Łukasz Guziak

KONFIGURACJA USŁUG SIECIOWYCH NA URZĄDZENIACH MIKROTIK

Bezpieczeństwo sieci

Helion

Redaktor prowadzący: Małgorzata Kulik

Projekt okładki: Studio Gravite/Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki

Grafika na okładce została wykorzystana za zgodą AdobeStock.com.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
helion.pl/user/opinie/koussi
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-289-2528-1

Printed in Poland.

Spis treści

Wstęp **5**

ROZDZIAŁ 1. **Ochrona. Podstawy** **7**
1.1. Nazwy i komentarze 8
1.2. Ustawienia czasu 10
1.3. Safe Mode 13
1.4. Identyfikacja usług, zmiana ich ustawień, wyłączenie zbędnych usług 16
1.5. Połączenie SSH za pomocą kluczy 20
1.6. Logowanie do routera/switcha z określonego hosta 24
1.7. Skrypty 25
1.8. Aktualizacja systemu 28
1.9. Neighbor Discovery 31
1.10. Wyłączenie niewykorzystywanych interfejsów 36
1.11. E-mail 37
1.12. Kopia ustawień urządzenia 38
1.13. Dostęp do urządzenia, warstwa 2. 43
1.13.1. MAC Telnet Server 44
1.13.2. MAC WinBox Server 47
1.13.3. MAC ping server 48
1.14. Hasła. Jak je zapamiętać? 50

ROZDZIAŁ 2. **Dostęp fizyczny do urządzenia** **52**
2.1. Blokada ekranu LCD 52
2.2. Console Port 54

ROZDZIAŁ 3. **Konta, grupy. Uwierzytelnienie za pomocą serwera RADIUS** **56**
3.1. Logowanie za pomocą konta lokalnego 56
3.1.1. Zarządzanie kontami 57
3.1.2. Logowanie za pomocą SSH 59
3.2. Logowanie za pomocą serwera RADIUS 64

ROZDZIAŁ 4. **Logowanie zdarzeń** **74**
4.1. Lokalne logowanie zdarzeń 75
4.2. Logowanie zdarzeń za pomocą zdalnego serwera 78
4.3. Logowanie zdarzeń via e-mail 83

ROZDZIAŁ 5. **MACVLAN** **89**

ROZDZIAŁ 6. **MACSec** **97**
6.1. Konfiguracja łącza MACSec 98
6.2. Konfiguracja łącza MACSec w sieciach VLAN 107

ROZDZIAŁ 7. **Port knocking** 121

ROZDZIAŁ 8. **Atak na serwer DHCP** 130
8.1. DHCP Starvation 130
8.2. DHCP Spoofing 138

ROZDZIAŁ 9. **Protokół dot1x** 144
9.1. MAC Authentication 144
9.2. Uwierzytelnienie za pomocą loginu i hasła 153
9.3. Dot1x w sieciach VLAN 157

ROZDZIAŁ 10. **Protokół IPSec** 168
10.1. Wprowadzenie do protokołu IPSec 168
10.2. Konfiguracja początkowa 175
10.3. Konfiguracja tunelu IPSec 178

ROZDZIAŁ 11. **Packet flow** 193
11.1. Wprowadzenie do packet flow 193
11.2. Przykład 1. — połączenie z routerem 197
11.3. Przykład 2. — komunikacja w ramach wspólnego bridge'a 198
11.4. Przykład 3. — wymiana danych pomiędzy interfejsami nienależącymi do bridge'a 199
11.5. Przykład 4. — dwa oddzielne bridge'e 199

ROZDZIAŁ 12. **Firewall** 201
12.1. Blokada połączenia z Facebookiem 201
12.2. Określenie czasu logowania 206
12.3. Zapobieganie atakom brute force 210
12.4. Filtrowanie ruchu DNS 228
12.4.1. Mechanizm DST-NAT 228
12.4.2. Static DNS 231
12.5. ICMP 234
12.5.1. ICMP flood 235
12.5.2. ICMP Smurf 237
12.5.3. Narzędzia diagnostyczne 239
12.6. Mangle firewall 245
12.7. Blokada połączenia z YouTube'em 253
12.8. Wykrywanie i blokada skanowania portów 258
12.9. RAW Firewall 263
12.10. Atak SYN flood 267
12.11. UDP flood 274

ROZDZIAŁ 13. **Dostęp fizyczny do urządzenia** 283

ROZDZIAŁ 14. **Docker na urządzeniach MikroTik** 287
14.1. Wirtualizacja vs konteneryzacja 287
14.2. Konfiguracja funkcji Container 288
14.3. Instalacja Pi-hole na dysku wewnętrznym routera 292
14.4. Instalacja na nośniku zewnętrznym 305

DODATEK **Certyfikacja MikroTik** 313

ROZDZIAŁ 7.

