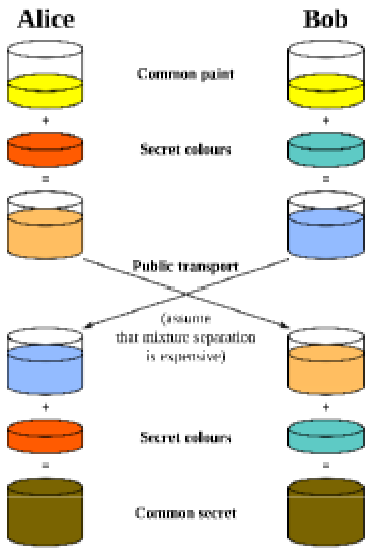
Lecture 8 Notes-Protocols & Firewalls

Protocols Outline

1. Protocols
2. TLS / HTTPS
3. VPNs
4. Firewalls
5. Deep Packet Inspections, Intrusion Prevention

Security Layer between HTTP and Transport Layer (TCP) – SSL/TLS

- Establishes a shared key to protect message confidentiality, integrity and authenticity
- main sub-protocols are TLS handshake to negotiate parameters, optional authentication, establish shared key
- and TLS record, the actual secure transport protocol
- Uses Diffie-Hellman key exchange to create shared secret



1. Alice and Bob agree on a base g and modulus n (these values are public)

2a. Alice generates random A and a=g^A mod n

2b. Bob generates a random B and b=g^B mod n

3. They exchange a and b

4. Shared key is K= b^A = g^{BA} mod n = g^{AB} mod n = a^B

TLS Phases

1. TLS Handshake

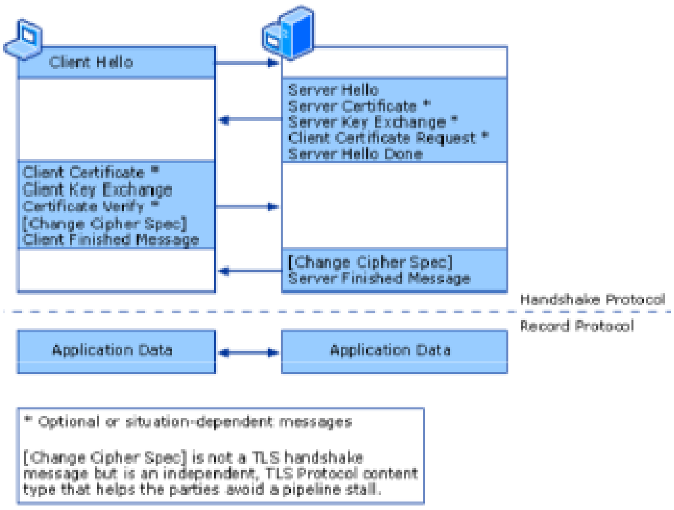
Can authenticate server and client. In HTTPS mostly only the server is authenticated. Results in a shared key and session ID or session ticket.

1. TLS Record

After the exchange of ChangeCipherSpec messages, all subsequent traffic is encrypted.

1. TLS Alert

Immediately closes a session



(Source: Microsoft)

Authentication with certificates

- A certificate provides additional information for a public key
- Owner of the matching private key
- Validity (exp date & time)
- Subject name
- Issuer name
- Other parameters

Trusted certificates

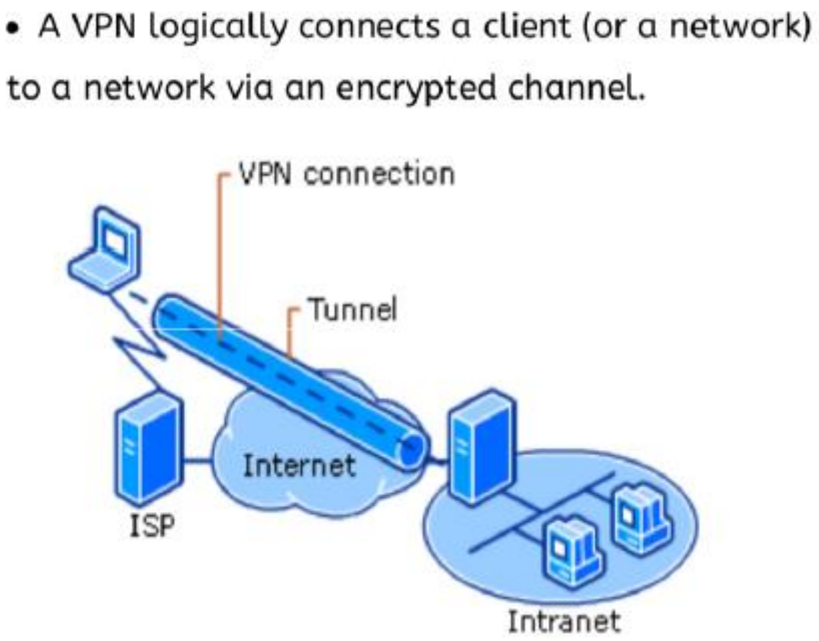
- A certificate digitally signed by a known certification authority
- Browsers come with a list of these authorities

