**ZADANIE A: Podstawowa konfiguracja interfejsów Cisco Firewall**

NUMER INSTRUKCJI   
(WEDŁUG LAB ROADMAP)

**043**

1. Router **Cisco PIX 515E Firewall**, łącząc go okablowaniem RJ45 w **układzie PC-firewall-PC.**

2. Należy połączyć kabel konsoli **DB9-RJ45** do odpowiedniego gniazda w ruterze i PC. Parametry połączenia konsoli dla urządzeń Cisco: 9600 kbps, 8 bitów danych, brak kontroli parzystości, 1 bit stopu, brak sterowania przepływem

3. Uruchomić ruter wcześniej nawiązując połączenie (**HyperTerminal**). Czynności związane z konfigurowaniem PIX Firewall (System Cisco IOS) są bardzo podobne do prac ze zwykłymi ruterami modularnymi Cisco.

4. Po uzyskaniu karetki należy zaktywować tryb uprzywilejowany- komenda **enable** lub **en**. Poprawne przejście zasygnalizuje symbol ‘**#**’.

5. Następnie należy przejść do trybu konfiguracji: *configure terminal lub conf t*

6. Należy wybrać interfejs do konfiguracji. Firewall posiada dwa interfejsy Fast Ethernet o symbolach **eth 0** (przeznaczony domyślnie dla **sieci publicznej**) i **eth 1** (przeznaczony domyślnie dla **chronionej sieci prywatnej**). Dla obydwu interfejsów należy zdefiniować IP, nazwę oraz włączyć interfejs (tu konfiguracja jest różna zależnie do wersji systemu operacyjnego):

PixFirewall(config)#interface eth 0

PixFirewall(config-if)#ip address 200.200.200.1 255.255.255.0

PixFirewall(config-if)#nameif outside

PixFirewall(config-if)#no shutdown

PixFirewall(config)#interface eth 1

PixFirewall(config-if)#ip address 192.168.123.150 255.255.255.0

PixFirewall(config-if)#nameif inside

PixFirewall(config-if)#no shutdown

lub:

PixFirewall(config)#ip address inside 200.200.200.1 255.255.255.0

PixFirewall(config)#ip address inside 192.168.123.150 255.255.255.0

gdzie **inside** dotyczy interfejsu **Ethernet 1**, zaś **outside** - **Ethernet 0**.

7. Należy sprawdzić zdefiniowane ustawienia: *PixFirewall#show ip int brief*

**ZADANIE B: Konfigurowanie NAT w PIX Firewall**

1. Posługując się konfiguracją z zadania A należy **włączyć NAT**: *PixFirewall(config)#nat-control*

2. Zdefiniować **pulę NAT** adresów publicznych, które ruter wykorzysta do emulacji NAT:

PixFirewall(config)#global (outside) 1 200.200.200.10-200.200.200.20 netmask 255.255.255.0

gdzie 1 to identyfikator puli adresów, a adresy IP do początek i koniec puli

3. Do tej samej puli dodać informację, o **prywatnym adresie bramki** do translacji NAT (będzie to IP rutera po stronie prywatnej):

PixFirewall(config)#nat (inside) 1 10.0.0.1 255.255.255.255

Konieczne jest posłużenie się tym samym numerem puli adresów (w przykładzie:1)

4. Określić **regułę rutowania NAT**: z dowolnego(0) adresu na dowolny(0) adres pakiety idące na zewnątrz mają być przekazywane na następną bramkę w sieci publicznej (WAN Gateway):

PixFirewall(config)#route outside 0 0 200.200.200.2

5. **Sprawdź** otrzymaną **konfigurację**:

PixFirewall(config)#show run **lub**

PixFirewall(config)#show running-config

6. Przetestuj działanie NAT używając stacji w sieci prywatnej, publicznej i analizatora przechwyconych pakietów.

**ZADANIE C:** **Definiowanie reguł filtrowania w Cisco PIX Firewall**

1. Posługując się konfiguracją z zadania B należy zdefiniować **listę ACL** podobnie jak dla zwykłego rutera Cisco:

PixFirewall(config)#access-list 100 deny tcp any any eq 23

gdzie 100 to ID nowej listy, deny (lub permit) to zezwolenie lub zakaz dołączany właśnie do listy, tcp to id protokołu, any any oznacza „z dowolnego IP na dowolny IP” (można zamienić na coś konkretnego), zaś eq 23 oznacza numer portu którego dotyczy zakaz (eq=equals, lt=less than, gt=greater than, neq=not equals).

**Zapisane listy** można sprawdzić komendą: *PixFirewall(config)#show access-lists*

2. Do listy należy dodać reguły **zezwalające na pozostały ruch** (jeżeli należy go przepuścić): PixFirewall(config)#access-list 100 permit ip any any

3. Należy **przypisać** **listę do interfejsu**. Ponieważ PIX Firewall posiada tylko dwa interfejsy list nie przypisuje się w trybie edycji konkretnego interfejsu. Zamiast tego określa się nazwę interfejsu w parametrze komendy: PixFirewall(config)# access-group 100 in interface outside

4. Sprawdź poprawność funkcjonowania filtra pakietów. Zdefiniuj inny filtr według własnego pomysłu.

5. Posługując się konfiguracją z zadania B należy zdefiniować **regułę przekierowania ruchu z zewnątrz** skierowanego na publiczny interfejs rutera 200.200.200.11 i port tcp 4444 do hosta 10.0.0.3 na port ftp: PixFirewall(config)#static (inside,outside) tcp 200.200.200.11 4444 10.0.0.3 ftp netmask 255.255.255.255

Taka reguła umożliwi udostępnienie na zewnątrz usług realizowanych w sieci prywatnej.

**Uwaga**: w nawiasie (inside,outside) nie można postawić znaków spacji (' ')

**Zadanie D: Uruchomienie Cisco ASDM**

**Cisco ASDM** (Security Appliance Device Manager) to **graficzne** **oprogramowanie** służące do zarządzania zabezpieczeniami firewall (PIX i ASA) przez HTTPS.

Po zainstalowaniu pakietu w PIX interfejs graficzny jest serwowany automatycznie w momencie użycia usługi HTTPS PIX. Odbywa się to na dwa sposoby:

* jako aplet Java
* jako aplikacja Java

Warunkiem poprawnego funkcjonowania ASDM w przeglądarce WWW jest posiadanie JRE w wersji nie nowszej niż 1.4 (kompatybilnej z ASDM w wersji 7.0). Trzeba zatem użyć odpowiedniej wersji Java.

**Sprawdzenie** **wersji** ASDM: *PixFirewall#show version*

W drugim przypadku należy zapisać instalator aplikacji na dysku (zostanie pobrany z PIX) i zainstalować ją. W celu uruchomienia ASDM bez użycia pakietu instalacji typu RPG czy MSI należy umieścić w wybranym katalogu 3 pliki pobrane z PIX lub z Internetu:

* asdm\_launcher.jar;
* jploader.jar;
* lzma.jar

Następnie należy uruchomić ASDM z linii komend (zakładając poprawność funkcjonowania ścieżki do jre):

java -D sun.swing.enableImprovedDragGesture=true -Xmx256m -Xms64m -classpath asdm\_launcher.jar;jploader.jar;lzma.jar com.cisco.launcher.Launcher

Przeprowadź szczegółową analizę wszelkiej funkcjonalności udostępnianej przez Cisco ASDM. Wykonaj czynności konfiguracyjne z wcześniejszych zadań przy użyciu ASDM.