Paweł Rajba
pawel@cs.uni.wroc.pl
http://itcourses.eu/

Information Systems Security

IT Infrastructure Security

Agenda

- Introduction
- Facility & Hardware Protection
- Network security
  - Security zones, Special Hosts
  - Access control
  - Firewalls, IDS/IPS, NGFM/UTM, SIEM
  - E-mail
  - Wireless
  - VPN, DNS
- Host & Platform Security, Mobile Security
- Hardening & Resilience

Introduction

> *Information technology infrastructure is defined broadly as a set of information technology (IT) components that are the foundation of an IT service; typically physical components (computer and networking hardware and facilities), but also various software and network components.*

Wikipedia

Introduction

- Facility & hardware protection
- Networking hardware
  - Routers, Switches, LAN cards, Access Points, Cables, etc.
- Software and network components
- Networking software
  - Network operations & management, operating systems, firewall, network security software

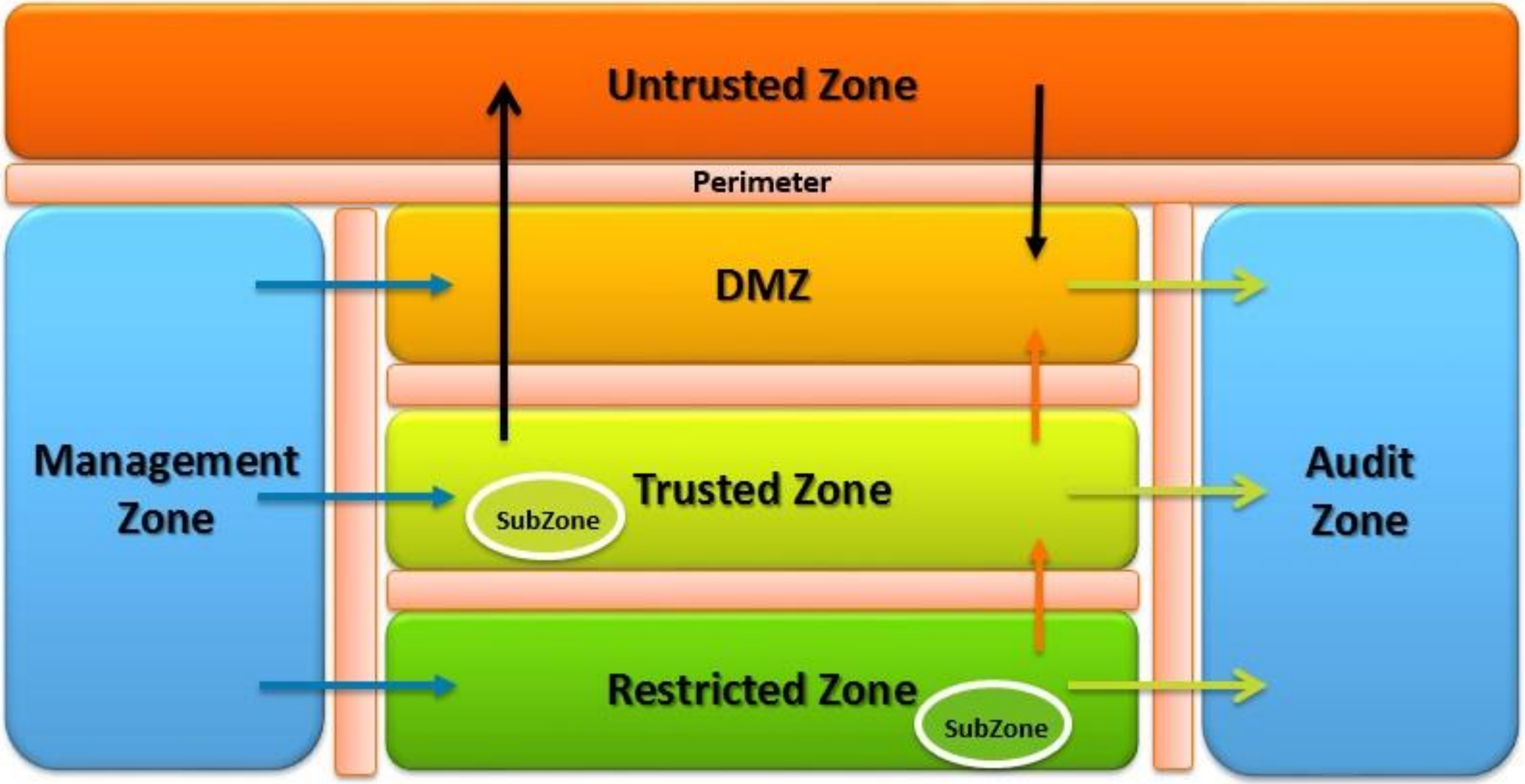
Facility & hardware protection

- Environmental damage (floods, fire, earthquake, power surges, etc.)
- Locking rooms, locking cabinets with infrastructure equipment, locking down computers
- Access control
  - Piggybacking
  - Tailgating
- Decomission and recycle hardware
  - Recycler should be certified, e.g. Basel Action Network
  - Check recycler environment or safety violations
  - Check if recycler sends used equipment or wastes to other business partners (aka downstream partners)
    - Be cautious if their partners are confidential or proprietary

Network security

- In general it is about delivering security requiments (e.g. CIA) on the network level
- It involves many aspects like
  - AAA (RADIUS, TACACS+, Kerberos)
  - Availability
    - Right Internet bandwidth
      - Plan for spikes in usage
      - Plan for growth
    - Backup connection
  - Wireless
  - Configuration consistency (central management)
- Example:
  - No matter in corporate office I will connect to, I have the same set of resources & accesses available

Network Security: Security zones



Network Security: Security zones

- A set of network elements under a common policy
- Usually we can identify security zone
  - Provider, owner, policy
- Common zone types
  - Untrusted, trusted, restricted, DMZ
- Zones can split a network to the following parts:
  - External, Outside, Inside

Network security: Special hosts

