Netskope ZTNA
(Zero Trust Network Access)

La solution « Zero Trust Network Access » (ZTNA) est un modèle de sécurité qui repose sur le principe de "ne jamais faire confiance" en limitant les accès et en surveillant constamment les activités.

Contrairement aux approches traditionnelles qui considèrent les utilisateurs internes comme fiables, en leur laissant libre accès au réseau du CNPF, le ZTNA nécessite une authentification et une autorisation rigoureuses pour chaque demande d'accès à ce dernier, qu'elle provienne d'un utilisateur interne ou externe.

BERNOIS Damien

CNPF Centre National de la Propriété Forestière

Table des matières

1. Présentation du fonctionnement du ZTNA 3
2. Une alternative au VPN 4
3. L'utilisation du service Netskope au sein du CNPF 5
4. Logique de gestion des droits des agents Netskope 7
5. Mise en place du système d'enrôlement 8
6. Utilisation de l'agent Netskope pour les utilisateurs 9
A. Interface des services Netskope 9
B. Détails du panneau de configuration de l'agent Netskope ..... **Erreur ! Signet non défini.**

1. Présentation du fonctionnement du ZTNA

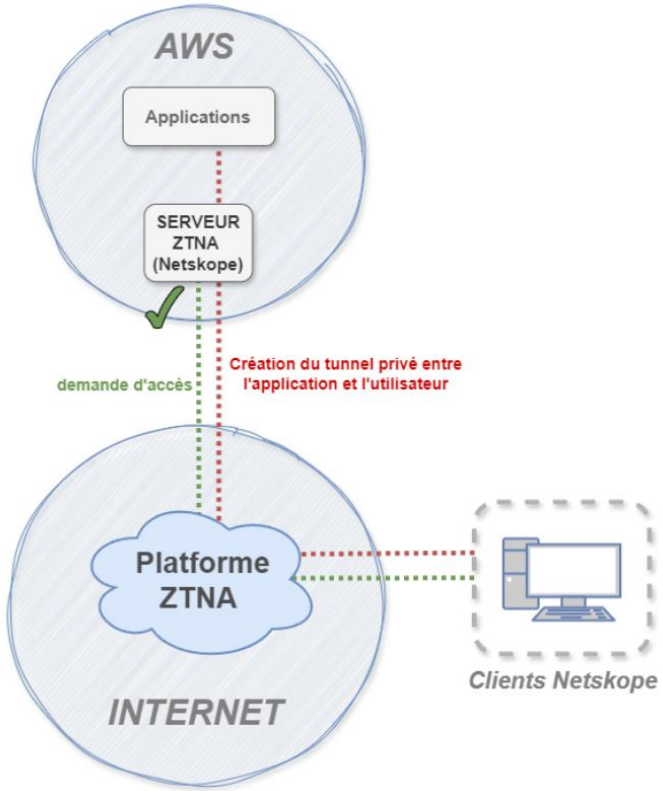
Le ZTNA a pour philosophie de ne laisser aucun trafic s'effectuer d'une part et d'autre de son réseau. Afin qu'un utilisateur interne (personnel sur site) ou externe (personnel hors site ou autres) puisse accéder au réseau, il lui faudra nécessairement un agent Netskope.

L'agent Netskope est disponible pour les systèmes d'exploitation les plus courants : iOS, Android, Linux, Windows et MacOS.

Le serveur ZTNA va pouvoir se baser sur plusieurs critères définis par l'administrateur afin de savoir s'il doit autoriser ou non un utilisateur Netskope à accéder aux ressources du réseau tel que :

- *L'identification et l'authentification de l'agent.*
- *La localisation de la machine (site, hors site).*
- *La fréquence de demandes parvenant de cet agent.*
- *La date.*
- *La conformité du poste de l'utilisateur (version du système, présence d'un antivirus, etc).*

Ce serveur ZTNA va servir de passerelle entre les postes utilisateurs et les applications. Il permet de créer un canal sécurisé unique (par communication entre une application et un utilisateur), privé et chiffré (par chiffrement TLS) entre ces deux derniers.



