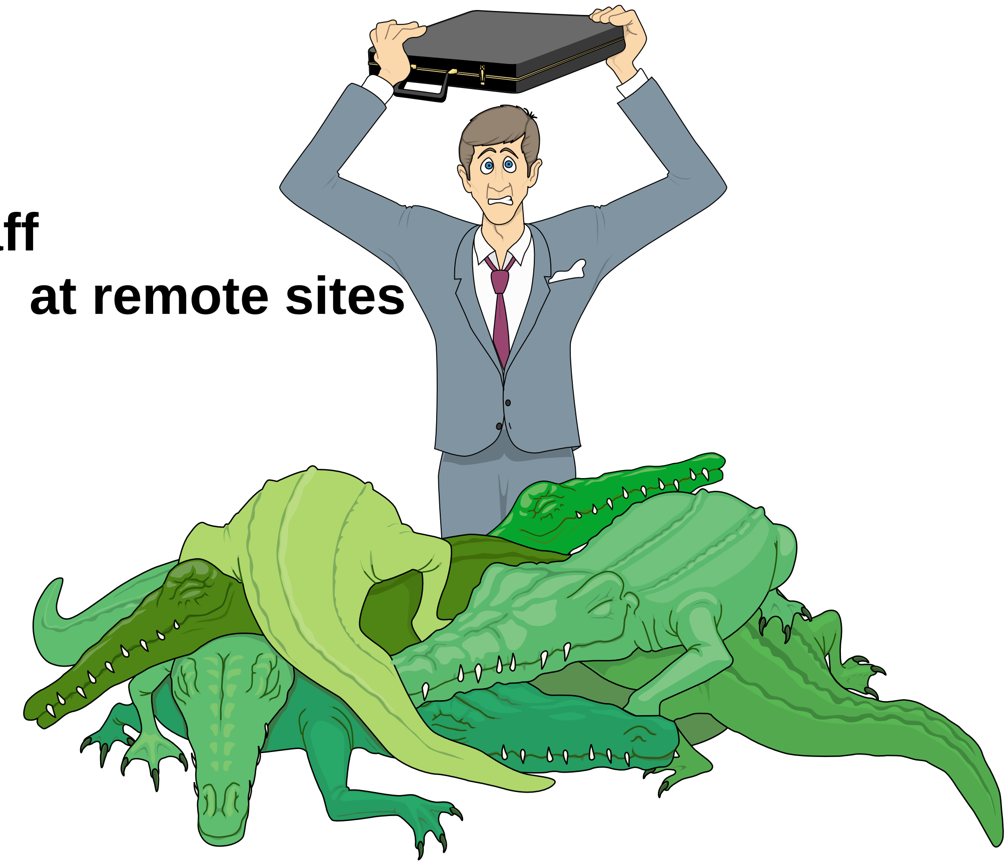
Building, Implementing, and Managing a VPN (Virtual Private Networks)

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

Outsourced VPNs



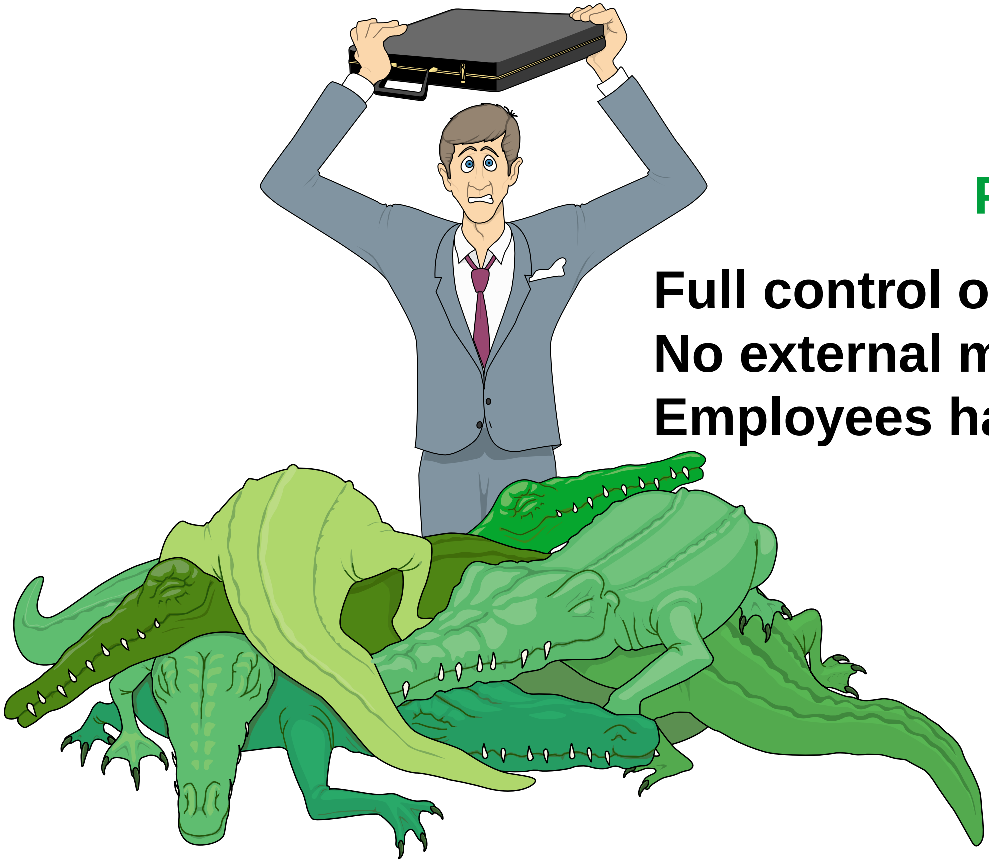
Positive

Lowers workload on IT staff
Handles connection setup at remote sites
High level of ISP service

Negative

Limited internal control of hardware
Complex security integration
Users must use specific ISP

Inhouse VPNs



Positive

Full control of VPN setup and management
No external management links to network
Employees have wide choice of ISPs

Negative

Internal help desk bears brunt of handling VPN problems
Add staff to handle deployment and management
Limited control over ISPs used

