|  |
| --- |
| Zaawansowane IP-Tables  Zasoby sieciowe zarządzanie i ochrona |

­­Paweł Ochota

Joanna Treder

Spis treści

[**1.** **Wstęp teoretyczny** 3](#_Toc324709753)

[**2.** **Podstawowa składnia IP-Tables - przypomnienie.** 5](#_Toc324709754)

[**3.** **Moduły** 8](#_Toc324709755)

[**4.** **ICMP** 9](#_Toc324709756)

[**5.** **MAC** 9](#_Toc324709757)

[**6.** **STATE** 10](#_Toc324709758)

[**7.** **COMMENT** 12](#_Toc324709759)

[**8.** **MULTIPORT** 12](#_Toc324709760)

[**9.** **LIMIT** 13](#_Toc324709761)

[**10.** **CONNLIMIT** 13](#_Toc324709762)

[**11.** **TIME** 14](#_Toc324709763)

[**12.** **TTL** 14](#_Toc324709764)

[**13.** **CONNTRACK** 15](#_Toc324709765)

[**14.** **MARK** 17](#_Toc324709766)

[**15.** **CONNMARK** 17](#_Toc324709767)

[**16.** **IPRANGE** 17](#_Toc324709768)

[**17.** **L7-FILTER** 18](#_Toc324709769)

[**18.** **Ćwiczenia** 20](#_Toc324709770)

[**19.** **Bibliografia** 21](#_Toc324709771)

1. **Wstęp teoretyczny**

Polecenie iptables służy do konfigurowania, zarządzania i inspekcji tablic zawierających reguły filtra pakietów znajdującego się w jądrze Linuksa. W systemach unixowych używane jest jako zapora sieciowa.

Moduł iptables składa się z tablic, z których każda zawiera wbudowane łańcuchy oraz może zawierać łańcuchy zdefiniowane przez użytkownika. Działanie iptables opiera się na trzech łańcuchach reguł filtrowania: INPUT (ruch przychodzący), OUTPUT (ruch wychodzący), FORWARD (ruch przechodni).

Każdy łańcuch jest tak naprawdę listą reguł, które określają kryteria dla pakietu. Jeżeli dany pakiet spełnia kryteria określone w regule to zostaje wykonana akcja. Ta akcja w dosłownym tłumaczeniu nazywa się celem (*ang. target*) i może być przekierowaniem do innego łańcucha w tej samej tablicy.

Celem może być nazwa łańcucha zdefiniowanego przez użytkownika lub jedna ze specjalnych wartości:

* **ACCEPT** - przepuszcza pakiet
* **DROP** - Blokuje i usuwa pakiet
* **REJECT** - Blokuje i usuwa pakiet oraz powiadamia o tym nadawcę
* **QUEUE** - Przepuszcza pakiet do przestrzeni użytkownika

Tablice dostępne w module iptables to:

* **filter** - Zawartość tej tablicy jest domyślnie pokazywana po wydaniu polecenia iptables --list. Jest to główna tabela, w której najczęściej tworzy się reguły. Domyślnie zawiera 3 łańcuchy:
  1. INPUT - obsługuje pakiety przychodzące z zewnątrz przeznaczone do lokalnego hosta,
  2. FORWARD - obsługuje pakiety routowane przez hosta (pomiędzy interfejsami sieciowymi),
  3. OUTPUT - obsługuje pakiety generowanie lokalnie przez hosta na którym pracuje netfilter.
* **nat** - Tablica stosowana jest dla pakietów, które nawiązują nowe połączenie. Zawiera 3 domyślne łańcuchy:
  1. PREROUTING - służy do modyfikowania pakietów przychodzących,
  2. OUTPUT - służy do modyfikowania pakietów generowanych lokalnie jeszcze przed routingiem,
  3. POSTROUTING - służy do modyfikowania pakietów, tuż przed wysłaniem.
* **mangle -** W tablicy tej należy umieszczać reguły, które zmieniają pakiety, ale nie są NATowane. W tej tablicy widoczne są wszystkie pakiety należące do danego połączenia. Dzieli się ona na 5 domyślnych łańcuchów:
  1. INPUT - obsługuje pakiety przychodzące z zewnątrz przeznaczone dla lokalnego hosta,
  2. OUTPUT — obsługuje pakiety generowanie lokalnie przez hosta na którym pracuje netfilter,
  3. FORWARD — obsługuje pakiety routowane przez hosta,
  4. PREROUTING - służy do modyfikowania pakietów przychodzących,
  5. POSTROUTING - służy do modyfikowania pakietów tuż przed wysłaniem.
* **raw** - Używana przed wszystkimi innymi tablicami. Zawiera następujące łańcuchy:
  1. PREROUTING- dla pakietów przychodzących przez jakiekolwiek urządzenie sieciowe (w rozumieniu eth0, ppp0, lo itd.),
  2. OUTPUT - dla pakietów wygenerowanych przez lokalne procesy.

