CHIMERE

OSSIR

Software-Defined Perimeter

13 février 2024

QUI SOMMES NOUS ?

2018 Ingénieurs Thales

01 / 2021 Chimere *by* Thales

10 / 2022 Spin-off

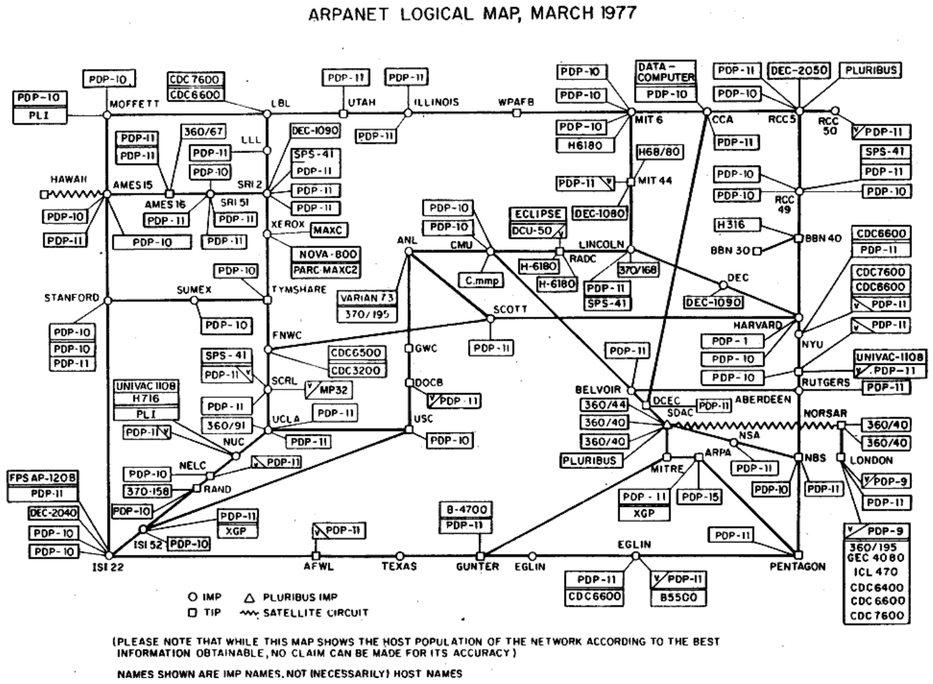
Guillaume-Alexandre Chaizy
CEO

Gabriel Ladet
CTO

AGENDA

- Une problématique aussi vieille qu’internet
- Le SDP, une solution ?
- Architectures et solutions SDP actuelles
- Le SDP par Chimere
- Question/Réponse

INTERNET ET SES ORIGINES

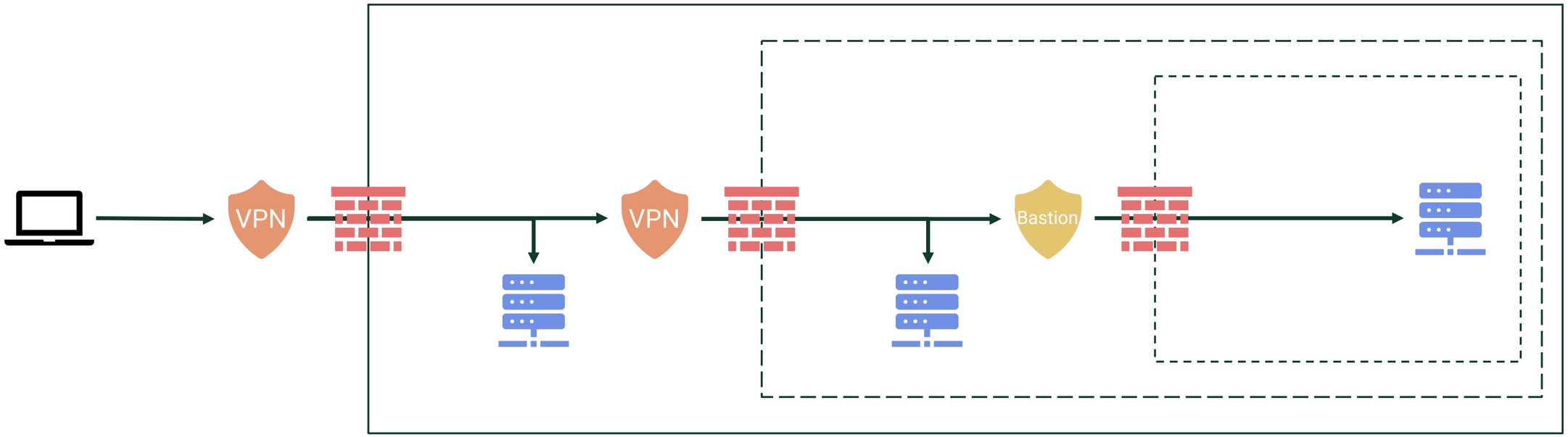


En **1974**, les protocoles TCP et IP sont conçus à une époque et dans un contexte très différents de ceux que l'on connait aujourd'hui : il n'y a pas encore de **cybermenaces** et le **réseau est peu étendu**.

Carte logique du réseau ARPANET en mars 1977, exposée au musée de l'Histoire de l'ordinateur.

