SONICWALL

TECH BRIEF: MOVE TO THE CLOUD AND ACHIEVE IDENTITY FEDERATION WITH SONICWALL SMA

Abstract

Deploying SonicWall SMA, a unified secure access gateway solution, enables organizations to move to the cloud confidently while reducing total cost of ownership. SMA delivers secure access from a single URL for authenticated users using authorized devices to mission critical applications hosted in a corporate datacenter or an external public cloud service.

Introduction

For many organizations, moving to the cloud is a strategic project that involves detailed planning and step by step migration of applications. As a result, IT departments are in various stages of moving their on-prem applications to a cloud-based SaaS solution, presenting a hybrid IT environment. To provide any-time, any-device secure access to any application for hybrid IT, organizations need a centralized solution that simplifies access control components of their infrastructure.

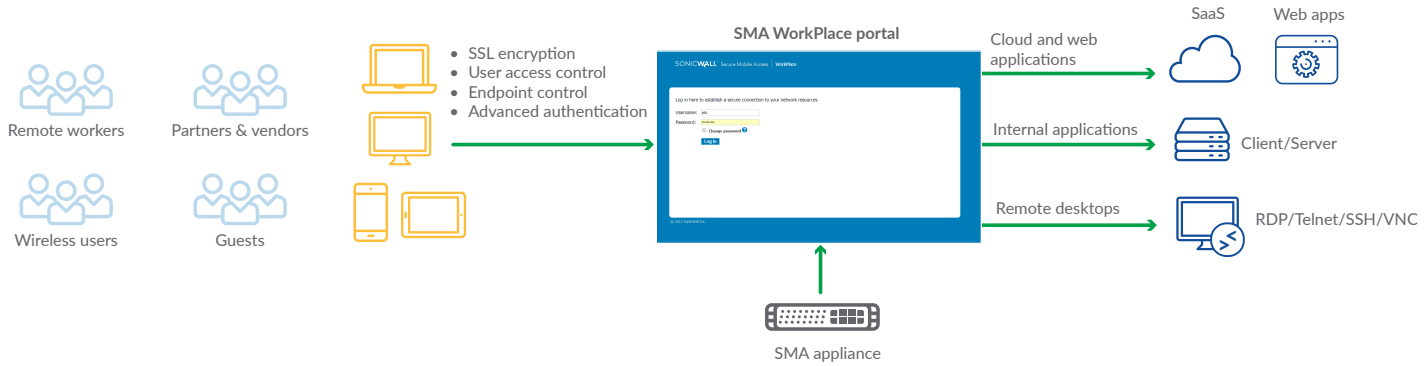
Achieving identity federation while ensuring network security

SonicWall SMA solves the key challenge of federating identities between an organizations' user directories and SAML-based identity providers (IdP). This means, every time an organization on-boards a cloud or a web application, users don't have to remember another URL and another password.

The solution proxies connection requests to a SAML-based IdP and on-premises user directories to ensure that corporate user identities are protected behind a hardened identity gateway. With this identity broker functionality as the core, SonicWall SMA delivers federated SSO initiated by both Service Providers (SPs), such as Salesforce and Office 365, and Identity Providers (IdPs), such as Ping identity and Microsoft ADFS.

Centralizing Single Sign-on (SSO) with SMA Workplace

SMA eliminates the need for multiple passwords, and can help stops bad security practices such as password reuse. SMA Workplace portal provides a centralized access portal, giving users one URL to access all mission critical applications from a standard web browser. Administrators can completely customize the portal to reflect corporate branding and deliver a consistent on-brand experience to all users. At the same time, SMA reduces total cost of ownership by consolidating the remote access infrastructure components, including SSL VPN, global load balancers, access control and endpoint control.



Unified web portal for secure access to cloud and on-prem resources

Unified web portal for secure access to cloud and on-prem resources

SMA provides secure SSO only to authorized endpoint devices that undergo enforced policy-based checks such as device type, OS version, and jailbreak status. The SMA access policy engine ensures that users can see only the authorized applications, and grants access after successful authentication. For enhanced security, administrators can seamlessly integrate the solution with leading MFA technologies.

