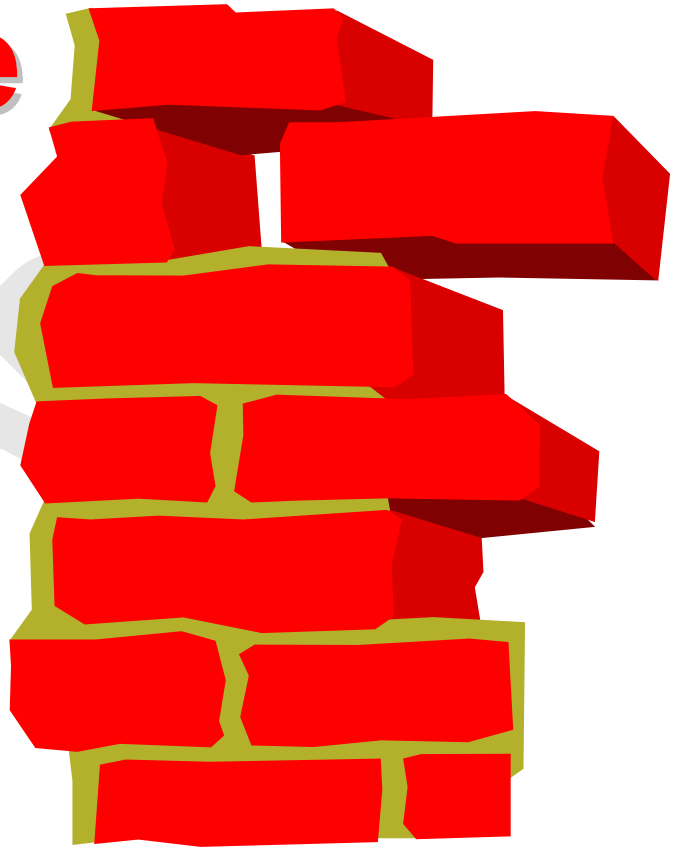
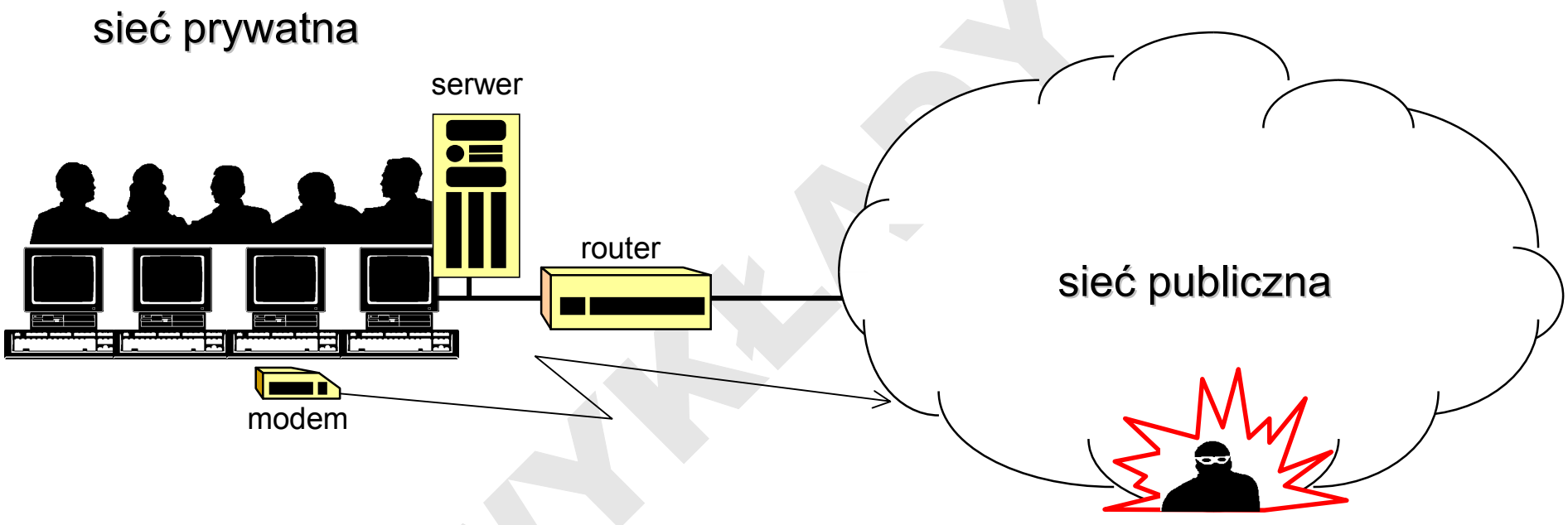
Zapory sieciowe (firewall) i translacja adresów



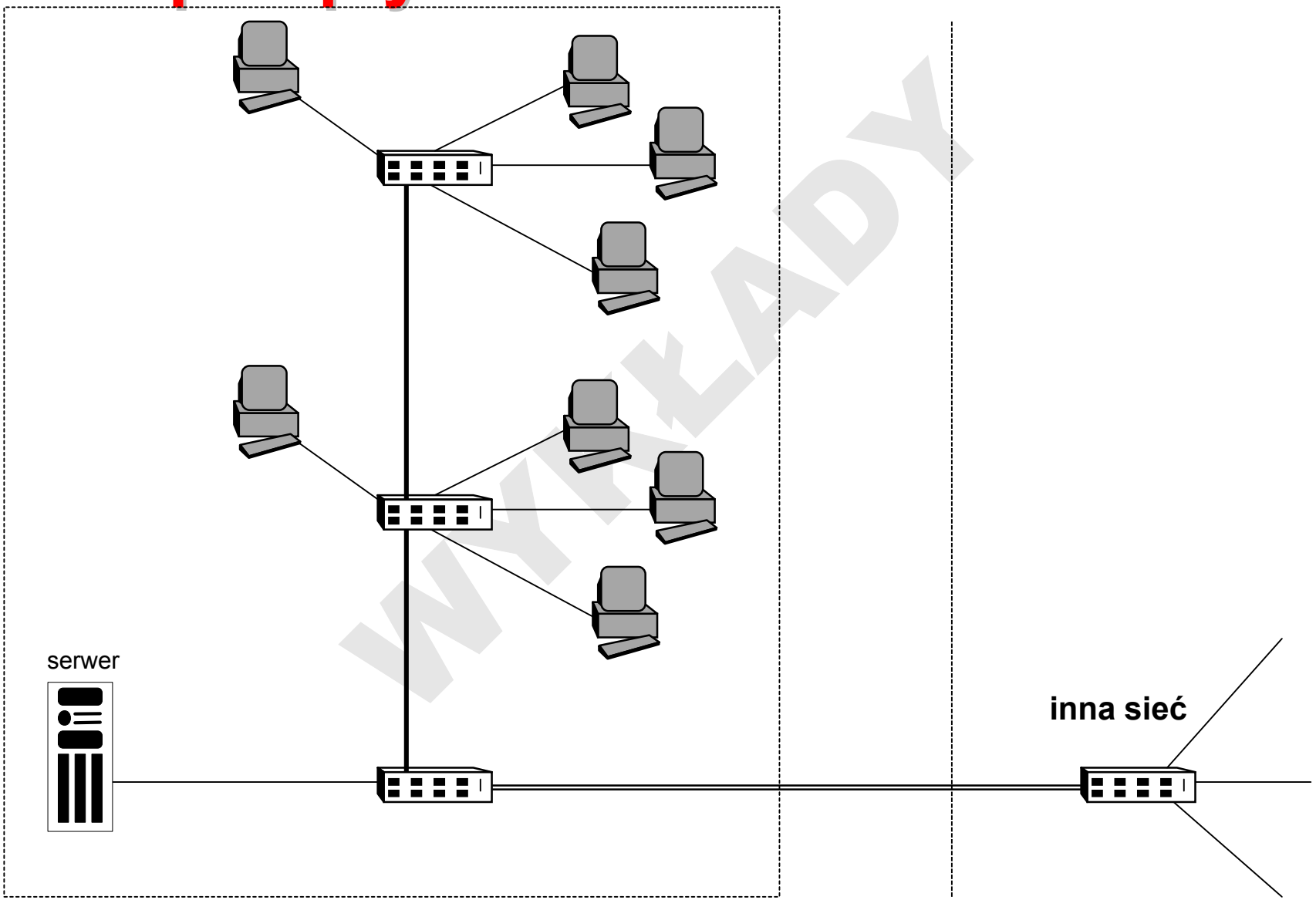
Zagadnienia

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

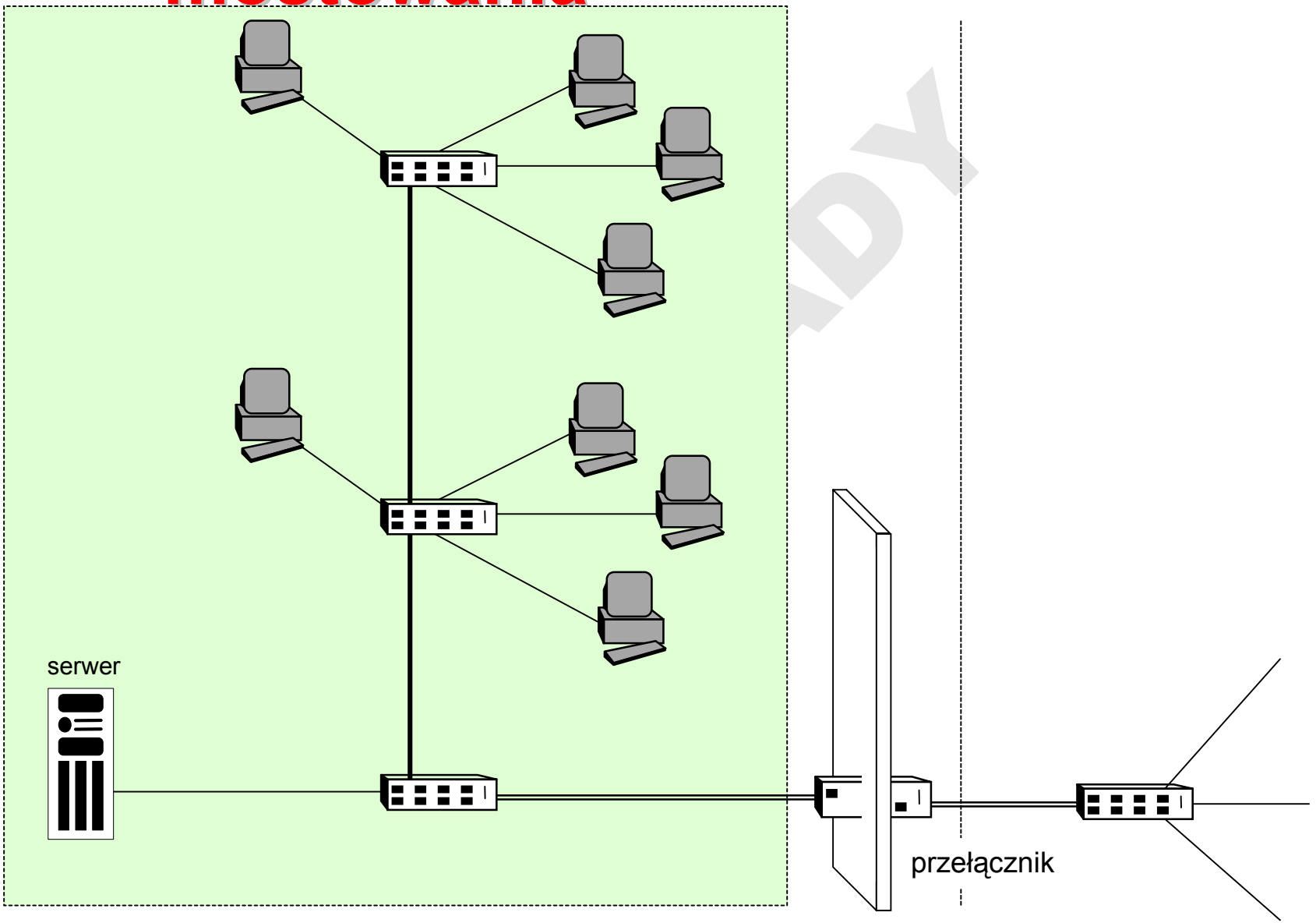
Scenariusz



Połączenie ze swobodnym przepływem

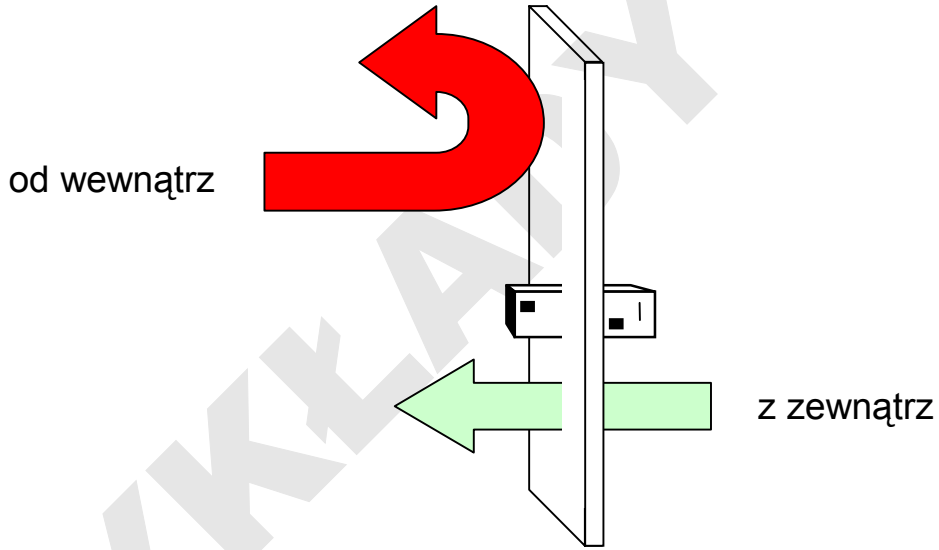


Połączenie za pomocą mostowania



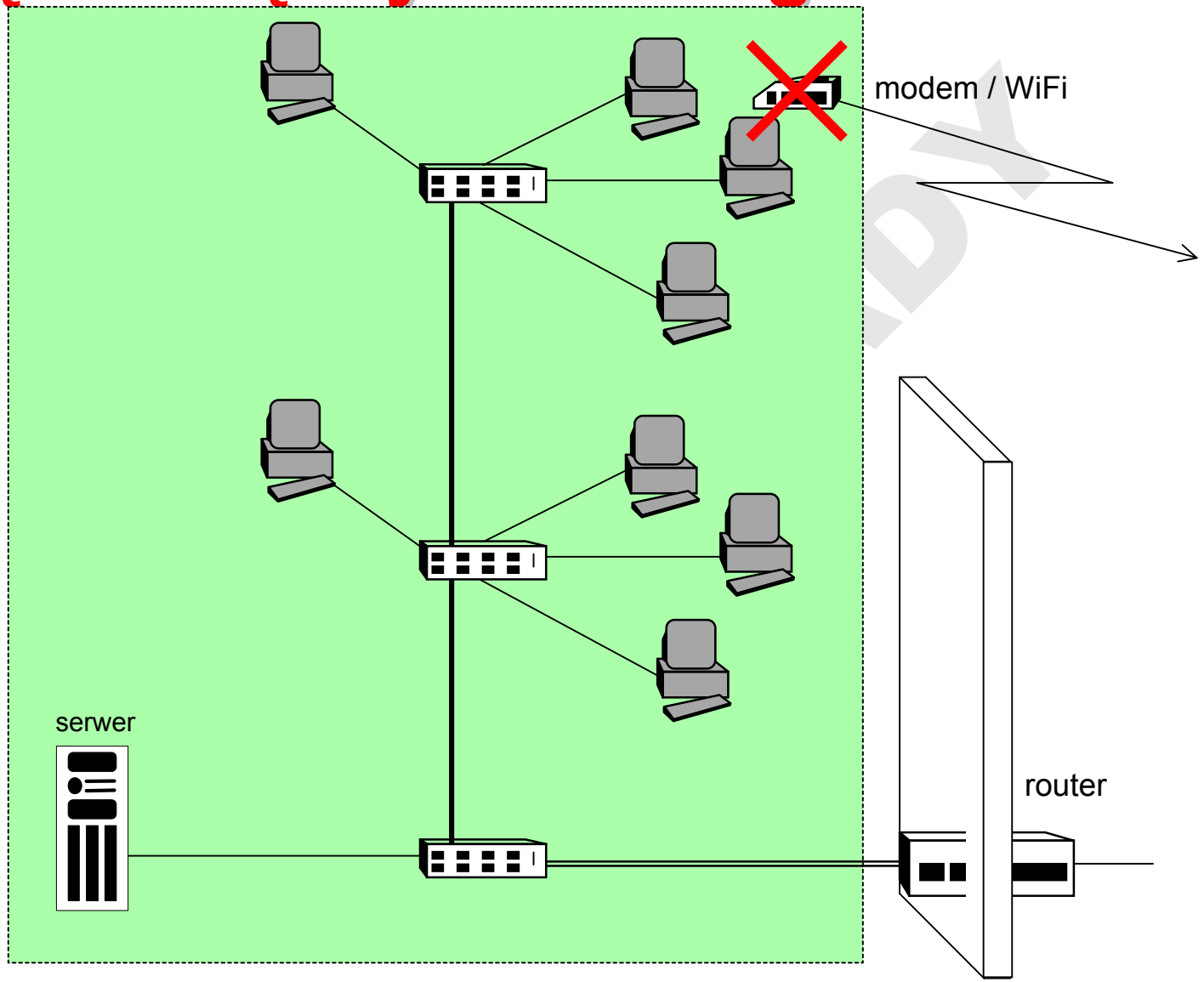
Mostowanie

Jednokierunkowa filtracja:

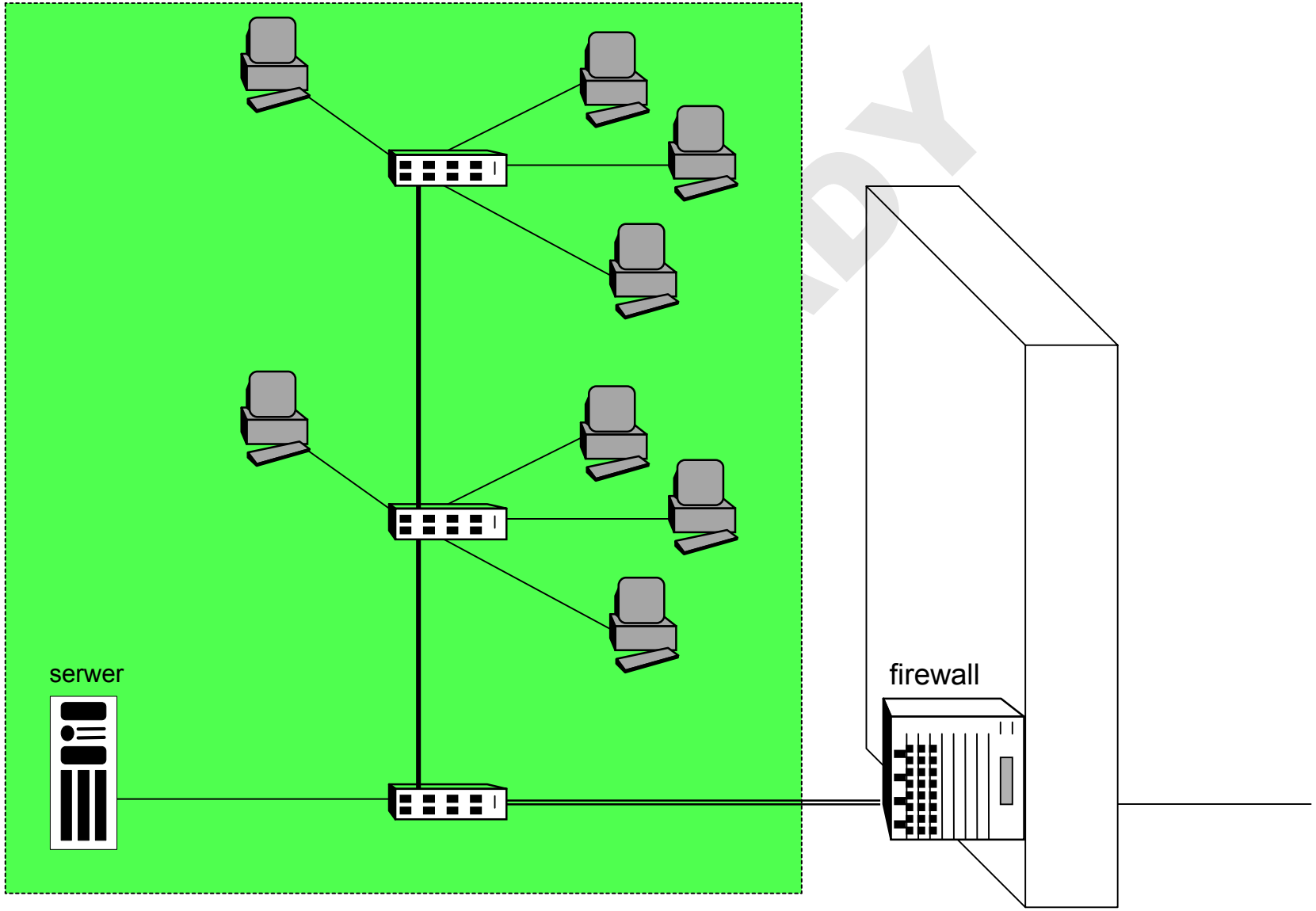


- przełączniki mogą filtrować ramki na podstawie adresów MAC
- ramki rozgłaszania i rozsyłania grupowego
- sieci VLAN

Połączenie za pomocą węzła międzysieciowego



Selektywne blokowanie (filtracja) ruchu



Firewall

Zapora czy ściana przeciwogniowa?

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

Słownik dziedzictwa amerykańskiego

Inne analogie:

- kontrola paszportowa i celna na granicy

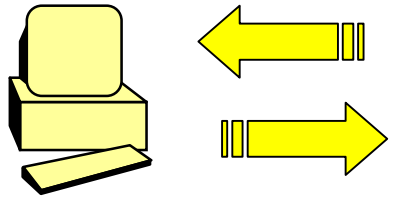
Zapory sieciowe

Podstawowe funkcje systemów firewall:

1. Filtracja pakietów

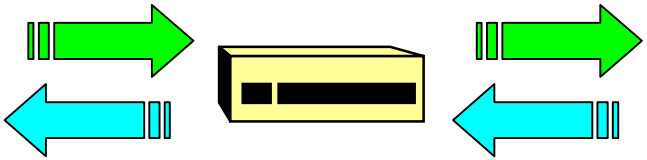
- podstawowa forma zabezpieczenia sieci – warstwa 3 (czasami 2-4) modelu OSI

1. Filtracja pakietów nadchodzących



2. Filtracja pakietów wychodzących

3. Filtracja pakietów propagowanych (routing)

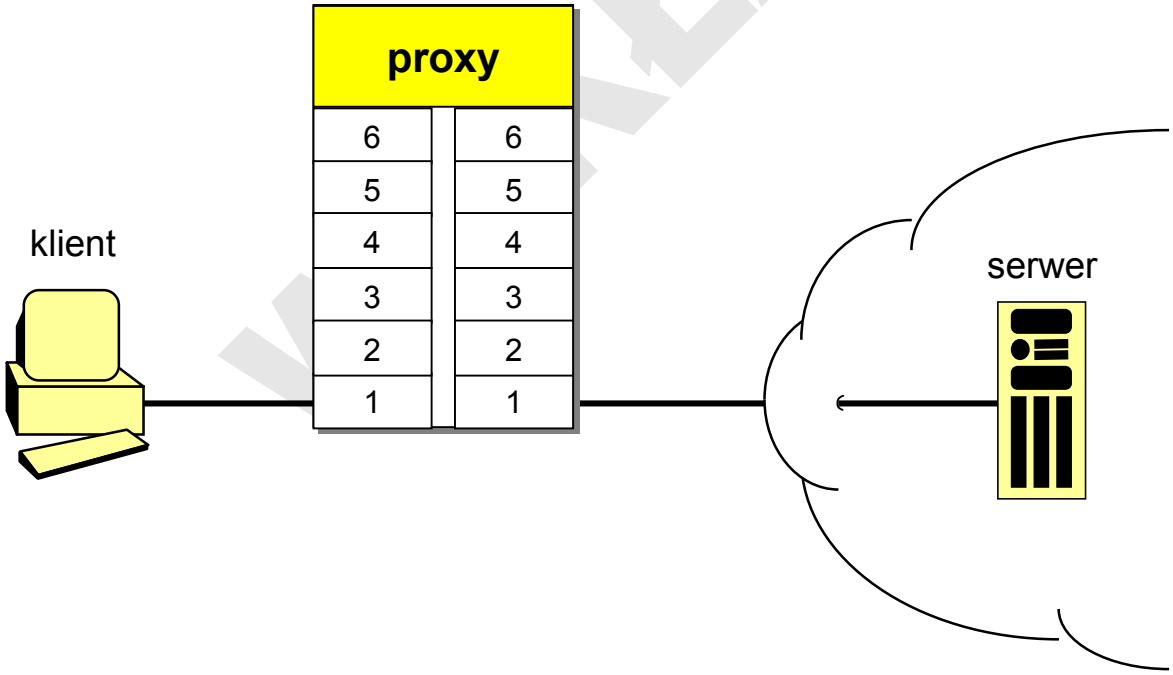


Zapory sieciowe

Podstawowe funkcje systemów firewall:

2. Pośredniczenie w realizacji usług

- aplikacje pośredniczące (*proxy services*) w komunikacji końcowych aplikacji użytkowych (np. klient-serwer) – warstwa 7 modelu OSI:



Zapory sieciowe

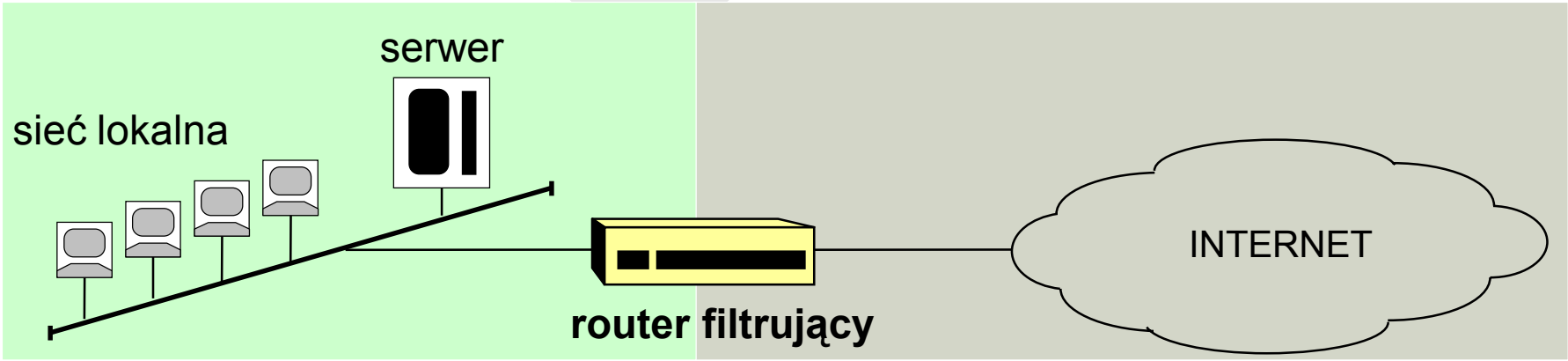
Podstawowe komponenty systemów firewall:

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

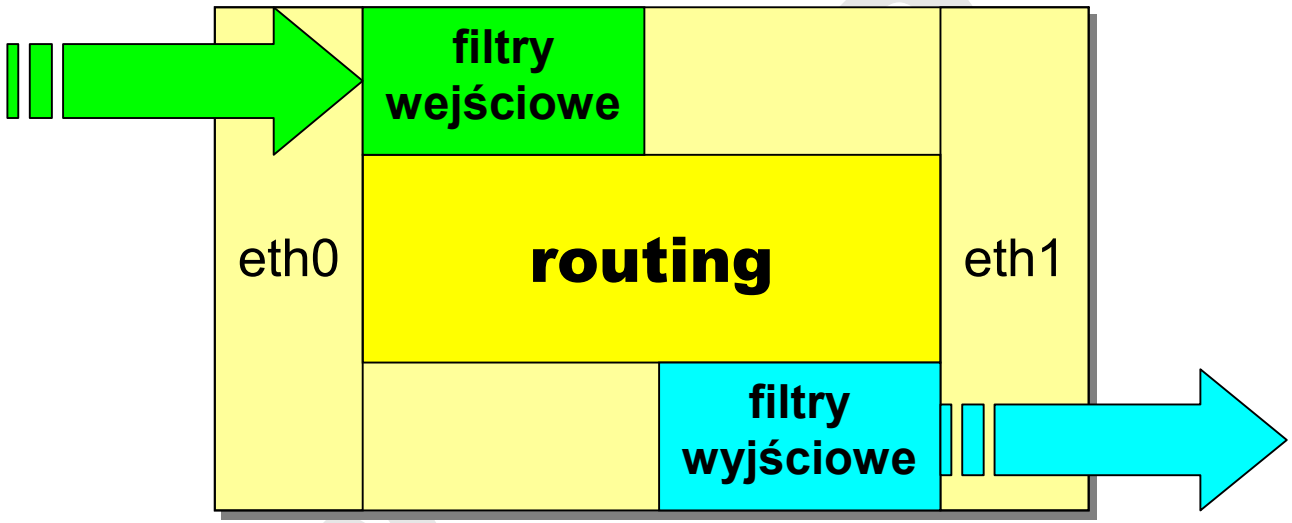
Reguły filtracji

- 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

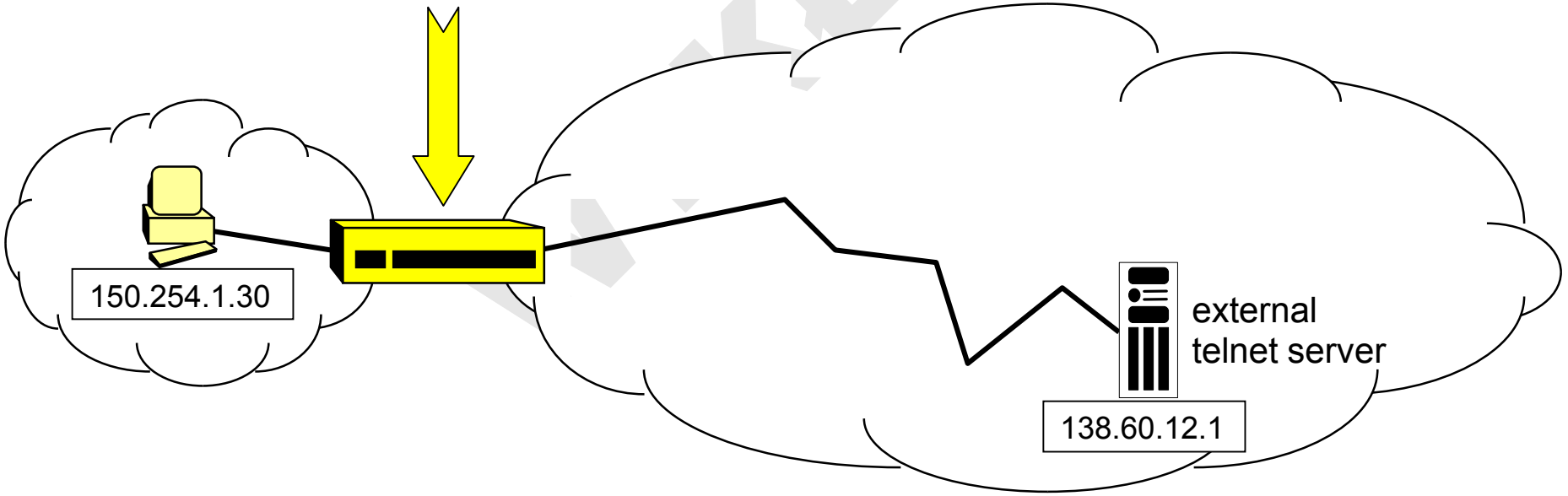
Filtry

- filtry statyczne
- filtry kontekstowe (dynamiczne reguły filtracji: SPF = *Stateful Packet Filtering*)
  - 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	>1023	23	*	przepuść
2.	do wewnątrz	138.60.12.1	150.254 .* .*	TCP	23	>1023	ACK=1	przepuść
3.	do wewnątrz	138.60 .12.1	150.254 .* .*	TCP	23	>1023	ACK=0	odrzuć
(default)	*	* .* .* .*	* .* .* .*	*	*	*	*	odrzuć

