

An Intelligent Approach to Comprehensive Disaster Recovery

How to implement a comprehensive disaster recovery plan, while eliminating cost and complexity to provide an optimal return on investment

CONTENTS

A Recipe for Disaster	2
Comprehensive Disaster Recovery	3
Data Recovery—Challenges, Criteria and Considerations	3
Network Recovery—Challenges, Criteria and Considerations	3
Access Recovery—Challenges, Criteria and Considerations	4
An Intelligent Approach	4
The SonicWALL Disaster Recovery Solution	4
Data Recovery: SonicWALL Continuous Data Protection (CDP)	4
Network Recovery: SonicWALL Network Security	5
Access Recovery: SonicWALL Secure Remote Access (SRA)	5
Conclusion	6



Abstract

Any event that can disrupt workflow or destroy mission-critical information can have potentially disastrous consequences for a business. The three fundamental areas of vulnerability during a disaster are loss of data, loss of secure network connectivity, and loss of physical access to business locations. A comprehensive approach to mitigating the impact of potential disasters includes establishing quick, flexible and reliable solutions for recovering data, secure networking and remote access. Total cost of ownership (TCO) can be most effectively minimized by reducing or eliminating unnecessary cost and complexity out of every phase of purchasing, preparing and deploying a disaster recovery solution.

A Recipe for Disaster

What constitutes a business disaster? It might be as unexpected as an earthquake or as routine as a heavy winter snowfall. Today, whether an organization runs 24/7 with distributed operational facilities and markets around the world, or only services a single geographic region, disasters are inevitable no matter the size of the company.

Several types of events can precipitate business disasters:

- *Data destroyed:* Data systems can be destroyed by malicious sabotage, either by internal or external attackers, such as disgruntled ex-employees or hackers. Computing devices and storage equipment can be physically destroyed during hurricanes, tornadoes, fires, floods, earthquakes and other naturally-occurring events, or by accidental or structural failures such as spilled coffee, burst water mains, electrical fires, fire protection sprinklers or foams. Data can be destroyed accidentally by inadvertently overwriting or erasure, or simply be lost or orphaned when a laptop or other edge computing device is lost, stolen, or not recovered from departing personnel.
- *Networks downed:* Similarly, secure network environments can go down due to malicious attack, natural disasters, or accident. Downed networks not only impact access to data and conventional business applications, but also converged communications technology such as Voice over IP (VoIP) and teleconferencing. Compromised network security can threaten network resources and put businesses at risk of regulatory noncompliance. Servers can be corrupted or overwhelmed by denial-of-service attacks. Earthquakes can snap cables. Construction crews dig up fiber lines. Servers and storage systems can be destroyed in fires or floods. Without a secure network, distributed business sites like retail stores become isolated and non-productive islands.
- *Access denied:* Additionally, disasters can prevent physical access to primary or distributed business sites. A corporate site itself can be destroyed by earthquakes, fires or floods. A site may be rendered inaccessible due to power grid blackouts, gas leaks or broken water mains. Access can also even be prohibited by barriers to commuting, such as extreme weather, event-related traffic gridlock or spikes in fluctuating fuel costs.

Business must prepare for each of these event types by having flexible, reliable disaster recovery mechanisms already in place.

Comprehensive Disaster Recovery

In order to prepare for comprehensive disaster recovery, businesses do not need to entirely duplicate every existing system and process. However, they do need to provide a means to instantaneously or rapidly divert core business processes to contingency systems, which in turn are able to support those processes at normal capacities on a temporary basis until disaster conditions have subsided or been remedied. As required by internal, industry or governmental regulatory compliance mandates, such as HIPAA or Sarbanes-Oxley, these processes may also need to ensure the continuity of data security and transactional records.

As examined above, most businesses have three fundamental areas of vulnerability during a disaster: loss of data, loss of secure network connectivity, and loss of the ability to physically access business locations. For a business to recover from a disaster, IT must be able to restore mission critical data and applications to functioning operational environments. IT must also be able to re-establish secure networking between business functions. And IT must ensure secure network access to business resources even if physical sites are inaccessible.

Broken down to address these primary vulnerabilities, comprehensive disaster recovery is more specifically made up of three elements:

- Data Recovery
- Network Recovery
- Access Recovery

The following sections examine the underlying challenges, solution criteria and IT considerations for each of these fundamental areas of vulnerability.

Data Recovery—Challenges, Criteria and Considerations

Any backup is only as reliable as its ability to recover business data and applications when they are needed most. With legacy solutions, like tape and CD-ROM devices, backup is manual and might only happen once a day—instead of every time a file is updated—and only if systems are connected to the network or backed up to a central server. With unreliable legacy products, an important version of a business file or system setting update might not get backed up due to user error, forgetfulness or simply bad timing.

