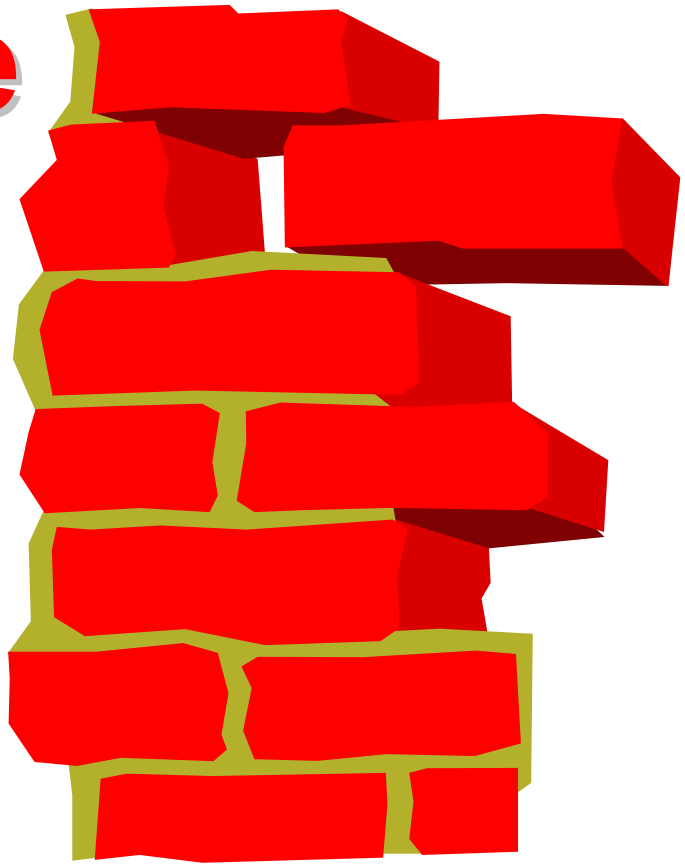
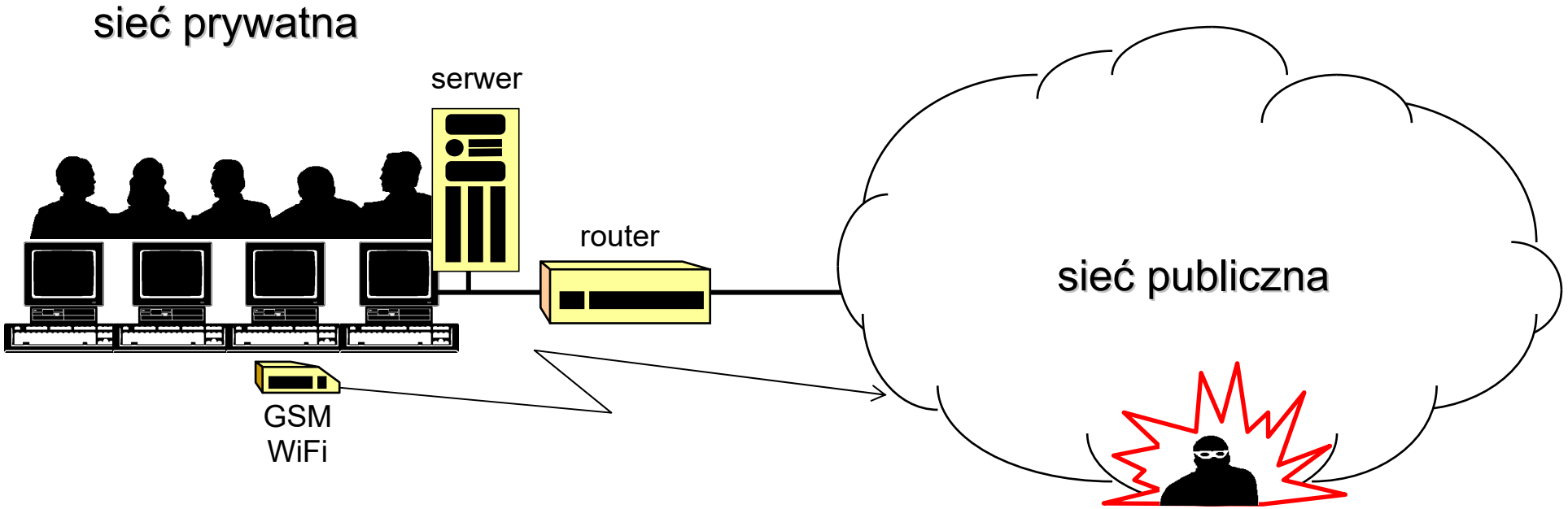
Zapory sieciowe (firewall) i translacja adresów



Zagadnienia

1. Filtracja pakietów
2. Bramy aplikacyjne
3. Translacja adresów
4. Funkcjonalność współczesnych zapór sieciowych

Scenariusz



Firewall

Zapora czy ściana przeciwogniowa?

Def.: **fire wall** – ognioodporny mur używany jako zapora zapobiegająca rozprzestrzenianiu się ognia.

Słownik dziedzictwa amerykańskiego

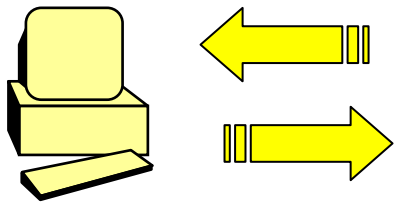
Zapory sieciowe

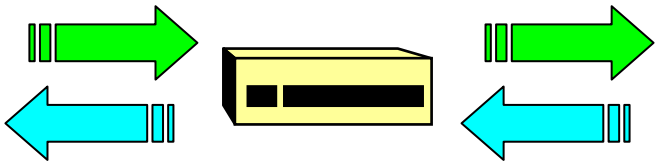
Podstawowe funkcje systemów firewall:

1. Filtracja pakietów

- warstwa 3 (+ 4) modelu OSI

1. Filtracja pakietów nadchodzących
2. Filtracja pakietów wychodzących
3. Filtracja pakietów propagowanych (routing)



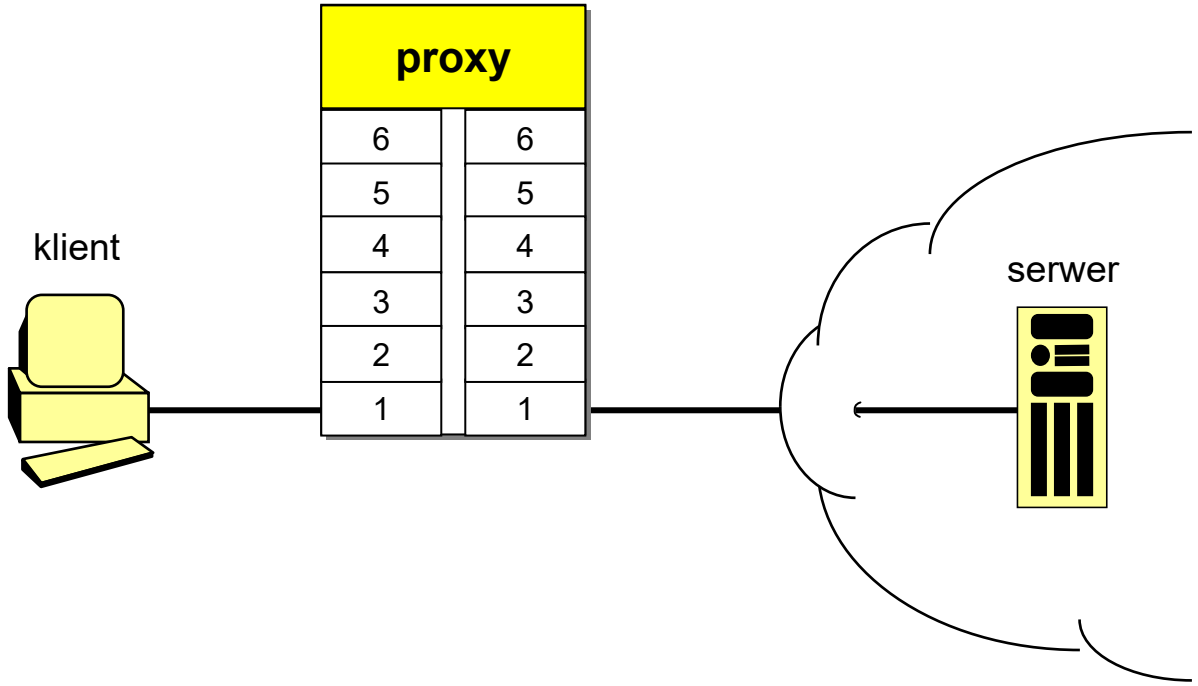


Zapory sieciowe

Podstawowe funkcje systemów firewall:

2. Brama aplikacyjna (Application Layer Gateway, ALG)

- aplikacje pośredniczące (*proxy*) w komunikacji aplikacji (OSI L7)



Zapory sieciowe

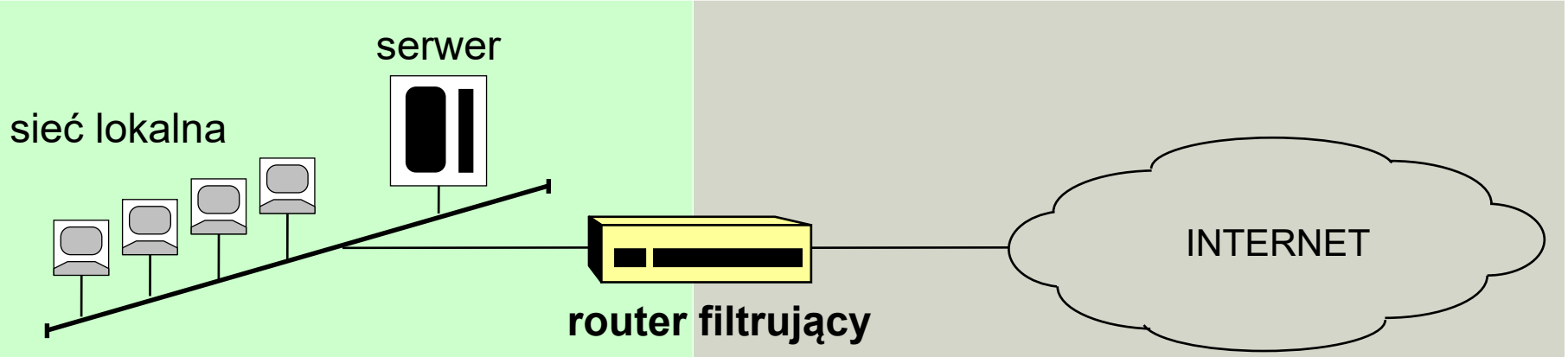
Podstawowe komponenty systemów firewall:

1. **Specjalizowany węzeł międzysieciowy (router)**
   - rozwiązanie najprostsze i najłatwiejsze w utrzymaniu
     - router filtrujący (*screening router*)
     - router szyfrujący (*ciphering router*)
2. **Komputer Twierdza** (*Bastion Host*)
3. **Strefa Zdemilitaryzowana** (*Demilitarized Zone – DMZ*)

