     premier-etage(eth-26-48,51-52)# untagged vlan 102
41     premier-etage(eth-26-48,51-52)# shutdown
42     premier-etage(eth-26-48,51-52)# exit
43
44     ! Management interface
45     premier-etage(config)# vlan 100
46     premier-etage(vlan-100)# ip address 192.168.100.3
47         255.255.255.0
48     premier-etage(vlan-100)# exit
49
50     premier-etage(config)# write memory
```

Listing 5.4: Configuration 1er étage

5.2.5.5 Switch du 2^{me} étage

```
1 Aruba-2930F-48G-45FPP# configure
2 Aruba-2930F-48G-45FPP(config)# hostname deuxieme-etage
3     ! Used ports
4
5     ! Cabinet + VoIP (ports 1-28)
6     deuxieme-etage(config)# interface 1-28
7     deuxieme-etage(eth-1-28)# untagged vlan 10
8     deuxieme-etage(eth-1-28)# tagged vlan 90
9     deuxieme-etage(eth-1-28)# exit
10    ! relations + VoIP (port 29)
11    deuxieme-etage(config)# interface 29
12    deuxieme-etage(eth-29)# untagged vlan 50
13    deuxieme-etage(eth-29)# tagged vlan 90
14    deuxieme-etage(eth-29)# exit
15    ! Communication + VoIP (port 30)
```

```
16      deuxieme-etage(config)# interface 30
17      deuxieme-etage(eth-30)# untagged vlan 60
18      deuxieme-etage(eth-30)# tagged vlan 90
19      deuxieme-etage(eth-30)# exit
20      ! Access point (port 31)
21      deuxieme-etage(config)# interface 31
22      deuxieme-etage(eth-31)# tagged vlan 80
23      deuxieme-etage(eth-31)# untagged vlan 100
24      deuxieme-etage(eth-31)# exit
25      ! Fiber optic ports (trunk)
26      deuxieme-etage(config)# interface 49-50
27      deuxieme-etage(eth-49-50)# tagged vlan
28          10,20,30,40,50,60,70,80,90,100
29      deuxieme-etage(eth-49-50)# untagged vlan 101
30      deuxieme-etage(eth-49-50)# no untagged vlan 1
31      deuxieme-etage(eth-49-50)# exit
32
33      ! Unused ports
34      deuxieme-etage(config)# interface 32-48,51-52
35      deuxieme-etage(eth-32-48,51-52)# untagged vlan 102
36      deuxieme-etage(eth-32-48,51-52)# shutdown
37      deuxieme-etage(eth-32-48,51-52)# exit
38
39      ! Management interface
40      deuxieme-etage(config)# vlan 100
41      deuxieme-etage(vlan-100)# ip address 192.168.100.4
42          255.255.255.0
43      deuxieme-etage(vlan-100)# exit

        deuxieme-etage(config)# write memory
```

Listing 5.5: Configuration 2^{me} étage

5.2.5.6 Explication de la configuration sur chaque Switch

Switch Rez-de-chaussée

- **Ports Data + VoIP :**
 - VLAN data en untagged (VLAN 30 à 70 selon service)
 - VLAN VoIP en tagged (VLAN 90)
- **Points d'accès Wi-Fi :**
 - Port 21 configuré pour VLAN invité (80)
- **Trunks :**
 - Ports 49-50 : Trunk principal avec tous VLANs
 - Port 51 : Services essentiels
 - Port 52 : Uniquement VLAN VoIP et gestion
- **LLDP-MED :**
 - L'autoconfiguration des terminaux VoIP est activé par défaut.
 - Permet la découverte automatique des paramètres

Switch 1^{er} étage

- Spécificités :
 - Même principe de configuration VoIP
 - Adaptation aux services spécifiques (Secrétariat, Admin)
 - Port 25 pour point d'accès Wi-Fi

Switch 2^{me} étage

- Spécificités :
 - Configuration massive des ports 1-28 pour le Cabinet
 - VoIP implémentée sur tous les ports de service
 - Port 31 pour point d'accès WiFi

Éléments Communs

- Sécurité :
 - Désactivation du VLAN 1 sur tous les ports
 - Ports inutilisés assignés au VLAN 102 et désactivés
- Gestion :
 - VLAN 100 dédié avec adresses distinctes par switch
 - Sauvegarde systématique (`write memory`)
- Connectivité :
 - Trunks fibre optique pour interconnexion
 - VLAN natif 101 pour la gestion des trunks

Schéma de Fonctionnement VoIP

1. Le téléphone IP reçoit :
 - Configuration via LLDP-MED (Activé par défaut)
 - Tag VLAN 90 pour la voix
2. Le PC connecté au téléphone :
 - Reçoit le VLAN data en untagged
 - Ne voit pas le trafic VoIP (VLAN taggué)
3. Le switch :
 - Priorise le trafic VLAN 90 (QoS)
 - Achemine voix et données séparément

Cette configuration offre :

- Une qualité de voix optimale (latence < 150ms)
- Une séparation stricte voix/données
- Une alimentation électrique fiable
- Une gestion centralisée
- Une sécurité renforcée

5.2.5.7 Configuration de MSTP

Configuration commune à tous les switches

