Fiche de Veille N°1

BTS SIO – OPTION SISR

Nom Prénom : Antoine MERY

Date : 17 janvier 2026

ZERO TRUST ARCHITECTURE (ZTA)

Sujet de la veille : Zero Trust Architecture (ZTA) : évolution de la sécurité réseau d'entreprise.

Contexte : Avec la généralisation du télétravail, du cloud et l'augmentation des attaques (ransomware, compromission d'identités), le modèle traditionnel "tout ce qui est dans le réseau interne est fiable" ne suffit plus. Le modèle **Zero Trust** s'impose comme une nouvelle façon de concevoir la sécurité réseau, basée sur l'identité, la segmentation et la vérification permanente[1].

Sommaire

1. ACTUALITÉS MAJEURES LIÉES AU ZERO TRUST

1.1 ANSSI : publication d'un guide Zero Trust pour les SI français

Date : 19/06/2025

Source : ANSSI – MesServicesCyber, "Zero Trust"[1]

L'ANSSI publie un guide dédié au modèle Zero Trust, destiné aux organisations françaises, qui explique les principes (suppression de la confiance implicite, contrôle continu des accès, segmentation) et propose une démarche progressive d'adoption[1]. Le document insiste sur le fait que le Zero Trust n'est pas un produit à acheter mais une **approche globale d'architecture** qui touche le réseau, l'IAM (identités), les applications et la supervision[1].

Analyse :

Pour un technicien / admin réseau SISR, cela signifie qu'il faudra **penser "Zero Trust" dès la conception du réseau** :

- VLANs plus fins
- Filtrage inter-VLAN strict
- Contrôle des accès basé sur l'identité (AD, MFA)
- Journalisation systématique

Ce guide ANSSI donne un cadre de référence fiable pour aligner les pratiques d'architecture réseau sur les attentes nationales de cybersécurité.

1.2 Zero Trust : définition et principes pour les entreprises

Date : 10/12/2025

Source : LockSelf – "Zero Trust : définition, principes et rôle en cybersécurité"[2]

LockSelf propose une synthèse claire du Zero Trust : il s'agit d'un modèle où **aucun utilisateur, équipement ou application n'est considéré comme fiable par défaut**, même sur le réseau interne[2]. Les trois grands principes mis en avant sont :

1. Vérification systématique (authentification forte, contrôle de contexte)
2. Application du moindre privilège
3. Considération permanente qu'une compromission est possible, ce qui impose segmentation et supervision renforcées[2]

Analyse :

Cette ressource est bien adaptée à un niveau BTS : elle permet de **comprendre le "pourquoi" du Zero Trust** avant de rentrer dans la technique. Pour la conception d'un réseau d'entreprise, cela amène à abandonner l'idée du "LAN de confiance" pour aller vers des **zones cloisonnées** (postes utilisateurs, serveurs, IoT, invité) avec des règles de pare-feu strictes entre elles.

1.3 Adoption et chiffres clés du Zero Trust
Date : 22/12/2025

Source : Zerothreat.ai – "Key Zero Trust Statistics for Security Leaders"[3]

Selon cette étude, une majorité d'organisations ont lancé ou prévoient un projet Zero Trust, avec une croissance annuelle du marché supérieure à 16% et une forte adoption des briques ZTNA (Zero Trust Network Access)[3]. L'étude montre que les entreprises ayant un niveau de maturité avancé en Zero Trust réduisent significativement le nombre d'incidents de sécurité réussis et améliorent leur temps de détection et de réponse[3].

Analyse :

Ces chiffres confirment que le Zero Trust n'est pas un "buzzword", mais une **orientation durable**. Pour un futur admin réseau, cela signifie que les compétences en segmentation, filtrage fin, ZTNA et IAM ne sont plus facultatives : elles seront **au cœur des fiches de poste** dans les années à venir.

---

2. PRATIQUES ET TECHNOLOGIES LIÉES AU ZERO TRUST

2.1 Micro-segmentation et fin du "gros VPN"
Date : 2025–2026

Sources : Zscaler – "5 Predictions for Zero Trust and SASE in 2025"[4], CyberAdvisors – "Zero Trust Framework Trends for 2025"[5]

Les analyses 2025–2026 montrent une transition des VPN "classiques" (accès réseau complet) vers des solutions **ZTNA**, où l'utilisateur n'accède qu'aux applications dont il a réellement besoin[4][5]. En parallèle, la **micro-segmentation** devient une bonne pratique : on ne se contente plus de quelques VLANs, on segmente par application, par rôle, voire par sensibilité des données, avec filtrage L3/L7 entre segments[4][5].

