Cisco PIX. Firewalle

Autor: zepół autorów
Tłumaczenie: Adam Jarczyk
ISBN: 83-246-0187-2
Tytuł oryginału: Cisco PIX Firewalls: Configure, Manage, Troubleshoot
Format: B5, stron: 544

Kompendium wiedzy na temat zapór sieciowych PIX

- Tworzenie różnych kontekstów zabezpieczeń
- Nowe możliwości Cisco PIX Security Appliance Software w wersji 7.0
- Reagowanie na ataki i ochrona przed nimi

Współczesne społeczeństwo jest w dużym stopniu zależne od komunikacji elektronicznej. Bezpieczeństwu informacji krążących w sieci poświęca się coraz więcej uwagi. Najcenniejszymi dobrami przedsiębiorstw stały się informacje zapisane na dyskach twardych. Dane te mają często ogromną wartość i poufny charakter, zatem rosną nakłady na ich ochronę. Stworzenie skutecznej polityki bezpieczeństwa danych to już nie kaprys i snobizm, lecz konieczność. Jednak nawet najlepsze zasady są niewiele warte bez zapór sieciowych.

Książka „Cisco PIX. Firewalle" zawiera wyczerpujące informacje na temat najnowszej serii zapór sieciowych firmy Cisco opartych na systemie operacyjnym PIX w wersji 7.0. W przejrzysty sposób opisuje funkcję dostępu zdalnego, metody wykorzystywania wirtualnych sieci prywatnych oraz sposoby rozszerzania zasięgu sieci korporacyjnej na pracowników zdalnych, oddziały znajdujące się w innych miastach, partnerów, dostawców i klientów firmy. Znajdziesz w niej także szczegółowy opis wszystkich ulepszeń dodanych do wersji 7.0, takich jak interfejsy oparte na wirtualnych sieciach lokalnych (VLAN), dynamiczny routing OSPF przez VPN, proxy uwierzytelniania HTTPS, obsługa kart przyspieszających VPN (VAC+) i obsługa serwera DHCP na więcej niż jednym interfejsie.

- Typy zapór sieciowych
- Zasada działania zapory sieciowej
- Opisy firewalli z serii CiscoPIX
- Obsługa poprzez interfejs konfiguracyjny
- Instalacja i korzystanie z ASDM
- Wykrywanie włamań
- Konfiguracja usług firewalli CiscoPIX
- Zarządzanie zaporą sieciową PIX
- Konfiguracja mechanizmów VPN
- Monitorowanie wydajności firewalla

Zabezpiecz sieć, stosując najlepsze narzędzia

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Rozdział 3.

Działanie zapory sieciowej PIX

W tym rozdziale:

- Konteksty bezpieczeństwa
- Absolutne minimum: ruch wychodzący
- Otwarcie dostępu do sieci z zewnątrz
- Wyjściowe ACL (nowe)
- Czasowe ACL (nowe)
- Kontrola NAT (nowe)
- Omijanie NAT
- Policy NAT
- Grupowanie obiektów
- Podsumowanie
- Rozwiązania w skrócie
- Pytania i odpowiedzi

Wprowadzenie

Po wyciągnięciu zapory sieciowej PIX z pudełka, podłączeniu, uruchomieniu i skonfigurowaniu podstawowych parametrów systemu, większość administratorów zajmujących się zabezpieczeniami najpierw konfiguruje odpowiednie przepuszczanie ruchu (tzn. zgodne z zasadami bezpieczeństwa firmy). Zapora sieciowa blokująca cały ruch jak popadnie nie służy niczemu. Aby odpowiednio zabezpieczała sieć, musi filtrować

ruch w obu kierunkach, przychodzący i wychodzący. Podstawową zasadą konfiguracji zapory sieciowej jest przepuszczanie tylko pożądanego ruchu i blokowanie niechcianego. Idea prosta, lecz nie zawsze łatwa w realizacji.

Niniejszy rozdział opisuje podstawy niezbędne do przepuszczania ruchu przez zapory sieciowe Cisco PIX. Jedną z najważniejszych podstaw jest translacja adresów, która występuje w dwóch odmianach: statycznej i dynamicznej. Po skonfigurowaniu translacji system PIX będzie automatycznie zezwalał na wszystkie połączenia z interfejsu o wyższym poziomie bezpieczeństwa do interfejsu o niższym poziomie bezpieczeństwa i blokował wszystkie połączenia z interfejsu o niższym poziomie bezpieczeństwa do interfejsu o wyższym poziomie bezpieczeństwa. Aby bardziej szczegółowo kontrolować dostęp, można dopuszczać i blokować określone typy ruchu za pomocą list dostępu.

Decyzje o przepuszczaniu i blokowaniu określonych transmisji składają się na reguły zapory sieciowej, zwykle w formie listy dostępu. Niezależnie od tego, czy konfigurujemy reguły dla ruchu wychodzącego, czy przychodzącego, proces ogólnie wygląda tak samo:

1. Konfiguracja translacji adresów.
2. Zdefiniowanie listy dostępu i zastosowanie jej do interfejsu.

Musimy zapewnić, że użytkownicy będą mieli dostęp do wymaganych usług sieciowych przez zaporę. Musimy też zapewnić dostępność zewnętrznych usług jednej lub wielu społecznościom użytkowników. Wprawdzie proces filtrowania ruchu przychodzącego i wychodzącego wygląda tak samo, lecz szczegóły czynności się różnią.

Zapory sieciowe Cisco PIX udostępniają kilka funkcji przydatnych w zarządzaniu ruchem, w tym:

- Grupowanie obiektów, upraszczające konfigurację i utrzymanie list dostępu.
- Czasowe ACL.
- Rejestrowanie zdarzeń list dostępu.
- Włączanie i wyłączanie wpisów w ACL.
- Kontrola NAT.
- NAT dla określonych adresów źródłowych — Policy NAT.

W treści niniejszego rozdziału przedstawimy przykłady ilustrujące poszczególne polecenia. Opiszemy też złożone studium przypadku, które utrwali wprowadzone pojęcia.

Konteksty bezpieczeństwa

Czy nie przydałoby się czasem sklonować zaporę sieciową Cisco PIX? Obsłużyć w sieci dwa zupełnie odmienne zestawy zasad bezpieczeństwa, na przykład jeden dla działu finansowego (bardzo restrykcyjny), a drugi dla działu informatycznego (wszystko wolno)?

Firma Cisco posłuchała użytkowników i w wersji 7.0 zaimplementowała coś, co otrzymało nazwę **kontekstów bezpieczeństwa** (ang. *security contexts*). Każdy skonfigurowany kontekst bezpieczeństwa ma własne zasady bezpieczeństwa, interfejsy i obsługiwane funkcje. Oznacza to, że nie wszystkie funkcje zapory sieciowej są obsługiwane w kontekstach bezpieczeństwa. Do niedostępnych w przypadku więcej niż jednego kontekstu stosowanego w urządzeniu należą:

- protokoły routingu dynamicznego,
- VPN,
- multiemisje.

Gdy system PIX uruchomiony w trybie pojedynczego kontekstu jest konwertowany do trybu wielokontekstowego, we wbudowanej pamięci flash zostaje utworzony nowy plik o nazwie *admin.cfg*. Jest to domyślny kontekst bezpieczeństwa administratora. Możemy przechowywać dodatkowe konteksty w tej samej pamięci flash lub pobierać je przez system PIX z sieci z użyciem TFTP, FTP lub HTTP(S).

Przy konwersji z trybu pojedynczego kontekstu bezpieczeństwa do trybu wielu kontekstów bezpieczeństwa oryginalna konfiguracja startowa **nie** zostaje zapisana, więc podczas pracy z kontekstami bezpieczeństwa należy zawsze wykonywać kopie robocze. Uruchomiona konfiguracja jest wykorzystywana do utworzenia dwóch nowych plików kontekstów bezpieczeństwa.

Do przełączenia zapory sieciowej Cisco PIX w tryb wielu kontekstów bezpieczeństwa służy polecenie `mode`. Opcje dostępne dla tego polecenia są następujące:

```
PIX1(config)# mode ?

configure mode commands/options:
  multiple   Multiple mode; mode with security contexts
  noconfirm  Do not prompt for confirmation
  single     Single mode; mode without security contexts
PIX1(config)#
```

Przejście z trybu pojedynczego do wielokrotnego wygląda tak:

```
PIX1(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]
!!
The old running configuration file will be written to flash

The admin context configuration will be written to flash

The new running configuration f

***
*** --- SHUTDOWN NOW ---
***
```

```
*** Message to all terminals:
***
***   change mode
file was written to flash
Security context mode: multiple

Rebooting...
```

Po potwierdzeniu urządzenie Cisco PIX uruchomi się ponownie, aby włączyć nowy tryb. Możemy potwierdzić stan urządzenia poleceniem `show`:

```
PIX1# show mode
Security context mode: multiple
PIX1#
```

Aby powrócić do pojedynczego kontekstu bezpieczeństwa, trzeba skopiować oryginalną konfigurację (zrobiłeś kopię zapasową, prawda?) do pamięci flash:

```
PIX1# copy flash:old_running.cfg startup-config
```

Teraz możemy wrócić do trybu pojedynczego:

```
PIX1(config)# mode single
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
```

Absolutne minimum: ruch wychodzący

Po ukończeniu wstępnej konfiguracji podstawowym zadaniem jest dopuszczenie ruchu wychodzącego (np. z sieci wewnętrznej do zewnętrznej). Połączenia wychodzące to takie, które odbywają się z interfejsu o wyższym poziomie bezpieczeństwa (np. sieci wewnętrznej organizacji) do interfejsu o niższym poziomie bezpieczeństwa (np. sieci zewnętrznej, takiej jak Internet). Wymaga to albo skonfigurowania translacji adresów, albo jawnego wyłączenia jej. Po skonfigurowaniu translacji adresów, jeśli nie zostały zastosowane żadne listy dostępu, to domyślnie cały ruch wychodzący jest dozwolony. Jest to podstawowa funkcja Adaptive Security Algorithm (ASA) i powód, dla którego poziomy bezpieczeństwa są tak ważne. Ponieważ PIX przeprowadza inspekcje stanu, po nawiązaniu połączenia wychodzącego transmisje powrotne należące do tego połączenia są dopuszczane z interfejsu o niższym poziomie bezpieczeństwa do interfejsu o wyższym poziomie bezpieczeństwa.

Metoda szczegółowego sterowania ruchem wychodzącym opiera się na:

- Skonfigurowaniu **dynamicznej** translacji adresów.
- Zdefiniowaniu listy dostępu i zastosowaniu jej do interfejsu PIX (opcjonalnie).

