CA Services
Retours d'experience

Frédéric Lala

Forum SiteMinder, 8 dec 2011

Mise en oeuvre de la Fédération

Architectures et composants

ca technologies

Composants CA de Fédération d'identités

Actuellement R12

- **Un composant FSS**
  - Extension à SiteMinder
  - Permet de gérer les cas d'utilisation complexes impliquant à la fois les concepts WAC / FED
    - Directory Mapping
    - Response
    - Authentication Scheme
    - Multi protocol SAML 1.0 1.1 2.0

- **Un composant FED Manager**
  - One Point Product (aucune dépendance)
  - Limité dans les faits aux cas d'utilisation représentatifs SAML 2.0
  - Composant peu invasif à déployer chez les partenaires
    - Ne nécessite pas de modifier les applications en profondeur
    - Permet de délimiter les domaines de responsabilités entre IdP et SP

Composants CA de Fédération d'identités

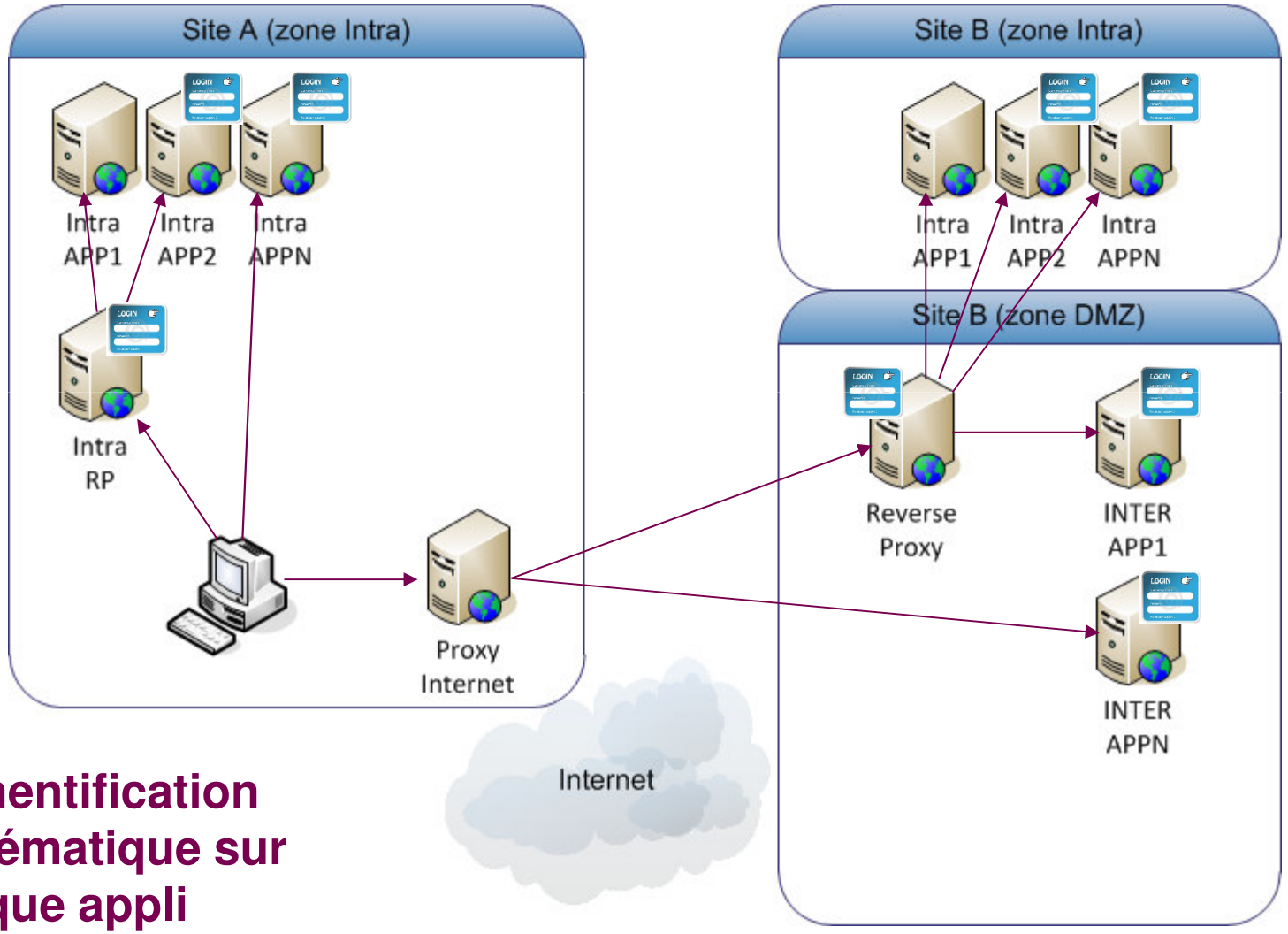
Prochainement R12.5 (TGV)

- **Rassemblement des deux types de déploiements sous le même installer**
- **Interface d'administration unique des deux types de déploiements sous la même interface**

Scénarios rencontrés

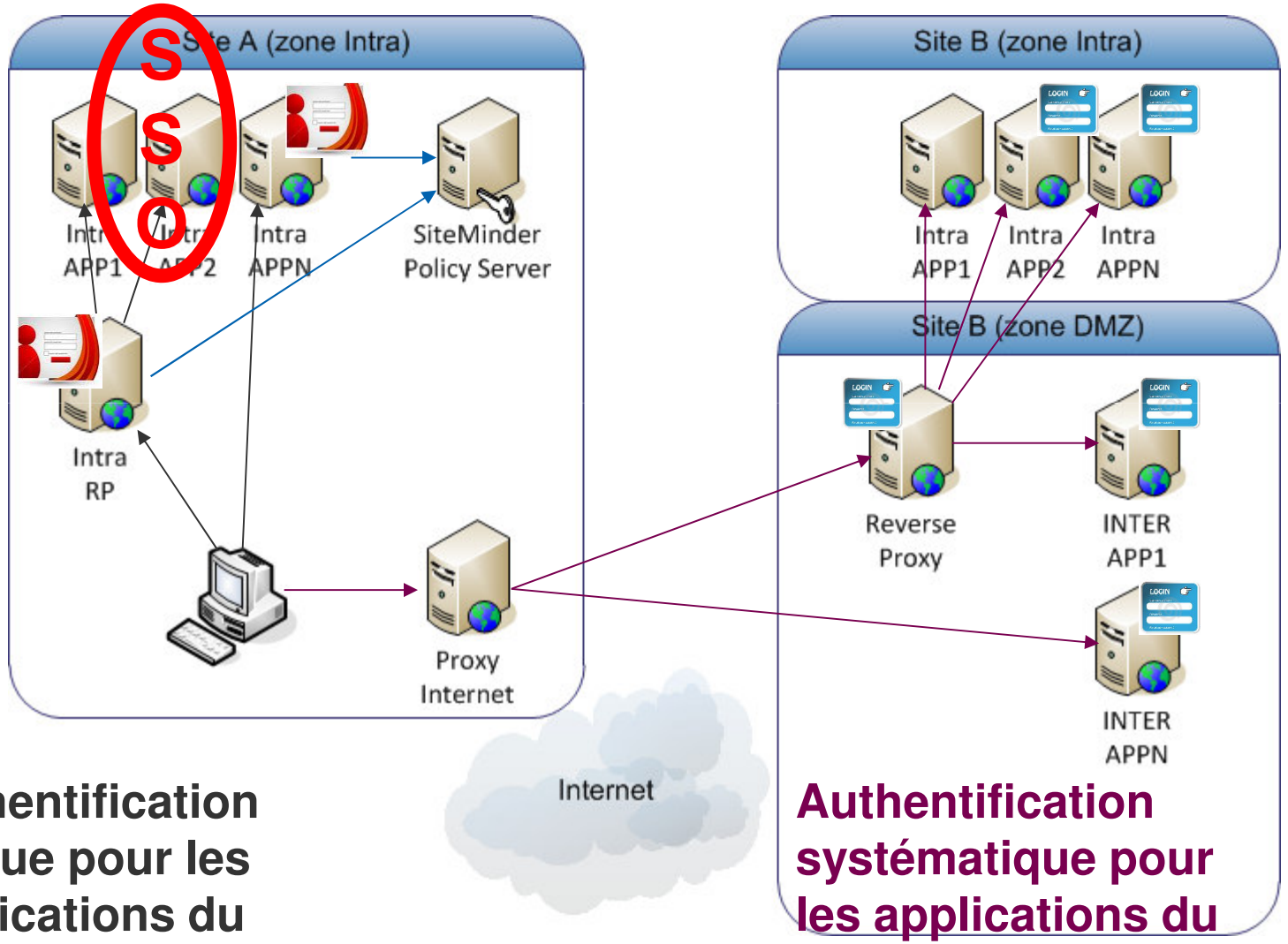
- **Scénario 1: Intra -> Partenaire**
- **Scénario 2: Partenaire -> IdP**
- **Solution de service IdP / SP**

Scénario 1: Intra -> Partenaire



Authentification systématique sur chaque appli (INTRA & EXTRA)

