Lee Benjamin

Messaging Architect

Consulting

ExchangeGuy

MVP Microsoft Most Valuable Professional

ExchangeGuy Consulting

- Email Systems for 20+ Years

ExchangeGuy

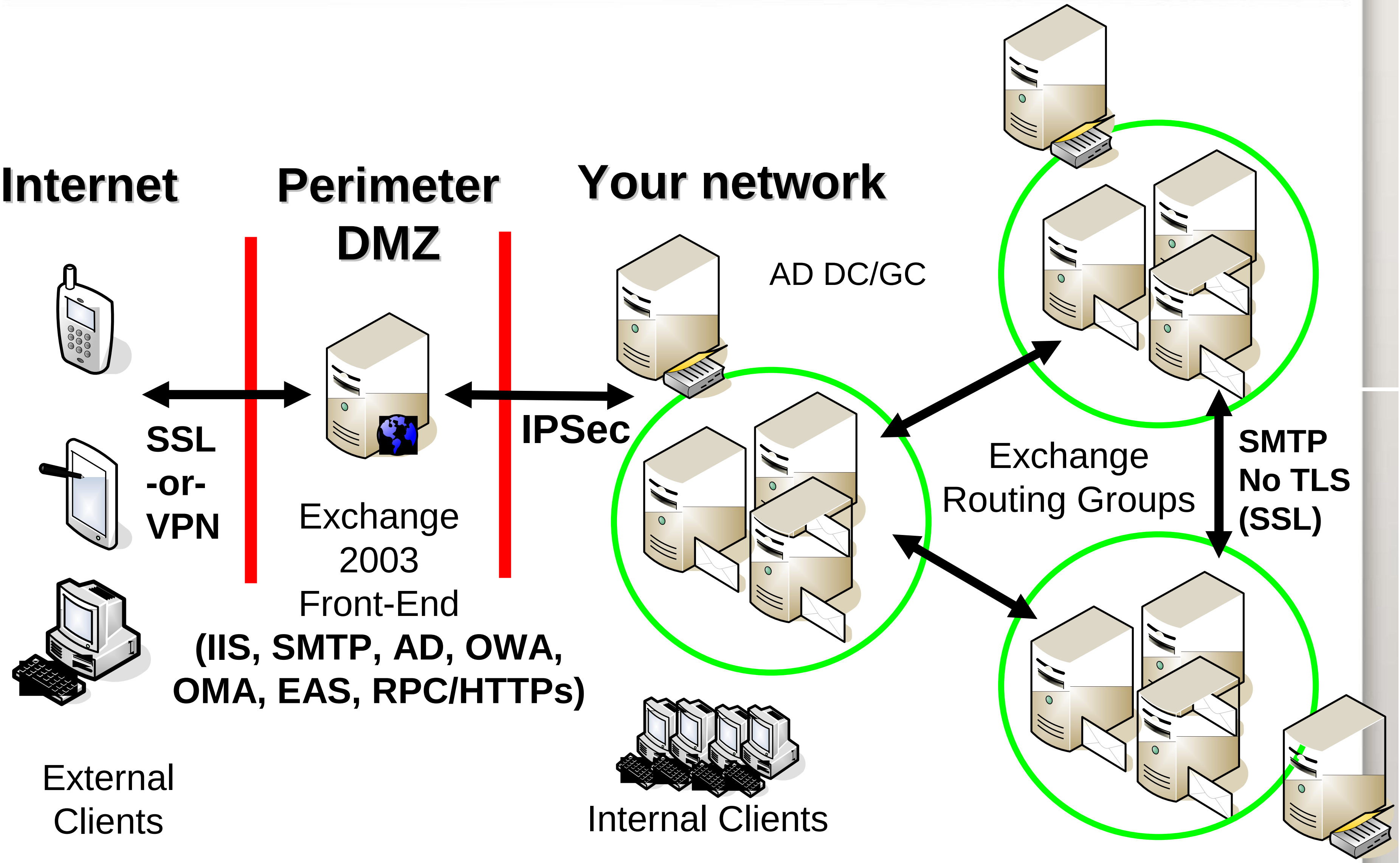
- Everything Exchange
  - Architecture, Migration/Upgrades, Security, Guidance,
    ISV Advisor, Strategy, Testing, Whitepapers, Reviews

- Trainer, Author, Speaker, User Groups, MVP

MVP Microsoft Most Valuable Professional

Agenda

- Exchange 2003 Security
-
- Security Fundamentals of Exchange 2007
- Additional Security
- Expanding Servers and Protocols
- Microsoft in the Security Space
- Questions



Internet

Perimeter DMZ

Your network

SSL -or- VPN

IPSec

AD DC/GC

Exchange 2003 Front-End

(IIS, SMTP, AD, OWA, OMA, EAS, RPC/HTTPs)

Exchange Routing Groups

SMTP No TLS (SSL)

