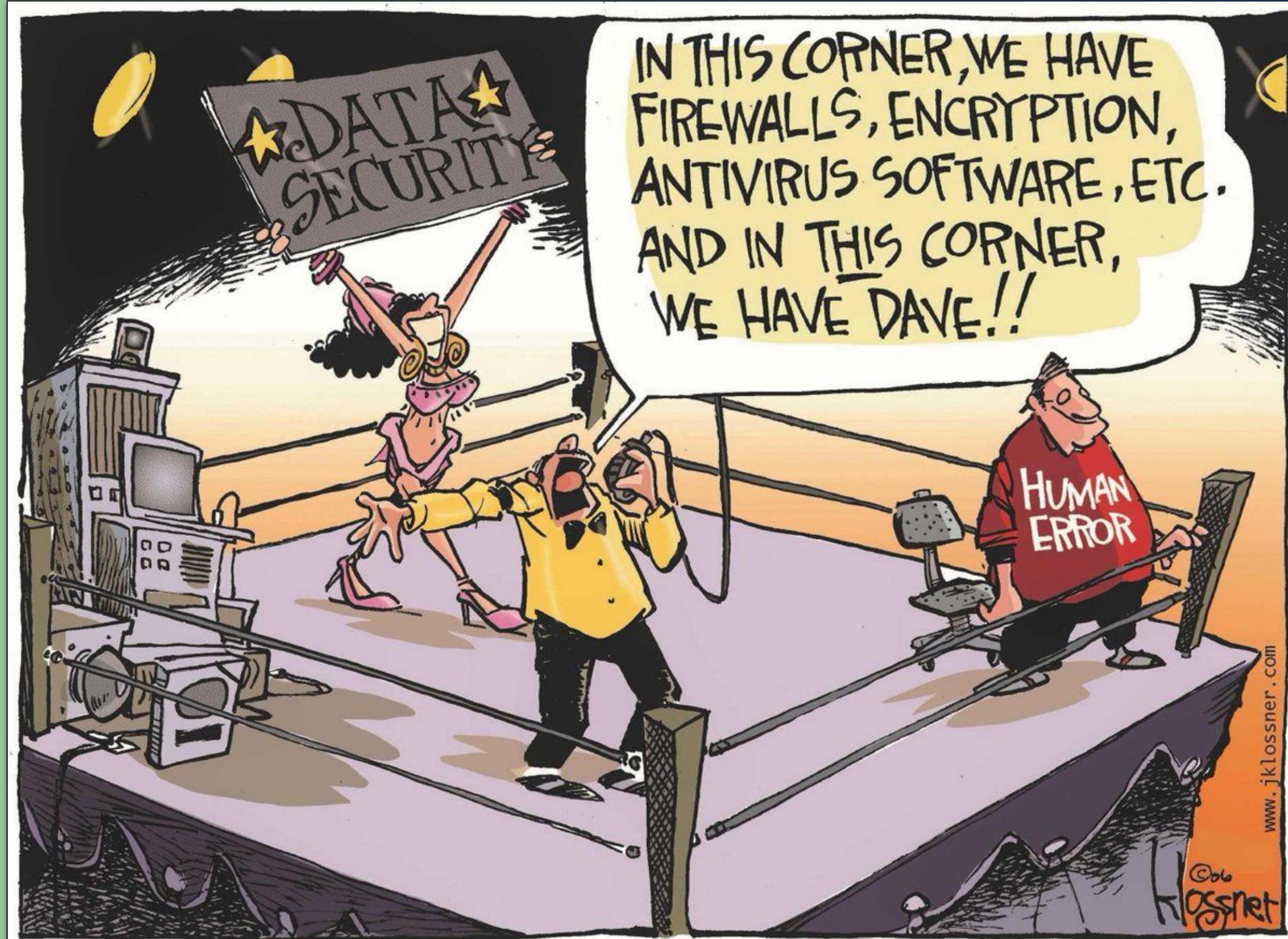


# „IPS/IDS, Ogniomurek i inne technologie”

W tematyce zabezpieczania sieci

.NET Group, Akademia Cybersecurity #2 @ZUT



Bezpieczeństwo nie jest łatwe...

- Firewall - od początku do obecnych rozwiązań
- Popularne ataki sieciowe
- Odpowiedź na zagrożenia w czasie rzeczywistym - systemy IPS/IDS
- Propozycja zintegrowania metod bezpieczeństwa - ASA
- Inne technologie warte uwagi
- Bezpieczeństwo ucieka w chmurę. SaaS

Rozkład jazdy

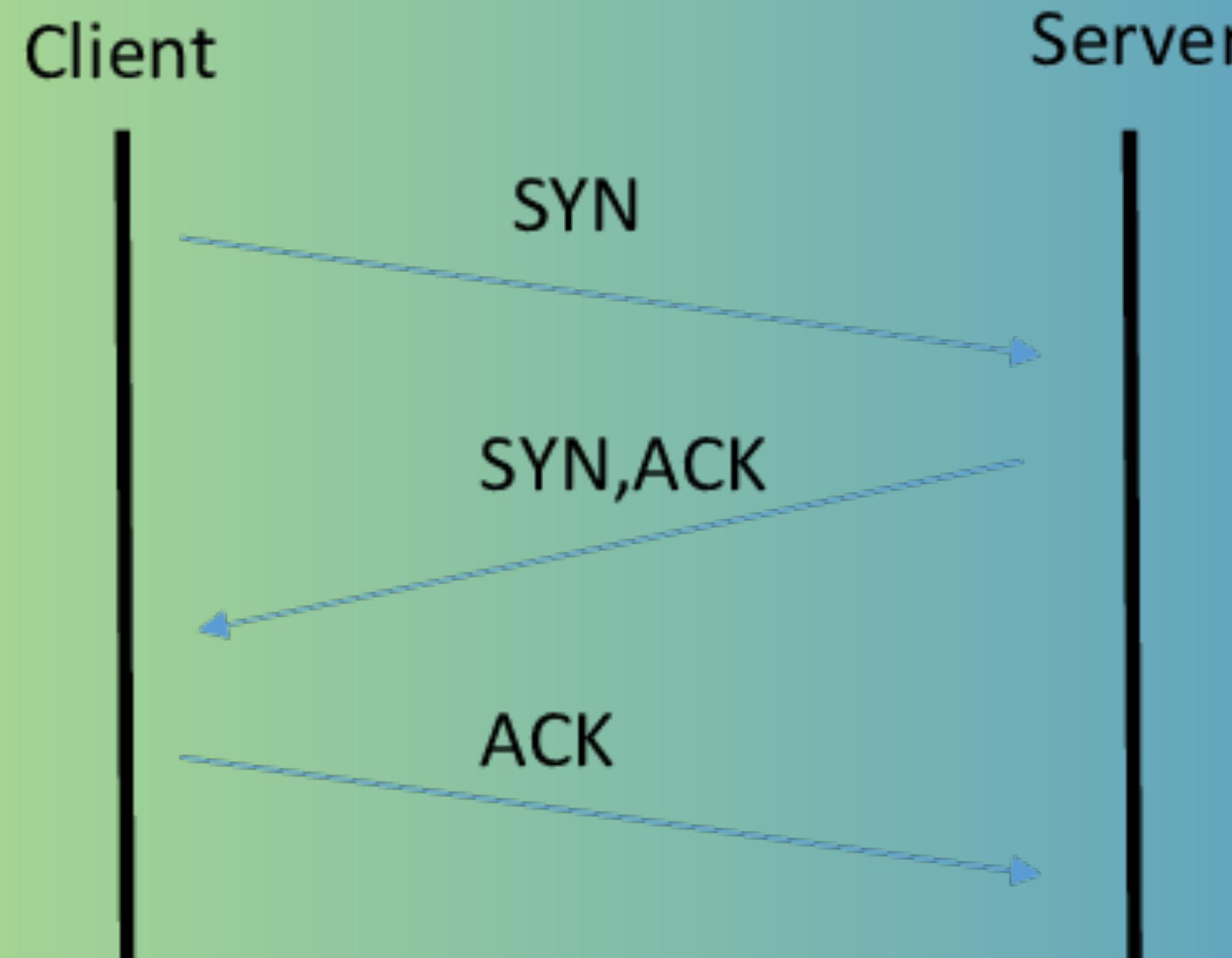
- 7 warstw modelu TCP/IP
- Enkapsulacja / Dekapsulacja
- Różnorodność protokołów
- Liczba i rodzaj urządzeń podłączonych do sieci

” Each implementation must expect to interoperate with others created by different individuals. (...) In general, an implementation should be conservative in its sending behavior, and liberal in its receiving behavior. That is, it should be careful to send well-formed datagrams, but should accept any datagram that it can interpret(...) ”

– RFC 760 – Department of Defense Standard Internet Protocol,  
January 1980

# Firewall

- Pomysł - filtrowanie pojedynczych pakietów
- Interesuje nas użyty protokół, zazwyczaj warstwy > 5
- Sprawdzamy adres źródłowy, port, protokół etc.



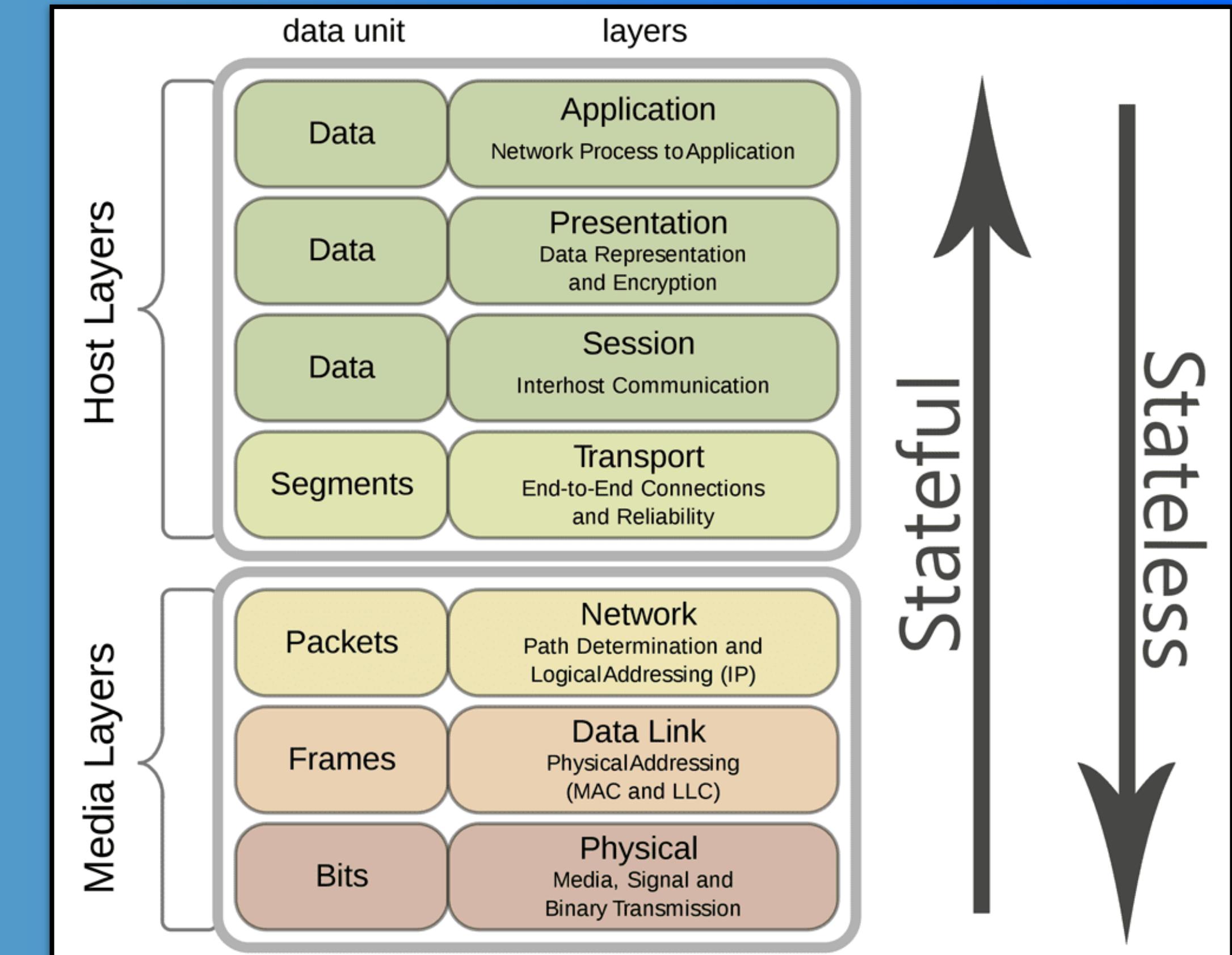
```
#> iptables -A INPUT -i eth0  
-p tcp --dport 80 -j ACCEPT  
  
#> iptables -A OUTPUT -o eth0  
-p tcp --sport 80 -j ACCEPT
```

# Firewall - filtrowanie pakietów

- Problem - kto zaczął komunikację?
- Śledzenie stanu połączenia (Context aware)

```
#> iptables -A INPUT -i eth0
-p tcp --dport 80 -m state --
state NEW,ESTABLISHED -j
ACCEPT

#> iptables -A OUTPUT -o eth0
-p tcp --sport 80 -m state --
state ESTABLISHED -j ACCEPT
```



Firewall - „Stateful firewall”

# Stateful

- Mniej wydajne, obciążają komunikację
- Blokują nieautoryzowane wyjście z sieci
- Podatne na przeciążenie sieci (ataki typu DoS)

# Packet Filtering

- Proste, wydajne
- „Drop all” blokuje większość prób ataków
- Podatne na złożone (composite) ataki (wiele pakietów)
- Firewall typu Circuit Level - jeszcze lepsza wydajność, brak inspekcji zawartości ruchu

