Bezpieczeństwo Sieci

    - Ex.Policies.3
    - Ex.ShowSecurityFlowSession.1
    - Ex.ShowInterfacesTerse.1
    - Ex.ShowSecurityPolicies.1
    - Ex.ShowSecurityNatSourceSummary.1
    - Ex.ShowSecurityNatSourceRuleAll.1
    - Ex.ShowARP.1
    - Ex.ShowARP.2
    - Ex.Save.1
    - Ex.Applications.1
    - Ex.Applications.2
    - Ex.Applications.3
    - Ex.NAT.1
    - Ex.NAT.2
    - Ex.NAT.3
    - Ex.NAT.4
    - Ex.RoutinOptions.NextHop.1
- Listy opcji
    - Ol.NAT.1
    - Ol.NAT.2-NAT STATIC

informacje ogólne

- `>` - karetka trybu ogólnego
- `#` - karetka trybu uprzywilejowanego

numeracja interfejsów (junyper)

- fe
- ge
- xe
- t1
- e1
- se - serial

Numeracja od zera.

- `ge-0/0/0.000`
- `ge-0/0/0 unit 0`

`<interfejs>-<>/<numer modułu>/<numer portu>.<unit>`

Domyślnie interfejsy są włączone.
Możliwe tryby pracy:

- `flow based`
- `packet based`

komendy ogólne

- `?` - podpowiada w dowolnym miejscu polecenia
- `run ...` - uruchamia polecenia poza trybem konfiguracyjnym
- `configure [private]`
- `load overrive <file name>`
- `run request system reboot`
- `run show ...`
- `show|compare` - pokazuje zmiany w konfiguracji dokonane od ostatniego commitu
- `commit [confirmed <liczba minut>]`
- `save <file name>` - zapisuje bieżącą konfigurację do pliku
- `rollback` - przywraca ustawienia z ostatniego commita
- `clear arp` - czysci tablice adresów

konfiguracja

- `set [security|interfaces|...]` - tworzy ustawienia
- `delete [security|interfaces|...]` - kasuje ustawienia
- `rename [security|interfaces|...]` - modyfikuje ustawienia

przydatne showy

- `show configuration groups junos-defaults [applications]`
- `show configuration system services`
- `show interfaces terse`
- `show route`
- `show security flow session` - Przykład
- `show security flow status` - powinien być `flow based`
- `show security nat source rule all`
- `show security nat source summary`
- `show security zones`
- `show arp`

inne

- `run file list|delete <file>`
- `run show log <file>`

Konfiguracja VLAN

Firewall

```
# set security zones security-zone INTERNET interfaces ge-0/0/1.400
# set interfaces ge-0/0/1 vlan-tagging
# set interfaces ge-0/0/1 unit 400 vlan-id 400
# set interfaces ge-0/0/1.400 vlan-id 400
# set interfaces ge-0/0/1.400 family inet address 1.1.4.1/30
```

Polecenia `set interfaces ge-0/0/1 unit 400 vlan-id 400` oraz `set interfaces ge-0/0/1.400 vlan-id 400` są sobie równoważne, notacja z `.` oraz `unit`.

Zobacz wywołanie

Kasowanie

```
lab@163# delete interfaces ge-0/0/1.400 family inet address 1.1.4.1/30
```

Zobacz wywołanie, Zobacz wywołanie

Włączanie odpowiednich usług (`ping`)

```
# set security zones security-zone INTERNET interfaces ge-0/0/1.400 host-
inbound-traffic system-services ping
```

Końcówka

Ze względu na jednoczesną konfiguracje dokonywaną przez wiele osób końcówki konfigurujemy w trybie `configure private`.

```
# set interfaces ge-0/0/1 vlan-tagging
# set interfaces ge-0/0/1.400 vlan-id 400
# set interfaces ge-0/0/1.400 family inet address 1.1.4.2/30
```

Zobacz wywołanie

Konfiguracja wirtualnego routera końcówki

```
# set routing-instances SERWER4 instance-type virtual-router
# set routing-instances SERWER4 interface ge-0/0/1.400
```

```
# set routing-instances SERWER4 routing-options static route 0/0 next-hop
1.1.4.1
```

Zobacz wywołanie

Wykorzystanie

```
> ping 1.1.4.2 routing-instance KOMP-KADRY-4
> telnet 1.1.4.2 port 80 routing-instance KOMP-KADRY-4
> show route table KOMP-KADRY-4
```

Konfiguracja Polityk

Polityki (Policies)

Polityki są czytane *po kolei* i działa pierwsza, która zostanie dopasowana. Kolejność jest zgodna z kolejnością dodawania polityk. Dobrze jest utworzyć politykę domyślną, która będzie ostatnia w kolejności.

