SonicWALL White Paper

Strategies for Increasing ISP Profitability

SONICWALL

Introduction

As Internet connectivity becomes a basic commodity, Internet Service Providers (ISPs) are experiencing intense pressure to provide service at the lowest possible price. But only the largest providers can successfully compete on price, and smaller providers are finding it difficult to maintain profitability.

In an increasingly saturated market, it's no longer enough to emulate business models that have been successful in the past, or are currently successful for the largest providers, such as AOL, Sprint, or UUnet. Competing on price is a dangerous strategy for even for the largest providers, because market share does not automatically translate into profitability. And for companies that do not already have a large market share, the chances for dramatically increasing their subscriber base in an increasingly competitive environment is becoming more and more remote.

Faced with these challenges, smaller ISPs are challenged to develop new business strategies that will enable them to claim a profitable share of the market. These strategies are not based on competitive pricing, but instead are focused on increasing and retaining a loyal customer base by delivering value-added services such as:

- Cost-effective firewall security services to protect against hacker attacks.
- Anti-virus protection to avoid catastrophic data losses.
- Virtual Private Network (VPN) connectivity for secure remote connectivity.
- Content filtering to prevent access to objectionable Web content.

According to Michael Porter, well-known former Professor of Business Administration at Harvard University, there are two ways to maximize profitability in a competitive marketplace. The first approach is the familiar concept of increasing market share, developing

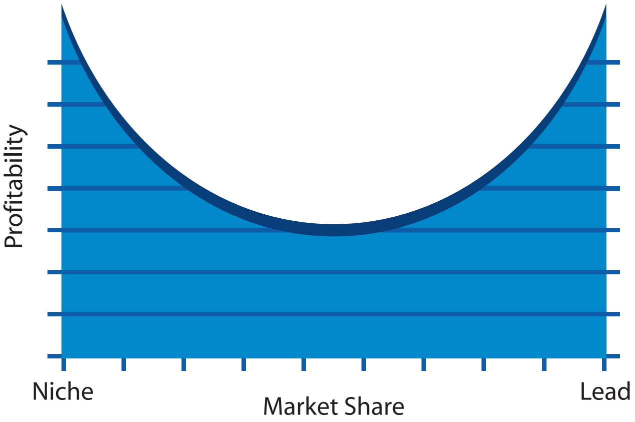

Figure 1: Porter's curve illustrates the opportunity for niche marketers to attain profitability by pursuing alternative strategies.

economies of scale, and competing on price. However, Porter identifies another strategy where niche players identify a target market, provide high levels of service that meet that target market's needs, and command a premium price (see Figure 1). For small-and-medium sized ISPs today, this service-based strategy is the key to success.
Figure 1: Porter's curve illustrates the opportunity for niche marketers to attain profitability by pursuing alternative strategies.

Differentiation Strategies that Increase Profitability

As the small and medium-size enterprise (SME) market adopts the Internet as a business-critical resource, significant opportunities have emerged for ISPs to offer specialized services. The Internet has enabled new services and opened new markets for businesses, and but is also exposing them to new types of risk that must be managed.

Comprehensive Internet security is a key issue for the SME market – particularly for companies with high-speed "always on" Internet connections. DSL and T1 connections offer powerful benefits to the companies that use them, but the risks that go along with high-speed connections to the Internet are great. According to a recent study fielded by Price Waterhouse Coopers, viruses and hacker attacks cost businesses around the globe more than 1.5 trillion dollars annually. The SME market needs protection from productivity and critical data loss, without the overhead of in-house Internet security expertise.

Providing solutions to these security challenges enables ISPs to move away from the business model of simply offering Internet connectivity. By developing differentiation

Challenging Market Forces for Small to Medium-Size ISPs

- Losing customers through price competition
- Constant equipment upgrade costs create a slow return on investment (ROI)
- Decreasing revenue opportunities as demand for inexpensive DSL connections eclipses T-1 and other traditional services
- Expensive ILEC leasing fees for DSL connectivity
- Replacement of per-minute service with flat-rate service reduces profitability

Case Study : Epoch Internet

"After looking at several different vendors, we chose SonicWALL. The units are easy to use, have a great feature set, and provide a nice upgrade path. And the price point is unbelievable for an ICSA-certified firewall — it's no wonder they're the market leader.

