**Juniper EX4400 switch teszt BGP Flowspec, és BGP RTBH update csomagok feldolgozásához**

A BGP FlowSpec és RTBH az elsődleges módja a standardizált ACL terjesztésének az interneten szolgáltatók között. A mérés célja, hogy a BME TMIT-en működő SmartCom Lab kipróbálja ezeket a technológiákat fizikai berendezéseken 100Gbps vonali ráta mellett.

1. Előkészítés:

A switch-re való belépéshez szükség van egy RS232/RJ45 (soros/etnernet), vagy USB/RJ45 átalakító kábelre, ezt kell a switch hátoldalán található „CON” elnevezésű portra csatlakoztatni.

Ezután terminálban csatlakozni kell a switchhez: baud 9600 8N1, no flow control

user: root, nincs password

Ezután be kell állítani a root jelszót, a management port IP címét, hogy lehessen SSH-n keresztül csatlakozni a switchez.

<https://www.juniper.net/documentation/us/en/hardware/ex4400/topics/topic-map/ex4400-configure-junos-os.html>

1. Config beállítások:

A beállításokhoz előbb át kell lépni CLI módba, a „cli” paranccsal.

Ezután a „configure” paranccsal lehet konfigurációs módba váltani.

Alapvetően a: „set <útvonal/paraméter> <érték>”

parancsokkal lehet beállításokat végezni, amiket a „commit” paranccsal lehet érvénysíteni. Visszavonni a még nem érvényesített paramétereket a „rollback” paranccsal lehet.

törölni a „delete <útvonal/paraméter> <érték>” paranccsal lehet.

* A BGP-flowspec-re vonatkozó beállításokat a következő doksi taglalja:

<https://www.juniper.net/documentation/en_US/day-one-books/DO_BGP_FLowspec.pdf>

* A BGP-RTBH-hoz a következő github repo ad támpontot:

<https://github.com/rendoaw/notes/blob/master/juniper/junos.rtbh.md>

A teljes switch konfig így néz ki:

root# show

## Last changed: 2022-04-21 10:48:57 UTC

version 21.2R2-S2.3;

#

# $Id:$

#

# Copyright (c) 2020, Juniper Networks, Inc.

# All rights reserved.

#

# Filename: ex4400-24t-factory.conf

# Platform: EX4400-24T

# Description: Factory default config for Junos.

#

#

system {

 root-authentication {

 encrypted-password "$6$ik2.qtpE$/LMf.DrELbylRxuICUfSqHus0UplFnUVf0/gJ5NkNb.d1RulDg2WXl7C.LGwti3oqFzxOnjXv5PGMMf.gnCmV."; ## SECRET-DATA

 }

 services {

 ssh {

 root-login allow;

 }

 netconf {

 ssh;

 rfc-compliant;

 yang-compliant;

 }

 }

 auto-snapshot;

 syslog {

 file interactive-commands {

 interactive-commands any;

 }

 file messages {

 any notice;

 authorization info;

 }

 }

 processes {

 dhcp-service {

 traceoptions {

 file dhcp\_logfile size 10m;

 level all;

 flag packet;

 }

 }

 }

 phone-home {

 server https://redirect.juniper.net;

 rfc-compliant;

 }

}

chassis {

 redundancy {

 graceful-switchover;

 }

}

interfaces {

 ge-0/0/0 {

 unit 0 {

 description FS0;

 family inet {

 address 192.168.2.1/30;

 }

 }

 }

 ge-0/0/1 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/2 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/3 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/4 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/5 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/6 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/7 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/8 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/9 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/10 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/11 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/12 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/13 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/14 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/15 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/16 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/17 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/18 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/19 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/20 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/21 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/22 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/0/23 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/1/0 {

 unit 0 {

 description to-B;

 family inet {

 address 10.10.10.1/30;

