White Paper

Solving Substantiation with SAML

Organizations are deploying distributed, hybrid architectures that can span multiple security domains. At any moment, a user could be accessing the corporate data center, the organization's cloud infrastructure, or even a third party, SaaS web application. SAML can provide the identity information necessary to implement an enterprise-wide single sign-on solution.

by Peter Silva
Technical Marketing Manager—Security

Contents

Introduction

Proving or asserting one's identity in the physical world is often as simple as showing a driver's license or state ID card. As long as the photo matches the face, that's typically all that is needed to verify identity. This substantiation of identity is a physical form of authentication, and depending on the situation, the individual is then authorized either to receive something or to do something, e.g., enter a bar, complete a purchase, etc.

In the digital world, identity verification is not as easy as showing the computer monitor a driver's license. To gain entry, you must provide information like a name, password, randomly generated token number—something you have, something you know, or something you are—to prove you are who you say you are.

Gaining access to corporate assets is no different. Many organizations have multiple different resource portals, however, each requiring digital proof of identity. Their users may also need to access partner portals, cloud based Software as a Service (SaaS) applications, or distributed, hybrid infrastructures that span multiple data centers, each requiring a unique user name and password. In addition, the average employee must maintain about 15 different passwords for both her private and corporate identities, with many of those passwords also being used for social media and other risky entities. Statistics show that 35 to 50 percent of help desk calls are related to password problems, with each call costing a company between $25 and $50 per request.

Security Assertion Markup Language (SAML) is an XML-based standard that allows secure web domains to exchange user authentication and authorization data. It directly addresses the problem of how to provide the users of web browsers with single sign-on (SSO) convenience. With SAML, an online service provider can contact a separate online identity provider to authenticate users who are attempting to access secure content. For example, a user might need to log in to Salesforce.com, but Salesforce (the service provider) has no mechanism to validate the user. Salesforce would then send a request to an identity provider, such as F5® BIG-IP® Access Policy Manager® (APM), to validate the requesting user's identity. BIG-IP APM version 11.3 supports SAML federation, acting as either a service provider or an identity provider, enhancing the employee's online experience and potentially reducing password-related tickets at the help desk.

Who Are You and What Do You Want?

Gone are the days when employees were statically mapped to their assigned resources. Over a decade ago, the majority of corporate employees worked in the office, connected to the organization's local area network (LAN). Their applications and resources ran behind firewalls and served those well-defined users, the employees. This approach was secure since, at the time, there were only two entry points: the front door of the building or a VPN. Verifying an employee's identity was fairly straightforward, since he would log in from the same desktop in the same cubicle with the same credentials on a daily basis.

Today, not only are applications running on the LAN/corporate data center, there are also corporate resources being delivered from cloud-based networks. These cloud resources might not have access to a corporate directory for employee validation. In addition, today's workforce is highly distributed, using a multitude of different access devices, yet organizations must still secure access to critical corporate resources. Rather than admitting individual users from their single, trusted desktops, organizations must now provide secure access from anywhere, at any time, from any device. This is not a simple task.

Any number of access hurdles can appear when organizations deliver services from hybrid architectures. Controlling who is granted access to which resources becomes a real challenge when users can get access from any browser, at any time, from any place. This situation is exacerbated by the purchasing and approval process that is unique to SaaS applications. Often, the purchase of a new cloud app is made directly by the user or business unit head, and frequently the immediate business needs and technological benefits of going to the cloud are put ahead of ensuring information is sufficiently secure. The challenge of security multiplies as partnerships, mergers, divestitures, and terminations dynamically impact who the users are and what they have access to. As if this weren't enough, every SaaS application out there has its own model for administering users, and that model usually doesn't integrate well with how organizations typically manage users behind a firewall.

The SaaS model makes it easier for users to initially access an application, but complexity quickly increases with the growing number of applications being served from multiple locations. Each application might have different password requirements. One might require six characters that can be any combination, and another might require seven with at least one number, while another might not

allow special characters at all. Also, some passwords expire every month, while others change each quarter, etc. The result is insecure passwords and, ultimately, vulnerable applications.

Each application in the cloud is designed with its own user directory—yet in the enterprise, directories are a single entity (often Active Directory) that governs access to core IT systems. IT needs a single directory that is federated with all of the SaaS applications in an organization's cloud services network, or headaches like password fatigue become a daily occurrence. The deeper issue is that the cloud service might not have access to an employee directory. Often, integrating with on-premises directories requires some sort of synchronization—which means employee information is outside the IT department's control—or the exposure of authentication services to the cloud provider, if the user store must remain on the premises. Both are risky.

Also, with increasing regulatory scrutiny, it's critical that IT teams are able to address compliance pressures. They must know who has access to what application (locally or in the cloud), at what privilege level, and who is actually using those privileges and how. IT staff must be able to react quickly to user status changes, such as automatically de-provisioning access when a user leaves the company, and to provide an audit trail of those actions.

