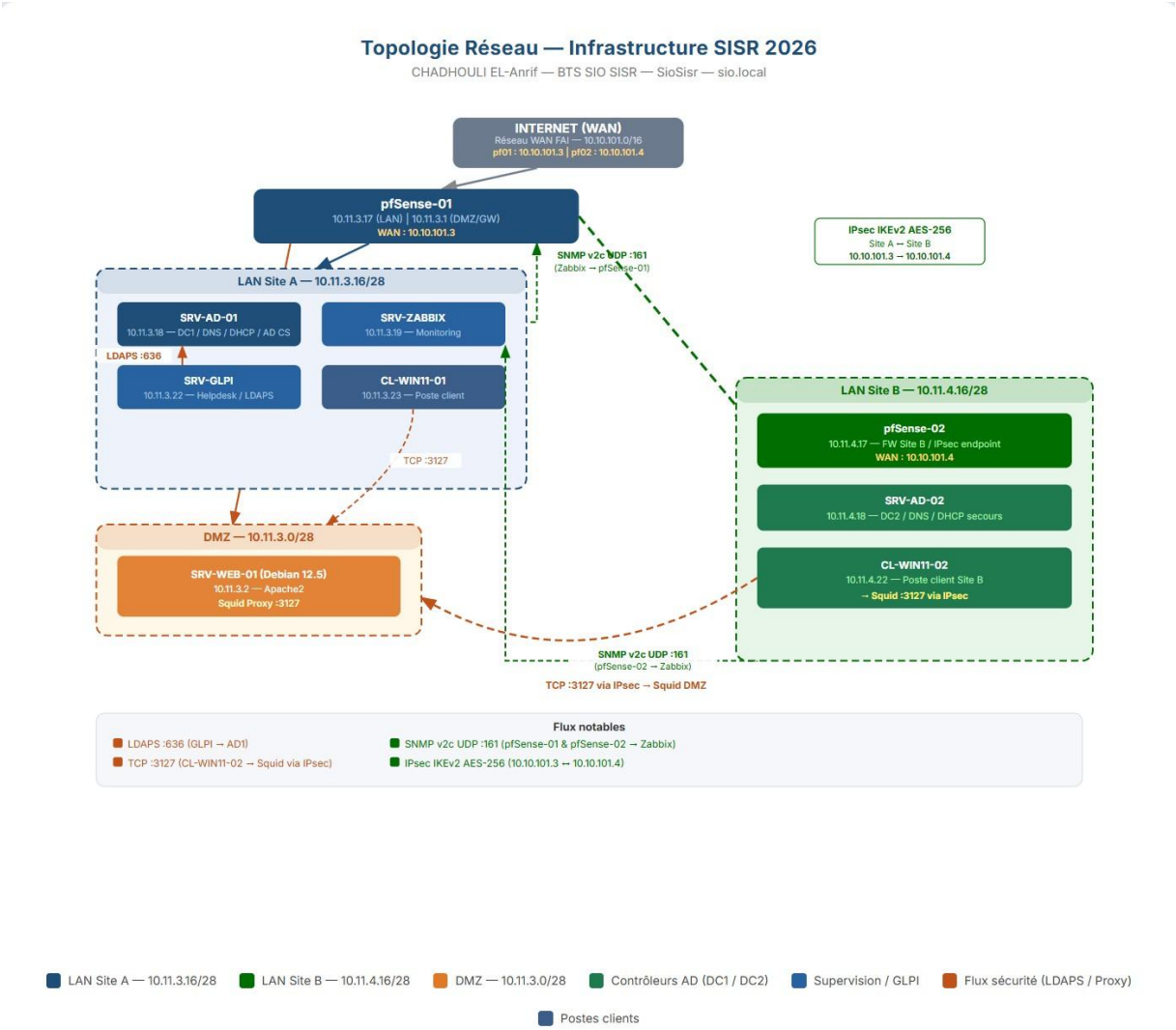
Infrastructure Réseau Bi-Site Sécurisée

Conception, déploiement et supervision d'une architecture multi-site avec filtrage web centralisé, tunnel IPsec AES-256 et supervision temps réel Zabbix

Candidat	**CHADHOULI EL-Anrif**
Établissement	**Campus Mewo, Metz**
Société support	**SioSisr — sio.local**
Formation	**BTS SIO — Option SISR**
Épreuve	**E6 — Session 2026**
Date épreuve	**22 / 04 / 2026**



RÉALISATIONS E6

R1	Infrastructure Bi-Site — pfSense, IPsec IKEv2, DMZ, Proxy Squid

Table des matières

SECTION I

Contexte et objectifs

Analyse de la situation initiale et définition des besoins de la société SioSisr

---

La société **SioSisr** dispose de deux sites géographiques hébergeant 50 collaborateurs répartis entre le Site A (siège) et le Site B (site de secours). À l'état initial, l'infrastructure présentait plusieurs défaillances critiques compromettant la confidentialité des données et la continuité de service.

■ Problème identifié	Impact	Solution déployée
Trafic inter-sites non chiffré	Interception des données sensibles en transit	Tunnel IPsec IKEv2 AES-256
Accès web non contrôlé	Navigation non filtrée, risques de malware et perte de productivité	Proxy Squid + SSL Bumping en DMZ isolée
Absence de DMZ	Services exposés colocalisés avec le LAN critique	Segmentation stricte /28 avec pare-feu inter-zones
Aucune supervision	Pannes non détectées, absence de traçabilité	Zabbix temps réel + alertes e-mail
Authentification LDAP en clair	Credentials exposés sur le réseau (Man-in-the-Middle)	Migration LDAPS port 636 + PKI interne AD CS

■ **Objectif principal :** Déployer une infrastructure bi-site sécurisée, résiliente et supervisée, garantissant la confidentialité des communications (AES-256), le contrôle des accès web (proxy Squid), la séparation des zones réseau (DMZ) et la continuité de service (PRA Active Directory).

SECTION II

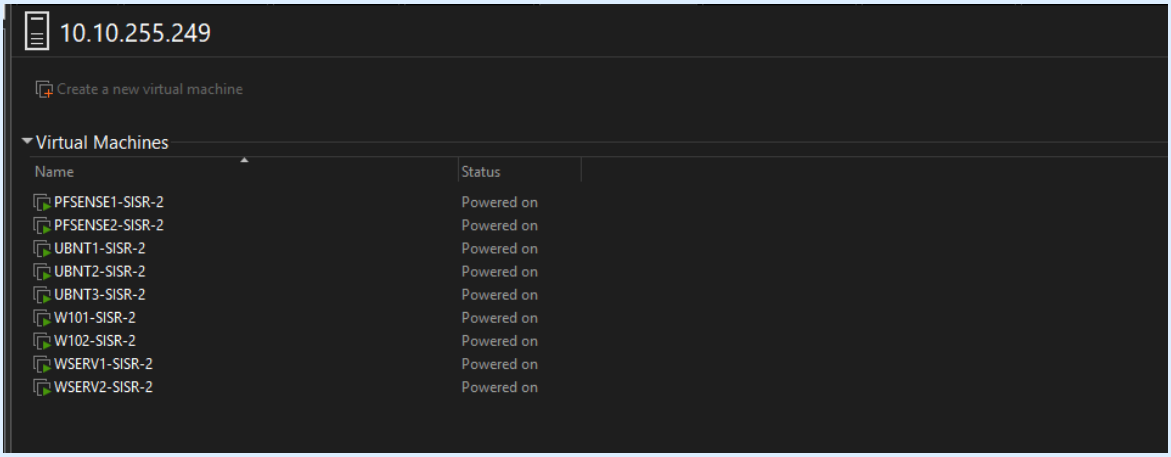
Provisionnement et virtualisation

Hyperviseur VMware ESXi — Cycle de déploiement des machines virtuelles

L'infrastructure repose entièrement sur un **hyperviseur de type 1 VMware ESXi (Bare Metal)** hébergé sur le serveur physique du Campus Mewo. Cette approche élimine la couche d'OS hôte, garantissant des performances maximales et une isolation matérielle stricte entre les VMs. L'administration s'effectue via **VMware vSphere Client**. Chaque VM a été provisionnée selon un cycle standardisé : création vSphere → montage ISO → installation OS → configuration réseau → installation VMware Tools → snapshot initial.

