

www.securecomputing.com



Secure Computing has been solving the most difficult network and application security challenges for over 20 years. We help our customers create trusted environments both inside and outside their organizations.

Secure Computing Corporation

Corporate Headquarters

4810 Harwood Road
San Jose, CA 95124 USA
Tel +1.800.379.4944
Tel +1.408.979.6100
Fax +1.408.979.6501

European Headquarters

East Wing, Piper House
Hatch Lane
Windsor SL4 3QP UK
Tel +44.1753.410900
Fax +44.1753.410901

Asia/Pac Headquarters

1604-5 MLC Tower
248 Queen's East Road
Wan Chai Hong Kong
Tel +852.2520.2422
Fax +852.2587.1333

Japan Headquarters

Level 15 JT Bldg.
2-2-1 Toranomman Minato-Ku
Tokyo 105-0001 Japan
Tel +81.3.5114.8224
Fax +81.3.5114.8226

SFPB-CI-01-B

SmartFilter products and Cisco solutions

SmartFilter products and Cisco solutions

Secure Computing's SmartFilter[®] products enable organizations to understand and monitor their Internet use, while taking effective steps to provide appropriate control over outbound Web access. Tightly integrated with Cisco solutions, SmartFilter products easily complement your existing network infrastructure.

The SmartFilter filtering line includes:

- SmartFilter: On-Box[™] filtering solution for enterprises of all sizes. SmartFilter offers fast performance with leading filtering speeds, and cost savings with no additional hardware requirements.
- Bess[®]: The #1 Web filtering application for education installed in over 40% of US schools and libraries. Offers custom education categories.

Cisco PIX

Bess and SmartFilter's tight integration enables Cisco PIX (running v6.2 or later) to take complete advantage of the industry's #1-rated Internet filtering database and robust features.

Cisco Routers

Bess' tight integration with Cisco Routers (running Cisco IOS Firewall v12.2(15)T or later) provides an easy-to-use, cost-effective filtering solution.

Cisco Content Engine

SmartFilter On-Box filtering is pre-installed and integrated into ACNS 4.1.x Cisco Content Engine and later. The SmartFilter/Content Engine filtering solution eliminates the need for additional servers and is a simple and cost effective way for organizations to filter content.

For customers who wish to run filtering in an off-box configuration, Bess also integrates with the Cisco Content Engine (running ACNS v4.1 or later).

Cisco Content Engine Network Module

SmartFilter is available as a pre-installed option on the router-integrated Content Engine Network Module.

For customers who wish to run filtering in an off-box configuration, Bess also integrates with the Cisco Content Engine Network module (running ACNS v4.1 or later).

Want more information?

For more information or to request a 30-day evaluation of any of our filtering products, please go to:

www.securecomputing.com/cisco.

SafeWord RemoteAccess,
Cisco compatible

Quick Glance Sheet

Eliminate the password risk

- Positively identifies Cisco VPN users
- Generates a new token-generated passcode every time you log in
- Integrates seamlessly with Microsoft Active Directory
- Delivers fast, easy installation: runs on existing servers
- Provides streamlined management and deployment

SafeWord RemoteAccess protects:

- Cisco VPNs and RADIUS devices
- Many Citrix MetaFrame applications
- Outlook Web Access

Positively identify remote users

SafeWord RemoteAccess, Cisco compatible, provides a complete strong authentication solution specifically designed to protect remote user access to Cisco VPNs, routers, and firewalls. SafeWord® RemoteAccess™ also protects Citrix® applications and Outlook Web Access.

With tight integration and simplified management through Active Directory, and with tokens that generate new passcodes with every user login, SafeWord RemoteAccess lets you easily and cost-effectively eliminate the password risk.

Use strong authentication to eliminate weak password security

Increasingly, users are accessing networks and applications remotely from around the world, and the most common way to identify these users is with only a password. But passwords can readily be hacked using a wide variety of attacks. In fact, industry experts estimate that 35 percent of corporate network passwords can be hacked within five minutes.

SafeWord RemoteAccess provides token-generated passcodes that significantly reduce these risks. Each user is assigned a token that can generate millions of unique codes based on an internal secret key. To log into your Cisco VPN or other resource, the user simply pushes a button on the token to generate the next one-time code, then enters this code along with a short memorized PIN. The SafeWord authentication server verifies each passcode, allowing access only to users with valid codes and PINs. After being used once, a one-time passcode is then useless, eliminating the risk of outsiders stealing, copying, or reusing passwords.



Simple management without redundant user accounts

SafeWord RemoteAccess installs rapidly and can be run on servers you already have in your network. It's managed entirely through a plug-in to the Microsoft Management Console (MMC), allowing you to easily assign tokens to your remote users, manage user PINs, and more. Where other authentication systems may require extensive training, additional hardware, and complex configuration, SafeWord RemoteAccess can be set up in minutes.



Installing SafeWord RemoteAccess is quick and easy.

Requirements

SafeWord RemoteAccess protects Cisco VPNs, routers, firewalls, other RADIUS devices, and is compatible with Cisco ACS. It also protects Citrix MetaFrame applications and Outlook Web Access. SafeWord RemoteAccess requires that users be managed through Active Directory, and its components can be installed on the Active Directory domain controller and other servers already in your network.

SafeWord server requirements:

- Can run on existing hardware used for Active Directory
- Windows 2000 or 2003 domain controller
- Active Directory populated with remote users
- 256 MB RAM minimum; 512 MB or above for configuring the Web Agents
- 300 MB disk space minimum; 3 GB disk space recommended

Want more information?

For more information or to request an evaluation, please go to: www.safeword.com/cisco.



SafeWord RemoteAccess 2.0 has been tested in accordance with interoperability criteria set by Cisco Systems, Inc. and is compatible with Cisco VPN 3005 Concentrator v3.6, Cisco PIX 520 v6.2(3), and Cisco Secure ACS v3.2.3. For full disclaimer, see SafeWord product documentation or visit www.safeword.com/cisco.