AKADEMIA GÓRNICZO-HUTNICZA
IM. STANISŁAWA STASZICA W KRAKOWIE

Systemy wykrywania zagrożeń

Marcin Niemiec

2021

Plan

- Warstwy ochrony
- Zapory sieciowe
- Systemy IDPS
- Sposoby wykrywania zagrożeń/włamań
- Inne rozwiązania bezpieczeństwa

Podstawowe narzędzia ochrony (podział chronologiczny)

- Zapora sieciowa/Firewall
- IDP, IPS, IDPS (*Intrusion Detection and Prevention System*)
- NGFW (*Next-Generation Firewall*)
- SIEM (*Security Information and Event Management*)
- …
- i inne (AV, Honey pot, itp.)

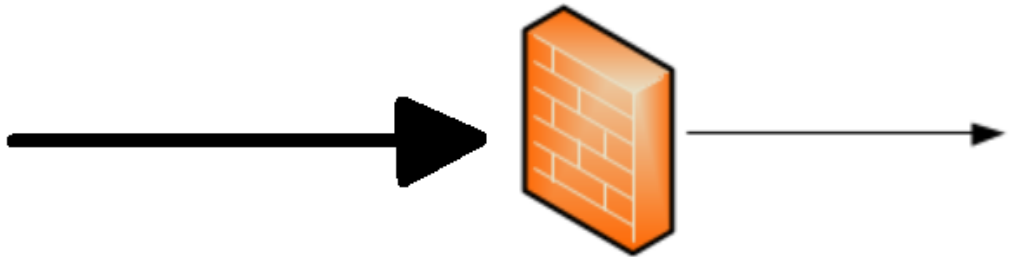
Warstwy ochrony

- NIDS (skanowanie ruchu sieciowego)
- AV (analiza kodu z punktu widzenia bezpieczeństwa)
- HIDS (bada zachowanie uruchomionych procesów – plik już uruchomiono)
- Sandbox (ochrona przez izolację, wirtualizacja zasobów)

Zapora sieciowa / Firewall

Filtrowanie pakietów na podstawie zdefiniowanych reguł (trzy główne generacje):

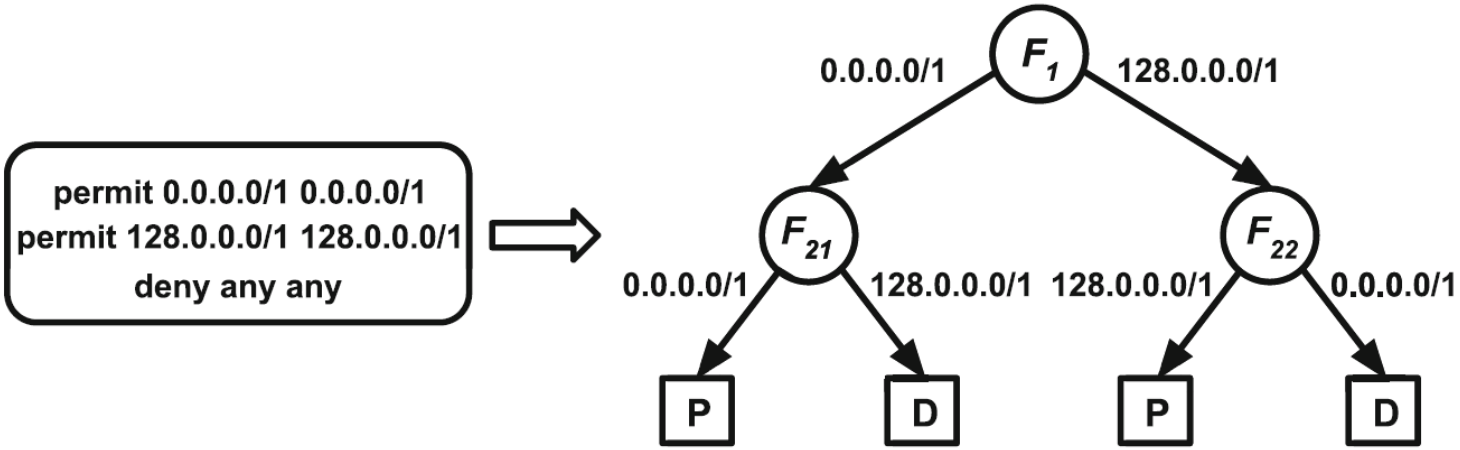
1) Filtrowanie bezstanowe (*stateless firewall*): pakiety czyli trzecia warstwa modelu OSI
2) Filtrowanie stanowe (*stateful firewall*): połączenia czyli czwarta warstwa modelu OSI
3) Monitorowanie aplikacji *(application firewall):* aplikacje/protokoły czyli wyższe warstwy OSI



