vFWCL instantiation, testing, and debugging

Pre-requisite

Setup the OOM Infrastructure; I've used OOM on Rancher in OpenStack

Running vFW demo - Close-loop

Video of onboarding

I had a hickup at the end, due to the fact I already had another vFW deployed, hence the ip it tried to assign was used. To fix this, I remove the existing stack.

Video of instantiation

I had a hickup for the vFW_PG due to the fact I pre-loaded on the wrong instance. After realizing, all went well.

1. Let's start by running the init goal (assuming K8S namespace, where ONAP has been installed is "onap")

```
cd oom/kubernetes/robot
$ ./demo-k8s.sh onap init
```
2. Login into the VNC. Password is password

3. Open the browser and navigate to the ONAP Portal

   Login using the **Designer** user. cs0008/demo123456!


4. **Virtual Licence Model creation**
   a. Open SDC application, click on the **OnBoard** tab.
      i. click **Create new VLM** (Licence Model)
         1. Use onap as Vendor Name, and enter a description
         2. click save
         3. click **Licence Key Group** and **Add Licence Key Group**, then fill in the required fields
         4. click **Entitlements Pools and Add Entitlement Pool**, then fill in the required fields
         5. click **Feature Groups and Add Feature Group**, then fill in the required fields. Also, under the **Entitlement Pools** tab, drag the created entitlement pool to the left. Same for the **License Key Groups**
         6. click **Licence Agreements and Add Licence Agreement**, then fill in the required fields. Under the tab **Features Groups**, drag the feature group created previously.
         7. then **check-in and submit**
         8. go back to **OnBoard** page

5. **Vendor Software Product onboarding and testing**
   a. click **Create a new VSP**
      i. First we create the vFW sinc; give it a name, i.e. vFW_SINC. Select the Vendor (onap) and the Category (Firewall) and give it a description.
      ii. Click on the warning, and add a licence model
      iii. Get the zip package: vfw-sinc.zip
      iv. Click on overview, and import the zip
      v. Click **Proceed to validation** then **check-in** then **submit**
   b. click **Create a new VSP**
      i. Then we create the vFW packet generator; give it a name, i.e. vFW_PG. Select the Vendor (onap) and the Category (Firewall) and give it a description.
5. ii. Click on the warning, and add a licence model
   iii. Get the zip package: vfw_pg.zip
   iv. Click on overview, and import the zip
   v. Click **Proceed to validation then check-in then submit**

6. Service Creation
   a. Log out and login as the **designer**: cs0008/demo123456!
   b. Go to the SDC home page
   c. Click **Add a Service**
   d. Fill in the required field
   e. Click **Create**
   f. Click on the **Composition** tab
   g. In the search bar, type "vFW" to narrow down the created VSP, and drag them both.
   h. Then click **Submit for Testing**

7. Service Testing
   a. Log out and login as the **tester**: jm0007/demo123456!
   b. Go to the SDC portal
   c. Test and accept the service

8. Service Approval
   a. Log out and login as the **governor**: gv0001/demo123456!
   b. Go to the SDC portal
   c. Approve the service

9. Service Distribution
   a. Log out and login as the **operator**: op0001/demo123456!
   b. Go to the SDC portal
   c. Distribute the service
   d. Click on the left tab monitor and click on arrow to open the distribution status
   e. Wait until everything is distributed (green tick)

Expected output:

10. Service Instance creation:
    a. Log out and login as the **user**: demo/demo123456!
    b. Go to the VID portal
    c. Click the **Browse SDC Service Models** tab
    d. Click **Deploy** on the service to deploy
    e. Fill in the required field, call it vFW_Service for instance. Once done, this will redirect you to a new screen
    f. Click **Add VNF**, and select the vFW_SINC VNF first
    g. Fill in the required field. Call it vFW_SINC_VNF, for instance.
    h. Click **Add VNF**, and select the vFW_PG_VNF first
    i. Fill in the required field. Call it vFW_PG_VNF, for instance.

11. SDNC preload:
    a. Then go to the SDNC Admin portal and create an account
        
        <kubernetes-host-ip>:30201/signup
        
        b. Login into the SDNC admin portal
        
        <kubernetes-host-ip>:30201/login
        
        c. Click **Profiles** then **Add VNF Profile**
1. The VNF Type is the string that looks like this: VfwPg_base_vpkg_module-0 It can be copy/paste from VID, when attempting to create the VF-Module
2. Enter 100 for the Availability Zone Count
3. Enter vFW for Equipment Role
4. Repeat the same for the other VNF
5. Pre-load the vFW SINC. Mind the following values:
   - service-type: it's the service instance ID of the service instance created step 9
   - vnf-name: the name to give to the VF-Module. The same name will have to be re-use when creating the VF-Module
   - vnf-type: Same as the one used to add the profile in SDNC admin portal
   - generic-vnf-name: The name of the created VNF, see step 9f
   - vfw_name_0: is the same as the generic-vnf-name
   - generic-vnf-type: Can be find in VID, please see video if not found.
   - dcae_collector_ip: Has to be the IP address of the dcaedoks00 VM

