product information

Ascend

Secure Access Firewall



Don't leave your network unprotected. Safeguard your company's valuable information assets with Secure Access Firewall, Ascend's integrated security solution.

Remote Access ▾ Internet/Intranet Access ▾ Corporate LAN

Ascend's Secure Access™ Firewall integrates state-of-the art dynamic firewall technology with Ascend's Pipeline® and MAX™ products to deliver a secure and cost-effective networking solution. Most corporate networks are only secured at the corporate LAN or not at all, leaving your company's assets vulnerable to unauthorized intruders. Because the Secure Access Firewall is integrated with Ascend's networking products, your network is protected at the corporate site, remote office and telecommuter's home office.

Secure Access Manager is a powerful Wind0ws-based application program that provides network managers with enterprise-wide control over configuring and managing Secure Access Firewalls from a central site. Network managers can point and click to select the firewall options needed for securing their network. By centralizing control, corporations reduce ongoing operating expense and simplify security management.

Secure Access Firewall and Secure Access Manager, as part of Ascend's comprehensive network security architecture, deliver an unparalleled solution for protecting your sensitive corporate data.

ASCEND

Networking Solutions with Advanced Built-in Security

Firewall and router are fully integrated into a cost-effective, single product solution

Secure Access Firewall eliminates the cost and complexity involved with purchasing, managing and maintaining stand-alone security products. It protects your company's information assets against unauthorized access at the corporate network, through the Internet and from remote locations.

- Next generation security technology (dynamic firewall)
- Application level firewall security (TFTP, FTP, Telnet)
- Extensive surveillance monitoring and logging
- Control and management of incoming/outgoing traffic
- Transparent operation for authorized users
- Available as a software option on the Pipeline 50, Pipeline 75, Pipeline 130, MAX 200Plus, MAX 1800, MAX 2000, MAX 4000, MAX 4002 and MAX 4004

Dynamic firewall technology restricts network access from unauthorized users

The dynamic firewall technology within Secure Access Firewall is a bullet-proof security system designed to regulate network access by opening communication ports only to authorized users. Dynamic rules can be written as needed to manage changing network traffic.

- Dynamically generates firewall rules for network access
- Adapts to changing network activity allowing for precise traffic control
- Opens only required ports for duration of a user session while keeping unused ports closed
- Closes ports at the termination of a session
- Applications not expressly permitted are denied

Secure Access Manager easily configures and manages your firewall from the central site

Secure Access Manager gives network administrators granular control over the security functions of the entire network directly from the central site. Through this Windows-based application, network administrators can configure the Secure Access Firewall(s) off-line and download the configuration to remote locations.

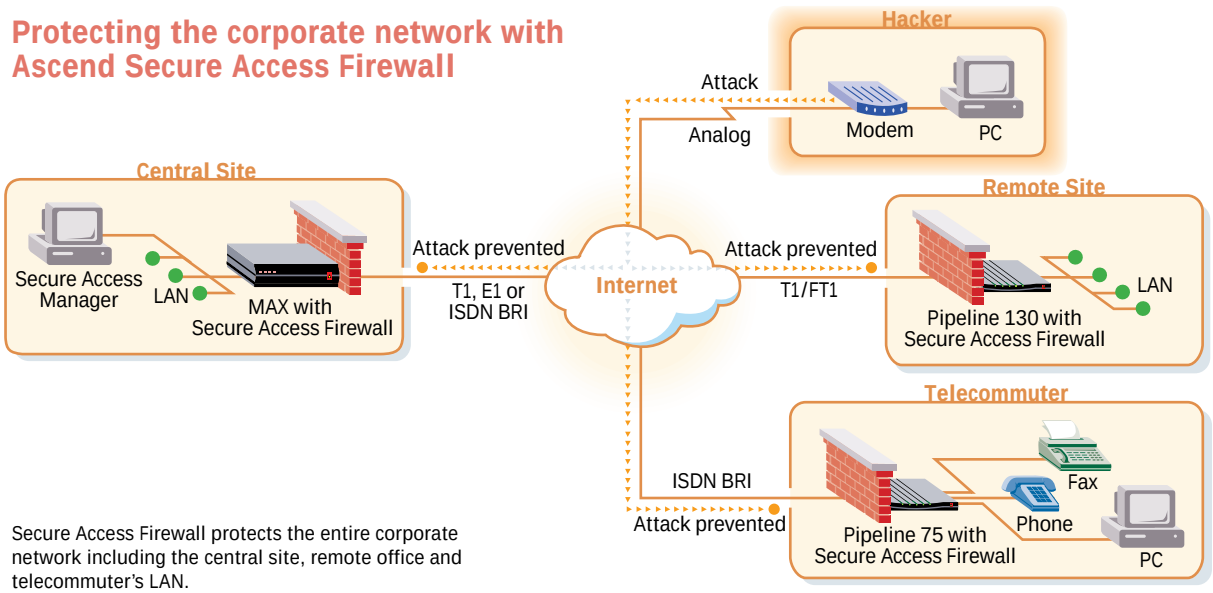
- GUI with point and click configurator
- Ability to select exactly what should be monitored and controlled
- Runs under Windows 3.X , Windows 95 and Windows NT

