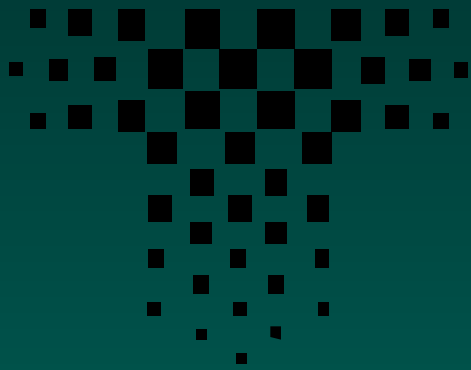


***IETF IPSec and the S/WAN Initiative
Secure Virtual Private Networking on the
Internet***



TIMESTEP
A Newbridge Company

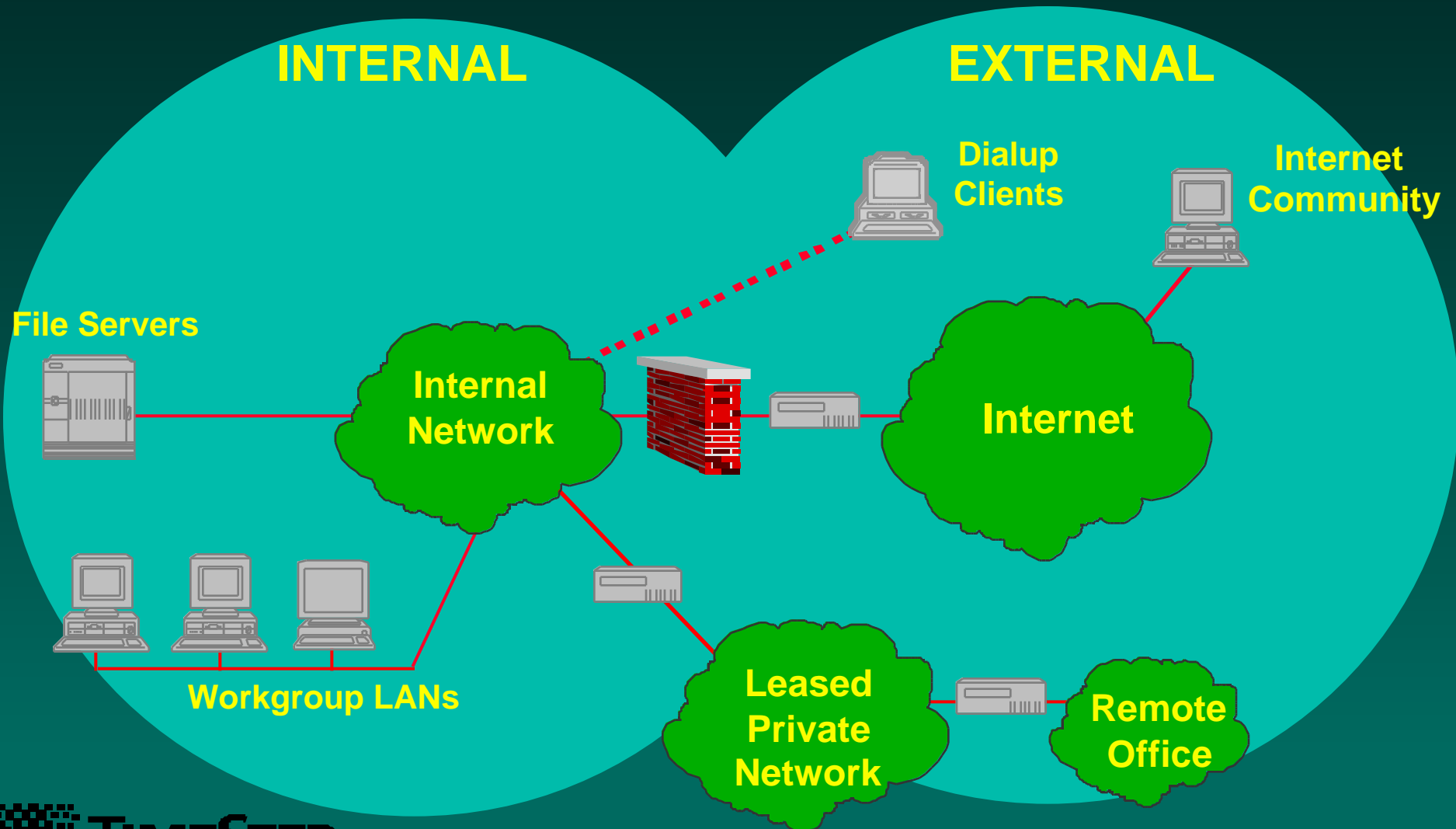
**Tony Rosati
Vice President
TimeStep
Corporation**

Agenda

- **Motivation for using Public Networks**
- **What is a VPN?**
 - Network Addressing Issues
 - Tunneling
 - Security Issues
 - IPSec, SWAN
- **Futures**

