

Product Integration Brief



Layer 7 SecureSpan/CloudSpan Integration notes for CA SiteMinder®

Revision 1.0

Layer 7 Technologies

Layer 7 Technologies helps enterprises secure and govern interactions between their organizations and the services they use in the cloud; across the internet; and out to mobile devices. Through its award-winning line of [SOA Gateways](#), [Cloud Brokers](#) and [API Proxies](#), Layer 7 gives enterprises the ability to control identity, data security, SLA and visibility requirements for sharing application data and functionality across organizational boundaries. With more than 150 customers spanning six continents, Layer 7 supports the most demanding commercial and government organizations. Layer 7 solutions are FIPS-compliant, STIG vulnerability tested and have met Common Criteria EAL4+ security assurance.

Layer 7's SecureSpan and CloudSpan families of gateways provide the role of a Policy Enforcement Point (PEP) between service providers and consumers, enforcing application-level policies around access control, data security, data mediation and SLA governance. These gateways integrate with existing Identity and Access Management (IAM) solutions to implement access decisions based on user, service, operation, message content, time of day, and other transaction metadata. CA SiteMinder® provides the existing authentication and authorization infrastructure that is extended to application traffic within Layer 7 gateways. SiteMinder becomes the Policy Decision Point (PDP) for these access control decisions. In some instances, CA SOA Security Manager® can also play this PDP role for web services based traffic.

Integration Summary

Many enterprises have made an investment in CA SiteMinder for managing user identities and authenticating and authorizing access to Web applications. As more data and applications are exposed via APIs using technologies such as SOAP, XML, REST and JSON for mobile, cloud and partner integrations, an application-aware security and governance layer becomes a necessity. Layer 7 gateways are hardware, virtual and software appliances designed to enforce policies around access control, data security and governance. These gateways can leverage an existing SiteMinder infrastructure for application-aware authentication and authorization decisions.

Layer 7 appliances uses a declarative Policy Manager to create a workflow that is executed upon incoming application traffic. Individual units of functionality called assertions are combined to define these larger policies. Assertions can express a requirement ("Require SSL or TLS"), perform an operation ("Transform message using XSLT") or interact with other networked systems ("Route using HTTP"). Assertions around access control include the extraction of various credential tokens, validation of those credentials against an authentication server, authorization of those credentials against an authorization server, and mapping of identities between the consumer domain and service provider domain. Composition of multiple assertions allows comprehensive access control, identity federation, and single sign-on capabilities.

Integration with CA SiteMinder involves installing and configuring the SiteMinder assertion and inclusion of that assertion in a policy within the Layer 7 Policy Manager. During service or API execution, the appropriate credentials and target details are extracted from the incoming request and sent to a CA SiteMinder Policy Server for evaluation. If the authentication and authorization are successful, processing continues and the message is delivered to its intended destination. If the user is not authenticated or authorized for the intended target, the message is rejected and an error is returned to the consumer.

