FICHE DE VEILLE N°2 – FÉVRIER 2026

Informations Document

BTS SIO – OPTION SISR
Nom Prénom : Antoine MERY
Date : 12 février 2026
Sujet : Zero Trust Architecture (ZTA) : évolution de la sécurité réseau d'entreprise

COMPTE RENDU DE VEILLE – FÉVRIER 2026

Contexte de cette veille

Cette deuxième fiche de veille fait suite à celle de janvier 2026 et présente les **évolutions et nouvelles informations** apparues depuis le 17 janvier 2026 concernant la Zero Trust Architecture (ZTA) et son application pratique pour les administrateurs réseau SISR.

Période couverte : 18 janvier 2026 → 12 février 2026

Sommaire

1.ACTUALITÉS MAJEURES DE FÉVRIER 2026

1.1 Zscaler acquiert SquareX : Zero Trust au niveau du navigateur

Date : 09 février 2026
Source : Solutions Numériques, "Zscaler acquiert SquareX et renforce la sécurité Zero Trust au niveau du navigateur"[1]

Information clé :

Zscaler, l'un des leaders du ZTNA (Zero Trust Network Access), a annoncé début février l'acquisition de SquareX, une startup spécialisée dans la sécurité au niveau du navigateur web[1]. Cette acquisition vise à étendre les capacités Zero Trust directement dans les **navigateurs standards** (Chrome, Firefox, Edge), sans nécessiter de navigateur d'entreprise dédié ni d'agent lourd[1].

Objectif technique :

Sécuriser les applications SaaS et les ressources internes accessibles depuis des **appareils non managés** (BYOD, postes personnels des télétravailleurs)[1]. Jusqu'à présent, les organisations utilisaient des VPN d'accès distant ou des VDI pour permettre l'accès depuis des appareils tiers[1]. Avec l'intégration SquareX, Zscaler peut désormais appliquer des politiques Zero Trust directement au niveau du navigateur.

Analyse SISR :

Cette évolution montre que le Zero Trust ne se limite plus aux équipements réseau classiques (pare-feu, VPN, switchs), mais s'étend désormais jusqu'au **navigateur de l'utilisateur final**. Pour un admin réseau, cela signifie :

- Comprendre que la sécurité s'applique à tous les niveaux : réseau (VLAN, firewall), accès (ZTNA), identité (AD/MFA), et maintenant **navigateur**
- Le VPN traditionnel continue d'être remplacé par des solutions plus granulaires
- Les appareils non managés (BYOD) deviennent sécurisables sans déployer d'agent complet

Impact métier :

Dans un contexte BTS SISR, cela renforce l'importance de **maîtriser les différentes couches de sécurité** : réseau local (VLAN), accès distant (ZTNA vs VPN), contrôle d'identité (AD/MFA) et désormais compréhension des mécanismes de sécurité applicative (navigateur, proxy, reverse proxy).

1.2 Confirmation de la transition VPN → ZTNA en 2026

Date : Février 2026
Source : Symmetric Group, "ZTNA vs VPN: Secure Remote Access Without VPN in 2026"[2]

Information clé :

Un article publié début février 2026 confirme l'accélération de la **transition des VPN traditionnels vers le ZTNA**[2]. Les organisations abandonnent progressivement les VPN qui donnent un accès réseau complet au profit de solutions ZTNA qui fournissent un accès **application par application** basé sur l'identité, la posture de l'appareil et les signaux de risque en temps réel[2].

Avantages du ZTNA par rapport au VPN classique :[2]

- Vérification de l'identité à chaque demande d'accès (pas de "confiance permanente" une fois connecté)
- Évaluation de la santé de l'appareil (antivirus à jour, patch de sécurité, etc.)
- Accès uniquement aux applications approuvées (et non à tout le réseau interne)
- Élimination de l'exposition réseau entrante (pas de ports VPN ouverts sur Internet)

Analyse SISR :

Cette tendance confirme ce qui avait été observé en janvier : **le VPN n'est plus adapté aux exigences modernes de sécurité**. Pour un technicien réseau :

- Comprendre la différence fondamentale : VPN = accès réseau / ZTNA = accès applicatif
- Savoir configurer des solutions ZTNA (Zscaler Private Access, Fortinet ZTNA, Cisco Secure Access)
- Maîtriser l'intégration avec Active Directory pour les politiques d'accès basées sur les groupes AD

Évolution par rapport à janvier :

En janvier, on avait identifié la tendance. En février, la **mise en œuvre s'accélère** : les éditeurs (Zscaler, Fortinet, Cisco) renforcent leurs offres ZTNA et les entreprises adoptent massivement ces solutions.

