RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

Zero Trust

Faut-il avoir confiance ?

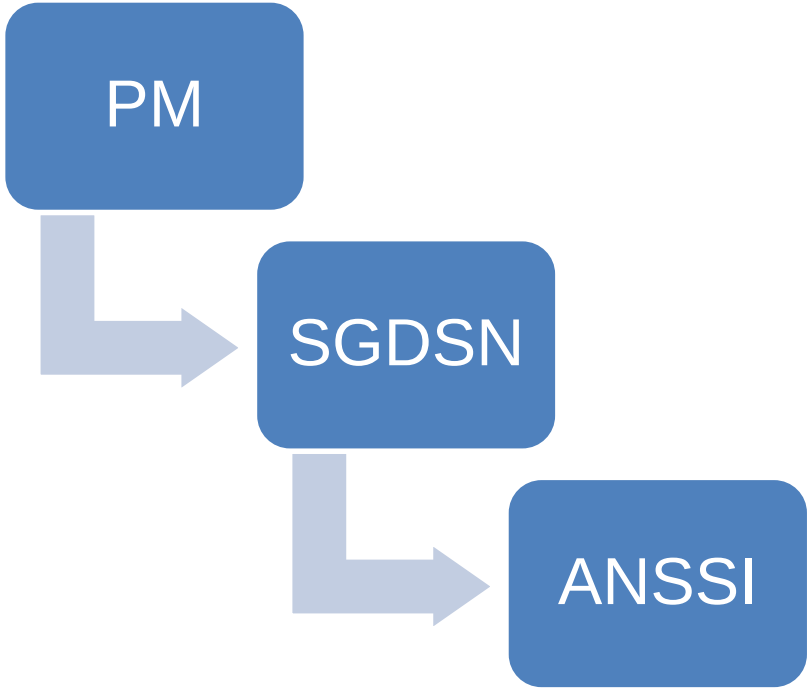
15/11/2022

Sommaire

1. Présentation de l'ANSSI et de la DAT
2. Historique du Zero Trust
3. Approche BeyondCorp
4. Propagation du Zero Trust
5. Avis de l'agence

1 - Présentation de l’ANSSI

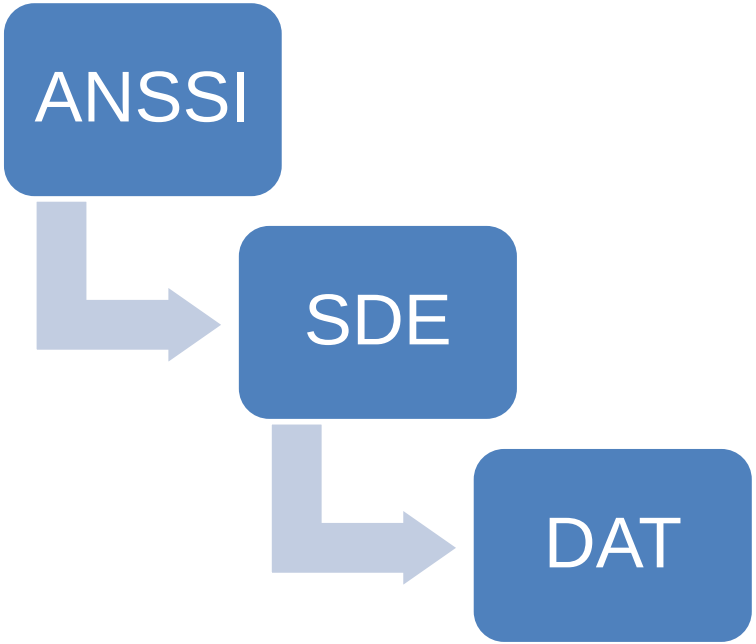
Le positionnement organisationnel de l'ANSSI



Les missions de l'ANSSI

- Soutenir les hautes autorités et administrations
- Accompagner les OIV et OSE
- Coopérer avec des partenaires de confiance
- Assurer le rôle d'autorité nationale de la sécurité à l'international
- Répondre aux attaques des services de l'Etat et des opérateurs privés les plus sensibles

La Division Assistance Technique (DAT)



2 - Historique du Zero Trust

2009 : L'opération Aurora

- Nom donné à une vague de compromission mi décembre 2009
- Une trentaine de sociétés américaines compromises
- Une partie du code source de Google est exfiltré
- L'attaque est attribuée par le gouvernement US au mode opératoire APT17/Elderwood, prétendument lié à la Chine

Déroulé de l'attaque sur Google

Source : Protecting your critical assets, McAfee, 2010

1. Utilisateur harponné
2. Navigation vers un site web malveillant
3. Exécution de javascript sur exploitant une vulnérabilité inconnue (Zero day).

Déroulé de l'attaque sur Google

Source : Protecting your critical assets, McAfee, 2010

4. Téléchargement d'un exécutable.
5. Installation d'une porte dérobée et établissement d'un lien persistent.
6. Exploitation de la porte dérobée pour accéder aux ressources internes

Conséquences de l'attaque sur Google

- Découverte de nombreuses vulnérabilités sur la solution de gestion de configuration logicielle
- Prise de conscience que la compromission d'un poste est un évènement réaliste, probable
- Lancement d'un projet de SI sur la base d'un nouveau modèle de sécurité. Le projet BeyondCorp.

