

# Messaging Security at Microsoft

Nam Ng  
Security Consultant  
Microsoft Corporation

# This session...

- Is about:
  - Securing the Exchange infrastructure  
...and how Microsoft IT does it
  - Based on Exchange Security Guides
    - Exchange Server 2003 Security Hardening Guide  
<http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/exsecure.mspx>
    - Securing Exchange Communications  
<http://www.microsoft.com/technet/security/guidance/secmod44.mspx>
- Is not about:
  - Protecting individual messages and S/MIME  
<http://www.microsoft.com/technet/itsolutions/msit/operations/trustmes.mspx>
  - Working with Exchange Active Directory permissions

# Session Objectives & Key Concepts

## ■ Session Objectives:

- Provide a broad overview of operational security principles for Exchange servers as outlined in Exchange Security Operations guide
- Show how these principles are applied by Microsoft IT
- Help you identify ways to immediately improve messaging security in customers environments

## ■ Key Concepts:

- Achieving messaging security at multiple layers
- Holistic approach to messaging security

# Agenda

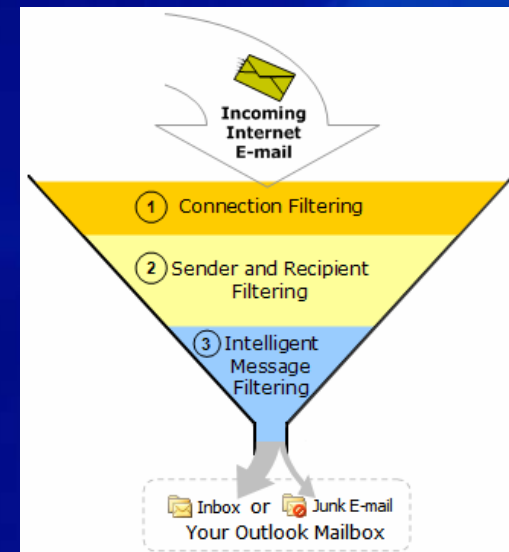
- E-mail Hygiene -maintaining secure messaging environment
- Hardening Exchange servers by role
- Securing Exchange communications
- Questions

# E-mail Hygiene

- E-mail hygiene is more than just AV/AS
- Threats:
  - Virus infected e-mail
  - UCE/Spam e-mail
  - Denial of Service (DoS) attacks
  - Mail bombing and NDR attacks
  - Directory Harvesting Attacks (DHA)
  - E-mail impersonation (spoofing) and phishing attacks
  - Unauthorized e-mail submission and relay

# Is E-mail Hygiene Important?

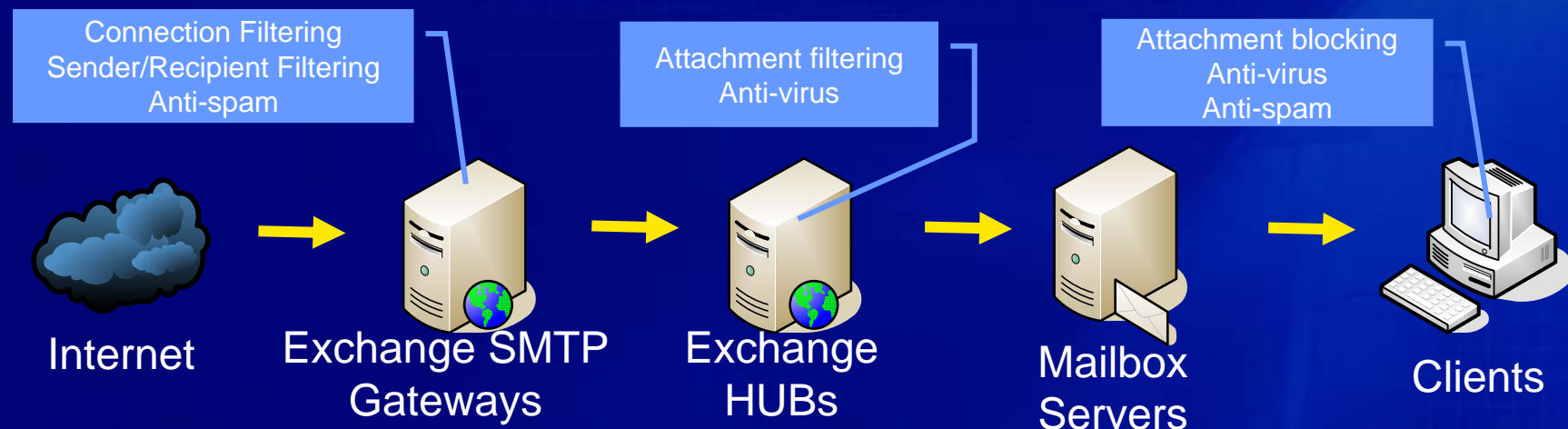
- Malicious and unsolicited e-mails - an annoyance to users
- ... but they are also a large hit to the infrastructure
- One day MS IT statistics (December 2004):
  - ... out of estimated **50,000,000+** e-mail submission attempts to *microsoft.com*
  - ...only about **1,500,000** were legitimate
- How to implement e-mail hygiene protection?
- Multi-layered defense is the key!