SAML as a Solution

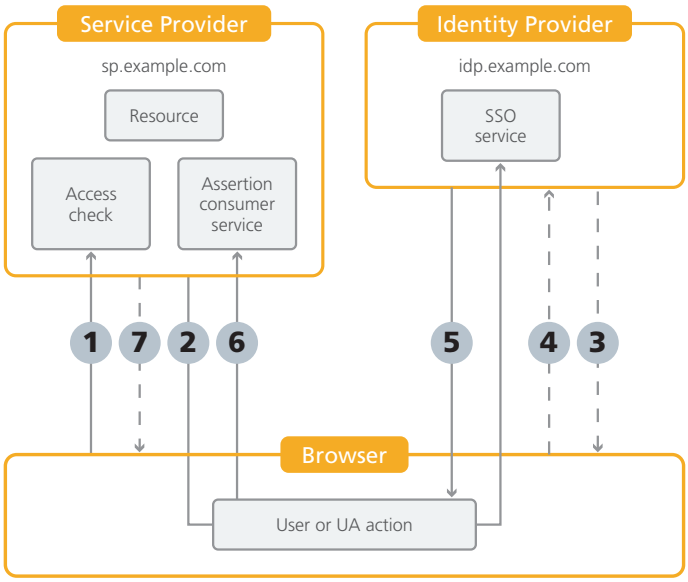
In early 2001, the OASIS Security Services Technical Committee (SSTC) was chartered *"to define an XML framework for exchanging authentication and authorization information."*[1] By the end of 2002, SAML version 1.0 specifications became an OASIS standard. Over the next couple of years, additional extensions were added, and in 2005, SAML 2.0, the current version, became the OASIS standard.

SAML is about the "what" that is transmitted, not the "how" it is transmitted, which is addressed by standards like HTTP/S. There are several pieces to the SAML lexicon:

- **Identity provider (IdP)**—The entity that authenticates the identity of the user; creates, signs, encrypts, and inserts the assertion; and redirects the user, with the assertion, to the target application.

1 Maler, Eve. Minutes of 9 January 2001 Security Services TC Telecon

- **Service provider (SP)**—The entity that has the requested services, redirects the user request to the IdP for authentication, consumes and validates the assertion, and redirects the authenticated user to the application.
- **SAML assertions**—The token or cookie used to authenticate a user or the security information that is exchanged between the SP and IdP.
- **Bindings**—How the information is exchanged or messaged, for instance, HTTP POST.
- **Profiles**—The detailed SAML use cases, like web browser SSO profile.
- **Metadata**—The how-to-configure information.



1. Request target resource
2. Redirect to SSO service for authentication
3. Request user identity
4. User logs in
5. Respond with signed HTML response and request assertion consumer service
6. POST signed response to target resource
7. Supply resource to user

The dominant use case for SAML is the web browser SSO profile. A user with a user agent, typically a web browser, requests some web content which is guarded by a SAML service provider. The service provider, needing to know the identity of the requesting user, sends an authentication request to a SAML identity provider using the web browser (the user agent). Based on the IdP response or assertion, an SSO service is established and the SP responds with the requested web resource.

BIG-IP APM as a SAML SP or IdP

BIG-IP APM version 11.3 can act as either a SAML service provider or a SAML identity provider, enabling both federation and SSO within an enterprise. BIG-IP APM is a flexible, high-performance access and security solution that provides unified global access to business-critical applications and networks. By consolidating remote access, web access management, VDI, and other resources in a single policy control point—and providing easy-to-manage access policies—BIG-IP APM frees valuable IT resources and enables cost-effective scaling.

BIG-IP APM as a Service Provider

When a user initiates a request from a SAML IdP and the resources, such as an internal SharePoint site, are protected by BIG-IP APM, BIG-IP APM consumes that SAML assertion (claim) and validates its trustworthiness. This ultimately allows the user access to the resource. If the user goes directly to BIG-IP APM (as an SP) to access a resource (e.g., SharePoint), then the user will be directed to the IdP to authenticate and get an assertion. Once a user is authenticated with a SAML IdP and accesses a resource behind BIG-IP APM, he or she will not need to authenticate again.

SP initiated request

Whenever the user tries to access a particular resource behind BIG-IP APM before going to the IdP first, this is known as SP initiated access, and BIG-IP APM is the SP. Since no session yet exists for that user, the BIG-IP APM access policy is initiated. The policy will typically send a SAML authentication request to the IdP's SSO URL. The IdP authenticates the user, provides an assertion, and redirects the user back to the BIG-IP APM (the SP) via the client (often a browser). BIG-IP APM then parses and validates the assertion. To do so, the access policy will connect to the SAML user directory (the IdP). If the assertion is valid, BIG-IP APM creates the session and session variables corresponding to information inside the assertion. These session variables can be used inside the access policy to enforce different conditions. The session is marked as valid, and the user then gets access to the requested resources mapped to them.

IdP initiated request

With an IdP initiated request, the user goes directly to the IdP first to get authenticated and receive an assertion. The user is then redirected with the

assertion to BIG-IP APM for access to a resource. The IdP can set a relay state indicating where on the SP network the user should be taken.