Historique du Zero Trust

12/2009
Opération Aurora

12/2014
BeyondCorp : A new approach to Enterprise Security

04/2016
BeyondCorp : Design to deployment at Google

03/2020
Microsoft : Zero Trust Maturity Model

Historique du Zero Trust

08/2020
NIST : Zero Trust Architecture

10/2020
ANSSI : Le modèle Zero Trust

05/2021
POTUS : Executive order 14028

06/2021
CISA : Zero Trust Maturity Model

01/2022
OMB : Federal Zero Trust Strategy

Evolution des recherches Google

Source : Résultat Google Trends pour « Zero Trust » de 2009 à aujourd'hui dans le monde

3 - Approche BeyondCorp

Le problème du niveau de confiance

- *"While most enterprises* ***assume that the internal network is a safe environment*** *in which to expose corporate applications, Google's experience has proven that* ***this faith is misplaced.*** *Rather, one should assume that an internal network is as fraught with danger as the public Internet and build enterprise applications based upon this assumption.*
- *"access depends solely on* ***device and user credentials****, regardless of a user's network location"*

Source : A new approach to Enterprise Security, BeyondCorp, Google, 2014

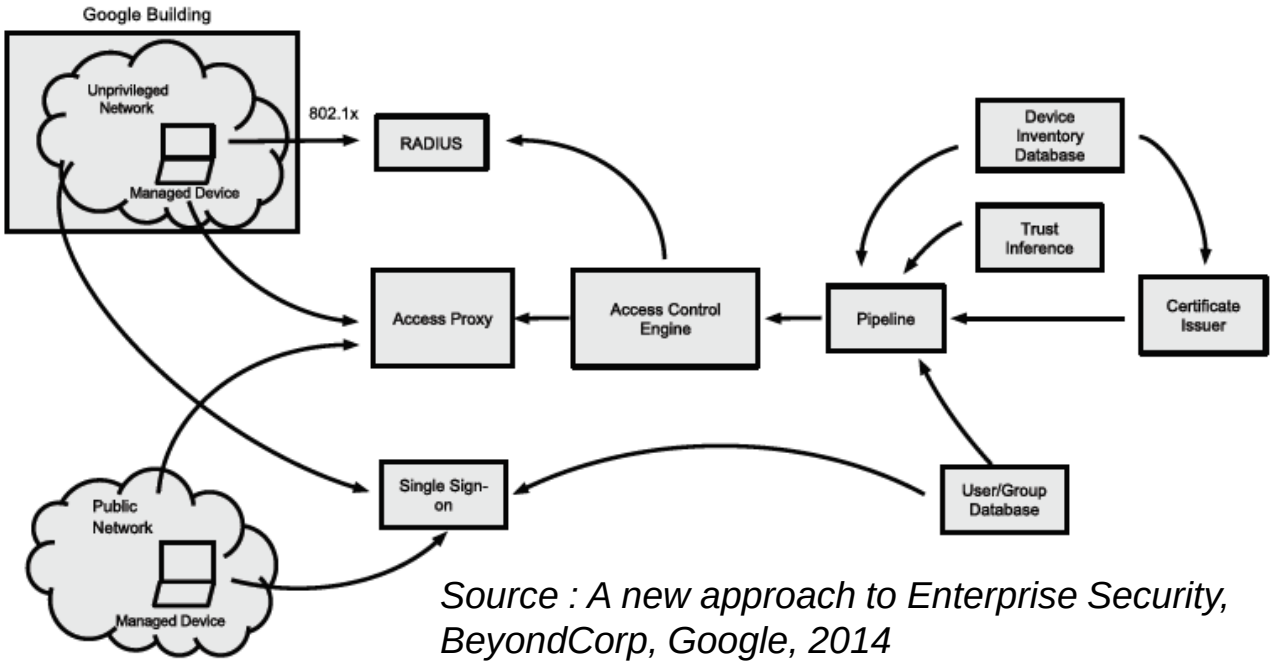
L’image de la salle des preuves

Avec de la défense périmétrique…

L’image de la salle des preuves

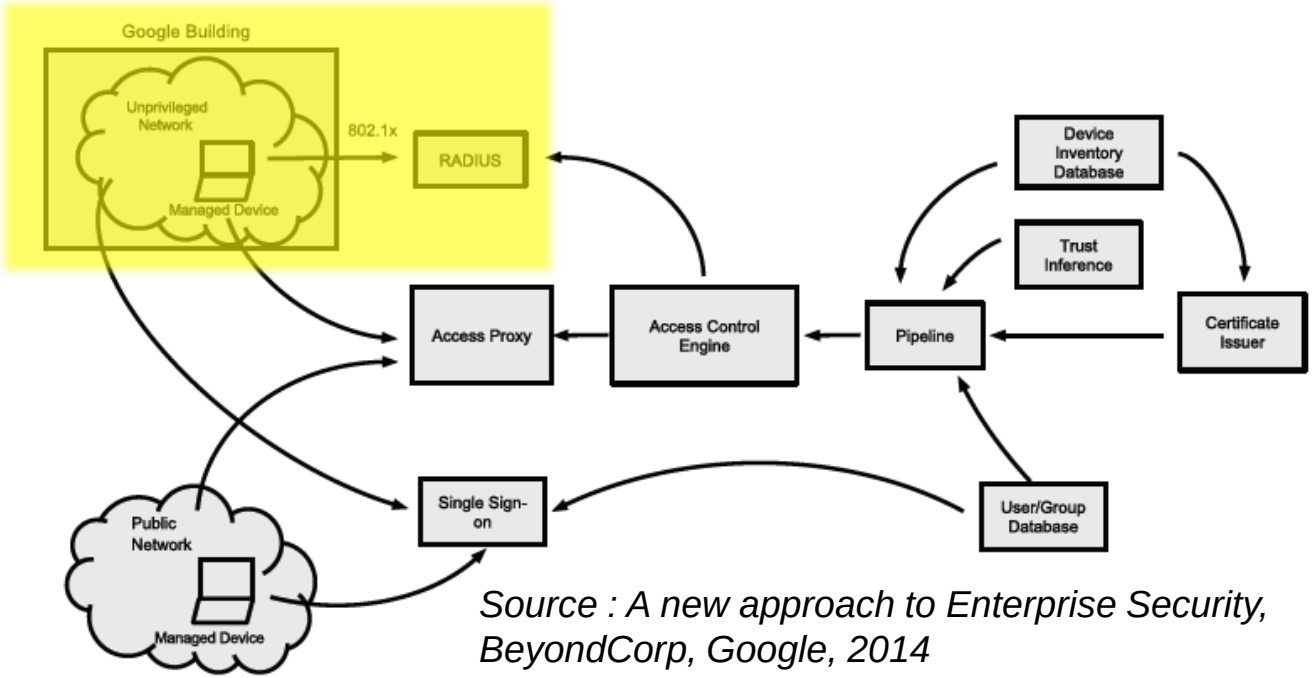
Avec de la défense en profondeur

BeyondCorp : Architecture générale



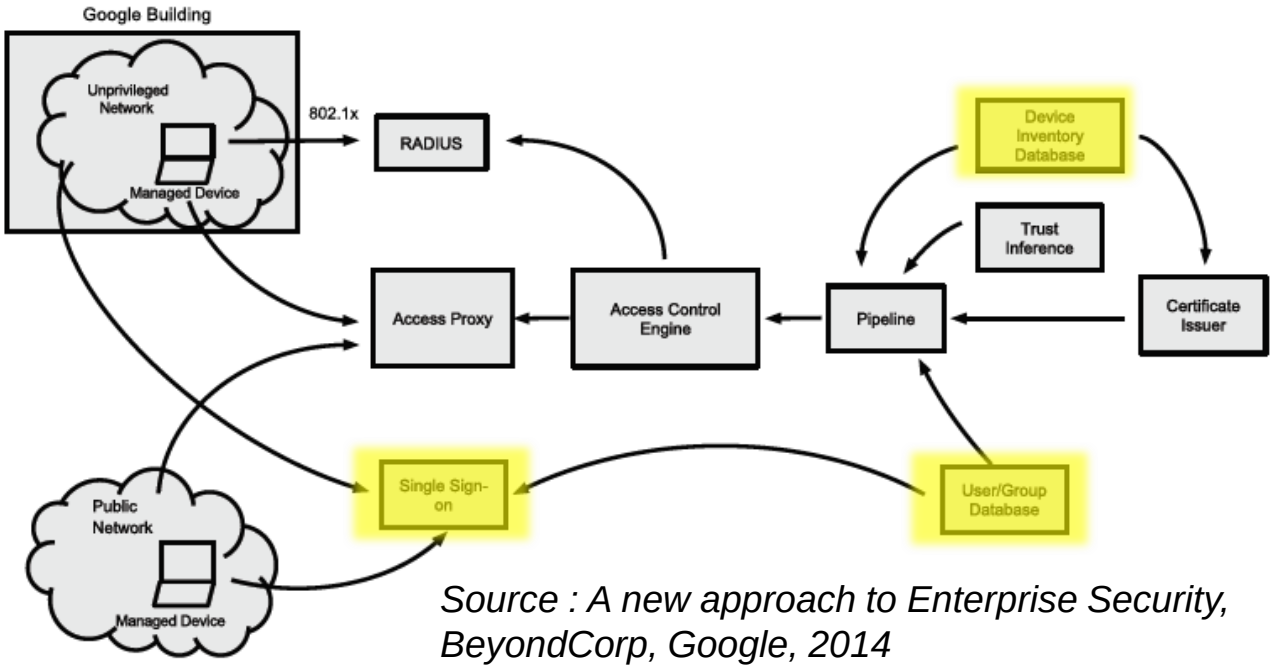
Source : A new approach to Enterprise Security, BeyondCorp, Google, 2014