Reguły

- Reguła: pojedynczy wpis
- Polityka bezpieczeństwa: spójny zestaw reguł realizujących określony cel

ACL (*Access Control List*): pojęcie wykraczające poza firewalle i systemy IDPS, choć często stosowane w tym kontekście



Sprawdzane elementy

- Źródłowy adres IP
- Docelowy adres IP
- Źródłowy port
- Docelowy port
- Protokół warstwy wyższej (transportowy)
- Interfejs urządzenia (wejściowy i wyjściowy)

Po dopasowaniu pakietu wykonywana jest określona akcja (np. wygenerowanie alarmu, usunięcie pakietu, rozłączenie połączenia, itp.)

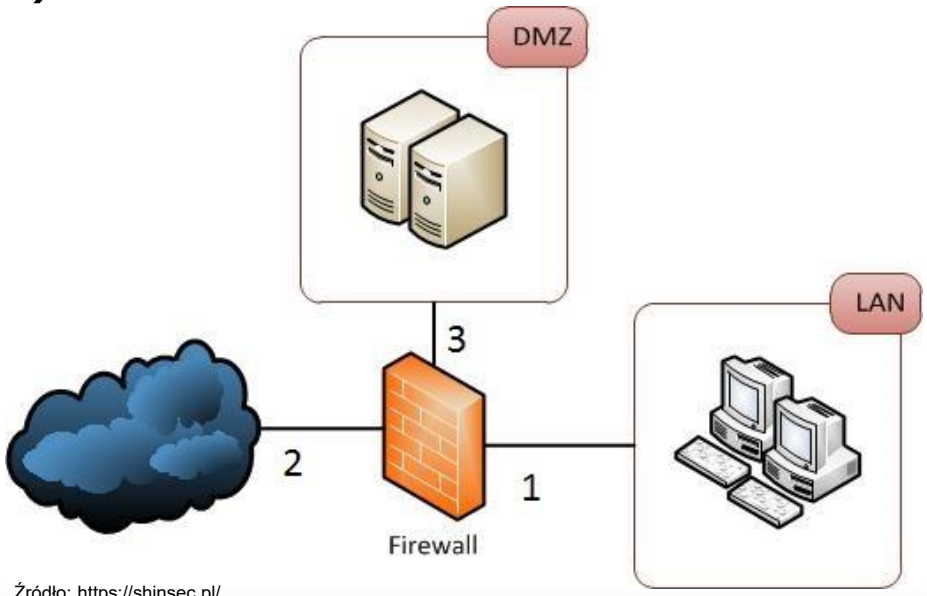
Zapory otwarte i zamknięte

Domyślna akcja:

- OTWARTE: wszystko co nie jest jawnie zabronione jest dozwolone
- ZAMKNIĘTE: wszystko co nie jest jawnie dozwolone jest domyślnie zabronione

Segmenty sieci, DMZ, VPN

DMZ (strefa zdemilitaryzowana, strefa ograniczonego zaufania) – wydzielona strefa z odrębną polityką bezpieczeństwa, zwykle mniej restrykcyjną (serwery www, FTP, pocztowe, DNS, itp.)



Źródło: https://shinsec.pl/

Intrusion Detection/Prevention

Proces polegający na monitorowaniu zdarzeń w systemie lub sieci i analizowaniu ich w celu wykrycia intruzów.

Współczesne systemy są w stanie monitorować system/sieć tak aby zapobiec ewentualnym atakom.

Dwa główne podejścia

Sygnatury ataków

- Efektywne dla znanych ataków
- „Pewne”, szybkie, precyzyjne
- Można samemu tworzyć nowe sygnatury
- Brak skalowalności – nawet dla podobnych ataków, wirusów polimorficznych, itp.