# E-mail Hygiene at Microsoft IT

## Layered Defense

- Exchange 2003 Server is used as platform
- Multiple protection layers:
  - Connection filtering
  - Sender and recipient filtering
  - Spam filtering
  - Attachment blocking
  - Anti-virus



# E-mail Hygiene at Microsoft IT

## Connection Filtering and RBLs

- Real-time DNS-based block lists
  - Check IP of sender against the block list using DNS queries
  - For the connecting IP of 1.2.3.4 RBL lookup against rbl.com provider is equivalent to `nslookup -q=A 4.3.2.1.rbl.com`
  - If DNS record for sender's IP exists, block it
- Exchange 2003
  - Supports multiple RBL providers
  - Terminates connection if IP address is black listed (SMTP protocol 550 error)
    - 550 5.7.1 E-mail rejected because 213.241.32.5 is listed by sbl-xbl.spamhaus.org. Please see <http://www.spamhaus.org/lookup.lasso> for more information. If you still need assistance contact [gtsrbl22@microsoft.com](mailto:gtsrbl22@microsoft.com)
  - Supports customizable response per configured provider

# E-mail Hygiene at Microsoft IT

## Sender and Recipient Filtering

- Sender and Recipient Filtering
  - Built into Exchange 2003 - Global Setting
  - Criteria based
  - Not as effective to combat spam, but is critical to fight mail bombing attacks
- One day Microsoft IT statistics (December 2004):
  - Filtering mail for **10** @microsoft.com recipients blocked 30,000,000+ malicious e-mail submission attempts
- Should we filter messages from our own domain in *inbound* mail?
  - It solves the problem of spoofing, but...
  - ... breaks remote distribution list scenarios
  - Sender ID is more proper approach to address the spoofing problem

# E-mail Hygiene at Microsoft IT

## Recipient Lookup

- Non Delivery Reports processing takes a significant amount of resources
- Recipient lookup feature validates recipients before accepting messages

```
C:\>telnet mailserver.domain.com 25
```

```
...
```

```
MAIL FROM:<>
```

```
250 2.1.0 <>....Sender OK
```

```
RCPT TO: <bogususer@domain.com>
```

```
550 5.1.1 User unknown
```

```
QUIT
```

- Result: No message payload is transmitted - savings in performance
- Microsoft IT statistics: up to 25 e-mail submission attempts/sec blocked by recipient lookup feature alone!

# E-mail Hygiene at Microsoft IT

## Recipient Lookup (continued)

- But, what if I do

```
RCPT TO: alias1@domain.com
```

```
RCPT TO: alias2@domain.com
```

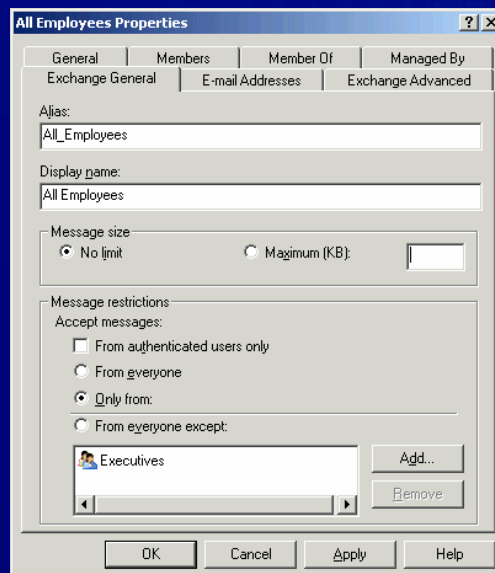
```
. . .
```

- Side effect: If carelessly implemented - possibility of rapid alias enumeration, a.k.a. Directory Harvest Attack (DHA)
  - Test: About 20 minutes to harvest all valid 4 character aliases within a domain
- Possible solution: Delay the 550 response for  $n$  seconds: slows down the attacker significantly. With 5 second delay it takes months to enumerate all 4 character alias combinations
- For Exchange 2003:  
<http://support.microsoft.com/default.aspx?kbid=842851>

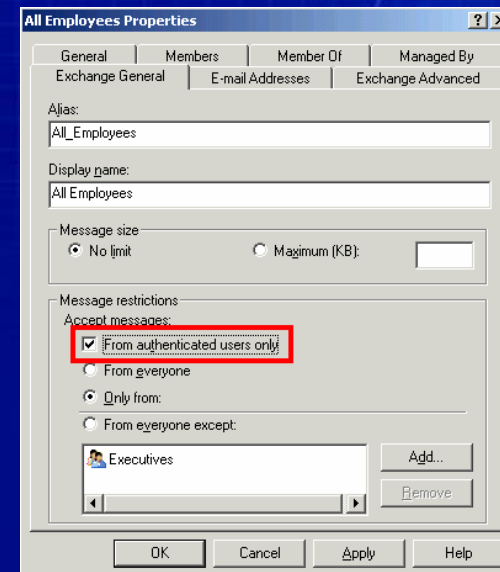
# E-mail Hygiene at Microsoft IT

## Restricted/Authenticated Distribution Groups

- Distribution Groups (DG) may contain large number of recipients. A single malicious message to a DG impacts a large number of users.
- Best Practice: Restrict large/sensitive internal DGs



Protects from most  
spam attacks, but...