Machine	Rôle	OS	IP	Zone
pfSense-01	Pare-feu / Routeur / VPN Site A	pfSense 2.7.2 CE (FreeBSD)	10.11.3.17 / 10.11.3.1	LAN A / DMZ
SRV-AD-01	DC1 — DNS / DHCP / PKI (AD CS)	Windows Server 2025	10.11.3.18	LAN A
SRV-ZABBIX	Supervision / Monitoring / Alerting	Debian 12.5	10.11.3.19	LAN A
SRV-GLPI	Inventaire ITSM / Helpdesk	Ubuntu 22.04 LTS	10.11.3.22	LAN A
SRV-WEB-01	Apache2 + Proxy Squid (SSL Bump)	Debian 12.5	10.11.3.2	DMZ
CL-WIN11-01	Poste client Site A	Windows 11 Pro 22H2	10.11.3.25 (DHCP)	LAN A
pfSense-02	Pare-feu / Routeur / VPN Site B	pfSense 2.7.2 CE (FreeBSD)	10.11.4.17	LAN B
SRV-AD-02	DC2 — DNS / DHCP secours / PRA	Windows Server 2025	10.11.4.18	LAN B
CL-WIN11-02	Poste client Site B	Windows 11 Pro 22H2	10.11.4.24 (statique)	LAN B

Console VMware — Inventaire des 9 VMs déployées]



Segmentation et adressage réseau

Architecture tri-zones avec masque /28 — isolation totale inter-zones

SECTION III

L'architecture repose sur une **séparation stricte en quatre zones réseau indépendantes**. Le masque **/28 (255.255.255.240)** a été fourni directement par le **Campus Mewo via la configuration de l'environnement ESXi** mis à disposition des étudiants : les plages 10.11.3.0/28 (DMZ), 10.11.3.16/28 (LAN A) et 10.11.4.16/28 (LAN B) étaient pré-attribuées dans l'infrastructure virtuelle de l'établissement. Ce découpage place la DMZ et le LAN A dans deux sous-réseaux distincts du même /24, rendant tout routage direct impossible entre zones.

Zone	Réseau	Passerelle pfSense	Plage hôtes	Rôle
LAN Site A	10.11.3.16/28	10.11.3.17 (pfSense-01)	10.11.3.17 → 10.11.3.30	Serveurs critiques, postes clients
DMZ Site A	10.11.3.0/28	10.11.3.1 (pfSense-01)	10.11.3.1 → 10.11.3.14	Zone isolée — SRV-WEB-01 (Proxy Squid)
LAN Site B	10.11.4.16/28	10.11.4.17 (pfSense-02)	10.11.4.17 → 10.11.4.30	Site de secours — DC2, clients
WAN (transit)	10.10.101.0/16	—	pfSense-01: .3 / pfSense-02: .4	Interconnexion WAN — tunnel IPsec

■ **Justification du masque /28 :** Ce masque a été imposé par le Campus Mewo via l'environnement ESXi mis à disposition des étudiants. Avec 14 adresses hôtes par sous-réseau, il oblige pfSense à disposer de **deux interfaces physiquement distinctes** — une patte DMZ (10.11.3.1) et une patte LAN (10.11.3.17) — forçant tout trafic inter-zones à traverser le moteur de filtrage du pare-feu. Aucun contournement par routage direct n'est possible.

Pare-feu pfSense-01 — Site A (WAN 10.10.101.3)

Politique de sécurité — filtrage stateful séquentiel Top-to-Bottom

---

pfSense constitue la **clé de voûte de la sécurité** de l'infrastructure. Son moteur évalue les règles **séquentiellement du haut vers le bas (Top-to-Bottom)** : dès qu'un paquet correspond à une règle, celle-ci est appliquée et l'évaluation s'arrête.

■ **Principe fondamental :** Les règles spécifiques (Proxy Squid, DNS, Zabbix, administration) sont systématiquement placées **en tête de liste**, avant toute règle générale. Une règle permissive en première position rendrait tous les blocages de sécurité inopérants.

4.1 — Règles LAN (10.11.3.16/28) — Interface opt1

Logique de **moindre privilège** : seuls les flux explicitement autorisés sortent du LAN. La navigation web directe est systématiquement bloquée pour forcer le passage par le proxy Squid centralisé.

#	Règle	Source	Dest.	Port	Proto	Action	Justification professionnelle
1	VPN_SRVAD01_Rep_SiteB	10.11.3.18	10.11.4.16/28	*	IPv4 *	PASS	Réplication AD bidirectionnelle DC1→DC2 via IPsec. Flux prioritaire pour cohérence annuaire.
2	SEC_AD_Bypass_Proxy_HTTPS	10.11.3.18	*	443	IPv4 TCP	PASS	Exempte AD1 du proxy Squid pour requêtes HTTPS (Windows Update, licences).
3	SEC_AD_Bypass_Proxy_HTTP	10.11.3.18	*	80	IPv4 TCP	PASS	Même logique pour HTTP. AD1 ne peut pas utiliser de proxy système.
4	ADM_Accès_WebGUI_SiteB	10.11.4.18	LAN addr	443	IPv4 TCP	PASS	WebGUI pfSense-01 depuis AD2 (Site B) — flux limité à la seule IP de gestion.

SECTION IV

5	ADM_Accès_WebGUI_LAN	LAN subnets	This FW	80-443	IPv4 TCP	PASS	Administration locale pfSense-01 par équipes IT du LAN Site A.
6	SRV_AD_DNS_Query	10.11.3.16/28	10.11.3.18	53	IPv4 UDP	PASS	Résolution DNS interne LAN → AD1. Garantit la résolution du domaine sio.local.
7	SRV_Proxy_Squid_Redirection	LAN subnets	10.11.3.2	3127	IPv4 TCP	PASS	Trafic LAN → Squid (SRV-WEB-01:3127). Règle centrale du filtrage web.
8	SRV_Zabbix_Agent_Data	10.11.3.19	10.11.3.2	10050	IPv4 TCP	PASS	Collecte métriques SRV-WEB-01 (agent Zabbix actif, port 10050).
9	SRV_Zabbix_SNMP_Query	10.11.3.19	This FW	161	IPv4 TCP	PASS	SNMP v2c Zabbix → pfSense-01 (CPU, RAM, bande passante, interfaces).
10	SEC_Block_Direct_WAN_Web	10.11.3.16/28	*	80-443	IPv4 TCP	BLOCK	Bloque navigation directe HTTP/HTTPS — force proxy Squid. [DÉSACTIVÉE — tests]
11	AUTORISATION_FLUX_INTERNES	LAN subnets	*	*	IPv4 *	PASS	Autres protocoles légitimes : ICMP, NTP, SMB, RDP, protocoles métier.
12	SRV_NTP_Time_Sync	*	This FW	123	IPv4 UDP	PASS	Sync NTP interne — cohérence horodatages logs et réplication AD.

Règles LAN pfSense-01 — Firewall → Rules → opt1

Floating | WAN | DMZ | LAN | IPsec

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	1/442 KiB	IPv4 *	10.11.3.18	*	10.11.4.16/28	*	*	none		VPN_SRVAD01_Rep_SiteB	
✓	1/5.09 MiB	IPv4 TCP	10.11.3.18	*	*	443 (HTTPS)	*	none		SEC_AD_Bypass_Proxy_HTTPS	
✓	0/283 KiB	IPv4 TCP	10.11.3.18	*	*	80 (HTTP)	*	none		SEC_AD_Bypass_Proxy_HTTPS	
✓	0/0 B	IPv4 TCP	10.11.4.18	*	LAN address	443 (HTTPS)	*	none		ADM_Accès_WebGUI_SiteB	
✓	0/0 B	IPv4 TCP	LAN subnets	*	This Firewall (self)	80 - 443	*	none		ADM_Accès_WebGUI_LAN	
✓	0/0 B	IPv4 UDP	10.11.3.16/28	*	10.11.3.18	53 (DNS)	*	none		SRV_AD_DNS_Query	
✓	5/126.62 MiB	IPv4 TCP	LAN subnets	*	10.11.3.2	3127	*	none		SRV_Proxy_Squid_Redirection	
✓	70/10.90 MiB	IPv4 TCP	10.11.3.19	*	10.11.3.2	10050	*	none		SRV_Zabbix_Agent_Data	
✓	0/0 B	IPv4 TCP	10.11.3.19	*	This Firewall (self)	161 (SNMP)	*	none		SRV_Zabbix_SNMP_Query	
✗	0/646 KiB	IPv4 TCP	10.11.3.16/28	*	*	80 - 443	*	none		SEC_Block_Direct_WAN_Web	
✓	411/2.57 GiB	IPv4 *	LAN subnets	*	*	*	*	none		AUTORISATION_FLUX_INTERNES_HORS_WEB	
✓	0/0 B	IPv4 UDP	*	123 (NTP)	This Firewall (self)	123 (NTP)	*	none		SRV_NTP_Time_Sync	

Add | Add | Delete | Toggle | Copy | Save | Separator

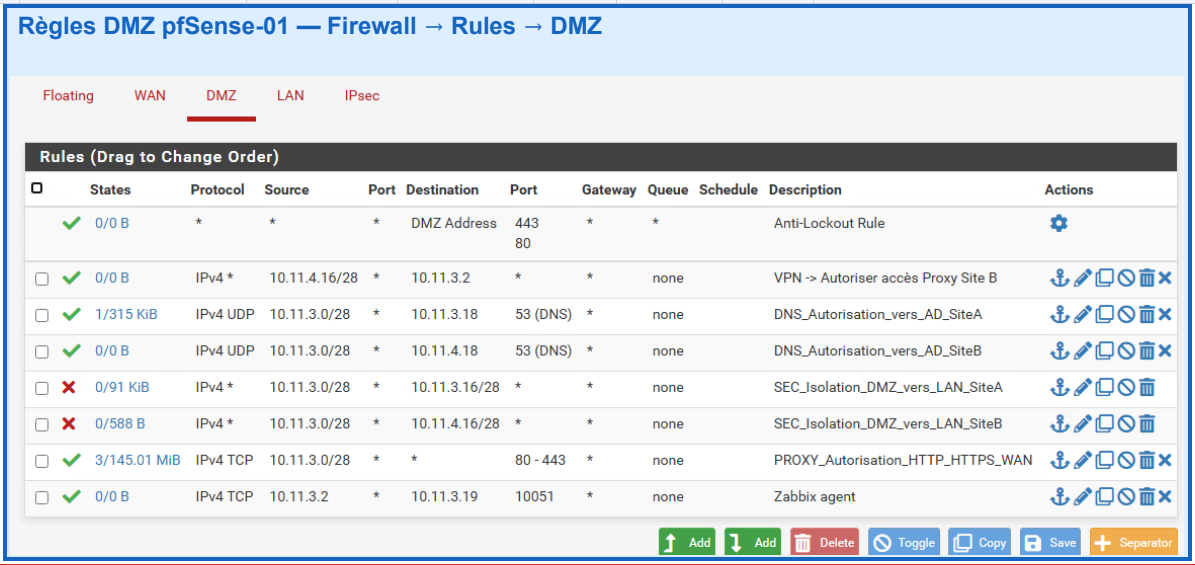
■■ **Note règle #10 SEC_Block_Direct_WAN_Web :** Désactivée temporairement (phase de tests). Elle doit être **réactivée en production** pour bloquer tout contournement du proxy Squid.

