

ANNEXE_A3_Note_technique_drasi_GTB

1. Objet de la note	2
2. Principes généraux d'architecture	2
2.1 GTB « Sûreté » (existante)	2
2.2 GTB « Technique » (nouvelle architecture)	3
3. Architecture réseau	4
3.1 Schéma	4
3.2 Segmentation logique	4
3.3 Interconnexion des sites distants	4
3.4 Gestion des flux	4
4. Exigences techniques - Réseau et protocoles	5
4.1 Protocoles de communication	5
4.2 Connectique et câblage	6
Standard de câblage	6
Recette et certification des liaisons	6
4.3 Continuité d'alimentation	6
5. Exigences de cybersécurité	7
5.1 Maîtrise des flux et cloisonnement	7
5.2 Sécurité des équipements et serveurs	7
5.3 Gestion des accès	7
5.4 Maintien en condition de sécurité	8
5.5 Modalités d'intervention du titulaire	8

1. Objet de la note

La présente note a pour objet :

- d'exposer l'architecture réseau cible de la GTB du bâtiment Clemenceau ;
- de préciser les principes de segmentation entre GTB technique et GTB sûreté ;
- de définir les exigences en matière de connectivité, câblage, sécurité et interopérabilité
- d'assurer la cohérence avec l'architecture réseau du rectorat et des sites distants.

2. Principes généraux d'architecture

L'architecture cible repose sur une séparation claire entre :

2.1 GTB « Sûreté » (existante)

Périmètre :

- Vidéosurveillance ;
- Contrôle d'accès.

Principe retenu :

En se basant sur le guide de "Recommandation sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection" de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) :

Les dispositifs de contrôle d'accès et de vidéoprotection présentent des niveaux d'exposition souvent élevés compte tenu de leur emplacement et de leur accessibilité. Ces dispositifs représentent donc une porte d'entrée significative pour une intrusion dans le système d'information de l'entité, notamment lorsque le réseau support ou le réseau fédérateur de ces dispositifs est partagé avec d'autres composants du SI. Les SI liés au contrôle d'accès physique et à la vidéoprotection doivent donc être considérés comme des SI à part entière, distincts du SI de l'entité.

R10

Cloisonner physiquement les SI de contrôle d'accès et de vidéoprotection

Les SI de contrôle d'accès et de vidéoprotection doivent être cloisonnés des autres composants du système d'information de l'entité. Il est hautement recommandé qu'un cloisonnement physique (câblage et équipements réseau dédiés) soit privilégié par rapport à un cloisonnement logique (VLAN par exemple), dont le niveau de robustesse peut être insuffisant dans ce contexte.

Cloisonner logiquement les SI de contrôle d'accès et de vidéoprotection

À défaut d'un cloisonnement physique, il est recommandé de cloisonner logiquement les SI de contrôle d'accès et de vidéoprotection par rapport aux autres composants du SI de l'entité en mettant en œuvre des mécanismes de filtrage, de chiffrement et d'authentification de réseau reposant sur le protocole IPsec. La mise en œuvre du protocole IPsec doit être conforme aux recommandations du guide de l'ANSSI [7].

- Maintien sur un réseau physiquement isolé ;
- Aucune interconnexion logique avec le réseau du rectorat ;
- Infrastructure indépendante (switches, câblage, serveurs dédiés).

Les serveurs (acquisition, installation, maintenance et support) sont à la charge du prestataire ou soumissionnaire durant toute la durée du marché. Aucune technologie d'accès à distance ne sera implémentée nativement sur les équipements (5G/4G, wifi etc.). Le prestataire fournira les cordons de brassage de cat. 6A minimum.

Les équipements actifs (switches) sont à la charge de la DRASI.

Objectif :

- Garantir une étanchéité complète entre le SI administratif et les systèmes de sûreté ;
- Réduire la surface d'attaque cyber ;
- Maintenir la conformité aux exigences de sécurité.

2.2 GTB « Technique » (nouvelle architecture)

Périmètre :

- CVC (chauffage, ventilation, climatisation) ;
- Éclairage ;
- Comptages énergétiques ;
- Automatismes techniques ;
- Supervision énergétique conforme BACS.