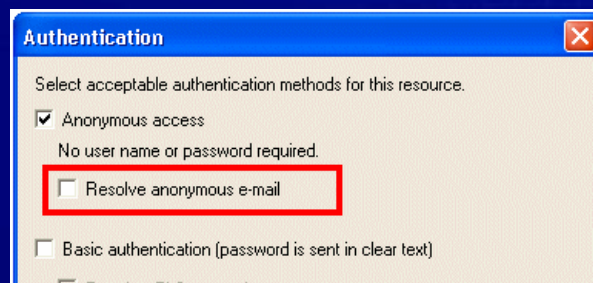


Much more secure!

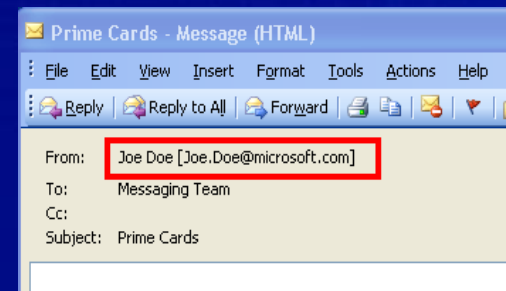
# E-mail Hygiene at Microsoft IT

## Mitigating the Spoofing Problem

- Root cause of spoofing - non authenticated SMTP mail submission
- Best practice: Minimize anonymous SMTP access internally
- For Internet e-mail must support anonymous SMTP connections
- Option 1: accept messages, but provide a visual indication to the user



**Exchange Gateway setting**



**Result on Outlook Clients**

# E-mail Hygiene at Microsoft IT

## Mitigating the Spoofing Problem

- Option 2: “authenticate” Internet messages as they are coming in
- Sender ID Framework - industry standard created to counter e-mail domain spoofing
  - Publish the list of approved e-mail servers in DNS (SPF record)
  - Authenticate incoming e-mail against this list
- For more info <http://www.microsoft.com/senderid>
- Microsoft IT supports the Sender ID initiative
  - Began Sender ID Framework implementation for microsoft.com
  - Microsoft.com Sender ID record
    - `nslookup -q=TXT microsoft.com.`

# E-mail Hygiene at Microsoft IT

## Spam Filtering

- Educating users about spam
- Spam fighting starts with guarding your e-mail address
- Fighting spam at multiple levels
  - Gateway (filtering)
  - Mailbox (move to Junkmail)
  - Client (move to Junkmail)
- MS IT uses the Intelligent Message Filter and Exchange 2003 SCL framework  
<http://www.microsoft.com/exchange/imf>

