Club Utilisateur CA Siteminder – Retour d'expérience Cora

Mise en œuvre de SPS chez Cora

Stratégie & Expertise numérique

Votre interlocuteur

Sylvain Guyot
Expert IAM et Sécurité – Exakis

sylvaing@exakis.com
+33 6 68 25 74 68

Des chiffres clés illustrant notre expertise

Une création en 2001

Un réseau de 7 agences en France et 2 en Suisse

Au service de plus de 500 clients en France et à l'international

300 consultants et experts dont 170 certifiés Microsoft

85% de fidélité clients depuis 2009

12 domaines de compétences Gold & Silver
Partenaire Microsoft de l'année !

Notre offre sécurité

IAM

- Provisioning et propagation des identités et des droits
- SSO/ Fédération
- Authentification forte
- Gestion des comptes à privilège
- Role mining

Objets connectés

- Mobile/MDM
- Machines non gérées
- Identification
- Authentification
- BYOD
- Sécurisation des SI Industriel
- Sécurisation des interconnexions des SI Entreprise/SI Industriel

Sécurisation des applications

- Publication/accès à distance
- Respect des engagements
- Chiffrement

Sécurisation des données

- Sécurisation des mails (chiffrement et signature)
- Chiffrement des fichiers
- Gestion du droit d'usage / DLP
- Sauvegarde et archivage
- Dématérialisation/ signature électronique
- Parefeu BDD

Gouvernance, audit et reporting

- Expression des besoins de sécurité
- Conformité (contrat, exploitation et processus)
- Audit
- Tests d'intrusion
- Analyse de risque

Agenda

- Rappels des besoins
- Présentation de l'Architecture
- Cas d'utilisation Extranet
- Cas d'utilisation Fédération Google App

Rappel des besoins

1er Besoin : Extranet

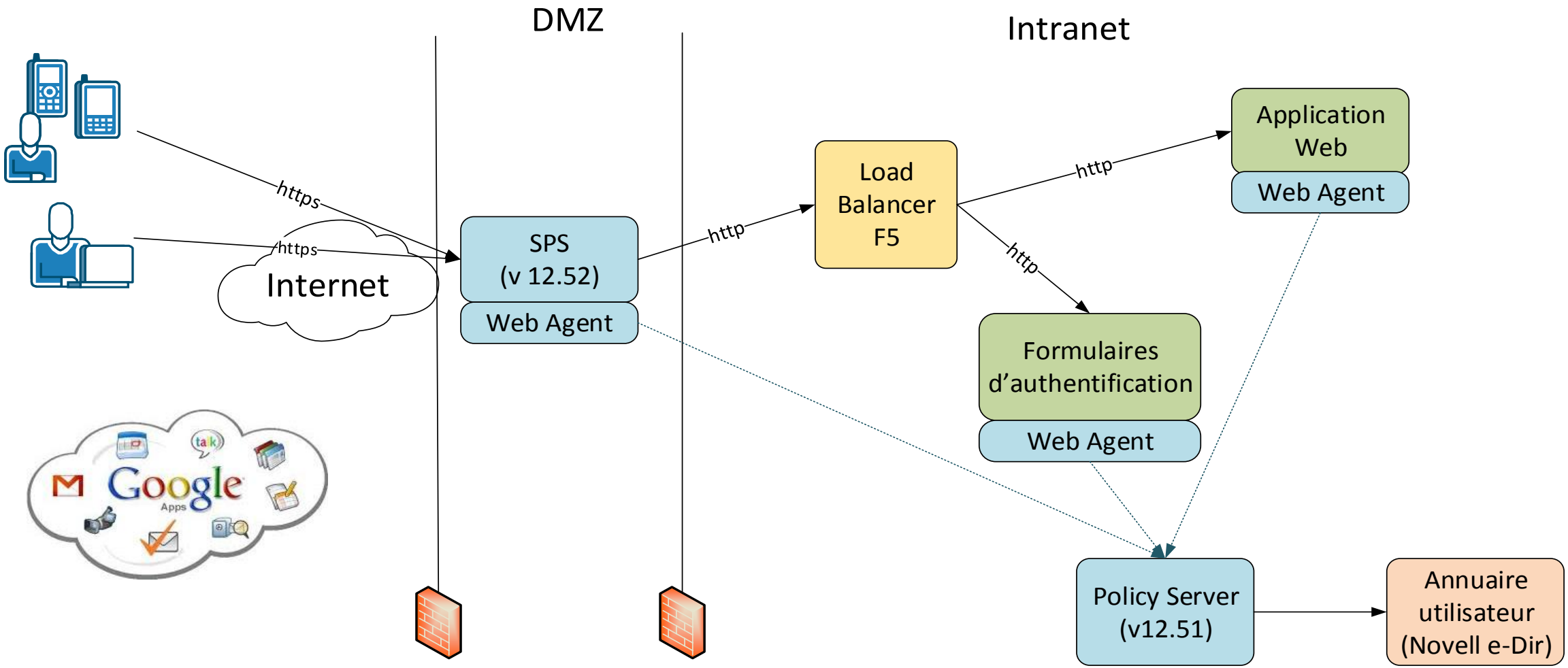
- Publication d'applications métier sur internet
  - Configuration du VPN compliqué à configurer sur des tablettes (split DNS, etc.)
- Utilisation de tablette Android

2ème Besoin : Fédération Google App

- Utilisation du login et du mot de passe interne lors d'un accès depuis internet
- SSO entre la session interne et l'accès à Google App (Drive – serveur de fichiers, Messagerie, etc.)

