UNIVERSITÉ DE RENNES 1

La sécurité périmétrique vs BeyondCorp

date de la formation :

16/01/2019

lieu de la formation : Rennes

orange™

UNIVERSITÉ DE RENNES 1

Sommaire

partie 1 : histoire de la sécurité informatique

partie 2 : sécurité périmétrique

partie 3 : BeyondCorp

Sommaire

partie 1 : histoire de la sécurité informatique

partie 2 : sécurité périmétrique

partie 3 : BeyondCorp

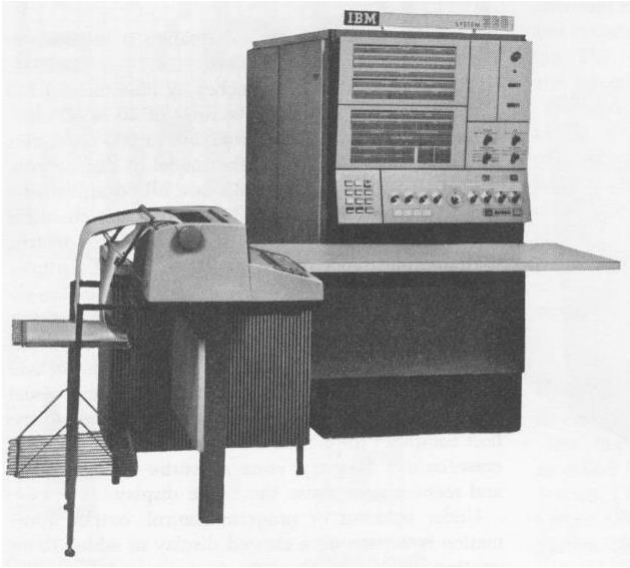
Histoire de la sécurité informatique

- L'informatique est une domaine d'activité récent, ses techniques d'ingénierie sont issues à l'origine des techniques :
  - Du génie civil
  - De l'industrie

- Les méthodologies et approches commencent à peine à se démarquer des approches historiques :
  - Waterfall vs Agile
  - Sillotage vs DevOps

Histoire de la sécurité informatique - avant

- La sécurité informatique a suivi la même histoire
- La sécurité des ordinateurs étaient originellement portées par la sécurité des bâtiments, l'essentiel de l'activité se passait à l'intérieur de l'entreprise
- Les accès informatiques à l'extérieur de l'entreprise par les salariés n'étaient que rarement nécessaires, souvent bloqués.
- Lorsqu'un accès réseau était nécessaire un firewall était mis en œuvre, pour protéger les ressources et personnes présentes à l'intérieur de l'entreprise de toute attaque venant de l'extérieur.



Histoire de la sécurité informatique - après

- Les infrastructures sont gérées par des industriels du cloud public, AWS, Google ou Microsoft.
- De plus en plus d'applications SaaS, Software as a Service, sont utilisées, et elles sont toutes, par nature, hébergées à l'extérieur de l'entreprise.
- Les postes de travail sont variés, mobiles, smartphones, tablettes, PC portables ou Chromebooks, et reliés à des réseaux mobiles, 3G, 4G ou WiFi.
- Les collaborateurs ont besoin et exigent l'accès à leurs applications en tout lieu, à toute heure (ATAWAD)

Sommaire

partie 1 : histoire de la sécurité informatique

partie 2 : sécurité périmétrique

partie 3 : BeyondCorp

Sécurité périmétrique

Sécurité périmétrique

- L'objectif est de découper le réseau d'entreprise en périmètres de sécurité logiques regroupant des entités ou fonctions afin de mettre en place des niveaux de sécurité à la fois imbriqués et séparés.

- La première étape est la définition d'un périmètre de sécurité autour du réseau d'entreprise face au réseau Internet.

- Il faut également définir un périmètre de sécurité autour de chacun de ces réseaux inclus dans le réseau intranet. Cette compartimentation du réseau intranet rend plus difficile une éventuelle pénétration.

Sécurité périmétrique

Sécurité périmétrique

- Cette approche part du constat que toute entreprise est dotée d'un « périmètre de sécurité »
  - il entoure les ressources qu'elle doit protéger contre les accidents naturels ou les attaques humaines.

- Ce périmètre est évident dans l'espace physique : les locaux, les équipements, les documents et les personnes doivent être protégés contre les intempéries et les agressions.

- Le système d'information (ordinateurs et réseaux) se trouve dans le périmètre de sécurité physique, par contre il engendre un nouveau périmètre de sécurité, moins évident
  - les données, systèmes d'exploitation et programmes informatiques

Sécurité périmétrique

- La sécurisation du SI d'une entreprise est conçue à partir d'une ligne de défense périmétrique dont le pare-feu est la pièce maîtresse
  - complétée par des zones d'accès plus ou moins réglementées en fonction de la sensibilité des ressources à protéger.

- La mise en œuvre de ce modèle de défense repose sur une vision tactique qui consiste à élever une ligne de défense et à la protéger des agressions externes.

- L'image périmétrique traditionnelle est celle des villes fortifiées dont la sécurité reposait sur des accès contrôlés concentrant les flux entrants et sortants.

Sécurité périmétrique - DMZ

- Le modèle de sécurité périmétrique applique les mêmes principes que la ville fortifiée

- Au sein d'un SI, la ligne de défense est généralement élaborée au travers d'une zone démilitarisée dont l'objectif est de concentrer les flux entrants et sortants du système d'information en un point unique.

