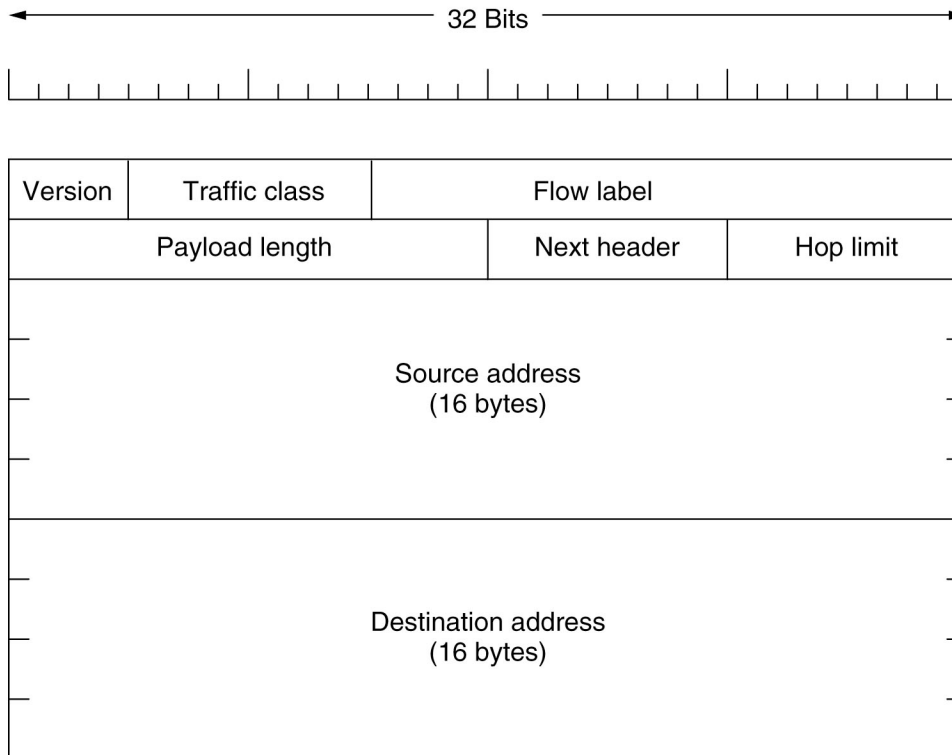
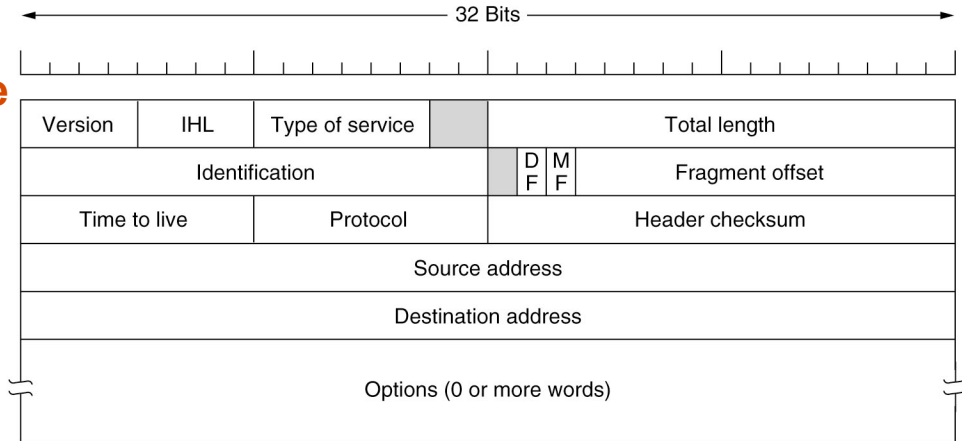


IPv4 versus IPv6

IP V4

- IHL describes how long the variable length header is
- ToS – reliability vs. speed
- Length – header & data
- ID – dest uses to assemble fragments
- Protocol – UDP, TCP etc.



IP V6

- Traffic class to support priority
- Flow label (experimental)
 - flow controllable
 - Can traffic be slowed in case of congestion?
- Header simplified because of option to add extension headers else indicates which transport handler to pass the packet to.