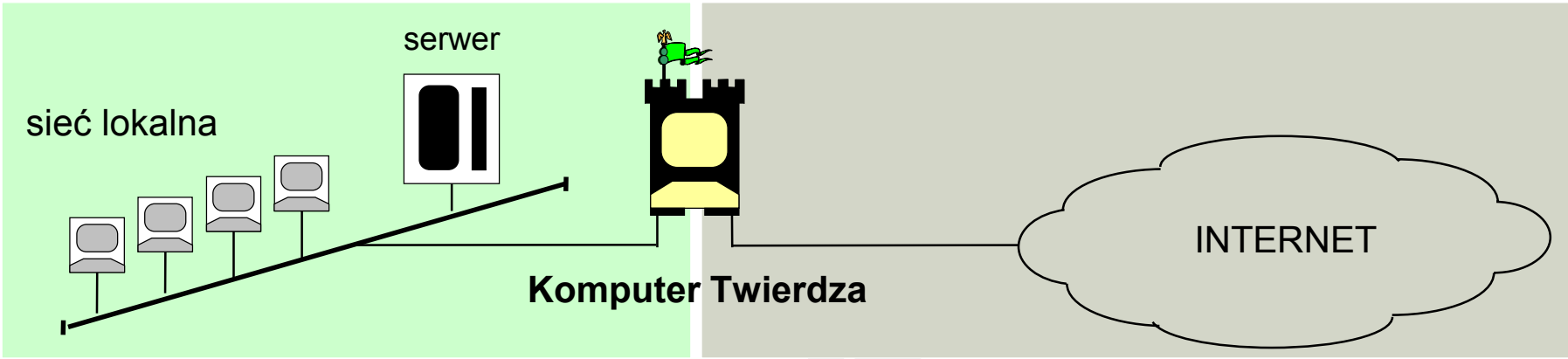


Router filtrujący

Statyczne reguły filtracji

- niektóre usługi trudno poddają się filtracji statycznej (np. FTP, X11, DNS)
- chociaż coraz powszechniej wprowadza się i stosuje tryby pracy zmodyfikowane pod kątem usprawnienia filtracji, np. tryb *passive* w protokole FTP (skądinąd użyteczny także np. przy korzystaniu z dostępu xDSL)

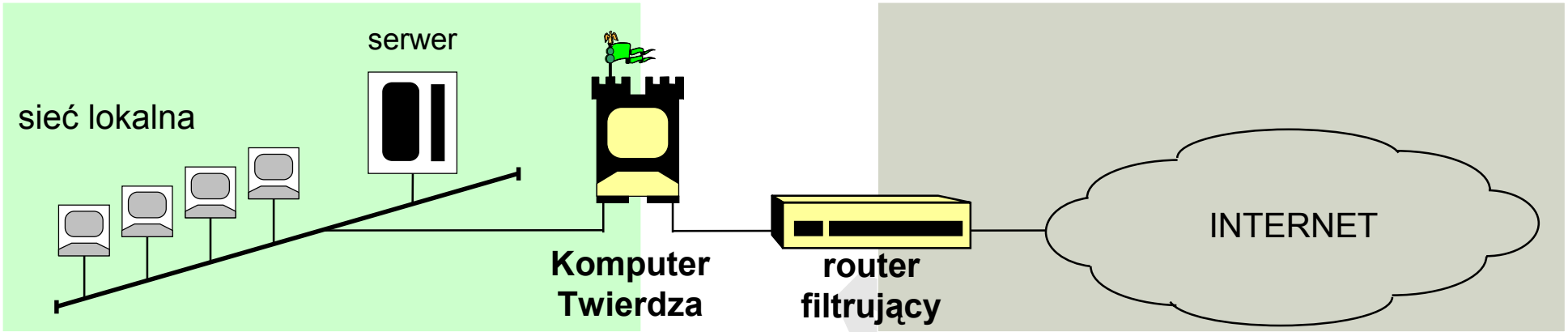
Komputer Twierdza



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 – usługi pośredniczące i zastępcze (*proxy*) rozwiązują problem usług trudnych do filtracji
- rejestracja zdarzeń (*auditing*)

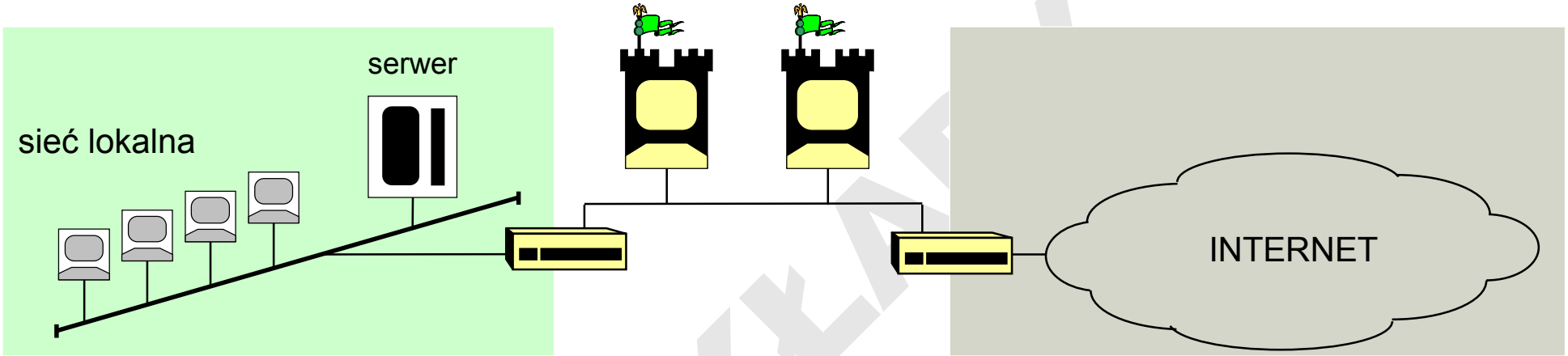
Filtracja podwójna



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

Podsieć ochronna

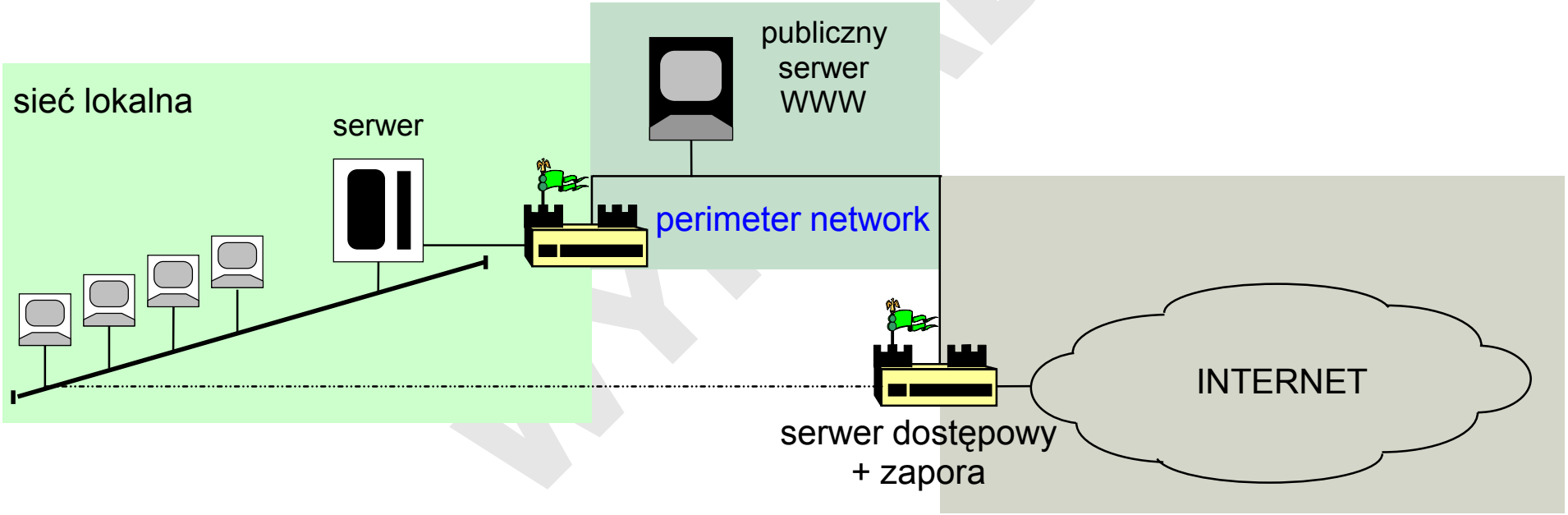
- „rozciągnięcie” Twierdzy na całą dedykowaną podsieć (*Screened Network*)



- ... 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)

Cele:

- rozszerzenie dostępu do sieci publicznej na stanowiska nie posiadające przydziału adresów publicznych (posiadające tylko adresy prywatne – RFC 1918)
- wykorzystanie wewnątrz sieci nieprzydzielonych publicznych adresów IP (za cenę braku możliwości komunikacji z takimi oficjalnymi adresami)
- ukrycie wewnętrznej struktury sieci przed światem zewnętrznym
- przekierowanie ruchu (portów: NAPT = *Network Address & Port Translation*)

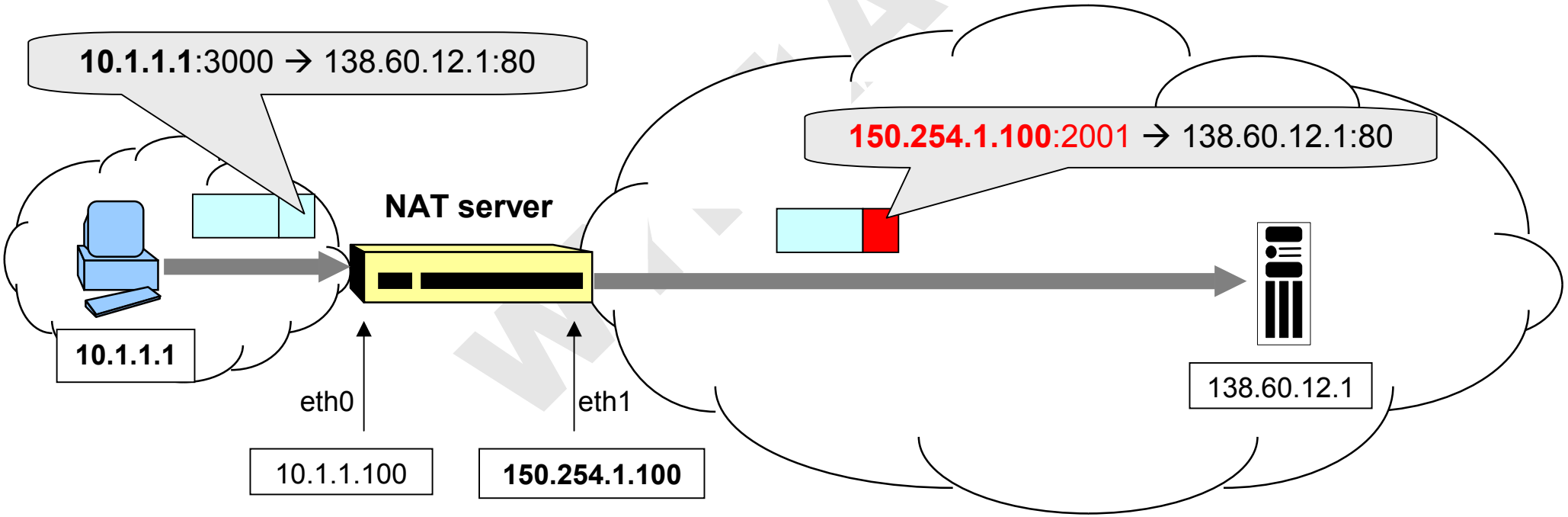
Metody:

- RFC1631 (translacja na pojedynczy adres, tj. N:1)
- RFC1597,1918 (translacja na pulę adresową, tj. N:M)

Translacja adresów źródłowych (SNAT)

Source NAT (SNAT)

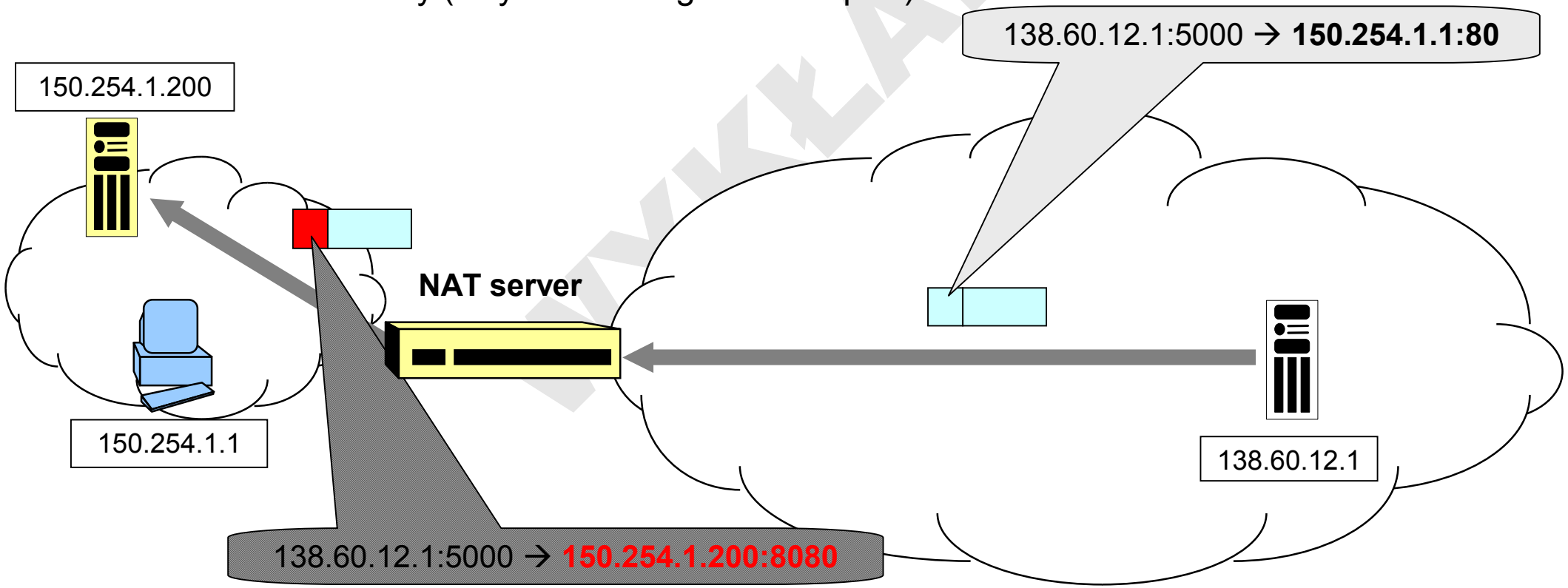
- pakiety wychodzące z sieci wewnętrznej otrzymują nowy adres źródłowy w nagłówku