Analyse :

En SISR, cela change la façon de concevoir les accès distants : au lieu de donner un accès VPN "global" au réseau, on déploie soit des portails applicatifs (reverse proxy, ZTNA), soit des règles précises par application. Sur un plan réseau, cela renforce l'intérêt de maîtriser **VLAN, ACL, pare-feu de niveau 7 et annuaire (AD)**.

2.2 Zero Trust et XDR / supervision avancée

Date : 05/01/2026

Source : CyberAdvisors – "Zero Trust Framework Trends for 2025"[5]

La tendance est à l'intégration du Zero Trust avec les plateformes **XDR (Extended Detection and Response)**, qui corrèlent les logs provenant du réseau, des postes, des identités et du cloud[5]. L'objectif est de détecter plus rapidement les mouvements latéraux d'un attaquant et d'adapter automatiquement les politiques (blocage d'un compte, demande de MFA supplémentaire, isolement d'un poste)[5].

Analyse :

Pour un admin réseau, cela implique de **bien configurer la journalisation** des équipements (switchs, routeurs, pare-feu, VPN, proxies, AD) vers un SIEM/XDR. La compétence ne se limite plus à "faire marcher le réseau", mais à **rendre le réseau observable** pour la sécurité.

---

3. FOCUS TECHNIQUE : APPLIQUER LE ZERO TRUST À UN RÉSEAU D'ENTREPRISE

3.1 Les trois piliers techniques pour un réseau Zero Trust

Sources : Fortinet – "Qu'est-ce que la sécurité Zero Trust ?"[6], Microsoft – "Qu'est-ce que l'architecture Zero Trust ?"[7]

1. Contrôle d'accès basé sur l'identité

- Utilisation d'Active Directory / Azure AD + MFA pour authentifier les utilisateurs et les admins[7][6]
- Règles d'accès qui se basent sur le **groupe AD**, le type d'appareil et le contexte (localisation, horaire), et non seulement sur l'IP

2. Segmentation et micro-segmentation

- VLANs séparés pour postes utilisateurs, serveurs, invités, IoT, administration[6]
- Pare-feu inter-VLAN avec des règles "appli / port / identité" minimales (principe du moindre privilège)

3. Supervision et réponse

- Centralisation des logs des équipements réseau et des serveurs[5]
- Détection des comportements anormaux (connexion admin depuis un pays inhabituel, volumes de données anormaux, etc.)

Intérêt :

Cela donne un **plan d'action concret** pour transformer un réseau pédagogique BTS (quelques VLANs, un pare-feu, un AD) en lab Zero Trust : segmentation plus fine, règles basées sur les groupes AD, et centralisation des logs.

3.2 Exemple de scénario SISR (inspiré du Zero Trust)

Objectif : sécuriser un petit réseau d'entreprise de 50 postes.

Architecture proposée

VLAN	Nom	Utilité
10	Utilisateurs	Postes de travail classiques
20	Serveurs	Active Directory, fichiers, applis
30	IoT	Caméras, imprimantes réseau, capteurs
40	Invités	Wi-Fi visiteurs, isolé du reste
99	Administration	Accès admin, outils de gestion

Règles de pare-feu inter-VLAN

De Utilisateurs (VLAN 10) vers Serveurs (VLAN 20) :

- HTTP/HTTPS vers serveurs applicatifs ✓
- SMB (445) vers serveur de fichiers ✓
- DNS (53) et NTP (123) ✓
- Tout le reste : **BLOQUÉ**

De Administration (VLAN 99) vers tous :

- RDP/SSH (3389, 22) vers serveurs ✓
- Accès console réseau ✓
- Tout est autorisé (confiance admin)

De Utilisateurs (VLAN 10) vers Administration (VLAN 99) :

- **COMPLÈTEMENT BLOQUÉ** (isolation stricte)

De IoT (VLAN 30) vers autres VLAN :

- IoT → Serveurs (pour NVR, base de données) ✓
- IoT → Utilisateurs : **BLOQUÉ**
- IoT → Internet : selon stratégie (caméras pouvant appeler des services cloud)

De Invités (VLAN 40) :

- Internet uniquement ✓
- Accès à aucun VLAN interne : **BLOQUÉ**

Lien avec le Zero Trust :

On supprime la "confiance implicite" du LAN en appliquant le **moindre privilège** et en contrôlant finement les flux entre segments. Cela correspond à la philosophie Zero Trust tout en restant réalisable dans un environnement de TP BTS.

