

# Firewall Overview and D-I-Y

e3sciences

## – Agenda

---

- Perspective
- Firewall functions
- Sample configurations
- Doing-it-yourself ( within reason )
  - A way of gaining experience and knowledge
  - We are not suggesting a cheap way out !
  - All the usual disclaimers apply
    - We take no responsibility anytime, anywhere for anything or the actions of any individual!

## – Perspective

---

- 7 out of 10 Attacks on systems are from within \*
  - Physical security has limited affect
    - Already has access to buildings etc.
  - Opportunity exists
    - What else is there to do between 9am and 5pm ?
  - Attacker already has pre-requisite knowledge
    - You trained them!
  - Or is this statistic a result of effective Firewall use?

\*1998 Computer Security Institute

## – Perspective

---

- Computer Software and networks are insecure - accept it !
  - Software vendors have limited liability licenses
    - Just click the “I Agree” part of installations
    - No business need for them to focus on security
    - Have a history of only resolving problems that disclosed
  - New vulnerability in software reported daily
    - Buffer overruns ( will we ever fix these ? )
  - Software is becoming more and more complex
    - Trend for problems will continue

## – Perspective

---

- Is the Internet the only place you risk attack from? What about :
  - Business Partners
    - Attack can come via a partners network ( across their Internet connection )
    - Do you know how secure partner networks are ?
  - Dial-in modems
    - Vendor support
      - Devices are often network connected
      - Often have unmonitored access
    - User machine + modem = uncontrolled external router ?

## – Perspective

---

- Is the Internet the only place you risk attack from? What about :
  - Home users on VPNs
    - A little corporate island at home - trusted
      - Goes directly through Firewall
    - Lacks Physical Security
    - Possibly a soft target
      - This is an island without the protection of a firewall
      - Consider Personal Firewalls
  - Your own organisation
    - No separation between sections of business
    - Use Firewalls between business units ?

## – Perspective

---

- If I install a Firewall I don't need to worry any more ?
  - Policy must be set appropriately
  - Monitor for attack
    - Consider Intrusion detection
    - Audit systems e.g. Virus Checkers, COPS, SATAN ( SAINT )
  - Plan to be attacked
    - Devise action plan in advance

## – Perspective

---

- Some of the most successful hacks used “Social Engineering” attacks
  - Phone the user and ask for the password
  - Phone the Help Desk and ask for password reset
  - Phone the network department and ask for dial-in numbers

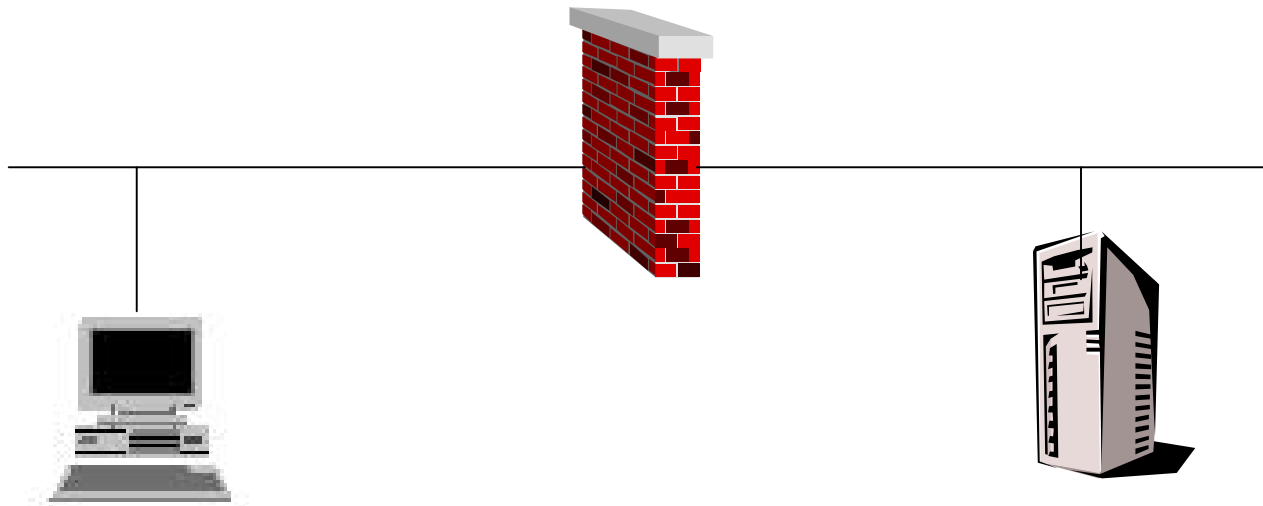
## – Firewall Functions

---

- What is a Firewall ?

