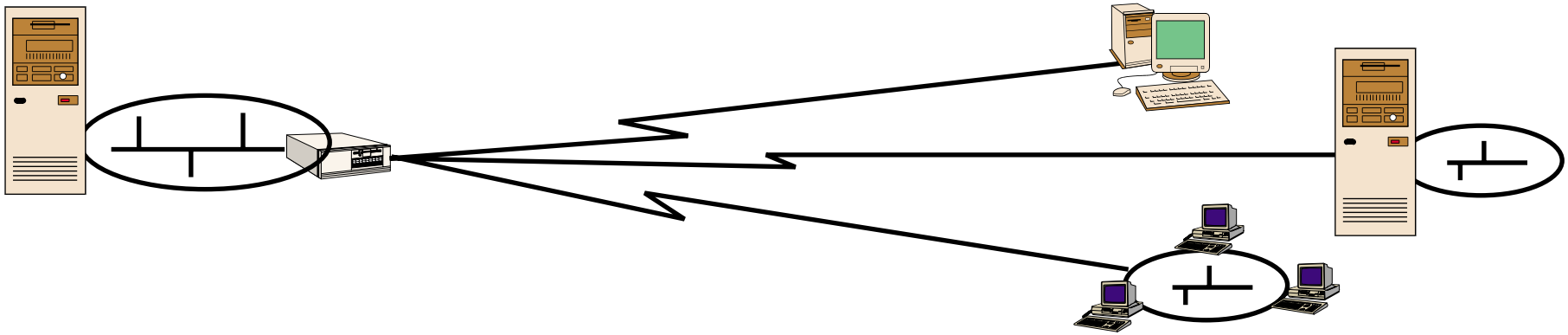
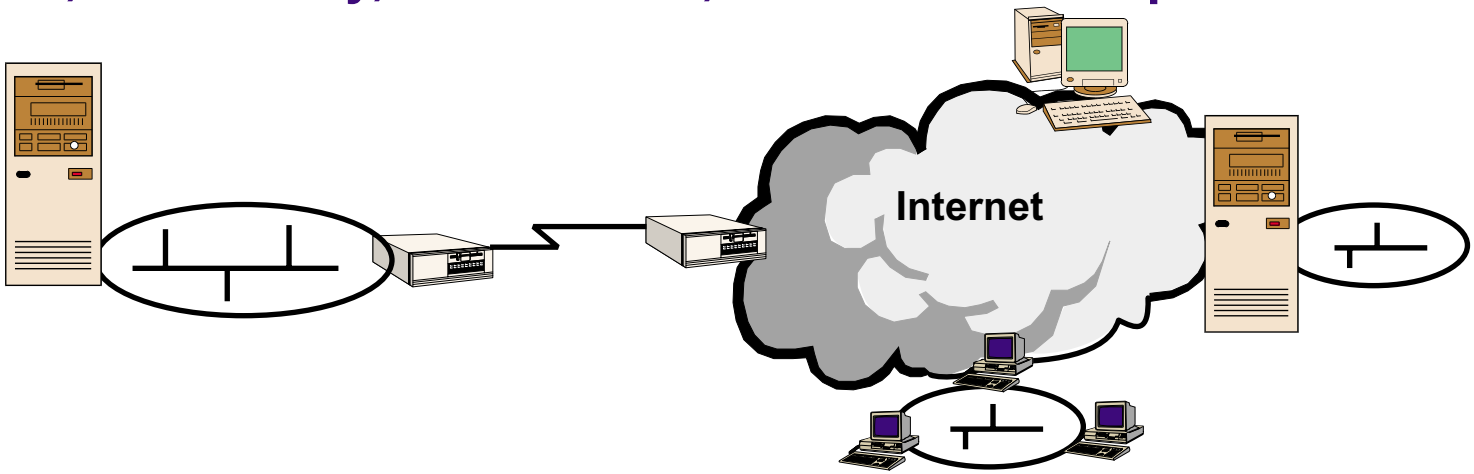
Introduction to VPNs (Virtual Private Networks)

Laura Jeanne Knapp
IBM/Tivoli Technical Evangelist
1-919-224-2205
Laura@lauraknapp.com
www.lauraknapp.com

Public Internet Instead of Private Network



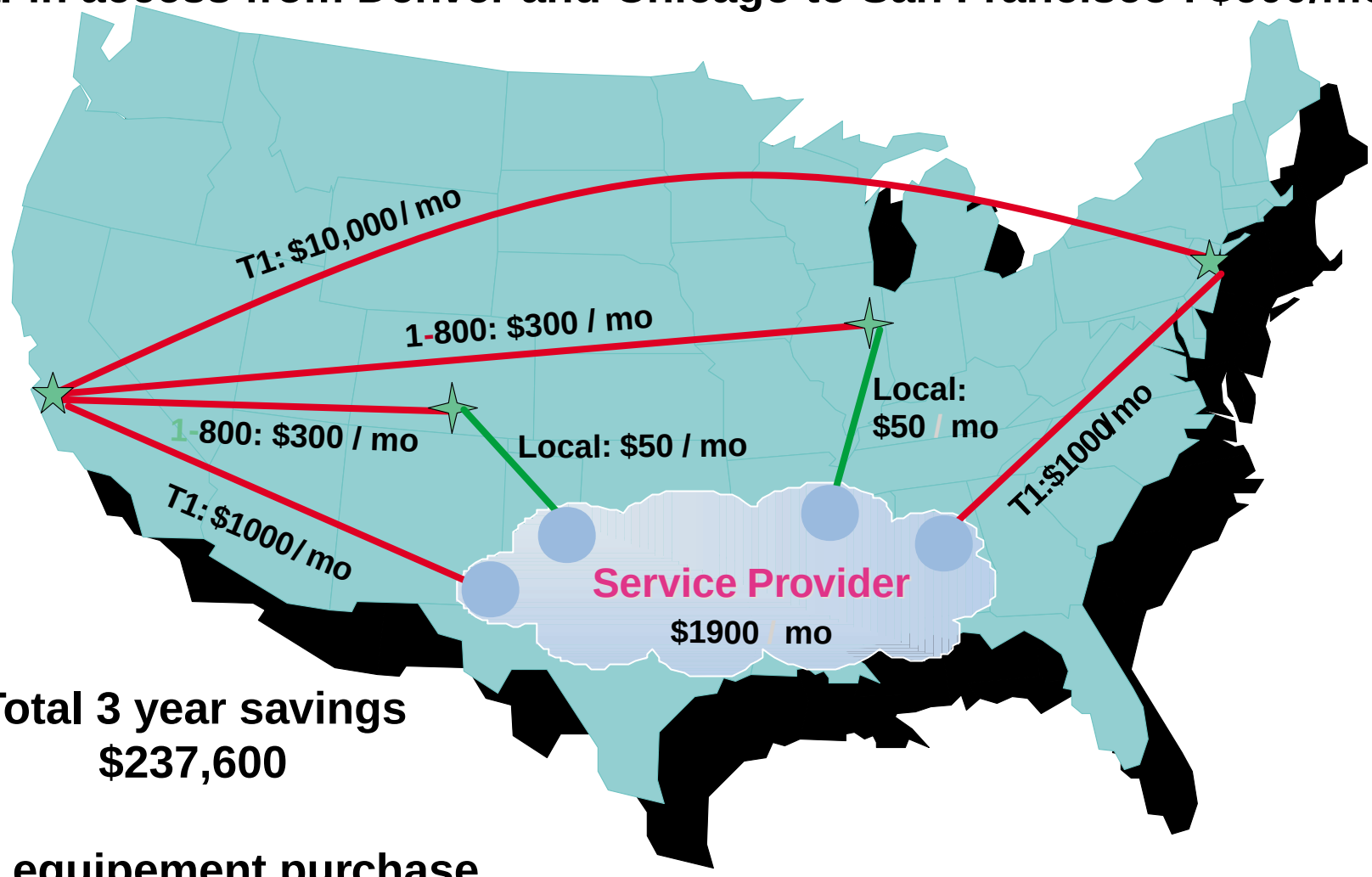
VPNs are a means of moving information between trusted network segments over untrusted network segments like dial, frame relay, leased lines, and customized private networks



A VIRTUAL Private Network replaces all of the above utilizing the public Internet
Performance and availability depend on your ISP and the Internet

