

SSL VPN Technology for Business Continuity

Microsoft Intelligent Application Gateway 2007

Executive Summary

An effective business continuity plan must include methods for ensuring that the business operates in situations in which employees and other personnel cannot physically access their offices and office-based computer equipment.

SSL VPN technology helps satisfy to this important component of business continuity planning by enabling access to business-critical applications and resources from any Internetconnected location, without the need to install, configure, or maintain any complicated or special infrastructure.

This document explains how SSL VPN technology provides an ideal solution for ensuring that employees have remote access to corporate applications from anywhere, whether they are forced to stay at home, are stuck in an airport, or are relocated to a temporary office.

The Threat: The Office Becomes Inaccessible

Traditional contingency planning requires that an enterprise consider all potential disturbances to business operations and prepare solutions to keep business activities running in the event that those threats materialize.

Organizations plan for several scenarios – those in which enterprise resources are destroyed, as well as situations in which the IT infrastructure is fully operational but workers simply cannot physically access their offices.

The latter situation, while less disturbing than the former, is far more common and without an alternative access plan in place business continuity is threatened; regular business functions cannot occur, resulting in potential delays in product delivery, impediments to customer service, or other detrimental effects.

Scenarios that fit into this classification include:

- **Bad weather conditions** – Roads may be closed due to heavy snow or flooding, or conditions may be too poor to drive. Additionally, employees may have traveled before bad weather arrived and may be stuck in locations far from their office.
- **Transportation disturbances** – Electrical outages, computer failures, or downed wires can affect the functioning of commuter trains and subways. Construction, political visits or even entertainment events may seriously disrupt transportation patterns.
- **Strikes** – Strikes in industries tied to transportation, or striking workers blocking transportation access can prevent workers from getting to their place of work.
- **Facilities problems** – Gas leaks, electrical failures, fires, heating or air conditioning problems may make working in the usual office environment unsafe, uncomfortable, or even illegal.
- **Natural disasters** – Hurricanes, forest fires, tornados, earthquakes, etc. may prevent workers from accessing their offices, yet still the data centers and communication lines function.
- **Political disturbances** – Political protests, demonstrations, and other disturbances may block areas necessary for transportation to the office.
- **Terrorism** – Even the mere threat of an attack can put an area on alert, in some cases causing authorities to block access to specific areas that may need to be accessed.
- **Personal issues** – Health (of the employee or family member), religious holidays, family events, etc. may all cause employees to be in locations other than the office when some extraordinary circumstance requiring immediate attention occurs.

In each of these cases, data centers are fully operational, employees may be available to work, and the main impediment to business continuity is the fact that the people cannot physically access the resources that they need to in order to perform their jobs. As such, organizations need to ensure that the physical location of the employees does not become a hindrance to regular business activity, and that operations can continue regardless of people's locations.

Employees should be able to connect to their data center from any computer anywhere: from their own homes, the homes of friends or family, from temporary offices and even from public places such as an Internet café. Essential business functions must continue even if employees cannot access the office.

Remote Access Technology for Business Continuity

So how does a medium-to-large-scale enterprise go about providing employees with access to corporate resources in a crisis situation when data centers and offices cannot be physically accessed? How can it ensure people can access systems from any location and any computer? And, how can it ensure that the mechanism for offering such remote access can be activated quickly in the event of an emergency, can be rapidly distributed widely to many people and differing groups within the organization, and is easy for non-technical employees to use?

Alternative Remote Access Technologies: IPsec VPN and Dial-up

Several technologies sometimes proposed as part of remote access solutions fall short when it comes to the requirements of contingency planning. IPsec VPN, for example, often deployed by companies to some portion of their employees, does not fit well into business continuity plans.

While traditional IPsec VPNs offer certain benefits for site-to-site and some employee remote access needs, they are typically not appropriate for contingency planning since they do not fulfill the criterion of providing access from anywhere.

With an IPsec VPN, users need special dedicated client software in order to access the resources they need, and that client must be pre-installed on a company owned PC or other pre-determined machine. Even if a company were inclined to implement a costly solution in which it provides laptops or home PCs to all critical employees, in the case of an unanticipated disruption such as illness or bad weather, one cannot assume that the employee has access to that computer.

A reliable business continuity plan needs to enable employees to access enterprise resources from any computer, and should not assume employees have specific machines with them.