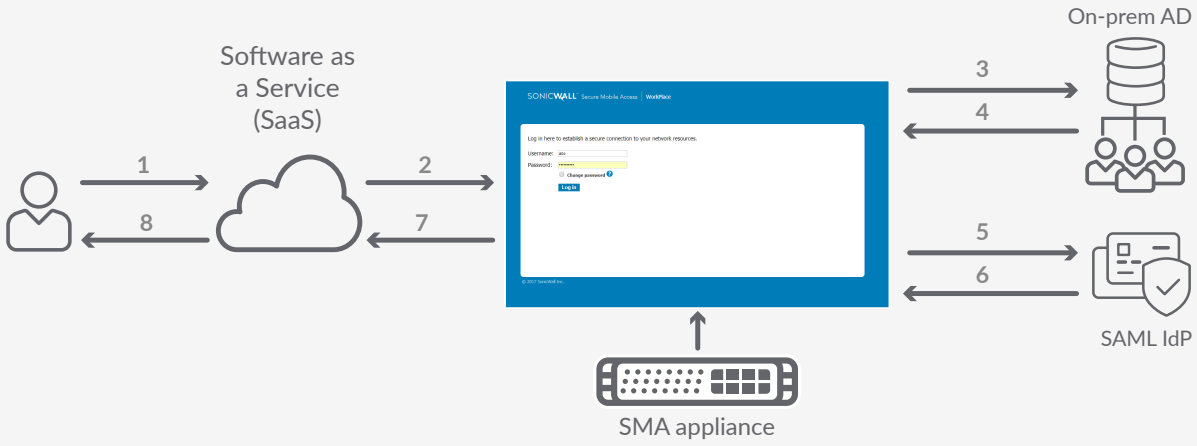
Once the user logs in successfully, the user is presented with a web user portal in the browser window, providing a single pane-of-glass-view to access any SaaS or local application. This web portal is platform agnostic, and supports all major device platforms including Windows, Mac OS, Linux, iOS and Android devices, and broad browser support across all these devices.

Use case scenarios

The diagrams below shows how SonicWall SMA achieves federation and centralizes SSO:

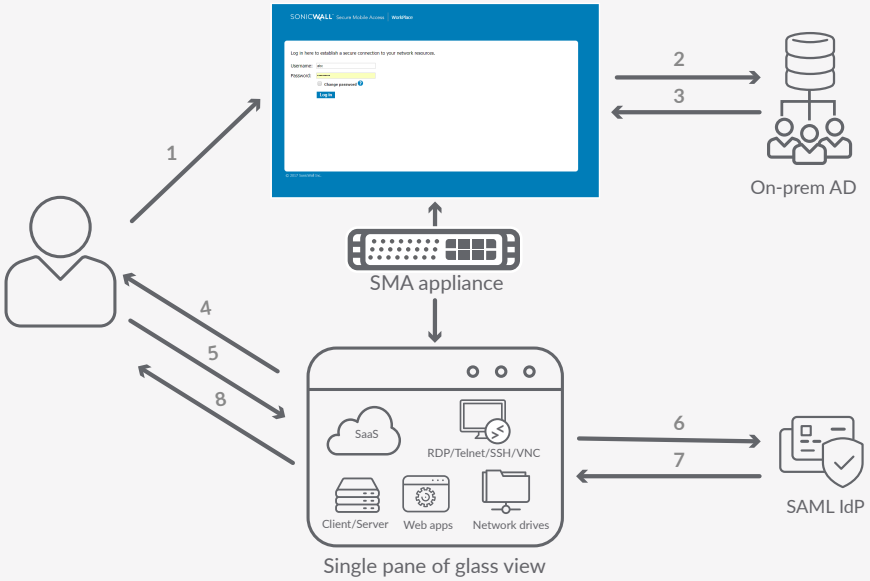
Scenario 1: Service Provider initiated SSO

1. User attempts to access a SaaS or a web application directly from a bookmark.
2. The application sends a redirect to SMA and back to user's browser, and the user is prompted for login. SMA acts as a SAML Idp proxy to obtain the SAML security token.
3. User then enters AD credentials. Organizations can configure a 2-factor authentication (2FA) or a multi-factor authentication (MFA) for added security.
4. SMA captures the AD credentials and sends redirect to the browser.
5. SMA injects the AD credentials into the SAML form.
6. The browser seamlessly authenticates the user to the SAML-based IdP.
7. IdP returns SAML security token to browser and redirects to SaaS or web application.
8. User accesses the SaaS or web application using security token from the SAML IdP.



Scenario 2: Identity Provider initiated SSO

1. User attempts to access SMA Workplace Portal and is prompted to log in.
2. User then enters AD credentials. Organizations can configure a 2-factor authentication (2FA) or a multi-factor authentication (MFA) for added security.
3. SMA captures the AD credentials and sends redirect to the browser.
4. SMA Workplace Portal presents user with a single-pane-of-glass view for all accessible applications and network resources.
5. User clicks on the link to access a particular SaaS or web application.
6. SMA sends redirect to browser and injects the AD credentials into the SAML form. The browser seamlessly authenticates the user to the SAML-based IdP.
7. IdP returns SAML security token to browser and redirects it to the SaaS or web application provider for validation.
8. SaaS or web application provider presents user with access to the SaaS or web application.



Conclusion

SonicWall SMA consolidates your remote access infrastructure, and lowers the upfront investment and total cost of ownership for your organization. A single solution provides SSL encryption, granular access control, endpoint control and advanced authentication with federated SSO. It reduces complexity in deploying and managing access security solutions. The solution offers the best of all worlds, combining enhanced user productivity with IT efficiency, cost effectiveness, security and compliance.

To learn more visit www.sonicwall.com/sma.

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 global businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
www.sonicwall.com