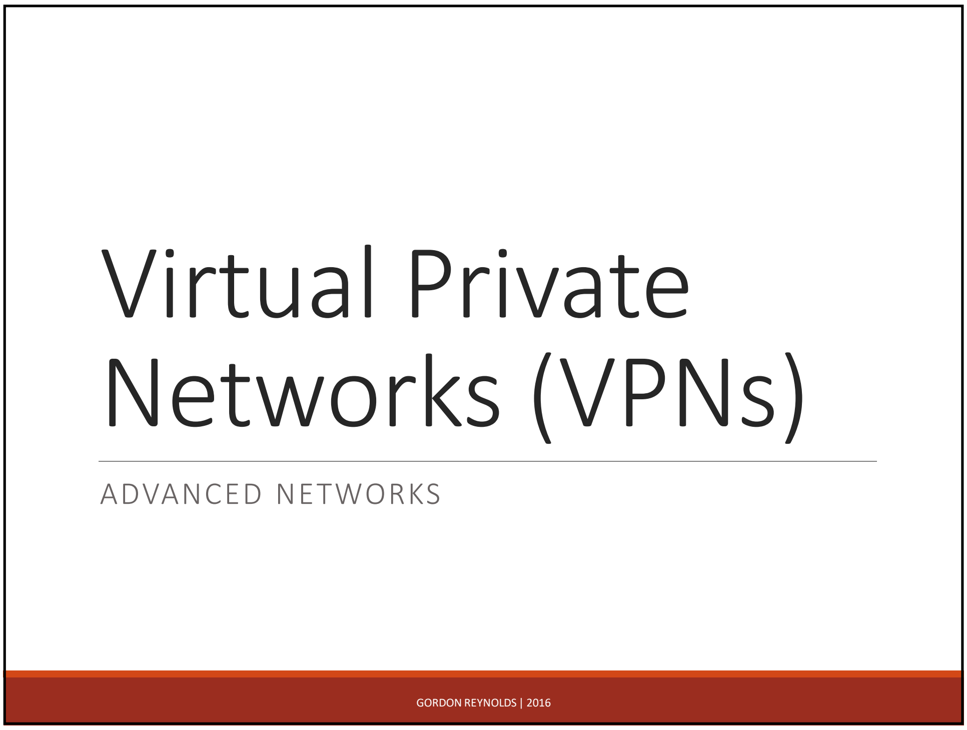
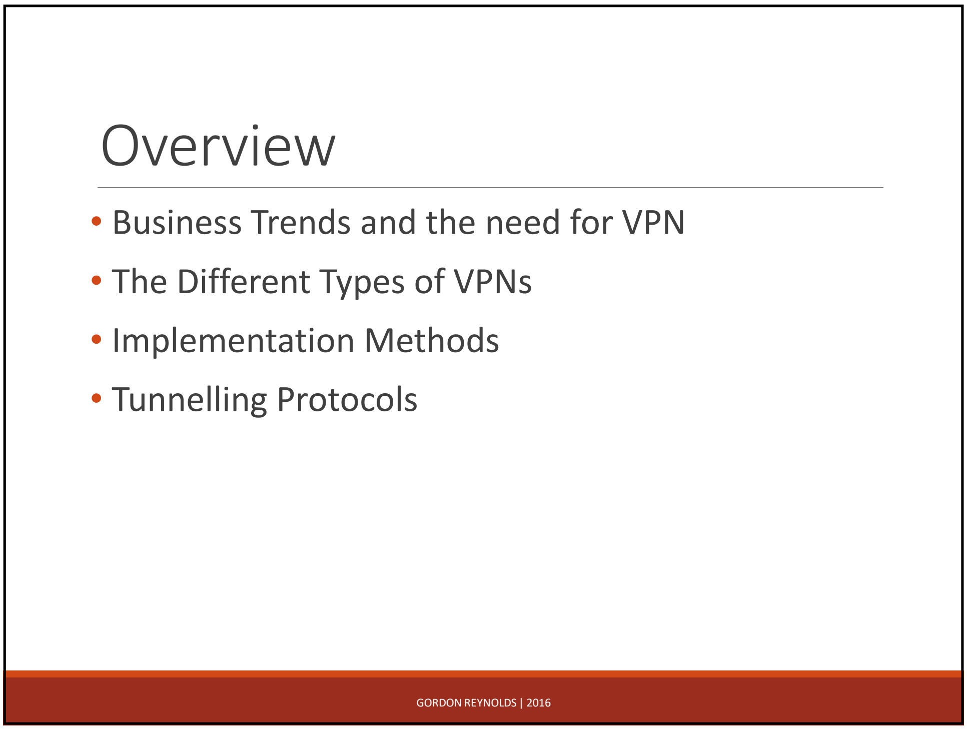


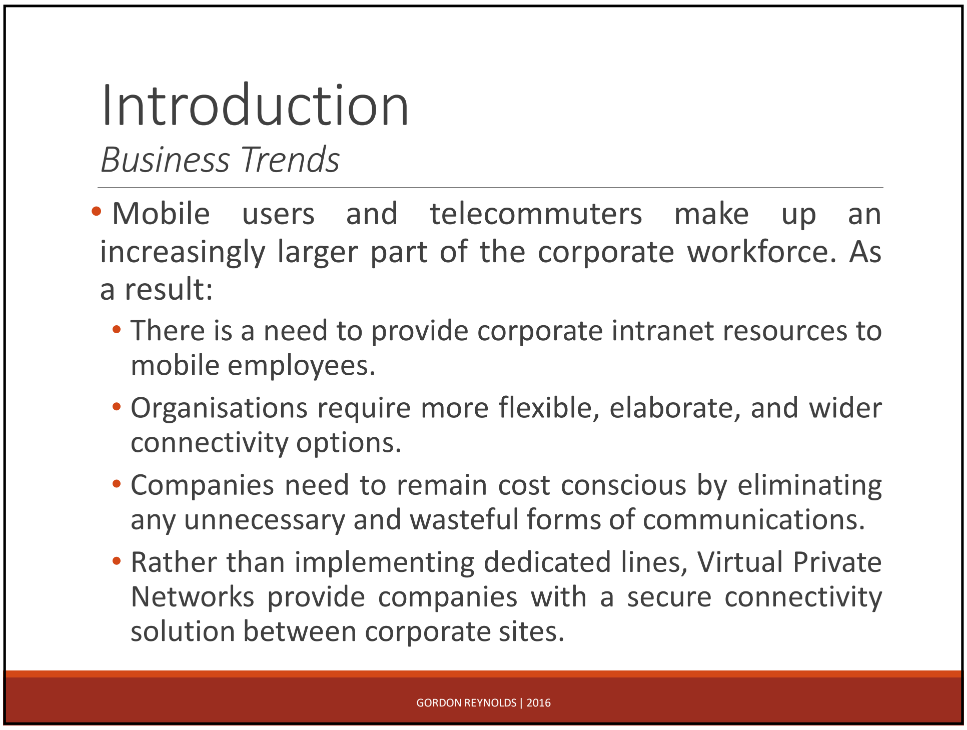
Virtual Private Networks (VPNs)

ADVANCED NETWORKS



Overview

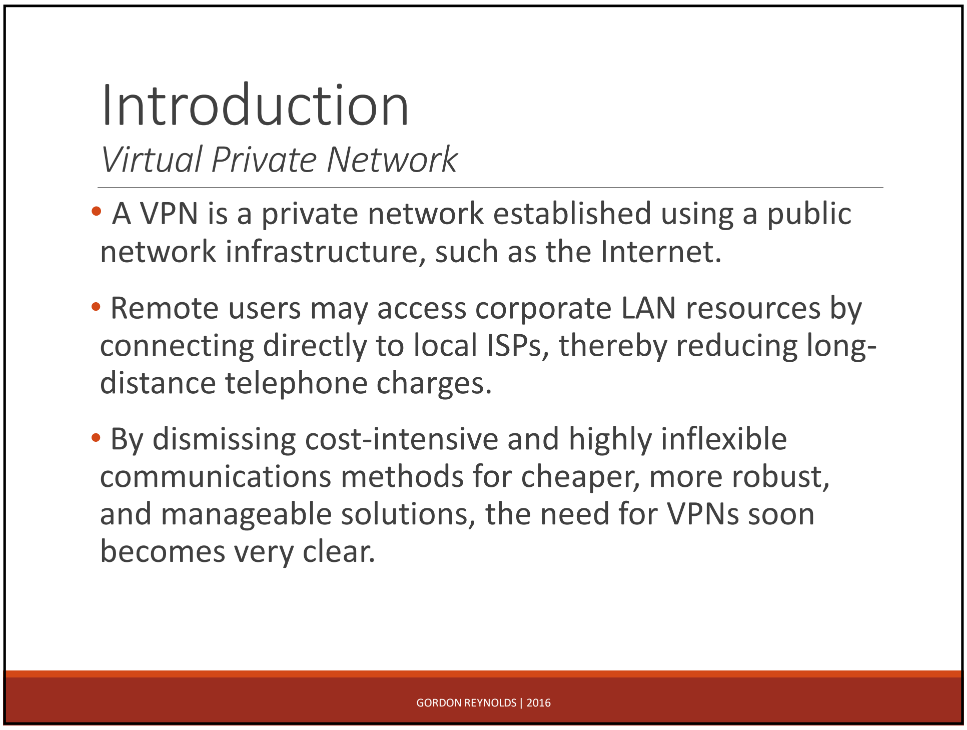
- Business Trends and the need for VPN
- The Different Types of VPNs
- Implementation Methods
- Tunnelling Protocols



