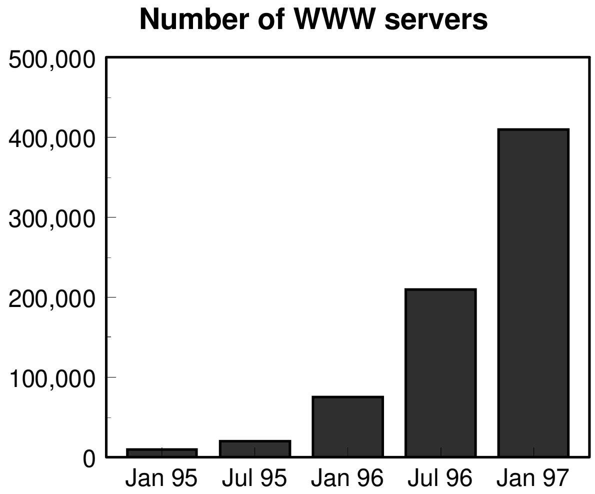
AS/400 Internet Security

Mark McKelvey
IBM Corporation
Rochester, MN

Internet Security Threat

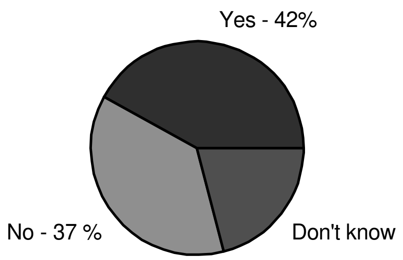


Explosive growth of the Internet

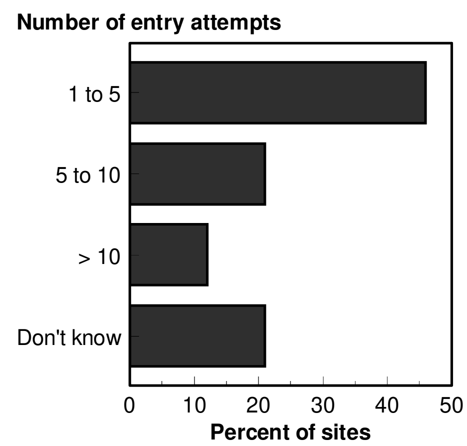
- Driven by world-wide web
- Change from research to commercial usage

Makes the Internet...

- Desirable place to do business
- Attractive place to steal from business



Percent whose computer systems had unauthorized use within the year.

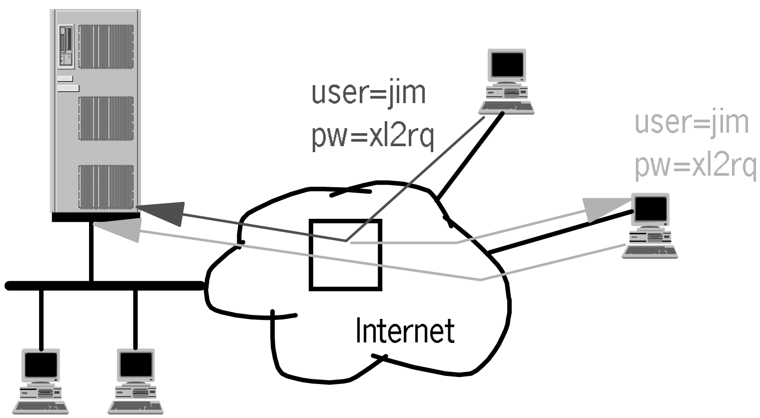


... and not just once.

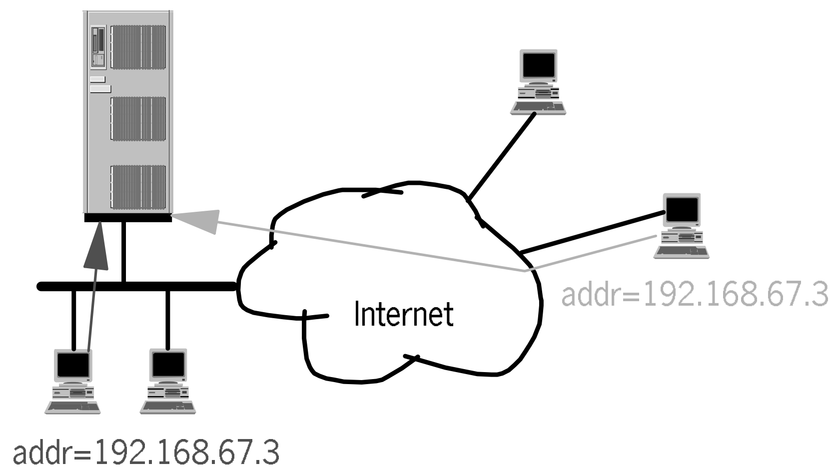
(from Computer Security Institute - May 96)

