Livrable 1 : Réponse au cahier des charges

Table des matières

1. Présentation du groupe

1.1. Composition et présentation

- ABGARYAN Arman : Responsable Infrastructure et Sécurité.
- Rôle : Chef de Projet.

1.2. Définition des rôles et responsabilités

- Chef de Projet : Gestion du planning, du budget et coordination des phases de test.
- Administrateur Réseaux : Configuration de la Haute Disponibilité sur pfSense, gestion de la DMZ et du VPN Road Warrior.
- Administrateur Systèmes : Déploiement des serveurs Active Directory, installation de Exchange et du serveur web eBrigade.
- Responsable Supervision & VoIP : Mise en œuvre de Zabbix et de la solution de téléphonie IP.

2. Lexique des acronymes utilisés

2.1. Définition des rôles et responsabilités

Acronyme	Définition
SIDSIC	Service Interministériel Départemental des Systèmes d'Informations et de Communication
SIDPC	Service Interministériel de Défense et de Protection Civiles
COD	Centre Opérationnel Départemental
ORSEC	Organisation de la Réponse de Sécurité Civile
REX	Retour d'Expérience
SIC	Systèmes d'Informations et de Communication

2.2. Réseaux et Infrastructures

Acronyme	Définition
AD / AD DS	Active Directory (Domain Services)
IpBX	Internet Protocol Private Branch Exchange
VoIP	Voix sur IP (Voice over IP)
LDAP	Lightweight Directory Access Protocol
SMTP	Simple Mail Transfer Protocol
CARP	Common Address Redundancy Protocol
CAL	Client Access License

3. Contexte du projet

3.1. La sécurité Civile en France

La sécurité civile représente l'ensemble des moyens mis en œuvre par l'État pour assurer la protection des citoyens, des biens et de l'environnement, que ce soit en temps de paix ou lors de crises majeures. Elle repose sur une organisation hiérarchisée allant du niveau national (Ministère de l'Intérieur) au niveau communal (Maire), en passant par les échelons zonaux et départementaux (Préfets).

En cas d'événement exceptionnel (catastrophe naturelle, accident technologique, crise sanitaire), le dispositif ORSEC (Organisation de la Réponse de Sécurité Civile) est activé par le Préfet pour coordonner l'ensemble des acteurs de secours (Sapeurs-Pompiers, associations agréées, services de l'État).

3.2. Le Service Interministériel Départemental (SIDSIC)

L'action du projet s'inscrit au cœur du SIDSIC (Service Interministériel départemental des systèmes d'informations et de communication). Placé sous l'autorité du secrétaire général de la préfecture, ce service est le garant de la continuité des liaisons gouvernementales.

Ses missions sont critiques :

- Maintenir en condition opérationnelle les systèmes informatiques et de communication (SIC).
- Gérer l'infrastructure du Centre Opérationnel Départemental (COD).
- Assurer le support technique en situation de crise pour permettre la coordination des opérations de secours.

3.3. Le centre Opérationnel Départemental (COD)

Le COD est l'organe de pilotage activé par le Préfet lors d'une crise. Il regroupe, dans des salles spécialisées (situation, décision, cellules de liaison), l'ensemble des décideurs et experts nécessaires à la gestion de l'événement. Pour fonctionner de manière optimale, le COD s'appuie sur une infrastructure technique lourde : postes de travail multi-écrans, cartographie opérationnelle, main courante informatisée et liaisons réseaux diversifiées (Internet, Radio, Satellite).

4. Rappel des besoins et des objectifs

4.1. Diagnostic et enjeux

Le projet émane de constats réalisés lors de précédents Retours d'Expériences (REX). Le Directeur du SIDSIC a souligné plusieurs vulnérabilités majeures :

- Instabilité des réseaux : Des coupures de téléphonie et d'accès Internet ont été constatées en salle de crise, forçant l'utilisation de réseaux mobiles souvent saturés.
- Isolement du terrain : Les agents déployés sur les lieux de l'événement manquent d'un accès sécurisé et fluide aux outils métiers habituels du COD pour échanger des informations en temps réel.

4.2. Besoins fonctionnels détaillés

Pour pallier ces faiblesses, la solution technique doit répondre à quatre piliers fondamentaux :

- La Résilience et Haute Disponibilité : Le système doit être capable de supporter la défaillance d'un routeur ou d'un lien WAN sans interrompre le travail des cellules de crise.
- L'Autonomie et la Souveraineté : Par mesure de sécurité et de continuité de service, tous les serveurs critiques (Messagerie Exchange, Téléphonie IpBX, Gestion eBrigade) doivent être hébergés localement sur l'infrastructure de la Préfecture.
- La Mobilité Sécurisée (Road Warrior) : Il est impératif de permettre aux agents de terrain de se connecter au réseau de la Préfecture via un VPN sécurisé pour utiliser la téléphonie IP (softphone), envoyer des courriels et mettre à jour la main courante eBrigade.

- La Supervision Proactive : Les administrateurs doivent disposer d'un tableau de bord en temps réel (Zabbix) pour surveiller l'état des équipements critiques et être alertés immédiatement par courriel en cas d'anomalie.

4.3. Objectifs techniques à atteindre

La proposition technique doit valider la mise en œuvre des éléments suivants pour une cible de 10 utilisateurs simultanés :

- Configuration d'un cluster de pare-feux pfSense avec basculement automatique.
- Déploiement d'un annuaire Active Directory redondé (Principal et Secondaire) pour l'authentification unique des services.
- Installation et sécurisation d'une DMZ pour l'accès web à l'application métier eBrigade.
- Mise en place de règles de filtrage réseau strictes pour garantir l'intégrité des données gouvernementales.
- Réalisation d'un maquettage virtuel complet permettant de prouver la viabilité de la solution avant son déploiement réel.