1. **Podstawowa składnia IP-Tables - przypomnienie.**

Podstawowa składnia do budowania reguł wygląda następująco:

|  |
| --- |
| **# iptables [-t tabela] komenda [łańcuch] [!] [wzorzec] [akcja]** |

**Wyjaśnienie słów kluczowych zawartych w powyższych instrukcjach**:

**[tabela] -**- nazwa jednej z czterech wbudowanych tabel. Te tabele to: filter, nat, mangle oraz raw. Nie podając parametru [-t] domyślnie polecenie dotyczyło będzie tabeli filter.

**[komenda]** - instrukcje służące do dodawania, usuwania, modyfikowania i ogólnie zarządzania łańcuchami iptables. Określone zostały jako:

-A (--append) [reguła]– dodanie reguły na końcu łańcucha.

-D (--delete) [łańcuch] [reguła | nr reguły] – Usunięcie podanej reguły w podanym łańcuchu. Podanie numery usunie regułę o tym numerze.

-R (--replace) łańcuch [reguła] [nr reguły] – Podmiana podanej reguły podanego łańcucha.

-I (--insert) łańcuch [reguła] [nr reguły]– Włożenie reguły do podanego łańcucha i jego wiersza. Bez podania numeru wiersza domyślnie reguła zostanie włożona do pierwszego wiersza.

-L (--list) – Wyświetlenie wszystkich reguł w podanej tabeli. Dodatkowo wykorzystywane z parametrami:

* -n – wyświetla przy listowaniu przez -L adresy IP hostów zamiast ich nazw (domyślnie iptables próbuje rozwiązać nazwy i wyświetlić nazwy hostów).
* -v - przy listowaniu pokazuje ilość wysłanych/odebranych przez dany łańcuch pakietów i bajtów oraz domyślną politykę łańcucha.
* --line-numbers - wyświetla (przy listowaniu przez -L) numery linii dla poszczególnych reguł.
* -x - podaje dokładne dane przy listowaniu liczby wysłanych/odebranych pakietów (domyślnie występują zaokrąglenia).

-F (--flush) [łańcuch] – Wyczyszczenie wpisów w podanym łańcuchu.

-Z (--zero) [łańcuch] – Wyzerowanie liczników liczących ilość przesłanych pakietów.

-N (--new-chain) [łańcuch]– Utworzenie nowego łańcucha użytkownika. To jest sposób by pewien blok reguł tyczących np. danego protokołu umieścić w łańcuchu zdefiniowanym przez użytkownika a następnie umieścić w łańcuchu PREROUTING, INPUT, OUTPUT, FORWARD lub POSTROUTING.

-X (--delete-chain) [łańcuch]– Usunięcie łańcucha zdefiniowanego przez użytkownika. Usunięcie jest możliwe jedynie wtedy gdy łańcuch ten nie ma żadnych reguł.

-P (--policy) [łańcuch] – Polityka domyślna łańcucha. Jeżeli pakiet nie pasuje do żadnego z podanych reguł to zostanie przepuszczony bądź odrzucony, zależnie od ustaleń polityki domyślnej.

