CA Siteminder
Roadmap & Strategy

Yannick Fhima
Security-Europe

Agenda

- SiteMinder Core
  - SiteMinder R12 SP3
  - SAP Agent R12
  - Content Aware Access
  - Generic Agent Framework
- SharePoint 2010
- IIS 7
- Web 2.0 / Identity 2.0

SiteMinder R12 SP3

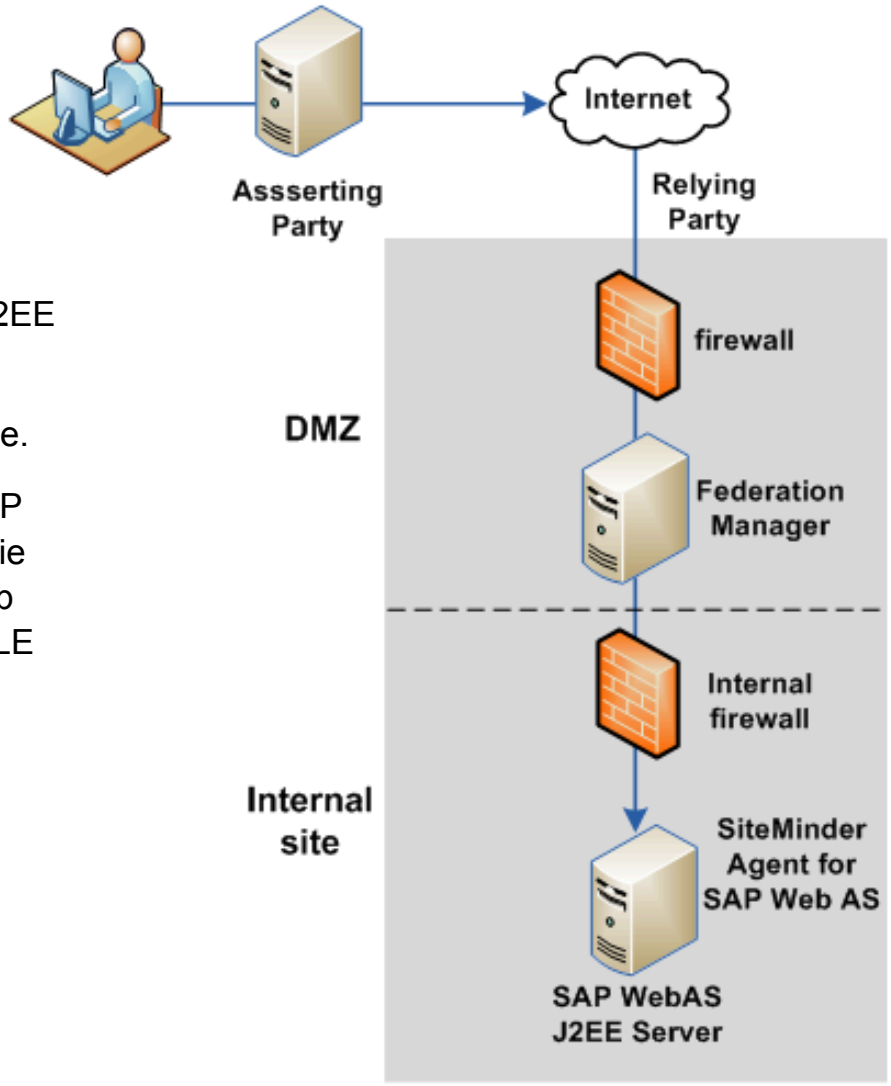
- ODBC-based policy stores can now be configured via the Policy Server configuration wizard
- X.509 Certificate authentication enhancements
  - Support for more secure SHA-2 family of digital signatures
  - Support for signed OCSP request/responses
  - Validation of OCSP responder signatures and CRL's signed with SHA-2 hashes
  - Support for processing certificate authority chains with OCSP
  - Configurable failover between OCSP and CRL's and vice versa
- Performance enhancements
  - Accelerated Agent to Policy Server initialization process via improved trusted host processing
  - Enable Web Agents to see new Policy Servers without requiring a restart via dynamic host configuration object enhancement
- Updated 3rd party components

Integration with target web applications at SP
Integration with SAP : federation mode

1. The federated user authenticates at the asserting party, which generates a SAML assertion and passes the assertion to Service Provider
2. Federation Manager collects credentials from **SAML Assertion** and generates a FEDPROFILE **cookie**
3. Federation Manager forwards the request to the SAP J2EE Server
4. The SAP Web Application server invokes the login module.
5. The SiteMinder login module (in the login stack of the SAP Web AS) extracts the contents of the FEDPROFILE cookie and authenticates the session of the user to the SAP Web AS based on the User Identity present in the FEDPROFILE cookie.
6. The SAP Web AS authorizes the user, and then allows access to the requested resource.

The user now has access to all protected SAP resources !

- No SiteMinder Policy Server
- No SiteMinder Web Agent
- SiteMinder Agent for SAP Web AS operating in Federation mode.



ca technologies

Integration with SAP : external users
Process steps

1. The federated user authenticates at the asserting party, which generates a SAML assertion and passes the assertion to Service Provider
2. Federation Manager collects credentials from **SAML Assertion** and generates a FEDPROFILE **cookie**
3. Federation Manager forwards the request to the SAP J2EE Server
   - The SAP J2EE server invokes the SAP Agent which checks if the HTTP request has a FEDPROFILE cookie
   - IF yes, SAP Agent retrieves the user identity and attributes from the cookie
   - The SAP Agent sets the user Principal to the Web AS username and also adds a principal in the form of a plain string which contains the user attributes retrieved from the FEDPROFILE cookie.
   - The Web AS J2EE server invokes the SAP Agent's CreateTicket login module, which creates the MYSAPSSO2 ticket (logon ticket) for the authenticated Web AS user.

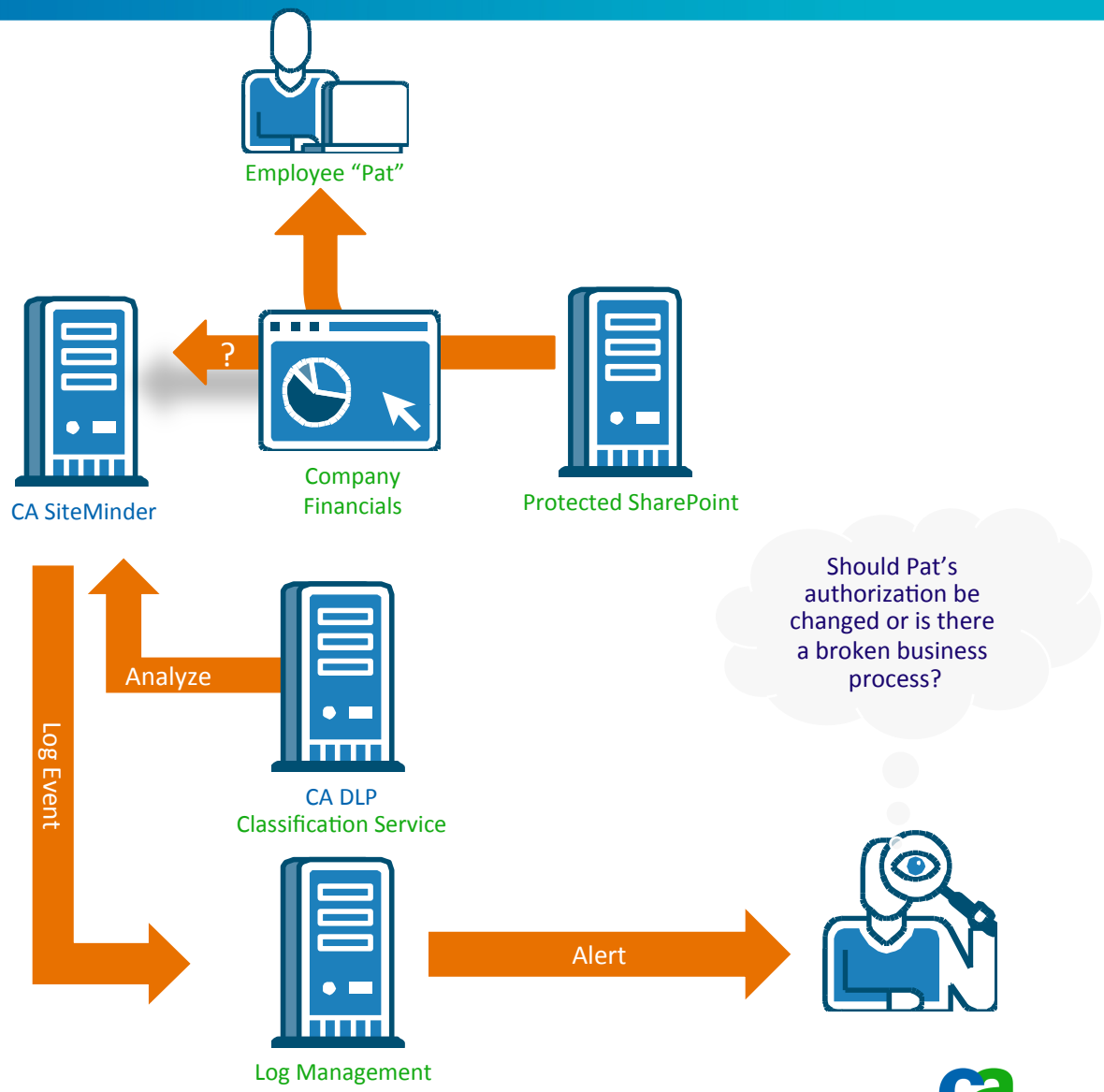
The user now has access to all protected SAP resources !