BeyondCorp : Réseau interne non privilégié



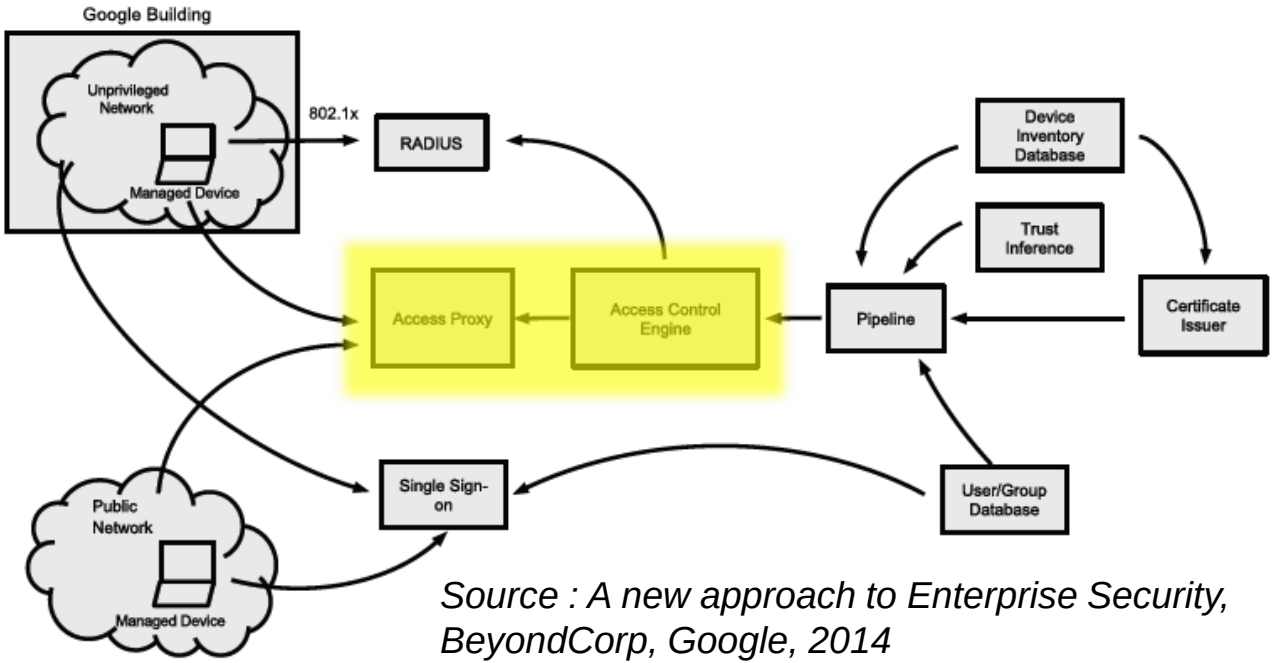
Source : A new approach to Enterprise Security, BeyondCorp, Google, 2014

BeyondCorp : Référentiels d'identité et authentification



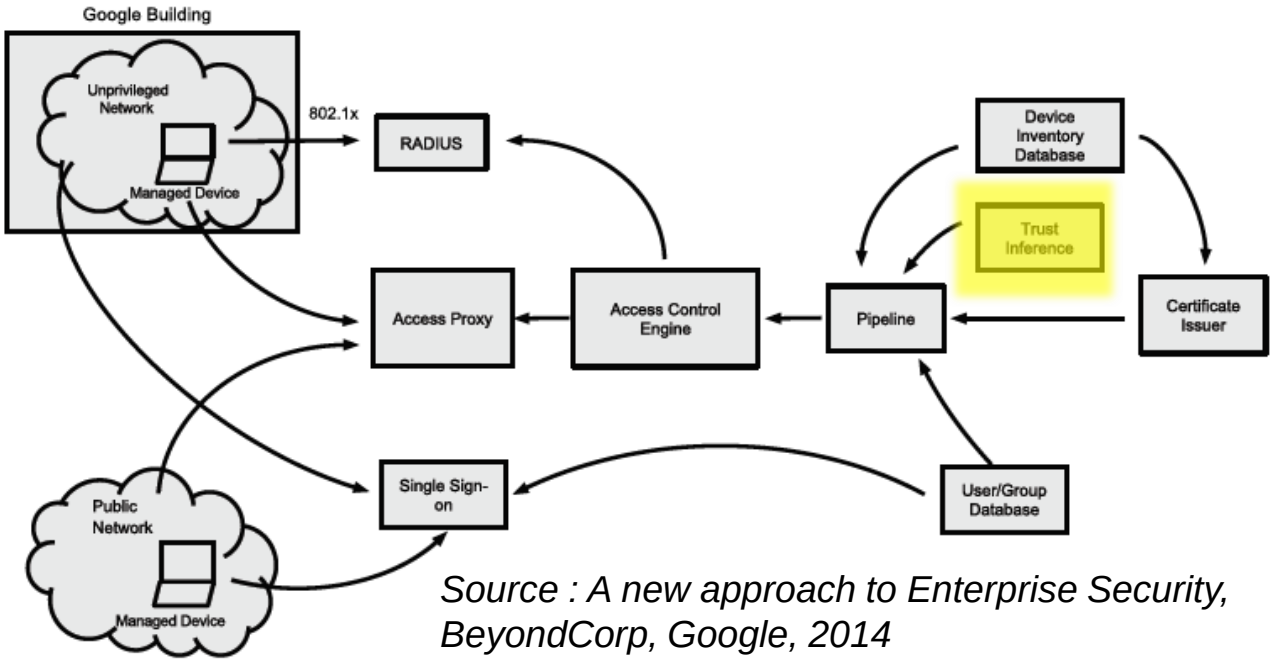
Source : A new approach to Enterprise Security, BeyondCorp, Google, 2014

