Maskowanie adresu IP

Mechanizm translacji adresów sieciowych NAT nazywany również maskowaniem adresu IP rozwiązuje problem ukrywania wewnętrznych hostów. NAT jest mechanizmem zastępczym – pojedynczy host wysyła żądania w imieniu wszystkich wewnętrznych hostów i ukrywa w ten sposób ich tożsamość dla sieci publicznej. Windows NT nie zapewnia takiej funkcji jeżeli zachodzi potrzeba użycia NAT trzeba zainstalować oprogramowanie firewall z innego źródła[1].

W Linuxie i systemach operacyjnych typu UNIX funkcja NAT wchodzi w skład pakietu. Mechanizm NAT ukrywa wewnętrzne adresy IP za pomocą zamiany wszystkich adresów wewnętrznych hostów na adres ściany ogniowej. Następnie ściana przesyła ładunek danych pochodzący z wewnętrznych hostów zaopatrując go we własny adres. Wykorzystuje przy tym numer portu TCP w celu śledzenia odwzorowań połączeń ze strony sieci publicznej z hostami wewnętrznymi. Z punktu widzenia Internetu cały ruch wydaje się pochodzić z jednego, obciążonego komputera. Mechanizm NAT skutecznie ukrywa wszystkie informacje warstw TCP/IP związane z hostami wewnętrznymi przed użytkownikami Internetu. Translacja adresów pozwala również na korzystanie w sieci wewnętrznej z dowolnego zakresu adresów IP, nawet jeżeli są one używane gdzieś w Internecie. Oznacza to, że nie trzeba rejestrować dużych bloków adresów w InterNIC lub zmieniać adresy wstępnie nadane w sieci, zanim została ona przyłączona do Internetu.

NAT pozwala także na rozdzielenie pojedynczego adresu IP na całą sieć. Wiele małych instytucji korzysta z pomocy dostawcy usług internetowych, który może niechętnie przydzielać duży blok adresów IP ponieważ jego puka jest ograniczona. Dzięki maskowaniu adresu użytkownik może współużytkować pojedynczy adres modemu (przyłączonego na stałe lub dial-up) bez konieczności informowania o tym swojego dostawcy. Wadą korzystania z NAT jest to, że jest on implementowany tylko na

poziomie warstwy transportowej. Oznacza to w praktyce, że informacja ukryta w części danych pakietu TCP/IP może być przesłana do usług wyższej warstwy i wykorzystania do eksploatacji słabości w innej warstwie lub do komunikowania się z koniem trojańskim.

Użytkownicy, którzy chcą zapobiegać naruszeniom bezpieczeństwa muszą korzystać z usług takich jak proxy. NAT rozwiązuje wiele problemów związanych z bezpośrednim połączeniem z internetem, ale nadal nie ogranicza całkowicie przepływu datagramów przez firewala. Osoba wyposażona w monitor sieciowy może obserwować ruch wychodzący ze ściany ogniowej i stwierdzić, że przekształca on adresy innych komputerów. Hakerzy mogą w takiej sytuacji przechwycić połączenia TCP lub je sfałszować. Takiemu zagrożeniu zapobiega tzw. proxy aplikacyjne. Pozwalają one całkowicie rozłączyć przepływ protokołów warstwy sieciowej przez ścianę ogniową i skierować ruch do protokołów warstwy wyższej takich jak HTTP, FTP i SMTP.

Proxy przyjmuje próbę połączenia z zewnętrznymi serwerami i następnie w imieniu klienta wykonuje żądanie połączenia do serwera docelowego. Gdy serwer zwraca dane proxy przekazuje je do klienta. Proxy aplikacyjne różnią się od mechanizmów NAT i filtrów tym, że aplikacja klienta internetowego jest konfigurowana tak, aby komunikowała się z proxy. Na przykład użytkownik przekazuje aplikacji Internet Explorer adres swojego proxy WWW i wtedy Internet Explorer przesyła wszystkie żądania WWW do proxy, zamiast odwzorowywania nazwy na adres IP i wykonywania połączenia bezpośrednio.

