

Administrowanie usługami sieciowymi

IPTables

Arkadiusz Brzozowski

Marcin Woźniak

Część teoretyczna

IPTables to program sterujący filtrem pakietów głównie używanym jako zaporę sieciową opracowany dla Linuxa. Implementowany w miejsce ipchains począwszy od serii jądra 2.4.x. Jest to zaporę typu firewall. Głównym założeniem takiej zapory jest zapobieganie niepożądanemu dostępowi do sieci. Zaletami takiej zapory jest ochrona systemu przed zagrożeniem z zewnątrz i monitorowanie ruchu w sieci, ale też niestety ogranicza dostęp do internetu i wymaga częstych uaktualnień, gdyż nowych typów klientów sieciowych i serwerów przybywa prawie codziennie. Program ten służy do konfigurowania, utrzymywania i sprawdzania tabel reguł filtrowania pakietów IP w jądrze Linuksa. Można zdefiniować kilka różnych tabel. Każda tabela zawiera kilka wbudowanych łańcuchów i może również zawierać łańcuchy zdefiniowane przez użytkownika. Każdy łańcuch to lista reguł. Każda reguła określa, co zrobić z pakietem. Nazywa się to „celem”, który może być skokiem do łańcucha zdefiniowanego przez użytkownika w tej samej tabeli.

Ipchains to poprzednik programu **iptables**, stosowany w systemach z jądrem starszym niż 2.4.X. Jeden, jak i drugi program odpowiadał za filtrowanie pakietów na podstawie dopasowań z określonymi zestawami reguł. Jednak iptables oferuje bardziej rozszerzalny sposób filtrowania pakietów, dając administratorowi większą kontrolę bez nadmiernej złożoności systemu.

Podstawowe różnice to:

- Używając iptables, każdy filtrowany pakiet jest przetwarzany przy użyciu reguł tylko z jednego łańcucha, a nie wielu łańcuchów.
- Cel DENY został zastąpiony przez DROP.
- Porządek ma znaczenie przy umieszczaniu opcji w regule.
- Interfejsy sieciowe muszą być powiązane z odpowiednimi łańcuchami w regułach.

Rozwiązania alternatywne:

ZyXEL ZyWALL USG40/40w to brama zabezpieczająca najnowszej generacji o wysokiej wydajności. Chroni przed złośliwym oprogramowaniem poprzez sprzętowy firewall, antywirus, antyspam, filtrowanie treści, IDP (system wykrywania i zapobiegania włamaniom) oraz inspekcję SSL. Wbudowany kontroler WLAN umożliwia centralne zarządzanie punktami bezprzewodowymi. Posiada funkcję równoważenia ruchu sieciowego i połączeń zapasowych z obsługą mobilnych urządzeń szerokopasmowych.

Cisco PIX 515E to urządzenie zabezpieczające o wszechstronnej konstrukcji z jedną szafą (1RU). Obsługuje do sześciu interfejsów 10/100 Fast Ethernet. Zapewnia przepustowość do 188 Mbps z możliwością obsługi ponad 130 000 jednoczesnych sesji. Niektóre modele zawierają zintegrowaną sprzętową akcelerację VPN zapewniającą do 140 MB/s przepustowości 3DES VPN i 140 Mb/s przepustowości AES-256 VPN.

Cisco ASA to kolejne urządzenie sieciowe, którego głównym zadaniem jest ochrona naszej sieci przed intruzami oraz nieautoryzowanym dostępem. Wymieniona ochrona polega na blokowaniu niedozwolonego ruchu sieciowego. Główne zadanie urządzenia polega na

filtrowaniu pakietów tak by sieć była zabezpieczona oraz by w sposób bezpieczny był zapewniony do niej dostęp. Aby to było możliwe wykorzystywane są następujące mechanizmy: filtrowanie pakietów realizowane z wykorzystaniem listy dostępu ACL oraz filtrowanie stanowe.

Iptables umożliwia definiowanie tabel zawierających łańcuchy reguł stosowanych dla pakietów. Każda z tabel służy do przetwarzania pakietów różnego rodzaju i zawiera kilka łańcuchów. Wyróżniamy tabele: filter, nat, mangle oraz raw.