“A Firewall is a system or group of systems that enforces access control policy between networks”

Firewall FAQ



## – Firewall Components

---

- Packet Filtering
- Application Proxy
- Network Address Translation ( NAT )

## – Firewall Components

---

- Packet Filtering
  - Block or Pass packets based on
    - Destination or origin address
    - Protocol ( UDP/TCP )
    - Port number e.g. 25 = SMTP, 21 = FTP, 23 = Telnet
  - Stateful Inspection - Allow packets to pass based on application traffic
    - Contents of previous packets e.g. FTP relies on remotely initiated data connection from remote host
    - A feature of commercial products only

## – Firewall Components

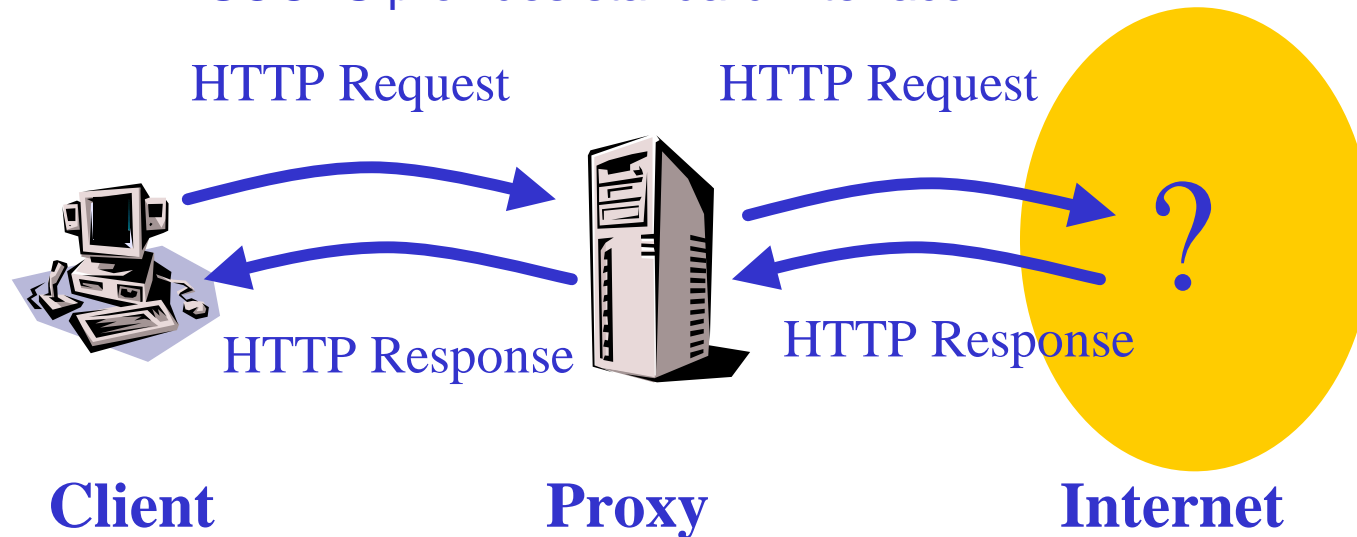
---

- Application Proxy
  - Proxy connects user to application using two connections - ensures there is no direct connection between networks
    - Disguises origin of connection
    - A control point between applications
      - Audit & Access control enforced
    - Locally cache results to improve response
    - Can be used to overcome routing issues
      - Non Internet addresses can use a proxy to access internet ( 10.\* 172.16.0.0-172.31.255.255 & 192.168.\* see RFC 1918 )

## – Firewall Components

---

- Application Proxy
  - Application needs to support proxy - many dont
    - Directly access proxy e.g. Web Browser
    - Replacing operating systems TCP/IP library to call proxy
      - Microsoft Proxy server replaces WinSock.dll
      - SOCKS provides standard interface



