

The Remote Access Imperative in Disaster Recovery

**Tim Clark, Partner
The FactPoint Group**

May 2006

**300 Third Street, Suite 10
Los Altos, CA 94022
650-233-1748
tclark@factpoint.com**

Executive Summary

Recent natural disasters, terrorist activities, and the avian flu outbreak have pushed disaster recovery to the forefront for governments and enterprises. However, disaster recovery does not just refer to catastrophic events. It could be something as simple as a snow storm, power outage, local celebration, or another event that keeps your workers from getting into the office. No matter what instigates the business disruption or how extreme it is, the business impact remains the same. Disruptions to normal business operations often result in missed opportunities, lost revenue, and a damaged reputation.

Every enterprise's goal in disaster recovery is business continuity—to keep core business functions operating under all circumstances. That's more and more challenging, as business threats now derive from a broad range of internal and external factors, both natural and man-made. The expected response time to a business disruption has also accelerated—employees, partners, customers, and regulators expect immediate resolution.

Disaster recovery spans many sectors of an enterprise, both physical and digital. For many organizations, disaster recovery has meant establishing clear telephone and communication links and ensuring a data storage, back-up, and recovery plan is in place. One of the most critical aspects of a disaster recovery plan is enabling employees, partners, and other constituencies to work from home or other remote locations and access critical resources and data as if they were in the office. If a disaster recovery plan does not include remote access, “business as usual” is virtually impossible.

Remote access is key to disaster recovery because typical business disruptions keep employees and other users away from the office and the local area network (LAN). For example, in the case of a widespread health crisis such as avian flu, employees may be forced to stay home because of official quarantines and travel restrictions. For organizations with a remote access solution, however, isolated employees can work productively from home as if they were in the office.

One technology has emerged as the leading solution for remote access: SSL VPNs—virtual private networks utilizing secure sockets layer (SSL) security protocols. SSL VPNs are best suited for secure remote access during an emergency because they allow workers and partners to connect safely through the Internet to corporate network

Disaster Recovery and Remote Access: A CIO Primer

- A botched disaster response can hurt revenue and the corporate brand.
- Regulatory mandates on auditing sensitive data do not disappear during a disaster.
- Secure remote access plays a critical role in disaster recovery plans.
- Equipping the backup data center with an SSL VPN appliance keeps business processes running during a disaster event.
- A low-maintenance SSL VPN reduces demands on IT in disaster recovery.

resources. This document explores best practices for disaster recovery and the role of SSL VPNs in that process.

Business drivers of disaster recovery planning

An enterprise must anticipate and plan for potential disasters. You can't start from scratch on the day of a disaster. At that point, it's too late. During a disaster, the inability to operate normally or provide access to critical resources can hurt revenue, damage a company's reputation, or mar the corporate brand. This is why responsibility for the once-mundane matter of disaster planning has risen from middle management to the highest echelons of the corporate hierarchy. A strong disaster recovery plan requires the involvement and commitment of both technology and business sides of an organization.

Business drivers for disaster recovery planning include:

- **Protecting the revenue stream:** A business interruption can result in lost revenue, customers, and business opportunities. That hurts virtually every stakeholder—investors, customers, employees, and partners.
- **Strengthening competitive positioning:** With an effective disaster recovery plan, you can position your company as a reliable partner or vendor, providing your customers and partners with assurance that you will continue to operate even during a disaster.
- **Maintaining productivity:** No one can foresee the specifics of a disaster, but since virtually all businesses rely on information and the network, keeping access available—and workers productive—is crucial. Don't limit access to employees. Customers, suppliers, business partners, and other third parties also may need secure remote access to appropriate corporate resources during a business interruption.
- **Assuring regulatory compliance:** Regulatory requirements such as Sarbanes-Oxley, HIPAA, and Basel 2 don't go away just because of a disaster. Organizations worldwide must ensure secure, auditable access to key

Chicago Housing Authority (CHA)

The CHA is a local government agency responsible to both the city of Chicago and the U.S. Department of Housing and Urban Development (HUD). The CHA found itself with a growing base of users and no way to ensure secure, remote access for all of its users within budget. The CHA needed a solution that enabled granular access to ensure the different user groups only accessed appropriate resources.

George Stephenson, Security Officer at the CHA, researched several options and concluded that an SSL VPN was the technology the CHA needed. Features of the SSL VPN that were particularly important included end-point control functions, such as device interrogation before the user authenticates to ensure the system can't be attacked by keystroke loggers or other security threats.