Introduction

Business Trends

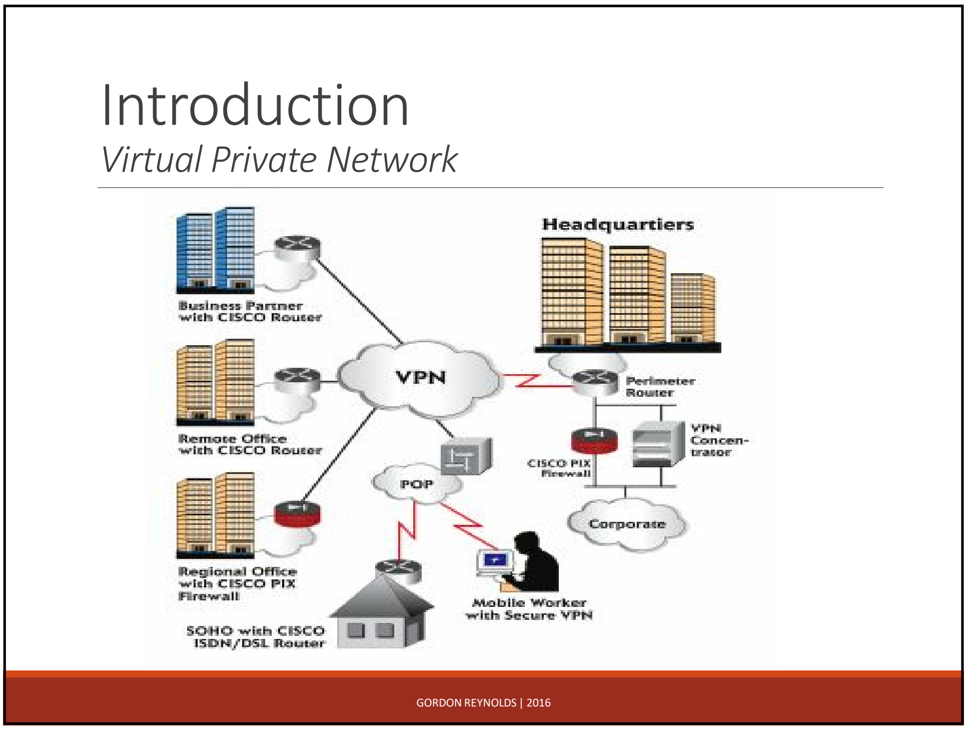
- Mobile users and telecommuters make up an increasingly larger part of the corporate workforce. As a result:
  - There is a need to provide corporate intranet resources to mobile employees.
  - Organisations require more flexible, elaborate, and wider connectivity options.
  - Companies need to remain cost conscious by eliminating any unnecessary and wasteful forms of communications.
  - Rather than implementing dedicated lines, Virtual Private Networks provide companies with a secure connectivity solution between corporate sites.



Introduction

Virtual Private Network

- A VPN is a private network established using a public network infrastructure, such as the Internet.
- Remote users may access corporate LAN resources by connecting directly to local ISPs, thereby reducing long-distance telephone charges.
- By dismissing cost-intensive and highly inflexible communications methods for cheaper, more robust, and manageable solutions, the need for VPNs soon becomes very clear.

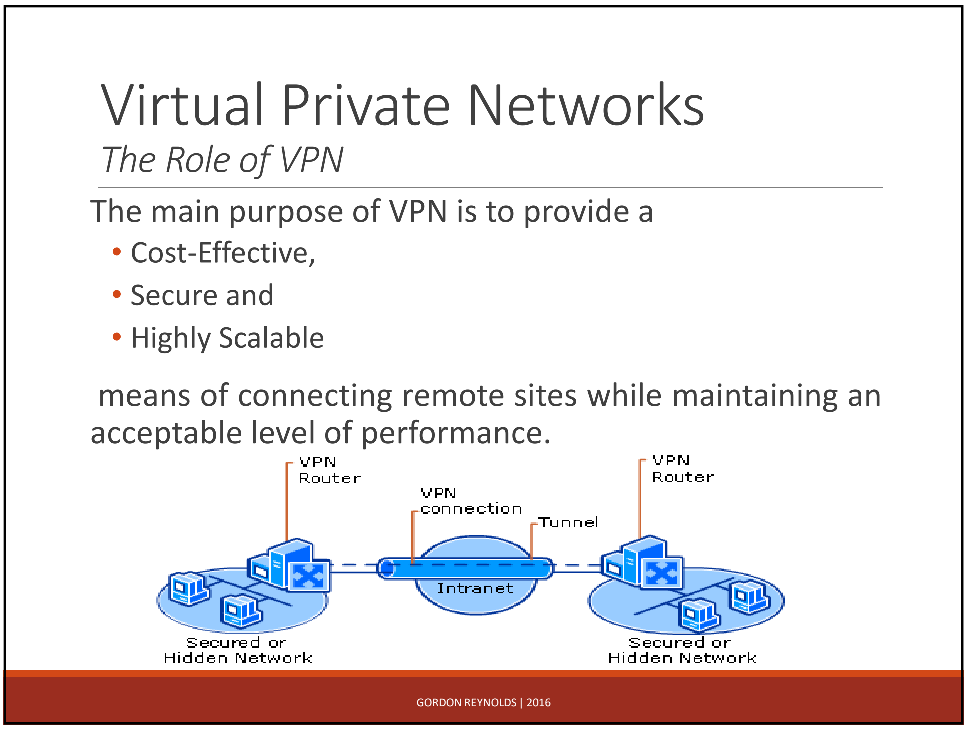


Introduction

Virtual Private Network

Headquarters
Business Partner with CISCO Router
VPN
Perimeter Router
Remote Office with CISCO Router
VPN Concen-trator
CISCO PIX Firewall
POP
Corporate
Regional Office with CISCO PIX Firewall
Mobile Worker with Secure VPN
SOHO with CISCO ISDN/DSL Router

GORDON REYNOLDS | 2016



Virtual Private Networks

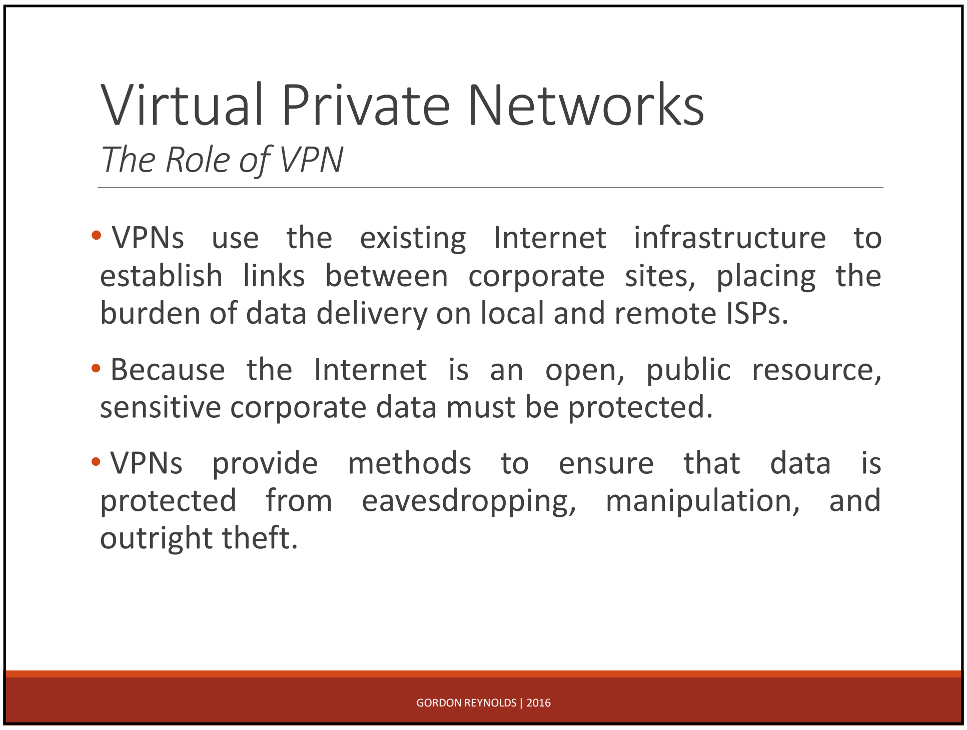
The Role of VPN

The main purpose of VPN is to provide a

- Cost-Effective,
- Secure and
- Highly Scalable

means of connecting remote sites while maintaining an acceptable level of performance.

