Array NETWORKS

SyferLock

AG Series Secure Access Gateways and SyferLock Provide Tokenless, Secure and Easy-to-Use Two-Factor and Multifactor Authentication

SyferLock Authentication Overview

SyferLock provides an innovative software-based alternative to hard tokens, smart cards and other authentication solutions. SyferLock delivers two-factor and multifactor authentication through patented software-based grids to convert static passwords or PINs into tokenless, one-time passwords/PINs (OTPs).

Increasingly, enterprises are turning to tokenless, software-based authentication to strengthen security, eliminate hardware tokens and reduce Total Cost of Ownership (TCO).

Integrated Solution Overview

Array AG Series secure access gateways address challenges faced by enterprise, service provider and public sector organizations in providing secure remote and mobile access to applications and cloud services. Available in a range of scalable, purpose-built appliances or as a virtual appliance for cloud and virtualized environments, the AG Series can support multiple communities of interest, connect users both in the office and on the go, and provide access to traditional enterprise applications as well as services running in public, private and hybrid clouds. Through interoperability with SyferLock's OTP authentication solutions, the AG Series adds an additional layer of defense against unauthorized access and misuse of data and applications.

Tokenless, Secure, Easy-to-Use Two-Factor/Multifactor Authentication

SyferLock's GridGuard is deployed as a virtual appliance in the enterprise network and integrates with the existing user registry to provide seamless user registration and authentication to SSL VPN secure access appliances such as the AG Series as well as cloud-based applications. SyferLock's GridGuard software-based authentication solutions support multiple deployment models for two-factor and multi-factor authentication.

How it Works

SyferLock's authentication solutions utilize patented software-based grids to convert static passwords or PINs into secure one-time passwords. These OTPs offer a simpler, more secure way to access information and applications while leveraging existing passwords and password infrastructure.

At login, a grid of cells is shown, each of which contains a static number or symbol in the center, and random numbers in the periphery that change with each authentication. Using the grid, the user associates their static password or PIN with the random numbers associated with the pre-selected position as their one-time password.

In the example below, a user with a static PIN of 2490 and a pre-selected corner of "top left" would input an OTP of 3347 for this login.

Interoperability with AG Series SSL VPN

Organizations that require an added layer of security for compliance with regulations such as HIPAA or PCI-DSS, for example, or that want to augment the multiple authentication methods offered by Array's AG Series secure access gateways, can utilize SyferLock's custom integration to add GridGuard two-factor/multifactor authentication as an additional layer of security. In deployment, the AG Series redirects inbound traffic to the SyferLock GridGuard virtual appliance for authentication before allowing the user to access the appropriate network resources.

Figure 1: GridGuard Example

AG Series Benefits

> Anytime, anywhere browser-based secure remote access enables increased productivity for employees, partners, tenants, customers, contractors and guests

> Simple scalable and secure remote desktop that enables use of PCs and virtual desktops from any device in any location

> Secure mobile access for individual native and Web applications for supporting Bring Your Own Device (BYOD) or secure access from managed smartphones and tablets

SyferLock Benefits

> Superior security – strongest browser-based authentication solution on the market

> Eliminates or mitigates a wide variety of attacks, such as key logging, shoulder surfing, brute force and dictionary attacks, and more

> Deviceless and software-based solutions substantially lower TCO

> Leverages current password infrastructure
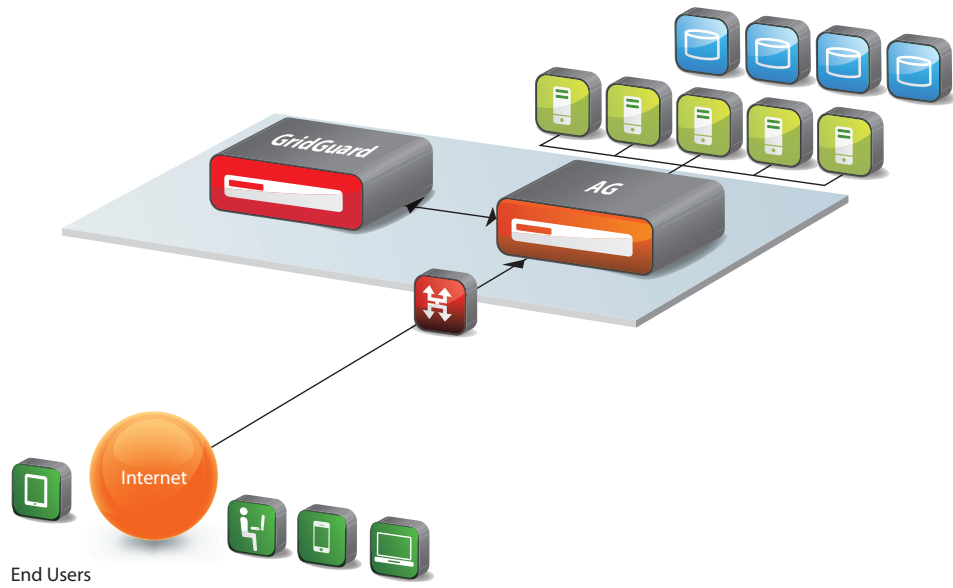
> Scalable and deployable in a high-availability cluster

Figure 2: Deployment Example