QUANT ICT
Smart Network

Dites adieu au VPN. Pourquoi le Zero Trust est le nouveau standard

Découvrez comment le Zero Trust Network Access (ZTNA) et le Secure Service Edge (SSE) remplacent les VPN classiques : plus sûrs, plus simples et prêts pour NIS2

HPE

Pourquoi le VPN a fait son temps

Autrefois, le réseau privé virtuel (VPN) était la référence en matière d'accès sécurisé à distance. Si vous étiez en dehors du bureau, le VPN était votre passerelle pour y revenir. Le VPN créait un « tunnel » sécurisé qui acheminait le trafic de l'utilisateur via une connexion chiffrée vers le réseau de l'entreprise.

On peut le comparer aux murailles d'un château dans le lieu de travail numérique. Pendant des années, le fossé et le pont-levis (VPN + pare-feu) empêchaient les intrus d'entrer, tandis que les employés à l'intérieur circulaient librement. Et dans bien des cas, ce mur existe encore. Le problème, c'est qu'aujourd'hui, les menaces ne viennent plus seulement de l'extérieur. Les attaquants trouvent le moyen de passer au-dessus, en dessous, et même à travers ces murs.

Les limites du VPN ne sont pas uniquement techniques. Elles découlent aussi de l'évolution du travail lui-même. Les employés ne se connectent plus uniquement depuis un bureau à domicile. Ils se connectent depuis des sites clients, des espaces de coworking, des salons d'aéroport et des chambres d'hôtel. Nombre des applications qu'ils utilisent ne se trouvent même plus sur votre réseau d'entreprise. Elles sont dans le cloud, hébergées à l'autre bout du monde.

Dans le même temps, votre écosystème d'utilisateurs est devenu plus complexe. Les employés ne sont pas les seuls à avoir besoin d'un accès : des fournisseurs externes, des sous-traitants, des consultants et des partenaires doivent souvent se connecter à vos systèmes.

Cela pose un problème. Les VPN classiques n'ont jamais été conçus pour cette réalité. Ils font transiter tout le trafic par une seule passerelle, créant des goulots d'étranglement. Ils accordent un large accès réseau après une seule authentification, ce qui crée des zones d'ombres en matière de sécurité. Et ils compliquent la vie à la fois des utilisateurs et des équipes IT.

À une époque où les menaces liées aux ransomwares et au phishing ne cessent de croître, le VPN est devenu un raccourci dangereux. Avec un VPN, “une fois entré, on a accès à tout “. Il n'y a pas de contrôle granulaire, pas de vérification continue. C'est un risque majeur aujourd'hui.

La solution consiste à cesser de présumer que quiconque, ou quoi que ce soit, mérite une confiance implicite. C'est le fondement du Zero Trust.

Qu'est-ce que le Zero Trust?

Le Zero Trust n'est pas un produit que l'on achète, que l'on branche et que l'on oublie. C'est une philosophie de sécurité qui bouleverse complètement l'ancien modèle.

Si l'on reprend l'analogie avec le château fort, autrefois l'objectif était d'empêcher les intrus de franchir les murs du château. Le Zero Trust adopte une autre approche: il part du principe que les menaces sont déjà à l'intérieur du château (de l'entreprise).

- Par conséquent, le Zero Trust signifie :
- Pas de confiance implicite.
- Chaque utilisateur, appareil et application doit prouver son identité à chaque fois.
- L'accès est limité aux seules ressources nécessaires, pas plus.

C'est comme remplacer la porte unique du château par de multiples points de contrôle gardés à l'intérieur des murs. Chaque pièce a un lecteur de badge. Chaque couloir a un garde. Si un pirate compromet les identifiants d'un utilisateur, il n'obtient pas les clés du royaume. Il accède à une petite salle, surveillée.

Le Zero Trust, c'est changer d'état d'esprit. La sécurité ne consiste plus à bâtir une barrière fixe en espérant qu'elle tienne. Il s'agit de s'assurer que chaque interaction, même minime, est vérifiée et appropriée. C'est pourquoi le Zero Trust est continu par essence : il vérifie encore et encore si une connexion doit toujours être autorisée.

