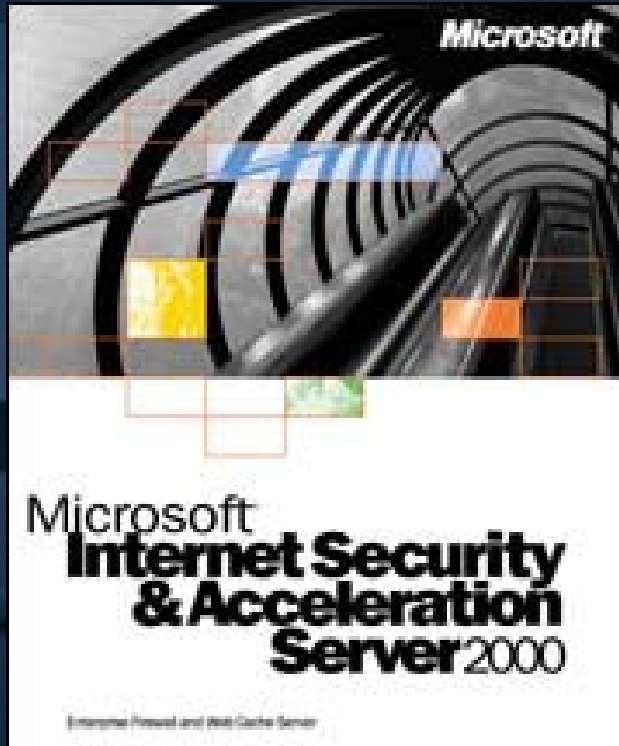


# Microsoft Internet Security and Acceleration Server 2000

## *Concepts and Functional Use*



Jim Harrison

Tom Shinder



# Agenda

- Introduction - Agenda
- Deployment scenarios
  - Enterprise Arrays
  - Standalone
- ISA clients
  - SecureNAT
  - Firewall
  - Web proxy
- Web / Server Publishing
- Troubleshooting techniques
  - Reading the logs (and understanding them)
  - Interpreting the Event log entries



# Deployment Scenarios

**Enterprise  
Arrays**

**Secure internetworking with a  
scalable, multi-layer firewall**

**Standalone**

**Fast access with a scalable, high  
performance Web cache**



# Enterprise Array

- **Centralized Domain Policy**
- **All Members in Same Active Directory Site**
- **Active Directory Required**
- **Multiple Policies**
- **“Array Level” control allowed**
- **Distributed Caching**
- **ISA Enterprise Version ONLY**
- **ISA Server Objects Added to Active Directory**

# Standalone ISA Server

- Does not support Enterprise Arrays
- Active Directory not required
- Member of AD or NT domain
- No Distributed Caching
- Hierarchical Caching Available
- Easiest to configure and manage
- Suitable for small and medium biz
- Beef up the hardware



# ISA Server Clients

- **Web proxy**
  - CERN-compatible proxy server
  - HTTP, HTTPS, FTP, Gopher protocols only
  - OS-independent
- **SecureNAT**
  - Uses ISA as a router
  - Simple protocols only
  - OS-independent
- **Firewall**
  - Winsock proxy (supports Proxy 2 client)
  - Complex protocols
  - Windows 9x and later



# Client support

- **Built-in DNS cache for Web & Firewall clients**
  - Eases DNS requirements in simple deployments
  - Can be disabled via registry if desired
- **Force web proxy for SecureNAT & Firewall clients via HTTP Redirector**
  - Can help enforce authenticated access policies
- **User Authentication for Web & Firewall clients**
  - Provides for user / group access policies
  - Basic, Integrated and W2K AD Digest authentication is supported
- **Outbound PPTP for SecureNAT clients**