- Dual-homed host
  - Host with multiple network interfaces
  - Can offer routing or not
  - If not, can offer shared application for different subnets
- Jump host
  - A hardened host which is an entry point to secured area
- Bastion host
  - Any firewall critical to network infrastructure

Network security: Access Control

- RADIUS: usually central authentication service for network devices
- TACACS+
  - CISCO protocol, central authentication service
  - Support AAA, full encryption
- Authentication
  - One-way, mutual,
  - Kerberos, X.509
  - SSO

Network Security: Firewalls

- Filter traffic, separate networks
- Several firewall categories
  - Packet-filtering
    - It can be also with stateful packet inspection (SPI)
  - Proxy, reverse-proxy
    - Verifies higher levels, e.g. allows only specific users
  - Application gateways
    - E.g. allows only GET command in FTP

Network Security: IDS/IPS

- Intrusion Detection/Prevention System
- Main types
  - Network IDS (NIDS)
    - Deployed as as network component
  - Host IDS (HIDS)
    - Agent on host monitoring system calls, app logs, file system modifications
  - VM Based IDS (VMIDS)
    - Monitor the VM environment

Network Security: NGFW, UTM

- Next-Generation Firewall or
  Unified Threat Management (UTM)
  - Products on the market offering complete solutions
  - Combining Firewall,IPS, IPS, Antivirus, URL filtering and more
  - Reporting on a regular basis

Network security: SIEM

- SIEM = Security Information Event Management
- Expected capabilities
  - Data aggregation
    - Combining data from many sources, including network, security, servers, databases, applications.
  - Correlation
    - Looks for common attributes, and links events together into meaningful bundles.
  - Alerting
    - The automated analysis of correlated events
  - Dashboards
    - Present informational charts to assist in seeing patterns, or identifying activity that is not forming a standard pattern
  - Compliance
    - Automate the gathering of compliance data, producing reports adapted to security, governance and auditing processes
  - Retention
    - Employing long-term storage of historical data to facilitate correlation of data over time, support compliance requirements and forensic investigations
  - Forensic analysis
    - The ability to search across logs on different nodes and time periods based on specific criteria.