Example Internet Security Exposures

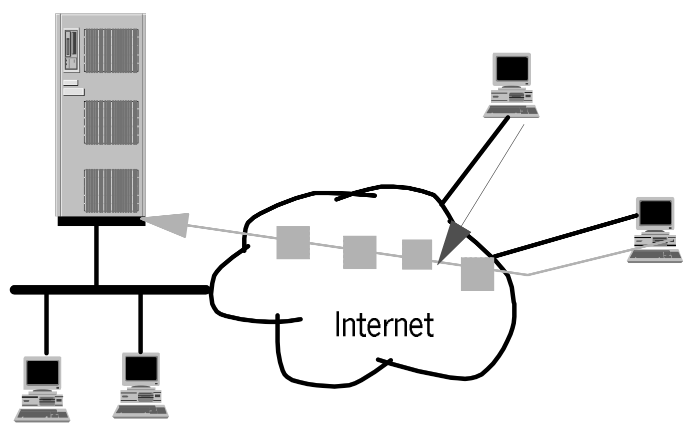
Sniffing



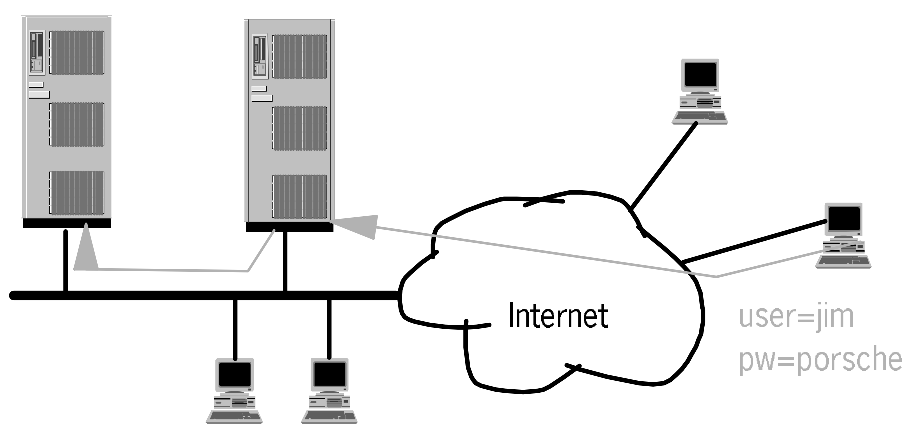
Spoofing



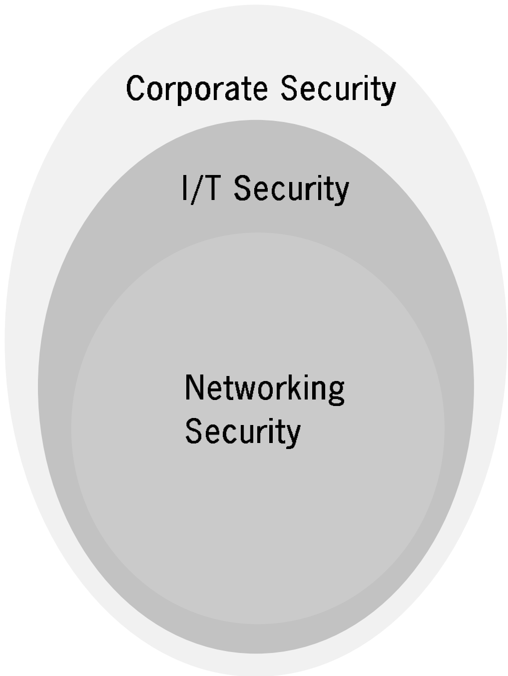
Denial of service



Trusted hosts

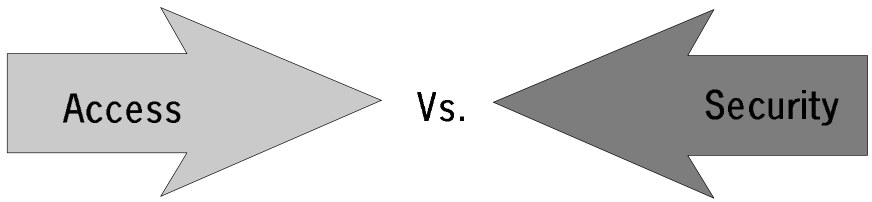


Internet Security Policy



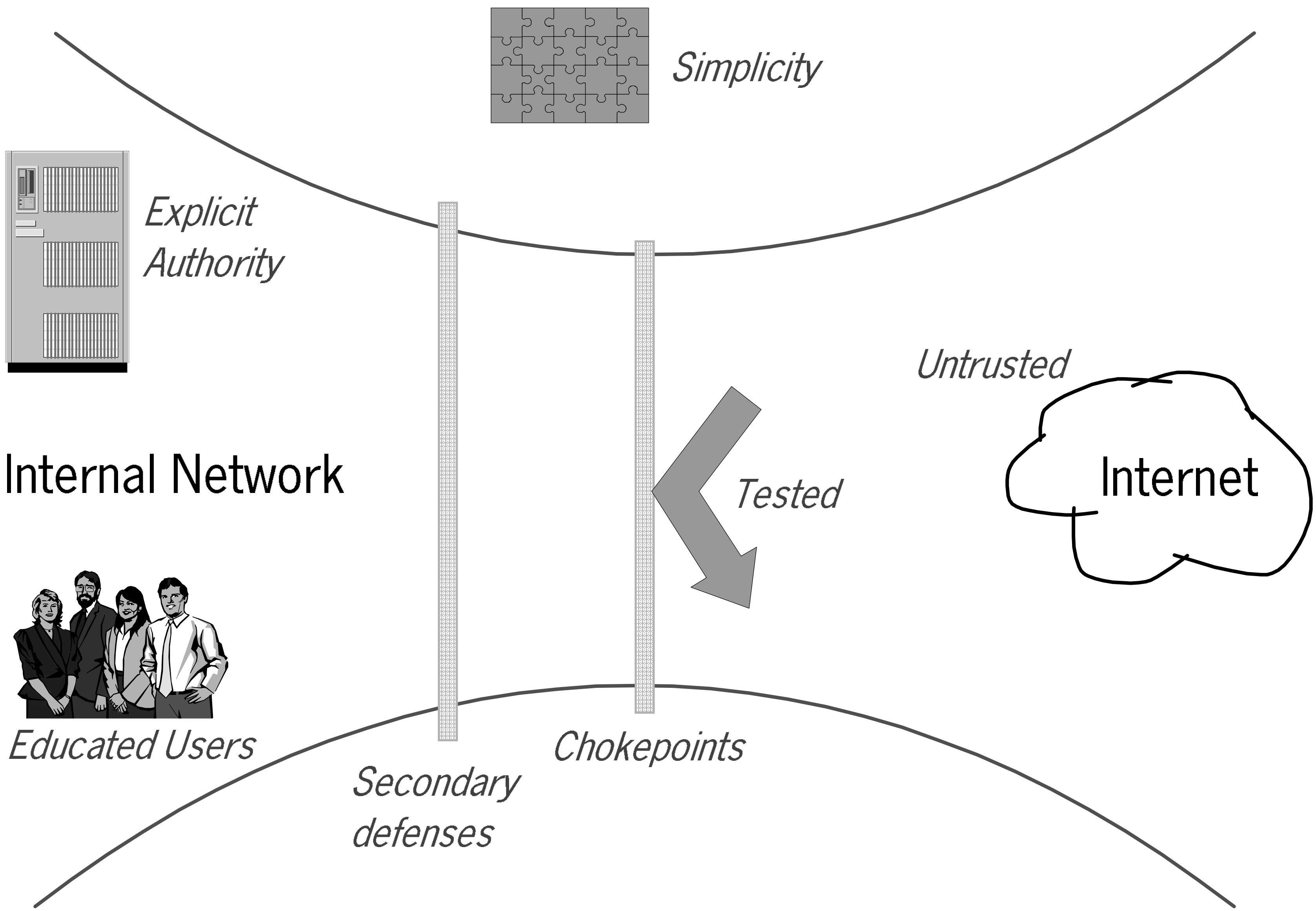
What are your security policies?

- What services are to be permitted (http, ftp, telnet...)?
- What Internet sites may be accessed?
- What may be accessed from the Internet?



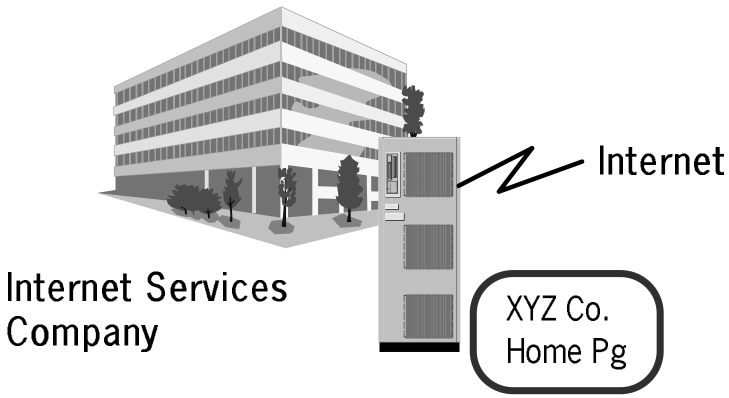
- FTP access<-> PC virus introduction
- Mail exchange<-> mail flooding
- Web server <-> web graffiti

