



Microsoft
Your potential. Our passion.™

Focused on **Security**.
Committed to Success.

U.S. National Security Team White Paper

Optimizing Branch Office Security and Productivity in the Financial Services Sector

Produced by the Microsoft U.S. National Security Team

Co-authored by Thomas W. Shinder, MD, MCSE, MVP, and Norm Barber, Strategic Security Advisor

About the U.S. National Security Team (NST)

The US National Security Team is composed of strategic security advisors who work with Microsoft customers, partners, MS internal constituencies and the information security industry to promote the adoption of security processes and technologies. Its goal is assist customers and partners to increase their security awareness and implementation to create more secure businesses, mitigate risk, and make security costs more effective. Its activities are informed by three simple tenets: protect the consumer, secure the enterprise and enable developers to write secure code.

As part of its mandate, in addition to producing white papers such as this one, the NST is responsible for developing and executing security-focused events and Security Round Tables across Microsoft's U.S. geographies. These events include the annual CSO Summit, which provides formal feedback to business groups, security industry updates from leading analysts, peer perspectives on security management from MSIT, and updates on the latest initiatives and industry trends in enterprise security.

The NST also focuses on driving vertical security solutions for a wide range of industries. To this end, the NST has produced a number of white papers that address the specific security needs of particular industries, such as the professional services and financial services industries.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2007 Microsoft Corporation. All rights reserved.

Microsoft, Forefront, Antigen, Excel, SharePoint, Windows, Windows Server System, and the Windows Server System logo are either registered trademarks or trademarks of Microsoft Corporation or Sybari Software, Inc. in the United States and/or other countries. Sybari Software, Inc. is a subsidiary of Microsoft Corporation.

All other trademarks are property of their respective owners.

Contents

Introduction	1
Preventing Security Issues at the Branch Office from Impacting the Main Office	3
Financial Services Branch Office Security Scenarios.....	3
ISA Server 2006 Solutions for Branch Office Security	5
Firewall Access Controls.....	5
Intelligent Firewall Application Inspection Filters.....	5
Sophisticated Worm and Flood Protection Controls.....	5
Integrated Intrusion Detection System and Intrusion Prevention System.....	6
Web Proxy Access Controls.....	6
Web Proxy Web Application Inspection Filters.....	6
Comprehensive Logging and Reporting.....	6
Real-Time Alerting.....	7
Intelligent Application Gateway (IAG) 2007 Solutions for Branch Office Security	8
Application Intelligence and Firewalling.....	8
Internal Reference Encryption.....	9
Secure Logoff.....	9
Remote Password Management.....	9
Robust logging and reporting.....	9
Attachment Wiper.....	9
Endpoint Compliance.....	10
Inactivity Timers.....	11
Improve Branch Office Efficiencies with Windows Server 2003 R2	12
Integrating Branch Offices with Distributed Servers.....	12
Integrating Branch Offices Using Centralized Servers.....	12
Converging Branch Office Integration Strategies.....	13
Improved Branch Office Services with R2.....	13
File Services.....	14
Print Services.....	15
Summary	16
For More Information	17

Introduction

Branch offices can provide competitive advantages for financial services companies. They can serve a number of functions, the most important of which would be to bring the company and its employees closer to customers. An increasing number of employees are being moved out of the main office into branches, as reflected in a Nemertes Research study done in 2005, which indicates that up to 91 percent of employees in large organizations work away from the main office.

Most financial services organizations have branch offices that require access to systems or applications stored at the main office. A connection to the main office enables branch-office employees to access information on main-office data servers, and enables employees to share and act on information quickly. Branch-office connections carry the risk, however, of distributing dangerous exploits initiated by hackers and malicious mobile code. Financial services organizations must have a method to allow secure, fast and reliable connections from the branch office to the main office.