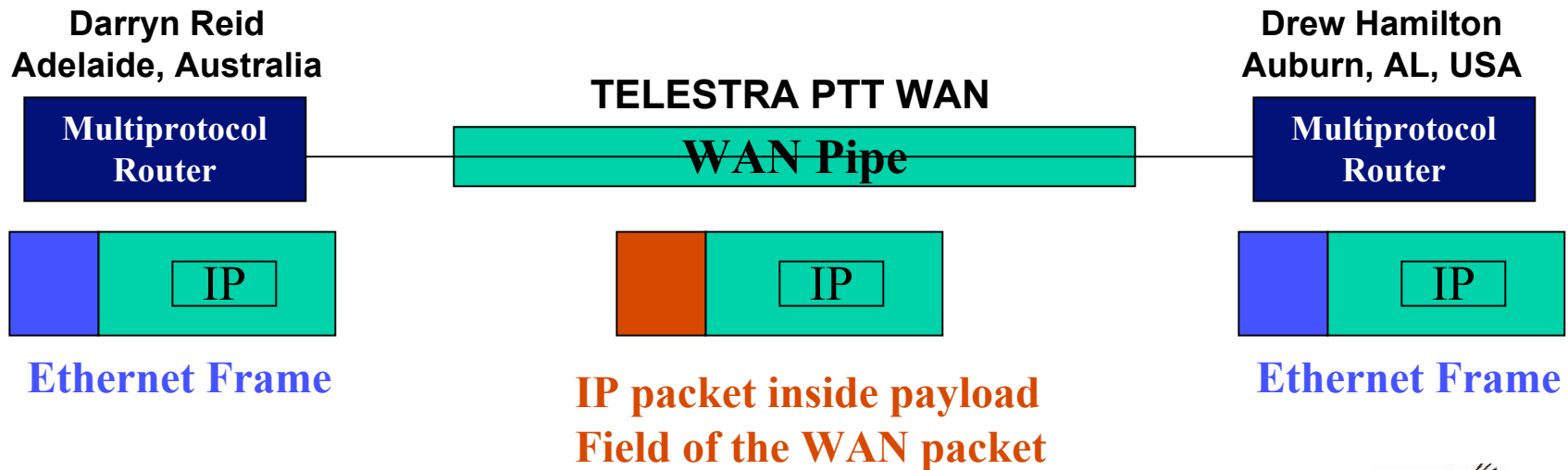
Definition of a VP(rivate)N

- A network where packets that are **internal to a private network** pass across a public network.
 - Without being obvious to hosts on the private network
 - Illusion of a dedicated, circuit-switched network
- In general, VPNs use encryption to protect the packets as they pass across the public network.
- VPN solutions are popular because it is often **cheaper** to connect two local networks via public networks (i.e. Internet connections) than via private networks



Tunneling Revisited

- A special case when source and destination networks are the same type, but there is a different network between them.
 - Reid's host sends an ethernet frame to an Adelaide-based multi-protocol router with the Auburn IP address encapsulated in the ethernet frame.
 - Adelaide router removes the IP packet and inserts into the payload of the WAN frame and addresses the WAN frame to the multi-protocol router in Auburn.
 - Auburn router receives the WAN packet, removes the IP packet and sends it to Hamilton's host.

