Le guide des RSSI pour un accès zero-trust efficace

Assurer une visibilité et un contrôle permanents sur tous les dispositifs et utilisateurs

Table des matières

Synthèse

Les meilleures pratiques en matière d'accès au réseau encouragent l'accès zero-trust (ZTA), à savoir un accès réseau avec vérification systématique. Les RSSI souhaitant déployer le ZTA disposent de nombreuses technologies conformes aux exigences d'une architecture zero-trust telles que formulées par le NIST (National Institute of Standards and Technology).[1] Toutefois, il peut être difficile de faire fonctionner toutes ces technologies ensemble, ce qui est pourtant essentiel pour éviter les failles de sécurité.

Dans une optique de respect des normes les plus récentes et en s'appuyant sur des décennies d'expérience en matière de cybersécurité, Fortinet a constaté que la stratégie ZTA la plus efficace consiste en une approche holistique qui offre une visibilité et un contrôle sur trois domaines clés : les utilisateurs présents sur le réseau, les dispositifs présents sur le réseau et les dispositifs gérés lorsqu'ils quittent le réseau.

Introduction

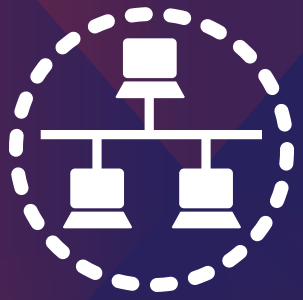
Alors que l'innovation numérique pèse sur la sécurité des réseaux, les RSSI voient leurs réseaux se fragmenter et leurs surfaces d'attaque s'étendre. Les réseaux présentent désormais de multiples « edges » et il est difficile d'instituer une seule frontière à défendre, ce qui rend inefficaces les stratégies de contrôle d'accès basées sur le périmètre 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. Les collaborateurs et les sous-traitants sont trop souvent impliqués dans des incidents majeurs de sécurité. 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 critères de la confiance accordée aux utilisateurs et aux dispositifs qui demandent l'accès aux ressources du réseau. Les meilleures pratiques ont évolué, passant d'une confiance par défaut dans tout ce qui se trouve au sein du réseau, à une confiance attribuée après validation, jusqu'à aboutir à une absence de confiance par défaut envers les utilisateurs et les dispositifs, auxquels sont attribués des privilèges d'accès minimums. C'est le principe d'un accès zero-trust (ZTA pour zero trust access), ou accès à vérification systématique.

Le ZTA a été affiné au cours de la décennie qui suit l'émergence de ce concept. Le dernier document du NIST sur le sujet reconnaît que le ZTA est un projet qui est toujours en cours. Ainsi, plutôt que de définir les spécificités de l'architecture, ce document propose un ensemble de principes directeurs et conseille aux professionnels de la sécurité de considérer la migration vers ZTA comme graduelle.

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

- Les solutions ZTA doivent fournir une visibilité continue sur les appareils et 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, l'emplacement ou la méthode d'accès.
- L'application des règles et la visibilité doivent pouvoir être maintenues lorsque les dispositifs 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 modèle dominant en matière d’accès au réseau, et une approche holistique est la clé du succès.

Voir et contrôler qui se trouve sur le réseau

L'entreprise numérique sans frontières prend en charge une diversité toujours plus importante d'utilisateurs. Outre les collaborateurs-utilisateurs traditionnels, il faut compter les intérimaires et consultants externes, les partenaires de la chaîne d'approvisionnement ou encore les clients qui vont accéder à des données et à des applications sur site ou dans le cloud. Réglementer l'accès aux ressources du réseau implique d'identifier l'utilisateur qui demande cet accès et de vérifier que cet utilisateur est habilité à accéder aux ressources demandées.