```
1 Aruba-2930F-486-4SFPP# configure
2
3     ! MSTP activation
4     Aruba-2930F-486-4SFPP(config)# spanning-tree
5     Aruba-2930F-486-4SFPP(config)# spanning-tree mode mstp
6
7     ! MSTP region configuration (identical on all switches)
8     Aruba-2930F-486-4SFPP(config)# spanning-tree config-name
9         RESEAU_ENTREPRISE
10    ! Revision number (identical on all switches)
11    Aruba-2930F-486-4SFPP(config)# spanning-tree config-revision
12        1
13    ! MSTP timing parameters
14    ! Interval between BPDUs (1 second)
15    Aruba-2930F-486-4SFPP(config)# spanning-tree hello-time 1
16    ! Maximum number of hops before BPDU expiration
17    Aruba-2930F-486-4SFPP(config)# spanning-tree max-hops 20
18    ! Time before STP information expires (6 seconds)
19    Aruba-2930F-486-4SFPP(config)# spanning-tree maximum-age 6
20    ! Delay before ports transition to "forwarding" state (
21        forward-delay >= (maximum-age / 2) + 1)
22    Aruba-2930F-486-4SFPP(config)# spanning-tree forward-delay 4
23
24    ! MSTP instances configuration with associated VLANs
25    ! VLAN cabinet, secretariat, sysinfo, administration,
26        relations, communication, reunion, invite, natif
27
28    Aruba-2930F-486-4SFPP(config)# spanning-tree instance 1 vlan
29        10 20 30 40 50 60 70 80 101
30    ! VLAN VoIP, gestion
31    Aruba-2930F-486-4SFPP(config)# spanning-tree instance 2 vlan
32        90 100
33
34    ! Protections and security options
35    ! Reactivates ports after 300 seconds
36    Aruba-2930F-486-4SFPP(config)# spanning-tree bpdu-protection
37        -timeout 300
38    ! Limits the rate of BPDUs to prevent attacks
39    Aruba-2930F-486-4SFPP(config)# spanning-tree bpdu-throttle
40
41    ! Notification traps configuration
42    ! Alert Blocks ports in case of BPDU loss
43    Aruba-2930F-486-4SFPP(config)# spanning-tree trap loop-guard
44    ! Alert Prevents an unauthorized switch from becoming root
45    Aruba-2930F-486-4SFPP(config)# spanning-tree trap root-guard
46    ! Alert if unexpected BPDU is received
47    Aruba-2930F-486-4SFPP(config)# spanning-tree trap errant-
48        bpdu
```

```
41 ! Alert in case of root bridge change
42 Aruba-2930F-486-4SFPP(config)# spanning-tree trap new-root
43 ! Alert in case of topology change
44 Aruba-2930F-486-4SFPP(config)# spanning-tree trap topology-
45     change instance 1
46 ! Alert in case of topology change
47 Aruba-2930F-486-4SFPP(config)# spanning-tree trap topology-
48     change instance 2
```

Listing 5.6: Configuration MSTP de base

Switch rez-de-chaussée (Root Bridge Principal)

```
1 Aruba-2930F-486-4SFPP# configure
2
3 ! Definition as primary root for all instances
4 ! Priority 0 = becomes root bridge for MSTI 1
5 Aruba-2930F-486-4SFPP(config)# spanning-tree instance 1
6     priority 0
7 ! Priority 0 = becomes root bridge for MSTI 2
8 Aruba-2930F-486-4SFPP(config)# spanning-tree instance 2
9     priority 0
10
11 ! Optimization of costs on fiber trunks
12 ! High cost for this path
13 Aruba-2930F-486-4SFPP(config)# spanning-tree instance 1
14     49-51 path-cost 1000
15 ! Medium cost for instance 2
16 Aruba-2930F-486-4SFPP(config)# spanning-tree instance 2
17     49-50 path-cost 500
18 ! Medium cost for port 52
19 Aruba-2930F-486-4SFPP(config)# spanning-tree instance 2 52
20     path-cost 500
21
22 ! Disable MSTP on edge ports (user access)
23 ! Enables portfast on ports 1-21
24 Aruba-2930F-486-4SFPP(config)# spanning-tree 1-21 admin-edge
    -port
    ! Disable ports if unauthorized BPDUs are detected
    ! Security against loops
    Aruba-2930F-486-4SFPP(config)# spanning-tree 1-21 admin-edge
        -port bpdu-protection
    ! Save configuration in NVRAM
    Aruba-2930F-486-4SFPP(config)# write memory
```

Listing 5.7: Configuration Root Bridge

Switch 1^{er} étage

```
1 Aruba-2930F-486-4SFPP# configure
```

```
2      ! Switch priority definition (non-root)
3      ! Secondary priority for MSTI 1
4      Aruba-2930F-486-4SFPP(config)# spanning-tree instance 1
5          priority 3
6      ! Secondary priority for MSTI 2
7      Aruba-2930F-486-4SFPP(config)# spanning-tree instance 2
8          priority 3
9
9      ! Trunk configuration (redundant paths)
10     ! High cost for instance 1
11     Aruba-2930F-486-4SFPP(config)# spanning-tree instance 1
12         49-50 path-cost 1000
13     ! Medium cost for instance 2
14     Aruba-2930F-486-4SFPP(config)# spanning-tree instance 2
15         49-50 path-cost 500
16
17     ! Disable MSTP on edge ports
18     ! Portfast on ports 1-25
19     Aruba-2930F-486-4SFPP(config)# spanning-tree 1-25 admin-edge
20         -port
21     ! BPDU protection
22     Aruba-2930F-486-4SFPP(config)# spanning-tree 1-25 admin-edge
23         -port bpdu-protection
24     Aruba-2930F-486-4SFPP(config)# write memory
```

Listing 5.8: Configuration Secondaire

Switch 2^{me} étage

```
1      Aruba-2930F-486-4SFPP# configure
2
3      ! Priorities identical to the $2^{\{nd\}}$ floor switch
4      Aruba-2930F-486-4SFPP(config)# spanning-tree instance 1
5          priority 3
6      Aruba-2930F-486-4SFPP(config)# spanning-tree instance 2
7          priority 3
8      ! Symmetric trunk configuration
9      Aruba-2930F-486-4SFPP(config)# spanning-tree instance 1
10         49-50 path-cost 1000
11     Aruba-2930F-486-4SFPP(config)# spanning-tree instance 2
12         49-50 path-cost 500
13
14     ! Edge ports (more numerous due to more users)
15     Aruba-2930F-486-4SFPP(config)# spanning-tree 1-31 admin-edge
16         -port
17     Aruba-2930F-486-4SFPP(config)# spanning-tree 1-31 admin-edge
18         -port bpdu-protection
19     Aruba-2930F-486-4SFPP(config)# write memory
```

Listing 5.9: Configuration Secondaire

Schéma de répartition des instances

Instance	VLANs	Caractéristiques
1	10,20,30,40,50,60,70,80,101	Arbre principal
2	90, 100	Coûts réduits, priorité haute

Commandes de validation

```

1 Aruba-2930F-486-4SFPP# show spanning-tree
2 Aruba-2930F-486-4SFPP# show spanning-tree mst-config
3 Aruba-2930F-486-4SFPP# show spanning-tree instance 1

```

Avantages de cette configuration

- **Redondance optimisée** : Bascules rapides (< 1s pour VoIP)
- **Priorisation** : VLAN VoIP toujours sur le chemin optimal
- **Sécurité** : Protection contre les boucles accidentielles
- **Compatibilité** : Conservation de toutes vos configurations existantes

5.2.5.8 Configuration SSH Sécurisée

Configuration de base