Polityka może mieć ustawienia

- `permit`
- `deny`
- `reject`

```
# set security policies from-zone KADRY to-zone INTERNET policy POLITYKA1
match source-address any
# ...security policies from-zone KADRY to-zone INTERNET policy POLITYKA1
match destination-address any
# ...rity policies from-zone KADRY to-zone INTERNET policy POLITYKA1 match
application junos-icmp-ping
# ...rity policies from-zone KADRY to-zone INTERNET policy POLITYKA1 then
permit
```

Polityka domyślna

```
lab@163# set security policies from-zone KADRY to-zone INTERNET policy
DOMYSLNA match source-address any destination-address any application any
lab@163# set security policies from-zone KADRY to-zone INTERNET policy
DOMYSLNA then deny
lab@163# set security policies from-zone KADRY to-zone INTERNET policy
DOMYSLNA then log session-init
```

Zmiana kolejności polityk

```
lab@163# insert security policies from-zone KADRY to-zone INTERNET policy
DOMYSLNA <before|after> policy POLITYKA1
```

```
lab@163# insert security policies from-zone KADRY to-zone INTERNET policy
DOMYSLNA after policy POLITYKAHTTP
```

Zobacz wywołanie

Strefy bezpieczeństwa (Security zones)

Addressbooki

W pierwszej kojeności dodajemy adresy do `addressbook`.

```
lab@163# set security zones security-zone KADRY address-book address KOMP-
KADRY-ADD192.168.4.10 192.168.4.10/32
```

Strefy

```
lab@163# ...ne INTERNET policy POLITYKAHTTP match source-address KOMP-
KADRY-ADD192.168.4.10
lab@163# ...urity policies from-zone KADRY to-zone INTERNET policy
POLITYKAHTTP match destination-address any
lab@163# ...curity policies from-zone KADRY to-zone INTERNET policy
POLITYKAHTTP match application junos-http
lab@163# ...curity policies from-zone KADRY to-zone INTERNET policy
POLITYKAHTTP then permit
```

Logi, Logging

```
lab@163# set system syslog file TRAFFIC_LOG user any
lab@163# set system syslog file TRAFFIC_LOG match "RT_FLOW"
lab@163# set security policies from-zone KADRY to-zone INTERNET policy
POLITYKA1 then log session-close session-init
```

```
lab@163# run file list /var/log

lab@163# run file delete /var/log/TRAFFIC_LOG
lab@163# run show log TRAFFIC_LOG
error: could not resolve file: TRAFFIC_LOG

lab@163# set system syslog user * any any
```

Aplikacje

Listowanie

```
lab@163# run show configuration groups junos-defaults
lab@163# run show configuration groups junos-defaults applications
```

Set Application

```
lab@163# set applications application XRX-1 protocol tcp
lab@163# set applications application XRX-1 destination-port 25
```

Zobacz wywołanie

Set Application-Set

```
lab@163# set applications application-set MOJE-XRX application XRX-1
lab@163# set applications application-set MOJE-XRX application XRX-2
```

lub

```
lab@163# set applications application-set MOJE-XRX application XRX-1,XRX-2
```

Zobacz wywołanie

NAT (Network Address Translation)

Show

```
lab@163# run show security nat source summary
lab@163# run show security nat source rule all
```

Zobacz wywołanie 1, Zobacz wywołanie 2

Set NAT

```
lab@163# set security nat source rule-set KADRY-INTERNET rule KADRY match
destination-address 1.1.4.0/24
lab@163# set security nat source rule-set KADRY-INTERNET from zone KADRY
lab@163# set security nat source rule-set KADRY-INTERNET to zone INTERNET
lab@163# set security nat source rule-set KADRY-INTERNET rule KADRY then
source-nat interface
```

Zobacz wywołanie

Set NAT with Pool

```
lab@163# set security nat source rule-set KADRY-INTERNET rule KADRY-1
lab@163# set security nat source rule-set KADRY-INTERNET rule KADRY-1 match
destination-address 7.7.4.0/29

lab@163# set security nat source pool POOL-7_7_10_0_29 address 2.2.4.5/32
lab@163# set security nat source rule-set KADRY-INTERNET rule KADRY-1 then
source-nat pool POOL-7_7_10_0_29
```

Zobacz wywołanie

```
lab@163# set security nat source pool POOL-8_8_4_0_24 address 1.1.4.10
[edit]
lab@163# set security nat source rule-set KADRY-INTERNET from zone KADRY
lab@163# set security nat source rule-set KADRY-INTERNET to zone INTERNET
lab@163# set security nat source rule-set KADRY-INTERNET rule KADRY-2 match
destination-address 8.8.4.0/24
lab@163# set security nat source rule-set KADRY-INTERNET rule KADRY-2 then
source-nat pool POOL-8_8_4_0_24
```

Zobacz wywołanie

NAT Proxy-ARP

Pozwala przyznawać pule adresów pulom adresów 😉

Przykładowo, gdy chcemy konkretną grupę użytkowników wystawiać w Internecie pod adresem 1.1.0.1, a serwery udostępniać jako 1.1.0.5.

