

Praca magisterska



Analiza możliwości wykorzystania interfejsu
WWW do definiowania zestawu reguł zapory
sieciowej

Autor: **Robert Korulczyk**

Promotor: **Dr inż. Grzegorz Koziel**

Cel i zakres pracy

Celem pracy jest zbadanie możliwości wykorzystania interfejsu WWW do definiowania reguł zapory sieciowej w systemie Linux.

Zakres pracy obejmuje następujące zagadnienia:

- Omówienie mechanizmów odpowiedzialnych za konfigurację zapory w systemie Linux;
- Omówienie technologii wykorzystanych do stworzenia graficznego interfejsu, pozwalającego na definiowanie reguł iptables;
- Stworzenie aplikacji internetowej, pozwalającej na graficzne definiowanie hostów i reguł dla zapory sieciowej;
- Testy aplikacji i analiza osiągniętych wyników.

Iptables

Iptables jest konsolowym programem działającym w przestrzeni użytkownika, który pozwala na konfigurowanie reguł odpowiedzialnych za filtrowanie pakietów sieciowych. Sam w sobie nie odpowiada jednak za filtrowanie pakietów – jest jedynie narzędziem pozwalającym skonfigurować odpowiednie mechanizmy zaimplementowane w jądrze Linuksa.

Składnia polecenia iptables:

```
iptables [-t tablica] komenda [wzorzec] [-j akcja]
```

Opis aplikaciji

Advanced Web-Based Iptables Rules Generator

[Home](#) [About](#) [Contact](#) [Login](#)

[Home](#) » [Login](#)

Login

Please fill out the following form with your login credentials:

*Fields with * are required.*

Username *

Password *

Hint: You may login with admin/admin.

Remember me next time

Opis aplikacji

Advanced Web-Based Iptables Rules Generator

[Home](#) [Configs](#) [Users](#) [About](#) [Contact](#) [Logout \(admin\)](#)

[Home](#) » [Configs](#) » [sieć 1](#) » Update

Update Config 1

*Fields with * are required.*

Name *

Command

Description

Global Vars

```
clear_tables="filter;nat;mangle"
clear_types="-F;-X"
default_drop="INPUT;FORWARD"
default_accept="OUTPUT"
chains="OUTPUT;INPUT;FORWARD"
```

Operations

[List Configs](#)

[Create Config](#)

[View Config](#)

[Manage Configs](#)

Opis aplikacji

Advanced Web-Based Iptables Rules Generator

[Home](#) [Configs](#) [Users](#) [About](#) [Contact](#) [Logout \(admin\)](#)

[Home](#) » [Configs](#) » [sieć 1](#) » [Rules](#) » [4](#) » **Update**

[Rules](#) [Hosts](#) [Groups](#) [Chains](#)

Update Rule 4

*Fields with * are required.*

Content *

```
-t {clear_tables} {clear_types}
```

Priority

Operations

[List Rules](#)

[Create Rule](#)

[View Rule](#)

[Manage Rules](#)

Opis aplikaciji

`iptables -t filter -F;`

`iptables -t filter -X;`

`iptables -t nat -F;`

`iptables -t nat -X;`

`iptables -t mangle -F;`

`iptables -t mangle -X;`

Opis aplikaciji

Rules

Displaying 1-7 of 7 results.

ID: [4](#)

Content: -t {clear_tables} {clear_types}

Priority: -200

ID: [5](#)

Content: -P {default_accept} ACCEPT

Priority: 1

ID: [6](#)

Content: -P {default_drop} DROP

Priority: 1

ID: [7](#)

Content: -A INPUT -d {ip} -p tcp --dport {tcp_in_open} -j ACCEPT

Priority: 50

ID: [9](#)

Content: -A INPUT -d {ip} -p tcp --dport {ssh_port} -j ssh_check

Priority: 50

ID: [8](#)

Content: -A INPUT -d {ip} -p tcp --dport {ssh_port} -j ACCEPT

Priority: 51

ID: [10](#)

Content: -A {chains} -m state --state ESTABLISHED,RELATED -j ACCEPT

Priority: 100

Operations

[Create Rule](#)

[Manage Rules](#)

Opis aplikacji

Advanced Web-Based Iptables Rules Generator

[Home](#) [Configs](#) [Users](#) [About](#) [Contact](#) [Logout \(admin\)](#)

[Home](#) » [Configs](#) » [sieć 1](#) » **Hosts**

[Rules](#) [Hosts](#) [Groups](#) [Chains](#)

Hosts

Displaying 1-3 of 3 results.