```

1 Aruba-2930F-486-4SFPP# configure
2 ! Create local admin user
3 Aruba-2930F-486-4SFPP(config)# password manager user-name "
4     admin" plaintext "admin"
5
6     ! Generate an SSH key
7 Aruba-2930F-486-4SFPP(config)# crypto key generate ssh
8
9     ! Enable SSH service
10 Aruba-2930F-486-4SFPP(config)# ip ssh
11
12     ! Access restriction (optional)
13 Aruba-2930F-486-4SFPP(config)# ip access-list standard 1
14 Aruba-2930F-48G-4SFPP(config-std-nacl)# permit
15     192.168.100.100 255.255.255.0
16 Aruba-2930F-48G-4SFPP(config-std-nacl)# exit
17 Aruba-2930F-486-4SFPP(config)# vlan 100
18 Aruba-2930F-48G-4SFPP(vlan-100)# ip access-group 1 in
19 Aruba-2930F-48G-4SFPP(vlan-100)# exit

Aruba-2930F-486-4SFPP(config)# write memory

```

Vérifications

```
1 Aruba-2930F-486-4SFPP# show ip ssh
2 Aruba-2930F-486-4SFPP# show crypto host-public-key
3 Aruba-2930F-486-4SFPP# show access-list 1
```

Paramètres avancés

```
1 ! Disable Telnet
2 Aruba-2930F-486-4SFPP(config)# no telnet-server
3
4 ! Banner configuration
5 Aruba-2930F-486-4SFPP(config)# banner motd "WARNING: Access
   restricted to authorized personnel"
```

5.2.5.9 Configuration SNMPv3 Sécurisée

Configuration SNMPv3 pour ArubaOS-switch

```
1 ! Global activation of SNMPv3
2 Aruba-2930F-486-4SFPP(config)# snmpv3 enable
3 SNMPv3 Initialization process.
4 Creating user 'initial'
5 Authentication Protocol: MD5
6 Enter authentication password: *****
7 Privacy protocol is DES
8 Enter privacy password: *****
9 User 'initial' has been created
10 Would you like to create a user that uses SHA? [y/n] n
11 User creation is done. SNMPv3 is now functional.
12 Would you like to restrict SNMPv1 and SNMPv2c messages to
   have read only
13 access (you can set this later by the command 'snmpv3
   restricted-access')?
14 [y/n] n
15
16 Aruba-2930F-486-4SFPP(config)# snmpv3 restricted-access
17 ! User creation with authentication and encryption
18 Aruba-2930F-486-4SFPP(config)# snmpv3 user networkmgr auth
   md5 authpass priv privpass
19
20 ! Group definition with maximum security
21 Aruba-2930F-486-4SFPP(config)# snmpv3 group managerpriv user
   networkmgr sec-model ver3
22
23 ! SNMP community configuration (for compatibility)
24 Aruba-2930F-486-4SFPP(config)# snmpv3 community index 30
   name public sec -name networkmgr tag mgrstation1
25
26 ! Destination of SNMP traps
```

```
27 Aruba-2930F-486-4SFPP(config)# snmp-server host  
28     192.168.100.100 community public trap -level all  
29 ! Remove initial user  
Aruba-2930F-486-4SFPP(config)# no snmpv3 user initial
```

Listing 5.10: Configuration SNMPv3 Sécurisée

Explications Détaillées

Authentification Utilisateur

- `snmpv3 user networkmgr auth md5 authpass priv privpass`
 - Crée un utilisateur `networkmgr` avec authentification MD5
 - Active le chiffrement des données (option `priv`)

Gestion des Groupes

- `snmpv3 group managerpriv user networkmgr sec-model ver3`
 - Crée un groupe `managerpriv` avec accès complet
 - Restreint l'accès au modèle de sécurité v3 (le plus sécurisé)

Compatibilité avec SNMPv2c

- `snmpv3 community index 30 name public [...]`
 - Maintient une compatibilité avec les anciens systèmes
 - Relie la communauté `public` à l'utilisateur SNMPv3

5.2.5.10 Configuration Syslog

```
1 Aruba-2930F-486-4SFPP# configure  
2 ! Syslog server  
3 Aruba-2930F-486-4SFPP(config)# logging 192.168.100.100  
4 Aruba-2930F-486-4SFPP(config)# logging severity warning
```

Explications de configuration

Commande `logging 192.168.100.100`

- Envoie les journaux système (*logs*) vers un serveur distant
- Adresse IP 192.168.100.100 est l'adresse de serveur Syslog
- Source définie sur VLAN 100 (gestion)

Commande `logging severity warning`

- Filtre les logs par niveau de严重性
- Niveaux disponibles (du moins au plus critique) :
 1. debugging
 2. informational

3. notice
 4. **warning** (niveau configuré)
 5. error
 6. critical
 7. alert
 8. emergency
- Ne transmet que les messages de niveau **warning** et supérieurs

5.2.5.11 Configuration NTP