# Email Hygiene at Microsoft IT

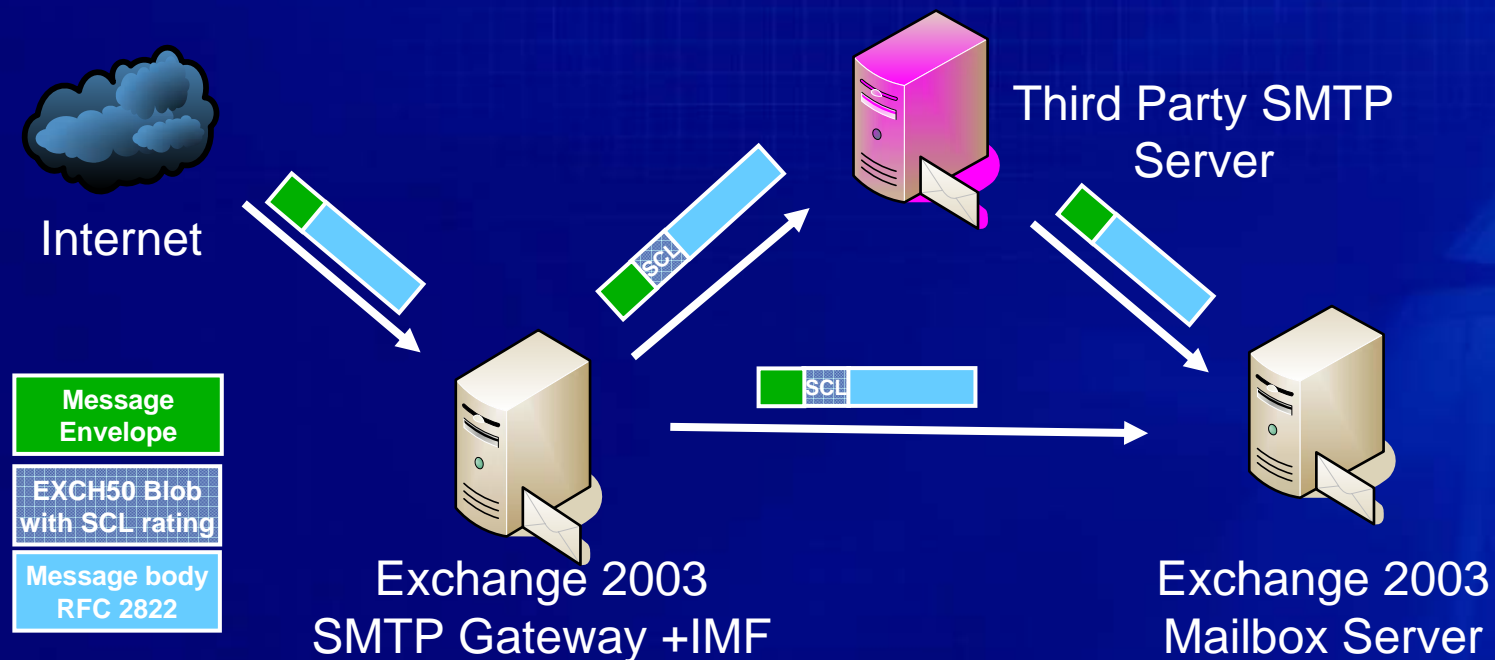
## Intelligent Message Filter (IMF)

- IMF is deployed on the front line Exchange 2003 gateways
- IMF examines messages and gives each an SCL value [0-9]
- Two thresholds: Gateway and Store
- Messages with a high SCL values are filtered at the gateway
  - Aggressive gateway threshold settings - higher filtering rate at the gateway
  - Reduces impact to users and the rest of the infrastructure
- SCL store level spam filtering
  - Assigned SCL rating persists with the message
  - If  $SCL > msExchUceStoreActionThreshold$  value, then Junkmail
- Exposing SCL in Outlook  
<http://blogs.msdn.com/exchange/archive/2004/05/26/142607.aspx>

# Email Hygiene at Microsoft IT

## Intelligent Message Filter (IMF)

- Key infrastructure design points:
  - IMF is positioned before anti-virus scanning
- To preserve SCL value SMTP transport behind IMF must
  - Be authenticated
  - Support EXCH50 blob propagation



# E-mail Hygiene at Microsoft IT

## E-mail Anti-virus

- 10,000 - 500,000 e-mail viruses per day are stopped by the MS IT gateways
- Best practice - scanning at multiple layers
- Possible options
  - Gateway
  - Information Store
  - Client
- The key to success is consistent enforcement of AV policies
- MS IT focus: E2K3 Gateway and Client scanning

