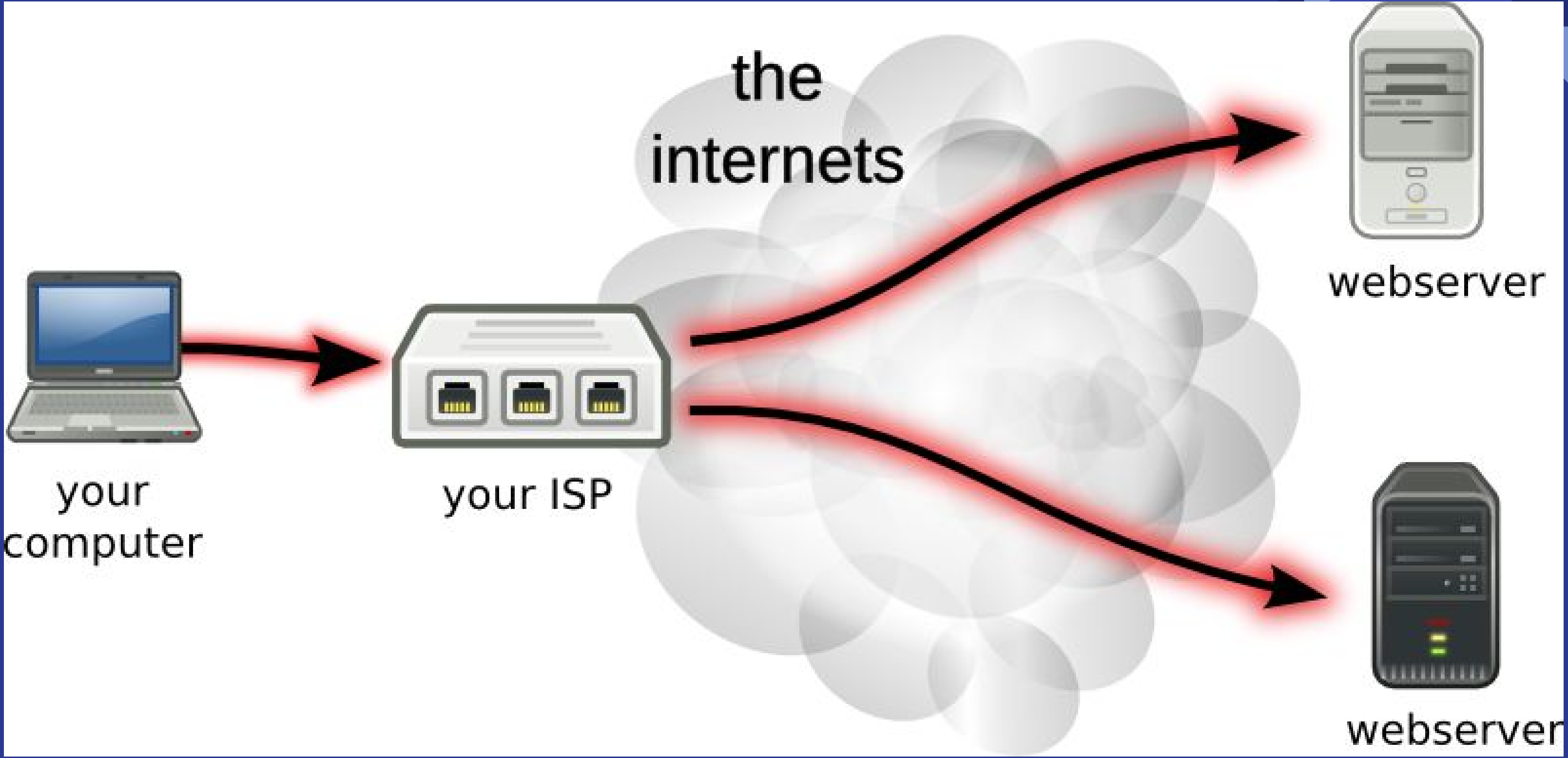
Virtual Private Network

By: Kelvin Kong, Ertan Aksoy, Aditya Arora

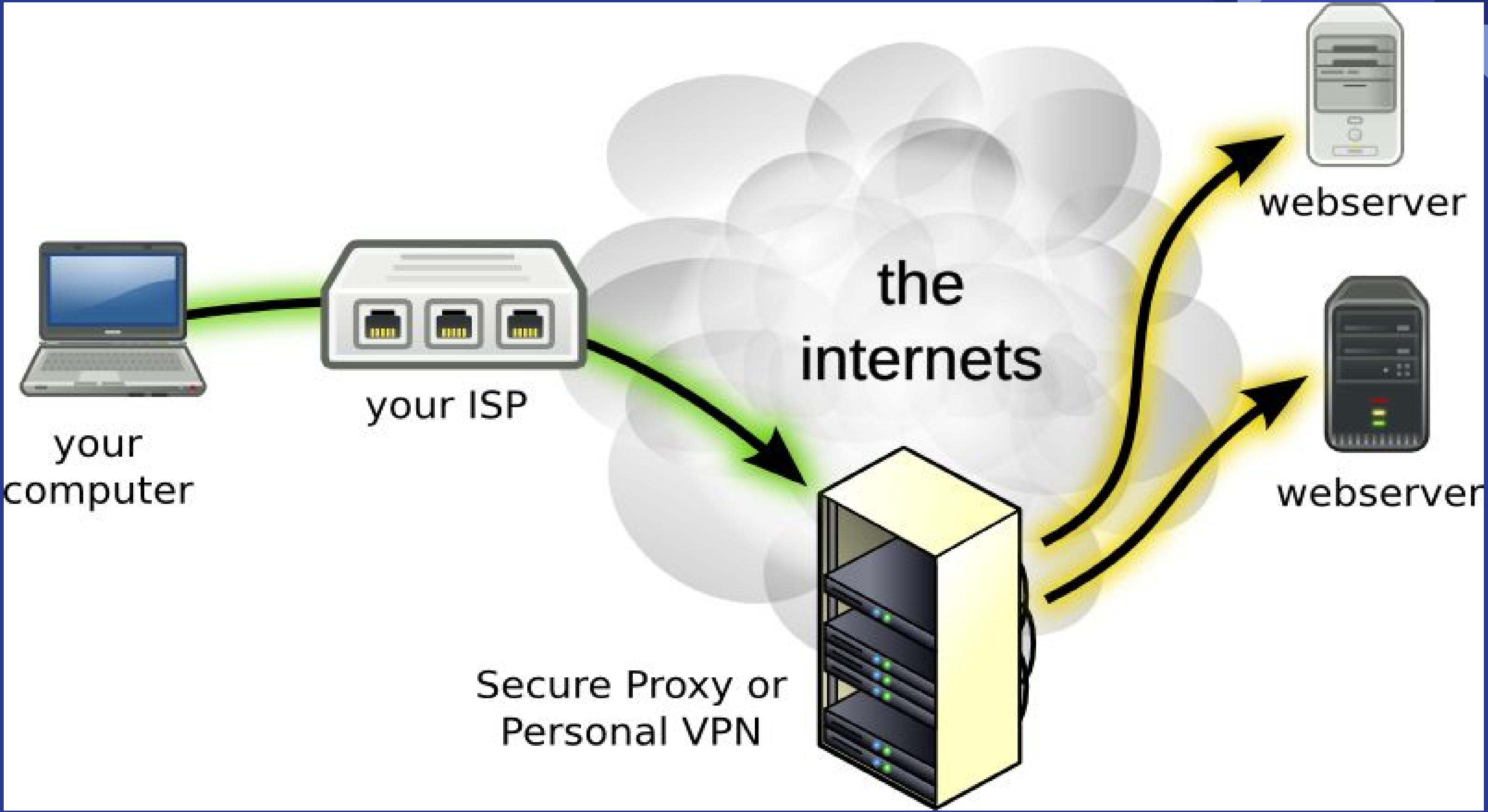
What is a VPN?

- Network connection that enables you to create a secure connection over the public Internet to private networks at a remote location
- All network traffic goes through a secure virtual tunnel between client and server and is encrypted
- Encryption, tunneling, protocols, data encapsulation and certified connections to provide secure connection

Access to the Internet (normal)



Access to the Internet (w. VPN)