Identification et authentification contre les intrusions

Les identités des utilisateurs peuvent être compromises. Les acteurs malveillants peuvent obtenir des noms d'utilisateur et des mots de passe soit par force brute (souvent facile car les mots de passe sont généralement faibles) ou des tactiques d'ingénierie sociale telles que le phishing par email. C'est pourquoi les entreprises ajoutent l'authentification multifactorielle (ou MFA pour multi-factor authentification) à leurs processus de connexion. Le MFA associe une information connue de l'utilisateur comme un nom d'utilisateur et/ou un mot de passe, et un élément dont l'utilisateur dispose, comme un dispositif de jetons qui génère un code à usage unique ou un générateur de jetons basé sur un logiciel. 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.

Des privilèges d'accès minimaux

Le deuxième défi consiste à empêcher les utilisateurs authentifiés d'abuser de leurs privilèges d'accès. À cette fin, les RSSI devraient imposer des règles qui restreignent le périmètre d'accès en fonction du rôle de l'utilisateur 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) pour permettre une application automatisée et une gestion aisée des politiques d'accès avec privilèges minimaux.

Il est également important de veiller à ce que cette couche de sécurité soit transparente vis-à-vis de la productivité ou la qualité de l'expérience de l'utilisateur. Les RSSI devraient opter pour des solutions ZTA avec authentification unique (SSO) et latence minimale. Ces deux fonctions contribuent à faciliter la conformité et à minimiser l'impact sur l'utilisateur.

Les solutions d’accès zero-trust devraient appliquer les politiques de contrôle d’accès avec fermeté, tout en améliorant la productivité et l’expérience des utilisateurs légitimes.

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 ne doivent pas pour autant accorder moins d'attention aux appareils accédant à leurs réseaux. Il s'agit notamment des appareils fixes ou mobiles des utilisateurs finaux, des équipements de bureau en réseau, des systèmes front-end des points de vente, des technologies opérationnelles et des multiples objets connectés et autres appareils disséminés relevant de l'Internet des objets (IoT). Les projections de croissance en matière de dispositifs IoT installés varient, mais la plupart prévoient qu'ils se chiffreront en milliards dans le monde entier dans les années à venir.

La gestion de ce parc de dispositifs s'annonce complexe compte tenu de leur dissémination à grande échelle, des différents niveaux de contrôle de ces appareils et de la présence d'appareils anciens et non compatibles avec les protocoles de communication standards. Les RSSI peuvent aider les administrateurs sécurité à mieux gérer leurs terminaux en leur donnant les outils dont ils ont besoin pour détecter, classer et contrôler efficacement l'accès de tout ce qui se trouve sur le réseau.

Le contrôle d'accès réseau (NAC) pour une visibilité ultra-rapide

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) capables d'identifier et de profiler automatiquement chaque appareil qui demande l'accès au réseau et de l'analyser pour détecter ses vulnérabilités. Au cours du processus de détection, la solution NAC doit détecter les tentatives d'attaque MAB (MAC Authentication Bypass ou contournement de l'authentification MAC) et enregistrer ces incidents. Elle doit aussi partager en temps réel les informations recueillies avec d'autres dispositifs réseau et composants de l'infrastructure de sécurité.

Ce processus NAC doit être mené en quelques secondes pour minimiser au plus vite le risque de piratage du dispositif. Ce qui doit inciter les RSSI à se méfier des solutions qui reposent sur l'analyse du trafic puisqu'elles permettent aux dispositifs de se connecter au réseau pendant l'identification. Le processus d'analyse peut prendre jusqu'à une demi-heure, une durée 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 est un « supplicant » dans le cadre du contrôle de la communication, ce qui facilite l'utilisation du protocole 802.1X. Cependant, les solutions basées sur 802.1X sont onéreuses à déployer sur les réseaux commutés. Idéalement, une solution NAC doit se déployer de manière simple à partir d'un emplacement centralisé et fonctionner de manière cohérente sur les réseaux filaires et sans fil. Elle doit également accompagner le rythme de croissance que connaissent les entreprises. De par sa position centrale, la solution NAC ne nécessite pas de capteurs pour chaque dispositif, ce qui allège les coûts de déploiement et de gestion.