Three key factors are driving the need to consider enhanced attention to branch office security and efficiency:

- **Corporate expansion leads to proliferation of branch offices.** As a corporation grows larger, so does its need to extend itself into branch offices to bring employees closer to customers and retain a high quality workforce. Branch-office expansion through acquisitions is a key growth strategy in the financial services sector. It brings with it infrastructure costs, including hardware and software required to connect branch offices to the main office. Today's financial services firms need a secure way to connect branch offices to data located at corporate headquarters.
- **Branch-office workers require increasing amounts of information available only at the main office.** With the increased number of branch-office employees and telecommuters joining the company comes increased demands for data contained at the main office. Not only do more branch employees require access to the same information that employees in the main office access, but there also is an increased amount of information these remote workers need to access because of server consolidation and process centralization.
- **Branch offices require data integration and convergence.** Remote locations generate significant operational costs and administrative challenges. Financial services organizations often are constrained by one simple prerequisite – distributed networks. The inherent limitations of distributed network architectures, which require WANs, have an undesirable effect on the efficiency of branch-office operations. Organizations operating branch offices are faced with fundamental cost-for-efficiency tradeoffs inherent in maintaining data availability and consistency over bandwidth-limited, high-latency networks.
- Financial service companies need to provide corporate branch-office workers fast, reliable and secure access to corporate data. The challenge is to enable connectivity without sacrificing security. Two powerful solutions are the ISA Server 2006, which

provides security for these off-site offices, and the Windows Server 2003 R2, which increases data availability and consistency, and reduces operational inefficiencies.

This white paper examines the problems that financial services sector companies face when attempting to provide secure and efficient data access to branch offices. It also provides solutions based on the features and capabilities included with ISA Server 2006, Whale IAG 2007 and Windows Server 2003 R2. This report specifically examines how to prevent security issues at branch offices from impacting main-office security, and how to reduce cost and operational inefficiencies inherent in distributed computing environments.

Preventing Security Issues at the Branch Office from Impacting the Main Office

Branch offices pose unique security concerns because of the following issues:

- **Branch offices are less closely managed and monitored.** In most companies, the majority of IT staff members are stationed at the main office, which means that many branch offices have small, inexperienced or non-existent IT staffs. This can lead to a lower level of management and monitoring at the branch office and an increased risk of security incidents. Financial services organizations need a way to increase branch-office security without incurring the overhead of additional employees, large-scale software updates or expensive network devices for each branch office.
- **Security breaches at branch offices can spread quickly to the main office.** Security practices tend to be more lax at branch offices, especially smaller ones. This might be due to a lower level of IT support for branch-office computers, a more relaxed attitude about computer security, or because branch-office computers tend to run older operating systems. Thus, the risk of a security event is higher at a branch office and can lead to infection or compromise not only of branch-office computers, but also of those at the main office. Companies need a way to prevent branch-office outbreaks from spilling over to the main office and beyond.
- **Visitors and malicious employees at branch offices can reconnoiter information contained on the main-office network.** In the same way that security practices at branch offices are generally less stringent than those at the main office, the same is often true for physical security. Corporate headquarters may have elaborate controls over who can enter main-campus facilities, but often find a more lax approach to building access at branches. The problem is that while confidential corporate data may not be stored at any of the branch offices, people who can access a networked computer at the branch office can connect to main-office information assets and steal or destroy that data from the remote office. Organizations need a solution that enables branch offices to access corporate data without putting the main office at risk.

Financial Services Branch Office Security Scenarios

The following scenarios help illustrate some security challenges that financial services sectors face in a branch-office environment:

- An analyst in a brokerage firm returns to his branch office after being on the road for a week. While connected to a hotel network, the analyst's computer was infected with a network worm designed to take down database servers. The analyst then connected his laptop to the branch-office network, and the worm immediately scanned the network and attacked the main-office's payroll database servers, resulting in the loss of key competitive information and intellectual property.
- A branch office of a national bank provides wireless access for its employees. A loan officer for the bank decided to enlist the help of a hacker to connect to the wireless access point and transfer money fraudulently into his own account. During the

investigation that followed, the perpetrator could not be identified because the branch-office devices were not enabled with tracking information.