Make sure image_name, flavor_name, public_net_id, onap_private_net_id, onap_private_subnet_id, key_name and pub_key reflect your environment

```bash
-H 'accept: application/json'
-H 'Authorization: Basic YWRtaW46S3A4Yko0U1hzek0wV1hsaGFzM2V1bGNzZTJnQxc4NH2hb0d8bUp2VXkyVQ=='
-H 'Content-Type: application/json'
-H 'x-fromappid: API client'
-d '{
  "input": {
    "vnf-topology-information": {
      "vnf-topology-identifier": {
        "service-type": "34992be5-b38c-46da-96b2-553e60f9c24b",
        "vnf-name": "vFW_SINC_Module",
        "vnf-type": "VfwSinc_base_vfw_module-0",
        "generic-vnf-name": "vFW_SINC_VNF",
        "generic-vnf-type": "vFW_SINC 0"
      },
      "vnf-assignments": {
        "availability-zones": [],
        "vnf-networks": [],
        "vnf-vms": []
      },
      "vnf-parameters": [
        {"vnf-parameter-name": "image_name", "vnf-parameter-value": "trusty"},
        {"vnf-parameter-name": "flavor_name", "vnf-parameter-value": "m1.medium"},
        {"vnf-parameter-name": "public_net_id", "vnf-parameter-value": "d87ff178-3eb7-44df-a57b-84636dbdc817"},
        {"vnf-parameter-name": "unprotected_private_net_id", "vnf-parameter-value": "zdfwlfw101_unprotected"},
        {"vnf-parameter-name": "unprotected_private_subnet_id", "vnf-parameter-value": "zdfwlfw101_unprotected_sub"},
        {"vnf-parameter-name": "protected_private_net_id", "vnf-parameter-value": "zdfwlfw101_protected"}
      ]
    }
  }
}'
```
"vnf-parameter-name": "protected_private_subnet_id",
"vnf-parameter-value": "zdfwlfw101_protected_sub"
},

"vnf-parameter-name": "onap_private_net_id",
"vnf-parameter-value": "onap_x0H4"
},

"vnf-parameter-name": "onap_private_subnet_id",
"vnf-parameter-value": "onap_x0H4"
},

"vnf-parameter-name": "unprotected_private_net_cidr",
"vnf-parameter-value": "192.168.10.0/24"
},

"vnf-parameter-name": "protected_private_net_cidr",
"vnf-parameter-value": "192.168.20.0/24"
},

"vnf-parameter-name": "onap_private_net_cidr",
"vnf-parameter-value": "10.0.0.0/16"
},

"vnf-parameter-name": "vfw_private_ip_0",
"vnf-parameter-value": "192.168.10.100"
},

"vnf-parameter-name": "vfw_private_ip_1",
"vnf-parameter-value": "192.168.20.100"
},

"vnf-parameter-name": "vfw_private_ip_2",
"vnf-parameter-value": "10.0.1.100.5"
},

"vnf-parameter-name": "vpg_private_ip_0",
"vnf-parameter-value": "192.168.10.200"
},

"vnf-parameter-name": "vsn_private_ip_0",
"vnf-parameter-value": "192.168.20.250"
},

"vnf-parameter-name": "vsn_private_ip_1",
"vnf-parameter-value": "10.0.1.100.4"
},

"vnf-parameter-name": "vfw_name_0",
"vnf-parameter-value": "vFW_SINC_VNF"
},

"vnf-parameter-name": "vsn_name_0",
"vnf-parameter-value": "zdfwlfw101snk01"
},

"vnf-parameter-name": "vnf_id",
"vnf-parameter-value": "vFirewal_vSink_demo_app"
},

"vnf-parameter-name": "vf_module_id",
"vnf-parameter-value": "vFirewall_vSink"
},

"vnf-parameter-name": "dcae_collector_ip",
"vnf-parameter-value": "10.195.200.38"
},

"vnf-parameter-name": "dcae_collector_port",
"vnf-parameter-value": "8080"
f. Pre-load the vFW PG. Mind the following values:

```json

[{
  "vnf-parameter-name": "repo_url_blob",
  "vnf-parameter-value": "https://nexus.onap.org/content/sites/raw"
},
{
  "vnf-parameter-name": "repo_url_artifacts",
  "vnf-parameter-value": "https://nexus.onap.org/content/groups/staging"
},
{
  "vnf-parameter-name": "demo_artifacts_version",
  "vnf-parameter-value": "1.1.1"
},
{
  "vnf-parameter-name": "install_script_version",
  "vnf-parameter-value": "1.1.1"
},
{
  "vnf-parameter-name": "key_name",
  "vnf-parameter-value": "onap_key_k0H4"
},
{
  "vnf-parameter-name": "pub_key",
  "vnf-parameter-value": "ssh-rsa AAAAB3NzaC1yc2EAAAADDAQABAQAAABACQMul5fnv0S4hXwXMxYx2YtqByeA+j82oH5toGPWENIr9u1hgRcIPWb5HSIDzhFLKy9KZ1ht5X2kzAcs1SKkod21VYyucG/QwqLNBNO5EMLVg6TudjUp/j/VDVsv9gp/xzIDsdHuhQ28VnRE88mKszTA4jRPFp4s4ic8eCes4nrydMrlbxeLjV3/+x/c77StQ7hD/3/l1JX8ztxgIrRcdxIQmMBWwb/4YSxjTbO0cwi4XY1RkzFY7vmO2VDrhfs0VtyvB8wa3AaqIP6CRz6QgbLjYjtiPbWmhKQ+0q0fJeb0Kkc7Beok7x58a3mlKhs wGSlJLaHCW1/b7n6C+lv adetalhouet@bell.corp.bce.ca"
},
{
  "vnf-parameter-name": "cloud_env",
  "vnf-parameter-value": "openstack"
}
],
"request-information": {
  "request-id": "robot12",
  "order-version": "1",
  "notification-url": "openecomp.org",
  "order-number": "1",
  "request-action": "PreloadVNFRequest"
},
"sdnc-request-header": {
  "svc-request-id": "robot12",
  "svc-notification-url": "http://openecomp.org:8080/adapters/rest/SDNCNotify",
  "svc-action": "reserve"
}
]

'
**service-type**: it's the service instance ID of the service instance created step 9

**vnf-name**: the name to give to the VF-Module. The same name will have to be re-use when creating the VF-Module

**vnf-type**: Same as the one used to add the profile in SDNC admin portal

**generic-vnf-name**: The name of the created VNF, see step 9h

**generic-vnf-type**: is the same as the generic-vnf-name

**vpg_name_0**: Can be find in VID, please see video if not found.

Make sure `image_name`, `flavor_name`, `public_net_id`, `onap_private_net_id`, `onap_private_subnet_id`, `key_name` and `pub_key` reflect your environment.