Porównanie

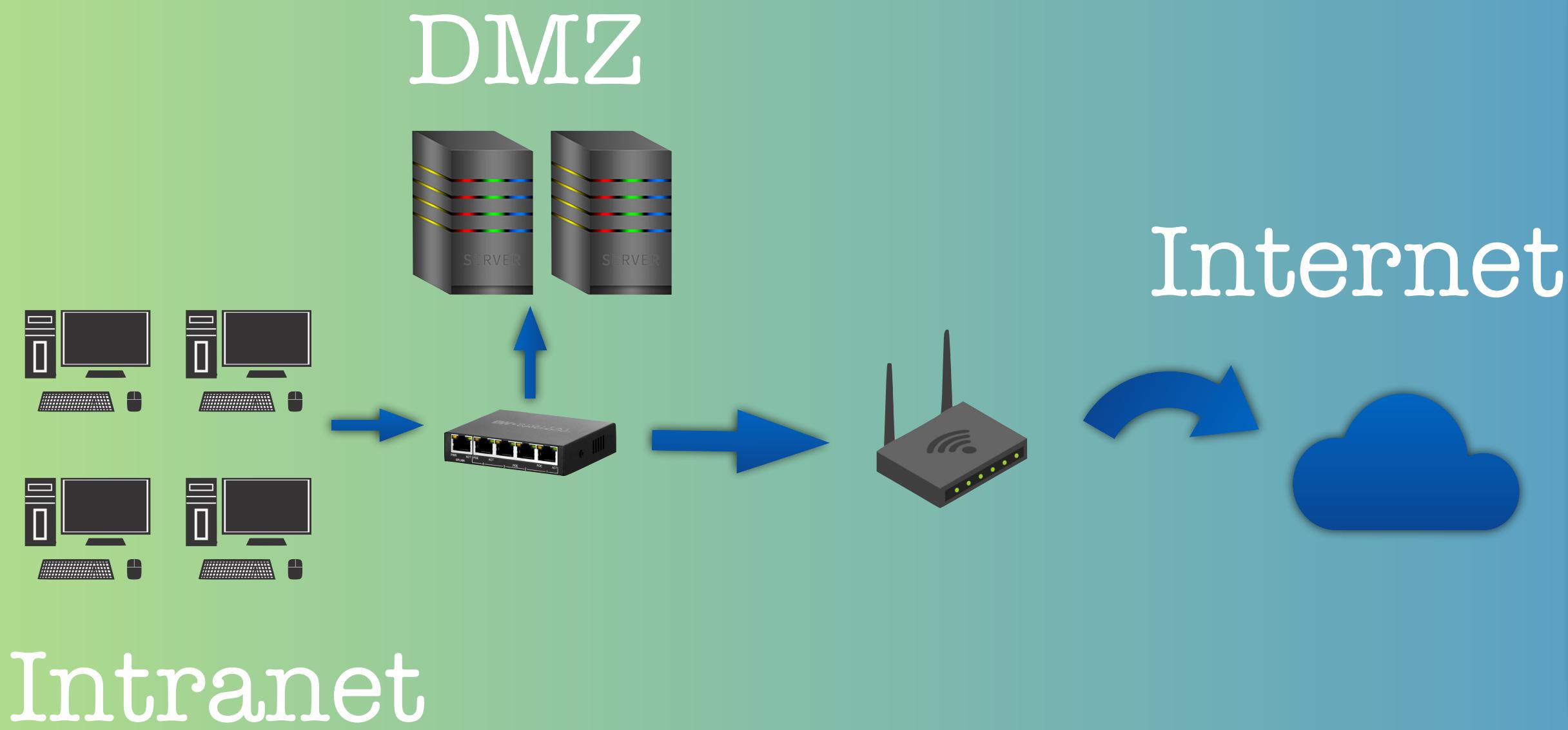
- Analiza wyższych warstw (głównie protokół HTTP)
- Rozwiążanie dedykowane do aplikacji webowych
- Zapobiega atakom na użytkownika
- Dodatkowe, np. reputacje stron internetowych



- Potencjalne wektory ataku:
- Code (i.e. SQL) Injection
- XSS
- Path traversal
- Document ID enumeration
- Znane błędy i exploity

# WAF - Web Application Firewall

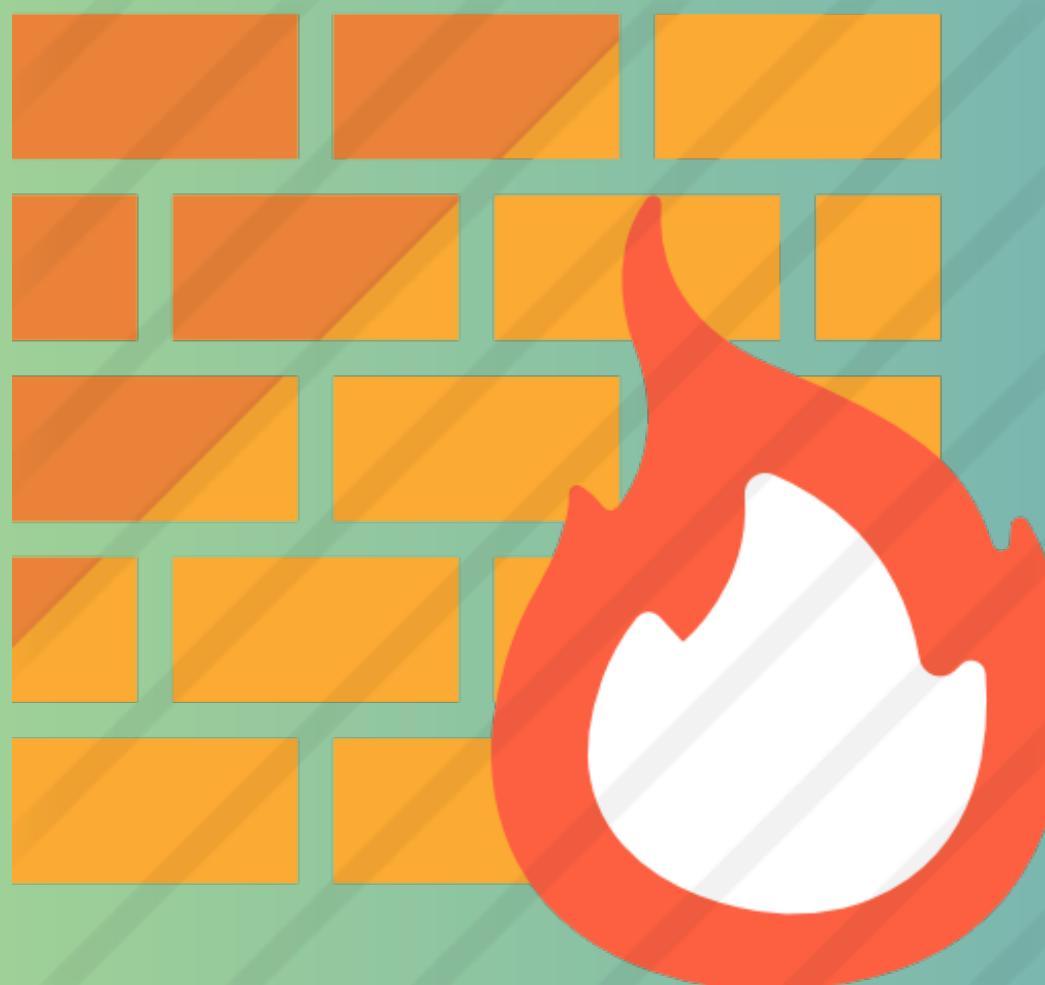
- Definiują pojęcie tzw. Stref - przypisanych do konkretnych portów urządzenia
- Każda komunikacja z konkretnej strefy, do konkretnej strefy posiada zestął zdefiniowanych reguł (policy)
- Przydatne w przypadku bardziej złożonej sieci (korporacje, instytucje finansowe etc.)



```
#> zone security INSIDE  
#> zone security INTERNET  
#> class-map (...)  
#> policy-map (...)  
#> zone pair (...)
```

# ZPF - Zone Policy Firewall

- Brak jednej spójnej definicji
- Zawierają w sobie elementy wszystkich z wcześniej wymienionych rozwiązań w jednej kompleksowej formie
- Wsparcie bezpieczeństwa mechanizmami AAA oraz ACL
- Często w implementacji znajdują się także mechanizmy IPS (Spoiler alert!)

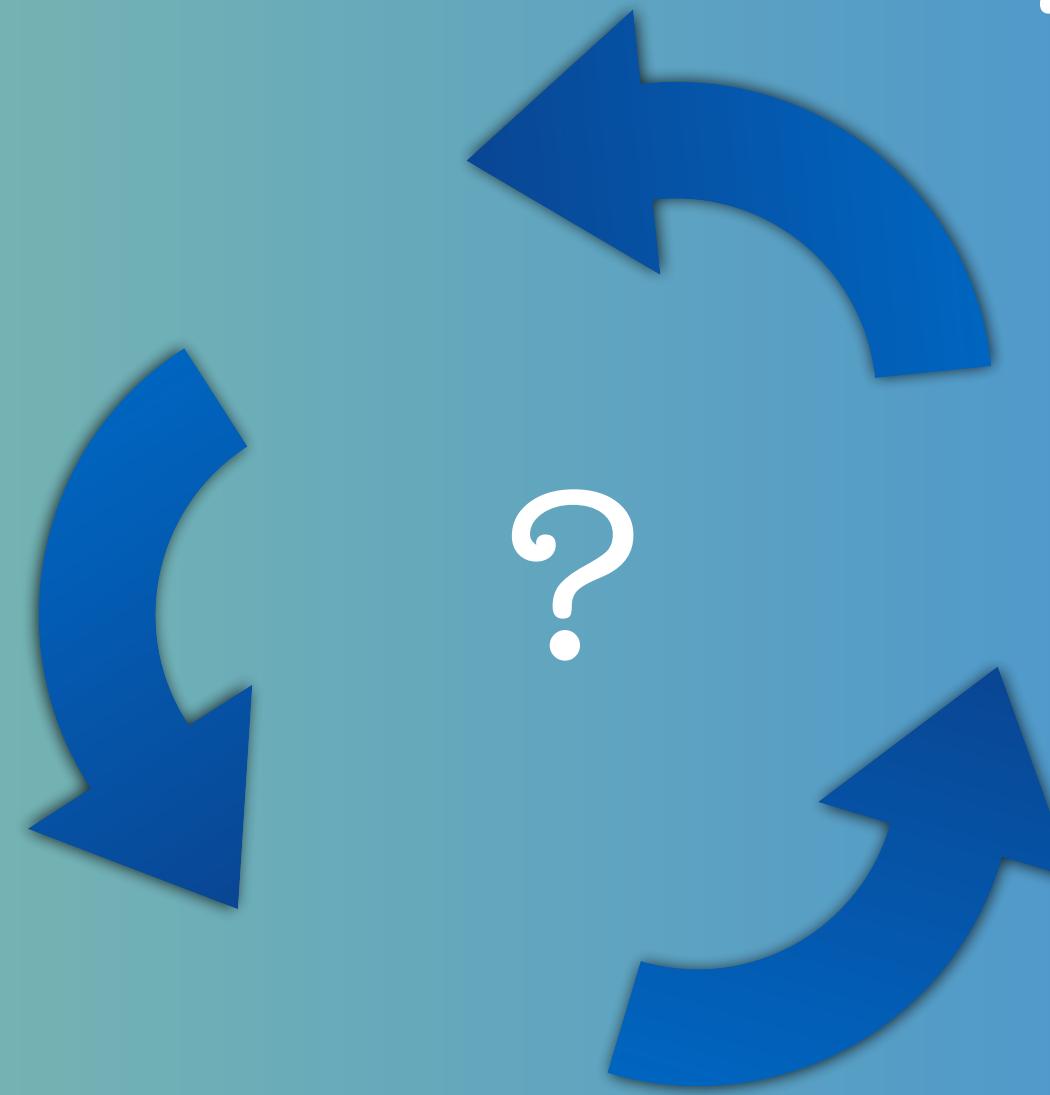
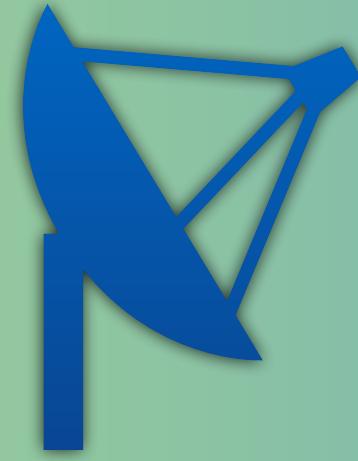


”Stateful firewalls and next-gen firewalls provide better log information than a packet filtering firewall. Both defend against spoofing and both filter unwanted traffic. Pros of next gen firewalls are: (...) website filtering based on site reputation, proactive protection, enforcement of security policies masked on multiple criteria, improved performance with NAT, VPN, stateful inspections, integrated IPS”

