Computer Networks

Topic 12:

Virtual Private Networks

Computer Networks

Topic 12 – Lecture 1:

VPN Theory

Scope and Coverage

This topic will cover:

- Virtual private networks (VPN)
- Advantages and disadvantages of VPN
- Installing and configuring VPN

Learning Outcomes

By the end of this topic, students will be able to:

- Explain the operation of a Virtual Private Network (VPN)
- Describe the advantages and disadvantages of a VPN
- Install and configure a VPN

What is a VPN?

- A private network that uses public telecommunication, such as the Internet, instead of leased lines to communicate.
- Remote network communication through Internet
- Used by companies/organisations who want to communicate confidentially
- Two parts:
  - Protected or “inside” network
  - “Outside” network or segment (less trustworthy)

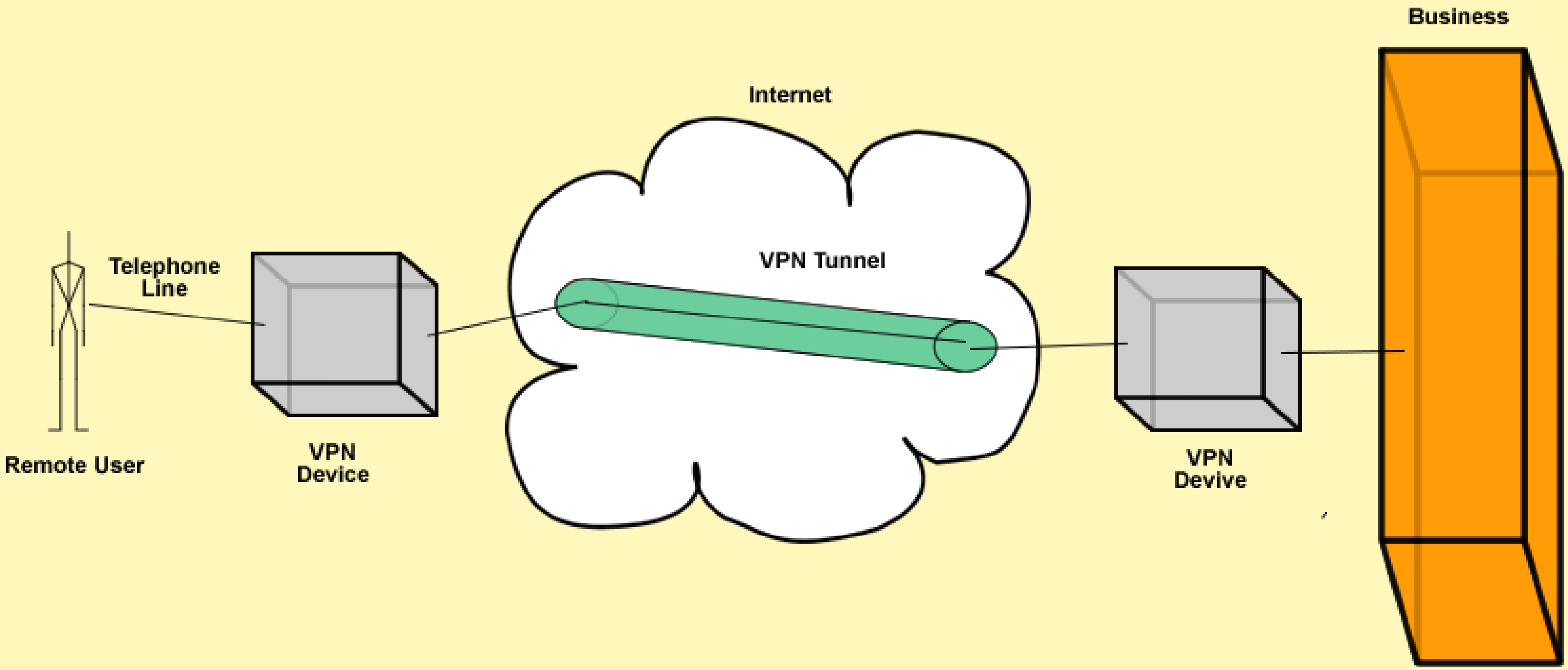
The User’s Perspective

- From the user’s perspective, it appears as a network consisting of dedicated network links.
- These links appear as if they are reserved for the VPN clients only.
- Because of encryption, the data appears to be private.

How a VPN Works - 1

- ***Two connections*** - one is made to the Internet and the second is made to the VPN
- ***Datagrams*** - contain data, destination and source information
- ***Firewalls*** - VPNs allow authorised users and data to pass through the firewalls
- ***Protocols*** - protocols create the VPN tunnels that allow a private connection over a public network

How a VPN Works - 2



Key Functions

- ***Authentication*** - validates that the data was sent from the sender
- ***Access Control*** - preventing unauthorised users from accessing the network
- ***Confidentiality*** - preventing the data from being read or copied as the data is being transported
- ***Data Integrity*** - ensuring that the data has not been altered

Encryption

- Encryption – public key
- Authentication – digital signatures
- A virtual connection is made through the Internet
- Datagrams are sent along the virtual connection
- The outer part of the datagram contains a header and may or may not be encrypted
- The inner part is encrypted

