Replacing Firewall (Brocade 5600 vRouter) with Firewall (vSRX)
## Update History

<table>
<thead>
<tr>
<th>Date</th>
<th>Update</th>
<th>Edition number</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018/10/24</td>
<td>first edition</td>
<td>1</td>
</tr>
</tbody>
</table>
Prerequisites
Prerequisites

*How to replace Firewall (Brocade 5600 vRouter) (vFW) with Firewall (vSRX)

*There is no change in the setting of the Internet-GW, Load balancer, or web server (Routing changes, etc.).

*Load balancer is two-arm model. For one-arm configuration, please replace the terms in accordance with your environment.

*Move the network used by the vFW to vSRX.
  => Communication is interrupted from disconnecting the network used by the vFW to the transfer to the vSRX.

*Please refer to the link below for basic vSRX configuration.

*Please configure the routing settings according to your configuration.

*When creating vSRX, the interface (Ge-0/0/0.0) is configured in the Trust zone.
  => After creation, please change each interface according to your environment.

*Both vFW and vSRX use stateful inspection.
  => If you use stateless firewall, please replace it according to your environment.

*Perform the migration after a pre-test.
Configuration and Migration Flow
Pre-migration Configuration (vFW Configuration)

* vFW rules deny all communications from external segments.
* Allow only HTTP/HTTPS communications from specific sources.
* Set up a virtual server inside LB.
* The following page describes vFW settings.
Pre-migration configuration (vFW Configuration) settings

Configuring vFW-01 Firewall Filter
set security firewall name From-Internet default-action 'drop'
set security firewall name From-Internet rule 10 action 'accept'
set security firewall name From-Internet rule 10 protocol 'tcp'
set security firewall name From-Internet rule 10 source address '180. xxx.xxx.xxx/32'
Set security firewall name From-Internet rule 10 destination port ' 80 '
Set security firewall name From-Internet rule 20 action 'accept'
Set security firewall name From-Internet rule 20 protocol 'tcp'
Set security firewall name From-Internet rule 20 source address '180. xxx.xxx.xxx/32'
set security firewall name From-Internet rule 20 destination port '443'
set security firewall name From-Internet rule 30 action 'accept'
set security firewall name From-Internet rule 30 protocol 'vrrp'
set security firewall name From-Internet rule 30 state 'enable'
set interface dataplane dp0s4 firewall in 'From-Internet'
Migration Configuration 1

1. firewall settings
   2. DNAT Configuration

192.168/20.0 24 (FW Segment)
- vFW-01
- dp0s 7.11

192.168/30.0 24 (external segment)
- Internet-GW (act)
- VRID 1
- VIP. 250

153. xxx.xxx.xxx/32
- Internet-GW (stb)
- VRID 1
- VIP. 250

172.16/10.0 24 (Server Segment)
- 1/1.6
- LB-01 (M)
- 1/2 6
- 1/2 7

172.16/10.0 24 (Server Segment)
- 1/1.7
- LB-02 (B)
- 1/2 7

180. xxx.xxx.xxx/32
- Client

192.168/30.0 24 (external segment)
- Internet-GW (act)
- VRID 1
- VIP. 250

192.168/30.0 24 (external segment)
- Internet-GW (stb)
- VRID 1
- VIP. 250

Step 1 vSRX Subscription
Step 2 vSRX Configuration
   1. firewall settings
   2. DNAT Configuration
Migration Configuration 2

1. Disconnect IF (communication interruption)

Disconnection time: approximately 50 minutes (measured value)
Migration Configuration 3

1. IF connection (communication interruption recovery)

192.168/20.0 24 (FW Segment)
VRID 30
VIP. 251

172.16/10.0 24 (Server Segment)
LB-01 (M)
1/1.6
1/2.6

http-vserver 172.16.100.1
https - vserver 172.16.100.2

Disconnection time: approximately 50 minutes (measured value)

Step 4 vSRX Configuration
Migration Configuration (Completed)