(following Wikipedia)

E-mail security

- One more communication channel
- Very often used to send a business information as a part of the process
- Two main perspectives: inbound and outbound
  - Outbound (before leaving the network)
    - Antimalware protection, e.g. inappropriate emails, SPAM
    - Unauthorized content, company-private information
  - Inbound (before entering the network)
    - Malware, phishing, or malicious emails.
- TLS: signatures and encryption
- Additional corporate protection, e.g.
  - Block forwarding the message
  - Allow reading after additional authentication

Wireless security

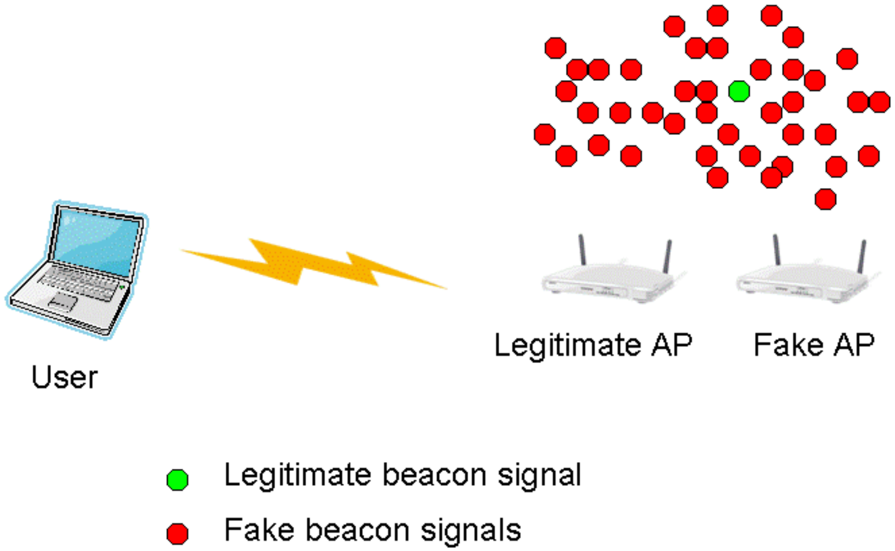
- Communication channel is very accessible
  - Attack Surface much bigger
- Confidentiality & Integrity
  - MITM
- Availability
  - Signal jamming
  - Wrong password policy and all accounts locked
- Privacy: http://www.cherrydata.pl/produkt-indoor-trax
- Authentication
  - Client device authN quite obvious, but what about network authentication?

Wireless security

- Beacon frame
  - A package of the information about the network
  - Beacon frames are transmitted periodically
- Some data items
  - SSID
  - Supported rates
  - Frequency-hopping (FH) Parameter Set
  - Direct-Sequence (DS) Parameter Set
  - Contention-Free (CF) Parameter Set
  - IBSS Parameter Set
  - Traffic indication map (TIM)

Wireless security

- Two quick problems
  - Devices are trying to connect to known networks
    - If not secured, they disclose network passwords
  - Beacon flood attack



https://www.cse.wustl.edu/~jain/cse571-07/ftp/wireless_hacking/index.html

Wireless security

- Protocols
  - WEP. Wired Equivalent Privacy (1999-2004)
    - Problem with IV collisions
    - Poor security and hard to configure
  - WPA. Wi-Fi Protected Access (2003-2012)
    - Versions WPA PSK (with preshared key) and WPA Enterprise (with authentication sever for keys and certificates generation), TKIP for encryption
    - Quick fix for WEP
    - Poor security, configurable medium
  - WPA2. Wi-Fi Protected Access version 2 (2004-)
    - Introducting AES as an encryption method
    - Part of 802.11i wireless security standard
    - Good security, configurable good
  - WPA3. Wi-Fi Protected Access version 3
    - Under development
    - Excelent security & configurability