5. Solutions Techniques

L'architecture technique retenue pour le Centre Opérationnel Départemental (COD) a été conçue autour d'un impératif majeur qui est la continuité de service en situation de crise.

Pour répondre aux exigences de résilience et de mobilité du cahier des charges, nous avons privilégié une approche hybride. Celle-ci combine la robustesse des solutions propriétaires imposées pour la gestion de l'identité et de la messagerie, à la flexibilité et au moindre coût des solutions Open Source pour la sécurité périmétrale, la téléphonie et la supervision.

5.1. Solution IpBX : Xivo

Le besoin de téléphonie IP locale est essentiel pour la coordination des secours sans dépendre exclusivement des réseaux mobiles saturés.

Critères	XIVO	3CX	FreePBX
Origine	Française	Chypre/USA	USA
Maintenance	Grosse mise à jour Régulière	Auto update uniquement sur le Cloud	Communautaire
Coût Licence	Gratuit	Payant au-delà de 4 appels	Gratuit
Couplage AD	LDAP/LDAPS	LDAP/LDAPS	LDAP/LDAPS
Souveraineté	Maximale (Code auditable)	Faible (Propriétaire)	Moyenne
Choix	✅	❌	❌

Nous avons choisi XiVO principalement pour sa souveraineté française, un point fort pour une administration publique, et son absence de coût de licence par utilisateur. La solution sera déployée sur une base Debian 13 et connectée à l'Active Directory via LDAP. Cela permettra aux agents d'utiliser des softphones sur leurs postes Windows 11 ou via le VPN pour passer des appels critiques en situation de crise.

5.2. Solution Softphone : Linphone

Critères	Linphone	MicroSIP	Zoiper
Origine	Française	? (Communautaire)	Suisse
Licence	Gratuit	Gratuit	Freemium
Fonctionnalités	Appel / Vidéo / Chat	Appel / Chat	Appel / Vidéo / Chat
Compatibilité	Multi-plateforme	Windows uniquement	Multi-plateforme

Chiffrement	Inclus	Inclus	Version payante
Choix	✅	❌	❌

Nous avons sélectionné Linphone pour sa parfaite synergie avec l'infrastructure XiVO, garantissant une solution de communication 100 % souveraine et sans coût de licence. Ce softphone français a été retenu pour sa capacité à sécuriser nos échanges critiques via les protocoles SRTP, ZRTP et SIPS, tout en offrant une compatibilité multi-plateforme native. Son intégration fluide avec XiVO permet de déployer rapidement les services de voix, vidéo et chat sur les postes Windows 11 de nos agents, assurant ainsi une continuité de service optimale en situation de crise.

5.3. Solution NG-FireWall / Routeur : PfSense

L'infrastructure de la Sécurité Civile nécessite une barrière de sécurité robuste capable de gérer deux accès Internet en haute disponibilité (HA) et d'assurer des tunnels chiffrés pour les agents mobiles.

Critères	PfSense	OPNsense	Cisco ASA
Origine	Etats-Unis	Pays-Bas	Etats-Unis
Maintenance	Mises à jour mensuelles	Bi-annuelle	Dépend du contrat
Coût Licence	Gratuit	Gratuit	Boitier + Abonnement
Technique HA	CARP	CARP	FHRP : HSRP/GLBP
Pérénnité 2026	Standard mondial	Croissante	Cycle de vie rigide
Choix	✅	❌	❌

Nous avons retenu pfSense pour sa gestion native de la haute disponibilité via le protocole CARP, garantissant la continuité des services du COD en cas de défaillance. Ce choix nous permet de respecter l'exigence OpenVPN du cahier des charges tout en intégrant Wireguard pour optimiser les performances de nos flux. Déployée en

cluster sur deux machines virtuelles avec synchronisation des tables d'états, la solution assure un basculement totalement transparent, indispensable à la résilience de notre infrastructure critique.

5.4. Solution VPN : Accès Distant (OpenVPN RoadWarrior)

L'accès distant sécurisé est le pilier de la mobilité pour la Sécurité Civile. Il permet d'étendre le réseau local de la Préfecture jusqu'au terminal de l'agent de terrain via un tunnel chiffré traversant Internet.

Critères	OpenVPN	WireGuard	IPsec (IKEv2)
Origine	Open Source	Open Source	Standard Industriel
Performance	Très bonne	Ultra-rapide	Très bonne
Sécurité	Robuste	Robuste	Robuste
Facilité d'usage	Client tiers requis	Client tiers requis	Natif
Choix	✅	❌	❌

Nous avons maintenu OpenVPN comme solution principale pour l'accès « Road Warrior », conformément aux exigences explicites du cahier des charges de l'AP4. Au-delà de cette conformité, ce choix se justifie par la stabilité éprouvée du protocole sur les réseaux mobiles (4G/5G), garantissant une connectivité résiliente pour nos agents lors d'interventions en conditions instables.

5.5. Solution Annuaire : Windows Server 2022

Le centre opérationnel doit centraliser l'authentification des 10 utilisateurs simultanés et appliquer des stratégies de sécurité strictes sur les postes Windows 11 Pro.