 }

 }

 }

 et-0/2/0 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/2/0 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 et-0/2/1 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/2/1 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 xe-0/2/1 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 et-0/2/2 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/2/2 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 xe-0/2/2 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 et-0/2/3 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 ge-0/2/3 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 xe-0/2/3 {

 unit 0 {

 family ethernet-switching {

 storm-control default;

 }

 }

 }

 irb {

 unit 0 {

 family inet {

 dhcp {

 vendor-id Juniper-ex4400-24t-ZC4321290021;

 }

 }

 family inet6 {

 dhcpv6-client {

 client-type stateful;

 client-ia-type ia-na;

 client-identifier duid-type duid-ll;

 vendor-id Juniper:ex4400-24t:ZC4321290021;

 }

 }

 }

 }

 lo0 {

 unit 0 {

 family inet {

 address 192.168.6.5/32;

 }

 }

 }

 me0 {

 unit 0 {

 family inet {

 address 192.168.60.1/24;

 }

 }

 }

 vme {

 unit 0 {

 family inet {

 dhcp {

 vendor-id Juniper-ex4400-24t-ZC4321290021;

 }

 }

 family inet6 {

 dhcpv6-client {

 client-type stateful;

 client-ia-type ia-na;

 client-identifier duid-type duid-ll;

 vendor-id Juniper:ex4400-24t:ZC4321290021;

 }

 }

 }

 }

}

forwarding-options {

 storm-control-profiles default {

 all;

 }

}

policy-options {

 policy-statement BH-IN {

 term blackhole {

 from community BLACKHOLE;

 then {

 community add no-export;

 next-hop 192.0.2.1;

 accept;

 }

 }

 term reject {

 then reject;

 }

 }

 policy-statement FS-RR-IN {

 term 1 {

 from {

 rib inetflow.0;

 route-filter 0.0.0.0/0 prefix-length-range /32-/32;

 }

 then accept;

 }

 term 2 {

 then reject;

 }

 }

 community BLACKHOLE members 100:5555;

 community no-export members 65535:65281;

}

routing-options {

 autonomous-system 12346;

 flow {

 term-order standard;

 }

}

protocols {

 router-advertisement {

 interface vme.0;

 interface irb.0;

 }

 ##

 ## Warning: One or more members of the VC require 'bgp' license

 ##

 bgp {

 group ibgp {

 family inet {

 flow;

 }

 }

 group BH {

 local-address 192.168.2.1;

 import BH-IN;

 neighbor 192.168.2.222;

 }

 group SP {

 export FS-RR-IN;

 neighbor 192.168.2.2 {

 family inet {

 flow;

 }

 }

 }

 traceoptions {

 file bgplog size 10k files 10;

 flag update receive detail;

 }

 bgp-error-tolerance {

 malformed-update-log-interval 10;

 malformed-route-limit 5;

 }

 peer-as 12346;

 }

 lldp {

 interface all;

 }

 lldp-med {

 interface all;

 }

 igmp-snooping {

 vlan default;

 }

 rstp {

 interface ge-0/0/1;

 interface ge-0/0/2;

 interface ge-0/0/3;

 interface ge-0/0/4;

 interface ge-0/0/5;

 interface ge-0/0/6;

 interface ge-0/0/7;

 interface ge-0/0/8;

 interface ge-0/0/9;

 interface ge-0/0/10;

 interface ge-0/0/11;

 interface ge-0/0/12;

 interface ge-0/0/13;

 interface ge-0/0/14;

 interface ge-0/0/15;

 interface ge-0/0/16;

 interface ge-0/0/17;

 interface ge-0/0/18;

 interface ge-0/0/19;

 interface ge-0/0/20;

 interface ge-0/0/21;

 interface ge-0/0/22;

 interface ge-0/0/23;

 }

}

vlans {

 default {

 vlan-id 1;

 l3-interface irb.0;

 }

}

* A management port a „me0 -> unit 0” útvonalon konfigolható.

