SAML 2.0 federation

This article describes SAML 2.0 and how it is used in Nexus Hybrid Access Gateway.

What is SAML 2.0?

Security Assertion Markup Language 2.0 (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between online business partners, in particular, between an identity provider and a service provider. This security information is expressed in the form of portable SAML assertions (tickets) that applications working across security domain boundaries can trust. The single most important requirement that SAML addresses is web browser single sign-on (SSO).

A user requests a service from the service provider. The service provider requests and obtains an identity assertion from the identity provider. On the basis of this assertion, the service provider can make an access control decision – in other words it can decide whether to perform some service for the connected user.

In Hybrid Access Gateway, a SAML federation is set up to enable Hybrid Access Gateway to act as service provider or identity provider.

> With SAML we refer to SAML 2.0.

SAML concepts

- Service provider
  The service provider will as the name implies provide some sort of service. In the case of Hybrid Access Gateway a service is a resource, tunnel-set or web-resource, which it provides access to. In the case of other providers it can be just about anything, that is, the service provider has something the user wants.
- Identity provider
  The identity provider handles the authentication of the user, that is, making sure that the user is the one he claims to be. In Hybrid Access Gateway this could be to require a Mobil Text login or some other sort of authentication.
- Subject
  The subject is the user that will be using the service at the service provider and will be authenticated by the identity provider. In Hybrid Access Gateway this is almost certain to be a user; however the SAML standard does not prohibit it from being some sort of device, for example, a computer, needing access to a service.
- Ticket
  The identity provider issues tickets (or SAML assertions) to authenticated users with the information agreed between the service provider and the identity provider. The ticket is signed by the server certificate of the identity provider. In Hybrid Access Gateway, a ticket will only be created when a user is authenticated and a value for the subject exists.
- Single Sign-On
  SAML solves the MDSSO (Multi Domain Single Sign-On) problem by providing a standard vendor-independent grammar and protocol for transferring information about a user from one web server to another independent of the server DNS domains.
- Federated identity
  Business partners agree on and establish a common, shared name identifier to refer to the user in order to share information about the user across the organizational boundaries. The user is said to have a federated identity when partners have established such an agreement on how to refer to the user.

Related information

- Add a SAML 2.0 federation
- Resources

Links

- Information about SAML 2.0 (Wikipedia)