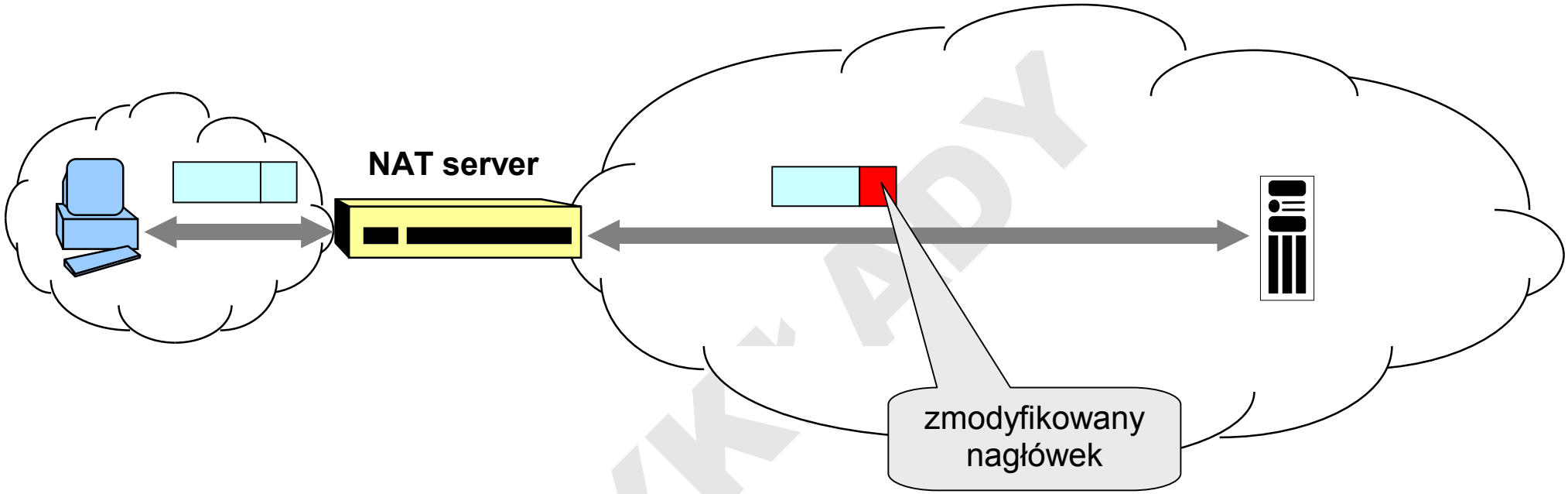
Translacja adresów docelowych (DNAT)

Destination NAT (DNAT)

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

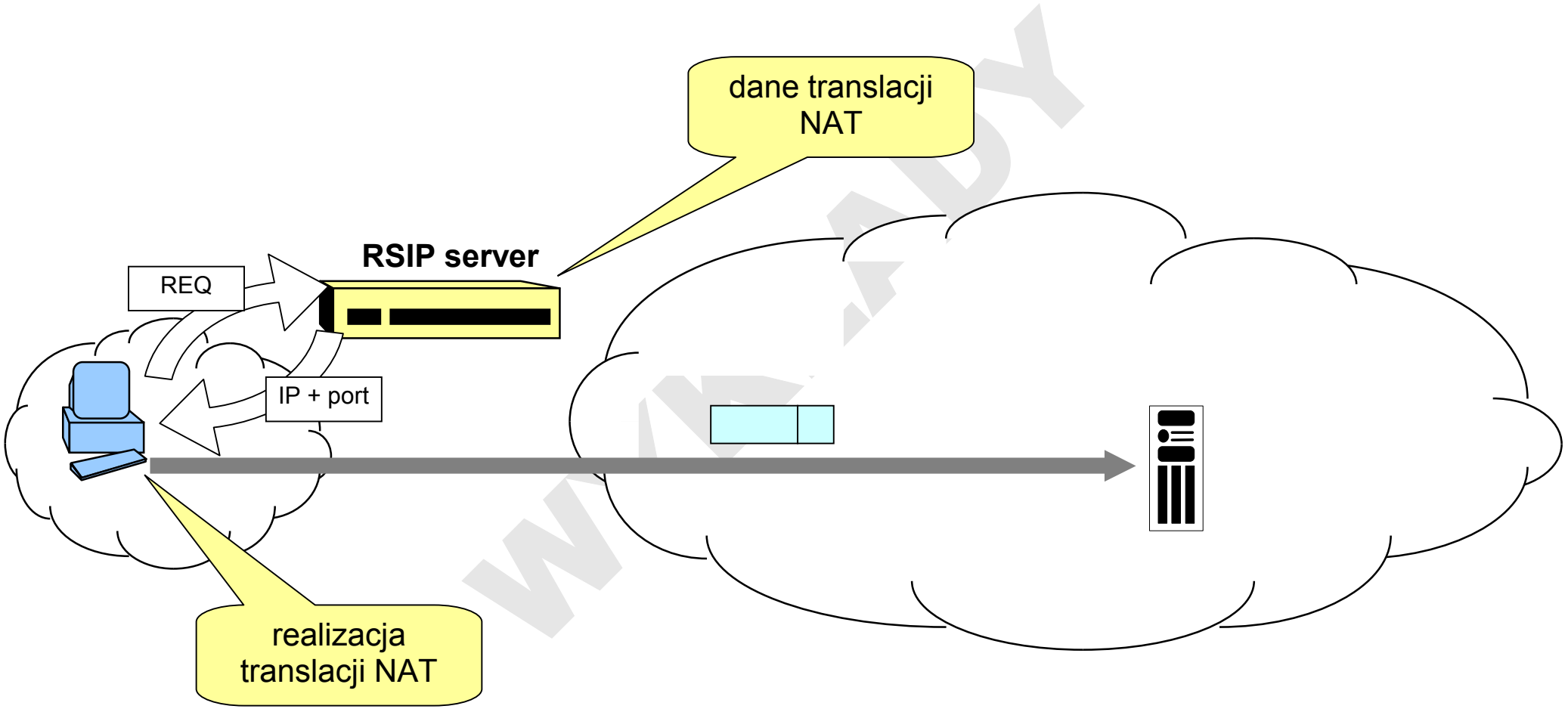


NAT ⇔ VPN



- NAT modyfikuje datagram, dlatego np. nie można korzystać z IPsec AH / ESP w trybie transportowym (bezpośrednim)

Realm-Specific Internet Protocol (RSIP)



Dodatkowa funkcjonalność

Łańcuch funkcji:

funkcje podstawowe:

funkcje dodatkowe:

- wykrywanie i rejestrowanie prób ataków na chronione systemy

Dodatkowa funkcjonalność

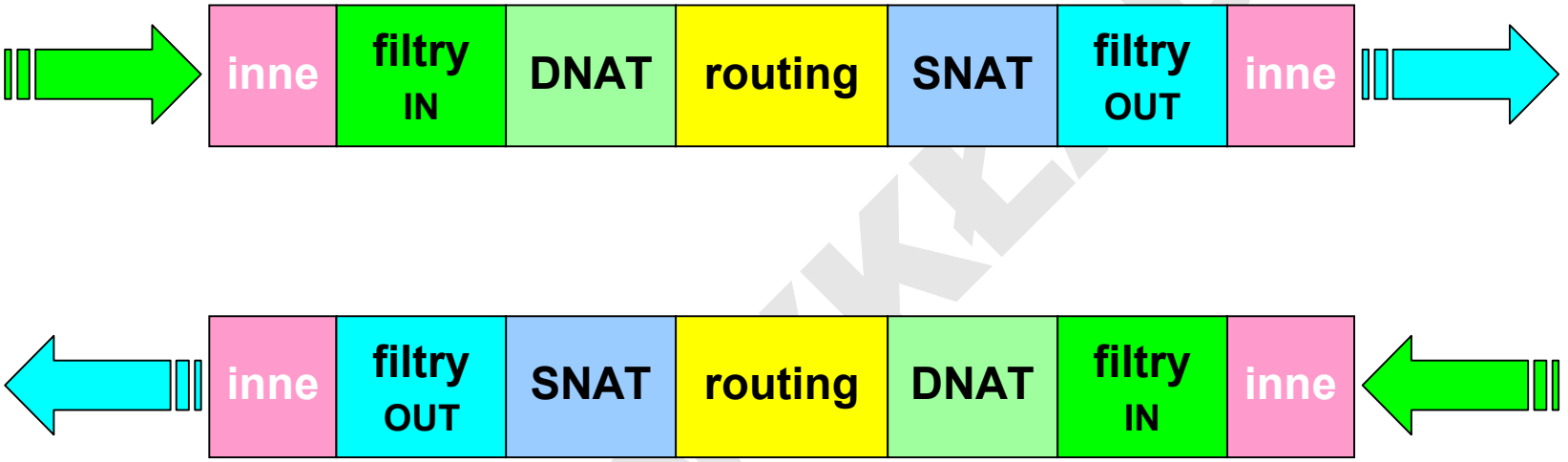
Funkcje dodatkowe:

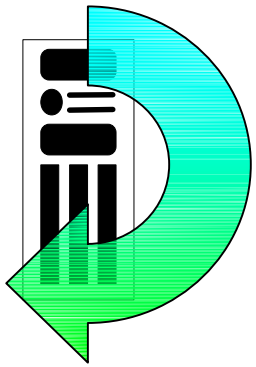
- obrona przed atakami DoS (*flood-wall*) – specyfikowanie dopuszczalnego rozmiaru strumienia wejściowego (np. w pakietach na sek.)
- kontrola fragmentacji IP i śledzenie numerów sekwencyjnych TCP (kontrola czy znajdują się w oczekiwanym zakresie)
- filtry IPv6, np. *ipf* (FreeBSD), rozpoznawanie tunelowania IPv6 w IPv4 (tzn. takich protokołów jak 6to4, 6over4, Toredo)
- inne wsparcie dla IPv6: fragmentacja, ICMPv6, ochrona przed atakami DoS analogicznymi jak dla IPv4
- integracja z różnymi zewnętrznymi modułami, np. systemami antywirusowymi, modułami sieciowej detekcji intruzów (IDS), czy kontroli treści i ograniczenia dostępu (np. *parental control*)

Dodatkowa funkcjonalność

Filtry statyczne (bezstanowe)

Round-trip – standardowy przepływ:



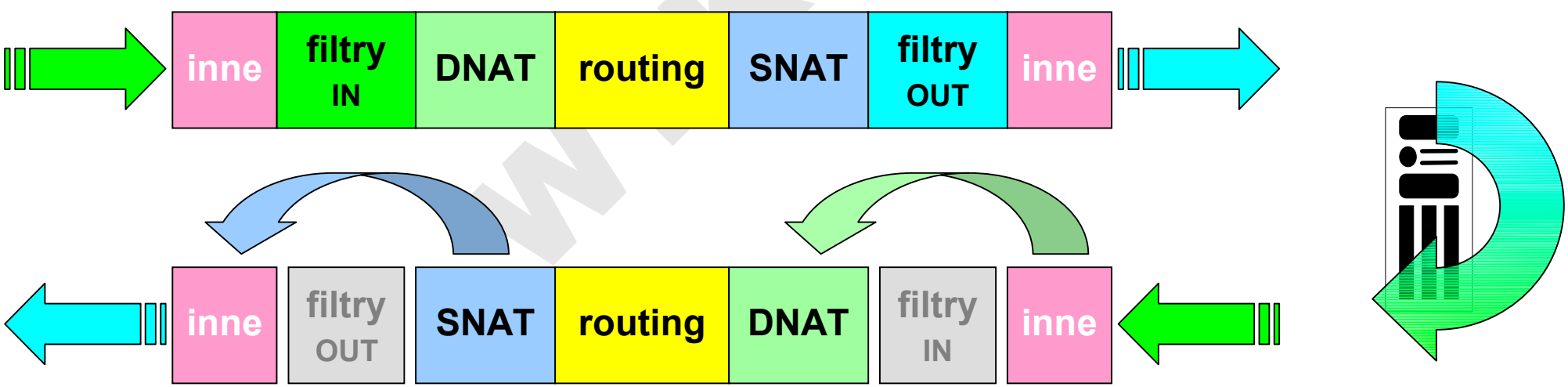


Dodatkowa funkcjonalność

Filtry kontekstowe

Weryfikacja kontekstu (*stateful inspection*):

- każda zainicjowana poprawnie sesja jest pamiętana na dynamicznych listach
- w drodze powrotnej pakiet jest sprawdzany na przynależność do zapamiętanej sesji – filtracja może być pominięta:



Problemy

Problemy technologiczne:

- usługi takie jak FTP
  - jeśli filtr kontekstowy w zaporze obsłuży komendę PORT 23 protokołu FTP, to czy będzie to naruszenie polityki bezpieczeństwa?
- mechanizmy takie jak 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

Ogień kroczący (*firewalking*):

- zapory często przepuszczają kilka wybranych autoryzowanych i na ogół uwierzytelnianych kanałów,
- które w praktyce czasami przepuszczają pewne pozornie nieszkodliwe protokoły (ICMP echo, zapytania DNS),
- umożliwiające wykrywanie składników sieci poza zaporami
- przykład zastosowania techniki ognia kroczącego:
  - zmodyfikowany *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)
  - i dalej sonduje się istnienie (i konfigurację) komputerów poza zaporą

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

Wsparcie w testowaniu zapór

- zespoły realizujące testowe ataki w warunkach rzeczywistych – tzw. *brygady tygrysa*

Problemy

Ostrożnie z tunelami:

- autoryzowane tunele VPN mogą być potencjalnym nośnikiem nieautoryzowanych treści poza kontrolą zapór ogniowych
- powinny być zaplanowane i zrealizowane w sposób przemyślany (m.in. zgodnie z zasadą minimalnego przywileju)
- również propagowanie połączeń (*port forwarding*) może przyczynić się do skutecznego ominięcia kontroli na zaporze
- podobnie dość rozpowszechniony SOAP (*Simple Object Access Protocol*)
- czy IPP (*Internet Printing Protocol*) przepuszczany przez port 80 zamiast 631
- skrajnie wywrotowy jest *httptunnel* (http://www.noccrew.org/software/httptunnel.html)

Problemy

Ostrożnie z tunelami:

