# Perimeter Network Security for Branch Offices with Microsoft Internet Security and Acceleration (ISA) Server 2000

Michael Arter

GIAC Security Essentials Certification (GSEC)
Practical V1.4b Option 1
November, 2003

## Table of Contents

# Abstract

Many branch office environments today are connected to the Internet through a dedicated frame relay circuit through the home office. This has generally been a secure and reliable connection, but is in many cases a bottleneck due to the typically low connection rates and increased demands for bandwidth. Advances in technology and increased competition from internet service providers bring new choices to the small or branch office environment for internet connectivity. Broadband technology now offers a small or branch office a much faster and in many cases less expensive alternative for connectivity to the Internet. However, these connections are "always up" and directly connected to the Internet, and as such represent increased exposure and risk of external attacks vs. a frame relay connection to a trusted network.

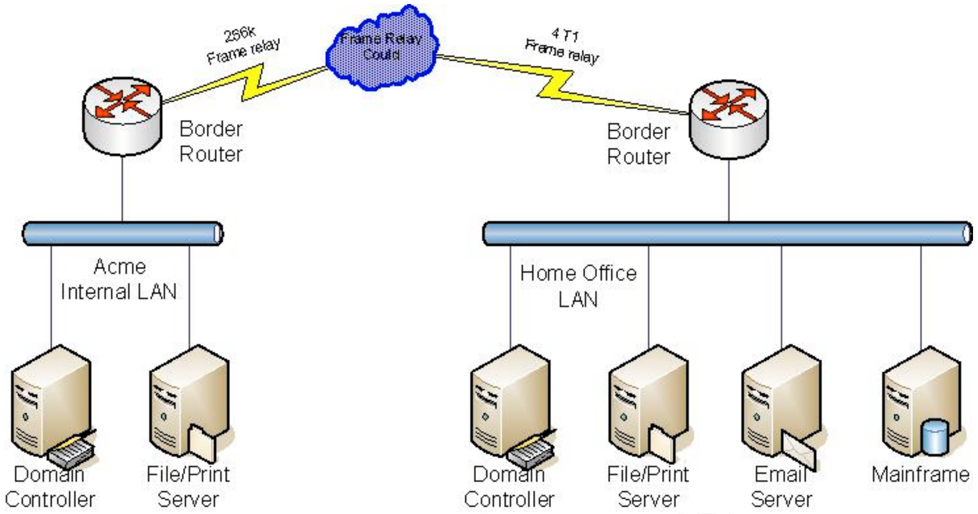
This Practical will look at the issues and challenges a hypothetical branch office faces from a perimeter security standpoint when directly connected to the Internet. It will then provide an overview of Microsoft's Internet Security & Acceleration (ISA) Server 2000 firewall and proxy server features and options, and offer a perimeter security solution using ISA Server 2000 as part of an overall perimeter security strategy.

# Branch Office Scenario

## *Acme Fire and Casualty*

This Practical will look at a hypothetical branch office environment consisting of 500 users in a suburban office complex in a mid-sized city, with a small onsite IT staff. Our company, Acme Fire and Casualty, is a regional insurance underwriter with a parent company on the east coast. Acme's user mix consists of remote and local sales, field adjusters, claims processing, clerical, and administrative or support tasks. About half the users are office based, the rest either home based telecommuters or remote users traveling on the road.

Acme is currently connected to the home office as shown:



Like many branch office environments, Acme has relied on the frame relay connection to the home office for many if not most IT services. It has given the branch office a secure, generally reliable, but slow connection that has recently become a bottleneck due to increasing user demands, and does not provide a productive option for remote users.

Corporate acquisitions and growth have brought some major changes to Acme and its parent company. IT Services are being decentralized to provide a more flexible administrative model and to accommodate growth. Corporate management has instructed the IT staff to accomplish the following goals:

- Provide all necessary network services locally, including user logons, file and print, email, claims entry, Internet access, etc., to eliminate reliance on home office network
- Assume delegated administrative and support duties for local users
- Provide secure connection to the Internet
- Provide secure connections between branch and home office
- Provide secure connections for telecommuters and remote users
- Provide secure access to claims entry for field adjusters
- Provide email access for remote users
- Eliminate the network connectivity bottleneck
- Monitor and enforce compliance with corporate policies for internet usage

## The Challenge

Acme's IT staff has many questions. "How can we provide the users with all these new services and still be secure? What are the threats? How can we identify and protect against them? How can we know if we're succeeding?" We'll answer those questions by taking a look at the challenges Acme now faces with a new internet connection, and then designing an overall perimeter security solution to respond to those challenges.