VPN Cost Savings

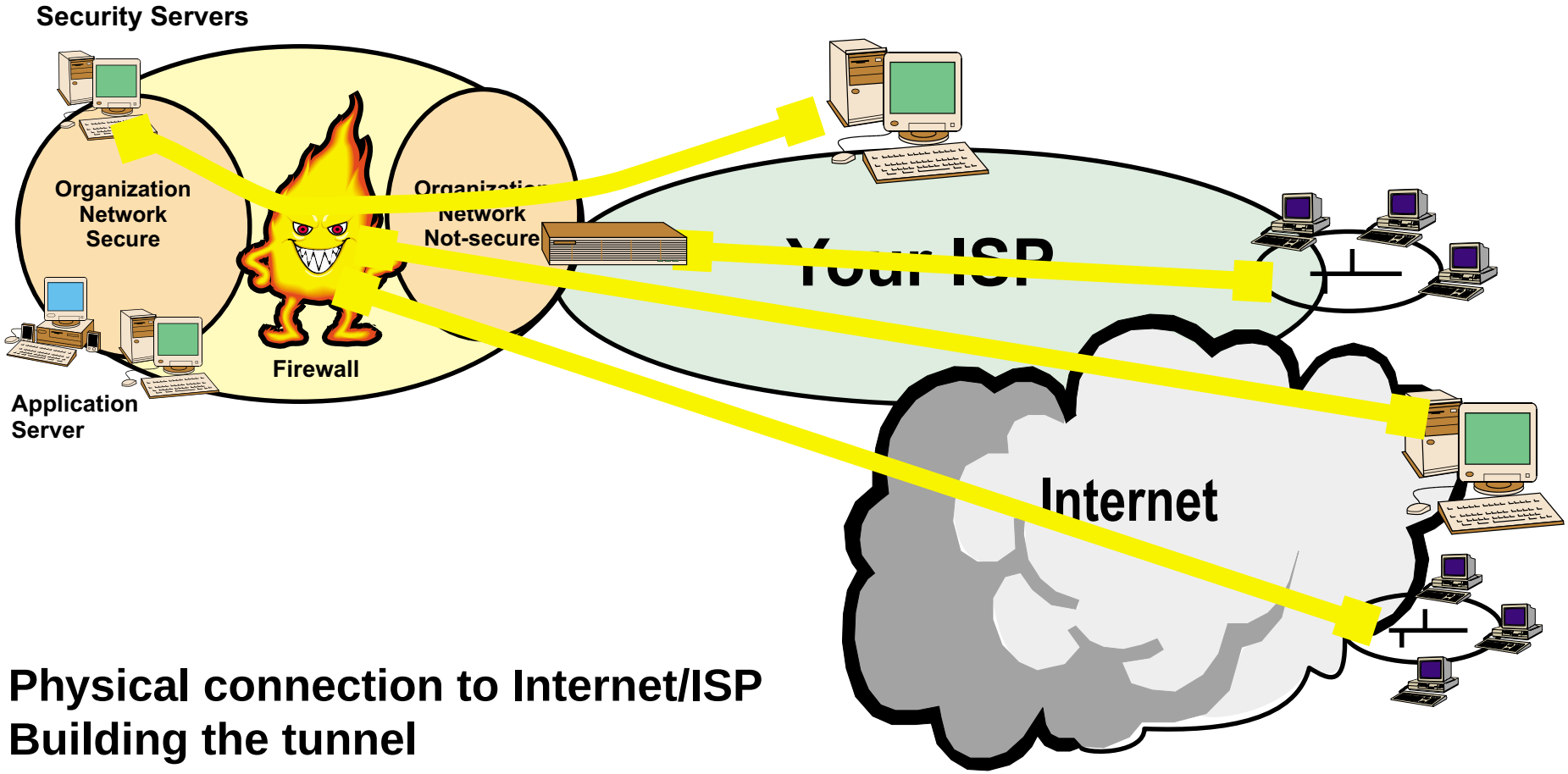
T1 connections between San Francisco and New York City : $10,000/mo
Dial-in access from Denver and Chicago to San Francisco : $600/mo



Total 3 year savings
$237,600

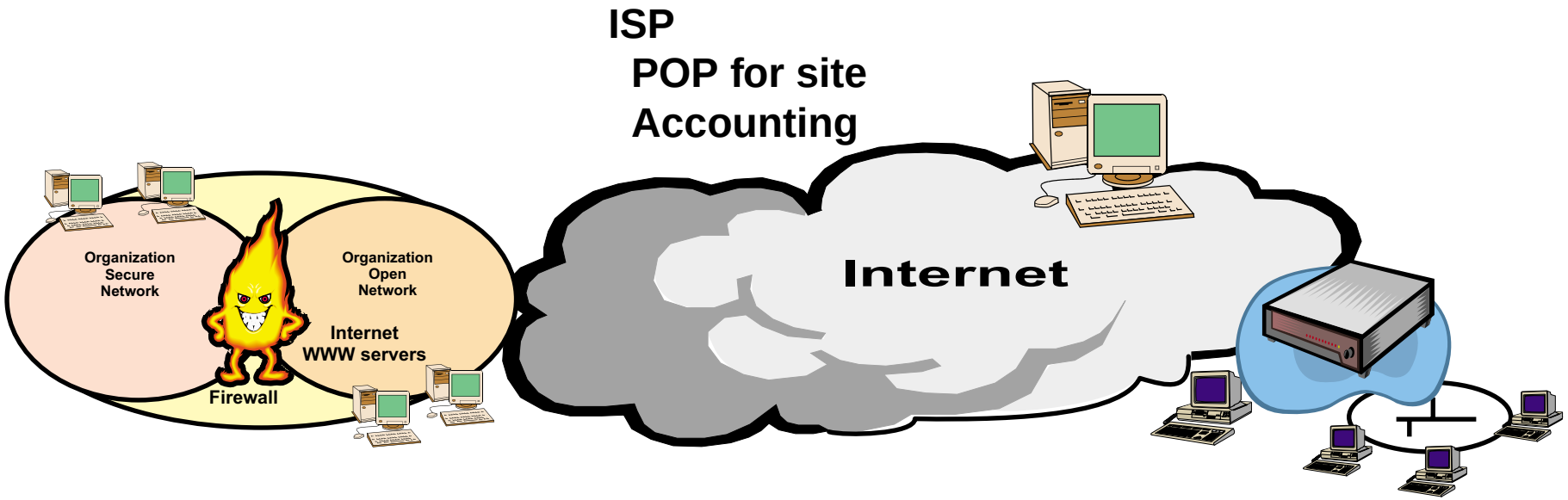
VPN equipement purchase
$7,800

Elements of a Virtual Private Network



Physical connection to Internet/ISP
Building the tunnel
Security servers
Management
Provisioning
Quality of Service (QoS)