- Le filtrage de ces flux est concentré en un point dont l'élément technique de base est le pare-feu (firewall).

Sécurité périmétrique - DMZ

- Afin de permettre de déterminer un équilibre entre les besoins d'échanger et l'exposition aux menaces et vulnérabilités, la DMZ permet de définir deux types de zones :
  - l'une plutôt ouverte aux internautes et potentiellement aux ennemis : les systèmes sont dits « sacrifiables », il s'agit de serveurs accessibles au public comme ceux du e-commerce ou web ou FTP. On y trouve également des données techniques pour le besoin de services comme les DNS et SMTP (Simple Mail Transfer Protocol) ;
  - l'autre plutôt ouverte aux partenaires et potentiellement amis, hébergeant également des données communes et propres aux zones publiques et privées comme les certificats ou les serveurs d'authentification.
- La première étape sera d'effectuer un cloisonnement entre privé et public à chaque niveau : câblage, réseau, applicatif. À des fins de surveillance, des sondes seront déployées sur les points stratégiques de la DMZ

Sécurité périmétrique - firewall

- La pièce maîtresse d'une zone démilitarisée (DMZ) est constituée d'un pare-feu.
- Entrant par le biais de l'accès WAN (Wide Area Network), chaque paquet fait l'objet d'une analyse fine avant d'être autorisé au transit sur le système.
- Plus encore, le pare-feu conserve en mémoire plusieurs paquets afin de valider leurs liens éventuellement suspects.
- Un pare-feu est utilisé principalement en coupure, en bordure du réseau privé d'entreprises et du réseau public.

Sécurité périmétrique - firewall

- Il contient un ensemble de règles prédéfinies permettant :
  - soit d'autoriser uniquement les communications ayant été explicitement autorisées
  - soit d'empêcher les échanges qui ont été explicitement interdits

- Le choix de l'une ou l'autre de ces méthodes dépend de la politique de sécurité adoptée par l'entité désirant mettre en œuvre un filtrage des communications.

- La première méthode est la plus sûre mais elle impose toutefois une définition précise et contraignante des besoins en termes de communication.

Sécurité périmétrique - firewall

- Aujourd'hui le pare feu est l'un des éléments essentiels de la sécurité réseau.

- Tous les principaux pare-feux du marché sont statefull, gèrent le niveau 3 et 4, et apportent ainsi un premier niveau de défense périmétrique. Un pare-feu permet :
  - De dissimuler la topologie du réseau et les services vulnérables.
  - De différencier le trafic entrant et sortant.
  - De délimiter des zones de confiance: réseau local, DMZ…
  - De constituer un point d'accès distant pour l'interconnexion des réseaux d'entreprise par les connexions VPN IPSEC.

Sécurité périmétrique - firewall

- Mais la généralisation de l'accès internet ouvre une brèche dans les politiques de filtrage : le port 80, est un point de passage privilégié pour les attaquants.
  - La contamination d'un poste de travail qui rencontre une faille XSS en surfant sur internet.
  - Les attaques de niveau applicatives vers les serveurs Web.
  - Les courriels avec des pièces jointes infectées ou pourriels, qui vont êtres relayés au moins jusqu'au serveur de mail interne.
  - La mobilité et le BYOD entrainent le risque de la connexion au réseau local d'un poste de travail ou terminal contaminé par un virus.
  - Le trafic chiffré avec SSL/TLS permet de faire passer du trafic malveillant sans possibilité de contrôle.

Sécurité périmétrique - firewall

- La réponse pour lutter contre ces menaces a été l'UTM : Unified Threat Management.

- C'est la possibilité de filtrer les paquets jusqu'au niveau 7 (applicatif) du modèle OSI. En analysant le trafic à la volée, et en le comparant à des bases de signature ou des modèles heuristiques, UTM permet d'accumuler sur un unique point du réseau les services suivants :
  - Filtrage au niveau IP et transport
  - Filtrage applicatif avec analyse du trafic HTTP, FTP, VoIP, P2P…
  - IPS (Intrusion Prevention system) qui va détecter ou bloquer les attaques connues à partir d'une base de signature
  - Antivirus et Antispam
  - Filtrage des URLs

Sécurité périmétrique - firewall

- Cependant il y a plusieurs inconvénients à utiliser tous les services d'UTM sur un firewall.

- En premier lieu la performance réseau. Un firewall est un point d'entrée critique exposé à un trafic très important. Déchiffrer tous les flux peut poser des problèmes de performance.

- Ensuite, cela pose un problème d'architecture sécurité. En effet cumuler toutes les fonctionnalités de sécurité sur un seul point du réseau constitue un Single Point of Failure (SPOF).

- L'indisponibilité ou la compromission du pare-feu pourrait ainsi compromettre toute la sécurité du réseau.