Principe retenu :

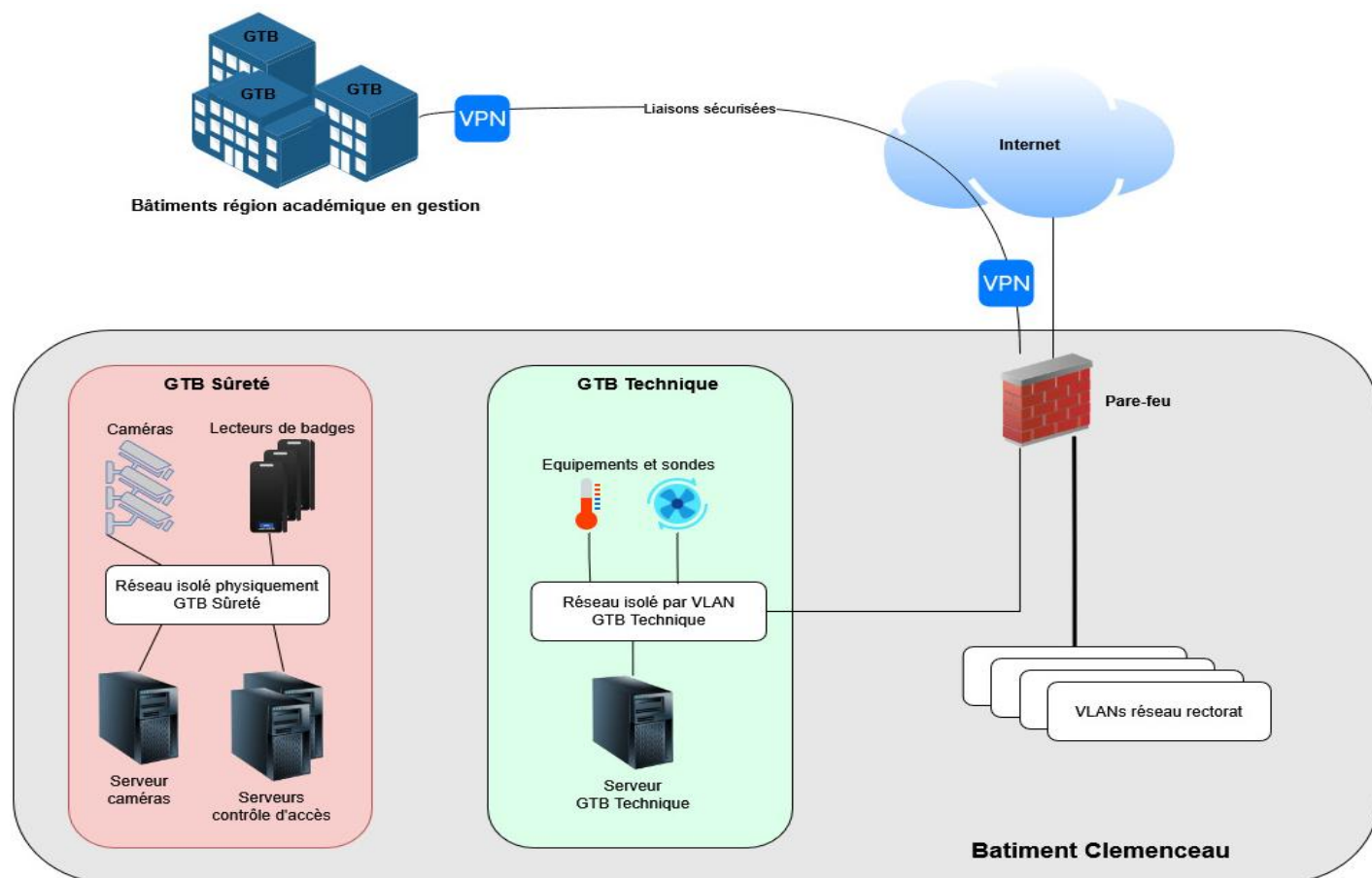
- Création d'un VLAN dédié GTB Technique ;
- Raccordement contrôlé au réseau du rectorat ;
- Filtrage strict via pare-feu ;
- Interconnexion avec les autres bâtiments via VPN existants.

Objectif :

- Permettre une GTB communicante ;
- Centraliser la supervision ;
- Permettre l'exploitation depuis les postes de la DRI ;
- Assurer le suivi énergétique multi-sites.