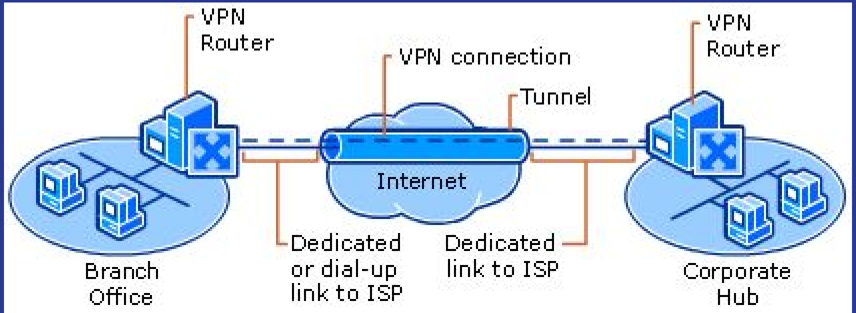


Types of VPNs

- Site-to-site VPNs
- Remote Access VPNs

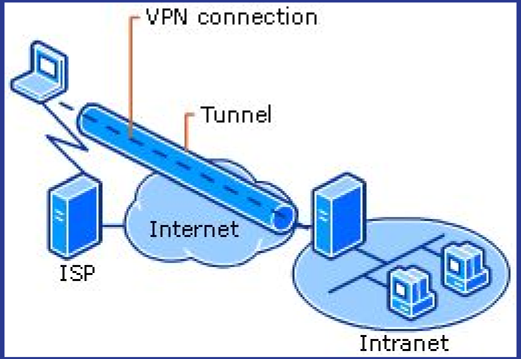
Site-to-site VPNs

- Used in corporate environment
- Ensures the safe encrypted connection of two or more local area networks (LANs)
- Two separated offices are virtually bridged together into a single LAN and users can access data throughout this network



Remote Access VPNs

- Connect an individual computer to a private network
- Two types of Remote Access VPNs:
  - Corporate VPNs
  - Personal VPNs



Corporate VPNs

- Allows users to connect to their company networks and remotely access resources and services on the networks
- VPN thinks that the user’s computer is on the same local network as the VPN

Personal VPNs

- Provide same secure connection as corporate VPNs
- However, personal VPNs are not used to connect to private networks to access private resources
- Useful for connecting to a public network
- All internet communication will be encrypted

Masking IP Address

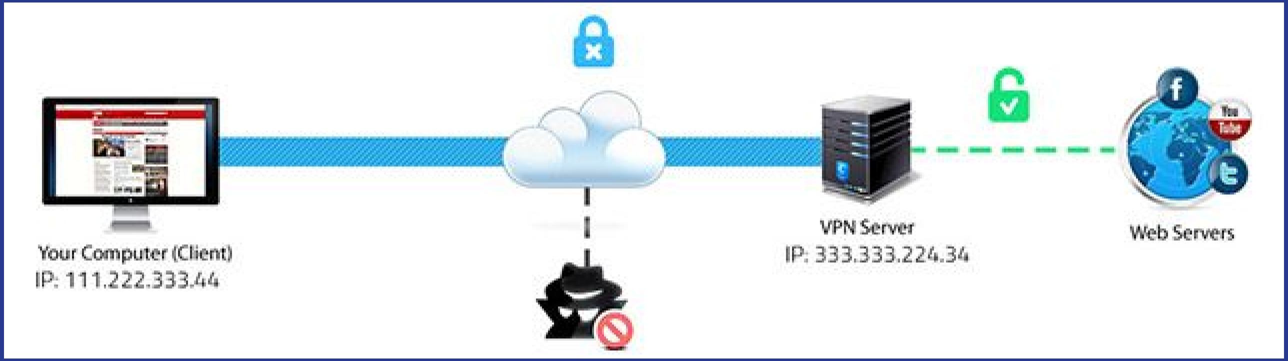
- A VPN masks your IP address, allowing you to surf the web anonymously
- Can connect from a geographic location that is different from where you are physically located
- Eg. Use a VPN to mask yourself to be in United States to use American Netflix

VPN Hardware and Software

- Client side:
    - Hardware: computer, smart phone, tablet, etc
    - Software: VPN client app running on device
- Server side:
    - Hardware: server computers and traffic routers
    - Software: traffic routing and communication between the servers and clients

VPN Traffic Flow

- Both inbound and outbound traffic is routed through VPN servers
- Depending on traffic direction, data is encrypted and decrypted either on client side or server side
- Eg. Want to watch a video on YouTube

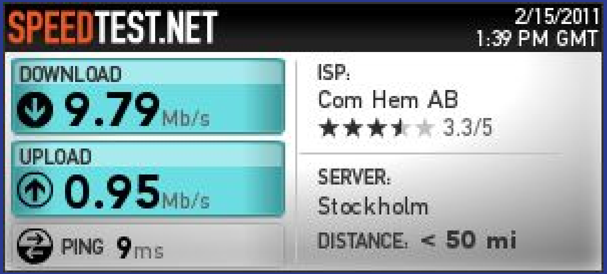


Encryption types

- Most common encryption: Blowfish (OpenVPN), Aes
- 128 bit and 256 bit and even more……
- Most VPNs are transitioning to using 256 bit.
- 256 bit and more could be overkill and cause worst performance.