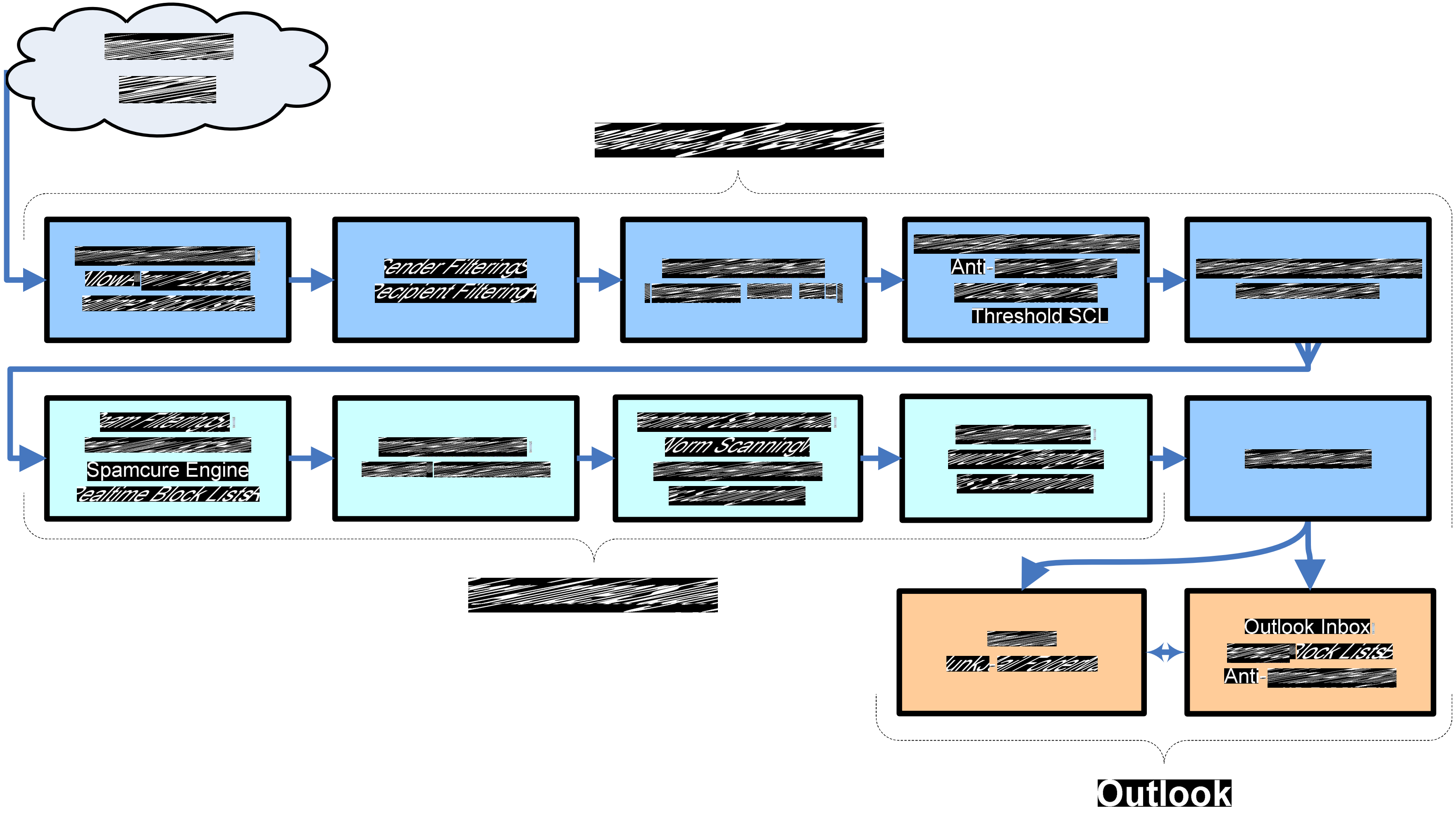
External Clients

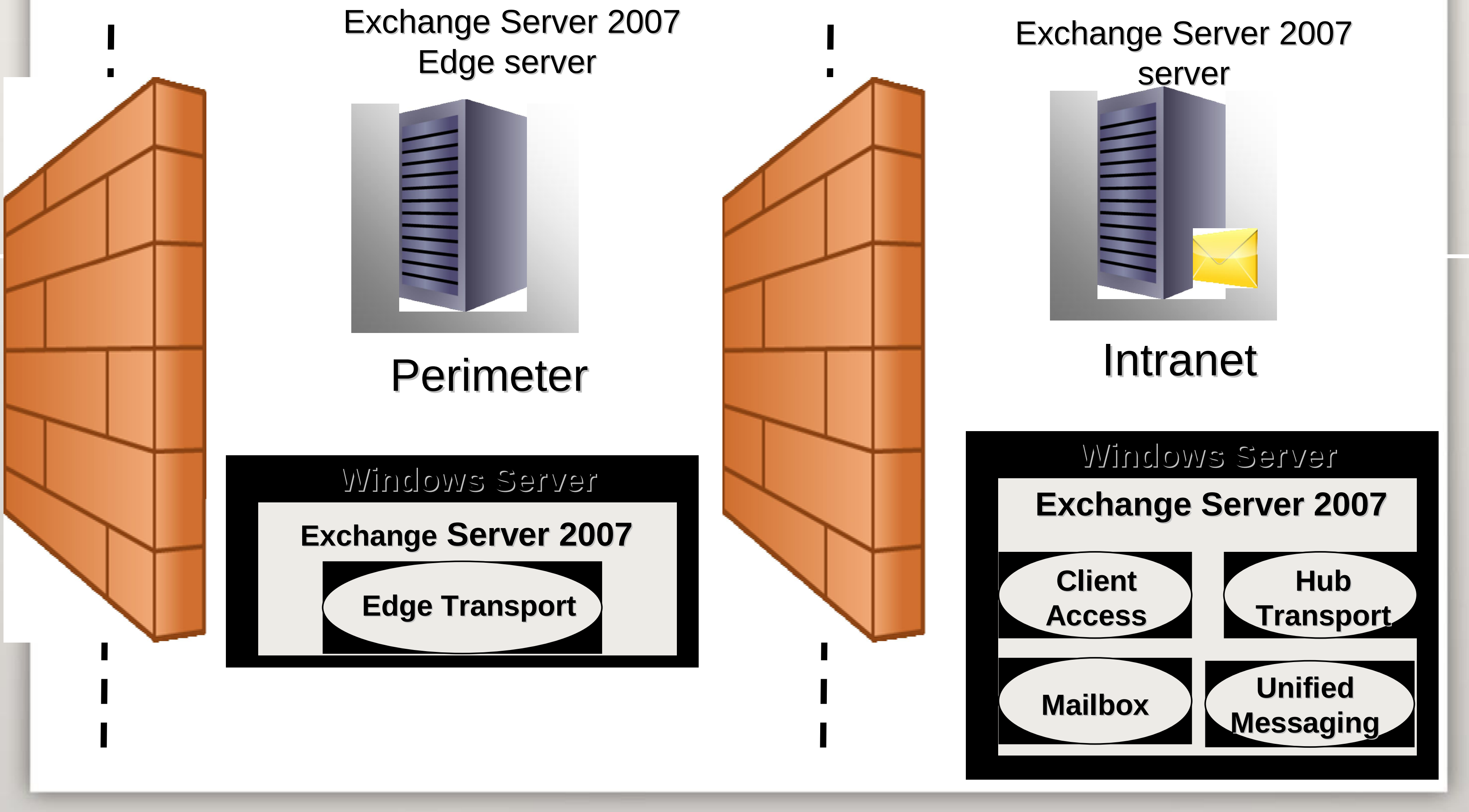
Internal Clients

Exchange 2003 Security

- Concerns with Exchange in the DMZ
  - Port 25, TLS Difficult, Other Ports
  - Active Directory in Perimeter
  - IIS Exposure, patches, etc.
- Internal Communications Between Servers
-
- Installed, Appliance, and/or Hosted
- Violation of ABM Treaty
  - Everything else goes here….

