

Assessing Business Continuity Solutions

Ensuring the uninterrupted operation of businesses is an issue of increasing importance not just for large enterprises but for medium and small organizations as well. More than ever before, highly available security solutions are a key business asset that not only protects data, but also helps a company grow by increasing employee productivity and mobility.

CONTENTS

Purpose	2
Background	2
The Challenges	2
Assessing a Robust Solution	3
Types of Solutions Available Today	4
Desired Capabilities	4
Integrated Solutions Tailored to Your Needs	6
Conclusion	8

Purpose

This paper discusses the effects of network downtime and the implications for IT managers. In order to guide readers in the assessment of business continuity solutions, the technologies necessary for a robust solution are identified and explained. Because different types of organizations have varying requirements, this paper highlights existing integrated business continuity solutions that address the needs of three common types of small and mid-sized companies.

Background

Today's highly connected organizations depend on vast amounts of critical data to support daily operations. If communications networks fail for any reason, significant losses can occur. Productivity plummets when employees and partners are unable to access e-mail or vital corporate information repositories. Revenue is lost, particularly for point-of-sale (POS) operations that must exchange customer purchase and inventory information with each transaction. When a disabled network impacts production schedules, valuable time is lost.

Equally important is the potential damage to a company's public image. Although more difficult to quantify, this type of risk is very real. In order to retain current customers and attract new ones, businesses must ensure that every customer interaction is satisfactory. Online shoppers can be lost in an instant if a Web site is down and competitive offerings are just a mouse-click away. These customers may be gone for good. Extrapolated over time, the cost of lost opportunities can be staggering.

Network downtime stems from two types of failures. First, in the event that the Internet Service Provider (ISP) experiences problems, where the broadband connection goes down, businesses can lose Internet connectivity and valuable work time. Second, even if a company still has Internet access, the virtual private network (VPN) could fail as a result of a network outage or Internet latency, leaving remote workers and business partners unable to access central office resources. This could have serious consequences if vendors or departments such as accounting or payroll are unable to access data to complete end of quarter bookkeeping, for example.

The Challenges

In order to support daily operations and maintain business continuity, an organization must be able to move vast amounts of data quickly, reliably and securely. But the complexity of managing a comprehensive network infrastructure is taxing IT departments like never before. Medium-sized companies, in particular, are feeling the pinch. While lacking the resources of larger organizations, these companies still have the same tasks to perform.

These issues are of particular relevance to IT managers who are held accountable for network outages, regardless of the cause. Therefore, IT managers are eager to implement "insurance policies" for their organizations—business continuity solutions designed to keep critical applications up and running at all times.

IDC projects a sizable increase in business continuity solution spending between 2002 and 2007, all translating into over \$118 billion in spending.¹ Clearly, business owners are placing great emphasis on the ability to ensure network reliability.

¹ Worldwide IT Security and Business Continuity Forecast, 2002 – 2007, IDC September 2003, IDC#30136, Volume: 1

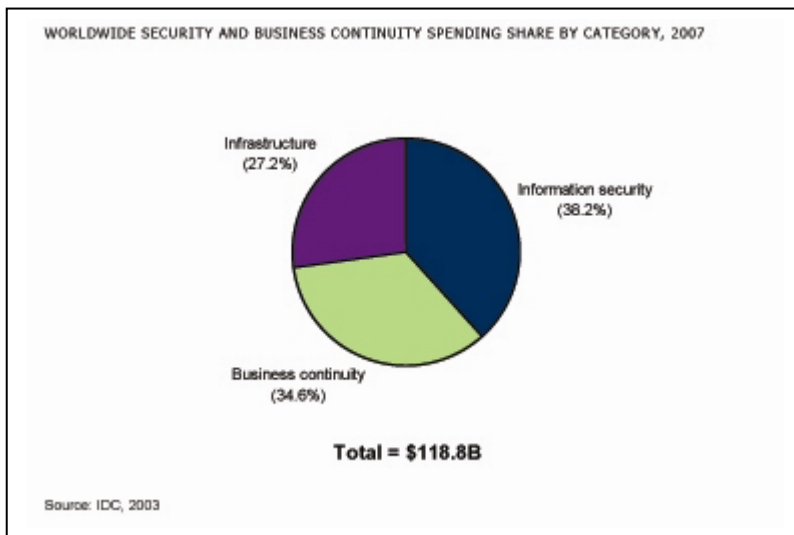


Figure 1
Worldwide Security and
Business Continuity
Spending Share by
Category¹

Assessing a Robust Solution

According to a 2003 survey conducted by SonicWALL Inc., customers purchasing business continuity solutions reported that network reliability is the number one factor that influences buying decisions. Network reliability is achieved using failover redundancy for all key components, thereby ensuring no single point of failure can impact network availability.

