# Resilience et Maîtrise grâce à l'Isolation Réseau

LIVRE BLANC



seclab-security.com

# Sommaire

# Introduction

Dans le paysage numérique hyperconnecté d'aujourd'hui, les organisations font face à des défis sans précédent en cybersécurité. À mesure que les systèmes deviennent de plus en plus interconnectés, la surface d'attaque s'étend de façon exponentielle, créant de nouvelles vulnérabilités exploitées rapidement par des attaquants sophistiqués.

**8.4 trillon $**

**Le coût mondial de la cybercriminalité a atteint environ 8,4 trillions de dollars en 2023 : un chiffre qui englobe les pertes directes, les coûts de réparation, les interruptions d'activité et les dommages à la réputation.**

*Source : Cybersecurity Ventures*

Ce paysage de menaces en constante évolution, accéléré par les progrès de l'intelligence artificielle et la professionnalisation des cybercriminels, exige des stratégies de protection robustes pour les infrastructures critiques et les systèmes sensibles. Bien que les approches traditionnelles de sécurité, telles que les Firewalls aient longtemps été des mesures défensives standards, elles montrent de plus en plus leurs limites face aux menaces persistantes avancées et aux méthodologies d'attaques sophistiquées (APT).

L'isolation réseau est devenue un paradigme de sécurité essentiel pour protéger les systèmes sensibles contre les menaces externes. Mais qu'est-ce qui constitue exactement une isolation efficace en cybersécurité ? En quoi diffère-t-elle de la simple segmentation ? Et comment les organisations peuvent-elles atteindre une véritable isolation réseau sans sacrifier la fonctionnalité opérationnelle requise dans les environnements interconnectés d'aujourd'hui ?

Ce livre blanc explore ces questions et présente la technologie d'Isolation Électronique révolutionnaire de SECLAB : une approche innovante qui offre une isolation réseau complète tout en permettant la communication bidirectionnelle essentielle aux opérations modernes.

# Ségrégation réseau : Un besoin réel

## Comprendre la ségrégation réseau

La ségrégation réseau constitue une stratégie de sécurité fondamentale consistant à séparer physiquement différents environnements réseau afin d'empêcher les mouvements latéraux de menaces et les accès non autorisés entre systèmes. Contrairement à la segmentation, qui ne divise les réseaux que logiquement à l'aide de contrôles virtuels, la véritable ségrégation établit des zones réseau distinctes, reliées uniquement par des interfaces contrôlées et supervisées.

La ségrégation réseau crée ainsi des zones isolées au sein du réseau, dans lesquelles les données et les activités des utilisateurs sont confinées. Si un segment venait à être compromis, cette isolation empêcherait la propagation de la menace, limitant considérablement l'impact d'un incident de sécurité. Lorsqu'elle est correctement mise en oeuvre, la ségrégation réseau permet :

- La prévention des mouvements latéraux lors d'attaques
- Le confinement des systèmes compromis
- La protection des données sensibles contre tout accès non autorisé
- La réduction de la surface d'attaque des systèmes critiques
- Une meilleure conformité aux exigences réglementaires

## Exigences règlementaires en matière de ségrégation réseau

La ségrégation réseau est devenue une exigence fondamentale dans de nombreux cadres réglementaires et normes internationales en matière de cybersécurité, parmi lesquels :

- **IEC 62443 :** Normes internationales relatives à la sécurité des systèmes d'automatisation et de contrôles industriels, imposant la segmentation et la ségrégation des réseaux.
- **NERC CIP Standards :** Normes obligatoires de fiabilité pour les opérateurs du réseau électrique nord-américain, définissant des exigences d'isolation réseau.
- **Directives NIS/NIS2 :** Réglementations européennes imposant aux fournisseurs d'infrastructures critiques de mettre en œuvre des mesures de sécurité appropriées, incluant la ségrégation réseau.
- **DORA (Règlement sur la résilience opérationnelle numérique) :** Règlementation européenne exigeant des entités financières la mise en place d'une gestion robuste des risques liés aux technologies de l'information et de la communication (TIC).