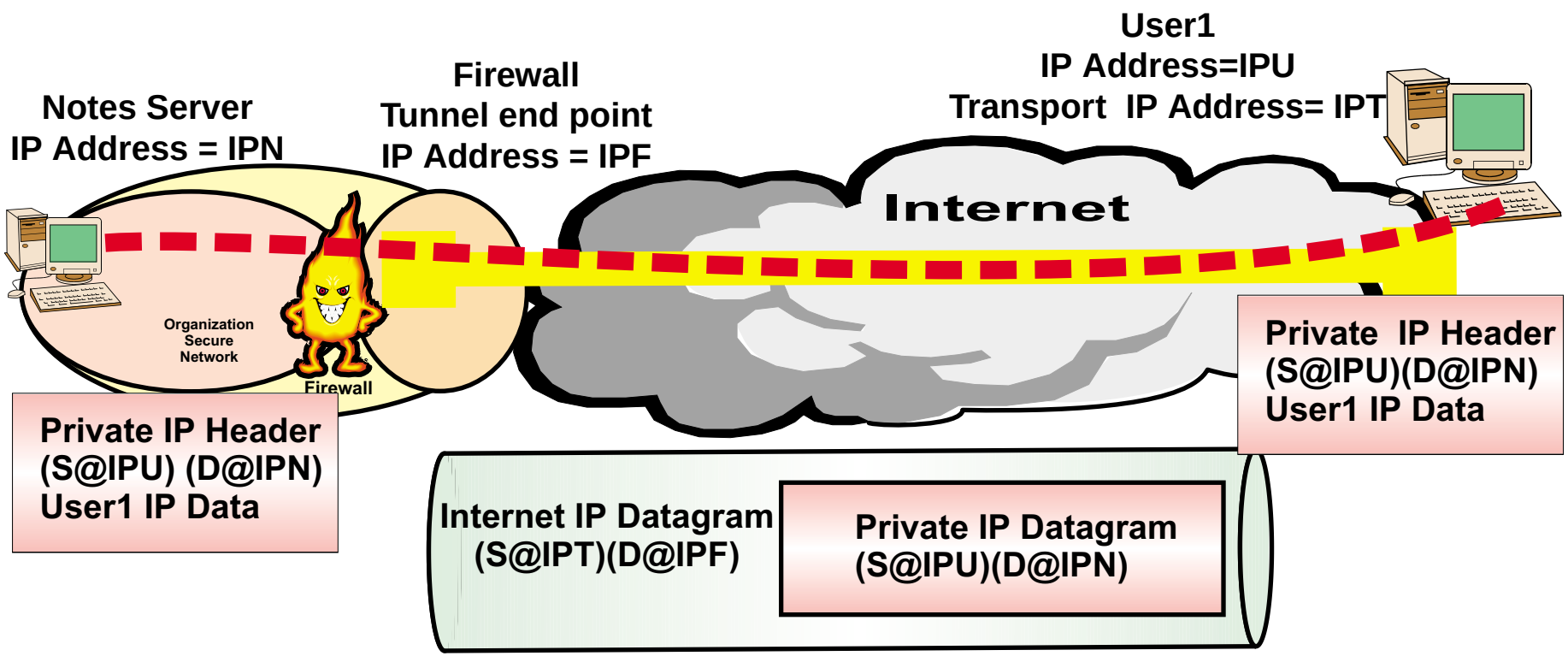
VPN - Functional Areas



Organization Network
- Accepts incoming requests
- Terminates tunnel
- Security servers
  - Authenticates user/packet/machine
  - Negotiates encryption
- Policy Servers
  - Enforces routing policy
  - Enforces access rights
- Allocates addresses
- Management

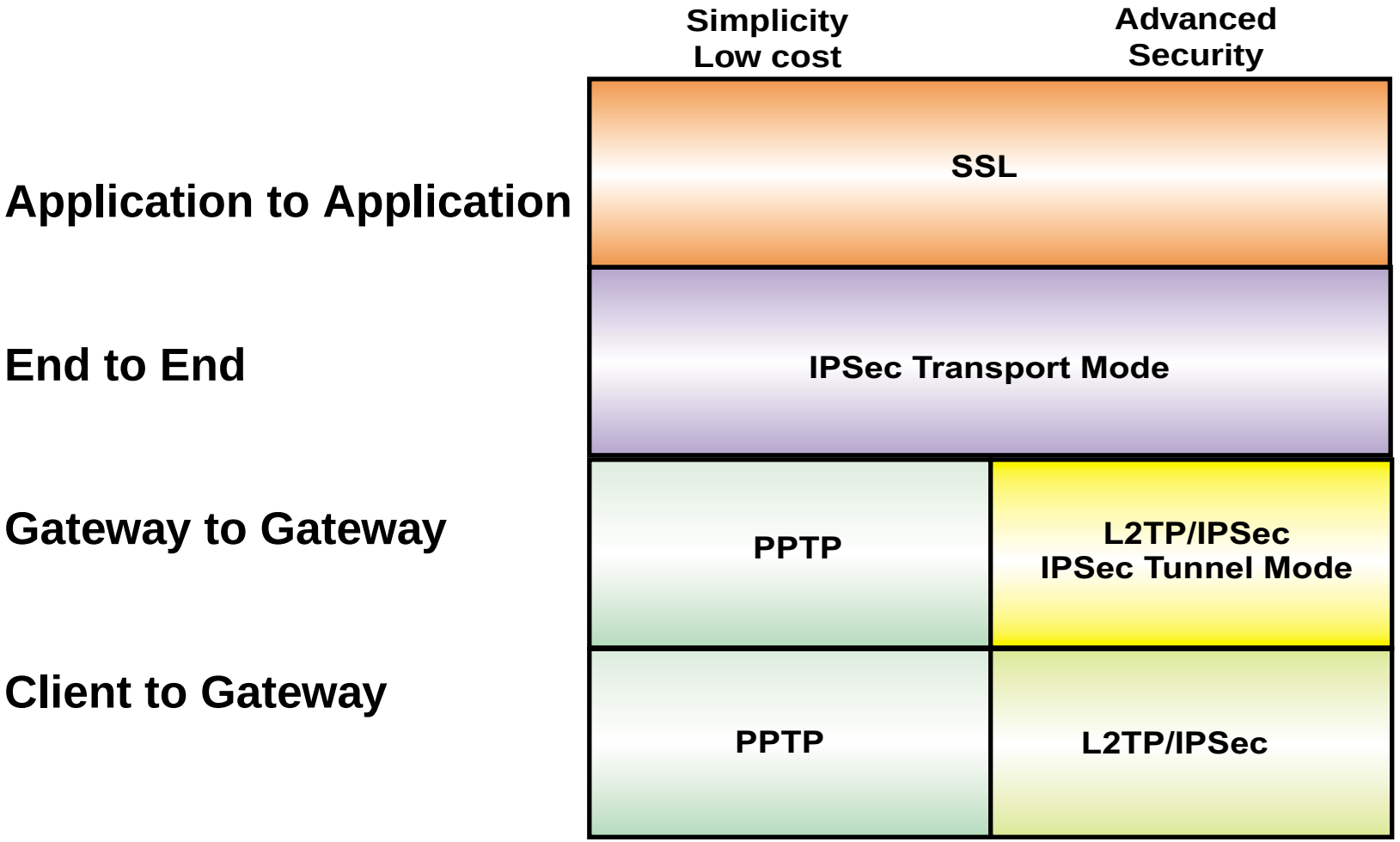
Remote site
- Initiates tunnel
- Negotiates with security servers for authentication and encryption
- Requests private IP address assignment from home network
- Requests public IP address assignment from ISP

VPN - Building the Tunnel - Encapsulation



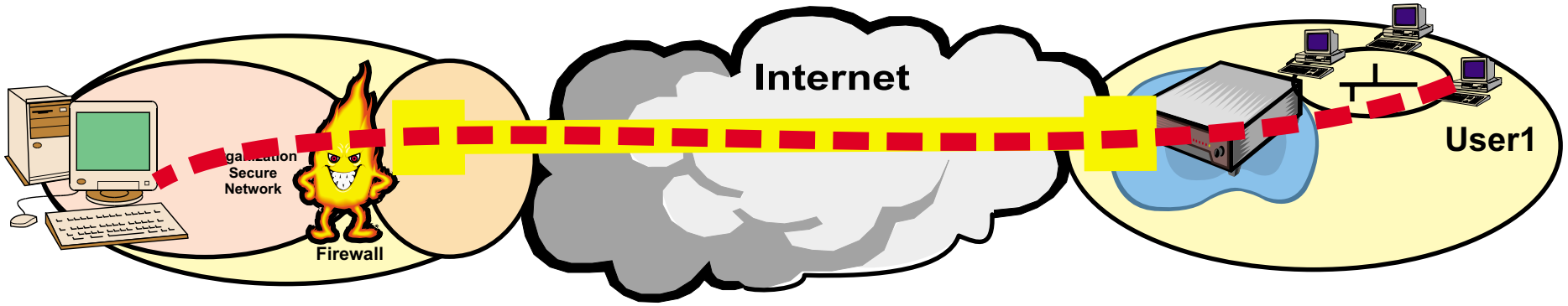
Tunneling includes
encapsulation
transmission
un-encapsulation

VPN - Technologies



PPTP - Point to Point Tunneling Protocol - Layer 2 - Multiprotocol
L2TP/IPSec - Layer 2 Tunneling Protocol - Multiprotocol - Encryption and Authentication
IPSec - IP Security - Layer 3 - IP protocol - Encryption and Authentication
SSL - Secure Sockets Layer - Layer 6/7 - Application - Encryption and Authentication

Building a VPN with IPSec



Builds the tunnel

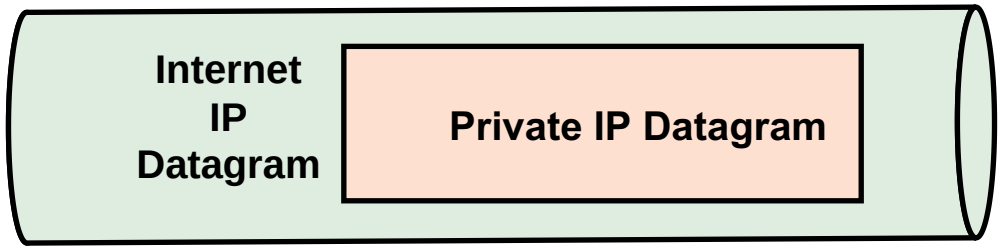
Integrated security technologies

ESP = Encapsulating Security Payloads - encrypts IP datagram
- **DES and 3DES are most common encryption mechanisms used**
- **May provide confidentiality, authentication, integrity, non-repudiation, replay protection, and traffic analysis protection**
- **Does everything AH does**