```bash
curl -X POST \
http://<kubernetes-host-ip>:30202/restconf/operations/VNF-API:preload-vnf-topology-operation \
-H 'accept: application/json' \
-H 'authorization: Basic YWRtaW46S3A4Yko0U1hzek0wVI1hsaGFzZM2V1bGNgZ2JjQXc4N9Zhb0dHUp2VXkyVQ==' \
-H 'content-type: application/json' \
-H 'x-fromappid: API client' \
-d '{
  "input": {
    "vnf-topology-information": {
      "vnf-topology-identifier": {
        "service-type": "df6e075a-119a-4790-a470-2474a692e3ce",
        "vnf-name": "vFW_PG_Module",
        "vnf-type": "vFW_PG..base_vpkg..module-0",
        "generic-vnf-name": "vFW_PG_VNF",
        "generic-vnf-type": "vFW_PG 0"
      },
      "vnf-assignments": {
        "availability-zones": [
        
        ],
        "vnf-networks": [
        
        ],
        "vnf-vms": [
        
        ]
      },
      "vnf-parameters": [
        {
          "vnf-parameter-name": "image_name",
          "vnf-parameter-value": "trusty"
        },
        {
          "vnf-parameter-name": "flavor_name",
          "vnf-parameter-value": "m1.medium"
        },
        {
          "vnf-parameter-name": "public_net_id",
          "vnf-parameter-value": "d87ff178-3eb7-44df-a57b-8463dbdc817"
        },
        {
          "vnf-parameter-name": "unprotected_private_net_id",
          "vnf-parameter-value": "zdfwlfw101_unprotected"
        },
        {
          "vnf-parameter-name": "unprotected_private_subnet_id",
          "vnf-parameter-value": "zdfwlfw101_unprotected_sub"
        },
        {
          "vnf-parameter-name": "onap_private_net_id",
          "vnf-parameter-value": "oam_onap_k0H4"
        },
        {
          "vnf-parameter-name": "onap_private_subnet_id",
          "vnf-parameter-value": "oam_onap_k0H4"
        },
        {
          "vnf-parameter-name": "unprotected_private_net_cidr",
          "vnf-parameter-value": "192.168.10.0/24"
        }
      }
    }
  }
}'}
["vnf-parameter-name": "protected_private_net_cidr",
"vnf-parameter-value": "192.168.20.0/24"
],
["vnf-parameter-name": "onap_private_net_cidr",
"vnf-parameter-value": "10.0.0.0/16"
],
["vnf-parameter-name": "vfw_private_ip_0",
"vnf-parameter-value": "192.168.10.100"
],
["vnf-parameter-name": "vpg_private_ip_0",
"vnf-parameter-value": "192.168.10.200"
],
["vnf-parameter-name": "vpg_private_ip_1",
"vnf-parameter-value": "10.0.80.2"
],
["vnf-parameter-name": "vsn_private_ip_0",
"vnf-parameter-value": "192.168.20.250"
],
["vnf-parameter-name": "vpg_name_0",
"vnf-parameter-value": "vFW_PG_VNF"
],
["vnf-parameter-name": "vnf_id",
"vnf-parameter-value": "vPacketGen_demo_app"
],
["vnf-parameter-name": "vf_module_id",
"vnf-parameter-value": "vPacketGen"
],
["vnf-parameter-name": "repo_url_blob",
"vnf-parameter-value": "https://nexus.onap.org/content/sites/raw"
],
["vnf-parameter-name": "repo_url_artifacts",
"vnf-parameter-value": "https://nexus.onap.org/content/groups/staging"
],
["vnf-parameter-name": "demo_artifacts_version",
"vnf-parameter-value": "1.1.1"
],
["vnf-parameter-name": "install_script_version",
"vnf-parameter-value": "1.1.1"
],
["vnf-parameter-name": "key_name",
"vnf-parameter-value": "vfw_key"
],
["vnf-parameter-name": "pub_key",
"vnf-parameter-value": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCmuLf5dnvO64h1wmxXyg2YtgByeA3j82oh5stoGPNENIr9u1hgRciPwb5HSIDzhFLKy9K021ht5X2EksAcis1TkkodzVLVyuCO/tqwlNN8O5EMLVm6TudjUp/j/Vdavv5Sgp/xzIDxSUh5QX5/HE888mKztsYAJj9P4s41c8eCes4nypMR1bxeLjV3J9/xJ77StQtbwB1JX8xtgRcdxIQmMBWw4Xj9jBo0Cwi4XXY1RzFsyS0VtvyVws6a3AqIP6C8z6QgbLYjtiFbWhmKQ+0qUJFjeb0Kkc7Beok7x5a3mHkhs wGSlaJLCaHC/Wib7n6C+lv adetalhouet@bell.corp.bce.ca"
],
["vnf-parameter-name": "cloud_env",
"vnf-parameter-value": "openstack"
]
"request-information": {
  "request-id": "robot12",
  "order-version": "1",
  "notification-url": "openecomp.org",
  "order-number": "1",
  "request-action": "PreloadVNFRequest"
},
"sdnc-request-header": {
  "svc-request-id": "robot12",
  "svc-notification-url": "http://openecomp.org:8080/adapters/rest/SDNCNotify",
  "svc-action": "reserve"
}
}

Expected result:

```
{
  "output": {
    "svc-request-id": "robot12",
    "response-code": "200",
    "ack-final-indicator": "Y"
  }
}
```

g. Create the VF-Module for vFW_SINC
   i. The instance name must be the `vnf-name` setup in the preload phase.
   ii. After a few minutes, the stack should be created.

h. Create the VF-Module for vFW_PG
   i. The instance name must be the `vnf-name` setup in the preload phase.
   ii. After a few minutes, the stack should be created.