W wersji 7.0 wymóg zdefiniowania zasad translacji adresów przed dopuszczeniem ruchu sieciowego z hostów wewnętrznych do zewnętrznych został wyeliminowany dzięki funkcji kontroli NAT. W nowszych konfiguracjach (np. w nowej instalacji PIX używającej systemu 7.0) reguły translacji nie są wymagane, a funkcja kontroli NAT jest automatycznie wyłączana poleceniem `no nat-control`. W konfiguracjach aktualizowanych (np. istniejąca zapora sieciowa PIX zmodernizowana do wersji 7.0) reguły translacji są wymagane, aby zachować funkcjonalność zdefiniowaną już w konfiguracji, a funkcja kontroli NAT jest automatycznie włączona poleceniem `nat-control`. Proszę zwrócić uwagę, że kontrola NAT jest czymś innym niż tożsamościowa NAT (`nat 0`). Zobacz podrozdział „Kontrola NAT".

Konfiguracja dynamicznej translacji adresów

Translacja adresów jest pierwszym wymogiem przepuszczania ruchu wychodzącego. Polega na mapowaniu przez NAT i (lub) PAT lokalnych adresów IP na globalne. Lokalne adresy IP to te, które znajdują się w sieci chronionej przez PIX (np. wewnętrznej sieci organizacji) i często należą do zakresów prywatnych adresów IP. Globalne adresy IP stosowane są w sieci, do której podłączony jest zewnętrzny interfejs PIX, i często są nimi publiczne, routowalne adresy IP. Konfiguracja translacji adresów powoduje konwersję przez PIX lokalnych adresów IP na adresy globalne poprzez odpowiednie podstawienie informacji w pakiecie. Po skonfigurowaniu NAT i (lub) PAT system PIX automatycznie pozwala na przechodzenie w zaporze sieciowej ruchu sieciowego z interfejsu o wyższym poziomie bezpieczeństwa do interfejsu o niższym poziomie bezpieczeństwa (czyli połączeń wychodzących). Oprócz tego PIX dopuszcza ruch powrotny związany z tymi połączeniami wychodzącymi.

Konfiguracja NAT/PAT jest procesem złożonym z dwóch kroków:

1. Identyfikacja za pomocą polecenia `nat` lokalnych adresów, które będą konwertowane.
2. Zdefiniowanie za pomocą polecenia `global` adresów globalnych, na które będą konwertowane adresy lokalne.

Rekordy translacji adresów są nazywane *translation slots* (*xlate*) i przechowywane są w **tablicy translacji**. Do wyświetlenia zawartości tej tablicy służy polecenie `show xlate`. Licznik czasu xlate monitoruje zawartość tablicy translacji i usuwa rekordy bezczynne od czasu dłuższego niż zdefiniowany limit czasowy. Domyślnie wartość tego limitu wynosi trzy godziny. Można go zmienić poleceniem `timeout xlate` i zweryfikować poleceniem `show running-config timeout xlate`.

Składnia polecenia `nat` wygląda następująco:

```
nat (rzeczywisty_int) numer_nat rzeczywisty_ip [maska [dns] [outside] [[tcp]
maks_poł_tcp [limit_emb] [norandomseq]]] [udp maks_poł_udp]
```

Opcje i parametry polecenia `nat`:

Parametr *rzeczywisty_int* wskazuje interfejs będący źródłem transmisji podlegających translacji. Musi być zgodny z nazwą zdefiniowaną dla interfejsu poleceniem `nameif`.

Parametr *nat_id* jest liczbą całkowitą z zakresu od 0 do 65 535, która tworzy mapowanie pomiędzy lokalnym adresem IP (*rzeczywisty_ip*), zidentyfikowanym przez polecenie `nat`, oraz globalnym adresem IP wskazanym przez polecenie `global`. Identyfikator 0 jest specjalny i służy do oznaczenia, że nie chcemy translacji wskazanych adresów lokalnych: adresy lokalne i globalne są takie same.

Parametr *maska* w połączeniu z *rzeczywisty_ip* służy do wskazania adresów IP przeznaczonych do translacji. Użycie opcjonalnego słowa kluczowego `dns` powoduje translację adresów zawartych w odpowiedziach DNS przy użyciu aktywnych wpisów w tablicy translacji. Opcjonalne słowo kluczowe `outside` pozwala na translację adresów zewnętrznych.

Opcjonalne słowo kluczowe `tcp` pozwala skonfigurować kilka parametrów związanych z TCP. Parametr *maks_poł_tcp* definiuje maksymalną dopuszczalną liczbę równoczesnych aktywnych połączeń TCP, natomiast *limit_emb* wskazuje, ile równoczesnych połączeń półotwartych TCP jest dozwolonych. Dla obu wartość domyślna wynosi 0, co oznacza nieograniczoną liczbę połączeń. Zbyt wiele takich połączeń może być wynikiem ataku DoS, którego skutki może zminimalizować wartość *limit_emb*.

Domyślnie podczas translacji adresów zapora sieciowa PIX generuje też losowe numery sekwencyjne segmentów TCP. Użycie opcjonalnego słowa kluczowego `norandomseq` wyłącza tę funkcję, co może być przydatne (a nawet niezbędne) przy dwukrotnej translacji adresów (np. gdy na trasie komunikacji stosowane są dwie zapory sieciowe), gdzie wielokrotne losowanie numeru nie jest pożądane.

Opcjonalne słowo kluczowe `udp` konfiguruje związany z UDP parametr *max_poł_udp*, który definiuje maksymalną dozwoloną liczbę równoczesnych aktywnych „połączeń" UDP.

> Z uwagi na bezstanowy charakter protokołu nie istnieje coś takiego jak „połączenie" UDP. Zapora sieciowa PIX jest stanowa i może zezwalać na ruch powrotny w odpowiedzi na datagram UDP. Bezstanowa natura UDP jest też powodem, dla którego nie istnieje parametr *limit_emb* dla słowa kluczowego `udp`, jak dla słowa kluczowego `tcp`. W UDP nie istnieją połączenia półotwarte.

Po wskazaniu poleceniem `nat` lokalnych adresów, które mają podlegać translacji, musimy zdefiniować adresy globalne, na które te adresy lokalne będą konwertowane. Do tego celu służy polecenie `global`:

```
global (mapowany_int) nat_id {mapowany_ip [-mapowany_ip] [netmask
mapowana_maska]}|interface
```

Parametr *mapowany_int* definiuje interfejs wyjściowy dla ruchu wychodzącego.

Parametr *nat_id* kojarzy jedną lub więcej instrukcji `nat` z instrukcją `global`.

Parametr *mapowany_ip* definiuje globalne adresy IP przeznaczone do translacji. Jeśli podamy tylko jeden adres IP, przeprowadzana będzie translacja portów i adresów (PAT). Jeśli wskażemy zakres adresów (przez - *mapowany_ip*), będzie używana translacja NAT,

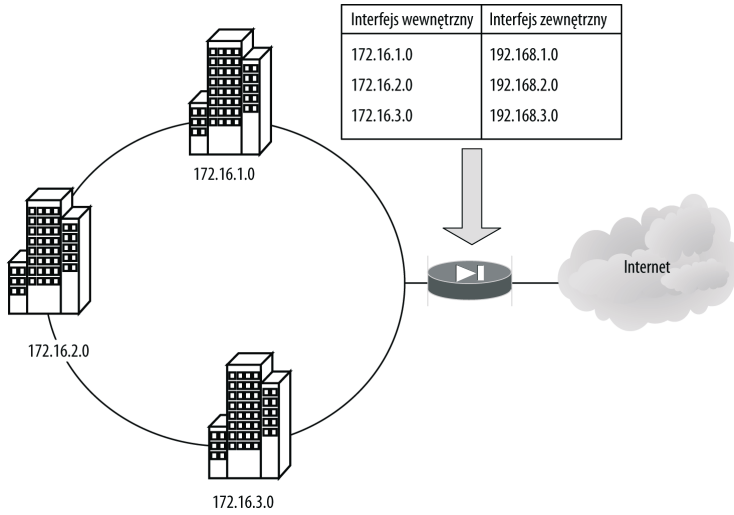
dopóki będą dostępne adresy globalne. Po wyczerpaniu tej puli przeprowadzana będzie translacja PAT.

Słowo kluczowe `netmask` jest kojarzone z zakresem *`mapowany_ip`* w celu zdefiniowania maski podsieci. Wskazuje ona zakres poprawnych adresów globalnych, których może używać PIX, i zapewnia, że urządzenie nie będzie do translacji używać adresów rozgłoszeniowych ani adresów sieci.

Jeśli globalny adres IP, który ma zostać użyty, jest przypisany do interfejsu (np. interfejsu zewnętrznego PIX), można go wskazać słowem kluczowym `interface` zamiast parametru *`mapowany_ip`*.

Użycie poleceń `nat` i `global` możemy zilustrować na przykładzie fikcyjnej organizacji. Nasza zmyślona firma Secure Corporation musi połączyć siecią trzy lokalizacje i zapewnić swoim pracownikom dostęp do Internetu. Firma nie ma własnych publicznych adresów IP i musi w swoich sieciach wewnętrznych używać adresów prywatnych, zdefiniowanych w RFC 1918. Adresy te nie są routowalne i nie można ich używać w sieciach publicznych, np. w Internecie. Secure Corporation używa adresów prywatnych, ponieważ nie chce być zmuszona do zmiany adresowania w przypadku zmiany dostawcy usług internetowych. Dzięki tym adresom firma może zmieniać publiczny adres IP, gdy wymagają tego okoliczności, a wymaga to od niej tylko skojarzenia nowych adresów IP z adresami prywatnymi. Strukturę sieci przedstawia rysunek 3.1. (Uwaga: sieć 192.168.0.0/16 należy do zakresu adresów prywatnych, lecz w niniejszym rozdziale będzie reprezentować przestrzeń publicznych adresów IP. Proszę pamiętać o tym podczas dalszej lektury).