VPN Needs

Client configuration and security

VPN and network integration

ISP services

Performance metrics

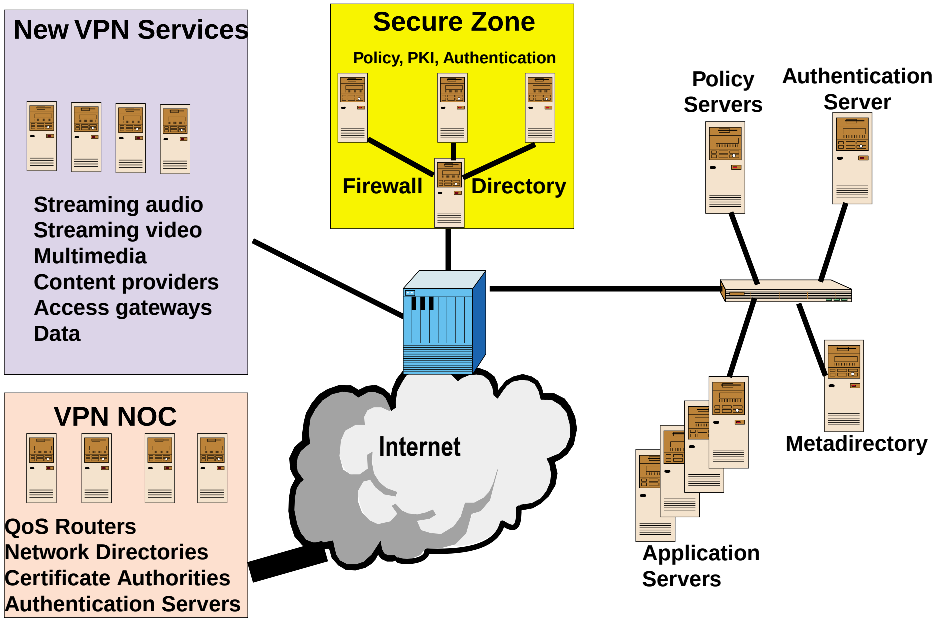
Administration

Service level management

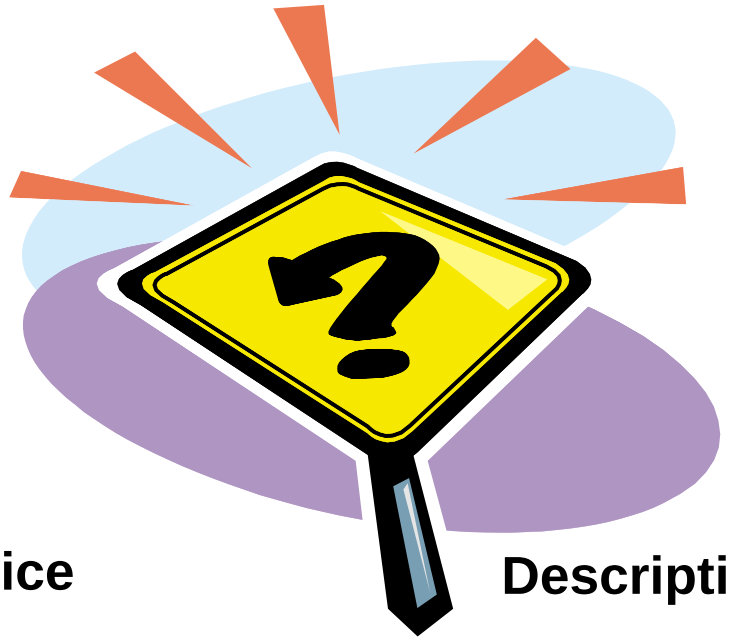
Reporting and management

Help desk integration

Extensibility



ISP Selection of Services

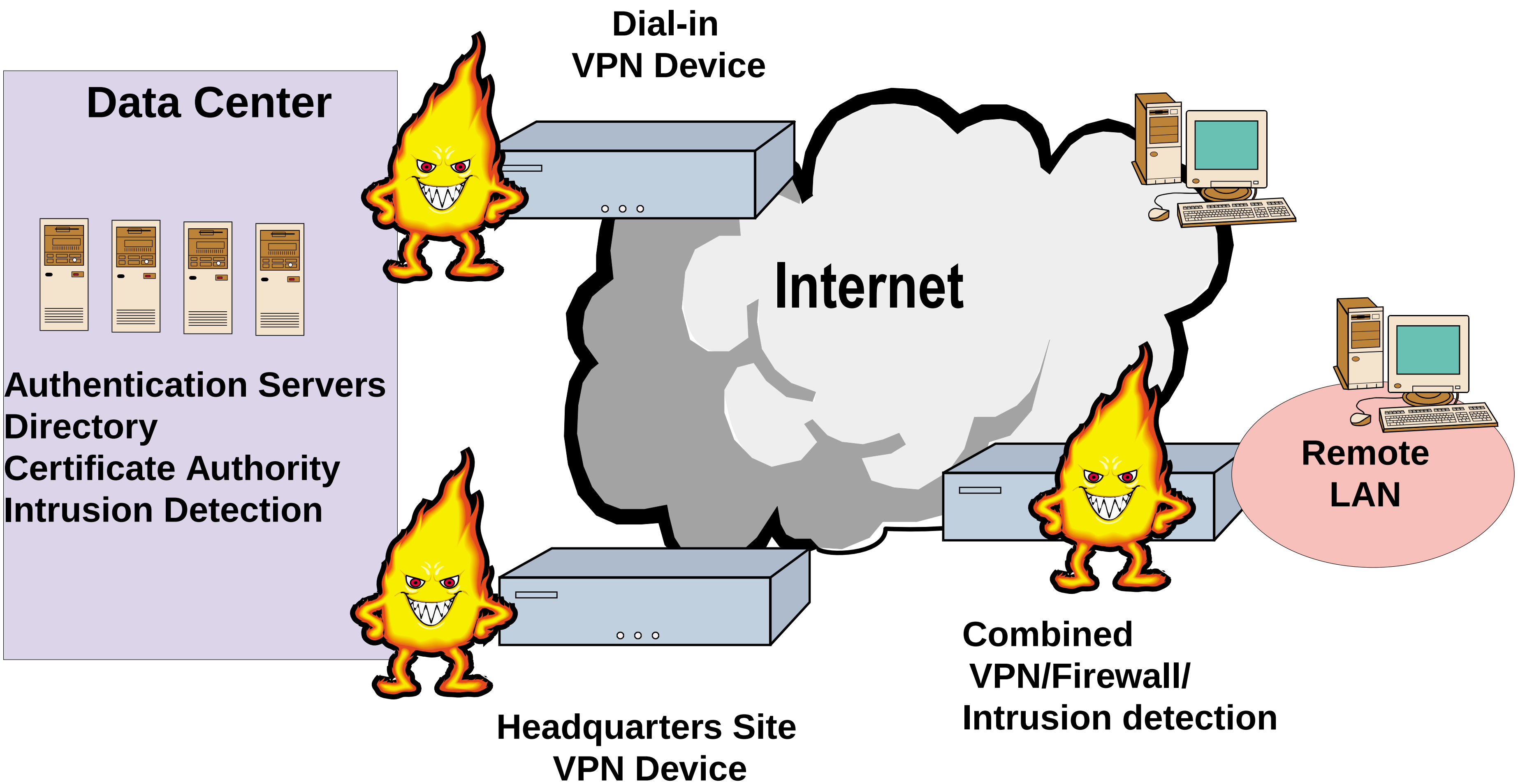


Type of Service	Description
Access	ISP supplies backbone, IT manager all else
SLA on ISP network	Guarantees on network latency and availability
Managed VPN equipment	ISP installs, configures, and manages VPN equipment
Turnkey VPN systems	ISP installs, configures and does day-day management
SLAs on VPN	Up time and latency applied to VPN equipment
SLAs on dial access	Guarantees on dial access speeds and call failure rates
Authentication services	ISP handles user authentication
Key management	Provider responsible for key distribution/revocation
Certificate authority	Higher level of security
Managed security services	ISP manages firewalls and security servers
VPN client deployment	Software distribution responsibility of ISP
End user support	Initial point of contact

Three Uses of VPNs

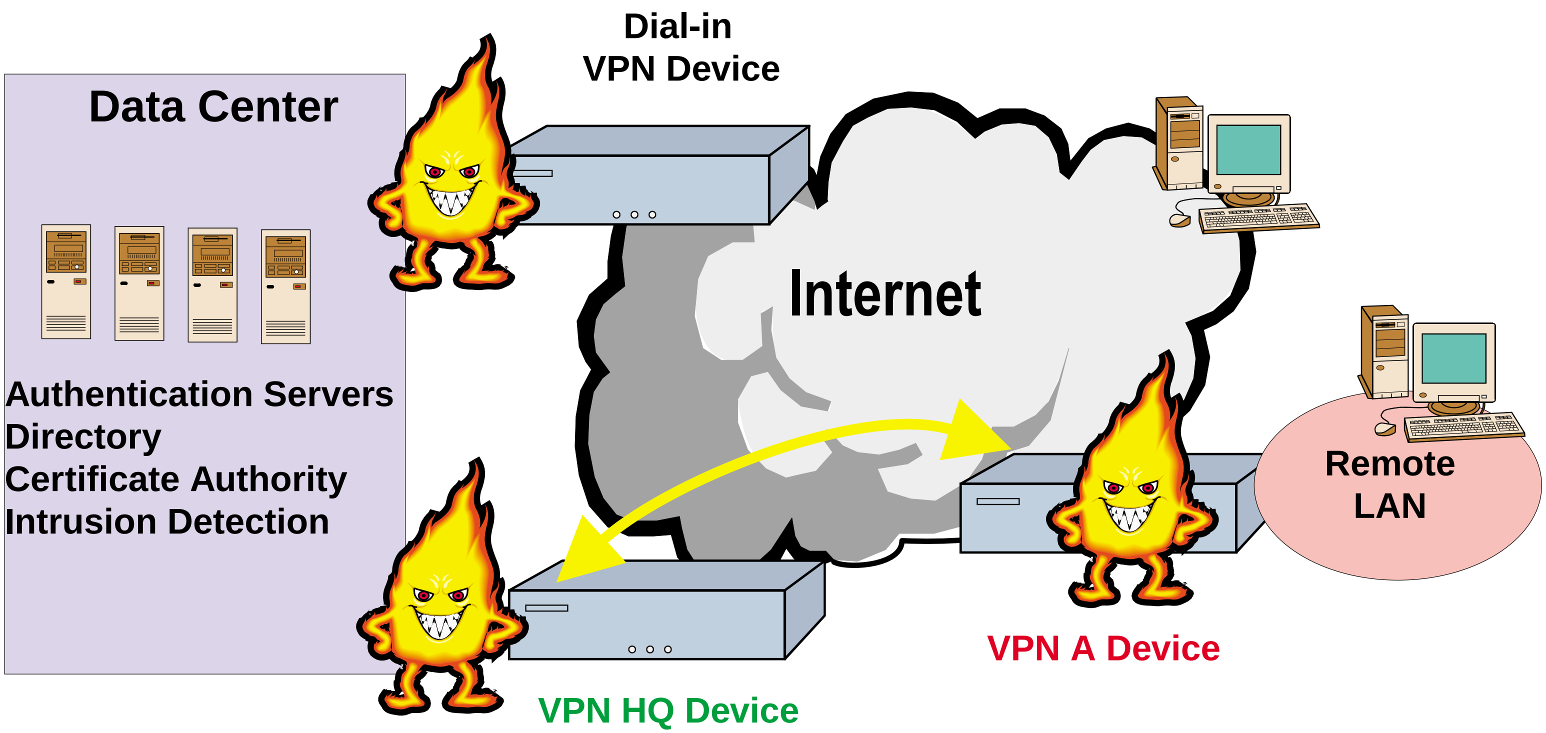
Use	Application	Alternative To	Benefits
Remote Access VPN	Remote Connectivity	Dedicated Dial ISDN	Ubiquitous Access Lower Cost
Intranet VPN	Site-to-Site Internal Connectivity	Leased Line	Extend Connectivity Lower Cost
Extranet VPN	Business-to-Business External Connectivity	Fax, Mail , EDI	Facilitates E-Commerce