Close loop

1. Run heatbridge robot tag to tell AAI about the relationship between the created HEAT stack (SINC one) and the service instance id.

   To run this, you need:
   - the heat stack name of the vSINC
   - the service instance id
$ ./demo-k8s.sh heatbridge vFW_SINC_Module 82678348-2f42-4ee7-bd29-0ef24b5e4bca vFW
Starting Xvfb on display :89 with res 1280x1024x24
Executing robot tests at log level TRACE
==============================================================================
OpenECOMP ETE
==============================================================================
OpenECOMP ETE.Robot
==============================================================================
OpenECOMP ETE.Robot.Testsuites
==============================================================================
OpenECOMP ETE.Robot.Testsuites.Demo :: Executes the VNF Orchestration Test ...
==============================================================================
Run Heatbridge :: Try to run heatbridge | PASS |
------------------------------------------------------------------------------
OpenECOMP ETE.Robot.Testsuites.Demo :: Executes the VNF Orchestration Test ... | PASS |
1 critical test, 1 passed, 0 failed
1 test total, 1 passed, 0 failed
==============================================================================
OpenECOMP ETE.Robot.Testsuites | PASS |
1 critical test, 1 passed, 0 failed
1 test total, 1 passed, 0 failed
==============================================================================
OpenECOMP ETE.Robot | PASS |
1 critical test, 1 passed, 0 failed
1 test total, 1 passed, 0 failed
==============================================================================
OpenECOMP ETE | PASS |
1 critical test, 1 passed, 0 failed
1 test total, 1 passed, 0 failed
==============================================================================
Output: /share/logs/demo/heatbridge/output.xml
Log: /share/logs/demo/heatbridge/log.html
Report: /share/logs/demo/heatbridge/report.html

2. Upload operational policy: this is to tell policy that for this specific instance, we should apply this policy.
   a. Retrieve from MSO Catalog the `modelInvariantUuid` for the `vFW_PG`. Specify in the below request the `service-model-name`, as defined step 5.c.

```
curl -X GET "http://<kubernetes-host>:30223/ecomp/mso/catalog/v2/serviceVnfs?serviceModelName=<service-model-names>" \
  -H 'Accept: application/json' \
  -H 'Authorization: Basic SW5mcmFQb3J0YWxDbGllbnQ6cGFzc3dvcmQxJA==' \
  -H 'Content-Type: application/json' \
  -H 'X-FromAppId: Postman' \
  -H 'X-TransactionId: get_service_vnfs'
```

Based on the payload below, result would be: 86a1bdd8-1f59-4796-bf30-3002108068f6
{
  "serviceVnfs": [
    {
      "modelInfo": {
        "modelName": "vFW_PG",
        "modelUuid": "7af8882e-f732-405f-b48b-38b6403654ea",
        "modelInvariantUuid": "86a1bd8-1f59-4796-bf30-302108068f6",
        "modelVersion": "1.0",
        "modelCustomizationUuid": "a2521929-d6da-46cc-9a62-ca3b6c3cef9b",
        "modelInstanceName": "vFW_PG 0"
      },
      "toscaNodeType": "org.openecomp.resource.vf.VfwPg",
      "nfFunction": "",
      "nfType": "",
      "nfRole": "",
      "nfNamingCode": "",
      "vfModules": [
        {
          "modelInfo": {
            "modelName": "VfwPg..base_vpkg..module-0",
            "modelUuid": "54a98442-52e3-46e8-8b40-193f04e92ff7",
            "modelInvariantUuid": "9c6c0369-a9c1-4419-94c9-aabf6250fc87",
            "modelVersion": "1",
            "modelCustomizationUuid": "35595818-2e09-4ad2-b6ce-2ffcc263489af"
          },
          "isBase": true,
          "vfModuleLabel": "base_vpkg",
          "initialCount": 1,
          "hasVolumeGroup": true
        }
      ]
    },
    {
      "modelInfo": {
        "modelName": "vFW_SINC",
        "modelUuid": "b8cc7acf-eba8-4ddb-950a-be52a96b28c8",
        "modelInvariantUuid": "edd473e1-7d08-4cf1-be31-0d705017f644",
        "modelVersion": "1.0",
        "modelCustomizationUuid": "c890203f-6b5b-4c43-aadb-250d8f6c5b0",
        "modelInstanceName": "vFW_SINC 0"
      },
      "toscaNodeType": "org.openecomp.resource.vf.VfwSinc",
      "nfFunction": "",
      "nfType": "",
      "nfRole": "",
      "nfNamingCode": "",
      "vfModules": [
        {
          "modelInfo": {
            "modelName": "VfwSinc..base_vfw..module-0",
            "modelUuid": "605ef192-e190-4043-97be-31ad64a2f8e",
            "modelInvariantUuid": "858e065b-7491-4e70-91e6-109a65c6102d",
            "modelVersion": "1",
            "modelCustomizationUuid": "acfa9f07-fe00-43ec-b9f9-0f874ce40c0a"
          },
          "isBase": true,
          "vfModuleLabel": "base_vfw",
          "initialCount": 1,
          "hasVolumeGroup": true
        }
      ]
    }
  ]
}

b. Under
invoke the script as follows:

```
Usage: update-vfw-op-policy.sh <k8s-host> <policy-pdp-node-port> <policy-drools-node-port>
<resource-id>
./update-vfw-op-policy.sh 10.195.197.53 30220 30221 86a1bdd8-1f59-4796-bf30-3002108068f
```