CA SM, FM, SOA SM r12.5

Themes	Marquee Use Cases	Product Features
Content Aware IAM	Access to resources can additionally be determined by analysis of the content of the resource	▪ SiteMinder can consult DLP products for static content analysis ▪ OOTB support for CA DLP ▪ SiteMinder access policies can be constructed with CA DLP Smart Tags
Identity Assurance	User access to resources can take into account risk factor applied to user authentication	▪ Risk factor assessed at authentication ▪ Risk factor included in SiteMinder session ▪ Risk factor can be included in SiteMinder policy ▪ OOTB support for Arcot RiskFort
Web 2.0 & ID 2.0	Single sign-on and access management support for web 2.0 application and authentication	▪ Enhanced support for web applications built with newer development tools ▪ OpenID RP support ▪ eGov 1.5 ▪ Additional federation enhancements
Service Enablement (delivered via SOA SM 12.5)	SiteMinder is a SOA enabled authentication and authorization engine for organizations evolving to a web services infrastructure	▪ Authentication web service ▪ Authorization web service ▪ Policy administration web services ▪ WS-Trust STS
Management Simplification	Enabling the organization to reduce the overall cost of ownership	• Agent discovery and object correlation • CA (DxGrid) Directory as high performance session service • Merge of Federation Mgr wizard driven UI into SiteMinder admin UI • ***Stretch***: Generic Agent Architecture – Phase 1

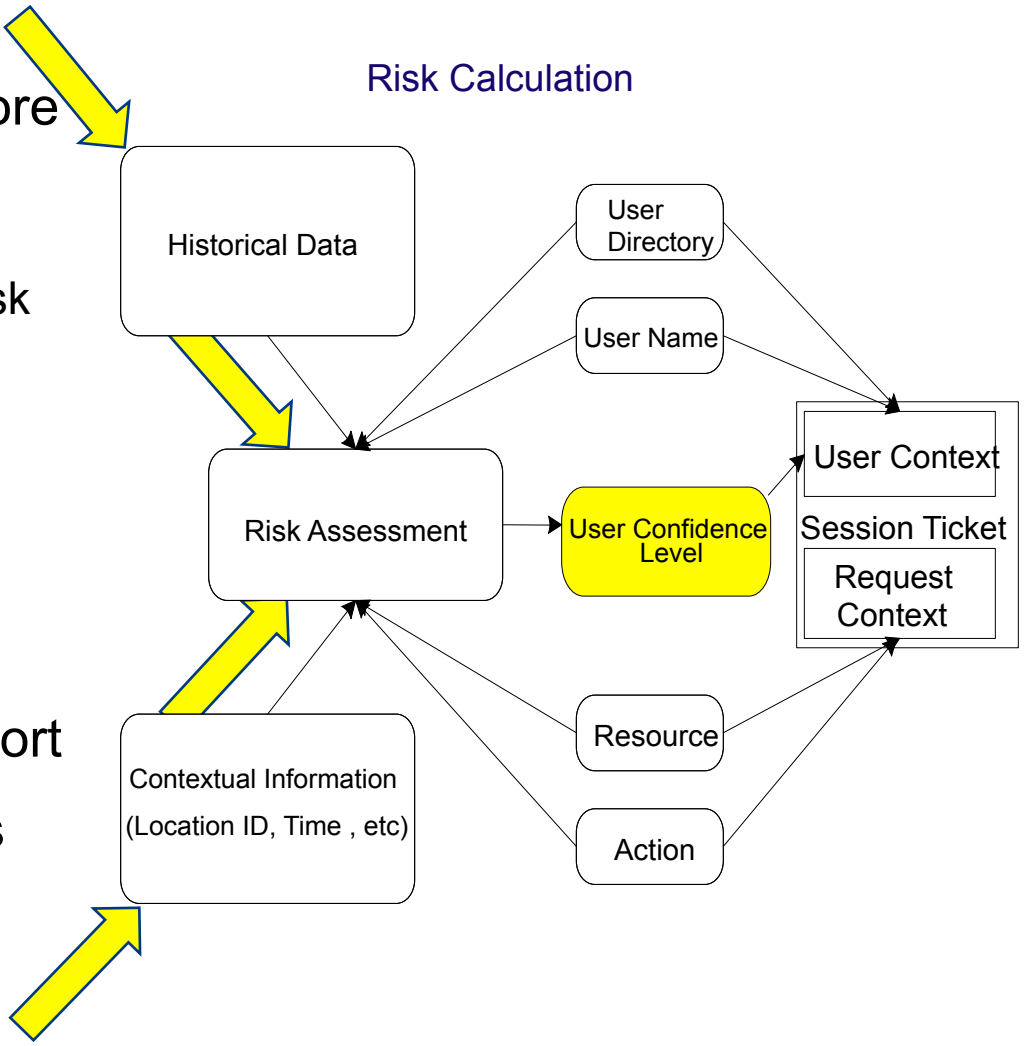
Content Aware Access- CA SM r12.5

- Pat attempts to access a newly uploaded document on a protected SharePoint site
- Before granting access Sharepoint checks with the Identity Centric DLP service to see if the content is sensitive and now has more intelligence to make the right decision
- Event information is shared with the log management solution to proactively address future violations