- Rappel des besoins
- Présentation de l'achitecture
- Cas d'utilisation Extranet
- Cas d'utilisation Fédération Google App

Architecture Siteminder SPS



Prérequis techniques

Existant :

- Avoir une infrastructure siteminder existante (12.5 minimum)

Flux à ouvrir

- Flux : SPS-> policy server
  - TCP/44441
  - TCP/44442
  - TCP/44443
- Flux : SPS -> F5
  - TCP/80 et TCP/443

Adresse IP publique pour avec le SPS sur internet + déclaration DNS

- sps.cora.fr

Certificats :

- Certificat serveur sps.cora.fr pour avoir le SSL
- Certificat pour la signature des assertions SAML générées par SPS (le même certificat a été utilisé dans notre cas)

- Rappel des besoins
- Présentation de l'architecture
- Cas d'utilisation Extranet
- Cas d'utilisation Fédération Google App

Configuration

Proxification souhaitée :

https://sps.cora.fr/<application> -> http://f5.coraint.cora/<application>

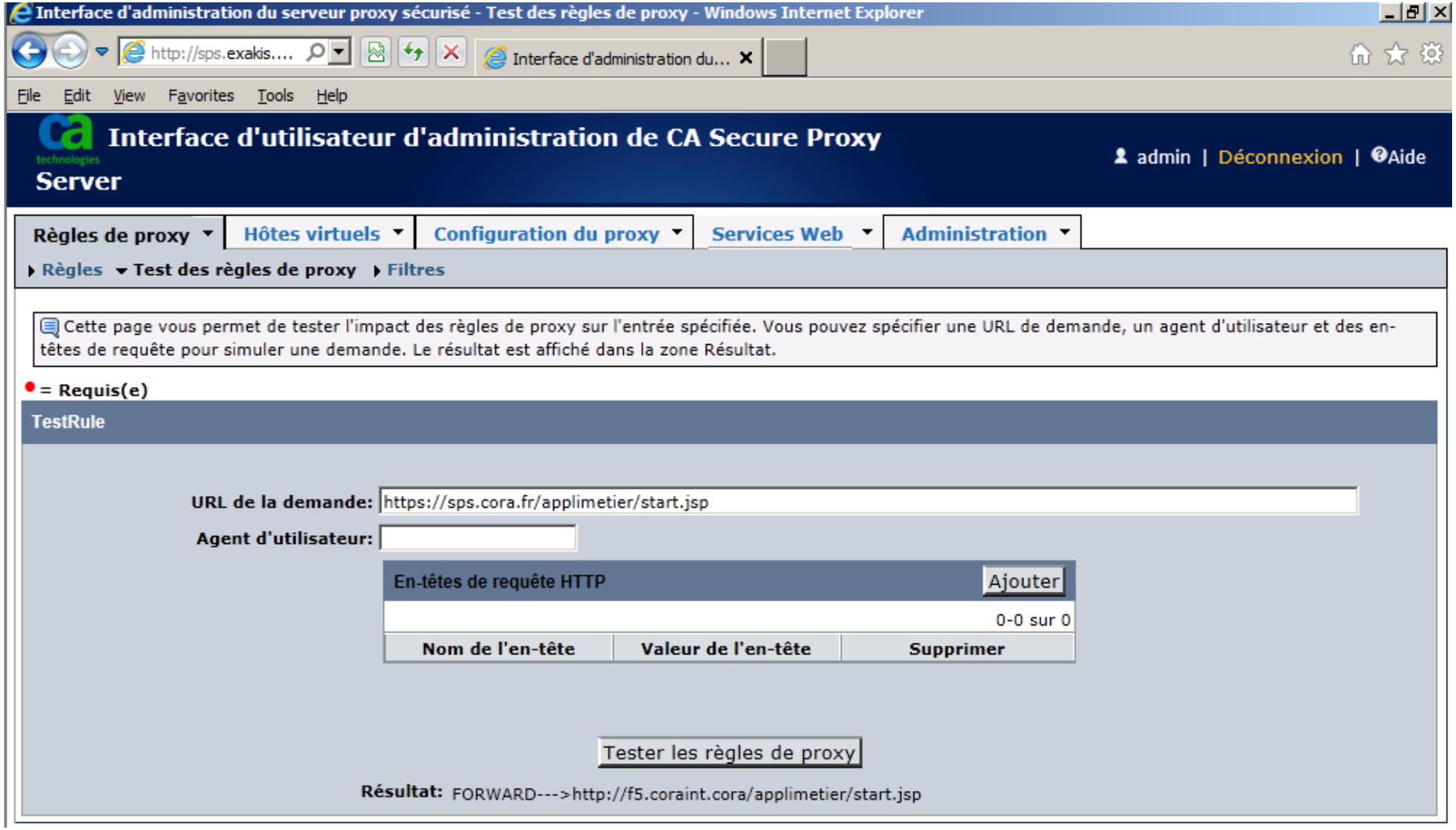
Le load balancer F5 fait lui-même office de reverse proxy et choisit le bon serveur en fonction de <application> de l'uri

Exemple : fichier **<sps_home>/proxy-engine/conf/proxyrules.xml**

```
<nete:proxyrules xmlns:nete="http://www.company.com/">
   <nete:cond type="host">
      <!-- replace banking.company.com with a virtual host defined in the server.conf file -->
      <nete:case value="sps.cora.fr">
         <!-- replace http://server1.company.com with the appropriate destination server -->
         <nete:forward>http://f5.coraint.cora$0</nete:forward>
      </nete:case>
      <nete:case value="sps.cora.fr:443">
         <!-- replace http://server1.company.com with the appropriate destination server -->
         <nete:forward>http://f5.coraint.cora$0</nete:forward>
      </nete:case>
      <nete:default>
         <!-- replace http://home.company.com with a default destination used for all requests that do not match the nete:case elements -->
         <nete:forward>http://f5.coraint.cora$0</nete:forward>
      </nete:default>
   </nete:cond>
</nete:proxyrules>
```

Test des règles de proxy

L'interface d'administration permet de tester les règles :



Autres Types de règles

Règles en fonction :

- du hostname de l'url
- d'un chemin dans l'uri
- d'un header http
  - useragent pour identifier un portable, une tablette,
  - cookie
  - Etc.

