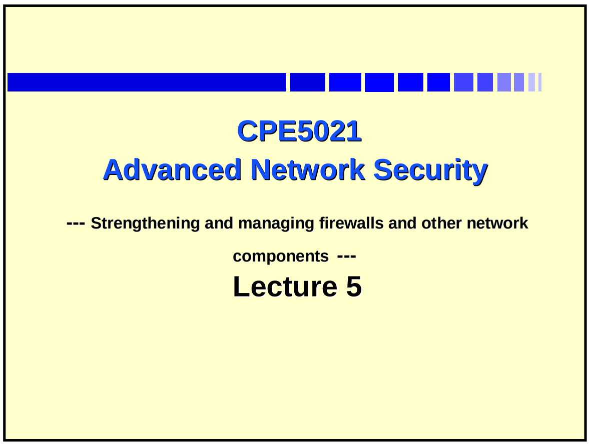
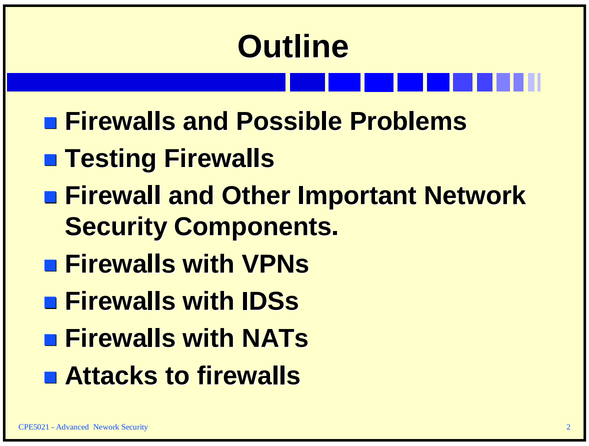


CPE5021
Advanced Network Security

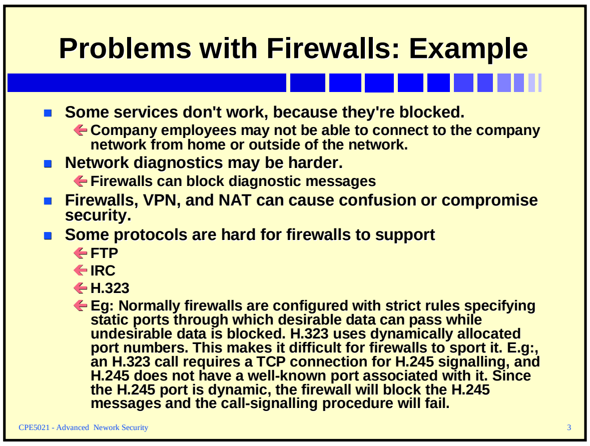
--- Strengthening and managing firewalls and other network components ---

Lecture 5



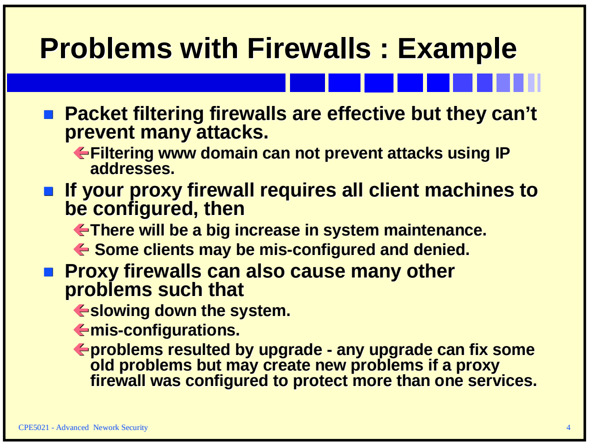
Outline

- Firewalls and Possible Problems
- Testing Firewalls
- Firewall and Other Important Network Security Components.
- Firewalls with VPNs
- Firewalls with IDSs
- Firewalls with NATs
- Attacks to firewalls