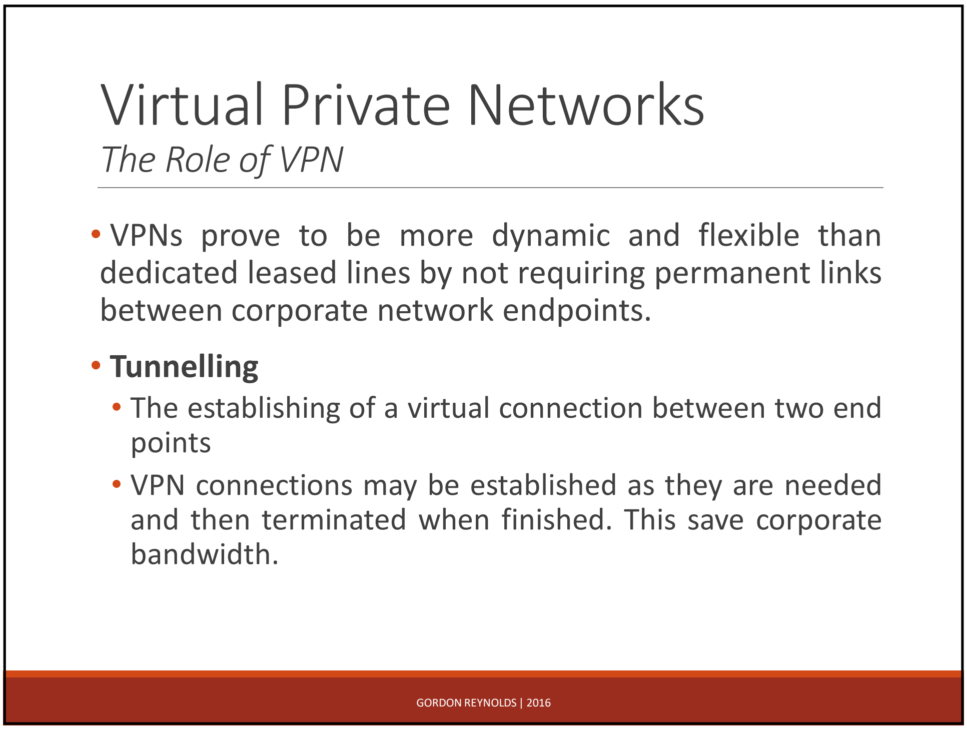
GORDON REYNOLDS | 2016



Virtual Private Networks

The Role of VPN

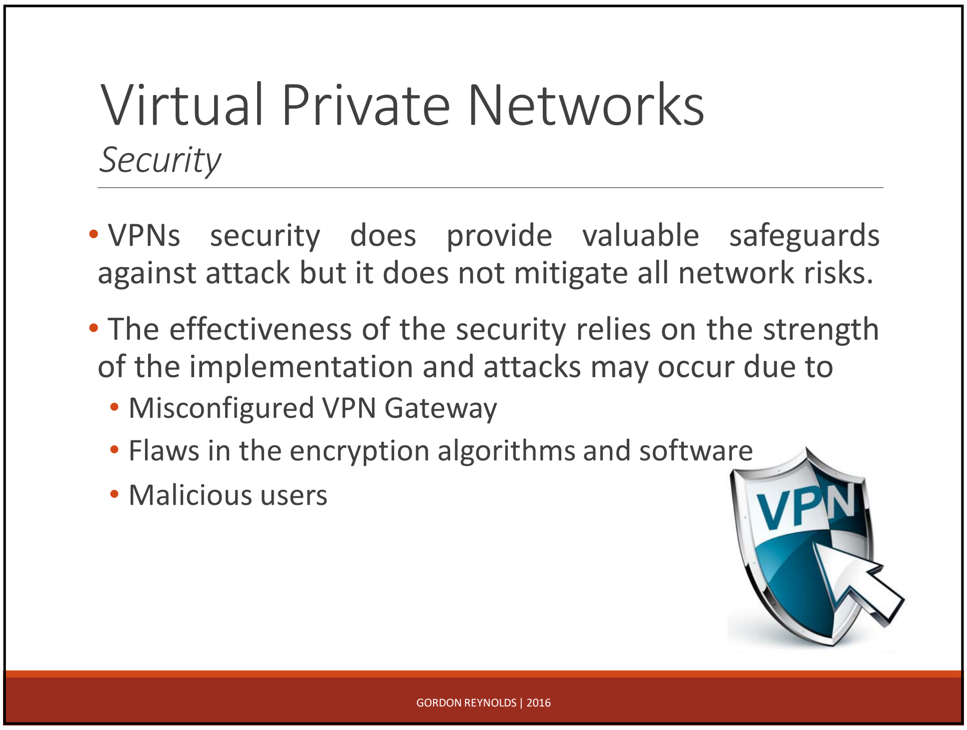
- VPNs use the existing Internet infrastructure to establish links between corporate sites, placing the burden of data delivery on local and remote ISPs.
- Because the Internet is an open, public resource, sensitive corporate data must be protected.
- VPNs provide methods to ensure that data is protected from eavesdropping, manipulation, and outright theft.



Virtual Private Networks

The Role of VPN

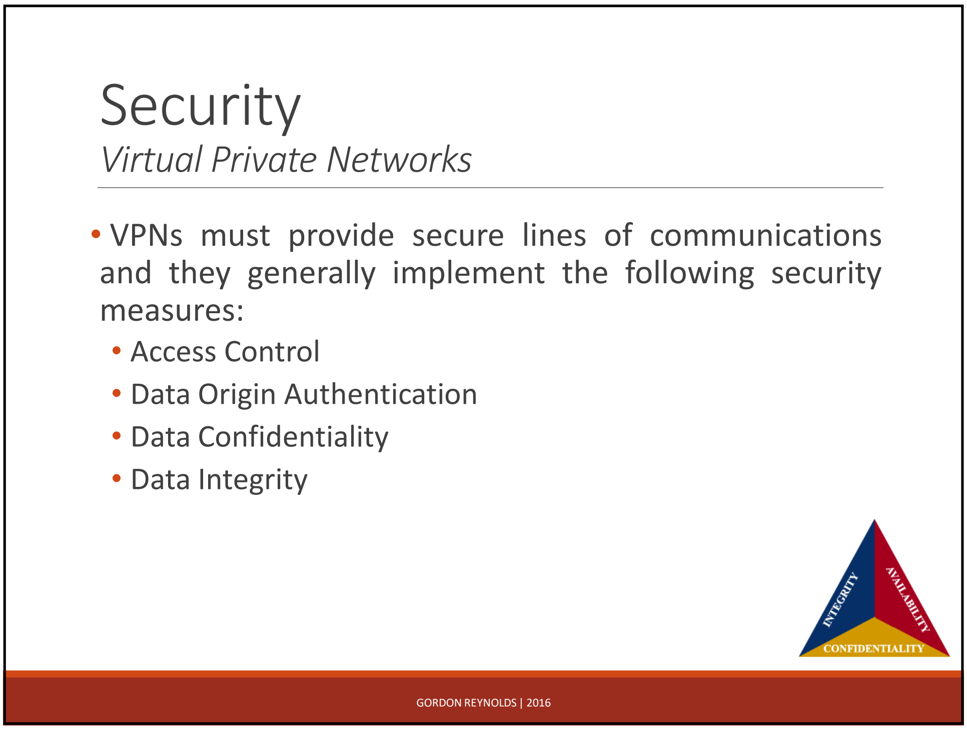
- VPNs prove to be more dynamic and flexible than dedicated leased lines by not requiring permanent links between corporate network endpoints.
- **Tunnelling**
  - The establishing of a virtual connection between two end points
  - VPN connections may be established as they are needed and then terminated when finished. This save corporate bandwidth.



