Konfiguracja LAN

Etap 1 - konfiguracja interfejsu LAN - dodajemy interfejs dla sieci lokalnej

#set interfaces ge-0/0/1 unit 0 family inet address 192.168.1.1/24

- ge-0/0/1 → port do sieci LAN
- 192.168.1.1 → brama dla hostów w LAN

Hosty będą miały np.:

IP: 192.168.1.10
GW: 192.168.1.1

Utworzenie stref bezpieczeństwa - wymagane w SRX (to jest firewall)
Firewall SRX działa na **strefach security**. Dodajemy strefę LAN:

#set security zones security-zone trust interfaces ge-0/0/1.0

Teraz mamy:

strefa	**interfejs**
trust	ge-0/0/1
untrust	ge-0/0/0

- **trust** → sieć wewnętrzna
- **untrust** → Internet

Zezwolenie na ruch do firewalla (host-inbound)

Pozwalamy hostom z LAN np. pingować firewall.
#set security zones security-zone trust host-inbound-traffic system-services ping

Oraz opcjonalnie ale nie zalecane w produkcji.
#set security zones security-zone trust host-inbound-traffic system-services ssh
Czyli będzie można zarządzać firewall z LAN.

Etap 2 - konfiguracja Source NAT. Bez NAT prywatne adresy **nie wyjdą do Internetu**.
Dodajemy regułę:

#set security nat source rule-set trust-to-untrust from zone trust
#set security nat source rule-set trust-to-untrust to zone untrust

I teraz tworzymy regułę NAT:

#set security nat source rule-set trust-to-untrust rule internet-nat match source-address 0.0.0.0/0
#set security nat source rule-set trust-to-untrust rule internet-nat then source-nat interface

Co to nam dało:
LAN IP → zamieniane na IP interfejsu WAN
Przykład: 192.168.1.10 → 10.0.137.250

Etap 3 - dodanie polityki firewall. Firewall **domyślnie blokuje wszystko.** Musimy dopuścić ruch z LAN do Internetu.

#set security policies from-zone trust to-zone untrust policy allow-internet match source-address any
#set security policies from-zone trust to-zone untrust policy allow-internet match destination-address any
#set security policies from-zone trust to-zone untrust policy allow-internet match application any
#set security policies from-zone trust to-zone untrust policy allow-internet then permit

Pamiętaj – zapisz konfigurację!!

#commit

zmienna	**znaczenie**
from-zone trust	ruch z LAN
to-zone untrust	do Internetu
application any	dowolny ruch
permit	zezwól

Etap 4 - konfiguracja hosta LAN np. VPC1 i test działania

Na komputerze w LAN:
IP: 192.168.1.10
Mask: 255.255.255.0
Gateway: 192.168.1.1
DNS: 8.8.8.8

Ping z hosta:

>ping 8.8.8.8

Na firewall możesz sprawdzić sesje:
>show security flow session

Sprawdzenie NAT:
>show security nat source translations

Finalna topologia

(LAN) 192.168.1.0/24 → 192.168.1.1 na ge-0/0/1 → (SRX) 10.0.137.250 na ge-0/0/0 → (ISP) 10.0.137.254 → Internet

Po testach przechodzimy do konfiguracji VLAN

Aby LAN był kompatybilny z VLAN usuwamy na vSRX

#delete interfaces ge-0/0/1 unit 0
#delete security zones security-zone trust interfaces ge-0/0/1.0

#commit