Dial-up remote access directly to the enterprise is also often considered as a solution; however dial-up is extremely costly, provides a slow connection, and is unfeasible in many crisis scenarios. If an unusually high number of people need to dial in (as would be the case during a crisis situation in which the office is inaccessible), all available modem lines would likely be fully utilized, and many users may be unable to gain access. In any event, dial-up solutions are being phased out in most companies due to the prohibitive costs of maintaining such modem banks for user access and long distance telephone charges.

SSL VPN – The Best Remote Access Tool for Business Continuity

SSL VPN technology offers an ideal platform for providing access in the event of such an emergency since it provides remote access from any Internet-connected device. It is easy to use, so users do not overwhelm the help desk when the help desk is already burdened with dealing with other emergency-related matters.

SSL VPN access can also be easily distributed to large user populations, so all employees can get access when they need it. SSL VPN provides browser-based access to corporate applications and resources through a single configurable Web page or set of pages.

Many homes have Internet access on home PCs, and Internet kiosks are widely available at hotels, cafés and conference centers, so this SSL-based connectivity provides the required ‘anywhere’ access. It leverages high-speed connections as well as dial-up, providing the fastest connection available to the user.

SSL VPN Requirements for Contingency

When considering implementing an SSL VPN for contingency planning, there are four main areas in which SSL VPN products may differ. Some of the issues are particularly relevant to the business continuity planner and fall into the categories of:

- Usability
- Functionality
- Scalability
- Security

Usability

During a business disruption, the IT department will likely have its hands full working on company-wide issues, and should not have to deal with increased help desk calls related to remote access. IT personnel working to bring up hundreds of servers after a power outage should not be deluged with questions from the help desk related to end-users trying to figure out how to access a specific application. An intuitive interface that mimics the type of access to which a user is accustomed will help avoid this problem.

User interfaces for the SSL VPN access should be customized so that varying user groups see their own entry pages, typical to their work environment.

The company brand should be evident throughout the portal experience so users are confident they are using a company-sanctioned access method.

A crisis is a terrible time to be training users; the SSL VPN should require an absolute minimum of user-education, if any at all.

Users, for example, typically do not know the names of servers they need to access (for example, for their email repositories or home directories), yet companies may have hundreds of email or file servers; the SSL VPN should automatically identify the user based on his or her login credentials, and provide them with transparent access to their usual file storage or email locations. Home directories and network shares should be accessible using the same drive-name conventions as in the office. File access should mimic the typical "File Explorer" method used in the office, enabling users to easily upload and download necessary files from any location, without asking for help.

For companies that enforce password changes on a regular basis, the SSL VPN must be able to support remote password management, which eliminates another potential burden on the IT helpdesk. If user passwords expire during an emergency, they can simply update them via the SSL VPN the next time they log on and continue working as usual. Alternatively, if the company policy is not to allow remote password updates, then the SSL VPN should inform users why they cannot access company resources. An SSL VPN that simply denies users access as if they had typed an incorrect password would lead to numerous frustrating helpdesk calls to an already overburdened support department.

In short, the user interface for the SSL VPN should be straightforward and user-friendly to eliminate the possibility of overwhelming the help desk when the IT department has other crucial issues to attend to.

Functionality

From a functionality perspective, it is essential that an SSL VPN used for contingency support be able to provide access to all the applications that the enterprise considers mission critical.

In a scenario where regular access to the physical office is disrupted, the only way to maintain “business as usual” is to provide access to the majority (or better yet – to all) of the applications that employees need to perform their jobs. This includes:

- Email (whether Microsoft® Exchange, IBM Lotus Domino, or some other email system)
- Networked files in their home directories or other network locations (whether Microsoft file
- Shares, Novell file stores, etc.)
- Customer contact databases
- Financial databases
- Other applications

While most SSL VPNs can provide access to standard Web applications in a straightforward manner, non-standard Web applications or client/server applications may pose problems to some. Further, various SSL VPN products handle client/server and Terminal Services differently. Most SSL VPNs tunnel RDP and/or ICA transparently over SSL for Microsoft Terminal Services or Citrix access, but some offer additional features like Single Sign-On to Citrix applications or Terminal Services to each user’s desktop PC without doing any time consuming per-user configuration. Some SSL VPN solutions also have specific support for popular enterprise programs such as Lotus Domino Web Access and Microsoft Outlook® Web Access, which enables them to provide additional features for these and other applications.

Scalability

Any business continuity plan that relies on an appliance to provide access to back-end resources needs to have built-in redundancy, and in the case of SSL VPNs this is possible through high availability implementations.