BeyondCorp : Proxy d'accès et Moteur de contrôle d'accès



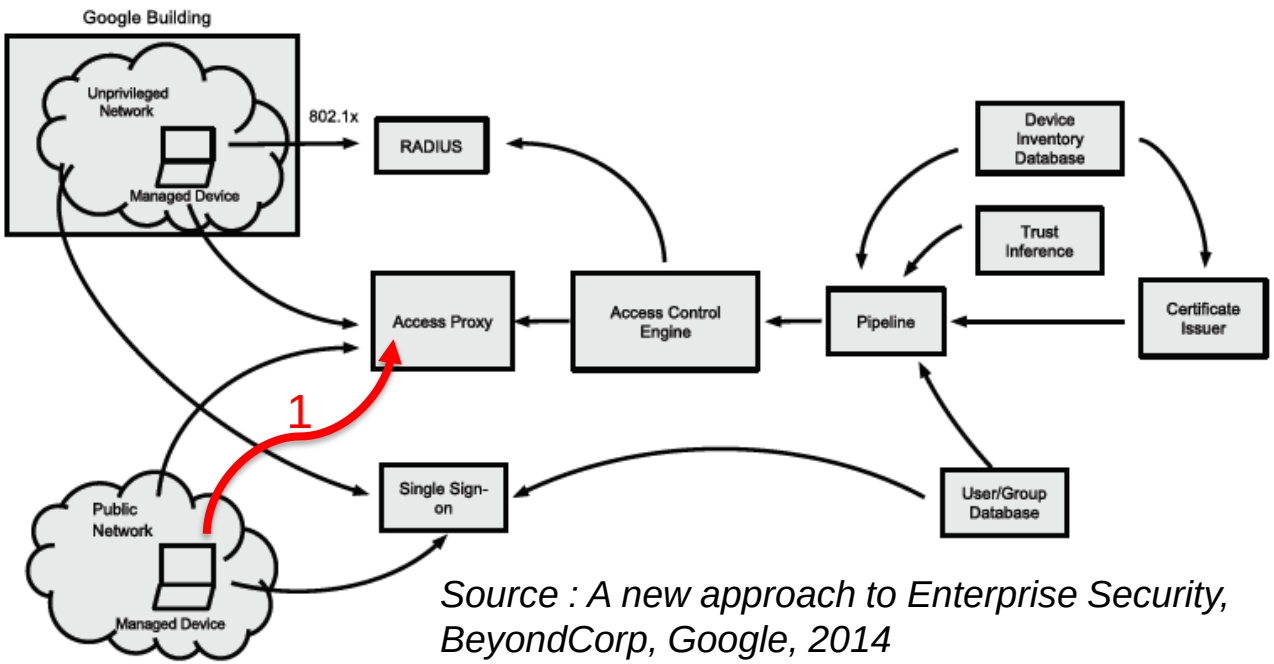
Source : A new approach to Enterprise Security, BeyondCorp, Google, 2014

BeyondCorp : Trust Inference



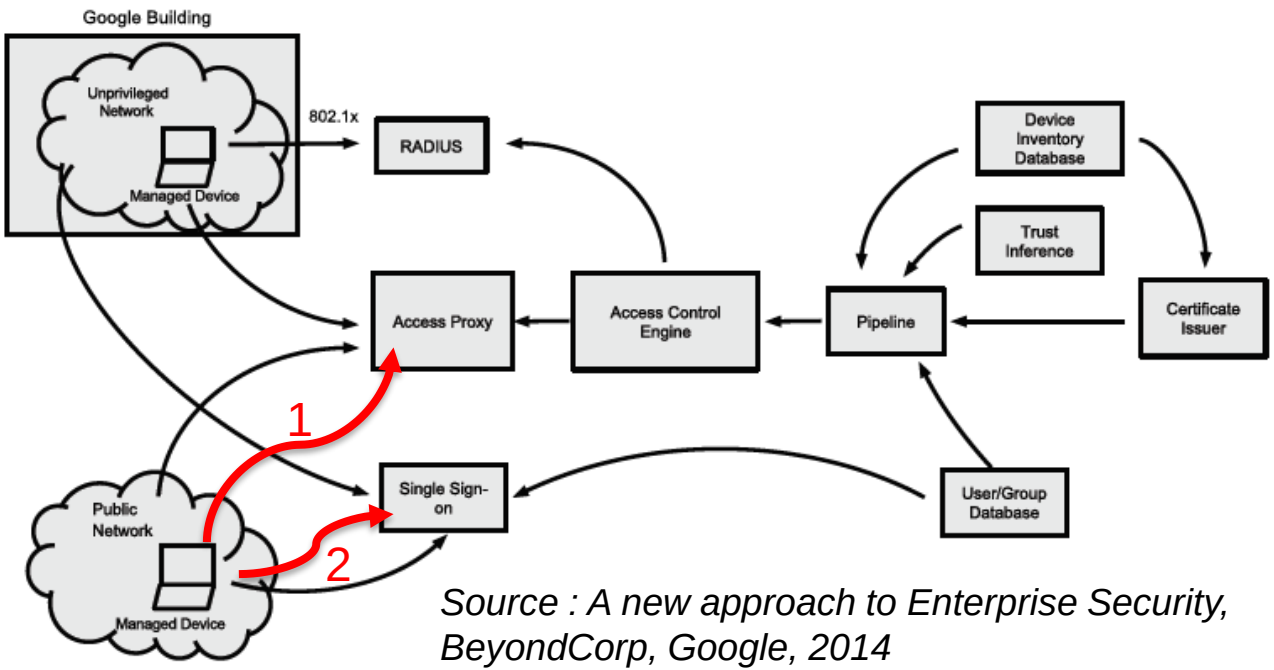
Source : A new approach to Enterprise Security, BeyondCorp, Google, 2014