Internet Security Principles

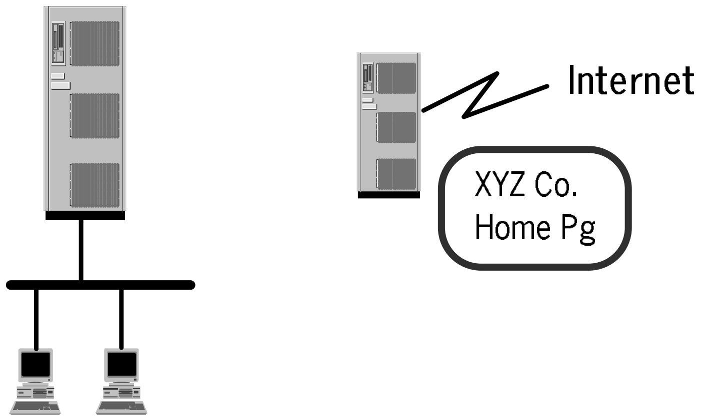


Connecting to the Internet

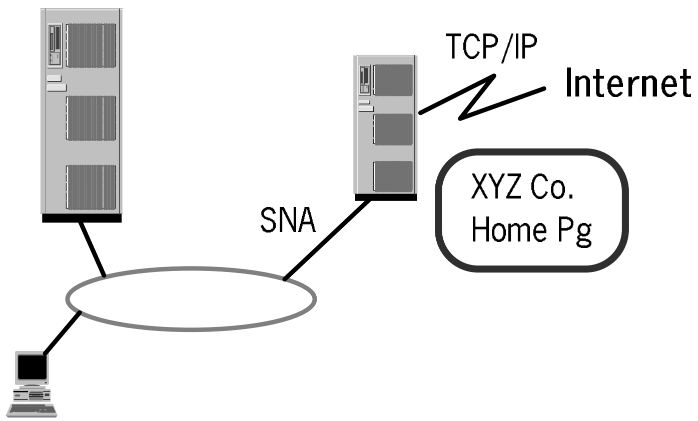
Hosting Services



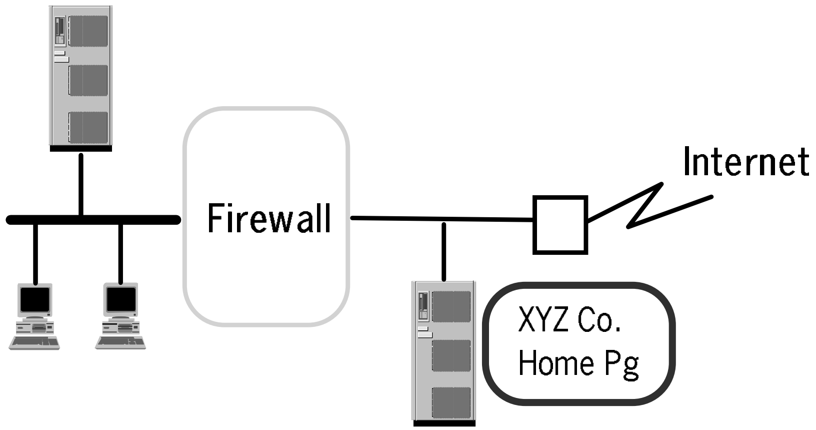
Isolated System



Partitioning by Protocol



Firewall

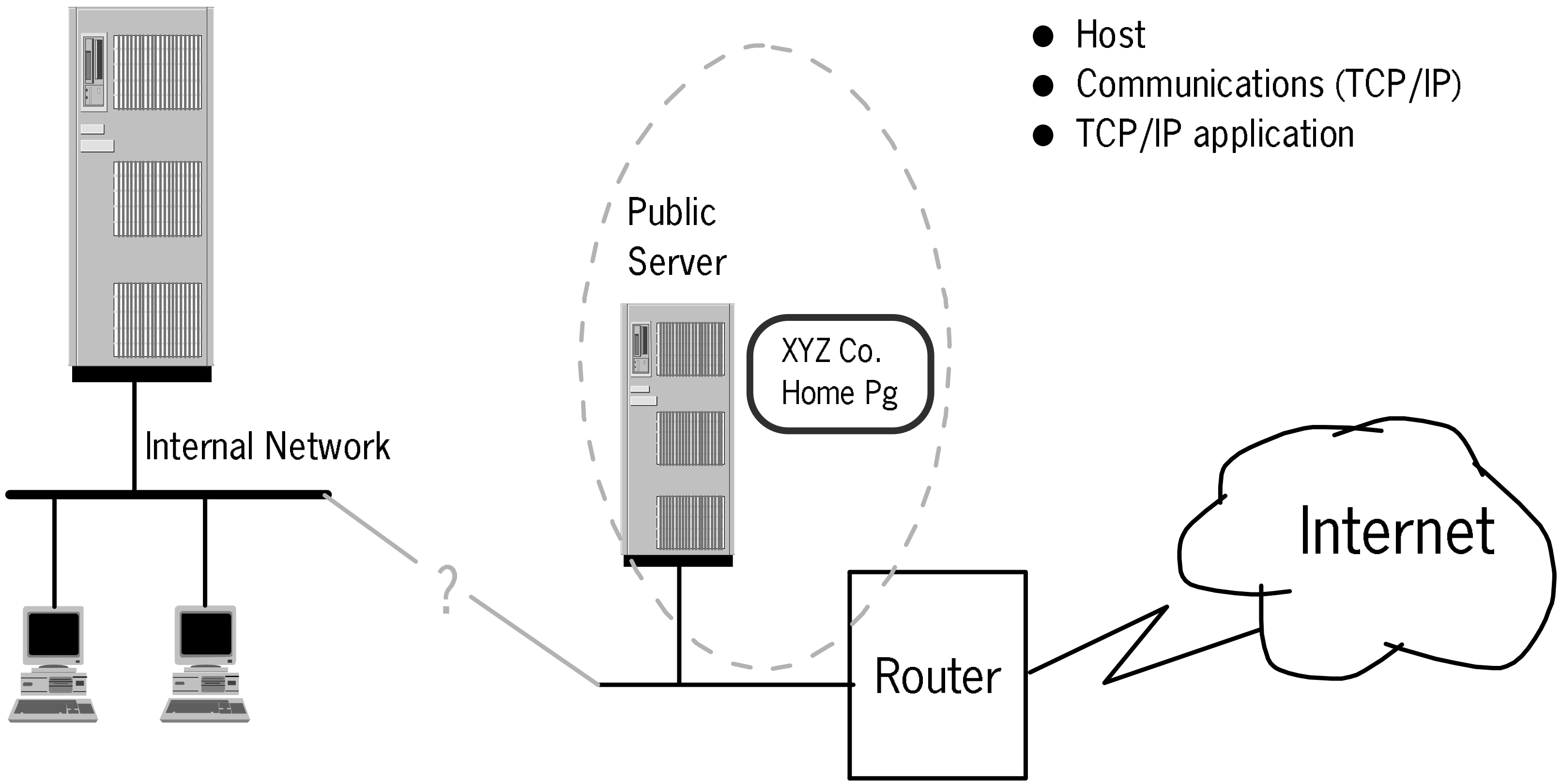


Protecting a Public Server

Public server must be secured even if it is isolated or if you have a firewall.

Layers of security

- Internet Service Provider
- Host
- Communications (TCP/IP)
- TCP/IP application