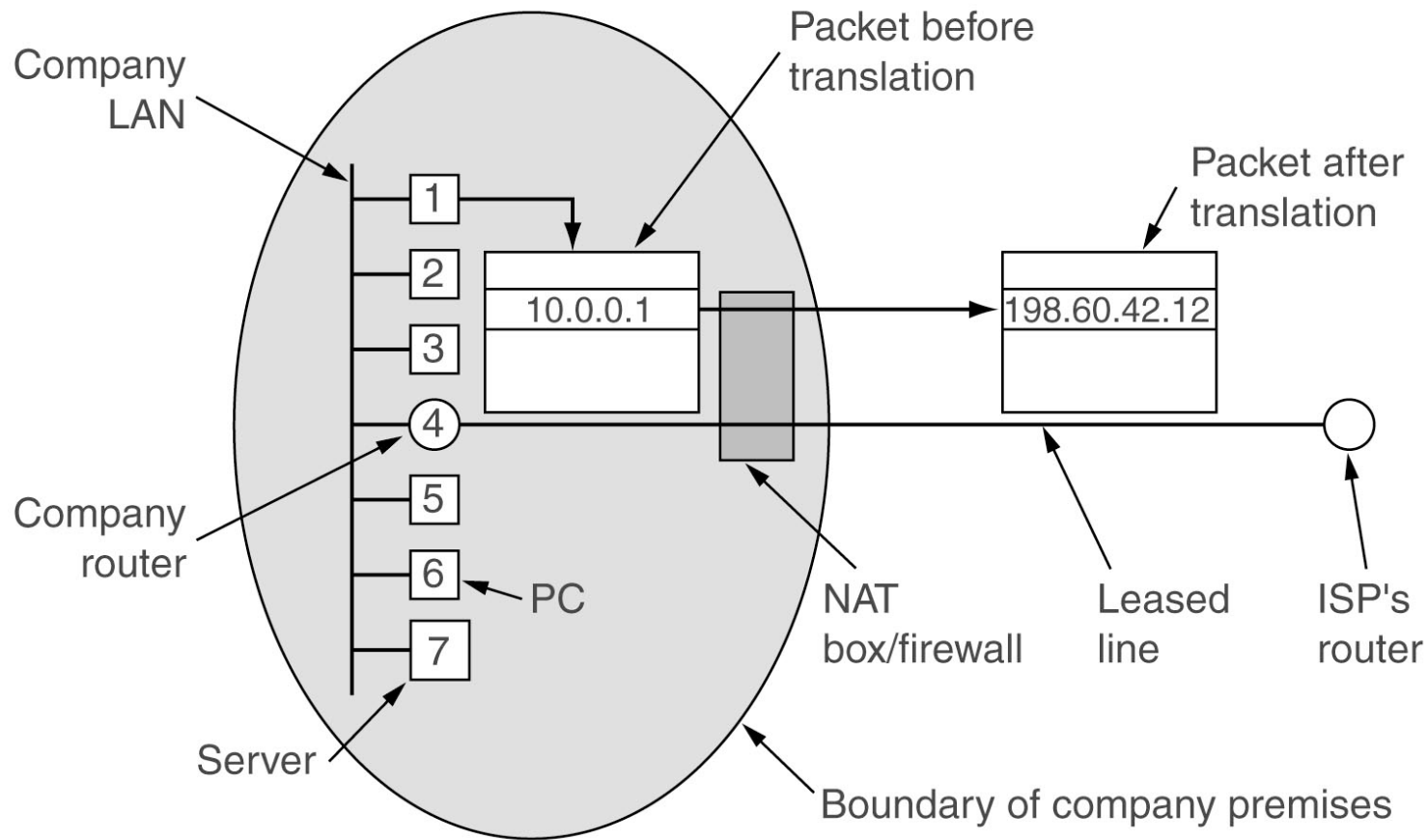


Firewalls

- **Traditionally, a firewall is a wall separating two areas, in a building, a car, etc., to prevent fire from propagating from one area to another.**
 - **By extension, it is used to separate two networks, to prevent hostile packets from one network from reaching the other.**
 - **The most common firewall configuration protects a company's private network from the Internet.**
 - **Firewalling traditionally operates by inspecting packet headers and discarding packets with undesirable header info.**



Tanenbaum's View of Firewalls in the Network



Firewall Characteristics

- **Firewalls**
 - have at least two network interfaces.
 - have rules to forward the packets.
- **A tightly configured firewall won't allow any incoming packets and will allow outgoing packets to only trusted machines.**
- **It is expensive to put security patches on every machine in the corporate network.**
- **Firewalls are *not fail-safe* and are a *central point of failure*.**



Firewall Deployment

- **When establishing an Internet firewall, the first thing you must decide is its basic architecture**
 - (assuming you have previously established your firewall requirements and the security policy it is intended to implement).
- **The most common boundary where firewalls are applied today is between an organization's internal networks and the Internet.**
 - In this context, architecture refers to the inventory of components (hardware and software), and the connectivity and distribution of functions among them.
 - There are two classes of firewall architectures, which we refer to as the *single layer* and the *multiple layer* architectures.