Rysunek 3.1. *Translacja adresów sieciowych*



Z rysunku 3.1 wynika, że każdej lokalizacji została przydzielona 24-bitowa sieć z zakresu zdefiniowanego w RFC 1918. Są to odpowiednio sieci 172.16.1.0/24, 172.16.2.0/24 i 172.16.3.0/24. Dostawca usług internetowych do każdej lokalizacji przydzielił 24-bitową podsieć (odpowiednio 192.168.1.0/24, 192.168.2.0/24 i 192.168.3.0/24), która musi być mapowana na zakres adresów prywatnych. Poniższa konfiguracja pozwala na mapowanie do każdego węzła unikatowego publicznego adresu IP, dynamicznie przydzielanego

z puli zdefiniowanej dla każdej lokalizacji. Transmisje, które mają podlegać translacji, są identyfikowane poleceniem `nat`, a następnie mapowane na pulę publicznych adresów IP, zdefiniowaną poleceniem `global`:

```
PIX1(config)# nat (inside) 1 172.16.1.0 255.255.255.0
PIX1(config)# global (outside) 1 192.168.1.1-192.168.1.254 netmask 255.255.255.0
PIX1(config)# nat (inside) 2 172.16.2.0 255.255.255.0
PIX1(config)# global (outside) 2 192.168.2.1-192.168.2.254 netmask 255.255.255.0
PIX1(config)# nat (inside) 3 172.16.3.0 255.255.255.0
PIX1(config)# global (outside) 3 192.168.3.1-192.168.3.254 netmask 255.255.255.0
PIX1(config)# exit
PIX1# clear xlate
```

Polecenie `clear xlate` służy do usunięcia zawartości tablicy translacji. Powinno być wykonane po każdej zmianie konfiguracji translacji; w przeciwnym razie ryzykujemy pozostawieniem przestarzałych wpisów w tablicy. Należy jednak pamiętać, że to polecenie jednocześnie przerywa wszystkie bieżące połączenia, które korzystały z translacji.

Możemy teraz sprawdzić poprawność konfiguracji, używając poleceń `show running-config nat` i `show running-config global`:

```
PIX1# show running-config nat
nat (inside) 1 172.16.1.0 255.255.255.0
nat (inside) 2 172.16.2.0 255.255.255.0
nat (inside) 3 172.16.3.0 255.255.255.0
PIX1# show running-config global
global (outside) 1 192.168.1.1-192.168.1.254 netmask 255.255.255.0
global (outside) 2 192.168.2.1-192.168.2.254 netmask 255.255.255.0
global (outside) 3 192.168.3.1-192.168.3.254 netmask 255.255.255.0
```

W tym prostym, lecz mało realistycznym przykładzie dostawca usług internetowych przydzielił wystarczająco dużo adresów publicznych, by pozwolić na mapowanie 1:1 pomiędzy adresami lokalnymi i globalnymi. A jak wyglądałaby sytuacja, gdyby dostawca usług nie dał wystarczającej liczby adresów publicznych? Zmodyfikujmy nasz przykład. Teraz ISP przyznał firmie Secure Corp. pojedynczy zakres adresów sieci 24-bitowej (192.168.1.0/24). Zamiast oddzielnej puli globalnej dla każdej lokalizacji mamy jedną, wspólną pulę, co oznacza, że potrzebna jest PAT. Translacja PAT pozwala mapować wiele adresów IP na jeden adres, dzięki temu, że obejmuje zarówno adres IP, jak i port źródłowy. Konfiguracja będzie teraz wyglądać następująco:

```
PIX1(config)# nat (inside) 1 172.16.1.0 255.255.255.0
PIX1(config)# nat (inside) 1 172.16.2.0 255.255.255.0
PIX1(config)# nat (inside) 1 172.16.3.0 255.255.255.0
PIX1(config)# global (outside) 1 192.168.1.1-192.168.1.254 netmask 255.255.255.0
PIX1(config)# exit
PIX1# clear xlate
```

PAT pozwala na używanie DNS, FTP, HTTP, poczty, RPC, RSH, Telnet, filtrowania URL i wychodzących poleceń `traceroute`. Nie współpracuje z H.323, buforującymi serwerami nazw i PPTP.

Aby włączyć NAT dla większej liczby interfejsów, należy użyć osobnych poleceń `global` dla każdego interfejsu. Kluczem jest ten sam `id` dla wszystkich poleceń `global`, pozwalający na mapowanie przez jeden zestaw poleceń `nat` dla interfejsów z translacją prywatnego adresu IP na jeden z kilku różnych zakresów adresów globalnych na podstawie miejsca przeznaczenia. Na przykład, poniższe polecenia konfigurują w PIX translację sieci 172.16.1.0 albo na adresy 192.168.1.0/24, albo przez PAT na adres IP interfejsu strefy zdemilitaryzowanej, zależnie od tego, przez który interfejs pakiet ma wyjść:

```
PIX1(config)# nat (inside) 1 172.16.1.0 255.255.255.0
PIX1(config)# global (outside) 1 192.168.1.1-192.168.1.254 netmask 255.255.255.0
PIX1(config)# global (dmz) 1 interface
PIX1(config)# exit
PIX1# clear xlate
```

Podobnie jak dla większości poleceń w zaporze sieciowej PIX, słowo kluczowe `no` użyte z poleceniami `nat` i `global` usuwa ustawienia z konfiguracji.

Blokowanie ruchu wychodzącego (definiowanie ACL)

Bez dodatkowej konfiguracji PIX pozwala na wysyłanie wszelkiego ruchu z interfejsów o wyższym poziomie bezpieczeństwa do interfejsów o niższym poziomie bezpieczeństwa. Jeśli chcemy zablokować jakiś ruch wychodzący, to musimy zrobić to jawnie. Kontrola nad ruchem wychodzącym, który ma prawo przejść przez zaporę sieciową PIX, zawsze stanowi element dobrze zaprojektowanych zasad bezpieczeństwa. W wersji 7.0 do tego celu służy tylko jedno narzędzie: listy dostępu.

W starszych wersjach oprogramowania PIX można było dodatkowo blokować ruch wychodzący poleceniem `outbound`. W wersji 7.0 zostało ono całkowicie zastąpione poleceniem `access-list` i nie jest już obsługiwane. Firma Cisco do pewnego czasu odradzała używania poleceń `outbound`, więc nie powinno to być niespodzianką. Istniejące polecenia `outbound` nie są automatycznie konwertowane na polecenia `access-list`. Punkt „Polecenia conduit i outbound" zawiera więcej informacji na ten temat oraz opis, jak konwertować polecenia `outbound` na `access-list`.

Listy dostępu

Listy dostępu w zaporach sieciowych PIX są bardzo podobne do stosowanych w routerach Cisco i mogą być używane do ograniczania ruchu sieciowego na podstawie kilku kryteriów, w tym adresu źródłowego, adresu docelowego, źródłowych portów TCP/UDP i docelowych portów TCP/UDP. Konfiguracja list dostępu jest procesem złożonym z dwóch kroków:

1. Zdefiniowanie listy dostępu przez utworzenie poleceniem `access-list` instrukcji `permit` i `deny`.
2. Zastosowanie listy dostępu do interfejsu poleceniem `access-group`.

Polecenie `access-list` obsługuje trzy różne podstawowe klasy protokołów: IP, TCP/UDP i ICMP. Dla każdej klasy ma nieco inną składnię:

```
access-list numer_ACL [line nr_linii] [extended] {deny|permit} protokół {host
źródłowe_IP|źródłowe_IP maska|any} {host docelowe_IP|docelowe_IP maska|any}
access-list numer_ACL [line nr_linii] [extended] {deny|permit} {tcp|udp} {host
źródłowe_IP|źródłowe_IP maska|any} [operator port] {host docelowe_IP|docelowe_IP
maska|any} [operator port]
access-list numer_ACL [line nr_linii] [extended] {deny|permit} icmp {host
źródłowe_IP|źródłowe_IP maska|any} {host docelowe_IP|docelowe_IP maska|any}
[typ_icmp]
```

Poniżej przedstawiamy parametry i słowa kluczowe wspólne dla wszystkich trzech odmian składni `access-list`. Parametry i słowa kluczowe dotyczące konkretnych wersji składni zostaną omówione w następnych punktach.

Parametr *numer_ACL* identyfikuje listę dostępu i może nim być nazwa albo liczba. Listy dostępu są przetwarzane sekwencyjnie od pierwszej pozycji do ostatniej. Pierwszy pasujący wpis zostaje zastosowany, a dalsze przetwarzanie jest wstrzymywane.

Słowo kluczowe `line` i parametr *nr_linii* pozwalają wstawiać wpisy na określonych pozycjach listy dostępu.

Słowo kluczowe `extended` identyfikuje rozszerzoną listę dostępu, która pozwala wskazywać źródłowe i docelowe adresy i porty IP.

Źródłowy adres IP jest definiowany parametrem *źródłowe_IP* i identyfikuje źródło transmisji.

Docelowy adres IP jest definiowany parametrem *docelowe_IP* i identyfikuje miejsce przeznaczenia transmisji.

Parametr *maska* wskazuje liczbę bitów maski podsieci stosowanej do parametru *źródłowe_IP* lub *docelowe_IP*.

Słowo kluczowe `any` oznacza wszystkie sieci lub hosty i jest odpowiednikiem sieci 0.0.0.0 i maski 0.0.0.0.

Słowo kluczowe `host`, po którym następuje adres IP, wskazuje pojedynczego hosta.

Składnia list dostępu w zaporach sieciowych PIX jest bardzo podobna do stosowanej w routerach IOS. Podstawowa różnica polega na tym, że w listach dostępu zapór sieciowych stosowane są standardowe maski podsieci, a w routerach odwrócone (wildcard). Na przykład, przy blokowaniu 24-bitowej podsieci w zaporze sieciowej PIX użyjemy maski 255.255.255.0, a w routerze Cisco maski 0.0.0.255.

Parametry i słowa kluczowe access-list dla protokołu IP

W składni polecenia `access-list` dla protokołu IP parametr *protokół* wskazuje protokół IP. Można podać wartość liczbową lub nazwę literałową. Tabela 3.1 przedstawia niektóre dostępne nazwy literałowe.

Tabela 3.1. *Literałowe nazwy protokołów i wartości*

Literał	Wartość	Opis
ah	51	Authentication Header for IPv6, RFC 1826
eigrp	88	Enhanced Interior Gateway Routing Protocol
esp	50	Encapsulated Security Payload for IPv6, RFC 1827
gre	47	Generic Routing Encapsulation
icmp	1	Internet Control Message Protocol, RFC 792
igmp	2	Internet Group Management Protocol, RFC 3228
igrp	9	Interior Gateway Routing Protocol
ip	0	Internet Protocol
ipinip	4	Ekapsulacja IP-in-IP
nos	94	Network Operating System (NetWare firmy Novell)
ospf	89	Protokół routingu Open Shortest Path First, RFC 1247
pcp	108	Payload Compression Protocol
snp	109	Sitara Networks Protocol
tcp	6	Transmission Control Protocol, RFC 793
udp	17	User Datagram Protocol, RFC 768

Parametry i słowa kluczowe access-list dla protokołów TCP i UDP

W składni polecenia `access-list` dla protokołów TCP i UDP parametry i słowa kluczowe mają następujące znaczenie:

Słowa kluczowe `tcp` i `udp` wskazują, czy dany wpis listy dostępu dotyczy ruchu TCP, czy UDP.

