Filtry pakietów

Pierwszymi ścianami ogniowymi w internecie były filtry pakietów. Filtr porównuje pakiety protokołów sieciowych (takich jak IP) i transportowych (takich jak TCP) z regułami zawartymi w bazie danych, po to by dalej przekazać tylko te pakiety, które odpowiadają kryteriom określonym w regułach. Filtry można zaimplementować w routerze albo w serwerze obsługującym stos protokołów TCP/IP.

Filtry zaimplementowane wewnątrz routerów nie pozwalają podejrzanemu ruchowi na dostęp do chronionej sieci, podczas gdy moduły filtrów TCP.IP na serwerach zapobiegają głównie temu, aby dany komputer odpowiadał na podejrzany ruch, jednak pakiety nadal docierają do sieci i mogą być skierowane do dowolnego umieszczonego w niej komputera. Filtry na routerach chronią wszystkie komputery w sieci docelowej przed podejrzanym ruchem, dlatego też filtrowanie w stosie TCP.IP serwera (tak jak jest to realizowane w systemie Windows NT) powinno być stosowane jedynie jako dodatkowe zabezpieczenie w stosunku do filtrowania w routerach a nie zamiast niego.

Zasady działania typowego filtra:

– filtr pomija próby nawiązania połączenia przychodzącego z zewnątrz sieci, przepuszcza próby nawiązania połączenia przychodzącego z wewnątrz.

– Eliminacja pakietów TCP przeznaczonych do portów, które nie powinny być dostępne dla internetu (na przykład port sesji NetBios), filtr powinien przepuszczać pakiety, które powinny przechodzić przez filtr (na przykład SMTP). W większości filtrów można dokładnie określić serwer do którego dopuszczany jest określony ruch – na przykład ruch SMTP do portu 25 może być dopuszczany tylko dla adresu IP serwera pocztowego.

– Filtr powinien ograniczać dostęp w ruchu przychodzącym z zewnątrz do pewnych zakresów IP.

Mało skomplikowane filtry pakietów lub routery z funkcją filtrowania pakietów, które wymagają otwarcia portów powyżej 1023 dla kanałów zwrotnych nie są urządzeniami bezpiecznymi. Nie zapobiegają mianowicie ustanawianiu przez użytkowników wewnętrznych lub koni trojańskich usługi na stacji klientom na portach powyżej 1023 i nasłuchiwaniu prób uzyskania połączenia z zewnątrz. Bardziej złożone ściany (filtry z badaniem stanu i proxy zabezpieczające) otwierają te kanały jedynie dla serwerów do których połączenie zwrotne powstaje w wyniku żądania pochodzącego z wewnątrz strefy chronionej – i to te właśnie ściany powinny być stosowane zamiast prostych filtrów pakietów, które nie potrafią określić stanu połączenia. Złożone filtry korzystają z firmowych algorytmów do badania stanów wszystkich połączeń które przez nie przechodzą, szukając znaków sygnalizujących włamanie takich jak wybór trasy przez nadawcę (source routing), zmianę trasy na podstawie komunikatu ICMP, podszywanie się pod adres IP. Połączenia, które wskazują te cechy są odrzucane.

Klientom wewnętrznym zezwala się na tworzenie połączeń do hostów zewnętrznych zaś hostom zewnętrznym w zasadzie zabrania się prób inicjowania połączenia. Kiedy host wewnętrzny decyduje się zainicjować połączenie TCP, wysyła komunikat TCP pod adres IP i numer portu serwera publicznego (np. microsoft.com:80 w przypadku kiedy chce się połączyć z witryną Microsoft). W tym inicjującym komunikacie przekazuje hostowi zewnętrznemu swój adres IP oraz numer portu, na którym będzie nasłuchiwał odpowiedzi (np. localhost:2050). Zewnętrzny serwer przesyła dane z powrotem do portu podanego przez wewnętrznego klienta. Ponieważ ściana ogniowa przegląda cały ruch wymieniany między dwoma hostami wie, że połączenie było zainicjowane przez wewnętrzny host przyłączony do jego wewnętrznego interfejsu, wie także jaki jest jego adres IP oraz na jakim porcie spodziewa się on otrzymać ruch zwrotny. Ściana pamięta aby zezwolić hostowi o adresie podanym w komunikacje połączenia na ruch powrotny pod ten adres, ale tylko do określonego portu.

Kiedy hosty objęte połączeniem zamkną połączenie TCP, ściana ogniowa usuwa pozycję, która zezwala zdalnemu hostowi na ruch zwrotny do hosta wewnętrznego ze swojej tablicy stanów (w pamięci połączeń).

Filtrowanie nie rozwiązuje całkowicie problemu bezpieczeństwa w Internecie. Po pierwsze, adresy IP komputerów chronionych filtrem są obecne w ruchu wyjściowym, co czyni łatwe określenie typu i liczby hostów sieci wewnętrznej przyłączonej do internetu i skierowanie ataku na te adresy. Filtrowanie nie ukrywa tożsamości hostów wewnątrz obszaru chronionego filtrem. Ponadto filtry nie mogą sprawdzać wszystkich fragmentów datagramów IP w oparciu o protokoły wyższych warstw, nie mogą na przykład przeglądać nagłówków TCP, które istnieją tylko w pierwszym fragmencie. Kolejne fragmenty nie mają tej informacji i mogą być jedynie porównywane do reguł warstwy IP, które są zazwyczaj łagodniejsze przy przepuszczaniu ruchu przez filtr, pozwala to eksploatować błędy w warstwie IP komputerów docelowych i może pozwolić na połączenie z koniem trojańskim zainstalowanym wewnątrz sieci.