

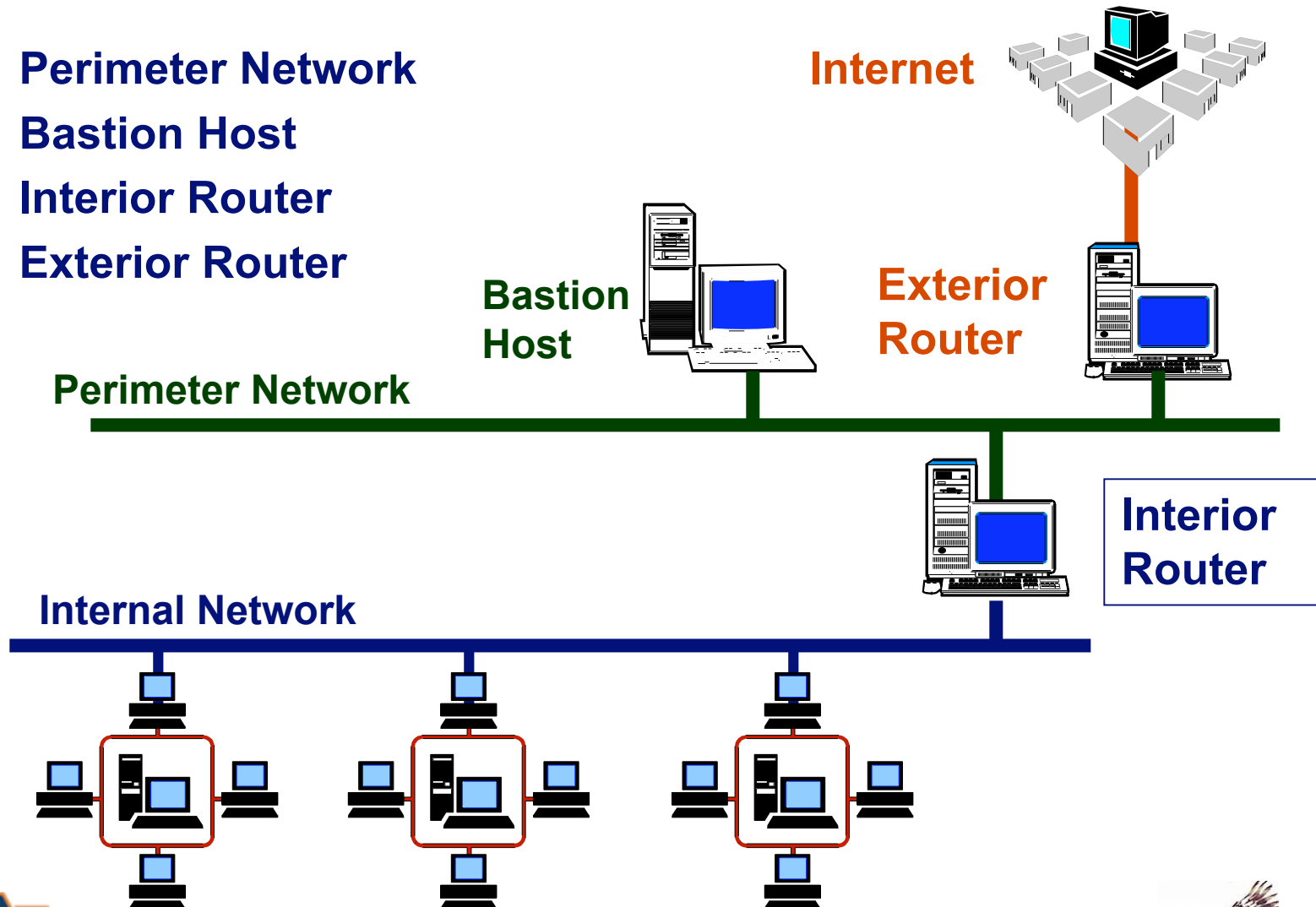
# Additional Firewall Topics

- Architectures with multiple screened subnets
- Network Address Translation (NAT)
- Proxy systems
- Naming and directory services
- Securing a bastion host
- Address forging
- Logging
- Forensic response