Speed Comparison

S.T Without VPN



SPEEDTEST.NET

2/15/2011
1:39 PM GMT

DOWNLOAD 9.79 Mb/s

UPLOAD 0.95 Mb/s

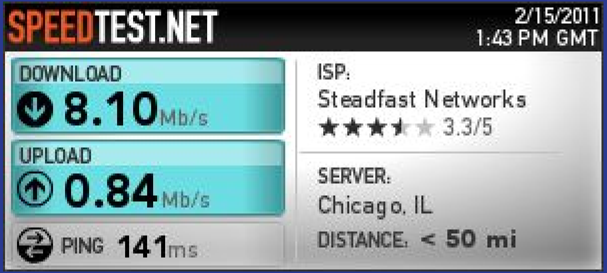
PING 9 ms

ISP:
Com Hem AB
★★★⯪☆ 3.3/5

SERVER:
Stockholm

DISTANCE: < 50 mi

S.T with VPN with 128 bit (BF)



SPEEDTEST.NET

2/15/2011
1:43 PM GMT

DOWNLOAD 8.10 Mb/s

UPLOAD 0.84 Mb/s

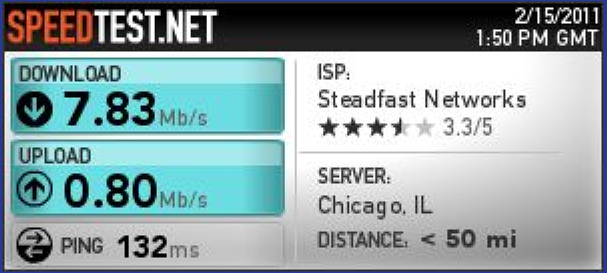
PING 141 ms

ISP:
Steadfast Networks
★★★⯪☆ 3.3/5

SERVER:
Chicago, IL

DISTANCE: < 50 mi

S.T with VPN with 256 bit (AES)



SPEEDTEST.NET

2/15/2011
1:50 PM GMT

DOWNLOAD 7.83 Mb/s

UPLOAD 0.80 Mb/s

PING 132 ms

ISP:
Steadfast Networks
★★★⯪☆ 3.3/5

SERVER:
Chicago, IL

DISTANCE: < 50 mi

VPN Tunneling

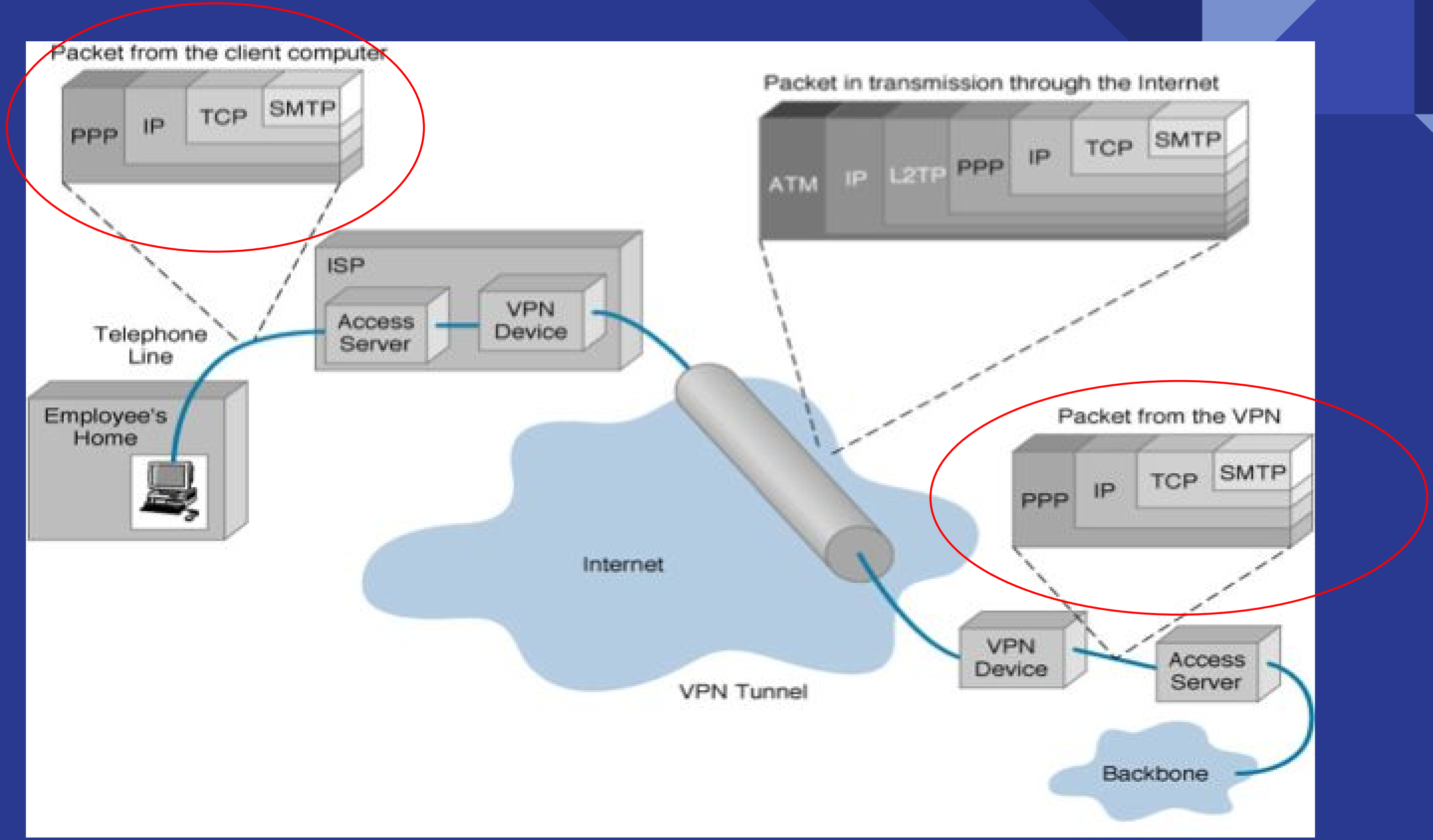
- A virtual point-to-point connection made through a public network
- Transports encapsulated datagrams