Sécurité périmétrique – the wall

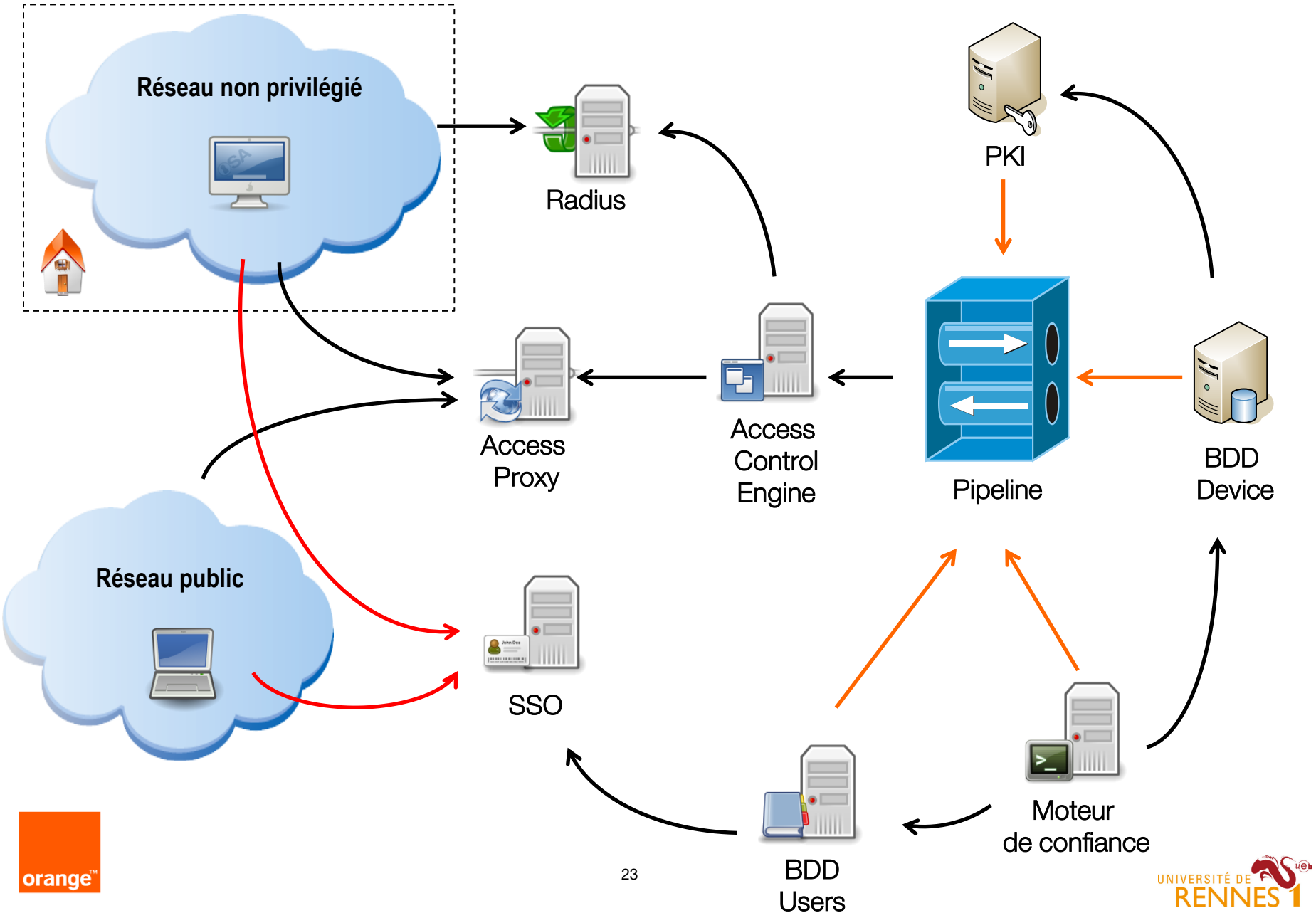
Sommaire

partie 1 : histoire de la sécurité informatique

partie 2 : sécurité périmétrique

partie 3 : BeyondCorp

BeyondCorp


Réseau non privilégié
Radius
PKI
Access
Proxy
Access
Control
Engine
Pipeline
BDD
Device
Réseau public
SSO
BDD
Users
Moteur
de confiance

Approche BeyondCorp

- Identifier le terminal
- Identifier l'utilisateur
- Supprimer la confiance dans le réseau
- Externaliser les applications et workflows
- Contrôle d'accès basé sur l'inventaire

Approche BeyondCorp

- Identifier le terminal
- Identifier l'utilisateur
- Supprimer la confiance dans le réseau
- Externaliser les applications et workflows
- Contrôle d'accès basé sur l'inventaire

Identifier le terminal - Base de donnée d'inventaire

- L'approche BeyondCorp utilise le concept de terminal infogéré
- Seuls les terminaux infogérés peuvent accéder aux applications de l'entreprise.
- Le processus de suivi et d'approvisionnement des périphériques alimentant une base de données d'inventaire de périphériques est l'une des pierres angulaires de ce modèle
- Un terminal évolue lors de son cycle de vie, BeyondCorp est conçu pour conserver les traces des différents changements faits sur le terminal.

Identifier le terminal - Base de donnée d'inventaire

- Les changements sur un terminal sont monitorés, analysés et rendus disponibles aux autres briques de BeyondCorp

- Comme une entreprise peut avoir plusieurs bases de données d'inventaire, une BDD centrale est mise en œuvre pour concentrer et normaliser les informations sur les terminaux

- Cette BDD centrale rend disponibles les informations sur les terminaux pour les systèmes avals.

Identifier le terminal - Identité du terminal

- Tous les terminaux infogérés doivent être identifiés de manière unique afin de correspondre aux entrées de la BDD d'inventaire.

- Un moyen d'arriver à cette identification est d'utiliser un certificat numérique, spécifique pour chaque terminal.

- Pour recevoir un certificat, un terminal doit être présent et correspondre au données de la base de donnée d'inventaire.

- Le certificat est stocké dans un module TPM logiciel ou physique voire un magasin de certificats.