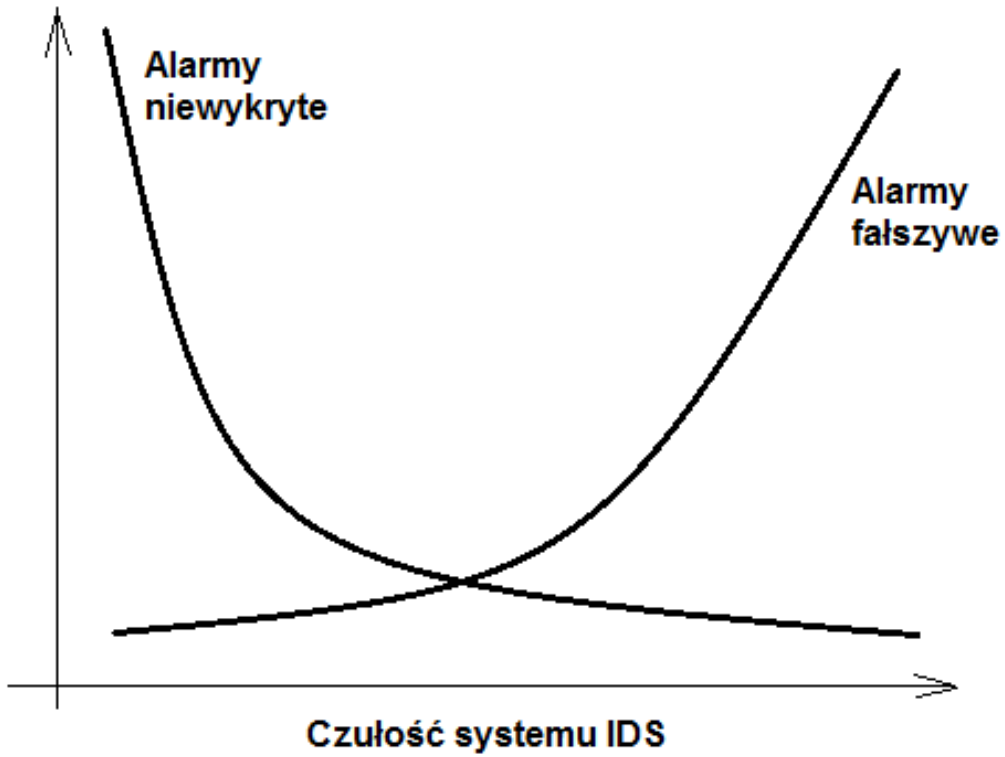
Dwa główne podejścia

Wykrywanie anomalii

- Wykrywanie nawet nieznanych ataków
- Zwykle wymaga wzorca ruchu (trenowanie)
- Potencjalnie skalowalne
- Duża ilość fałszywych alarmów

False positives

Normalne zachowanie systemu, zakwalifikowane przez system IDS jako atak



Przykładowe metryki

- Użytkownicy:
  - Częstotliwość logowania w danym okresie czasu
  - Czas od ostatniego logowania
  - Źródłowy adres IP
  - Długość trwania sesji
  - Rozmiar wysyłanych danych
  - Zużycie zasobów w sesji
  - Liczba niepoprawnych prób uwierzytelniania
- Programy/aplikacje
  - Częstotliwość uruchamiania programu/aplikacji
  - Zużycie zasobów przez aplikację
  - Odczyt/zapis do plików
  - Liczba odrzucanych żądań dostępu do plików/uruchomienia aplikacji