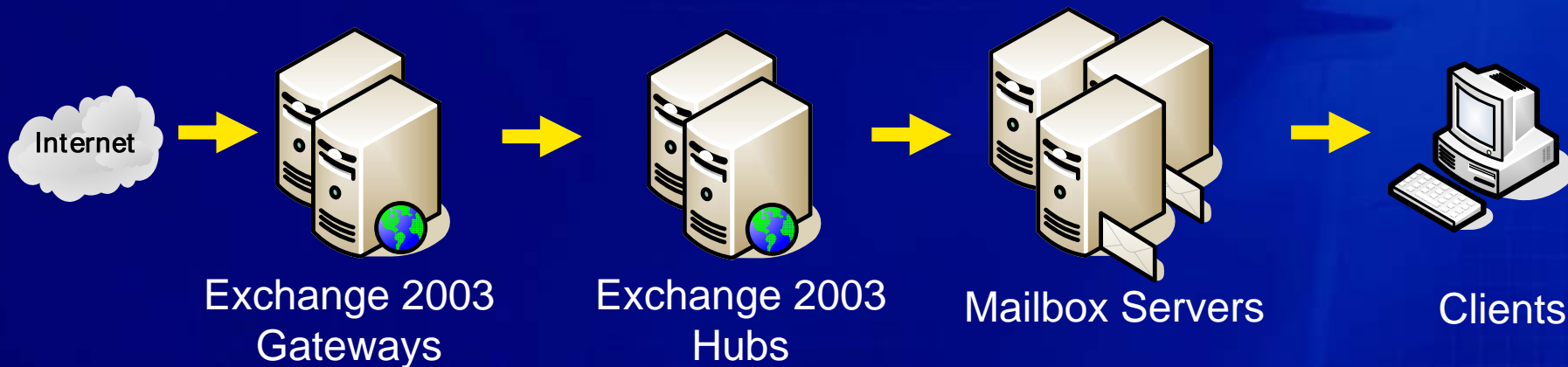
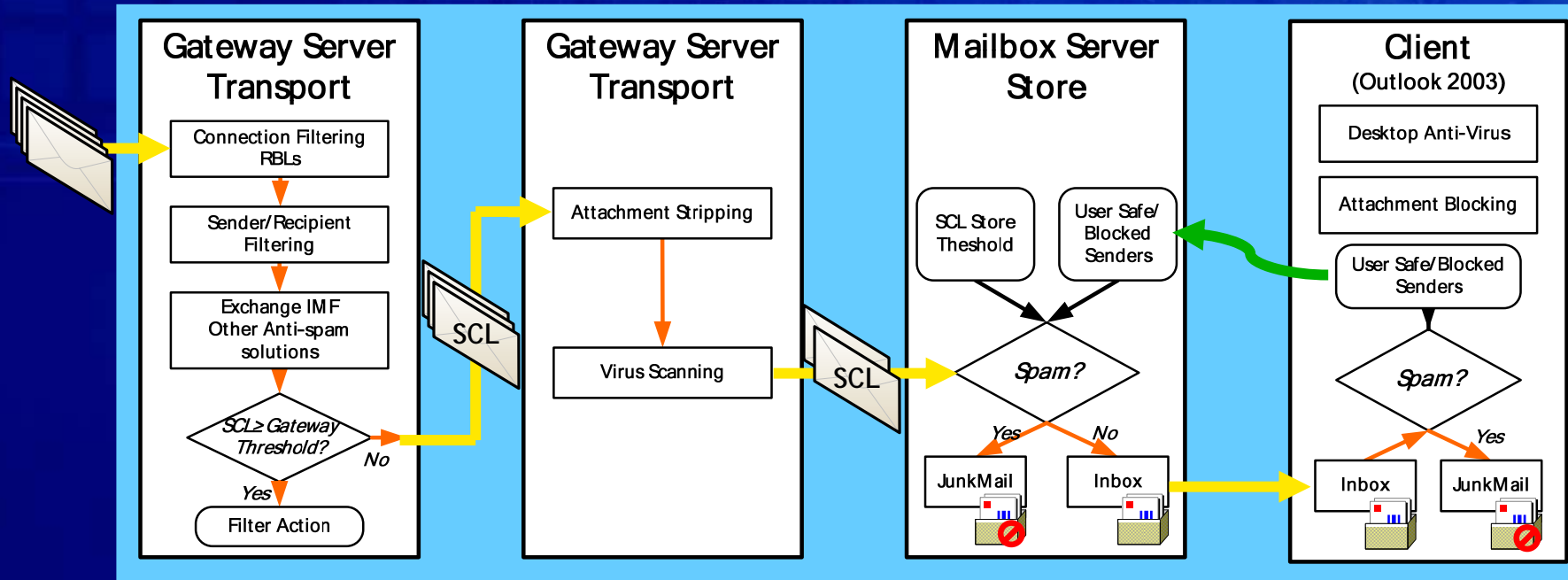
# E-mail Hygiene at Microsoft IT

## Attachment Blocking

- Mitigates the risks for new/unknown e-mail viruses
- Enforced at two levels: client and gateway
- Client level:
  - Outlook 2003 attachment blocking (Q829982)
- Gateway level:
  - Executable attachment stripping for all inbound mail
  - Occurs prior to virus scanning - performance wins

# E-mail Hygiene at Microsoft IT

Bringing it All Together



# Securing the Clients

- Many out of the box security features
  - Kerberos authentication for Outlook 2003
  - Attachment blocking for Outlook/Outlook Web Access
  - Web beacon blocking
  - Junk mail filtering
- Additional client security
  - Limit the client types in use to only those required
  - Proactively block outdated/vulnerable clients from accessing the Exchange store (Q288894)

# Hardening Exchange Servers

- Hardening the Operating System
  - Also see Windows Server 2003 Security Guide (<http://go.microsoft.com/fwlink/?LinkId=21638>)
- Hardening Exchange Platform

# Hardening Windows

- Security group membership
  - Who has administrator privileges on the Exchange server?
- User rights on Exchange servers
  - Exchange 2003 denies regular domain users the "Allow log on locally" rights
- File and share level permissions
  - Who can access the Exchange tracking logs share?
- Windows services
  - Do I need the "Wireless configuration" service on Exchange?

