An Internet Firewall

Marcus J. Ranum

(mjr@dco.dec.com)

Digital Equipment Corporation

Washington Open Systems Resource Center

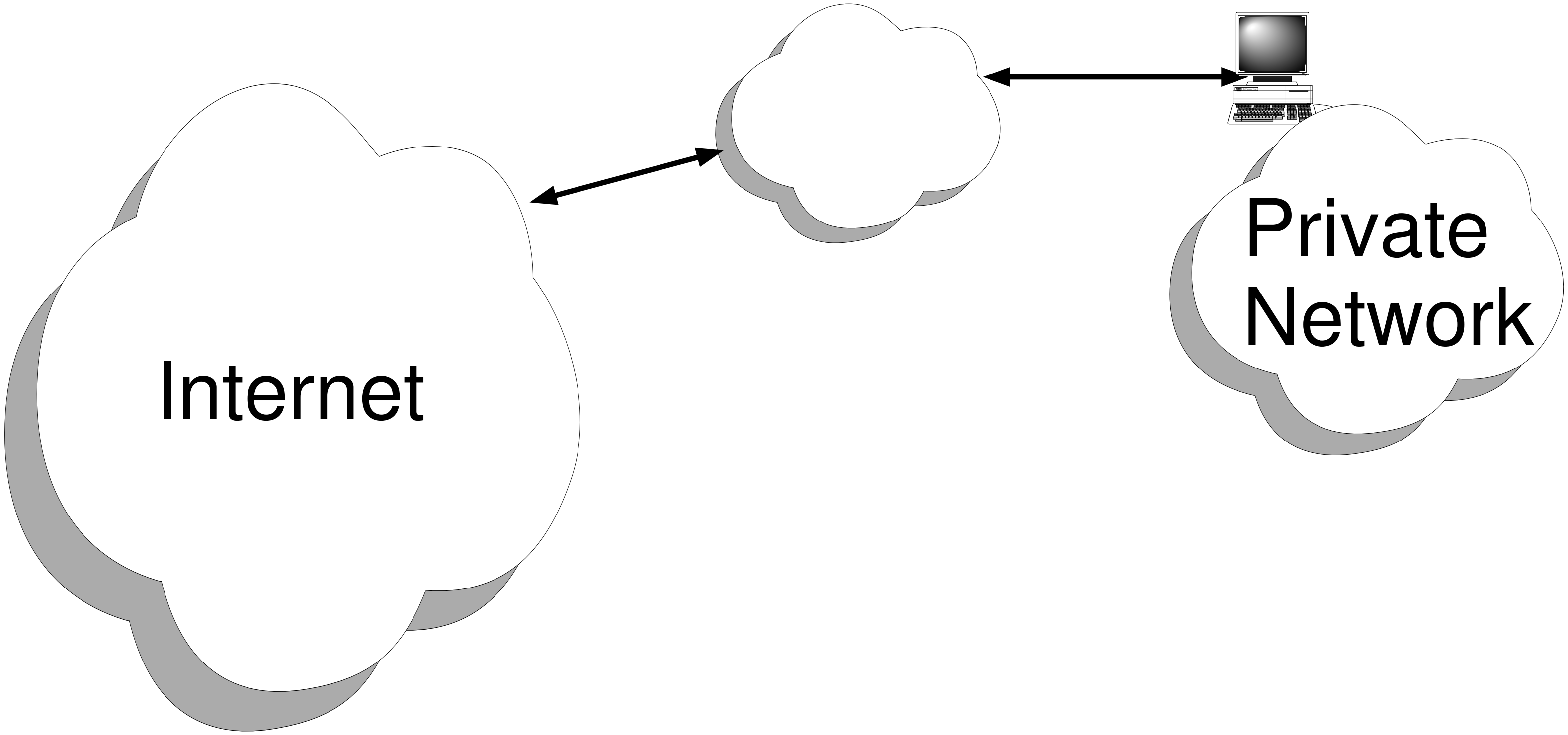