```
1 Aruba-2930F-486-4SFPP# configure
2   ! Synchronization with FortiGate and Algerian servers
3   Aruba-2930F-486-4SFPP(config)# timesync ntp
4   Aruba-2930F-486-4SFPP(config)# ntp enable
5   Aruba-2930F-486-4SFPP(config)# ntp server 192.168.100.1
6     iburst
7   Aruba-2930F-486-4SFPP(config)# ntp unicast
8   Aruba-2930F-486-4SFPP(config)# clock timezone gmt +1:00
9
10  ! Verification
11  Aruba-2930F-486-4SFPP(config)# show ntp association
12  Aruba-2930F-486-4SFPP(config)# show ntp status
13  Aruba-2930F-486-4SFPP(config)# show time
```

Commandes de Configuration

- **timesync ntp** : Active la synchronisation temporelle via NTP
- **ntp enable** : Active le service NTP sur l'équipement
- **ntp server 192.168.100.1 iburst** :
 - Spécifie le serveur NTP (ici un FortiGate à 192.168.100.1)
 - Option **iburst** : Envoie rafale de paquets pour synchronisation rapide
- **ntp unicast** : Utilise le mode unicast pour la communication NTP
- **clock timezone gmt +1:00** : Commande de base pour définir le fuseau horaire, décalage horaire une heure d'avance par rapport à GMT/UTC.

Commandes de Vérification

- **show ntp association** : Affiche les associations NTP actives
- **show ntp status** : Montre le statut de synchronisation
- **show time** : Affiche l'heure actuelle de l'équipement

5.2.5.12 Schéma de Flux SNMPv3, SYSLOG, NTP

Service	Protocole/Port	Destination
SNMPv3	UDP 161	192.168.100.100
Syslog	UDP 514	192.168.100.100
NTP	UDP 123	192.168.100.1

Cette configuration assure :

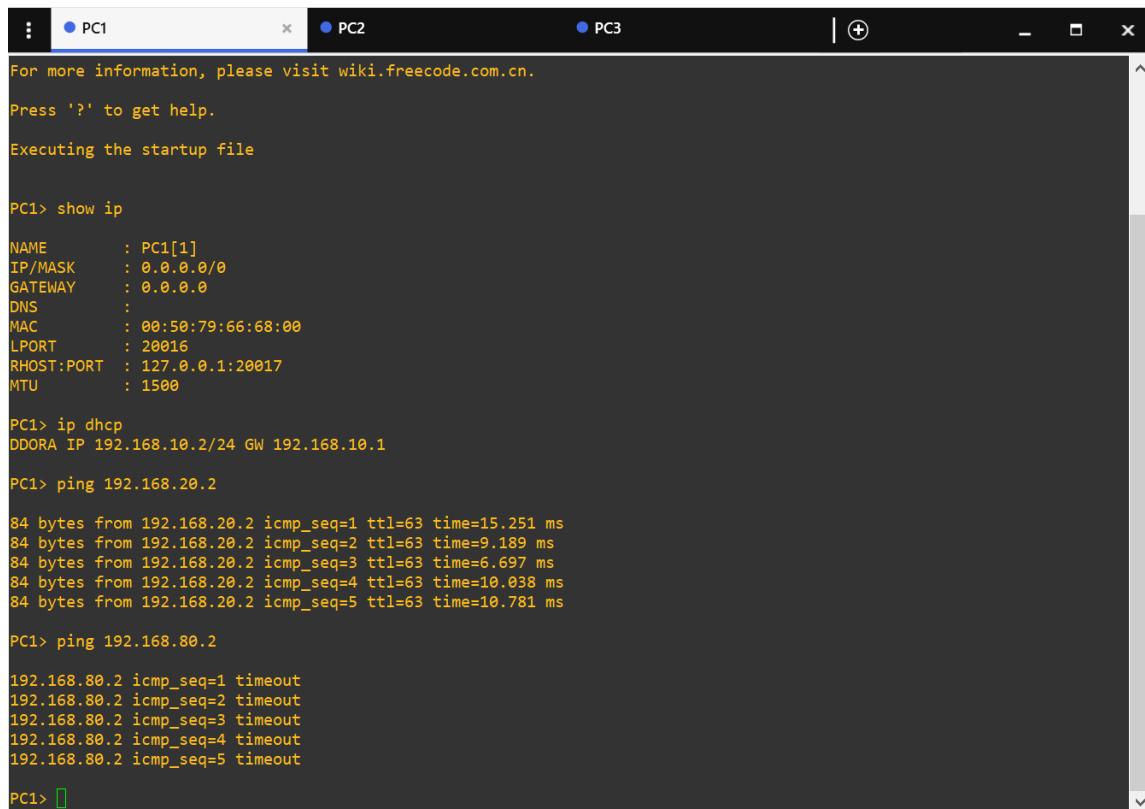
- Une gestion sécurisée (chiffrement AES/SHA)
 - Une journalisation centralisée
 - Une synchronisation temporelle précise
 - Une conformité aux spécificités algériennes

5.2.6 Vérification

Cette section présente les résultats des tests de connectivité entre les VLAN, la vérification du filtrage web et la vérification configuration MSTP. Les tests confirment que les VLAN des services communiquent entre eux, tandis que le VLAN invité est isolé. De plus, le filtrage web bloque efficacement l'accès à Facebook pour les VLAN des services.

5.2.6.1 Connectivité entre les VLAN

Les tests suivants démontrent la connectivité entre les VLAN des services et l'isolation du VLAN invité.



```

For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC1> show ip

NAME      : PC1[1]
IP/MASK   : 0.0.0.0/0
GATEWAY   : 0.0.0.0
DNS       :
MAC       : 00:50:79:66:68:00
LPORT     : 20016
RHOST:PORT: 127.0.0.1:20017
MTU       : 1500

