Clause de non-responsabilité: Cette traduction a été réalisée automatiquement dans le but d'aider les francophones non anglophones à comprendre la publication spéciale NIST 800-207. AB AUDIT met à votre disposition le document en l'état et ne supporte aucune responsabilité quant aux erreurs qui pourraient être ou auraient été introduites lors de la traduction. Document téléchargeable à partir de **www.ab-audit.com**

NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

Cette publication est disponible gratuitement à l'adresse suivante :
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

National Institute of Standards and Technology
U.S. Department of Commerce

Clause de non-responsabilité: Cette traduction a été réalisée automatiquement dans le but d'aider les francophones non anglophones à comprendre la publication spéciale NIST 800-207. AB AUDIT met à votre disposition le document en l'état et ne supporte aucune responsabilité quant aux erreurs qui pourraient être ou auraient été introduites lors de la traduction. Document téléchargeable à partir de **www.ab-audit.com**

NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Division des technologies de réseau avancées Laboratoire des technologies de l'information

Stu Mitchell
Stu2Labs
Stafford,
Virginie

Sean
Connelly, *Agence de cybersécurité et de sécurité des infrastructures, Département de la sécurité intérieure*

Cette publication est disponible gratuitement à l'adresse suivante :
https://doi.org/10.6028/NIST.SP.800-207

Août 2020

Département du Commerce des États-Unis
Wilbur L. Ross, Jr., secrétaire

Institut national de normes et de technologie
Walter Copan, directeur du NIST et sous-secrétaire au Commerce pour les normes et la technologie

Clause de non-responsabilité: Cette traduction a été réalisée automatiquement dans le but d'aider les francophones non anglophones à comprendre la publication spéciale NIST 800-207. AB AUDIT met à votre disposition le document en l'état et ne supporte aucune responsabilité quant aux erreurs qui pourraient être ou auraient été introduites lors de la traduction. Document téléchargeable à partir de **www.ab-audit.com**

Autorité

Cette publication a été élaborée par le NIST conformément à ses responsabilités statutaires en vertu de la Federal Information Security Modernization Act (FISMA) de 2014, 44 U.S.C. § 3551 *et suivants.*, Droit public (P.L.) 113-283. Le NIST est responsable de l'élaboration de normes et de directives en matière de sécurité de l'information, y compris des exigences minimales pour les systèmes d'information fédéraux, mais ces normes et directives ne s'appliqueront pas aux systèmes de sécurité nationale sans l'approbation expresse des fonctionnaires fédéraux compétents exerçant une autorité politique sur ces systèmes. Cette ligne directrice est conforme aux exigences de la circulaire A-130 de l'Office of Management and Budget (OMB).

Rien dans cette publication ne doit être interprété comme contredisant les normes et directives rendues obligatoires et contraignantes pour les organismes fédéraux par le secrétaire au Commerce en vertu d'une autorité légale. Ces directives ne doivent pas non plus être interprétées comme modifiant ou remplaçant les pouvoirs existants du secrétaire au Commerce, du directeur de l'OMB ou de tout autre fonctionnaire fédéral. Cette publication peut être utilisée par des organisations non gouvernementales sur une base volontaire et n'est pas soumise au droit d'auteur aux États-Unis. L'attribution serait toutefois appréciée par le NIST.

Publication spéciale 800-207 de l'Institut national des normes et de la technologie
Tribune Natl. Inst. Technol. Spec. Publ. 800-207, 59 pages (août 2020)
CODEN : NSPUE2

Cette publication est disponible gratuitement à
l'adresse suivante :
https://doi.org/10.6028/NIST.SP.800-207

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Les commentaires sur cette publication peuvent être soumis à l'adresse suivante :

Institut national de normes et de technologie
À l'attention de : Division des technologies de réseau avancées, Laboratoire des technologies de l'information 100 Bureau Drive (Mail Stop 8920) Gaithersburg, MD 20899-8920
Courriel : zerotrust-arch@nist.gov

Tous les commentaires peuvent être publiés en vertu de la loi sur la liberté de l'information (FOIA).

Rapports sur la technologie des systèmes informatiques

Le Laboratoire des technologies de l'information (ITL) du National Institute of Standards and Technology (NIST) promeut l'économie et le bien-être public des États-Unis en assurant la direction technique de l'infrastructure de mesure et de normalisation du pays. ITL élabore des essais, des méthodes d'essai, des données de référence, des mises en œuvre de preuves de concept et des analyses techniques pour faire progresser le développement et l'utilisation productive des technologies de l'information. Les responsabilités d'ITL comprennent l'élaboration de normes et de directives de gestion, administratives, techniques et physiques pour la sécurité et la confidentialité rentables des informations autres que liées à la sécurité nationale dans les systèmes d'information fédéraux. La publication spéciale de la série 800 rend compte des recherches, des directives et des efforts de sensibilisation d'ITL en matière de sécurité des systèmes d'information, ainsi que de ses activités de collaboration avec l'industrie, le gouvernement et les organisations universitaires.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

Abstrait

Le Zero Trust (ZT) est le terme désignant un ensemble évolutif de paradigmes de cybersécurité qui déplacent les défenses des périmètres statiques basés sur le réseau pour se concentrer sur les utilisateurs, les actifs et les ressources. Une architecture Zero Trust (ZTA) utilise les principes Zero Trust pour planifier l'infrastructure et les flux de travail industriels et d'entreprise. Le Zero Trust suppose qu'il n'y a pas de confiance implicite accordée aux actifs ou aux comptes d'utilisateurs en fonction uniquement de leur emplacement physique ou réseau (c'est-à-dire les réseaux locaux par rapport à Internet) ou de la propriété des actifs (entreprise ou propriété personnelle). L'authentification et l'autorisation (à la fois l'objet et l'appareil) sont des fonctions discrètes exécutées avant l'établissement d'une session vers une ressource d'entreprise. Le Zero Trust est une réponse aux tendances des réseaux d'entreprise qui incluent les utilisateurs distants, le BYOD (Bring Your Own Device) et les actifs basés sur le cloud qui ne sont pas situés à l'intérieur des limites d'un réseau appartenant à l'entreprise. Le Zero Trust se concentre sur la protection des ressources (actifs, services, flux de travail, comptes réseau, etc.), et non sur les segments de réseau, car l'emplacement du réseau n'est plus considéré comme le composant principal de la posture de sécurité de la ressource. Ce document contient une définition abstraite de l'architecture Zero Trust (ZTA) et présente des modèles de déploiement généraux et des cas d'utilisation où le Zero Trust pourrait améliorer la posture globale de sécurité des technologies de l'information d'une entreprise.

Mots-clés

architecture; cybersécurité; entreprise; la sécurité du réseau ; Confiance zéro.

Remerciements

Ce document est le fruit d'une collaboration entre plusieurs organismes fédéraux et est supervisé par le Conseil fédéral des DPI. Le sous-groupe d'architecture est responsable de l'élaboration de ce document, mais il y a des personnes spécifiques qui méritent d'être reconnues. Il s'agit notamment de Greg Holden, chef de projet du projet ZTA du Federal CIO Council ; Alper Kerman, chef de projet pour l'effort NIST/National Cybersecurity Center of Excellence ZTA ; et Douglas Montgomery.

Audience

Ce document a pour but de décrire le Zero Trust pour les architectes de sécurité d'entreprise. Il vise à faciliter la compréhension du Zero Trust pour les systèmes civils non classifiés et à fournir une feuille de route pour migrer et déployer des concepts de sécurité Zero Trust dans un environnement d'entreprise. Les responsables de la cybersécurité des agences, les administrateurs réseau et les gestionnaires peuvent également obtenir des informations sur le Zero Trust et le ZTA à partir de ce document. Il n'est pas prévu qu'il s'agisse d'un plan de déploiement unique pour ZTA, car une entreprise aura des cas d'utilisation commerciaux uniques et des ressources de données qui nécessitent des protections. En commençant par une solide compréhension de l'activité et des données de l'organisation, vous adopterez une approche solide du Zero Trust.

Informations sur la marque

Toutes les marques déposées ou les marques commerciales appartiennent à leurs organisations respectives.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

Avis de divulgation de brevet

AVIS : Le Laboratoire des technologies de l'information (ITL) a demandé aux titulaires de revendications de brevet dont l'utilisation pourrait être requise pour se conformer aux directives ou aux exigences de cette publication de divulguer ces revendications de brevet à ITL. Toutefois, les titulaires de brevets ne sont pas tenus de répondre aux appels de brevets d'ITL et ITL n'a pas entrepris de recherche de brevets afin de déterminer quels brevets, le cas échéant, peuvent s'appliquer à cette publication.

À la suite de l'appel lancé par le RIT pour l'identification de revendications de brevet dont l'utilisation pourrait être nécessaire pour se conformer aux orientations ou aux exigences de la présente publication, une ou plusieurs de ces revendications ont été notifiées.

Par le biais de la publication, ITL ne prend pas position quant à la validité ou à la portée d'une revendication de brevet ou de tout droit s'y rapportant. Le ou les titulaires de brevets connus ont toutefois fourni au NIST une lettre d'assurance indiquant soit (1) une clause de non-responsabilité générale indiquant qu'ils ne détiennent pas et n'ont pas l'intention de détenir actuellement une ou plusieurs revendications de brevet essentielles, soit (2) qu'ils négocieront des licences libres de droits ou portant des redevances avec d'autres parties sur une base manifestement non discriminatoire avec des conditions et des conditions raisonnables.

Des détails peuvent être obtenus auprès de **zerotrust-arch@nist.gov.**

Aucune déclaration n'est faite ou sous-entendue qu'il s'agit de la seule licence qui pourrait être requise pour éviter la contrefaçon de brevet dans l'utilisation de cette publication.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

Table des matières (traduite non mise à jour)

1 Introduction 1
1.1 Historique des efforts Zero Trust liés aux agences fédérales 2
1.2 Structure de ce Document 2
2 Les bases du Zero Trust 4
2.1 Les principes du Zero Trust 6
2.2 Une vue Zero Trust d'un réseau 8
3 Composants logiques de l'architecture Zero Trust 9
3.1 Variantes des approches de l'architecture Zero Trust 11
3.1.1 ZTA utilise une gouvernance des identités améliorée 11
3.1.2 ZTA utilisant la micro-segmentation 12
3.1.3 ZTA à l'aide de l'infrastructure réseau et des périmètres définis par logiciel. 12
3.2 Variations déployées de l'architecture abstraite 13
3.2.1 Déploiement basé sur l'agent de périphérique/la passerelle 13
3.2.2 Déploiement basé sur Enclave 14
3.2.3 Basé sur un portail de ressources Déploiement 15
3.2.4 Application de l'appareil Bac à sable 16
3.3 Algorithme de confiance 17
3.3.1 Variations de l'algorithme de confiance 19
3.4 Composants réseau/environnement 21
3.4.1 Configuration réseau requise pour prendre en charge ZTA 21
4 Scénarios de déploiement/cas d'utilisation 23
4.1 Entreprise avec installations satellites 23
4.2 Multi-cloud/Cloud-to-Cloud Enterprise 24
4.3 Entreprise avec services contractuels et/ou accès non employé 25
4.4 Collaboration au-delà des frontières de l'entreprise 26
4.5 Entreprise avec contact public ou client Services 27
5 Menaces associées à l'architecture Zero Trust 28
5.1 Subversion du processus décisionnel de la ZTA 28
5.2 Déni de service ou perturbation du réseau 28
5.3 Identifiants volés/menaces internes 29
5.4 Visibilité sur le réseau 29

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

5.5 Stockage des informations système et réseau 30
5.6 Recours à des formats de données ou à des solutions propriétaires 30
5.7 Utilisation d'entités non physiques (NPE) dans l'administration de la ZTA 30
6 Architecture Zero Trust et interactions possibles avec les autorités fédérales existantes Direction 32
6.1 Cadre de gestion des risques ZTA et NIST 32
6.2 Cadre de confidentialité Zero Trust et NIST 32
6.3 ZTA et architecture fédérale de gestion des identités, des identifiants et des accès 33
6.4 ZTA et les connexions Internet de confiance 3.0 33
6.5 ZTA et EINSTEIN (NCPS – National Cybersecurity Protection System) 34
6.6 Programme de diagnostic et d'atténuation continus (CDM) ZTA et DHS 34
6.7 ZTA, Cloud Smart et la stratégie fédérale en matière de données 35
7 Migration vers une architecture Zero Trust 36
7.1 Pure Zero Trust Architecture 36
7.2 Architecture hybride basée sur le périmètre et ZTA 36
7.3 Étapes de l'introduction de ZTA dans un réseau architecturé basé sur le périmètre 37
7.3.1 Identifier les acteurs de l'entreprise 38
7.3.2 Identifier les actifs appartenant à l'entreprise 38
7.3.3 Identifier les processus clés et évaluer les risques associés à l'exécution Processus 39
7.3.4 Formulation de politiques pour le candidat ZTA 39
7.3.5 Identifier les solutions candidates 40
7.3.6 Déploiement initial et surveillance 40
7.3.7 Élargissement de la ZTA 41
Références 42

Liste des annexes

Annexe A — Acronymes 45
Annexe B — Lacunes relevées dans l'état actuel de la technologie en ZTA 46
B.1 Enquête technologique 46
B.2 Lacunes qui empêchent un passage immédiat à ZTA 47
B.2.1 Absence de termes communs pour la conception, la planification et l'approvisionnement de ZTA 47

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

B.2.2 Perception que ZTA entre en conflit avec la cybersécurité fédérale existante Manifeste

B.3 Lacunes systémiques qui ont un impact sur ZTA 47

B.3.3 Standardisation des interfaces entre Composants 47

B.3.4 Normes émergentes qui remédient à la dépendance excessive à l'égard des API propriétaires. 48

B.4 Lacunes dans les connaissances sur le ZTA et les futurs domaines de recherche 48

B.4.5 Réponse de l'attaquant à ZTA 49

B.4.6 Expérience utilisateur dans un environnement ZTA 49

B.4.7 Résilience de ZTA face aux perturbations de l'entreprise et du réseau 49

B.5 Références 50

Liste des figures

Figure 1 : Accès Zero Trust 5

Figure 2 : Logique Core Zero Trust Composants 9

Figure 3 : modèle d'agent de périphérique/passerelle 14

Figure 4 : modèle de passerelle Enclave 15

Figure 5 : Modèle de portail de ressources 16

Figure 6 : Bacs à sable d'application 17

Figure 7 : Entrée de l'algorithme de confiance 18

Figure 8 : Entreprise avec des employés à distance 24

Figure 9 : Cas d'utilisation multicloud 24

Figure 10 : Entreprise avec non-employé Accès 25

Figure 11 : Collaboration inter-entreprise 26

Figure 12 : Cycle de déploiement de ZTA 37

Liste des tables

Tableau B-1 : Résumé des lacunes relevées en matière de déploiement 46

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

1 Introduction

L'infrastructure d'une entreprise typique est devenue de plus en plus complexe. Une même entreprise peut exploiter plusieurs réseaux internes, des bureaux distants avec leur propre infrastructure locale, des personnes distantes et/ou mobiles et des services cloud. Cette complexité a dépassé les méthodes traditionnelles de sécurité réseau basée sur le périmètre, car il n'existe pas de périmètre unique et facilement identifiable pour l'entreprise. La sécurité du réseau basée sur le périmètre s'est également avérée insuffisante, car une fois que les attaquants franchissent le périmètre, les mouvements latéraux ne sont pas entravés.

Cette entreprise complexe a conduit au développement d'un nouveau modèle de cybersécurité connu sous le nom de « Zero Trust » (ZT). Une approche ZT est principalement axée sur la protection des données et des services, mais peut et doit être étendue pour inclure tous les actifs de l'entreprise (appareils, composants d'infrastructure, applications, composants virtuels et cloud) et les sujets (utilisateurs finaux, applications et autres entités non humaines qui demandent des informations aux ressources). Dans l'ensemble du présent document, le terme « objet » sera utilisé, à moins que la section ne se rapporte directement à un utilisateur final humain, dans laquelle le terme « utilisateur » sera spécifiquement utilisé au lieu du terme « objet » plus générique. Les modèles de sécurité Zero Trust supposent qu'un attaquant est présent dans l'environnement et qu'un environnement appartenant à l'entreprise n'est pas différent, voire plus fiable, qu'un environnement n'appartenant pas à l'entreprise. Dans ce nouveau paradigme, une entreprise ne doit supposer aucune confiance implicite et analyser et évaluer en permanence les risques pour ses actifs et ses fonctions commerciales, puis mettre en place des mesures de protection pour atténuer ces risques. Dans le cadre du Zero Trust, ces protections impliquent généralement de minimiser l'accès aux ressources (telles que les données et les ressources de calcul et les applications/services) aux seuls sujets et actifs identifiés comme nécessitant un accès, ainsi que d'authentifier et d'autoriser en permanence l'identité et le niveau de sécurité de chaque demande d'accès.

Une architecture Zero Trust (ZTA) est une architecture de cybersécurité d'entreprise basée sur les principes Zero Trust et conçue pour prévenir les violations de données et limiter les mouvements latéraux internes. Cette publication traite de ZTA, de ses composants logiques, des scénarios de déploiement possibles et des menaces. Il présente également une feuille de route générale pour les organisations souhaitant migrer vers une approche de conception Zero Trust et aborde les politiques fédérales pertinentes qui peuvent avoir un impact ou influencer une architecture Zero Trust.

ZT n'est pas une architecture unique, mais un ensemble de principes directeurs pour le flux de travail, la conception du système et les opérations qui peuvent être utilisés pour améliorer la posture de sécurité de n'importe quelle classification ou niveau de sensibilité [FIPS199]. La transition vers ZTA est un voyage concernant la façon dont une organisation évalue les risques dans sa mission et ne peut pas simplement être accomplie avec un remplacement complet de la technologie. Cela dit, de nombreuses organisations ont déjà des éléments d'un ZTA dans leur infrastructure d'entreprise aujourd'hui. Les entreprises doivent s'efforcer de mettre en œuvre progressivement des principes Zero Trust, des changements de processus et des solutions technologiques qui protègent leurs actifs de données et leurs fonctions commerciales par cas d'utilisation. La plupart des infrastructures d'entreprise fonctionneront en mode hybride Zero Trust/basé sur le périmètre, tout en continuant à investir dans des initiatives de modernisation

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

informatique et à améliorer les processus métier de l'organisation.

Les organisations doivent mettre en œuvre des pratiques complètes de sécurité de l'information et de résilience pour que le Zero Trust soit efficace. Lorsqu'il est mis en balance avec les politiques et les conseils de cybersécurité existants, la gestion des identités et des accès, la surveillance continue et les meilleures pratiques, un ZTA peut protéger contre les menaces courantes et améliorer la posture de sécurité d'une organisation en utilisant une approche de gestion des risques.

1.1 Historique des efforts Zero Trust liés aux agences fédérales

Le concept de Zero Trust est présent dans la cybersécurité avant même que le terme « Zero Trust » ne soit inventé. La Defense Information Systems Agency (DISA) et le ministère de la Défense ont publié leurs travaux sur une stratégie d'entreprise plus sécurisée baptisée « black core » (BCORE). Le noyau noir impliquait de passer d'un modèle de sécurité basé sur le périmètre à un modèle axé sur la sécurité des transactions individuelles. Les travaux du Forum de Jéricho en 2004 ont fait connaître l'idée de la dépérimétisation, c'est-à-dire la limitation de la confiance implicite basée sur l'emplacement du réseau et les limites de la dépendance à des défenses uniques et statiques sur un grand segment de réseau [JERICHO]. Les concepts de dépérimétisation ont évolué et se sont améliorés pour devenir le concept plus large de Zero Trust, qui a ensuite été inventé par John Kindervag[1] alors qu'il travaillait chez Forrester.[2] Le Zero Trust est alors devenu le terme utilisé pour décrire diverses solutions de cybersécurité qui ont éloigné la sécurité de la confiance implicite basée sur l'emplacement du réseau et se sont plutôt concentrées sur l'évaluation de la confiance par transaction. L'industrie privée et l'enseignement supérieur ont également connu cette évolution, passant d'une sécurité basée sur le périmètre à une stratégie de sécurité basée sur les principes du Zero Trust.

Depuis plus d'une décennie, les agences fédérales sont invitées à adopter une sécurité basée sur les principes Zero Trust, en renforçant leurs capacités et leurs politiques telles que la Federal Information Security Modernization Act (FISMA) suivie du Risk Management Framework (RMF) ; la gestion fédérale de l'identité, des titres d'identité et des accès (FICAM) ; Trusted Internet Connections (TIC) ; et les programmes de diagnostic et d'atténuation continus (CDM). Tous ces programmes visent à restreindre l'accès aux données et aux ressources aux parties autorisées. Lorsque ces programmes ont été lancés, ils étaient limités par les capacités techniques des systèmes d'information. Les politiques de sécurité étaient en grande partie statiques et étaient appliquées à de grands « points d'étranglement » qu'une entreprise pouvait contrôler pour obtenir le plus grand effet possible de l'effort. Au fur et à mesure que la technologie évolue, il devient possible d'analyser et d'évaluer en permanence les demandes d'accès de manière dynamique et granulaire afin d'atténuer l'exposition des données due à des comptes compromis, à des attaquants surveillant un réseau et à d'autres menaces.

1.2 Structure du présent document

Le reste du document est organisé comme suit :

- **La section 2** définit ZT et ZTA et énumère certaines hypothèses lors de la conception d'un ZTA pour une entreprise. Cette section comprend également une liste des principes de la conception ZT.
- **La section 3** documente les composants logiques, ou blocs de construction, de ZT. Il est possible que des implémentations uniques composent différemment les composants ZTA

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

tout en servant les mêmes fonctionnalités logiques.

[1] https://go.forrester.com/blogs/next-generation-access-and-zero-trust/

[2] Toute mention de produits ou de services commerciaux dans les documents du NIST n'est fournie qu'à titre d'information ; elle n'implique pas une recommandation ou une approbation de la part du NIST.