IP: 192.168.60.1

* A „interfaces -> ge-0/0/0” a switch elülső oldalán található bal felső port. Ezt használjuk arra, hogy a BGP-speaker-ek kapcsolódjanak hozzá. Ez a port „router” módba van állítva, nem vesz részt az ethernet switchingben.

IP: 192.168.2.1/30, vagyis a 192.168.2.1 a címe, és pl. a 192.168.2.2 kliens címen tud még fogadni.

* A „policy-options” alatt lehet megadni, hogy pl. az egyes BGP opciókat hogyan dolgozza fel a switch.

Itt pl. a „policy-statement BH-IN” a Black-hole-ra vonatkozik (ha BLACKHOLE communityt talál a BGP update-ben, akkor kiértékeli)

A „policy-statement FS-RR-IN” pedig a Flowspec mitigáció bellításait tartalmazza.

* a „protocols -> bgp” alatt a „BH” (blackhole), és „SP” (flowspec) csoportok a BGP speakerekre vonatkozó kapcsolati infokat tartalmazzák, valamit hogy mi alapján kell kiértékelni a vett BGP update üzeneteket. [a „neighbor”-nál meghatározott IP címről várja a kapcsolódást, ezt át kell írni „192.168.2.2”-re, ha RTBH tesztet akarunk végezni]
* a „traceoptions” és „bgp-error-tolerance” opciók a logolás miatt kellenek; a „bgplog” fileba íródnak a részletes infók.
1. Flowspec teszt:

Kapcsolódjunk a BGP speakerünkkel a switchhez:

* IP source: 192.168.2.2
* IP destination (server): 192.168.2.1
* port: 179
* AS-Id: 12346

pl. IP cím beállítás: „sudo ifconfig eno1:0 192.168.2.2

BGP speaker indítása: „./sga\_fsactuator”

BGP update küldése (MP\_REACH) esetén ellenőrizzük, hogy a switch feldolgozta-e a beérkező kérést:

root> show bgp neighbor 192.168.2.2

Peer: 192.168.2.2+47394 AS 12346 Local: 192.168.2.1+179 AS 12346

 Group: SP Routing-Instance: master

 Forwarding routing-instance: master

 Type: Internal State: Established Flags: <Sync>

 Last State: OpenConfirm Last Event: RecvKeepAlive

 Last Error: None

 Export: [ FS-RR-IN ]

 Options: <AddressFamily PeerAS Refresh>

 Options: <GracefulShutdownRcv>

 Address families configured: inet-flow

 Holdtime: 90 Preference: 170

 Graceful Shutdown Receiver local-preference: 0

 Number of flaps: 4

 Last flap event: TransportError

 Malformed attributes log interval: 10 route limit: 5

 Peer ID: 192.168.2.2 Local ID: 192.168.6.5 Active Holdtime: 90

 Keepalive Interval: 30 Group index: 1 Peer index: 0 SNMP index: 5

 I/O Session Thread: bgpio-0 State: Enabled

 BFD: disabled, down

 NLRI for restart configured on peer: inet-flow

 NLRI advertised by peer: inet-unicast inet-flow inet6-flow

 NLRI for this session: inet-flow

 Peer does not support Refresh capability

 Stale routes from peer are kept for: 300

 Peer does not support Restarter functionality

 NLRI of all end-of-rib markers sent: inet-flow

 Peer does not support Receiver functionality

 Peer does not support LLGR Restarter or Receiver functionality

 Peer does not support 4 byte AS extension

 Peer does not support Addpath

 Table inetflow.0 Bit: 20000

 RIB State: BGP restart is complete

 Send state: in sync

 Active prefixes: 1

 Received prefixes: 1

 Accepted prefixes: 1

 Suppressed due to damping: 0

 Advertised prefixes: 0

 Last traffic (seconds): Received 21 Sent 21 Checked 335

 Input messages: Total 15 Updates 1 Refreshes 0 Octets 367

 Output messages: Total 14 Updates 0 Refreshes 0 Octets 277

 Output Queue[1]: 0 (inetflow.0, inet-flow)