Result can look like, with debug enable (/bin/bash -x)

```
$ ./update-vfw-op-policy.sh 10.195.197.53 30220 30221 86a1bdd8-1f59-4796-bf30-3002108068f
+ '[' 4 -ne 4 ']
+ K8S_HOST=10.195.197.53
+ POLICY_PDP_PORT=30220
+ POLICY_DROOLS_PORT=30221
+ RESOURCE_ID=86a1bdd8-1f59-4796-bf30-3002108068f
+ echo
  + echo
  + echo 'Removing the vFW Policy from PDP..'
  + echo
  + echo
  + curl -v -X DELETE --header 'Content-Type: application/json' --header 'Accept: text/plain' --header 'ClientAuth: cHl0aG9uOnRlc3Q=' --header 'Authorization: Basic dGVzdHBkcDphbHBoYTEyMw==' --header 'Environment: TEST' -d '{
    "pdpGroup": "default",
    "policyComponent": "PDP",
    "policyName": "com.BRMSParamvFirewall",
    "policyType": "BRMS_Param"
}' http://10.195.197.53:30220/pdp/api/deletePolicy
  * Trying 10.195.197.53...  
  * Connected to 10.195.197.53 (10.195.197.53) port 30220 (#0)  
  > DELETE /pdp/api/deletePolicy HTTP/1.1  
  > Host: 10.195.197.53:30220  
  > User-Agent: curl/7.54.0  
  > Content-Type: application/json  
  > Accept: text/plain  
  > ClientAuth: cHl0aG9uOnRlc3Q=  
  > Authorization: Basic dGVzdHBkcDphbHBoYTEyMw==  
  > Environment: TEST  
  > Content-Length: 128  
  > * upload completely sent off: 128 out of 128 bytes  
  < HTTP/1.1 200 OK  
  < Server: Apache-Coyote/1.1  
  < Content-Type: text/plain; charset=ISO-8859-1  
  < Content-Length: 91  
  < Date: Wed, 20 Dec 2017 20:17:22 GMT  
  < * Connection #0 to host 10.195.197.53 left intact  
  Transaction ID: af030f0c-0c2b-43a1-blec-6abf4ca73799 --The policy was successfully deleted.+
```

```
Updating vFW Operational Policy..

```bash
+ echo
  "policyConfigType": "BRMS_PARAM",
  "policyName": "com.BRMSParamvFirewall",
  "policyDescription": "BRMS Param vFirewall policy",
  "policyScope": "com",
  "attributes": {
    "WATCHING": {
      "controller": "amsterdam"
    },
    "RULE": {
      "templateName": "ClosedLoopControlName",
      "closedLoopControlName": "ControlLoop-vFirewall-d0a1dfc6-94f5-4fd4-a5b5-4630b438850a",
      "controlLoopYaml": "controlLoop%0D%0A++version%3A+2.0.0%0D%0A++abatement%3A+false%0D%0A++policies%3A%0D%0A+++id%3A+unique-policy-id-1-modifyConfig%0D%0A+++name%3A+modify+packet+gen+config%0D%0A+++actor%3A+APPC%0D%0A+++recipe%3A+ModifyConfig%0D%0A+++target%3A+vFirewall%0D%0A+++%23+TBD+-+Cannot+be+known+until+instantiation+is+done%0D%0A+++resourceID%3A+86a1bdd8-1f59-4796-b330-30021b0068f0%0D%0A+++type%3A+VNF%0D%0A+++retry%3A+0%0D%0A+++timeout%3A+300%0D%0A+++success%3A+true%0D%0A+++failure%3A+false%0D%0A+++failure_timeout%3A+86a1bdd8-1f59-4796-b330-30021b0068f0%0D%0A+++failure_exception%3A+false%0D%0A+++failure_retries%3A+0%0D%0A+++failure_guard%3A+false%0D%0A+++failure_retries_guard%3A+false%0D%0A+++failure_retries_exception%3A+false%0D%0A+++failure_retries_exception_guard%3A+false%0D%0A
  }
}
```

* Trying 10.195.197.53...
  * TCP_NODELAY set
  * Connected to 10.195.197.53 (10.195.197.53) port 30220 (#0)
  * Connected to 10.195.197.53 (10.195.197.53) port 30220 (list of 0)
  * GET /pdp/api/updatePolicy HTTP/1.1
  * Host: 10.195.197.53:30220
  * User-Agent: curl/7.54.0

> HTTP/1.1 200 OK
> Server: Apache-Coyote/1.1
> Content-Type: text/plain;charset=ISO-8859-1
> Content-Length: 149
> Date: Wed, 20 Dec 2017 20:17:42 GMT
> Content-Length: 1327

+ CONTENT-TYPE: application/json
+ ACCEPT: text/plain
+ AUTHORIZATION: Basic dGVzdHBkcDphbHBoYTEyMw==
+ ENVIRONMENT: TEST
+ CONTENT-LENGTH: 1327
+ EXPECT: 100-continue
+ CONTENT-TYPE: application/json
+ ACCEPT: text/plain
+ AUTHORIZATION: Basic dGVzdHBkcDphbHBoYTEyMw==
+ ENVIRONMENT: TEST
+ CONTENT-LENGTH: 1327

* Connection #0 to host 10.195.197.53 left intact
Transaction ID: 20f4e273-d193-466c-8cce-e643a8545f5f -- Policy with the name com.BRMS_Param_BRMSParamvFirewall.2.xml was successfully updated. + sleep 5
  + echo
  + echo 'Pushing the vFW Policy ..'
PUSHING THE VFW POLICY...
  + echo
  + echo