Le serveur va créer ce canal et donner accès aux applications pour l'utilisateur en interceptant la requête (par exemple : « auth-cnpf.fr » ou l'adresse IP).

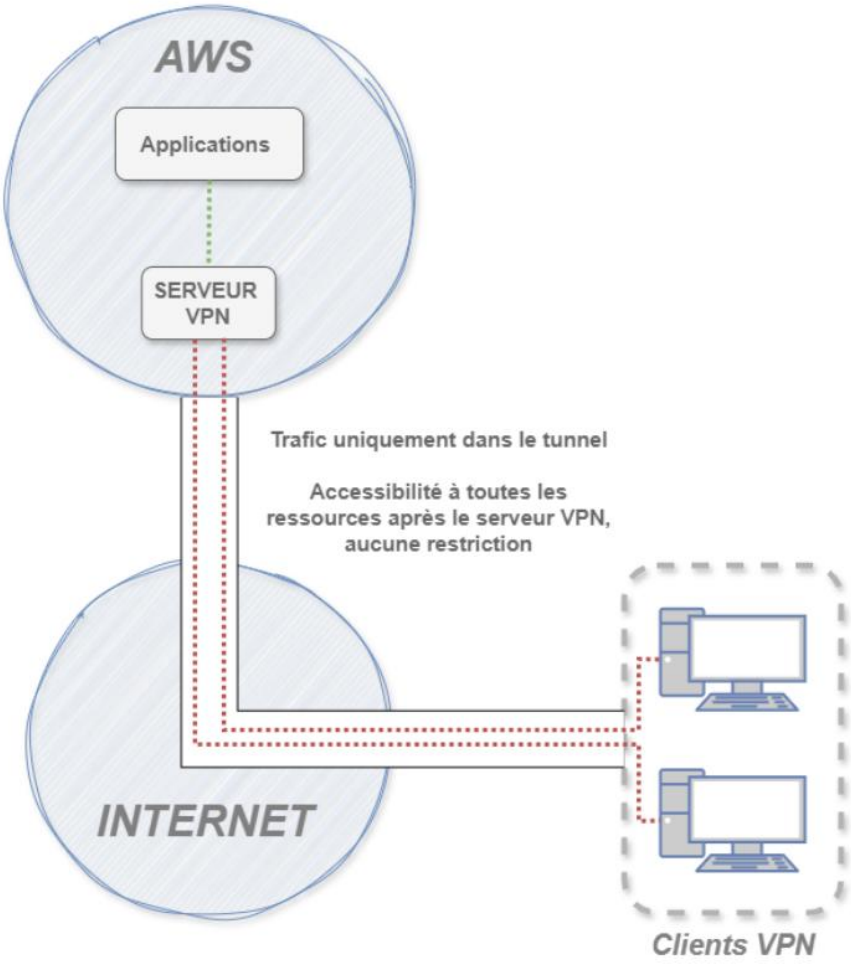
2. Une alternative au VPN

Traditionnellement, l'utilisation d'un VPN comportait des risques de sécurité liés à son fonctionnement. En revanche, le ZTNA permet de s'affranchir de ces problèmes grâce à sa flexibilité et son fonctionnement mieux adapté aux besoins d'aujourd'hui.

Un accès VPN traditionnel d'un utilisateur à une ou plusieurs application(s) se fait par l'accès à un tunnel créé et maintenu par le VPN entre les clients et les ressources du réseau.

Ce fonctionnement soulève de nombreux risques tels que :

- *Aucune sécurité et vérification d'une part et autre du tunnel VPN.*
- *Le tunnel donne accès à toutes les ressources, aucune restriction d'accès lorsqu'un utilisateur est dans ce tunnel.*
- *Gourmands en ressources (souvent coûts élevés du trafic inter-tunnel).*
- *Retard du VPN par rapport à la mobilité et aux besoins du cloud.*
- *Ouverture de port lors de la communication, possibilité de propager une infection dans le réseau.*