VPN - Key Security Items



VPN devices authenticate themselves before establishing the tunnel
VPN devices set up session encryption over the tunnel
End users must authenticate themselves

VPN - VPN Device Authentication
Manual Key Distribution

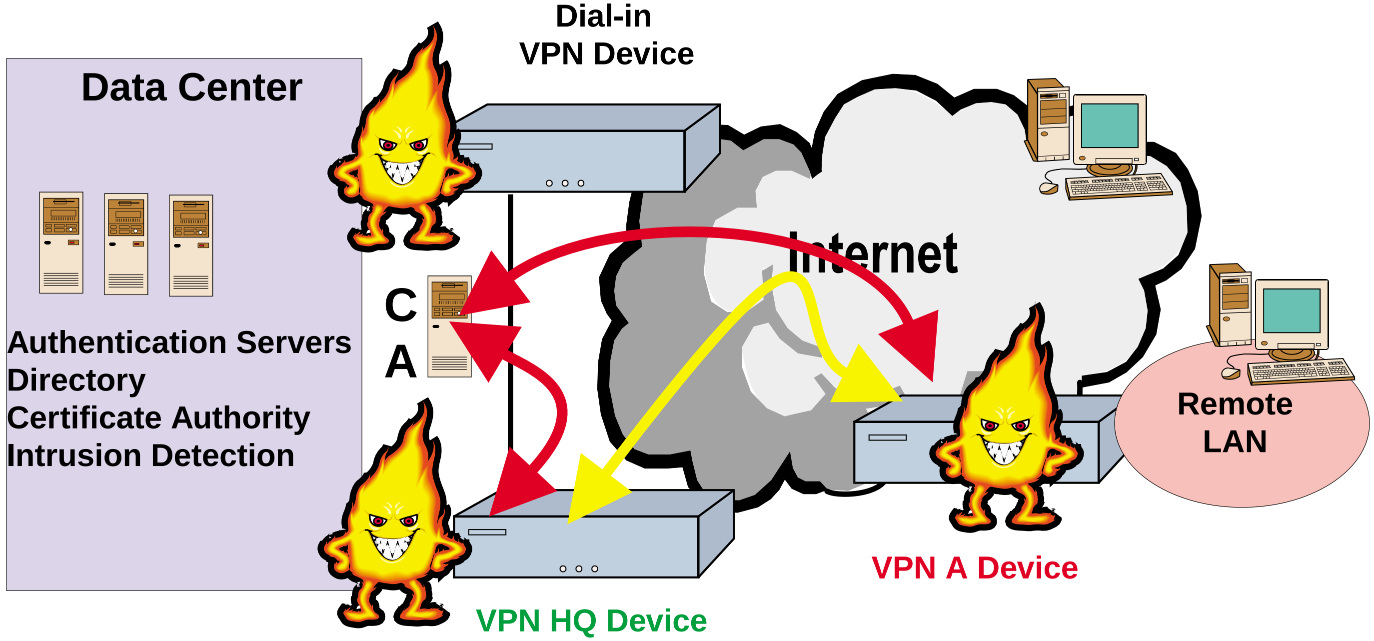


Public/Private keys manually entered into VPN devices

VPN A wants to set up a tunnel with VPN HQ
VPN A sends request encrypted with VPN A private key
VPN HQ uses VPN A s public key to decrypt - VPN HQ communicating with VPN A
VPN HQ sends response with encrypted with VPN HQ private key
VPN A uses VPN HQ s public key to decrypt - VPN A communicating with VPN HQ

Not scalable

VPN - VPN Device Authentication Digital Certificate Key Distribution

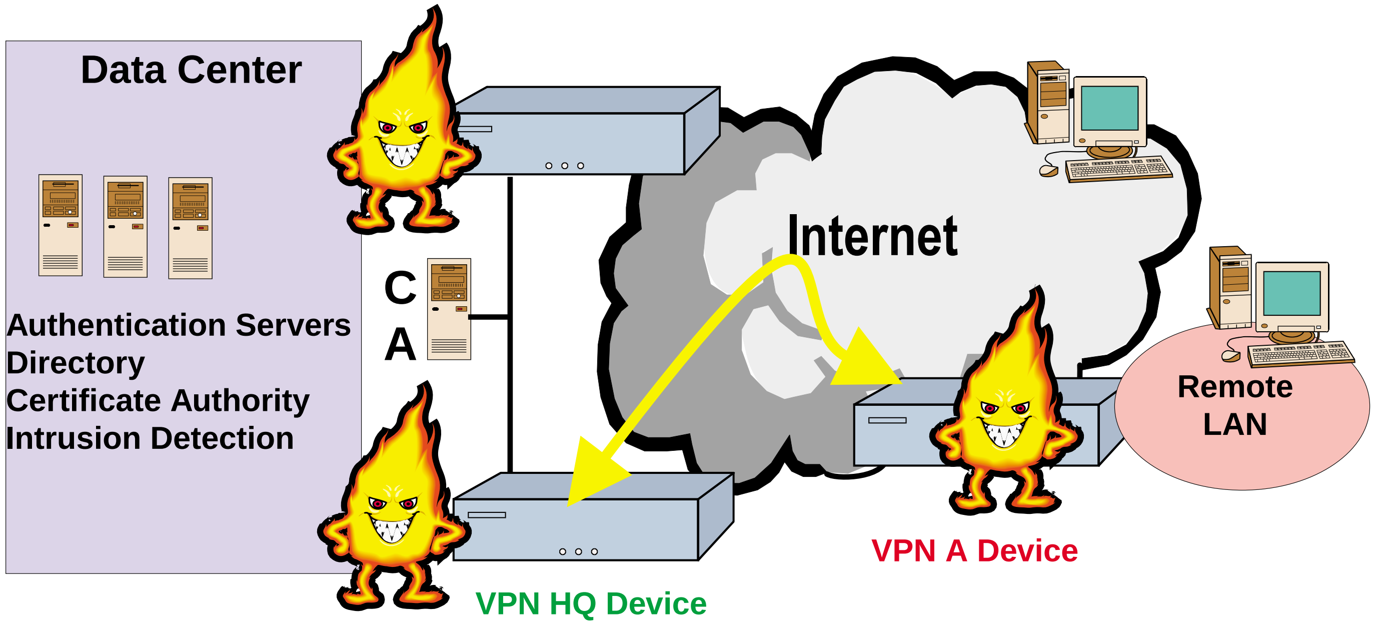


VPN A wants to initiate a tunnel with VPN HQ

VPN A generates a private/public key pair
sends the public key to the CA (certificate authority)
VPN HQ generates a private/public key pair
sends the public key to the CA and registers it
VPN A initiates private key encrypted tunnel request with VPN HQ
VPN HQ asks CA for VPN A public key, decrypts request, validates from VPN A
VPN HQ issues private key encrypted response to VPN A
VPN A asks CA for VPN HQ public key, decrypts request, validates from VPN HQ

VPN - Session Keys

Protocols like IPSec and L2TP/IPSec require key exchanges



VPN A wants to initiate a secure session with VPN HQ

VPN A generates a random symmetric key for this session
VPN A encrypts the symmetric key with the public key of VPN HQ
VPN HQ receives, decrypts with his private key
VPN HQ can now have a secure session with VPN A, both using random keys

VPN - Ways to Authenticate Users

Passwords

One-time passwords

Challenge response system
(Radius or TACACS)