~Cisco

# Next Generation Firewalls

Hardware

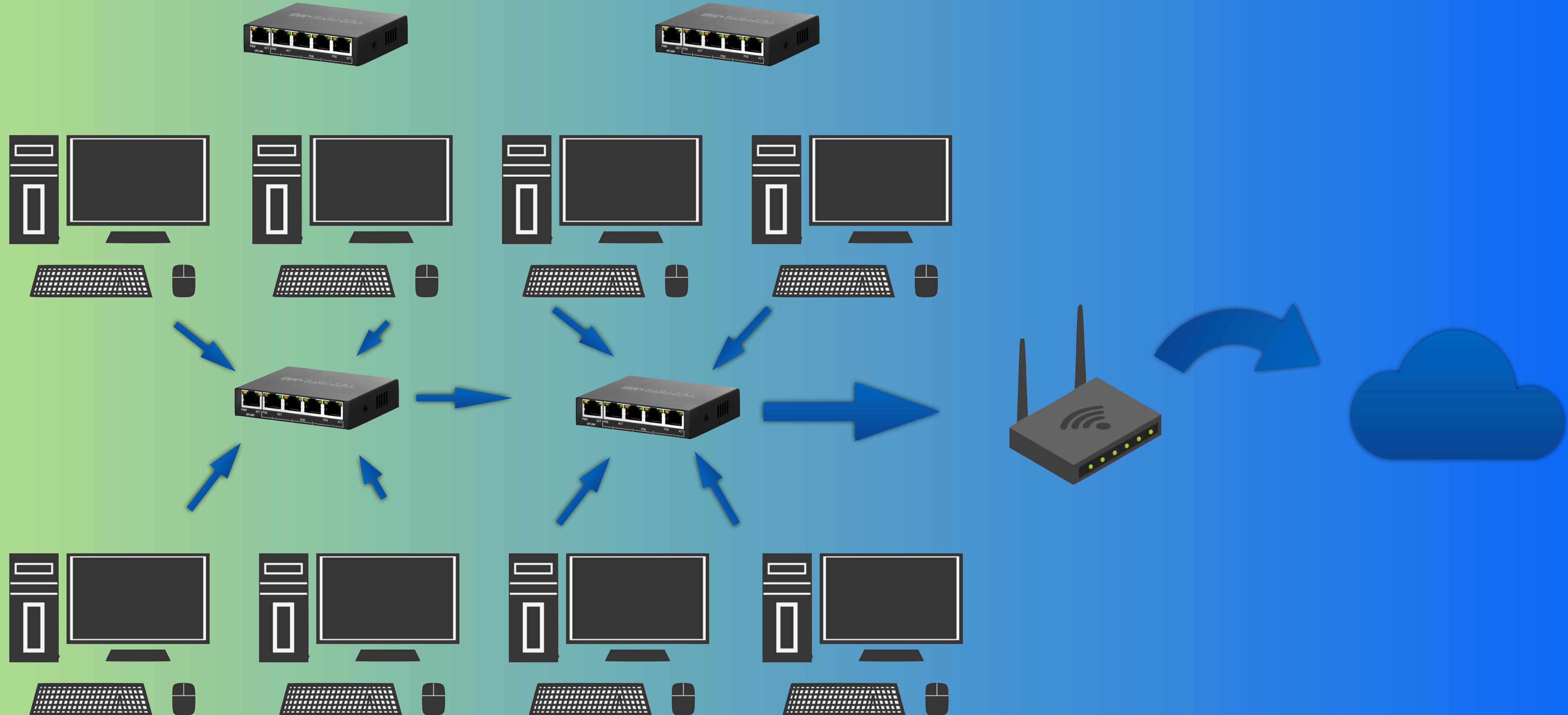


Cloud  
(Także tzw.  
Proxy Firewalls)

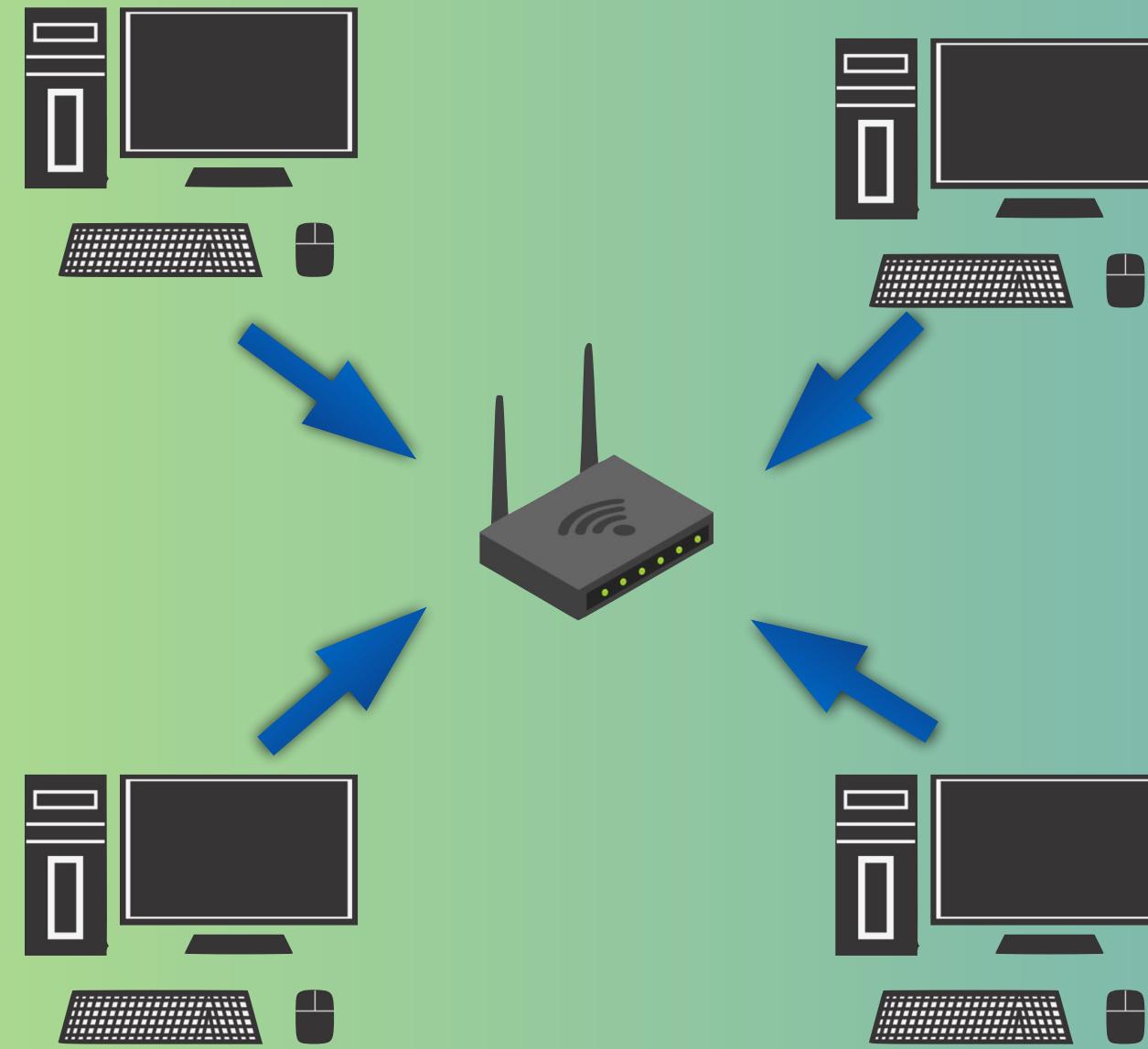


Software

Różne rodzaje implementacji



# Wektory ataków



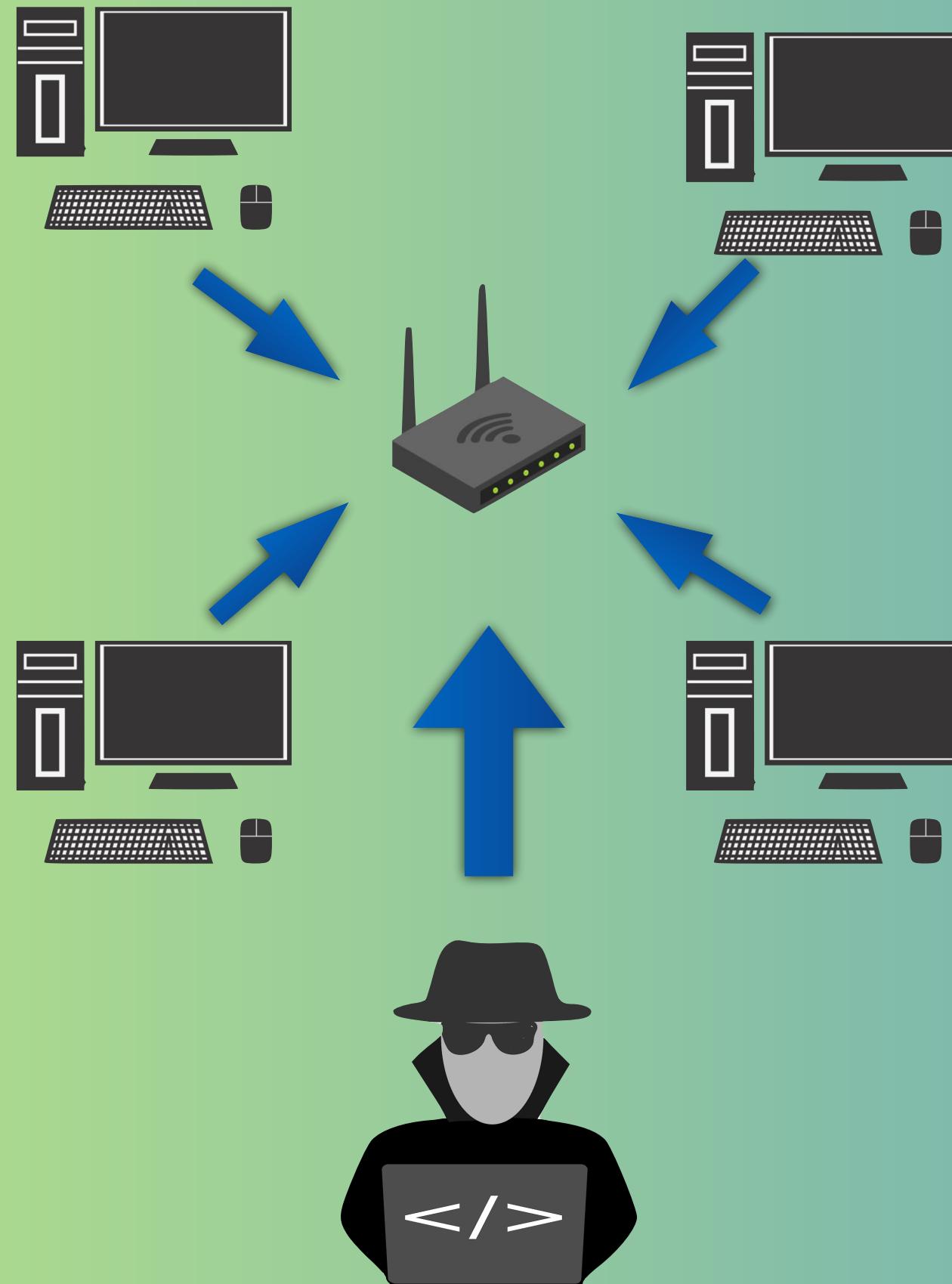
```
#> show arp
```

ARP aging time: 1200 seconds

Host	HW Address	VLAN	Type
10.9.221.221	cc:e1:7f:2e:54:01	1	D
10.9.221.209	00:26:3e:aa:ff:40	1	D
172.16.1.2	f8:c0:01:08:02:11	15	D