Destination NAT dla DMZ 1.1.X.0/25
DMZ 10.10.X.20 <-> INTERNET 1.1.X.5

Set

```
lab@163# set security nat proxy-arp interface ge-0/0/1.400 address 1.1.4.10
to 1.1.4.20
```

Zobacz wywołanie

Routing Options

Next-hop

```
lab@163# delete routing-options static route 0.0.0.0/0 next-hop 192.168.4.1
lab@163# set routing-options static route 0.0.0.0/0 next-hop 1.1.4.2
```

Zobacz wywołanie

Ciekawostki prowadzącego

- ELASTIC - narzędzie do analizy ruchu (bardzo dobre)
- SIEM - narzedzia siemowskie, analiza logow, System Information and Event Mamanegement
- PAT losuje porty od 1024-65353 (2B)
- ARP (Address Resolution Protocol)
- Pool dla NAT pokrywa sie z interfejsem = problem; rozwiazanie to Proxy NAT

Przykłady

Ex.VLAN.1

```
[edit]
lab@163# set security zones security-zone INTERNET interfaces ge-0/0/1.400

[edit]
lab@163# set interfaces ge-0/0/1 vlan-tagging

[edit]
lab@163# set interfaces ge-0/0/1 unit 400 vlan-id 400

[edit]
lab@163# set interfaces ge-0/0/1.400 vlan-id 400 ||| to samo co wyzej

[edit]
lab@163# set interfaces ge-0/0/1.400 family inet address 1.1.4.1/30

[edit]
lab@163# show | compare
[edit interfaces]
+   ge-0/0/1 {
+       vlan-tagging;
+       unit 400 {
+           vlan-id 400;
+           family inet {
+               address 1.1.4.1/30;
+           }
+       }
+   }
[edit security zones]
+    security-zone INTERNET {
+        interfaces {
+            ge-0/0/1.400;
+        }
+    }
```

Ex.VLAN.2

```
[edit]
lab@138# set interfaces ge-0/0/1 vlan-tagging

[edit]
lab@138# set interfaces ge-0/0/1.400 vlan-id 400

[edit]
lab@138# set interfaces ge-0/0/1.400 family inet address 1.1.4.2/30
```

```
[edit]
lab@138# show | compare
[edit interfaces]
+   ge-0/0/1 {
+       vlan-tagging;
+       unit 400 {
+           vlan-id 400;
+       }
+   }
```

Ex.VLAN.3

```
[edit]
lab@138# set routing-instances SERWER4 instance-type virtual-router

[edit]
lab@138# set routing-instances SERWER4 interface ge-0/0/1.400

[edit]
lab@138# show | compare
[edit interfaces]
+   ge-0/0/1 {
+       vlan-tagging;
+       unit 400 {
+           vlan-id 400;
+       }
+   }
[edit]
+  routing-instances {
+      SERWER4 {
+          instance-type virtual-router;
+          interface ge-0/0/1.400;
+      }
+  }
```

Ex.VLAN.4

```
lab@163# delete interfaces ge-0/0/1.400 family inet address 1.1.4.1/30

[edit]
lab@163# set interfaces ge-0/0/1.400 family inet address 1.1.4.1/25

[edit]
lab@163# show|compare
[edit interfaces ge-0/0/1 unit 400 family inet]
+       address 1.1.4.1/25;
-       address 1.1.4.1/30;
```

Ex.VLAN.5

```
lab@138# delete interfaces ge-0/0/1.400 family inet address 1.1.4.2/30

[edit]
lab@138# show|compare
[edit interfaces ge-0/0/1 unit 400 family inet]
-       address 1.1.4.2/30;
```