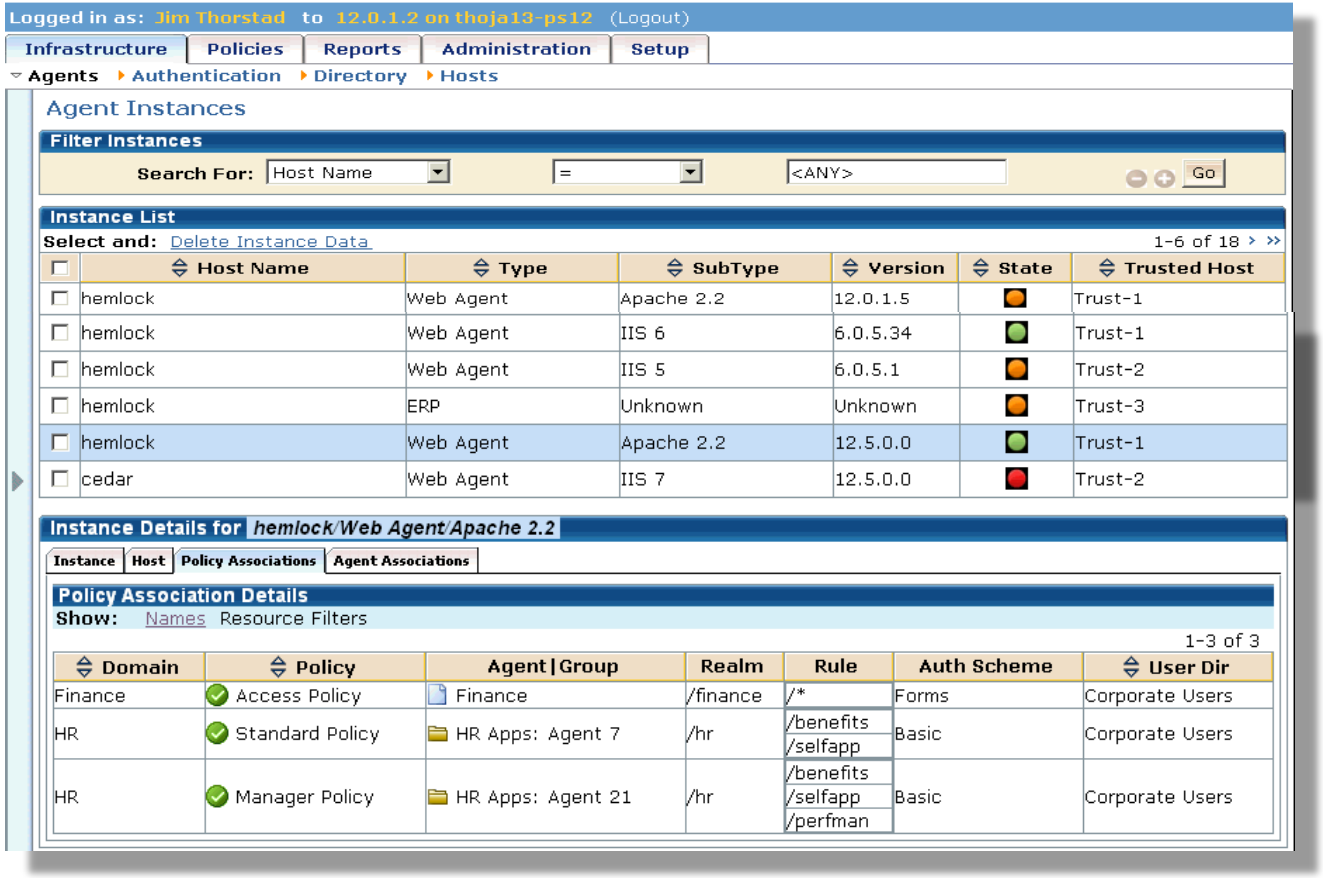
Identity Assurance - CA SM r12.5

- Support authentication risk score
  - Introduce option of authentication risk into policy decisions
    - Accept an externally defined risk score (integer) during authentication
    - Carry risk score in SiteMinder session ticket
    - Possible to utilize risk score during policy evaluation
- OOTB Support for Arcot RiskFort
- Internal API's Available to CA's GSE and Services Teams
  - In support of customer custom integration requirements



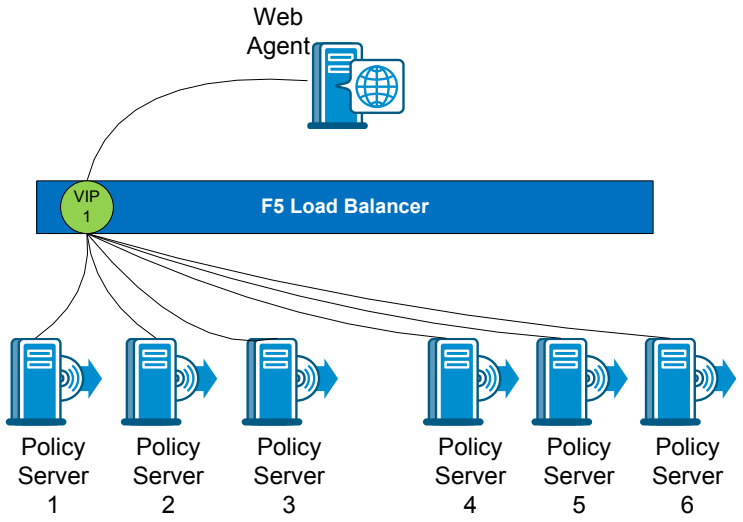
Management Simplification - CA SM r12.5

- What's Connected to the CA SiteMinder System?
- What policies and settings are associated with this agent instance?



Other Enhancements - CA SM r12.5

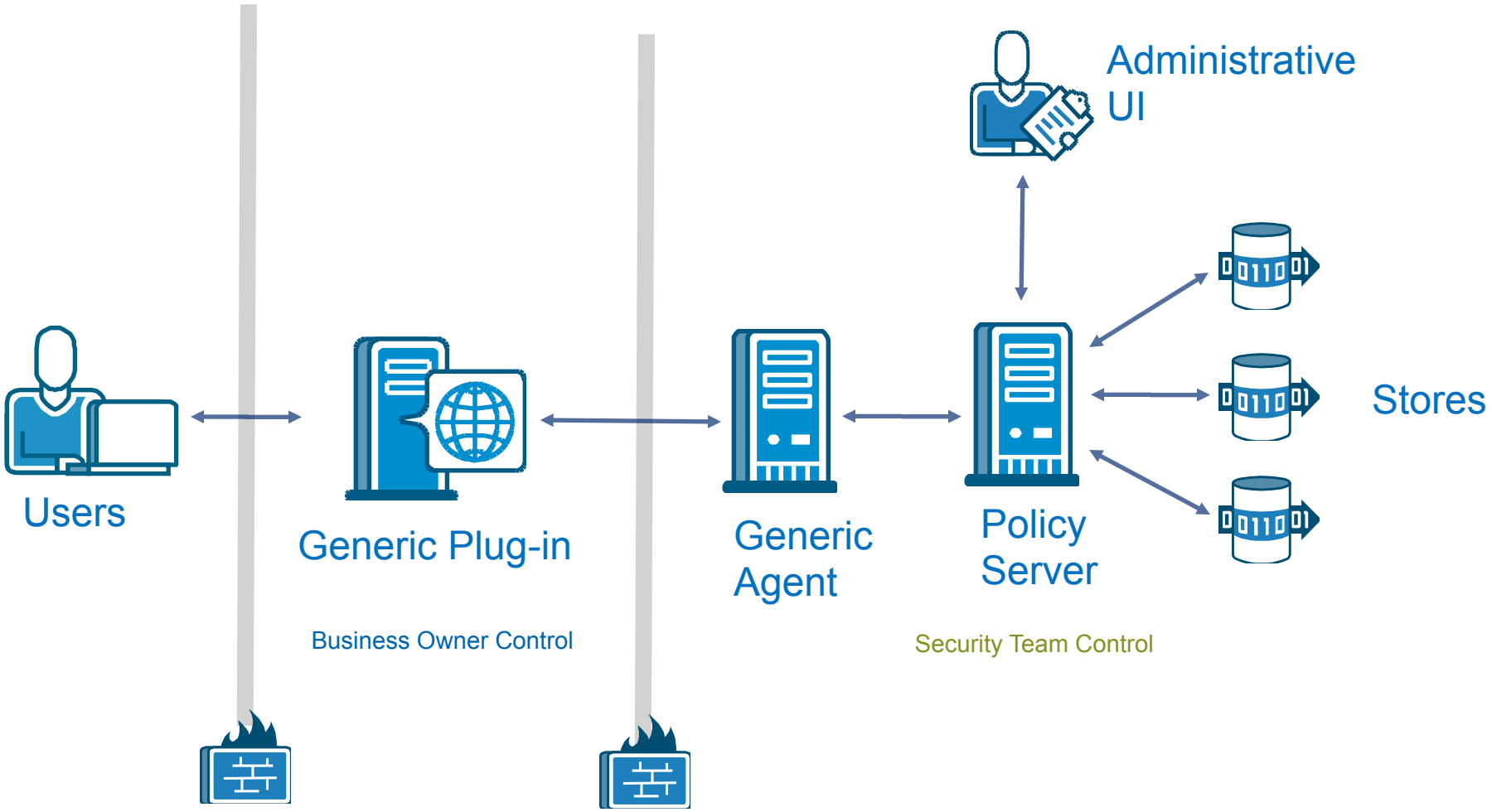
- High performance session service based on DxGrid
  - Alternative to SQL Server replication or Oracle RAC for SiteMinder session store
  - Support for using stored session attributes in policies
- Support for F5 hardware load balancers
- Expanded Options for Directory Mapping
  - Improved ability to integrate multiple repositories
- Directory Provider Enhancements
  - Improved delivery of messages from directory during auth or password change



