Architecture Zero Trust
Qu'est-ce la stratégie Zero Trust et comment l'implémenter ?

Alcatel·Lucent Enterprise

eBook
Architecture Zero Trust

Table des matières

Qu'est-ce qu'une architecture Zero Trust ?

Que signifie l'expression architecture Zero Trust (ZTA, confiance zéro) ? Cette architecture consiste à authentifier et à autoriser chaque utilisateur et chaque appareil avant que l'accès aux données ne soit autorisé. Cette stratégie a pour principe directeur de « ne jamais faire confiance, toujours vérifier ».

Une analogie vous permettra de mieux comprendre.

Si nous considérons la sécurité traditionnelle comme une forteresse qui protège un village, nous construirions le mur de la forteresse (connu sous le nom de pare-feu) autour du village (c'est-à-dire, l'entreprise). Tout ce qui vient de l'extérieur de la forteresse est considéré comme non fiable et est minutieusement contrôlé, alors que tout ce qui se trouve à l'intérieur de la forteresse est implicitement digne de confiance et autorisé. Cette frontière de confiance est à la fois physique et implicite, selon le côté de la forteresse où l'on se trouve, car tant que l'on se trouve du « bon » côté du mur, aucune vérification supplémentaire n'est nécessaire. Si nous considérons cette approche en termes de réseau d'entreprise, il peut y avoir une segmentation de base sous la forme de VLAN, de SSID, de sous-réseaux ou d'interfaces liés à un pare-feu, mais cette segmentation est statique et se rapporte davantage à l'évolutivité et à la gestion du réseau qu'à la sécurité.

Aujourd'hui, l'approche du pare-feu (forteresse) perd toutefois de son efficacité par elle-même, pour de nombreuses raisons. La première est la mobilité. Les utilisateurs se connectent à d'autres réseaux situés à l'extérieur de l'entreprise et peuvent ainsi créer des menaces. La deuxième est le fait que les invités ne sont pas nécessairement tous dignes de confiance. On pourrait faire valoir que nous ne devrions tout simplement pas faire aveuglément confiance aux employés (ceux qui se trouvent à l'intérieur de la forteresse). Et la troisième est l'ajout toujours plus important d'appareils IoT au réseau. Ils présentent des risques plus élevés en matière de sécurité car ils ne sont pas nécessairement approuvés et gérés par le service informatique, et ils ne disposent généralement pas de capacités de sécurité. Dans le cadre de l'approche traditionnelle « forteresse/village », « pare-feu/entreprise », si un utilisateur ou un appareil est compromis, rien ou presque rien n'empêche la menace de s'étendre à d'autres utilisateurs et appareils. Une fois à l'intérieur, vous avez la possibilité de vous déplacer librement.

Dans l'analogie de la forteresse, si le mur constitue le seul élément qui protège le village des intrus, le jour où ces derniers apprendront à l'escalader - et cela arrivera un jour - on peut s'attendre à un carnage.

La question est de savoir comment éviter cette situation. Réfléchissons-y par rapport à l'approche « Ne jamais faire confiance » ou « Zero Trust ».

Dans le cas du Zero Trust, aucun utilisateur ou dispositif n'est digne de confiance. Qu'ils se trouvent sur site ou hors site, ils sont soumis aux mêmes contrôles. On ne peut faire confiance les yeux fermés aux utilisateurs internes. Chaque accès est alors authentifié et autorisé.

Une fois encore, dans l'analogie de la forteresse, cela signifierait qu'en plus de la forteresse qui protège le village des menaces extérieures, chaque maison et chaque bâtiment possède sa propre sécurité pour se protéger des risques provenant d'acteurs malfaisants vivant à l'intérieur de la forteresse. Au niveau de l'entreprise, ce que l'on appelle la micro-segmentation définie par logiciel va encore plus loin. Outre la forteresse et la sécurité mise en place autour des bâtiments, des gardes de sécurité personnels surveillent tous nos faits et gestes. Et où que nous allions, on nous demande notre passeport. Dans le réseau d'entreprise, cette frontière de confiance est floue, distribuée et mobile. Elle n'est pas liée à un emplacement, à un port de commutation ou à un VLAN particulier. Elle dépend, entre autres, de l'identité, de l'appareil, de la situation et du moment de la journée. Elle est définie par logiciel et s'adapte à tout instant. Dans cette approche, les composants doivent être gérés et capables de réagir et de se reconfigurer, si nécessaire, afin de répondre aux menaces ou aux changements dans le flux de travail.