"Once our customers have a SonicWALL installed, there's a lot we can do with it. Anti-virus, VPN, content filtering — they're all great services that customers need and we can charge for. And now that remote management is available, we can control it all from our central office."

Alfredo Narez, Sr. Product Manager, Access and Security Products, Epoch Internet

Epoch Internet is a Tier One service provider that specifically targets the small and medium-size enterprise (SME) market. They offer DSL, DS3, T1, and T3 access services, own and manage their own backbone network, and have peering agreements with other Tier One providers.

In addition to firewall security, Epoch Internet has identified a strong market for VPN services, which provide additional security through advanced data encryption techniques.

strategies to address the security issues confronting the small-to-medium enterprise market, ISPs can offer a specialized range of services that will increase profitability, reduce exposure to price-based competition, and increase customer loyalty.

Specifically addressing the timely concern of Internet security, ISPs can attract and retain customers by introducing value-added services such as firewall security, anti-virus protection, VPNs, and content filtering.

Once these value-added services are in place, customers view their provider in a very different light. Instead of simply providing the commodity of Internet connectivity, the ISP becomes an indispensable business partner that helps customers manage their risks, tap into previously closed markets, and operate in new, exciting ways.

The SonicWALL Internet Security Solution

Until now, two prime factors have prevented most ISPs from offering firewall protection to their clients: cost and complexity. The SonicWALL Internet security appliances overcome both of these factors, delivering a robust, feature-rich product line with an entry point of under $500. The products are designed for simple, trouble-free configuration and operation, and can be installed and maintained by existing SME personnel without extensive training.

To purchase a device capable of providing ICSA-certified firewall capability, ISPs have had to pay large sums of money, creating an ROI lag that could extend to several years. Short-term profitability was impossible, creating a powerful disincentive for entering the market.

Unlike traditional solutions offered by other vendors, the SonicWALL appliances are stand-alone devices that do not rely on UNIX or Windows systems. Instead, a real-time operating system running on solid-state hardware delivers a more reliable solution, designed to increase security by reducing complexity. In addition, ISPs are not forced to incur the costs of purchasing a high-end workstation to manage the system.

Monthly service charges from ISPs using other firewall products can range from $800 to $1500 per month. For ISPs that adopt the SonicWALL Internet security solution, potential revenues of several hundred dollars represent a dramatic price break for customers, and still enable providers to reach profitability after only 4 to 6 months. The low-cost devices can be easily installed at the customer's premises and managed from the ISP's Network Operations Center (NOC). ROI occurs after a short period of months instead of years, and then the devices become a steady source of revenue.

Key benefits delivered by the SonicWALL Internet appliances include:

- **Quick return on investment (ROI)** helps service providers gain profitability from their investment within the first four to six months of operation, ensuring profitability before hardware becomes obsolete.
- **ICSA-certified firewall** ensures business-critical security through the use of stateful packet inspection.
- **Platform for comprehensive Internet security** enables add-on revenue for ISPs for additional services such as VPN, network anti-virus, content filtering, and more.
- **Ease of use** translates into lower cost of ownership, by eliminating the need for equipment to be maintained by UNIX engineers and security experts. SonicWALL appliances are pre-configured for maximum security, unlike traditional firewalls that must be configured on a rule-by-rule basis.

- **Remote management capabilities** open up another rich revenue stream for ISPs, enabling them to manage a distributed network of SonicWALL appliances for their clients.
- **Free Lifetime Software Upgrades** for SonicWALL appliances ensures protection from the latest security threats. In addition, as additional services are supported and made available through upgrades, new marketing opportunities and revenue streams are created.