Messaging Protection 2003





Exchange Server 2007
Edge server

Perimeter

Windows Server

Exchange Server 2007

Edge Transport

Exchange Server 2007
server

Intranet

Windows Server

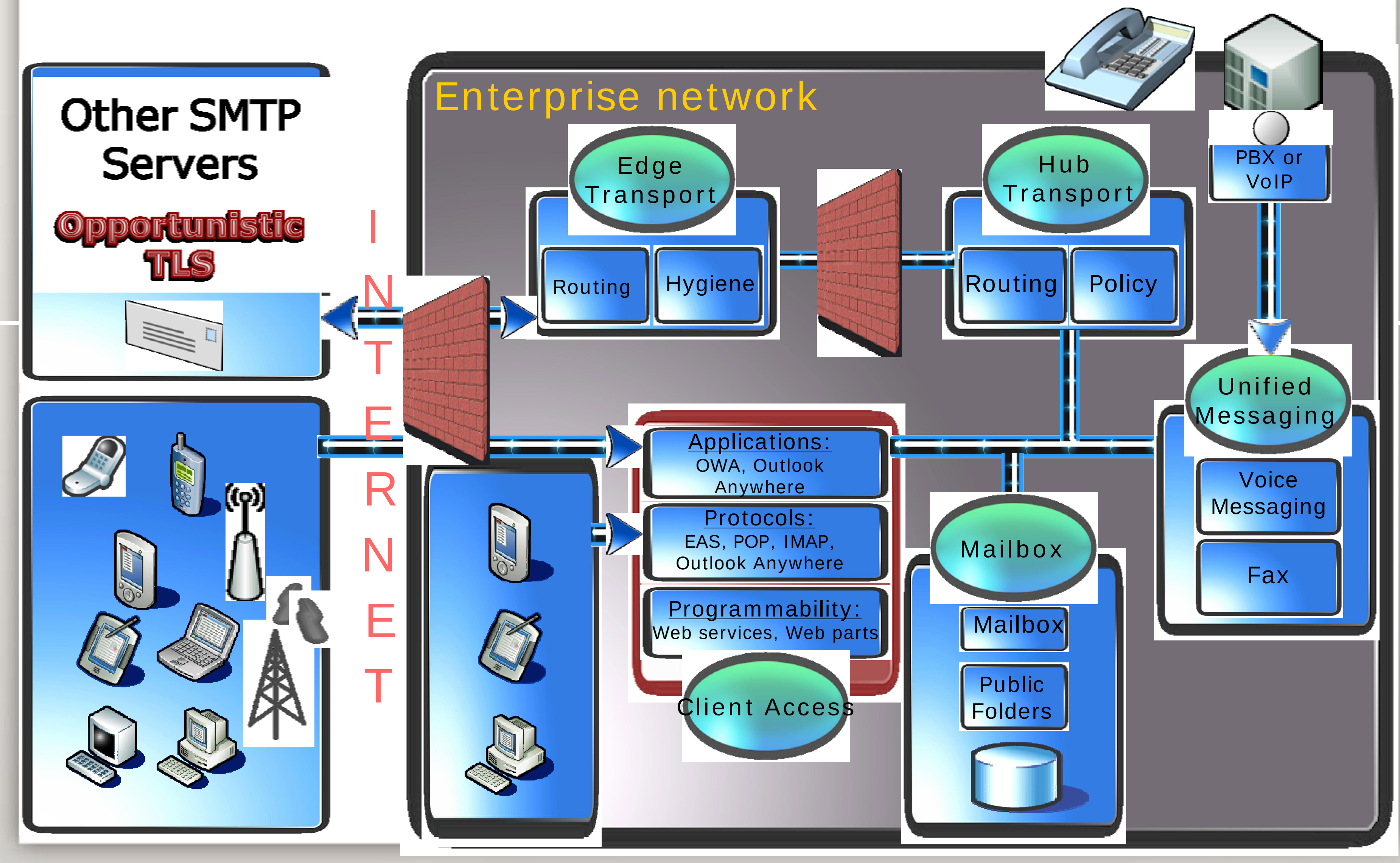
Exchange Server 2007

Client Access

Hub Transport

Mailbox

Unified Messaging



Other SMTP Servers

Opportunistic TLS

INTERNET

Enterprise network

Edge Transport

Routing

Hygiene

Hub Transport

Routing

Policy

PBX or VoIP

Unified Messaging

Voice Messaging

Fax

Applications:
OWA, Outlook Anywhere

Protocols:
EAS, POP, IMAP, Outlook Anywhere

Programmability:
Web services, Web parts

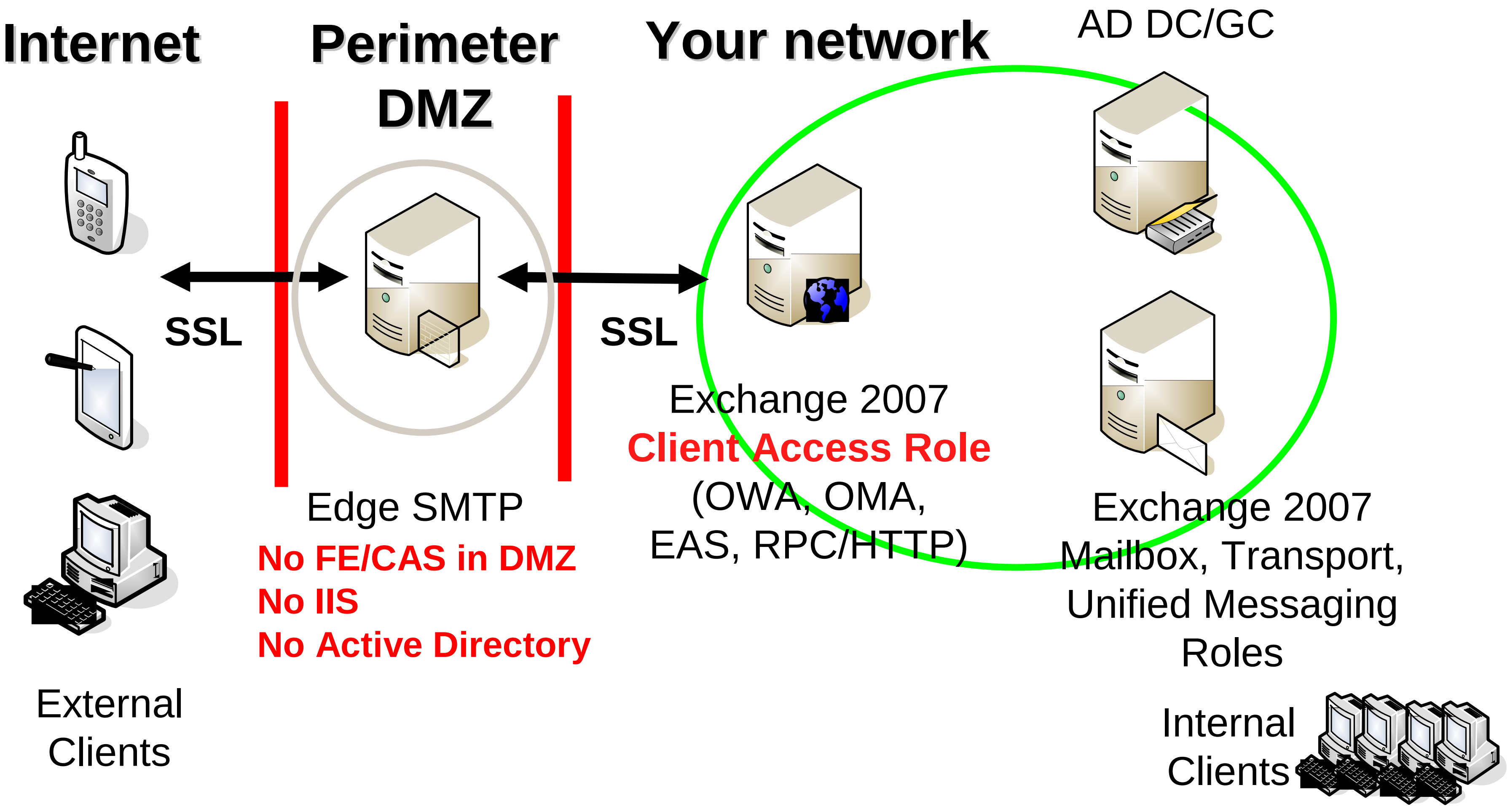
Client Access

Mailbox

Mailbox

Public Folders

Exchange 2007 and the Perimeter



Internet

Perimeter DMZ

Your network

AD DC/GC

SSL

SSL

Edge SMTP

No FE/CAS in DMZ

No IIS

No Active Directory

Exchange 2007

Client Access Role

(OWA, OMA, EAS, RPC/HTTP)