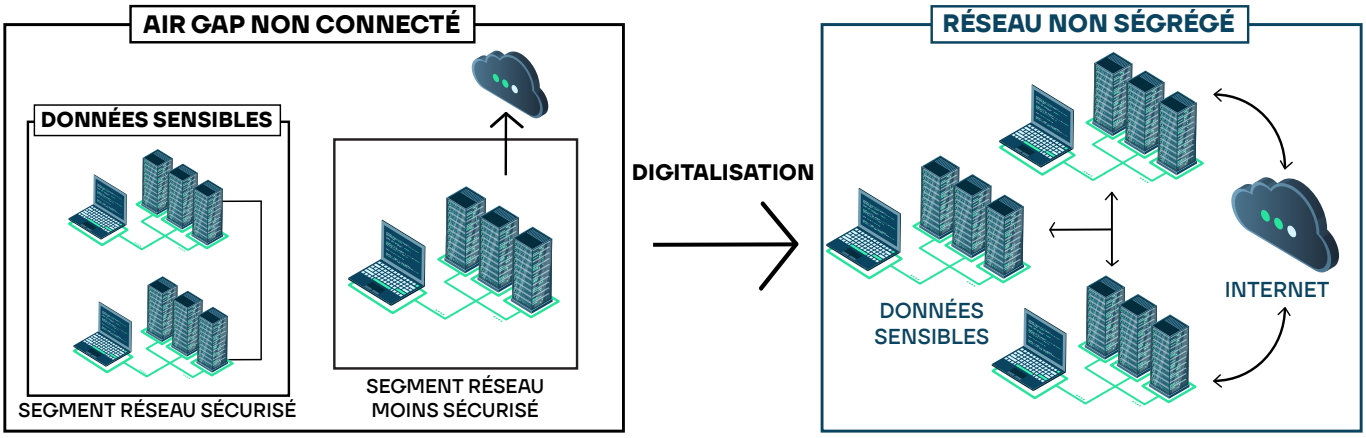
## Les limites des Air Gaps physiques

Traditionnellement, les environnements les plus sécurisés reposaient sur des air gaps physiques : des réseaux totalement déconnectés, sans aucun canal de communication numérique entre les systèmes.

Bien que cette approche offre un niveau de sécurité très élevé, elle engendre d'importants défis opérationnels :

- Impossibilité de partager des données en temps réel entre environnements
- Transferts de données manuels inefficaces et chronophages
- Coûts opérationnels accrus et besoins renforcés en personnel
- Frein à la transformation numérique et aux efforts de modernisation
- Risque d'erreur humaine lors des transferts manuels

Avec l'accélération de la transformation numérique dans tous les secteurs, la mise en œuvre stricte d'un air gap physique devient de plus en plus impraticable. Cette évolution pousse les organisations à rechercher des solutions offrant un niveau de sécurité équivalent, tout en apportant davantage de flexibilité opérationnelle.




*Réseau connecté et non ségrégé à la suite de la digitalisation*

# Les Firewalls n'isolent pas, ils filtrent

## La nature filtrante des Firewalls

Les Firewalls représentent la technologie de sécurité réseau la plus répandue, mais il est essentiel d'en comprendre les limites fondamentales. De par leur conception, les Firewalls sont des dispositifs de routage sophistiqués qui filtrent le trafic sur la base de règles prédéfinies.

Lorsqu'un paquet répond aux critères définis dans une règle de Firewall il est transmis tel quel vers sa destination. Cette caractéristique de conception fondamentale implique que les Firewalls :

- Autorisent des connexions réseau directes entre des environnements séparés
- Conservent la structure d'origine des paquets réseau à travers les frontières
- Créent des canaux de communication bidirectionnels susceptibles d'être exploités
- Exposent l'ensemble de la pile protocolaire à d'éventuelles attaques

## Vulnérabilité inhérente au modèle du Firewall

Le modèle de sécurité des firewalls présente plusieurs faiblesses inhérentes :

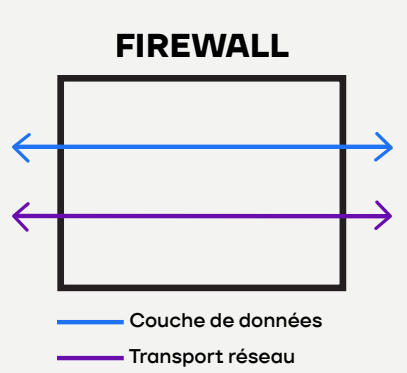
1. **Protection basée sur le logiciel :** les Firewalls reposent sur des configurations logicielles qui peuvent être vulnérables, mal configurées ou exposées à des attaques zero-day
2. **Mises à jour et correctifs nécessaires :** pour garantir la sécurité, les Firewalls exigent des mises à jour constantes, ce qui crée des fenêtres potentielles de vulnérabilité
3. **Complexité des règles :** à mesure que les jeux de règles deviennent plus complexes, le risque de mauvaise configuration augmente considérablement
4. **Exposition de la pile protocolaire :** en transmettant les paquets dans leur intégralité, les Firewalls exposent les piles réseau, pilotes et composants du système d'exploitation aux attaques
5. **Facilitation de la reconnaissance :** les Firewalls permettent souvent le trafic de scan réseau, ce qui aide les attaquants à cartographier les réseaux protégés

## Firewalls : conçus pour la segmentation et non la ségrégation

Il est essentiel de comprendre que les Firewalls n'ont jamais été conçus pour assurer une véritable ségrégation réseau. Leur fonctionnalité principale repose sur des interconnexions contrôlées via le filtrage des paquets, créant essentiellement une barrière perméable plutôt qu'une vraie frontière.