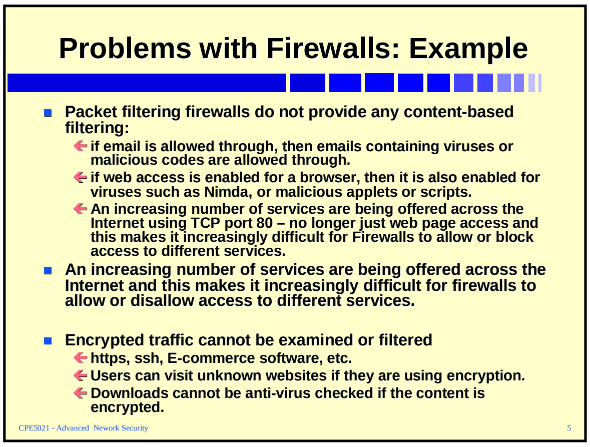
Problems with Firewalls: Example

- Some services don't work, because they're blocked.
  - Company employees may not be able to connect to the company network from home or outside of the network.
- Network diagnostics may be harder.
  - Firewalls can block diagnostic messages
- Firewalls, VPN, and NAT can cause confusion or compromise security.
- Some protocols are hard for firewalls to support
  - FTP
  - IRC
  - H.323
  - Eg: Normally firewalls are configured with strict rules specifying static ports through which desirable data can pass while undesirable data is blocked. H.323 uses dynamically allocated port numbers. This makes it difficult for firewalls to sport it. E.g:, an H.323 call requires a TCP connection for H.245 signalling, and H.245 does not have a well-known port associated with it. Since the H.245 port is dynamic, the firewall will block the H.245 messages and the call-signalling procedure will fail.



Problems with Firewalls : Example

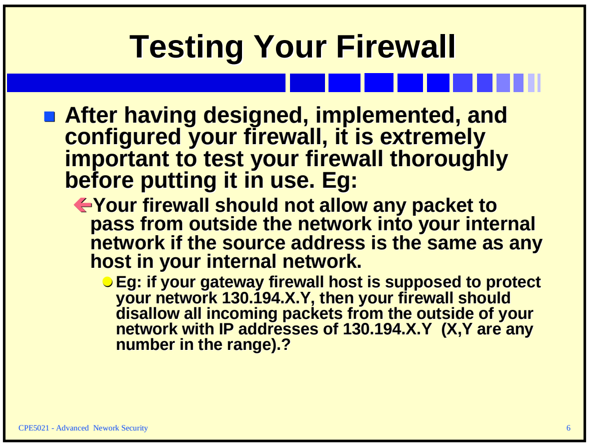
- Packet filtering firewalls are effective but they can't prevent many attacks.
  - Filtering www domain can not prevent attacks using IP addresses.
- If your proxy firewall requires all client machines to be configured, then
  - There will be a big increase in system maintenance.
  - Some clients may be mis-configured and denied.
- Proxy firewalls can also cause many other problems such that
  - slowing down the system.
  - mis-configurations.
  - problems resulted by upgrade - any upgrade can fix some old problems but may create new problems if a proxy firewall was configured to protect more than one services.



Problems with Firewalls: Example

- Packet filtering firewalls do not provide any content-based filtering:
  - if email is allowed through, then emails containing viruses or malicious codes are allowed through.
  - if web access is enabled for a browser, then it is also enabled for viruses such as Nimda, or malicious applets or scripts.
  - An increasing number of services are being offered across the Internet using TCP port 80 – no longer just web page access and this makes it increasingly difficult for Firewalls to allow or block access to different services.
- An increasing number of services are being offered across the Internet and this makes it increasingly difficult for firewalls to allow or disallow access to different services.

- Encrypted traffic cannot be examined or filtered
  - https, ssh, E-commerce software, etc.
  - Users can visit unknown websites if they are using encryption.
  - Downloads cannot be anti-virus checked if the content is encrypted.



Testing Your Firewall

- After having designed, implemented, and configured your firewall, it is extremely important to test your firewall thoroughly before putting it in use. Eg:
  - Your firewall should not allow any packet to pass from outside the network into your internal network if the source address is the same as any host in your internal network.
    - Eg: if your gateway firewall host is supposed to protect your network 130.194.X.Y, then your firewall should disallow all incoming packets from the outside of your network with IP addresses of 130.194.X.Y (X,Y are any number in the range).?

Testing and Securing Your Firewalls

- If you are running Squid or another proxy server on the firewall, make sure that only the needed port is open
  - Daemons such as Telnetd, FTPd, HTTPd and others should be shut down when they are not needed.
  - If you do need to leave certain ports open, be prepared to conduct regular scans of your firewall to test the daemons listening on these ports.
- You may require the ability to remotely administer your firewall sometimes. However, you should consider disabling all remote logins to your internal system.
- It is best to allow only interactive logins at your firewall hosts.
- If you must log in the firewall host from other machines, use only a relatively secure login application, such as SSH with one time passwords.

Testing Your Firewall

- Regularly testing your firewall system and verifying that it operates properly increase your confidence that it will perform as designed. In general, a firewall professional has to at least test the following:
  - Host hardware (processor, disk, memory, network interfaces, etc.).
  - Operating system software (booting, console access programs, start-up scripts, etc.).
  - Network interconnection equipment (cables, switches, hubs, routers, APs, etc.).
  - Firewalls.
    - Check all possible flaws in the software is difficult and need requires knowledge, but you still can use software such as a packet injector and listening sniffer (together with other tools: port canners and some hacking tools) to test your firewalls.
    - Check if configuration files, log files, audit files are modified by unauthorised people or processe.

