VPN “What is it” and “How do I”

LightSys Technology Services, Inc.

Summary

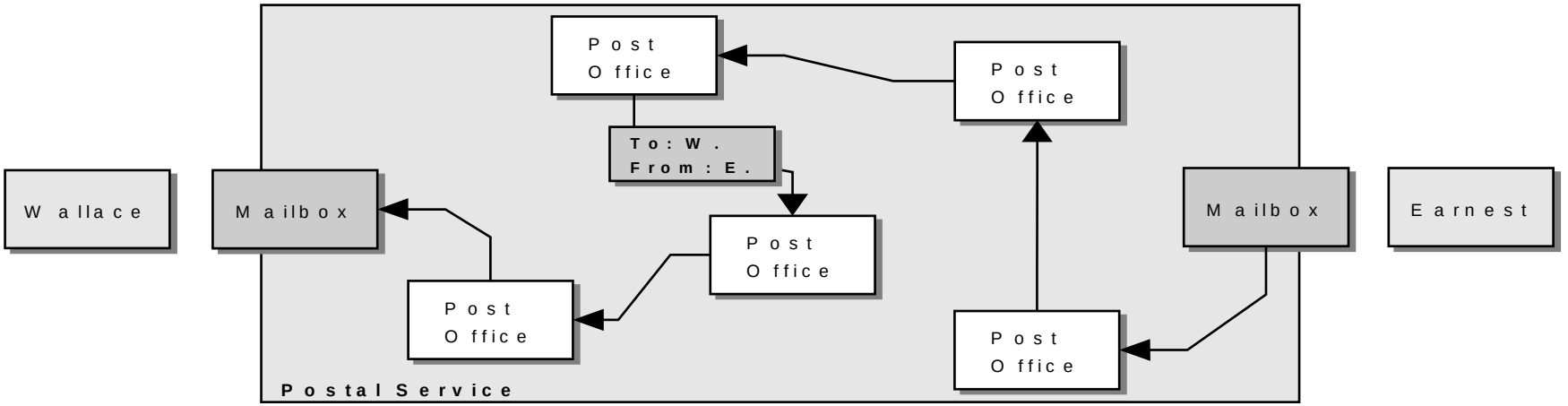
- IP Tunneling (Packet Encapsulation)
- Encrypted Tunnels
- Virtual Private Networking (VPN)
- VPN Technologies

Packet Encapsulation

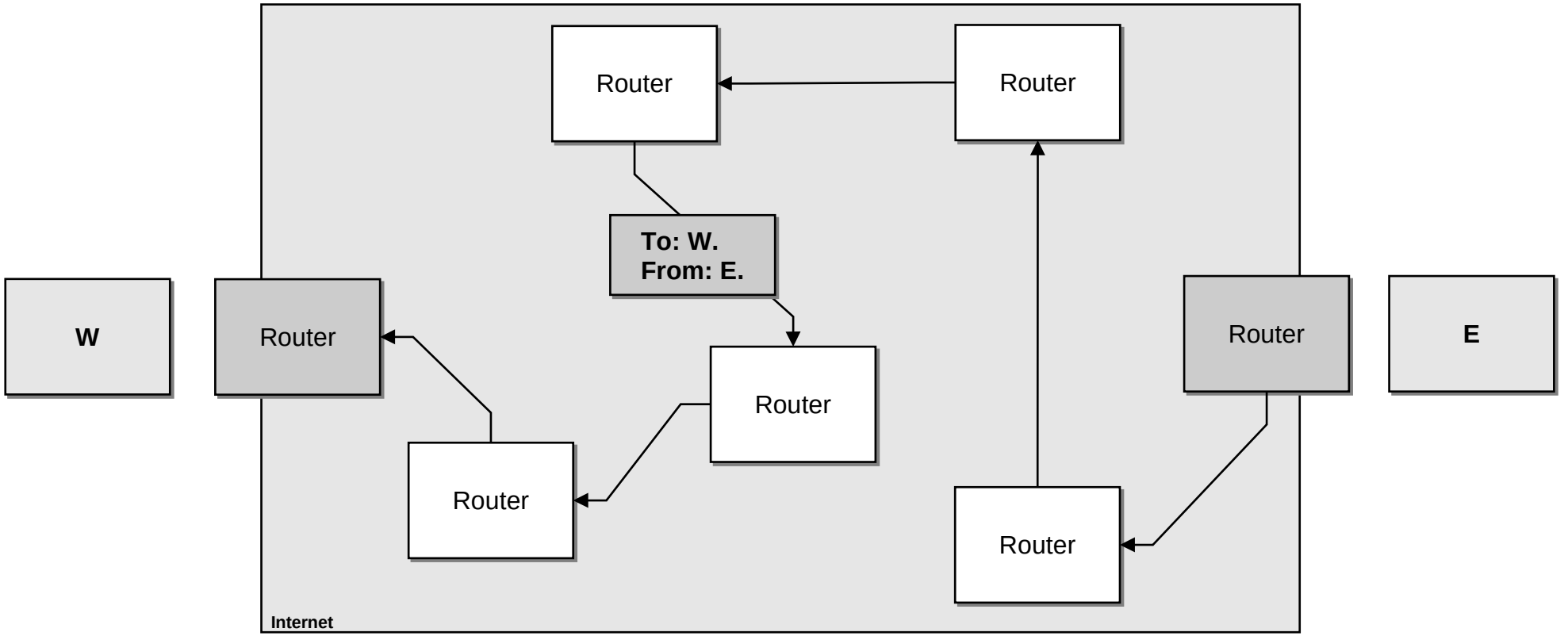
- Putting one packet inside another
  - Taking a packet addressed to one person
  - Putting that packet inside a larger package which is addressed to someone else
  - Upon arrival, the original package is removed from the larger one
  - The original package is then delivered as appropriate on the original address.