## *The Internet*

Stephen Northcutt's Inside Network Perimeter Security begins with a question:

> The security of your network is evaluated daily. A rich question to ask is, "Are you the one doing it?" The answer, hopefully, is that someone on your side is involved in assessment, but overwhelming evidence reports that you are not alone. Internet facing systems (computers with IP addresses that can be reached from the Internet) receive between seven and hundreds or even thousands of attack attempts every day. Many of these are simple scans and probes that we know how to defend against, but others catch us by surprise and the next thing we know we are in clean up mode.[1]

Connection to the Internet is a necessity for productivity in any branch office environment. Connection to the internet comes with its risks, not only from a server operating system and application standpoint but from client operating systems as well.

Attacks can target virtually any operating system. The SANS Institute was established in 1989 as a cooperative research and education organization. SANS publishes a list of the top 10 vulnerabilities for Windows and the top 10 for Unix/Linux. According to SANS:

> The vast majority of worms and other successful cyber attacks are made possible by vulnerabilities in a small number of common operating system services. Attackers are opportunistic. They take the easiest and most convenient route and exploit the best-known flaws with the most effective and widely available attack tools. They count on organizations not fixing the problems, and they often attack indiscriminately, scanning the Internet for any vulnerable systems. The easy and destructive spread of worms, such as Blaster, Slammer, and Code Red, can be traced directly to exploitation of unpatched vulnerabilities"[2]

A review of those vulnerabilities confirms that not only server operating systems and applications are popular attack targets, but now with client machines interacting with the Internet, many popular attacks have evolved against client operating systems and particularly browsers. Patches are created to fix those vulnerabilities, but sometimes those patches don't get applied in a timely manner. Perimeter security systems that can look for those attack signatures can protect unpatched systems by blocking the attack at the firewall instead of letting the traffic through to the internal network.

What's being done about this? Not as much as could be done. Unfortunately, many times nothing is done to protect against known vulnerabilities. USA

[1] Northcutt, pg 3.
[2] SANS, pg 1.

Today's *USA Today Snapshots* recently summarized a portion of the results of 451 business technology and security professionals surveyed by Information Week as to the barriers in implementation. The responses to the question "What are the barriers to effective computer security in your organization?" were as follows[3]:

- 46% cited increasing sophistication of threats
- 42% cited capital expense
- 41% cited lack of time
- 25% cited pace of change or lack of qualified staff
- 24% cited complexity of technology
  Note: multiple responses were allowed.

Threats can come from within also. Users may not always follow corporate policies and guidelines, particularly when the internet is available. Users may download and open email attachments, executables or any number of potentially dangerous actions. User productivity can also suffer due to visiting inappropriate websites during work hours. Some method of monitoring user activity, enforcing corporate policies, and reporting those results is needed.

## *Security Strategies*

Many companies dedicate a lot of resources to "security" but it's not always effective. Many times a company will implement a good security strategy in one area but not understand or ignore other area with just as much exposure. An overall strategy must be adopted with proper balance of resources expended to all areas.

Information security expert and author Eric Cole feels that many companies want to implement good security strategy but they just don't do it. In an article titled "How to secure your Company", published by online magazine Computerworld, Eric discusses four strategies that every company should apply when designing a security strategy[4].

- Know thy system
- Principle of least privilege
- Defense in depth
- Prevention is ideal, but detection is a must

The first principle is to "know thy system". Organization IT staffs need to fully understand what resources and services are present in their network environment to know what they're trying to protect. Knowledge of internal resources is critical to know what and how to defend against the vulnerabilities that those resources. What services are running? What ports are open? What

[3] Gannett, pg. 1
[4] Cole, pg 1.

kind of traffic is present on the network? Only after those issues are identified can a good strategy of defense can be developed.

Next is the "principal of least privilege". Acme should evaluate the necessary permissions required to accomplish the intended task, grant those permission and no more. This requires substantial time and effort, but in the long run it results in a much more secure environment.

A "Defense in depth" strategy is an effective and widely accepted strategy to secure a perimeter environment. This can be defined as two lines of perimeter defense, back to back, each based on a different platform, operating system or vendor product. The objective is to prevent the exploit that penetrated the first line of defense from automatically penetrating the second. Nothing is totally secure, but if you can present two different barriers to reaching the internal network, at a minimum it will take that much longer for attackers to penetrate the perimeter security.

Finally, the concept of "Prevention is ideal, but detection is a must" assumes the inevitable, that penetration of the perimeter security system will occur. No system is impenetrable, and knowing when and where you are being attacked is perhaps as essential as preventing that attack in the first place. Intrusion Detection systems, both network and host based, auditing and logging are all essential tools to know when and where network resources have been compromised, and can in some cases lead to identification of the intruder.