As part of its disaster recovery initiative, the CHA placed one of its Aventail SSL VPN appliances at its backup data center to ensure redundancy of its network. Now, whenever the main center goes down or there are other business disruptions, all CHA remote users are automatically redirected to the backup data center. For the end users, there is no difference in how they access and no latency issues when connecting.

information assets to maintain compliance, even during business disruptions. These include Gramm-Leach-Bliley in the U.S., the European Union's Directive on Data Protection, and Japan's Personal Information Protection Act.

- **Reducing risk and security threats.** During a business disruption, your organization is vulnerable to hackers and other security threats. A secure remote access solution protects your intellectual property and critical corporate resources. By allowing authenticated users access only to specifically authorized resources, you ensure that those who need the information get it quickly, and those without authorized access are kept out.

Technology requirements for disaster recovery planning

To achieve these business goals and a successful disaster recovery initiative, your remote access solution should adhere to these key technology requirements:

- **Easy to deploy** – Let all users access the VPN from a Web portal page from the company Web site or other URL that everyone knows. The solution should also be easy to use and easy to manage, since a disaster is not the time for extensive training.
- **Quickly scalable** – Allow IT staff to scale the remote access quickly to accommodate a spike in VPN traffic. With a disaster, all users could now be remote, and the solution should have adequate capacity plus failover capability to ensure no downtime.
- **Access to all applications** – For successful remote access, during an emergency or not, users must be able to access all appropriate network resources, including Web-based applications, file shares, client/server applications, Windows Terminal Services, etc. A solution that supports Web conferencing and VoIP is also important during an emergency, since traditional phone systems may not be working.
- **Highest Level of Security** – Don't sacrifice privacy or security to maintain business as usual. By placing an SSL VPN at the perimeter of the data center and leveraging its policy controls, enterprises can closely control who accesses which information and block unauthorized access. Establish all access controls beforehand, so when a disaster strikes, the security policies are in place.
- **Ensure Compliance** – Keeping a clear audit trail of who is accessing which information could become even more important during a disaster. An SSL VPN can provide granular access controls to ensure only authorized users can access resources and provide auditing and reporting of that access

What triggers a “disaster recovery event”?

Disaster recovery means planning not only for major disasters but also for more common emergency situations. Don't assume that only once-in-a-lifetime events—a 100-year flood or terrorist attack—require an emergency response. Disaster recovery planning means preparing for those not-so-extraordinary situations that thousands of companies face every day when something unexpected disrupts normal business operations.

Some activities that can trigger a “disaster recovery event” include:

- **Health crises:** Global pandemics like the avian flu, as well as regional epidemics and other public health crises, can cause major business disruptions, including quarantines, travel restrictions or evacuations. More employees may need to work remotely from home, so as not to risk exposure or potentially spread disease. Employees and partners also may need secure remote access to temporarily relocated business resources. For a business checklist of preparations for a flu pandemic, see <http://www.pandemicflu.gov/plan/businesschecklist.html>. Many apply to other disasters too.
- **Natural disasters and catastrophic events:** It does not take a tsunami or a tornado for Mother Nature to wreak havoc with your business. A fire at a data center, a heavy rain or snow storm, or a lightning strike can turn a normal business day into a crisis. These incidents may keep employees at home, interrupt power supply or result in a breakdown in the supply chain—all of which disrupt everyday business operations.
- **Technology outages:** Weather is not the only reason power or other utilities shut down. A car accident may affect a power grid or a hot summer season could lead to brown-outs. Even a phone or Blackberry outage can hinder operations. Organizations with a strong disaster recovery plan ensure that all network users can be redirected immediately to a redundant data center that backs up corporate resources.
- **Cyber attacks:** A cyber attack on your network could slow or cut e-mail communications. A hacked e-commerce Web site can mean an instant hit to a merchant's revenue. For a just-in-time manufacturer, a supply chain interruption could prevent filling a key customer's order or push the revenue into the next quarter, causing the manufacturer to miss its earnings target. Address all of these risks in the disaster recovery plan.
- **Governance crises:** On a more systemic level, consider the risk of a corporate governance crisis when a partner loses the personal data of millions of your customers. A disaster recovery plan must address how to determine the cause, how to inform customers, when to go public with the information, how to prevent a recurrence, and how to repair the company brand afterwards.
- **Outsourcing issues:** Outsourcing opens the company to security breaches, missed deadlines, distant events, and quality problems from an outsourcing partner. In other words, the resiliency of your supply chain becomes critically important during an

emergency, so you may need to dictate backup plans to your suppliers to cover any disaster. And your customers or partners may impose the same requirement on you.

- **Lost computers:** An executive who loses a corporate laptop computer also can initiate a disaster response. First, the missing laptop must be blocked from accessing the corporate network—you must assume it's in unfriendly hands. Then, the executive may need to access sensitive data on your network from a less secure or unmanaged device.

