Agenda

- Introduction to ISA Server 2006
- Secure Application Publishing
- Branch Office Protection
- Firewall and Proxy Enhancements
- Monitoring ISA with MOM
ISA Server 2006

- **Application Layer Firewall**
  - Protects internal resource from the outside
  - Separate from the rest of the network
  - Control how Internet resources are used
  - Examines each network packet against your rules

- **VPN**

- **Proxy Server**
  - Makes network requests and forwards data
  - Caches sites for improved performance
ISA Server 2006 Editions

ISA Server 2006 Standard Edition

ISA Server 2006 Enterprise Edition
Appliances

- Preinstalled on optimized hardware
- Partner solutions extends ISA
  - Antivirus gateways, URL filtering, availability
- Both for Standard and Enterprise Edition
  - Enterprise get extended NLB and caching functionalities
- Support for unattended installation using a USB flash drive
Appliances - Benefits

- Easy deployment
- Everything is tested
- Hardened configuration -> Reduced attack surface
- Extra configuration tools and web administration
Advantages of Appliances

- Easier purchase process – no separate software licensing complexity
- Lower cost of deployment
- Plug & Play, Set & Forget
  - Controlled components and drivers
  - Automated patch management (on some offerings)
- Fewer calls to tech support
- Easy roll-back to factory configuration
- Quick learning curve for IT administrators
- Appliances are the whole solution, not just part
A Traditional Firewall’s View of a Packet

- Only packet headers are inspected
- Application layer content appears as “black box”

- Forwarding decisions based on port numbers
- Legitimate traffic and application layer attacks use identical ports

<table>
<thead>
<tr>
<th>IP Header:</th>
<th>TCP Header:</th>
<th>Application Layer Content:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address, Dest. Address, TTL, Checksum</td>
<td>Sequence Number Source Port, Destination Port, Checksum</td>
<td>???????????????????????????????</td>
</tr>
</tbody>
</table>

- Internet
- Corporate Network

- Expected HTTP Traffic
- Unexpected HTTP Traffic
- Attacks
- Non-HTTP Traffic
ISA Server’s View of a Packet

Packet headers and application content are inspected

- IP Header: Source Address, Dest. Address, TTL, Checksum
- TCP Header: Sequence Number, Source Port, Destination Port, Checksum
- Application Layer Content: 
  ```html
  <html><head><meta http-equiv="content-type" content="text/html; charset=UTF-8"><title>MSNBC - MSNBC Front Page</title><link rel="stylesheet"
</html>
```

- Forwarding decisions based on content
  - Only legitimate and allowed traffic is processed

Internet ↔ Allowed HTTP Traffic ↔ Corporate Network

- Prohibited HTTP Traffic
- Attacks
- Non-HTTP Traffic
Multi-Network Support

- Simplify complexity and administration of managing network security
  - Subdivide network into multiple segments with a single ISA license
  - Extend virtual firewall protection across each segment

- Enforce rules on per network basis

- Easy setup
  - Network templates
ISA 2004/2006 Policy Model

- Single, ordered rule base
- Logical and easier to understand
- Easy to view and to audit
- Default System Policy
Default System Policy/Lockdown

- System Policy – a default set of access rules applied to the ISA Server itself
- Lockdown mode:
  - Protects the operating system when firewall services are offline because...
    - Security event triggers firewall service shut down
    - Planned firewall service shut down
    - ISA Server reboot
Exploring some basic tasks
Application Publishing

- Use internal resources from the Internet
- Outlook Web Access
- Publish through one external IP address
- Cached content to external client
- Supports IIS authentication methods
- Pre-authenticate users
- Path configuration
OWA Publishing

ISA Server is the host

- ISA terminates all connections
- Decrypts HTTPS
- Inspects content
- Inspects URL against rules
- Re-encrypts for delivery to OWA
What is Publishing?

- ISA Server impersonates internal servers through a reverse proxy process
  - To make internal sites/services accessible to users outside the corporate network, including partners
  - To add a layer of security at the network edge
The Solution

- Automatic translation of links to internal shares
- Strong user/group based access controls
- Load balancing of server farms
- Exchange & SharePoint publishing tools
- NTLM, Kerberos authentication support
- Smartcard & one-time password support
- Inspection of encrypted traffic using SSL Bridging
- Single sign-on for access to multiple servers
- Pre-authentication so only valid traffic reaches servers
- Remote User
- Hacker
- Internet link
- ISA 2006
- Exchange Farm
- Active Directory
- SharePoint Farm
- Internal Network
Branch Office Gateway

Key Differentiating Points

- Easy Integration with Existing Branch Office Infrastructure
- Integrated Application-Layer Firewall Provides Added Protection
- Integrated Cache Functionality Increases Speed
- Integrated S2S VPN Functionality Lowers TCO
- Centralized Management from HQ
Branch Office
Performance Improvements

