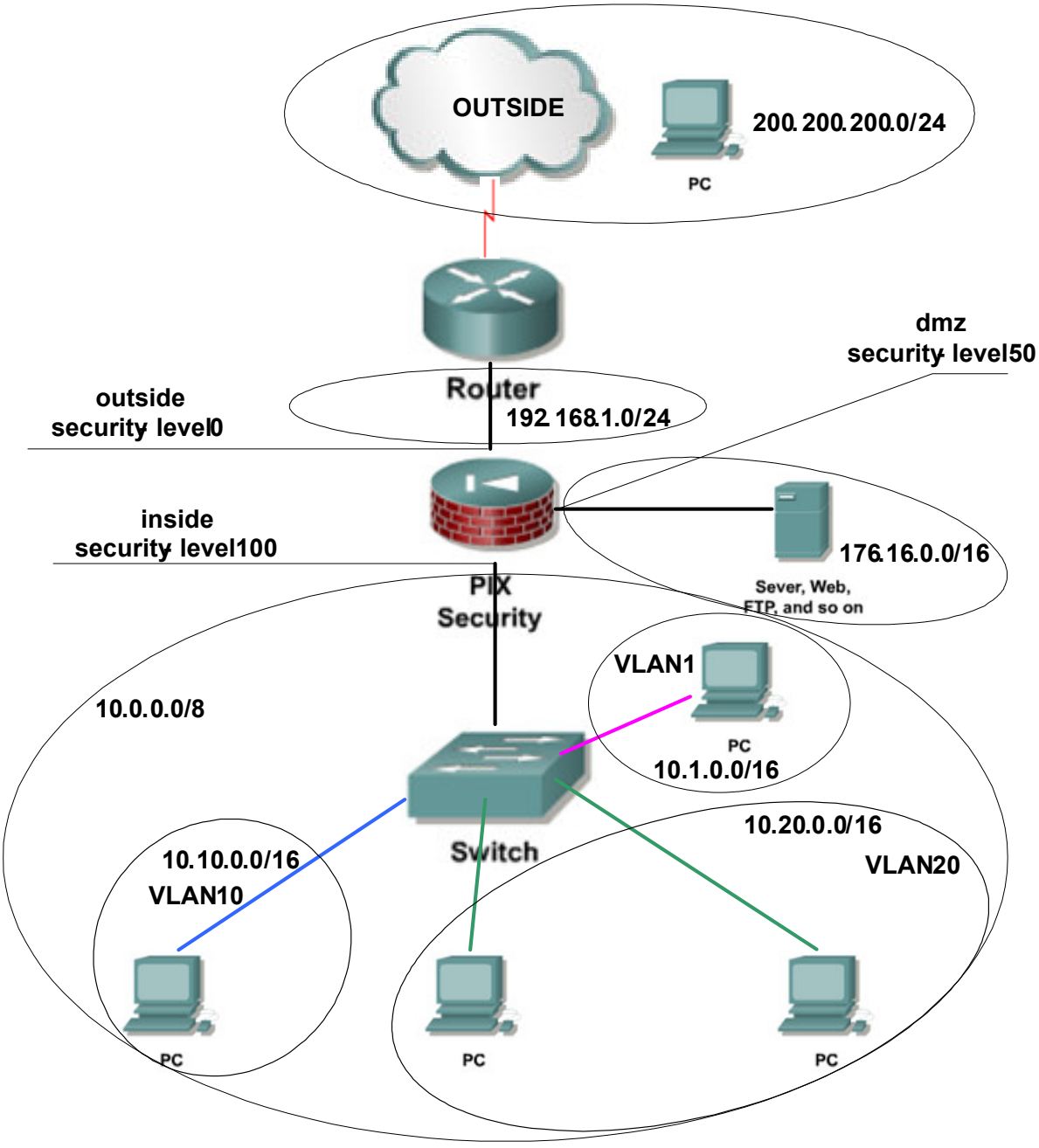
Filtrowanie pakietów, Statyczna translacja adresów

