Ascend

July 1, 1996

Technical Overview

Access Denied: The Benefits of Integrated Firewall Security

Richard Sekar

ASCEND

Access Denied:
The Benefits of Integrated Firewall Security

TABLE OF CONTENTS

1.0 Executive Overview

With the commercial development of the Internet, the need to protect your corporate resources has become critical. The applications used to provide this protection are called "firewalls." While firewalls have existed in various forms for several years, they recently have become popular as a commercial product.

Most commercial firewall products are **stand-alone, or managed component, firewall** applications. These systems usually require the following elements: specialized firewall software; firewall configuration and management software; a dedicated platform used to run these applications; and a router (which may or may not be a current part of your network inventory) used to establish a connection to the Internet.

Another type of firewall solution provides a router for Internet connection, firewall protection and system management functions all in **a single solution**. These products are known as **integrated or fully integrated firewall solutions.** The firewall and router combine to provide a more secure network solution than the piecemeal approach used by stand-alone systems.

This document describes the advantages to implementing an integrated firewall solution compared to a mix of stand-alone firewall and router products.

ADVANTAGES OF A FULLY INTEGRATED FIREWALL

The benefits of an integrated firewall solution can be summarized as follows:

- Because the firewall is embedded in the router, both network and system router are protected against attacks.
- Integrated solutions run on unique operating systems, eliminating security “holes” and bugs inherent to common operating systems, which can be exploited by hackers to circumvent a stand-alone firewall.
- The router/firewall solution offers an economical package with a low initial investment since users do not need a dedicated workstation, custom software and separate router.
- Integrated solutions provide a lower cost of ownership since maintenance costs such as operating system upgrades and user training are eliminated or significantly reduced.
- A single vendor solution reduces interoperability problems, reduces support costs and lightens the load on internal help desk resources.
- A single solution simplifies system management and configuration.

For the first time, network managers have a viable, affordable solution for enterprisewide deployment. An integrated firewall solution gives you the ability to quickly establish and implement a security policy—and make ad hoc changes to policies as your organization grows and changes.

2.0 Introduction

DENY ACCESS TO HACKERS AND INTRUDERS; SECURE YOUR NETWORK

Independent studies made by industry publications and market analysis firms have repeatedly shown that network break-ins occur on over 20% of networks worldwide. A recent U.S. Senate report[1] indicated that over 250,000 attacks had been made on Pentagon computer systems in 1995 alone. In internal testing, Defense Information Systems Agency personnel were able to gain access to 65% of the computer systems they attempted to hack. Of these attempts, only 4% were detected; less than 1% drew any type of active response.

Some hacking attempts are simply malicious in intent, such as the insertion of a virus into your system. Others are more criminal, with the acquisition of your valuable corporate information the goal. If your network is connected to the Internet, hackers can break in and access this information without leaving any traces of their activity.

While the up-front cost of securing your network might seem like an unnecessary burden, the downstream cost of not securing your net is potentially much higher. Consider what the loss of your firm's financial, customer or new product data might mean to the future of your company.

Traditionally, the standalone components required to secure a network against unauthorized access are:

- a ROUTER, which provides the physical connection to the Internet,
- a FIREWALL, which protects the system behind the router from unauthorized access, and
- a hardware and a common OS to run the firewall.

The cost of purchasing a complete system when using stand-alone components can amount to as much as $40,000 or more.

In contrast, an integrated solution such as Ascend's Secure Access™ Firewall dramatically reduces your costs for network protection. The firewall software option to Ascend products starts as low as $500 per unit for unlimited users. It requires a single product, not three components. Moreover, the router/firewall combination offers protection at the very edge of the remote network—denying the opportunity for hackers to interfere with the router or the LAN.

Ascend Secure Access Firewall is fully integrated into Ascend's Pipeline and MAX product families to offer an affordable alternative to stand-alone systems.

