



Microsoft<sup>®</sup>  
**Internet Security &  
Acceleration Server 2006**

**Securing and Accelerating Branch Office  
Communications using ISA Server 2006**

White Paper

Published: June 2006

For the latest information, please see <http://www.microsoft.com/isaserver/>

# Table of Contents

Executive Summary.....	3
Introduction .....	4
Helping to prevent Security Issues at the Branch Office from Impacting the Main Office.....	6
ISA Server 2006 Solutions for Preventing Branch Office Security Issues from Impacting the Main Office .....	6
Firewall Access Controls .....	7
Intelligent Firewall Application Inspection Filters.....	7
Sophisticated Worm and Flood Protection Controls .....	7
Integrated Intrusion Detection System and Intrusion Prevention System.....	8
Web Proxy Access Controls .....	8
Web Proxy Web Application Inspection Filters .....	8
Comprehensive Logging and Reporting.....	9
Real-Time Alerting.....	9
Reducing the Cost and Administration Overhead for Maintaining Branch Office Connectivity .....	10
ISA Server 2006 Solutions for Reducing the Cost and Administration Overhead for Maintaining Branch Office Connectivity .....	10
Remote Access VPN Server .....	11
Site-to-Site VPN Gateway .....	11
Server Application Publishing .....	12
Web Application Publishing.....	12
Flexible Deployment Options .....	12
Integrated High Availability Features .....	13
Solving Branch Office Network Employee Productivity Problems.....	14
ISA Server 2006 Solutions for Employee Productivity .....	14
Remote Access and Site-to-Site VPN Servers .....	15
High Performance Web Cache.....	15
Cache Rules.....	15
Content Download Jobs .....	15
Web Proxy Chaining Rules .....	15
HTTP Compression.....	16
Quality of Service Controls for Web Connections .....	16
Integrated NLB .....	16
Summary .....	17

## **Executive Summary**

Many companies have branch offices that need access to information stored on the main office network. A branch office connection to the main office enables branch office employees to access information on the main office content servers. Although branch office connectivity provides branch office employees the ability to quickly share and act on information, branch office connections also carry with them the risk of spreading dangerous exploits and attacks initiated by hackers and other malicious individuals. Organizations must have some method to allow secure, fast, and reliable connections from the branch office to the main office.

There are three primary challenges to branch office connectivity:

- Securing the branch office connection
- Reducing the cost and administrative overhead of the branch office connection
- Improving employee productivity by accelerating the branch office connection

A secure connection is mandatory so that viruses, worms, and other exploits coming from branch offices will not spread to the main office. Reducing the cost and administrative overhead of branch office connections is vital because without a cost-effective and streamlined solution, the company could quickly see deployment and maintenance costs spiral out of control. Employee productivity is closely aligned with the speed at which information can be accessed, so acceleration of the branch office link is a pivotal requirement.

Microsoft® Internet Security and Acceleration (ISA) Server 2006 can be used to help solve the problems of securing, managing, and accelerating branch office connections to the main office. ISA Server 2006 is an integrated firewall, Web proxy, remote access virtual private network (VPN) server, and site-to-site VPN gateway. Each of the ISA Server 2006 technologies can be applied individually or together to provide an excellent combination of security, reliability, and accessibility for branch office employees to access main office information resources.

## Introduction

Many companies have branch offices that require information stored at the main office. A branch office connection to the main office enables branch office employees to access information on main office servers. Branch office connections to the main office enable employees to quickly share and act on information. However, branch office connections also carry the risk of distributing dangerous exploits initiated by hackers and malicious mobile code. Organizations must have some method to allow secure, fast, and reliable connections from the branch office to the main office.

There are important issues that today's companies need to address regarding branch office connectivity. Some of these issues include:

- **Corporate expansion leads to proliferation of branch offices**

As the 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 brings with it infrastructure costs that include hardware and software required to connect branch offices to the main office. Today's businesses need a way to connect branch offices to the data located at corporate headquarters.