PC1> ip dhcp
DDORA IP 192.168.10.2/24 GW 192.168.10.1

PC1> ping 192.168.20.2

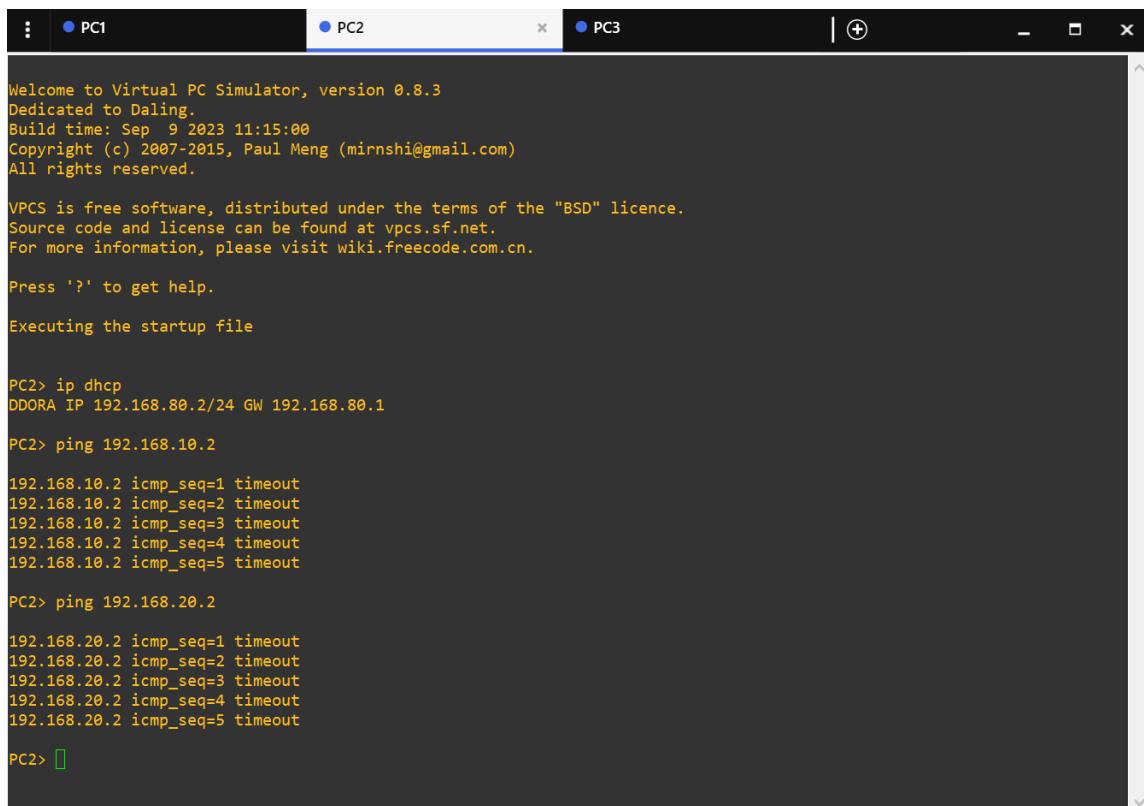
84 bytes from 192.168.20.2 icmp_seq=1 ttl=63 time=15.251 ms
84 bytes from 192.168.20.2 icmp_seq=2 ttl=63 time=9.189 ms
84 bytes from 192.168.20.2 icmp_seq=3 ttl=63 time=6.697 ms
84 bytes from 192.168.20.2 icmp_seq=4 ttl=63 time=10.038 ms
84 bytes from 192.168.20.2 icmp_seq=5 ttl=63 time=10.781 ms

PC1> ping 192.168.80.2

192.168.80.2 icmp_seq=1 timeout
192.168.80.2 icmp_seq=2 timeout
192.168.80.2 icmp_seq=3 timeout
192.168.80.2 icmp_seq=4 timeout
192.168.80.2 icmp_seq=5 timeout

```

FIGURE 5.86 : (VLAN cabinet) : Connectivité vers VLAN 20 (succès) et VLAN 80 (échec)



```
Welcome to Virtual PC Simulator, version 0.8.3
Dedicated to Daling.
Build time: Sep 9 2023 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

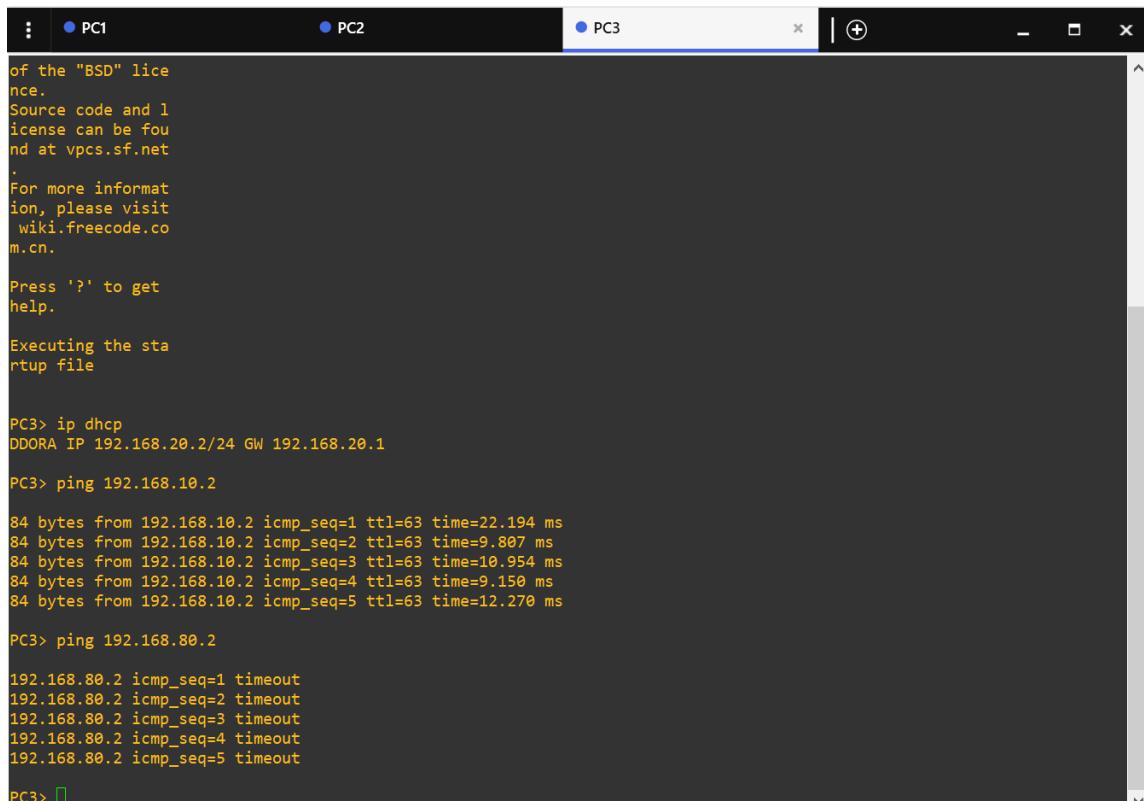
PC2> ip dhcp
DDORA IP 192.168.80.2/24 GW 192.168.80.1

PC2> ping 192.168.10.2
192.168.10.2 icmp_seq=1 timeout
192.168.10.2 icmp_seq=2 timeout
192.168.10.2 icmp_seq=3 timeout
192.168.10.2 icmp_seq=4 timeout
192.168.10.2 icmp_seq=5 timeout

PC2> ping 192.168.20.2
192.168.20.2 icmp_seq=1 timeout
192.168.20.2 icmp_seq=2 timeout
192.168.20.2 icmp_seq=3 timeout
192.168.20.2 icmp_seq=4 timeout
192.168.20.2 icmp_seq=5 timeout

PC2> 
```

FIGURE 5.87 : (VLAN invité) : Échec des requêtes vers les VLAN des services



```
of the "BSD" lice
nse.
Source code and l
icense can be fou
nd at vpcs.sf.net
.

For more informat
ion, please visit
wiki.freecode.co
m.cn.

