CLOUDFLARE

LIVRE BLANC

Guide de l'architecture Zero Trust

Découvrez les étapes à suivre, les outils et les équipes dont vous avez besoin pour transformer votre réseau et moderniser votre sécurité

Contenu

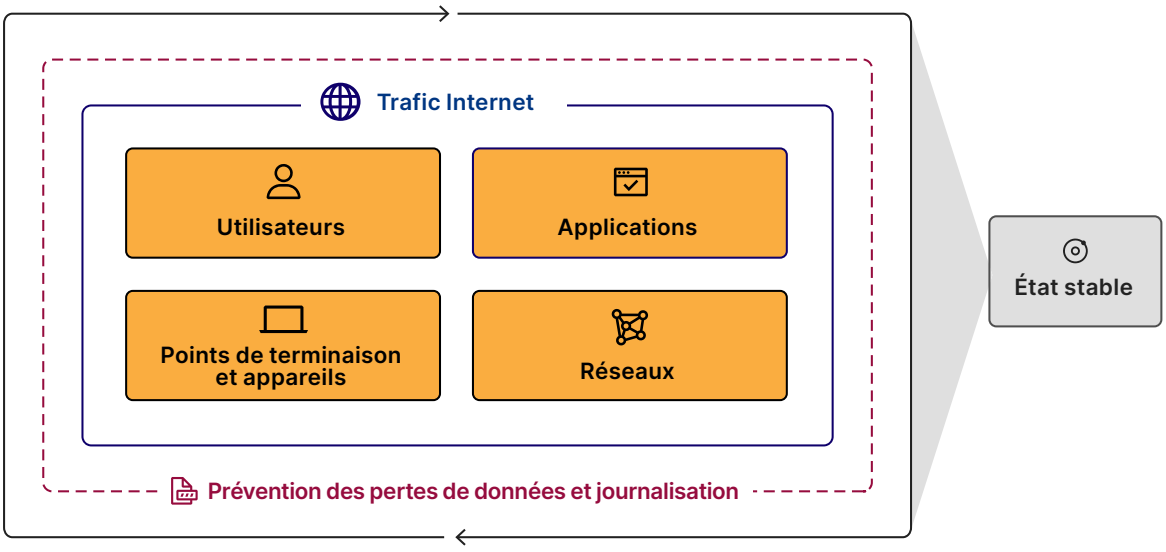
Introduction

L'architecture réseau traditionnelle était construite autour du concept de réseau périmétrique, un modèle qui accorde un niveau de confiance implicite à tous les utilisateurs une fois ces derniers inscrits sur le réseau. Le passage à l'hébergement cloud, au télétravail et aux autres formes de modernisation a engendré plusieurs difficultés autour de cette idée d'architecture réseau périmétrique traditionnelle.

Ces défis peuvent être résolus par la mise en œuvre d'une architecture Zero Trust, capable de s'assurer que l'ensemble du trafic entrant et sortant de votre entreprise est bien vérifié et autorisé. La mise en œuvre d'une architecture Zero Trust peut s'effectuer par étapes, sans perturber la productivité et la connectivité de vos collaborateurs.

Ce guide a été rédigé par des experts de la sécurité afin de vous proposer une architecture Zero Trust agnostique en termes de fournisseurs et un exemple de calendrier de mise en œuvre. Ce dernier part du principe qu'une entreprise commence son parcours Zero Trust depuis le tout début, mais se veut un outil utile pour toutes les entreprises.

La sécurité organisationnelle se divise en sept composants principaux à prendre en compte lors de la mise en œuvre d'une architecture Zero Trust exhaustive. L'ordre dans lequel vous les déployez n'a pas besoin de respecter l'arrangement présenté dans les sections consacrées aux composants et à l'architecture de référence ci-dessous.



Les composants d'une architecture Zero Trust

	Composant		Objectif	Level of Effort	Page
Phase 1		**Trafic Internet**	Déployer le filtrage DNS à l'échelle mondiale	▮	9
		Applications	Surveiller les e-mails entrants et filtrer les tentatives de phishing	▮	13
		DLP et journaux	Identifier les mauvaises configurations et les données partagées publiquement dans les outils SaaS	▮	20
Phase 2		**Utilisateurs**	Établir une identité d'entreprise	▮▮	5
		Utilisateurs	Appliquer une MFA de base pour toutes les applications	▮	6
		Applications	Appliquer le HTTPS et les DNSSEC	▮	17
		Trafic Internet	Bloquer ou isoler les menaces dissimulées derrière le SSL	▮▮	9-10
		Applications	Application de politiques Zero Trust pour les applications publiquement adressables	▮	14-16
		Applications	Protéger les applications contre les attaques sur la couche 7	▮	16
		Réseaux	Fermer tous les ports entrants ouverts sur Internet à des fins de distribution des applications	▮	12
Phase 3		**Applications**	Dresser l'inventaire de toutes les applications d'entreprise	▮▮	13-14
		Applications	Application de politiques Zero Trust pour les applications SaaS	▮▮	14-16
		Réseaux	Segmenter l'accès réseau des utilisateurs	▮▮▮	11
		Applications	Accès réseau Zero Trust pour les applications adressables de manière privée	▮	14-16
		Appareils	Mettre en œuvre une solution de MDM/UEM afin de contrôler les appareils d'entreprise	▮▮	7
		DLP et journaux	Définir les données sensibles et l'endroit où elles résident	▮▮	18-19
		Utilisateurs	Envoyer des jetons d'authentification basés sur le matériel	▮▮	6
		DLP et journaux	Se tenir à jour des acteurs malveillants connus	▮	21
Phase 4		**Utilisateurs**	Appliquer une MFA basée sur des jetons physiques	▮▮	6
		Applications	Application de politiques et accès réseau Zero Trust pour toutes les applications	▮▮▮	14-16
		DLP et journaux	Établir un SOC à des fins d'examen des journaux, de mise à jour des politiques et d'atténuation	▮▮	20
		Appareils	Mettre en œuvre la protection des points de terminaison	▮▮	7
		Appareils	Dresser l'inventaire de tous les appareils, API et services de l'entreprise	▮	8
		Réseaux	Utiliser une liaison Internet à large bande à des fins de connectivité entre bureaux régionaux	▮▮▮	11-12
		DLP et journaux	Journaliser et examiner l'activité des collaborateurs sur les applications sensibles	▮▮	18
		DLP et journaux	Empêcher les données sensibles de quitter vos applications	▮▮▮	19
		État stable	Approche DevOps en matière d'application des politiques régissant les nouvelles ressources	▮▮	22
		État stable	Mettre en œuvre l'évolution automatique des ressources en accès direct	▮▮▮	22-23