Router filtrujący

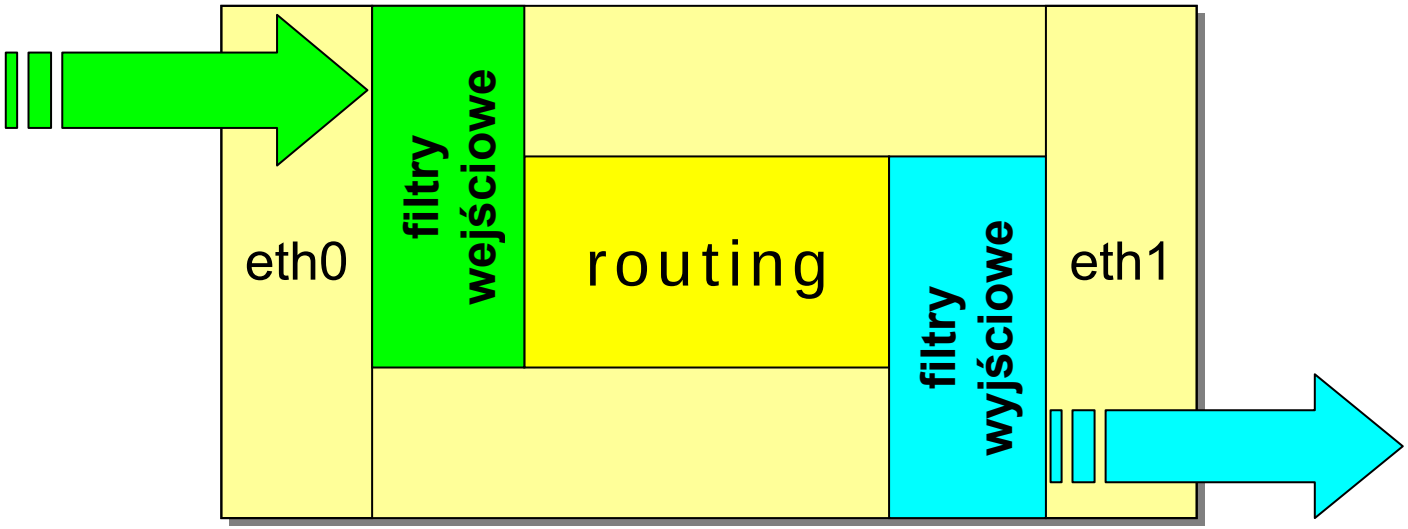
Reguły filtracji

- operują na parametrach analizowanych pakietów, takich jak:
  - adresy z nagłówka protokołu sieciowego (źródłowy i docelowy)
  - typ protokołu (PDU i SDU, np. protokołu transportowego)
  - rodzaj usługi (numer portu z nagłówka protokołu transportowego)