Virtual Private Networks

Security

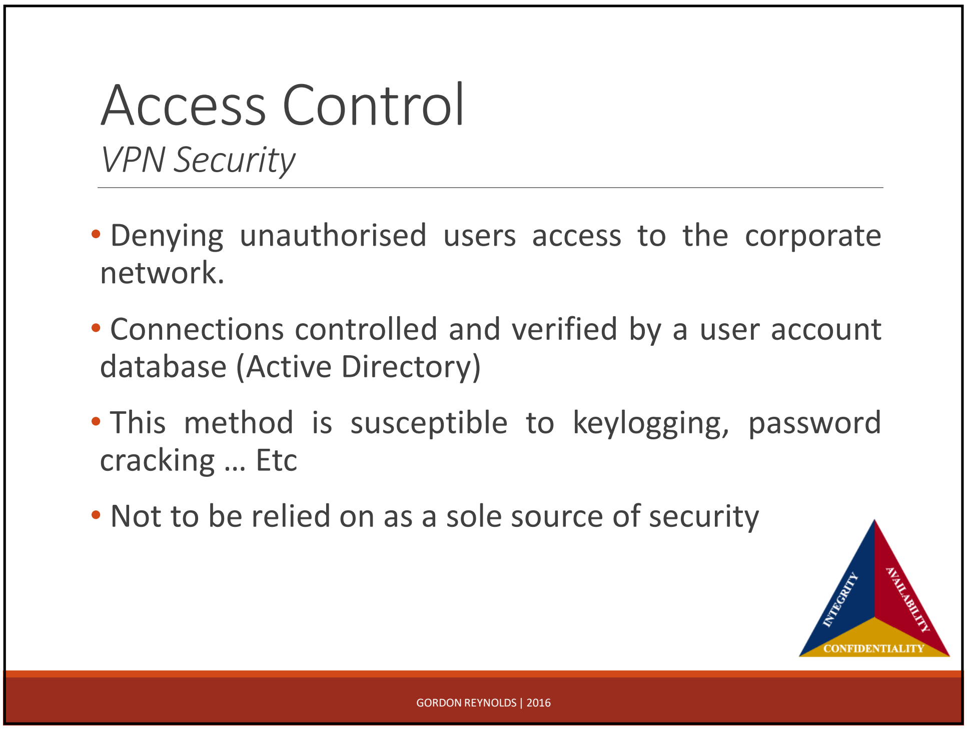
- VPNs security does provide valuable safeguards against attack but it does not mitigate all network risks.
- The effectiveness of the security relies on the strength of the implementation and attacks may occur due to
  - Misconfigured VPN Gateway
  - Flaws in the encryption algorithms and software
  - Malicious users



Security

Virtual Private Networks

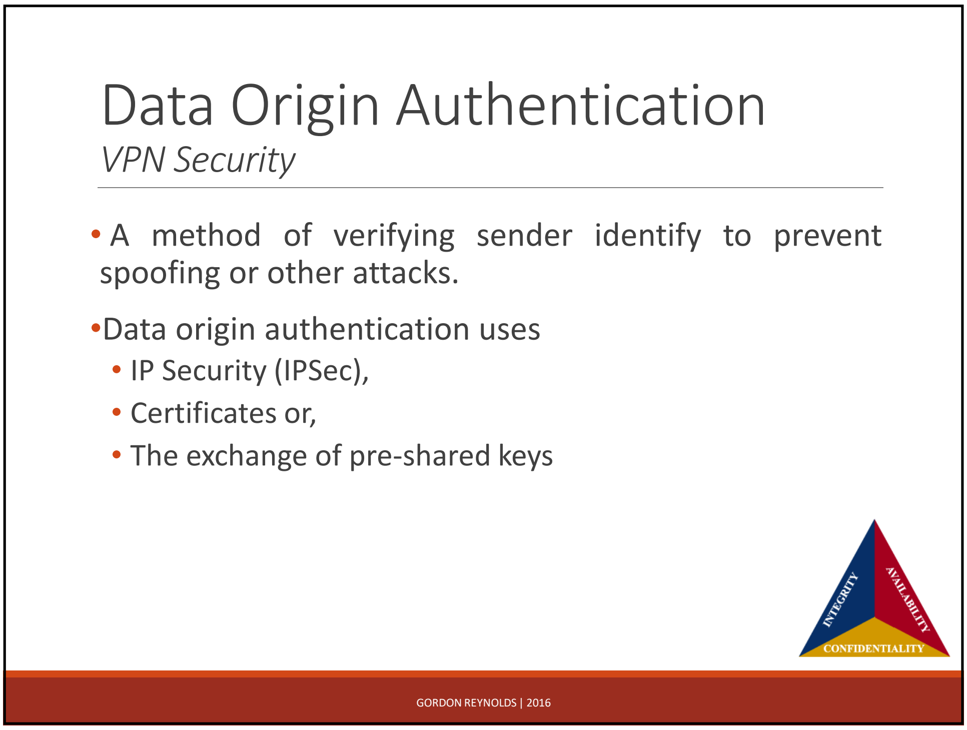
- VPNs must provide secure lines of communications and they generally implement the following security measures:
  - Access Control
  - Data Origin Authentication
  - Data Confidentiality
  - Data Integrity



Access Control

VPN Security

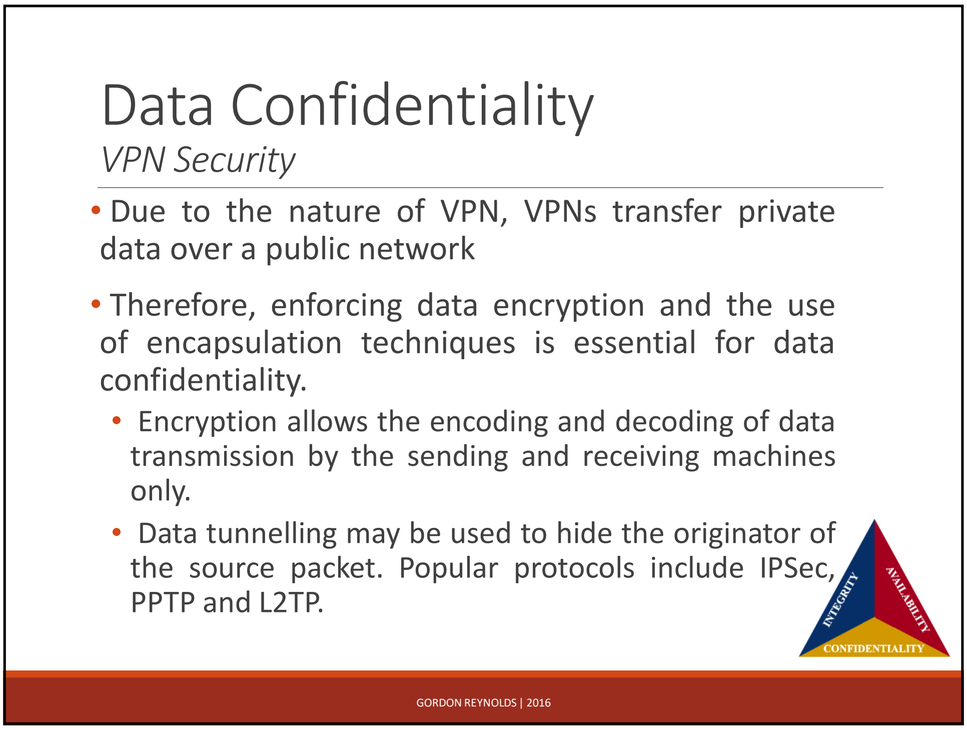
- Denying unauthorised users access to the corporate network.
- Connections controlled and verified by a user account database (Active Directory)
- This method is susceptible to keylogging, password cracking … Etc
- Not to be relied on as a sole source of security



Data Origin Authentication

VPN Security

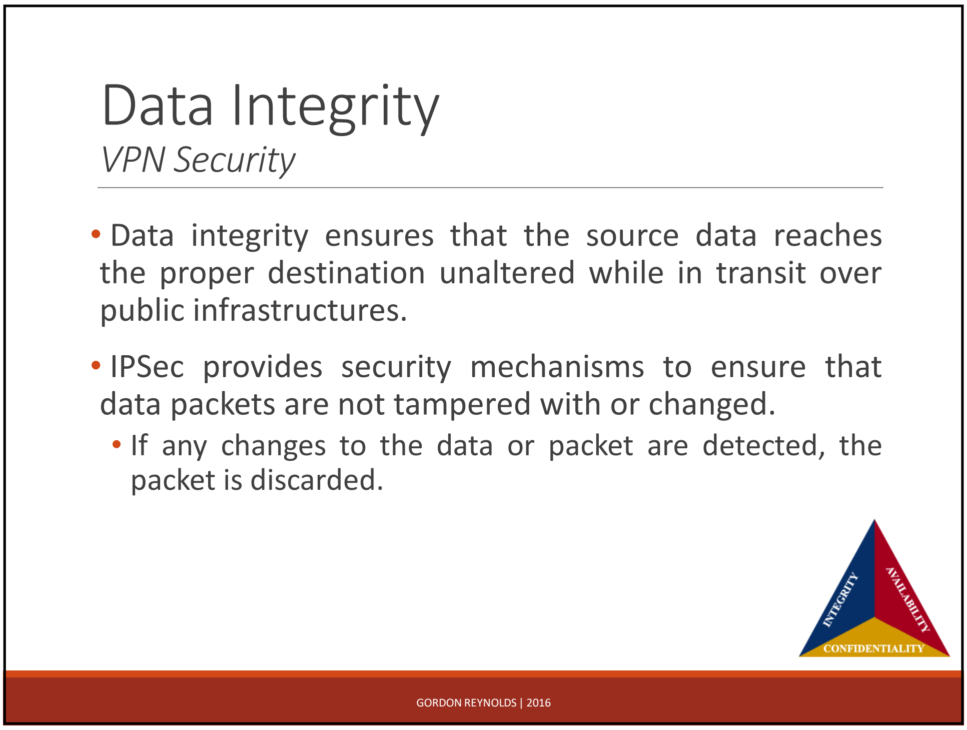
- A method of verifying sender identify to prevent spoofing or other attacks.
- Data origin authentication uses
  - IP Security (IPSec),
  - Certificates or,
  - The exchange of pre-shared keys



