

TIMEnavigator™

Improving

Data Security with Time Navigator

OVERVIEW >>

Enterprises today create and maintain critical corporate data in a wide variety of locations, both inside the firewall of an internal network, and also outside the protection of the network on web servers, application servers and in remote offices. Security and protection of data in these demilitarized zones (DMZs) outside traditional network protection is an increasing concern of IT personnel.

In today's highly competitive and regulated environment, enterprise backup and restore software solutions must maintain the integrity, confidentiality and availability of corporate data regardless of where it is located.

This white paper provides information on maintaining security levels and backing up data in the DMZ architectures through firewalls, and other data protection strategies, to give the IT Department a better understanding of backup and restore security. The security is not only a network configuration, but also a software philosophy to improve the computer enterprise policy.

Time Navigator is an enterprise-class Backup and Restore Application for files and databases, designed for maximum data protection and availability in high security environments. Developed by Atempo, one of the world's leading providers of enterprise data backup software, Time Navigator is available for Windows, Unix and Linux environments.

Contents

- Securing the Enterprise 1**
- Secure Enterprise-wide Backup – Is It Possible? 2**
 - Backing Up Outside the Enterprise Network – the Firewall Dilemma 3
 - Backing Up Outside the Enterprise Network – the Time Navigator Solution 3
- Other Time Navigator Security Features 5**
 - Multiple Backup 5
 - Data Partitioning 6
 - User Profiles 6
 - Backup Server Security 7
 - Attributes Backup and Restore 7
- Conclusion 8**

Securing the Enterprise

In today's corporations, mission critical data resides not only in the corporate network, but around the world in remote offices, on email servers, on application servers and in remote databases. Information must be shared across departments, across enterprises and outside the enterprise with customers and partners. New storage architectures like SAN and NAS are accepted parts of the network. And 7x24x365 data accessibility is a reality.

Business continuity and compliance are now security issues. Government regulations such as Sarbanes-Oxley and HIPAA define who has access to data. And this access, as well as the data itself, is no longer inside the protection of the data center. Corporate data is accessible via Internet portals and stored outside the data center at remote sites vulnerable to unauthorized access, misuse or theft.

End users are increasingly demanding that data is always available, always accessible, always reliable, always correct and always private. Companies are faced with a variety of data threats – external, internal, intentional, accidental. The result is an enterprise tightrope walk - improving access to information leading to improved productivity and a positive impact on the bottom line balanced against the increase in data security breaches. Factors weighing in are issues like who is authorized to access the data and how can data outside the trusted arm of the data center be protected.

Once upon a time, all data was on a single server. Security was easy, and few people were involved. Now, networked storage architectures allow connections of hundreds, thousands, or even millions of storage devices behind many servers. Much of this data is not behind any firewall at all.

This white paper discusses how data security can be initiated and maintained in both an internal and external network, and how to backup and restore data in a demilitarized (DMZ)¹ architecture and through a firewall. Today's realities of backup and restore will be outlined, to give the IT Department a better understanding of both backup and restore security challenges, as well as demonstrated solutions.

¹A demilitarized (DMZ) zone is a computer or small sub-network that sits between a trusted internal network, such as a corporate private local area network and an untrusted external network, such as the public Internet. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers. The term comes from military use, meaning a buffer area between two enemies.

Secure Enterprise-wide Backup – Is It Possible?

Many enterprises employ DMZ architectures to limit access rights and prevent network attacks to an internal network, and to decrease risks associated with an enterprise network opened to an external network. Firewalls are often installed as network components providing network-level protection for the enterprise network. The firewall provides services to trace and to limit network access through known port numbers². The firewall is the only host who is known to all networks, and presents one interface to the inside public network, one interface to the outside private network and one interface to the DMZ. Only hosts that need to connect outside of the firewall are installed within the DMZ network.

With network security becoming more and more complex, DMZ architectures are rapidly becoming standard. An extranet architecture offering services to many users connected via a web browser that diffuses public information is one example where DMZ solutions are necessary. Additional data locations that may drive installations of a DMZ architecture are:

- Web server
- Front end to an e-commerce server
- E-mail server
- VPN endpoints
- Application server
- FTP server

Anyone or any application that needs access to data from the external to the internal network, or vice versa, needs one network authorization (port). A firewall serves as the controller of these accesses. The DMZ architecture also provides security insurance for services and applications inside the enterprise.

²Port number defines a software connection between 2 hosts through an IP network. All network applications use this method to establish one computer dialogue; some examples: web browser, e-mail software, database, etc.

Backing Up Outside the Enterprise Network – the Firewall Dilemma

Savvy organizations recognize that it is necessary to ensure the backup and the restore of their corporate data on the public network (intranet or extranet) as well as within the corporation. While some companies simply install a backup server in the public network, those who understand the link between security and storage improve their data security by installing the backup server within their private network (enterprise network) and initiate backups from within the enterprise network.

