「SRX300 セキュアルータ動作レポート」

BGPルータ / ファイアウォール / 負荷試験

ジュニパーネットワークス株式会社

2018年8月

目次

1. 概要
2. 検証 ①（BGP + ファイアウォール負荷試験）
3. 検証 ②（検証 ① + VRRP / MED）
4. まとめ

1. 概要

＝ 検証目的

- Juniper SRX300※を使用した ISP 連携環境を想定した動作検証

＝ 検証 ①

- EBGP によるルート情報の受信
- セキュリティポリシーによる通信制御およびロギング
- 通信負荷を印加した動作

＝ 検証 ②

- 検証 ①（EBGP ルート受信、セキュリティーポリシー制御）
- MED 値の付与と BGP アドバタイズ
- VRRP 構成を介したクライアント間通信

＝ 結果

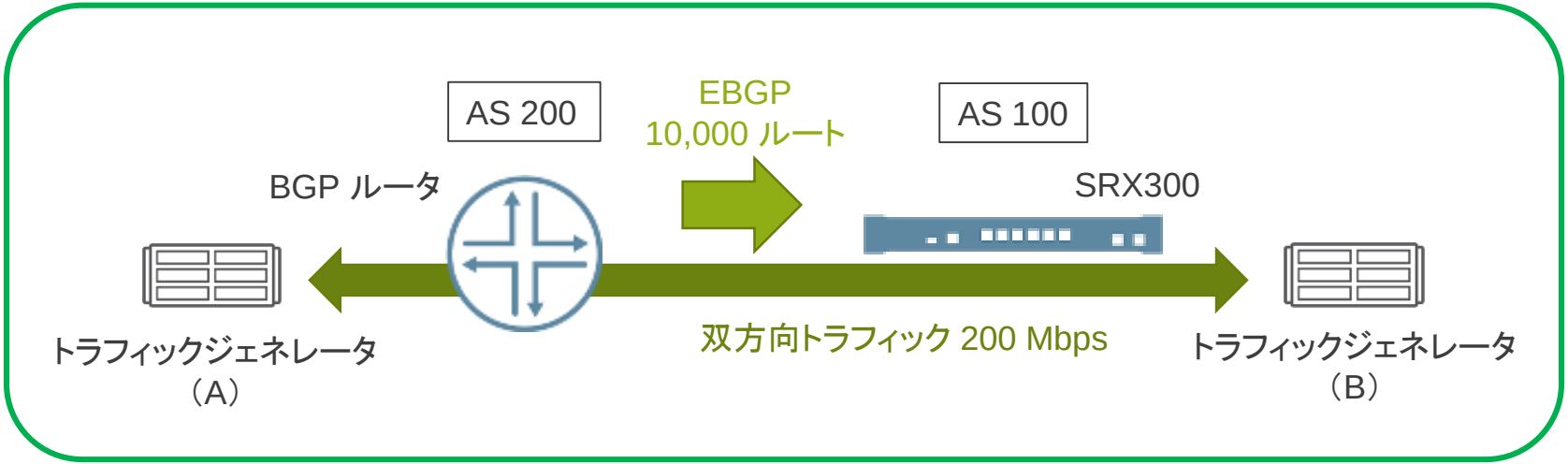
- 全ての検証項目が正常に動作
- 通信による負荷状況においても安定して稼働

（ ※使用 Junos バージョン: 15.1X49-D130 ）

2. 検証 ①（BGP + ファイアウォール負荷試験）

＝ 検証構成 ①

- BGP ルータから SRX300 に約 10,000 のルート情報をアドバタイズ
- トラフィックジェネレータ間（A、B）で双方向の通信を SRX300 のセキュリティポリシーで制御および、ロギング
- 許可トラフィックを双方向で印加（200 Mbps）



2. 検証 ①（BGP + ファイアウォール負荷試験）

＝ BGP ルートの受信動作

- SRX300 で受信した 10,000 以上の BGP ルート情報が正常にルーティングテーブルに追加される動作を確認

```
root@SRX300> show route summary
Autonomous system number: 100
Router ID: 10.1.1.1

inet.0: 10207 destinations, 10208 routes (10207 active, 0 holddown, 0 hidden)
              Direct:      3 routes,      3 active
               Local:      3 routes,      3 active
                 BGP:  10202 routes,  10201 active
```