4.2 — Règles DMZ (10.11.3.0/28) — Interface DMZ

La DMZ héberge uniquement **SRV-WEB-01** (Apache2 + Proxy Squid, 10.11.3.2). Principe de *défense en profondeur* : SRV-WEB-01 peut sortir sur Internet, mais **aucun flux initié depuis la DMZ vers le LAN n'est autorisé**.

#	Règle	Source	Dest.	Port	Proto	Action	Justification professionnelle
—	Anti-Lockout Rule (système)	*	DMZ Addr	443/80	*	PASS	Règle système pfSense non supprimable. Protège contre le verrouillage accidentel de l'admin.
1	VPN → Autoriser accès Proxy Site B	10.11.4.16/28	10.11.3.2	*	IPv4 *	PASS	Clients Site B → proxy Squid via IPsec. Règle centrale du filtrage web centralisé.
2	DNS_Autorisation_vers_AD_SiteA	10.11.3.0/28	10.11.3.18	53	IPv4 UDP	PASS	SRV-WEB-01 résout noms domaine via AD1. Indispensable pour les ACL Squid.
3	DNS_Autorisation_vers_AD_SiteB	10.11.3.0/28	10.11.4.18	53	IPv4 UDP	PASS	DNS secours vers AD2 — PRA si AD1 indisponible.
4	SEC_Isolation_DMZ_vers_LAN_SiteA	10.11.3.0/28	10.11.3.16/28	*	IPv4 *	BLOCK	Isolation critique DMZ→LAN A. Confine toute compromission de SRV-WEB-01. [DÉSACTIVÉE]
5	SEC_Isolation_DMZ_vers_LAN_SiteB	10.11.3.0/28	10.11.4.16/28	*	IPv4 *	BLOCK	Isolation DMZ→LAN B — empêche mouvement latéral via IPsec. [DÉSACTIVÉE]
6	PROXY_Autorisation_HTTP_HTTPS_WAN	10.11.3.0/28	*	80-443	IPv4 TCP	PASS	Squid sort sur Internet pour relayer les requêtes HTTP/HTTPS des clients.
7	Zabbix agent (10051)	10.11.3.2	10.11.3.19	10051	IPv4 TCP	PASS	Remontée active métriques SRV-WEB-01 → SRV-ZABBIX (mode actif, port 10051).

Règles DMZ pfSense-01 — Firewall → Rules → DMZ



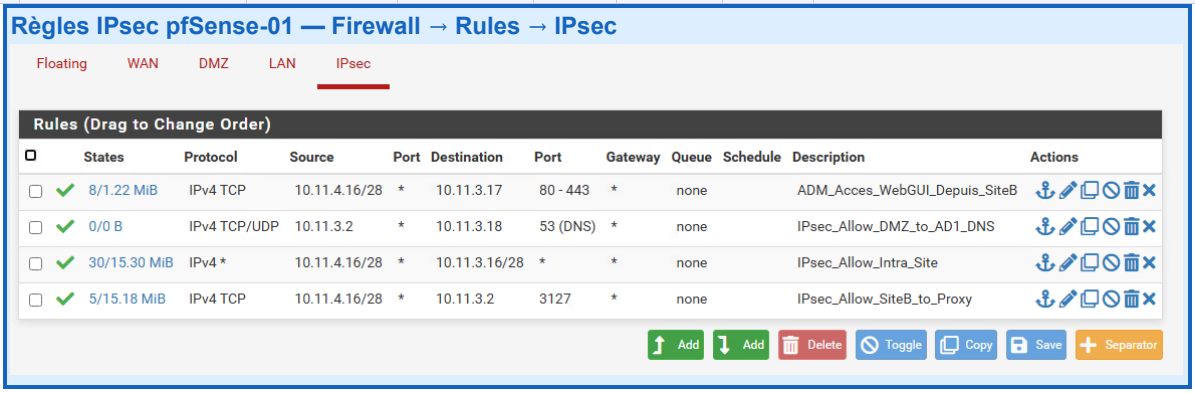
■■ **Note critique — Règles d'isolation DMZ désactivées :** Les règles #4 et #5 constituent le pilier de la défense en profondeur. Elles doivent être **impérativement réactivées en production** pour garantir que la compromission de SRV-WEB-01 ne se propage pas au LAN critique.

4.3 — Règles IPsec — pfSense-01 Site A (enc0)

L'interface IPsec (enc0) de pfSense-01 filtre le trafic **entrant depuis le tunnel Site B → Site A**, déjà déchiffré par la Phase 2 IPsec.

#	Règle	Source	Dest.	Port	Proto	Action	Justification professionnelle
1	ADM_Acces_WebGUI_Depuis_SiteB	10.11.4.16/28	10.11.3.17	80-443	IPv4 TCP	PASS	Administration pfSense-01 depuis LAN Site B via tunnel IPsec.
2	IPsec_Allow_DMZ_to_AD1_DNS	10.11.3.2	10.11.3.18	53	IPv4 TCP/UDP	PASS	SRV-WEB-01 (DMZ) → AD1 résolution DNS sio.local via tunnel.
3	IPsec_Allow_Intra_Site	10.11.4.16/28	10.11.3.16/28	*	IPv4 *	PASS	Flux généraux inter-sites : réplication AD, sauvegardes, Zabbix, ICMP.
4	IPsec_Allow_SiteB_to_Proxy	10.11.4.16/28	10.11.3.2	3127	IPv4 TCP	PASS	Clients Site B → proxy Squid:3127 via tunnel — filtrage web centralisé.

Règles IPsec pfSense-01 — Firewall → Rules → IPsec



SECTION V

Pare-feu pfSense-02 — Site B (WAN 10.10.101.4)

Politique de sécurité symétrique — site secondaire PRA

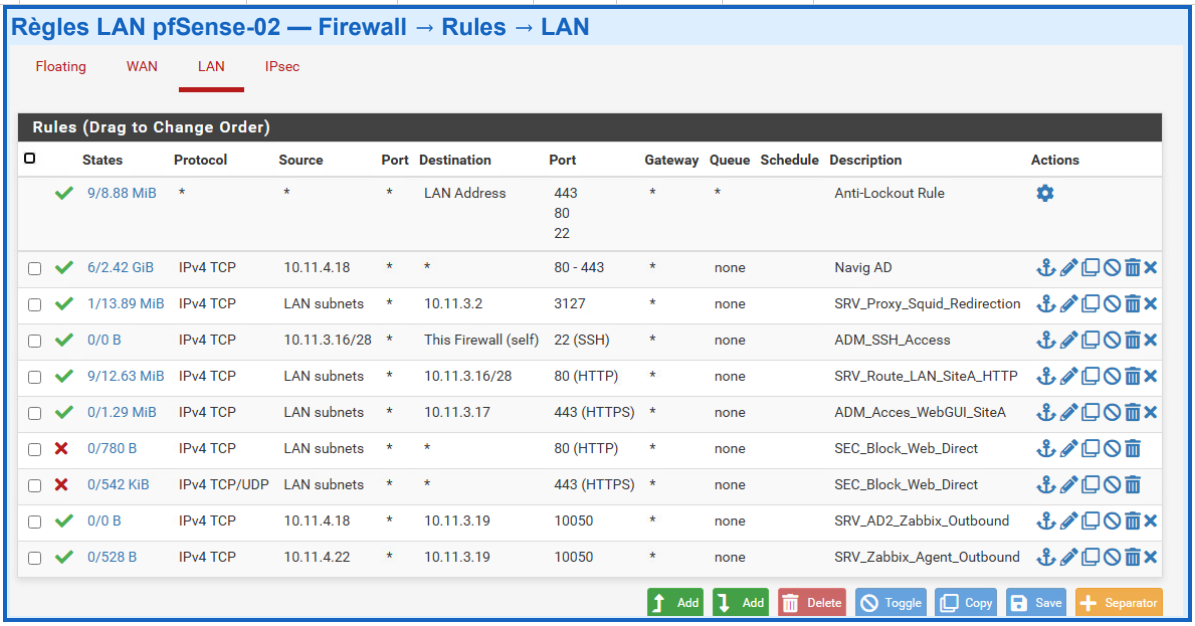
---

pfSense-02 assure la sécurité du **LAN Site B (10.11.4.16/28)**. Sa logique de filtrage est *symétrique* à pfSense-01 : le trafic web est redirigé vers le proxy centralisé du Site A via le tunnel IPsec, assurant un filtrage uniforme sur les deux sites.

