GUIDE DE CONFIGURATION

CLOUDFLARE

Cloudflare One, notre plateforme SASE

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

INDEX

Remarque : d'autres scénarios d'utilisation seront ajoutés

À propos de ce guide

Ce guide de configuration est destiné aux praticiens dotés d'une orientation technique et fournit des exemples illustratifs de la manière dont les organisations peuvent simplifier et renforcer leur architecture de connectivité réseau et de sécurité avec Cloudflare One, notre plateforme SASE. Cloudflare One réunit les services de connectivité réseau et des services de sécurité Zero Trust – tous mis en œuvre sur le réseau mondial de Cloudflare.

La première partie de ce guide de configuration se concentre sur la transformation et la modernisation exhaustives en illustrant tous les éléments de connectivité et de sécurité pouvant être mis en œuvre, alignés sur la connectivité réseau entrante, la connectivité réseau sortante et les applications, avant et après Cloudflare. Elle compare l'approche existante, reposant sur un périmètre de sécurité centralisé et faisant appel à des solutions multi-fournisseurs, et l'approche du réseau mondial de Cloudflare, fondée sur une architecture de plateforme composable unique.

Les sections suivantes présentent des scénarios d'utilisation technique courants – d'abord, comment ce problème est généralement résolu avec une approche traditionnelle, puis comment Cloudflare One résout le même problème avec davantage d'efficacité et une expérience améliorée.

Deux scénarios d'utilisation ont été priorisés en raison de leur popularité auprès des clients, mais ils ne représentent en aucun cas l'étendue complète des fonctionnalités de Cloudflare One.

- Accès sécurisé pour les applications web privées et publiques
- Filtrage DNS pour le personnel sur site et en télétravail

Nous continuerons à enrichir ce guide avec des scénarios d'utilisation supplémentaires tels que l'accès sécurisé aux réseaux privés, la protection avancée contre les menaces/la protection des données, etc.

Transformation : comparaison avant et après Cloudflare

Connectivité sécurisée, rapide, fiable et privée pour tous les utilisateurs

Tout utilisateur

Les organisations doivent déployer une connectivité sécurisée, rapide, fiable et privée pour deux groupes d'utilisateurs.

Les utilisateurs gérés sont des collaborateurs qui accèdent à une ressource avec un appareil de l'entreprise ou un appareil personnel depuis leur domicile, leur bureau ou n'importe quel endroit situé entre ces deux points.

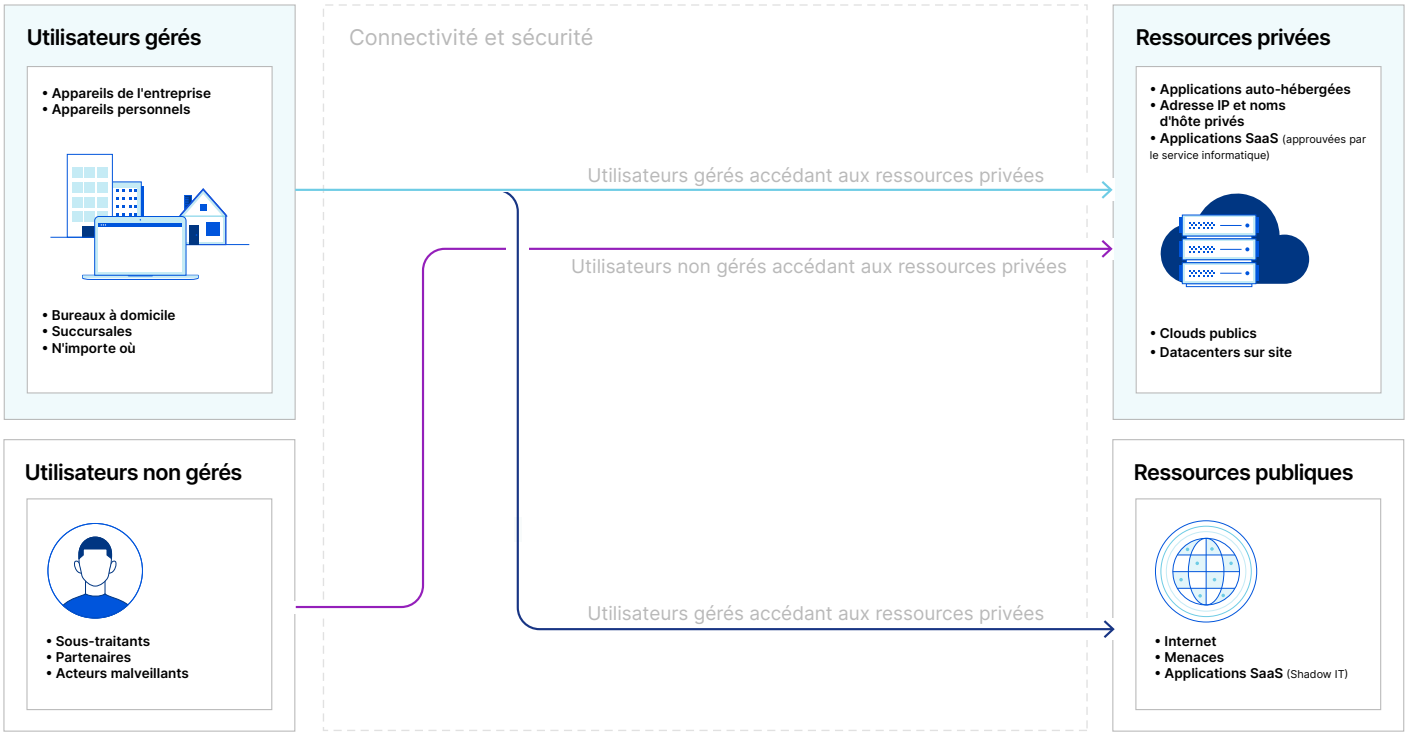
Les utilisateurs non gérés incluent les sous-traitants ou les partenaires autorisés à accéder à une ressource, mais également les acteurs malveillants indésirables.

Ressource

Les organisations doivent déployer une gestion des accès intégrant une protection contre les menaces et une protection des données pour deux groupes de ressources.

Les ressources privées incluent les applications auto-hébergées et les adresses IP ou noms d'hôtes privés dans les Clouds publics et les datacenters sur site, ainsi que les applications SaaS approuvées par le service informatique.

Les ressources publiques sur Internet incluent les applications SaaS non approuvées et les menaces.



Comparaison de la connectivité et de la sécurité avant et après Cloudflare

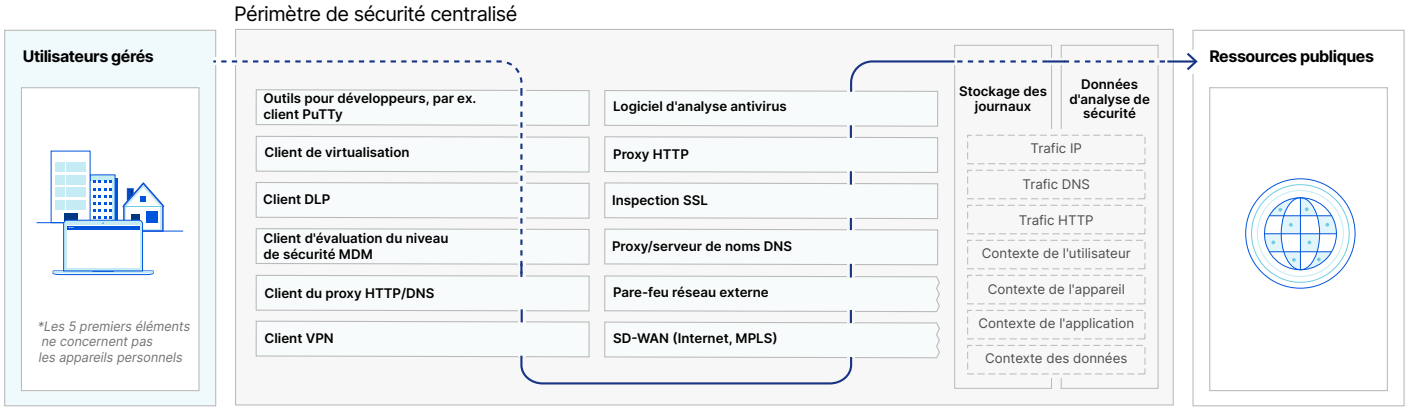
Sur les six pages suivantes, une série de diagrammes avant/après fournissent progressivement des informations détaillées concernant tous les éléments de connectivité et de sécurité indispensables à votre organisation pour permettre aux utilisateurs gérés d'accéder aux ressources publiques et aux utilisateurs gérés ou non gérés d'accéder aux ressources privées.

Le premier diagramme « avant » illustre les points de terminaison de traitement et de connectivité réseau déployés dans un périmètre de sécurité centralisé.

Le deuxième diagramme « après » illustre les services de Cloud comparables fournis via le réseau mondial de Cloudflare.

1a. Simplifier la connectivité et la sécurité pour les ressources publiques

Avant Cloudflare



= Première instance de l'élément ------ = Trafic réseau non acheminé/filtré à travers ces composants

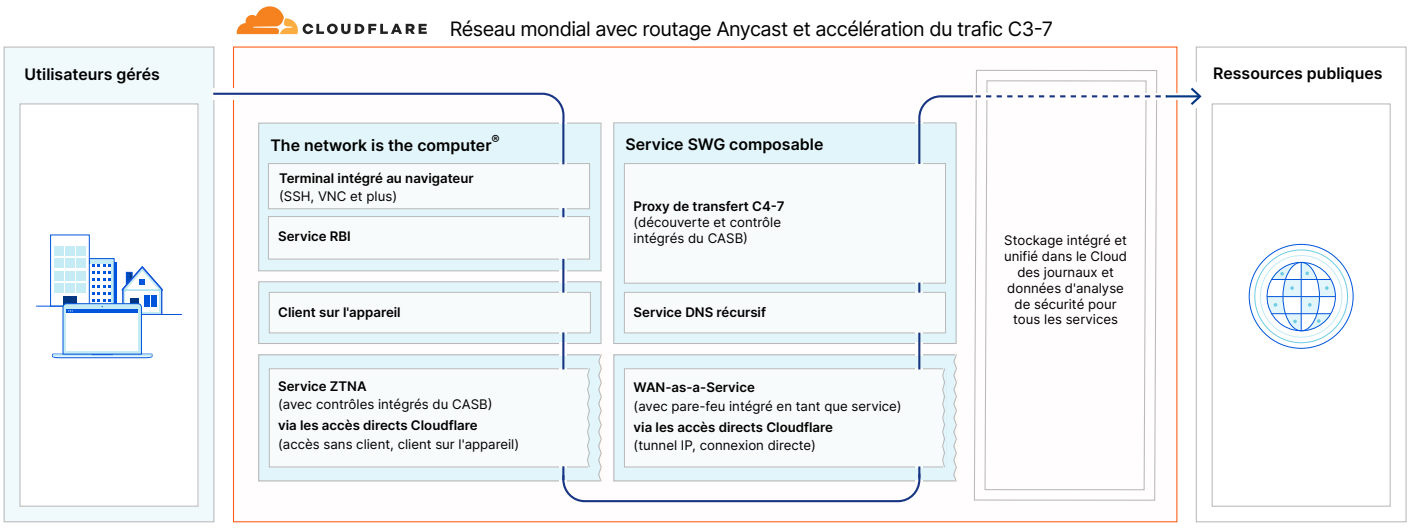
Utilisateurs gérés
(vers ressources publiques et privées)

Les équipes informatiques devaient gérer de nombreux clients pour la connectivité et la sécurité – ou pire, elles ne pouvaient rien faire pour les appareils personnels. Outils de développement et VPN pour l'accès privé. Proxy HTTP/DNS pour l'accès public. Virtualisation, DLP et MDM pour une protection renforcée.