Capable of supporting a broad range of services, the SonicWALL appliances offer far more than ICSA-approved firewalling capability. Instead, they become a service delivery platform capable of transforming a $39 per month DSL client into an account that can generate revenues of of serveral hundred dollars per month, a dramatic increase over revenues generated by basic Internet connectivity. The combination of a low base cost and the broad array of services supported by SonicWALL presents a unique opportunity for ISPs to realize substantial increases in revenue.

Global Management

The SonicWALL Global Management System (GMS) opens several new markets for ISPs. GMS delivers remote management of SonicWALL devices located at the customer premises, which offers several key benefits to service providers:

- Centralized management enables ISPs to manage up to 1,000 SonicWALL Internet security appliances in remote locations.
- Additional marketing opportunities to provision SonicWALL Network Anti-Virus, SonicWALL VPN, and SonicWALL Content Filtering services are created once a customer has established firewall services.
- Eliminates the need for truck rolls and a staff of installation/repair technicians. Units can be configured at the ISP's central site or by a value-added reseller (VAR), and easily installed by the customer. SonicWALL has developed partnerships with thousands of resellers, and can easily help an ISP find a VAR to partner with in their area.
- Software upgrades and configuration updates can be easily handled from the ISP's central site, providing a flexible solution that grows with the customer's changing business needs.
- Group management enables configuration templates to be applied with drag-and-drop convenience, automatically activating customized service packages.

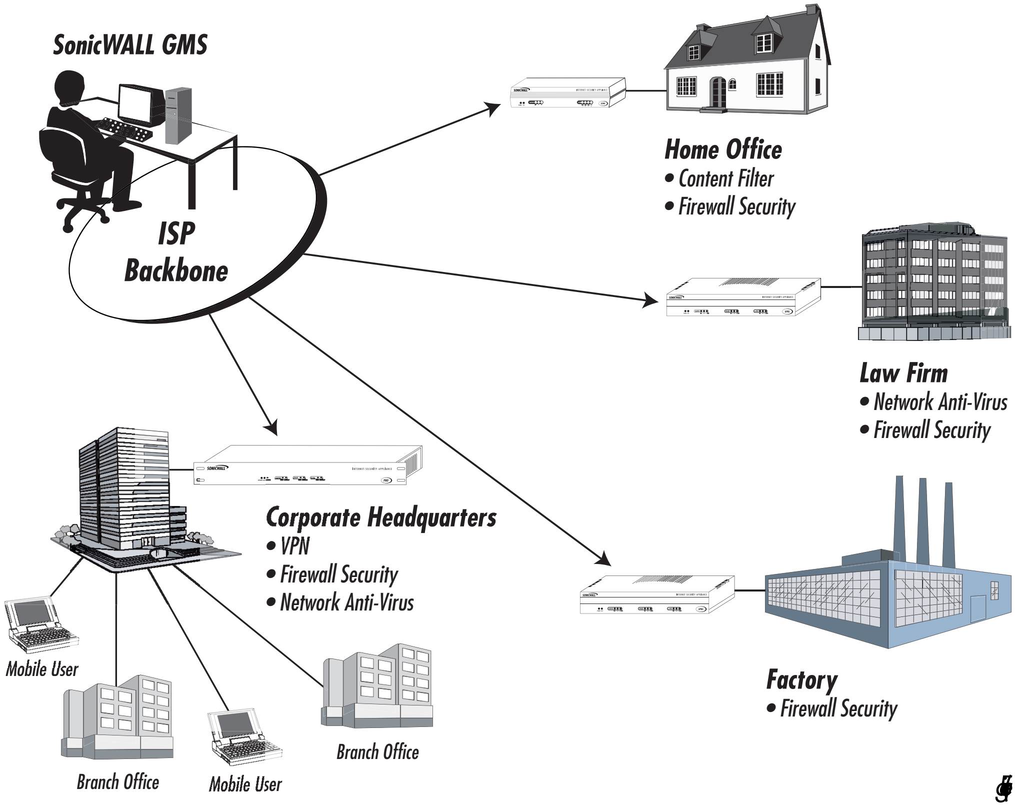

Figure 2: ISP managing different customer networks and rolling out value-added services with SGMS

