Network Security

Dr. Ihsan Ullah

Department of Computer Science & IT
University of Balochistan, Quetta
Pakistan

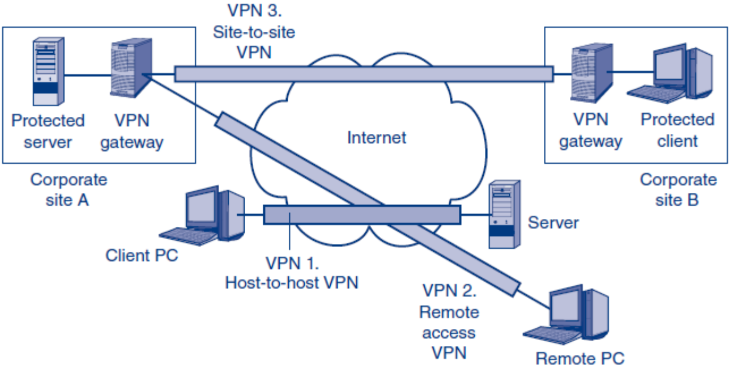
April 11, 2015

Virtual private networks (VPNs)

- A virtual private network (VPN) is created by using a cryptographic system to secure communication over an untrusted network (the Internet, a wireless LAN, etc.).

Types of VPN

- Host-to-host VPN, remote access VPN and site-to-site VPN



Types of VPN I

Host-to-host VPN

- Connects a single client over an untrusted network to a single server
- Connection to an e-commerce server on the Internet

Remote Access VPN

- A remote access VPN connects a single remote PC over an untrusted network to a site network
- Remote access users connect to a VPN gateway, which authenticates them and gives them access to authorized resources within the site

Types of VPN II

Site-to-Site VPN

- Protects all traffic flowing over an untrusted network between a pair of sites
- Sending VPN gateway encrypts outgoing messages
- Receiving VPN gateway then decrypts incoming messages and pass these messages to the correct destination hosts in the receiving site

Secure Sockets Layer (SSL)

- Created by Netscape corporation
- Renamed to Transport Layer Security (TLS) by IETF (Internet Engineering Task Force)
- Began as a host-to-host VPN standard; recently became a remote access VPN, thanks to the emergence of SSL/TLS gateways
- Often used to provide security to transactions that take place over HTTP
- Secures TCP by providing confidentiality, data integrity and server and client authentication
- Can be employed by any application that runs over TCP

SSL handshake I

1. Client requests a TCP connection with the server
2. Server establishes the connection
3. The client sends a list of cryptographic algorithms it supports along with nonce
4. From the list, the server chooses a symmetric algorithm, a public key algorithm and a MAC algorithm. Server sends its choices to the client along with a certificate and its nonce
5. The client verifies the certificate, extracts the server's public key, generates a Pre-Master Secret (PMS), encrypts the PMS with the server's public key, and sends the encrypted PMS to the server

SSL handshake II

6. Using the standard key derivation function, the client and server independently compute the Master Secret (MS) from the PMS and nonces(control against replay attack). The MS is then sliced up to generate two encryption keys and two MAC keys
7. The client sends a MAC of all the handshake messages.
8. The server sends a MAC of all the handshake messages.

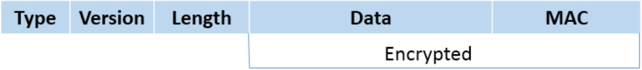
SSL data transfer I

- Both parties have the same four keys after the handshake
- Consider Alice and Bob as the two entities
- The four keys will be as follows:
  - $E_B =$ session encryption key for data sent from Bob to Alice
  - $M_B =$ session MAC key for data sent from Bob to Alice
  - $E_A =$ session encryption key for data sent from Alice to Bob
  - $M_A =$ session MAC key for data sent from Alice to Bob
- SSL breaks the data stream into records, appends a MAC to each record for integrity checking, and then encrypts the record + MAC

SSL data transfer II

- To create the MAC, Bob inputs the record data along with the key M_B into a hash function
- To encrypt the package record+MAC, Bob uses his session encryption key E_B
- This encrypted package is then passed to TCP for transport over the Internet

SSL record



Type	Version	Length	Data	MAC
			Encrypted	

- The type field differentiates between a handshake message and a data message
- Also used to close connection
- The length field is used to extract the SSL record from the TCP byte stream

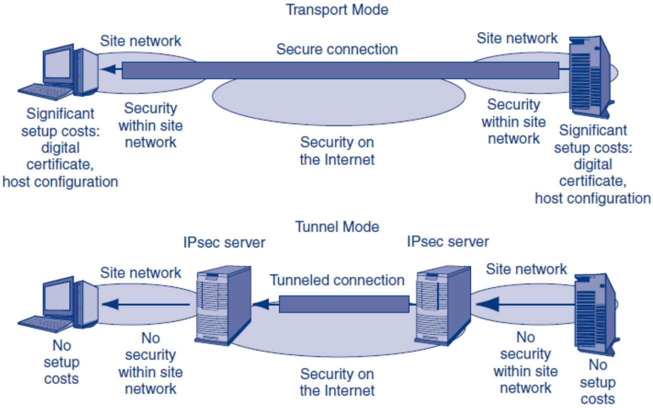
IPSec

- A family of IETF cryptographic security standards collectively called IPsec (IP security)
- Secure the IP (including everything within an IP packet's data field)
- Gives transparent protection to transport layer and application layer messages
- IPsec is the gold standard in VPN security offering the strongest protection and centralized control
- More complex and therefore more expensive to introduce than SSL/TLS

IPSec operating modes

Two operating modes:

- Transport mode and tunnel mode



Transport Mode
Site network
Secure connection
Site network
Significant setup costs: digital certificate, host configuration
Security within site network
Security on the Internet
Security within site network
Significant setup costs: digital certificate, host configuration
Tunnel Mode
IPsec server
IPsec server
Site network
Tunneled connection
Site network
No setup costs
No security within site network
Security on the Internet
No security within site network
No setup costs

IPSec transport mode

Pros

- Gives host-to-host security by implementing host-to-host VPN
- Provides security when packets travel over internal site networks as well as across the Internet

Cons

- Requires to set up IPsec explicitly on every client and server
- Turns firewalls useless because they cannot read a packet's plaintext content to filter it

IPSec tunnel mode

- Only protects traffic between two IPsec gateways at different sites
- Encryption/decryption occurs only at gateways
- Easier management and lower cost
- Firewall friendly
- No protection within the site

IPSec protection types

- Three types of protection through three IPSec protocols

Authentication

- Authenticates the sender through a packet header
- Authentication Header (AH) protocol

Confidentiality

- Confidentiality is ensured through encryption
- Encapsulating Security Payload (ESP) protocol
- Also supports authentication

Key management

- Internet Security Association and Key Management Protocol