AH = Authentication Header - validates sender and indicates data integrity
- **MD5 and SHA1 are most common authentication mechanisms used**
- **Provides integrity and authentication but not confidentiality**

IKE - Internet Key Exchange (aka:ISAKMP/Oakley) Protocol

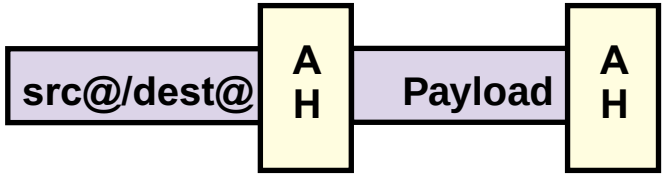
IPSec Tunneling and Transport



AH-Authentication Header
IP Protocol 51

Original IP Datagram

AH-Tunnel

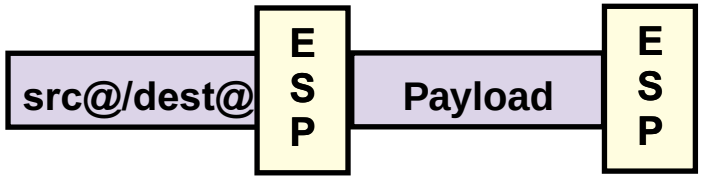


AH-Transport

ESP-Encapsulating Security Protocol
IP Protocol 50

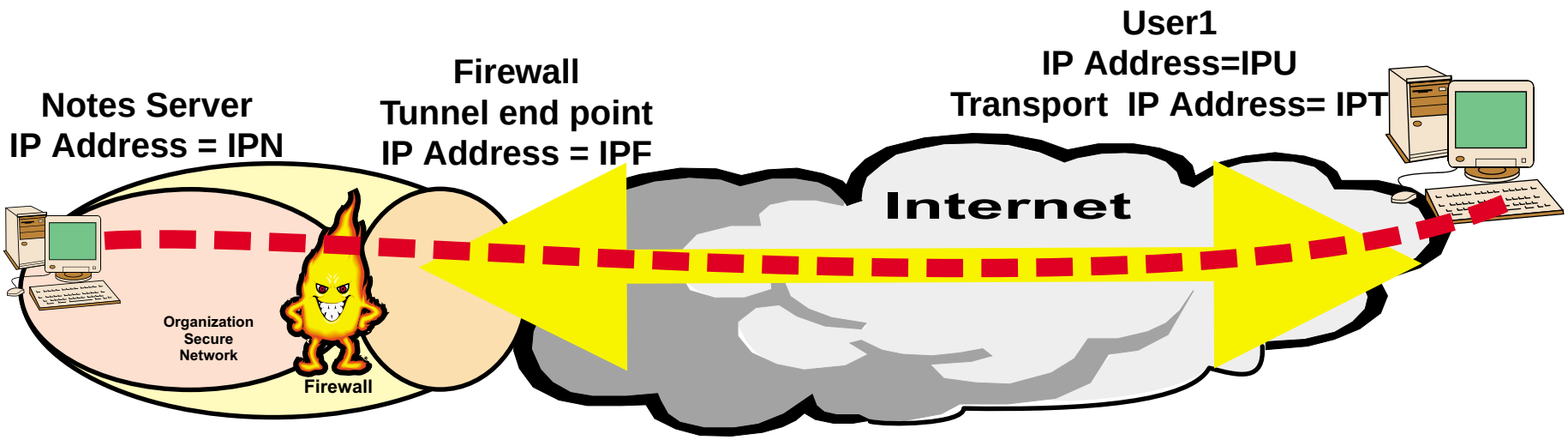
Original IP Datagram

ESP-Tunnel



ESP-Transport

IPSec VPN
Internet Key Exhange



Agree on parameters
Exchange keys
Use encrypted tunnels

Manual Key Management
- Administrator sets up keys at both ends
- Not scalable

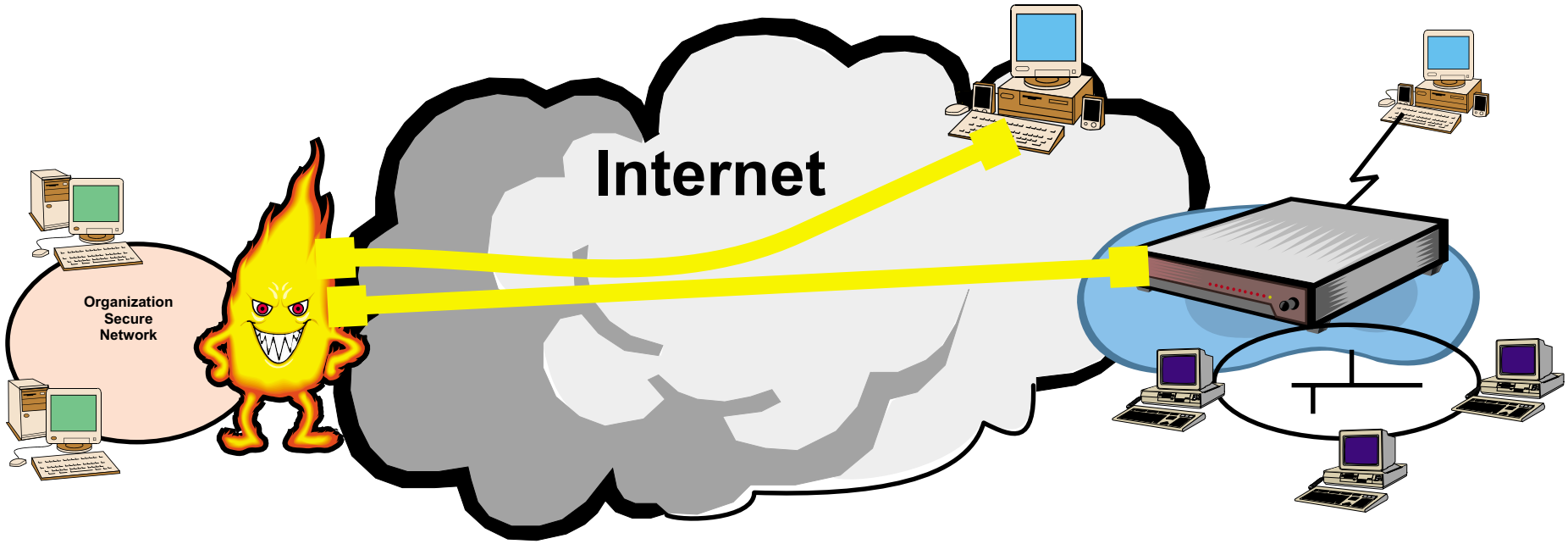
Automated Key Managment
- On-demand creation of keys
- Complex to configure
- Scalable

Two parties negotiate
- Encryption algorithm
- Hash digests
- Authentication
- Key strength
- Security association lifetimes