Cette distinction fondamentale explique pourquoi les Firewalls peuvent être contournés par :

- Menaces persistantes avancées opérant via des protocoles autorisés
- Vulnérabilités zero-day dans le logiciel du Firewall
- Jeux de règles complexes qui créent involontairement des failles de sécurité
- Techniques d'ingénierie sociale compromettant les identifiants
- Menaces internes malveillantes exploitant des accès légitimes




*Fonctionnement d'un Firewall*

# Data Diodes : dépassées et inadaptées

## Les origines et fonctionnements des Data Diodes

Les Data Diodes sont nées des besoins militaires et du renseignement en matière de flux d'informations unidirectionnels physiquement garantis. Cette technologie repose sur un principe simple : les données peuvent entrer, mais ne peuvent jamais sortir d'un environnement protégé.  Au coeur des Data Diodes, on retrouve :

- Une fibre optique avec un émetteur d'un côté et un récepteur de l'autre
- Un matériel qui garantit physiquement le flux unidirectionnel des données
- Aucun composant logiciel susceptible d'être compromis

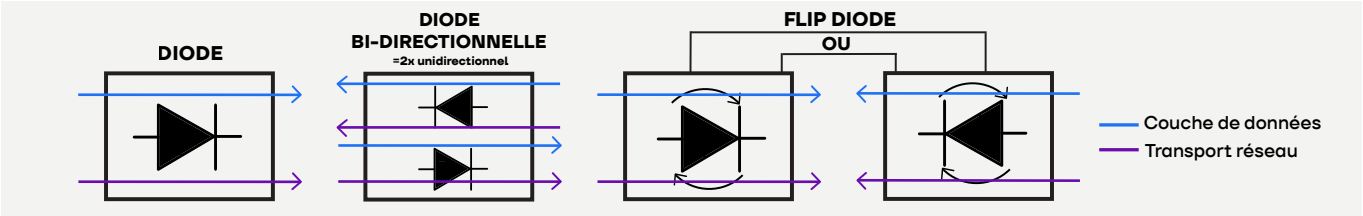
Cette approche matérielle offre une sécurité exceptionnelle pour des cas d'usage spécifiques, mais elle s'accompagne de limitations fonctionnelles importantes.

## La réalité unidirectionnelle des Data Diodes

Malgré les affirmations marketing concernant les «Data Diodes bidirectionnelles», ces solutions se classent invariablement dans l'une des trois catégories suivantes :

1. **Diodes unidirectionnelles doublées :** deux data diodes séparées permettant un flux unidirectionnel indépendant dans des directions opposées
2. **Diodes réversibles :** systèmes pouvant fonctionner dans l'une ou l'autre direction, mais jamais simultanément
3. **Architectures hybrides :** combinaisons de diodes avec des Firewalls air-gapped temporisés

Ces approches tentent de résoudre le problème fondamental des Data Diodes : leur incapacité intrinsèque à prendre en charge des protocoles bidirectionnels tels que TCP/IP, qui nécessitent des paquets d'acquittement.




*Différents types de fonctionnement des Data Diodes*

## Défis de compatibilité des protocoles

Les Data Diodes rencontrent des défis importants avec les protocoles réseau modernes :

**Implémentation UDP :**

- Nécessite des « passerelles » (ordinateurs) de chaque côté de la diode
- Permet l'adressage IP, mais entraîne la perte des paquets de réponses UDP
- Fonctionne correctement uniquement pour les communications sans état

**Gestion du TCP/IP :**

- Nécessite des proxies compatibles avec le protocole de part et d'autre
- La passerelle d'entrée doit simuler les réponses aux clients
- La passerelle de sortie ne peut initier que de nouvelles connexions vers les serveurs
- Les réponses des serveurs reçues par la passerelle de sortie doivent être ignorées
- Limitation aux protocoles spécifiquement pris en charge

Pour les communications chiffrées, les Data Diodes rencontrent des défis encore plus importants, car elles perturbent l'échange bidirectionnel des clés asymétriques nécessaire aux protocoles de chiffrement modernes. Cela oblige les organisations à choisir entre :

- Échanger manuellement les clés de chiffrement (au détriment de la sécurité)
- Utiliser la Data Diode elle-même comme point de terminaison cryptographique (créant une nouvelle surface d'attaque)
- Mettre en œuvre des contournements complexes avec prise en charge limitée des protocoles

# Isolation Électronique SECLAB : Un changement de paradigme

## Une technologie née d'une nécessité opérationnelle

La technologie d'Isolation Électronique de SECLAB est née d'un besoin critique exprimé par des clients industriels : comment concilier la sécurité d'une isolation physique des réseaux avec la maintien de la fonctionnalité opérationnelle des communications bidirectionnelles.

Développée et perfectionnée au cours de plus d'une décennie de déploiements dans les environnements les plus exigeants (installations militaires, sites nucléaires, systèmes de contrôle ferroviaires et infrastructures hydroélectriques), cette technologie brevetée constitue une avancée fondamentale en matière de sécurité réseau.

