Rodzaje zapór ogniowych

Na rynku dostępnych jest wiele produktów sprzedawanych pod nazwą „Firewall”, lecz różnią się one poziomem oferowanych zabezpieczeń. Filtry pakietowe (Network Level) na podstawie adresu źródłowego i docelowego oraz portu pojedynczego pakietu decydują, czy dana przesyłka może zostać przesłana dalej, czy też nie. Zwyczajny router nie jest zwykle w stanie takiej decyzji podjąć, lecz bardziej nowoczesne konstrukcje mogą przechowywać wewnętrzne informacje o stanie połączeń przechodzących przez niego, zawartości niektórych strumieni danych itp. Filtry pakietowe są zwykle bardzo szybkie, jednak ich wadą jest, że podane kryteria selekcji mogą okazać się niewystarczające dla niektórych usług internetowych, przez co do sieci byłyby przepuszczane niepożądane pakiety, a wtedy… Jedną z możliwych prób ataku może być umieszczenie pakietów wyższego poziomu w fałszywych ramkach MAC lub protokołu warstwy 3 (sieciowa) i 4 (transportowa) modelu ISO/OSI. Często wystarczy tylko zmienić adres nadawcy pakietu. W takim przypadku filtr pakietowy jest bezradny.

Bramki typu Circuit Level są w stanie przyporządkowywać pakiety do istniejących połączeń TCP i dzięki temu kontrolować całą transmisję. Zaawansowane systemy potrafią także kojarzyć pakiety protokołu UDP, który w rzeczywistości kontroli połączeń nie posiada.

Firewalle Application Level to, generalnie rzecz ujmując, hosty, na których uruchomiono proxy servers, które nie zezwalają na bezpośredni ruch pakietów pomiędzy sieciami oraz rejestrują i śledzą cały ruch przechodzący przez niego. Proxies potrafią więc niejako odseparować wiarygodną część sieci od podejrzanej; mogą magazynować najczęściej żądane informacje – klient kieruje swoje żądanie do proxy, który wyszukuje obiekt w swoich lokalnych zasobach i zwraca zamawiającemu. Dla każdej aplikacji (czyli usługi sieciowej, np. http, ftp, telnet, smtp, snmp, …) istnieje osobny proxy,

dla którego definiowane są reguły według których podejmowana jest decyzja o zaakceptowaniu bądź odrzuceniu połączenia. Niewątpliwym minusem tego rozwiązania jest konieczność stosowania wielu proxies do obsługi różnych aplikacji; jeżeli dla danego protokołu nie jest dostępny odpowiedni proxy, to dane przesyłane w tym formacie nie będą w ogóle przepuszczane przez bramkę. Na rynku dostępne są też systemy z proxies definiowanymi przez użytkownika funkcjonującymi jednakże nie na płaszczyźnie aplikacji, lecz analogicznie do filtrów pakietowych i bramek Circuit Level.

Zapory ogniowe (ang. **firewalls**) są kluczowymi elementami zabezpieczeń sieci komputerowych, chroniącymi przed nieautoryzowanym dostępem oraz atakami. Służą do monitorowania i kontrolowania ruchu sieciowego, decydując, które połączenia są dozwolone, a które mają zostać zablokowane. W zależności od metody pracy, zapory ogniowe dzielą się na kilka rodzajów, z których każdy ma swoje specyficzne zastosowanie i cechy.

Zapora ogniowa oparta na filtracji pakietów to jeden z najstarszych i najprostszych typów zapór. Działa na podstawie analizy nagłówków pakietów danych, takich jak adresy IP, porty oraz protokoły. Tego typu zapora porównuje przychodzące i wychodzące pakiety z zestawem reguł i decyduje, czy dany pakiet jest dozwolony, czy też powinien zostać zablokowany. Jest to rozwiązanie szybkie i łatwe w implementacji, jednak nie zapewnia pełnej ochrony przed bardziej zaawansowanymi atakami, które mogą obejmować np. ataki na poziomie aplikacji.

Zapora ogniowa oparta na stanie połączenia (ang. **stateful inspection firewall**) to bardziej zaawansowana forma zapory, która nie tylko filtruje pakiety na podstawie ich nagłówków, ale także monitoruje stan aktywnych połączeń. Dzięki temu zapora może kontrolować, czy dany pakiet należy do już istniejącego połączenia, czy jest próbą nawiązania nowego, potencjalnie nieautoryzowanego połączenia. Zapory te są bardziej bezpieczne, ponieważ mogą śledzić cały kontekst komunikacji i blokować pakiety, które nie pasują do

dozwolonych połączeń.

Zapora ogniowa oparta na analizie głębokiej zawartości (ang. **deep packet inspection firewall**) idzie o krok dalej, analizując całą zawartość pakietów, a nie tylko ich nagłówki. Dzięki tej metodzie zapora może wykrywać złośliwe oprogramowanie, wirusy, czy inne zagrożenia, które mogą być ukryte w danych aplikacji, nawet jeśli wyglądają one na legalne. Tego typu zapory są bardziej zasobożerne, ale zapewniają wyższy poziom bezpieczeństwa, ponieważ mogą identyfikować ataki na poziomie aplikacji, takie jak SQL injection czy ataki DDoS.

Zapory ogniowe proxy pełnią rolę pośrednika pomiędzy wewnętrzną siecią a siecią zewnętrzną, czyli między użytkownikiem a usługą, z której ten korzysta. Zamiast łączyć się bezpośrednio z docelowym serwerem, zapora proxy wysyła żądanie w imieniu użytkownika. Może filtrować ruch, ukrywać prawdziwy adres IP użytkownika oraz pełnić funkcję buforowania danych, co poprawia wydajność. Dzięki pełnej kontroli nad połączeniem zapora proxy może również chronić przed atakami, które próbują wykorzystać luki w aplikacjach.

Zapory ogniowe nowej generacji (NGFW) to najnowsze rozwiązania, które łączą funkcje tradycyjnych zapór z dodatkowymi mechanizmami ochrony, takimi jak systemy wykrywania i zapobiegania włamaniom (IDS/IPS), analiza zachowań, kontrola aplikacji oraz integracja z usługami chmurowymi. NGFW oferują bardzo wysoką skuteczność w ochronie przed nowoczesnymi zagrożeniami, takimi jak ataki typu APT (Advanced Persistent Threat) czy złośliwe oprogramowanie w chmurze. Dzięki zaawansowanej analizie danych zapory nowej generacji mogą również blokować ataki na poziomie aplikacji i użytkownika.

Różne typy zapór ogniowych są stosowane w zależności od wymagań danej sieci i poziomu bezpieczeństwa, jaki ma zostać osiągnięty. Starsze rozwiązania, takie jak zapory oparte na

filtracji pakietów, mogą być wystarczające w prostszych środowiskach, natomiast zapory nowej generacji stanowią kompleksową ochronę przed współczesnymi, wysoce zaawansowanymi zagrożeniami.

W serwisie dyplom.com.pl prezentujemy obronione prace dyplomowe, które mogą służyć za wzór do napisania własnej pracy - gdyby potrzebowali jeszcze Państwo konsultacji to polecamy stronę pisanie prac - fachowa pomoc w pisaniu prac.