VPN - Tunneling with L2TP and IPSec

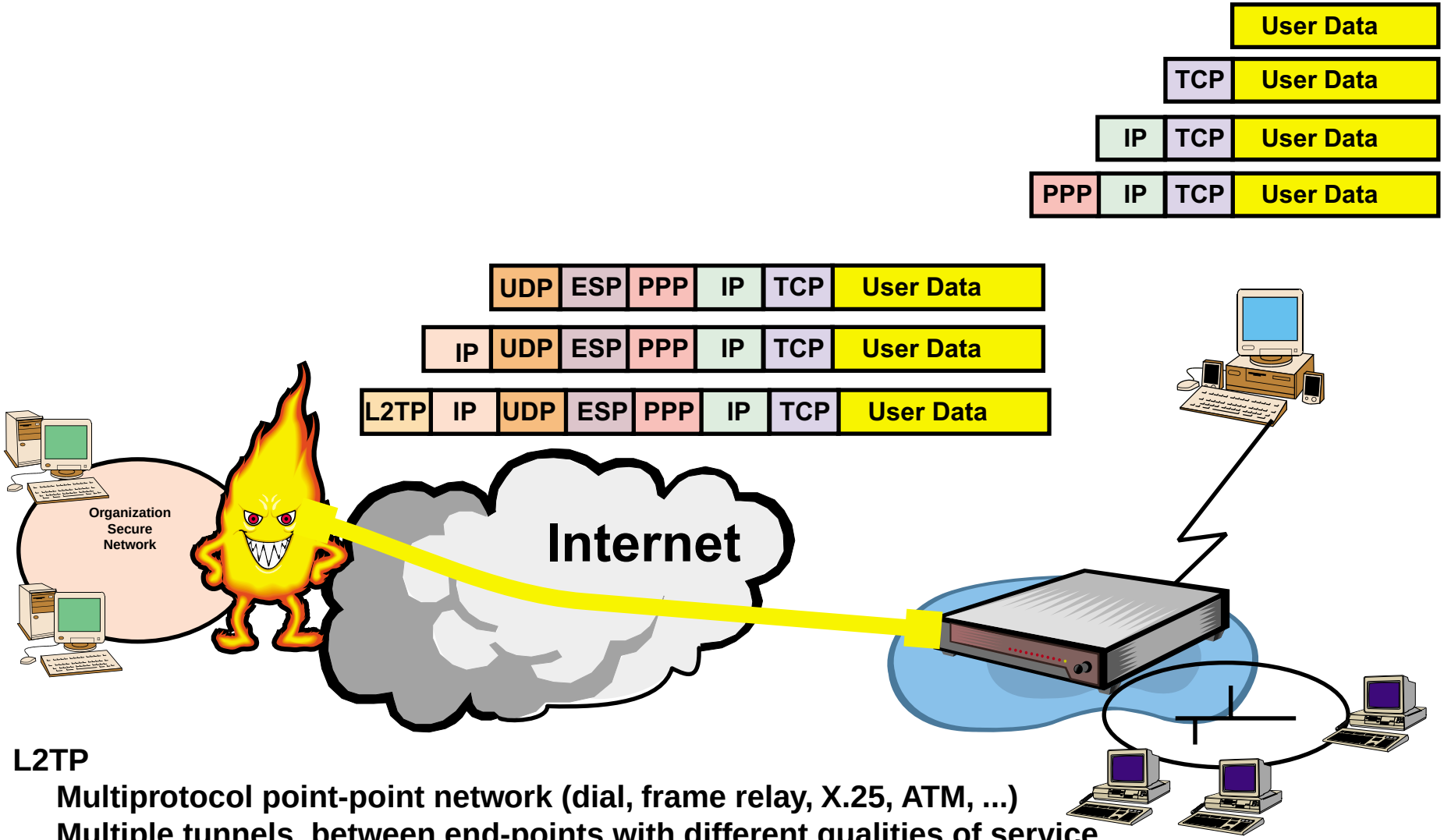
L2TP ⟷ L2TP — Domain authentication (userID/password, smart card, etc)

IPSec ⟷ IPSec — Machine authentication, Encryption



IPSec IKE negotiation
Establish IPSec ESP for L2TP UDP port 1701
L2TP tunnel setup, management over IPSec
User authentication to domain

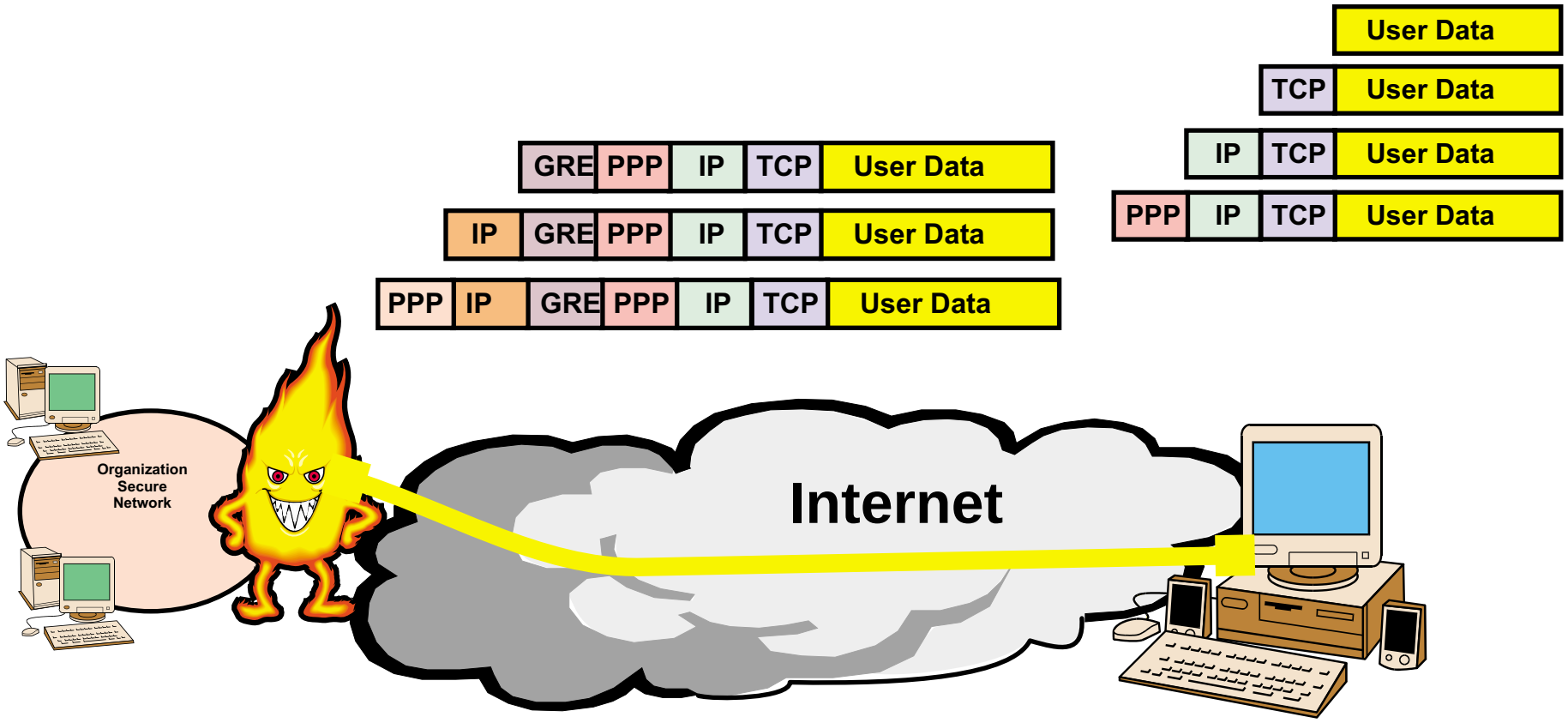
VPN - L2TP Frames



L2TP

- Multiprotocol point-point network (dial, frame relay, X.25, ATM, ...)
- Multiple tunnels between end-points with different qualities of service
- 4 bytes of overhead when compression used
- Tunnel authentication
- Can be used with IPSec to provide authentication and encryption