digital™

Some ways of hooking up to the Internet

Way #1: No hookup at all

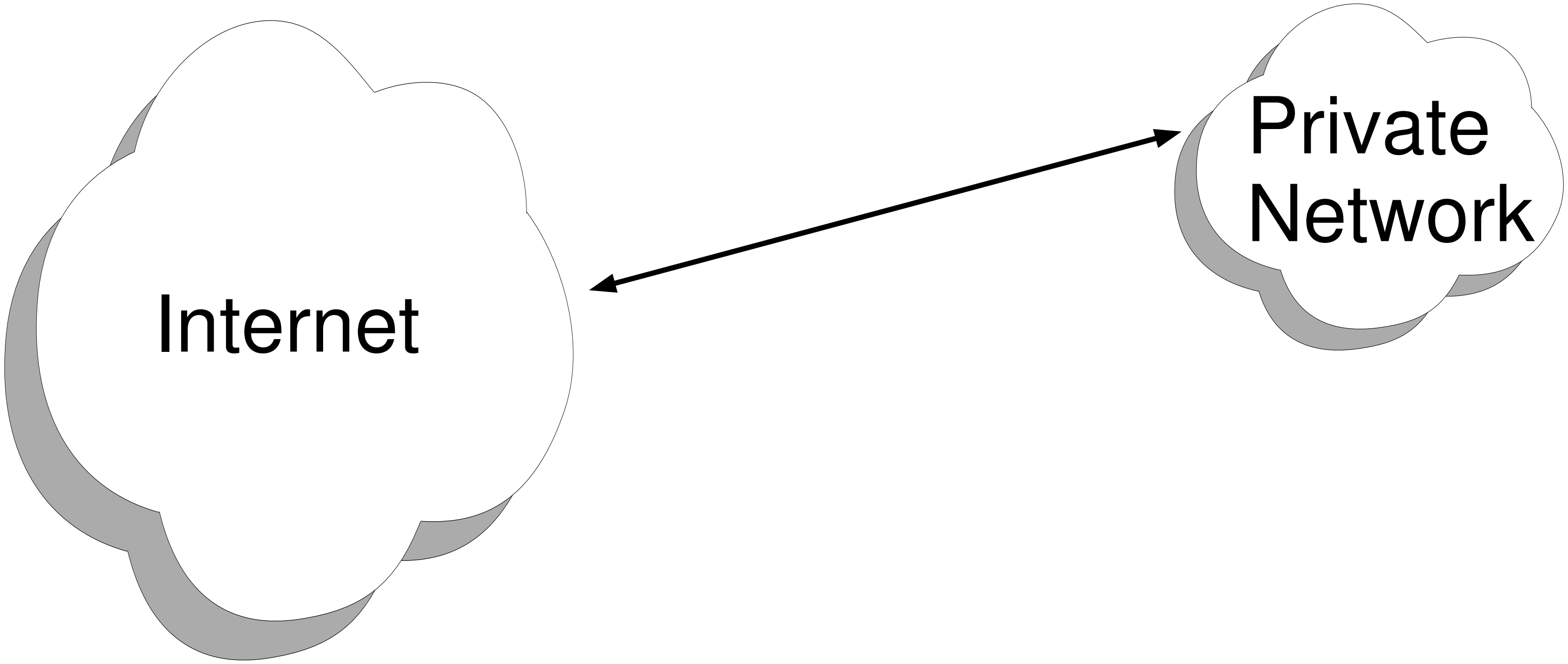
Some ways of hooking up to the Internet(cont)