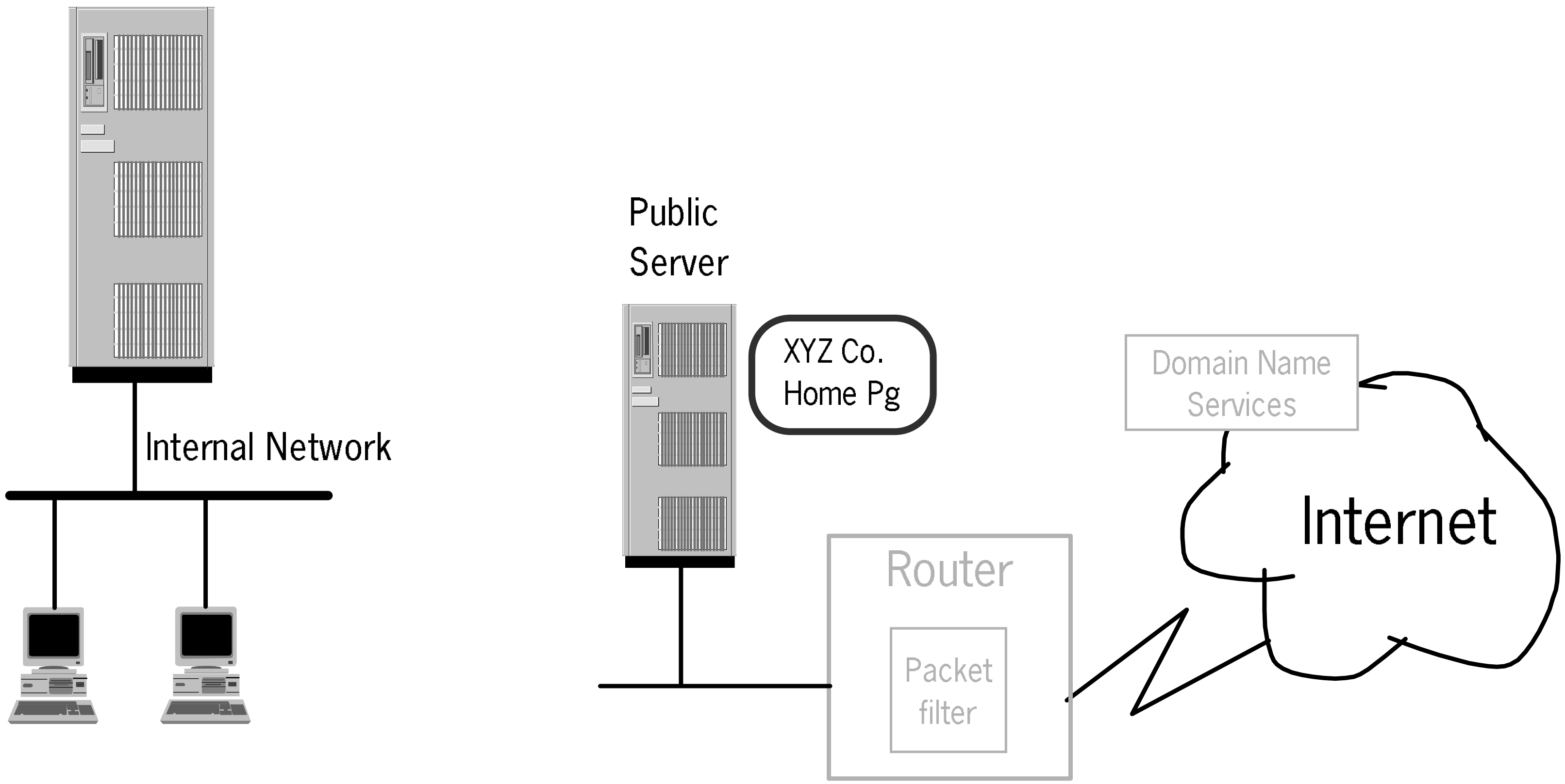


Internet Service Provider Security

Block incoming telnet connections

Block finger, snmp, ...

Provide Domain Name Services



AS/400 Host Security

Enable Resource Security

- QSECURITY >= 40

Password attack prevention

- QPWDMINLEN = 6 ...
- QMAXSGN = 3
- QMAXSGNACT = 3
- QAUTOVRT = 0

Tightly control "high-powered" profiles

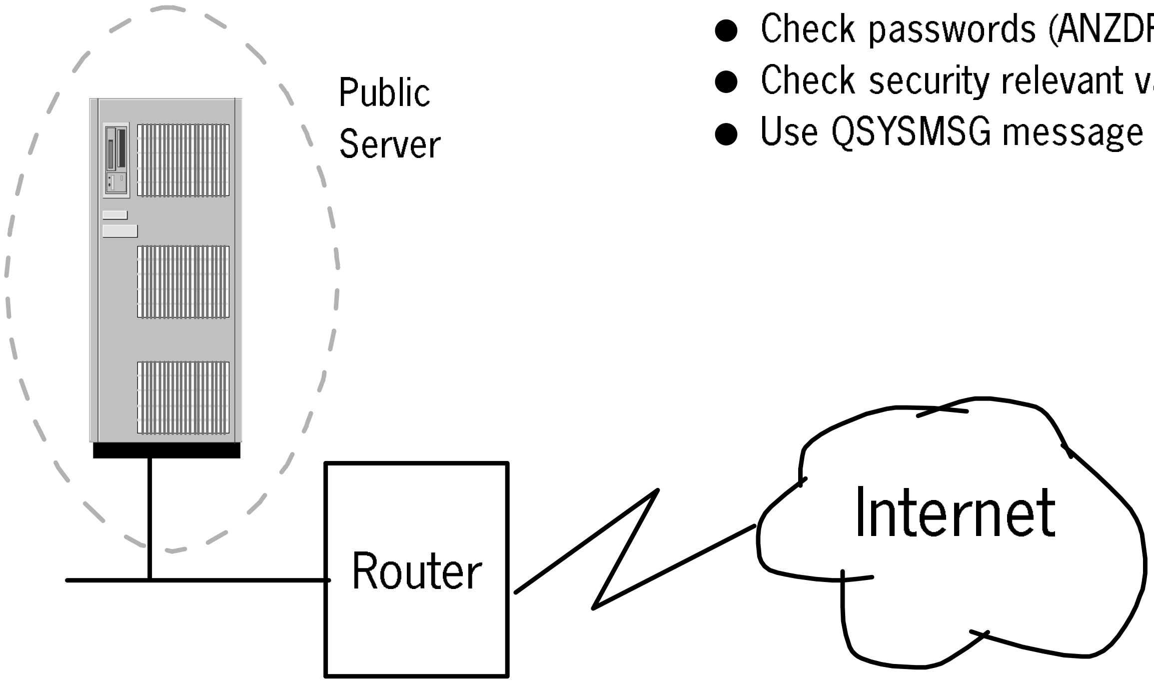
- QLMTSECOFR = 1
- Limit profiles with *ALLOBJ, *SECADM an *IOSYSCFG

Use Object Security

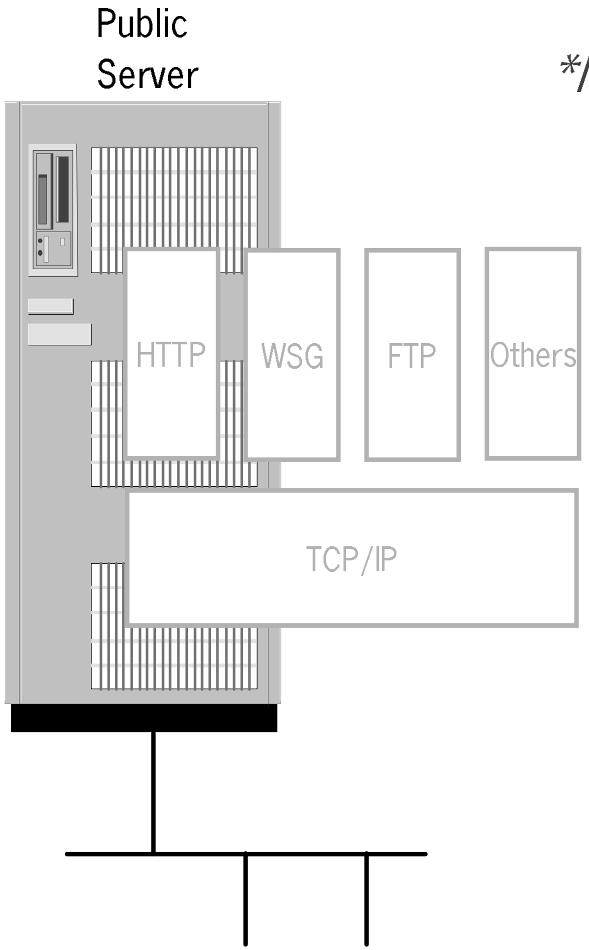
- The libraries you create should be PUBLIC(*EXCLUDE)

Verify and Monitor

- GO SECTOOLS or GO SECBATCH
- Check passwords (ANZDFTPWD)
- Check security relevant values (PRTSYSSEC)
- Use QSYSMSG message queue



TCP/IP Security



**IOSYSCFG authority controls who can make changes*

Only start TCP/IP applications you need

- CHGCMDDFT CMD(STRTCPSVR) NEWDFT('SERVER(*HTTP)')
- CHGTELNA AUTOSTART(*NO)
- CHGWSGA AUTOSTART(*NO)...