1.3 Intégration de l’IA dans le Zero Trust

Date : 20 janvier 2026
Source : Informatique News, « Zero Trust et IA : renforcer la cyber-résilience en entreprise »[3]

Information clé :

L’intégration de l’**intelligence artificielle (IA)** et du **machine learning** dans les architectures Zero Trust devient une réalité opérationnelle[3]. Les plateformes Zero Trust utilisent désormais l’IA pour :

- **Tri automatique des incidents** de sécurité (distinction entre vrais positifs et faux positifs)
- **Amélioration de la précision de détection** des comportements anormaux
- **Adaptation dynamique des politiques** en fonction du contexte (horaire inhabituel, localisation anormale, volume de données inhabituel)
- **Facilitation de la réponse** aux incidents (proposition automatique d’actions correctives : blocage de compte, demande de MFA supplémentaire, isolement de VLAN)

Analyse SISR :

L’IA vient renforcer la **supervision et la détection** (pilier 3 du Zero Trust identifié en janvier). Pour un admin réseau, cela implique :

- Comprendre que les SIEM/XDR modernes intègrent de l’IA pour corréler les logs
- Savoir configurer les sources de logs (pare-feu, AD, VPN, proxies) pour alimenter ces systèmes intelligents
- Interpréter les alertes générées automatiquement par l’IA

Lien avec le métier SISR :

Cette évolution confirme que la compétence « supervision et logging » identifiée en janvier n’est plus optionnelle : **centraliser les logs et les analyser devient une compétence clé** pour un futur admin réseau.

2.PRATIQUES ET TECHNOLOGIES : APPROFONDISSEMENTS

2.1 Micro-segmentation : précisions techniques

Date : 29 janvier 2026
Source : FireSecure, "La Micro-Segmentation des Réseaux"[4]

Information clé :

Un article technique publié fin janvier apporte des **précisions sur les différentes approches de micro-segmentation**[4] :

Approche	Description
Basée sur les hôtes	Utilisation d'agents logiciels installés sur chaque machine pour contrôler le trafic entrant/sortant (pare-feu logiciel avec règles centralisées)
Basée sur le réseau	Utilisation de pare-feu de nouvelle génération (NGFW) et de SDN (Software-Defined Networking) pour appliquer des politiques de segmentation au niveau de l'infrastructure réseau
Basée sur les applications	Segmentation en fonction des flux applicatifs et des services plutôt que des adresses IP (exemple : isoler chaque micro-service d'une application)

Table 1: Les trois approches de micro-segmentation réseau

Méthodologie de mise en place :[4]

1. **Cartographier le réseau** : identifier les actifs critiques et analyser les flux de communication entre eux
2. **Définir des politiques de sécurité** : établir des règles d'accès et des niveaux de privilège (qui peut accéder à quoi ?)
3. **Implémenter des outils de micro-segmentation** : utiliser des solutions comme VMware NSX, Cisco Tetration, Illumio, ou des NGFW (FortiGate, Palo Alto)
4. **Surveiller et ajuster** : analyser les journaux de trafic, identifier les anomalies et affiner les règles de segmentation

Analyse SISR :

Cette méthodologie est **directement applicable dans un contexte BTS** :

- En TP, on peut reproduire l'étape 1 (cartographie réseau avec Wireshark, analyse des flux)
- En projet, on peut concevoir des politiques de segmentation (étape 2) avec justification des choix (principe du moindre privilège)
- En lab GNS3/Packet Tracer, on peut implémenter une micro-segmentation basée sur le réseau (étape 3) avec pare-feu FortiGate/pfSense
- En projet de veille, on peut documenter la surveillance (étape 4) avec centralisation des logs (Graylog, ELK)

Évolution par rapport à janvier :

En janvier, on avait identifié le **principe** de micro-segmentation. En février, on dispose d'une **méthodologie concrète** pour la mettre en œuvre, applicable dans un contexte pédagogique BTS.

2.2 Active Directory et IAM : renforcement des bonnes pratiques

Date : 13 janvier 2026 et 24 juillet 2025
Sources : IT-Connect, "Active Directory en 2026 : pourquoi le mot de passe reste la première faille"[5] ; Aduneo, "Active Directory et IAM en 2025 : guide pour prévenir les risques"[6]

Information clé :

Deux articles récents rappellent que **76% des attaques ciblant les entreprises exploitent des vulnérabilités liées à Active Directory**[6]. La première faille reste le **mot de passe faible ou compromis**[5]. Les bonnes pratiques 2026 pour sécuriser l'Active Directory sont :