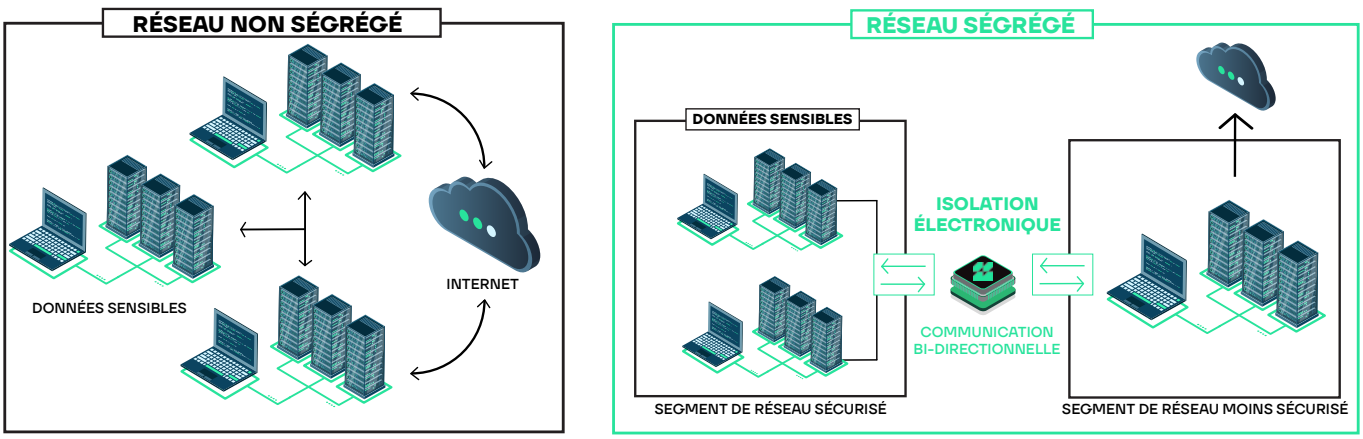
*Secure Xchange Network Seclab*

## L'avantage de l'Isolation Électronique

La technologie d'Isolation Électronique de SECLAB, intégrée à la gamme de produits SecXN, offre une véritable ségrégation réseau grâce à une approche révolutionnaire :

1. **Rupture protocolaire complète** : Plutôt que de se limiter à filtrer les paquets, SecXN supprime complètement et reconstruit les protocoles réseau (couches OSI 1 à 4)
2. **Intégrité des données applicatives :** Bien que les couches réseau soient détruites et reconstruites, les données applicatives (couches 5 à 7) restent intactes, permettant une fonctionnalité complète
3. **Sécurité assurée par le matériel :** Ce processus s'effectue au niveau matériel, grâce à des circuits électroniques spécialisés, plutôt que par des composants logiciels vulnérables

Cette approche crée de manière efficace un « air gap électronique » entre les réseaux, tout en permettant un échange de données contrôlé, offrant une sécurité comparable à celle de l'isolation physique, avec les avantages opérationnels de l'interconnexion.




*Réseau ségrégé avec communication bidirectionnelle via l'Isolation Électronique comparé à un réseau connecté non ségrégé*

## Comment l'Isolation Électronique fonctionne

SecXN met en œuvre la technologie d'Isolation Électronique à travers un processus en trois étapes:

| Phase 1 : Supression | Phase 2 : Transmission | Phase 3 : Reconstruction |
|---|---|---|
| Chaque paquet IP provenant du réseau source voit ses couches 1 à 4 complètement supprimées, ne laissant que la charge utile de l'application (couches 5 à 7). | La charge utile passe par un canal matériel dédié, sans aucune information de transport. | De nouvelles couches réseau propres (couches 1 à 4) sont générées et associées aux données applicatives originales avant leur transmission vers le réseau de destination. |

Ce processus breveté garantit que :

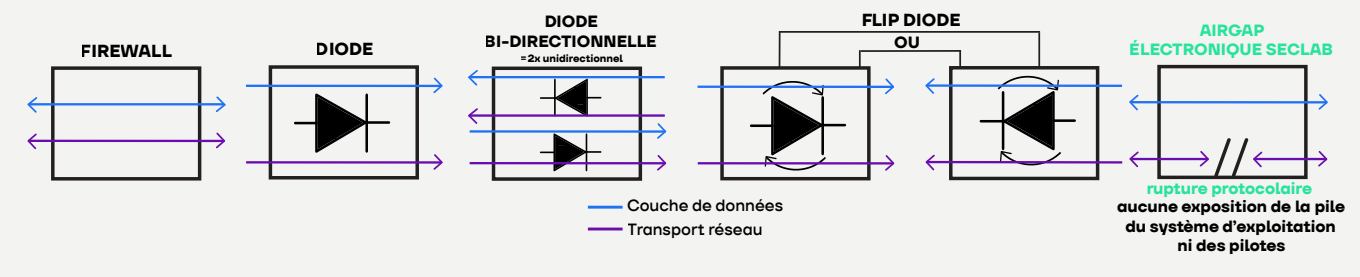
- Aucun paquet réseau d'origine ne traverse jamais la frontière
- Les attaques au niveau transport ne peuvent pas pénétrer dans le réseau protégé
- La reconnaissance réseau devient impossible
- Les piles IP du système d'exploitation, pilotes et firmwares réseau restent protégés
- Les applications fonctionnent normalement sans nécessiter de modification

## Communications bidirectionnelles avec une isolation totale

Contrairement aux Data Diodes, la technologie d'Isolation Électronique de SECLAB prend en charge de véritables communications bidirectionnelles sans compromettre la sécurité :

- **Prise en charge complète du TCP/IP :** Permet des communications TCP/IP bidirectionnelles sans personnalisation spécifique aux protocoles
- **Compatibilité avec les protocoles chiffrés :** Fonctionne parfaitement avec VPN, SSH, HTTPS et autres protocoles sécurisés
- **Support natif des applications :** Aucune modification des applications ni proxy spécial requis
- **Contrôle de direction :** Permet aux administrateurs de définir quel côté peut initier la connexion pour chaque flux

Cette capacité unique résout la limitation fondamentale des Data Diodes, tout en offrant une sécurité supérieure à celle des Firewalls.




