

I. Serwer dostępowy do sieci Internet – skrócony opis

Dwoma głównymi grupami usług serwera dostępowego są:

1. Usługi bramy sieciowej
2. Usługi podziału łącza

Skrypty i pliki konfiguracyjne wymienionych usług zlokalizowane są w katalogu `/usr/local/isp/`

Za wyżej wymienione usługi odpowiadają następujące skrypty :

1. *multi-isp* – brama sieciowa, routing
2. *firewall* (wraz z plikami konfiguracyjnymi) – brama sieciowa, firewall
3. *shaper* (wraz z plikami konfiguracyjnymi) – podział łącza

1. Multi-isp **

Skrypt jest odpowiedzialny za tworzenie odpowiedniej tablicy routingu, w przypadku wykorzystywania więcej niż jednego łącza WAN. Bazuje na narzędziu *ip* z pakietu *iproute2*. Tablica routingu jest tworzona każdorazowo w momencie uruchomienia systemu i nie wymaga czynności obsługowych. Modyfikacja konieczna jest jedynie w przypadku zmiany ustawień TCP/IP dla łącz WAN oraz konfiguracji nowej podsieci w sieci LAN. Konfiguracja umożliwia m.in.:

- 1) Routing danego użytkownika, lub podsieci wybranym łączem WAN
- 2) Routing danych usług wybranym łączem WAN – nie dotyczy sesji p2p

2. Firewall

Skrypt definiujący działania dla pakietów transmisji danych związane z bezpieczeństwem i kontrolą ruchu. Bazuje na narzędziu *iptables*. Główne funkcje:

- 1) Zapora sieciowa, autoryzacja MAC-IP, translacja adresów (NAT)
- 2) ograniczenie ilości jednocześnie nawiązywanych połączeń
- 3) ograniczenie transferu klienta w pkt/s
- 4) blokada przekazywania spamu i wirusów sieciowych
- 5) klasyfikacja ruchu p2p
- 6) znakowanie pakietów na potrzeby graficznych statystyk użytkowników (*lstat*) oraz tablicy routingu (opcjonalnie)

Struktura firewall'a

Lp	Nazwa pliku	Poziom dostępu	Lokalizacja - katalog	Funkcja
1.	firewall	***	/usr/local/isp/	Główny plik firewall'a - skrypt
2.	fire.cfg	**	/usr/local/isp/fire/	Ustawienia główne, adresy, komunikaty LAN
3.	fire.imac	*		Autoryzacja MAC-IP
4.	fire.ippport	**		Przekierowania portów,
5.	17-proto	***		Filtry layer7

3. Shaper

Skrypt odpowiedzialny za podział łącza. Bazuje na narzędziu *tc* z pakietu *iproute2*. Realizuje wymienione funkcje:

1. Dwustopniowy dynamiczny podział łącza w obu kierunkach transmisji (download/upload) – algorytm htb
 - 1.1 Podział ze względu na typ usługi (klasyfikacja wg portów źródłowych/docelowych)
 - 1.2 Podział ze względu na użytkownika sieci LAN (klasyfikacja wg IP źródłowego/docelowego)
2. Zapewnienie równomiernego podziału w ramach każdej klasy usługi/ użytkownika – algorytm sfq

Struktura shapera

Lp	Nazwa pliku	Poziom dostępu	Lokalizacja - katalog	Funkcja
1.	shaper	***	/usr/local/isp/	Główny plik shaper'a - skrypt
2.	shape.cfg	**	/usr/local/isp/shape/	Ustawienia główne, adresy, prędkości łącza
3.	shape.class.usr	*		Prędkości klas dla poszczególnych użytłk. – down/up
4.	shape.class.srv	**		Prędkości klas dla poszczególnych usług – down/up
5.	shape.filter.srv	***		Filtry klasyfikujące ruch do klas poszczególnych usług – down/up

Poziom dostępu:

* - przewidziany do bieżącej edycji

** - przewidziany do edycji dla administratora systemu

*** - przewidziany do edycji dla autora konfiguracji

II. Firewall – opis funkcji oraz zagrożeń jakim przeciwdziałają

1. Firewall – zaporę sieciową
2. autoryzacja MAC-IP
3. translacja adresów (NAT) - maskarada IP, przekierowania portów
4. ograniczenie ilości jednocześnie nawiązywanych połączeń – moduł connlimit
5. ograniczenie transferu klienta w pkt/s – moduł hashlimit
6. blokada przekazywania spamu
7. blokada przekazywania wirusów sieciowych
8. klasyfikacja ruchu p2p i umieszczanie go w odpowiednich klasach – moduł ipp2p oraz 17
9. znakowanie pakietów na potrzeby graficznych statystyk użytkowników (lstat)

- Firewall – zaporę sieciową.