https://www.netspotapp.com/wifi-encryption-and-security.html

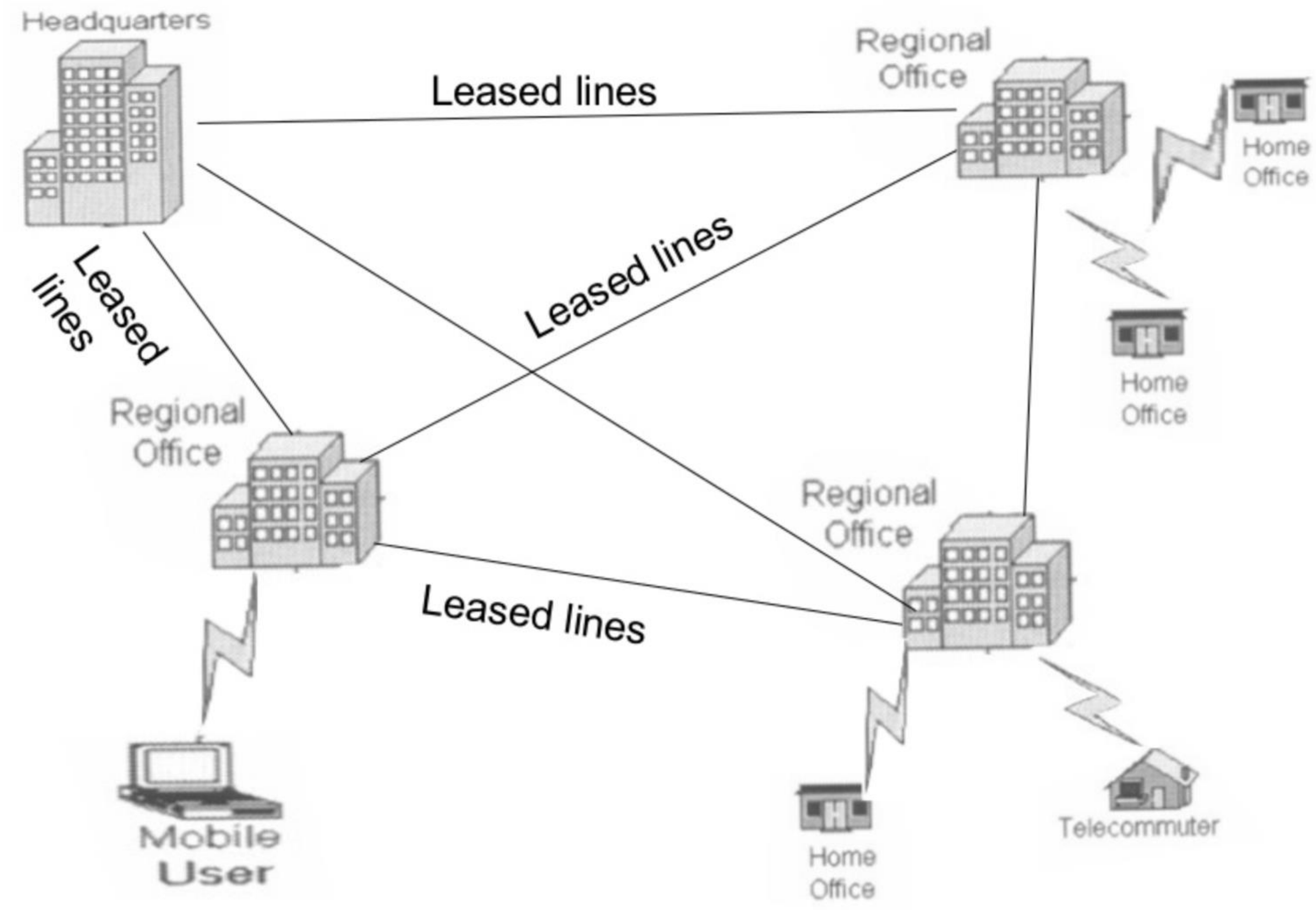
Virtual Private Networks

- At beginning there was a concept of private network
  - Distributed across different locations
  - Completely isolated
  - Created an impression of an own part of the Internet
  - Quite costly
- VPN gives the possibility to achieve the same: create a network that virtually private, but phisycally public