3. Architecture réseau

3.1 Schéma



3.2 Segmentation logique

Le titulaire devra intégrer la GTB technique dans un VLAN dédié fourni par la DRASI.

Les règles suivantes s'appliquent :

- les adresses IP seront définies par la DRASI ;
- aucun accès vers la GTB sûreté ;
- filtrage des flux inter-VLAN via pare-feu ;
- principe du moindre privilège appliqué à l'ensemble des communications.

3.3 Interconnexion des sites distants

Les bâtiments distants concernés par ce projet GTB (10 à 12 sites gérés par la DRI) sont interconnectés via des VPN existants administrés par la DRASI.

La GTB technique devra :

- utiliser ces liaisons VPN ;
- fonctionner sans nécessiter d'ouverture directe vers Internet ;
- permettre une segmentation logique par site ;

3.4 Gestion des flux

Les flux devront être :

- documentés (matrice des flux obligatoire) ;
- priorisés si nécessaire (QoS) ;
- limités aux seuls services indispensables :
 - supervision,
 - historisation,
 - synchronisation horaire,
 - sauvegardes,
 - administration contrôlée,
 - mises à jour.

Toute matrice de flux devra être validée par la DRASI avant mise en production.

4. Exigences techniques - Réseau et protocoles

4.1 Protocoles de communication

Les équipements devront utiliser exclusivement des protocoles ouverts normalisés (maintenus à jour en cas d'obsolescence et pérenne dans le temps) :

- BACnet/IP
- Modbus TCP
- KNX IP

Les exigences suivantes s'appliquent :

- favorisation d'un protocole sécurisé ;
- justification du choix du protocole ;
- activation des mécanismes de sécurisation natifs (ex. BACnet Secure Connect si disponible) ;
- désactivation des services et ports non utilisés ;
- documentation exhaustive des objets, points et variables exposés ;
- interdiction de protocoles propriétaires fermés non documentés ;
- tout protocole devenu obsolète devra être remplacé par son successeur.

Exigence de pérennité et cycle de vie des équipements

Le titulaire devra garantir la pérennité des matériels proposés :

- Les équipements ne devront pas être en fin de vie (EOL – End Of Life) ;
- Le candidat devra fournir une attestation constructeur précisant :
 - date de fin de commercialisation ;
 - date de fin de support ;
 - durée prévisionnelle de disponibilité des mises à jour de sécurité ;
 - disponibilité des pièces détachées.
- La durée minimale de **maintien en condition opérationnelle devra être de 10 ans** ;
- Toute solution reposant sur une technologie susceptible d'être abandonnée devra être explicitement justifiée ;

- Le titulaire devra proposer une stratégie de migration en cas d'obsolescence anticipée.

4.2 Connectique et câblage

Le titulaire devra prévoir :

Étude détaillée des besoins de raccordement

- réaliser une étude détaillée des besoins de raccordement ;
- indiquer explicitement dans son offre le nombre de prises réseau RJ45 nécessaires au raccordement de l'ensemble des équipements de la GTB technique ;
- préciser la localisation prévisionnelle de chaque prise ;
- fournir un schéma de principe d'implantation des équipements et de leur raccordement réseau ;
- fournir des câbles **Cat 6A** de longueur 1, 2 et 3 ml et **de couleur bleu** pour différencier visuellement les jarretières « GTB » dans les locaux techniques ;
- intégrer une réserve de capacité minimale de 20 % pour évolutions futures.

Câblage cuivre

- catégorie 6A minimum ;
- respect des longueurs normatives ;
- repérage normalisé.

Standard de câblage

- préciser le standard retenu (T568A ou T568B) ;
- garantir l'homogénéité sur l'ensemble de l'installation ;
- documenter le plan de brassage ;
- intégrer une réserve de capacité minimale de 20 %.

Recette et certification des liaisons

- Chaque liaison cuivre devra faire **l'objet d'une certification Cat 6A minimum**.
- Un rapport de recette (type Fluke ou équivalent) devra être fourni en DOE.
- Les mesures devront inclure :
 - longueur ;
 - affaiblissement ;
 - NEXT / PSNEXT ;
 - conformité aux normes en vigueur.
- L'absence de rapport de recette conforme pourra entraîner la non-validation des prestations concernées.