# Client Access Policy

- Site and Content Rules
- Protocol Rules
- IP Packet Filters

Internet Security and Acceleration Server

File Action View Help

Internet Security and Acceleration Server

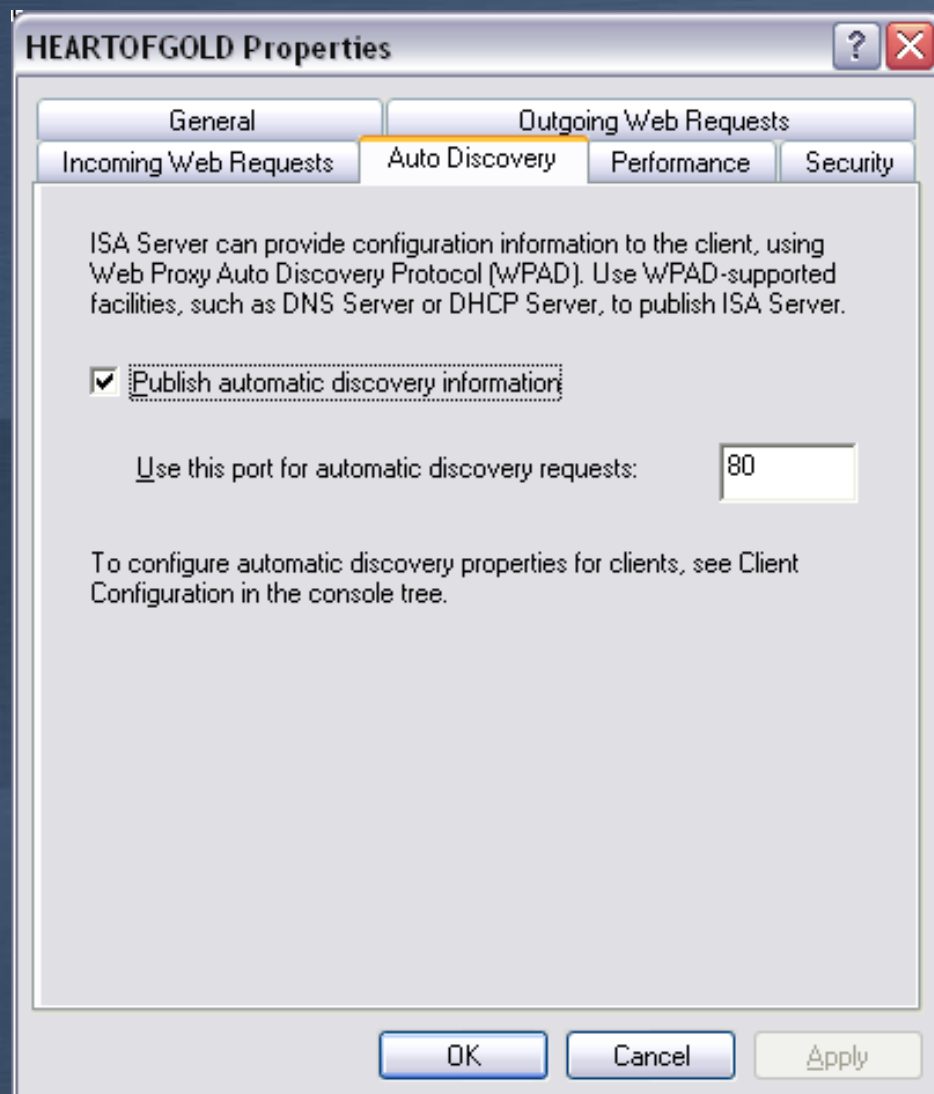
- Servers and Arrays
  - HEARTOFGOLD
    - Monitoring
    - Computer
    - Access Policy
      - Site and Content Rules
      - Protocol Rules
      - IP Packet Filters
    - Publishing
    - Bandwidth Rules
    - Policy Elements
    - Cache Configuration
    - Monitoring Configuration
    - Extensions
    - Network Configuration
    - Client Configuration
  - H.323 Gatekeepers