5.1 — Règles LAN (10.11.4.16/28) — Interface LAN pfSense-02

#	Règle	Source	Dest.	Port	Proto	Action	Justification professionnelle
—	Anti-Lockout Rule (système)	*	LAN Addr	443/80/22	*	PASS	Règle système pfSense — protège l'accès administration. Non modifiable.
1	Navig AD (10.11.4.18)	10.11.4.18	*	80-443	IPv4 TCP	PASS	Exempte AD2 du proxy — Windows Update, licences. DC ne supporte pas proxy système.
2	SRV_Proxy_Squid_Redirection	LAN subnets	10.11.3.2	3127	IPv4 TCP	PASS	LAN Site B → proxy Squid centralisé Site A:3127 via tunnel IPsec.
3	ADM_SSH_Access	10.11.3.16/28	This FW	22	IPv4 TCP	PASS	SSH pfSense-02 depuis LAN Site A uniquement — administration distante.
4	SRV_Zabbix_SNMP_Query	10.11.3.19	10.11.4.17	161	IPv4 UDP	PASS	SNMP v2c Zabbix → pfSense-02 via tunnel IPsec — supervision centralisée.
5	SRV_Route_LAN_SiteA_HTTP	LAN subnets	10.11.3.16/28	80	IPv4 TCP	PASS	HTTP inter-sites — accès applications métier hébergées Site A.
6	ADM_Acces_WebGUI_SiteA	LAN subnets	10.11.3.17	443	IPv4 TCP	PASS	Équipes IT Site B administrent pfSense-01 via WebGUI HTTPS.
7	SEC_Block_Web_Direct (HTTP)	LAN subnets	*	80	IPv4 TCP	BLOCK	Bloque HTTP direct Site B — force proxy centralisé. [DÉSACTIVÉE — à réactiver]
8	SEC_Block_Web_Direct (HTTPS+QUIC)	LAN subnets	*	443	IPv4 TCP/UDP	BLOCK	Bloque HTTPS+QUIC direct — anti-contournement proxy. [DÉSACTIVÉE — à réactiver]

Règles LAN pfSense-02 — Firewall → Rules → LAN

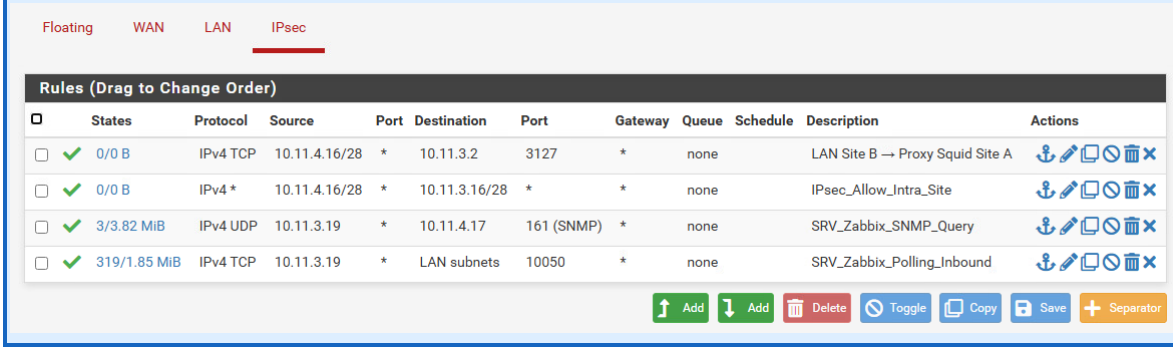


SECTION VI

5.2 — Règles IPsec — pfSense-02 Site B (enc0)

#	Règle	Source	Dest.	Port	Proto	Action	Justification professionnelle
1	LAN Site B → Proxy Squid Site A	10.11.4.16/28	10.11.3.2	3127	IPv4 TCP	PASS	Retour des réponses proxy Squid vers les clients Site B. Sans cette règle, réponses bloquées.
2	IPsec_Allow_Intra_Sit e	10.11.4.16/28	10.11.3.16/ 28	*	IPv4 *	PASS	Flux généraux inter-sites : réplication AD, sauvegardes nocturnes, SNMP, ICMP.
3	SRV_Zabbix_SNMP_Query	10.11.3.19	10.11.3.17	161	IPV4 UDP	Pass	Supervision Pfsense B
4	SRV_Zabbix_Polling_Inbound	10.11.3.19	Lan Net	10050	IPV4 TCP	Pass	Supervision Site B

Règles IPsec pfSense-02 — Firewall → Rules → IPsec]



Proxy Squid en zone DMZ — SRV-WEB-01 (10.11.3.2)

Architecture de filtrage web centralisé avec SSL Bumping

Le déploiement du proxy Squid sur une **VM Debian 12.5 dédiée en DMZ isolée** est le résultat d'une décision d'architecture motivée par des impératifs de sécurité majeurs.

6.1 — Justification de l'architecture : défense en profondeur

■■ **Contexte sécurité :** Fin 2023, Netgate a **retiré officiellement le package Squid de pfSense** suite à la découverte de plus de **55 CVE non corrigés**, dont des Heap Overflow permettant l'exécution de code arbitraire à distance sans authentification (CVSS > 9.0). Maintenir Squid directement sur pfSense aurait exposé l'infrastructure à une compromission root totale — contrôle du pare-feu, des tunnels VPN et de l'accès WAN.

Critère	Squid sur pfSense (déprécié)	Squid sur Debian 12.5 DMZ
Sécurité CVE	55+ CVE — package gelé	apt upgrade régulier — patches actifs
Isolation	Colocataire du pare-feu central	VM dédiée en zone DMZ cloisonnée
Impact si compromis	Contrôle total pfSense + VPN + WAN	Confinement DMZ — LAN et firewall protégés
Mises à jour	Fin de support Netgate	Mainteneur Squid actif — roadmap claire
Configuration	Interface GUI limitée	squid.conf natif — ACL granulaires

Performance	Partage CPU/RAM avec pfSense	Ressources dédiées — pas de contention

6.2 — Fonctionnement du SSL Bumping

Le proxy intercepte les flux HTTPS via une **attaque man-in-the-middle contrôlée** : il déchiffre les trames TLS avec son certificat interne *Squid Proxy CA*, applique les ACL sur le contenu déchiffré, puis rechiffre avant transmission. Ce mécanisme est transparent grâce au certificat CA déployé via **GPO_Certificat_Proxy** (Active Directory CS).

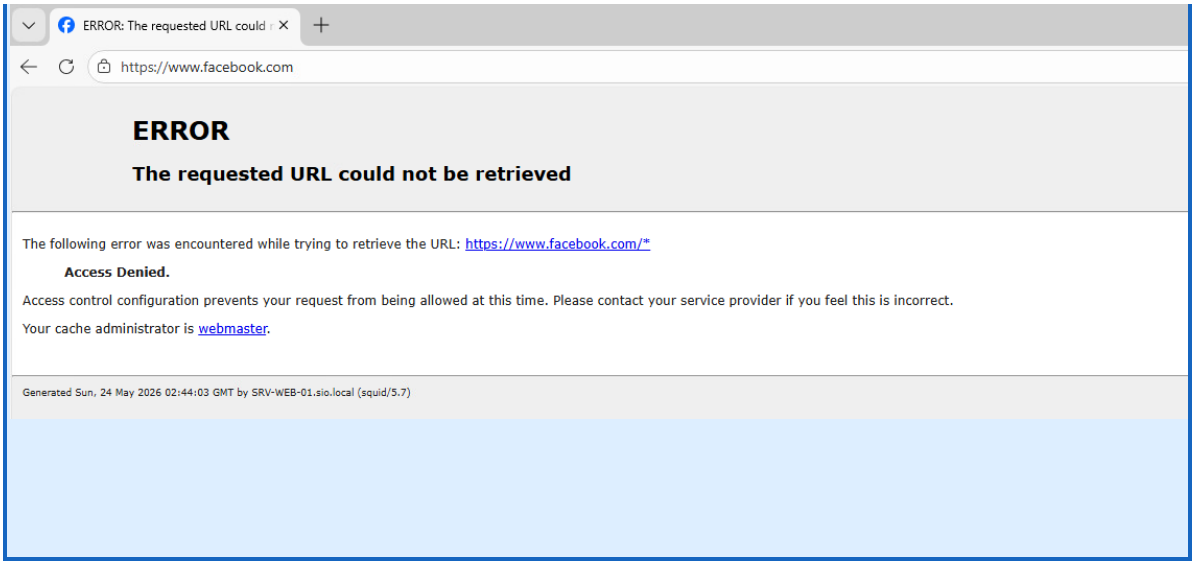
Catégorie filtrée	Exemples de domaines bloqués
Réseaux sociaux	Facebook, Instagram, Twitter/X, TikTok, LinkedIn
Streaming & médias	YouTube, Netflix, Twitch, Dailymotion, Prime Video
Paris sportifs & jeux	Winamax, Betclic, PMU, FDJ, Pokerstars
Contenus adultes	Sites classifiés PEGI-18 (Blacklist UT1 Toulouse)
Publicités & trackers	Domaines publicitaires — protection vie privée