Network Diagram:
- **Client** connected to **InterNet**
  - **Internet-GW (act)** VRID 1 VIP. 250
  - **Internet-GW (stb)** VRID 1 VIP. 250
- **192.168/20.0 24 (FW Segment)**
  - **vFW-01**
    - Ge-0/0/1.11
    - Ge-0/0/2.11
  - **1/1.6 LB-01 (M)**
  - **1/2 6**
  - **1/2 7**
  - **VRID 30 VIP. 251**
- **192.168/30.0 24 (external segment)**
  - **153. xxx.xxx.xxx/32**
  - **192.168/30.0 24 (external segment)**
- **172.16/10.0 24 (Server Segment)**
  - **1/1.7 LB-02 (B)**
  - **VRID 30 VIP. 251**
  - **http-vserver 172.16.100.1**
  - **https - vserver 172.16.100.2**
  - **172.16/10.0 24 (Server Segment)**
- **172.16/10.0 24 (Server Segment)**
  - **1/1.6 LB-01 (M)**
  - **1/2 6**
  - **1/2 7**
- **InterNet-GW (act)** VRID 1 VIP. 250
- **InterNet-GW (stb)** VRID 1 VIP. 250

Connections:
- **Client** to **InterNet**
- **vFW-01** to **InterNet-GW (act)** VRID 1 VIP. 250
- **vFW-01** to **InterNet-GW (stb)** VRID 1 VIP. 250
- **InterNet-GW (act)** VRID 1 VIP. 250 to **http-vserver 172.16.100.1**
- **InterNet-GW (stb)** VRID 1 VIP. 250 to **https - vserver 172.16.100.2**
- **InterNet-GW (act)** VRID 1 VIP. 250 to **InterNet-GW (stb)** VRID 1 VIP. 250
- **InterNet-GW (act)** VRID 1 VIP. 250 to **InterNet-GW (stb)** VRID 1 VIP. 250

Addresses:
- **180. xxx.xxx.xxx/32**
- **153. xxx.xxx.xxx/32**
- **192.168.100.1**
- **192.168.100.2**
- **172.16.100.1**
- **172.16.100.2**
- **172.16.100.1**
- **172.16.100.2**
Step 1 vSRX Subscription
Step 1 vSRX Subscription

Please refer to the link below to apply for vSRX.

After logging in to the control panel screen, click Cloud Computing.
Click "NETWORK", "firewall", and "vSRX"
Click the Create Firewall button and enter the required settings for "Details" and "interface". Enter the management IP address in the interface setting. After entering the settings, click "Create Firewall".
Step 2 -1 vSRX Configuration (firewall settings)
Step 2 -1 vSRX Configuration  
(firewall settings)

See below for zone based firewall settings.  

Create an area in the firewall that is logically called the "zones" and make the interface belong to a zone.  
The policy required for incoming packets is set on a per-zone basis, allowing the same policy to be applied to interfaces belonging to the zone.

To set up a zone-based firewall, you need "Address Group Settings" and "Application Set Settings"
Step 2 -1 vSRX Configuration (firewall settings)

Please set up the address group referring to the following URL.

When you configure packet filtering, you can set rules based on IP addresses, and you can assign simple names to IP addresses to set packet filtering conditions. If you want to group multiple IP addresses, create an address book for each IP address and create an address set containing multiple address books.

For reference, the vSRX-01 configuration values are:

user @ vSRX-01 # set security address-book global address CLIENT _ 01 180. xxx.xxx.xxx/32
user @ vSRX-01 # set security address-book global address-set CLIENT _ GROUP address CLIENT _ 01
user @ vSRX-01 # commit
Step 2 - vSRX Configuration
(firewall settings)

Please set the application set referring to the following URL.

You can define applications that are pre-registered with vSRX, or you can name them arbitrarily, to make them a condition for packet filtering.

For reference, the vSRX-01 configuration values are:

user @ vSRX-01 # set applications HTTP _ DEF protocol tcp destination-port 80
user @ vSRX-01 # set applications application HTTPS _ DEF protocol tcp destination-port 443
user @ vSRX-01 # set applications application-set HTTP _ HTTPS _ DEF application HTTP _ DEF
user @ vSRX-01 # set applications application-set HTTP _ HTTPS _ DEF application HTTPS _ DEF
user @ vSRX-01 # commit
Step 2 -1 vSRX Configuration (firewall settings)

Allow communications that originate from the created address set and application set (packet), and block other communications (packet) with a zone-based firewall.

All communication from external segment is rejected, and only HTTP/HTTPS communication from specific source (180. xxx.xxx.xxx/32) is permitted as follows.

```
user @ vSRX-01 # set security policies from-zone untrust to -zone trust policy PERMIT _ GROUP match source-address CLIENT _
GROUP
user @ vSRX-01 # set security policies from-zone untrust to -zone trust policy PERMIT _ GROUP match destination-address any
user @ vSRX-01 # set security policies from -zone untrust to -zone trust policy PERMIT _ GROUP match application HTTP _
HTTPS _ DEF
user @ vSRX-01 # set security policies from-zone untrust to -zone trust policy PERMIT _ GROUP then permit
user @ vSRX-01 # commit
```
Step 2 - vSRX Configuration (DNAT Configuration)
Step 2 -2 vSRX Configuration (DNAT Configuration)

See below for Destination NAT configuration.
After logging in to the CLI,
Switch to shell command mode > operation mode > configuration mode.