Generic Agent Concept

- Separate existing agent functionality into web server plug-in and agent logic
- Web server plug-in will be a very simple adapter mapping the web server environment to the generic agent API
- Generic agent will be independent of web server deployed
- A Generic Agent API will be developed which will include support for administrative operations
- Agent upgrades will be accomplished by upgrading the Generic Agent not the web server plug-in

Generic Agent Architecture



Service Enablement
Delivered via SOA Security Manager 12.5

- Authentication
  - Authentication against SiteMinder auth schemes and custom auth schemes
- Authorization
  - Authorize a user to get access to a specific resource/URI
  - Support for XACML 2.0 Request/Response to authorize a user to get access to set of resources/URIs
- Policy Management
  - SOAP-RPC based web services operations for policy administration tasks
- STS
  - WS-Trust

SharePoint 2010

SharePoint 2010 Integration

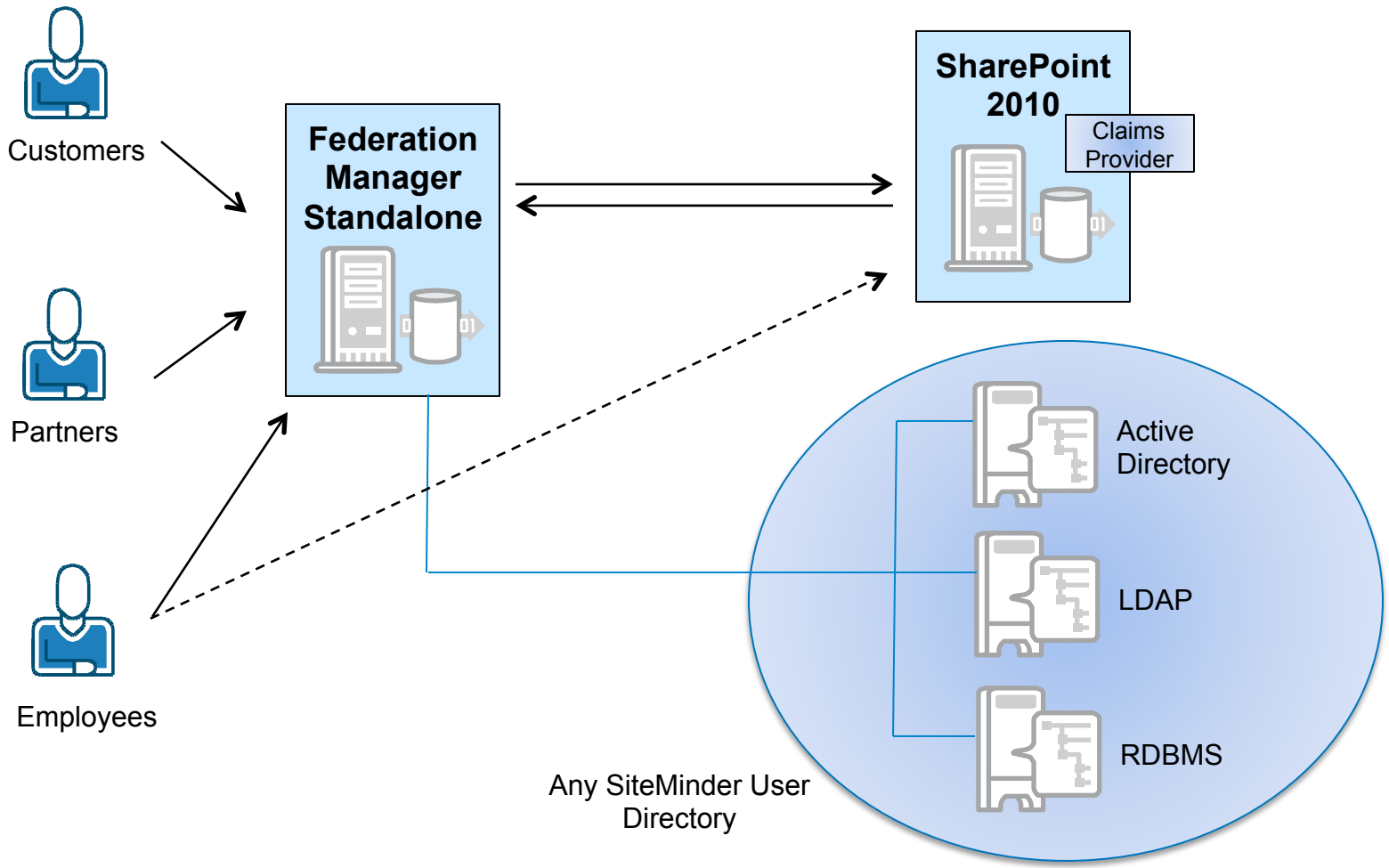
- Authentication
  - Flexible authentication models
  - Full Session Management across all Protected SharePoint Sites and Servers
  - SSO between SharePoint and other Enterprise Applications.
- Authorization
  - Coarse-grained access control for SharePoint Sites
- Auditing
  - Centralize audit data across all protected SharePoint Sites and Servers
- Supports SharePoint user experience
  - SharePoint Claims Provided on behalf of both Federated and Internal Users

Integration with SharePoint

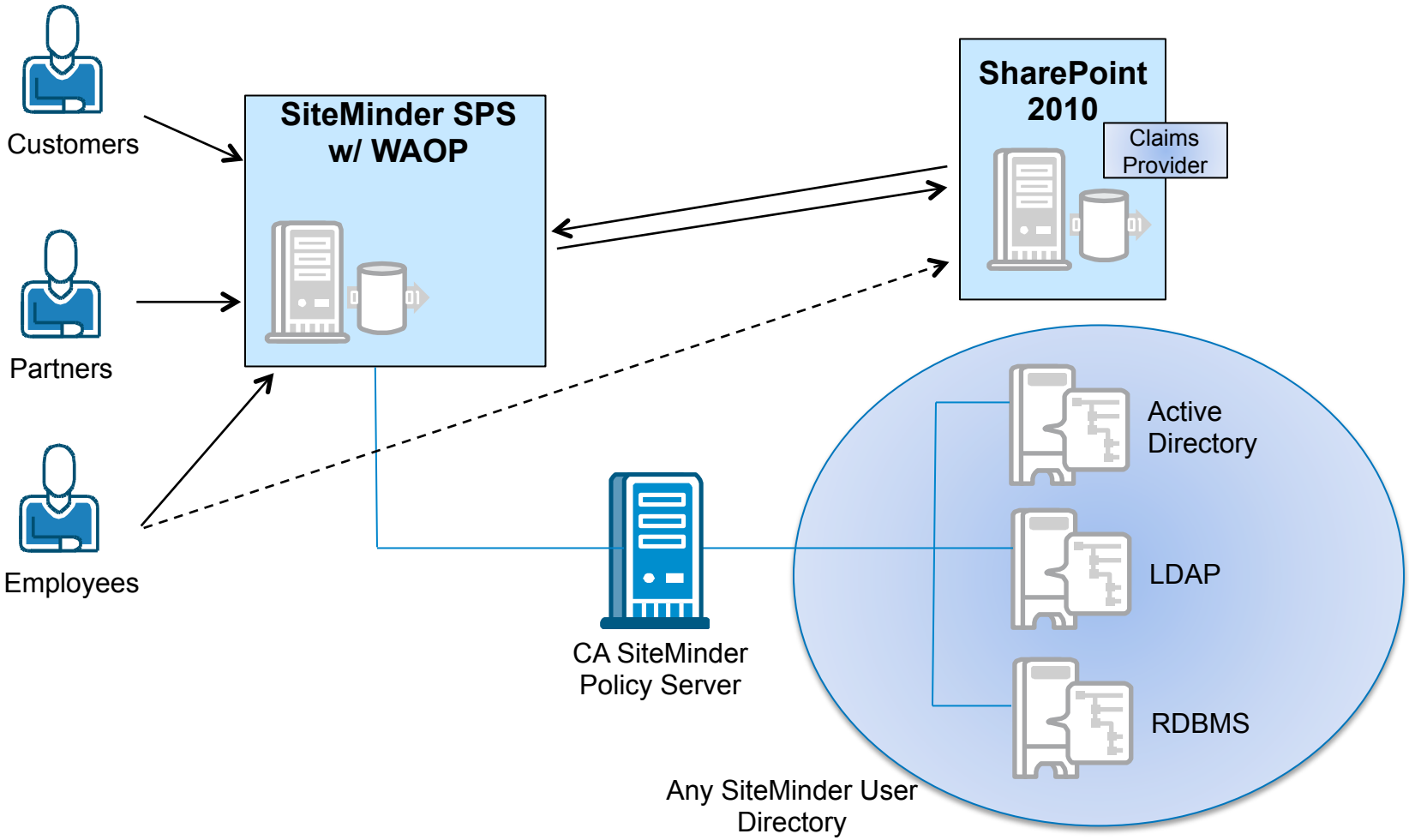
- Two deployment options are provided by the solution to enable SiteMinder support for SharePoint 2010.
  - The first is a light weight federation solution for, but who do not already own or operate a SiteMinder enterprise deployment.
  - The second integrates to SiteMinder using SPS