Configuration Squid — SSH SRV-WEB-01 : cat /etc/squid/squid.conf

```
root@SRV-WEB-01:~# cat /etc/squid/squid.conf
# ====================A==================================
# CONFIGURATION SQUID - MODE MANUEL (GPO) + SSL BUMP
# Auteur : CHADHOULI EL-Anrif - BTS SIO SISR 2026
# Serveur : SRV-WEB-01 - 10.11.3.2 - Debian 12.5
# ========================================================


# --------------------------------------------------------
# RESEAUX AUTORISES
# --------------------------------------------------------
acl networklan    src 10.11.3.16/28
acl site_b_lan     src 10.11.4.16/28



# --------------------------------------------------------
# LISTES DE BLOCAGE
# --------------------------------------------------------
acl cat_porn            dstdomain "/etc/squid/blacklists/porn/domains"
acl cat_social_networks dstdomain "/etc/squid/blacklists/social_networks/domains"
acl sites_interdits     dstdomain "/etc/squid/sites_bloques.txt"
acl test_manuel         dstdomain .facebook.com .napflix.tv .pornhub.com .youtube.com \
                                  .netflix.com .crunchyroll.com .winamax.fr


# --------------------------------------------------------
# PORT MANUEL AVEC SSL BUMP
# Aucun mot "intercept" - proxy explicite configure cote client
# --------------------------------------------------------
http_port 3127 ssl-bump \
    generate-host-certificates=on \
    dynamic_cert_mem_cache_size=4MB \
    cert=/etc/squid/squid-ca.crt \
    key=/etc/squid/squid-ca.key


# --------------------------------------------------------
# MOTEUR SSL BUMP
# --------------------------------------------------------
sslcrtd_program /usr/lib/squid/security_file_certgen \
    -s /var/lib/squid/ssl_db \
    -M 4MB
sslcrtd_children 5

acl step1 at_step SslBump1
ssl_bump peek  step1
ssl_bump bump  all
```

Test de blocage Squid — Chrome → Facebook.com bloqué

SECTION VIII



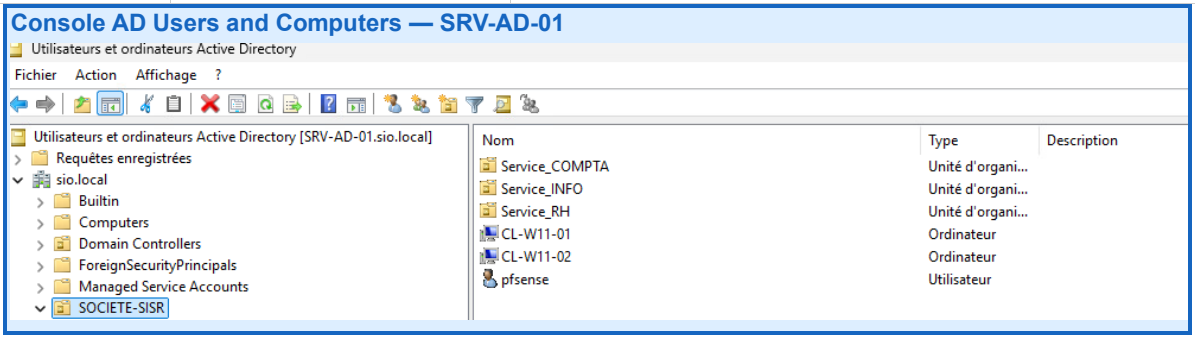
Infrastructure Active Directory — sio.local

Contrôleurs de domaine redondants — DC1 Site A / DC2 Site B (PRA)

7.1 — SRV-AD-01 — Contrôleur principal (10.11.3.18)

SRV-AD-01 constitue le **cœur de l'infrastructure d'identités** de SioSisr. Il cumule quatre rôles critiques : annuaire AD DS, résolution DNS interne, attribution d'adresses DHCP, et Autorité de Certification interne (AD CS) pour l'émission des certificats PKI utilisés par le proxy Squid et LDAPS.

Service	Configuration	Détail
AD DS	Domaine sio.local	Gestion des identités, authentification Kerberos, politiques de groupe
DNS	Zone sio.local	Résolution interne + récursive vers Internet pour les serveurs
DHCP	Scope 10.11.3.23–10.11.3.30/28	GW : 10.11.3.17 | DNS : 10.11.3.18 / 10.11.4.18
AD CS (PKI)	Autorité de Certification interne	Émission certificat Squid Proxy CA + certificats LDAPS
FSRM	Quota Hard Limit 200 Mo	Alerte e-mail automatique à 85% de remplissage

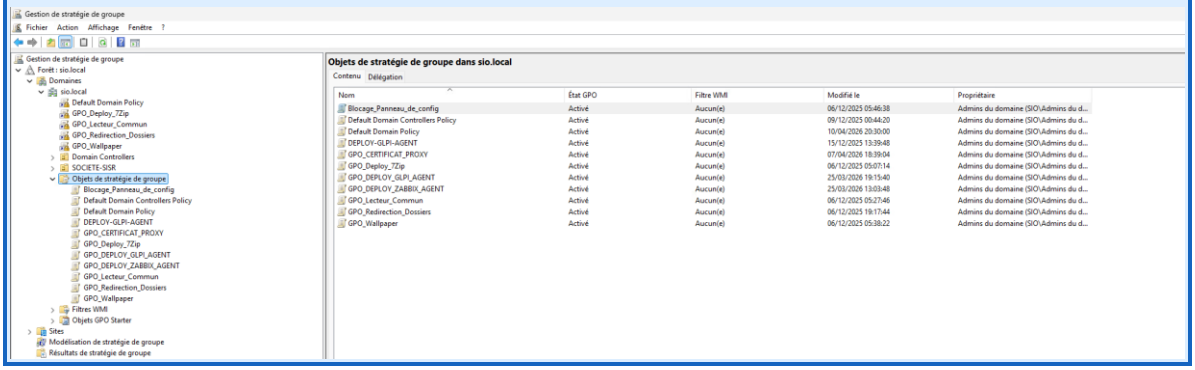


7.2 — GPO déployées

Nom GPO	Fonction	Cible

GPO_ProxySquid	Configuration proxy 10.11.3.2:3127 sur tous les navigateurs	Tous les postes clients
GPO_Certificat_Proxy	Déploiement certificat racine Squid Proxy CA (magasin Windows)	Tous les postes clients
DEPLOY-GLPI	Installation silencieuse agent GLPI (MSI)	Tous les postes
GPO_Deploy_7Zip	Installation silencieuse 7-Zip	Tous les postes
GPO_Lecteur_Commun	Montage automatique P: (Service) et U: (Personnel)	Utilisateurs du domaine
GPO_Redirection_Dossiers	Redirection Documents et Bureau vers \\10.11.3.18\	Utilisateurs du domaine
Blocage_Panneau_de_config	Restriction accès paramètres système Windows	Utilisateurs non-admin
GPO_Wallpaper	Application fond d'écran entreprise SioSisr	Tous les postes

Console GPMC (gpmc.msc) — Arborescence des GPO



7.3 — ACL NTFS — Partages réseau \\10.11.3.18\Commun

Dossier	Service_INFO	Service_RH	Service_COMPTA
RH\	Lecture / Écriture	Lecture / Écriture	■ Accès refusé
COMPTA\	Lecture / Écriture	■ Accès refusé	Lecture / Écriture
INFO\	Lecture / Écriture	■ Accès refusé	■ Accès refusé

Tunnel IPsec IKEv2 Site-à-Site

Chiffrement AES-256 — Interconnexion sécurisée pfSense-01 ↔ pfSense-02

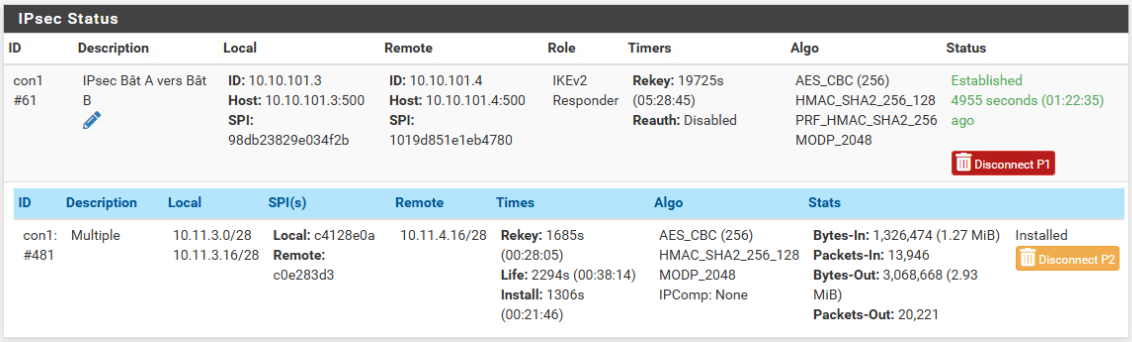
Le tunnel IPsec constitue l'**épine dorsale de l'infrastructure bi-site**. Il assure trois fonctions critiques : la réplication Active Directory entre DC1 et DC2, les sauvegardes nocturnes chiffrées vers le Site A, et le routage du trafic web des clients Site B vers le proxy Squid centralisé. L'état du tunnel est **Established** et supervisé en permanence via un Keep Alive Ping vers 10.11.3.18.

