Ataki na systemy komputerowe

cz. 1. Sieci komputerowe

Czyli na co?

- Urządzenia końcowe – PC, urządzenia mobilne, urządzenia IoT
- Serwery – DNS (serwery nazw domen), bazy danych
- Pozostałe urządzenia infrastruktury sieciowej – rutery, centrale, przełączniki itp.,
- Systemy – SCADA (sieci przemysłowe), systemy krytyczne (zarządzające infrastrukturą krytyczną)

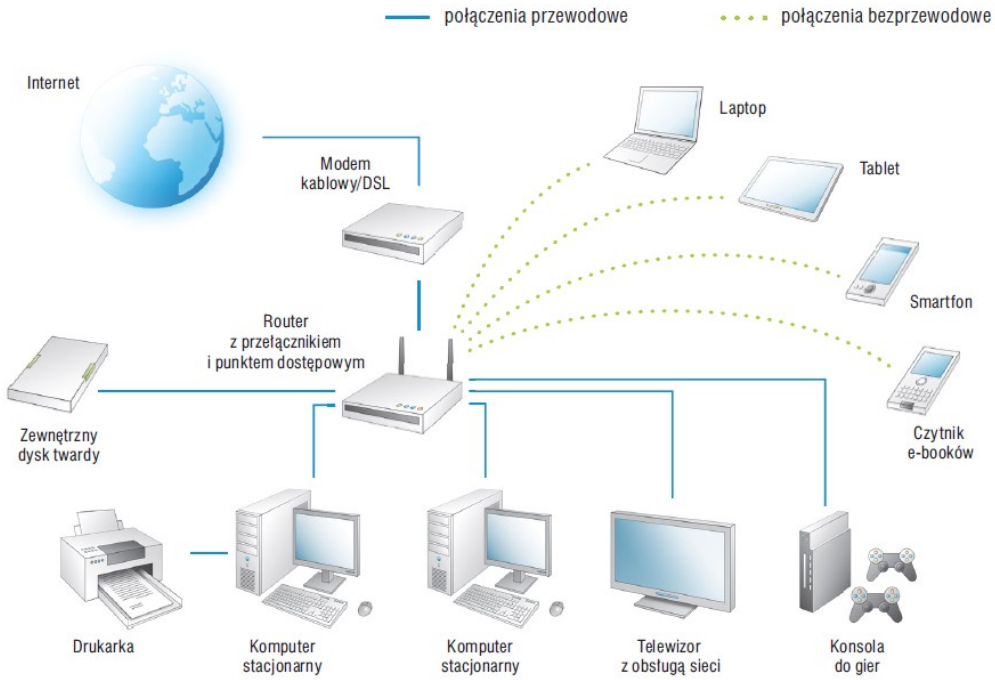
LAN, Wi-Fi

LAN – Local Area Network

Wi-Fi - Wireless Fidelity

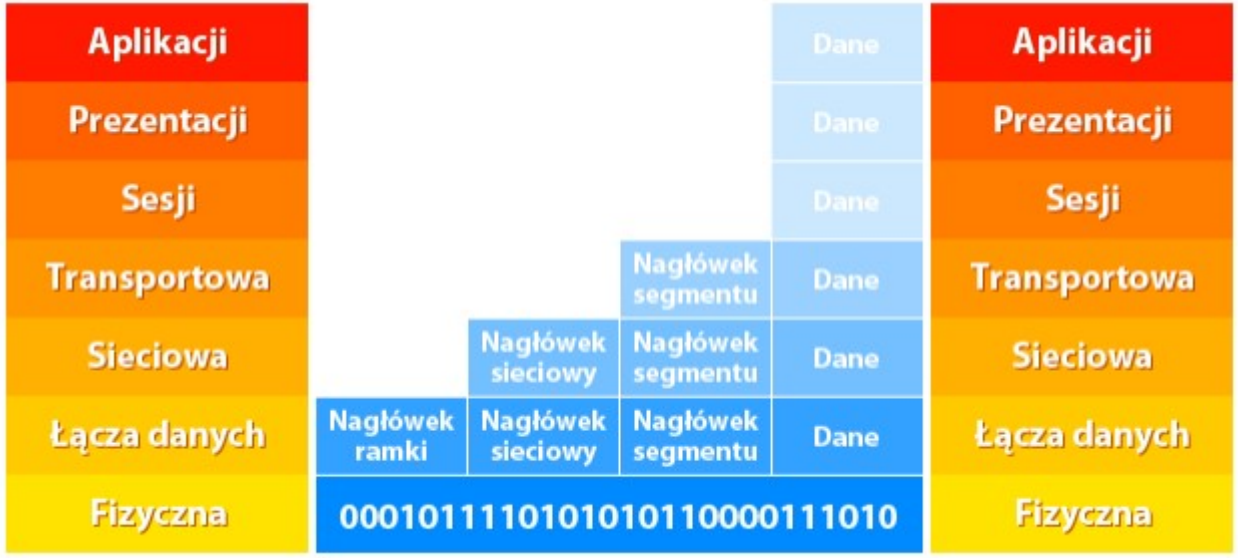
LAN, Wi-Fi

LAN – Local Area Network



LAN, Wi-Fi

Model OSI



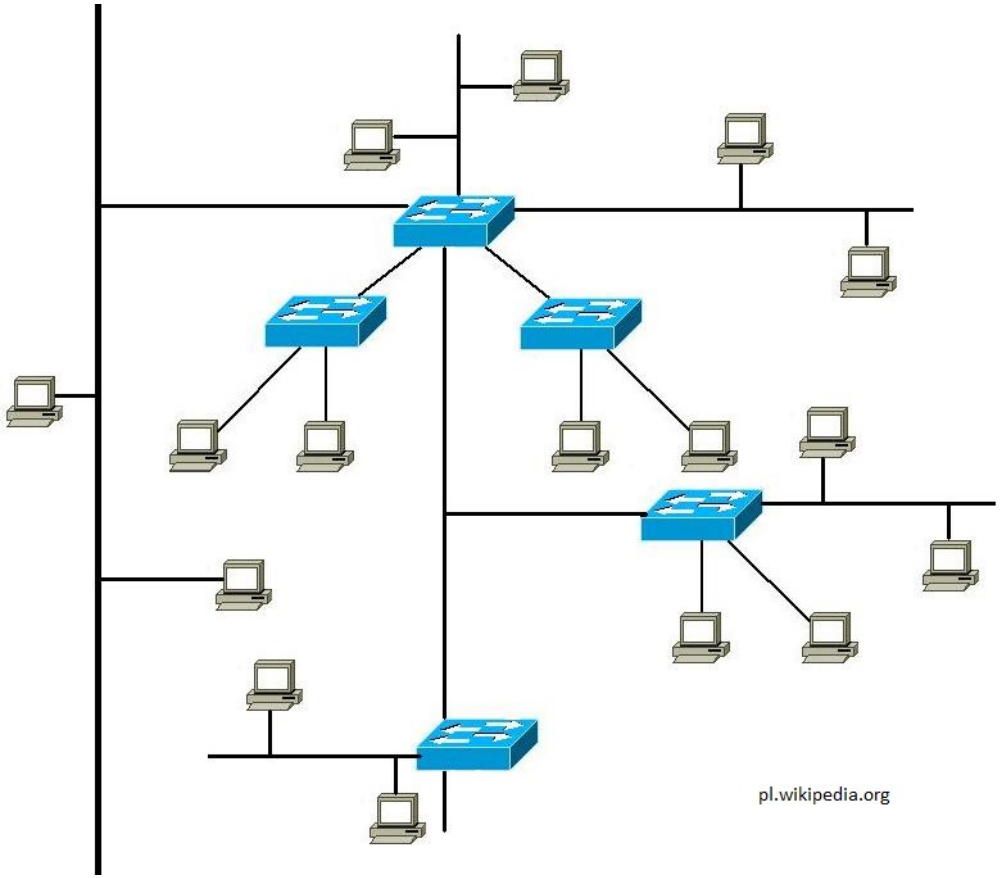
LAN, Wi-Fi

LAN:

