

Wstęp

W dokumencie niniejszym starałem się zebrać zestaw podstawowych zasad pozwalających na skonfigurowanie osobistego firewalla w domu tak, by jego użycie nie wiązało się z dodatkowymi uciążliwościami. Mówiąc o konfiguracji, mam na myśli typową dla wszelkich firewalli listę reguł, tworzących kryteria dla filtru pakietów, a nie ustawienia wyglądu, dostępu itp. charakterystyczne dla danej aplikacji. Ze względu na to, że każdy wykorzystuje sieć w nieco inny sposób, nie ma uniwersalnego, żelaznego zestawu reguł, który można by zastosować wszędzie. Jest jednak pewien zbiór minimalny, który starałem się wskazać. Omówię także sposób dopasowania konfiguracji firewalla do używanych aplikacji. W dalszej części dokumentu przedstawiona jest przykładowa konfiguracja dla firewalla użytkownika korzystającego ze standardowych usług internetowych, którą można się posłużyć do stworzenia własnego zestawu reguł.

Wierzę, że zawarte tu informacje przekonają choć część czytelników, że obsługa firewalla osobistego nie jest czymś nadzwyczaj skomplikowanym, a kontrola nad maszyną daje nie tylko większe poczucie bezpieczeństwa ale i satysfakcję.

Podstawowe pojęcia

Zrozumienie zasad konstrukcji reguł wymaga znajomości kilku podstawowych pojęć związanych z ruchem w sieci Internet. Jeżeli znasz podstawy działania sieci opartych o TCP/IP, możesz spokojnie pominąć tę część.

Dane w sieci Internet przesyłane są w porcjach zwanych pakietami. Każdy komputer, który komunikuje się z innymi w sieci Internet musi posiadać swój adres IP. W pewnym uproszczeniu, adresy IP są unikalne dla każdego komputera, który komunikuje się w sieci globalnej i mają postać xxx.xxx.xxx.xxx, gdzie każdy ciąg xxx jest liczbą z zakresu 0-255. Używane są trzy protokoły, na bazie których może być prowadzona wymiana informacji: ICMP, UDP oraz TCP. Pierwszy z nich służy celom diagnostycznym oraz administracyjnym. Najprostszym przykładem zastosowania ICMP jest polecenie ping. TCP jest protokołem używanym przez większość popularnych usług, m.in. http (np. przeglądanie stron WWW) czy smtp (wysyłanie poczty elektronicznej). W protokole tym wymiana danych następuje przez połączenie między dwoma maszynami. Polega ono na wymianie określonej sekwencji pakietów oznaczającej początek połączenia, wymianie danych oraz zamknięciu połączenia. Protokół UDP jest znacznie prostszy – dane przesyłane są w pojedynczych pakietach od jednego komputera do drugiego, bez zestawiania specjalnego połączenia.

Oprócz adresu IP każdy komputer w sieci posiada (w sensie logicznym) dwa zestawy portów, za pośrednictwem których może się komunikować – po jednym zestawie dla protokołów TCP i UDP. Porty w każdym z zestawów są ponumerowane od 1 do 65535. Tak więc port 135 TCP i 135 UDP to dwa różne porty. Większość typowych usług ma przypisane standardowe numery portów, z których korzysta się do komunikacji z nimi. Jest to znaczne ułatwienie (również w konfiguracji firewalla), ale nie wymóg. Na przykład, usłudze http przypisany jest standardowo port 80 TCP. Jeżeli komputer oferuje daną usługę, na przykład udostępnia strony WWW, aplikacja obsługująca ją otwiera odpowiedni port. Taki komputer nazywamy serwerem danej usługi. Komputer, który chce

uzyskać dostęp do usługi (klient) otwiera jeden ze swoich portów i wysyła z niego pakiety pod adres IP serwera na port tej usługi. Pakiet można więc opisać zestawem dwóch adresów IP (klienta i serwera) oraz dwóch numerów portów (źródłowego i docelowego). W przypadku protokołu UDP ewentualne odpowiedzi mogą być kierowane na ten sam lub inny port klienta. W protokole TCP całe połączenie odbywa się w ramach tych samych portów¹. W przypadku protokołu ICMP nie mówimy o portach, lecz o różnych komunikatach w zależności od tego, jaką informację niesie.