Problem with Way #1: No hookup at all + an enterprising individual



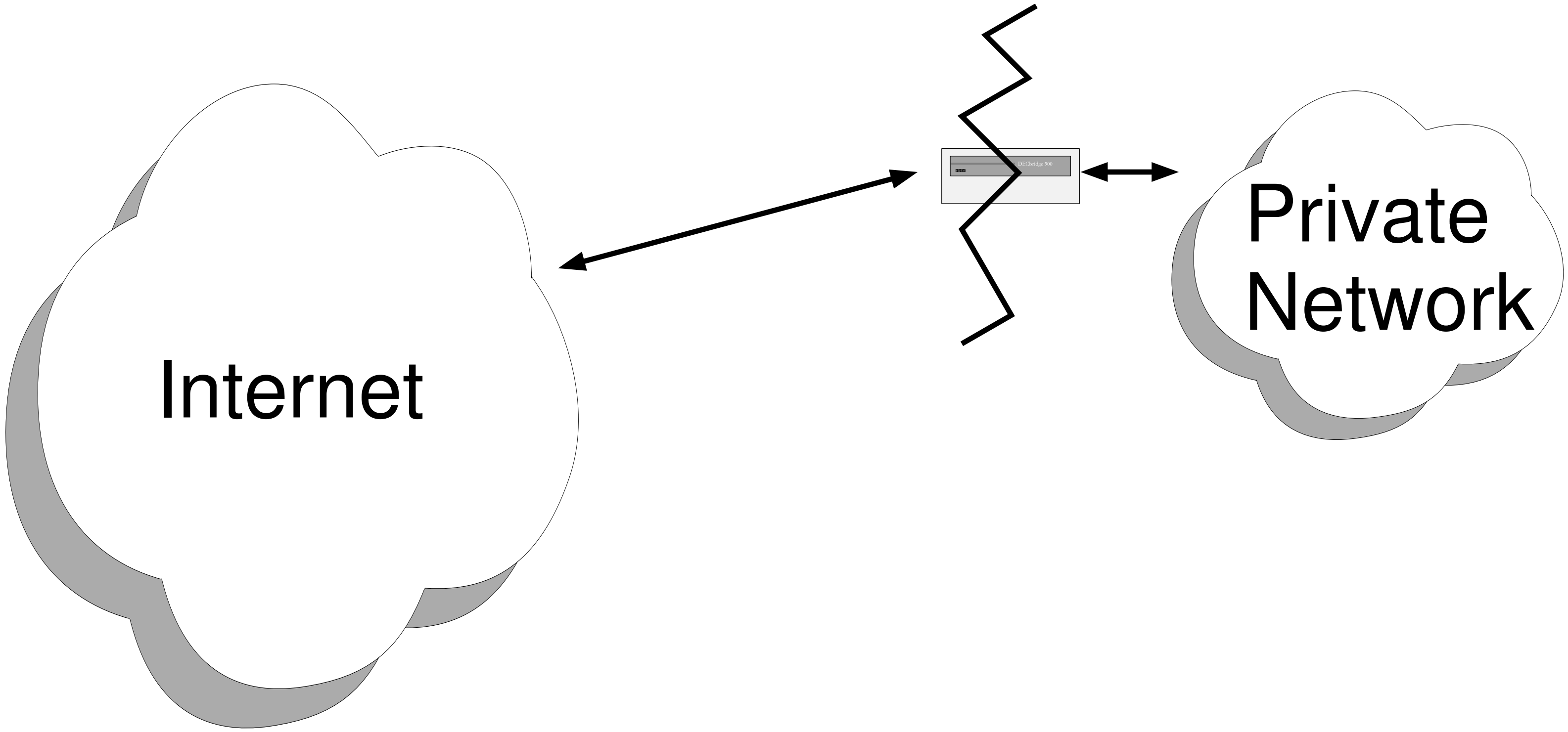
Some ways of hooking up to the Internet(cont)

Way #2: Just hook right up and make sure all your hosts are as secure as you want them to be