However, the use of a firewall in enterprise architectures presents a problem when backing up a platform located within the DMZ with a backup server located outside the DMZ. To successfully backup all data in the corporation, the backup and restore solution must be optimized to work securely and seamlessly both inside and outside the firewall. However, the majority of backup solutions on the market today require a varied number of ports to “remain open” to allow communication between the platform to be backed up and the backup server. This method is unacceptable from a security point of view, as it opens up the DMZ, and therefore the trusted internal network, to potential unauthorized access and destruction of corporate data.

Backing Up Outside the Enterprise Network – the Time Navigator Solution

Time Navigator, Atempo’s flagship backup and recovery product for high performance enterprise environments, is designed to reduce the complexity of managing data within modern storage networks resulting in lower total cost of ownership and greater return on investment of storage resources. Taking a leadership role, Time Navigator was the first backup and restore solution to solve the problem of backing up through the corporate firewall. Time Navigator carries out backup on a DMZ platform by establishing a communication path that is always initiated and controlled by the backup server, located inside the secure enterprise network and outside the DMZ. Moreover, the communication between the Time Navigator backup server and the platforms to be backed up is established by using only one TCP port and one UDP port, which makes it possible to precisely identify any and all network traffic and prevent harm to the internal network.

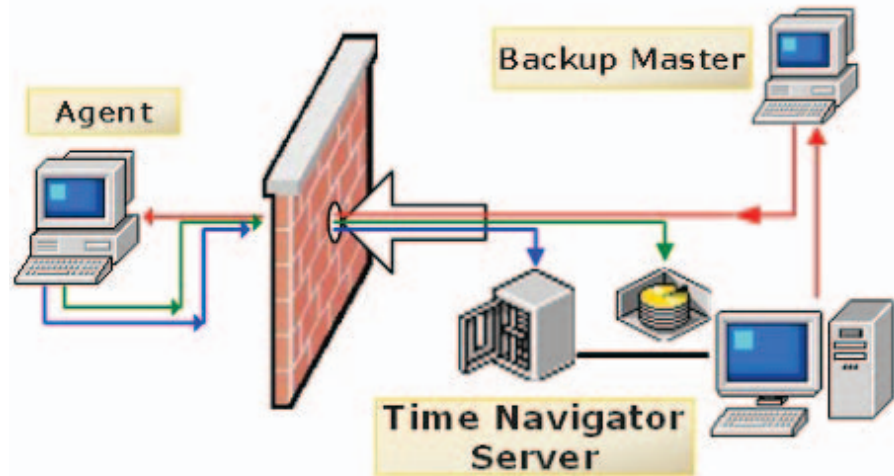


Figure 1. Secure Backup and Restore Through the Firewall.

Figure 1 shows how a backup session works with Time Navigator software. The client to be backed up is installed in the public network behind the Firewall. The Backup Master and the Time Navigator Backup Server are installed in the private network. The Backup Server is dedicated to manage the data backup for the Client. To backup and restore a client outside the firewall, the Time Navigator Backup Server Scheduler first launches a backup job (red line). Time Navigator Backup Server then contacts the Backup Master to initialize a Backup session. Time Navigator Backup Master starts the Backup process and contacts the clients in the public network outside the firewall (red line). The communication can only be started by the Backup Master, and uses only one TCP port and one UDP port, both outbound. The client outside the firewall is never authorized to open an inbound network relationship. The Agent receives one request for data and then sends both the metadata (green line) back to the Catalog on the Server and the file system data (blue line) to the library completing the backup. Agent data is sent through the same port initially opened as an outbound connection by the Backup Master. All network traffic is identifiable and traceable.

Other Time Navigator Security Features

Multiple Backup

Within Time Navigator, all backup sessions can be directed simultaneously towards several sets of disk and tape media in order to create “production” backup sets and “disaster” backup sets. This is ideal when, for frequent and urgent restorations, data must be available in an online library, or when, to protect the data against major disaster, it is better to store the media out of the production site or in fireproofed safes. The media, then, could be used to restore complete environments.

Time Navigator makes it possible to perform backups in double, triple or quadruple specimens at the time of the same backup session, which avoids all the post tape duplication operations. Figure 2 shows a typical multiple backup scenario. In this illustration, data flow is unique between the Time Navigator Client and the Time Navigator Server. Data flow is duplicate within the Time Navigator Backup Server cache and is written to several local tape drives through a SAN on two different libraries. Each library can be installed in a separate building, while the Time Navigator Backup Server could be installed at either site or a third site. Checking operations are processed within cache. Media can be of different technologies within the same library or the same or different technology in different libraries.