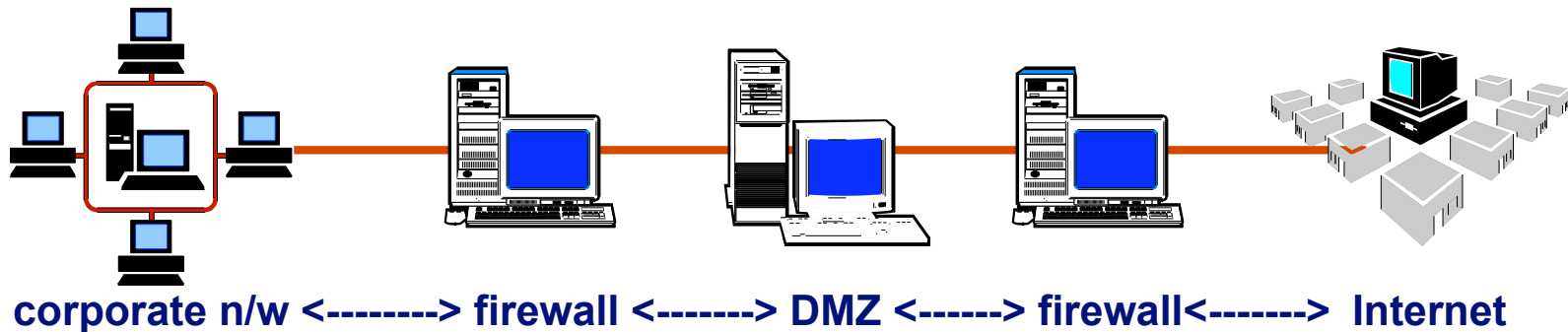
Single Layer Firewalls

- In a single layer architecture, one network host is allocated all firewall functions and is connected to each network for which it is to control access.
- This approach is usually chosen when containing cost is a primary factor or when there are only two networks to interconnect.
- It has the advantage that everything there is to know about the firewall resides on that one host.
- The greatest disadvantage of the single layer approach is its susceptibility to implementation flaws or configuration errors -- depending on the type, a single flaw or error might allow firewall penetration



Multiple Layer Architecture

- In a multiple layer architecture, the firewall functions are distributed among a small number of hosts, typically connected in series, with DMZ networks between them.
- This approach is more difficult to design and operate, but can provide substantially greater security by diversifying the defenses you are implementing.
- The most common design approach for this type of architecture is an Internet firewall composed of two hosts interconnected with one DMZ network.



1. A firewall implements your security policy

Firewall Best Practices

- A firewall enforces some security policy.
- If you didn't have a security policy before you put the firewall in place, you do now.
- It may be unwritten, but it's still a security policy.
- If you haven't made explicit decisions about what you want the security policy to be, it's probably not the best policy for your site, and it will certainly be difficult for you to maintain it over time.
- In order to have a good firewall, you need a good security policy--one that is written down and widely agreed to.



2. A firewall is not usually a single device

Firewall Best Practices

- Except in the most simple of cases, a firewall is seldom a single device; it is usually a collection of devices acting in concert.
- Even if you buy a commercial "all-in-one" firewall appliance, you'll still have to configure other machines (your public web server, for example) to work along with it.
- And these other machines should really be regarded as part of the firewall.
- This has all sorts of implications for how you configure and manage these machines, what they trust, what trusts them, and so on.
- You cannot simply choose one box, call it "the firewall," and expect it to assume all responsibility for security.



3. Firewalls are not off-the-shelf items

Firewall Best Practices

- **Selecting a firewall is more like buying a house than choosing where to go on vacation.**
- **Firewalls and houses are complicated, you have to live with them every day, and you use them for more than just a week or two.**
- **Both need to be maintained, otherwise the weather gets to them or they fall apart.**
- **Building a firewall requires carefully selecting and configuring a solution that meets your needs, and then consistently maintaining it over time.**
- **There are a lot of decisions to be made, and the answer that's right for one site may be completely wrong for another.**



4. A firewall will not solve all problems

5. Use a default deny policy

- **Don't expect a firewall to give you security all by itself.**
 - A firewall protects you from a certain class of threats, where people on the outside attempt to attack the inside directly.
 - It won't protect you from people on the inside; it won't even protect you from every attack from the outside; just those it can detect.
- **Your normal approach should be to deny everything and only allow things you know are both necessary and safe.**
 - New vulnerabilities arise every day; trying to shut out just what's unsafe means fighting a constant battle to keep up.



