Virtual Private Networks

Cmput 410 – Presentations

November 25 - 2004

Virtual Private Networking Outline

- Introduction
- Types of VPNs
- Tunneling
- Security
- Encryption
- Future of VPNs

Virtual Private Networking

Introduction

VPN - Definition

- a way to provide remote access to an organization's network
- utilizes a public telecommunication infrastructure (e.g. Internet)
- Various forms of security mechanisms to maintain privacy

VPNs - Why ?

- Organizations need accurate and secure information
- Not all operations are done in the same office, or even country
- Need an affordable option

VPNs - History

- Originally, organizations with such a need used leased lines (some still do)
- Very Secure
- Very Expensive
  - Overhead to install
  - Maintenance
  - Increase with distance

VPNs - History

- VPNs offer low cost option
  - Use existing infrastructure (internet)
  - No or little $ increase with distance
  - Minimum overhead and maintenance expenses
- How about Security ?

VPNs - History

Public precaution

- Information sent through various public hubs.
- Data can easily be extracted
- Thus the use of various encryption and tunneling techniques to maintain privacy

VPNs – Basic Concepts

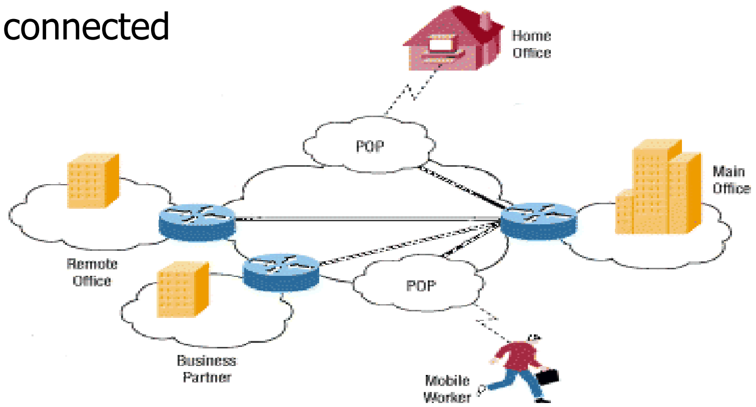
Therefore, the basic idea of VPNs involve

- the secure packaging of packets
- transmission through virtual tunnels
- the emulation of locally being connected

= affordable and secure option to leased line

VPNs – What it does

Allows clients, customers, organizations... to stay connected



VPNs – Common functionalities

- support for remote access to an intranet
- support for connections between multiple intranets within the same organization
- Support for the joining of networks between two organizations, forming an extranet.

VPNs – Done the right way

A well designed VPN should contain

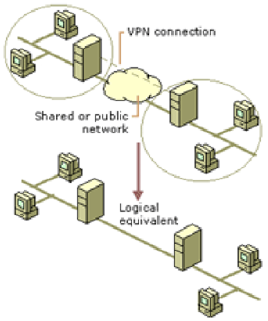
- Security
- Reliability
- Scalability
- Network Management
- Policy Management

Virtual Private Networking

Types of VPNs

Types of VPNs

- Site to Site VPN
  - Intranet Based VPN
  - Extranet Based VPN
- Remote Access VPN



Site to Site VPN

- Intranet: Connects two office LANs securely and transparently across the internet.

- Extranet: Connects two different companies’ office LANs to allow secure sharing of data across the internet.

Site to Site VPN

- One to one connections
- Encrypted IP tunnel

- Advantages
- Disadvantages

Remote Access VPN

- Virtual Private Dial-Up Network
- Connects a remote user to an office LAN securely across the internet
- Advantages
- Disadvantages

Virtual Private Networking

Tunneling

What is Tunneling?

- Mechanism for the transportation of network specific packets over foreign networks

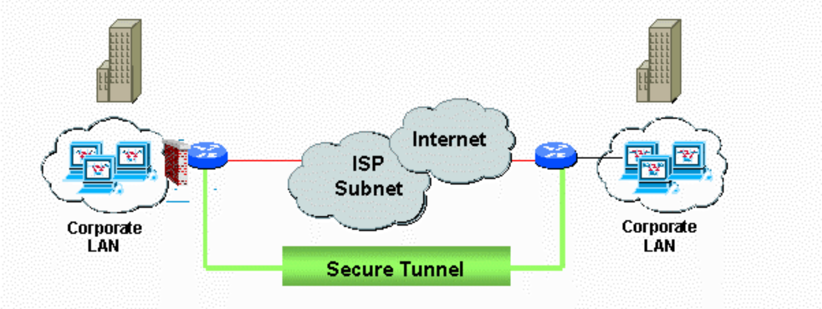
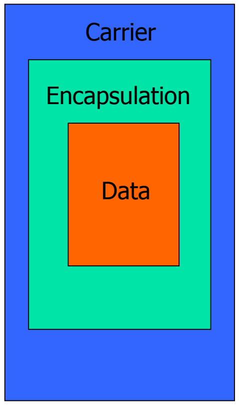


Figure 1: Site-to-Site VPN

VPN Tunneling Protocols

- Carrier
  - The protocol used by the network that the information is traveling over
- Encapsulation
  - The protocol (PPTP, GRE, IPSec, L2F, L2TP) that wraps, thereby encrypting, the original data
- Passenger
  - The original data (IPX, NetBeui, IP) being carried



Carrier

Encapsulation

Data

Example

Data
Carrier
Encapsulation
©2001 How Stuff Works

Tunneling with VPNs

- Site-to-site
  - Commonly uses GRE as an encapsulation protocol
  - Other protocols such as IPSec exist
- Remote-access
  - Predominately uses PPTP (Microsoft)
  - L2F (Cisco)
  - L2TP (PPTP Forum, Cisco, IETF)