La liste ci-dessous décrit la manière dont nous définissons les différents niveaux d'effort requis pour chaque étape :

- ▮ **- Effort minime :** cette opération peut être effectuée par un utilisateur individuel ou une petite équipe.
- ▮▮ **- Effort moyen :** cette opération nécessite une équipe et une préparation avancée.
- ▮▮▮ **- Effort important :** cette opération nécessite plusieurs équipes et un plan de projet.

Le guide de l'architecture Zero Trust

Utilisateurs

La catégorie des utilisateurs englobe les employés, les sous-traitants et les clients. Pour mettre en œuvre le Zero Trust, une entreprise doit tout d'abord disposer d'une image précise des utilisateurs auxquels accorder sa confiance et des éléments sur lesquels leur accorder cette dernière. Cette représentation est également connue sous le nom d'identité. L'entreprise doit ensuite établir un moyen d'authentifier l'identité de ses utilisateurs de manière sécurisée.

Établir une identité d'entreprise

Niveau d'effort	**- Effort moyen**
Équipe(s) impliquée(s)	• L'équipe responsable de votre fournisseur d'identité (en général le service de sécurité ou le service informatique) • Les administrateurs qui gèrent les applications internes utilisées par les collaborateurs et les partenaires
Produit(s)	Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin
Résumé	Une identité d'entreprise unifiée est nécessaire pour authentifier avec précision et autoriser l'accès des utilisateurs aux applications professionnelles. Une identité d'entreprise cohérente permettra de fluidifier la mise en œuvre précise des politiques pour vos applications. Points supplémentaires à prendre en compte : • Votre entreprise est-elle en cours de fusion-acquisition ? Comment comptez-vous consolider les banques d'identité ? • Utilisez-vous des protocoles d'authentification non web (p. ex. Active Directory, ntlm, Kerberos) ?
Étapes à suivre	1. Ajoutez tous les utilisateurs de l'entreprise au fournisseur d'identité. a. Ces valeurs peuvent souvent être synchronisées à partir d'un système de RH, comme Workday, ADP, etc. 2. Vérifiez l'exactitude des informations de chaque utilisateur. 3. Envoyez des instructions d'inscription aux nouveaux utilisateurs afin de définir des identifiants de connexion.

Appliquer l'authentification multifacteurs pour toutes les applications

Niveau d'effort	▮ - **Effort minime** (en cas d'application d'une MFA de base ▮▮ - **Effort moyen** (en cas d'utilisation de clés physiques)
Équipe(s) impliquée(s)	• L'équipe responsable de votre fournisseur d'identité (en général le service de sécurité ou le service informatique) • Les administrateurs qui gèrent les applications internes utilisées par les collaborateurs et les partenaires
Produit(s)	**Fournisseurs d'identité :** Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin **Proxys inverses pour applications :** Microsoft Azure AD App Proxy, Akamai EAA, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA) **Clés physiques :** Yubico
Résumé	L'authentification multifacteurs (MFA, Multi-Factor Authentication) constitue la meilleure protection contre les identifiants utilisateur dérobés lors d'attaques par phishing ou de fuites de données. La plupart des solutions de MFA peuvent être activées directement au niveau du fournisseur d'identité (IdP, Identity Provider). Pour les applications qui ne s'intègrent pas directement à votre IdP, vous pouvez envisager de déployer un proxy inverse pour applications en amont de l'application devant mettre en œuvre la MFA.
Étapes à suivre	1. Prévenez les utilisateurs internes de la mise en œuvre de la MFA. Proposez des options d'inscription aux solutions d'authentification par SMS ou basées sur une application. 2. Activez la MFA au niveau de votre fournisseur d'identité. 3. Activez le proxy inverse pour applications en amont des applications non intégrées à votre IdP. 4. (Bonus) Distribuez des clés physiques à vos collaborateurs par courrier postal ou en personne. 5. (Bonus) Appliquez la MFA par clé physique uniquement pour vos applications les plus sensibles.

Points de terminaison et appareils

La catégorie des points de terminaison et des appareils inclut l'ensemble des appareils, API ou services logiciels utilisés au sein d'une entreprise ou disposant d'un accès à des données organisationnelles. Les entreprises doivent tout d'abord dresser un inventaire précis de l'intégralité des appareils, API et services dont elles se servent, avant de mettre en œuvre des politiques Zero Trust basées sur le contexte de l'appareil, de l'API ou du service.

Mettre en œuvre la gestion des appareils mobiles

Niveau d'effort	**- Effort moyen**
Équipe(s) impliquée(s)	• Équipe informatique
Produit(s)	**Mac:** Jamf, Kandji **Windows:** Microsoft Intune
Résumé	La majorité des architectures Zero Trust nécessitent l'installation d'un élément logiciel sur au moins un sous-ensemble de machines utilisateur. La plupart des entreprises s'appuient sur une solution de gestion des appareils mobiles (MDM, Mobile Device Management) pour gérer ce logiciel et sa configuration sur leur parc d'appareils.
Étapes à suivre	Consultez le site web du fournisseur de MDM pour les détails spécifiques.