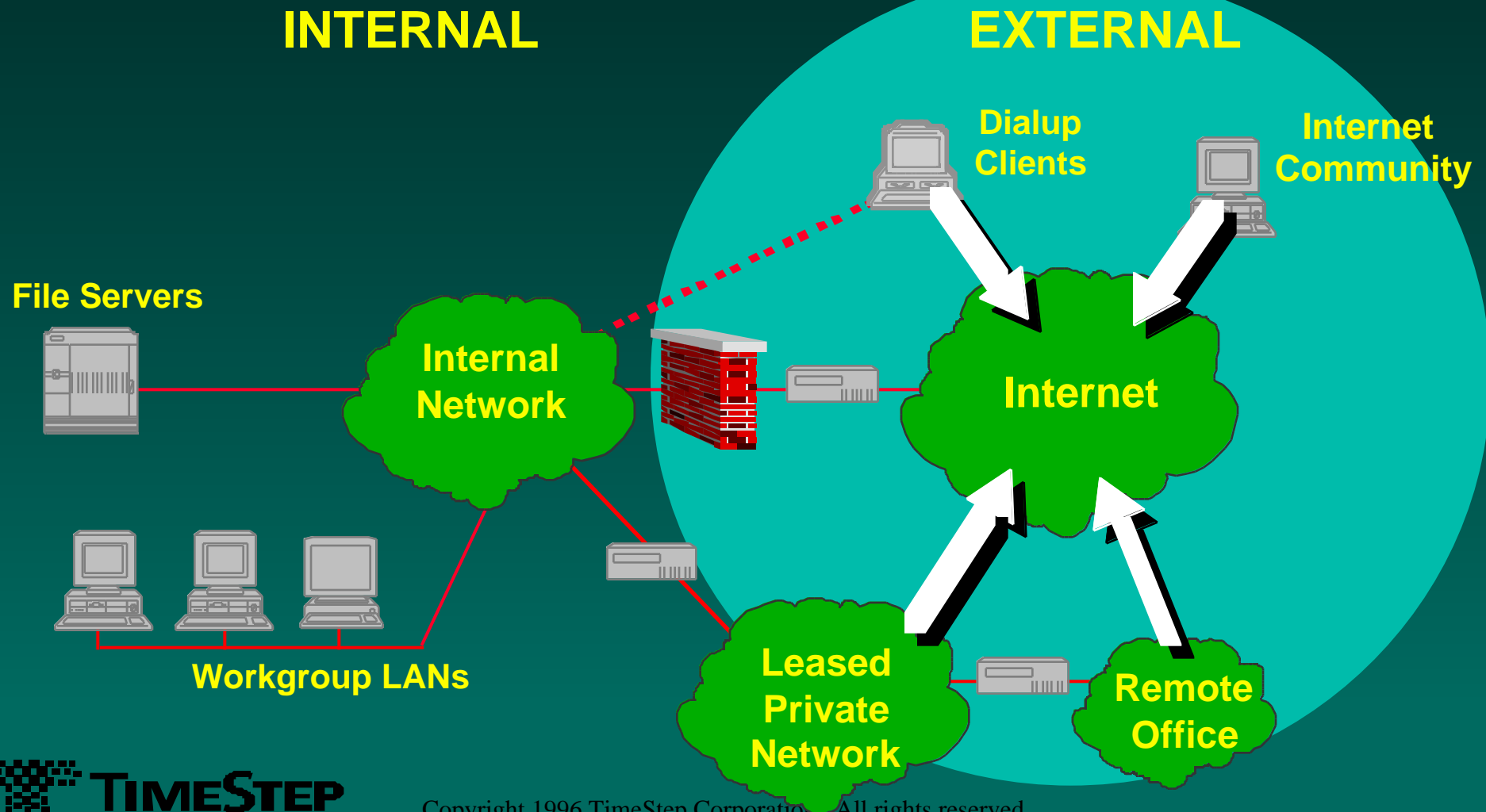
Enterprise Networking

A Mixed Bag of Networking Technologies



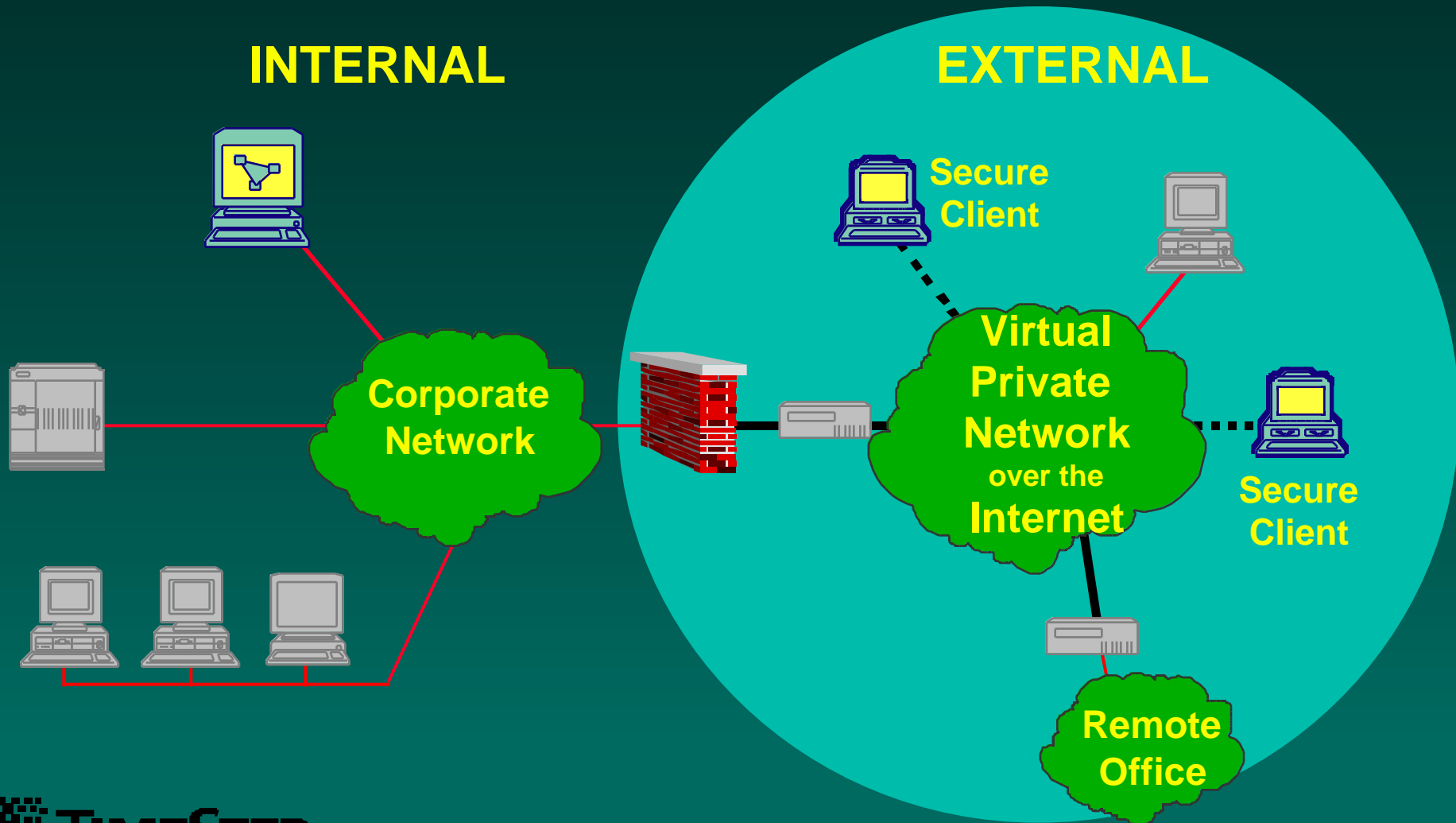
Virtual Private Networking

The Consolidation of Networking Technologies



Virtual Private Networking

Enables Inexpensive and Ubiquitous Networking



Private Network

Expensive

Internal Addresses

Security (Perceived)