- huby

- switche

Switche w trybie podstawowym
nie wypuszczają ruchu
na inne porty gałęzi

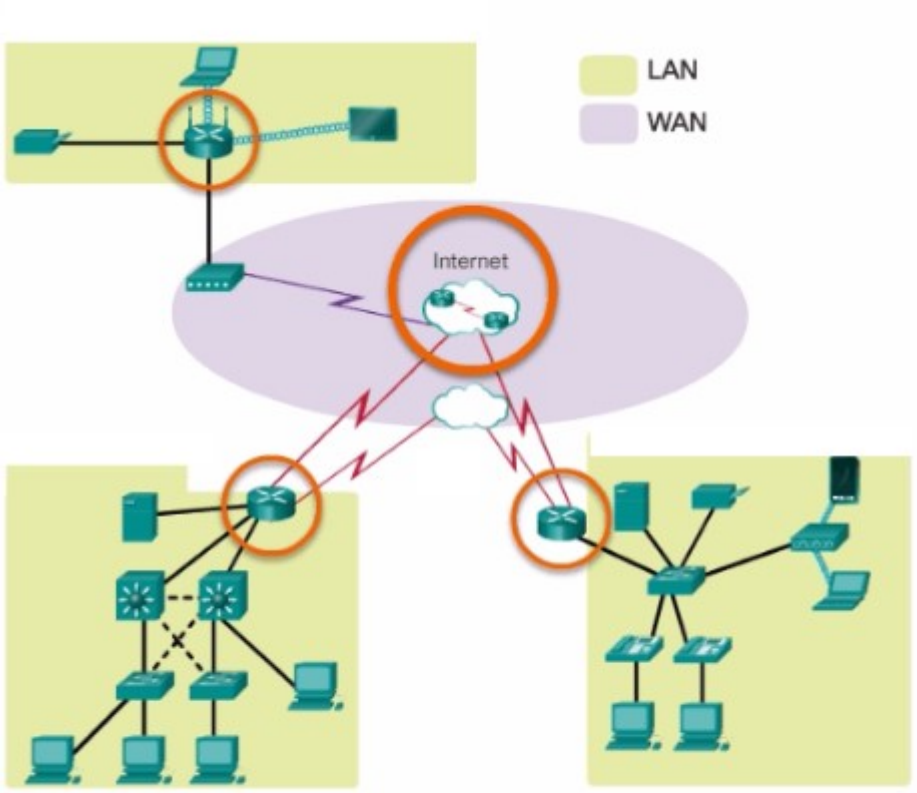


LAN, Wi-Fi

Stosowane metody zabezpieczeń zgodne ze standardem 802.11:

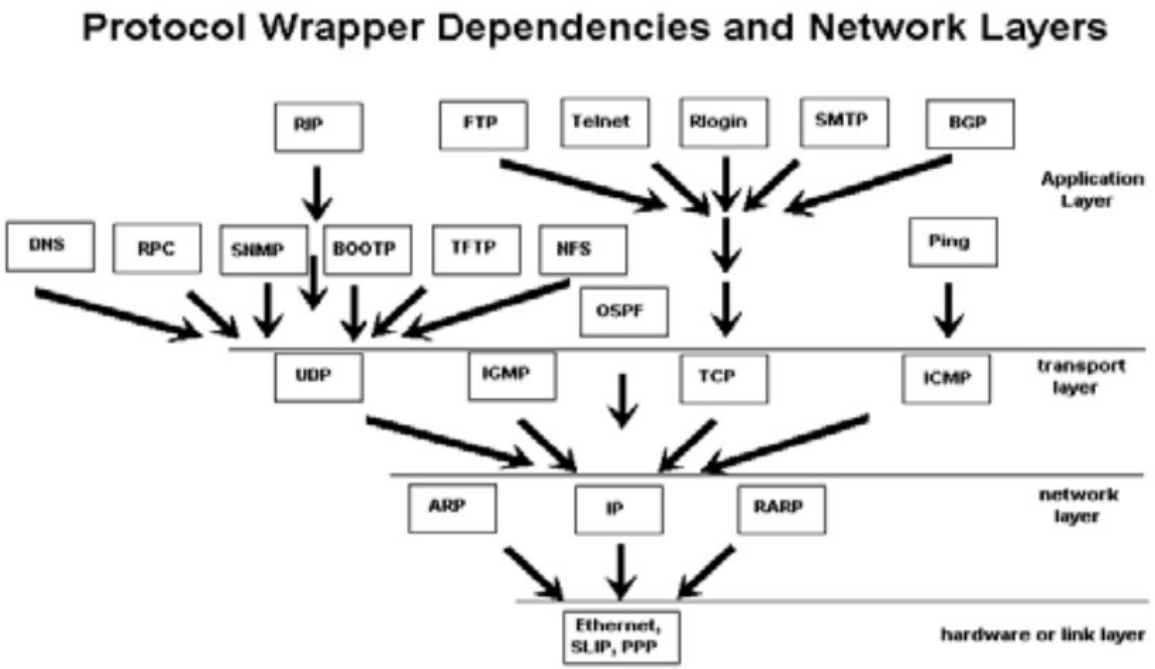
- uwierzytelnianie – identyfikacja i weryfikacja autentyczności informacji przesyłanych przez użytkownika, który łączy się z siecią (IEEE 802.1X)
- protokół WEP (ang. *Wired Equivalent Privacy*) – działa na zasadzie współdzielonego klucza szyfrującego o długości 40 do 104 bitów i 24-bitowym wektorze inicjującym. WEP jest aktualnie bardzo złym zabezpieczeniem, które nie chroni nas przed włamaniami z zewnątrz. W średnio obciążonej sieci klucze WEP można złamać w 90% przypadków, poniżej 1 godziny pasywnego nasłuchiwania pakietów.
- protokoły WPA/WPA2 – nowe, dużo bardziej bezpieczne mechanizmy szyfrowania przesyłanych danych
- autoryzacja – zgoda lub brak zgody na żądaną usługę przez uwierzytelnionego użytkownika. Zabezpieczenie to jest wykonane przez punkt dostępu lub serwer dostępu.
- rejestracja raportów – rejestr akcji użytkownika związanych z dostępem do sieci. Kontrola raportów pozwala na szybką reakcję administratorów na niepokojące zdarzenia w sieci.