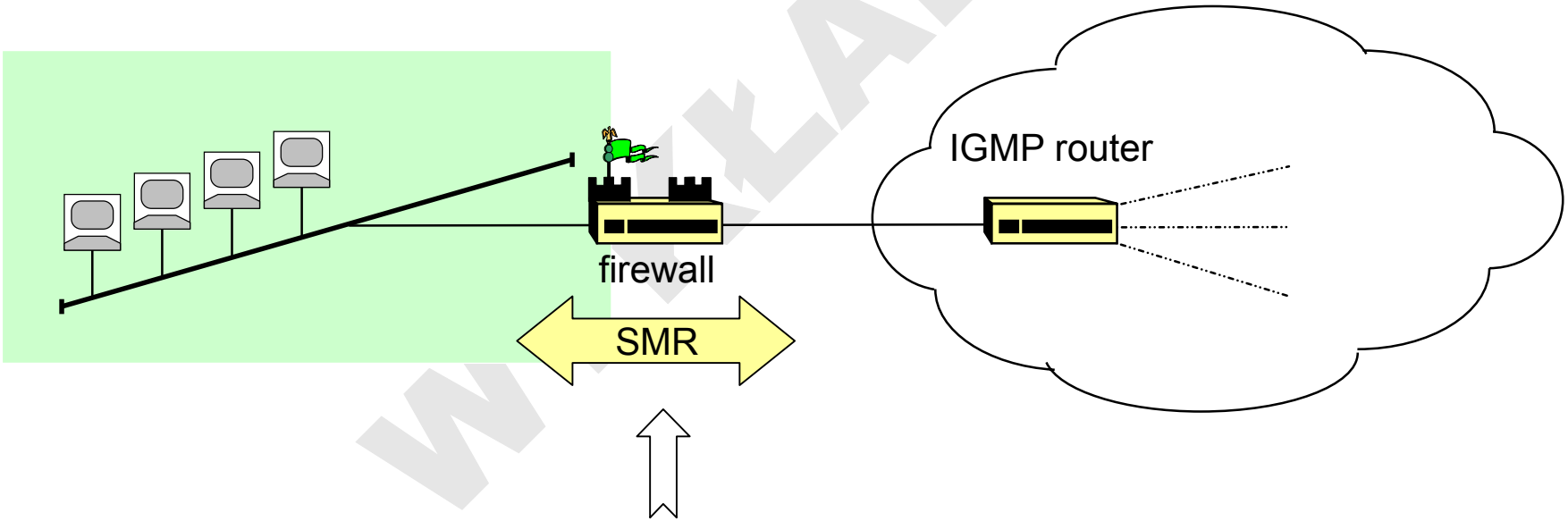
IPsec + firewall

- definicja reguł filtracji musi uwzględniać konieczność przepuszczania protokołów ESP (nr 50) i AH (nr 51) oraz UDP dla ISAKMP (port 500/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 – wymagane zamknięte grupy użytkowników

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 (np. Cisco PIX)

moduły jądra systemów Linux (np. netfilter/iptables) lub BSD (np. ipf/ipfw)

Systemy zintegrowane:

Firewall 1 (CheckPoint; SUN, Bay Networks)

Gauntlet Firewall (Network Associates)

Raptor Firewall (Axent, Symantec)

NetScreen (NetScreen)

SideWinder (Secure Computing)

Netguard (Guardian)

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

m0n0wall (freeware: http://m0n0.ch/wall/)

Produkty

PIX = Private Internet eXchange (Cisco)

- translacja adresów IP (NAT)
  - adresy prywatne (RFC1597, RFC1918) – translacja N:M
  - NAPT – tu nazywane PAT (*Port Address Translation*) – translacja N:1
- zaszyfrowany tunel wirtualny VPN IPsec (z ISAKMP)
- funkcje TCP intercept: Flood Guard, IP Frag Guard, DNS Guard, Mail Guard, RFC 2827
- filtry URL i kontrola treści (Java filtering, ActiveX blocking)
- AAA (RADIUS, TACACS+)
- logging (syslog)
- obsługa konfiguracji lustrzanej w trybie *fail-over*

Produkty

FireWall-1 (CheckPoint Software)

- system zaporowy VPN-1/FireWall-1 flagowy produkt CheckPoint (systematycznie najpopularniejszy w swojej klasie wg wielu analiz rynku)
- VPN-1/FireWall-1 stanowi też komponent specjalizowanych urządzeń, np. Crossbeam X40S, Nortel ASF
- dostępne są liczne produkty określane nazwą Firewall Appliance lub Security Appliance, gdzie oprogramowanie CheckPoint zainstalowane jest przez dostawcę urządzeń
- cena uzależniona od rozmiaru sieci wewnętrznej i waha się od 3000$ dla 25 do 10000$ dla 250 chronionych adresów (wersja Enterprise bez ograniczenia liczby adresów IP – od 19000 $)

FireWall-1

Funkcje systemu FireWall-1

- FireWall-1 to zintegrowany pakiet zabezpieczeń zawierający mechanizmy:
  - kontroli dostępu
  - uwierzytelniania użytkowników
  - szyfrowania transmisji danych
  - translacji adresów sieciowych
  - analizy zawartości sesji (wirusy, złośliwe aplety, niepożądana zawartość WWW)
  - audytu
  - zcentralizowanego administrowania polityką bezpieczeństwa
- umożliwia uwierzytelnianie:
  - użytkownika (integracja z LDAP)
  - klienta
  - sesji

FireWall-1

Architektura systemu FireWall-1

FireWall-1 zawiera:

- moduł sterujący obejmujący:
  - konsolę graficzną
  - rejestr polityki bezpieczeństwa
  - bazę obiektów (użytkowników, usług, węzłów sieci, w tym urządzeń sieciowych, kluczy)
  - rejestry zdarzeń
- moduły filtracji pakietów i kontroli usług (mogą być rozproszone):
  - Inspection Modules (filtracja stanowa)
  - Security Servers – uwierzytelnianie i kontrola treści (np. antywirus, antyspam, filtry URL, Java/ActiveX screening, SYNDefender Gateway)

FireWall-1

Architektura systemu FireWall-1

Moduł sterujący

- zawiera graficzną konsolę Rule Base Editor – edytor zasad bezpieczeństwa
- zapisane w edytorze zasady i własności obiektów sieciowych (sieci, węzłów, usług, użytkowników) są podstawą do wygenerowania reguł Inspection Script (w obiektowym języku INSECT – możliwa ręczna edycja)
- kompilowanego w celu otrzymania kodu Inspection Code wysyłanego następnie do modułów filtracji pakietów i kontroli usług
- tworzy rejestry zdarzeń
- zbiera statystyki za pomocą SNMP

FireWall-1

Sposoby uwierzytelniania:

- hasła dostępowe systemu FireWall-1
- poprzez system operacyjny (hasła systemowe)
- S/Key
- tokeny SecurID
- RADIUS, TACACS, TACACS+, Axent Pathways Defender (moduł Raptora)
- poprzez przedłożenie ważnego certyfikatu X.509 lub biletu Kerberos

FireWall-1

Ochrona kryptograficzna:

- możliwe jest ustanawianie tuneli VPN, szyfrowanie sesji i certyfikacja kluczy
- poprzez moduł RSA Keon (RSA Security) często stosowany w e-commerce
- dodatkowy moduł Keon Certificate Server pozwala wykorzystać certyfikaty PKI udostępniane za pośrednictwem IPsec/IKE lub z repozytorium LDAP

FireWall-1

Wymagania techniczne

systemy operacyjne:

- CheckPoint SecurePlatform
- MS Windows XP, 2000 (≥SP1), Windows NT 4.0 (SP6a)
- Solaris 7 (tryb 32b), Solaris 8 (32b i 64b), HP-UX od 10.20 (32b), AIX od 4.2.1
- Linux: RedHat (od 6.2 wzwyż), ...

obsługiwane interfejsy sieciowe:

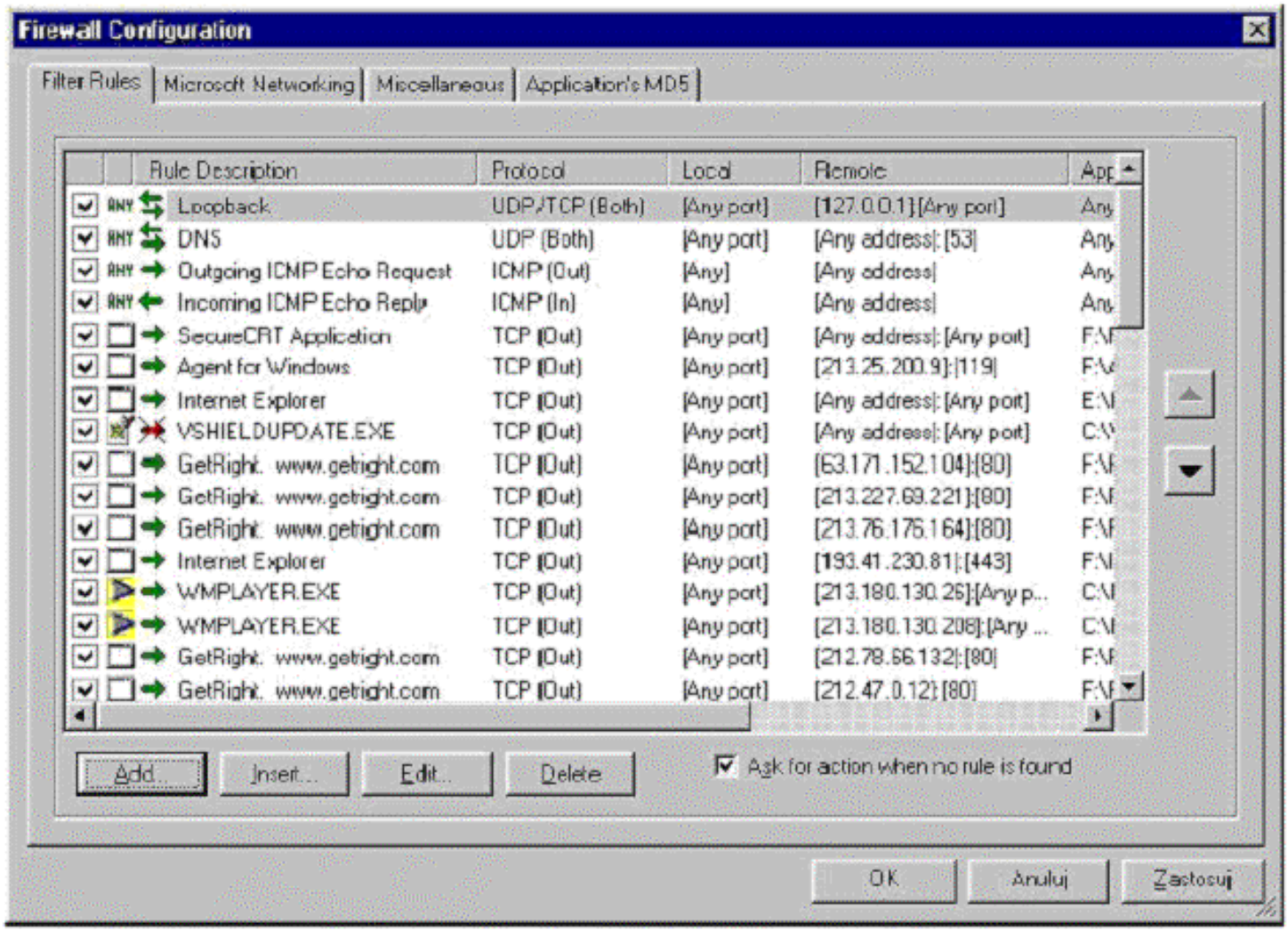
- ATM, Ethernet, FastEthernet, FDDI, Gigabit Ethernet, Token Ring

konsola GUI:

- Windows XP, 2000, NT, 9X, ME; Solaris, HP-UX, AIX

Produkty

Edytor reguł filtracji – GUI:

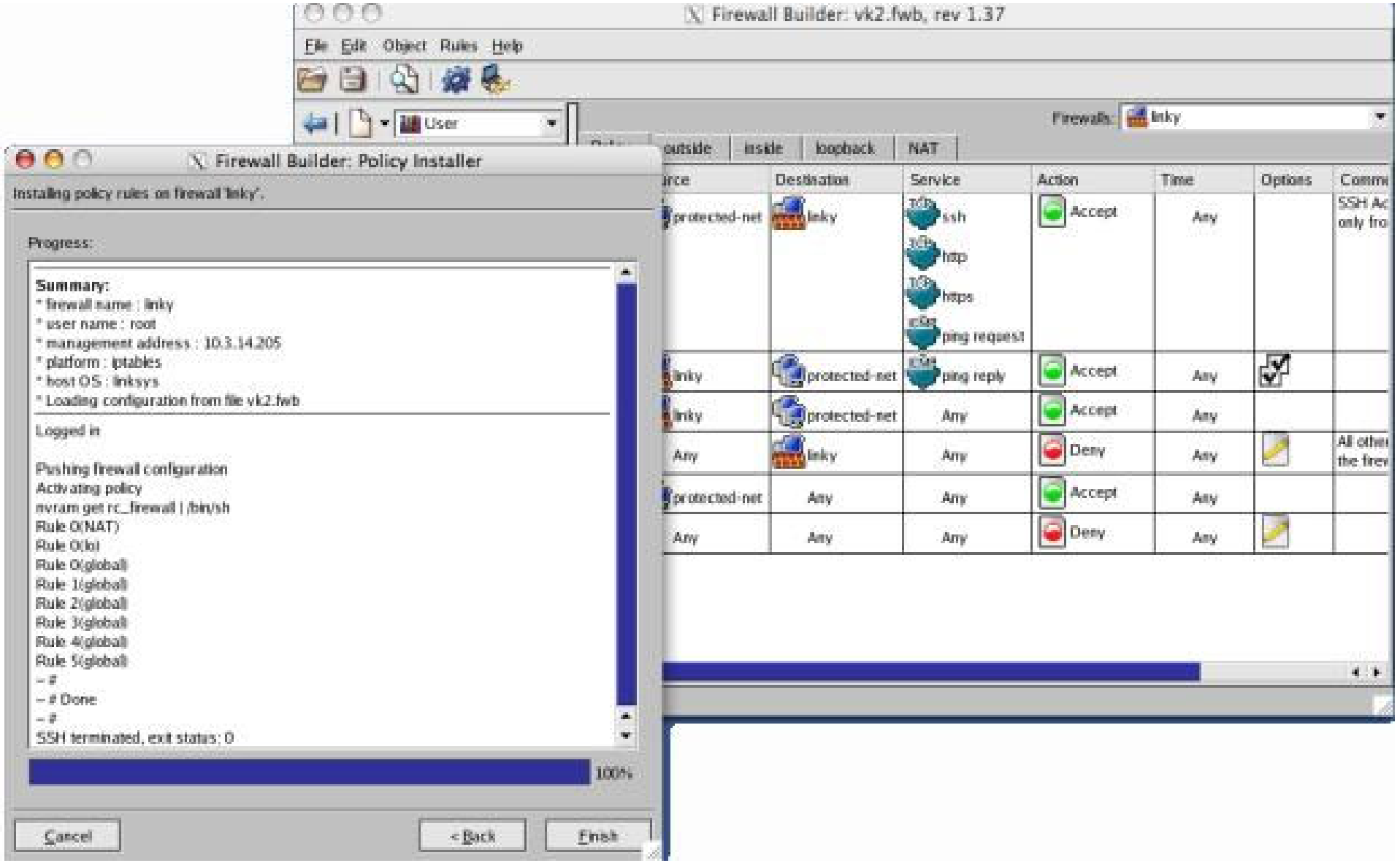


Produkty

Generatory reguł filtracji:

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

Produkty


Firewall Builder: vk2.fwb, rev 1.37
File Edit Object Rules Help
User
Firewalls: linky
outside inside loopback NAT
Destination Service Action Time Options
protected-net linky ssh http https ping request Accept Any
linky protected-net ping reply Accept Any
linky protected-net Any Accept Any
Any linky Any Deny Any
protected-net Any Any Accept Any
Any Any Any Deny Any
Firewall Builder: Policy Installer
Installing policy rules on firewall 'linky'.
Progress:
Summary:
* firewall name : linky
* user name : root
* management address : 10.3.14.205
* platform : iptables
* host OS : linksys
* Loading configuration from file vk2.fwb
Logged in
Pushing firewall configuration
Activating policy
nvram get rc_firewall | /bin/sh
Rule 0(NAT)
Rule 0(lo)
Rule 0(global)
Rule 1(global)
Rule 2(global)
Rule 3(global)
Rule 4(global)
Rule 5(global)
-- #
-- # Done
-- #
SSH terminated, exit status: 0
100%
Cancel
< Back
Finish