## Perimeter Security

Now that our branch office will be connected directly to the internet, perimeter security is one of the first areas Acme must consider. A comprehensive perimeter defense system must be implemented to protect the corporate assets connected to the internet while still allowing users access to necessary resources to do their job. More often than not, the first line of perimeter defense is a firewall.

## Firewalls

A firewall can be loosely defined as any device that controls network traffic based on rules. The National Institute of Standards and Technology (NIST) in their publication SP-800-10, defines a firewall as:

> …an approach to security; it helps implement a larger security policy that defines the services and access to be permitted, and it is an implementation of that policy in terms of a network configuration, one or more host systems and routers, and other security measures such as advanced authentication in place of static passwords. The main purpose of a firewall *system* is to control access to or from a protected network

(i.e., a site). It implements a network access policy by forcing connections to pass through the firewall, where they can be examined and evaluated.[5]

## Types of Firewalls

Firewalls fall into one or more of the following three categories, based on their functionality. Those three categories and a brief explanation are:

- **Stateless packet filtering firewall**. A stateless packet filtering firewall operates at Layer 3 of the OSI model, and inspects basic information within every packet entering and leaving the firewall. This is typically deployed at border routers. It is faster that proxy or stateful firewalls. Packet filter firewalls can be configured to block many well-known attacks such as Denial of Service (DoS) attacks using ICMP, Ping of Death, source routed attacks, and out-of-band attacks such as SYN-FIN attacks, etc.
- **Stateful packet filtering firewall**. A stateful packet firewall keeps track of connections in a state table and analyzes packets based on those connection states. A stateful firewall knows when traffic attempting to enter the network is in response to a connection established from within the network, and can deal with connections requiring secondary connections, dynamic ports, etc. A stateful firewall can also recognize and block traffic that is part of an unestablished, non-permitted connection, such as attempts at reconnaissance.
- **Proxy/application layer firewall**. Proxy/application layer firewalls are able to inspect traffic above the packet level and can inspect the entire packet. They can intermediate between the source and the destination so that internal clients never actually connect with the target; the proxy server makes the connection and inspects the entire packet to assure that the protocol and port are compliant with the rules database. Special plugins and filters allow application layer firewalls to be configured to inspect and apply rules for specific applications.

Because both stateless and stateful packet filter firewalls are dependant on transport-layer source and destination ports, many common network attacks are able to bypass those firewalls and exploit weaknesses by tunneling data within packets destined for commonly used ports such at HTTP over port 80. Windows uses RPC protocol extensively, and most application layer firewalls do not inspect RPC traffic, leaving the environment vulnerable to RPC exploits. ISA Server 2000 has filters which are designed to inspect RPC and other Windows specific protocols and traffic, giving it a significant advantage over other firewall products when deployed in a Windows environment.

[5] NIST, pg 1.

### Defense in Depth

A “Defense in Depth” strategy is a widely accepted best practice design approach to perimeter security. The National Security Agency (NSA) states that

> “Defense in Depth is practical strategy for achieving Information Assurance in today’s highly networked environments. It is a “best practices” strategy that relies on the intelligent application of techniques and technologies that exist today.”[6]

This strategy generally uses two layers of defense implemented in a back-to-back configuration so that an intruder must pass through two separate, distinct barriers. The most effective use of that strategy is to implement those two layers using different vendor products or technologies, so that when one layer is compromised, the second layer represents a new challenge to the intruder.

## Acme’s Solution

To meet management’s new directives, the IT staff has proposed the following:

- Install servers locally to provide user directory and related services and establish secure replication with home office servers
- Replace the current fractional T1 frame relay connection with local broadband service directly connected to the internet at 1024kbps
- Install a Defense in Depth perimeter firewall system
- Install VPN tunnel between branch and home office
- Install a VPN server for access by remote users
- Install a local mail server and allow access to remote users
- Install a secure web server for claims form entry

Until now, Acme had relied on the security protection provided by the home office. This responsibility will now transfer to the branch office. Acme must find a solution that allows them to quickly and effectively implement a perimeter protection system that allows users to accomplish their work, keep outside intruders from gaining access to the corporate network, and perhaps as important as anything, integrate with the existing Windows Active Directory environment and provide a way to manage the solution without adding staff or extensive training.