Once customers recognize the need for firewall security, key marketing opportunities are available to generate additional revenues. These value added services include:

- **ICSA-certified firewall protection** Defending Internet access customers from hackers, data thieves and Denial of Service attacks through the use of SonicWALL's stateful packet inspection firewall is a valuable service.
- **Anti-Virus protection** This key service is designed to combat a critical problem for all computer users. Available on a subscription basis, SonicWALL Network Anti-Virus offers an additional service that adds to the monthly revenue stream. Virus definitions are updated continually and automatically, and downloaded at the click of a mouse.

- **Virtual Private Networks (VPNs)** Offering a secure way of extending services on the corporate network to customers and business partners, IPSec-encrypted VPN tunnels are supported by all of the SonicWALL appliances. VPNs enable businesses to achieve secure connectivity to remote and branch offices without the expense of leased lines, creating another potential revenue steam for service providers.
- **Content filtering** Ideal for schools and libraries as well as businesses, content filtering restricts user access to undesirable Internet sites. ISPs can purchase a block of content filter subscription licenses from SonicWALL, and then generate additional revenue by applying them to customer's firewalls as demand occurs. Updated lists of banned sites are automatically distributed on a weekly basis.

This managed environment provides a secure climate where businesses are protected from the dangers of high-speed, always-on access Internet access, including unauthorized network access, costly data loss from virus attacks, and productivity loss (and even lawsuits) from inappropriate content. Further, VPN enables secure data communication between remote locations, with powerful ARCFour, DES, or Triple DES encryption, ensuring Fortune 500-level security. Customers operating in a secure environment will view their ISP as a business partner instead of as a commodity vendor, and will be more likely to develop an ongoing relationship and less likely to change providers.

For ISPs who do not wish to assume responsibility for selling, installing and maintaining SonicWALL appliances on customer premises, several SonicWALL value-added resellers (VARs) are now offering these services in partnership with ISPs. It is significant to note that sufficient revenue potential exists to support the entry of a third-party VAR, while still offering attractive profits for the ISP and significant cost savings for the end user. For more information, contact SonicWALL sales at 1-888-557-6642.

Opening the Door to a New Business Model

The SonicWALL Internet security solution represents an important marketing opportunity for ISPs, enabling them to broaden their product offerings with value-added services and distance themselves from business models based solely on price. SonicWALL is the market leader in affordable, high-performance firewalling solutions for the small and medium-size business market, and has a complete range of appliances that provide a platform for comprehensive Internet security. By offering cost-effective SonicWALL firewall, anti-virus, VPN, and content filtering solutions, ISPs can increase profitability and succeed in an increasingly competitive environment.

SonicWALL Internet Security Appliance

High-speed, always-on Internet connections offer businesses significant advantages but also threaten network security. Hackers or unauthorized users may steal or corrupt important information. SonicWALL state-of-the-art technology provides robust, reliable, and affordable Internet security for businesses with a few users to several thousand users.

To protect the private network against Internet-based theft, destruction, or modification of data, SonicWALL implements firewall security with stateful packet inspection. SonicWALL allows data from the Internet only if it's part of a session that was initiated by a user on the secure private network; hackers and other unauthorized Internet users will be blocked.

SonicWALL protects the network from Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood, IP Spoofing, and LAND Attack. When new hacker attacks are discovered, SonicWALL adds protection from them to the SonicWALL software and automatically notifies the administrator of the new firmware releases. All registered SonicWALL customers get free software updates.

SonicWALL VPN Upgrade provides an easy, affordable, and secure means for businesses to connect offices and partners together. Using data encryption and the Internet, SonicWALL VPN provides secure communications between two or more sites without the expense of leased site-to-site lines. Encryption methods include 168 bit Data Encryption Standard (Triple-DES), 56 bit Data Encryption Standard (DES) and 56 bit ARCFour (ARC4). SonicWALL VPN can be used with other VPN products with the same IPSec implementation, such as Check Point Firewall-1, Cisco PIX and Axent Raptor. SonicWALL VPN Upgrade also includes a single-user license VPN client for Windows to allow secure remote management. SonicWALL VPN is included in the SonicWALL PRO.