VPN Tunneling Protocols

- Three main protocols:
  - Point-to-point Tunneling Protocol (PPTP)
  - Layer Two Tunneling Protocol (L2TP)
  - Secure Socket Tunneling Protocol (SSTP)
- All depend on original Point-to-point Protocol (PPP)

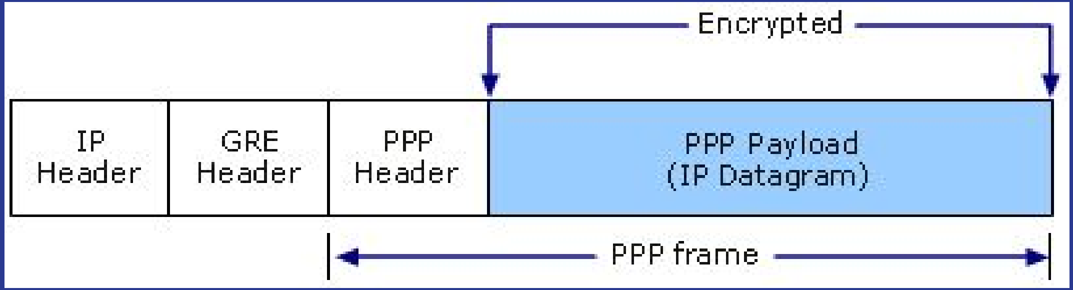
Point-to-point Protocol

- For IP, PPP encapsulates IP packets with PPP frames and then retransmits the encapsulated PPP-packets across a point-to-point link


Packet from the client computer
PPP
IP
TCP
SMTP
Packet in transmission through the Internet
ATM
IP
L2TP
PPP
IP
TCP
SMTP
ISP
Access Server
VPN Device
Telephone Line
Employee's Home
Internet
VPN Tunnel
Packet from the VPN
PPP
IP
TCP
SMTP
VPN Device
Access Server
Backbone

Point-to-point Tunneling Protocol

- Encapsulates PPP frames in IP datagrams for transmission over the network



Encrypted

IP Header

GRE Header

PPP Header

PPP Payload (IP Datagram)