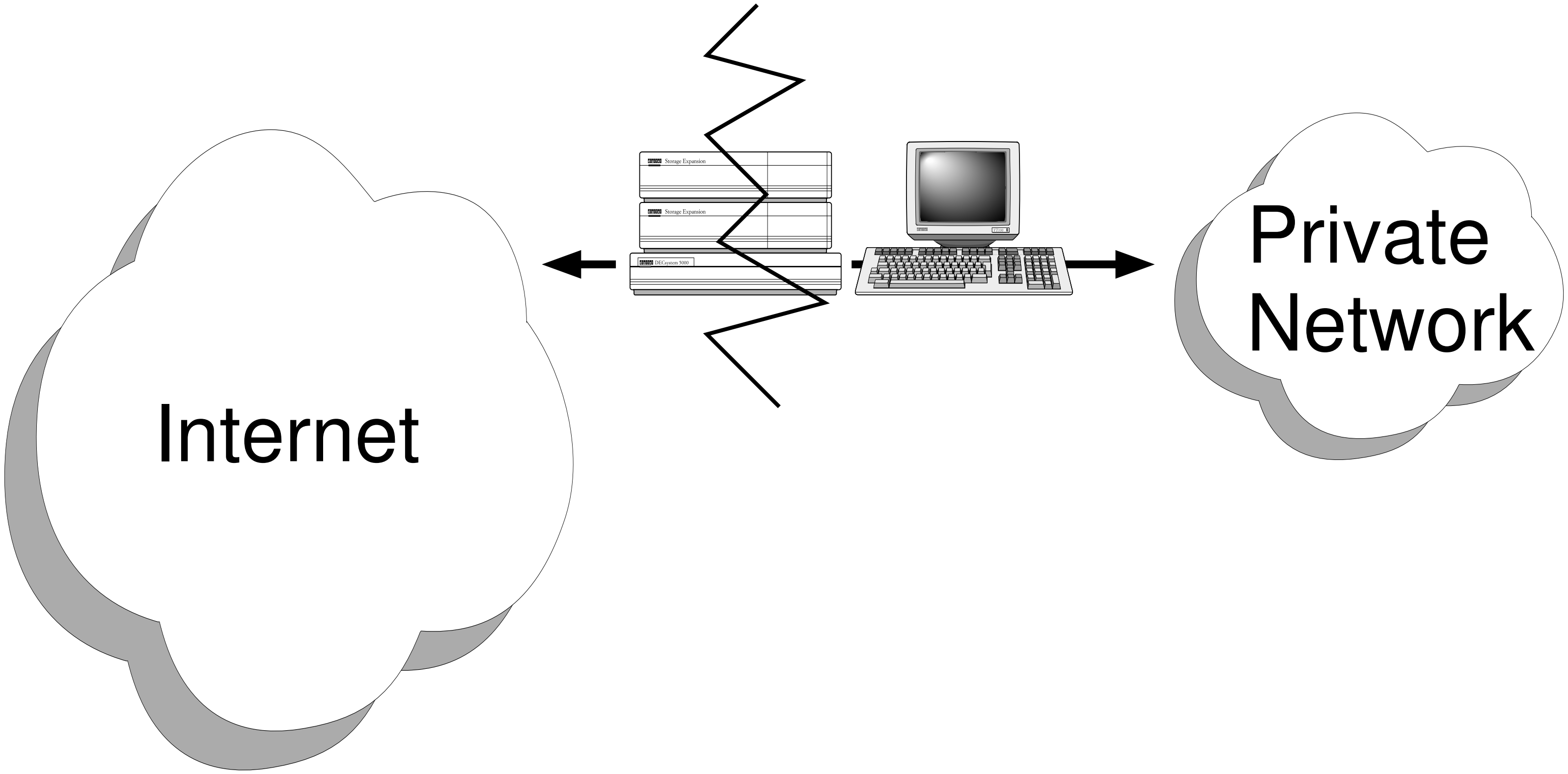
Some ways of hooking up to the Internet(cont)