Data Confidentiality

VPN Security

- Due to the nature of VPN, VPNs transfer private data over a public network
- Therefore, enforcing data encryption and the use of encapsulation techniques is essential for data confidentiality.
  - Encryption allows the encoding and decoding of data transmission by the sending and receiving machines only.
  - Data tunnelling may be used to hide the originator of the source packet. Popular protocols include IPSec, PPTP and L2TP.

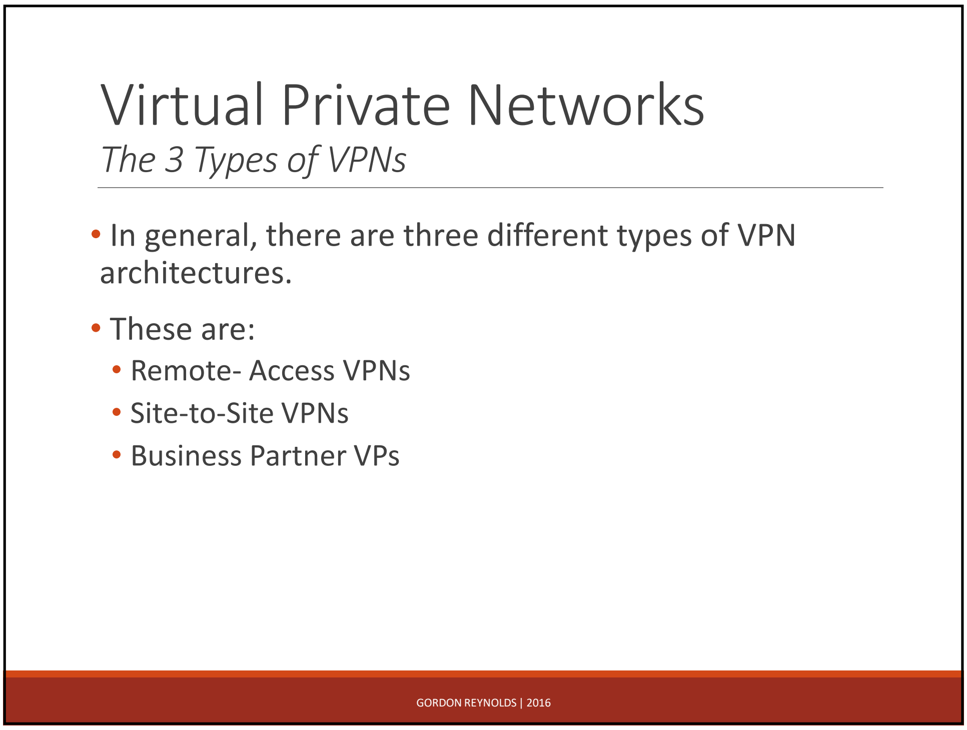


Data Integrity

VPN Security

- Data integrity ensures that the source data reaches the proper destination unaltered while in transit over public infrastructures.
- IPSec provides security mechanisms to ensure that data packets are not tampered with or changed.
  - If any changes to the data or packet are detected, the packet is discarded.

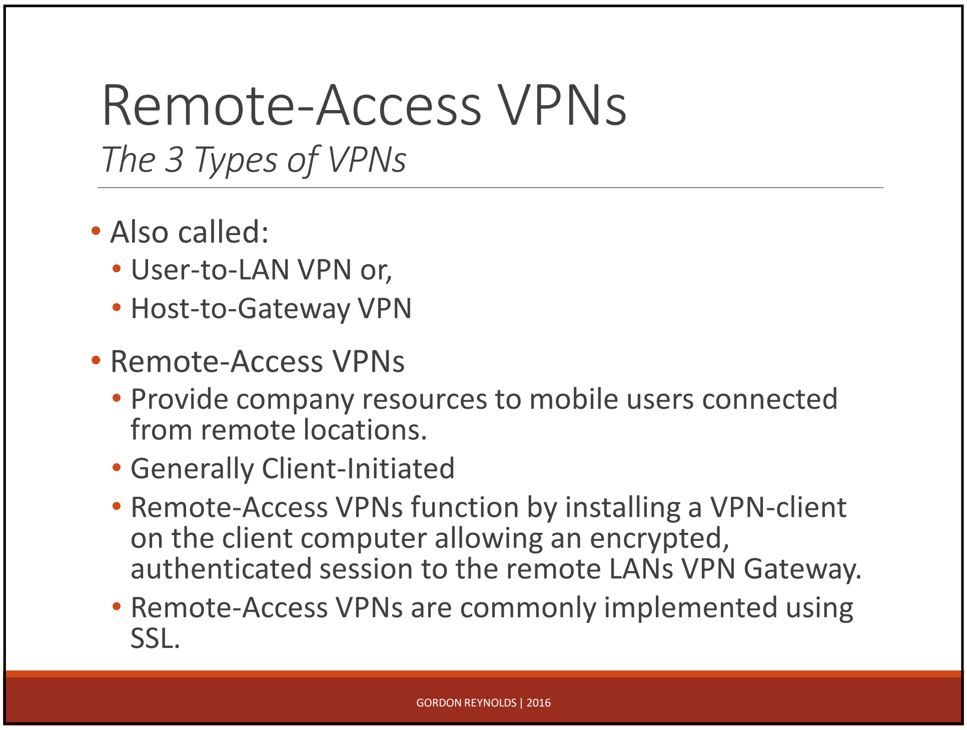
INTEGRITY
AVAILABILITY
CONFIDENTIALITY



Virtual Private Networks

The 3 Types of VPNs

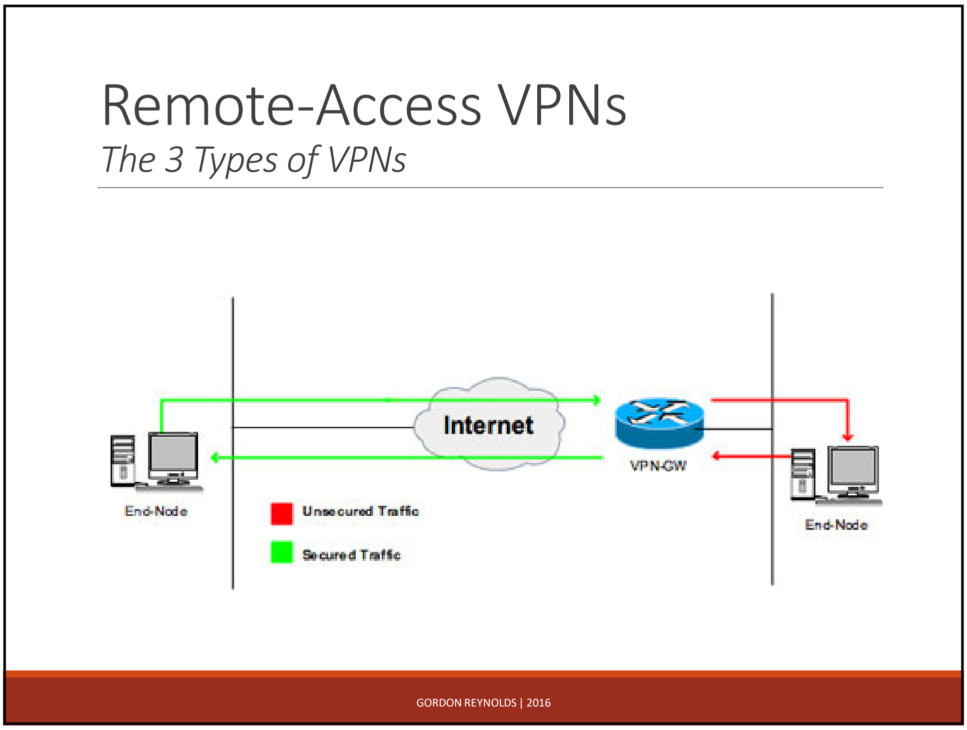
- In general, there are three different types of VPN architectures.
- These are:
  - Remote- Access VPNs
  - Site-to-Site VPNs
  - Business Partner VPs