Port knocking

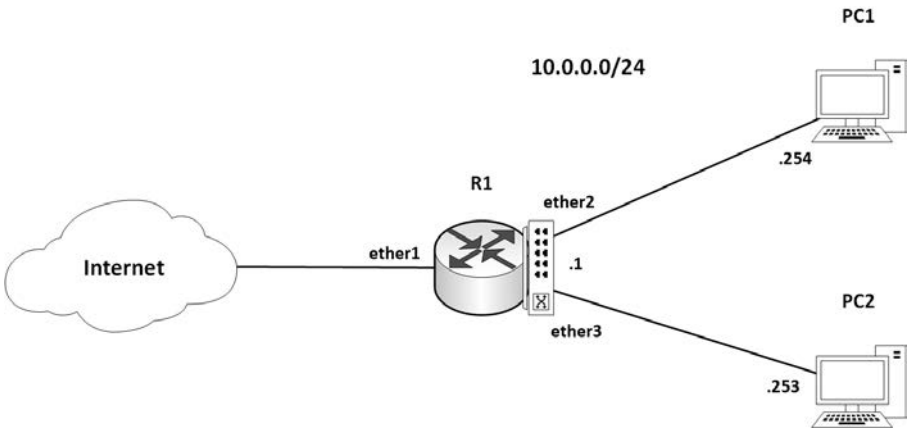
Port knocking to technika stosowana w celu zabezpieczenia dostępu do usług sieciowych. Na urządzeniach MikroTik jest stosowana w celu uzyskania dostępu do urządzenia. **Dostęp do panelu zarządzania lub terminala jest możliwy po wykonaniu w odpowiedniej kolejności sekwencji „puknięć" na określone porty.** Router monitoruje ruch sieciowy po rozpoznaniu poprawnej sekwencji, dynamicznie modyfikuje reguły firewalla, tak aby host mógł z nim nawiązać połączenie.

W tym rozdziale:

- Zabezpieczysz sieć za pomocą techniki port knocking.

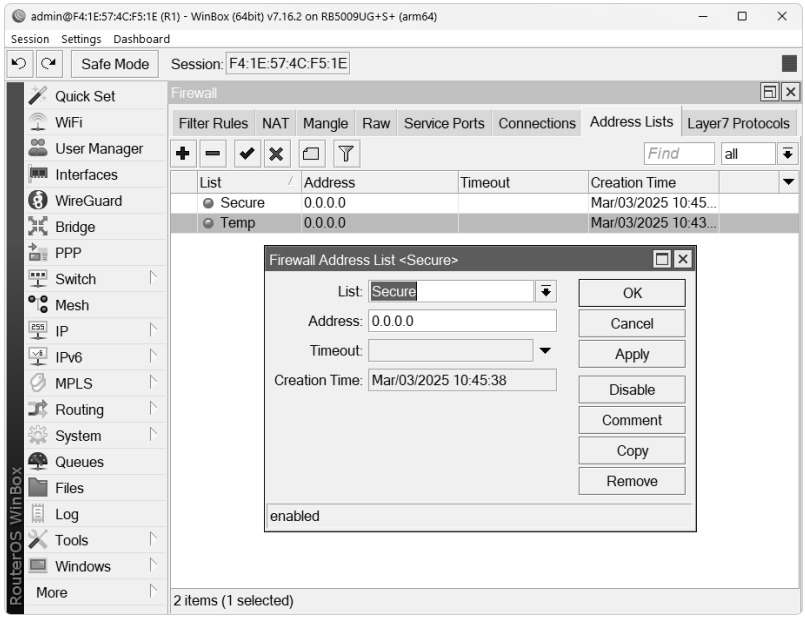
Port knocking działa w warstwie trzeciej modelu ISO/OSI — oznacza to, że wykorzystuje adresy IP. Po skonfigurowaniu funkcji połączenie z routerem będzie mogło zostać wykonane z określonego adresu IP.

Topologia sieciowa została pokazana na rysunku 7.1. Komputer *PC1* uzyska dostęp do panelu zarządzania routera *R1* tylko wtedy, gdy wykonana została sekwencja dwóch połączeń. W pierwszym połączeniu musi zostać użyty port *TCP* o numerze *6677*, zaś w drugim port *TCP 7788*. Czas nawiązania drugiego połączenia nie może przekroczyć jednej minuty. Drugi komputer *PC2* z routerem *R1* nawiąże sesje SSH.



RYSUNEK 7.1. Topologia sieciowa

Konfigurację rozpoczynamy od utworzenia dwóch list o nazwach *Secure* oraz *Temp*. Do pierwszej listy zostaną przypisane urządzenia zdalne, które nawiązały z routerem połączenie, druga lista jest tymczasowa dla urządzeń, które próbują nawiązać połączenie. Listy tworzy się na zakładce *Address Lists* w opcjach zapory sieciowej (z menu wybierz *IP*, a następnie *Firewall*) — rysunek 7.2.



RYSUNEK 7.2. Router R1, utworzenie list

Kolejnym etapem jest konfiguracja reguł. Zadaniem pierwszej reguły będzie dodanie wpisu do listy *Temp*. Każdy host, który nawiąże połączenie z routerem na porcie *TCP* o numerze *6677*, zostanie dodany do tej listy.