Press '?' to get
help.

Executing the sta
rtup file

PC3> ip dhcp
DDORA IP 192.168.20.2/24 GW 192.168.20.1

PC3> ping 192.168.10.2
84 bytes from 192.168.10.2 icmp_seq=1 ttl=63 time=22.194 ms
84 bytes from 192.168.10.2 icmp_seq=2 ttl=63 time=9.807 ms
84 bytes from 192.168.10.2 icmp_seq=3 ttl=63 time=10.954 ms
84 bytes from 192.168.10.2 icmp_seq=4 ttl=63 time=9.150 ms
84 bytes from 192.168.10.2 icmp_seq=5 ttl=63 time=12.270 ms

PC3> ping 192.168.80.2
192.168.80.2 icmp_seq=1 timeout
192.168.80.2 icmp_seq=2 timeout
192.168.80.2 icmp_seq=3 timeout
192.168.80.2 icmp_seq=4 timeout
192.168.80.2 icmp_seq=5 timeout

PC3> 
```

FIGURE 5.88 : (vlan secretariat) : Connectivité vers VLAN 10 (succès) et VLAN 80 (échec)

5.2.6.2 Accès à Facebook

Les figures suivantes montrent le filtrage web actif sur les VLAN des services, bloquant l'accès à Facebook.

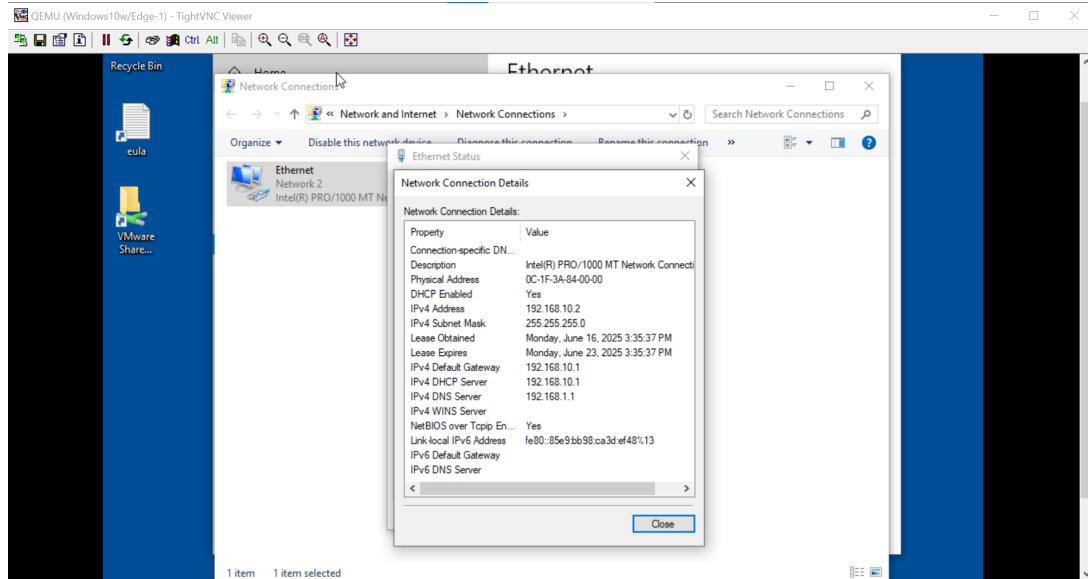


FIGURE 5.89 : Configuration réseau d'une machine dans VLAN cabonet

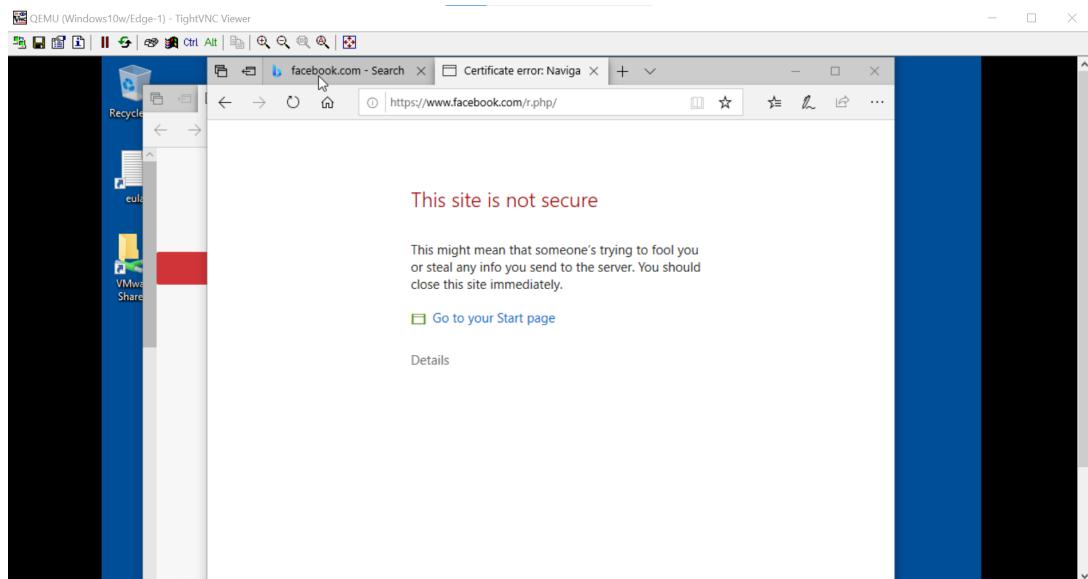
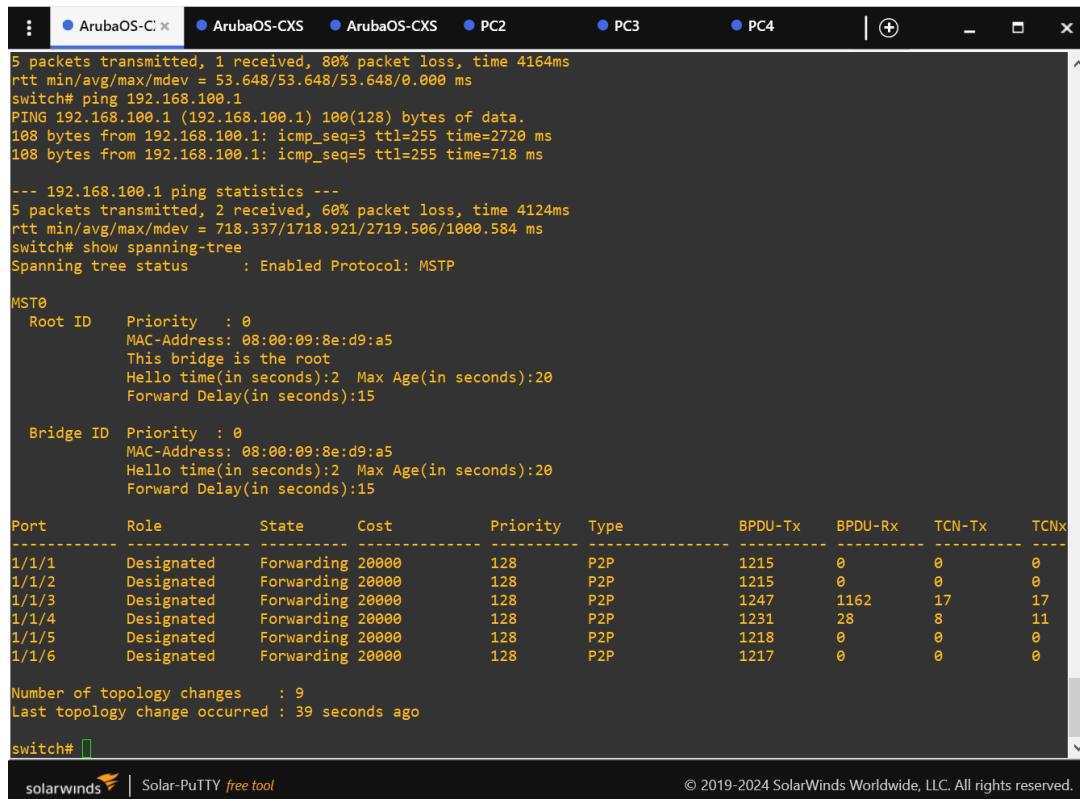


FIGURE 5.90 : Message de blocage lors de la tentative d'accès à Facebook

5.2.6.3 Configuration MSTP

CHAPITRE 5. CONCEPTION ET RÉALISATION