- **La section 4** énumère quelques cas d'utilisation possibles où un ZTA peut rendre les environnements d'entreprise plus sûrs et moins susceptibles d'être exploités avec succès. Il s'agit notamment d'entreprises avec des employés à distance, de services cloud et de réseaux invités.
- **La section 5** traite des menaces qui pèsent sur une entreprise à l'aide d'un ZTA. Bon nombre de ces menaces sont similaires à n'importe quel réseau architecturé, mais peuvent nécessiter des techniques d'atténuation différentes.
- **La section 6** traite de la façon dont les principes de la ZTA s'intègrent dans les directives existantes pour les organismes fédéraux et/ou les complètent.
- **La section 7** présente le point de départ de la transition d'une entreprise (comme un organisme fédéral) vers une ZTA. Cela inclut une description des étapes générales nécessaires à la planification et au déploiement d'applications et d'une infrastructure d'entreprise guidées par les principes de ZT.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

2 Zero Trust Basics

Le Zero Trust est un paradigme de cybersécurité axé sur la protection des ressources et le principe selon lequel la confiance n'est jamais accordée implicitement, mais doit être évaluée en permanence. L'architecture Zero Trust est une approche de bout en bout de la sécurité des ressources et des données de l'entreprise qui englobe l'identité (personnes et entités non personnelles), les informations d'identification, la gestion des accès, les opérations, les points de terminaison, les environnements d'hébergement et l'infrastructure d'interconnexion. L'objectif initial devrait être de limiter les ressources à ceux qui ont besoin d'accéder et de n'accorder que les privilèges minimaux (par exemple, lecture, écriture, suppression) nécessaires à l'exécution de la mission. Traditionnellement, les agences (et les réseaux d'entreprise en général) se sont concentrés sur la défense du périmètre et les sujets authentifiés ont un accès autorisé à une large collection de ressources une fois sur le réseau interne. Par conséquent, les mouvements latéraux non autorisés dans l'environnement ont été l'un des plus grands défis pour les agences fédérales.

Les connexions Internet de confiance (TIC) et les pare-feu de périmètre d'agence fournissent des passerelles Internet puissantes. Cela permet de bloquer les attaquants sur Internet, mais les TIC et les pare-feu de périmètre sont moins utiles pour détecter et bloquer les attaques provenant de l'intérieur du réseau et ne peuvent pas protéger les sujets en dehors du périmètre de l'entreprise (par exemple, les travailleurs à distance, les services basés sur le cloud, les appareils de périphérie, etc.).

Une définition opérationnelle de l'architecture Zero Trust et Zero Trust est la suivante :

> *Le Zero Trust* (ZT) fournit un ensemble de concepts et d'idées conçus pour minimiser l'incertitude dans l'application de décisions d'accès précises, du moindre privilège par demande, dans les systèmes et services d'information face à un réseau considéré comme compromis. *L'architecture Zero Trust* (ZTA) est un plan de cybersécurité d'entreprise qui utilise des concepts Zero Trust et englobe les relations entre les composants, la planification des flux de travail et les politiques d'accès. Par conséquent, une entreprise Zero Trust est l'infrastructure réseau (physique et virtuelle) et les politiques opérationnelles qui sont en place pour une entreprise dans le cadre d'un plan d'architecture Zero Trust.

Une entreprise décide d'adopter le Zero Trust comme stratégie de base et de générer une architecture Zero Trust sous la forme d'un plan élaboré en tenant compte des principes Zero Trust (voir la section 2.1 ci-dessous). Ce plan est ensuite déployé pour produire un environnement Zero Trust à utiliser dans l'entreprise.

Cette définition se concentre sur le nœud du problème, à savoir l'objectif d'empêcher l'*accès non autorisé aux données et aux services*, tout en rendant l'*application du contrôle d'accès aussi granulaire que possible*. En d'autres termes, les sujets autorisés et approuvés (combinaison de l'utilisateur, de l'application (ou du service) et de l'appareil) peuvent accéder aux données à l'exclusion de tous les autres sujets (c'est-à-dire les attaquants). Pour aller plus loin, le mot « ressource » peut être substitué au mot « données » de sorte que ZT et ZTA concernent l'accès aux ressources (par exemple, les imprimantes, les ressources de calcul, les actionneurs de l'Internet des objets [IoT]) et pas seulement l'accès aux données.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

Pour réduire les incertitudes (car elles ne peuvent pas être éliminées), l'accent est mis sur l'authentification, l'autorisation et la réduction des zones de confiance implicites tout en maintenant la disponibilité et en minimisant les retards temporels dans les mécanismes d'authentification. Les règles d'accès sont aussi granulaires que possible afin d'appliquer les privilèges les moins nécessaires pour effectuer l'action dans la demande.

Dans le modèle abstrait d'accès illustré à la figure 1, un sujet doit accéder à une ressource d'entreprise. L'accès est accordé par le biais d'un point de décision stratégique (PDP) et d'un point d'application de politique (PEP) correspondant.[3]

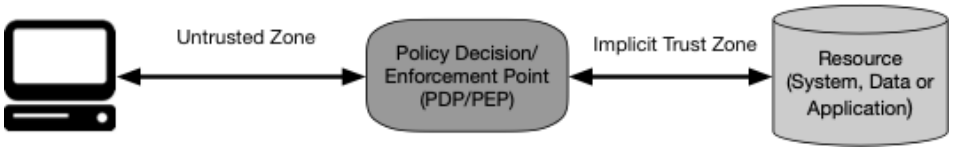


Figure 1 : Accès Zero Trust

Le système doit s'assurer que l'objet est authentique et que la demande est valide. Le PDP/PEP rend un jugement approprié pour permettre au sujet d'accéder à la ressource. Cela implique que le Zero Trust s'applique à deux domaines fondamentaux : l'authentification et l'autorisation. Quel est le niveau de confiance quant à l'identité du sujet pour cette demande unique ? L'accès à la ressource est-il permis compte tenu du niveau de confiance dans l'identité du sujet ? L'appareil utilisé pour la demande dispose-t-il d'une posture de sécurité appropriée ? Y a-t-il d'autres facteurs qui devraient être pris en compte et qui modifient le niveau de confiance (p. ex., l'heure, l'emplacement du sujet, la posture de sécurité du sujet) ? Dans l'ensemble, les entreprises doivent élaborer et maintenir des politiques dynamiques basées sur les risques pour l'accès aux ressources et mettre en place un système pour s'assurer que ces politiques sont appliquées correctement et de manière cohérente pour les demandes d'accès aux ressources individuelles. Cela signifie qu'une entreprise ne doit pas s'appuyer sur une fiabilité implicite dans laquelle si le sujet a atteint un niveau d'authentification de base (par exemple, en se connectant à une ressource), toutes les demandes de ressources ultérieures sont supposées être tout aussi valides.

La « zone de confiance implicite » représente une zone où toutes les entités sont approuvées au moins au niveau de la dernière passerelle PDP/PEP. Prenons l'exemple du modèle de contrôle des passagers dans un aéroport. Tous les passagers passent le contrôle de sécurité de l'aéroport (PDP/PEP) pour accéder aux portes d'embarquement. Les passagers, les employés de l'aéroport, l'équipage de l'avion, etc., se pressent dans la zone du terminal, et toutes les personnes sont considérées comme dignes de confiance. Dans ce modèle, la zone de confiance implicite est la zone d'embarquement.

Le PDP/PEP applique un ensemble de contrôles afin que tout le trafic au-delà du PEP ait un niveau de confiance commun. Le PDP/PEP ne peut pas appliquer de politiques supplémentaires au-delà de son emplacement dans le flux de trafic. Pour permettre au PDP/PEP d'être aussi précis que possible, la zone de confiance implicite doit être aussi petite que possible.

Le Zero Trust fournit un ensemble de principes et de concepts pour rapprocher les PDP/PEP de la ressource. L'idée est d'authentifier et d'autoriser explicitement tous les sujets, actifs et flux de

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

travail qui composent l'entreprise.

[3] Partie des concepts définis dans OASIS XACML 2.0 https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

2.1 Les principes du Zero Trust

De nombreuses définitions et discussions sur ZT mettent l'accent sur le concept de suppression des défenses périmétriques étendues (par exemple, les pare-feu d'entreprise) en tant que facteur. Cependant, la plupart de ces définitions continuent de se définir par rapport aux périmètres d'une manière ou d'une autre (comme la micro-segmentation ou les micro-périmètres ; voir la section 3.1) dans le cadre des capacités fonctionnelles d'un ZTA. Ce qui suit est une tentative de définir ZT et ZTA en termes de principes de base qui devraient être impliqués plutôt que ce qui est exclu. Ces principes constituent l'objectif idéal, même s'il faut reconnaître que tous les principes ne peuvent pas être pleinement mis en œuvre dans leur forme la plus pure pour une stratégie donnée.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

Une architecture Zero Trust est conçue et déployée dans le respect des principes de base Zero Trust suivants :

1. **Toutes les sources de données et tous les services informatiques sont considérés comme des ressources.** Un réseau peut être composé de plusieurs classes d'appareils. Un réseau peut également avoir des dispositifs à faible encombrement qui envoient des données à des agrégateurs/stockage, des logiciels en tant que service (SaaS), des systèmes envoyant des instructions à des actionneurs et d'autres fonctions. En outre, une entreprise peut décider de classer les appareils personnels en tant que ressources si elle peut accéder à des ressources appartenant à l'entreprise.
2. **Toutes les communications sont sécurisées, quel que soit l'emplacement du réseau.** L'emplacement du réseau seul n'implique pas la confiance. Les demandes d'accès à partir de ressources situées sur une infrastructure réseau appartenant à l'entreprise (par exemple, à l'intérieur d'un périmètre de réseau hérité) doivent répondre aux mêmes exigences de sécurité que les demandes d'accès et les communications à partir de tout autre réseau n'appartenant pas à l'entreprise. En d'autres termes, la confiance ne doit pas être automatiquement accordée en fonction de la présence de l'appareil sur l'infrastructure réseau de l'entreprise. Toutes les communications doivent être effectuées de la manière la plus sécurisée possible, protéger la confidentialité et l'intégrité, et fournir une authentification à la source.
3. **L'accès aux ressources individuelles de l'entreprise est accordé à la session.** La confiance dans le demandeur est évaluée avant que l'accès ne soit accordé. L'accès doit également être accordé avec le moins de privilèges nécessaires pour accomplir la tâche. Il peut s'agir uniquement d'un « moment récent » pour cette transaction particulière et ne pas se produire directement avant le lancement d'une session ou l'exécution d'une transaction avec une ressource. Toutefois, l'authentification et l'autorisation d'une ressource n'accordent pas automatiquement l'accès à une autre ressource.
4. **L'accès aux ressources est déterminé par une politique dynamique, y compris l'état observable de l'identité du client, de l'application/du service et de l'actif demandeur, et peut inclure d'autres attributs comportementaux et environnementaux.** Une organisation protège les ressources en définissant les ressources dont elle dispose, qui sont ses membres (ou la capacité d'authentifier les utilisateurs d'une communauté fédérée) et l'accès aux ressources dont ces membres ont besoin. Pour Zero Trust, l'identité du client peut inclure le compte d'utilisateur (ou l'identité de service) et tous les attributs

associés attribués par l'entreprise à ce compte ou les artefacts permettant d'authentifier les tâches automatisées. L'état de la ressource demandée peut inclure des caractéristiques de l'appareil telles que les versions logicielles installées, l'emplacement réseau, l'heure/la date de la demande, le comportement précédemment observé et les informations d'identification installées. Les attributs comportementaux comprennent, sans s'y limiter, l'analyse automatisée des sujets, l'analyse des appareils et les écarts mesurés par rapport aux modèles d'utilisation observés. La stratégie est l'ensemble des règles d'accès basées sur les attributs qu'une organisation attribue à un sujet, à une ressource de données ou à une application. Les attributs environnementaux peuvent inclure des facteurs tels que le demandeur l'emplacement du réseau, l'heure, les attaques actives signalées, etc. Ces règles et attributs sont basés sur les besoins du processus opérationnel et le niveau de risque acceptable. Les politiques d'accès aux ressources et d'autorisation d'action peuvent varier en fonction de la sensibilité de la ressource/des données. Les principes du moindre privilège sont appliqués pour restreindre à la fois la visibilité et l'accessibilité.

5. **L'entreprise surveille et mesure l'intégrité et la sécurité de tous les actifs détenus et associés.** Aucun actif n'est intrinsèquement fiable. L'entreprise évalue la posture de sécurité de l'actif lors de l'évaluation d'une demande de ressource. Une entreprise mettant en œuvre un ZTA doit établir un système de diagnostic et d'atténuation continus (CDM) ou un système similaire pour surveiller l'état des appareils et des applications et doit appliquer des correctifs/correctifs si nécessaire. Les ressources dont il s'avère qu'elles sont subverties, qui présentent des vulnérabilités connues et/ou qui ne sont pas gérées par l'entreprise peuvent être traitées différemment (y compris le refus de toutes les connexions aux ressources de l'entreprise) que les appareils appartenant à l'entreprise ou associés à celle-ci qui sont considérés comme étant dans leur état le plus sécurisé. Cela peut également s'appliquer aux appareils associés (par exemple, les appareils personnels) qui peuvent être autorisés à accéder à certaines ressources, mais pas à d'autres. Cela nécessite également la mise en place d'un système de surveillance et de reporting robuste pour fournir des données exploitables sur l'état actuel des ressources de l'entreprise.
6. **L'authentification et l'autorisation de toutes les ressources sont dynamiques et strictement appliquées avant que l'accès ne soit autorisé.** Il s'agit d'un cycle constant d'obtention d'accès, d'analyse et d'évaluation des menaces, d'adaptation et de réévaluation continue de la confiance dans la communication continue. Une entreprise mettant en œuvre un ZTA devrait disposer de systèmes de gestion des identités, des identifiants et des accès (ICAM) et de gestion des actifs. Cela inclut l'utilisation de l'authentification multifacteur (MFA) pour l'accès à certaines ou à toutes les ressources de l'entreprise. Une surveillance continue avec possibilité de réauthentification et de réautorisation se produit tout au long des transactions de l'utilisateur, telles que définies et appliquées par la politique (par exemple, basée sur le temps, nouvelle ressource demandée, modification de la ressource, activité anormale du sujet détectée) qui s'efforce d'atteindre un équilibre entre sécurité, disponibilité, facilité d'utilisation et rentabilité.
7. **L'entreprise recueille autant d'informations que possible sur l'état actuel des actifs, de l'infrastructure réseau et des communications et les utilise pour améliorer sa posture de sécurité.** Une entreprise doit collecter des données sur la posture de sécurité des actifs, le trafic réseau et les demandes d'accès, traiter ces données et utiliser toutes les informations obtenues pour améliorer la création et l'application des politiques. Ces données peuvent également être utilisées pour fournir un contexte aux demandes d'accès des sujets (voir la section 3.3.1).

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

Les principes ci-dessus tentent d'être agnostiques en matière de technologie. Par exemple, l'« identification de l'utilisateur (ID) » peut inclure plusieurs facteurs tels que le nom d'utilisateur/le mot de passe, les certificats et le mot de passe à usage unique. Ces principes s'appliquent au travail effectué au sein d'une organisation ou en collaboration avec une ou plusieurs organisations partenaires, et non aux processus opérationnels anonymes, publics ou destinés aux consommateurs. Une organisation ne peut pas imposer de politiques internes à des acteurs externes (par exemple, des clients ou des utilisateurs d'Internet en général), mais peut être en mesure de mettre en œuvre certaines politiques basées sur ZT pour les utilisateurs non professionnels qui ont une relation spéciale avec l'organisation (par exemple, les clients enregistrés, les personnes à charge des employés, etc.).

2.2 Une vue Zero Trust d'un réseau

Il existe quelques hypothèses de base pour la connectivité réseau pour toute organisation qui utilise ZTA dans la planification et le déploiement du réseau. Certaines de ces hypothèses s'appliquent à l'infrastructure réseau appartenant à l'entreprise, et d'autres s'appliquent aux ressources appartenant à l'entreprise fonctionnant sur infrastructure réseau n'appartenant pas à l'entreprise (par exemple, fournisseurs de Wi-Fi public ou de cloud public). Ces hypothèses sont utilisées pour diriger la formation d'un ZTA. Le réseau d'une entreprise mettant en œuvre un ZTA doit être développé selon les principes du ZTA décrits ci-dessus et avec les hypothèses suivantes.

1. **L'ensemble du réseau privé de l'entreprise n'est pas considéré comme une zone de confiance implicite.** Les actifs doivent toujours agir comme si un attaquant était présent sur le réseau de l'entreprise, et la communication doit se faire de la manière la plus sécurisée possible (voir le principe 2 ci-dessus). Cela implique des actions telles que l'authentification de toutes les connexions et le chiffrement de tout le trafic.
2. **Les périphériques du réseau ne doivent pas appartenir à l'entreprise ou ne pas être configurables par celle-ci.** Les visiteurs et/ou les services contractuels peuvent inclure des actifs n'appartenant pas à l'entreprise qui ont besoin d'un accès au réseau pour remplir leur rôle. Cela inclut les stratégies BYOD (Bring Your Own Device) qui permettent aux sujets d'entreprise d'utiliser des appareils n'appartenant pas à l'entreprise pour accéder aux ressources de l'entreprise.
3. **Aucune ressource n'est intrinsèquement fiable.** La posture de sécurité de chaque actif doit être évaluée via une PPE avant qu'une demande ne soit accordée à une ressource appartenant à l'entreprise (similaire au principe 6 ci-dessus pour les actifs et les sujets). Cette évaluation doit être continue aussi longtemps que dure la session. Les appareils appartenant à l'entreprise peuvent avoir des artefacts qui permettent l'authentification et fournissent un niveau de confiance supérieur à la même demande provenant d'appareils n'appartenant pas à l'entreprise. Les informations d'identification du sujet seules ne suffisent pas pour l'authentification de l'appareil auprès d'une ressource d'entreprise.
4. **Toutes les ressources de l'entreprise ne se trouvent pas sur une infrastructure appartenant à l'entreprise.** Les ressources comprennent des sujets d'entreprise à distance ainsi que des services cloud. Les actifs appartenant à l'entreprise ou gérés peuvent avoir besoin d'utiliser le réseau local (c'est-à-dire non entreprise) pour la connectivité de base et les services réseau (par exemple, la résolution DNS).

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

5. **Les sujets et les ressources d'entreprise distants ne peuvent pas faire entièrement confiance à leur connexion au réseau local.** Les sujets distants doivent supposer que le réseau local (c'est-à-dire n'appartenant pas à l'entreprise) est hostile. Les ressources doivent supposer que tout le trafic est surveillé et potentiellement modifié. Toutes les demandes de connexion doivent être authentifiées et autorisées, et toutes les communications doivent être effectuées de la manière la plus sécurisée possible (c'est-à-dire assurer la confidentialité, la protection de l'intégrité et l'authentification de la source). Voir les principes de ZTA ci-dessus.
6. **Les ressources et les flux de travail qui se déplacent entre l'infrastructure d'entreprise et l'infrastructure externe doivent avoir une politique et une posture de sécurité cohérentes.** Les actifs et les charges de travail doivent conserver leur niveau de sécurité lorsqu'ils se déplacent vers ou depuis une infrastructure appartenant à l'entreprise. Cela inclut les appareils qui se déplacent des réseaux d'entreprise vers les réseaux non d'entreprise (c'est-à-dire les utilisateurs distants). Cela inclut également les charges de travail migrant des centres de données sur site vers des instances cloud non professionnelles.

3 Composants logiques de l'architecture Zero Trust

Il existe de nombreux composants logiques qui composent un déploiement ZTA dans une entreprise. Ces composants peuvent être exploités en tant que service sur site ou par le biais d'un service basé sur le cloud. Le modèle de cadre conceptuel de la figure 2 montre la relation de base entre les composants et leurs interactions. Notez qu'il s'agit d'un modèle idéal montrant les composants logiques et leurs interactions. À partir de la figure 1, le point de décision de stratégie (PDP) est décomposé en deux composants logiques : le moteur de stratégie et l'administrateur de stratégie (définis ci-dessous). Les composants logiques ZTA utilisent un plan de contrôle distinct pour communiquer, tandis que les données d'application sont communiquées sur un plan de données (voir la section 3.4).

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

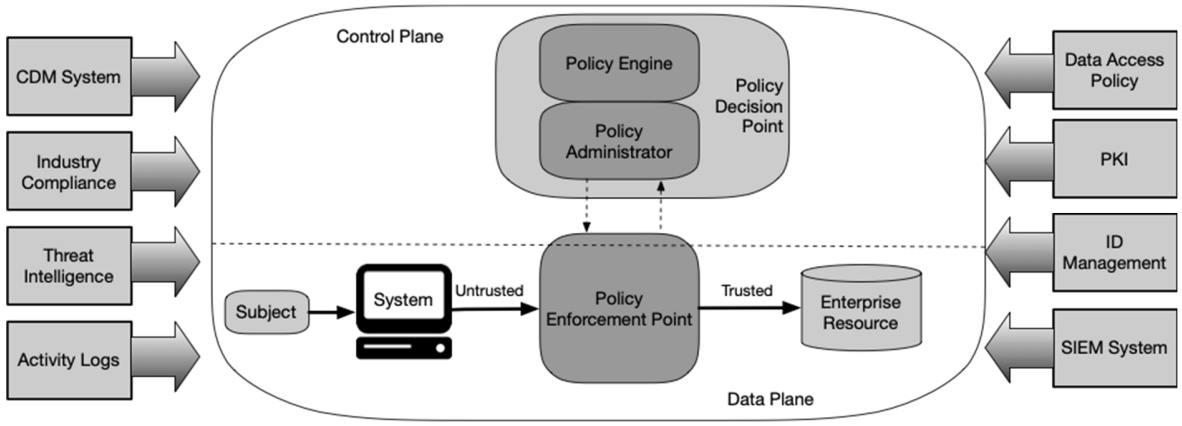


Figure 2 : Composants logiques Zero Trust de base

Les descriptions des composants :

- **Moteur de politiques (PE) :** ce composant est responsable de la décision finale d'accorder l'accès à une ressource pour un sujet donné. Le PE utilise la politique d'entreprise ainsi que des données provenant de sources externes (par exemple, les systèmes CDM, les services de renseignement sur les menaces décrits ci-dessous) comme entrée dans un algorithme de confiance (voir la section 3.3 pour plus de détails) pour accorder, refuser ou révoquer l'accès à la ressource. Le PE est associé au composant administrateur de stratégie. Le moteur de stratégies prend et consigne la décision (telle qu'approuvée ou refusée), et l'administrateur de stratégies exécute la décision.
- **Administrateur de stratégie (PA) :** ce composant est chargé d'établir et/ou d'arrêter le chemin de communication entre un sujet et une ressource (via des commandes aux PEP concernées). Il génère tout jeton ou référence d'authentification spécifique à une session et d'authentification utilisé par un client pour accéder à une ressource d'entreprise. Il est étroitement lié à l'EP et s'appuie sur sa décision d'autoriser ou de refuser une séance. Si la session est autorisée et la demande authentifiée, l'AP configure la PPE pour permettre le démarrage de la session. Si la session est refusée (ou si une approbation précédente est annulée), le PA signale au PEP d'arrêter la connexion. Certaines implémentations

peuvent traiter le PE et le PA comme un seul service ; ici, il est divisé en deux composantes logiques. L'AP communique avec le PEP lors de la création du chemin de communication. Cette communication se fait via le plan de contrôle.