Paramètre	Phase 1 — Canal IKE (Contrôle)	Phase 2 — Tunnel ESP (Données)
Protocole	IKEv2	ESP (Encapsulating Security Payload)
Mode	—	Tunnel IPv4
Authentification	Mutual PSK (Pre-Shared Key)	—
Chiffrement	AES-256 bits	AES-256 bits

SECTION X

Intégrité (Hash)	SHA-256	SHA-256
Groupe Diffie-Hellman	Groupe 14 — 2048 bits	PFS Groupe 14 — 2048 bits
Réseaux encapsulés	10.10.101.3 ↔ 10.10.101.4	10.11.3.16/28 ↔ 10.11.4.16/28
Keep Alive	—	Ping → 10.11.3.18 (AD1)

[INSÉRER VOTRE CAPTURE ICI — Statut tunnel IPsec — pfSense → VPN → IPsec → Status



Sauvegarde et Plan de Reprise d'Activité

Redondance géographique — continuité de service garantie

L'architecture PRA repose sur la **réplication Active Directory bidirectionnelle** via le tunnel IPsec et sur des sauvegardes nocturnes automatisées. En cas de défaillance du Site A, SRV-AD-02 prend en charge l'authentification et active son scope DHCP de secours (10.11.4.23–10.11.4.30/28) — **RTO < 15 min**, aucune intervention manuelle requise.

Composant	Détail
Source des données	SRV-AD-02 (10.11.4.18) — données critiques DC secondaire
Destination	\\10.11.3.18\Backup sur SRV-AD-01 Site A
Chiffrement du transfert	AES-256 via tunnel IPsec IKEv2 — aucune donnée en clair
Outil de sauvegarde	Windows Server Backup (natif WS2025)
Planification	Tâche nocturne à 02h00 — creux réseau garanti
Script PowerShell	C:\Scripts\Backup-AD.ps1 — Tâche planifiée : Backup-ADNightly
Basculement DHCP	Scope AD2 activé manuellement si AD1 défaillant — RTO < 15 min

[INSÉRER VOTRE CAPTURE ICI — AD Sites and Services — Réplication DC1 ↔ DC2]

Montre la console AD Sites and Services avec les deux sites (SiteA, SiteB) et le lien de réplication bidirectionnel entre SRV-AD-01 et SRV-AD-02.

SECTION XI

```
PS C:\Users\Administrateur> repadmin /showrepl

Repadmin : exécution de la commande /showrepl sur le contrôleur de domaine complet localhost
Default-First-Site-Name\SRV-AD-01
Options DSA : IS_GC
Options de site : (none)
GUID de l'objet DSA : 76a2ed84-f0af-4985-a6c5-0a3716bfa372
ID de l'invocation DSA : 71ece5c0-33cc-4d38-89b3-91b4f54556f7

=== INSTANCES VOISINES ENTRANTES ==================================

DC=sio,DC=local
    Default-First-Site-Name\SRV-AD-02 via RPC
        GUID de l'objet DSA : 91cf05c1-7bcd-4593-9e90-da79a8f20e74
        La dernière tentative, le 2026-02-28 00:59:11, a réussi.

CN=Configuration,DC=sio,DC=local
    Default-First-Site-Name\SRV-AD-02 via RPC
        GUID de l'objet DSA : 91cf05c1-7bcd-4593-9e90-da79a8f20e74
        La dernière tentative, le 2026-02-28 00:59:11, a réussi.

CN=Schema,CN=Configuration,DC=sio,DC=local
    Default-First-Site-Name\SRV-AD-02 via RPC
        GUID de l'objet DSA : 91cf05c1-7bcd-4593-9e90-da79a8f20e74
        La dernière tentative, le 2026-02-28 00:59:11, a réussi.

DC=DomainDnsZones,DC=sio,DC=local
    Default-First-Site-Name\SRV-AD-02 via RPC
        GUID de l'objet DSA : 91cf05c1-7bcd-4593-9e90-da79a8f20e74
        La dernière tentative, le 2026-02-28 00:59:11, a réussi.

DC=ForestDnsZones,DC=sio,DC=local
    Default-First-Site-Name\SRV-AD-02 via RPC
        GUID de l'objet DSA : 91cf05c1-7bcd-4593-9e90-da79a8f20e74
        La dernière tentative, le 2026-02-28 00:59:11, a réussi.
```

Supervision temps réel — Zabbix (10.11.3.19)

Monitoring centralisé — 9 hôtes supervisés — Alertes e-mail automatiques

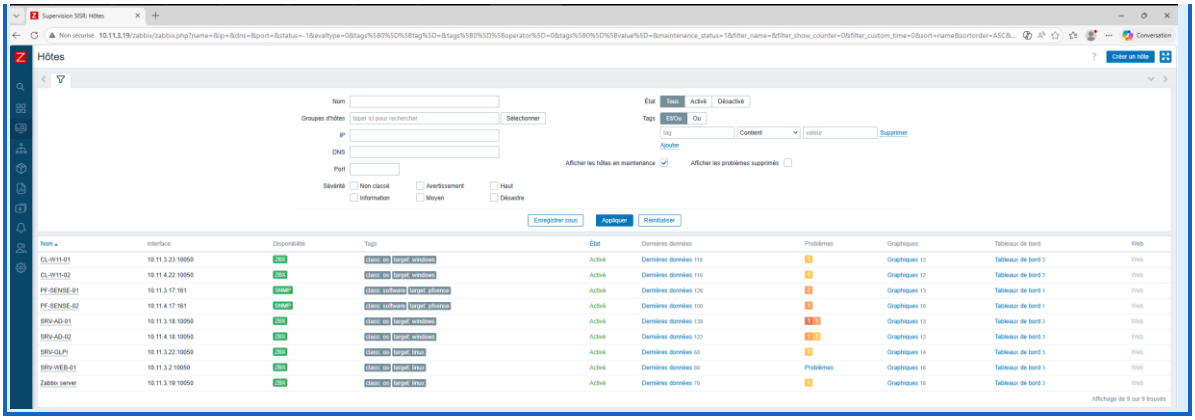
---

SRV-ZABBIX centralise la supervision de l'ensemble du parc. Les agents Zabbix sont déployés sur tous les serveurs Windows et Linux. Les pare-feux pfSense sont supervisés via **SNMP v2c** (absence d'agent disponible sur FreeBSD), avec une ACL restrictive limitant les requêtes SNMP à la seule IP de SRV-ZABBIX.

Hôte supervisé	IP	Méthode	Métriques clés
pfSense-01	10.11.3.17	SNMP v2c	CPU, RAM, bande passante, états interfaces, tunnel IPsec
pfSense-02	10.11.4.17	SNMP v2c	CPU, RAM, bande passante, états interfaces, tunnel IPsec
SRV-AD-01	10.11.3.18	Agent Zabbix	CPU, RAM, disque, services AD/DNS/DHCP
SRV-AD-02	10.11.4.18	Agent Zabbix	CPU, RAM, disque, réplication AD (latence)
SRV-ZABBIX	10.11.3.19	Agent (auto)	MariaDB, processus Zabbix, disque, RAM
SRV-GLPI	10.11.3.22	Agent Zabbix	CPU, RAM, disque, services Docker, GLPI
SRV-WEB-01	10.11.3.2	Agent Zabbix	CPU, RAM, disque, processus Squid/Apache
CL-WIN11-01	10.11.3.25	Agent Zabbix	CPU, RAM, disque, connexion réseau
CL-WIN11-02	10.11.4.24	Agent Zabbix	CPU, RAM, disque, connexion réseau

Dashboard Zabbix — Monitoring → Hosts

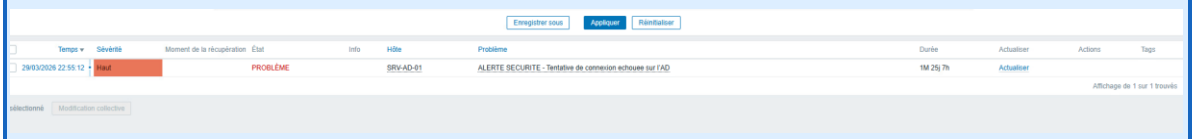
SECTION XII



Déclencheurs (Triggers) configurés

Déclencheur	Condition	Sévérité	Action
CPU surchargé	CPU > 85% pendant 5 min consécutives	Avertissement	Notification e-mail immédiate
RAM critique	RAM > 90%	Haute	Notification e-mail + escalade
Disque — avertissement	Espace disque > 80%	Avertissement	Alerte e-mail
Disque — saturation critique	Espace disque > 95%	Critique	Alerte e-mail critique
Service down	AD, DNS, Squid ou Zabbix arrêté	Critique	Notification immédiate
Brute-force détecté	≥ 3 échecs d'authentification consécutifs	Critique	Alerte e-mail critique
Tunnel IPsec down	Ping Keep Alive 10.11.3.18 KO	Critique	Notification critique — impact bi-site