*Comparaison des fonctionnements d'un Firewall, Data Diodes et de l'Isolation Électronique Seclab*

# Analyse Comparative : Firewalls, Data Diodes et Isolation Électronique

## Analyse des besoins clients

Les organisations modernes expriment trois exigences de sécurité essentielles qui mettent en évidence les limites des approches traditionnelles :

**Besoin d'une garantie absolue qu'aucun trafic réseau ne pourra jamais pénétrer dans le réseau OT**

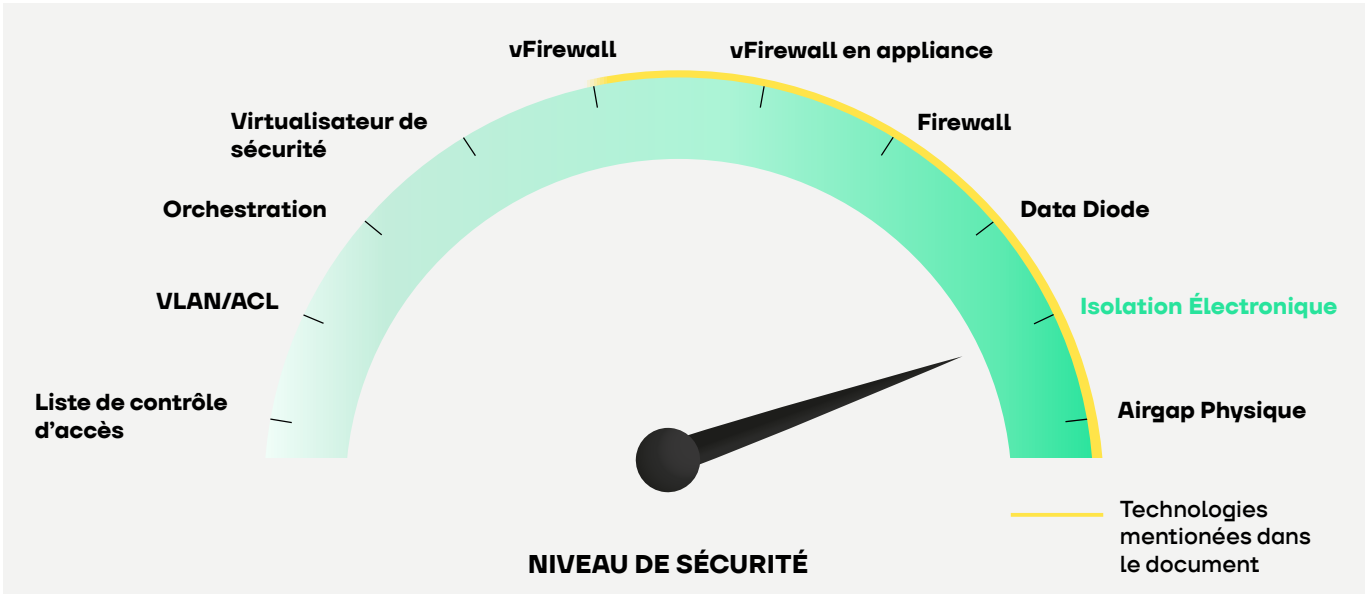
- Firewalls : Ne peuvent pas offrir cette garantie en raison de leur architecture fondée sur le filtrage du trafic
- Data Diodes : Répondent à cette exigence d'isolation, mais au prix d'une communication strictement unidirectionnelle, limitant ainsi les échanges essentiels
- Isolation Électronique : Garantie d'isolation totale tout en permettant une communication pleinement bidirectionnelle et sécurisée

**Besoin de contrôler les interconnexions réseaux**

- Firewalls : Complexité importante lors du déploiement et de la maintenance et restent sujets à des vulnérabilités logicielles
- Data Diodes : Contrôle limité et uniquement dans un sens de communication
- Isolation Électronique : Contrôle complet des échanges grâce à une administration double (une par zone)

**Besoin d'utiliser des services TCP/IP standards entre deux réseaux qui ne doivent pas être interconnectés**

- Firewalls : Point de défaillance unique (SPOF) sur le plan de la cybersécurité
- Data Diodes : Passerelles spécifiques nécessaires pour fonctionner avec TCP/IP, contraintes sur les protocoles utilisés et tout mécanisme d'acquittement bloqué
- Isolation Électronique : Compatibilité totale avec les protocoles TCP/IP et UDP/IP, séparation infaillible garantie, aucune vulnérabilité ne peut compromettre la ségrégation




*Jauge du niveau de sécurité selon les différentes technologies*

Les trois tableaux suivants présentent une analyse comparative selon trois axes : l'architecture de sécurité, les capacités opérationnelles et la protection contre les menaces, pour les Firewalls, les Data Diodes et la solution d'Isolation Électronique de SECLAB.