The concept of tunneling

- Earnest on the East coast
- Wallace on the West coast
- E sends W a package via post-office

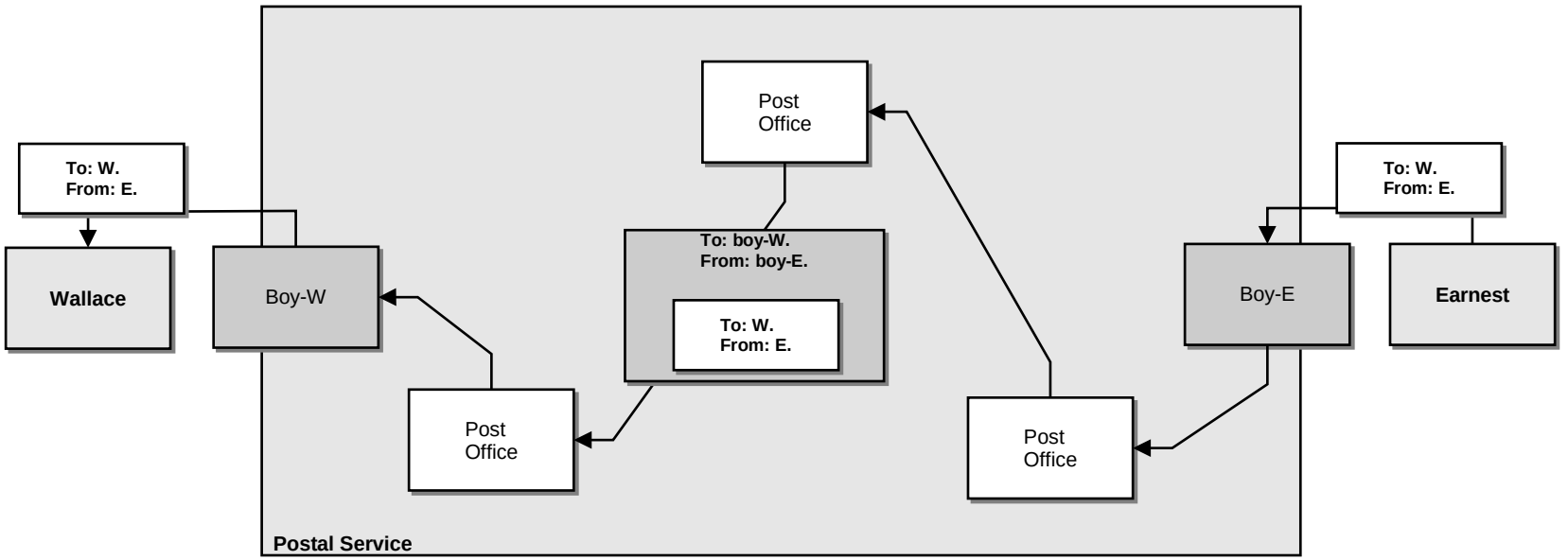


Postal vs. Internet version

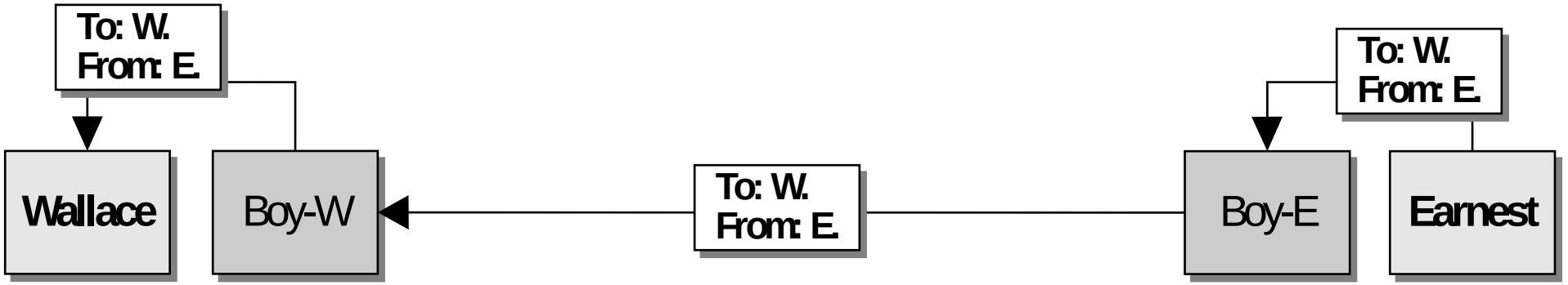


Packages through a tunnel

- Earnest and Wallace each have office boys
- Earnest and Wallace just give the package to the boys and let them deal with it.