Critères	Windows Server (AD DS)	Samba 4 (Linux)
Origine	Etats-Unis	Open Source (Tranquil IT)
Maintenance	Critique	Communautaire
Coût Licence	~850$ (Std 16-core)	Gratuit
CALs (10 users)	~400$	Gratuit
Replication	Native	Partielle/Complexe
Choix	✅	❌

Le choix de Windows Server 2022 est dicté par l'imposition du cahier des charges qui demande un environnement Windows pour les serveurs et les postes clients. Nous avons opté pour une architecture à deux contrôleurs de domaine (Principal et Secondaire) afin d'assurer la continuité du service d'authentification.
L'implémentation se fera via le rôle AD DS pour permettre un couplage direct avec la messagerie Exchange et l'IpBX XiVO

5.6. Solution de Supervision : Zabbix

Pour garantir la qualité de service, les administrateurs doivent être alertés immédiatement en cas de panne d'un équipement critique.

Critères	Zabbix	Prometheus	Centreon
Origine	Lettonie	Etats-Unis	France
Pérennité/ Maintenance	Version LTS	Régulière	Version LTS
Architecture	Tout-en-un (SQL/AGENT/SNMP)	Base de données de séries temporelles	Basé sur des moteurs de scripts

Méthode de collecte	Pull & Push (Agent / SNMP)	Pull (Via HTTP / Exporters)	Pull (SNMP / Plugins)
Visualisation	Tableaux de bord & Maps natifs	Nécessite souvent Grafana	Vues personnalisées
Alerting	Natif	Nécessite Alertmanager	Natif
Coût Licence	Gratuit	Gratuit	Freemium (Limité à 100 hôtes)
Choix	✅	❌	❌

Nous avons retenu Zabbix comme solution « tout-en-un » pour répondre précisément aux besoins de supervision de nos routeurs pfSense et de nos serveurs Windows. Nous pourrons superviser les équipements critiques de manière efficace à l'aide de l'ICMP. Enfin, l'intégration avec le serveur de messagerie Exchange permet de notifier les administrateurs en temps réel, assurant une réactivité optimale face aux incidents de l'infrastructure.

5.7. Solution de Messagerie : Exchange

La communication par courriel est vitale pour l'envoi des rapports d'intervention. Elle doit être intégrée à l'annuaire pour faciliter la gestion des comptes.

Critères	Microsoft Exchange	MDaemon
Origine	Etats-Unis	Etats-Unis
Pérennité / Maintenance	Mises à jour critique	Active
Intégration AD	Native	Connecteur LDAP
Haute Disponibilité	Haute Disponibilité	Réplication de fichiers
Coût	~900 $ + CALs	~450 $
Choix	✅	❌

Nous avons sélectionné Microsoft Exchange Server afin d'offrir une expérience utilisateur fluide et une synchronisation optimale des calendriers et contacts via ActiveSync. Ce choix garantit une interopérabilité maximale avec notre infrastructure Active Directory, permettant aux agents sur le terrain de rester parfaitement coordonnés avec le COD en toute circonstance.

6. Infrastructure du système d'information

6.1. Tableau récapitulatif

Pour structurer notre déploiement et faciliter le mapping de nos machines virtuelles, nous avons synthétisé l'ensemble de l'infrastructure cible dans le tableau récapitulatif suivant :

	VM1	VM2
Nom	SECCIV-RTE-01	SECCIV-RTE-02
Rôles	Routeur / NG-FIREWALL / HA / OpenVPN	Routeur / NG-FIREWALL / HA / OpenVPN
OS	FreeBSD pfSense	FreeBSD pfSense
Version	2.7.2	2.7.2
IP/CIDR	LAN : 192.168.1.1/24 VIP LAN : 192.168.1.254/24 DMZ : 172.20.20.1/24 VIP DMZ : 172.20.20.254 WAN : DHCP PFSYNC : 192.168.2.1/30	LAN : 192.168.1.2/24 VIP LAN : 192.168.1.254/24 DMZ : 172.20.20.2/24 VIP DMZ : 172.20.20.254 WAN : DHCP PFSYNC : 192.168.2.2/30
Passerelle		
Coeurs	1	1
Mémoire	512 MiB	512 MiB
Stockage	20 Go	20 Go

	VM3	VM4
Nom	SECCIV-SRVW01	SECCIV-SRVW02
Rôles	AD / DNS / DHCP / RADIUS	AD / DNS / DHCP / RADIUS
OS	Windows Server 2022	Windows Server 2022
Version	21H2	21H2
IP/CIDR	192.168.1.10/24	192.168.1.11/24
Passerelle	192.168.1.254	192.168.1.254
Coeurs	2	2

