

Locking down Exchange Server: Securing Exchange Server 2003

E-mail Security Webcast Series: Part 2 of 5

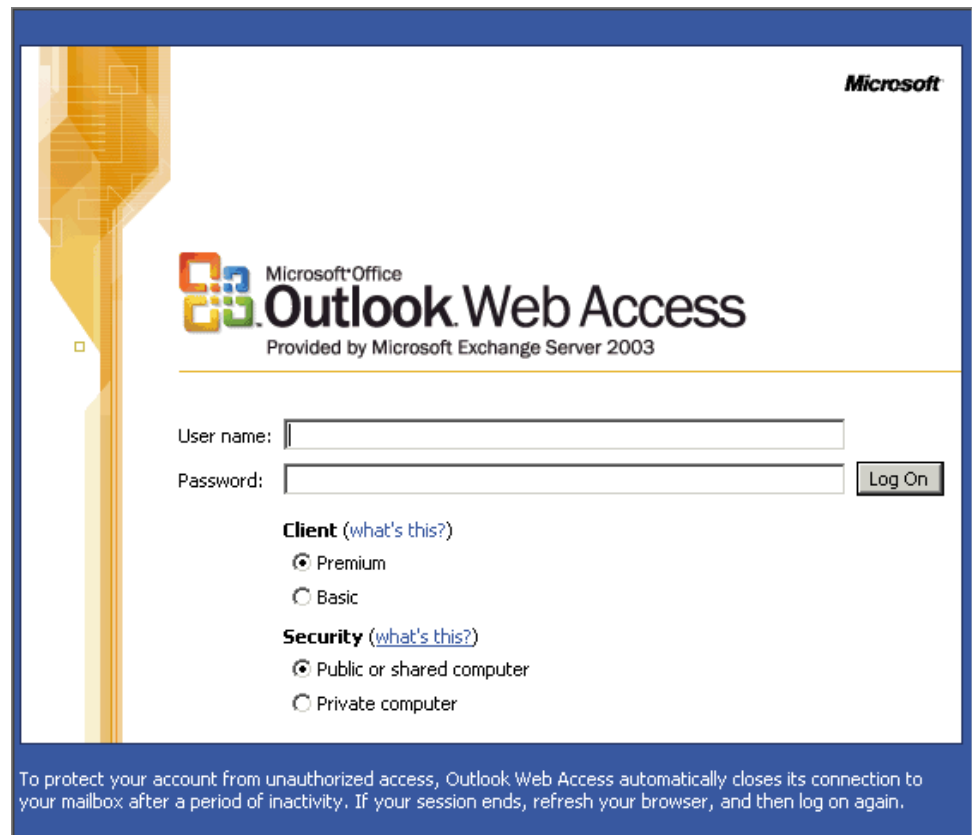
Speaker: Lee Benjamin



LeeB@ExchangeGuy.com

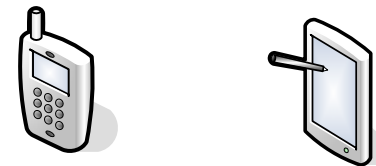
Secure OWA (Outlook Web Access)

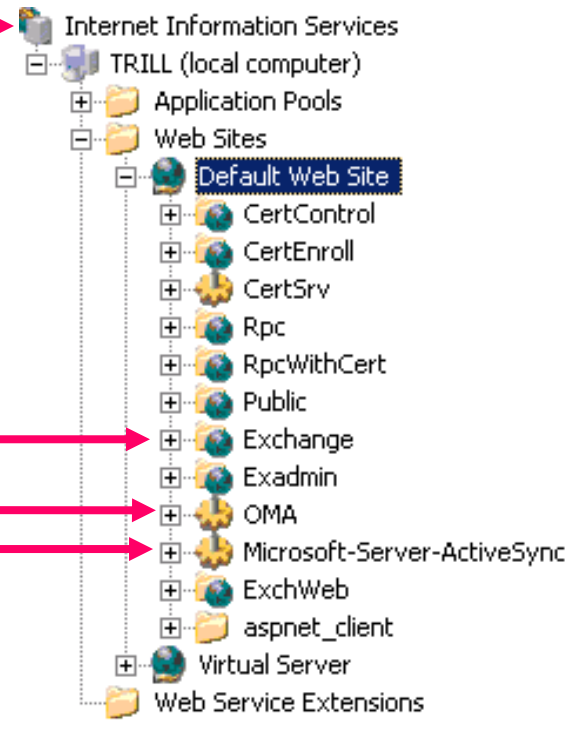
- **Add a Certificate and Use HTTPS://**
- **OWA Default Integrated Login**
- **Forms Based Authentication**
 - Kiosk
 - Roaming Users
 - Timed Logout
- **OWA Administration Tool**