The role of SSL VPNs in disaster recovery

With today's heavy reliance on information, maintaining access to critical resources during a business interruption is fundamental. This is true across all industries and company sizes—from a small insurance office to a multinational manufacturing enterprise. Secure sockets layer virtual private networks (SSL VPNs) have emerged as the technology of choice for secure remote access.

The benefits of an SSL VPN for disaster recovery include:

- **SSL VPNs are clientless:** No special software or configuration is needed. SSL VPNs can be used from devices not managed by your IT department, including airport kiosks and home PCs, which reduces support burden and costs.
- **They work from any Internet browser:** This makes access easy from both managed and unmanaged devices.
- **SSL VPNs operate at the application layer:** There is never a direct connection to the network, so users only connect to the resource.
- **SSL VPNs enable finely grained access controls:** A user connects to the SSL VPN appliance and— after valid authentication—can only access resources for which he or she has access privileges.
- **SSL VPNs have strong end point security:** The device is interrogated to ensure identity and its state of security and allowed appropriate access or denied access based on the information.
- **They provide strong encryption:** With an SSL VPN, the entire data stream is encrypted using SSL—the security protocol used for Internet traffic.

Disaster recovery infrastructure—a model of redundancy

Redundancy is the model to follow for disaster recovery and remote access. Maintain a completely redundant backup data center in addition to your main corporate data center. A remote access solution, such as the Aventail® SSL VPN, should be at the perimeter of each of these data centers to assure only authorized access to critical applications. (See Figure 1.)

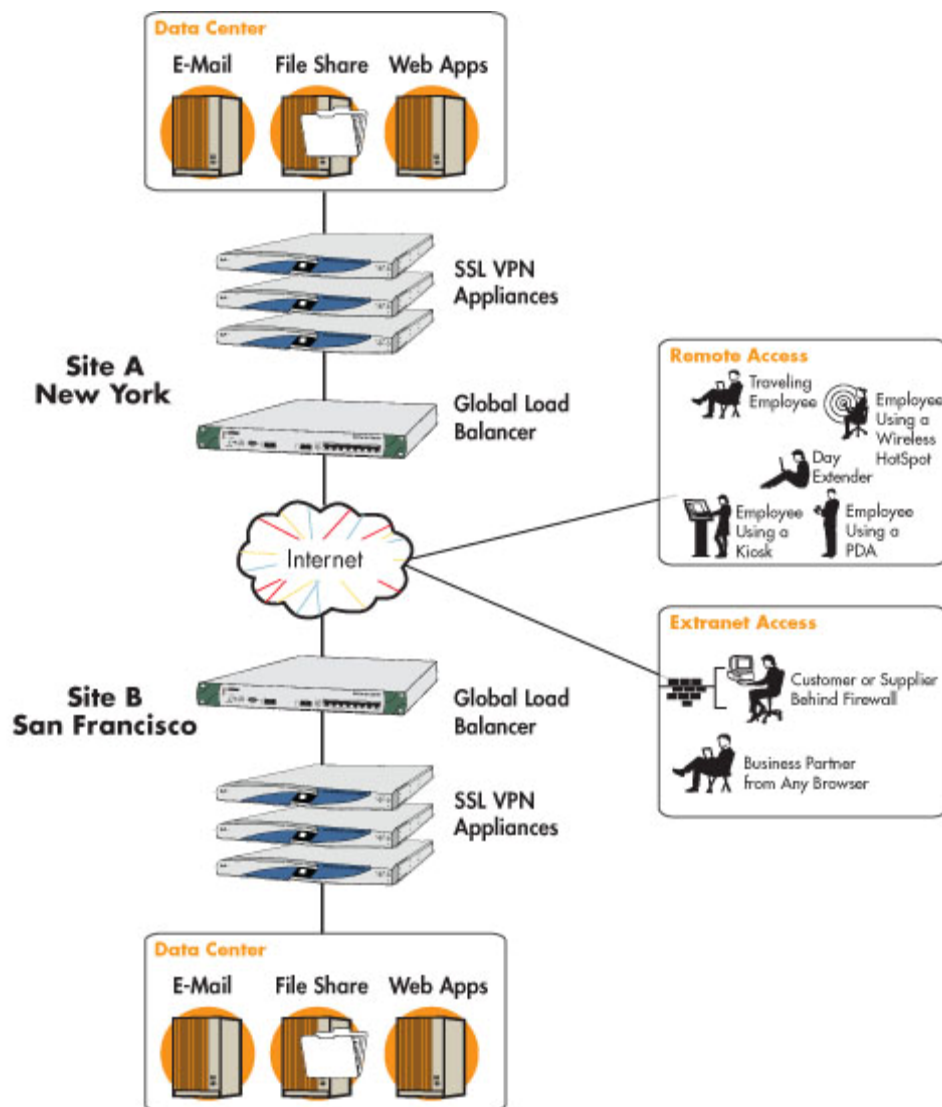


Figure 1. Following a redundancy model for disaster recovery, an Aventail SSL VPN can help ensure that users have access to the resources they need at any time. If the main data center goes down due to a business interruption, all users can be pointed to the backup data center via the portal.