# Screened Subnet Architectures

- Perimeter Network
- Bastion Host
- Interior Router
- Exterior Router



# What is a Bastion Host?

## SANS Institute Intrusion Detection FAQ

- A bastion host is a computer that is fully exposed to attack.
- The system is on the public side of the demilitarized zone (DMZ), unprotected by a firewall or filtering router.
  - Frequently the roles of these systems are critical to the network security system. Indeed the firewalls and routers can be considered bastion hosts.
  - Due to their exposure a great deal of effort must be put into designing and configuring bastion hosts to minimize the chances of penetration.
  - Other types of bastion hosts include web, mail, DNS, and FTP servers.
  - Some network administrators will also use sacrificial lambs as bastion hosts, these systems are deliberately exposed to potential hackers to both delay and facilitate tracking of attempted break-ins.



# Configuring a Bastion Host

- **Effective bastion hosts are configured very differently from typical hosts.**
- **Each bastion host fulfills a specific role, all unnecessary services, protocols, programs, and network ports are disabled or removed.**
- **Bastion hosts do not share authentication services with trusted hosts within the network so that if a bastion is compromised the intruder will still not have 'the keys to the castle.'**
- **A bastion host is hardened to limit potential methods of attack.**



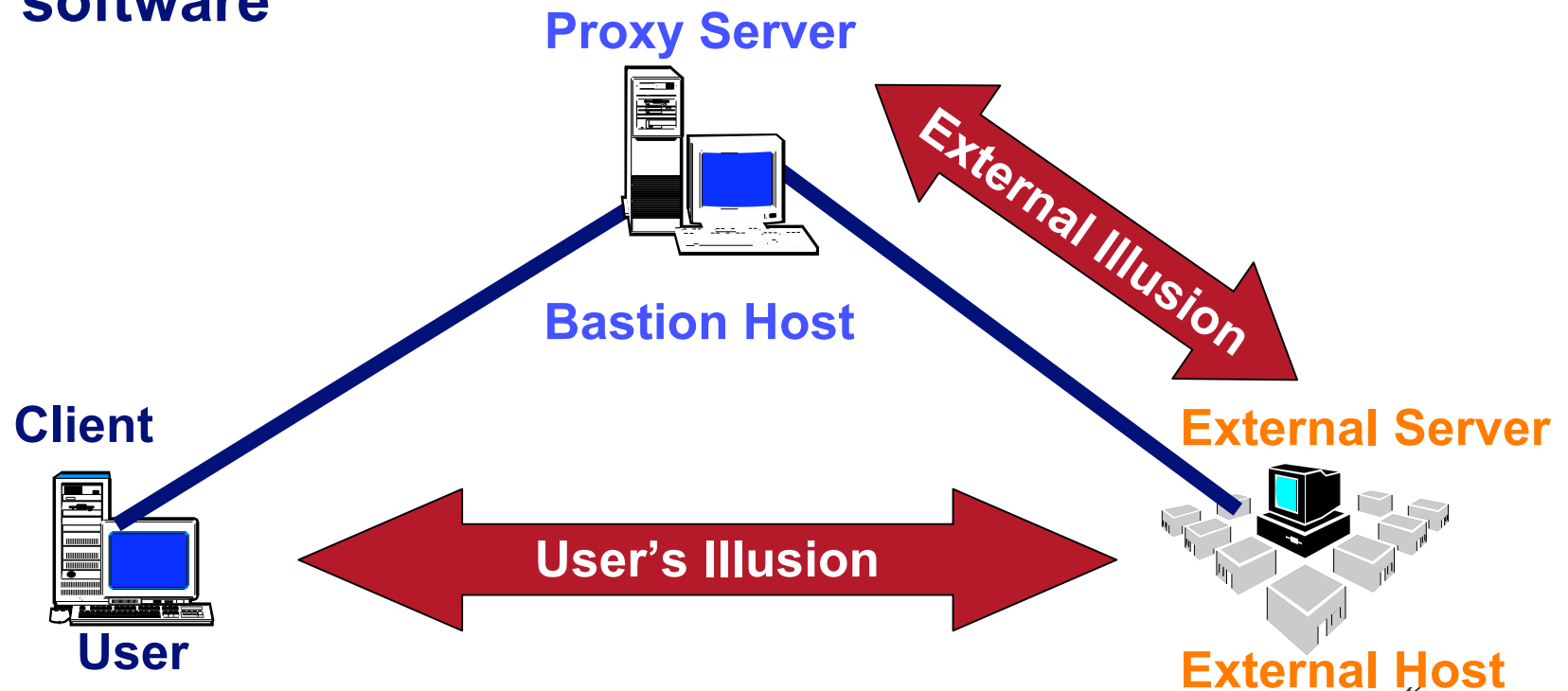
# Hardening a Bastion Host

- The specific steps to harden a particular bastion host depend upon the intended role of that host as well as the operating system and software that it will be running.  
**Access Control Lists**
- (ACLs) will be modified on the file system and other system objects; all unnecessary TCP and UDP ports will be disabled; all non-critical services and daemons will be removed; as many utilities and system configuration tools as is practical will also be removed.
- All appropriate service packs, hot fixes, and patches should be installed.
- Logging of all security related events need to be enabled and steps need to be taken to ensure the integrity of the logs so that a successful intruder is unable to erase evidence of their visit.
- Any local user account and password databases should be encrypted if possible.



# Proxy Servers – reality and illusion

- Proxy systems deal with insecurity problems by avoiding user logins on the dual homed host and by forcing connections through controlled software