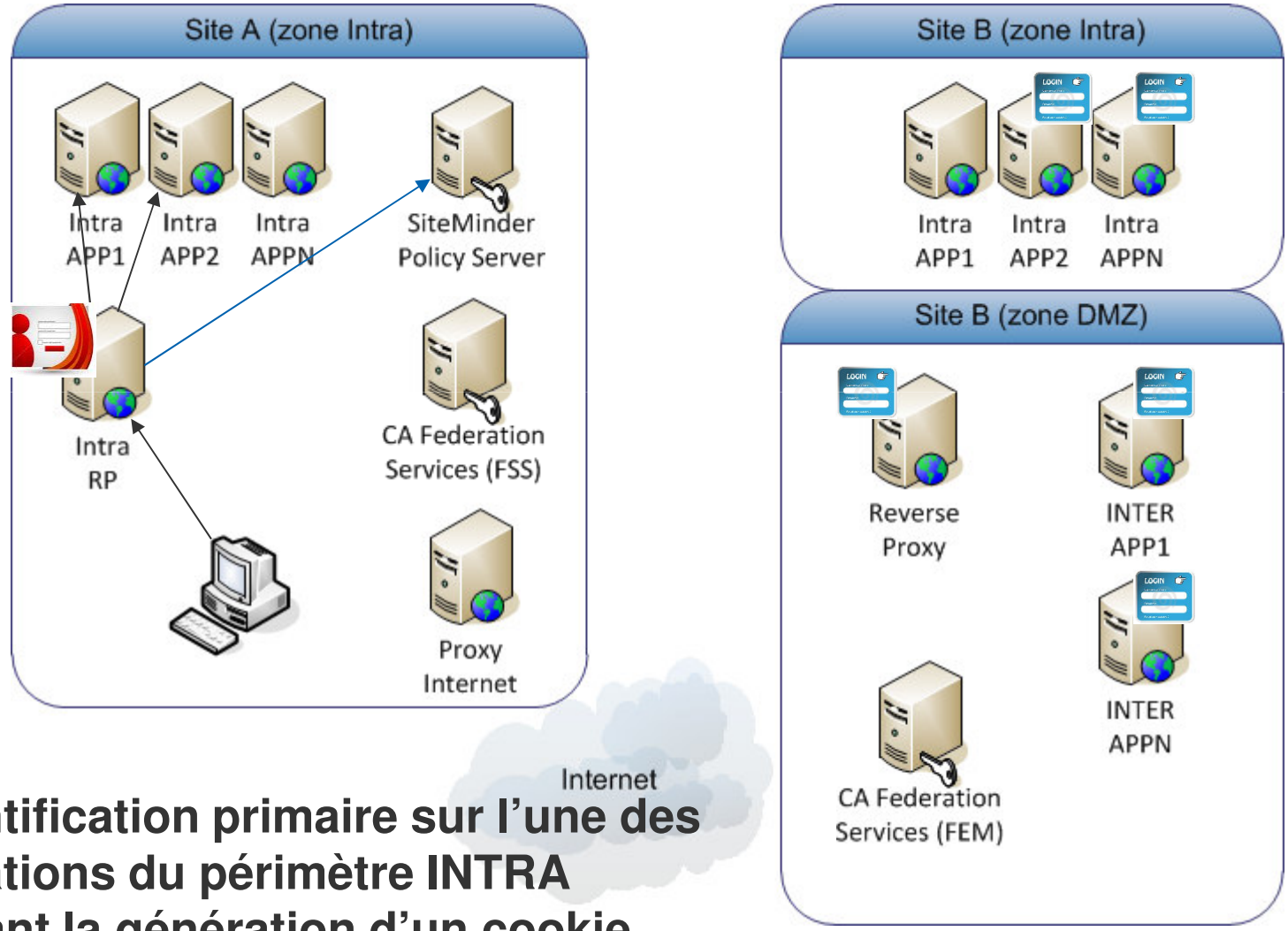
Scénario 1: Intra -> Partenaire



Authentification unique pour les applications du périmètre INTRA

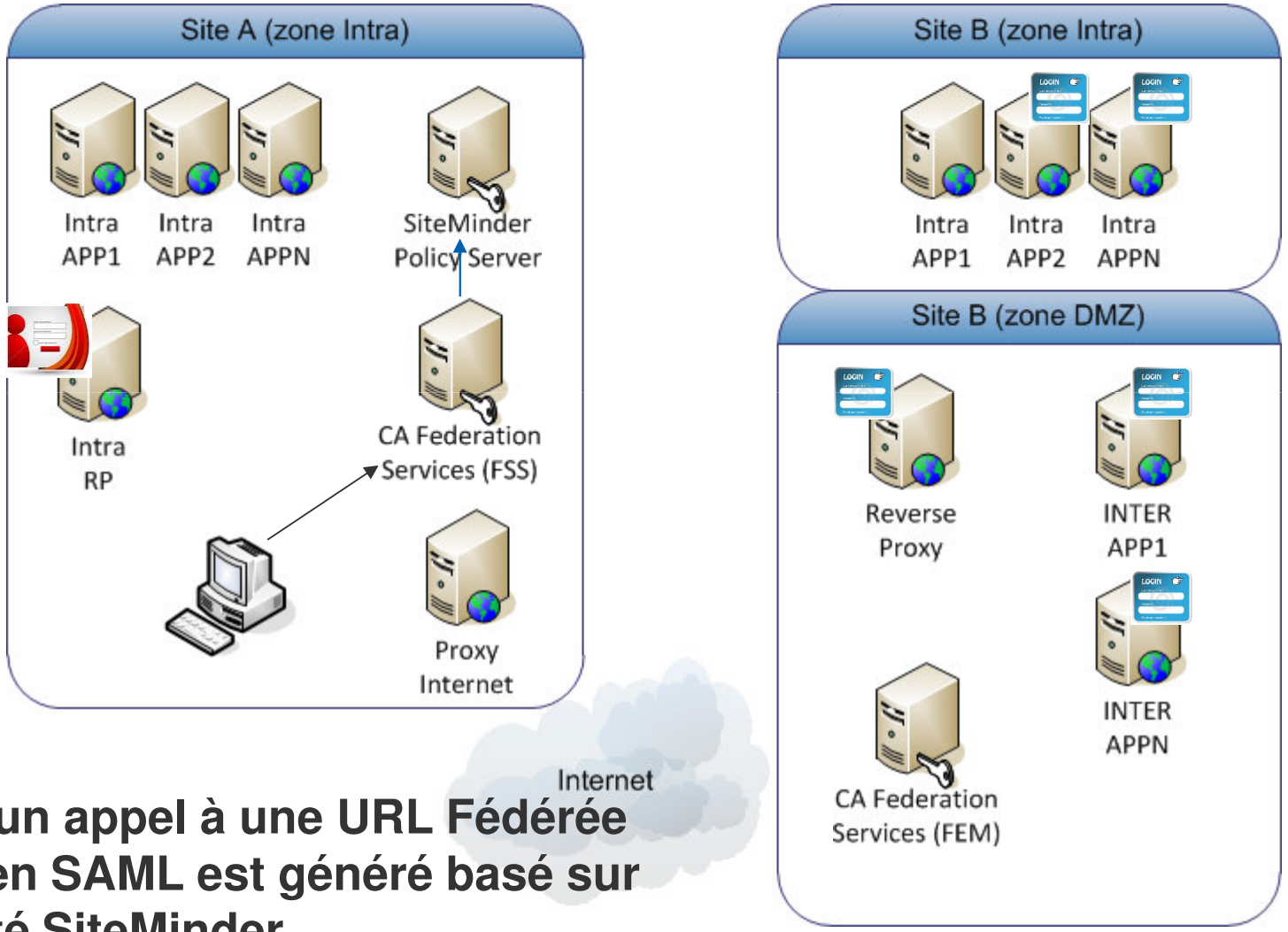
Authentification systématique pour les applications du périmètre EXTRA

Scénario 1: Intra -> Partenaire



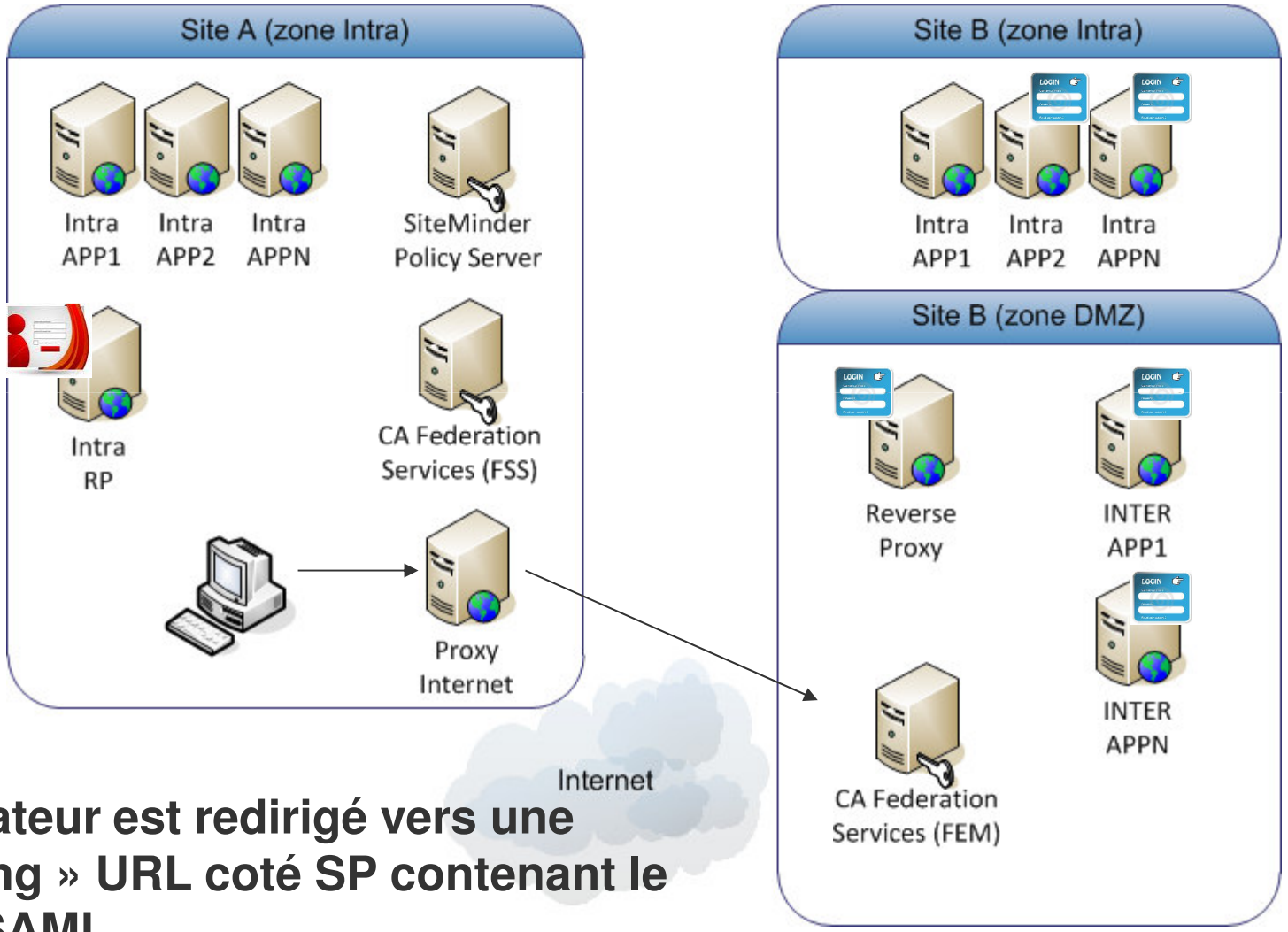
Authentification primaire sur l'une des applications du périmètre INTRA induisant la génération d'un cookie SMSESSION