Inne podejścia do wykrywania zagrożeń

- Heurystyka (zachowanie)
- Sztuczna inteligencja

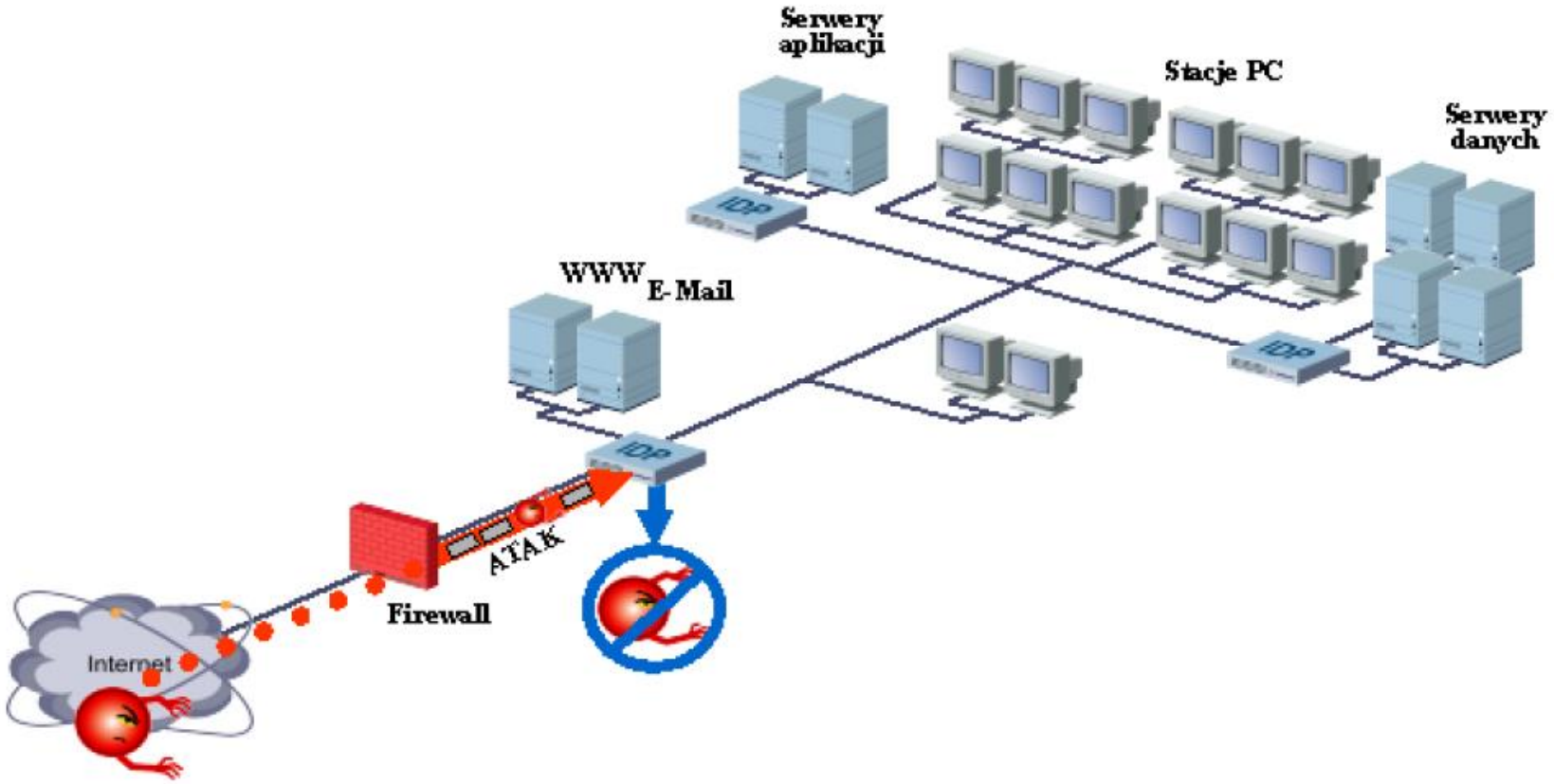
?

Aplikacje IDS

Przykłady darmowych systemów IDS:

- **Snort** (*Network IDS*)
- **OSSEC** (*Host-based IDS*)