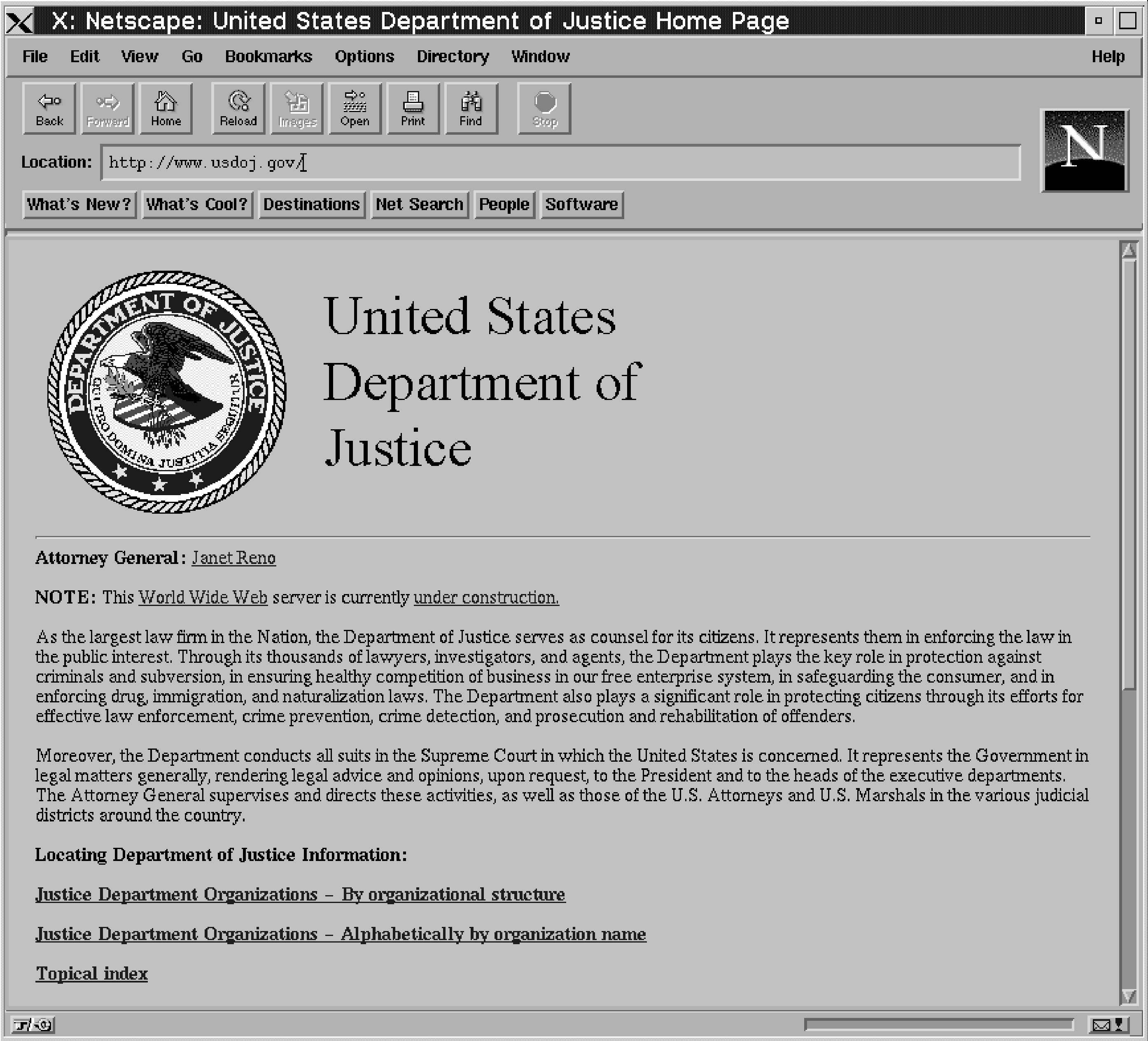
No IP forwarding

- CHGTCPA IPDTAGFWG(*NO)

Don't define host name of internal systems

Define only one route (default)

An HTTP Server Victim



Internet Connection Server (HTTP)

Server directives control which directories can be accessed

http://yourserver.com/App1/Main.htm

http://yourserver.com/App1/Pgm/UPDATE

requests from the Internet

```
Exec /App1/Pgm/*  /QSYS.LIB/APP1.LIB/*
Pass /App1/*      /www/html/App1/*
DirAccess   OFF
```

Libraries (QSYS.LIB)

APP1

QGPL

WEBTOOLS

Directories

/www

/html

/App1

/App2

- PASS controls which files can be accessed
- Use MAP and PASS to provide an alias for file locations
- EXEC controls which cgi-bin programs can be run
- Don't mix cgi-bin programs with other programs
- Don't put any sensitive data in directories accessible by URLs
- Don't allow directories to be viewed

Internet Connection Server (HTTP)

Server PROTECTION directives control who can access data

Example Security Models

Application #1 - public application

- No userid or password required
- Programs and data are accessed using a default profile (e.g. QTMHHTTP)

Application #2 - employees only

- AS/400 user profile and password required (basic authentication)
- Programs and data are accessed using the user profile

Application #3 - limited set of Internet users only

- "Internet userid" and password required (basic authentication)
- Userid are entries in a Validation List object
- Programs and data are accessed using a default profile (e.g. WEBAPP3)

Normal AS/400 object level security "backs up" the server directives

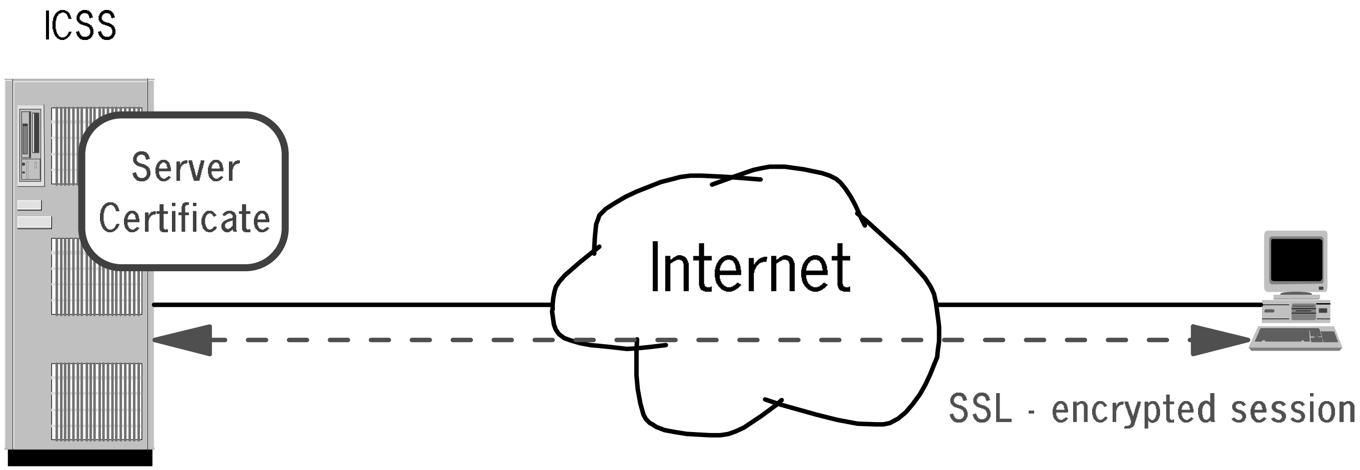
Internet Connection Secure Server

Securing the public server is not enough

- Internet users want secure communications (e.g. passwords)
- Internet users want secure transactions (e.g. credit card numbers)

Internet Connection Secure Server

- Provides encryption support for HTTP
- Secure Sockets Layer (SSL)
- Certificate identifies the server to the browser
- US/Canada and International versions



CGI-BIN Considerations

Validate form input - HTML can be changed

```
<p>Pick the flavor to order:
<form method="POST" action="update">
<select name="flavor">
<option>grape
<option>orange
<option>cherry
</select>
<input type="submit" value=OK">
</form>
```