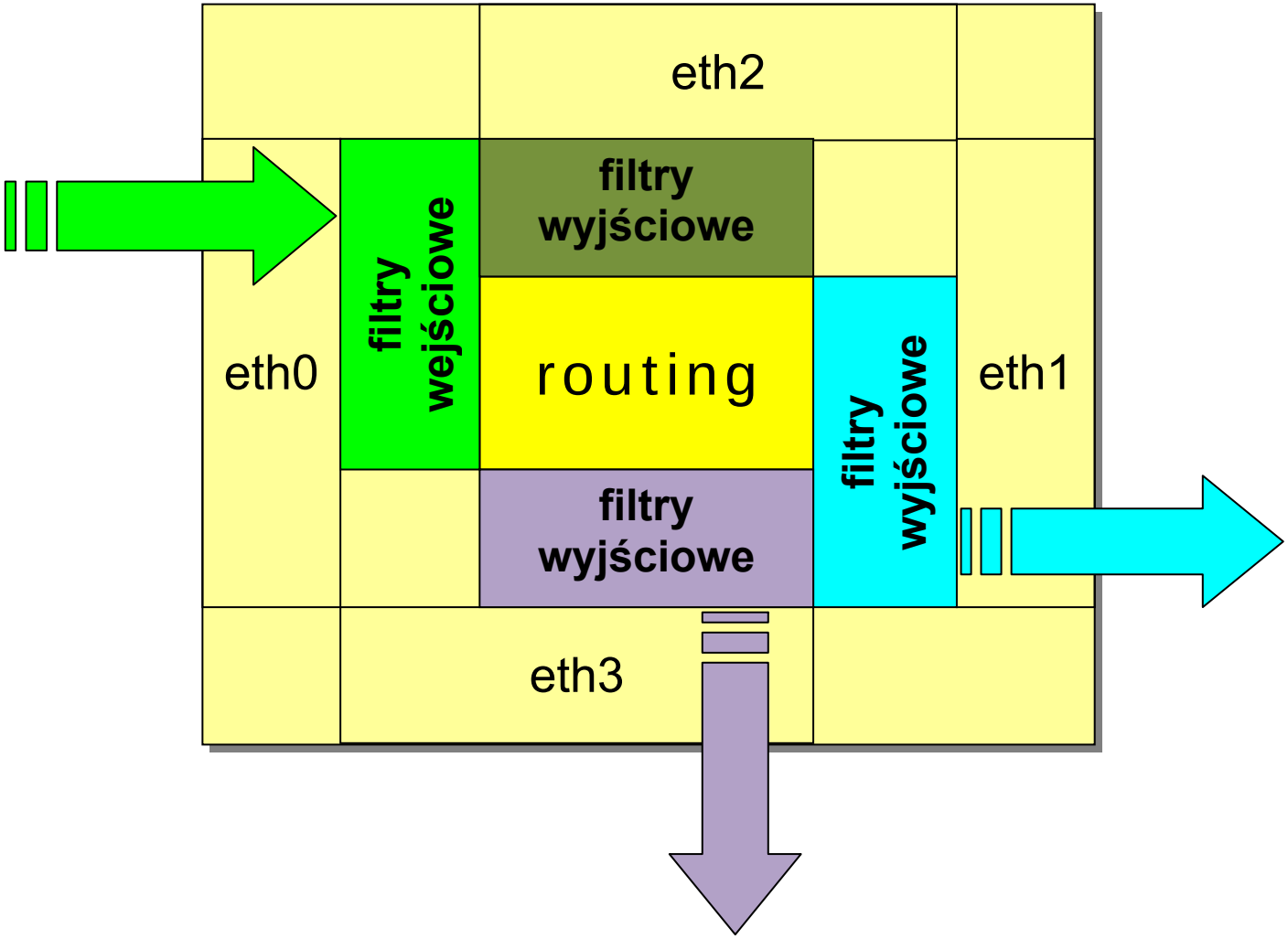
Router filtrujący

Model filtracji



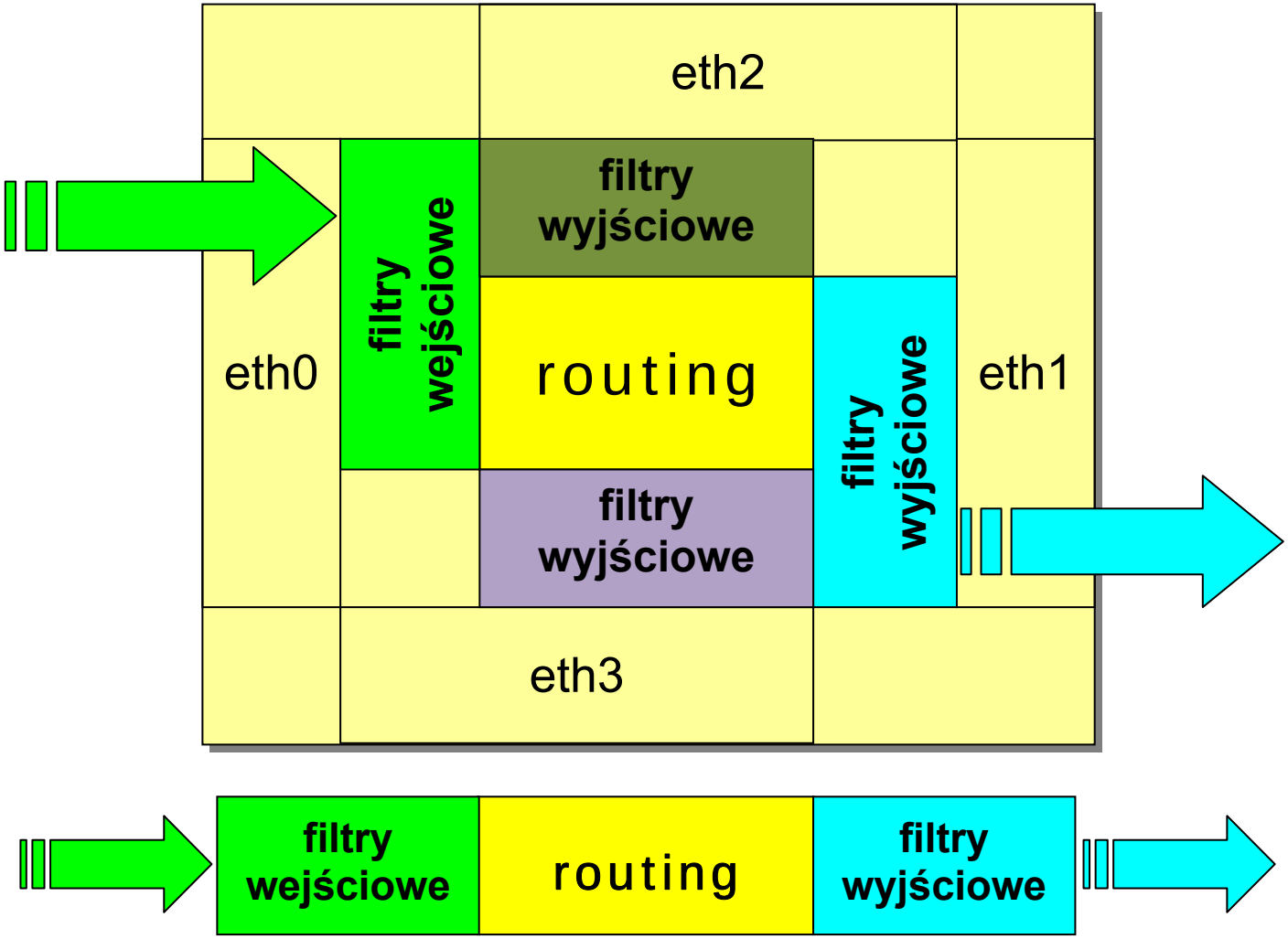
Router filtrujący

Model filtracji



Router filtrujący

Model filtracji



Router filtrujący

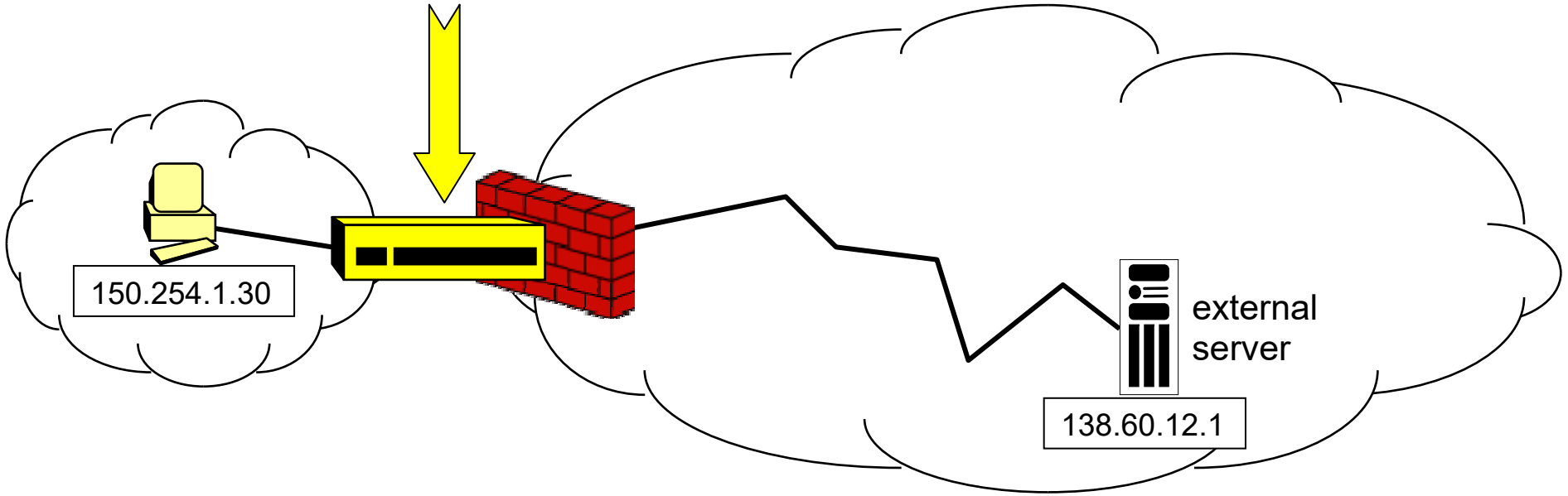
Filtry

- filtry statyczne
- filtry kontekstowe (dynamiczne reguły filtracji)
  - w trakcie pracy aktualizowane są informacje o bieżących sesjach (asocjacjach protokołu sieciowego)
  - decyzje o filtracji pakietów podejmowane są z uwzględnieniem stanu sesji, do której przynależą
- filtracja nieliniowa:
  - elastyczne definiowanie wyrażeń warunkowych (zagnieżdżone reguły logiczne)

Router filtrujący

Statyczne reguły filtracji

reguła	kierunek ruchu	nadawca pakietu	odbiorca pakietu	protokół transportowy	port nadawcy	port odbiorcy	flagi	działanie
1.	na zewnątrz	150.254.*.*	138.60.12.1	TCP	*	80	*	przepuść
2.	do wewnątrz	138.60.12.1	150.254.*.*	TCP	80	*	ACK=1	przepuść
3.	do wewnątrz	138.60.12.1	150.254.*.*	TCP	80	*	ACK=0	odrzuć
4.	*	*.*.*.*	*.*.*.*	*	*	*	*	odrzuć

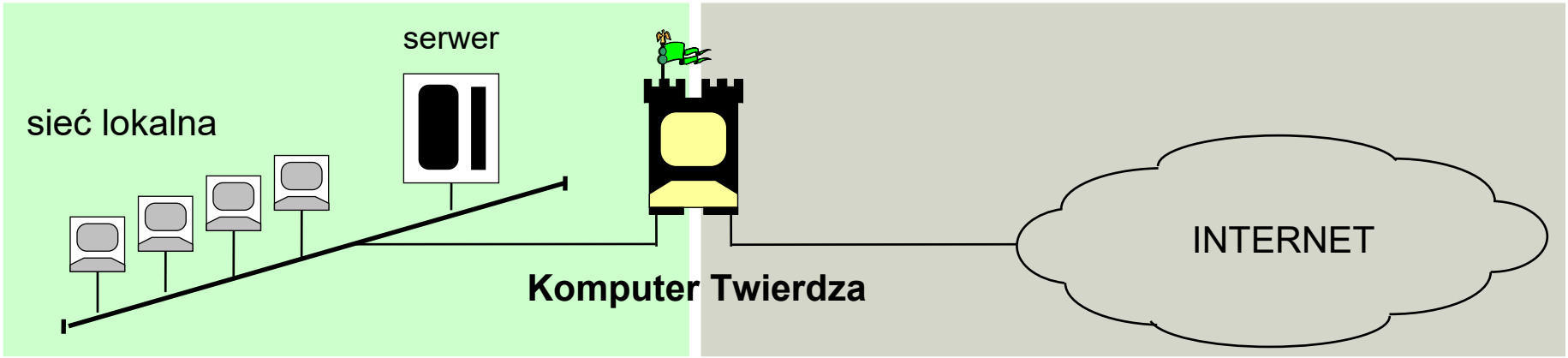


Router filtrujący

Statyczne reguły filtracji

- niektóre usługi/protokoły trudno poddają się filtracji statycznej (np. FTP, X11, DNS)
- dlatego wprowadza się i stosuje tryby pracy zmodyfikowane pod kątem usprawnienia filtracji, np. tryb *passive* w protokole FTP

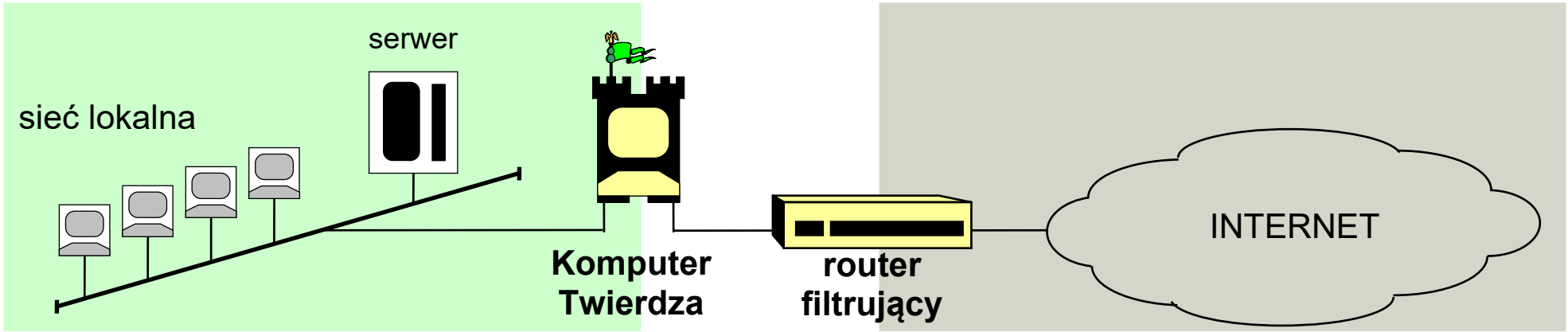
Komputer Twierdza



Komputer z odseparowanymi interfejsami sieciowymi (*Dual-Homed Host Gateway*)

- fizyczna i logiczna separacja prywatnej sieci lokalnej od zewnętrznej sieci publicznej
- tylko Komputer Twierdza jest widoczny z sieci publicznej
- aby wtargnąć do sieci prywatnej trzeba uprzednio zawładnąć Komputerem Twierdzą
- brama aplikacyjna – *proxy* rozwiązuje problem usług trudnych do filtracji
- rejestracja zdarzeń (*auditing*)

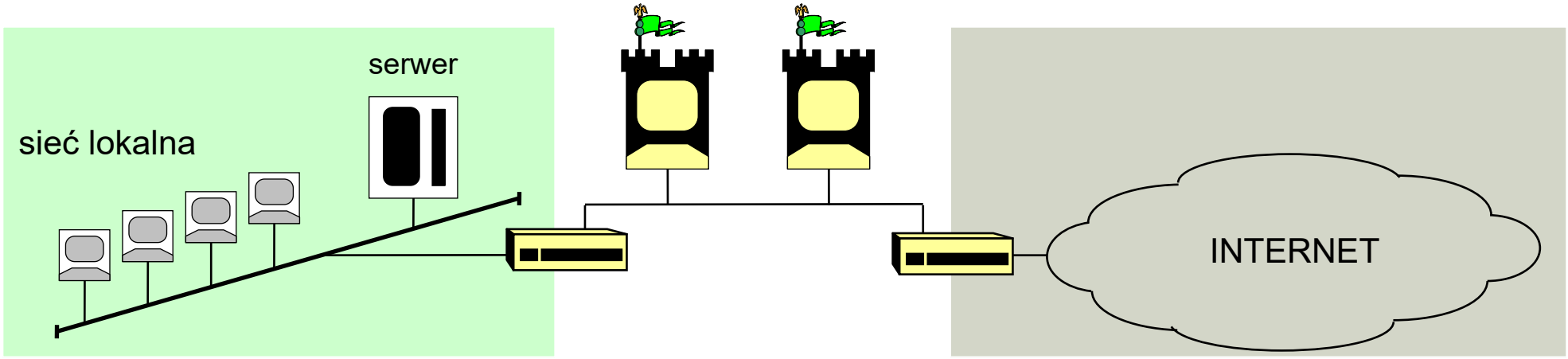
Filtracja podwójna



- brama aplikacyjna poprzedzona routerem filtrującym (*Screened Host Gateway*)

Podsieć ochronna

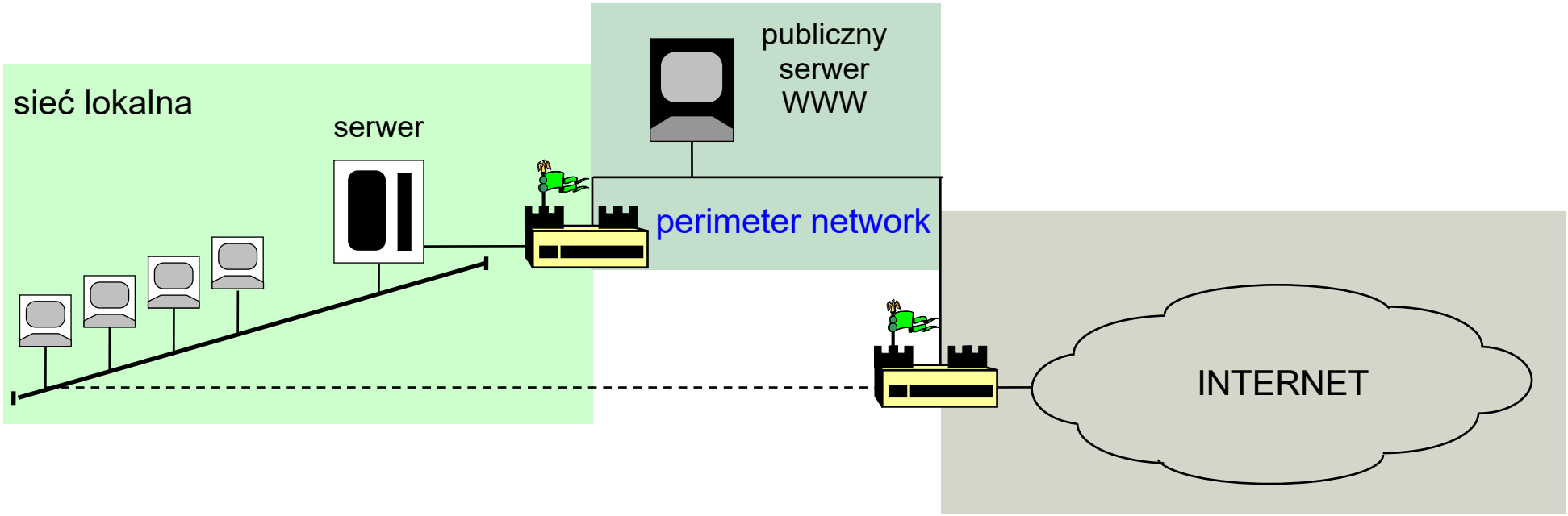
- „rozciągnięcie” Twierdzy na całą dedykowaną podsieć (*Screened Network*)



