

SiteMinder - CloudMinder integration use-case

Frédéric LALA – CA Services

24 jan 2013

agility
made possible™



Introduction

- Contexte

- Client possédant une infrastructure SiteMinder
- Authentications par formulaires & X509

- Nouveau besoin

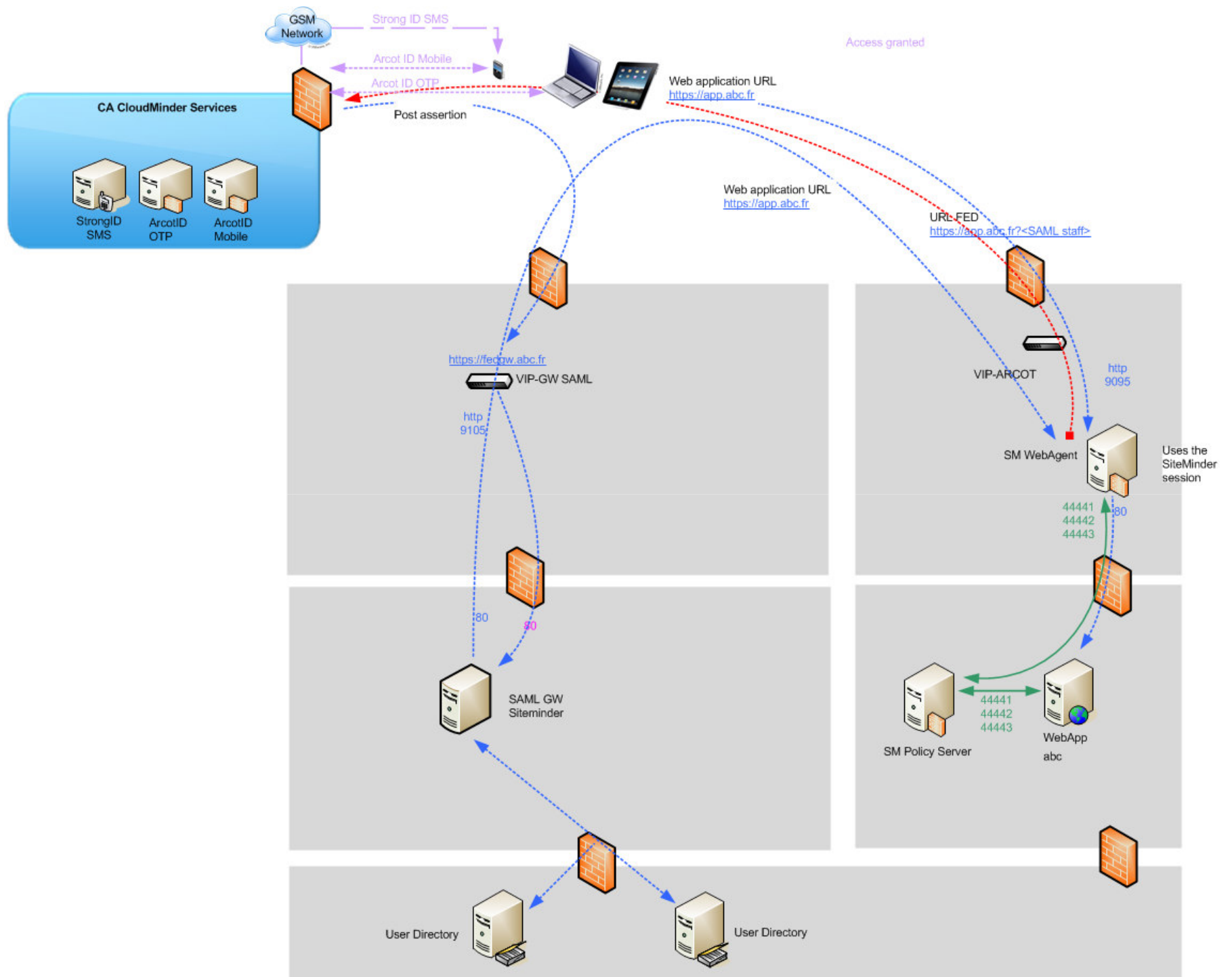
- Authentications renforcées, 2 facteurs, pour les accès depuis l'extérieur ou pour certaines applications
- OTP envoyé par SMS
- Soft token pour authentication forte logicielle