While 60% of business data on laptops and other edge devices, legacy backups don't let IT automate policies to ensure mobile and remote devices get backed up reliably and consistently. Many backup solutions do not provide the granular control to block unproductive files like MP3s that can consume bandwidth and storage space.

Businesses need to protect not only their data, but also the systems that access that data. Legacy systems like tape can make it difficult-to-impossible to recover applications and databases like Exchange, SQL Server or Active Directory, or full operating systems and settings from workstations and servers. Businesses also need the performance to backup and restore rapidly expanding volumes of data, while meeting stricter regulatory compliance for data archiving. And should disaster strike, IT needs the flexibility to immediately recover the most current data to new locations or computer platforms.

Network Recovery—Challenges, Criteria and Considerations

Network continuity disasters can be categorized between failures in either hardware or services. Businesses can establish hardware failover by providing two components that serve the same function (or redundant functionality within a single device). Should the active firewall fail, the passive unit automatically detects and assumes responsibility for securing traffic. Hardware failover can be used in "active-active" mode to enable load balancing, whereby the secondary connection not only provides redundancy but also enhances network performance by sharing the traffic load.

Many organizations establish WAN connectivity through third-party service providers. Stateful synchronization can provide automatic failover to a backup ISP connection if the primary connection goes down, which is of vital importance to retail/POS businesses. Similarly, 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. Tunnel transition must take place transparently, automatically and immediately without waiting for intervention from the administrator. In disaster scenarios, 3G wireless capability can be applied to support ISP and WAN failover from temporary or contingent locations.

Access Recovery—Challenges, Criteria and Considerations

Maturing mobile technologies, global markets and heightened focus on disaster preparedness has made secure remote access a business imperative. IT is now mandated with providing secure remote access over virtual private networks (VPNs) that are easy for users and cost-effective to implement.

Any disaster recovery implementation is not complete without a secure remote access solution because, during a business disruption, all network users could suddenly be working from home and other remote locations. Ideally, this solution must be able to handle a significant spike in remote access traffic when it is needed most, while still maintaining security and cost controls.

Additionally, clientless VPNs (e.g., SSL VPNs) are optimal in disaster situations, where client-based VPNs (e.g. IPSec VPNs) could be difficult or impossible to deploy. In a disaster, even if a company still has Internet access, established client-based VPNs could potentially 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.

An Intelligent Approach

Fundamentally, disaster recovery is a means to minimize the cost of a potential disruption in normal operations. By extension, business should also minimize the cost of the disaster recovery solution itself.

Total cost of ownership can be most effectively minimized by reducing or eliminating unnecessary cost and complexity out of every phase of purchasing, preparing and deploying a disaster recovery solution. An intelligent approach should:

- *Reduce upfront purchase costs*—by applying industry-standard platforms that are flexibly deployed and seamlessly interact with existing infrastructure
- *Reduce preparedness costs*—by streamlining management with intuitive administration and centralized control
- *Reduce recovery costs*—by speeding recovery time and minimizing operational downtime
- *Increase ROI* —by leveraging the value of disaster recovery technology to support standard operations and promote productivity

The SonicWALL Disaster Recovery Solution

SonicWALL® offers comprehensive disaster recovery solutions for any size organization. SonicWALL ensures data recovery with solutions for real-time, hands-free disk-based data backup for servers, laptops and PCs, as well as instant restoration from local or offsite locations to multiple platform types. SonicWALL ensures secure network recovery with multi-layered UTM firewalls featuring high-availability failover and flexible 3G wireless connectivity. And SonicWALL ensures access recovery with secure remote access solutions that enable isolated workers to remain as productive from home or other contingent locations as if they were in the office.

Because SonicWALL is committed to improving the performance and productivity of businesses by engineering the cost and complexity out of its disaster recovery solutions, SonicWALL solutions offer an intelligent foundation for any disaster recovery initiative.

Data Recovery: SonicWALL Continuous Data Protection (CDP)

SonicWALL CDP offers the only complete end-to-end disk-based backup and recovery solution for small and mid-size businesses, with flexible options to address any disaster recovery scenario. SonicWALL CDP takes the complexity out of safeguarding business data by automating tedious tasks to provide a true low-touch solution, with flexible Offsite Data Backup, Site-to-Site Data Backup, Local Archiving and Bare Metal Recovery options to address any disaster recovery scenario. Policy-driven CDP is transparent to the end-user, ensuring that data, applications and systems are reliably protected.