`operator` i *`port`* wskazują porty źródłowy i docelowy.

Aby wskazać wszystkie porty, nie trzeba podawać operatora i portu.

Aby wskazać pojedynczy port, należy użyć jako operatora słowa kluczowego `eq`.

Aby wskazać wszystkie porty o numerach niższych niż podany, należy użyć jako operatora słowa kluczowego `lt`.

Aby wskazać wszystkie porty o numerach wyższych niż podany, należy użyć jako operatora słowa kluczowego `gt`.

Aby wskazać wszystkie porty z wyjątkiem jednego, należy użyć jako operatora słowa kluczowego `neq`.

Aby wskazać zakres portów, należy użyć jako operatora słowa kluczowego `range`.

Port może być wskazany z podaniem liczby lub nazwy. Listę nazw portów przedstawia tabela 3.2.

Tabela 3.2. *Literałowe nazwy portów i wartości*

Nazwa	Protokół	Port	Nazwa	Protokół	Port	Nazwa	Protokół	Port
bgp	TCP	179	http	TCP	80	radius	UDP	1812
biff	UDP	512	hostname	TCP	101	rip	UDP	520
bootpc	UDP	68	ident	TCP	113	smtp	TCP	25
bootps	UDP	67	irc	TCP	194	snmp	UDP	161
chargen	TCP	19	isakmp	UDP	500	snmptrap	UDP	162
citrix-ica	TCP	1494	klogin	TCP	543	sqlnet	TCP	1521
cmd	TCP	514	kshell	TCP	544	sunrpc	TCP, UDP	111
daytime	TCP	13	login	TCP	513	syslog	UDP	514
discard	TCP, UDP	9	lpd	TCP	515	tacacs	TCP, UDP	49
dnsix	UDP	195	mobile-ip	UDP	434	talk	TCP, UDP	517
domain	TCP, UDP	53	nameserver	UDP	42	telnet	TCP	23
echo	TCP, UDP	7	netbios-dgm	UDP	138	tftp	UDP	69
exec	TCP	512	netbios-ns	UDP	137	time	UDP	37
finger	TCP	79	nntp	TCP	119	uucp	TCP	540
ftp	TCP	21	ntp	UDP	123	who	UDP	513
ftp-data	TCP	20	pim-auto-rp	TCP, UDP	496	whois	TCP	43
gopher	TCP	70	pop2	TCP	109	www	TCP	80
h323	TCP	1720	pop3	TCP	110	xdmcp	UDP	177

Proszę zauważyć, że zdefiniowane w systemie mapowanie `http` jest takie samo jak `www` i jest tłumaczone na nie w konfiguracji.

Parametry i słowa kluczowe access-list dla protokołu ICMP

W składni polecenia `access-list` dla protokołu ICMP parametry i słowa kluczowe mają następujące znaczenie:

Słowo kluczowe `icmp` oznacza, że dany wpis listy dostępu dotyczy ruchu ICMP.

Parametr *`typ_icmp`* identyfikuje typ komunikatu ICMP i może być wskazany z podaniem liczby lub nazwy. Listę typów komunikatów ICMP i odpowiadających im nazw literałowych przedstawia tabela 3.3.

Po skonfigurowaniu listy dostępu należy zastosować ją do interfejsu poleceniem:

```
access-group access-list {in|out} interface nazwa_interfejsu
```

Parametry i słowa kluczowe polecenia `access-group` są następujące:

Parametr *`access-list`* definiuje, które instrukcje listy dostępu mają stosować się do interfejsu. Wartość tego parametru musi odpowiadać *`numer_ACL`* (nazwie) wskazanej w poprzednich poleceniach `access-list`.

Tabela 3.3. *Typy komunikatów ICMP*

Typ ICMP	Literał
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-reply
14	timestamp-request
15	information-request
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect

Słowo kluczowe `in` albo `out` służy do wskazania, czy lista dostępu dotyczy pakietów przychodzących do interfejsu (`in`), czy wychodzących z interfejsu (`out`).

Słowo kluczowe `interface` i parametr *`nazwa_interfejsu`* wskazuje interfejs, do którego mają stosować się instrukcje `access-list`.

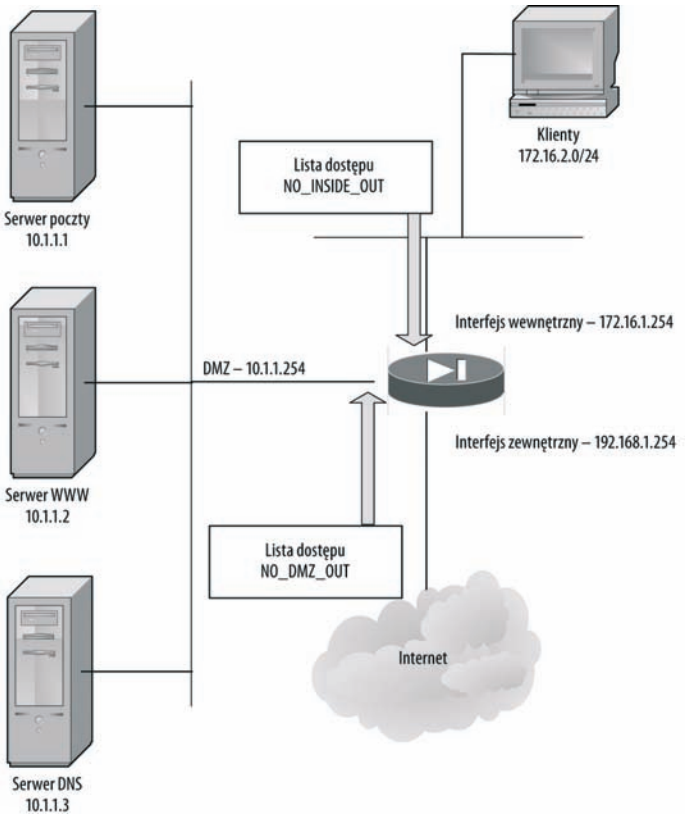
Zastosowanie listy dostępu do interfejsu poleceniem `access-group` dopuszcza lub blokuje ruch wchodzący do wskazanego interfejsu.

W starszych wersjach oprogramowania PIX listy dostępu w zaporze sieciowej mogły być stosowane tylko do ruchu **przychodzącego** do interfejsu przez użycie słowa kluczowego `in`. W wersji 7.0 listy dostępu mogą też obowiązywać dla ruchu **wychodzącego** z interfejsu, jeśli użyjemy słowa kluczowego `out`.

Listy dostępu mają na końcu ukrytą instrukcję `deny all`. Jeśli dana transmisja nie jest wprost dozwolona przez listę dostępu, to zostanie zablokowana. Możemy tworzyć bardzo złożone listy dostępu, po prostu podążając za przepływem tego, co powinno być dozwolone lub nie. Dla pojedynczego interfejsu może być jednocześnie stosowana tylko jedna lista dostępu.

Przyjrzyjmy się teraz naszej fikcyjnej firmie Secure Corp., która właśnie kupiła nową zaporę sieciową PIX dla swojej sieci w Nowym Jorku, jak na rysunku 3.2. Klienty w tej sieci znajdują się po stronie interfejsu wewnętrznego PIX (pojedyncza sieć 172.16.1.0/24), natomiast serwery w strefie zdemilitaryzowanej (sieć 10.1.1.0/24). ISP przydzielił firmie do użytku sieć publiczną 192.168.1.0/24.

Rysunek 3.2. *Lista dostępu dla ruchu wychodzącego*



Wewnętrzne klienty nie powinny mieć prawa wysyłania określonych typów transmisji, na przykład związanych z drogami infekcji przez złośliwe oprogramowanie. Obejmuje to protokół służący do udostępniania plików CIFS/SMB (ang. *Common Internet File System*/*Server Message Block*), bootp, SNMP (ang. *Simple Network Management Protocol*), SQL*Net, Kazaa i sieci P2P. Poza tymi typami ruchu sieciowego, wprost zabronionymi, klienty powinny mieć nieograniczony dostęp do Internetu.

Serwery w DMZ powinny mieć dostęp do Internetu wyłącznie przy użyciu protokołów, które obsługują ich podstawowe funkcje. Na przykład, serwer poczty elektronicznej powinien mieć prawo do wysyłania i odbierania transmisji SMTP (ang. *Simple Mail Transfer Protocol*), serwer WWW powinien mieć prawo do wysyłania i odbierania tylko HTTP (ang. *HyperText Transfer Protocol*) i HTTP przez SSL (HTTPS), a serwer DNS tylko ruchu związanego z usługą DNS (ang. *Domain Name Service*).

Interfejs DMZ ma wyższy poziom bezpieczeństwa niż interfejs zewnętrzny, więc wszelki ruch inicjowany przez serwery DMZ w stronę Internetu będzie domyślnie dozwolony. Chcemy zastosować do serwerów w DMZ te same ograniczenia co dla klientów wewnętrznych. Ponieważ z serwerów nikt nie powinien przeglądać WWW, firma zdefiniowała zasadę zakazującą wychodzącego ruchu WWW (tzn. HTTP i HTTPS) z serwerów w DMZ.