Po otwarciu zakładki *Filter Rules* i wybraniu ikony plusa na karcie *General* uzupełnij pola (rysunek 7.3):

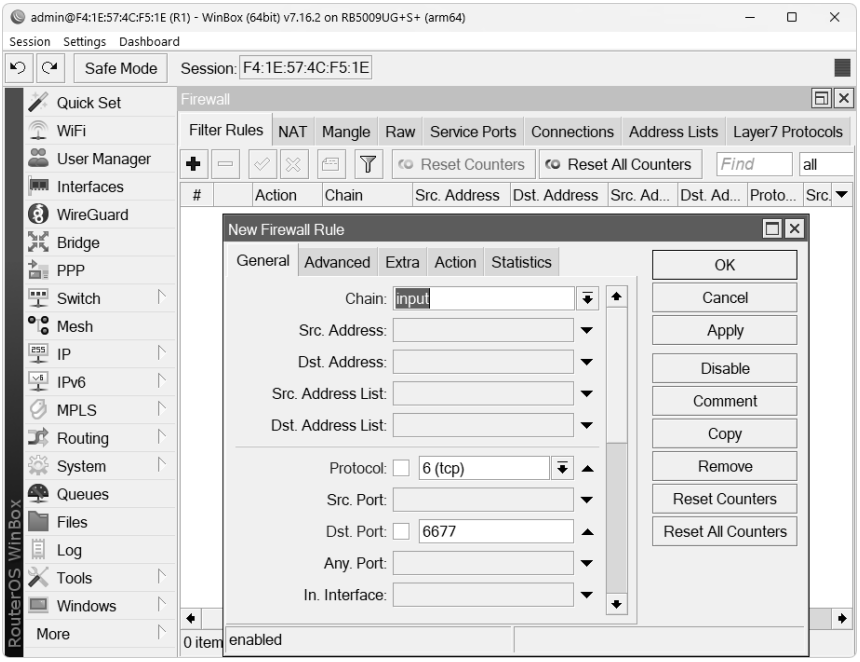
- *Chain*: wybierz *input* (ponieważ połączenie jest realizowane z routerem);
- *Protocol*: wskaż *tcp*;
- *Dst. Port*: wpisz numer portu *6677*.

To nie koniec konfiguracji reguły — kolejne ustawienia znajdują się na karcie *Action*. Z rozwijanej listy w polu *Action* wybierz ustawienie *add src to address list*, w polu *Address List* wskaż listę *Temp*, zaś w polu *Timeout* określ czas (*00:01:00*, jedna minuta), po którym host zostanie usunięty z listy. Na czas konfiguracji i testowania mechanizmu można włączyć logowanie wystąpienia zdarzenia, zaznacz opcję *Log* — rysunek 7.4.

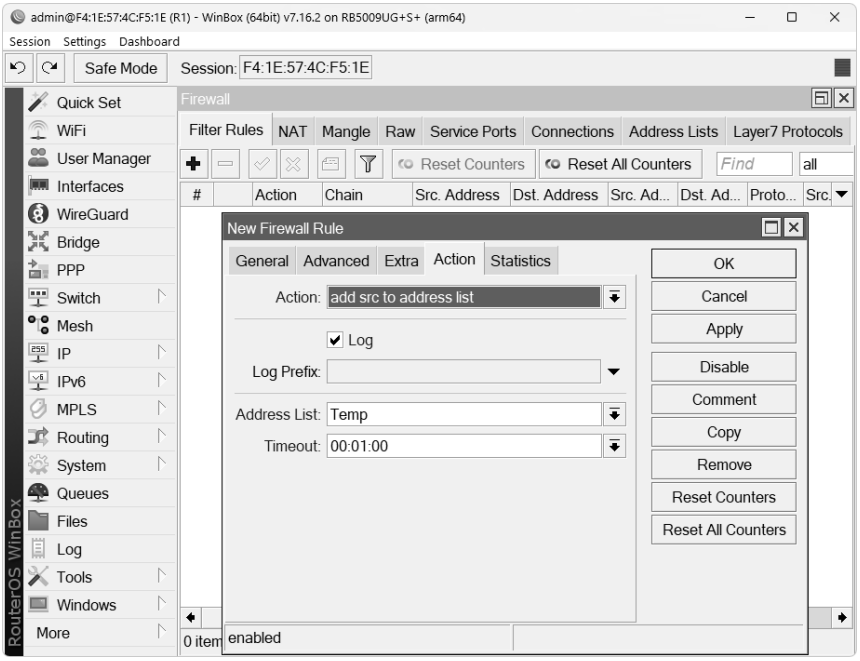
Aby mechanizm działał poprawnie, niezbędna jest druga reguła — jej zadaniem będzie dodanie hosta do listy *Secure*, ale tylko pod warunkiem, że znajduje się on na liście tymczasowej *Temp* i nawiązał połączenie z portem *TCP 7788*.