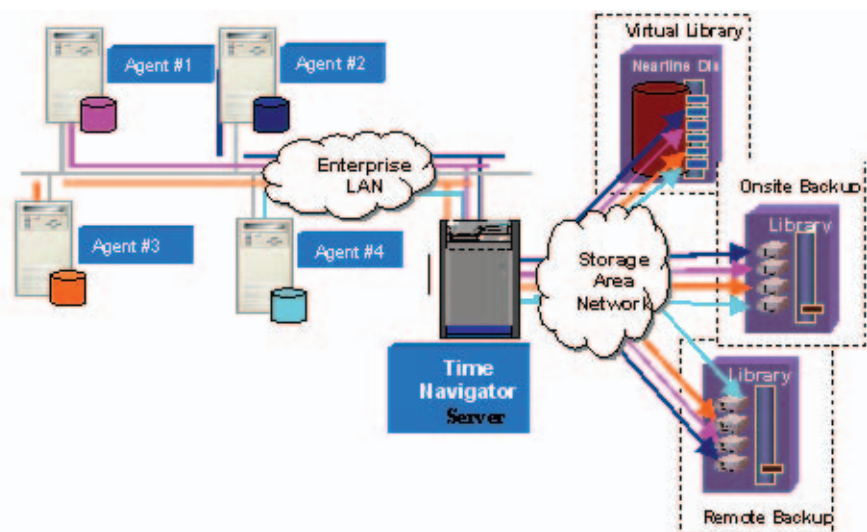


Figure 2. Off-Site Multiple Copies Architecture.

Data Partitioning

Time Navigator's data partitioning feature is designed to provide secure backup for enterprises with many customers. Time Navigator incorporates the ability to run multiple environments simultaneously for separate backup. Tape drive libraries and other shared storage can retain their dedicated pools and media.

For many enterprises that provide backup and restore services for clients, one client's data cannot be mixed with another's. Consequently, data partitioning is a key component for corporations that host many environments with many different customers and who need to logically separate one customer's data from another's. Time Navigator incorporates the ability to run multiple environments that are logically separate from each other for safe, uncontaminated backup of all client data.

User Profiles

With Time Navigator, security used for the backup data is based on the corresponding operating system security levels. Consequently, users can access only the data for which they have reading rights, and can restore data only in one directory in which they have writing rights.

Moreover, the backup administrator does not need to be a super-user, which might represent a potential security threat. The administrator can activate an additional password level to reach the Time Navigator application to ensure safe access to the Time Navigator administration tools.

Backup Server Security

Time Navigator references the complete information relating to the backup (files, files attributes, owner, file location on tape, as well as the cartridge management) in a database called the Time Navigator Catalog.

Safety of the Time Navigator Backup Server is ensured by the autosaving of this Catalog, including all the metadata necessary for server restoration. An emergency licence allows the transformation of any client machine into the server, permitting restoration even when the main backup server is disabled. With Time Navigator's associated high availability option, server and peripherals can also be duplicated. The implementation of an incremental replication strategy will make it possible for the secondary server to periodically duplicate the backups carried out by the principal server.

Attributes Backup and Restore

Within the file system, several bits that determine access permissions to the file define file permissions. Through a simple mechanism, operating systems like Unix and Netware define access permissions for three class levels: user, group and others (the rest of the world). The Windows operating system defines different permissions levels. The Access Control List (ACL), a mechanism to restrict access to data, is a finer-grained extended permission.

With Time Navigator, all file and directory extended attributes are backed up. Using native agents, Time Navigator backs up all file types across the range of supported platforms, including file systems, special files, all file attributes, ACLs, rights and dates associated with files. Before a restarting launch, the user could select only the restore of files attributes. In daily administration, this feature helps the administrator better manage the issues involved.

Companies using Atempo's Time Navigator have the comfort of backing up corporate data securely and seamlessly regardless of location. Recently, a world leader in IT services and management consulting selected Time Navigator for its innovative approach to addressing backup security issues.

The company had the challenge to provide hosting services with high performance backup and restore capabilities, offer multiple service level agreements with specific quality of service levels to its clients, and to provide hot standby disaster recovery centers.

Being able to offer its clients the guarantee of data protection with secure backup through firewalls played a key role in the selection of Time Navigator.

Conclusion

Integral to network security is the confidence that the complete data backup and full restore are ensured. As security continues to grow more complex, it is important that the backup software solution implemented in an enterprise respects basic security best practices and provides a single integrated solution without disturbing or interrupting the enterprise security configuration. DMZ architectures are now a main part of network security if enterprises need to protect and to check the external connection to their application servers. In addition, security policies do not stop with network considerations. Off-site backup, duplicate backup, disaster recovery processes and authentication connections are additional areas where data protection can always be improved.

Atempo has designed Time Navigator with an understanding of security as an important component of enterprise architecture. Time Navigator embraces the problematics of enterprise security and network technologies with its innovative, leading approach to whole enterprise backup. Time Navigator delivers a single solution for enterprise backup and restore with a robust feature set for rapid and secure client backup through the firewall and complete enterprise backup.