Firewall – podstawy teoretyczne

Wysłany dnia: 29-08-2007 18:31  Krzysztof Jozwiak *Komentarz*

Każda główna wersja jądra. systemu ma swojego firewalla. Dla jąder serii a 2.0.x to ipfwadm, seria 2.2 to ipchains a dla jąder 2.4 netfilter (najbardziej nowoczesny).

Do jąder serii 2.4 został włączony kod firewalla i translacji adresów (tzw. maskarady) o nazwie netfilter. Programem służącym do zarządzania nim jest iptables. Składnia tego programu jest bardzo podobna do ipchains (firewall w jądrach 2.2) ale rozszerzalna. Oznacza to iż jej funkcjonalność można rozszerzyć bez potrzeby ponownej kompilacji jądra.

Polecenie iptables możemy używać zarówno do konfiguracji firewalla, jak również translacji adresów (tzw. Maskarady oraz NAT) i zliczania ruchu.. Istnieją dlatego dwie tablice reguł: filter i net. Domyślną tablicą jest filter (czyli ta odpowiedzialna za filtrowanie pakietów) dopóki nie zmienimy tego zachowania przy pomocy opcji -t.

Zanim rozpoczniemy korzystanie z iptables należy załadować moduł odpowiedzialny za firewall. Najłatwiej tego dokonać korzystając z polecenia modprobe:

```
modprobe ip_tables
```

W netfilter udostępniono pięć wbudowanych łańcuchów. ?ańcuchy INPUT i FORWARD są dostępne dla tablicy filter, PREROUTING i POSTROUTING są dostępne dla tablicy nat, natomiast łańcuch OUTPUT jest dostępny dla obu tablic.

Składnia poleceń iptables

Ogólna składnia większości poleceń iptables jest następująca:

iptables polecenie określenie-reguły rozszerzenia

Opcje:

-A łańcuch

Dodanie jednej lub kilku reguł na koniec zadanego łańcucha. Jeżeli zostanie podana nazwa hosta źródłowego lub docelowego, z którą związany jest więcej niż jeden adres IP, reguła zostanie dodana do każdego adresu.

-I łańcuch numer_reguły

Wstawianie jednej lub więcej reguł na początek zadanego łańcucha. Jeżeli zostanie podana nazwa hosta źródłowego lub docelowego, z którą związany jest więcej niż jeden adres IP, reguła zostanie dodana do każdego adresu.

-D łańcuch

Usunięcie jednej lub kilku reguł z zadanego łańcucha, który takie reguły zawiera.

-D łańcuch numer_reguły

Usunięcie reguły znajdującej się na pozycji numer_reguły z zadanego łańcucha. Liczenie reguł zaczyna się od 1 w przypadku pierwszej reguły w łańcuchu.

-R łańcuch numer_reguły

Zastąpienie reguły na pozycji numer_reguły w zadanym łańcuchu regułą o podanej charakterystyce.

-C łańcuch

Sprawdzenie zadanym łańcuchem datagramu opisanego przez regułę. To polecenie zwróci komunikat opisujący, w jaki sposób łańcuch przetworzył datagram. Jest bardzo przydatne do testowania konfiguracji firewalla.

-L [łańcuch]

Wyświetlenie (wylistowanie) reguł z zadanego łańcucha lub ze wszystkich, jeżeli żadnego nie podano.

-F [łańcuch]

Usunięcie (wyczyszczenie) reguł z zadanego łańcucha lub ze wszystkich, jeżeli nie podano żadnego.

-N łańcuch

Utworzenie nowego łańcucha o podanej nazwie. Może istnieć tylko jeden łańcuch o takiej samej nazwie. W ten sposób tworzy się łańcuchy definiowane przez użytkownika.

-X [łańcuch]

Usunięcie zadanego łańcucha zdefiniowanego przez użytkownika lub wszystkich, jeżeli nie podano za żadnego. Aby to polecenie odniosło skutek, nie może być odwołań do usuniętego łańcucha w żadnym innym łańcuchu reguł.

-P łańcuch polityka

Ustawienie domyślnej polityki dla zadanego łańcucha. Dopuszczalne polityki to: ACCEPT, DROP, QUENE i RETURN. ACCEPT pozwala na przepuszczenie datagramu. DROP powoduje iż datagram jest odrzucany. QUENE powoduje, że datagram jest przekazywany do przestrzeni użytkownika w celu dalszego przetwarzania. RETURN powoduje, że kod firewalla IP wraca do łańcucha, który go wywołał i kontynuuje działanie od następnej reguły.

Parametry definicji reguły

Istnieje kilka parametrów iptables używanych do definiowania reguły. Gdy wymagane jest zdefiniowanie reguły, musi zostać podana każda z nich albo zostaną przyjęte wartości domyślne.

-p[!] protokuł

Określa nazwę protokołu, którego ma dotyczyć reguła. Dopuszczalne nazwy protokołów to: tcp, udp, icmp lub numer protokołu IP (nazwy i numery protokołów są podane w /etc/protocols). Znak ! neguje dalszą cześć reguły, czyli dotyczy datagramu który będzie pasował do każdego protokołu poza podanym.