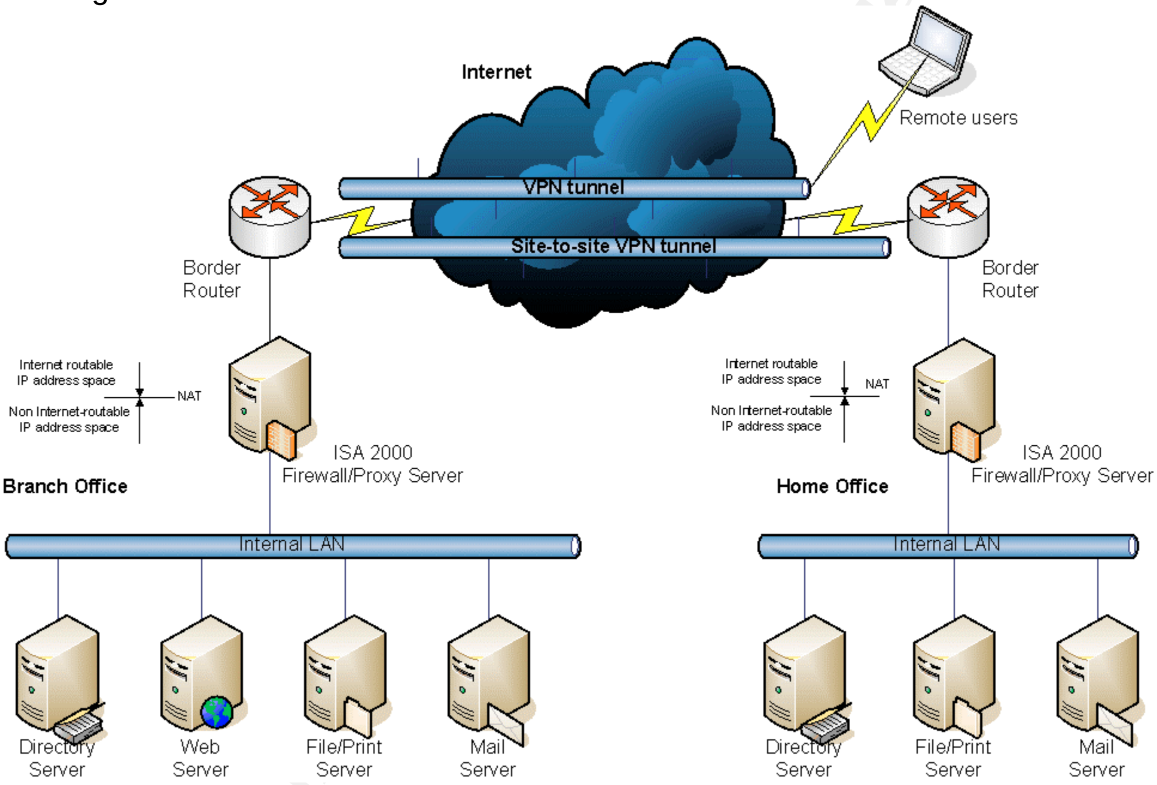
After working with corporate IT in identifying and evaluating the internal resources and services Acme is trying to provide and protect, the IT staff has decided to implement a back-to-back perimeter security system using a border router running a Firewall IOS and Microsoft Internet Security & Acceleration (ISA) Server 2000 as an integrated firewall and proxy server. All access to and from the internal network will pass through this system. The border router will perform stateful packet filtering and use access control lists, and the ISA server will be

[6] NSA, pg 1.

configured as an integrated firewall and proxy server. Web, FTP, VPN and web based email will be provided, and an encrypted VPN tunnel to the home office. Corporate has decided to implement ISA Server 2000 as a part of their perimeter security system as well, which will allow both a centralized and local policy administration of ISA. Corporate will utilize ISA for VPN connections to allow for secure site-to-site VPN connections from branch offices.

### A Perimeter Security System Design for Acme

Acme has chosen to implement a Defense in depth perimeter security system utilizing back to back firewalls as shown:



This design will allow Acme to meet all the requirements of the corporate directives. A review of those directives and the choices Acme made to meet those directives will be reviewed in a subsequent section, but first an overview of ISA Server 2000.

### Microsoft Internet Security and Acceleration Server (ISA) 2000

#### Background

Previous versions of Proxy Server, ISA's predecessor, were effective as proxy servers, but were not known for their effectiveness as firewalls. Microsoft's Internet Security and Acceleration Server (ISA) 2000 has evolved into an extensible, scalable, enterprise firewall and integrated web cache proxy server and has achieved multiple independent industry certifications as a firewall.

