Debian - uniwersalna instalacja/Konfigurowanie iptables

iptables to program sterujący filtrem pakietów (głównie używanym jako zapora sieciowa bądź NAT) opracowany dla systemu operacyjnego Linux.
Program może być używany jako filtr pakietów, bądź tzw. stanowa zapora dla systemów Linux z jądrem począwszy od serii 2.4.x, kontrolujący połączenia wchodzące i wychodzące do sieci komputerowej lub stacji roboczej.
Wymaga jądra skompilowanego z modułem ip_tables.
Iptables wymaga uprawnień roota do uruchomienia.
W większości dystrybucji Linuksowych iptables jest instalowane w katalogu /usr/sbin/iptables, jednakże w niektórych z nich można go znaleźć w /sbin/iptables.

Po zainstalowaniu Debiana firewall - którym jest iptables jest nie skonfigurowany i cały ruch przychodzący i wychodzący jest otwarty. Możemy to sprawdzić, w terminalu wpisujemy:

iptables -L

Powinniśmy zobaczyć

Chain INPUT (policy ACCEPT)

target prot opt source destination

Chain FORWARD (policy ACCEPT)

target prot opt source destination

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

Zagadnienia

1. Opis funkcji
2. System V czy SystemD - określenie programu inicjalizującego
3. Tworzenie skryptu firewalla dla System V
4. Usuwanie skryptu
5. Błędy skryptu
6. Skrypt zaawansowany

7. Tworzenie skryptu firewalla dla Systemd
8. Ufw - frontend dla iptables

Opis funkcji

INPUT – to pakiety odbierane, wchodzące do naszego komputera

OUTPUT– to pakiety wygenerowane, wychodzące z naszego komputera

FORWARD – to pakiety przekazywane, przechodzące przez nasz komputer

ACCEPT - akceptuje pakiet, wpuszcza pakiet do komputera

DROP - odrzuca pakiet, nie wpuszcza pakietu do komputera.

REJECT - odrzuca pakiet i odsyła z powrotem do źródła, powiadamiając o tym nadawcę

System V czy SystemD - określenie programu inicjalizującego

Sysvinit (System V) - jest to pierwszy program uruchamiany w systemach Linux przez jądro w trakcie procesu uruchamiania systemu operacyjnego. Następnie na podstawie plików konfiguracyjnych lub skryptów startowych init uruchamia pozostałe procesy systemowe.

Sysvinit był domyślnym w Debianie, łącznie z wersją Wheezy (7.0).
Debian Jessie (8.0) posiada Systemd - program inicjalizujący, zarządzający systemem i usługami (units - programy działające w tle, uruchomione jednorazowo lub cyklicznie. Począwszy od wersji 15.04 Ubuntu podczas startu korzysta z demona systemd.

Aby sprawdzić czy Debian używa Systemd, w terminalu wpisujemy:

systemd --version

Wynik

systemd 215

+PAM +AUDIT +SELINUX +IMA +SYSVINIT +LIBCRYPTSETUP +GCRYPT +ACL +XZ -SECCOMP -APPARMOR

Oznacza to, że jest zainstalowany Systemd w wersji 215.

W takim wypadku tworzysz skrypt dla Systemd (patrz poniżej - Tworzenie skryptu firewalla dla Systemd)

możesz użyć polecenia dpkg -S /sbin/init

otrzymasz wynik systemd-sysv: /sbin/init

Oznacza to, że Debian startuje używając Systemd,

jeśli otrzymasz wynik sysvinit: /sbin/init

Oznacza, że Debian startuje używając System V

Tworzenie skryptu firewalla dla System V

Skrypt firewalla, będzie się uruchamiał wraz ze startem komputera.

Uruchamiamy edytor tekstu, wpisując w terminalu nano

Tam wklejamy przykładowy skrypt firewalla

Przykładowa konfiguracja iptables blokująca połączenia przychodzące

Następnie zapisz plik nadając mu nazwę firewall

Wpisz ponownie ls by zobaczyć czy tam jest nasz plik firewall

Jeśli jest plik firewall to skopiuj plik firewall do katalogu init.d. W katalogu tym znajdują się skrypty startowe uruchamiane podczas ładowania systemu. W terminalu wpisz cp firewall /etc/init.d/

Następnie jeśli nie ma błędów nadaj plikowi firewall prawa uruchamiania chmod +x /etc/init.d/firewall

Tworzymy dowiązanie do uruchomienia serwisu w trybach pracy 2345 oraz zatrzymania serwisu w trybach pracy 016 – wpisując update-rc.d firewall defaults 90

update-rc.d - instaluje lub usuwa dowiązania do skryptów startowych w stylu System-V

Uruchamiamy ponownie komputer. Wraz ze startem nasz zestaw reguł filtrujących powinien wystartować.