- **Authentification multifactorielle (MFA)** obligatoire pour tous les comptes à privilèges (administrateurs, comptes de service critiques)[6]
- **Principe du moindre privilège (least privilege)** : chaque utilisateur n'a que les droits strictement nécessaires à son activité[6]
- **Surveillance continue** des activités suspectes : détection des connexions admin depuis des pays inhabituels, des tentatives de connexion répétées, des modifications de groupes sensibles[6]
- **Segmentation réseau** pour isoler les contrôleurs de domaine (DC) : placer les DC dans un VLAN dédié avec accès strictement contrôlé[6]
- **Comptes administratifs distincts** des comptes standards : un admin ne doit pas utiliser son compte admin pour consulter ses emails ou naviguer sur Internet[6]
- **Stations d'administration dédiées (PAW - Privileged Access Workstation)** : poste durci utilisé uniquement pour les tâches d'administration[6]

Analyse SISR :

Ces bonnes pratiques sont **directement applicables dans un contexte BTS** :

- Configurer la MFA sur un lab Active Directory (avec DUO, Microsoft Authenticator, Google Authenticator)
- Structurer l'AD avec des groupes granulaires et appliquer le moindre privilège
- Placer les contrôleurs de domaine dans un VLAN dédié (VLAN 99 "Administration" comme dans le scénario de janvier)
- Configurer la journalisation de l'AD et centraliser les logs vers un SIEM

Lien avec le pilier 1 du Zero Trust :

Ces bonnes pratiques renforcent le **pilier 1 : contrôle d'accès basé sur l'identité**. Pour un admin réseau SISR, la maîtrise d'Active Directory devient indissociable de la sécurité réseau.

2.3 Pare-feu de nouvelle génération (NGFW) : évolutions 2026

Date : 13 décembre 2024 et février 2026
Sources : Verified Market Reports, "Les 7 principales tendances des pare-feu de nouvelle génération"[7] ; Fortinet, "Pare-feu de nouvelle génération (NGFW)"[8]

Information clé :

Les pare-feu de nouvelle génération continuent d'évoluer en 2026 avec plusieurs tendances clés :[7]

1. **Convergence des technologies de sécurité** : les NGFW intègrent désormais prévention d'intrusions (IPS), antivirus, filtrage d'URL, détection avancée de menaces (ATP) dans une plateforme unifiée
2. **Intégration de l'IA et du machine learning** : analyse des modèles de trafic réseau, détection d'anomalies en temps réel, adaptation automatique aux menaces émergentes
3. **Architecture Zero Trust intégrée** : les NGFW modernes supportent nativement les principes Zero Trust (vérification continue, moindre privilège, segmentation)
4. **Sécurité centrée sur le cloud** : solutions de pare-feu basées sur le cloud pour environnements hybrides et multi-cloud
5. **Protection avancée contre les menaces** : veille sur les menaces (threat intelligence), sandboxing (exécution de fichiers suspects dans un environnement isolé), analyse comportementale
6. **Intégration 5G** : support des réseaux 5G et des cas d'usage IoT massi fs (millions d'objets connectés)
7. **Gestion simplifiée** : interfaces centralisées pour administrer plusieurs pare-feu depuis une console unique

Exemple concret : FortiGate (Fortinet) :[8]

FortiGate est le pare-feu le plus déployé au monde (> 50% de parts de marché) grâce à ses **processeurs de sécurité brevetés** qui offrent des performances élevées pour inspecter le trafic chiffré (HTTPS, TLS) sans ralentir le réseau[8].

Analyse SISR :

Pour un technicien réseau, ces évolutions signifient :

- Les pare-feu ne se limitent plus à filtrer les ports (L3/L4), ils inspectent le contenu applicatif (L7), détectent les malwares, bloquent les URL malveillantes
- La maîtrise d'un NGFW (FortiGate, pfSense avec plugins IPS, Palo Alto) devient une compétence clé
- Les pare-feu modernes s'intègrent avec l'AD pour appliquer des règles basées sur les groupes (exemple : groupe "Comptabilité" peut accéder au serveur ERP, groupe "RH" peut accéder au SIRH)

Lien avec le pilier 2 du Zero Trust :

Les NGFW sont au cœur du **pilier 2 : segmentation et micro-segmentation**. Ils permettent d'appliquer des règles granulaires entre VLANs en se basant sur l'identité (groupe AD) et le contenu applicatif.