## Industry Certification

To establish the credibility of ISA 2000 as a firewall, Microsoft applied for and achieved certification by ICSA Labs, a subsidiary of TruSecure Corporation. ICSA Labs is recognized as a leader in information security product certification. Microsoft achieved ICSA certification for ISA Server 2000 in January 2001. Author Dr. Tom Shinder, in his book Configuring ISA Server 2000 states:

> The speed at which Microsoft was able to achieve ICSA certification was unusually fast. As a result of the ICSA certification and the fact that ISA Server is able to provide the same degree of security that people have come to expect from products that have had ICSA certification, ISA server is likely to be adopted on a much wider scale that Proxy Server 2.0.[7]

Microsoft recently announced that ISA 2000 has also achieved Common Criteria certification. Microsoft states on their website:

> It is a Microsoft corporate goal to provide rigorous third-party auditing for all Microsoft security products, at a level comparable to or better than that of other vendors. As a result, Microsoft is committed to building on the CC certification achieved by ISA Server 2000 by pursuing higher-level certifications.[8]

Common Criteria's website states that "The Common Criteria.org website serves as an international Common Criteria Support Environment (CCSE). The site offers international Evaluation Laboratories, Sponsors, Developers and other interested parties an arena for raising issues about the content and interpretation of the Common Criteria (CC)." An overview of the Common Criteria Organization is available at http://www.commoncriteria.org/docs/aboutus.html.

## Architectural Overview

ISA Server 2000 is a scalable, integrated multilayer firewall and web cache server. The firewall provides filtering at the packet, circuit and application layers. It uses stateful packet filtering to examine all data passing through the firewall, and policy based routing and rulesets. The web cache server provides significant improvement in network performance and end user experience by storing frequently accessed web content. The firewall and cache function can be installed alone, independently of each other or integrated on the same server.

## ISA Features

The Firewall functionality of ISA includes the following:

[7] Shinder, pg xxxvi.
[8] Microsoft, pg 1.

- Network Address Translation (NAT and SecureNAT) services
- Stateful packet filter inspection
- Circuit layer session inspection and control
- Application layer filtering
    - Email content screening, anti-virus plugins, URL content filtering
    - Detects well known attacks on open ports such as DNS, POP3, HTTP and SMTP
- Support for HTTP, FTP, IRC, H.323, streaming media filters
    - Allows additional custom defined protocols
- Advanced authentication using Windows Basic, NTLM, Kerberos and digital certifications
- Integrated VPN
    - Supports PPTP and L2TP/IPSec tunneling
    - Encrypted site-to-site connections and user VPN connections
- System hardening scripts
- Integrated Intrusion Detection
- Email content screening
- Inspects SSL encrypted traffic
- Configurable report and alerts
- Logging
- Secure server publishing
- Transparent to users

The ISA Web cache proxy server includes the following features:

- High performance web cache
- Transparent caching to user
- Standalone, or distributed and hierarchical caching arrays
- Active Caching analyzes web traffic patterns to maintain active content for frequently accessed web pages
- Scheduled content download to pre-fetch specified URL content during off hours
- Streaming media support
- Reverse proxy secure publishing of internal web servers

Policy-based access control is used to control access based on strong authentication of users and groups.  Users and groups can be local to the ISA server or can be part of Active Directory, depending on the type of installation. Policy-based access control can be based on Client Address Sets (IP), Destination Sets (defined by URL, IP address or local path), Protocols, Content Groups for HTTP and tunneled FTP, Schedule based, and bandwidth priorities using QOS.

Administration is simplified by use of the Microsoft Management Console (MMC) giving the administrator a familiar graphical user interface for all management tasks.  Taskpad views can be created and permissions delegated to allow a granular delegation of administrative tasks. A Software Development Kit allows customized tasks and scripting to further extend the flexibility of ISA administration.

## ISA Versions

ISA 2000 Server is available in two versions, Standard Edition and Enterprise Edition. Standard edition is appropriate for small environments where ISA's full featured firewall, whether combined with the Proxy server or not, provides a fully effective perimeter defense. It is installed as a standalone version, and does not require domain membership. It uses local policies only, and is limited in scalability, as it can not be a member of a distributed caching array. It does however support hierarchical caching. Standard edition supports up to four processors.

ISA Enterprise edition provides scalability with its ability to join arrays, which allows centralized administration and integration with Active Directory. Enterprise policies are stored and administrated in Active Directory, with the option to add local policies on each server that extend the enterprise array policy. Enterprise edition supports distributed caching arrays, and supports up to eight processors when running on the appropriate version of the operating system for multiple processor support.

