

## Preparing for Emergencies: Using SSL VPN Technology to Ensure Business Continuity

Businesses of all kinds are drafting plans for disaster preparedness. Recent events – from natural disasters to terrorist threats - have convinced many IT professionals that emergencies may no longer be a question of “if” but rather “when.” In truth, most organizations will never experience full-blown catastrophe. However, even an electrical outage, bad weather, highway closure, or network disruption can keep workers from reaching the resources they need, endangering a company’s reputation and financial stability.

As a result, many organizations are putting Continuity of Operations (COOP) programs in place for use during emergencies. These plans may include redundant systems, offsite data storage, backup processes, and geographically dispersed datacenters, which reside beyond the boundaries of a localized event. These investments form the building blocks of a Disaster Recovery (DR) plan. However, these tactics are meaningless if employees can’t reach their offices or get access to the organization’s Local Area Network (LAN).

That’s why secure, portable remote access is the cornerstone of an effective DR plan. In a crisis, having fast access to crucial applications and resources regardless of time, place or circumstance can make the difference between continuity and catastrophe.

This paper describes the key technology elements required to run a fail-safe disaster recovery system with browser-based SSL VPN technology. By presenting real-world examples—such as a field hospital set-up outside New Orleans for victims of Hurricane Katrina—we’ll address technical requirements for implementing a disaster-ready remote access solution, and introduce the AEP Netilla Security Platform (NSP), a leading SSL VPN from AEP Networks, as an ideal approach for ensuring business continuity regardless of conditions or events.

## Ensuring Business Continuity through SSL VPNs

---

Remote access products used to sustain an organization during a crisis shouldn’t be bolted-on solutions for emergency use alone. They must form a key component of an organizations’ IT infrastructure. According to Gartner, “remote access is not an accessory network; it is an extension of mission-critical company IT services, and it needs to work correctly under random circumstances” (Gartner, John Girard, “Ten Remote Access Failures Your Company Could Avoid in an Emergency”, November 2005). In other words, employees cannot be expected to negotiate an unfamiliar technology at the height of an emergency; they need to be familiar with the solution as part of their normal work routine.

As such, the best DR plans integrate technologies that meet business-level objectives – such as improving employee efficiency, decreasing IT and help desk costs, and lowering overall Total Cost of Ownership (TCO) – while also providing a lifeline to vital resources during a crisis.

For these reasons, SSL VPNs have emerged as a logical and popular choice for business continuity and overcoming catastrophic events. With their low costs, application access flexibility, high security, and overall simplicity, SSL VPNs are well suited for the diverse remote access needs of today’s enterprise, while satisfying the unique demands during emergency situations.

Some compelling drivers that have established SSL VPNs as the ideal foundation for DR plans include:

**Portability through web-based accessibility:** SSL VPNs allow authorized users to log in from any web-enabled device (PCs, Macs, mobile PDAs and smartphones). This level of transportability lets users gain access to business-critical resources from devices completely out of the control or reach of an IT department. This approach is well suited for a typical emergency situation where workers may be trapped at home and unable to get to the office. SSL VPNs have an edge over IPSec VPNs in this scenario because employees without company-issued laptops or devices with VPN clients can still work from home on their own devices.

**Protecting the network through proxy technology:** DR solutions must ensure that an organization's key business assets remain fully protected at all times, and are not compromised during the confusion that often results in a crisis. SSL VPNs like AEP Networks' NSP mitigate these concerns through the use of application layer proxy technology. This means that application resources run in "virtual" sessions, inside the user's browser, rather than in local sessions on the user's computer. The application terminal servers and web servers themselves remain on private, non-routable IP addresses, are never directly exposed to the public Internet, even during an emergency. Internal addresses that do not resolve publicly can be safely and securely accessed over any Internet-connected device, while private network resources remain safe behind the SSL VPN appliance.

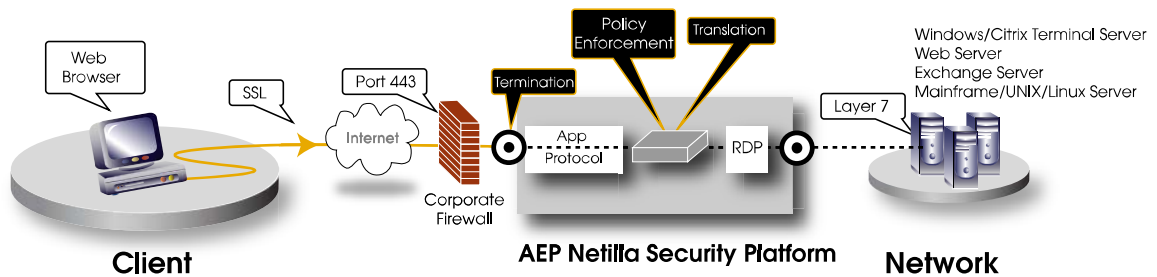
**Policy-based identification and authorization:** During a crisis, organizations must make certain that critical business, financial, healthcare or government assets are restricted to only users who need these resources. By their very nature, SSL VPNs protect the integrity of the network at all times – even during emergencies – through fine-grained access controls based on identity. This ensures that only authorized users can access – or even know about – the applications that they have been expressly permitted to use. These authentication technologies focus on authenticating actual users as opposed to devices, a definitive advantage for DR situations where access may occur from a variety of changeable locations.