Działanie firewalla polega na filtrowaniu pakietów (dla UDP i ICMP) oraz połączeń według zadanych kryteriów (tzw. reguł) opartych przede wszystkim o adresy IP oraz porty. Pozwala to na uchronienie się przed niepowołanym dostępem do usług udostępnianych przez nas lub przez nasz system a także daje kontrolę nad połączeniami nawiązanymi przez programy.

Konstruowanie reguł

Podstawową zasadą, którą należy mieć na uwadze przy konstruowaniu zbioru reguł dla firewalla jest to, że są one analizowane przez niego w kolejności umieszczenia ich na liście. Pierwsza reguła, do której zostanie dopasowany analizowany pakiet będzie wykonana bez względu na to, jakie reguły następowały po niej. Kolejne reguły zostaną całkowicie zignorowane. W szczególności, umieszczenie na początku listy reguły pasującej do wszystkich pakietów oznaczałoby, w zależności od zdefiniowanej akcji, efektywne wyłączenie filtrowania lub blokowanie wszystkich pakietów. Stąd prosty wniosek, że umieszczanie reguł na liście powinno odbywać się według ich szczegółowości – im bardziej ogólna reguła, tym niżej na liście.

Reguły podstawowe

Poniżej przedstawione są typowe reguły, mające zazwyczaj zastosowanie przy najpopularniejszych formach korzystania z Internetu w domu (np. poczta, www). Konieczność zastosowania niektórych z nich może być dyskutowana w przypadku konkretnych użytkowników. Na przykład, reguła filtrująca ruch NetBIOS uniemożliwi udostępnianie plików i drukarek w sieci lokalnej. Jeżeli wykorzystujemy tę funkcjonalność, powinniśmy odblokować ruch NetBIOS do wybranych adresów. Oczywiście, taka reguła, jako bardziej szczegółowa, powinna znaleźć się przed regułą blokującą dostęp dla pozostałych adresów.

Pozwalamy na odpytywanie serwerów DNS.

Protokół:	UDP
Kierunek:	In/Out
Porty lokalne:	wszystkie
Aplikacja:	wszystkie
Adres:	wszystkie
Porty zdalne:	53
Czynność:	POZWALAJ

Pozwalamy na ruch w obrębie lokalnej maszyny (wymagają tego niektóre programy i usługi systemowe). Adres IP 127.0.0.1 jest adresem zarezerwowanym, oznaczającym: „maszyna lokalna”.

Protokół ² :	Wszystkie
Kierunek:	In/Out

¹ Oczywiście, wartości dla źródła i celu są zamienione w pakietach będących odpowiedziami serwera. Jednak z punktu widzenia firewalla w protokole TCP bierzemy pod uwagę jedynie nawiązanie połączenia.

² Zastosowana tu nomenklatura nie odnosi się do żadnego konkretnego oprogramowania. Podane pola, niezależnie od ich nazwy, występują w każdym oprogramowaniu typu firewall.

Porty lokalne:	wszystkie
Aplikacja:	wszystkie
Adres:	127.0.0.1
Porty zdalne:	wszystkie
Czynność:	POZWALAJ

Blokujemy ruch NetBIOS w obu kierunkach³.

Protokół:	TCP/UDP
Kierunek:	In
Porty lokalne:	137, 138, 139, 445
Aplikacja:	wszystkie
Adres:	wszystkie
Porty zdalne:	wszystkie
Czynność:	BLOKUJ

Protokół:	TCP/UDP
Kierunek:	Out
Porty lokalne:	wszystkie
Aplikacja:	wszystkie
Adres:	wszystkie
Porty zdalne:	137, 138, 139, 445
Czynność:	BLOKUJ

Pozwalamy na komunikację z serwerem DHCP. Jest to usługa, pozwalająca na automatyczne skonfigurowanie parametrów dostępu do sieci przez serwer dostawcy. Jeżeli konfigurując dostęp do Internetu musiałeś ręcznie wpisywać dane takie jak adres IP czy adresy serwerów DNS, oznacza to, że twój dostawca nie korzysta z tego protokołu i reguła ta nie jest potrzebna

Protokół:	UDP
Kierunek:	In/Out
Porty lokalne:	wszystkie
Aplikacja:	wszystkie
Adres:	wszystkie
Porty zdalne:	67
Czynność:	POZWALAJ

Pozwalamy na selektywny ruch ICMP.

