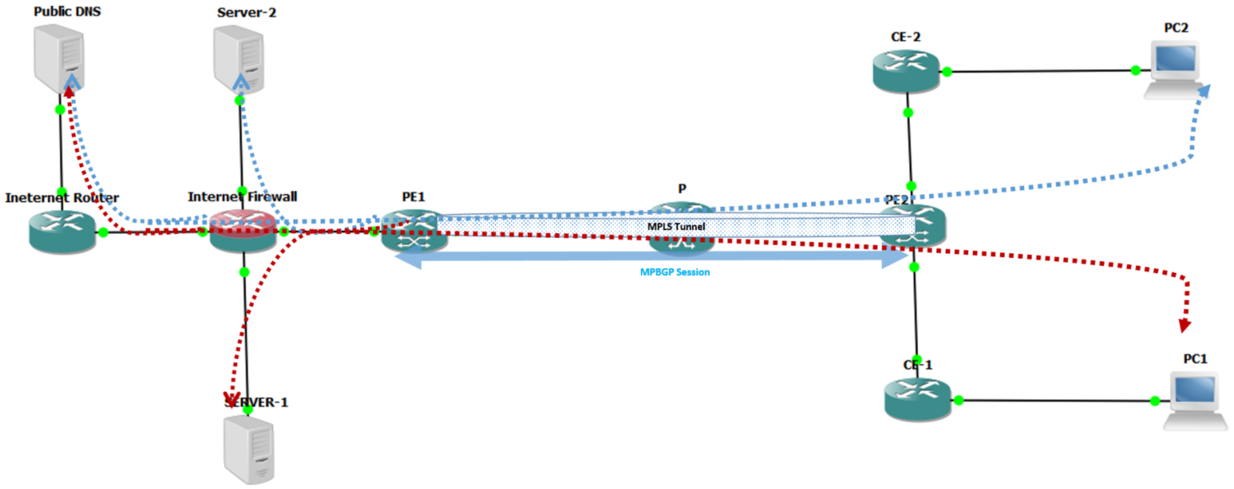
Packet Expert

Kashif Nawaz – JNCIEs (SP & Sec), RHCE and CKA

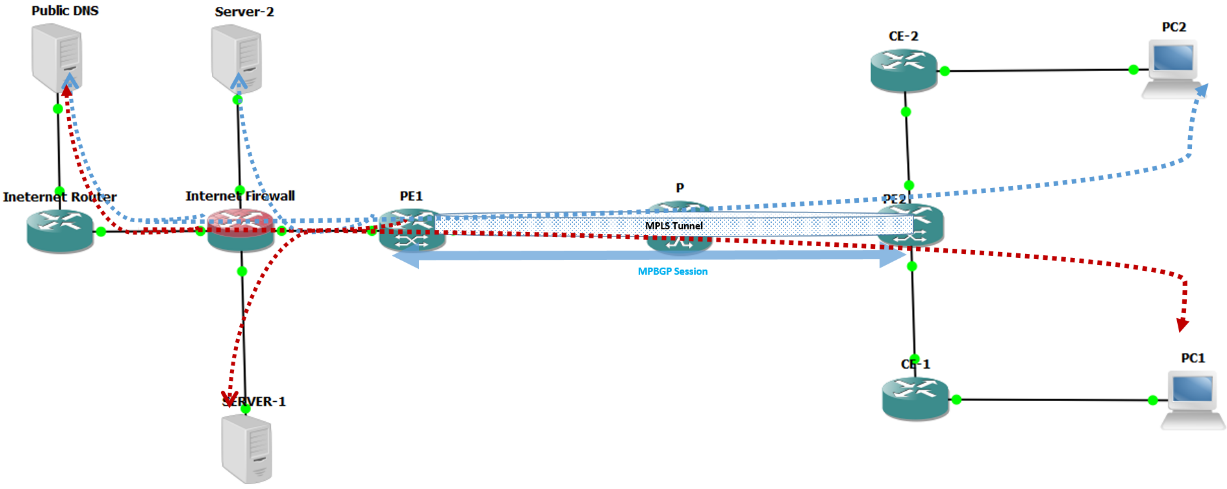
ROUTING

Integrating SRX in Svc Provider Network (Routing and Multi-tenancy Considerations)



Date: September 16, 2016 Author: packetexpert □ **0 Comments**

Service Providers networks are always have complex requirements of multi-tenancy, routing & security and pose challenges to network architects. In this blog I will write about SRX integration in Svc Provider Network while highlighting methodologies how to handle challenges of implementing security features with multi-tenancy and routing consideration.