Redundancy is typically implemented at each network connection point. At the hardware level, a network might have dual routers or firewalls. There can also be external redundancy, such as two different ISP connections into the same router or firewall.

A good business continuity solution for small and mid-sized networks should provide a comprehensive yet cost-effective set of features. Buyers want a product that scales to the size of their organization. They don't want to pay for more bandwidth than necessary, yet they need a flexible solution that can keep pace with their company's changing requirements.

The solution also must be quick to deploy and easy to administer, especially if an organization has limited IT resources. Finally, ease of management is a key benefit that will continue to pay dividends over time.

In summary, a good business continuity solution should offer:

- Network reliability via failover redundancy
- Ease of use
- Manageability/flexibility
- Extensive features and functionality
- Excellent price/performance

Types of Solutions Available Today

Excellent technologies are being used in today's business continuity solutions. Products targeting enterprises offer a comprehensive suite of features and functions but are expensive and need ample staffing to manage. However, these products aren't designed to address the needs of organizations with limited resources.

Some companies customize a solution by cobbling together best-in-class components from various vendors. The downside is that this approach can be complicated, costly, and fraught with integration and maintenance issues that IT Managers generally prefer to avoid. The training requirements of a cobbled together solution make it prohibitive for a resource-limited IT organization.

The ideal answer is a fully integrated business continuity solution that can scale to exact price/performance specifications. Packages that provides all of the necessary functionality—and perhaps even some bonus capabilities for enhanced productivity—meet the IT manager's greatest needs.

Desired Capabilities

The following section provides guidelines for evaluating potential solutions. It explains vital technologies used in most business continuity solutions on the market today. Organizations' exact requirements will vary based on size and function; to warrant serious consideration, any business continuity solution should incorporate at least some of these core technologies.

ISP failover

ISP failover provides dual connections to the Internet and can be accomplished in one of two ways: either through connections to two different ISPs, or with two separate interfaces to two geographically dispersed locations of the same ISP. Regardless of the approach, the result ensures an automatic back-up if one line fails for any reason. By distributing the risk, a company minimizes its vulnerability to a network outage.

VPN redundancy

Similar to ISP failover, VPN redundancy allows remote/branch offices and business partners to seamlessly establish a VPN connection to a secondary gateway at corporate headquarters if the connection to the primary gateway fails. Maintaining a continuous connection with the central office ensures that remote employees and business partners can access the vital information they need, when they need it.

The switch from one VPN tunnel to another should be transparent to employees, partners, customers—and even to the network administrator. Although the network administrator will receive a notification alert, no intervention should be required. Tunnel transition must take place automatically and immediately without waiting for intervention from the administrator.

WAN failover

Two different types of media can be used to provide a WAN failover connection. If the primary Internet access connection is T1 or broadband then the secondary connection might be a more economical alternative such as analog or ISDN. This approach is often used by retail businesses with numerous POS locations.

Another approach is to use different service providers for independent connections so that any problem encountered by one provider does not affect other areas of business. For example, an organization might choose to have DSL service through SBC but opt to have its back-up analog connection failover to a different vendor such as AT&T. Again, the concept is to minimize risk by spreading dependency over multiple carriers.

Additional Productivity Enablers

Some solutions also include technologies that enhance efficiency, thus providing an even greater return on investment. This additional functionality enables an organization to leverage both primary and secondary connections, thereby enhancing network resources while providing back-up to the core infrastructure.

Load balancing

Load balancing optimizes both primary and secondary connections so that neither sits idle, improving your network connectivity investment. The secondary connection not only provides back-up insurance but also enhances network performance by sharing the traffic load. Cross-media redundancy provides another type of load balancing. In this scenario, failover capabilities utilize different types of Internet services. For example, the T1 could serve as the primary connection with DSL as the back-up; or a business might opt to establish failover from DSL to an analog modem. Both connections can be used for load balancing, with the primary connection loaded more heavily if the secondary link is slower. Or, the two connections could be designated to carry different types of traffic: e-mail on the link with the greatest bandwidth and regular Web traffic or other application-specific transmissions on the secondary connection.

Hardware failover

To ensure network reliability, hardware failover provides two components that serve the same function. Should the active unit fail, the passive unit automatically detects and assumes responsibility for forwarding traffic. This redundancy can be achieved by deploying two identical routers or firewalls. Or, a company might opt for internal redundancy with two WAN interfaces contained within the same box. Hardware failover can be used in “active-active” mode to enable Load Balancing, thus providing a highly efficient method for distributing WAN traffic.

