WHITE PAPER

Integrating Single Sign-on Across the Cloud

By David Strom

McAfee®
An Intel Company

TABLE OF CONTENTS

McAfee®
An Intel Company

Single sign-on (SSO) isn't something new: we have had various products for more than a decade to manage a proliferation of passwords and security profiles. Indeed, many of us make use of Microsoft's Active Directory to provide SSO within the enterprise network. What is new is the explosion of Web-based software-as-a-service (SaaS) business applications and access to them from external company partners. Both of these things have made the SSO problem more complex and a lot harder to implement, since the identity boundary needs to be extended to third-party applications and users. Web-based SSO gateways now have to combine both cloud-based SaaS logins with local desktop Windows, Active Directory and other on-premises application logins for smoother federated identity integration and to enable identity management for Web applications both inside and outside the corporate firewall.

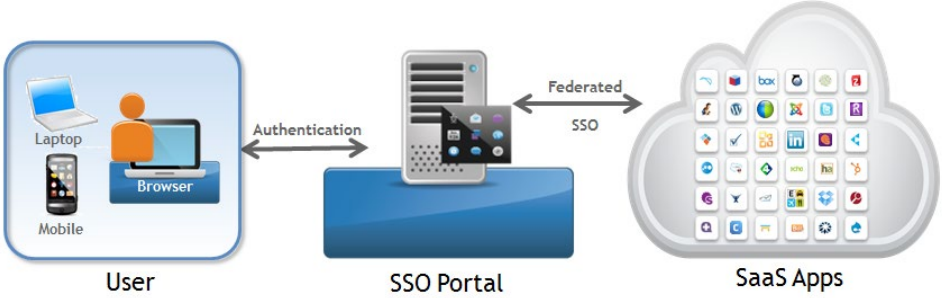
Standards for provisioning and de-provisioning have not kept pace with the growth of SaaS applications.

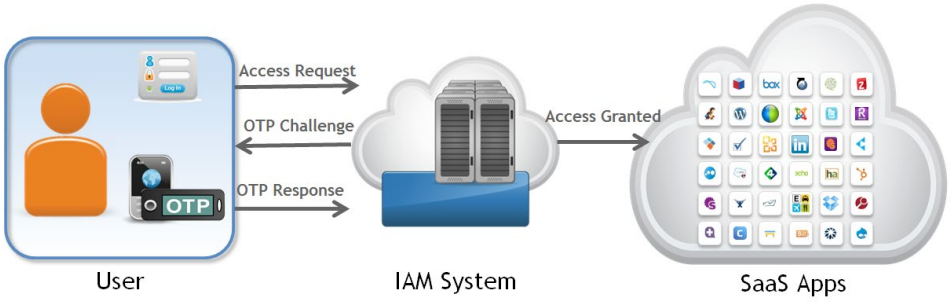
Besides this integration, a number of new standards such as *Security Assertion Markup Language* (SAML), OpenID and OAuth have made for more automated exchanges of identity information between Web applications and security gateways. These standards allow for automated sign-ons via exchanging XML-based tokens and other information securely among websites, and make configuring trusted, federated SSO between systems a lot simpler. Not every SaaS site supports all of these standards, but more are getting on board every day as a result of the popularity and reach of the SSO products. And, as the number of Web-based applications supported by enterprises continues to escalate, the problem to integrate them and manage the entire collection of identities will only gets more complex.

Unfortunately, standards for provisioning and de-provisioning have not kept pace with the growth of SaaS applications. The recently developed *Simple Cross-Domain Identity Management* (SCIM) protocol has the potential to help with this particularly complex problem, but has not yet achieved critical mass with the Service Provider community.

In this white paper, we will look at these trends, and discuss some of the issues involved with the integration and federation of identity across the cloud. We'll also look how several McAfee products, including the McAfee Web Gateway and Cloud Single Sign On, resolve these issues.

The Virtual Private Network (VPN) used to be the end goal for a typical security officer: making sure that the protection of a local network could be extended to remote users. The better VPNs offered Active Directory (AD) integration as a way to simplify the login process when users were offsite





and needed to connect to the internal network. However, having a VPN is just the beginning now of a wide series of security measures for the enterprise. Part of the problem is that often users are mixing access to cloud-based apps with access via the VPN to the central on-premises network apps, and many VPNs weren't designed for this hybrid collection of apps. Another part of the problem is that once a PC is authenticated and connected to the central network, that doesn't guarantee that it is infection-free.

