

4-1-2

Safer EMail

The Key Points

Authenticity of Servers

Encrypted Transport

It's Easy

- Do not use pop, it is in the clear
- Use pop3s, port 995 over TLS/SSL
- Do not use imap, it is in the clear
- Use imaps, port 993 over TLS/SSL
- And they Authenticate the Servers using X.509 Certificates. CHECK IT!

Fetch Using IMAP4S

▼ **randy@psg.com**

- Server Settings
- Copies & Folders
- Composition & Addressing
- Junk Settings
- Synchronization & Storage
- OpenPGP Security
- Return Receipts
- Security

▼ randy@iij.ad.jp

Server Type: IMAP Mail Server

Server Name: Port: Default: 993

User Name:

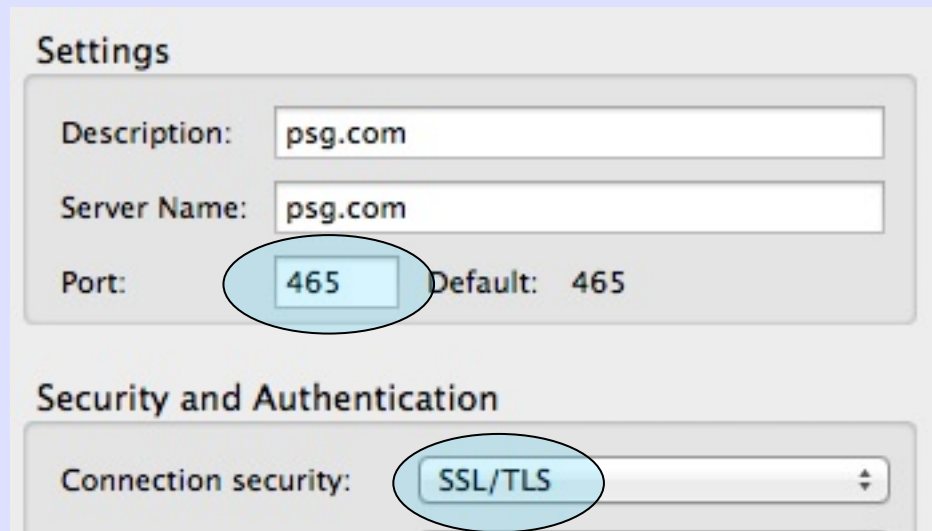
Security Settings

Connection security:

Authentication method:

SMTPS over TLS/SSL

- Do Not Use Unencrypted SMTP/25



The image shows a screenshot of an email client's settings window. The 'Settings' section is expanded, showing fields for 'Description' (psg.com), 'Server Name' (psg.com), and 'Port' (465). The 'Port' field is circled in blue. Below this, the 'Security and Authentication' section is also expanded, showing a 'Connection security' dropdown menu set to 'SSL/TLS', which is also circled in blue. The 'Default' port is listed as 465.

Settings

Description: psg.com

Server Name: psg.com

Port: 465 Default: 465

Security and Authentication

Connection security: SSL/TLS

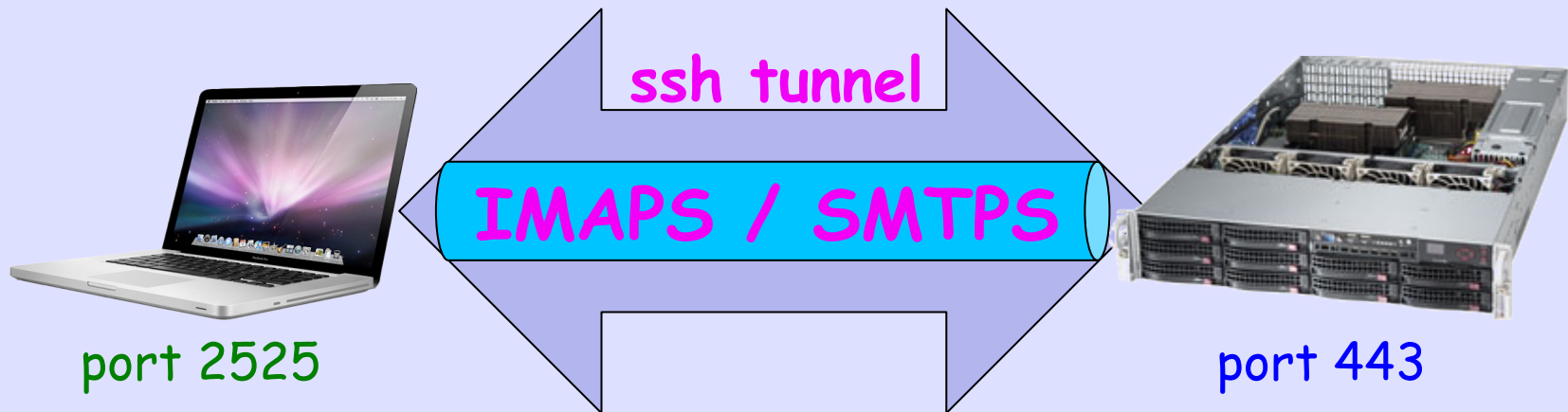
Authenticate Servers

- Assume the Wire is Tapped
- Assume Someone will Spoof Servers
- Know Your Servers' Root Certificates
- Confirm Certificates on Configuration
- Choose Good Passphrases