＜SRX300 のルーティング情報＞

BGP ルート情報

2. 検証 ①（BGP + ファイアウォール負荷試験）

＝ セキュリティポリシーを使用したトラフィック制御

- SRX300 で双方向の許可通信、遮断通信に関連した各セキュリティポリシーのログ出力を確認

```
root@SRX300> show log Traffic-Log
Jun 26 14:53:14  SRX300 RT_FLOW: RT_FLOW_SESSION_CREATE: session created
10.101.1.101/63->10.102.1.102/445 0x0 None 10.101.1.101/63->10.102.1.102/445 0x0 N/A
N/A N/A N/A 17 BtoA IXIA BGP-Zone 60368 N/A(N/A) ge-0/0/1.0 UNKNOWN UNKNOWN UNKNOWN

Jun 26 14:53:14  SRX300 RT_FLOW: RT_FLOW_SESSION_CREATE: session created
10.102.1.102/63->10.101.1.101/445 0x0 None 10.102.1.102/63->10.101.1.101/445 0x0 N/A
N/A N/A N/A 17 AtoB BGP-Zone IXIA 60369 N/A(N/A) ge-0/0/0.0 UNKNOWN UNKNOWN UNKNOWN

Jun 26 14:53:41  SRX300 RT_FLOW: RT_FLOW_SESSION_DENY: session denied 10.101.1.101/1-
>10.102.1.102/1 0x0 unkn 61(0) BtoA_deny IXIA BGP-Zone UNKNOWN UNKNOWN N/A(N/A) ge-
0/0/1.0 UNKNOWN policy deny

Jun 26 14:53:41  SRX300 RT_FLOW: RT_FLOW_SESSION_DENY: session denied 10.102.1.102/1-
>10.101.1.101/1 0x0 unkn 61(0) AtoB_deny BGP-Zone IXIA UNKNOWN UNKNOWN N/A(N/A) ge-
0/0/0.0 UNKNOWN policy deny
```

許可ログ（B → A）

許可ログ（A → B）

遮断ログ（B → A）

遮断ログ（A → B）

＜SRX300 トラフィックログ情報＞

2. 検証 ①（BGP + ファイアウォール負荷試験）

＝ 許可通信の印加時の動作

- SRX300 で双方向の許可通信（フレームサイズ：512 bytes の udp パケット）を10分間 200Mbps で印加
  - トラフィックジェネレータ間で通信ロスや遅延がないことを確認
  - 機器リソースの使用率が安定した状態で動作していることを確認

```
root@SRX300> show chassis routing-engine
Routing Engine status:
    Temperature                 48 degrees C / 118 degrees F
    CPU temperature             62 degrees C / 143 degrees F
    Total memory              4096 MB Max  1065 MB used ( 26 percent)
      Control plane memory    2624 MB Max   682 MB used ( 26 percent)
      Data plane memory       1472 MB Max   383 MB used ( 26 percent)
    5 sec CPU utilization:
      User                      12 percent
      Background                 0 percent
      Kernel                     8 percent
      Interrupt                  0 percent
      Idle                      80 percent
```