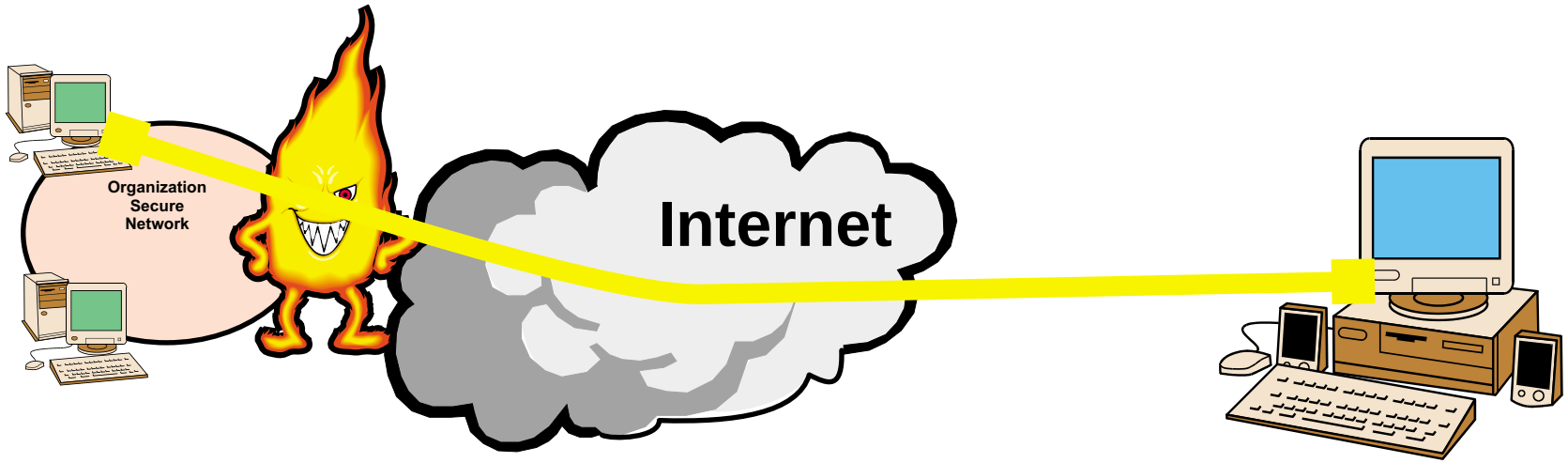
VPN - Tunneling with PPTP and PPoE



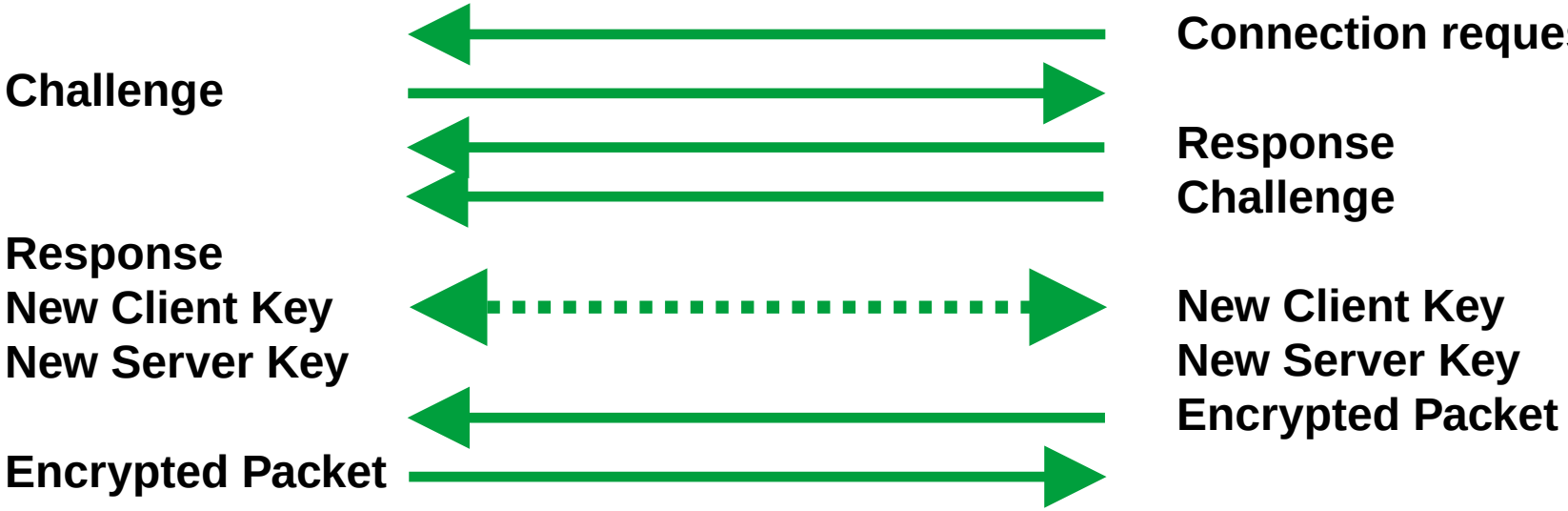
PPTP

- PPoE is Point-Point protocol over Ethernet
- Single tunnel between end-points : single device support (GRE = generic routing encapsulation)
- 6 bytes of overhead when compression used
- No tunnel authentication
- With RADIUS server supports authentication and accounting
- CHAP V2 fixes password, masquerading, and encryption weakness
- 40 or 128 bit RC4 packet encryption

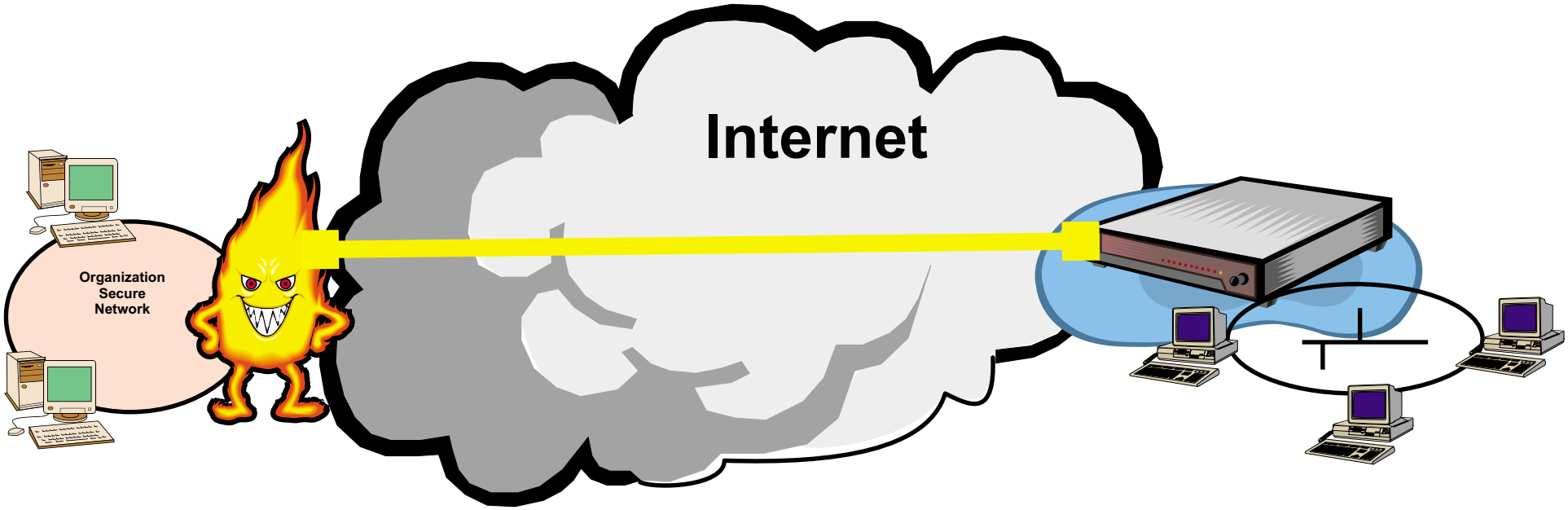
VPN - PPTP Security



CHAP V2 Authentication with 40 or 128 bit RC4 encryption



VPN - Tunneling with Proprietary Mechanisms



Most widely used today

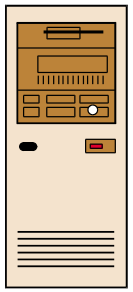
Since ISP owns the entire tunnel, they can use a mixture of standards, emerging standards, and proprietary mechanisms to make the tunnel

End user client code distributed by ISP -- Must use same ISP

These tunnels are dedicated and are not generally taken up and down

VPN - Tunneling with Secure Sockets (SSL)

Browser



WEB Server

Client Hello
- Protocol version
- Session ID
- Cipher suite
- Compression method
- Client hello random number

Server Hello
- Protocol version
- Session ID
- Cipher suite
- Compression method
- Server hello random number

Client verify server certificate
- Client certificate
- or client key exchange

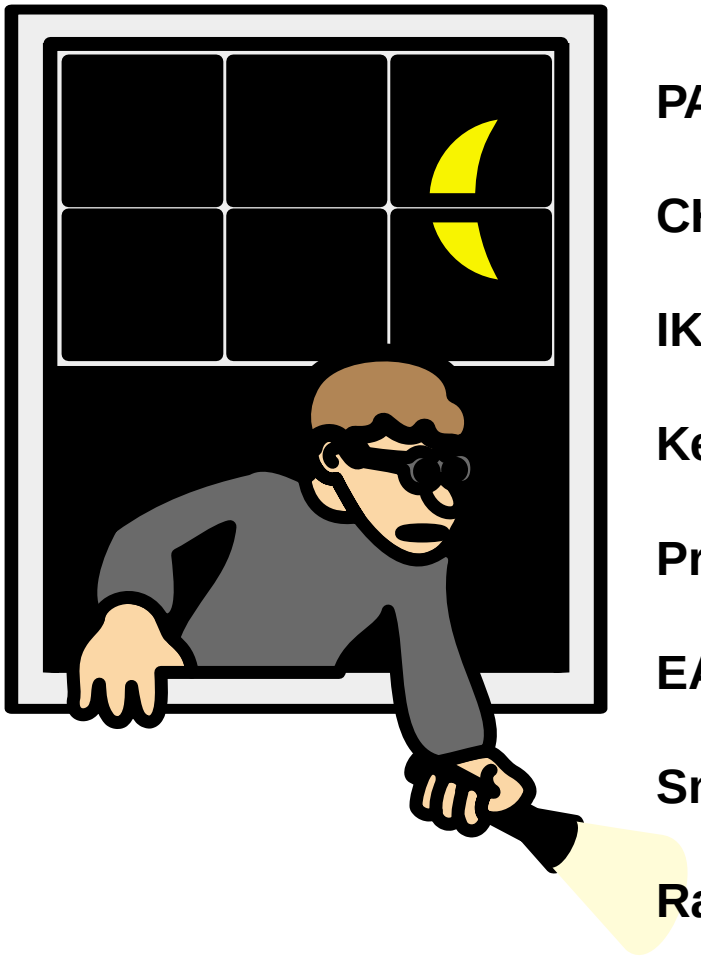
Server certificate
- Certificate request
- or server key exchange