Identifier le terminal - Identité du terminal

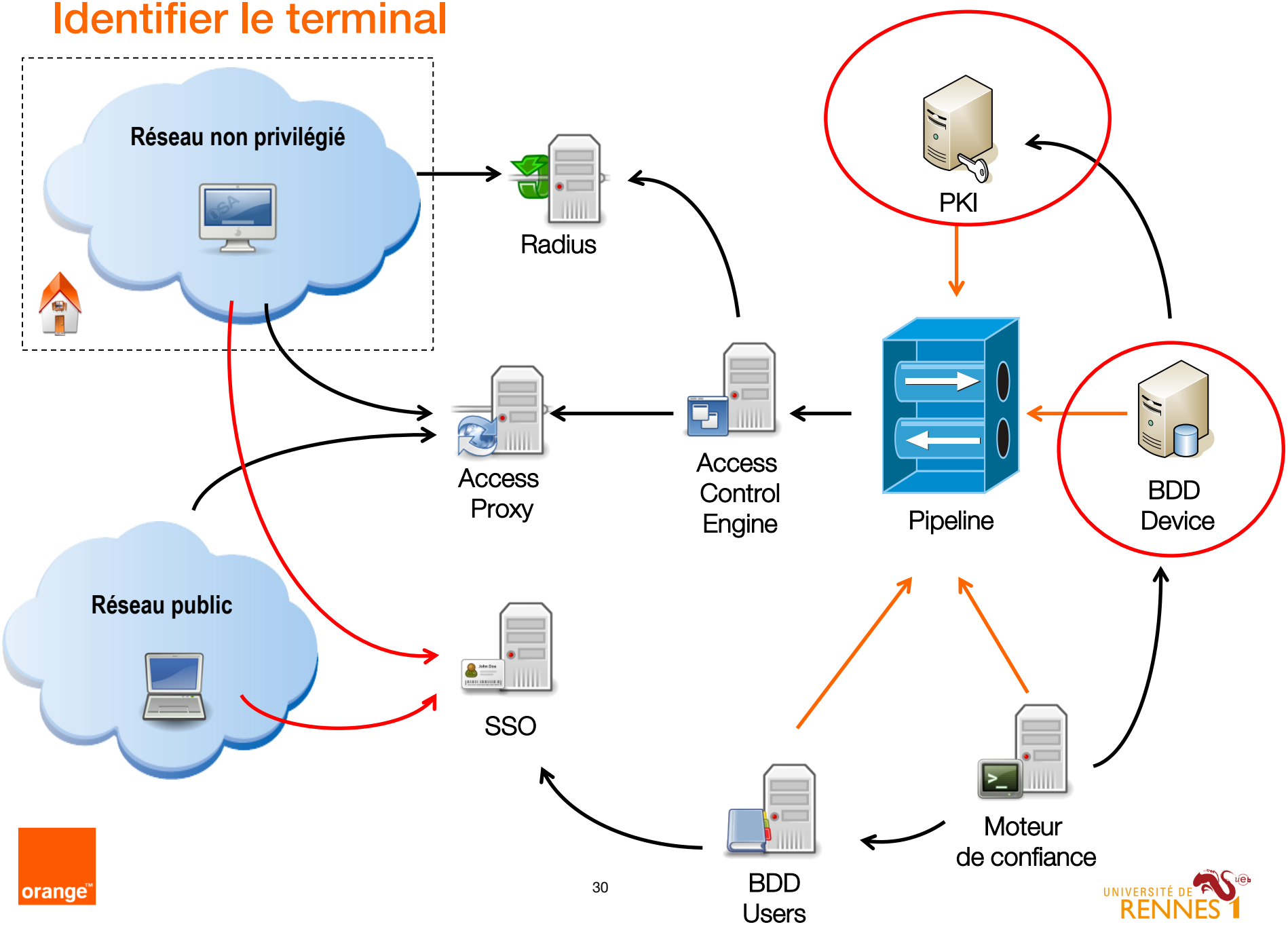
- Le processus de qualification du terminal valide ou non l'usage du magasin des certificats, et seuls les terminaux considérés comme suffisamment sûrs peuvent être classés comme des terminaux infogérés.

- Ces vérifications sont renforcées par un renouvellement périodique des certificats

- Une fois installé, le certificat est utilisé dans toutes les communications avec les services de l'entreprise.

- Le certificat identifiant le terminal mais ne lui permettant pas à lui-seul de fournir des privilèges d'accès.

Identifier le terminal



Approche BeyondCorp

- Identifier le terminal
- Identifier l'utilisateur
- Supprimer la confiance dans le réseau
- Externaliser les applications et workflows
- Contrôle d'accès basé sur l'inventaire

Identifier l'utilisateur – BDD des utilisateurs et groupes

- BeyondCorp aussi trace et gère tous les utilisateurs dans une BDD des utilisateurs et des groupes.

- Cette base de données est intimement liée aux processus RH de l'entreprise afin de gérer la catégorisation des emplois, les login et l'appartenance aux groupes pour tous les utilisateurs.