# Protokół ARP (Address Resolution Protocol)

# NDP Protocol => IPv6



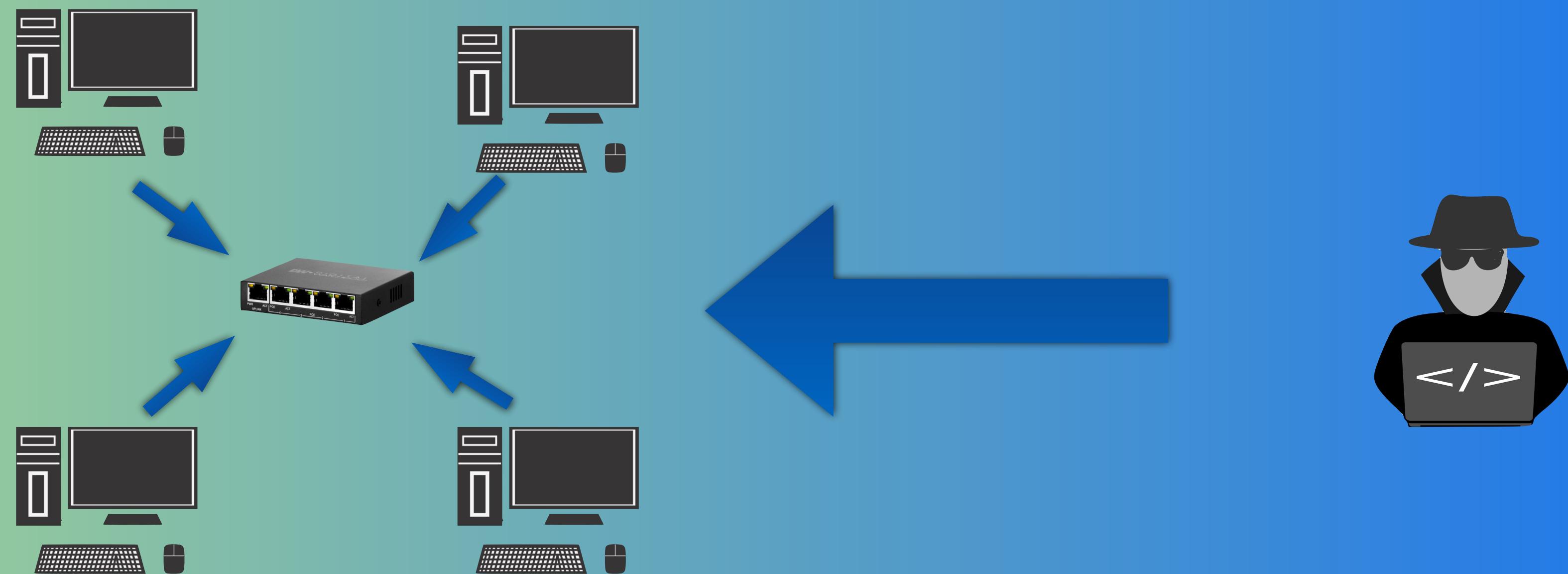
#> show arp

ARP aging time: 1200 seconds

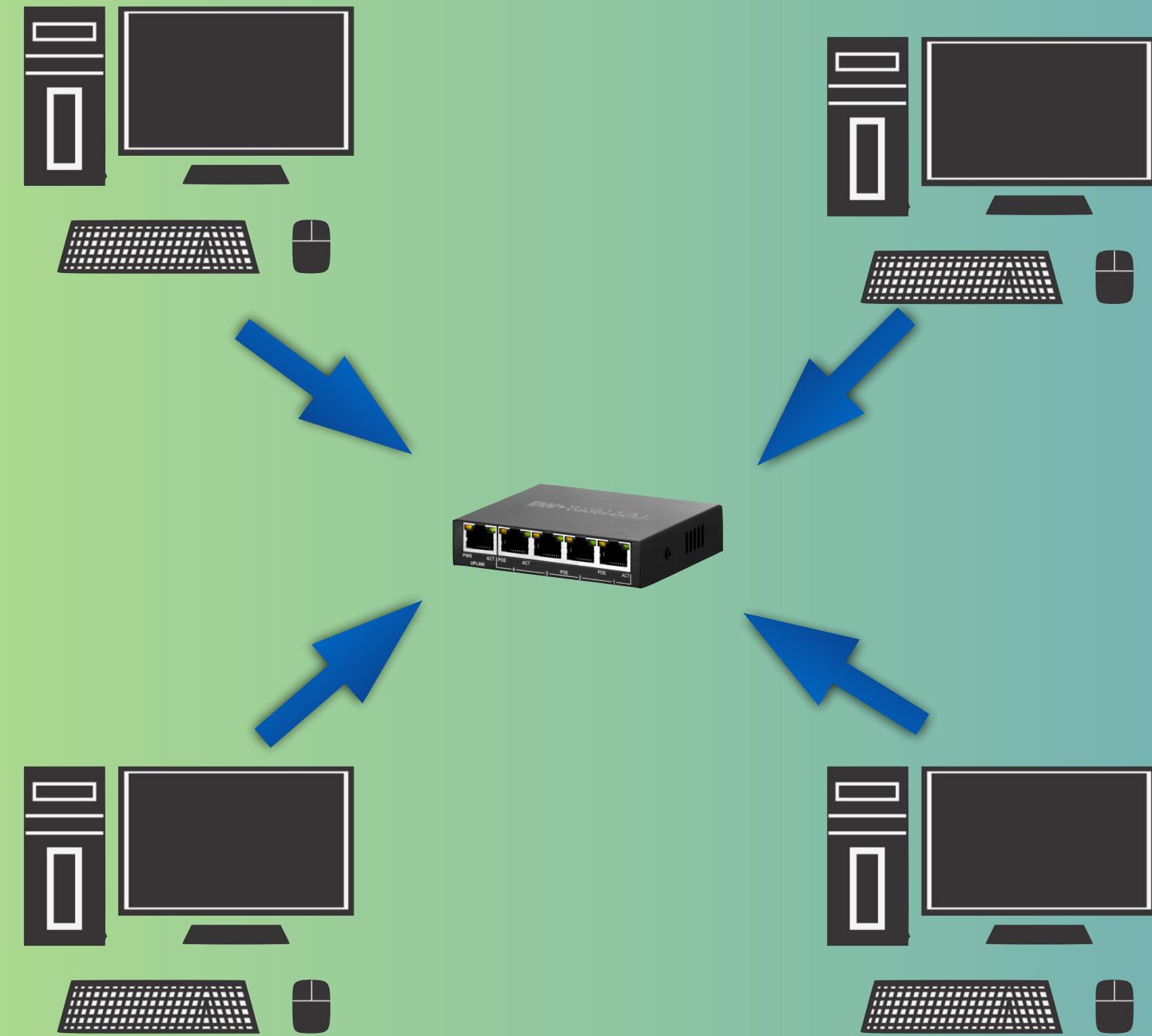
Host	HW Address	VLAN	Type
10.9.221.221	cc:e1:7f:2e:54:01	1	D
10.9.221.209	aa:bb:cc:dd:ee:ff	1	D
172.16.1.2	f8:c0:01:08:02:11	15	D

Ryszard

# ARP Spoofing



# CAM Table Spoofing

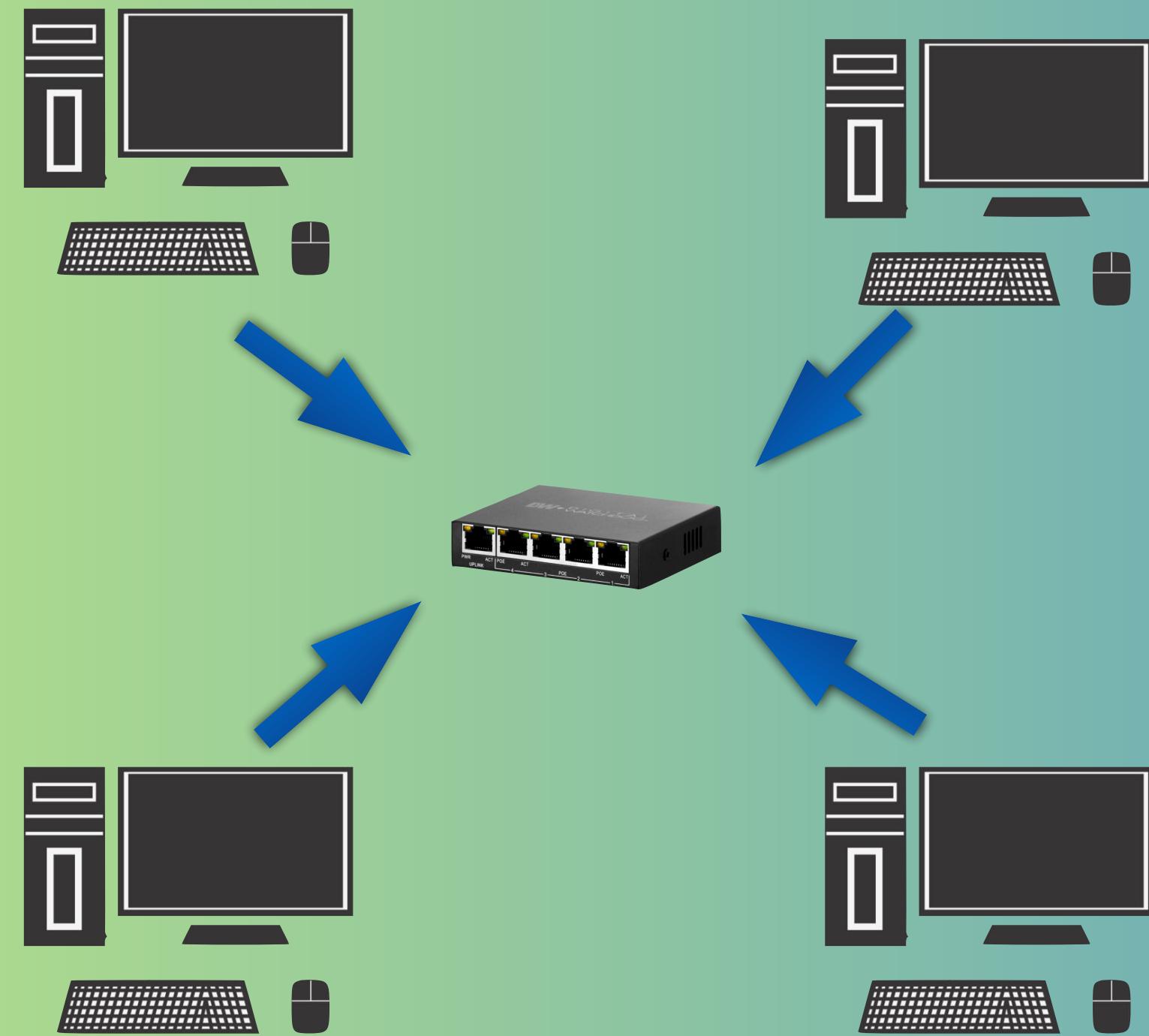


hey, I am new. I need IP



192.168.0.1

Protokół DHCP (Dynamic Host Config. Protocol)