Tabela **filter** jest domyślną tabelą. Zawiera wbudowane łańcuchy:

- **INPUT** dla pakietów przeznaczonych do lokalnych gniazd
- **FORWARD** dla pakietów routowanych przez lokalny komputer
- **OUTPUT** dla pakietów generowanych lokalnie

Tabela **nat** jest sprawdzana, gdy napotkany jest pakiet tworzący nowe połączenie. Składa się z trzech wbudowanych łańcuchów:

- **PREROUTING** do zmiany pakietów, gdy tylko nadejdą
- **OUTPUT** do zmiany pakietów generowanych lokalnie przed routingiem
- **POSTROUTING** do zmiany pakietów, gdy mają wyjść

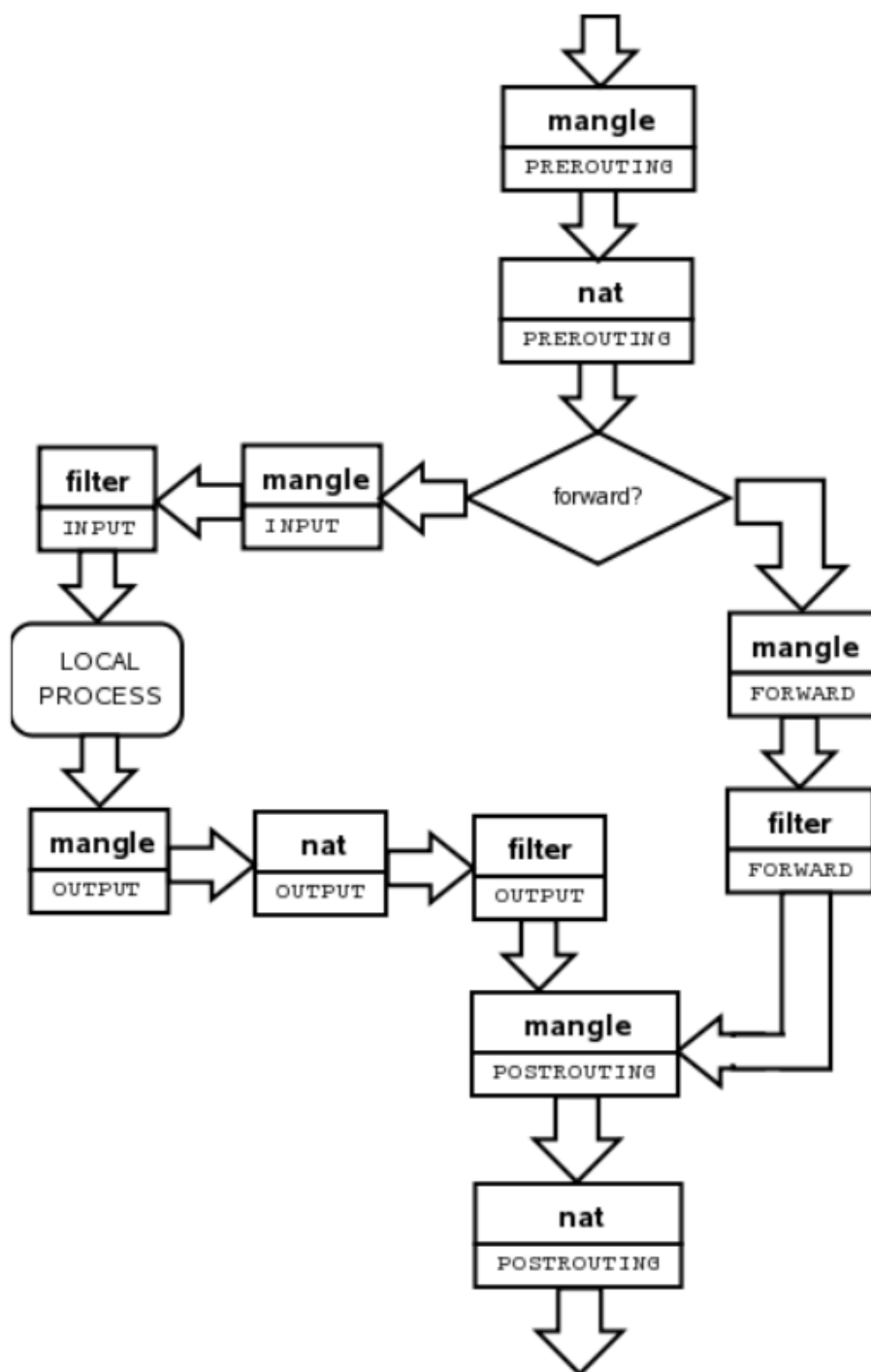
Tabela **mangle** jest używana do specjalistycznej zmiany pakietów. Zawiera łańcuchy:

- **PREROUTING** do zmiany przychodzących pakietów przed routingiem
- **OUTPUT** do zmiany pakietów generowanych lokalnie przed routingiem
- **INPUT** dla pakietów przychodzących do lokalnego komputera,
- **FORWARD** do zmiany pakietów kierowanych przez lokalny komputer
- **POSTROUTING** do zmiany pakietów w momencie, gdy mają wychodzić

Tabela **raw** jest używana głównie do konfigurowania zwolnień ze śledzenia połączeń w połączeniu z celem NOTRACK. Zawiera łańcuchy:

- **PREROUTING** dla pakietów przychodzących przez dowolny interfejs sieciowy
- **OUTPUT** dla pakietów generowanych przez lokalne procesy

Diagram przepływu pakietów przez zaporę sieciową IPTables



Na początku pakiet dociera do interfejsu wejściowego. Jeśli mamy pakiet routowany to idziemy w prawo, a jak nie, to w lewo. Dobieramy odpowiedni interfejs wejściowy. Tam są

wykonywane właściwe instrukcje i ostatecznie pakiet opuszcza stację przez interfejs wyjściowy.

Składnia polecenia IPTables:

Ogólna postać reguły:

iptables [-t tablica] komenda [wzorzec] [akcja]

Komendy:

- **-P [łańcuch] [polityka]** - ustawienie domyślnej polityki dla łańcucha. Domyślna polityka stosowana jest dopiero wówczas, gdy pakiet nie pasuje do żadnej reguły łańcucha.
- **-A [łańcuch]** - dodanie reguły do podanego łańcucha.
- **-I [łańcuch] [nr reguły]** - wstawienie reguły do podanego łańcucha, jeśli zostanie podany nr reguły wtedy reguła zostanie wpisana w to miejsce zmieniając kolejność pozostałych.
- **-L [łańcuch]** – wyświetlenie wszystkich reguł łańcucha, najczęściej używane z opcją -v.
- **-F [łańcuch]** – usunięcie wszystkich reguł z podanego łańcucha (lub ze wszystkich łańcuchów danej tablicy).
- **-D [łańcuch] [nr reguły]** – usunięcie konkretnej reguły w podanym łańcuchu, jeśli zostanie podany nr reguły wtedy zostanie usunięta reguła o tym numerze.
- **-R [łańcuch] [nr reguły]** – zastąpienie reguły o danym numerze w określonym łańcuchu.

Opcje wzorca:

- **-s [ip]** – adres IP źródłowy (może być uogólniony do adresu sieci)
- **-d [ip]** – adres IP docelowy (może być uogólniony do adresu sieci)
- **-p [protokół]** – wybór protokołu (tcp, udp, icmp lub all, czyli wszystkie protokoły stosu TCP/IP)
- **-i interfejs wejściowy**
- **-o interfejs wyjściowy**
- **--sport port:[port]** – port źródłowy
- **--dport port:[port]** – port docelowy
- **-m moduł** – załadowanie modułu rozszerzającego. Dzięki temu można wykorzystać kolejne opcje danego modułu

Najważniejsze akcje:

- **-j ACCEPT** – przepuszczanie dopasowanych pakietów
- **-j DROP** – usunięcie dopasowanych pakietów
- **-j REJECT** – odrzucenie dopasowanych pakietów
- **-j LOG** – logowanie dopasowanych pakietów bez usunięcia ich z łańcucha
- **-j RETURN** – usunięcie pakietu z łańcucha, pozwalając jednocześnie, aby pakiet był dalej sprawdzany w kolejnych łańcuchach
- **-j SNAT** – translacja adresów źródłowych
- **-j DNAT** – translacja adresów docelowych

- **-j SAME** – translacja adresów źródłowych i docelowych
- **-j REDIRECT** – przekierowanie pakietów do lokalnego systemu
- **-j MASQUERADE** – translacja adresów źródłowych na dynamicznie przyznawany na interfejsie adres

Przykłady wywołań polecenia *iptables*:

- Wylistowanie wszystkich reguł:
iptables -L -v
- Stworzenie nowego łańcucha(o nazwie CwAUS, domyślnie utworzy się w tabeli filter):
iptables -N CwAUS
- Dodanie CwAUS jako cel do łańcucha INPUT:
iptables -A INPUT -j CwAUS
- Dodanie reguły z akceptacją połączeń z http oraz HTTPS(-D w miejsce -A jeśli chcemy usunąć):
iptables -A CwAUS -p tcp -m multiport --dports 80,443 -j ACCEPT
- Dodanie reguły z akceptacją pakietów icmp z sieci 158.75.112.0/24
iptables -A CwAUS -s 158.75.112.0/24 -p icmp -j ACCEPT
- Opróżnienie łańcucha CwAUS z reguł w nim umieszczonych
iptables -F CwAU
- Usunięcie łańcucha CwAUS
iptables -X CwAUS