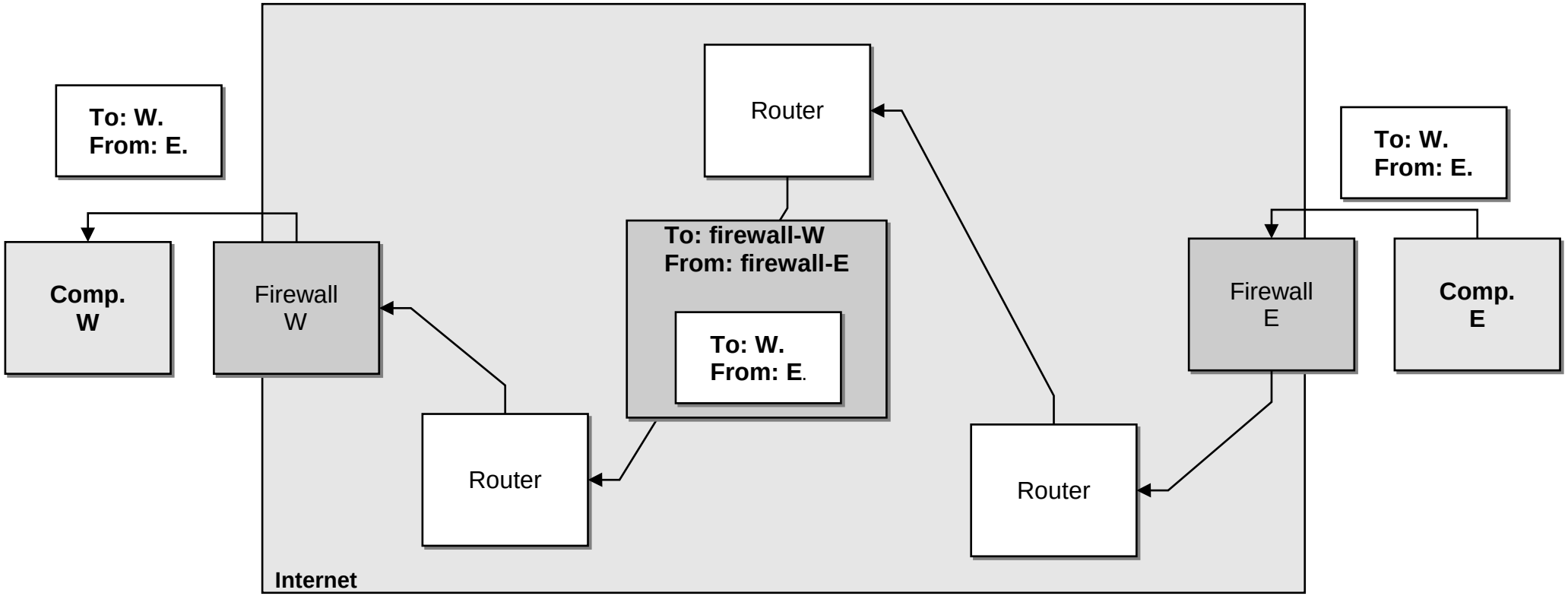


Looking at it simply

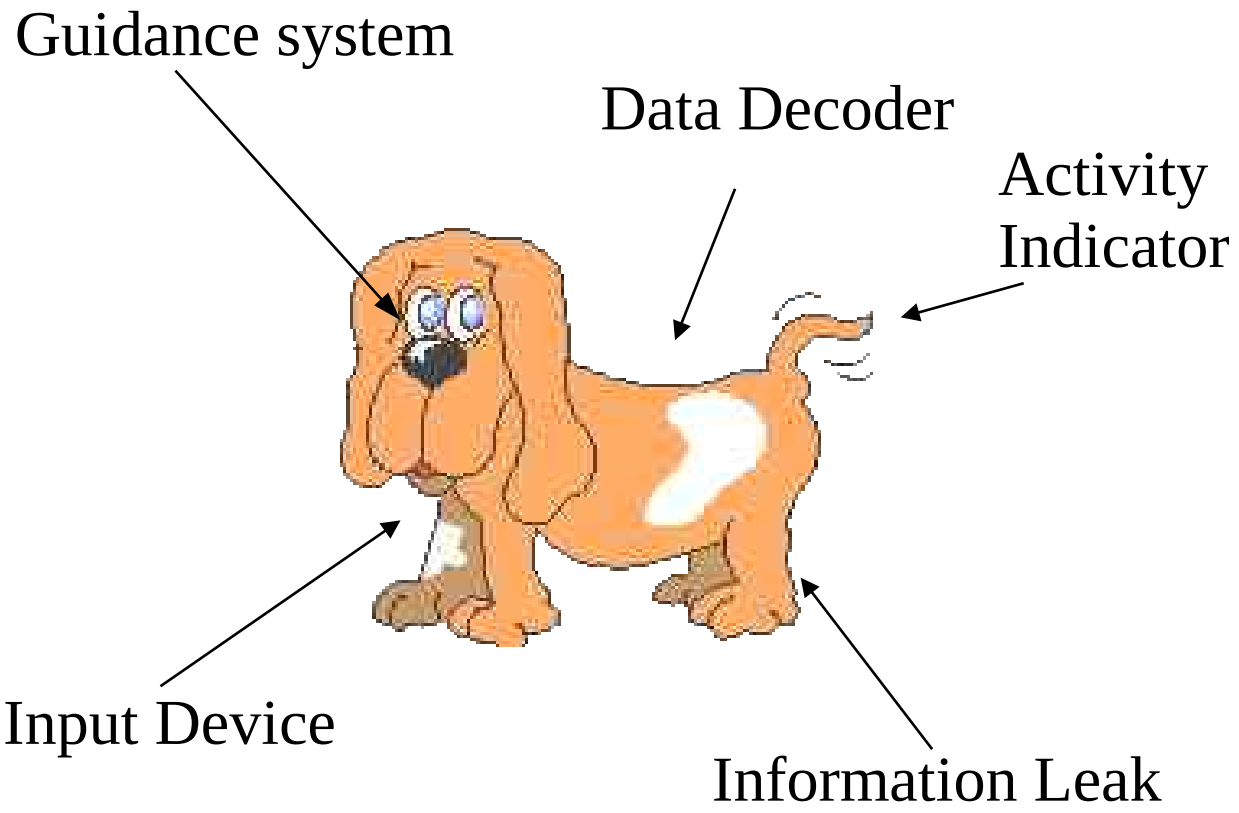


Looking at tunneling electronically

- Firewalls take the place of the boys
- Routers take the place of the postal people