Po ponownym uruchomieniu aby to sprawdzić wpisz iptables –L zobaczysz reguły

Możemy użyć również komendy do zatrzymania firewalla /etc/init.d/firewall stop

lub do jego uruchomienia /etc/init.d/firewall start

Błędy skryptu

Jeśli stworzymy skrypt firewall dla sysvinit, używając go w systemd otrzymamy przy starcie systemu komunikat - systemd-sysv-generator [179]: Ignoring creation of an alias firewall.service for itse.
Oznacza to, że skrypt nie został stworzony dla systemd i firewall.service został zignorowany.
Mimo to skrypt ten został uruchomiony i działa.

Aby to sprawdzić wpisz w terminalu komendę systemctl status firewall

Otrzymasz wynik w terminalu

Active: active (exited) - oznacza że skrypt działa, ale nie wie gdzie jest jego daemon by go monitorować.
Jeśli istnieje musimy go zdefiniować w pliku unita, konfigurując opcje Type i ExecStart, zgodnie z dokumentacją systemd.

Usuwanie skryptu

Aby usunąć skrypt musimy wejść do katalogu init.d wpisując w terminalu cd /etc/init.d/

Następnie musimy usunąć plik firewall wpisując rm firewall

Następnie musimy usunąć dowiązanie do skryptu update-rc.d firewall remove

Tworzenie skryptu firewalla dla Systemd

Utwórz skrypt firewalla dla systemd wykorzystując tym razem sam systemd.

Utwórz skrypt firewalla, który będzie się uruchamiał wraz ze startem komputera.

Uruchom edytor tekstu nano, wpisując w terminalu

Tam wklejamy przykładowy skrypt firewalla

Następnie zapisz plik nadając mu nazwę firewall w katalogu

Wpisz ponownie ls by zobaczyć czy tam jest nasz plik firewall

Jeśli widzisz plik firewall to skopiuj plik firewall do katalogu /etc/systemd/system/'.

W terminalu wpisujemy cp firewall /etc/systemd/system/

Następnie jeśli nie ma błędów nadajemy plikowi firewall prawa uruchamiania

chmod 755 /etc/systemd/system/firewall

Następnie utwórz usługę firewall.service w terminalu wpisujemy

nano /etc/systemd/system/firewall.service

W edytorze nano wyświetli się pusty dokument tam wklejamy skrypt usługi dla systemud.

Następnie zapisz plik. Uruchom usługę firewall.service wpisując systemctl enable firewall.service

Następnie uruchom firewalla wpisując systemctl start firewall.service

Następnie sprawdź czy działają reguły w iptables wpisując iptables -L

Powinny wyświetlić się nam reguły. Ponadto sprawdź status firewalla wpisując

systemctl status firewall.service

Otrzymasz mniej więcej komunikat

firewall.service - firewall

Loaded: loaded (/etc/systemd/system/firewall.service; enabled; vendor preset:

'"Active: active (exited)"' since Thu 2017-03-16 16:24:03 CET; 1min 44s ago

'"mar 16 16:24:03 debian systemd[1]: Started firewall."'

Komunikaty Active: active (exited) i mar 16 16:24:03 debian systemd[1]: Started firewall. oznaczają że usługa firewall.service działa prawidłowo.

Ufw - frontend dla iptables

UFW jest graficzną nakładką dla IPtables, jego zaletą jest to że jest bardzo prosty w obsłudze i jest mniej plików do konfiguracji. Aby go zainstalować, wpisujemy komendę: apt-get install ufw

po instalacji możemy ustawić jego autostart w pliku konfiguracyjnym: nano /etc/ufw/ufw.conf

zmieniamy wartość z: ENABLED=no

na ENABLED=yes

możemy także dodać obsługę protokołu IPv6: IPV6=yes