WAN



[https://ccnacompletecourse.blogspot.com/2019/09/basic-initial-cisco-router.html]

Protokoły



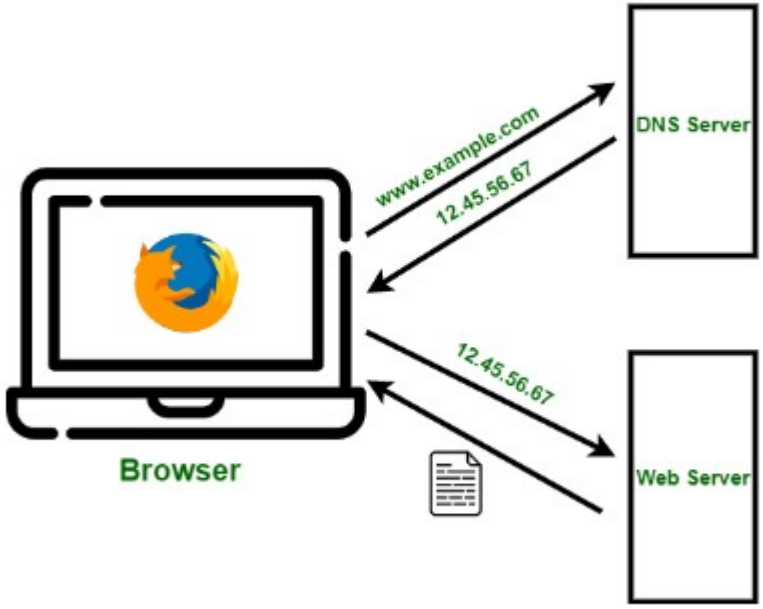
Components and means of communication within the Local Area Network: An analytical study
Yaser Mohammed Mohammed Al Sawy