- ... a nawet kaskadę podsieci
- ... jeśli ktoś naprawdę czuje taką potrzebę

Strefa Zdemilitaryzowana

- Strefa Zdemilitaryzowana (DMZ) – wydzielona podsieć zawierająca komponenty świadomie (!) wyjęte spod kontroli obejmującej całą resztę sieci wewnętrznej, np.:
  - publiczne zasoby (np. ogólnodostępny serwis WWW)
  - przynęty, pułapki



- Strefę Zdemilitaryzowaną należy dobrze kontrolować!

Translacja adresów

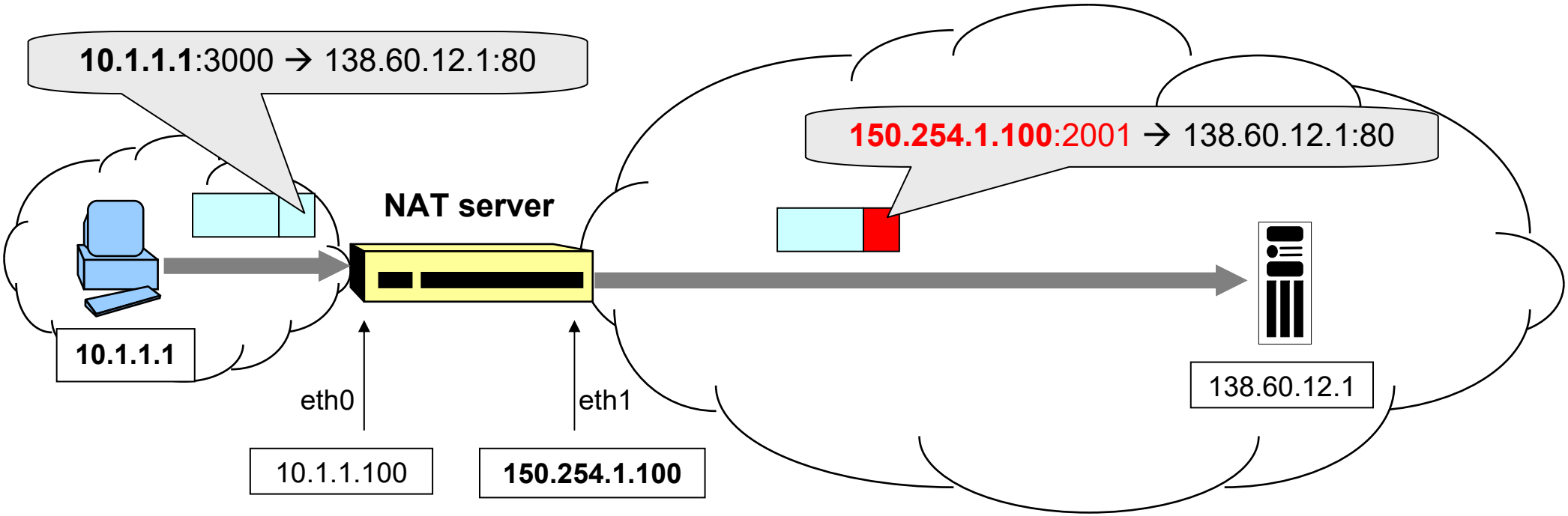
Network Address Translation (NAT)

- rozszerzenie dostępu do sieci publicznej na stanowiska nieposiadające adresów publicznych (adresy prywatne – RFC 1918)
- ukrycie wewnętrznej struktury sieci przed światem zewnętrznym
- przekierowanie portów (NAPT = *Network Address & Port Translation*)
- RFC1631 (translacja na pojedynczy adres, tj. N:1)
- RFC1597,1918 (translacja na pulę adresową, tj. N:M)

Translacja adresów źródłowych (SNAT)

Source NAT (SNAT)

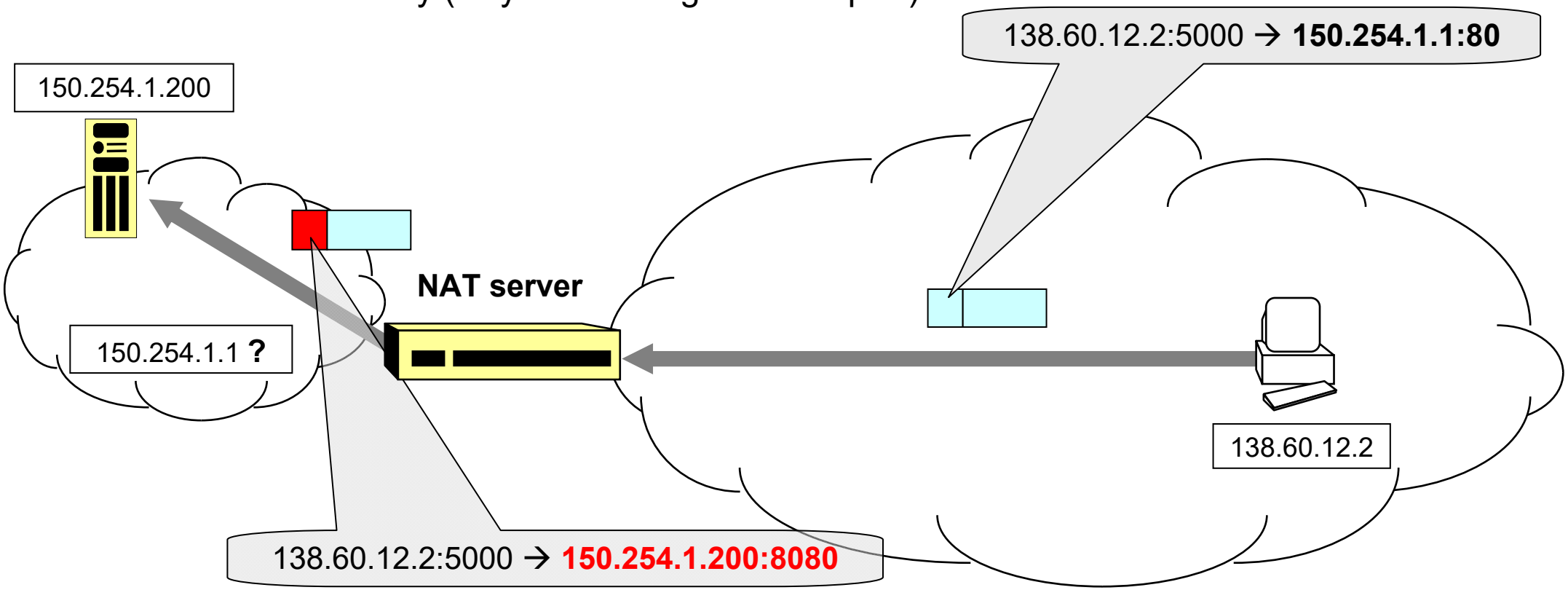
- pakiety wychodzące z sieci wewnętrznej otrzymują nowy adres źródłowy w nagłówku



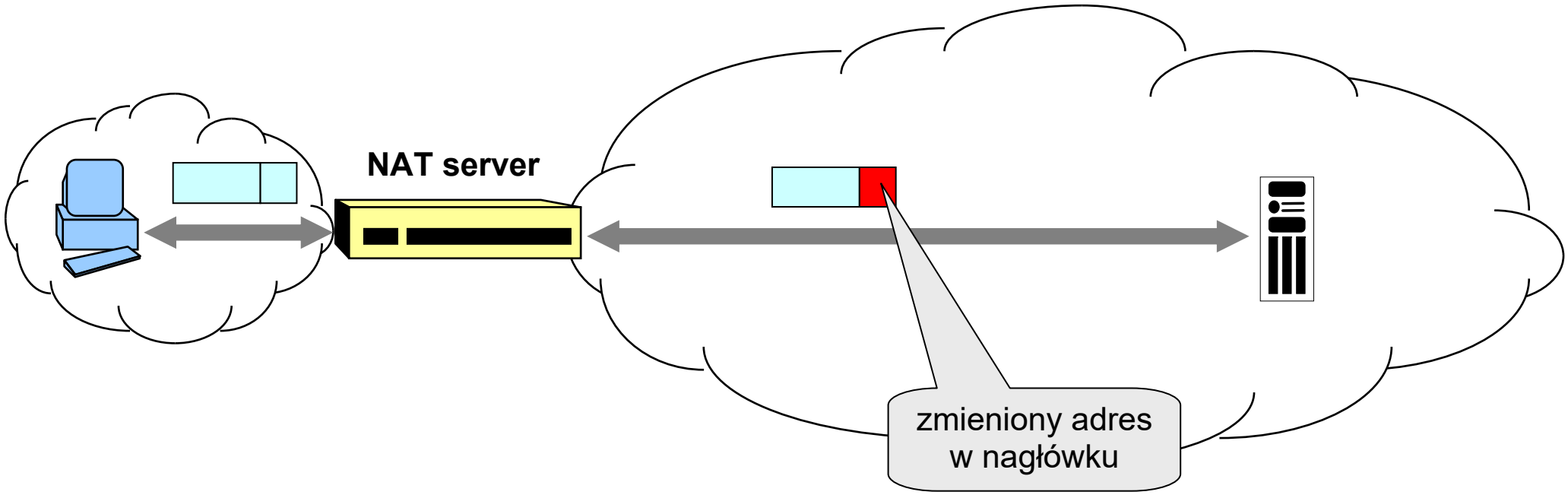
Translacja adresów docelowych (DNAT)

Destination NAT (DNAT)

- pakiety przychodzące ze strony inicjującej (na ogół – sieci zewnętrznej) otrzymują nowy adres docelowy (w tym w szczególności – port)



NAT + VPN



- IPsec w trybie transportowym (bezpośrednim)? NAT modyfikuje nagłówek datagramu!
- IPsec ESP – gdzie jest numer portu do translacji?
- IKE/ISAKMP – jaka jest tożsamość stron tunelu?

