Ascend

OVERVIEW SUMMARY

Secure Access [Version 2.0]

Product Positioning

Secure Access™ 2.0, a component of Ascend's SecureConnect™ security strategy, is an ideal choice for companies who want to use the Internet as a secure Intranet. The combination of firewalls and authentication/encryption in one package offers rock solid protection of the LAN behind the firewall in addition to providing data integrity, privacy and data origin authentication on every packet. In other words, the combination of firewalls, encryption and authentication denies inbound traffic from all but trusted users while allowing selected outbound traffic with complete privacy.

Secure Access is a critical security component in IP-based environments ranging from large, private WANs to local dial up connections for extremely security-conscious customers.

Product Overview

Secure Access 2.0 adds IPSec encryption and authentication capability to Ascend Secure Access Firewalls on the Pipeline® (50/75/85/130 (Authentication Headers)/220) platforms, providing scalable, secure IP connections for users, corporations and ISPs. A new PC product, Secure Access Personal Edition for Windows 95 and NT, is also now available. Secure Access can be used to encrypt and authenticate, on a packet-by-packet basis, today's VPN protocols, thereby making them safe for unsecure channels such as the Internet. Also, for all IP environments, Secure Access can be used to create encrypted, authenticated IP tunneling. Because Secure Access is based upon standards, Secure Access works with other IPSec-compliant equipment.

Target Applications

- *Multi-office Corporation* – Companies can now use the Internet for encrypted, virtual private networking.
- *IPSec Client to a Gateway* – Remote users (can be mobile) can encrypt traffic across the Internet while maintaining firewall protection.
- *Secured Electronic Commerce* – Trading partners can use encryption and authentication to secure all traffic between their respective sites.

ASCEND

Features

Feature	Description/Benefit
Encryption Encapsulating Security Payload (ESP): • 40- and 56-bit DES-CBC • 168-bit 3DES-CBC	Provides confidentiality by obscuring data in IP datagrams so it can be used only by the intended parties. Ascend provides two encryption algorithms—Data Encryption Standard (DES) and triple-Data Encryption Standard (3DES)—used to obscure traffic from would-be attackers. DES is considered very secure. End points share secret keys; one for transmit and another for receive.
Encapsulation Modes	• *Transport mode:* Encapsulates the upper-layer protocol (such as TCP) and uses a cleartext IP header. Used primarily in client-to-client or the client side of client to gateway encryption. • *Tunnel mode*: Secure IP Tunneling; encapsulates the entire IP datagram and wraps it with another header. It obscures IP addresses behind gateways, preventing some traffic analysis attacks.
Authentication Authentication Headers: • 96-bit MD5 • 96-bit SHA-1	It provides integrity and validates origin of data on a packet level. And it protects both the IP datagram payload and its headers. Authentication Headers can be used with encryption if confidentiality is also needed.
Multiple Encryption/Authentication Combinations	Each encryption (DES, 3DES) and authentication (MD5, SHA-1) type can be used individually or in combination.
Firewall Integration	Ascend uses Secure Access Firewall to simultaneously allow, deny, encrypt, decrypt and authenticate individual packets. It is used to protect a LAN from outside intruders while simultaneously allowing "friendly" traffic into a site.
Graphical User Interface	The GUI interface allows simple and quick setup of IP encrypted tunnels and the firewalls residing at each end of the tunnels. This also allows granular control of overall security policy.

Frequently Asked Questions

1. *What is Ascend Secure Access Version 2.0?*

   Ascend Secure Access Version 2.0 is a dynamic firewall combined with IPSec encryption. Part of Ascend's SecureConnect family of products, Secure Access 2.0 allows companies to secure all points on their remote network and set up encrypted VPNs.

2. *What is SecureConnect?*

   SecureConnect is Ascend's family of security products. These products provide a complete solution for setting up and using secure sessions across the Internet. They provide companies with the industry's most robust solution available for safeguarding their information. The products work hand-in-glove with Ascend's MAX and Pipeline products to provide affordable and state-of-the art security to networks of any size. The SecureConnect family of products includes:

   - Secure Access Firewall and Encryption is NCSA-certified and offers stateful inspection-based dynamic firewall technology. In addition, it offers extensive encryption capabilities which allows users to conduct secure sessions over the Internet.
   - Ascend Access Control™, which extends the industry-standard RADIUS server to include numerous authentication, identification, authorization and accounting functions enhancements.