```

ArubaOS-C: ArubaOS-CXS ArubaOS-CXS PC2 PC3 PC4
5 packets transmitted, 1 received, 80% packet loss, time 4164ms
rtt min/avg/max/mdev = 53.648/53.648/53.648/0.000 ms
switch# ping 192.168.100.1
PING 192.168.100.1 (192.168.100.1) 100(128) bytes of data.
108 bytes from 192.168.100.1: icmp_seq=3 ttl=255 time=2720 ms
108 bytes from 192.168.100.1: icmp_seq=5 ttl=255 time=718 ms

--- 192.168.100.1 ping statistics ---
5 packets transmitted, 2 received, 50% packet loss, time 4124ms
rtt min/avg/max/mdev = 718.337/1718.921/2719.506/1000.584 ms
switch# show spanning-tree
Spanning tree status : Enabled Protocol: MSTP

MST0
  Root ID  Priority : 0
    MAC-Address: 08:00:09:8e:d9:a5
    This bridge is the root
    Hello time(in seconds):2  Max Age(in seconds):20
    Forward Delay(in seconds):15

  Bridge ID Priority : 0
    MAC-Address: 08:00:09:8e:d9:a5
    Hello time(in seconds):2  Max Age(in seconds):20
    Forward Delay(in seconds):15

Port      Role     State   Cost    Priority Type        BPDU-Tx   BPDU-Rx   TCN-Tx   TCNx
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1/1/1    Designated Forwarding 20000 128    P2P       1215      0         0         0
1/1/2    Designated Forwarding 20000 128    P2P       1215      0         0         0
1/1/3    Designated Forwarding 20000 128    P2P       1247      1162      17        17
1/1/4    Designated Forwarding 20000 128    P2P       1231      28        8         11
1/1/5    Designated Forwarding 20000 128    P2P       1218      0         0         0
1/1/6    Designated Forwarding 20000 128    P2P       1217      0         0         0

Number of topology changes : 9
Last topology change occurred : 39 seconds ago
switch# 

```

solarwinds | Solar-PuTTY free tool © 2019-2024 SolarWinds Worldwide, LLC. All rights reserved.

FIGURE 5.91 : Switch du rez-de-chaussée



```

ArubaOS-CXS ArubaOS-C: ArubaOS-CXS PC2 PC3 PC4
!
!
https-server vrf mgmt
switch# ping 192.168.100.1
PING 192.168.100.1 (192.168.100.1) 100(128) bytes of data.
108 bytes from 192.168.100.1: icmp_seq=1 ttl=255 time=388 ms
108 bytes from 192.168.100.1: icmp_seq=2 ttl=255 time=267 ms
108 bytes from 192.168.100.1: icmp_seq=3 ttl=255 time=169 ms
108 bytes from 192.168.100.1: icmp_seq=4 ttl=255 time=788 ms
108 bytes from 192.168.100.1: icmp_seq=5 ttl=255 time=122 ms

--- 192.168.100.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4013ms
rtt min/avg/max/mdev = 122.003/346.795/787.817/238.656 ms
switch# show spanning-tree
Spanning tree status : Enabled Protocol: MSTP

MST0
  Root ID  Priority : 0
    MAC-Address: 08:00:09:8e:d9:a5
    Hello time(in seconds):2  Max Age(in seconds):20
    Forward Delay(in seconds):15

  Bridge ID Priority : 12288
    MAC-Address: 08:00:09:7e:84:79
    Hello time(in seconds):2  Max Age(in seconds):20
    Forward Delay(in seconds):15

Port      Role     State   Cost    Priority Type        BPDU-Tx   BPDU-Rx   TCN-Tx   TCNx
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1/1/1    Root     Forwarding 20000 128    P2P       1028      1020      16        15
1/1/2    Designated Forwarding 20000 128    P2P       1013      92        11        10
1/1/3    Designated Forwarding 20000 128    P2P       987       0         0         0

Number of topology changes : 12
Last topology change occurred : 68 seconds ago
switch# 

```

solarwinds | Solar-PuTTY free tool © 2019-2024 SolarWinds Worldwide, LLC. All rights reserved.

FIGURE 5.92 : Switch du 1^{er} étage