- To enable this solution, a SiteMinder Claims Provider module must be installed on all SharePoint 2010 servers. This component translates SiteMinder claims asserted by Federation Manager to a form consumable by SharePoint 2010 applications (claims augmentation) and allows SharePoint administrators to lookup and query available SiteMinder claims from within SharePoint administrative tools (i.e. People Picker).

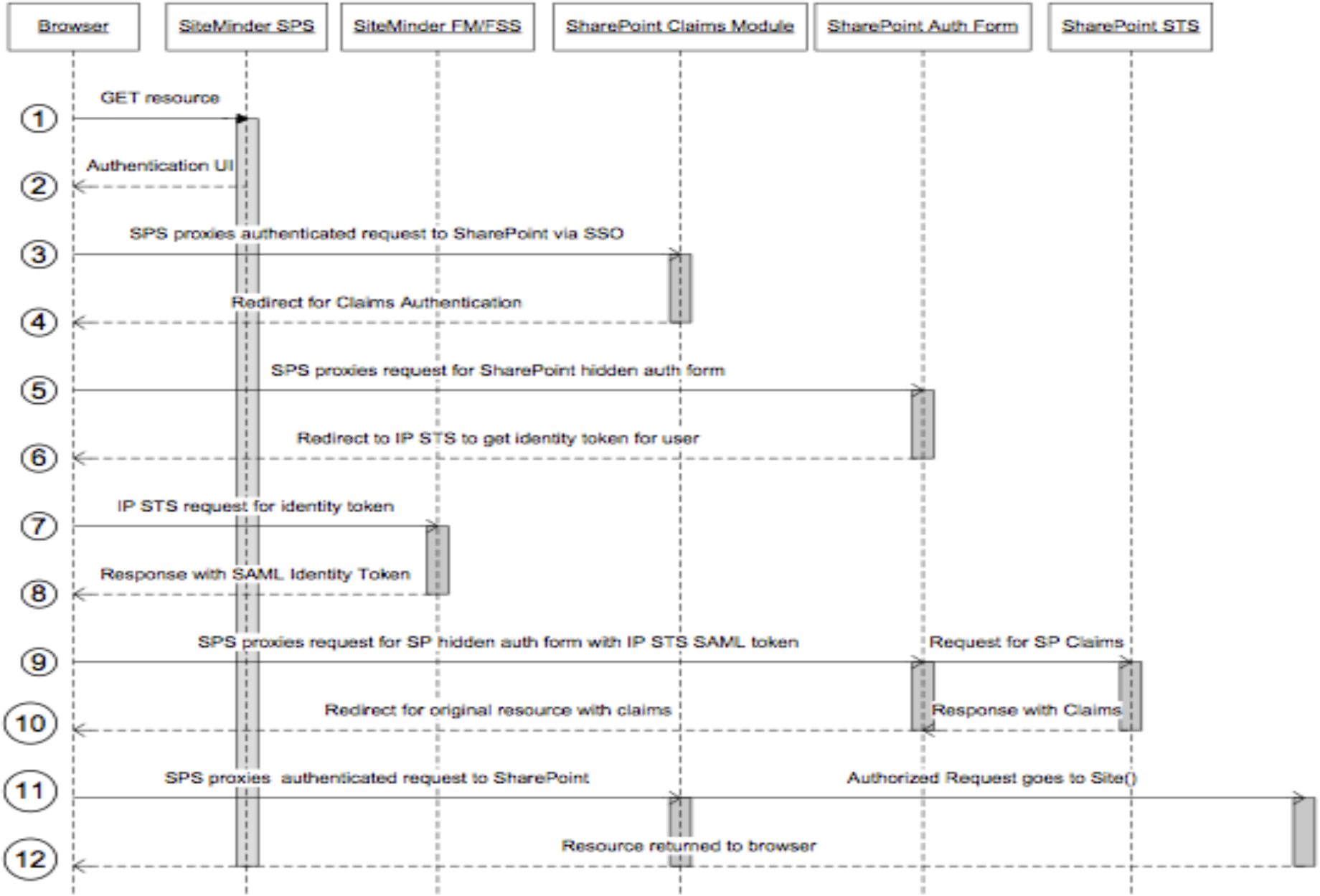
Integration with target web applications at SP
Integration with Sharepoint 2010



Integration with target web applications at SP
Integration with Sharepoint 2010



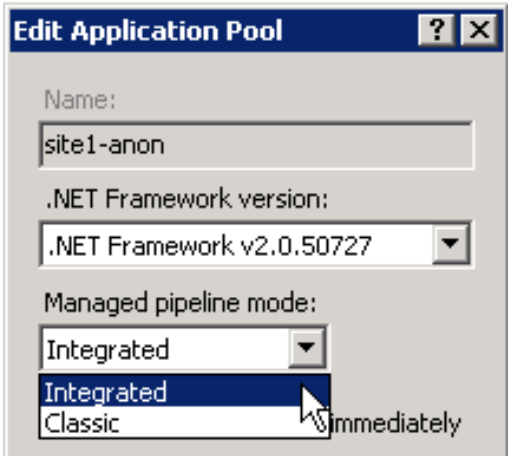
Sequence Diagram

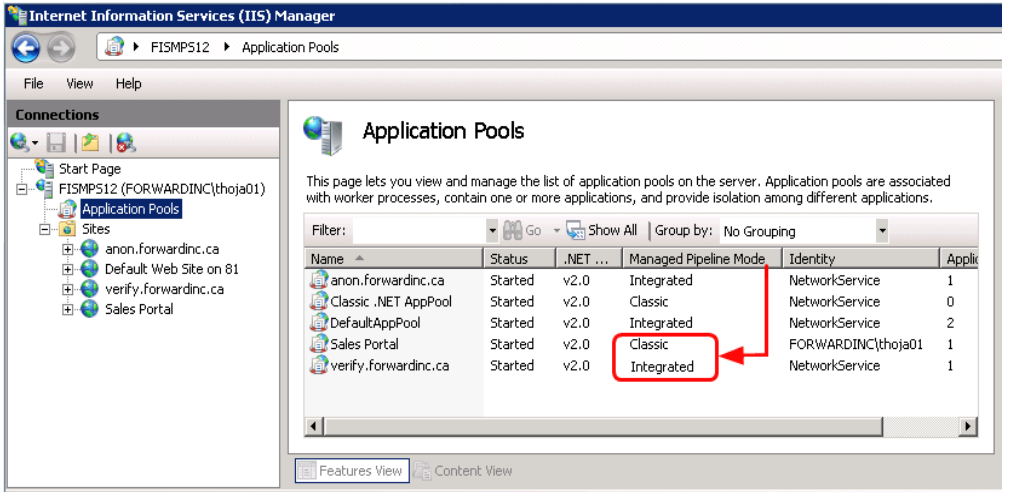


IIS 7
Enhanced Web Agent

IIS Web Agent

- Supports integrated & classic pipeline modes
- Supports “enable 32-bit applications” option
  - Enables SiteMinder protection of both 32-bit and 64-bit apps on one 64-bit IIS server
- Supports IIS application routing feature (ARR)
- Configuration supports for IIS virtual sites
  - Eliminates error prone manual configuration steps
- Support for IIS 7 and 7.5
- Support for IIS 7.x clusters
- Inline credentials (IWA)





Web 2.0 / Identity 2.0

Web 2.0 - Scope

- SiteMinder has traditionally protected classic web applications. The user interface of these applications is rendered through plain browser.
- The user interface is reactive - responds to HTTP responses and displays HTML content generated by a web content application hosted by the Web Server. The user interface flow is partially controlled by SiteMinder HTTP redirection and post preservation

Web 2.0 - Scope

- In contrast, Web 2.0 applications are often characterized as “Rich Internet Applications”. This “richness” is typically achieved by using technologies such as *Ajax, Silverlight, Adobe Flex...*
- The user interface is proactive: the script engine actively manages the display and sends *asynchronous* requests to the backend application. The user interface flow is thus controlled by the script engine.