Exchange 2007

Mailbox, Transport, Unified Messaging Roles

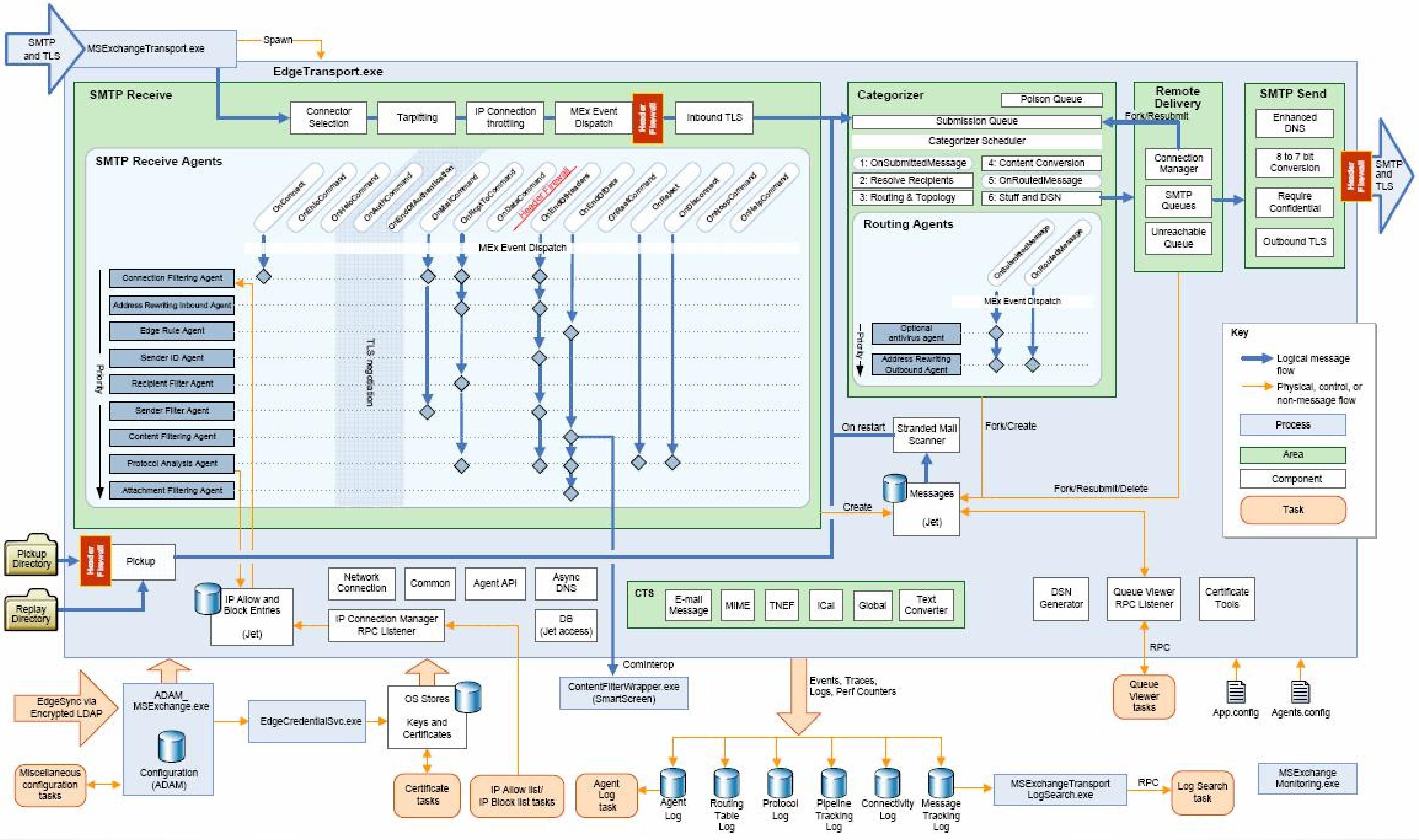
External Clients

Internal Clients

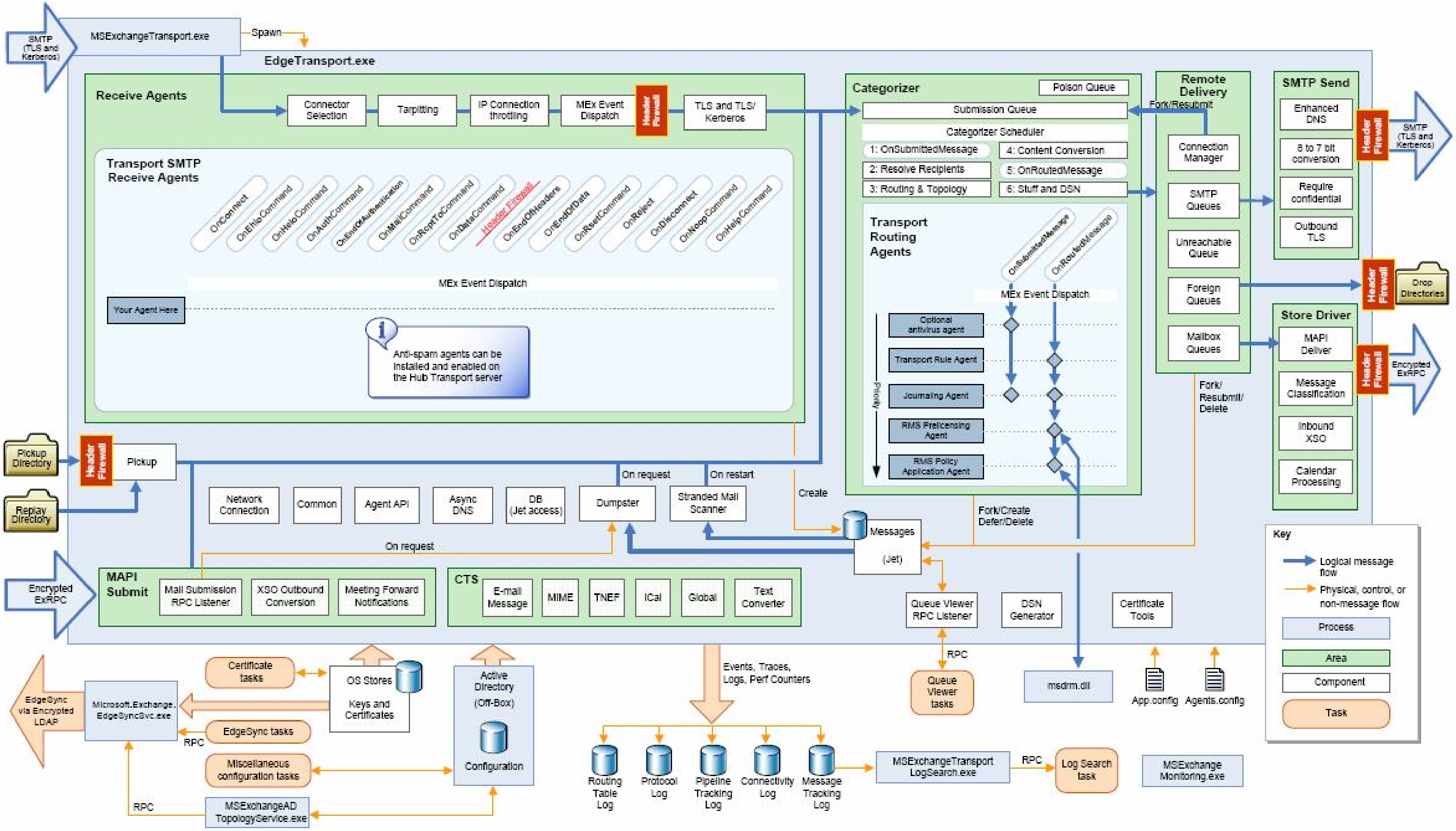
No Client Access Server Role in Perimeter