Change cipher spec
- finished

Change cipher spec
- finished

Application data ⟷ **Application data**

VPN - Confused about Security



	L2TP	PPTP	IPSec
PAP, CHAP	X	X	
CHAP v2	X	X	
IKE			X
Kerberos			X
Private Key Exchange			X
EAP	X	X	
SmartCard/Token	X	X	
Radius	X	X	
RC4 encryption		X	
DES, 3DES encryption	X		X

VPN - Issues

Pervasiveness of interoperable code

Client code distribution

Use of token/biometric systems

Simultaneous Internet access

Compression and encryption

Key distribution

Key management

Integration into Policy Management System

Vendor interoperability

Administration support

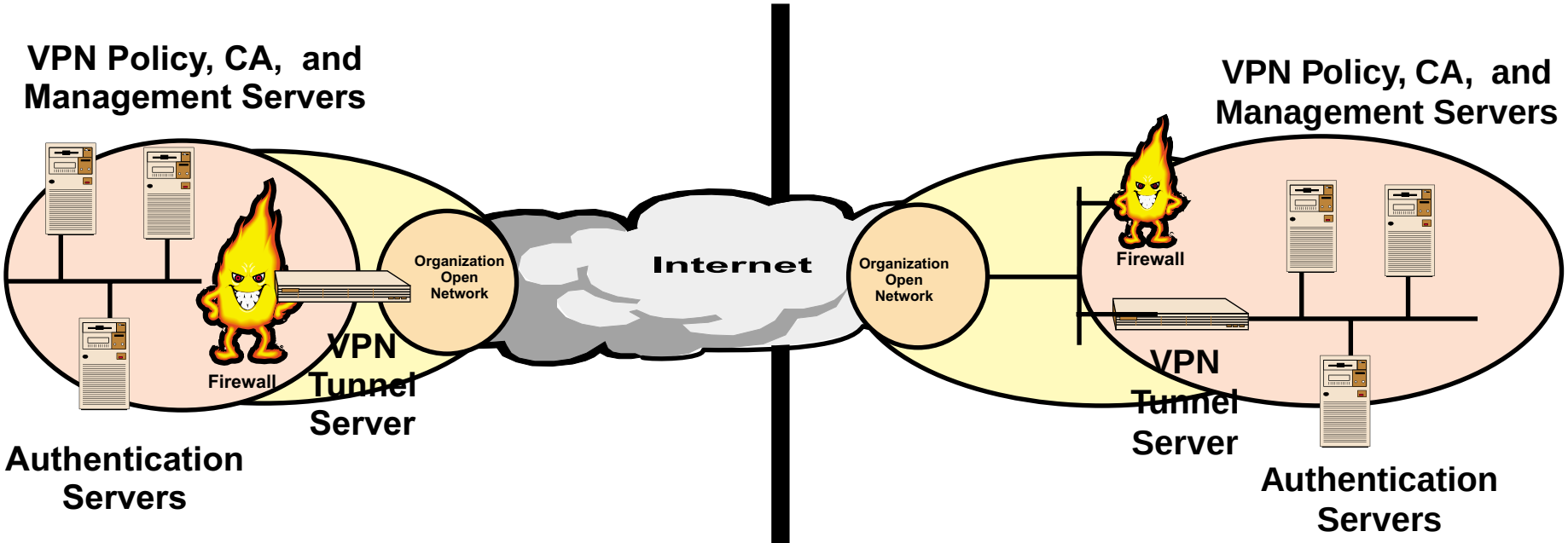
Performance of the Internet or any public shared network

VPN - Tunneling Comparisons

	L2TP/IPSec	IPSec	PPTP	SSL
Mode	Client/server	Host-host	Client/server	Client/server
Layer	2	3	2	7
Protocols	Multiprotocol	IP	Multiprotocol	IP
Security				
User Authentication	PKI		PKI	Log-in
Machine Authentication		PKI		
Packet Authentication		X	X	
Packet Encryption	DES, 3DES, PGP	DES, 3DES	X	
Key Management	IKE	IKE	PKI	Private Key

*Provided outside of specification

VPN - Design Options



Tunnel Server in line with Firewall

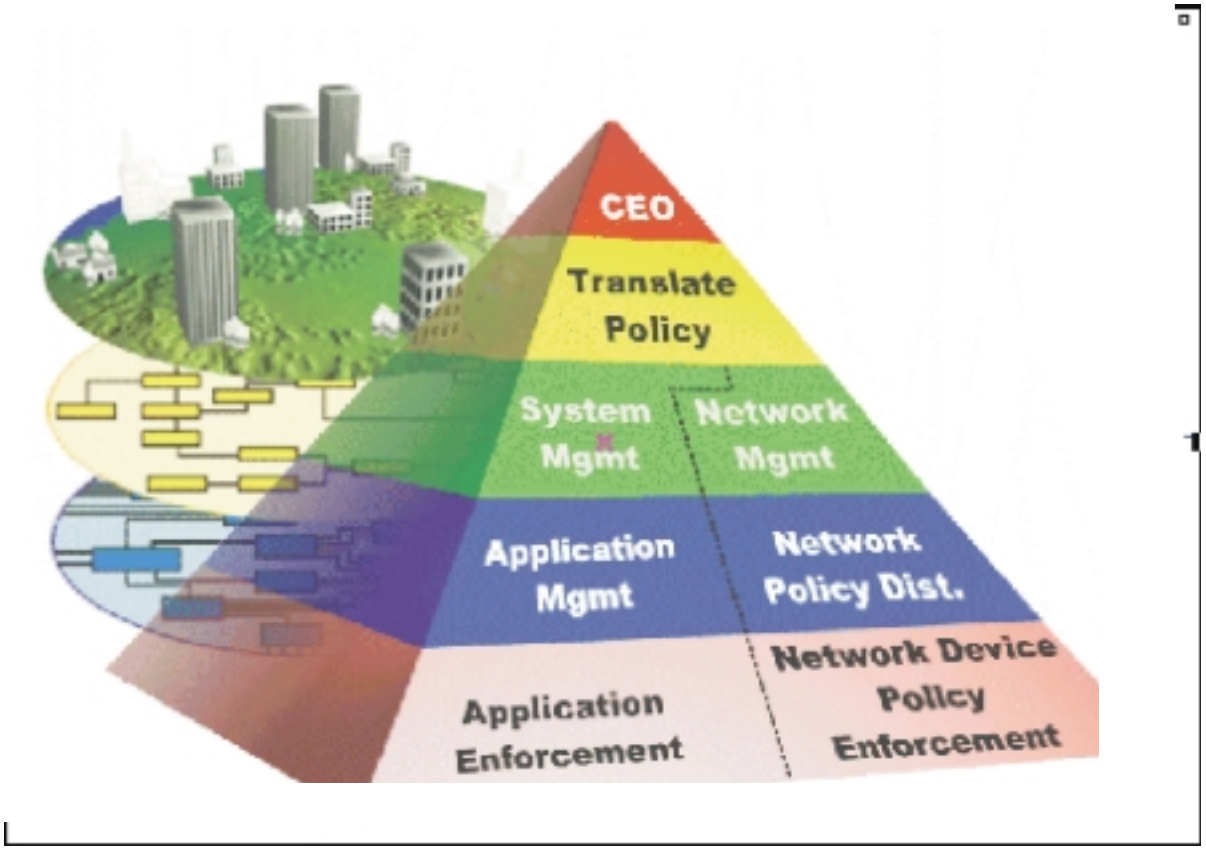
If using intrusion detection systems based on IP address, place VPN tunnel termination before the intrusion detection system

Can the firewall s performance scale with VPN traffic

Tunnel Server in parallel with Firewall

Use other authentication mechanism (not IP address) like tokens, time of day, biometrics