- **Telecommuting workers become a type of branch office worker**

In addition to dedicated corporate branch offices, telecommuting workers are a fast growing type of branch office worker. Telecommuting workers work from home offices, hotel rooms, and any location outside of the corporate main office. This growing force of remote workers requires access to main office information resources to the same extent as workers situated in dedicated branch office structures.

- **Branch office workers require increasing amounts of information available only at the main office**

With the increased number of branch office employees and telecommuting workers joining the company, comes increased demands for data contained at the main office. Not only are there more employees requiring access to the same information that main office employees access, but there is also an increase in the amount of main office information that these workers need to access because of server consolidation and centralization of data management.

- **Business partners require increasing amounts of information located only at the main office**

Many companies have close relationships with partners and need to connect partner networks to the main office to provide partners with information that can speed processing orders, reduce overhead in product development, share information to accelerate new business opportunities, and much more. These partner networks share much in common with conventional branch office networks, in that partners need access to the information located on the same servers in the same main office location. Companies require a method allowing partners access to information quickly and reliably without exposing other, proprietary information to which the partners must not have access.

Companies need to provide corporate branch office, telecommuting workers, and partners access to corporate data in a fast, reliable, and secure way. The corporate challenge is to enable this connectivity without sacrificing security and increasing the risk of data leakage. One powerful solution is to use ISA Server 2006 to provide connectivity, reliability, accessibility, and security resources for these off-site offices. ISA Server 2006—whether it acts in a role of Web proxy server, network firewall, or VPN server and gateway—can help solve all these problems of branch office connectivity.

This white paper examines the problems companies have when trying to provide data access to remote offices and provides solutions based on features and capabilities included with ISA Server 2006. This white paper specifically examines the problems of and solutions to:

- Helping to prevent security issues at branch offices from impacting main office security.
- Reducing the cost and administrative overhead for maintaining branch office connectivity.
- Increasing branch office employee productivity.

## **Helping to prevent Security Issues at the Branch Office from Impacting the Main Office**

Because the concept of streamlined and integrated branch office connectivity is attractive, there are security concerns that must be addressed before beginning the planning stage of a branch office connectivity solution. Branch offices pose unique security concerns because of the following issues:

- **Branch offices are less closely managed and monitored**

In most companies, the bulk of the information technology (IT) staff is stationed at the main office. While this is an accepted practice because the majority of corporate data is located at the main office, this situation can leave branch office IT staffs small, inexperienced, or even non-existent. This can lead to a lower level of management and monitoring at the branch office and potentially increase the risk of security incidents that would not otherwise occur in the more highly managed main office. Companies need a way to increase security at the branch offices 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 quickly spread to the main office**

General computer security policies tend to be more lax at branch offices, especially smaller branch offices. This might be due to a lower level of IT support for branch office computers, a more relaxed attitude about computer security practices, or because branch office computers tend to run older operating systems than those in the main corporate office. Consequently, the risk of a security event is higher at the branch office, and this can lead to infection or compromise not only of branch office computers, but also of those at the main office. The infection or attack can even spread to other branch offices. Companies need a way to prevent outbreaks at the branch offices from spilling over to the main office and beyond.

- **Visitors and part-time employees at branch offices can reconnoiter information contained on the corporate network**

In the same way that general computer security practices at branch offices are generally less rigorous than those at the main office, the same is often true for physical security. The corporate headquarters may have elaborate controls over who can enter main campus facilities, but often find a more lax approach to building access at branch offices. 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 have the ability to connect to main office information assets and potentially steal or destroy that data from the remote office. A solution is required to enable branch offices to access corporate data without putting the main office information infrastructure at risk.

Branch office issues can quickly become main office concerns if there isn't a method to prevent it. ISA Server 2006 can solve these problems by bringing state-of-the-art firewall, Web proxy, and 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.

## **ISA Server 2006 Solutions for Preventing Branch Office Security Issues from Impacting the Main Office**

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 of the roles that ISA Server 2006 can play is that of a network firewall. Network firewalls enable companies to strictly control what type of information moves through the firewall, which users can move that information, and when users can move that information. The firewall can also log and report all information crossing the firewall, including the name of the user who accessed the information and applications users used to get the information. A company can place an ISA Server 2006 firewall at the branch office to prevent unauthorized users from accessing corporate data, while at the same time enabling approved users to access work related corporate information.