- **Point d'application de la politique (PEP) :** ce système est chargé d'activer, de surveiller et éventuellement de mettre fin aux connexions entre un sujet et une ressource d'entreprise. Le PPE communique avec le DP pour transmettre les demandes et/ou recevoir des mises à jour des politiques de la part du DP. Il s'agit d'un composant logique unique dans ZTA, mais il peut être divisé en deux composants différents : le client (par exemple, un agent sur un ordinateur portable) et le côté ressource (par exemple, un composant de passerelle devant la ressource qui contrôle l'accès) ou un composant de portail unique qui agit comme un gardien des chemins de communication. Au-delà de la PPE se trouve la zone de confiance (voir section 2) qui héberge la ressource d'entreprise.

En plus des composants de base d'une entreprise mettant en œuvre un ZTA, plusieurs sources de données fournissent des informations et des règles de politique utilisées par le moteur de règles lors de la prise de décisions d'accès. Il s'agit notamment de sources de données locales ainsi que de sources de données externes (c'est-à-dire non contrôlées ou créées par l'entreprise). Il peut s'agir de :

- **Système de diagnostic et d'atténuation continus (CDM) :** il rassemble des informations sur l'état actuel de l'actif de l'entreprise et applique des mises à jour à la configuration et aux composants logiciels. Un système CDM d'entreprise fournit au moteur de stratégies des informations sur la ressource qui effectue une demande d'accès, par exemple si elle exécute le système d'exploitation corrigé approprié, l'intégrité des composants logiciels approuvés par l'entreprise ou la présence de composants non approuvés et si la ressource présente des vulnérabilités connues. Les systèmes CDM sont également chargés d'identifier et éventuellement d'appliquer un sous-ensemble de politiques sur les appareils non professionnels actifs sur l'infrastructure de l'entreprise.
- **Système de conformité sectorielle :** Cela permet de s'assurer que l'entreprise reste conforme à tout régime réglementaire auquel elle peut être soumise (par exemple, FISMA, exigences de sécurité de l'information du secteur de la santé ou de la finance). Cela inclut toutes les règles de politique qu'une entreprise élabore pour assurer la conformité.
- **Flux(s) de renseignements sur les menaces :** il fournit des informations provenant de sources internes ou externes qui aident le moteur de stratégies à prendre des décisions d'accès. Il peut s'agir de plusieurs services qui prennent des données de sources internes et/ou externes et fournissent des informations sur les attaques ou les vulnérabilités récemment découvertes. Cela inclut également les failles logicielles récemment découvertes, les programmes malveillants récemment identifiés et les attaques signalées contre d'autres ressources auxquelles le moteur de règles voudra refuser l'accès à partir des ressources de l'entreprise.
- **Journaux d'activité du réseau et du système :** ce système d'entreprise regroupe les journaux d'actifs, le trafic réseau, les actions d'accès aux ressources et d'autres événements qui fournissent des informations en temps réel (ou en temps quasi réel) sur la posture de sécurité des systèmes d'information d'entreprise.
- **Stratégies d'accès aux données :** il s'agit des attributs, des règles et des stratégies relatifs à l'accès aux ressources de l'entreprise. Cet ensemble de règles peut être encodé

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

(via l'interface de gestion) ou généré dynamiquement par le moteur de stratégies. Ces stratégies sont le point de départ de l'autorisation d'accès à une ressource, car elles fournissent les privilèges d'accès de base pour les comptes et les applications/services de l'entreprise. Ces politiques doivent être fondées sur la mission, les rôles et les besoins définis de l'organisation.

- **Infrastructure à clé publique (PKI) d'entreprise :** ce système est responsable de la génération et de la journalisation des certificats émis par l'entreprise pour les ressources, les sujets, les services et les applications. Cela inclut également l'écosystème mondial des autorités de certification et l'ICP fédérale[4], qui peut ou non être intégrée à l'ICP de l'entreprise. Il peut également s'agir d'une PKI qui n'est pas construite sur des certificats X.509.
- **Système de gestion des identifiants :** il est responsable de la création, du stockage et de la gestion des comptes d'utilisateurs d'entreprise et des enregistrements d'identité (par exemple, un serveur LDAP (Lightweight Directory Access Protocol)). Ce système contient les informations nécessaires (par exemple, le nom, l'adresse e-mail, les certificats) et d'autres caractéristiques de l'entreprise telles que le rôle, les attributs d'accès et les ressources attribuées. Ce système utilise souvent d'autres systèmes (tels qu'une PKI) pour les artefacts associés aux comptes d'utilisateurs. Ce système peut faire partie d'une communauté fédérée plus large et peut inclure des employés non liés à l'entreprise ou des liens vers des actifs non liés à l'entreprise à des fins de collaboration.
- **Système de gestion des informations et des événements de sécurité (SIEM) :** il collecte des informations centrées sur la sécurité pour une analyse ultérieure. Ces données sont ensuite utilisées pour affiner les politiques et avertir d'éventuelles attaques contre les actifs de l'entreprise.

3.1 Variantes des approches de l'architecture Zero Trust

Il existe plusieurs façons pour une entreprise d'adopter un ZTA pour les flux de travail. Ces approches varient dans les composants utilisés et dans la principale source de règles de politique d'une organisation. Chaque approche met en œuvre tous les principes de ZT (voir la section 2.1), mais peut utiliser un ou deux (ou un composant) comme principal moteur des politiques. Une solution ZT complète comprendra des éléments des trois approches. Ces approches comprennent une gouvernance des identités améliorée, une micro-segmentation logique et une segmentation basée sur le réseau.

Certaines approches se prêtent plus à certains cas d'utilisation que d'autres. Une organisation qui cherche à développer un ZTA pour son entreprise peut constater que le cas d'utilisation qu'elle a choisi et les politiques existantes pointent vers une approche plutôt que d'autres. Cela ne signifie pas que les autres approches ne fonctionneraient pas, mais plutôt que d'autres approches pourraient être plus difficiles à mettre en œuvre et nécessiter des changements plus fondamentaux dans la façon dont l'entreprise gère actuellement ses activités.

3.1.1 ZTA utilise une gouvernance des identités améliorée

L'approche améliorée de gouvernance de l'identité pour l'élaboration d'un ZTA utilise l'identité des acteurs comme élément clé de la création de la politique. S'il n'y avait pas de sujets demandant l'accès aux ressources de l'entreprise, il n'aurait pas été nécessaire de créer des politiques d'accès. Pour cette approche, les stratégies d'accès aux ressources d'entreprise sont

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

basées sur l'identité et les attributs attribués. La principale exigence d'accès aux ressources est basée sur les privilèges d'accès accordés à l'objet donné. D'autres facteurs, tels que l'appareil utilisé, l'état des actifs et les facteurs environnementaux, peuvent modifier le calcul final du niveau de confiance (et l'autorisation d'accès final) ou adapter le résultat d'une manière ou d'une autre, par exemple en n'accordant qu'un accès partiel à une source de données donnée en fonction de l'emplacement du réseau. Ressources individuelles ou PPE

[4] https://www.idmanagement.gov/topics/fpki/

Les composants protégeant la ressource doivent disposer d'un moyen de transmettre les demandes à un service du moteur de stratégies ou d'authentifier l'objet et d'approuver la demande avant d'accorder l'accès.

Les approches améliorées basées sur la gouvernance des identités pour les entreprises sont souvent utilisées à l'aide d'un modèle de réseau ouvert ou d'un réseau d'entreprise avec un accès visiteur ou des appareils non professionnels fréquents sur le réseau (comme avec le cas d'utilisation de la section 4.3 ci-dessous). L'accès au réseau est initialement accordé à toutes les ressources, mais l'accès aux ressources de l'entreprise est limité aux identités disposant des privilèges d'accès appropriés. Il y a un inconvénient à accorder une connectivité réseau de base, car les acteurs malveillants pourraient toujours tenter de reconnaître le réseau et/ou utiliser le réseau pour lancer des attaques par déni de service, en interne ou contre un tiers. Les entreprises doivent toujours surveiller et répondre à ce comportement avant qu'il n'affecte les flux de travail.

L'approche basée sur l'identité fonctionne bien avec le modèle de portail de ressources (voir la section 3.2.3), car l'identité et l'état de l'appareil fournissent des données de support secondaires pour les décisions d'accès. D'autres modèles fonctionnent également, en fonction des politiques en place. Les approches axées sur l'identité fonctionnent également bien pour les entreprises qui utilisent des applications/services basés sur le cloud qui peuvent ne pas permettre l'utilisation de composants de sécurité ZT détenus ou exploités par l'entreprise (tels que de nombreuses offres SaaS). L'entreprise peut utiliser l'identité des demandeurs pour élaborer et appliquer des politiques sur ces plateformes.

3.1.2 ZTA utilisant la micro-segmentation

Une entreprise peut choisir de mettre en œuvre un ZTA en plaçant des ressources individuelles ou des groupes de ressources sur un segment de réseau unique protégé par un composant de sécurité de passerelle. Dans cette approche, l'entreprise place des périphériques d'infrastructure tels que des commutateurs intelligents (ou des routeurs) ou des pare-feu de nouvelle génération (NGFW) ou des périphériques de passerelle à usage spécial pour agir en tant que PEP protégeant chaque ressource ou petit groupe de ressources associées. Alternativement (ou en plus), l'entreprise peut choisir de mettre en œuvre une micro-segmentation basée sur l'hôte à l'aide d'agents logiciels (voir la section 3.2.1) ou de pare-feu sur le(s) actif(s) de terminaux, Ces périphériques de passerelle accordent dynamiquement l'accès aux requêtes individuelles d'un client, d'un actif ou d'un service. Selon le modèle, la passerelle peut être le seul composant PEP ou faire partie d'une PPE en plusieurs parties composée de la passerelle et de l'agent côté client (voir la section 3.2.1).

Cette approche s'applique à une variété de cas d'utilisation et de modèles de déploiement, car le dispositif de protection agit comme le PEP, la direction de ces dispositifs agissant comme le composant PE/PA. Cette approche nécessite un programme de gouvernance des identités (IGP) pour fonctionner pleinement, mais s'appuie sur les composants de passerelle pour agir en tant que PEP qui protège les ressources contre les accès et/ou la découverte non autorisés.

La principale nécessité de cette approche est que les composants PEP sont gérés et doivent être capables de réagir et de se reconfigurer selon les besoins pour répondre aux menaces ou aux changements dans le flux de travail. Il est possible de mettre en œuvre certaines fonctionnalités d'une entreprise micro-segmentée en utilisant des passerelles moins avancées et même des pare-

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

feu sans état, mais le coût d'administration et la difficulté à s'adapter rapidement aux changements en font un très mauvais choix.

3.1.3 ZTA utilisant l'infrastructure réseau et les périmètres définis par logiciel

La dernière approche utilise l'infrastructure réseau pour mettre en œuvre un ZTA. La mise en œuvre de ZTA pourrait être réalisée à l'aide d'un réseau de superposition (c'est-à-dire la couche 7), mais pourrait également être configurée à la plus basse des échelles pile réseau OSI). Ces approches sont parfois appelées approches de périmètre défini par logiciel (SDP) et incluent souvent des concepts issus des réseaux définis par logiciel (SDN) [SDNBOOK] et des réseaux basés sur l'intention (IBNVN). Dans cette approche, l'assistant de mesure agit en tant que contrôleur de réseau qui met en place et reconfigure le réseau en fonction des décisions prises par l'EP. Les clients continuent de demander l'accès via des PPE, qui sont gérées par le composant PA.

Lorsque l'approche est mise en œuvre au niveau de la couche réseau de l'application (c.-à-d. la couche 7), le modèle de déploiement le plus courant est l'agent/passerelle (voir la section 3.2.1). Dans cette implémentation, l'agent et la passerelle de ressources (agissant en tant que PEP unique et configurés par l'AP) établissent un canal sécurisé utilisé pour la communication entre le client et la ressource. Il peut y avoir d'autres variantes de ce modèle, ainsi que pour les réseaux virtuels cloud, les réseaux non basés sur IP, etc.

3.2 Variations déployées de l'architecture abstraite

Tous les composants ci-dessus sont des composants logiques. Il n'est pas nécessaire qu'il s'agisse de systèmes uniques. Un seul actif peut remplir les fonctions de plusieurs composants logiques, et de même, un composant logique peut être composé de plusieurs éléments matériels ou logiciels pour effectuer les tâches. Par exemple, une infrastructure à clé publique gérée par l'entreprise peut se composer d'un composant responsable de l'émission de certificats pour les appareils et d'un autre utilisé pour l'émission de certificats aux utilisateurs finaux, mais les deux utilisent des certificats intermédiaires émis par la même autorité de certification racine d'entreprise. Dans certaines offres de produits ZT actuellement disponibles sur le marché, les composants PE et PA sont combinés en un seul service.

Il existe plusieurs variantes du déploiement de certains composants de l'architecture, qui sont décrites dans les sections ci-dessous. Selon la configuration d'un réseau d'entreprise, plusieurs modèles de déploiement ZTA peuvent être utilisés pour différents processus métier au sein d'une même entreprise.

3.2.1 Déploiement basé sur l'agent de périphérique/la passerelle

Dans ce modèle de déploiement, le PEP est divisé en deux composants qui résident sur la ressource ou en tant que composant directement devant une ressource. Par exemple, chaque ressource fournie par l'entreprise dispose d'un agent de périphérique installé qui coordonne les connexions, et chaque ressource a un composant (c'est-à-dire une passerelle) qui est placé directement devant afin que la ressource communique uniquement avec la passerelle, servant essentiellement de proxy pour la ressource. L'agent est un composant logiciel qui dirige une partie (ou la totalité) du trafic vers la PEP appropriée afin que les demandes soient évaluées. La passerelle est chargée de communiquer avec l'administrateur de stratégie et d'autoriser uniquement les chemins de communication approuvés configurés par l'administrateur de stratégie (voir Figure 3).

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

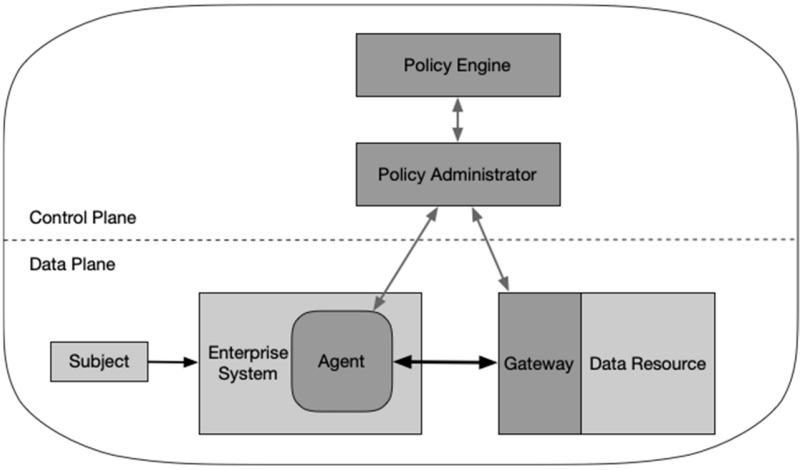


Figure 3 : modèle d'agent de périphérique/passerelle

Dans un scénario typique, un sujet disposant d'un ordinateur portable fourni par l'entreprise souhaite se connecter à une ressource d'entreprise (par exemple, une application/base de données de ressources humaines). La demande d'accès est prise en charge par l'agent local et transmise à l'administrateur de la stratégie. L'administrateur de stratégies et le moteur de stratégies peuvent être une ressource locale d'entreprise ou un service hébergé dans le cloud. L'administrateur de la stratégie transmet la demande au moteur de stratégie pour évaluation. Si la demande est autorisée, l'administrateur de stratégie configure un canal de communication entre l'agent de périphérique et la passerelle de ressources appropriée via le plan de contrôle. Il peut s'agir d'informations telles qu'une adresse de protocole Internet (IP), des informations de port, une clé de session ou des artefacts de sécurité similaires.
L'agent de périphérique et la passerelle se connectent ensuite, et les flux de données d'application/de service chiffrés commencent. La connexion entre l'agent de périphérique et la passerelle de ressources est interrompue lorsque le flux de travail est terminé ou lorsqu'elle est déclenchée par l'administrateur de stratégie en raison d'un événement de sécurité (par exemple, délai d'expiration de la session, échec de la réauthentification).

Ce modèle est mieux utilisé pour les entreprises qui disposent d'un programme de gestion des appareils robuste ainsi que de ressources discrètes pouvant communiquer avec la passerelle. Pour les entreprises qui utilisent fortement les services cloud, il s'agit d'une implémentation client-serveur du périmètre défini par logiciel (SDP) CSA-SDP (Cloud Security Alliance) de la Cloud Security Alliance (CSA). Ce modèle convient également aux entreprises qui ne souhaitent pas qu'une politique BYOD soit en place. L'accès n'est possible que via l'agent de périphérique, qui peut être placé sur les actifs appartenant à l'entreprise.

3.2.2 Déploiement basé sur Enclave

Ce modèle de déploiement est une variante du modèle d'agent de périphérique/passerelle ci-dessus. Dans ce modèle, les composants de passerelle ne peuvent pas résider sur des ressources ou devant des ressources individuelles, mais plutôt à la limite d'une enclave de ressources (par exemple, un centre de données sur site), comme illustré à la figure 4. En général, ces ressources servent à une seule fonction métier ou ne peuvent pas communiquer directement avec une passerelle (par exemple, un système de base de données hérité qui ne dispose pas d'une interface

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

de programmation d'application [API] pouvant être utilisée pour communiquer avec une passerelle). Ce modèle de déploiement peut également être utile pour les entreprises qui utilisent des micro-services basés sur le cloud pour un seul processus métier (par exemple, notification aux utilisateurs, recherche dans une base de données, versement des salaires). Dans ce modèle, l'ensemble du cloud privé est situé derrière une passerelle.

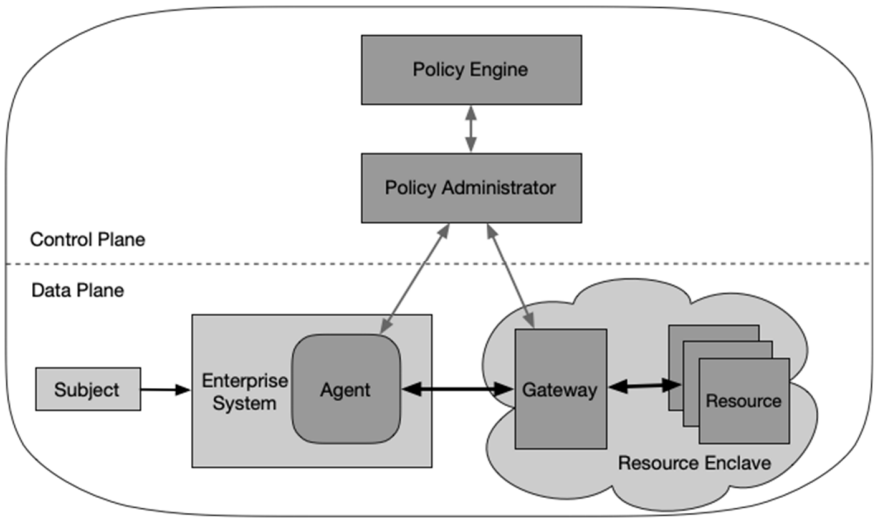


Figure 4 : modèle de passerelle Enclave

Il est possible que ce modèle soit hybride avec le modèle agent de périphérique/passerelle. Dans ce modèle, les ressources d'entreprise disposent d'un agent de périphérique utilisé pour se connecter aux passerelles Enclave, mais ces connexions sont créées à l'aide du même processus que le modèle de base de l'agent/passerelle de périphérique.

Ce modèle est utile pour les entreprises qui disposent d'applications héritées ou de centres de données locaux qui ne peuvent pas disposer de passerelles individuelles. L'entreprise a besoin d'un programme robuste de gestion des actifs et de la configuration pour installer/configurer les agents de périphérique. L'inconvénient est que la passerelle protège un ensemble de ressources et peut ne pas être en mesure de protéger chaque ressource individuellement. Cela peut également permettre aux sujets de voir des ressources auxquelles ils n'ont pas le privilège d'accéder.

3.2.3 Déploiement basé sur le portail de ressources

Dans ce modèle de déploiement, le PEP est un composant unique qui agit comme une passerelle pour les demandes du sujet. Le portail de passerelle peut être destiné à une ressource individuelle ou à une enclave sécurisée à un ensemble de ressources utilisées pour une seule fonction métier. Par exemple, un portail de passerelle vers un cloud privé ou un centre de données contenant des applications héritées, comme le montre la figure 5.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

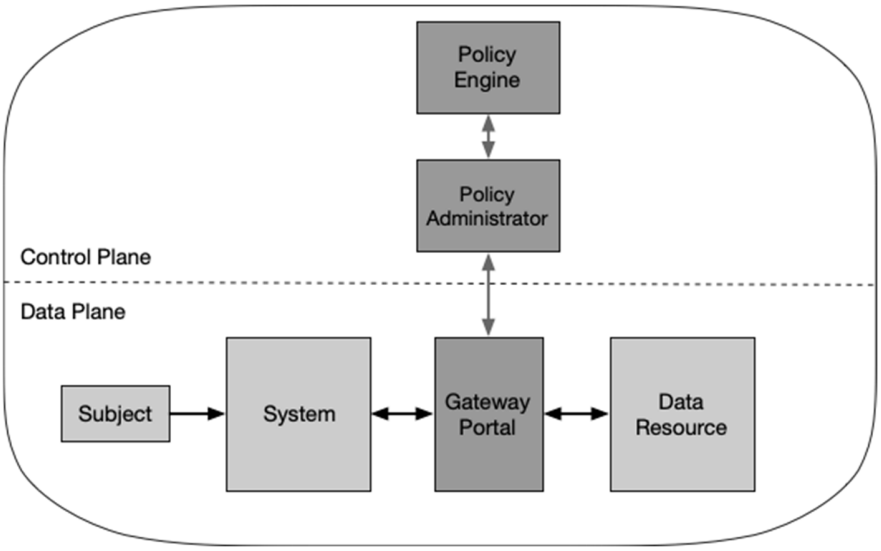


Figure 5 : Modèle de portail de ressources

Le principal avantage de ce modèle par rapport aux autres est qu'il n'est pas nécessaire d'installer un composant logiciel sur tous les appareils clients. Ce modèle est également plus souple pour les politiques BYOD et les projets de collaboration interorganisationnelle. Les administrateurs d'entreprise n'ont pas besoin de s'assurer que chaque appareil dispose de l'agent de périphérique approprié avant de l'utiliser. Cependant, des informations limitées peuvent être déduites des appareils demandant l'accès. Ce modèle ne peut analyser les ressources et les appareils qu'une fois qu'ils se connectent au portail PEP et peut ne pas être en mesure de les surveiller en permanence à la recherche de logiciels malveillants, de vulnérabilités non corrigées et d'une configuration appropriée.