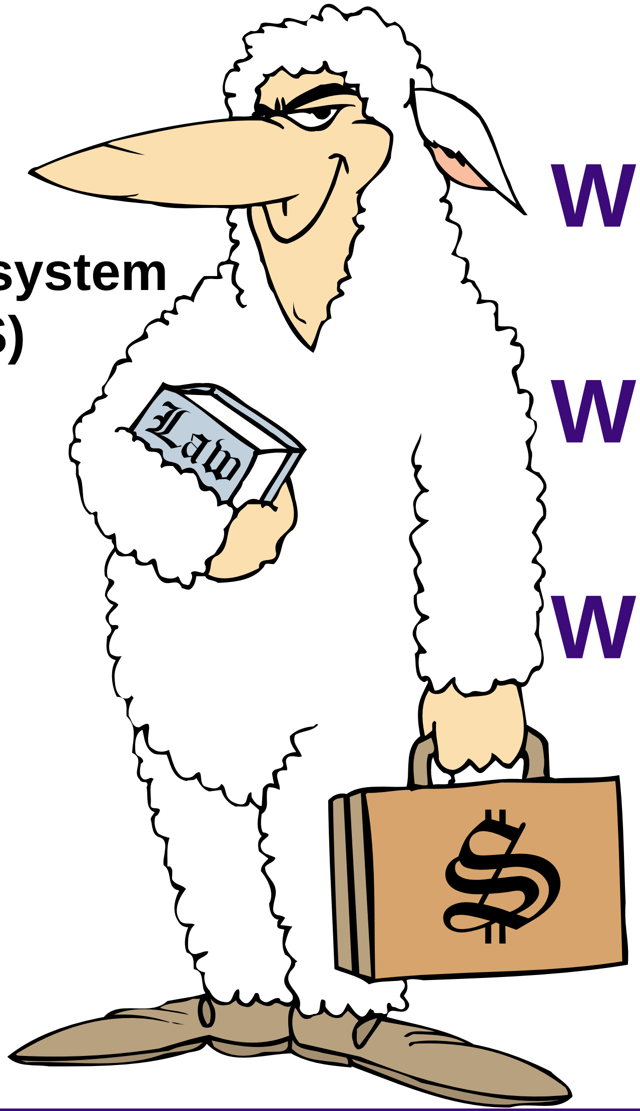
Token systems

Biometrics

Digital certificates

Smart cards

Combinations

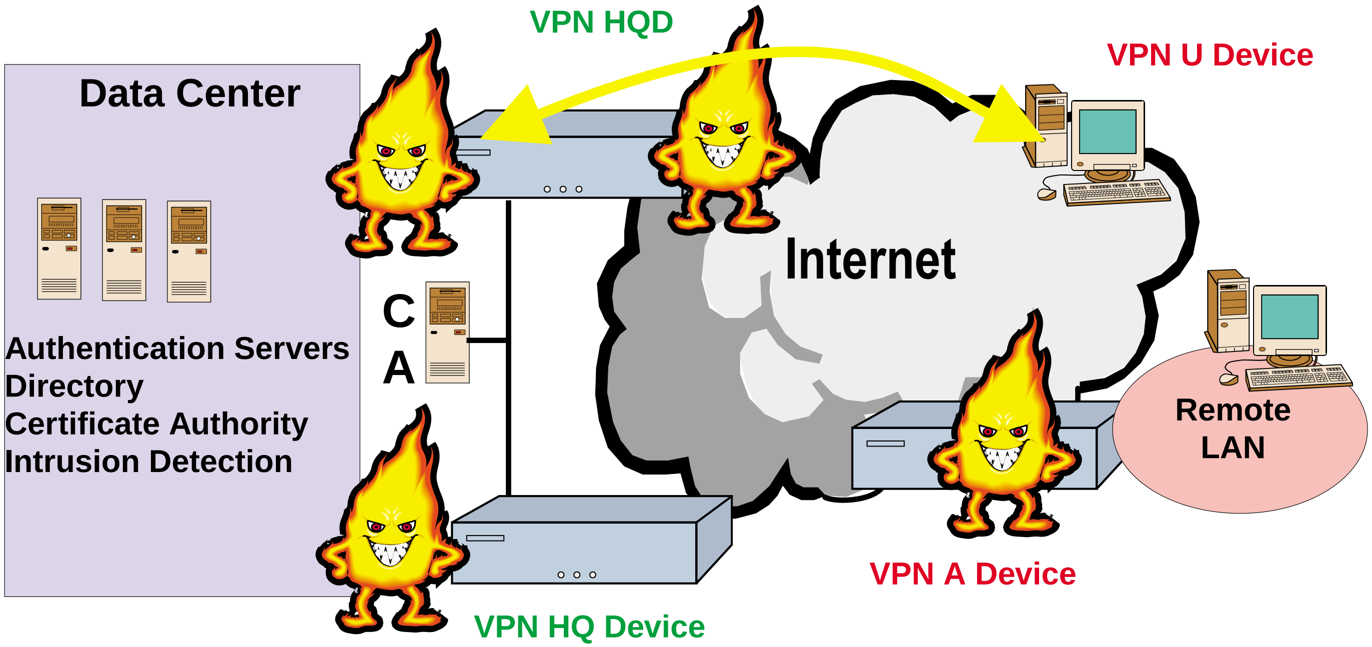


What you know

What you have

Who you are

VPN - User Authentication Using Certificates



VPN U wants to initiate a tunnel with VPN HQD

A digital certificate and a private key was generated by a certificate manager
Digital certificate distributed to the VPN U normally via e-mail or HTTP
VPN HQD asks CA for VPN U public key, decrypts request, validates from VPN U
VPN HQD issues private key encrypted response to VPN U
VPN U asks CA for VPN HQD public key, decrypts request, validates from VPN HQD

VPN - Managing an In-House CA

Generate a private/public key pair or store a user generated public key

Issuing public keys

Maintain a repository

Revoking certificates

Maintaining key life cycle

Key backup and recovery

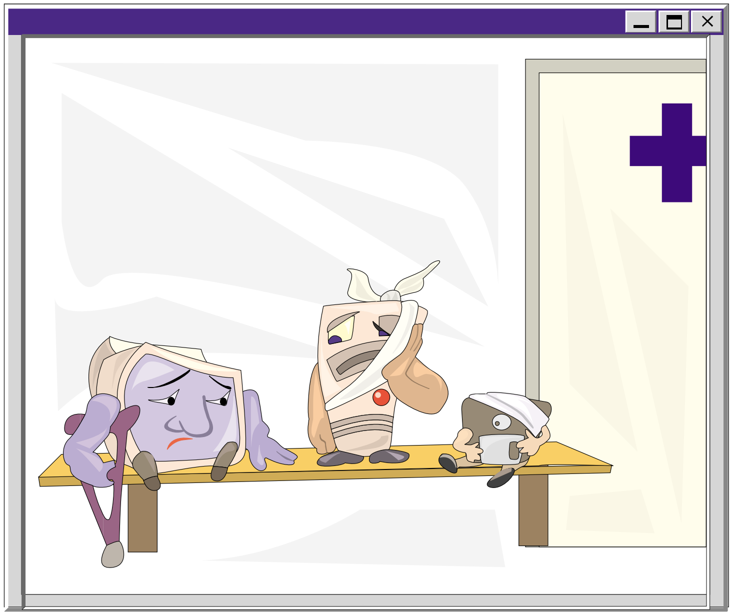
Automatic updates of key pairs

Maintaining key histories

Issuing CRL (certificate revocation list)

VPN - Need CA to Support Two Key Pairs

Need key backup and non-repudiation therefore need different key pairs for encryption and signing(authentication)



Encryption key backup and recovery

- Need to retrieve encrypted data when decryption key corrupted
- Users may lose, break, or corrupt the encryption devices

Private signing key needs to be generated and under the control of the user at all times

- Need password or smartcard protection
- If signing key is lost, corrupted, or broken a new key is generated