A summary of characteristics of each version:

| Standard Edition | Enterprise Edition |
|---|---|
| Standalone only | Single or Multiserver array with centralized management |
| Local policies only | Enterprise and Array policies |
| Supports up to 4 CPUs | Unlimited support of CPUs |

## ISA Installation Types

ISA installations are either installed as a standalone installation or a member of an array. A summary of characteristics of each installation type:

| Standalone | Array Member |
|---|---|
| Does not require Active Directory | Must be a member of an Active Directory domain |
| Can be installed in a Windows NT 4.0 domain (running on Windows 2000 server or greater) | Can only be installed in an Active Directory domain |
| Local policies only | Enterprise and Array policies |
| Standard or Enterprise edition | Enterprise edition only |

An advantage of arrays is the ability to manage the entire array as one entity. ISA can integrate with Active Directory for simplified management, policy replication and user level pass-through authentication and control. The policy is stored and replicated in Active Directory, providing fault tolerance, load balancing and scalability. A single server can represent an array; however, by adding additional ISA servers as members of an array, load balancing, redundancy and fault tolerance can be scaled as required. In the Enterprise Array mode, multiple ISA servers can be configured and administered using domain replicated Array policies. Further customization is available when the Enterprise policy allows local policies in addition to Array policies.

## ISA Modes

ISA can be installed in several modes, specifically in Firewall Mode, Cache Mode, or integrated, which includes both Firewall and Cache mode. A summary of characteristics of each installation mode:

| **Feature** | **Firewall** | **Cache** | **Integrated** |
|---|---|---|---|
| Server publishing | Yes | No | Yes |
| Web publishing | No | Yes | Yes |
| VPN | Yes | No | Yes |
| Packet Filtering | Yes | No | Yes |
| Application Filtering | Yes | No | Yes |
| Access Policy | Yes | HTTP only | Yes |
| Real time monitoring and alerts | Yes | Yes | Yes |
| Reporting | Yes | Yes | Yes |

## ISA Client Types

ISA supports several types of clients, depending on the client needs. A brief description of the client types follows:

- **Firewall Client** requires an agent to be installed and enabled on the client computer. It is supported by all
- **SecureNAT Client** is a computer configured to use the ISA server as its default gateway. This does not require any software installation on the client
- **Web Proxy Client** is a computer whose browser is configured to use the ISA server as a Web Proxy server. This does not require any software installation on the client

A computer may be either a Firewall Client or a SecureNAT client, but not both. Any computer can be a Web Proxy Client, including Firewall and SecureNAT clients. A comparison of features and requirements of each client type:

| **Feature** | **SecureNAT** | **Firewall** | **Web Proxy** |
|---|---|---|---|
| Installation required? | No* | Yes | No** |

| | | | |
|---|---|---|---|
| Operating system support | Any OS with TCP/IP support | Any Windows OS | All platforms |
| Protocol Support | Requires application layer filter for multi-connection protocols | All Winsock applications | HTTP, HTTPS, FTP, Gopher |
| User-level authentication | No | Yes | Yes |
| Server applications | No config required | Requires configuration file | N/A |

* Configure computer to use ISA server as default gateway

** Configure Web Browser to use ISA server as Web Proxy server

## ISA Dependencies and Requirements

ISA Server 2000 runs on either Microsoft Windows Server 2000 or Windows 2003 Server. ISA will run on the Standard edition, however if Network Load Balancing is used ISA must be installed on a version of the OS supporting NLB such as Windows 2000 Advanced Edition or Windows Server 2003 Standard Edition. Note that Windows Server 2003 supports NLB on multiple interfaces which is an advantage for ISA to provide load balancing on both internal and external interfaces.

ISA server must have at least two network connections. The LAN connection will be a Network Interface Card (NIC), but the external connection could be a permanent connection to the internet or it could be a dial on demand interface such as ISDN.

## ISA Scalability and Performance

ISA Server 2000 supports:

- Enterprise Arrays (Enterprise edition only)
- SMP support for multiple processors
- Network Load Balancing
  - Limited to one interface (internal or external) on Windows 2000
  - NLB configurable on both multiple interfaces on Windows Server 2003
- Distributed and hierarchical chained arrays
- Caching Array Routing Protocol (CARP) is a hash based routing protocol which eliminates duplication of cache content on multiple servers with a caching array

ISA's throughput performance has been tested and documented by Microsoft in a White Paper titled Microsoft Internet Security and Acceleration Server 2000

Performance. Based on independent testing by Network Computing Magazine, ISA Server achieved a throughput of 1.5 GB/s for downstream HTTP traffic.