La principale différence avec ce modèle est qu'il n'y a pas d'agent local qui gère les demandes, et l'entreprise peut donc ne pas avoir une visibilité totale ou un contrôle arbitraire sur les actifs, car elle ne peut les voir/analyser que lorsqu'elle se connecte à un portail. L'entreprise peut être en mesure d'utiliser des mesures telles que l'isolation du navigateur pour atténuer ou compenser. Ces ressources peuvent être invisibles pour l'entreprise entre ces sessions. Ce modèle permet également aux attaquants de découvrir et de tenter d'accéder au portail ou de tenter une attaque par déni de service (DoS) contre le portail. Les systèmes de portail doivent être bien provisionnés pour assurer la disponibilité en cas d'attaque DoS ou de perturbation du réseau.

3.2.4 Sandboxing de l'application de l'appareil

Une autre variante du modèle de déploiement agent/passerelle consiste à exécuter des applications ou des processus vérifiés de manière compartimentée sur les ressources. Il peut s'agir de machines virtuelles, de conteneurs ou d'une autre implémentation, mais l'objectif est le même : protéger l'application ou les instances d'applications contre un hôte potentiellement compromis ou d'autres applications s'exécutant sur l'actif.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

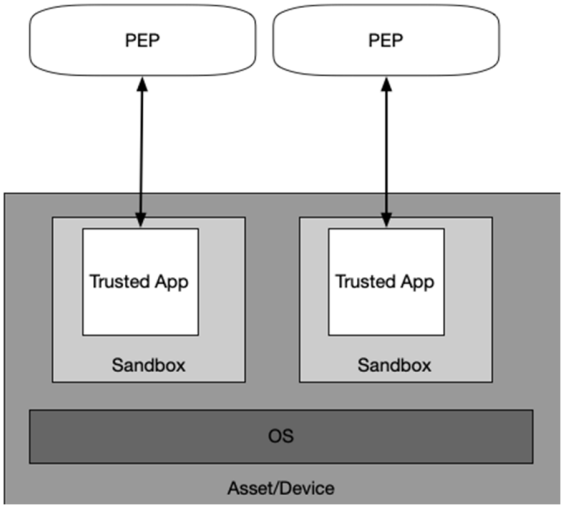


Figure 6 : Bacs à sable d'application

Dans la figure 6, l'appareil concerné exécute des applications approuvées et vérifiées dans un bac à sable. Les applications peuvent communiquer avec le PEP pour demander l'accès aux ressources, mais le PEP refusera les demandes d'autres applications sur l'actif. Dans ce modèle, le PEP peut être un service local d'entreprise ou un service cloud.

Le principal avantage de cette variante de modèle est que les applications individuelles sont segmentées par rapport au reste de l'actif. Si l'actif ne peut pas être analysé à la recherche de vulnérabilités, ces applications individuelles en bac à sable peuvent être protégées contre une infection potentielle par un logiciel malveillant sur l'actif hôte. L'un des inconvénients de ce modèle est que les entreprises doivent gérer ces applications en bac à sable pour toutes les ressources et peuvent ne pas avoir une visibilité totale sur les ressources des clients. L'entreprise doit également s'assurer que chaque application en bac à sable est sécurisée, ce qui peut nécessiter plus d'efforts que la simple surveillance des appareils.

3.3 Algorithme de confiance

Pour une entreprise avec un déploiement ZTA, le moteur de politiques peut être considéré comme le cerveau et l'algorithme de confiance du PE comme son processus de pensée principal. L'algorithme de confiance (TA) est le processus utilisé par le moteur de politique pour accorder ou refuser l'accès à une ressource. Le moteur de politiques prend des données provenant de plusieurs sources (voir la section 3) : la base de données de politiques avec des informations observables sur les sujets, les attributs et les rôles des sujets, les modèles de comportement historiques des sujets, les sources de renseignements sur les menaces et d'autres sources de métadonnées. Le processus peut être regroupé en grandes catégories et illustré à la figure 7.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

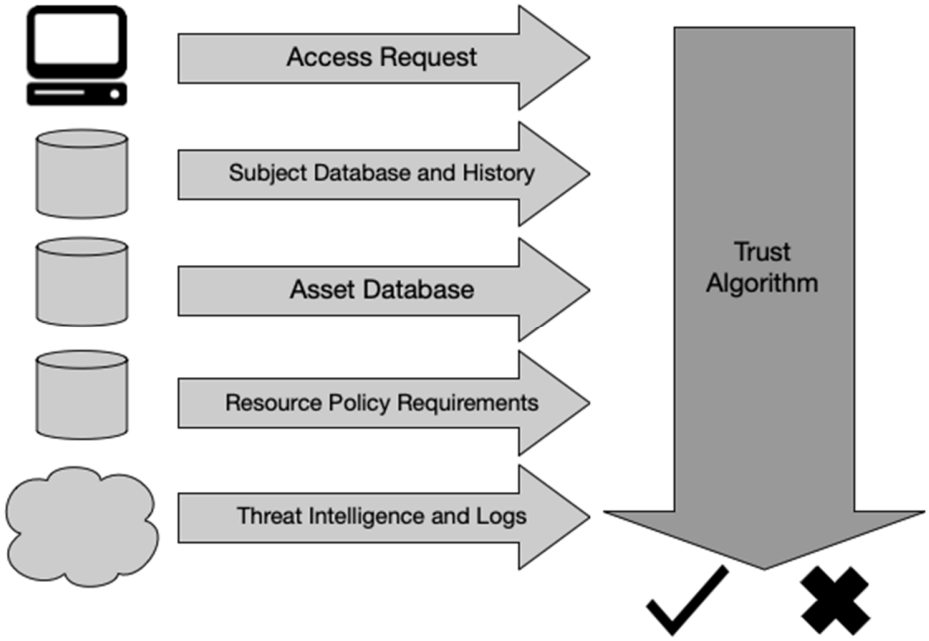


Figure 7 : Entrée de l'algorithme de confiance

Dans la figure, les entrées peuvent être divisées en catégories en fonction de ce qu'elles fournissent à l'algorithme de confiance.

- **Demande d'accès :** il s'agit de la demande réelle du sujet. La ressource demandée est l'information principale utilisée, mais des informations sur le demandeur sont également utilisées. Il peut s'agir de la version du système d'exploitation, du logiciel utilisé (par exemple, l'application demandée apparaît-elle sur une liste d'applications approuvées ?) et du niveau du correctif. En fonction de ces facteurs et de la sécurité des actifs, l'accès aux actifs peut être restreint ou refusé.
- **Base de données sujet :** Il s'agit du « qui » qui demande l'accès à une ressource [SP800-63]. Il s'agit de l'ensemble des sujets (humains et processus) de l'entreprise ou des collaborateurs et d'une collection d'attributs/privilèges de sujet attribués. Ces sujets et attributs constituent la base des politiques d'accès aux ressources [SP800-162] [NISTIR 7987]. Les identités des utilisateurs peuvent inclure une combinaison d'identité logique (par exemple, l'ID de compte) et les résultats des vérifications d'authentification effectuées par les PPE. Les attributs de l'identité qui peuvent être pris en compte dans le calcul du niveau de confiance comprennent le temps et la géolocalisation. Un ensemble de privilèges accordés à plusieurs sujets pourrait être considéré comme un rôle, mais les privilèges devraient être attribués à un sujet sur une base individuelle et non simplement parce qu'ils peuvent s'inscrire dans un rôle particulier dans l'organisation. Cette collection doit être codée et stockée dans un système de gestion des identifiants et une base de données de politiques. Cela peut également inclure des données sur le comportement observé par le passé chez certains variants (TA) (voir section 3.3.1).
- **Base de données d'actifs (et état observable) :** il s'agit de la base de données qui contient l'état connu de chaque actif appartenant à l'entreprise (et éventuellement connu hors entreprise/BYOD) (physique et virtuel, dans une certaine mesure). Celui-ci est

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

comparé à l'état observable de l'actif à l'origine de la demande et peut inclure la version du système d'exploitation, le logiciel présent et son intégrité, l'emplacement (emplacement réseau et géolocalisation) et le niveau du patch. Selon l'état de la ressource par rapport à cette base de données, l'accès aux ressources peut être restreint ou refusé.

- **Exigences en matière de ressources :** cet ensemble de stratégies complète la base de données d'ID utilisateur et d'attributs [SP800-63] et définit les exigences minimales pour l'accès à la ressource. Les exigences peuvent inclure des niveaux d'assurance de l'authentificateur, tels que l'emplacement réseau MFA (par exemple, refuser l'accès à partir d'adresses IP étrangères), la sensibilité des données et les demandes de configuration des actifs. Ces exigences doivent être élaborées à la fois par le dépositaire des données (c'est-à-dire les responsables des données) et ceux qui sont responsables des processus opérationnels qui utilisent les données (c'est-à-dire ceux qui sont responsables de la mission).
- **Threat Intelligence :** il s'agit d'un ou plusieurs flux d'informations sur les menaces générales et les logiciels malveillants actifs opérant sur Internet. Il peut également s'agir d'informations spécifiques sur les communications vues à partir de l'appareil qui peuvent être suspectes (telles que des requêtes pour d'éventuels nœuds de commande et de contrôle de logiciels malveillants). Ces flux peuvent être des services externes ou des analyses et découvertes internes, et peuvent inclure des signatures d'attaque et des mesures d'atténuation. C'est le seul composant qui sera très probablement sous le contrôle d'un service plutôt que de l'entreprise.

Le poids d'importance de chaque source de données peut provenir d'un algorithme propriétaire ou être configuré par l'entreprise. Ces valeurs de pondération peuvent être utilisées pour refléter l'importance de la source de données pour une entreprise.

La décision finale est ensuite transmise à l'AP pour exécution. Le travail de l'AP consiste à configurer les PEP nécessaires pour permettre la communication autorisée. Selon la façon dont le ZTA est déployé, cela peut impliquer l'envoi des résultats d'authentification et des informations de configuration de connexion aux passerelles et aux agents ou aux portails de ressources. Les AM peuvent également suspendre ou interrompre une session de communication pour réauthentifier et réautoriser la connexion conformément aux exigences de la politique. L'assistant personnel est également responsable de l'émission de la commande permettant de mettre fin à la connexion en fonction de la politique (par exemple, après un délai d'expiration, lorsque le flux de travail est terminé, en raison d'une alerte de sécurité).

3.3.1 Variations de l'algorithme de confiance

Il existe différentes façons de mettre en œuvre une AT. Différents responsables de la mise en œuvre peuvent souhaiter peser les facteurs ci-dessus différemment en fonction de l'importance perçue des facteurs. Il y a deux autres caractéristiques majeures qui peuvent être utilisées pour différencier les AT. La première est la façon dont les facteurs sont évalués, qu'il s'agisse de décisions binaires ou de parties pondérées d'un « score » ou d'un niveau de confiance complet. La seconde est la façon dont les demandes sont évaluées par rapport à d'autres demandes du même sujet, de la même application/service ou du même appareil.

- **Basé sur des critères ou sur un score :** un TA basé sur des critères suppose un

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

ensemble d'attributs qualifiés qui doivent être remplis avant que l'accès à une ressource ne soit accordé ou qu'une action (par exemple, lecture/écriture) soit autorisée. Ces critères sont configurés par l'entreprise et doivent être configurés indépendamment pour chaque ressource. L'accès n'est accordé ou une action appliquée à une ressource que si tous les critères sont remplis. Une TA basée sur un score calcule un niveau de confiance basé sur les valeurs de chaque source de données et les poids configurés par l'entreprise. Si le score est supérieur à la valeur de seuil configurée pour la ressource, l'accès est accordé ou l'action est effectuée.

Dans le cas contraire, la demande est refusée ou les privilèges d'accès sont réduits (par exemple, l'accès en lecture est accordé, mais pas l'accès en écriture pour un fichier).

- **Singulier ou contextuel :** Un assistant d'enseignement unique traite chaque demande individuellement et ne prend pas en compte l'histoire du sujet lors de son évaluation. Cela peut permettre des évaluations plus rapides, mais il existe un risque qu'une attaque ne soit pas détectée si elle reste dans le rôle autorisé d'un sujet. Un TA contextuel prend en compte l'historique récent du sujet ou de l'agent de réseau lors de l'évaluation des demandes d'accès. Cela signifie que le PE doit conserver des informations d'état sur tous les sujets et applications, mais qu'il peut être plus susceptible de détecter un attaquant utilisant des informations d'identification subverties pour accéder à des informations selon un modèle atypique de ce qu'il voit pour le sujet donné. Cela signifie également que le PE doit être informé du comportement des utilisateurs par l'AP (et les PEP) avec lesquels les sujets interagissent lorsqu'ils communiquent. L'analyse du comportement du sujet peut être utilisée pour fournir un modèle d'utilisation acceptable, et les écarts par rapport à ce comportement peuvent déclencher des vérifications d'authentification supplémentaires ou des refus de demandes de ressources.

Les deux facteurs ne sont pas toujours dépendants l'un de l'autre. Il est possible d'avoir un TA qui attribue un niveau de confiance à chaque sujet et/ou appareil et qui considère toujours chaque demande d'accès indépendamment (c'est-à-dire singulière). Cependant, les TA contextuelles et basées sur le score permettraient d'offrir un contrôle d'accès plus dynamique et granulaire, car le score fournit un niveau de confiance actuel pour le compte demandeur et s'adapte aux facteurs changeants plus rapidement que les politiques statiques modifiées par des administrateurs humains.

Idéalement, un algorithme de confiance ZTA doit être contextuel, mais cela n'est pas toujours possible avec les composants d'infrastructure disponibles pour l'entreprise. Une TA contextuelle peut atténuer les menaces lorsqu'un attaquant reste proche d'un ensemble « normal » de demandes d'accès pour un compte sujet compromis ou une attaque interne. Il est important d'équilibrer la sécurité, la facilité d'utilisation et la rentabilité lors de la définition et de la mise en œuvre d'algorithmes de confiance. Le fait d'inciter continuellement un sujet à se réauthentifier contre un comportement conforme aux tendances et aux normes historiques de sa mission, de sa fonction et de son rôle au sein de l'organisation peut entraîner des problèmes d'utilisabilité. Par exemple, si un employé du service RH d'une agence accède normalement à 20 à 30 enregistrements d'employés au cours d'une journée de travail typique, un TA contextuel peut envoyer une alerte si les demandes d'accès dépassent soudainement 100 enregistrements en une journée. Un TA contextuel peut également envoyer une alerte si quelqu'un fait des demandes d'accès en dehors des heures normales de bureau, car il peut s'agir d'un attaquant exfiltrant des enregistrements en utilisant un compte RH compromis. Il s'agit d'exemples où un TA contextuel peut détecter une attaque alors qu'un TA unique peut ne pas détecter le nouveau comportement.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

Dans un autre exemple, un comptable qui accède généralement au système financier pendant les heures normales de bureau essaie maintenant d'accéder au système au milieu de la nuit à partir d'un endroit méconnaissable. Une TA contextuelle peut déclencher une alerte et exiger que le sujet satisfasse à un niveau de confiance plus strict ou à d'autres critères, comme indiqué dans la publication spéciale 800-63A du NIST [SP800-63A].

L'élaboration d'un ensemble de critères ou de pondérations/valeurs seuils pour chaque ressource nécessite une planification et des tests. Les administrateurs d'entreprise peuvent rencontrer des problèmes lors de la mise en œuvre initiale de ZTA, où les demandes d'accès qui devraient être approuvées sont refusées en raison d'une mauvaise configuration. Cela se traduira par une première phase de « réglage » du déploiement. Il peut être nécessaire d'ajuster les critères ou les pondérations de notation pour s'assurer que les politiques sont appliquées tout en permettant aux processus métier de l'entreprise de fonctionner. La durée de cette phase de réglage dépend des métriques définies par l'entreprise pour l'avancement et la tolérance en cas de refus/approbations d'accès incorrect pour les ressources utilisées dans le flux de travail.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

3.4 Composants réseau/environnement

Dans un environnement ZT, il doit y avoir une séparation (logique ou éventuellement physique) des flux de communication utilisés pour contrôler et configurer le réseau et les flux de communication d'application/service utilisés pour effectuer le travail réel de l'organisation. Il est souvent décomposé en un *plan de contrôle* pour la communication de contrôle du réseau et un plan de *données* pour les flux de communication d'application/service [Gilman].

Le plan de contrôle est utilisé par divers composants d'infrastructure (appartenant à l'entreprise et provenant de fournisseurs de services) pour maintenir et configurer les actifs. juger, accorder ou refuser l'accès aux ressources ; et effectuer toutes les opérations nécessaires pour mettre en place des chemins de communication entre les ressources. Le plan de données est utilisé pour la communication réelle entre les composants logiciels. Ce canal de communication peut ne pas être possible avant que le chemin n'ait été établi via le plan de contrôle. Par exemple, le plan de contrôle peut être utilisé par l'AP et le PEP pour configurer le chemin de communication entre le sujet et la ressource d'entreprise. La charge de travail de l'application/du service utilise ensuite le chemin d'accès au plan de données qui a été établi.

3.4.1 Configuration réseau requise pour prendre en charge ZTA

1. **Les actifs d'entreprise disposent d'une connectivité réseau de base.** Le réseau local (LAN), contrôlé par l'entreprise ou non, fournit le routage et l'infrastructure de base (par exemple, DNS). L'actif d'entreprise distant n'utilise pas nécessairement tous les services d'infrastructure.

2. **L'entreprise doit être en mesure de faire la distinction entre les actifs qu'elle possède ou gère et la posture de sécurité actuelle des appareils.** Ceci est déterminé par les informations d'identification émises par l'entreprise et non par l'utilisation d'informations qui ne peuvent pas être authentifiées (par exemple, les adresses MAC du réseau qui peuvent être usurpées).

3. **L'entreprise peut observer l'ensemble du trafic réseau.** L'entreprise enregistre les paquets visibles sur le plan de données, même si elle n'est pas en mesure d'effectuer une inspection de la couche application (c'est-à-dire la couche OSI 7) sur tous les paquets.

L'entreprise filtre les métadonnées relatives à la connexion (par exemple, la destination, l'heure, l'identité de l'appareil) afin de mettre à jour dynamiquement les politiques et d'informer le PE lorsqu'il évalue les demandes d'accès.

4. **Les ressources d'entreprise ne doivent pas être accessibles sans l'accès à une PPE.** Les ressources d'entreprise n'acceptent pas les connexions entrantes arbitraires à partir d'Internet. Les ressources n'acceptent les connexions configurées personnalisées qu'une fois qu'un client a été authentifié et autorisé. Ces voies de communication sont mises en place par le PEP. Les ressources peuvent même ne pas être détectables sans accéder à une PPE. Cela empêche les attaquants d'identifier les cibles en scannant et/ou en lançant des attaques DoS contre les ressources situées derrière les PPE. Notez que toutes les ressources ne doivent pas être cachées de cette façon ; certains composants de l'infrastructure réseau (par exemple, les serveurs DNS) doivent être accessibles.

5. **Le plan de données et le plan de contrôle sont logiquement séparés.** Le moteur de stratégies, l'administrateur de stratégies et les points de terminaison privilégiés communiquent sur un réseau qui est logiquement séparé et qui n'est pas directement accessible par les ressources et les ressources de l'entreprise. Le plan de données est utilisé pour Trafic de données d'application/service. Le moteur de stratégies, l'administrateur de stratégies et les points de terminaison privilégiés utilisent le plan de contrôle pour communiquer et gérer les chemins de communication entre les ressources. Les PEP doivent être en mesure d'envoyer et de recevoir des messages à partir des plans de données et de contrôle.

6. **Les actifs d'entreprise peuvent atteindre le composant PEP.** Les sujets d'entreprise doivent être en mesure d'accéder au composant PEP pour accéder aux ressources. Il peut s'agir d'un portail Web, d'un périphérique réseau ou d'un agent logiciel sur l'actif d'entreprise qui permet la connexion.

7. **Le PEP est le seul composant qui accède à l'administrateur de stratégie dans le cadre d'un flux d'entreprise.** Chaque PPE fonctionnant sur le réseau d'entreprise dispose d'une connexion à l'administrateur de stratégie pour établir les chemins de communication entre les clients et les ressources. Tout le trafic des processus d'entreprise passe par une ou plusieurs PPE.

8. **Les ressources d'entreprise distantes doivent pouvoir accéder aux ressources de l'entreprise sans avoir à traverser l'infrastructure réseau de l'entreprise.** Par exemple, un sujet distant ne doit pas être obligé d'utiliser un lien vers le réseau d'entreprise (c'est-à-dire un réseau privé virtuel [VPN]) pour accéder à des services utilisés par l'entreprise et hébergés par un fournisseur de cloud public (par exemple, un courrier électronique).

9. **L'infrastructure utilisée pour soutenir le processus de décision d'accès ZTA devrait être évolutive pour tenir compte des changements dans la charge du processus.** Les PE, PA et PEP utilisés dans un ZTA deviennent les composants clés de tout processus commercial. Le retard ou l'incapacité à joindre une PPE (ou l'incapacité des PPE à joindre l'AP/EP) a un impact négatif sur la capacité à exécuter le flux de travail. Une entreprise qui met en œuvre un ZTA doit provisionner les composants pour la charge de travail attendue ou être en mesure de faire évoluer rapidement l'infrastructure pour gérer une utilisation accrue en cas de besoin.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

10. **Les actifs de l'entreprise peuvent ne pas être en mesure d'atteindre certaines PPE en raison de politiques ou de facteurs observables.** Par exemple, il peut exister une politique indiquant que les actifs mobiles peuvent ne pas être en mesure d'atteindre certaines ressources si l'actif demandeur est situé en dehors du pays d'origine de l'entreprise. Ces facteurs peuvent être basés sur l'emplacement (géolocalisation ou emplacement réseau), le type d'appareil ou d'autres critères.