- Solution proposée

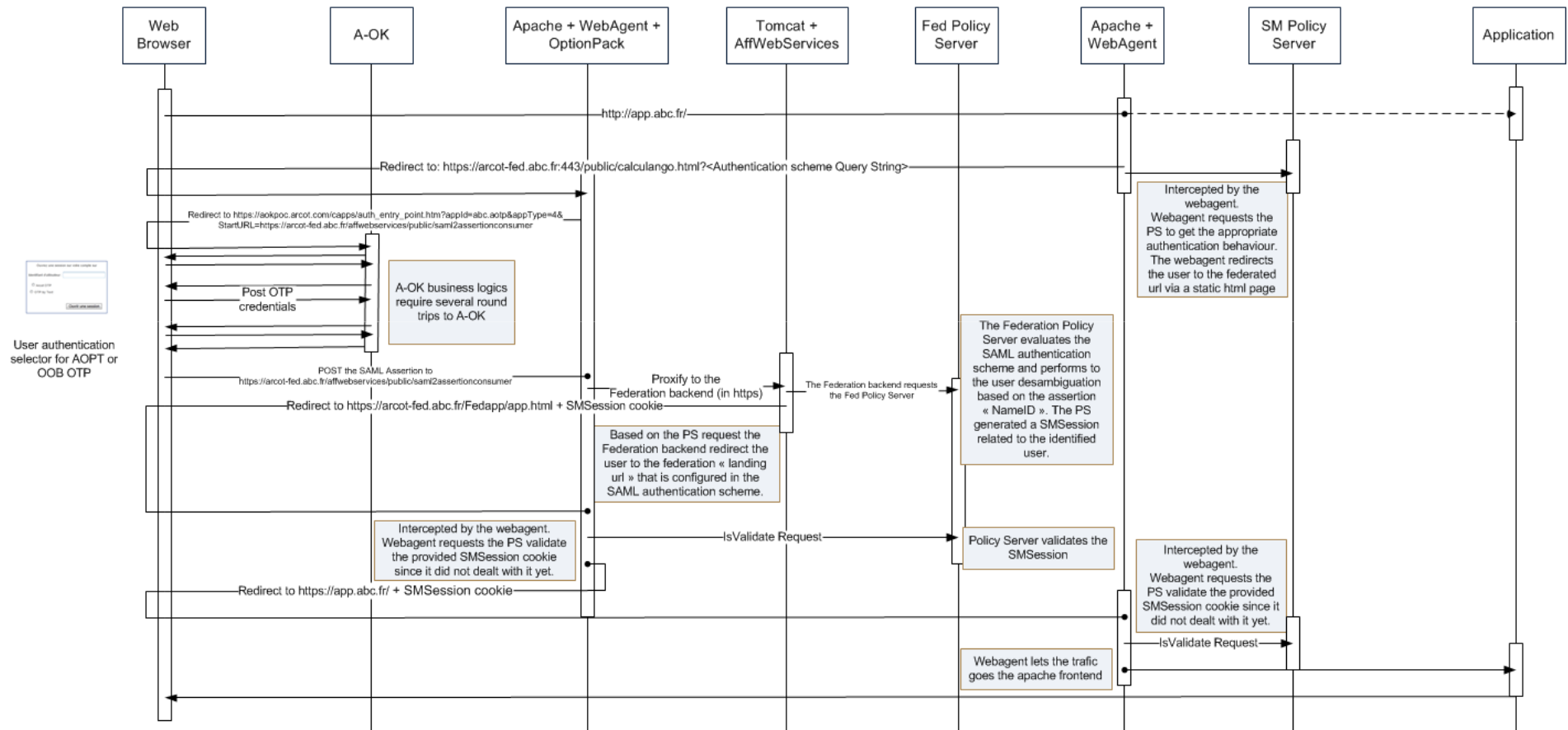
- Authentication forte logicielle et double authentication par OTP
- CA AuthMinder as a service : A-OK / CloudMinder
- Intégration SAML

Strong Authentication process

1. The user attempts to access the « Web application URL »
2. SM WebAgent detect that A-OK is protecting the requested URL and will redirect the user to the SAML GW through the «Web application Federated URL »
3. SAML GW redirect the user to the A-OK authentication URL
4. A-OK validate the credentials and generate a SAML assertion then redirect the user to the SAML GW through the « Web application Federated URL »
5. SAML GW consume the SAML assertion and generate a SiteMinder session cookie (cookie FED) and redirects the user to « Web application URL »
6. SM WebAgent detects & accepts the session cookie generated by the Fed GW and forward to the Web Server
7. The user Access the « Web application URL »