Construction de l'url cible :

$0 : ajoute l'uri entière à l'url cible

$1 : ajoute la partie de l'uri après de chemin filtré

Exemples : **<sps_home>/proxy-engine/examples/proxyrules**

Configuration Siteminder

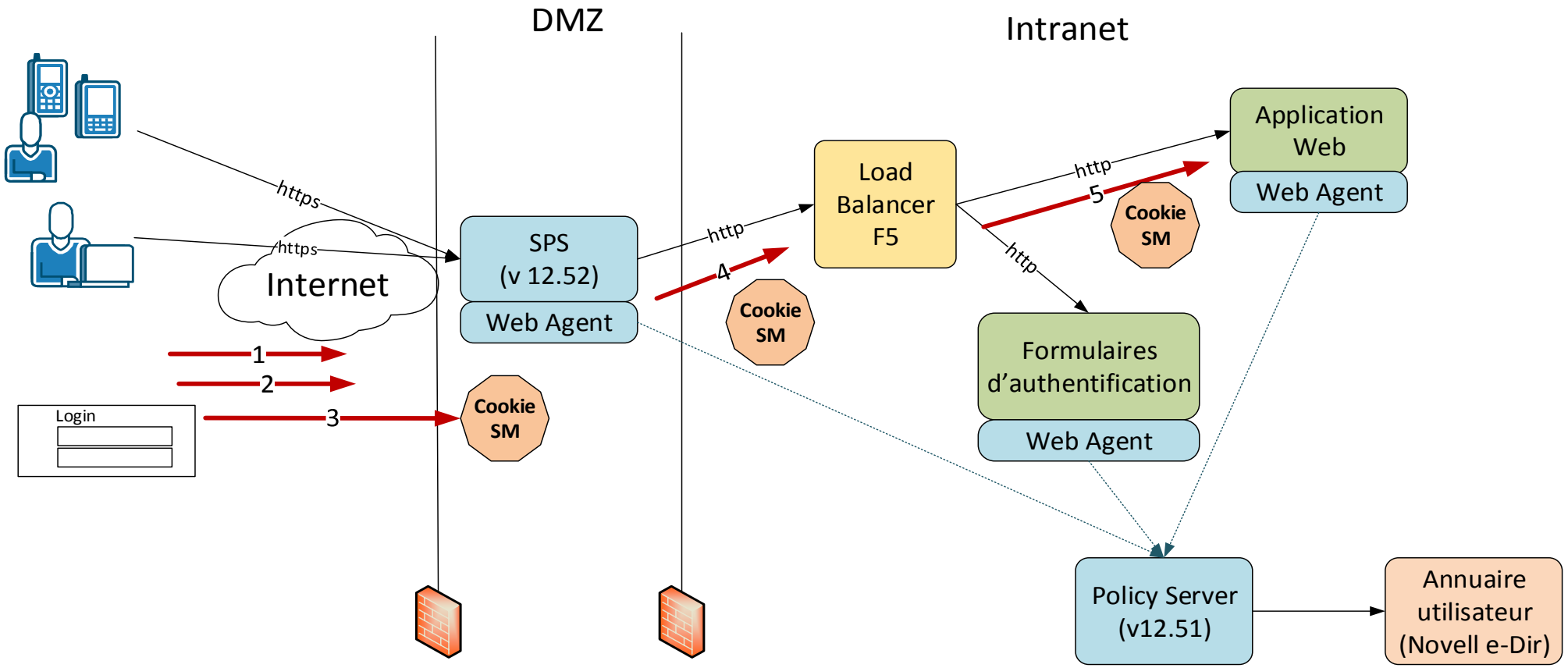
Nécessité de reprotéger l'application depuis l'url rentrée (agent = agent SPS)

Permet :

- un schéma d'authentification différent (authentification forte)
- règle de sécurisation différentes (plus restrictive éventuellement)

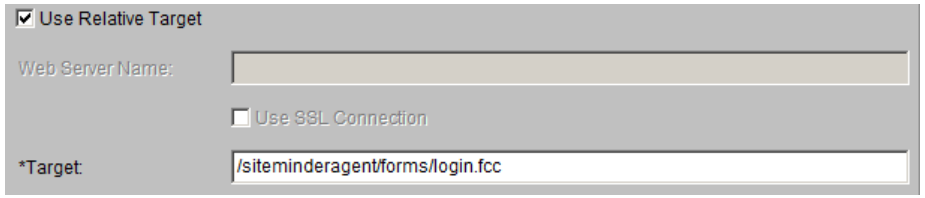
Cinématique

Le cookie SM_SESSION généré dans le domaine « cora.fr » est recopié par le proxy SPS sur la requête sur le serveur cible:



Difficultés rencontrées

- Configuration SSL
  - Difficulté pour démarrer le service apache (Windows) si la clé privée est protégée par une passphrase non vide
- Url pour le formulaire fcc d'authentification sur le SPS
  - Schéma d'authentification formulaire html:



  - Le fichier login.fcc doit être à l'emplacement suivant sur le serveur SPS :

<sps_home>/proxy-engine/examples/siteminderagent/forms/login.fcc

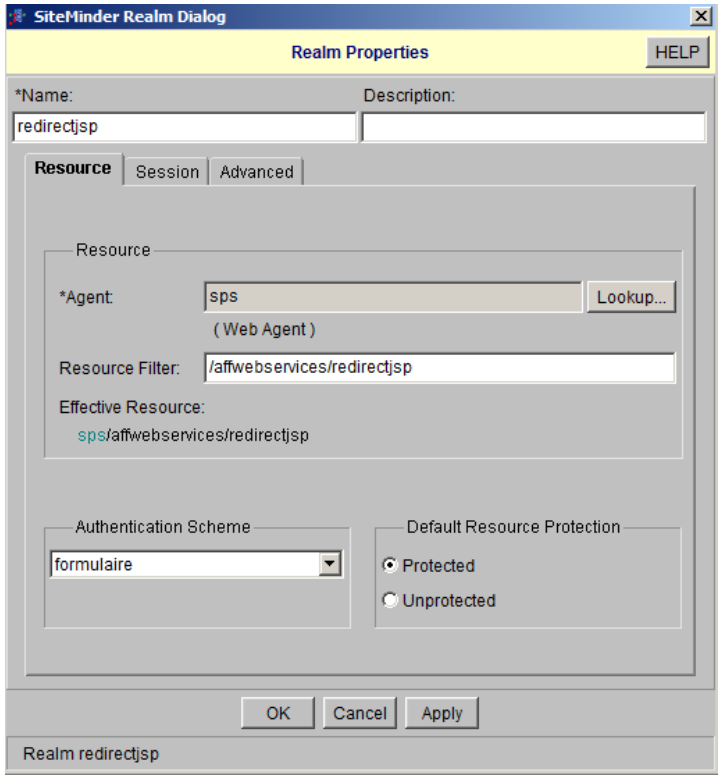
- Contraintes inhérentes à un Reverse Proxy
  - Attention !!, toutes les ressources de l'appli doivent être définie en relatif (images, css, js introuvables, ...)

