LIVRE BLANC

# Au-delà du SD-WAN : sécurité Zero Trust et Internet en tant que WAN d'entreprise

Pourquoi le SD-WAN, l'accès sécurisé et la protection contre les menaces sont étroitement liés

Akamai

## L'avenir du réseau étendu d'entreprise

Les réseaux étendus (WAN) existent depuis les années 1960, aux premiers débuts de la communication entre ordinateurs. Ils continuent à être développés et améliorés au fur et à mesure de l'évolution de la technologie et de l'augmentation des demandes de trafic. Pour les entreprises d'aujourd'hui, les réseaux WAN constituent l'infrastructure permettant d'obtenir un réseau unifié sur tous les sites.

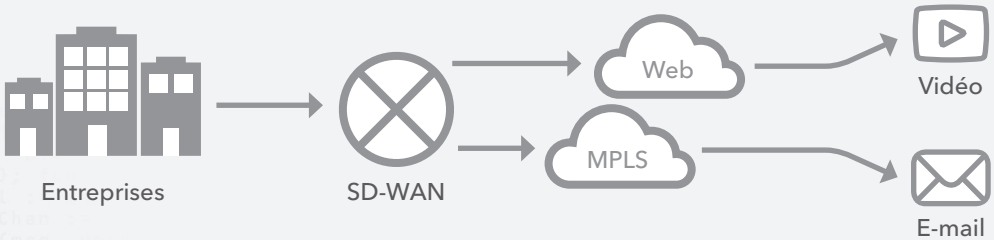
Cependant, cette sous-structure critique n'est pas sans contraintes. Les réseaux WAN fournissent souvent une bande passante faible ou insuffisante, causent des problèmes au niveau des performances d'applications spécifiques, affichent une fiabilité fluctuante et peuvent présenter un risque pour votre entreprise en matière de sécurité. En outre, les réseaux WAN sont souvent construits sur des lignes louées ou sont loués auprès de fournisseurs de services disposant d'une infrastructure qui utilise des méthodes de commutation de circuits ou de commutation de paquets, telles que le mode de transfert asynchrone (ATM) et la commutation multiprotocole par étiquette (MPLS), en plus de l'Internet public. Bien que cette dernière option soit un peu plus rentable, cela reste un statu quo très coûteux qui ne se prête pas à l'évolutivité.

## Un réseau d'entreprise en pleine transformation

En réponse à ces défis en termes de performances, de sécurité et de coûts, les entreprises adoptent des réseaux étendus à définition logicielle (SD-WAN), tout en réduisant les coûts et en favorisant l'agilité.

Émergeant de l'innovation des réseaux SDN (réseaux à définition logicielle) et NFV (virtualisation des fonctions réseau) initialement utilisés dans les centres de données, les services informatiques ont rapidement adopté cette technologie pour les réseaux destinés à connecter leurs organisations.

En d'autres termes, les réseaux SD-WAN séparent les sphères des données et du contrôle au sein du réseau étendu. Le SD-WAN surveille les performances de l'ensemble des connexions de données WAN (MPLS, ATM et Internet) et sélectionne la connexion la plus appropriée pour chaque type de trafic en fonction des performances de la liaison actuelle, du coût de la connexion et des besoins de l'application ou du service.




**SD-WAN en action**

Un réseau SD-WAN peut acheminer les e-mails via MPLS, car la latence n'est pas un problème majeur et le coût par bit envoyé est le plus faible. Inversement, le réseau SD-WAN peut acheminer le trafic de visioconférence via Internet pour garantir des performances optimales et une latence minimale, mais à un coût par bit plus élevé.

## Internet pourrait-il devenir le nouveau WAN d'entreprise ?

Les réseaux SD-WAN peuvent parfaitement être flexibles, efficaces et économiques s'ils utilisent plusieurs services de transport, y compris l'Internet public. Cependant, puisqu'il n'y a pas de garantie de performances ni de SLA pour ces options de transport, les réseaux SD-WAN utilisent Internet uniquement pour les applications dont les performances ne sont pas essentielles.

Pour augmenter l'utilisation d'Internet afin de fournir plus de trafic WAN d'entreprise de manière efficace, rentable et sécurisée (et de sorte à coexister avec les déploiements SD-WAN actuels), vous devez adopter une approche qui supprime les limites d'Internet sous-jacentes. Pour ce faire, vous pouvez utiliser une plateforme en bordure de l'Internet afin de fournir des applications professionnelles sécurisées, rapides et fiables sur le Web, sans les exposer publiquement. Cela vous permet d'optimiser votre investissement actuel dans le réseau SD-WAN tout en réduisant davantage les coûts au fur et à mesure que vous transférez plus de trafic vers Internet.

Le routage d'une plus grande partie du trafic d'entreprise vers Internet est totalement logique compte tenu de la trajectoire des réseaux d'entreprise actuels. L'augmentation des charges de travail dans le cloud, ainsi que la diversification et la mobilité des utilisateurs et des terminaux, signifient que les flux de travail dépendent déjà en grande partie d'Internet. Cette tendance continue à se développer.