Typowa architektura



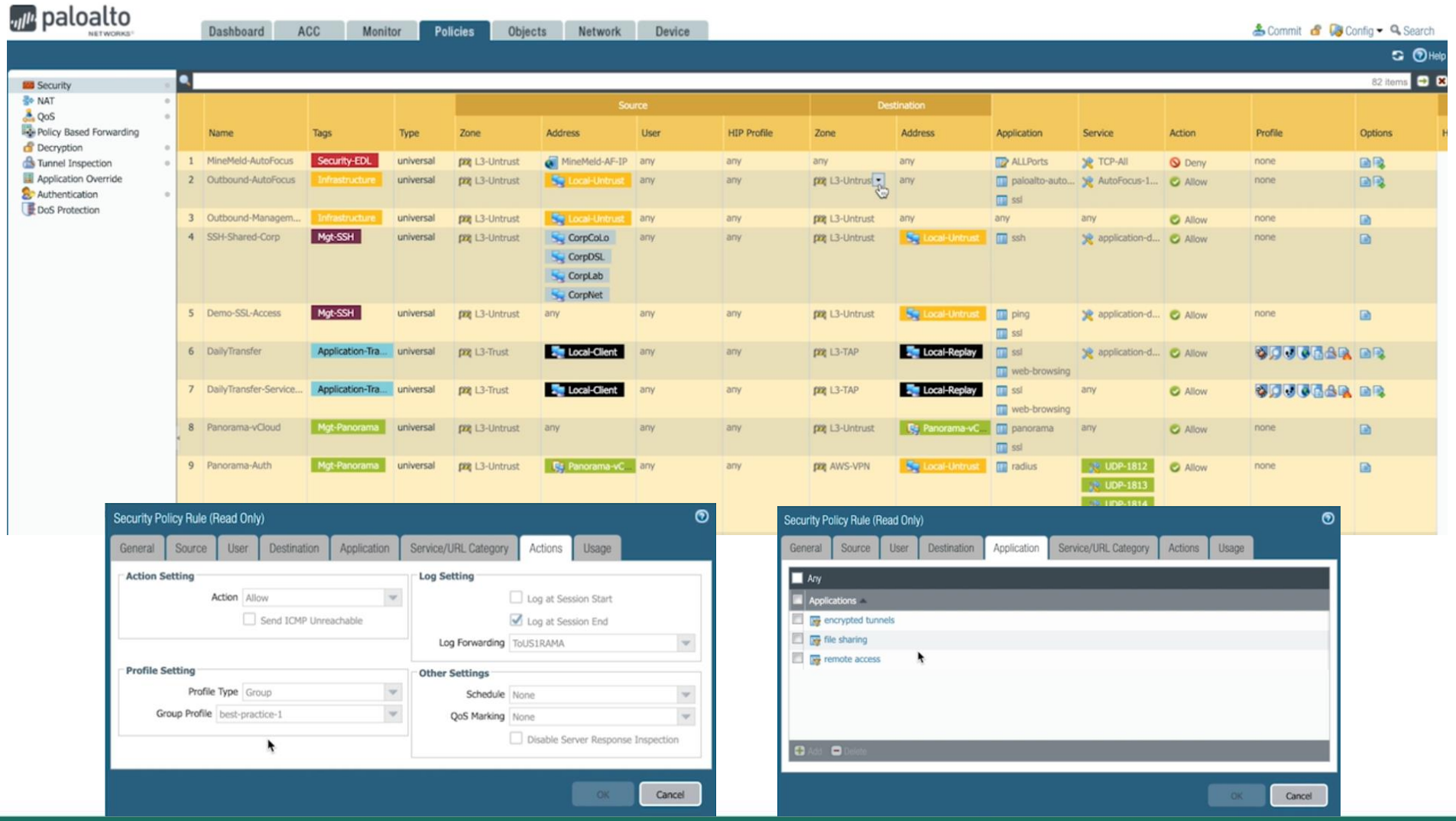
Źródło: http://juniper.clico.pl

Konfiguracja zapór

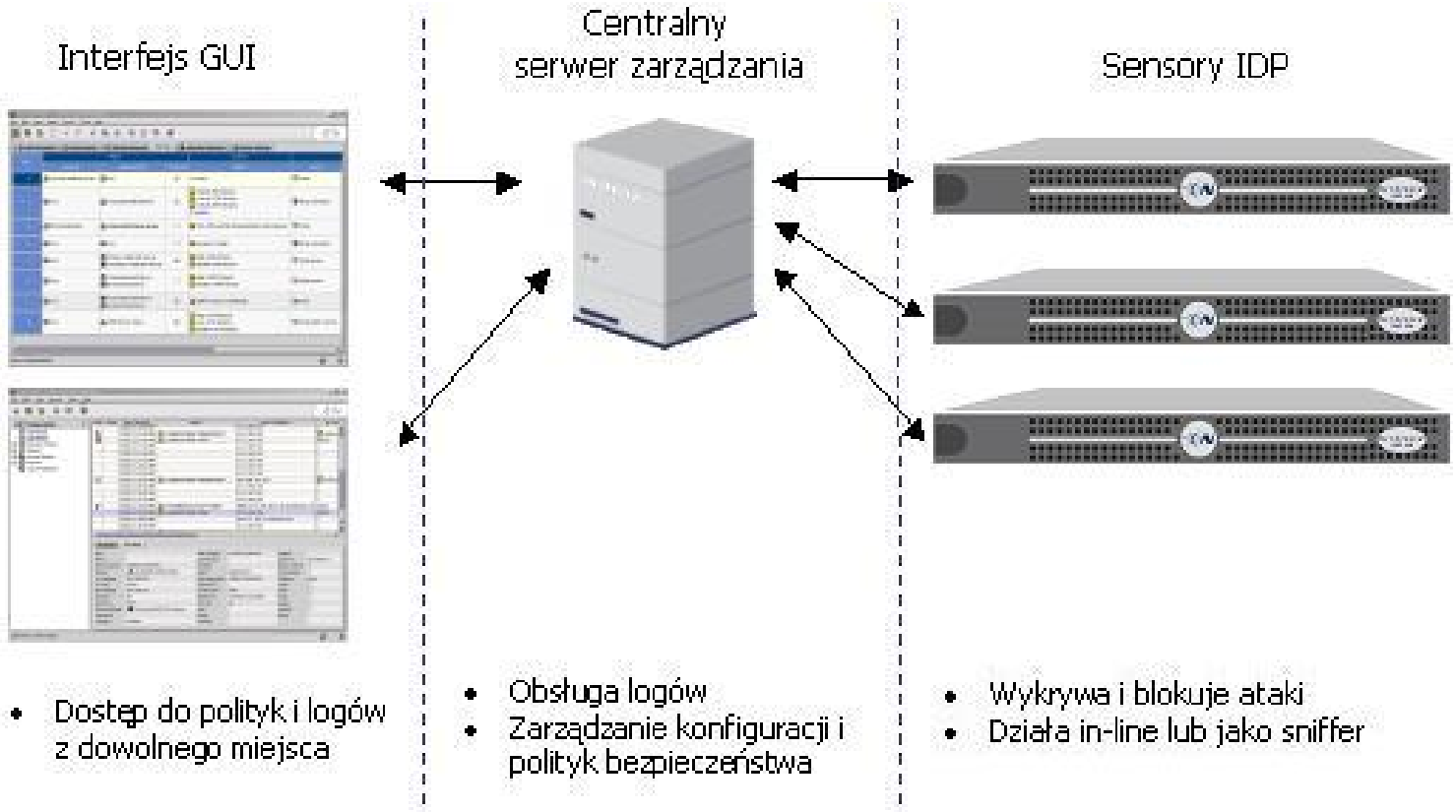
- Podział sieci na strefy (zewnętrzna, wewnętrzna, DMZ, itd.) – zwykle przypisane do danych interfejsów
- Podział zasobów na grupy (np. serwery)
- Podział zagrożeń na grupy:
  - ze względu na świadczone usługi
  - ze względu na użyte protokoły
  - ze względu na poziom zagrożenia (krytyczne, poważne, niskie, neutralne, itp.)