Comprendre la macro et micro-segmentation

Dans une architecture Zero Trust, il existe deux types de segmentation : la macro et la micro. Dans le cadre de notre analogie, le mur de la forteresse est la macro-segmentation, et les agents de sécurité personnels représentent la micro-segmentation.

Dans la **macro-segmentation**, le réseau physique est divisé en différents segments logiques. Ces segments peuvent être un VLAN, une combinaison de VLAN et VRF (Virtual Routing and Forwarding) ainsi qu'un VPN lorsqu'on parle de Shortest Path Bridging (SPB), de MPLS, ou même de tunnels VXLAN ou GRE. Tout trafic entre les utilisateurs ou les appareils sur différents segments est contrôlé par un pare-feu. Toutes les entreprises utilisent la segmentation, d'une manière ou d'une autre, mais pas toujours pour des raisons de sécurité. Très souvent, ce type de segmentation est recherché pour des raisons d'évolutivité, d'administration ou d'organisation. Si deux appareils sont affectés à des VLAN différents mais qu'ils peuvent pas communiquer sans passer par un pare-feu, alors ils se trouvent sur le même macro-segment. Un exemple type de ce genre de segmentation est l'exécution de la téléphonie IP sur des VLAN et des VRF séparés qui sont logiquement isolés des PC.

Alors, comment pouvons-nous associer les utilisateurs ou les appareils à ces segments ? Bien qu'il soit possible de le faire de manière statique, par port de commutateur ou SSID par exemple, cette procédure est vraiment devenue obsolète. Elle est trop rigide et n'est pas de bon augure pour les utilisateurs mobiles. L'idéal pour vous serait d'avoir un système d'authentification défini par logiciel, de sorte que lorsqu'un utilisateur ou un appareil se connecte et s'authentifie, un profil lui est attribué. Le profil placera l'utilisateur ou l'appareil sur le bon segment, indépendamment de l'emplacement physique, du port du commutateur ou du SSID.

Si la macro-segmentation présente des avantages en matière de sécurité, elle est souvent adoptée pour des raisons organisationnelles ou administratives. Par exemple, les caméras et les serrures de porte sont contrôlées par le groupe de sécurité d'accès, alors que les thermostats le sont par le groupe de maintenance des bâtiments.

La micro-segmentation va encore plus loin. On part du principe que les utilisateurs ne sont pas tous identiques et qu'ils n'ont pas tous un besoin légitime d'accéder à l'ensemble des ressources. Le même profil qui associe les utilisateurs à un segment comprend également un ensemble de règles qui ajoutent un contrôle à faible granularité sur les privilèges des utilisateurs/appareils différents selon les rôles, tels que les RH par rapport à la finance. C'est ce que l'on appelle l'**accès basé sur les rôles**, lequel est directement lié au **principe du moindre privilège**. Ainsi, même si les caméras et les serrures de porte se trouvent sur le même segment, elles n'ont pas besoin d'utiliser les mêmes ressources. La caméra doit communiquer avec l'enregistreur vidéo et la serrure de porte avec son serveur. Tout comme une caméra n'a pas à communiquer avec une serrure de porte, deux serrures de porte n'ont pas besoin de communiquer entre elles. Ces autorisations rigoureuses sont mises en œuvre par le biais de règles appartenant au profil et sont appliquées dynamiquement à l'appareil après authentification.

La micro-segmentation doit être définie par logiciel pour plusieurs raisons. Ni les utilisateurs ni les appareils IoT ne sont statiques. Ils se déplacent, se connectent et se déconnectent, et les règles ne peuvent donc pas être liées à un emplacement ou à un port. En effet, les configurations de la micro-segmentation doivent être dynamiques et basées sur la combinaison de plusieurs facteurs, notamment, mais sans s'y limiter, l'identité de l'utilisateur ou de l'appareil, l'heure de la journée et l'emplacement.

En résumé, lorsque la communication entre différents segments est contrôlée par un pare-feu, on parle de macro-segmentation. Lorsque la communication au sein d'un même segment est contrôlée par des règles de contrôle d'accès au réseau (NAC) associées à l'appareil ou au rôle de l'utilisateur, on parle alors de micro-segmentation.

Pourquoi vous avez besoin des deux

Que se passe-t-il si vous n'utilisez qu'un seul type de segmentation ?