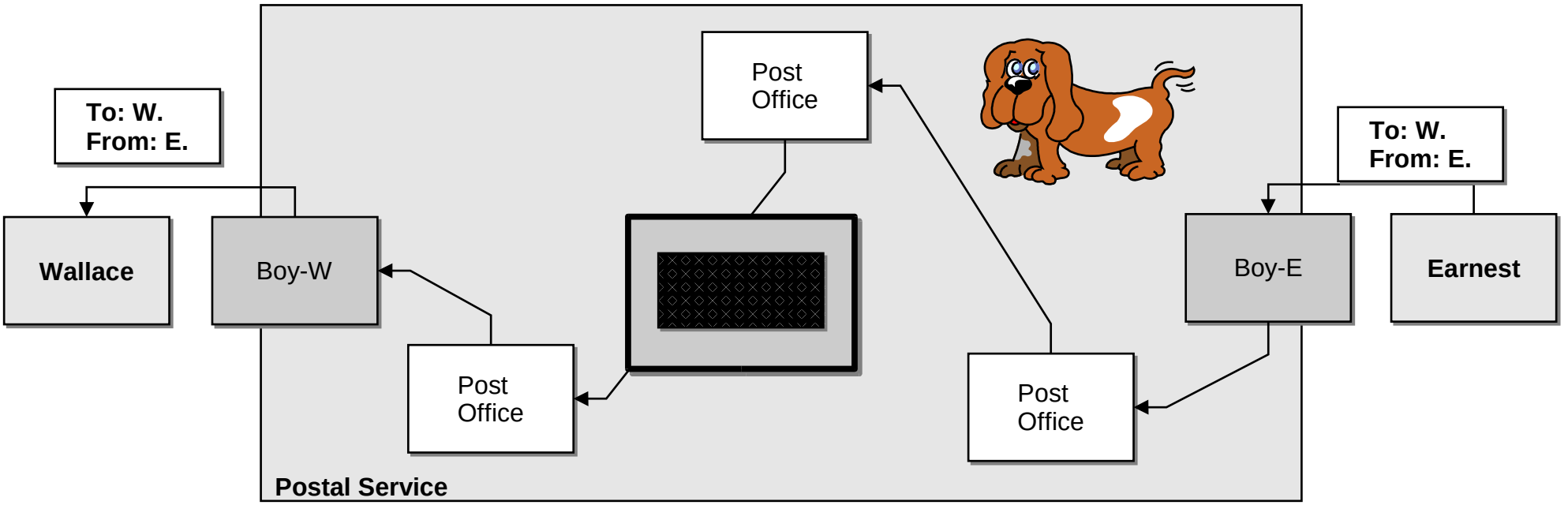


Introducing the packet sniffer

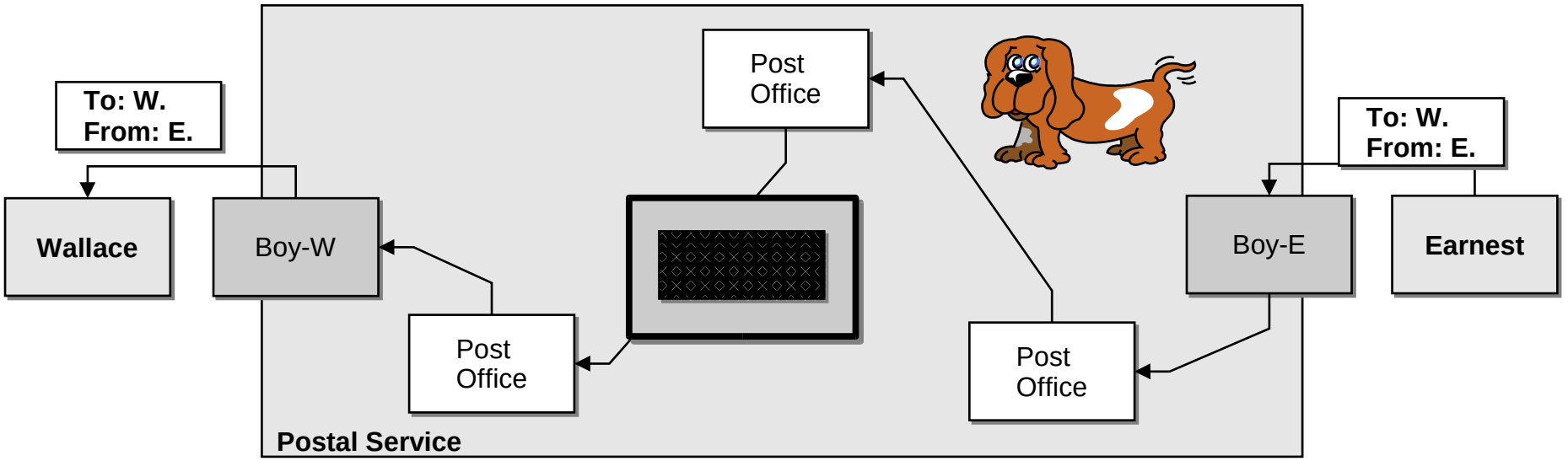


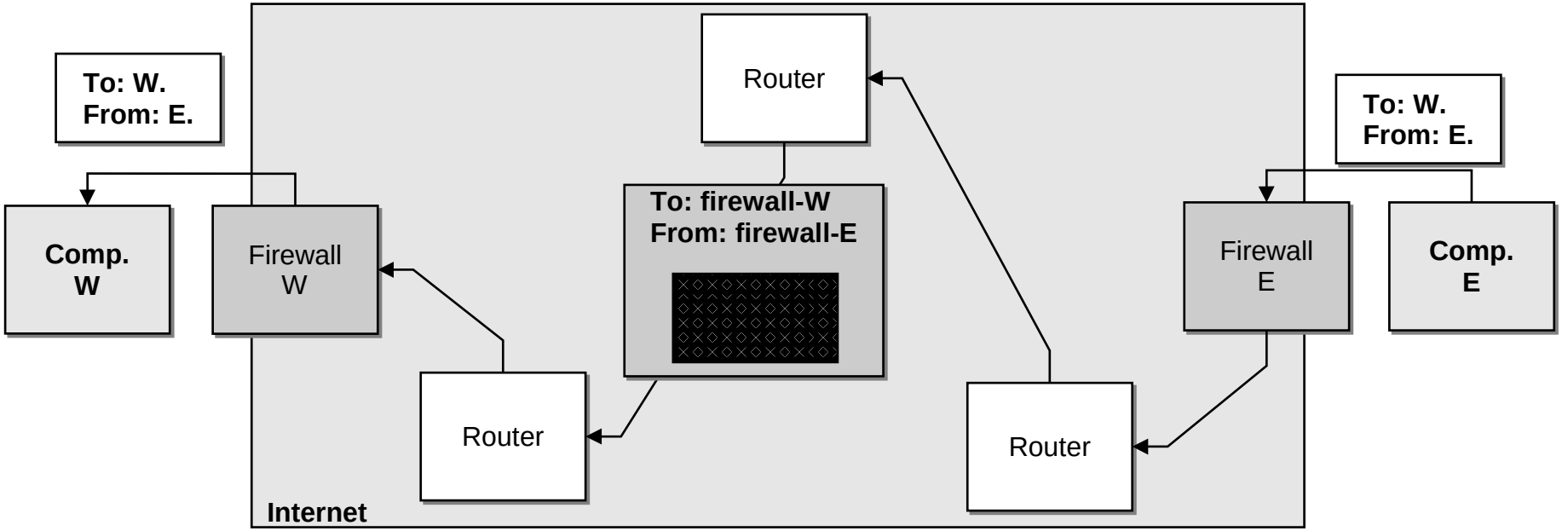
Encrypted Tunnels

- The boys put everything in airtight safes to send back and forth
- The sniffer cannot smell the secure cookies