[1] Govt. Acct. Office Report #B266140

3.0 Ascend Secure Access Firewall Benefits

THE PRIMARY BENEFITS OF A FULLY INTEGRATED SOLUTION

- Network **and** system router are protected against attacks
- Eliminates exploitation of security "holes" inherent to a common OS
- Low initial investment
- Low cost of ownership
- Greatly reduced support costs — infrequent help desk calls
- Ease of management
- Extremely affordable network-wide deployment

3.1 Your system router is protected against attacks

Since stand-alone firewall products are installed behind the router, the router itself is exposed to hacker attacks from the Internet (Figure 1). Although routers are relatively invulnerable to novice hackers or the average net surfer, experienced hackers can change or modify the router's configuration files. This won't necessarily give hackers internal net access, but they can use ICMP redirects and other routing protocols to forward data leaving your company to any address without your knowledge.

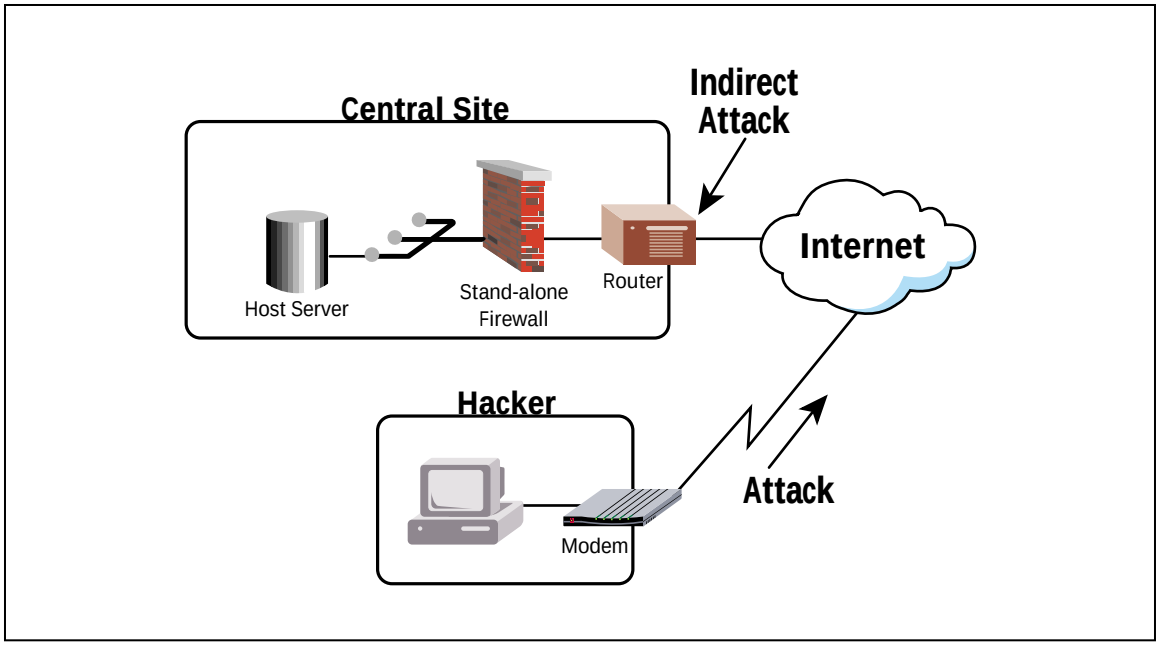

Figure 1 – Stand-alone firewall system.

There are other possibilities for the hacker as well. They might change the passwords and security features on the router, thus denying access for legitimate users. Also, hackers can bombard the router continuously with access demands in order to trigger “denial of service” faults to legitimate requests. Or they can create an electronic back door to the router without modifying your normal access procedure, giving them continued access to your network undetected.