Web 2.0 - Scope

— Theses engines which enable “richness” in Web 2.0 applications, however pose a problem when these applications are protected by SiteMinder:

1. ***SiteMinder generated HTTP redirection*** (including cookie provider) messages may conflict with the state machine of the script engine. F

   For example, if ***IdleTimeoutURL*** has been defined in ACO, SiteMinder will redirect to this URL if the session has timed out. If the script engine has not been programmed to handle this redirection, either HTTP 302 message or the redirected content, it may reach an indeterminate state.

Web 2.0 - Scope

2. Post preservation – this case arises when the user posts a request, but the session has either expired or does not exist, i.e., first time access, and a redirection to credential collector is required.

- In these scenarios, the Web Agent preserves the posted data in a form with java script and returns the form to the user with HTTP 200 status.
- In the Web 2.0 application, the script will most likely fail when it receives the SiteMinder specific content – java script form.

SiteMinder integration of Web 2.0

— To handle 1 and 2, SiteMinder will send ***customized responses*** to the web application client instead of its usual interjections.

Use Case 1 - WebApp Client Custom Response

— SiteMinder responds using a Web Application Client Custom response instead of its native response – redirection, post preservation

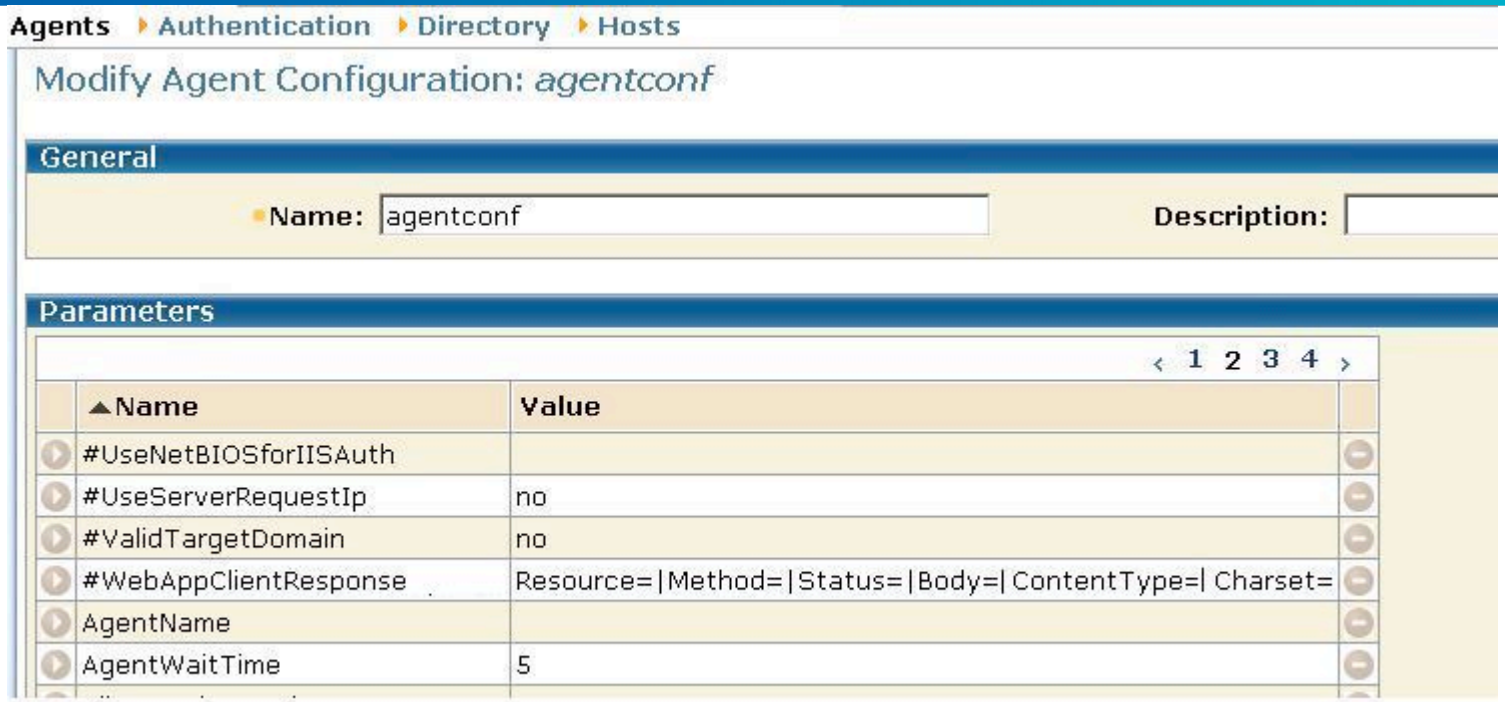
— Web Application Client requests a resource as an un-authenticated entity or requests a resource to which it is not authorized to access

1. Web Application Client requests a resource
2. SiteMinder determines a SiteMinder native response is required to be sent to the Web Application Client
   - may be due to a timeout or other policy violation
3. SiteMinder responds with a custom response that can be handled by the Web Application Client
4. The Web Application Client handles the custom message gracefully

Administrator Perspective

- The Custom Response will have the following parts
  - HTTP Status – provided by the SiteMinder
  - HTTP Body – custom body configured which the WAC can handle. It may optionally include the following SiteMinder generated data:

ACO Example



— As shown above, this new ACO setting (WebAppClientResponse. The administrator simply needs to fill out the values for these attributes when he wants to use this ACO setting.

WebAppClientResponse:**Resource**=/web20/dir/*|**Method**=GET,POST|**Status**=200| **Body**=C:\location\custombody_1.txt|**Content-Type**=application/xml|**Charset**=us-ascii

Use Case 2 - HTTP Method Support

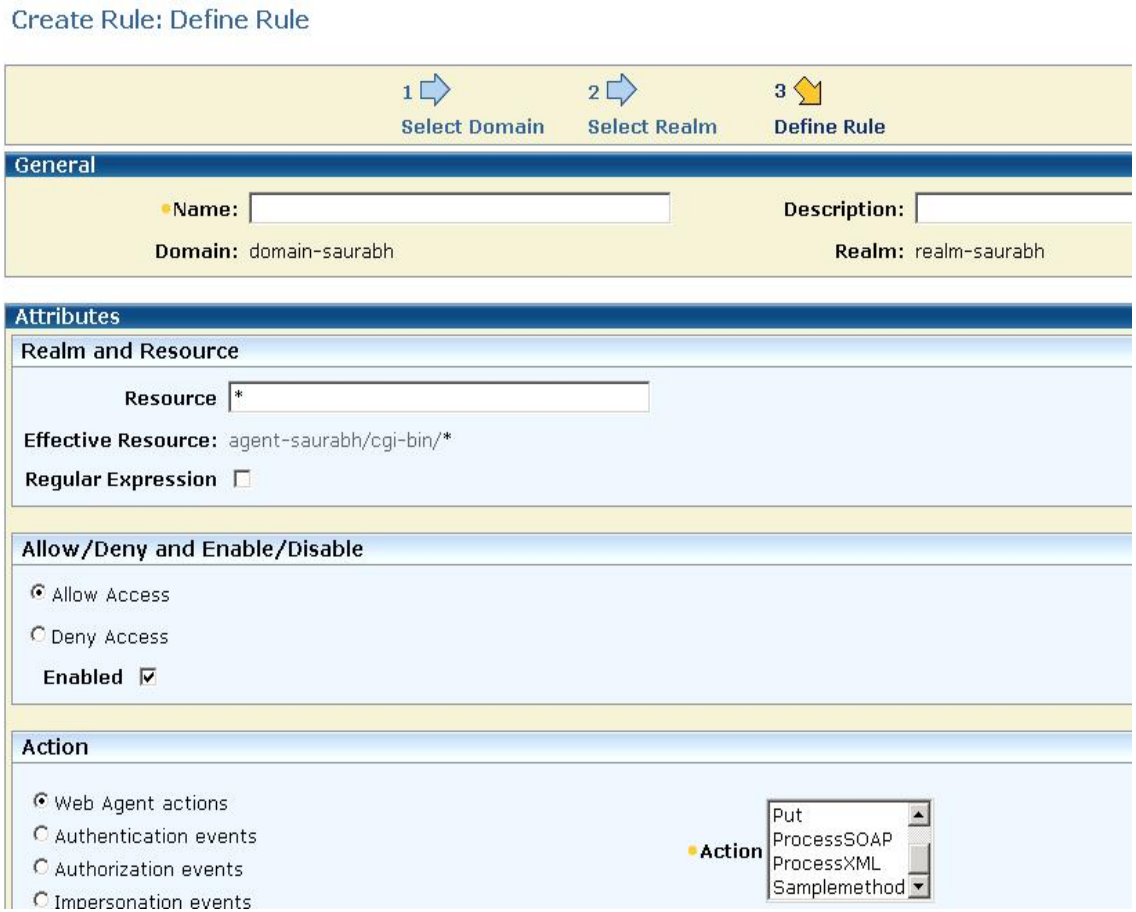
— Support additional HTTP 1.1 methods : Web Application Client accesses a resource using an HTTP method other than GET, PUT or POST