Ressources publiques

Les équipes de sécurité comptaient sur le client VPN ou le SD-WAN pour acheminer le trafic des utilisateurs distants ou présents dans les bureaux à travers le pare-feu réseau, le proxy DNS, l'inspection SSL, le proxy HTTP et les équipements d'analyse antivirus afin de protéger l'accès aux ressources publiques.

Après Cloudflare



= Première instance de l'élément ------ = Trafic réseau non acheminé/filtré à travers ces compos

Utilisateurs gérés
(vers ressources publiques et privées)

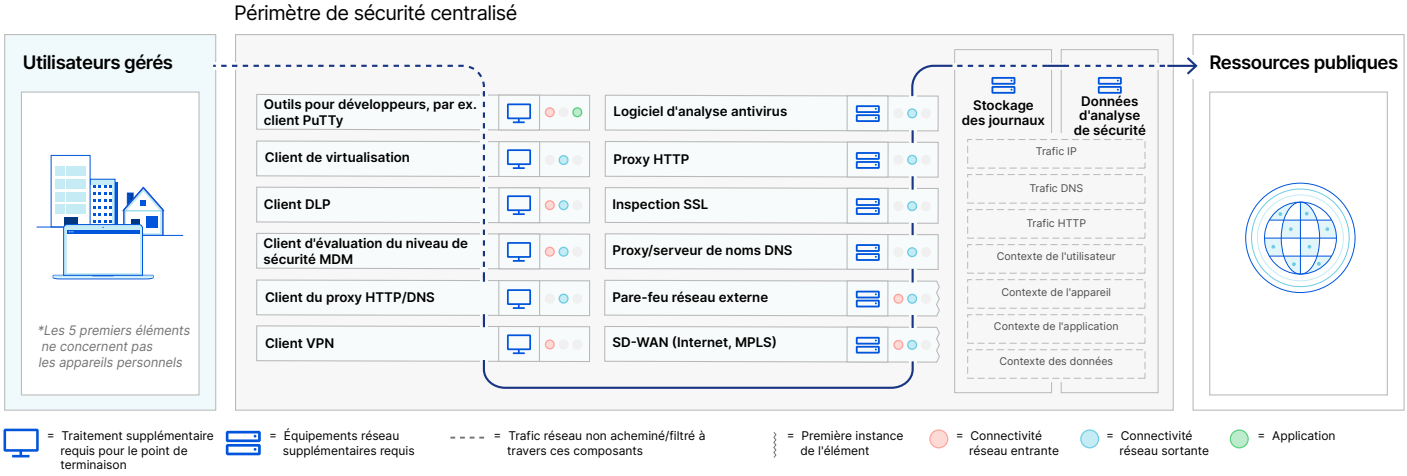
Le réseau supprime de nombreuses fonctions de l'ordinateur, ou un client consolide de nombreuses fonctions.

Ressources publiques

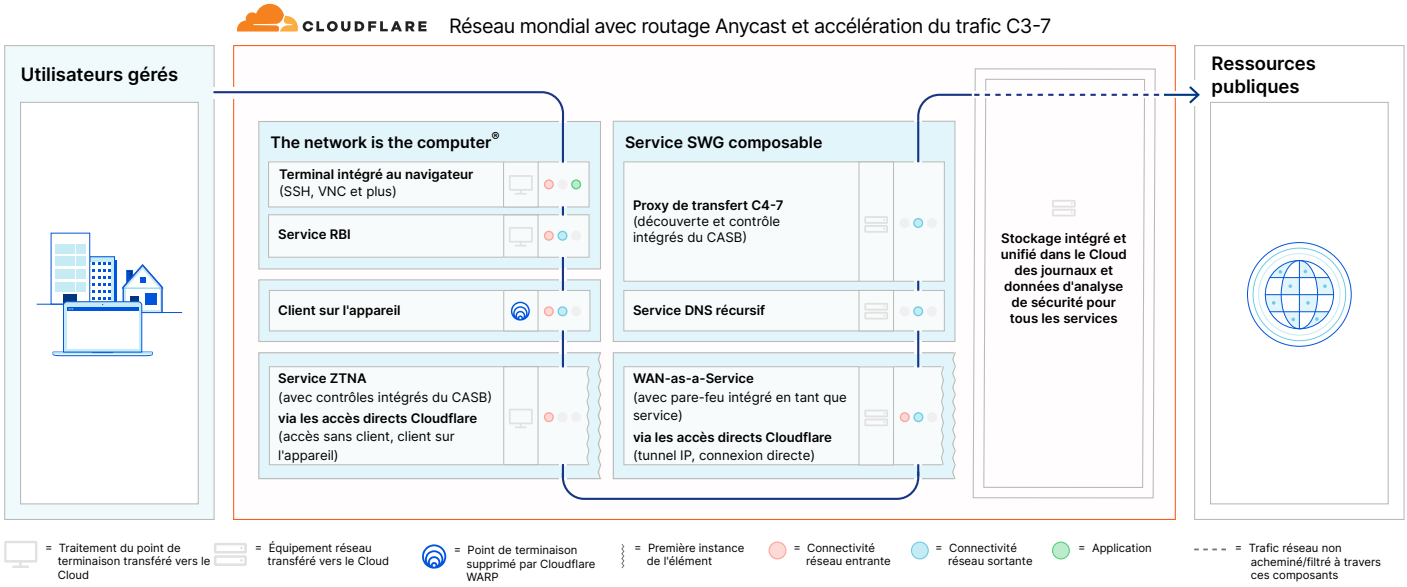
Notre service SWG composable inspecte le trafic en une seule passe avant ou après l'adoption de notre service WAN-as-a-Service et/ou notre service ZTNA avec sécurité intégrée.

1b. Simplifier la connectivité et la sécurité des ressources publiques

Avant Cloudflare



Après Cloudflare



Services Cloud-native

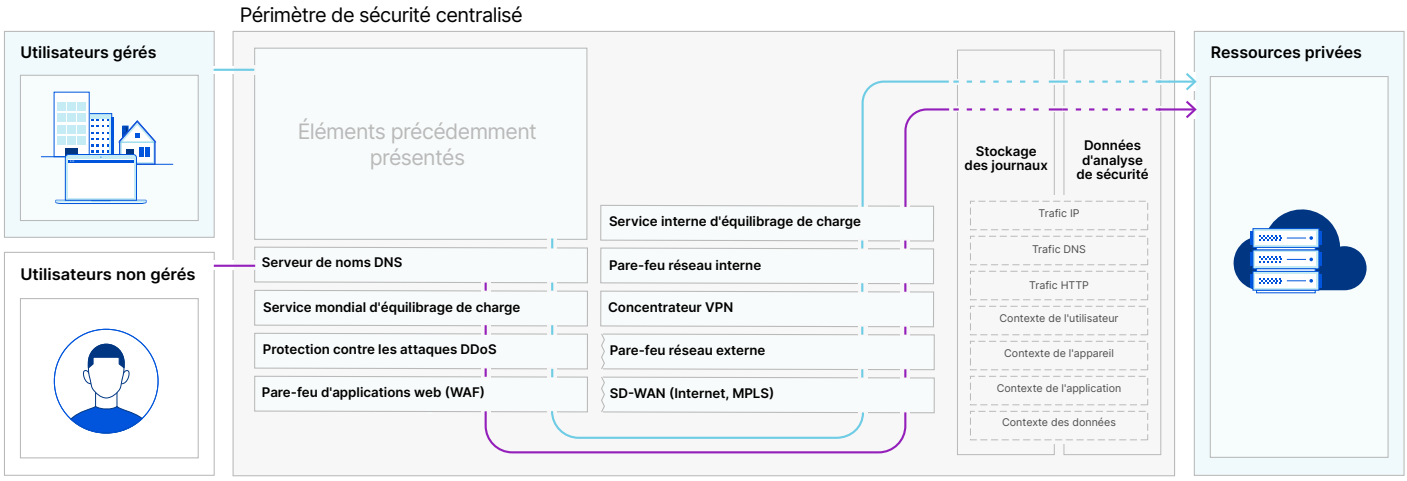
Les exigences applicables aux équipements réseau et de traitement sont réduites.

Architecture composable

Les piles de connectivité réseau entrante et sortante sont unifiées avec la pile d'applications, assurant une sécurité et des performances exhaustives.

2a. Simplifier la connectivité et la sécurité des ressources privées

Avant Cloudflare



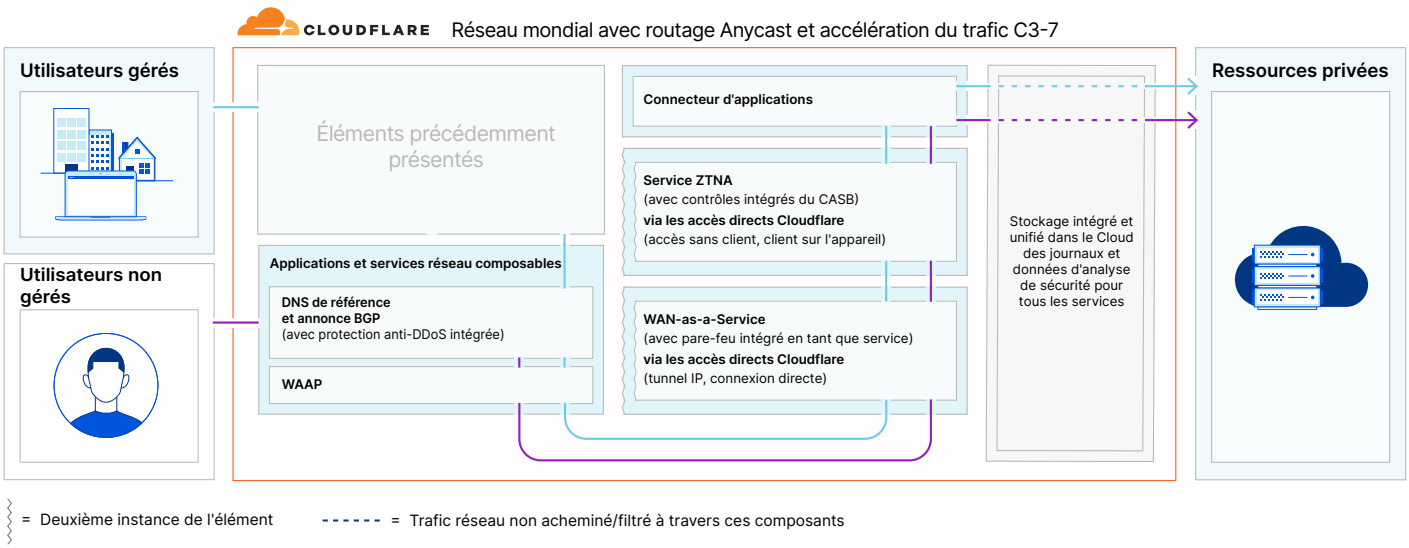
Utilisateurs non gérés

Les équipes réseau devaient gérer l'annonce publique de la disponibilité des ressources privées auprès des sous-traitants et partenaires, tout en protégeant l'infrastructure contre les attaques DDoS ou l'exploitation de vulnérabilités par des acteurs malveillants.

