ROZDZIAŁ 1

WSTĘP ORAZ PODSTAWY TEORETYCZNE

1 Wstęp oraz podstawy teoretyczne

Książka wraz z ćwiczeniami i zadaniami są przeznaczone dla średnio zaawansowanych oraz zaawansowanych użytkowników programu PT.

Chcąc ułatwić naukę i poznawanie podstawowych możliwościami konfigurowania blokad ruchu w sieci za po mocą urządzeń Cisco, autorzy przygotowali ćwiczenia oraz zadania kontrolne, wspomagające proces nauczania w zakresie filtrowania ruchu sieciowego.

Przygotowane opisy oraz ćwiczenia zostały przygotowane w oparciu o wersję programu **Packet Tracer 7.2.1**, czyli aktualną wersję w trakcie przygotowania książki do wydruku. Do poprawnego otwarcia wszystkich ćwiczeń niezbędna jest wersja programu 7.2.1 lub wersja nowsza (**7.2.2** opublikowana w trakcie przygotowywania książki). Dlatego niektóre nazwy znajdujące się w książce będą miały oznaczenia **7.2.X**)

Format nazw plików. Nazwy pliku rozpoczynają się od wyrazu: **cwiczenie** lub **zadanie**.

cwiczenie<nr rozdziału>.<nr ćwiczenia>.<dodatkowy_opis>.pkt

Format nazw plików zawierających zadania kontrolne:

zadanie<nr rozdziału>. <nr zadania>.<dodatkowy_opis>.pka

Przykłady (**pliki PKT, PKA**) do ćwiczeń oraz zadań zostały opublikowane na specjalnej stronie internetowej naszego wydawnictwa, pod adresem: **http://pt8.itstart.pl**. Chcąc uzyskać pełny dostęp do plików, należy się zalogować przy pomocy

- loginu: **firewall**
- hasła: **pt8@F1R#W@LL**

Pliki zostały podzielone na dwie kategorie: **Ćwiczenia** i **Zadania,** znajdują się w następujących podkatalogach:

- **cwiczenia**
- **zadania**

W podkatalogach zadań(**gdzie N oznacza nr zadania**) znajdują się pliki :

- **zadanieN.answer-network.pkt**
- **zadanieN.initial-network.pkt**
- **zadanieN.pka**
- **zadanieN-activity-wizard-password.txt**
- **zadanieN-config-data-for-instructors-only.txt**

Uwaga ogólna: Po wykonaniu konfiguracji urządzenia typu firewall **(np. ASA 5505, ASA 5506)** należy bezwzględnie zapisać konfigurację w pamięci NVRAM (polecenie **write memory**) a potem wykonać restart urządzenia (polecenie **reload**).

1.1 Co to jest i do czego służy firewall ?

Bardzo trudno definiować co to jest Firewall (pol. zapora sieciowa), może to być dedykowany sprzęt wraz ze specjalnym oprogramowaniem, służący do blokowania niepowołanego (niechcianego) dostępu do komputera a także bardzo złożony system działający w chmurze (w specjalizowanych serwerowniach) zajmujący się bezpieczeństwem korporacyjnych oraz prywatnych sieci.

W ujęciu ogólnym zapora sieciowa służy do zaawansowanego filtrowania oraz inspekcji ruchu sieciowego. Inspekcja ruchu sieciowego może realizować następujące funkcje:

- **Rozpoznawanie aplikacji**

  Firewall nowej generacji potrafi odróżnić logowanie do portali społecznościowych oraz przeglądanie informacji, publikowania informacji, rozmów głosowych lub czatu. Dzięki możliwościom zapór sieciowych nowej generacji można przykładowo zezwolić na przeglądanie Facebooka, przy jednoczesnym wyłączaniu wprowadzania statusów lub dodatkowych apletów (np. rozmów on-line).

  To samo dotyczy innych aplikacji społecznościowych i aplikacji webowych. Rozpoznawanie aplikacji i blokowanie niepożądanych połączeń jest przydatne również w klasycznym środowisku informatycznym, szczególnie w sieciach technologicznych wykorzystujących automatykę przemysłową.