Na zakładce *Filter Rules* ponownie wybierz ikonę plusa i po otwarciu nowego okna (karta *General*) skonfiguruj pola (rysunek 7.5):

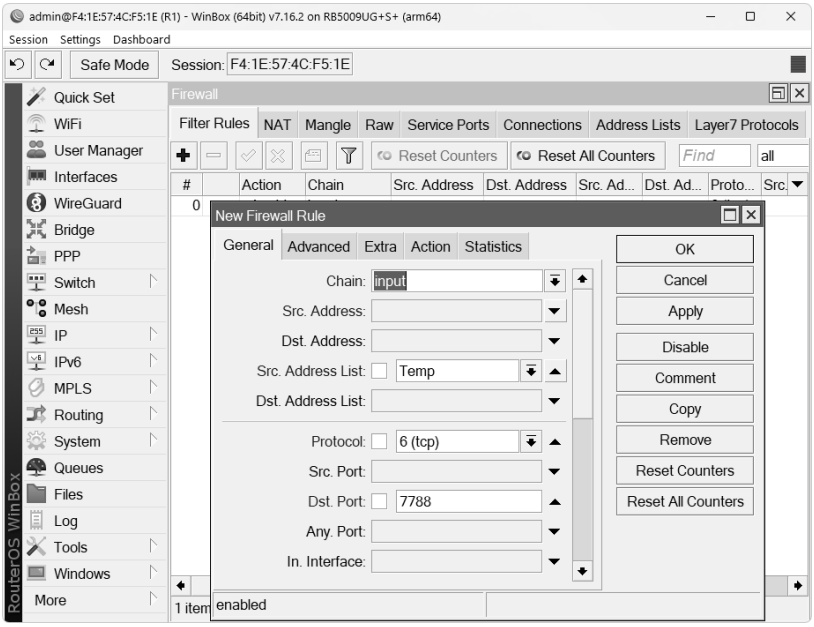
- *Chain*: wybierz *input*;
- *Src. Address List*: wybierz listę tymczasową *Temp*;
- *Protocol*: wskaż *tcp*;
- *Dst. Port*: wpisz numer portu *7788*.



RYSUNEK 7.3. Router R1, karta General, konfiguracja reguły

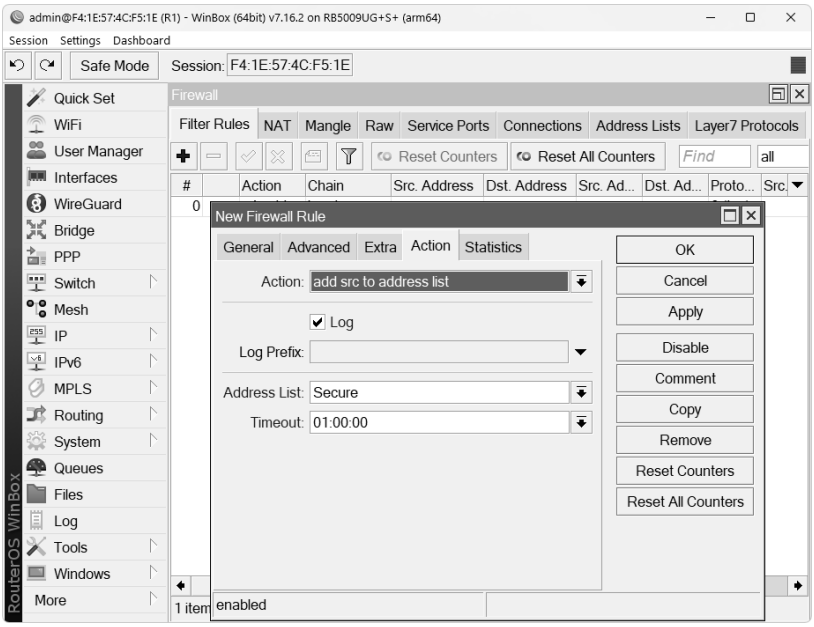


RYSUNEK 7.4. Router R1, karta Action, konfiguracja reguły



RYSUNEK 7.5. Router R1, karta General, konfiguracja reguły

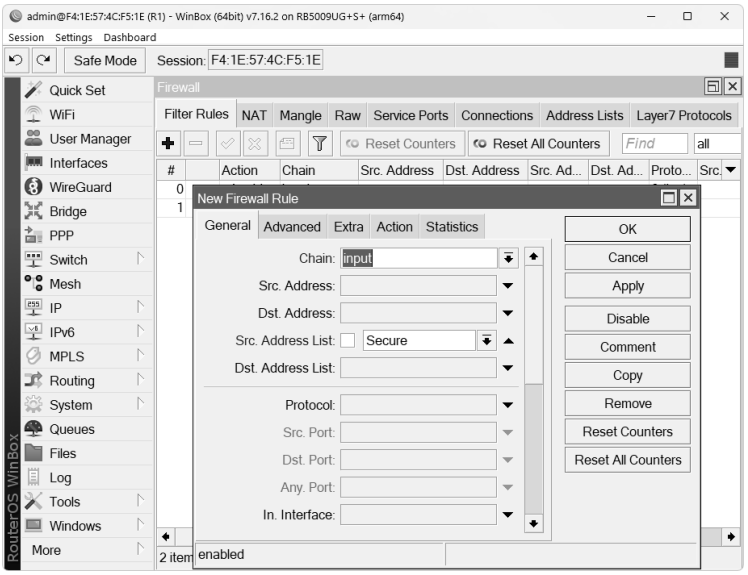
Identycznie jak podczas konfiguracji poprzedniej reguły, na karcie *Action* z rozwijanej listy w polu *Action* wybierz ustawienie *add src to address list*, w polu *Address List* wskaż listę *Secure*, zaś w polu *Timeout* określ czas (*01:00:00*, jedna godzina), po którym host zostanie usunięty z listy — rysunek 7.6.