Stateful synchronization

This feature provides automatic failover to a backup ISP if the primary connection goes down. The failover transition is invisible to end-users and protects transactions in process from being lost or corrupted. Stateful synchronization is of vital importance to retail/POS businesses.

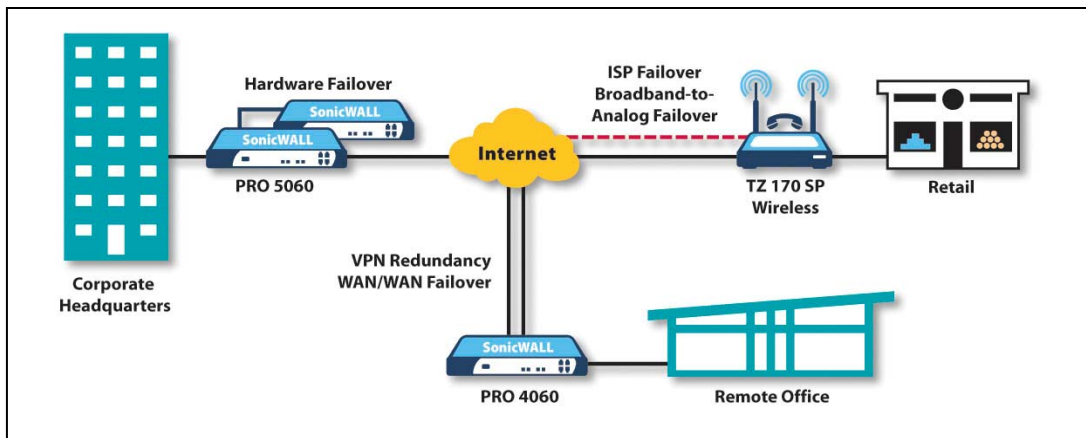


Figure 2
Desired Network
Capabilities for Business
Continuity

Integrated Solutions Tailored to Your Needs

Companies need a highly reliable business continuity solution that offers enterprise-class functionality tailored to their size and budget. The package must be easy to deploy and manage, with the flexibility to adapt to changing business requirements.

SonicWALL offers a range of end-to-end business continuity solutions that are fully integrated, tested and proven. These products are geared to address the specific requirements of the following types of organizations:

- Central, remote or branch offices
- Telecommuters and small offices
- Retail/POS businesses

It is essential to maintain secure connectivity between central, remote and branch offices. Remote and branch offices need access to headquarters' resources, while the central office must receive reports and sales orders from outlying sites. Reliable, always-on communications boost the productivity of employees at all locations.

To address these requirements, SonicWALL offers the PRO 5060, a high-performance, multi-service gigabit security gateway designed for medium-to-large networks with complex requirements. The PRO 5060 integrates high-speed gateway anti-virus, intrusion prevention, content filtering, enforced desktop anti-virus, deep packet inspection technology and IPSec VPN into a single solution that is easy to deploy and manage. Available in both 10/100/1000 copper and copper/fiber interface configurations, the PRO 5060 incorporates a wide array of networking and security features, making it an ideal solution for a multitude of applications.



SonicWALL's entire PRO Series integrates support for SonicWALL's portfolio of advanced security services, including gateway anti-virus, remote access VPN, content filtering, instant messenger and peer-to-peer application control and intrusion prevention. Installation and set-up is simple due to an intuitive Web management interface and easy-to-use wizards. Using object-based management, administrators can quickly configure multiple security zones for rapid deployment. Secure remote management is equally easy using a standard Web browser or SonicWALL's award-winning Global Management System for monitoring and managing a distributed deployment.

PRO Series	PRO 2040	PRO 3060	PRO 4060	PRO 5060c	PRO 5060f
VPN redundancy	✓	✓	✓	✓	✓
WAN failover					
WAN/WAN/Analog	✓*	✓	✓	✓	✓
WAN/WAN	✓	✓	✓	✓	✓
WAN/Analog	✓*	✓*	✓	✓	✓
Load balancing	✓*	✓*	✓	✓	✓
Hardware failover	✓*	✓*	✓	✓	✓
Stateful synchronization	✓*	✓*	✓	✓	✓

**With SonicOS Enhanced Firmware Upgrade*

Figure 3
PRO Series Capabilities

Telecommuters and small offices

The demand for telecommuting and mobile services for travelers is eroding the walls of the traditional office. Wherever they may be, today’s workers rely on access to information and resources in order to conduct their daily business activities. Because of this dependence on communications links, ISP failover is critical to protect the network. And for small offices with modest budgets, a business continuity solution must also be cost-effective yet scalable for the future.