Scénario 1: Intra -> Partenaire



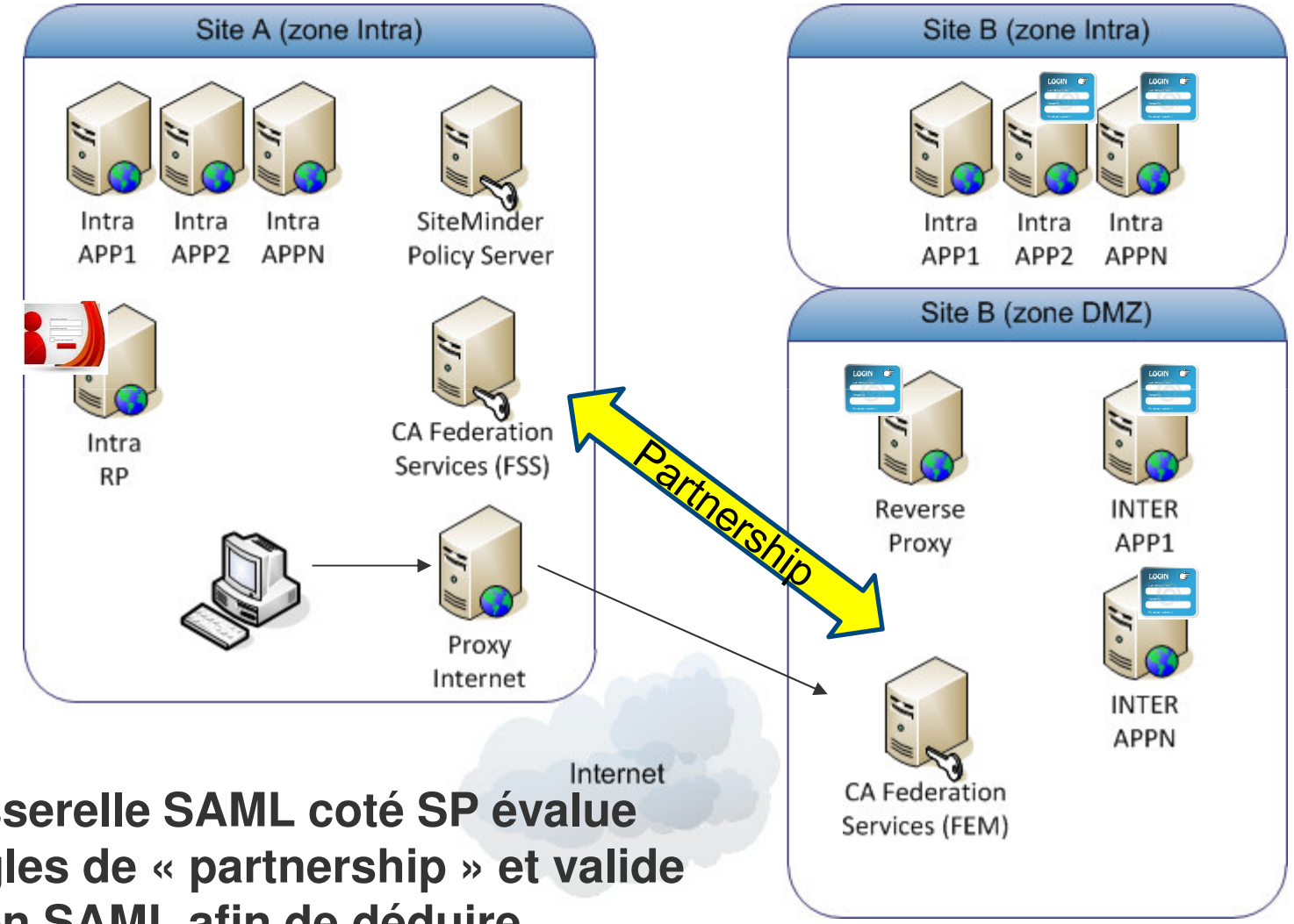
Lors d'un appel à une URL Fédérée
Un token SAML est généré basé sur l'identité SiteMinder

Scénario 1: Intra -> Partenaire



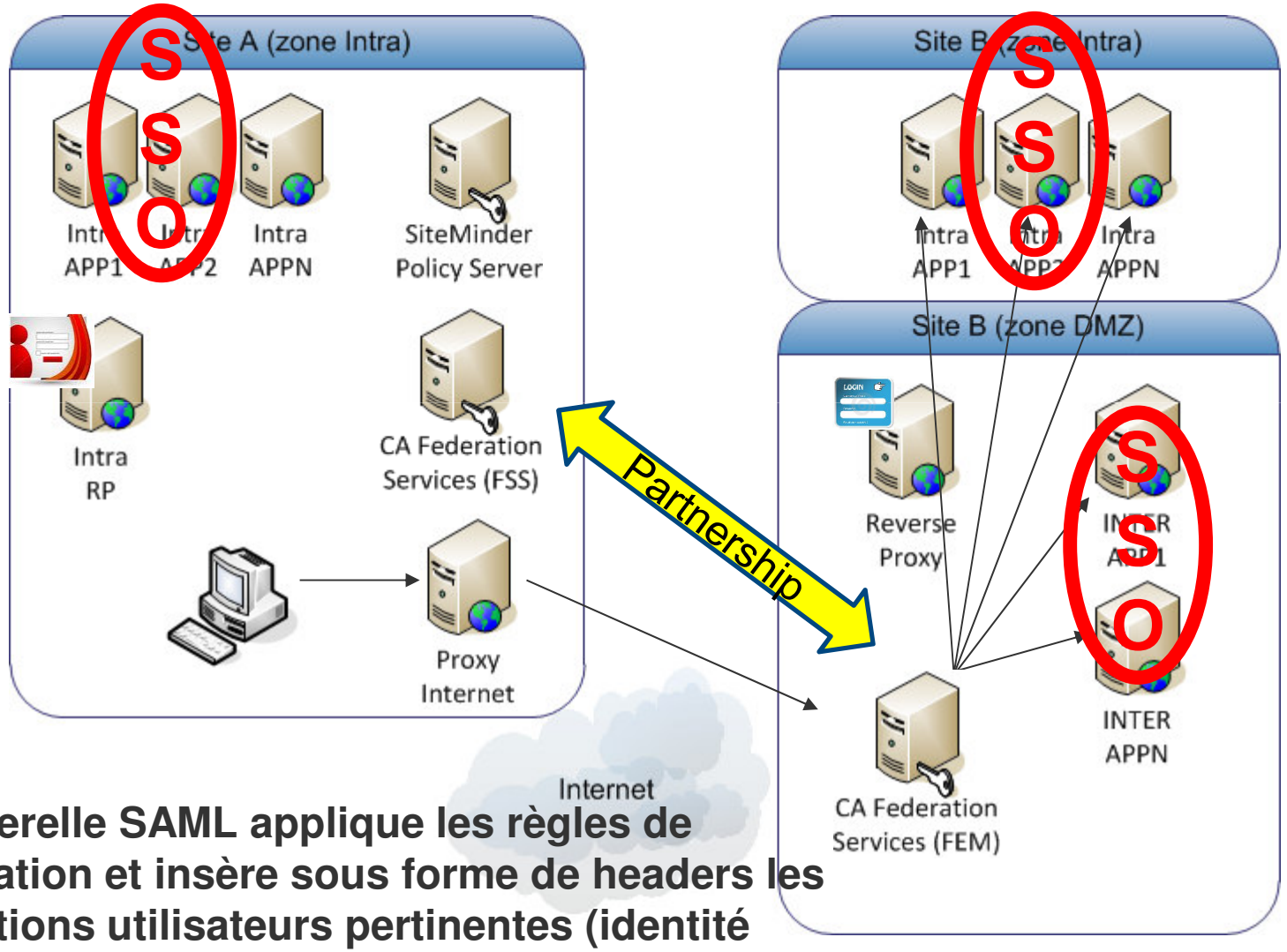
L'utilisateur est redirigé vers une « landing » URL coté SP contenant le token SAML

Scénario 1: Intra -> Partenaire



La passerelle SAML coté SP évalue les règles de « partnership » et valide le token SAML afin de déduire l'identité de l'utilisateur coté SP

Scénario 1: Intra -> Partenaire



La passerelle SAML applique les règles de proxification et insère sous forme de headers les informations utilisateurs pertinentes (identité issue de l'IdP ou du SP)

Scénario 1: Intra -> Partenaire

Coté Identity Provider

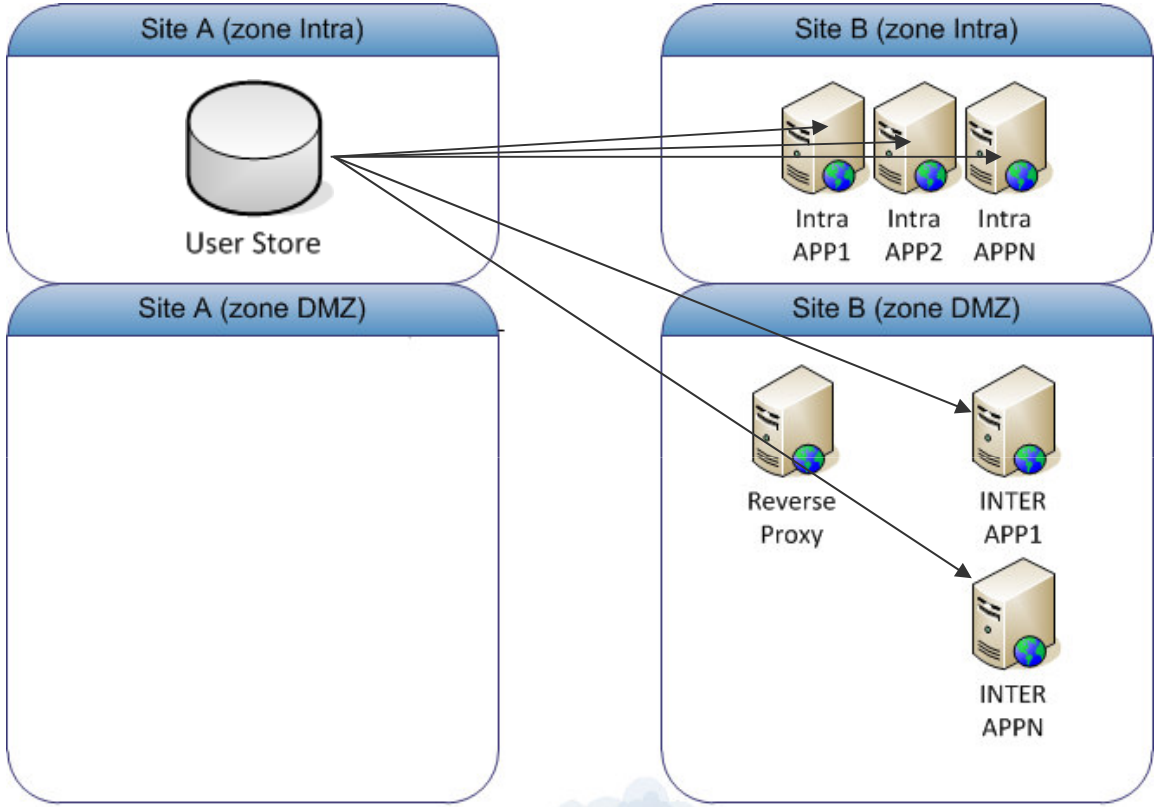
- SiteMinder déjà déployé
- SSO avéré entre les applications Intranet
- Authentification primaire réalisé sur l'infrastructure SiteMinder IdP
- Besoin de connecter des applications partenaires sans que les utilisateurs doivent se re-signer