Ex.Policies.1

```
lab@163# set security zones security-zone KADRY address-bookadd KOMP-KADRY-
ADD192.168.4.10
                                                ^
syntax error.
lab@163# ... KADRY address-book address KOMP-KADRY-ADD192.168.4.10
192.168.4.10/32

lab@163# ...olicies from-zone KADRY to-zone INTERNET policy POLITYKAHTTP
match source-address ?
Possible completions:
  192.168.4.10/32      Address from address book
  KOMP-KADRY-ADD192.168.4.10  The address in address book
  [                    Open a set of values
  any                  Any IPv4 or IPv6 address
  any-ipv4             Any IPv4 address
  any-ipv6             Any IPv6 address
[edit]
lab@163# ...ne INTERNET policy POLITYKAHTTP match source-address KOMP-
KADRY-ADD192.168.4.10

[edit]
lab@163# ...urity policies from-zone KADRY to-zone INTERNET policy
POLITYKAHTTP match destination-address any

[edit]
lab@163# ...curity policies from-zone KADRY to-zone INTERNET policy
POLITYKAHTTP match application junos-http

[edit]
lab@163# ...curity policies from-zone KADRY to-zone INTERNET policy
POLITYKAHTTP pe

^
syntax error.
lab@163# ...curity policies from-zone KADRY to-zone INTERNET policy
POLITYKAHTTP then permit

lab@163# show|compare
```

```
[edit security policies]
     from-zone KADRY to-zone INTERNET { ... }
+    from-zone INTERNET to-zone KADRY {
+        policy POLITYKAFTP {
+            match {
+                source-address 1.1.4.2;
+                destination-address KOMP-KADRY-ADD192.168.4.10;
+                application junos-ftp;
+            }
+            then {
+                permit;
+            }
+        }
+    }
[edit security zones security-zone INTERNET]
+     address-book {
+         address 1.1.4.2 1.1.4.2/32;
+     }
```

Ex.Policies.2

```
lab@163# run show security policies
Default policy: deny-all
From zone: KADRY, To zone: INTERNET
  Policy: POLITYKA1, State: enabled, Index: 4, Scope Policy: 0, Sequence
number: 1
    Source addresses: any
    Destination addresses: any
    Applications: junos-icmp-ping
    Action: permit
  Policy: POLITYKAHTTP, State: enabled, Index: 5, Scope Policy: 0, Sequence
number: 2
    Source addresses: KOMP-KADRY-ADD192.168.4.10
    Destination addresses: any
    Applications: junos-http
    Action: permit
From zone: INTERNET, To zone: KADRY
  Policy: POLITYKAFTP, State: enabled, Index: 6, Scope Policy: 0, Sequence
number: 1
    Source addresses: 1.1.4.2
    Destination addresses: KOMP-KADRY-ADD192.168.4.10
    Applications: junos-ftp
    Action: permit
```

Ex.Policies.3

```
lab@163> show security policies
Default policy: deny-all
From zone: KADRY, To zone: INTERNET
```

```
  Policy: DOMYSLNA, State: enabled, Index: 4, Scope Policy: 0, Sequence
number: 1
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: deny, log
  Policy: POLITYKA1, State: enabled, Index: 5, Scope Policy: 0, Sequence
number: 2
    Source addresses: any
    Destination addresses: any
    Applications: junos-icmp-ping
    Action: permit, log
  Policy: POLITYKAHTTP, State: enabled, Index: 6, Scope Policy: 0, Sequence
number: 3
    Source addresses: KOMP-KADRY-ADD192.168.4.10
    Destination addresses: any
    Applications: junos-http
    Action: permit
From zone: INTERNET, To zone: KADRY
  Policy: POLITYKAFTP, State: enabled, Index: 7, Scope Policy: 0, Sequence
number: 1
    Source addresses: 1.1.4.2
    Destination addresses: KOMP-KADRY-ADD192.168.4.10
    Applications: junos-ftp
    Action: permit

lab@163> configure
Entering configuration mode

[edit]
lab@163# insert security policies from-zone KADRY to-zone INTERNET policy
DOMYSLNA after policy POLITYKAHTTP

[edit]
lab@163# show|compare
[edit security policies from-zone KADRY to-zone INTERNET]
!     policy POLITYKA1 { ... }
!     policy POLITYKAHTTP { ... }

[edit]
lab@163# commit
commit complete

[edit]
lab@163# run show security policies
Default policy: deny-all
From zone: KADRY, To zone: INTERNET
  Policy: POLITYKA1, State: enabled, Index: 5, Scope Policy: 0, Sequence
number: 1
    Source addresses: any
    Destination addresses: any
    Applications: junos-icmp-ping
    Action: permit, log
  Policy: POLITYKAHTTP, State: enabled, Index: 6, Scope Policy: 0, Sequence
```

```
number: 2
    Source addresses: KOMP-KADRY-ADD192.168.4.10
    Destination addresses: any
    Applications: junos-http
    Action: permit
  Policy: DOMYSLNA, State: enabled, Index: 4, Scope Policy: 0, Sequence
number: 3
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: deny, log
From zone: INTERNET, To zone: KADRY
  Policy: POLITYKAFTP, State: enabled, Index: 7, Scope Policy: 0, Sequence
number: 1
    Source addresses: 1.1.4.2
    Destination addresses: KOMP-KADRY-ADD192.168.4.10
    Applications: junos-ftp
    Action: permit
```