Protocols

- There are three main protocols used:
  - IP Security (IPsec)
  - Point-to-Point Tunneling Protocol (PPTP)
  - Layer 2 Tunneling Protocol (L2TP)

IPsec

- An open standard protocol suite
- Provides privacy and authentication services
- Has two modes of operation
- ***Transport Mode*** encrypts data but not the header
- ***Tunnel Mode*** encrypts both data and header

PPTP

- A data link protocol
- Used to establish a direct connection between two networking nodes
- Creates the virtual connection across the Internet
- Can provide:
  - Connection authentication
  - Transmission encryption
  - Compression

L2TP

- A tunneling protocol
- Does not provide encryption or confidentiality, but relies on an encryption protocol that it passes within the tunnel
- The entire L2TP packet, including payload and header, is sent within a UDP datagram.

Protocols Working Together

- It is common to carry PPTP sessions within an L2TP tunnel.
- L2TP does not provide confidentiality or strong authentication by itself.
- IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity.
- The combination of these two protocols is generally known as L2TP/IPsec.

Advantages

- Cost effective
- Greater scalability
- Easy to add/remove users
- Mobility
- Security

Disadvantages

- Understanding of security issues
- Unpredictable Internet traffic
- Difficult to accommodate products from different vendors

Computer Networks

Topic 12 – Lecture 2:

Implementing VPN

VPN Connections

- A VPN is a secure, private communication tunnel between two or more devices across a public network (e.g. the Internet)
- VPN devices can be:
  - a computer running VPN software
  - a special device like a VPN enabled router
- Remote computers can connect to an office network
- Two computers in different locations can connect to each other over the Internet

VPN Categories

- There are several types of VPN
- There are different ways of classifying VPNs
- We divide them into 2 broad categories based upon architecture:
  - Client-initiated VPNs
  - Network access server (NAS)-initiated VPNs

Client-Initiated VPNs

- Users establish a tunnel across the ISP shared network to the customer network.
- Customer manages the client software that initiates the tunnel
- Advantage - they secure the connection between the client and ISP
- Disadvantage - they are not as scalable and are more complex than NAS-initiated VPNs

NAS-Initiated VPNs

- Users connect to the ISP NAS which establishes a tunnel to the private network.
- More robust than client-initiated VPNs
- Do not require the client to maintain the tunnel-creating software
- Do not encrypt the connection between the client and the ISP
  - not a concern for most customers, because the Public Switched Telephone Network (PSTN) is much more secure than the Internet.

VPNs and the Workplace

- VPNs can run from a remote client PC, remote office router across the Internet, or an IP service provider network to one or more corporate gateway routers (remote access).
- VPNs between a company’s offices are a company intranet.
- VPNs to external business partners are extranets.

Extranet

- An extranet is where the Internet or one or two Service Providers are used to connect to business partners.
- Extends network connectivity to:
  - Customers
  - Business partners
  - Suppliers
- Security policy is very important as potentially the VPN could be used for large orders or contracts.

Intranet

- Intranet VPNs extend a basic remote access VPN to other corporate offices.
- Connectivity is across the Internet or across the Service Provider IP backbone.
- Service levels are likely to be maintained and enforced within a single Service Provider.
- For VPNs across the Internet (multiple Service Providers) there are no performance guarantees
  - no one is in charge of the Internet!

Remote Access VPN - 1

- Encrypted connections between mobile or remote users and their corporate networks
- Remote user can make a local call to an ISP, as opposed to a long distance call to the corporate remote access server
- Ideal for a telecommuter or mobile sales people
- VPN allows mobile workers & telecommuters to take advantage of broadband connectivity

Remote Access VPN - 2

- Utilises access technologies to allow remote users to become part of a corporate VPN
- Usually involves the use of the Point-to-Point Protocol (PPP) and tunnels that extend the PPP connection from the access server to the corporate network
- In Microsoft Point-to-Point Tunneling Protocol (PPTP) the tunnel is extended from the access server out to the end-user PC.

Virtual Private Dial-Up Networking

- Virtual private dial-up networking (***VPDN***) enables users to configure secure networks that rely upon ISPs to tunnel remote access traffic.
- Remote users can connect using local dial-up
- Dial-up service provider forwards the traffic
- Network configuration and security remains in the control of the client
- The dialup service provider provides a virtual pipe between the sites.

VPN in Industry

- ***Healthcare***: transferring confidential patient information within a healthcare provider
- ***Manufacturing***: suppliers can view inventories & allow clients to purchase online safely
- ***Retail***: securely transfers sales data or customer info between stores & headquarters
- ***Banking***: enables account information to be transferred safely within departments & branches

VPN – Future Trends?

- As the VPN market becomes larger, more applications will be created along with more VPN providers and new VPN types.
- Networks may converge to create an integrated VPN.
- Improvements in protocols are expected which could improve the performance and services available via VPNs.

References

- Tanenbaum, A.S. & Weatherall, D.J. (2010). *Computer Networks*, 5th edition. Pearson Education.
- The Cisco website: http://www.cisco.com/
- The Microsoft website: http://technet.microsoft.com/en-us/library/cc739294(WS.10).aspx

Topic 12 – Virtual Private Networks

Any Questions?