Variety of Protocols

Public Network

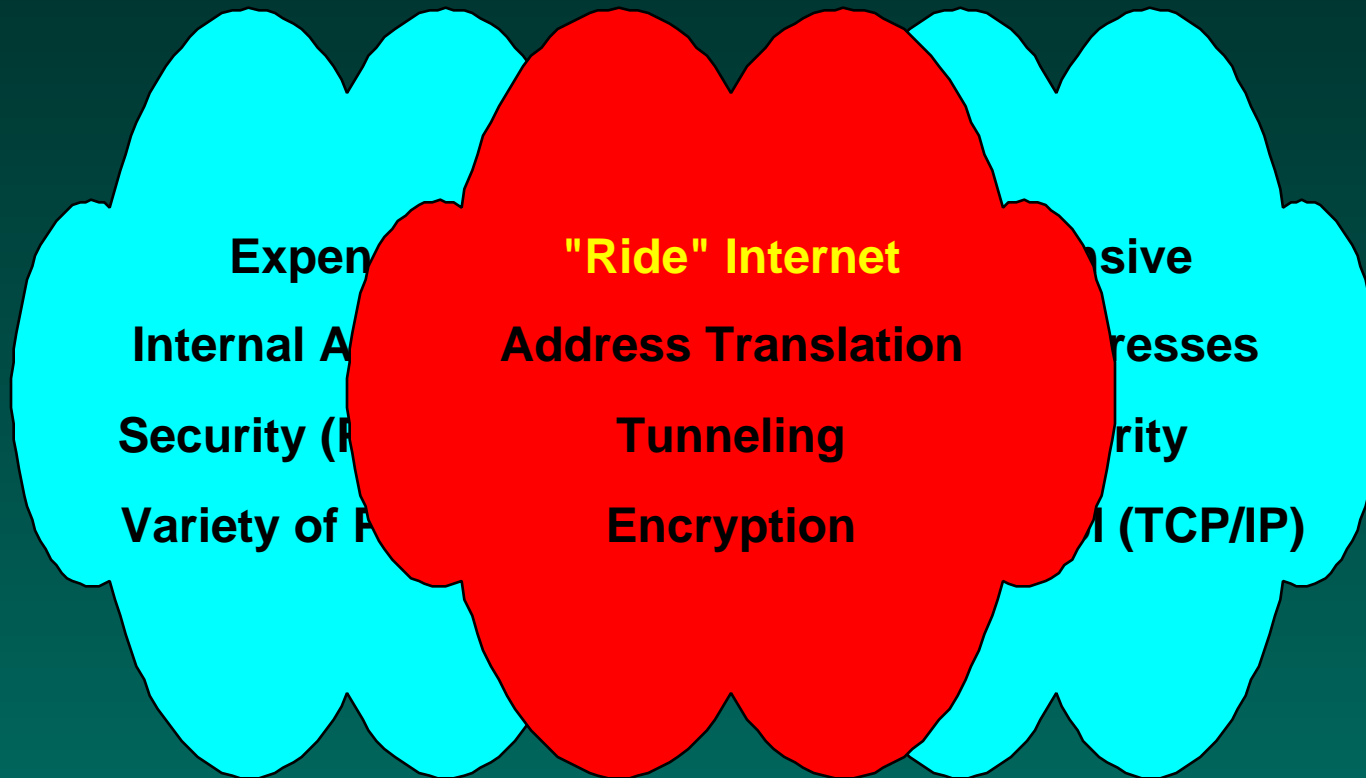
Inexpensive

Global Addresses

No Security

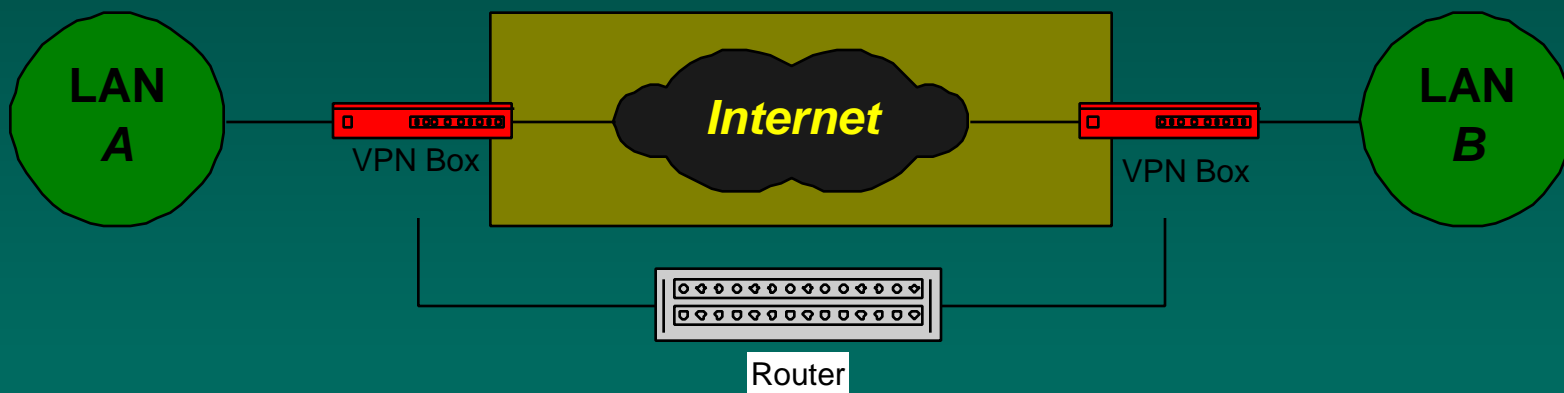
One Protocol (TCP/IP)

Virtual Private Network Solution

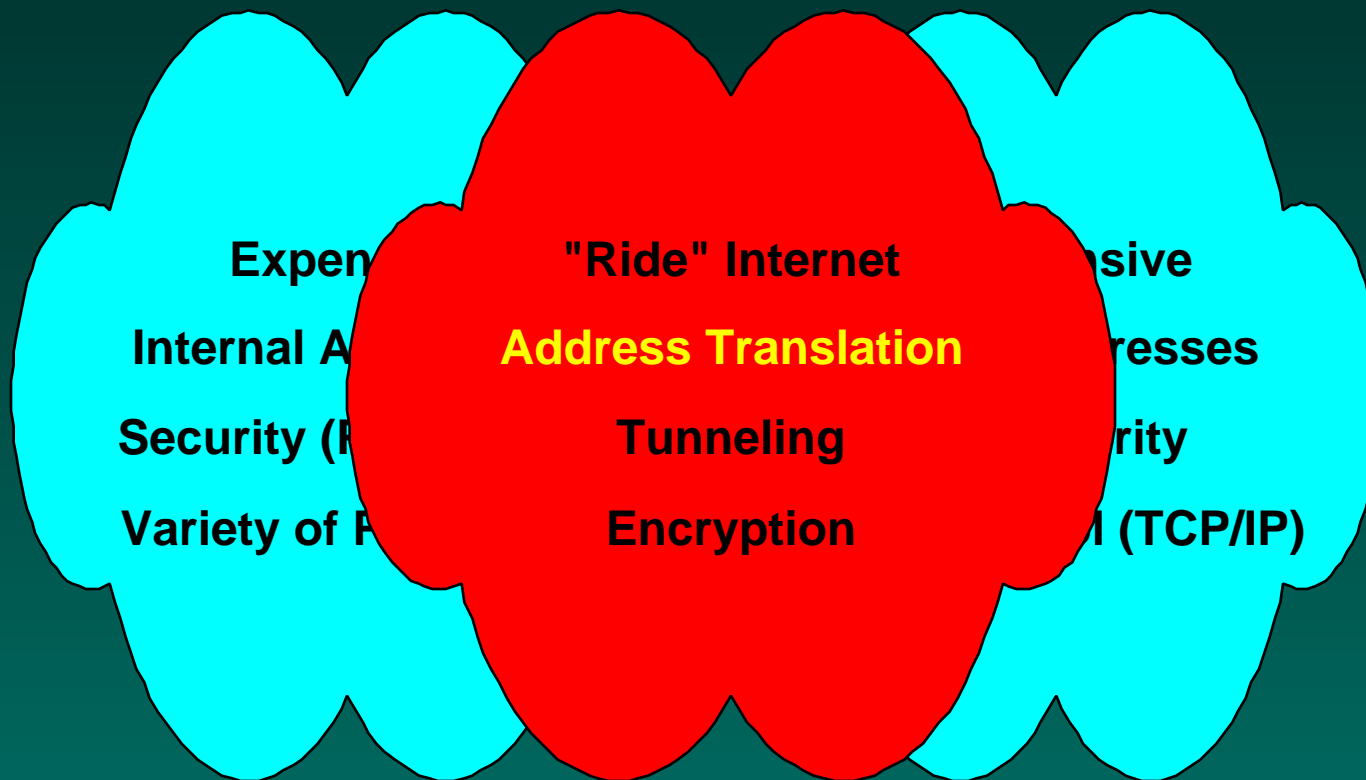


What is a VPN?