### **Intelligent Firewall Application Inspection Filters**

Traditional hardware network firewalls can detect and block attacks that were popular in the early years of the Internet. These attacks take place at the network layer of the TCP/IP communications protocol. While network-layer protection is still important for information security, network-layer protection is limited in its ability to protect corporate information assets.

The problem with network-layer protection is that it does not include protection for applications that run the business. Mail servers, Web servers, news servers, database servers, file servers, media servers, CRM servers, data collaboration servers, and more are all applications that need protection. Application protection is mandatory because intruders are now more sophisticated. They aren't only interested in creating havoc, many of them prefer to steal information covertly and use it for criminal gain.

ISA Server 2006 helps protect against these types of attacks on your corporate application servers by using smart application inspection filters. When ISA Server 2006 protects corporate applications, it first checks that there are no network-level attacks. Then ISA Server uses its smart application-layer inspection filters to mitigate attacks leveraged against key corporate applications containing your company's business intelligence. ISA Server computers at the branch offices help protect against application attackers situated at branch office locations.

### **Sophisticated Worm and Flood Protection Controls**

The media is replete with stories on worm attacks that disable computers, destroy data, and significantly increase the total cost of ownership for the corporate computing infrastructure. Blaster, Sasser, Witty, and other worms have wreaked havoc on corporate networks throughout the world.

In many cases, these worms are introduced at branch office locations from an infected portable computer that is connected to the branch office network, and then subsequently spread to corporate headquarters, where the worm then distributes itself to all the other branch offices. Worms and similar exploits can disable computers, destroy data, and flood corporate Internet and wide area network (WAN) links to make communications virtually impossible until the infection is removed. The removal process 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 emanating from compromised computers at the branch office. ISA Server worm and flood protection detects worm-like behavior coming from infected computers and their connections to the main office. Not only does this help mitigate the spread of infection, it significantly reduces chances that a branch office worm infestation will saturate the branch office link to the main office. This protection enables users to continue to access data stored on main office servers to complete their work.

## **Integrated Intrusion Detection System and Intrusion Prevention System**

Corporate security officers and network administrators need to know when potential attacks start so they can respond quickly. To meet this goal, intrusion detection systems can be introduced to detect a possible attack and alert key personnel about the situation. An intrusion prevention system builds on the intrusion detection system by blocking attacks detected by the intrusion detection system.

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

## **Web Proxy Access Controls**

To this point, this white paper has focused on using ISA Server 2006 as a branch office firewall. Many companies have an existing firewall infrastructure and cannot or do not want to replace the current infrastructure because of costs and other fiscal and operational considerations. The problem that these companies have is that these firewalls provide only simple network-level protection, and they want to improve their security by bringing in an application-layer inspection device without displacing these firewalls.

This problem is solved by introducing an ISA Server 2006 Web proxy to the branch office. Web proxies can be used to control all Web traffic moving between branch office computers and the main office as well as traffic to and from the Internet. A Web proxy can be added anywhere on the branch office network in the same way as a file or mail server. This doesn't require complex changes to the corporate networking infrastructure and can provide strong Web proxy-based access controls.

ISA Server 2006 includes a powerful Web proxy enabling the company to control what information that 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 firewalls at the branch office and provides strong user account-based access control over corporate information flow. For example, if a user is not authorized to access data on a particular Web server at the main office or on the Internet, that user's access is denied. Strong Active Directory® directory service-integrated user-based or group-based access controls are the hallmark of the ISA Server program's exceptional ability to control, record, and report all communications coming from branch office locations.

## **Web Proxy Web Application Inspection Filters**

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

ISA Server 2006 includes a number of technologies that can be used to protect both users and Web sites. One of the more powerful features is the ISA Server Hypertext Transfer Protocol (HTTP) 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 Web sites if either the Web site or the user's computer is compromised.