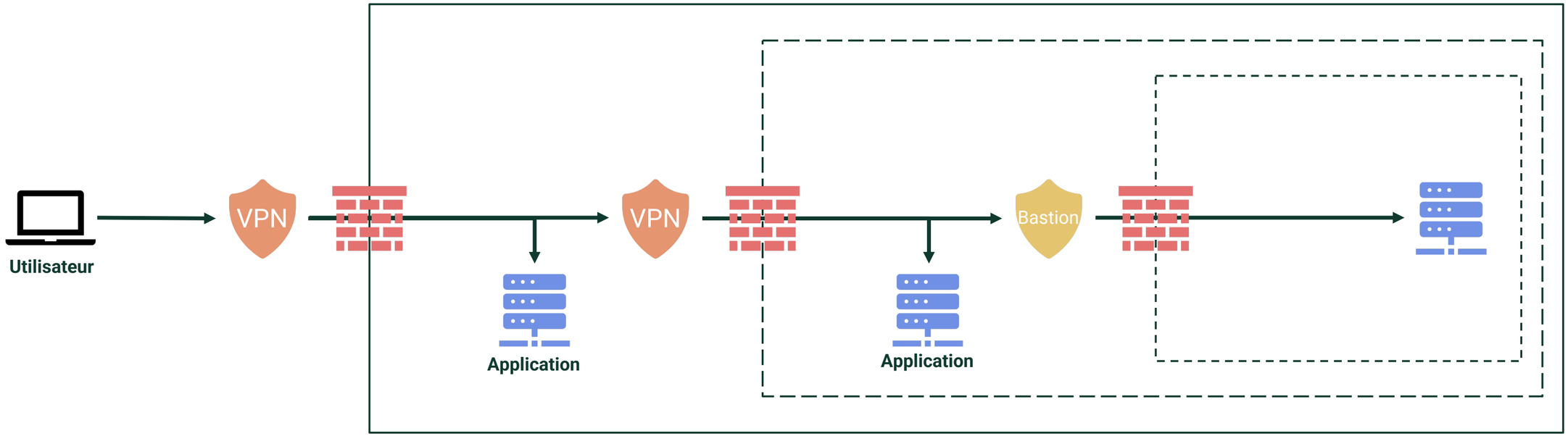
SÉCURISER SON EXPOSITION ET LES ACCÈS

Ajouter des couches de protection

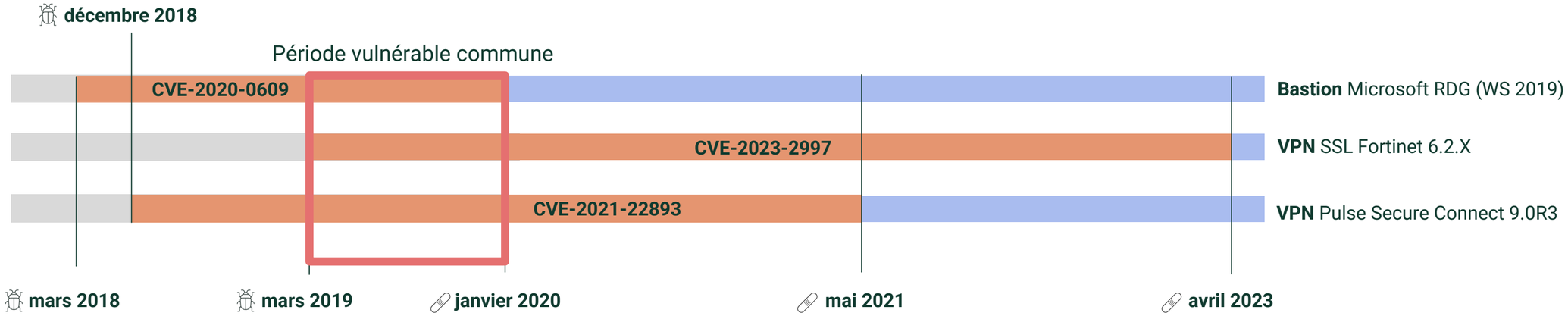


VULNERABILITÉS

Ajouter des couches de protection

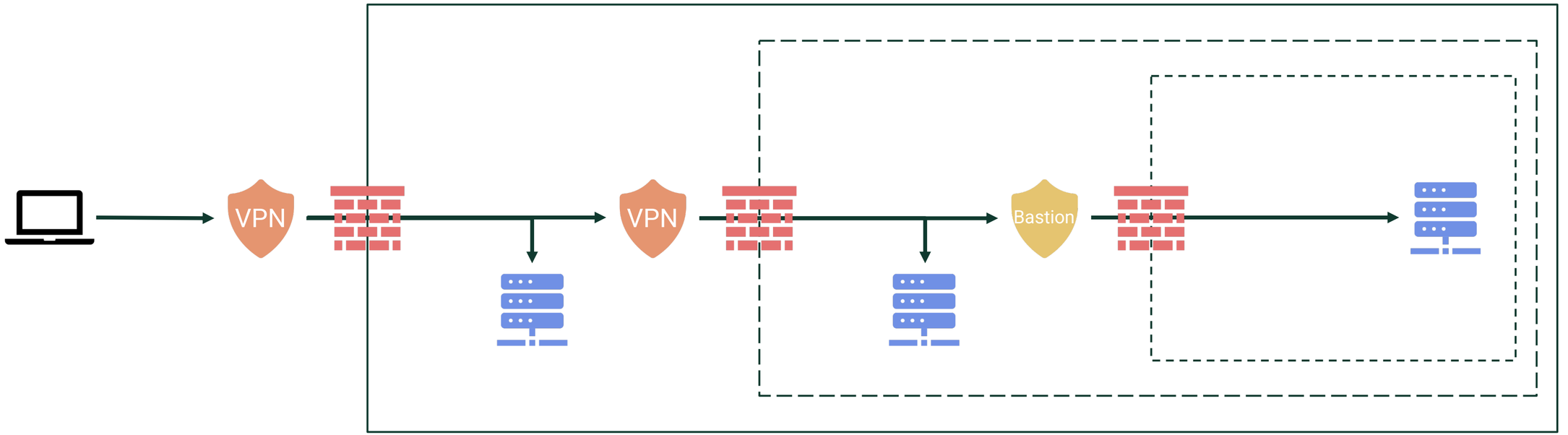


Timeline



3 PROBLÉMATIQUES PRINCIPALES

Ajouter des couches de protection



Exposition des services

Défense périmétrique

Contrôles d’accès

SDP

Software-Defined Perimeter

SDP PAR LA CSA (CLOUD SECURITY ALLIANCE)

SDP apporte la faculté de :

- Cacher les réseaux et les ressources
- Interdire les accès aux utilisateurs non autorisés
- Apporter un modèle de politique d’accès basé sur l’identité
- Fournir de la micro-segmentation

Software-Defined Perimeter (SDP) Specification v2.0 | CSA (cloudsecurityalliance.org).

ARCHITECTURE SDP

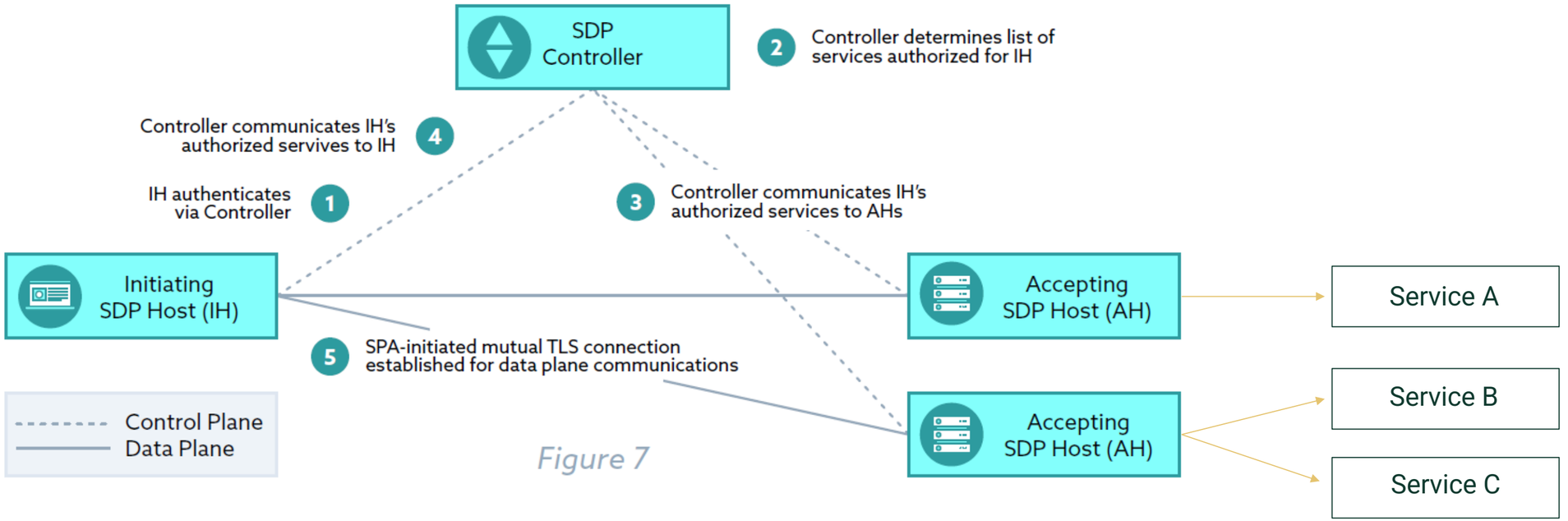


Figure 7

Software-Defined Perimeter (SDP) Specification v2.0 | CSA (cloudsecurityalliance.org).