Web proxies and SSO gateways come from two separate worlds, and only recently have there been solutions that attempt to combine them.

Access Control: Web and SSO Gateways

The Web Proxy/Gateway also used to be a fairly simple device that could cache frequently accessed sites and block particular URLs that were either not part of the work focus or that contained known threats. But now these proxies have to be more sophisticated and work closely with SSO gateways and the numerous SaaS applications, along with standard security apparatus such as firewalls, intrusion prevention devices and other protective measures.

Web proxies and SSO gateways come from two separate worlds, and only recently have there been solutions that attempt to combine them and federate identities across both kinds of products. As enterprises build or buy more Web-based applications, the distinction between what is found on premises and what lives in the cloud is no longer relevant. And, as they staff their projects with outside contractors, partners, and others, the difference between who is are listed in their internal staff directory and who isn't aren't becomes less important. We need better mechanisms to protect the corporate network, no matter where users are coming from and which apps they are using.

Adding to this complexity is the fact that encryption has become more widely deployed across the Web and proxies have had to get smarter about how to decrypt these pages.

Web Gateway Key Features

Here are some features to look for in a modern Web gateway:

- First, does the gateway offer **granular applications control and policy creation**? The product should easily recognize a wide variety of applications so administrators don't have to spend a lot of time figuring out how to specify them in the gateway. IT professionals want to be able to pick and choose the allowable corporate applications, and block the others.
- Next, how does the gateway **handle zero day threat detection and**

other security issues? The biggest issue for current security managers is being able to detect zero-day threats where there is no virus signature and no current behavior profile of the attack. Having this ability is a big help to screening out malware and traffic before it hits the network and infects any of its endpoints. In the past, security managers needed a variety of protection products including anti-virus, Web filtering, and anti-phishing tools to keep the bad stuff from infecting their networks and endpoints, but since these are zero day threats which have no signature, these approaches are not particularly effective. McAfee's Web Gateway and Web SaaS offering utilize a unique patented *Gateway* anti-malware engine that uses signatureless emulation of active code to detect zero hour attacks.

- Third, does the **gateway** include data loss protection (DLP) or integrate with DLP devices? Some of the web gateway vendors are working hand-in-hand with their DLP solutions for more effective security and control. For example, McAfee embeds its DLP protection in McAfee Web Gateway. Furthermore, does the gateway integrate with the SSO gateway? With McAfee Web Gateway, it does.

If IT professionals are going to deploy SSO across their organizations, the last thing they want to do is to manually provision (or terminate) each user one at a time.

SSO Key Features

Let's turn to the SSO gateways themselves. SSO products used to be either based in the cloud or on-premises, but that distinction is no longer relevant: today we need a hybrid approach that integrates logins across both environments. In fact, it is getting harder to tell the difference between the two approaches, and the best situation is to offer both on premises and cloud-based solutions, or have bits of code that reside in both places to accomplish their SSO operations. Let's look at some of the key features in a modern SSO product.

First is the **automated provisioning of new user identities**. If IT professionals are going to deploy SSO across their organizations, the last thing they want to do is to manually provision (or terminate) each user one at a time. Part of the problem is that not every SaaS vendor supports automated provisioning from every SSO product. The way most SSO products work is to connect to an internal Active Directory server or some other identity repository, grabbing and provisioning the current users with SaaS accounts using one of the identity standards such as SAML and OpenID. Ideally, a gateway should be able to initiate provisioning, which makes the bulk on-boarding process a lot easier. However, due to the lack of accepted standards, in most instances provisioning requires the target SaaS application (or service provider) to expose an API that the SSO product (or identity provider) can use for provisioning.

Another feature is the **support for just-in-time (JIT) user provisioning**. This means once the SaaS provider and the SSO vendor have exchanged certificates, users can be set up on a new SaaS-based app with a minimum of fuss and bother. One method to establish trust is to make use of an exchange of certificates. A second is to use XML-based standards along with secure Web forms to establish a trust relationship for the login. Having both methods can be quite powerful, and indeed can free users from even having to keep track of their passwords on particular SaaS-based accounts, since the SSO gateway sets everything up for them from the first time that they use each account.