Ex.ShowSecurityFlowSession.1

```
lab@163# run show security flow session
Session ID: 76, Policy name: self-traffic-policy/1, Timeout: 1800, Valid
  In: 172.30.33.68/60664 --> 172.30.33.163/23;tcp, If: ge-0/0/0.0, Pkts:
1062, Bytes: 55972
  Out: 172.30.33.163/23 --> 172.30.33.68/60664;tcp, If: .local..0, Pkts:
715, Bytes: 58560

Session ID: 987, Policy name: POLITYKA1/4, Timeout: 2, Valid
  In: 192.168.4.10/39 --> 1.1.4.2/18457;icmp, If: ge-0/0/2.401, Pkts: 1,
Bytes: 84
  Out: 1.1.4.2/18457 --> 192.168.4.10/39;icmp, If: ge-0/0/1.400, Pkts: 1,
Bytes: 84

Session ID: 988, Policy name: POLITYKA1/4, Timeout: 2, Valid
  In: 192.168.4.10/40 --> 1.1.4.2/18457;icmp, If: ge-0/0/2.401, Pkts: 1,
Bytes: 84
  Out: 1.1.4.2/18457 --> 192.168.4.10/40;icmp, If: ge-0/0/1.400, Pkts: 1,
Bytes: 84

Session ID: 989, Policy name: POLITYKA1/4, Timeout: 4, Valid
  In: 192.168.4.10/41 --> 1.1.4.2/18457;icmp, If: ge-0/0/2.401, Pkts: 1,
Bytes: 84
  Out: 1.1.4.2/18457 --> 192.168.4.10/41;icmp, If: ge-0/0/1.400, Pkts: 1,
Bytes: 84
Total sessions: 4
```

Ex.ShowInterfacesTerse.1

```
[edit]
lab@163# run show interfaces terse
Interface               Admin Link Proto    Local                 Remote
ge-0/0/0                up    up
ge-0/0/0.0              up    up   inet     172.30.33.163/24
gr-0/0/0                up    up
ip-0/0/0                up    up
lsq-0/0/0               up    up
lt-0/0/0                up    up
mt-0/0/0                up    up
sp-0/0/0                up    up
sp-0/0/0.0              up    up   inet
sp-0/0/0.16383          up    up   inet     10.0.0.1            -->
10.0.0.16
                                            10.0.0.6            --> 0/0
                                            128.0.0.1           -->
128.0.1.16
                                            128.0.0.6           --> 0/0
ge-0/0/1                up    up
ge-0/0/1.400            up    up   inet     1.1.4.1/30
ge-0/0/1.32767          up    up
ge-0/0/2                up    up
ge-0/0/2.401            up    up   inet     192.168.4.1/24
ge-0/0/2.32767          up    up
ge-0/0/3                up    down
ge-0/0/4                up    down
ge-0/0/5                up    down
ge-0/0/6                up    down
ge-0/0/7                up    down
ge-0/0/8                up    down
ge-0/0/9                up    down
ge-0/0/10               up    down
ge-0/0/11               up    down
ge-0/0/12               up    down
ge-0/0/13               up    down
ge-0/0/14               up    down
ge-0/0/15               up    down
fxp2                    up    up
fxp2.0                  up    up   tnp      0x1
gre                     up    up
ipip                    up    up
irb                     up    up
lo0                     up    up
lo0.16384               up    up   inet     127.0.0.1           --> 0/0
lo0.16385               up    up   inet     10.0.0.1            --> 0/0
                                            10.0.0.16           --> 0/0
                                            128.0.0.1           --> 0/0
                                            128.0.1.16          --> 0/0
lo0.32768               up    up
lsi                     up    up
mtun                    up    up
pimd                    up    up
pime                    up    up
```

```
pp0                     up    up
ppd0                    up    up
ppe0                    up    up
st0                     up    up
tap                     up    up
vlan                    up    up
```