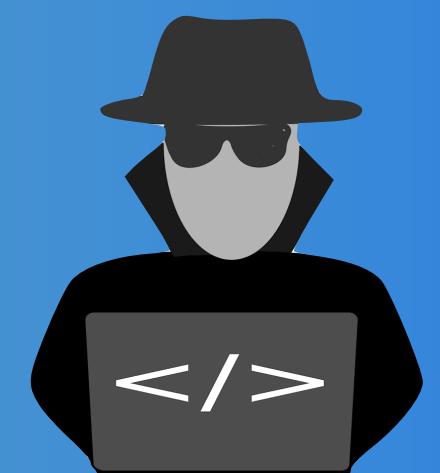


hey, I am new. I need IP

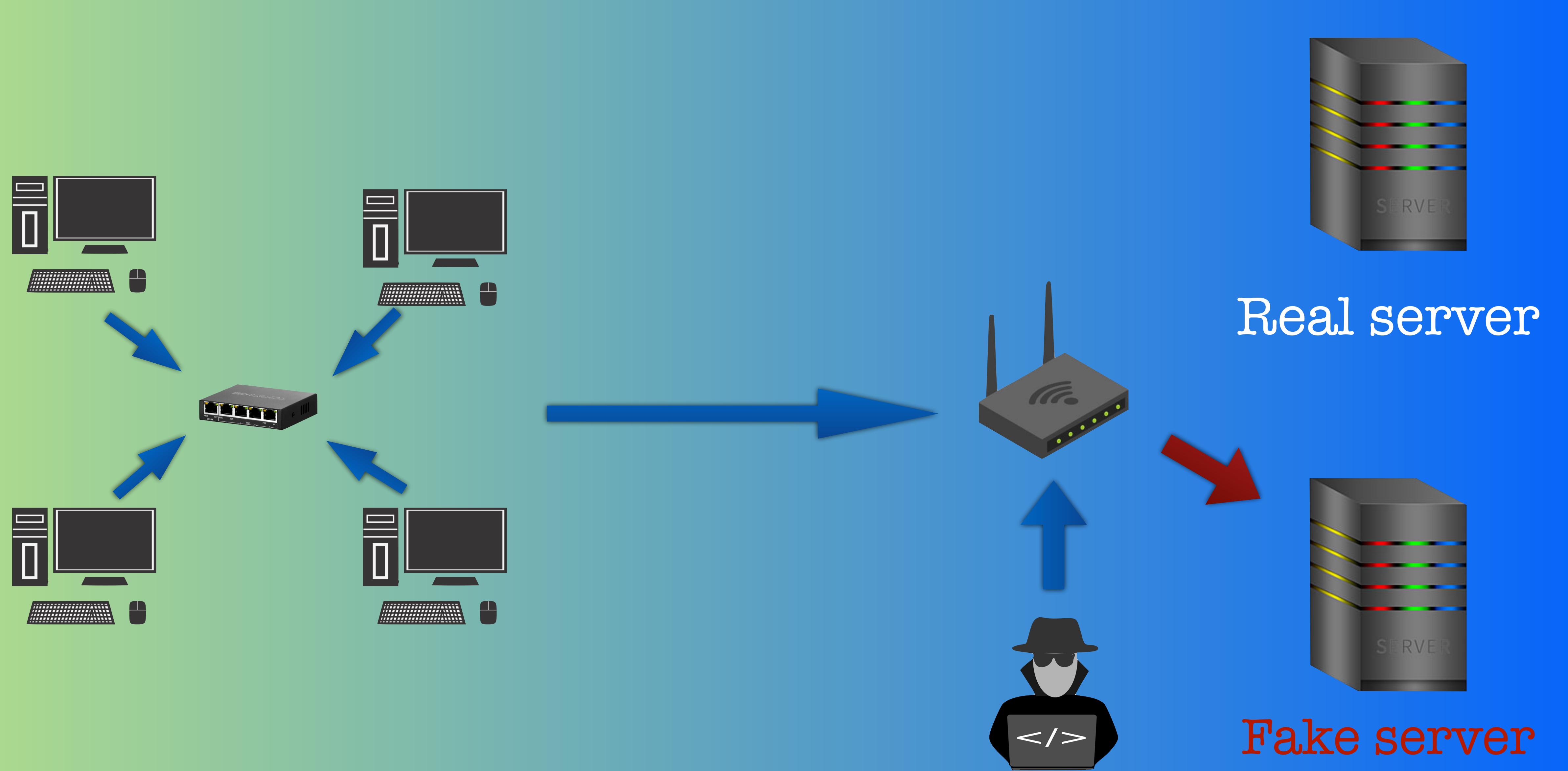


192.168.0.1

MiTM

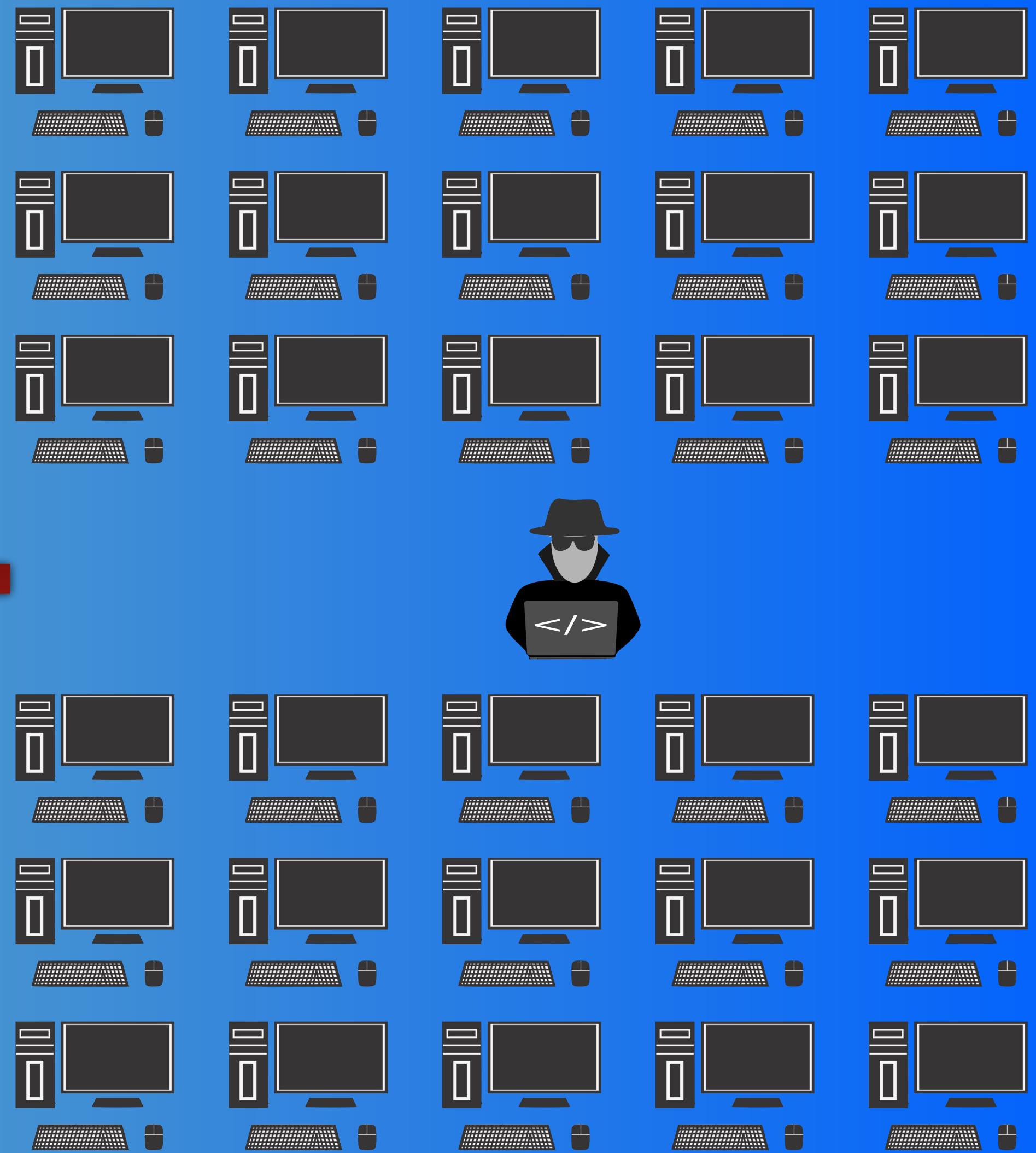
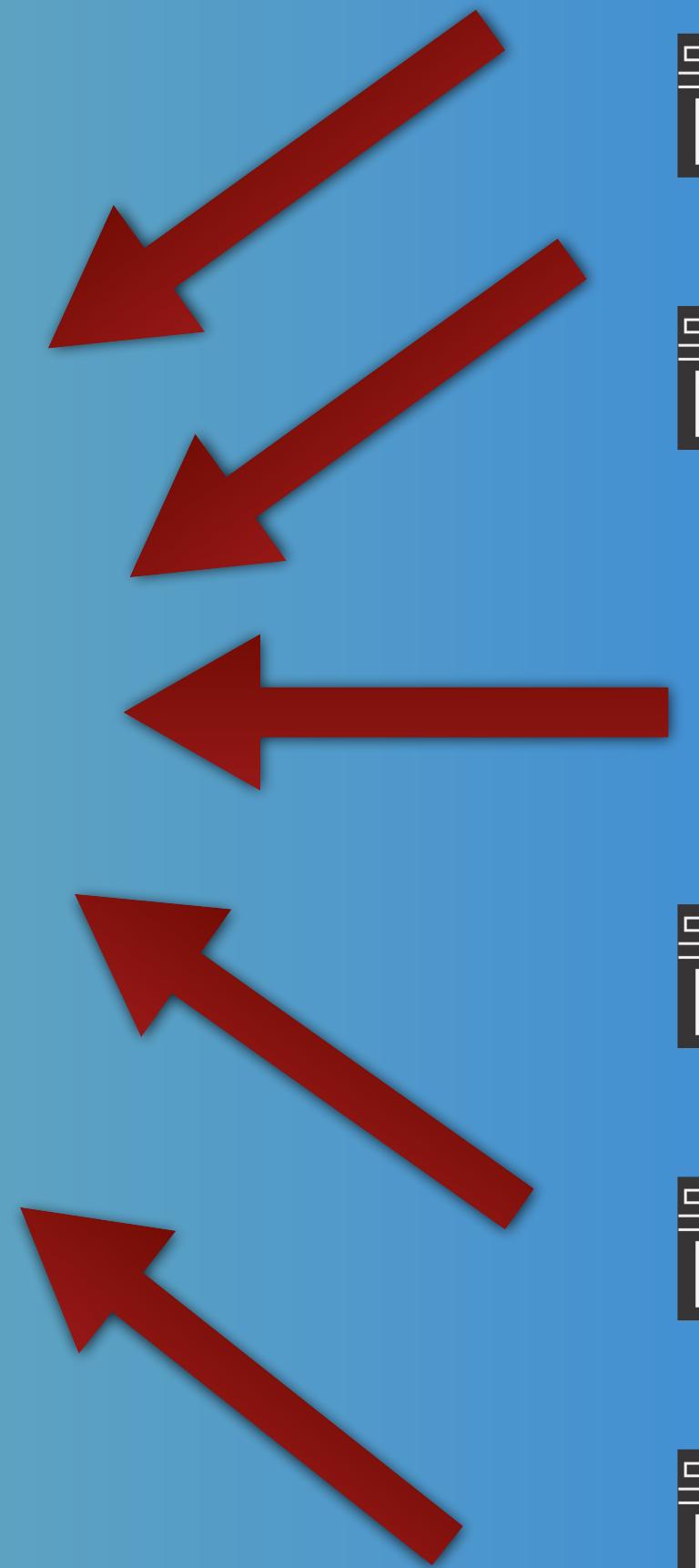
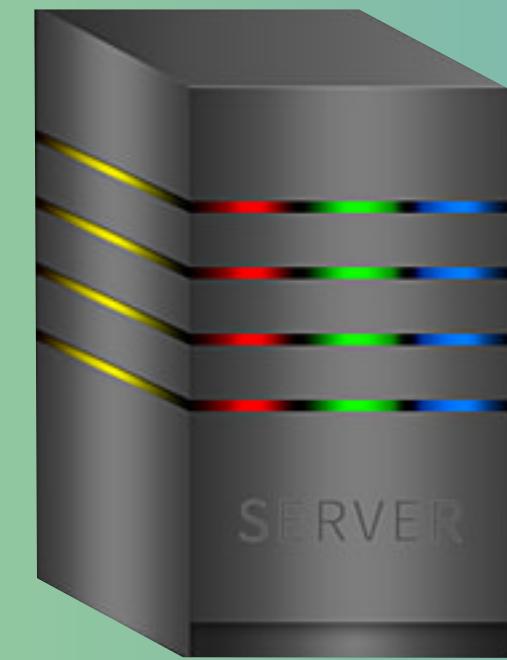
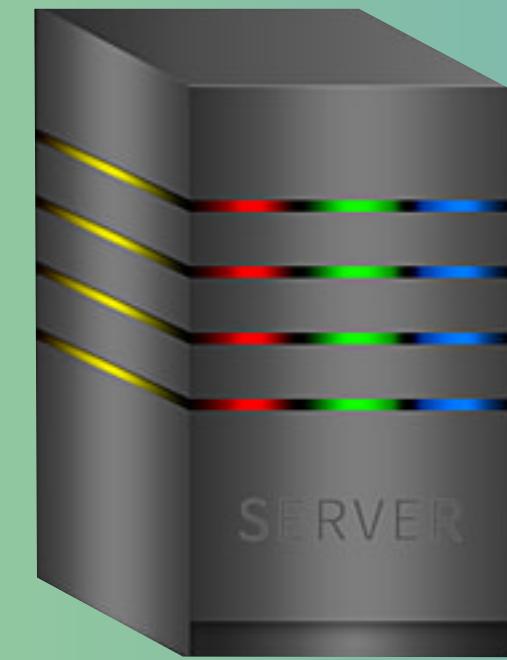
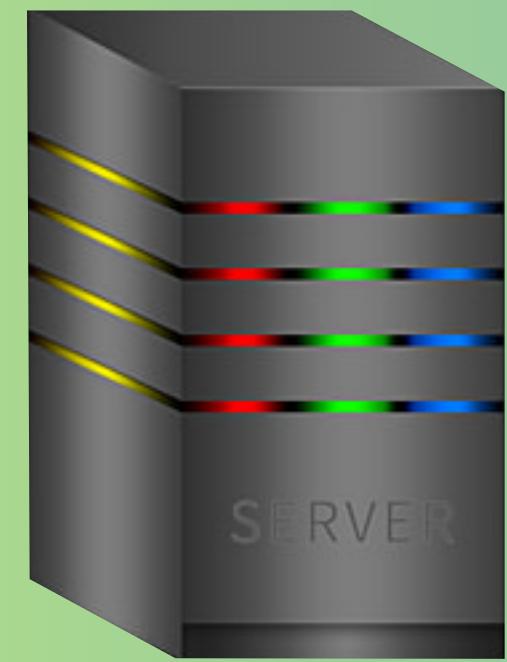


# DHCP Snooping



# DNS Spoofing

mojbiznes.com

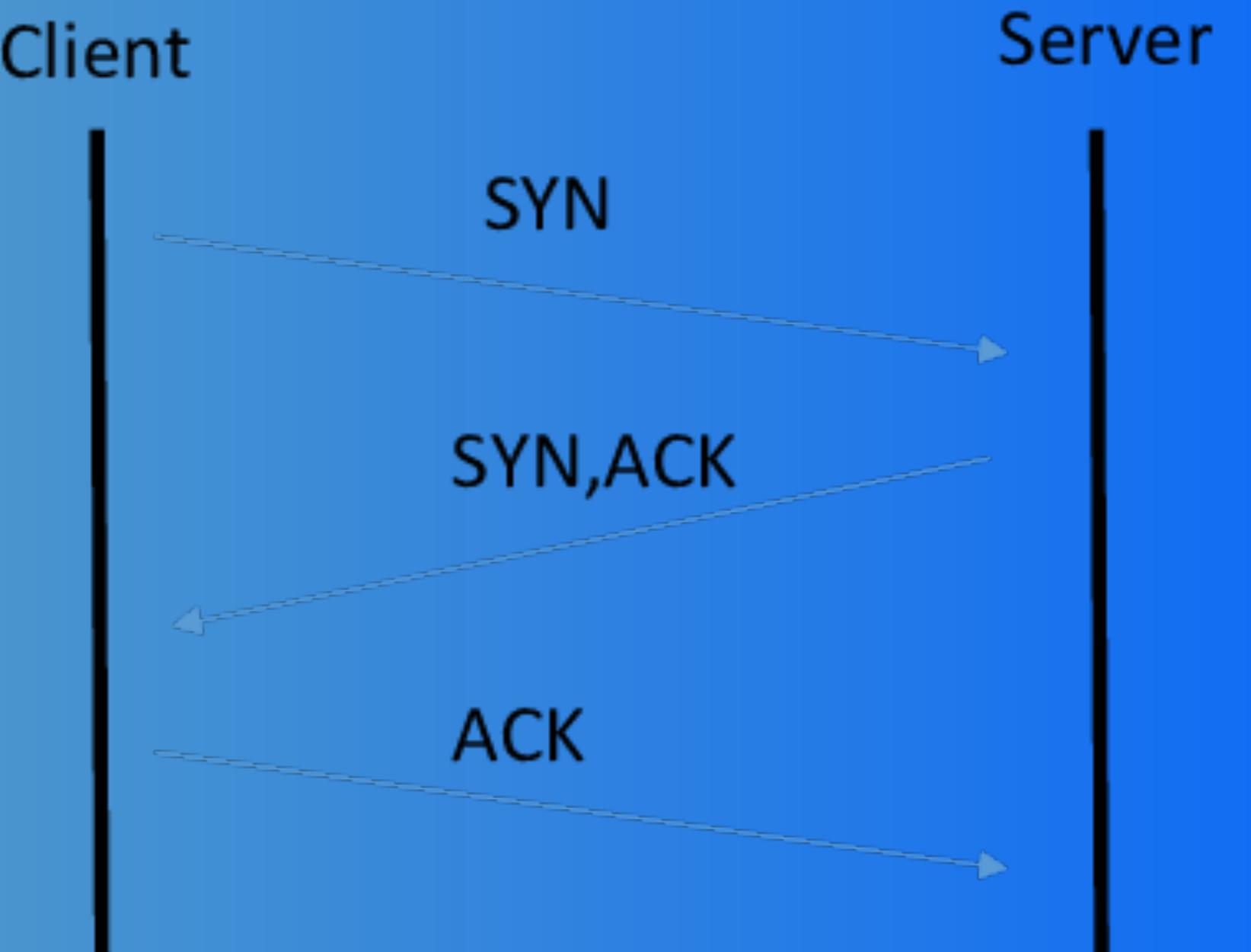


Ataki typu DoS (Denial Of Service)

Czy potrzebujemy tej  
armii zombie?