Sequence Diagram



SiteMinder - SiteMinder R12.5 migration path

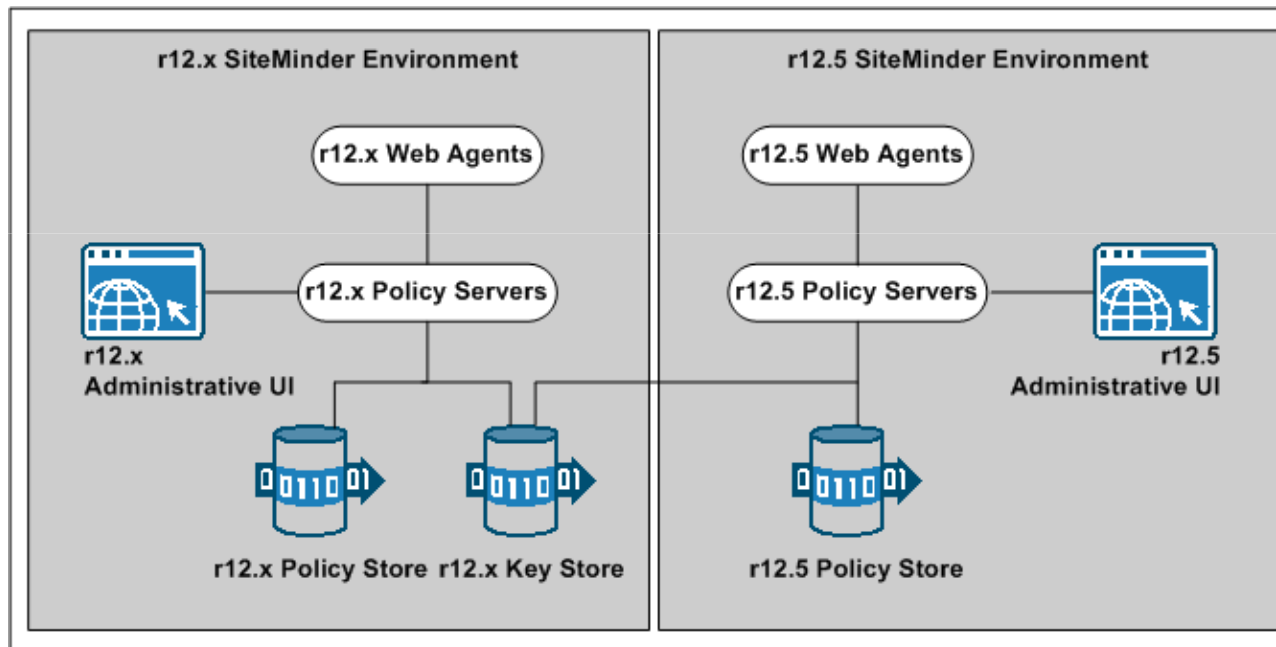
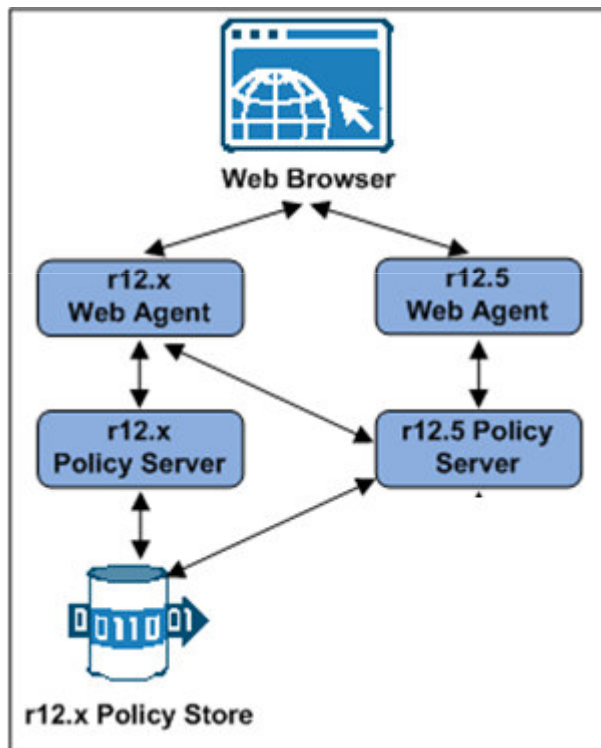
Frédéric LALA – CA Services