-s[!] adres[/maska]

Określa adres źródłowy datagramu, który będzie pasował do tej reguły. Adres może być podany w postaci nazwy hosta, nazwy sieci lub adresu IP. Opcjonalny parametr maska definiuję maskę sieci, która ma być zastosowana. Może być ona podana tradycyjnie (np. /255.255.255.0) lub w postaci współczesnej (tj. /24)

-d[!] adres[/maska]

Określa adres docelowy datagramu, który będzie pasował do tej reguły. Adres może być podany w postaci nazwy hosta, nazwy sieci lub adresu IP. Opcjonalny parametr, maska definiuję maskę sieci, która ma być zastosowana. Może być ona podana tradycyjnie (np. /255.255.255.0) lub w postaci współczesnej (tj. /24)

-j cel

Określa jakie działanie ma być podjęte, gdy reguła zostanie dostosowana. Dopuszczalne cele to ACCEPT, DROP, QUENE i RETURN. Można także podać cel obsługiwany przez rozszerzenia. Jeżeli żaden cel nie zostanie podany, nie zostanie podjęte żadne działanie poza uaktualnieniem datagramu i licznika bajtów.

-i [!] nazwa_interfejsu

Określa nazwę interfejsu, który przyjął datagram. Znak ! odwraca wynik dopasowania. Jeżeli nazwa interfejsu kończy się znakiem +, pasował będzie każdy interfejs, którego nazwa rozpoczyna się zadanym ciągiem. Na przykład, -i ppp+ będzie pasować do dowolnego urządzenia sieciowego PPP, a -i ! eth+ będzie pasował do wszystkich urządzeń poza ethernetem.

-o [!] bazwa_interfejsu

Określa nazwę interfejsu, który na który skierowany jest datagram. Znak ! odwraca wynik dopasowania. Jeżeli nazwa interfejsu kończy się znakiem +, pasował będzie każdy interfejs, którego nazwa rozpoczyna się zadanym ciągiem. Na przykład, -i ppp+ będzie pasować do dowolnego urządzenia sieciowego PPP, a -i ! eth+ będzie pasował do wszystkich urządzeń poza ethernetem.

[!] -f

?ądanie aby reguła dotyczyła tylko drugiego i następnych fragmentów datagramu. Nie dotyczy pierwszego datagramu.

opcje

-v Nakazuje iptables wyświetlać bogate wyniki.

-n Nakazuje iptables aby wyświetlał adresy IP i porty jako liczby, nie próbując zamieniać ich na odpowiadające im nazwy. Opcja bardzo przydatna w przypadku braku DNSa lub jego niepoprawnej konfiguracji.

-x Nakazuje aby wszystkie liczby wyświetlane przez iptables były dokładne, bez zaokrąglania.

-n -numery_wierszy Nakazuje przy wyświetleniu zestawów reguł pokazywanie numerów wierszy. Numer wiersza odpowiada pozycji reguły w łańcuchu.

rozszerzenia

Iptables jest narzędziem rozszerzanym przez opcjonalne moduły bibliotek dzielonych. Istnieją standardowe rozszerzenia udostępniane przez funkcje iptables. Aby z nich skorzystać, należy podać poleceniu iptables ich nazwę poprzez argument -m nazwa.

Rozszerzenie TCP: używanie z -m tcp -p tcp

–sport [!][port[:port]]

–dport[!] [port[:port]]

–tcp-flags [!] maska lista

[!] –syn

Powoduje, iż reguła pasuje tylko do datagramów z ustawionym bitem SYN i wyzerowanymi bitami ACK i FIN. Datagramy te są używane do otwierania połączeń TCP i dlatego ta opcja jest używana do obsługi żądań połączeń. Opcja ta to skrót od:

–tcp-flags SYN, RST, ACK SYN

Rozszerzenie UDP: używanie -m udp -p udp

–sport[!] [port[:port]]

Określa port, z którego musi pochodzić datagram, aby pasował do reguły. Porty mogą być podane jako zakres przez określenie górnego i dolnego limitu zakresu, które należy rozdzielić dwukropkiem. Na przykład 20:25 oznacza wszystkie porty od 20 do 25 włącznie. Znak ! może być użyty do zanegowania wartości.

–dport[!] [port[:port]]

Określa port, do którego musi być skierowany datagram, aby pasował do reguły. Porty mogą być podane jako zakres przez określenie górnego i dolnego limitu zakresu, które należy rozdzielić dwukropkiem. Na przykład 20:25 oznacza wszystkie porty od 20 do 25 włącznie. Znak ! może być użyty do zanegowania wartości.

Rozrzerzenie ICMP: używanie -m icmp -p icmp

–icmp-type [!] nazwa_typu

Określa typ komunikatu ICMP pasującego do reguły. Typ może być określony przez numer lub nazwę. Niektóre dopuszczalne nazwy to: echo-request, echo-replay, source-quench, time-exceeded, destination-unreachable, network-unreachable, host-unreachable, protocol-unreachable i port-unreachable.

Rozszerzenie MAC: używanie -m mac

–mac-source [!] adres

Określa adres hosta Ethernet, który wysłał datagram pasujący do tej reguły. Ma to jedynie sens w łańcuchach wejściowym i przekazującym reguły, ponieważ wszystkie datagramy, które przechodzą przez łańcuch wychodzący, są wysyłane przez nas.

Typy datagramów ICMP

Typ	Mnemonika iptables	Opis typu
0	echo-replay	Powtórzenie odpowiedzi
3	destination-unreachable	Cel nieosiągalny
4	source-quench	?ródło nieaktywne
5	redirect	Przekierowanie
8	echo-request	?ądanie powtórzenia
11	time-exceesed	Czas upłynął
12	parameter-problem	Problem z parametrem
13	timestamp-request	?ądanie znacznika czasu
14	timestamp-replay	Wysyłanie znacznika czasu w odpowiedzi
15	none	żądanie informacji
16	none	Wysyłanie informacji w odpowiedzi
17	address-mask-request	?ądanie maski adresu
18	address-mask-reply	Wysłanie maski adresu w odpowiedzi

Spis wszystkich pakietów typu ICMP poznasz wydając polecenie **iptables -p icmp -h**