ARCHITECTURE SDP

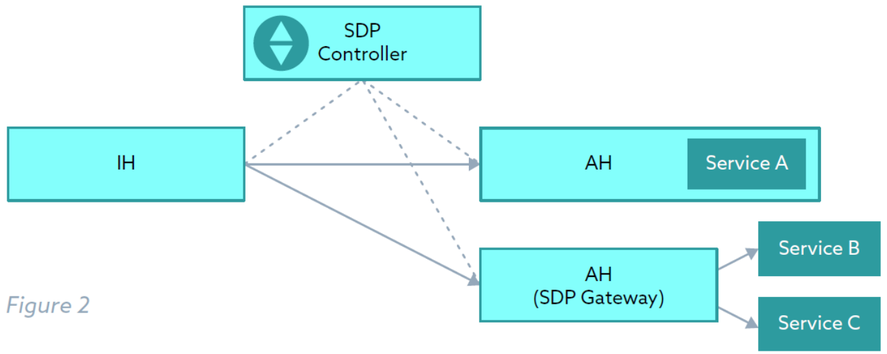


Figure 2

Services non exposés directement

Mais la passerelle peut l'être.

Segmentation des accès par service

Et non par réseau.

Contrôles d'accès « temps réel » et centralisés

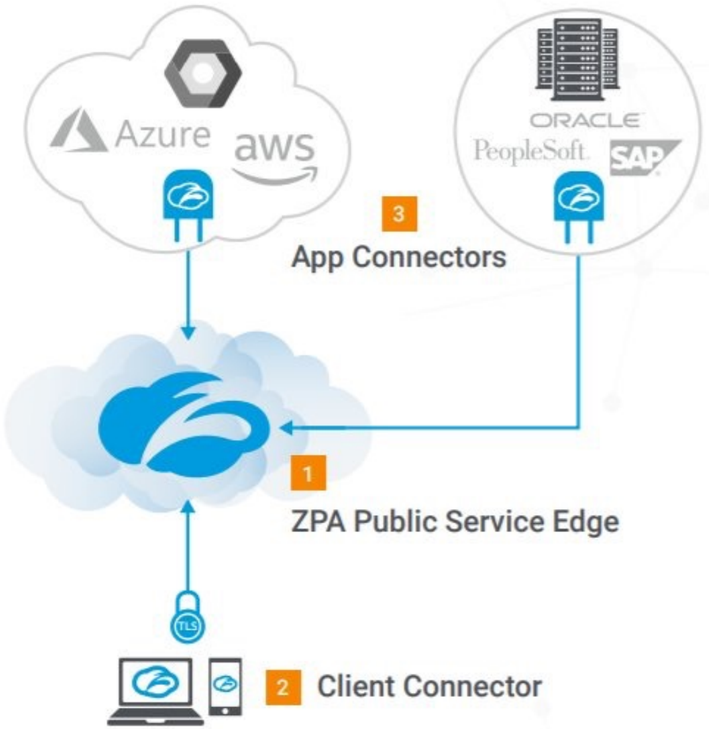
Basé sur les identités

Software-Defined Perimeter (SDP) Specification v2.0 | CSA (cloudsecurityalliance.org).

SOLUTIONS ACTUELLES

A travers deux exemples

ZSCALER ZPA



Zero Trust Network Architecture

1 ZPA Public Service Edge
- Brokers a secure connection between a Client Connector and an App Connector
- Hosted in cloud
- Used for authentication
- Customizable by admins

2 Client Connector
- Mobile client installed on devices
- Requests access to an app

3 App Connector
- Sits in front of apps in Azure, AWS, and other public cloud services
- Listens for access requests to apps
- No inbound connections

Canal de contrôle

Canal de données

IH

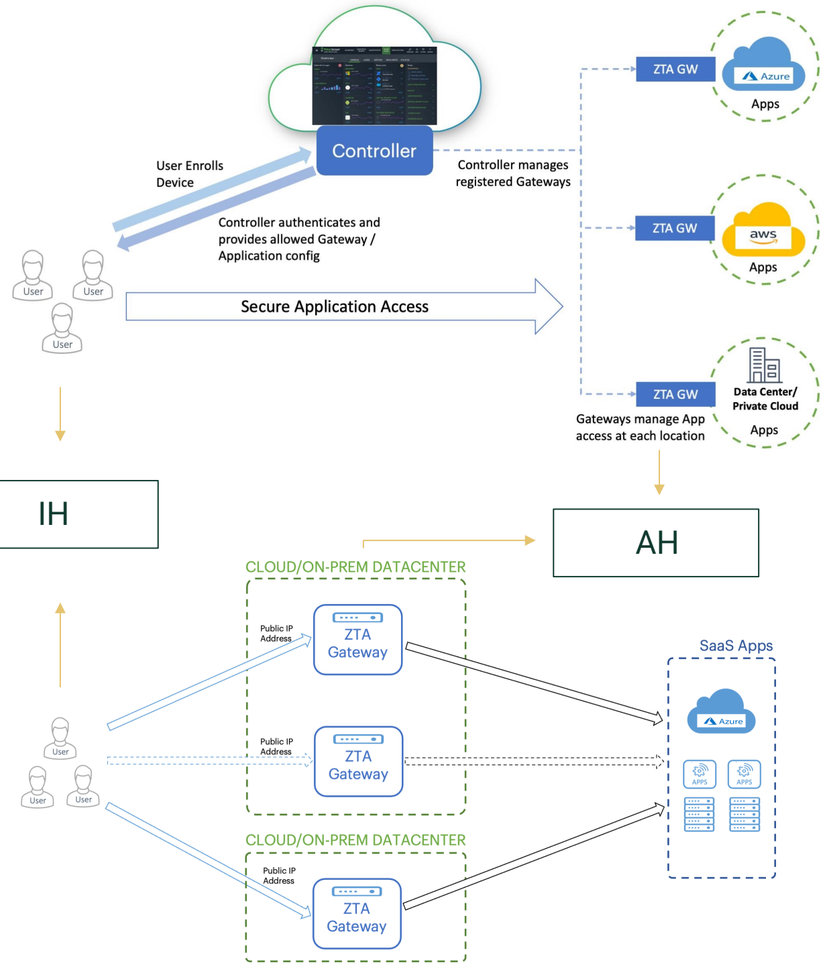
AH

Understanding the ZPA Cloud Architecture | Zscaler

« Le ZTNA établit uniquement des connexions sortantes, garantissant ainsi que les utilisateurs non autorisés n'ont aucune visibilité sur l'infrastructure du réseau et des applications. Les adresses IP ne sont jamais visibles sur Internet, créant ainsi un ***darknet*** *qui rend le réseau indétectable »*