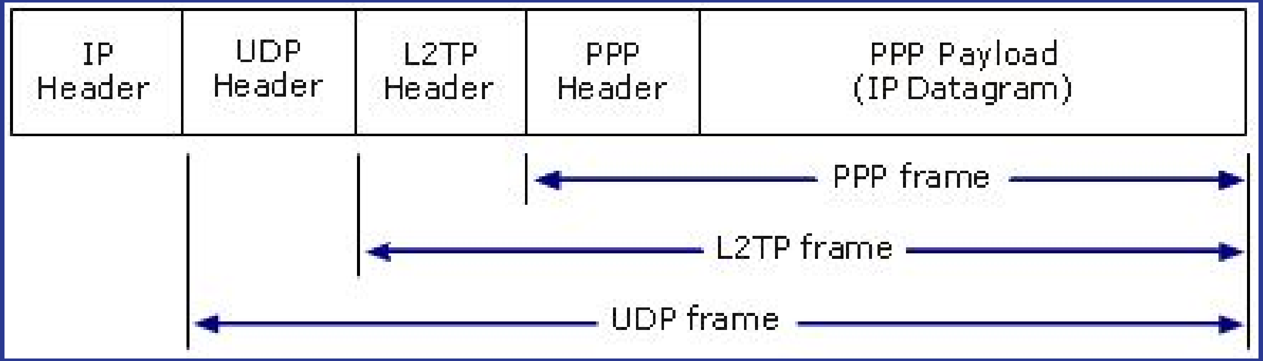
PPP frame

Layer Two Tunneling Protocol

- Combination of PPTP and Layer 2 Forwarding (L2F)
- L2TP relies on Internet Protocol security (IPsec) for encryption services
- Encapsulation for L2TP/IPsec packets consist of two layers

L2TP Encapsulation

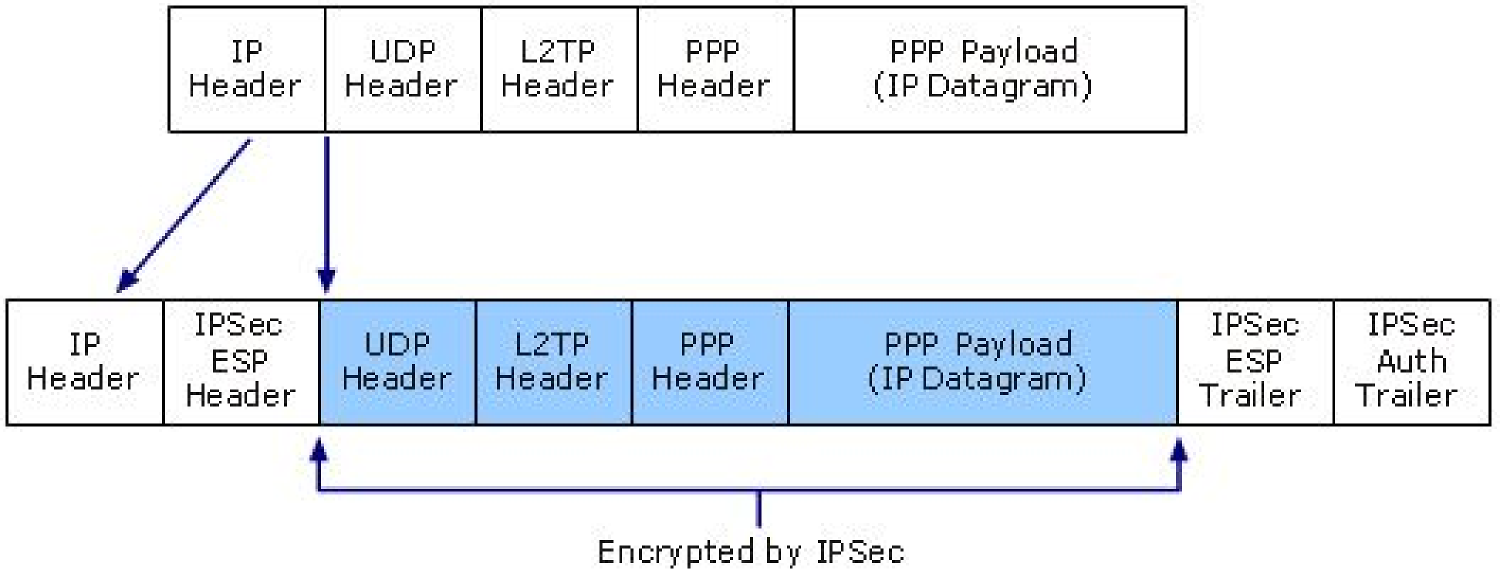
- A PPP frame is wrapped with an L2TP header and a UDP header



IPsec Encapsulation

- Resulting L2TP message is then wrapped with:
  - An IPsec Encapsulating Security Payload (ESP) header and trailer
  - IPsec Authentication trailer that provides message integrity and authentication
  - IP header that has source and destination IP address corresponding to the VPN client and VPN server
- L2TP message encrypted with DES or 3DES