Mettre en œuvre la protection des points de terminaison

Niveau d'effort	**- Effort moyen**
Équipe(s) impliquée(s)	• Équipe de sécurité • Équipe informatique
Produit(s)	VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender
Résumé	Un logiciel de protection des points de terminaison est installé sur la machine d'un utilisateur et analyse cette dernière à la recherche de menaces connues, capables d'affecter les appareils. Ce logiciel peut également servir à assurer la conformité des correctifs et des mises à jour des systèmes d'exploitation. Le signal émis par votre logiciel de protection des points de terminaison peut (et doit) être utilisé dans vos politiques de contrôle des accès aux applications.
Étapes à suivre	1. Installez le logiciel de protection des points de terminaison sur les machines des utilisateurs à l'aide d'une solution MDM. 2. Activez la protection contre les menaces et le contrôle de la conformité au niveau de la plateforme de protection des points de terminaison.

Dresser l'inventaire des appareils, API et services de l'entreprise

Niveau d'effort	**- Effort minime**
Équipe(s) impliquée(s)	• Équipe de sécurité • Équipe informatique
Produit(s)	**Parc d'appareils :** VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender, Oomnitza **Parc d'API/services :** Cloudflare application connector, Zscaler Private Access (ZPA)
Résumé	Vous pouvez utiliser un logiciel de protection des points de terminaison et un logiciel de gestion de ressources pour surveiller l'ensemble des appareils distribués aux utilisateurs. Veillez à maintenir une liste précise des appareils afin de suivre la validité des appareils et leurs possibilités d'accès à des applications spécifiques. Les API et les services doivent également être détectés et consignés au sein d'un inventaire. Vous pouvez tirer parti de l'analyse du réseau pour identifier les nouvelles API et les nouveaux services logiciels autorisés à communiquer sur un réseau interne ou externe.
Étapes à suivre	1. Installez le logiciel de protection des points de terminaison sur les machines des utilisateurs à l'aide d'une solution MDM. 2. Installez la solution d'analyse des API/services sur votre réseau.

Trafic Internet

Le trafic Internet comprend l'ensemble du trafic utilisateur destiné à des sites web situés en dehors de la sphère de contrôle de votre entreprise. Il peut aussi bien concerner les missions liées à l'activité que l'utilisation personnelle de sites web. L'intégralité du trafic sortant reste vulnérable aux attaques lancées par des sites et des logiciels malveillants. Les entreprises doivent mettre en place des mesures de visibilité et de contrôle sur le trafic utilisateur destiné à Internet.

Bloquer les requêtes DNS vers les menaces ou les destinations à risque connues

Niveau d'effort	**- Effort minime**
Équipe(s) impliquée(s)	• Équipe informatique avec accès à la configuration du routeur ou de la machine • Équipe de sécurité
Produit(s)	**Filtrage DNS :** Cisco Umbrella DNS, Cloudflare Gateway, DNSFilter, Zscaler Shift
Résumé	Vous pouvez appliquer le filtrage DNS via la configuration du routeur ou directement sur la machine d'un utilisateur. Il s'agit de l'un des moyens les plus rapides de protéger les utilisateurs contre les sites web malveillants connus.
Étapes à suivre	**Filtrage DNS :** mettez à jour la configuration du réseau Wi-Fi de votre bureau afin d'utiliser le service de résolution DNS approprié. L'opération peut servir à bloquer les sites web malveillants connus.

Bloquer ou isoler les menaces dissimulées derrière le SSL/TLS

Niveau d'effort	**- Effort moyen**
Équipe(s) impliquée(s)	• Équipe informatique avec accès à la configuration du routeur ou de la machine • Équipe de sécurité
Produit(s)	**Déchiffrement TLS :** Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA) **Isolation du navigateur :** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation

Bloquer ou isoler les menaces dissimulées derrière le SSL/TLS (suite)

Résumé	Certaines menaces se cachent derrière le protocole SSL et ne peuvent être bloquées que via l'inspection HTTPS. Afin de mieux protéger les utilisateurs, veillez à tirer parti d'une solution de déchiffrement TLS afin de repérer les menaces cachées dissimulées derrière le SSL.
Étapes à suivre	**Déchiffrement TLS :** 1. Assurez-vous que le logiciel sur client approprié est installé sur la machine de l'utilisateur. a. Vérifiez la présence d'un VPN ou de tout autre logiciel susceptible d'interférer avec le trafic web sortant sur l'appareil. 2. Configurez le déchiffrement TLS dans le certificat racine de l'appareil. 3. Activez des politiques détaillant à quel moment éviter de déchiffrer le trafic utilisateur. a. Cette opération doit être effectuée pour les sites qui reposent sur l'association de certificat (certificate pinning). b. Certaines entreprises évitent également de déchiffrer le trafic personnel de l'utilisateur (p. ex. les opérations bancaires, le trafic lié aux réseaux sociaux, etc.). **Isolation de navigateur :** 1. Browser isolation can be deployed via the on-device client software or via an isolation link. Both approaches should be considered.

Réseaux

La catégorie des réseaux comprend tous les réseaux publics, privés et virtuels établis au sein d'une entreprise. Les entreprises doivent commencer par dresser l'inventaire de leurs réseaux existants et les segmenter afin d'empêcher les mouvements latéraux. Elles peuvent ensuite définir des politiques Zero Trust permettant de contrôler avec précision à quels segments d'un réseau les utilisateurs, points de terminaison et appareils peuvent accéder.