High availability can provide load balancing/fail over in a single location with multiple SSL VPN appliances, or spread throughout multiple locations in various cities, or even different continents. Global load balancing is key when using SSL VPNs for a site failure scenario, which will be discussed briefly later in this paper. High availability can also be used to absorb “bursty” access – situations in which during a business disruption a larger number of people than usual attempt to utilize remote access to corporate resources.

Another crucial scalability question is how the SSL VPN handles different user groups within the same organization. During a disruption, there will likely be many different groups within a company that will require access to key resources, but these groups often need access to completely different application suites. Management may also decide that certain groups should have access to more applications than others, in order to keep essential services running.

Different groups within the company may need to authenticate to multiple user directories, including LDAP, Microsoft Active Directory®, or other data repositories. The SSL VPN should support varying levels of access to different groups, even with different user directories, with an easy-to-manage administrative interface. And the SSL VPN should be capable of offering users different interfaces based on their access rights.

Security

During any challenge to business continuity, the company is in a slightly weakened state, and security becomes even more important than usual. When people are accessing corporate resources in a different way than they usually do, malicious hackers may try to piggyback on the unusual situation and seize that moment to launch attacks against corporate networks and computers.

Because the organization is more vulnerable to attack than when operations are running smoothly, the SSL VPN itself must be secure beyond reproach. For this reason, security should be inherent in the SSL VPN platform, rather than simply an add-on; it is important to select an SSL VPN that handles security issues with built-in mechanisms, rather than relying on third-party tools to attempt to deal with this crucial issue.

SSL VPN security issues fall into two distinct categories: those stemming from the fact that SSL VPNs must allow access from all browsers including those not under organizational control (endpoint security issues), and those created by allowing access from the Internet into the internal network (server-side issues).

With regards endpoint security, since users may be accessing from locations such as Internet kiosks or borrowed computers, the SSL VPN needs to ensure that sensitive files are not left on access devices. Some SSL VPNs eliminate this risk by using a cache-cleaning mechanism, however it is important to check that the SSL VPN wipes clean information saved in locations other than standard systems caches (as is the case with Domino Web Access or Citrix, which do not use the usual /Temp directory).

Timeouts are another important endpoint security issue, as employees may neglect to logout, or may browse to another web site without realizing that their session is still live. The SSL VPN should enable multiple levels of inactivity timeouts, in a way that is unobtrusive to the legitimate user, but will not allow illegitimate users access.

The SSL VPN needs to ensure that after the user logs off (or is timed out) their access credentials are wiped from the browser machine.

There are many other endpoint security issues, including compliance of the endpoint with corporate or other regulations and presence of desktop search tools that might cache sensitive information and documents. For more information see the Intelligent Application Gateway 2007 features overview on our website.

For server-side issues, enterprises must take care to not put back-end resources at risk simply by providing a new method to access them. The SSL VPN should be built on a solid platform that is impenetrable to hackers at the Operating System level, the networking protocol level, and the application level. All requests to the SSL VPN must be filtered – with any inappropriate requests blocked by the SSL VPN before they cause problems in internal systems. Such a solution can protect the back end resources from rogue requests in the form of viruses and worms, as well as the most determined hacker.

SSL VPN for Data Center Failure

SSL VPNs can be useful for the rare case of complete data center failure (destruction through fire, earthquake, terrorism, etc.). Ideally, a mirrored backup of the destroyed data center exists in another location; it is recommended that the SSL VPN be implemented as high availability, with at least one SSL VPN appliance located outside the destroyed center. In such a crisis, employees would be expected to either work from home, or else from a backup facility where they would typically receive a desk, chair and Internet-connected PC. At the backup site, rather than plan to configure hundreds or thousands of client machines, the quickest way to get vast numbers of employees up and running is through an SSL VPN, using browser-based access to the mirrored backup center. In addition, those working at home could use the SSL VPN to access the mirrored backup center.

Conclusion

SSL VPNs are an ideal component of a business continuity plan, since they can provide employees with access to key corporate applications and files from any location in a secure and user-friendly manner. They are better suited to such access than other remote access technologies (including IPsec VPNs and dial-up) as they provide much wider scale access, with little-to-no additional training necessary for users.

When looking for an SSL VPN to deploy enterprise-wide, one must consider key issues such as usability, functionality, scalability and security, as not all SSL VPNs meet the demands of a business continuity plan.

For further information on IAG 2007 and its SSL VPN component, or to arrange for a live demonstration, please contact: sales@celestix.com