Name	Scope	Action	Protocol	Applies To	Schedule
Camera	Array	Allow	Camera	Any request	Always
DNS Q	Array	Allow	DNS Query	Any request	Always
DNS ZT	Array	Allow	DNS Zone Transfer	Any request	Always
Finger	Array	Allow	Finger	Any request	Always
FTP	Array	Allow	FTP	Any request	Always
HTTP	Array	Allow	HTTP	Any request	Always
ICQ	Array	Allow	ICQ 2000	Any request	Always
KCLS WebPac	Array	Allow	KCLS WebPac	Any request	Always
MS-Games	Array	Allow	IRC,MS-Games	Any request	Always
MSN Msgr	Array	Allow	MSN Msgr (Real),Net2Phone	Any request	Always
Netmeeting	Array	Allow	H.323 Protocol	Any request	Always
NEWS	Array	Allow	NNTP	Any request	Always
NTP	Array	Allow	NTP (UDP)	Any request	Always
POP	Array	Allow	POP3	Any request	Always
RDP	Array	Allow	RDP (Terminal Services),RDP-3390	Any request	Always
SMTP	Array	Allow	SMTP	Any request	Always
SSL	Array	Allow	HTTPS	Any request	Always
Streaming Media	Array	Allow	MMS - Windows Media,PNM - RealNetworks protocol (Client),RTSP	Any request	Always
TELNET	Array	Allow	Telnet	Any request	Always
WhoIs	Array	Allow	WhoIs	Any request	Always

# WPAD Configuration

- Auto Discovery listener

This is the heart and soul of WPAD and WSPAD functionality



# Outgoing Web Requests

## ■ Outgoing Web Requests

In order for ISA to function as a Web proxy, the Outbound Web Requests Listener has to be properly configured.

The screenshot shows the 'HEARTOFGOLD Properties' dialog box with the 'Outgoing Web Requests' tab selected. The 'Identification' section has two radio buttons: 'Use the same listener configuration for all internal IP addresses' (selected) and 'Configure listeners individually per IP address'. Below this is a table with columns: Server, IP Address, Display N..., Authentic..., and Server C... The table contains one entry: HEARTOFGOLD, <All internal IP addresses>, and Integrated. There are 'Add...', 'Remove', and 'Edit...' buttons below the table. The 'ICP port' is set to 8080 and the 'SSL port' is set to 8443. There is a checkbox for 'Enable SSL listeners' which is unchecked. The 'Connections' section has a 'Configure...' button and a checkbox for 'Ask unauthenticated users for identification' which is unchecked. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Server	IP Address	Display N...	Authentic...	Server C...
HEARTOFGOLD	<All internal IP addresses>		Integrated	