RYSUNEK 7.6. Router R1, karta Action, konfiguracja reguły

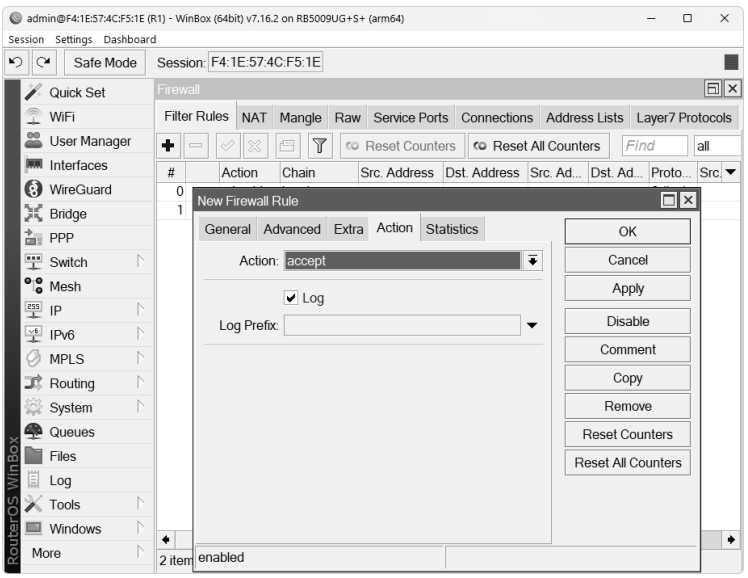
To nie koniec tworzenia reguł, należy bowiem utworzyć kolejne dwie — reguła numer trzy zezwoli na nawiązanie połączenia z routerem hostom znajdującym się na liście *Secure*, zaś czwarta zabroni tego wszystkim innym.

Po otwarciu okna tworzenia nowej reguły uzupełnij pola *Chain* i *Src. Address Lists* kolejno wartościami *input* i *Secure* — rysunek 7.7.



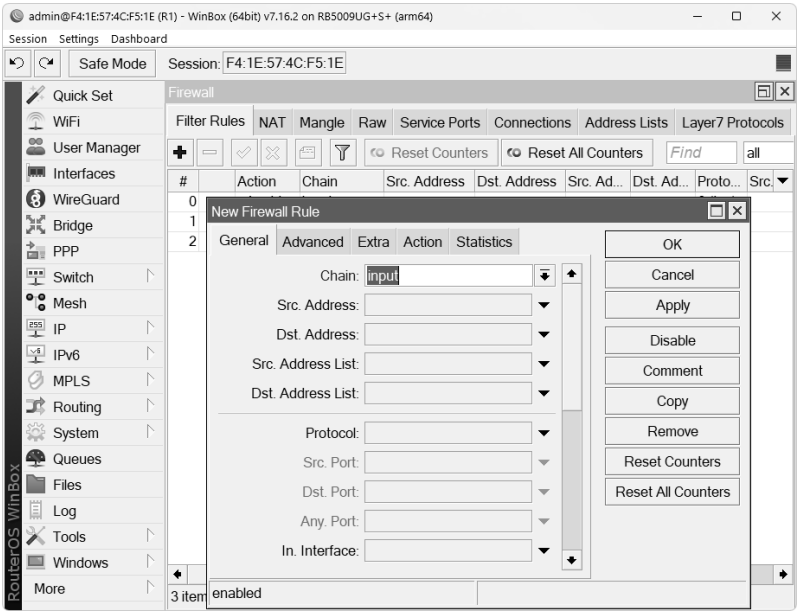
RYSUNEK 7.7. Router R1, karta General, konfiguracja reguły

Na karcie *Action*, w polu *Action*, wybierz ustawienie *accept* — rysunek 7.8.



