

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

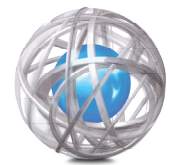
- No complex programming or lengthy installations for network administrators
- Software-based backend platform leverages existing IT infrastructure

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



SSL-VPN	Web	PKI	SSO
AEP Networks	AEP Networks	Charismathics gmbh	Citrix
Alcatel Lucent	Check Point Software Inc.	Check Point (Pointsec)	IBM Corporation
Array Networks	Cisco Systems, Inc.	Cryptomathic	Microsoft Corporation
Avaya	Citrix	Entrust	Novell
Celestix Networks, Inc.	Computer Associates (Netegrity)	Logos	Oracle
Check Point Software Inc.	CyberSafe Ltd.	McAfee Inc. (Safeboot)	
Cisco Systems, Inc.	HP	Microsoft Corporation	
Citrix	IBM Corporation	Oracle	
CyberSafe Ltd.	Juniper Networks	Thales e-Security	
F5 Networks	Microsoft Corporation	Utimaco Safeware AG	
Fortinet, Inc.	NETASQ		
HP	Novell		
IBM Corporation	Oracle		
Juniper Networks	SonicWALL		
Microsoft Corporation (Whale Communications)	Stonesoft		
NETASQ	Thales e-Security		
Network Engines	WatchGuard		
Nomadix			
Nortel Networks Corporation			
Novell			
Oracle			
SafeNet			
SonicWALL			
Stonesoft			
Thales e-Security			
WatchGuard			



DIGIPASS BY VASCO

For more information go to www.vasco.com or contact your nearest VASCO sales office.

About VASCO

VASCO designs, develops, markets and supports patented DIGIPASS®, DIGIPASS PLUS®, VACMAN®, IDENTIKEY® and aXs GUARD® authentication products for the financial world, remote access, e-business and e-commerce. With tens of millions of products sold, VASCO has established itself as the world leader in Strong User Authentication for e-Banking and Enterprise Security for blue-chip corporations and governments worldwide.

www.vasco.com

BRUSSELS (Europe)
phone: +32.2.609.97.00
email: info-europe@vasco.com

BOSTON (North America)
phone: +1.508.366.3400
email: info-usa@vasco.com

SYDNEY (Pacific)
phone: +61.2.8061.3700
email: info-australia@vasco.com

SINGAPORE (Asia)
phone: +65.6323.0906
email: info-asia@vasco.com