# HTTP Redirector

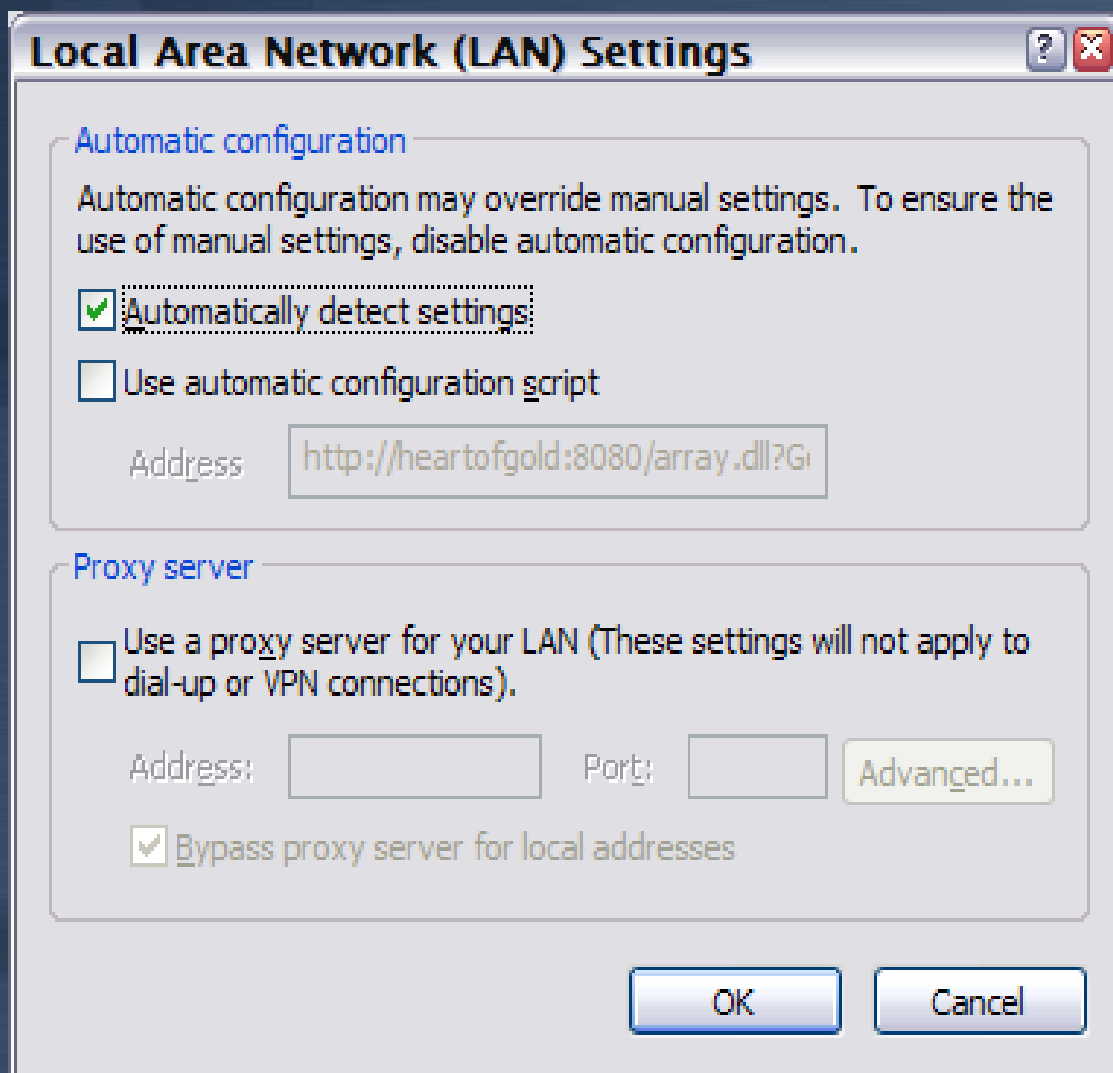
- Controls firewall and SecureNAT client web access



# Web Proxy Clients

- Application or browser proxy settings use <ISAServer>:8080
- All ISA operating modes
- Non-MS clients if CERN-proxy compliant
- ISA Auto-detect supports IE5 and later only
- Protocols
  - HTTP, HTTPS, FTP (download), Gopher
- No secondary protocols
- Basic, Integrated, Digest Authentication
- DNS C.O.D.

# Browser configuration for WPAD



The image shows a Windows dialog box titled "Local Area Network (LAN) Settings". It has a standard Windows window title bar with a question mark icon and a close button. The dialog is divided into two sections: "Automatic configuration" and "Proxy server".

**Automatic configuration**

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

- Automatically detect settings:
- Use automatic configuration script

Address:

**Proxy server**

- Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address:  Port:

- Bypass proxy server for local addresses

At the bottom of the dialog are two buttons: "OK" and "Cancel".

# RAS browser settings

The image shows a Windows dialog box titled "MS Settings" with a question mark and close button in the top right corner. The dialog is divided into three sections: "Automatic configuration", "Proxy server", and "Dial-up settings".

**Automatic configuration**  
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

- Automatically detect settings
- Use automatic configuration script

Address:

**Proxy server**

- Use a proxy server for this connection (These settings will not apply to other connections).

Address:  Port:

- Bypass proxy server for local addresses

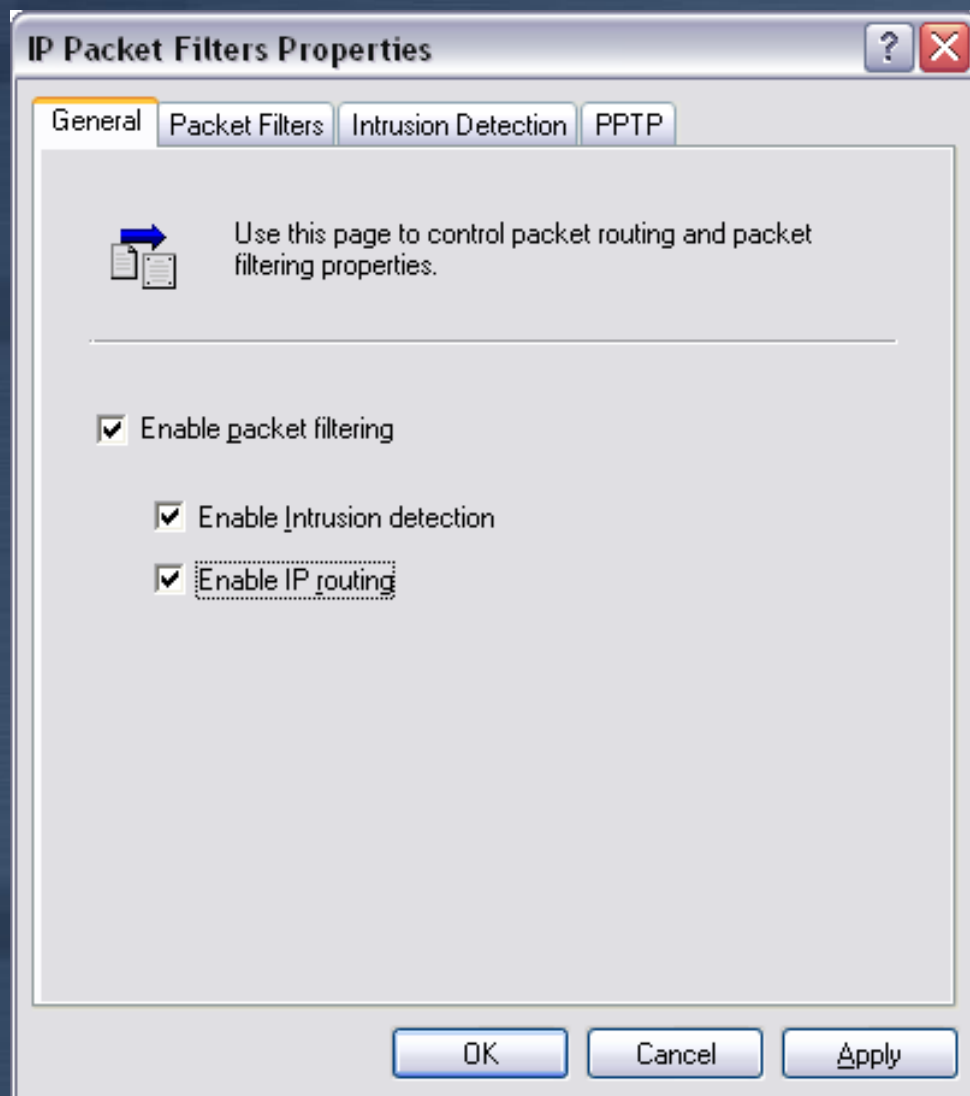
**Dial-up settings**

User name:

Password:

Domain:

# ISA Configuration for SecureNAT Clients





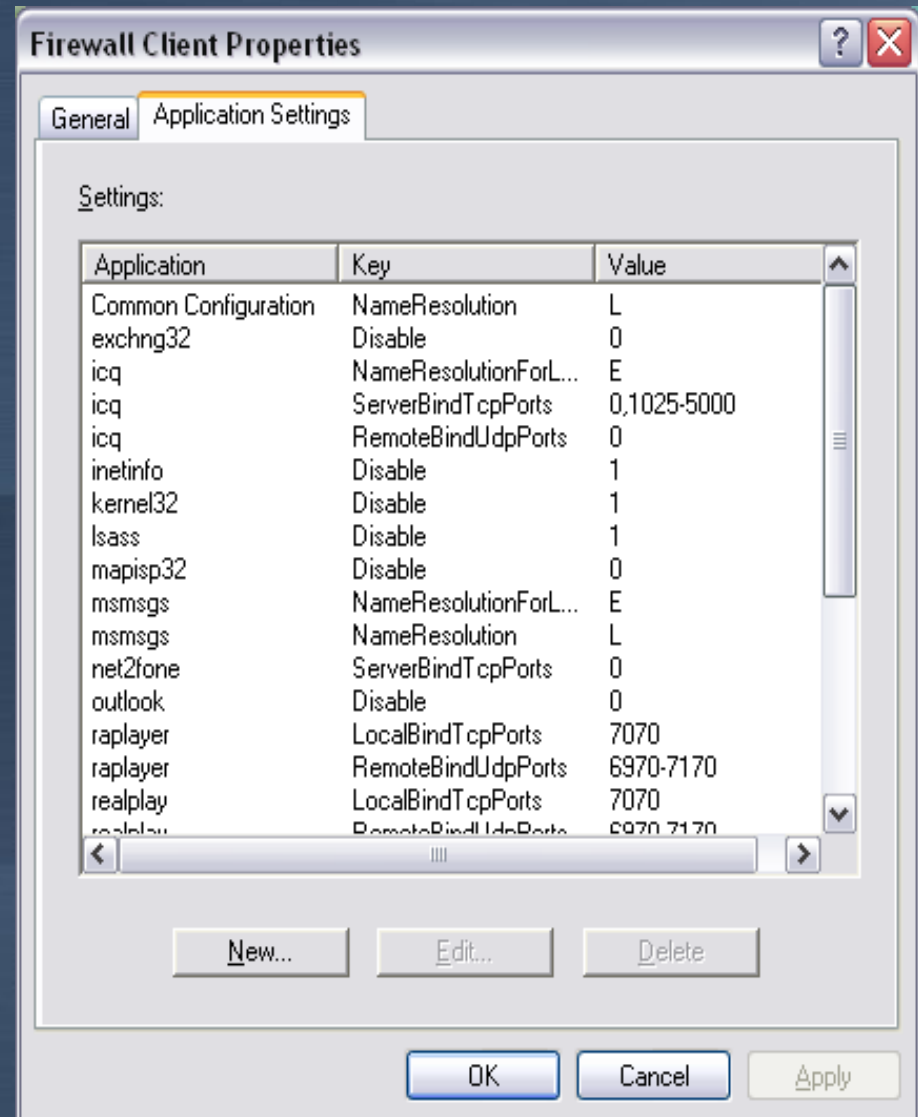
# SecureNat Clients

- Host computer uses ISA as its default route
- Only Firewall and Integrated modes
- Non-MS clients
- No ISA Auto-detect capabilities
- Can use any simple protocol that is defined and allowed
- No user Authentication
- Requires separate DNS structure

# ISA Configuration for Firewall Clients

## ■ Application Settings

ISA Firewall client functionality can be configured on a per-application, per-host basis for very granular control over client functionality





# Firewall Clients

- ISA or Proxy 2 client software is installed on the LAT host
- Firewall and Integrated modes only
- Non-MS clients are not supported
- Auto-detect works for ISA and Proxy 2
- Protocols; any defined and allowed
- Allows secondary protocols
- Client Authentication uses interactive logon credentials
- DNS C.O.D.



# Web and Server publishing

- Web Publishing
- Server Publishing
- Packet Filtering



# Web Publishing

- **Single IP Address for Multiple Sites**
- **Access Control at Listener**
- **Examines HTTP Header**
- **Port Redirection**
- **SSL Bridging of HTTP requests**
- **HTTP Bridging of SSL requests**
- **Caching of inbound requests**
- **Plug in Support**



# Server Publishing

- Publish All Services
- Access Control – Client Address Sets
- No Port Redirection
- Can use Application Filters
- One IP Address per Service
- Watch out for contention!