Ressources privées (d'utilisateurs gérés et non gérés)

Les équipes de sécurité comptaient sur le client VPN ou le SD-WAN pour acheminer le trafic des utilisateurs à travers les pare-feu réseau, les concentrateurs VPN et les systèmes d'équilibrage de charge afin de sécuriser l'accès aux ressources privées.

Après Cloudflare



Utilisateurs non gérés

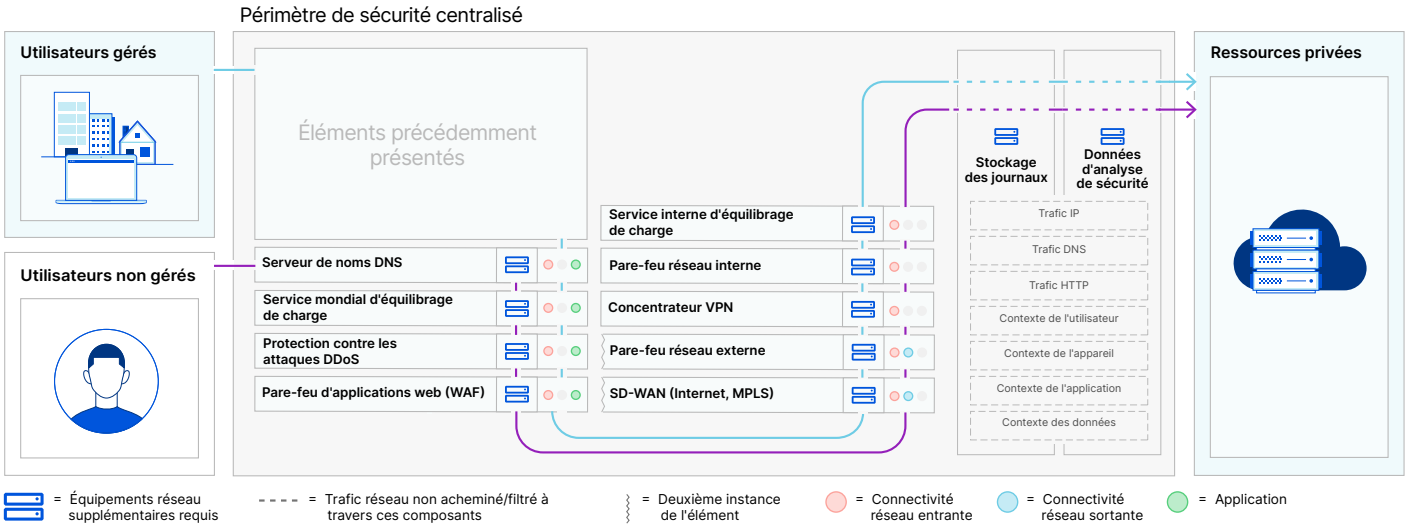
Nos services d'application et de réseau composables éliminent cette charge, avant ou après l'adoption de nos services ZTNA ou WAN-as-a-Service avec sécurité intégrée.

Ressources privées (d'utilisateurs gérés et non gérés)

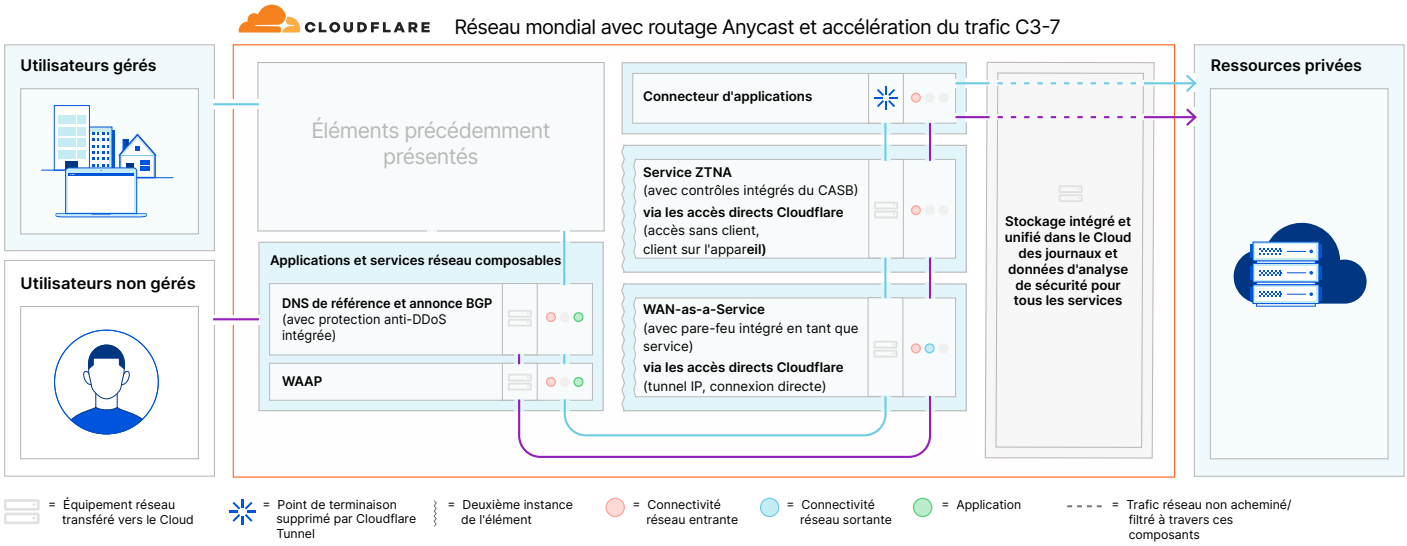
Nos services ZTNA et/ou WAN-as-a-Service avec sécurité intégrée simplifient l'accès avec notre connecteur d'applications.

2b. Simplifier la connectivité et la sécurité des ressources privées

Avant Cloudflare



Après Cloudflare



Services Cloud-native

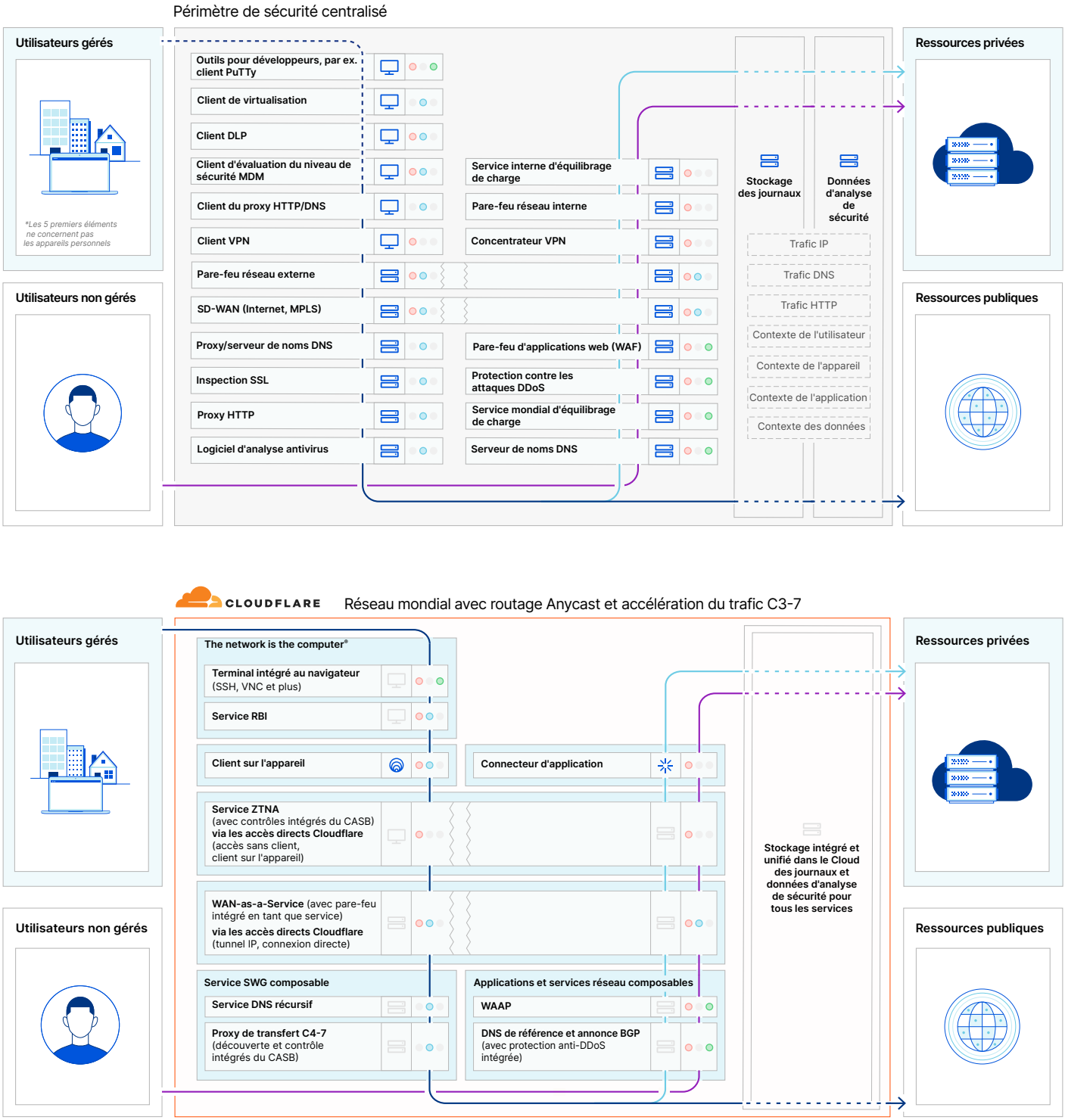
Les exigences applicables aux équipements réseau et de traitement sont réduites.

Architecture composable

Les piles de connectivité réseau entrante et sortante sont unifiées avec la pile d'applications, assurant une sécurité et des performances de bout en bout.

Simplifier la connectivité et la sécurité de toutes les ressources

Cette vue réunit les diagrammes 1 et 2.