3.CONFIRMATION DES TENDANCES IDENTIFIÉES EN JANVIER

3.1 Croissance du marché ZTNA

Date : Décembre 2025
Source : LinkedIn / Comprehensive ZTNA as a Service Solutions Market Trends 2026-2033[9]

Information clé :

Le marché mondial du ZTNA devrait croître à un taux annuel de **plus de 20%** sur les 5 prochaines années, pour atteindre **8 milliards de dollars d'ici 2028**[9]. Les facteurs de croissance sont :

- Augmentation des cybermenaces (ransomware, phishing, compromission d'identifiants)
- Mandats réglementaires pour la protection des données (RGPD en Europe, CCPA en Californie, directives NIS2 en Europe)
- Prolifération des objets IoT qui augmentent la surface d'attaque

Opportunités émergentes :[9]

- Intégration du ZTNA avec la détection de menaces pilotée par l'IA
- Automatisation de la gestion des politiques d'accès
- Extension vers des secteurs critiques (santé, finance, gouvernement)

Analyse SISR :

Cette croissance confirme que les compétences en **ZTNA, segmentation, IAM et supervision** identifiées en janvier ne sont pas des tendances passagères mais des **compétences pérennes** pour les 5-10 prochaines années.

Pour un étudiant BTS SISR, cela signifie :

- Prioriser l'apprentissage de ces technologies dans les projets et TP
- Se former sur les solutions ZTNA (Zscaler, Fortinet ZTNA, Cisco Secure Access)
- Comprendre les enjeux de conformité réglementaire (RGPD, NIS2) qui poussent les entreprises à adopter le Zero Trust

3.2 Défis de déploiement du Zero Trust

Date : 08 septembre 2025
Source : Le Monde Informatique, "Une majorité de RSSI peinent à déployer une stratégie Zero Trust"[10]

Information clé :

Malgré l'engouement pour le Zero Trust, une enquête de septembre 2025 révèle que **la majorité des RSSI (Responsables de la Sécurité des Systèmes d'Information) peinent à déployer une stratégie Zero Trust complète**[10]. Les défis identifiés sont :

- Complexité de l'architecture (nécessite de coordonner réseau, identité, applications, cloud)
- Longue durée de mise en œuvre (transformation progressive, pas de "big bang")
- Coût initial élevé (investissement dans de nouvelles solutions ZTNA, NGFW, SIEM)
- Résistance au changement (habitudes VPN ancrées, formation des équipes IT nécessaire)

Analyse SISR :

Cette information est importante pour **garder une vision réaliste** : le Zero Trust est une **approche globale et complexe**, pas une simple configuration à activer. Pour un technicien réseau :

- Comprendre que la transition vers Zero Trust prend du temps (plusieurs mois à plusieurs années)
- Accepter qu'il s'agit d'une **transformation progressive** : on commence par des segments critiques (accès admin, serveurs sensibles), puis on étend progressivement
- Développer des compétences en **conduite du changement** : former les utilisateurs, documenter les nouvelles procédures, accompagner les équipes

Opportunité pour les étudiants BTS :

Les entreprises cherchent des profils capables de **comprendre et déployer le Zero Trust**. Un étudiant SISR qui maîtrise ces concepts aura un avantage compétitif lors de ses recherches d'alternance / stage / premier emploi.

4.SYNTHÈSE DES APPORTS DE FÉVRIER 2026

Ce qui a été confirmé depuis janvier

- La transition VPN → ZTNA s'accélère (passage de la tendance à la mise en œuvre massive)
- La micro-segmentation devient une bonne pratique standard (méthodologie concrète disponible)
- L'Active Directory reste au cœur de la sécurité réseau (mais nécessite des bonnes pratiques strictes : MFA, moindre privilège, segmentation des DC)
- Les NGFW évoluent vers des plateformes unifiées intégrant IA, Zero Trust, cloud et 5G

Ce qui est nouveau en février

- **Zero Trust au niveau du navigateur** : extension de la sécurité jusqu'au navigateur de l'utilisateur (acquisition Zscaler/SquareX)
- **IA intégrée au Zero Trust** : détection automatique d'anomalies, tri des incidents, adaptation dynamique des politiques
- **Méthodologie concrète de micro-segmentation** : 4 étapes applicables en environnement BTS
- **Chiffres de marché précis** : croissance ZTNA > 20% par an, 8 milliards USD d'ici 2028
- **Défis réels de déploiement** : complexité, durée, coût, résistance au changement

IMPACT SUR LES COMPÉTENCES SISR

Compétences renforcées ce mois-ci

Compétence	Renforcement en février 2026
Segmentation réseau	Méthodologie concrète de micro-segmentation en 4 étapes (cartographie, politiques, implémentation, surveillance)
Gestion des identités (IAM)	Bonnes pratiques AD 2026 : MFA obligatoire, moindre privilège, comptes admin dédiés, PAW
Pare-feu NGFW	Compréhension des fonctions avancées : IPS, ATP, sandboxing, IA intégrée, intégration AD
ZTNA	Compréhension de la différence VPN/ZTNA, enjeux de déploiement, solutions du marché (Zscaler, Fortinet, Cisco)
Supervision (SIEM/XDR)	Intégration de l'IA pour le tri d'incidents, importance de la centralisation des logs