# Packet Filtering

- **Not true Server Publishing**
- **Used for DMZ Servers**
- **Direct Access to Servers**
- **Very Limited Access Control**
- **Not Recommend for Services on ISA Server**
- **Primarily for outbound access to non-TCP/UDP Protocols**



# Troubleshooting

- Use the isainfo script
- Log analysis
- W2K troubleshooting techniques
- Network troubleshooting techniques



# ISA Logs

## ■ IP Logs

- All traffic that is refused by the mspfltex service (can log “allowed” as well)

## ■ WEB Logs

- All the traffic that is handled by the w3proxy service

## ■ FW Logs

- All the traffic that is handled by the fwsrv service

## ■ Log Configuration Option

- W3C format
- ISA format



# Packet Filter Logs

- All traffic that was refused (ignored) by the Packet Filtering Service (mispftex)
- Can log “allowed” traffic, but makes for huge log files



# WEB Proxy logs

- All traffic that was either allowed or denied by the Web Proxy Service
- Client credentials depend on settings in the Incoming and Outgoing web requests listeners
- Also contains cache hit data



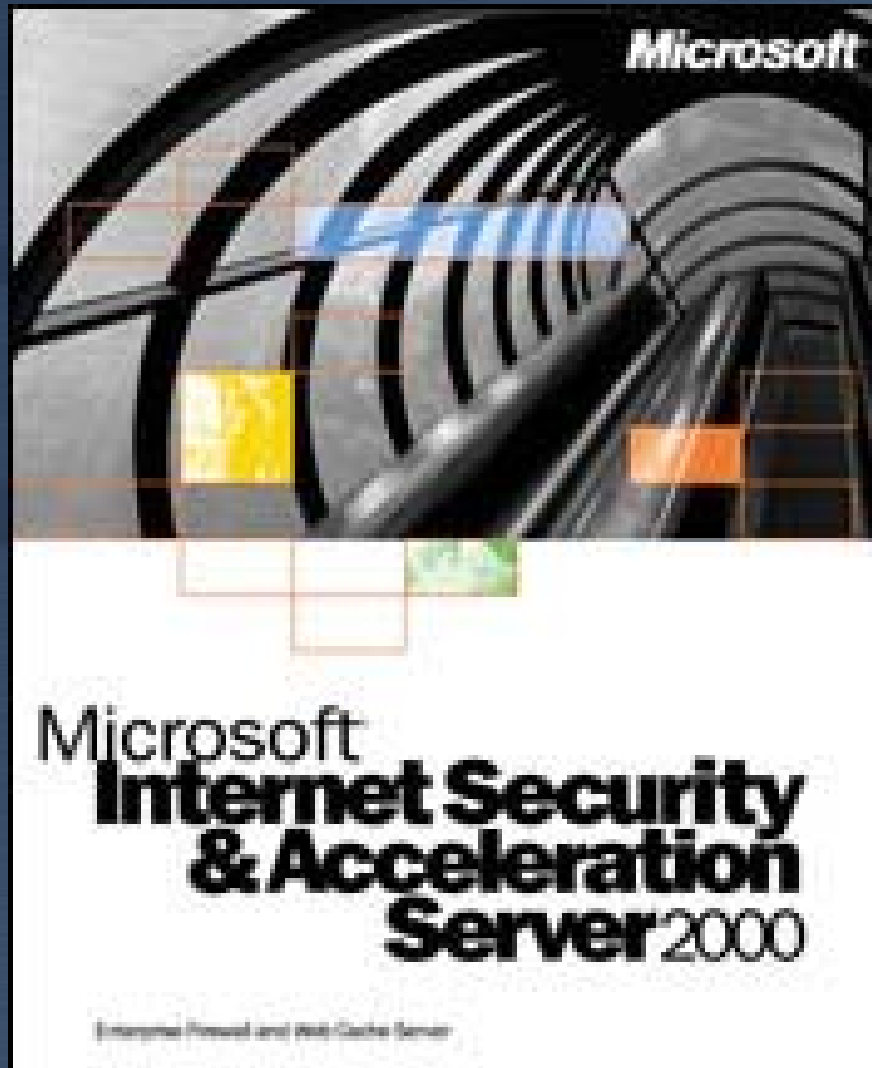
# Firewall Service logs

- All traffic that was allowed or denied by the Firewall service.
- Useful for determining what protocols / ports are being used by an app



# Event Logs

- **Application Event logs**
  - All ISA services log here
- **Security Event Logs**
  - Depends on your Auditing
- **System Event Logs**
  - Can also assist with issue resolution



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

<http://www.isaserver.org>