- A corporate spy posing as a delivery person brings in packages to a large hedge fund's branch office. The receptionist leaves her desk for a few minutes, and during that time the spy uses the receptionist's computer to connect to the company's SharePoint collaboration service and download proprietary information about an upcoming merger.
- During a business trip, a managing director for an investment management firm focused on distressed and undervalued debt and equity securities saves passwords in his laptop's Internet browser. A thief who works for a competitor steals the computer and gains access to the managing director's e-mail account, which contains highly sensitive information about negotiations for a major restructuring. He uses the information to blackmail the managing director's firm for millions of dollars.
- An employee in an international reinsurance organization works out of a branch office in Canada. The employee has discovered that he can make extra money by infecting machines at the branch office with a trojan that will send spam e-mail messages through the main office's mail server. Blacklist operators discover that the organization's mail server is sending millions of spam messages, and they blacklist the company. It takes several weeks to rectify the blacklisting and costs the company millions of dollars in brand equity.

As illustrated in the above scenarios, branch-office issues can quickly can become main-office concerns. ISA Server 2006 and IAG 2007 can help alleviate these concerns by bringing state-of-the-art firewall, Web proxy, and VPN and SSL VPN technologies within the reach of branch offices, and provide them with the same high level of security formerly deployed only at main corporate-office networks. In addition, Windows Server 2003 R2 builds on the security provided by ISA Server 2006 and the IAG 2007 to reduce overhead and increase branch-office efficiencies.

ISA Server 2006 Solutions for Branch Office Security

ISA Server 2006 provides the following solutions to branch office security concerns:

- Firewall access controls
- Intelligent firewall application inspection filters
- Sophisticated worm and flood protection controls
- Integrated intrusion detection system and intrusion prevention system
- Web proxy access controls
- Web proxy Web application inspection filters
- Comprehensive logging and reporting
- Real-time alerting

Firewall Access Controls

One role that ISA Server 2006 plays is that of a network's firewall, which enables financial services companies to control what and when information moves through the firewall, and who has access. The firewall can log and report all information crossing the firewall, including the name of the user and the applications used to access the information. An ISA Server 2006 firewall at the branch office can prevent unauthorized users from accessing corporate data.

Intelligent Firewall Application Inspection Filters

Traditional "hardware" network firewalls can detect and block attacks that were popular during the early years of the Internet. While network-layer protection is important, it is limited in its ability to protect against leakage of financial-services information.

Network-layer protection does not protect applications that run the business. Servers for mail, Web, news, database, files, media, CRM and data collaboration need protection. Application protection is mandatory because intruders have become more sophisticated. They prefer to steal information covertly and use it for criminal gain.

ISA Server 2006 helps protect against corporate application attacks by using application-inspection filters to prevent network-level attacks. Then ISA Server uses smart application-layer inspection filters to mitigate attacks leveraged against corporate applications that contain business intelligence.

Sophisticated Worm and Flood Protection Controls

The media is replete with stories on worm attacks that disable computers, destroy data and increase the cost of ownership. In many cases, an infected portable computer introduces a worm to branch offices, and it subsequently spreads to headquarters. Removal can be time-consuming and expensive.

ISA Server 2006 includes a comprehensive array of worm and flood protection controls that protect the main office from worm floods at the branch office. ISA Server detects worm-like behavior from infected computers and blocks connections to the main office. Not only does this

help mitigate the spread of infection, it reduces chances that a branch-office worm infestation will saturate the branch-office link. This protection enables users to continue to access data at the main office.

Integrated Intrusion Detection System and Intrusion Prevention System

Financial services firms need to know when attacks start so they can respond quickly. Intrusion detection systems can detect a possible attack and alert key personnel. An intrusion prevention system adds further protection by blocking detected attacks.