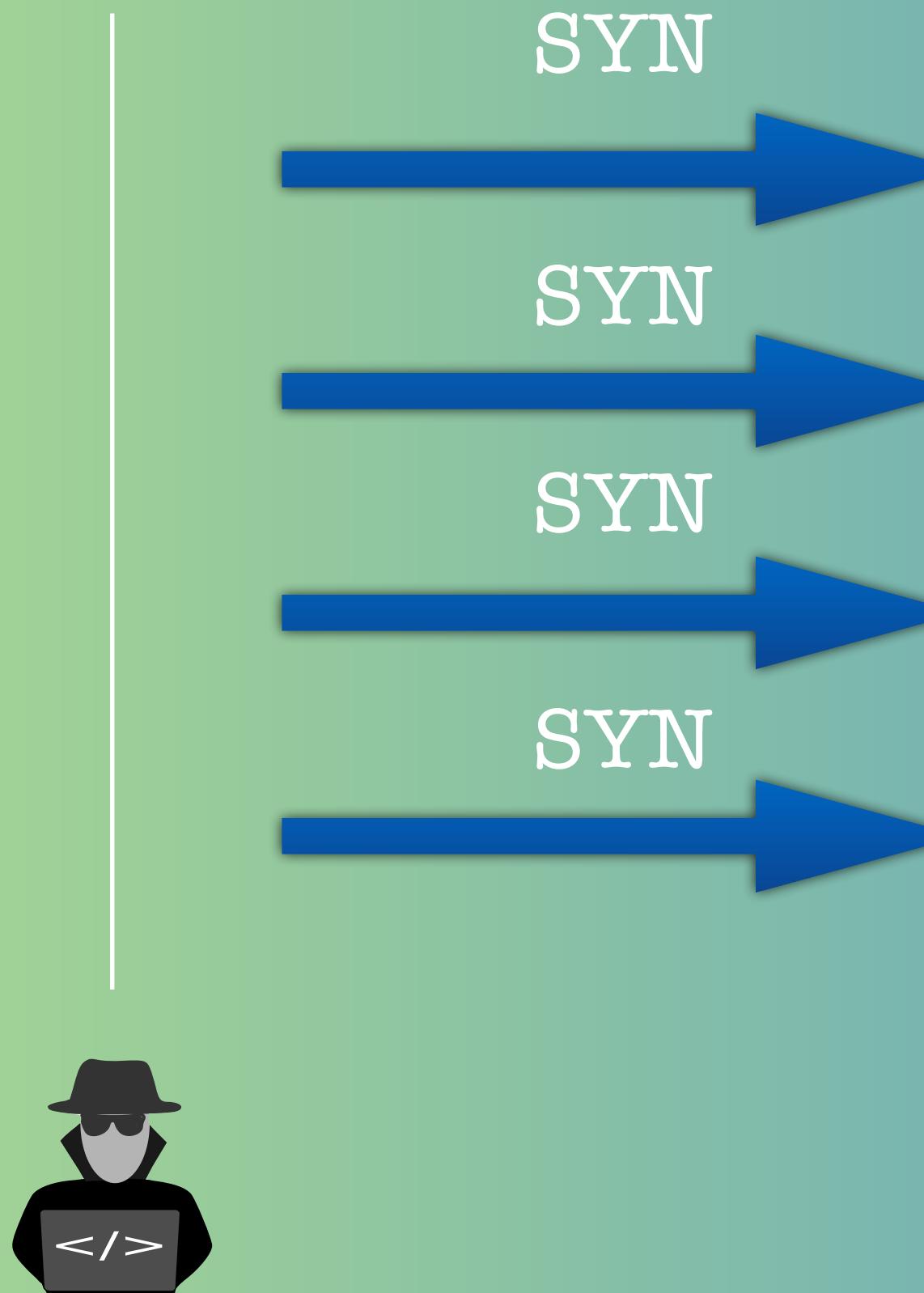
Nie.



Ataki typu DoS

Czy potrzebujemy tej  
armii zombie?

Client                  Server



Nie.

Ataki typu DoS - SYN Flood / Slow Loris

# Volume based



- Tak naprawdę wszystko, czym da się zalać
- UDP flood, ICMP flood, nieprawidłowe pakiety

# Protocol / Error based



- Ping Of Death - dowolność implementacji bywa groźna
- Smurf DDoS - nagła zmiana routera
- Ataki na wyższe warstwy, wykorzystanie exploitów

Ataki typu DoS - Inne przykłady

- Mamy dużo czasu
- Zazwyczaj słaba, mało płatna pracę
- Antyspołeczność



Tyl3 n@ t3m@t?



(Log #12312) 2020-01-31-11-23  
logging security incident  
(Log #12313) (...)  
(Log #12314) (...)  
(Log #12315) (...)

Co na to powie automotive?

# Pasywne

- Nasłuchiwanie ruchu sieciowego
- Połączenie się z portami znanych protokołów
- 

# Aktywne

- Wysyłanie pakietów SYN + RST (halfway scanning)
- NULL SCAN - wysyłanie pustych pakietów
- UDP Scan
- XMAS Scan (PSH, URG, FIN)

Narzędzia: nmap, zenmap, nikto, HPing3

Open

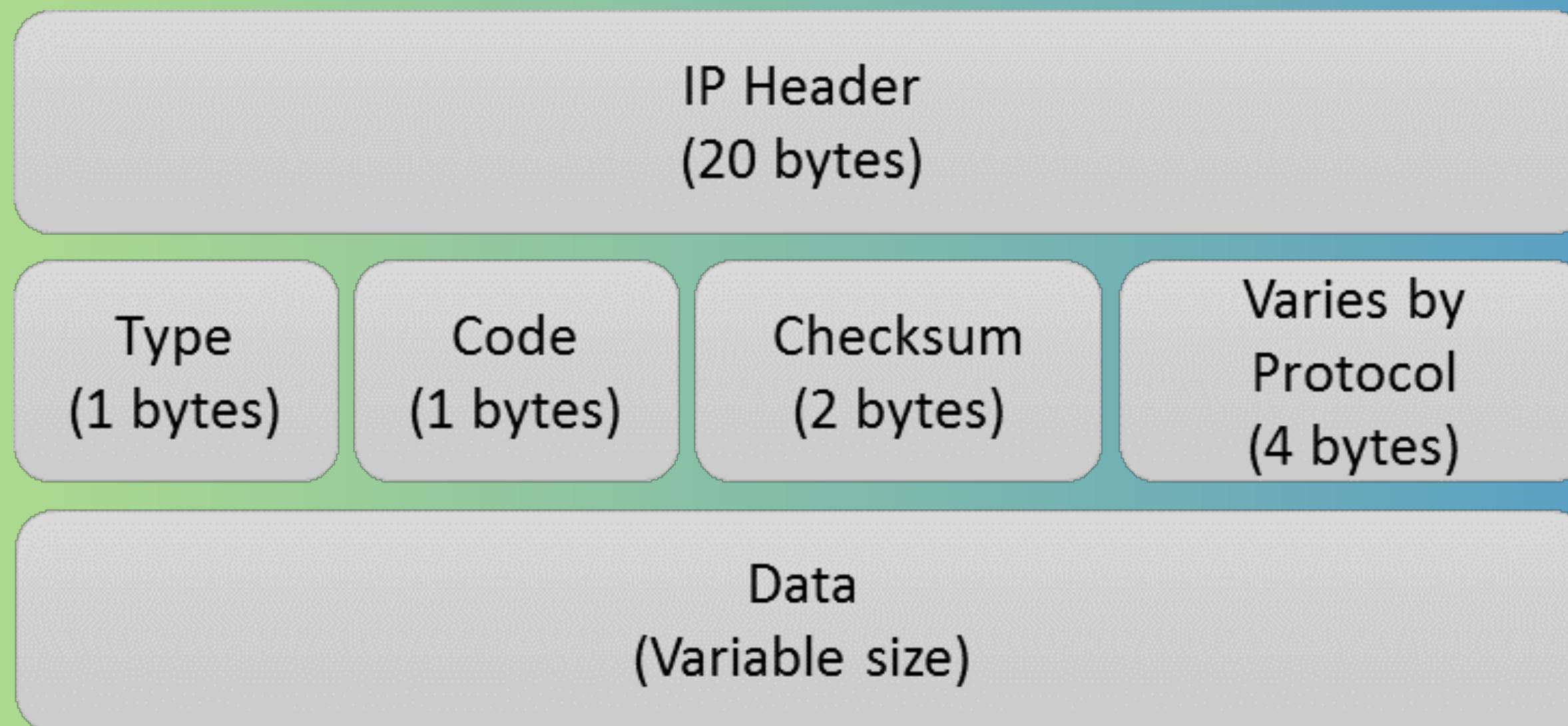
Closed

Filtered

Unfiltered

- Wspomniane „conservative in sending behavior”
- Przesyłanie pakietów TCP w ICMP, DNS, HTTP i innych protokołach
- Eksfiltracja danych ukrytych w normalnych pakietach (a.k.a stegano)

## ICMP



Eksfiltracja danych / Tunelowanie ruchu TCP

- Kombinacja różnych technik ukrywania danych w znanych protokołach
- Duża wolność tworzenia

” An advanced evasion technique enables the successful delivery of known malicious code without detection by:

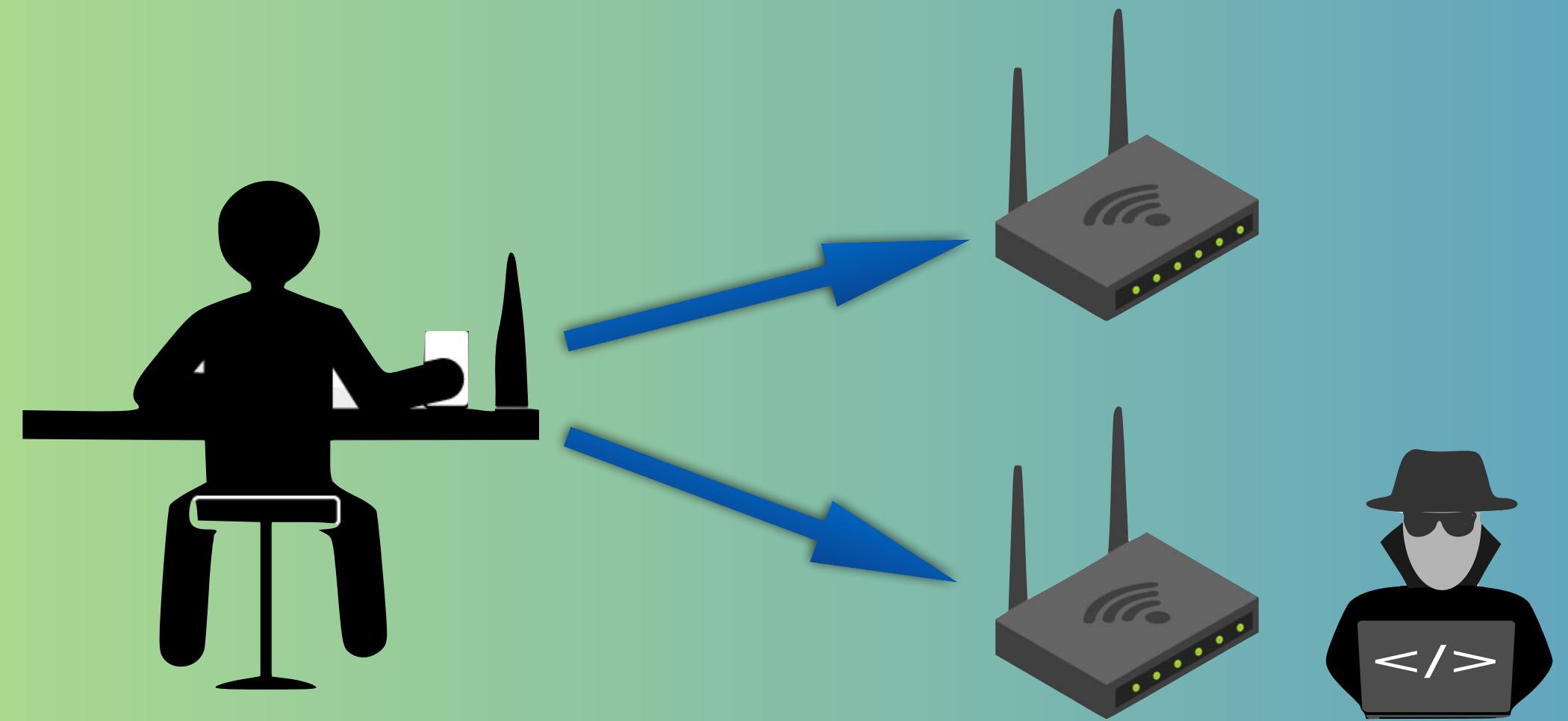
- ✓ Combining one or several known evasion methods to create a new technique that's delivered over several layers of the network simultaneously
- ✓ Being able to change the combination of evasions during the attack
- ✓ Evading inspection through clever design ”

Eksfiltracja danych, AET (Advanced Evasion Techniques)

