# Le guide du RSSI pour un accès Zero Trust efficace

## Une visibilité et un contrôle permanents sur tous les dispositifs et utilisateurs

# Table des matières

## Synthèse

Les meilleures pratiques en matière d'accès réseau impliquent de migrer vers l'accès Zero Trust (accès avec vérification systématique) ou ZTA. Les RSSI qui cherchent à mettre en œuvre le ZTA trouveront de nombreuses technologies conçues pour répondre aux exigences de l'architecture Zero Trust du National Institute of Standards and Technology (NIST).[1] Toutefois, il peut être difficile de faire fonctionner toutes ces technologies ensemble afin d'éviter les carences en sécurité.

Conforme aux normes les plus récentes et s'appuyant sur des décennies d'expérience en matière de cybersécurité, Fortinet a constaté que la stratégie ZTA la plus efficace est une approche holistique qui offre une visibilité et un contrôle dans trois domaines clés : qui se trouve sur le réseau, ce qui se trouve sur le réseau et que deviennent les appareils gérés lorsqu'ils quittent le réseau.

# Introduction

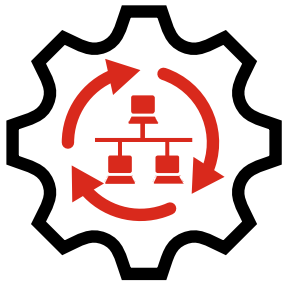
Alors que l'innovation numérique pèse sur la sécurité des réseaux, les RSSI voient leurs réseaux se fragmenter et leur surface d'attaque s'étendre. Comme les réseaux ont désormais des « edges » étendus, il est difficile de créer une seule frontière à défendre, ce qui rend inefficaces les stratégies de contrôle d'accès basées sur le périmètre du réseau. En outre, il devient de plus en plus difficile de distinguer les utilisateurs internes, dignes de confiance, des utilisateurs externes, inconnus ou peu fiables. A noter que les collaborateurs et sous-traitants sont souvent impliqués dans des violations majeures du réseau. Même les utilisateurs qui sont en conformité peuvent devenir des vecteurs d'attaques, puisqu'ils se déplacent sur et hors du réseau, souvent avec leurs appareils personnels.

En conséquence, les RSSI ont dû repenser les bases de la confiance accordée aux utilisateurs et aux appareils qui demandent l'accès aux ressources du réseau. Les meilleures pratiques ont évolué, passant de la confiance dans tout ce qui se trouve à l'intérieur du réseau, à la vérification unique gage de confiance, pour finir par la méfiance vis-à-vis de tous les appareils et utilisateurs et la fourniture d'un accès avec privilège moindre. D'où un nouveau modèle d'accès, le ZTA (zero trust access) ou accès à vérification systématique.

Les exigences du ZTA ont été affinées pendant plus d'une décennie après la création de ce terme. Le dernier document du NIST sur l'architecture à vérification systématique reconnaît que le ZTA est un projet encore en cours. Ainsi, plutôt que de définir les spécificités de l'architecture, il propose un ensemble de principes directeurs et conseille aux professionnels de la sécurité de considérer le passage au ZTA comme une migration.

En tant que partenaire des RSSI dans cette migration, Fortinet a développé une approche holistique pour un ZTA efficace. Cette approche repose sur trois piliers :

- Les solutions ZTA doivent fournir une visibilité continue sur les appareils et les utilisateurs connectés au réseau, ainsi que sur les ressources réseau auxquelles ils tentent d'accéder.
- Elles doivent pouvoir appliquer des politiques de sécurité quels que soient le type de dispositif, le lieu de connexion ou la méthode d'accès.
- Leur application et la visibilité qu'elles procurent doivent pouvoir être maintenues lorsque les appareils sont hors ligne.



**Les « edges » des réseaux sont multiples, ce qui rend inefficace tout contrôle d'accès basé sur le périmètre. Le ZTA est le nouveau modèle dominant de l'accès au réseau, et une approche holistique est la clé de son succès.**

# Voir et contrôler qui se trouve sur le réseau

L'entreprise numérique sans frontières s'adresse à une diversité toujours plus importante d'utilisateurs. Outre les collaborateurs-utilisateurs traditionnels, il faut compter les sous-traitants, les partenaires de la chaîne d'approvisionnement et les clients qui ont besoin d'accéder à des données et applications présentes sur site ou dans le cloud. Gérer l'accès aux ressources du réseau implique à la fois d'identifier l'utilisateur qui demande l'accès et de vérifier que l'utilisateur est habilité à accéder aux ressources demandées.