Coté Service Provider

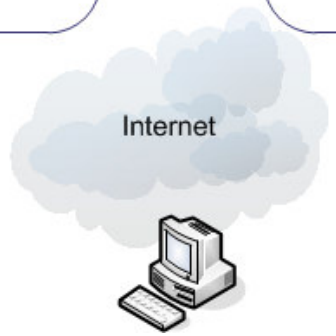
- Applications cibles (multi ou mono clients) exposées directement à partir de l'internet
- Pas de solution WAM SiteMinder déployée
- Pas de solution de fédération d'identités déployée

ca technologies

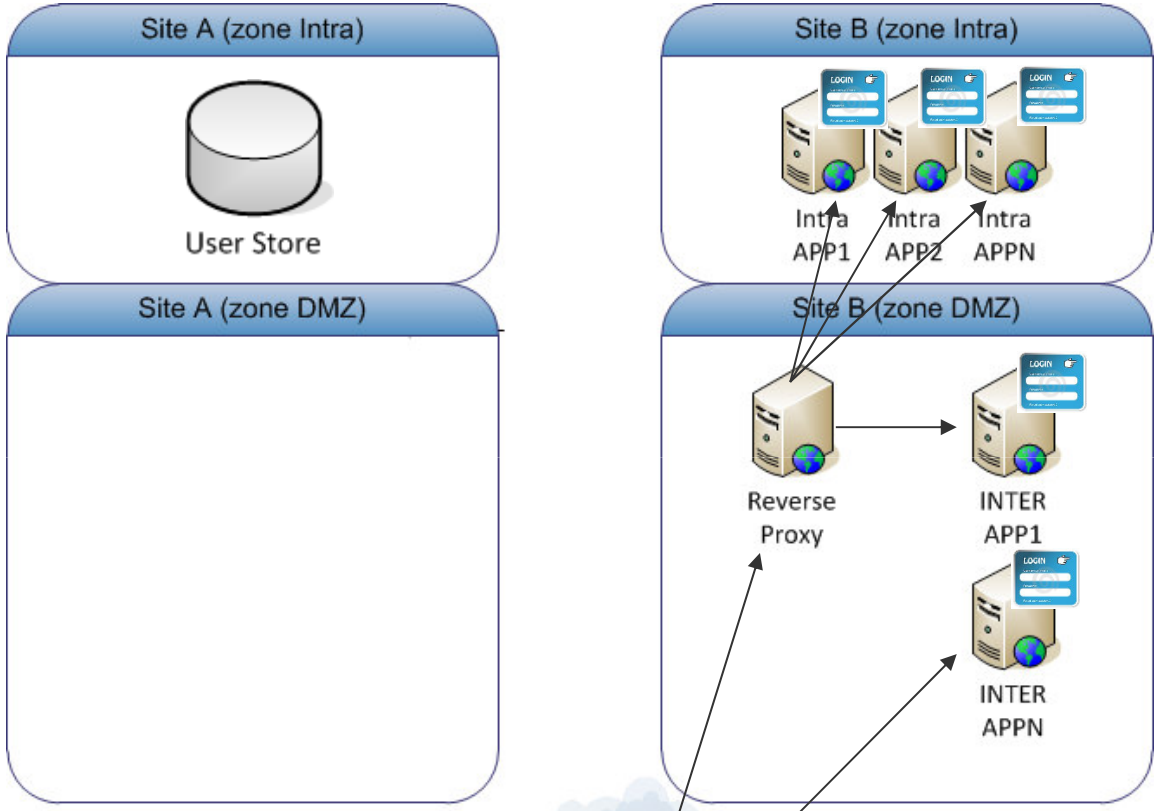
Scénario 2: Partenaire -> IdP



Un système d'extraction / provisioning des comptes client est réalisé dans les applicatifs partenaires



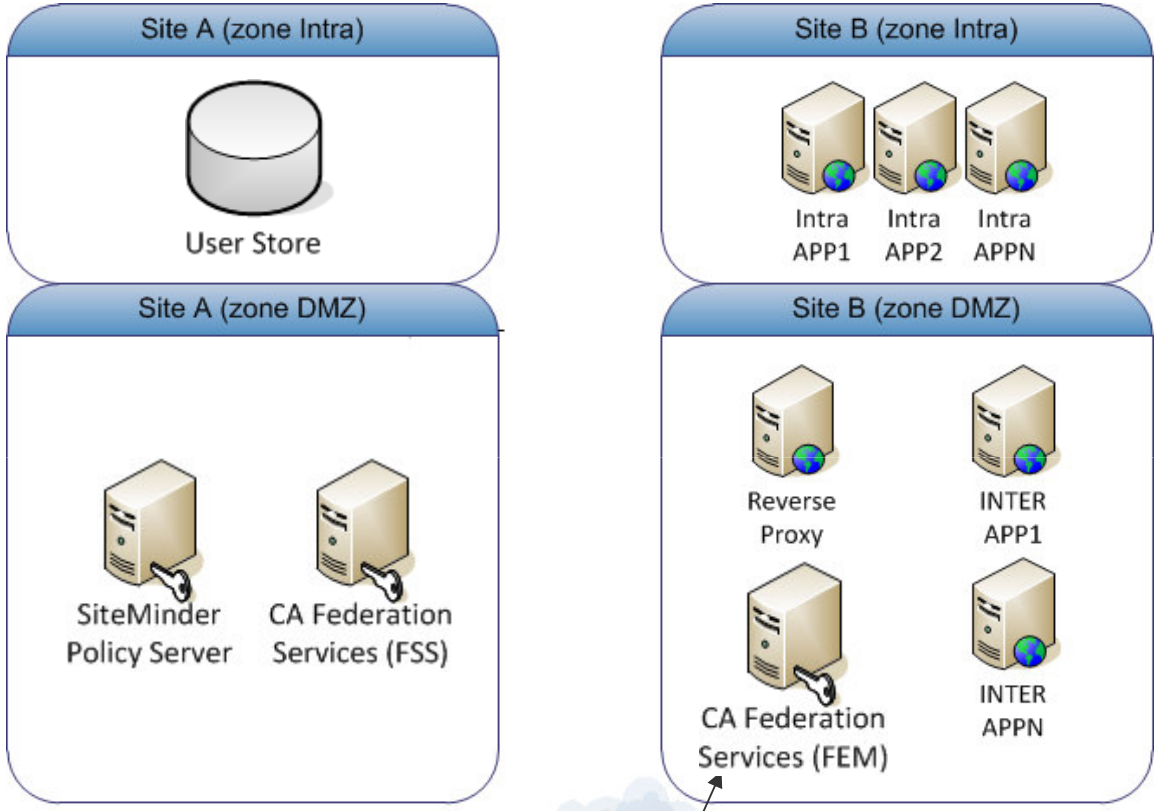
Scénario 2: Partenaire -> IdP



Les utilisateurs du site A utilisent un service du site B via Internet en utilisant leur compte provisionné au préalable

Authentification systématique avec un compte spécifique aux applicatifs partenaires

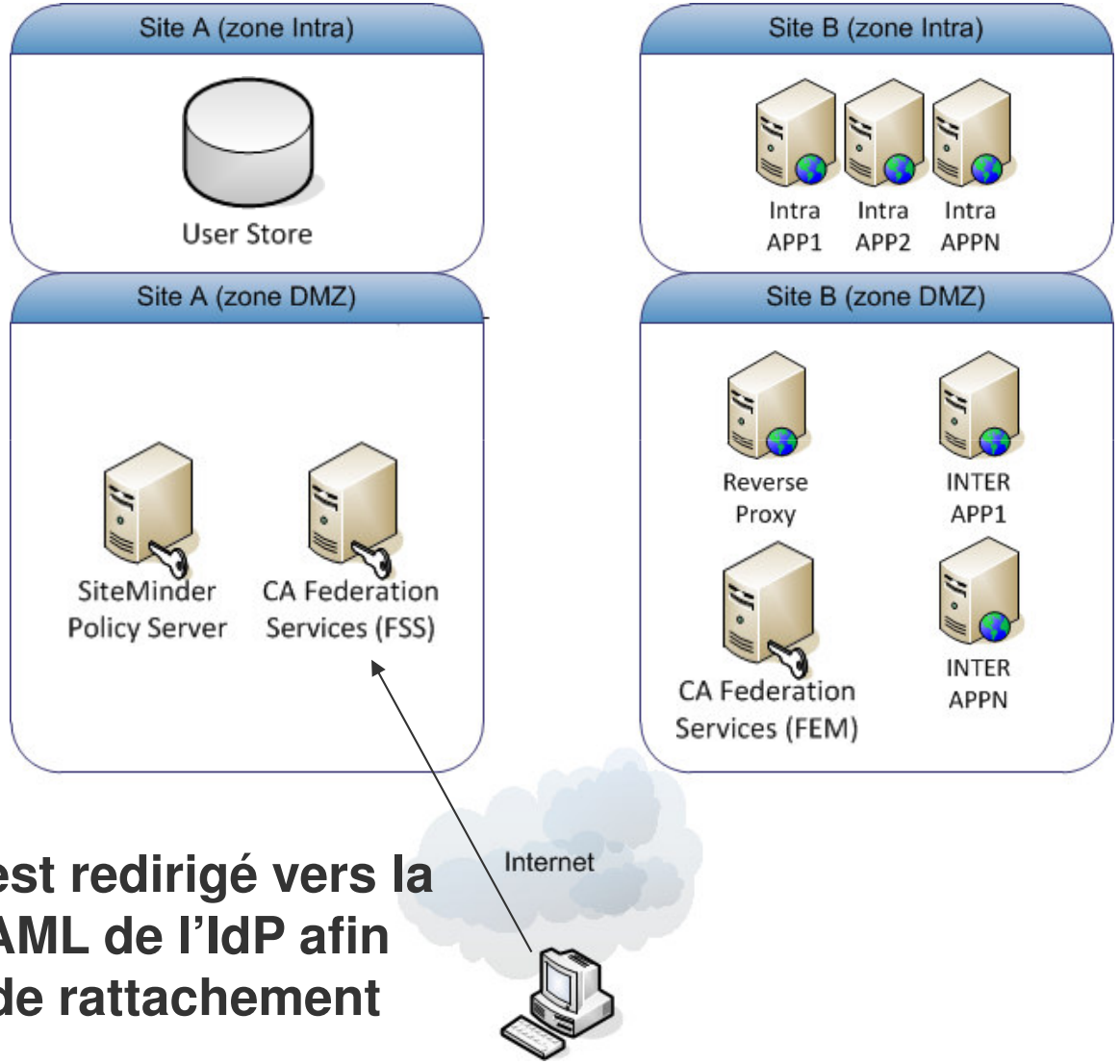
Scénario 2: Partenaire -> IdP



Les utilisateurs du site A se connectent à la passerelle SAML SP. Celui-ci redirige l'utilisateur sur la passerelle SAML de l'IdP de l'utilisateur.