Postal vs. Electronic



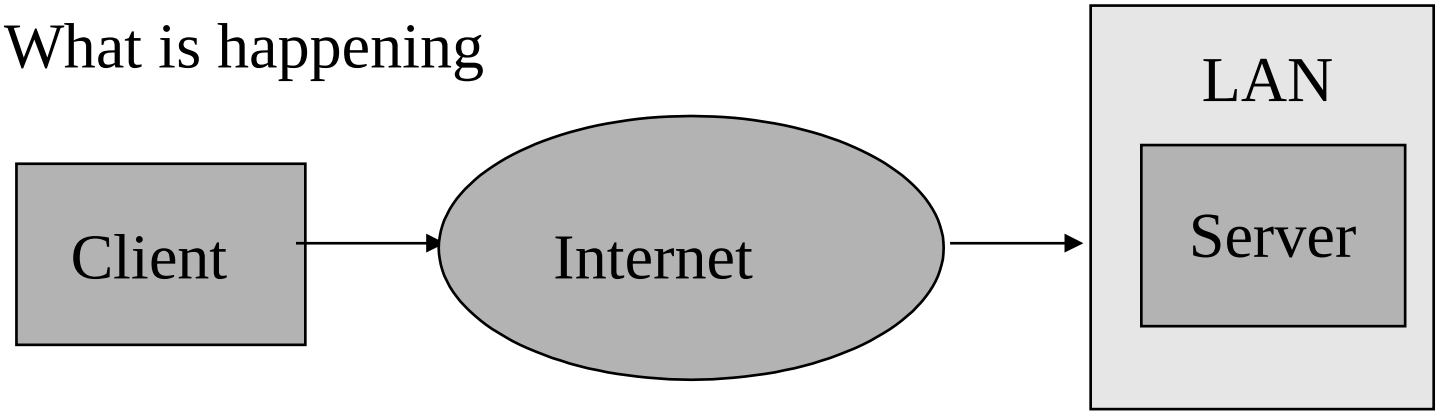


Virtual Private Networking (VPN)

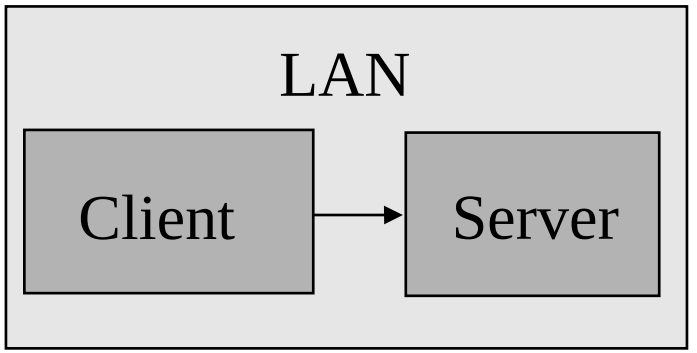
- A VPN is specially crafted tunnel
- A VPN allows you to transparently connect two offices (or a remote user to an office) in a secure manner so that the offices can communicate as if they were directly connected in the same building, but do so across a public network (such as the Internet or a frame relay network).

VPN The Basics

What is happening

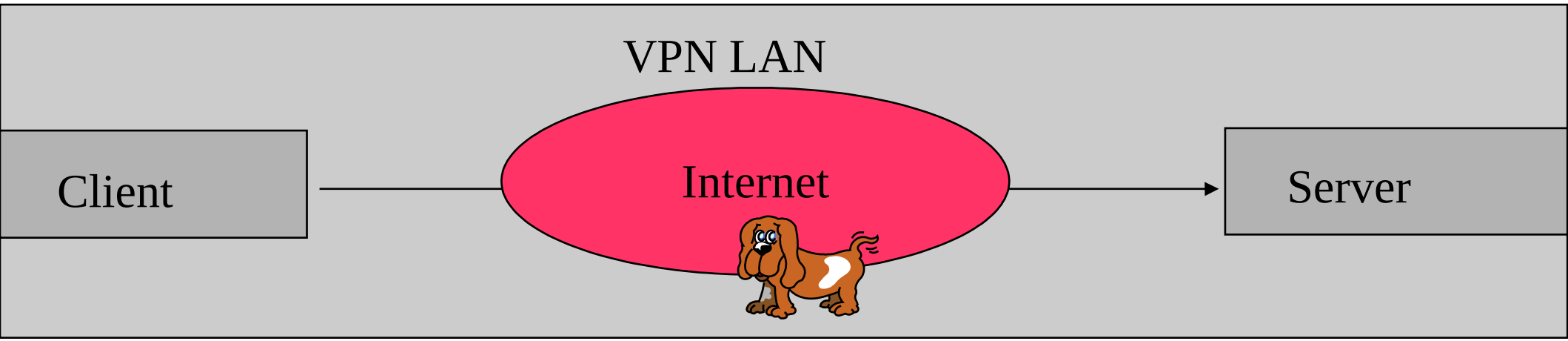


What it looks like



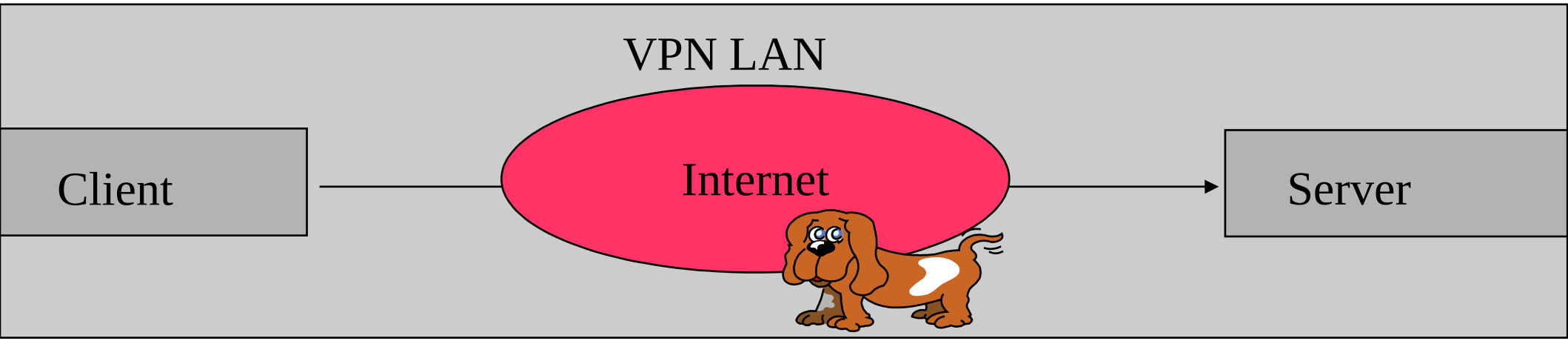
VPN Introduction

- Authenticating across a VPN (across the Internet) can be interesting.