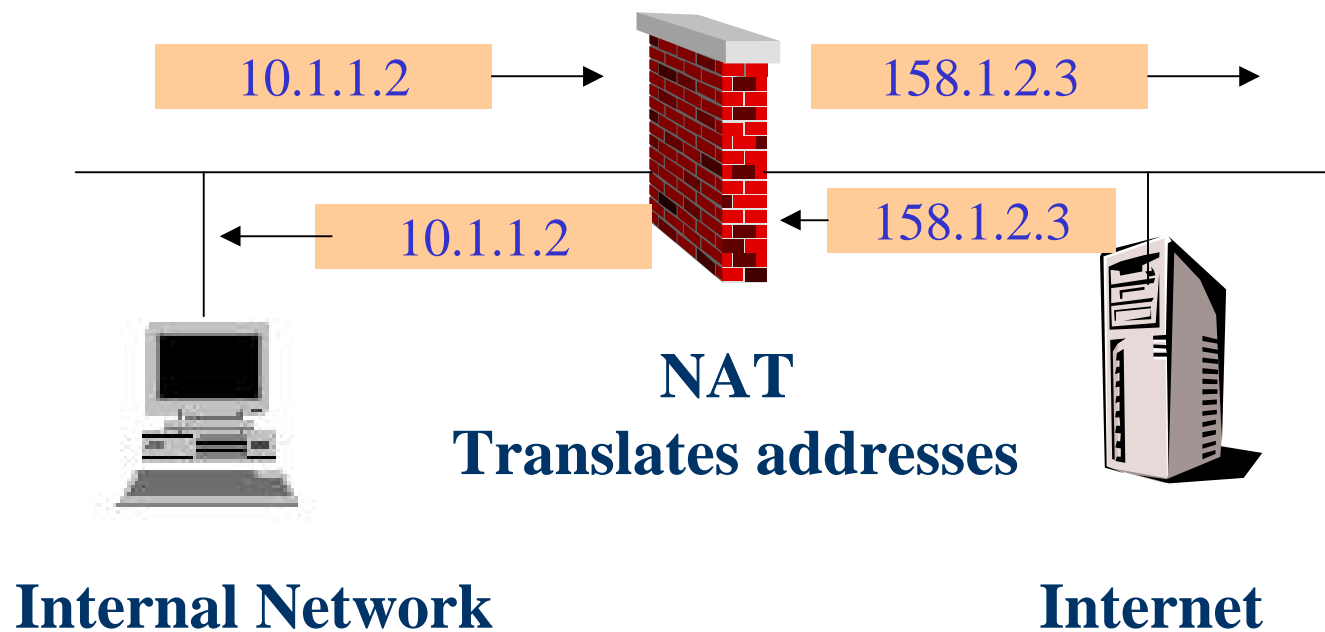
## – Firewall Components

---

- Network Address Translation
  - User accessing external network is given a translated address
    - Disguise internal network structure
    - Make users anonymous
  - Can be used to overcome routing issues
    - Gives direct access to non-routable addresses