## Comparaison des Architectures de Sécurité

| Caractéristiques | Firewalls | Data Diodes | Isolation Électronique SECLAB |
|---|---|---|---|
| **Modèle de Sécurité** | Filtrage logiciel | Flux unidirectionnel matériel | Rupture protocolaire matérielle |
| **Support des protocoles** | Bidirectionel complet ✓ | Unidirectionel limité | Bidirectionel complet ✓ |
| **Exposition au réseau** | Connectivité réseau directe | Pas de chemin retour | Isolation réseau complète ✓ |
| **Vulnerabilité aux exploits logiciels** | Elevée | Faible ✓ | Faible ✓ |
| **Besoin de mises à jour** | Continu | Minimal ✓ | Minimal ✓ |
| **Protection contre la reconnaissance** | Limitée | Complète ✓ | Complète ✓ |
| **Support des applications standard** | Complet ✓ | Limité | Complet ✓ |

## Comparaison des Capacités Opérationnelles

| Capacités | Firewalls | Data Diodes | Isolation Électronique SECLAB |
|---|---|---|---|
| **Communication bidirectionnelle** | Oui ✓ | Non (avec solutions de contournement) | Oui ✓ |
| **TCP/IP Support** | Complet ✓ | Limité/Proxy | Complet ✓ |
| **Prise en charge des protocoles chiffrés** | Complet ✓ | Limitée/Complexe | Complet ✓ |
| **Gestion à distance** | Oui ✓ | Limitée | Oui (sécurisée) ✓ |
| **Compatibilité applicative** | Élevée ✓ | Faible | Élevée ✓ |
| **Complexité d'implémentation** | Modérée | Élevée | Facile à modérée (limitation : ne peut pas être virtualisé) |
| **Exigences de maintenance** | Élevées | Faibles ✓ | Très faibles ✓ |

| Comparaison de la Protection contre les Menaces | | | |
|---|---|---|---|
| **Menace** | **Protection Firewalls** | **Protection Data Diodes** | **Protection Isolation Électronique SECLAB** |
| **Exploits zero-day** | Vulnérable | Protégé (une seule direction) | Protégé (dans les deux sens) ✓ |
| **Reconnaissance du réseau** | Protection limitée | Protection élevée ✓ | Protection élevée ✓ |
| **Mouvement latéral** | Protection limitée | Protection élevée ✓ | Protection élevée ✓ |
| **Paquets malformés** | Vulnérable | Protégé (une seule direction) | Protégé (dans les deux sens) ✓ |
| **Interne malveillant** | Vulnérable | Protection limitée | Protection élevée ✓ |

# Applications concrètes et cas d'usages

## Protection des infrastructures critiques

La technologie d'Isolation Électronique offre une protection idéale pour les environnements d'infrastructures critiques où sécurité et fonctionnalités opérationnelles sont essentielles :

- **Installations de production d'énergie :** Protection des systèmes de contrôle industriel tout en permettant la supervision
- **Systèmes de transports :** Sécurisation de la signalisation ferroviaire avec maintien de la visibilité opérationnelle
- **Gestion des services publics :** Isolation des systèmes SCADA tout en autorisant la collecte de données
- **Installations de défense :** Partage contrôlé d'informations entre domaines de sécurité

## Accès à distance sécurisé et surveillance

Les capacités bidirectionnelles de la technologie d'Isolation Électronique la rendent particulièrement précieuse pour les scénarios d'accès à distance sécurisés :

- **Maintenance à distance industrielle :** Permettre l'accès des fournisseurs sans exposer les systèmes critiques
- **Solutions de surveillance sécurisées :** autoriser la collecte de données opérationnelles sans créer de vecteurs d'attaque
- **Systèmes de réponse d'urgence :** Soutenir les communications critiques lors d'incidents de sécurité
- **Securité IoT :** Créer des zones sécurisées pour les appareils connectés tout en conservant le contrôle

## Cyber Recovery et continuité des opérations

La technologie d'Isolation Électronique constitue la base d'une architecture de cyber recovery robuste capable de résister à des attaques sophistiquées :

- **Environnements de sauvegarde isolés :** Permettre la création d'environnements de sauvegarde totalement isolés tout en maintenant la connectivité opérationnelle
- **Opérations en clean room :** En cas d'incident cyber majeur, permettre la mise en place d'environnements en clean room
- **Garantie de continuité des opérations :** Assurer que la reprise après cyberattaque ne nécessite pas un arrêt complet des opérations
- **Classification et protection des données :** Permettre la mise en œuvre de stratégies avancées de protection des données

## Conformité réglementaire

La solution SecXN aide les organisations à respecter des exigences réglementaires strictes en matière de ségrégation réseau :

- **Conformité NERC CIP :** Répondre aux exigences du secteur de l'énergie pour les périmètres de sécurité électronique
- **Normes du secteur de la défense :** Répondre aux exigences rigoureuses de sécurité de niveau militaire
- **Conformité à la directive NIS2 :** Respecter les exigences de l'UE concernant la protection des infrastructures critiques
- **Règlementations des services financiers :** Soutenir le respect de DORA et d'autres exigences propres au secteur financier

Un tableau en annexe présente une répartition détaillée des dernières normes et directives, en mettant en évidence leur impact sur les organisations en matière de protection des données.