4 Scénarios de déploiement/cas d'utilisation

Tout environnement d'entreprise peut être conçu en tenant compte des principes Zero Trust. La plupart des organisations ont déjà certains éléments de Zero Trust dans leur infrastructure d'entreprise ou sont en train de mettre en œuvre des politiques et des bonnes pratiques en matière de sécurité de l'information et de résilience.
Plusieurs scénarios de déploiement et cas d'utilisation se prêtent facilement à une architecture Zero Trust. Par exemple, ZTA a ses racines dans des organisations géographiquement dispersées et/ou ayant une main-d'œuvre très mobile. Cela dit, toute organisation peut bénéficier d'une architecture Zero Trust.

Dans les cas d'utilisation ci-dessous, ZTA n'est pas explicitement indiqué, car l'entreprise dispose probablement d'infrastructures basées sur le périmètre et éventuellement d'infrastructures ZTA. Comme nous l'avons vu à la section 7.2, il y aura probablement une période pendant laquelle les composants ZTA et l'infrastructure de réseau basée sur le périmètre seront en fonctionnement simultané dans une entreprise.

4.1 Entreprise avec installations satellites

Le scénario le plus courant implique une entreprise avec un seul siège social et un ou plusieurs emplacements géographiquement dispersés qui ne sont pas reliés par une connexion réseau physique appartenant à l'entreprise (voir la figure 8). Les employés sur le site distant peuvent ne pas disposer d'un réseau local appartenant à l'ensemble de l'entreprise, mais doivent tout de même accéder aux ressources de l'entreprise pour effectuer leurs tâches. L'entreprise peut disposer d'une liaison MPLS (Multiprotocol Label Switch) vers le réseau du siège de l'entreprise, mais ne dispose pas d'une bande passante adéquate pour l'ensemble du trafic ou ne souhaite pas que le trafic destiné aux applications/services basés sur le cloud passe par le réseau du siège de l'entreprise. De même, les employés peuvent être en télétravail ou dans un endroit éloigné et utiliser des appareils appartenant à l'entreprise ou à leur personnel. Dans de tels cas, une entreprise peut souhaiter accorder l'accès à certaines ressources (par exemple, l'agenda des employés, les e-mails), mais refuser l'accès ou restreindre les actions aux ressources plus sensibles (par exemple, la base de données RH).

Dans ce cas d'utilisation, le ou les PE/PA sont souvent hébergés en tant que service cloud (ce qui offre généralement une disponibilité supérieure et n'oblige pas les travailleurs à distance à s'appuyer sur l'infrastructure de l'entreprise pour accéder aux ressources cloud) avec des actifs finaux disposant d'un agent installé (voir la section 3.2.1) ou accédant à un portail de ressources (voir la section 3.2.3). Il n'est peut-être pas plus réactif d'héberger le ou les PE/PA sur le réseau local de l'entreprise, car les bureaux distants et les travailleurs doivent renvoyer tout le trafic vers le réseau de l'entreprise pour atteindre les applications/services hébergés par les services cloud.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

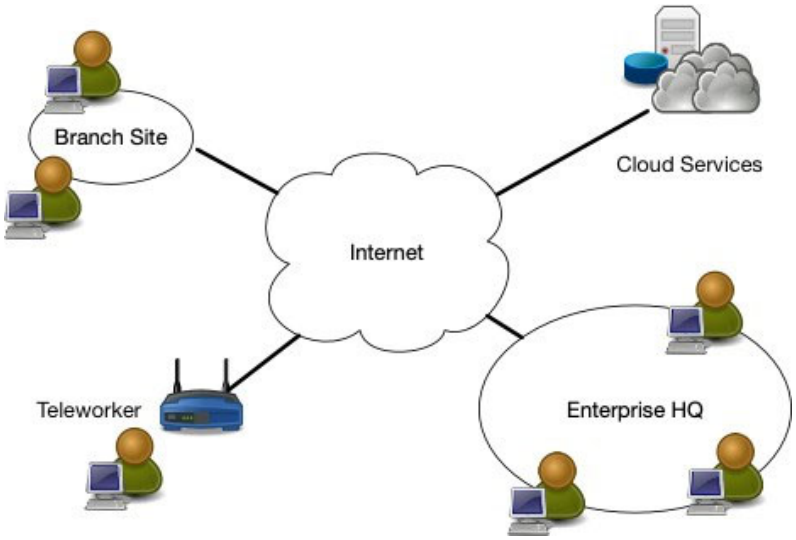


Figure 8 : Entreprise avec des employés à distance

4.2 Multi-cloud/Cloud-to-Cloud Enterprise

Un cas d'utilisation de plus en plus courant pour le déploiement d'un ZTA est celui d'une entreprise utilisant plusieurs fournisseurs de cloud (voir figure 9). Dans ce cas d'utilisation, l'entreprise dispose d'un réseau local, mais utilise au moins deux fournisseurs de services cloud pour héberger des applications/services et des données. Parfois, l'application/le service est hébergé sur un service cloud distinct de la source de données. Pour des raisons de performances et de facilité de gestion, l'application hébergée dans le fournisseur de cloud A doit pouvoir se connecter directement à la source de données hébergée dans le fournisseur de cloud B plutôt que de forcer l'application à revenir via le réseau d'entreprise.

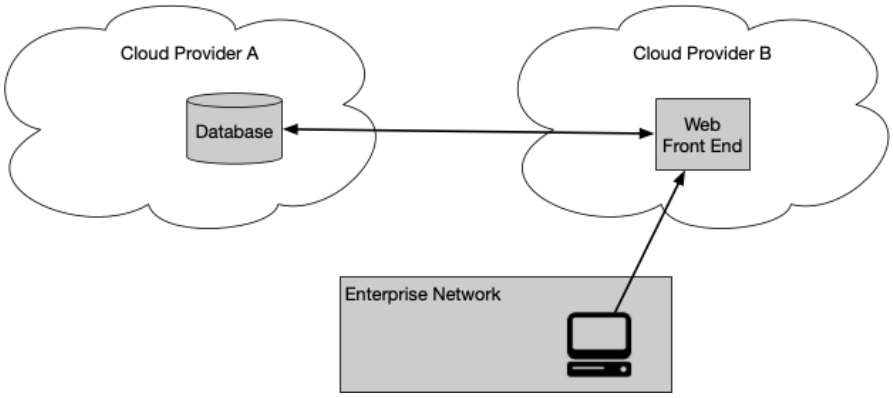


Figure 9 : Cas d'utilisation multicloud

Ce cas d'utilisation est la mise en œuvre serveur-serveur de la spécification de périmètre défini par logiciel (SDP) DE LA CSA [CSA-SDP]. À mesure que les entreprises adoptent des applications et des services hébergés dans le cloud, il devient évident que s'appuyer sur le périmètre de l'entreprise pour la sécurité devient un handicap. Comme nous l'avons vu à la section 2.2, les principes de ZT sont d'avis qu'il ne devrait pas y avoir de différence entre une infrastructure de réseau détenue et exploitée par une entreprise et une infrastructure détenue et

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

exploitée par un autre fournisseur de services. L'approche Zero Trust de l'utilisation du multicloud consiste à placer les PPE aux points d'accès de chaque application/service et source de données. Le PE et le PA peuvent être des services situés dans le cloud ou même chez un troisième fournisseur de cloud. Le client (via un portail ou un agent local installé) accède ensuite directement aux PEP. De cette façon, l'entreprise peut toujours gérer l'accès aux ressources, même lorsqu'elles sont hébergées en dehors de l'entreprise. L'un des défis est que les différents fournisseurs de cloud ont des méthodes uniques pour mettre en œuvre des fonctionnalités similaires. Les architectes d'entreprise devront savoir comment mettre en œuvre leur ZTA d'entreprise avec chaque fournisseur de cloud qu'ils utilisent.

4.3 Entreprise avec services contractuels et/ou accès non employé

Un autre scénario courant est celui d'une entreprise qui comprend des visiteurs sur site et/ou des fournisseurs de services contractuels qui ont besoin d'un accès limité aux ressources de l'entreprise pour effectuer leur travail (voir la figure 10). Par exemple, une entreprise dispose de ses propres applications/services, bases de données et actifs internes. Il s'agit notamment de services sous-traités à des fournisseurs qui peuvent être sur place à l'occasion pour assurer l'entretien (p. ex., des systèmes de chauffage et d'éclairage intelligents qui appartiennent à des fournisseurs externes et qui sont gérés par eux). Ces visiteurs et fournisseurs de services auront besoin d'une connectivité réseau pour effectuer leurs tâches. Une entreprise Zero Trust pourrait faciliter cela en permettant à ces appareils et à tout technicien de service en visite d'accéder à Internet tout en masquant les ressources de l'entreprise.

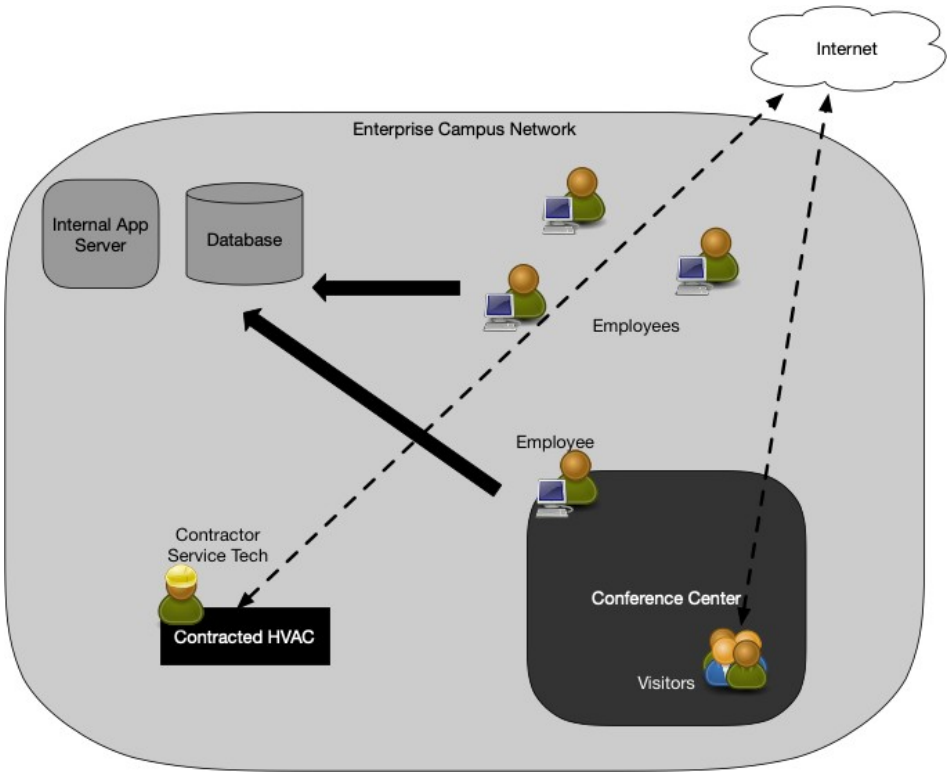


Figure 10 : Entreprise avec accès pour les non-employés

Dans cet exemple, l'organisation dispose également d'un centre de conférence où les visiteurs interagissent avec les employés. Encore une fois, avec une approche ZTA des SDP, les appareils

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

et les sujets des employés sont différenciés et peuvent être en mesure d'accéder aux ressources appropriées de l'entreprise. Les visiteurs du campus peuvent avoir accès à Internet, mais ne peuvent pas accéder aux ressources de l'entreprise. Ils ne sont peut-être même pas en mesure de le faire. Découvrir les services d'entreprise via des analyses de réseau (c'est-à-dire empêcher la reconnaissance active du réseau/les mouvements est-ouest).

Dans ce cas d'utilisation, le ou les PE et PA peuvent être hébergés en tant que service cloud ou sur le LAN (en supposant peu ou pas d'utilisation des services hébergés dans le cloud). Les actifs de l'entreprise peuvent avoir un agent installé (voir la section 3.2.1) ou accéder aux ressources via un portail (voir la section 3.2.3). Le ou les PA garantissent que toutes les ressources non liées à l'entreprise (celles qui n'ont pas d'agents installés ou qui ne peuvent pas se connecter à un portail) ne peuvent pas accéder aux ressources locales, mais peuvent accéder à Internet.

4.4 Collaboration au-delà des frontières de l'entreprise

Un quatrième cas d'utilisation est la collaboration inter-entreprises. Par exemple, il s'agit d'un projet impliquant des employés de l'entreprise A et de l'entreprise B (voir figure 11). Les deux entreprises peuvent être des agences fédérales distinctes (G2G) ou même une agence fédérale et une entreprise privée (G2B).
L'entreprise A exploite la base de données utilisée pour le projet mais doit autoriser l'accès aux données à certains membres de l'entreprise B. L'entreprise A peut configurer des comptes spécialisés pour que les employés de l'entreprise B puissent accéder aux données requises et refuser l'accès à toutes les autres ressources, mais cela peut rapidement devenir difficile à gérer. Le fait que les deux organisations soient inscrites dans un système de gestion Federated ID permettrait d'établir plus rapidement ces relations, à condition que les PPE des deux organisations puissent authentifier les sujets dans une communauté Federated ID.

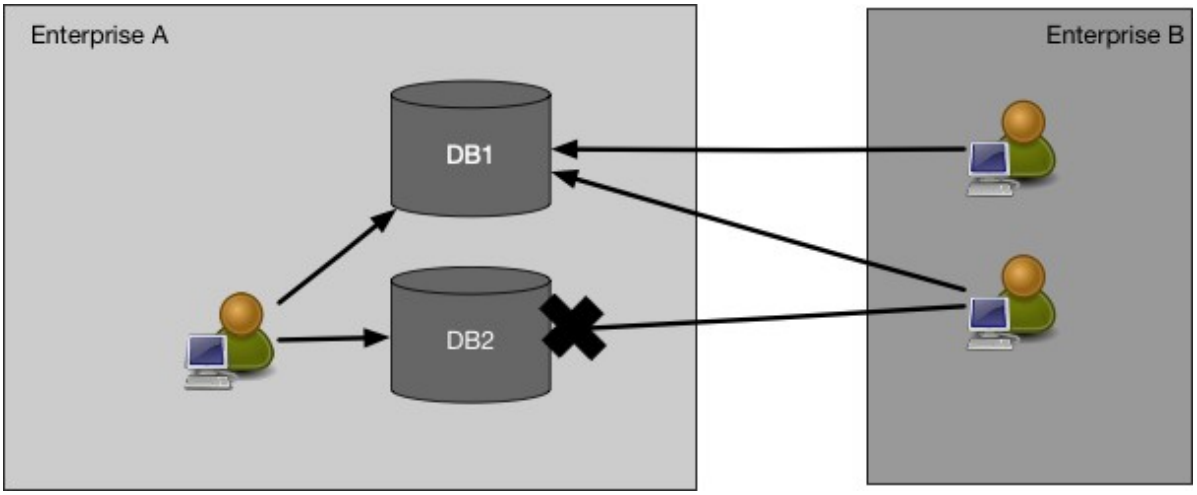


Figure 11 : Collaboration inter-entreprise

Ce scénario peut être similaire au cas d'utilisation 1 (Section 4.1), car les employés des deux entreprises peuvent ne pas se trouver sur les infrastructures réseau de leurs organisations et les ressources auxquelles ils doivent accéder peuvent se trouver dans un environnement d'entreprise ou être hébergées dans le cloud. Cela signifie qu'il n'est pas nécessaire d'avoir des règles de pare-feu complexes ou des listes de contrôle d'accès (ACL) à l'échelle de l'entreprise permettant à certaines adresses IP appartenant à l'entreprise B d'accéder aux ressources de l'entreprise A en fonction des politiques d'accès de l'entreprise A. La façon dont cet accès est réalisé dépend de la

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

technologie utilisée. À l'instar du cas d'utilisation 1, un PE et un PA hébergés en tant que service cloud peuvent fournir une disponibilité à toutes les parties sans avoir à établir un VPN ou similaire. Les employés de l'entreprise B peuvent être invités à installer un agent logiciel sur leur actif ou à accéder aux ressources de données nécessaires par le biais d'une passerelle web (voir section 3.2.3).

4.5 Entreprise avec services publics ou clients

Une caractéristique commune à de nombreuses entreprises est un service public qui peut inclure ou non l'enregistrement des utilisateurs (c'est-à-dire que les utilisateurs doivent créer ou avoir reçu un ensemble d'identifiants de connexion). Il peut s'agir d'un grand public, d'un ensemble de clients ayant une relation d'affaires existante ou d'un ensemble spécial d'utilisateurs non professionnels, tels que les personnes à charge des employés. Dans tous les cas, il est probable que les actifs demandeurs ne soient pas la propriété de l'entreprise et que l'entreprise soit limitée quant aux politiques internes de cybersécurité qui peuvent être appliquées.

Pour une ressource générale destinée au public qui ne nécessite pas d'identifiants de connexion pour y accéder (par exemple, une page Web publique), les principes de ZTA ne s'appliquent pas directement. L'entreprise ne peut pas contrôler strictement l'état des ressources demandes, et les ressources publiques anonymes (par exemple, une page Web publique) n'ont pas besoin d'informations d'identification pour être accessibles.

Les entreprises peuvent établir des politiques pour les utilisateurs publics enregistrés, tels que les clients (c'est-à-dire ceux qui ont une relation d'affaires) et les utilisateurs spéciaux (par exemple, les personnes à charge des employés). Si les utilisateurs sont tenus de produire ou d'obtenir des informations d'identification, l'entreprise peut mettre en place des politiques concernant la longueur du mot de passe, le cycle de vie et d'autres détails, et peut fournir l'authentification multifacteur en tant qu'option ou exigence. Cependant, les entreprises sont limitées dans les politiques qu'elles peuvent mettre en œuvre pour cette classe d'utilisateurs. Des informations sur les demandes entrantes peuvent être utiles pour déterminer l'état de la fonction publique et détecter d'éventuelles attaques se faisant passer pour des utilisateurs légitimes. Par exemple, on sait qu'un portail d'utilisateur enregistré est accessible par les clients enregistrés à l'aide de l'un des navigateurs Web courants. Une augmentation soudaine des demandes d'accès provenant de types de navigateurs inconnus ou de versions obsolètes connues pourrait indiquer une attaque automatisée d'une sorte ou d'une autre, et l'entreprise pourrait prendre des mesures pour limiter les demandes provenant de ces clients identifiés. L'entreprise doit également être au courant de toute loi ou réglementation concernant les informations qui peuvent être collectées et enregistrées sur les utilisateurs et les actifs demandeurs.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

5 Menaces associées à l'architecture Zero Trust

Aucune entreprise ne peut éliminer les risques de cybersécurité. Lorsqu'il est complété par les politiques et les conseils de cybersécurité existants, la gestion des identités et des accès, la surveillance continue et la cyberhygiène générale, une ZTA correctement mise en œuvre et maintenue peut réduire les risques globaux et protéger contre les menaces courantes. Cependant, certaines menaces ont des caractéristiques uniques lors de la mise en œuvre d'un ZTA.

5.1 Subversion du processus décisionnel de la ZTA

Dans ZTA, le moteur de règles et l'administrateur de stratégies sont les composants clés de l'ensemble de l'entreprise. Aucune communication entre les ressources de l'entreprise n'a lieu à moins qu'elle ne soit approuvée et éventuellement configurée par le PE et le PA. Cela signifie que ces composants doivent être correctement configurés et entretenus. Tout administrateur d'entreprise disposant d'un accès de configuration aux règles du PE peut être en mesure d'effectuer des modifications non approuvées ou de commettre des erreurs susceptibles d'interrompre les opérations de l'entreprise. De même, un système de sonorisation compromis pourrait permettre l'accès à des ressources qui ne seraient pas approuvées autrement (par exemple, à un appareil subverti appartenant à un particulier). Pour atténuer les risques associés, les composants PE et PA doivent être correctement configurés et surveillés, et toute modification de configuration doit être consignée et soumise à un audit.

5.2 Déni de service ou perturbation du réseau

Dans ZTA, l'AP est le composant clé pour l'accès aux ressources. Les ressources d'entreprise ne peuvent pas se connecter les unes aux autres sans l'autorisation de l'assistant personnel et, éventuellement, une action de configuration. Si un attaquant perturbe ou refuse l'accès à la ou aux PEP ou PE/PA (c'est-à-dire une attaque DoS ou un détournement de route), cela peut avoir un impact négatif sur les opérations de l'entreprise. Les entreprises peuvent atténuer cette menace en faisant en sorte que l'application de la politique réside dans un environnement cloud correctement sécurisé ou qu'elle soit répliquée dans plusieurs endroits en suivant les conseils sur la cyber-résilience [SP 800-160v2].

Cela atténue le risque, mais ne l'élimine pas. Les botnets tels que Mirai produisent des attaques DoS massives contre les principaux fournisseurs de services Internet et perturbent le service pour des millions d'internautes.[5] Il est également possible qu'un attaquant intercepte et bloque le trafic vers une PPE ou une AP à partir d'une partie ou de la totalité des comptes d'utilisateurs d'une entreprise (par exemple, une succursale ou même un seul employé à distance). Dans ce cas, seule une partie des sujets de l'entreprise est touchée. Cela est également possible dans les anciens VPN d'accès à distance et n'est pas propre à ZTA.

Un fournisseur d'hébergement peut également mettre accidentellement hors ligne un EP ou un PA basé sur le cloud. Les services cloud ont connu des perturbations par le passé, qu'il s'agisse d'infrastructure en tant que service (IaaS)[6] ou de SaaS.[7] Une erreur de fonctionnement peut empêcher l'ensemble d'une entreprise de fonctionner si le moteur de stratégies ou le composant administrateur de stratégies devient inaccessible à partir du réseau.

[5] https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/
[6] https://aws.amazon.com/message/41926/
[7] https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=12286870

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

Il existe également un risque que les ressources de l'entreprise ne soient pas accessibles à partir de l'AP, de sorte que même si l'accès est accordé à un sujet, l'AP ne peut pas configurer le chemin de communication à partir du réseau. Cela peut se produire en raison d'une attaque DDoS ou simplement en raison d'une utilisation intensive inattendue. Ceci est similaire à toute autre interruption du réseau dans la mesure où certains ou tous les sujets de l'entreprise ne peuvent pas accéder à une ressource particulière parce que cette ressource n'est pas disponible pour une raison quelconque.