Et si vous pouviez passer à l'étape suivante en établissant un réseau WAN d'entreprise sécurisé, évolutif et efficace sur Internet ?

Dans ce livre blanc, nous allons aborder les processus de transformation de votre réseau avec des solutions SD-WAN et de sécurité Zero Trust, et vous aider à positionner votre entreprise pour une évolution au-delà du SD-WAN et l'adoption d'un réseau d'entreprise entièrement basé sur Internet.

**Une plateforme en bordure de l'Internet vous permet de fournir des applications professionnelles sécurisées, rapides et fiables sur le Web, sans les exposer publiquement.**

> *D'ici la fin de l'année 2023, plus de 90 % des initiatives d'actualisation de l'infrastructure en bordure de l'Internet d'un WAN seront basées sur des plateformes virtuelles d'infrastructure client (vCPE) ou des logiciels/appliances WAN définis par logiciel (SD-WAN) plutôt que sur des routeurs traditionnels (par rapport à moins de 40 % aujourd'hui). »*
>
> *– Gartner, Magic Quadrant for WAN Edge Infrastructure, octobre 2018*

## La valeur du SD-WAN

Les avantages majeurs du SD-WAN sont l'équilibrage des liaisons, la configuration automatique des terminaux et l'insertion de services de sécurité tiers. Ces capacités peuvent avoir un impact significatif, notamment par l'amélioration de l'expérience utilisateur, la réduction des coûts de liaison et la diminution des dépenses d'exploitation. Il existe de nombreux exemples d'adoption réussie de cette technologie.

**Des dizaines de fournisseurs proposent différentes fonctionnalités SD-WAN, mais elles peuvent être généralisées en trois catégories :**

1. *Contrôle flexible des liaisons*
2. *Facilité de gestion*
3. *Insertion de services*

### Contrôle flexible des liaisons

Le contrôle flexible des liaisons est le principal avantage du SD-WAN. Puisque de nombreuses entreprises s'orientent majoritairement vers le cloud, l'acheminement du trafic via un réseau privé vers un centre de données (servant de fait de point de contrôle centralisé), n'est pas pratique. Le SD-WAN résout ce problème en utilisant le contrôle intelligent du trafic, notamment la sélection de routage dynamique. Par ailleurs, le SD-WAN établit des points de sortie Internet locaux ou de succursales qui acheminent le trafic vers le cloud au lieu de passer par un centre de données. Ce service est aussi appelé Accès direct à Internet (DIA). Ainsi, toutes les applications héritées, y compris les applications vocales et vidéo, sont envoyées sur les liaisons MPLS, tandis que les applications cloud et le trafic Internet sont directement dirigés vers Internet.