Après

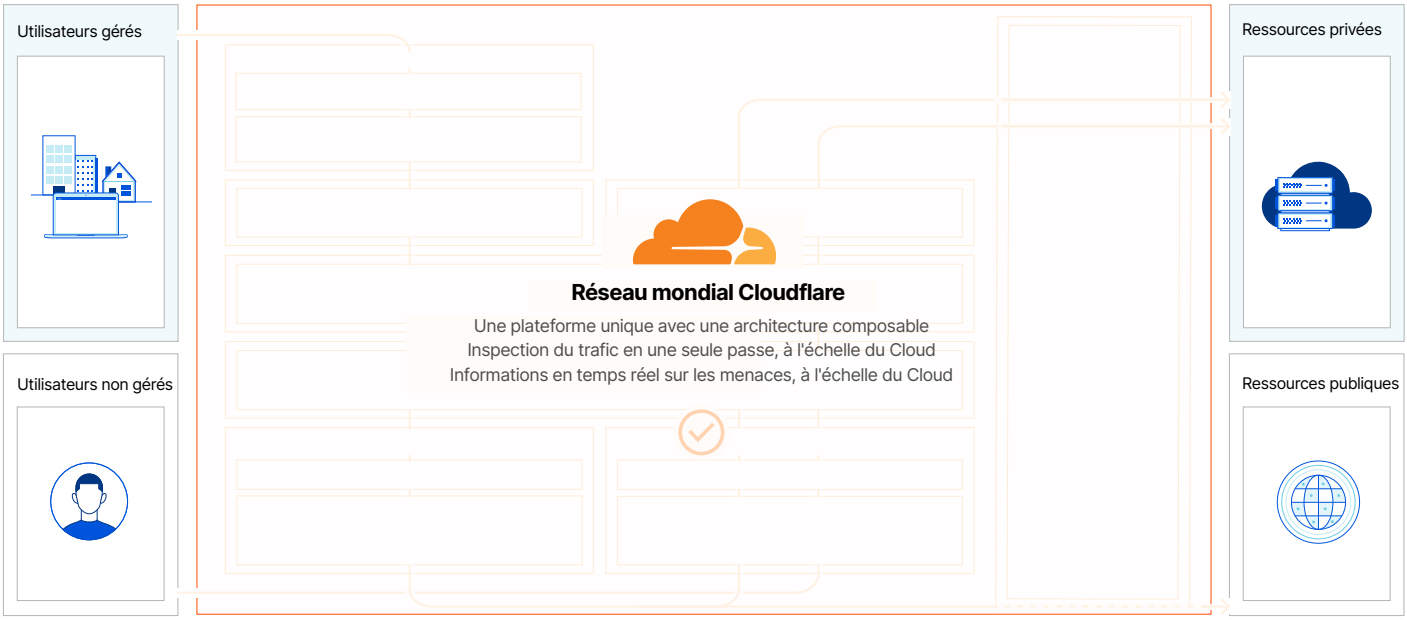
Les éléments de connectivité et de sécurité sont réutilisés lorsqu'un utilisateur quelconque accède à une ressource quelconque, ce qui améliore l'efficacité et l'expérience. De plus, nos services ZTNA et WAN-as-a-Service incluent des composants traditionnellement gérés dans des silos par les équipes informatiques, réseau et de sécurité.

Une plateforme unique pour une connectivité et une sécurité simplifiées au maximum

Périmètre de sécurité centralisé et réseau mondial de Cloudflare

Avant

Les équipes informatiques, réseau et de sécurité se fiaient aux solutions de nombreux fournisseurs, possédant chacune une architecture différente ; par conséquent, les intégrations point à point entraînaient la présence de failles de connectivité et de sécurité, ainsi que des performances limitées.



Après

Toutes les équipes bénéficient d'une plateforme unique, avec la même architecture composable, permettant d'éliminer les failles et les compromis en matière de performance. Notre plateforme peut être déployée sur toutes les infrastructures, et est conçue pour s'adapter à votre monde, et non l'inverse. Vous pouvez déployer autant de services que vous le souhaitez, dans l'ordre de votre choix ; l'ensemble de la plateforme fonctionnera toujours de manière uniforme.

Scénario d’utilisation 1 : Accès sécurisé pour les applications web

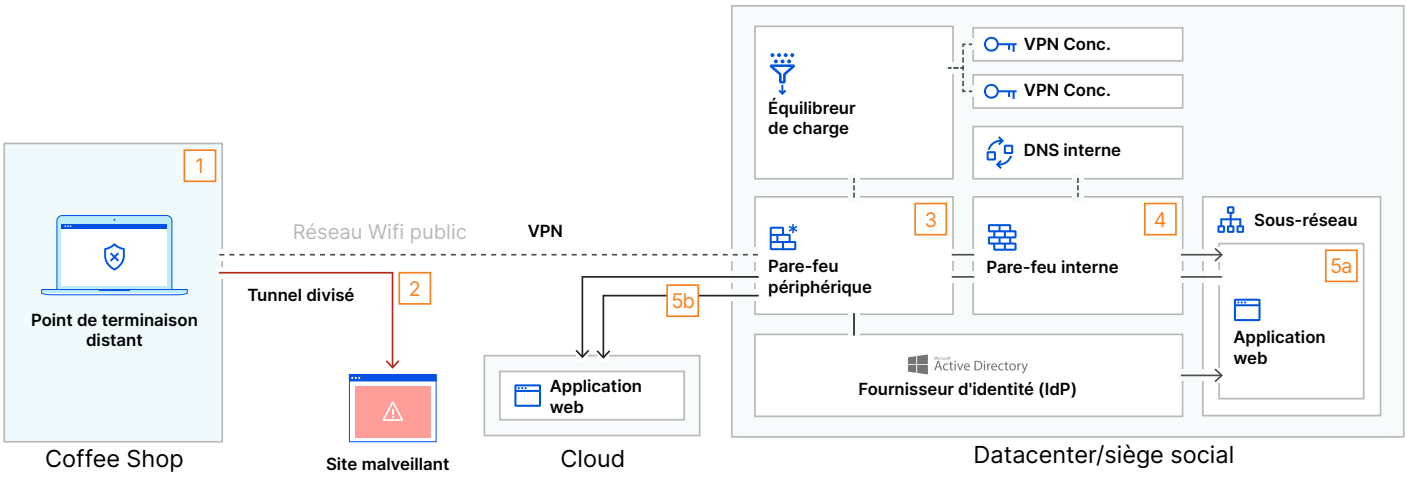
Configuration existante – premier aperçu

Ce diagramme représente une méthode traditionnelle de déploiement d'un accès à distance aux applications web. Ici, un employé en télétravail accède aux ressources de l'entreprise, plus précisément à des applications web privée (auto-hébergée) et publique (dans le Cloud).

Nous avons inclus quelques-unes des mesures de sécurité les plus courantes que toute organisation devrait raisonnablement déployer, notamment un pare-feu périphérique, un pare-feu interne pour la segmentation et un VPN.

De gauche à droite, ce scénario illustre le déroulement d'une session lorsqu'un utilisateur se connecte depuis un lieu public – un scénario sur lequel reposeront les diagrammes de conception suivants.

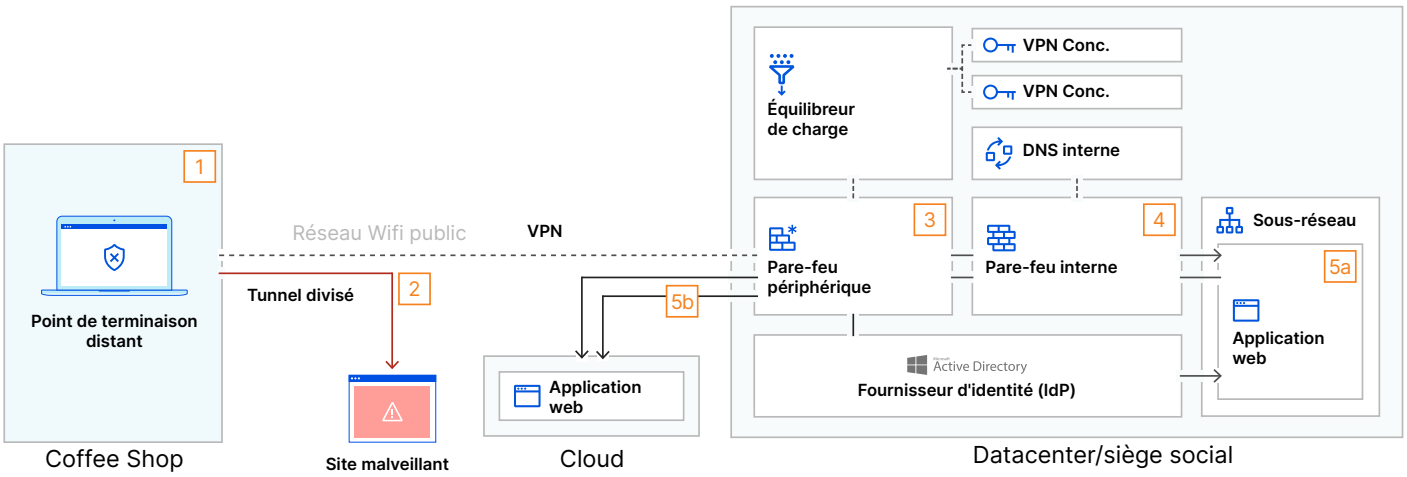
Remarque : ce diagramme représente uniquement les équipements, les appareils et les flux de trafic impliqués dans cette transaction réseau spécifique, et ne fournit pas un instantané complet de toutes les technologies qui seraient présentes dans une architecture réseau existante.



	Action du réseau/de la sécurité
1	Un appareil distant se connecte aux ressources de l'entreprise via un réseau Wifi public
2	L'appareil distant atteint la périphérie de l'entreprise via un client VPN, mais le reste du trafic est acheminé par tunnellisation fractionnée
3	Le VPN se termine au niveau du pare-feu périphérique ou du concentrateur VPN derrière le pare-feu.
4	La politique du pare-feu permet à l'utilisateur distant d'accéder à un sous-réseau avec une application web privée
5	L'utilisateur accède à l'application web via une adresse IP/URL privée **[5a]** ou une URL publique **[5b]** après s'être authentifié auprès du fournisseur d'identité

Configuration existante – failles de sécurité

Dans ce diagramme, une colonne est ajoutée au tableau ci-dessous, présentant les failles de sécurité associées à chaque étape spécifique de ce scénario, qui rendent une organisation vulnérable.