Converts HTTP/HTTPS communications destined for 153. xxx.xxx.xxx/32 to the load balancer Virtual Server.
For reference, the vSRX-01 configuration values are listed on the next page.
Step 2 - vSRX Configuration
(DNAT Configuration)

The IP address translation settings for accessing the Virtual Server of the load balancer are as follows:

user @ vSRX-01 # set security nat destination pool POOL1 address 172.16.100.10/24 port 80
user @ vSRX-01 # set security nat destination pool POOL2 address 172.16.100.20/24 port 443
user @ vSRX-01 # set security nat destination rule-set RULE1 from zone untrust
user @ vSRX-01 # set security nat destination rule-set RULE1 rule RULE1 -1 match destination-address 153. xxx.xxx.xxx/32
user @ vSRX-01 # set security nat destination rule-set RULE1 rule RULE1 -1 match destination-port 80
user @ vSRX-01 # set security nat destination rule-set RULE1 rule RULE1 -2 match destination-address 153. xxx.xxx.xxx/32
user @ vSRX-01 # set security nat destination rule-set RULE1 rule RULE1 -2 match destination-port 443
user @ vSRX-01 # set security nat destination rule-set RULE1 rule RULE1 -2 then destination-nat pool POOL2
user @ vSRX-01 # commit
Step 3 vFW Settings (Disconnect Interface)
Step 3 Configure vFW (Disconnect Interface)

Please disconnect the logical network of firewall.
After logging in to the control panel screen, click "NETWORK" and "Brocade 5600 vRouter" to select the firewall.
Step 3 Configure vFW
(Disconnect Interface)

From that interface, click "Disconnect Logical Network"

If you click "Disconnect Logical Network", Communication is lost.
Step 4 vSRX Configuration (interface settings)
Step 4 vSRX Configuration
(interface settings)

To configure IP address and enable communication for interface that is configured on the vSRX, you must configure the interface and IP address on the ECL 2.0 customer portal.

Set the IP address of vSRX to the IP address used in the vFW.

vSRX interface is not initially configured to belong to a zone, except for ge-0/0/0. To communicate, you must belong to one of the zones of the zone-based firewall.

To allow incoming communication to IP address of interface, you need to configure the host to allow that communication under host-inbound-traffic.
Step 4 vSRX Configuration  
(interface settings)

Please refer to the link below to configure the vSRX interface on the ECL 2.0 customer portal.  
After logging in to the control panel screen, click Cloud Computing.  
Click "NETWORK", "firewall", and "vSRX"
Step 4 vSRX Configuration
(interface settings)

Click "Edit Firewall Interface" on vSRX.
Step 4 vSRX Configuration  
(interface settings)

Open the interface tab you want to edit, check "Edit this interface" and specify the logical network and static IP address you want to connect to.
After entering the set value, click "Edit Firewall Interface".

Please make sure to check "Edit this interface". If unchecked, edits are not reflected.

For your information, the following are the vSRX-01 configuration values:
Step 4 vSRX Configuration  
(interface settings)

Refer to the link below to configure the vSRX interface using the CLI.
https://ecl.ntt.com/en/documents/tutorials/rsts/vSRX/basic/basic.html#vsrx-cli-ssh

After logging in to the CLI,
Switch to shell command mode > operation mode > configuration mode.

For your information, the commands you enter in the CLI are:
* In this verification, ping is permitted in the host-inbound-traffic configuration.
  * If you have additional services or protocols that you want to allow, please refer to the link below for additional information.
  * Please set it accordingly.

```
user @ vSRX-01 # set interfaces ge-0/ 0/1 unit 0 family inet address 192.168.30.11/24
user @ vSRX-01 # set security zones security-zone untrust interfaces ge-0/0/1.0 host-invound-traffic system-services ping
user @ vSRX-01 # set interfaces ge-0/ 0/2 unit 0 family inet address 192.168.20.11/24
user @ vSRX-01 # set security zones security-zone trust interfaces ge-0/0/2.0 host-invound-traffic system-services ping
user @ vSRX-01 # commit
```

When the interface setting is completed, communication is restored.