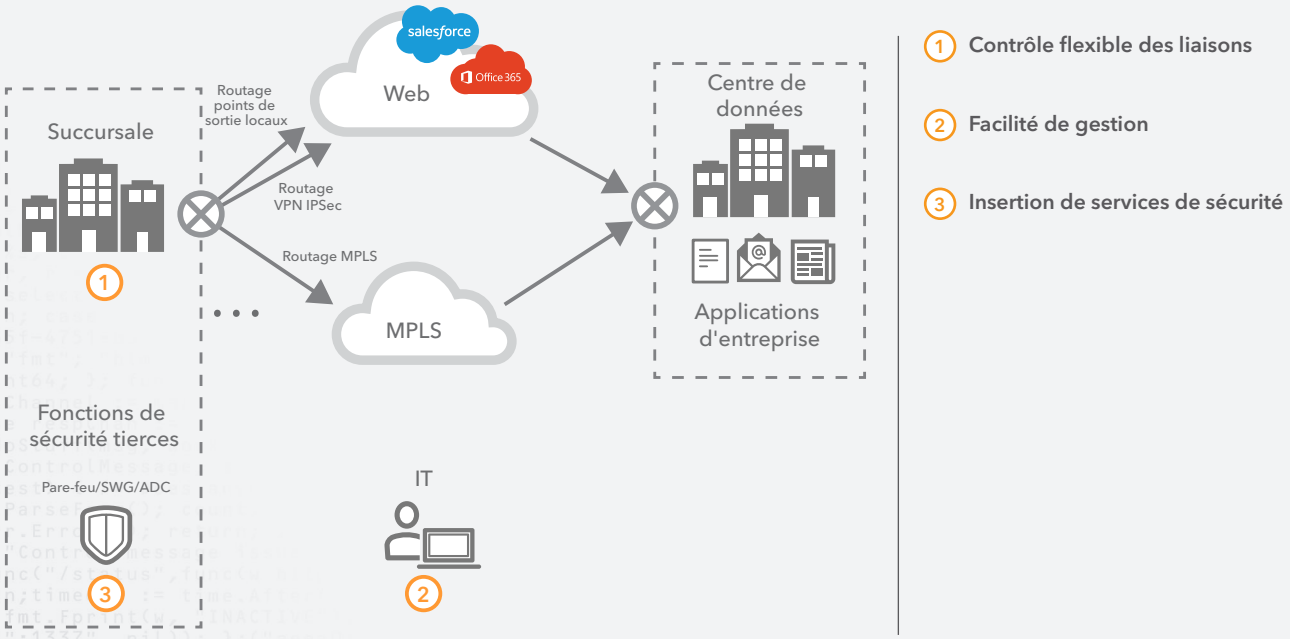
## Facilité de gestion

Les fournisseurs SD-WAN peuvent également fournir une gestion simplifiée, ce qui facilite le fonctionnement et l'administration des terminaux du réseau. Depuis les années 1990, les réseaux WAN d'entreprise se composent de terminaux de réseau, comme des commutateurs et des routeurs à plusieurs couches. Ces terminaux sont en grande partie gérés par appliance. En d'autres termes, les administrateurs doivent configurer et gérer entre plusieurs centaines et plusieurs milliers de terminaux individuellement, en surveillant les logiciels de chaque terminal, à l'échelle de l'entreprise. Même si les terminaux échangent dynamiquement des informations de routage ou permettent une haute disponibilité à l'aide de protocoles de routage, cela représente un travail colossal. Avec le SD-WAN, la gestion complète des terminaux peut être effectuée dans une console unique centralisée.

## Insertion de services

Enfin, certains fournisseurs SD-WAN se spécialisent dans l'insertion de services. L'accessibilité IP est l'exigence minimale pour un réseau étendu (WAN), à savoir la connectivité réseau de couche 3 au sein de l'entreprise. Cependant, à mesure que la mise en réseau a évolué, les fonctions de sécurité ont également subi des modifications : pare-feu, systèmes de prévention des intrusions (IPS) et contrôleurs de diffusion d'applications, pour n'en citer que quelques-unes. Avant, vous aviez besoin d'une conception de routage complexe pour ajouter ces fonctionnalités au réseau, car les terminaux qui fournissent ces services ne parvenaient généralement pas à communiquer avec les protocoles de routage dynamique (OSPF [Open Shortest Path First], BGP [Border Gateway Protocol]), ce qui entraînait une combinaison complexe de routage statique et de redistribution. Le SD-WAN facilite la configuration de ces technologies, souvent fournies par des tiers, et leur gestion via un portail unifié.

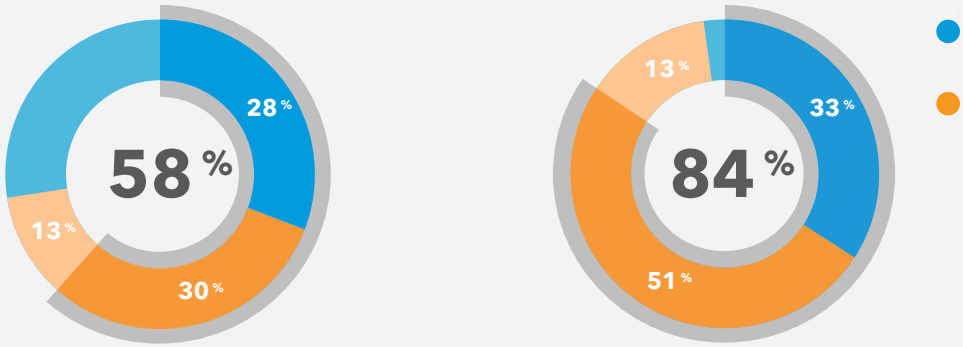
## Valeur commerciale du SD-WAN



## Un nouveau modèle : la sécurité Zero Trust

La nouvelle architecture nécessite une nouvelle sécurité. Au fur et à mesure du transfert des transactions vers le cloud et Internet, les réseaux sont devenus très distribués, ce qui génère des surfaces d'attaque supplémentaires. Les applications, les utilisateurs, les données et les terminaux ont quitté la zone de contrôle traditionnelle, faisant disparaître ce qui était autrefois le périmètre de confiance de l'entreprise. Par conséquent, la création et la mise en œuvre d'un modèle de sécurité basé sur un périmètre d'entreprise ne sont plus viables. Une stratégie de défense actuelle doit tenir compte des charges et des forces de travail distribuées d'aujourd'hui.

### Dans quelle mesure êtes-vous d'accord / n'êtes-vous pas d'accord ?




*« Le périmètre du réseau est indéfendable dans l'écosystème technologique actuel des réseaux de cloud distribués et des utilisateurs mobiles/distants. »*

*« La transformation digitale nécessite des ajustements au niveau des stratégies de sécurité traditionnelles (basées sur le périmètre). »*

Forrester Research, Build Your Zero Trust Security Strategy With Microsegmentation, septembre 2018

Un modèle de sécurité Zero Trust suppose qu'il n'existe pas de notion d'« interne » et que chaque utilisateur et chaque terminal est considéré de la même manière comme non fiable. Chaque demande d'accès nécessite une authentification et une autorisation. Les applications et les données ne sont fournies qu'après vérification et, même après celle-ci, de façon temporaire et avec une portée limitée. Cette structure de sécurité traite toutes les applications comme si elles étaient connectées à Internet et considère que le réseau est compromis et hostile. En outre, la visibilité est essentielle ; la journalisation complète et l'analyse des comportements sont incontournables.