Name: [serwer pocztowy](#)
Address: 192.168.1.101
Vars: tcp_in_open="587;465;110;995;143;993" ssh_port="1101"

Name: [serwer www 1](#)
Address: 192.168.1.102
Vars: ssh_port="1102"

Name: [serwer www 2](#)
Address: 192.168.1.103
Vars: ssh_port="1103"

Operations

[Create Host](#)

[Manage Hosts](#)

Opis aplikacji

Advanced Web-Based Iptables Rules Generator

[Home](#) [Configs](#) [Users](#) [About](#) [Contact](#) [Logout \(admin\)](#)

[Home](#) » [Configs](#) » [sieć 1](#) » [Groups](#) » [serwery www](#)

[Rules](#) [Hosts](#) [Groups](#) [Chains](#)

View Group #1

ID	1
Name	serwery www
Vars	tcp_in_open="80;443;21"

Hosts:

- [serwer www 1](#) (192.168.1.102) - ssh_port="1102"
- [serwer www 2](#) (192.168.1.103) - ssh_port="1103"

Assigned to Rules:

- [-A INPUT -d {ip} -p tcp -dport {tcp_in_open} -j ACCEPT](#)

Operations

- [List Groups](#)
- [Create Group](#)
- [Update Group](#)
- [Delete Group](#)
- [Manage Groups](#)
- [Add Hosts to Group](#)
- [Delete Hosts from Group](#)

Opis aplikaciji

Advanced Web-Based Iptables Rules Generator

[Home](#) [Configs](#) [Users](#) [About](#) [Contact](#) [Logout \(admin\)](#)

[Home](#) » [Configs](#) » [sieć 1](#) » [Hosts](#) » serwer www 1

[Rules](#) [Hosts](#) [Groups](#) [Chains](#)

View Host #2

ID	2
Name	serwer www 1
Address	192.168.1.102
Vars	ssh_port="1102"

Operations

[List Hosts](#)
[Create Host](#)
[Update Host](#)
[Delete Host](#)
[Manage Hosts](#)

In Groups:

- [serwery www](#) - tcp_in_open="80;443;21"
 - [-A INPUT -d {ip} -p tcp --dport {tcp_in_open} -j ACCEPT](#)

Assigned to Rules:

- [-A INPUT -d {ip} -p tcp --dport {ssh_port} -j ssh_check](#)
- [-A INPUT -d {ip} -p tcp --dport {ssh_port} -j ACCEPT](#)

Opis aplikacji

Advanced Web-Based Iptables Rules Generator

[Home](#) [Configs](#) [Users](#) [About](#) [Contact](#) [Logout \(admin\)](#)

[Home](#) » [Configs](#) » [sieć 1](#) » [Chains](#) » [ssh_check](#)

[Rules](#) [Hosts](#) [Groups](#) [Chains](#)

View Chain #1

ID	1
Name	ssh_check

Rules:

- [-m recent --rdest --rcheck --hitcount 3 --seconds 60 -j LOG --log-prefix "SSH attack: "](#)
- [-m recent --rdest --rcheck --hitcount 3 --seconds 60 -j DROP](#)
- [-m recent --rdest --set -j RETURN](#)

Operations

- [List Chains](#)
- [Create Chain](#)
- [Update Chain](#)
- [Delete Chain](#)
- [Manage Chains](#)
- [Add Rule to Chain](#)

Opis aplikacji

Advanced Web-Based Iptables Rules Generator

[Home](#) [Configs](#) [Users](#) [About](#) [Contact](#) [Logout \(admin\)](#)