REFERENCE TOPOLOGY

Devices have been classified into following segments based on their role:-

- **Remote Customer Network** (consist of Customer PCs connected to Provide Edge through Customer Edge).
- **Provider Network** (Consist of Provider Edge Routers and Provider Back Bone Rout
- **Data Center Network** (Consist of Internet Firewall and Server inside Data Center directly connected with Internet Firewall).
- **Internet Edge** (Consist of Internet Router connected with Internet Firewall hence providing internet access to Customer Networks connected with Data Center through provider network).

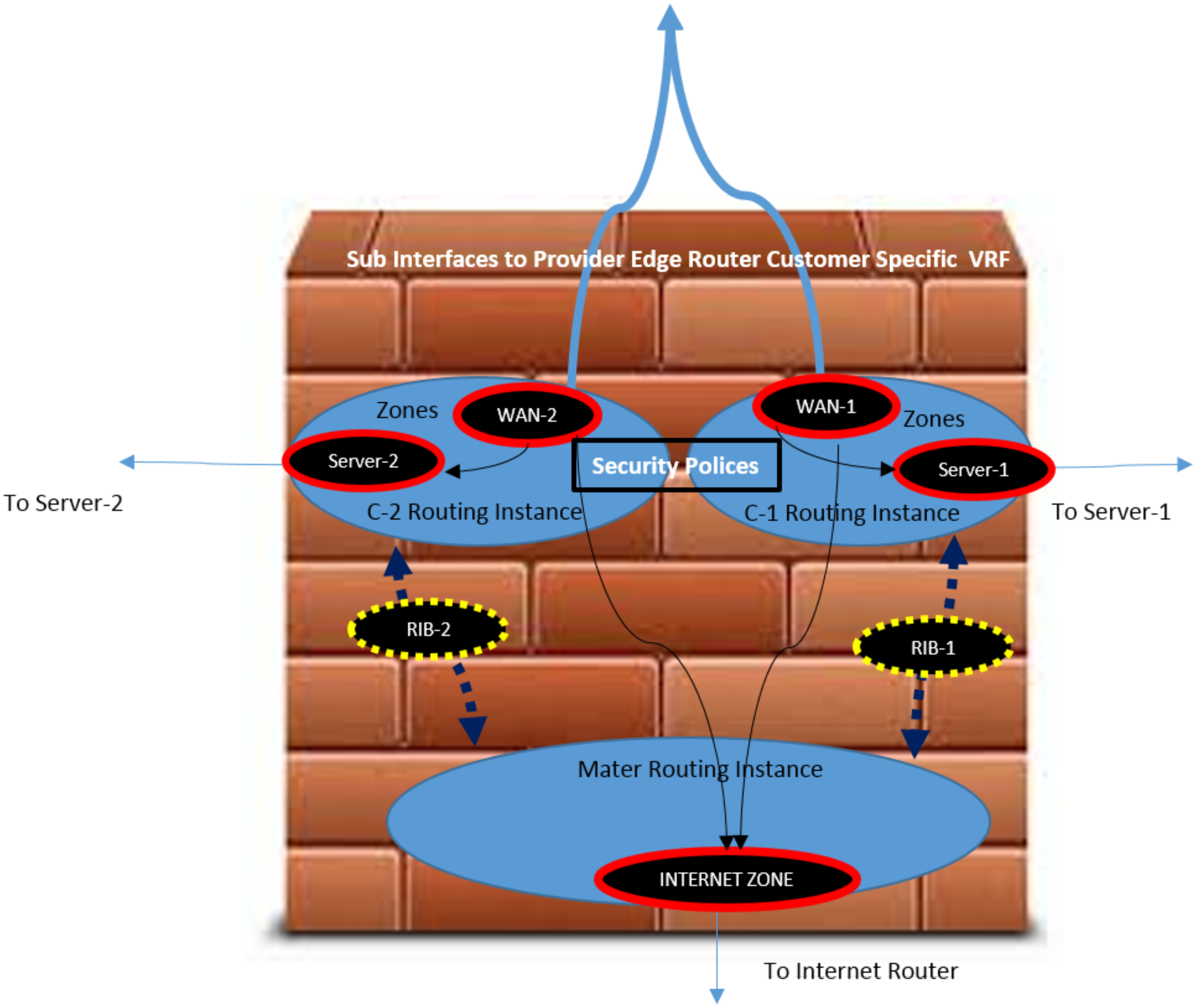
Traffic flow and security requirements are as under:-