- **Ograniczona ochrona aplikacji webowych**

  Nowoczesny firewall potrafi obronić firmowe oprogramowanie z interfejsem webowym przed atakami wstrzyknięcia kodu, nadużyć interfejsów API, a także aplikacyjnych ataków DDoS. W ten sposób można wprowadzić ograniczenia na parametry, które znajdują się w wywołaniach aplikacji i zablokowaćograniczoną możliwość nadużyć. Metoda ta bardzo dobrze nadaje się również do tymczasowego zablokowania pewnej ograniczonej podatności aplikacji oraz do usunięcia luk w bezpieczeństwie.

- **Rozpoznawanie tożsamości**

  W epoce rosnącej roli ruchu człowiek-maszyna szczególnego znaczenia nabiera możliwość odróżnienia aktywności zalogowanych użytkowników. Autoryzacja użytkowników za pomocą systemów uwierzytelnienia umożliwia odróżnienie złośliwego oprogramowania działającego przed zalogowaniem od danego rzeczywistego użytkownika.

- **Ochrona przed nieznanym złośliwym kodem**

  Ataki tego typu są prowadzone przy użyciu złośliwego oprogramowania, które charakteryzuje się dużą zmiennością. Włamywacze testują wykrywanie kodu przez najważniejsze narzędzia antywirusowe i potrafią wdrożyć techniki jego omijania. W praktyce oznacza to, że oprogramowanie antywirusowe ma ograniczoną skuteczność przy ochronie przed nieznanym złośliwym kodem.

  Nowoczesne firewalle potrafią przechwycić przesyłany plik i poddać go analizie w kontrolowanym środowisku piaskownicy (tzw. **sandbox**). Aktywność uruchomionego w badanym środowisku pliku jest analizowana po to, by wykryć złośliwe programy nie na podstawie samego kodu, ale na podstawie jego zachowania w testowym środowisku.

- **Rozpoznawanie wykorzystania podatności**

  Napastnicy w atakach wykorzystują wielką różnorodność złośliwego oprogramowania, na przykład tzw. **eksploitów**, czyli fragmentów kodu odpowiedzialnych za przełamanie zabezpieczeń. Jeśli zapora sieciowa zawiera moduł detekcji wykorzystania podatności, to może wykryć próby ataków.

- **Obrona przed atakami odmowy obsługi po stronie Data Center**

  Atak odmowy obsługi może mieć różne formy – np. ataki, które polegają na zalewie żądań i blokowaniu łącza. O wiele mniejszy ruch wywołują tak zwane ataki powolne DDoS, w których serwis jest obciążany wieloma wolnymi połączeniami zajmującymi zasoby. Groźne są również ataki wykorzystujące słabość aplikacji internetowych. Ataki wolumetryczne można blokować po stronie operatora, ale nadal trzeba blokować połączenia, które są atakiem DDoS albo przeszły niezauważone przez proces filtrowania prowadzony przez operatora chmurowego.

1.2 Co to jest zapora sieciowa?

Zapora sieciowato obecnie połączenie ochrony sprzętowej i programowej połączenia sieci wewnętrznej LAN w celu ochrony przed nieuprawnionym dostępem z zewnątrz, tzn. sieci publicznych (WAN, Internet).

Zapora sieciowa to także w ujęciu bardzo wąskim, oprogramowanie używane do utrzymywania bezpieczeństwa sieci prywatnej. Zapory sieciowe blokują nieautoryzowany dostęp do lub z sieci prywatnych i są często stosowane w celu uniemożliwienia nieautoryzowanym użytkownikom sieci lub nielegalnemu oprogramowaniu uzyskania dostępu do sieci prywatnych podłączonych do Internetu.

Zapora sieciowa może być zaimplementowana za pomocą sprzętu, oprogramowania lub kombinacji obu powyższych.