[Home](#) » [Configs](#) » sieć 1

[Rules](#) [Hosts](#) [Groups](#) [Chains](#)

View Config #1

Name	sieć 1
Description	Testowa sieć nr 1.
Command	iptables
Global Vars	clear_tables="filter;nat;mangle" clear_types="-F;-X" default_drop="INPUT;FORWARD" default_accept="OUTPUT" chains="OUTPUT;INPUT;FORWARD"

- Hosts: [3](#)
- Groups: [1](#)
- Chains: [1](#)
- Rules: [7](#)

Operations

- [List Configs](#)
- [Create Config](#)
- [Update Config](#)
- [Delete Config](#)
- [Manage Config](#)
- [Generate Rule Set](#)

Opis aplikaciji

Advanced Web-Based Iptables Rules Generator

[Home](#) [Configs](#) [Users](#) [About](#) [Contact](#) [Logout \(admin\)](#)

[Home](#) » [Configs](#) » [sieć 1](#) » **Generated Rule Set**

[Rules](#) [Hosts](#) [Groups](#) [Chains](#)

Rule Set for Config #1

Log

Rule Set

```
iptables -t filter -F;
iptables -t filter -X;
iptables -t nat -F;
iptables -t nat -X;
iptables -t mangle -F;
iptables -t mangle -X;
iptables -N ssh_check;
iptables -A ssh_check -m recent --rdest --rcheck --hitcount 3 --seconds 60 -j LOG --log-prefix "SSH
attack: ";
iptables -A ssh_check -m recent --rdest --rcheck --hitcount 3 --seconds 60 -j DROP;
iptables -A ssh check -m recent --rdest --set -j RETURN;
```

Raw Link <http://webtests/awbirg/config/generateRaw/?hash=b9daf857bd13eaa5ae65e2c025fe>

Operations

- [List Config](#)
- [View Config](#)
- [Create Config](#)
- [Update Config](#)
- [Delete Config](#)
- [Manage Config](#)

Wygenerowane reguły

```
iptables -t filter -F;
iptables -t filter -X;
iptables -t nat -F;
iptables -t nat -X;
iptables -t mangle -F;
iptables -t mangle -X;
iptables -N ssh_check;
iptables -A ssh_check -m recent --rdest --rcheck --hitcount 3 --seconds 60 -j LOG --log-prefix
"SSH attack: ";
iptables -A ssh_check -m recent --rdest --rcheck --hitcount 3 --seconds 60 -j DROP;
iptables -A ssh_check -m recent --rdest --set -j RETURN;
iptables -P OUTPUT ACCEPT;
iptables -P INPUT DROP;
iptables -P FORWARD DROP;
iptables -A INPUT -d 192.168.1.101 -p tcp --dport 587 -j ACCEPT;
iptables -A INPUT -d 192.168.1.101 -p tcp --dport 465 -j ACCEPT;
iptables -A INPUT -d 192.168.1.101 -p tcp --dport 110 -j ACCEPT;
iptables -A INPUT -d 192.168.1.101 -p tcp --dport 995 -j ACCEPT;
iptables -A INPUT -d 192.168.1.101 -p tcp --dport 143 -j ACCEPT;
iptables -A INPUT -d 192.168.1.101 -p tcp --dport 993 -j ACCEPT;
iptables -A INPUT -d 192.168.1.102 -p tcp --dport 80 -j ACCEPT;
```