```

switch# show spanning-tree
Spanning tree status      : Enabled Protocol: MSTP

MST0
Root ID  Priority   : 0
MAC-Address: 08:00:09:8e:d9:a5
Hello time(in seconds):2 Max Age(in seconds):20
Forward Delay(in seconds):15

Bridge ID Priority   : 12288
MAC-Address: 08:00:09:ad:35:a6
Hello time(in seconds):2 Max Age(in seconds):20
Forward Delay(in seconds):15

Port      Role       State     Cost      Priority Type        BPDU-Tx   BPDU-Rx   TCN-Tx   TCNx
-----  -----
1/1/1    Alternate  Blocking  20000     128     P2P        56        768       7        11
1/1/2    Root       Forwarding 20000     128     P2P        680       99        13       8
1/1/3    Designated Forwarding 20000     128     P2P        744       0         0        0
1/1/4    Disabled   Down      20000     128     Shr        0         0         0        0
1/1/5    Designated Forwarding 20000     128     P2P        744       0         0        0

Number of topology changes   : 7
Last topology change occurred : 91 seconds ago

switch# show spanning-tree detail
Spanning tree status      : Enabled Protocol: MSTP

MST0
Root ID  Priority   : 0
MAC-Address: 08:00:09:8e:d9:a5
Hello time(in seconds):2 Max Age(in seconds):20
Forward Delay(in seconds):15

Bridge ID Priority   : 12288
MAC-Address: 08:00:09:ad:35:a6
Hello time(in seconds):2 Max Age(in seconds):20
Forward Delay(in seconds):15
    
```

 FIGURE 5.93 : Switch du 2^{ème} étage

Conclusion

La conception et la mise en œuvre du réseau ont permis de répondre aux besoins fonctionnels et de sécurité, avec une segmentation VLAN efficace, une gestion centralisée et des politiques optimisées pour la VoIP. Les tests en simulation (GNS3) ont validé la robustesse de l'architecture avant son déploiement réel.

CONCLUSION GÉNÉRALE

Au terme de ce mémoire, nous avons démontré l'importance capitale de la sécurisation d'un réseau local dans un environnement professionnel où la confidentialité, l'intégrité et la disponibilité des données constituent des enjeux stratégiques. En partant d'un diagnostic générique d'une infrastructure réseau typique d'une institution publique, plusieurs vulnérabilités courantes ont été identifiées, soulignant la nécessité de renforcer les dispositifs de protection.

La mise en place de VLANs a permis de segmenter le réseau selon des besoins fonctionnels standards, limitant ainsi les risques de propagation d'attaques internes. L'intégration d'un pare-feu a renforcé le filtrage des flux entrants et sortants, en instaurant des politiques de sécurité adaptées aux services déployés. De plus, la configuration du protocole MSTP a évité les boucles réseau et amélioré la qualité de service (QoS).

Cette étude de cas illustre qu'avec une analyse rigoureuse des besoins et une bonne maîtrise des technologies réseaux, il est tout à fait possible de sécuriser efficacement une infrastructure locale sans recourir à des solutions complexes ou onéreuses. Ce travail a également représenté une opportunité d'enrichissement professionnel, en appliquant les connaissances acquises dans un contexte simulé et hypothétique.

Enfin, il convient de rappeler que la sécurité réseau n'est jamais un état figé, mais un processus continu d'adaptation face à l'évolution constante des menaces. Il est donc essentiel d'assurer une veille technologique permanente et de maintenir les dispositifs de protection à jour pour garantir la résilience des systèmes d'information.

BIBLIOGRAPHIE

- [1] Understanding and Configuring VLAN Trunk Protocol(VTP). cisco.
- [2] Aruba, a Hewlett Packard Enterprise company. Aruba 2930F Switch Series Installation and Getting Started Guide, Mai 2021. Document Part Number : a00110676en_us.
- [3] Gildas Avoine, Pascal Junod, Philippe Balbiani Oechslin, and Sylvain Pasini. Sécurité informatique. Vuibert, 2010.
- [4] Christophe Bloch, Laurent ;Wolfhugel. Sécurité informatique : principes et méthode. Eyrolles, 2007.
- [5] Makarevitch N. Bloch L., Wolfhugel C. Securite informatique : Principes et methode. Eyrolles, 2009.
- [6] Cisco Systems. 802.1x authentication on catalyst 6500 series switches. https://www.cisco.com/c/fr_ca/support/docs/switches/catalyst-6500-series-switches/81871-8021xauth-cat65k.pdf. Consulté le 8/5/2025.
- [7] Robert Crocfer David Puche Jérôme Hennecart Sébastien Lasson Marion Agé Franck Ebel, Sébastien Baudru. Sécurité informatique - Ethical Hacking - Apprendre l'attaque pour mieux se défendre. Editions ENI, 2009.
- [8] Olivier Goffinet. Redondance de liens : Spanning-tree (stp, rstp, pvst+). <https://cisco.goffinet.org/ccna/redondance-de-liens/spanning-tree-rapid-stp-pvst-cisco/>.
- [9] Hewlett-Packard. Procurve lldp (link layer discovery protocol). <https://fr.scribd.com/document/822159686/ProCurve-lldp>, 2021. Document technique HP/Aruba.
- [10] Jean-Philippe Bay Jean-François Pillou. Tout sur la sécurité informatique. Dunod, 4 edition, 2016.
- [11] Christophe Wolfhugel Laurent Bloch. Sécurité informatique : Principes et méthode à l'usage des DSI, RSSI et administrateurs.
- [12] Chris Lewis. Cisco Switched Internetworks : VLANs, ATM & Voice Data Integration. McGraw-Hill, 1 edition, 1999.
- [13] Paul RASCAGNERES. Sécurité informatique et Malwares Analyse et contre-mesures. 0.

BIBLIOGRAPHIE

- [14] Mulayam Singh. SPANNING TREE PROTOCOL : Most important topic in switching. BookRix, 2022.
- [15] Douicher Yacer and Sissoko Seydou. Mise en place d'un Pare-Feu en utilisant Le Smoothwall. PhD thesis, Université Mouloud Mammeri, 2012.
- [16] Touzi Yasmine and Larbi Khadidja. Mise en place d'une sécurité réseau basée sur l'utilisation des VLANs et des VACLs au niveau de l'entreprise ENIEM. PhD thesis, Université Mouloud Mammeri, 2017.