VPN Introduction

- Better to have encryption



VPN The Basics

- Tunneling and Encryption....
  - To keep matters simple, we will cover just a few of the current favorites VPN technologies.
  - They all use a "tunnel" to connect the computers
  - Both the client and server need to think they each have an address "local" to each other, which is why you need to use a tunnel.

VPN The Basics

- Tunneling and Encryption....
  - Once you have a tunnel set up, you will have a different IP address associated with that tunnel than you have with your connection to the Internet.
  - That IP address should be the same as one on the LAN to which you are connecting.
  - From the server side, you will see that the VPN server is receiving the packets for the client IP.
  - This makes the client appear as if it is on the LAN, and not as if it were an untrusted computer on the Internet.

VPN The Basics

- Tunneling and Encryption....
  - The second half of a VPN is encryption.
    - You will want to have an encryption layer on the VPN so that you can trust that unscrupulous (or scrupulous) folks along the way are not snatching up your LAN traffic.
  - We will explain VPNs, usually by two technologies.
    - First by the tunneling technologies involved,
    - Then by the encryption technologies.

VPN An Example (PPTP)

- PPTP comes bundled with Win95 and higher.
  - This is simply called "Microsoft VPN" on your computer, the technical name for it is PPTP (Point-to-Point Tunneling Protocol).
- PPTP is simple
- By default does not have encryption enabled
- And therefore insecure by default
  - though you can turn encryption on

VPN An Example (PPTP)

- Say you had a dial-up client in the Arctic
- A server based in the US with a dedicated Internet connection.
- When the client dials-up, it is indistinguishable from the other computers on the Internet as far as the server is concerned.
- The server wants to block everyone.

VPN An Example (PPTP)

- The client starts the VPN.
- Handshakes on port 1723
- Authenticates itself via unencrypted (plain text) password
- Makes a tunnel between the two computers using PPP (Point-to-Point Protocol).
  - PPP is the basic protocol for connecting a dial-up computer to the Internet, so the infrastructure is pretty simple.

VPN An Example (PPTP)

- To conect to the LAN
  - Your browse master needs to be aware of the client so it can display it on the browse-list, as well as passing the browse list back to the client so it can see the rest of the network.
    - If your VPN server is on the same machine as your file and printsharing server, this usually requires no other configuration.
    - Otherwise you need to have a WINS server, and your client needs to point to it.
  - And finally, you will want to log onto the network if you have a PDC.

VPN An Example (PPTP)

- To conect to the LAN
  - Once the VPN has been established, the client goes through the same procedure for authentication as if it were on the LAN.
  - This means passing the passwords across the Internet. No wonder they added encryption to VPNs!

VPN An Example (PPTP)

- Encrypting the VPN....
  - PPTP on the client has a check-box that allows you to encrypt your VPN connection.
  - From the server end, you can also state that you will not accept an insecure connection.
  - The initial handshaking is done unencrypted, but the remaining communication, including password verification, is done through an encrypted format.
  - For PPTP, this is done through MPPE which uses GRE packets (protocol 27).

VPN An Example (PPTP)

- Encrypting the VPN....
  - Note: GRE packets are not TCP/IP packets. They use IP, but are their own protocol, and many older firewalls cannot handle it.
    - Most equipment today can handle it, but you still often need to specifically specify that you are going to use it.
    - Read the manual for any firewalling equipment you use before commit to using PPTP with encryption.
    - Linux can handle GRE, but you need to recompile the kernel of the Linux machine you use to connect to the VPN.

VPN Technologies

- Overview
  - You have a cross-reference which you can refer to throughout the session.
  - It names the protocols
  - It explains how they interact with each other.

VPN Technologies

- PPP, the Point-to-Point Protocol....
  - The original use of PPP was with a dial-up connection to the Internet.
    - A point-to-point connection is set up over the phone line.
    - The client computer is given an IP address
    - The server forwards all traffic for the client across the phone link.
  - The extension to a VPN protocol is fairly simple.
    - Instead of a phone line, a tunnel is set up as the point-to-point connection.
    - An IP address is given to the client
    - The VPN server forwards all traffic for the client across the tunnel link.

VPN Technologies

- IP-in-IP Tunneling....
  - Described in the "tunneling" section of this workshop.
  - Works through simple encapsulation of each TCP/IP packet, giving a different source and destination to the packet.
  - The only modification to the original packet is in changing the TTL (Time to live) for the data to allow packets to be dropped when needed.

VPN Technologies

- IP-in-IP Tunneling....
  - IP-in-IP has no encryption
  - IP-in_IP has no real handshaking.
  - You can inadvertently successfully set up a single-ended tunnel, where the packets are shipped off into never-never land.
  - There is no authentication done on packets, and no handshaking to let the sender know if packets did not arrive, unless supplied in the connections going across the IP-in-IP tunnel (which is usually the case).

VPN Technologies

- PPTP....
  - PPTP is the modification of the PPP protocol for tunnels.
  - By default it has no encryption.
  - It can use CHAP or MS-CHAP authentication
    - CHAP sends plain-text passwords,
    - MS-CHAP(1) has an easily broken encryption,
    - MS-CHAP(2) fixes the most glaring security issues.
  - The encrypted PPTP is sent over GRE (Generic Routing Encapsulation) packets.

VPN Technologies

- PPTP....
  - MPPE is used to encrypt PPTP.
  - MPPE uses the RSA RC4 algorithm.
  - The length of the session key to be used for initializing encryption tables can be negotiated to 40-bit or 128-bit.
    - 40 bit is horribly insecure - use 128 bit
  - PPTP works on many platforms, but to set it up with encryption on Linux at this time requires a kernel rebuild.