BeyondCorp : Sum up flow chart



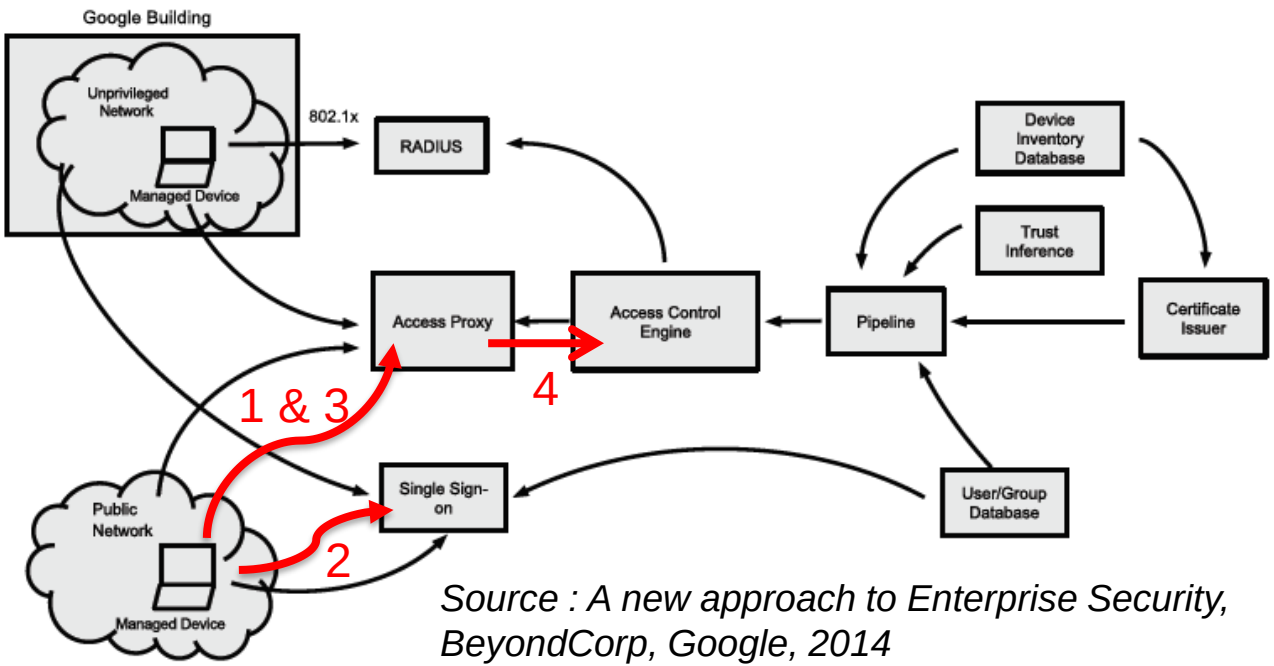
Source : A new approach to Enterprise Security, BeyondCorp, Google, 2014