Conclusion

As organizations prepare a disaster recovery plan, it's important to include remote access as a fundamental part of the disaster recovery infrastructure. During a disaster or other business interruption, the ability to access critical corporate information and maintain productivity is more important than ever. What's more, a remote access solution can help protect your revenue stream and guard your company's reputation.

Secure remote access allows employees, customers, and partners to access key data and applications on the network without being at a company facility. It enables access from anywhere, on any device, via any Internet connection while maintaining absolute security from internal and external threats.

By guarding the revenue stream and keeping the business running during a crisis, the disaster recovery plan protects the corporate reputation. That makes the company a stronger, more reliable vendor and partner—creating competitive advantage over less-prepared rivals. The disaster recovery plan also meets regulatory requirements for audit trails on sensitive or protected information. Having secure remote access in the disaster recovery plan reduces the burden on IT when an event does happen.

But all those benefits depend on one thing—advance planning.

About SonicWALL

SonicWALL® is a recognized global leader in secure networking infrastructure and data protection. The company designs, develops and manufactures solutions that provide comprehensive network and data protection including network security, secure remote access, Web and e-mail security, and backup and recovery. With appliance-based solutions—as well as value-added subscription services —SonicWALL’s rich portfolio of solutions delivers the comprehensive enterprise-class Internet and data protection necessary to safeguard organizations of all sizes. In July of 2007 SonicWALL acquired Aventail Corporation, a leading SSL VPN solution provider. For more information, go to www.sonicwall.com.

About Aventail

Aventail is the best-of-breed SSL VPN product company, delivering the easiest secure remote access solution for today’s mobile enterprise. With more than two million end users around the globe, Aventail is the SSL VPN of choice among mid to large-sized organizations worldwide, including AT&T, the Environmental Protection Agency (EPA), Chicago Housing Authority, DuPont, Radiology Ltd, James Richardson International, Organization for Economic Cooperation and Development (OECD), Overlake Hospital, IBM Global Services, and hundreds more. For more information, go to www.aventail.com.

Aventail Secure Access for Disaster Recovery

The Aventail SSL VPN enables enterprises to immediately provide all employees, partners, and other users access to critical network resources from any device and any network environment. Since Aventail provides clientless access, no special software is needed, and users do not need to be working on a managed device to gain access. Aventail is working with many of its partners and customers on developing and implementing disaster recovery plans that include a strong remote-access solution. The depth and breadth of Aventail’s SSL VPN ensure remote access to the corporate network during a disaster recovery event. Aventail has the broadest application reach to all resources, including Web, client/server, server-based, host-based, and even complex applications like VoIP. For users, the Aventail SSL VPN is easy to use, with transparent secure access from any network environment or device - including Linux, Mac, Windows, and Windows Mobile. Network managers are assured the highest level of security with Aventail End Point Control, which provides the ability to enforce policy based upon IT’s level of trust for the remote user and his or her environment. Aventail’s solution scales from 5 to 5,000 users or more with either an integrated or external load balancer—making it as easy to manage all users, from just a few to hundreds or thousands.

About the FactPoint Group

The FactPoint Group (www.factpoint.com) is a boutique market research and consulting firm in Silicon Valley specializing in the early adoption of new technologies. The FactPoint Group has been producing world class research, analysis, and consulting since 1993 and continues to help enterprise software vendors and enterprise customers sell and use new technology solutions. Tim Clark is co-founder and partner at FactPoint. Recently, his research has focused on disaster recovery, utility computing, network security, sensor networks, open-source licensing, enterprise blogs and wikis, and Web services. Previously, Clark was senior analyst with Jupiter Media Metrix and Net Market Makers. Before becoming an analyst, Tim was a reporter and editor for 24 years, working as senior editor and columnist for CNET's News.com, where he covered e-commerce and Internet security.

©2007 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc.

© 2007 Aventail Corporation. All rights reserved. Aventail, Aventail End Point Control, Aventail Smart Access, Aventail Smart Tunneling, Aventail Unified Policy, and their respective logos are trademarks, registered trademarks, or service marks of Aventail Corporation. Other product and company names mentioned are the trademarks of their respective owners.