zscaler™

IVANTI ZTA



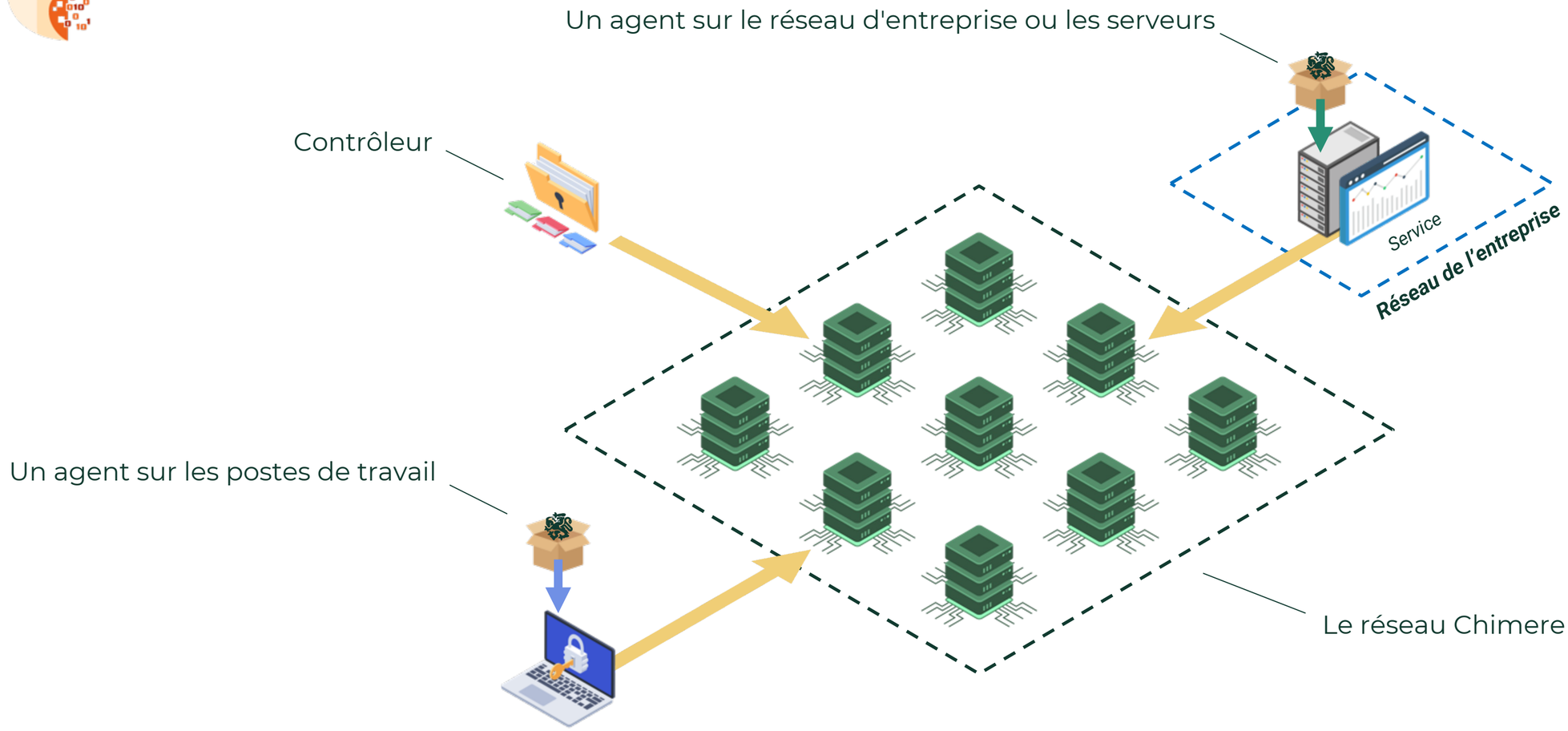
Solution d'accès réseau Zero Trust (ZTNA) | Ivanti

AVANTAGES ET INCONVÉNIENTS DES IMPL.

Implémentation	« Invisibilité » des points d'entrée	Indépendance
Broker tiers	✅	❌
Passerelles exposées	❌	✅

CHIMERE

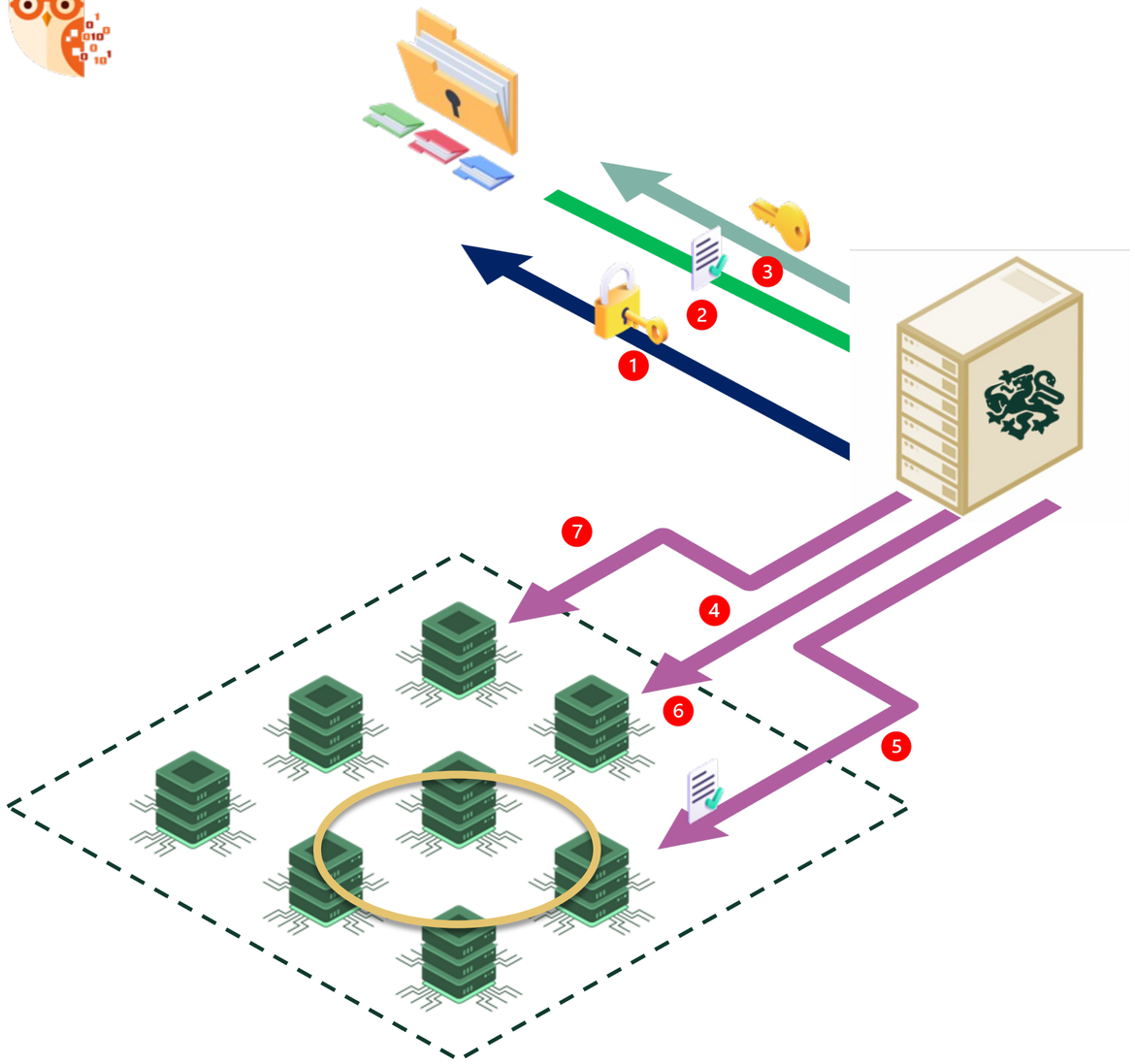
CHIMERE EN 4 COMPOSANTS



PROPRIÉTÉ 1

Accès aux services par clés cryptographiques

L'AGENT DE TRANSFERT



Pour chaque application à protéger, l'agent de transfert:

1
- Etablit une connexion sécurisée avec le Manager Chimere **CM** de la société, à travers le réseau Chimere et s'authentifie à l'aide d'une **clé d'API A1**.