Segmenter l'accès réseau des utilisateurs

Niveau d'effort	**- Effort important**
Équipe(s) impliquée(s)	• Équipe de sécurité • Équipe informatique
Produit(s)	**Accès réseau Zero Trust (ZTNA) :** Cloudflare Zero Trust (Access and Gateway used together), Netskope Private Access, Zscaler Private Access (ZPA)
Résumé	En règle générale, les utilisateurs peuvent accéder à l'ensemble d'un réseau privé à l'aide d'un VPN ou tant qu'ils se trouvent dans les locaux de l'entreprise à laquelle appartient le réseau. La mise en place d'un cadre Zero Trust nécessite que les utilisateurs n'aient accès qu'aux segments du réseau dont ils dont besoin pour accomplir une tâche donnée. Les solutions de réseau Zero Trust permettent aux utilisateurs d'accéder à distance à un réseau local, mais en restant soumis à des politiques précises basées sur l'utilisateur, l'appareil et d'autres facteurs.
Étapes à suivre	1. Assurez-vous que la solution ZTNA peut accéder au réseau privé. a. L'opération s'effectue généralement à l'aide d'un connecteur d'applications ou d'un tunnel GRE/IPSec. 2. Installez le client ZTNA sur les appareils des utilisateurs à l'aide d'une solution MDM. 3. Définissez des politiques afin de segmenter les accès des utilisateurs sur l'ensemble du réseau privé.

Utiliser une liaison Internet à large bande à des fins de connectivité entre bureaux régionaux

Niveau d'effort	**- Effort important**
Équipe(s) impliquée(s)	• Équipe d'ingénierie réseau • Équipe informatique
Produit(s)	Cloudflare Magic WAN, Cato Networks, Aryaka FlexCore

Utiliser une liaison Internet à large bande à des fins de connectivité entre bureaux régionaux (suite)

Résumé	La connectivité entre les emplacements d'un réseau privé (p. ex. les datacenters et les bureaux régionaux) a généralement été établie à l'aide de liaisons Multi-Protocol Label Switching (MPLS) ou d'autres formes de liaisons privées proposées par les fournisseurs de télécommunications. Ces liaisons MPLS s'avèrent d'ordinaire coûteuses. En outre, maintenant que la qualité du réseau Internet commercial s'est accrue, les entreprises peuvent fournir le même niveau d'accès sécurisé en routant le trafic Internet via des tunnels sécurisés pour un coût bien moindre.
Étapes à suivre	1. Choisissez deux emplacements connectés par MPLS pour commencer. Ces emplacements auront besoin de disposer d'une connectivité à Internet d'une manière ou d'une autre. 2. Définissez une paire de tunnels Anycast GRE or IPsec redondants sur vos circuits Internet à destination du réseau périphérique de votre fournisseur de WAN cloud. 3. Vérifiez l'intégrité et la connectivité entre ces tunnels. Testez les performances (débit, latence, perte de paquets, gigue) des charges de travail du trafic afin qu'elles soient aussi proches que possible de celles du trafic de production. 4. Modifiez les politiques de routage afin de faire migrer le trafic de production du MPLS aux tunnels Internet. 5. Répétez l'opération pour l'emplacement connecté par MPLS suivant. 6. Désactivez les circuits MPLS.

Fermer tous les ports entrants ouverts sur Internet à des fins de distribution des applications

Niveau d'effort	**- Effort minime**
Équipe(s) impliquée(s)	• Équipe d'ingénierie réseau
Produit(s)	**Proxys inverses Zero Trust :** Akamai EAA, Cloudflare Access, Netskope, Zscaler Private Access (ZPA)
Résumé	Les ports entrants ouverts sur le réseau peuvent être identifiés à l'aide de technologies d'analyse. Il s'agit d'un vecteur d'attaque courant. Les proxys inverses Zero Trust vous permettent d'exposer une application web de manière sécurisée, sans ouvrir de port entrant. L'enregistrement DNS de l'application reste le seul enregistrement publiquement visible de cette dernière. Il est en outre protégé à l'aide de politiques Zero Trust. À titre de couche supplémentaire de sécurité, vous pouvez utiliser un service d'accès réseau Zero Trust pour tirer parti d'un DNS interne/privé (plus de détails ci-dessous).
Étapes à suivre	1. Installez un connecteur d'applications pour le proxy inverse (en général, un daemon ou une machine virtuelle au sein du même réseau). 2. Connectez l'application de proxy inverse au connecteur d'applications. 3. Fermez tous les ports entrants sur le réseau privé à l'aide d'une règle de pare-feu.

Applications

La catégorie des applications englobe toutes les ressources dans lesquelles des données organisationnelles résident ou au sein desquelles des processus métier sont exécutés. Les entreprises doivent tout d'abord dresser une liste de leurs applications existantes, avant de définir des politiques Zero Trust pour chacune d'elles ou, dans certains cas, bloquer les applications non autorisées.

Surveiller les applications de courrier électronique et filtrer les tentatives de phishing

Niveau d'effort	**- Effort minime**
Équipe(s) impliquée(s)	• L'équipe responsable de la configuration de votre fournisseur de courrier électronique (en général le service informatique)
Produit(s)	**Sécurité des e-mails dans le cloud :** Cloudflare Area 1 Email Security, Mimecast, TitanHQ **Isolation du navigateur :** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation
Résumé	Le courrier électronique est l'un des rares canaux de communication permettant aux acteurs malveillants de bénéficier d'un accès illimité à vos collaborateurs. Le déploiement d'une passerelle e-mail sécurisée constitue une étape essentielle dans le processus visant à empêcher ces derniers de recevoir des e-mails malveillants ou non fiables. Les équipes de sécurité doivent également examiner la possibilité de mettre en quarantaine (au sein d'un navigateur isolé) les liens qui ne se révèlent pas suffisamment suspects pour être complètement bloqués.
Étapes à suivre	1. Configurez les enregistrements MX de votre domaine afin qu'ils pointent vers le service de passerelle e-mail sécurisée. 2. Surveillez les faux positifs lors des premières semaines. 3. (Bonus) Mettez en œuvre une solution d'isolation du navigateur basée sur les liens pour traiter les liens envoyés par e-mail et à la limite de la suspicion.