ISA Server 2006 includes a comprehensive set of intrusion detection mechanisms that detect possible attacks coming from branch offices at both the network and application layers. When the attacks are detected, ISA Server can inform security personnel immediately and then block the attack to protect network information, integrity and performance.

Web Proxy Access Controls

Web proxies can control all Web traffic moving between the branch and main offices, as well as traffic to and from the Internet. Adding a Web proxy doesn't require complex changes to the corporate network infrastructure and can provide strong Web proxy-based access controls.

ISA Server 2006 includes a powerful Web proxy that enables the company to control what information different users can access at precise times of day, and optionally, on different days of the week. The ISA Server Web proxy works in conjunction with any existing firewall at the branch office and provides strong user-account-based access control.

Web Proxy Web Application Inspection Filters

In addition to providing user-based or group-based access control over Web sites, an ISA Server 2006 Web proxy can enforce enhanced security policies over allowed connections. Even when the company has locked down a list of sites, legitimate work-related sites or user's computers can become compromised and used to attack approved Web sites. A Web proxy can clean connections so that neither users' computers nor Web sites can harm one another.

ISA Server 2006 includes technologies to protect both users and Web sites. One powerful feature is the ISA Server HTTP Security filter, which inspects the Web connections to confirm that no dangerous commands or data move over the Web channel. This enables companies to create a list of approved Web sites, but limits access to those sites if either the site or the user's computer is compromised.

Comprehensive Logging and Reporting

Financial services security and compliance managers require detailed information about data users' access through the branch-office firewall. Detailed logging should include the user's name, the day and time, and the nature of the information accessed during the branch office's connection to corporate and Internet Web servers. This data must be available for network audits, forensic analysis and industry standards compliance testing.

ISA Server 2006 firewall logging and reporting provides all this information and much more. The default log settings enable the ISA Server 2006 firewall to gather detailed information about user activity, and then create illustrative reports using the ISA Server 2006 built-in reporting engine.

Real-Time Alerting

Network security officers need to know in real time the current status of the firewalls and Web proxies. Real-time alerts provide critical information required to respond to possible attacks, performance issues, and system hardware or firewall service failures. ISA Server 2006 administrators receive real-time alerts about firewall status via e-mail, pager or systemwide alerts using enterprise management and control consoles.

ISA Server 2006 is supported fully by the Microsoft Operations Manager (MOM), which enables the ISA Server computer to be part of a centrally managed security environment. The ISA Server 2006 MOM pack provides the MOM server with application intelligence required to detect and interpret configuration, management and security issues. It then alerts administrators using MOM alerting.

Intelligent Application Gateway (IAG) 2007 Solutions for Branch Office Security

Many financial services organizations are discovering that full network connectivity as seen in site-to-site VPNs or dedicated WAN links are not required. These companies realize that the goal of branch-office connectivity to main-office resources is not to provide LAN-like connectivity, but rather to provide reliable access to branch-office users for main-office resources.

One compelling data access solution is an SSL VPN. Unlike site-to-site VPNs or dedicated WAN links, the SSL VPN provides access to main-office information over a typical Internet connection. SSL VPN technology enables access to a wide variety of main-office applications. These applications may have native Web interfaces, or no Web interface at all. The SSL VPN solution will “webify” non-Web based applications to enable secure access.

The Microsoft Intelligent Application Gateway (IAG) 2007 is an SSL VPN solution that can obviate a financial services organization’s need to site-to-site VPN or dedicated WAN links, while at the same time providing secure access with robust application functionality.

IAG 2007 provides the following security solutions for secure branch office access:

- Application intelligence and firewalling
- Internal reference encryption
- Secure logoff
- Remote password management
- Robust logging and reporting
- Attachment wiper
- Endpoint compliance
- Inactivity timers

Application Intelligence and Firewalling

An application firewall is a powerful tool against known attacks as well as vulnerabilities not yet discovered or patched. Deploying an SSL VPN without an application firewall creates severe risks.