2
- Récupère la liste des utilisateurs autorisés à accéder à l'application depuis le **Manager CM**.

3
- Génère une paire de clés ED25519 (**Kpub1, Kpriv1**)
- Transmet la clé **Kpub1** au Manager Chimere **CM**

Puis, à intervalles réguliers (toutes les 5 minutes):

4
- Etablit des connexions TLS avec un ensemble de serveurs **M** du réseau Chimere
- Dérive une clé de chiffrement symétrique **Ks1**, depuis **Kpub1** et un élément public **E1** fourni par le réseau Chimere

5
- Etablit un fichier **D1 chiffré avec Ks1** contenant la liste des serveurs **M** et le télécharge sur une **HashTable distribuée** du réseau Chimere

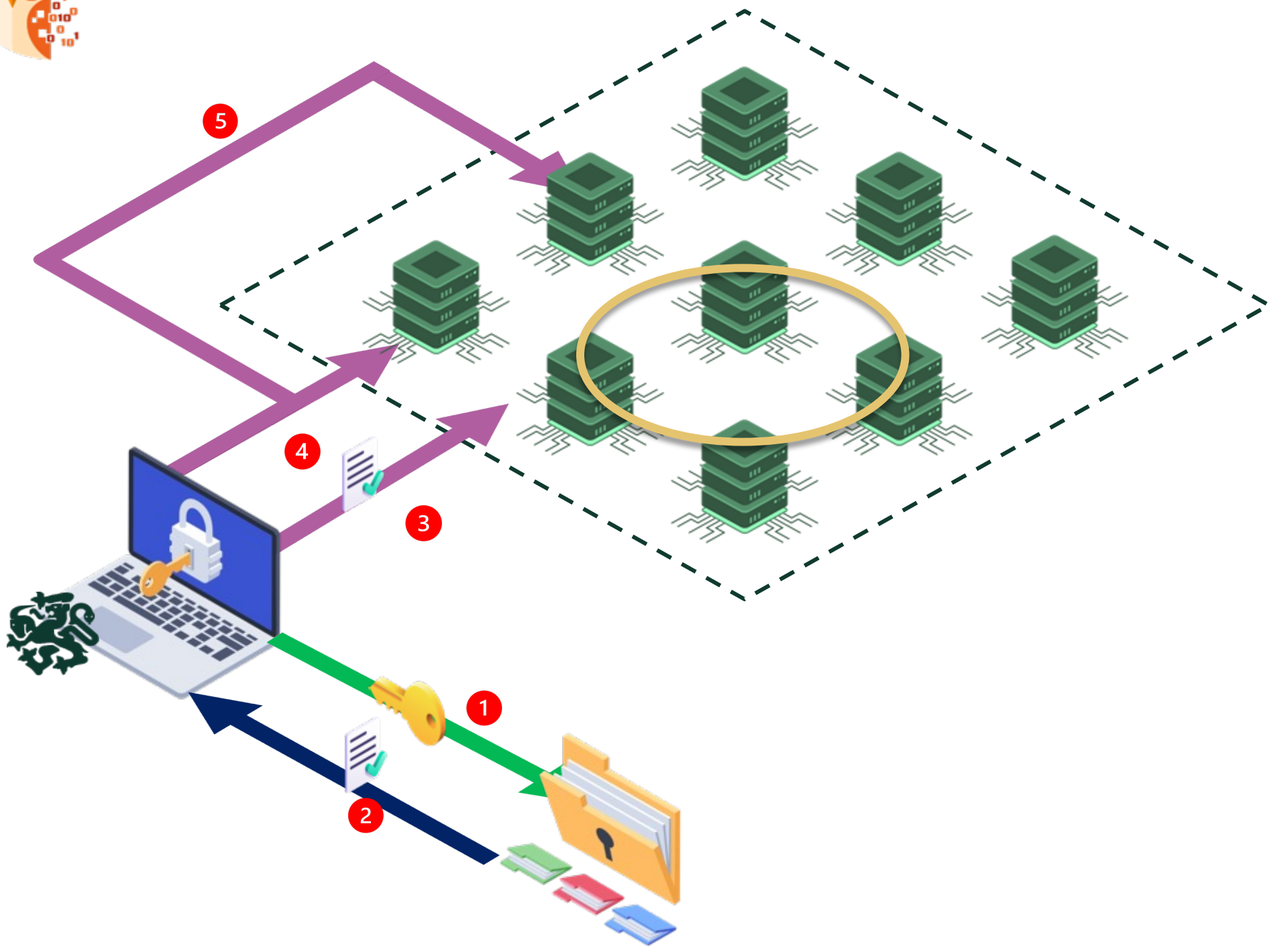
Le service est à présent publié à travers le réseau Chimere et est accessible via **Kpub1** et **un port virtuel**.

Lorsqu'un utilisateur souhaite accéder à l'application :

6
- L'agent de transfert reçoit une requête depuis l'un des serveurs **M**, avec les éléments cryptographiques de l'utilisateur, un handshake Diffie-Hellman et un serveur **N du réseau Chimere sur lequel effectuer la rencontre.**

7
- Si l'utilisateur est autorisé, l'agent initie une connexion **TLS** jusqu'au serveur **N**, finalise la connexion, puis initie la connexion TCP jusqu'au service final protégé.

L'AGENT UTILISATEUR



Sur les postes utilisateur, l'agent :

1. Etablit une connexion sécurisée avec le Manager Chimere **CM** de la société, à travers le réseau Chimere et s'authentifie à l'aide d'un **certificat X509** et **une paire de clés RSA**.
2. Reçoit les clés **KPub** de chaque service auquel l'utilisateur a accès, ainsi qu'une **URL d'accès**.

Lorsqu'un utilisateur tente d'accéder à une application via son URL:

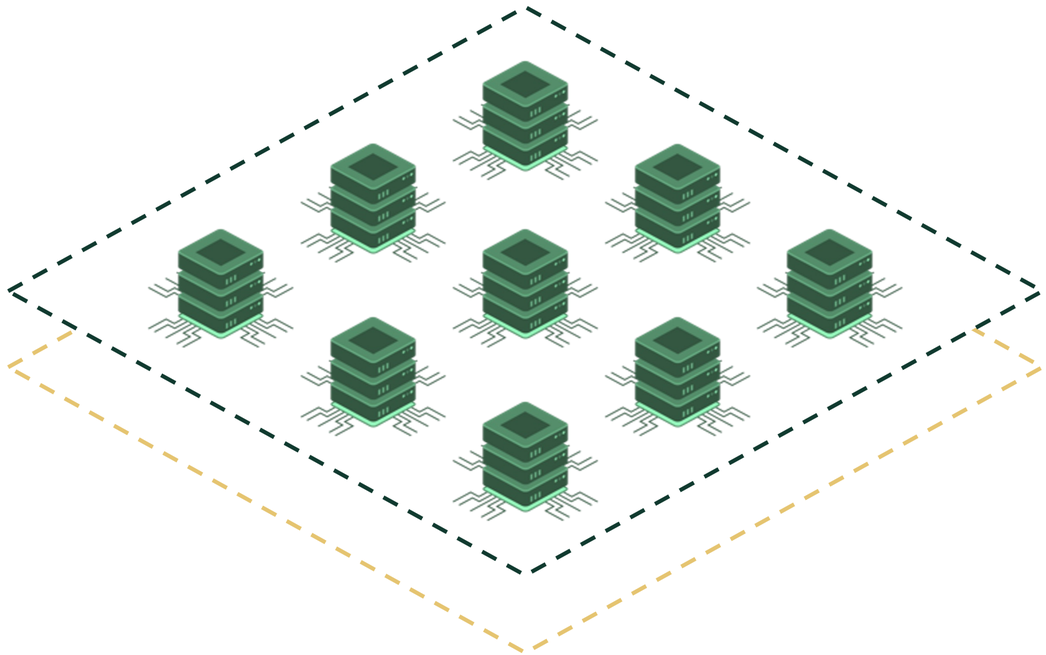
- L'agent utilisateur utilise la clé **KPub1** correspondante et dérive la clé **Ks1** en utilisant **E1** récupéré depuis le réseau Chimere

