

Business Continuity & Disaster Recovery: *Why You Should Consider An SSL VPN As Part of Your Overall Plan*

By Hari Krishnan

Access to corporate applications and data is obviously vital to help keep a business running as usual. A wide range of concerns – ranging from a snow storm that prevents people from coming to work to site failures that can prevent access to information systems – can quickly disrupt business processes. The business impact itself can be significant, leading to poor customer service, loss of credibility and brand, as well as loss of revenue and market share. Businesses need to consider remote access as a key element of their continuity planning to ensure their employees can continue to work remotely should disaster strike at the corporate office.

Real-Time Remote Access During A Disaster: If you look at any organization today, there's a wide variety of business processes and applications – including customer support, manufacturing, and accounting -- that rely heavily upon real time access to information. Yet there are a wide range of disasters that can easily disrupt these processes – essentially preventing people from physically coming into the office. Obviously, a breakout of the avian flu would represent one such disaster, but there also other, more common disasters such as a major snowstorm or hurricane. A disaster can also be defined as simply as an application or site being down. The effects of this downtime can be significant in terms of your ability to provide customer service, not to mention a loss of credibility and business reputation and the associated loss of revenue.

It's therefore very important to consider a remote access solution as a key element of any disaster recovery or business continuity plan. This will ensure that people can get access to information, with minimal disruption to business processes, allow your employees to continue to work remotely from any location, and ensure that your business partners or suppliers gain uninterrupted access to important information.

What To Look For: From a business continuity and disaster recovery standpoint, there are some key elements to look for in choosing a remote access solution. The basic question to first look is the type of remote access solution you need. In the past, many organizations used IPSec VPN remote access solutions to provide secure access to applications. However, over the past two years, a new technology has emerged that solves the cost, complexity and predictability problems commonly associated with IPSec. Keeping with technologists' love for acronyms, the solutions are called SSL VPNs (Secure Socket Layer Virtual Private Networks). All a company needs to support this type of access is a PC, laptop, PDA, or cell phone that has an Internet browser installed.

The SSL VPN allows travelers, business partners, and home office workers to reliably and securely access email and other applications from various types of devices, anywhere in the world, anytime. Also, because SSL VPNs utilize encryption capabilities that already come built into Web browsers, they don't require separate software installation and maintenance on each user device beyond the browser. This eliminates the deployment and ongoing support costs of traditional remote VPNs that require client software to be loaded on every device.

Another advantage with SSL VPN is that it's a very flexible solution. You can provide access not only to your employees, but also to your partners and suppliers. And they can gain this access from their own machines, without having those machines managed by your organization.

Because SSL VPNs allow you to provide access to a wide range of devices and users, it's important to be able to set appropriate access policies – to make sure users are coming from trusted devices, and are authorized access to appropriate resources. With SSL VPNs, you can set a wide range of very granular policies to allow access to specific resources, based not only on who the user is, but also based upon which devices they are coming from – from a corporate laptop to a kiosk.

Why Ease of Deployment Is Critical: SSL VPN solutions are also very easy to deploy, and during times of disaster, this is very important. If disaster strikes, you won't have much time to roll out any kind of software or perform a client installation, especially when dealing with a large amount of end users. With an SSL VPN solution, you can pre-define your access policies and pre-provision your users up front, so you can immediately "hit the switch" when you need to, and your remote access system is ready to go.

Before a disaster, from a user perspective, there are three things that you need to make sure that your users have. One is obviously a device they can use to access the Internet and the applications. Second, employees or partners need a URL that they know is available so they can log in. Often this URL can be set up and disseminated up front, or used in a backup site in case the primary site goes down during a disaster. Finally, you need a way to distribute user credentials. If you are using strong authentication such as Secure ID, you can easily send these tokens before a disaster hits, so users can quickly access their credentials during an emergency.

Another thing to look for in any remote access solution revolves around your performance and scalability requirements. During a business-as-usual scenario, you may have a very small fraction of people who are simultaneously and remotely accessing your applications. However, during times of disaster, the numbers can be much higher, so your scalability requirements can be much larger. It's therefore important to plan for these peak capacities and have this notion built into your overall contingency plan so your network can accommodate these increased numbers when the need arises.

What If Your Entire Site Goes Down? But what if your entire site goes down during a flood, hurricane or earthquake? You obviously lose the ability to provide remote access to your applications. That's why *availability* is just as important as *accessibility*. Typically, businesses have some sort of backup data center, where they have their applications provisioned. But you also need an infrastructure device that lets you direct users to the best performing site or most available site should one of them go down. There are traffic managers available that can virtualize your applications and sites, so you can quickly redirect the users to the appropriate site based upon the proximity, or the availability of the applications. Essentially, you can set policies that ensure users can get to the application despite a site failure.

Summary: Remote access is an important part of any business continuity or disaster recovery plan. Accordingly, SSL VPN devices are an effective way to provide remote access during a disaster, specifically in the flexibility they provide in not only offering secure access from managed corporate machines, but also from unmanaged computers such as home PCs, or even public machines like kiosks. SSL VPNs also very easy to set up and manage – you don't have to push out a client to each end user's machine – which can save a lot of time and effort. Finally, it's important to consider availability when considering accessibility, in case an application or even an entire site goes down. In this regard, traffic managers represent another important piece of the puzzle should disaster strike.



Hari Krishnan is a Product Manager at F5 Networks. He can be reached at H.Krishnan@f5.com



THE WORLD RUNS BETTER WITH F5.