Wymogi firmy Secure Corporation mogą zaspokoić dwie listy dostępu ruchu wychodzącego: jedna dla interfejsu wewnętrznego i jedna dla interfejsu DMZ. Poniższe polecenia definiują i wprowadzają do użytku listę dostępu wychodzącego dla interfejsu wewnętrznego:

```
PIX1(config)# access-list NO_INSIDE_OUT deny tcp any any eq 135
PIX1(config)# access-list NO_INSIDE_OUT deny udp any any eq 135
PIX1(config)# access-list NO_INSIDE_OUT deny udp any any eq netbios-ns
PIX1(config)# access-list NO_INSIDE_OUT deny udp any any eq netbios-dgm
PIX1(config)# access-list NO_INSIDE_OUT deny tcp any any eq netbios-ssn
PIX1(config)# access-list NO_INSIDE_OUT deny udp any any eq 139
PIX1(config)# access-list NO_INSIDE_OUT deny tcp any any eq 445
PIX1(config)# access-list NO_INSIDE_OUT deny udp any any eq 445
PIX1(config)# access-list NO_INSIDE_OUT deny udp any any eq tftp
PIX1(config)# access-list NO_INSIDE_OUT deny udp any any eq bootpc
PIX1(config)# access-list NO_INSIDE_OUT deny udp any any eq bootps
PIX1(config)# access-list NO_INSIDE_OUT deny udp any any eq snmp
PIX1(config)# access-list NO_INSIDE_OUT deny udp any any eq snmptrap
PIX1(config)# access-list NO_INSIDE_OUT deny tcp any any eq sqlnet
PIX1(config)# access-list NO_INSIDE_OUT deny tcp any any eq 1214
PIX1(config)# access-list NO_INSIDE_OUT deny tcp any any eq 3408
PIX1(config)# access-list NO_INSIDE_OUT deny tcp any any eq 3531
PIX1(config)# access-list NO_INSIDE_OUT permit any any
PIX1(config)# access-group NO_INSIDE_OUT in interface inside
PIX1(config)# exit
```

Poniższe polecenia definiują i wprowadzają do użytku listę dostępu wychodzącego dla interfejsu DMZ, która różni się od listy dla interfejsu wewnętrznego przede wszystkim tym, że blokuje ruch WWW:

```
PIX1(config)# access-list NO_DMZ_OUT deny tcp any any eq 135
PIX1(config)# access-list NO_DMZ_OUT deny udp any any eq 135
PIX1(config)# access-list NO_DMZ_OUT deny udp any any eq netbios-ns
PIX1(config)# access-list NO_DMZ_OUT deny udp any any eq netbios-dgm
PIX1(config)# access-list NO_DMZ_OUT deny tcp any any eq netbios-ssn
PIX1(config)# access-list NO_DMZ_OUT deny udp any any eq 139
PIX1(config)# access-list NO_DMZ_OUT deny tcp any any eq 445
PIX1(config)# access-list NO_DMZ_OUT deny udp any any eq 445
PIX1(config)# access-list NO_DMZ_OUT deny udp any any eq tftp
PIX1(config)# access-list NO_DMZ_OUT deny udp any any eq bootpc
PIX1(config)# access-list NO_DMZ_OUT deny udp any any eq bootps
PIX1(config)# access-list NO_DMZ_OUT deny udp any any eq snmp
PIX1(config)# access-list NO_DMZ_OUT deny udp any any eq snmptrap
PIX1(config)# access-list NO_DMZ_OUT deny tcp any any eq sqlnet
PIX1(config)# access-list NO_DMZ_OUT deny tcp any any eq 1214
PIX1(config)# access-list NO_DMZ_OUT deny tcp any any eq 3408
PIX1(config)# access-list NO_DMZ_OUT deny tcp any any eq 3531
PIX1(config)# access-list NO_DMZ_OUT deny tcp any any eq www
```

```
PIX1(config)# access-list NO_DMZ_OUT deny tcp any any eq https
PIX1(config)# access-list NO_DMZ_OUT permit tcp 10.1.1.1 any eq smtp
PIX1(config)# access-list NO_DMZ_OUT permit tcp 10.1.1.3 any eq dns
PIX1(config)# access-list NO_DMZ_OUT permit udp 10.1.1.3 any eq dns
PIX1(config)# access-group NO_DMZ_OUT in interface DMZ
PIX1(config)# exit
```

Należy wspomnieć, że nie zajęliśmy się jeszcze konfiguracją ruchu przychodzącego. Powyższe listy dostępu jedynie pozwalają serwerom inicjować kontakt z innymi serwerami, tak jak klientom. Na przykład, serwer poczty może wysyłać wiadomości do innej domeny, lecz nie może odbierać poczty. Serwer DNS może rozwiązywać nazwy z innych domen, lecz nie może odpowiadać na zapytania z innej domeny. W podrozdziale „Otwarcie dostępu do sieci z zewnątrz" omówimy szczegółowo konfigurację ruchu przychodzącego.

Jedną z funkcji przydatnych podczas konfiguracji PIX jest polecenie `name`, które mapuje nazwę (alias) na adres IP. Podczas konfiguracji, zamiast wskazywać hosta przez adres IP, możemy użyć nazwy. To może pomóc w konfiguracji i rozwiązywaniu problemów ze złożonymi konfiguracjami. Może też ułatwić zmiany adresów: nazwa pozostaje, lecz adres IP można zmienić bez modyfikacji list dostępu. Składnia polecenia wygląda tak:

```
name adres_ip nazwa
```

Na przykład, poniższe polecenia mapują nazwy *emailserver*, *webserver* i *dnsserver* odpowiednio na adresy IP 10.1.1.1, 10.1.1.2 i 10.1.1.3:

```
PIX1(config)# name 10.1.1.1 emailserver
PIX1(config)# name 10.1.1.2 webserver
PIX1(config)# name 10.1.1.3 dnsserver
```

Teraz zamiast adresów IP będziemy mogli posługiwać się nazwami *emailserver*, *webserver* i *dnsserver*.

Otwarcie dostępu do sieci z zewnątrz

Prędzej czy później, w każdej sieci zajdzie potrzeba umożliwienia niezaufanym i nieznanym hostom inicjowania sesji z naszymi zaufanymi i chronionymi urządzeniami — np. z serwerami. Na przykład, użytkownicy z Internetu mogą chcieć nawiązywać połączenia z naszymi serwerami w DMZ. Zapora sieciowa PIX nie byłaby specjalnie przydatna, gdyby nie umożliwiała przepuszczania i kontroli ruchu z niezaufanych źródeł do sieci zawierających krytyczne systemy, na przykład serwer WWW firmy. ASA w systemie PIX traktuje ruch przychodzący (z interfejsu o niższym poziomie bezpieczeństwa do interfejsu o wyższym poziomie bezpieczeństwa) inaczej niż ruch wychodzący.

W przeciwieństwie do wychodzącego, ruch przychodzący jest domyślnie blokowany. Gwarantuje to, że granice zdefiniowane przez poziomy bezpieczeństwa interfejsów są realne i nie są omijane. Podobnie jak w przypadku ruchu wychodzącego, konfiguracja

ruchu przychodzącego jest procesem złożonym z dwóch kroków. Należy zdefiniować translację statyczną i utworzyć listę dostępu, która będzie dopuszczać przychodzące transmisje.

Polecenie `conduit` zostało w wersji 7.0 całkowicie zastąpione przez listy dostępu. Firma Cisco odradzała użycie tego polecenia już w wersjach 6.x, więc nie powinno to być większą niespodzianką.

Statyczna translacja adresów

Gdy publicznie dostępny serwer (w miarę możliwości położony w DMZ) jest chroniony przez zaporę sieciową PIX, trzeba wprost pozwolić na połączenia z interfejsu o niższym poziomie bezpieczeństwa do interfejsu o wyższym poziomie bezpieczeństwa. Dopuszczenie ruchu przychodzącego zaczyna się od skonfigurowania statycznej translacji adresów. Polecenie `static` mapuje trwale globalne adresy IP na lokalne. Składnia polecenia wygląda tak:

```
static (rzeczywisty_int, mapowany_int) {mapowany_ip|interface} {rzeczywisty_ip
[netmask maska]}|{access-list nazwa_listy_dost} [dns] [norandomseq [nailed]]
[[tcp][max_poł_tcp [limit_emb]] [udp max_poł_udp]
```

Parametry i słowa kluczowe polecenia `static` są następujące:

Parametr *rzeczywisty_int* wskazuje interfejs, z którym połączony jest serwer podlegający translacji.

Parametr *mapowany_int* wskazuje interfejs mapowanego globalnego adresu IP. Jest to interfejs, na którym udostępniamy urządzenie (np. serwer).

Parametr *mapowany_ip* jest globalnym adresem IP, który powinien posłużyć do translacji.

Parametr *rzeczywisty_ip* jest lokalnym adresem IP, który powinien podlegać translacji. Zwykle jest to rzeczywisty adres urządzenia (np. serwera), które udostępniamy.

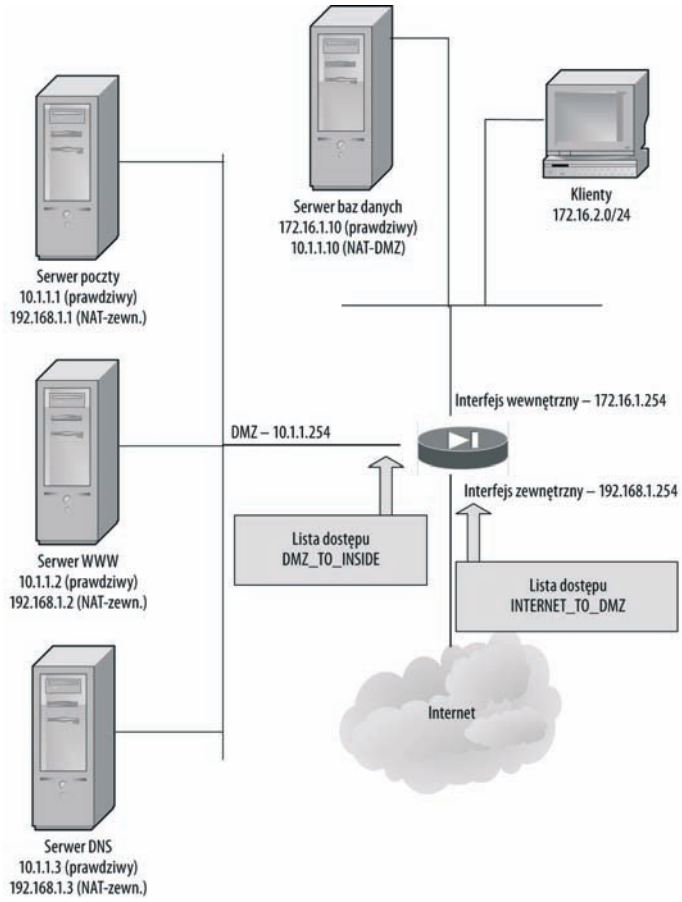
Słowo kluczowe `netmask` i parametr *maska* są używane przy jednoczesnej translacji statycznej więcej niż jednego adresu IP.

Wartość domyślna parametrów *max_poł_tcp*, *limit_emb* i *max_poł_udp* wynosi 0 (bez ograniczeń). Ich znaczenie jest takie samo jak w poleceniu `nat`.