What got sent →

← What came back

```
<form method="POST"
 action="http://yourserver.com/cgi-bin/update">
<select name="flavor">
<option selected>apple
</select>
<input type="submit" value=OK">
</form>
```

Hidden variables aren't really hidden

```
<form method="POST" action="/cgi-bin/query">
<input type="hidden" name=employeenum value="12345 ">
<input type="submit" value="Query current salary">
</form>
```

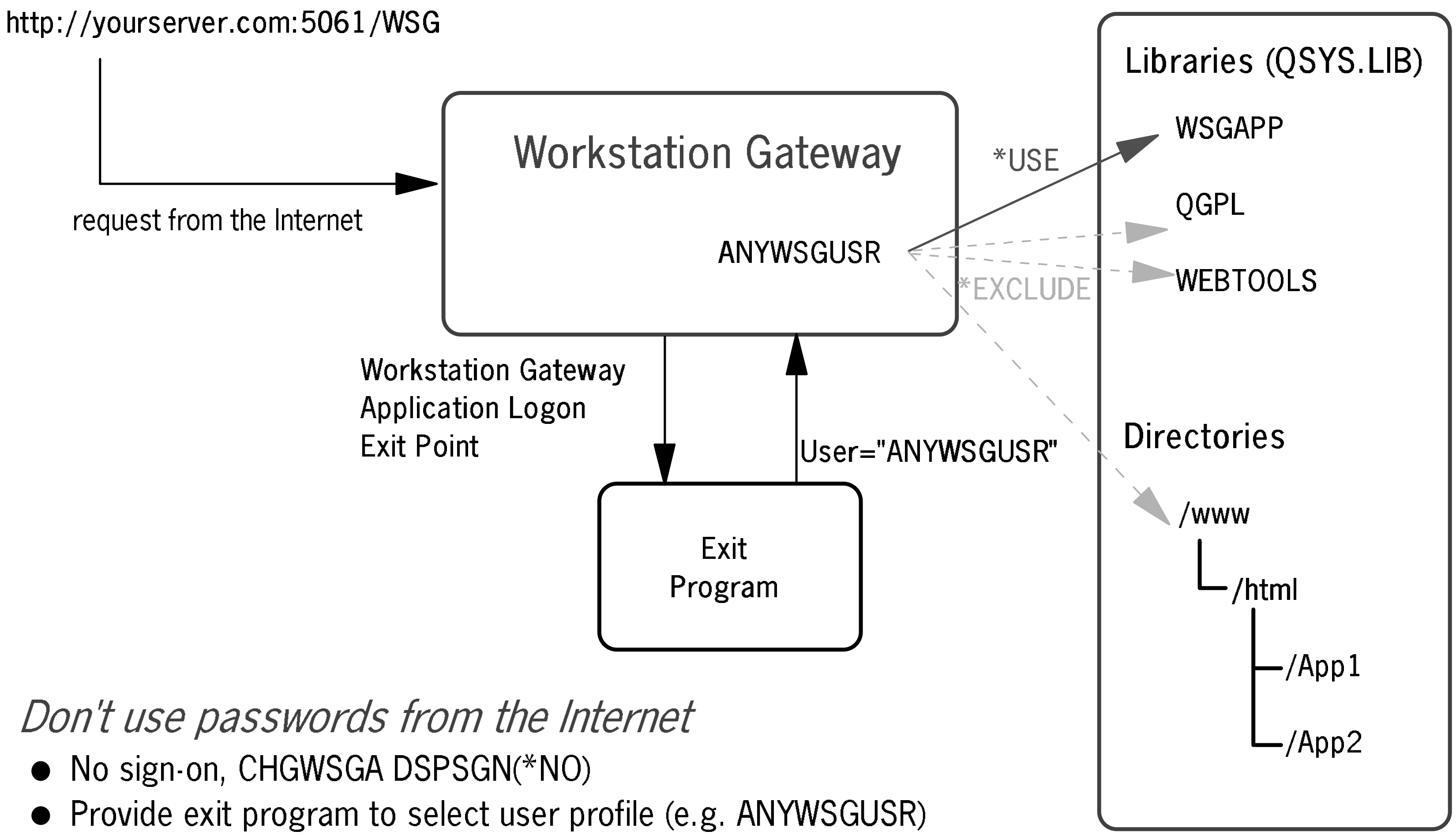
What got sent →

← What came back

```
<form ...
... value="09876 ">
...
</form>
```

Javascript field auditing can be disabled

Workstation Gateway

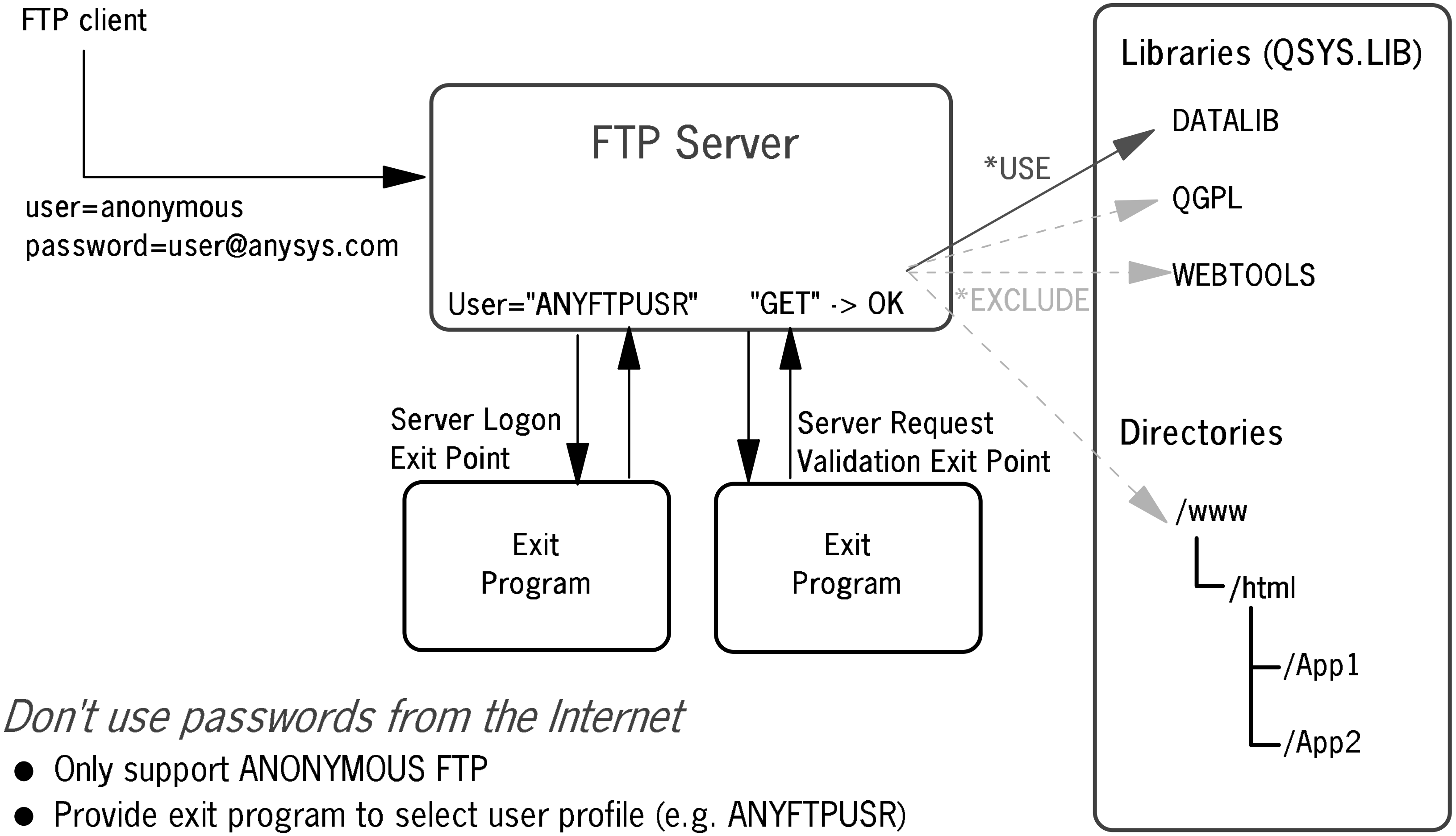


Don't use passwords from the Internet

- No sign-on, CHGWSGA DSPSGN(*NO)
- Provide exit program to select user profile (e.g. ANYWSGUSR)
- Strictly limit access of Workstation Gateway user
- Don't check client's IP address