3. Télécharge le fichier **D1** en interrogeant la HashTable distribuée du réseau Chimere, et déchiffre la liste des serveurs **M** en utilisant la clé **Ks1.**
4. Etablit une connexion TLS **T** vers un serveur N du réseau Chimere, et communique les éléments cryptographiques de l'utilisateurs, la moitié de la négociation Diffie-Hellman et l'identité du service **N** vers un serveur **M** sélectionné.
5. Si les autorisations de l'utilisateur pour accéder au service final sont confirmées, la connexion est finalisée et l'échange de données peut démarrer à travers le serveur **N**.

PROPRIÉTÉ 2

Le chiffrement de bout-en-bout n’est pas une option

CHIFFREMENT ET PRIMITIVES CRYPTOGRAPHIQUES

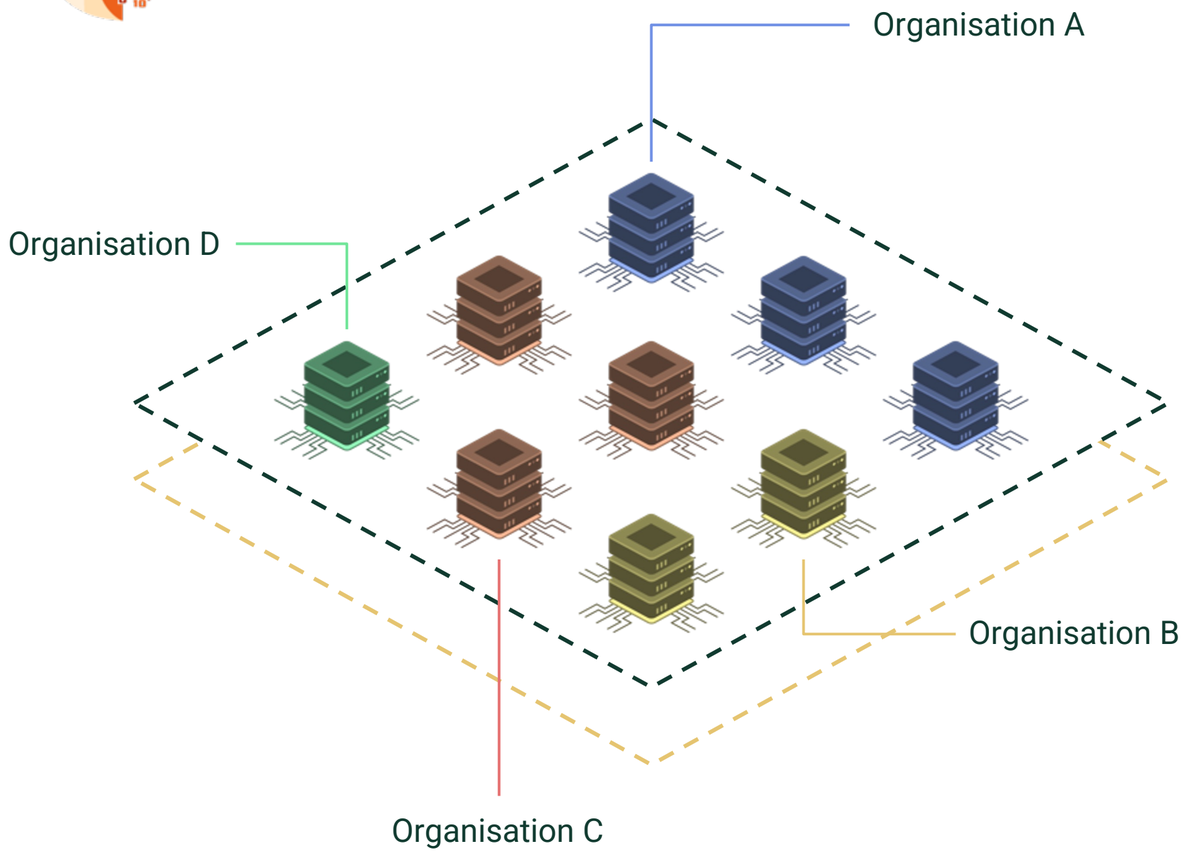


- Les nœuds communiquent entre eux à travers des **connexions TLS**, de la même façon que les agents communiquent avec les nœuds.
- L'algorithme de chiffrement de bout-en-bout employé est **AES 128** en **Counter mode**.
- Les clés de session sont négociées avec **ECDH**.

PROPRIÉTÉ 3

L’indépendance sur la disponibilité

OPÉRER SES PROPRES NOEUDS



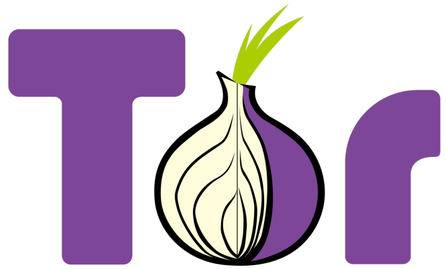
- Possibilité d'opérer et maintenir ses propres nœuds
- Conservation des propriétés 1 et 2

AVANTAGES ET INCONVÉNIENTS DES IMPL.

Implémentation	« Invisibilité » des points d'entrée	Indépendance
Broker tiers	✓	✗
Passerelles exposées	✗	✓
Chimere	✓	✓

L'IMPLÉMENTATION TOR

Réseau communautaire



Chiffrement de bout-en-bout natif (services cachés)

Accès aux services par clés (adresses .onion)