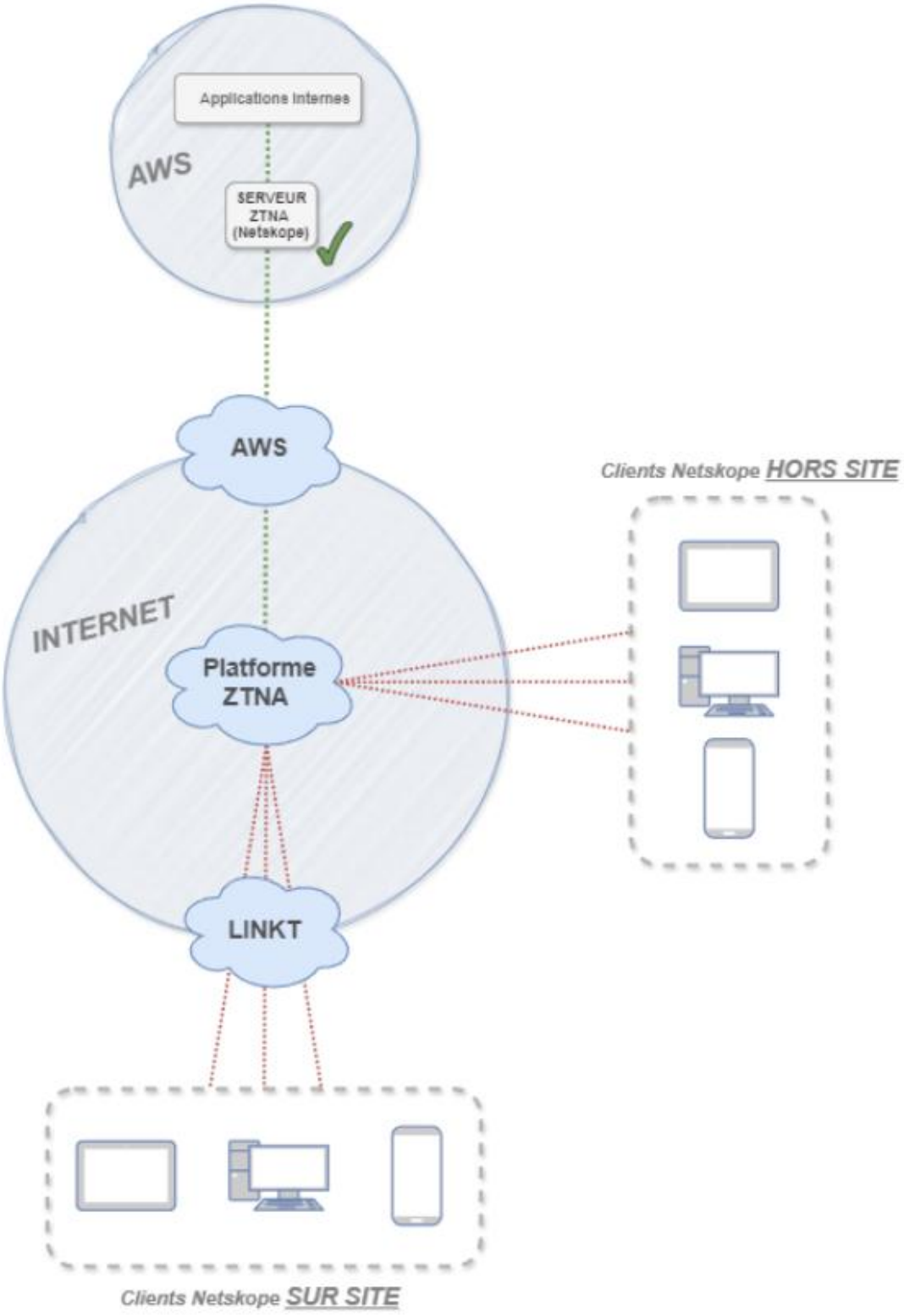
3. L'utilisation du service Netskope au sein du CNPF

La mise en place du service ZTNA de Netskope sur le réseau du CNPF apporte de nombreux avantages par rapport au VPN classique mis en place ultérieurement. Dont principalement en termes de sécurité et de gestion du flux vers les ressources, comme expliqué précédemment.