Zero Trust et NIS2

La directive européenne NIS2 préconise explicitement les capacités offertes par le Zero Trust. Visant à renforcer la cybersécurité dans des secteurs essentiels et importants comme l'énergie, la santé, l'industrie et le secteur public, NIS2 définit des attentes claires sur la manière dont les organisations contrôlent et surveillent les accès. Concrètement, cela implique :

- **Une visibilité sur qui accède à quoi :** la capacité de tracer et journaliser toute activité utilisateur sur les applications, systèmes et données.
- **Le principe du « moindre privilège » :** s'assurer que les utilisateurs n'obtiennent que les accès strictement nécessaires à leur rôle.
- **Une surveillance et un audit continus :** supervision permanente pour détecter les comportements suspects et prouver la conformité lors des audits.

ZTNA, SSE et SASE en termes simples

Zero Trust est le principe. Pour le rendre opérationnel, il faut des technologies qui l'appliquent. Trois acronymes clés entrent en jeu.

ZTNA – Zero Trust Network Access

Le ZTNA est le premier niveau d'application du Zero Trust. Au lieu de vous connecter à tout le réseau, il ne vous connecte qu'au service ou à l'application dont vous avez besoin. Si vous êtes un fournisseur qui doit intervenir sur le logiciel de contrôle d'une machine, le ZTNA vous octroie cet accès-là, et rien d'autre. Il fonctionne en authentifiant l'utilisateur et l'appareil, en vérifiant leur profil de sécurité, puis en créant une connexion chiffrée directe vers la ressource autorisée, sans exposer le réseau au sens large.

SSE – Secure Service Edge

Le SSE est l'ensemble de sécurité basé sur le cloud. Il inclut :

- **ZTNA** pour le contrôle d'accès au niveau des applications.
- **Secure Web Gateway (SWG)**, qui filtre et inspecte tout le trafic web pour bloquer les sites malveillants, le phishing et les téléchargements dangereux.
- **Cloud Access Security Broker (CASB)** : s'intercale entre les utilisateurs et les applications cloud (Microsoft 365, Salesforce, etc.) pour surveiller l'usage, appliquer des règles et empêcher les partages non autorisés.
- **Data Loss Prevention (DLP)** : analyse les données en mouvement et au repos pour détecter et bloquer la sortie non autorisée d'informations sensibles (données personnelles, secrets industriels, etc.).

Le SSE vise à sécuriser l'accès des utilisateurs où qu'ils se trouvent, tout en offrant aux administrateurs une visibilité et un contrôle complets. .

SASE – Secure Access Service Edge

Le SASE combine le SSE avec le SD-WAN (réseau étendu défini par logiciel). Outre la sécurité, il optimise les performances réseau entre sites, data centers et services cloud. Avec le SASE, la sécurité suit l'utilisateur : elle n'est pas liée au bureau, au pare-feu ou à la passerelle VPN.

Pourquoi changer ?
Les 6 principaux avantages

1. Bien plus sûr que le VPN

Les VPN reposent sur l'hypothèse que la frontière du réseau fait office de gardien. Mais une fois la connexion établie, l'utilisateur dispose d'un accès étendu, y compris à des systèmes dont il n'a pas besoin. Ainsi, si un pirate vole des identifiants ou exploite une faille VPN, il peut se déplacer latéralement sur le réseau, chercher des faiblesses et causer plus de dégâts.
Le ZTNA/SSE supprime cette confiance aveugle :

- **L'accès est spécifique à l'application.**
- **Les autorisations sont vérifiées en continu.**
- **Chaque session est authentifiée, autorisée et journalisée.**

La sécurité se déplace aussi du réseau vers l'utilisateur. Peu importe d'où l'utilisateur se connecte : la sécurité est intégrée à chaque requête. Pensez au VPN comme à un passe-partout du bâtiment. Le ZTNA, lui, est un badge qui n'ouvre que les pièces autorisées, et seulement tant que vous en avez besoin.