Different algorithms can be used for signing and encryption

Updating key pairs

- Same as forcing users to change passwords at regular intervals

VPN - Need Certificate Policy Statement

Standards and applicability

Identification and authentication

Key management

Local security policies

Technical security practices

Operational practices

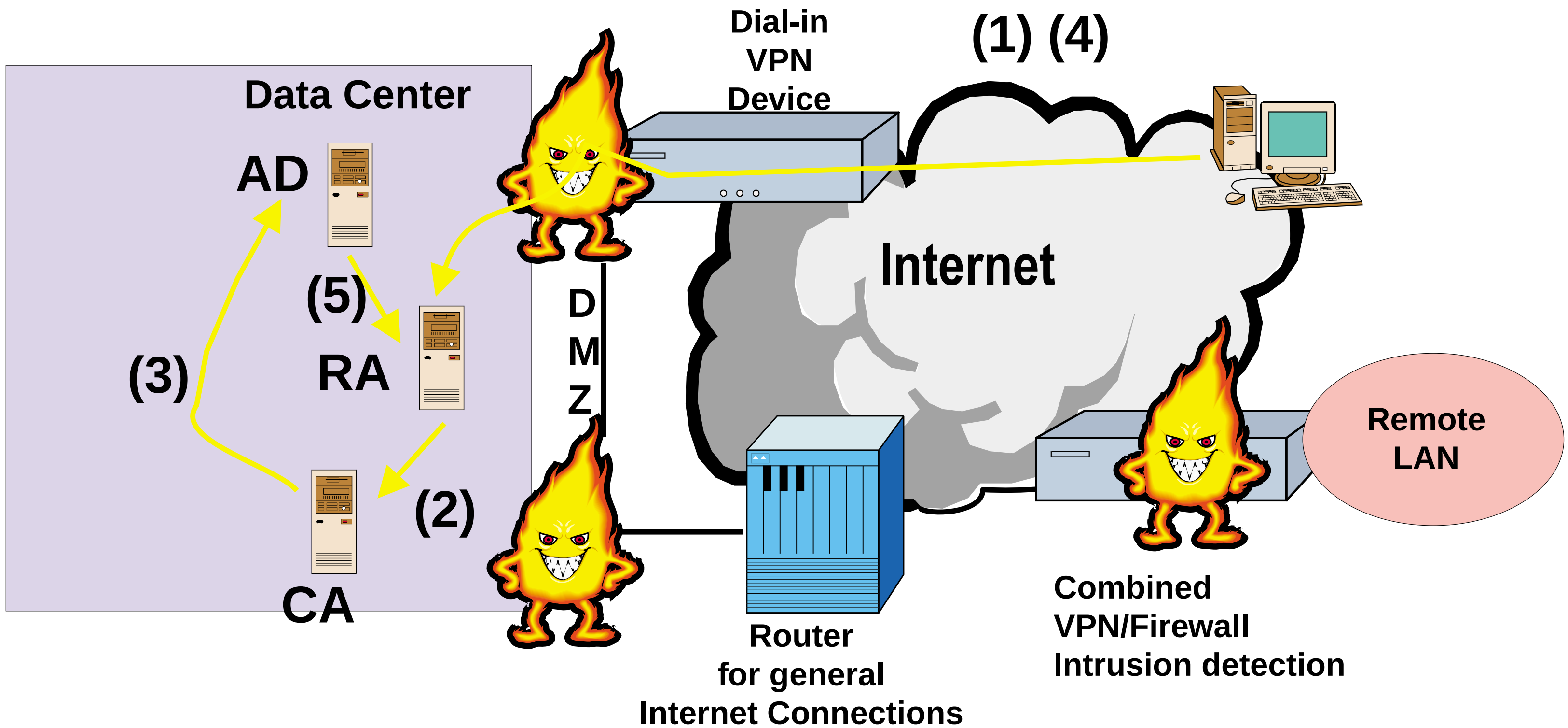
Legal provisions

Cross certification agreements

Certification and CRL profile

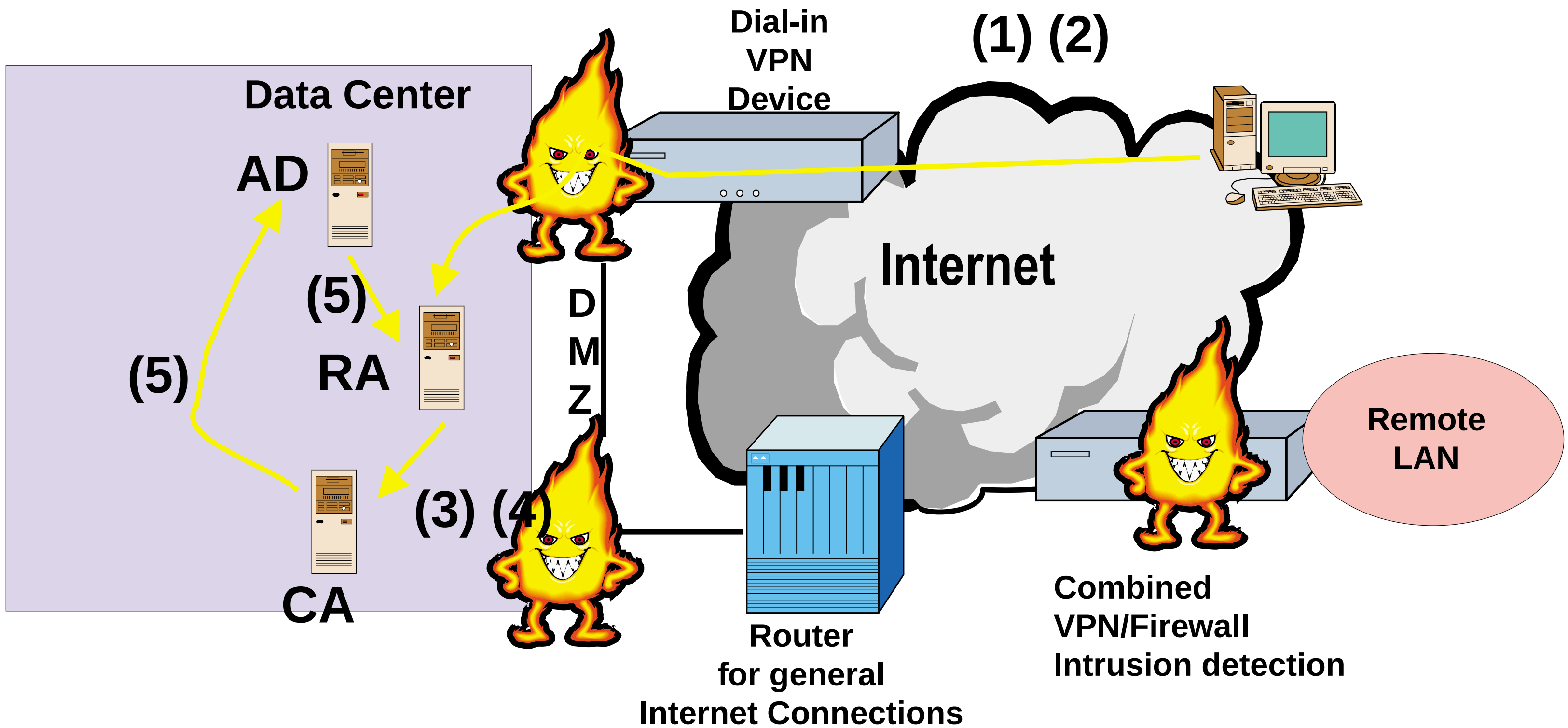
Administration of policy

VPN - Central Registration



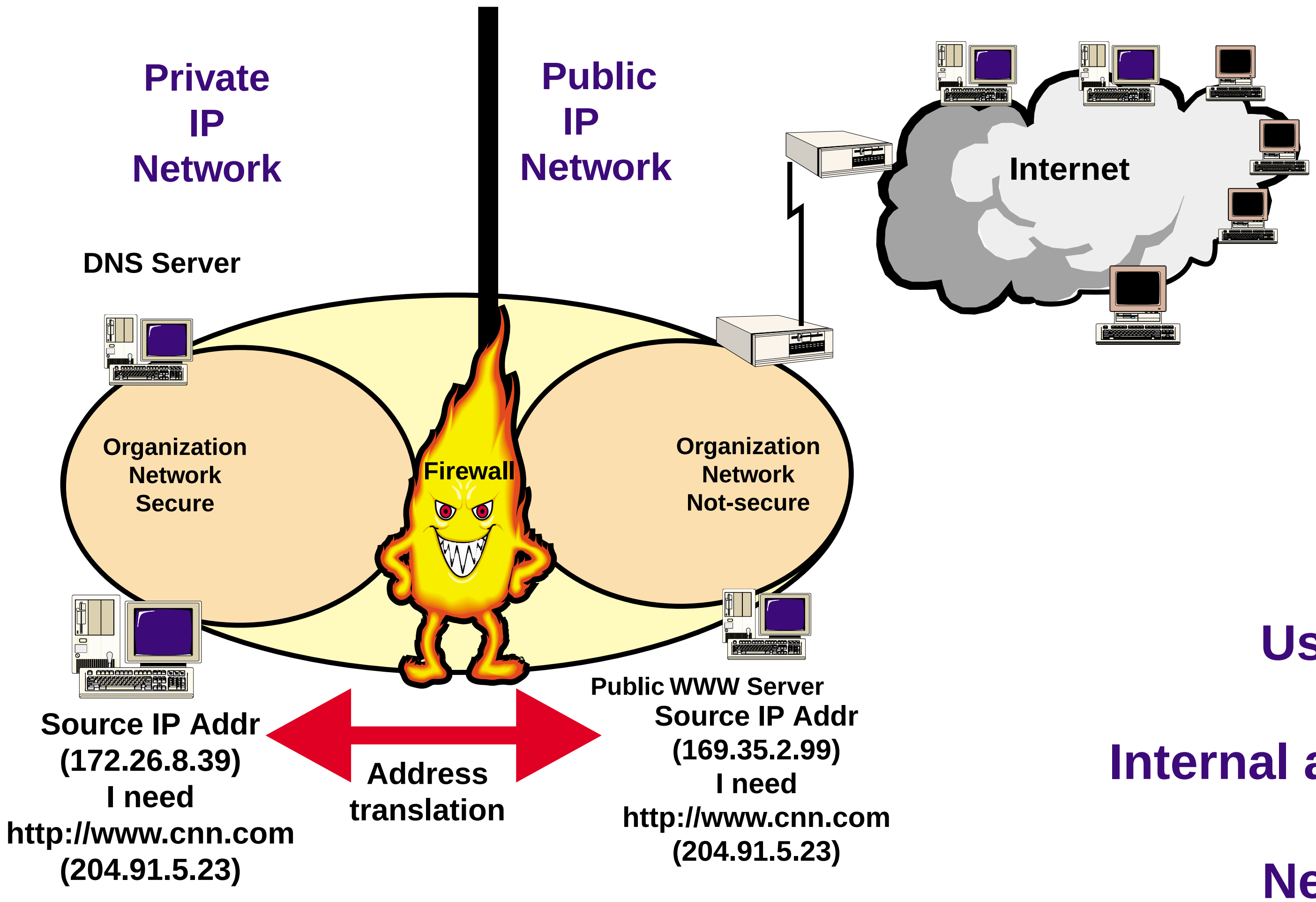
(1) User asks for web access to internal site
(2) Registration authority (RA) accepts and asks Certificate Authority (CA) for verification
(3) CA is processed and stored pending approval
(4) User asks for web enrollment status
(5) Approved certificate is stored in Active Directory (AD) and sent to registration authority
(6) Certificate is retrieved and installed by user

VPN - Distributed Registration



(1) User login upon request from RA
(2) Authenticated user conducts web enrollment request
(3) Certificate request is sent to CA
(4) Certificate is processed and stored in certificate database
(5) Certificate is sent to AD and stored in AD then sent to RA for issue
(6) Certificate is issued to and installed at user

