netskope

APERÇU DE LA SOLUTION

Proxy web et cloud de nouvelle génération

Fournit les fonctionnalités de proxy de nouvelle génération (Next Gen SWG) pour stopper les malwares, détecter les menaces avancées, filtrer les sites web par catégorie, protéger les données et contrôler les applis et les services cloud pour tous les utilisateurs, lieux d'accès et appareils. Un proxy inline à passage unique pour sa capacité à décoder le trafic du cloud et du web, y compris les instances et les activités.

APERÇU

- Contrôles granulaires du trafic web et cloud, y compris les instances, les activités et les données
- Protection avancée des données et contre les menaces en un seul passage, avec détection des comportements anormaux
- Une seule console avec contrôles partagés des politiques pour le proxy, le Cloud/SaaS et la DLP
- Un proxy inline mature qui protège des entreprises du Fortune 100 depuis plus de 8 ans
- Performances cloud et accessibilité mondiale permettant de protéger tous les utilisateurs et tous les appareils, où qu'ils soient

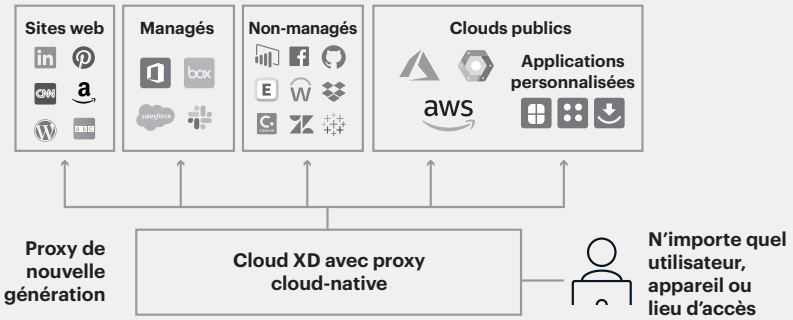
Les entreprises utilisent en moyenne 2 415 applis cloud dont 98 % sont non-managées, et 89 % des utilisateurs travaillent dans le Cloud.

LE PAYSAGE DE LA SÉCURITÉ WEB ÉVOLUE

Aujourd'hui, les entreprises utilisent en moyenne 2 415 applis web et 89 % de leurs utilisateurs travaillent dans le Cloud[1]. Plus de 98 % de ces applis ne sont pas-managées et échappent à la protection traditionnelle par API. Ce n'est pas le cas avec le proxy de nouvelle génération de Netskope qui analyse des milliers d'applis cloud en temps-réel. Les menaces liées au Cloud sont présentes tout le long de la kill chain et représentent 61% des téléchargements de malwares en 2021[2], principalement à partir d'applis de stockage cloud. Le SaaS est devenu la première cible d'attaques qui utilisent des domaines de confiance et des certificats valides pour éviter les dispositifs de sécurité traditionnels, et dont la tâche est souvent facilitée par le whitelisting.

Avec l'adoption du Cloud, certains mouvements de données échappent aux défenses web traditionnelles ; soit par manque de visibilité ou en raison de contrôles sommaires Autoriser/Bloquer sans compréhension du contexte. Les données peuvent se déplacer entre instances personnelles et professionnelles d'applications cloud, entre applications cloud managées et non-managées, et entre applications à faible risque et à risque élevé qui ne devraient pas être utilisées. En plus d'identifier les instances, il s'agit de pouvoir comprendre les activités et les anomalies associées, ainsi que le contenu lui-même et le contexte général. Inscrite au cœur de l'architecture Secure Access Service Edge (SASE), le proxy de nouvelle génération fournit le contexte des données ainsi qu'un contrôle granulaire des politiques pour le trafic cloud et web.

[1] Netskope Cloud & Threat Report 2020
[2] Netskope Cloud & Threat Report 2021



Le proxy de nouvelle génération sécurise le Web et le Cloud

- Accès aux sites web et aux URL
- Applis cloud managées et personnalisées
- Des milliers d'applis cloud non-managées
- Clouds publics
- Appareils managés et BYOD
- Contexte de données pour le SASE
- Métadonnées pour alimenter l'apprentissage automatique

CONTRÔLES GRANULAIRES DES POLITIQUES AVEC CLOUD XD

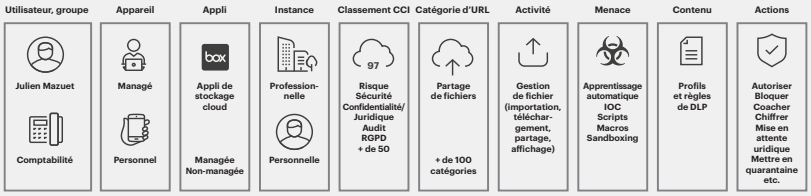
Les sites web dynamiques d'aujourd'hui reposent sur le même langage que les applications et services cloud. Pouvoir décoder ce langage est une capacité essentielle pour les solutions de proxy de nouvelle génération – pour la visibilité à la fois des menaces liées au cloud et des mouvements de données sensibles dans le cloud. Le transit de données au sein d'applications non-managées encourage l'adoption de solutions proxy cloud capables de sécuriser tous les utilisateurs et tous les appareils, où qu'ils soient. Cette tendance entraîne à son tour la convergence de fonctionnalités proxy, cloud/SaaS inline et DLP permettant ensemble une protection sophistiquée des données et la détection des menaces pour le trafic cloud et web.