---

4. CONCLUSION & PERSPECTIVES PERSONNELLES

L'étude de la Zero Trust Architecture montre que **la sécurité réseau ne se limite plus à un pare-feu en bordure**, mais se déploie partout : dans le LAN, dans l'IAM, dans le cloud et dans la supervision[7][1]. Pour un futur technicien / admin réseau, cela implique de maîtriser simultanément les **fondamentaux SISR** (VLAN, routage, firewall, AD) et une vision plus globale centrée sur l'identité et la segmentation.

Pour mon avenir professionnel, comprendre et pratiquer les principes du Zero Trust me permettra :

- De **concevoir des architectures réseau plus solides** face aux ransomwares et aux compromissions d'identifiants
- De dialoguer avec les RSSI et architectes sur des bases modernes (ZTNA, micro-segmentation, XDR, MFA)
- De me distinguer lors de mes stages / alternance en proposant des **améliorations concrètes** (segmentation logique, durcissement des accès, meilleure exploitation des logs)

---

5. Pistes de montée en compétence pour les prochaines semaines

Concepts à approfondir

- **Micro-segmentation** : conception de schémas de VLAN/VRF par rôle et sensibilité, écriture de règles inter-VLAN minimales
- **Identity-based access / IAM** : utilisation des groupes AD pour piloter les ACL sur firewall, proxy, VPN/ZTNA
- **ZTNA / SASE** : comprendre comment remplacer un VPN "full tunnel" par un accès appli par appli
- **Supervision & logging** : centralisation des logs (firewall, AD, proxy, VPN) et création d'alertes simples

Idées de projets pratiques

1. **Lab GNS3/Packet Tracer :** reproduire le scénario SISR ci-dessus avec VLANs, pare-feu, Active Directory et tests de connectivité
2. **Configuration d'un serveur DHCP par VLAN** avec options spécifiques (gateway, DNS) et plages d'adresses dédiées
3. **Audit de segmentation** : analyser un vrai réseau d'entreprise et proposer une amélioration basée sur les principes Zero Trust
4. **Mise en place d'un outil de centralisation de logs** (Graylog, Splunk gratuit) et création d'alertes de sécurité simples

---

Références

[1]

ANSSI – Guide "Zero Trust" sur MesServicesCyber.
https://messervices.cyber.gouv.fr/guides/zero-trust

[2] LockSelf – "Zero Trust : définition, principes et rôle en cybersécurité" (décembre 2025).
https://www.lockself.com/blog/zero-trust-definition-principes-cybersecurite

[3] Zerothreat.ai – "Key Zero Trust Statistics for Security Leaders" (décembre 2025).
https://zerothreat.ai/blog/zero-trust-statistics

[4] Zscaler – "5 Predictions for Zero Trust and SASE in 2025: What's Next?" (avril 2025).
https://www.zscaler.com/blogs/product-insights/5-predictions-zero-trust-and-sase-2025-what-s-next

[5] CyberAdvisors – "Zero Trust Framework Trends for 2025" (janvier 2026).
https://blog.cyberadvisors.com/zero-trust-framework-trends-for-2025

[6] Fortinet – "Qu'est-ce que la sécurité Zero Trust ? Fonctionnement" (décembre 2024).
https://www.fortinet.com/fr/resources/cyberglossary/what-is-the-zero-trust-network-security-model

[7] Microsoft – "Qu'est-ce que l'architecture Zero Trust ?" (décembre 2023).
https://www.microsoft.com/fr-fr/security/business/security-101/what-is-zero-trust-architecture

---

Document réalisé pour le BTS SIO SISR – Veille informatique

Cette fiche de veille est destinée à un étudiant de 1ère année et synthétise les informations essentielles sur la Zero Trust Architecture, adaptées au niveau et aux compétences du cursus.