Sprzętowe NGFW

Przykładowy interfejs



Typowa architektura



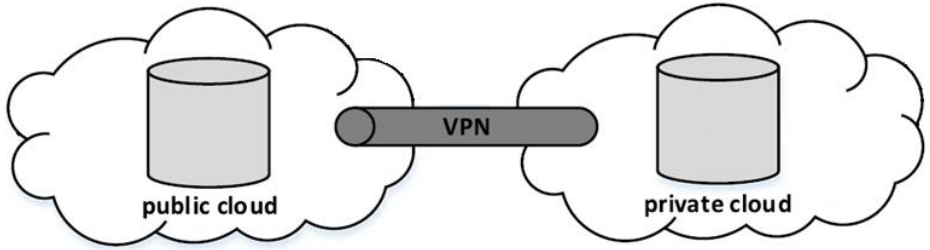
Źródło: http://www.ht.poznan.pl

Problemy otwarte

- Brak ochrony przed zagrożeniami z wewnątrz sieci lub gdy architektura sieci umożliwia inną drogę komunikacji
- System IDS/IPS może sam stać się celem ataków (blokowanie portów, tryb transparentny)
- Dostosowanie systemu IDS/IPS do konkretnej sieci/systemu
- Utrzymanie systemu IDS/IPS (rozsądny administrator)
- Ogromna ilość logów

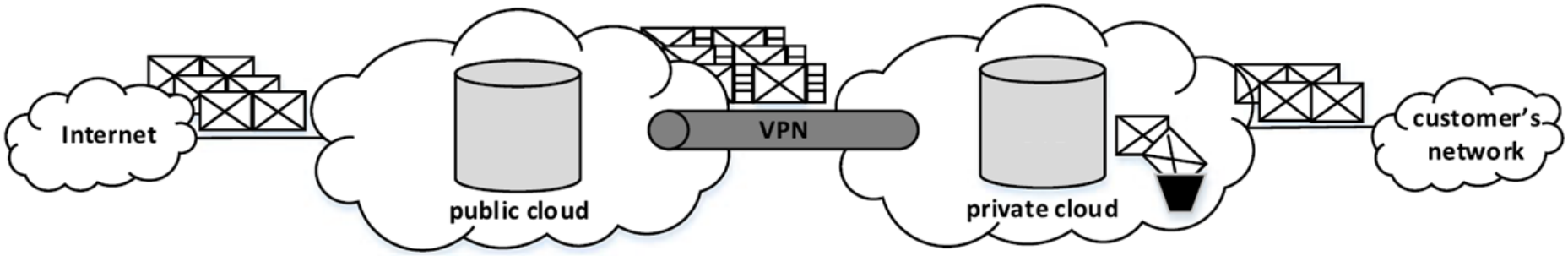
Zapory/IDPS w chmurze

- Chmura obliczeniowa – odporność na awarie, opłaty tylko za zużyte zasoby, z perspektywy użytkownika zasoby są nieograniczone (za wyjątkiem ustalonych limitów dla danego klienta)
- SECaaS (Security-as-a-Service)
- Chmury publiczne (np. AWS, GC), prywatne (np. OpenStack) i hybrydowe
- Wyzwania: wydajność vs. poufność