**Les principes fondamentaux de la sécurité Zero Trust incluent les éléments suivants :**

- *Garantie que toutes les ressources font l'objet d'un accès sécurisé, quel que soit leur emplacement ou le modèle d'hébergement employé*
- *Adoption d'une stratégie de « privilège minimal » et de « refus par défaut » lors de l'exécution de l'accès aux applications*
- *Inspection et consignation du trafic (à la fois pour les applications que vous contrôlez et pour celles que vous ne contrôlez pas) afin d'identifier les activités malveillantes*

**Il existe deux principaux composants qui prennent en charge la mise en œuvre de la sécurité Zero Trust :**

- *Proxy basé sur l'identité pour un accès sécurisé aux applications*
- *Passerelle Internet sécurisée pour la protection des utilisateurs*

## Proxy basé sur l'identité pour un accès sécurisé aux applications

Si les utilisateurs, les données et les applications sont sur le cloud et si l'accès direct à Internet (DIA) permis par le réseau SD-WAN fournit la connexion, pourquoi ne pas transférer le système de sécurité et la pile DMZ également vers le cloud ? Ainsi, vous pouvez exploiter la sécurité Zero Trust pour garantir un accès sécurisé aux applications que vous contrôlez, tout en limitant les risques associés aux utilisateurs qui accèdent à des applications que vous ne contrôlez pas.

Si vous optez pour une configuration de VPN simple pour fournir un accès aux applications d'entreprise, vous risquez de procurer aux utilisateurs connectés un accès IP à la totalité de votre réseau. Ceci présente un risque très élevé et va à l'encontre des principes de la sécurité Zero Trust. Pourquoi les employés des centres d'appels devraient-ils avoir accès aux référentiels de code source ? Pourquoi un sous-traitant utilisant votre système de facturation aurait-il des droits vis-à-vis des terminaux de traitement des cartes de crédit ? L'accès ne devrait être accordé qu'aux applications nécessaires à l'exécution d'un rôle. Le VPN traditionnel n'autorise pas cet accès granulaire, et requiert plutôt une dépendance permanente par rapport à un modèle de réseau hub-and-spoke.

Une architecture de proxy basé sur l'identité (IAP) permet d'accéder aux applications via un proxy situé dans le cloud. L'identité et l'autorisation se produisent en bordure de l'Internet et sont basées sur les principes du « besoin de savoir » et du moindre privilège similaires à l'accès via des périmètres définis par logiciel (SDP), mais utilisent plutôt des protocoles HTTPS standard au niveau de la couche d'application (couche 7).

### Les deux façons dont un IAP peut fonctionner

Vous intégrez un réseau de diffusion de contenu (CDN) à des transactions à l'échelle internationale afin d'améliorer la réponse des applications

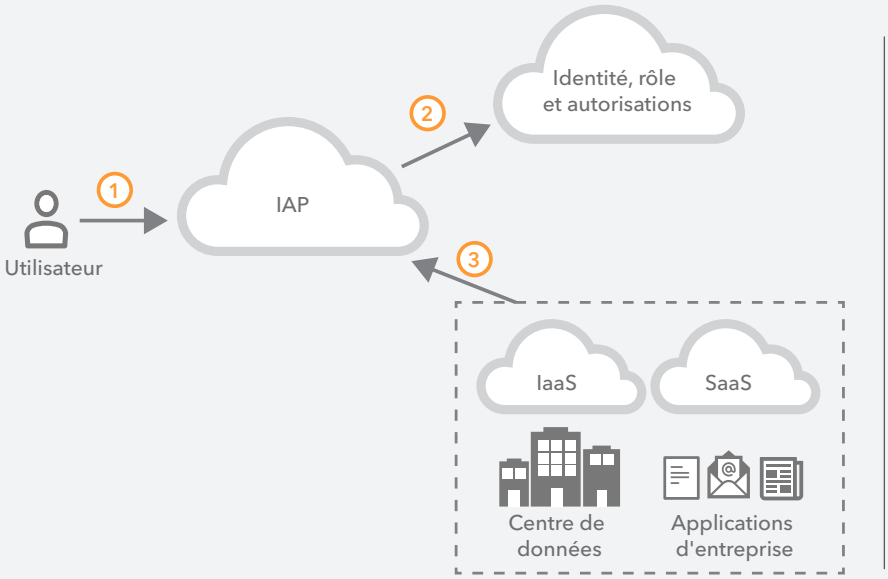
*OU*

Vous utilisez un Web Application Firewall (WAF) pour protéger les serveurs Web de l'entreprise contre les vulnérabilités courantes, telles que l'injection SQL et les scripts intersites.

Un composant clé d'un IAP est le référentiel d'identité, qui vérifie la confiance des utilisateurs et des terminaux (authentification) et ce à quoi ils peuvent accéder (autorisation). Ce référentiel d'identité peut se baser sur des répertoires d'entreprise ou des fournisseurs d'identités basés sur le cloud. Même avant la validation de l'identité d'un utilisateur, la vérification du profil d'un terminal permet de s'assurer que le terminal qui tente d'accéder répond à certains critères de sécurité, par exemple détenir un certificat, exécuter le dernier système d'exploitation, être protégé par mot de passe ou être doté de la solution de détection et de réponse des terminaux appropriée et opérationnelle.