- BITS caching for Microsoft update platform
  - Reduce the impact of software updates on network bandwidth in the branch office
  - Improve value of ISA 2006 by reducing days-of-risk in branch office locations

- Compression of HTTP content
  - Compress HTTP content before going over the WAN to accelerate Web browsing and improve bandwidth usage
  - Cache compressed and uncompressed content

- DiffServ (Differentiated Services) to prioritize HTTP and HTTPS application traffic
  - Improve response time for critical HTTP and HTTPS applications
  - Determine what traffic has priority over other traffic based on URL and corresponding configured DiffServ service level
Branch Office Gateway

ISA Server 2004/2006 Features

- Easy Deployment
- Better Protection
- Better Management
- Lower Connectivity Costs
- Bandwidth Optimization

Flexible Branch Office Network Topology
Integrated Firewall
Integrated S2S VPN Gateway
HTTP Caching
Distributed Caching & Web Proxy Chaining

BITS Caching Complements R2 Remote Differential Caching
Enterprise Policies

Enterprise policies:
- Multiple “template” policies for an organization
- Arrays are assigned Enterprise Policies

Effective policy:
- Calculated from Enterprise Policies and Array Policies
- Result: An ordered set of allow/deny rules
Enterprise Policy Structure

An enterprise policy consists of:

- Enterprise rules (before)
- Array policy “Place Holder”
- Enterprise rules (after)
Configuration Storage Server

ISA 2006 Server Array

Local configuration copy

Management Console

ISA 2006 Server Array

Local configuration copy

ISA 2006 Server Array

Local configuration copy

CSS

Replication

CSS
Balancing Outbound Access

- **ftp.microsoft.com**
  - IP: 157.31.56.100

- **Internet**
  - NLB Cluster

- **ISA-1 - External**
  - DIP: 128.1.1.2
  - VIP: 128.1.1.100

- **ISA-1 - Internal**
  - DIP: 10.10.10.1
  - VIP: 10.10.10.100

- **ISA-2 - Internal**
  - DIP: 10.10.10.2
  - VIP: 10.10.10.100

**Internal Client:** 12.12.12.1

© 2005 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.
Integrated security
Application filtering, BITS caching
Secure access
HTTP compression, traffic prioritization
Efficient management
Easy deployment, fast propagation of policies

ISA Server 2006
Integrated Security

- BITS caching, Background Intelligent Transfer Service
  - Transfers files between client and server
  - Uses leftover bandwidth
  - Maintains transfers if disconnected

- Windows Updates
  - Data is cached on the ISA Server
  - Subsequent users pull them from the local cache
Secure Access

- **HTTP compression**
  - When someone requests the response are compressed at the ISA server at the HQ
  - It reaches the branch and gets decompressed

- **Traffic Prioritizing**
  - Control when bandwidth is limited
  - Diffserv protocol
  - ISA inspects requests and assigns priority depending on destination
Effective Management

- Branch Office Connectivity Wizard
- Answer files for unattended installation
- More effective policy propagation
- Reduced server requirements
- Optimization for low bandwidth use
- Secure Remote Management is possible
- Templates and configuration tools
Configure the Branch Office Gateway
Proxy server features

- Enhanced worm resiliency, mitigate the impact on the network
- Faster alert triggers and responses
- To avoid DOS attacks ISA Server controls:
  - Log throttling measures the volume of denied records
  - Memory consumption
  - Pending DNS queries
The Solution

- Enhanced protection against DoS, DDoS & DNS attacks
- Integrated application-layer firewall & web proxy
- Integrated Network Load Balancing for high availability
- Enhanced protection against DoS, DDoS & DNS attacks
- Comprehensive alert triggers & responses
- Security-enhanced remote management using TLS
- Built-in traffic inspection for over 120 protocols
- Customizable cache rules for flexibility
- Fast RAM & on-disk caching for fast web page response times
- Enhanced worm protection through connection quotas

INTERNET WORK

Attacker

External Web Site

Internet

ISA Server 2006 Array

© 2005 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.
Flood Resiliency

Protect ISA Server from—
- Worm propagation
- Syn floods
- Denials of service
- Distributed DoS
- HTTP bombing

In some cases, computers behind ISA are also protected, but this isn’t the primary goal of the feature.
Web Access Protection
Key Differentiating Points

- Deep Content Inspects Actual Content of Traffic
- Multi-network Architecture Eases Infrastructure Integration
- Flexible SDK allows Easy Development of New Application Filters
- CARP Provides High Performance for Caching
- Easy-to-Use UI Makes Configuration Easier
Monitoring ISA Server 2006

- MOM Management pack
- Health indicators
- Knowledge from the designers
Monitoring and Alarming

Real-time Firewall Status

Alarming Mechanism
Summary

- Firewall, VPN, Proxy
- Application Publishing
- Branch Office
  - Caching
  - Compression
  - Prioritizing of traffic