**[łańcuch]**- nazwa stworzonego przez nas lub wbudowanego w tabelę łańcucha. Wbudowane łańcuchy odnoszą się automatycznie do pewnych pakietów, na przykład łańcuch INPUT w tabeli filter stosuje się automatycznie do wszystkich pakietów, których celem jest nasz host.

**[wzorzec]**- pozostałe opcje dla łańcucha, które można ponadto zanegować za pomocą [!], m.in. :

* -s – adres IP hosta lub sieci.
* -d – adres IP docelowy hosta lub sieci.
* -p – nazwa protokołu, do wyboru tcp, udp, icmp, all lub inne zdefiniowane w /etc/protocols.
* -i – interfejs wejściowy.
* -o – interfejs wyjściowy.
* --sport – nr portu źródłowego.
* --dport – nr portu docelowego.
* -m – załadowanie dodatkowego modułu.

**[akcja]**- akcją łańcucha może być łańcuch zdefiniowany przez użytkownika. Możliwe akcje to:

* **ACCEPT** (zaakceptuj pakiet) - przepuszcza pakiet bez zmian.
* **DROP** (odrzuć pakiet) - nie przepuszcza pakietu.
* **QUEUE** (kolejkuj) - kieruje pakiet do przestrzeni użytkownika (jeśli jest ona obsługiwana przez kernel).
* **RETURN** (powróć) - kończy modyfikację pakietu w tym łańcuchu i powraca do łańcucha, z którego aktualny został wywołany.

1. **Moduły**

Moduły rozszerzają podstawowe możliwości iptables. Aby załadować moduł, należy wykorzystać przełącznik –m wraz z nazwą wybranego modułu dla polecenia iptables:

iptables –m <nazwa modułu>

Aby skorzystać z pomocy dla wybranego modułu, należy dodać do polecenia przełącznik –h:

iptables –m <nazwa modułu> -h

W zależności od wersji i dystrybucji systemu zestaw modułów może być różny. Istnieją również repozytoria modułów, w których umieszcza się stworzone przez użytkowników moduły.

Przykładowe moduły:

* **conntrack** – śledzenie stanu połączenia, do którego należy dany pakiet.
* **state** – określenie stanu połączenia.
* **ttl** – odczytanie zawartości pola TTL w nagłówku.
* **mac** – wskazanie adresu MAC.
* **icmp** – podanie typu komunikatu protokołu ICMP.
* **time** – określenie przedziału czasowego, w którym obowiązuje dana reguła.

Niektóre moduły takie jak icmp lub tcp nie wymagają przełącznika –m, aby z nich skorzystać wywołuje się odpowiedni protokół z przełącznikiem –p. Nie możemy użyć nazwy protokołu, do którego moduł nie istnieje.

Nie ma ograniczenia co do ilości używanych modułów w jednej regule, można korzystać z wielu w tej samej regule.

1. **ICMP**

ICMP jest internetowym protokołem komunikatów kontrolnych (ang. *Internet Control Message Protocol*), który jest wykorzystywany w programach ping oraz traceroute. Moduł icmp jest używany przy diagnostyce i sprawdzaniu połączeń między hostami. Moduł ten posiada tylko jedną opcję: --icmp-type, określającą jakiego typu komunikaty mają zostać przefiltrowane.

Aby zablokować możliwość wykorzystania takich narzędzi jak traceroute przez inne hosty na naszym hoście, należy wpisać polecenie:

|  |
| --- |
| # iptables –A INPUT –p icmp –j DROP |

W ten sposób zablokujemy również możliwość „pingowania” naszego hosta, aby odblokować tę możliwość możemy posłużyć się opcją --icmp-type, wpisujemy:

|  |
| --- |
| # iptables –A INPUT –p icmp --icmp-type echo-request  -j ACCEPT |

Wszystkie pakiety wykorzystujące inne polecenia protokołu icmp zostaną odrzucone.