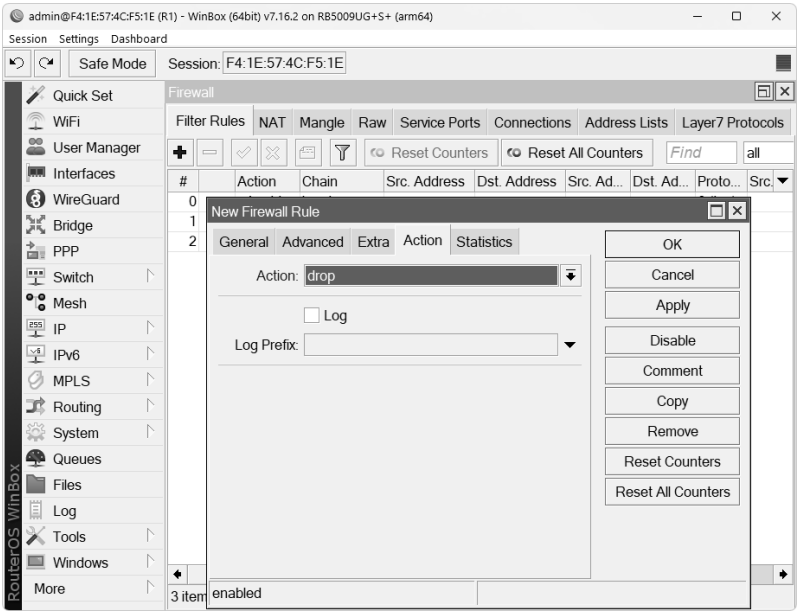
RYSUNEK 7.8. Router R1, karta Action, konfiguracja reguły

Ustawienie blokady połączenia z routerem dla pozostałych urządzeń wymaga wykonania dwóch ustawień. Po utworzeniu nowej reguły w polu *Chain* wskaż *input* — rysunek 7.9.



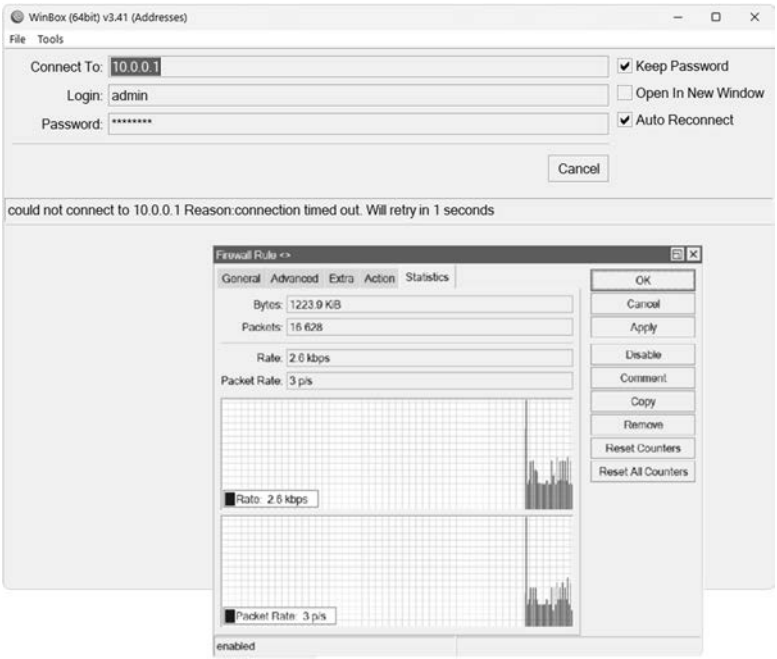
RYSUNEK 7.9. Router R1, karta General, konfiguracja reguły

Na karcie *Action*, w polu *Action*, wybierz ustawienie *drop* — rysunek 7.10.



RYSUNEK 7.10. Router R1, karta Action, konfiguracja reguły

Mechanizm port knocking został skonfigurowany, sprawdźmy zatem, jak działa — z komputera *PC1* (IP *10.0.0.254*) następuje próba połączenia z routerem (IP *10.0.0.1*), lecz kończy się ona niepowodzeniem. Ponieważ host nie znajduje się na liście *Security*, próba połączenia zostaje zablokowana (zadziała ostatnia reguła *drop*) — rysunek 7.11.



RYSUNEK 7.11. Blokada połączenia z routerem R1

Aby można było nawiązać połączenie z routerem, należy sprawić, aby informacja o hoście *PC1* została dodana do listy *Temp*, a następnie *Secure*. Zatem wykonajmy to.

