# Solutions LM Control dans une infrastructure informatique

## Classification

☐ Document public

Document sans limitation de stockage et de diffusion

☒ Document restreint aux acteurs

Disponible en interne aux collaborateurs désignés, peut être diffusé en interne par mail, peut être imprimé et sauvegardé sur support amovible mais uniquement stocké dans les locaux sous contrôle d'accès.

☐ Document confidentiel

Obligatoirement protégé par un mot de passe, interdiction d'imprimer, de copier sur un support amovible non chiffrée et/ou de diffuser par mail non-chiffré

## Historique du Document

| Version | Date | Nom | Fonction | Objet |
|---|---|---|---|---|
| V.4.1 | Le 17/01/25 | NDIAYE Cheikh<br>ROMAN Christophe | Chef de Projet<br>Resp. Technique | MàJ ports marque blanche |
| V.4.0 | Le 08/01/25 | NDIAYE Cheikh<br>ROMAN Christophe | Chef de Projet<br>Resp. Technique | Mise à jour plage des ports |
| V.3.0 | Le 24/10/24 | NDIAYE Cheikh<br>ROMAN Christophe | Chef de Projet<br>Resp. Technique | Généralisation pour toutes les activités CB LM Control |
| V.2.1 | Le 10/06/24 | NDIAYE Cheikh | Chef de Projet | Plage de ports FTPS étendue |
| V.2.1 | Le 19/06/24 | NDIAYE Cheikh | Chef de Projet | Plage de ports FTPS étendue |
| V.2.1 | Le 17/02/22 | NDIAYE Cheikh | Chef de Projet | 1ère rédaction du document |

Ce document définit les règles de pare-feu à mettre en place dans une Infrastructure réseau (en fonction de l'activité bancaire), pour le bon fonctionnement des Solutions LM Control.

Il est à destination du DSI.

# 1. Utilisation d'un système bancaire sur un réseau d'entreprise

Il n'existe aucune contrainte sécuritaire pour une entreprise à autoriser un tiers à utiliser son réseau informatique pour la transmission des flux financiers.

**Sécurité logicielle :**
Les applications installées dans le matériel bancaire INGENICO sont étanches, sécurisées et signées. Toute action non autorisée met hors service le matériel.

**Sécurité réseau :**
Le système bancaire Ingenico de gamme Telium se connecte uniquement au serveur bancaire avec un paramétrage fixe.

Dans aucun cas le système bancaire accède ou a besoin d'accéder au réseau interne de votre site.

Le matériel Ingenico sous base Telium peut fonctionner en DHCP ou en IP fixe.

En résumé, le service informatique a la possibilité :

- De mettre en place des VLAN
- De mettre en place une solution de translation d'adresse réseau (SNAT)
- De mettre en place un filtrage par adresse MAC pour identifier le matériel
- D'autoriser l'accès internet uniquement à la passerelle monétique et au port utilisé
- Les autres ports peuvent être fermés et les autres adresses IP interdites
- De créer un sous réseau IP réservé au système bancaire.

Bande passante utilisée par le système bancaire :
Le système bancaire communique quelques kilo-octets par jour. (2Mo/mois)

## 2. Intégration de la solution LM Control dans une infrastructure réseau

Si vous souhaitez vous connecter au réseau LAN de l'Entreprise :

Vous avez plusieurs possibilités pour assurer la continuité et le bon fonctionnement de votre infrastructure.

Vous pouvez par exemple mettre en place un VLAN pour séparer les flux et ainsi bloquer toute communication entre les 2 réseaux.

De plus nos solutions ont des adresses IP avec des ports fixes. Et avec la mise en place de SNAT (translation d'adresse réseau) et les règles de trafic sortant, vous disposez d'un contrôle déclaratif complet sur la connectivité internet sortante. Vous pourrez tout verrouiller et juste nous donner accès à notre équipement depuis l'extérieur (Virtual_host) et nous le joindrons via une règle de pare feu avec des ports spécifiques que nous vous communiquerons.

- Les communications avec nos appareils sont toujours sortantes. Il n'y a pas de risque pour votre infrastructure. Ils communiquent vers nos serveurs.
- Nous pourrons aussi vous donner l'adresse mac de nos équipements de sorte à faire un filtrage par adresse Mac (pour allouer ou non l'accès à votre réseau).
- Avec toutes ces préconisations, nous pourrons nous brancher sur votre réseau sans affecter votre activité, ou votre sécurité.
- À noter que l'impact sur votre bande passante sera quasi insignifiant (la Bande Passante d'un bancaire est d'environ 2 Mo pour 1000 transactions

## 3. Adresses IP et ports LM Control en fonction des activités CB

Ci-dessous, l'ensemble des adresses IP et ports que nous utilisons en fonction de nos activités CB.

| Activité CB | Service | Adresse IP / URL | Port |
|---|---|---|---|
| **Bancaire Autonome** | Passerelle Bancaire Payview (primaire) | 15.236.14.32 | 40005 **(Ou*Port Marque Blanche dédié)** |
| | Passerelle Bancaire Payview (secondaire) | 15.236.147.23 | 40005 **(Ou*Port Marque Blanche dédié)** |
| | TEM | 35.195.97.84 | 7019 |
| | Tetra Connect | tetra-connect.com | 443 |
| | Serveur de temps | time.nist.gov | 123 |

*Port Marque Blanche dédié : Si vous avez souscrit à la marche Blanche sur Payview, un port spécifique vous sera attribué et communiqué.

| Activité CB | Service | Adresse IP / URL | Port |
|---|---|---|---|
| **TOUCH' N PAY** | All In One Data Control | 85.90.48.5 | 990 ; 50000 à 53000 (pour FTPS) |
| | Touch' N Pay | www.touchnpay.fr | 443 ; 80 |
| | TEM | 0.debian.pool.ntp.org<br>1.debian.pool.ntp.org<br>2.debian.pool.ntp.org<br>3.debian.pool.ntp.org | 123 |
| | TeamViewer | *teamviewer.com | 5938 ; 443 ; 80 |

| Activité CB | Service | Adresse IP / URL | Port |
|---|---|---|---|
| **PAYZILY / AZTEK** | Payzily | api.licences.payzily.com | 8445 |
| | Payzily | www.payzily.com | 8444 |

| Activité CB | Service | Adresse IP / URL | Port |
|---|---|---|---|
| **Axis** | Serveur Axis primaire | 91.208.214.1 | 42999 |
| | Serveur Axis secondaire | 91.208.214.2 | 42999 |
| | Serveur TMS (Mises à jour) | 91.208.214.34 | 7004 |
| | Serveur de temps | time.nist.gov | 123 |

| Activité CB | Service | Adresse IP / URL | Port |
|---|---|---|---|
| **Full Offer** | Serveur Axis primaire | 91.208.214.1 | 42194 |
| | Serveur Axis secondaire | 91.208.214.2 | 42194 |
| | Serveur TMS (Mises à jour) | 91.208.214.34 | 7004 |
| | Serveur de temps | time.nist.gov | 123 |

| Activité CB | Service | Adresse IP / URL | Port |
|---|---|---|---|
| **PAYZILY PROD** | Izly | 85.90.48.170 | 5167 |
| | Izly | periph.izly.fr | 443 |

| Activité CB | Service | Adresse IP / URL | Port |
|---|---|---|---|
| **APPLICATION DE FACTURATION PAR QR CODE** | Facturation QR Code | qr-invoice.touchnpay.fr | 9022 |