1. **MAC**

Adres MAC jest adresem fizycznym karty sieciowej nadawanym przez producenta karty podczas produkcji. Za pomocą tego modułu w iptables możemy filtrować pakiety nie tylko po samym adresie IP ale również po adresie MAC. Z punktu widzenia bezpieczeństwa korzystanie z modułu mac jest często niezbędne, jednak należy pamiętać, że narzuca on dodatkowe obciążenie. Aby skorzystać z możliwość filtrowania po adresie MAC, należy dodać do polecenia opcję --mac-source, która jest zarazem jedyną opcją modułu mac. Podawany adres musi posiadać format: xx:xx:xx:xx:xx:xx. Dodatkowo należy pamiętać, że moduł działa tylko dla łańcuchów PREROUTING, FORWARD i INPUT.

Aby zabezpieczyć się przed nieautoryzowanym dostępem do jakiejś usługi na naszym hoście, można podać regułę wiążącą konkretny adres IP z konkretnym adresem MAC, np.:

|  |
| --- |
| # iptables –A INPUT –p tcp –s 10.2.30.12 –m --mac- source 00-0A-E1-22-3E-11 –j ACCEPT |

Reguła dotyczy pakietów kierowanych do naszego hosta i oznacza, że jeżeli:

* jest to pakiet TCP,
* adresem źródłowym IP jest 10.2.30.12,
* adresem źródłowym MAC jest 00-0A-E1-22-3E-11,

to taki pakiet należy przepuścić.

1. **STATE**

Za pomocą modułu state można wykorzystać pracę systemu śledzenia połączeń (ang*. Stateful packet filtering*). Dzięki temu systemowi, zamiast sprawdzać wszystkie pakiety możemy sprawdzać tylko te, nawiązujące nowe połączenia, więc nie ma sensu ich oddzielnie filtrować. Również pakiety nie będące częścią żadnego znanego nam połączenia mogą zostać odrzucone bez ich analizowania. Nie wykorzystując tego modułu w regule przeprowadzamy tzw. Filtrację bez śledzenia stanu pakietów, a więc wykorzystanie modułu state poprawia wydajność firewalla.

W iptables wyróżnia się cztery stany połączeń:

* NEW – pakiety, które tworzą nowe połączenie,
* ESTABLISHED – pakiety, które należą do nawiązanego połączenia,
* RELATED – pakiety tworzące nowe połączenie, związane z już istniejącym połączeniem,
* INVALID – pakiety, które nie należą do żadnego połączenia.

Zwiększenie wydajności zapory ogniowej odbywa się przede wszystkim dzięki zastosowaniu logicznego ułożenia reguł. W iptables reguły czytane są po kolei i w takiej kolejności są dopasowywane do pakietów. Zatem, aby zmniejszyć opóźnienie ruchu sieciowego spowodowane filtracją oraz obciążenie serwera na samym początku należy umieszczać reguły, do których dopasowana jest największa liczba pakietów. Należy pamiętać, że optymalizacji reguł można dokonywać dopiero po stworzeniu zapory i jej przeanalizowaniu.

Polityk tworzenia zapór jest wiele, jedna z najpopularniejszych polega na blokowaniu wszystkiego oprócz niezbędnych usług i ewentualnym logowaniu odrzuconych połączeń. Wykorzystując do tego odpowiednią politykę kolejności przepuszczania pakietów można zoptymalizować przetwarzanie pakietów przez zaporę. Przykład budowania takiej zapory:

* + 1. Ustawienie domyślnej polityki na DROP.
    2. Przepuszczanie wszystkich pakietów w stanie ESTABLISHED oraz RELATED.
    3. Sprawdzenie pakietów w stanie NEW. Na podstawie tych warunków logicznych przepuścić pakiety bądź nie. Jeżeli zostały przepuszczone to kolejne transmisje będą zaakceptowane przez regułę wcześniejszą dotyczącą stanu ESTABLISHED. Jeżeli ustalone już połączenie wywoła kolejne połączenie zostanie również automatycznie przepuszczone przez regułę wcześniejszą jako pakiety w stanie RELATED.
    4. Odrzucanie pakietów w stanie INVALID.
    5. Opcjonalnie pozostałe pakiety logujemy w celach diagnostycznych.
    6. Ostatecznie pakiety niedopasowane do reguł zostaną odrzucone.