Le réseau CHIMERE n’est pas le réseau Tor

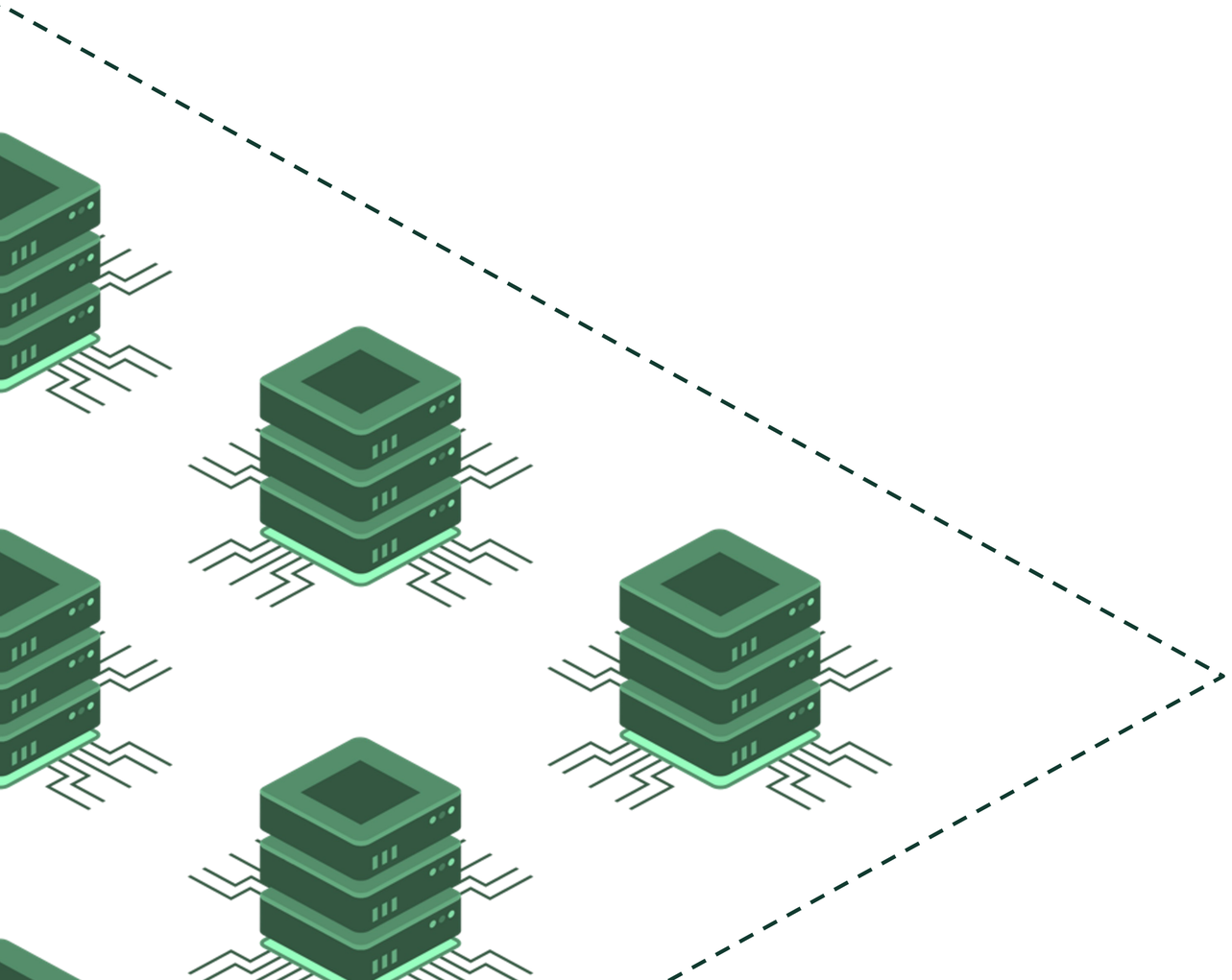
Les réseaux sont distincts mais certains mécanismes sous-jacents sont communs

CHIMERE

Chimere est une solution française et européenne de **Zero-Trust Network Access** qui fournit de l'accès distant sécurisé, sans tiers de confiance.

LE RÉSEAU CHIMERE

Fonctionne sur du cloud public et standard



- Multi-Cloud français : OVH et Scaleway

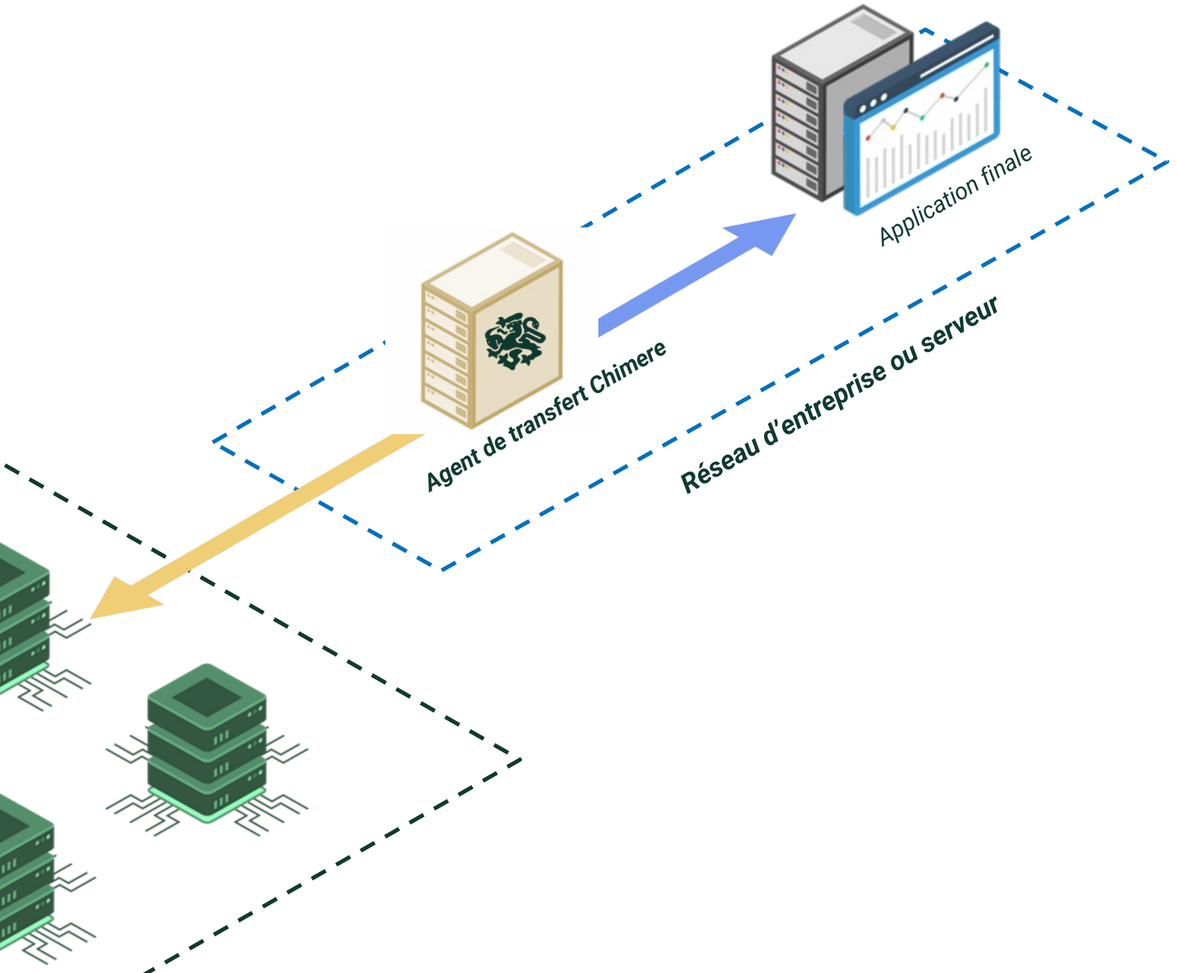
Performances :

