Praca magisterska

Analiza możliwości wykorzystania interfejsu WWW do definiowania zestawu reguł zapory sieciowej

Autor: **Robert Korulczyk**

Promotor: **Dr inż. Grzegorz Kozieł**

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.

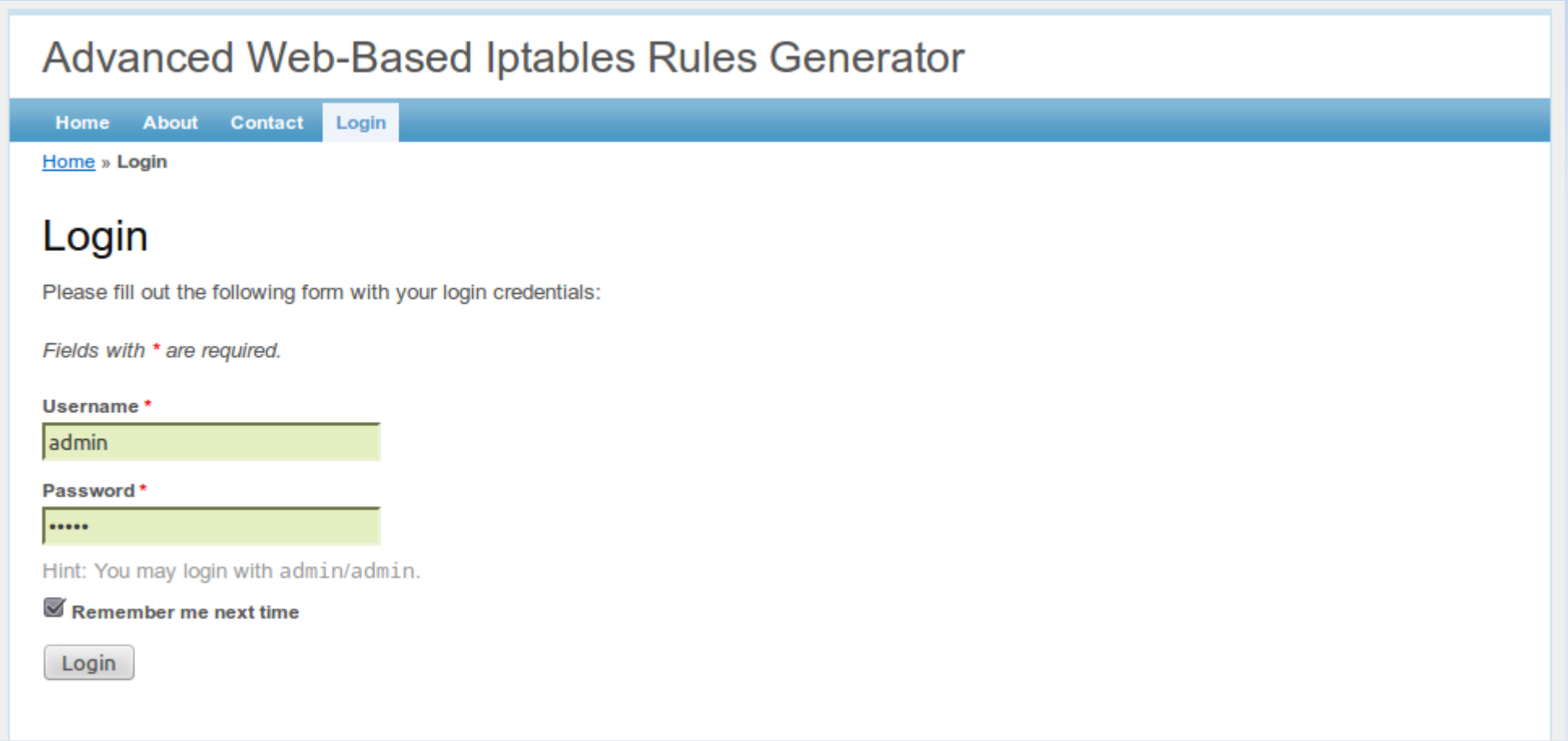
Iptables

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.