Przykładowa implementacja dla domyślnej tabeli filter i łańcucha INPUT:

|  |
| --- |
| # iptables –P INPUT DROP  # iptables –A INPUT –m state --state  ESTABLISHED,RELATED –j ACCEPT  # iptables –A INPUT –p tcp –m state --state NEW –m tcp --dport 80 –j ACCEPT  . . .  # iptables –A INPUT –m state INVALID –j DROP  # iptables –A INPUT –j LOG –log-prefix “DROP\_INPUT ” --log-tcp-options --log-ip-options --log-tcp-sequence |

Pierwsza linia ustawia nam politykę domyślną na DROP, czyli wszelkie przychodzące pakiety są odrzucane. Kolejna linia akceptuje pakiety w stanie ESTABLISHED i RELATED. Do tej linii zostanie dopasowanych najwięcej pakietów a więc występuje ona na początku. Kolejna reguła akceptuje zapytania przychodzące na port 80. Może tutaj wystąpić wiele innych reguł, jednakże należy pamiętać aby odrzucać pakiety w stanie INVALID. Na koniec warto wykorzystać cel LOG aby zalogować odrzucone pakiety.

1. **COMMENT**

Moduł comment służy do dodawania komentarzy do reguł. Maksymalna długość komentarza to 255 znaków. Posiada tylko jedną opcję --comment po której podaje się komentarz w podwójnym lub pojedynczym cudzysłowie.

Przykład:

|  |
| --- |
| # iptables –A INPUT –p icmp –m comment --comment „odrzucanie pingów” –j DROP |

Komentarz widoczny jest przy listing reguł, przy poleceniu iptables –L.

1. **MULTIPORT**

Moduł multiport umożliwia zastosowanie w regule wielu portów, ich ilość jest ograniczona maksymalnie do 15. Udostępnia on następujące opcje:

* --sport – porty lub zakres portów źródłowych,
* --dport – porty lub zakres portów docelowych,
* --ports – porty lub zakres portów źródłowych/docelowych – bez znaczenia.

Przykładowe użycie (zablokowanie dostępu do naszego serwera WWW na porcie 80 i 443):

|  |
| --- |
| # iptables – A INPUT –p tcp –m multiport --dport 80,433 –j DROP |

1. **LIMIT**

Moduł limit pozwala ograniczać pakiety dopasowane do reguł, w których występuje. Opcje dostępne w tym module to:

* --limit – średnia częstotliwość dopasowania reguły, wyrażona w jednostkach czasu: sekunda, minuta, godzina, dzień,
* --limit-burst – seria dopasowanych pakietów w jednostce czasu podanej w opcji --limit, po której powyższy mechanizm ograniczania pakietów zostanie uruchomiony (domyślna wartość do 5).

Poniższy przykład przedstawia regułę chroniącą serwer WWW przed atakiem zwanym „powódź pakietów TCP”:

|  |
| --- |
| # iptables -A INPUT –p tcp --dport 80 –m limit  --limit 1/s –m state --state NEW –j ACCEPT |

Reguła ta przepuszcza maksymalnie 5 pakietów na sekundę (ponieważ taka jest domyślna wartość --limit-burst), pozostałe pakiety z nawiązanej już sesji TCP mogą by wymieniane bez limitu. Jeżeli w ciągu jednej sekundy do tej reguły zostanie dopasowanych 6 pakietów TCP (zostanie nawiązanych 6 połączeń z serwerem na sekundę) wtedy uruchomi się mechanizm limitujący, który dopóki napływ pakietów nie zmniejszy się do ilości 5 na sekundę będzie przepuszczał tylko jeden pakiet na sekundę.