L2TP and IPsec encapsulation



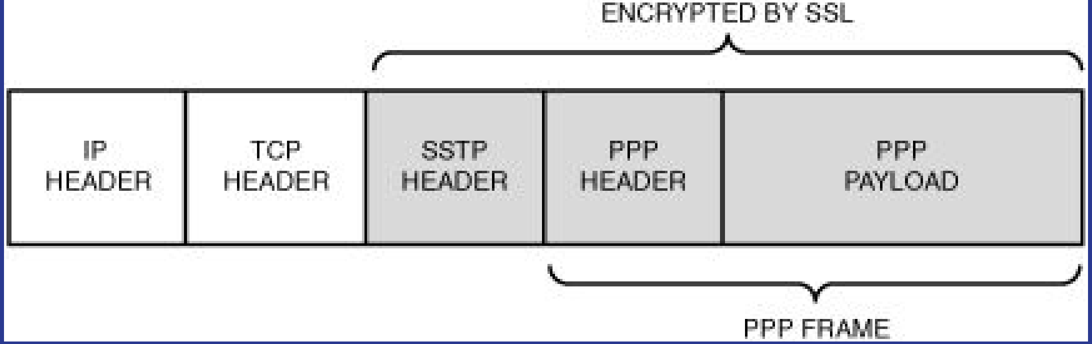
IP Header	UDP Header	L2TP Header	PPP Header	PPP Payload (IP Datagram)

IP Header	IPSec ESP Header	UDP Header	L2TP Header	PPP Header	PPP Payload (IP Datagram)	IPSec ESP Trailer	IPSec Auth Trailer

Encrypted by IPSec

Secure Socket Tunneling Protocol

- Uses the HTTPS protocol over TCP port 433 to pass traffic through firewalls and Web proxies that might block PPTP and L2TP/IPsec traffic
- Encapsulate PPP traffic over the Secure Sockets Layer (SSL) channel of the HTTPS protocol

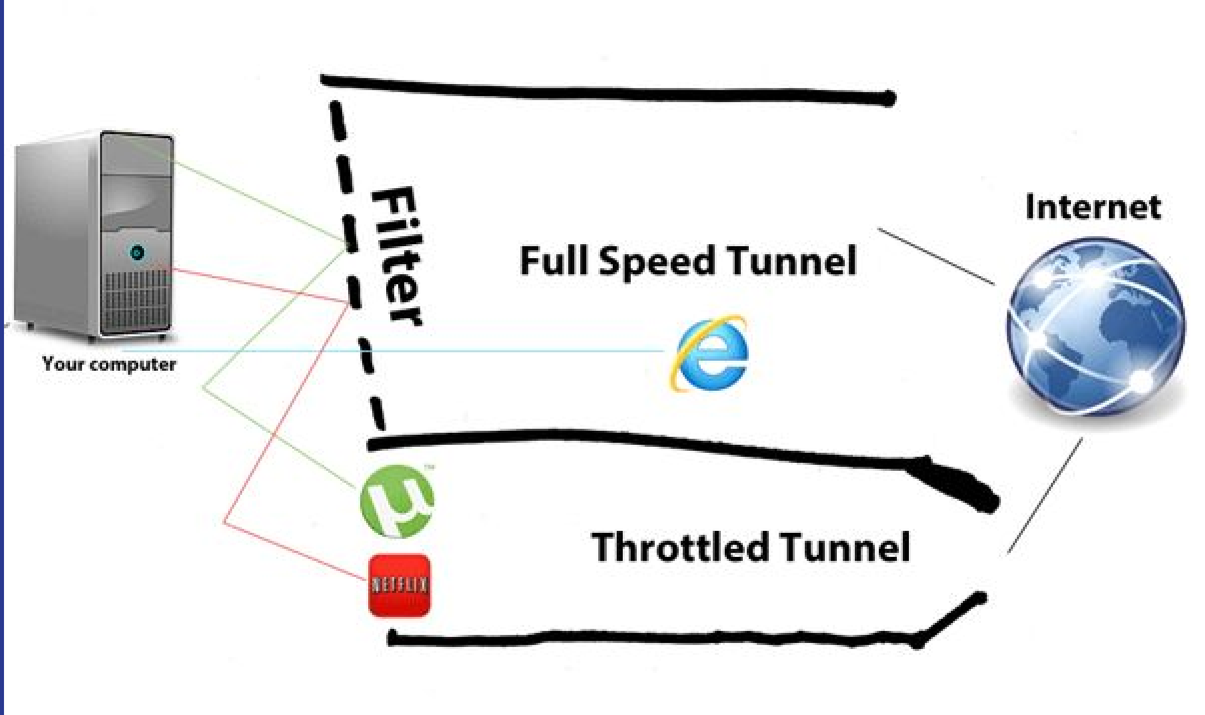


Issue: ISP Throttling

- ISPs like to reserve the right to slow down your internet

- Usually on high traffic sites:
  - Video Streaming sites: Netflix, Hulu, youtube
  - Online Gaming: League of Legends, World of Warcraft.
  - File-sharing software and torrents: BitTorrent