- Rappel des besoins
- Présentation de l'architecture
- Cas d'utilisation Extranet
- Cas d'utilisation Fédération Google App

Prérequis

- Configurer SSL sur le serveur SPS (prérequis fédération SAML)
- Protéger la page d'authentification SPS dans Siteminder

https://sps.cora.fr/affwebservices/redirectjsp/redirect.jsp



Configuration

Utilisation de la WAM UI (cf. guide Runbook CASM-Google-FederationRunbook-ver1.0.pdf)

1. Création d'une entité IDP SAML2 locale (remplacer « exakis.com » par « cora.fr »)

Entity Type

Entity Location:	Local
Entity Type:	SAML2 IDP

Entity Details

Entity ID:	https://sps.exakis.com
Entity Name:	idp-exakis
Description:	
Base URL:	https://sps.exakis.com
Default SLO Confirm URL:	
SOAP Artifact Resolution URL:	https://sps.exakis.com/affwebservices/public/saml2ars
SSO Service URL:	https://sps.exakis.com/affwebservices/public/saml2sso
SLO Service URL:	https://sps.exakis.com/affwebservices/public/saml2slo
SLO SOAP Service URL:	https://sps.exakis.com/affwebservices/public/saml2slosoap
User Consent Service URL:	https://sps.exakis.com/affwebservices/public/saml2userconsent
Attribute Service URL:	https://sps.exakis.com/affwebservices/public/saml2attrsvc
SOAP Manage NameID Service URL:	https://sps.exakis.com/affwebservices/public/saml2nidsoap

Default Signature and Encryption Options

Signing Private Key Alias:	le-f920000f-2728-4876-bcb5-461f97d7d97d
Signed Authentication Requests Required:	No

Supported Name ID Formats and Attributes

Supported Name ID Formats	Supported Assertion Attributes	
Selected Formats	**Assertion Attribute**	**Supported Format**
Email Address		

Configuration

2. Création d'une entité SP SAML2 distante:

Entity Type

Entity Location: Remote
Entity Type: SAML2 SP

Entity Details

Entity ID: google.com
Entity Name: Google
Description:

Remote Assertion Consumer Service URLs

Index	Binding	URL	Default
0	HTTP-POST	https://www.google.com/a/exakis.com/acs	No

Remote SLO Service URLs

Binding	Location URL	Response Location URL

Manage Name ID Service URLs

Binding	Location URL	Response Location URL

Signature and Encryption Options

Verification Certificate Alias: le-f920000f-2728-4876-bcb5-461f97d7d97d
Encryption Certificate Alias:
Sign Authentication Requests: No