In the Network Computing Magazine benchmark test, Microsoft ISA Server 2000 won in the performance category. ISA Server also scored the best application level filtering throughput (170Mbps), above the rest of the participants, outperforming the nearest competitor by 39%. In the maximum concurrent connections test ISA Server achieved 10,000 concurrent connections. Test information is available at http://www.networkcomputing.com/1405/1405f3.html.

### *Acme's Implementation of ISA Server 2000*

As part of Acme's Defense in Depth perimeter security system, Acme will install ISA Server 2000 in a back-to-back configuration behind the broadband internet facing border router. The border router is running a Firewall IOS, and will be configured to use stateful packet filtering and access control lists. The second layer of that system, ISA Server 2000, will be installed as described below. When the ISA server configuration or option specifically addresses one or more of the corporate directives Acme must comply with, that configuration will be noted. Those choices and options follow.

- Acme will install ISA Server 2000 Enterprise Edition running on Windows Server 2003 Standard Edition. Corporate guidelines will be used to harden the standard server build.
    - ISA will be installed on an Active Directory domain member server to allow for integration with AD users, groups and policies. The integration with AD will give administrators a centralized, consistent management interface, and provide more granular control.
- ISA will be installed as an Enterprise Array member, joining the Corporate ISA Enterprise Array for centralized administration of Enterprise policies. .
    - Before ISA could be installed as an Enterprise array, the AD schema was extended as part of the original installation at corporate. The schema extension is replicated so that it need only be done once.
    - The Enterprise policy was configured to allow array-level policies to be used by local administrators. Array-level policies can only further restrict the Enterprise policy, not loosen it. The Enterprise policy was also configured to allow publishing rules.
    - By default, ISA server will not allow any traffic to pass; all ports and protocols are denied. The Enterprise policy was configured to allow any HTTP and FTP traffic initiated from within the network. No restrictions were put on users, groups, destinations or hours of access. These restrictions will be determined at the array policy level. Acme configured the array level policy to restrict HTTP traffic based on the URL content filtering, and created a rule to prevent FTP traffic except by specific group membership.

- ISA will be installed in the Integrated Mode; the server will be configured both as a firewall and a proxy server. This will meet the requirement to "Provide secure connection to the Internet".
    - ISA Firewall will be configured as follows:
        - ISA will be configured to provide SecureNAT, an extension of Windows Network Address Translation (NAT). The internet facing network connection for ISA will use an internet routable public IP address. The internal network facing network connection will be configured with a private IP address on the internal corporate network. All address translation for services requested by internal clients for internet based services will be transparently translated by the ISA server.
        - ISA will be configured to use packet filters. Packet filters will be configured for L2TP and PPTP, DHCP, DNS and ICMP traffic.
        - ISA will be configured to enable Intrusion Detection for the following attacks: Windows out-of-band (WinNuke), Land, Ping of Death, IP half scan, UDP bomb, and port scans.
    - ISA Proxy server will configured as follows:
        - Enable HTTP and FTP caching
        - Enable Active Caching to automatically retrieve expired content from frequently accessed web pages
        - Enable Scheduled Content Download to configure download of web content during off hours for certain URLs accessed by users
        - Configure Automatic Proxy discovery to have ISA publish a browser configuration script and publish a WPAD DNS entry for access the configuration script
- ISA will be configured as a site-to-site VPN server connecting to a VPN server at the home office. This connection will use L2TP/IPSec for tunneling and encryption, and will be "nailed up", or always available without having to be initiated by a client. This connection will carry Active Directory replication traffic, SMTP mail traffic, and RPC traffic. This will meet the requirement to "Provide secure connections between the branch and home office".
- ISA will be configured as a VPN server for remote users. VPN traffic will be accepted using either L2TP/IPSec when available or PPTP for down-level client compatibility. This will allow remote users to authenticate to the corporate network across the Internet using a native Microsoft client. This authentication will be integrated into Active Directory and using the Windows account and password, gives users the same access to network resources as if they were logged on locally. This will meet the requirement to "Provide secure connections for telecommuters and remote users".