```bash
  "pdpGroup": "default",
  "policyName": "com.BRMSParamvFirewall",
  "policyType": "BRMS_Param"
```
2.


* Trying 10.195.197.53...
* TCP_NODELAY set
* Connected to 10.195.197.53 (10.195.197.53) port 30220 (#0)
> PUT /pdp/api/pushPolicy HTTP/1.1
> Host: 10.195.197.53:30220
> User-Agent: curl/7.54.0
> Content-Type: application/json
> Accept: text/plain
> ClientAuth: cHl0aG9uOnRlc3Q=
> Authorization: Basic dGVzdHBkcDphbHBoYTEyMw==
> Environment: TEST
> Content-Length: 99
>
* upload completely sent off: 99 out of 99 bytes
HTTP/1.1 200 OK
< Server: Apache-Coyote/1.1
< Content-Type: text/plain;charset=ISO-8859-1
< Content-Length: 162
< Date: Wed, 20 Dec 2017 20:17:48 GMT
<
* Connection #0 to host 10.195.197.53 left intact
Transaction ID: e8bc4ae1-d0b0-483e-b1ba-871486651240 --Policy 'com.Config_BRMS_Param_BRMSParamvFirewall.2.xml' was successfully pushed to the PDP group 'default'.
sleep 20
+ echo
+ echo 'Restarting PDP-D ..'
Restarting PDP-D ..
+ echo
+ echo
++ kubectl --namespace onap-policy get pods
++ sed 's/ .*/\n'/
++ grep drools
+ POD=drools-870120400-5b5k1
++ kubectl --namespace onap-policy exec -it drools-870120400-5b5k1 -- bash -c 'source /opt/app/policy/etc/profile.d/env.sh && policy stop && sleep 5 && policy start'
Defaulting container name to drools.
Use 'kubectl describe pod/drools-870120400-5b5k1' to see all of the containers in this pod.
[drools-pdp-controllers]

L []: Stopping Policy Management... Policy Management (pid=5452) is stopping... Policy Management has stopped.
[drools-pdp-controllers]
L []: Policy Management (pid 5722) is running
+ sleep 20
+ echo
+ echo
+ echo 'PDP-D amsterdam maven coordinates ..'
PDP-D amsterdam maven coordinates..
+ echo
+ echo
+ curl -vvv --silent --user @1b3rt:31nst31n -X GET http://10.195.197.53:30221/policy/pdp/engine/controllers/amsterdam/drools
+ python -m json.tool
* Trying 10.195.197.53...
* TCP_NODELAY set
* Connected to 10.195.197.53 (10.195.197.53) port 30221 (#0)
* Server auth using Basic with user '@1b3rt'
> GET /policy/pdp/engine/controllers/amsterdam/drools HTTP/1.1
> Host: 10.195.197.53:30221
Authorization: Basic QDFiM3JD0jMx6bnV0MzFu
User-Agent: curl/7.54.0
Accept: */*

HTTP/1.1 200 OK
Date: Wed, 20 Dec 2017 20:18:49 GMT
Content-Type: application/json
Content-Length: 382
Server: Jetty(9.3.14.v20161028)

{ [382 bytes data]
  "alive": true,
  "artifactId": "policy-amsterdam-rules",
  "brained": true,
  "groupId": "org.onap.policy-engine.drools.amsterdam",
  "locked": false,
  "modelClassLoaderHash": 665564874,
  "recentSinkEvents": [],
  "recentSourceEvents": [],
  "sessionCoordinates": [
    "org.onap.policy-engine.drools.amsterdam:policy-amsterdam-rules:0.6.0:closedloop-amsterdam"
  ],
  "sessions": [
    "closedloop-amsterdam"
  ],
  "version": "0.6.0"
}

PDP-D control loop updated..


{ [1207 bytes data]
  "closedLoopControlName": "ControlLoop-vCPE-48f0c2c3-a172-4192-9ae3-052274181b6e",
  "controlLoopYaml": "ControlLoop%0A+version%3A+2.0.0%0A+controlLoopName%3A+ControlLoop-vCPE-48f0c2c3-a172-4192-9ae3-052274181b6e%0A+trigger_policy%3A+unique-policy-id-1-restart%0A+timeout%3A+3600%0A+abatement%3A+true%0A+policies%3A+"+id%3A+ Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+Restart%3A+id%3A+ Restart%3A+target%3A+VM%0A+retry%3A+3+timeout%3A+1200+success%3A+final_success+failure%3A+final_failure+failure_timeout%3A+final_failure_timeout+failure_retries%3A+"
3A+final_failure_retries%0D%0A+++failure_exception%3A+final_failure_exception%0D
0A+++failure_guard%3A+final_failure_guard"
],
{
 "closedLoopControlName": "ControlLoop-vFirewall-d0a1dfc6-94f5-4fd4-a5b5-4630b438850a",
 "controlLoopYaml": "controlLoop%3A%0D%0A++version%3A+2.0.0%0D%0A++controlLoopName%0D%0A+++id%3A+unique-policy-id-1-modifyConfig%0D%0A+++name%3A+ModifyConfig%0D%0A+++description%3A+ModifyConfig%0D%0A+++actor%3A+APPC%0D%0A+++recipe%3A+ModifyConfig%0D%0A+++target%3A+VNF%0D%0A+++retry%3A+0%0D%0A+++timeout%3A+300%0D%0A+++success%3A+final_success%0D%0A+++failure%3A+final_failure%0D%0A+++failure_timeout%3A+final_failure_timeout%0D%0A+++failure_retries%3A+final_failure_retries%0D%0A+++failure_exception%3A+final_failure_exception%0D%0A+++failure_guard%3A+final_failure_guard",
 "closedLoopControlName": "ControlLoop-vDNS-6f37f56d-a87d-4b85-b6a9-cc953cf779b3",
 "controlLoopYaml": "controlLoop%3A%0D%0A++version%3A+2.0.0%0D%0A++controlLoopName%0D%0A+++id%3A+unique-policy-id-1-scale-up%0D%0A+++name%3A+Create+a+new+VF+Module%0D%0A+++description%3A+Create+a+new+VF+Module%0D%0A+++actor%3A+SO%0D%0A+++recipe%3A+VF+Module+Create%0D%0A+++target%3A+VNF%0D%0A+++retry%3A+0%0D%0A+++timeout%3A+1200%0D%0A+++success%3A+final_success%0D%0A+++failure%3A+final_failure%0D%0A+++failure_timeout%3A+final_failure_timeout%0D%0A+++failure_retries%3A+final_failure_retries%0D%0A+++failure_exception%3A+final_failure_exception%0D%0A+++failure_guard%3A+final_failure_guard",
 "closedLoopControlName": "ControlLoop-VOLTE-2179b738-fd36-4843-a71a-a8c24c70c55b",
 "controlLoopYaml": "controlLoop%3A%0D%0A++version%3A+2.0.0%0D%0A++controlLoopName%0D%0A+++id%3A+unique-policy-id-1-restart%0D%0A+++name%3A+Restart+the+VM%0D%0A+++description%3A+Restart+the+VM%0D%0A+++actor%3A+VFC%0D%0A+++recipe%3A+Restart%0D%0A+++target%3A+VM%0D%0A+++retry%3A+3%0D%0A+++timeout%3A+1200%0D%0A+++success%3A+final_success%0D%0A+++failure%3A+final_failure%0D%0A+++failure_timeout%3A+final_failure_timeout%0D%0A+++failure_retries%3A+final_failure_retries%0D%0A+++failure_exception%3A+final_failure_exception%0D%0A+++failure_guard%3A+final_failure_guard"
]
}

3. Mount APPC
a. Get the VNF instance ID, either through VID or through AAI. Below the AAI request

