

Instrukcja do zajęć laboratoryjnych

Temat ćwiczenia:

**Realizacja kontroli ruchu w sieci IP
z wykorzystaniem list dostępowych (ACL)**

Numer ćwiczenia: 5

Laboratorium z przedmiotu:
Systemy i sieci telekomunikacyjne 2

Kod przedmiotu: TS1A510 207

Instrukcję opracował:
dr inż. Andrzej Zankiewicz

1. Ogólna charakterystyka ćwiczenia

Każdy system operacyjny routerów Cisco (IOS) ma wbudowany mechanizm filtrowania ruchu poprzez listy dostępu (ACL – *Access Control List*). Filtrowanie pakietów jest jedną z podstawowych metod zabezpieczenia i ograniczenia ruchu w sieci. Mechanizm ten pozwala określić pomiędzy jakimi sieciami (źródłowa, docelowa) może odbywać się komunikacja, a także umożliwić wskazanie typu pakietów oraz aplikacji dopuszczanych do korzystania z danego połączenia. Lista ACL stanowi zestaw kryteriów, na podstawie których odpowiednie procesy routera podejmują decyzję, co zrobić z pakietami danego typu. Ta decyzja musi być jednoznaczna i sprowadza się do wyboru między dwoma stanami: zgoda na przetworzenie pakietu (*allow*) lub odmowa (*deny*). Pojęcie list dostępu wykracza znacznie poza operację prostego filtrowania pakietów przez router, a listy ACL mają zastosowanie m.in. w takich elementach konfiguracyjnych routera, jak:

- Ustalenie priorytetów i kolejowania ruchu na interfejsach routera. Procesy te pozwalają wskazać kolejność przetwarzania pakietów na poszczególnych interfejsach oraz umożliwiają zrównoważenie ruchu w sieci.
- Ograniczenie zawartości uaktualnień tras wysyłanych przez protokoły routingu dynamicznego. To ograniczenie może również dotyczyć uaktualniania tablicy routingu przez router odbierający ogłoszenia tras. Proces ten nazywany jest również filtrowaniem tablicy routingu.
- Wskazanie tras otrzymywanych protokołem RIP w celu wykonania operacji zwiększenia metryki.
- Określenie pakietów, które spowodują zainicjowanie dodzwanianego połączenia DDR (*Demand Dial Routing*) z innym urządzeniem w sieci rozległej.
- Wskazanie ruchu, który ma być dodatkowo zabezpieczony, np. uwierzytelniany lub szyfrowany specjalizowanymi procesami w rodzaju protokołu IPsec.
- Opisanie ograniczeń dostępu do routera poprzez wirtualne linie terminalowe, czyli poprzez telnet.

Listy dostępu są więc podstawą do konfiguracji wielu procesów związanych nie tylko z bezpieczeństwem sieci. Celem ćwiczenia jest zapoznanie z zasadami tworzenia i wykorzystywania rozszerzonych i kontekstowych list dostępu dla protokołów IP oraz usług korzystających z protokołów transportowych TCP i UDP.

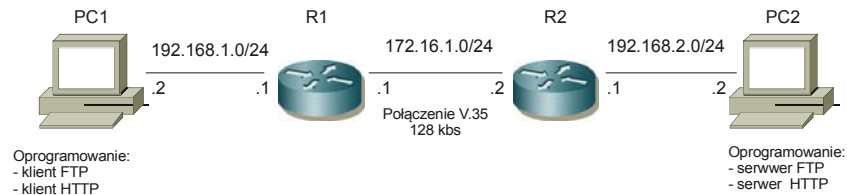
2. Przygotowanie do zajęć

Przed przystąpieniem do wykonywania ćwiczenia należy zapoznać się z następującymi materiałami:

- Całość niniejszej instrukcji.
- Podstawowe informacje o listach dostępu np. w publikacji [3].
- Nawiązywanie połączeń i przebieg transmisji w protokołach TCP oraz FTP (zarówno w trybie pasywnym jak i aktywnym).
- Dokumentacja systemów operacyjnych routerów CISCO dotycząca konfiguracji list dostępu.

3. Plan wykonywania ćwiczenia laboratoryjnego

1. Połączyć routery **R1**, **R2** oraz komputery **PC1** i **PC2** według poniższego schematu.
2. Nadać poszczególnym routerom odpowiednie nazwy (**R1**, **R2**).
3. Skonfigurować adresy IP na poszczególnych interfejsach zgodnie z danymi zamieszczonymi na schemacie.
4. Skonfigurować pozostałe parametry interfejsów routerów (np. szybkość pracy szeregowych portów DCE).