- ISA will be configured for logging, monitoring and alerting. This will meet the requirement to "Monitor and enforce compliance with corporate guidelines for internet usage" as well as a component of the overall security strategy.
  - Logging will be configured for Packet Filters, Firewall service and Web Proxy service, and will write to an ODBC database for consolidation and analysis. These logs are truncated daily.
  - Alerting will be configured. ISA has 45 different alerts with the ability to create custom alerts. Each alert can be configured to log events to Event Viewer, send an email and/or page to network personnel as may be appropriate.
  - Reporting will be configured to generate web based daily, weekly and monthly summary reports of Web Usage, Application Usage, Traffic & Utilization and Security events. These reports will be published on an intranet server with controlled access.
- ISA will use a 3rd party URL content filtering plugin from SurfControl. This application extension plugin integrates the subscription based URL database which is broken down by categories to allow Acme to use the ISA Server MMC to configure and administrator URL content filter rules. A list of inappropriate sites and categories will be used to block access for all users. For instances where access to those URLs is needed for testing, etc, a security group will be created in Active Directory to allow specific access to normally prohibited URL for users placed in those groups. This will assist in meeting the requirement to "Monitor and enforce compliance with corporate policies for internet usage". Information about the SurfControl plugin for ISA server is available at http://www.surfcontrol.com/products/web/ms_isa/
- Acme will configure their Exchange email server to allow access to email using Secure Socket Layer (SSL) protocol over port 443. ISA will be configured to securely publish that service to the Internet, allowing users to access their email using any Internet browser when a VPN connection is not available. This will meet the requirement to "Provide email access for remote users". More information about publishing OWA through ISA server is available at http://www.isaserver.org/tutorials/pubowa2003toc.html
- ISA will use an anti-virus application layer plugin for scanning all HTTP and FTP traffic. More information about available plugins is available at http://www.isaserver.org/software/ISA/Anti_Virus/
- Acme has created a web interface for claims adjusters to enter data and process claims. To allow access to this web interface from outside the corporate network, the web server will be published through ISA server using HTTPS and SSL. This will allow claims adjusters to access and enter data from any internet browser when a VPN connection is not feasible. This will meet the requirement to "Provide secure access to claims entry for field adjusters".

- NAT Client configuration is very simple. The ISA server was placed as the last IP gateway before the Internet, so all default gateways point to or lead to the ISA server. This forces all internet bound traffic to pass through the ISA server, and rules and filters are automatically applied.
- Web Proxy client configuration is accomplished by publishing automatic browser configuration scripts as previously described. The web browser client is by default configured to “Automatically detect settings”. This will utilize the DHCP record for WPAD (Windows Proxy Automatic Discovery) and point the client browser to the published automated configuration script.

## References

Northcutt, Stephen. Inside Network Perimeter Security. First edition. New Riders Publishing. July, 2003.

SANS Institute. “The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus”. Version 4.0. October 8, 2003. URL: http://www.sans.org/top20/

SANS Institute. “About the SANS Institute”. Date unknown. URL: http://www.sans.org/aboutsans.php

Cole, Eric. “How to Secure your Company.” June 26, 2003. Computerworld, an IDG Company. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,82515,00.html

National Institute of Standards and Technology (NIST), SP 800-10 “Keeping your Site Comfortably Secure: An Introduction to Internet Firewalls”. December 1994. URL: http://csrc.nist.gov/publications/nistpubs/800-10/node31.html#SECTION00510000000000000000

National Security Agency (NSA). “Defense in Depth; A practical strategy for achieving Information Assurance in today’s highly networked environments.” URL: http://nsa2.www.conxion.com/support/guides/sd-1.pdf

Shinder, Dr. Thomas W. Configuring ISA Server 2000: Building Firewalls for Windows 2000. Syngress Publishing, Inc. 2001.

Microsoft Corporation. “ISA Server 2000 Achieves Common Criteria Certification”. September 17, 2003. Microsoft Corporation. URL: http://www.microsoft.com/isaserver/techinfo/deployment/commoncrit.asp.

ICSA Labs. Welcome to ICSA Labs’ Firewall Community: Certification Program. Date unknown. URL: http://www.icsalabs.com/html/communities/firewalls/index.shtml.

Microsoft Corporation. MCSE Microsoft Internet Security and Acceleration Server 2000 Training Kit. Microsoft Press. 2001

Microsoft Corporation. “Microsoft Internet Security and Acceleration Server 2000 Overview.” Version 1.1. March 2002. URL: http://www.microsoft.com/isaserver/evaluation/productguide_v1.1.doc

Gannett Co. Inc. USA Today. “USA Today Snapshots.” October 14, 2003.

Microsoft Corporation.  Internet Security and Acceleration Server 2000 Performance.  Version 1.5.  October 13, 2003.  Microsoft Corporation.  URL: http://download.microsoft.com/download/f/2/f/f2fccc11-82ea-4fe6-9f7f-013d654f3e86/Firewall%20Performance%20Test.doc

Network Computing Magazine.  CMP Media LLC.  Security: Application-Level Firewalls: Smaller Net, Tighter Filter.  March 21, 2003.  URL: http://www.networkcomputing.com/1405/1405f3.html

http://www.microsoft.com/ISAServer/

http://www.isaserver.org/

http://isatools.org/