1. **CONNLIMIT**

Zadaniem modułu connlimit jest ograniczenie maksymalnej ilości połaczeń z tego samego adresu IP lub sieci. Dostępne są dwie opcje:

* --connlimit-above n – limit połączeń, po przekroczeniu którym zasada reguły zacznie obowiązywać,
* --connlimit-mask – maska sieci, która wyróżnia grupę adresów IP traktowanych jako jedno źródło.

Przykład: Blokada więcej niż 2 połączeń na port 23 (telnet).

|  |
| --- |
| # iptables -A INPUT -p tcp --dport 23 -m connlimit --connlimit-above 2 -j REJECT |

1. **TIME**

Moduł time określa w jakim czasie dana reguła ma obowiązywać. Najważniejsze opcje tego modułu to:

* --timestart – dopasowuje pakiet, który przyjdzie po zadanym czasie w ciągu dnia. Dopuszczalny format: hh:mm[:ss],
* --timestop – dopasowuje pakiet, który przyjdzie przed zadanym czasie w ciągu dnia. Format j.w.,
* --weekdays – dopasowuje pakiet w wybrane dni tygodnia. Dni w formacie trzyliterowym: Mon, Tue, Wed, Thu, Fri, Sat, Sun, lub jako cyfry od 1 do 7,
* --monthdays – dopasowuje pakiet w wybrane dni miesiąca. Dni w zakresie od 1 do 31 (dla danego miesiąca).

Przykład:

|  |
| --- |
| # iptables –A FORWARD –m time --monthdays 10 --timestart 9:00 --timestop 17:00 –j ACCEPT |

Przepuszczanie ruchu sieciowego każdego 10-tego dnia miesiąca w godzinach od 9:00 do 17:00.

1. **TTL**

Moduł ten jest odpowiedzialny za zmianę pola TTL (ang. *Time To Live*) nagłówka IP pakietu. Pole TTL pozwala na ustalenie ilości skoków jakie pakiet może wykonać w sieci. Po przejściu przez każdy router wartość jest zmniejszana o 1. W momencie gdy wartość pola równa będzie 0 pakiet nie zostanie przesłany dalej. Najważniejsze opcje:

* --ttl-set wartość – ustawia TTL na określoną wartość.
* --ttl-dec x – zmniejsza wartość TTL o x.
* --ttl-inc x – zwiększa wartość TTL o x.
* --ttl-eq x – dopasowuje pakiet, którego TTL jest podanej wartości.

Przykład: Odrzucenie pakietów wchodzących przez eth0 i posiadających wartość TTL 127:

|  |
| --- |
| # iptables –A FORWARD –I eth0 –m ttl --ttl-eq 127  –j DROP |

1. **CONNTRACK**

Moduł ten pozwala śledzenie stanu połączenia, do którego należy dany pakiet. Przyjmuje on następujące opcje:

* --ctstate stan[,...] - dopasowuje pakiety na podstawie przynależności do jednego z podanych stanów połączenia. Opis dostępnych stanów znajduje się poniżej.
* --ctproto protokół - dopasowuje pakiet na podstawie protokołu warstwy 4 (UDP. ICMP. itp.). Można podać numer protokołu, lub jego nazwę (zgodnie z /etc/protocols).
* --ctorigsrc adres - dopasowuje pakiet na podstawie oryginalnego adresu źródłowego.
* --ctorigdst adres - dopasowuje pakiet na podstawie oryginalnego adresu docelowego.
* --ctreplsrc adres - dopasowuje pakiet na podstawie adresu źródłowego odpowiedzi.
* --ctrepldst adres - dopasowuje pakiet na podstawie adresu docelowego odpowiedzi.
* --ctorigsrcport port - dopasowuje pakiet na podstawie oryginalnego portu źródłowego.
* --ctorigdstport port - dopasowuje pakiet na podstawie oryginalnego portu docelowego.
* --ctreplsrcport port - dopasowuje pakiet na podstawie portu źródłowego odpowiedzi.
* --ctrepldstport port - dopasowuje pakiet na podstawie portu docelowego odpowiedzi.
* --ctstatus status[,...] - dopasowuje pakiet na podstawie statusu połączenia. Poniżej znajdują się opisy możliwych statusów.
* --ctexpire czas[:czas] - dopasowuje pakiet na podstawie pozostałego czasu życia wpisu w tablicy conntrack. Można podać albo pojedynczą wartość w sekundach, albo zakres czasu.
* --ctdir {ORIGINAL|REPLY} - dopasowuje pakiet na podstawie kierunku ruchu pakietów. ORIGINAL oznacza kierunek, w którym połączenie zostało zainicjowane, a REPLY kierunek powrotny. Nie podanie tej opcji powoduje, że zostaną dopasowane pakiety idące w obu kierunkach.