Other vendors have similar products that are SSL-enabled

FTP



Don't use passwords from the Internet

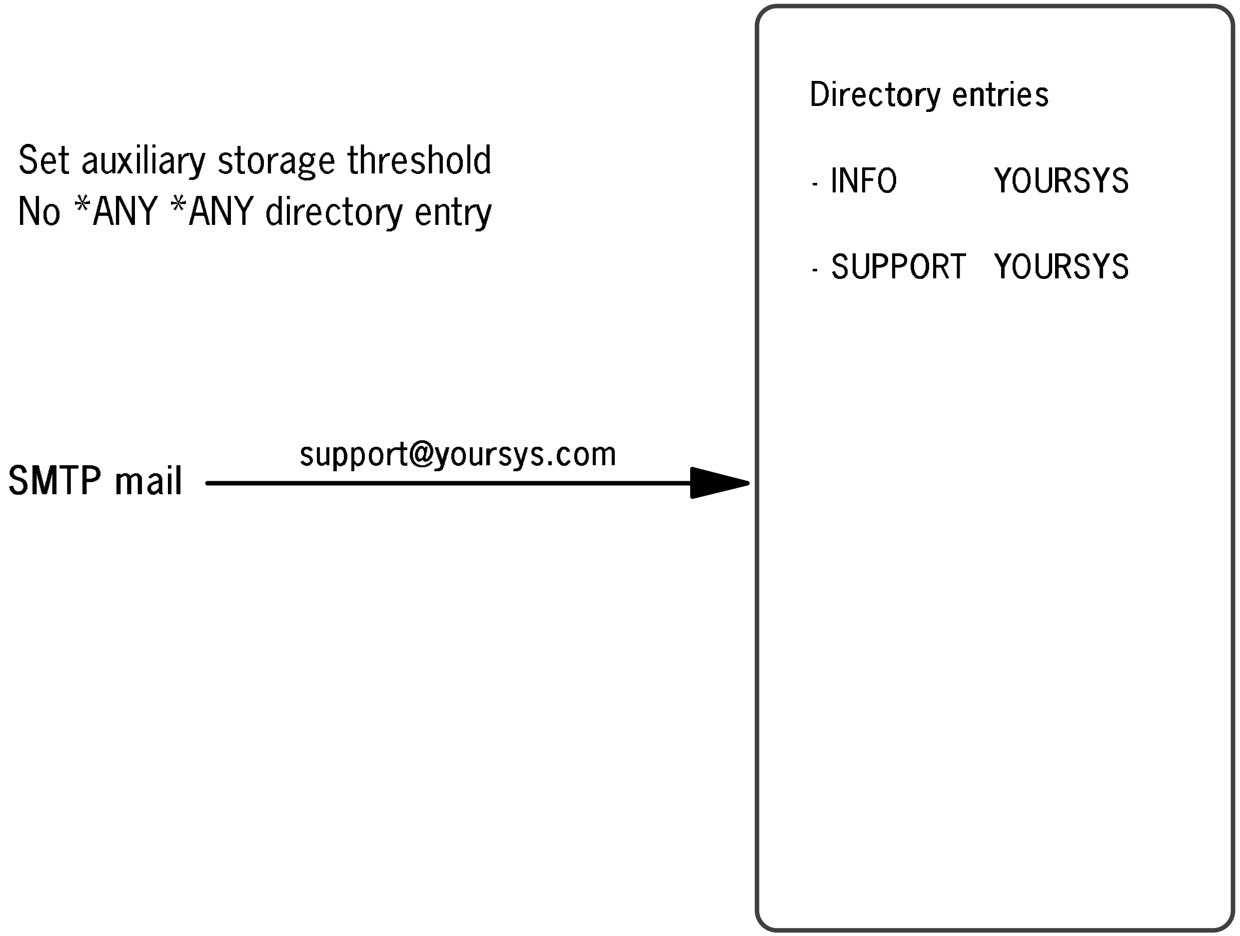
- Only support ANONYMOUS FTP
- Provide exit program to select user profile (e.g. ANYFTPUSR)
- Provide exit program to determine allowed operations (e.g. GET only)
- Strictly limit access of FTP user
- Don't check client's IP address

Mail

A public server should have limited or no mail support

- Don't want to store mail on system accessible by the public
- Not for general mail delivery

- Set auxiliary storage threshold
- No *ANY *ANY directory entry



Other TCP/IP Applications

When the AS/400 system is accessible from the Internet

Telnet

- Don't start it! But if you must...
- Set QLMTSECOFR, QMAXSIGN, QMAXSGNACT, QAUTOVRT
- Set maximum storage per user profile

SNMP

- Don't start it! But if you must...
- Set community name (like a password)
- Only allow GETs

LPD

- Don't start it!

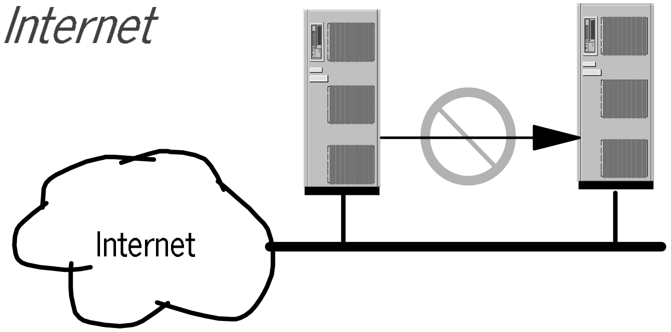
TCP/IP File Server

- Don't install it!

Preventing Hacker Written Applications

When the AS/400 system is accessible from the Internet

- Don't allow trojan-horse applications to be installed
- Don't allow your system to be used to attack others



- Don't install compilers
- Restrict usage of TCP/IP communications

TCP/IP port restrictions can limit usage of well known ports (ADDTCPPORT)

Lower port	Upper port	Protocol	User profile (deny/permit)
23 (telnet)	*only	*tcp	QUSER/--
20 (ftp)	21	*tcp	QUSER/QTCP
25 (smtp)	*only	*tcp	QUSER/--
80 (http)	*only	*tcp	QUSER/QTMHHTTP
5061 (wsg)	*only	*tcp	QUSER/QTMTWSG
161 (snmp)	*only	*tcp	QUSER/--
161 (snmp)	*only	*udp	QUSER/--