Na rysunku 3.3 firma Secure Corporation ma trzy serwery w sieci DMZ. Poniższe polecenia `static` ustanawiają statyczną translację adresów dla tych serwerów:

```
PIX1(config)# static (dmz, outside) 192.168.1.1 10.1.1.1 netmask 255.255.255.255 0 0
PIX1(config)# static (dmz, outside) 192.168.1.2 10.1.1.2 netmask 255.255.255.255 0 0
PIX1(config)# static (dmz, outside) 192.168.1.3 10.1.1.3 netmask 255.255.255.255 0 0
```

Rysunek 3.3.
Statyczna translacja adresów



Polecenia te definiują translację niezbędną, by serwery w DMZ były dostępne pod adresami 192.168.1.1, 192.168.1.2 i 192.168.1.3. Jeśli DMZ zawiera większą liczbę serwerów, to zamiast konfigurować osobny wpis dla każdego, możemy użyć pojedynczego polecenia `static` z odpowiednią maską podsieci. Na przykład, dla czternastu serwerów w DMZ o IP od 10.1.1.1 do 10.1.1.14 polecenie będzie wyglądać tak:

```
PIX1(config)# static (dmz, outside) 192.168.1.0 10.1.1.0 netmask 255.255.255.240 0 0
```

Rozważmy teraz scenariusz, w którym serwer WWW położony w DMZ musi korzystać z serwera baz danych połączonego z interfejsem wewnętrznym PIX, jak na rysunku 3.3.

Proces wygląda tak samo: zawsze gdy interfejs o niższym poziomie bezpieczeństwa wymaga dostępu do interfejsu o wyższym poziomie bezpieczeństwa, trzeba zdefiniować statyczną translację. Poniższa konfiguracja przekłada rzeczywisty adres wewnętrznego serwera baz danych (172.16.1.10) na adres dostępny dla serwera WWW w DMZ (10.1.1.10):

```
PIX1(config)# static (inside, dmz) 10.1.1.10 172.168.1.10 netmask 255.255.255.240 0 0
```

Sama translacja statyczna nie wystarczy, by umożliwić komunikację z niższego do wyższego poziomu bezpieczeństwa — musimy zdefiniować listę dostępu, która będzie jawnie zezwalała na nią. Polecenie `static` tworzy tylko statyczne mapowanie pomiędzy globalnym i lokalnym adresem IP. Domyślną czynnością dla transmisji przychodzących jest jej odrzucenie, więc naszym następnym krokiem musi być utworzenie listy dostępu, która wpuści komunikację do zapory sieciowej PIX.

Listy dostępu

Tworzenie listy dostępu zezwalającej na ruch przychodzący wygląda podobnie jak przy ruchu wychodzącym. Składnia polecenia wraz ze wszystkimi parametrami jest taka sama. Podstawowa różnica polega na tym, że aby zezwolić na komunikację z niższego do wyższego poziomu bezpieczeństwa, musimy najpierw skonfigurować translację statyczną. Dla przykładu Security Corp. z rysunku 3.3 zdefiniujemy i zastosujemy dwie listy dostępu: jedną, która zezwala na komunikację z Internetu do serwerów w DMZ, i drugą, która zezwala na komunikację z serwera WWW w DMZ z wewnętrznym serwerem baz danych.

Poniższe polecenia definiują i wprowadzają listę dostępu dla komunikacji wchodzącej z Internetu do sieci DMZ:

```
PIX1(config)# access-list INTERNET_TO_DMZ permit tcp any host 192.168.1.1 eq smtp
PIX1(config)# access-list INTERNET_TO_DMZ permit tcp any host 192.168.1.2 eq web
PIX1(config)# access-list INTERNET_TO_DMZ permit tcp any host 192.168.1.2 eq https
PIX1(config)# access-list INTERNET_TO_DMZ permit tcp any host 192.168.1.3 eq dns
PIX1(config)# access-list INTERNET_TO_DMZ permit udp any host 192.168.1.3 eq dns
PIX1(config)# access-group INTERNET_TO_DMZ in interface Outside
PIX1(config)# exit
```

Poniższe polecenia definiują i stosują listę dostępu z DMZ do sieci wewnętrznej:

```
PIX1(config)# access-list DMZ_TO_INSIDE permit tcp host 10.1.1.2 host 10.1.1.10 eq
sqlnet
PIX1(config)# access-group DMZ_TO_INSIDE in interface DMZ
PIX1(config)# exit
```

Przypominamy, że na końcu każdej listy dostępu znajduje się ukryta reguła `deny all`. Gwarantuje ona, że komunikacja z interfejsu o niższym poziomie bezpieczeństwa do interfejsu o wyższym poziomie bezpieczeństwa, która nie została wprost dopuszczona, będzie zablokowana. W naszym przykładzie lista dostępu `DMZ_TO_INSIDE` dopuszcza tylko komunikację SQL*Net pomiędzy serwerem WWW w DMZ i wewnętrznym serwerem baz danych. W instrukcji `access-list` zostały podane adresy IP, zarówno źródłowy, jak i docelowy. Dla interfejsu można zastosować tylko jedną listę dostępu (w jednym kierunku), a lista `DMZ_TO_INSIDE` musi być połączona z instrukcjami listy dostępu `NO_DMZ_OUT` z poprzedniego podrozdziału, aby spełnić wymogi zasad bezpieczeństwa pożądane przez Secure Corporation.

Listy dostępu ICMP

ICMP jest użytecznym protokołem diagnostycznym, znanym najlepiej chyba z dwóch narzędzi: ping i traceroute. Oba narzędzia generują komunikaty ICMP i używają odpowiedzi do ustalenia osiągalności urządzenia i trasy do niego. Niewystarczająco kontrolowany ICMP może też być dla napastników najbardziej przydatnym narzędziem do infiltrowania organizacji. Na dodatek niektóre protokoły mogą potrzebować ICMP do odkrywania tras lub stwierdzania osiągalności hosta przed nawiązaniem sesji. Wszystko to razem powoduje, że rozwiązywanie problemów z ICMP jest niełatwe. Brak odpowiedzi ICMP może oznaczać problem z siecią albo fakt, że zapora pełni swoje zadanie — chroni nasze sieci.

Z tego powodu zapory sieciowe PIX domyślnie blokują ICMP, z pewnymi wyjątkami: urządzenia mogą sprawdzać poleceniem `ping` bezpośrednio podłączone interfejsy urządzenia zapory sieciowej. Urządzenia mogą sprawdzać się nawzajem przez `ping`, o ile transmisja nie przechodzi przez zaporę sieciową. Komunikacja ICMP z sieci zewnętrznej do każdego interfejsu o wyższym poziomie bezpieczeństwa jest domyślnie blokowana. Zanim otworzymy dostęp ICMP przez zaporę sieciową, musimy ustalić, jakie transmisje i pomiędzy którymi sieciami są potrzebne. Jeśli coś nie ma dla nas wartości, to nie powinno być dozwolone.

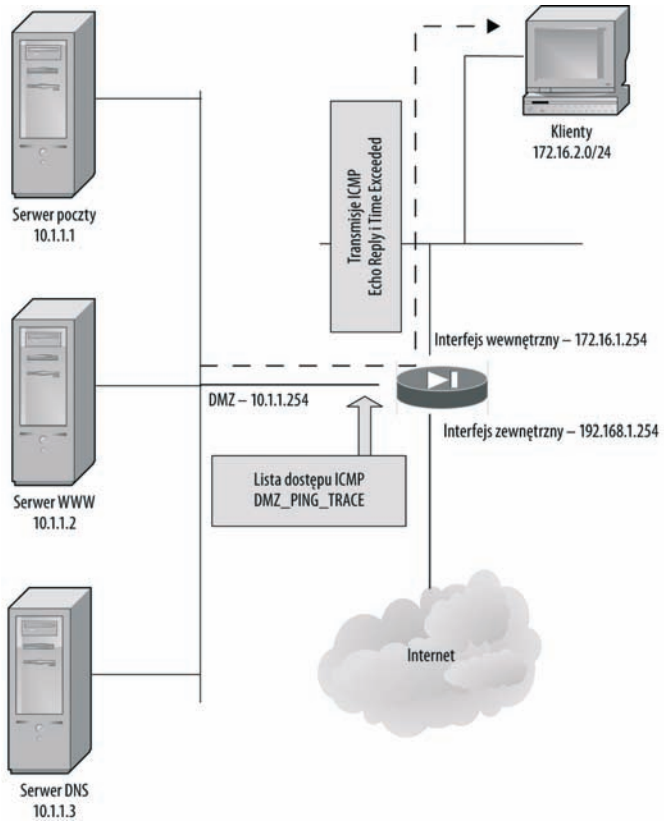
Stosowane są dwa podejścia do przepuszczania komunikacji ICMP przez PIX:

- **Listy dostępu** — ICMP jest protokołem bezpołączeniowym, więc potrzebujemy list dostępu, zezwalających na ICMP w obu kierunkach (stosując listy zarówno do interfejsów źródłowych, jak i docelowych).
- **Mechanizm inspekcji ICMP** — musimy włączyć mechanizm inspekcji ICMP, który traktuje konwersacje ICMP jak połączenia mające stan. Mechanizm inspekcji ICMP używa MPF (ang. *Modular Policy Framework*) — nowej funkcji oprogramowania PIX 7.0.

W niniejszym rozdziale pokażemy, jak za pomocą list dostępu pozwalać na przechodzenie ICMP przez PIX. W przykładzie z rysunku 3.4 chcemy, by urządzenia z sieci wewnętrznej mogły sprawdzać poleceniami `ping` i `traceroute` urządzenia w sieci DMZ.

Domyślnie komunikacja ICMP z sieci wewnętrznej do DMZ jest dozwolona, więc nie musimy stosować listy dostępu dla interfejsu wewnętrznego. Aby przepuścić transmisje powrotne z DMZ, musimy zezwolić na następujące transmisje:

- Dla poleceń `ping` wydawanych z DMZ pakiety ICMP Echo z sieci wewnętrznej na zewnątrz są domyślnie dozwolone, lecz musimy przepuścić pakiety ICMP Echo Reply z DMZ do sieci wewnętrznej.
- Dla poleceń `traceroute` z sieci wewnętrznej do DMZ pakiety wychodzące są domyślnie przepuszczane, lecz musimy jeszcze dopuścić pakiety ICMP Time Exceeded z DMZ do sieci wewnętrznej.