Mémoire	8 GiB	8 GiB
Stockage	60 Go	60 Go

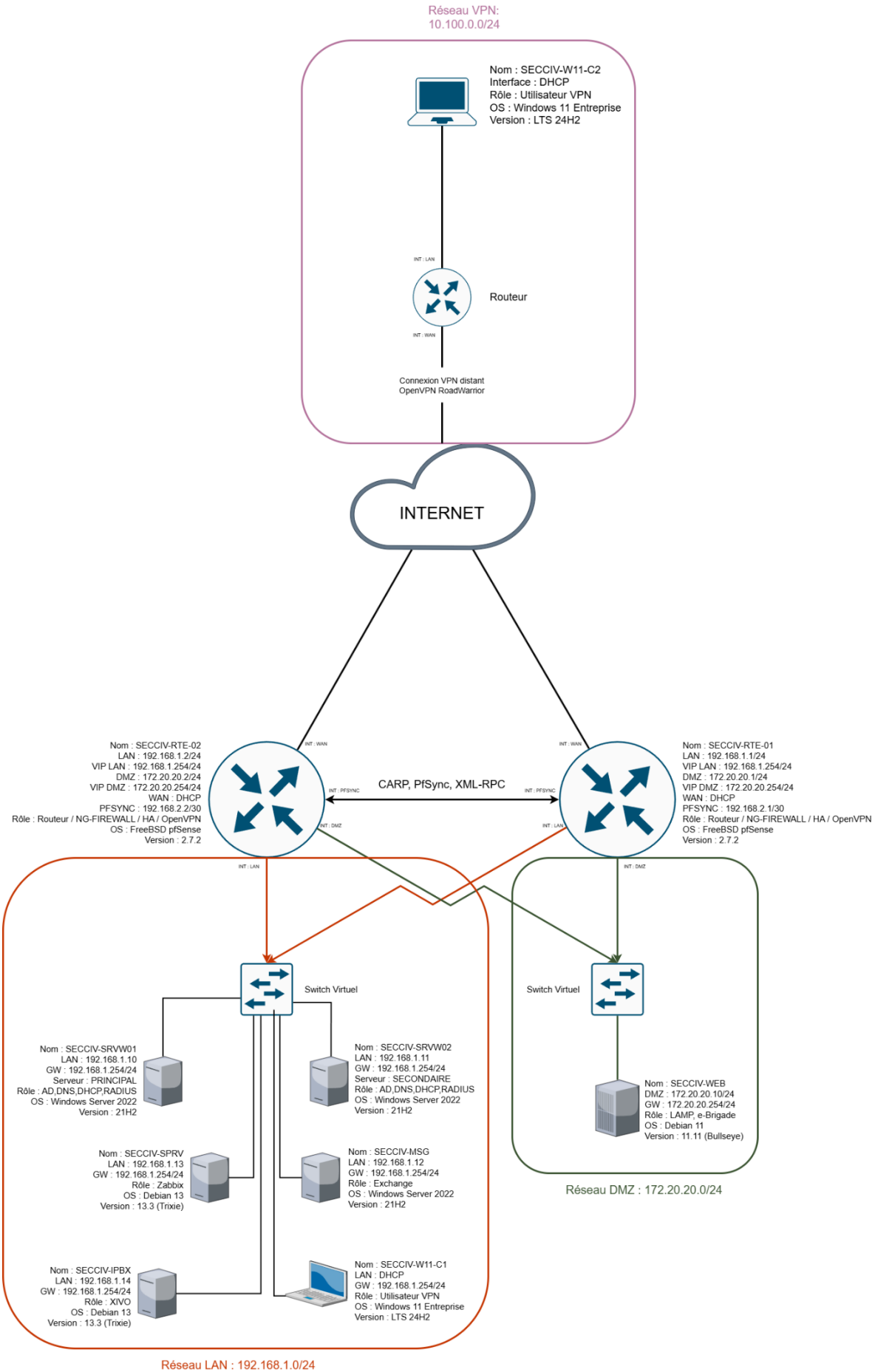
	VM5	VM6
Nom	SECCIV-MSG	SECCIV-SPRV
Rôles	Messagerie Exchange	Zabbix
OS	Windows Server 2022	Debian 13
Version	21H2	13.3 (Trixie)
IP/CIDR	192.168.1.12/24	192.168.1.13/24
Passerelle	192.168.1.254	192.168.1.254
Coeurs	2	1
Mémoire	16 GiB	2 GiB
Stockage	120 Go	40 Go

	VM7	VM8
Nom	SECCIV-IPBX	SECCIV-WEB
Rôles	Xivo	e-Brigade
OS	Debian 13	Debian 11
Version	13.3 (Trixie)	11.11 (Bullseye)
IP/CIDR	192.168.1.14/24	172.20.20.254/24
Passerelle	192.168.1.254	192.168.1.254
Coeurs	1	1
Mémoire	4 GiB	4 GiB
Stockage	40 Go	20 Go

	VM9	VM10
Nom	SECCIV-W11-C1	SECCIV-W11-C2
Rôles	Client	Client VPN
OS	Windows 11 Entreprise	Windows 11 Entreprise
Version	LTS 24H2	LTS 24H2
IP/CIDR	DHCP	DHCP
Passerelle	192.168.1.254	10.100.255.254/16
Coeurs	1	1
Mémoire	4 GiB	4 GiB
Stockage	60 Go	60 Go

6.2. Schéma réseau

Voici l'architecture réseau conçue pour répondre aux impératifs de continuité de service et de résilience de la Sécurité Civile.