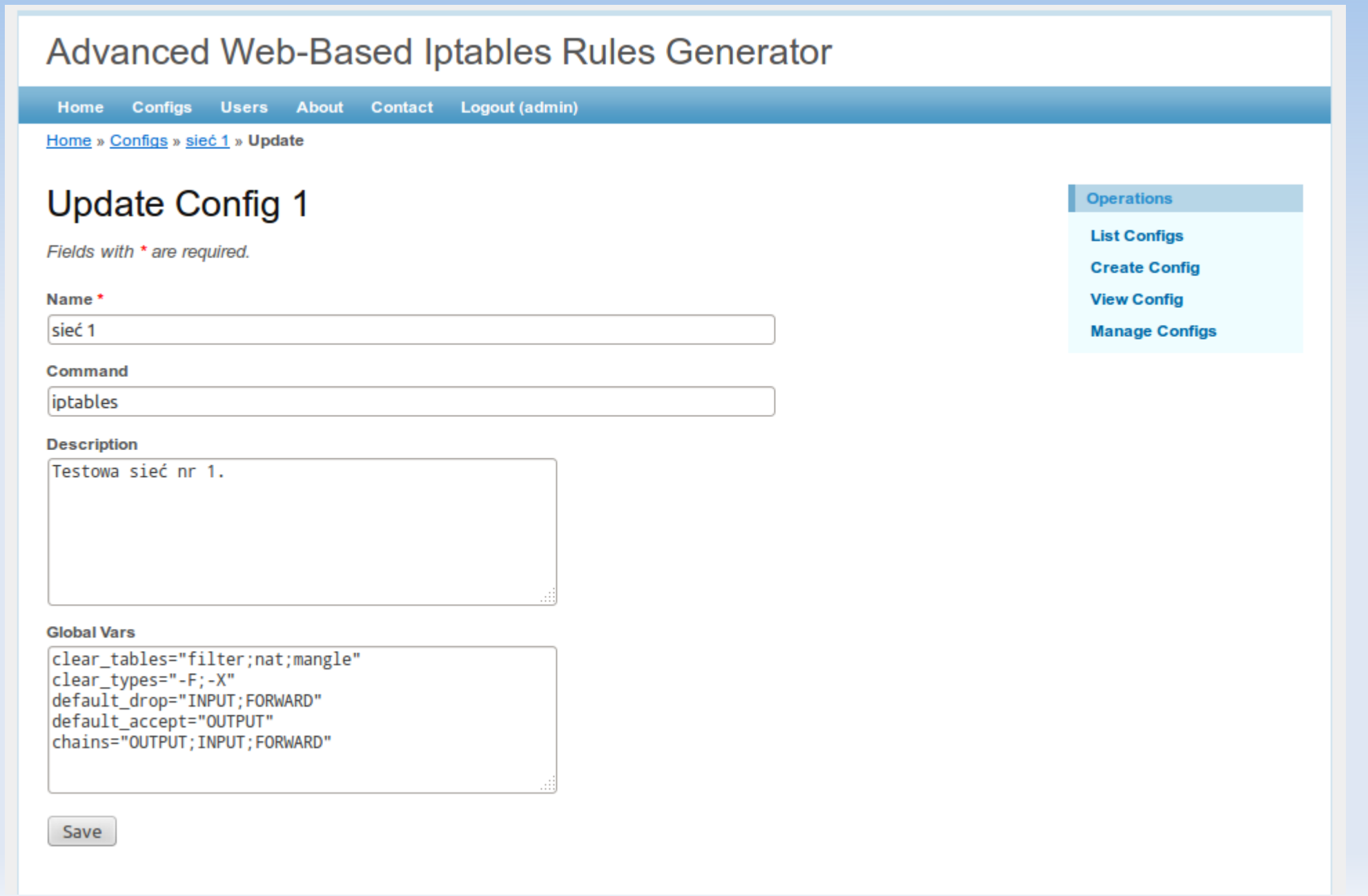
Składnia polecenia iptables:

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

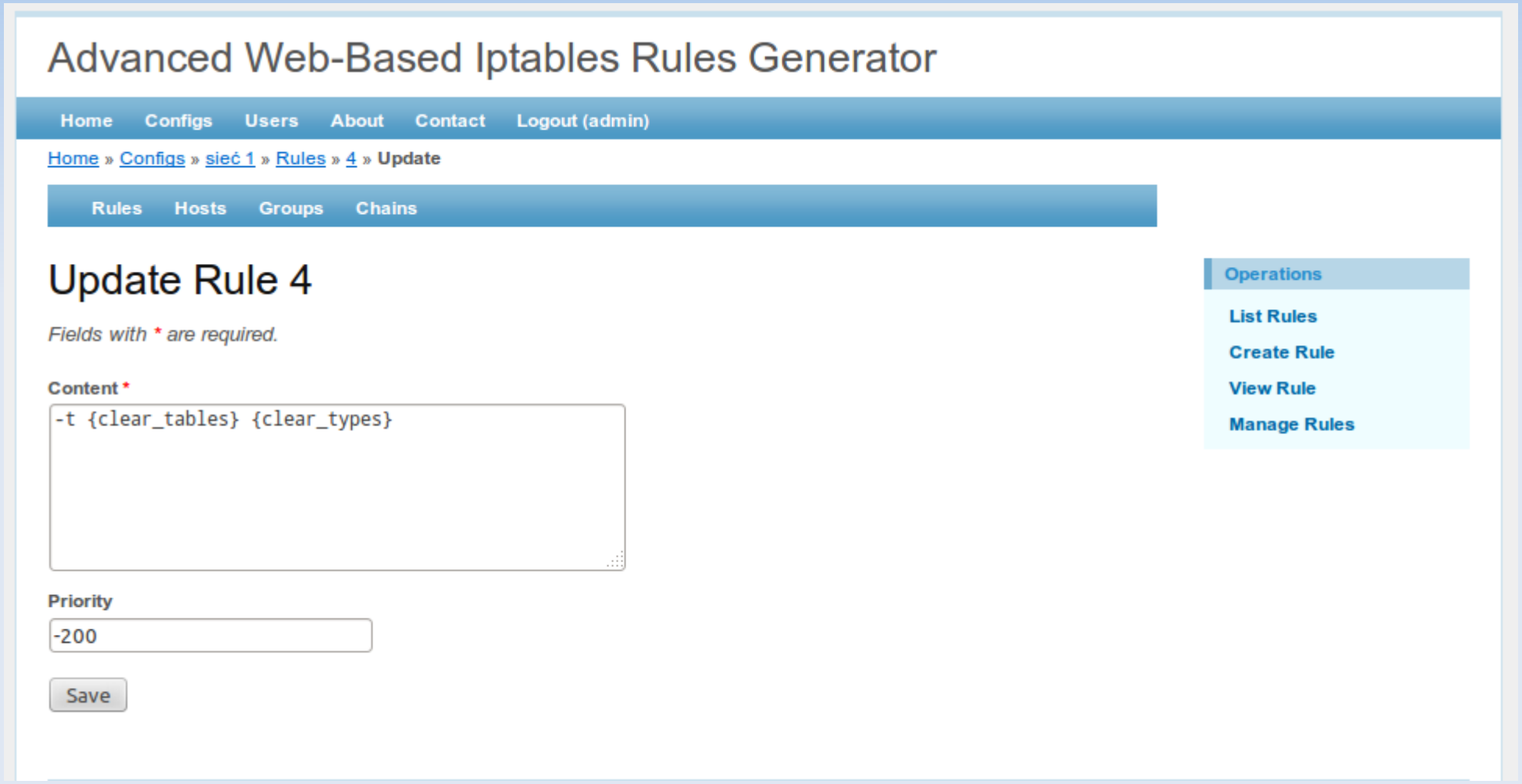
Opis aplikacji



Opis aplikacji



Opis aplikacji



Opis aplikacji

```
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 aplikacji

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

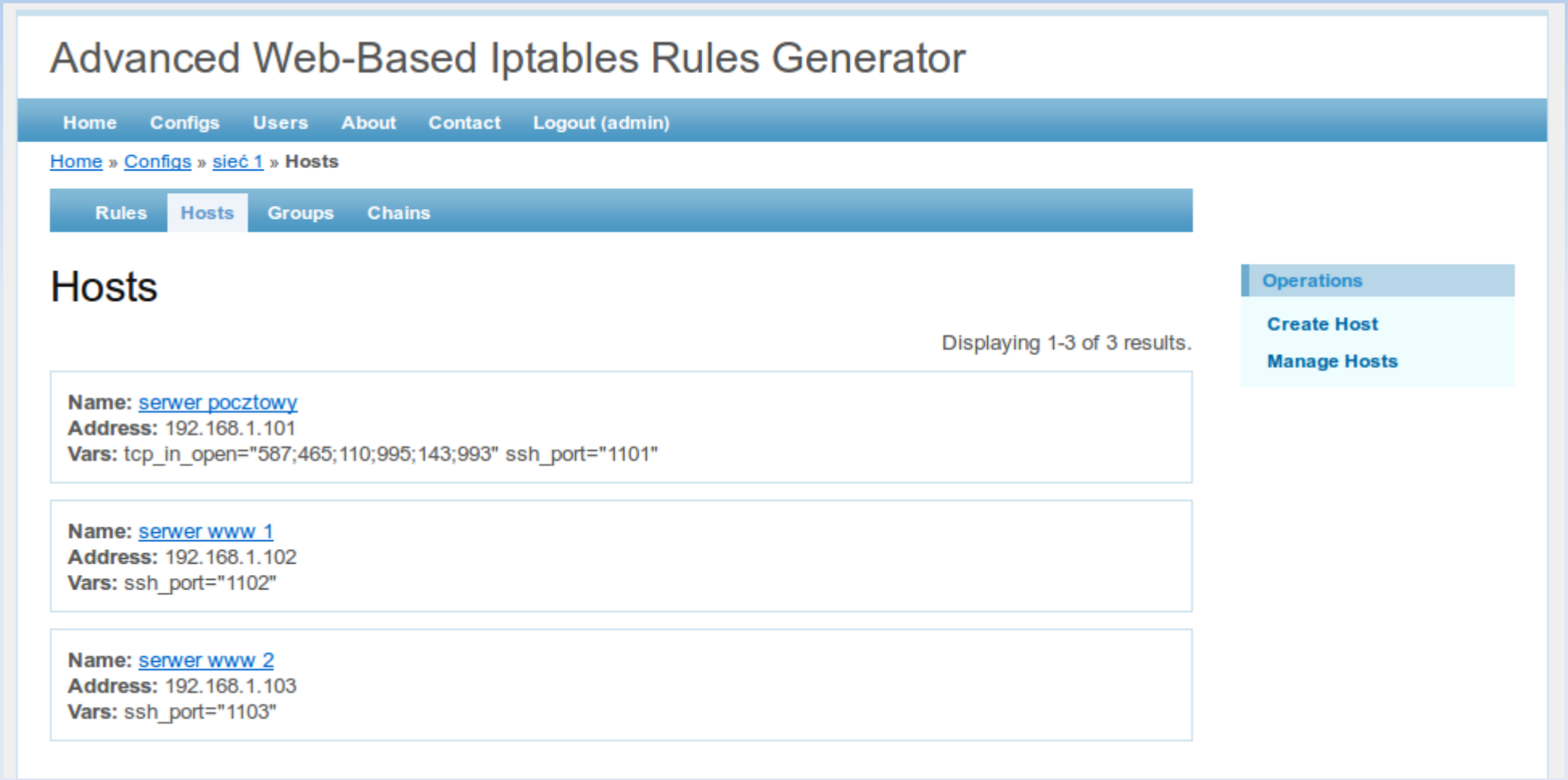