In addition to the built-in ISA Server 2006 Web inspection security features, ISA Server includes a Web protection extensibility component. Companies can use the ISA Server 2006 Software Development Kit (SDK), which comes free with ISA Server 2006, to create custom Web security application filters, or they can purchase prebuilt Web security additions from third-party vendors.

For more information about Web security enhancements for ISA Server 2006, visit the Microsoft ISA Server partners Web site at <http://www.microsoft.com/isaserver/partners/default.msp>.

### **Comprehensive Logging and Reporting**

Security and compliance managers must have detailed information about data that users access through the branch office Web proxy. Detailed logging should include the name of the user accessing information, the day and time the user accesses this information, and the nature of the information the user accesses during the branch office 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 Web proxy logging and reporting provides all this information and much more. The default log settings enable the ISA Server 2006 Web proxy to gather detailed information about user activity, and then create illustrative reports using the ISA Server 2006 built-in reporting engine. You can customize reports to provide detailed summary information about user activity when connecting to the corporate and Internet Web servers, and integrated third-party reporting applications can be used to provide highly specific information about user activity through the ISA Server 2006 Web proxy.

For more information about third-party enhancements to ISA Server 2006 reporting, see the [Microsoft ISA Server 2006 Partners Web site](#).

### **Real-Time Alerting**

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

ISA Server 2006 is fully supported by the Microsoft Operations Manager (MOM), which enables the ISA Server computer to be part of a centrally managed services and 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 ISA Server 2006 or MOM administrators using MOM alerting.

For more information about Microsoft Operations Manager, see the MOM home page at the [Microsoft Operations Manager Web site](#).

## **Reducing the Cost and Administration Overhead for Maintaining Branch Office Connectivity**

Branch office connections to the main office network and information resources can be potentially expensive to deploy, manage, and maintain. Some of the major cost and overhead-related issues regarding branch office connectivity to the main office include the following:

- **Dedicated WAN links are a major line item in network infrastructure budgets**

There are a number of ways you can join branch office networks to the main office. One of the most common is to purchase a dedicated WAN link such as a T1 or T3 line. Dedicated WAN links are reliable and can be purchased to support the level of bandwidth required for branch office communications to the main office. The challenge with dedicated WAN links is that they can be prohibitively expensive. Companies need a way to connect branch office employees to the main office in a more cost competitive way. One popular alternative to dedicated WAN links is a site-to-site VPN. Site-to-site VPNs use virtual private networking technologies to create a virtual intranet connection between the main and branch offices over commodity priced Internet connections.

- **Site-to-site VPNs can be difficult to deploy, configure, and manage**

Some organizations may be considering site-to-site VPN links or have them already in place and might want to consider alternatives because site-to-site VPN connections can potentially be difficult to deploy, configure, and manage. These companies seek alternatives to site-to-site VPN links, which provide the same level of application and content access that site-to-site VPN connections provide while avoiding potential downsides of VPN connectivity.

- **High availability equipment is expensive to acquire, configure, and maintain**

Branch offices need reliable connections to the main office. This often requires that multiple gateways to the main office be purchased, set up, and maintained to ensure redundancy in case of link failure. High availability equipment can be prohibitively expensive. Organizations need a way to provide high availability in a cost-effective manner.

- **Help desk costs for application configuration issues add a hidden expense**

One of the hidden costs inherent in all branch office deployments is Help desk overhead. These expenses are related to the cost of reconfiguring user applications based on user location. Branch office employees frequently leave the branch office and take their portable computers to the main office or to off-site locations. Businesses require a flexible solution where users can move to any location and reliably connect to business information without complex and expensive application reconfiguration.

Whether your company's branch offices use a dedicated WAN link, site-to-site VPN connections, or even no physical or virtual connectivity to the main office, ISA Server 2006 can help reduce the cost and administrative overhead involved in maintaining branch office connections.