Protokoły sieciowe

ARP
IP
TCP
UDP
ICMP
DNS
FTP
Telnet(22)
SSH (23)
HTTP(80)
HTTPS(443)
SSL/TLS
IPSec

Bold – protokoły zabezpieczone/zabezpieczające

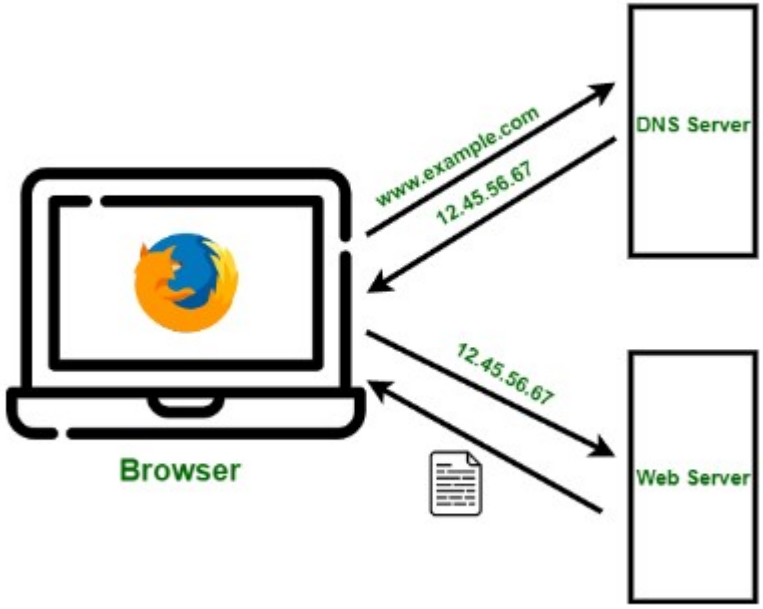
DNS



https://www.geeksforgeeks.org/working-of-domain-name-system-dns-server/

DNS

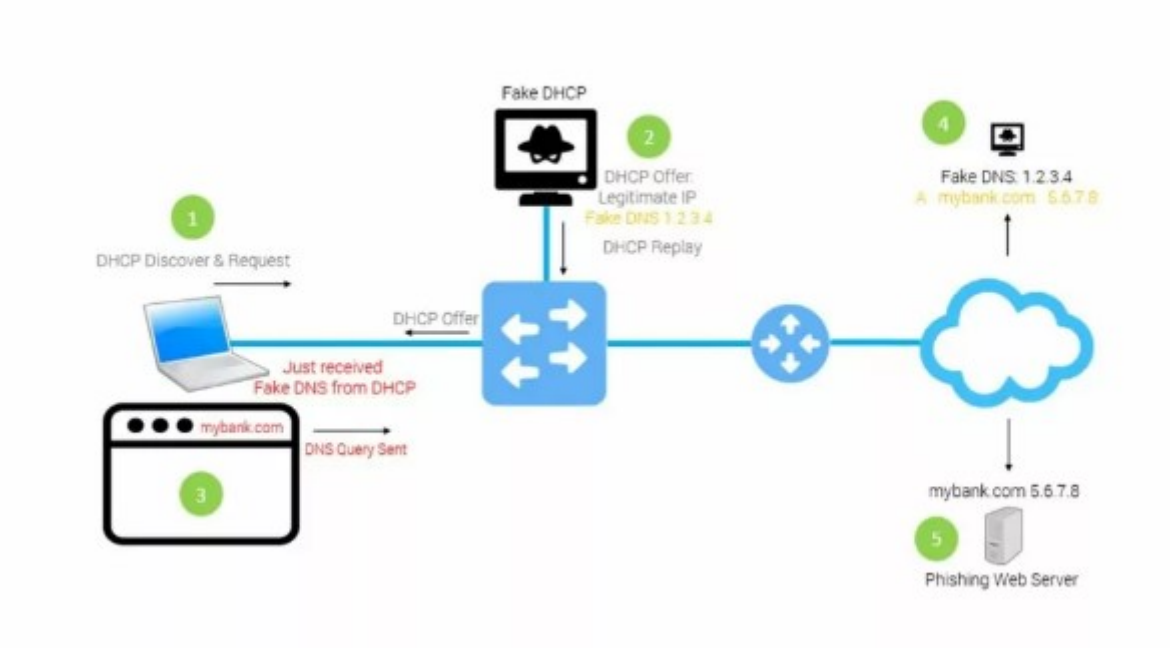
Jest też urządzeniem, które może blokować serwisy!!!



https://www.geeksforgeeks.org/working-of-domain-name-system-dns-server/

DNS (MITM)

[https://www.grandmetric.com/pl/bezpieczenstwo-sieci-lan/]