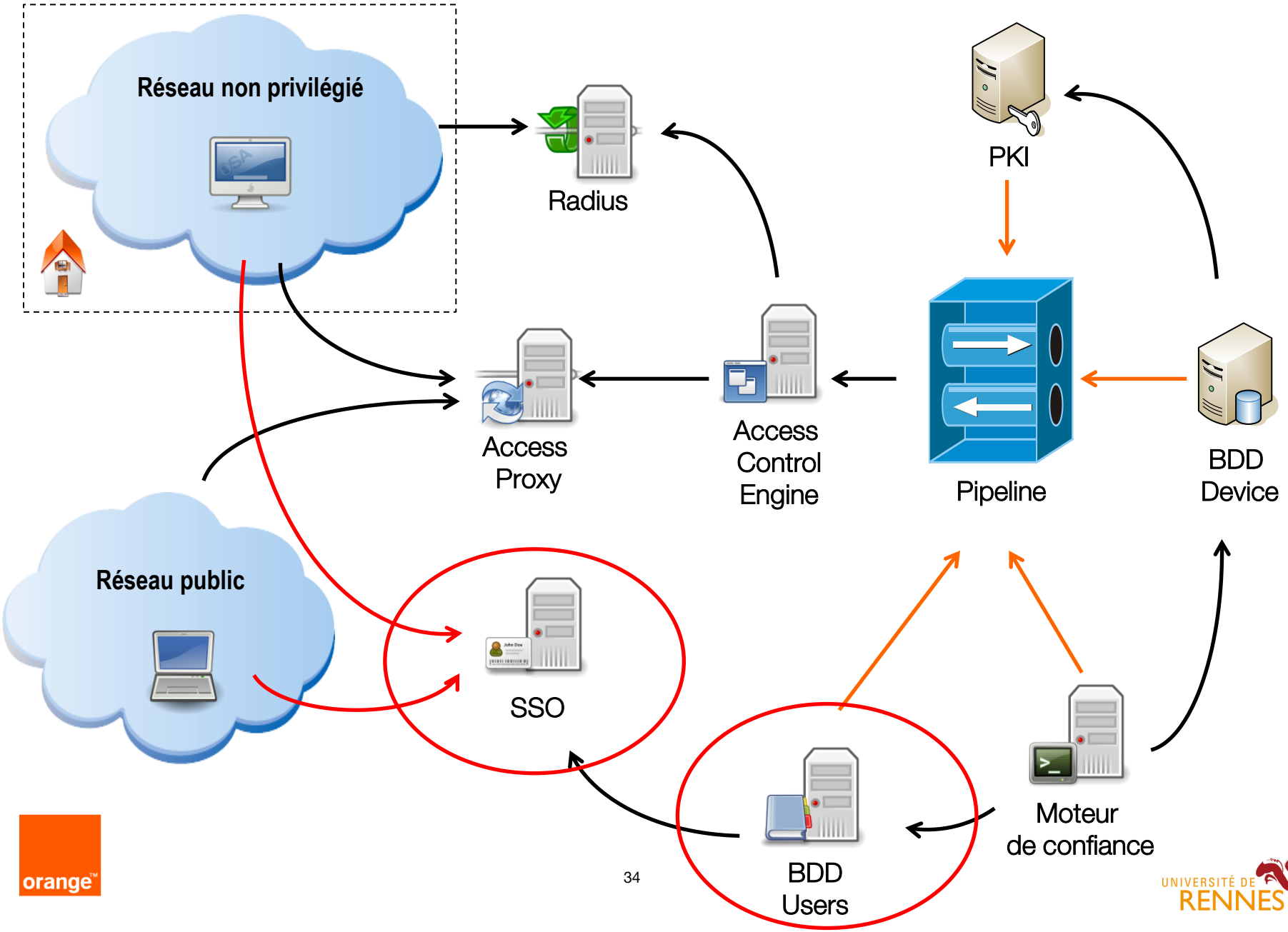
- A chaque arrivée d'employé, changement de rôle ou de responsabilité, voire de cessation d'activité, la base de données est mise à jour.

- Ce système permet de savoir toutes les informations nécessaires sur les utilisateurs qui doivent accéder aux ressources de l'entreprise

Identifier l'utilisateur - Système de SSO

- Un système de SSO externalisé est utilisé en tant que portail d'authentification des utilisateurs.
- Ce portail valide les facteurs primaires et secondaires d'authentification des utilisateurs demandant l'accès aux ressources de l'entreprise.
- Après validation auprès de la BDD des utilisateurs et des groupes, le système de SSO génère des jetons avec une courte durée de vie
- Ces jetons peuvent être utilisé comme élément du processus d'autorisation d'accès aux ressources.

Identifier l'utilisateur



Approche BeyondCorp

- Identifier le terminal
- Identifier l'utilisateur
- Supprimer la confiance dans le réseau
- Externaliser les applications et workflows
- Contrôle d'accès basé sur l'inventaire

Confiance du réseau - Réseau sans privilèges

- Afin d'égaliser accès local et distant, BeyondCorp définit et déploie un réseau sans privilèges qui ressemble de très près à un réseau externe, en conservant un adressage privé.

- Le réseau sans privilèges ne se connecte qu'à Internet, des services d'infrastructure limités (i.e. DNS, DHCP, and NTP), et des systèmes de gestion de configuration comme Puppet ou Ansible.

- Tous les terminaux sont assignés à ce réseau alors qu'il sont physiquement présents dans les locaux de l'entreprise.

- Une ACL gérée de manière très stricte fait le lien entre ce réseau et les autres parties du réseau de l'entreprise.