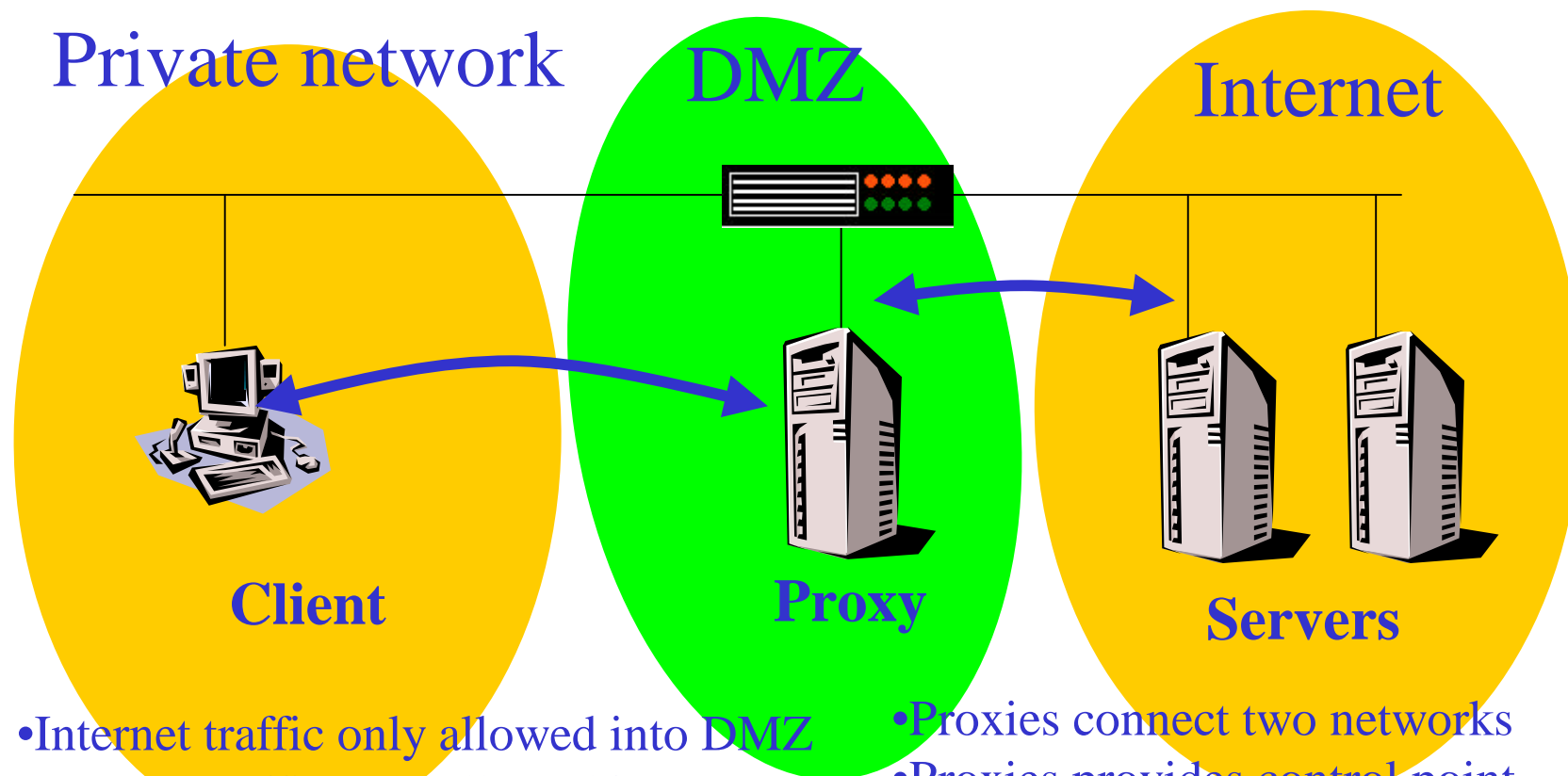
## – Firewall Components

- Network Address Translation Example



# Sample Configurations

## Screened Subnet

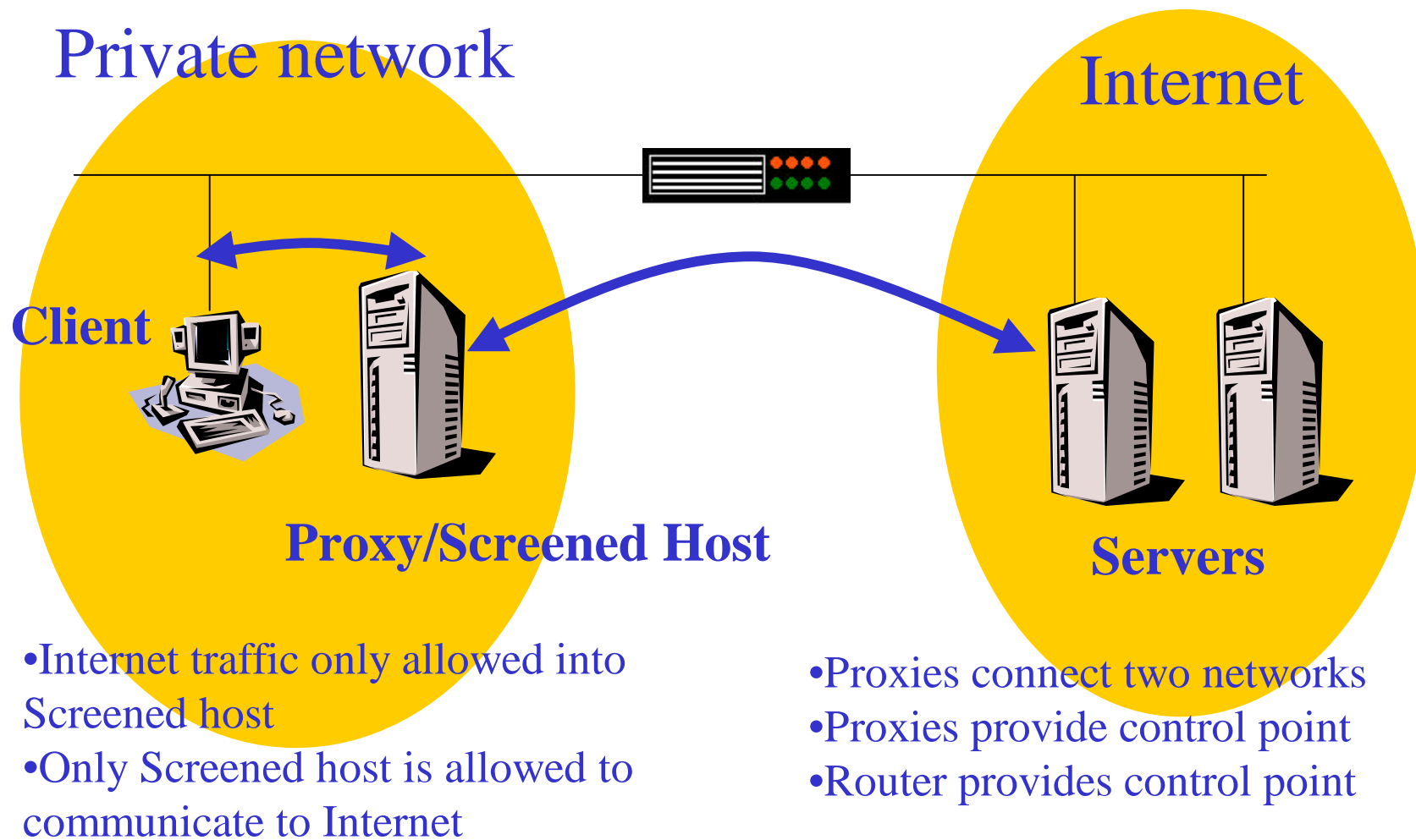


- Internet traffic only allowed into DMZ
- Internal traffic only allowed into DMZ
- No traffic can pass directly through DMZ

- Proxies connect two networks
- Proxies provides control point
- Router provides control point