Host Hardware Testing : Eg

- Firewall logs can quickly use up hard drive space, especially in busy networks.
  - Regularly use the df -h command to discover the total amount of hard drive space you have left. Or create a simple crontab entry that sends you this information automatically:

    6 5 * mon df -h | mail -s “DISK” firewallexpert@monash.edu.au*

  - Use *vmstat* to find the amount of RAM and virtual RAM used on the system.
  - Use *top* (or Gtop and Ktop) to see the processes that occupy the largest percentage of CPU time.

Check and Test Your OS

- Use software tools to keep track of changes to your OS and its important files:
  - E.g: use *Tripwire* to keep track of changes to the /etc/passwd and /etc/shadow files.
  - Use COPS or Tiger to check:
    - the programs and files run in /etc/rc* and cron(tab) files.
- Test if your OS has vulnerable kernel.
- Check if all patches needed by your OS have been installed.
- Check if your OS has been upgraded.
- Check if your OS has backdoors or provides remote accesses with insufficient security controls or has bugs that a hacker can take advantage of.
- Regularly check if any new vulnerability has been discovered.
- Use vulnerability testing for specific Operating Systems.

Testing Your Firewall Guidelines

- Exhaustive tests of all the possibilities are expensive and practically not possible.
- However we can use boundary tests.
  - identify boundaries in your packet filter rules.
  - then test the regions immediately adjacent to each boundary.

Testing Your Firewall Guidelines

- For each rule:
  - identify every boundary in the rule. In general, each constrained parameter in a rule contributes either one or two boundaries and the space being partitioned is a multidimensional packet attribute space.
    - For example, a rule that permits TCP packets from any host to your Web server host on port 80 will check three attributes (protocol, destination address, and destination port). The attribute space is partitioned into three regions: TCP packets to Web server at ports less than 80, port 80, and ports greater than 80.
- For each region:
  - generate some test traffic which you have engineered to stay within that region. You verify that the firewall either rejects or forwards traffic for a given region. Within a smallest region (lowest level of partition), all traffic should be rejected or forwarded; that is the purpose for partitioning the packet attribute space.

Testing Your Firewall Guidelines

- Tests also should be conducted thoroughly:
  - Test the routing configuration, packet filtering rules (including service-specific testing), and logging and alert options separately and together.
  - Test the firewall system as a whole (such as hardware/software failure recovery, sufficient log file space, proper archival procedure of logs, performance monitoring).
  - Exercise both normal conditions and not-normal conditions.

Employ Firewall Testing Tools

- There is no way that you can manually test a firewall as complete as possible, you need to employ firewall testing tools:
  - Network traffic generators (Eg: SPAK (Send PAcKets), ipsend, Ballista, etc.).
  - Network monitors (Eg: tcpdump and Network Monitor)
  - Port scanners (Eg: strobe, nmap, etc)
  - Vulnerability detection tools (Eg: COPS, Tiger, ISS, Nessus, SINT, MacAnalysis, etc.)
  - Intrusion detection systems Snort, Cisco IDS, etc.

Firewalls with VPNs

- If you plan to install a VPN device in your network, you need to consider where to place it.
  - A VPN inside a firewall: you may need to upgrade the firewall host to enable passthrough of encrypted IPSec or VPN's packets.
  - A VPN outside a firewall: traffic between the VPN device and the firewall is not checked by the firewall.
  - Integrate a VPN with a firewall: this solution is more sophisticated but it is more secure (you may need to enhance your hardware and software to perform both VPN and firewall functions efficiently – there are many products with built-in firewall-VPN-router functions).

Firewalls with VPNs

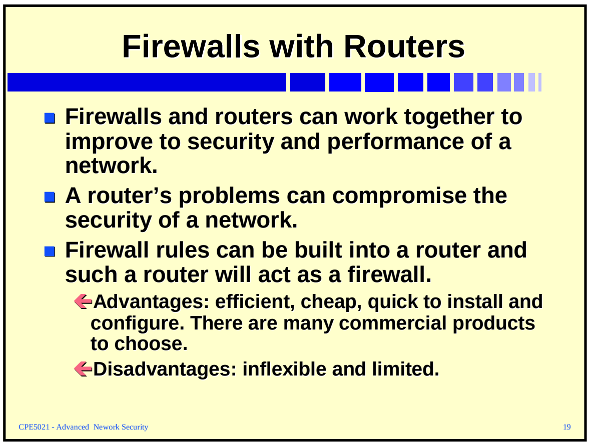
- A VPN gateway can also go on DMZ or bypass the firewall and connect directly to the internal networks.
  - If your VPN gateway is on DMZ, then the gateway firewall may not fully protect your network and you need at least another firewall.
  - If it bypasses the firewall, then VPN users may create many vulnerabilities.
    - Given access to hosts on both sides of a firewall, a tunnel to bypass the firewall could be built. Such access could be gained with a trojan horse to connect from the inside back to the machine of the attacker.
    - Also arbitrary connections from the outside to machines behind the firewall (even if they are supposedly totally blocked from the in- and outside by the firewall) can be established, for example to communicate with infiltrated programs like viruses.