To protect against worms and hackers compromising an organization’s infrastructure, IAG 2007 subjects incoming requests to stringent security checks before relaying any data to application servers on the internal network. Application-level control includes thoroughly inspecting URLs, methods and parameters, and all other incoming data. The inspection rules can be based on the “positive logic” of the application, indicating a controlled set of legitimate URLs, method and parameter combinations to which the requests are expected to conform. This prevents application-level attacks based on malformed URLs. IAG 2007 also supports “negative logic” rules to block specifically known attacks from reaching internal servers.

Internal Reference Encryption

A major technical challenge associated with providing access to internal applications across the Internet is that of internal references within applications. Data, code and links may utilize system-naming conventions that do not work across the Internet. Although all SSL VPNs offer technology to perform translations of such references, each translation algorithm and implementation is unique. IAG 2007's host address translation engine encrypts all information related to the internal network so that external users never see anything that could assist to them in launching attacks against internal resources.

Secure Logoff

To prevent credentials from being cached on the access machine, IAG 2007 utilizes patent-pending Secure Logoff technology. IAG 2007 utilizes this innovative proprietary mechanism as a replacement for "HTTP Basic Authentication," eliminating the possibility of malicious users reinstating user sessions.

Remote Password Management

Sound security policies dictate that passwords be modified periodically. If an organization forces its users to change passwords every few months by expiring old passwords, users must have the capacity to change their passwords before they lose access, regardless of whether they are in or out of the office.

IAG 2007 supports remote password management by providing remote users with prompts when passwords are nearing expiration, and enables employees to update passwords from any browser. It also supports remote resetting of token PINs for technologies such as RSA SecurID.

Robust logging and reporting

The Event Logger logs and records gateway-related events in a variety of tool and output formats. Using the event logs, the administrator can gather information about system usage and user activities, and request alerts about security events.

Administrator can query and retrieve events recorded by the event logging reporter. IAG 2007 provides a powerful tool for selecting, filtering and sorting the required events by numerous parameters. The administrator can display an on-screen report, print or extract a report to Microsoft Excel format for further data manipulation.

Attachment Wiper

The Attachment Wiper is a "virtual shredder" that upon completion of a user session erases all traces of the session from the access device. It will be triggered when:

- A user logs off
- There is a timeout after a period of inactivity
- The user is automatically logged off after a scheduled logoff threshold passes and the user does not re-authenticate
- The browser crashes
- The user closes the Web browser

- The system is shut down

The ability of the Attachment Wiper to ensure that security is maintained even after a browser crash or system shutdown means that sensitive data will not be leaked, even under irregular conditions.

The Attachment Wiper erases the following:

- Temporary files created by the opening of attachments during the user session
- Browser cache entries created during the user session including non-standard caches such as those used by IBM Lotus Domino Web Access (iNotes) and Citrix Metaframe
- Temporary files created by the downloading of files or any other mechanism during the user session
- URL entries memorized for AutoComplete
- Form-field contents memorized for AutoComplete
- Cookies generated during the user session
- Any history information created during the user session
- Any user credentials memorized by the browser during the user session

The Attachment Wiper only will erase information created during the user's SSL VPN session; all other temporary files, cookies, etc. will be left intact.

Additionally, the Attachment Wiper runs by default in "file-shredding" mode, causing all deletions to conform to DoD 5220.22-M standard and ensuring that data cannot be reinstated using specialized electromagnetic equipment. The file-shredding feature also ensures compliance with HIPAA and GLB regulations.

Endpoint Compliance

Since SSL VPNs derive much potency from their ability to enable access from computers not under organizational control, enterprises must implement endpoint security policies to govern the level of access that specific devices may achieve.

To identify machines and set security policies accordingly, users can download client certificates from IAG 2007. Users can present the certificates later during future access sessions to indicate to IAG 2007 that the machine is "trusted" and that appropriate security policies (i.e. more leniency than for non-trusted machines) should be used. IAG 2007 can check the client machine for specific files, registry values or even hardware devices (SmartCards or USB Tokens) to determine whether the system is a "trusted" device. This prevents data breaches due to stolen user credentials.