- Solutions for interconnecting regionally dispersed networks via Public Networks
- Ideally, connections through Internet are “virtually private” and appear as transparent as a router

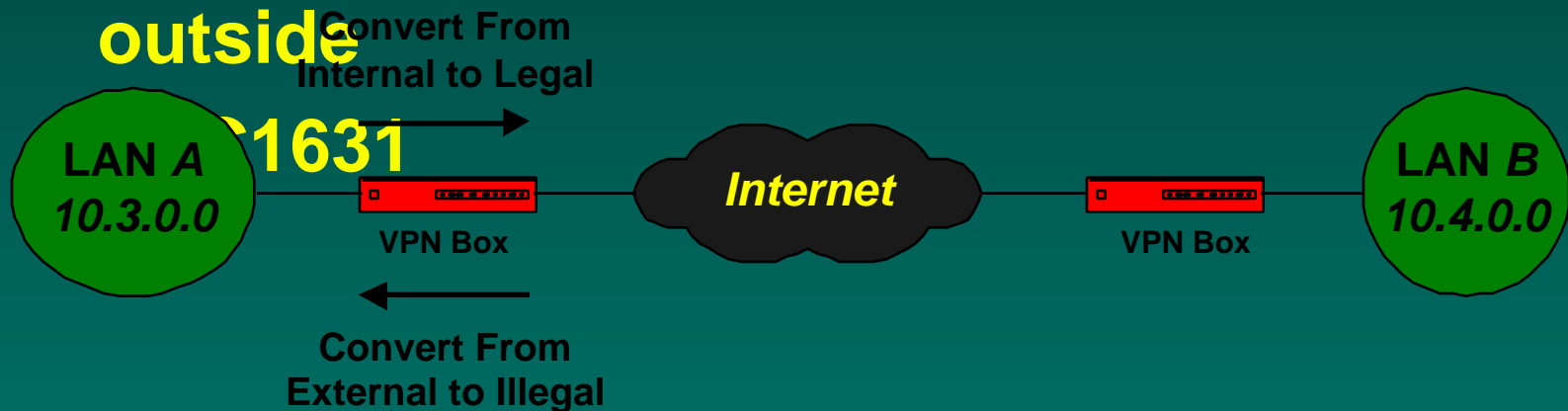


Virtual Private Network Solution

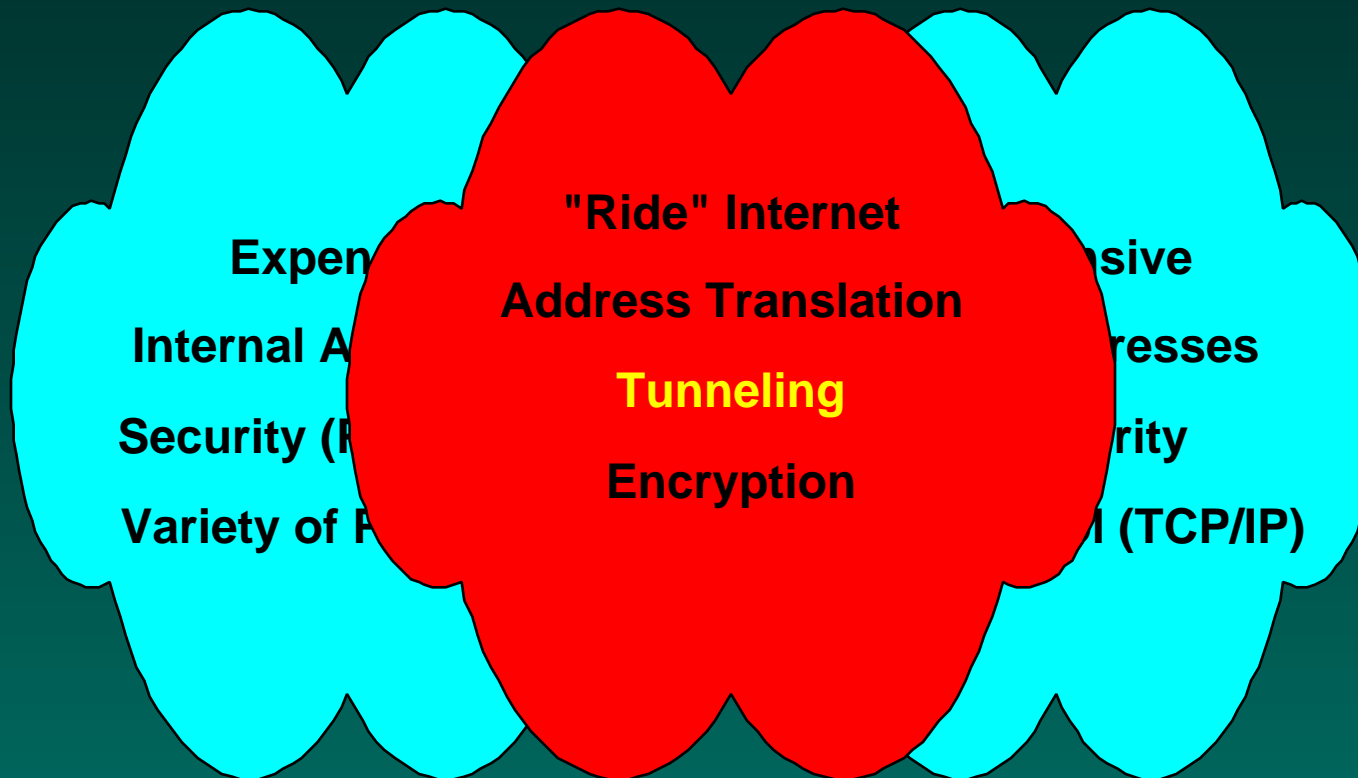


Network Address Translation

- Internal Addresses may be “illegal” on Internet
 - Hides internal topology from outside world
 - Few Class B addresses remaining
- NAT presents only legal addresses to outside