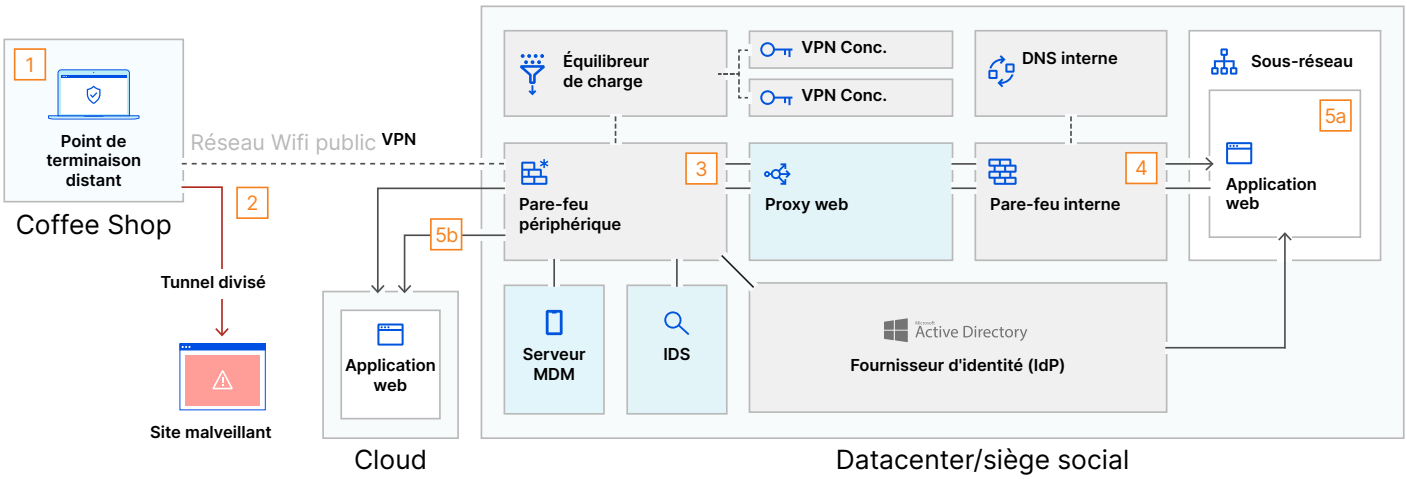


	Action du réseau/de la sécurité	Solution existante pertinente	Faille de la configuration existante
1	Un appareil distant se connecte aux ressources de l'entreprise via un réseau Wifi public	Client VPN d'entreprise	Un appareil non sécurisé sur un réseau Wifi public est une cible pour les acteurs malveillants.
2	Le point de terminaison distant atteint la périphérie de l'entreprise via un client VPN, mais le reste du trafic est acheminé par tunnellisation fractionnée	Client VPN d'entreprise	La sécurité spécifique au VPN ne protège pas le trafic acheminé par tunnellisation fractionnée
3	Le VPN se termine au niveau du pare-feu périphérique ou du concentrateur VPN derrière le pare-feu.	Équilibreur de charge Pare-feu périphérique Concentrateur VPN	Les règles de trafic entrant du pare-feu/VPN peuvent exposer des ports/protocoles à l'Internet, élargissant ainsi la surface d'attaque potentielle.
4	La politique du pare-feu permet à l'utilisateur distant d'accéder à un sous-réseau avec une application web privée	Pare-feu interne	L'utilisateur a accès à des ressources ne correspondant pas à sa fonction
5	L'utilisateur accède à l'application web via une adresse IP/URL privée **[5a]** ou une URL publique **[5b]** après s'être authentifié auprès du fournisseur d'identité	Active Directory DNS interne (privé)	Si le point de terminaison est compromis, l'application/le réseau de l'entreprise est exposé

Configuration existante – compléments de sécurité requis

Pour remédier aux failles du modèle présentées à la page précédente, l'organisation doit maintenant modifier son architecture réseau existante. Dans ce diagramme, une colonne est ajoutée au tableau ci-dessous, détaillant les solutions typiques pour protéger les utilisateurs et les ressources.

La superposition de modules complémentaire de sécurité ajoute à l'environnement existant de la complexité, ainsi que des coûts de gestion permanents, probablement avec plusieurs fournisseurs.



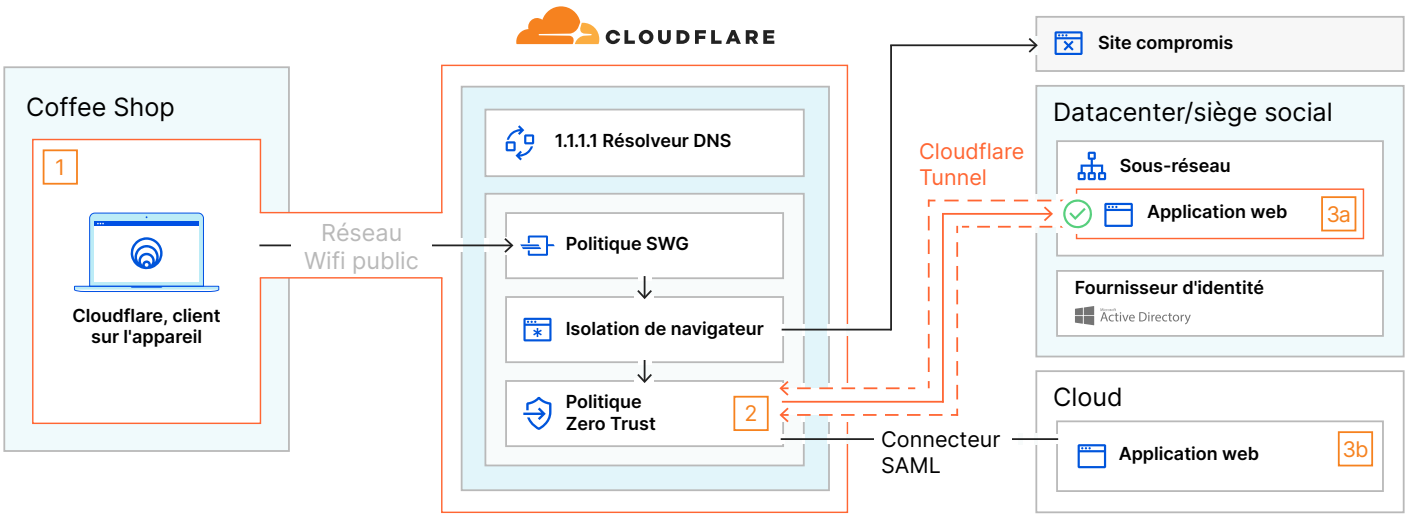
	Action du réseau/de la sécurité	Solution existante pertinente	Faille de la configuration existante	Module complémentaire de sécurité requis
1	Un appareil distant se connecte aux ressources de l'entreprise via un réseau Wifi public	Client VPN d'entreprise	Un appareil non sécurisé sur un réseau Wifi public est une cible pour les acteurs malveillants.	Plateforme de protection des points de terminaison (EPP)
2	L'appareil distant atteint la périphérie de l'entreprise via un client VPN, mais le reste du trafic est acheminé par tunnellisation fractionnée	Client VPN d'entreprise	La sécurité spécifique au VPN ne protège pas le trafic acheminé par tunnellisation fractionnée	Désactiver la tunnellisation fractionnée
3	Le VPN se termine au niveau du pare-feu périphérique ou du concentrateur VPN derrière le pare-feu.	Équilibreur de charge Pare-feu périphérique Concentrateur VPN	Les règles de trafic entrant du pare-feu/VPN peuvent exposer des ports/protocoles à l'Internet, élargissant ainsi la surface d'attaque potentielle.	Système de détection des intrusions (IDS)
4	La politique du pare-feu permet à l'utilisateur distant d'accéder à un sous-réseau avec une application web privée	Pare-feu interne	L'utilisateur a accès à des ressources ne correspondant pas à sa fonction	Proxy web
5	L'utilisateur accède à l'application web via une adresse IP/URL privée [5a] ou une URL publique [5b] après s'être authentifié auprès du fournisseur d'identité	Active Directory DNS interne (privé)	Si le point de terminaison est compromis, l'application/le réseau de l'entreprise est exposé	Serveur de gestion des appareils mobiles (MDM)

Configuration de Cloudflare One

Le diagramme ci-dessous indique comment une organisation peut adopter une approche plus simple et plus efficace pour sécuriser l'accès aux applications en déployant Cloudflare One.

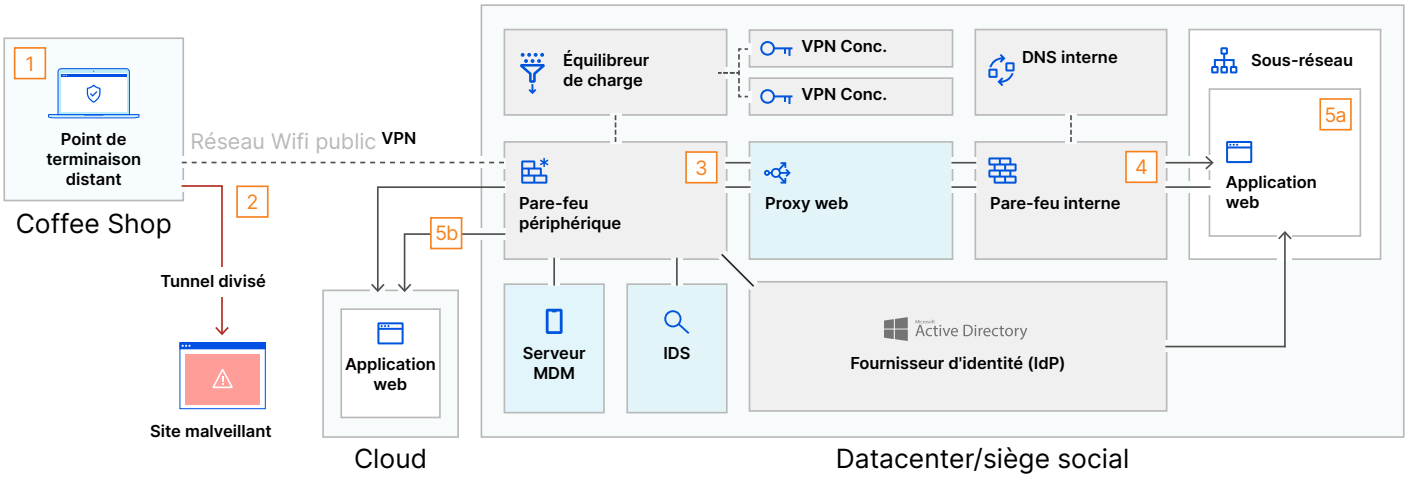
Ici, une grande partie de l'architecture réseau existante précédemment présentée est transférée à Cloudflare, et de nombreux défauts du de la configuration existante sont corrigés, sans qu'il soit nécessaire de déployer des solutions supplémentaires.

Avec Cloudflare One, le trafic entre l'utilisateur distant et les ressources de l'organisation est acheminé sur le réseau mondial de Cloudflare, avec une inspection en une passe. Tous les services présentés ci-dessous sont déployés dans tous les datacenters de Cloudflare, présents dans plus de 250 villes dans plus de 100 pays.