4.3 Continuité d'alimentation

Les éléments critiques devront être protégés par onduleur rackable (existant ou à prévoir) :

- serveurs GTB ;
- automates principaux ;

Autonomie minimale à définir selon criticité.

5. Exigences de cybersécurité

La GTB constitue un système industriel connecté (OT raccordé au SI).

À ce titre, elle devra respecter les principes de cybersécurité définis par le maître d'ouvrage et la DRASI.

Les exigences décrites au présent article viennent compléter les dispositions d'architecture réseau définies à l'article 3.

5.1 Maîtrise des flux et cloisonnement

Le titulaire devra :

- formaliser une matrice complète des flux (source, destination, protocole, port, justification) ;
- limiter strictement les flux aux besoins fonctionnels identifiés ;
- documenter toute communication inter-systèmes ;
- permettre la journalisation des connexions (**6 mois minimum**) ;
- garantir l'absence de flux non maîtrisé vers Internet.

Aucun équipement de la GTB ne devra initier de communication externe non validée par la DRASI.

5.2 Sécurité des équipements et serveurs

Les équipements devront permettre :

- permettre une authentification par comptes nominatifs ;
- intégrer une gestion des profils (administrateur / exploitant / lecture seule) ;
- assurer la traçabilité des actions ;
- imposer le changement des mots de passe par défaut ;
- supporter le chiffrement TLS 1.2 minimum ;
- permettre la désactivation des services non sécurisés (Telnet, HTTP non chiffré, SNMPv1/v2c, etc.).

5.3 Gestion des accès

Accès internes (DRI)

- accès via le réseau rectorat ;
- accès HTTPS sécurisé ;
- authentification forte obligatoire (MFA - Multi-Factor Authentication), compatible avec les standards de sécurité rectorat ;
- journalisation des connexions (**6 mois minimum**).
- compatibilité avec annuaire centralisé si possible ;
- traçabilité des connexions ;
- impossibilité de comptes partagés ;
- désactivation automatique des comptes inactifs.

Accès prestataires

- aucun accès permanent autorisé ;
- accès distant uniquement sur demande validée ;
- appel téléphonique au cours duquel le code OTP sera donné oralement, la première partie du code (fixe) étant connue du prestataire seul ;
- deux comptes techniques (un géré par la DRI et un par la DRASI) associés chacun à une clé d'authentification forte ;
- tenue à jour de liste des personnels habilités à prendre la main à distance (on ne donnera pas le code OTP à une personne non présente dans la liste) ;
- traçabilité complète des interventions ;
- suppression immédiate des accès en fin d'intervention.

5.4 Maintien en condition de sécurité

Le titulaire devra fournir :

- une procédure de gestion des mises à jour ;
- une politique de correction des vulnérabilités ;
- un engagement de support et de correctifs ;
- une documentation des versions logicielles et firmwares.
- engagement contractuel de notification des vulnérabilités sous 72h ;
- délai maximal de correction des failles critiques ;
- obligation de compatibilité TLS 1.2 minimum (TLS 1.3 privilégié) ;
- interdiction d'équipements nécessitant des services non sécurisés activés par défaut.

5.5 Modalités d'intervention du titulaire

Le titulaire pourra intervenir selon deux modalités encadrées :

1. Intervention physique in situ

- accès autorisé uniquement après validation du maître d'ouvrage ;
- enregistrement obligatoire en main courante ;
- production d'un compte rendu détaillé sous 48h ;
- suppression immédiate des accès temporaires créés.

2. Intervention distante sécurisée

Toute intervention distante devra :

- utiliser exclusivement l'architecture VPN DRASI ;
- interdire toute ouverture directe vers Internet ;
- recourir à une authentification forte (MFA) ;

- utiliser des comptes techniques ;
- être limitée dans le temps ;
- être journalisée intégralement (**6 mois minimum**) ;
- faire l'objet d'une validation préalable.

Aucun accès permanent ne sera autorisé.

3. Convention tiers de confiance

Lorsque l'accès distant est nécessaire :

- **signature d'une convention de tiers de confiance ;**
- définition précise des responsabilités ;
- encadrement du périmètre technique ;
- obligation de suppression des accès après intervention.