

Zapory ogniowe dla zwykłego użytkownika

Nie tylko dla ekspertów

Zapory stają się coraz bardziej wyrefinowane. Na szczęście, narzędzia do ich konfiguracji są coraz prostsze w obsłudze i bardziej przystępne dla przeciętnego użytkownika.

JOE CASAD I ACHIM LEITNER

Twój komputer pozwala Ci widzieć świat, ale nie chcesz, żeby świat widział Ciebie. Włamywacze działają w sposób coraz bardziej wyszukany, i nie wystarczy już nadzieja, że nie zauważą Twojej niepozornej stacji roboczej. Jeśli masz połączenie z Internetem, dobrze mieć również jakąś zaporę.

Zapory przyjmują różne kształty, rozmiary i ceny. Co ciekawe, to, co kiedyś zwano firewallem, teraz jest tylko jednym z wielu rodzajów urządzeń zapewniających bezpieczeństwo. Tradycyjna zapora ogniowa jest rodzajem rutera działającego w warstwie 3 modelu referencyjnego OSI. Warstwę 3 stanowi stos protokołu Internet Protocol, odczytujący ad-

resy IP i decydujący, gdzie kierować paczki IP. Zapora dodatkowo kontroluje nagłówki warstwy 4 (TCP i UDP), identyfikując usługi i oceniając flagi.

Jednak nowoczesne zapory mogą działać na innych poziomach stosu protokołów (Rysunek 1). To wielopoziomowe podejście może rozciągać się w dół do warstwy 2, gdzie funkcjonuje tzw. *bridgewall*. O ile zwykły most (lub switch) bierze pod uwagę jedynie adresy MAC, o tyle *bridgewall* sprawdza pakiety warstw od 2 aż do 4. *Bridgewall* to pełnowartościowy filtr pakietów o elastyczności switcha.

Furtka poziomu aplikacji stanowi dodatkową warstwę ochrony na wyższym poziomie. Furtka podczepia się pod połączenie TCP, działając jako pośrednik pomiędzy klientem a serwerem. Pozwala to zaporze na wgląd do protokołu aplikacji i wykrywanie nielegalnych pakietów, łamiących reguły protokołów określonych w RFC.

Oczywiście, o wiele bardziej egzotyczne rodzaje zapór to drogi sprzęt przeznaczony do dużych sieci i złożonych konfiguracji. Interesuje nas bardziej to, co można osiągnąć pod samym Linuxem i łatwo dostępnymi narzędziami. Jak się przekonasz w trakcie lektury tego numeru, Linux ma niezły zestaw oprogramowania do stawiania zapór ogniowych, w tym potężne narzędzia ułatwiające proces konfiguracji firewala, nie trzeba więc być ekspertem, by sobie z tym poradzić.



Na początku, w artykule „Łatwiejsza zapora”, pokażemy, jak używać programu KDE Guarddog do konfiguracji IPtables i IPchains. Kolejny artykuł, „Most zwodzony”, omawia narzędzia konfigurujące zaporę mostową warstwy 2. Zobaczysz, jak działają *bridgewalle*, i kiedy warto je stosować.

Jednym z problemów w zarządzaniu zaporami jest obfitość danych zapisywanych w logach firewala. W naszym trzecim artykule opisano dostępne narzędzia służące do analizy tych dzienników. W końcowym artykule, „Przygotowanie tabeli”, czytelnicy zapoznają się z narzędziem Shorewall (skrót od Shoreline Firewall) – kolejnym niebędącym zaporą samą w sobie, lecz ułatwiającym konfigurację teje.

Żaden temat nie jest tak ważny jak bezpieczeństwo, a żadne narzędzie nie jest bardziej krytyczne dla bezpieczeństwa sieci niż firewall. Nasze artykuły w tym miesiącu mają pokazać, że zapory nie są tylko dla profesjonalistów – ale dla każdego, kto ma połączenie z Internetem.

Temat miesiąca

Łatwiejsza zapora19

Guarddog pomaga niedoświadczonemu użytkownikowi zabezpieczyć komputer przed atakiem.

Most zwodzony22

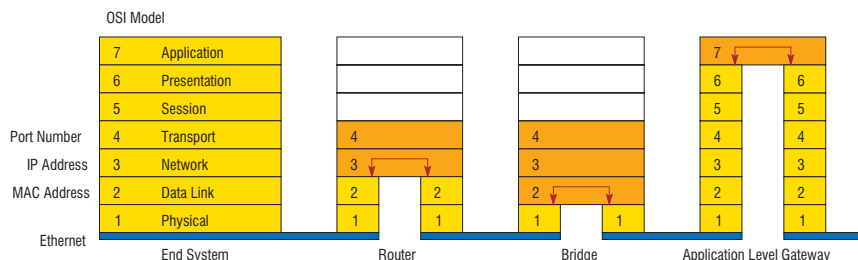
Filtry pakietów na poziomie mostu mają wiele zalet i można je dodać do sieci nie zmieniając konfiguracji składników sieci.

Szukanie śladów26

Narzędzia do automatycznej analizy logów pomagają administratorom wyłuskiwać istotne informacje.

Przygotowanie tabeli29

Kiedy użytkownicy konfigurują domowe stacje robocze, często zapominają o bezpieczeństwie.



Rysunek 1: Nowoczesne firewalle działają jako mosty (po lewej), routery (po środku) albo furtki poziomu aplikacji (po prawej).