Encrypt Critical EMail

- Assume the Wire is Tapped
- Use a Personal X.509 PKCS#12 User Certificate with SMIME - T'Bird etc.
- Use a PGP key with Enigma - T'Bird

I Tunnel & Use IMAPS



```
$ ssh -N ssh.psg.com -p 443 -L 2525:127.0.0.1:25
```

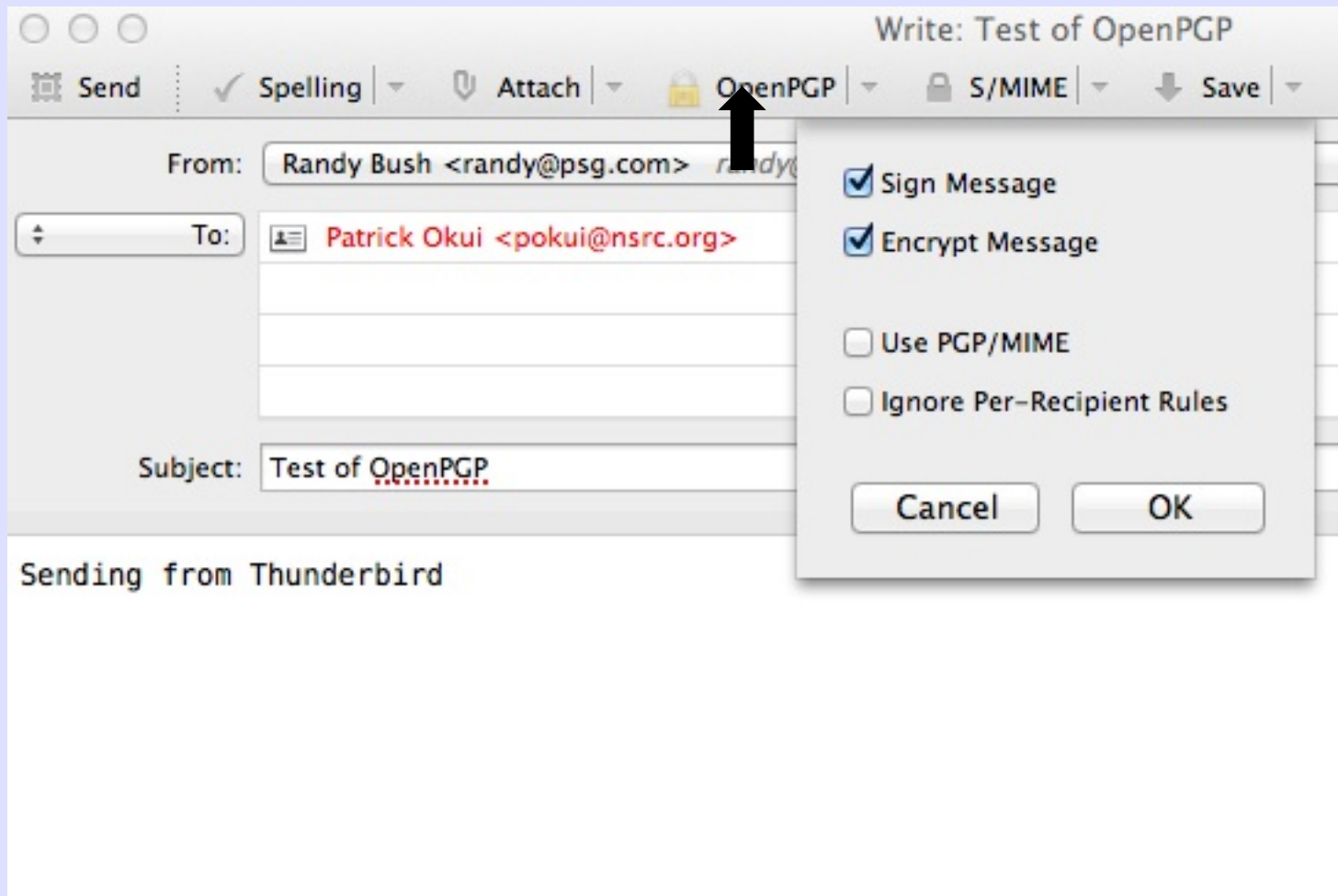
Target
Host

Tunnel
Port

Port on
MacBook

Tunnel
EndPoint

Using PGP



Of Course
All Our Mail Goes To
The NSA, GCHQ,
PLA, ...

Or You Can Give It
To The World's
Largest Spy Agency
Google / GMail