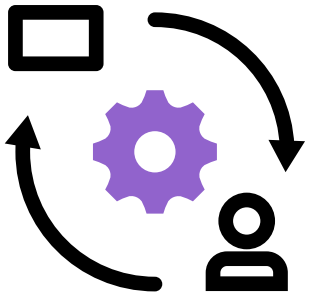
## Identification et authentification pour prévenir les violations

Les identités des utilisateurs sont facilement compromises. Les acteurs malveillants peuvent obtenir des noms d'utilisateur et des mots de passe soit par force brute (ce qui est souvent facile compte tenu de mots de passe généralement faibles), soit par des tactiques d'ingénierie sociale telles que le phishing par courrier électronique. C'est pourquoi les entreprises ajoutent l'authentification multifactorielle (ou MFA) à leurs processus de connexion. Le MFA tire parti d'un élément connu de l'utilisateur, comme un nom d'utilisateur et/ou un mot de passe, et d'un élément dont l'utilisateur dispose, comme un dispositif de jetons qui génère un code à usage unique ou un logiciel de génération de jetons. D'ici 2024, 70 % des applications devraient utiliser le MFA.[2] Les nouvelles solutions biométriques (empreintes digitales, scanners du visage et de l'iris) promettent également de minimiser le risque de vol d'identité.

## Accès à moindre privilège

Le deuxième défi consiste à empêcher les utilisateurs authentifiés d'abuser de leurs privilèges d'accès. À cette fin, les RSSI devraient imposer des politiques d'accès à moindre privilège, qui limitent l'accès au minimum nécessaire pour l'utilisateur, en fonction de son rôle dans l'organisation ou de sa relation avec celle-ci. Les solutions d'authentification et d'autorisation doivent être intégrées à l'infrastructure de sécurité du réseau de l'entreprise (et à une base de données Active Directory basée sur des politiques) pour permettre une application automatisée et une gestion aisée des règles d'accès à moindre privilège.

Il est également important de veiller à ce que ces interventions de sécurité n'entravent pas la productivité ou la qualité de l'expérience de l'utilisateur. Les RSSI devraient opter pour des solutions ZTA qui prennent en charge l'authentification SSO (single sign-on) et fonctionnent avec une latence minimale. Ces deux fonctions contribuent à faciliter la conformité et l'expérience de l'utilisateur.



**Les solutions d’accès Zero Trust devraient appliquer fermement les politiques de contrôle d’accès, tout en améliorant la productivité et l’expérience de l’utilisateur légitime.**

# Voir et contrôler ce qui se trouve sur le réseau

Si les RSSI sont, à juste titre, préoccupés par le comportement non conforme et imprévisible des utilisateurs, ils doivent s'intéresser également aux appareils qui accèdent à leurs réseaux. Il s'agit notamment des dispositifs d'utilisateurs finaux (fixes et mobiles), des équipements de bureau en réseau, des systèmes front-end des magasins (points de vente par exemple), des technologies opérationnelles et des nombreux capteurs et autres objets connectés disséminés, connus collectivement sous le nom d'Internet des objets (IoT). Les projections de croissance des dispositifs IoT installés varient, mais la plupart prévoient qu'ils se compteront en milliards dans le monde entier dans les années à venir.

Le défi de la gestion de tous ces appareils réside dans leur grande dispersion, les différents niveaux de supervision des appareils et l'incompatibilité des appareils obsolètes à des protocoles de communication standards. Les RSSI peuvent aider les administrateurs sécurité à résoudre les problèmes de gestion des endpoints (terminaux) en leur donnant les outils dont ils ont besoin pour détecter, classer et contrôler efficacement l'accès à tout ce qui se trouve sur le réseau.

## Le contrôle d'accès réseau (NAC) ultrarapide

Pour savoir ce qui se trouve sur le réseau à tout moment, les RSSI ont besoin d'outils de contrôle d'accès au réseau (NAC) qui identifient et profilent automatiquement chaque appareil lorsque ce dernier demande l'accès au réseau, tout en l'analysant pour détecter ses vulnérabilités. Au cours du processus de détection, la solution NAC devrait détecter les tentatives d'attaque MAB (MAC Authentication Bypass) et enregistrer ces incidents. Elle devrait aussi partager les informations qu'elle recueille en temps réel avec d'autres dispositifs de réseau et composants de l'infrastructure de sécurité.

Les processus NAC devraient être menés en quelques secondes afin de minimiser le risque de compromettre le dispositif. C'est pourquoi les RSSI doivent se méfier des outils qui reposent sur l'analyse du trafic. De tels outils permettent aux appareils de se connecter au réseau pendant l'identification. Pourtant, le processus d'analyse peut prendre jusqu'à une demi-heure, pendant laquelle le réseau peut être compromis.

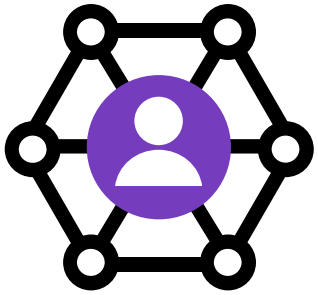
Une autre mise en garde concerne les solutions qui reposent sur le protocole Wi-Fi 802.1X. Elles fonctionnent bien pour les réseaux sans fil, où chaque client dispose d'un demandeur (supplicant) dans le cadre du contrôle de la communication, ce qui rend le protocole 802.1X facile à utiliser. Cependant, les solutions basées sur 802.1X sont onéreuses à déployer sur les réseaux commutés. Idéalement, une solution NAC devrait être facile à déployer à partir d'un emplacement central et fonctionner sur les réseaux filaires et sans fil. Ceci permettrait de soutenir le rythme de croissance que connaissent les entreprises. Avec un emplacement central, la solution NAC ne nécessite pas de capteurs pour chaque dispositif, ce qui évite toute inflation des coûts de déploiement et de gestion.