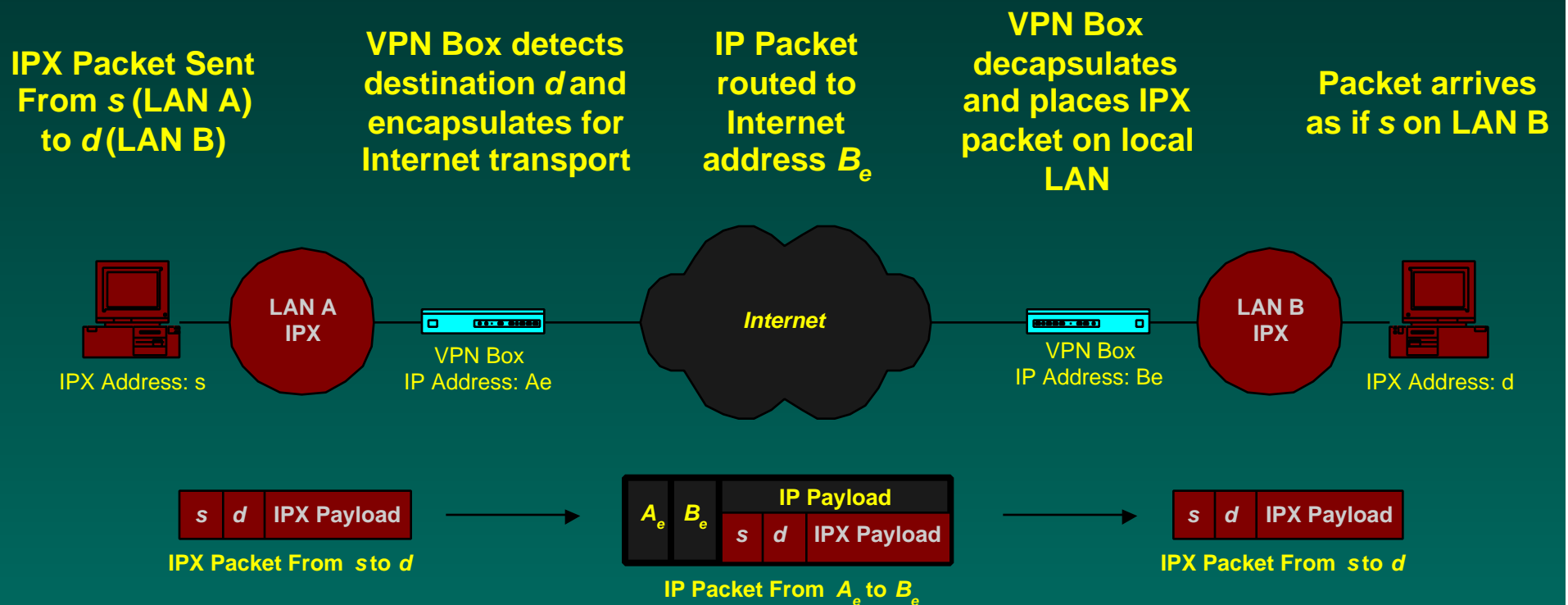
Virtual Private Network Solution



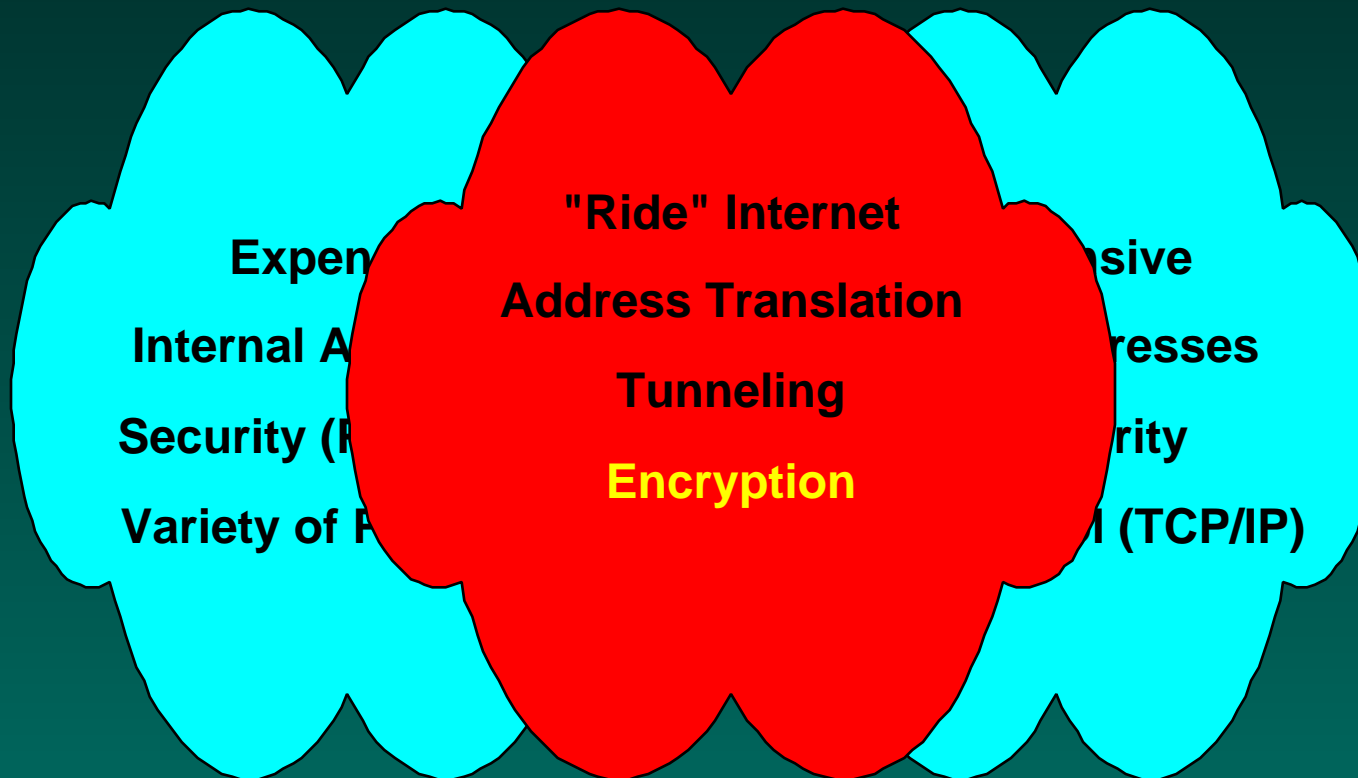
Internet *Tunnels*

- Uses TCP/IP as a carrier for all packets between two sites, regardless of protocols or packet types
- Packets destined for remote LANs are *encapsulated* with TCP/IP headers before they exit
- Packets arriving from remote LANs are *decapsulated* before being placed on the local LAN

Tunnel Example



Virtual Private Network Solution



The role of RSA's S/WAN Initiative

- Promote multi-vendor virtual private networks (VPNs) among firewall and TCP/IP vendors
- To make recommendations and additions to IETF IPSec WG standards

Who's Involved ?