Dresser l'inventaire de toutes les applications d'entreprise

Niveau d'effort	**- Effort moyen**
Équipe(s) impliquée(s)	• Équipe de sécurité
Produit(s)	**Passerelle web sécurisée et CASB avec identification de l'informatique fantôme :** Cloudflare Gateway, Microsoft Defender for Cloud Apps, Netskope Next Gen SWG, Zscaler Internet Access (ZIA)

Dresser l'inventaire de toutes les applications d'entreprise (suite)

Résumé	Les équipes de sécurité ont un besoin essentiel de disposer d'un inventaire complet des applications utilisées sur l'ensemble de l'activité. Ces équipes découvriront souvent des applications non autorisées ou inconnues utilisées à l'échelle de l'entreprise, selon un phénomène fréquemment qualifié d'« informatique fantôme » (Shadow IT). Une passerelle web sécurisée (Secure Web Gateway, SWG) dotée d'une fonctionnalité de déchiffrement TLS peut servir à identifier les applications. La passerelle web sécurisée peut également être utilisée pour bloquer les applications non approuvées ou les utilisateurs d'applications (p. ex. les comptes Dropbox personnels).
Étapes à suivre	1. Activez la fonctionnalité d'identification de l'informatique fantôme dans la passerelle web sécurisée. 2. Assurez-vous que le client de la passerelle web sécurisée est bien installé sur les appareils des utilisateurs. 3. Laissez circuler le trafic des utilisateurs pendant deux à trois semaines. 4. Examinez la liste des applications identifiées. 5. Bloquez les éventuelles applications non approuvées à l'aide de politiques de passerelle web sécurisée. 6. Protégez les applications approuvées à l'aide de politiques Zero Trust.

Application de politiques Zero Trust pour les applications

Niveau d'effort	 - **Effort minime** (pour les applications les plus essentielles)  **- Effort important** (pour toutes les applications)
Équipe(s) impliquée(s)	• Équipe de sécurité • Équipe de développement d'applications • Équipe informatique
Produit(s)	**Proxys inverses Zero Trust :** Azure App Proxy, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA) **Accès réseau Zero Trust (ZTNA) :** Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA) **CASB:** Cloudflare CASB, Netskope CASB, Zscaler CASB **Isolation de navigateur à distance :** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation

Application de politiques Zero Trust pour les applications (suite)

Résumé	Les applications doivent être protégées à l'aide de politiques Zero Trust qui prennent en compte l'identité de l'utilisateur, l'appareil et le contexte du réseau avant d'authentifier et d'autoriser l'accès. Elles doivent ainsi disposer de politiques détaillées, capables de mettre en œuvre le principe du moindre privilège, notamment pour les applications qui contiennent des données sensibles. Les applications se divisent en trois types principaux et le modèle de sécurité Zero Trust varie pour chacun d'eux. Les trois principaux types d'applications sont les suivants : 1. Applications privées auto-hébergées (uniquement adressables sur le réseau de l'entreprise) 2. Applications publiques auto-hébergées (adressables sur l'ensemble d'Internet) 3. Applications SaaS **Remarque :** si le contexte de l'appareil ou le statut de conformité constitue une politique de sécurité requise, un client logiciel sur l'appareil sera alors généralement nécessaire.
Étapes à suivre	**Applications privées auto-hébergées** 1. Créez un tunnel chiffré entre l'application et la couche de politique Zero Trust. En règle générale, il s'agira d'un « connecteur d'applications » ou d'un tunnel GRE/IPSec. 2. Assurez-vous que les utilisateurs du client ZTNA sur appareil puissent accéder au résolveur DNS privé. 3. Créez des politiques basées sur le contexte de l'utilisateur, de l'appareil et du réseau afin de définir qui peut accéder à l'application. **Applications publiques auto-hébergées** 1. Faites migrer le DNS de référence ou un enregistrement CNAME vers le proxy inverse pour applications. 2. Assurez-vous que tous les ports entrants soient fermés pour le réseau de l'application. 3. Créez des politiques basées sur le contexte de l'utilisateur, de l'appareil et du réseau afin de définir qui peut accéder à l'application. **Applications SaaS** La mise en œuvre de politiques Zero Trust pour les applications SaaS peut s'effectuer par l'intermédiaire d'une poignée d'options différentes. **Proxy d'identité** Cloudflare, Netskope et Zscaler proposent des proxys d'identité permettant le même déploiement de politiques qu'une application de proxy inverse auto-hébergée. L'opération nécessite que le proxy d'identité soit configuré en tant que fournisseur SSO (Single Sign On, authentification unique) de l'application SaaS. 1. Supprimez l'intégration SSO existante de l'application SaaS, le cas échéant. 2. Intégrez le proxy d'identité à l'application SaaS. 3. Assurez-vous d'envoyer les attributs SAML appropriés aux fins de création d'utilisateur et de mise à jour de ces derniers. 4. Définissez des politiques basées sur le contexte de l'utilisateur, de l'appareil et du réseau.