 Trace options: detail recv update

 Trace file: /var/log/bgplog size 10240 files 10

A logban is ellenőrizhetjük a BGP-update feldolgozását:

root> show log bgplog

Apr 22 07:00:37 trace\_on: Tracing to "/var/log/bgplog" started

Apr 22 07:26:02.353210 BGP RECV 192.168.2.2+47394 -> 192.168.2.1+179

Apr 22 07:26:02.353239 BGP RECV message type 2 (Update) length 67

Apr 22 07:26:02.353248 BGP RECV Update PDU length 67

Apr 22 07:26:02.353263 BGP RECV flags 0x40 code Origin(1): IGP

Apr 22 07:26:02.353275 BGP RECV flags 0x40 code ASPath(2) length 0: <null>

Apr 22 07:26:02.353283 BGP RECV flags 0x40 code LocalPref(5): 100

Apr 22 07:26:02.353294 BGP RECV flags 0x90 code MP\_reach(14): AFI/SAFI 1/133

Apr 22 07:26:02.353333 BGP RECV 144.31.12.51,\*,srcport=53/72

Apr 22 07:26:02.353355 BGP RECV flags 0xc0 code Extended Communities(16): 8006:0:0

Apr 22 07:26:02.353443 bgp\_rcv\_nlri: Peer 192.168.2.2 (Internal AS 12346)

Apr 22 07:26:02.353463 bgp\_rcv\_nlri: 144.31.12.51,\*,srcport=53/72

A létrehozott FS szabály megtekintése:

root> show route table inetflow.0 extensive

inetflow.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

144.31.12.51,\*,srcport=53/term:1 (1 entry, 1 announced)

TSI:

KRT in dfwd;

Action(s): discard,count

 \*BGP Preference: 170/-101

 Next hop type: Fictitious, Next hop index: 0

 Address: 0xc5883fc

 Next-hop reference count: 1

 Source: 192.168.2.2

 Next hop:

 State: <Active Int Ext SendNhToPFE>

 Local AS: 12346 Peer AS: 12346

 Age: 9:30

 Validation State: unverified

 Task: BGP\_12346.192.168.2.2

 Announcement bits (1): 0-Flow

 AS path: I

 Communities: traffic-rate:0:0

 Accepted

 Localpref: 100

 Router ID: 192.168.2.2

 Thread: junos-main

A Flowspec rule eltávolítása után (BGP-update: MP\_UNREACH):

Table inetflow.0 Bit: 20000

 RIB State: BGP restart is complete

 Send state: in sync

 Active prefixes: 0

 Received prefixes: 0

 Accepted prefixes: 0

 Suppressed due to damping: 0

 Advertised prefixes: 0

 Last traffic (seconds): Received 5 Sent 5 Checked 1059

 Input messages: Total 43 Updates 2 Refreshes 0 Octets 945

 Output messages: Total 41 Updates 0 Refreshes 0 Octets 790

 Output Queue[1]: 0 (inetflow.0, inet-flow)

Log:

Apr 22 07:38:22.603996 BGP RECV 192.168.2.2+47394 -> 192.168.2.1+179

Apr 22 07:38:22.604033 BGP RECV message type 2 (Update) length 65

Apr 22 07:38:22.604046 BGP RECV Update PDU length 65

Apr 22 07:38:22.604055 BGP RECV flags 0x40 code Origin(1): IGP

Apr 22 07:38:22.604065 BGP RECV flags 0x40 code ASPath(2) length 0: <null>

Apr 22 07:38:22.604085 BGP RECV flags 0x40 code LocalPref(5): 100

Apr 22 07:38:22.604093 BGP RECV flags 0x90 code MP\_unreach(15): AFI/SAFI 1/133

Apr 22 07:38:22.604124 BGP RECV 144.31.12.51,\*,srcport=53/72

Apr 22 07:38:22.604139 BGP RECV flags 0xc0 code Extended Communities(16): 8006:0:0