1. Web Application Client issues an HTTP request with a method other then GET, PUT or POST
2. SiteMinder evaluates the current security policies
3. SiteMinder either allows access to the resource or denies, depending upon the result from 2 above

Administrator Perspective

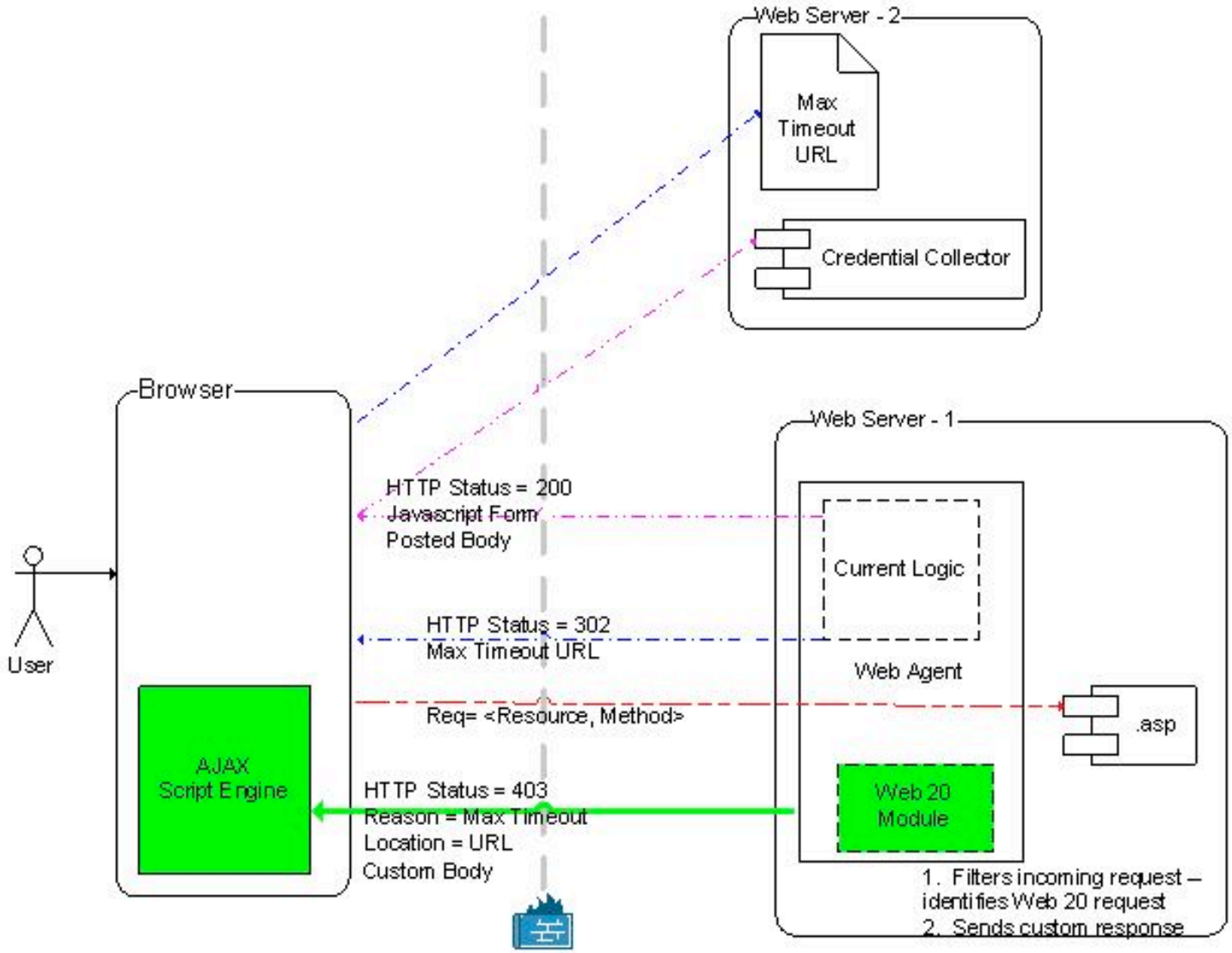
- The SiteMinder administrator will configure the required ACO setting to enable this feature. Also, the administrator can configure SiteMinder rules with the newly introduced HTTP methods for protection of resources.
- Currently the policy store supports GET, PUT and POST HTTP methods by default. Support for additional methods such as DELETE, HEAD, … will be added.
- This addition will enable an administrator to define rules using these newly introduced HTTP methods