Schemat sieci



Filtrowanie pakietów

Filtrowanie pakietów (lista dostępu - *access list*)

Definicja listy dostępu (adres źródła, adres celu):

PIX(config)# access-list 101 extended permit tcp any 176.16.0.0 255.255.0.0 eq ftp

PIX(config)# access-list 101 extended permit tcp any any eq www

PIX(config)# access-list 101 extended deny ip any any

Dodanie listy dostępu do interfejsu (na ruch wchodzący do interfejsu):

PIX(config)# access-group 101 in interface inside-PRAC

Ruch pakietów ICMP przez PIX

Domyślnie ping przez PIX jest zabroniony.

Przepuszczenie komunikatu „echo reply" przez interfejs „outside" PIX:

PIX(config)# access-list 102 extended permit icmp any any echo-reply

PIX(config)# access-group 102 in interface outside

Przepuszczenie komunikatu „echo" i „echo reply" przez interfejs „dmz" PIX:

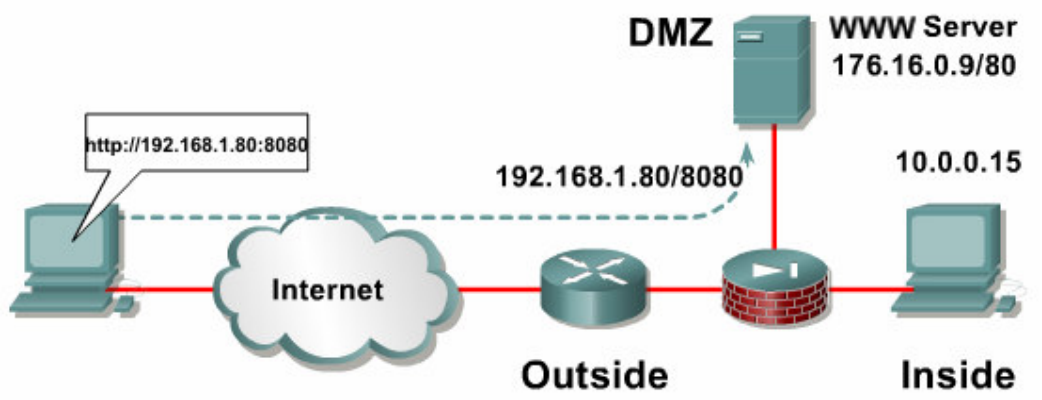
PIX(config)# access-list 103 extended permit icmp any any echo

PIX(config)# access-list 103 extended permit icmp any any echo-reply

PIX(config)# access-group 103 in interface dmz

Statyczna translacja adresów

Statyczna translacja adresów z przekierowaniem portów



Statyczny NAT + przekierowanie portów:

(adres celu, po zmianie adresu celu):

PIX(config)# static (dmz,outside) tcp 192.168.1.80 8080 176.16.0.9 80 netmask 255.255.255.255

Aby możliwa była komunikacja z interfejsu o mniejszym poziomie bezpieczeństwa do interfejsu o wyższym poziomie bezpieczeństwa należy dodać odpowiednią *access-list*:

PIX(config)# access-list 102 extended permit tcp any host 192.168.1.80 eq 8080

PIX(config)# access-group 102 in interface outside

Imiona i Nazwiska:

…….

…….

…….

…….

…….

Czynności wstępne:

01. Przywrócić połączenia urządzeń.
02. Usunąć zapisane konfiguracje na urządzeniach (switch, router, pix).
03. Przywrócić konfiguracje urządzeń (switch, router, pix) z serwera TFTP.
04. Zainstalować serwery **www** i **ftp** na hostach w sieciach „dmz" i „outside" .

Uwaga: strona na serwerze **www** w sieci „outside" i „dmz" powinny się różnić.