Możliwe stany:

* INVALID - pakiet nie należy do żadnego znanego połączenia,
* NEW - pakiet rozpoczyna nowe połączenie,
* ESTABLISHED - pakiet należy do istniejącego połączenia,
* RELATED - pakiet rozpoczyna połączenie powiązane z istniejącym,
* SNAT - wirtualny stan oznaczający, że oryginalny adres źródłowy pakietu jest inny niż adres docelowy odpowiedzi (czyli jest SNATowany),
* DNAT - wirtualny stan oznaczający, że oryginalny adres docelowy pakietu jest inny niż adres źródłowy odpowiedzi (czyli jest DNATowany).

Możliwe statusy:

* NONE - żaden z poniższych.
* EXPECTED - to połączenie jest spodziewane, np. zostało przewidziane przez moduł pomocniczy conntrack,
* SEEN\_REPLY - conntrack zaobserwował pakiety idące w obu kierunkach tego połączenia,
* ASSURED - wpis w tablicy conntrack nie powinien być nigdy przedwcześnie skasowany,
* CONFIRMED - połączenie jest potwierdzone, rozpoczynający pakiet opuścił lokalną maszynę.

Jeżeli używany jest NAT, to we wszystkich tablicach prócz raw za pomocą tego modułu można dopasowywać pakiety na podstawie rzeczywistych adresów, z których pakiety pochodzą i na które zostaną wysłane.

Przykład:

|  |
| --- |
| # iptables -A FORWARD -m conntrack --ctorigsrc 192.168.100.10 |

Powyższa reguła dopasuje pakiety, których oryginalnym adresem źródłowym jest 192.168.100.10. Pakiety te będą należeć do połączeń nawiązywanych przez hosta 192.168.100.10.

1. **MARK**

Moduł ten pozwala na dopasowanie pakietu na podstawie znacznika przypisanego temu pakietowi. Posiada tylko jeden parametr --mark wartość[/maska], który specyfikuje dopasowywaną wartość znacznika oraz maskę. Znacznik pakietu jest najpierw poddawany operacji AND z maską, a potem porównywany z podaną wartością (wartość == znacznik & maska). Domyślną wartością maski jest 0xFFFFFFFF.

Przykład:

|  |
| --- |
| # iptables -A FORWARD -m mark --mark 1/1 -j ACCEPT |

Dopasowuje pakiety, które mają ostatni bit znacznika ustawiony na 1.

1. **CONNMARK**

Moduł ten dopasowuje pakiety na podstawie znacznika połączenia (ang. *connection mark*). Jest to inny rodzaj znacznika, niż mark. Znaczniki connmark ustawia się za pomocą celu CONNMARK. Dopasowanie to posiada jedną opcję:

--mark wartość[/maska], która dopasowuje pakiet na podstawie wartości znacznika połączenia. Jeżeli maska jest podana to najpierw robiona jest operacja bitowa AND z maską, a potem porównanie z podaną wartością (wartość == connmark & maska).

1. **IPRANGE**

Moduł ten pozwala na dopasowanie pakietu na podstawie zadanego zakresu adresów IP. Moduł ten posiada dwie opcje:

* --src-range od[-do] - dopasowuje pakiet na podstawie przynależności adresu źródłowego do zadanego zakresu.
* --dst-range od[-do] - dopasowuje pakiet na podstawie przynależności adresu docelowego do zadanego zakresu.