Restrict use of sockets APIs

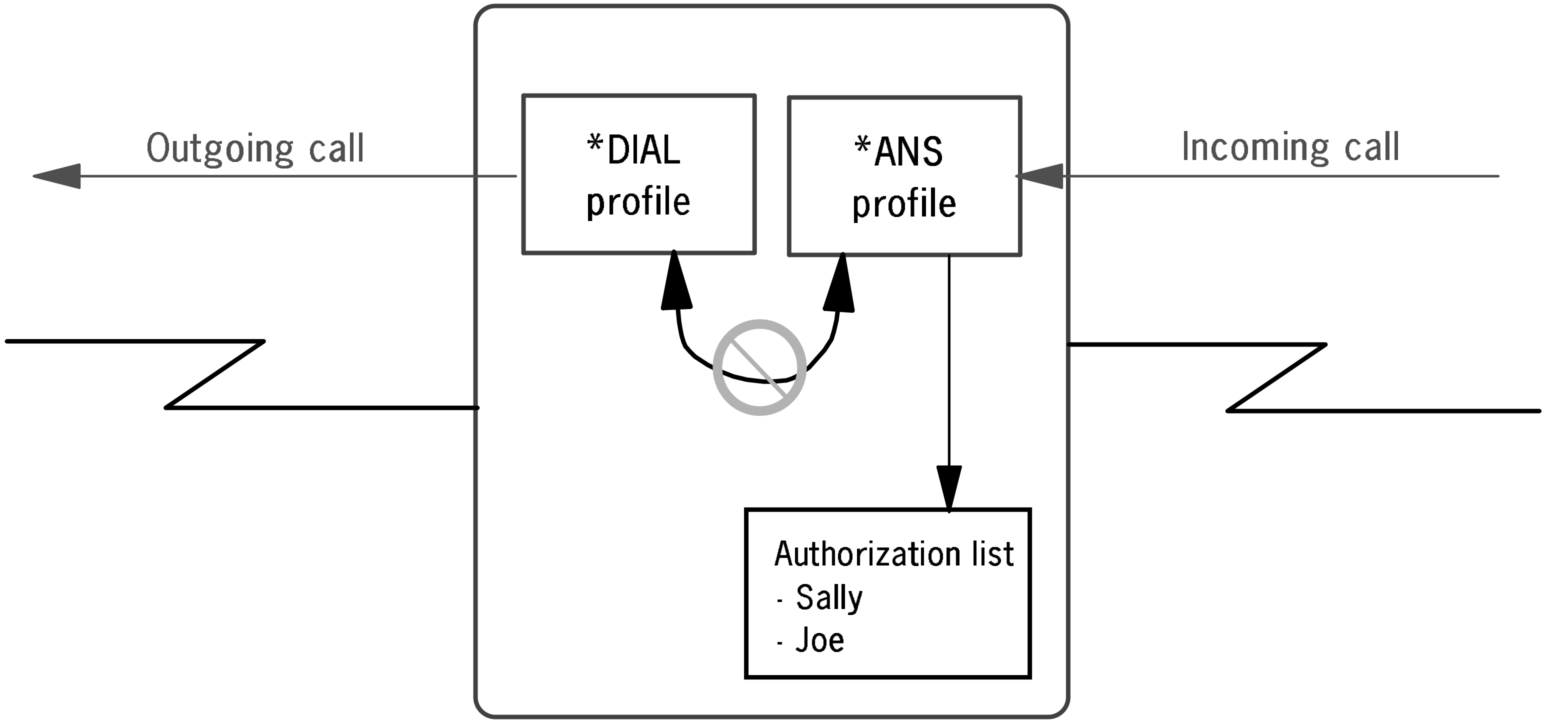
- Service programs QSOSRV1 and QSOSRV2 --> PUBLIC(*EXCLUDE)
- Authorize specific profiles to the service programs (QTCP, QTMHHTTP...)

Serial Link IP (SLIP)

SLIP provides dial-up connections which could be a "back door"

- Don't allow your system to be used to attack others

- Avoid having SLIP configuration profiles for both *ANS and *DIAL
- Disallow IP forwarding via SLIP configuration profiles
- Create special user profile to authenticate incoming connections
- Create authorization list to control who can use SLIP configuration profile



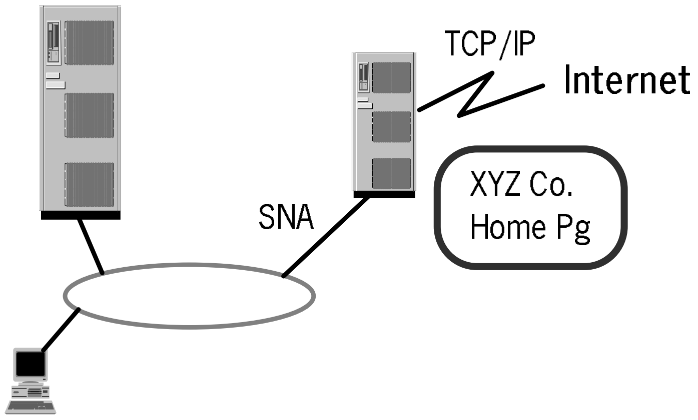
Connecting to the Internal Network

Securing the public server is not enough

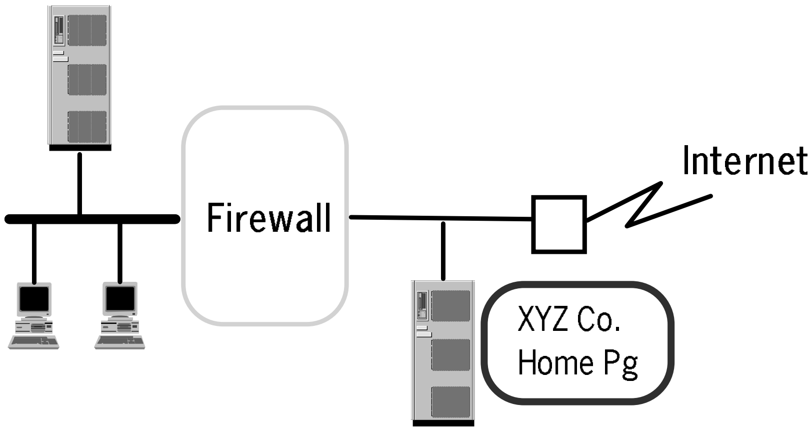
- Users want to send mail over the Internet
- Users want to use web browsers to access Internet web sites
- Up-to-the-minute data required on the web server

Access to the internal network must be protected

Partitioning by Protocol



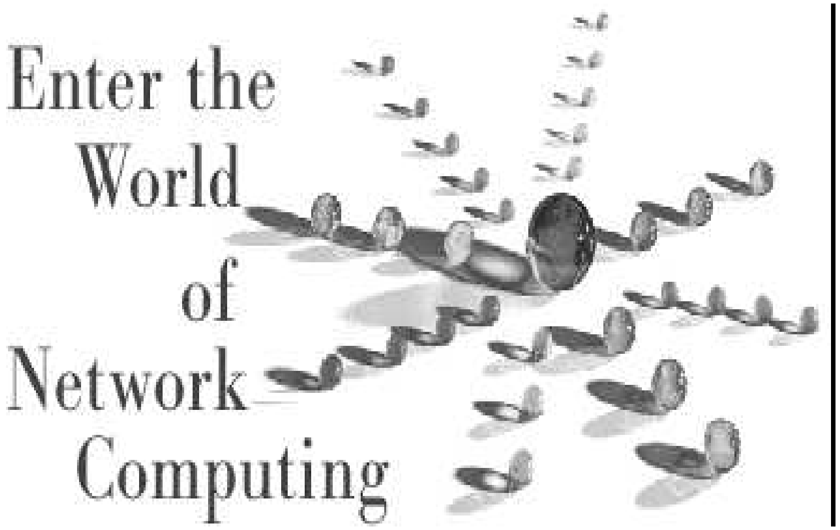
Firewall



AS/400 Internet Security Summary

AS/400 security features make it a good Internet Server

- Proven operating system integrity
- Excellent host level security
- Integrated communications security



Trademarks

AS/400, IBM, and OS/400 are trademarks of the IBM Corporation in the United States or other countries or both.

Other company, product, and service names may be trademarks or service marks of others.

Resources

IBM SecureWay, AS/400 and the Internet, G325-6321

Tips and Tools for Securing Your AS/400, SC41-3300

http://www.ibm.com/Security