05. Przeprowadzić testy:
    - Połączenie z sieci „inside-PRACOWNICY" do serwera **www** i **ftp** w strefie „dmz" ……..
    - Połączenie z sieci „inside-PRACOWNICY" do serwera **www** i **ftp** w strefie „outside" ……
    - Połączenie z sieci „inside-DYREKCJA" do serwera **www** i **ftp** w strefie „dmz" ……..
    - Połączenie z sieci „inside-DYREKCJA" do serwera **www** i **ftp** w strefie „outside" ……..
    - Połączenie z sieci „dmz" do serwera **www** i **ftp** w strefie „outside" ……..
    - Połączenie z sieci „outside" do serwera **www** i **ftp** w strefie „dmz" ……..

authentication-proxy

(korekta w związku ze zmianami w strukturze sieci):

01. Poprawić autoryzację użytkowników na pix tak aby:
    - wszystkie połączenia z sieci „inside-PRACOWNICY" wymagały autoryzacji,
    - wszystkie połączenia z sieci „inside-DYREKCJA" jej nie wymagały.
02. Przeprowadzić testy:
    - Usunąć wszystkich autoryzowanych użytkowników (**clear uauth**).
    - Czy przy połączeniu z sieci „inside-PRACOWNICY" do serwera **www** lub **ftp** w sieci „outside" wymagana jest autoryzacja? ……
    - Czy przy połączeniu z sieci „inside-DYREKCJA" do serwera **www** lub **ftp** w sieci „outside" wymagana jest autoryzacja? ……

Filtracja pakietów:

01. Dodać filtrację pakietów (listy dostępu) tak aby:
    - Z sieci „inside-PRACOWNICY” był możliwy dostęp do dowolnego serwera **ftp** w sieci „dmz”
    - Z sieci „inside-PRACOWNICY” był możliwy dostęp do dowolnego serwera **www** w dowolnej sieci.
    - Pozostałe połączenia z sieci „inside-PRACOWNICY” zabronione.
02. Przeprowadzić testy:
    - Połączenie z sieci „inside-PRACOWNICY” do serwera **www** w strefie „dmz” ……..
    - Połączenie z sieci „inside-PRACOWNICY” do serwera **ftp** w strefie „dmz” ……..
    - Połączenie z sieci „inside-PRACOWNICY” do serwera **www** w strefie „outside” ……
    - Połączenie z sieci „inside-PRACOWNICY” do serwera **ftp** w strefie „outside” ……

Ruch pakietów ICMP przez PIX

01. Otworzyć ruch dla komunikatu „echo reply” przez interfejs „outside” PIX.
02. Otworzyć ruch dla komunikatu „echo” i „echo reply” przez interfejs „dmz” PIX.
03. Przeprowadzić testy:
    - Ping z hosta z sieci „inside-PRACOWNICY” do hosta z sieci „outside” …….
    - Ping z hosta z sieci „inside-DYREKCJA” do hosta z sieci „outside” …….
    - Ping z hosta z sieci „inside-PRACOWNICY” do hosta z sieci „dmz” …….
    - Ping z hosta z sieci „inside-DYREKCJA” do hosta z sieci „dmz” …….
    - Ping z hosta z sieci „dmz” do hosta z sieci „outside” …….

Statyczny NAT + przekierowanie portów:

01. Dodać statyczny NAT z przekierowaniem portów tak aby było możliwe połączenie z sieci „outside” do serwera **www** w sieci „dmz”.
02. Przeprowadzić testy:
    - Połączenie z sieci „dmz” do serwera **www** w strefie „outside” ……..
    - Połączenie z sieci „dmz” do serwera **ftp** w strefie „outside” ……..
    - Połączenie z sieci „outside” do serwera **www** w strefie „dmz” ……..
    - Połączenie z sieci „outside” do serwera **ftp** w strefie „dmz” ……..

Czynności końcowe:

01. Zapisać konfiguracje urządzeń na serwerze TFTP.

02. Usunąć konfiguracje urządzeń.