Surveillance features safeguard network by monitoring and recording network activity

The activity and access surveillance features in Secure Access Manager monitor and record all attempted break-ins to the network whether they occur directly at the corporate site or from a remote location. Access is managed by controlling incoming and outgoing data, looking for unsecure connections or information and by preventing unauthorized users from logging onto internal systems.

- Syslog is used to log surveillance reports at a central site
- Tracking at any level of detail from high-level session summaries down to binary packet contents
- Provides audit trail of would-be intruders
- Highly selective to avoid clutter and false alarms
- Rejected traffic logs include reason for service denial

Protecting the corporate network with Ascend Secure Access Firewall



Secure Access Firewall protects the entire corporate network including the central site, remote office and telecommuter's LAN.

Comparing Static Filtering to Secure Access Firewall

Secure Access fortifies standard security features to provide an iron-clad security architecture

Ascend's remote networking products have security features that, when integrated with Secure Access Firewall, provide a comprehensive security solution. Standard security features complement Ascend Secure Access to provide a more complete security solution.

- RADIUS and TACACS+ (on all MAX family products)
- Authentication using PAP, CHAP and Calling Line ID
- Token-based security including support for multiple vendors' products
- Automatic callback ensures calls are originated from authorized locations
- Telnet password
- Password protected terminal server access (on all MAX family products)
- UNIX password authentication
- Data/call/generic filtering

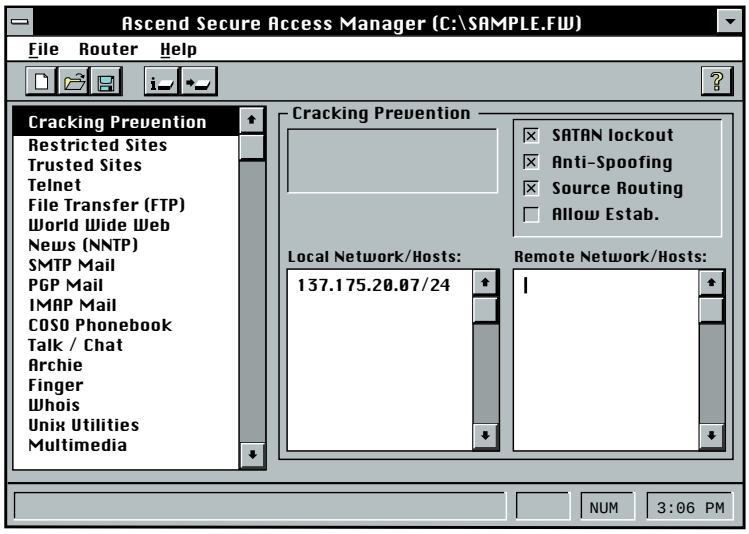
Transparently protects your network without impeding performance

Secure Access Firewall features authenticate users when they initially log into the network. After their identity has been validated, users are free to access network applications without interruption.

- Initial authentication is valid for duration of session
- Transparent to Internet applications (Telnet, FTP, WWW) as permitted by network administrators
- No client or server application modifications required
- Protects all types of TCP/IP servers

Many existing firewall products are based on a static packet filtering technology that provide only limited protection for your company's network against only novice hackers. For example, static packet filtering is limited to filtering incoming and outgoing traffic based solely on source and destination IP address. Static packet filtering limits your control and potentially places your network at risk by keeping all the high numbered (1024-65535) ports open or all of them closed. If all ports are open, the intruders can break-in to your network. If all ports are closed, even authorized users are prevented from entering the network.

