Konfiguracja i ustawianie zapory ogniowej

Naszym przykładem jest komputer klasy i486-DX66 z 16 Mb pamięci RAM oraz 500Mb partycją Linux. System ten posiada dwie karty sieciowe, jedną połączoną z naszą siecią prywatną, a drugą do sieci lokalnej nazywanej strefą zdemilitaryzowaną (DMZ). DMZ posiada router połączony do Internetu. Dobrze jest użyć jednej karty sieciowej oraz modemu z PPP dla podłączenia do intenetu.

Firewall powinien posiadać dwa adresy IP.

Jeśli wszystkim czego nam potrzeba jest filtrujący firewall dobrze jest zaopatrzyć się jedynie Linuxa i podstawowe pakiety sieciowe. Jednym z pakietów który może nie zawierać się w naszej dystrybucji jest IP Firewall Administration tool. Jeśli jest nam potrzebny serwer proxy należy użyc jednego z niżej wymienionych pakietów:

1. SOCKS
2. TIS Firewall Toolkit (FWTK)

Trusted Information System jest fragmentem kolekcji programów zaprojektowanych dla firewalli. Program ten udostępnia podobne rzeczy jak SOCK, ale jest zbudowany na innych zasadach. Tam gdzie Socks posiada jeden program przeprowadzający wszystkie transakcje z internetem, TIS dostarcza jednego programu dla każdego z narzędzi których chcemy użyć w firewallu.

Dla pokazania kontrastu użyjmy przykładów WWW i dostępu za pomocą telnetu. Używając SOCKS, ustawiamy jeden plik konfiguracyjny i jednego demona. Używając tego pliku tak telnet jak i WWW są dostępne, podobnie jak inne usługi których nie zakazaliśmy.

W pakiecie TIS ustawiamy jednego demona dla (osobno) WWW i

Telnetu z osobnymi plikami konfiguracyjnymi. Po zrobieniu tego inne usługi internetowe są zakazane dopóki ich nie ustawimy. Jeśli demon dla specyficznych usług jest niedostępny (tak jak talk), istnieją ,,plug-in-y" dla demona, ale nie są tak elastyczne i łatwe w konfiguracji jak inne narzędzia.

Różnica wygląda na niewielką, jest jednak istotna. SOCKS pozwala administratorowi na spokój. Przy niewłaściwie ustawionym SOCKS serwerze osoba z wewnątrz może uzyskać większy dostęp do Internetu niż było początkowo planowane. Z pakietem TIS użytkownicy wewnątrz sieci mają jedynie taki dostęp na jaki zezwolił administrator.

SOCKS są łatwiejszy do konfiguracji, łatwiejszy do kompilacji i pozwala na większą elastyczność. TIS jest bardziej bezpieczny, jeśli chcemy ustawiać użytkowników wewnątrz chronionej sieci. Obydwa dostarczają całkowitego bezpieczeństwa z zewnątrz.