Problems with certificate

- Certificate revocation (certificate that has been revoked before its exp date due to violation of policy, private-key compromised, user no longer have private-key etc.)
- Relation between name and principal
- New policies are stricter making less efficient

Virtual Private Network (VPN)

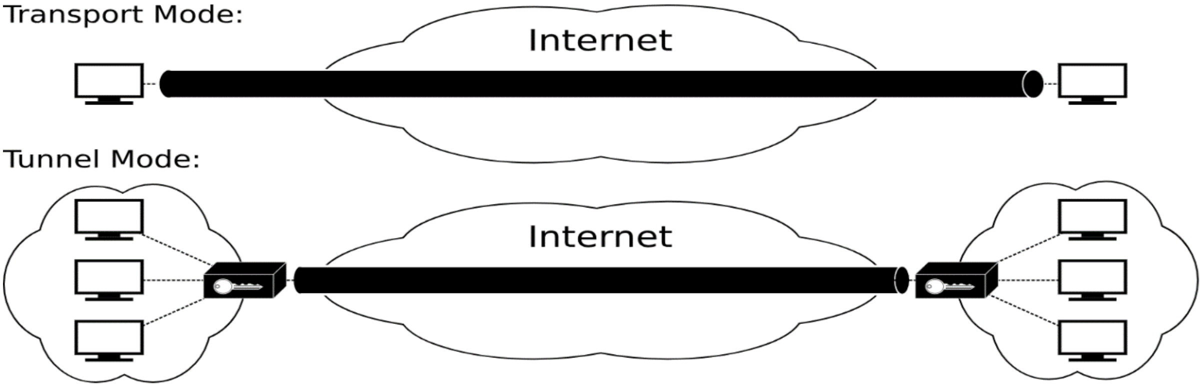
- Routes packets between different networks
- Tunnel established through TLS, IPSec
- Security only between tunnel endpoints



- A VPN logically connects a client (or a network) to a network via an encrypted channel.

IPSEC – A protocol suite on the level of IP packets:

- Can authenticate and encrypt data for each IP packet during transmission
- Transport mode: Payload in IP packets is encrypted, integrity of header is protected. Used for end-to-end communication between two devices.
- Tunneling mode: Entire IP packet is encrypted and authenticated, encapsulated into a new IP packet and header. Used to create VPNs and host-to-host / network-to-network communication



IPSec Core Protocols

Authentication Header (AH) – provides connectionless integrity by using a hash function and a secret shared key in the AH algorithm. Also guarantees data origin by authenticating IP packets.

Encapsulating Security Payload (ESP) – Provides confidentiality through encryption for IP packets, but can also provide origin authenticity, data integrity through hash functions, anti-replay and limited traffic flow integrity. Mostly uses AES

IPSec Authentication

- Before AH or ESP can be used, keys need to be established (security association)
- IKE internet key exchange is used
- IKE can use pre-shared keys or certificates

Protecting Keys – An alternative way to establish security associations

- Use a Trusted Platform Module TPM to generate and protect keys
- Provides a secure device identity
- TLS and IKE can both use TPM-based authentication

Firewall Outline

1. Firewalls
2. Network View on Firewalls – Perimeter Protection
3. DMZ – demilitarized zone
4. Next generation firewalls
5. Virus scanner

Firewall

- A barrier between internal network and outside network
- Filters traffic using security rules that define what can go in and out

Packet filter firewall

- Operates on Network layer (and above)
- Filters based on source and destination IP addresses, protocols, ports, current stage of a connection
- Static filtering rule set
- Standard security mechanisms and cost-effective

How does it work?

- Firewall software inspects the first few bytes of TCP or UDP headers in an IP packet
- Finds application protocol and port (e.g. HTTP with port 80 or SMTP with port 25)
- Traffic from inside out is allowed (except when explicitly blocked)
- E.g. would block network management traffic (SNMP on UDP ports 161, 162)
- Traffic from outside in should be blocked if not explicitly permitted

Which traffic should be permitted?

- Different rules for existing connections and new connections
- Depends on applications/services running behind the firewall

Minimum information one needs to define:

1. Source IP address (or range)
2. Destination IP address (or range)
3. Destination port (or range)

Source IP addresses examples:

1. Any address should be able to connect to a web server.
2. Management access should be restricted to specific IP addresses.