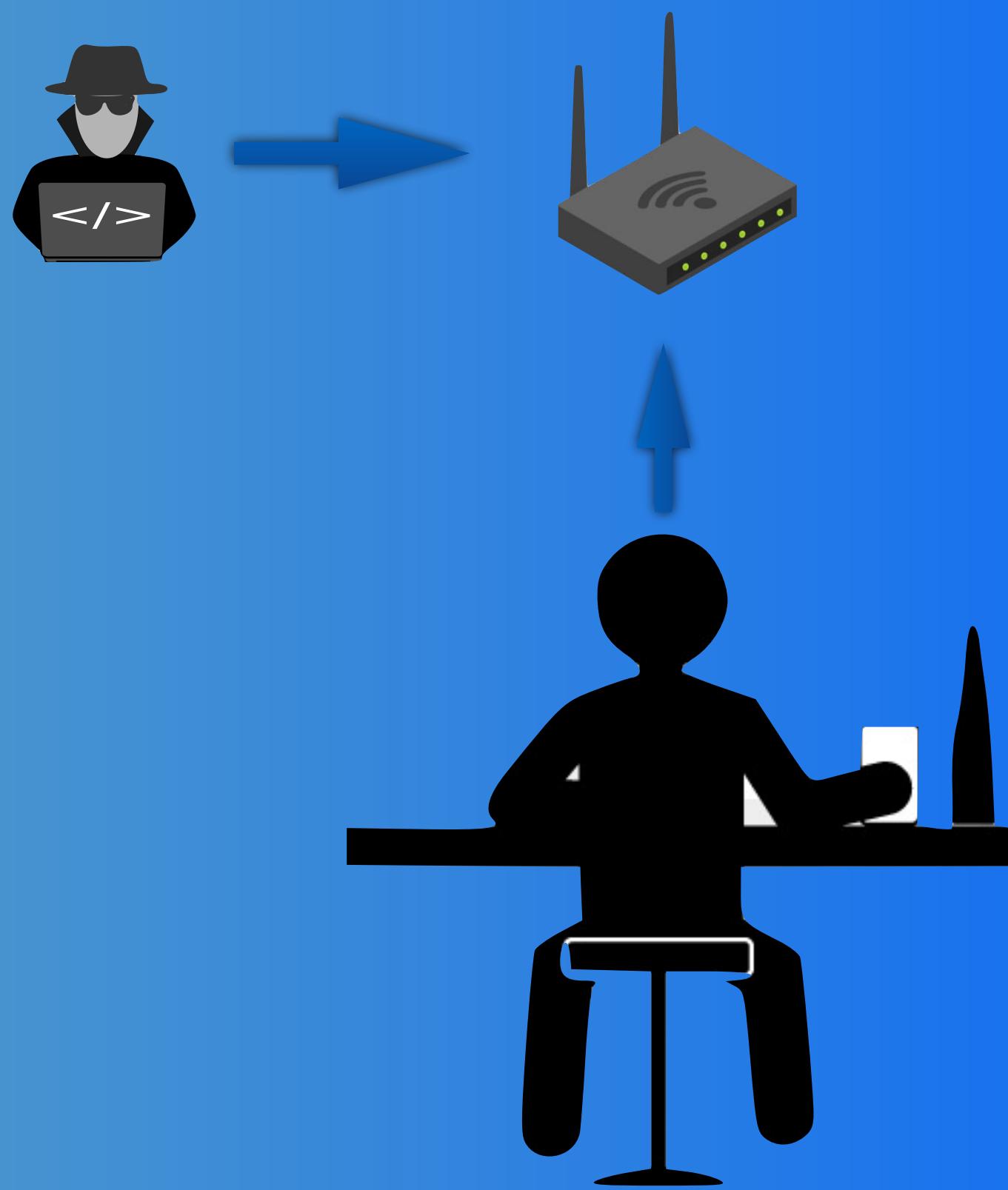


Inne - „inside job”, social engineering

# Atak tzw. Evil Twin



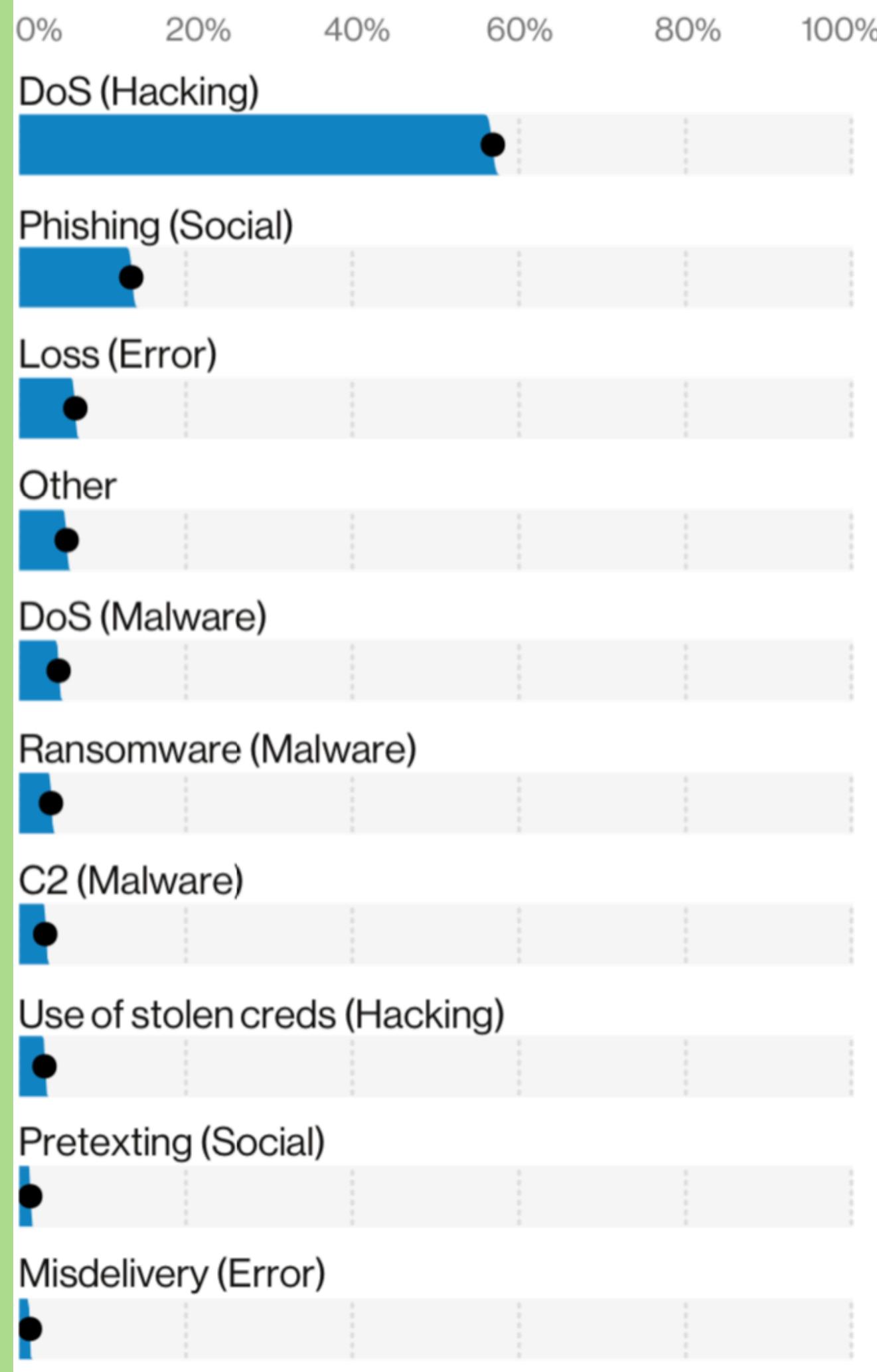
# Sniffing



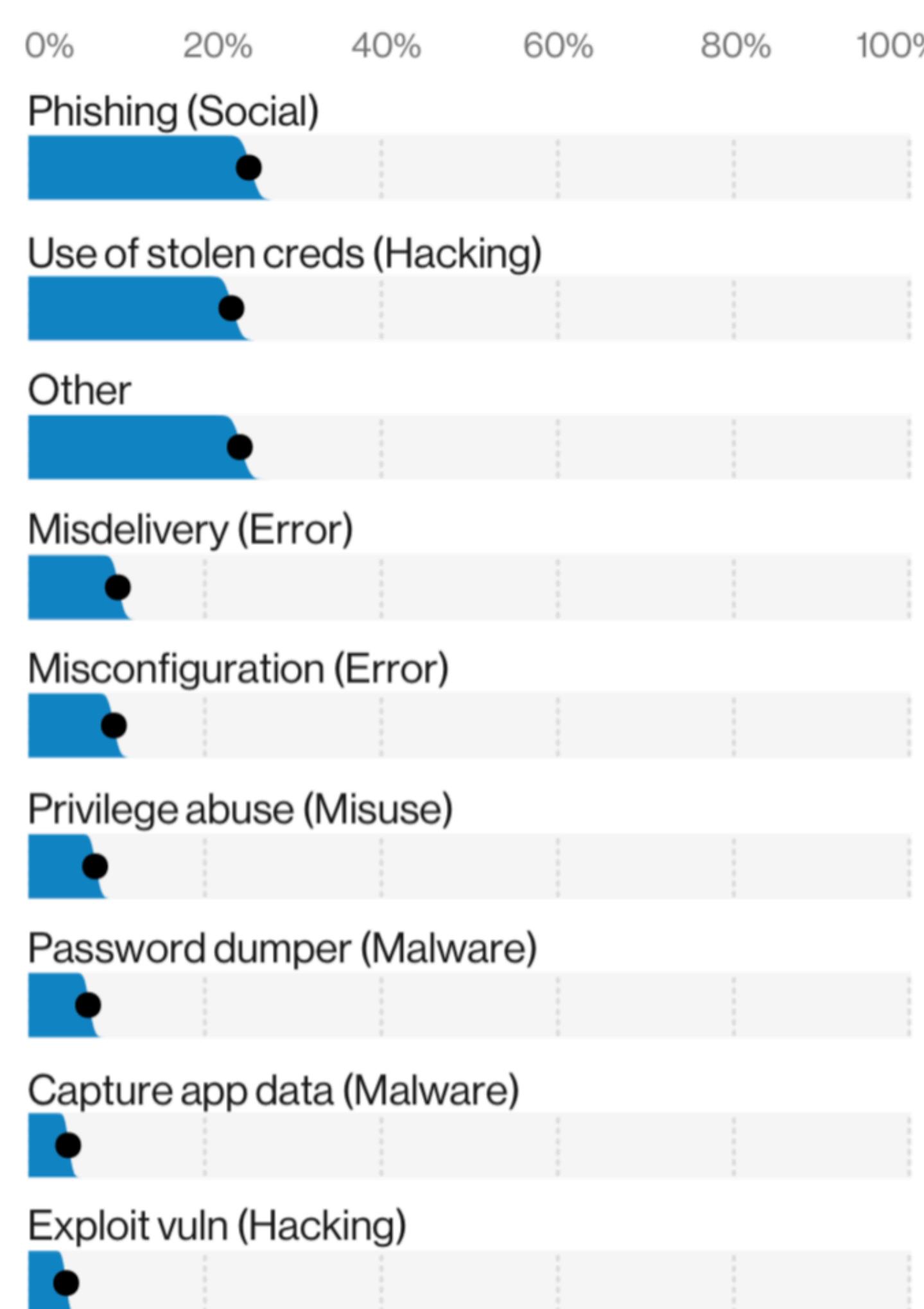
\*Czy ataki te rzeczywiście funkcjonują?\*

Inne - Ataki na prywatne osoby

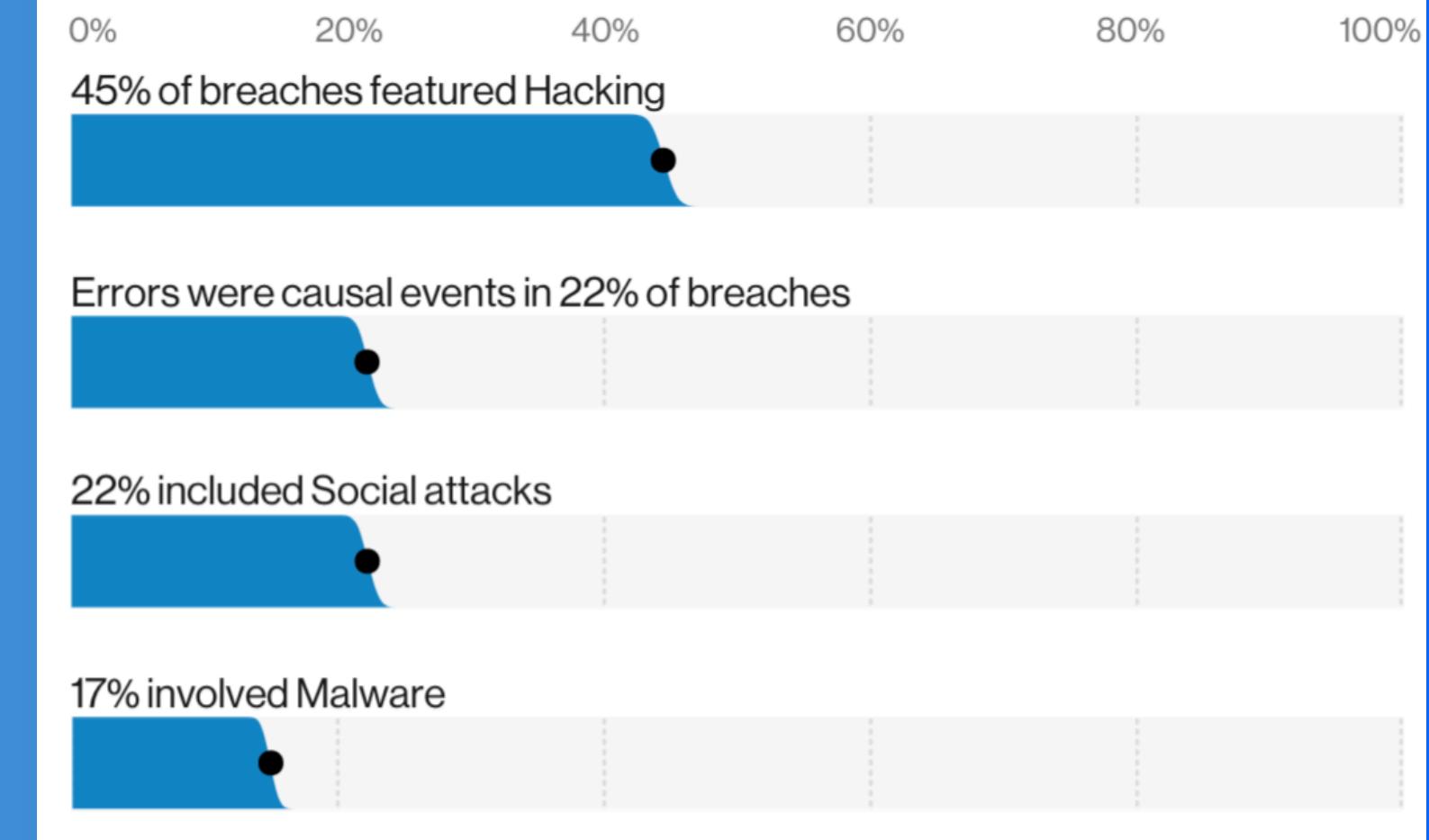
**Figure 12.** Top threat Action varieties in incidents (n = 23,619)