Policy Based Networks

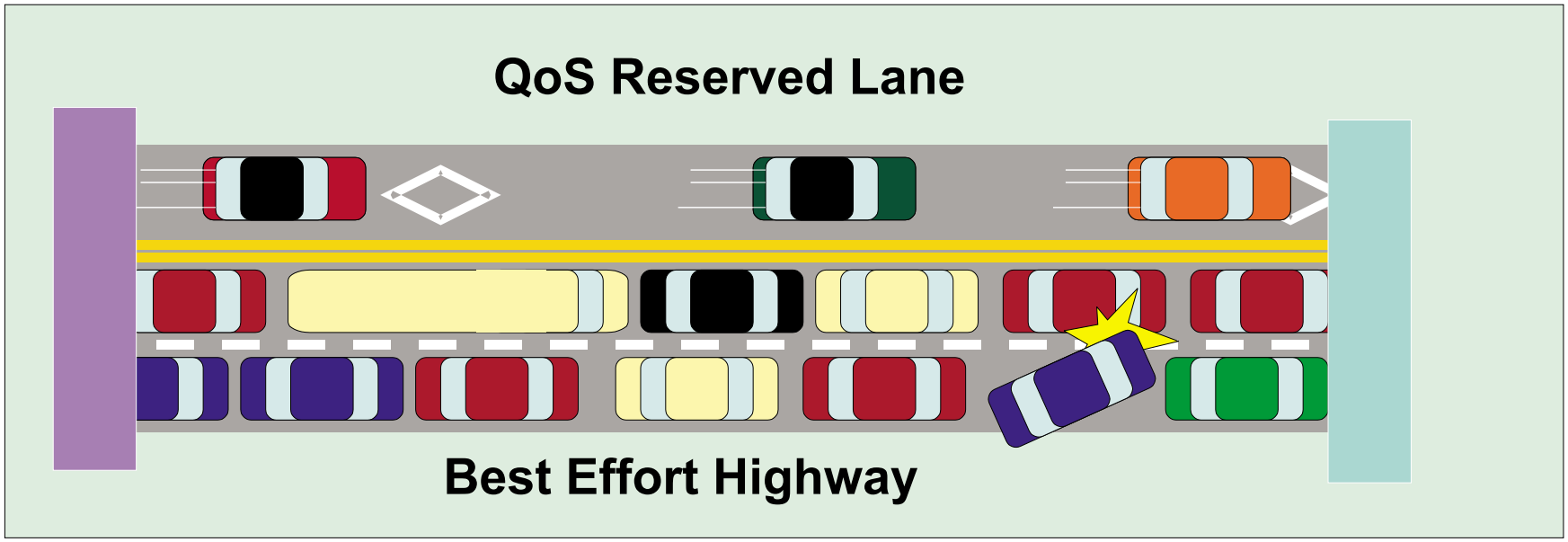


Stores and distributes policy from common directory

Common repository for server, network, client, application information

Globally defined for client, resources, and applications by individual, group, or role

VPN - The Missing Piece
Quality of Service



DiffServ - Differentiated services

MPLS - Multiprotocol Label Swapping

RSVP - Resource Reservation Protocol

Managing VPNs

Verifies Policy

User response time

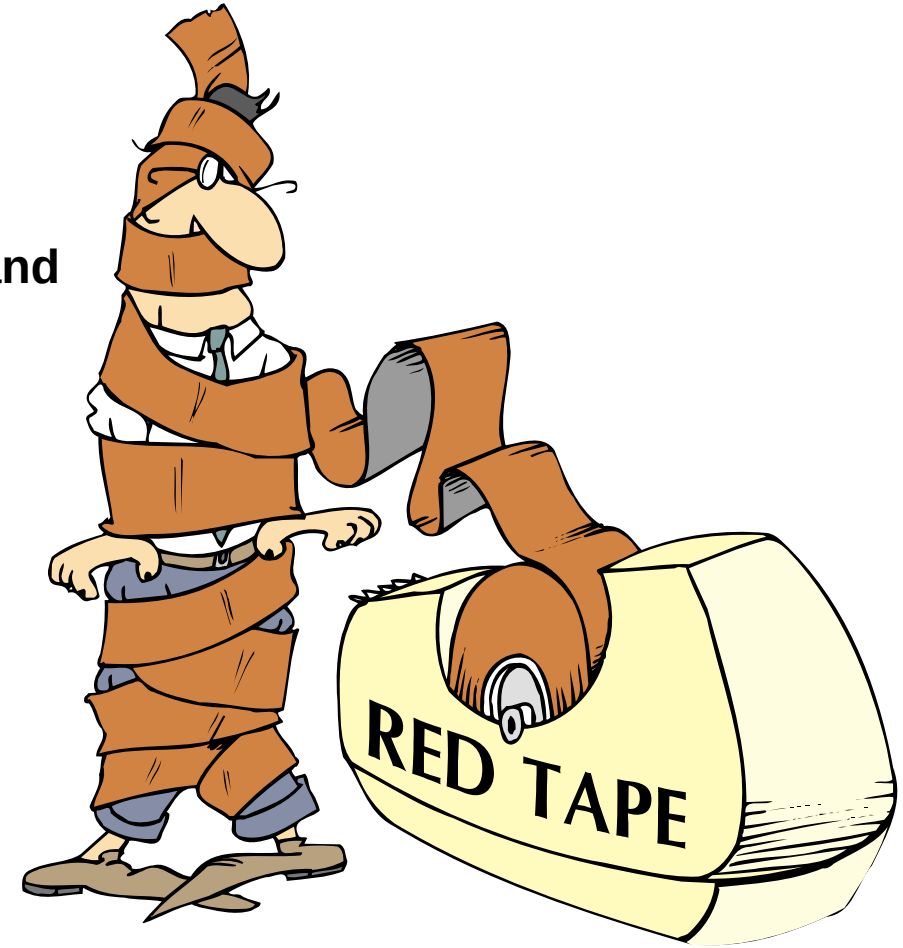
Logging and trapping of authentication and encryption errors

QoS monitoring

Operational center for VPN tunnels

Key Management
- **Key assignment**
- **Key revocation**
- **Automatic key exchange**
- **Ease of canceling key**
- **International issues**

Interface into Policy Management System



VPN Glossary

AH	Authentication Header in IPSec
AIAG	Automotive Industry Action Group
ANS	Automotive Network Exchange
ATM	Asynchronous Transfer Mode
CHAP	Challenge Handshake Authentication Protocol
DES	Data Encryption Standard (64 bit)
3DES	Triple DES (192 bit)
DiffServ	Differentiated Services
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
GRE	General Routing Encapsulation
ICSA	International Computer Security Association
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	IP Security Protocol
ISAKMP	Internet Security Associations /Key Management Protocol
ISP	Internet Service Provider
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunnel Protocol
MIME	Multipurpose Internet Mail Extensions
MPLS	Multiprotocol Label Swapping
NAS	Network Access Server
NAT	Network Address Translation
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
POP	Point of Presence
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
QOS	Quality of Service
RADIUS	Remote Authentication Dial-in User Services
RAS	Remote access Server
RSA	Encryption company/standards setter
RSVP	Resource Reservation Protocol
SSL	Secure Sockets Layer
TACACS	Terminal Access Controller Access Control Systems
VPN	Virtual Private Network

VPN Bibliography

Information from the IETF (Internet Engineering Task Force}:

Active IETF Working Groups: www.ietf.org/html.charters/wg-dir.html
Search for Internet Drafts: search.ietf.org/search/brokers/internet-drafts/query.html
Search for RFCs: www.rfc-editor.org/rfcsearch.html
VPN Mailing List : majordomo@listserv.iegroup.com
Send a message with the text: subscribe vpn [y our e-mail address]

Bibliography of VPN Information on the web: http://kubarb.phsx.ukans.edu/~tbird/vpn/vpn-general.html
Glossary compiled by the same folks: http://kubarb.phsx.ukans.edu/~tbird/vpn/vpn-glossary.html
Their mailing list: Listserv@securityfocus.com

News in the area of encryption: www.eff.org/pub/Crypto/
EFF is the Electronic Frontier Foundation

Computer Security Resource Clearinghouse: csrc.ncsl.nist.gov
NIST is the US National Institute of Standards and Technology

Directory of security products and services: www.infowar.com/P_and_s/p_and_s.html-ssi
Infowar is a security services company

Worldwide encryption mechanisms: cwis.kub.nl/~frw/people/koops/cls-sum.htm
Tilburg University -- Catholic University of Brabant, Netherlands

White Paper on VPNs: www.employees.org/~ferguson/vpn.pdf
Employees.Org is a volunteer group of Cisco employees

US legislation on privacy and cryptography: www.cdt.org/crypto/ **All Valid 7/2000**
CDT is the Center for Democracy and Technology **Most current**