- Latence moyenne : **60ms**
- Débit par connexion TCP établie : **8Mo/s**

OVHcloud Scaleway

L'AGENT DE TRANSFERT

Un logiciel pour publier les applications sur le réseau Chimere



- Opéré par la société souhaitant se protéger
- S'installe sur le serveur portant l'application ou sur une machine déportée
- Fait le lien entre le réseau Chimere et l'application à protéger à travers des flux TLS exclusivement sortants
- Disponible sur Linux, Windows Server (CLI ou interface graphique) et en application Docker

docker Windows Server Linux

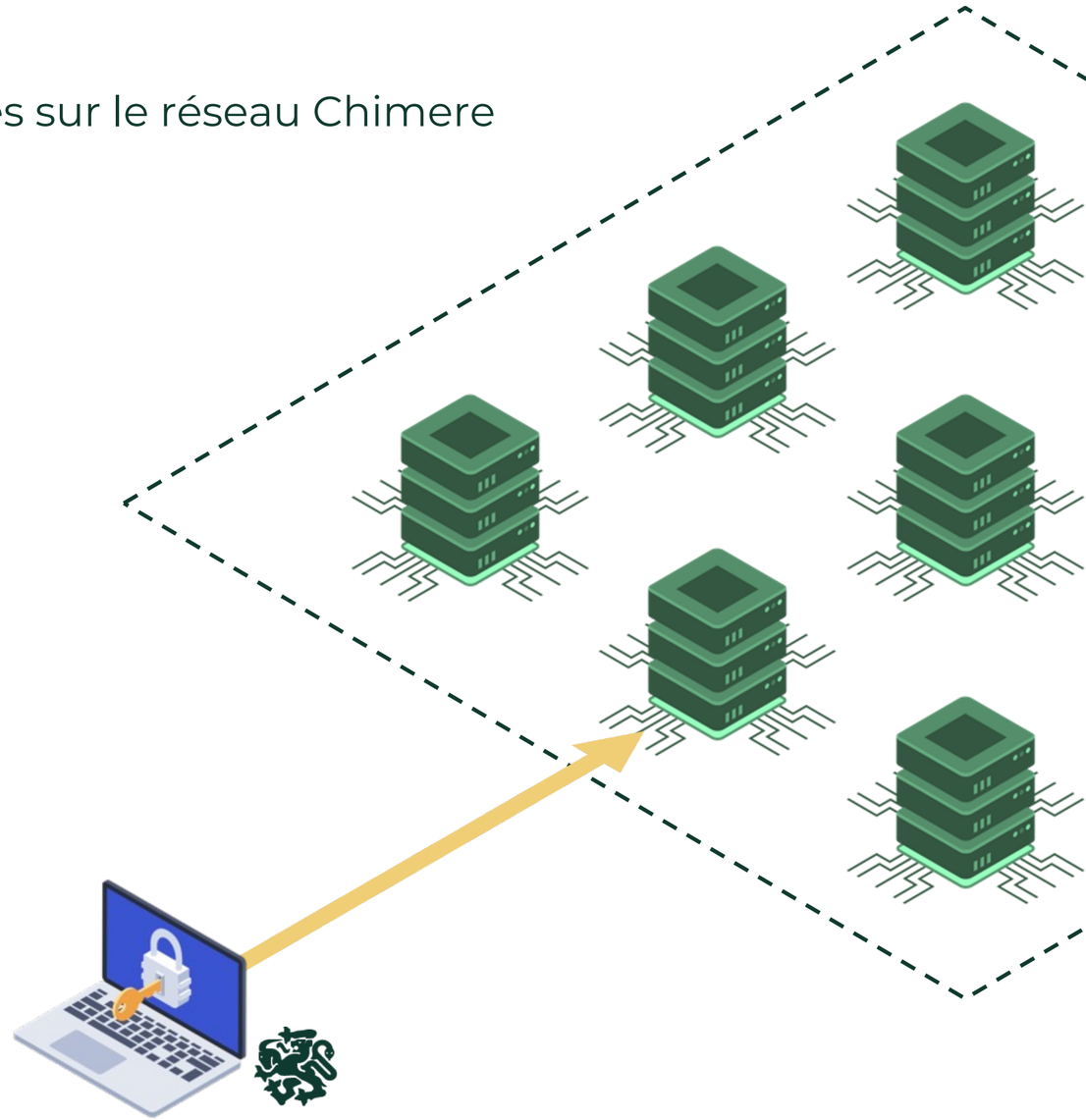
L'AGENT UTILISATEUR

Un logiciel pour accéder aux applications publiées sur le réseau Chimere

- L'équivalent d'un client VPN
- Opéré par l'utilisateur ou sa société
- S'installe sur le poste de travail
- Permet d'accéder aux applications sans changer les habitudes de l'utilisateur*

*Conservation des clients lourds habituels et des URLs d'accès

- Affiche la liste des applications sécurisées auxquelles l'utilisateur a accès

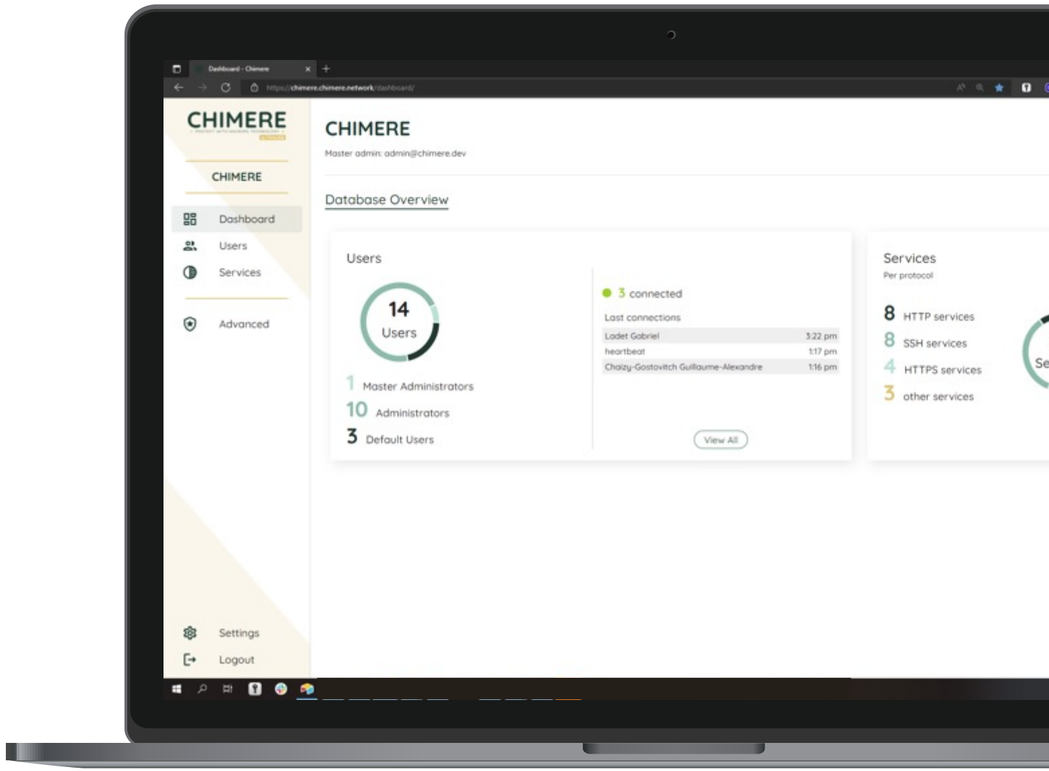


Windows macOS android A venir - 2024 Linux A venir - 2024

LE MANAGER CHIMERE

Une application Docker pour gérer les clés cryptographiques, propager et révoquer les droits d'accès

- Opéré par la société souhaitant se protéger
- Hébergé au choix par la société souhaitant se protéger ou par la société Chimere
- Se synchronise avec les fournisseurs d'identité (SCIM) ou gère les informations d'identité en « stand-alone »
- Propage et révoque les droits d'accès aux applications en temps réel



CAS D'USAGES

- Accès d'administration SSH, RDP, VDI
- Obfuscation de la passerelle VPN
- Nomadisme numérique
- Accès prestataires aux applications du SI

Merci !

13 février 2024

Illustration credits: Storyset