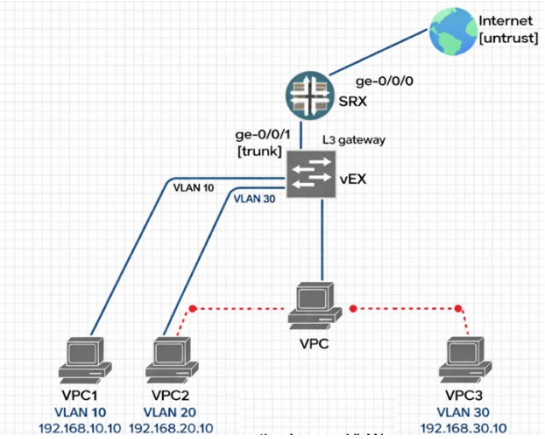
Po testach LAN przechodzimy do konfiguracji VLAN.

Aby LAN był kompatybilny z VLAN usuwamy:

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

Założenia

- ge-0/0/0 → do Internetu (untrust)
- ge-0/0/1 → do przełącznika (trunk)
- vEX → access VLAN dla VPC
- VPC mają mieć Internet, ale nie widzieć się między VLAN-ami
- Routing między VLAN realizuje SRX (L3 gateway)



VLAN-y i adresacja

Przykładowa adresacja dla czytelności

VLAN	Nazwa	Sieć	Gateway (SRX)
10	VLAN10	192.168.10.0/24	192.168.10.1
20	VLAN20	192.168.20.0/24	192.168.20.1
30	VLAN30	192.168.30.0/24	192.168.30.1

Etap 1 - konfiguracja przełącznika (vEX)

Założenie

- ge-0/0/0 → trunk do SRX
- ge-0/0/1 → VPC1 (VLAN10)
- ge-0/0/2 → VPC2 (VLAN20)
- ge-0/0/3 → VPC3 (VLAN30)

Tworzymy VLANy w trybie #configuration

#set vlans VLAN10 vlan-id 10
#set vlans VLAN20 vlan-id 20
#set vlans VLAN30 vlan-id 30

Port trunk do SRX na przełączniku vEX

#set interfaces ge-0/0/0 unit 0 family ethernet-switching port-mode trunk
#set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members [VLAN10 VLAN20 VLAN30]

Porty access do VPC

#set interfaces ge-0/0/1 unit 0 family ethernet-switching port-mode access
#set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members VLAN10

#set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode access
#set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members VLAN20

#set interfaces ge-0/0/3 unit 0 family ethernet-switching port-mode access
#set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members VLAN30

Zapisujemy zmiany w konfiguracji

commit

Etap 2 - Konfiguracja trunk + VLAN na vSRX

Teraz robimy tzw. router-on-a-stick na ge-0/0/1 (kilka vlanów na 1 kabel)

Jeżeli jest coś przypięte do ge-0/0/1.0 to kasujemy

Tworzymy podinterfejsy VLAN

#set interfaces ge-0/0/1 flexible-vlan-tagging
#set interfaces ge-0/0/1 encapsulation flexible-ethernet-services

VLAN 10

#set interfaces ge-0/0/1 unit 10 vlan-id 10
#set interfaces ge-0/0/1 unit 10 family inet address 192.168.10.1/24

VLAN 20

#set interfaces ge-0/0/1 unit 20 vlan-id 20
#set interfaces ge-0/0/1 unit 20 family inet address 192.168.20.1/24

VLAN 30

#set interfaces ge-0/0/1 unit 30 vlan-id 30
#set interfaces ge-0/0/1 unit 30 family inet address 192.168.30.1/24

Etap 3 - Strefy bezpieczeństwa

Tworzymy osobne strefy (żeby VLAN się nie widziały) Jeśli interfejs **nie jest w strefie**, to firewall **nie przepuści ruchu,** polityki **nie będą działać:**

#set security zones security-zone VLAN10 interfaces ge-0/0/1.10
#set security zones security-zone VLAN20 interfaces ge-0/0/1.20
#set security zones security-zone VLAN30 interfaces ge-0/0/1.30

Teraz Host-inbound traffic (ping do firewalla) - pozwala hostom **pingować firewall (gateway)**. Bez tego SRX blokuje ruch **do samego siebie**.

#set security zones security-zone VLAN10 host-inbound-traffic system-services ping
#set security zones security-zone VLAN20 host-inbound-traffic system-services ping
#set security zones security-zone VLAN30 host-inbound-traffic system-services ping

commit

Etap 4 - NAT do Internetu

Musimy zrobić source NAT (PAT) dla wszystkich VLAN.