Réseau VPN:
10.100.0.0/24
Nom : SECCIV-W11-C2
Interface : DHCP
Rôle : Utilisateur VPN
OS : Windows 11 Entreprise
Version : LTS 24H2
INT : LAN
Routeur
INT : WAN
Connexion VPN distant
OpenVPN RoadWarrior
INTERNET
Nom : SECCIV-RTE-02
LAN : 192.168.1.2/24
VIP LAN : 192.168.1.254/24
DMZ : 172.20.20.2/24
VIP DMZ : 172.20.20.254/24
WAN : DHCP
PFSYNC : 192.168.2.2/30
Rôle : Routeur / NG-FIREWALL / HA / OpenVPN
OS : FreeBSD pfSense
Version : 2.7.2
INT : WAN
INT : PFSYNC
CARP, PfSync, XML-RPC
INT : DMZ
INT : LAN
Nom : SECCIV-RTE-01
LAN : 192.168.1.1/24
VIP LAN : 192.168.1.254/24
DMZ : 172.20.20.1/24
VIP DMZ : 172.20.20.254/24
WAN : DHCP
PFSYNC : 192.168.2.1/30
Rôle : Routeur / NG-FIREWALL / HA / OpenVPN
OS : FreeBSD pfSense
Version : 2.7.2
Switch Virtuel
Switch Virtuel
Nom : SECCIV-SRVW01
LAN : 192.168.1.10
GW : 192.168.1.254/24
Serveur : PRINCIPAL
Rôle : AD,DNS,DHCP,RADIUS
OS : Windows Server 2022
Version : 21H2
Nom : SECCIV-SRVW02
LAN : 192.168.1.11
GW : 192.168.1.254/24
Serveur : SECONDAIRE
Rôle : AD,DNS,DHCP,RADIUS
OS : Windows Server 2022
Version : 21H2
Nom : SECCIV-SPRV
LAN : 192.168.1.13
GW : 192.168.1.254/24
Rôle : Zabbix
OS : Debian 13
Version : 13.3 (Trixie)
Nom : SECCIV-MSG
LAN : 192.168.1.12
GW : 192.168.1.254/24
Rôle : Exchange
OS : Windows Server 2022
Version : 21H2
Nom : SECCIV-IPBX
LAN : 192.168.1.14
GW : 192.168.1.254/24
Rôle : XIVO
OS : Debian 13
Version : 13.3 (Trixie)
Nom : SECCIV-W11-C1
LAN : DHCP
GW : 192.168.1.254/24
Rôle : Utilisateur VPN
OS : Windows 11 Entreprise
Version : LTS 24H2
Nom : SECCIV-WEB
DMZ : 172.20.20.10/24
GW : 172.20.20.254/24
Rôle : LAMP, e-Brigade
OS : Debian 11
Version : 11.11 (Bullseye)
Réseau LAN : 192.168.1.0/24
Réseau DMZ : 172.20.20.0/24

6.3. Matrice des flux

La sécurisation de cette architecture repose sur une matrice des flux exhaustive, indispensable pour définir les règles d'interconnexion entre les services et appliquer des autorisations protocolaires strictes sur chaque interface (Source et Destination).

Interface WAN :

Protocole	Zone Source	Zone Destination	Source	Destination	Port	NAT	Deny/Pass	Description
UDP	*	WAN	*	*	1194 (OpenVPN)	❌	Pass	Autorise la connexion au OpenVPN.
TCP	WAN	DMZ	*	SECCIV-WEB	80 (HTTP)	✅	Pass	Accès HTTP vers e-Brigade (via règle NAT).
TCP	WAN	DMZ	*	SECCIV-WEB	443 (HTTPS)	✅	Pass	Accès HTTPS vers e-Brigade (via règle NAT).
ICMP	*	WAN	*	*	*	❌	Pass	Autorise le "Ping" depuis l'extérieur (utile pour les tests).
TCP/UDP	*	*	*	*	*	❌	Deny	Règle Deny All : Bloque tout le reste par défaut.

Interface DMZ :

Protocole	Zone Source	Zone Destination	Source	Destination	Port	NAT	Deny/Pass	Description

TCP/UDP	*	*	*	*	*	❌	Deny	Règle Deny All : Bloque tout le reste par défaut.

Interface OpenVPN :

Protocole	Zone Source	Zone Destination	Source	Destination	Port	NAT	Deny/Pass	Description
TCP/UDP	OpenVPN	LAN	OpenVPN subnet	SECCIV-SRVW01, SECCIV-SRVW02	53 (DNS)	❌	Pass	Résolution des noms de serveurs internes
TCP	OpenVPN	LAN	OpenVPN subnet	SECCIV-SRVW01, SECCIV-SRVW02	389 (LDAP)	❌	Pass	Authentification sécurisée et recherche d'objets dans l'annuaire Active Directory.
TCP	OpenVPN	LAN	OpenVPN subnet	SECCIV-SRVW01, SECCIV-SRVW02	3268 (Global catalog)	❌	Pass	Permet aux clients de trouver rapidement des objets dans l'ensemble de la forêt Active Directory.
TCP	OpenVPN	LAN	OpenVPN subnet	SECCIV-SRVW01, SECCIV-SRVW02	88 (Kerberos)	❌	Pass	Assure l'authentification sécurisée et la délivrance des tickets de session pour les utilisateurs du domaine
TCP	OpenVPN	LAN	OpenVPN subnet	SECCIV-SRVW01, SECCIV-SRVW02	135 (Remote Procedure Call)	❌	Pass	Gestion des services Windows distants et application des stratégies de groupe (GPO).