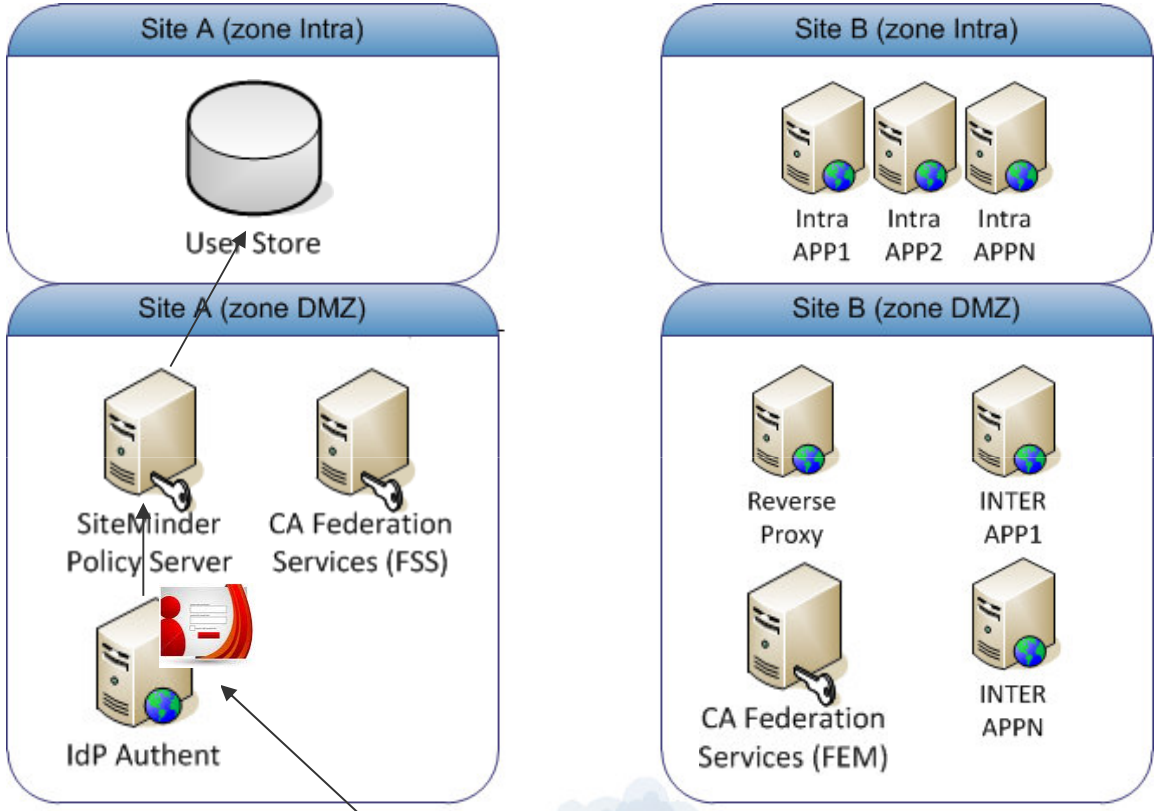
Si le SP dispose de plusieurs IdP (environnements multi clients), la fonctionnalité de IdP Discovery peut être utilisé

Scénario 2: Partenaire -> IdP



L'utilisateur est redirigé vers la passerelle SAML de l'IdP afin que son IdP de rattachement l'identifie

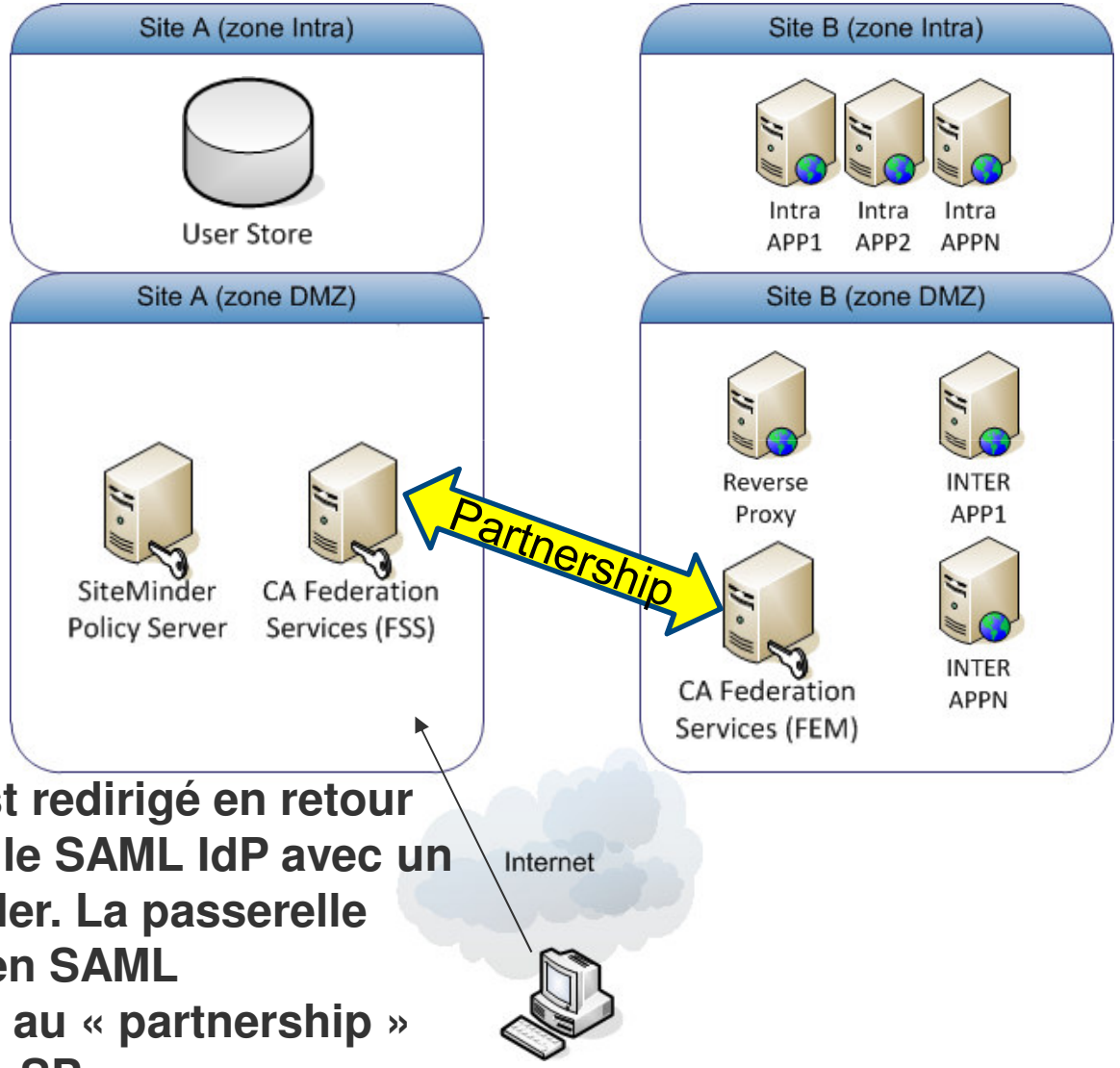
Scénario 2: Partenaire -> IdP



L'utilisateur est redirigé une page protégée par l'infrastructure SSO de l'IdP ou par une infrastructure dédiée IdP. L'utilisateur doit s'authentifier s'il ne l'ai pas déjà …

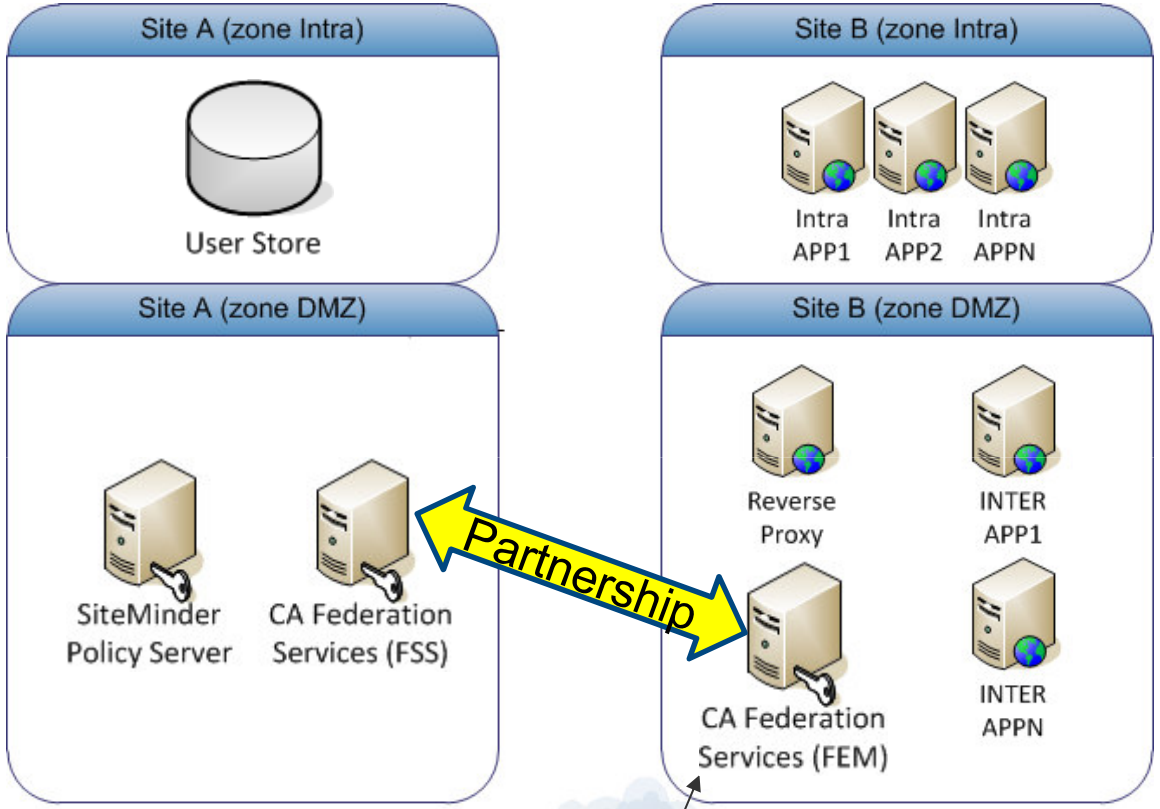
L'authentification est réalisée par le composant Policy Server sur l'annuaire de l'IdP