Mobile Devices

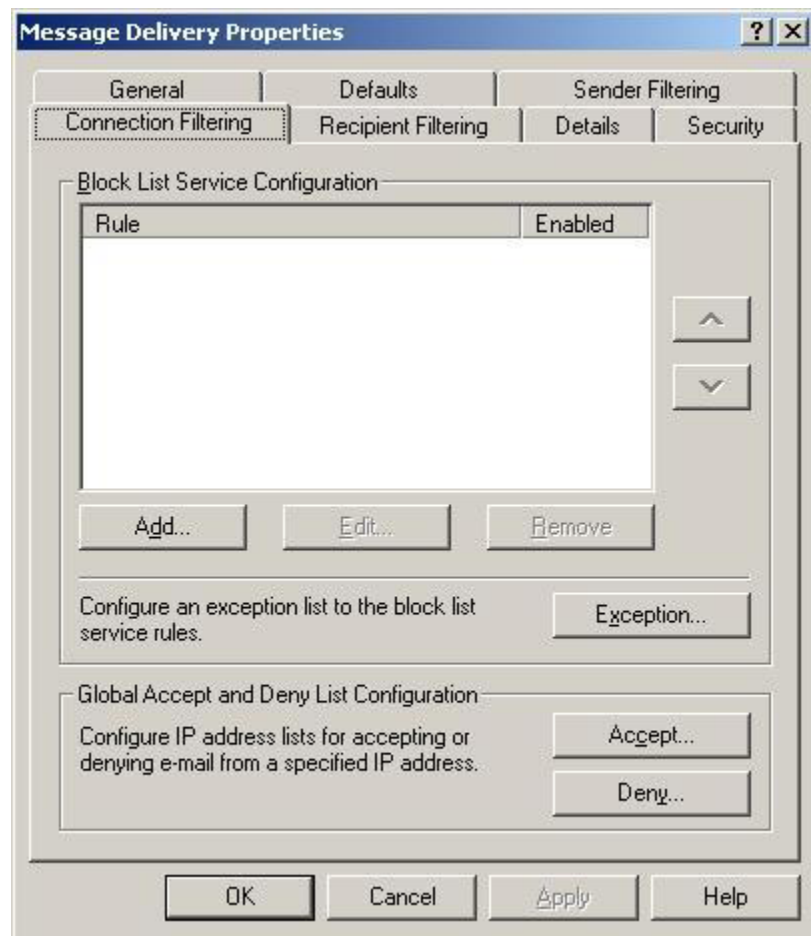
Same HTTPS Security as OWA!



- **Manage Security from Within IIS**
 - IIS Virtual Directory Like Outlook Web Access
 - Can Apply SSL in IIS and on Mobile Device
 - **Outlook Mobile Access (OMA)**
 - Plain HTTP, No Icons, No Frames, No Attachments
 - Cell Phones and Any Browser (enable unsupported devices)
 - **ExchangeActiveSync**
 - Synchronize PocketPC and SmartPhones
 - Over the Internet or Cellular Network, Also WiFi
 - Directly to the Exchange Server
 - Sync to Pocket Outlook
 - Pocket Inbox, Calendar, Contacts, Tasks, Notes
 - **FYI... Desktop ActiveSync 4.0**
 - Removes Sync over Network (WiFi)
 - Why? Security, Was Not Encrypted
 - Still Supports BlueTooth (Link to Com Port)
 - Will Return, But Choice Not to Delay Windows Mobile 5.0
 - Continue to Use ActiveSync 3.8 if Needed
- 