10 Vendors Interoperate!



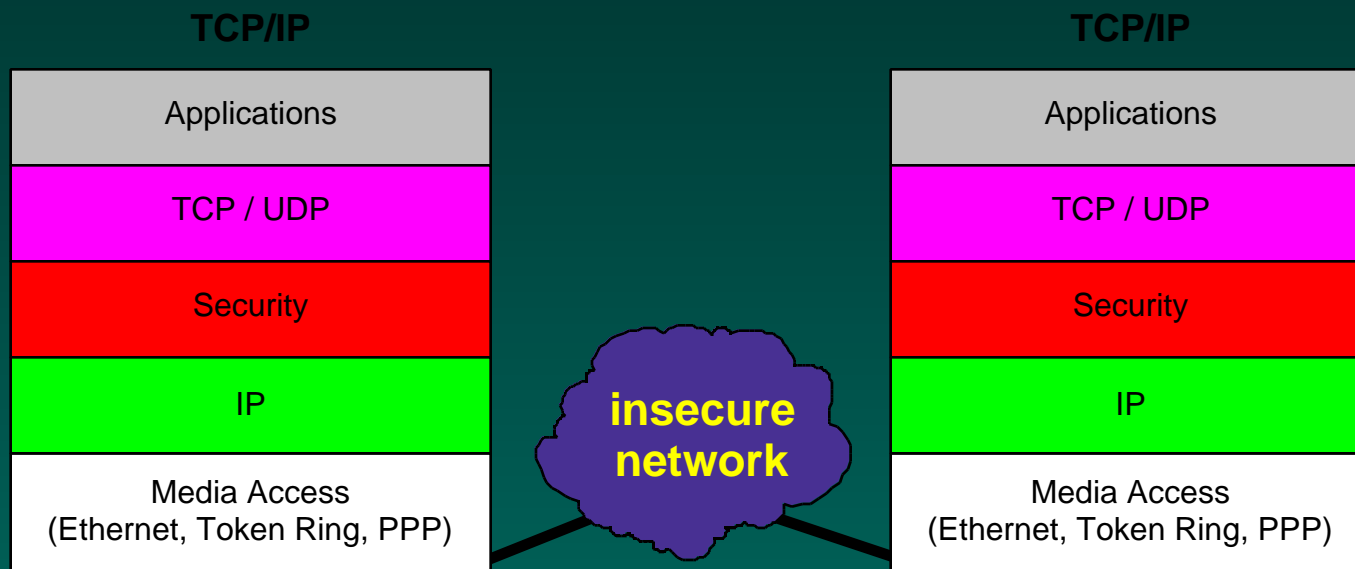
IETF IPSec

Security Standards for IP Network-Layer

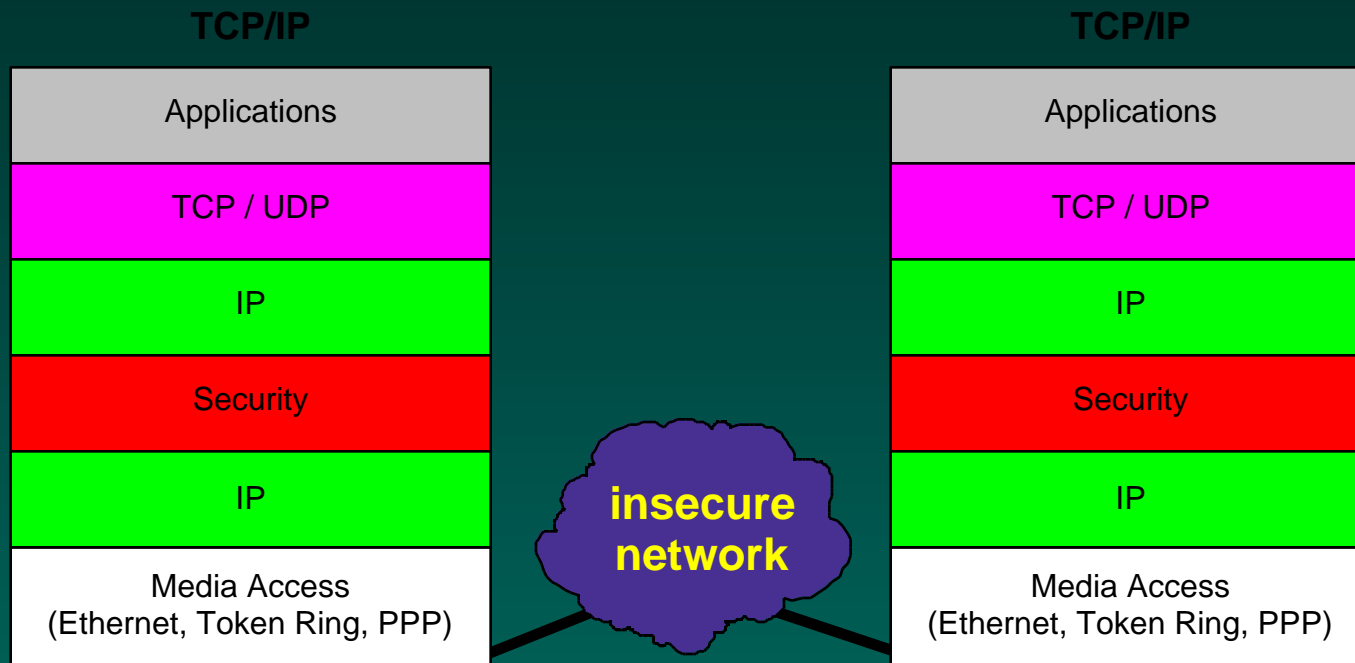
Why Network (IP) Layer?

- **Transparent to applications**
- **Independent of Networking topologies**
- **Limited or No User Impact**
- **Control over all packets for source and destinations**

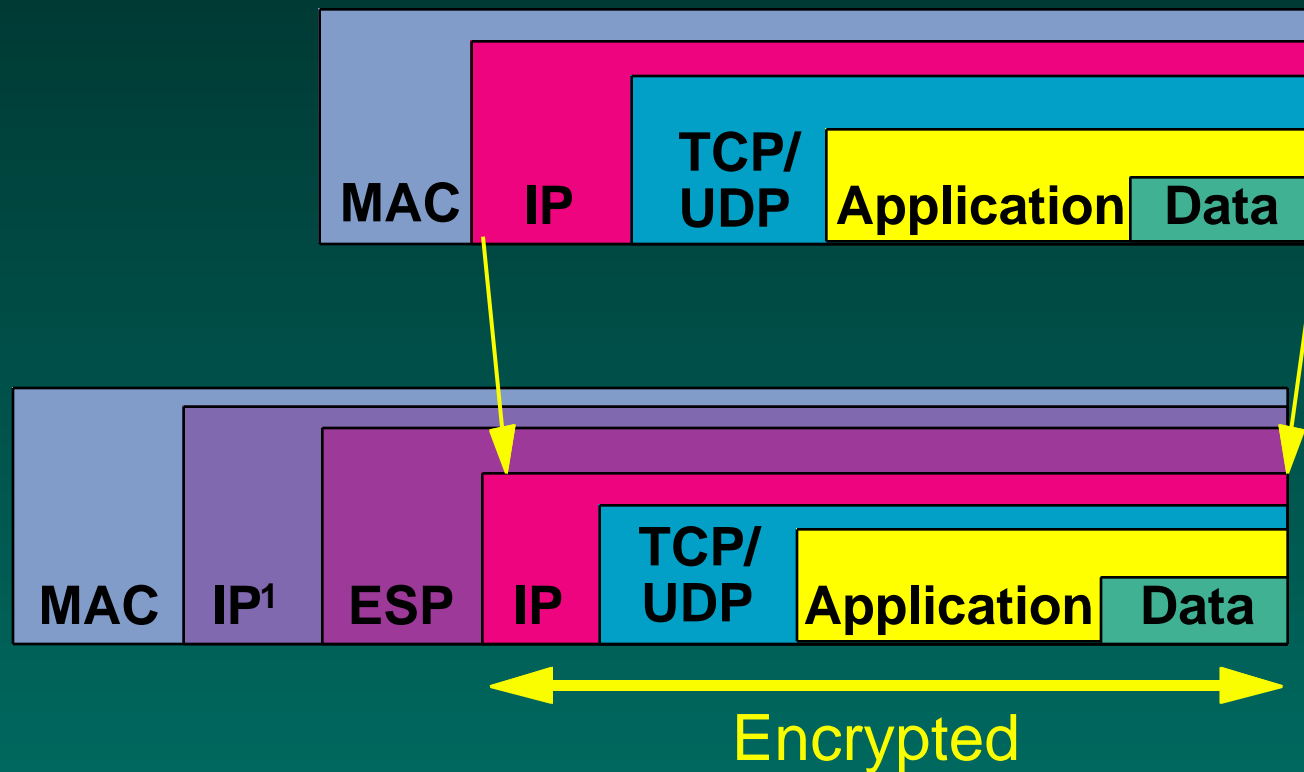
IPSec Transport Mode



IPSec Tunnel Mode



Encapsulating Security Payload (ESP Tunneling Mode)



IPSec Security Architecture

- **Overall Architecture (RFC 1825)**
 - Sets out high-level goals and guidelines
 - Key negotiation and authentication
 - Data confidentiality / Data Integrity
- **Authentication Header (RFC 1826)**
 - General framework for integrity mechanisms
- **Encapsulating Security Payload (RFC 1827)**
 - General framework for confidentiality mechanisms
- **Key Exchange Protocol (ISAKMP/Oakley draft)**

Security Associations

- **Abstraction for any secured connection**
- **Mainly consists of:**
 - partner's identity for the association
 - security mechanisms used
 - keying material
- **Key negotiation phase established SAs**
- **Security processing phase refers to / updates SAs**

IPSec Key Agreement

- **Techniques for securely arriving at Security Associations**
- **ISAKMP/Oakley the mandatory key exchange protocol for IPSec**
 - ISAKMP offers a framework for negotiating security associations
 - Oakley offers a mechanism for negotiating keying material