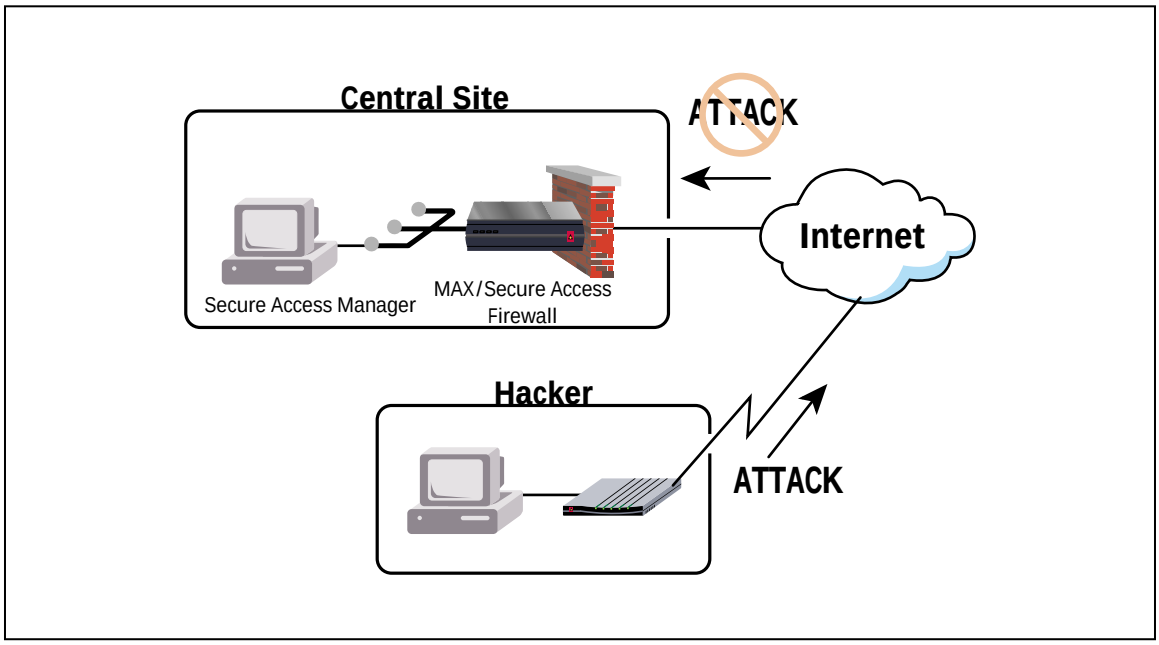

Figure 2 – Integrated router/firewall solution.

In a fully integrated system, the firewall is located at the front of the router, protecting the network against attacks via the Internet (Figure 2). Importantly, this design also prevents attempts to break into the router.

Any traffic that enters your network is intercepted by the firewall, which processes data and, if permitted, forwards information to the router for further dissemination. This eliminates possible holes in your network security screen common to stand-alone firewall and router configurations.

3.2 Eliminates exploitation of security "holes"/ bugs inherent to a common OS

Most stand-alone firewall applications run on the widely available UNIX operating system, which contains security holes or other bugs that hackers can exploit. This is a dynamic condition, requiring vigilant monitoring and costly OS modification to maintain adequate network security. Hackers can potentially use these software bugs to their advantage to circumvent a stand-alone firewall. Even for those operating systems that have received National Security Administration (NSA) certification, network managers must monitor frequently for new security-related OS bugs.

Ascend's firewall application runs on a proprietary microkernel OS, which is embedded on the router itself. This system is not subject to the common weaknesses found in the commercial operating systems used by many stand-alone firewalls. Since it is not commercially available, *Ascend's router OS is not open to hacker experimentation and exploitation common with UNIX.*

3.3 Low initial investment

The combined cost of the individual components with a stand-alone system is much higher than the fully integrated router/firewall solution. You are required to purchase the router itself, the firewall software and/or hardware, and the network management software needed to configure and manage your setup. The cost of a stand-alone system can be broken down into the following categories:

- *Router.* Any connection to the Internet requires a router. Depending upon the type of connection, whether leased line or a digital, the cost of the equipment typically varies from about $2,000 to several thousands of dollars.
- *Firewall application.* This software runs on either a common operating system such as UNIX and Windows NT, or it requires a specially designed high-security OS.
- *Dedicated firewall computer platform.* Most firewall applications require a dedicated workstation, which can add as much as $7,000 to $20,000 to start-up costs.
- *Management software.* Configuring stand-alone firewall systems typically requires the expertise of a specialized technician, who must enter alphanumeric strings from the command line. The Boolean-type rules used by many firewall products lend themselves to typing and logic errors—potentially creating major security holes in your network. Additional charges may be incurred for acquiring an optional GUI interface.

An integrated firewall/router solution offers a *low initial investment* because it eliminates the need for multiple hardware and software components. Also, Ascend's firewall solution includes Secure Access Manager, Windows-based configuration software that offers point-and-click setup of Secure Access Firewall sites. There is no need for acquiring additional firewall management tools—Secure Access Manager gives you fine-grained control over your firewalls and remote management features at no additional charge.