2. Accès à tout moment, en tout lieu

Pour les utilisateurs, le VPN rime souvent avec :

- **Penser à se connecter.**
- **Attendre l'établissement de la connexion sécurisée.**
- **Subir des lenteurs, car le trafic transite d'abord par le réseau de l'entreprise.**

Le ZTNA/SSE supprime ces tracas. Les connexions sont transparentes et la protection est toujours active, où que soit l'utilisateur. Les performances sont souvent meilleures, car le trafic peut être acheminé directement vers l'application (cloud) plutôt que de faire un détour par une passerelle VPN centrale.
Tant que la connexion Internet et le datacenter sont opérationnels, le service reste disponible sans action de l'utilisateur. Quand la sécurité fonctionne discrètement en arrière-plan, les gens ne s'en plaignent pas : ils travaillent. C'est exactement ce qu' assure le ZTNA.

3. Moins de complexité pour l'IT

Dans de nombreuses organisations, le parc VPN est un patchwork de clients, de versions et de configurations. Le supporter prend du temps et engendre des risques.
Le ZTNA/SSE est synonyme de simplification :

- **Une plateforme cloud unique pour toutes les politiques d'accès.**
- **Application cohérente pour tous les utilisateurs et appareils.**
- **Changements de règles instantanés sans reconfiguration des terminaux.**

Avec une politique centrale, vous appliquez les changements à l'échelle de l'organisation instantanément, sans toucher chaque client ZTNA individuellement. Ce changement allège fortement la charge opérationnelle des équipes IT et réduit les risques de mauvaises configurations.

4. Donner un accès aux tiers sans risque

L'une des sources les plus courantes d'octroi excessif d'autorisations est l'accès externe. Un prestataire doit intervenir sur un système, mais via le VPN il se retrouve avec un accès bien plus large que nécessaire. Avec le ZTNA :

- **Il se connecte via un portail sécurisé dans le navigateur.**
- **Il ne voit que ce qui le concerne.**
- **Aucun logiciel VPN à installer, aucune connexion réseau permanente**

C'est particulièrement utile pour les projets de courte durée : vous accordez et révoquez l'accès instantanément.

5. Visibilité totale, conforme aux exigences NIS2

Le VPN vous dit qui s'est connecté et combien de temps. Le ZTNA/SSE vous dit :

- **Quelles applications ont été utilisées.**
- **Quelles actions ont été effectuées.**
- **D'où l'utilisateur s'est connecté.**

Et tout cela est journalisé pour l'audit, la conformité et la réponse à un incident. Ce niveau d'information transforme la visibilité en contrôle. Sans lui, vous comptez sur la chance pour repérer les problèmes avant qu'ils n'escaladent. Avec ZTNA/SSE, vous détectez les activités suspectes en temps réel et intervenez avant qu'elles ne deviennent une brèche.

6. Pérenne et prêt pour la conformité

Le paysage des menaces continuera d'évoluer. Les réglementations comme NIS2 et le RGPD aussi. ZTNA/SSE vous prépare aux deux :

- **Principe de minimisation de l'exposition des données : les utilisateurs ne voient pas et ne téléchargent pas ce dont ils n'ont pas besoin.**
- **Prévention de la perte de données et inspection de contenu intégrées.**
- **Rapports de conformité simplifiés grâce à des rapports détaillés.**

Secteurs où le Zero Trust fait la différence

Zero Trust, SSE et SASE ne sont pas des solutions de niche. Ils répondent à des défis communs à de nombreuses organisations. Dans les secteurs couverts par NIS2, l'enjeu est encore plus élevé : une brèche n'est pas seulement une mauvaise nouvelle, elle peut aussi signifier des amendes lourdes, une perte de confiance et des arrêts coûteux. Trois situations où passer au Zero Trust change la donne :

Santé

Un médecin généraliste peut accéder à distance et en toute sécurité aux dossiers hospitaliers depuis son cabinet, sans exposer d'autres parties du réseau. L'hôpital satisfait aux exigences de NIS2 en matière de visibilité et de contrôle des accès, et les données patients restent protégées.