Ex.ShowSecurityPolicies.1

```
lab@163# run show security policies
Default policy: deny-all
From zone: KADRY, To zone: INTERNET
  Policy: DOMYSLNA, State: enabled, Index: 4, Scope Policy: 0, Sequence
number: 1
    Source addresses: any
    Destination addresses: any
    Applications: any
    Action: deny, log
  Policy: POLITYKA1, State: enabled, Index: 5, Scope Policy: 0, Sequence
number: 2
    Source addresses: any
    Destination addresses: any
    Applications: junos-icmp-ping
    Action: permit, log
  Policy: POLITYKAHTTP, State: enabled, Index: 6, Scope Policy: 0, Sequence
number: 3
    Source addresses: KOMP-KADRY-ADD192.168.4.10
    Destination addresses: any
    Applications: junos-http
    Action: permit
From zone: INTERNET, To zone: KADRY
  Policy: POLITYKAFTP, State: enabled, Index: 7, Scope Policy: 0, Sequence
number: 1
    Source addresses: 1.1.4.2
    Destination addresses: KOMP-KADRY-ADD192.168.4.10
    Applications: junos-ftp
    Action: permit
```

Ex.ShowSecurityNatSourceSummary.1

```
lab@163# run show security nat source summary
Total pools: 0

Total rules: 1
Rule name          Rule set       From              To
Action
KADRY              KADRY-INTERNET KADRY             INTERNET
interface
```

Ex.ShowSecurityNatSourceRuleAll.1

```
lab@163# run show security nat source rule all
Total rules: 1
Total referenced IPv4/IPv6 ip-prefixes: 1/0

source NAT rule: KADRY                Rule-set: KADRY-INTERNET
  Rule-Id                    : 1
  Rule position              : 1
  From zone                  : KADRY
  To zone                    : INTERNET
    Destination addresses    : 1.1.4.0         - 1.1.4.255
    Destination port         : 0               - 0
  Action                        : interface
    Persistent NAT type         : N/A
    Persistent NAT mapping type : address-port-mapping
    Inactivity timeout          : 0
    Max session number          : 0
  Translation hits           : 0
```

Ex.ShowARP.1

```
lab@163# run show arp
MAC Address       Address         Name                      Interface
Flags
a8:d0:e5:a8:10:81 1.1.4.2         1.1.4.2                   ge-0/0/1.400
none
f8:b1:56:ab:39:d3 172.30.33.68    172.30.33.68              ge-0/0/0.0
none
00:24:dc:d0:7c:01 192.168.4.10    192.168.4.10              ge-0/0/2.401
none
Total entries: 3
```

Ex.ShowARP.2

```
lab@139> show arp
MAC Address       Address         Name                    Interface
Flags
f8:b1:56:9c:af:57 172.30.33.67    172.30.33.67             ge-0/0/0.0
none
f8:b1:56:ab:39:d3 172.30.33.68    172.30.33.68             ge-0/0/0.0
none
f8:b1:56:ab:53:0b 172.30.33.70    172.30.33.70             ge-0/0/0.0
none
f8:b1:56:ab:6e:c4 172.30.33.72    172.30.33.72             ge-0/0/0.0
none
```

```
f8:b1:56:ab:9b:a9 172.30.33.77    172.30.33.77              ge-0/0/0.0
none
a8:d0:e5:a2:12:82 192.168.4.1     192.168.4.1               ge-0/0/1.401
none
a8:d0:e5:a2:18:82 192.168.5.1     192.168.5.1               ge-0/0/1.501
none
a8:d0:e5:a2:13:02 192.168.6.1     192.168.6.1               ge-0/0/1.601
none
00:17:cb:41:c1:82 192.168.9.1     192.168.9.1               ge-0/0/1.901
none
00:17:cb:41:c0:82 192.168.11.1    192.168.11.1              ge-0/0/1.1101
none
a8:d0:e5:a2:15:82 192.168.12.1    192.168.12.1              ge-0/0/2.1201
none
Total entries: 11
```

Ex.Save.1

```
lab@163# save BEZPIECZENSTWO-J29.11.2019
Wrote 170 lines of configuration to 'BEZPIECZENSTWO-J29.11.2019'
```

Ex.Applications.1

```
lab@163# set applications ?
Possible completions:
> application          Define an application
> application-set      Define an application set
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups

lab@163# set applications application XRX-1 protocol tcp
lab@163# set applications application XRX-1 destination-port 25
lab@163# show|compare
[edit]
+  applications {
+      application XRX-1 {
+          protocol tcp;
+          destination-port 25;
+      }
+  }
```

```
lab@163# set applications application XRX-2 protocol tcp
lab@163# set applications application XRX-2 destination-port 21
lab@163# show|compare
[edit]
+  applications {
```

```
+      application XRX-1 {
+          protocol tcp;
+          destination-port 25;
+      }
+      application XRX-2 {
+          protocol tcp;
+          destination-port 21;
+      }
+  }
```

