SRA One-Time Passwords

Enable two-factor authentication to thwart keylogger attacks

Introduction

One of the many enhanced features found in Dell™ SonicWALL™ Secure Remote Access (SRA) solutions is end-user authentication, either through an internal database or through integration with one of many dynamic authentication methods, including Dell Quest Defender, Active Directory, RADIUS and LDAP. The SRA solutions notify users prior to password expiration, and can change passwords before or after expiration, even when part of a Microsoft® Active Directory domain. Dell SonicWALL SRA solutions offer support for Active Directory nested groups, as well as TLS/SSL support for LDAP/AD. In addition, all appliances offer tokenless two-factor authentication as part of the standard feature set.

The problem with standard passwords

Proper security protocol dictates a rigorous password regimen, which imposes a policy of difficult passwords on each end user. Passwords should be difficult to guess, have both alpha and numeric characters, and be changed on a regular basis. Furthermore, users should never write down or share passwords. Proper password policy prevents the occurrence of illegal access through stolen passwords in most cases, but in reality, it is hard to enforce. End users want the easiest path, and tend to be resistant to difficult passwords. They create passwords that are easy to remember. They write them down. They share them with their co-workers. This defeats the whole purpose of the password security policy.

Using a password alone, or single-factor authentication, is adequate in light security environments where data is not sensitive. However, when there is a more stringent need for protection, security demands the use of two factors. The most efficient second factor is a one-time password, which goes beyond simply serving as a second authentication factor, but also mitigates some of the drawbacks of the memorized password. One-time use prevents criminals from stealing, keylogging or sniffing these passwords.

Because a new password is generated for every login, if an attacker keylogs, steals or sniffs that password, it would be useless.

Tokenless solution

There is no question that two-factor authentication should be the solution of choice for remote environments requiring high levels of security. By definition, two-factor authentication requires two separate authenticators. The Dell SonicWALL One-Time Password (OTP) solution calls for a standard network password, and a one-time password generated by the server. Some other two-factor authentication solutions use a network password and a physical hardware token that generates the one-time password.

One-time passwords

OTP is an important feature offering on the Dell SonicWALL SRA series. This feature provides an enhanced level of user authentication, and is especially useful in protecting against the threats caused by keylogger programs. The OTP feature, a variation of two-factor authentication, generates a one-time password, which the user enters along with their username and standard network password. Because the SSL VPN appliance generates a new password for every login, if an attacker keylogs, steals or sniffs that password, it would be useless. Users enter the one-time password into the Virtual Office, NetExtender or Mobile Connect login interface.

How does the user get the one-time password?

After entering in their regular user name and password, the SSL VPN appliance dynamically generates a one-time password. Users will receive an email at a predefined personal email address or a text message to mobile phone, which will contain the temporary one-time password generated by the SSL VPN appliance. No additional hardware token or card is required.

SSL VPN standard feature set

Two-factor authentication typically comes with a separate solution, which requires separate installation and costs extra. With Dell SonicWALL SSL VPN, the tokenless two-factor authentication capability comes included as a standard part of the feature set with all Dell SonicWALL SSL VPN appliances.

Dell Quest Defender

Dell Quest Defender enhances security by enabling two-factor authentication and multi-factor authentication to network, Web and applications-based resources. Defender uses the scalability and security of Active Directory for identity storage and management, enabling administrators to use their existing skill set to manage two-factor authentication and eliminating the costs and time involved in setting up and maintaining proprietary databases.

For More Information

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

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

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.