Examinons la macro-segmentation. Le problème lié à l'utilisation de cette approche uniquement est que le pare-feu devient un goulot d'étranglement car tout le trafic doit passer par lui pour l'authentification et l'autorisation, ce qui peut entraîner des problèmes de performance. Vous pouvez déployer plusieurs pare-feu au niveau de la couche de distribution, mais cela peut s'avérer assez coûteux et n'améliorera pas nécessairement les performances puisque les pare-feu n'ont pas de débit filaire. En outre, il existe alors plusieurs points d'application des règles et plusieurs endroits pour les mettre à jour, ce qui complique la gestion.

L'autre option, qui consiste à n'utiliser que la micro-segmentation, est tout aussi problématique. Si l'application des règles se fait par le biais de politiques NAC, ces listes de politiques deviendront très longues et complexes, et vous risquez d'épuiser les limites de capacité de l'appareil.

En résumé, il est préférable de trouver un juste équilibre entre ces deux types de segmentation. Laissez le pare-feu contrôler le trafic entre les différents segments (verticaux) et les politiques NAC contrôler le trafic au sein d'un segment donné (latéral).

La combinaison de ces deux segmentations vous permet d'agir sur les menaces de sécurité qui débordent d'un segment de sécurité à un autre, ainsi que sur celles qui se déplacent latéralement à travers le même segment. En termes plus concrets, la micro-segmentation représente un moyen d'empêcher qu'un attaquant qui a réussi à compromettre une caméra n'utilise cette brèche comme pivot pour compromettre d'autres ressources telles qu'une serrure de porte.

L'objectif consiste à authentifier chaque connexion et à attribuer des autorisations à chaque utilisateur ou appareil. Cela signifie que la segmentation doit permettre d'empêcher la propagation des menaces par le biais de mouvements latéraux, ainsi que la surveillance continue et la mise en quarantaine de tout utilisateur ou appareil devenant non conforme.

Comment l’implémenter ?

Dans le cas d'une nouvelle situation, il serait relativement facile de concevoir une architecture Zero Trust en utilisant la micro-segmentation dès le début. Mais, dans des situations existantes, la mise à niveau du réseau avec la micro-segmentation risque d'entraîner le blocage des utilisateurs, des appareils et des applications en raison d'un échec de l'authentification ou de politiques incomplètes. Il serait difficile, voire improbable, qu'une entreprise puisse migrer en une seule fois - en un seul cycle de mise à niveau.

Dans les environnements existants, il y aura nécessairement une période de coexistence entre les architectures Zero Trust et celles qui ne le sont pas, et la migration sera effectuée une seule couche ou un seul emplacement à la fois. Ce qui est important, c'est que vous vérifiez que les éléments de l'infrastructure déployés, ainsi que leur mode de déploiement, soient flexibles et capables de fonctionner dans un mode Zero Trust ou micro-segmenté lorsque d'autres éléments de l'infrastructure seront prêts. Cela signifie que l'infrastructure devra pouvoir interopérer avec les composants existants et futurs.

La méthodologie

La mise en place d'une architecture Zero Trust s'effectue en cinq étapes : surveiller, valider et évaluer, planifier, simuler et appliquer.

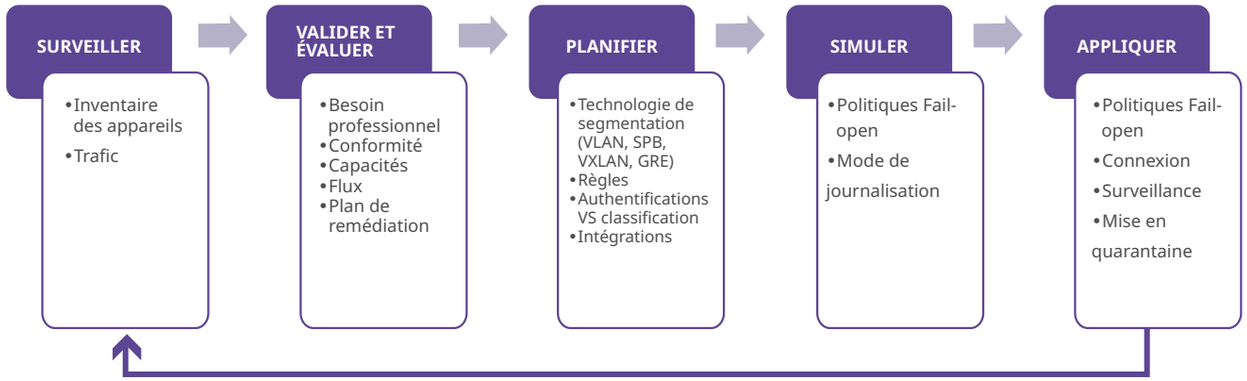

Figure 1 - La méthodologie

Étape 1 : surveiller

Avant toute chose, vous devez commencer à surveiller et à établir une carte et un inventaire de ce que vous possédez dans votre réseau.

