Ascend

TECHNICAL OVERVIEW

Ascend Secure Access Firewall Control Protocol



Background

The growing use of the Internet for private purposes has increased the need for security. Many methods and levels of security have been implemented, such as Ascend Secure Access™ Firewalls, application gateways (including proxy servers), intrusion detection systems, virus scanners, authentication packages and more. Currently, most of these types of products are considered to be standalone entities that do not interoperate with other security mechanisms.

The market, however, has been asking for a more integrated approach. Customers are demanding that they be able to combine the features of diverse security products that can control network traffic across geographically separate locations. Security is strengthened when the flow of network traffic to and from a company can be based on a number of methods supported by multiple vendors.

Overview

To fulfill the emerging market demand, Ascend created Secure Access Firewall Control Protocol (FCP). The goal of the FCP developers was to create a specification other products could incorporate so they can cause dynamic updates to the Secure Access Firewall. These products will use the FCP protocol to reshape a Secure Access Firewall whenever they discover an event that should trigger its change.

How Firewall Control Protocol works:

- Third-party partner product becomes Secure Access Firewall “Aware” by incorporating the FCP protocol.
- Network administrator prepares an FCP-ready Secure Access Firewall ruleset which remains dormant until enabled.
- Network administrator configures the FCP partner product so it can enable the FCP rule. Since these products perform different security functions, a wide variety of conditions can cause them to enable an FCP-ready ruleset.
- FCP Partner product sends an FCP message to the Ascend Secure Access Firewall.
- Ascend Secure Access Firewall unit authenticates the source and content of the FCP message.
- Secure Access Firewall enables the FCP-ready ruleset and incorporates the FCP message’s contents into its rules.
- The dynamic rules continue in the Secure Access Firewall until a predefined time-out expires or the FCP partner product sends a disable-rule request to Secure Access.

Secure Access Firewall FCP Rulesets

Rules in Secure Access Firewall rulesets provide protection that ranges from simple IP address blocking to service-based packet controls of high granularity. Secure Access Firewall rules fall into two general categories:

1. Disabling of packet forwarding based on your network policy or because of a security breach.
2. Enabling of packet forwarding to provide fine-grained access control for authenticated users and systems.

Example Applications

- A virus checker running behind Secure Access examines incoming e-mail files arriving via the Internet. When the checker determines a message has a virus, the checker sends an FCP message to Secure Access Firewall that causes it to deny any further email messages from that IP address. The network administrator investigates the infected message was sent by a malicious hacker or a legitimate user who unknowingly transmitted infected files.
- An intrusion detection program running on a Web server monitors the WWW traffic sent to the server. If suspicious activity occurs, the program sends FCP messages that cause Secure Access Firewall to block incoming WWW packets to the server.
- An internal monitoring program screens outgoing Internet traffic to see if users are visiting in appropriate sites or tying up excessive amounts of bandwidth. If the program discovers either condition, it sends an FCP message to Secure Access Firewall, causing a change which blocks access to services or to the offending sites.

Summary

Firewall Control Protocol and Ascend Secure Access Firewall offer:

- An open protocol that enables third-party security products to control access through Secure Access Firewalls.
- A dynamic network perimeter security solution that protects the entire network.
- A firewall control mechanism that is enhanced by every FCP-compliant security product you add to your network.

Worldwide and North American Headquarters
Ascend Communications, Inc.
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 Page: http://www.ascend.com

European Headquarters
Aspen House
Barley Way
Ancells Business Park
Fleet
Hampshire GU13 8UT
United Kingdom
Tel: +44 1252.360000
Fax: +44 1252.360001

Asia-Pacific Headquarters
Suite 1908
Bank of America Tower
12 Harcourt Road
Hong Kong
Tel: +852.2844.7600
Fax: +852.2810.0298

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

Latin, South America and the Caribbean Headquarters
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502, United States
Tel: 510.769.6001
Fax: 510.747.2300

Ascend and the Ascend logo are registered trademarks and all Ascend product names are trademarks of Ascend Communications, Inc. Other brand and product names are trademarks of their respective holders.

05-18b
3/98