5.3 Identifiants volés/menaces internes

La mise en œuvre correcte de ZT, de politiques de sécurité de l'information et de résilience, ainsi que les meilleures pratiques réduisent le risque qu'un attaquant obtienne un large accès via des identifiants volés ou des attaques internes. Le principe ZT de l'absence de confiance implicite basée sur l'emplacement du réseau signifie que les attaquants doivent compromettre un compte ou un appareil existant pour prendre pied dans une entreprise. Un ZTA correctement développé et mis en œuvre devrait empêcher un compte ou un actif compromis d'accéder à des ressources en dehors de son champ d'application normal ou de ses modèles d'accès. Cela signifie que les comptes disposant de politiques d'accès autour des ressources qui intéressent un attaquant seraient les principales cibles des attaquants.

Les attaquants peuvent utiliser le phishing, l'ingénierie sociale ou une combinaison d'attaques pour obtenir les informations d'identification de comptes de valeur. « Précieux » peut signifier différentes choses en fonction de la motivation de l'attaquant. Par exemple, les comptes d'administrateur d'entreprise peuvent être précieux, mais les attaquants intéressés par un gain financier peuvent envisager des comptes qui ont accès à des ressources financières ou de paiement de valeur égale. La mise en œuvre de l'authentification multifacteur pour les demandes d'accès peut réduire le risque de perte d'informations provenant d'un compte compromis. Toutefois, un attaquant disposant d'informations d'identification valides (ou un initié malveillant) peut toujours être en mesure d'accéder aux ressources pour lesquelles le compte a été autorisé à accéder. Par exemple, un attaquant ou un employé compromis qui possède les informations d'identification et les actifs appartenant à l'entreprise d'un employé des ressources humaines valide peut toujours être en mesure d'accéder à une base de données d'employés.

ZTA réduit les risques et empêche les comptes ou actifs compromis de se déplacer latéralement sur le réseau. Si les informations d'identification compromises ne sont pas autorisées à accéder à une ressource particulière, l'accès à cette ressource leur sera toujours refusé. De plus, un algorithme de confiance contextuelle (voir la section 3.3.1) est plus susceptible de détecter cette attaque et d'y répondre rapidement que lorsqu'elle se produit dans un réseau hérité basé sur le périmètre. L'AT contextuel peut détecter les modèles d'accès qui ne se comportent pas normalement et refuser l'accès aux ressources sensibles du compte compromis ou de la menace interne.

5.4 Visibilité sur le réseau

Comme nous l'avons mentionné à la section 3.4.1, tout le trafic est inspecté et enregistré sur le réseau, puis analysé afin d'identifier et de réagir aux attaques potentielles contre l'entreprise. Cependant, comme nous l'avons également mentionné, une partie (peut-être la majorité) du trafic sur le réseau d'entreprise peut être opaque aux outils d'analyse de réseau de couche 3. Ce trafic

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

peut provenir d'actifs n'appartenant pas à l'entreprise (par exemple, des services contractuels qui utilisent l'infrastructure de l'entreprise pour accéder à Internet) ou d'applications/services qui résistent à la surveillance passive. L'entreprise qui ne peut pas effectuer d'inspection approfondie des paquets ou examiner le trafic chiffré et qui doit utiliser d'autres méthodes pour évaluer un éventuel attaquant sur le réseau.

Cela ne signifie pas que l'entreprise n'est pas en mesure d'analyser le trafic chiffré qu'elle voit sur le réseau. L'entreprise peut collecter des métadonnées (par exemple, les adresses source et de destination, etc.) sur le trafic crypté et l'utiliser pour détecter un attaquant actif ou un éventuel logiciel malveillant communiquant sur le réseau. Les techniques d'apprentissage automatique [Anderson] peuvent être utilisées pour analyser le trafic qui ne peut pas être déchiffré et examiné. L'utilisation de ce type d'apprentissage automatique permettrait à l'entreprise de classer le trafic comme valide ou potentiellement malveillant et susceptible d'être corrigé.

5.5 Stockage des informations système et réseau

Une menace connexe pour la surveillance et l'analyse du trafic réseau est le composant d'analyse lui-même. Si les analyses de moniteur, le trafic réseau et les métadonnées sont stockés à des fins d'élaboration de politiques contextuelles, d'analyse judiciaire ou d'analyse ultérieure, ces données deviennent une cible pour les attaquants. Tout comme les diagrammes de réseau, les fichiers de configuration et d'autres documents d'architecture de réseau assortis, ces ressources doivent être protégées. Si un attaquant parvient à accéder à ces informations, il peut être en mesure d'obtenir des informations sur l'architecture de l'entreprise et d'identifier les actifs pour une reconnaissance et une attaque plus approfondies.

Une autre source d'informations de reconnaissance pour un attaquant dans une entreprise ZT est l'outil de gestion utilisé pour coder les politiques d'accès. À l'instar du trafic stocké, ce composant contient des politiques d'accès aux ressources et peut fournir à un attaquant des informations sur les comptes les plus précieux à compromettre (par exemple, ceux qui ont accès aux ressources de données souhaitées).

Comme pour toutes les données d'entreprise précieuses, des protections adéquates doivent être mises en place pour empêcher les accès non autorisés et les tentatives d'accès. Comme ces ressources sont vitales pour la sécurité, elles doivent avoir les politiques d'accès les plus restrictives et être accessibles uniquement à partir de comptes d'administrateur désignés ou dédiés.

5.6 Recours à des formats de données ou à des solutions propriétaires

ZTA s'appuie sur plusieurs sources de données différentes pour prendre des décisions d'accès, notamment des informations sur le sujet demandeur, les actifs utilisés, les renseignements d'entreprise et externes et l'analyse des menaces. Souvent, les ressources utilisées pour stocker et traiter ces informations ne disposent pas d'une norme commune et ouverte sur la façon d'interagir et d'échanger des informations. Cela peut conduire à des cas où une entreprise est enfermée dans un sous-ensemble de fournisseurs en raison de problèmes d'interopérabilité. Si un fournisseur rencontre un problème de sécurité ou une perturbation, une entreprise peut ne pas être en mesure de migrer vers un nouveau fournisseur sans un coût extrême (par exemple, le remplacement de plusieurs actifs) ou sans passer par un long programme de transition (par exemple, traduire les règles de politique d'un format propriétaire à un autre). À l'instar des attaques DoS, ce risque n'est pas propre à ZTA, mais comme ZTA dépend fortement de l'accès dynamique aux

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

informations (à la fois de l'entreprise et des fournisseurs de services), les perturbations peuvent affecter les fonctions commerciales essentielles d'une entreprise. Pour atténuer les risques associés, les entreprises doivent évaluer les fournisseurs de services sur une base holistique en tenant compte de facteurs tels que les contrôles de sécurité des fournisseurs, les coûts de changement d'entreprise et la gestion des risques de la chaîne d'approvisionnement, en plus de facteurs plus typiques tels que les performances, la stabilité, etc.

5.7 Utilisation d'entités non physiques (NPE) dans l'administration de la ZTA

L'intelligence artificielle et d'autres agents logiciels sont déployés pour gérer les problèmes de sécurité sur les réseaux d'entreprise. Ces composants doivent interagir avec les composants de gestion de ZTA (par exemple, moteur de stratégies, administrateur de stratégies), parfois à la place d'un administrateur humain. Comment ces composants s'authentifient dans une entreprise mettant en œuvre un ZTA est une question ouverte. On suppose que la plupart des systèmes technologiques automatisés utilisent des moyens d'authentification lors de l'utilisation d'une API pour fournir des composants de ressources.

Le plus grand risque lors de l'utilisation d'une technologie automatisée pour la configuration et l'application des politiques est la possibilité que des faux positifs (actions inoffensives confondues avec des attaques) et des faux négatifs (attaques confondues avec une activité normale) aient un impact sur la posture de sécurité de l'entreprise. Cela peut être réduit grâce à une analyse de réajustement régulière pour corriger les décisions erronées et améliorer le processus de décision.

Le risque associé est qu'un attaquant soit en mesure d'induire ou de contraindre un NPE à effectuer une tâche qu'il n'a pas le privilège d'accomplir. L'agent logiciel peut avoir une barre d'authentification inférieure (par exemple, clé API ou MFA) pour effectuer des tâches administratives ou liées à la sécurité par rapport à un utilisateur humain. Si un attaquant peut interagir avec l'agent, il pourrait théoriquement inciter l'agent à accorder à l'attaquant un meilleur accès ou à effectuer une tâche pour le compte de l'attaquant. Il existe également un risque qu'un attaquant accède aux informations d'identification d'un agent logiciel et se fasse passer pour l'agent lors de l'exécution de tâches.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

6 Architecture Zero Trust et interactions possibles avec les directives fédérales existantes

Plusieurs politiques et orientations fédérales existantes recoupent la planification, le déploiement et l'exploitation d'une ZTA. Ces politiques n'empêchent pas une entreprise de passer à une architecture plus orientée Zero Trust, mais peuvent influencer le développement d'une stratégie Zero Trust pour une agence. Lorsqu'il est complété par les politiques et les directives de cybersécurité existantes, l'ICAM, la surveillance continue et la cyberhygiène générale, le ZTA peut renforcer la posture de sécurité d'une organisation et la protéger contre les menaces courantes.

6.1 Cadre de gestion des risques ZTA et NIST

Le déploiement d'une ZTA implique l'élaboration de politiques d'accès autour des risques acceptables pour la mission ou le processus opérationnel désigné (voir la section 7.3.3). Il est possible de refuser tout accès réseau à une ressource et de n'autoriser l'accès que via un terminal connecté, mais cela est disproportionné dans la majorité des cas et pourrait empêcher l'accomplissement du travail. Pour qu'un organisme fédéral puisse remplir sa mission, il y a un niveau de risque acceptable. Les risques associés à l'exécution de la mission doivent être identifiés et évalués, et acceptés ou atténués. Pour y parvenir, le cadre de gestion des risques (RMF) du NIST a été élaboré [SP800-37].

La planification et la mise en œuvre de ZTA peuvent modifier les limites d'autorisation définies par l'entreprise. Cela est dû à l'ajout de nouveaux composants (par exemple, le moteur de stratégies, l'administrateur de stratégies et les PPE) et à la réduction de la dépendance à l'égard des défenses de périmètre du réseau. Le processus global décrit dans le RMF ne changera pas dans un ZTA.

6.2 Cadre de confidentialité Zero Trust et NIST

La protection de la vie privée des utilisateurs et des renseignements personnels (p. ex., les renseignements personnels) est une préoccupation majeure pour les organisations. La protection de la vie privée et des données est incluse dans les programmes de conformité tels que FISMA et la loi HIPAA (Heath Insurance Portability and Accountability Act). En réponse, le NIST a produit un cadre de protection de la vie privée à l'intention des organisations [NISTPRIV]. Ce document fournit un cadre pour décrire les risques d'atteinte à la vie privée et les stratégies d'atténuation, ainsi qu'un processus permettant à une entreprise de cerner, de mesurer et d'atténuer les risques pour la vie privée des utilisateurs et les renseignements personnels stockés et traités par une organisation. Cela comprend les renseignements personnels utilisés par l'entreprise pour soutenir les opérations ZTA et tous les attributs biométriques utilisés dans les évaluations des demandes d'accès.

Une partie des exigences fondamentales de ZT est qu'une entreprise doit inspecter et consigner le trafic (ou au moins consigner et inspecter les métadonnées lorsqu'elle traite du trafic qui ne peut pas être déchiffré par les systèmes de surveillance) dans son environnement. Une partie de ce trafic peut contenir des informations privées ou présenter des risques associés à la vie privée. Les organisations devront identifier tous les risques possibles associés à l'interception, à l'analyse et à la journalisation du trafic réseau [NISTIR 8062]. Il peut s'agir d'actions telles que l'information

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

des utilisateurs, l'obtention du consentement (via une page de connexion, une bannière ou similaire) et l'éducation des utilisateurs d'entreprise. Le cadre de confidentialité du NIST [NISTPRIV] pourrait aider à développer un processus formel pour identifier et atténuer tout risque lié à la confidentialité pour une entreprise développant une architecture Zero Trust.

6.3 ZTA et architecture fédérale de gestion des identités, des identifiants et des accès

L'approvisionnement par objet est un composant clé de ZTA. Le moteur de stratégies ne peut pas déterminer si les tentatives de connexion sont autorisées pour se connecter à une ressource si le PE ne dispose pas d'informations suffisantes pour identifier les sujets et les ressources associés. Des politiques strictes de provisionnement et d'authentification doivent être mises en place avant de passer à un déploiement plus aligné sur le Zero Trust. Les entreprises ont besoin d'un ensemble clair d'attributs et de politiques de sujet qui peuvent être utilisés par un PE pour évaluer les demandes d'accès.

L'Office of Management and Budget (OMB) a publié la M-19-17 sur l'amélioration de la gestion de l'identité pour le gouvernement fédéral. L'objectif de la politique est d'élaborer « ... une vision commune de l'identité en tant que catalyseur de l'exécution de la mission, de la confiance et de la sécurité de la Nation » [M-19-17]. Le mémo appelle toutes les agences fédérales à former un bureau ICAM pour régir les efforts liés à l'émission et à la gestion de l'identité. Bon nombre de ces politiques de gestion doivent utiliser les recommandations de la norme NIST SP 800-63-3, *Digital Identity Guidelines* [SP800-63]. Comme la ZTA dépend fortement d'une gestion précise de l'identité, tout effort de la ZTA devra intégrer la politique ICAM de l'agence.

6.4 ZTA et les connexions Internet de confiance 3.0

TIC est une initiative fédérale de cybersécurité gérée conjointement par l'OMB, le DHS et la General Services Administration (GSA), et vise à établir une base de référence en matière de sécurité du réseau dans l'ensemble du gouvernement fédéral. Historiquement, le TIC était une stratégie de cybersécurité basée sur le périmètre qui obligeait les agences à consolider et à surveiller leurs connexions réseau externes. Inhérent au TIC
1.0 et TIC 2.0 est l'hypothèse que l'intérieur du périmètre est « fiable », tandis que ZTA suppose que l'emplacement du réseau n'implique pas de « confiance » (c'est-à-dire qu'il n'y a pas de « confiance » sur le réseau interne d'une agence). TIC 2.0 fournit une liste de capacités de sécurité basées sur le réseau (par exemple, filtrage de contenu, surveillance, authentification, etc.) à déployer au point d'accès TIC au périmètre de l'agence ; bon nombre de ces capacités sont alignées sur les principes ZT.

TIC 3.0 a été mis à jour pour prendre en charge les services infonuagiques et les appareils mobiles [M-19-26]. Dans TIC 3.0, il est reconnu que la définition de « confiance » peut varier dans des contextes informatiques spécifiques et que les agences ont des tolérances au risque différentes pour définir les zones de confiance. De plus, TIC 3.0 dispose d'un manuel de capacités de sécurité TIC mis à jour, qui définit deux types de capacités de sécurité :
(1) les fonctionnalités de sécurité universelles qui s'appliquent au niveau de l'entreprise, et (2) les capacités de sécurité PEP qui sont des capacités au niveau du réseau à appliquer à plusieurs points d'application de politiques (PEP), tels que définis dans les cas d'utilisation TIC. Les capacités de sécurité de la PPE peuvent être appliquées à n'importe quelle PPE appropriée située le long d'un flux de données donné plutôt qu'à une seule PPE au périmètre de l'agence. Un grand nombre de ces fonctionnalités de sécurité TIC 3.0 prennent directement en charge ZTA (par exemple, le trafic chiffré, l'authentification forte, la microsegmentation, l'inventaire du réseau et

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

du système, etc.). TIC 3.0 définit des cas d'utilisation spécifiques qui décrivent la mise en œuvre de zones de confiance et de capacités de sécurité dans des applications, des services et des environnements spécifiques.

TIC 3.0 se concentre sur les protections de sécurité basées sur le réseau, tandis que ZTA est une architecture plus inclusive couvrant la protection des applications, des utilisateurs et des données. Au fur et à mesure que TIC 3.0 fait évoluer son utilisation
, il est probable qu'un cas d'utilisation de ZTA TIC sera développé pour définir les protections réseau à déployer aux points d'application de ZTA.

6.5 ZTA et EINSTEIN (NCPS – National Cybersecurity Protection System)

NCPS (connu sous le nom d'EINSTEIN) est un système intégré de systèmes qui offre des capacités de détection d'intrusion, d'analyse avancée, de partage d'informations et de prévention des intrusions pour défendre le gouvernement fédéral contre les cybermenaces. Les objectifs de la NCPS, qui s'alignent sur les objectifs globaux du Zero Trust, sont de gérer les cyberrisques, d'améliorer la cyberprotection et de donner aux partenaires les moyens de sécuriser le cyberespace. Les capteurs EINSTEIN permettent au National Cybersecurity and Communications Integration Center (NCCIC) de la CISA de défendre les réseaux fédéraux et de répondre aux incidents importants dans les agences fédérales.

Le placement des capteurs NCPS pour la connaissance de la situation du DHS est basé sur une défense de réseau de périmètre au sein du gouvernement fédéral, tandis que ZTA rapproche les protections des actifs, des données et de toutes les autres ressources. Le programme NCPS évolue pour s'assurer que la connaissance de la situation est préservée grâce à l'utilisation d'informations de sécurité sur le trafic basé sur le cloud, ce qui contribue à jeter les bases d'une télémétrie de connaissance de la situation élargie à partir des systèmes ZTA. Les fonctions de prévention des intrusions du NCPS devraient également évoluer pour être en mesure d'éclairer l'application des politiques à la fois dans les emplacements actuels du NCPS et dans les systèmes ZTA. À mesure que la ZTA sera adoptée dans l'ensemble du gouvernement fédéral, la mise en œuvre de la SNPC devra évoluer constamment, ou de nouvelles capacités devront être déployées pour atteindre les objectifs de la SNPC. Les intervenants en cas d'incident pourraient exploiter les informations provenant de l'authentification, de l'inspection du trafic et de la journalisation du trafic des agences disponibles pour les agences fédérales qui ont mis en œuvre une architecture Zero Trust. Les informations générées dans un ZTA peuvent mieux éclairer la quantification de l'impact d'un événement ; les outils d'apprentissage automatique pourraient utiliser les données ZTA pour améliorer la détection ; et des journaux supplémentaires de ZTA peuvent être conservés pour des analyses après coup par les intervenants en cas d'incident.

6.6 Programme de diagnostic et d'atténuation continus (CDM) ZTA et DHS

Le programme CDM du DHS est un effort visant à améliorer la technologie de l'information (TI) des agences fédérales. Il est essentiel qu'une agence ait une vision des actifs, de la configuration et des sujets qui la composent. Pour protéger un système, les agences doivent mettre en place des processus permettant de découvrir et de comprendre les composants et les acteurs de base de leur infrastructure :

- **Qu'est-ce qui est connecté ?** Quels appareils, applications et services sont utilisés par l'organisation ? Cela comprend l'observation et l'amélioration de la

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

posture de sécurité de ces artefacts au fur et à mesure que des vulnérabilités et des menaces sont découvertes.

- **Qui utilise le réseau ?** Quels utilisateurs font partie de l'organisation ou sont externes et autorisés à accéder aux ressources de l'entreprise ? Il s'agit notamment des ENP qui peuvent effectuer des actions autonomes.
- **Que se passe-t-il sur le réseau ?** Une entreprise a besoin d'informations sur les modèles de trafic et les messages entre les systèmes.
- **Comment les données sont-elles protégées ?** L'entreprise a besoin d'une politique définie sur la façon dont les informations sont protégées au repos, en transit et en cours d'utilisation.

La mise en œuvre d'un programme MDP solide est la clé du succès de la ZTA. Par exemple, pour passer à ZTA, une entreprise doit disposer d'un système permettant de découvrir et d'enregistrer les actifs physiques et virtuels afin de créer un inventaire utilisable. Le programme CDM du DHS a lancé plusieurs efforts pour renforcer les capacités nécessaires au sein des agences fédérales pour passer à une ZTA. Par exemple, le DHS

Le programme HWAM (Hardware Asset Management) est un effort visant à aider les agences à identifier les appareils sur leur infrastructure réseau afin de déployer une configuration sécurisée. Il s'agit d'une étape similaire aux premières étapes de l'élaboration d'une feuille de route vers la ZTA. Les agences doivent avoir une visibilité sur les actifs actifs sur le réseau (ou ceux qui accèdent aux ressources à distance) pour catégoriser, configurer et surveiller l'activité du réseau.

6.7 ZTA, Cloud Smart et la stratégie fédérale en matière de données

La stratégie Cloud Smart[8] , la politique mise à jour de l'initiative d'optimisation des centres de données [M-19-19] et la stratégie fédérale de données[9] influencent toutes certaines exigences pour les agences qui planifient un ZTA. Ces politiques exigent que les agences inventorient et évaluent la manière dont elles collectent, stockent et accèdent aux données, à la fois sur site et dans le cloud.

Cet inventaire est essentiel pour déterminer quels processus et ressources opérationnels bénéficieraient de la mise en œuvre d'un ZTA. Les ressources de données, les applications et les services qui sont principalement basés sur le cloud ou principalement utilisés par des travailleurs à distance sont de bons candidats pour une approche ZTA (voir la section 7.3.3), car les sujets et les ressources sont situés en dehors du périmètre du réseau d'entreprise et sont susceptibles de tirer le meilleur parti de l'utilisation, de l'évolutivité et de la sécurité.

Une considération supplémentaire dans le cadre de la Stratégie fédérale en matière de données est la façon de rendre les ressources de données des organismes accessibles aux autres organismes ou au public. Cela correspond au cas d'utilisation de la collaboration inter-entreprises ZTA (voir Section 4.4). Les agences qui utilisent un ZTA pour ces actifs devront peut-être tenir compte des exigences de collaboration ou de publication lors de l'élaboration de la stratégie.