New Method

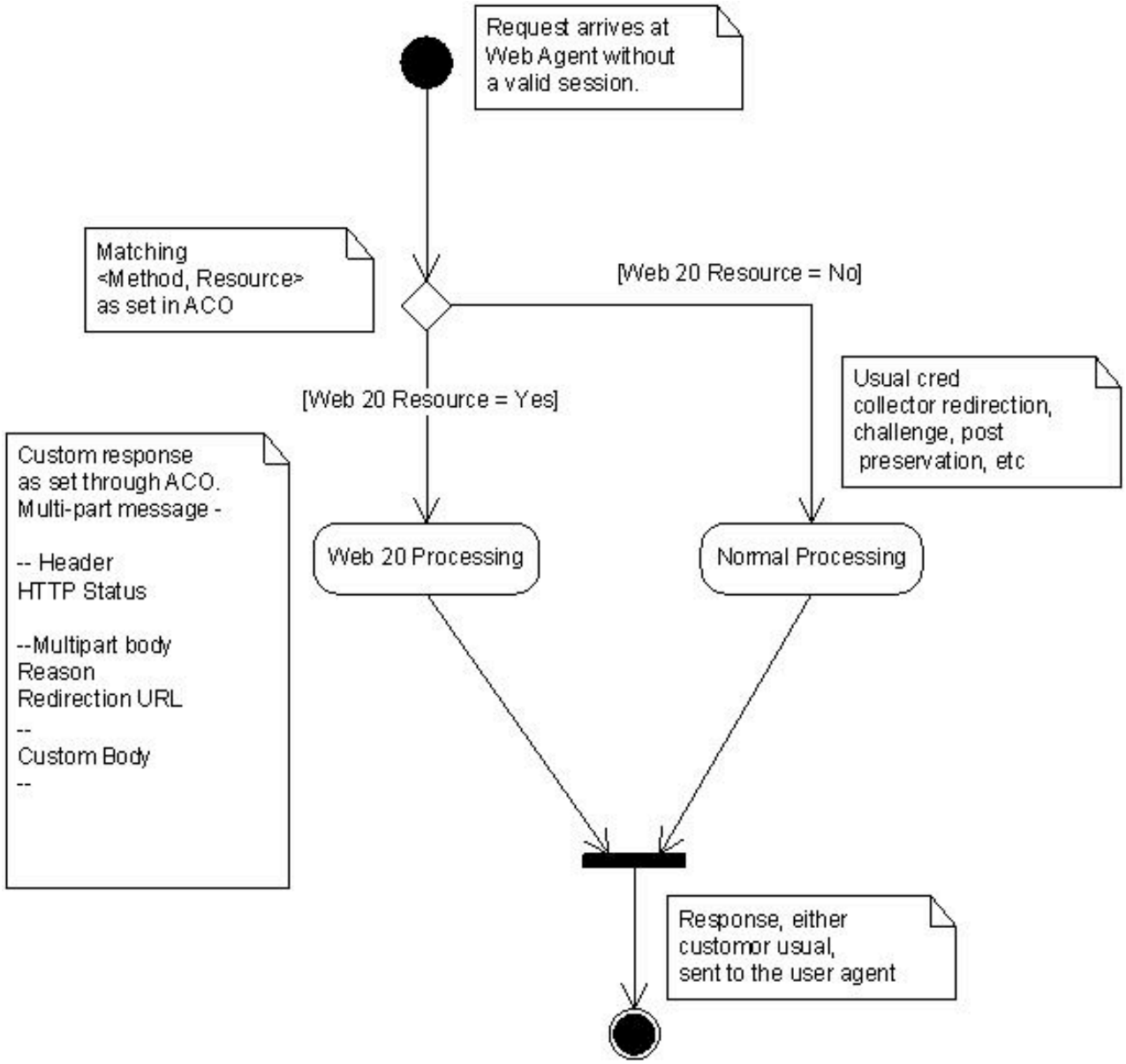


— The figure shows that the custom action added above in the “Web Agent” Agent type gets displayed automatically in the Rule dialog. Thereafter, the Siteminder would automatically take care of protecting the methods displayed in the Rule dialog.

Architecture



Sequence - Flow



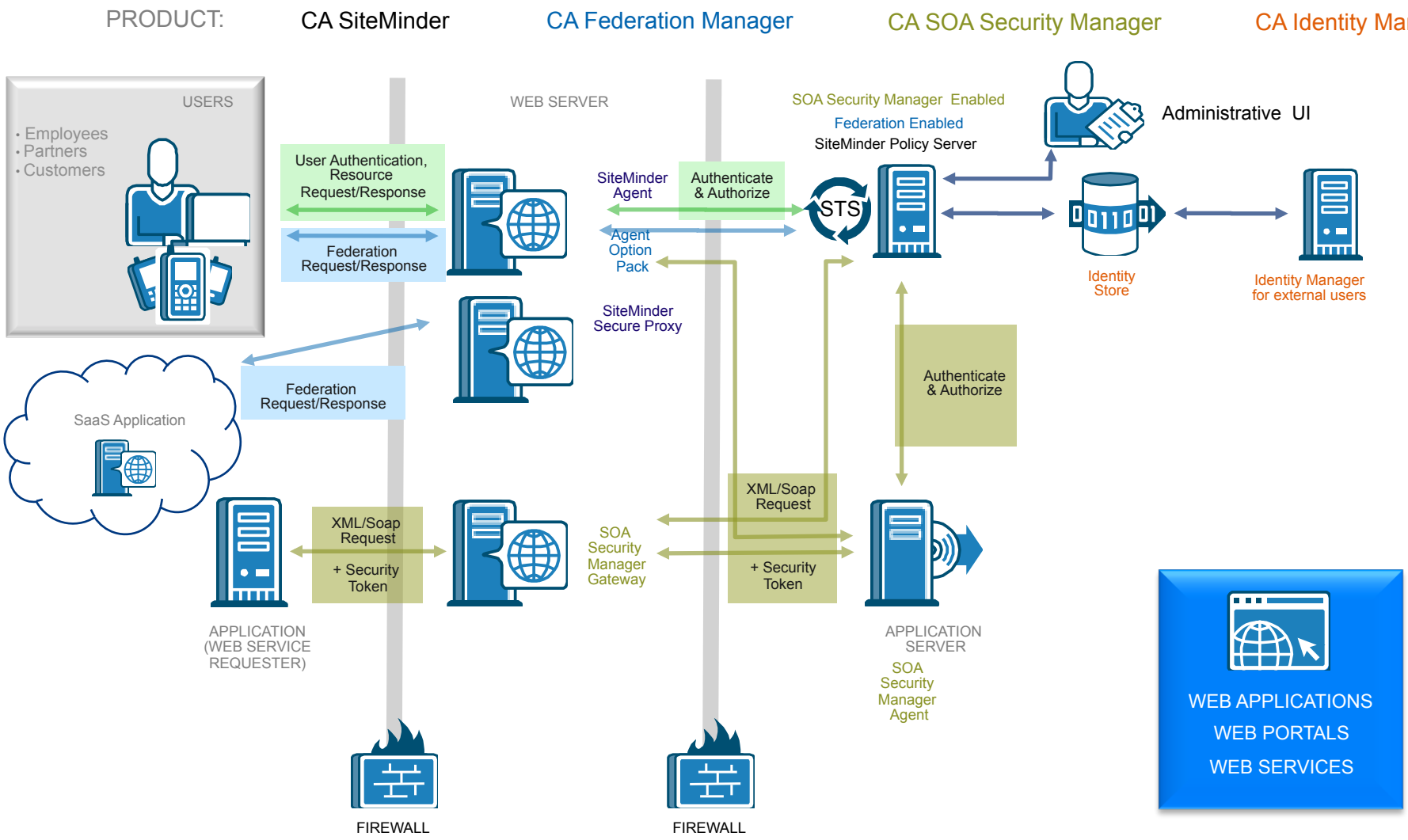
Web 2.0/ID 2.0 - CA SM, FM r12.5

- Support Web 2.0 Applications (e.g., AJAX, Silverlight…)
- OpenID 2.0 compliant authentication scheme (ICAM OpenID 2.0 Profile)
- eGov 1.5
- SLO/SOAP
- New ACO Settings Make it Possible to:
  - Overlook heartbeat requests to support the spirit of the SiteMinder idle timeout
  - Ignore uninteresting requests to minimize auditing load
  - Provide a customizable response to the application so it can handle authentication (status code and body)

Roadmap

SiteMinder Product Family

Comprehensive & Integrated Yet Modular Solution



SiteMinder Product Family Roadmap

Release	High Level Description / Key Features	H2 2010	H1 2011	H2 2011
SiteMinder R12 SP2 ASA Agent release	• Cryptographic algorithm enhancements • Key platform support	August		
SiteMinder r12 SP3	• SHA-2 digital signature support • Sequential CDP processing for cert auth (with SHA-2) • OCSP to CRL fall back	Sept end		
Federation Manager r12.1 SP3 & SOA Security Manager r12.1 SP3	• Built and released on SiteMinder r12 SP3 policy server	Dec end		
SiteMinder IIS Agent	• Wizard for configuring virtual web sites on IIS • Support IIS clustering and native module architecture • Support application request routing		March end	
SiteMinder Solution for SharePoint 2010	• Single Sign on with SM session mgmt. • Coarse grain authz • Integration with Principal picker		March end	
SIteMinder SPS r12.5	• Graphical Admin UI • Target feature parity with web agent • Support kerberos auth scheme • Wily Introscope support		June end	

Targeted
Being Planned

SiteMinder Product Family Roadmap

Release	High Level Description / Key Features	H2 2010	H1 2011	H2 2011
SiteMinder r12.5 (& Federation Manager)	• Content aware access control (DLP ready) • Identity assurance – risk factor integrated with authn and authz decision • Support Web 2.0 apps (Ajax, Adobe Flex, Java Webstart) • OpenID RP support • Agent discovery and object correlation • CA (DxGrid) Directory as high performance session service • eGov 1.5 (as part of FM on SM) • Merge of Federation Mgr wizard driven UI into SiteMinder admin UI • Generic Agent Architecture		June end	
SOA Security Manager r12.5	• Authn Web Service for SM • Authz Web Service for SM (incl. XACML request/response) • Policy Mgmt. Web Service for SM • STS			Q3

Targeted
Being Planned

CA SiteMinder Product Family Roadmap Overview