Application de politiques Zero Trust pour les applications (suite)

Étapes à suivre	**Passerelle web sécurisée et authentification unique** L'autre approche consiste à passer par un fournisseur d'authentification unique existant pour déterminer quels utilisateurs peuvent accéder ou non à l'application SaaS. La passerelle web sécurisée, dotée d'une adresse IP dédiée, peut alors être utilisée pour s'assurer que seuls les utilisateurs d'appareils gérés et contrôlés par inspection du trafic peuvent accéder à l'application SaaS. 1. Ajoutez l'application SaaS au fournisseur SSO. 2. Créez des politiques afin de définir quels utilisateurs sont autorisés. 3. Ajoutez l'adresse IP de l'instance de passerelle web sécurisée à la liste d'autorisation de l'application SaaS (la plupart des applications SaaS prennent en charge les listes d'autorisation dans leurs paramètres de sécurité de base). 4. Créez des politiques de passerelle web sécurisée permettant de contrôler quels utilisateurs sont autorisés à accéder à l'application SaaS.

Protéger les applications contre les attaques sur la couche 7 (attaques DDoS, attaques par injection, bots, etc.)

Niveau d'effort	**- Effort minime**
Équipe(s) impliquée(s)	• Équipe de sécurité • Équipe de développement d'applications
Produit(s)	Akamai, AWS, Azure, Cloudflare, GCP
Résumé	Les applications auto-hébergées sont vulnérables aux attaques sur la couche 7, qui regroupent les attaques DDoS, les attaques par injection de code et les attaques de bots, parmi bien d'autres. Les équipes de sécurité doivent déployer un pare-feu d'applications web (WAF) et une protection contre les attaques DDoS en amont de toutes les applications auto-hébergées, qu'elles soient adressables publiquement ou de manière privée.
Étapes à suivre	1. Ajoutez l'enregistrement du DNS de référence de n'importe quelle application publique. 2. Activez le pare-feu d'applications web (WAF) et la protection contre les attaques DDoS.

Appliquer le HTTPS et les DNSSEC

Niveau d'effort	**- Effort minime**
Équipe(s) impliquée(s)	• Équipe de sécurité • Équipe de développement d'applications
Produit(s)	Akamai, AWS, Azure, Cloudflare, GCP
Résumé	Les applications web auto-hébergées doivent mettre en œuvre le HTTPS et les DNSSEC. L'utilisation de ces protocoles permet de prévenir les risques potentiels d'analyse et d'interception de paquets (packet sniffing) ou de détournement de domaine.
Étapes à suivre	1. Ajoutez l'enregistrement du DNS de référence de n'importe quelle application publique. 2. Définissez le HTTPS sur Strict et activez les DNSSEC.

Prévention des pertes de données et journalisation

Une fois l'ensemble des éléments Zero Trust de votre architecture établis, cette dernière générera d'importants volumes de données sur les événements qui se produisent au sein de votre réseau. Il est désormais temps de mettre en œuvre les fonctionnalités de prévention des pertes de données et de journalisation. Un ensemble de processus et d'outils existent pour vous permettre de vous concentrer sur la conservation des données sensibles au sein de l'entreprise, ainsi que sur l'identification des potentialités en matière de fuites de données. Les entreprises doivent tout d'abord comprendre à quel endroit leurs données sensibles résident, avant de définir des mesures de contrôle Zero Trust permettant de bloquer l'accès à ces données et leur exfiltration.

Définir un processus de journalisation et d'examen du trafic sur les applications sensibles

Niveau d'effort	- Effort moyen
Équipe(s) impliquée(s)	• Équipe de sécurité
Produit(s)	**Passerelle web sécurisée (SWG) :** Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA) **Gestion de l'information et des événements de sécurité (SIEM) :** DataDog, Splunk, SolarWinds
Résumé	Les solutions de passerelle web sécurisée disposent de fonctionnalités permettant de transmettre les journaux du trafic utilisateur vers un outil SIEM (Security Incident and Event Monitoring, gestion de l'information et des événements de sécurité). Les équipes de sécurité devraient adopter l'examen des journaux du trafic destiné aux applications sensibles en tant qu'exercice régulier. Le SIEM vous permet de configurer des alertes spécifiques relatives au trafic anormal ou malveillant, que vous pouvez ensuite affiner au fil du temps.
Étapes à suivre	1. Assurez-vous que l'ensemble du trafic utilisateur destiné aux applications est bien mis en proxy à l'aide de la passerelle web sécurisée (SWG). 2. Activez la fonctionnalité de transfert ou d'extraction de journaux (log push/log pull) entre votre SWG et votre SIEM. 3. Définissez un intervalle spécifique d'examen des journaux de trafic par l'équipe de sécurité. 4. Dans le SIEM, configurez des alertes basées sur les constatations relevées au fil du temps.

Définir les données sensibles et l'endroit où elles résident

Niveau d'effort	- Effort moyen
Équipe(s) impliquée(s)	• Équipe de sécurité • Équipe chargée de la conformité/juridique
Produit(s)	**Gestion de l'information et des événements de sécurité (SIEM) :** DataDog, Splunk, SolarWinds

Définir les données sensibles et l'endroit où elles résident (suite)

Résumé	Les données sensibles varient considérablement selon les secteurs. Les entreprises de technologie se soucient ainsi de protéger leur code source, tandis que les prestataires de soins médicaux se concentrent essentiellement sur la conformité (par exemple, à l'HIPAA aux États-Unis). Il s'avère donc important de bien définir les données que votre entreprise considère comme sensibles, ainsi que l'endroit où elles résident. Une définition minutieuse des données sensibles, suivie d'un inventaire précis de ces dernières, permettra d'étayer la mise en œuvre des outils de prévention des pertes de données.
Étapes à suivre	1. Examinez les journaux de trafic dans les outils du SIEM ou directement au sein d'une passerelle web sécurisée afin d'identifier les applications et les banques de données cibles. 2. Dressez l'inventaire des données sensibles existantes.