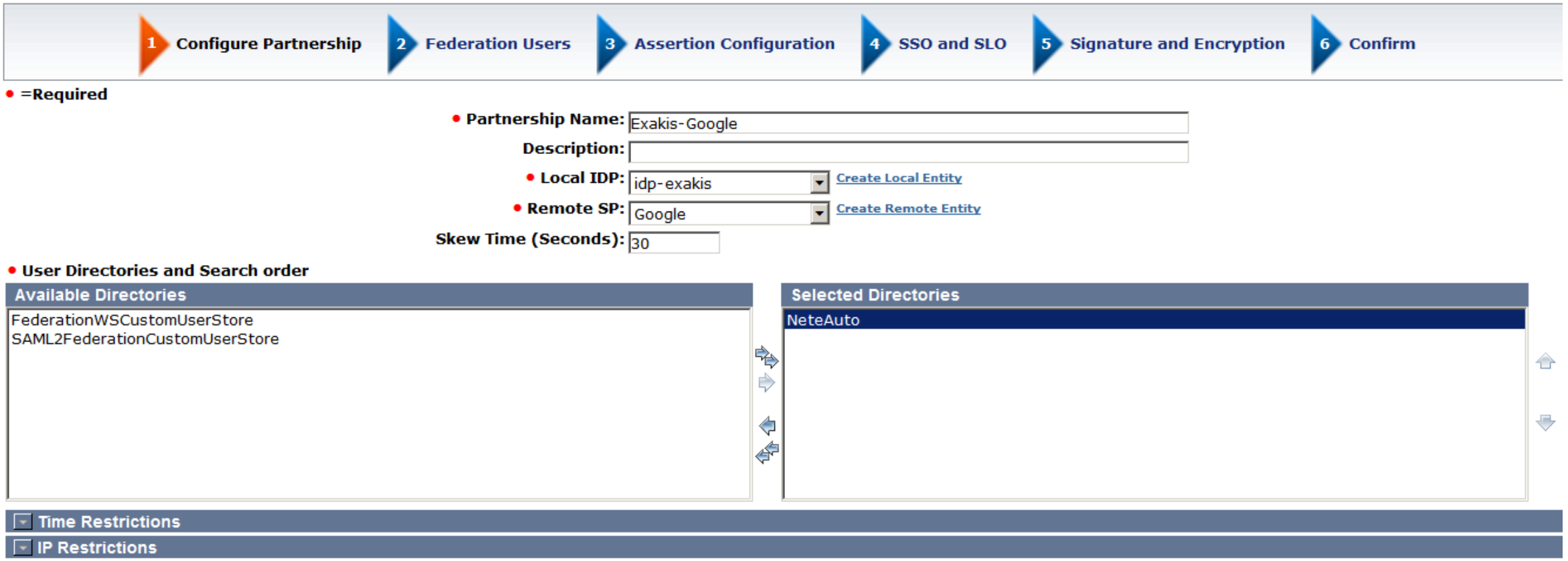
Name ID Formats

Supported Name ID Formats

Selected Formats
Email Address

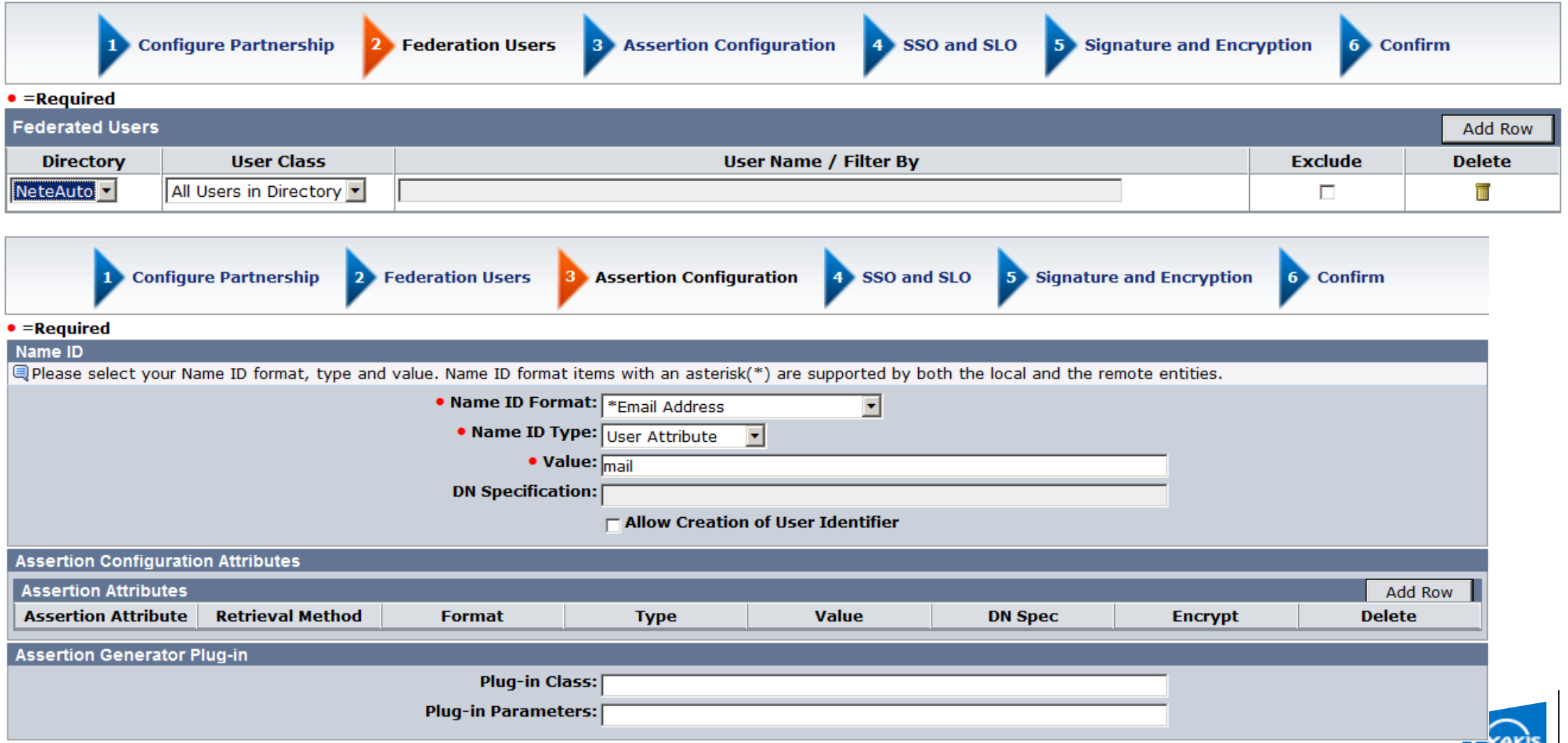
Configuration

3. Création d'un « Partnership » SAML 2 IDP -> SP :



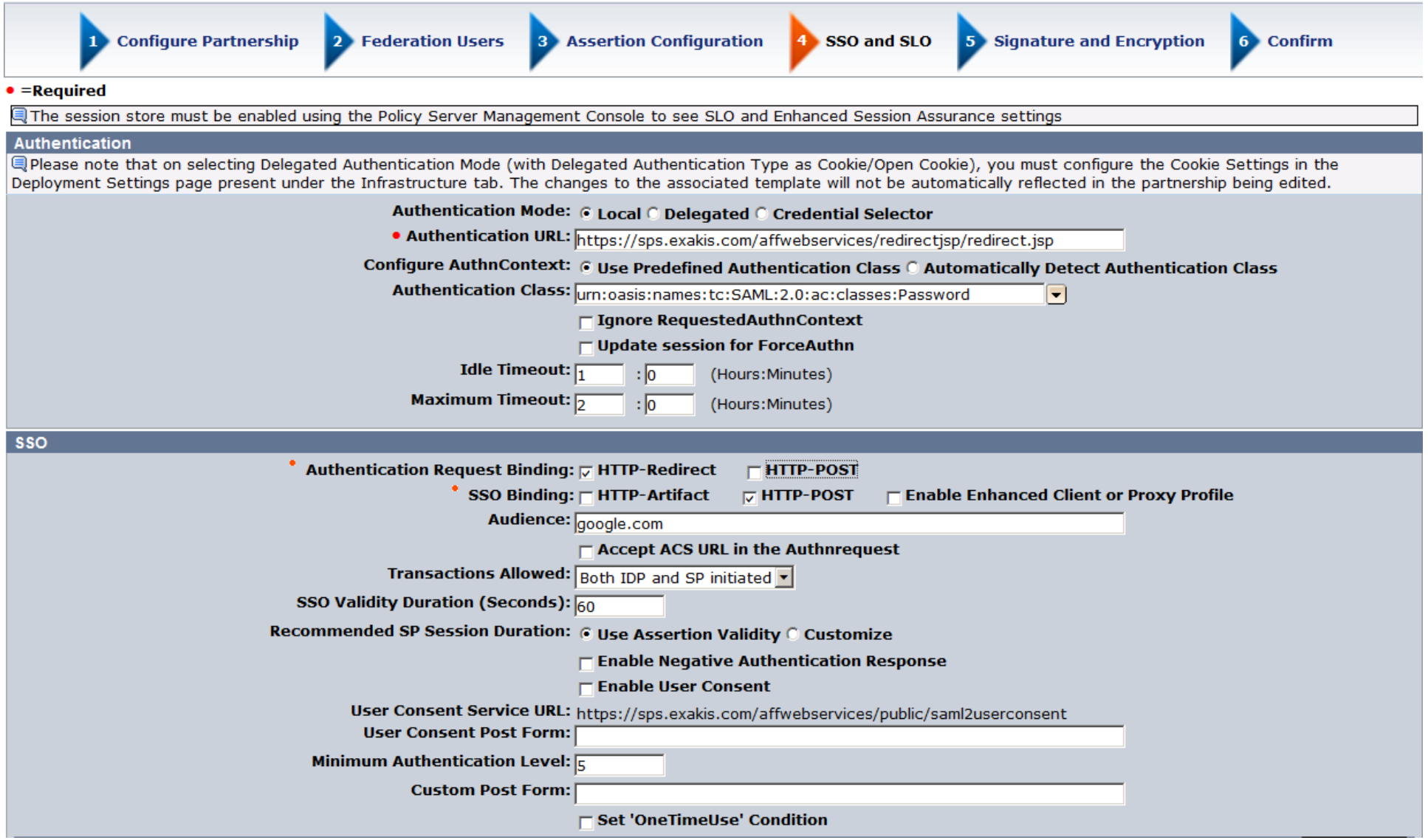
Configuration

Création d'un « Partnership » IDP SAML 2 -> SP (suite) :



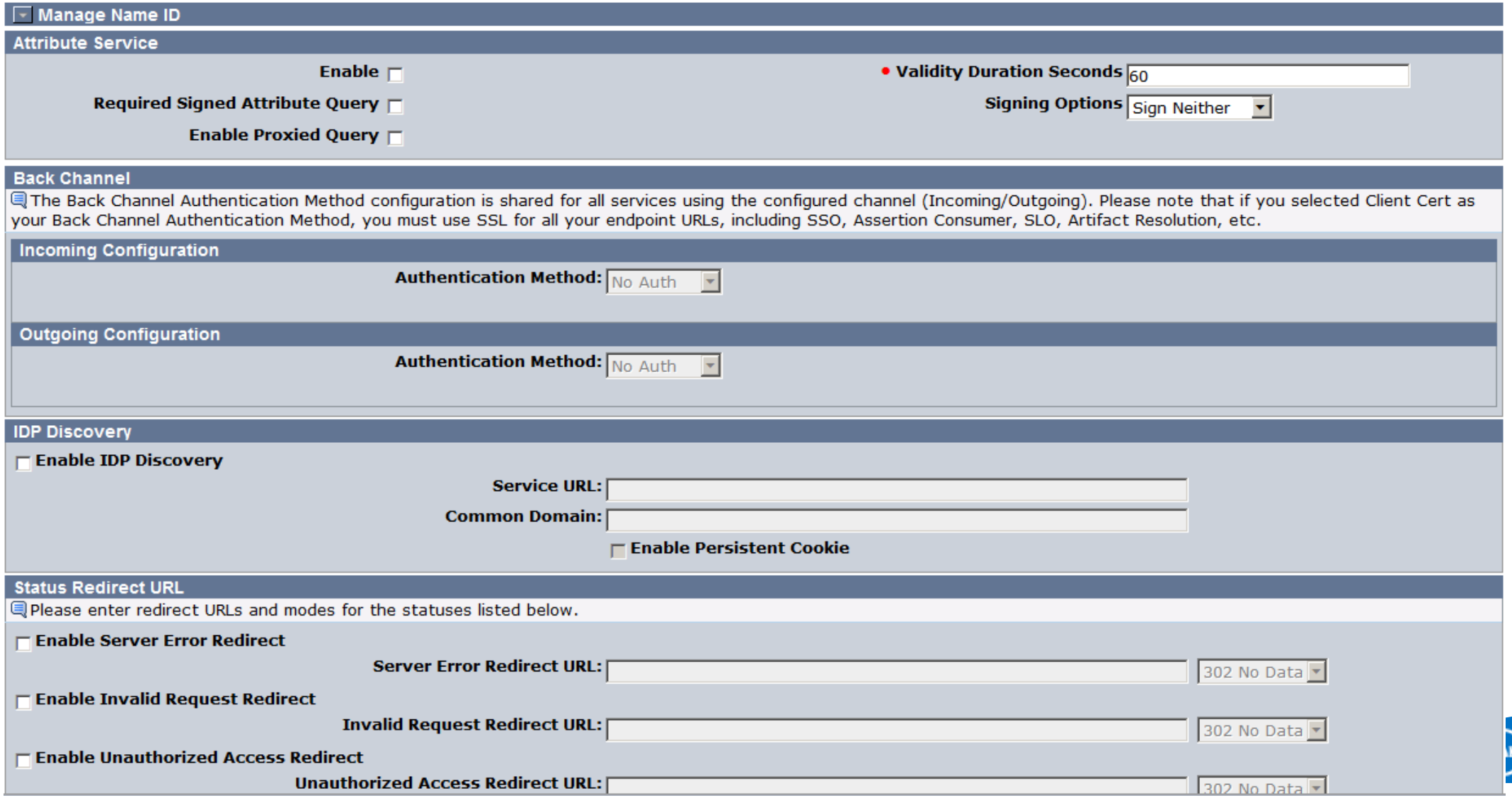
Configuration

Création d'un « Partnership » IDP SAML 2 -> SP (suite) :



Configuration

Création d'un « Partnership » IDP SAML 2 -> SP (suite) :



Configuration

Création d'un « Partnership » IDP SAML 2 -> SP (suite) :

1 Configure Partnership | 2 Federation Users | 3 Assertion Configuration | 4 SSO and SLO | 5 Signature and Encryption | 6 Confirm