6. Give in gracefully, but not easily

Firewall Best Practices

- People will always want to do unsafe things.
- If you allow every request, you will end up with an insecure network.
- If you deny every request, you will still end up with an insecure network; you just won't know where the insecurities are because people will have hidden them from you.
- People who cannot work with you will work around you every time.
- You need to find ways to meet people's needs, even if those ways involve some amount of controlled risk.



7. Use a layered approach

8. Only install what you need

Firewall Best Practices

- **Don't depend on a single device in a single place.**
 - Instead, put together multiple layers of security, so that no single failure will immediately compromise what you care most about.
- **Firewall machines should not be configured with a vendor's complete software distribution like normal computers.**
 - Any machine that is part of a firewall should be stripped to a bare minimum.
 - Even if you think something is safe, don't install it unless you actually need it.



9. Use all available resources

10. Trust only what you verify

Firewall Best Practices

- **Don't build a firewall based on information from a single source, particularly if that source is not a vendor.**
 - There are a large number of resources available: vendor information, books, mailing lists, and web sites, for examples.
- **Don't trust the manual, the check boxes in the graphical user interface, or the vendor's statements about the way something works.**
 - Test to make sure connections that should be denied are denied.
 - And test to make sure connections that should be allowed are allowed.



11. Reevaluate decisions over time

12. Expect failure

Firewall Best Practices

- **The house you bought five years ago may not be the one that suits your needs today.**
 - Similarly, the firewall you installed a year ago may no longer be the best solution for your situation today.
 - With a firewall you should regularly reevaluate your decisions and needs to make sure you still have an appropriate solution.
 - Changing your firewall, like moving to a new house, will require significant effort and careful planning.
- **Plan for the worst.**
 - Machines will go down, well-intentioned people will do the wrong thing, evil-intentioned people will succeed in damaging you.
 - But make sure it's not a total catastrophe when these things happen.



Definitions relating to Firewalls

- **Firewall**
 - A component or set of components that restrict access between a protected network and the Internet, or between other sets of networks.
- **Host**
 - A computer system attached to a network.
- **Bastion Host**
 - A computer system that must be highly secured because it is vulnerable to attack, usually because it is exposed to the Internet and is a main point of contact for users of internal networks.
- **Packet**
 - The fundamental unit of communication on the Internet.



More Definitions

- **Perimeter network**
 - A network added between a protected network and an external network, in order to provide an additional layer of security.
 - A perimeter network is sometimes called a DMZ.
- **Proxy**
 - A program that deals with external servers on behalf of internal clients.
 - Proxy clients talk to proxy servers, which relay approved client requests on to real servers and relay answers back to clients



NAT

- **Network address translation (NAT)**
 - A procedure by which a router changes data in packets to modify the network addresses.
 - This allows a router to conceal the addresses of network hosts on one side of it.
 - This technique can enable a large number of hosts to connect to the Internet using a small number of allocated addresses or can allow a network that is configured with illegal and unroutable addresses to connect to the Internet using valid addresses.
 - Not an actual security technique, but provides some small degree of protection.
 - Generally NAT runs on the same routers that make up part of the firewall



Packet Filtering

- The action a device takes to selectively control the flow of data to and from a network.
- Packet filters allow or block packets, usually while routing them from one network to another (most often from the Internet to an internal network and vice versa).
- To accomplish packet filtering, you set up a set of rules that specify what types of packets (e.g., those to or from a particular IP address or port) are to be allowed and what types are to be blocked.
- Packet filtering may occur in a router, in a bridge, or on an individual host.