Scénario 2: Partenaire -> IdP



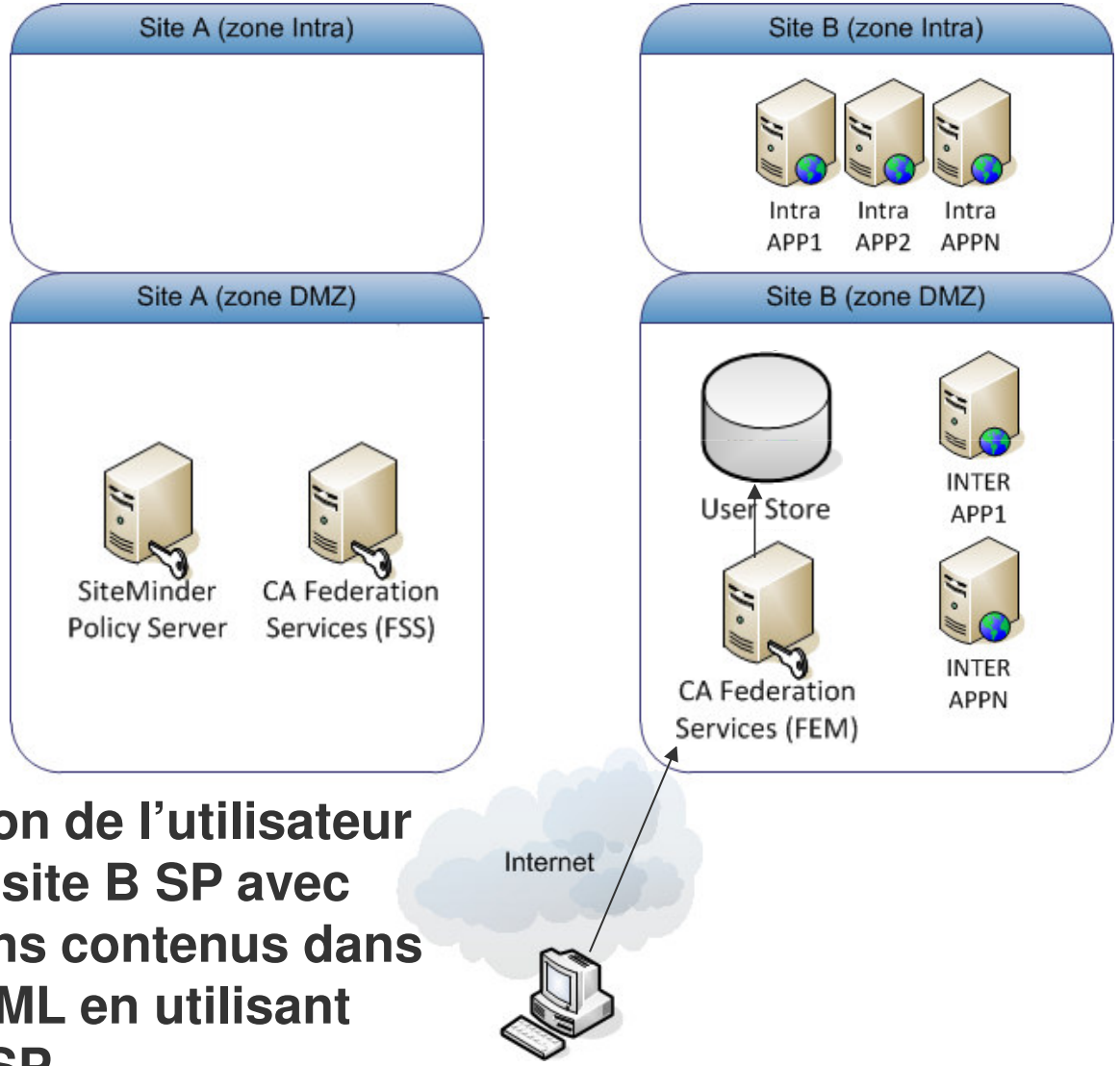
L'utilisateur est redirigé en retour sur la passerelle SAML IdP avec un token SiteMinder. La passerelle génère un token SAML conformément au « partnership » entre l'IdP et le SP

Scénario 2: Partenaire -> IdP



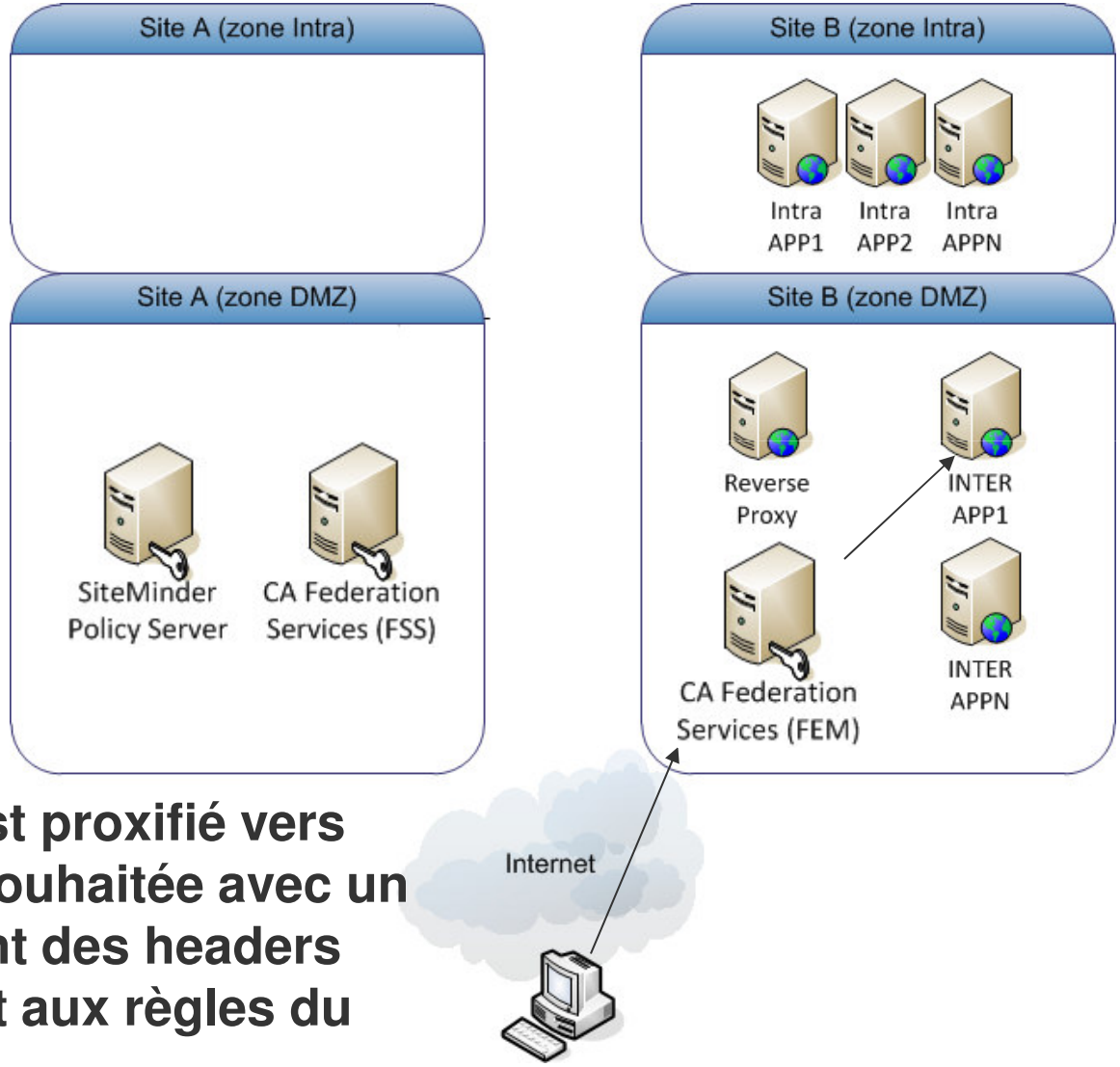
L'assertion SAML est posté sur la passerelle SAML du SP contenant toutes les informations utiles à l'identification de l'utilisateur coté SP

Scénario 2: Partenaire -> IdP



Désambiguation de l'utilisateur d'annuaire du site B SP avec les informations contenus dans l'assertion SAML en utilisant l'annuaire du SP