Empêcher les données sensibles de quitter vos applications

Niveau d'effort	**- Effort important**
Équipe(s) impliquée(s)	• Équipe de sécurité • Équipe informatique • Équipe chargée de la conformité/juridique
Produit(s)	**Solutions internes de prévention des pertes de données :** Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA)
Résumé	Les solutions internes de prévention des pertes de données (Data Loss Prevention, DLP) inspectent le trafic utilisateur et les téléchargements/téléversements de fichiers à la recherche de données sensibles. Ces données sensibles sont disponibles au sein de listes prédéfinies et bien connues (p. ex. données à caractère personnel, SSN, cartes de paiement, etc.). Un administrateur peut aussi configurer manuellement des schémas spécifiques pour ces dernières. Veillez à activer les mesures de contrôle DLP pour les applications sensibles. Ces mesures peuvent également être étendues à l'ensemble du trafic utilisateur.
Étapes à suivre	1. Installez le client logiciel du fournisseur de solution DLP. 2. Assurez-vous qu'aucun VPN ou autre outil susceptible de perturber la connectivité n'existe. 3. Assurez-vous d'avoir activé le déchiffrement TLS et veillez à ce qu'un certificat racine soit présent sur chaque machine utilisateur. 4. Activez les mesures de contrôle DLP. 5. Surveillez les événements de blocage DLP et vérifiez s'ils sont valides ou s'il s'agit de faux positifs.

Identifier les mauvaises configurations et les données partagées publiquement dans les outils SaaS

Niveau d'effort	▮ - **Effort minime**
Équipe(s) impliquée(s)	• Équipe de sécurité
Produit(s)	**Cloud Access Security Broker (CASB) basé sur API :** Cloudflare CASB, DoControl, Netskope, Zscaler CSPM
Résumé	Les agents de sécurité des accès au cloud (CASB) s'intègrent aux plus grandes applications SaaS par le biais d'une intégration d'API. Le CASB analysera ensuite l'application SaaS à la recherche de problèmes connus en termes de mauvaise configuration des outils de sécurité et de données partagées publiquement. Les équipes de sécurité doivent établir un calendrier régulier d'examen des constatations du CASB.
Étapes à suivre	1. Connectez chaque application SaaS en suivant les instructions d'intégration du fournisseur de l'API. 2. Analysez chaque application SaaS. 3. Examinez les résultats d'analyse et commencez à déployer des mesures correctives dans chaque application SaaS, le cas échéant.

Établir un centre d'opérations de sécurité (SOC, Security Operations Center) à des fins d'examen des journaux, de mise à jour des politiques et d'atténuation

Niveau d'effort	▮▮ - **Effort moyen**
Équipe(s) impliquée(s)	• Équipe de sécurité
Produit(s)	**Aucun**
Résumé	Pour une équipe de sécurité, le SOC constitue une fonction essentielle au sein du cadre Zero Trust. Il doit se concentrer sur l'examen des alertes de sécurité et des informations contenues dans les journaux, de même que sur l'ajustement des politiques Zero Trust sur l'ensemble des produits de sécurité principaux.
Étapes à suivre	1. Examinez les journaux dans le SIEM ou directement au sein du produit de sécurité. 2. Identifiez les alertes ou les éventuelles activités anormales. 3. Mettez à jour les politiques Zero Trust pour chaque outil en fonction des conclusions de l'analyse.

Se tenir à jour des acteurs malveillants connus

Niveau d'effort	- **Effort minime**
Équipe(s) impliquée(s)	• Équipe de sécurité
Produit(s)	**Fournisseurs d'informations sur les menaces :** Cloudflare Radar, CISA, OWASP
Résumé	Plusieurs fournisseurs se concentrent sur la compilation d'une liste des acteurs et des sites malveillants connus. Ces flux d'informations sur les menaces peuvent être automatiquement chargés au sein d'une passerelle web sécurisée afin de protéger les utilisateurs contre les attaques.
Étapes à suivre	1. Connectez le flux d'informations sur les menaces dans la passerelle web sécurisée. 2. Activez la protection contre les menaces dans la solution de filtrage DNS et HTTP.

État stable

Une fois l'architecture Zero Trust définie pour l'ensemble des autres éléments de votre organisation, vous pouvez entreprendre un certain nombre d'actions pour amener votre entreprise à un état de stabilité Zero Trust, afin d'assurer la cohérence avec l'architecture à compter de ce point.

Employer une approche DevOps afin d'assurer l'application cohérente des politiques pour toutes les nouvelles ressources

Niveau d'effort	- Effort important
Équipe(s) impliquée(s)	• Équipe de sécurité • Équipe de développement d'applications
Produit(s)	**Automatisation de l'infrastructure :** Ansible, Puppet, Terraform
Résumé	Les outils d'automatisation de l'infrastructure permettent aux développeurs de déployer automatiquement une sécurité Zero Trust dans le cadre de leur pipeline de développements d'applications. Il conviendra d'établir un processus de tests en interne qui s'activera si une application est déployée à l'aide d'une protection par proxy inverse Zero Trust.
Étapes à suivre	1. Définissez une politique standard pour les nouvelles applications. 2. Ajoutez des tests au processus de déploiement d'applications nécessitant une protection par proxy inverse Zero Trust.

Mettre en œuvre l'évolution automatique des ressources en accès direct

Niveau d'effort	 **- Effort important**
Équipe(s) impliquée(s)	• Équipe de sécurité • Équipe de développement d'applications
Produit(s)	**Solutions d'équilibrage de charge :** Akamai, Cloudflare **Automatisation de l'infrastructure :** Ansible, Puppet, Terraform

Mettre en œuvre l'évolution automatique des ressources en accès direct (suite)

Résumé	Les solutions d'équilibrage de charge peuvent se révéler des outils bien efficaces pour s'assurer que l'infrastructure individuelle d'une application ne soit jamais surchargée. Elles permettent également de proposer un niveau de redondance en cas de défaillance du serveur de l'application. Les outils d'automatisation de l'infrastructure peuvent servir à activer de nouvelles ressources en cas de franchissement de seuils de trafic spécifiques.
Étapes à suivre	1. Configurez une solution d'équilibrage de charge en amont de votre connecteur d'applications par proxy inverse Zero Trust. 2. Activez des règles d'équilibrage de charge basées sur les volumes de trafic et/ou la position géographique des utilisateurs. 3. Mettez en œuvre des politiques d'automatisation de l'infrastructure permettant d'activer de nouvelles machines virtuelles si une charge suffisante est générée sur un ensemble spécifique d'applications.