3. *How do Secure Access Firewall and Encryption work together?*

   With Secure Access products, companies can establish robust firewall protection for central sites and remote locations as well as individual PCs. These rules also can allow only encrypted in-bound sessions, thereby limiting traffic through the firewall to specific tunnel endpoints.

4. *Which products support the encryption capabilities in Secure Access?*

   SecureConnect Phase I is currently available in Ascend's Pipeline 50/75/85/130 (Authentication Header)/220 units. In Phase II, SecureConnect will be available on Ascend's MAX products.

5. *How is an encrypted tunnel set up?*

   An encrypted tunnel is a bundle of up to four security associations.

6. *What forms of encryption does Secure Access support?*

   Secure Access supports the AH-MD5 (keyed MD5, RFC 1828) and AH-SHA-1 (keyed SHA, RFC 1852) authentication transforms, as well as the ESP-DES-CBC (RFC 1829) and ESP-3DES-CBC (triple DES, RFC 1851) encryption transforms.

7. *What is the relationship between IPSec and protocols such as ATMP, PPTP, L2F and L2TP?*

   IPSec can tunnel with IP much like other protocols available, except that it has the additional benefit of obscuring data as well as authenticating and verifying packets. Tunneling protocols add the ability to tunnel non-IP protocols within IP, but they do not include encryption. In fact, L2TP prescribes IPSec as its security mechanism. Importantly, IPSec can be used to encrypt other tunneling protocols.

Competitive Information

	Ascend	Cisco	Livingston	Shiva	3Com	Bay Networks
IPSec support	Full IPSec support	Yes, in PIX only	None	None	None	Authentication only (no encryption)
Encryption	40-bit DES, 56-bit DES, 168-bit Triple DES	IPSec in PIX, proprietary DES implementation in 25xx	None	None	None	None
PC client Encryption	PC client with firewall	None (Cisco recommends third party product)	None	None	None	None
GUI	Yes	Yes	PMconsole, GUI for Windows and UNIX	None	Menu (DOS-like)	None
Mobile user support	Yes	None	None	None	None	None
Radius-based Web Authentication	Yes, complete user-by-user dynamic firewalls based on WWW authentication	None	Static filters only	None	Static filters only	None
Integrated firewall	Integrated into Pipeline, DSLPipe, MAX and MAX TNT™	Only via PIX; still must add a router.	Static packet filtering only	None	Packet filtering only (stateful for FTP)	None
Cracking prevention	Yes	Yes	None	None	None	None
Custom firewalls	Yes	None	None	None	None	None

Product Name, Models and Pricing

Secure Access Model # (pre-installed)	Secure Access Model # (add-on to exiting units)	Description	Price	Availability (firewall available now)
ASA-PC-CD	Not Applicable	Secure Access PC Client for Windows 95, NT – Firewall & Encryption	$99	60 days
P50-1UBRI-ASA P50-1SBRI-ASA	P50-SWUP-ASA	Secure Access for Pipeline 50 – Firewall & Encryption	$500	30 days
P75-1UBRI-ASA P75-1SBRI-ASA	P75-SWUP-ASA	Secure Access for Pipeline 75 – Firewall & Encryption	$500	30 days
P85-1UBRI-ASA P85-1SBRI-ASA	P85-SWUP-ASA	Secure Access for Pipeline 85 – Firewall & Encryption	$500	30 days
P130-L56-ASA P130-FT1-ASA P130-SBRI-V35-ASA P130-LS56-2N-ASA	P130-SWUP-ASA	Secure Access for Pipeline 130 – Firewalls and AH only	$1000	30 days
DSL-S-ASA	DSL-S-SWUP-ASA	Secure Access for DSLPipe – Firewalls and Authentication Header only	$1000	30 days
P22-SO-ASA	P22-SWUP-ASA	Secure Access for P220 – Firewall & Encryption	$2000	30 days

Worldwide and North American Headquarters
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502, United States
Tel: 510.769.6001
Fax: 510.747.2300
North American E-mail:
info@ascend.com
International E-mail:
air-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

Japan Headquarters
Level 19 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

Asia-Pacific Headquarters
Suite 1419, Central Building
1 Pedder Street
Central, Hong Kong
Tel: +852.2844.7600
Fax: +852.2810.0298

Latin, South America and the Caribbean Headquarters
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502, United States
Tel: 510.769.6001
Fax: 510.747.2669

ASCEND

Remote Networking Solutions That Work.™