### **ISA Server 2006 Solutions for Reducing the Cost and Administration Overhead for Maintaining Branch Office Connectivity**

ISA Server 2006 solves the problems related to cost and complexity of branch office connectivity using the following technologies:

- Remote access VPN server
- Site-to-site VPN gateway
- Server application publishing

- Web application publishing
- Flexible deployment options
- Integrated high availability features

## **Remote Access VPN Server**

A remote access VPN server can accept VPN connections from individual computers at remote locations and provide those computers with a level of access to main office corporate data assets similar to access by computers physically wired to the corporate local area network (LAN).

Remote access VPN connections can be initiated from computers located anywhere in the world. Remote access VPN connections are especially popular among telecommuters. The challenge companies have with remote access VPN connections is that these connections must be secure, and users must have access restricted only to the information they require.

ISA Server 2006 solves the problem of securing remote access VPN connections by providing a built-in remote access VPN client and server. The ISA Server 2006 remote access VPN server can be placed on the main office corporate network, and then telecommuters and branch office workers can initiate the VPN connection to the main office using the integrated Microsoft Windows® VPN client. ISA Server 2006 Enterprise Edition can support an unlimited number of VPN client connections based on server hardware and Internet bandwidth constraints.

Connections from VPN clients are secured by the main office ISA Server 2006 remote access VPN server. Unlike many hardware-based VPN servers, the ISA Server 2006 remote access VPN server enables a company to tightly control access based on the user account connecting to the VPN server. ISA Server 2006 supports tightly controlled user-based and group-based access control for remote access VPN clients, so that users are allowed to access only the information they require to accomplish their work, but nothing more. In addition, ISA Server 2006 performs both stateful packet and application-layer inspection over all VPN client connections.

## **Site-to-Site VPN Gateway**

Remote access VPN client connections must be established one at a time. If a branch office has 50 users, each user must connect to the main office remote access VPN server individually. If each user needs to connect to the main office at the same time, this requires 50 simultaneous remote access VPN connections to the main office remote access VPN server. Each remote access VPN connection uses some VPN server processor and memory resources and potential exists for a hardware-based limit on the number of remote access VPN connections.

A popular way to solve this problem is to connect branch offices to the main office using a site-to-site VPN connection. In contrast to the remote access VPN, a site-to-site VPN connection connects the entire branch office network to the corporate headquarters. This allows all employees at the branch office connectivity to the main office using a single site-to-site VPN connection. This reduces load on the main office VPN gateway and enables companies to connect many more branch office employees to the main office. The challenge is to ensure that users are able to connect only to those application servers required to perform their work.

ISA Server 2006 solves these problems by including an integrated site-to-site VPN gateway. The site-to-site VPN gateway enables companies to place an ISA Server computer at the branch office and create a site-to-site VPN connection to the main office. The main office site-to-site VPN gateway can be another ISA Server 2006 computer, or a third-party VPN gateway. ISA Server solves security issues for branch office employee access by using the same user-based and group-based access control that the remote access VPN server provides. Branch office employees access information at the main office based on their account privileges. If the user's account has access to the main office information requested, access is allowed. Employees are denied access to all information for which they have no need to access.

In addition to strong user-based and group-based access controls over branch office connections, ISA Server 2006 provides the same level of stateful packet and application inspection that it provides for all other communications moving through the firewall.

## **Server Application Publishing**

Some companies want to avoid using site-to-site VPN connections. They want to provide branch office users access to information on the corporate network but do not want to incur any additional administrative overhead incumbent in designing, deploying, and maintaining site-to-site VPN connections. These companies want to put together what is essentially a virtual VPN. The challenge is how to allow this type of access and ensure secure connectivity.

ISA Server 2006 can solve this problem using its built-in server application publishing features. Using ISA Server 2006, you can create server publishing rules for the main office applications that branch office employees need to access. Encrypted communications for e-mail, file transfer, and other data can be configured to ensure privacy. Access controls at the main office ISA Server 2006 firewall can be configured to ensure only branch offices are able to connect to these corporate resources.

## **Web Application Publishing**

Companies not wanting to deploy site-to-site VPN links, or who have existing dedicated WAN links that they do not want to replace, need a method to provide secure Web connections from branch offices to the main office. Off-site employees also need a way to access Web application servers.