Rysunek 3.4. *Listy kontroli dostępu ICMP*

Osiągniemy to następującymi poleceniami:

```
PIX1(config)# access-list DMZ_PING_TRACE permit icmp 10.1.1.0 255.255.255.0
172.16.0.0 255.255.240.0 echo-reply
PIX1(config)# access-list DMZ_PING_TRACE permit icmp 10.1.1.0 255.255.255.0
172.16.0.0 255.255.240.0 time-exceeded
PIX1(config)# access-group DMZ_PING_TRACE in interface DMZ
PIX1(config)# exit
```

Przekierowanie portów

Przekierowanie portów pozwala na wykorzystanie jednego publicznego adresu IP dla więcej niż jednego serwera. Można za jego pomocą zdefiniować mapowanie pomiędzy portem w publicznym adresie IP i portem w prywatnym adresie IP. Aby umożliwić przekierowanie, musimy jednak utworzyć listę dostępu, ponieważ komunikacja odbywa się z interfejsu o niższym poziomie bezpieczeństwa do interfejsu o wyższym poziomie bezpieczeństwa.

Ponieważ mapowanie może odbywać się na poziomie portów, jeden adres IP może służyć jako brama dla wielu serwerów za zaporą sieciową PIX. Na przykład, firma Secure Corp. zainstalowała sieć w swojej siedzibie w Toronto, gdzie otrzymała tylko jeden publiczny adres IP od ISP. W tej lokalizacji firma ma dwa serwery WWW, jeden

serwer Telnet i jeden serwer FTP. Jak może udostępnić wszystkie te usługi przez jeden adres IP? Odpowiedź brzmi: dokonując przekierowania portów poleceniem `static`:

```
static (rzeczywisty_int, mapowany_int) {tcp|udp} {mapowany_ip|interface}
mapowany_port {rzeczywisty_ip rzeczywisty_port [netmask maska]}|{access-list
nazwa_listy_dost} [dns] [norandomseq [nailed]] [[tcp][max_poł_tcp [limit_emb]] [udp
max_poł_udp]
```

Omówiliśmy już wcześniej polecenie `static`, więc nie będziemy ponownie opisywać tych samych parametrów. W powyższej składni wprowadziliśmy jednak kilka nowych parametrów:

- Słowa kluczowe `tcp` i `udp` służą do wskazania statycznego przekierowania portu TCP lub UDP przez statyczną PAT.
- Parametry *mapowany_port* i *rzeczywisty_port* wskazują odpowiednio port mapowany (tzn. zewnętrzny port dostępny spoza PIX) i port rzeczywisty (tzn. faktyczny port nasłuchujący w serwerze).
- Zamiast parametru *mapowany_ip* możemy użyć słowa kluczowego `interface`, aby wskazać adres IP interfejsu PIX zdefiniowanego w parametrze *mapowany_int*. Ta opcja jest ważna, jeśli nie mamy żadnych dodatkowych publicznych adresów IP, nadających się do użytku.

Aby skonfigurować przekierowanie portów dla pierwszego serwera WWW z użyciem publicznego adresu IP urządzenia PIX jako adresu publicznego serwera WWW, użyjemy polecenia:

```
PIX1(config)# static (dmz, outside) tcp interface 80 10.1.1.1 80
```

Jeśli firma chce też udostępniać Telnet, FTP i jeszcze jeden serwer WWW, to musimy dodać jeszcze trzy polecenia `static`, mapujące globalne porty na właściwe serwery. Ponieważ port WWW jest już zajęty, do łączenia się z drugim serwerem WWW został wybrany port z wysokiego zakresu (8080). Ten przykład został zilustrowany na rysunku 3.5. Dodatkowe polecenia to:

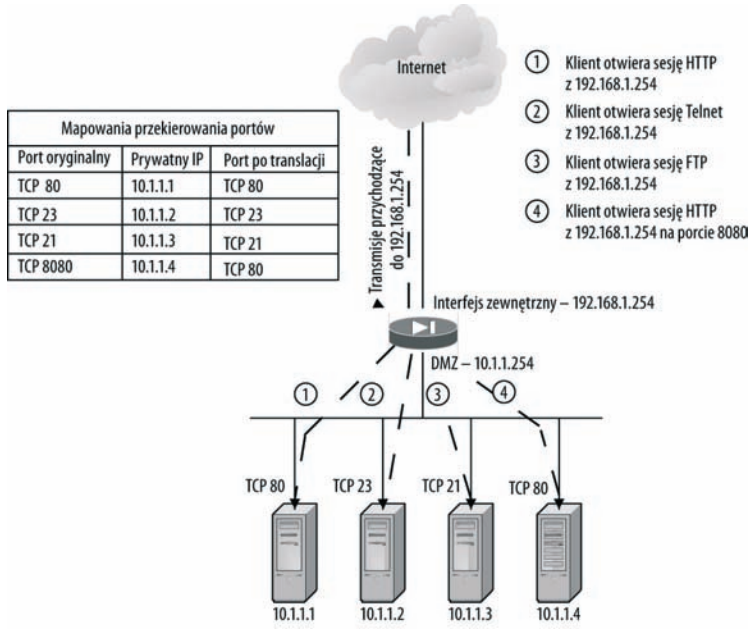
```
PIX1(config)# static (dmz, outside) tcp interface 23 10.1.1.2 23
PIX1(config)# static (dmz, outside) tcp interface 21 10.1.1.3 21
PIX1(config)# static (dmz, outside) tcp interface 8080 10.1.1.4 80
```

Włączanie i wyłączanie wpisów w ACL (nowe)

W oprogramowaniu PIX w wersji 7.0 została dodana możliwość tymczasowego wyłączania wpisów na liście dostępu bez usuwania ich z pliku konfiguracyjnego. Jest to potężne narzędzie do rozwiązywania problemów i precyzyjnego „dostrajania" list kontroli dostępu. Przy rozwiązywaniu problemów z komunikacją przez zaporę sieciową PIX, jeśli nie mamy pewności, który wpis kontroli dostępu stwarza problem, możemy selektywnie wyłączać wpisy, dodając słowo kluczowe `inactive` w odpowiedniej instrukcji `access-list`. Tak samo możemy tymczasowo wyłączyć wpis, który może się przydać w przyszłości. Na przykład, aby wyłączyć wpis w ACL zezwalający na przychodzący ruch WWW do serwera WWW w strefie zdemilitaryzowanej, użyjemy polecenia:

```
PIX1(config)# access-list INTERNET_TO_DMZ permit tcp any host 10.1.1.2 eq 80
inactive
PIX1(config)# exit
```

Rysunek 3.5. *Przekierowanie portów*



Wyjściowe ACL (nowe)

Listy dostępu mogą być używane do filtrowania niepewnych transmisji wychodzących, na przykład CIFS, TFTP, bootp, SNMP, SQL*Net, Kazaa i sieci P2P. We wcześniejszym przykładzie utworzyliśmy i zastosowaliśmy listy dostępu dla interfejsów wewnętrznego i DMZ, blokujące te transmisje w stronę Internetu. To prowadzi nas do nowej funkcji oprogramowania PIX 7.0, nazwanej „Outbound ACL" (wyjściowe listy kontroli dostępu). W poprzednich wersjach systemu operacyjnego PIX listy dostępu mogły być stosowane tylko do pakietów przychodzących na interfejs. W wersji 7.0 dzięki funkcji wyjściowych ACL listy dostępu mogą być stosowane zarówno do pakietów przychodzących, jak i wychodzących z interfejsu. Dla jednego interfejsu możemy jednak zastosować tylko jedną ACL w każdym kierunku.

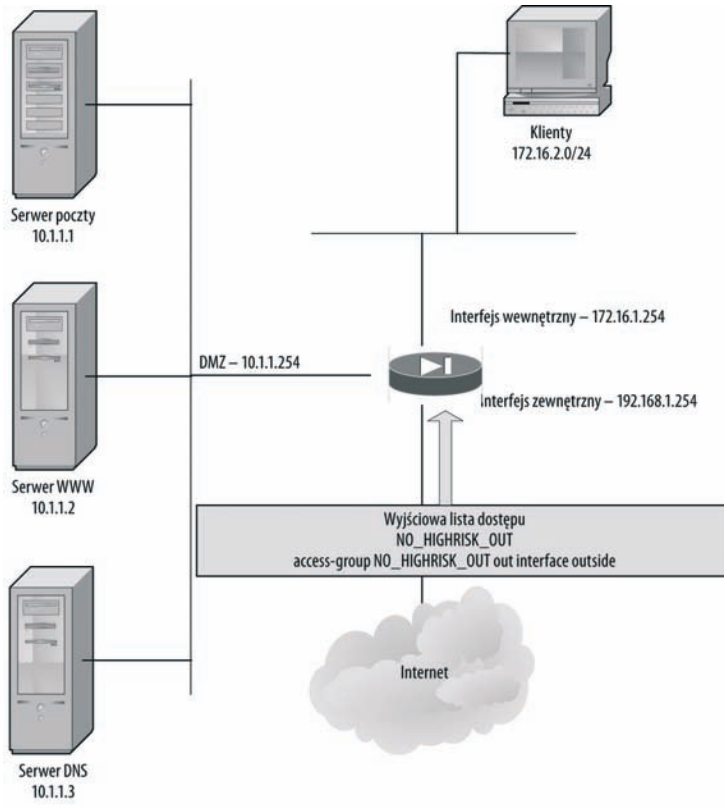
W kontekście wyjściowych ACL pojęcia połączeń „przychodzących" i „wychodzących" mają inne znaczenie niż przy opisywaniu przepływu transmisji przez granice sieci. W wyjściowych ACL dotyczy to list kontroli dostępu dla konkretnego interfejsu i komunikacji przychodzącej do urządzenia PIX albo wychodzącej z niego. W przypadku przekraczania granic sieci komunikacja „przychodząca" oznacza przepływ z interfejsu o niższym poziomie bezpieczeństwa do interfejsu o wyższym poziomie bezpieczeństwa, a „wychodząca" na odwrót.

Do implementowania wyjściowych ACL służy polecenie `access-group` ze słowem kluczowym `out` zamiast `in`:

```
access-group access-list out interface nazwa_interfejsu
```

W poprzednim przykładzie Secure Corporation utworzyliśmy i zastosowaliśmy **wejściowe** listy dostępu dla interfejsów wewnętrznego i DMZ, zapobiegające **wejściu** do PIX tej komunikacji o wysokim poziomie zagrożenia. Zamiast tego możemy utworzyć pojedynczą **wyjściową** listę dostępu i zastosować ją do interfejsu zewnętrznego PIX, zapobiegając **wyjściu** z PIX tej komunikacji o wysokim poziomie zagrożenia. Takie rozwiązanie, przedstawione na rysunku 3.6, jest o wiele bardziej skalowalne, ponieważ lista dostępu jest tworzona i stosowana tylko raz, niezależnie od liczby interfejsów. W poprzednich wersjach systemu trzeba było wprowadzać odpowiednie wpisy kontrolujące dostęp do osobnych ACL dla każdego interfejsu.