# Proxy Servers

- A server that sits between a client application, such as a Web browser, and a real server.
  - It intercepts all requests to the real server to see if it can fulfill the requests itself.
  - If not, it forwards the request to the real server.
- Proxy servers have two major functions
  - **Improve Performance:** Proxy servers can dramatically improve performance because proxy servers save the results of all requests for a certain amount of time.
    - Consider the case where both user X and user Y access the WWW through a proxy server.
      - First user X requests a certain Web page, which we'll call Page 1.
      - Sometime later, user Y requests the same page.
      - Instead of forwarding the request to the Web server where Page 1 resides, which can be a time-consuming operation, the proxy server simply returns the Page 1 that it already fetched for user X.
    - Since the proxy server is often on the same network as the user, this is a much faster operation. Real proxy servers can support hundreds or thousands of users.
  - **Filter Requests:** Proxy servers can also be used to filter requests. For example, a company might use a proxy server to prevent its employees from accessing a specific set of Web sites.



# Securing the Network Apps

- The last step to securing a bastion host may be the most difficult: securing whatever network application the host is running.
- Very often the vendor of a web or streaming media server doesn't consider security risks while developing their product.
- It is usually up to the system administrator to determine through testing what ACLs they need to modify to lock down the network application as thoroughly as possible without disabling the very features that make it a useful tool.
- It is also necessary to closely track the latest announcements from the vendor regarding security problems, workarounds, and patches.
- The more popular network applications also tend to inspire the creation of independent mailing lists, newsgroups, and websites that can be tracked for additional insights.



# Network Address Translation (NAT)

(Cisco)



- Developed by Cisco, Network Address Translation is used by a device (firewall, router or computer) that sits between an internal network and the rest of the world.
- NAT has many forms and can work in several ways



# Static NAT

- **Static NAT - Mapping an unregistered IP address to a registered IP address on a one-to-one basis. Particularly useful when a device needs to be accessible from outside the network.**
  - unregistered means a host with an IP address but no domain name registered in the DNS.