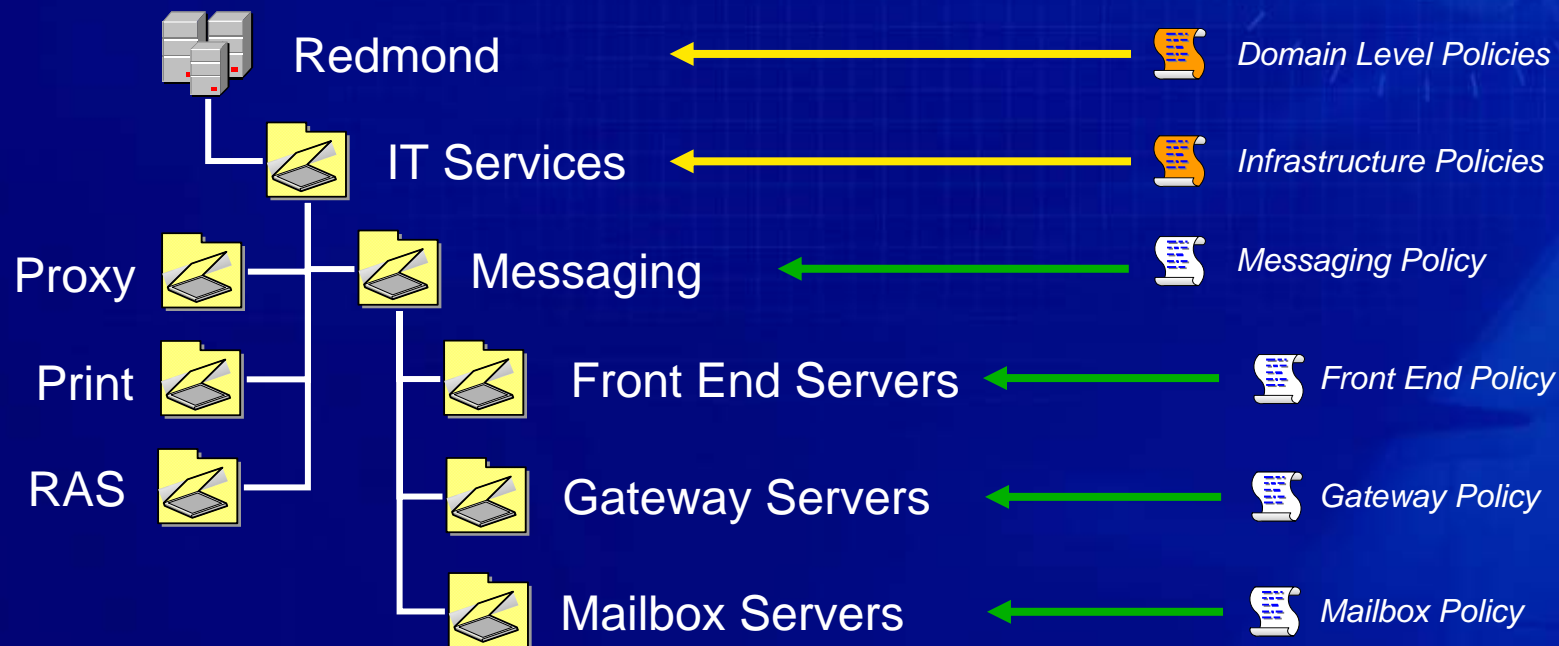
# Hardening Windows (con't)

- Internet Information Server (IIS)
  - Should I have */scripts* and */IISAdmin* directories?
  - IIS Lockdown for IIS versions prior to 6.0 (KB309508)
- File level anti-virus
  - If misconfigured, will cause database corruption (KB823166 & KB328841)
- Consistency is the key!
  - ... but how to achieve it across all Exchange servers in the ORG?
- Windows Group Policies (GPO) can help!

# Hardening Windows Platform

## Using Windows Group Policies

- “Role based” approach
- Active Directory Organizational Units are used to group servers by role



- New Exchange servers automatically receive security settings according to their role

# Hardening Exchange

- Exchange 2003 *Secure by default* examples
  - Legacy protocols (POP3/IMAP4) are disabled
  - OMA is disabled
  - OWA password changes are off
  - Kerberos authentication between OWA FE and BE
  - Anonymous SMTP relaying is off
  - Top Level Public Folders are locked down
  - 10MB message limits
  - Tightened permissions
- Special case - upgrade scenarios!
  - Existing settings are often not changed

# Hardening Exchange by Role

## Exchange Front End Servers at Microsoft IT

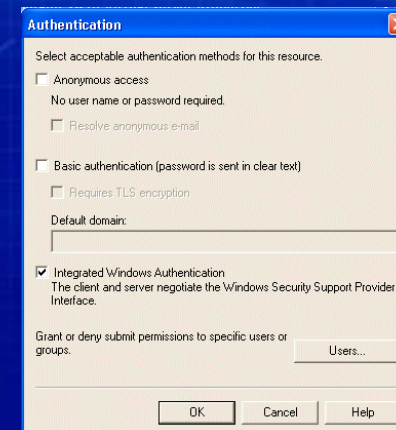
- OWA, OMA, EAS, RPC/HTTPs on a single consolidated platform (Exchange 2003)
- Reduced attack surface
  - POP3/IMAP4/SMTP are disabled
  - Information Store is removed
- Forms based authentication and session timeouts for OWA
- Reduced infrastructure exposure for RPC/HTTPs
  - Leverage Exchange 2003 SP1 RPC/HTTP enhancements
  - No DC exposure for RPC/HTTPs
  - Only ports 6001, 6002 and 6004 of the Back End are allowed
- SSL is enforced between the client and the FE server at all stages
- Kerberos authentication between the Front End and Back End servers