Cele reguł dostępne w tabeli *filter*:

- **ACCEPT** – IPtables zatrzymuje dalsze przetwarzanie, a pakiet przekazywany jest do końca aplikacji lub systemu operacyjnego do przetworzenia.
- **DROP** – IPtables zatrzymuje dalsze przetwarzanie, a pakiet zostaje zablokowany.
- **LOG** – informacje o pakiecie są wysyłane do syslog daemon do logowania. IPtables kontynuuje przetwarzanie z kolejną regułą w tabeli. Ponieważ nie możemy wykonać LOG i DROP w tym samym czasie, dlatego najpierw wykona się LOG, później DROP.
- **REJECT** – działa tak jak DROP, ale REJECT zwróci dodatkowo komunikat o błędzie do hosta wysyłającego, który pakiet został zablokowany.
- **DNAT** – służy do tłumaczenia adresu sieci docelowej.
- **SNAT** – służy do tłumaczenia źródłowych adresów sieciowych przepisując źródłowy adres IP pakietu. Adres źródłowy definiowany jest przez użytkownika.
- **MASQUE RADE** – służy do tłumaczenia adresu sieci źródłowej. Domyślnie źródłowy adres IP jest taki sam, jak używany przez interfejs zapory.

iptables-save jest używane w celu zrzucenia zawartości tabeli IP w łatwo przetwarzalnym formacie na standardowe wyjście. Wyróżniamy **iptables-save** dla IP wersji 4 oraz **ip6tables-save** dla IP wersji 6. Składnia:

➤ **iptables-save** [-M modprobe] [-c] [-t tabela]

➤ **ip6tables-save** [-M modprobe] [-c] [-t tabela]

-M (modprobe program) – podaje ścieżkę do programu modprobe. Domyślnie określana ścieżka na podstawie /proc/sys/kernel/modprobe.

-c, --counters – dołącza do wyjścia bieżące wartości wszystkich pakietów i liczników bajtów.

-t, --table (nazwa tabeli) – ogranicza wyjście tylko do jednej tabeli. Jeśli nie podano, wyjście zawiera wszystkie dostępne tabele.

iptables-restore jest używane, aby przywrócić tabele IP z danych podanych na standardowym wejściu. Wyróżniamy **iptables-restore** dla IP wersji 4 oraz **ip6tables-restore** dla IP wersji 6. Składnia:

➤ **iptables-restore** [-chntv] [-M modprobe]

➤ **ip6tables-restore** [-chntv] [-M modprobe] [-T nazwa]

-c, --counters – przywraca wartości wszystkich pakietów i liczników bajtów

-h, --help – wyświetla krótkie podsumowanie opcji programu.

-n, --noflush – nie opróżnia poprzedniej zawartości tabeli. Jeśli nie podano, zostanie opróżniona cała poprzednia zawartość odpowiedniej tabeli.

-t, --test - tylko przetwarza i tworzy zbiór reguł, ale go nie wykonuje.

-v, -verbose – wypisuje dodatkowe informacje, przydatne do debugowania, podczas przetwarzania zbioru reguł.

-M (modprobe program) – podaje ścieżkę do programu modprobe. Domyślnie określana ścieżka na podstawie /proc/sys/kernel/modprobe.

-T, --table (nazwa tabeli) – przywraca tylko tabelę o danej nazwie, nawet jeśli strumień wejściowy zawiera inne tabele.

Domyślne reguły dla *iptables* w Fedora 31, którego używamy, znajdują się w pliku /etc/sysconfig/iptables.