BeyondCorp : Sum up flow chart



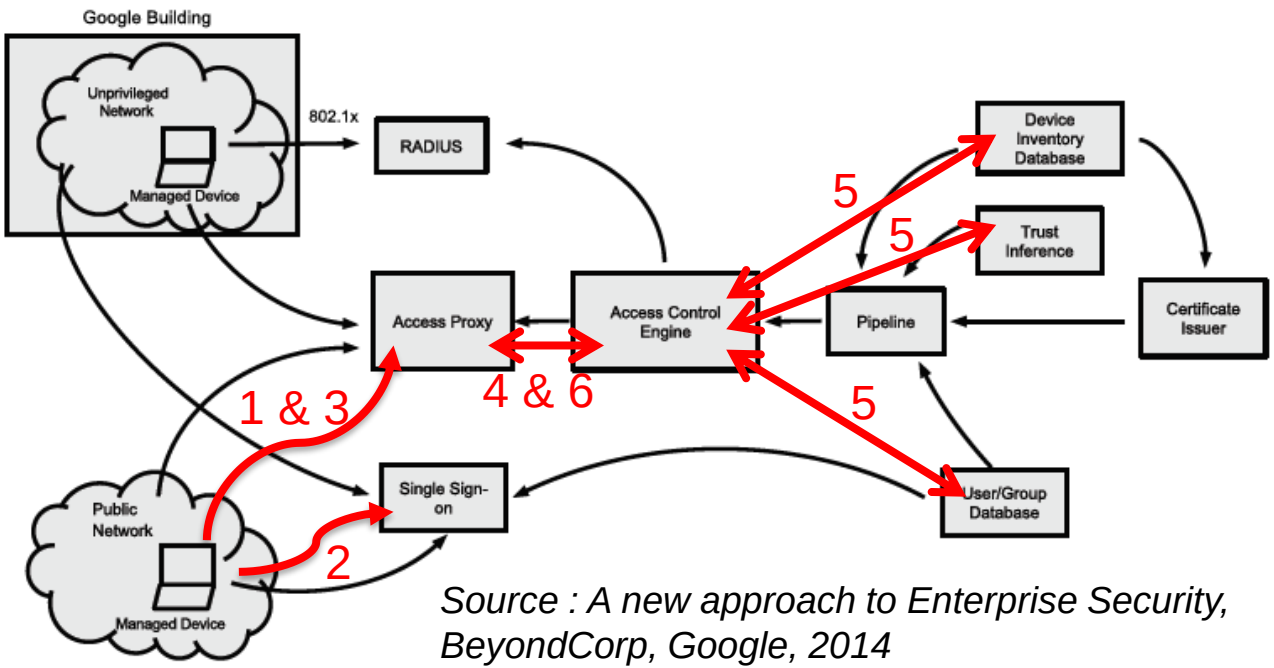
Source : A new approach to Enterprise Security, BeyondCorp, Google, 2014

BeyondCorp : Sum up flow chart



Source : A new approach to Enterprise Security, BeyondCorp, Google, 2014

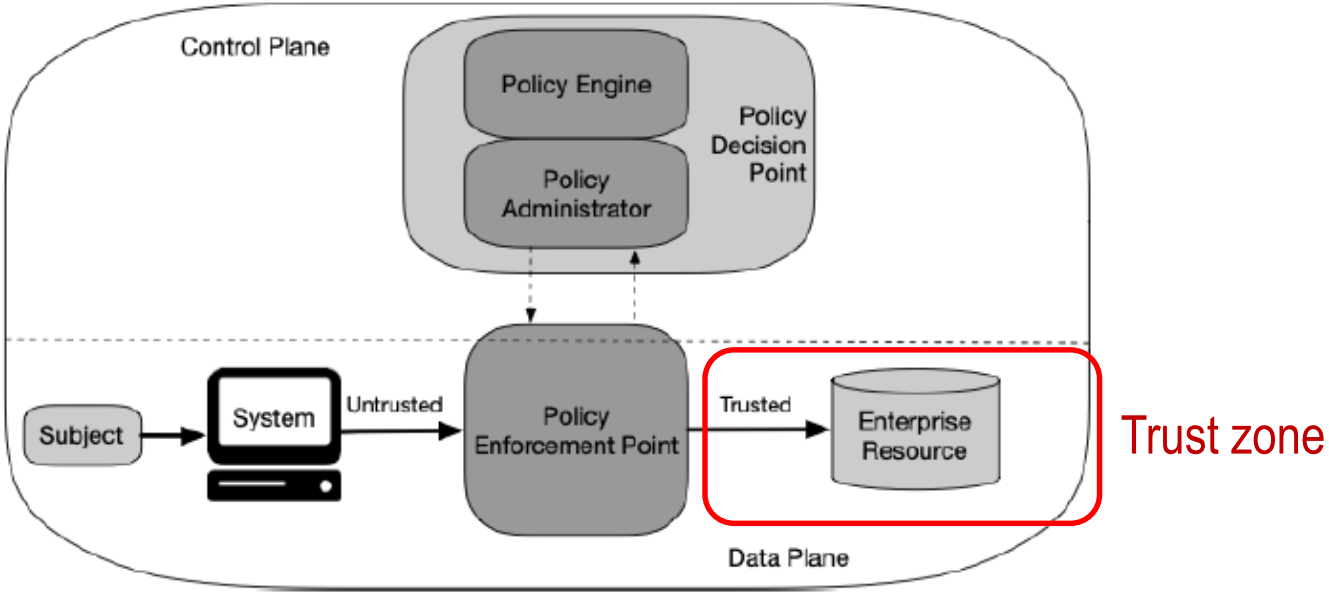
BeyondCorp : Sum up flow chart



Source : A new approach to Enterprise Security, BeyondCorp, Google, 2014

4 – Propagation du Zero Trust

NIST : Architecture simplifiée du contrôle d'accès ZT



Source : Zero Trust Architecture, SP. 800-207, NIST, 2020

NIST : standardise l'approche ZT

1. Toutes les sources de données et services sont considérées comme des ressources
2. Toutes les communications sont sécurisées indépendamment du réseau d'accès
3. Les accès sont accordés par session
4. Les accès sont déterminés de façon dynamique
5. L'entreprise supervise la posture de sécurité de l'ensemble de ses biens
6. L'authentification est systématiquement faite avant l'accès aux ressources
7. L'entreprise collecte un maximum d'informations sur l'état de ses biens, de son infrastructure réseau, et l'utilise pour continuellement améliorer sa politique d'accès.