# Considérations de déploiement

## Intégration avec une infrastructure de sécurité existante

Le SecXN est conçu pour compléter et améliorer les architectures de sécurité existantes :

- ✓ Fonctionne de manière transparente pour les applications et les utilisateurs
- ✓ Peut être déployé en parallèle avec les outils de sécurité existants
- ✓ Supporte les protocoles et interfaces réseaux standards
- ✓ Nécessite des modifications minimales des configurations réseau existantes

## Modèles de déploiement

Les modèles de déploiement courants pour le SecXN incluent :

| Déploiement de passerelle | Déploiement de défense en profondeur | Protection des systèmes critiques |
|---|---|---|
| • Positionnée entre des zones du réseau de sensibilité différente<br>• Contrôle tout le trafic entre ces environnements segmentés<br>• Fournit une application centralisée de la sécurité | • Plusieurs appareils SecXN créant des couches de sécurité<br>• Chaque couche met en œuvre des politiques de sécurité spécifiques<br>• Application progressive de la sécurité à travers le réseau | • Appareils SecXN dédiés protégeant des systèmes critiques individuels<br>• Application granulaire des politiques pour des applications spécifiques<br>• Sécurité maximale pour les actifs de grande valeur |

## Considérations administratives

Le SecXN prend en charge des contrôles administratifs robustes :

- ✓ Séparation des responsabilités entre les domaines de sécurité
- ✓ Plusieurs administrateurs et rôles avec une authentification locale basée sur mot de passe (sans dépendre de l'intégrité des annuaires)
- ✓ Journalisation et surveillance complète des audits
- ✓ Mécanismes de mise à jour sécurisés avec vérification cryptographique

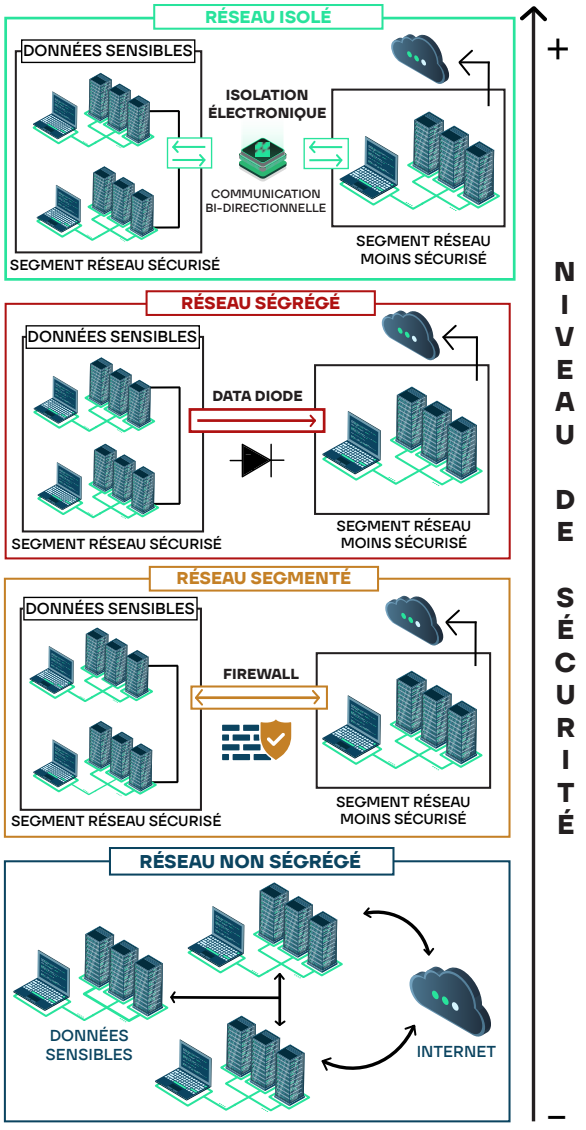
# Conclusion

À mesure que les cybermenaces gagnent en sophistication et en impact, les organisations doivent adopter des approches de sécurité qui offrent une véritable protection sans compromettre leurs capacités opérationnelles.
Les technologies traditionnelles telles que les Firewalls et Data Diodes présentent chacune des limites importantes à cet égard : les Firewalls ne garantissent pas une isolation totale et les Data Diodes empêchent les communications bidirectionnelles essentielles.