Remote-Access VPNs

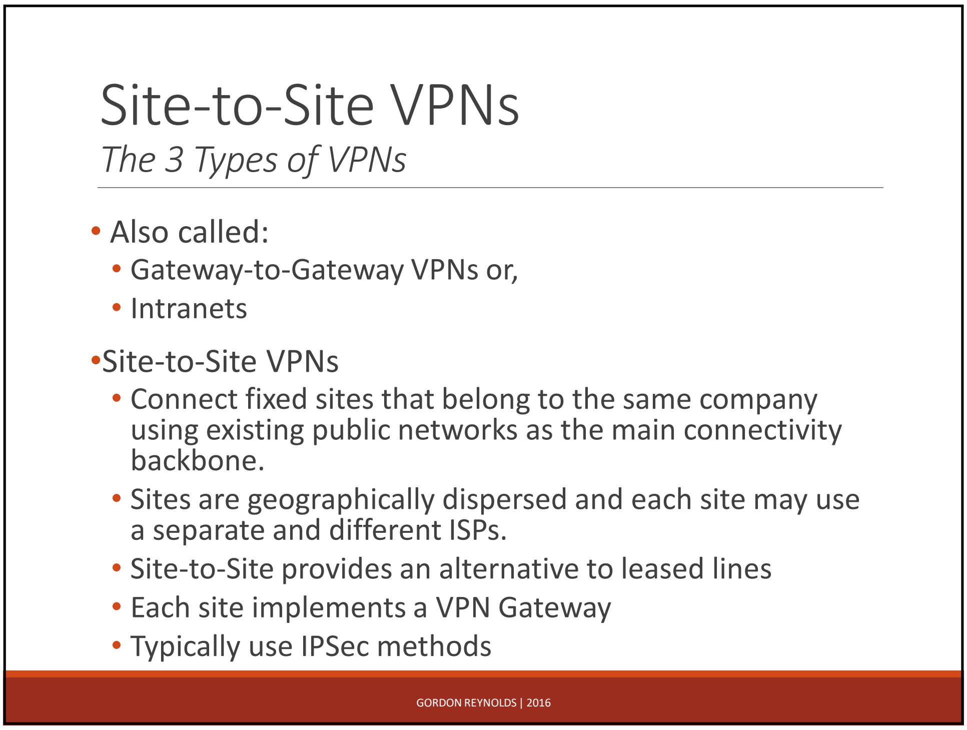
The 3 Types of VPNs

- Also called:
  - User-to-LAN VPN or,
  - Host-to-Gateway VPN
- Remote-Access VPNs
  - Provide company resources to mobile users connected from remote locations.
  - Generally Client-Initiated
  - Remote-Access VPNs function by installing a VPN-client on the client computer allowing an encrypted, authenticated session to the remote LANs VPN Gateway.
  - Remote-Access VPNs are commonly implemented using SSL.



Remote-Access VPNs

The 3 Types of VPNs



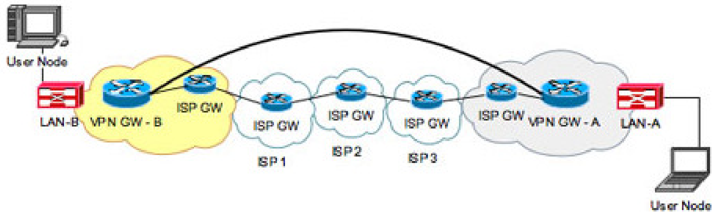
Site-to-Site VPNs

The 3 Types of VPNs

- Also called:
  - Gateway-to-Gateway VPNs or,
  - Intranets
- Site-to-Site VPNs
  - Connect fixed sites that belong to the same company using existing public networks as the main connectivity backbone.
  - Sites are geographically dispersed and each site may use a separate and different ISPs.
  - Site-to-Site provides an alternative to leased lines
  - Each site implements a VPN Gateway
  - Typically use IPSec methods

Site-to-Site VPNs

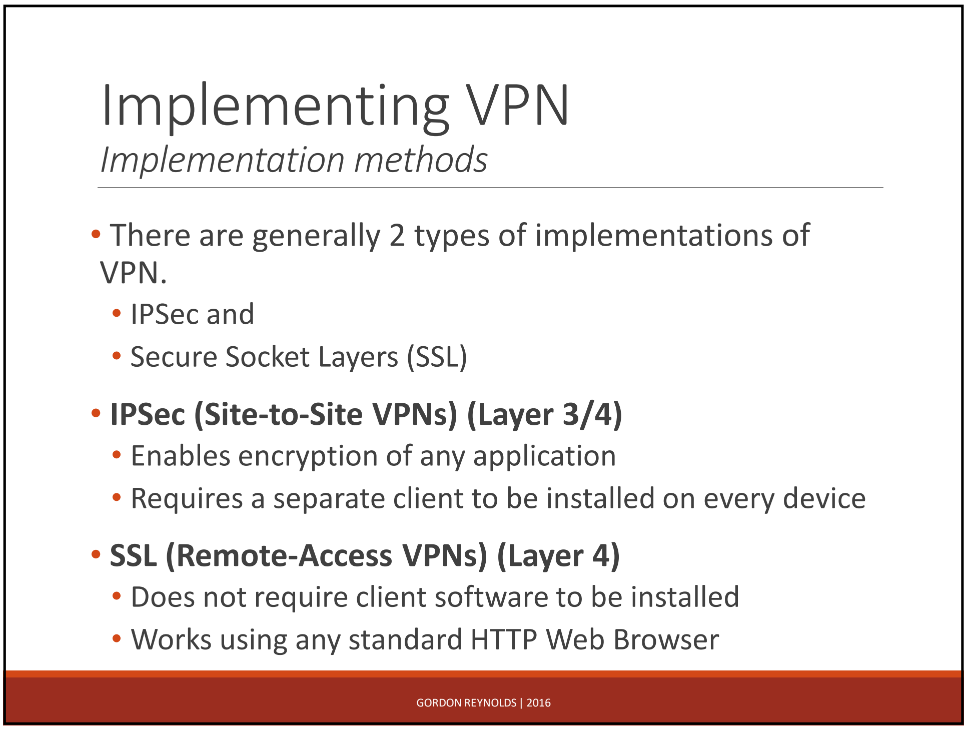
The 3 Types of VPNs



Business Partner VPNs

The 3 Types of VPNs

- Another form of secure Site-to-Site VPNs
- Also known as Extranet VPN
- Used to connect Corporate Partner sites to their business partners or customers.
- Typically IPSec is used due to being inexpensive and it provides a quick deployment.

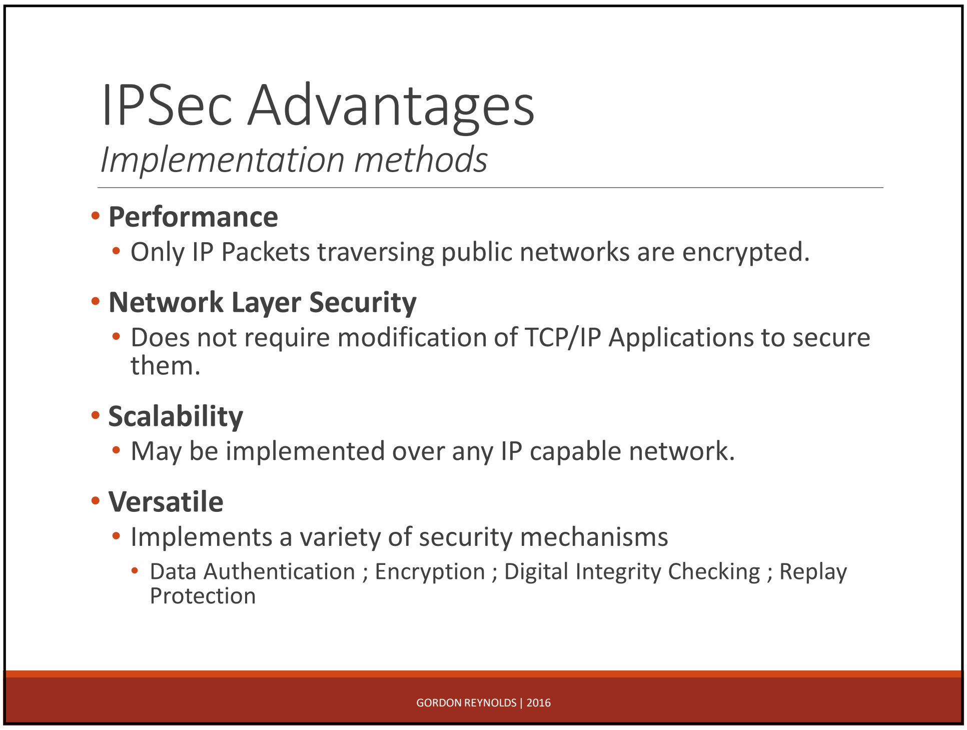


Implementing VPN

Implementation methods

- There are generally 2 types of implementations of VPN.
  - IPSec and
  - Secure Socket Layers (SSL)
- **IPSec (Site-to-Site VPNs) (Layer 3/4)**
  - Enables encryption of any application
  - Requires a separate client to be installed on every device
- **SSL (Remote-Access VPNs) (Layer 4)**
  - Does not require client software to be installed
  - Works using any standard HTTP Web Browser