Signature

- [ ] **Disable Signature Processing**

Signing Private Key Alias: le-f920000f-2728-4876-bcb5-461f97d7d97d — Import Generate

Signing Algorithm: RSAwithSHA1

Verification Certificate Alias: le-f920000f-2728-4876-bcb5-461f97d7d97d — Import Generate

Artifact Signature Options: Sign Neither

Post Signature Options: Sign Assertion

- [ ] **Require Signed Authentication Requests**
- [ ] **Require Signed ArtifactResolve**
- [ ] **Sign ArtifactResponse**

Encryption

Encryption Options: [ ] **Encrypt Name ID** [ ] **Encrypt Assertion**

Encryption Certificate Alias: Select one... — Import Generate

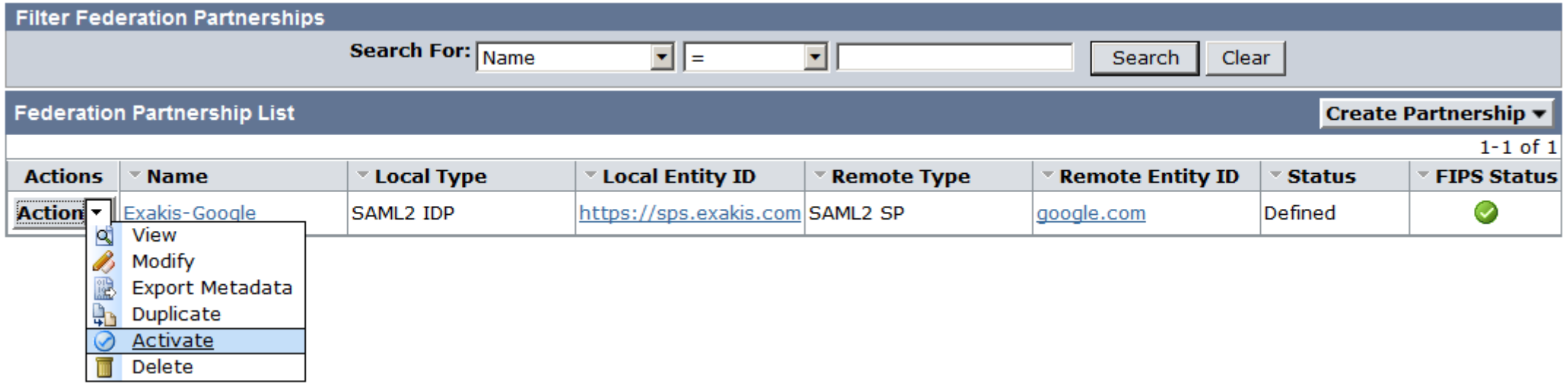
Block Algorithm: 3DES

Key Algorithm: RSA-V15

Decryption Private Key Alias: Select one... — Import Generate

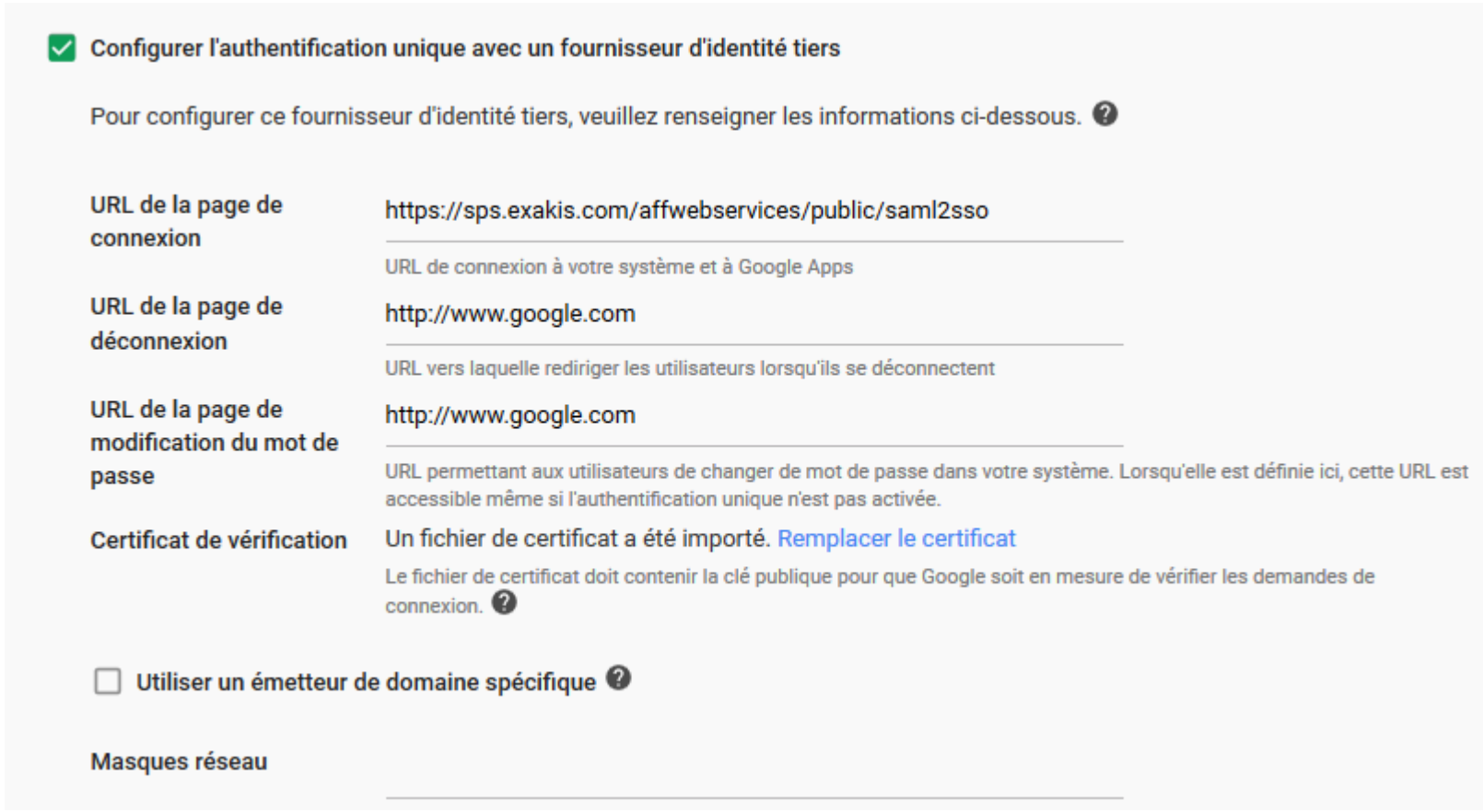
Configuration

4. Activer le « Partnership » :



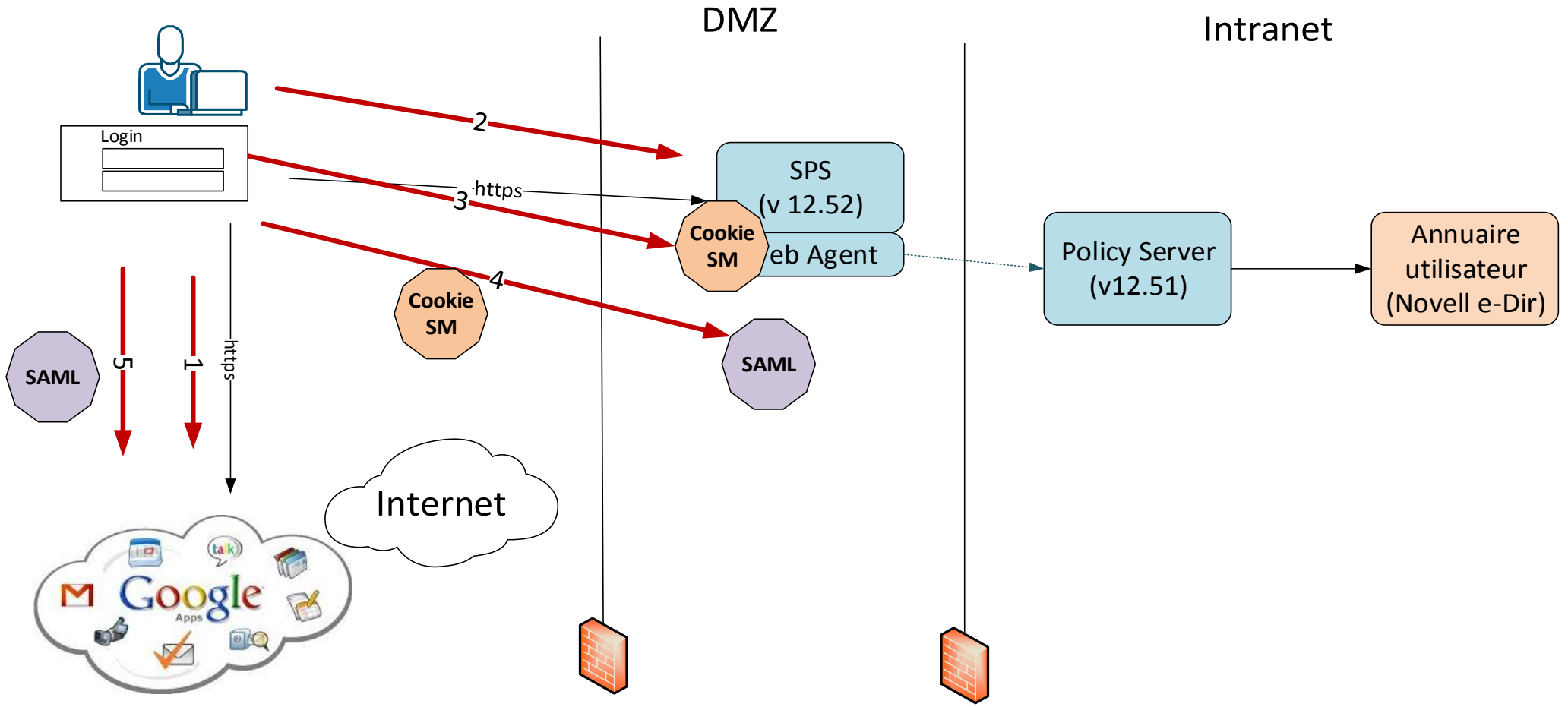
Configuration

Configuration du côté du SP



Cinématique

Cas SP-initiated : l'utilisateur appelle l'url : https://drive.google.com/a/cora.fr



Difficultés rencontrées

- Configuration du « partenariat » entre Cora et Google App
  - Erreur de time out (Tunnel Agent Failure) sur la WAM UI lors de la création du “Partnership” au moment de choisir l’annuaire utilisateur (lenteurs liées à un bouclage spécifique annuaire eDir cora : inclusion de grp croisés)