```bash
curl -X GET \nhttps://<kubernetes-host>:30233/aai/v8/network/generic-vnfs/ \n-H 'Accept: application/json' \n-H 'Authorization: Basic QUFWJokFB05w=='
-H 'Content-Type: application/json' \n-H 'X-FromAppId: Postman' \n-H 'X-TransactionId: get_generic_vnf'
```

In the result, search for the vFW_PG_VNF and get its vnf-id. In the payload below, it would be e6fd06b4-4f36-4a21-963c-cc9060127633

```json
{
 "generic-vnf": [
  {
   "vnf-id": "9663a27e-8fbe-4fde-bc33-064ae45caee6",
   "vnf-name": "vFW_SINC_VNF",
   "vnf-type": "vFW_Service/vFW_SINC 0",
   "service-id": "75a0214a-6519-4505-b418-134e9b836023",
   "prov-status": "PREPROV",
   "orchestration-status": "Created",
   "in-maint": false,
   "is-closed-loop-disabled": false,
   "resource-version": "1513788953961",
   "closedLoop
```
"persona-model-id": "edd473e1-7d08-4cf1-be31-0d705017f644",
"persona-model-version": "1.0",
"relationship-list": [
  {
    "related-to": "service-instance",
    "relationship-data": {
      {
        "relationship-key": "customer.global-customer-id",
        "relationship-value": "Demonstration"
      },
      {
        "relationship-key": "service-subscription.service-type",
        "relationship-value": "vFWCL"
      },
      {
        "relationship-key": "service-instance.service-instance-id",
        "relationship-value": "63b55891-ebc6-40bf-b884-2e2427280a83"
      }
    },
    "related-to-property": {
      {
        "property-key": "service-instance.service-instance-name",
        "property-value": "vFWServiceInstance-20-12"
      }
    }
  }
],
"vf-modules": {
  "vf-module": [
    {
      "vf-module-id": "fc8ba83f-2ebf-4066-bb3a-f581667f77da",
      "vf-module-name": "vFW_SINC_Module",
      "heat-stack-id": "vFW_SINC_Module/09b1a25e-4ef0-4490-9b05-d79c00c7d218",
      "orchestration-status": "active",
      "is-base-vf-module": true,
      "resource-version": "1513790007998",
      "persona-model-id": "858e065b-7491-4c70-91e6-109a65c6102d",
      "persona-model-version": "1"
    }
  ]
},
"vnf-id": "e6fd60b4-f436-4a21-963c-cc9060127633",
"vnf-name": "vFW_PG_VNF",
"vnf-type": "vFW_Service/vFW_PG 0",
"service-id": "75af21a4-6519-4505-b418-134e9e836023",
"prov-status": "PREPROV",
"orchestration-status": "Created",
"in-maint": false,
"is-closed-loop-disabled": false,
"resource-version": "1513788903856",
"persona-model-id": "86a1bdd8-1f59-4796-bf30-3002108068f6",
"persona-model-version": "1.0",
"relationship-list": {
  "related-to": "service-instance",
  "relationship-data": {
    "relationship-key": "customer.global-customer-id",
    "relationship-value": "Demonstration"
  }
}
b. Get the public IP address of the Packet Generator from your deployment.

c. In the below curl request, replace <vnf-id> with the VNF ID retrieved at step 2.a (it needs to be updated at two places), and replace <vnf-ip> with the ip retrieved at step 2.b.