In contrast, Secure Access Firewall gives you more granular control over users entering the network. It uses state-of the-art technology to create dynamic rules and adapt them to changing network traffic. These rules can be modified to accept or reject conditions depending on your specifications (applications, protocols, network addresses, ports, session state, direction, etc.). Once a session has been initiated, Ascend's firewall monitors requests to open ports between terminating points. It opens only designated ports and keeps all other ports closed. When the session has ended, the ports are immediately closed, eliminating the potential for hackers to infiltrate the network and your company's sensitive data.



Secure Access Manager

Secure Access Manager simplifies configuring all Secure Access Firewalls from a central site using Windows-based software. Network administration can handle configurations off line and download them to remote locations at a later date.

Specifications

Granularity of Secure Access Firewall	Network addresses, host names, UDP, TCP, ICMP, source/destination ports Direction: send, receive TCP session "state": syn, ack, rst, estab, fin
Application Firewall	TFTP, FTP, Telnet, WWW NNTP, SMTP, Ping POP mail, talk/chat, Real Audio, archie, finger Whois, UNIX utilities, Secure Shell, X.11, UUCP, LAN manager, time services, cracking prevention (SATAN, source routing, anti-spoofing), restricted sites, trusted sites, SNMP
Secure Access Manager	Windows 3.X, Windows '95 and Windows NT Surveillance monitoring and logging
Standard Security	PAP, CHAP, Callback, Token card, CLID, RADIUS and TACACS+ (for MAX products), local and UNIX password

Ascend's Networking with Integrated Security

Ascend Secure Access is available on the following products:

MAX™ family	MAX 200Plus, MAX 1800, MAX 2000, MAX 4000, MAX 4002 and MAX 4004
Pipeline® family	Pipeline 50, Pipeline 75 and Pipeline 130

Ascend's Remote Networking Products

MAX™ Family

Designed specifically for remote access server applications. Supports ISDN BRI, ISDN PRI, T1/E1 and Ethernet on the base unit.* Allows simultaneous calls from ISDN BRI, frame relay and/or modem users over ISDN PRI, channelized T1/E1, or ISDN BRI lines.

Pipeline® Family

Pipeline products are designed to connect users in small or home offices to backbone networks and/or the Internet. Pipeline models support Ethernet to ISDN, Switched 56 or Leased 56 services, and Ethernet to 56 Kbits/s or 64 Kbits/s frame relay services.*

Multiband™ Family

Multiband bandwidth-on-demand controllers are designed primarily for videoconferencing applications and let users dial-up bandwidth in increments of 56/64 Kbits/s up to 4 Mbits/s, using all types of digital access lines*—Switched 56, T1/E1, ISDN BRI, ISDN PRI and network carrier services.

* Depending on model and configuration

Ascend Communications, Inc.

Worldwide and North American Headquarters
1275 Harbor Bay Parkway
Alameda, CA 94502
United States
Tel: 510.769.6001
Fax: 510.814.2300
E-mail: info@ascend.com
Toll Free: 800.621.9578
Fax Server: 415.688.4343
Web Site: http://www.ascend.com

European Headquarters
Rosemount House
Rosemount Avenue
West Byfleet
Surrey KT14 6NP
United Kingdom
Tel: +44 (0) 1932.350.115
Fax: +44 (0) 1932.350.199

Asia-Pacific Headquarters
Level 14 Shinjuku Daiichi Seimei Bldg.
2-7-1 Nishi-Shinjuku
Shinjuku-ku, Tokyo 163-07
Japan
Tel: 81.3.5325.7397
Fax: 81.3.5325.7399
Web Site: http://www.ascend.co.jp

Ascend Communications, Inc. (NASDAQ: ASND) is a leading, worldwide provider of remote networking solutions for corporate central sites, Internet Service Provider points of presence, remote offices, mobile workers and telecommuters. Ascend develops, manufactures, markets, sells and supports products with bandwidth on demand to extend existing corporate networks for applications such as remote LAN access, Internet access, telecommuting, SOHO connectivity and videoconferencing/multimedia access. Detailed information on Ascend products, news announcements, seminars, service and support is available on Ascend's home page at the World Wide Web site http://www.ascend.com.

Ascend markets the MAX, Pipeline, Multiband and Secure Access families of products. Ascend products are available in more than 30 countries worldwide.

MAX™, Multiband™, Pipeline® and Secure Access™ are trademarks of Ascend Communications, Inc. Other trade names mentioned in this publication belong to their respective owners.

Specifications are subject to change without notice.

© Copyright 1996
Ascend Communications, Inc.

01-23

ISO 9001
REGISTERED

ASCEND Remote Networking Solutions That Work.™