ISA Server 2006 solves this problem by providing a comprehensive Web application toolset. Using built-in ISA Server Web publishing wizards, organizations can easily provide secure branch office access to Microsoft Exchange Web services (including Microsoft Outlook® Web Access, Outlook Mobile Access, Microsoft Exchange ActiveSync®, and Outlook remote procedure call (RPC) over HTTP), Microsoft Windows SharePoint® Services, and any other Web-based line of business application. ISA Server 2006 Web application publishing can be easily configured to allow users access only to those Web applications that they require for their work and prevent access to extraneous information.

## **Flexible Deployment Options**

As discussed earlier, companies have the option to use a dedicated WAN link, a remote access VPN connection, a site-to-site VPN, or even use no physical or logical connectivity and leverage the ISA Server application publishing wizards. The company's challenge is to deploy a branch office access and security solution in the most cost-effective and secure way possible. This means introducing the application security solution in such a way as to minimize disruption of the existing network infrastructure.

ISA Server 2006 solves this problem by providing an array of branch office deployment options:

- **Single interface Web proxy server**

An ISA Server computer with a single network interface card (NIC) can be placed anywhere on the branch office network to provide secure access to main office Web applications. This single NIC solution works for branch offices with dedicated WAN links to the main office, a site-to-site VPN connection, or no physical or virtual connection to the main office. The single NIC deployment requires no changes to the current networking infrastructure and does not require input from the network infrastructure team.

- **Multiple interface network firewall for existing WAN connections**

An ISA Server computer with multiple NICs can be placed at the branch office to provide strong network and application security for branch office connections. In this configuration,

ISA Server provides exceptionally strong user-based and group-based access controls over all content that branch office users might access at the main office and comprehensively logs and reports all of these connections. In addition, the ISA Server computer can stop network worms and other flood-based attacks when it is an inline device.

- **Multiple interface network firewall and VPN gateway for site-to-site VPN**

Another powerful deployment option for ISA Server 2006 is to make the ISA Server computer a network firewall and site-to-site VPN gateway for the branch office. This scenario is ideal for organizations that do not have existing dedicated WAN links or that want to save money by moving away from dedicated WAN link infrastructures. The ISA Server 2006 firewall and site-to-site VPN gateway provides secure access to the Internet and branch office by acting as a network and application protection choke point for dangerous communications.

- **Multiple interface network firewall for remote application access without VPN connectivity or WAN links**

For those organizations that don't have dedicated WAN links and don't want to deploy a site-to-site VPN, ISA Server 2006 can be used as a network and application protection firewall that provides access to resources hosted at the main office over the Internet. An ISA Server 2006 firewall or Web proxy at the main office completes the secure application access solution by using secure application and Web publishing.

## **Integrated High Availability Features**

Branch offices require reliable access to main office data. Each hour of lost connectivity can cost thousands of dollars in lost sales and opportunities. If the branch application security device providing connectivity to the main office becomes unavailable, users will not be able to securely access main office information. Companies not only need a fast and secure connectivity solution, but also a reliable solution.

ISA Server 2006 Enterprise Edition solves the problem of ensuring highly reliable access to main office information by including integrated Network Load Balancing (NLB). NLB enables organizations to create collections of two or more ISA Server computers at branch offices and the main office and have these collections automatically take over duties of ISA Server computers that are disabled. If a branch office employee connects to the main office through one ISA Server computer and that ISA Server computer becomes disabled, other ISA Server computers in its group take over so that users are unaware of the outage and continue working.

NLB in ISA Server 2006 works for all deployment modes, including firewall, Web proxy, remote access VPN, and site-to-site VPN gateway.

## **Solving Branch Office Network Employee Productivity Problems**

Branch office employees need to get their work done as quickly and efficiently as possible. Employee productivity can be impaired if information required to complete their work is not provided to them quickly. Productivity can come to a stop if critical information is unavailable because of connectivity or bandwidth problems.