Table 2: Compétences SISR renforcées en février 2026

Nouvelles compétences à développer

- Compréhension des mécanismes de sécurité au niveau applicatif (navigateur, proxy, reverse proxy)
- Capacité à expliquer les enjeux de conformité réglementaire (RGPD, NIS2) qui poussent vers le Zero Trust
- Compétences en conduite du changement (accompagnement des utilisateurs, formation, documentation)

5.CONCLUSION DE LA VEILLE DE FÉVRIER 2026

Le mois de février 2026 confirme que le Zero Trust n'est plus une **approche théorique** mais une **réalité opérationnelle** :

- Les éditeurs investissent massivement (acquisition Zscaler/SquareX, renforcement des offres ZTNA)
- Les technologies évoluent rapidement (IA intégrée, sécurité au niveau du navigateur, NGFW convergents)
- Le marché croît à un rythme soutenu (> 20% par an)
- Les bonnes pratiques se précisent (méthodologie de micro-segmentation, sécurisation AD 2026)

Pour un étudiant BTS SIO SISR, cela signifie :

- Les compétences Zero Trust (segmentation, ZTNA, IAM, supervision) sont **pérennes et recherchées**
- La transition est en cours mais **complexe et progressive** (opportunité de se positionner comme facilitateur)
- La maîtrise technique doit s'accompagner d'une **compréhension des enjeux** (conformité, conduite du changement, coût/bénéfice)

Pour la prochaine veille (mars 2026) :

- Surveiller les évolutions réglementaires (NIS2 en Europe, directives sectorielles)
- Approfondir SASE (convergence réseau/sécurité dans le cloud)
- Identifier des retours d'expérience concrets d'entreprises ayant déployé le Zero Trust

6.RÉFÉRENCES

[1] Solutions Numériques. (2026, 9 février). *Zscaler acquiert SquareX et renforce la sécurité Zero Trust au niveau du navigateur*. https://www.solutions-numeriques.com/zscaler-acquiert-squarex-et-renforce-la-securite-zero-trust-au-niveau-du-navigateur/

[2] Symmetric Group. (2026, février). *ZTNA vs VPN: Secure Remote Access Without VPN in 2026*. https://www.symmetricgroup.com/blog/goodbye-vpn-why-ztna-sase-are-replacing-traditional-remote-access-in-2026.html

[3] Informatique News. (2026, 20 janvier). *Garder une longueur d'avance sur les cyber-adversaires en intégrant l'IA à la sécurité Zero Trust*. https://www.informatiquenews.fr/garder-une-longueur-davance-sur-les-cyber-adversaires-en-integrant-ia-a-la-securite-zero-trust-u

[4] FireSecure. (2026, 29 janvier). *La Micro-Segmentation des Réseaux*. https://firesecure.fr/micro-segmentation-reseaux/

[5] IT-Connect. (2026, 13 janvier). *Active Directory en 2026 : pourquoi le mot de passe reste la première faille et comment la combler*. https://www.it-connect.fr/active-directory-en-2026-pourquoi-le-mot-de-passe-reste-la-premiere-faille-et-comment-la-combler/

[6] Aduneo. (2025, 24 juillet). *Active Directory et IAM en 2025 : guide pour prévenir les risques*. https://www.aduneo.com/identites/active-directory-et-iam-roles-enjeux-et-bonnes-pratiques-pour-prevenir-les-risques

[7] Verified Market Reports. (2024, 13 décembre). *Les 7 principales tendances des pare-feu de nouvelle génération*. https://www.verifiedmarketreports.com/fr/blog/top-7-trends-in-next-generation-firewall/

[8] Fortinet. (n.d.). *Pare-feu de nouvelle génération (NGFW)*. https://www.fortinet.com/fr/products/next-generation-firewall

[9] LinkedIn. (2025, décembre). *Comprehensive ZTNA as a Service Solutions Market Trends 2026-2033*. https://www.linkedin.com/pulse/comprehensive-ztna-service-solutions-market-trends-20262033-ggiif

[10] Le Monde Informatique. (2025, 8 septembre). *Une majorité de RSSI peinent à déployer une stratégie Zero Trust*. https://www.lemondeinformatique.fr/actualites/lire-une-majorite-de-rssi-peinent-a-deployer-une-strategie-zero-trust-97796.html