Part of evaluating the automated provisioning feature in a SSO supplier is in understanding how each product recovers from mistakes that admins will make in the specifying the login process. Given the amount of information that each product requires for its automation, it is easy to make typos or small syntax errors that can take hours to figure out and correct. So the debugging information that a product supplies is critical in keeping IT pros from getting frustrated or wasting time testing SSO services.

And it isn't just automated provisioning, but **the depth of support for Active Directory**, too. Products should automatically recognize the groups of user accounts, such as network administrators. They should also do two-way synchronization of user accounts with Active Directory so that as admins add or delete users from one, their actions are matched on the other side. And they should support federated identity synchronization with outside networks, such as setting up a partner portal so that individual logins from partner organizations don't need to be manually created on a SSO system. The best situation is to use the Active Directory group identities as the basis of how a gateway configures their SSO roles and policies. McAfee has very flexible configuration rules and can set up individual apps with a particular identity repository and choose whether each app needs to have a separate two-factor authenticationprocess. McAfee also offers SSO and Web gateway integration, which offers further flexibility and ease of configuration.

One of the biggest issues with SaaS is protecting the application against unauthorized access.

Next is **how many pre-built application SSO connectors are available** from the SSO provider? The McAfee SSO solution comes with hundreds of different SSO connectors. Many vendors, including McAfee's gateways, have Web forms-based mechanisms to add new apps to their SSO gateways. This is essential because in certain cases this is the only automation method available for those applications.

However, this involves a lot of trial-and-error experimentation, so it is best to choose those vendors who have a larger collection of connectors to start with. One factor to consider is the SSO security model that's available to match up the gateway, the app, and the identity provider. By that term, we mean whether the SSO gateway employs a single method per user, per app, or per identity provider.

One of the biggest issues with SaaS is protecting the application against unauthorized access. For many, the preferred method is to employ two-factor authentication to validate a user's identity. Since multiple SaaS apps may need to be protected, a two-factor authentication system must be able to support multiple accounts. McAfee's system can also be configured to require includes a one-time password two-factor authentication solution into the end user launchpad, either with or without two-factor authentication to used to protect individual applications,to and provide the highest levels of security. This means that specific apps can be provisioned for stronger authentication methods so that each app can use a different method. Many of its competitors only allow for a single two-factor token to protect the entire user account, which is both less flexible and less secure.

Next is how **policies are set up to connect particular identity providers with particular apps**. The McAfee SSO solution comes with a large collec-

tion of identity providers including AD, LDAP, Google, OpenID, Salesforce, various SQL databases and others. One of the interesting things is how flexible and complex the product can be: admins can set up separate policies for particular apps that connect to particular identity providers. As an example, admins can restrict logins per app by IP address range, to specific mobile devices, and by day of the week and time of day.

Finally, IT pros need to **examine the SSO gateway's over-the-wire behavior**. Part of vetting any of these products is in understanding exactly what information is transmitted and whether it is encrypted across the Internet to prevent any man-in-the-middle attacks. Does the SSO gateway protect any of the identity provider's user data in its queries to authenticate the user, or does it store a local copy of any AD user information in a place that is insecure? The better SSO gateways can access multiple AD user stores, in case the route to one is down, for more redundant operations.

Part of vetting any of these products is in understanding exactly what information is transmitted and whether it is encrypted across the Internet to prevent any man-in-the-middle attacks.

Conclusion

There are many issues involved with extending the notion of identity across the cloud, from the way a Web gateway works to how SSO gateways provision user accounts. What is needed is a flexible cloud-based identity store that can keep track of logins from the central enterprise directory and augment it with logins from partners and customers as needed, along with links to both on-premises and cloud apps. The ultimate goal is being able to automate user provisioning and application connections in such a way as to authenticate the right people to run the right apps without a lot of IT overhead and manual intervention, or end user password management. We've just touched on a few of the issues that anyone looking to purchase these kinds of products, and integrate them into their existing IT infrastructure, will need to understand and evaluate for the proper security posture.

Author Bio

David Strom is a well-published author on networking and Internet topics with two books and thousands of magazine articles spanning a 25-year career. He was the founding editor-in-chief of Network Computing magazine and has managed other IT-based publications on channel, enterprise computing, enthusiast and OEM B2B topics. He can be found at david@strom.com, @dstrom on Twitter, and Strominator.com.

McAfee®
An Intel Company