

**Kontrola ruchu TCP/IP poprzez
złożone i kontekstowe listy dostępowe (ACL)**

Numer ćwiczenia: 3

Laboratorium z przedmiotu:
Zarządzanie i bezpieczeństwo w sieciach teleinformatycznych

Kod przedmiotu: TS1D6220

Instrukcję opracował:
dr inż. Andrzej Zankiewicz

1. Ogólna charakterystyka list dostępowych

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 umożliwia 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:

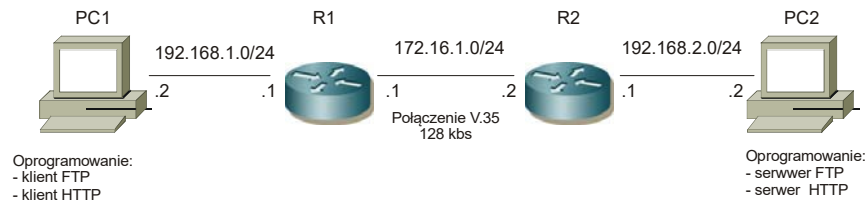
- Ustalenie priorytetów i kolejowania ruchu na interfejsach routera. Procesy te pozwalają wskazać kolejność przetwarzania pakietów na poszczególnych interfejsach oraz umożliwiają zrównoważenie ruchu w sieci.
- Ograniczenie zawartości uaktualnień tras wysyłanych przez protokoły routingu dynamicznego. 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 dostępowe mogą być podzielone na następujące grupy:

- listy standardowe – filtrują tylko na podstawie źródłowych adresów IP;
- listy rozszerzone – w regułach filtracji mogą uwzględniać źródłowe i docelowe adresy IP, źródłowe i docelowe numery portów TCP, flagi (znaczniki TCP), protokoły (np. ip, tcp, udp, icmp);
- listy złożone:
 - o dynamiczne listy ACL – pozwalają na dynamiczne uaktywnienie zdefiniowanej wcześniej reguły listy po pomyślnym uwierzytelnieniu się użytkownika na routerze poprzez telnet lub SSH;
 - o zwrotne listy ACL – zezwalają na ruch wyjściowy, a ruch wejściowy ograniczają do odpowiedzi na sesje rozpoczęte na routerze (jest to bardziej precyzyjna forma filtracji niż listy rozszerzone z parametrem *established*);
 - o czasowe listy ACL – umożliwiają kontrolę dostępu na podstawie pory dnia i tygodnia.
- listy kontekstowe (CBAC – *Context-Based Access List*) - pozwalają na filtrację ruchu na podstawie protokołu warstwy aplikacyjnej (np. ftp) bez konieczności parametrów sieciowych tego ruchu (np. numerów portów TCP).

2. 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, FTP oraz DNS na stacji **PC2** oraz odwrotnie.
8. Skonfigurować w **R2** kontekstową listę dostępu (CBAC) pozwalającą na nawiązywanie FTP do stacji **PC2**. Sprawdzić poprawność pracy ustawionej listy (także poprzez analizę liczby „trafień” danej listy) zarówno w przypadku FTP pasywnego jak i aktywnego. W poszczególnych próbach nawiązywania połączeń zwrócić uwagę jakie numery portów TCP są wykorzystywane. Na czym polega problem ze zbudowaniem analogicznej listy bez wykorzystania CBAC?
9. Zbudować w **R1** zwrótną listę dostępową pozwalającą na korzystanie przez **PC1** z usługi serwera DNS pracującej na stacji **PC2**. Zaproponować listę ACL realizującą zbliżoną funkcjonalność, ale bez wykorzystania listy zwrótniej. Na czym polega korzyść z wykorzystania w tym przypadku listy zwrótniej?
10. Skonfigurować na **R1** dynamiczną listę dostępu pozwalającą na dostęp do usługi WWW na PC2 tylko dla użytkowników, którzy poprawnie uwierzytelniają się poprzez *telnet* na routerze **R1**.

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.

3. Literatura

1. Józefiak A.: CCNA 200-125. Zostań administratorem sieci komputerowych Cisco. Helion, Gliwice, 2017.
2. Graziani R., Vachon B.: Akademia sieci Cisco. CCNA Exploration. Semestr 4. Sieci WAN – zasady dostępu. Wydawnictwo PWN-MIKOM, Warszawa 2009.
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 oraz w witrynie www.cisco.com)