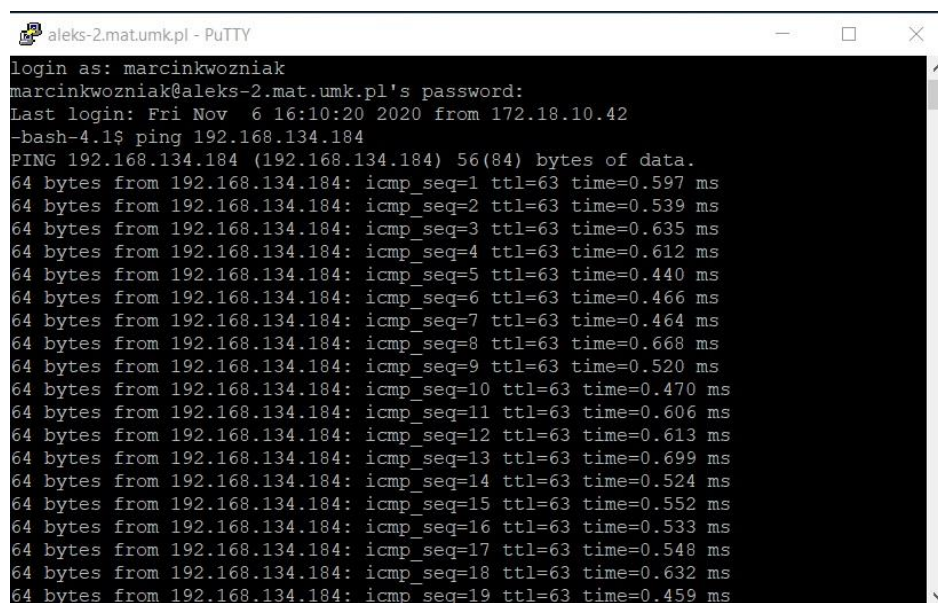
Część praktyczna

1. Zawartość łańcucha:

```
[root@localhost marcin]# iptables -L CwAUS -v
Chain CwAUS (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- lo any anywhere anywhere
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:ssh
0 0 ACCEPT tcp -- any any anywhere anywhere multiport dports http,https
0 0 ACCEPT tcp -- any any anywhere anywhere ctstate RELATED,ESTABLISHED
0 0 REJECT icmp -- any any 158.75.112.120 anywhere reject-with icmp-host-unreachable
0 0 ACCEPT icmp -- any any 158.75.112.0/24 anywhere
0 0 ACCEPT icmp -- any any 158.75.2.0/24 anywhere
0 0 ACCEPT icmp -- any any 192.168.134.0/24 anywhere
19 3505 DROP all -- any any anywhere anywhere
```

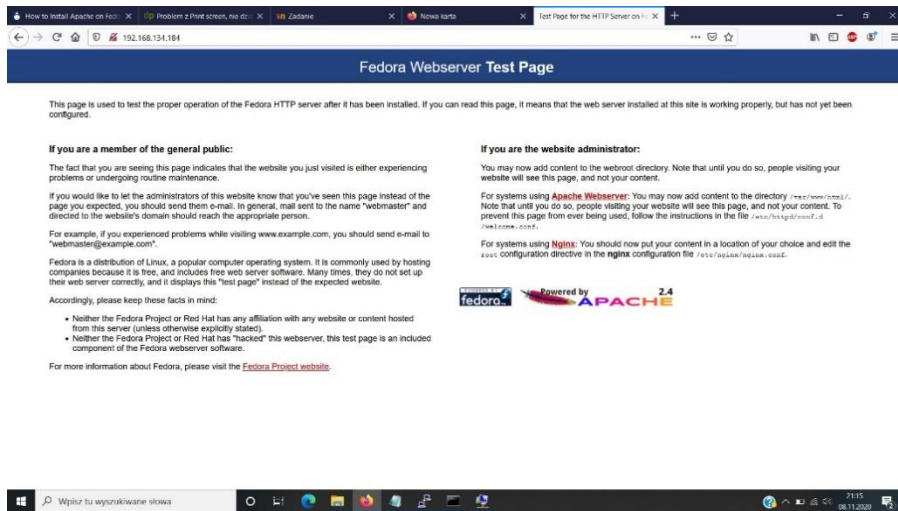
2. Dostępność :