Confiance du réseau - Authentification 802.1X

- Pour tous les accès avec et sans fil, l'entreprise utilise des serveurs RADIUS pour assigner les terminaux à des réseaux appropriés via une authentification 802.1X

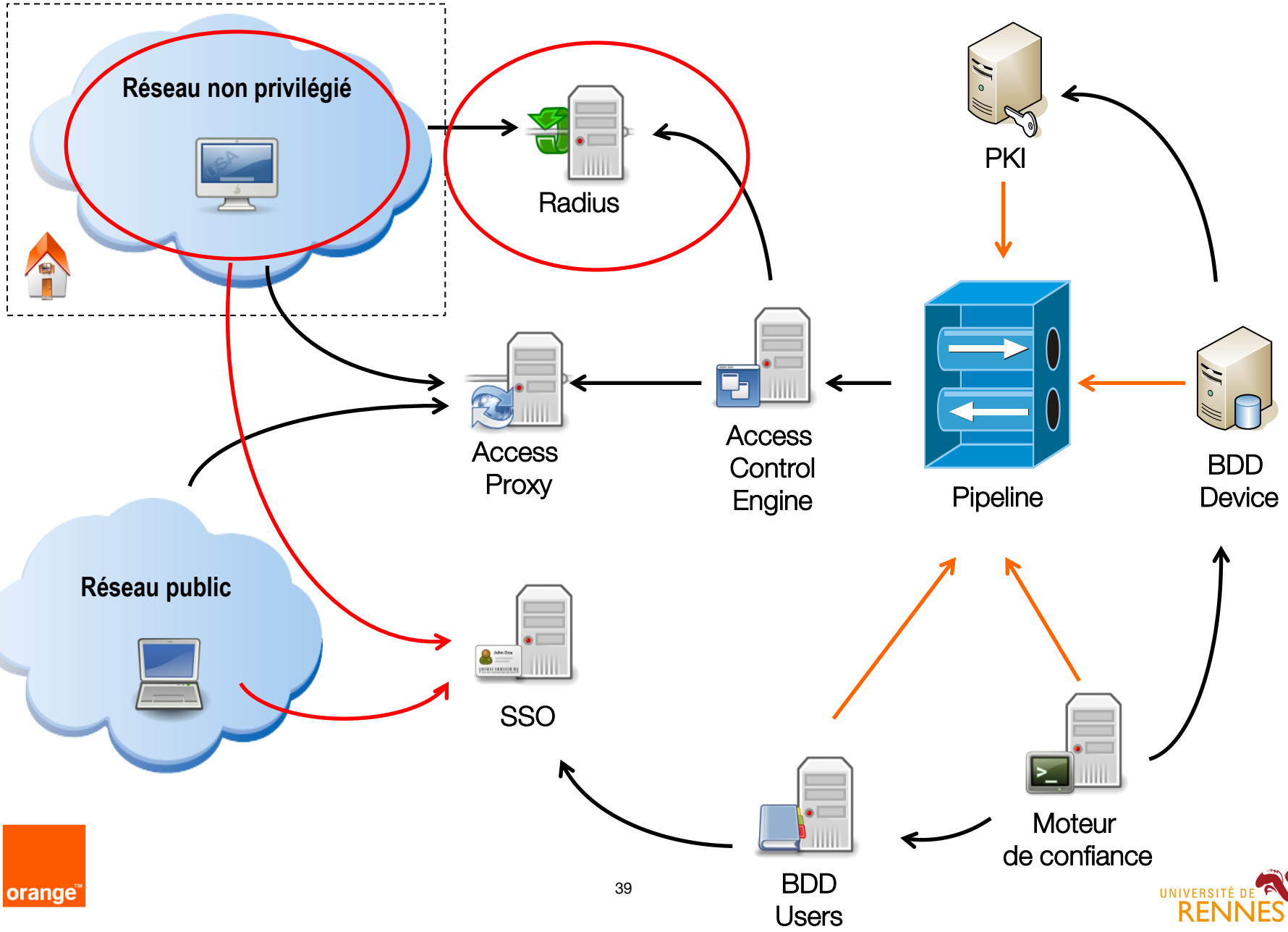
- BeyondCorp privilégie l'assignement dynamique plutôt que statique aux VLAN.

- Cette approche implique que plutôt que de se fier à la configuration statique du switch, les serveurs RADIUS informent les switch de l'assignement approprié au bon VLAN pour le terminal authentifié.

Confiance du réseau - Authentification 802.1X

- Les terminaux infogérés fournissent leur certificat lors du handshake 802.1X.
- Ces terminaux authentifiés sont assignés au réseau sans privilèges
- Les terminaux non-reconnus et/ou non infogérés sont assignés à un réseau de remédiation ou réseau invité

Supprimer la confiance dans le réseau



Approche BeyondCorp

- Identifier le terminal
- Identifier l'utilisateur
- Supprimer la confiance dans le réseau
- Externaliser les applications et workflows
- Contrôle d'accès basé sur l'inventaire

Externaliser les applications - Proxy d'accès

- Toutes les applications de l'entreprise sont exposées aux clients externes et internes via un proxy d'accès sur Internet. Ce proxy impose le chiffrement entre le client et l'application

- Ce proxy est configuré pour chaque application et fournit des fonctionnalités de base telles que :
  - accessibilité globale
  - load balancing,
  - vérification liées au contrôle d'accès
  - santé de l'application
  - protection anti déni de service.