VPN - Network Issues



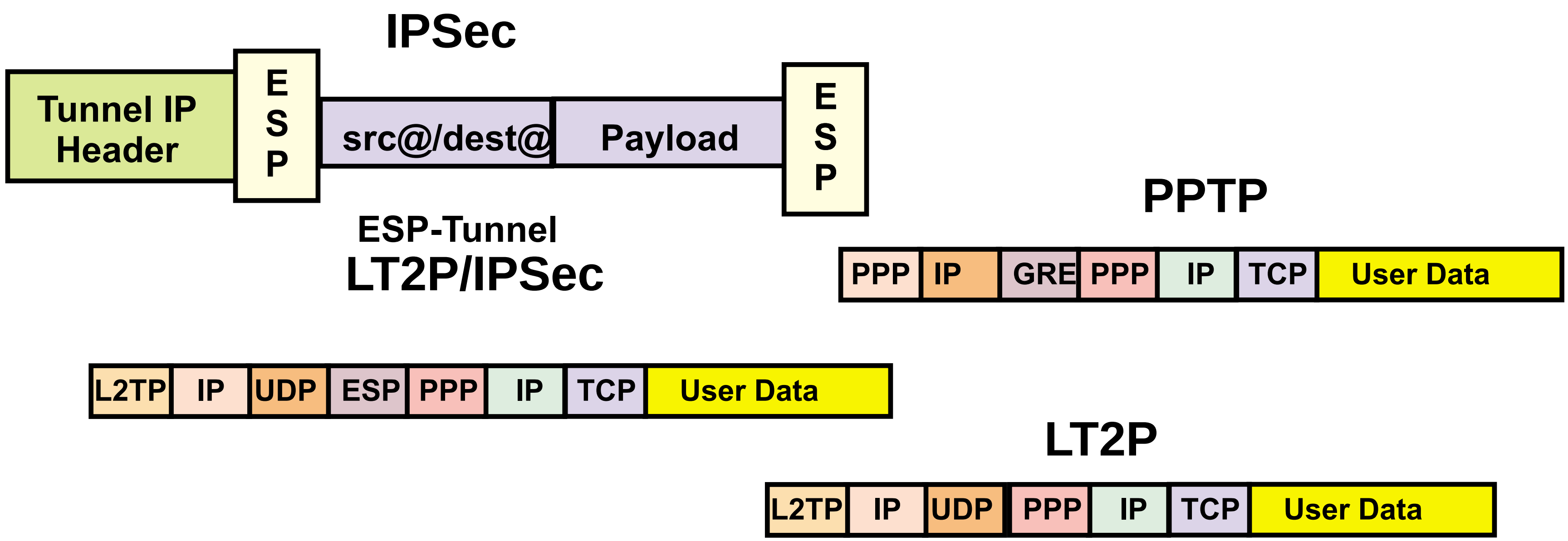
Use of NAT servers

Internal and external DNS

Newer applications

ISPs that change IP address in flight

VPN - NAT Addressing and VPNs



Can NAT work with all VPN protocols?
Need to access IP and TCP checksums, so these cannot be encrypted

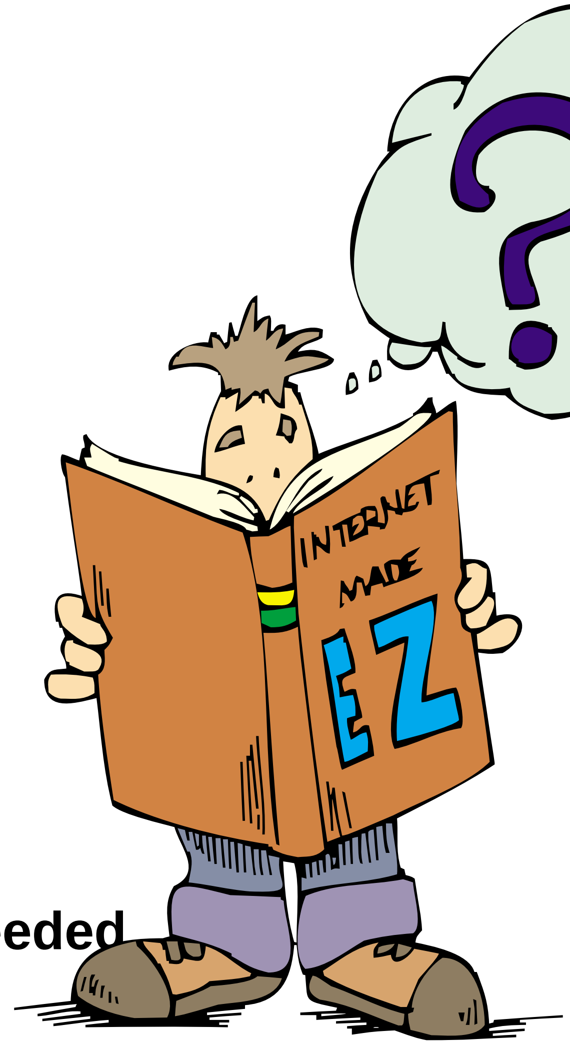
You loose end-end traceability

VPNs make NAT very complex and therefore a vulnerable part of your network

New solutions coming out of IETF to solve several of these issues
Will your supplier support these.........and how fast!

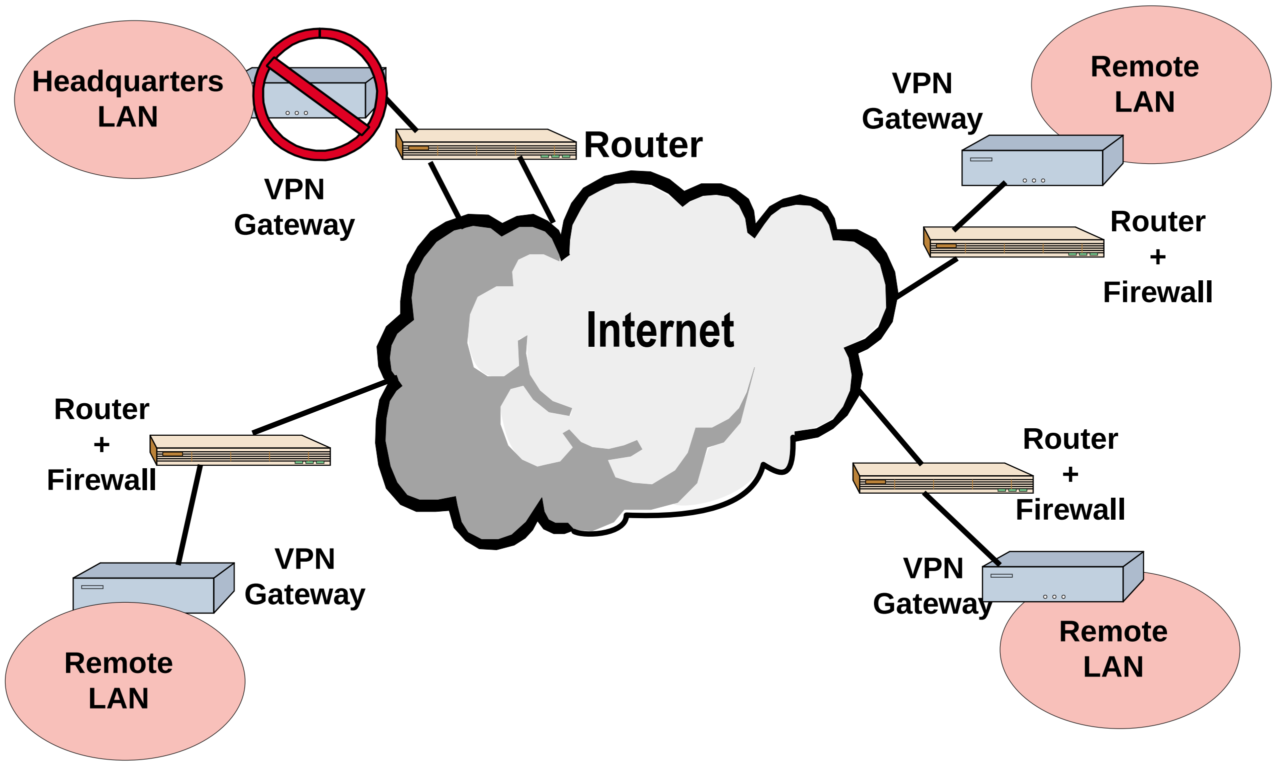
VPN - 10 Steps to Implementation

1. Gather requirements
   - Ports
   - Classes of users
   - Locations
   - Servers
2. Get upper level management involved
3. Determine technology and products
4. Install a test bed
5. Size the systems
6. Design security and VPN placement
7. Determine update strategy
8. Install and configure
9. Monitor and manage and change as needed