Les outils de sécurité web traditionnelles (« Autoriser » ou « Bloquer ») sont remplacées par des contrôles détaillés des politiques permettant ainsi une compréhension du contenu et du contexte de l'utilisateur, appli, instance, classement des risques, données et activité. Une activité impliquant des données confidentielles dans une instance professionnelle d'une application n'a rien de suspect. Mais la même activité au sein d'une instance personnelle pourrait indiquer une fuite ou un vol de données par un employé sur le point de quitter l'entreprise.

DÉFINIR LA NOUVELLE GÉNÉRATION DES PROXY

Tenter de relever les défis de sécurité à l'aide de défenses traditionnelles entraîne de nombreuses lacunes. Une solution associant un proxy traditionnel axé sur le trafic web et un CASB offrant la protection par API des applications cloud managées peut sembler complète. Pourtant, cette solution passera à côté des milliers d'applications cloud non-managées adoptées par les entreprises et leurs utilisateurs dans le cadre de leur transformation numérique. En ajoutant des contrôles Accepter/Bloquer à ces applications cloud avec un proxy traditionnel ou en utilisant un pare-feu de nouvelle génération (NGFW) qui les place sur liste blanche, vous passez à côté des déplacements de données, des menaces cloud et du contexte. Et même en utilisant des Risk Ratings pour bloquer les applis à haut risque ou en encourageant les utilisateurs à utiliser des alternatives plus sécurisées, il suffit là encore d'« autoriser » certaines applis cloud. Les activités, le contenu et le contexte resteront perdus. En réalité, les proxy traditionnels, les NGFW et même les solutions de protection des endpoints perdent de la visibilité en raison de l'adoption du Cloud et de la mobilité. Ils ne seront plus aussi efficaces.

Les données et le contexte sont la pierre angulaire des proxy de nouvelle génération et un pilier de l'architecture SASE, et ce pour de nombreuses raisons. Aujourd'hui, de plus en plus d'utilisateurs et de données se trouvent hors du périmètre des data centers. Pour cette raison, l'avenir repose sur la DLP dans le cloud. Chaque jour, les utilisateurs accèdent aux Web, à des applis managées et non-managées, à des Clouds publics et à des applis cloud publiques. Ces cinq destinations voient toutes transiter des données que les règles et politiques de DLP cloud inline sont en mesure de protéger. Par ailleurs, les menaces liées au Cloud sont désormais présentes à toutes les étapes de la kill chain, et des méthodes comme le cloud phishing compromettent les accès et échappent aux dispositifs de défense traditionnels, y compris les défenses au niveau des end-points. Le proxy de nouvelle génération va au-delà des journaux web traditionnels : elle fournit de riches métadonnées qui alimentent la détection des anomalies (menaces et comportements) par l'apprentissage automatique du trafic web et cloud.



Julien du service comptabilité – ordinateur de bureau – utilise une instance personnelle Box – importation de fichiers – vérification DLP – coacher si PCI, PII, etc.
Julien du service comptabilité – ordinateur de bureau – utilise une instance professionnelle Box – importation de fichiers – recherche de logiciels malveillants/menaces
Julien du service comptabilité – mobile – utilise une instance professionnelle Box – téléchargement de fichiers – mode lecture seule
Julien du service comptabilité – ordinateur de bureau – visite un site web de jeux d'argent – bloquer le site – coacher l'utilisateur avec une alerte AUP