# Hardening Exchange by Role

## Exchange Gateway Servers at Microsoft IT

- No anonymous SMTP relaying, even internally
- No SMTP authentication is exposed to the Internet
  - Prevents password guessing
- Secure authentication for internal connections
  - If anonymous is enabled "Send As" check can't be enforced
- Explicit maximum message size and DSNs on SMTP Virtual Servers

```
←220 microsoft.com ESMTP Server
→ehlo
←250-maila.microsoft.com Hello [207.46.125.18]
←250-THRN
←250-SIZE 10485760
←250-DSN
```



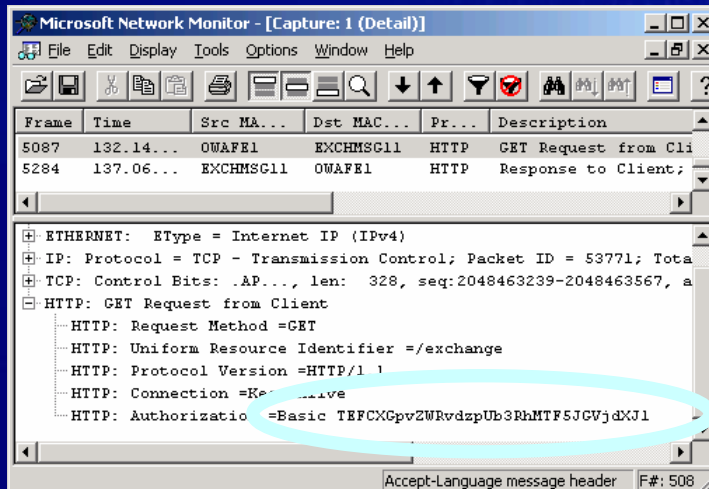
Prevents remote servers from transmitting large messages

# Securing Exchange Communications

- What do you want to secure?
  - User data in transit
  - User credentials
  - System data in transit
- What do you want to secure against?
  - External threats
  - Internal threats

# Securing Authentication

- Use Windows Integrated authentication
- Proactively disable insecure (Basic) authentication throughout the messaging infrastructure wherever possible

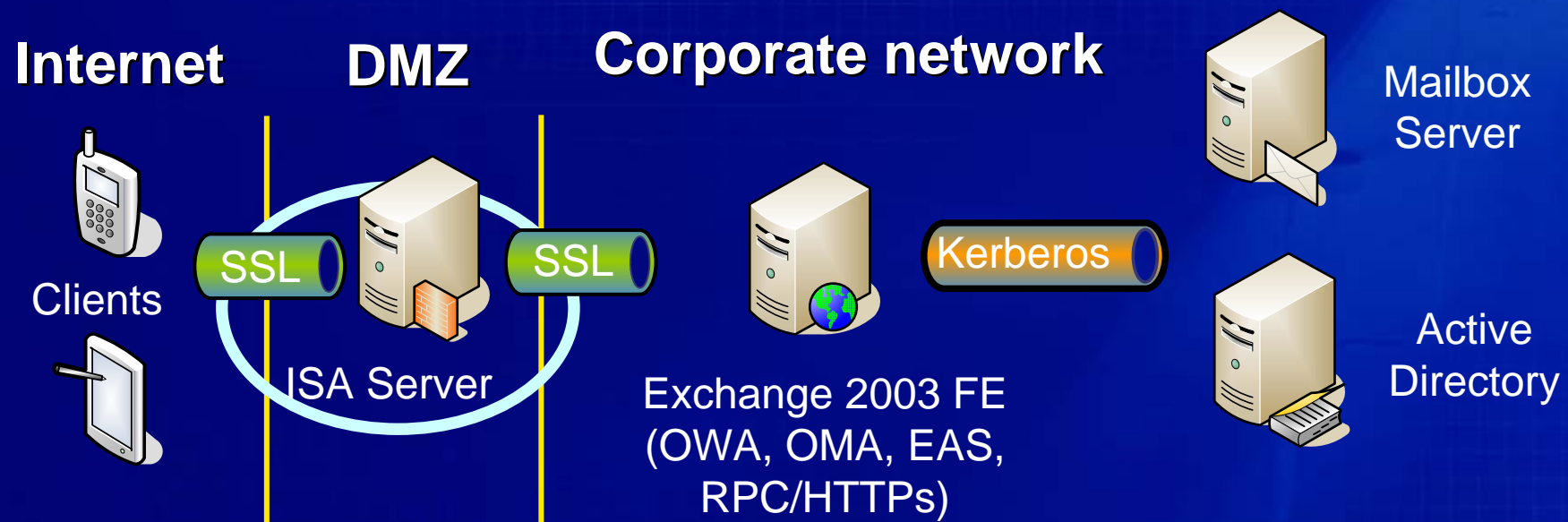


```
C:\>base64
>> decode TEFCXGpvZWRvdzpwUb3RhMTF5JGVjdXJl
DOMAINjoedoe:Tota11y$ecure
decode succeeded
```