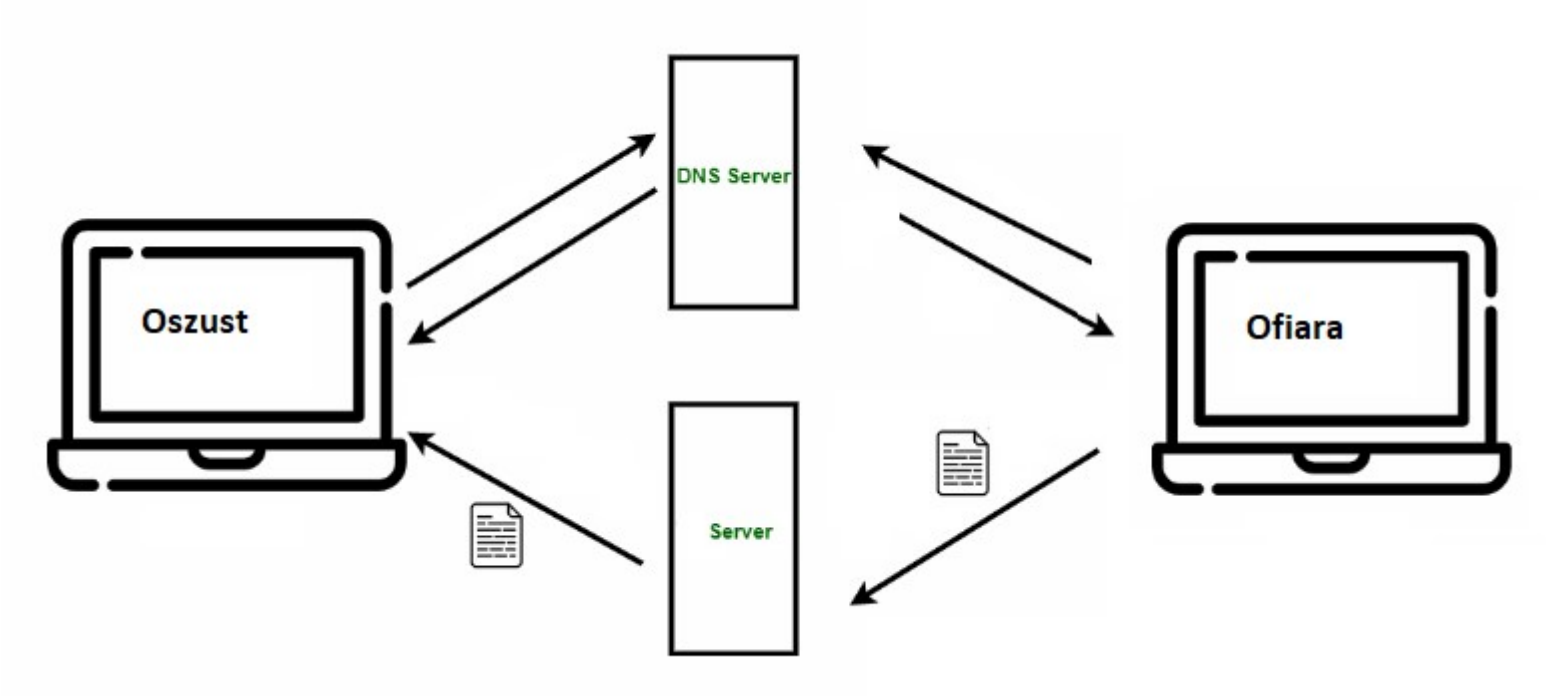


DNS

- **DNS over TLS (DoT): Jest to sposób na enkapsulację komunikacji DNS w warstwie transportowej TLS (Transport Layer Security), co zapewnia poufność i integralność danych. DoT używa standardowego portu TCP 853.**

- **DNS over HTTPS (DoH): Jest to alternatywny sposób na przekazywanie zapytań DNS przez protokół HTTP w celu wykorzystania jego szyfrowania za pośrednictwem warstwy aplikacji. DoH używa standardowego portu TCP 443, czyli portu HTTPS.**

DNS - komunikacja



Firewall

Podstawowe zadania firewalla obejmują:

- **Filtrowanie ruchu sieciowego: Firewall może analizować ruch sieciowy na podstawie określonych reguł i decydować, czy przepuścić czy zablokować pakiety na podstawie różnych kryteriów, takich jak adres IP, port, protokół, itp.**
- **Ochrona przed atakami z zewnątrz: Firewall może blokować próby nieautoryzowanego dostępu do sieci, takie jak ataki typu brute-force na porty usług, próby wykorzystania luk w zabezpieczeniach, itp.**
- **Kontrola dostępu: Firewall może kontrolować, które aplikacje i usługi sieciowe mogą uzyskać dostęp do sieci oraz które zasoby sieciowe mogą być dostępne z zewnątrz.**
- **Monitorowanie ruchu sieciowego: Firewall może rejestrować ruch sieciowy w celu analizy zdarzeń, wykrywania anomalii oraz zapewnienia zgodności z politykami bezpieczeństwa.**
- **Przekierowywanie ruchu sieciowego: Firewall może przekierowywać ruch sieciowy na podstawie określonych reguł, np. przekierowywanie ruchu na serwery wewnętrzne.**
- **Szyfrowanie i deszyfrowanie ruchu: Niektóre zaawansowane firewalle mogą obsługiwać funkcje szyfrowania i deszyfrowania ruchu, np. w przypadku protokołu SSL/TLS, w celu analizy ruchu zaszyfrowanego.**
- **Zdalne połączenia bezpieczne: Niektóre firewalle umożliwiają tworzenie tuneli VPN (Virtual Private Network), zapewniając bezpieczne i prywatne połączenia zdalne do sieci firmowej.**