Wygenerowane reguły

```
iptables -A INPUT -d 192.168.1.102 -p tcp --dport 443 -j ACCEPT;
iptables -A INPUT -d 192.168.1.102 -p tcp --dport 21 -j ACCEPT;
iptables -A INPUT -d 192.168.1.103 -p tcp --dport 80 -j ACCEPT;
iptables -A INPUT -d 192.168.1.103 -p tcp --dport 443 -j ACCEPT;
iptables -A INPUT -d 192.168.1.103 -p tcp --dport 21 -j ACCEPT;
iptables -A INPUT -d 192.168.1.101 -p tcp --dport 1101 -j ssh_check;
iptables -A INPUT -d 192.168.1.102 -p tcp --dport 1102 -j ssh_check;
iptables -A INPUT -d 192.168.1.103 -p tcp --dport 1103 -j ssh_check;
iptables -A INPUT -d 192.168.1.101 -p tcp --dport 1101 -j ACCEPT;
iptables -A INPUT -d 192.168.1.102 -p tcp --dport 1102 -j ACCEPT;
iptables -A INPUT -d 192.168.1.103 -p tcp --dport 1103 -j ACCEPT;
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT;
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT;
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT;
```


Opis aplikaciji

```
root@awbirg1:~# wget -O rules -o output http://webtests/awbirg/config/generateRaw/?hash=b9daf857bd13eaa5ae65e2c025fe7791107423aa
root@awbirg1:~# chmod +x rules
root@awbirg1:~# bash rules
root@awbirg1:~# iptables --list
Chain INPUT (policy DROP)
target     prot opt source                destination            tcp dpt:submission
ACCEPT     tcp  --  anywhere                192.168.1.101          tcp dpt:ssmtp
ACCEPT     tcp  --  anywhere                192.168.1.101          tcp dpt:pop3
ACCEPT     tcp  --  anywhere                192.168.1.101          tcp dpt:pop3s
ACCEPT     tcp  --  anywhere                192.168.1.101          tcp dpt:imap2
ACCEPT     tcp  --  anywhere                192.168.1.101          tcp dpt:imaps
ACCEPT     tcp  --  anywhere                192.168.1.102          tcp dpt:http
ACCEPT     tcp  --  anywhere                192.168.1.102          tcp dpt:https
ACCEPT     tcp  --  anywhere                192.168.1.102          tcp dpt:ftp
ACCEPT     tcp  --  anywhere                192.168.1.103          tcp dpt:http
ACCEPT     tcp  --  anywhere                192.168.1.103          tcp dpt:https
ACCEPT     tcp  --  anywhere                192.168.1.103          tcp dpt:ftp
ssh_check  tcp  --  anywhere                192.168.1.101          tcp dpt:1101
ssh_check  tcp  --  anywhere                192.168.1.102          tcp dpt:1102
ssh_check  tcp  --  anywhere                192.168.1.103          tcp dpt:1103
ACCEPT     tcp  --  anywhere                192.168.1.101          tcp dpt:1101
ACCEPT     tcp  --  anywhere                192.168.1.102          tcp dpt:1102
ACCEPT     tcp  --  anywhere                192.168.1.103          tcp dpt:1103
ACCEPT     all  --  anywhere                anywhere               state RELATED,ESTABLISHED

Chain FORWARD (policy DROP)
target     prot opt source                destination            state RELATED,ESTABLISHED
ACCEPT     all  --  anywhere                anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination            state RELATED,ESTABLISHED
ACCEPT     all  --  anywhere                anywhere

Chain ssh_check (3 references)
target     prot opt source                destination            recent: CHECK seconds: 60 hit_count: 3 name: DEFAULT side: dest LOG level warning prefix "SSH attack: "
DROP       all  --  anywhere                anywhere               recent: CHECK seconds: 60 hit_count: 3 name: DEFAULT side: dest
RETURN     all  --  anywhere                anywhere               recent: SET name: DEFAULT side: dest
root@awbirg1:~#
```

Podsumowanie i wnioski

- Przeanalizowano możliwości, jakie daje interfejs WWW przy konfiguracji zapory w systemie Linux.
- Zastosowanie zmiennych pozwoliło znacznie zmniejszyć wymagany nakład pracy przy tworzeniu zestawu reguł.
- Dzięki podsumowaniom w widokach reguł, hostów i grup możliwe jest dużo prostsze zrozumienie polityki dotyczącej danego obiektu.
- Zastosowanie zmiennych pozwala na łatwiejsze dostosowanie reguł do zmian w sieci.

Dziękuję za uwagę