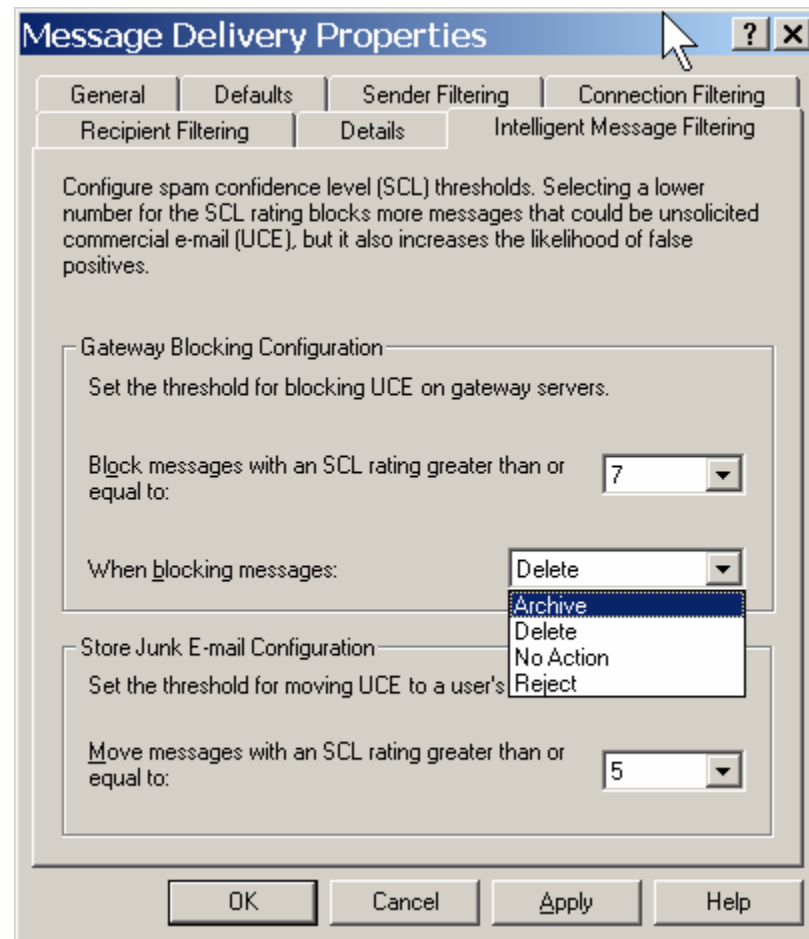
Controlling Exchange Message Delivery

- **Recipient Filtering and Sender Filtering**
- **Connection Filtering**
 - Real Time Block Lists (RBL)
 - Lists of bad Domains and IP Addresses
 - SpamHaus, ORDB, SpamCop
 - Can Use More Than 1
 - Arbitrary Who Gets Blocked
- **Defaults Tab**
 - Sending message size
 - Receiving message size



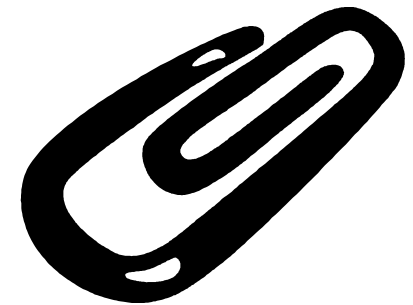
SPAM and IMF

- **Exchange Intelligent Message Filtering**
- **Free Add-on for Exchange 2003 Service Pack 1**
 - Included in SP2
- **Basic Solution with Minimal Control**
 - 3rd Party Add-ons (See Slipstick.com)
 - More Granular
 - Archive Viewers
 - Products using SCL (Spam Confidence Level)
- **Ideally Deploy On The Perimeter**