5. Skonfigurować w routerach **R1** i **R2** routing statyczny tak, aby było dostępne połączenie pomiędzy stacjami **PC1** i **PC2**.
6. Sprawdzić poprawność działania struktury (tzn. dostępność wszystkich przyłączonych sieci z poziomu wybranego routera oraz hosta) odczytując jego tablicę routingu (polecenie **sh ip route**) oraz korzystając z komend **ping** i **traceroute**.
7. Z poziomu stacji **PC1** sprawdzić dostępność usług WWW i FTP na stacji **PC2** oraz odwrotnie. Na stacjach zainstalowane są serwery udostępniające pliki o nazwach *test_http.zip* (serwer WWW) oraz *test_ftp.zip* (serwer FTP). Serwer FTP może pracować zarówno w trybie aktywnym jak i pasywnym. Rodzaj użytego trybu wybierany jest w oprogramowaniu klienta FTP.
8. W routerze **R1** skonfigurować listę dostępu blokującą odpowiedzi **ping** (komunikat *echo replay* protokołu ICMP) wysyłane przez stację **PC1**. Sprawdzić poprawność pracy ustawionej listy (także poprzez analizę liczby „trafień” danej listy).
9. Skonfigurować i sprawdzić poprawność pracy listy dostępu blokującej dostęp do usługi WWW na stacji **PC1**.
10. Skonfigurować listę dostępu blokującą nawiązywanie połączeń TCP do stacji **PC1**. Lista ta nie powinna blokować możliwości nawiązywania połączeń TCP przez stację **PC1** (np. do usług WWW oraz FTP w trybie pasywnym udostępnianych przez stację **PC2**). Wskazówka: nawiązanie połączenia TCP wymaga przyjęcia przez stację segmentu TCP z ustawioną flagą SYN, utworzona lista powinna dopuszczać do stacji **PC1** ruch tylko z połączeń TCP nawiązanych uprzednio przez tę stację. Dlaczego tak utworzona lista nie pozwala na nawiązywanie przez stację **PC1** połączeń FTP w trybie aktywnym?
11. Zmodyfikować listę utworzoną w poprzednim punkcie tak, aby stacja **PC1** mogła nawiązywać połączenia FTP także w trybie aktywnym.
12. Usunąć listy ACL utworzone w poprzednich punktach. Skonfigurować listę pozwalającą stacji **PC1** na nawiązywanie tylko połączeń WWW do dowolnych

hostów. Każdy inny rodzaj ruchu TCP wychodzącego oraz przychodzącego do stacji **PC1** i nie związanego z nawiązanym przez **PC1** połączeniem WWW powinien być blokowany. Wskazówka: można w tym celu wykorzystać opcję *established* w rozszerzonej liście dostępu.

13. Zaproponować i przetestować wykorzystanie listy ACL do zliczania liczby połączeń przyjmowanych przez określoną usługę (np. WWW) na stacji **PC2**.
14. Skonfigurować kierowanie komunikatów związanych z użyciem utworzonych list dostępowych do serwera usługi syslog.

W sprawozdaniu należy zamieścić wyniki uzyskane przy wykonywaniu poszczególnych części ćwiczenia oraz ich interpretację, a także własne uwagi i spostrzeżenia powstałe w trakcie wykonywania ćwiczenia.

4. Wymagania BHP

Zgodnie z podanymi na pierwszych zajęciach i potwierdzonymi przez studentów zasadami obowiązującymi w pomieszczeniu, w którym odbywają się ćwiczenia. Stosowny regulamin BHP jest też wywieszony w pomieszczeniu laboratorium.

5. Literatura

1. Graziani R., Vachon B.: Akademia sieci Cisco. CCNA Exploration. Semestr 4. Sieci WAN – zasady dostępu. Wydawnictwo PWN-MIKOM, Warszawa 2009.
2. Pierścionek W., Zejer P.: Kurs przygotowawczy do egzaminu CCNA. Część 7. *PC Kurier* 19/2001.
3. Dooley K., Brown I.J.: Cisco. Receptury. Helion, Gliwice, 2004.
4. Sedayao J.: Cisco IOS. Listy dostępu. RM, Warszawa 2001.
5. Dokumentacja techniczna *Cisco* (dostępna w laboratorium na CD-ROM oraz w witrynie www.cisco.com)