Prevent Throttling by ISP



Prevention of ISP Throttling

Encrypting your data

Easily accomplished through the use of an VPN like OpenVPN

Potential Security Threats to VPN

1) Viruses, Malware, Trojans, etc………
2) Transfer of Private Company Data
3) Corporate VPNs

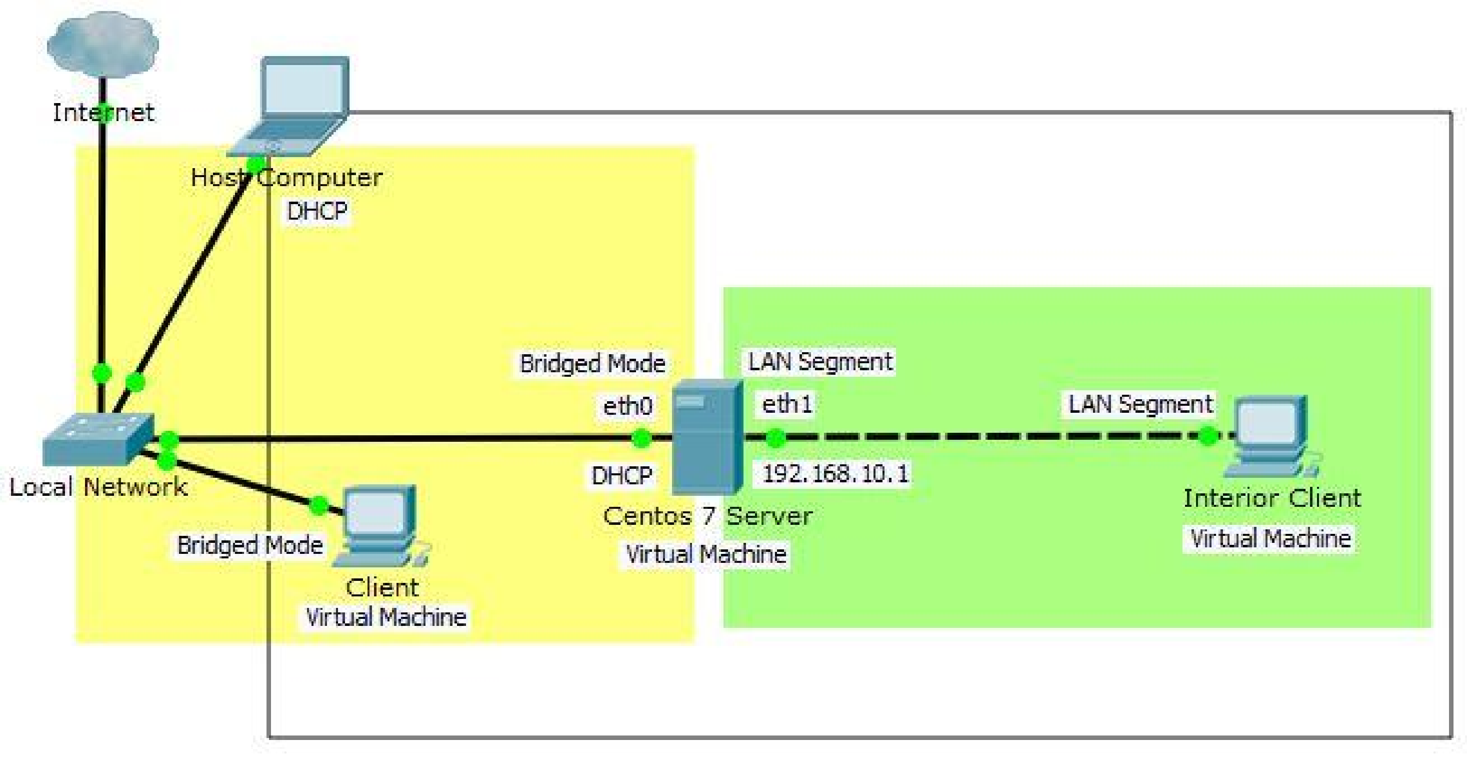
Demo - OpenVPN

OpenVPN

- OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange.

CentOS

- CentOS (abbreviated from Community Enterprise Operating System) is a Linux distribution that attempts to provide a free, enterprise-class, community-supported computing platform which aims to be functionally compatible with its upstream source, Red Hat Enterprise Linux (RHEL)


Internet
Host Computer
DHCP
Bridged Mode
eth0
LAN Segment
eth1
LAN Segment
Local Network
DHCP
192.168.10.1
Interior Client
Virtual Machine
Centos 7 Server
Virtual Machine
Bridged Mode
Client
Virtual Machine

Advantages

- Strong Security
- High Reliability

Disadvantages

- Proxy Problems
- High Overheads