10. Get promoted, so you don't have to manage it!

VPN - Failure Detection

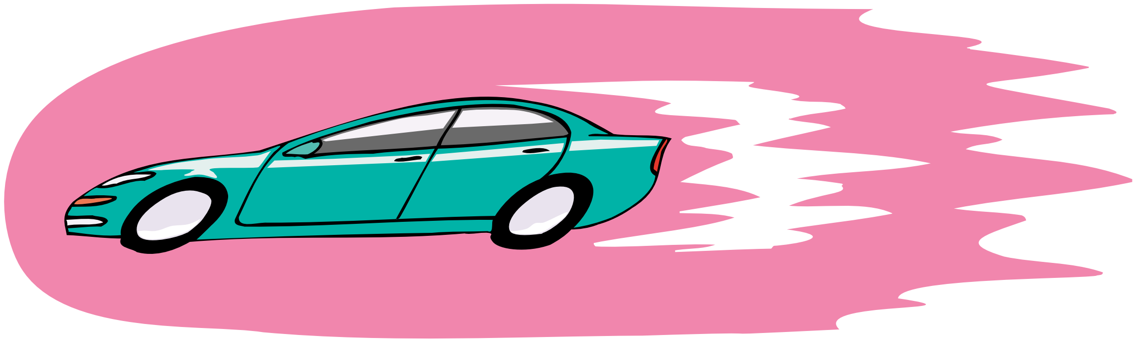


Need standard mechanism for VPN boxes to let each other know they are still active

If VPN gateway server fails, the other servers with established connections continue to send data

A server only finds out the HQ VPN gateway tunnel server has failed when it tries to switch encryption keys

VPN - Performance Issues



Problem	Issue	Solution
Client performance	Encryption and tunneling may overwhelm PC CPU	Pentium PC
High speed client	Encryption, tunneling, and high speed may overwhelm PC CPU	Hardware assisted encryption or next generation client
Packet fragmentation	May create up to 20-30 percent more packets due to multiple encapsulations	Compress data streams before encryption or use lower MTU
Session establishment	Simultaneous session establishment may bog down central site VPN, for example at the start of the day	Over-plan your central site VPN device
Aggregation	As remote users move to high speed access (cable modems/ADSL) your central device will have to encrypt and decrypt data faster	Over-plan your central site VPN device

VPN Availability Issues

Redundant power supplies, backplanes, and cooling fans

Automatic activation of backup link

Connection to multiple provider networks

Hot swapping of failed components

Most support SNMP alerts and alarms

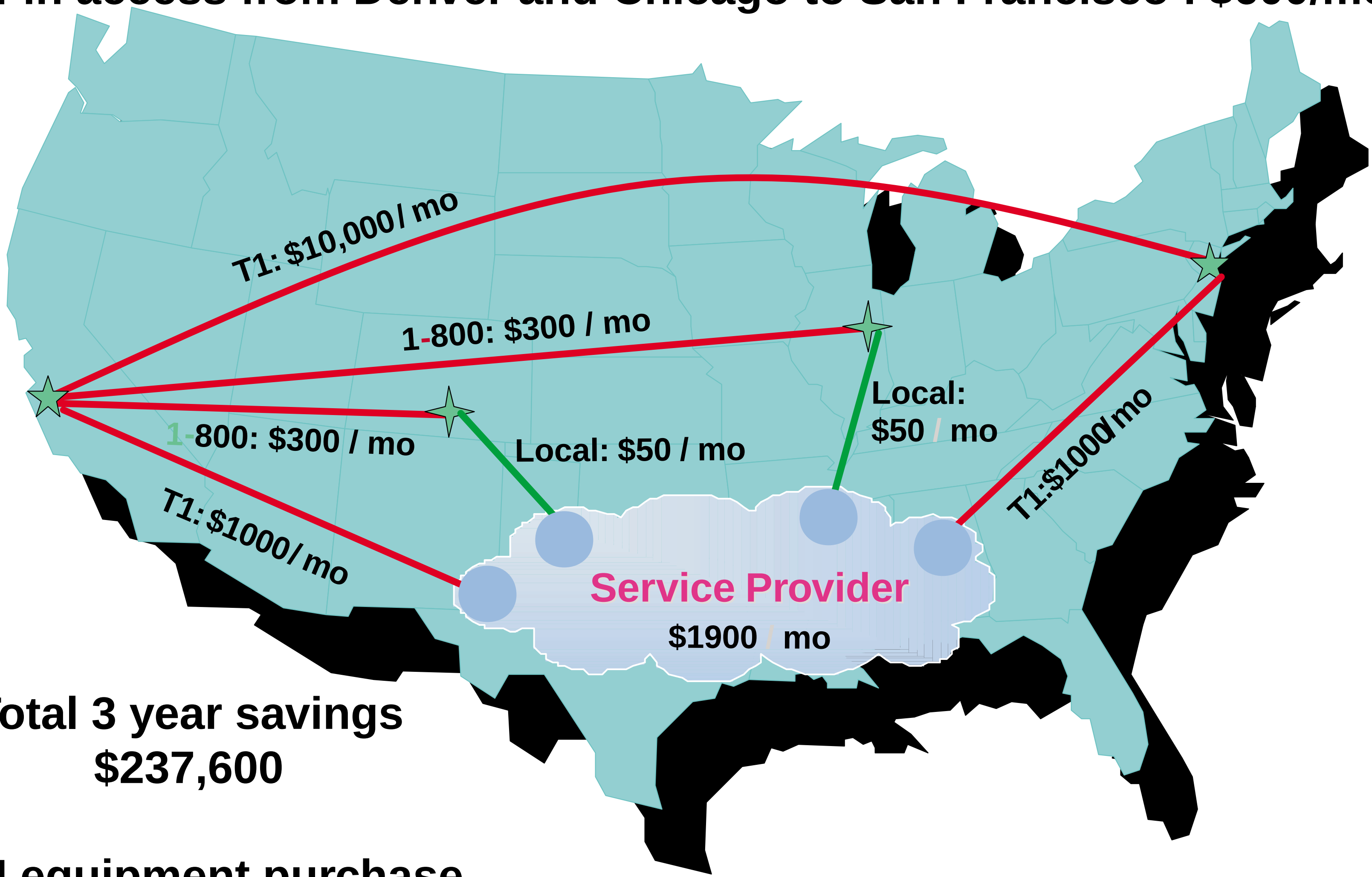
Slowly implementing threshold for key components

MTTR (mean time to repair) usually several hours to a day

Automatic performance monitoring and traffic rerouting

VPN Cost Savings

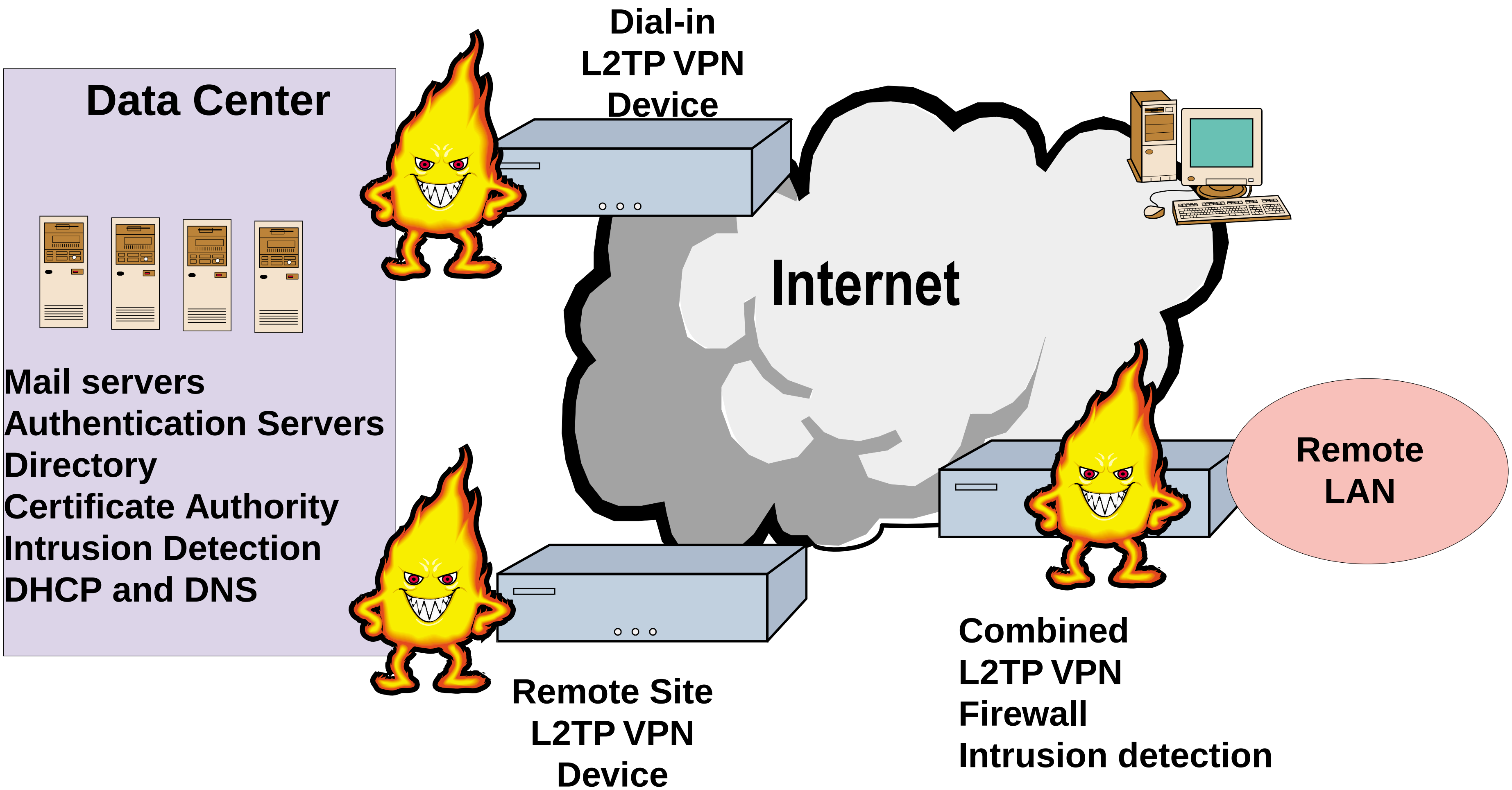
T1 connections between San Francisco and New York City : $10,000/mo
Dial-in access from Denver and Chicago to San Francisco : $600/mo