Virtual Private Networks

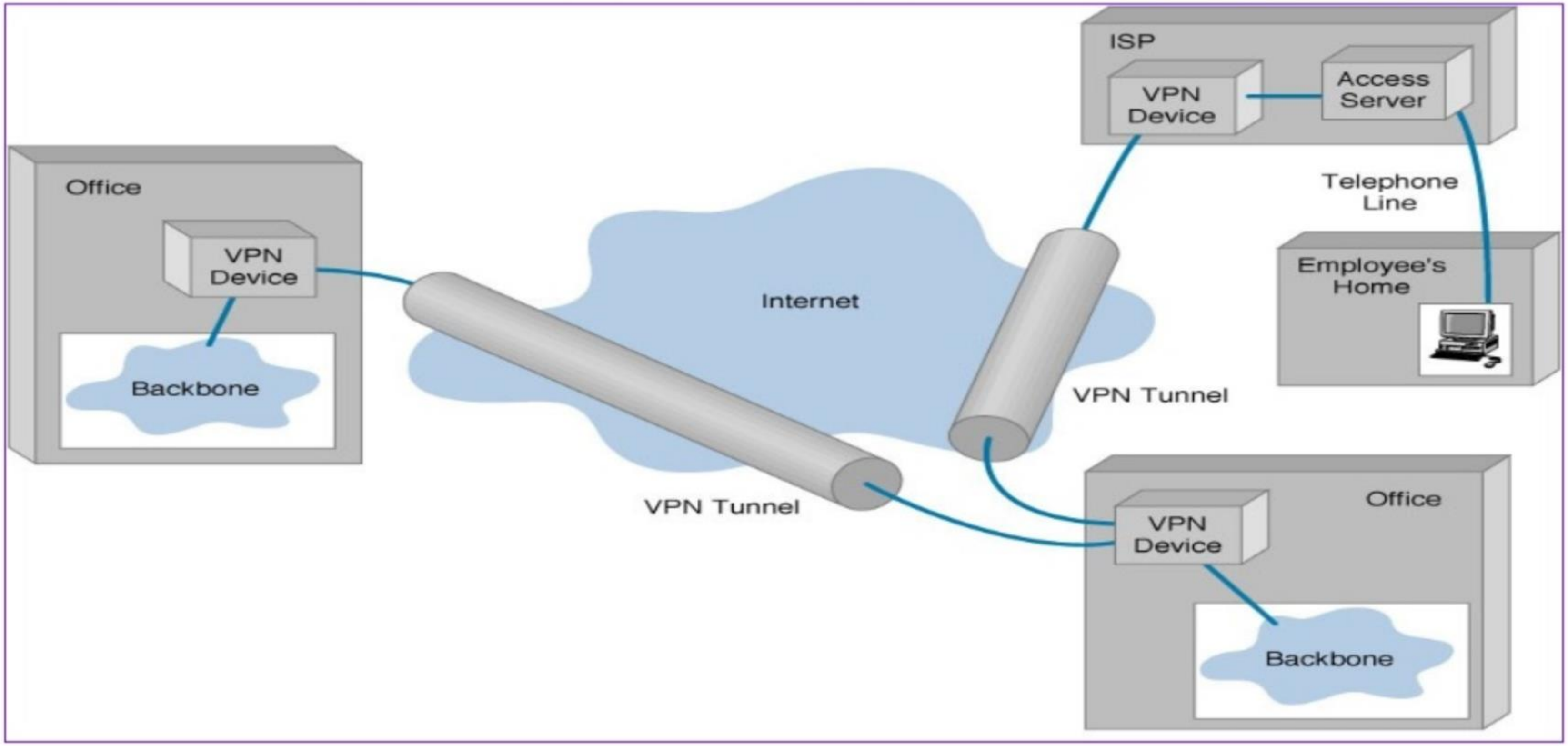
- Materials
  - https://www.slideshare.net/rajurmr22/virtual-private-network-43030792
  - https://www.slideshare.net/Kajal_Thakkar/vpn-14074779
  - https://www.slideshare.net/Shiraz316/vpn-69977677
  - https://www.cactusvpn.com/beginners-guide-to-vpn/
  - https://www.lifewire.com/vpn-tunneling-explained-818174
  - https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_73/rzaja/rzajagetstart.htm

VPN: traditional approach



https://www.slideshare.net/Kajal_Thakkar/vpn-14074779

VPN: virtual approach



https://www.slideshare.net/Kajal_Thakkar/vpn-14074779

VPN: main elements

- Tunelling & Encapsulation
  - We will focus primarily on that one
- Confidentiality (Encryption) & Data Integrity
- Authentication & Access Control
- Firewall

VPN: tunelling

- Idea
  - Placing packet inside another packet before transporting over the Internet
  - Outer packet protects the content from the public view and ensures packet is flowing withing a tunel
- Steps
  - Packets constructed in a specific VPN protocol format
  - Encapsulated within some other base or carrier protocol
  - Transmitted between VPN client and server
  - De-encapsulated on the receiving side