L'IAP offre un avantage considérable par rapport aux autres technologies d'accès : non seulement les utilisateurs sont vérifiés, mais le trafic des utilisateurs est inspecté et les demandes d'application individuelles peuvent être annulées, examinées et autorisées. Lorsqu'une transaction a été interrompue sur le proxy, des services supplémentaires peuvent être intégrés, ce qui permet d'améliorer l'expérience utilisateur et la protection des applications.

## Proxy basé sur l'identité (IAP)




1. Demande d'accès
2. Confirmer l'identité, le rôle et les autorisations
3. Fournir l'accès via le proxy

L'IAP s'appuie également sur des contrôles d'accès au niveau des applications, et non sur des règles de pare-feu : les stratégies configurées peuvent refléter l'intention des utilisateurs et des applications, et pas uniquement les ports et les adresses IP. Tout comme les SDP, cette approche peut masquer les applications et autres ressources dans le cloud ou derrière le pare-feu, et ne contient aucun client pour les applications Web.

Au fur et à mesure du développement de l'adoption du cloud, le défi de la migration des applications d'entreprise s'est précisé. De nombreuses entreprises ont du mal à exploiter le cloud, aussi bien pour les applications natives du cloud que pour les applications traditionnelles. L'IAP peut être non seulement utilisé pour authentifier les utilisateurs des applications SaaS natives, mais également pour « SaaSifier » les applications héritées dans le centre de données. De plus, un proxy facilite la migration vers le cloud et la modernisation des applications sans recourir à une stratégie complète de remplacement. Les entreprises peuvent ainsi adopter une approche méthodique et progressive pour mettre en œuvre une sécurité Zero Trust tout en réduisant la dette technique associée aux contrôles du périmètre existants et aux VPN traditionnels.

## Passerelle Internet sécurisée pour la protection des utilisateurs

L'un des aspects essentiels de la transition vers un modèle de sécurité Zero Trust est de garantir la sécurité des utilisateurs lorsqu'ils accèdent à des applications que vous ne contrôlez pas. De nombreuses cybermenaces se cachent derrière chaque clic sur Internet. Auparavant, lorsque les utilisateurs étaient liés au réseau de l'entreprise et aux terminaux gérés, la protection contre les logiciels malveillants, le ransomware et l'hameçonnage se limitait au déploiement d'antivirus sur les terminaux, à l'installation d'appliances dans un centre de données, et à l'inspection et au contrôle a posteriori du trafic.

**Avec des utilisateurs répartis sur plusieurs sites, Internet devient le réseau d'entreprise de prédilection : une SIG basée sur le cloud vous offre une passerelle sécurisée pour protéger les utilisateurs de manière proactive, où qu'ils se trouvent.**

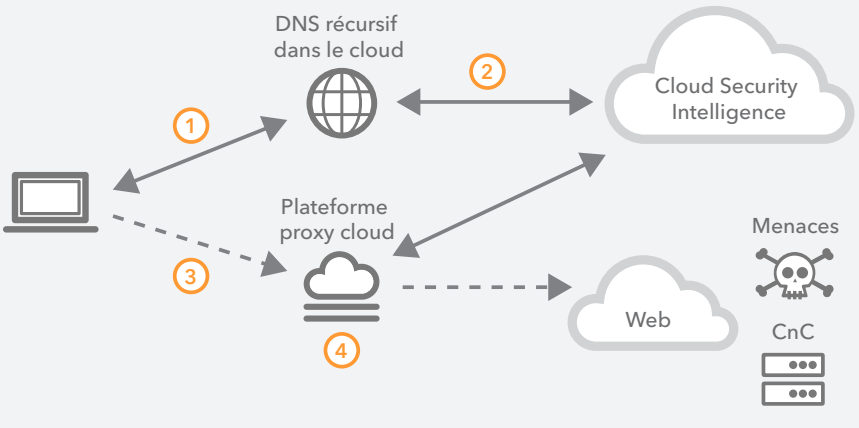
Cependant, les utilisateurs travaillent de moins en moins sur site, les terminaux ne sont plus gérés et Internet devient le réseau d'entreprise de prédilection. La connectivité DIA rend les solutions centrales de sécurité, de contrôle et d'inspection obsolètes. Une autre solution consiste à recréer la pile d'appliances de sécurité à chaque point de sortie Internet. Cependant, pour la plupart des entreprises, cette solution est vouée à l'échec, tant sur le plan logistique que financier. Et, plus important encore, la complexité inhérente à cette approche introduit des failles de sécurité, qui sont en contradiction directe avec les meilleures pratiques Zero Trust.

Utiliser une passerelle Internet sécurisée (SIG) basée sur le cloud est une méthode plus simple, plus rapide et plus rentable pour sécuriser le trafic DIA. Une SIG est une passerelle sécurisée vers Internet qui protège de manière proactive les utilisateurs, où qu'ils se trouvent, contre les menaces avancées, en autorisant le contrôle et l'inspection du trafic risqué. Pour ce faire, vous devez examiner chaque demande DNS, bloquer les requêtes vers les domaines malveillants, autoriser les requêtes vers les domaines sécurisés à se poursuivre normalement, et transmettre les requêtes concernant des domaines à risque à un proxy situé dans le cloud, pour une inspection plus poussée.