La micro-segmentation au service du ZTA

L'application de politiques de contrôle d'accès est essentielle pour tous les dispositifs, mais elle est particulièrement difficile pour les objets connectés. Ces dispositifs sont généralement de faible puissance et de taille compacte, sans ressources CPU et mémoire supplémentaires pour prendre en charge les processus de sécurité. Ils disposent également souvent de systèmes d'exploitation non standards et pas toujours compatibles avec les outils de sécurité pour terminaux. Par conséquent, la sécurité de ces objets n'est pas fiable, et c'est le réseau qui doit, lui-même, fournir la sécurité nécessaire.

En raison de l'envergure des environnements IoT, les RSSI qui envisagent des solutions ZTA doivent donner la priorité au contrôle de ces objets connectés. Le contrôle d'accès, qui ne peut être mis en œuvre dans les dispositifs eux-mêmes, doit provenir du réseau. Dans cette optique, il s'agit de faire appel à des pare-feux de nouvelle génération (Next-Generation Firewall, NGFW), pour micro-segmenter le réseau et regrouper les dispositifs IoT similaires. Cette approche prévient les mouvements latéraux au sein du réseau et rend l'accès aux appareils plus difficile pour les hackers et les vers. D'autre part, elle réduit 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 doivent pouvoir traiter tout le trafic entre segments avec une latence minimale. C'est à ce titre que le mécanisme de contrôle ZTA ne sera pas un obstacle à la productivité des entreprises.

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 qui sont hors du réseau

L'une des caractéristiques des entreprises digitales est la nature éphémère de la connectivité et de l'utilisation du réseau. Les services de cloud offrent un accès omniprésent, ce qui signifie que les utilisateurs peuvent se déplacer, déconnecter leur appareil du réseau à un endroit pour le reconnecter ailleurs. Ils peuvent aussi initier une tâche de travail sur un appareil et la poursuivre sur un autre. Le contrôle des appareils gérés qui sont hors réseau est un défi. Ces dispositifs peuvent être sécurisés un première fois lorsqu'ils se connectent au réseau, puis être compromis lorsqu'ils sont hors ligne, pour enfin infecter le réseau à leur retour.

Pour surmonter cette difficulté, les RSSI doivent envisager la sécurité des terminaux dans le cadre d'une solution ZTA. Une solution de sécurité des terminaux doit permettre un contrôle de la sécurité hors réseau, par une analyse des vulnérabilités, un filtrage Web et une politique pertinente de patching. Elle doit aussi offrir des options sûres et flexibles de connexion par réseau privés virtuels (VPN). Comme pour les outils de gestion des identités, la solution de sécurité des terminaux doit proposer une fonctionnalité SSO pour une plus grande facilité d'utilisation. Lorsqu'un terminal est connecté au réseau, la solution de sécurité doit relayer les informations sur l'état de l'appareil aux autres composants du réseau et de sécurité, afin d'évaluer les risques et déterminer le niveau d'accès approprié.

Synthèse

Le contrôle d'accès zero-trust n'est pas un concept nouveau. Les RSSI sont donc susceptibles d'être submergés de conseils sur les technologies et les solutions ZTA. Des directives sectorielles à l'image de la norme SP 800-207 du NIST[3] fournissent un processus pertinent de transition vers le ZTA. Travailler avec les principaux fournisseurs de sécurité réseaux et sélectionner des outils intégrés et automatisés peut aider à pallier les principaux défis de l'accès zero-trust aux réseaux : savoir qui se trouve sur le réseau et ce qui s'y trouve, contrôler l'accès aux ressources et atténuer les risques découlant de ces accès.

[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.

www.fortinet.fr

693421-A-0-FR

décembre 7, 2020 11:55 AM