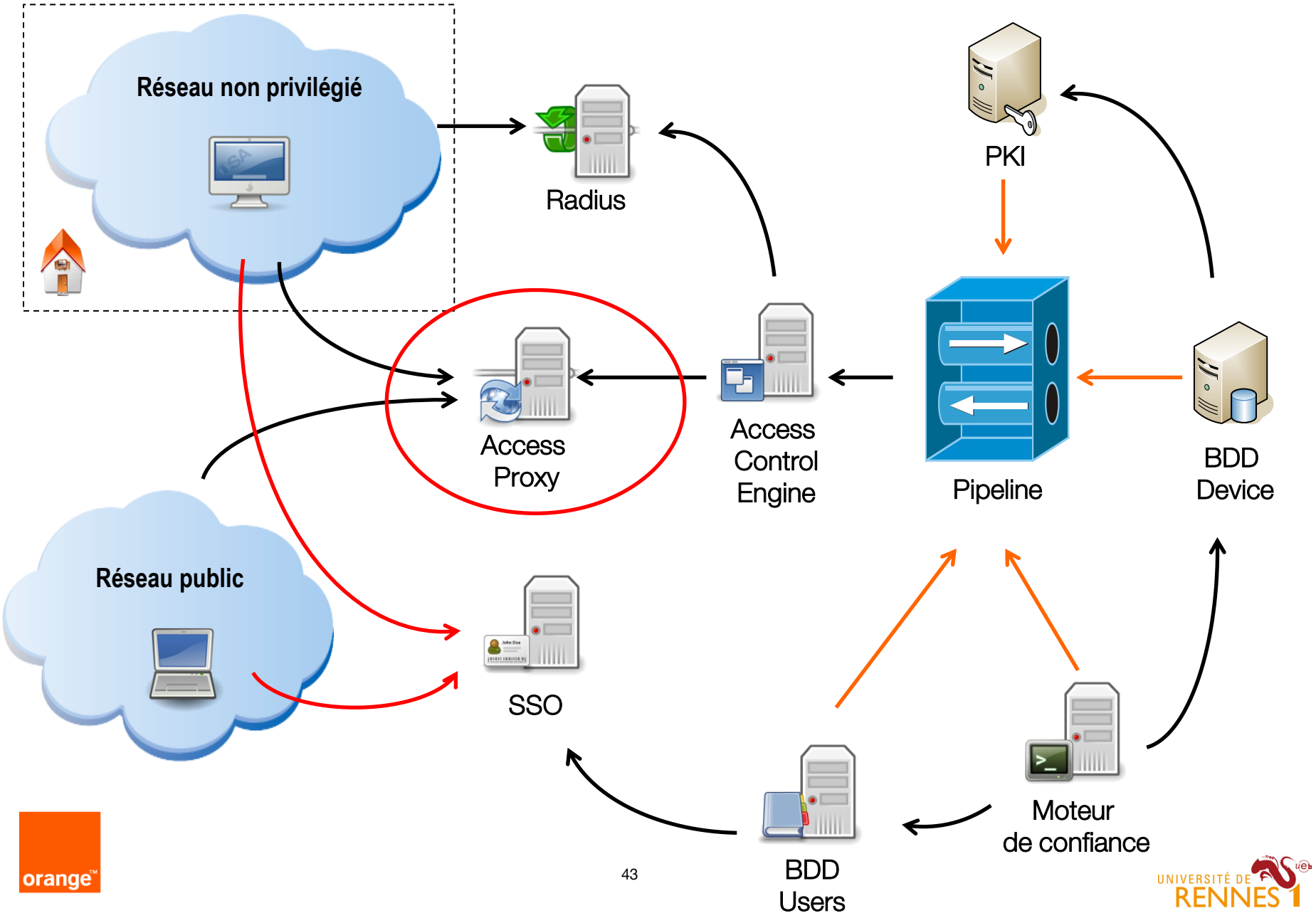
- Ce proxy délègue les requêtes considérées comme appropriées aux applications après les vérification liées au contrôle d'accès

Externaliser les applications - Entrées DNS publiques

- Toutes les applications de l'entreprise sont exposées à l'extérieur et sont enregistrées dans un DNS public

- Un CNAME pointe sur les applications via le proxy d'accès

Externaliser les applications et process



Approche BeyondCorp

- Identifier le terminal
- Identifier l'utilisateur
- Supprimer la confiance dans le réseau
- Externaliser les applications et workflows
- Contrôle d'accès basé sur l'inventaire

Contrôle d'accès - Moteur de confiance

- Le niveau d'accès donné à un utilisateur et/ou un terminal peut changer au cours du temps

- En interrogeant des sources de données multiples, il est possible de déterminer le niveau de confiance à assigner à un utilisateur ou terminal

- Ce niveau de confiance peut alors être utilisé par le gestionnaire de contrôle d'accès lors de son workflow de décision

Contrôle d'accès - Moteur de confiance

- Par exemple, un terminal qui n'a pas été mis à jour avec un patch OS récent peut être relégué à un niveau de confiance réduit

- Une classe de terminaux particulière, comme un modèle spécifique de smartphone ou tablette, peut être assigné à un niveau particuliers de confiance

- Un utilisateur accédant à des applications depuis un nouvel emplacement peut être assigné à un niveau de confiance différent.

- Des règles statiques et heuristiques sont utilisées pour déterminer ces niveaux de confiance.