À ce stade final, lorsque le proxy reçoit une requête HTTPS, il compare l'URL demandée à une base de connaissances sur les menaces située dans le cloud, et bloque les URL malveillantes. Pour toutes les autres URL demandées et classées comme risquées, le proxy envoie le contenu Web pour analyser la charge utile en ligne via plusieurs moteurs d'analyse des programmes malveillants. Ces moteurs utilisent de nombreuses techniques de détection (signature, sans signature et apprentissage machine) pour identifier et bloquer les menaces connues et les menaces « zero day » inconnues. Grâce à plusieurs méthodes de détection, vous pouvez diriger une charge utile vers le ou les moteurs les plus adaptés en fonction du type de contenu, ce qui garantit des taux de détection optimaux et un faible taux de faux positifs.

Il est important de noter que cette approche est assez différente de l'approche adoptée par les équipements de sécurité hérités, tels que les passerelles Web sécurisées (SWG). Plus précisément, les SWG autorisent l'ensemble du trafic Internet (en inspectant aussi bien le bon trafic que le mauvais), ce qui peut être particulièrement préjudiciable aux pages Web complexes et au contenu HTTPS plus lourd. Cette approche nuit aux performances, introduit des temps de latence et augmente le volume de sites Web et d'applications interrompues résultant de cette validation par proxy de l'ensemble du trafic. Les SWG se traduisent souvent par davantage d'incidents de sécurité et de faux positifs, ce qui entraîne des demandes d'assistance et monopolise les ressources informatiques.

## Architecture Secure Internet Gateway




1. **Recherche DNS**
2. **Catégorisation du domaine comme bénin, malveillant ou suspect**
3. **Domaines suspects redirigés vers le proxy cloud**
4. **Renseignements sur les menaces URL et analyse de la charge utile**

Un proxy intelligent et sélectif peut exploiter le DNS comme point d'accès à Internet et comme première couche de sécurité. En permettant au trafic sécurisé d'accéder directement à Internet, en bloquant le trafic de mauvaise qualité et en utilisant un proxy uniquement pour le trafic risqué, cette approche offre les avantages suivants :

- *Sécurité simplifiée*
- *Réduction de la latence et amélioration des performances*
- *Moins de pages Web et d'applications interrompues*

## Transformation du réseau avec réduction des risques : mise en œuvre d'une sécurité Zero Trust dans un environnement SD-WAN

De nombreuses entreprises qui migrent vers des architectures basées sur Internet considèrent le SD-WAN comme un élément clé en raison de son contrôle des liaisons et de sa capacité à potentiellement réduire les coûts liés à la propriété MPLS. Elles peuvent utiliser des réseaux haut débit ou sans fil pour augmenter ou compléter les connexions MPLS, créant ainsi un WAN hybride. Cependant, si elles utilisent déjà la connectivité DIA, il est logique qu'elles emploient un modèle de sécurité suivant la même approche.

Au fur et à mesure de l'adoption du SD-WAN, les entreprises doivent transformer leur sécurité et passer d'une structure basée sur le périmètre à une structure Zero Trust en bordure de l'Internet. Quelle est donc notre position aujourd'hui, et qu'elle est la prochaine étape ?

**Les réseaux SD-WAN se trouvent généralement dans l'une des trois situations suivantes, en fonction de l'état d'esprit et de la stratégie à long terme de l'entreprise :**

1. *WAN privé traditionnel avec répartition centralisée : SD-WAN envisagé, mais pas encore implémenté*
2. *Mise en œuvre hybride d'un réseau WAN privé traditionnel vers des sites existants et du SD-WAN vers des succursales plus récentes*
3. *Principalement SD-WAN*

Une approche de sécurité Zero Trust peut s'adapter à tous ces scénarios. Cependant, si l'entreprise envisage ou a commencé à mettre en œuvre un réseau SD-WAN, elle a peut-être déjà adopté Internet comme un outil de réseau d'entreprise viable et est donc prête à utiliser une stratégie de sécurité Zero Trust pour son environnement réseau d'entreprise.

Examinons l'état actuel des architectures afin d'identifier la façon dont chacun peut mettre en œuvre la sécurité Zero Trust, puis passer à l'état futur souhaité.

### WAN privé traditionnel avec répartition centralisée

Si les motivations qui sous-tendent la migration SD-WAN sont le coût, l'agilité et la flexibilité (des avantages qu'une architecture réseau basée sur Internet peut apporter), il pourrait être judicieux de se passer complètement du SD-WAN et d'adopter directement une structure Zero Trust. L'IAP permet un accès aux applications basé sur l'approche Zero Trust, quel que soit leur emplacement, tandis que la SIG fournit aux utilisateurs un accès Internet sécurisé, sans que les entreprises n'aient à créer de systèmes de sécurité à chaque point de sortie Internet.