1.3 Rodzaje filtrowania ruchu sieciowego

Wyróżniamy podstawowe rodzaje filtrowania ruchu sieciowego:

- **Packet filtering**
  Filtrowanie polega na sprawdzaniu danych przesyłanych w pakietach, czyli skąd przychodzi i dokąd powinien być wysłany pakiet. Na podstawie reguł niektóre pakiety są odrzucane lub przesyłane. Wszystkie Firewalle potrafią to zrobić i odbywa się to w warstwie sieci.

- **Statefulpacketinspection**
  Pakiet może być początkiem nowego połączenia lub może być częścią istniejącego połączenia. Jeśli nie jest jednym z nich, prawdopodobnie jest bezużyteczny i można go usunąć.

- **Application-layer**

  Zapory warstwy aplikacji mogą sprawdzać faktyczne transportowane dane. Wiedzą, jak działają niektóre protokoły, na przykład FTP lub HTTP. Następnie mogą sprawdzić, czy dane znajdujące się w pakiecie są prawidłowe (dla tego protokołu). Jeśli nie, to usuwają je.

1.4 Rodzaje zapór sieciowych

Wyróżniamy podstawowe rodzaje zapór sieciowych, czylifirewalli to między innymi:

- **Firewalleprogramowe**: często są uruchamiane jako dodatkowe programy na komputerach używanych do innych celów. Są one często nazywane osobistymi zaporami sieciowymi, które mogą być aktualizacjami na komputerach osobistych.
- **Firewallesprzętowe**: zapory sprzętowe wykonane na bazie sprzętu. Działają na dedykowanym komputerze (lub urządzeniu). Często oferują one lepszą wydajność niż zapory programowe, ale są również droższe.
- **Firewallesprzętowo-programowe**: najnowocześniejsze zapory sprzętowe działają w oparciu o bazę sprzętową oraz specjalne aplikacje w chmurze. Działają na dedykowanym komputerze (lub urządzeniu). Często oferują one lepszą wydajność niż zapory programowe, ale są najdroższe.

Obecne nowoczesnefirewalle(ang. NextGeneration Firewall)potrafią:

- Uruchamiać aplikacje antywirusowe (Anti-virus profile)
- Sprawdzaćpodatnościna ataki (Vulnerability profile)
- Sprawdzać ataki szpiegowskie (Anti-spyware profile)
- Blokować pliki (File-blocking)
- Filtrować adresy URL (URL-Filtering)
- Zabezpieczać przed atakami DoS (ProtectagainstDenial of Service)

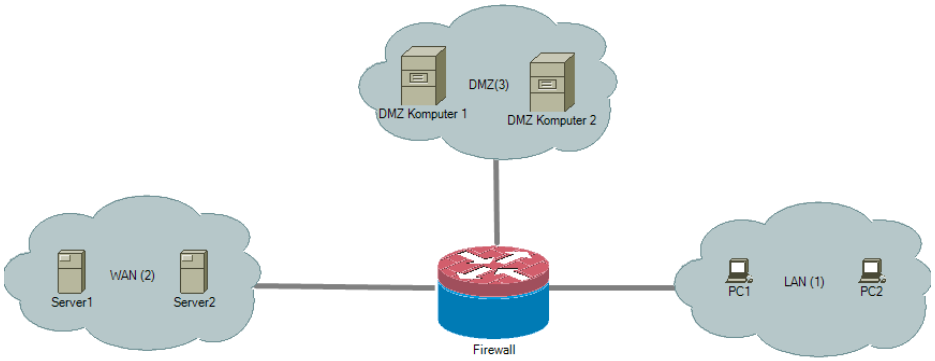
1.5 Strefa (sieć) zdemilitaryzowana DMZ

Co to jest strefa lub sieć zdemilitaryzowana?

DMZ to strefa, gdzie umieszczamy serwery, do których dostęp będą mieli użytkownicy, którym(w stopniu ograniczonym) nie do końca powinniśmy ufać. Poprzez izolację serwera w DMZ, możemy ukryć lub zablokować dostęp do reszty naszej sieci.