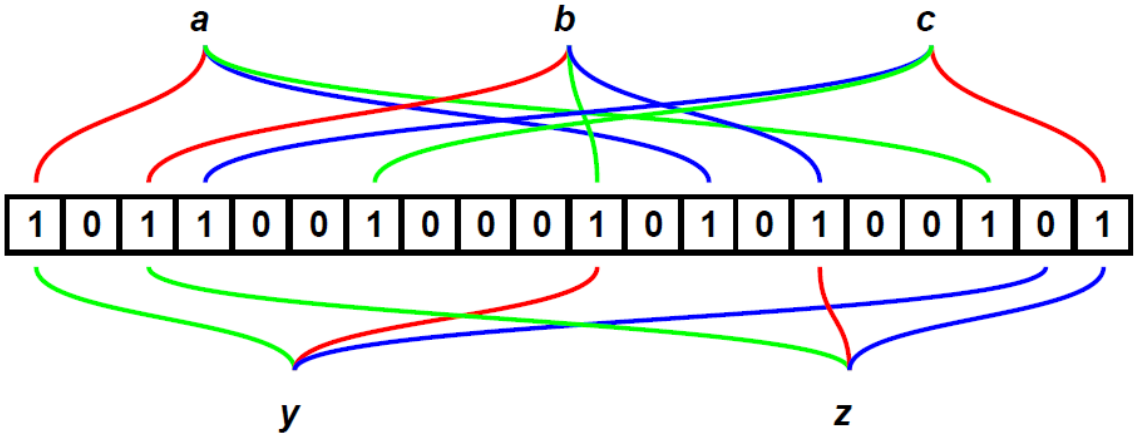
Zapory/IDPS w chmurze

- Problem poufności polityki bezpieczeństwa (otwarte porty, zagrożenia przed którymi chroni się klient, rodzaje i wersje oprogramowania, godziny pracy systemów, itp.)
- Anonimizacja polityki bezpieczeństwa
- Oznaczanie pakietów



Anonimizacja polityki bezpieczeństwa

- Zgrubne filtrowanie (filtry Blooma)



- False positives

Szyfrowanie homomorficzne

- Wykonywanie operacji na szyfrogramach
- Prosty przykład (RSA):