TCP	OpenVPN	LAN	OpenVPN subnet	SECCIV-SRVW01, SECCIV-SRVW02	123 (NTP)	❌	Pass	Synchronisation horaire indispensable pour la validité des tickets d'authentification
TCP	OpenVPN	LAN	OpenVPN subnet	SECCIV-SRVW01, SECCIV-SRVW02	445 (SMB)	❌	Pass	Accès sécurisé aux dossiers et fichiers partagés du réseau local.
TCP	OpenVPN	LAN	OpenVPN subnet	SECCIV-SRVW01, SECCIV-SRVW02	49152-65535 (Randomly allocated high TCP ports)	❌	Pass	Gestion des services Windows distants et application des stratégies de groupe (GPO).
TCP	OpenVPN	LAN	OpenVPN subnet	SECCIV-MSG	25 (SMTP)	❌	Pass	Envoi et consultation des courriels via le serveur Exchange.
TCP	OpenVPN	LAN	OpenVPN subnet	SECCIV-MSG	143 (IMAP)	❌	Pass	Envoi et consultation des courriels via le serveur Exchange.
UDP	OpenVPN	LAN	OpenVPN subnet	SECCIV-IPBX	5060 (SIP)	❌	Pass	Signalisation (SIP)
UDP	OpenVPN	LAN	OpenVPN subnet	SECCIV-IPBX	10000 - 20000 (RTP)	❌	Pass	Transport de la voix (RTP) pour la téléphonie VoIP Linphone.
TCP	OpenVPN	DMZ	OpenVPN subnet	SECCIV-WEB	80 (HTTP)	❌	Pass	Consultation de l'application métier e-Brigade hébergée en zone DMZ.
TCP	OpenVPN	DMZ	OpenVPN subnet	SECCIV-WEB	443 (HTTPS)	❌	Pass	Consultation de l'application métier e-Brigade hébergée en zone DMZ.
ICMP	OpenVPN	*	OpenVPN subnet	*	*	❌	Pass	Autorise les tests de connectivité basiques vers toutes les zones pour faciliter le

								diagnostic réseau par l'administrateur.
TCP/UDP	*	*	*	*	*	❌	Deny	Règle Deny All : Bloque tout le reste par défaut.

Interface LAN :

Protocole	Zone Source	Zone Destination	Source	Destination	Port	NAT	Deny/Pass	Description
TCP/UDP	LAN	LAN	LAN subnet	SECCIV-SRVW01, SECCIV-SRVW02	53 (DNS)	❌	Pass	Résolution des noms de serveurs internes
TCP	LAN	LAN	LAN subnet	SECCIV-SRVW01, SECCIV-SRVW02	389 (LDAP)	❌	Pass	Authentification sécurisée et recherche d'objets dans l'annuaire Active Directory.
TCP	LAN	LAN	LAN subnet	SECCIV-SRVW01, SECCIV-SRVW02	3268 (Global catalog)	❌	Pass	Permet aux clients de trouver rapidement des objets dans l'ensemble de la forêt Active Directory.
TCP	LAN	LAN	LAN subnet	SECCIV-SRVW01, SECCIV-SRVW02	88 (Kerberos)	❌	Pass	Assure l'authentification sécurisée et la délivrance des tickets de session pour les utilisateurs du domaine
TCP	LAN	LAN	LAN subnet	SECCIV-SRVW01, SECCIV-SRVW02	135 (Remote Procedure Call)	❌	Pass	Gestion des services Windows distants et application des stratégies de groupe (GPO).
UDP	LAN	LAN	LAN subnet	SECCIV-SRVW01, SECCIV-SRVW02	123 (NTP)	❌	Pass	Synchronisation horaire indispensable pour la validité des tickets d'authentification

TCP	LAN	LAN	LAN subnet	SECCIV-SRVW01, SECCIV-SRVW02	445 (SMB)	❌	Pass	Accès sécurisé aux dossiers et fichiers partagés du réseau local.
TCP	LAN	LAN	LAN subnet	SECCIV-SRVW01, SECCIV-SRVW02	49152-65535 (Randomly allocated high TCP ports)	❌	Pass	Gestion des services Windows distants et application des stratégies de groupe (GPO).
TCP	LAN	LAN	LAN subnet	SECCIV-MSG	25 (SMTP)	❌	Pass	Envoi et consultation des courriels via le serveur Exchange.
TCP	LAN	LAN	LAN subnet	SECCIV-MSG	143 (IMAP)	❌	Pass	Envoi et consultation des courriels via le serveur Exchange.
UDP	LAN	LAN	LAN subnet	SECCIV-IPBX	5060 (SIP)	❌	Pass	Signalisation (SIP)
UDP	LAN	LAN	LAN subnet	SECCIV-IPBX	10000 - 20000 (RTP)	❌	Pass	Transport de la voix (RTP) pour la téléphonie VoIP Linphone.
TCP	LAN	LAN	LAN subnet	SECCIV-MSG	443 (HTTPS)	❌	Pass	Consultation de l'application Exchange ECP.
TCP	LAN	LAN	LAN subnet	SECCIV-SPRV	443 (HTTPS)	❌	Pass	Consultation de l'application de supervision.
TCP	LAN	DMZ	LAN subnet	SECCIV-WEB	80 (HTTP)	❌	Pass	Consultation de l'application métier e-Brigade hébergée en zone DMZ.
TCP	LAN	DMZ	LAN subnet	SECCIV-WEB	443 (HTTPS)	❌	Pass	Consultation de l'application métier e-Brigade hébergée en zone DMZ.
ICMP	LAN	*	LAN subnet	*	*	❌	Pass	Autorise les tests de connectivité basiques vers toutes les zones pour faciliter le diagnostic réseau par l'administrateur.
TCP/UDP	*	*	*	*	*	❌	Deny	Règle Deny All : Bloque tout le reste par défaut.

7. Etude budgétaire

7.1. Devis externe

Ce chiffrage externe englobe l'acquisition de matériels serveurs et réseaux de gamme professionnelle, les licences logicielles conformes aux besoins des 10 utilisateurs simultanés, ainsi qu'une prestation de services évaluée à 280 heures de travail technique. Cet investissement assure au SIDPC une infrastructure souveraine, capable de supporter des situations de crise majeures tout en offrant une mobilité sécurisée aux agents de terrain.