- Was Exchange 2003 Front-End Server
  - -ActiveSync
-
- Extra Protection for IIS and AD
- Reduce Open Ports on Internal Firewall
- Most IPSEC Tunnels Done Wrong, or Non-Existent
- HTTPS Through The Firewalls...

-
  - No connection to Active Directory required
  - EdgeSync pushes AD data out to Edge servers
- Supports Internet MTA features
  - Address Rewrite, Smarthost
  - Automatic TLS, Internal and External
- Resilient to Internet floods and attacks
  - Exchange anti-spam, Built in resilience
  - Managed code, No IIS
- ISV Solutions on Edge
- Edge is Optional



Microsoft® Exchange Server 2007 Edge Transport Server Role Architecture

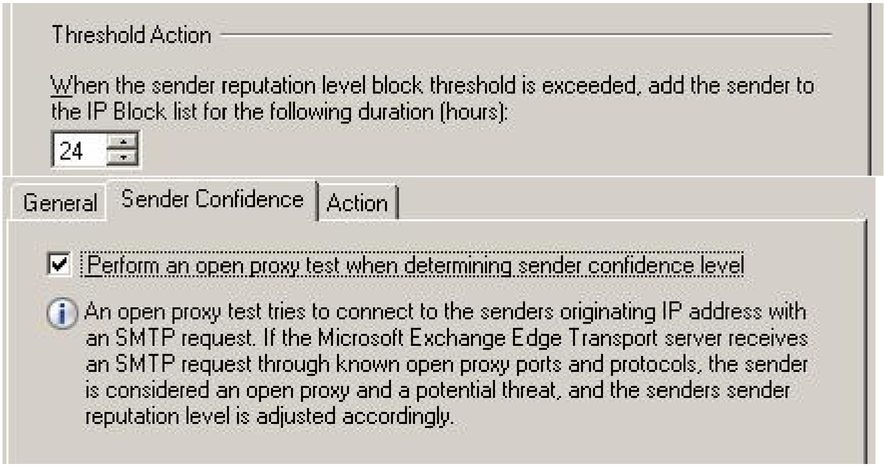


Microsoft Exchange Server 2007 Hub Transport Server Role Architecture

Sender Reputation Services

- IP Reputation Service and Protocol Analysis
  - Sender Reputation built from Hotmail data
  - Distributed via Microsoft update packages

  ?á Also learns from connections and messages that are seen on the local server



Threshold Action

When the sender reputation level block threshold is exceeded, add the sender to the IP Block list for the following duration (hours):

24

☑ Perform an open proxy test when determining sender confidence level

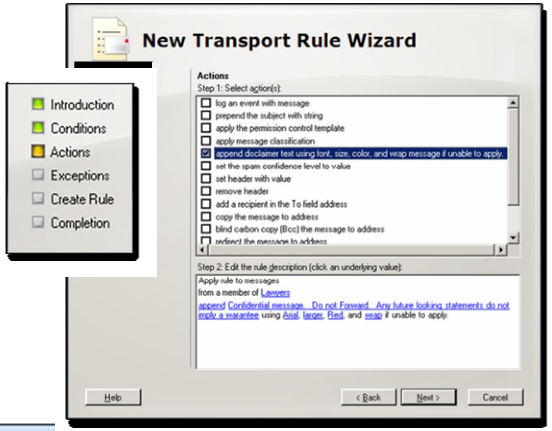
An open proxy test tries to connect to the senders originating IP address with an SMTP request. If the Microsoft Exchange Edge Transport server receives an SMTP request through known open proxy ports and protocols, the sender is considered an open proxy and a potential threat, and the senders sender reputation level is adjusted accordingly.

?á Builds server local reputation and blocks targeted spam attacks

- Based on average spam rating
- Open proxy checks
- Protocol anomalies

Transport Rules and Compliance Folders

- Transport rules
  - Inspect and take action…, modify (e.g. add disclaimer), encrypt, route
- Flexible email retention
- Multi-mailbox search for discovery
- Retention rules
- Granular journaling
- Third party opportunity



New Transport Rule Wizard

Actions

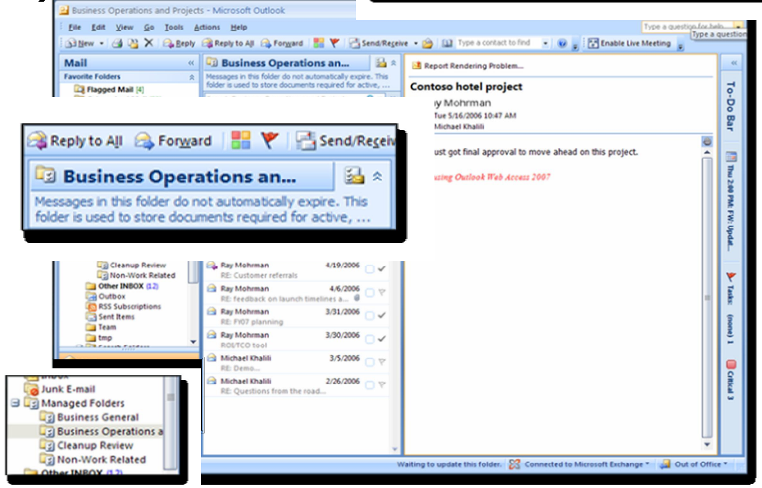
Step 1: Select action(s):

- ☐ log an event with message
- ☐ prepend the subject with string
- ☐ apply the permission control template
- ☐ apply message classification
- ☑ append disclaimer text using font, size, color, and wrap message if unable to apply.
- ☐ set the spam confidence level to value
- ☐ set header with value
- ☐ remove header
- ☐ add a recipient in the To field address
- ☐ copy the message to address
- ☐ blind carbon copy (Bcc) the message to address
- ☐ redirect the message to address

Step 2: Edit the rule description (click an underlying value):

Apply rule to messages
from a member of Lawyers
append Confidential message. Do not Forward. Any future looking statements do not imply a warantee using Arial, larger, Red, and wrap if unable to apply.