To determine the security level of machines not otherwise certified, IAG 2007 can scan the access device to check for conformity to policies that have been set by the organization. It can check for anti-virus software, personal firewalls and other security mechanisms, as well as how recently the software was updated. Policies for the user's session can be set dynamically according to the results of this scan. The granularity of the IAG endpoint policy engine coupled with application intelligent technology allows for better implementation of sound business policies over any other SSL VPN access solution.

Inactivity Timers

A necessary element of browser-side security, inactivity timeouts protect organizations from users who neglect to log off after a session. For legitimate users, however, these timeouts can cause much inconvenience or loss of work. For example, SSL VPN may automatically log a user out while he is composing a long email or completing a long Web form.

To combat this challenge, IAG 2007 utilizes non-intrusive timeouts whereby users are warned that a timeout based on inactivity will occur soon. The user then has the opportunity to prevent the timeout.

Improve Branch Office Efficiencies with Windows Server 2003 R2

Maintaining remote locations often generates significant operational costs and administrative challenges. The financial services sector is often constrained by one simple prerequisite – distributed networks. The inherent limitations of distributed network architectures, which require WANs, have an undesirable effect on the efficiency of branch-office operations.

Branch offices are faced with fundamental cost-for-efficiency tradeoffs. They must accommodate distributed networks with integration strategies that follow one of two paths: 1) deploy per-branch office servers that offer better productivity at an increased management cost, or 2) provide services to the branch office through centralized servers that minimize management difficulties but limit the overall performance and autonomy of their remote locations.

Each integration strategy presents organizations with a unique set of challenges.

Integrating Branch Offices with Distributed Servers

IT groups have embarked on a strategy for accommodating branch-office workloads by physically locating servers at remote sites to make available applications and services necessary for branch operations. These servers provide the performance and availability needed for a productive branch environment. They introduce, however, a difficult management model:

- Most branch offices do not have onsite administrators. Administration occurs remotely. If branch-office issues cannot be resolved remotely, expensive remedies are often required, including sending an administrator onsite or hiring third-party consultants.
- Management toolsets often are inefficient and do not provide a centralized view of all branch offices. Current tools provide limited functionality for restoring branch services remotely or recovering branch data after remote-server failure.
- Deploying branch servers requires additional hardware, software and infrastructure support. These servers can become a single point of failure.
- Branch autonomy and WAN infrastructure boundaries curtail enterprise-wide collaboration and create “mini data centers.” This forces branch offices into managing enterprise data in isolation.

Integrating Branch Offices Using Centralized Servers

Improvements in technology and increased costs of managing branch-office servers led many financial services companies to shift their strategy to consolidation. Organizations moved branch-office workloads to data centers. Centralized servers simplified administration of an enterprise’s distributed computing environment, minimized its infrastructure requirements and reduced overall support costs.

However, the inefficiency of WAN infrastructures, with low bandwidth and high latency, can have a negative impact on branch office productivity.

- Most client-server applications and their underlying network protocols were designed to operate across local area networks (LANs). These protocols perform poorly when exposed to limited bandwidth and high-latency WANs.

- The WAN infrastructure diminishes the effectiveness of a serverless branch office. If WAN connectivity becomes unavailable, the branch office ceases to function and end-user productivity diminishes.

Converging Branch Office Integration Strategies

Prior to Windows Server 2003 R2, organizations were forced to solve these problems in varying ways. Many financial services firms attempt to mitigate WAN inefficiencies by deploying WAN-optimized client-server applications in branch and central locations. While many technologies have a positive impact on bandwidth utilization, they typically address only a subset of branch challenges.