La migration vers la ZTA nécessite une connaissance détaillée des équipements (physiques et virtuels), des sujets (y compris les privilèges des utilisateurs) et des processus métiers qui touchent ou circulent sur le réseau. Une connaissance incomplète conduira le plus souvent à un échec lorsque l'accès est refusé en raison d'informations insuffisantes. Ce problème se pose tout particulièrement en cas de « shadow IT » inconnue ou d'« IoT fantôme » au sein de l'organisation.

Commencez à surveiller les appareils et les flux de trafic. Créez un rapport d'inventaire de tous les appareils détectés sur le réseau, classés par type, fabricant, modèle, système d'exploitation, entre autres. Le rapport doit également indiquer où et avec quel port de commutateur ou SSID l'appareil a été vu pour la dernière fois. Ces informations peuvent être recueillies à partir d'éléments tels que l'adresse MAC, la signature DHCP et l'agent utilisateur HTTP.

La majorité des outils tiers ne fournissent qu'une adresse IP, et non le type d'équipement. L'idéal serait de disposer d'un outil qui permettrait de créer un inventaire des IoT/appareils afin de faciliter la création rapide de profils NAC pour chaque type d'appareil.

L'autre élément d'information nécessaire à la création de politiques est le flux de trafic. Selon l'équipement dont vous disposez, vous pouvez obtenir ces informations à partir d'outils de surveillance des flux tels que sFlow, Netflow ou Deep Packet Inspection (DPI).

Ce processus sera itératif. La première fois que vous activerez la surveillance, les rapports ne seront peut-être pas aussi utiles, mais au fur et à mesure que vous progresserez dans les étapes suivantes, ils deviendront plus spécifiques et précieux. Les informations recueillies au cours de cette étape seront essentielles pour les prochaines étapes.

Étape 2 : valider et évaluer

L'étape suivante consiste à valider ces résultats, et à évaluer les besoins de l'entreprise. Tout IoT fantôme ne pouvant être justifié devrait être supprimé car il élargit inutilement la surface d'attaque. Pour le reste, vous devrez identifier les sujets (utilisateurs et appareils), les flux de trafic et de travail, car ils devront être pris en compte dans vos politiques. Par exemple, vous devrez décider qui pourra accéder à des équipements spécifiques, et le type d'autorisation accordé pour ces équipements. Appliquez le principe du moindre privilège.

La micro-segmentation ne signifie pas qu'il faille relâcher les autres politiques de sécurité telles que les politiques de mot de passe ou les mises à jour de micrologiciels. Les capacités individuelles devront être évaluées. Ces appareils peuvent-ils prendre en charge l'authentification basée sur un certificat ? Existe-t-il un outil de gestion qui permette d'émettre et d'appliquer ces certificats ? Quels sont les flux de trafic requis ? Vous devrez peut-être obtenir ces informations auprès du fabricant, mais vous devrez également les confronter à vos propres rapports d'analyse du trafic. Si vous découvrez des équipements non conformes à la politique de l'entreprise, vous aurez besoin d'un plan de remédiation afin de les mettre en conformité, ou vous devrez mettre en place des contrôles supplémentaires.

Étape 3 : planifier

À ce stade, vous connaissez déjà les équipements, les sujets (utilisateurs), le trafic et les flux de travail. Vous devez maintenant transformer ces connaissances en politiques d'authentification et de sécurité afin de mettre en œuvre l'architecture de micro-segmentation requise. Comme mentionné précédemment, pour obtenir de meilleurs résultats, vous devriez combiner macro-segmentation et micro-segmentation. N'oubliez pas que dans la plupart des scénarios existants, vous serez limité par l'architecture déjà en place.

Pour la macro-segmentation, vous disposez de plusieurs options telles que les VLAN, VRF, VPN SPB, tunnels VXLAN ou GRE et des fonctions spéciales comme le VLAN privé. Chacune de ces options présente ses avantages et ses inconvénients et peut être utile dans différentes situations. Pour la micro-segmentation, vous devrez connaître les politiques à inclure dans le profil pour chaque type d'utilisateur ou d'appareil. Enfin, vous devrez définir comment associer les utilisateurs et les appareils à leur segment et leurs politiques. En fait, cela passe par l'authentification ou la classification, ce qui peut inclure l'empreinte numérique de l'appareil.