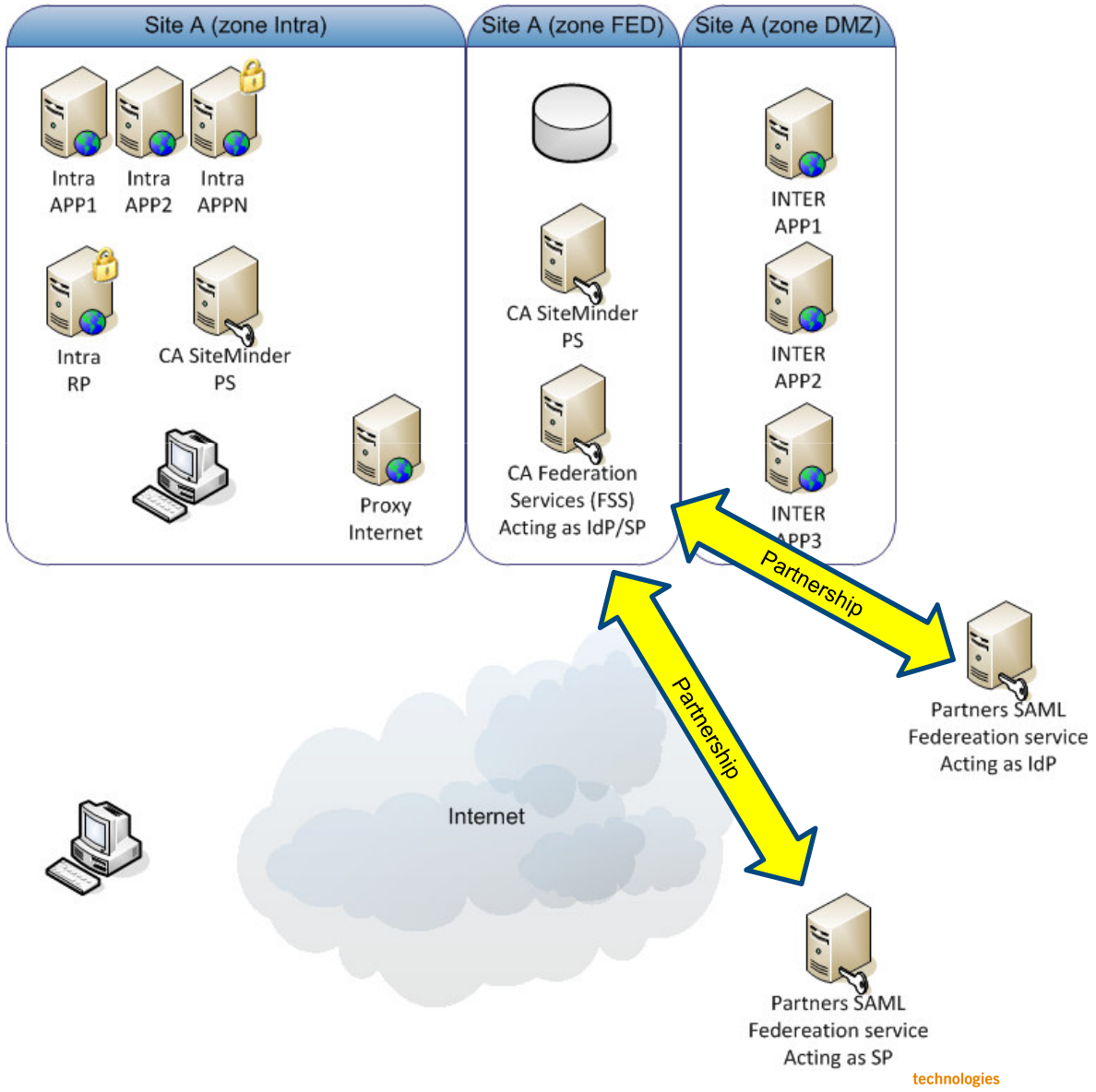
Scénario 2: Partenaire -> IdP



L'utilisateur est proxifié vers l'application souhaitée avec un enrichissement des headers conformément aux règles du SP

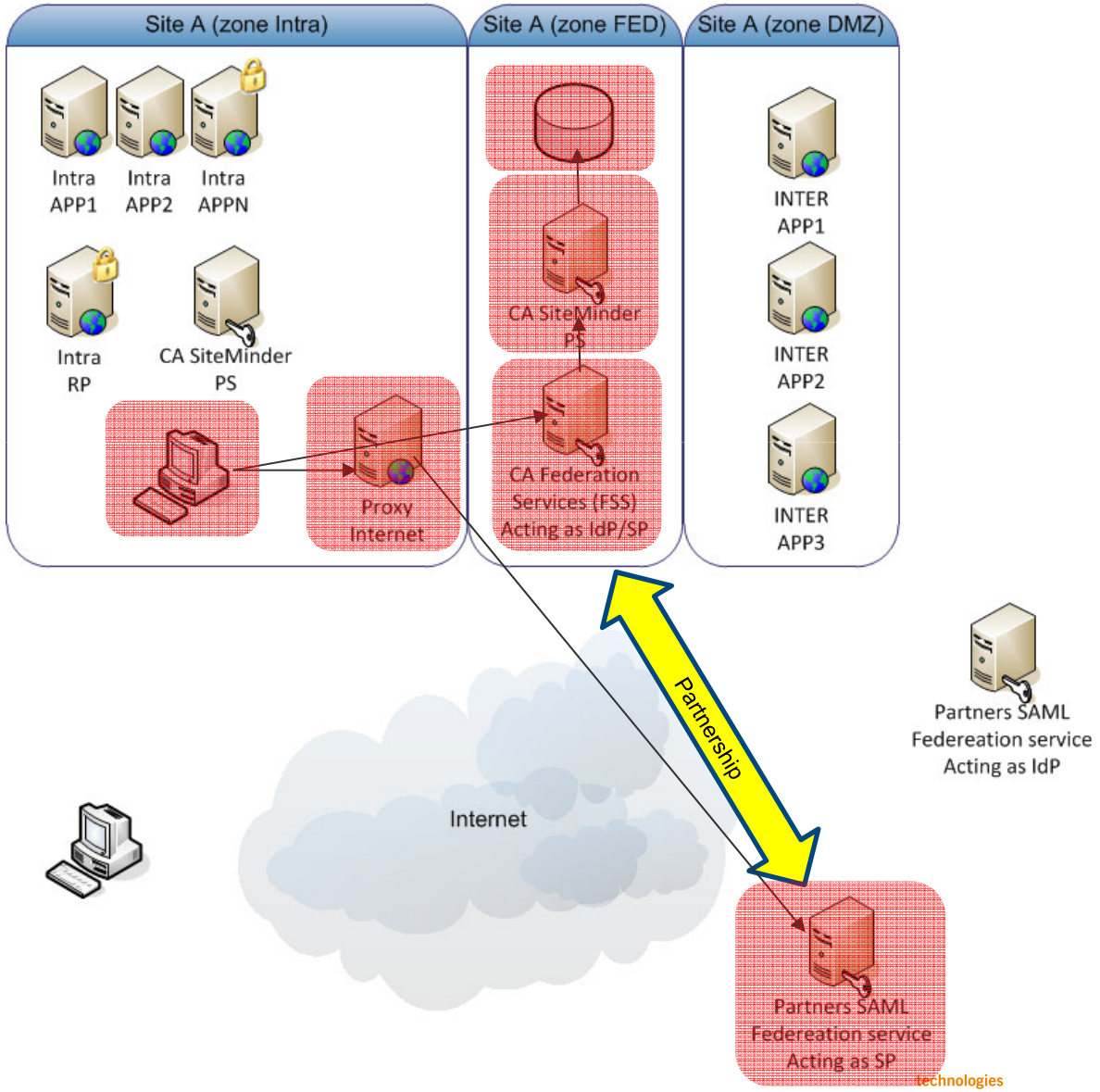
Solution de service IdP / SP

Un même site peut être à la fois IdP et SP. Ceci revient à mettre en place une solution de service de fédération d'identité complexe.
Celle-ci peut être adossée à la solution WAM SiteMinder existante ou peut être déployée sous forme de solution « EndPoint »



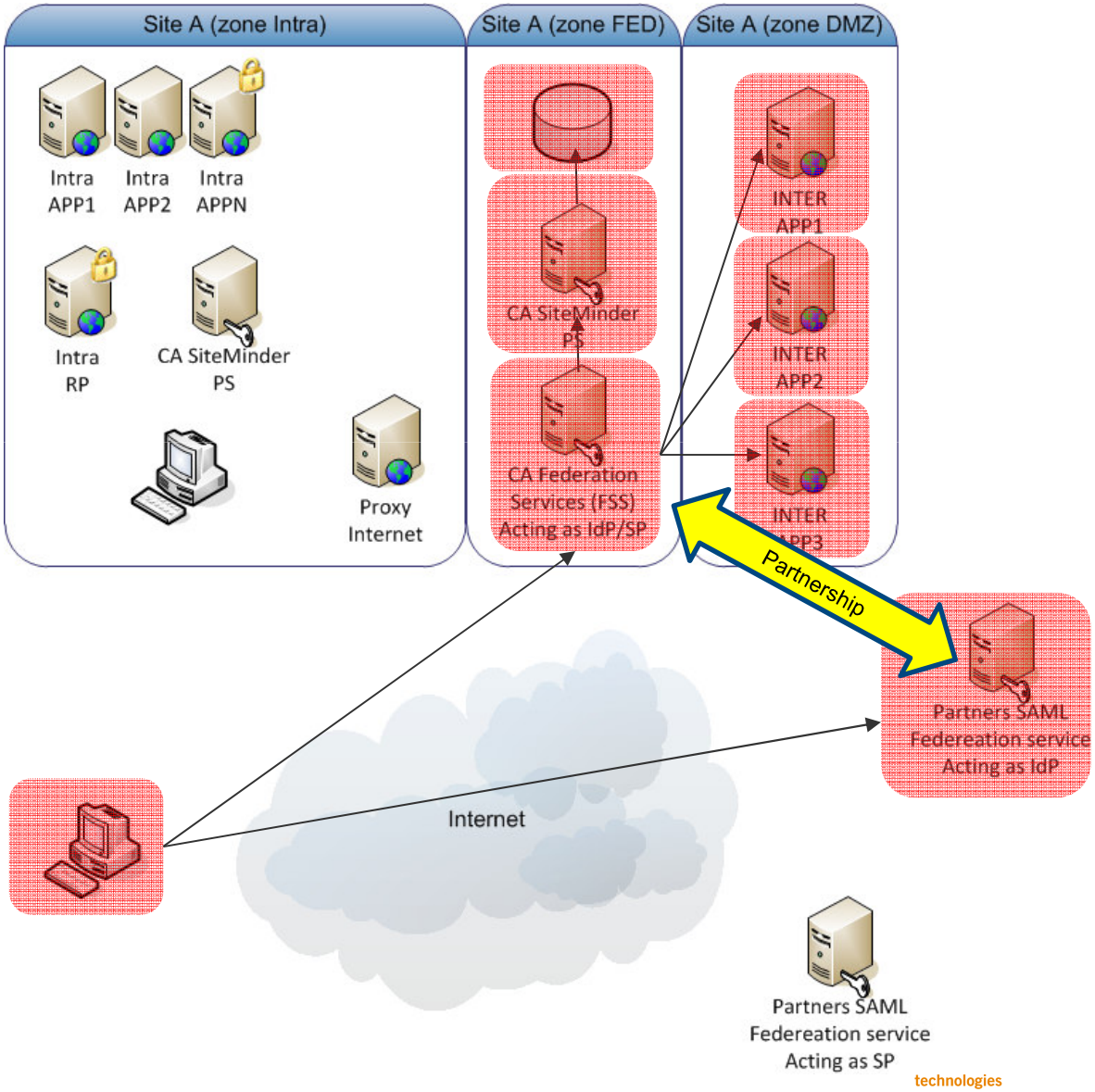
Solution de service IdP / SP

Cheminement d'un flux impliquant les composants IdP du site A



Solution de service IdP / SP

Cheminement d'un flux impliquant les composants SP du site A



Monitoring SiteMinder

“*Chronique d’un incident SiteMinder*”