Way #3: A screening router



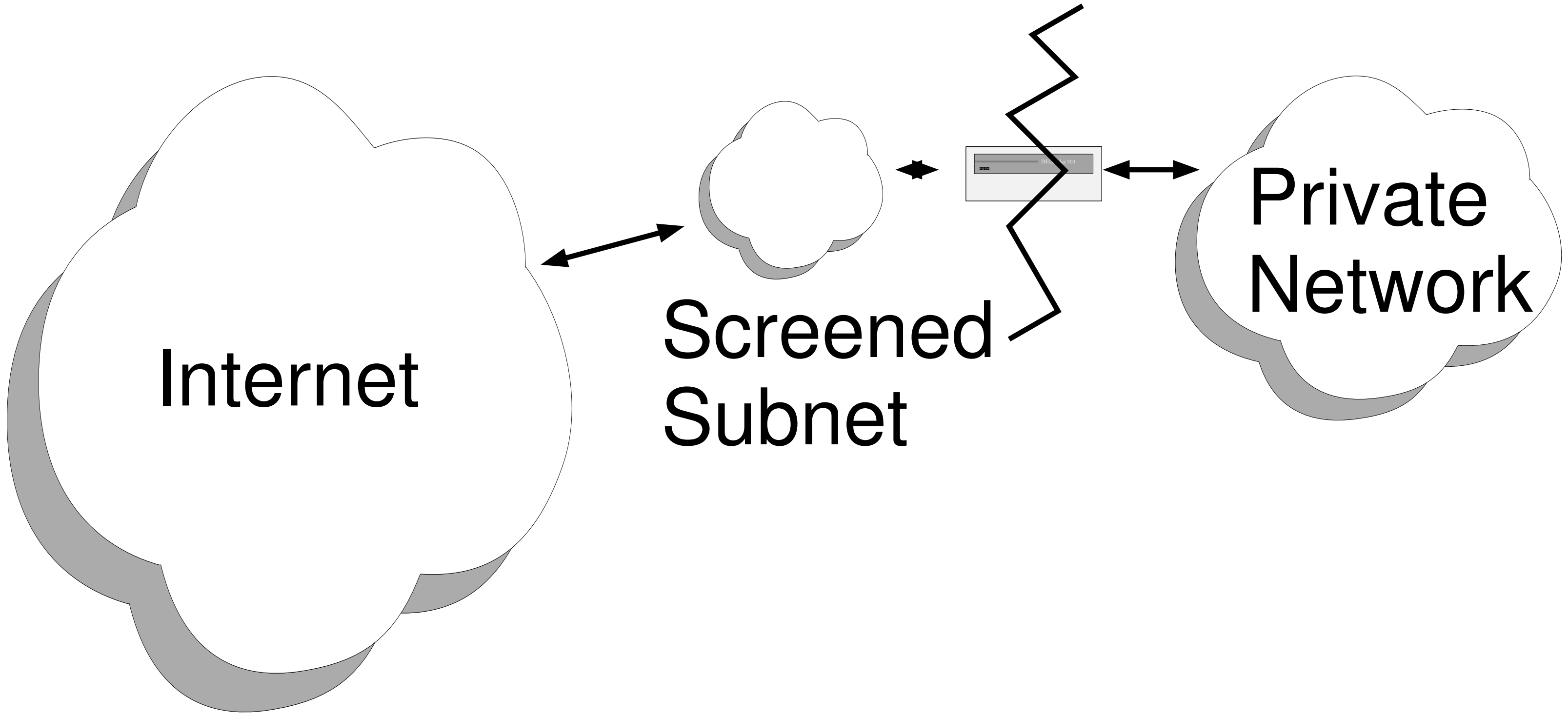
Some ways of hooking up to the Internet(cont)