Companies with branch office employees can suffer low employee productivity due to slow or unreliable access to data in a number of situations. Some of these include:

- **Main office and Internet servers are slow to respond or offline**

The Internet is not a reliable network. There are many network devices between the branch office user and Internet Web sites to which the user needs access. If any link between the branch office and the desired Web site becomes unavailable, users can become frustrated and unable to complete their work. One solution to this problem is to use a Web proxy. Web proxies can cache content from mission-critical Web sites on the Internet or main office so that even if the Web sites are slow to respond or offline, content can still be delivered to the employee from a Web proxy cache.

- **Corporate Internet and WAN link bandwidth is saturated**

As Internet use becomes increasingly critical, so do the demands on the Internet link. With increased use of existing corporate Internet connections comes the prospect of bandwidth saturation. High speed and reliable Internet connections are expensive. Upgrading Internet connections not only incurs the increased expense inherent in the service, but potentially additional costs related to hardware and software upgrades necessary to support the connection. Branch office links to the main office suffer from the same bandwidth challenges as the number of users who need information from the main office increases. Technologies such as Web proxy and VPN can reduce the bandwidth required to obtain the same amount of information and reduce load on WAN and Internet links.

- **Intranet servers are unavailable**

Users at main and branch offices often require access to large amounts of information on corporate Web servers. Access to this information is critical for almost every employee on the network, including those at branch offices. If mission-critical servers become unavailable, workflow could come to a stop. Branch offices are an even higher risk of being unable to access information, because they use comparatively unstable dedicated WAN links or site-to-site VPN connections. By introducing a caching Web proxy at the branch office, branch office employees always have access to data on the main office Web server.

- **Branch office bandwidth is limited by slow WAN and VPN connections**

Branch office employees can still have productivity limited even when links to the main office are available. Like the overtaxed corporate Internet connection, branch office WAN or site-to-site VPN links can become saturated by the increased burden of application traffic. Accessing even a small amount of information over busy lines can slow employee data access and productivity. Caching, Web proxy and VPN technologies work together to increase availability so that employees can access data more quickly.

## **ISA Server 2006 Solutions for Employee Productivity**

ISA Server 2006 solves the problems listed in the previous section by using the following technologies:

- Remote access and site-to-site VPN servers

- High performance Web cache
- Cache rules
- Content download jobs
- Web proxy chaining rules
- HTTP compression
- Quality of Service controls for Web connections
- Integrated NLB

### **Remote Access and Site-to-Site VPN Servers**

ISA Server 2006 remote access VPN servers and site-to-site VPN gateways support all industry standard VPN protocols, including the Point-to-Point Tunneling Protocol (PPTP), Layer Two Tunneling Protocol over Internet Protocol security (L2TP/IPsec), and IPsec tunnel mode. ISA Server 2006 VPN technologies enable a company to accelerate access to data moving over VPN connections by compressing data within the VPN. Data compression within the VPN tunnel can potentially double the amount of traffic that can move over an Internet link, enabling data throughput at almost twice link speed.

### **High Performance Web Cache**

ISA Server 2006 includes a high performance in-memory and disk-based Web cache. The in-memory cache allows the ISA Server computer to hold the most popular and most recently accessed Web content in ultra-fast RAM. Less popular and older Web content is stored in hard disk-based cache. The combination of in-memory and disk-based caches enables ISA Server to return gigabytes of cached Web content at near wire speed to main and branch office employees.

### **Cache Rules**

There is a wide variety of content from Internet and corporate Web servers that can be cached. However, a company may not want to cache all cacheable content. For example, the company may choose to cache only work-related information. The company may want to cache static content but not dynamic content, because the latter changes frequently. Another company may want to cache all content, even if the Web server hosting content does not indicate content as cacheable.

ISA Server 2006 provides organizations with a high level of control over many aspects of caching, including the following:

- Which content is cached
- How long the content is cached
- Maximum size of cached Web objects
- Total amount of content cached over a period of time

### **Content Download Jobs**

Some content must always be available to branch office employees even when the Internet connection to the main office fails. ISA Server 2006 can make this content available continuously using the ISA Server content download job feature. A content download job can be configured to automatically download into the ISA Server Web proxy cache information that must always be available. Content download jobs can also be scheduled on a custom basis so that the Web proxy cache is automatically updated with the latest version of required content.