Protokół:	ICMP
Kierunek:	Out
Typ:	Echo Request
Aplikacja:	wszystkie
Adres:	wszystkie
Czynność:	POZWALAJ

Protokół:	ICMP
Kierunek:	In
Komunikat:	Echo Reply, Time Exceeded, Destination Unreachable

³ W podanym przykładowym zestawie reguła ta mogłaby zostać pominięta ze względu na zalecaną regułę „blokuj wszystko”. Warto jednak zapisać ją wprost z dwóch przyczyn: nie ryzykujemy w ten sposób przypadkowego pozostawienia usługi NetBIOS otwartej, np. wyłączając na pewien czas inną regułę, a także sprawiamy, że pakiety wysyłane do naszego komputera przez robaki wykorzystujące NetBIOS będą odrzucane bez przeglądania kolejnych reguł na liście, a więc nieco szybciej.

Aplikacja:	wszystkie
Adres:	wszystkie
Czynność:	POZWALAJ

Protokół:	ICMP
Kierunek:	In/Out
Komunikat:	wszystkie
Aplikacja:	wszystkie
Adres:	wszystkie
Czynność:	BLOKUJ

Przepuszczamy ruch związany z przeglądaniem serwisów w przeglądarkach (http[s], proxy, ftp)...

Protokół:	TCP
Kierunek:	Out
Porty lokalne:	wszystkie
Aplikacja:	wszystkie
Adres:	wszystkie
Porty zdalne ⁴ :	80, 443, 8080, 3128, 20, 21
Czynność:	POZWALAJ

...oraz korzystaniem z klientów poczty i news (pop3, smtp, imap, nntp)

Protokół:	TCP
Kierunek:	Out
Porty lokalne:	wszystkie
Aplikacja:	wszystkie
Adres:	wszystkie
Porty zdalne:	25, 110, 119, 143
Czynność:	POZWALAJ

Ustawienia specyficzne dla aplikacji

Należy sprawdzić, jakich portów i jakiego protokołu używa do komunikacji dana aplikacja. Może być w tym pomocna funkcja samego firewalla wyświetlająca alarm informujący o próbie nawiązania połączenia. W alarmie takim zawarte będą wszystkie interesujące nas informacje. Często potrzebne dane podawane są także w dokumentacji lub na stronie internetowej producenta oprogramowania. Pozostaje stworzyć regułę, pozwalającą wybranej aplikacji na używanie danych portów. Reguły dedykowane konkretnej aplikacji powinny znaleźć się blisko początku listy jako bardzo szczegółowe.

UWAGA: Należy pamiętać, że pozwalanie na nawiązywanie połączeń przychodzących jest potencjalnie bardziej ryzykowne niż przepuszczanie jedynie połączeń wychodzących. W miarę możliwości należy korzystać jedynie z programów, które nie wymagają otwierania portu na lokalnym komputerze.

Dla przykładu przedstawiam regułę, pozwalającą na korzystanie z popularnego komunikatora Gadu-Gadu. Według danych producenta, używa on do komunikacji z serwerem portu TCP 8074. W polu 'Aplikacja' podajemy ścieżkę programu, który upoważniamy do nawiązywania połączeń.

Protokół:	TCP
-----------	-----

⁴ Uwaga: Porty 3128 i 8080 tcp są typowymi portami używanymi przez serwery proxy. Jeżeli serwer, z którego korzystasz używa innych portów, należy zmienić te numery na właściwe. Jeżeli nie korzystasz z proxy, powinieneś w ogóle pominąć te porty.

Kierunek:	Out
Porty lokalne:	wszystkie
Aplikacja:	Gadu-Gadu
Adres:	wszystkie
Porty zdalne:	8074
Czynność:	POZWALAJ

Pozwalając niektórym aplikacjom na szerszy dostęp do Internetu niż pozostałym należy pamiętać, że „zaufanie” przypisujemy danemu plikowi wykonywalnemu w systemie. Jego podmiana, np. przez konia trojańskiego, oznaczać będzie, że aplikacja, na którą została dokonana podmiana uzyska nadane przez nas uprawnienia. Oczywiście w pełni legalnym przypadkiem takiej sytuacji jest aktualizacja programu. Wiele firewallei osobistych monitoruje zmiany w programach wykonywalnych, które łączą się z Internetem, pozwalając użytkownikowi na akceptację ewentualnych zmian.