Exemple de calendrier de mise en œuvre

Chaque déploiement d'architecture Zero Trust est unique, mais la plupart des projets suivent un ensemble d'étapes commun. Le tableau ci-dessous présente un calendrier recommandé pour une entreprise qui démarre tout juste son processus de déploiement d'une architecture Zero Trust.

Chronologie		Objectif	Produits pertinents
Phase 1	☐	**Déployer le filtrage DNS à l'échelle mondiale**	Cisco Umbrella DNS, Cloudflare Gateway, DNSFilter, Zscaler Shift
	☐	**Surveiller les e-mails entrants et filtrer les tentatives de phishing**	**Sécurité des e-mails dans le cloud :** Cloudflare Area 1 Email Security, Mimecast, TitanHQ **Isolation du navigateur :** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation
	☐	**Identifier les mauvaises configurations et les données partagées publiquement dans les outils SaaS**	Cloudflare CASB, DoControl, Netskope, Zscaler CSPM
Phase 2	☐	**Établir une identité d'entreprise**	Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin
	☐	**Appliquer une MFA de base pour toutes les applications**	**Fournisseurs d'identité :** Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin **Proxys inverses pour applications :** Microsoft Azure AD App Proxy, Akamai EAA, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA)
	☐	**Appliquer le HTTPS et les DNSSEC**	Akamai, AWS, Azure, Cloudflare, GCP
	☐	**Bloquer ou isoler les menaces dissimulées derrière le SSL**	**Déchiffrement TLS :** Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA) **Isolation du navigateur :** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation
	☐	**Application de politiques Zero Trust pour les applications publiquement adressables**	**Proxys inverses Zero Trust :** Azure App Proxy, Cloudflare Access, Netskope Private Access, Zscaler Private Access (ZPA)
	☐	**Protéger les applications contre les attaques sur la couche 7**	Akamai, AWS, Azure, Cloudflare, GCP
	☐	**Fermer tous les ports entrants ouverts sur Internet à des fins de distribution des applications**	Akamai EAA, Cloudflare Access, Netskope, Zscaler Private Access (ZPA)
Phase 3	☐	**Dresser l'inventaire de toutes les applications d'entreprise**	**Passerelle web sécurisée et CASB avec identification de l'informatique fantôme :** Cloudflare Gateway, Microsoft Defender for Cloud Apps, Netskope Next Gen SWG, Zscaler Internet Access (ZIA)
	☐	**Application de politiques Zero Trust pour les applications SaaS**	**Accès réseau Zero Trust (ZTNA) :** Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA) **CASB:** Cloudflare CASB, Netskope CASB, Zscaler CASB

Phase 4	☐ **Segmenter l'accès réseau des utilisateurs**	**Accès réseau Zero Trust (ZTNA) :** Cloudflare Zero Trust (Access and Gateway used together), Netskope Private Access, Zscaler Private Access (ZPA)
	☐ **Accès réseau Zero Trust pour les applications adressables de manière privée**	Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA)
	☐ **Mettre en œuvre une solution de MDM/UEM afin de contrôler les appareils d'entreprise**	**Mac:** Jamf, Kandji **Windows:** Microsoft Intune
	☐ **Définir les données sensibles et l'endroit où elles résident**	DataDog, Splunk, SolarWinds
	☐ **Envoyer des jetons d'authentification basés sur le matériel**	**Clés physiques :** Yubico
	☐ **Se tenir à jour des acteurs malveillants connus**	Cloudflare Radar, CISA, OWASP
	☐ **Appliquer une MFA basée sur des jetons physiques**	**Clés physiques :** Yubico
	☐ **Application de politiques et accès réseau Zero Trust pour toutes les applications**	Cloudflare Access, Netskope Private Access, Zscaler Internet Access (ZIA)
	☐ **Établir un SOC à des fins d'examen des journaux, de mise à jour des politiques et d'atténuation**	S.O.
	☐ **Mettre en œuvre la protection des points de terminaison**	VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender
	☐ **Dresser l'inventaire de tous les appareils, API et services de l'entreprise**	**Parc d'appareils :** VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender, Oomnitza **Parc d'API/services :** Cloudflare application connector, Zscaler Private Access (ZPA)
	☐ **Utiliser une liaison Internet à large bande à des fins de connectivité entre bureaux régionaux**	Cloudflare Magic WAN, Cato Networks, Aryaka FlexCore
	☐ **Définir un processus de journalisation et d'examen de l'activité des collaborateurs sur les applications sensibles**	**Passerelle web sécurisée (SWG) :** Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA) **Gestion de l'information et des événements de sécurité (SIEM) :** DataDog, Splunk, SolarWinds
	☐ **Empêcher les données sensibles de quitter vos applications (p. ex. données à caractère personnel, cartes de paiement, SSN, etc.)**	Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access (ZIA)
	☐ **Employer une approche DevOps afin d'assurer l'application des politiques pour toutes les nouvelles ressources**	Ansible, Puppet, Terraform
	☐ **Mettre en œuvre l'évolution automatique des ressources en accès direct**	**Solutions d'équilibrage de charge :** Akamai, Cloudflare **Automatisation de l'infrastructure :** Ansible, Puppet, Terraform

+33 7 57 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

RÉV. : BDES-3584.2022AUG09