Cisco Advanced Security in ACI – Lab 2.0 – LTRSEC-3001 CL17-Berlin

- FTD Device Package GoTo L2 Attached Service Graph
- ASA Device Package L3outs and PBR Service Graphs

https://github.com/cisco-security/aci-scripts/tree/master/pod3-lab2.0-asa-ftd-graphs

The python scripts included in the GitHub build a Tenant pod3 with its three service graphs. Please refer to below diagram of the tenant for better understanding of this description. ASA5525-X model in multi-context mode is used and one of the contexts is allocated to this service graph. The user context is registered and used with a managed (service policy model). Web-to-app uses a set of ASA5525-X appliances in a cluster mode while app-to-db uses a set of ASA5525-X appliances in Failover mode.

1. app-to-db contract adds FTDv in L3FW mode L2 attached to app and db EPGs. This service graph uses a hybrid managed model with APIC communicating to FMC via REST-APIs, and configuring a registered FTD appliances. Once configured according to APIC L4-L7 device parameters, APIC tells FMC to deploy this config to FTD
2. web-to-app contract adds a PBR service graph, using one-arm model in communication path between web and app EPGs inside the same 'web' Bridge Domain.
3. Finally, out-to-web contract adds ASA L3FW L3 attached with OSPF L3outs between campus network (outside) and web EPG, which has an SVI in its Bridge Domain.

The rebuild-mypod.bash script is a wrapper around all the python scripts that in proper order orchestrate this tenant with its service graphs. Each python script will print the XML sent to APIC.

The python scripts depend on underlying pre-configured settings to execute properly. Those would have to be updated to match the new APIC env you plan to deploy this in. Such items include names of: VVM and physical domains, imported ASA device package, pre-configured vPC (if used for ASA data plane), etc. ASAv appliance can be used in this case as well, which would eliminate the need for a physical domain currently used under device registration.

Here are some examples of the items you will need to update:

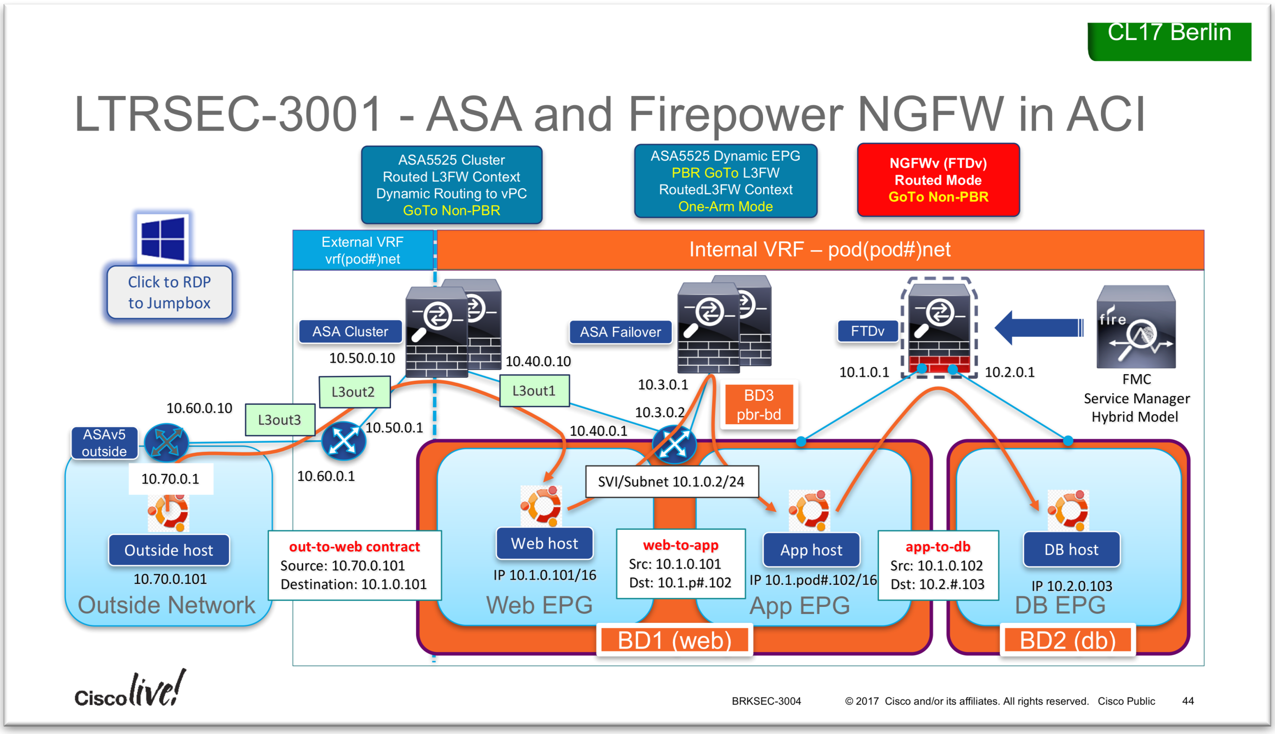
```
egrep 'vmm1|Phy|vpc|asa_fover' *
faba-asa-cluster-pods.py:    vnsRsALDevToPhysDomP =
cobra.model.vns.RsALDevToPhysDomP(vnsLDevVip, tDn=u'uni/phys-asa_phys')
faba-asa-cluster-pods.py:    vnsRsCIfPathAtt2 = cobra.model.vns.RsCIfPathAtt(vnsCIf2,
tDn=u'topology/pod-1/protpaths-101-102/pathep-[vpc_aaep_asa1-asa2]' )
faba-asa-pbr-device.py:    vnsRsALDevToPhysDomP =
cobra.model.vns.RsALDevToPhysDomP(vnsLDevVip, tDn=u'uni/phys-asa_fover')
faba-ftdv-dev.py:    vnsRsALDevToDomP = cobra.model.vns.RsALDevToDomP(vnsLDevVip,
tDn=u'uni/vmmp-VMware/dom-lab_vmm1')
```

```
faba-ftdv-dev.py:    vnsRsCDevToCtrlrP = cobra.model.vns.RsCDevToCtrlrP(vnsCDev,
tDn=u'uni/vmmp-VMware/dom-lab_vmm1/ctrlr-VC1')
faba-l3out.py:    l3extRsPathL3OutAtt = cobra.model.l3ext.RsPathL3OutAtt(l3extLIfP,
addr=u'0.0.0.0', descr=u'', encapScope=u'local', targetDscp=u'unspecified', llAddr=u'::',
mac=u'00:22:BD:F8:19:FF', mode=u'regular', encap=u'vlan-%d' % l3out1_vlan, ifInstT=u'ext-svi',
mtu=u'1500', tDn=u'topology/pod-1/protpaths-101-102/pathep-[vpc_aaep_asa1-asa2]')
faba-tenant-apps.py:    fvRsDomAtt = cobra.model.fv.RsDomAtt(fvAEPg, instrImedcy=u'lazy',
resImedcy=u'lazy', encap=u'unknown', tDn=u'uni/vmmp-VMware/dom-lab_vmm1')
```

Please refer this YouTube link for an instructional video and demo:

Advanced Security in ACI - 2.0 Training Lab and Demo:
http://cs.co/csco-security-in-aci-demo

Here is the diagram used in this lab/demo:



CL17 Berlin

LTRSEC-3001 - ASA and Firepower NGFW in ACI

BRKSEC-3004   © 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public   44