24 jan 2013

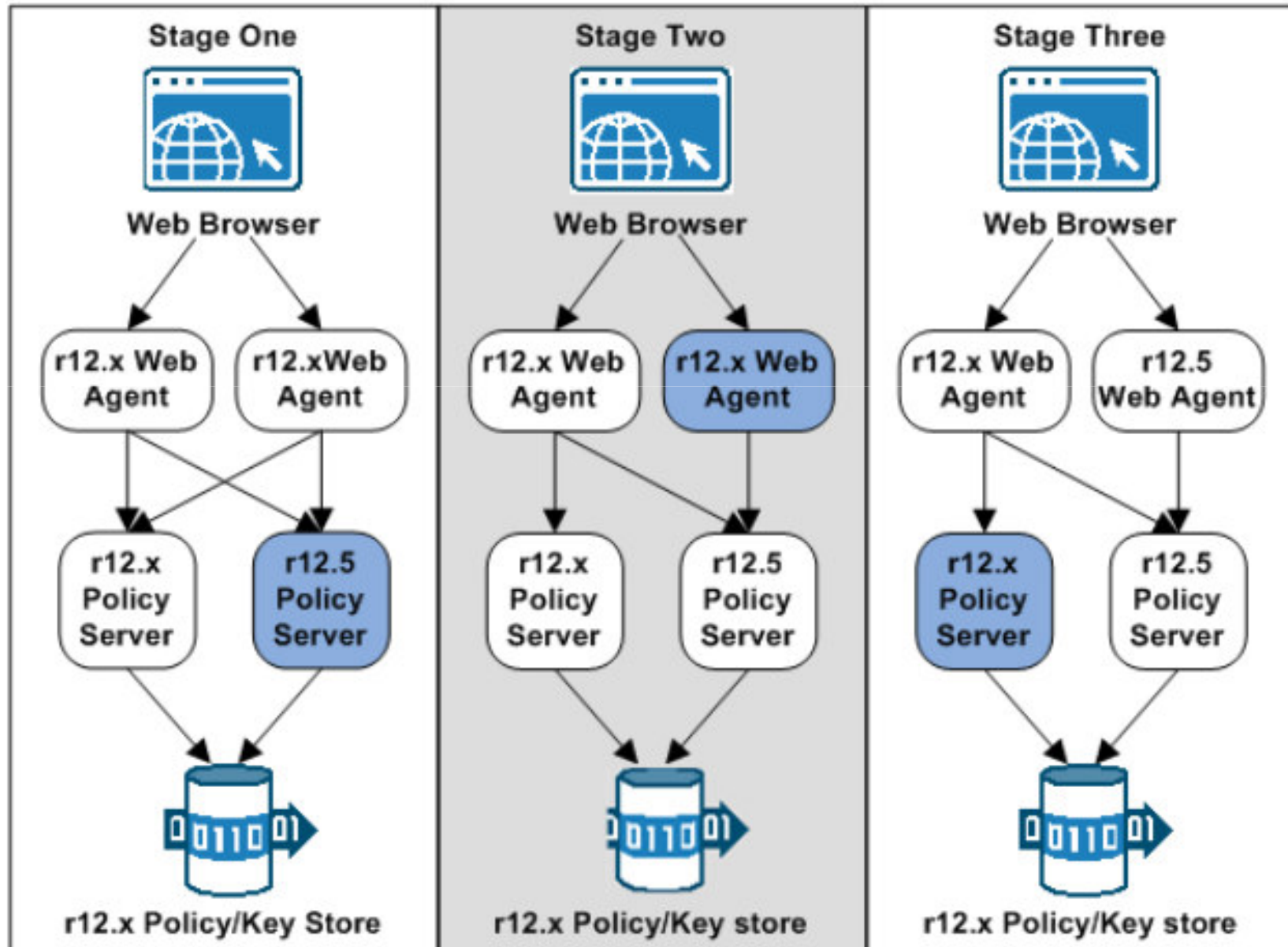
agility
made possible™



Migration path Mixed mode vs Parallel mode



Standard migration path



Standard migration path