GORDON REYNOLDS | 2016

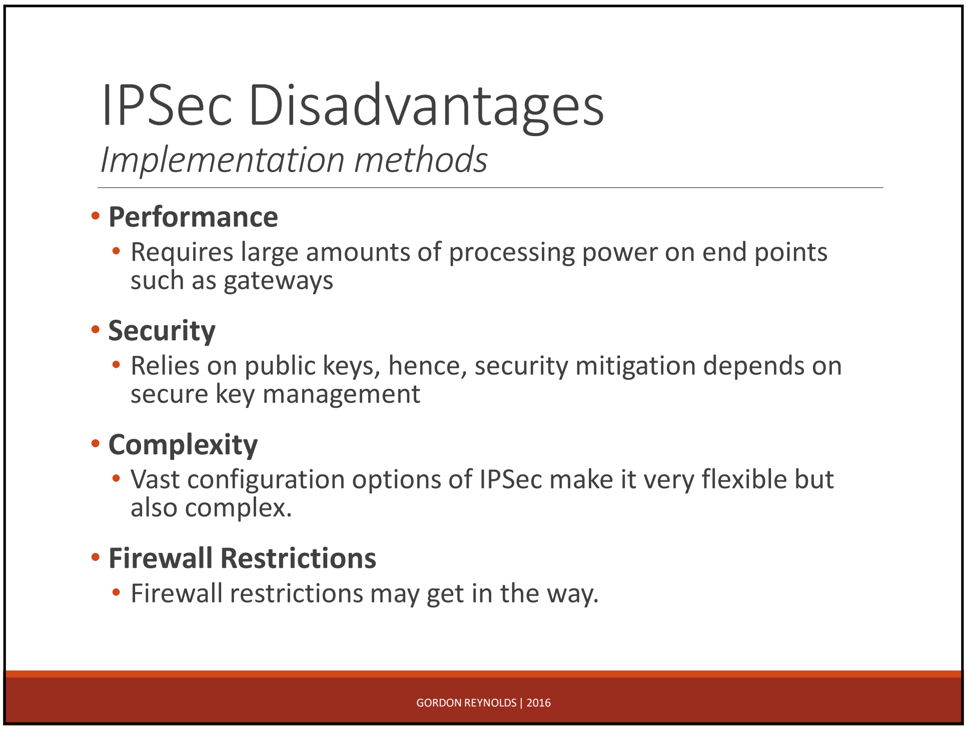


IPSec Advantages

Implementation methods

- **Performance**
  - Only IP Packets traversing public networks are encrypted.
- **Network Layer Security**
  - Does not require modification of TCP/IP Applications to secure them.
- **Scalability**
  - May be implemented over any IP capable network.
- **Versatile**
  - Implements a variety of security mechanisms
    - Data Authentication ; Encryption ; Digital Integrity Checking ; Replay Protection

GORDON REYNOLDS | 2016

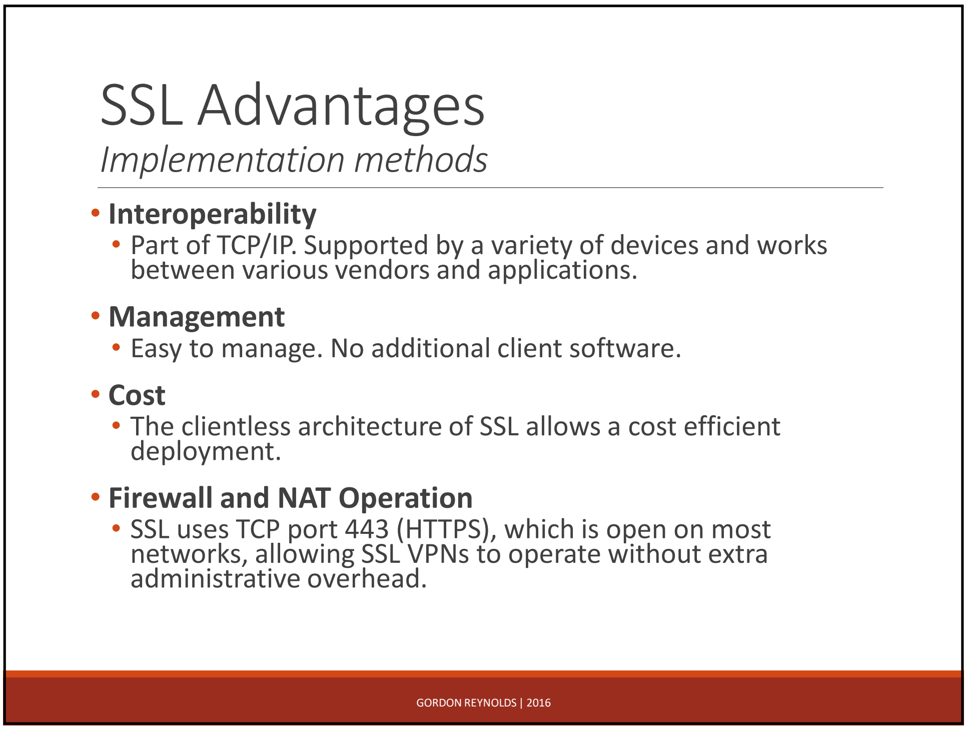


IPSec Disadvantages

Implementation methods

- **Performance**
  - Requires large amounts of processing power on end points such as gateways
- **Security**
  - Relies on public keys, hence, security mitigation depends on secure key management
- **Complexity**
  - Vast configuration options of IPSec make it very flexible but also complex.
- **Firewall Restrictions**
  - Firewall restrictions may get in the way.

GORDON REYNOLDS | 2016

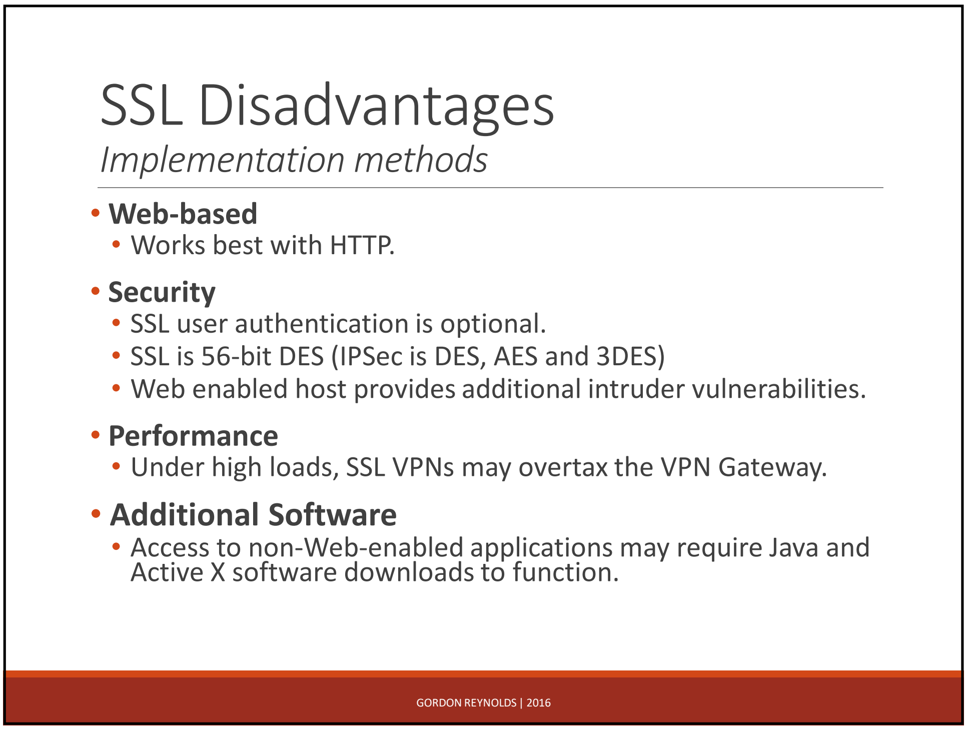


SSL Advantages

Implementation methods

- **Interoperability**
  - Part of TCP/IP. Supported by a variety of devices and works between various vendors and applications.
- **Management**
  - Easy to manage. No additional client software.
- **Cost**
  - The clientless architecture of SSL allows a cost efficient deployment.
- **Firewall and NAT Operation**
  - SSL uses TCP port 443 (HTTPS), which is open on most networks, allowing SSL VPNs to operate without extra administrative overhead.