Ces avantages sont des clés majeures afin d'assurer l'intégrité et la sécurité des ressources du CNPF. Chaque utilisateur aura accès strictement à la ressource dont il aura besoin et à laquelle il sera autorisé à communiquer, et ce grâce à la gestion et la flexibilité qu'offre le service ZTNA Netskope.

Netskope permet tout comme un VPN de donner un accès aux ressources de destination que l'utilisateur soit sur site (en interne/« on premise ») ou hors site (à distance/« remote »).

Actuellement notre unique serveur Netskope sur trouve sur AWS. Par la suite, nous envisageons de mettre en place un deuxième serveur Netskope sur AWS afin qu'il puisse prendre la relève et assuré une redondance du service si le premier serveur vient à ne plus être fonctionnel et/ou ne plus pouvoir assuré son service.


Applications Internes
AWS
SERVEUR ZTNA (Netskope)
AWS
INTERNET
Platforme ZTNA
LINKT
Clients Netskope HORS SITE
Clients Netskope SUR SITE

4. Logique de gestion des droits des agents Netskope

Netskope nous permet de pouvoir manager chacun des flux provenant des agents rattachés à notre service Netskope, vers nos ressources. De ce fait, nous partons du postulat que seulement et uniquement les machines (quelles soient internes ou externes au réseau du CNPF) ayant un agent Netskope répertorié dans serveur Netskope pourront demander et avoir un accès à une application quelconque dans nos ressources.

Lorsqu'un personnel vient à partir de l'entreprise, nous désactivons son compte sur l'annuaire LDAP, par la suite, la licence de son agent Netskope sera supprimé, il ne pourra donc plus accéder à notre serveur Netskope et donc ne plus accéder à nos ressources, malgré qu'il ait pu garder une machine du parc informatique du CNPF.

Pour gérer des demandes, nous avons créé différents groupes qui se basent sur l'importation des différents groupes et utilisateurs répertoriés dans l'annuaire LDAP.

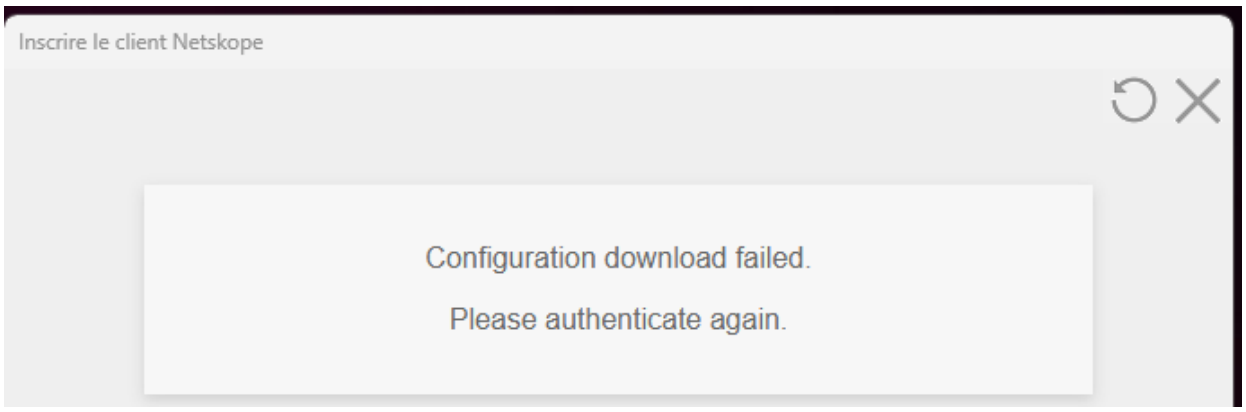
5. Mise en place du système d'enrôlement

Le système d'enrôlement proposé par Netskope a pour fonctionnalité première de s'assurer, lors de l'intégration d'un nouvel agent sur notre serveur Netskope Publisher, que ce dernier soit légitime à être enregistré, ainsi que de récupérer les configurations adéquates.