[8] Stratégie fédérale en matière de cloud computing : https://cloud.cio.gov/strategy/
[9] Stratégie fédérale en matière de données : https://strategy.data.gov/

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

7 Migration vers une architecture Zero Trust

La mise en œuvre d'un ZTA est un parcours plutôt qu'un remplacement complet de l'infrastructure ou des processus. Une organisation doit chercher à mettre en œuvre progressivement des principes Zero Trust, des changements de processus et des solutions technologiques qui protègent ses actifs de données de plus grande valeur. La plupart des entreprises continueront à fonctionner en mode hybride Zero Trust/basé sur le périmètre pendant une période indéterminée, tout en continuant à investir dans des initiatives de modernisation informatique en cours. Le fait de disposer d'un plan de modernisation informatique qui inclut le passage à une architecture basée sur les principes ZT peut aider une entreprise à élaborer des feuilles de route pour les migrations de flux de travail à petite échelle.

La migration d'une entreprise vers une stratégie dépend de sa posture et de ses opérations actuelles en matière de cybersécurité. Une entreprise doit atteindre un niveau de compétence de base avant qu'il ne soit possible de déployer un environnement significatif axé sur les ZT [ACT-IAC]. Cette base de référence comprend l'identification et le catalogage des actifs, des sujets, des processus métier, des flux de trafic et des mappages de dépendances pour l'entreprise. L'entreprise a besoin de ces informations avant de pouvoir dresser une liste de processus opérationnels candidats et des sujets/actifs impliqués dans ce processus.

7.1 Pure Zero Trust Architecture

Dans une approche greenfield, il serait possible de construire une architecture Zero Trust à partir de zéro. En supposant que l'entreprise connaisse les applications/services et les flux de travail qu'elle souhaite utiliser pour ses opérations, elle peut produire une architecture basée sur les principes Zero Trust pour ces flux de travail. Une fois les flux de travail identifiés, l'entreprise peut affiner les composants nécessaires et commencer à cartographier la façon dont les composants individuels interagissent. À partir de là, il s'agit d'un exercice d'ingénierie et d'organisation dans la construction de l'infrastructure et la configuration des composants. Cela peut inclure des changements organisationnels supplémentaires en fonction de la façon dont l'entreprise est actuellement configurée et opérationnelle.

En pratique, il s'agit rarement d'une option viable pour les agences fédérales ou toute organisation disposant d'un réseau existant. Cependant, il peut arriver qu'une organisation soit appelée à assumer une nouvelle responsabilité qui nécessiterait la construction de sa propre infrastructure. Dans ces cas, il peut être possible d'introduire les concepts ZT dans une certaine mesure. Par exemple, une agence peut se voir confier une nouvelle responsabilité qui implique la création d'une nouvelle application, d'un nouveau service ou d'une nouvelle base de données. L'agence a pu concevoir l'infrastructure nouvellement nécessaire autour des principes ZT et de l'ingénierie système sécurisée [SP8900-160v1], comme l'évaluation de la confiance des sujets avant d'accorder l'accès et l'établissement de micro-périmètres autour des nouvelles ressources. Le degré de succès dépend de la dépendance de cette nouvelle infrastructure vis-à-vis des ressources existantes (par exemple, les systèmes de gestion des identités).

7.2 Architecture hybride basée sur le périmètre et ZTA

Il est peu probable qu'une entreprise importante puisse migrer vers le Zero Trust en un seul cycle de mise à jour technologique. Il peut y avoir une période indéfinie pendant laquelle les flux de

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

travail ZTA coexistent avec des flux de travail non ZTA dans une entreprise. La migration vers une approche ZTA de l'entreprise peut se faire un processus métier à la fois. L'entreprise doit s'assurer que les éléments communs (par exemple, la gestion des ID, la gestion des appareils, la journalisation des événements) sont suffisamment flexibles pour fonctionner dans une architecture de sécurité hybride basée sur ZTA et sur le périmètre. Les architectes d'entreprise peuvent également souhaiter limiter les solutions candidates ZTA à celles qui peuvent s'interfacer avec des composants existants.

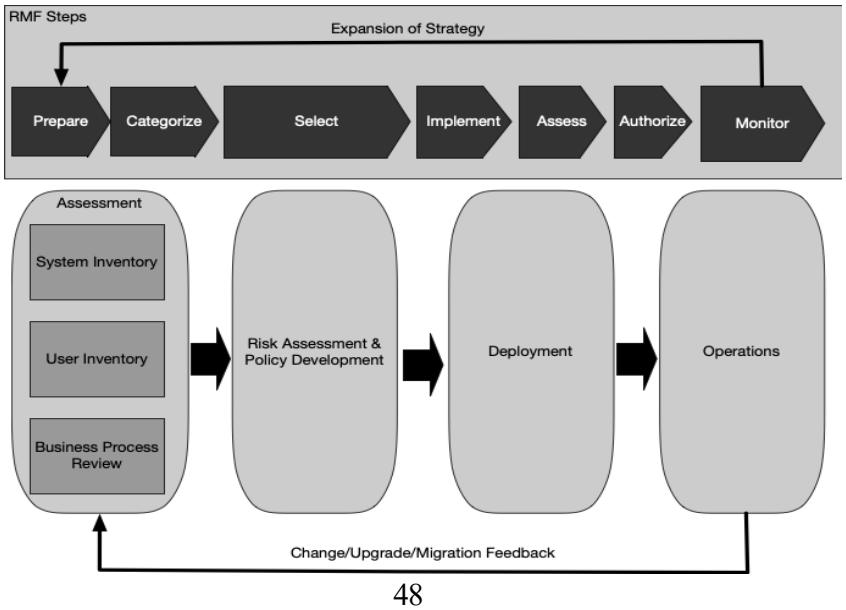
La migration d'un flux de travail existant vers un ZTA nécessitera probablement (au moins) une refonte partielle. Les entreprises peuvent profiter de cette occasion pour adopter des pratiques d'ingénierie système sécurisée [SP800-160v1] si elles ne l'ont pas déjà fait pour les flux de travail.

7.3 Étapes de l'introduction de ZTA dans un réseau architecturé basé sur le périmètre

La migration vers ZTA exige qu'une organisation ait une connaissance détaillée de ses actifs (physiques et virtuels), de ses sujets (y compris les privilèges des utilisateurs) et de ses processus métier. Le PE accède à ces connaissances lors de l'évaluation des demandes de ressources. Des connaissances incomplètes mèneront le plus souvent à une défaillance du processus opérationnel lorsque le PE refuse les demandes en raison d'un manque d'informations. Cela se pose particulièrement si des déploiements inconnus de « shadow IT » fonctionnent au sein d'une organisation.

Avant d'entreprendre un effort pour apporter ZTA à une entreprise, il doit y avoir une enquête sur les actifs, les sujets, les flux de données et les flux de travail. Cette prise de conscience constitue l'état fondamental qui doit être atteint avant qu'un déploiement ZTA ne soit possible. Une entreprise ne peut pas déterminer quels nouveaux processus ou systèmes doivent être mis en place si elle n'est pas au courant de l'état actuel des opérations. Ces enquêtes peuvent être menées en parallèle, mais les deux sont liées à l'examen des processus d'affaires de l'organisation. Ces étapes peuvent être mises en correspondance avec les étapes du CGR [SP800-37], car toute adoption d'un ZTA est un processus visant à réduire les risques pour les fonctions opérationnelles d'un organisme. Le chemin vers la mise en œuvre d'un ZTA peut être visualisé à la figure 12.

Figure 12 : Cycle de déploiement de ZTA



This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

Une fois l'inventaire initial créé, il y a un cycle régulier de maintenance et de mise à jour. Cette mise à jour peut soit modifier les processus opérationnels, soit ne pas avoir d'impact, mais une évaluation des processus opérationnels doit être effectuée. Par exemple, un changement de fournisseur de certificats numériques peut ne pas sembler avoir d'impact significatif, mais peut impliquer la gestion du magasin racine de certificats, la surveillance des journaux de transparence des certificats et d'autres facteurs qui ne sont pas apparents au premier abord.

7.3.1 Identifier les acteurs de l'entreprise

Pour qu'une entreprise Zero Trust puisse fonctionner, le PE doit avoir une connaissance des sujets de l'entreprise. Les sujets pourraient englober à la fois des NPE humains et possibles, tels que des comptes de service qui interagissent avec des ressources.

Les utilisateurs disposant de privilèges spéciaux, tels que les développeurs ou les administrateurs système, nécessitent un examen plus approfondi lorsqu'ils se voient attribuer des attributs ou des rôles. Dans de nombreuses architectures de sécurité héritées, ces comptes peuvent disposer d'une autorisation générale pour accéder à toutes les ressources de l'entreprise. ZTA doit permettre aux développeurs et aux administrateurs de disposer d'une flexibilité suffisante pour répondre à leurs besoins commerciaux tout en utilisant des journaux et des actions d'audit pour identifier les modèles de comportement d'accès. Les déploiements ZTA peuvent exiger des administrateurs qu'ils satisfassent à un niveau de confiance ou à des critères plus stricts, comme indiqué dans NIST SP 800-63A, section 5 [SP800-63A].

7.3.2 Identifier les actifs appartenant à l'entreprise

Comme nous l'avons mentionné à la section 2.1, l'une des principales exigences de ZTA est la capacité d'identifier et de gérer les appareils. ZTA exige également la capacité d'identifier et de surveiller les appareils n'appartenant pas à l'entreprise qui peuvent se trouver sur l'infrastructure réseau de l'entreprise ou qui accèdent aux ressources de l'entreprise. La capacité à gérer les actifs de l'entreprise est essentielle à la réussite du déploiement de ZTA. Cela comprend les composants matériels (par exemple, les ordinateurs portables, les téléphones, les appareils IoT) et les artefacts numériques (par exemple, les comptes d'utilisateurs, les applications, les certificats numériques). Il n'est peut-être pas possible d'effectuer un recensement complet de tous les actifs appartenant à l'entreprise, de sorte qu'une entreprise doit envisager de développer la capacité d'identifier, de catégoriser et d'évaluer rapidement les actifs nouvellement découverts qui se trouvent sur l'infrastructure appartenant à l'entreprise.

Cela va au-delà du simple catalogage et de la maintenance d'une base de données d'actifs d'entreprise. Cela inclut également la gestion et la surveillance de la configuration. La capacité d'observer l'état actuel d'un bien fait partie du processus d'évaluation des demandes d'accès (voir la section 2.1). Cela signifie que l'entreprise doit être en mesure de configurer, d'examiner et de mettre à jour les ressources d'entreprise, telles que les ressources virtuelles et les conteneurs. Cela inclut également son emplacement physique (selon les meilleures estimations) et son emplacement réseau. Ces informations devraient éclairer le PE lorsqu'il prend des décisions d'accès aux ressources.

Les actifs n'appartenant pas à l'entreprise et le « shadow IT » appartenant à l'entreprise doivent également être catalogués aussi bien que possible. Il peut s'agir de tout ce qui est visible par

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

l'entreprise (par exemple, l'adresse MAC, l'emplacement du réseau) et complété par la saisie des données de l'administrateur. Ces informations ne sont pas seulement utilisées pour les décisions d'accès (car les collaborateurs et les ressources BYOD peuvent avoir besoin de contacter les PPE), mais aussi pour la surveillance et l'enregistrement forensique par l'entreprise. Le Shadow IT présente un problème particulier dans la mesure où ces ressources appartiennent à l'entreprise, mais ne sont pas gérées comme les autres ressources. Certaines approches ZTA (principalement basées sur le réseau) peuvent même rendre les composants du Shadow IT inutilisables, car ils peuvent ne pas être connus et inclus dans les politiques d'accès au réseau.

De nombreuses agences fédérales ont déjà commencé à identifier les actifs de l'entreprise. Les organismes qui ont établi des capacités de programme CDM, tels que HWAM [HWAM] et Software Asset Management (SWAM) [SWAM], disposent d'un riche ensemble de données à partir desquelles s'appuyer pour mettre en œuvre un ZTA. Les organismes peuvent également disposer d'une liste de processus candidats à la ZTA qui impliquent des actifs de grande valeur (AVC) [M-19-03] qui ont été identifiés comme étant essentiels à la mission de l'organisme. Ce travail devrait exister à l'échelle de l'entreprise ou de l'agence avant qu'un processus opérationnel puisse être (re)conçu avec un ZTA. Ces programmes doivent être conçus pour être extensibles et adaptables aux changements de l'entreprise, non seulement lors de la migration vers ZTA, mais aussi lors de la prise en compte des nouveaux actifs, services et processus métier qui font partie de l'entreprise.

7.3.3 Identifier les processus clés et évaluer les risques associés à l'exécution du processus

Le troisième inventaire qu'une agence devrait entreprendre consiste à identifier et à classer les processus opérationnels, les flux de données et leur relation avec les missions de l'agence. Les processus métier doivent indiquer les circonstances dans lesquelles les demandes d'accès aux ressources sont accordées ou refusées. Une entreprise peut souhaiter commencer avec un processus métier à faible risque pour la première transition vers ZTA, car les perturbations n'auront probablement pas d'impact négatif sur l'ensemble de l'organisation. Une fois que l'on a acquis suffisamment d'expérience, des processus métier plus critiques peuvent devenir des candidats.

Les processus métier qui utilisent des ressources basées sur le cloud ou qui sont utilisés par des travailleurs à distance sont souvent de bons candidats pour ZTA et verraient probablement des améliorations en termes de disponibilité et de sécurité. Plutôt que de projeter le périmètre de l'entreprise dans le cloud ou d'amener les clients dans le réseau de l'entreprise via un VPN, les clients d'entreprise peuvent demander directement des services cloud. Les PEP de l'entreprise garantissent que les stratégies d'entreprise sont respectées avant que l'accès aux ressources ne soit accordé à un client. Les planificateurs doivent également tenir compte des compromis potentiels en matière de performances, d'expérience utilisateur et d'une éventuelle fragilité accrue du flux de travail qui peuvent survenir lors de la mise en œuvre de ZTA pour un processus métier donné.

7.3.4 Formulation de politiques pour le candidat ZTA

Le processus d'identification d'un service candidat ou d'un flux de travail d'entreprise dépend de plusieurs facteurs : l'importance du processus pour l'organisation, le groupe de sujets concernés et l'état actuel des ressources utilisées pour le flux de travail. La valeur de l'actif ou du flux de travail en fonction du risque pour l'actif ou le flux de travail peut être évaluée à l'aide du cadre de gestion des risques du NIST [SP800-37].

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

Une fois l'actif ou le flux de travail identifié, identifiez toutes les ressources en amont (par exemple, les systèmes de gestion d'ID, les bases de données, les micro-services), les ressources en aval (par exemple, la journalisation, la surveillance de la sécurité) et les entités (par exemple, les sujets, les comptes de service) qui sont utilisées ou affectées par le flux de travail. Cela peut influencer le choix du candidat lors de la première migration vers ZTA. Une application/un service utilisé par un sous-ensemble identifié de sujets de l'entreprise (par exemple, un système d'achat) peut être préféré à un autre qui est vital pour l'ensemble de la base de sujets de l'entreprise (par exemple, le courrier électronique).

Les administrateurs d'entreprise doivent ensuite déterminer l'ensemble de critères (s'ils utilisent une TA basée sur des critères) ou les pondérations du niveau de confiance (s'ils utilisent une TA basée sur le score) pour les ressources utilisées dans le processus métier candidat (voir la section 3.3.1). Les administrateurs peuvent avoir besoin d'ajuster ces critères ou valeurs pendant la phase de réglage. Ces ajustements sont nécessaires pour s'assurer que les politiques sont efficaces, mais qu'elles n'entravent pas l'accès aux ressources.

7.3.5 Identifier les solutions candidates

Une fois qu'une liste de processus métier candidats a été développée, les architectes d'entreprise peuvent composer une liste de solutions candidates. Certains modèles de déploiement (voir la section 3.1) sont mieux adaptés à des flux de travail particuliers et aux écosystèmes d'entreprise actuels. De même, certaines solutions de fournisseurs sont mieux adaptées à certains cas d'utilisation que d'autres. Voici quelques facteurs à prendre en compte :

- **La solution nécessite-t-elle l'installation de composants sur l'actif client ?** Cela peut limiter les processus métier où des actifs n'appartenant pas à l'entreprise sont utilisés ou souhaités, tels que le BYOD ou les collaborations inter-agences.
- **La solution fonctionne-t-elle lorsque les ressources des processus d'entreprise existent entièrement sur site ?** Certaines solutions supposent que les ressources demandées résideront dans le cloud (trafic nord-sud) et non dans un périmètre d'entreprise (trafic est-ouest). L'emplacement des ressources de processus d'affaires candidates influencera les solutions candidates ainsi que le ZTA pour le processus.
- **La solution permet-elle d'enregistrer les interactions à des fins d'analyse ?** L'un des éléments clés de ZT est la collecte et l'utilisation de données liées au flux de processus qui sont répercutées sur le PE lors de la prise de décisions d'accès.
- **La solution offre-t-elle une prise en charge étendue de différentes applications, services et protocoles ?** Certaines solutions peuvent prendre en charge un large éventail de protocoles (web, Secure Shell [SSH], etc.) et de transports (IPv4 et IPv6), tandis que d'autres peuvent ne fonctionner qu'avec un objectif restreint, comme le web ou l'e-mail.
- **La solution nécessite-t-elle des modifications du comportement du sujet ?** Certaines solutions peuvent nécessiter des étapes supplémentaires pour effectuer un flux de travail donné. Cela peut modifier la façon dont les sujets de l'entreprise exécutent le flux de travail.

Une solution consiste à modéliser un processus d'entreprise existant comme un programme pilote plutôt que comme un simple remplacement. Ce programme pilote pourrait être généralisé

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

pour s'appliquer à plusieurs processus d'affaires ou spécifique à un cas d'utilisation. Le projet pilote peut être utilisé comme un « terrain d'essai » pour ZTA avant de passer au déploiement de ZTA et de s'éloigner de l'infrastructure de processus héritée.

7.3.6 Déploiement initial et surveillance

Une fois le flux de travail candidat et les composants ZTA choisis, le déploiement initial peut commencer. Les administrateurs d'entreprise doivent mettre en œuvre les stratégies développées à l'aide des composants sélectionnés, mais peuvent souhaiter fonctionner en mode d'observation et de surveillance dans un premier temps. Peu d'ensembles de stratégies d'entreprise sont complets dans leurs premières itérations : les comptes d'utilisateurs importants (par exemple, les comptes administrateurs) peuvent se voir refuser l'accès aux ressources dont ils ont besoin ou ne pas avoir besoin de tous les privilèges d'accès qui leur ont été attribués.

Le nouveau flux de travail métier de ZT pourrait être utilisé en mode de reporting uniquement pendant un certain temps pour s'assurer que les politiques sont efficaces et réalisables. Cela permet également à l'entreprise de comprendre les demandes d'accès aux ressources et aux ressources de base, le comportement et les modèles de communication. Le rapport uniquement signifie que l'accès doit être accordé pour la plupart des demandes, et que les journaux et les traces des connexions doivent être comparés à la politique initialement développée. Des politiques de base, telles que le refus des requêtes qui échouent à l'authentification multifacteur (MFA) ou qui proviennent d'adresses IP connues, contrôlées par des attaquants ou subverties, doivent être appliquées et consignées. Cependant, après le déploiement initial, les politiques d'accès doivent être plus souples afin de collecter des données issues des interactions réelles du workflow ZT. Une fois les modèles d'activité de base du workflow établis, les comportements anormaux peuvent être plus facilement identifiés. S'il n'est pas possible d'adopter une approche plus souple, les opérateurs de réseaux d'entreprise doivent surveiller attentivement les journaux et se préparer à modifier les politiques d'accès en fonction de leur expérience opérationnelle.

7.3.7 Élargissement de la ZTA

Lorsque la confiance est suffisante et que l'ensemble des politiques de flux de travail est affiné, l'entreprise entre dans la phase opérationnelle stable. Le réseau et les actifs sont toujours surveillés, et le trafic est enregistré (voir la section 2.1), mais les réponses et les modifications de politique sont effectuées à un rythme plus lent, car elles ne doivent pas être graves. Les sujets et les parties prenantes des ressources et des processus concernés doivent également apporter un retour d'expérience pour améliorer les opérations. À ce stade, les administrateurs d'entreprise peuvent commencer à planifier la phase suivante du déploiement de ZT. À l'instar du déploiement précédent, il faut identifier un flux de travail et un ensemble de solutions candidats et élaborer des politiques initiales.

Toutefois, si une modification est apportée au flux de travail, l'architecture ZT opérationnelle doit être réévaluée. Les modifications importantes apportées au système, telles que l'ajout de nouveaux appareils, les mises à jour majeures des logiciels (en particulier les composants logiques ZT) et les modifications de la structure organisationnelle, peuvent entraîner des modifications du flux de travail ou des stratégies. En effet, l'ensemble du processus devrait être reconsidéré en supposant qu'une partie du travail a déjà été faite. Par exemple, de nouveaux appareils ont été achetés, mais aucun nouveau compte utilisateur n'a été créé, de sorte que seul l'inventaire des appareils doit être mis à jour.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

Références

[ACT-IAC] Conseil consultatif de l'American Council for Technology and Industry (2019) *Zero Trust Cybersecurity, Current Trends*. Disponible chez https://www.actiac.org/zero-trust-cybersecurity-current-trends

[Anderson] Anderson B, McGrew D (2017) Apprentissage automatique pour la classification du trafic de logiciels malveillants chiffrés : prise en compte des étiquettes bruyantes et de la non-stationnarité. *Actes de la 23e conférence internationale ACM SIGKDD sur la découverte de connaissances et l'exploration de données* (ACM, Halifax, Nouvelle-Écosse, Canada), pp 1723-1732. https://doi.org/10.1145/3097983.3098163

[BCORE] CIO du ministère de la Défense (2007). Département de la Défense, Global Information Grid Architecture, Vision, version 1.0, juin 2007. Disponible chez http://www.acqnotes.com/Attachments/DoD%20GIG%20Architectural %20Vision,%20June%2007.pdf

[ASC-SDP] Cloud Security Alliance (2015) Spécification SDP 1.0. Disponible chez https://cloudsecurityalliance.org/artifacts/sdp-specification-v1-0/

[FIPS199] National Institute of Standards and Technology (2004) Normes pour la catégorisation de la sécurité des informations et des systèmes d'information fédéraux. (Département du Commerce des États-Unis, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

[Gilman] Gilman E, Barth D (2017) *Zero Trust Networks : Building Secure Systems in Untrusted Networks* (O'Reilly Media, Inc., Sebastopol, CA), 1ère éd.