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

PIX 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 (głównie Windows)
- filtrujący ruch sieciowy wchodzący i wychodzący

przykłady:

Personal Firewall (Sygate)

Personal Firewall (Kerio)

Norton Personal Firewall (Symantec)

Desktop Firewall (McAffe)

BlackICE Defender (Network ICE)

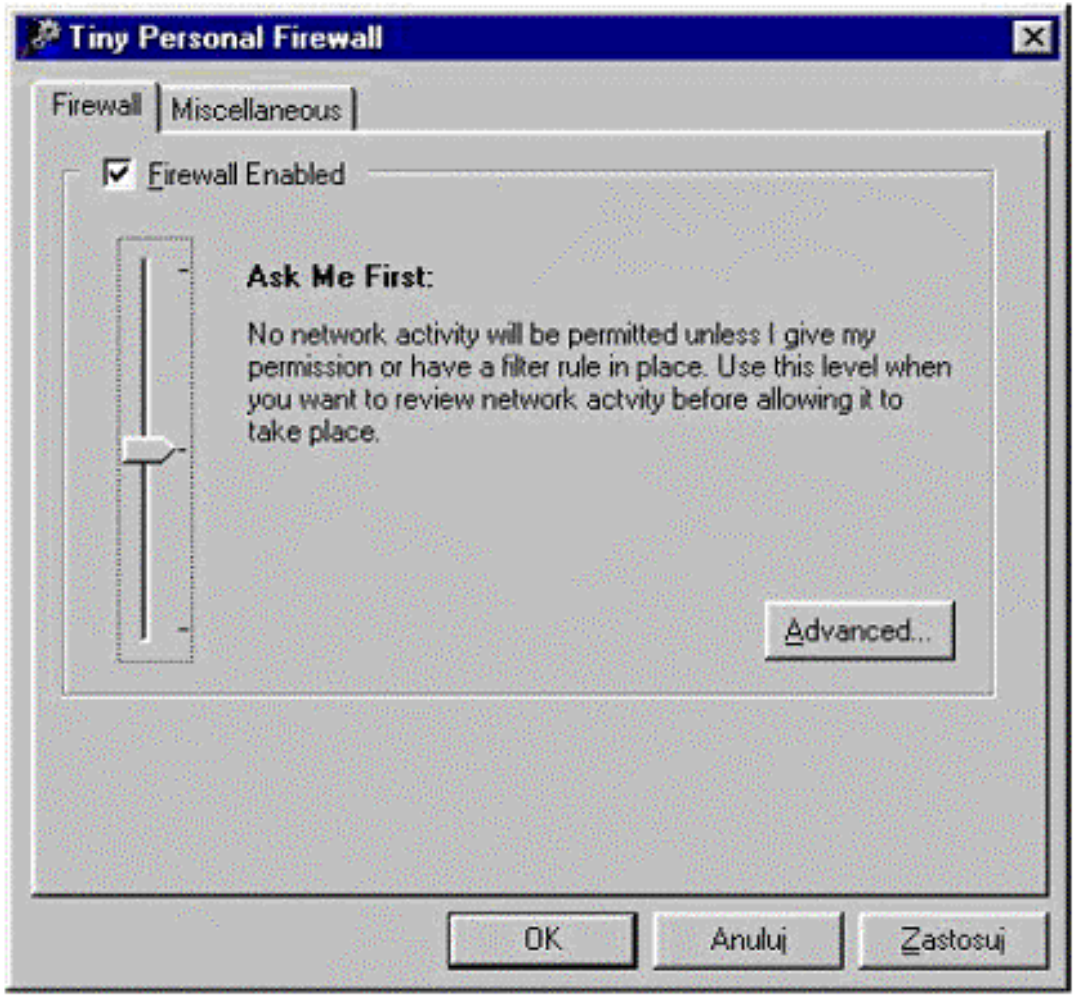
Interceptor (eSonic)

darmowe pakiety np. Tiny Firewall, Zone Alarm, Enigma Firewall

wrappery połączeń w systemach Unix/Linux, np. tcpd

Produkty

Tiny Firewall (Tiny Software)

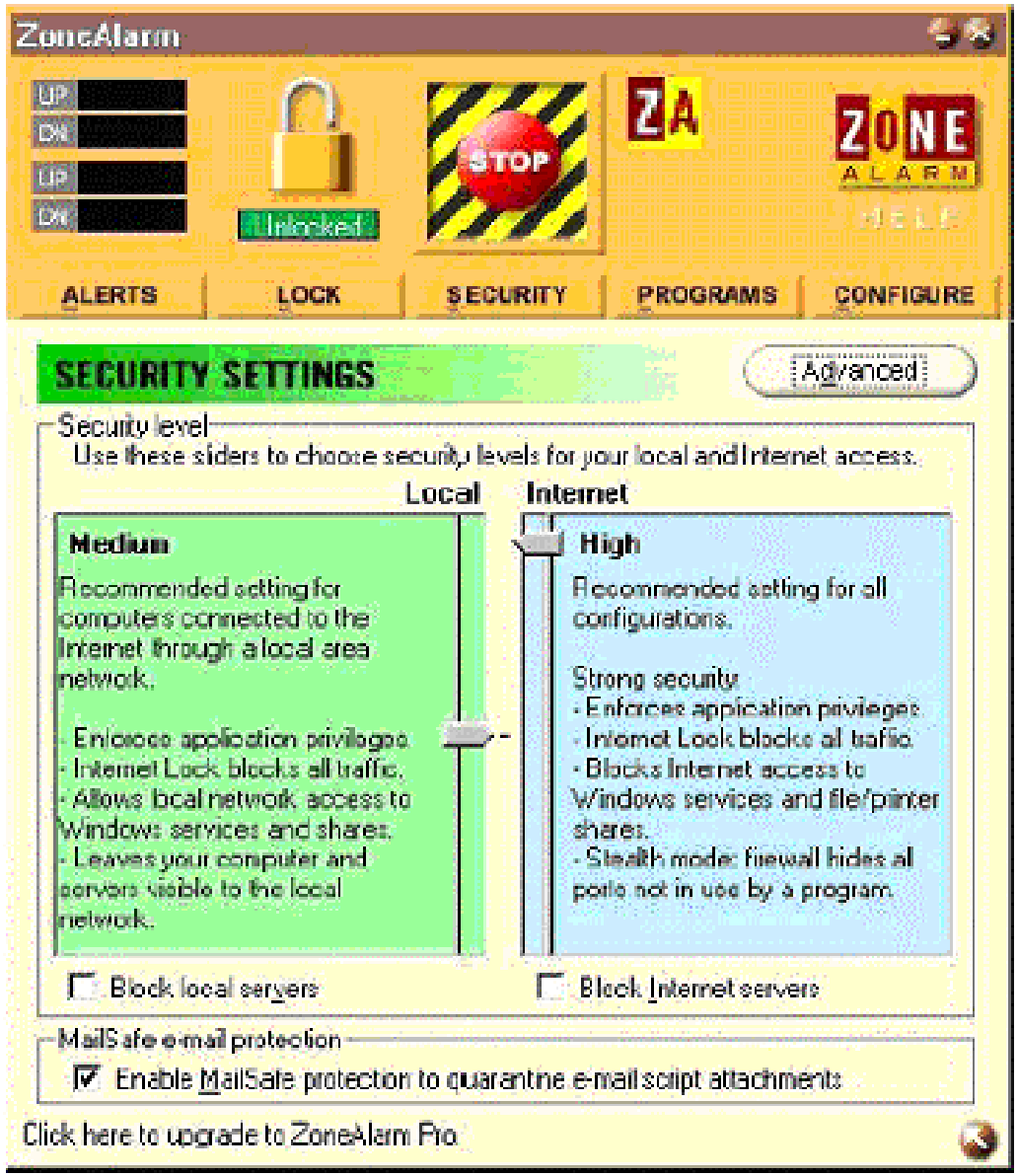


- uczenie się reguł
- m.in. detekcja wykorzystania `CreateRemoteThread()`

Produkty

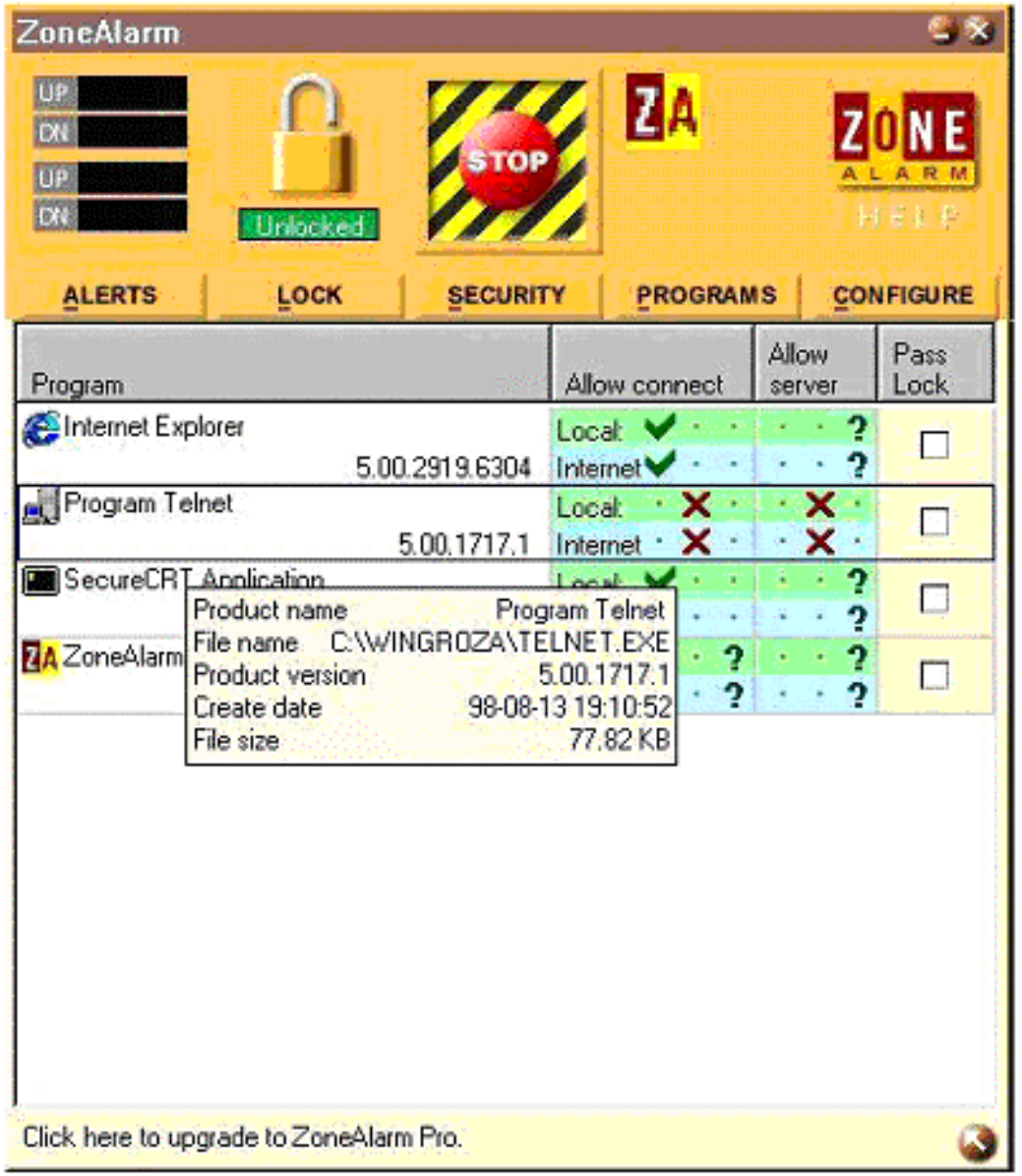
ZoneAlarm (Zone Labs)

- wydzielenie stref zaufanych (sieć lokalna) oraz niebezpiecznych (sieć publiczna)



Produkty

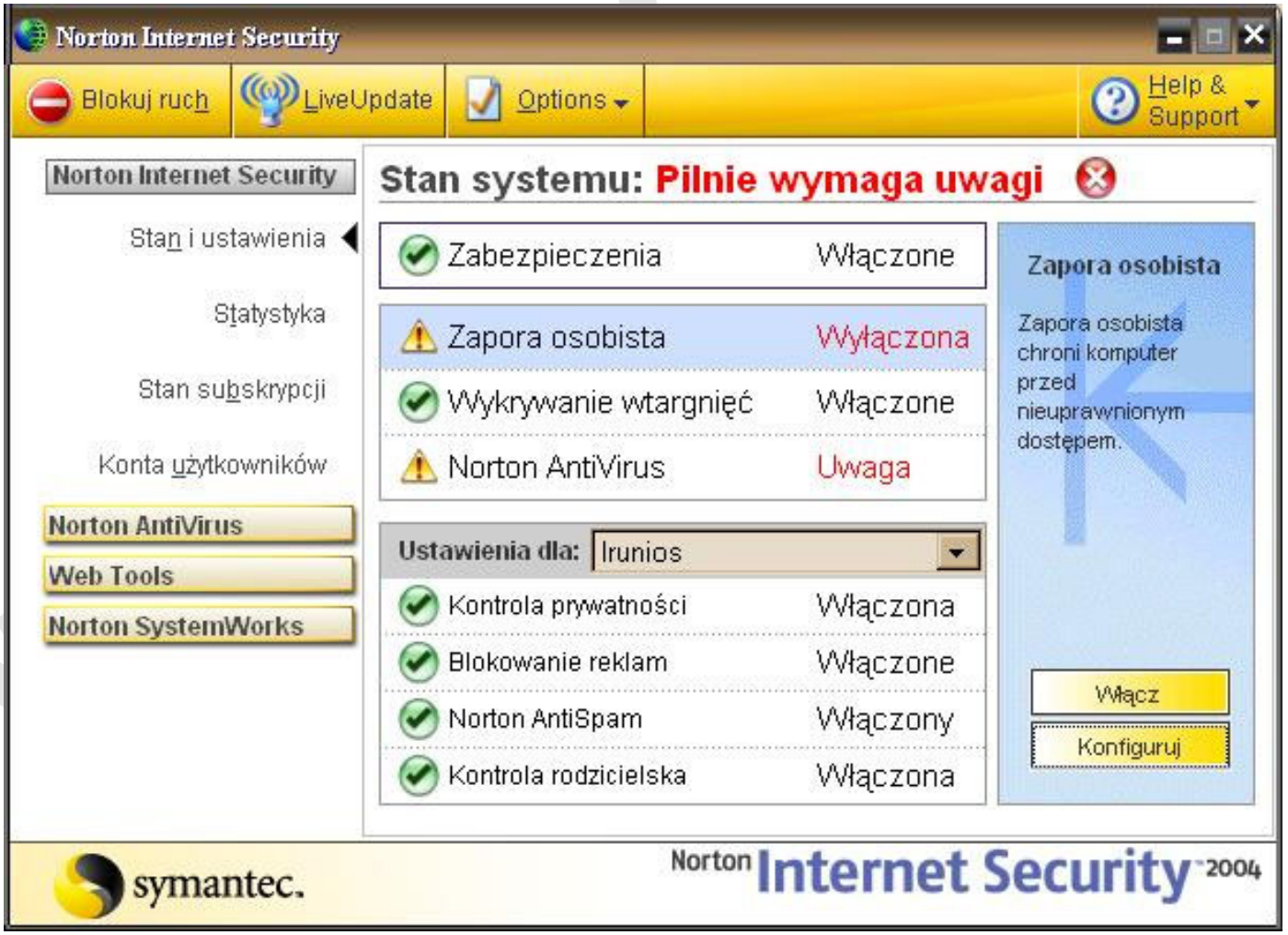
- kontrola dostępu do sieci na poziomie poszczególnych programów