La technologie d'Isolation Électronique de SECLAB, intégrée à la gamme certifiée de produits SecXN, représente une approche révolutionnaire de la ségrégation des réseaux qui répond à ces limitations.

En combinant une sécurité matérielle et une prise en charge complète des protocoles, la technologie offre les bénéfices suivants :

- ✓ Véritable isolation réseau empêchant toute reconnaissance et tout mouvement latéral.
- ✓ Protection complète contre les attaques de la couche transport dans les deux sens.
- ✓ Prise en charge complète des communications bidirectionnelles, y compris des protocoles chiffrés.
- ✓ Fonctionnement transparent ne nécessitant aucune modification des applications.
- ✓ Sécurité certifiée et validée par l'ANSSI (Secure Xchange Network (Sec-XN)Version 3.4.0 | ANSSI) déployée dans les environnements les plus critiques.




*Comparaison du niveau de sécurité selon les architectures réseau*

Pour les organisations cherchant à protéger leurs infrastructures critiques, leurs données sensibles ou leurs environnements réglementés, la technologie d'Isolation Électronique de SECLAB offre une combinaison inégalée de sécurité et de fonctionnalité.

**Isolation Électronique SECLAB : utiliser des services réseau sans communication réseau.**

## Annexe

Dernières règlementations et directives : quels impacts aura la protection des données sur les organisations ?

| Normes | Zones géographiques concernées | Organisations ciblées | Obligations | Recommandations |
|---|---|---|---|---|
| **IEC 62443**<br>Objectif : Garantir la disponibilité, l'intégrité et la confidentialité des systèmes IACS dans les environnements industriels. | International | IEC 62443 est spécifiquement conçue pour les systèmes d'automatisation et de contrôle industriels (IACS). | IEC 62443 définit sept exigences de sécurité essentielles, couvrant l'identification, l'authentification, le contrôle des privilèges, la garantie d'intégrité des données et la résilience face aux attaques. | IEC 62443 recommande la séparation physique entre réseaux critiques et non-critiques afin de limiter la surface d'attaque. |
| **Loi de programmation militaire (LPM)**<br>Objectif : Moderniser les équipements, renforcer le renseignement militaire et investir dans les défenses cyber, spatiales et maritimes. | International | La LPM s'adresse aux opérateurs d'importance vitale (OIV) et aux systèmes d'information d'importance vitale (SIIV). | L'article 16 de la LPM impose la mise en œuvre de mesures de cloisonnement. | Ces mesures de cloisonnement peuvent être mises en œuvre via la segmentation ou l'isolation physique. |
| **Cadre de cybersécurité du NIST (CSF)**<br>Objectif : Aider les entreprises à hiérarchiser leurs axes d'amélioration et à mesurer leurs progrès en matière de cybersécurité. | International | Le cadre de cybersécurité du NIST est conçu pour différents types d'organisations publiques et privées, des petites entreprises aux grandes multinationales. | Le cadre NIST fournit une méthodologie de gestion des risques, identifiant et hiérarchisant les vulnérabilités cyber, puis les mesures correctives. | Ce processus favorise la sensibilisation aux lacunes de la gestion cyber et à l'identification des mesures correctives nécessaires. |
| **NERC-CIP**<br>Objectif : Améliorer la sécurité des systèmes de distribution d'électricité en veillant à ce que des mesures adéquates soient mises en place pour se protéger contre les cyberattaques et autres menaces de sécurité. | États-Unis | NERC-CIP s'adresse aux entreprises d'électricité responsables de la production et de la gestion des réseaux électriques. | CIP-005 exige la création de périmètres de sécurité électronique (ESP) pour séparer les systèmes BES cyber.<br>CIP-015 vise la surveillance du trafic à l'intérieur des ESP. | NERC-CIP recommande la segmentation des réseaux essentiels pour isoler les systèmes critiques, se défendre contre les attaques et limiter l'exposition aux réseaux externes. |
| **NIS 2**<br>Objectif : Renforcer la cybersécurité du tissu économique et administratif des États membres de l'UE. | Union Européenne | NIS2 s'applique aux entreprises de plus de 50 employés et à certaines autorités locales ayant un chiffre d'affaires supérieur à 1 M€. | NIS 2 impose la protection des réseaux et systèmes d'information utilisés pour assurer les services essentiels des secteurs clés. | Des mesures juridiques, techniques ou organisationnelles doivent être mises en place selon les risques existants. |
| **DORA**<br>Objectif : Renforcer la cybersécurité et la résilience opérationnelle numérique du secteur financier. | Union Européenne | DORA s'applique à la majorité des entités financières. | DORA impose implicitement le cloisonnement des réseaux pour limiter la propagation des attaques, notamment pour les processus financiers connectés. | DORA encourage des approches telles que la micro-segmentation et le « Zero Trust ». |

seclab®

The Cyber-Physical systems company.

## Contactez-nous


contact@seclab-security.com

seclab-security.com

@Seclab

**Bureaux Montpellier**
205 impasse John Locke,
34470 Pérols, France

**Bureaux Paris**
Liberty Tower, 17 place des reflets
92400 Courbevoie, France