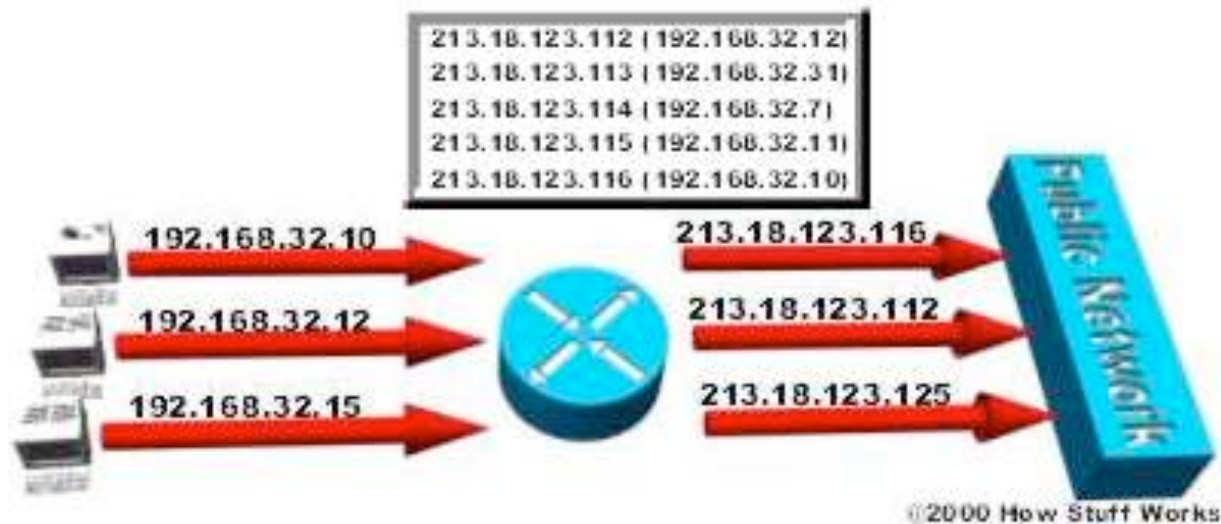


**In static NAT, the computer with the IP address of 192.168.32.10 will always translate to 213.18.123.110.**



# Dynamic NAT

- Dynamic NAT - Maps an unregistered IP address to a registered IP address from a group of registered IP addresses.

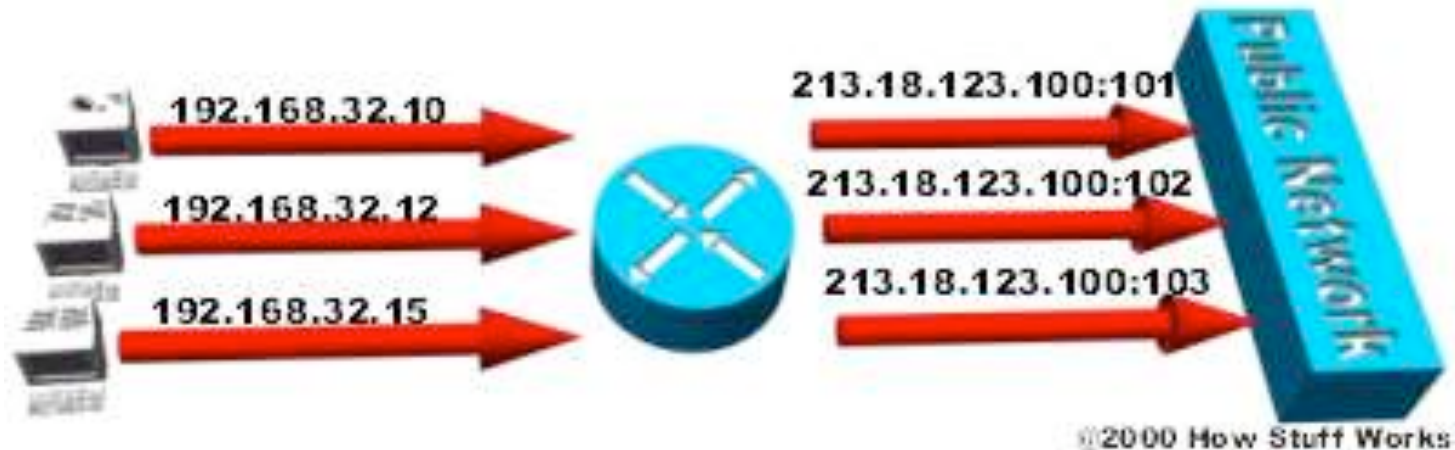


In dynamic NAT, the computer with the IP address 192.168.32.10 will translate to the first available address in the range from 213.18.123.100 to 213.18.123.150.



# Overloading

- **Overloading** - A form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address by using different ports.
- This is known also as **PAT (Port Address Translation)**, single address NAT or port-level multiplexed NAT.