Way #4: One host, two ethers, IP forwarding turned off

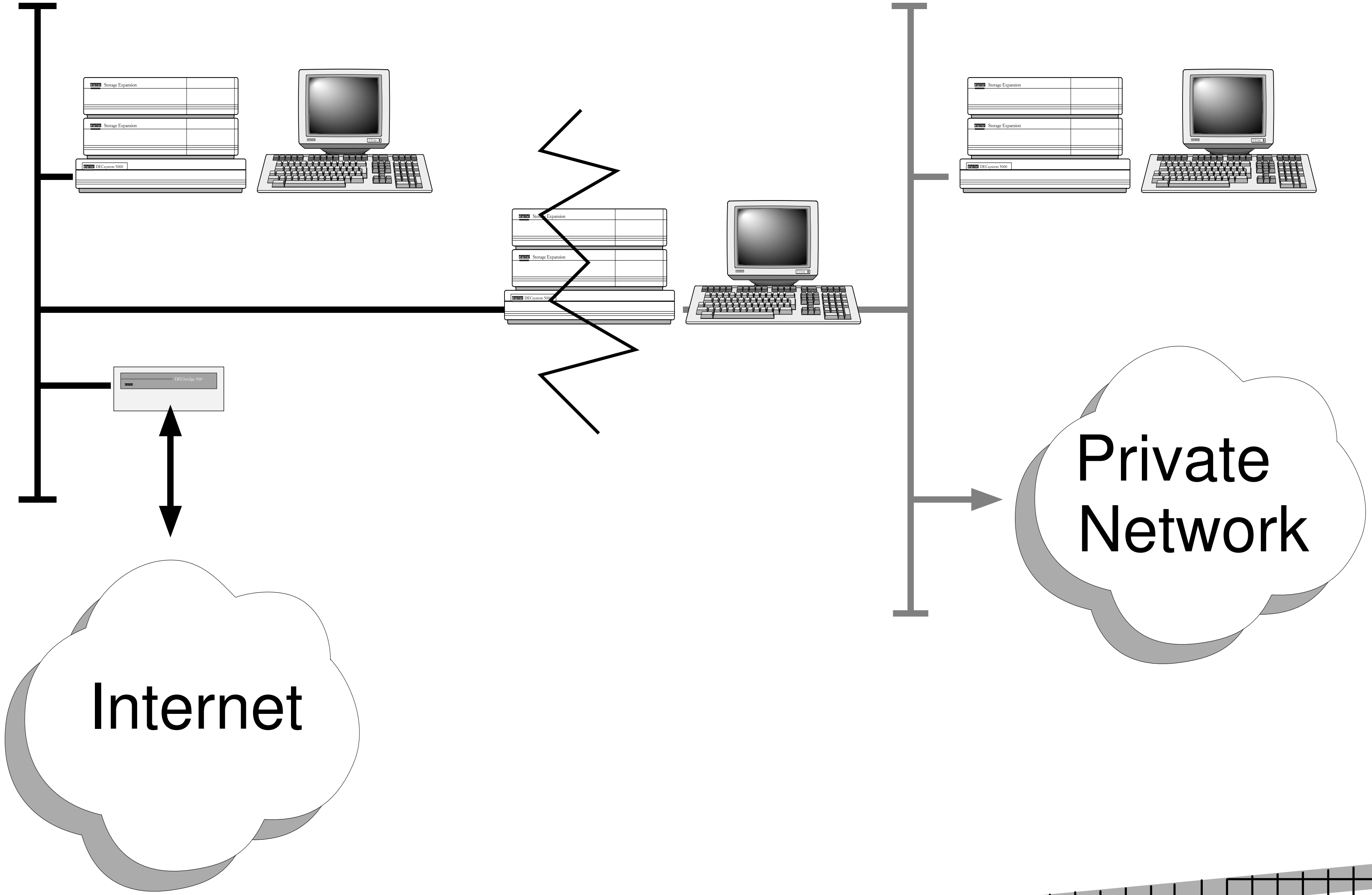


Some ways of hooking up to the Internet(cont)