```
curl -X PUT
   /topology-netconf/node/<vnf-id> \
   -H 'Accept: application/xml'
   -H 'Authorization: Basic YWRtaW46S3A4Yko0U1hzek0wV1hsaGFrM2V1bGNzETJnQXc4NH2hb0dHbUpVXXkyVQ==' 
   -H 'Content-Type: text/xml'
   -d '<node xmlns="urn:TBD:params:xml:ns:yang:network-topology">
     <node-id><vnf-id></node-id>
     <host xmlns="urn:opendaylight:netconf-node-topology"><vnf-ip></host>
     <port xmlns="urn:opendaylight:netconf-node-topology">2831</port>
     <username xmlns="urn:opendaylight:netconf-node-topology">admin</username>
     <password xmlns="urn:opendaylight:netconf-node-topology">admin</password>
     <tcp-only xmlns="urn:opendaylight:netconf-node-topology">false</tcp-only>
   </node>'
```

If you want to verify the NETCONF connection has successfully being established, use the following request (replace <vnd-id> with yours)

```
curl -X GET
   /topology-netconf/node/<vnf-id> \
   -H 'Accept: application/json'
   -H 'Authorization: Basic YWRtaW46S3A4Yko0U1hzek0wV1hsaGFrM2V1bGNzETJnQXc4NH2hb0dHbUpVXXkyVQ=='
```

Result should be:
"node": {
  "node-id": "e6fd60b4-f436-4a21-963c-cc9060127633",
  "netconf-node-topology:available-capabilities": {
    "available-capability": {
      "capability-origin": "device-advertised",
      "capability": "urn:ietf:params:netconf:capability:exi:1.0"
    },
    "capability-origin": "device-advertised",
    "capability": "urn:ietf:params:netconf:capability:candidate:1.0"
  },
  "capability-origin": "device-advertised",
  "capability": "urn:ietf:params:netconf:base:1.1"
},
"capability-origin": "device-advertised",
"capability": "urn:ietf:params:netconf:base:1.0"
},
"capability-origin": "device-advertised",
},
"capability-origin": "device-advertised",
},
"capability-origin": "device-advertised",
},
"capability-origin": "device-advertised",
},
"capability-origin": "device-advertised",
},
"capability-origin": "device-advertised",
"capability": "(urn:ietf:params:xml:ns:yang:ietf-access-control-list?revision=2016-07-08)ietf-access-control-list"
},
"capability-origin": "device-advertised",
},
"capability-origin": "device-advertised",
},
"capability-origin": "device-advertised",
},
"capability-origin": "device-advertised",
"capability-origin": "device-advertised",
},

"capability-origin": "device-advertised",
},

"capability-origin": "device-advertised",
},

"capability-origin": "device-advertised",
},

"capability-origin": "device-advertised",
},

"capability-origin": "device-advertised",
"capability": "(urn:sal:restconf:event:subscription?revision=2014-07-08)sal-remote-augment"
},

"capability-origin": "device-advertised",
},

"capability-origin": "device-advertised",
},

"capability-origin": "device-advertised",
},

"capability-origin": "device-advertised",
},

"capability-origin": "device-advertised",
},

"capability-origin": "device-advertised",
},

"capability-origin": "device-advertised",
},

"capability-origin": "device-advertised",
<table>
<thead>
<tr>
<th>Capability Origin</th>
<th>Capability</th>
</tr>
</thead>
</table>
| `device-advertised` | }
d. Using NETCONF, let's get the current streams being active in our Packet Generator. The number of streams will change along the time, this is the result of close-loop policy. When the traffic goes over a certain threshold, DCAE will publish an event on the unauthenticated DCAE_CL_OUTPUT topic that will be picked up by APPC, that will send a NETCONF request to the packet generator to adjust the traffic it's sending.
4. Browse to the sdfw1fw1101snk01 on port 667 to see a graph representing the traffic being received:

http://<zdfw1fw1101snk01>:667/

As you can see in the below graph, looking at the top right square, we can see the first two fluctuations are going from very low to very high. This is when close-loop isn’t running. Once close-loop is running, you’ll have some medium bars.

5. Check the events sent by Virtual Event Collector (VES) to Threshold Crossing Analytic (TCA) app:

```
curl -X GET
   http://<K8S_IP>:3904/events/unauthenticated.SEC_MEASUREMENT_OUTPUT/group1/C1
   -H 'Accept: application/json' 
   -H 'Content-Type: application/cambria'
```

The VES resides in the VNF itself, whereas the TCA is an application running on Cask. A DCAE component.

6. Check the events sent by TCA on unauthenticated.DCAE_CL_OUTPUT:

```
curl -X GET
   http://<K8S_IP>:3904/events/unauthenticated.DCAE_CL_OUTPUT/group1/C1
   -H 'Accept: application/json' 
   -H 'Content-Type: application/cambria'
```

Those events are the resulting of the TCA application, e.g. TCA has noticed an event was crossing a given threshold, hence is sending a message of that particular topic. Then Policy will grab this event and perform the appropriate action, as defined in the Policy. In the case of vFWCL, Policy will send an event on the APPC_CL topic, that APPC will consume. This will trigger a NETCONF request to the packet generator to adjust the traffic.

I hope everything worked for you, if not, please leave a comment. Thanks