[HWAM] Département de la Sécurité intérieure (2015) *Description de la capacité de gestion des actifs matériels (HWAM*). Disponible chez https://www.us-cert.gov/sites/default/files/cdm_files/HWAM_CapabilityDescription.pdf

[IBNVN] Cohen R, Barabash K, Rochwerger B, Schour L, Crisan D, Birke R, Minkenberg C, Gusat M, Recio R, Jain V (2013) Une approche basée sur l'intention pour la virtualisation de réseau. *Symposium international IFIP/IEEE 2013 sur la gestion intégrée des réseaux (IM 2013).* (IEEE, Gand, Belgique), pp 42-50. Disponible chez https://ieeexplore.ieee.org/document/6572968

[JÉRICHO] Le Forum de Jéricho (2007) *Les commandements du Forum de Jéricho*, version 1.2. Disponible chez https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

[M-19-03] Bureau de la gestion et du budget (2018) Renforcer la cybersécurité des agences fédérales en améliorant l'actif de grande valeur Programme. (Maison-Blanche, Washington, DC), mémorandum M-19-03 de l'OMB, 10 décembre 2018. Disponible à l'adresse https://www.whitehouse.gov/wp-content /uploads/2018/12/M-19-03.pdf

[M-19-17] Bureau de la gestion et du budget (2019) Permettre l'exécution de la mission grâce à une meilleure gestion de l'identité, des identifiants et des accès. (Maison-Blanche, Washington, DC), note de service M-19-17 de l'OMB, 21 mai 2019. Disponible à l'adresse https://www.whitehouse.gov/wp-content /uploads/2019/05/M-19-17.pdf

[M-19-19] Bureau de la gestion et du budget (2019) Mise à jour sur l'initiative d'optimisation des centres de données (DCOI). (Maison-Blanche, Washington, DC), mémorandum M-19-19 de l'OMB, 25 juin 2019. Disponible chez https://datacenters.cio.gov/assets/files/m_19_19.pdf

[M-19-26] Bureau de la gestion et du budget (2019) Mise à jour de l'initiative Trusted Internet Connections (TIC). (Maison-Blanche, Washington, DC), mémorandum M-19-26 de l'OMB, 12 septembre 2019. Disponible chez https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf

[NISTIR 7987] Ferraiolo DF, Gavrila S, Jansen W (2015) Policy Machine : fonctionnalités, architecture et spécifications. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7987, Rev. 1. https://doi.org/10.6028/NIST.IR.7987r1

[NISTIR 8062] Brooks SW, Garcia ME, Lefkovitz NB, Lightman S, Nadeau EM (2017) Une introduction à l'ingénierie de la protection de la vie privée et à la gestion des risques dans les systèmes fédéraux. (National Institute of Standards and Technology, Gaithersburg, MD), rapport inter-agences ou interne (IR) 8062 du NIST. https://doi.org/10.6028/NIST.IR.8062

[NISTPRIV] National Institute of Standards and Technology (2020) Cadre de protection de la vie privée : un outil pour améliorer la protection de la vie privée grâce à la gestion des risques d'entreprise, version 1.0. (Institut national des normes et de la technologie, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.01162020

[SDNBOOK] Nadeau T, Gray K (2013) *SDN : Réseaux définis par logiciel : un examen faisant autorité des technologies de programmabilité du réseau.* (O'Reilly) 1ère éd.

[SP800-37] Groupe de travail interarmées (2018) Cadre de gestion des risques pour les systèmes d'information et les organisations : une approche du cycle de vie des systèmes pour la sécurité et la protection de la vie privée. (Institut national des normes et de la technologie, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

https://doi.org/10.6028/NIST.SP.800-37r2

[SP800-63] Grassi PA, Garcia ME, Fenton JL (2017) Directives d'identité numérique. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, comprend des mises à jour à partir du 2 mars 2020. https://doi.org/10.6028/NIST.SP.800-63-3

[SP800-63A] Grassi PA, Fenton JL, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) Directives d'identité numérique : inscription et vérification de l'identité. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63A, comprend des mises à jour à partir du 2 mars 2020. https://doi.org/10.6028/NIST.SP.800-63A

[SP800-160v1] Ross R, McEvilley M, Oren JC (2016) Ingénierie de la sécurité des systèmes : considérations pour une approche multidisciplinaire dans l'ingénierie de systèmes sécurisés dignes de confiance. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Comprend des mises à jour en date du 21 mars 2018. https://doi.org/10.6028/NIST.SP.800-160v1

[SP800-160v2] Ross R, Pillitteri V, Graubart R, Bodeau D, McQuaid R (2019) Développer des systèmes cyber-résilients : une approche d'ingénierie de la sécurité des systèmes. (Institut national des normes et de la technologie, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 2. https://doi.org/10.6028/NIST.SP.800-160v2

[SP800-162] Hu VC, Ferraiolo DF, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone KA (2014) Guide de définition et considérations du contrôle d'accès basé sur les attributs (ABAC). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-162, comprend des mises à jour à partir du 2 août 2019. https://doi.org/10.6028/NIST.SP.800-162

[NAGE] Département de la Sécurité intérieure (2015) *Description de la capacité de gestion des actifs logiciels (SWAM).* Disponible chez https://www.us-cert.gov/sites/default/files/cdm_files/SWAM_CapabilityDescription.pdf

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

Annexe A — Acronymes

API	Interface de programmation d'applications
BYOD	Apportez votre propre appareil
MDP	Diagnostic et atténuation continus
Le DHS	Département de la Sécurité intérieure
Déni de service	Déni de service
G2B	De gouvernement à entreprise (secteur privé)
G2G	De gouvernement à gouvernement
NIST	Institut national de normes et de technologie
NPE	Entité non physique
PAPA	Administrateur de politiques
PDP	Point de décision politique
PE	Moteur de politiques
ENTRAIN	Point d'application de la politique
PKI	Infrastructure à clé publique
RMF	Cadre de gestion des risques du NIST
SDN	Software-Defined Network
SDP	Périmètre défini par logiciel
SIEM	Informations de sécurité et surveillance des événements
TIC	Connexions Internet fiables
VPN	Réseau privé virtuel
ZT	Confiance zéro
ZTA	Zero Trust Architecture

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

Annexe B — Lacunes relevées dans l'état actuel de la technologie en ZTA

La maturité actuelle des composants et des solutions Zero Trust a été étudiée au cours des recherches menées dans le cadre de l'élaboration de ce document. Cette enquête a conclu que l'état actuel de l'écosystème ZTA n'est pas assez mature pour être adopté à grande échelle. Bien qu'il soit possible d'utiliser les stratégies ZTA pour planifier et déployer un environnement d'entreprise, il n'existe pas de solution unique qui fournit tous les composants nécessaires. De plus, peu de composants ZTA disponibles aujourd'hui peuvent être utilisés pour tous les différents flux de travail présents dans une entreprise.

Voici un résumé des lacunes relevées dans l'écosystème ZTA et des domaines qui nécessitent une enquête plus approfondie. Certains de ces domaines ont une certaine base de travail, mais la façon dont les principes de ZTA changent ces domaines n'est pas bien connue, car il n'y a pas assez d'expérience avec divers environnements d'entreprise axés sur ZTA.

B.1 Enquête technologique

Plusieurs fournisseurs ont été invités à présenter leurs produits et leurs points de vue sur le Zero Trust. L'objectif de cette enquête était d'identifier les éléments manquants qui empêchent les agences de passer à une infrastructure d'entreprise basée sur le Zero Trust dès maintenant ou de maintenir une mise en œuvre ZTA existante. Ces lacunes peuvent être classées en deux catégories : déploiement immédiat (immédiat ou à court terme), lacunes systémiques qui affectent la maintenance ou les opérations (à court ou à moyen terme) et connaissances manquantes (domaines de recherche future). Ils sont résumés dans le tableau B-1.

Tableau B-1 : Résumé des lacunes relevées en matière de déploiement

Catégorie	Exemples de questions	Lacunes identifiées
Déploiement immédiat	• Comment les exigences en matière d'approvisionnement doivent-elles être rédigées ? • Comment un plan ZTA fonctionne-t-il avec les exigences TIC, FISMA et autres ?	• Absence d'un cadre et d'un vocabulaire communs pour ZTA • Perception que ZTA entre en conflit avec la politique existante
Systémique	• Comment éviter la dépendance vis-à-vis d'un fournisseur ? • Comment les différents environnements ZTA interagissent-ils ?	• Trop de dépendance aux API des fournisseurs

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

Domaines nécessitant davantage de recherches	• Comment les menaces vont-elles évoluer face à ZTA ? • Comment les processus d'entreprise vont-ils changer face à ZTA ?	• À quoi ressemble un compromis réussi dans une entreprise avec un ZTA • Expérience documentée de l'utilisateur final dans une entreprise dotée d'un ZTA

B.2 Lacunes qui empêchent un passage immédiat à ZTA

Ce sont les problèmes qui ralentissent actuellement l'adoption d'un ZTA. Ces problèmes ont été classés comme des problèmes immédiats, et aucune réflexion n'a été prise en compte pour la maintenance ou la migration future dans cette catégorie. Une entreprise avant-gardiste peut également considérer que la catégorie de maintenance est une préoccupation immédiate pour empêcher le déploiement initial des composants ZTA, mais ces questions sont considérées comme une catégorie distincte pour la présente analyse.

B.2.1 Absence de termes communs pour la conception, la planification et l'approvisionnement de ZTA

Le Zero Trust en tant que stratégie de conception et de déploiement de l'infrastructure d'entreprise est encore un concept en formation. L'industrie ne s'est pas encore regroupée autour d'un seul ensemble de termes ou de concepts pour décrire les composants et les opérations de ZTA. Il est donc difficile pour les organisations (par exemple, les agences fédérales) d'élaborer des exigences et des politiques cohérentes pour la conception d'une infrastructure d'entreprise Zero Trust et l'approvisionnement en composants.

Le moteur des sections 2.1 et 3.1 est une première tentative de former une base neutre de termes et de concepts pour décrire ZTA. Les composants abstraits de ZTA et les modèles de déploiement ont été développés pour servir de termes de base et de façons de penser à ZTA. L'objectif est de fournir une méthode commune de visualisation, de modélisation et de discussion des solutions ZTA lors de l'élaboration des exigences de l'entreprise et de la réalisation d'études de marché. Les sections ci-dessus peuvent s'avérer incomplètes à mesure que l'on acquiert de l'expérience avec ZTA dans les agences fédérales, mais elles servent actuellement de base à un cadre conceptuel commun.

B.2.2 Perception que ZTA entre en conflit avec les politiques fédérales existantes en matière de cybersécurité

On pense à tort que ZTA est un cadre unique avec un ensemble de solutions incompatibles avec la vision existante de la cybersécurité. Le Zero Trust doit plutôt être considéré comme une évolution des stratégies de cybersécurité actuelles, car de nombreux concepts et idées circulent depuis longtemps. Les agences fédérales ont été encouragées à adopter une approche plus Zero Trust en matière de cybersécurité par le biais des directives existantes (voir la section 6). Si un organisme dispose d'un système de gestion de l'identité mature et de solides capacités CDM, il est sur la voie d'un ZTA (voir la section 7.3). Cet écart est basé sur une idée fausse de ZTA et de la façon dont elle a évolué par rapport aux paradigmes de cybersécurité précédents.

B.3 Lacunes systémiques qui ont un impact sur ZTA

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

Ce sont les lacunes qui affectent la mise en œuvre et le déploiement initiaux de ZTA et la poursuite de l'exploitation/maturité. Ces lacunes pourraient ralentir l'adoption de la ZTA dans les agences ou entraîner une fragmentation de l'industrie des composants ZTA. Les lacunes systémiques sont des domaines où des normes ouvertes (produites par un organisme d'élaboration de normes [SDO] ou un consortium industriel) peuvent aider.

B.3.3 Standardisation des interfaces entre les composants

Au cours de l'enquête technologique, il est devenu évident qu'aucun fournisseur ne propose une solution unique qui fournira une confiance zéro. De plus, il n'est peut-être pas souhaitable d'utiliser une solution à fournisseur unique pour atteindre le Zero Trust et risquer ainsi la dépendance vis-à-vis d'un fournisseur. Cela conduit à l'interopérabilité au sein des composants non seulement au moment de l'achat, mais aussi au fil du temps.

L'éventail des composants au sein de l'entreprise au sens large est vaste, de nombreux produits se concentrant sur un seul créneau au sein du Zero Trust et s'appuyant sur d'autres produits pour fournir des données ou un service à un autre composant (par exemple, l'intégration de l'authentification multifacteur pour l'accès aux ressources). Pour réaliser cette intégration, les fournisseurs s'appuient trop souvent sur des API propriétaires fournies par des entreprises partenaires plutôt que sur des API standardisées et indépendantes des fournisseurs. Le problème avec cette approche est que ces API sont propriétaires et contrôlées par un seul fournisseur. Le fournisseur qui contrôle peut modifier le comportement de l'API, et les intégrateurs sont tenus de mettre à jour leurs produits en conséquence. Cela nécessite des partenariats étroits entre les communautés de fournisseurs pour assurer une notification précoce des modifications dans les API, qui peuvent affecter la compatibilité entre les produits. Cela ajoute une charge supplémentaire pour les fournisseurs et les consommateurs : les fournisseurs doivent consacrer des ressources pour modifier leurs produits, et les consommateurs doivent appliquer des mises à jour à plusieurs produits lorsqu'un fournisseur apporte une modification à son API propriétaire. De plus, les fournisseurs sont tenus d'implémenter et de gérer des wrappers pour chaque composant partenaire afin de permettre une compatibilité et une interopérabilité maximales. Par exemple, de nombreux fournisseurs de produits MFA sont tenus de créer un wrapper différent pour chaque fournisseur de cloud ou système de gestion des identités afin qu'il puisse être utilisé dans différents types de combinaisons de clients.

Du côté du client, cela génère des problèmes supplémentaires lors de l'élaboration des exigences d'achat de produits. Il n'existe pas de normes sur lesquelles les acheteurs peuvent s'appuyer pour identifier la compatibilité entre les produits. Par conséquent, il est très difficile de créer une feuille de route pluriannuelle pour passer à ZTA, car il est impossible d'identifier un ensemble minimum d'exigences de compatibilité pour les composants.

B.3.4 Normes émergentes qui remédient à la dépendance excessive à l'égard des API propriétaires

Comme il n'existe pas de solution unique pour développer un ZTA, il n'existe pas d'ensemble unique d'outils ou de services pour une entreprise Zero Trust. Ainsi, il est impossible de disposer d'un protocole ou d'un cadre unique permettant à une entreprise de passer à un ZTA. Actuellement, il existe une grande variété de modèles et de solutions cherchant à devenir l'autorité principale de ZTA.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

Cela indique qu'il est possible d'élaborer un ensemble de protocoles ou de cadres ouverts et normalisés pour aider les organisations à migrer vers une ZTA. Les SDO comme l'Internet Engineering Task Force (IETF) ont spécifié des protocoles qui peuvent être utiles pour échanger des informations sur les menaces (appelés XMPP-Grid [1]). La Cloud Security Alliance (CSA) a produit un cadre pour le périmètre défini par logiciel (SDP) [2] qui peut également être utile dans ZTA. Les efforts devraient viser à examiner l'état actuel des cadres liés à la ZTA ou des protocoles nécessaires à une ZTA utile et à identifier les endroits où des travaux sont nécessaires pour produire ou améliorer ces spécifications.

B.4 Lacunes dans les connaissances sur le ZTA et les futurs domaines de recherche

Les lacunes énumérées ici n'empêchent pas une organisation d'adopter un ZTA pour son entreprise. Il s'agit de zones grises dans la connaissance des environnements ZTA opérationnels, et la plupart découlent d'un manque de temps et d'expérience avec des déploiements Zero Trust matures. Ce sont là des axes de travail d'avenir pour les chercheurs.

B.4.5 Réponse de l'attaquant à ZTA

Un ZTA correctement mis en œuvre pour une entreprise améliorera la posture de cybersécurité de l'entreprise par rapport à la sécurité traditionnelle basée sur le périmètre du réseau. Les principes de ZTA visent à réduire l'exposition des ressources aux attaquants et à minimiser ou à empêcher les mouvements latéraux au sein d'une entreprise en cas de compromission d'un actif hôte.

Cependant, les attaquants déterminés ne resteront pas les bras croisés, mais changeront plutôt de comportement face à la ZTA. La question ouverte est de savoir comment les attaques vont changer. Il est possible que les attaques visant à voler des informations d'identification soient étendues à l'authentification multifacteur (par exemple, le phishing, l'ingénierie sociale). Une autre possibilité est que, dans une entreprise hybride basée sur ZTA/périmètre, les attaquants se concentrent sur les processus métier qui n'ont pas été appliqués selon les principes ZTA (c'est-à-dire qui suivent la sécurité traditionnelle basée sur le périmètre du réseau), c'est-à-dire qu'ils ciblent les fruits à portée de main pour tenter de s'implanter dans le processus commercial ZTA.

Au fur et à mesure que ZTA mûrit, que d'autres déploiements sont observés et que l'expérience est acquise, l'efficacité de ZTA à réduire la surface d'attaque des ressources peut devenir évidente. Il faudra également élaborer des indicateurs de succès de ZTA par rapport aux anciennes stratégies de cybersécurité.

B.4.6 Expérience utilisateur dans un environnement ZTA

Il n'y a pas eu d'examen rigoureux de la façon dont les utilisateurs finaux agissent dans une entreprise qui utilise un ZTA. Cela est principalement dû au manque de grands cas d'utilisation de ZTA disponibles pour l'analyse. Cependant, des études ont été menées sur la façon dont les utilisateurs réagissent à l'authentification multifacteur et à d'autres opérations de sécurité qui font partie d'une entreprise ZTA, et ce travail pourrait constituer la base de la prédiction de l'expérience et du comportement de l'utilisateur final lors de l'utilisation des flux de travail ZTA dans une entreprise.

Une série d'études qui peuvent prédire comment ZTA affecte l'expérience de l'utilisateur final

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

est le travail effectué sur l'utilisation de la MFA dans les entreprises et la fatigue de la sécurité. La fatigue de la sécurité [3] est le phénomène dans lequel les utilisateurs finaux sont confrontés à tant de politiques et de défis de sécurité qu'elle commence à avoir un impact négatif sur leur productivité. D'autres études montrent que l'authentification multifacteur peut modifier le comportement de l'utilisateur, mais le changement global est mitigé [4] [5]. Certains utilisateurs acceptent facilement l'authentification multifacteur si le processus est simplifié et implique des appareils qu'ils ont l'habitude d'utiliser ou d'avoir avec eux (par exemple, des applications sur un smartphone). Cependant, certains utilisateurs n'apprécient pas d'avoir à utiliser des appareils personnels pour les processus d'entreprise ou ont l'impression d'être constamment surveillés pour détecter d'éventuelles violations des politiques informatiques.

B.4.7 Résilience de ZTA face aux perturbations de l'entreprise et du réseau

L'enquête sur l'écosystème des fournisseurs de ZTA a révélé le large éventail d'infrastructures qu'une entreprise déployant un ZTA devrait prendre en compte. Comme indiqué précédemment, il n'existe pas à l'heure actuelle de fournisseur unique d'une solution Zero Trust complète. Par conséquent, les entreprises achèteront plusieurs services et produits différents, ce qui peut conduire à un réseau de dépendances pour les composants. Si un composant vital est perturbé ou inaccessible, il peut y avoir une cascade de défaillances qui ont un impact sur un ou plusieurs processus métier.

La plupart des produits et services étudiés s'appuyaient sur une présence dans le cloud pour assurer leur robustesse, mais même les services cloud sont connus pour devenir inaccessibles à la suite d'une attaque ou d'une simple erreur. Lorsque cela se produit, les éléments clés utilisés pour prendre les décisions d'accès peuvent être inaccessibles ou ne pas être en mesure de communiquer avec d'autres composants. Par exemple, les composants PE et PA situés dans un cloud peuvent être accessibles lors d'une attaque par déni de service distribué (DDoS), mais peuvent ne pas être en mesure d'atteindre toutes les PEP situées avec des ressources. Des recherches sont nécessaires pour découvrir les points d'étranglement possibles des modèles de déploiement ZTA et l'impact sur les opérations réseau lorsqu'un composant ZTA est inaccessible ou a une accessibilité limitée.

Les plans de continuité des opérations (COOP) d'une entreprise devront probablement être révisés lors de l'adoption d'un ZTA. Un ZTA facilite de nombreux facteurs COOP, car les travailleurs à distance peuvent avoir le même accès aux ressources qu'ils avaient sur site. Cependant, des politiques telles que l'authentification multifacteur peuvent également avoir un impact négatif si les utilisateurs ne sont pas correctement formés ou manquent d'expérience. Les utilisateurs peuvent oublier ou ne pas avoir accès aux jetons et aux appareils d'entreprise en cas d'urgence, ce qui aura un impact sur la vitesse et l'efficacité des processus métier de l'entreprise.

B.5 Références

[1] Cam-Winget N (éd.), Appala S, Pope S, Saint-André P (2019) Utilisation du protocole XMPP (Extensible Messaging and Presence Protocol) pour l'échange d'informations de sécurité. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 8600. https://doi.org/10.17487/RFC8600

[2] Groupe de travail sur le périmètre défini par logiciel « SDP Specification 1.0 » Cloud Security Alliance. Avril 2014.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

[3] Stanton B, Theofanos MF, Spickard Prettyman S, Furman S (2016) Fatigue de sécurité. *Professionnel de l'informatique* 18(5) :26-32. https://doi.org/10.1109/MITP.2016.84

[4] Strouble D, Shechtman GM, Alsop AS (2009) Effets de la productivité et de la convivialité de l'utilisation d'un système de sécurité à deux facteurs. *Actes de SAIS 2009* (AIS, Charleston, SC), p 37. Disponible chez http://aisel.aisnet.org/sais2009/37

[5] Weidman J, Grossklags J (2017) J'aime ça mais je le déteste : perceptions des employés à l'égard d'une transition institutionnelle vers l'authentification à deux facteurs BYOD. *Actes de la 33e conférence annuelle sur les applications de sécurité informatique (ACSAC 2017)* (ACM, Orlando, FL), pp 212-224. https://doi.org/10.1145/3134600.3134629

Clause de non-responsabilité: Cette traduction a été réalisée automatiquement dans le but d'aider les francophones non anglophones à comprendre la publication spéciale NIST 800-207. AB AUDIT met à votre disposition le document en l'état et ne supporte aucune responsabilité quant aux erreurs qui pourraient être ou auraient été introduites lors de la traduction. Document téléchargeable à partir de www.ab-audit.com