SonicWALL offers the TZ 170 in three node configurations to support 10, 25 or an unlimited number of users. The TZ 170 is a single, scalable solution that provides low total cost of ownership. This flexible security platform features an integrated 5-port auto-MDIX switch and an optional port. The optional port can be configured as a WorkPort to isolate telecommuters from the home network, a second LAN for added network flexibility, a second WAN for ISP failover and load balancing or as a WLAN for secure wireless access. As a business continuity solution, the TZ 170 offers all of the desired capabilities and most of the bonus productivity enablers*.

The TZ 170 integrates support for SonicWALL’s portfolio of optional security services. With its intuitive Web management interface and easy-to-use wizards, set-up and configuration is a snap. Secure remote management is also effortless, using a standard Web browser or SonicWALL’s award-winning Global Management System for distributed deployments.



TZ 170 Series				
	TZ 170 SP Wireless	TZ 170 SP	TZ 170 Wireless	TZ 170
VPN redundancy	✓	✓	✓	✓
WAN failover				
WAN/WAN/Analog	✓	✓*	NA	NA
WAN/WAN	✓	✓*	✓*	✓*
WAN/Analog	✓	✓	NA	NA
Integrated Modem	✓	✓	NA	NA
Load balancing	✓	✓*	✓*	✓*

**With SonicOS Enhanced Firmware Upgrade*

**Figure 4
TZ 170 Series Capabilities**

Retail/POS businesses

POS businesses such as retail stores, banks and gas stations exchange customer purchase and inventory information with every transaction. Such businesses need assurance that critical customer account information always will be available and that each transaction will transmit securely and reliably.

For the retail/POS industry, SonicWALL offers two different versions of a 10-node desktop security appliance with an integrated analog modem. These products feature an integrated VPN that supports both broadband and dial-up connections for maximum availability. The TZ 170 SP and TZ 170 SP Wireless support DSL with a back-up analog link.

TZ 170 SP and TZ 170 SP Wireless are the only products capable of providing broadband-to-broadband-to-analog WAN failover to ensure continuous uptime for IPSec VPN tunnels. This protects retailers from losing sales should their broadband connection go down. Using the integrated analog modem, the flexible TZ 170 SP/TZ 170 SP Wireless products let businesses choose between establishing an Internet connection via broadband or dial-up.

With a feature set tailored to address retail/POS requirements, the TZ 170 SP/TZ 170 SP Wireless incorporate all the basic capabilities desired in a business continuity solution. These products are highly cost-effective for organizations that don't require the full functionality of an enterprise package. The TZ 170 SP and TZ 170 SP Wireless are easy to deploy in POS locations and convenient to carry on the road for remote access. TZ 170 SP/TZ 170 SP Wireless support SonicWALL's award-winning Global Management System as well as SonicWALL's complete line of security services including gateway anti-virus, intrusion prevention, desktop enforced anti-virus and content filtering.

Conclusion

When shopping for a business continuity solution, look for products that provide:

- Network reliability via failover redundancy
- Ease of use
- Manageability/flexibility
- Enterprise-class features and functionality
- Excellent price/performance

SonicWALL offers solutions with ISP failover, VPN redundancy, WAN failover, load balancing, hardware failover and stateful synchronization technologies. Targeted to the specific needs of various sizes and types of organizations, these optional SonicWALL products comprise an integrated business continuity solution that protects the entire company, giving users peace of mind.

About SonicWALL

SonicWALL, Inc. is a leading provider of integrated network security, mobility, and productivity solutions for the SMB, enterprise, e-commerce, education, healthcare, retail/point-of-sale, and government markets. Core technologies include firewall, VPN, wireless, gateway anti-virus, intrusion prevention, desktop enforced anti-virus, and content filtering, along with award-winning security management solutions. Together, these products and technologies provide the most comprehensive distributed enforcement architecture available

The company has shipped over 500,000 units that protect millions of computer users. A growing number of respected analysts, editors, and other industry leaders cite SonicWALL's skill in delivering complete and manageable security solutions to a broad range of markets. SonicWALL delivers robust, affordable solutions including Internet security appliances, value-added security services and transaction security products geared to the needs of small- and medium-sized businesses.

SonicWALL backs its products with optional 24x7 technical support, in-depth consulting and design services, and Technical Training and Certification courses. These services are designed to help customers effectively plan, deploy and manage their security infrastructures.

*Support for bonus productivity enablers on TZ 170 Series appliances requires SonicOS Enhanced.