Packet Header Information

- **IP Source Address**
- **IP Destination Address**
- **Protocol (i.e. TCP, UDP, ICMP packet)**
- **TCP or UDP source port**
- **TCP or UDP destination port**
- **ICMP message type**



How Packet Filtering Works

- **Routers know things not reflected in packet headers**
 - The interface the packet arrives on
 - The interface the packet will go out on
- **Routers can track packets historically**
 - Whether this packet seems to be a response to another packet
 - Source was the destination of a recent packet and its destination is the source of that other packet
 - How many other packets have recently been seen to or from the same host
 - Whether this packet is identical to a recently seen packet
 - If this packet is part of a larger packet that has been broken into parts (fragmented)



Packet Filtering Options

- **Basic routers**
 - **Send** the packet to its destination
 - **Drop** the packet – just forget it, without notifying sender
 - **Reject** the packet – refuse to forward it and return error to sender
 - **Log information** about the packet
 - **Set off an alarm** to notify someone about the packet immediately
- **More sophisticated routers**
 - **Modify** the packet (do a NAT for instance)
 - **Redirect** -- send the packet on to a destination other than the one that it was bound for (force transactions through a proxy server or perform load balancing)
 - **Modify the filtering rules** (for instance, to accept replies to a UDP packet or to deny all traffic from a site that has sent hostile packets)



Programming a Screening Router

- **Block all incoming connections from systems outside the internal network except for incoming SMTP connections (so that you can receive email)**
- **Block all connections to and from certain systems you distrust**
- **Allow electronic mail and FTP services, but block dangerous services such as:**
 - TFTP
 - Remote X
 - RPC
 - rlogin
 - rsh
 - rcp



Disadvantages of packet filtering

- Packet filtering reduces router performance
- Packet filtering rules are often hard to configure
 - Level of difficulty ranges
 - From slightly mind twisting to brain-numbingly impossible
- Once configured, filtering rules can be hard to test
- Packet filtering capabilities of many of the products are incomplete, making implementation of certain types of highly desirable filters difficult or impossible
- Packet filtering packages may have bugs in them
 - These defects CAN result in serious security problems
 - Usually a proxy that fails simply stops passing data, while a failed packet filtering implementation may allow packets it should have denied