Idéalement, vous devriez investir dans une technologie (segmentation définie par logiciel) qui vous permet de créer des politiques d'authentification flexibles afin de pouvoir facilement mettre à jour les profils du réseau.

Nous vous suggérons de concevoir le flux d'authentification dans cet ordre :

1. Authentification par le biais de certificats 802.1x en utilisant le serveur RADIUS. L'authentification génère un enregistrement d'authentification. Ces informations peuvent être partagées avec un pare-feu.
2. Si vous ne pouvez pas authentifier l'appareil à l'aide des certificats 802.1x, vous devriez alors essayer l'authentification MAC. L'authentification MAC est loin d'être aussi sûre que la norme 802.1x, mais elle est préférable à l'absence totale d'authentification, et ce jusqu'à ce que vous soyez prêt à passer à la norme 802.1x.
3. Si aucun profil n'est renvoyé, vous pouvez tenter l'empreinte numérique, que vous pouvez également utiliser pour établir une correspondance avec un segment de profil et des règles. Cela ne génère pas d'enregistrement d'authentification ou de comptabilité mais le résultat est enregistré dans la base de données de l'inventaire des IoT.
4. Enfin, vous pouvez disposer d'une fonction « fourre-tout » par défaut au cas où des profils ne seraient pas renvoyés, ou si tout le reste échoue. Lors des premières étapes, vous devrez toujours associer l'appareil à un profil qui conduira au même segment et aux mêmes règles et enregistrera l'appareil dans la base de données d'inventaire.

La structure de ce flux doit être flexible afin que vous puissiez l'adapter au fur et à mesure de votre progression. Par exemple, vous devrez peut-être supprimer l'authentification MAC dans un premier temps et l'ajouter plus tard, après avoir obtenu la liste des adresses MAC à partir du rapport d'inventaire. Et à mesure que vous affinez le processus, vous pourriez, par exemple, modifier le segment et les règles associés au profil par défaut pour en faire des règles très restrictives n'autorisant l'accès qu'à un hôte bastion.

Vous pourriez également partager le rôle de l'appareil avec le pare-feu afin que les règles du pare-feu puissent être basées sur le rôle de l'appareil et pas seulement sur celui du sous-réseau ou de l'adresse IP. Les avantages de cette intégration sont doubles. Premièrement, le pare-feu peut appliquer des politiques rigoureuses à ces appareils IoT. Deuxièmement, les politiques de pare-feu sont désormais basées sur l'utilisateur ou le rôle et ne sont donc plus liées à un sous-réseau ou à une adresse IP, permettant ainsi une nouvelle conception et une nouvelle segmentation du réseau.

Le processus sera itératif et vous devrez l'ajuster, le régler et l'affiner à mesure que vous gagnerez en maturité dans votre utilisation de l'authentification et de la segmentation.

Étape 4 : simuler

Vous aurez beau essayer de planifier, il est peu probable que vous réussissiez lors de votre premier essai. Toute erreur dans la conception du plan d'authentification, toute omission dans la « liste des autorisations » de la politique de sécurité se traduira par la défaillance du processus métier. Vous devrez appliquer des politiques d'authentification et d'accès en mode « Fail-open ». Cela signifie que les appareils et les utilisateurs qui ne se sont pas authentifiés seront tout de même autorisés sur le réseau, et que les flux de trafic inattendus seront toujours autorisés. Mais tout cela sera consigné dans des journaux qui vous permettront d'affiner les schémas d'authentification et de politique.

Étape 5 : appliquer

Après quelques ajustements, vous ne constaterez plus d'échecs d'authentification ou de refus de flux légitimes. Vous pourrez ensuite transformer ces politiques « Fail-open » en politiques « Fail-close », ce qui signifie que les appareils indésirables seront bloqués et que les flux illégitimes seront arrêtés.

Vous devrez évidemment continuer à surveiller les appareils et flux de trafic inattendus, en répétant le cycle complet si nécessaire.

Une dernière chose

Dans le cadre de la surveillance continue, de l'enregistrement et de la mise en quarantaine, nous vous recommandons d'investir également dans un système externe de détection des intrusions (IDS). Bien qu'une série d'attaques par dénis de service distribués (DDoS) puissent être identifiées directement par le commutateur lui-même, un IDS externe est également en mesure de détecter un plus large éventail d'attaques telles que des virus ou d'autres anomalies. Vous vous souvenez peut-être qu'il y a quelques années, plusieurs caméras de vidéosurveillance avaient été infectées par le logiciel malveillant Mirai, ou encore du jour au cours duquel ces appareils avaient lancé une attaque coordonnée sur les serveurs DNS mondiaux qui a affecté des services tels que Twitter, Spotify ou Paypal. Ces attaques ne seront peut-être pas détectées par vos commutateurs, mais un IDS dédié y parviendra très certainement.