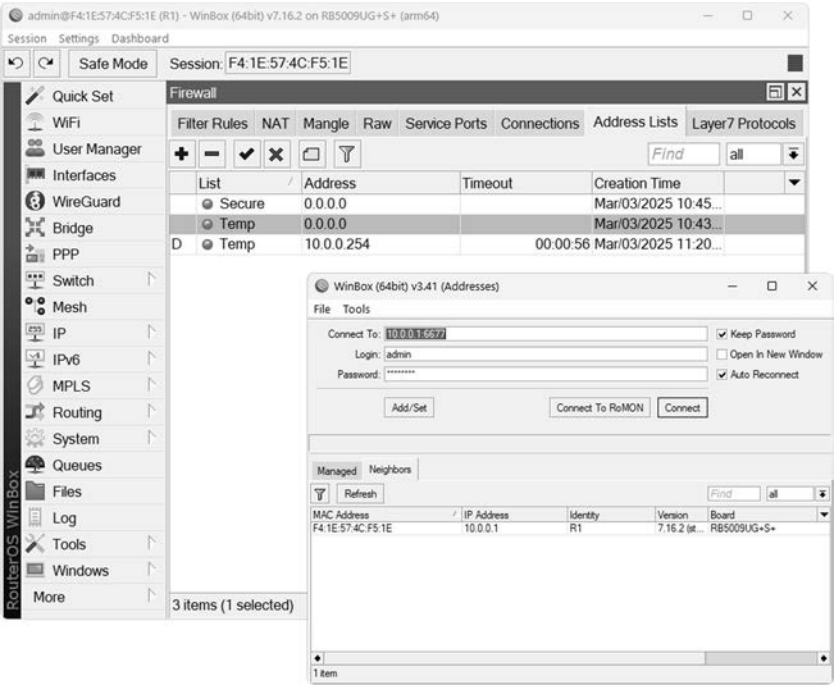
Dodanie hosta *PC1* do listy *Temp* nastąpi po nawiązaniu połączenia z routerem na porcie *TCP 6677* (IP *10.0.0.1:6677*). Na liście tej wpis będzie widniał przez minutę, co oznacza, że tyle mamy czasu, aby wykonać krok drugi, czyli nawiązać drugie połączenie z portem *TCP 7788* — rysunek 7.12.

Po nawiązaniu drugiego połączenia (IP *10.0.0.1:7788*) host nawiązujący połączenie zostaje umieszczony na liście *Secure* — przez godzinę ma on dostęp do routera. Po tym czasie zostanie usunięty z listy *Secure* — rysunek 7.13.

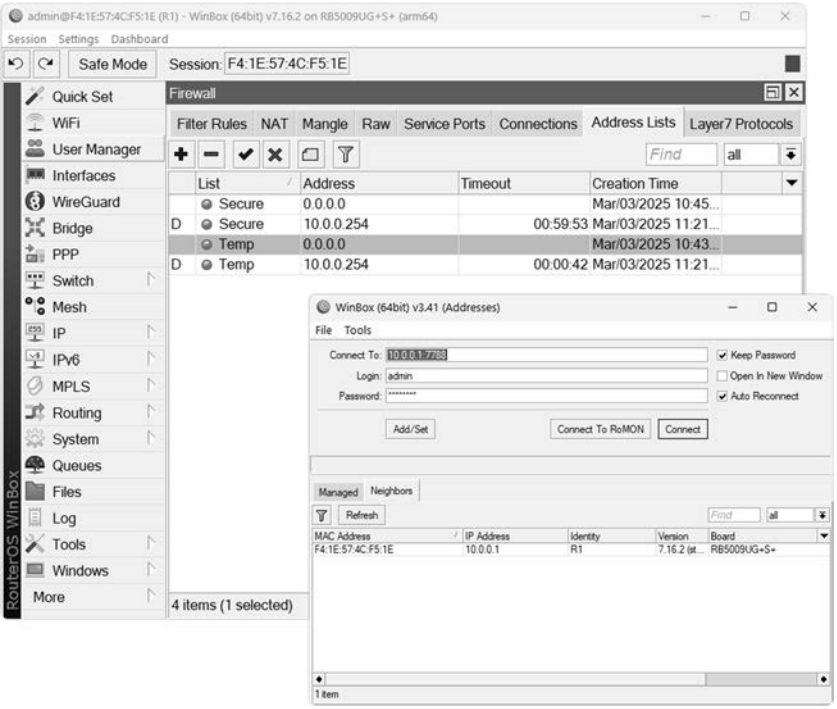
Ponieważ podczas konfiguracji włączyliśmy logowanie reguł, w dzienniku urządzenia odnajdziemy wpisy, które świadczą o ich wykonaniu. Ich treść będzie podobna do tych zaprezentowanych poniżej:

input: in:bridge1 out:(unknown 0), connection-state:new src-mac 24:5e:be:64:96:8e, proto TCP (SYN), 10.0.0.254:48031->10.0.0.1:6677, len 52;

input: in:bridge1 out:(unknown 0), connection-state:new src-mac 24:5e:be:64:96:8e, proto TCP (SYN), 10.0.0.254:48082->10.0.0.1:7788, len 52.

