

Dlaczego firewall nie wystarczy?

Zapora ogniowa

Firewall (urządzenie lub oprogramowanie) służy od ochrony przed nieuprawnionym dostępem do sieci dzięki filtrowaniu przychodzących i wychodzących z sieci połączeń. Firewall wykrywając nieprawidłowe połączenia blokuje je.

Paczka z danymi

Każdy przesyłany w sieci pakiet składa się z 2 części: nagłówka oraz obszaru danych, czyli właściwej zawartości pakietu. Nagłówek pakietu zawiera informacje wymagane do przesłania pakietu od nadawcy do odbiorcy. Obszar danych z kolei informuje o treści, które mają zostać przesłane za pomocą pakietu. Obrazowo można porównać to do wysyłania paczki. Na opakowaniu (nagłówku) znajdują się podstawowe informacje o adresacie, nadawcy i sposobie wysyłki, zaś wewnątrz znajduje się zawartość (obszar danych).

Analiza nagłówka

Pakiet przechodzący przez firewall analizowany jest pod kątem informacji zawartych w nagłówku. Firewall jest w stanie sprawdzić podstawowe informacje o pakiecie, czyli skąd i dokąd jest on przesyłany czy też jaki port w komunikacji jest wykorzystywany. Po przefiltrowaniu nagłówka pakietu firewall określa czy dany ruch powinien zostać zablokowany lub jeśli ruch jest zgodny z wyznaczonymi regułami, połączenie zostaje przepuszczone przez zaporę.



Firewall sprawdza jedynie nagłówek pakietu, nie analizuje jego zawartość. Może to spowodować przeniknięcie szkodliwej zawartości przez zaporę.

Analiza pakietu przez IPS

Uzupełnieniem zabezpieczenia sieci jest system wykrywania i blokowania włamań (Intrusion Prevention System). IPS podobnie jak firewall sprawdza przesyłany w sieci pakiet pod kątem zawartości jego nagłówka, ale dodatkowo posiada mechanizm, dzięki któremu wnika w głąb pakietu, analizując jego treść. Pozwala to na sprawdzenie wnętrza przesyłanego w sieci pakietu.



IPS sprawdza cały pakiet czyli nagłówek wraz z jego treścią. Jeśli pakiet jest niepoprawnie zbudowany lub jeśli w jego treści znajduje się niebezpieczna zawartość, system zablokuje połączenie.

Firewall nie wystarczy

Intrusion Prevention System dokonuje pełnej analizy ruchu (od warstwy 3 do 7 modelu ISO/OSI). Dzięki temu jest w stanie wykryć czy dany prawidłowy pakiet powinien zostać przepuszczony, czy też należy go zablokować, gdyż stanowi zagrożenie dla sieci. W sytuacji, gdy firewall zezwala na niebezpieczne połączenia, IPS okazuje się jedyną zaporą chroniącą sieć przed atakami.