→ NAT-T (RFC 3947), STUN (RFC 5389), ICE (RFC 8445)

Dodatkowa funkcjonalność

Łańcuch funkcji:

funkcje podstawowe:

funkcje dodatkowe:

- wykrywanie i rejestrowanie prób ataków na chronione systemy

Dodatkowa funkcjonalność

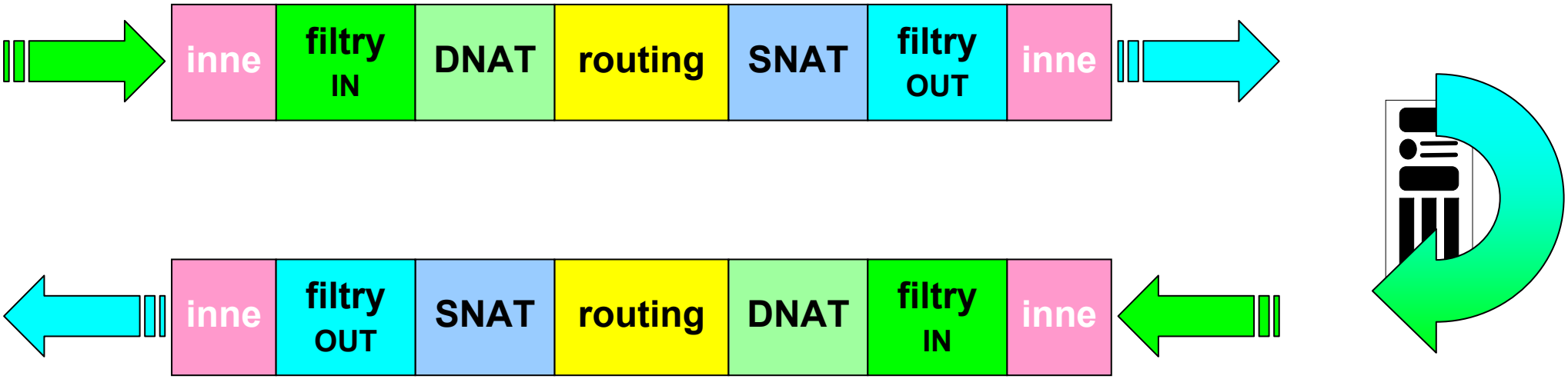
Funkcje dodatkowe:

- obrona przed atakami DoS (*flood-wall*) – specyfikowanie dopuszczalnego rozmiaru strumienia wejściowego (np. w pakietach na sek.)
- kontrola fragmentacji IP, poprawności segmentów TCP, SCTP
- IPv6, rozpoznawanie tunelowania IPv6 w IPv4 (6to4, 6over4, Toredo,...), ICMPv6, ...
- integracja z różnymi zewnętrznymi modułami, np. systemami antywirusowymi, modułami sieciowej detekcji intruzów (NIDS), czy kontroli treści i ograniczenia dostępu (np. *parental control*)

Dodatkowa funkcjonalność

Filtry statyczne (bezstanowe)

Round-trip – standardowy przepływ:



Dodatkowa funkcjonalność

Filtry kontekstowe

SPF = *Stateful Packet Filtering* (SPI = *Stateful Packet Inspection*):

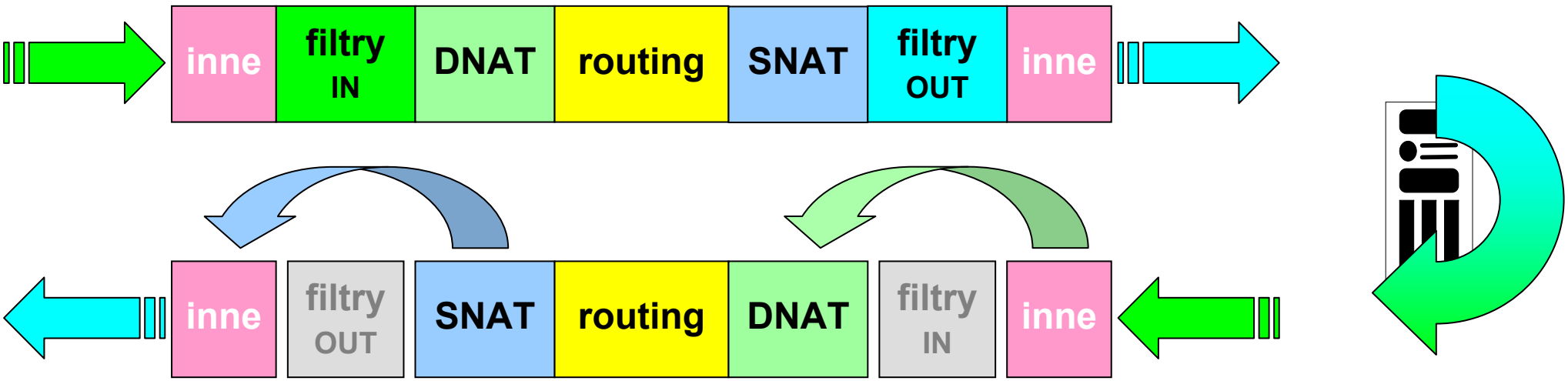
- każda zainicjowana poprawnie sesja jest pamiętana na dynamicznych listach
- pakiet jest weryfikowany z uwzględnieniem przynależności do istniejącej sesji
- co ułatwia filtrację trudnych pakietów (czyli innych niż SYN, SYN/ACK)
- i obsługę protokołów wielopołączeniowych (np. wychwycenie polecenia PORT w połączeniu kontrolnym FTP pozwala dynamicznie odblokować żądany port dla połączenia danych)

Dodatkowa funkcjonalność

Filtry kontekstowe

Round-trip z SPF:

- w drodze powrotnej pakiet jest sprawdzany na przynależność do zapamiętanej sesji
  – filtracja może być pominięta:



Problemy

Problemy technologiczne:

- dynamiczne reguły:
  - filtr kontekstowy zapory widzi komendę PORT protokołu FTP i otwiera żądany port
  - wymuszanie otwierania portów → *protocol smuggling*:

    URL: `http://nice.server.lan:21/\nPORT 150.254.32.1.122.105`

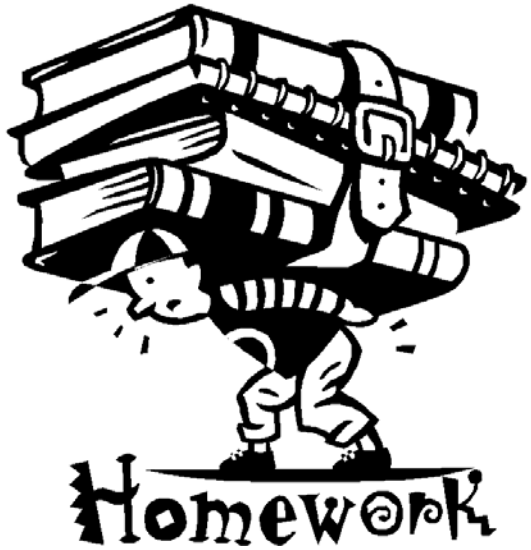
    może otworzyć port 31337

Problemy

Problemy technologiczne:

- fragmentacja IP:
  - odrzucanie tylko pierwszych fragmentów umożliwia wyciek informacji w strumieniu wyjściowym
  - istnieją narzędzia do tak perfidnego fragmentowania, by flagi ACK i SYN nagłówka TCP nie pojawiały się w pierwszym fragmencie
  - można scalać fragmenty na zaporze – uwaga na błędy przy scalaniu!
  - można narzucić wymóg, aby pierwszy fragment zawierał co najmniej 16B danych (a najlepiej cały nagłówek TCP)

Problemy



Firewalking

- zapory często w praktyce czasami przepuszczają pewne pozornie nieszkodliwe protokoły (np. ICMP, DNS)
- umożliwiające wykrywanie składników sieci poza zaporami
- np. zmodyfikowanym *traceroute*:
  - seria pakietów o coraz wyższym TTL pozwala ostatecznie określić ilość przeskoków do zapory
  - po osiągnięciu zapory zwiększa się numer portu UDP tak długo aż osiągnie się taki, który zapora przepuści (np. 53)
  - a nawet pozwala dalej sondować adresy/porty za zaporą

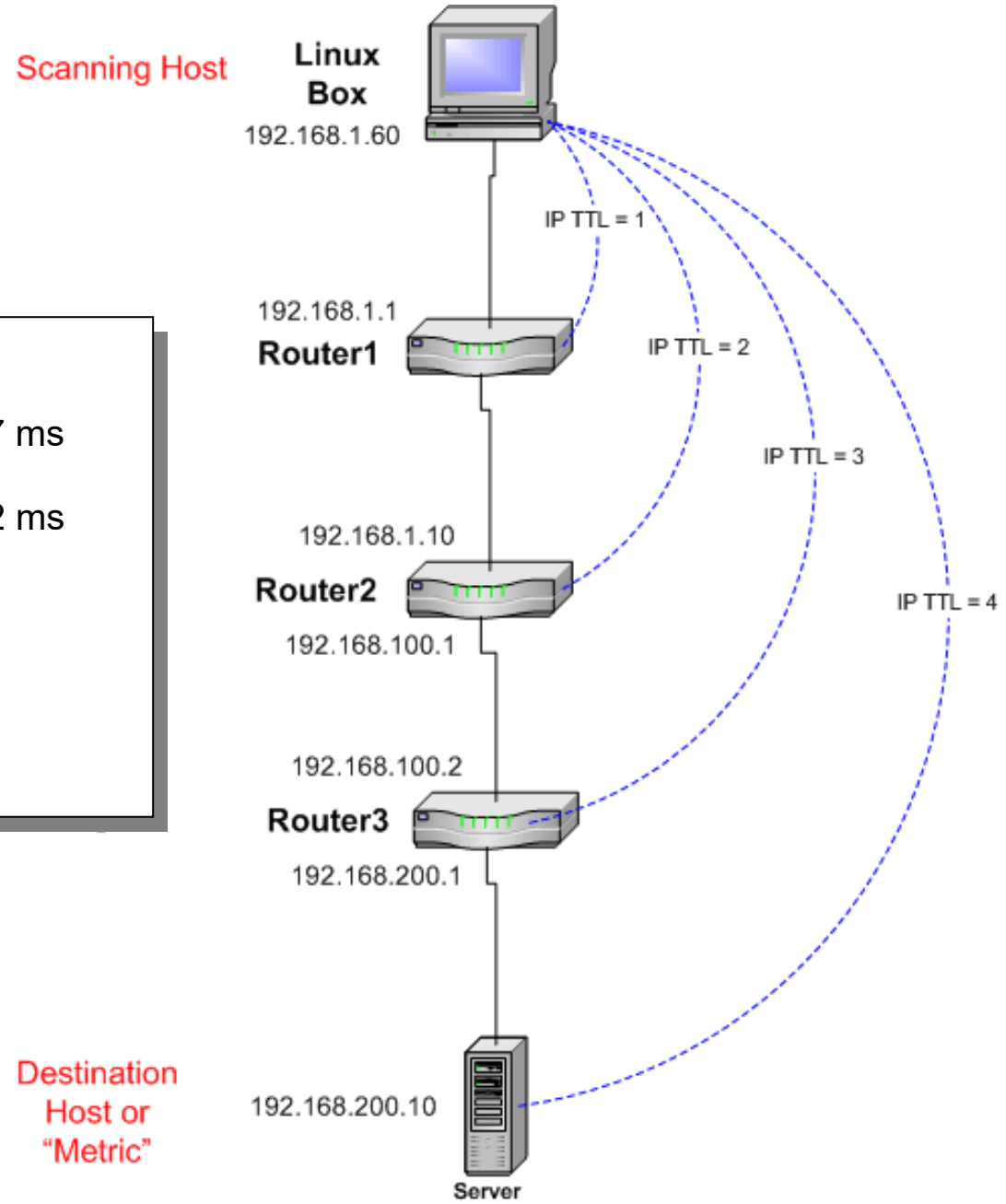
```
# traceroute 192.168.200.10

1     192.168.1.1      0.540 ms 0.394 ms 0.397 ms

2     192.168.1.10     2.455 ms 2.479 ms 2.512 ms

3     * * *

4     * * *
```