Help
< Back
Next >
Cancel



Business Operations and Projects - Microsoft Outlook

File Edit View Go Tools Actions Help
New Reply Reply to All Forward Send/Receive Type a contact to find Enable Live Meeting
Type a question for help
Mail
Favorite Folders
Flagged Mail [4]
To-Do Bar
Tasks: (none) 1
Critical 3

Business Operations an...

Messages in this folder do not automatically expire. This folder is used to store documents required for active, ...

Report Rendering Problem...

Contoso hotel project

y Mohrman
Tue 5/16/2006 10:47 AM
Michael Khalili

ust got final approval to move ahead on this project.

sing Outlook Web Access 2007

Cleanup Review
Non-Work Related
Other INBOX (12)
Outbox
RSS Subscriptions
Sent Items
Team
tmp

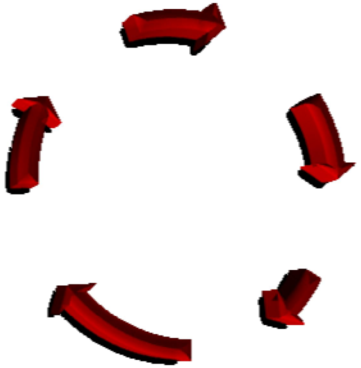
Ray Mohrman RE: Customer referrals	4/19/2006
Ray Mohrman RE: feedback on launch timelines a...	4/6/2006
Ray Mohrman RE: FY07 planning	3/31/2006
Ray Mohrman ROI/TCO tool	3/30/2006
Michael Khalili RE: Demo...	3/5/2006
Michael Khalili RE: Questions from the road...	2/26/2006

Junk E-mail
Managed Folders
Business General
Business Operations a
Cleanup Review
Non-Work Related
Other INBOX (12)

Waiting to update this folder. Connected to Microsoft Exchange Out of Office

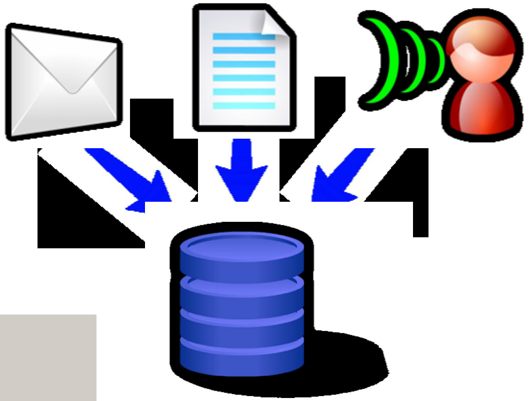
Are You Sure You Want To Send That Email ??

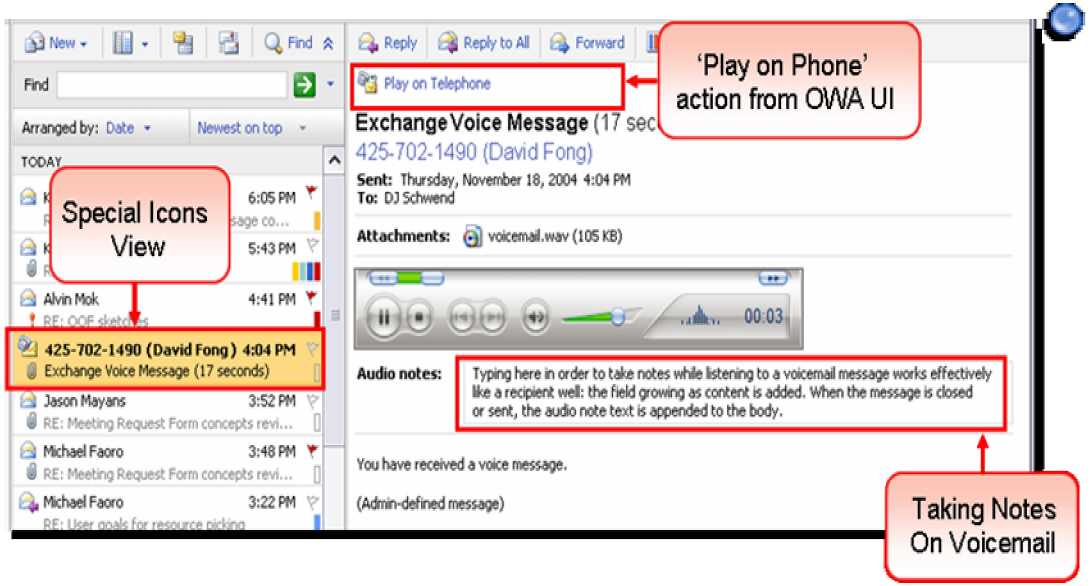
Data Protection (LCR/CCR/SCR)



- Backup for Availability
  - Copies of Exchange Databases (CDF
  - Transaction Log Shipping
- LCR - Local Continuous Replication
  - Same server, different disk/array
- CCR- Cluster Continuous Replication
  - Storage- Shared Cluster Storage SCC –or- Not Shared Cluster MCC or MNS
  - Stretch Cluster MCC/MNS, Longhorn Server*
- In SP1… SCR – Standby Continuous Replication

Anywhere Access Universal Inbox





6:05 PM
5:43 PM
Alvin Mok 4:41 PM
RE: OOF sketches
425-702-1490 (David Fong) 4:04 PM
Exchange Voice Message (17 seconds)
Jason Mayans 3:52 PM
RE: Meeting Request Form concepts revi...
Michael Faoro 3:48 PM
RE: Meeting Request Form concepts revi...
Michael Faoro 3:22 PM
RE: User goals for resource picking

Exchange Voice Message (17 sec
425-702-1490 (David Fong)
Sent: Thursday, November 18, 2004 4:04 PM
To: DJ Schwend

Attachments: voicemail.wav (105 KB)

Audio notes: Typing here in order to take notes while listening to a voicemail message works effectively like a recipient well: the field growing as content is added. When the message is closed or sent, the audio note text is appended to the body.

You have received a voice message.

(Admin-defined message)