3.4 Low total cost of ownership

Maintenance poses a hidden cost of ownership. Before purchasing a firewall, consider the following:

- Operating system changes
- Upgrades
- Downtime
- Technical resources

The multiple components needed for stand-alone firewall systems create an additional support burden for network managers. Each of the separate products—router, firewall software, firewall hardware and the workstation's operating system—add significantly to cost of system ownership in both time and money. Your staff must be trained not only on the individual components but on assuring interoperability.

Upgrading or changing one of the components could affect the operation of other parts in a stand-alone system. Moreover, the workstation in a stand-alone system typically is dedicated to the task of running the firewall, effectively eliminating its use for other computing tasks.

In contrast, a *fully integrated solution minimizes training costs, costs associated with desktop and/or office real estate, operating system upgrades and maintenance.* The operating system is embedded within the router, upgrades can be accomplished remotely and do not affect other equipment in your network, there is only one piece of equipment to manage, and maintenance of the firewall is simplified through a Windows-based interface. As a result, your total cost of ownership is significantly reduced.

3.5 Greatly reduced support costs – infrequent help-desk calls

Installing stand-alone routers and firewalls requires a great deal of "tinkering" and adjustment on both units to provide maximum security and prevent hackers from breaking into the network. This tedious task also represents hidden costs in downtime and resource allocation. Cross-vendor interoperability issues also present potential conflicts and place burdens on in-house and multiple vendor technical support.

Interoperability problems are not an issue with an integrated solution. You can turn to a single manufacturer for support—eliminating finger-pointing that can occur between multiple manufacturers of components in a stand-alone system.

3.6 Ease of management

System administrators are forced to undergo a complicated set of setup procedures to manage interrelated but separate components. These systems generally require separate configuration and management applications that may run on separate environments.

Fully integrated solutions simplify configuration and management through a single set-up application such as Secure Access Manager, the Windows-based application for managing central site and router site firewall configurations.

3.7 Extremely affordable network-wide deployment

Stand-alone firewalls and routers require a high investment on the equipment, making deployment throughout the enterprise too expensive for most companies (Figure 3). Unfortunately, this can leave your network with significant security holes. Hackers can encroach upon the remote host and use it as a springboard to launch a successful attack on a firewall-protected central site.

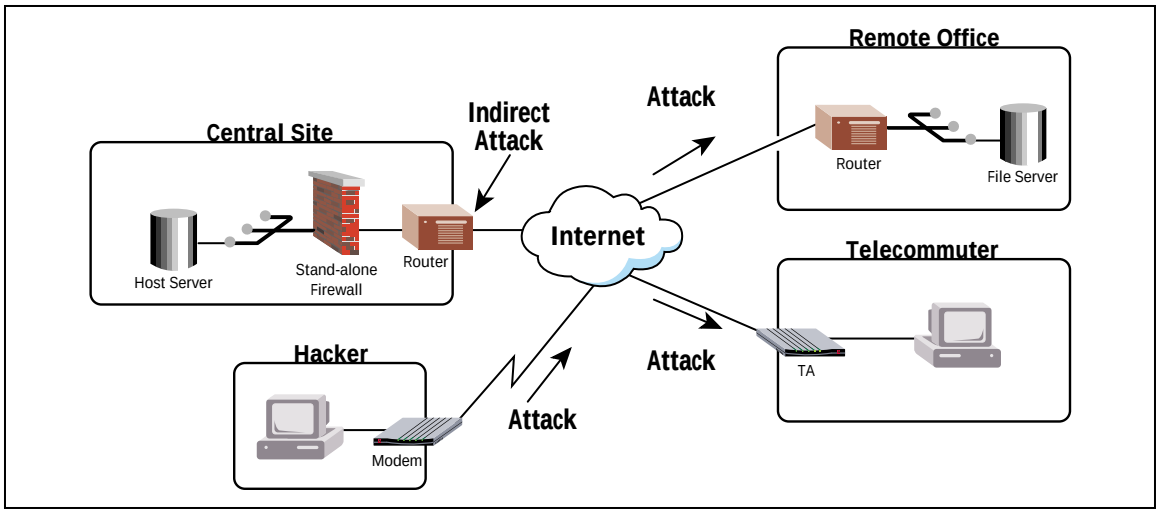

Figure 3 – Expensive stand-alone products leave remote sites unprotected.