Rysunek 3.6.
Wyjściowe ACL



Konfiguracja wyjściowych ACL dla Secure Corporation będzie wyglądać tak:

```
PIX1(config)# access-list NO_HIGHRISK_OUT deny tcp any any eq 135
PIX1(config)# access-list NO_HIGHRISK_OUT deny udp any any eq 135
PIX1(config)# access-list NO_HIGHRISK_OUT deny udp any any eq netbios-ns
PIX1(config)# access-list NO_HIGHRISK_OUT deny udp any any eq netbios-dgm
PIX1(config)# access-list NO_HIGHRISK_OUT deny tcp any any eq netbios-ssn
PIX1(config)# access-list NO_HIGHRISK_OUT deny udp any any eq 139
PIX1(config)# access-list NO_HIGHRISK_OUT deny tcp any any eq 445
PIX1(config)# access-list NO_HIGHRISK_OUT deny udp any any eq 445
PIX1(config)# access-list NO_HIGHRISK_OUT deny udp any any eq tftp
PIX1(config)# access-list NO_HIGHRISK_OUT deny udp any any eq bootpc
PIX1(config)# access-list NO_HIGHRISK_OUT deny udp any any eq bootps
```

```
PIX1(config)# access-list NO_HIGHRISK_OUT deny udp any any eq snmp
PIX1(config)# access-list NO_HIGHRISK_OUT deny udp any any eq snmptrap
PIX1(config)# access-list NO_HIGHRISK_OUT deny tcp any any eq sqlnet
PIX1(config)# access-list NO_HIGHRISK_OUT deny tcp any any eq 1214
PIX1(config)# access-list NO_HIGHRISK_OUT deny tcp any any eq 3408
PIX1(config)# access-list NO_HIGHRISK_OUT deny tcp any any eq 3531
PIX1(config)# access-list NO_HIGHRISK_OUT permit any any
PIX1(config)# access-group NO_HIGHRISK_OUT out interface Outside
PIX1(config)# exit
```

Czasowe ACL (nowe)

W wersji 7.0 została dodana obsługa czasowych ACL, w których poszczególne wpisy mogą być konfigurowane jako aktywne i egzekwowane we wskazanym okresie. Ta nowa funkcjonalność jest implementowana poprzez nowe polecenie `time-range` i rozszerzenie istniejącego polecenia `access-list` o nowe słowo kluczowe (`time-range`). Aby wprowadzić czasowe ograniczenia wpisu w liście dostępu, należy:

1. Zdefiniować przedział czasu nowym poleceniem `time-range`.
2. Utworzyć lub zmodyfikować wpis w liście dostępu tak, aby używał tego przedziału czasowego, słowem kluczowym `time-range` w poleceniu `access-list`.

Polecenie `time-range` ma składnię:

```
time-range nazwa
```

Parametr *nazwa* przypisuje nazwę do definiowanego przedziału czasowego. Po wprowadzeniu tego polecenia przechodzimy do trybu konfiguracji przedziału czasowego. W tym trybie parametry czasowe definiowane są poleceniami `absolute`, `periodic` i `no`. Polecenie `absolute` definiuje czas bezwzględny, w którym będzie obowiązywać wpis w liście dostępu. Jego składnia wygląda tak:

```
absolute [end czas data] [start czas data]
```

Znaczenie słów kluczowych `start` i `end` jest oczywiste.

Parametr *czas* ma format *GG:MM* (np. `20:00`), a *data* ma format *dzień miesiąc rok* (np. `1 January 2006`).

Polecenie `periodic` definiuje powtarzające się okresy, w których przedział czasu będzie obowiązywał. Ma następującą składnię:

```
periodic dni-tygodnia czas to [dni-tygodnia] czas
```

Parametry i słowa kluczowe polecenia `periodic` mają następującą formę:

Pierwsze wystąpienie parametru *dni-tygodnia* wskazuje początkowy dzień tygodnia przedziału czasowego. Potencjalną wartością parametru może być dowolny pojedynczy dzień lub kombinacja dni: `Monday`, `Tuesday`, `Wednesday`, `Thursday`, `Friday`, `Saturday` i `Sunday`. Oprócz tego dopuszczalne są jeszcze wartości:

- `daily` (codziennie),
- `weekends` (weekendy),
- `weekdays` (dni robocze).

Drugie wystąpienie parametru *dni-tygodnia* wskazuje końcowy dzień tygodnia dla przedziału czasowego. Jest opcjonalne i może być pominięte, jeśli zakres zaczyna się i kończy w tym samym dniu.

Pierwsze wystąpienie parametru *czas* wskazuje początek przedziału czasowego, natomiast drugie oznacza zakończenie przedziału i **nie** jest opcjonalne. Parametr *czas* ma format *GG:MM* (np. `20:00`). W pojedynczym poleceniu `time-range` dozwolone jest stosowanie większej liczby poleceń `periodic`. Oprócz tego, gdy dla polecenia `time-range` są wskazane zarówno wartości `absolute`, jak i `periodic`, polecenia `periodic` są ewaluowane jedynie w okresie bezwzględnego przedziału czasowego, a nie poza nim.

Polecenie `no` przywraca domyślne ustawienia konfiguracji dla słów kluczowych `absolute` i `periodic` polecenia `time-range` — przed wcześniej wpisanym poleceniem wstawiamy słowo kluczowe `no`.

Działanie funkcji przedziałów czasowych zależy oczywiście od dokładności zegara PIX. Zalecana jest synchronizacja zegara PIX z serwerem NTP.

Teraz, po zdefiniowaniu przedziału czasowego poleceniem `time-range`, musimy użyć go do wskazania okresu aktywności wpisu w liście dostępu za pomocą polecenia `access-list`. Ogólna składnia polecenia dla pracy z przedziałami czasowymi ma postać:

```
access-list numer_ACL [line nr_linii] [extended] {deny|permit} {tcp|udp} {host
źródłowe_IP|źródłowe_IP maska|any} [operator port] {host docelowe_IP|docelowe_IP
maska|any} [operator port] time-range nazwa_przedziału
```

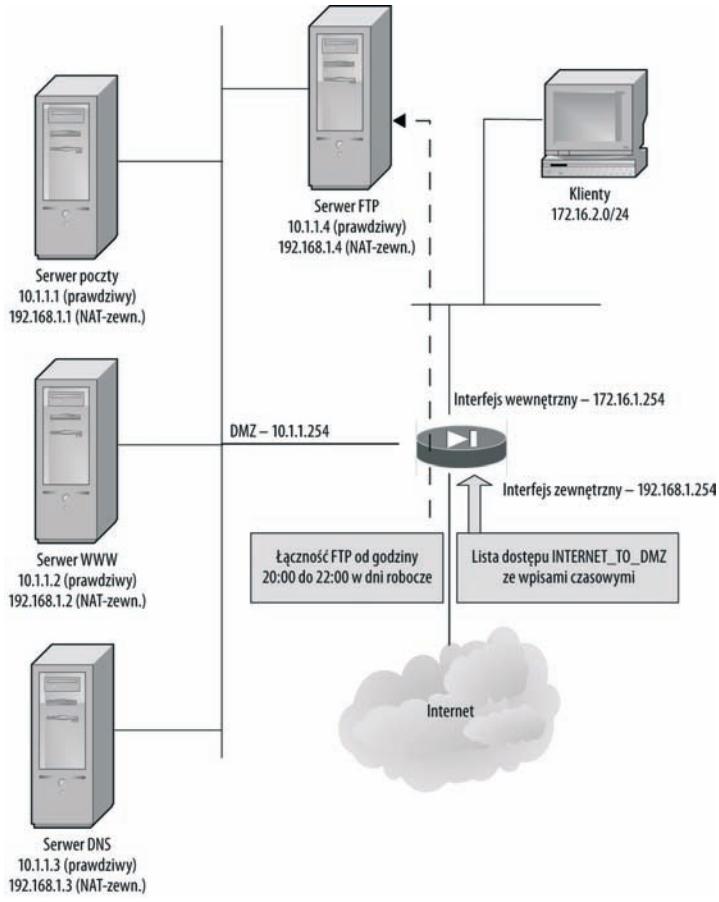
Sposób użycia list dostępu został omówiony w niniejszym rozdziale już wcześniej. Aby instrukcja `access-list` była aktywna tylko we wskazanym przedziale czasu, wystarczy dodać słowo kluczowe `time-range` i parametr *nazwa_przedziału*, którym jest nazwa zdefiniowana wcześniej poleceniem `time-range`.

Załóżmy na przykład, że firma Secure Corporation zainstalowała w strefie zdemilitaryzowanej serwer FTP jako punkt pośredni wymiany plików, jak na rysunku 3.7. Wymiana danych przez FTP odbywa się każdej nocy w dni robocze o wskazanej godzinie. Firma nie chce niepotrzebnie udostępniać serwera FTP, gdy nie jest używany, więc zostały zaimplementowane czasowe ACL, które pozwalają na komunikację FTP do i z serwera tylko wtedy, gdy jest to potrzebne.

Istniejąca lista dostępu `INTERNET_TO_DMZ` została rozbudowana za pomocą poleceń:

```
PIX1(config)# static (dmz, outside) 192.168.1.4 10.1.1.4 netmask 255.255.255.255 0 0
PIX1(config)# time-range PARTNER_FTP_TIME
PIX1(config-time-range)# periodic weekdays 20:00 to 22:00
PIX1(config-time-range)# exit
```

Rysunek 3.7.
Czasowe ACL




```
PIX1(config)# access-list INTERNET_TO_DMZ permit tcp any host 192.168.1.4 eq ftp
time-range PARTNER_FTP_TIME
PIX1(config)# access-list INTERNET_TO_DMZ permit tcp any host 192.168.1.4 eq ftp-
data time-range PARTNER_FTP_TIME
PIX1(config)# access-group INTERNET_TO_DMZ in interface Outside
PIX1(config)# exit
```

Kontrola NAT (nowe)

Wersja 7.0 upraszcza wprowadzanie PIX do eksploatacji, eliminując wymóg definiowania zasad translacji adresów przed pozwoleniem na wychodzenie komunikacji sieciowej z hosta w sieci wewnętrznej do sieci zewnętrznych. Tę funkcję udostępnia nowe polecenie `nat-control`. Po jej włączeniu poleceniem `nat-control` zostaje zachowany uprzedni wymóg zdefiniowania reguł translacji przed dopuszczeniem komunikacji z interfejsu wewnętrznego do interfejsu zewnętrznego PIX. Po wyłączeniu funkcji poleceniem `no nat-control` reguły translacji nie są do tego wymagane.