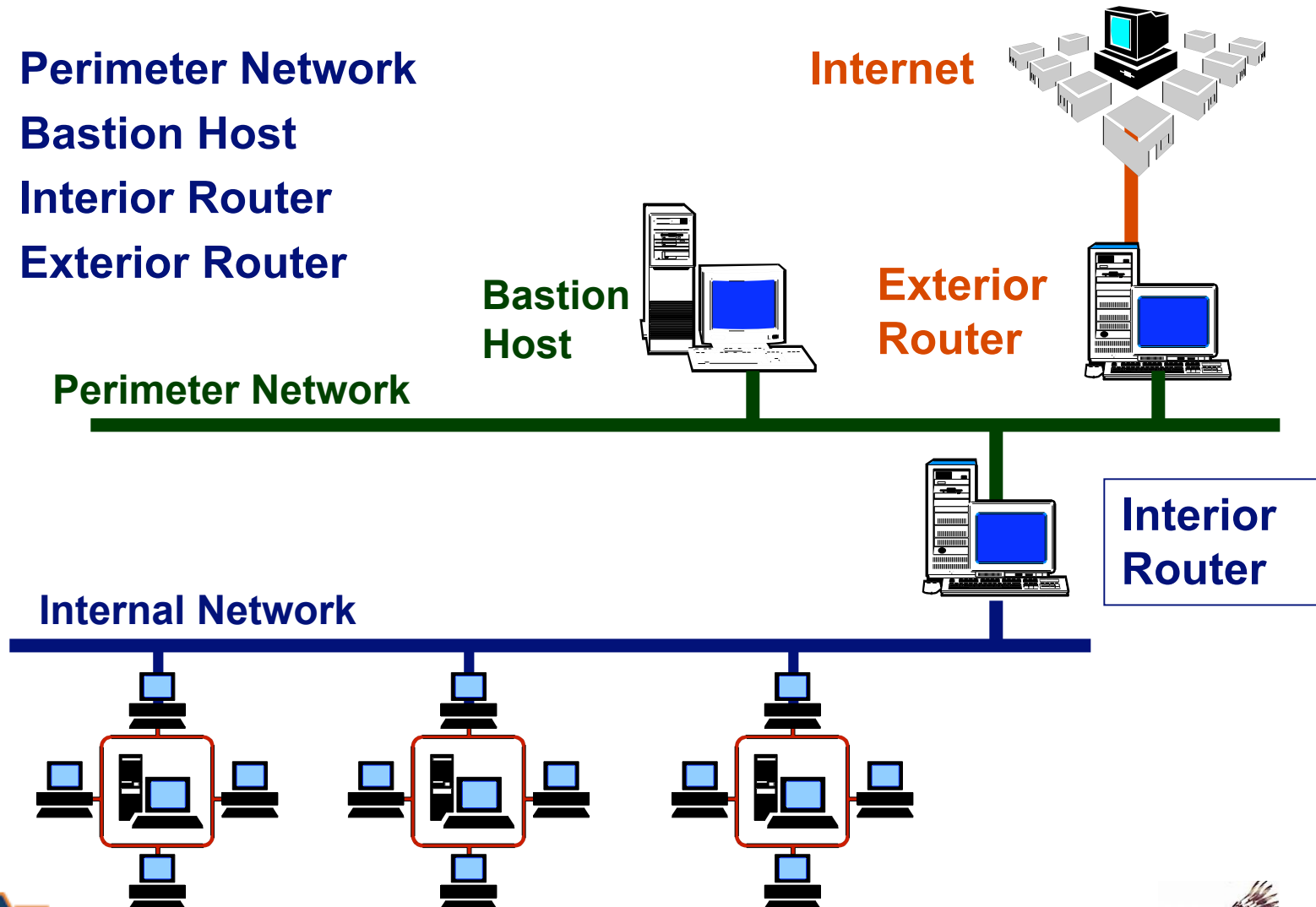
DMZ

- **A Demilitarized Zone is used by a company that wants to host its own internet services without sacrificing unauthorized access to its private network.**
- **The DMZ sits between the Internet and an internal network's line of defense, usually some combination of firewalls and bastion hosts.**
- **Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.**



Screened Subnet Architectures

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



Perimeter Network

- An additional network between the external network and the protected internal network
- In many network configurations, it is possible for any machine on a given network to see the traffic for every machine on that network
 - Ethernet for example
- Snoopers can watch for passwords during telnet, FTP and rlogin sessions
 - File transfers can also be monitored
- On a perimeter network, only the traffic on that net can be monitored
 - Traffic between the bastion host and the ROTW can still be monitored
 - Strictly internal traffic require another level of compromise



Bastion Host

- **Bastion host is the main POC for incoming connections from the outside world such as....**
 - Incoming email (SMTP) sessions to deliver electronic mail to the site
 - Incoming FTP connections to the site's anonymous FTP server
 - Incoming Domain Name System (DNS) queries about the site
- **Outbound services (from internal clients to servers on the Internet) are handled either of these ways....**
 - Set up packet filtering on both interior and exterior routers to allow internal clients to access external servers directly
 - Set up proxy services to run on the bastion host to allow internal clients to access external servers indirectly.
 - Also set up packet filtering to allow the internal clients to talk to the proxy servers on the bastion host and vice versa, but to prohibit direct communications between internal clients and the outside world
- **How to secure a bastion host will be addressed later**



Interior Router

- Sometimes called a choke router
- Protects the internal network both from the Internet and from the perimeter net
- Interior router does most of the packet filtering
 - Allows selected services outbound from the internal net to the Internet
 - These services are the services your site can safely support and safely provide using packet filtering rather than proxies
 - You have to decide what is safe
 - Services the interior router allows between your bastion host and your internal network are not necessarily the same services the interior router allows between the Internet and the internal network



Exterior Router

- Sometimes called an access router
- Generally do little packet filtering
 - Rules have to be essentially on the interior and exterior routers, so a flaw in one will likely compromise the other
 - Some filtering can be done to secure the bastion host – but other techniques are typically used to secure the bastion
- Exterior routers often provided by an external group
 - Internet Provider
 - OIT
- Exterior routers can and do block any incoming packets that have forged source addresses
- Filtering outbound packets does limit the ability of miscreants to use your network for further malevolent activity



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

