

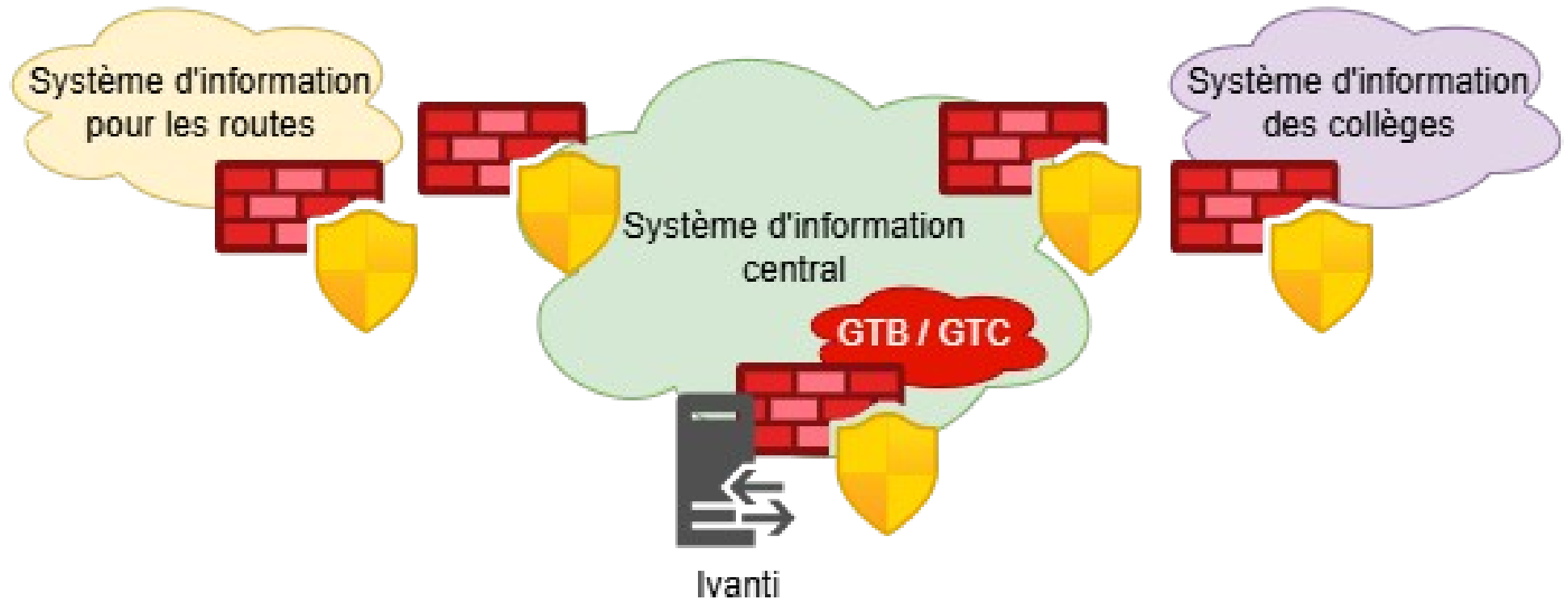
Mise en place du WebSSO LemonLDAP::NG au Département de l'Isère



Plan

- Présentation des SI du département
- Le projet d'authentification centralisée
- Autres Projets
- Annonces

Département de l'Isère



Besoin D38

Remplacement du reverse proxy Ivanti

- reverse proxy
- portail d'authentification
- portail applicatif
- fédération d'identités
- portail de configuration du reverse proxy

En complément

- SSO : Remplacement de l'ADFS
- Authentification multi facteurs

Solutions étudiées

Keycloak



- portail d'authentification
- ~~portail applicatif~~
- fédération d'identités
- ~~portail de configuration du reverse proxy~~
- SSO
- authentification multifacteurs

Vulture



- portail d'authentification
- ~~portail applicatif~~
- fédération d'identités
- portail de configuration du reverse proxy
- SSO
- Authentification multifacteurs