VPN Technologies

- L2TP (Layer 2 Tunneling Protocol, named after the layer 2 in the OSI model)
  - L2TP is another tunneling protocol that does not include encryption.
  - One of the neat things about L2TP is that it can tunnel more protocols than just TCP/IP
    - NetBEUI, IPX/SPX, etc.
    - Most people do not want these other protocols on their LAN any more unless they have a Novell server.
  - Windows 2000 and XP have native drivers for L2TP.

VPN Technologies

- L2TP....
  - The most common way to add encryption to L2TP is by using IPSec.
  - With IPSec the L2TP packets get encrypted before they are sent and are unencrypted at the other end, so none of the original packet is visible.

VPN Technologies

- IPSec....
  - IPSec is an encryption and authentication protocol that can do tunneling also.
  - It uses three main components.
    - ESP (Encapsulating Security Payload) to encrypt and/or authenticate data
    - AH (Authentication Header) to provide a packet authentication service
    - IKE (Internet Key Exchange) to negotiate connection parameters, including keys, for the other two.

VPN Technologies

- IPSec....
  - IPSec only uses 3DES at this time for the data encryption.
  - It uses other cryptography for authentication (HMAC with MD5 or SHA)
  - It uses Diffie-Hellman key agreement.
  - Many firewalls support IPSec natively, so it has a high probability of fitting into your network scheme.

VPN Technologies

- SSL....
  - SSL is an authentication and encryption transport protocol that can be layered over other protocols.
  - SSL is not guaranteed to be secure.
    - It will negotiate security protocols the same way a modem negotiates the speed of it's connection.
    - Just as your modem does not always connect at as high a speed as you would like it to, SSL does not always provide the maximum security we would like - much depends on the server.

VPN Technologies

- SSL....
  - The server can be configured as to which types of authentication to negotiate first, and which ones to negotiate to.
  - Older browsers may not support the newer encryption protocols, 128 bit encryption.
  - You can configure your server to not negotiate to anything but high-strength encryption.
- Stunnel is a package that creates a tunnel over SSL.
  - It can be used in VPN packages to run ip-in-ip or PPP over SSL.

VPN Technologies

- CIPE....
  - CIPE is a stable, though not highly supported VPN tool that currently only really works for Windows NT/2000 and Linux machines.
  - It is a light-weight protocol using UDP packets and the Blowfish cipher.
  - CIPE creates an encrypted tunnel similar to that of PPTP.
  - It does not have the authentication schemes that IPSec has.
  - The CIPE protocol does work through firewalls well and is simple to set up.

VPN Technologies

- CIPE....
  - On recent Linux systems, CIPE is available in the kernel,
  - On older Linux systems you will have to rebuild the kernel to make it work.

VPN Technologies

- SSH....
  - SSH is an application layer protocol
    - It has some interesting features to allow it to be used in a VPN setup.
  - By itself, SSH simply authenticates and executes remote programs on the server computer.
  - The basic SSH commands are:
    - SSH (Secure SHell)
    - SFTP (Secure FTP)
    - SCP (Secure Copy)

VPN Technologies

- SSH....
  - SSH allows you to do port forwarding over the secure channel it sets up.
  - Originally this was to allow you to export your Xwindows display across the secure link.
  - It was simple to set it up to export other ports, so that was added also.

VPN Technologies

- SSH....
  - Then someone wondered if they could run PPP over a SSH channel.
  - With a little effort, they were able to do so.
    - This created a secure PPP link
    - Set up the tunnel end-points
    - Encrypted all the information in-between

VPN Technologies

- Mixing Protocols....
  - Much of the strength of your VPN comes from mixing protocols.
  - Because IPSec has such good authentication and security, it is often used in conjunction with another tunneling protocol to create a very strong VPN.
  - We will not discuss all the possible combinations of the protocols we have listed.
  - It should be noted that IPSec, while also used in conjunction with other protocols, can be used as a tunnel in it's own right
    - many VPNs only use IPSec.

VPN Technologies

- L2TP + IPSec....
  - L2TP over IPSec is one of the more secure and flexible VPN configurations.
    - It has the strong security of IPSec,
    - It has the flexibility of L2TP.
  - A number of vendors are offering solutions that adhere to these standards. (see www.vpnc.org)

VPN Technologies

- L2TP + IPSec....
  - With Windows 2000 and XP, Microsoft has launched it's second attempt at a good VPN solution.
  - From it's outside appearance, it uses standard implementations of L2TP and IPSec to build it's VPN.
  - Microsoft has drifted from a few of the standards, which may cause headaches under some circumstances.

VPN Technologies

- PPP + SSH....
  - PPP over SSH really only works on Linux or other Unix based derivatives.
  - The originator of the "ppp-ssh HowTo" writes: "I believe that the ssh/ppp technique is no longer beneficial for building a VPN for non-illegal purposes in most cases, so I have discontinued maintaining this HOWTO."
    - This does not mean that PPP/SSH is inherently illegal
    - It just that it may look less like a VPN than other VPN setups
    - statistical analysis of the timing/sizes of packets might suggest that VPN activity is likely

VPN Technologies

- PPP + SSH....
  - PPP over SSH has some technical problems and is very complex to set up.
  - It does have some interesting benefits.
    - It is difficult to recognize it as a VPN because of the nature of the protocol (it may appear to be simple SSH traffic).
    - It also requires less configuration through firewalls, as ssh traffic is simple to handle.
    - Furthermore, it can be used out-of-the-box on nearly all Linux kernels without recompiling.

Some Definitions

- Transport Layer Protocol:
  - The Transport Layer is the 4th layer in the OSI model.
  - It takes care of end-to-end control, error checking, and making sure all packets arrive.

Some Definitions

- Transport Layer Encapsulation Protocol:
  - The Transport Layer is the 4th layer in the OSI model.
  - It takes care of end-to-end control, error checking, and making sure all packets arrive.
  - A transport layer encapsulation protocol takes the contents at the transport layer and repackages them (often encrypting at the same time).