Reguły końcowe – „blokuje wszystko” vs. „blokuje przychodzące”

Zgodnie z zasadą sekwencyjnego przeglądania reguł do momentu napotkania pierwszej pasującej, ostatnie reguły umieszczone na liście dotyczą pakietów niepasujących do kryteriów określonych wcześniej. Jest to więc ruch, którego występowania nie spodziewamy się – w zamysle niepożądany.

Wygodną regułą, która pozwala na zablokowanie tego ruchu jest prosta zasada „blokuje wszystko”. Przed włączeniem tej reguły należy poprawnie skonfigurować reguły dla wszystkich aplikacji łączących się z Internetem według powyższych opisów i upewnić się, że wszystko działa jak należy.

Należy pamiętać, że reguła „blokuje wszystko” powinna być umieszczona jako ostatnia na liście reguł. Zasada wykonywania reguł według kolejności sprawia, że umieszczenie jej na początku skutecznie zablokuje połączenie z siecią. Szczególnie w przypadku tej reguły zaleca się włączyć logowanie, tzn. rejestrację każdego przypadku wykonania reguły, co umożliwi zdiagnozowanie ewentualnych problemów spowodowanych działaniem firewallea.

Protokół:	Wszystkie
Kierunek:	In/Out
Porty lokalne:	wszystkie
Aplikacja:	wszystkie
Adres:	wszystkie
Porty zdalne:	wszystkie
Czynność:	BLOKUJ

Niektórzy opowiadają się za rozwiązaniem mniej radykalnym, w którym ruch wychodzący jest swobodnie przepuszczany a ruch przychodzący zatrzymywany. Zaletą takiego rozwiązania jest gwarancja, że wszystkie nasze aplikacje będą mogły swobodnie łączyć się z Internetem – nawet bez określania specyficznych reguł. Wadą jest zrezygnowanie z jakiegokolwiek kontroli nad tym które aplikacje, z jakimi adresami i w jaki sposób się łączą. W ten sposób tracimy sporą część funkcjonalności firewallea i zdecydowanie zwiększamy zagrożenie działaniem koni trojańskich oraz programów typu spyware. Taka praktyka bywa często stosowana w sieciach korporacyjnych ze względu na łatwość administracji. Uważa się ją jednak za niedoskonałą, a w przypadku komputera domowego, gdzie mamy bezpośrednią kontrolę nad instalowanymi aplikacjami, zdecydowanie jej nie zalecam.

Administracja i rozwiązywanie problemów

W zasadzie, raz skonfigurowany firewall powinien spełniać swoje zadanie bez konieczności częstego modyfikowania listy reguł. Od czasu do czasu możemy jednak napotkać problemy z działaniem pewnych usług, np. czatów czy programów interaktywnych na stronach WWW, wymagających połączeń z serwerem na nietypowych portach. Jeżeli nasz firewall dysponuje opcją alertowania przy próbie nawiązania połączenia przez aplikację, jest to najwygodniejszy sposób wykrycia problemu. Aby informacje te były wyświetlane, może okazać się konieczne czasowe wyłączenie reguł blokujących ruch na końcu listy – warto zapoznać się z pomocą i dokumentacją oprogramowania. Następnie, wykorzystując zebrane informacje o docelowych adresach, portach, protokole i samej aplikacji, należy skonstruować regułę pozwalającą na działanie usługi. Sposób postępowania jest dokładnie taki sam jak przy konstrukcji reguł dla aplikacji opisanej powyżej.

O ile włączone jest logowanie, należy okresowo przeglądać i czyścić zawartość pliku, do którego zapisywane są logi. Wśród zawartych tam informacji należy zwrócić uwagę na wszelkie zablokowane połączenia wychodzące. Mogą one być zwiastunem niewykrytych jeszcze problemów opisanych wyżej lub kłopotów administracyjnych (np. trojan w systemie, nietypowe zachowanie aplikacji). Odrzucone połączenia przychodzące to w większości typowy „szum” w sieci, do którego niestety zalicza się ruch generowany przez próby infekcji robaków. Jeżeli nie jesteś pewien, czy dane połączenie jest w tych kategoriach typowe, czy nie, możesz poszukać aktualnych informacji na temat ruchu na danym porcie w sieci – np. na tej stronie:

<http://www.robertgraham.com/pubs/firewall-seen.html>.