VPN: tunelling

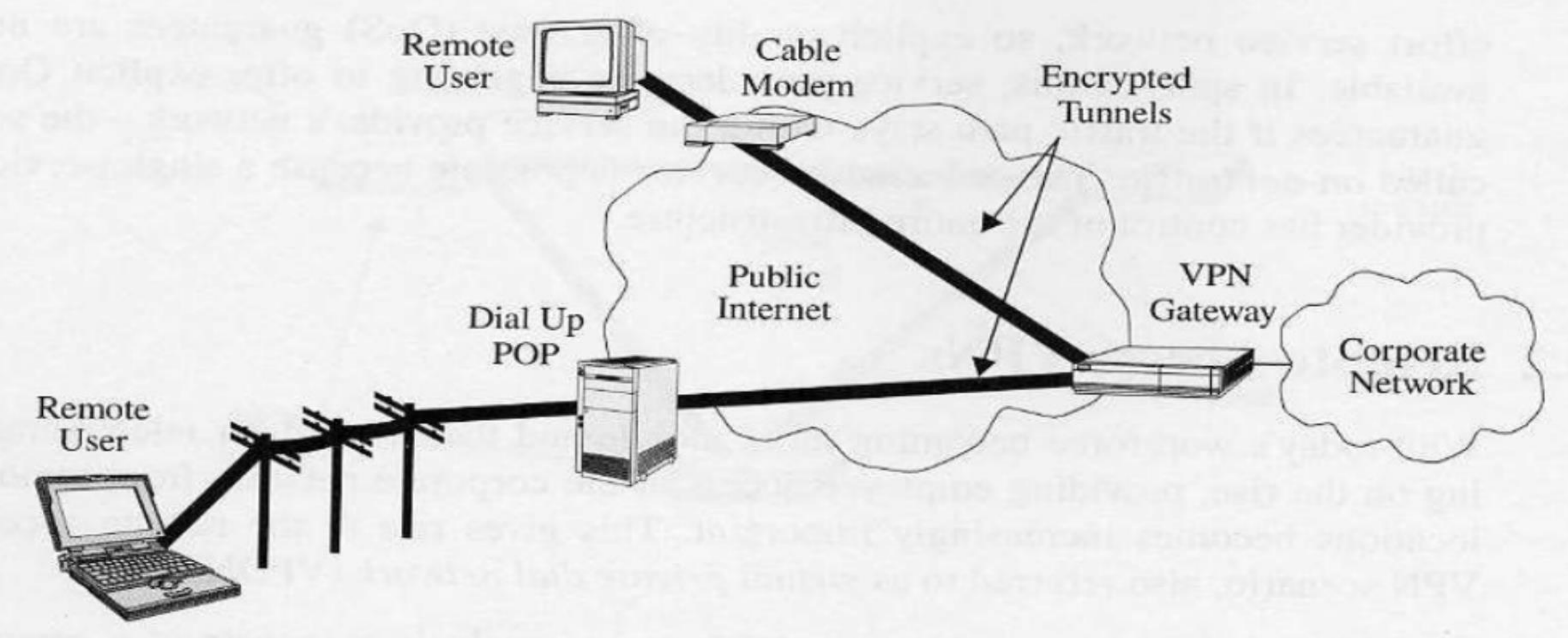
- Types of tunneling
  - Voluntary
    - The connection is created by the remote user
    - Then the client manages the connection
  - Compulsory
    - Remote host initiates a connection to its ISP
    - The ISP then establishes an L2TP connection between the remote user and the corporate network
    - This typs hides the details of VPN server from VPN client
      - As it stops at ISP
- Main difference: the endpoint
  - Voluntary tunel → the tunnel ends at the remote client
  - Compulsory tunnel → the tunnel ends at the ISP

VPN: tunelling

- Tunneling protocols
  - Point-to-point Tunneling Protocol (PPTP)
  - Layer 2 Tunneling Protocol (L2TP)
  - Internet Protocol Security (IPSec)