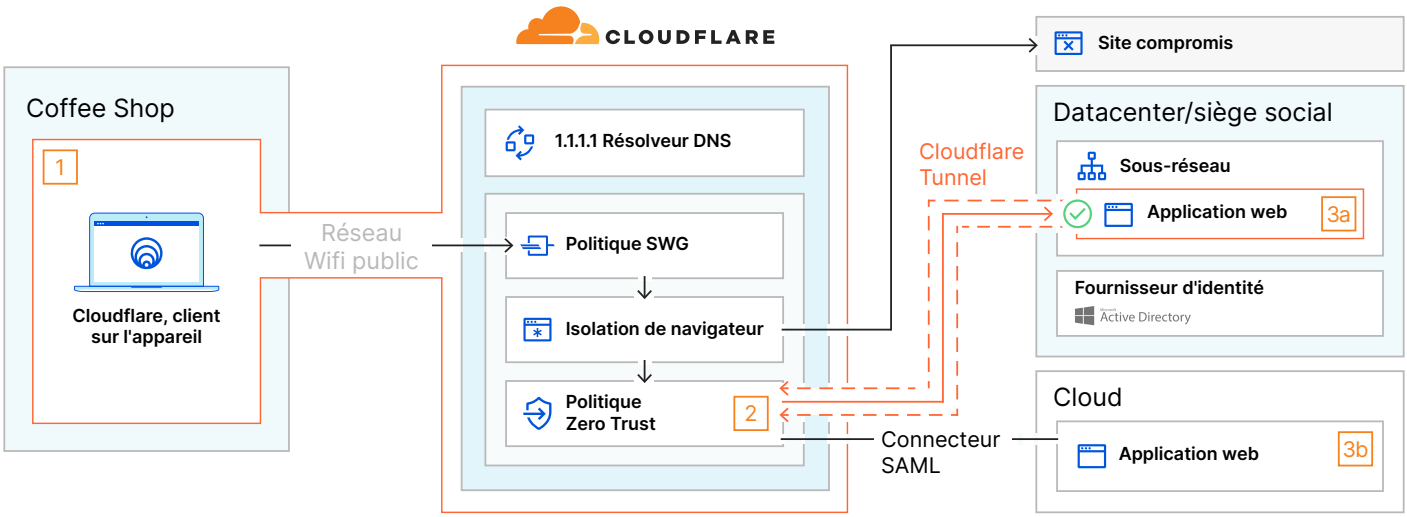


	Action du réseau/de la sécurité	Composant pertinent de Cloudflare One	Correction de la faille de la configuration
1	Un appareil distant se connecte aux ressources de l'entreprise via Cloudflare	Client Cloudflare de l'appareil Politique Secure Web Gateway Isolation du navigateur	Le client local Secure Web Gateway permet à Cloudflare One de filtrer le trafic DNS/HTTP/réseau vers l'appareil de l'utilisateur via une politique de passerelle L'isolation de navigateur absorbe/isole l'impact des attaques de logiciels malveillants lancées depuis les sites web
2	L'utilisateur est soumis aux vérifications du fournisseur d'identité et du niveau de sécurité de l'appareil dans Cloudflare	Politique Zero Trust	La politique Zero Trust effectue une vérification du niveau de sécurité de l'appareil avant d'autoriser l'accès, ce qui réduit le risque de compromission des appareils La politique Zero Trust authentifie l'utilisateur auprès de la ressource, et non auprès du réseau sous-jacent, empêchant tout mouvement latéral
3	Accès à l'application web [privée | publique] directement via le [tunnel Cloudflare | connecteur SAML]	Cloudflare Tunnel 1.1.1.1 Résolveur DNS	Cloudflare Tunnel établit une connexion sécurisée avec l'application web et élimine l'utilisation de règles de pare-feu explicites.

Configuration existante – compléments de sécurité requis



Configuration de Cloudflare One



Configuration existante – compléments de sécurité requis

	Action du réseau/de la sécurité	Solution existante pertinente	Faille de la configuration existante	Module complémentaire de sécurité requis
1	Un appareil distant se connecte aux ressources de l'entreprise via un réseau Wifi public	Client VPN d'entreprise	Un appareil non sécurisé sur un réseau Wifi public est une cible pour les acteurs malveillants.	Plateforme de protection des points de terminaison (EPP)
2	L'appareil distant atteint la périphérie de l'entreprise via un client VPN, mais le reste du trafic est acheminé par tunnellisation fractionnée	Client VPN d'entreprise	La sécurité spécifique au VPN ne protège pas le trafic acheminé par tunnellisation fractionnée	Désactiver la tunnellisation fractionnée
3	Le VPN se termine au niveau du pare-feu périphérique ou du concentrateur VPN derrière le pare-feu.	Équilibreur de charge Pare-feu périphérique Concentrateur VPN	Les règles de trafic entrant du pare-feu/VPN peuvent exposer des ports/protocoles à l'Internet, élargissant ainsi la surface d'attaque potentielle.	Système de détection des intrusions (IDS)
4	La politique du pare-feu permet à l'utilisateur distant d'accéder à un sous-réseau avec une application web privée	Pare-feu interne	L'utilisateur a accès à des ressources ne correspondant pas à sa fonction	Proxy web
5	L'utilisateur accède à l'application web via une adresse IP/URL privée **[5a]** ou une URL publique **[5b]** après s'être authentifié auprès du fournisseur d'identité	Active Directory DNS interne (privé)	Si le point de terminaison est compromis, l'application/le réseau de l'entreprise est exposé	Serveur de gestion des appareils mobiles (MDM)

Configuration de Cloudflare One

	Action du réseau/de la sécurité	Composant pertinent de Cloudflare One	Correction de la faille de la configuration
1	Un appareil distant se connecte aux ressources de l'entreprise via Cloudflare	**Client Cloudflare de l'appareil** **Politique Secure Web Gateway** **Isolation du navigateur**	Le client local Secure Web Gateway permet à Cloudflare One de filtrer le trafic DNS/HTTP/réseau vers l'appareil de l'utilisateur via une politique de passerelle L'isolation de navigateur absorbe/isole l'impact des attaques de logiciels malveillants lancées depuis les sites web
2	L'utilisateur est soumis aux vérifications du fournisseur d'identité et du niveau de sécurité de l'appareil dans Cloudflare	**Politique Zero Trust**	La politique Zero Trust effectue une vérification du niveau de sécurité de l'appareil avant d'autoriser l'accès, ce qui réduit le risque de compromission des appareils La politique Zero Trust authentifie l'utilisateur auprès de la ressource, et non auprès du réseau sous-jacent, empêchant tout mouvement latéral
3	Accès à l'application web [privée | publique] directement via le [tunnel Cloudflare | connecteur SAML]	**Cloudflare Tunnel** **1.1.1.1 Résolveur DNS**	Cloudflare Tunnel établit une connexion sécurisée avec l'application web et élimine l'utilisation de règles de pare-feu explicites.

Scénarios d’utilisation 2 : Filtrage DNS

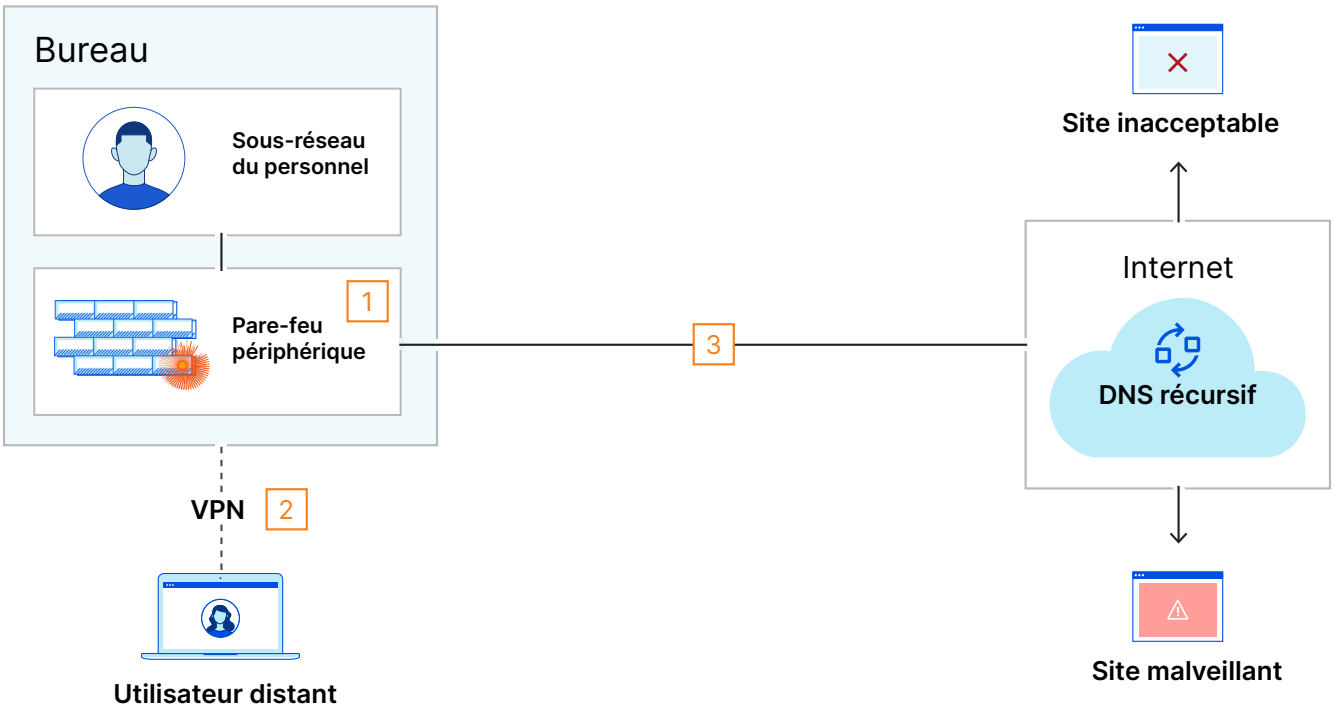
Configuration existante – premier aperçu

Ce diagramme représente la manière dont les organisations mettent en œuvre le filtrage DNS pour le personnel présent sur site et en télétravail dans un environnement existant.

En général, le filtrage DNS pour les organisations est assuré via les fonctionnalités intégrées des solutions sur site (par exemple, un pare-feu). Les requêtes des utilisateurs en télétravail sont transmises à travers ce pare-feu, le trafic étant d'abord acheminé à travers un VPN à tunnel complet.

Pour résoudre les sites web, l'organisation transmet ses requêtes DNS à un DNS récursif (par exemple, le 8.8.8.8 de Google).

Remarque : comme dans les autres chapitres de ce guide, cet environnement existant ne représente pas toutes les technologies présentes dans une agence, mais uniquement celles impliquées dans ce scénario d'utilisation spécifique.



