Bringing British Education to You
www.nccedu.com

Network Security and Cryptography

Topic 10:
Virtual Private Networks

V1.0

Bringing British Education to You
www.nccedu.com

Network Security and Cryptography

Topic 10 – Lecture 1:
Introduction to VPN

V1.0

Scope and Coverage

This topic will cover:

- Virtual Private Network technologies
- Issues with Virtual Private Networks

V1.0

Learning Outcomes

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

- Configure access control mechanisms
- Explain Virtual Private Networks

What is VPN?

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

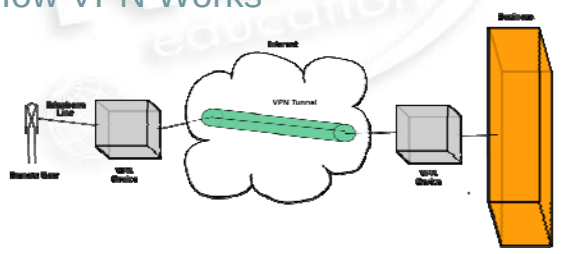
The User’s Perspective

- 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
  - Hence it appears to be a private connection
- Because of encryption, the data appears to be private

How VPN Works

- 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 VPN Works



Key Functions

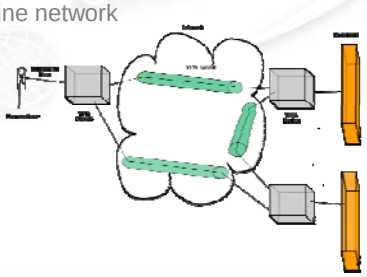
- Authentication - validates that the data was sent from the sender
- Access Control - preventing unauthorised users from accessing the network
- Confidentiality - preventing the data from being read or copied as the data is being transported
- Data Integrity - ensuring that the data has not been altered

Encryption & Tunnelling

- Encryption – public key encryption techniques are used
- 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

A Network

- Multiple VPN connections can be made to create a genuine network



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
- Each connection is a ***security association*** (SA)
  - Has one security identifier for each direction
  - Each security identifier is carried in packets and used to look up keys, etc.

IPsec Transport Mode

- IPsec header is inserted just after the IP header
- Protocol field of IP header is modified to indicate that the IPsec header follows
- IPsec header contains security information:
  - SA identifier
  - Sequence number
  - Possibly an integrity check on the payload

IPsec Tunnel Mode

- Whole IP packet including header is encapsulated in a new IP packet with a IPsec header
- Useful when the tunnel end is not the final destination
  - E.g. tunnel ends at company firewall
  - Firewall deals with encapsulating IP packets into IPsec packets and decapsulating
  - Machines on internal network do not have to be aware of IPsec as they receive and send IP packets

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 tunnelling 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

Network Security and Cryptography

Topic 10 – Lecture 2:
VPN Connections

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 computer can connect to an office network
- Two computers in different locations can connect over the Internet

VPN Categories

- There are several types of VPN
- There are different ways of classifying VPNs
- We use two 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 is that they secure the connection between the client and ISP
- Disadvantage is that they are not as scalable and are more complex than NAS-initiated VPNs

Virtual Private Networks Topic 10 - 10.25

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

V1.0 © NCC Education Limited

Virtual Private Networks Topic 10 - 10.26

VPNs and the Workplace

- VPNs can run from a remote client PC or 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**

V1.0 © NCC Education Limited

Virtual Private Networks Topic 10 - 10.27

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

V1.0 © NCC Education Limited

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

- 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

- 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's Point-to-Point Tunneling Protocol (PPTP) it also extends the tunnel 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 dial-up service provider provides a virtual pipe between the sites

VPN in Industry

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

VPN in Small Businesses

- Operating systems often have built-in VPN protocols
- These often rely on usernames and passwords
  - Not very secure or private
- Standard VPNs require the deployment of software and clients
  - Costs money and time
- SSL VPNs are easy to install and use ports already available for secure traffic over the Internet

SSL VPNs

- Connect securely via a standard Web browser
- No special software required on client computers
- Traffic between Web browser and the SSL VPN device is encrypted with the SSL protocol
- Support access control by:
  - User
  - Device
  - Location

SSL & Data Protection

- SSL encrypts data
- Each SSL certificate uses public key encryption techniques
- The SSL handshake either authenticates the server and client or blocks unauthorized users
- Keeps data confidential and protected

SSL Portal VPN

- Allows a single SSL connection to a website
- User securely accesses multiple network services from the website
- Can use any modern browser
- User is authenticated via method supported by the portal
- User then has access to a web page that acts as the portal to other services

SSL Tunnel VPN

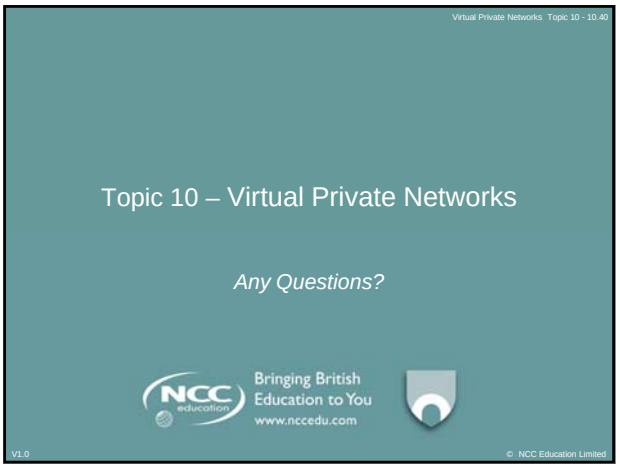
- Allows a web browser to securely access multiple network services through a tunnel running under SSL
  - Includes applications and protocols that are not web-based
- Requires a web browser that can run active content
- Can provide functionality not accessible via SSL portal VPNs

SSL Costs

- Initial costs are higher
  - Requires purchase of SSL Certificate
- Can save money in the long run
  - Reduced management/administration costs
  - Plus the savings from having secure communications

References

- Sybex, (2001). *Hacking Exposed: Networking Complete*. 2nd Edition. John Wiley & Sons.
- Tanenbaum, A.S. (2003). *Computer Networks*. 4th Edition. Prentice Hall.


Virtual Private Networks Topic 10 - 10.40
Topic 10 – Virtual Private Networks
Any Questions?
Bringing British
Education to You
www.nccedu.com
V1.0
© NCC Education Limited