Cryptographic Algorithms

- **Key Negotiation**
 - Diffie-Hellman
- **Authentication**
 - RSA / DSA
- **Data Integrity**
 - Keyed-MD5 / SHA, HMAC-MD5 / SHA
- **Encryption**
 - DES, 3-DES, RC5

ISAKMP & Oakley

- **ISAKMP: Internet Security Association and Key Management Protocol**
 - defines protocol structures
- **Oakley Key Exchange Protocol**
 - defines how to combine ISAKMP structures in a handshaking mechanism

Oakley Main Mode

- **Negotiate policy under which to protect subsequent communication**
- **Exchange Diffie-Hellman public values and any ancillary information necessary to complete the exchange**
- **Authenticate the Diffie-Hellman exchange**
- **Identity Protection**

Oakley Quick Mode

- Only used when an existing ISAKMP Security Association has been established
- Used to establish ESP and AH Security Associations

Oakley Aggressive Mode

- Can be used instead of Main Mode
- Does not provide identity protection
- Faster than Main Mode

ISAKMP Security Association

- **Situation**
 - Identity
 - Secrecy
 - Integrity
- **Proposal**
 - Protocol
 - Transform
 - Transform Attributes

ESP Transform Example

ESP-DES-MD5

- Combined privacy, authentication, integrity and replay prevention
- Privacy = DES CBC
- Integrity = HMAC MD5
- Replay prevention = Counter

ESP-DES-MD5 Example

- **Packet Format**
 - Security Parameter Index (SPI)
 - Initialization Vector (IV)
 - Replay Prevention Field
 - Payload data + padding
 - HMAC Digest

How will IPSec work with other security standards?

What IPSec Doesn't Cover

Security Policy

- **Who talks to whom at what security level?**
 - Clear, Blocked
 - Confidential using DES, RC5, Skipjack...
 - Data integrity using keyed MD5, SHA...
- **How do we monitor control the security policy?**
 - Alarms, Audit trail...

What IPSec Doesn't Cover

Public Key Exchange

Options for obtaining public keys

- Certificates (PKIX)
 - many vendors offer PKI
- DNS Entries (DNSSEC)
 - gaining some momentum since DNS infrastructure exists
- Web-of-Trust
 - used for PGP
 - less maintainable and scaleable

Certificates

- Form of Digital Identity
- Binds ID to Public Key
- Signed by Trusted Authority (CA)
- ITU X.509v3 Structure

ID:	"John Smith"
Public Key:	RSA-512: 451f6c882..8b
Serial Number:	2772-18811
Expiry:	January 1, 1998
Issuer:	2770-19199

CA Signature:	DSA: 177f31cbe94..1f
---------------	----------------------

Public-Key Infrastructures (PKIs)

- Who maintains certificates?
- Protocols for obtaining them?
 - HTTP, LDAP, SNMP
- PKIs offer technology or services or both
- Corporate-Wide Certificate Authorities
- World-Wide CAs with Hierarchical-

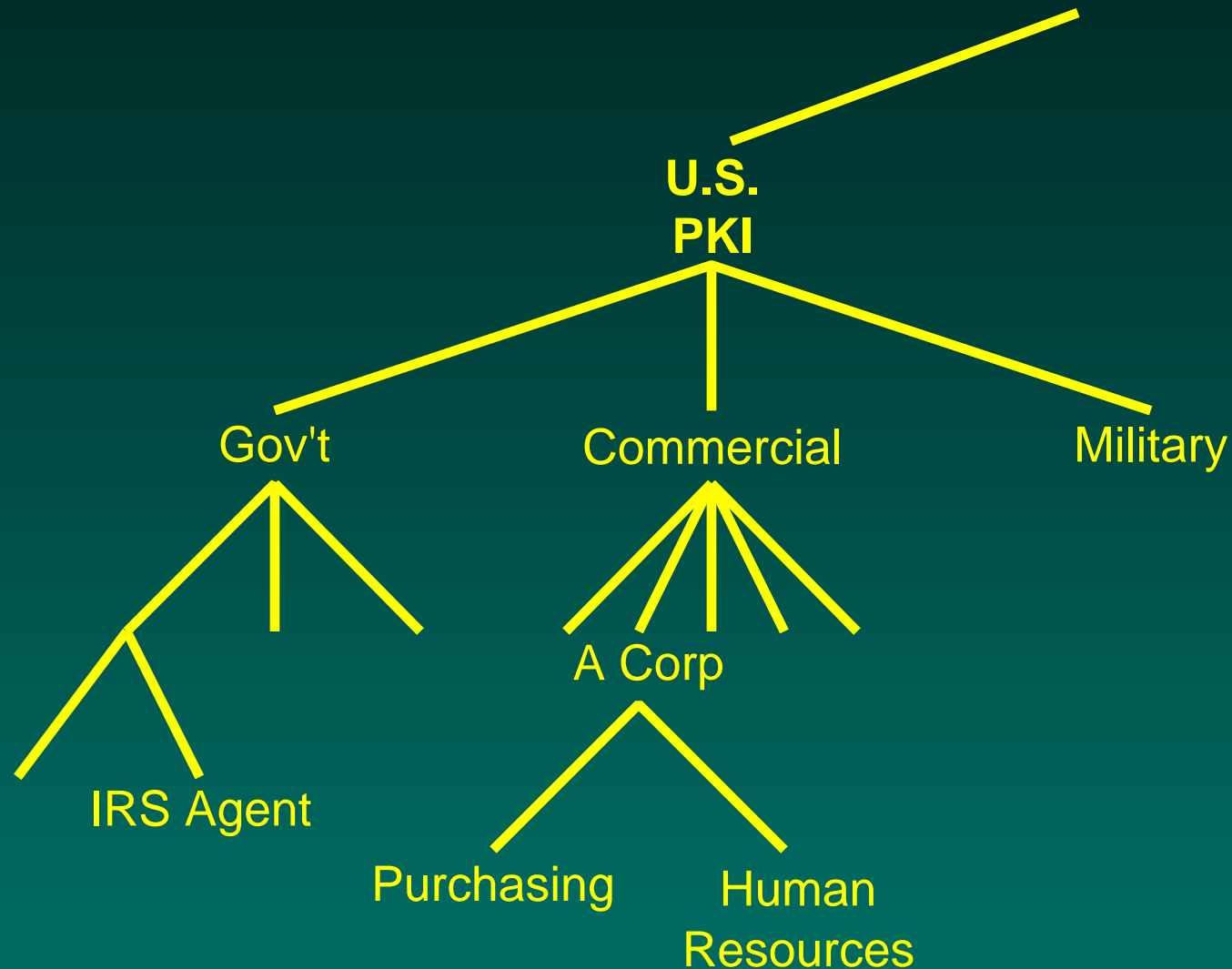
Certification



TIMESTEP

Copyright 1996 TimeStep Corporation. All rights reserved.