Une fois l'attaque détectée, l'IDS transmettra à votre système de gestion de réseau (NMS) les adresses IP des appareils affectés. Idéalement, votre NMS sera capable de localiser ces appareils dans sa base de données et modifiera leurs profils en un « rôle de quarantaine ».

Le « rôle de quarantaine », très restrictif, n'autorise généralement la communication qu'avec un hôte bastion de façon à permettre la restauration de l'appareil, par exemple en définissant un mot de passe fort, ou en mettant à jour son micrologiciel, entre autres.

Pourquoi ALE ?

Les solutions Alcatel-Lucent Enterprise Digital Age Networking intègrent une segmentation robuste et flexible définie par logiciel avec des politiques NAC DPI dynamiques qui permettent une évolution progressive vers une architecture Zero Trust.

Le réseau de l'ère numérique est la stratégie d'Alcatel-Lucent Enterprise qui permet aux entreprises et aux organisations d'entrer dans l'ère de la transformation numérique. Il repose sur trois piliers :

- Un réseau autonome qui connecte facilement, automatiquement et en toute sécurité les personnes, les processus, les applications et les objets. Le réseau autonome d'ALE est basé sur un portefeuille rationalisé, complété par une véritable plateforme de gestion unifiée, qui fournit des politiques de sécurité communes à l'ensemble de nos réseaux LAN et WLAN. Il procure également une souplesse de déploiement en intérieur, en extérieur ainsi que dans les environnements industriels. La gestion du réseau peut être effectuée sur site, dans le cloud ou dans le cadre d'un déploiement hybride, selon les préférences du client.
- Une intégration efficace et sécurisée de l'IoT: la segmentation permet de conserver les appareils dans leurs segments spécifiques et de minimiser le risque d'exposer l'appareil et le réseau. La segmentation de l'IoT amène les entreprises à appréhender automatiquement et en toute simplicité le comportement suspect d'un appareil et à préserver la sécurité du réseau en continu.
- L'innovation des processus métiers par l'automatisation des flux de travail : l'intégration en temps réel des paramètres utilisateurs, applications et objets IoT aux données de géolocalisation dans les plateformes de collaboration, permet de simplifier la création et le déploiement de nouveaux processus métiers et services numériques automatisés, notamment en informant les administrateurs de la sécurité et du réseau de toute violation au moment où elle se produit.

Disposez-vous d'un outil capable de créer un inventaire de l'IoT/des appareils ? Possédez-vous un outil qui vous permet de surveiller les flux d'applications ? Vos commutateurs et points d'accès sans fil actuels sont-ils prêts pour la segmentation définie par logiciel ? Si vous ne possédez pas encore ces outils, veuillez nous contacter et nous vous aiderons à les obtenir.

Les points clés

Concluons avec quelques points clés :

- Pour avoir une architecture Zero Trust véritablement efficace, vous devez utiliser à la fois la macro-segmentation et la micro-segmentation
- La mise en place d'une ZTA s'effectue en cinq étapes : surveiller, valider et évaluer, planifier, simuler et appliquer
- La ZTA basée sur la micro-segmentation repose sur trois piliers : l'authentification, avec 802.1x EAP-TLS comme norme d'excellence ; des politiques différenciées associées au rôle de l'utilisateur ou de l'appareil, qui renvoient au principe du moindre privilège ; et la surveillance continue et la mise en quarantaine
- Dans les environnements hybrides et mobiles, la micro-segmentation doit être définie par logiciel, c'est-à-dire qu'elle doit être dynamique et basée sur des politiques, et non de manière statique, sinon elle serait difficilement applicable

La migration vers une ZTA par la micro-segmentation est un processus, et il est peu probable qu'une entreprise de taille importante y parvienne en un seul cycle de mise à niveau. Mais à chaque cycle de mise à niveau, de reconception ou d'amélioration continue, vous pouvez vous rapprocher de cet objectif si vous mettez en place l'infrastructure et la conception appropriées.

Alcatel-Lucent Enterprise s'engage à développer des technologies et des solutions réseau qui aident les organisations à exploiter tout leur potentiel métier grâce à la transformation numérique.

Alcatel·Lucent Enterprise