Należy podawać pełne zakresy adresów IP, zapis niekompletny jest uzupełniany zerami, np. 192 to 192.0.0.0. Zakres, dla którego pierwszy adres IP jest większy od drugiego nie dopasuje żadnego adresu.

Przykład: Dopasowanie pakietów z hostów z zakresu od 192.168.1.10 do 192.168.1.20 (włącznie).

|  |
| --- |
| # iptables -A FORWARD -m iprange --src-range 192.168.1.10-192.168.1.20 -j ACCEPT |

1. **L7-FILTER**

L7-filter służy do analizy, identyfikacji oraz klasyfikacji pakietów internetowych. W przeciwieństwie do innych klasyfikatorów, L7 nie bierze pod uwagę wyłącznie podstawowych wartości, takich np. jak numery portów czy adres IP nadawcy. **Dokonuje analizy wewnętrznej pakietu**, zdefiniowanego za pomocą wyrażeń regularnych. Zdefiniowane wzorce znajdują się w plikach \*.pat.

Przykładowy pakiet SSH opatrzony jest wyrażeniem:

^ssh-[12]\.[0-9]

Natomiast HTTP:

http/(0\.9|1\.0|1\.1) [1-5][0-9][0-9] [\x09-\x0d -~]\*(connection:| content-type:| contentlength:| date:)|post [\x09-\x0d -~] \* http:/[01]\.[019]

Głównym zastosowaniem tego narzędzia jest identyfikacja pakietów, które wykorzystują nieprzewidywalne numery portów (peer to peer). Potrafi ono wyłapać pakiety pochodzące z takich programów jak Jabber czy BitTorrent. Dodatkowo L7 znajduje zastosowanie w sytuacjach, gdy staramy się dopasować ruch na portach innych niż standardowe (np. http na porcie 1111) albo do rozróżniania protokołów, które dzielą port (np. jakieś protokoły peer to peer wykorzystujące port 80. Wtedy zamiast blokować cały ruch na tym porcie możemy zablokować samo peer to peer, przepuszczając inne pakiety).

Przy pomocy zidentyfikowanych i sklasyfikowanych pakietów możemy:

* śledzić, jakie pakiety znajdują się w sieci,
* kontrolować pasmo (Traffic Control),
* blokować wybrane pakiety.

Przykładowe protokoły: bittorrent, cvs, http, imap, jabber, smtp, ssh, subversion, telnet, worldofwarcraft, yahoo.

Istnienie możliwość dodawania własnych wzorców.

L7-filer został wydany w dwóch wersjach, kernel i userspace.

1. **Ćwiczenia**

Zadania do zrealizowania:

1. Ograniczenie liczby pakietów ICMP-echo do 3 na minutę.
2. Użycie modułu comment w celu opisania stworzonej poprzednio reguły.
3. Dopuszczenie ruchu sieciowego codziennie od 8:00 do 11:00.
4. Utworzenie statystyk pakietów, które łączą się z portem 80.
5. Akceptacja pakietów przychodzących ustanowionych i związanych z innymi połączeniami.
6. Zablokowanie możliwości pingowania hosta dla podanego adresu MAC.
7. Zmiana wartości pola TTL każdego przychodzącego pakietu na 56.
8. Zablokowanie więcej niż 4 połączeń na porcie 80.
9. Zablokowanie dostępu do portów 80, 20 i 21 (usługa http i ftp).

1. **Bibliografia**
2. [http://debian.linux.pl](http://debian.linux.pl/)
3. <http://pl.wikibooks.org/wiki/Sieci_w_Linuksie/Netfilter/iptables/dopasowania>
4. <http://mediawiki.ilab.pl/images/e/ef/Bsi_12_lab.pdf>
5. <http://www.marcinmazurek.com/teksty/conntrack/conntrack.pdf>