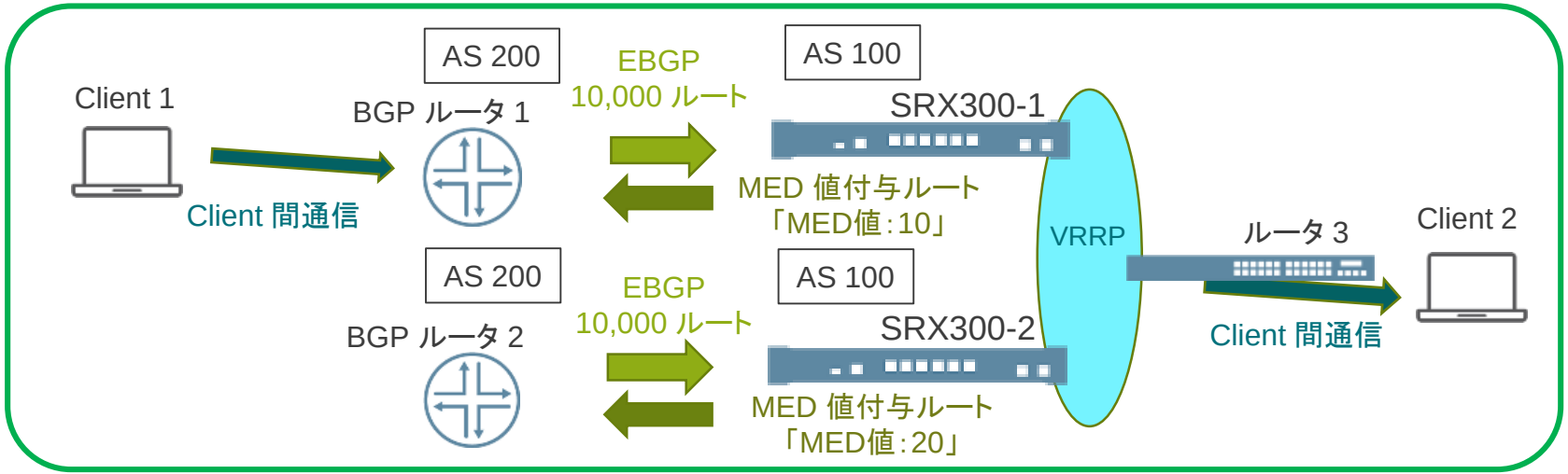
CPU 使用率 10% 前後で推移
（※非印加時：1% 前後）

＜SRX300 機器リソース情報＞

3. 検証 ②（検証 ① + VRRP / MED）

検証構成 ②

- SRX300-1 と SRX300-2 で VRRP を構成
- BGP ルータ（1、2）から双方の SRX300 に約 10,000 のルート情報をアドバタイズ
- 双方の SRX300 （1、2）から MED 値を付与したルート情報を BGP ルータ（1、2）にアドバタイズ
- Client1 から Client2 への通信を SRX300-1 の許可および、遮断セキュリティポリシーで制御



3. 検証 ②（検証 ① + VRRP / MED）

＝ VRRP 構成

- SRX300-1 と SRX300-2 間で VRRP が正しく構成されていることを確認

```
root@SRX300-2> show vrrp detail
Physical interface: ge-0/0/1, Unit: 0, Address: 10.101.1.2/24
  Index: 73, SNMP ifIndex: 504, VRRP-Traps: disabled, VRRP-Version: 2
  Interface state: up, Group: 25, State: backup, VRRP Mode: Active
  Priority: 200, Advertisement interval: 1, Authentication type: simple
  Advertisement threshold: 3, Computed send rate: 0
  Preempt: yes, Accept-data mode: yes, VIP count: 1, VIP: 10.101.1.100
  Dead timer: 3.171s, Master priority: 254, Master router: 10.101.1.1
  Virtual router uptime: 4d 00:32
  Tracking: disabled
```

＜SRX300-2 VRRP 情報＞

VRRP バックアップ（SRX300-2）で
マスター（SRX300-1）を認識

3. 検証 ②（検証 ① + VRRP / MED）

＝ BGP ルートの受信動作

- SRX300-1 と SRX300-2 で受信した 10,000 以上の BGP ルート情報が正常にルーティングテーブルに追加される動作を確認

```
root@SRX300-1> show route summary
Autonomous system number: 100
Router ID: 10.1.1.1
inet.0: 10212 destinations, 10213 routes (10212 active, 0 holddown, 0 hidden)
              Direct:      3 routes,      3 active
               Local:      4 routes,      4 active
                BGP:  10202 routes,  10201 active
              Static:      4 routes,      4 active
```

BGP ルート情報（SRX300-1）

```
root@SRX300-2> show route summary
Autonomous system number: 100
Router ID: 10.2.1.1
inet.0: 10206 destinations, 10207 routes (10206 active, 0 holddown, 0 hidden)
              Direct:      2 routes,      2 active
               Local:      2 routes,      2 active
                BGP:  10202 routes,  10201 active
              Static:      1 routes,      1 active
```