  - Solution de contournement : création du “Partnership” en choisissant un autre Annuaire Utilisateur (AD), puis modification du “Partnership” pour changer l’annuaire utilisateur

- La fédération (sso) n'est uniquement active à partir d'url google spécifiques (ex : drive.gogle.com/a /cora.fr pour accès drive avec sso). L’authentification se fait toujours par le mot de passe google :
  - Lors de l’accès par l’url http://www.google.com
  - Lors de l’accès depuis un smartphone

=> Fédération SAML Google App sans doute non mise en place en production chez Cora.

- Rappel des besoins
- Présentation de l'architecture
- Cas d'utilisation Extranet
- Cas d'utilisation Fédération Google App
- Cas d'utilisation Cookie Provider

Besoin

Avoir du SSO avec sa session siteminder interne « coraint.cora » quand on accède à Google App

Configuration

1. Déployer un site web interne accessible par l'url http://cp.cora.fr
   - chargé de fournir des cookies siteminder dans le domaine internet « cora.fr »
2. Protéger ce site par un web agent
   - Configurer l'attribut « CookieProvider » du web agent par une url dans le domaine interne « coraint.cora » elle-même protégée par un web agent : ex. http://*portail.coraint.cora*/siteminderagent/SmMakeCookie.ccc

Cinématique

Etat initial : l'utilisateur possède un cookie dans le domaine interne « coraint.cora »