CONNECT
Arman ABGARYAN
17 Rue Brooklyn67000 France
Siren 789251394
Mail arman@connect-info.fr

Devis N°D-495768
Émis le 25/02/2026 Validité 27/03/2026

ASS NAT CHEFS SERV INTERM DEFENSE PROTECTION CIVILE (SIDPC)
Direction De La Securite Civile 5 Place De La République67000 France
Siren 493084750

Prestation / Service / Produit	Quantité	Prix HT	Prix TTC	TVA
PARTIE 1 : RÉSEAU & SÉCURITÉ (PHYSIQUE)	01 unité	0.00€	0.00€	0%
Netgate 4100 BASE (ou équivalent mini-PC 4x Intel i226) Routeur Pare-feu HA	02 unité	1300.00€	1560.00€	20%
Aruba Instant On 1930 (24 Ports Gigabit) Switchs de Distribution	02 unité	560.00€	672.00€	20%
PARTIE 2 : SERVEUR DE VIRTUALISATION	01 unité	0.00€	0.00€	0%
Dell PowerEdge R450 (12C, 64Go RAM, RAID 1 SSD) Serveur d'Applications	01 unité	3950.00€	4740.00€	20%
APC Smart-UPS 1000VA (Rackable) Onduleur (Protection)	01 unité	550.00€	660.00€	20%
PARTIE 3 : LOGICIELS & LICENCES	01 unité	0.00€	0.00€	0%
Licence Standard (16-Core) Windows Server 2022	02 unité	1700.00€	2040.00€	20%
Licence Standard MS Exchange Server	01 unité	750.00€	900.00€	20%
Accès CALs (Pack 10) Windows + Exchange CALs	02 unité	900.00€	1080.00€	20%
PARTIE 4 : PRESTATIONS (280 HEURES)	01 unité	0.00€	0.00€	0%
Installation, Config HA, VPN, Exchange (60€/h) Main d'œuvre Ingénierie	280 heure	16800.00€	20160.00€	20%

Total HT	**26510.00€**
Total TTC	**31812.00€**

Montant TVA	**5302.00€**

Conditions

Paiement à 30 jours. Pas d'escompte pour règlement anticipé.

En cas de retard de paiement, indemnité forfaitaire légale pour frais de recouvrement : 40€.

Les pénalités de retard correspondent à : 2.7% du montant TTC.

Dispense d'immatriculation au RCS et au répertoire des métiers.

Le montant global de cette infrastructure est estimé à 31 812,00 € TTC, incluant l'acquisition des équipements, les licences logicielles ainsi que 280 heures de prestations d'ingénierie et de déploiement.

7.2. Devis interne

Ce chiffrage interne détaille la mobilisation des ressources propres du SIDSIC pour la réalisation du projet. Il intègre l'acquisition des équipements serveurs et réseaux nécessaires, les licences logicielles obligatoires pour les 10 utilisateurs simultanés, ainsi que la valorisation de 280 heures de travail technique effectuées par les agents du service. Cette approche permet de rationaliser les coûts pour la Préfecture tout en garantissant le déploiement d'une infrastructure souveraine et résiliente, parfaitement adaptée aux missions critiques du Centre Opérationnel Départemental (COD).

ASS NAT CHEFS SERV INTERM DEFENSE PROTECTION CIVILE (SIDPC)

Devis N°D-495768

Émis le 25/02/2026 Validité 27/03/2026

Arman Abgaryan
Direction De La Securite Civile 5 Place De La République67000 France
Siren 493084750
Mail arman@sidpc.com

ASS NAT CHEFS SERV INTERM DEFENSE PROTECTION CIVILE (SIDPC)

Direction De La Securite Civile 5 Place De La République67000 France
Siren 493084750

Prestation / Service / Produit	Quantité	Prix HT	Prix TTC	TVA
Matériel Réseau 2 Routeurs Physiques + 2 Switchs	01 unité	1860.00€	1860.00€	0%
Matériel Serveur Dell R450 + Onduleur	01 unité	4500.00€	4500.00€	0%
Licences Pack Microsoft (Server + Exchange + CALs)	01 unité	3350.00€	3350.00€	0%
Main d'œuvre Temps agent SIDSIC (280h @ 45€/h)	280 heure	12600.00€	12600.00€	0%

Total HT	**22310.00€**
Total TTC	**22310.00€**
Montant TVA	**0.00€**

Conditions

Paiement à 30 jours. Pas d'escompte pour règlement anticipé.

En cas de retard de paiement, indemnité forfaitaire légale pour frais de recouvrement : 40€.

Les pénalités de retard correspondent à : 2.7% du montant TTC.

Dispense d'immatriculation au RCS et au répertoire des métiers.

Le coût opérationnel interne est estimé à 22310,00 €, incluant l'investissement matériel et logiciel ainsi que les 280 heures de prestations d'ingénierie réalisées par les ressources internes du SIDSIC. Cette solution permet d'atteindre les objectifs de haute disponibilité et de mobilité sécurisée à un coût optimisé pour l'administration.

7.3. Le choix du matériel

Pour garantir la disponibilité du Centre Opérationnel Départemental (COD), nous avons segmenté la sécurité périmétrale du reste de l'infrastructure.