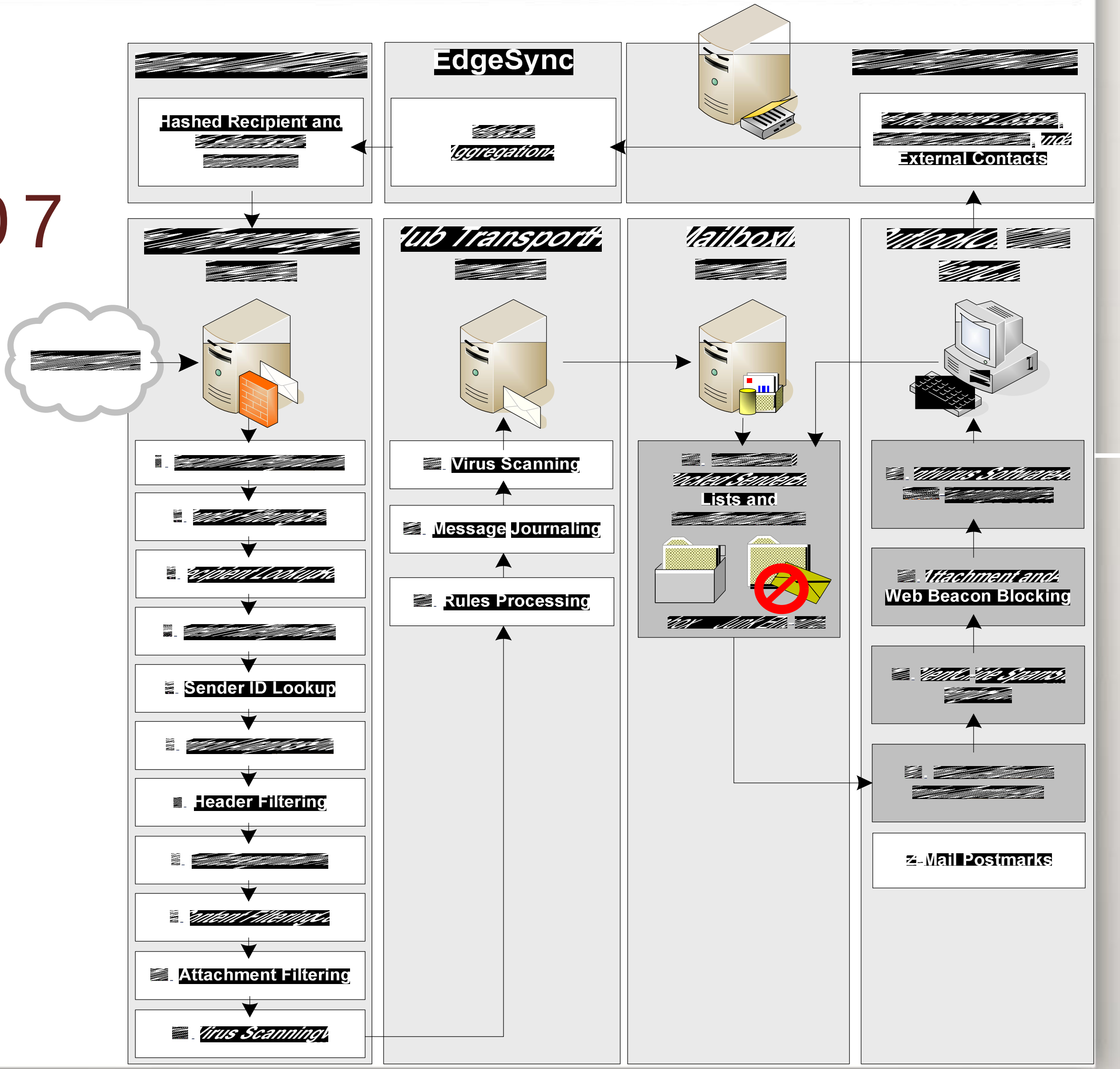
'Play on Phone' action from OWA UI

Special Icons View

Taking Notes On Voicemail

- Unified messaging
  - Email, voicemail and fax to inbox
  - Voice access from regular phone
  - Speech-enabled auto attendant
  - *VoIP to SIP PBX*

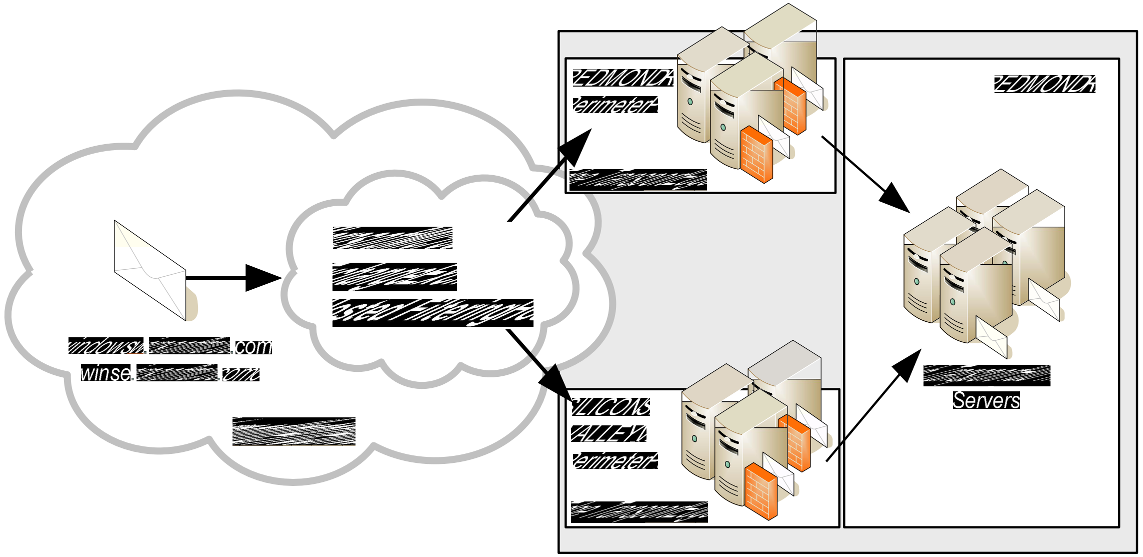
Server 2007 Messaging Protection



?áManaged service with anti-spam, antivirus, policy filtering and disaster recovery