## La micro-segmentation permet le contrôle ZTA

L'application de politiques de contrôle d'accès est essentielle pour tous les dispositifs, mais elle est particulièrement difficile pour les appareils IoT. Il s'agit généralement d'appareils de faible puissance et compacts, sans capacités CPU ou de mémoire supplémentaire pour les processus de sécurité. Ils ont également tendance à présenter des systèmes d'exploitation non standards qui ne sont pas nécessairement compatibles avec les outils de sécurité des terminaux utilisés pour les sécuriser. Par conséquent, la sécurité de l'appareil n'est pas fiable, et le réseau lui-même doit fournir la sécurité nécessaire.

En raison du déploiement à grande échelle de l'IoT, les RSSI doivent donner la priorité au contrôle de l'IoT lorsqu'ils envisagent des solutions ZTA. Le contrôle d'accès ne peut pas être mis en œuvre au sein même des dispositifs et doit donc provenir du réseau. Le moyen d'y parvenir est de micro-segmenter le réseau avec des pare-feu de nouvelle génération (Next-Generation Firewall, NGFW), en regroupant les dispositifs IoT similaires. Ceci renforce le réseau de deux façons. D'abord, en obstruant les mouvements latéraux (est-ouest) sur le réseau, ce qui rend l'accès aux appareils plus difficile pour les pirates et les vers. Deuxièmement, en réduisant le risque qu'un appareil infecté serve de vecteur par lequel un hacker peut s'en prendre au reste du réseau.

Comme les autres composants de la solution ZTA, les NGFW devraient être conçus de manière à traiter tout le trafic entre les segments, avec une latence minimale. Le mécanisme de contrôle ZTA des appareils ne constitue ainsi un obstacle à la productivité au sein de l'organisation.



**Les RSSI doivent s’assurer que les administrateurs sécurité disposent des outils nécessaires pour détecter, classer et contrôler efficacement tout ce qui se trouve sur le réseau, à partir d’un emplacement central.**

## Contrôler les appareils gérés hors du réseau

L'une des caractéristiques des entreprises numériques est la nature transitoire de la connectivité et de l'utilisation du réseau. Les services cloud ont permis un accès omniprésent, ce qui signifie que les utilisateurs peuvent se déplacer, déconnecter leur appareil du réseau à un endroit et le reconnecter à un autre. Ils peuvent aussi commencer à travailler sur un appareil et continuer sur un autre. Le contrôle des appareils gérés lorsqu'ils sont hors réseau est un défi : même sécurisés la première fois qu'ils se connectent au réseau, ils peuvent être compromis lorsqu'ils sont hors ligne et infecter le réseau à leur retour.

Pour surmonter cette difficulté, les RSSI doivent envisager la sécurité des endpoints dans le cadre d'une solution ZTA. Une solution de sécurité des endpoints doit contrôler l'application des bonnes pratiques hors du réseau, avec une analyse des vulnérabilités, le filtrage Web et le patching. Elle doit aussi offrir des options sûres et flexibles pour la connectivité des réseaux privés virtuels (VPN). Comme pour les outils de gestion de l'identité, la solution de sécurité des endpoints doit prendre en charge la fonctionnalité SSO pour une plus grande facilité d'utilisation. Une fois qu'un endpoint est connecté au réseau, la solution de sécurité doit relayer les informations sur l'état du endpoint aux autres composants du réseau et de sécurité, afin d'évaluer les risques et de déterminer le niveau d'accès approprié.

## Synthèse

L'accès Zero Trust n'est pas un concept nouveau. Les RSSI sont donc susceptibles d'être inondés de conseils sur les technologies et les solutions ZTA. Des directives du secteur comme la SP 800-207 du NIST[3] fournissent un schéma réaliste de transition vers le ZTA. Travailler avec les principaux fournisseurs de sécurité des réseaux et sélectionner des outils intégrés et automatisés peut aider à surmonter les principaux défis de l'accès réseau ZTA : savoir qui se trouve sur le réseau et ce qui s'y trouve, contrôler l'accès aux ressources et atténuer les risques que cet accès comporte.

[1] Scott Rose, et al., « Draft (2nd) NIST Special Publication 800-207, Zero Trust Architecture », NIST, février 2020.

[2] Michael Kelley, et al., « Gartner Magic Quadrant for Access Management », Gartner, 12 août 2019.

[3]Scott Rose, et al., « Draft (2nd) NIST Special Publication 800-207, Zero Trust Architecture », NIST, février 2020.

France
TOUR ATLANTIQUE
24ème étage, 1 place de la Pyramide
92911 Paris La Défense Cedex
France
Ventes: +33 (0) 1 80 42 05 40

www.fortinet.com/fr



août 24, 2021 10:57 AM

ebook-effective-zero-trust-access_fr_imp

693421-B-0-FR