SonicWALL Network Anti-Virus eliminates the challenges of managing network-wide anti-virus solutions. SonicWALL Network Anti-Virus transparently deploys an agent configured by the administrator to each of the systems to be protected - no desktop-by-desktop installation or configuration required. Because the agent is automatically updated each time end-users access the Internet, SonicWALL Network Anti-Virus ensures that all nodes on the network are protected with the most current anti-virus engines.

Content filtering allows businesses to create and enforce Internet access policies tailored to the needs of the organization. An optional Content Filter List subscription is available which allows the administrator to select categories of Internet sites, such as pornography or racial intolerance, to block or monitor access. Automatic weekly updates of the customizable Content Filter List make sure that access restrictions to new and relocated sites are properly enforced. Users may be given a password to bypass the filter, giving them unrestricted access to the Internet.

SonicWALL Global Management System is a scalable, cost-effective solution that extends the SonicWALL Internet security appliance's renowned ease of installation and administration, giving network administrators the tools to easily manage the security policies of remote, geographically distributed networks. The recent proliferation of inexpensive high-speed broadband access has accelerated the connection of branch offices, telecommuters and key business partners to corporate headquarters. SonicWALL GMS reduces staffing requirements, speeds up deployment and lowers the cost of delivering services to these remote locations by centralizing the management and monitoring of security policies.

SonicWALL's Key Features

- **Firewall Security**. SonicWALL Internet security appliances use stateful packet inspection to protect the private LAN from hackers and vandals on the Internet.
- **IPSec VPN**. SonicWALL VPN provides an easy, affordable, and secure means for businesses to connect offices and partners together. Encryption methods include 168 bit Data Encryption Standard (Triple-DES), 56 bit Data Encryption Standard (DES) and 56 bit ARCFour (ARC4). SonicWALL VPN can be used with IPSec VPN products such as Check Point Firewall-1, Cisco PIX and Axent Raptor.
- **Network Anti-Virus**. SonicWALL Network Anti-Virus, based on Network Associates' market-leading anti-virus product, ensures corporations are protected against the latest virus outbreaks as soon as cures are available.
- **Internet Content Filtering**. SonicWALL's content filtering functions allow businesses to create and enforce Internet access policies tailored to the needs of the organization. An optional subscription to the CyberNOT Content Filter List is available.
- **AutoUpdate**. SonicWALL Internet security appliances maintain the highest level of security by automatically checking if firmware updates with protection against newly discovered hacker attacks are available. All firmware updates are free for the life of the product.
- **ICSA Certified**. SonicWALL Internet security appliances have been awarded the internationally accepted ICSA Firewall Certification.

SonicWALL Feature Chart

The following chart shows the number of LAN IP addresses (nodes) supported and other features in each SonicWALL model.

SonicWALL Model	Nodes	VPN	Anti-Virus	DMZ Port	10/100 Ethernet
SonicWALL Telecommuter	5	Included	Optional		
SonicWALL SOHO/10	10	Optional	Optional		
SonicWALL SOHO/50	50	Optional	Optional		
SonicWALL DMZ	Unlimited	Optional	Optional	Included	
SonicWALL XPRS	Unlimited	Optional	Optional	Included	Included
SonicWALL PRO	Unlimited	Included	Optional	Included	Included
SonicWALL PRO-VX	Unlimited	Included	Optional	Included	Included

SONICWALL

SonicWALL, Inc.
1160 Bordeaux Drive
Sunnyvale, CA 94089-1209
Tel: 408-745-9600
Fax: 408-745-9300
E-mail: sales@sonicwall.com
Web: http://www.sonicwall.com

Rev A. 8/00