BGP ルート情報（SRX300-2）

＜SRX300-1 および SRX300-2 のルーティング情報＞

3. 検証 ②（検証 ① + VRRP / MED）

＝ MED 値を付与した BGP ルートのアドバタイズ動作

- SRX300-1 と SRX300-2 で MED 値の付与をしたルートが正常にアドバタイズされる動作を確認

```
BGP-RI-1.inet.0: 10210 destinations, 10211 routes (10210 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.1.0.0/24             *[BGP/170] 03:34:47, MED 10, localpref 100
                           AS path: 100 I, validation-state: unverified
                         > to 10.1.1.1 via ge-0/0/1.0
10.10.1.0/24            *[BGP/170] 04:09:31, MED 10, localpref 100
                           AS path: 100 I, validation-state: unverified
                         > to 10.1.1.1 via ge-0/0/1.0
```

SRX300-1 で付与の MED 値（BGP ルータ 1）

```
BGP-RI-2.inet.0: 10206 destinations, 10207 routes (10206 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.10.1.0/24            *[BGP/170] 04:08:10, MED 20, localpref 100
                           AS path: 100 I, validation-state: unverified
                         > to 10.2.1.1 via ge-0/0/2.0
10.101.1.0/24           *[BGP/170] 04:08:10, MED 20, localpref 100
                           AS path: 100 I, validation-state: unverified
                         > to 10.2.1.1 via ge-0/0/2.0
```

SRX300-2 で付与の MED 値（BGP ルータ 2）

＜BGP ルータ 1 および BGP ルータ 2 のルーティング（BGP）情報＞

3. 検証 ②（検証 ① + VRRP / MED）

＝ セキュリティポリシーを使用した特定通信トラフィックの制御

- SRX300-1 で Client1 から Client2 への遮断通信のログ出力、許可通信のセッション情報を確認
  (任意通信「any」の遮断ポリシー、特定通信「tcp/445」の遮断ポリシー、特定通信「icmp」の許可ポリシーを使用)

```
root@SRX300> show log Traffic-Log | match denied
Jul  2 17:45:37  SRX300 RT_FLOW: RT_FLOW_SESSION_DENY: session denied
10.3.1.1/64636->10.10.1.1/22 0x0 junos-ssh 6(0) C1toC2_deny BGP VRRP UNKNOWN
UNKNOWN N/A(N/A) ge-0/0/0.0 UNKNOWN policy deny

Jul  2 17:58:55  SRX300 RT_FLOW: RT_FLOW_SESSION_DENY: session denied
10.3.1.1/60343->10.10.1.1/445 0x0 junos-smb-session 6(0) C1toC2_deny-445 BGP
VRRP UNKNOWN UNKNOWN N/A(N/A) ge-0/0/0.0 UNKNOWN policy deny

root@SRX300> show security flow session protocol icmp
Session ID: 31554, Policy name: C1toC2_allow/5, Timeout: 2, Valid
  In: 10.3.1.1/4 --> 10.10.1.1/50739;icmp, Conn Tag: 0x0, If: ge-0/0/0.0, Pkts:
1, Bytes: 84,
  Out: 10.10.1.1/50739 --> 10.3.1.1/4;icmp, Conn Tag: 0x0, If: ge-0/0/1.0,
Pkts: 1, Bytes: 84,
```

任意通信の遮断ログ
（Client1 → Client2）

tcp/445 通信の遮断ログ
（Client1 → Client2）

許可通信 icmp の
セッション情報
（Client1 → Client2）

＜SRX300-1 の遮断ログ情報および、セッション情報＞

4. まとめ

＝ 結果のまとめ

Juniper SRX300 を ISP 接続連携用のルータとして使用した想定下で、
BGP を使った動的なルーティング情報の受信および、MED 値を付加したルーティング情報の配布処理、
さらには VRRP 構成を組んだ環境での動作を確認しました。

また、ルータとしての動作だけでなく、セキュリティポリシーを使ったファイアウォールとしての通信制御や
ロギング処理が、一定の通信負荷を印加した状況で、同時に問題無く行える結果となりました。

以上より、SRX300 がファイアウォール機能を備えた「セキュアルータ」として、複雑な接続環境において
豊富な機能性により柔軟に対応し、安心してご利用いただけることがわかります。

JUNIPER NETWORKS | Engineering Simplicity