– Lori Hyde CCNA (za articles.techrepublic.com)

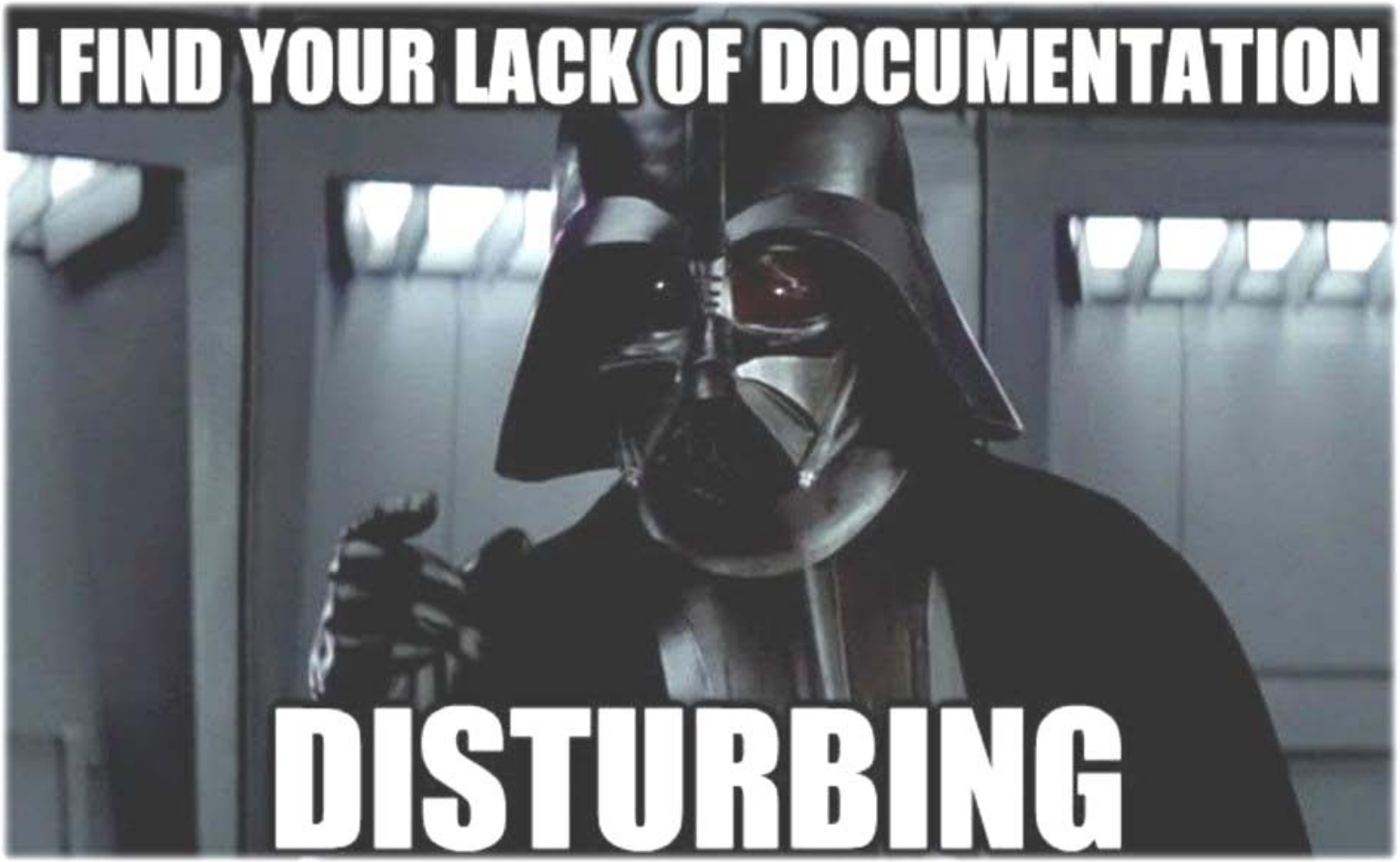
Problemy

Pielęgnacja reguł filtracji:

- duże zbiory reguł
- częste zmiany personelu
- brak dokumentacji – brak pielęgnacji starych reguł (odziedziczonych po poprzednim administratorze)
- problemy wewnętrzne: duże organizacje – złożona polityka bezpieczeństwa – wielość nachodzących na siebie domen bezpieczeństwa

Problemy

Pielęgnacja reguł filtracji:



Problemy

Ostrożnie z tunelami:

- autoryzowane tunele VPN mogą być potencjalnym nośnikiem nieautoryzowanych treści poza kontrolą zapór ogniowych
- również propagowanie połączeń (*port forwarding*) może prowadzić do omijania kontroli na zaporze
- WebServices i protokół SOAP tunelowany w HTTP
- czy IPP (*Internet Printing Protocol*) przepuszczany przez port 80 zamiast 631
- skrajnie wywrotowe *httptunnel* czy *dns2tcp*

Problemy

Ostrożnie z tunelami:

IPsec + firewall

- definicja reguł filtracji musi uwzględniać konieczność przepuszczania protokołów ESP (nr 50) i AH (nr 51) oraz ISAKMP (port 500/udp)

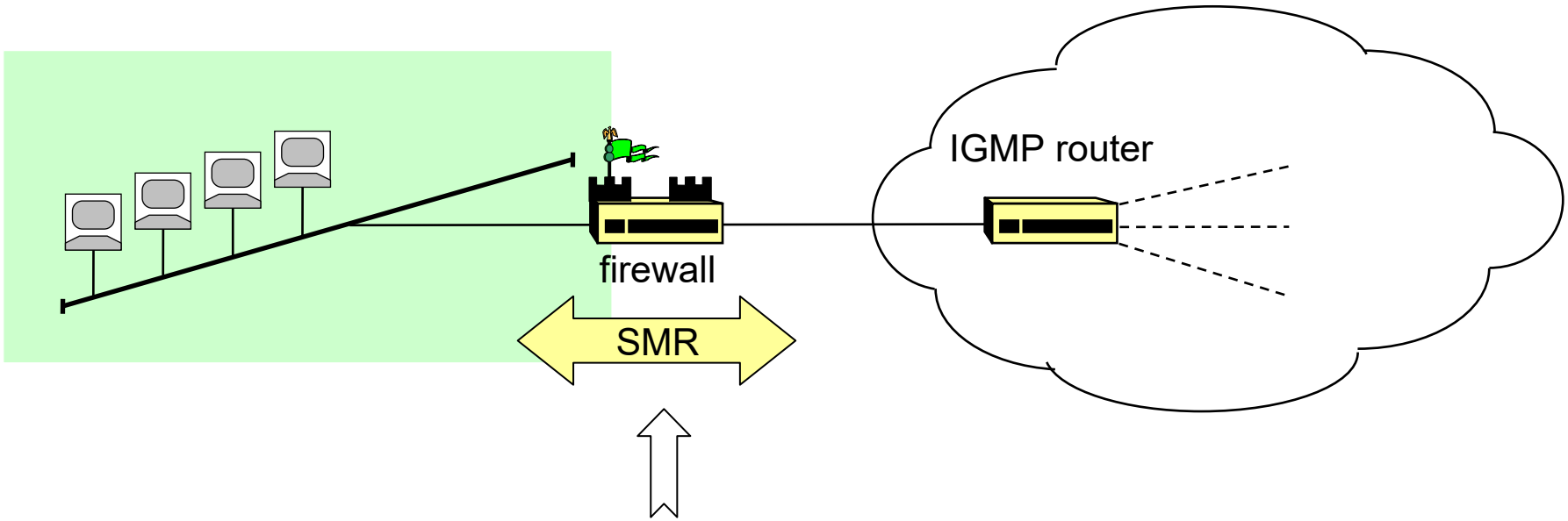
Podobnie:

- przy uwierzytelnianiu protokołem Kerberos (Windows AD) również porty 88/tcp i 88/udp
- i dla NAT-T port 4500/udp

Problemy

Multicast:

- blokowanie adresów klasy D uniemożliwi pracę np. RIPv.2 (adres 224.0.0.9)
- bezpieczne przepuszczanie ruchu IGMP wymaga tunelu (np. GRE) z routerem IGMP



- chyba że zapora jest jednocześnie proxy-agentem IGMP
  – protokół SMR (*Stub Multicast Routing*)

Problemy

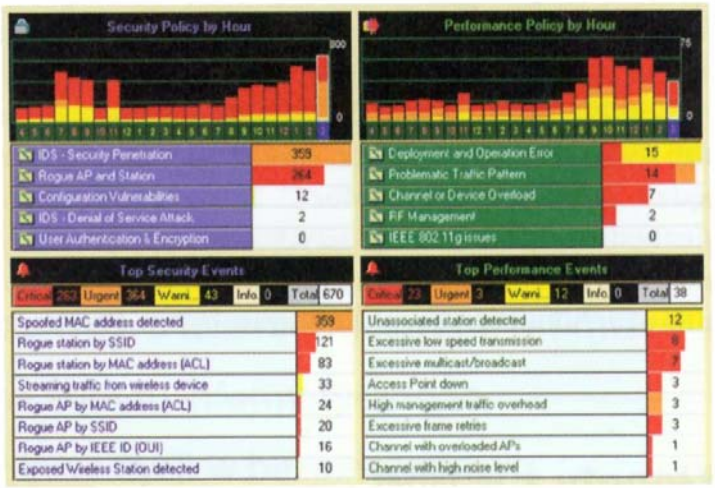
Routing źródłowy a Komputer Twierdza:

- Komputer Twierdza z usługami zastępczymi wymaga wyłączenia routingu w systemie operacyjnym
- niektóre jądra, mimo że zostaną skonfigurowane tak, by nie przekazywać pakietów, będą jednak i tak to robić dla pakietów z trasowaniem źródłowym
- rozwiązaniem może być ingerencja w kod źródłowy jądra (o ile dostępny) i całkowite usunięcie fragmentów odpowiedzialnych za przekazywanie pakietów

Problemy

Łączność bezprzewodowa:

- absolutnie poza kontrolą zapór stacjonarnych
- wymagane zamknięte grupy użytkowników
- lub skanowanie sieci w celu wykrycia intruzów
- WIDP (*Wireless Intrusion Detection & Prevention*)



Produkty

Klasa: Firewall

Typowe funkcje:

- filtracja pakietów IP
- komputer twierdza, proxy-services dla najpopularniejszych usług (ftp, mail, WWW)
- translacja adresów IP SNAT
- tunele VPN
- obrona przed atakami DoS/DDoS

Produkty

Przykłady

Filtry pakietów:

moduły lub funkcje systemu operacyjnego routerów, np. w Cisco IOS

dedykowane urządzenia filtrujące (tzw. *appliance*, np. Cisco ASA, Juniper IGS)

moduły jądra Linux (np. netfilter iptables/nftables), BSD (np. ipf/ipfw), BPF, eBPF

Systemy zintegrowane:

Firewall 1 (CheckPoint; SUN, Bay Networks)

Next Generation Firewall (PaloAlto Networks)

Gauntlet Firewall (Network Associates)

Raptor Firewall (Axent, Symantec)

NetScreen (NetScreen)

IPcop (freeware: http://www.ipcop.org)

m0n0wall (freeware: http://m0n0.ch/wall/, projekt zakończony)

Produkty

ASA = Adaptive Security Appliance (Cisco)

- NAT
- AAA (RADIUS, TACACS+)
- tunel VPN IPsec lub SSL
- funkcje TCP intercept: Flood Guard, IP Frag Guard, DNS Guard, Mail Guard, RFC 2827
- filtry URL i kontrola treści (script filtering)
- logging (syslog)
- obsługa konfiguracji lustrzanej w trybie *fail-over* (active/standby i active/active)

Produkty

ISG – Integrated Security Gateway (Juniper)

- wydajność zapory 4 Gb/s, do 30 000 polityk (zbiorów reguł)
- wydajność VPN 2 Gb/s (3DES/AES), do 10 000 tuneli
- moduł IDS/IPS
- zintegrowany Web Filtering, możliwość kooperacji z zewnętrznym modułem (Redirected Web Filtering)
- konfiguracje zreplikowane i równoległe (active/passive, active/active, full mesh)

Produkty

SRX Series Services Gateways (Juniper)

- wydajność zapory 120 Gb/s, do 80 000 polityk (zbiorów reguł)
- wydajność VPN 30 Gb/s (3DES+SHA-1/AES-256)
- moduł IDS/IPS 30 Gb/s
- intensywność strumienia nowych połączeń (3-way handshake): 350 000 /s
- SYN cookies
- TCP reassembly (fragmented packet protection)
- protocol anomaly detection (zero-day coverage)
- ☺ moc zasilania do 5 kW

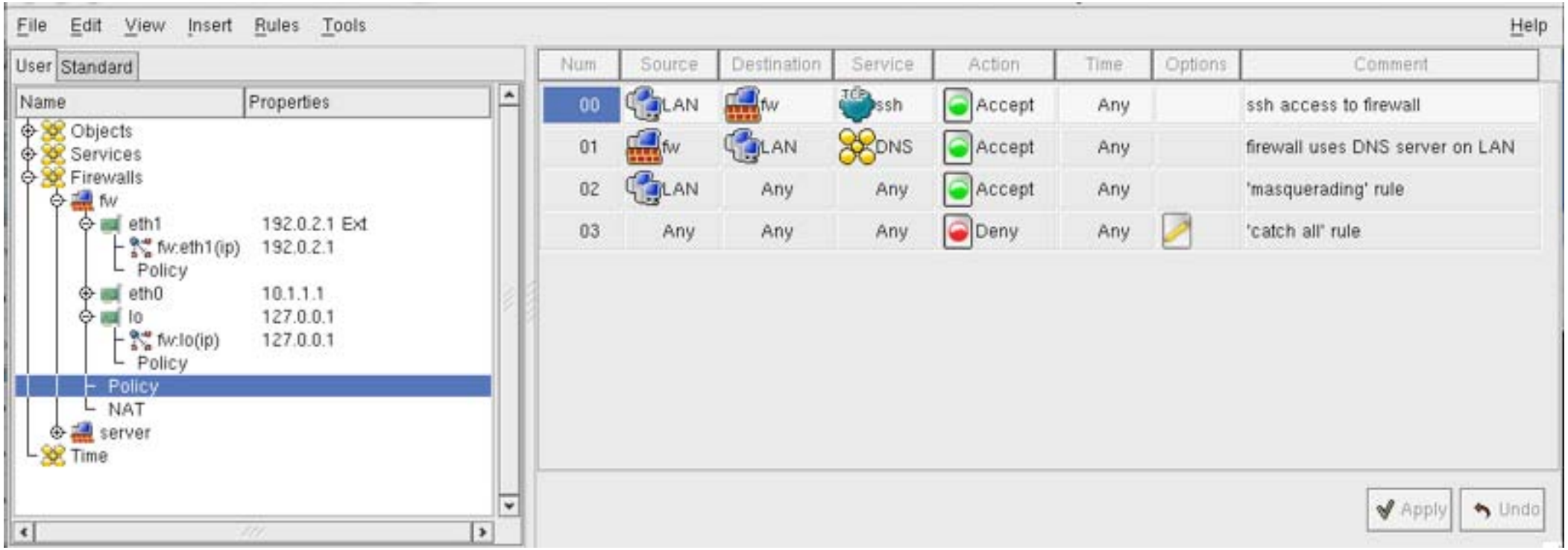
Produkty

PaloAlto Next-Generation Firewalls

Produkty

Generatory reguł filtracji:

Cisco PIX Device Manager, SuSE firewall, Firestarter, Firewall Builder ...



Produkty

iptables script:

```
echo 30 > /proc/sys/net/ipv4/tcp_fin_timeout
echo 1800 > /proc/sys/net/ipv4/tcp_keepalive_intvl

IPTABLES="/sbin/iptables"

$IPTABLES -P OUTPUT  DROP
$IPTABLES -P INPUT   DROP
$IPTABLES -P FORWARD DROP

$IPTABLES -A INPUT   -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A OUTPUT  -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

# Anti-spoofing rule
$IPTABLES -N eth1_In_RULE_0
$IPTABLES -A INPUT  -i eth1  -s 192.0.2.1  -j eth1_In_RULE_0
$IPTABLES -A INPUT  -i eth1  -s 10.1.1.1  -j eth1_In_RULE_0
$IPTABLES -A INPUT  -i eth1  -s 10.1.1.0/24  -j eth1_In_RULE_0
$IPTABLES -A FORWARD  -i eth1  -s 192.0.2.1  -j eth1_In_RULE_0
$IPTABLES -A FORWARD  -i eth1  -s 10.1.1.1  -j eth1_In_RULE_0
$IPTABLES -A FORWARD  -i eth1  -s 10.1.1.0/24  -j eth1_In_RULE_0
$IPTABLES -A eth1_In_RULE_0 -j LOG --log-level info --log-prefix "RULE 0 DENY"
$IPTABLES -A eth1_In_RULE_0 -j DROP
 . . .
```

Produkty

Cisco ASA script:

```
nameif eth0 inside security0
nameif eth1 outside security1

timeout conn 1:0:0
timeout udp 0:2:0
timeout h323 0:5:0

clear access-list
clear icmp
clear object-group

! Anti-spoofing rule
access-list outside_acl  remark 0(outside)
access-list outside_acl deny   ip host 192.0.2.1 any
access-list outside_acl deny   ip host 10.1.1.1 any
access-list outside_acl deny   ip 10.1.1.0 255.255.255.0 any

access-list outside_acl  remark 1(global)
access-list outside_acl permit tcp host 192.0.2.1 10.1.1.0 255.255.255.0 eq 53
access-list inside_acl  remark 1(global)
access-list inside_acl permit tcp host 10.1.1.1 10.1.1.0 255.255.255.0 eq 53
access-list outside_acl permit udp host 192.0.2.1 10.1.1.0 255.255.255.0 eq 53
access-list inside_acl permit udp host 10.1.1.1 10.1.1.0 255.255.255.0 eq 53
 . . .
```

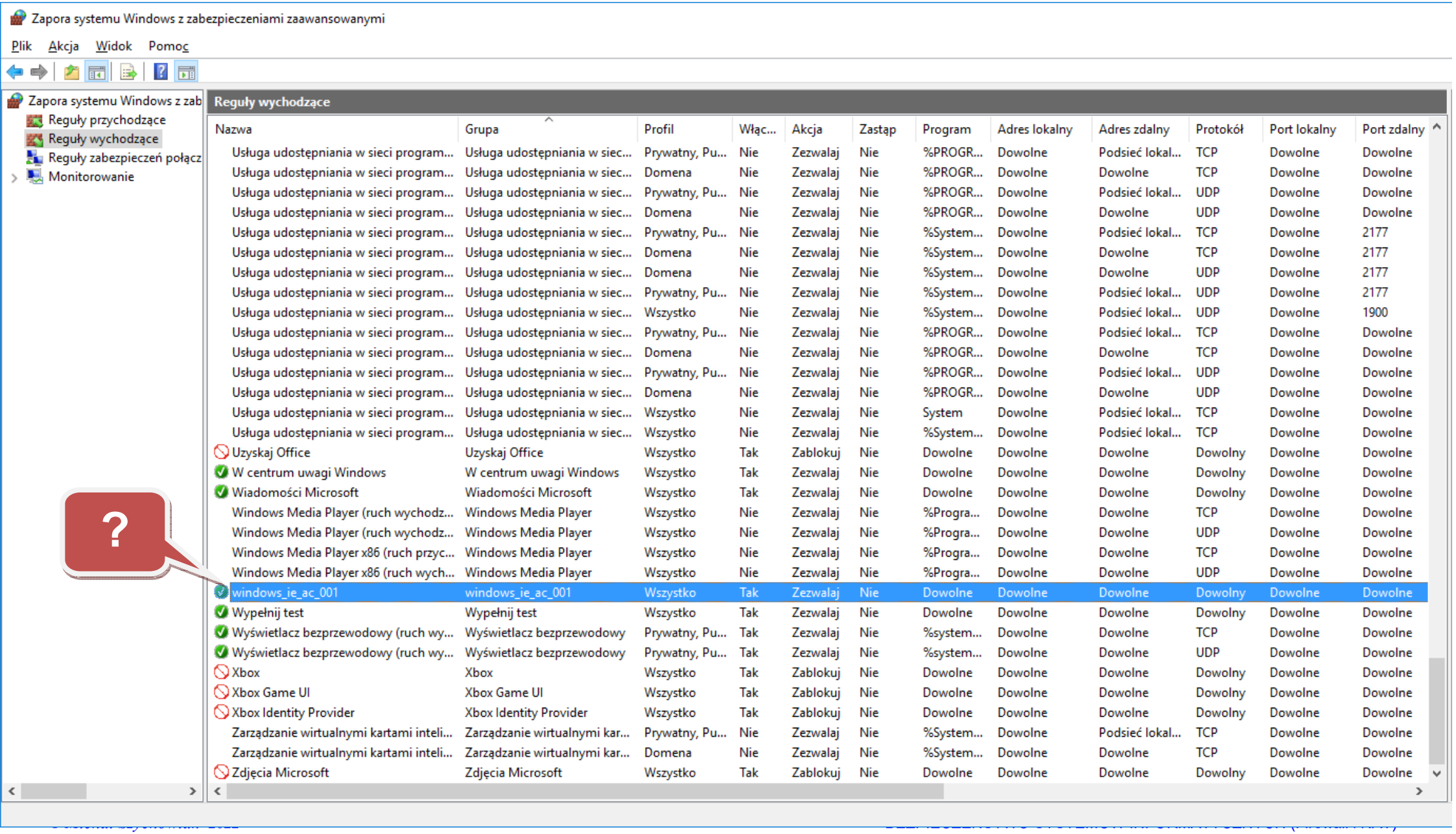
Produkty

Klasa: Personal Firewall

Podstawowa funkcjonalność:

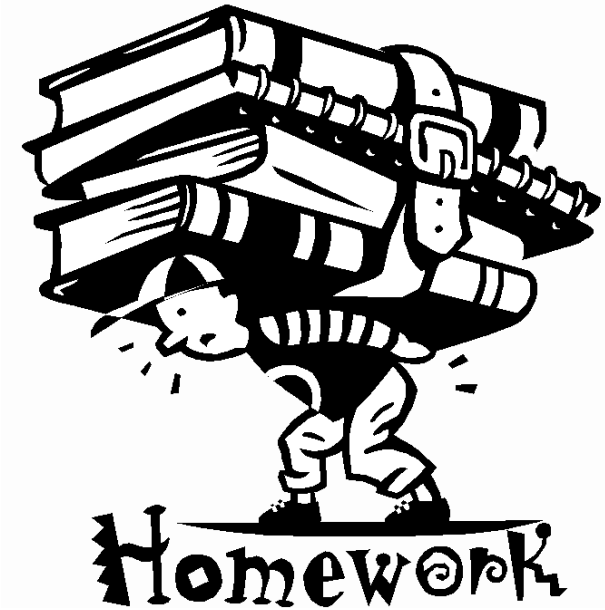
- zabezpieczenie jednostanowiskowe (komputer osobisty)
- instalowane jako moduł systemu operacyjnego
- filtrujący ruch sieciowy wchodzący i wychodzący
- często + antywirus, antyspamer, filtr www, ...

Produkty


Zapora systemu Windows z zabezpieczeniami zaawansowanymi
Plik Akcja Widok Pomoc
Zapora systemu Windows z zab
Reguły przychodzące
Reguły wychodzące
Reguły zabezpieczeń połącz
Monitorowanie
Reguły wychodzące
Nazwa | Grupa | Profil | Włąc... | Akcja | Zastąp | Program | Adres lokalny | Adres zdalny | Protokół | Port lokalny | Port zdalny
Usługa udostępniania w sieci program... | Usługa udostępniania w siec... | Prywatny, Pu... | Nie | Zezwalaj | Nie | %PROGR... | Dowolne | Podsieć lokal... | TCP | Dowolne | Dowolne
Usługa udostępniania w sieci program... | Usługa udostępniania w siec... | Domena | Nie | Zezwalaj | Nie | %PROGR... | Dowolne | Dowolne | TCP | Dowolne | Dowolne
Usługa udostępniania w sieci program... | Usługa udostępniania w siec... | Prywatny, Pu... | Nie | Zezwalaj | Nie | %PROGR... | Dowolne | Podsieć lokal... | UDP | Dowolne | Dowolne
Usługa udostępniania w sieci program... | Usługa udostępniania w siec... | Domena | Nie | Zezwalaj | Nie | %PROGR... | Dowolne | Dowolne | UDP | Dowolne | Dowolne
Usługa udostępniania w sieci program... | Usługa udostępniania w siec... | Prywatny, Pu... | Nie | Zezwalaj | Nie | %System... | Dowolne | Podsieć lokal... | TCP | Dowolne | 2177
Usługa udostępniania w sieci program... | Usługa udostępniania w siec... | Domena | Nie | Zezwalaj | Nie | %System... | Dowolne | Dowolne | TCP | Dowolne | 2177
Usługa udostępniania w sieci program... | Usługa udostępniania w siec... | Domena | Nie | Zezwalaj | Nie | %System... | Dowolne | Dowolne | UDP | Dowolne | 2177
Usługa udostępniania w sieci program... | Usługa udostępniania w siec... | Prywatny, Pu... | Nie | Zezwalaj | Nie | %System... | Dowolne | Podsieć lokal... | UDP | Dowolne | 2177
Usługa udostępniania w sieci program... | Usługa udostępniania w siec... | Wszystko | Nie | Zezwalaj | Nie | %System... | Dowolne | Podsieć lokal... | UDP | Dowolne | 1900
Usługa udostępniania w sieci program... | Usługa udostępniania w siec... | Prywatny, Pu... | Nie | Zezwalaj | Nie | %PROGR... | Dowolne | Podsieć lokal... | TCP | Dowolne | Dowolne
Usługa udostępniania w sieci program... | Usługa udostępniania w siec... | Domena | Nie | Zezwalaj | Nie | %PROGR... | Dowolne | Dowolne | TCP | Dowolne | Dowolne
Usługa udostępniania w sieci program... | Usługa udostępniania w siec... | Prywatny, Pu... | Nie | Zezwalaj | Nie | %PROGR... | Dowolne | Podsieć lokal... | UDP | Dowolne | Dowolne
Usługa udostępniania w sieci program... | Usługa udostępniania w siec... | Domena | Nie | Zezwalaj | Nie | %PROGR... | Dowolne | Dowolne | UDP | Dowolne | Dowolne
Usługa udostępniania w sieci program... | Usługa udostępniania w siec... | Wszystko | Nie | Zezwalaj | Nie | System | Dowolne | Podsieć lokal... | TCP | Dowolne | Dowolne
Usługa udostępniania w sieci program... | Usługa udostępniania w siec... | Wszystko | Nie | Zezwalaj | Nie | %System... | Dowolne | Podsieć lokal... | TCP | Dowolne | Dowolne
Uzyskaj Office | Uzyskaj Office | Wszystko | Tak | Zablokuj | Nie | Dowolne | Dowolne | Dowolne | Dowolny | Dowolne | Dowolne
W centrum uwagi Windows | W centrum uwagi Windows | Wszystko | Tak | Zezwalaj | Nie | Dowolne | Dowolne | Dowolne | Dowolny | Dowolne | Dowolne
Wiadomości Microsoft | Wiadomości Microsoft | Wszystko | Tak | Zezwalaj | Nie | Dowolne | Dowolne | Dowolne | Dowolny | Dowolne | Dowolne
Windows Media Player (ruch wychodz... | Windows Media Player | Wszystko | Nie | Zezwalaj | Nie | %Progra... | Dowolne | Dowolne | TCP | Dowolne | Dowolne
Windows Media Player (ruch wychodz... | Windows Media Player | Wszystko | Nie | Zezwalaj | Nie | %Progra... | Dowolne | Dowolne | UDP | Dowolne | Dowolne
Windows Media Player x86 (ruch przyc... | Windows Media Player | Wszystko | Nie | Zezwalaj | Nie | %Progra... | Dowolne | Dowolne | TCP | Dowolne | Dowolne
Windows Media Player x86 (ruch wych... | Windows Media Player | Wszystko | Nie | Zezwalaj | Nie | %Progra... | Dowolne | Dowolne | UDP | Dowolne | Dowolne
windows_ie_ac_001 | windows_ie_ac_001 | Wszystko | Tak | Zezwalaj | Nie | Dowolne | Dowolne | Dowolne | Dowolny | Dowolne | Dowolne
Wypełnij test | Wypełnij test | Wszystko | Tak | Zezwalaj | Nie | Dowolne | Dowolne | Dowolne | Dowolny | Dowolne | Dowolne
Wyświetlacz bezprzewodowy (ruch wy... | Wyświetlacz bezprzewodowy | Prywatny, Pu... | Tak | Zezwalaj | Nie | %system... | Dowolne | Dowolne | TCP | Dowolne | Dowolne
Wyświetlacz bezprzewodowy (ruch wy... | Wyświetlacz bezprzewodowy | Prywatny, Pu... | Tak | Zezwalaj | Nie | %system... | Dowolne | Dowolne | UDP | Dowolne | Dowolne
Xbox | Xbox | Wszystko | Tak | Zablokuj | Nie | Dowolne | Dowolne | Dowolne | Dowolny | Dowolne | Dowolne
Xbox Game UI | Xbox Game UI | Wszystko | Tak | Zablokuj | Nie | Dowolne | Dowolne | Dowolne | Dowolny | Dowolne | Dowolne
Xbox Identity Provider | Xbox Identity Provider | Wszystko | Tak | Zablokuj | Nie | Dowolne | Dowolne | Dowolne | Dowolny | Dowolne | Dowolne
Zarządzanie wirtualnymi kartami inteli... | Zarządzanie wirtualnymi kar... | Prywatny, Pu... | Nie | Zezwalaj | Nie | %System... | Dowolne | Podsieć lokal... | TCP | Dowolne | Dowolne
Zarządzanie wirtualnymi kartami inteli... | Zarządzanie wirtualnymi kar... | Domena | Nie | Zezwalaj | Nie | %System... | Dowolne | Dowolne | TCP | Dowolne | Dowolne
Zdjęcia Microsoft | Zdjęcia Microsoft | Wszystko | Tak | Zablokuj | Nie | Dowolne | Dowolne | Dowolne | Dowolny | Dowolne | Dowolne
?

Produkty

Klasa: Personal Firewall



Problemy:

→ funkcja `CreateRemoteThread()` w Windows

Produkty

Klasa: Bramy aplikacyjne

Przykłady

- WWW proxy:

  Squid WWW Proxy – typowy WWW proxy + web cache

- inne:

  Dual Gatekeper – proxy dla protokołu H.323 (NetMeeting) polecenia sterujące: 1720/tcp oraz 1731/tcp; dane multimedialne: RTP (na UDP) – filtracja bezstanowa bezużyteczna, jak dla FTP

  Cisco OIS ALG

  AEP Networks SmartGate

Produkty

Certyfikaty ICSA Labs (www.icsalabs.com)

- ICSA (dawniej National Computer Security Association, Verizon) bada produkty klasy COTS (*commercial of the shelf*)
- zestaw testów: Modular Firewall Product Certification Criteria
- oprócz zapór testują również produkty VPN pod względem zgodności ze specyfikacją IPsec