GORDON REYNOLDS | 2016

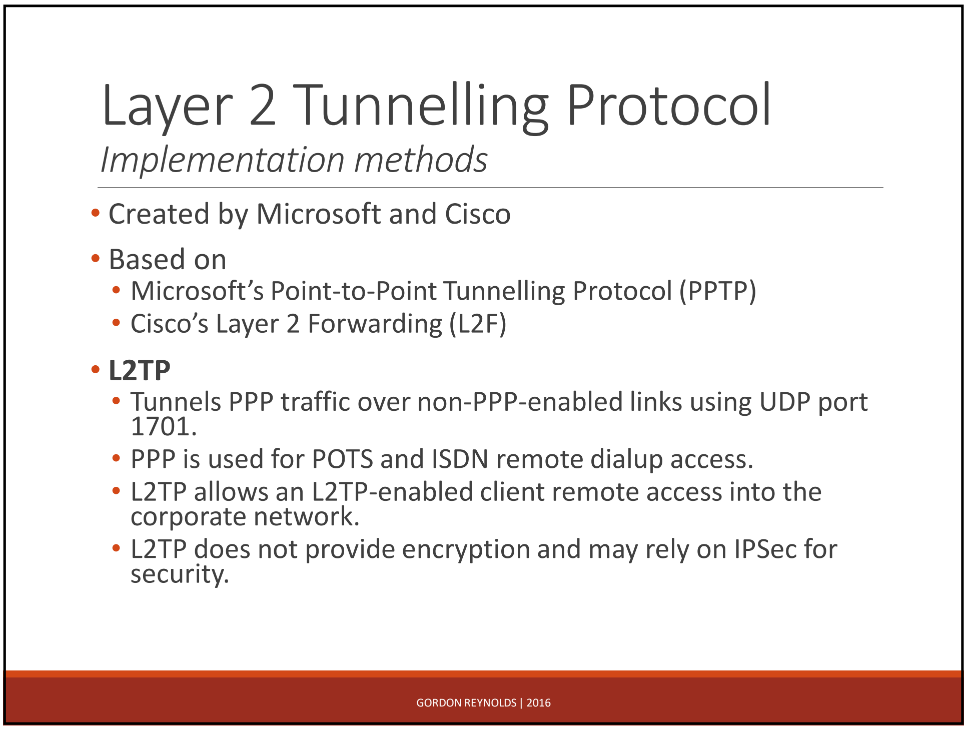


SSL Disadvantages

Implementation methods

- **Web-based**
  - Works best with HTTP.
- **Security**
  - SSL user authentication is optional.
  - SSL is 56-bit DES (IPSec is DES, AES and 3DES)
  - Web enabled host provides additional intruder vulnerabilities.
- **Performance**
  - Under high loads, SSL VPNs may overtax the VPN Gateway.
- **Additional Software**
  - Access to non-Web-enabled applications may require Java and Active X software downloads to function.

GORDON REYNOLDS | 2016

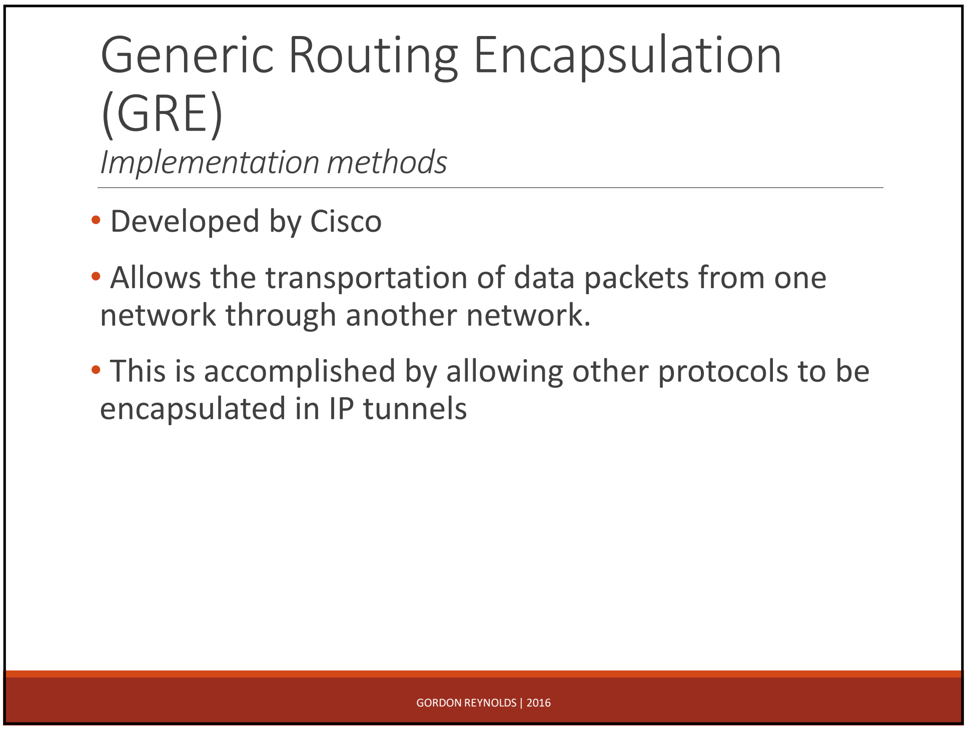


Layer 2 Tunnelling Protocol

Implementation methods

- Created by Microsoft and Cisco
- Based on
  - Microsoft's Point-to-Point Tunnelling Protocol (PPTP)
  - Cisco's Layer 2 Forwarding (L2F)
- **L2TP**
  - Tunnels PPP traffic over non-PPP-enabled links using UDP port 1701.
  - PPP is used for POTS and ISDN remote dialup access.
  - L2TP allows an L2TP-enabled client remote access into the corporate network.
  - L2TP does not provide encryption and may rely on IPSec for security.

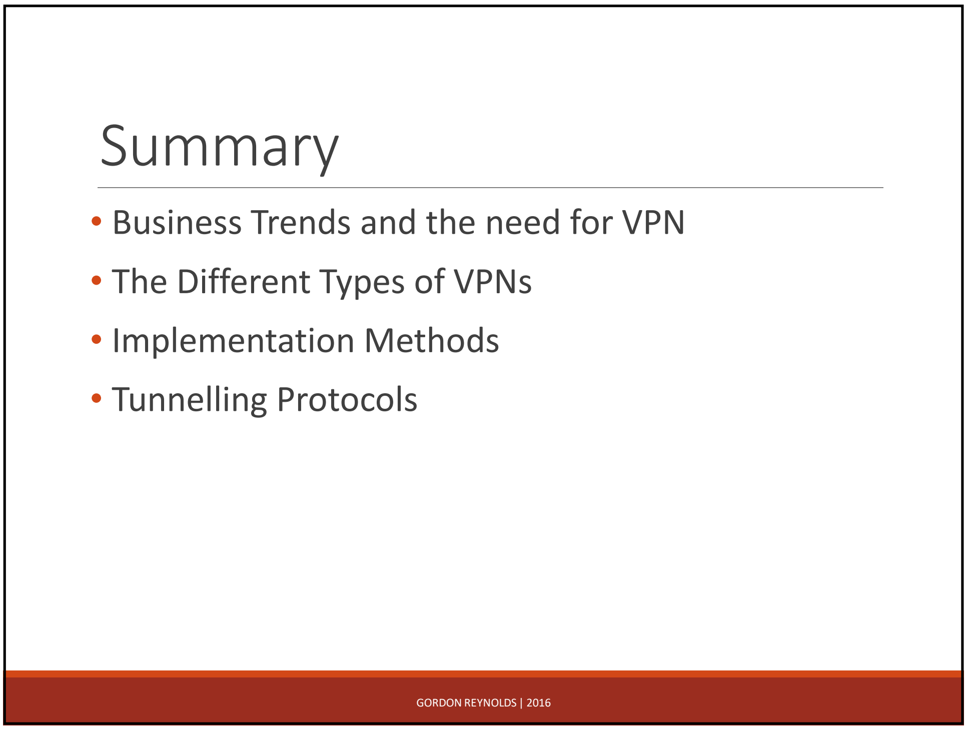
GORDON REYNOLDS | 2016



Generic Routing Encapsulation (GRE)

Implementation methods

- Developed by Cisco
- Allows the transportation of data packets from one network through another network.
- This is accomplished by allowing other protocols to be encapsulated in IP tunnels



Summary

- Business Trends and the need for VPN
- The Different Types of VPNs
- Implementation Methods
- Tunnelling Protocols