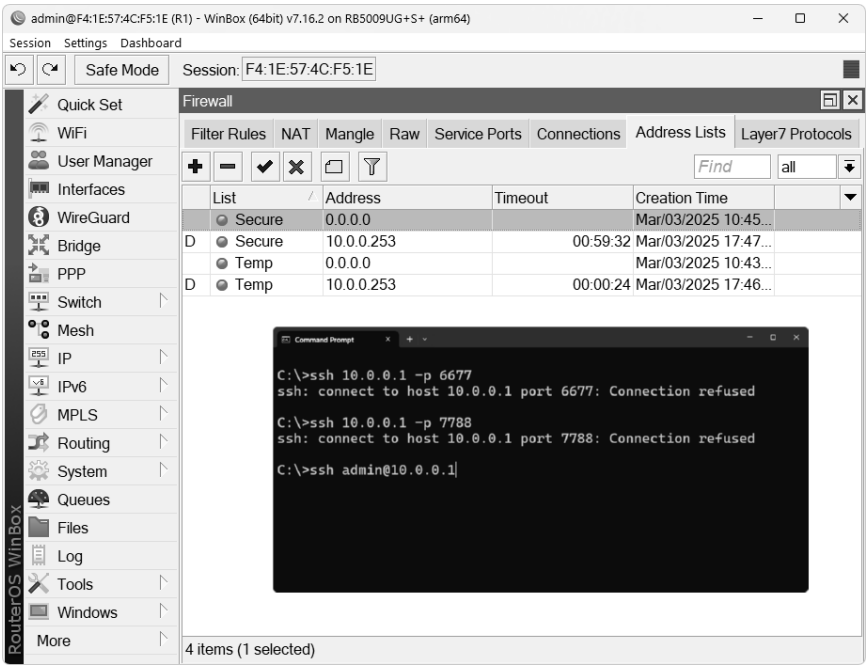


RYSUNEK 7.12. Nawiązanie pierwszego połączenia (10.0.0.1:6677), dodanie informacji do listy Temp



RYSUNEK 7.13. Nawiązanie drugiego połączenia (10.0.0.1:7788), dodanie informacji do listy Secure

Identyczne działanie należy wykonać, aby host *PC2* (IP *10.0.0.253*) mógł połączyć się z routerem za pomocą protokołu SSH. Najpierw wykonujemy połączenie z portem *TCP 6677*, następnie z portem *TCP 7788* i ostatecznie uzyskujemy dostęp do wiersza poleceń urządzenia — rysunek 7.14.



RYSUNEK 7.14. Komputer PC2, nawiązanie sesji SSH z routerem R1

Konfiguracja port knocking może zostać wykonana w terminalu. Polecenia, jakich należy użyć, zostały pokazane na listingu 7.1.

LISTING 7.1. Konfiguracja mechanizmu port knocking

```
#utworzenie list
ip firewall address-list add list=Temp
ip firewall address-list add list=Secure

#utworzenie reguł
#reguła 1 — nawiązanie połączenia z portem TCP 6677, dodanie hosta do listy Temp
ip firewall filter add action=add-src-to-address-list address-list=Temp address-list
↪-timeout=1m chain=input dst-port=6677 log=yes protocol=tcp

#reguła 2 — nawiązanie połączenia z portem TCP 7788, dodanie hosta do listy Secure
ip firewall filter add action=add-src-to-address-list address-list=Secure address-list
↪-timeout=1h chain=input dst-port=7788 log=yes protocol=tcp src-address-list=Temp

#reguła 3 — pozwolenie na nawiązanie połączenia z urządzeniem hostom, które znajdują się na liście Secure
ip firewall filter add action=accept chain=input src-address-list=Secure

#reguła 4 — zabronienie połączenia z routerem wszystkim innym urządzeniom
ip firewall filter add action=drop chain=input
```


PROGRAM
PARTNERSKI
GRUPY HELION
1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ
Zmień swoją stronę WWW w działający bankomat!
Dowiedz się więcej i dołącz już dzisiaj!
http://program-partnerski.helion.pl
GRUPA
Helion

KONFIGURACJA USŁUG SIECIOWYCH NA URZĄDZENIACH MIKROTIK

Bezpieczeństwo sieci

Zadbaj o bezpieczeństwo sieci MikroTik

W dobie powszechnej cyfryzacji, gdy niemal każda dziedzina życia została przeniesiona do sieci, kwestia bezpieczeństwa i ochrony danych nabrała kluczowego znaczenia. Administrator powinien nieustannie śledzić zmieniające się zagrożenia, a także posiadać praktyczną wiedzę na temat technik zabezpieczania środowisk sieciowych.

Ta książka zawiera omówienie zarówno podstawowych, jak i zaawansowanych aspektów związanych z bezpieczeństwem sieci opartych na rozwiązaniach MikroTik. To kontynuacja cyklu Łukasza Guziaka poświęconego specyfice urządzeń firmy MikroTik, które stanowią alternatywę dla sprzętu marki Cisco. **Pozycja ta pozwoli Ci się przygotować do egzaminu MTCSE (MikroTik Certified Security Engineer).**

W książce znajdziesz między innymi takie zagadnienia jak:

- **protokoły bezpieczeństwa**
- **metody szyfrowania**
- **zarządzanie dostępem**
- **logowanie zdarzeń**
- **filtrowanie ruchu sieciowego**
- **symulacja ataków sieciowych**
- **sposoby zapobiegania atakom na sieci MikroTik**
- **konteneryzacja**

Helion
helion.pl
HELION S.A.
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej!

ISBN 978-83-289-2528-1

Cena: 89,00 zł