Point to Point Tunneling Protocol

- Two types of information flows
  - Control messages
  - Data packets

- Authentication
- Encryption
- Packet filtering

Relies on underlying PPP protocol

Virtual Private Networking

Security

VPN Security

- A well-designed VPN uses several methods for keeping your connection and data secure:

*Firewalls

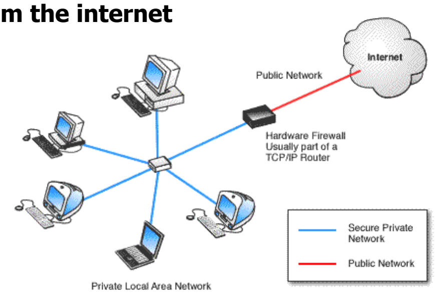
*AAA Server

*IPSec

*Encryption

VPN Security: Firewalls

Protection of private networks from the internet



Control Over

-Which files are allowed to leave private network
-How employees will connect to Web sites
-What ports packets can pass through

VPN Security: AAA Servers

Authentication [Who you are]

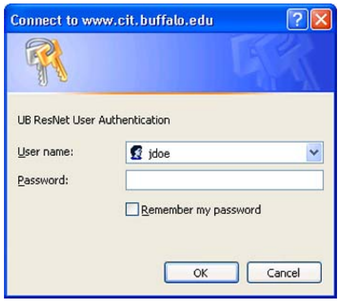
-username/password
-database retrieval

Authorization [What you are allowed to do]

-enforces policies
-different privileges for different users

Accounting [What you actually do]

-logs session information
-allows for statistical analysis
-billing purposes



Connect to www.cit.buffalo.edu

UB ResNet User Authentication

User name: jdoe

Password:

□ Remember my password

Virtual Private Networking

Encryption

VPN Encryption: IPSec

IPSec (Internet Protocol Security) is the protocol commonly used with VPNs. It has 2 modes:

- Tunnel – encrypts both the header and payload of the packet
- Transport – encrypts only the payload

VPN Encryption: Definition

- Encryption: "the process of encoding information in such a way that only the person (or computer) with the key can decode it“ (How Encryption Works http://computer.howstuffworks.com/encryption.htm)
- two methods:
  - symmetric-key encryption
  - public key encryption

VPN Encryption: Symmetric Key Encryption

- Relatively uncommon
- Each computer has the same private key that is used for encryption and decryption
- The problem is how to send the private key without allowing others to potentially "steal" or copy the key while it is being transported over an unsecured network

VPN Encryption: Public-key Encryption

- more commonly used, especially over the internet
- invented in 1976 by Whitfield Diffie and Martin Hellman, (aka Diffie-Hellman encryption
- It's usage is best illustrated by a short story about Alice and Bob (RSA Encryption - Tutorial http://www.woodmann.com/crackz/Tutorials/Rsa.htm)

VPN Encryption: Public-key Encryption - Story

Notes:

- a common public-key cryptosystem is RSA
- A very simple cryptosystem could be reversing the order of each word.
  - eg. Hello there -> olleh ereht

VPN Encryption: Public-key Encryption - Story

1. Alice and Bob agree on a public-key cryptosystem.
2. Bob generates a pair of mathematically linked keys : one public, one private.
3. Bob transmits his public key to Alice over any insecure medium.
4. Bob keeps the private key a secret.
5. Alice uses Bob's public key and the encryption algorithm to encrypt her message, creating a ciphertext.
6. Alice transmits the ciphertext to Bob.
7. Bob decrypts the ciphertext using the same algorithm and his private key.

VPN Encryption: Public-key Encryption

- Keys in public-key cryptography must have a "trapdoor function" which allows computation in one direction to be relatively easy (ie. the encryption), and decryption (without the proper key) to be relatively impossible

VPN Encryption: RSA

- Keys are commonly made using RSA (defined by Rivest, Shamir, and Adleman)
- This algorithm generates keys as follows (RSA Encryption – Tutorial http://www.woodmann.com/crackz/Tutorials/Rsa.htm)

VPN Encryption: RSA

1. Take two large primes, p and q
2. Compute their product n = pq; n is called the modulus
3. Choose a number, e , less than n and relatively prime to (p-1)(q-1), which means e and (p-1)(q-1) have no common factors except 1
4. Find another number d such that (ed - 1) is divisible by (p-1)(q-1). The values e and d are called the public and private exponents, respectively
5. The public key is the pair (n, e); the private key is (n, d)
6. The factors p and q may be kept with the private key, or destroyed.

Notes: p & q are large primes, with ~200 digits each

VPN Encryption: RSA

- not known if RSA is secure
  - know how to prove if an algorithm is inherently "slow‟
- best/fastest way to crack such encryption is using factorization, finding the two large prime numbers used to create the key

VPN Encryption: RSA - Factorization

- Factorization algorithms can take a long time to find the answers
- for example factoring a 512 bit number, as part of a security challenge from RSA labs, took 292 CPU years (about 3.7 months in calendar time) in 1999 (http://www.rsasecurity.com/)
- a 578 bit number was factorized in 2003, which took less time than the 512 bit one because of improved algorithms and faster hardware (http://www.rsasecurity.com/)

Virtual Private Networking

The Future of VPNs

VPN Encryption: The Future

- Factorization techniques are improving as hardware gets faster
- Probable that in the future that current encryption techniques will be solvable (ie. crackable) in a short amount of time, rendering them useless
- It's believed "If no new methods are developed, then 2048-bit RSA keys will always be safe from factorization, but one can't predict the future.‟ (Cryptography FAQ (06/10: Public Key Cryptography http://www.faqs.org/faqs/cryptography-faq/part06/)