ICMP- działający ping z maszyny aleks-2:



```
aleks-2.mat.umk.pl - PuTTY
login as: marcinkwozniak
marcinkwozniak@aleks-2.mat.umk.pl's password:
Last login: Fri Nov 6 16:10:20 2020 from 172.18.10.42
-bash-4.1$ ping 192.168.134.184
PING 192.168.134.184 (192.168.134.184) 56(84) bytes of data.
64 bytes from 192.168.134.184: icmp_seq=1 ttl=63 time=0.597 ms
64 bytes from 192.168.134.184: icmp_seq=2 ttl=63 time=0.539 ms
64 bytes from 192.168.134.184: icmp_seq=3 ttl=63 time=0.635 ms
64 bytes from 192.168.134.184: icmp_seq=4 ttl=63 time=0.612 ms
64 bytes from 192.168.134.184: icmp_seq=5 ttl=63 time=0.440 ms
64 bytes from 192.168.134.184: icmp_seq=6 ttl=63 time=0.466 ms
64 bytes from 192.168.134.184: icmp_seq=7 ttl=63 time=0.464 ms
64 bytes from 192.168.134.184: icmp_seq=8 ttl=63 time=0.668 ms
64 bytes from 192.168.134.184: icmp_seq=9 ttl=63 time=0.520 ms
64 bytes from 192.168.134.184: icmp_seq=10 ttl=63 time=0.470 ms
64 bytes from 192.168.134.184: icmp_seq=11 ttl=63 time=0.606 ms
64 bytes from 192.168.134.184: icmp_seq=12 ttl=63 time=0.613 ms
64 bytes from 192.168.134.184: icmp_seq=13 ttl=63 time=0.699 ms
64 bytes from 192.168.134.184: icmp_seq=14 ttl=63 time=0.524 ms
64 bytes from 192.168.134.184: icmp_seq=15 ttl=63 time=0.552 ms
64 bytes from 192.168.134.184: icmp_seq=16 ttl=63 time=0.533 ms
64 bytes from 192.168.134.184: icmp_seq=17 ttl=63 time=0.548 ms
64 bytes from 192.168.134.184: icmp_seq=18 ttl=63 time=0.632 ms
64 bytes from 192.168.134.184: icmp_seq=19 ttl=63 time=0.459 ms
```

HTTP- domyślna strona po zainstalowaniu apache:



3. Niemożliwe spingowanie z ultra60:

```

158.75.112.120 - PuTTY
login as: marcinkwozniak
Using keyboard-interactive authentication.
Password for marcinkwozniak@ultra60:
Last login: Fri Nov  6 16:03:33 2020 from 172.18.10.42
[marcinkwozniak@ultra60 ~]$ ping 192.168.134.184
PING 192.168.134.184 (192.168.134.184): 56 data bytes
92 bytes from 192.168.134.184: Destination Host Unreachable
Vr HL TOS Len  ID Flg  off TTL Pro  cks      Src      Dst
 4  5  00 0054 d7a9   0 0000 3f  01 4ddb 158.75.112.120 192.168.134.184

92 bytes from 192.168.134.184: Destination Host Unreachable
Vr HL TOS Len  ID Flg  off TTL Pro  cks      Src      Dst
 4  5  00 0054 d7aa   0 0000 3f  01 4dda 158.75.112.120 192.168.134.184

92 bytes from 192.168.134.184: Destination Host Unreachable
Vr HL TOS Len  ID Flg  off TTL Pro  cks      Src      Dst
 4  5  00 0054 c28e   0 0000 3f  01 62f6 158.75.112.120 192.168.134.184

92 bytes from 192.168.134.184: Destination Host Unreachable
Vr HL TOS Len  ID Flg  off TTL Pro  cks      Src      Dst
 4  5  00 0054 a32f   0 0000 3f  01 8255 158.75.112.120 192.168.134.184

```

4. Aby zachować nasze ustawienia iptables tak, aby działały po restarcie systemu należy użyć komendy:

Iptables-save > /etc/sysconfig/iptables

Bibliografia

https://www.powerserver.pl/d9042_zyxel_zywall_usg_40_i_40w.html

<https://www.cisco.com/web/ANZ/cpp/refguide/hview/security/pix.html>

<https://www.bhpex.pl/blog/informatyka/cisco-asa-podstawowa-konfiguracja/>

http://wazniak.mimuw.edu.pl/index.php?title=Bezpiecze%C5%84stwo_system%C3%B3w_komputerowych_laboratorium_12:Systemy_programowych_zap%C3%B3r_siec_iowych#Modu.C5.82y_rozszerzaj.C4.85ce_IPTABLES

https://www.researchgate.net/publication/299846030_Packet_Filtering_using_IP_Tables_in_Linux

<http://manpages.ubuntu.com/manpages/bionic/pl/man8/iptables-save.8.html>

<http://manpages.ubuntu.com/manpages/bionic/pl/man8/iptables-restore.8.html>

<https://linux.die.net/man/8/iptables>

https://docs.fedoraproject.org/en-US/Fedora/11/html/Security_Guide/sect-Security_Guide-IPTables-Differences_Between_IPTables_and_IPChains.html