Bullet-proof network protection requires safeguarding all of your remote sites (Figure 4). Since your network already includes a router for external communications to the Internet or central site, a firewall solution such as Ascend's Secure Access Firewall fits seamlessly into an existing structure.

For customers who already own Ascend MAX and Pipeline products[2], installing Secure Access Firewall requires a simple software upgrade. The investment is as low as $500 per unit—a fraction of the cost of stand-alone systems. For customers who are installing Ascend products, Secure Access Firewall is installed as a software option.

For the first time, end-to-end network security that provides state-of-the-art firewall protection is an affordable solution for any company—from Ascend, the leader in remote networking.

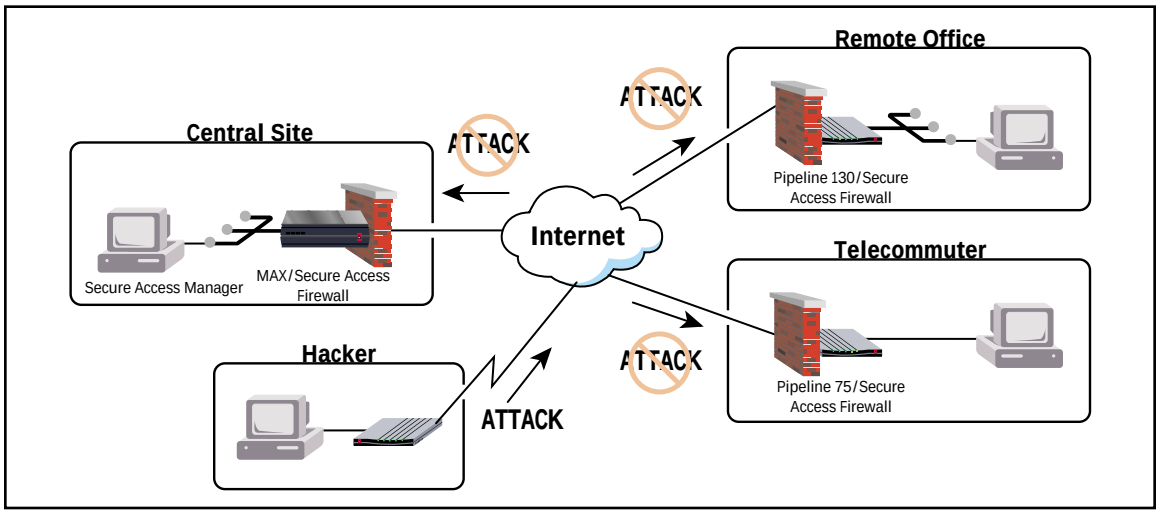

Figure 4 – Secure Access Firewall gives companies the ability to install bullet-proof security across the enterprise.

[2] Secure Access Firewall is an option in the following Ascend products: MAX 200Plus, MAX 1800, MAX 2000, MAX 4002/4004, Pipeline 50, Pipeline75, Pipeline 130

4.0 Summary

A fully integrated products such as Ascend's Secure Access Firewall offers the best possible combination:

- Superior security and performance
- Reduced initial and on-going costs
- Ease of management and use.

Feature Comparison	**Fully-integrated Solution**	**Stand-alone Firewalls**
Router	Protected	Unprotected and exposed to attack
Operating System	Not available for experimentation and exploitation	Commonly available to hackers for experimentation and exploitation of bugs
Start-up costs	Single component, low cost	multiple components, high cost
Maintenance and support	Single manufacturer	Multiple manufacturers
Setup and Management	GUI, point and click	Boolean logic, command line entry

Ascend. Remote Networking Solutions That Work.™

Ascend Communications, Inc.
1275 Harbor Bay Parkway
Alameda, CA 94502, USA
TEL: 510.769.6001
FAX: 510.814.2300

E-mail: info@ascend.com
Toll Free: 800.621.9578
FAX Server: 415.688.4343
Internet Home Page:
http://www.ascend.com