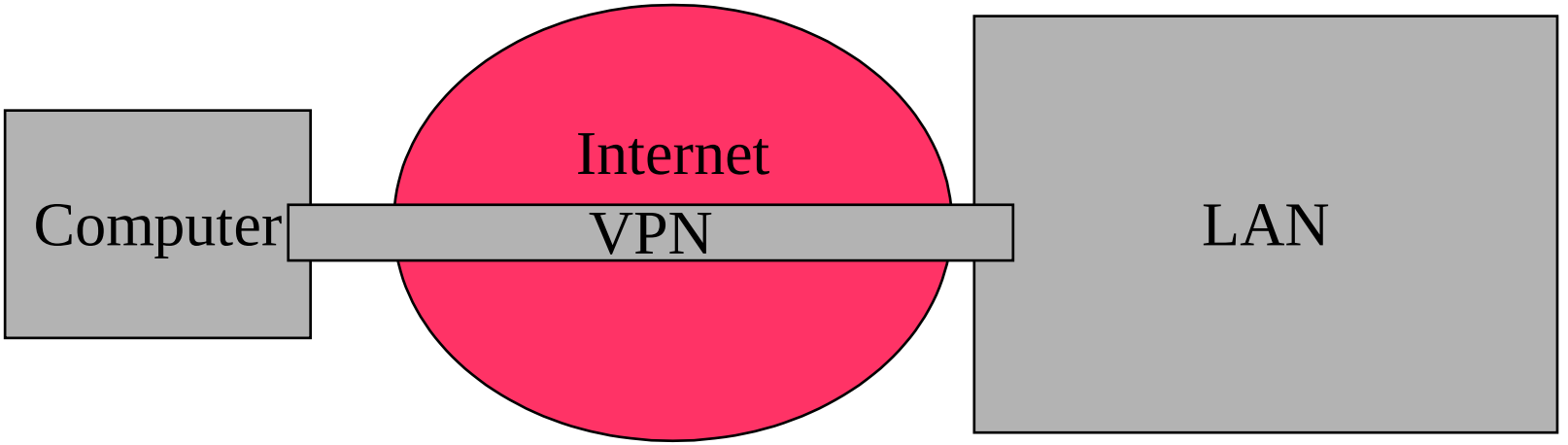
Some Definitions

- Application-Layer Protocol:
  - The application layer is layer 7 in the OSI model.
  - It deals with user authentication, privacy, and constraints on data and syntax.
  - Examples of application layer protocols are
    - Telnet
    - HTTP
    - FTP
    - SSH
    - Etc.

Where do you use a VPN?

When traffic originates from an untrusted segment.

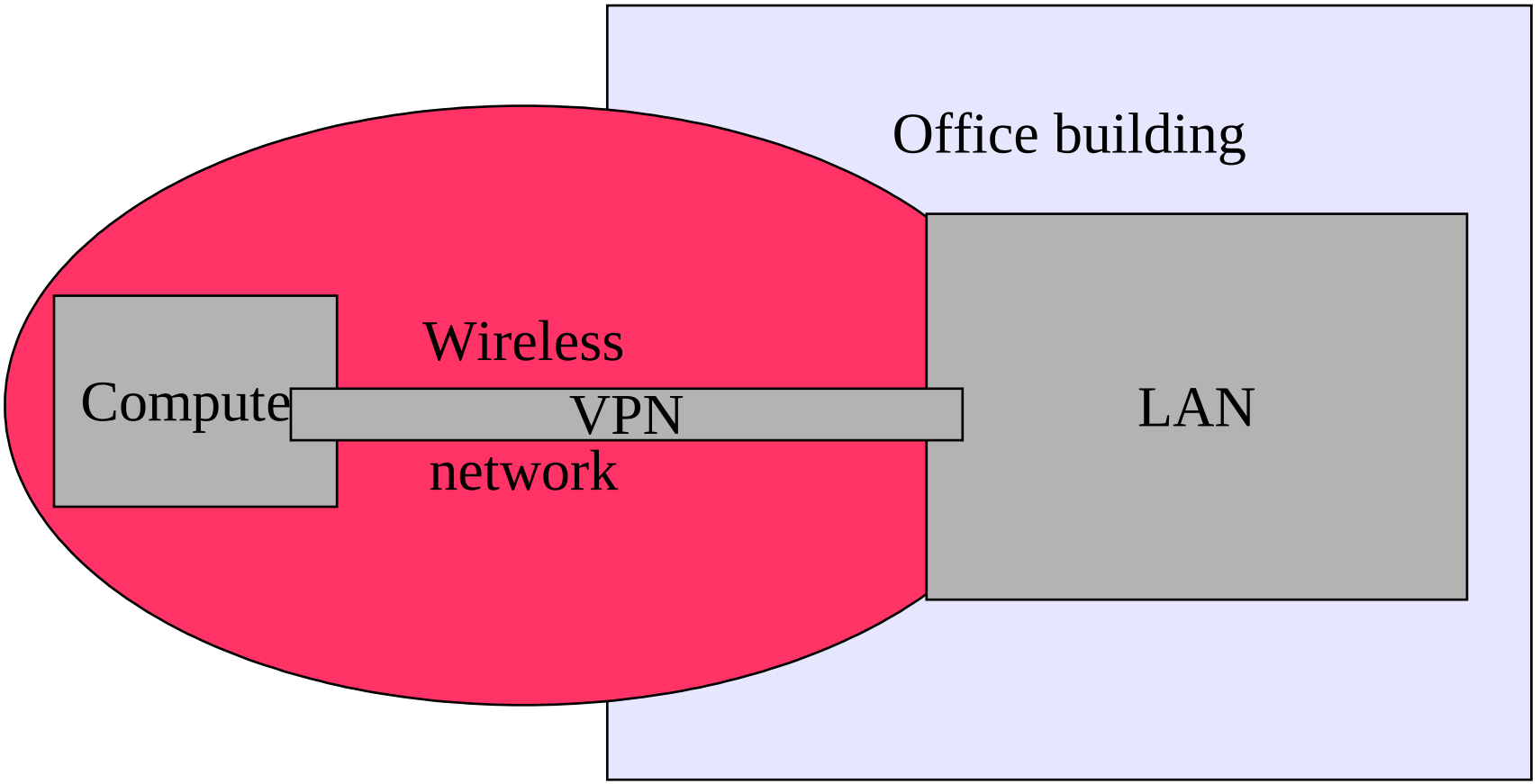
When connecting to the LAN from the outside



Where do you use a VPN?

When traffic originates from an untrusted segment.

Computers connecting over wireless



Where do you use a VPN?

When traffic flows across an untrusted segment.

LAN connecting to LAN