- *Idifde -d "CN=Microsoft Exchange, CN=Services, CN=Configuration, DC=contoso, DC=com" -r "(objectClass=protocolCfgSMTPServer)" -p Subtree -l msExchAuthenticationFlags -f CON:*
  - *1 - Anonymous, 2 - Basic, 4 - Windows Integrated*
- If Basic authentication is absolutely required, use transport level security (SSL/TLS, IPSEC)

# Securing Mobile Messaging Communications

- Reduced exposure - the Exchange FE servers are in CorpNet rather than in the DMZ
- ISA 2004 is used to protect Exchange FE servers - SSL bridging mode
- Certificate on the FE server must be trusted and "verifiable" by ISA

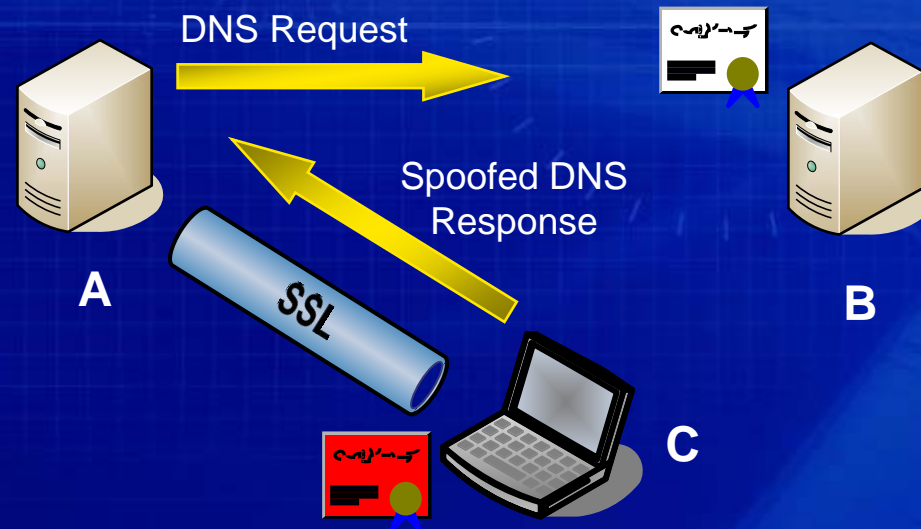


# Using IPSEC for Exchange

- IPSEC was essential to secure Exchange 2000 FE-to-BE OWA transactions in Microsoft IT environment
  - IPSEC policies example
    - Exchange FE: *me* → *any*; *TCP any* → *80*; *Encrypt (Kerberos)*
    - Exchange BE: *Respond only*
  - You can be really creative with IPSEC if “block on fail” is needed
  - Use GPO to apply IPSEC policies by server role
- Exchange 2003 FE-to-BE uses Kerberos authentication
  - User credentials are encrypted by default
  - IPSEC is still possible to protect data traveling between FE and BE, but beware of data exposure at the next hop (SMTP)

# Using SSL/TLS

## ■ Does SSL/TLS provide security?



## ■ Best Practices:

- Use certificates trusted by communicating parties
- Ensure that clients/servers perform full certificate validation (i.e. trust chain, common name, expiration)
- When enabling SSL, don't permit non-SSL connections

# Conclusion

## ■ Key things to remember

- Stay up-to-date with software and patch versions at all levels
- Establish layered e-mail hygiene defenses
- Enforce e-mail security at multiple levels
- Secure Exchange servers by role
- Consistently enforce OS security settings (for example, through Group Policies)
- Do periodic audits to ensure that security levels are maintained
- Be cognizant of security in upgrade scenarios
- Use only secure authentication methods and enforce SSL/TLS or IPSEC where needed

# IT Showcase: How Microsoft Does IT

Customer-ready resources from Microsoft IT

- IT Showcase on TechNet  
<http://www.microsoft.com/technet/itshowcase/>
- IT Showcase on Microsoft Services  
<http://www.microsoft.com/itshowcase/>

Get with IT

The Microsoft logo is displayed in a bold, italicized, white sans-serif font. The letters are slightly shadowed, giving them a three-dimensional appearance. The logo is centered horizontally on a dark blue background that features a faint grid pattern and a large, semi-transparent image of a hand holding a pen, suggesting a design or engineering theme.

***Microsoft***<sup>®</sup>

© 2006 Microsoft Corporation. All rights reserved. This presentation is for informational purposes only.  
MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.