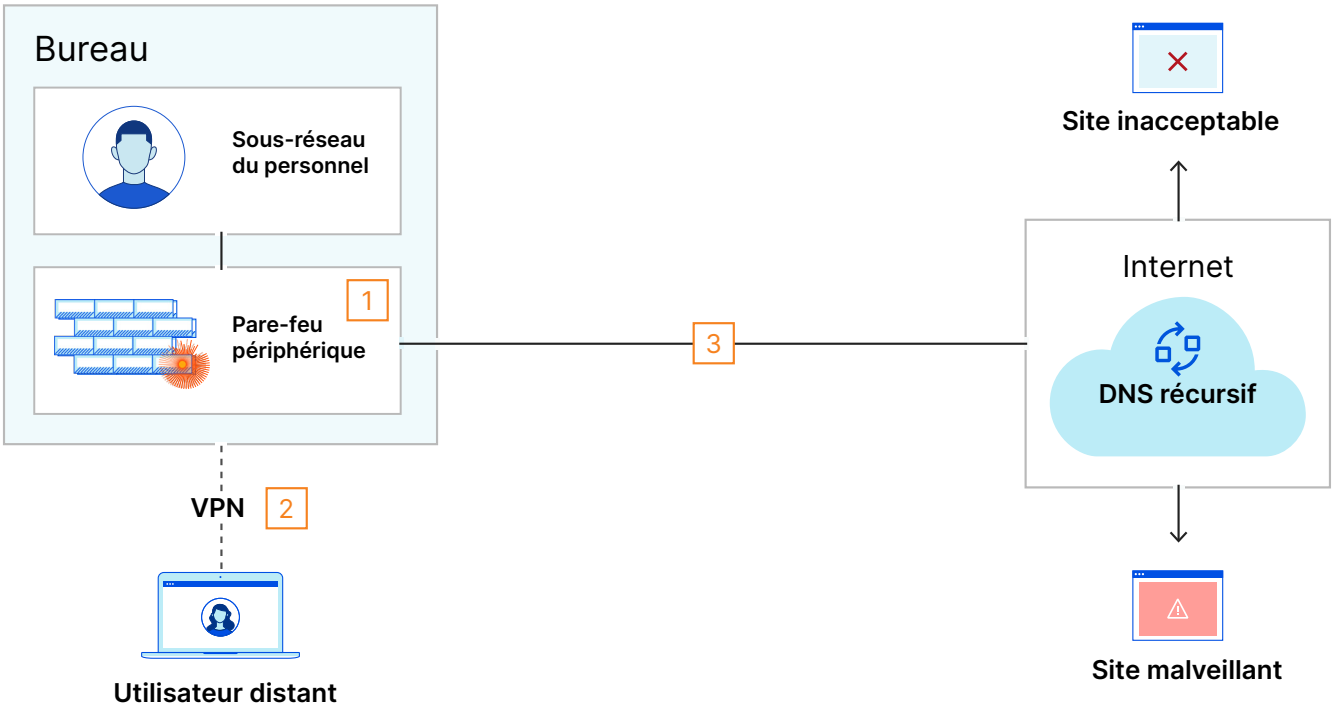
	Événement lié au DNS
1	Les requêtes DNS d'un utilisateur sur site sont filtrées, pour des raisons de sécurité, par la fonctionnalité intégrée du pare-feu périphérique
2	Les requêtes DNS d'un utilisateur en télétravail sont filtrées après qu'il se connecte au tunnel VPN complet de l'organisation
3	Les requêtes DNS sortantes sont transmises en clair.

Modèle existant – failles opérationnelles

Dans ce diagramme, une colonne est ajoutée au tableau ci-dessous, présentant les défis associés à ce modèle traditionnel.

Le principal défi est que l'utilisation d'équipements matériels locaux pour assurer le filtrage DNS à grande échelle finira par grever les performances pour tous les utilisateurs, particulièrement si ce matériel est également responsable d'autres services essentiels (par exemple, la terminaison du VPN de l'utilisateur en télétravail).

En outre, l'envoi de requêtes DNS sans chiffrement (qui a lieu par défaut) crée un nouveau vecteur d'attaque, dont le risque est inconnu.



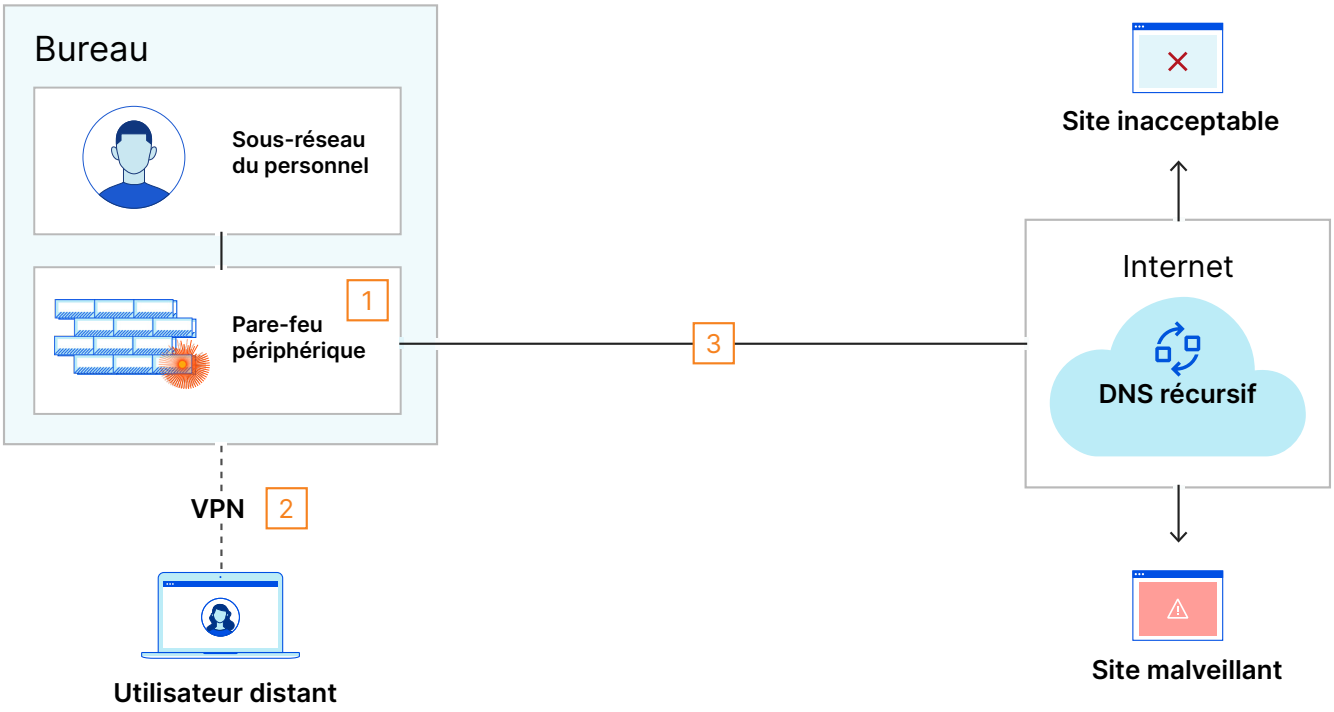
	Événement lié au DNS	Composants pertinents	Faille de la configuration
1	Les requêtes DNS d'un utilisateur sur site sont filtrées, pour des raisons de sécurité, par la fonctionnalité intégrée du pare-feu périphérique	Pare-feu périphérique	Se fier au pare-feu périphérique pour traiter un trop grand nombre d'opérations essentielles peut dégrader les performances pour l'ensemble de l'organisation.
2	Les requêtes DNS d'un utilisateur en télétravail sont filtrées après qu'il se connecte au tunnel VPN complet de l'organisation	Concentrateur VPN Pare-feu périphérique	Un VPN à tunnel complet exerce une « double contrainte » sur les paquets Internet, ce qui peut créer un goulet d'étranglement pour l'ensemble de l'organisation.
3	Les requêtes DNS sortantes sont transmises en clair.	UDP 53	Le trafic DNS via le port UDP 53 n'est pas chiffré, et n'est donc pas privé. Toute personne observant cette faille peut scruter le comportement de l'utilisateur sur le web

Configuration existante – modifications du réseau requises

Pour remédier aux failles de la configuration présentées à la page précédente, l'organisation doit maintenant modifier son architecture réseau existante. Dans ce diagramme, une colonne supplémentaire est ajoutée au tableau ci-dessous, présentant les solutions communes avec leurs inconvénients particuliers.

Ici, l'achat de nouveau matériel pour gérer davantage d'utilisateurs ou augmenter la bande passante disponible entraînera des dépenses d'investissement et d'exploitation plus élevées dans le temps.

Les organisations qui tentent d'étendre cette approche par elles-mêmes se heurtent souvent à des difficultés de croissance considérables. En réalité, de nombreuses organisations évitent complètement le filtrage DNS, précisément à cause de ces problèmes opérationnels.



	Événement lié au DNS	Composants pertinents	Faille de la configuration	Solution autre que Cloudflare
1	Les requêtes DNS d'un utilisateur sur site sont filtrées, pour des raisons de sécurité, par la fonctionnalité intégrée du pare-feu périphérique	Pare-feu périphérique	Se fier au pare-feu périphérique pour traiter un trop grand nombre d'opérations essentielles peut dégrader les performances pour l'ensemble de l'organisation.	Filtre DNS discret
2	Les requêtes DNS d'un utilisateur en télétravail sont filtrées après qu'il se connecte au tunnel VPN complet de l'organisation	Concentrateur VPN Pare-feu périphérique	Un VPN à tunnel complet exerce une « double contrainte » sur les paquets Internet, ce qui peut créer un goulet d'étranglement pour l'ensemble de l'organisation.	Augmenter la bande passante du FAI Matériel plus performant Activer la tunnellisation fractionnée
3	Les requêtes DNS sortantes sont transmises en clair.	UDP 53	Le trafic DNS via le port UDP 53 n'est pas chiffré, et n'est donc pas privé. Toute personne observant cette faille peut scruter le comportement de l'utilisateur sur le web	DNS via TLS/HTTPS