— Zabbix — Triggers : Brute-force



Configuration → Hosts → [hôte] → Triggers. Montre le déclencheur 'Brute-force (≥3 échecs auth)' avec expression et sévérité visibles

Inventaire et helpdesk — GLPI (10.11.3.22)

ITSM centralisé — déploiement Docker — inventaire automatique

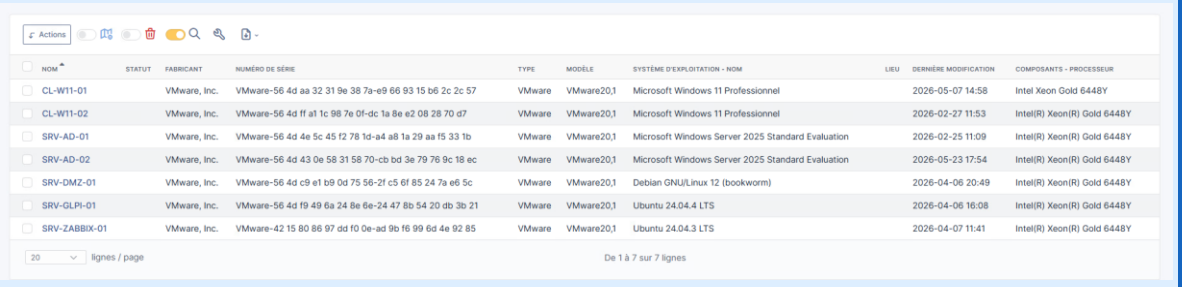
---

SRV-GLPI centralise la gestion du parc informatique et l'helpdesk. Il est déployé sous **Docker** sur Ubuntu 22.04 LTS, garantissant l'isolation des services, la facilité de sauvegarde (export de volume Docker) et la reproductibilité via docker-compose.yml. L'inventaire automatique est assuré par l'**agent GLPI déployé via GPO** (MSI silencieux) sur tous les postes Windows du domaine.

- **Inventaire automatique :** remontée matérielle, logiciels, licences et configuration réseau de chaque poste
- **Ticketing helpdesk :** création, suivi, assignation et résolution des incidents utilisateurs
- **Authentification LDAPS :** connexion sécurisée via Active Directory (port 636, TLS) — suppression des comptes locaux
- **Déploiement GPO DEPLOY-GLPI :** installation silencieuse de l'agent GLPI-Agent via MSI

Interface GLPI — Dashboard et inventaire automatique

Montre le dashboard GLPI avec les postes CL-WIN11-01 et CL-WIN11-02 inventoriés automatiquement (matériel, logiciels, config réseau détectés via l'agent).



Actions

NOM	STATUT	FABRICANT	NUMÉRO DE SÉRIE	TYPE	MODÈLE	SYSTÈME D'EXPLOITATION - NOM	LIEU	DERNIÈRE MODIFICATION	COMPOSANTS - PROCESSEUR
CL-W11-01		VMware, Inc.	VMware-56 4d aa 32 31 9e 38 7a-e9 66 93 15 b6 2c 2c 57	VMware	VMware20,1	Microsoft Windows 11 Professionnel		2026-05-07 14:58	Intel Xeon Gold 6448Y
CL-W11-02		VMware, Inc.	VMware-56 4d ff a1 1c 98 7e 0f-dc 1a 8e e2 08 28 70 d7	VMware	VMware20,1	Microsoft Windows 11 Professionnel		2026-02-27 11:53	Intel(R) Xeon(R) Gold 6448Y
SRV-AD-01		VMware, Inc.	VMware-56 4d 4e 5c 45 f2 78 1d-a4 a8 1a 29 aa f5 33 1b	VMware	VMware20,1	Microsoft Windows Server 2025 Standard Evaluation		2026-02-25 11:09	Intel(R) Xeon(R) Gold 6448Y
SRV-AD-02		VMware, Inc.	VMware-56 4d 43 0e 58 31 58 70-cb bd 3e 79 76 9c 18 ec	VMware	VMware20,1	Microsoft Windows Server 2025 Standard Evaluation		2026-05-23 17:54	Intel(R) Xeon(R) Gold 6448Y
SRV-DMZ-01		VMware, Inc.	VMware-56 4d c9 e1 b9 0d 75 56-2f c5 6f 85 24 7a e6 5c	VMware	VMware20,1	Debian GNU/Linux 12 (bookworm)		2026-04-06 20:49	Intel(R) Xeon(R) Gold 6448Y
SRV-GLPI-01		VMware, Inc.	VMware-56 4d f9 49 6a 24 8e 6e-24 47 8b 54 20 db 3b 21	VMware	VMware20,1	Ubuntu 24.04.4 LTS		2026-04-06 16:08	Intel(R) Xeon(R) Gold 6448Y
SRV-ZABBIX-01		VMware, Inc.	VMware-42 15 80 86 97 dd f0 0e-ad 9b f6 99 6d 4e 92 85	VMware	VMware20,1	Ubuntu 24.04.3 LTS		2026-04-07 11:41	Intel(R) Xeon(R) Gold 6448Y

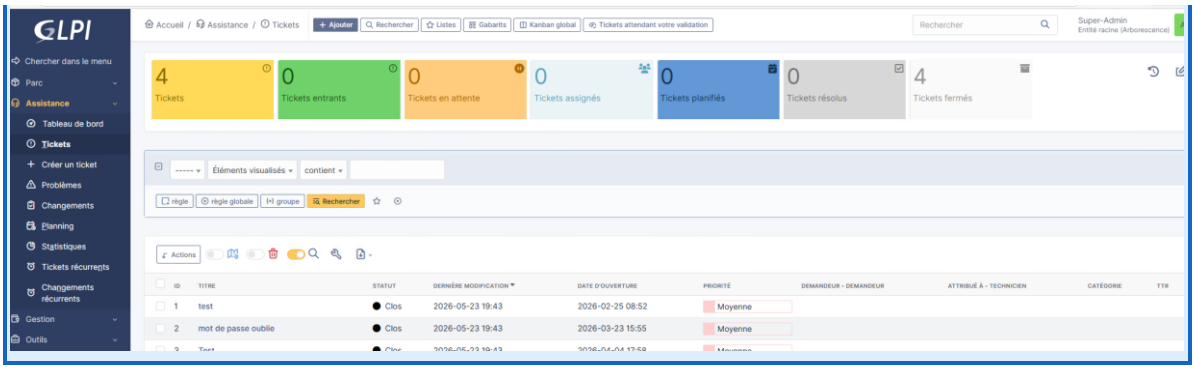
20 lignes / page

De 1 à 7 sur 7 lignes

GLPI — Ticket helpdesk créé

Montre un ticket créé dans GLPI avec son statut, sa priorité et son assignation visibles dans le tableau de bord helpdesk.

SECTION XI



Sécurisation de l'authentification — Migration LDAP → LDAPS

Chiffrement TLS des credentials Active Directory — validation Wireshark

---

12.1 — Constat : une authentification en clair (risque identifié)

L'authentification initiale de GLPI vers Active Directory utilisait **LDAP standard sur le port 389**. Les identifiants transitaient en clair, exposant l'infrastructure à une attaque *Man-in-the-Middle* : sur un segment LAN accessible, n'importe quelle machine peut capturer les trames LDAP et lire directement les mots de passe des comptes Active Directory.