**Meeting regulatory requirements:** Organizations with stringent regulatory mandates must maintain their compliance commitments at all times. Many regulatory mandates, such as HIPAA for the healthcare industry or Sarbanes Oxley for financial services, include rules that compel organizations to have critical systems back up and running at full capacity during or shortly after a disaster, while ensuring the confidentiality of information.

**Replicating the office through server-based computing:** Many SSL VPNs have been designed to deliver secure access to web-based applications. The NSP offers this functionality but also goes further by giving users secure, proxy-based access to Windows, Citrix, UNIX and mainframe applications

through a web browser. The NSP supports these environments through the use of an automatic “client push” approach.

As shown in Figure 1, when a user connects to the network for the first time, the NSP can package a Java applet that contains everything that particular client needs in order to connect to the network applications. Administrators therefore do not have to send each user disks to install a driver onto the machine, and end users are not required to do anything other than click an icon; the NSP provides the appropriate client seamlessly and without administrative intervention.



**Figure 1: Application Layer Proxy Technology**

This approach is also well suited for web-based intranet applications and portals, where the NSP terminates, examines, and rewrites HTTP requests (no Java applet is required in this circumstance).

Authorized remote users now gain instant, clientless access to key business applications, and do so from any location. By incorporating remote printing, client drive mapping, and web-based file server access, the NSP effectively recreates the main office environment from any authorized computer, meeting a vital requirement for business continuity.

**Enforcing corporate policy through endpoint security:** Opening up your network for access from various locations outside of your IT department’s control can create new risks of digital leakage and endpoint threats. SSL VPNs can address these concerns through an integrated endpoint security solution, ensuring that remote PCs adhere to corporate security policy before they gain access to your network. The NSP adds key security features like cache cleaning, a secure virtual desktop, adaptive policies and host checking, helping to mitigate remote access dangers and providing a portable, end-to-end security solution.

### Remote Access Helps Doctors Do Their Jobs During Hurricane Katrina Disaster

*In August 2005, New Orleans experienced full-scale tragedy. When Hurricane Katrina hit the city and surrounding area, everything was wiped out, including hospitals. With so many injured by the hurricane, temporary emergency hospitals were set-up in the surrounding area. The Thibodaux Regional Medical Center—55 miles from New Orleans—established one of those emergency hospitals to care for Hurricane Katrina victims.*

*Thibodaux Regional worked with the Red Cross, which had created a makeshift hospital in dormitory rooms at the local university. Doctors worked at the university ‘hospital’ to triage patients. Thibodaux used the AEP Netilla Security Platform SSL VPN solution to give doctors remote access in the emergency hospital. Having remote access meant doctors could sign-on to the network and applications from the makeshift hospital to access to patient information, laboratory results, and other protected health information. As a result, turnaround time for patient care was quick.*

*“Emergency response after the hurricane hit was critical. If it hadn’t been for remote access from AEP, doctors and labs wouldn’t have been able to connect with the hospital. By setting up remote access, we lessened the ‘life or death’ situation,” said Terry Evans, CIO of the Thibodaux Regional Medical Center.*

*The temporary hospital created after Hurricane Katrina has been dismantled, but it was a great lesson on disaster recovery, says Evans. “We have the capability to establish access anywhere. Because there are other local hospitals using AEP Networks’ NSP/MEDITECH environment, we could quickly port our data and provide access through their network in the event our facilities are ever affected by other storms.”*