Industrie

Un technicien à l'étranger se connecte en toute sécurité au système de contrôle d'une ligne de production, sans toucher au reste du réseau de l'usine.

Secteur public & éducation

Le personnel et les prestataires se connectent en toute sécurité, où qu'ils soient. Les administrateurs voient et contrôlent précisément ce qui est accessible — essentiel pour la conformité dans le secteur public.

Par où commencer avec le Zero Trust

Passer au Zero Trust n'a rien d'insurmontable. Les mises en œuvre les plus réussies sont souvent celles qui commencent petit, démontrent rapidement leur valeur, puis s'étendent. Six étapes pour démarrer :

1. **Cibler les risques majeurs :** Commencez par identifier les systèmes ou données dont la compromission serait la plus dommageable.
2. **Cartographier les besoins d'accès :** déterminez précisément qui a besoin de quoi. Vous découvrirez souvent des comptes inutilisés ou des droits trop larges à clôturer immédiatement.
3. **Lancer un pilote :** déployez ZTNA/SSE sur un petit groupe. Utilisez leurs retours pour affiner les règles et processus.
4. **Rester fluide :** intégrez l'authentification SSO et la MFA pour que la sécurité ne ralentisse pas les utilisateurs.
5. **Surveiller et adapter :** exploitez la visibilité de la plateforme pour suivre l'utilisation, détecter les anomalies et affiner les règles. Le monitoring de l'expérience numérique aide l'IT à repérer les problèmes de performance avant les utilisateurs.
6. **Étendre par étapes :** une fois le pilote stabilisé, élargissez à d'autres équipes, sites et partenaires.

Rappelez-vous : le Zero Trust est un trajet, pas un projet unique. Chaque étape réduit votre surface d'attaque, améliore votre résilience et renforce votre conformité, tout en maintenant l'activité.

Pourquoi choisir Quant ICT comme partenaire ?

Le Zero Trust relève autant de l'expertise que de la technologie. Quant ICT apporte les avantages suivants :

- **Indépendance vis-à-vis des fournisseurs :** intégration ZTNA/SSE dans des environnements hétérogènes.
- **Adoption fluide :** connexion à vos systèmes d'identité existants, comme Azure AD ou Microsoft MFA.
- **Technologie éprouvée :** HPE Aruba Networking fournit l'infrastructure cloud sécurisée supporte notre solution. Cette plateforme offre l'évolutivité, la résilience et le contrôle des politiques nécessaires au Zero Trust, tout en garantissant une expérience utilisateur homogène.
- **Service continu :** avec Quant-as-a-Service, vous bénéficiez d'une surveillance, de mises à jour et d'un support permanents.

"Nous n'implémentons pas pour disparaître ensuite. Nous restons à vos côtés, nous surveillons et nous adaptons, car les menaces et vos besoins évoluent sans cesse."

Votre VPN a-t-il besoin d'être remplacé ?

Le VPN a été conçu pour une autre époque. Aujourd'hui, il peut vous ralentir, créer des zones d'ombres en matière de sécurité et ne pas répondre aux besoins de conformité. Le Zero Trust, appliqué via ZTNA/SSE, est le nouveau standard. Il vous apporte :

- **Une sécurité renforcée en limitant la confiance.**
- **Une gestion IT plus simple.**
- **Une expérience utilisateur plus fluide.**
- **Une visibilité complète pour la conformité.**

Avec Quant ICT, vous pouvez évoluer vers le Zero Trust à votre rythme : commencer à petite échelle, grandir intelligemment et garder une longueur d'avance sur les menaces.

QUANT ICT
Smart Network

QUANT ICT
Industrieweg 4 bus 5
3001 – Heverlee

www.quant.be
+ 32 16 380 840
info@quant.be