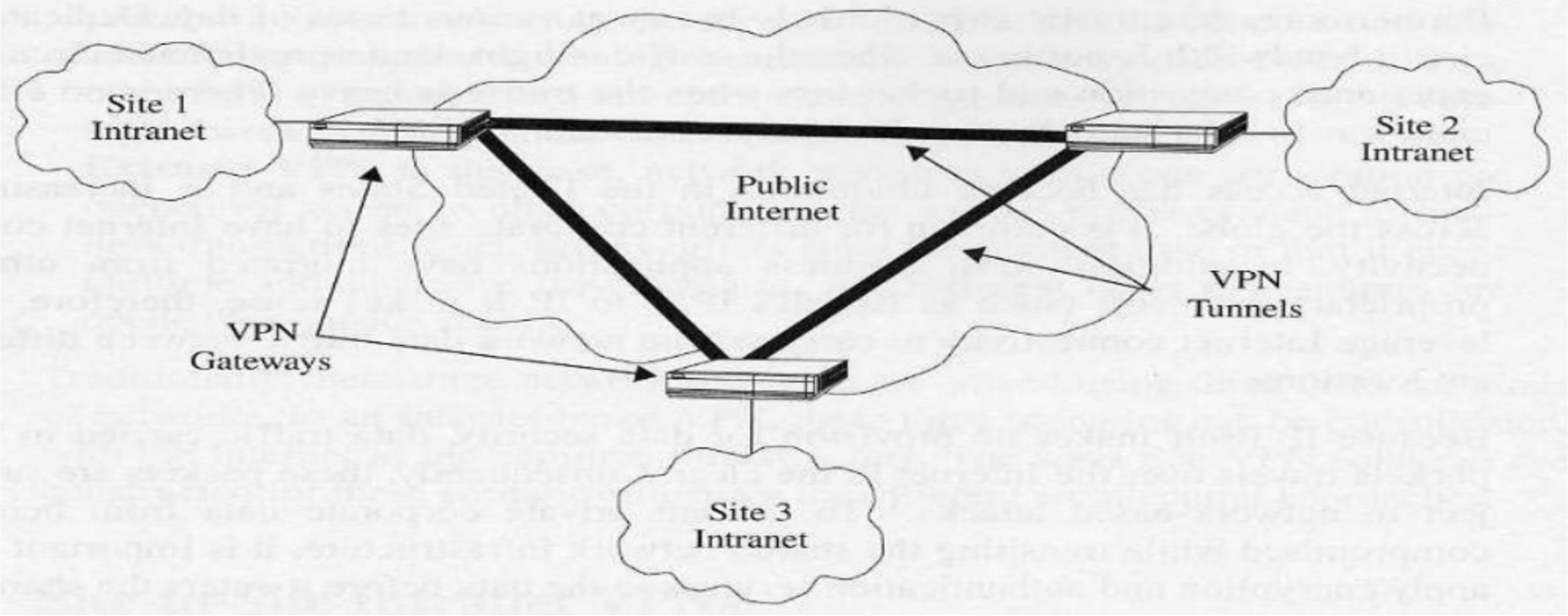
VPN: types

- Remote access VPN



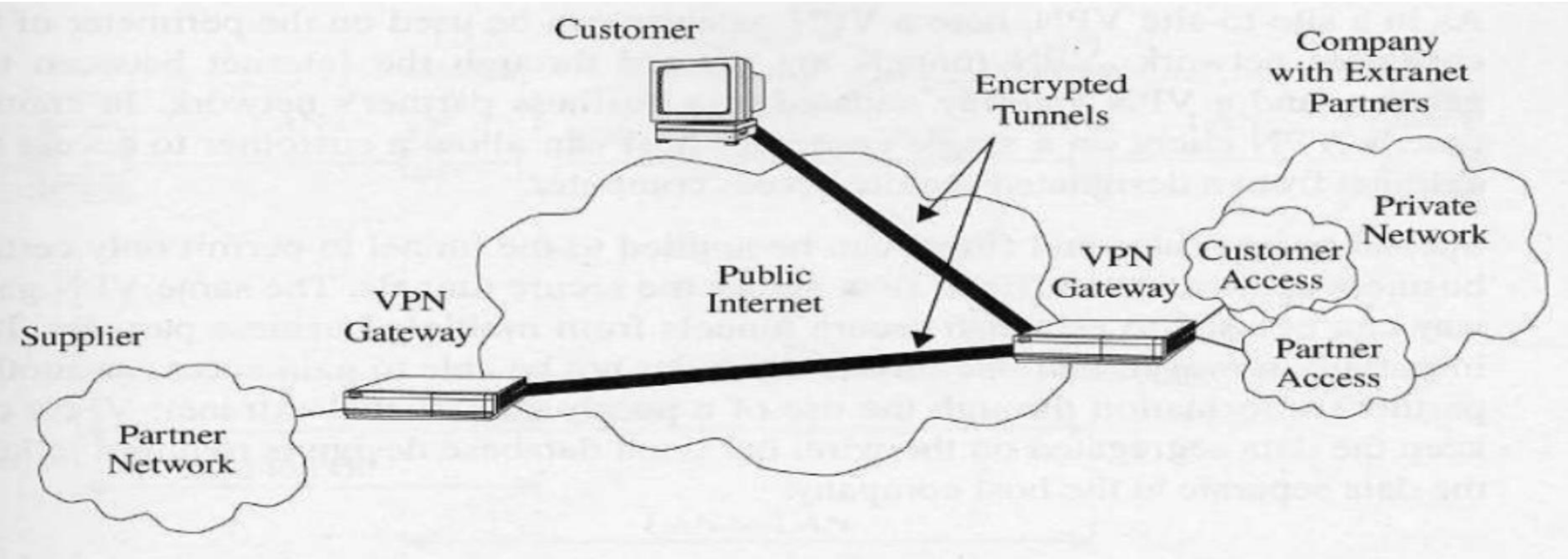
VPN: types

- Intranet VPNs



VPN: types

- Extranet VPNs



DNS Security

- Right configuration
- Protection
  - on host level (file hosts)
  - on the local domains configuration
  - configurations in DNS providers
- Additional protection
  - DNS Sec (signing DNS records)
  - DNS Crypt (signing DNS responses)
  - DNS over HTTPS
- Other threats
  - Cache poisoning (wrong answer cached for long time)
  - DNS Flood (no Internet without DNS)
  - Privacy issues (all requests going through one DNS provider)

Domain approach

- Centralisation of different aspects
  - Directories (accounts, certificates, etc.)
  - Policies
  - Permissions
  - Configurations
  - Management
    - Accounts lifecycle
    - Pushing policies
    - …

Host & platform security

- Managed vs. unmanaged devices
- Applicable from smartphone to superextraserver
- Combination of hardware and OS
- Some good practices for production platforms:
  - Production env. must be separated from dev and test
  - Regular scans for changes in executables
  - Strict maintenance procedures
    - Both for hardware and software
  - Non-production software should be removed (e.g. text editors, compilers, etc.)
    - If needed they can be installed temporarily
  - Software and OS upgrades procedures should be very strict (patch management)
  - Access control designed with care and based on requirements