Contrôle d'accès - Gestionnaire de contrôle d'accès

- Un gestionnaire de contrôle d'accès au niveau du proxy d'accès fournit un mécanisme d'autorisation du service vers les applications de l'entreprise, et ce pour chaque requête

- La décision d'autorisation établit des assertions sur l'utilisateur, les groupes auxquels il appartient et les informations du terminal issues de la base de données d'inventaire

- Si nécessaire, le gestionnaire de contrôle d'accès peut imposer un contrôle d'accès basé sur la localisation.

- Le niveau de confiance de l'utilisateur et du terminal sont aussi incorporés dans la décision d'autorisation

Contrôle d'accès - Gestionnaire de contrôle d'accès

- Par exemple, un accès au bugtracker de l'entreprise peut être restreint aux développeurs plein-temps qui utilisent un terminal de développement

- Un accès à une application financière peut être restreinte aux employés plein-temps et mi-temps appartenant au groupe des opérations financières et n'utilisant pas un terminal de développement

- Le gestionnaire de contrôle d'accès peut aussi restreindre des parties d'une application de plusieurs façons

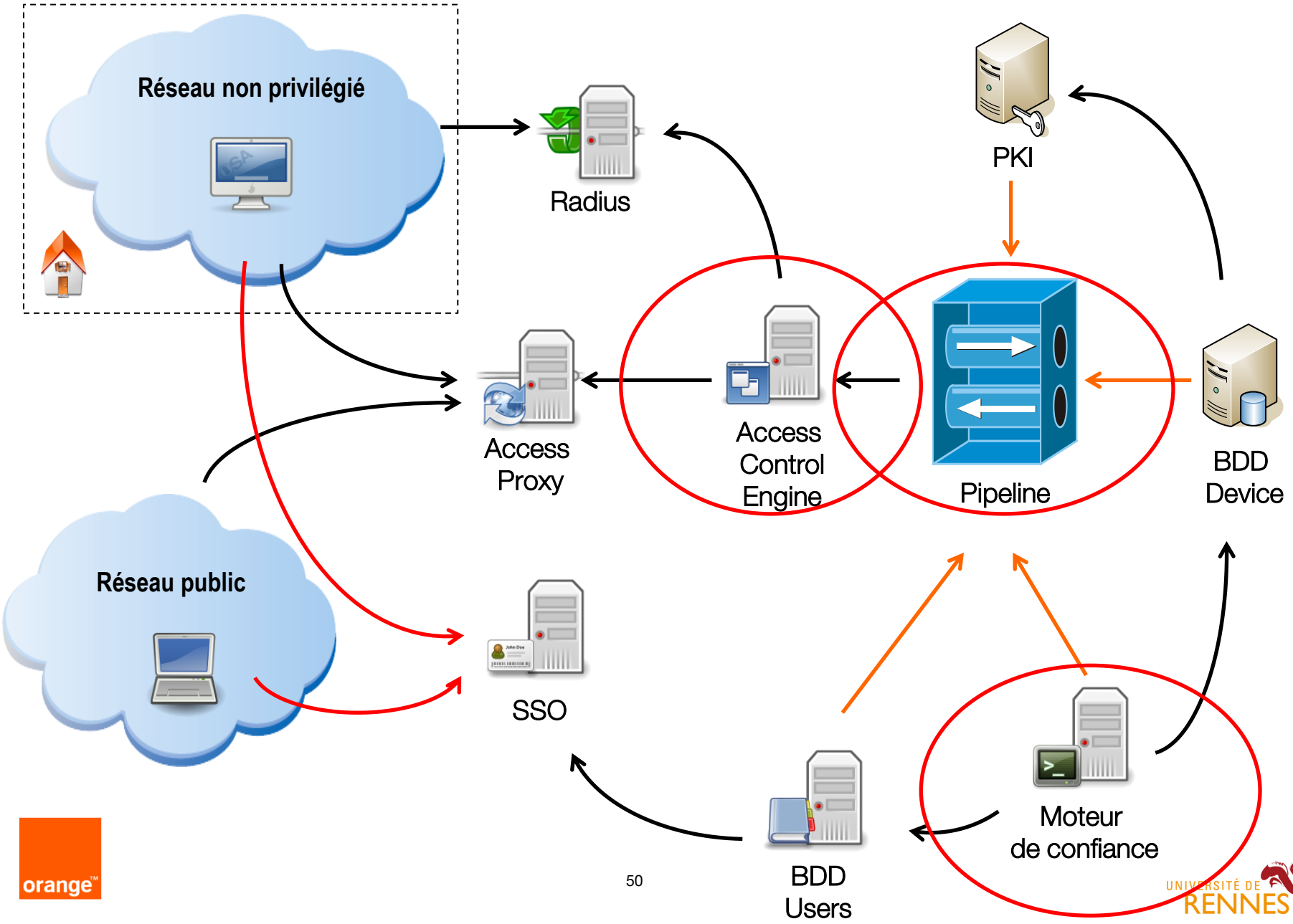
- Par exemple, accéder à une entrée dans le bugtracker peut demander un contrôle d'accès moins stricte que le mettre à jour ou effectuer des recherche

Contrôle d'accès - Pipeline de contrôle d'accès

- Le gestionnaire de contrôle d'accès est constamment alimenté par une pipeline qui extrait dynamiquement les informations utiles pour les décisions d'accès

- Ces informations incluent entre-autres :
  - Les listes blanches des certificats
  - Les niveaux de confiance des utilisateurs et terminaux
  - Les détails d'inventaire sur les utilisateurs et terminaux

Contrôle d'accès basé sur l'inventaire



Questions

orange™

UNIVERSITÉ DE RENNES 1

Merci