Cloud XD offre un contexte de politique détaillé

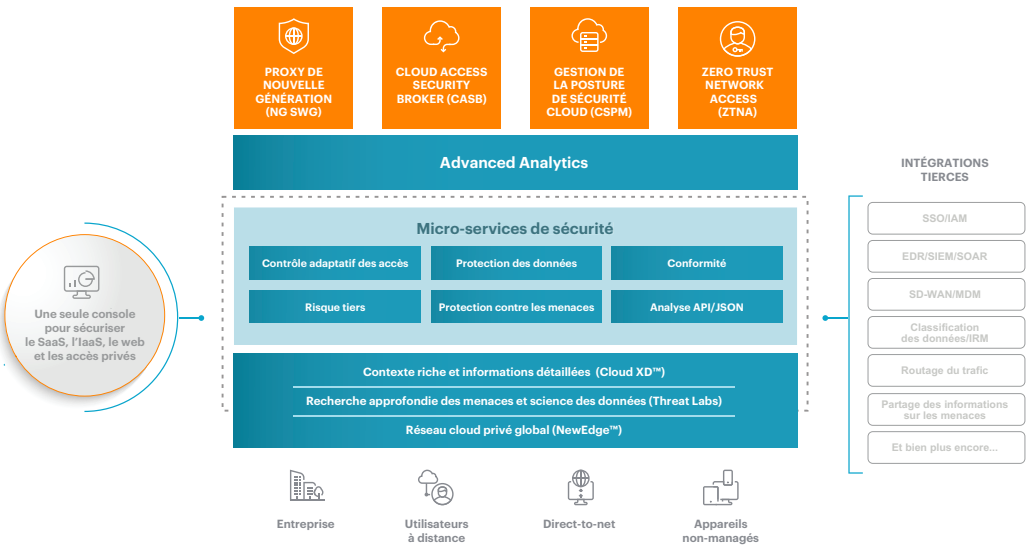
- Utilisateur, groupe ou unité organisationnelle
- Appareil managé ou personnel
- URL, appli, catégorie et classement des risques
- Instance professionnelle ou personnelle
- Activité et contenu pour le contexte
- Protection avancée contre les menaces
- Règles et politiques de DLP avancées
- Menaces internes et comportements anormaux

CONTRÔLES GRANULAIRES, MÉTADONNÉES ET DÉTECTION DES COMPORTEMENTS ANORMAUX

Dans un monde idéal, la prévention règlerait tous les problèmes. Mais dans la réalité, les équipes de sécurité doivent détecter et gérer les menaces, et mettre en œuvre de nouvelles mesures de manière rétrospective. Pour ce faire, elles ont besoin des métadonnées portant sur le trafic web et cloud (applis, instances, données et activités) fournies par les proxy de nouvelle génération. Ces métadonnées alimentent aussi l'apprentissage automatique afin de détecter les menaces avancées et les comportements suspects, y compris les menaces internes et les comptes compromis. Les actions Autoriser/Bloquer ne font plus l'affaire. La solution ? « Autoriser » grâce à des contrôles granulaires, et la collecte de métadonnées riches permettant de développer des bases de référence pour ensuite détecter des anomalies avec l'apprentissage automatique, ainsi que de lancer des procédures d'enquête et de correction. Les proxy de nouvelle génération rendent transparents le trafic web et cloud et ce pour les données et leur contexte, une caractéristique indispensable, mais impossible de voir pour les proxy traditionnels.

LA FLEXIBILITÉ DE RENFORCER VOTRE ARCHITECTURE SASE

Le changement prend du temps, et la solidité d'une architecture se construit depuis ses fondations. Le proxy de Netskope repose sur une architecture cloud-native, avec des micro-services évolutifs permettant d'adopter des capacités de sécurité supplémentaires à mesure qu'avance votre transformation. En associant Netskope Private Access au proxy de nouvelle génération, vous obtenez une solution complète qui couvre les cinq destinations citées plus haut. En complément, le Zero Trust Network Access (ZTNA) offre un accès sécurisé aux applis privées situées dans les data centers et le cloud public. Les options de protection contre les menaces incluent des analyses standard, avancées et comportementales. Pour la Data Loss Prevention (DLP), il existe des options standard et avancées. Ces défenses et politiques courantes peuvent aussi être appliquées à l'analyse CASB par API des applis cloud managées ainsi qu'à la gestion de la posture de sécurité cloud (CSPM) pour les Clouds publics, le tout à partir d'une seule console.



La plateforme de microservices cloud-native de Netskope couvre de nombreuses fonctionnalités au sein de votre architecture SASE, et vous offre un contexte de données riche et des contrôles de politiques granulaires.