Un élément à prendre en considération : si l'entreprise prend déjà en charge des services en temps réel, tels que la VoIP et la visioconférence via un fournisseur de services cloud Internet, elle est idéalement placée pour adopter une architecture réseau et d'accès basée sur Internet. Si ces services sont toujours hébergés majoritairement sur site, il peut être envisagé de conserver un certain niveau de réseau « privé » entre les sites, qu'ils soient de nature privée (par exemple, MPLS) ou basés sur SD-WAN.

## Hybride avec WAN traditionnel et SD-WAN

Dans ce scénario, les entreprises ont déjà franchi la première étape vers une architecture basée sur Internet plus efficace.

**Dans ces environnements, il est important de comprendre comment le trafic utilisateur est géré :**

- *Les utilisateurs disposent-ils d'un accès direct à Internet depuis des bureaux distants ou la liaison Internet est-elle utilisée uniquement pour la mise en réseau vers les sites principaux ?*
- *Où les applications utilisateur principales sont-elles basées ? Sur site, dans un centre de données ou dans le cloud ?*
- *Si le cloud est utilisé, comment les utilisateurs se connectent-ils à ces applications ? Sont-elles facilitées par l'intermédiaire du DIA depuis une succursale ou les utilisateurs sont-ils acheminés vers une liaison de connexion directe ?*
- *Quelle est l'étendue de l'utilisation des applications SaaS ?*
- *En cas de DIA au niveau de la succursale, quelle est l'étendue du système de sécurité à chaque emplacement ?*

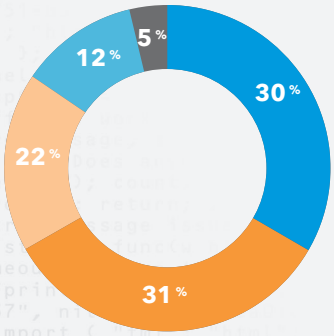
Les réponses varient naturellement en fonction du traitement du trafic utilisateur et, par conséquent, la migration du réseau aura des degrés de complexité différents. Cependant, deux constantes existent : l'utilisation d'Internet augmentera et il faudra passer de la sécurité périmétrique à un modèle Zero Trust.

Prenons l'exemple d'une connectivité DIA depuis un bureau distant. Une SIG peut offrir une protection supplémentaire au système de sécurité centralisé et remplacer une partie du système, réduisant ainsi la complexité et les coûts.

Si les utilisateurs accèdent à des applications basées sur le cloud, une approche IAP pourrait à la fois renforcer la sécurité de l'entreprise et améliorer l'expérience utilisateur. Elle pourrait également améliorer les performances des applications en permettant un accès direct aux applications sur Internet à l'aide d'un réseau de diffusion de contenu (CDN).

Vous pouvez continuer à passer d'un WAN traditionnel à un environnement SD-WAN en activant la connectivité DIA pour les bureaux distants et en adoptant les principes de sécurité Zero Trust.

### Quels sont vos plans d'entreprise pour utiliser la technologie du réseau étendu à définition logicielle (SD-WAN) aujourd'hui ?




- Utilisation actuelle
- Essai au cours de l'année prochaine
- Adoption planifiée au cours des deux prochaines années
- Utilisation envisagée, mais pas prévue
- Utilisation ni envisagée ni prévue

Forrester Research, Digital Transformation Drives Distributed Store Networks to the Breaking Point, avril 2018

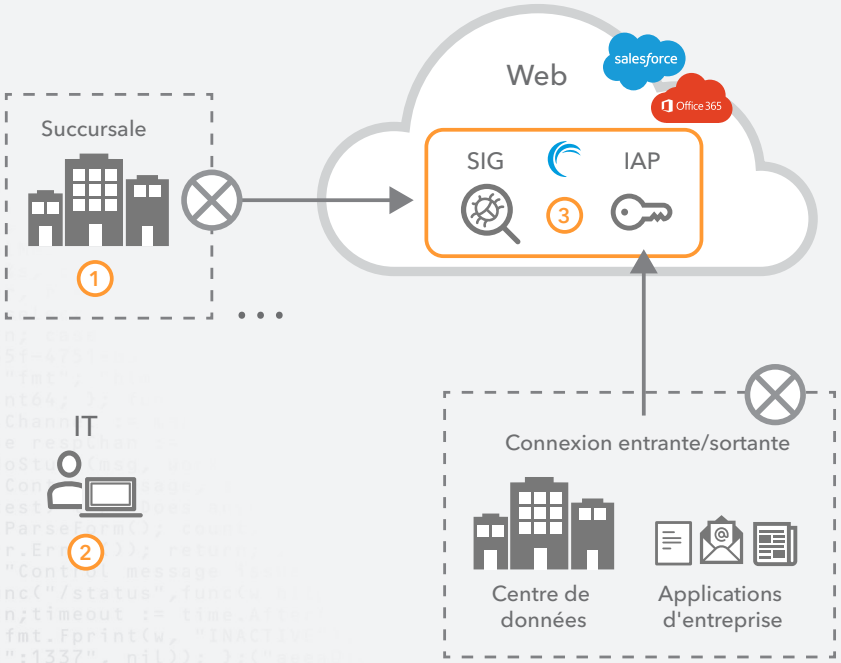
## Principalement SD-WAN

À ce stade, les entreprises ont vraisemblablement abandonné le réseau WAN privé traditionnel et utilisent un routage intelligent sur l'ensemble des liaisons Internet entre sites pour les communications inter-bureaux, exploitant pleinement les avantages du DIA. Ces entreprises s'appuient déjà sur l'accès à Internet dans la plupart des sites. Par conséquent, faire évoluer le réseau au-delà du SD-WAN est la direction logique à prendre.