Zabezpieczenie serwera oraz systemów użytkowników sieci LAN przed niepożądanym dostępem z zewnątrz.

- Autoryzacja MAC-IP

Zapewnia blokadę dostępu dla nieautoryzowanych par adresów MAC-IP. Dostęp tylko klientów, blokowanie obcych użytkowników podpiętych samowolnie.

- Translacja adresów - maskarada IP

Maskowanie adresów IP polega na ukryciu (zamaskowaniu) adresów IP komputerów w sieci LAN przez router podłączony do Internetu z publicznym adresem IP. Tym samym wszystkie komputery widoczne są od strony Internetu jako jedna maszyna. Pozwala to na dostęp do Internetu komputerom nie posiadającym publicznego adresu IP (192.168.*.* czy też 10.*.*.*)
Maskowanie adresów IP zapewnia dodatkowo wyższy poziom bezpieczeństwa sieci lokalnej, ograniczając możliwości potencjalnych ataków na stacje robocze.

- Translacja adresów – przekierowania portów

Przekierowanie portów umożliwia m.in.

- świadczenie usług internetowych (serwer ftp, serwer WWW, korzystanie z p2p w trybie active (High ID w przypadku sieci edonkey) przez komputery korzystające z maskarady IP.

- przekierowanie wolnego publicznego adresu IP na komputer z adresem z prywatnym

- Ograniczenie liczby jednocześnie nawiązywanych połączeń.

W skutek niewłaściwego korzystania z programów p2p, generują one bardzo wiele połączeń (niektórzy użytkownicy potrafią wygenerować kilka tysięcy), co w skrajnych przypadkach może prowadzić do zapychania łącza. Należy pamiętać że w przypadku korzystania z maskarady IP każde takie połączenie jest obsługiwane przez odpowiedni moduł, nadmierna liczba połączeń może spowodować przepełnienie bufora w którym są przechowywane wszystkie połączenia, co skutkuje uniemożliwieniem nawiązania następnym połączeń innym użytkownikom.

- Ograniczenie transferu w pakietach na sekunde.

Warto zwrócić uwagę na fakt, że ograniczenie liczby połączeń jest skuteczne tylko odnośnie protokołu TCP. Sesje UDP nie podlegają limitowaniu connlimitem. Aby zapobiec sytuacji w której poszczególni klienci lub ich grupa powodują tzw. zapychanie łącza w wyniku generowania zbyt dużej liczby pkt/s należy limitować transfer liczony właśnie w pkt/s.

- Blokada spamu i wirusów sieciowych.

Użytkownicy systemów zaatakowanych przez wirusy i robaki internetowe, są najczęściej nieświadomi jakich problemów przysparzają operatorowi łącza. Ponieważ zarażone systemy stają się źródłem rozprzestrzeniania wirusów, zagrożeniu podlegają inni współużytkownicy. W sieci Internet istnieją mechanizmy obronne przed zarażonymi systemami, jednym z nich są tak zwane listy spammerskie, „czarne listy” zawierające adresy IP systemów będących źródłem wirusów lub spamu. Z czarnych list korzystają m.in. serwery poczty, blokując dostęp systemom które na nich figurują. Ponieważ cały ruch z sieci LAN przechodzi przez serwer dostępowy, z punktu widzenia innych użytkowników sieci Internet to właśnie on jest źródłem wirusów i spamu. W efekcie adres IP serwera dostępowego trafia na listy spammerskie, co skutkuje blokadą dostępu do niektórych serwerów pocztowych, a konsekwencji uniemożliwieniem korzystania z usługi email przez klientów sieci LAN.

Innym efektem działania zawirusowanych systemów, jest zapychanie łącza szkodliwymi pakietami, z powodu ograniczonej przepustowości szczególnie uciążliwe w sieciach opartych o technologię wifi.

- Klasyfikacja ruchu p2p

Trudność z kontrolowaniem ruchu p2p polega na tym, że aplikacje p2p korzystają z wielu różnych portów, stąd niemożliwe jest sklasyfikowanie tej usługi za pomocą standardowych mechanizmów podziału łącza, bazujących na tym, że określone usługi korzystają z ustalonych portów. Brak klasyfikacji ruchu p2p prowadzi do zapychania łącza, co skutkuje utrudnieniem, lub wręcz uniemożliwieniem innym użytkownikom korzystania z usług podstawowych typu WWW, czy email.

Więcej na ten temat w artykule „Kontrola ruchu peer-to-peer w sieciach dostępowych”.