Because most recovery involves a single file, the self-directed restore of SonicWALL CDP helps meet service levels while reducing burden on IT support. CDP ensures that all files are available in multiple historic versions, and that all servers and its applications—including Exchange, SQL and Active Directory database—are protected with multiple-point-in-time versions for disaster recovery. With capacity up to 9 TB at typical compression, GbE connectivity, RAID 5, and field-replaceable components, CDP is designed to meet today's demanding requirements for performance and reliability.

An ideal alternative for tape-based backup systems, CDP provides foolproof, intuitive continual protection. CDP ensures reliability and speeds recovery by automatically generating e-mail alerts on any compromised connectivity and regularly-scheduled reports on backup activity. Extensible across multiple platforms including Windows and Linux®, CDP can instantly recover data, applications or entire workstation or server systems onto original, new or virtual devices. CDP secures data using industry-standard encryption anytime it is transmitted offsite, offering complete business information availability for servers, desktops and mobile laptops.

No other solution offers such comprehensive protection while still being so easy-to-manage.

Network Recovery: SonicWALL Network Security

SonicWALL Network Security solutions incorporate multiple security technologies in a single platform to provide higher performance protection, reliable communications, low total cost of ownership and flexible connectivity options. Other existing network security solutions can be technologically limited, notoriously expensive or painful to deploy and use. SonicWALL eliminates these concerns by focusing on engineering the cost and complexity out of a high-performance security infrastructure. This frees business resources to be more productive.

SonicWALL offers network security appliances that can ensure continuous uptime for IPSec VPN tunnels by automatically failing over to an alternate WAN connection should the broadband connection fail. Once the broadband is re-established, the network security appliance fails back, providing the best connection speed possible. SonicWALL also provides network security appliances¹ featuring optional 3G wireless broadband, enabling network access in an instant without the need for a fixed Internet connection.

For added flexibility in disaster scenarios, the SonicWALL Secure Distributed Wireless Solution flexibly and rapidly scales to fit any deployment by simply distributing SonicPoint-N Dual-Band™ 802.11n wireless access points throughout a site location. SonicWALL network security appliances automatically detect and configure SonicPoints as they are added, to deliver seamless, secure wireless LAN (WLAN) connectivity and advanced security features and services.

Access Recovery: SonicWALL Secure Remote Access

SonicWALL Secure Remote Access solutions already play an intrinsic role in overall disaster recovery planning for many enterprises, serving as a secure application access gateway at main data centers, ensuring a model of redundancy at the data center, and serving as a gateway to hot, warm, or cold disaster recovery (DR) facilities. Because SonicWALL offers the easiest-to-use and easiest-to-control SRA solutions available, it is perfect for network managers who need to provide their users with secure remote access, under any circumstances.

The SonicWALL Aventail® E-Class Secure Remote Access (SRA) Series of clientless SSL VPN solutions delivers secure, easy-to-manage remote access control for the mobile enterprise, supporting up to 2,000 concurrent users from a single appliance. These solutions increase user productivity and maximize IT control by providing authorized access to any application from a broad range of cross-platform devices. Built on the powerful, proven SonicWALL Aventail SSL VPN platform, the solutions provide access control by first detecting the security of the endpoint; protecting applications with granular policy based on who the user is and the endpoint used for access; and then connecting authorized employees and business partners effortlessly from a broad range of cross-platform devices only to authorized resources.

The SonicWALL Secure Remote Access (SRA) Series provides small-to-midsize business (SMB) teleworkers with an easy, affordable and scalable solution for clientless secure remote access to email, files, intranets, applications, remote desktops, servers and other wired or wireless network resources, over a standard Web browser.

SonicWALL Virtual Assist provides a clientless remote support tool for SonicWALL E-Class SRA and SRA Series solutions that enables an IT technician to assume control of a teleworker's PC or laptop in order to provide technical assistance. With the teleworker's permission, the technician can gain instant access to the computer using a Web browser, making it easy to diagnose and fix a problem remotely without the need for a pre-installed "fat" client.

In addition, SonicWALL Virtual Access functionality enables authorized end-users to gain secure remote access to their unattended Windows-based computers from anywhere. Moreover, SonicWALL Web Application Firewall offers a subscription-based service that employs a dynamically updated signature database to protect against modern Web-based threats.

Conclusion

Every business is vulnerable to potential disaster. Yet organizations are additionally challenged by increasingly limited budgets and resources. Disaster recovery does not have to be overly costly or complex. It just has to be done right.

Incorporating easy, flexible and affordable Continuous Data Protection, Network Security, and Secure Remote Access, the SonicWALL Disaster Recovery Solution offers any business an intelligent framework for disaster recovery preparedness.



SonicWALL, Inc. 2001 Logic Drive, San Jose, CA 95124 T +1 408.745.9600 F +1 408.745.9300 www.sonicwall.com

©2010 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice. 06/2010