Quelle est l'étape suivante ? Commencer à réduire la dépendance vis-à-vis des liaisons MPLS en déplaçant les applications vers Internet afin d'offrir flexibilité et rentabilité. Les applications d'entreprise sont accessibles via IAP, même dans un environnement DIA. Si les applications se trouvent déjà dans un environnement cloud, il n'est pas logique d'y accéder en acheminant le trafic vers un centre de données avant de le séparer au niveau d'un emplacement central (par exemple, à l'aide d'une topologie de type connexion directe).

Enfin, cet environnement est parfaitement adapté à un futur état de connectivité et d'accès basés à 100 % sur Internet, où toutes les applications d'entreprise sont accessibles via IAP, qu'elles se situent sur site ou dans le cloud. L'ensemble du trafic utilisateur peut être sécurisé via SIG. En outre, si les fournisseurs basés sur Internet fournissent des communications en temps réel, vocales ou vidéo par exemple, il est possible de supprimer complètement le réseau SD-WAN, et même le réseau WAN, de l'entreprise. Les coûts et la complexité peuvent ainsi être réduits, et la sécurité renforcée grâce à un modèle architectural Zero Trust.

### Valeur de l'architecture basée sur Internet avec un modèle de sécurité Zero Trust




1. **Accès réseau le plus simple**
   - Accès Internet uniquement
   - Pas d'accès sortant/entrant
2. **Facilité de gestion**
   - Point de gestion unique
   - Surveillance des terminaux
   - Surveillance des utilisateurs
3. **Optimisation du contrôle sécuritaire**
   - Prévention des attaques « zero-day »
   - AAA centralisé (authentification, autorisation et comptabilité)
   - Contrôle de la posture du client
   - Prévention contre le hameçonnage, les logiciels malveillants et attaques CnC

## Transformez votre entreprise

Les réalités actuelles de l'entreprise augmentent l'exposition dans un environnement qui s'accompagne déjà de risques et de complexité. Un modèle de réseau régi par des transactions en étoile sur un WAN privé est aussi obsolète que la défense de l'entreprise basée sur le périmètre : les architectures réseau et de sécurité doivent évoluer. Bien que le SD-WAN permette actuellement à un réseau d'entreprise de gérer efficacement le trafic et de déplacer les charges de travail vers le cloud, ce modèle de réseau doit continuer à perdurer. L'Internet est le WAN d'entreprise du futur proche.

Pour Akamai, l'utilisation du SD-WAN, ainsi que de services d'accès et de sécurité conformes à la norme Zero Trust, constitue la première étape de la transition vers Internet en tant que réseau d'entreprise. Associez le SD-WAN à Akamai Intelligent Edge Platform, et vous pourrez appliquer des règles d'accès et de sécurité universelles, et garantir à l'utilisateur final des expériences d'application rapides et fiables sur Internet.

Akamai peut vous aider à orienter l'évolution de votre réseau et de votre sécurité. Pour en savoir plus sur l'évaluation Zero Trust d'Akamai, contactez l'équipe chargée de votre compte Akamai. Vous recevrez des recommandations tangibles de la part de nos experts en sécurité sur la manière de commencer ou de faire progresser votre transformation Zero Trust. Vous pouvez également vous reporter à *3 moyens simples pour commencer à mettre en œuvre la sécurité Zero Trust dès aujourd'hui* pour obtenir des ressources permettant de démarrer votre transition.

Akamai sécurise et fournit des expériences digitales pour les plus grandes entreprises du monde. L'Intelligent Edge Platform d'Akamai englobe tout, de l'entreprise au cloud, afin d'offrir rapidité, agilité et sécurité à ses clients et à leurs entreprises. Les plus grandes marques mondiales comptent sur Akamai pour les aider à concrétiser leur avantage concurrentiel grâce à des solutions agiles qui développent la puissance de leurs architectures multi-cloud. Akamai place les décisions, les applications et les expériences au plus près des utilisateurs, et éloigne les attaques et les menaces. Les solutions de sécurité en périphérie, de performances Web et mobiles, d'accès professionnel et de diffusion vidéo du portefeuille d'Akamai s'appuient également sur un service client exceptionnel, des analyses et une surveillance 24 h/24 et 7 j/7, 365 jours par an. Pour savoir pourquoi les plus grandes marques internationales font confiance à Akamai, visitez www.akamai.com/fr/fr/, blogs.akamai.com/fr/, ou @Akamai_FR sur Twitter. Vous trouverez nos coordonnées dans le monde entier à l'adresse www.akamai.com/fr/fr/locations.jsp. Publication : 06/19.