ID: 10
Content: -A {chains} -m state --state ESTABLISHED,RELATED -j ACCEPT
Priority: 100

Operations

Create Rule

Manage Rules

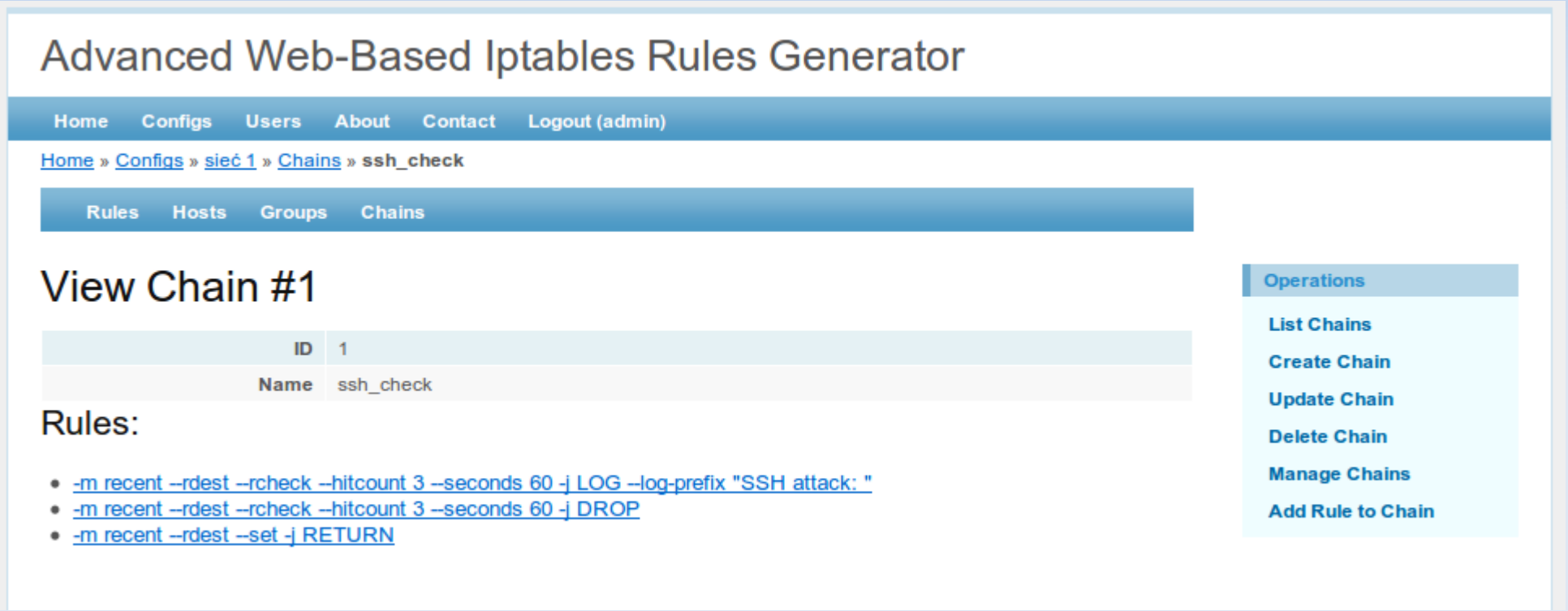
Opis aplikacji



Opis aplikacji

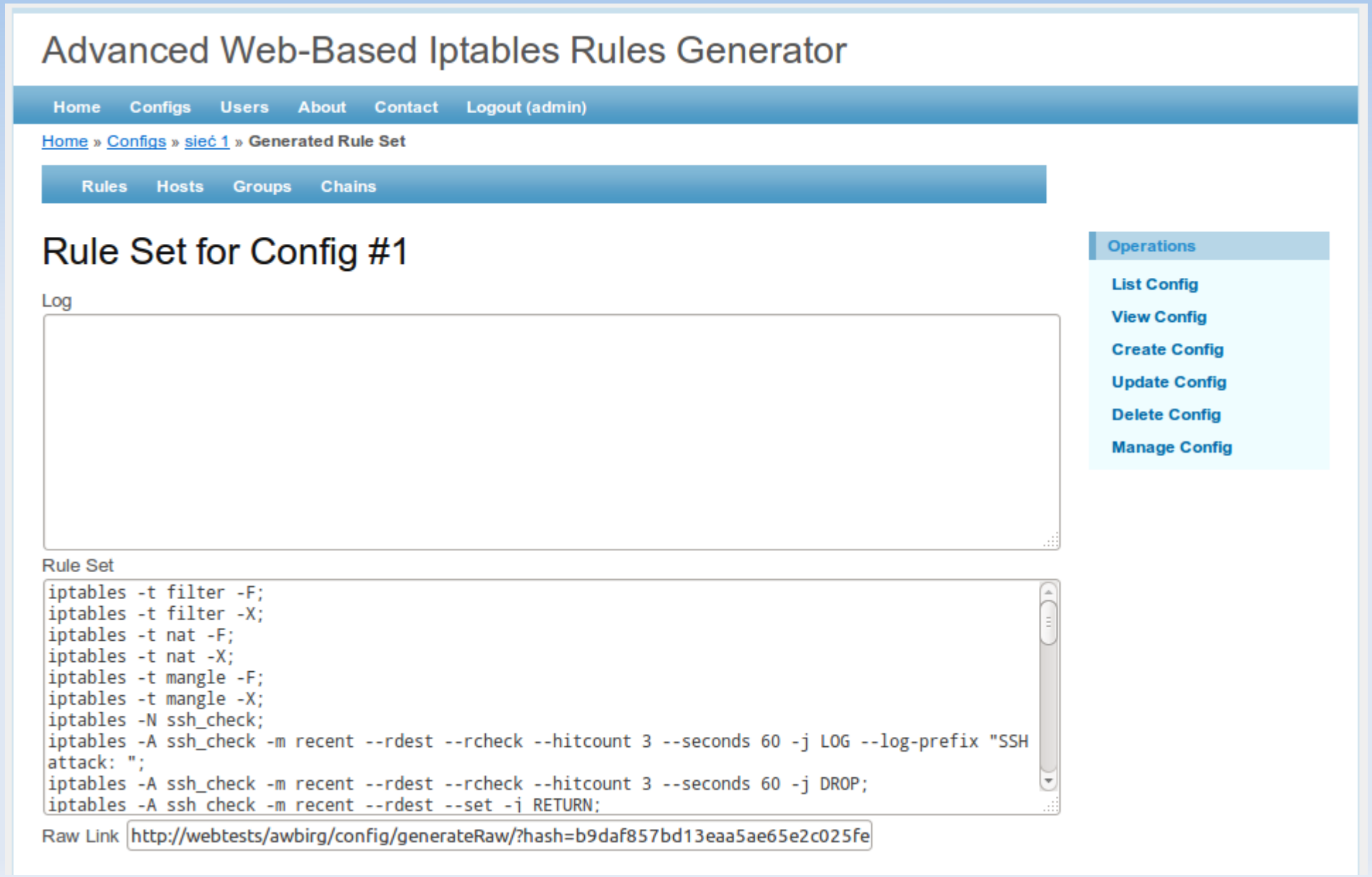
Opis aplikacji

Opis aplikacji



Opis aplikacji

Opis aplikacji



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 aplikacji

```
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
ACCEPT     tcp  --  anywhere             192.168.1.101        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
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED

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

Chain ssh_check (3 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere             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 dotyczacej danego obiektu.
- Zastosowanie zmiennych pozwala na łatwiejsze dostosowanie reguł do zmian w sieci.

Dziękuję za uwagę