

Secure the access to your SonicWALL environment

The combined technologies of SonicWALL SSL-VPNs and VASCO's Strong Authentication can now provide an easy-to-use remote access with increased security.



THE PROBLEM

VASCO's Strong Authentication addresses the gap caused by using insecure static passwords for the authentication of users that require remote access to networks and applications via SonicWALL SSL-VPN.

SOLUTION

VASCO DIGIPASS® authenticators allow employees and partners to gain access to sensitive information and internal applications from a remote location without compromising security or user convenience. VASCO provides Two-Factor Strong Authentication based on One-Time Password technology to protect user login and insures only authenticated users gain access.

By integrating DIGIPASS Strong Authentication with SonicWALL SSL-VPN solutions, the customer receives an easy-to-deploy remote access solution with increased security. All access options incorporate Two-Factor Authentication from VASCO. The SonicWALL SSL-VPN and VASCO technology combination satisfies security and infrastructure requirements while providing a simplified end user experience.

HOW IT WORKS

The SonicWALL SSL-VPNs communicate with VASCO's VACMAN® Middleware backend software through RADIUS protocol. Users are prompted for their VASCO DIGIPASS One-Time Password when they attempt to access the network via the SonicWALL SSL-VPNs. Upon successful user authentication, SonicWALL SSL-VPNs provide session encryption and highly granular access control.



BENEFITS

High Security

- High level of security with granular access control
- Comprehensive audit system
- Secure access from anywhere, at any time
- Compatible with most firewalls

Seamless Integration

- No complex programming or lengthy installations for network administrators
- Software-based backend platform leverages existing IT infrastructure

Scalability

- Add more users and/or applications as required without an infrastructure overhaul

Low Total Cost of Ownership

- Significant savings in user administration and support costs
- No new servers or appliances required to implement strong authentication
- Replace deployment of IPSec client management