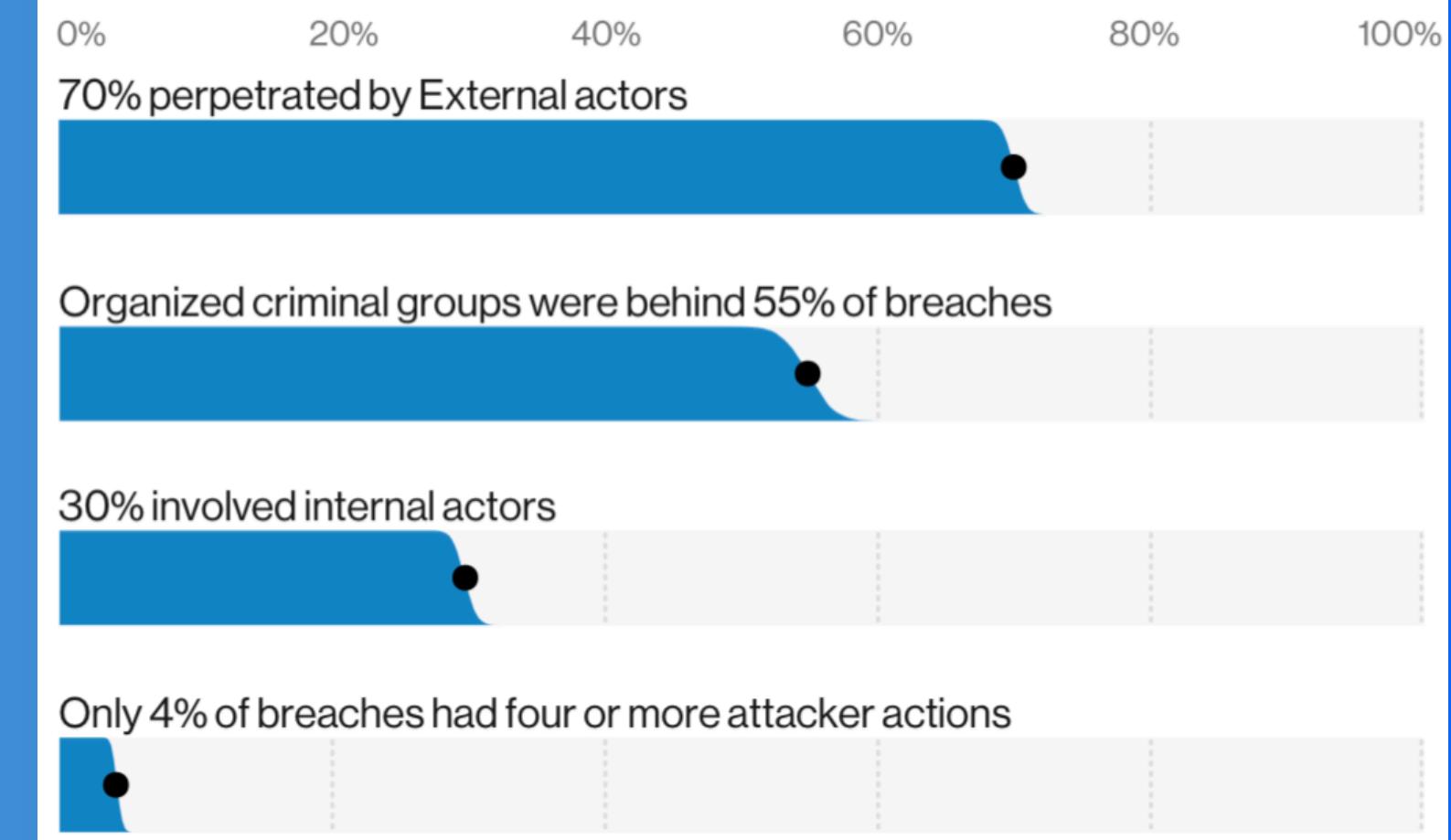
**Figure 13.** Top threat Action varieties in breaches (n = 2,907)



**Figure 2.** What tactics are utilized? (Actions)



**Figure 3.** Who's behind the breaches?

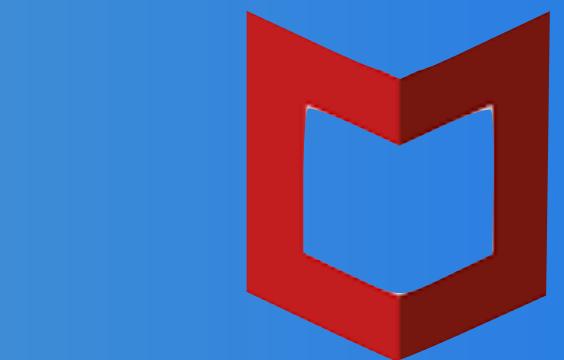


Rzeczywistość - Raport Verizon

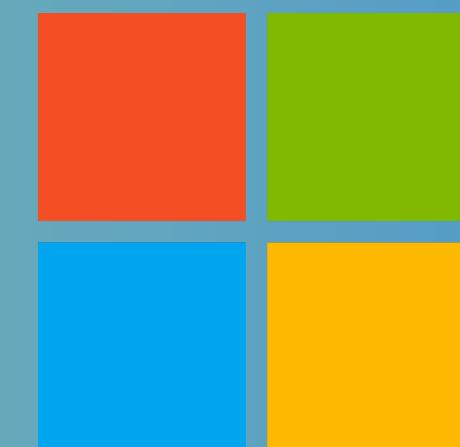
# W zasadzie większość znanych firm



Bitdefender



McAfee



Microsoft

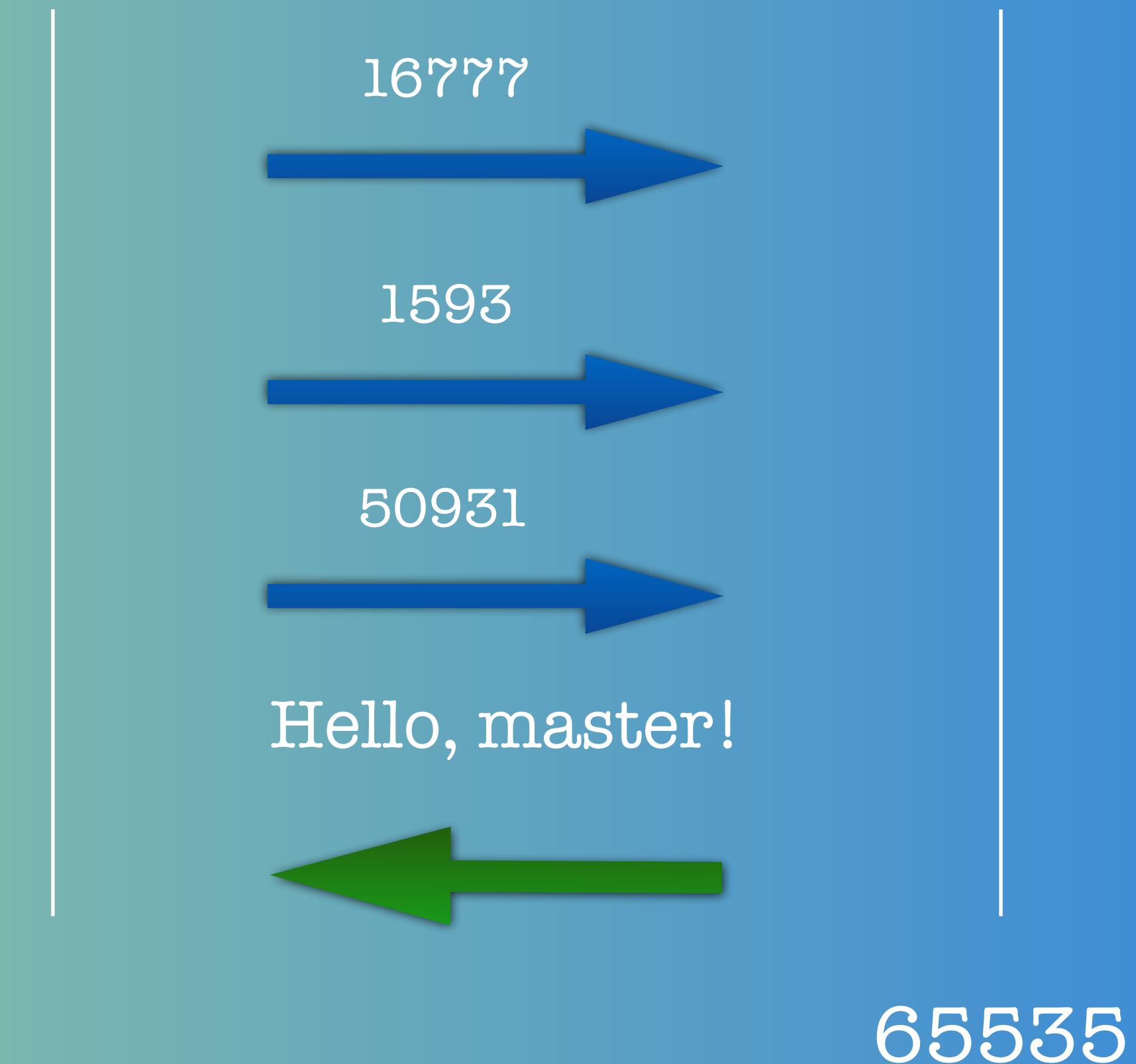
(...)

Szukaj: „{nazwa firmy} threat report 2020 ”

## Inne ciekawe raporty

Client

Server



Ciekawostka - port knocking (knockd(1))

- Identyfikacja prawdopodobnych incydentów, logowanie informacji, tworzenie raportów
- Identyfikacja zagrożeń na podstawie **sygnatur** (AV-like)
- Pasywna analiza ruchu sieciowego



IDS - Intrusion Detecton system

## Sygnatura

set of rules that protect against common network attacks, severe breaches or just to gather information

## Pattern-based

- Wyszukiwanie określonych wzorców w zawartości transmitowanego ruchu sieciowego
- Mechanizm podobny do GREPa albo YARA
- Wzorce proste (atomic) - pojedynczy pakiet
- Wzorce złożone (composite) - wiele pakietów, różne protokoły, różne źródła

## Anomaly-based

- Odstępstwa od „normalnego” ruchu sieciowego
- Wymagają procesu nauki wzorców który nie może być niczym zakłócony

## Policy-based

- Wzorce prawidłowego/oczekiwanej ruchu tworzone przez administratorów ręcznie na podstawie historycznej analizy ruchu sieciowego
- Trudno jest sprofilować całą sieć w dużej korporacji

TYPE -	TRIGGER	- ACTION
atom.	anomaly	log
comp.	policy	drop
	pattern	block future
	?	allow
		inspect

# Rodzaje sygnatur

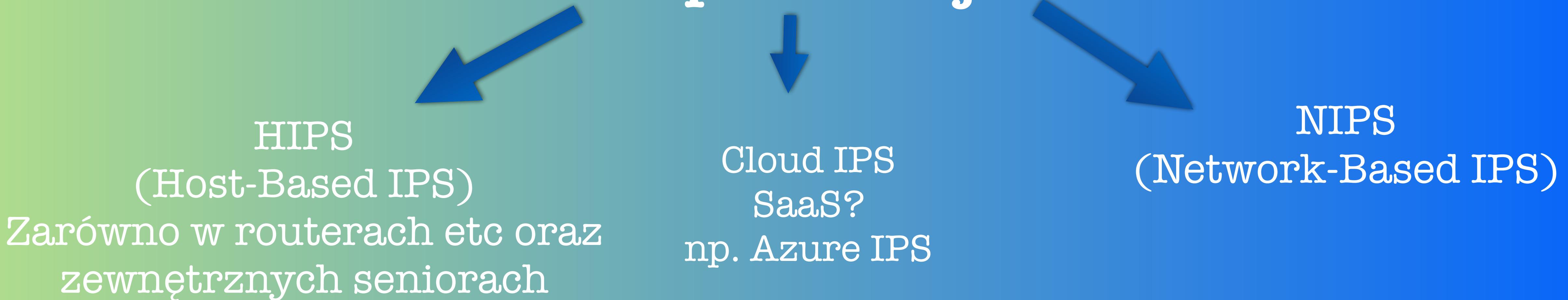
- Niestety tak. Pomimo dogłębnej analizy ruchu sieciowego, systemy IDS służą wyłącznie do detekcji
- Bardziej podatne na AET
- Z drugiej strony, urządzenia te nie wpływają znacząco na jakość usług sieciowych
- Awaria urządzenia nie powoduje awarii całej sieci
- Czy mamy alternatywę?



Problemy?

- Proaktywna ochrona
- Możliwość zatrzymania niepożądanego ruchu
- Implementacja w postaciach: **inline** oraz **promiscuous**
- Większe obciążenie nakładane na sieć
- W przypadku awarii sensora, awaria sieci
- Możliwość zatrzymania nieznanego zagrożenia (0-day)

## Implementacja



IPS (Intrusion Prevention System)



INTERNET SECURITY



## Computer protection

[Home 1](#)[Computer scan](#)[Update](#)[Tools](#)[Setup](#)[Help and support](#)[Refer a friend](#)

Real-time file system protection

Enabled: immediate detection and cleaning of malware on your computer.  
C:\Users\przem\AppData\Local\Microsoft\Edge\User Data\Default\Cache\f\_0090fe

Device control

Enabled



Host Intrusion Prevention System (HIPS)

Enabled: detection and prevention of unwanted behavior from applications.



Gamer mode

Paused: performance optimizations for games and presentation.



Webcam protection

Enabled: protect your webcam from misuse and spying attempts.  
Rule based webcam access activated[Pause Antivirus and antispyware protection](#)

Import/Export settings



Advanced setup

ENJOY SAFER TECHNOLOGY™



Szybki start do wykrywania



Działanie w trybie bezpieczenia

# IPS - Przykłady

- Urządzenie integrujące w sobie cechy Firewalla, IPS, Identity Firewalla (AD), koncentratora VPN, wirtualizacji, failover feature\*
- 



“Firepower and ASA with firepower are taking over the market now. Firepower integrates AMP (Advanced Malware Protection), stateful firewalls and next generation IPS”

~Cisco

Cisco ASA (Adaptive Security Appliance)

- systemy SIEM (Security Information and Event Management)
- systemy DLP (Data Leak Prevention)
- Nawet Vulnerability Assessment Scanner (Nessus, OpenVAS)
- Web filtering - rankingowanie stron www, ochrona przed stronami phishingowymi

Inne, ciekawe rozwiązania

- Większość informacji na slajdach została zamieszczona na podstawie informacji z kursu CCNA, CCNAs oraz na bazie doświadczeń autora prezentacji (z kursu Professional Secure Networks w Staffordshire University)
- <https://niebezpiecznik.pl/post/3-rady-na-dzien-bezpiecznego-internetu/>
- <https://cybersecurity.att.com/solutions/azure-intrusion-detection>
- <https://www.imperva.com/learn/ddos/ddos-attacks/>
- <https://www.lanner-america.com/blog/stateless-vs-stateful-packet-filtering-firewalls-better/>
- <https://www.compuquip.com/blog/the-different-types-of-firewall-architectures>
- <https://www.geeksforgeeks.org/zone-based-firewall/>

## Bibliografia