Examples of WAN optimization techniques include:

- Microsoft Exchange Server 2003 and 2007, and RPC over HTTP, provide Microsoft Outlook client functionality over the Internet; HTTP as a protocol is optimized for use on latency-bound and low bandwidth networks
- Microsoft ISA Server 2006 Web content caching at WAN boundaries.
- Proprietary technologies such as Transaction Prediction and Scalable Data Referencing, which attempt to predict end-user actions.

Financial services organizations also have examined products claiming to improve distributed file systems through file caching. These technologies only are point solutions that do not fully address the complete scope of branch-office issues. Although they mitigate some branch integration challenges, they typically are cost-prohibitive and require a significant hardware investment.

By leveraging Windows Server 2003 R2 file and print technologies for branch-office environments, organizations can capture the production benefits of remote branch servers while harnessing administrative efficiencies of a centralized management framework.

Improved Branch Office Services with R2

Windows Server 2003 R2 delivers technologies needed for seamless integration of branch office servers into a larger enterprise ecosystem. R2 enables customers to maintain performance, availability and productivity benefits of a local branch server while avoiding connectivity and management overhead.

To achieve this vision, R2 provides a branch-office framework for deployment and management of key server roles that conceptually is:

- **Optional.** Remote clients can fail over from the local branch-office server to another server by closest site selection if local services become unavailable. They automatically fail back to a preferred server when services are restored.
- **Disposable.** The branch office server performs as a service cache that does not hold a unique state and does not require system backup. If the server fails, there is no impact on branch office functionality.
- **Replaceable.** If the branch server fails, it can be replaced. Data recovery is automated.

R2 is the first component in a wave of upcoming branch-office technologies that offers features streamlining operations for remote file- and print-servers. R2 features deliver advantages for branch office integration through:

- **Enhanced Management Tools.** Microsoft Management Console 2.1 has been expanded to include an enterprise-wide administration framework for managing file and print services. Administrators will benefit from the familiar “look and feel” of Microsoft’s standard management interface.
- **Advanced Compression Technologies.** Remote Data Compression (RDC) is a WAN-friendly compression technology that replicates only the changes needed to ensure file consistency.
- **Centralized Data Stores.** Centralized data stores reduced the management costs of disbursed mini data centers. Replication of branch office data is automated to a central location at specified intervals when there is available bandwidth, minimizing round trips.
- **Robust File Replication.** R2 includes a completely rewritten replication engine for the Distributed File System (DFS). DFS Replication provides a multi-master file replication service that is significantly more scalable and efficient than its predecessor, File Replication Services (FRS). If WAN connections fail, data can be stored and forwarded when WAN connections become available.
- **Increased End-User Productivity.** Branch servers will provide reliable and consistent access to the latest data that end-users and applications rely on. The server employs local data to handle local requests or central servers if a local server becomes unresponsive.

File Services

One fundamental problem with integrating branch offices is the underlying dependency on file system operations. Most file-system protocols, such as UNIX’s Network File System (NFS) and Microsoft’s Common Internet File System (CIFS), do not operate efficiently over low-bandwidth or high-latency networks.

Microsoft’s R2 provides an efficient framework for server-to-server file communications. R2 employs state-of-the-art compression algorithms and efficient replication mechanisms, which ensure that files contain a minimal set of information to ensure consistency and transfers occur only when needed.

Distributed File System (DFS) Technologies

Remote Differential Compression (RDC) is an advanced WAN-compatible compression technology that optimizes data transfers over limited-bandwidth networks. Instead of transferring similar or redundant data repeatedly, RDC identifies changes within and across files (called deltas) and transmits only those changes to achieve bandwidth savings.

For example, the deltas caused by a simple title change in a 3-megabyte (MB) Microsoft PowerPoint presentation would take less than a second to replicate over a WAN in contrast to one minute or more for the entire file.

RDC also can copy any similar file from any client or server to another using data common to both computers. This effectively reduces the size of the data sent and the overall bandwidth

requirements for the transfer. Local differencing techniques (sometimes called patching) compute the differences between two local files, detecting insertions, removals and rearrangements of data. The differences are used to transform the old version to a new version.