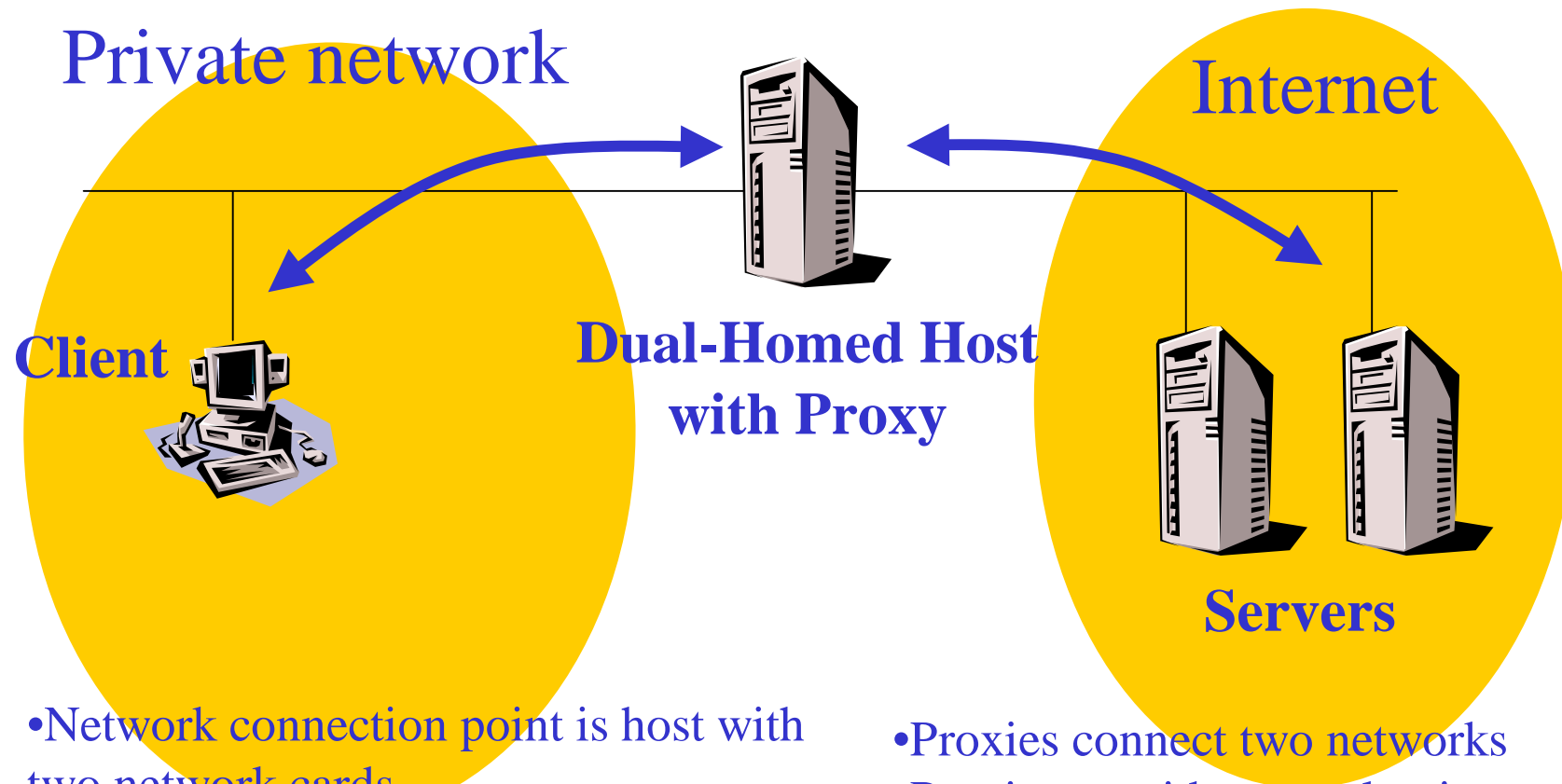
# Sample Configurations

## Screened Host



# Sample Configurations

## Dual Homed Host



- Network connection point is host with two network cards
- IP Forwarding is disabled through Dual-Homed host

- Proxies connect two networks
- Proxies provide control point

## – Do-It-Yourself

---

- Build a Firewall system ( Bastion Host ):
  - Remove unnecessary software
  - Disable or limit remote logon
  - Disable/configure IP forwarding
  - Install Application proxies
  - Disable autoboot ( e.g. Floppy-Disk Boot )
  - Make file systems read-only
  - See LINUX Firewall Building FAQ:  
<http://www.linuxdoc.org/HOWTO/Firewall-HOWTO.html>

## – Do-It-Yourself

---

- Firewalls - sources

- TIS Firewall Toolkit

- <ftp://ftp.tis.com/pub/firewalls>

- SMAP - Execute SMTP under non-root user
      - NetACL - protect access to inetd services
      - Ftp-GW - FTP Proxy
      - Plug-GW - generic proxy

- Mason - Linux firewall config tool

- <http://mason.stearns.org/>

- Network Address Translation - Linux

- <http://ipmasq.cjb.net/>

- TCP Wrappers and The Coroners Toolkit

- <ftp://ftp.porcupine.org/pub/security/index.html>

## – Do-It-Yourself

---

- Firewalls - sources
  - Application proxies ( HTTP, FTP, NNTP etc. )
    - ANALOGX Proxy - Win32 Proxy  
<http://www.analogx.com/>
    - SQUID - Linux proxy  
<http://www.squid-cache.org/>
  - Generic Proxy
    - aproxy -<http://www.dilledabb.de/projects/aproxy.html>
  - Personal Firewalls
    - Zone Alarm  
<http://www.zonelabs.com>
    - Black ICE Defender  
<http://www.networkkice.com>