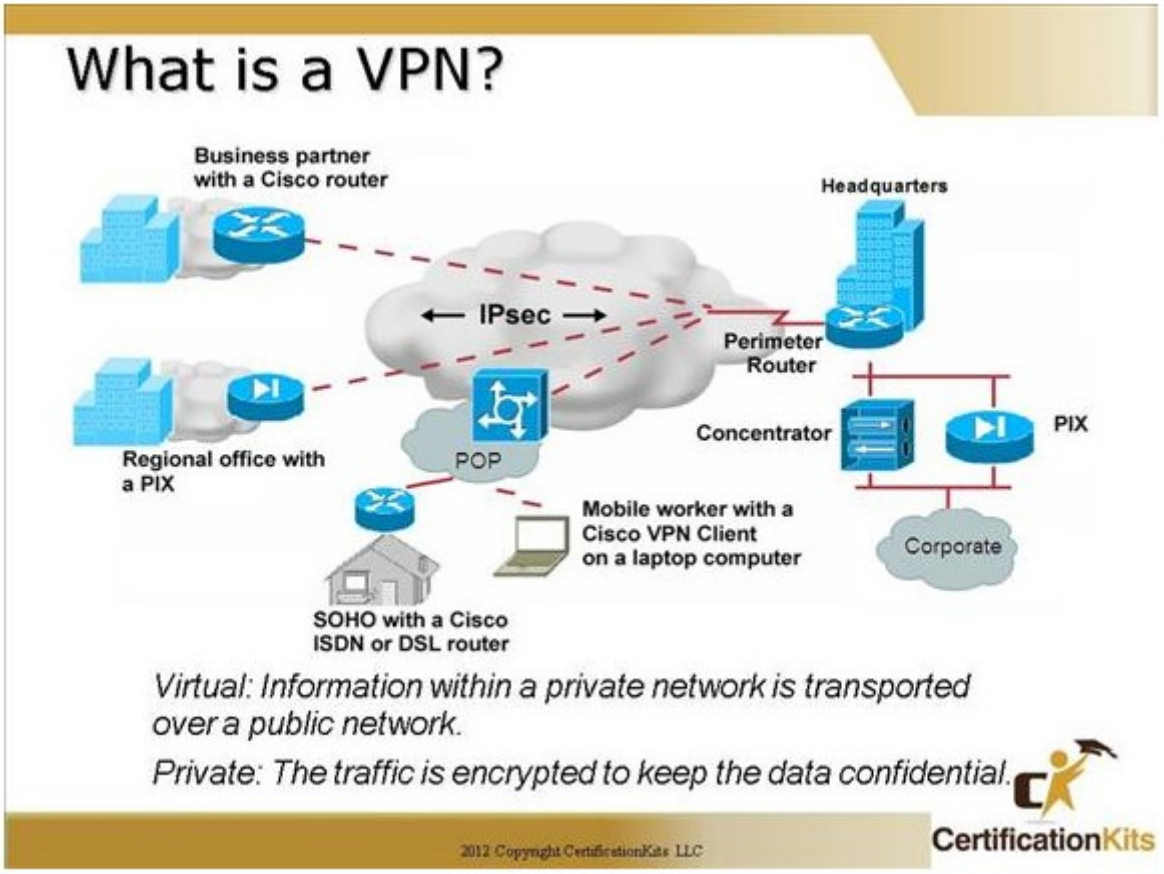
Proxy serwer/Web proxy

Communication without proxy server

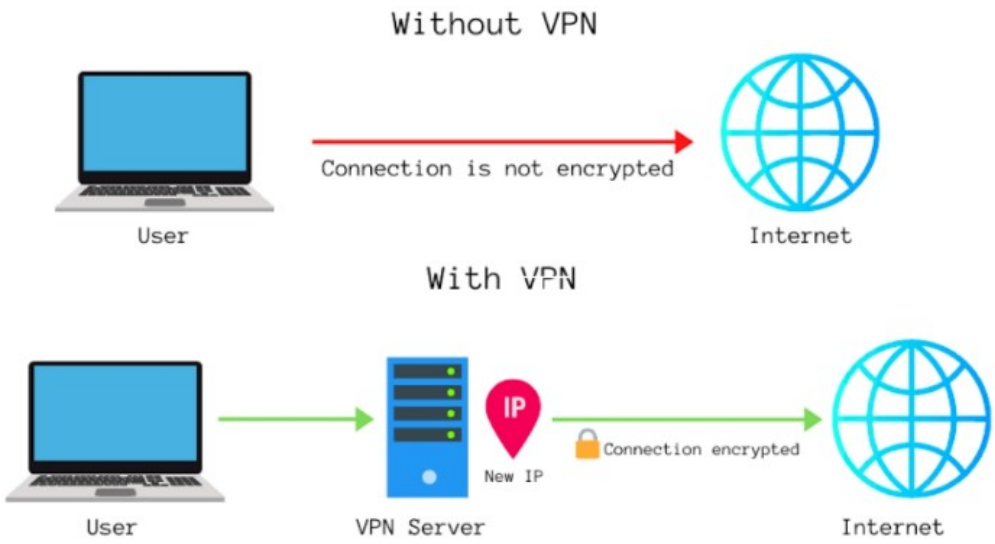
Communication with proxy server

[https://www.javatpoint.com/what-is-a-proxy-server-and-how-does-it-work]

VPN – rozwiązanie dla korpo



Web VPN

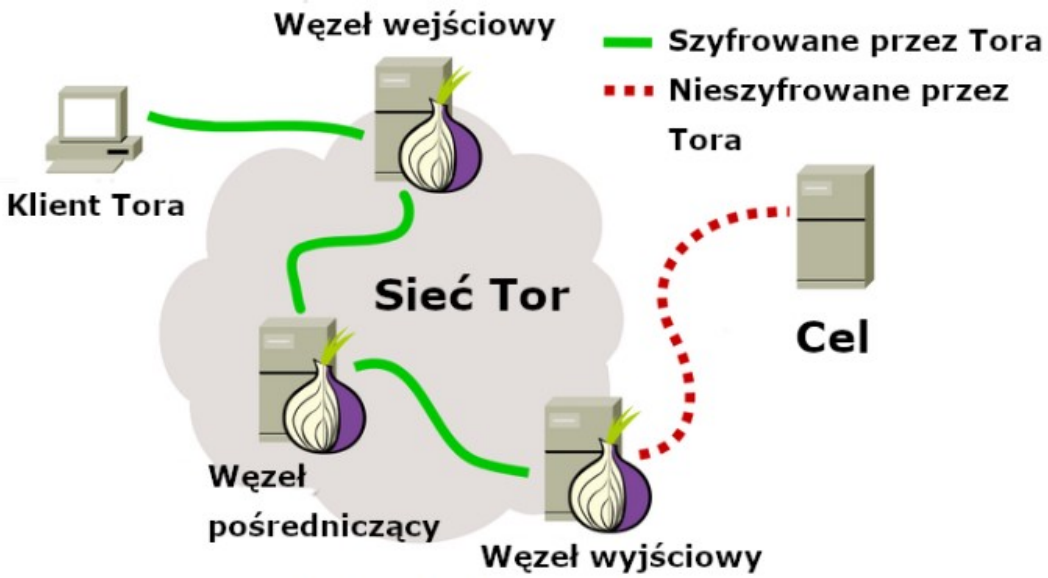


[https://www.cyberyodha.org/2023/02/what-is-virtual-private-networkvpn.html]

Deep Web i Dark Web

[https://surfshark.com/pl/blog/deep-web-vs-dark-web] Deep web, czyli „głęboka sieć”, obejmuje wszystkie strony internetowe, które nie są indeksowane przez wyszukiwarki (czyli przez Google), i które są zazwyczaj używane jako zaplecze techniczne. Dark web, czyli „ciemna sieć”, to specjalnie ukryta część deep webu, do której możesz się dostać tylko ze specjalnej przeglądarki

Dark Web



https://bezpiecznyblog.pl/tor-podstawy/

KONIEC