Les Routeurs Netgate 4100 (Sécurité & VPN)

Le choix de boîtiers physiques dédiés plutôt qu'une virtualisation totale permet d'isoler la fonction de passerelle.

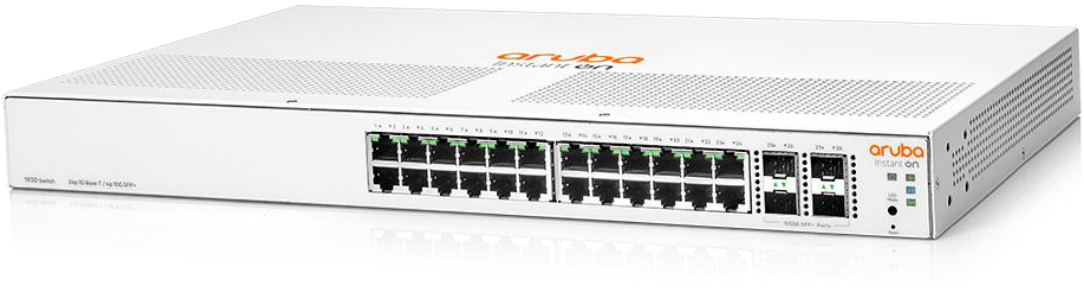
- Rôle : Ils gèrent le tunnel OpenVPN Road Warrior pour les agents mobiles et le filtrage de pare-feu.
- Avantage HA : En cas de défaillance du routeur maître, le protocole CARP bascule le trafic sur le second boîtier en moins d'une seconde.

Le Serveur Dell PowerEdge R450 :

Ce serveur unique hébergera toutes les machines virtuelles.

- Mémoire vive (64 Go) : Dimensionnée pour supporter les 16 Go de Microsoft Exchange et les 16 Go cumulés des deux contrôleurs de domaine Active Directory.
- Stockage RAID 1 : Assure la continuité de service des bases de données de messagerie et de la main courante e-Brigade même si un disque dur tombe en panne.

Les Switchs Aruba 1930 :



Ce switch nous permettra de faire du :

- LACP (Agrégation de liens) : Sécurise et double la bande passante entre le serveur Dell et le réseau.
- QoS (Qualité de Service) : Priorise le flux vocal XiVO pour garantir des appels fluides en situation de crise.
- Spanning Tree (STP) : Évite les boucles réseau critiques lors de l'utilisation de plusieurs liens redondants.
- Port Security : Bloque les accès physiques non autorisés sur les prises réseau du COD pour protéger l'infrastructure.

L'Onduleur APC Smart-UPS 1000VA :

Mission : Protéger le matériel contre les microcoupures et garantir une autonomie suffisante lors d'une panne de courant à la Préfecture pour que la cellule de crise puisse basculer sur des procédures de secours.

8. La planification des tâches

8.1. Gantt

La conduite de ce projet de modernisation s'articule autour d'un calendrier rigoureux de 280 heures, structuré en cinq phases clés allant de l'audit initial à la validation technique finale. Ce diagramme de Gantt garantit une progression logique des déploiements, en priorisant d'abord la résilience de l'infrastructure réseau (pfSense HA) avant l'intégration des services applicatifs critiques comme la messagerie Exchange ou la téléphonie XiVO. Cette planification stratégique permet au SIDSIC de respecter les échéances impératives de livraison tout en réservant un temps substantiel aux phases de tests et de recettage, indispensables pour garantir la fiabilité du système en situation de crise réelle.

Tâches

Nom	Date de début	Date de fin	Durée	ID
P0 : Début / Fin	23/01/2026	16/04/2026	60	23
P1 : ANALYSE	23/01/2026	06/02/2026	11	1
Lancement du projet et analyse du CdC SIDPC	23/01/2026	23/01/2026	1	3
Étude comparative (pfSense vs IPsec, XiVO vs 3CX)	26/01/2026	05/02/2026	9	4
Validation des solutions avec le formateur	06/02/2026	06/02/2026	1	5
P2 : CONCEPTION	09/02/2026	26/02/2026	14	6
Plan d'adressage IP (LAN, DMZ, VPN)	09/02/2026	12/02/2026	4	8
Rédaction des devis interne et externe	13/02/2026	19/02/2026	5	9
Finalisation et mise en page du LIVRABLE 1	20/02/2026	26/02/2026	5	10
Dépôt du dossier du Livrable 1	27/02/2026	27/02/2026	0	11
P3 : RÉALISATION	06/03/2026	20/03/2026	11	12
Soutenance Phase 1 : Analyse & Planification	06/03/2026	06/03/2026	0	13
Setup pfSense HA (CARP) et OpenVPN RoadWarrior	09/03/2026	12/03/2026	4	14
Déploiement Active Directory (SRVW01 & SRVW02)	13/03/2026	20/03/2026	6	15
P4 : INTÉGRATION	23/03/2026	10/04/2026	15	16
Setup Exchange (MSG) et XiVO (IPBX)	23/03/2026	30/03/2026	6	17
eBrigade (WEB) et Supervision Zabbix (SPRV)	31/03/2026	03/04/2026	4	18
Tests de basculement HA et rédaction du LIVRABLE 2	06/04/2026	10/04/2026	5	19
P5 : VALIDATION	13/04/2026	16/04/2026	4	20
BTS BLANC E5 : Oral Professionnel	13/04/2026	13/04/2026	0	21
BTS BLANC E6 : Soutenance Technique AP4	17/04/2026	17/04/2026	0	22

Diagramme de Gantt