## – Do-It-Yourself

---

- How weak is your security ? Many free or inexpensive tools can help ( be careful) :
  - Password Strength
    - L0phtcrack - crack NT passwords from SAM dump  
<http://www.securitysoftwaretech.com/l0phtcrack>
    - Crack - crack UNIX passwords  
<http://www.users.dircon.co.uk/~crypto/>
    - RACF Password cracker  
<http://os390-mvs.hypermart.net/cracker.htm>
    - L0pht readsmb - crack NT passwords off the network!  
<http://www.securitysoftwaretech.com/l0phtcrack>
    - NT/W2K Password Filter DLL  
<http://support.microsoft.com/support/kb/articles/Q151/0/82.ASP>

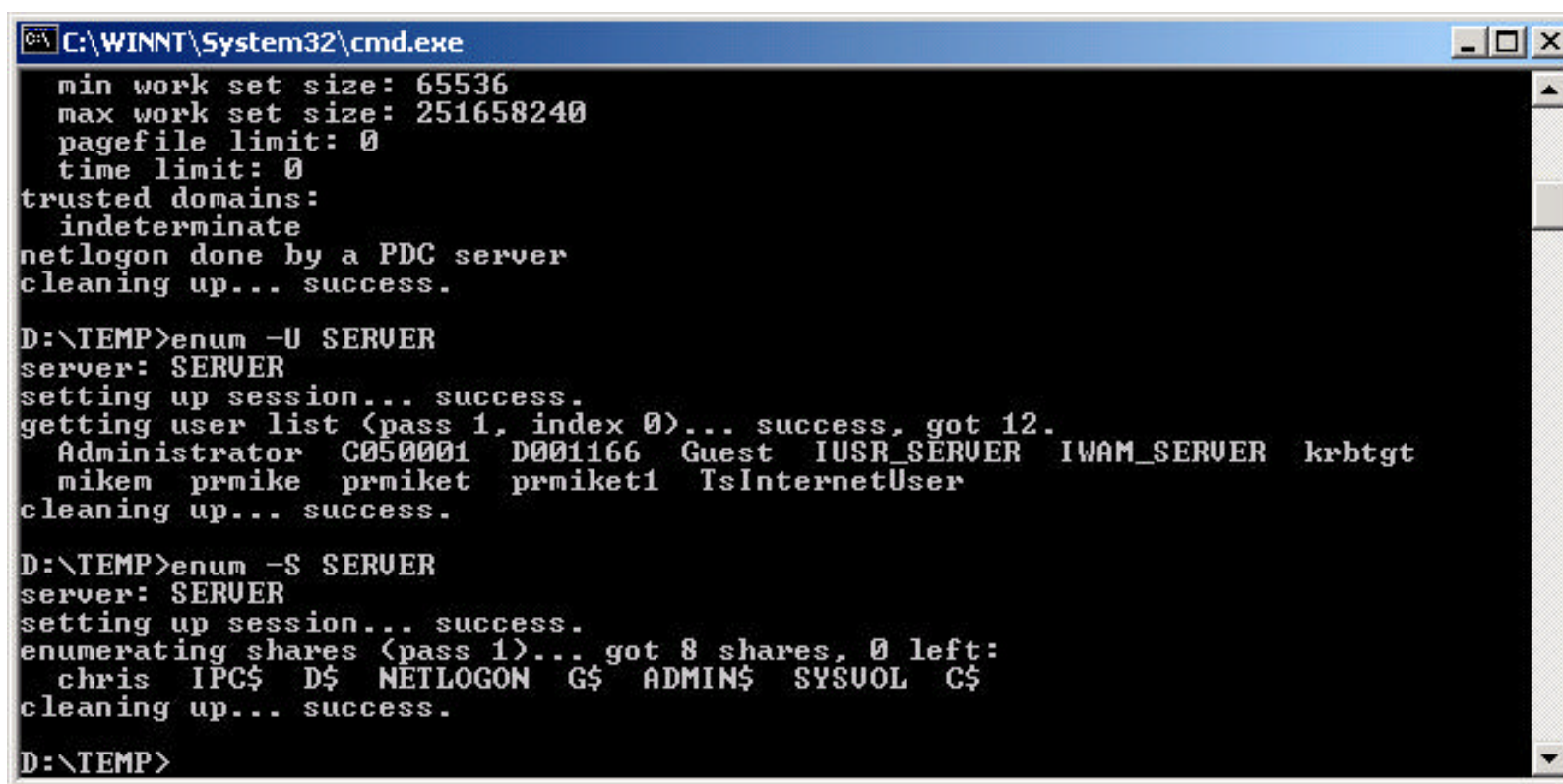
## – Do-It-Yourself

---

- How weak is your security ? Many free tools can help ( be careful) :
  - COPS - audit UNIX system -  
<http://www.fish.com/cops/>
  - SATAN <http://www.fish.com/satan/>
  - nmap - (unix )scan machines for open ports  
[www.insecure.org/nmap](http://www.insecure.org/nmap)
  - RAZOR Tools ( Unix & Win32 )  
<http://razor.bindview.com/tools/index.shtml>