Firewalls with IDSs

- Firewalls are not a complete solution to network security and IDS should be used together with firewalls.
- An IDS can sit behind your external gateway (or router) and in front of your gateway firewall.
  - Advantages: it enforces security and covers what firewalls can't. It works well with firewalls.
  - Disadvantages: it can cause false alarms, it is not easy to set up and configured, and can be expensive.

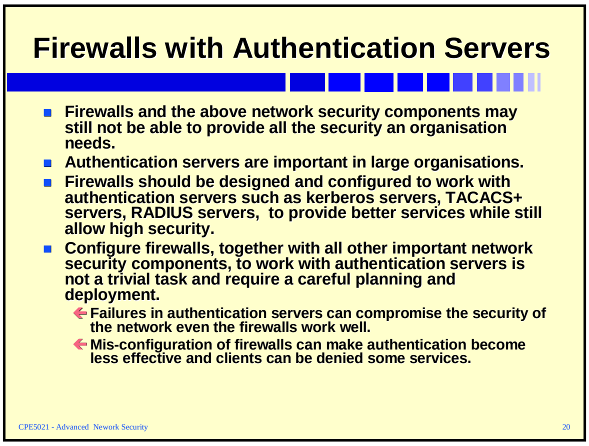
Firewalls with NATs

- Network Address Translation (NAT), by itself, is not a security procedure. Instead, NAT hides the internal network addressing from the external network and lets hosts on private IP networks communicate with hosts on public networks
- Static NAT can cause problems when used together with firewalls.
- If static NAT is not suitable, use dynamic NAT together with firewalls
- A NAT box is not a firewall.
  - Advantages: it allows more IP addresses, cheap and easy to install and configure.
  - Disadvantages:
    - it often causes problems with new services such as multimedia; it makes it hard to configure firewalls and other security components such as VPN, IDS, IPSec.
    - If a NAT box is configured with static address mapping, intruders can discover the addresses and attack hosts as if no firewall was in place



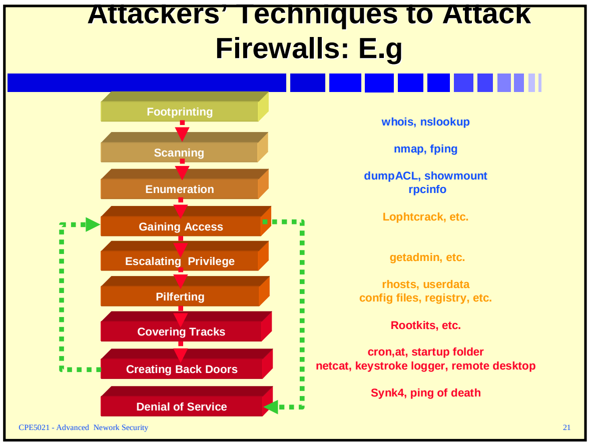
Firewalls with Routers

- Firewalls and routers can work together to improve to security and performance of a network.
- A router's problems can compromise the security of a network.
- Firewall rules can be built into a router and such a router will act as a firewall.
  - Advantages: efficient, cheap, quick to install and configure. There are many commercial products to choose.
  - Disadvantages: inflexible and limited.



Firewalls with Authentication Servers

- Firewalls and the above network security components may still not be able to provide all the security an organisation needs.
- Authentication servers are important in large organisations.
- Firewalls should be designed and configured to work with authentication servers such as kerberos servers, TACACS+ servers, RADIUS servers, to provide better services while still allow high security.
- Configure firewalls, together with all other important network security components, to work with authentication servers is not a trivial task and require a careful planning and deployment.
  - Failures in authentication servers can compromise the security of the network even the firewalls work well.
  - Mis-configuration of firewalls can make authentication become less effective and clients can be denied some services.



Attackers' Techniques to Attack Firewalls: E.g

Footprinting — whois, nslookup

Scanning — nmap, fping

Enumeration — dumpACL, showmount rpcinfo

Gaining Access — Lophtcrack, etc.

Escalating Privilege — getadmin, etc.

Pilferting — rhosts, userdata config files, registry, etc.

Covering Tracks — Rootkits, etc.

Creating Back Doors — cron,at, startup folder netcat, keystroke logger, remote desktop

Denial of Service — Synk4, ping of death