#set security nat source rule-set INTERNET-NAT from zone VLAN10
#set security nat source rule-set INTERNET-NAT from zone VLAN20
#set security nat source rule-set INTERNET-NAT from zone VLAN30
#set security nat source rule-set INTERNET-NAT to zone untrust

#set security nat source rule-set INTERNET-NAT rule NAT-ALL match source-address 0.0.0.0/0
#set security nat source rule-set INTERNET-NAT rule NAT-ALL then source-nat interface

commit

Etap 5 - Polityki bezpieczeństwa

VLAN → Internet (zezwalamy)

#set security policies from-zone VLAN10 to-zone untrust policy VLAN10-INET match source-address any destination-address any application any
#set security policies from-zone VLAN10 to-zone untrust policy VLAN10-INET then permit

#set security policies from-zone VLAN20 to-zone untrust policy VLAN20-INET match source-address any destination-address any application any
#set security policies from-zone VLAN20 to-zone untrust policy VLAN20-INET then permit

#set security policies from-zone VLAN30 to-zone untrust policy VLAN30-INET match source-address any destination-address any application any
#set security policies from-zone VLAN30 to-zone untrust policy VLAN30-INET then permit

commit

SRX domyślnie blokuje ruch pomiędzy strefami, czyli zostawiamy bez polityki między VLAN.

- VLAN10 ↔ VLAN20
- VLAN10 ↔ VLAN30
- VLAN20 ↔ VLAN30

Etap 6 - Konfiguracja hostów VPC

VPC (VLAN10)

IP: 192.168.10.10
Maska: 255.255.255.0
GW: 192.168.10.1

VPC2 (VLAN20)

IP: 192.168.20.10
GW: 192.168.20.1

VPC3 (VLAN30)

IP: 192.168.30.10
GW: 192.168.30.1

Testujemy

Ping 8.8.8.8 z każdej VPC
Dostęp do Internetu
Brak pingu między VLAN-ami

Dodajemy DHCP na SRX dla VLAN 10/20/30

Użyjemy do tego **system services dhcp (legacy DHCP server)** - najprostsze i w pełni wystarczające w labie.

Założenia adresacji (jak wcześniej)

VLAN	Sieć	Gateway (SRX)	DHCP zakres
10	192.168.10.0/24	192.168.10.1	192.168.10.100–200
20	192.168.20.0/24	192.168.20.1	192.168.20.100–200
30	192.168.30.0/24	192.168.30.1	192.168.30.100–200

Etap 1 - Włączenie DHCP globalnie

#set system services dhcp-local-server group VLAN-DHCP interface ge-0/0/1.10
#set system services dhcp-local-server group VLAN-DHCP interface ge-0/0/1.20
#set system services dhcp-local-server group VLAN-DHCP interface ge-0/0/1.30

Etap 2 - Konfiguracja pul adresowych

VLAN10

#set access address-assignment pool VLAN10 family inet network 192.168.10.0/24
#set access address-assignment pool VLAN10 family inet range DHCP-RANGE low 192.168.10.100
#set access address-assignment pool VLAN10 family inet range DHCP-RANGE high 192.168.10.200
#set access address-assignment pool VLAN10 family inet dhcp-attributes router 192.168.10.1
#set access address-assignment pool VLAN10 family inet dhcp-attributes name-server 8.8.8.8

VLAN20

#set access address-assignment pool VLAN20 family inet network 192.168.20.0/24
#set access address-assignment pool VLAN20 family inet range DHCP-RANGE low 192.168.20.100
#set access address-assignment pool VLAN20 family inet range DHCP-RANGE high 192.168.20.200
#set access address-assignment pool VLAN20 family inet dhcp-attributes router 192.168.20.1
#set access address-assignment pool VLAN20 family inet dhcp-attributes name-server 8.8.8.8

VLAN30

#set access address-assignment pool VLAN30 family inet network 192.168.30.0/24
#set access address-assignment pool VLAN30 family inet range DHCP-RANGE low 192.168.30.100

#set access address-assignment pool VLAN30 family inet range DHCP-RANGE high 192.168.30.200
#set access address-assignment pool VLAN30 family inet dhcp-attributes router 192.168.30.1
#set access address-assignment pool VLAN30 family inet dhcp-attributes name-server 8.8.8.8

commit

Testujemy cała konfigurację:

Sprawdzenie interfejsów VLAN na SRX

>show interfaces terse | match ge-0/0/1

Pozwoli sprawdzić czy interfejs trunk i podinterfejsy VLAN są aktywne (**up/up**) i mają adresy IP.

Sprawdzenie sesji firewall na SRX

>show security flow session

Pozwoli sprawdzić czy firewall widzi ruch między hostem a Internetem (czy polityki firewall działają).

Sprawdzenie NAT na SRX

>show security nat source translations

Pozwoli sprawdzić adres prywatny z VLAN jest zamieniany na adres WAN (czy NAT działa).

Test połączenia z hosta na VPC

ping 192.168.10.1
ping 8.8.8.8

Pozwoli sprawdzić czy host ma połączenie z gateway oraz z Internetem.