## Planning Your Infrastructure: Geographical Diversity

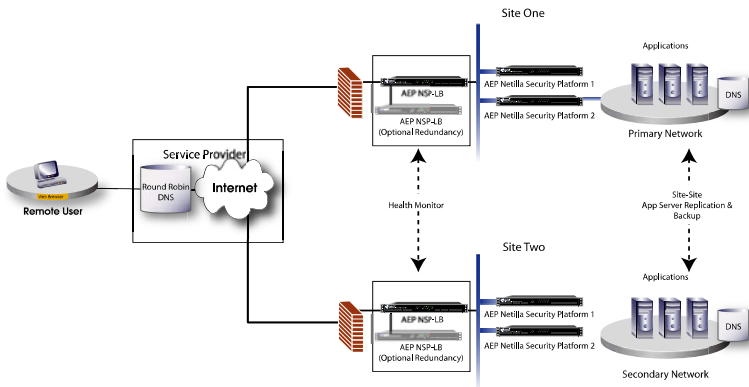
Many organizations have wisely deployed multiple datacenters in geographically-dispersed locations to improve resilience in case one or more datacenters become unavailable. It is therefore important that the application access infrastructure that will sustain an organization during a crisis be able to support this kind of arrangement.

The NSP, which supports local clustering using the AEP Netilla SSL VPN Load Balancer (NSP-LB) for scale and high availability, also extends this technology for geographical diversity. This approach provides load sharing and failover between independent NSP clusters in physically disparate data centers, enabling the transparent delivery of application services and resources across multiple locations. In this scenario, any designated backup facility (active/active or active/passive) can take over operations instantaneously, allowing remote users to continue to work with key resources regardless of the local situation.

As shown in Figure 2, a cluster of NSPs is configured with an NSP-LB at one datacenter, while a second cluster is located at another geographically located site (there is no theoretical limit to the number of data center sites that can be tied together). System health information is sent between the NSP Load Balancers at each site. If one site should become



unavailable – or even begin to exhibit performance degradation - users are automatically redirected to the alternate site, providing seamless continuity in the case of a disaster.



**Figure 2: Geographical Diversity and Load Sharing**

**Insuring Against the Unknown:  
Disaster Recovery Demand Licensing**

A sound remote access strategy represents a strong defense against disaster. Just as important is ensuring that your access solution is flexible enough to meet sudden spikes in demand that will accompany emergency situations. During a localized event, an organization must be prepared to accommodate a larger number of users quickly, but for a relatively short period of time.

For this reason, AEP has crafted a Disaster Recovery Demand License. This program provides a cost-effective insurance policy to meet expanded demand by adding additional capacity on short notice to an existing NSP deployment, above and beyond the capacity defined for everyday use. Organizations can subscribe to the service by paying a small up-front fee, representing a fraction of the cost of access licenses. In the case of a DR event, AEP’s 24x7 customer care team can immediately initiate the expanded license pool, providing seamless expansion to accommodate the increased user environment.

This approach is well-suited for both active/passive and active/active availability. In an active/active arrangement, where multiple production datacenters are tied together for greater capacity and scale, the NSP-LB monitors the performance and availability of each NSP cluster at each datacenter location, managing users’ requests and intelligently directing users to the most appropriate location based on performance, hardware status, or other health-related variables. Should the NSP-LB sense deteriorating performance, it will alert the IT staff that a failure is imminent and begin moving new users to a more appropriate cluster of NSPs, as defined by policy.

In an active/passive scenario, the same intelligent monitoring senses the health information of the main site, and immediately activates the DR site for application access should a failure occur or appear likely to occur at the main location.

---

From the remote workers' perspective, there is no change to the methodology or process employed for access; logging in remains as simple as launching a web browser to the same URL as before the emergency. On the backend, the NSP-LB's negotiate the connection and move users to the most appropriate - or available – application environment for fail-safe business continuity.

The NSP thus delivers a vital lifeline – seamlessly and without interruption – between remote workers and key application resources, even if an entire datacenter or multiple datacenters become unavailable. Note that multiple NSP-LBs can also be clustered at each datacenter, eliminating single points of failure and ensuring that your organization can meet any crisis with confidence.

## Conclusion

---

Emergencies, whether natural or manmade, cause disruptions to our social fabric and can inflict huge economic losses as governments, businesses and individuals struggle to adjust and recover. During such times, the fact that some or all of an enterprise's employees are equipped to work from home – with no special requirements other than a username and password to access an SSL VPN – can significantly help economic and business activity continue or reassume, allowing organizations to overcome temporary crises or long term disasters.

AEP Networks has long specialized in products that grant off-site employees, mobile workers, partners and suppliers with fast, secure access to applications and resources, from any location, at any time, simply and safely through a web browser. That's why thousands of users throughout the public and private sector rely on AEP for their business continuity plans every day.

### Contact AEP:

---

**Phone:** +1 732.652.5200

**Email:** [info@aepnetworks.com](mailto:info@aepnetworks.com)

**Web:** [www.aepnetworks.com](http://www.aepnetworks.com)

---