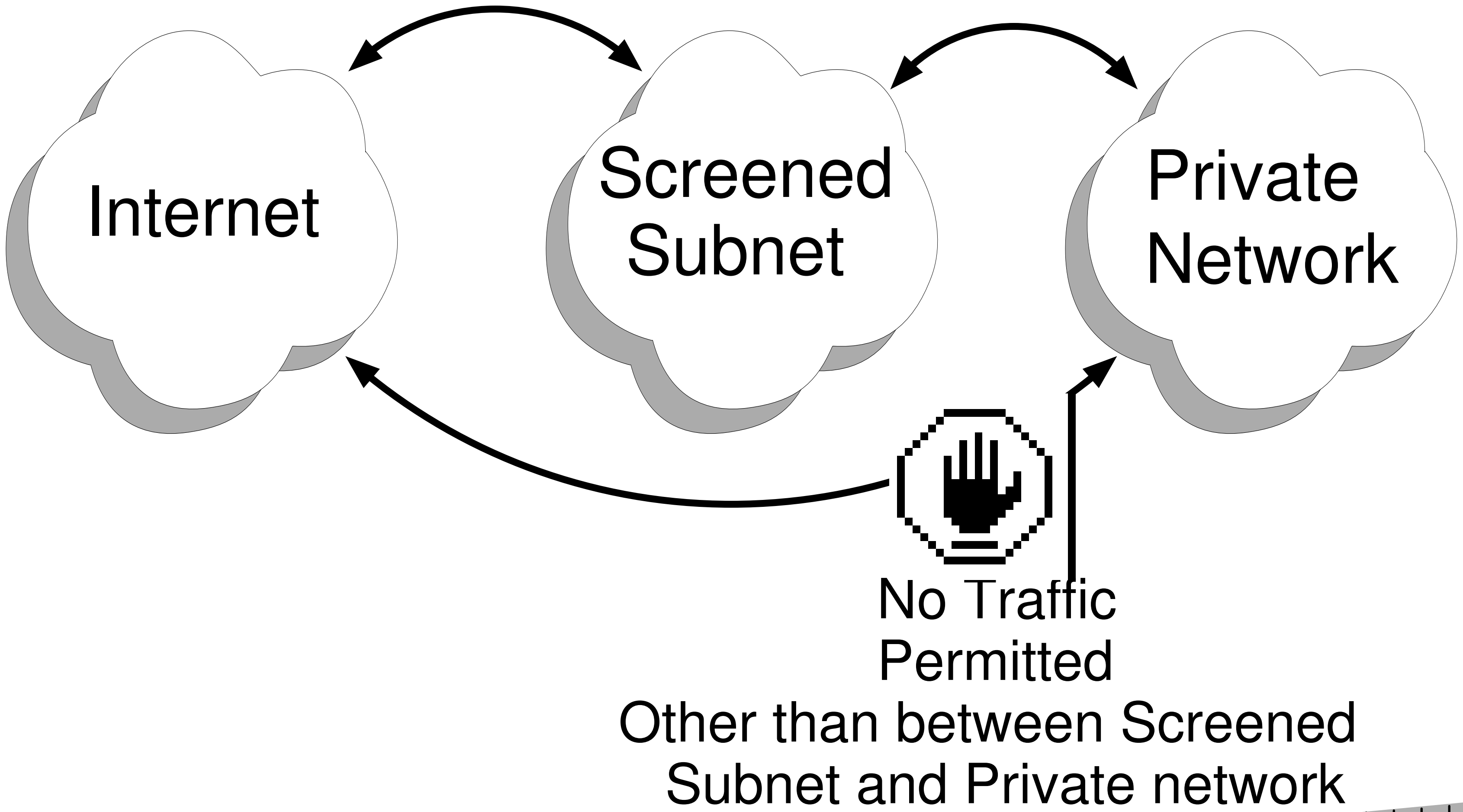
Way #5: A screened subnet



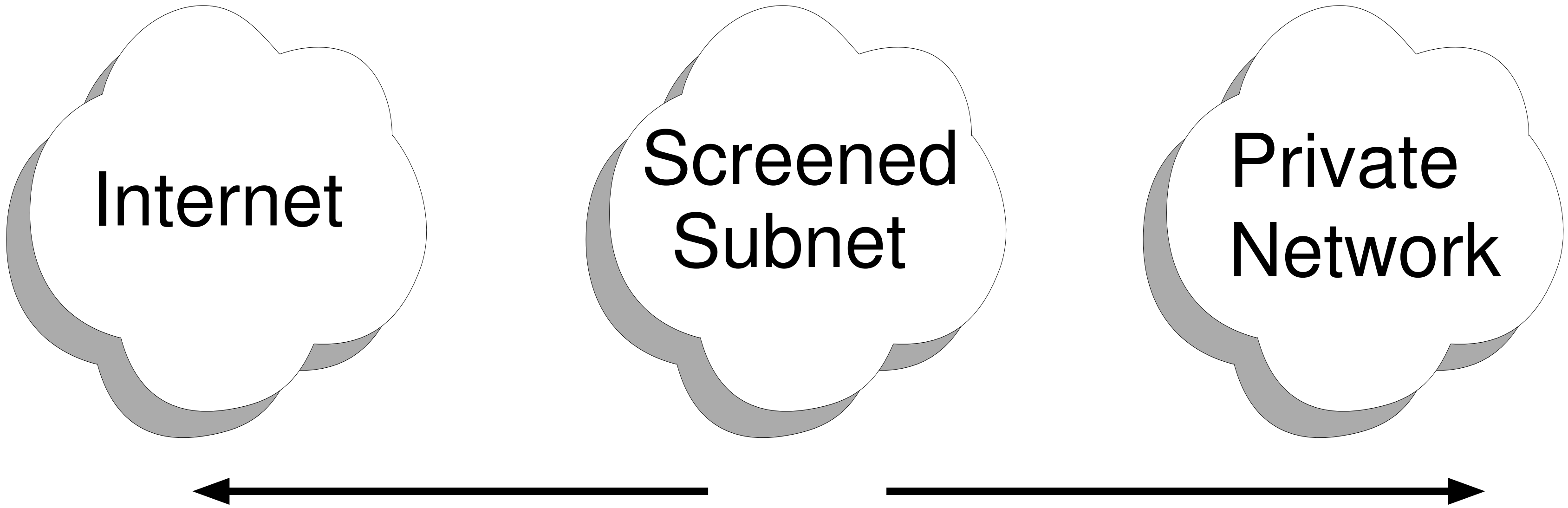
How we do it



Packet Screening



Routing Policy



Route to Screened Subnet Advertised. No route to Private Network advertised.

Route to Screened Subnet Advertised. No route to Internet advertised.

Advantages of Screened Subnets

You don’t have to show routes to your private network and your private network doesn’t need routes to the internet

Harder to break in to; it requires you to first compromise a machine on the "red" net before you can attack the "blue" net

Much harder to "open up" the internal network to the internet without someone noticing, since an attacker would need to make routes visible

Systems and Services

Three Systems:

Gatekeeper: The external and most visible host

- **Serves applications and files**

Gate: The screening router

- **Runs IP packet screening software ("screend")**

Mailgate: Handles internal IP and DECnet mail queues

- **Runs both DECnet and IP**

Applications

No user accounts on gatekeeper

Internal users can access selected Internet services through trusted application gateways

FTP - Trusted File Transfer gateway allows interactive FTP from user's desktop

Telnet - Trusted Telnet gateway allows interactive access to Internet hosts from user's desktop

Mail - Transparently gatewayed via sendmail

Name Service and USENET news run on gatekeeper

Authentication and Logging

All services connecting from outside are checked for permissions based on origin and destination

Most are simply disabled

Some user services can be tied to a handheld cryptographic authenticator (Telnet and FTP)

Everything interesting is logged and logs are kept for years, stored on an "inside" host

Logs are scanned automatically at intervals and sent to systems managers

Sucker Traps

In order to be secure you need to know when someone is sniffing at your gateway

Be familiar with the most frequently used attacks on systems

Insert logging and alarms that will fire when someone tests your system

This is <u>not</u> un-sportsmanlike behavior

Some Conclusions

Keep user accounts off your gateway

Providing dependable service reduces temptation for individuals to set up private internet links

Log everything and use simple heuristics to look for trouble

Leaving baited traps will help warn you that someone is looking for trouble

Know your enemy