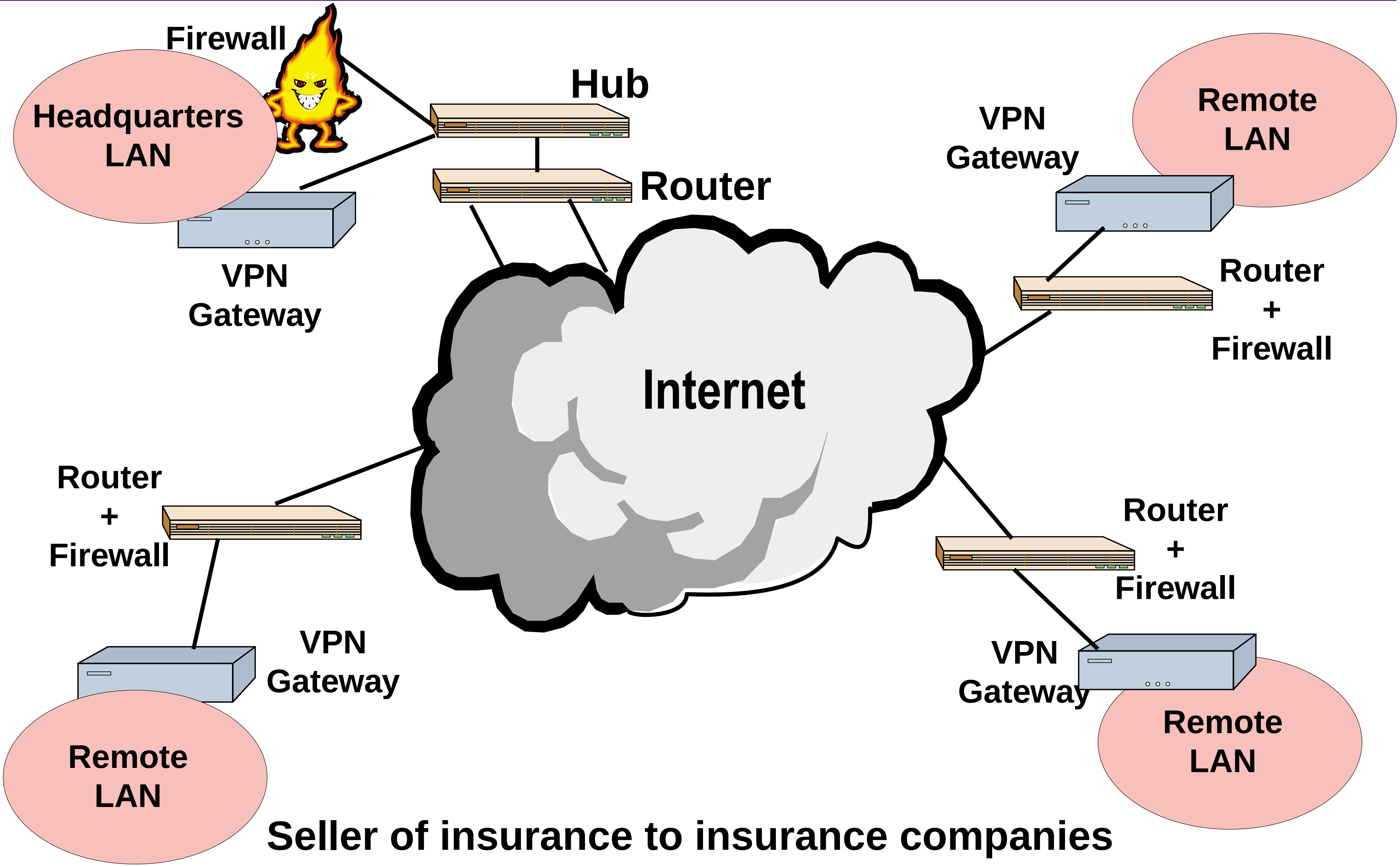
Total 3 year savings
$237,600

VPN equipment purchase
$7,800

Large Worldwide Consulting Firm

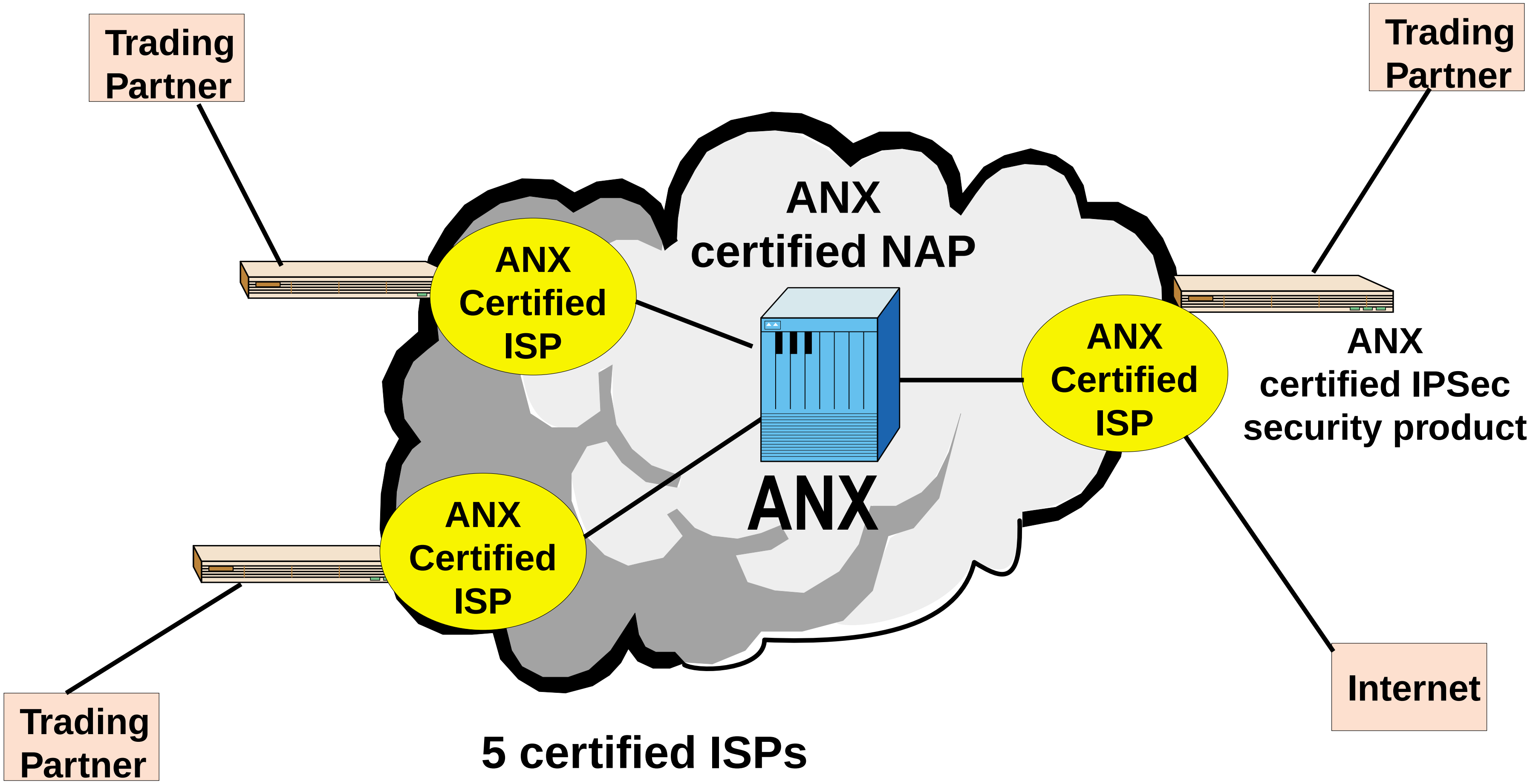


From No-Network to VPN



Seller of insurance to insurance companies
No legacy network allowed them to jump to VPN
VPN gateway has combined encryption and authentication

Automotive Network Exchange



5 certified ISPs
Run ANX traffic over private networks
Seven ANX certified NAPs
Specified performance and technical requirements
Telcordia runs security services

VPN Progress