Product Integration Brief

Layer 7 SecureSpan/CloudSpan Integration notes for CA SiteMinder®

Revision 1.0

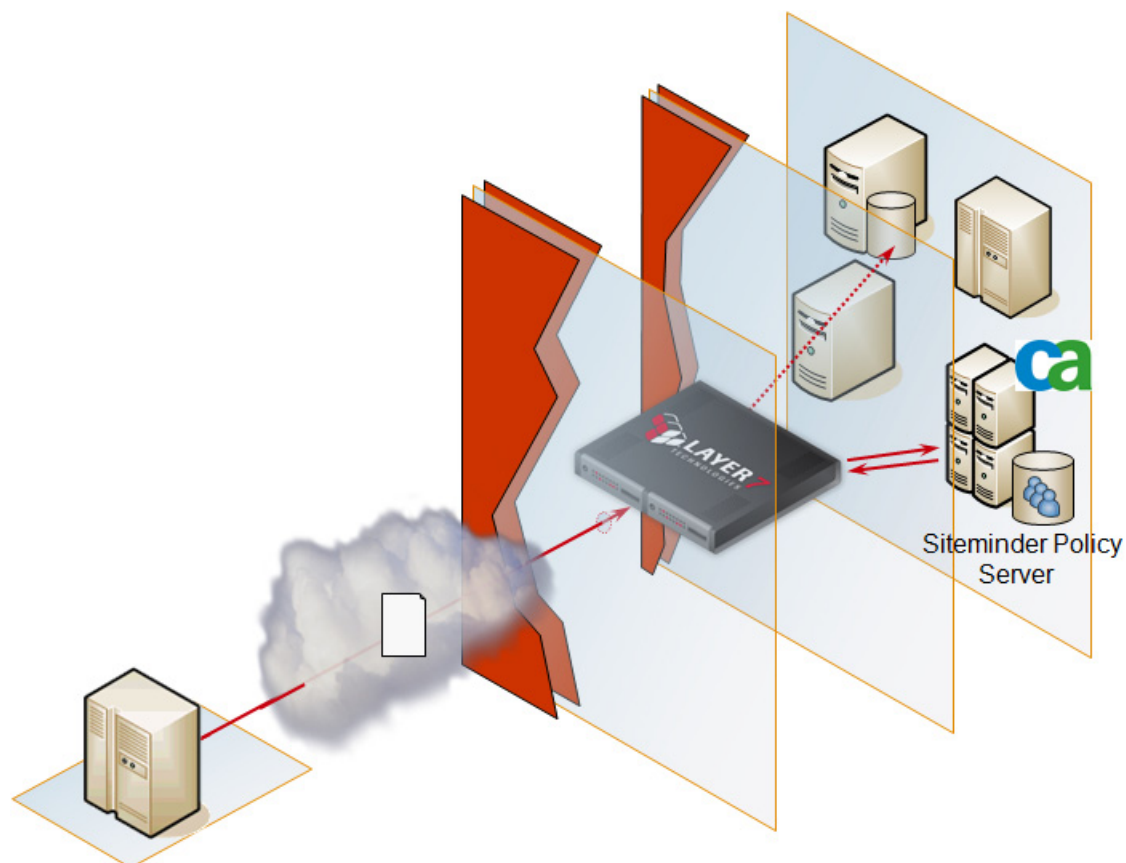


Figure 1: Layer 7 gateways use a callout to a CA SiteMinder Policy Server to make an access control decision

System Requirements

Layer 7 Gateways are available as hardware appliances, virtual appliances deployed on VMware or Xen, and software installations for RHEL, SUSE or Solaris. In addition, cloud-based instances of the gateways are available for Amazon AWS and Cloud Commons. More information is available on the Layer 7 [website](#).

Integration with CA SiteMinder versions 6.0 and r12 is supported by Layer 7 Gateways version 5.3.1 or higher.

Integration Details

Integration of a Layer 7 Gateway with CA SiteMinder consists of two distinct parts:

- Installation and configuration of the SiteMinder policy assertion is required before the first use of the assertion, and only needs to be modified if connection data has been changed.
- Use of the *Authenticate with SiteMinder Protected Resource* assertion within a policy will delegate authentication and authorization tasks for the service being exposed by the Gateway.

Product Integration Brief



Layer 7 SecureSpan/CloudSpan Integration notes for CA SiteMinder®

Revision 1.0

Before the SiteMinder assertion can be used, it must be installed and configured on the Gateway. This task is described in the *Layer 7 Custom Assertion Installation Manual*. The document walks through the process of installing the assertion and defining connection information in the `siteminder.agent.properties` cluster property. Instructions are provided for creating a new configuration or migrating an existing configuration from another gateway.

Once installed, the SiteMinder assertion allows delegation of authentication and authorization decisions to the SiteMinder Policy Server. This involves a callout from the Gateway to the defined Policy Server with a set of credentials extracted during policy execution and a resource against which to authorize the credentials. Configuration of the assertion is described in the *Layer 7 Policy Authoring User Manual*, in the section titled *Authenticate with SiteMinder Protected Resource Assertion*.

Sample Use Case Scenario

Layer 7's integration with SiteMinder is often used to extend the existing web application protection to new APIs based upon SOAP or REST standards. In this case, incoming user credentials are extracted from the request and the service call is authorized through a callout to the SiteMinder policy server. Service operations are mapped to a URL-style resource to enable SiteMinder to make a decision about the request.

In the following example, a Layer 7 Gateway is proxying a simple SOAP request to list the products in a warehouse. The user credentials are extracted from an HTTP Basic Authentication header and delivered to the SiteMinder Policy Server defined as "layer7" in the SiteMinder assertion's configuration properties.

The Layer 7 Policy Manager contains three assertions. The first extracts the credentials, the second sends those credentials along with the resource to the Policy Server, and the third routes successfully authenticated and authorized requests to the appropriate backend SOAP service.

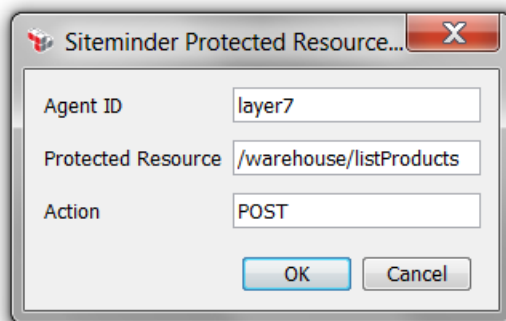
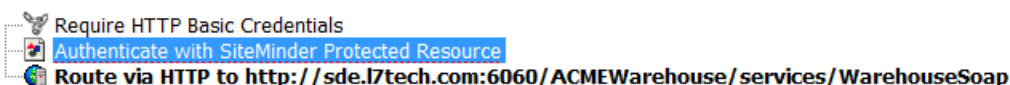


Figure 2: The SiteMinder Protected Resource assertion retrieves an authorization decision from the Policy Server

This simplified example can be enriched with additional assertions to require protocol level-security, transformation, threat protection, logical evaluation of the request or other policy tasks. Additionally CA SOA Security Manager can be added to this scenario to provide a layer of web service security that extends from the Layer 7 Gateway to the warehouse products application.

Product Integration Brief

Layer 7 SecureSpan/CloudSpan Integration notes for CA SiteMinder®

Revision 1.0



Contact Information

Layer 7 Technologies

1100 Melville St., Suite 405
Vancouver, BC V6E 4A6
Phone: 800-681-9377
Fax: 604-681-9387
Email: info@layer7.com
Website: www.layer7.com

CA Technologies

One CA Plaza
Islandia, NY 11749
Phone: 800-225-5224
Fax: 631 342-6800
Email: TechnologyPartnerProgram@ca.com
Website: support.ca.com

Support

Product support is available 24 hours a day through Layer 7's self-service portal, located at

<http://www.layer7.com/support>.

Support can also be reached by telephone at 888-681-9377 in North America; for international numbers, see the support link above.

Appendices