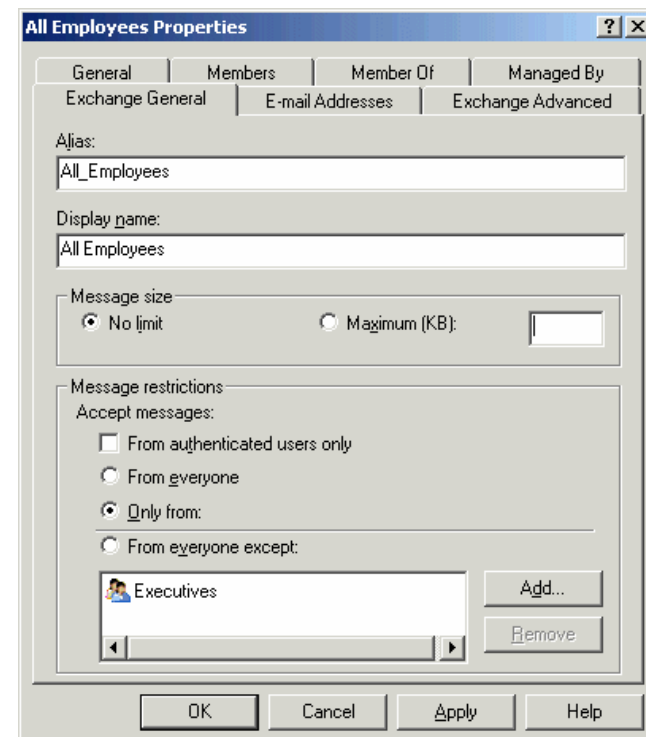
Attachment Blocking

- **The Problem...**
- **Can Already Turn Off Attachments in OWA**
 - Using HTTPS the Messages are Encrypted
 - But You Still Download Attachments
- **Front-End/Back-End Dependant**
 - Can Apply to Front-End Server Only
 - Internet OWA Users Get No Access to Attachments
 - Internal Users Connecting Directly to Back-End can use OWA with Attachments
 - Back-End Server is Really a Front-End Server Too!
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;830827>