Produkty

Norton Internet Security (Symantec)

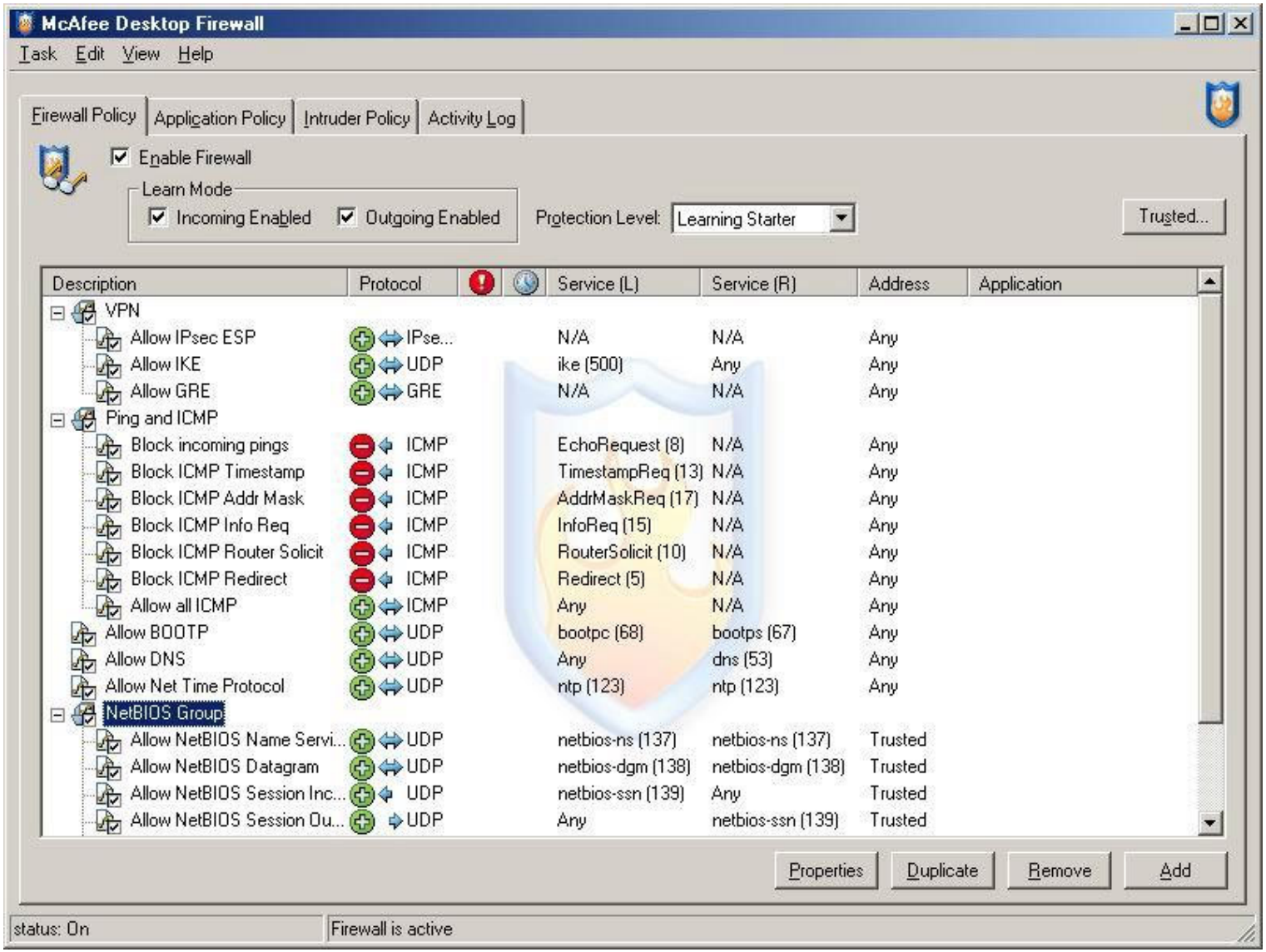
- personal firewall
- antywirus (poczta, komunikatory)
- ochrona przed atakami
- antyspamer
- filtr www (blokada reklam, cookies, i pop-up)
- wielopoziomowy parental-control



Produkty

Desktop Firewall (McAfee)

- predefiniowane reguły filtracji



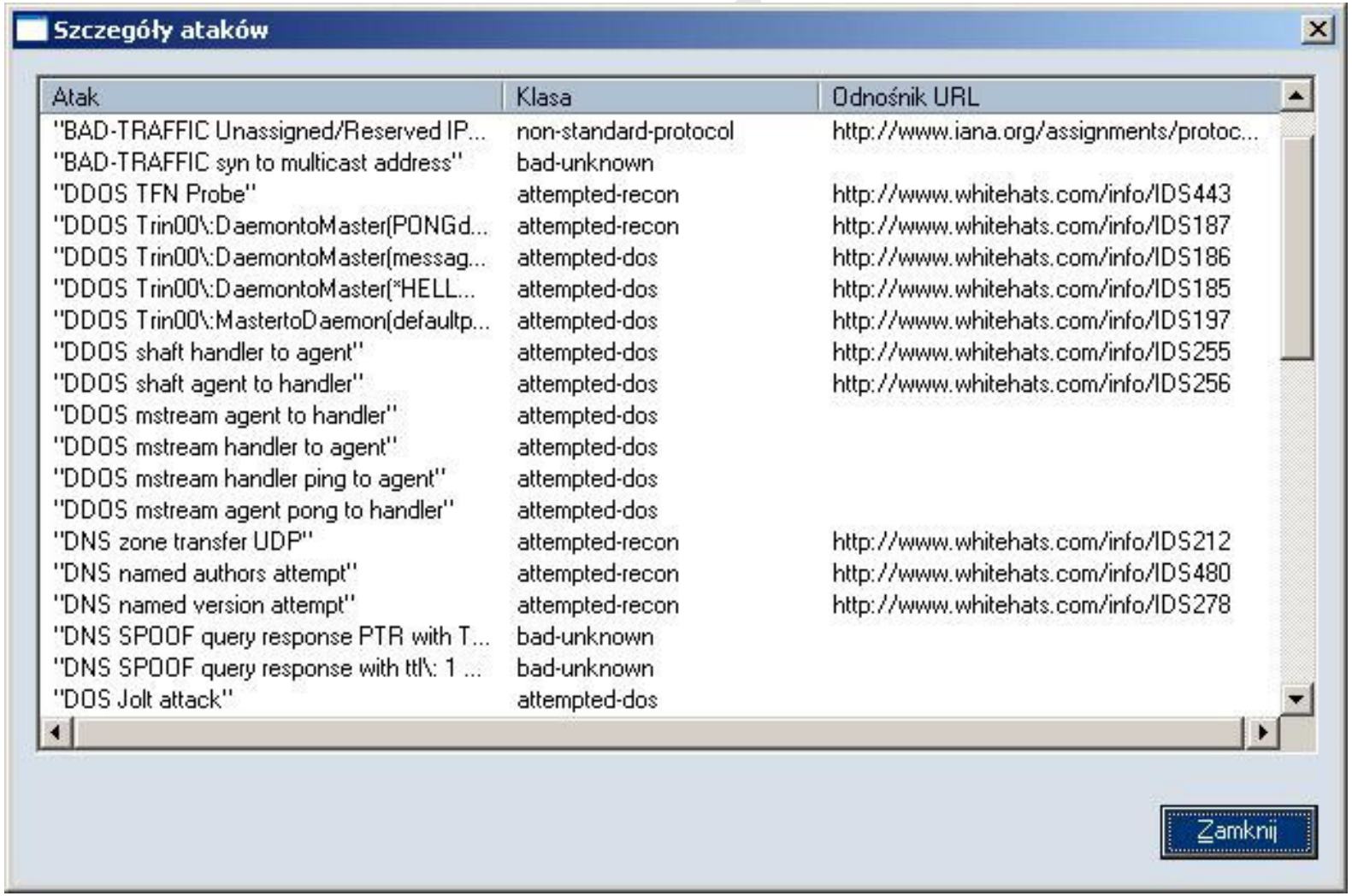
Produkty

- ochrona przed popularnymi atakami

Produkty

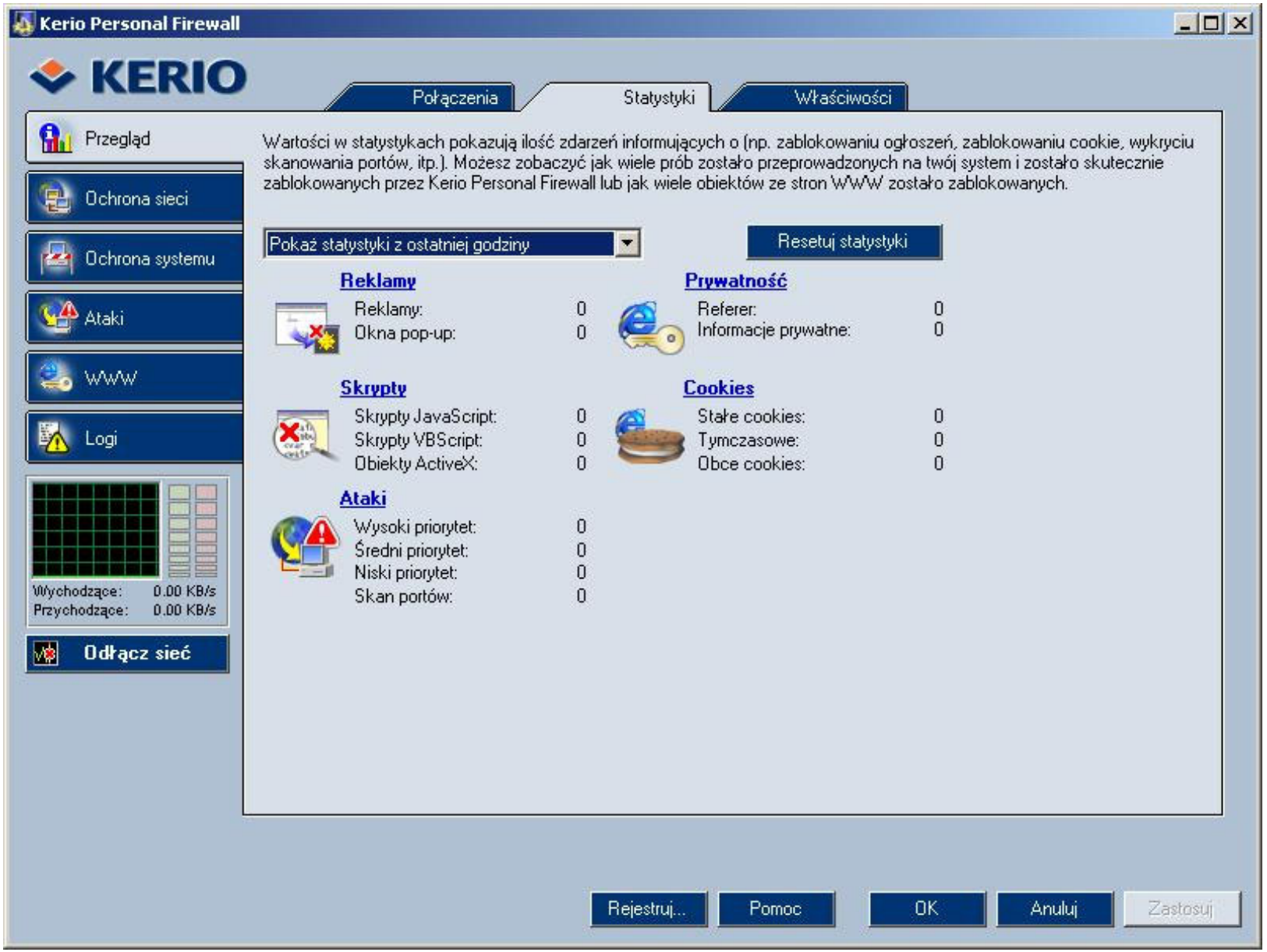
Kerio Personal Firewall (Kerio)

- obrona przed wieloma klasami ataków (wykorzystuje system detekcji Snort http://www.snort.org)



Produkty

- kompleksowa ochrona systemu
- w tym kontrola uruchamiania aplikacji i ich integralności



Produkty

Klasa: Bramy aplikacyjne

Przykłady

- najpowszechniejsze WWW proxy:

  Squid WWW Proxy – typowy WWW proxy + web cache

  Microsoft Proxy Server – oprócz usługi serwera (WebProxy Service) wymagana konfiguracja klientów: WinSock Proxy (WSP) dla MS Windows lub SOCKS proxy (dla klientów innych niż MS Windows); WSP obsługuje również IPX/SPX

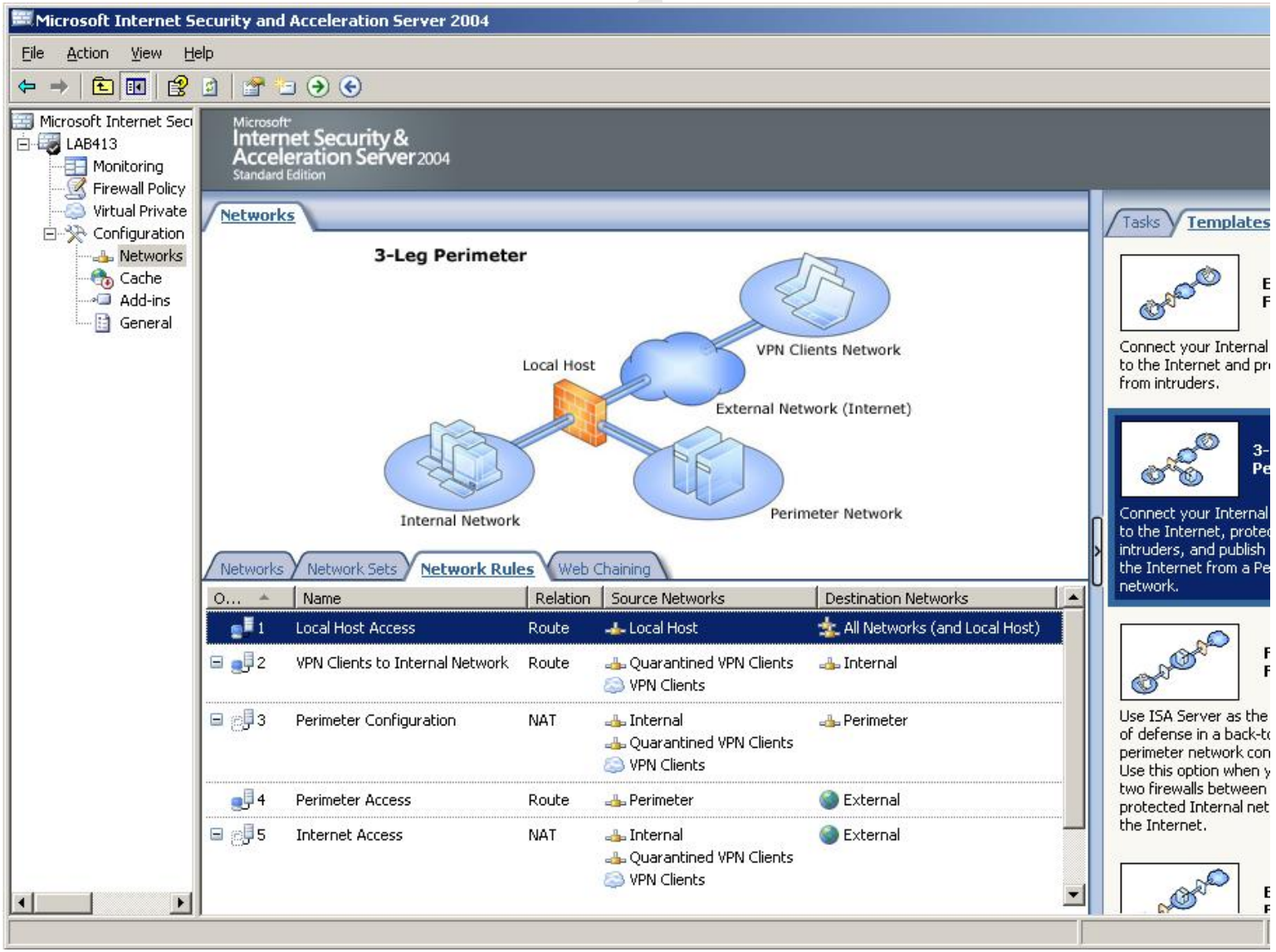
- inne:

  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

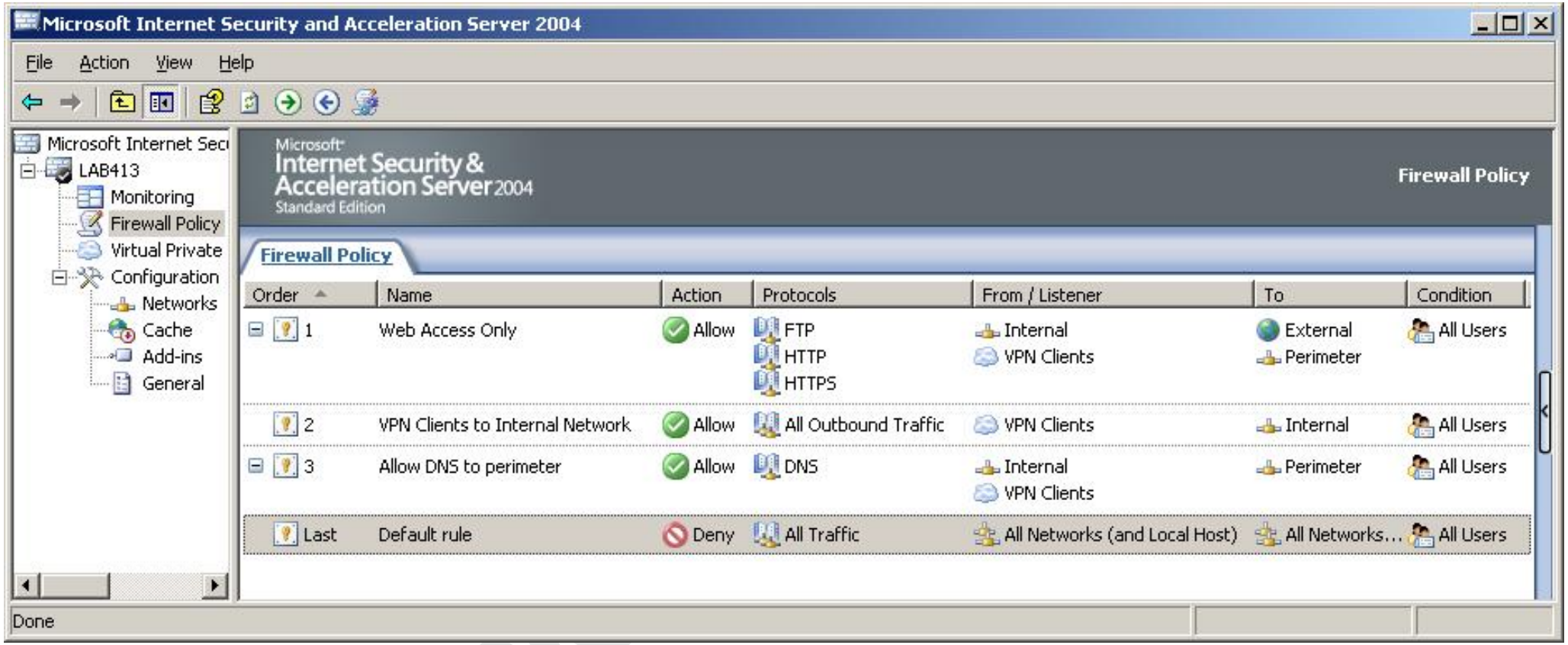
Produkty

Microsoft ISA 2004 (Internet Security & Acceleration Server)

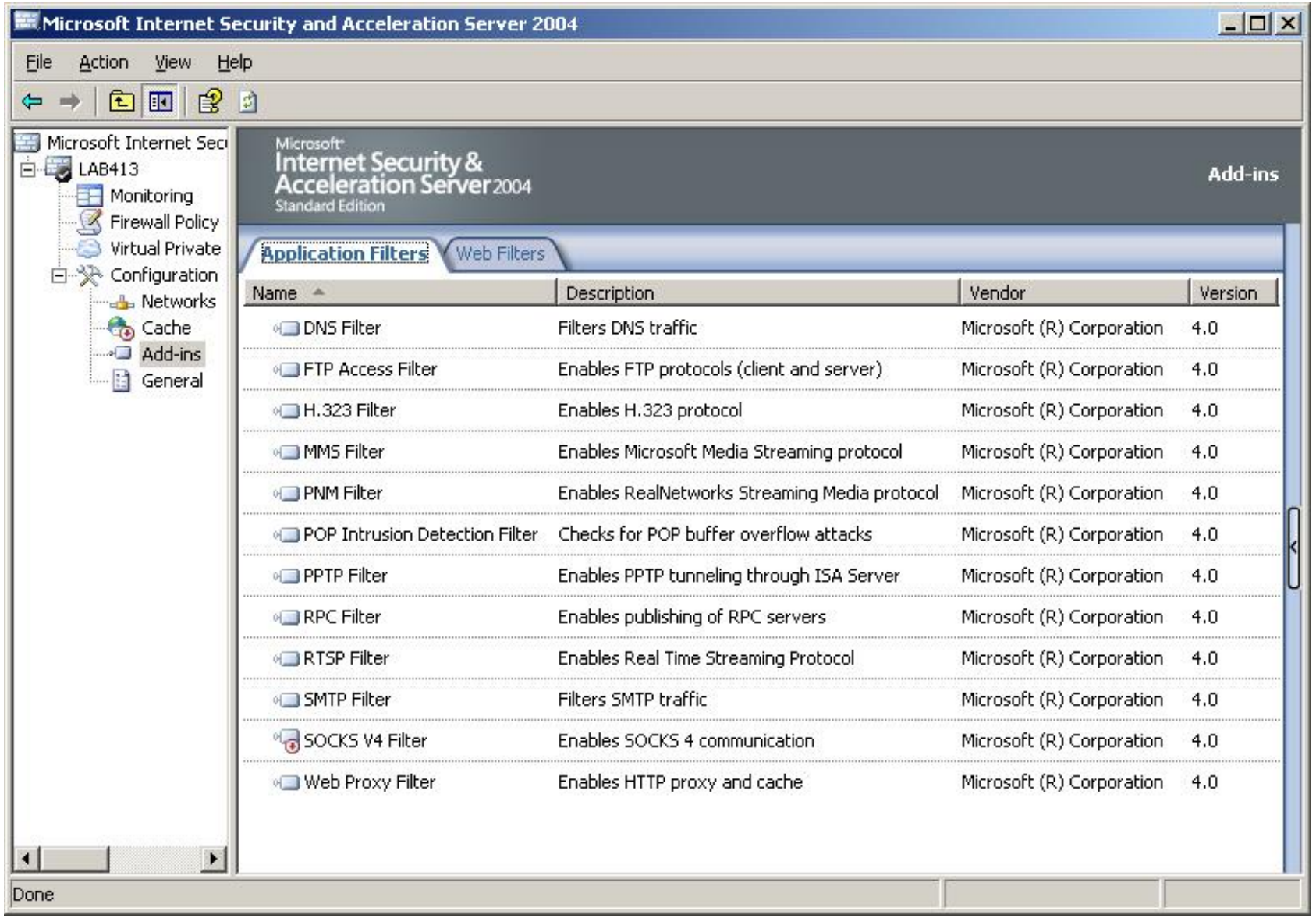
- oferowane również w sprzęcie (np. firmy Rimapp)
- wiele predefiniowanych konfiguracji (szablony)



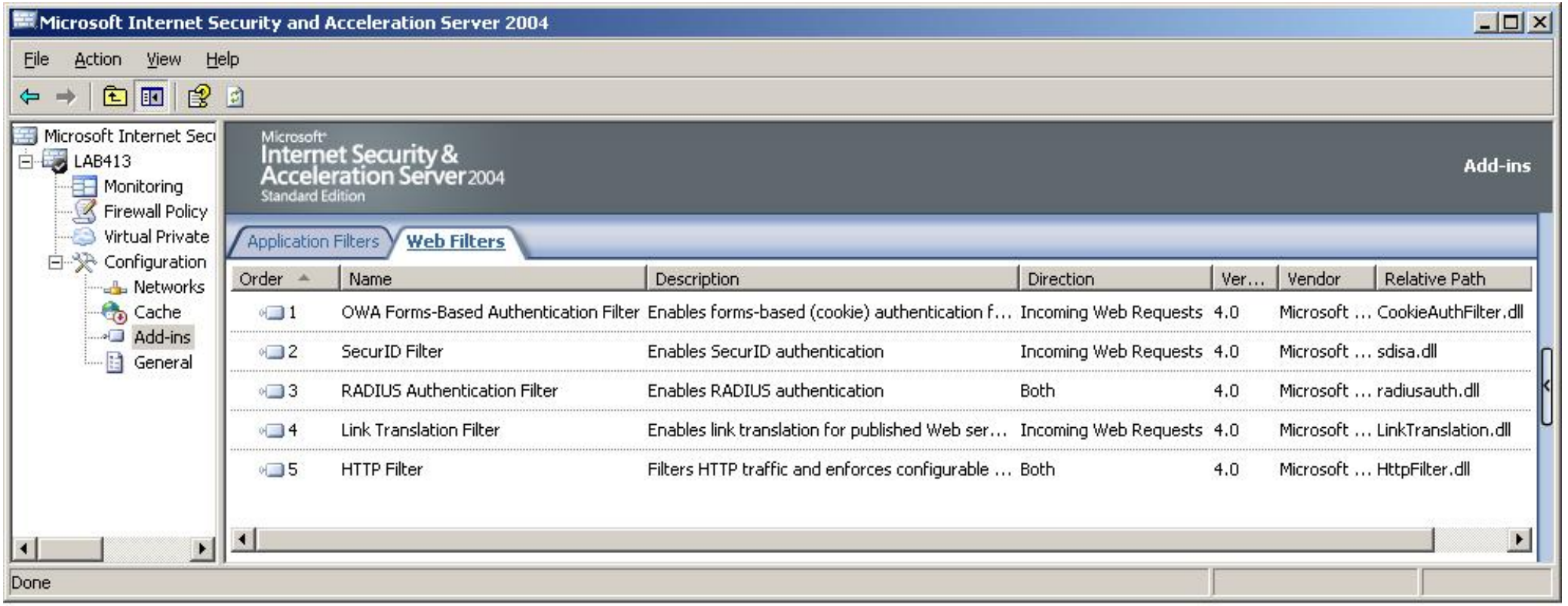
Produkty


Microsoft Internet Security and Acceleration Server 2004
File Action View Help
Microsoft Internet Sec
LAB413
Monitoring
Firewall Policy
Virtual Private
Configuration
Networks
Cache
Add-ins
General
Microsoft Internet Security & Acceleration Server 2004
Standard Edition
Firewall Policy
Firewall Policy
Order
Name
Action
Protocols
From / Listener
To
Condition
1
Web Access Only
Allow
FTP
HTTP
HTTPS
Internal
VPN Clients
External
Perimeter
All Users
2
VPN Clients to Internal Network
Allow
All Outbound Traffic
VPN Clients
Internal
All Users
3
Allow DNS to perimeter
Allow
DNS
Internal
VPN Clients
Perimeter
All Users
Last
Default rule
Deny
All Traffic
All Networks (and Local Host)
All Networks...
All Users
Done

Produkty


Microsoft Internet Security and Acceleration Server 2004
File Action View Help
Microsoft Internet Sec
LAB413
Monitoring
Firewall Policy
Virtual Private
Configuration
Networks
Cache
Add-ins
General
Microsoft
Internet Security & Acceleration Server 2004
Standard Edition
Add-ins
Application Filters
Web Filters
Name
Description
Vendor
Version
DNS Filter
Filters DNS traffic
Microsoft (R) Corporation
4.0
FTP Access Filter
Enables FTP protocols (client and server)
Microsoft (R) Corporation
4.0
H.323 Filter
Enables H.323 protocol
Microsoft (R) Corporation
4.0
MMS Filter
Enables Microsoft Media Streaming protocol
Microsoft (R) Corporation
4.0
PNM Filter
Enables RealNetworks Streaming Media protocol
Microsoft (R) Corporation
4.0
POP Intrusion Detection Filter
Checks for POP buffer overflow attacks
Microsoft (R) Corporation
4.0
PPTP Filter
Enables PPTP tunneling through ISA Server
Microsoft (R) Corporation
4.0
RPC Filter
Enables publishing of RPC servers
Microsoft (R) Corporation
4.0
RTSP Filter
Enables Real Time Streaming Protocol
Microsoft (R) Corporation
4.0
SMTP Filter
Filters SMTP traffic
Microsoft (R) Corporation
4.0
SOCKS V4 Filter
Enables SOCKS 4 communication
Microsoft (R) Corporation
4.0
Web Proxy Filter
Enables HTTP proxy and cache
Microsoft (R) Corporation
4.0
Done

Produkty


Microsoft Internet Security and Acceleration Server 2004
File Action View Help
Microsoft Internet Sec
LAB413
Monitoring
Firewall Policy
Virtual Private
Configuration
Networks
Cache
Add-ins
General
Microsoft Internet Security & Acceleration Server 2004
Standard Edition
Add-ins
Application Filters
Web Filters
Order
Name
Description
Direction
Ver...
Vendor
Relative Path
1 OWA Forms-Based Authentication Filter Enables forms-based (cookie) authentication f... Incoming Web Requests 4.0 Microsoft ... CookieAuthFilter.dll
2 SecurID Filter Enables SecurID authentication Incoming Web Requests 4.0 Microsoft ... sdisa.dll
3 RADIUS Authentication Filter Enables RADIUS authentication Both 4.0 Microsoft ... radiusauth.dll
4 Link Translation Filter Enables link translation for published Web ser... Incoming Web Requests 4.0 Microsoft ... LinkTranslation.dll
5 HTTP Filter Filters HTTP traffic and enforces configurable ... Both 4.0 Microsoft ... HttpFilter.dll
Done

Testy

Aplikacje testowe

- Tooleaky (http://tooleaky.zensoft.com)
- Yalta (http://www.soft4ever.com/security_test/En)
- Firehole (http://keir.net/firehole.html)

Skanery online

- SecuritySpace (http://www.securityspace.com/smysecure/single_index.html)
- Hackerwhacker (http://www.hackerwhacker.com)
- ShieldsUp (http://grc.com)
- PcFlank (http://www.pcflank.com/test.htm)
- Sygate (http://scan.sygatetech.com)

Testy

Certyfikaty ICSA Labs (www.icsalabs.com)

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