Hierarchical CA PKIs



Other VPN Related Work

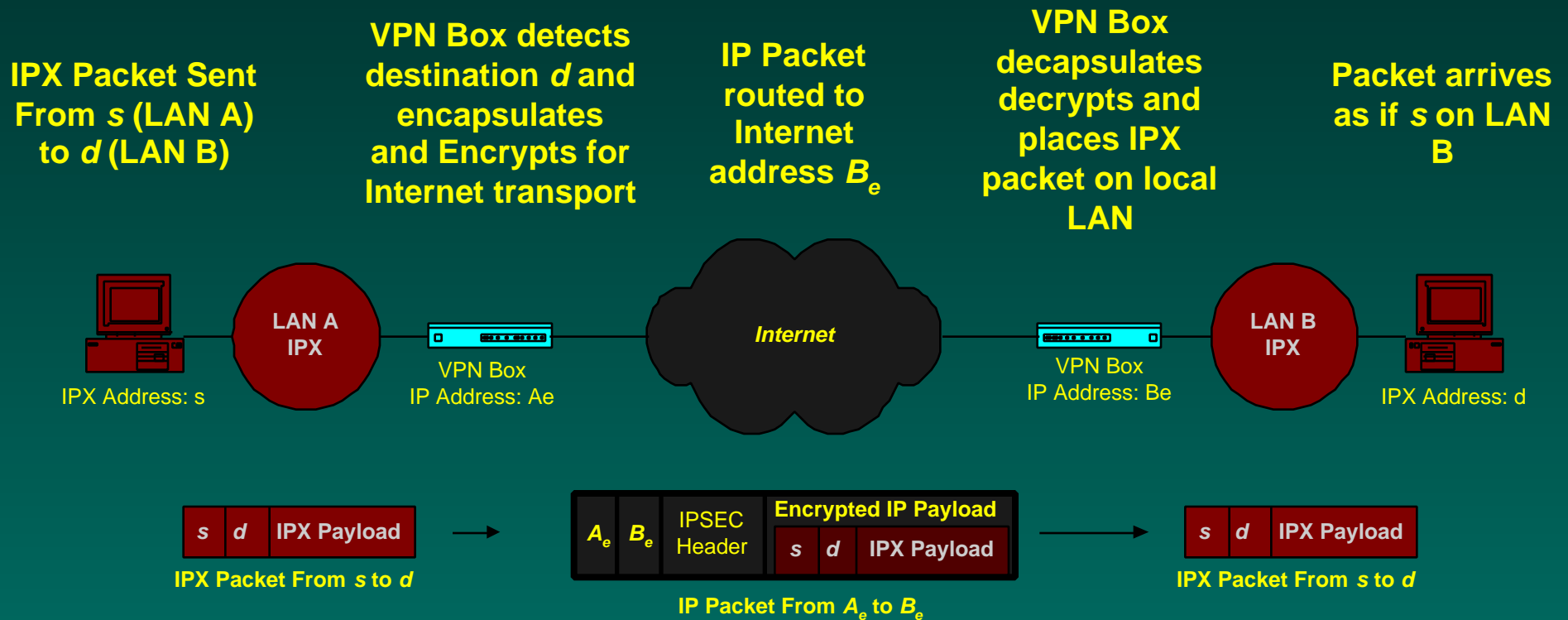
Protection of Keys

- **Standards related to the protection of keys**
 - FIPS 140-1
- **Hardware devices**
 - Dedicated VPN Boxes
 - PCMCIA Cards
 - Smart Cards
 - RSA PKCS#11 CRYPTOKI

Putting it all Together

Encrypted Tunnels with Address Translation

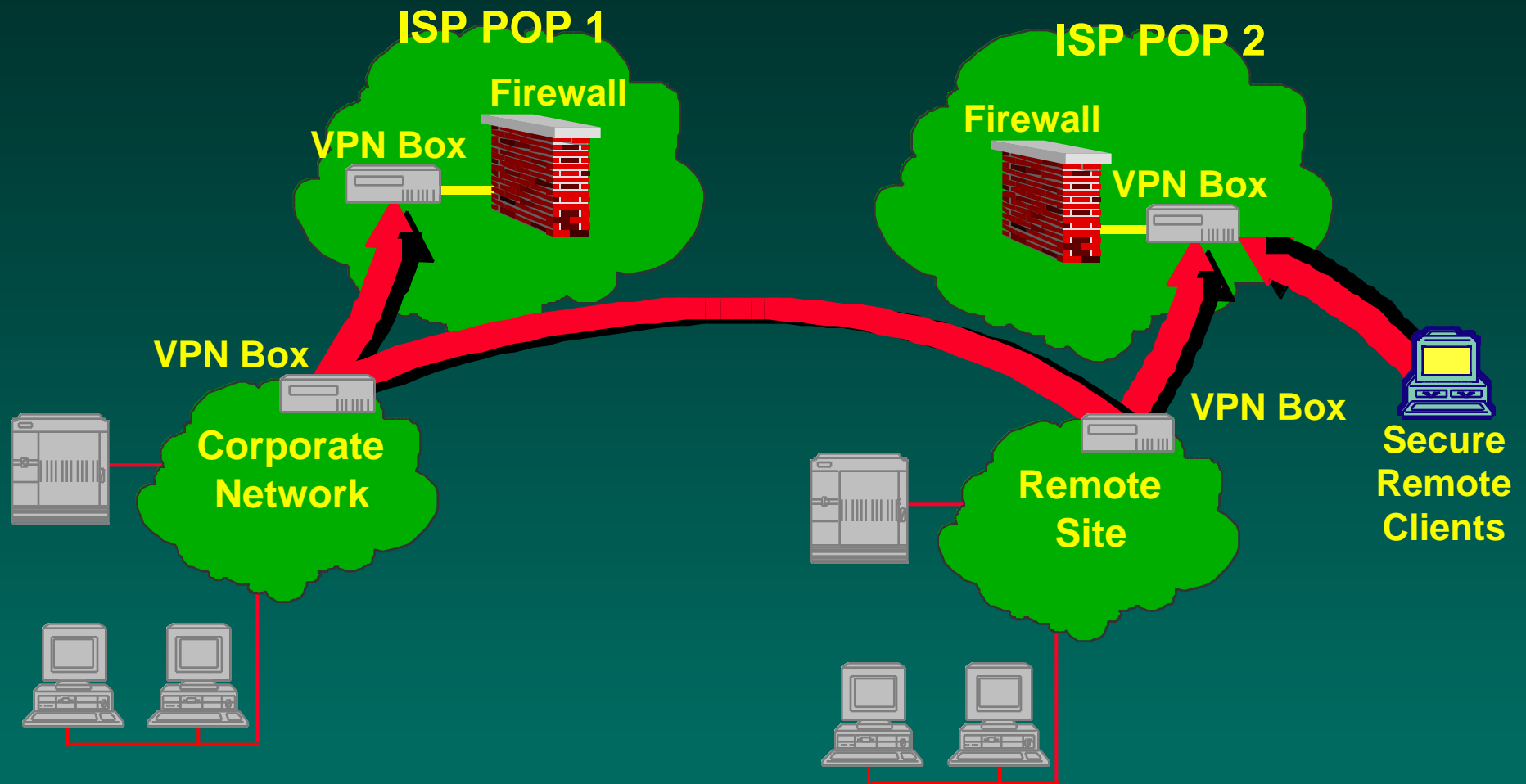
Encrypted Tunnels



Internet Tunneling Possibilities

Internet Tunneling

Complement and Maximize Firewall Usage



In Conclusion...

- Internet is exploding, offering cheap expansive WAN connections
- VPN offers standards-based techniques for riding the Internet with confidentiality and integrity
- VPN solutions are upon us...

Contacting TimeStep

info@timestep.com

<http://www.timestep.com>

TimeStep Corporation
362 Terry Fox Drive
Kanata, Ontario, K2K 2P5
Phone: (613) 599-3610
FAX: (613) 599-3617
1-800-383-8211



Copyright 1996 TimeStep Corporation. All rights reserved.