Przykład, w którym dane można przesyłać w następujących kierunkach:

- dopodsieciwewnętrznej 1 (**LAN**)
- do podsieci zewnętrznej 2 (**WAN**)
- do podsieci zewnętrznej 3 (**DMZ**)



Rysunek 1.1. Strefy sieciowe: 1- sieć LAN,2 - sieć WAN,3 - sieć DMZ

W Firewallu należy zdecydować (skonfigurować),rozpoznać rodzaj ruchu sieciowego, skąd pochodzi i dokąd ma być przekazany (cel ruchu) oraz jak ma zostać przekazany.

1.6 Poziomy zaufania

W firewallach ASA wyróżniamy następujące poziomy zaufania (poziomy bezpieczeństwa) (**ang.*security level***):

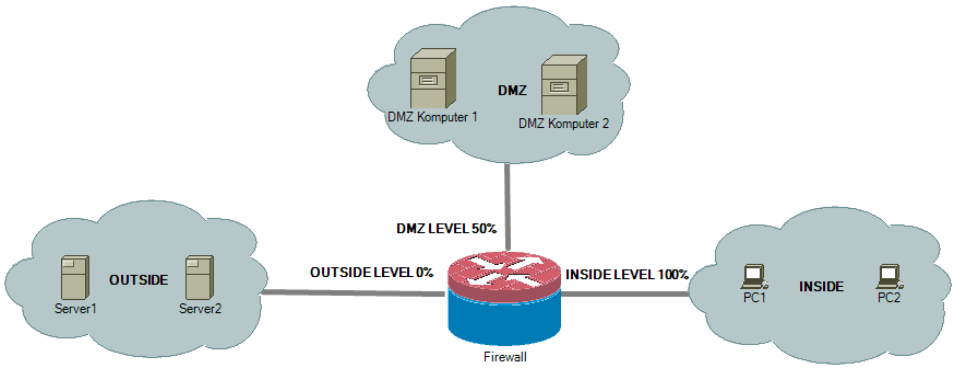
- **Security level 0** – najniższy poziom zaufania w ASA i domyślnie jest przypisany do interfejsu zewnętrznego. Jest on używany zazwyczaj dla sieci WAN. Ruch z zewnątrz nie będzie dostarczany do wewnętrznych interfejsów. Filtrowanie ruchu jest możliwe za pomocą ACL.
- **Security level od 1 do 99** –pośredni poziom zaufania w ASA, np. 50 oznacza, że ruch zostanie dopuszczony z poziomu 100 do poziomu 50 (ale nie odwrotnie), a także z poziomu 50 do poziomu 0(ale nie odwrotnie).

- **Security level 100** – najwyższy poziomzaufania w ASA i domyślnie jest przypisany do interfejsu wewnętrznego. Jest on używany zazwyczaj dla sieci LAN. Ruch z wewnątrz będzie dostarczany do wszystkich innych interfejsów.

1.7 Strefy podsieci oraz domyślne poziomy zaufania

W firewallach ASA wyróżniamy następujące trzy podstawowe strefy (podsieci):

- **inside** – Strefa wewnętrzna (sieć wewnętrzna) mająca domyślny poziom zaufania 100
- **outside** – Strefa zewnętrzna (sieć zewnętrzna) mająca domyślny poziom zaufania 0
- **dmz** – Strefa DMZ (sieć zdemilitaryzowana) mająca domyślny poziom zaufania 50

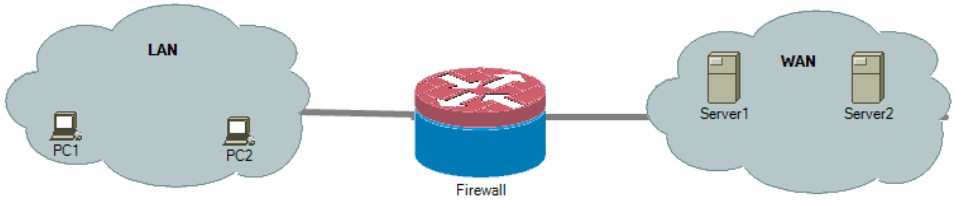


Rysunek 1.2. Strefy sieciowe: DMZ, OUTSIDE, INSIDE

1.8 Rodzaje topologii zabezpieczeń

Wyróżniamy trzy podstawowe rodzaje topologii:

1.8.1 TOPOLOGIA LAN-WAN

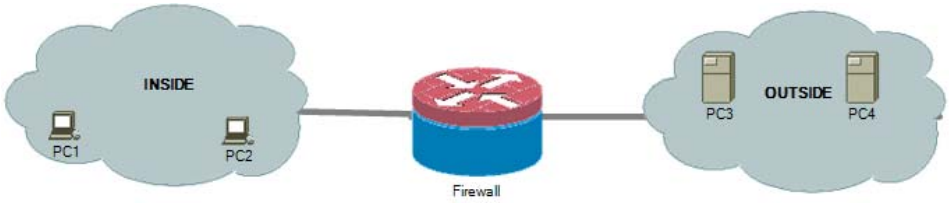


Rysunek 1.3. Rodzaje topologii: LAN-WAN

Założenia:

- Firewall rozdziela sieci zaufaną (LAN) od sieci niezaufanej (WAN).
- Firewall chroni sieć LAN przed dostępem z sieci WAN.

1.8.2 TOPOLOGIA INSIDE-OUTSIDE

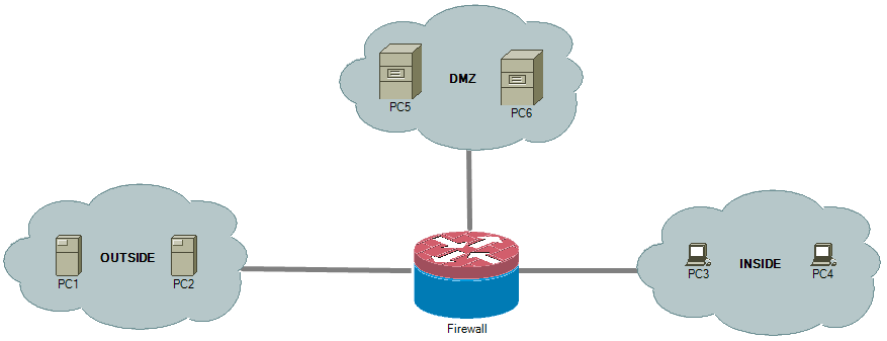


Rysunek 1.4. Rodzaje topologii: INSIDE-OUTSIDE

Założenia:

- Sieć INSIDE znajduje się w strefie o najwyższym poziomie zaufania.
- Sieć OUTSIDE znajduje się w strefie o najniższym poziomie zaufania.
- Ruch z strefy o najwyższym poziomie zaufania do strefy o wyższym poziomie(**INSIDE TO OUTSIDE**) zaufania,**nie jest blokowany i jest kontrolowany**.
- Ruch z strefy o najniższym poziomie zaufania do strefy o wyższym poziomie(**OUTSIDE TO INSIDE**) zaufania **jestblokowanyijest kontrolowany**.
- Ruch w strefie INSIDE jest **dozwolony**.

1.8.3 TOPOLOGIA OUTSIDE-DMZ-INSIDE



Rysunek 1.5. Rodzaje topologii: INSIDE-DMZ-OUTSIDE

Założenia:

- Sieć (strefa) **DMZ** ma poziom zaufania pomiędzy poziomem strefy INSIDE i OUTSIDE
- Ruch z strefy o najwyższym poziomie zaufania (100) do strefy o niższym poziomie(0) (**INSIDE TO OUTSIDE**) zaufania **nie jest blokowany i jest kontrolowany**.
- Ruch z strefy o najniższym poziomie zaufania (0) do strefy o wyższym poziomie (100)(**OUTSIDE TO INSIDE**) zaufania **jestblokowanyijest kontrolowany**.
- Ruch ze strefy o wyższym poziomie (100) do strefy DMZ (50) poziomie **jest dozwolony i kontrolowany**.
- Ruch ze strefy o niższym poziomie (0) do strefy DMZ (50) poziomie **jest niedozwolony i kontrolowany**.