    - enum - get user info
    - many others .....

## - Do-It-Yourself

### - Enum - retrieve info via NULL Session



```
C:\WINNT\System32\cmd.exe
min work set size: 65536
max work set size: 251658240
pagefile limit: 0
time limit: 0
trusted domains:
  indeterminate
netlogon done by a PDC server
cleaning up... success.

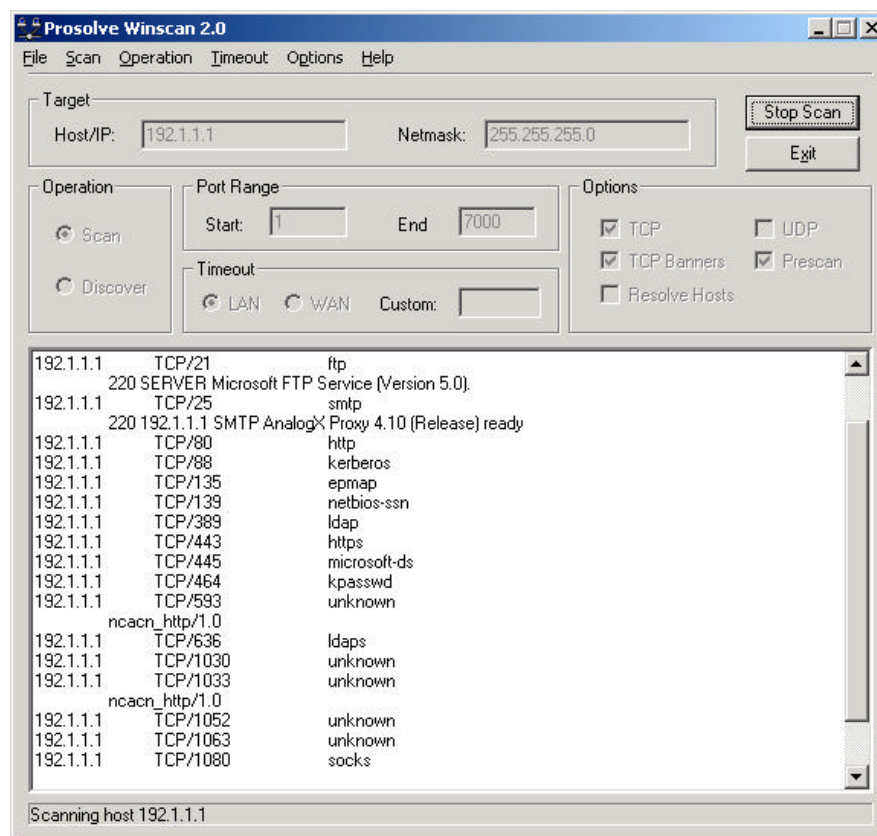
D:\TEMP>enum -U SERVER
server: SERVER
setting up session... success.
getting user list (pass 1, index 0)... success, got 12.
  Administrator C050001 D001166 Guest IUSR_SERVER IWAM_SERVER krbtgt
  mikem prmike prmiket prmiket1 TsInternetUser
cleaning up... success.

D:\TEMP>enum -S SERVER
server: SERVER
setting up session... success.
enumerating shares (pass 1)... got 8 shares, 0 left:
  chris IPC$ D$ NETLOGON G$ ADMIN$ SYSVOL C$
cleaning up... success.

D:\TEMP>
```

## – Do-It-Yourself

- Winscan ( win32 ) scan ports  
[www.prosolve.com](http://www.prosolve.com)



– The End

---

? ? ? ? ?  
? Questions ?  
? ? ? ? ?  
? ?