12.2 — Solution : LDAPS port 636 avec certificat AD CS

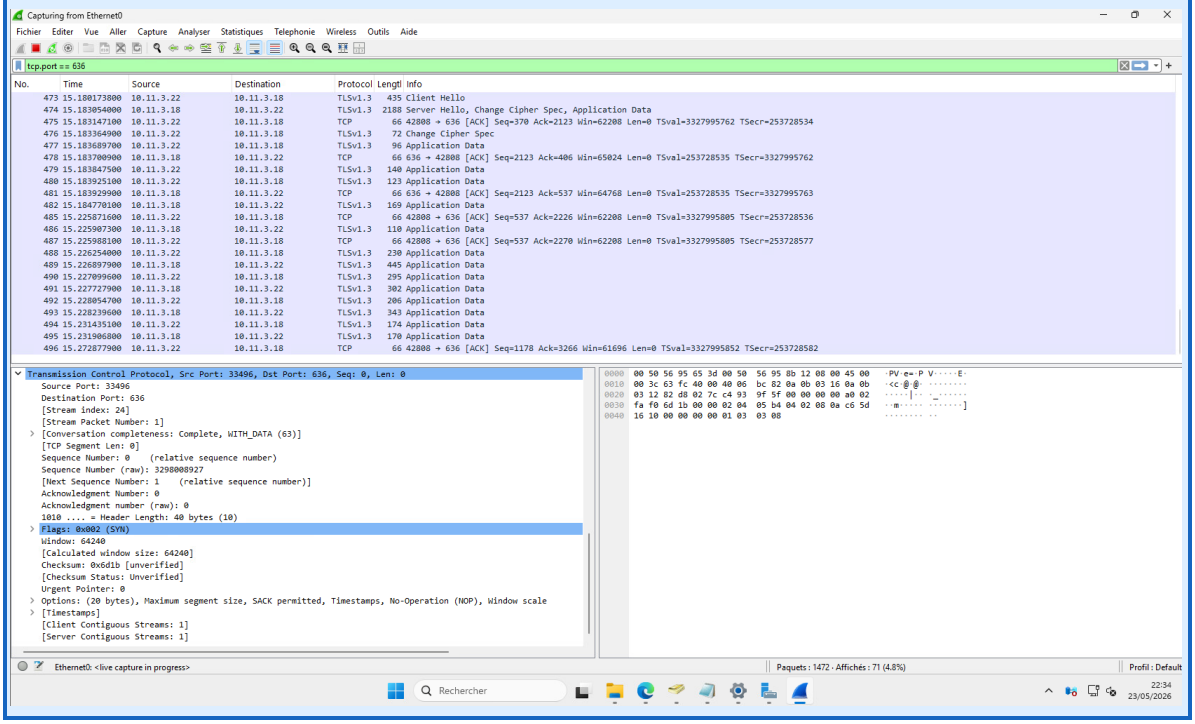
Étape	Action	Détail technique
1	Génération du certificat	Console AD CS sur SRV-AD-01 → émission certificat 'Contrôleur de domaine' lié au FQDN srv-ad-01.sio.local
2	Export du certificat racine	Export .crt → import dans le magasin Ubuntu de SRV-GLPI via update-ca-certificates
3	Reconfiguration GLPI	Configuration → Authentification LDAP → port 636, TLS activé, chemin certificat CA renseigné
4	Validation Wireshark	Capture lors d'une authentification : trames TCP 636 chiffrées TLS — aucun identifiant lisible ■

■ **Résultat obtenu :** Tous les flux GLPI ↔ Active Directory sont désormais chiffrés TLS. Une capture Wireshark lors d'une authentification ne révèle aucun identifiant — les trames TCP 636 ne contiennent que des données chiffrées. La validation par capture réseau constitue une preuve irréfutable de l'efficacité de la mesure.

Wireshark — Validation LDAPS port 636 (filtre : tcp.port == 636

SECTION XII

PREUVE PRINCIPALE. Capture lors d'une authentification GLPI → AD. Les trames TCP 636 doivent afficher du trafic TLS chiffré sans aucun identifiant lisible en clair.



Plan d'adressage IP final

Table exhaustive — tous les équipements et interfaces

Site	Machine	Adresse IP	Interface(s)	Rôle	OS
A	pfSense-01	10.11.3.17 (LAN) / 10.11.3.1 (DMZ) / 10.10.101.3 (WAN)	LAN/DMZ/WAN	Pare-feu / VPN / Routeur	pfSense 2.7.2 CE
A	SRV-AD-01	10.11.3.18	LAN A	DC1 / DNS / DHCP / PKI	Windows Server 2025
A	SRV-ZABBIX	10.11.3.19	LAN A	Supervision / Alerting	Debian 12.5
A	SRV-GLPI	10.11.3.22	LAN A	Inventaire ITSM / Helpdesk	Ubuntu 22.04 LTS
A	CL-WIN11-01	10.11.3.25 (DHCP)	LAN A	Poste client Site A	Windows 11 Pro 22H2

SECTION XIII

DMZ	SRV-WEB-01	10.11.3.2	DMZ	Apache2 + Proxy Squid	Debian 12.5
B	pfSense-02	10.11.4.17 (LAN) / 10.10.101.4 (WAN)	LAN B/WAN	Pare-feu Site B / IPsec	pfSense 2.7.2 CE
B	SRV-AD-02	10.11.4.18	LAN B	DC2 / DNS / DHCP secours / PRA	Windows Server 2025
B	CL-WIN11-02	10.11.4.24 (statique)	LAN B	Poste client Site B	Windows 11 Pro 22H2

SECTION XIV

Matrice de flux consolidée — Règles pfSense majeures

Vue globale des flux autorisés et bloqués sur l'ensemble de l'infrastructure

Source	Destination	Port / Proto	Pare-feu	Action	Description
LAN A 10.11.3.16/28	SRV-WEB-01 10.11.3.2	TCP 3127	pfSense-01 LAN	PASS	Accès proxy Squid — filtrage web LAN Site A
LAN A 10.11.3.16/28	AD1 10.11.3.18	UDP 53	pfSense-01 LAN	PASS	DNS interne → contrôleur de domaine
LAN A 10.11.3.16/28	Internet WAN	TCP 80/443	pfSense-01 LAN	BLOCK	Navigation directe interdite — bypass proxy bloqué
LAN A 10.11.3.16/28	Internet WAN	UDP 443 (QUIC)	pfSense-01 LAN	BLOCK	Anti-contournement proxy — HTTP/3 bloqué
SRV-ZABBIX 10.11.3.19	pfSense-01 10.11.3.17	UDP 161	pfSense-01 LAN	PASS	SNMP v2c — supervision pare-feu Site A
SRV-ZABBIX 10.11.3.19	SRV-WEB-01 10.11.3.2	TCP 10050	pfSense-01 LAN	PASS	Agent Zabbix — monitoring proxy Squid
DMZ 10.11.3.0/28	Internet WAN	TCP 80/443	pfSense-01 DMZ	PASS	Sortie web proxy Squid → Internet
DMZ 10.11.3.0/28	AD1 10.11.3.18	UDP/TCP 53	pfSense-01 DMZ	PASS	DNS interne SRV-WEB-01 → AD1
DMZ 10.11.3.0/28	LAN A 10.11.3.16/28	Any	pfSense-01 DMZ	BLOCK	Isolation totale DMZ → LAN (défense profondeur)
DMZ 10.11.3.0/28	LAN B 10.11.4.16/28	Any	pfSense-01 DMZ	BLOCK	Isolation totale DMZ → LAN Site B
LAN B 10.11.4.16/28	SRV-WEB-01 10.11.3.2	TCP 3127	pfSense-02 LAN	PASS	Proxy centralisé Site B via IPsec
LAN B 10.11.4.16/28	Internet WAN	TCP 80/443	pfSense-02 LAN	BLOCK	Navigation directe interdite Site B
SRV-ZABBIX 10.11.3.19	pfSense-02 10.11.4.17	UDP 161	IPsec	PASS	SNMP v2c — supervision pare-feu Site B via IPsec
GLPI 10.11.3.22	AD1 10.11.3.18	TCP 636	pfSense-01 LAN	PASS	LDAPS — authentification chiffrée TLS

LAN A ↔ LAN B	—	Any (IPsec)	IPsec enc0	PASS	Tunnel IPsec — réplication AD, sauvegardes, supervision

Cahier de recette — Tests de validation fonctionnelle

9 tests exécutés — Infrastructure validée en production

L'ensemble des tests de recette a été conduit dans un environnement de production virtuelle sur VMware ESXi. Chaque test valide un composant critique de l'architecture et constitue une **preuve de fonctionnement documentée** pour l'épreuve E6.

N°	Test	Condition d'exécution	Résultat attendu	Statut
1	Basculement DHCP (PRA)	Éteindre AD1 → activer scope AD2 → ipconfig /renew	DHCP Server = 10.11.4.18	■ SUCCÈS
2	Blocage HTTPS par Squid	Firefox (proxy configuré) → accéder à youtube.com	Page 'Accès interdit par proxy'	■ SUCCÈS
3	Forçage proxy — blocage direct	Retirer proxy Firefox → accéder à google.com	Connexion refusée — règle BLOCK TCP 80/443	■ SUCCÈS
4	Quota FSRM 200 Mo	Copier fichier 300 Mo dans \\10.11.3.18\Partages\INFO	Écriture bloquée + notification e-mail	■ SUCCÈS
5	Tunnel IPsec Site-à-Site	Ping CL-WIN11-02 (10.11.4.24) → CL-WIN11-01 (10.11.3.25)	Ping réussi — tunnel Established	■ SUCCÈS
6	Supervision Zabbix	Dashboard → vérifier les 9 hôtes supervisés	9 hôtes en vert, métriques actualisées temps réel	■ SUCCÈS
7	Sauvegarde AD inter-sites	Vérifier \\10.11.3.18\Backup après exécution nocturne	Fichiers présents, datés du jour, taille cohérente	■ SUCCÈS
8	Ticketing GLPI	Créer un ticket helpdesk via l'interface web GLPI	Ticket créé, visible dans le tableau de bord	■ SUCCÈS
9	Chiffrement LDAPS	Capture Wireshark lors d'une authentification GLPI → AD	TCP 636 — flux TLS chiffré, aucun identifiant lisible	■ SUCCÈS

■ **Statut global : INFRASTRUCTURE VALIDÉE — 9/9 tests de recette concluants.** Le tunnel IPsec AES-256 assure la confidentialité inter-sites, le proxy Squid centralise le filtrage web des deux sites, Active Directory gère les identités avec redondance PRA, et Zabbix assure la supervision temps réel de 9 hôtes.