Ex.Applications.2

```
lab@163# set applications application-set MOJE-XRX application XRX-1
lab@163# set applications application-set MOJE-XRX application XRX-2

lab@163# set applications application-set MOJE-XRX application XRX-1,XRX-2

lab@163# show|compare
[edit]
+  applications {
+      application XRX-1 {
+          protocol tcp;
+          destination-port 25;
+      }
+      application XRX-2 {
+          protocol tcp;
+          destination-port 21;
+      }
+      application-set MOJE-XRX {
+          application XRX-1;
+          application XRX-2;
+      }
+  }
```

Ex.Applications.3

```
lab@163# show|compare
[edit]
+  applications {
+      application XRX-1 {
+          protocol tcp;
+          destination-port 25;
+      }
+      application XRX-2 {
+          protocol tcp;
+          destination-port 21;
+      }
+      application-set MOJE-XRX {
+          application XRX-1;
```

```
+          application XRX-2;
+      }
+      application-set STANDARD-APP {
+          application junos-ftp;
+          application junos-http;
+          application junos-https;
+          application junos-ssh;
+      }
+  }
```

Ex.NAT.1

```
lab@163# set security nat source rule-set KADRY-INTERNET ?
Possible completions:
> rule                 Source NAT rule
> from                 Where is the traffic from
> to                   Where is the traffic to
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
[edit]
lab@163# set security nat source rule-set KADRY-INTERNET rule KADRY match
destination-address 1.1.4.0/24

[edit]
lab@163# set security nat source rule-set KADRY-INTERNET from zone KADRY

[edit]
lab@163# set security nat source rule-set KADRY-INTERNET to zone INTERNET

[edit]
lab@163# show|compare
[edit security]
+   nat {
+       source {
+           rule-set KADRY-INTERNET {
+               from zone KADRY;
+               to zone INTERNET;
+               rule KADRY {
+                   match {
+                       destination-address 1.1.4.0/24;
+                   }
+                   ## Warning: missing mandatory statement(s): 'then'
+               }
+           }
+       }
+   }


lab@163# set security nat source rule-set KADRY-INTERNET rule KADRY then
source-nat interface
```

```
[edit]
lab@163# show|compare
[edit security]
+   nat {
+       source {
+           rule-set KADRY-INTERNET {
+               from zone KADRY;
+               to zone INTERNET;
+               rule KADRY {
+                   match {
+                       destination-address 1.1.4.0/24; // 32 zawiera sie w
24
+                   }
+                   then {
+                       source-nat {
+                           interface;
+                       }
+                   }
+               }
+           }
+       }
+   }
```

Ex.NAT.2

```
lab@138# set interfaces ge-0/0/1 unit 400 family inet address 7.7.4.5/24

lab@163# delete routing-options
lab@163# set routing-options static route 0/0 next-hop 192.168.4.1

[edit]
lab@163# set security nat source rule-set KADRY-INTERNET rule KADRY-1

[edit]
lab@163# set security nat source rule-set KADRY-INTERNET rule KADRY-1 match
destination-?
Possible completions:
+ destination-address  Destination address
+ destination-address-name  Address/address-set from address book
> destination-port     Destination port
[edit]
lab@163# set security nat source rule-set KADRY-INTERNET rule KADRY-1 match
destination-address 7.7.4.0/29

[edit]
lab@163# set security nat source pool POOL-7_7_10_0_29 address 2.2.4.5/32

[edit]
lab@163# set security nat source rule-set KADRY-INTERNET rule KADRY-1 then
source-nat pool POOL-7_7_10_0_29
```

```
lab@163# show|compare
[edit security nat source]
+     pool POOL-7_7_10_0_29 {
+         address {
+             2.2.4.5/32;
+         }
+     }
[edit security nat source rule-set KADRY-INTERNET]
       rule KADRY { ... }
+      rule KADRY-1 {
+          match {
+              destination-address 7.7.4.0/29;
+          }
+          then {
+              source-nat {
+                  pool {
+                      POOL-7_7_10_0_29;
+                  }
+              }
+          }
+      }


lab@163# run show route

inet.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1.1.4.0/30         *[Direct/0] 00:41:47
                    > via ge-0/0/1.400
1.1.4.1/32         *[Local/0] 01:14:38
                      Local via ge-0/0/1.400
172.30.33.0/24     *[Direct/0] 01:14:31
                    > via ge-0/0/0.0
172.30.33.163/32   *[Local/0] 01:14:39
                      Local via ge-0/0/0.0
192.168.4.0/24     *[Direct/0] 00:41:43
                    > via ge-0/0/2.401
192.168.4.1/32     *[Local/0] 01:14:38
                      Local via ge-0/0/2.401
```