FORMULES DE PROXY DE NOUVELLE GÉNÉRATION DE NETSKOPE	PROFESSIONNELLE	ENTREPRISES
PLATEFORME DE SÉCURITÉ CLOUD		
Réseau global NewEdge – réseau privé à très haute performance, de niveau opérateur, ultra-rapide et interconnecté avec les principaux fournisseurs de services cloud, offrant une couverture mondiale de data centers	O	O
Redirection du trafic – un seul client pour le Web, le Cloud, les applications de bureau, les applications mobiles et les clients de synchronisation, ou prise en charge des tunnels IPsec/GRE pour le trafic sur site	O	O
Forward et reverse-proxy – prend en charge des appareils managés avec client vers le Cloud et le Web, ainsi que les appareils non-managés sans client (par ex. le BYOD) vers des applications cloud gérées	O	O
Cloud XD – offre de la visibilité sur le contenu et le contexte dans des milliers d'applications cloud, y compris sur les activités et les instances, pour déterminer des contrôles de politiques granulaires	O	O
Authentification – de nombreuses solutions SSO/MFA/IAM, SAML, AD et LDAP	O	O
Inspection TLS – prise en charge native de la TLS v1.3 et des exclusions par les contrôles de politiques	O	O
Reporting et SkopeIT – reposant sur 90 jours de sauvegarde de données, plus long selon contrat, rapports standard et requêtes ponctuelles portant sur l'ensemble de l'utilisation web et cloud. En plus : export de données et API ouverte permettant l'intégration avec des solutions tierces	O	O
Advanced Analytics – une plateforme de BI et d'analyse de big data fournissant des tableaux de bord prédéfinis, des personnalisations et des outils de recherche riches pour plus de 500 attributs de métadonnées couvrant 13 mois d'activité web et cloud	En option	En option
Cloud Threat Exchange – partage bidirectionnel des indicateurs de compromission (IOC) depuis et vers la pile de sécurité et nœuds d'extrémité, avec intégrations clé en main pour vos solutions EPP, SIEM et IR, ou autre intégration de votre création	O	O
SERVICES DE SÉCURITÉ CLOUD		
Cloud Confidence Index (CCI) – classement des risques pour les applications et services cloud avec une base de données de plus de 33 000 entrées ; coaching utilisateurs pour les encourager à utiliser des alternatives plus sécurisées à l'aide de contrôles de politiques	O	O
Filtrage des URL – plus de 120 catégories, les langues de plus de 200 pays, des catégories personnalisées ou spécifiques à YouTube, des services de traduction, un outil de recherche sécurisé, le blocage silencieux des publicités, le classement dynamique des pages web non-évaluées, un outil d'examen des sites, un service de reclassification, et l'analyse du trafic par catégorie ou domaine	O	O
Protection standard contre les menaces – solutions anti-malware, protection contre l'exfiltration du trafic client, analyse permettant de déterminer le véritable type d'un fichier, plus de 40 flux d'informations sur les menaces, analyse statique inline reposant sur l'apprentissage automatique de fichiers PE (Portable Executable), et règles de détection des anomalies séquentielles par UEBA	O	O
Protection avancée contre les menaces – décapsulation récursive de code sur plus de 350 types de programmes d'installation, de packageurs, et de compresseurs. Analyse et heuristique pré-exécution de plus de 3 500 types de formats de fichier, et plus de 3 000 identificateurs de menaces via des indicateurs de risques statiques et binaires. Sandboxing multi-étapes pour plus de 30 types de fichiers, y compris les fichiers exécutables, les scripts et les documents. Nombreux modèles et moteurs d'apprentissage automatique managés par Netskope, et forward-proxy chaining pour le sandboxing tiers ou le RBI		O
Analyses comportementales – modèles UEBA reposant sur l'apprentissage automatique pour détecter les menaces internes, les comptes compromis et les exfiltrations de données, règles de détection des anomalies séquentielles par UEBA personnalisé, indice de confiance des utilisateurs, chronologie de corrélation des événements, et actions déclenchées par les scores des utilisateurs		O
Isolation ciblée de navigateur à distance (RBI) – rendus pixel pour les sites web non-catégorisés et présentant un risque de sécurité, pour sécuriser l'expérience web des utilisateurs quels que soient le navigateur et le système d'exploitation	En option	En option
Protection standard des données (DLP) – analyse des données en mouvement pour les applications et services cloud, et analyse du trafic web, des fichiers et des formulaires. Inclut plus de 40 modèles de conformité aux réglementations en vigueur (RGPD, PCI, PHI, code source, etc.) Exploite plus de 3 000 identificateurs de données pour plus de 1 500 types de fichiers, le regex personnalisé, des schémas et des dictionnaires. En plus : inclut désormais la classification de documents standard par apprentissage automatique (par ex : CV)	O	O
Protection avancée des données (DLP) – inclut le fingerprinting des dossiers avec degré de similitude et correspondance exacte des données inline. En plus : inclut désormais la classification des documents (par ex. : brevets, codes sources, formulaires fiscaux) et des images (captures d'écran, permis de conduire, cartes d'identité, passeports) par apprentissage automatique inline		O

Netskope propose aussi une formule « SWG Standard » dédiée au routage du trafic web, lequel inclut le filtrage des URL et une protection standard contre les menaces, ainsi qu'une solution « Web Inline » qui offre uniquement le filtrage des URL.

netskope

Netskope Security Cloud offre une visibilité sans pareille ainsi qu'une détection des menaces et une protection des données en temps réel où que vous soyez et depuis n'importe quel périphérique. Seul Netskope comprend le Cloud et adopte une approche centrée sur les données pour offrir aux équipes de sécurité le juste équilibre entre protection et rapidité dont elles ont besoin pour sécuriser leur transformation numérique. Réimaginez votre périmètre avec Netskope.