Chronique d’un incident SiteMinder

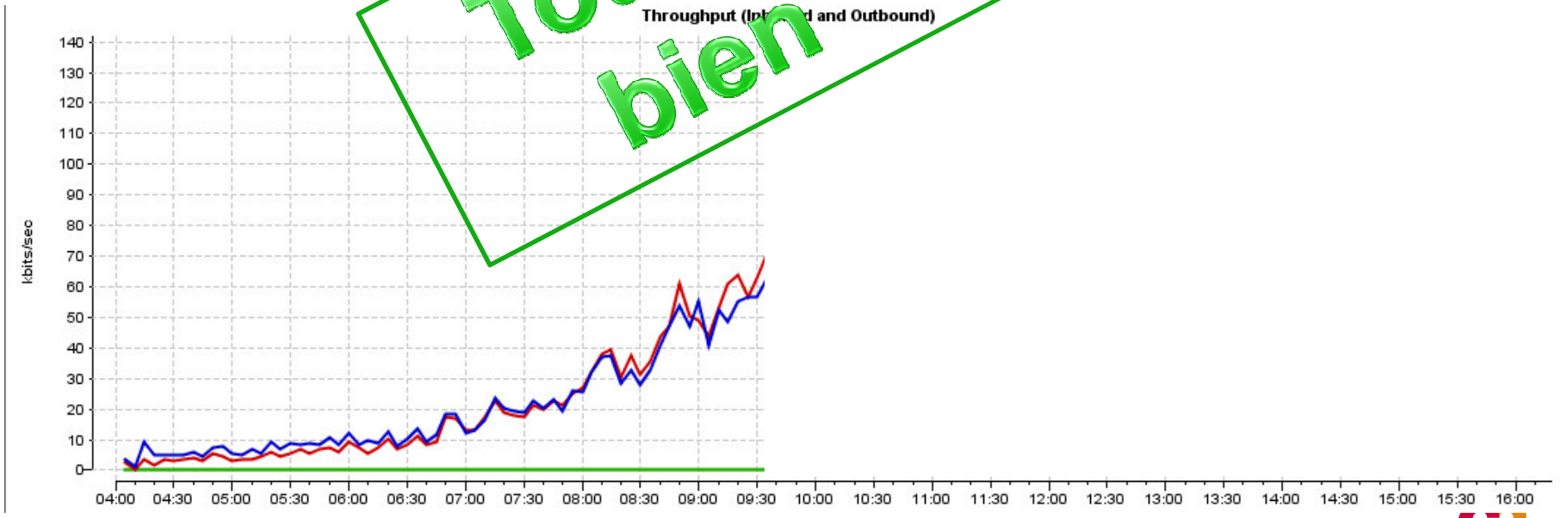
Contexte client

- 2 clusters SiteMinder de 2 nœuds chacun
- Chaque cluster protège des applications spécifiques et est backup de l’autre cluster
- User Store SGBD
- Pas ou peu de monitoring / métrologie

ca technologies

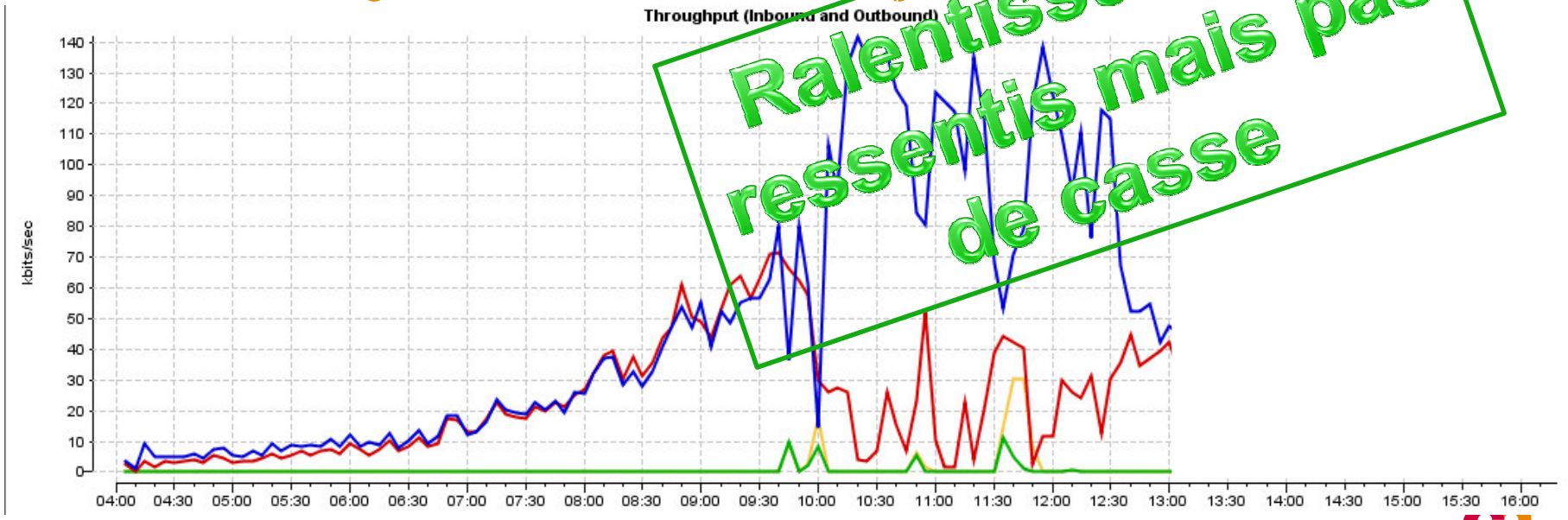
Chronique d'un incident SiteMinder

- Montée en charge de type gaussienne
- Courbe de charge réseau confondue pour chaque cluster (rouge/bleu et jaune/vert)
- Charge négligeable pour le cluster (jaune/vert)



Chronique d'un incident SiteMinder

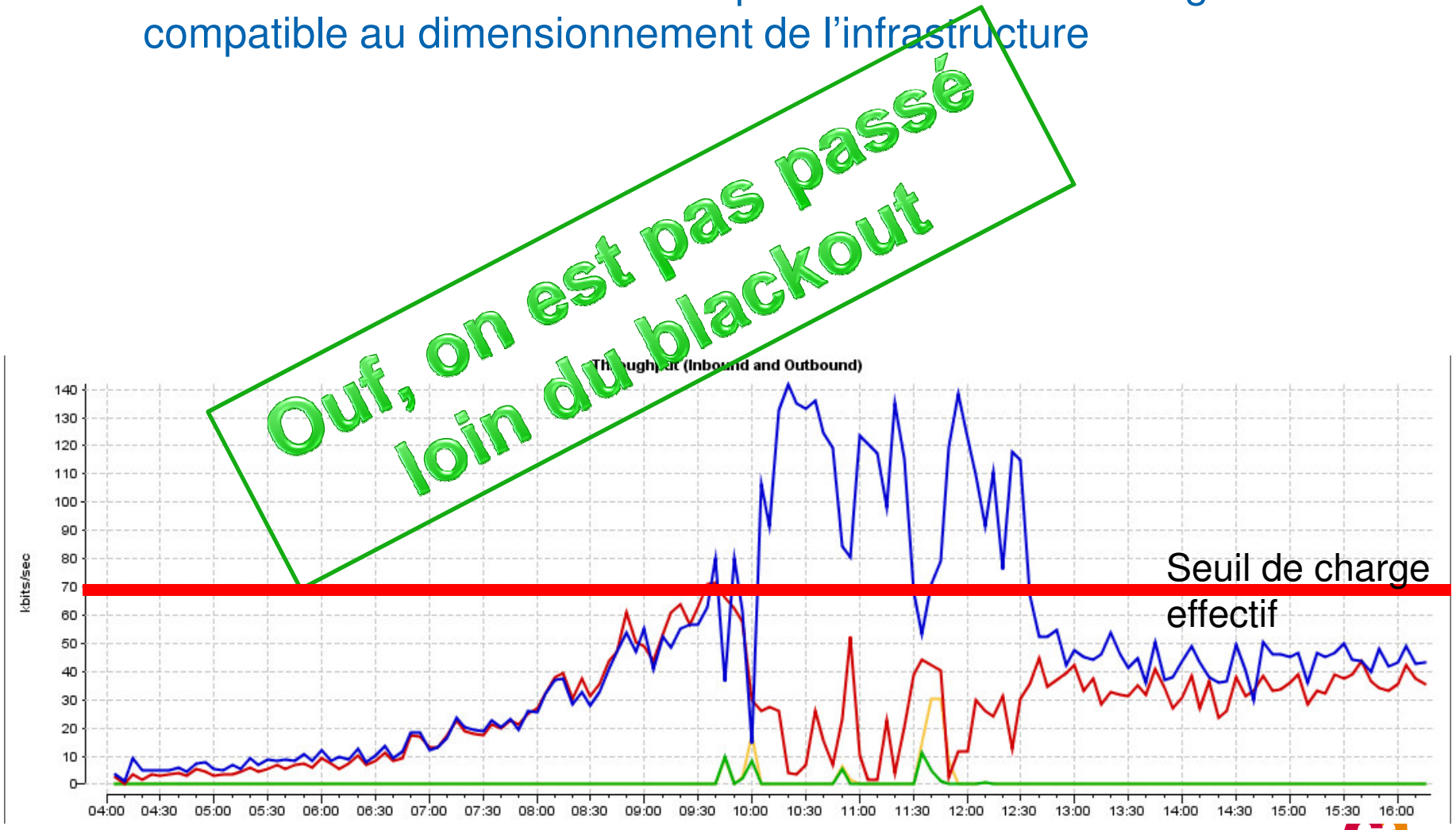
- Dégradation des temps de réponses du SGDB
- Chargement de la Queue Worker
- Timeout sur les requêtes WebAgent
  - Réémission des demandes -> accroissement du volume réseau
  - Augmentation du nombre de sockets entre WA -> PS
  - Déséquilibre de la répartition de charge du fait de l'engorgement des PS
  - Délestage vers le second cluster (jaune vert)



ca technologies

Chronique d'un incident SiteMinder

- Retour à la normal en début d'après midi avec une charge compatible au dimensionnement de l'infrastructure



Ce qu'il faut retenir

- L'incident est une conjonction de deux facteurs:
  - Forte augmentation de la charge suite au raccordement d'une grosse application
  - Dégradation transitoire des temps de réponse du User Store
    - Requêtes SQL peu optimisées

- Pas/Peu de métrologie permettant de d'identifier les occurrences de problèmes composant par composant afin de cibler les actions avant la contamination aux autres composants (syndrome du « pas nous pas nous »)

ca technologies

merci