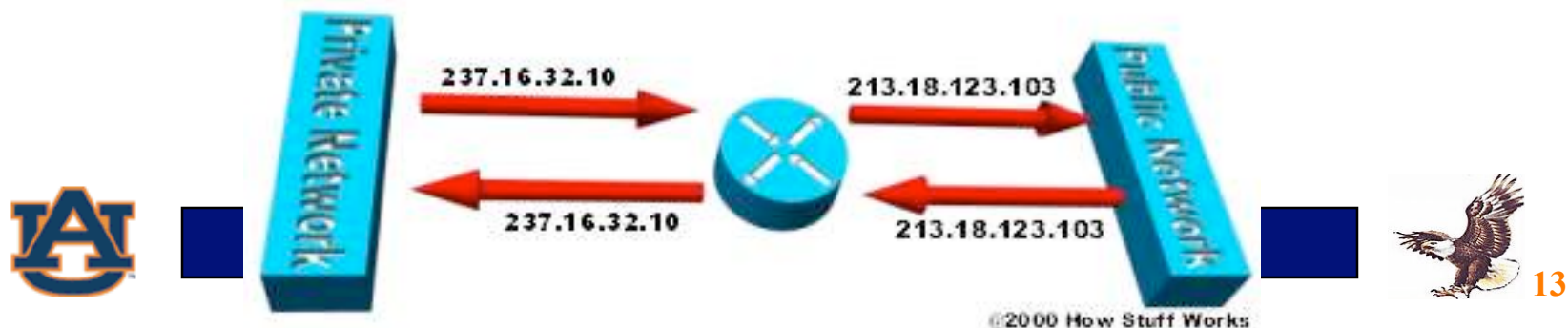


In overloading, each computer on the private network is translated to the same IP address (213.18.123.100), but with a different port number assignment.



# Overlapping

- **Overlapping** - When the IP addresses used on your internal network are registered IP addresses in use on another network, the router must maintain a lookup table of these addresses so that it can intercept them and replace them with registered unique IP addresses.
  - It is important to note that the NAT router must translate the "internal" addresses to registered unique addresses as well as translate the "external" registered addresses to addresses that are unique to the private network.
  - This can be done either through static NAT or by using DNS and implementing dynamic NAT.
- The internal IP range (237.16.32.xx) is also a registered range used by another network.
  - Therefore, the router is translating the addresses to avoid a potential conflict with another network.
  - It will also translate the registered global IP addresses back to the unregistered local IP addresses when information is sent to the internal network.



# “Personal Firewalls”

- **BlackIce Case Study**
  - Limited rule setting
  - Four rule sets
    - **Paranoid: Blocks all unsolicited inbound traffic**
    - **Nervous: Blocks all unsolicited inbound traffic except some interactive content on the web sites**
    - **Cautious: Blocks unsolicited network traffic that accesses operating system and networking services**
    - **Trusting: All ports open and unblocked, all inbound traffic allowed**
  - Severity levels
  - Response levels
  - Application profiling



# Firewall Selection

- **Single Purpose Router or a General Purpose Computer?**
  - Packet filtering should be only activity on the device
  - Combinations of proxy servers and/or bastion hosts may be implemented on routing device
    - **Serious increase in hardware performance requirements**
- **Simple specification of rules**
  - Packet filtering is complicated to begin with because the protocols are complex, rule implementation should not add complexity.
- **It should allow rules based on any header or meta-packet criteria**
  - Header information is in the packet
  - Meta-packet information are those things routers recognize outside of the header



# Applying filtering rules

- **Apply rules in the order specified**
  - Reordering makes it more difficult to analyze what is going on
  - Any quirks or bugs in the rule set may be obscured
  - Reordering rules can break a rule set that would otherwise work correctly
    - **Example**
      - Rule A permits the university network to reach your research subnet
      - Rule B locks out a hostile subnet at the university out of everything else
      - Rule C disallows Internet access to your subnet
    - **Rule order ABC**
      - Packet from hostile subnet allowed to research subnet (rule A)
    - **Rule order BAC**
      - Packet from hostile subnet denied access to research subnet (rule B)
  - Rule may have limited granularity



# More packet filtering guidelines

- **Allow rules to be applied separately to incoming and outgoing packets on a per-interface basis**
  - provide maximum flexibility
  - when only outgoing packets can be viewed then:
    - **The filtering system is always “outside” of its filters**
    - **More difficult to detect forged packets**
      - Forgery is most easily detected when the packet enters from outside the system
      - Routers can generate packets themselves and sometimes process internal packets (due to fixed paths for example).
  - **Filtering outgoing packets only is more complicated when the router has multiple ports**
- **Allow option to log accepted or dropped packets**
- **Support good testing and validation capabilities**