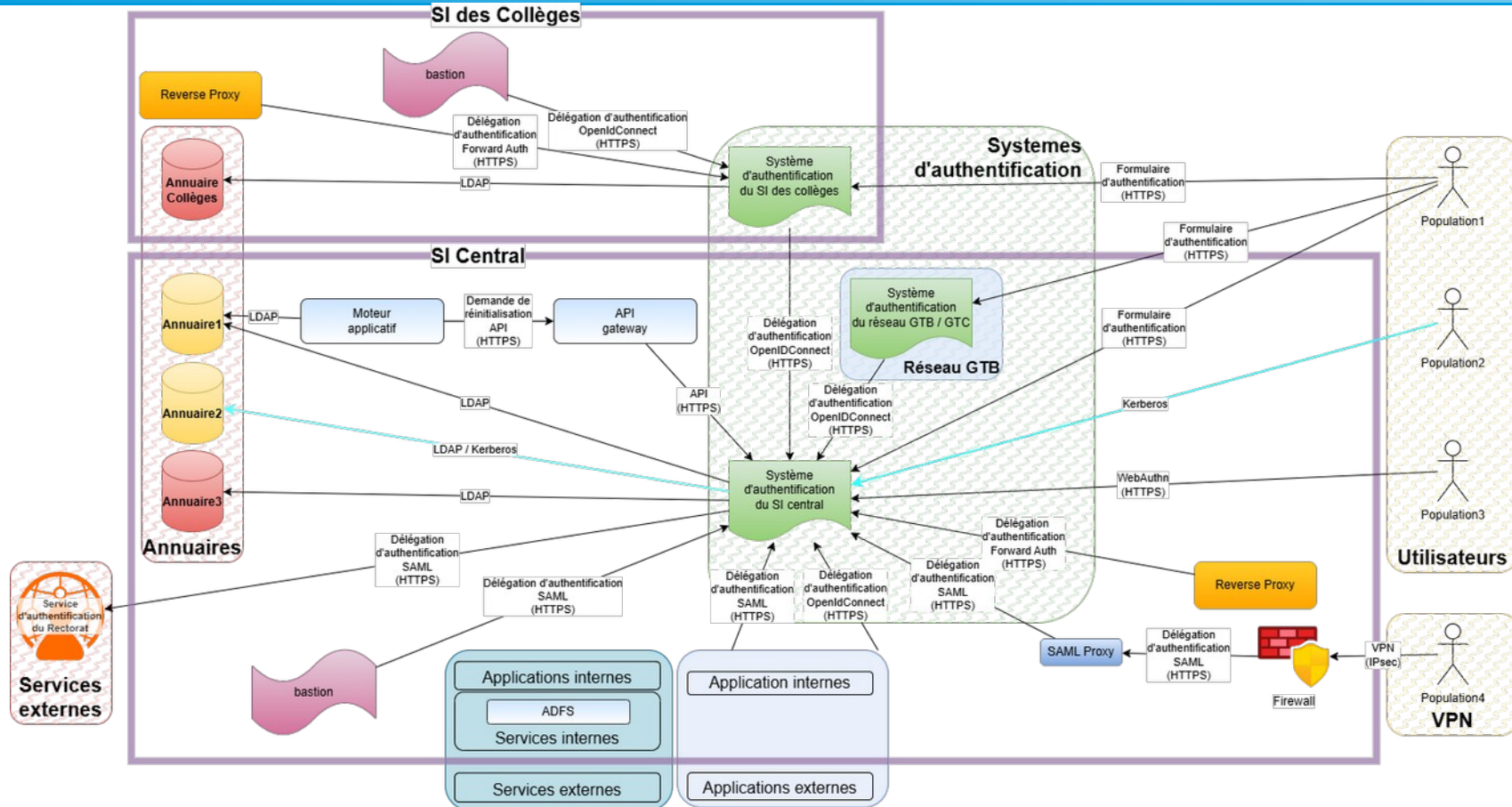
Solution mise en œuvre

LemonLDAP::NG + Traefik

- portail d'authentification
- portail applicatif
- fédération d'identités
- ~~portail de configuration du reverse proxy~~
- SSO
- Authentification multifacteurs



Architecture déployée



Portails d'Authentification



Bilan

Points positifs :

- Intégration réussi dans le SI
- Flexibilité et adaptabilité
- 2FA sur toutes les applications
- Moins de connections directes aux annuaires
- Centralisation de l'authentification des 3 SI
- Pas difficulté à connecter des applications web et mobile :
 - OpenID connect : 38
 - SAML : 13 dont VPN Forti
- Très bon accompagnement de Worteks :
 - Installation
 - Configuration
 - Formation

Points négatifs :

- Interface de configuration vieillissante
- Documentation pas toujours très claire ;-)

Autres solutions mises en œuvre

Collège : LSC



- Agrégation des annuaires AD des collèges
 - 180 actuellement, cible 194
 - Juste les informations nécessaires
- Authentification centralisée avec SSSD pour la connexion distante
- Script lancé toutes les 2 heures

SI Central : openLdap-ltb

- Annuaire des Partenaires et Intervenants
- Politique de mot de passe

SI Central : Self Service Password (SSP)

- Changement d'outil : Manage Engine
- Développement en cours, dispo en version 1.9 :
- Envoi d'un mail pour demander à l'utilisateur de saisir ses questions/réponses, mail perso, tel perso
- Envoi d'un mail pour l'expiration des mots de passe
- Format HTML pour les mails

Fonctionnalités souhaitées :

- Enrôler un TOTP
- Enrôler un WebAuthn

Annonces



- Assistant exploitant l'intelligence artificielle du Conseil Départemental de l'Isère
- Développement Interne
- Mise en disponibilité en open source :
 - <https://gitlab.adullact.net/iris/iris>
- Authentification OIDC via Lemonldap



- Où : La rampe Echirolles
- Quand : 23 Février 2027
- Thème : la transition et la transformation numérique par les modèles ouverts