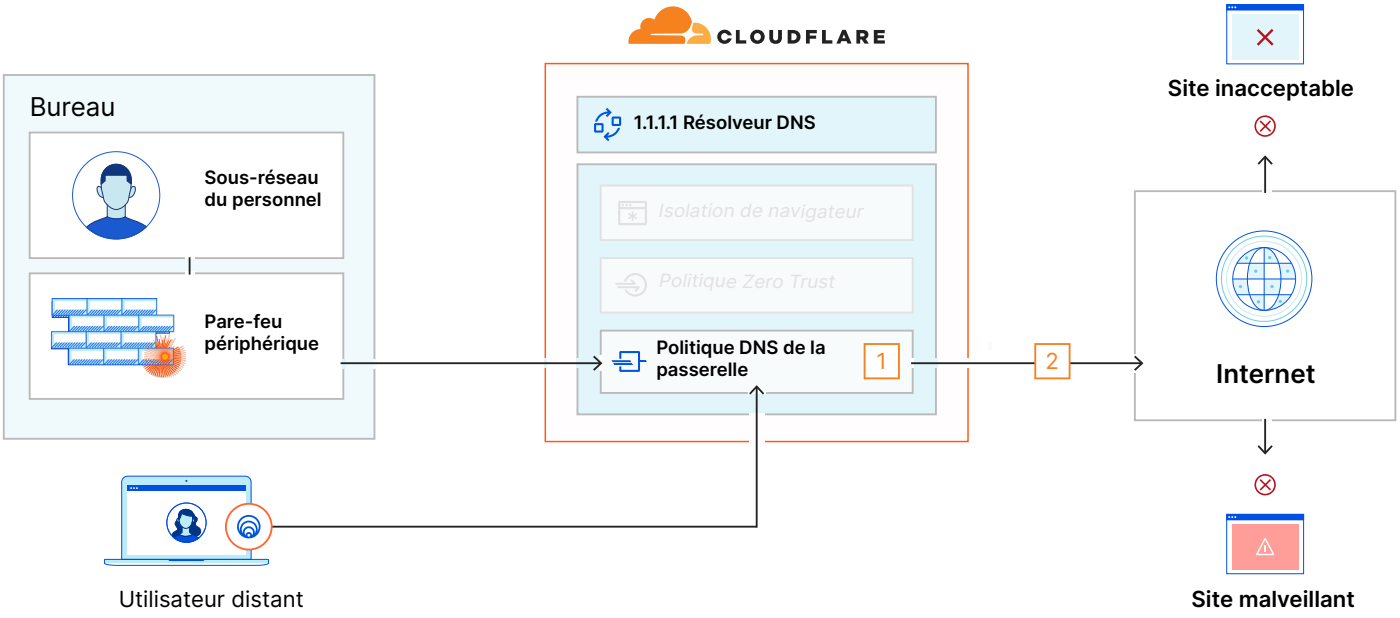
Configuration de Cloudflare One

Les organisations qui adoptent Cloudflare One dirigent leur trafic vers le réseau mondial de Cloudflare et peuvent appliquer un filtrage DNS pour l'ensemble de leur personnel, sans se soucier des limites opérationnelles de leur matériel local.

Le filtre DNS de Cloudflare est facile à déployer pour les utilisateurs sur site et en télétravail :

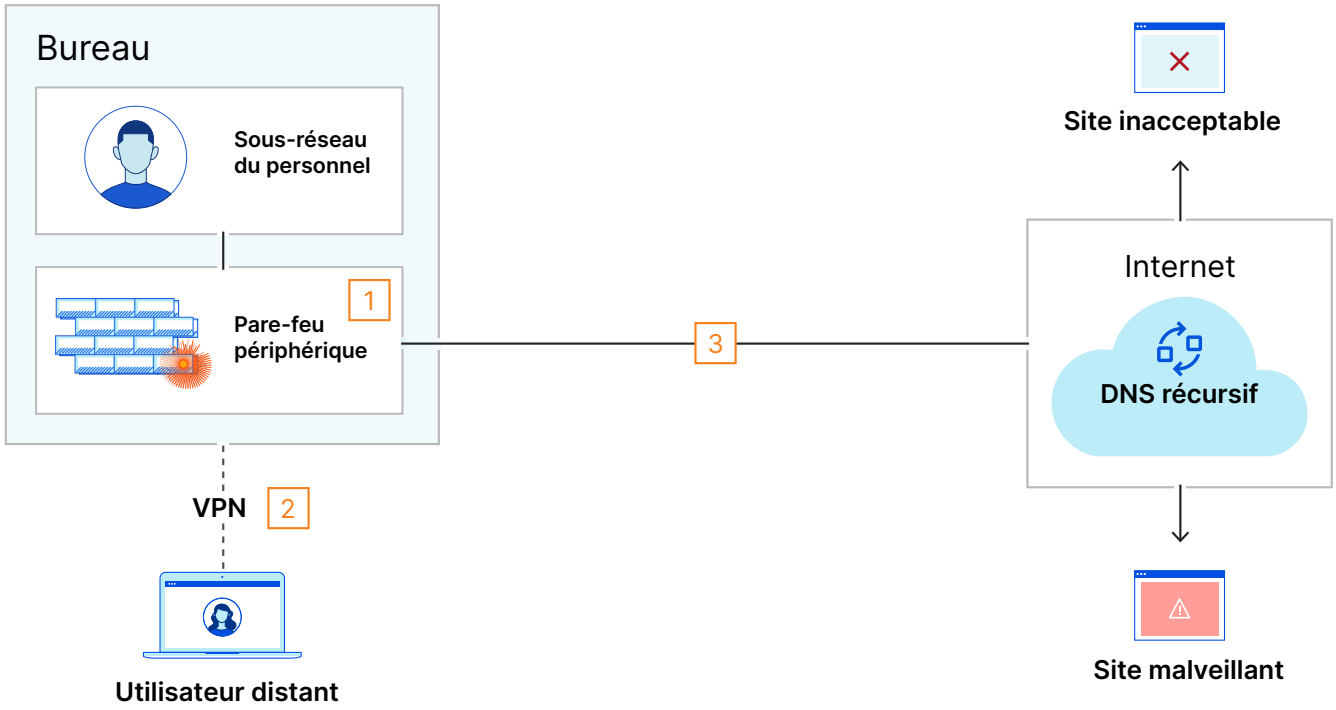
- Le trafic des utilisateurs à l'agence est transmis à Cloudflare sur la base de l'adresse IP sortante du pare-feu périphérique
- Le trafic des utilisateurs en télétravail est transmis à Cloudflare depuis notre client sur l'appareil

De plus, le résolveur DNS 1.1.1.1 de Cloudflare prend en charge le DNS avec TLS/HTTPs, remédiant à la faille de sécurité expliquée dans l'environnement existant.

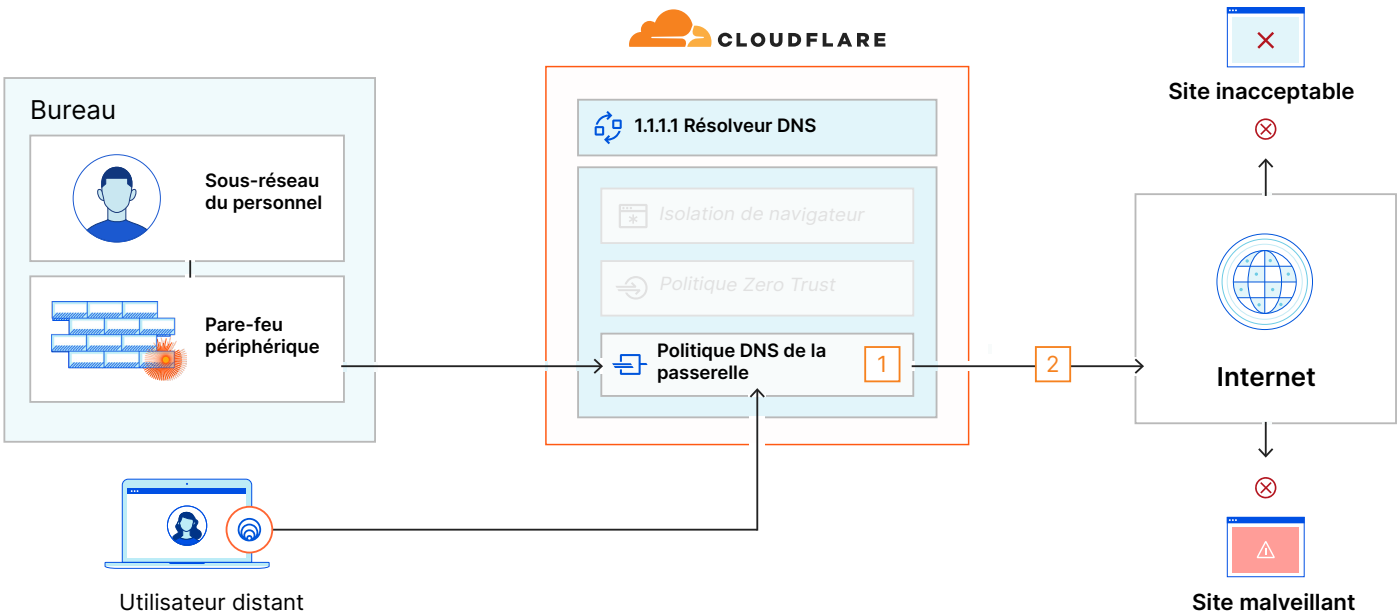


	Événement lié au DNS	Composant pertinent de Cloudflare One	Correction de la faille de la configuration
1	Le contenu des requêtes DNS des utilisateurs sur site et en télétravail est filtré par Cloudflare.	Passerelle web sécurisée	Les politiques DNS de la **passerelle** soulagent le matériel local du filtrage DNS (ou le traitent pour la première fois)
2	Les requêtes DNS de l'organisation sont chiffrées avant leur transmission.	1.1.1.1 Résolveur DNS	Le **résolveur DNS 1.1.1.1** de Cloudflare prend en charge le DNS avec TLS/HTTPs, permettant ainsi de chiffrer les requêtes DNS et de gêner les tentatives de reconnaissance hostiles

Configuration existante



Modèle Cloudflare One



Configuration existante

	Événement lié au DNS	Composants pertinents	Faille de la configuration	Solution autre que Cloudflare
1	Les requêtes DNS d'un utilisateur sur site sont filtrées, pour des raisons de sécurité, par la fonctionnalité intégrée du pare-feu périphérique	Pare-feu périphérique	Se fier au pare-feu périphérique pour traiter un trop grand nombre d'opérations essentielles peut dégrader les performances pour l'ensemble de l'organisation.	Filtre DNS discret
2	Les requêtes DNS d'un utilisateur en télétravail sont filtrées après qu'il se connecte au tunnel VPN complet de l'organisation	Concentrateur VPN Pare-feu périphérique	Un VPN à tunnel complet exerce une « double contrainte » sur les paquets Internet, ce qui peut créer un goulet d'étranglement pour l'ensemble de l'organisation.	Augmenter la bande passante du FAI Matériel plus performant Activer la tunnellisation fractionnée
3	Les requêtes DNS sortantes sont transmises en clair.	UDP 53	Le trafic DNS via le port UDP 53 n'est pas chiffré, et n'est donc pas privé. Toute personne voyant cela peut scruter le comportement de l'utilisateur sur le web	DNS via TLS/HTTPS

Configuration de Cloudflare One

	Événement lié au DNS	Composant pertinent de Cloudflare One	Correction de la faille de la configuration
1	Le contenu des requêtes DNS des utilisateurs sur site et en télétravail est filtré par Cloudflare.	Passerelle web sécurisée	Les politiques DNS de la passerelle soulagent le matériel local du filtrage DNS (ou le traitent pour la première fois)
2	Les requêtes DNS de l'organisation sont chiffrées avant leur transmission.	1.1.1.1 Résolveur DNS	Le résolveur DNS 1.1.1.1 de Cloudflare prend en charge le DNS avec TLS/HTTPs, permettant ainsi de chiffrer les requêtes DNS et de gêner les tentatives de reconnaissance hostiles