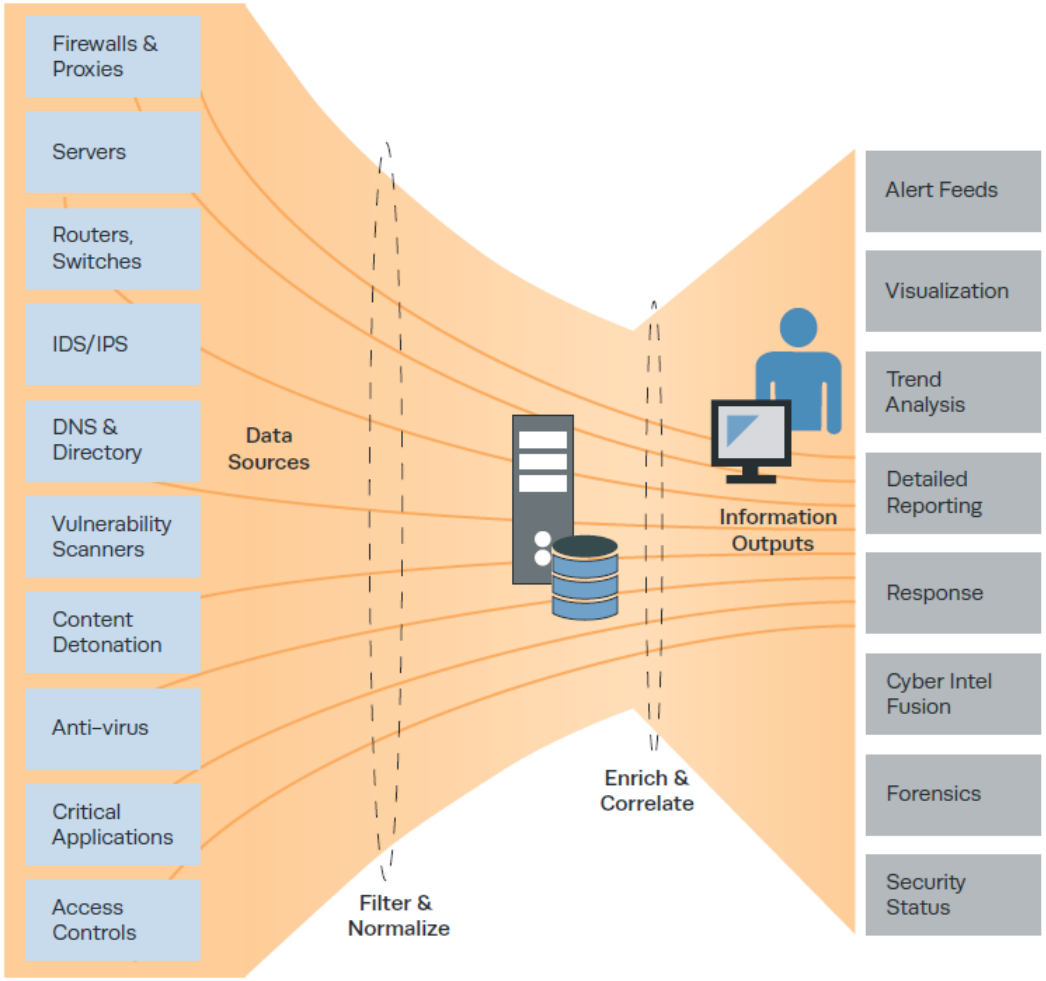
$$C_1 = M_1^e \bmod n$$

$$C_2 = M_2^e \bmod n$$

$$C_1 C_2 = M_1^e M_2^e \bmod n = (M_1 M_2)^e \bmod n$$

SIEM (*Security Information and Event Management*)

- Centralny system wykrywania zagrożeń
- Informacje z wielu urządzeń i systemów
- Korelacja zdarzeń w sieci



Źródło: C. Zimmerman: "Ten Strategies of a World-Class Cybersecurity Operations Center"

SIEM (przykłady)

- SIEM (*Security Information and Event Management*)
  - Splunk Enterprise Security
  - IBM Qradar
  - OSSIM
  - ELK Stack (Elastic Stack)

Bezpieczeństwo systemu

- firewall
- uwierzytelnianie
- kontrola dostępu
- antywirus
- IDPS
- wykrywanie anomalii
- SIEM
- honey pot
- …

To wszystko może być niewiele warte bez rozsądnego administratora

Podsumowanie

- Warstwy ochrony
- Zapora sieciowa
- Systemy IDPS
- Sposoby wykrywania zagrożeń/włamań
- Inne rozwiązania bezpieczeństwa

Myśl przewodnia…

Podstawowe sposoby wykrywania włamań/zagrożeń to:

- porównanie do wzorca ataku/zagrożenia (*podobieństwo świadczy o zagrożeniu*) oraz
- porównanie do typowego ruchu (*różnica może świadczyć o ataku*).

AKADEMIA GÓRNICZO-HUTNICZA
IM. STANISŁAWA STASZICA W KRAKOWIE

Dziękuję za uwagę!

Snort: Reguły

- Przykład:

```
alert tcp $EXTERNAL_NET 27374 -> $HOME_NET any (msg:"BACKDOOR
   subseven 22"; flags: A+; content: "|0d0a5b52504c5d3030320d0a|";
   reference:arachnids,485;
   reference:url,www.hackfix.org/subseven/; sid:103;
   classtype:misc-activity; rev:4;)
```

- Część przed nawiasem to „nagłówek reguły”
- Część w nawiasie to „opcje reguły”

Snort: Reguły

```
alert tcp $EXTERNAL_NET 27374 -> $HOME_NET any (msg:"BACKDOOR
   subseven 22"; flags: A+; content:
   "|0d0a5b52504c5d3030320d0a|"; reference:arachnids,485;
   reference:url,www.hackfix.org/subseven/; sid:103;
   classtype:misc-activity; rev:4;)
```

- `alert` action to take; also **`log, pass, activate, dynamic`**
- `tcp` protocol; also **`udp, icmp, ip`**
- `$EXTERNAL_NET` source address; this is a variable – specific IP is ok
- `27374` source port; also **`any`**, negation (**`!21`**), range (**`1:1024`**)
- `->` direction; best not to change this, although **`<>`** is allowed
- `$HOME_NET` destination address; this is also a variable here
- `any` destination port

Snort: Reguły

```
alert tcp $EXTERNAL_NET 27374 -> $HOME_NET any (msg:"BACKDOOR
   subseven 22"; flags: A+; content:
   "|0d0a5b52504c5d3030320d0a|"; reference:arachnids,485;
   reference:url,www.hackfix.org/subseven/; sid:103;
   classtype:misc-activity; rev:4;)
```

- **msg:"BACKDOOR subseven 22";** message to appear in logs
- **flags: A+;** tcp flags; many options, like `SA, SA+, !R, SF*`
- **content: "|0d0…0a|";** binary data to check in packet; content without | (pipe) characters do simple content matches
- **reference…;** where to go to look for background on this rule
- **sid:103;** rule identifier
- **classtype: misc-activity;** rule type; many others
- **rev:4;** rule revision number

Snort: Przykłady

- drop icmp any any -> any any
- alert ip any any -> any any (msg: "IP Packet detected";)
- alert icmp any any -> any any (msg: "ICMP Packet found";)
- alert icmp 192.168.1.4 any -> 192.168.1.1 any (msg: "HEARTBEAT";)
- alert tcp 192.168.1.0/24 any -> ![192.168.1.0/24] any (content: "GET"; msg: "GET matched";)