In this scenario, the client connects to the IdP and authenticates, so a SAML assertion is created. The user is redirected to BIG-IP APM, and the IdP sends the assertion to BIG-IP APM's assertion consumer service through a browser. Since there is no existing user session between the client and BIG-IP APM, the access policy runs and the user directory is consulted to determine the authentication object and the IdP connector. This information is used to validate the assertion, while the assertion consumer service in BIG-IP APM validates the digital signature on the SAML response. BIG-IP APM populates session variables based on the assertion and typically initiates access control. Using the redirect mechanism, BIG-IP APM attempts to provide the user with access to the target resource and the request is passed to the server, assuming it is not blocked by access control.

The configuration of BIG-IP APM as a SAML SP can be customized, achieved with metadata (from the IdP), or performed using a template.

BIG-IP APM as an Identity Provider

Provided there is an SP that accepts assertions, a user can authenticate with BIG-IP APM to create an assertion. BIG-IP APM authenticates the user and displays resources. When the user clicks on an application, BIG-IP APM generates an assertion. That assertion can be passed on to the SP, which allows access to the resource without further authentication. When the user visits the SP first, the process is SP initiated; when the user goes directly to the IdP (in this case, BIG-IP APM) first to authenticate, the process is IdP initiated.

With BIG-IP APM as the IdP in scenarios with requests initiated either by the SP or the IdP, the BIG-IP APM access policy typically will provide a log in page and authenticate. When authentication is successful, a SAML resource is assigned to the session, which provides the session with two objects: the SAML SSO object and the SP connector object. The SAML SSO describes how an assertion should be created, and the SP connector describes how it should be sent to the service provider.

Specifically with an IdP initiated request, when the user goes directly to the IdP (BIG-IP APM) first to authenticate, a log in page will normally be provided, as above, and a web portal page displayed. The access policy also runs, since no BIG-IP APM session exists. The access policy displays the web portal that has one or more SAML resources, which allows the user to select the resource on a given SP. After the

selection of the resource, an SSO is used and the assertion is created. The user is redirected to the SP with the assertion. The IdP service describes how the assertion is created, the SP connector, and where to send it.

With an SP initiated request or when the user goes to the SP first and tries to access a protected resource without an appropriate assertion, the SP generates an authentication request and redirects the user to BIG-IP APM (the IdP) with a request to authenticate the user and then redirect him back with an assertion. The redirection to BIG-IP APM with the authentication request will set the issuer (the entity ID of the SP), indicating where the assertion can be sent back to.

In this instance, like the others, the access policy runs when the user is redirected to BIG-IP APM, since no session exists for that user. The access policy takes the authentication request, validates it, and creates a BIG-IP APM session. The access policy then authenticates the user. Upon success, it uses the entity ID to find a SAML SSO object and it creates an assertion. An SP connector is identified by matching the issuer in the authentication request to the SP entity ID. The SP connector will identify the SAML IdP service, and in this situation, a portal page is not created; the client is simply redirected back to the SP with the requested assertion.

If all goes well, the client is able to access to protected resource from the SP.

BIG-IP APM in a SAML Federation

SAML can be used to federate autonomous BIG-IP APM systems. This allows a user to connect to one BIG-IP device, authenticate, and transparently move to other participating BIG-IPs devices. Session replication is not part of SAML, but administrators can populate session information on participating systems. This means that BIG-IP device federation does not enable the use of a single session within the federation; it only enables information exchange among multiple members of the federation.

Each participating BIG-IP device maintains its own independent session with the client, and each has its own access policy that executes separately and independently. Participating federation members can exchange information with any other federation members outside of sessions where needed. A common configuration is to have a dedicated BIG-IP device as a primary member to which users are authenticated and that provides information to other members. This allows a number of other BIG-IP devices to work in conjunction with that primary member. The primary member is dedicated as an IdP, while the other participating members operate as SPs.

An Efficient SAML Solution

The benefits of deploying BIG-IP APM as a SAML solution certainly include better password management, fewer help desk calls, and an improved user experience, but BIG-IP APM can also add additional context to requests. For instance, it can include endpoint inspection results as attributes to inform the application of the client's security posture. In addition, IT administrators do not need to retrofit applications (e.g., .NET apps do not need a Kerberos claims plug-in). Another advantage is extensive session variable support, which allows organizations to customize each user session. BIG-IP APM can bring SAML to resources and applications with minimal back-end changes—or none. These benefits all complement the values of BIG-IP APM to the overall traffic management of an organization's IT infrastructure, which include providing strategic points of control and enabling organizations to scale, adapt, and align with changing business demands to drive business forward.

Conclusion

IT infrastructure has changed dramatically over the past few years, with many applications moving to cloud-based services. Corporate employees have also morphed into a mobile workforce that requires secure access to that infrastructure any time, from anywhere, and with any device. Bridging the identity gap between physically and logically separated services allows organizations to stay agile in this ever-changing environment and gives users the secure access they need around the clock.

BIG-IP APM version 11.3, in addition to delivering high availability and protecting organizations' critical assets, provides a SAML 2.0 solution that offers the identity bridge needed to manage access across systems.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com