- Customer 1 Network (PC-1) requires access to Server-1 installed in Data Center and to Public DNS Server reachable via Internet Edge Router.
- Customer 2 Network (PC-2) requires access to Server-2 installed in Data Center and to Public DNS Server reachable via Internet Edge Router.
- Complete isolation of customer routing domains (end to end).
- Implementation of security features (State full firewall, IPS, UTM and App Fire Wall) on clients' traffic accessing the servers inside the Data Centre to Public Server.

Provider Network Implementation:-

- IGP (OSFP / IS-IS) between Provider Edge and back bone router to provider reachability for signaling protocol (RSVP / LDP).
- MP-BGP Session among Provider Edge Routers to exchange MPVPN NLRI.
- Routing between Customer Edge and Provider can be static / IGP or BGP.

Main focus of this discussion will be on Internet Firewall (SRX) for security, multi-tenancy and routing consideration.



Multi-Tenancy is ensured by creating separate routing instances for Customer-1 and Customer-2 .

- Interfaces connected to Server-1 and Server-2 placed in specific Routing Instance.
- For connectivity between Internet Firewall and Provider Edge Router sub interfaces (on same physical interface) configured in Customer Specific VRF on both devices.
- In order to ensure internet reach-ability for customer remote network following approach is suited.
  - On Internet Firewall interface connected to Internet Router is automatically placed in Master Routing Instance so internet routes received form Internet Router (through BGP) are available in Internet Firewall Mater Routing Table.
  - For exchange of routing information from Customer to Master Routing Instance following approach is suited.
    - Separate RIB groups (for both customers) are configured with “import-rib” statement and applied to “interface-routes” and OSPF in Customer Instances.
    - It enables sharing of Customer Interface routes and Customer Remote Network Routes (reached in Internet Firewall though OSPF connectivity with Provider Edge Router).
    - In order to further control the route leakage (as per Customer requirement routes for Server placed in Data Center must not be leaked to Master Instance) routing policy can be configured and applied to rib-group (as import policy)
    - In order to share Mater Routing instance Interface routes and Internet Routes, routing policy can be configured and applied as “instance-import” inside Customer Instances.

  - Now these routes are only available in Customer Instance routing table but not advertised to Remote Customer Networks.
  - To achieve the desired results the same policy needs to apply to OSPF as export policy inside Customer Instance.
  - It will enable the advertisement of these routes to Provider Edge Router which will further re-distribute these routes to Remote Customer Network through MPBGP session between Provider Edge routers.

Despite of desired route sharing, Remote Customer Network still unable to reach Internet because Internet do not have reach-ability information for these private sub nets. Source NAT must be configured on Internet Firewall for traffic originated from Customer Instances and heading toward Internet Router to resolve this issue. Off course security, polices are required to allow the traffic form Customer WAN-Zone to Sever-Zone / Internet-Zone.

All these scenarios and requirements can be simulated in GNS3 using vSRX. I used vSRX in packet mode for Provider and Internet Router and off course in state full mode for Internet Firewall to simulate all scenarios.

ROUTING

Published by packetexpert

Every new second is coming up with some innovation in the IT industry , the basic and foremost important building block behind all technology innovations and updates is the "PACKET". I always endeavored to understand packet anatomy started from switch access port , securing it and then further traversing through IP / MPLS network till its destination. During my journey to understand packet anatomy I achieved 2 x JNCIEs (SP and Security) and currently learning Open-stack and SDN besides bit of automation stuff using Python. View all posts by packetexpert