?áMicrosoft IT uses for some subdomains

?áCan also be used for outbound email



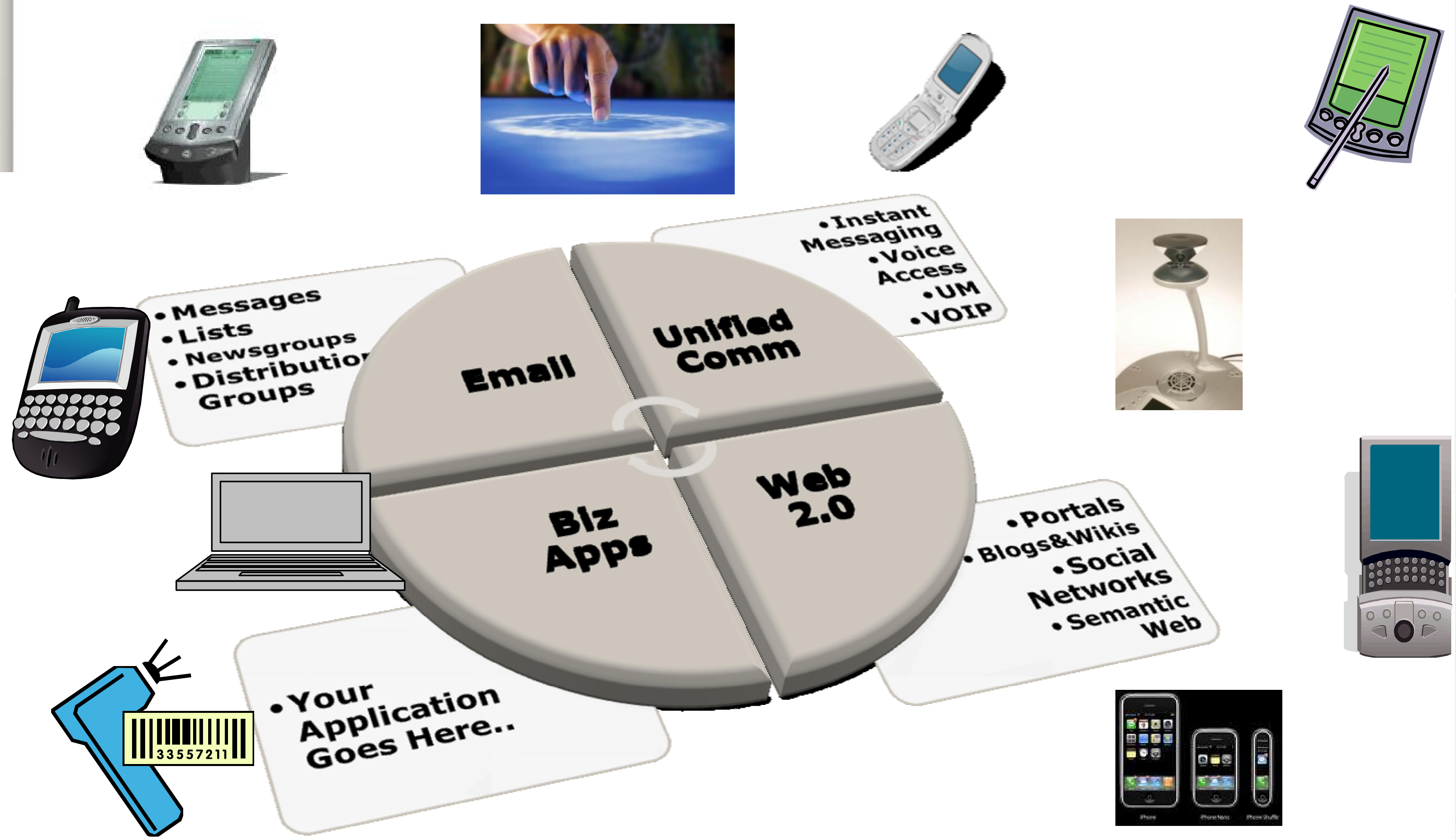
Sybari

- Multiple Scan Engines
  - Microsoft, Norman, CA, AhnLab, Authentium, VirusBuster, Kaspersky, Sophos
- Single Management Platform
  - Updates, Reporting, System Center (MOM) Management Pack, etc.
- ForeFront

Exchange 2007 SP1

- Added security and email protection
  - Military and government security needs
- Introduces new functionality and new scenarios
  - Standby Continuous Replication (SCR)
- Extends functionality and increases accessibility
  - Public folder administration and PF OWA access
- More…
  - S/MIME back in OWA

Not Just Exchange...

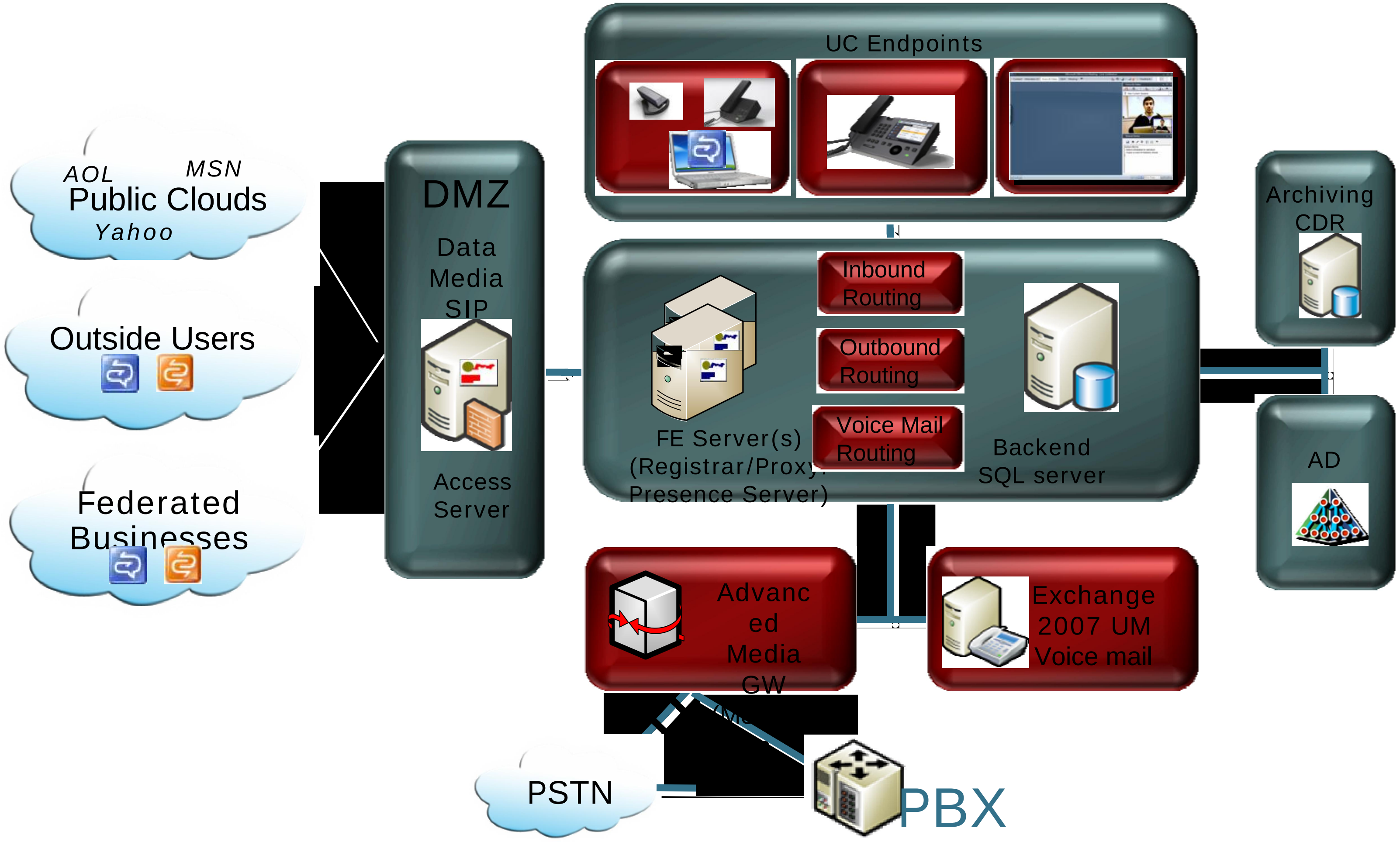


Email
- Messages
- Lists
- Newsgroups
- Distribution Groups

Unified Comm
- Instant Messaging
- Voice Access
- UM
- VOIP

Web 2.0
- Portals
- Blogs&Wikis
- Social Networks
- Semantic Web

Biz Apps
- Your Application Goes Here..



AOL
MSN
Public Clouds
Yahoo

Outside Users

Federated Businesses

DMZ
Data
Media
SIP
Access Server

UC Endpoints

Inbound Routing
Outbound Routing
Voice Mail Routing

FE Server(s)
(Registrar/Proxy/
Presence Server)

Backend SQL server

Archiving CDR

AD

Advanced Media GW

Exchange 2007 UM Voice mail

PSTN

PBX

Questions?

LeeB@ExchangeGuy.com

www.ExchangeGuy.com

Exchange User Group

www.ExchangeServerBoston.com

ExchangeGuy