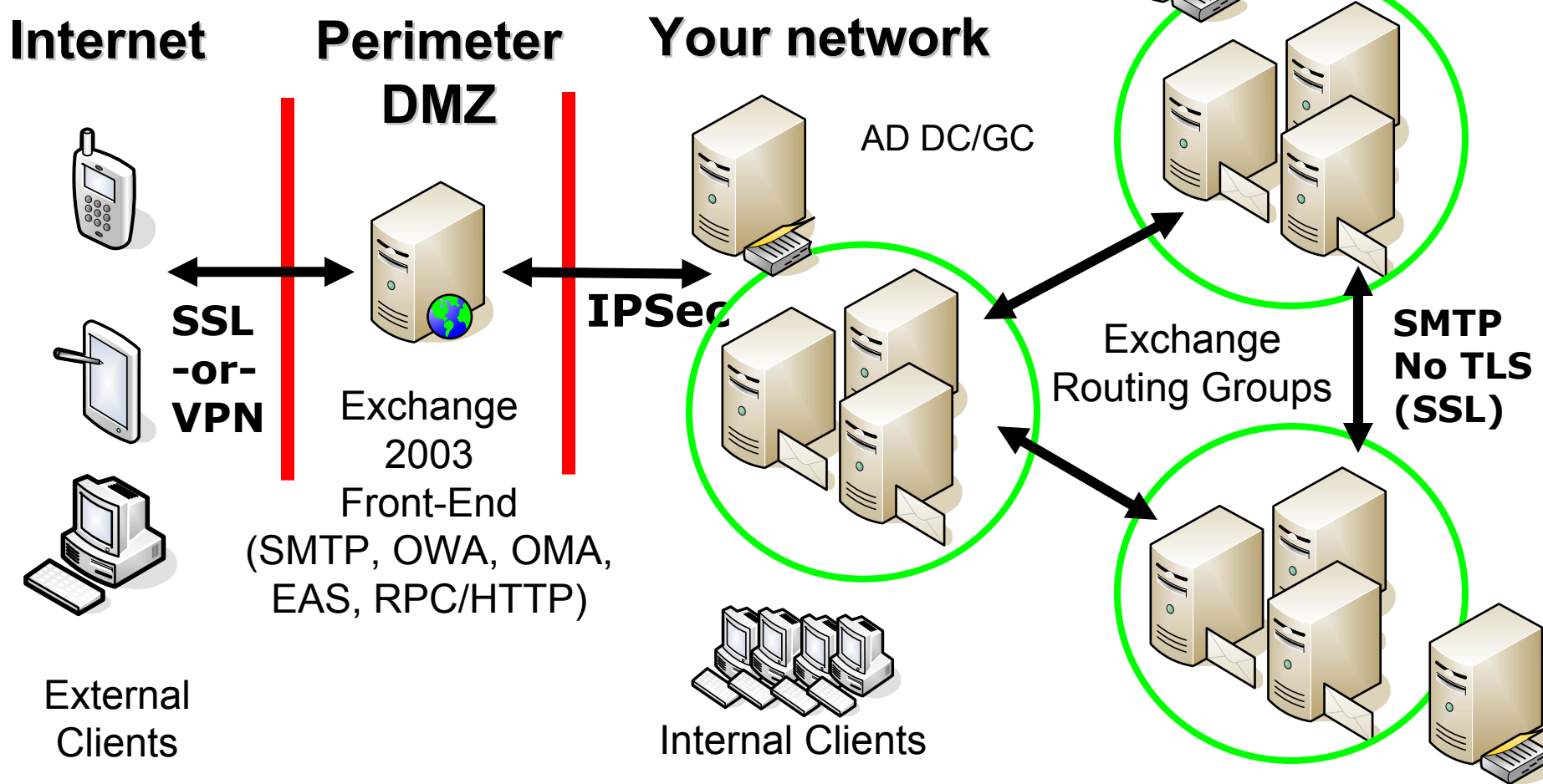


Block External Sending to DL's

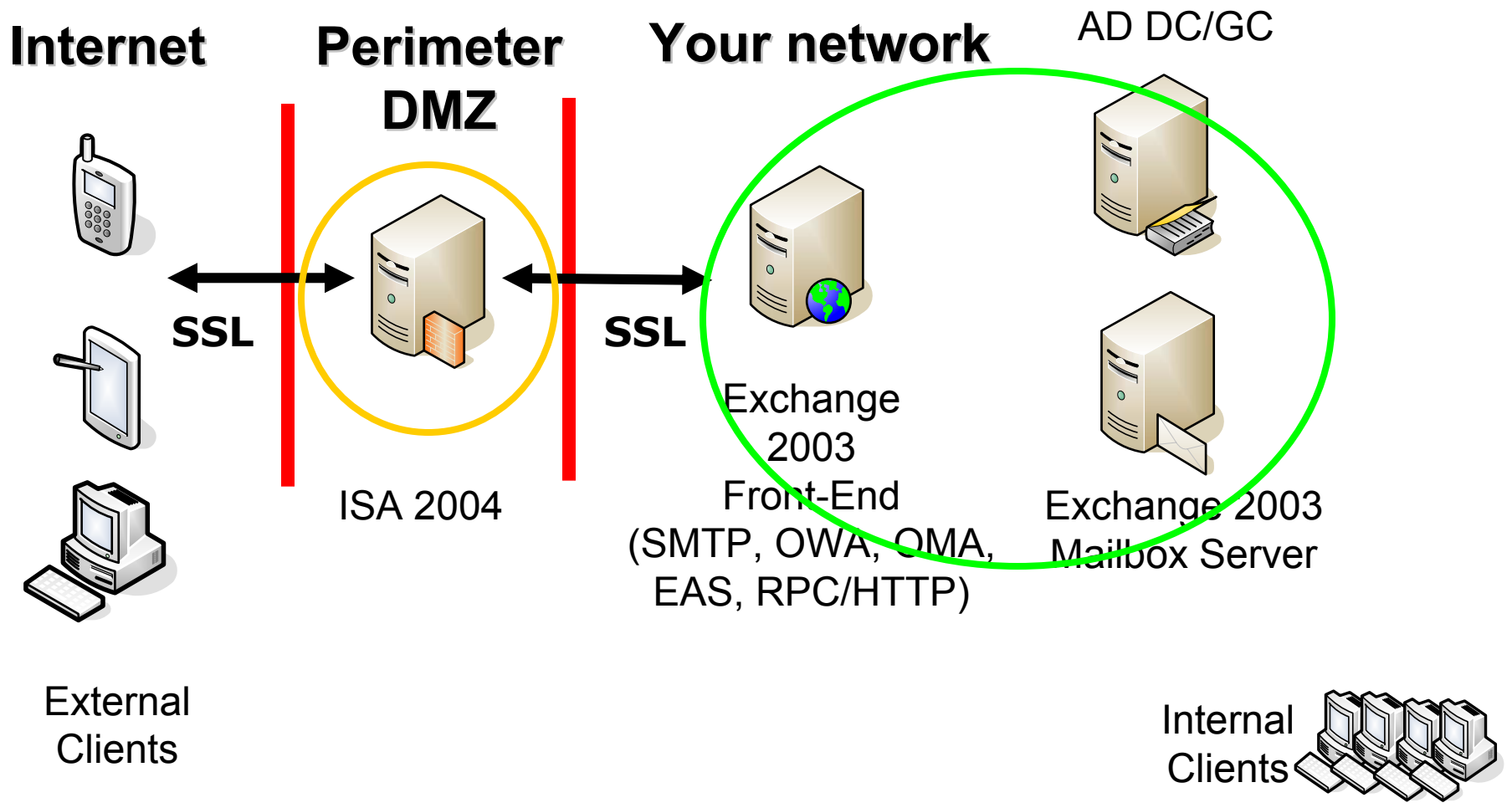
- **Prevent Unauthorized Sending to Distribution Lists (ok, Groups)**
- **Old Way- Add the DL to the DL**
- **New Way- Authenticated Users Checkbox**



FE/BE Exchange Network



ISA Server and Exchange



Using ISA Server 2004

- **Secure Publishing of Exchange Services**
- **Detect Exchange Specific Threats**
- **Move Forms-Based Authentication Off Exchange**
- **Stateful Packet Inspection**
- **ISA in Addition to Existing Firewalls**
- **ISA in 3RD Party Appliances**

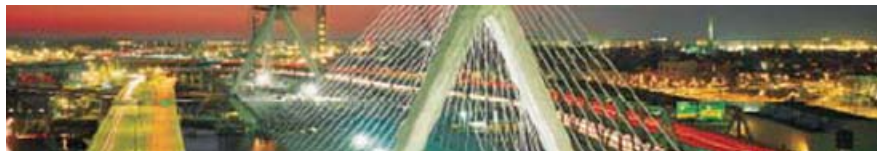
Resources

- **Exchange Team Blog**
 - <http://blogs.technet.com/exchange>
- **Exchange Best Practices Analyzer**
 - <http://www.exbpa.com>
- **Exchange Server 2003 Technical Documentation Library**
 - <http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/default.msp>
 - Message Security Guide for Exchange Server 2003
 - Ten Additional Exchange Security Documents
- **Exchange Virtual Labs**
 - Web-based Access To Labs
- **Utilities and Add-On Products**
 - <http://www.Slipstick.com>
- **TechTarget Articles**
 - <http://www.SearchExchange.com>

Thanks!



LeeB@ExchangeGuy.com
www.ExchangeGuy.com



www.ExchangeServerBoston.com