

Cybersecurity: Technology and Governance

Audun Jøsang
1st edition 2024
Springer Nature



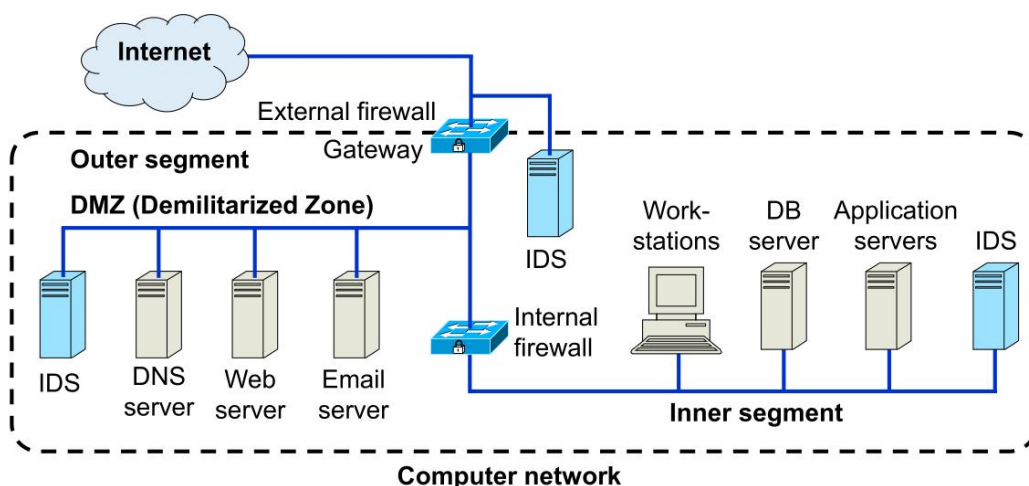
Exercises

Chapter 6: Network Security

Task 1: Security Protocols

- What is a security protocol, and what can it be used for?
- Provide examples of security functions/services that are supported by security protocols.
- Name at least four well-known security protocols.
- At which layers of the Internet stack (and OSI stack) do TLS and IPsec operate? Why is a port number reserved for HTTPS (HTTP with TLS) but not for IPsec?

Task 2: Firewalls



Look at the figure above that shows a simple network architecture with firewalls.

- What is the purpose of DMZ? What services are typically available there?
- How are internal network segments protected from attacks from the internet via DMZs?
- At which layers of the internet stack (and the OSI stack) does a packet filter firewall operate?
- What type of firewall can filter traffic based on user data in data packets?

Task 3: TLS Inspection

- Describe legitimate reasons for using TLS inspection.
- Describe TLS inspection abuse threat scenarios.
- How can a user tell if TLS inspection is being used in an HTTPS web connection?

Task 4: Forward secrecy

- a) What is meant by forward secrecy?
- b) How is forward secrecy achieved?
- c) Name a key establishment security protocol that supports "forward secrecy" (sometimes called "perfect forward secrecy")?
- d) Name a security protocol that **didn't** support forward secrecy. Say why not (i.e., how it establishes session keys)

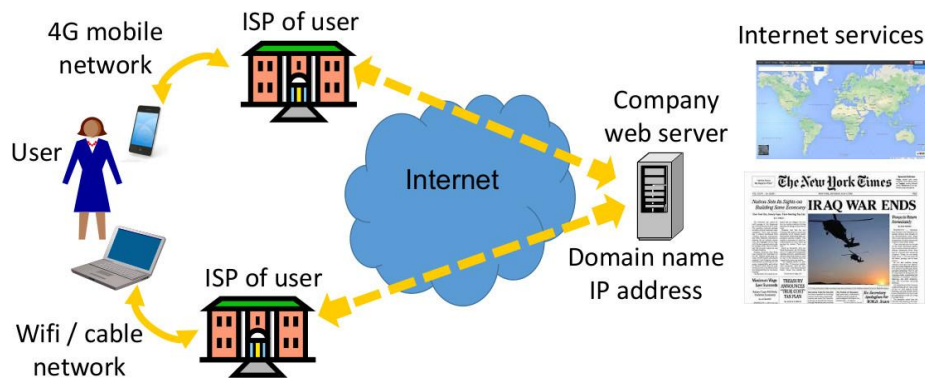
Task 5: TLS

TLS is a security protocol used on the Internet, but TLS is actually made up of several separate sub-protocols. The latest version is TLS 1.3 from 2018.

- a) What IP port is reserved for http over TLS? What URL prefix indicates that an application is using http over TLS?
- b) Briefly describe where in the OSI and TCP/IP protocol layers TLS operates.
- c) Briefly explain the purpose of the TLS Handshake protocol.
- d) Name the security services that the TLS Record protocol supports in a TLS connection.
- e) How are the TLS Handshake Protocol and TLS Record Protocol related?

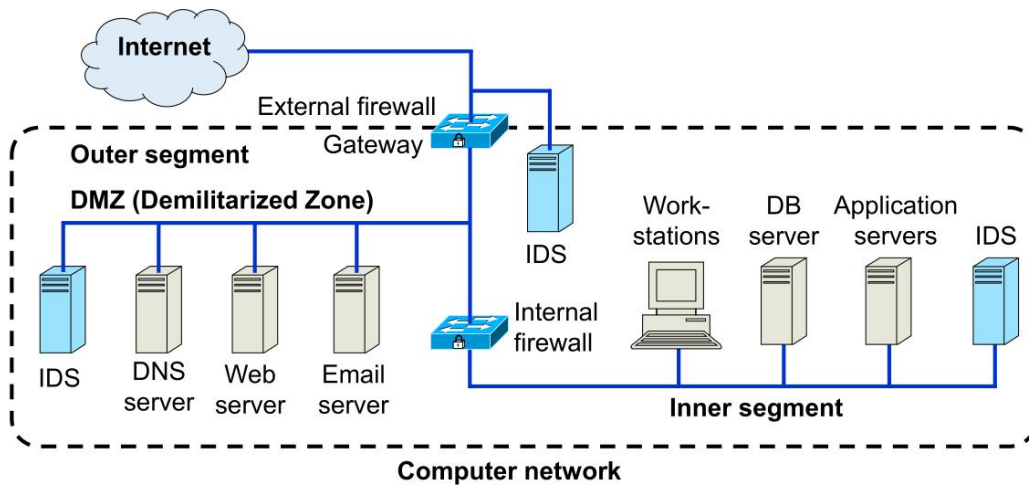
Task 6: VPN

The user's ISP (Internet Service Provider) can normally see the domain name/IP address of the web server that the user is accessing, as illustrated in the figure below. This can be a privacy issue if users don't want any third party to see their internet activity.



- a) When using a cloud VPN, what traffic data is hidden from the user's ISP?
- b) When using a cloud VPN, what traffic data can the VPN provider obtain?
- c) When using Tor, what traffic data is hidden from the user's ISP?
- d) When using Tor, what traffic data can the Tor access server see?
- e) How can you prevent your ISP from knowing you're using Tor?

Task 7: Packet Filter and Intrusion Detection



With regard to the figure above.

- What is a typical secure configuration (filter rules) for the firewalls?
- What are natural locations for NIDS's ? Explain why.
- What is the purpose of placing an IDS outside the gateway, when most of the attack traffic is filtered out in the gateway/outer firewall anyway?