Ex.NAT.3

```
lab@163# set security nat source pool POOL-8_8_4_0_24 address 1.1.4.10
[edit]
lab@163# set security nat source rule-set KADRY-INTERNET from zone KADRY
lab@163# set security nat source rule-set KADRY-INTERNET to zone INTERNET
lab@163# set security nat source rule-set KADRY-INTERNET rule KADRY-2 match
destination-address 8.8.4.0/24
lab@163# set security nat source rule-set KADRY-INTERNET rule KADRY-2 then
source-nat pool POOL-8_8_4_0_24
```

```
lab@163# run show configuration security nat
source {
    pool POOL-7_7_10_0_29 {
        address {
            2.2.4.5/32;
        }
    }
    pool POOL-8_8_4_0_24 {
        address {
            1.1.4.10/32;
        }
    }
    rule-set KADRY-INTERNET {
        from zone KADRY;
        to zone INTERNET;
        rule KADRY {
            match {
                destination-address 1.1.4.0/24;
            }
            then {
                source-nat {
                    interface;
                }
            }
        }
        rule KADRY-1 {
            match {
                destination-address 7.7.4.0/29;
            }
            then {
                source-nat {
                    pool {
                        POOL-7_7_10_0_29;
                    }
                }
            }
        }
        rule KADRY-2 {
            match {
                destination-address 8.8.4.0/24;
            }
            then {
                source-nat {
                    pool {
                        POOL-8_8_4_0_24;
                    }
                }
            }
        }
    }
}
```

Ex.NAT.4

```
lab@163# set security nat proxy-arp interface ge-0/0/1.400 address 1.1.4.10
to 1.1.4.20
lab@163# show|compare
[edit security nat]
+    proxy-arp {
+        interface ge-0/0/1.400 {
+            address {
+                1.1.4.10/32 to 1.1.4.20/32;
+            }
+        }
+    }

lab@163# run show arp
MAC Address       Address         Name                      Interface
Flags
a8:d0:e5:a8:10:81 1.1.4.2         1.1.4.2                   ge-0/0/1.400
none
f8:b1:56:ab:39:d3 172.30.33.68    172.30.33.68              ge-0/0/0.0
none
00:24:dc:d0:7c:01 192.168.4.10    192.168.4.10              ge-0/0/2.401
none
Total entries: 3
```

Ex.RoutinOptions.NextHop.1

```
[edit]
lab@163# delete routing-options static route 0.0.0.0/0 next-hop 192.168.4.1

[edit]
lab@163# show|compare
[edit]
-  routing-options {
-      static {
-          route 0.0.0.0/0 next-hop 192.168.4.1;
-      }
-  }

[edit]
lab@163# set routing-options static route 0.0.0.0/0 next-hop 1.1.4.2

[edit]
lab@163# show|compare
[edit routing-options static]
-    route 0.0.0.0/0 next-hop 192.168.4.1;
+    route 0.0.0.0/0 next-hop 1.1.4.2;
```

Listy opcji

Ol.NAT.1

```
lab@163# set security nat ?
Possible completions:
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
> destination          Configure Destination NAT
> proxy-arp            Configure Proxy ARP
> proxy-ndp            Configure Proxy NDP
> source               Configure Source NAT
> static               Configure Static NAT
> traceoptions         NAT trace options

lab@163# set security nat source rule-set KADRY-INTERNET ?
Possible completions:
> rule                 Source NAT rule
> from                 Where is the traffic from
> to                   Where is the traffic to
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups

lab@163# set security nat source rule-set KADRY-INTERNET rule KADRY then ?
Possible completions:
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
> source-nat           Source NAT action
[edit]
lab@163# set security nat source rule-set KADRY-INTERNET rule KADRY then
source-nat ?
Possible completions:
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
> interface            Use egress interface address
  off                  No action
> pool                 Use Source NAT pool
[edit]
lab@163# set security nat source rule-set KADRY-INTERNET rule KADRY then
source-nat interface ?
Possible completions:
  <[Enter]>            Execute this command
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
> persistent-nat       Persistent NAT info
  |                    Pipe through a command
```

Ol.NAT.2-NAT STATIC

Z tego nie korzystamy.

```
lab@163# set security nat static rule-set KADRY-INTERNET ?
Possible completions:
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
> from                 Where is the traffic from
> rule                 Static NAT rule

lab@163# set security nat static rule-set KADRY-INTERNET from zone KADRY

lab@163# set security nat static rule-set KADRY-INTERNET rule KADRY match ?
Possible completions:
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
> destination-address  Destination address
> destination-address-name  Address from address book

lab@163# set security nat static rule-set KADRY-INTERNET rule KADRY match
destination-address 1.1.4.0/24

lab@163# set security nat static rule-set KADRY-INTERNET rule KADRY then ?
Possible completions:
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
> static-nat           Static NAT action
```