  - Admin accounts mustn’t be used for routine operations
  - Endpoint protection including antimalware protection

Host & platform security: good practices

- Backup often
- Permissions on
  - file and folder level
  - shared folders level
- Documents password protected
- EFS encryption
- Encryption of removable devices (USB sticks)
- Use PKI
- Use IPSec
- Secure wireless communication
- Use Windows Rights Management Services (RMS)

Mobile devices

- List allowed software
- Strategy for software updates
- Restricted access to a device (e.g. PIN)
- Antimalware solutions
- Review connectivity methods, especially automated wifi connectivity
  - Passwords may be exposed as well as man-in-the-middle attacks can be executed
- Enable remote data wipe option if available.
- Regularly back up the mobile device
- Consider solutions like MobileIron or Microsoft Intune

Hardening

- Reducing its surface of vulnerability
- Can be applied to any component of the IT infrastruture
  - But can be also adding a new component (e.g. IDS)
- Some examples
  - Closing selected opened ports
  - Strict access control policy
  - Applying hardening scripts changing options in OS
- Why system is not hardened by default?

Resilience

- Avoid single point of failure
  - Double everything
- Automated recovery and configuration
  - Remember about regular tests
- Comprehensive loggin and monitoring
  - To detect coming failure before it occurs
- Performance and capacity planning
  - Very connected to resilience