### **Web Proxy Chaining Rules**

Businesses often deploy multiple layers of Web proxy servers. Web proxy servers can be connected to other Web proxies in a communications chain allowing connecting Web proxies to benefit from larger Web caches on the Web proxies to which they're connected.

A common example of this type of Web proxy communications network is a branch office Web proxy linked to a main office Web proxy. In most cases, the main office Web proxy has a much larger Web cache than the branch office. This enables the branch office Web proxy to receive content from the main office Web proxy instead of going to Internet Web servers to receive content.

The company saves the cost of Internet bandwidth that would otherwise be required to obtain content from the Internet Web servers and content is delivered to branch office users more quickly. ISA Server 2006 allows you to create Web proxy chaining rules to create high performance Web proxy networks.

### **HTTP Compression**

You can transport less data faster than more data over a network connection. ISA Server 2006 takes advantage of this fact by reducing the size of information crossing the network over a Web connection. Using industry standard methods of HTTP compression, ISA Server 2006 compresses information it sends and receives over the network. HTTP compression reduces the bandwidth required to communicate over the intranet to the Internet and over branch office WAN links. Because less bandwidth is required, employees are able to connect to information resources much more quickly.

### **Quality of Service Controls for Web Connections**

There is a tremendous variety of traffic moving over corporate networks. Network routers, firewalls, switches, and other devices make a *best effort* attempt to deliver data over the network. All connections are treated equally. Many companies recognize that connections and data transfers to and from some servers are more important than others. Quality of Service (QoS) controls allow you to prioritize communications to key corporate assets.

ISA Server 2006 includes a built-in QoS feature enabling you to give higher priority to connections to key corporate and Internet servers. Users who connect to these servers receive information much faster than when they connect to other servers for which there is no preferential treatment. The ISA Server 2006 QoS enables you to streamline communications to essential sites while providing *best effort* connections to sites that are not mission critical.

### **Integrated NLB**

While other ISA Server 2006 technologies discussed in this section help accelerate access to main office resources by branch office employees, NLB is targeted at making this information highly available and to minimizing downtime. ISA Server 2006 can be configured in an NLB array of servers at the main office, the branch office, or both to ensure that branch office users are able to access corporate information even when one or more of the ISA Server computers are disabled.

## Summary

Many companies have branch offices that need access to information stored on the main office network. A branch office connection to the main office enables branch office employees to access information on the main office content servers. While branch office connectivity to the main office provides branch office employees the ability to quickly share and act on information, these branch office connections also carry with them the ability to speed the spread of dangerous exploits and attacks initiated by hackers and other malicious individuals. Organizations must have some method to allow secure, fast, and reliable connections from the branch office to the main office.

There are three primary challenges to branch office connectivity:

- Securing the branch office connection.
- Reducing the cost and administrative overhead of the branch office connection.
- Improving employee productivity by accelerating the branch office connection.

A secure connection is mandatory so that viruses, worms, and other exploits originating at the branch office do not spread to the main office network. Reducing the cost and administrative overhead of branch office connections is vital because without a cost-effective and streamlined solution, the company could quickly see deployment and maintenance costs spiral out of control. Employee productivity is closely aligned with the speed at which information can be accessed, so acceleration of the branch office link is a pivotal requirement.

ISA Server 2006 can be used to help solve the problems of securing, managing, and accelerating branch office connections to the main office. ISA Server 2006 is an integrated firewall, Web proxy, remote access VPN server, and site-to-site VPN gateway. Each of the ISA Server 2006 technologies can be applied individually or together to provide an excellent combination of security, reliability, and accessibility for branch office employees to main office information resources.



This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

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.

© 2006 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows Server, Exchange, Internet Security and Acceleration (ISA) Server 2006, Microsoft Operations Manager, Outlook, PowerPoint, SharePoint, Windows Mobile, are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.