Destination IP addresses examples:

1. IP address of the server running a service that should be accessed
2. Destination address needs to be defined
3. Never allow any IP address

Destination port examples:

1. Specifies the service accessed via a particular port.
2. Example: A Web-server needs incoming connections on port 80 (HTTP) and port 443 (HTTPS).
3. Never allow any port

Where to place a firewall

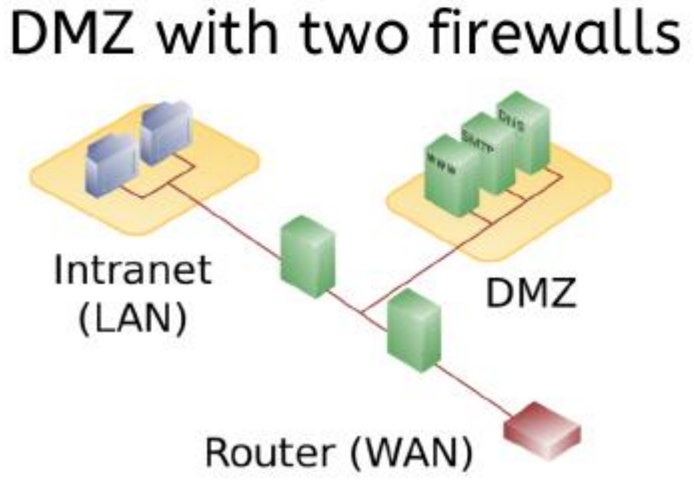
- Firewall software on PCs is essential, but not sufficient
- In a home network, the router usually also acts as firewall
- Proper placing is crucial for company network

Even simple company network has:

- An **internal network** with PCs, servers, printers, etc.
- Mail server, web-server, VPN gateway, etc.
- The **internal network** should not be directly accessible.
- Web server or mail server needs to be accessible.

Solution – **Demilitarized Zone** – DMZ

Create a zone that is considered less secure than the **internal network**, but still protected from outside access.



Examples of filtering

1. Prevent malicious software to send out data
2. Block IP spoofing
   (technique used by attackers to impersonate another machine by manipulating IP packet header with a ‘spoofed’ source IP address.
3. Block outbound traffic from critical network areas or computers
4. Only allow outbound HTTP traffic through a proxy
5. Logging of denied outbound traffic
6. Denied outbound traffic can help to detect infections,
   Any outbound connections that are not Web traffic would trigger a "deny" alert.

Network address translation (NAT) – a method of remapping one IP address space into another by modifying network address information in the IP packets of packets during transmission.

Proxies and NAT:

Firewalls also provide

- Network and port-address translation (NAT).
  Internal network uses internal IP addresses not visible to the outside
- Proxies (e.g. for HTTP) can hide individual devices in the internal network

Not direct security functionalities but hide some information from outside attackers.

Why firewalls are not enough

More and more applications connect internal networks to the internet:

- Social networks
- Remote access (TeamViewer)
- Unified messaging (Skype, WeChat)
- Collaboration tools (Googles Docs, OneNote, OneDrive, iCloud)

More difficulties

- Port hopping: Applications change their ports during a session
- Hiding in TPS encryption: TLS can mask application traffic
- Applications use non-standard ports
- Tunnel in other services: e.g. P2P file-sharing or messengers running over HTTP

Perimeter security has obvious constraints

- Firewalls don't help against internal attackers
- Once an attack was successful, firewalls cannot help
- Internet of things, mobile networks, etc.

Skype
Microsoft Office 365
Tor
YouTube
Salesforce
Zoho
Gmail
web browser
GoToMyPC
Google Apps
Box
Facebook
Oracle CRM

Intrusion Detection System (IDS)

- Monitors networks and/or system activities
- Alert when potentially malicious activity is found
- Logs information about activities

Intrusion Prevention System (IPS)

- IDS with additional active functionality
- Attempts to block or stop malicious activities

Monitoring actions (examples)

- Detect port scans
- Detect OS fingerprinting attempts (attacker analyzes protocols, data packets to attempt to detect what OS the device is on)
- Look for specific attacks (e.g. buffer overflow)
- Find and block known malware
- Detect server message block (SMB) probes (exploit to protocol that provide shared access files, printers, serial ports)
- Find anomalies

Reaction actions (examples)

- Drop malicious packets and send alarm
- Block traffic from some IP addresses
- Correct fragmentation in packet streams
- Raise alerts – trigger human intervention/incident response teams

2 types of detections – IDS/IPS should have both

- Signature-based – fast, generate less false positives, and do not need learning phase.
- Anomaly-based – can detect unknown attacks

Next-Generation Firewalls (NGF)

- Promise of an integrated security approach
- Proxy for all traffic (even encrypted)
- Look at everything (applications, logical segments, roles, services, users)

Potential NGF problems

- Policy rules too complex
- Proxy for TLS breaks end-to-end security
- Encapsulated encryption still possible
- Privacy issues
- Single point of attack with full access to decrypted data

Virus Scanner – Anti-virus Software

- Can efficiently prevent infections with known malware.
- Is the first thing to be manipulated by malware
- Unable to detect new malware