Proxy aplikacyjne nie muszą być uruchamiane na komputerach-ścianach ogniowych. Każdy serwer, zarówno wewnątrz jak i na zewnątrz sieci użytkownika, może spełniać funkcję proxy. Jednak bez ściany ogniowej nie można osiągnąć prawdziwego bezpieczeństwa, potrzebne są oba rozwiązania. Niezbędny jest co najmniej jeden filtr pakietów po to, aby chronić serwer proxy przed atakami w warstwie sieciowej typu uniemożliwienia działania [2].

Jeżeli zaś proxy nie jest uruchomione na komputerze pełniącym rolę ściany ogniowej, trzeba otworzyć kanał w ścianie w taki lub inny sposób. Najlepsza jest sytuacja, gdy ściana ogniowa spełnia rolę proxy. Zapobiegałoby to przekazywaniu pakietów przychodzących z sieci publicznej do sieci użytkownika. Niektóre ściany ogniowe typu proxy są bardziej złożone od innych. Ponieważ mają one mechanizmy filtrów oraz maskowania IP, można za ich pomocą blokować próby połączeń wychodzących (port80 w przypadku HTTP) do zdalnych hostów zamiast wymagać, aby oprogramowanie klienta było odpowiednio skonfigurowane z uwzględnieniem usługi proxy. Proxy firewala łączy się odpowiednio ze zdalnym serwerem i żąda danych w imieniu zablokowanego klienta. Odszukane dane są zwracane do klienta za pomocą mechanizmu NAT i wygląda to tak, jakby pochodziły ze zdalnego serwera [3].

Proxy zabezpieczające potrafią także wykonywać filtrowanie określonej zawartości na poziomie warstwy aplikacyjnej. Na przykład niektóre proxy HTTP szukają etykiet na stronach HTML, które odwołują się do wbudowanych apletów Java lub ActiveXi następnie usuwają z nich zawartość. Zapobiega to wykonaniu apletu na komputerze klienckim i eliminuje ryzyko przypadkowego załadowania przez klienta konia trojańskiego. Tego typu działanie jest bardzo ważne, ponieważ filtrowanie IP, stosowanie proxy i maskowanie adresu nie zapobiegną naruszeniu bezpieczeństwa sieci, jeżeli użytkownik załaduje aplet ActiveX z koniem trojańskim.. W miarę przechodzenia do warstw wyższych sieci usługi bezpieczeństwa są coraz ściślej określane. Na przykład filtrowanie dotyczy warstw IP i następnie TCP oraz UDP.

Aplikacje, które korzystają z IP w połączeniu z innymi protokołami na przykład Banyan Vines, muszą stosować specjalne, bardzo kosztowne lub niezwykle silne ściany ogniowe. Proxy są bardzo ściśle określone ponieważ mogą one pracować tylko dla konkretnej aplikacji. Na przykład HTTP wymaga oddzielnego modułu proxy niż FTP lub Telnet. W miarę

rozwoju protokołów (szczególnie HTTP zmienia się szybko) moduł proxy związany z danym protokołem musi być aktualizowany. Istnieje wiele protokołów, które są własnością producenta lub są na tyle rzadkie, że nie ma dla nich proxy zabezpieczającego. Przykładem protokołu aplikacyjnego, który jest własnością i nie ma proxy zabezpieczającego jest Lotus Notes. Protokoły te muszą być przesyłane poprzez filtry warstwy sieciowej lub można dla nich użyć uniwersalne proxy TCP, który odtwarza pakiet ale nie ingeruje w przesyłane dane. Przykładem proxy uniwersalnego jest pakiet SOCKS, nazywany czasem bramą warstwy obwodowej. Mimo, że proxy uniwersalne nie może zapobiec atakowi z zawartości protokołu, jest bezpieczniejsze niż filtrowanie routingu, ponieważ pakiety warstwy sieciowej są całkowicie odtworzone i usunięte są z nich zniekształcenia, które mogłyby być nie wykryte przez ścianę ogniową.

---

[1] Windows 2000 posiada wbudowany NAT.

[2] Atak typu Ping of Death.

[3] Taki typ proxy nazywany jest proxy przezroczystym (ang. Transparent)