Source : Zero Trust Architecture, SP. 800-207, NIST, 2020

Zero Trust et administrations US

- 12 mai 2021 : un ordre exécutif de la présidence étatsunienne impose l'adoption du **cloud** et de la **ZTA** aux administrations fédérales.

(b) Within 60 days of the date of this order, the head of each agency shall:

(i) update existing agency plans to prioritize resources for the adoption and use of cloud technology as outlined in relevant OMB guidance;

(ii) develop a plan to implement Zero Trust Architecture, which shall incorporate, as appropriate, the migration steps that the National Institute of Standards and Technology (NIST) within the Department of Commerce has outlined in standards and guidance, describe any such steps that have already been completed, identify activities that will have the most immediate security impact, and include a schedule to implement them; and

Source : Executive Order 14028, GSA, mai 2021

CISA : Guide de maturité

	Identity	Device	Network / Environment	Application Workload	Data
Traditional	• Password or multifactor authentication (MFA) • Limited risk assessment	• Limited visibility into compliance • Simple inventory	• Large macro-segmentation • Minimal internal or external traffic encryption	• Access based on local authorization • Minimal integration with workflow • Some cloud accessibility	• Not well inventoried • Static control • Unencrypted
	Visibility and Analytics	Automation and Orchestration		Governance	
Advanced	• MFA • Some identity federation with cloud and on-premises systems	• Compliance enforcement employed • Data access depends on device posture on first access	• Defined by ingress/egress micro-perimeters • Basic analytics	• Access based on centralized authentication • Basic integration into application workflow	• Least privilege controls • Data stored in cloud or remote environments are encrypted at rest
	Visibility and Analytics	Automation and Orchestration		Governance	
Optimal	• Continuous validation • Real time machine learning analysis	• Constant device security monitor and validation • Data access depends on real-time risk analytics	• Fully distributed ingress/egress micro-perimeters • Machine learning-based threat protection • All traffic is encrypted	• Access is authorized continuously • Strong integration into application workflow	• Dynamic support • All data is encrypted
	Visibility and Analytics	Automation and Orchestration		Governance	

Source : Zero Trust Maturity Model, CISA, juin 2021

- Juin 2021 : La CISA publie un guide de maturité Zero Trust.
  - 5 piliers :
    - Identité
    - Equipement
    - Réseau
    - Application
    - Données
  - 3 niveaux :
    - Traditionnel
    - Avancé
    - Optimal

5 - L’avis de l’agence

Le Zero Trust c'est

- C'est un modèle de sécurité utilisant des principes connus (défense en profondeur, moindre privilège, mircrosegmentation)
- C'est avoir une connaissance parfaite de ses applicatifs, ses données, ses utilisateurs, ses équipements et les flux entre tous ces éléments pour mettre en œuvre un contrôle d'accès granulaire
- C'est être capable de déployer une infrastructure d'authentification centralisée de ses utilisateurs et de ses équipements
- C'est adapté aux applications webs, voire ça demande une adaptation des applications au modèle
- Cela implique de travailler très précisément sur les cas d'usage (qui, quand, comment, dans quelles conditions, pour quelles données)
- C'est être capable d'identifier et collecter des signaux, pour chaque utilisateur et chaque équipement pour établir un score de confiance
- C'est très coûteux, très complexe, très long

Le Zero Trust ce n'est pas

- Ce n'est pas une technologie, ni une solution clé en main
  - Attention à la délégation des fonctions de sécurité critiques à des prestataires (reverse proxy, SSO, IGC)
- Ce n'est pas qu'un projet technique
  - Cela doit répondre à un besoin et nécessite l'adhésion métier et la prise en compte des contraintes opérationnelles
- Ce n'est pas la réponse à tous les besoins, ni tous les problèmes de sécurité
  - Choisir les cas d'usages (incompatible des clients lourd, difficulté d'utilisation d'UDP)
  - Cela ne remplace pas l'hygiène de sécurité (MCO, MCS, etc.)
- Cela ne remplace surtout pas la défense périmétrique

Et le BYOD ?

- Les architectures de type Zero Trust permettent-elles de travailler avec des équipements personnels ?

- *"BeyondCorp uses the concept of a "managed device," which is* ***a device that is procured and actively managed by the enterprise****."*

Source : A new approach to Enterprise Security, BeyondCorp, Google, 2014

Et le Cloud ?

Cloud public

Zero Trust Architecture

Et la défense périmétrique ?

- La défense périmétrique a-t-elle encore sens dans une architecture Zero Trust ?

Zero Trust : Takeaway

Zero Trust c'est de la défense en profondeur, dynamique et automatisée

- BYOD : Le ZT ne permet pas de travailler avec ses équipements personnels
- Cloud : Le ZT n'oblige pas à migrer son SI dans le cloud
- Défense périmétrique : Le ZT ne doit en aucun cas remplacer la défense périmétrique
- Transformation/Maturité : Le ZT nécessite du temps, des ressources, des moyens

Merci pour votre attention
Questions ?