Microsoft's internal RDC performance testing suggests that bandwidth reduction factors may reach as high as 400:1.

DFS contains a scalable, multi-mastered state-based file replication service that synchronizes file servers. It supports:

- Automatic recovery from database loss or corruption
- Scheduling and bandwidth throttling
- Multiple replication topologies
- RDC compression for WAN efficiency

DFS namespaces allow administrators to group shared folders located on different servers and present them to users as a virtual tree of folders known as a *namespace*. A namespace provides numerous benefits, including increased availability of data, load sharing and simplified data migration. Users can navigate these virtual namespaces without needing to keep track of the physical server hosting the data.

If local servers become unavailable, DFS namespace configurations provide for client failover by closest site selection and fail back to a preferred server. For example, if fail back is enabled on a DFS link that has targets in both the branch and the hub, branch clients automatically will fail over to the hub when service is unavailable.

Print Services

Windows Server 2003 R2 also offers centralized printer control for streamlining the administration of enterprise-wide printers.

Print Management Console

Through the Printer Management Console (PMC), administrators have a central interface for managing all printers connected to all print servers within a financial services organization. With PMC, administrators can monitor printer errors, deploy printer connections to clients, automatically find and install printers on a local branch office subnet, or run configuration scripts. PMC allows branch servers to perform as print servers because they are manageable remotely on a one-to-many basis.

Summary

Branch offices provide financial services organizations the ability to increase business agility by enabling employees to be closer to corporate customers. While the potential to increase responsiveness and profit exists, branch offices also carry with them significant security and operational challenges. Microsoft can help mitigate many risks imposed by branch offices with ISA Server 2006 or IAG 2007. ISA Server provides enterprise-grade network and application-layer firewalling, which protects the branch office from Internet attacks and cordons off the branch office in the event of a security breach. The IAG 2007 is a powerful SSL VPN solution that provides secure remote access to a key line of business applications from anywhere using only a Web browser. Microsoft helps solve several data management inefficiencies inherent in branch office deployments with Windows Server 2003 R2. The combination of ISA Server 2006, IAG 2007 and Windows Server 2003 R2 provide financial services organizations with a powerful suite of applications that will enhance the security and efficiency of branch-office operations.

For More Information

- **Microsoft Internet Security and Acceleration Server 2006**
<http://www.microsoft.com/isaserver/default.aspx>
- **Microsoft Branch Infrastructure Promotion**
<http://www.microsoft.com/technet/branchoffice/promo.aspx>
- **ISA Server 2006 Branch Office Security**
<http://www.microsoft.com/forefront/edgesecurity/bos.aspx>
- **Microsoft Branch Office Home Page**
<http://www.microsoft.com/technet/branchoffice/default.aspx>
- **Windows Server 2003 R2 Helps Integrate the Branch Office**
<http://www.microsoft.com/windowsserver2003/R2/branchoffice/default.aspx>
- **Improve Branch Office Security Learning Path**
<http://www.microsoft.com/technet/security/learning/branchoffice.aspx>
- **Intelligent Application Gateway 2007 Home Page**
<http://www.microsoft.com/forefront/edgesecurity/iag/default.aspx>
- **IAG 2007 Technology and Features Overview**
<http://download.microsoft.com/download/F/0/2/F0229C11-B47E-4002-A444-60207C6E11F5/IAG%202007%20Technical%20Overview-WP-200702.doc>
- **SSL VPN for Business Continuity** <http://download.microsoft.com/download/F/0/2/F0229C11-B47E-4002-A444-60207C6E11F5/SSL%20VPN%20for%20Bus%20Continuity-WP-200702.doc>
- **Microsoft Extends Secure Access Platform with Launch of Intelligent Application Gateway 2007** <http://www.microsoft.com/Presspass/press/2007/feb07/02-01IAG07PR.aspx>