Ascend

Secure Access (Version 2)

FAQ

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 does the Firewall and Encryption in Secure Access work together?*

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

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

   In the first phase of SecureConnect implementation, it is on Ascend's 50/75/85/130 (Authentication Header)/220 units. In the second phase, SecureConnect will be available on Ascend's MAX products.

5. *What is different about Secure Access (Version 2)? How does it affect the current security products?*

   Secure Access 2.0 combines IPSec encryption and authentication capability to Secure Access Firewall. The encryption component is shipped "dormant" until is activated via "feature codes" obtained from Ascend.

6. *Why are feature codes required to activate the encryption capabilities? How do I get the codes?*

   To date, federal regulations require manufacturers to track users of encryption products. This is accomplished by capturing demographic information when the feature codes are requested. By using the feature codes, manufacturers can specify the level of encryption activated (40-bit, 56-bit or unlimited encryption capabilities) based on U.S. eligibility regulations. Users can apply for feature codes by visiting Ascend's Web site, and the code is sent electronically within about an hour.

ASCEND

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 now 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.

8. *What is a security association?*

   A security association is the type of cryptography applied (Authentication Header or Encapsulated Security Payload), the algorithm used, remote and local IP addresses, initialization vector length and secret keys.

9. *What is an encrypted tunnel?*

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

10. *What is a mobile scheme? How does it differ from a static one?*

    A static scheme has a fixed remote tunnel IP address. A mobile scheme does not have a tunnel IP address configured; rather, the address of the remote tunnel endpoint is learned from the first inbound packet of a session from the remote system. Mobile schemes are useful when the remote system is a customer of an Internet Service Provider, which dynamically assigns IP addresses to customers as they dial in.

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

    The two tunnel endpoints are configured with each other's IP address (or wild card if it is a mobile scheme) by using the Secure Access Manager software. Authentication and encryption parameters (keys) are transmitted and received between both endpoints. Firewall rules can also be used to apply specific rules to individual tunnels.

12. *How does the system handle sites not specified as a tunnel endpoint? For example, if I use an Ascend Pipeline® to connect to my ISP and then set up encrypted sessions with my company across the country, can I still use the Internet for other functions?*

    The system encrypts only to sites which are designated as tunnel endpoints. The types of traffic designated in the firewall definition are routed through the encrypted tunnel. If access to other sites is allowed by the firewall rules (i.e. those to whom there is no encrypted session defined), then that traffic is sent in the clear (unencrypted).

13. *What is session stealing?*

    Some attackers can watch a gateway and see Internet traffic as users are allowed or denied access. Session stealing occurs when a particular user is granted access, then attackers sneak in as if they were that user. This is why user-level authentication via an unsecured environment such as the Internet needs augmentation. The Authentication Header feature in Secure Access prevents this type of attack.

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

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

15. *What are the key lengths used for DES, 3DES, MD5 and SHA-1?*

    Keys are a hexadecimal number constituting a secret shared between the tunnel endpoints:

    - MD5 - 128 bits
    - SHA-1 - 160 bits
    - DES - 56 bits
    - 3DES - 3 separate 56 bit keys

16. *What is CBC?*

    CBC stands for Cipher Block Chaining. This is a technique of chaining data from previous blocks and feeding it into the current block of encrypted data.

17. *What is an Initialization Vector (IV)?*

    An initialization vector is a function which provides random data to obscure the first block of data. This random block has no meaning, but is simply a way to make sure that data (for example, the header to an IP packet) is encrypted differently each time. Ascend's IPsec encryption allows the user to choose initialization vectors of either 32 or 64 bits (for flexible interoperability), and handles the IV function transparently to the user. When used in conjunction with CBC, this further randomizes the result of encrypting data.

18. *Does IPSec compete with other encryption techniques such as SSL and S-HHTP?*

    No, SSL and SHTTP are application level encryption formats. They can be used independently of IPSec and do not affect how it operates. These algorithms are usually used for transactional and other application-specific uses, such as encrypting your credit card number for Web purchases. Secure Access Encryption encrypts and authenticates not only the credit card information but all information from any application.

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
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

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.™

15-10-FAQ
08/97