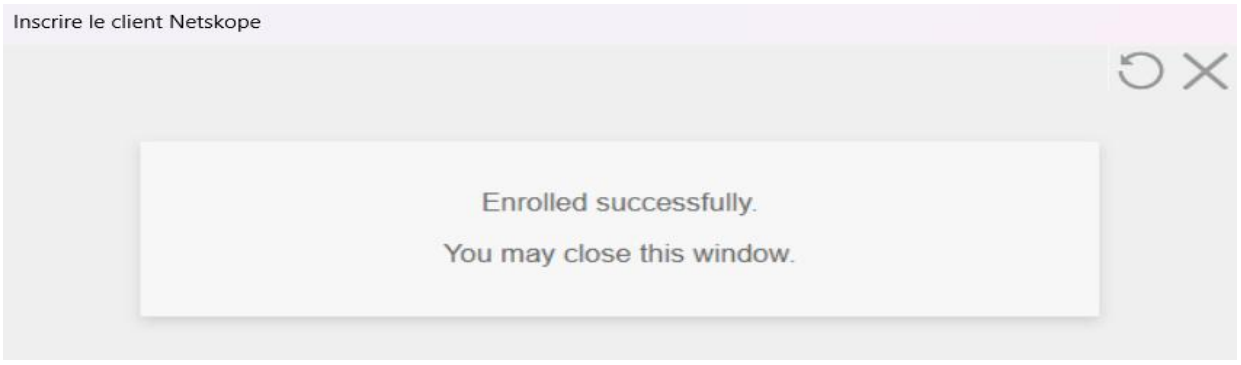
De plus, Netskope conseille fortement de mettre en place cette fonctionnalité afin de pallier les failles de sécurité récemment soulignées par ce dernier. Effectivement, un utilisateur quelconque extérieur pouvait, à l'aide des informations du tenant, domain et host de notre organisation, intégrer notre infrastructure ZTNA et ainsi pouvoir communiquer avec le reste de notre infrastructure.

À la suite de cette mise en place, lors du déploiement du logiciel sur un poste utilisateur, ce dernier devra avoir conscience de 3 points : l'ID de l'organisation, l'ID de l'enrôlement, ainsi que l'ID du chiffrement de l'enrôlement. Sans ces 3 éléments, la mise à jour de la configuration ne pourra pas être assurée.

- Déploiement avec l'ancienne commande (sans les options de l'enrôlement) :

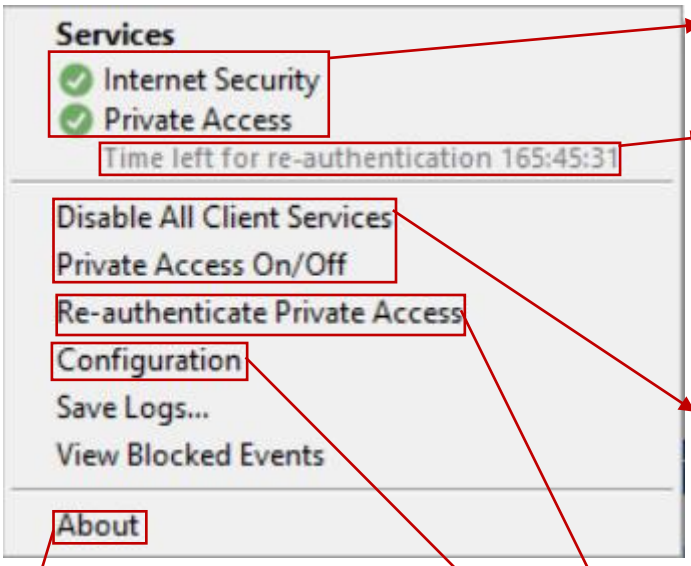


- Déploiement avec la nouvelle commande (avec les options de l'enrôlement) :



6. Utilisation de l'agent Netskope pour les utilisateurs

A. Interface des services Netskope



Lien privé avec le serveur Netskope actif

Temps avant la prochaine authentification nécessaire afin d'accéder aux services Netskope et donc aux ressources (avec un temps de souplesse de 10 minutes)

Activation/désactivation des services et liens de l'agent vers le serveur Netskope (accessible au groupe SDN-ONLY)

Forcer la réauthentification de l'utilisateur

Version de l'agent Netskope

Détails de la configuration de l'agent Netskope